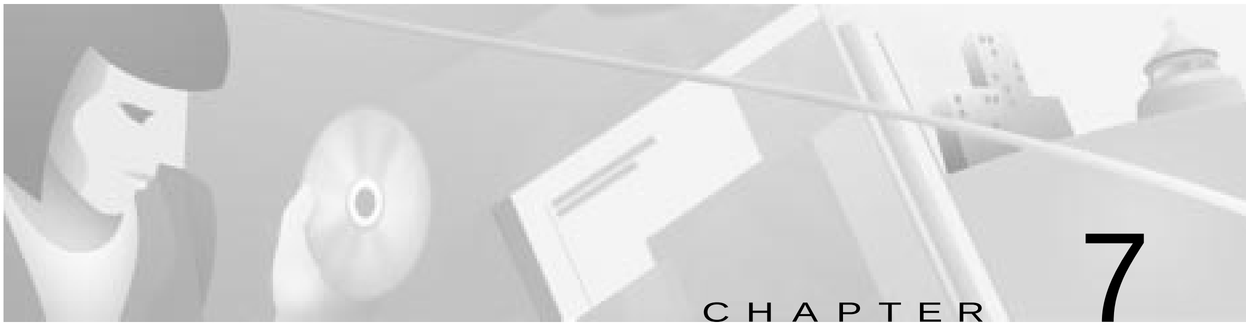


CHAPTER 7

Tunneling Protocols

Tunneling protocols are the heart of virtual private networking. The tunnels make it possible to use a public TCP/IP network, such as the Internet, to create secure connections between remote users and a private corporate network.

The secure connection is called a tunnel, and the VPN 3000 Concentrator Series uses tunneling protocols to:

- Negotiate tunnel parameters.
- Establish tunnels.
- Authenticate users and data.
- Manage security keys.
- Encrypt and decrypt data.
- Manage data transfer across the tunnel.
- Manage data transfer inbound and outbound as a tunnel endpoint or router.

The VPN Concentrator functions as a bidirectional tunnel endpoint: it can receive plain packets from the private network, encapsulate them, create a tunnel, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination; or it can receive encapsulated packets from the public network, unencapsulate them, and send them to their final destination on the private network.

The VPN Concentrator supports the three most popular VPN tunneling protocols:

- PPTP: Point-to-Point Tunneling Protocol.
- L2TP: Layer 2 Tunneling Protocol.
- IPSec: IP Security Protocol.

It also supports L2TP over IPSec, which provides interoperability with the Windows 2000 VPN client. The VPN Concentrator is also interoperable with other clients that conform to L2TP/IPSec standards, but it does not formally support those clients.

This section explains how to configure the system-wide parameters for PPTP and L2TP, how to configure IPSec LAN-to-LAN connections, and how to configure IKE proposals for IPSec Security Associations and LAN-to-LAN connections.

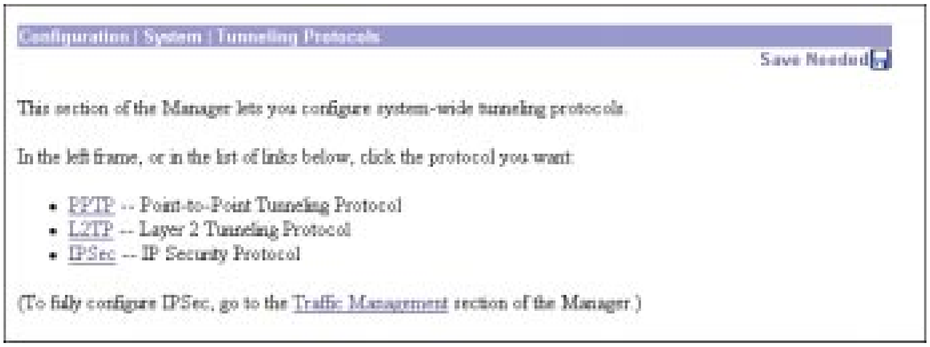
To configure L2TP over IPSec, see **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals**, and **Configuration | User Management**.

Configuration | System | Tunneling Protocols

This section of the Manager lets you configure system-wide parameters for tunneling protocols.

- **PPTP**: Configure PPTP parameters.
- **L2TP**: Configure L2TP parameters.
- **IPSec**: Configure IPSec parameters and connections.
  - **LAN-to-LAN**: IPSec LAN-to-LAN connections between two VPN Concentrators (or between the VPN Concentrator and another secure gateway).
  - **IKE Proposals**: IKE proposals for IPSec Security Associations and LAN-to-LAN connections.

Figure 1 Configuration | System | Tunneling Protocols screen



Configuration | System | Tunneling Protocols

This section of the Manager lets you configure system-wide tunneling protocols.

In the left frame, or in the list of links below, click the protocol you want:

- PPTP -- Point-to-Point Tunneling Protocol
- L2TP -- Layer 2 Tunneling Protocol
- IPSec -- IP Security Protocol

(To fully configure IPSec, go to the Traffic Management section of the Manager.)

Configuration | System | Tunneling Protocols | PPTP

This screen lets you configure system-wide PPTP (Point-to-Point Tunneling Protocol) parameters.

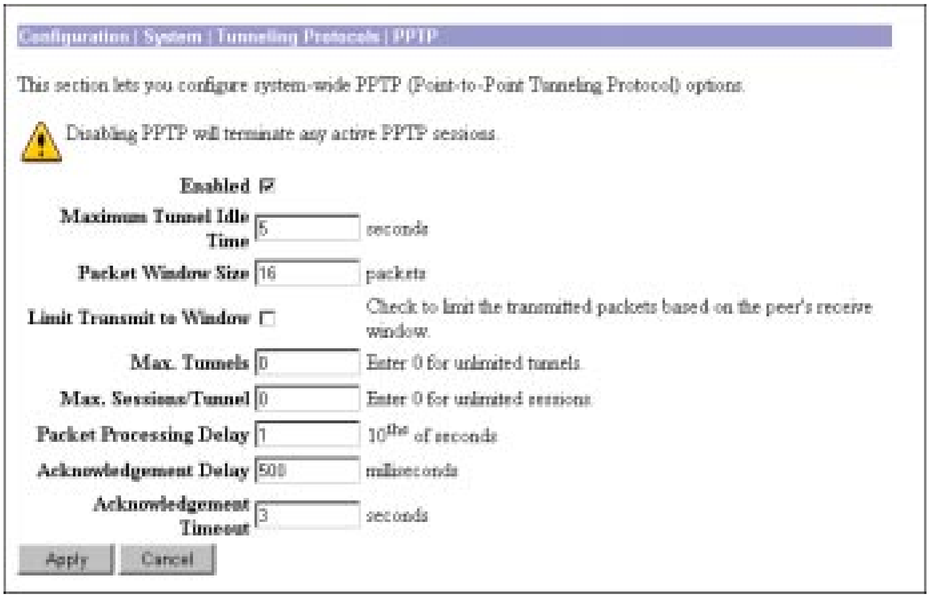
The PPTP protocol defines mechanisms for establishing and controlling the tunnel, but uses Generic Routing Encapsulation (GRE) for data transfer.

PPTP is a client-server protocol. The VPN Concentrator always functions as a PPTP Network Server (PNS) and supports remote PC clients. The PPTP tunnel extends all the way from the PC to the VPN Concentrator.

PPTP is popular with Microsoft clients. Microsoft Dial-Up Networking (DUN) 1.2 and 1.3 under Windows 95/98 support it, as do versions of Windows NT 4.0 and Windows 2000. PPTP is typically used with Microsoft encryption (MPPE).

You can configure PPTP on rules in filters; see **Configuration | Policy Management | Traffic Management**. Groups and users also have PPTP parameters; see **Configuration | User Management**.

Figure 2 Configuration | System | Tunneling Protocols | PPTP screen



Configuration | System | Tunneling Protocols | PPTP

This section lets you configure system-wide PPTP (Point-to-Point Tunneling Protocol) options.

Disabling PPTP will terminate any active PPTP sessions.

Enabled	☑	
Maximum Tunnel Idle Time	5	seconds
Packet Window Size	16	packets
Limit Transmit to Window	□	Check to limit the transmitted packets based on the peer's receive window.
Max. Tunnels	0	Enter 0 for unlimited tunnels.
Max. Sessions/Tunnel	0	Enter 0 for unlimited sessions.
Packet Processing Delay	1	10ths of seconds
Acknowledgement Delay	500	milliseconds
Acknowledgement Timeout	3	seconds

Note Cisco supplies default settings for PPTP parameters that ensure optimum performance for typical VPN use. We strongly recommend that you not change the defaults without advice from Cisco personnel.

Enabled

Check the box to enable PPTP system-wide functions on the VPN Concentrator, or clear it to disable. The box is checked by default.

Warning **Disabling PPTP terminates any active PPTP sessions.**

Maximum Tunnel Idle Time

Enter the time in seconds to wait before disconnecting an established PPTP tunnel with no active sessions. An open tunnel consumes system resources. Enter `0` to disconnect the tunnel immediately after the last session terminates (no idle time). Maximum is `86400` seconds (24 hours). The default is `5` seconds.

Packet Window Size

Enter the maximum number of received but unacknowledged PPTP packets that the system can buffer. The system must queue unacknowledged PPTP packets until it can process them. Minimum is `0`, maximum is `32`, default is `16` packets.

Limit Transmit to Window

Check the box to limit the number of transmitted PPTP packets to the client’s packet window size. Ignoring the window improves performance, provided that the client can ignore the window violation. The box is not checked by default.

Max. Tunnels

Enter the maximum allowed number of simultaneously active PPTP tunnels. Minimum is `0`, maximum depends on the VPN Concentrator model; e.g., Model 3060 = `5000`. Enter `0` for unlimited tunnels (the default).

Max. Sessions/Tunnel

Enter the maximum number of sessions allowed per PPTP tunnel. Minimum is `0`, maximum depends on the VPN Concentrator model; e.g., Model 3060 = `5000`. Enter `0` for unlimited sessions (the default).

Packet Processing Delay

Enter the packet processing delay for PPTP flow control. This parameter is sent to the client in a PPTP control packet. Entries are in units of 100 milliseconds (0.1 second). Maximum is `65535`; default is `1` (0.1 second).

Acknowledgement Delay

Enter the number of milliseconds that the VPN Concentrator will wait to send an acknowledgement to the client when there is no data packet on which to piggyback an acknowledgement. Enter `0` to send an immediate acknowledgement. Minimum delay is `50`, maximum is `5000`, default is `500` milliseconds.

Acknowledgement Timeout

Enter the number of seconds to wait before determining that an acknowledgement has been lost; i.e., before resuming transmission to the client even though the transmit window is closed. Minimum is `1`, maximum is `10`, default is `3` seconds.

Apply / Cancel

To apply your PPTP settings and to include them in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Tunneling Protocols** screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Tunneling Protocols** screen.

Configuration | System | Tunneling Protocols | L2TP

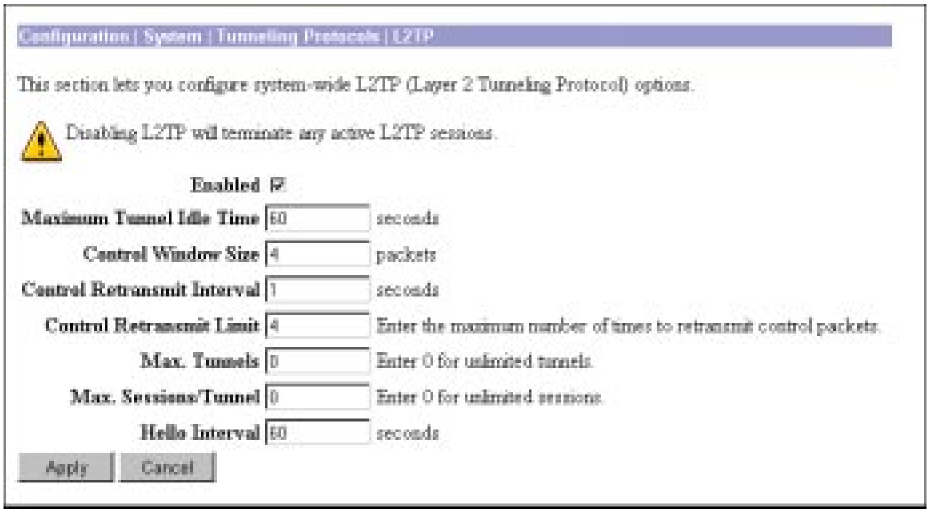
This screen lets you configure system-wide L2TP (Layer 2 Tunneling Protocol) parameters.

L2TP is a client-server protocol. It combines many features from PPTP and L2F (Layer 2 Forwarding), and is regarded as a successor to both. The L2TP protocol defines mechanisms both for establishing and controlling the tunnel and for transferring data.

The VPN Concentrator always functions as a L2TP Network Server (LNS) and supports remote PC clients. The L2TP tunnel extends all the way from the PC to the VPN Concentrator. When the client PC is running Windows 2000, the L2TP tunnel is typically layered over an IPSec transport connection.

You can configure L2TP on rules in filters; see **Configuration | Policy Management | Traffic Management**. Groups and users also have L2TP parameters; see **Configuration | User Management**.

Figure 3 Configuration | System | Tunneling Protocols | L2TP screen



Configuration | System | Tunneling Protocols | L2TP

This section lets you configure system-wide L2TP (Layer 2 Tunneling Protocol) options.

Disabling L2TP will terminate any active L2TP sessions.

Enabled ☑

Maximum Tunnel Idle Time 60 seconds

Control Window Size 4 packets

Control Retransmit Interval 1 seconds

Control Retransmit Limit 4 Enter the maximum number of times to retransmit control packets.

Max. Tunnels 0 Enter 0 for unlimited tunnels.

Max. Sessions/Tunnel 0 Enter 0 for unlimited sessions.

Hello Interval 60 seconds

Note Cisco supplies default settings for L2TP parameters that ensure optimum performance for typical VPN use. We strongly recommend that you not change the defaults without advice from Cisco personnel.

Enabled

Check the box to enable L2TP system-wide functions on the VPN Concentrator, or clear it to disable. The box is checked by default.

Warning **Disabling L2TP terminates any active L2TP sessions.**

Maximum Tunnel Idle Time

Enter the time in seconds to wait before disconnecting an established L2TP tunnel with no active sessions. An open tunnel consumes system resources. Enter `0` to disconnect the tunnel immediately after the last session terminates (no idle time). Maximum is `86400` seconds (24 hours). The default is `60` seconds.

Control Window Size

Enter the maximum number of unacknowledged L2TP control channel packets that the system can receive and buffer. Minimum is `1`, maximum is `16`, and default is `4` packets.

Control Retransmit Interval

Enter the time in seconds to wait before retransmitting an unacknowledged L2TP tunnel control message to the remote client. Minimum is `1` (the default), and maximum is `10` seconds.

Control Retransmit Limit

Enter the number of times to retransmit L2TP tunnel control packets before assuming that the remote client is no longer responding. Minimum is `1`, maximum is `32`, and default is `4` times.

Max. Tunnels

Enter the maximum allowed number of simultaneously active L2TP tunnels. Minimum is `0`, maximum depends on the VPN Concentrator model; e.g., Model 3060 = `5000`. Enter `0` for unlimited tunnels (the default).

Max. Sessions/Tunnel

Enter the maximum number of sessions allowed per L2TP tunnel. Minimum is `0`, maximum depends on the VPN Concentrator model; e.g., Model 3060 = `5000`. Enter `0` for unlimited sessions (the default).

Hello Interval

Enter the time in seconds to wait when the L2TP tunnel is idle (no control or payload packets received) before sending a Hello (or “keep-alive”) packet to the remote client. Minimum is `1`, maximum is `3600`, and default is `60` seconds.

Apply / Cancel

To apply your L2TP settings and to include them in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Tunneling Protocols** screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Tunneling Protocols** screen.

Configuration | System | Tunneling Protocols | IPSec

This section of the Manager lets you configure IPSec LAN-to-LAN connections, and IKE (Internet Key Exchange) parameters for IPSec Security Associations and LAN-to-LAN connections.

IPSec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol. Both LAN-to-LAN connections and client-to-LAN connections can use IPSec.

In IPSec terminology, a “peer” is a remote-access client or another secure gateway. During tunnel establishment under IPSec, the two peers negotiate Security Associations that govern authentication, encryption, encapsulation, key management, etc. These negotiations involve two phases: first, to establish the tunnel (the IKE SA); and second, to govern traffic within the tunnel (the IPSec SA).

In IPSec LAN-to-LAN connections, the VPN Concentrator can function as initiator or responder. In IPSec client-to-LAN connections, the VPN Concentrator functions only as responder. Initiators propose SAs; responders accept, reject, or make counter-proposals—all according to configured SA parameters. To establish a connection, both entities must agree on the SAs.

The Cisco VPN Client complies with the IPSec protocol and is specifically designed to work with the VPN Concentrator. However, the VPN Concentrator can establish IPSec connections with many protocol-compliant clients. Likewise, the VPN Concentrator can establish LAN-to-LAN connections with other protocol-compliant VPN devices (often called “secure gateways”).

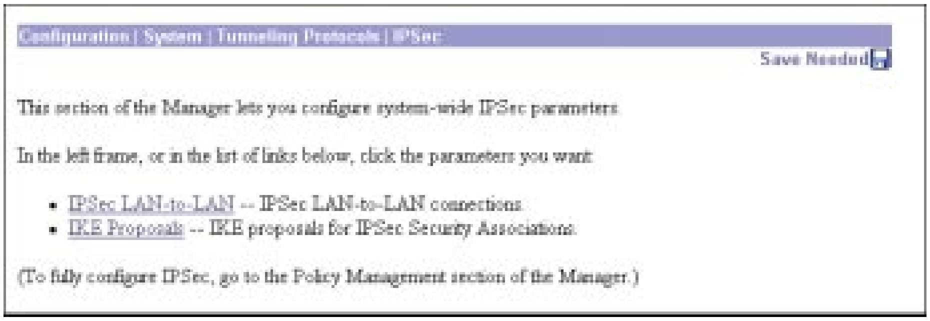
The Cisco VPN Client supports these IPSec attributes:

- Main mode for negotiating phase one ISAKMP Security Associations (SAs) when using digital certificates for authentication
- Aggressive mode for negotiating phase one ISAKMP Security Associations (SAs) when using preshared keys for authentication
- Authentication Algorithms:
  - ESP-MD5-HMAC-128
  - ESP-SHA1-HMAC-160
- Authentication Modes:
  - Preshared Keys
  - X.509 Digital Certificates
- Diffie-Hellman Groups 1 and 2
- Encryption Algorithms:
  - DES-56
  - 3DES-168
  - ESP-NULL
- Extended Authentication (XAuth)
- Mode Configuration (also known as ISAKMP Configuration Method)

- Tunnel Encapsulation Mode

You configure IKE proposals (parameters for the IKE SA) here. You apply them to IPSec LAN-to-LAN connections in this section, and to IPSec SAs on the **Configuration | Policy Management | Traffic Management | Security Associations** screens. Therefore, you should configure IKE proposals before configuring other IPSec parameters. Cisco supplies default IKE proposals that you can use or modify.

Figure 4 Configuration | System | Tunneling Protocols | IPSec screen



Configuration | System | Tunneling Protocols | IPSec

This section of the Manager lets you configure system-wide IPSec parameters.

In the left frame, or in the list of links below, click the parameters you want:

- IPSec LAN-to-LAN -- IPSec LAN-to-LAN connections.
- IKE Proposals -- IKE proposals for IPSec Security Associations.

(To fully configure IPSec, go to the Policy Management section of the Manager.)

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

This section of the Manager lets you configure, add, modify, and delete IPSec LAN-to-LAN connections between two VPN Concentrators.

While the VPN Concentrator can establish LAN-to-LAN connections with other protocol-compliant VPN secure gateways, these instructions assume VPN Concentrators on both sides. And here, the “peer” is the other VPN Concentrator or secure gateway.

In a LAN-to-LAN connection, IPSec creates a tunnel between the public interfaces of two VPN Concentrators, which correspondingly route secure traffic to and from many hosts on their private LANs. There is no user configuration or authentication in a LAN-to-LAN connection; all hosts configured on the private networks can access hosts on the other side of the connection, at any time.

If you have a WAN connection as the public interface, you still use this section to configure a LAN-to-WAN connection.

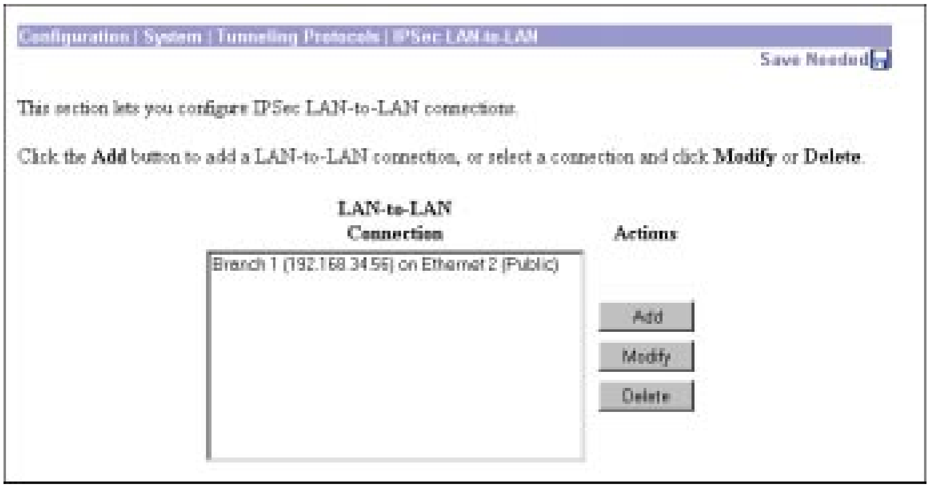
To fully configure a LAN-to-LAN connection, you must configure identical basic IPSec parameters on both VPN Concentrators, and configure mirror-image private network addresses or network lists.

The VPN Concentrator also provides a network autodiscovery feature that dynamically discovers and updates the private network addresses on each side of the LAN-to-LAN connection, so you don’t have to explicitly configure them. This feature works only when both devices are VPN Concentrators and both VPN Concentrators have routing enabled on the private interface. However, network autodiscovery is not allowed on a WAN interface.

You must configure a public interface on the VPN Concentrator before you can configure an IPSec LAN-to-LAN connection. See the **Configuration | Interfaces** screens. You must also configure IKE proposals before configuring LAN-to-LAN connections. See the **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals** screens.

You can configure only one LAN-to-LAN connection with each VPN Concentrator (or other secure gateway) peer.

Figure 5 Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN screen



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

Save Needed

This section lets you configure IPSec LAN-to-LAN connections.

Click the **Add** button to add a LAN-to-LAN connection, or select a connection and click **Modify** or **Delete**.

LAN-to-LAN Connection

The **LAN-to-LAN Connection** list shows connections that have been configured. The connections are listed in the order you configure them, in the format: `Name (Peer IP Address) on Interface`; for example, `Branch 1 (192.168.34.56) on Ethernet 2 (Public)`. If no connections have been configured, the list shows **--Empty--**.

Add / Modify / Delete

To configure and add a new connection, click **Add**. See the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add** screen. If you have not configured a public interface, the Manager displays the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | No Public Interfaces** screen.

To modify the parameters of a configured connection, select the connection from the list and click **Modify**. See the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Modify** screen.

To delete a configured connection, select the connection from the list and click **Delete**. *There is no confirmation or undo.* The Manager deletes the connection, its LAN-to-LAN filter rules, SAs, and group. The Manager then refreshes the screen and shows the remaining connections in the list.

Warning **Deleting a connection immediately deletes any tunnels—and user sessions—using that connection.**

Reminder:

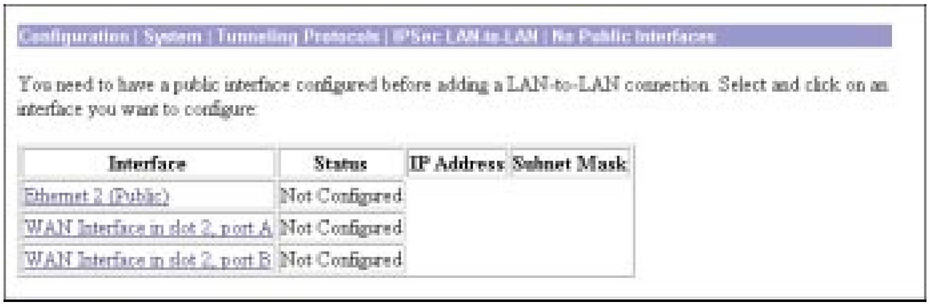
The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

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

The Manager displays this screen if you have not configured a public interface on the VPN Concentrator and you try to add an IPSec LAN-to-LAN connection. The public interface need not be enabled, but it must be configured with an IP address and the **Public Interface** parameter enabled.

You should designate only one VPN Concentrator interface as a public interface.

Figure 6 Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | No Public Interfaces screen



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

You need to have a public interface configured before adding a LAN-to-LAN connection. Select and click on an interface you want to configure:

Interface	Status	IP Address	Subnet Mask
Ethernet 2 (Public)	Not Configured		
WAN Interface in slot 2, port A	Not Configured		
WAN Interface in slot 2, port B	Not Configured		

Click the highlighted link to configure the desired public interface. The Manager opens the appropriate **Configuration | Interfaces** screen.

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

These screens let you:

- **Add**: Configure and add a new IPSec LAN-to-LAN connection.
- **Modify**: Modify parameters of a configured IPSec LAN-to-LAN connection.

You must configure a public interface on the VPN Concentrator before you can configure an IPSec LAN-to-LAN connection. See the **Configuration | Interfaces** screens.

You can configure only one LAN-to-LAN connection with each VPN Concentrator (or other secure gateway) peer.

The maximum number of LAN-to-LAN connections supported is determined by the hardware and is model-dependent.

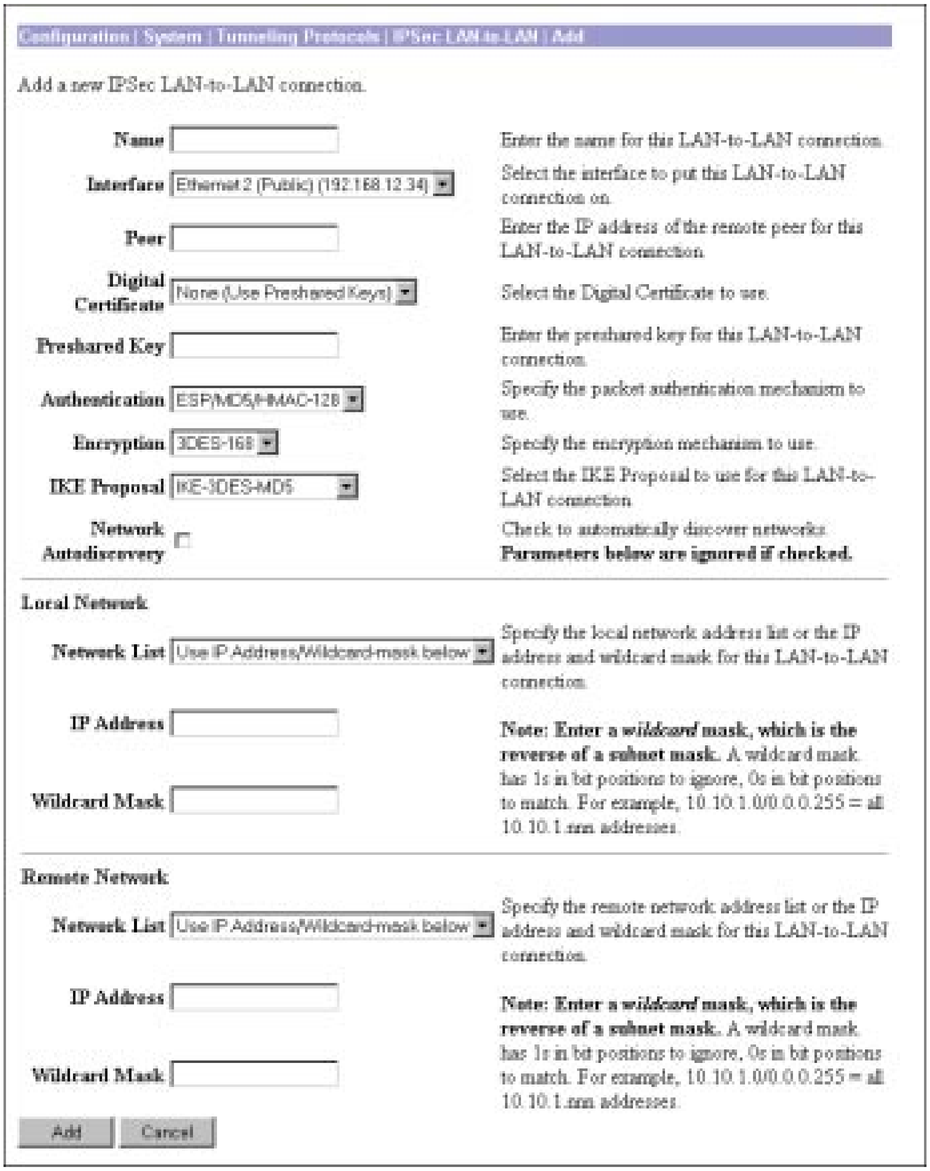
Table 1 Maximum LAN-to-LAN connections for each VPN Concentrator model

VPN Concentrator Model	Maximum Number of Sessions
3005	100
3015	100
3030	500

Table 1 Maximum LAN-to-LAN connections for each VPN Concentrator model

VPN Concentrator Model	Maximum Number of Sessions
3060	1,000
3080	1,000

Figure 7 Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add or Modify screen



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

Add a new IPSec LAN-to-LAN connection.

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

Local Network

Network List	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.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet mask.** 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.nnn addresses.
Wildcard Mask		

Remote Network

Network List	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.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet mask.** 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.nnn addresses.
Wildcard Mask		

When you **Add** or **Modify** a connection on these screens, the VPN Concentrator automatically:

- Creates or modifies two filter rules with the **Apply IPSec** action: one inbound, one outbound, named `L2L:<`*`Name`*`> In` and `L2L:<`*`Name`*`> Out`.
- Creates or modifies an IPSec Security Association named `L2L:<`*`Name`*`>`.
- Applies these rules to the filter on the public interface and applies the SA to the rules. If the public interface doesn't have a filter, it applies the Public (default) filter with the rules above.

- Creates or modifies a group named with the **Peer** IP address. If the VPN Concentrator internal authentication server hasn't been configured, it does so, and adds the group to the database.

All of the rules, SAs, filters, and group have default parameters or those specified on this screen. You can modify the rules and SA on the **Configuration | Policy Management | Traffic Management** screens, the group on the **Configuration | User Management | Groups** screens, and the interface on the **Configuration | Interfaces** screens. However, we recommend that you keep the configured defaults. You cannot delete these rules, SAs, or group individually; the system automatically deletes them when you delete the LAN-to-LAN connection.

To fully configure a LAN-to-LAN connection, you must configure identical IPSec LAN-to-LAN parameters on both VPN Concentrators, and configure mirror-image local and remote private network addresses. For example:

Configure	On this VPN Concentrator	On peer VPN Concentrator
Local Network	`10.10.0.0/0.0.255.255`	`11.0.0.0/0.255.255.255`
Remote Network	`11.0.0.0/0.255.255.255`	`10.10.0.0/0.0.255.255`

If you use network lists, you must also configure and apply them as mirror images on the two VPN Concentrators. If you use network autodiscovery, you must use it on both VPN Concentrators.

Warning **On the Modify screen, any changes take effect as soon as you click Apply. If client sessions are using this connection, changes delete the tunnel—and the sessions—without warning.**

Name

Enter a unique descriptive name for this connection. Maximum 32 characters. Since the created rules and SA use this name, we recommend that you keep it short.

Interface

Add screen:

- Click the drop-down menu button and select the configured public interface on this VPN Concentrator for this end of the LAN-to-LAN connection. The list shows all interfaces (Ethernet or WAN) that have the **Public Interface** parameter enabled. See **Configuration | Interfaces**.

Modify screen:

- The screen shows the configured public interface on this VPN Concentrator for this end of the LAN-to-LAN connection. You cannot change the interface. To move the connection to another interface, you must delete this connection and add a new one for the other interface.

Peer

Enter the IP address of the remote peer in the LAN-to-LAN connection. This must be the IP address of the public interface on the peer VPN Concentrator. Use dotted decimal notation; e.g., `192.168.34.56`.

Digital Certificate

This parameter specifies whether to use preshared keys or a PKI (Public Key Infrastructure) digital identity certificate to authenticate the peer during Phase 1 IKE negotiations. See the discussion under **Administration | Certificate Management**.

Click the drop-down menu button and select the option. The list shows any digital certificates that have been installed, plus:

- **None (Use Preshared Keys)** = Use only preshared keys to authenticate the peer during Phase 1 IKE negotiations. This is the default selection.

Preshared Key

Enter a preshared key for this connection. Use a minimum of 4, a maximum of 32 alphanumeric characters; e.g, `sZ9s14ep7`. The system displays your entry in clear text.

This key becomes the password for the IPSec LAN-to-LAN group that is created, and you must enter the same key on the peer VPN Concentrator. (This is *not* a manual encryption or authentication key. The system automatically generates those session keys.)

Authentication

This parameter specifies the data, or packet, authentication algorithm. Packet authentication proves that data comes from whom you think it comes from; it is often referred to as “data integrity” in VPN literature. The IPSec ESP (Encapsulating Security Payload) protocol provides both encryption and authentication.

Click the drop-down menu button and select the algorithm:

- **None** = No data authentication.
- **ESP/MD5/HMAC-128** = ESP protocol using HMAC (Hashed Message Authentication Coding) with the MD5 hash function using a 128-bit key. This is the default selection.
- **ESP/SHA/HMAC-160** = ESP protocol using HMAC with the SHA-1 hash function using a 160-bit key. This selection is more secure but requires more processing overhead.

Encryption

This parameter specifies the data, or packet, encryption algorithm. Data encryption makes the data unreadable if intercepted.

Click the drop-down menu button and select the algorithm:

- **Null** = Use ESP without encryption; no packet encryption.
- **DES-56** = Use DES encryption with a 56-bit key.
- **3DES-168** = Use Triple-DES encryption with a 168-bit key. This selection is the most secure and it is the default selection.

IKE Proposal

This parameter specifies the set of attributes for Phase 1 IPSec negotiations, which are known as IKE proposals. See the **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals** screen. You must configure, activate, and prioritize IKE proposals before configuring LAN-to-LAN connections.

Click the drop-down menu button and select the IKE proposal. The list shows only active IKE proposals in priority order. Cisco-supplied default active proposals are:

- **CiscoVPNClient-3DES-MD5** = Use preshared keys (XAUTH) and MD5/HMAC-128 for authentication. Use 3DES-168 encryption. Use D-H Group 2 to generate SA keys. This selection allows XAUTH user-based authentication and is the default.
- **IKE-3DES-MD5** = Use preshared keys and MD5/HMAC-128 for authentication. Use 3DES-168 encryption. Use D-H Group 2 to generate SA keys.
- **IKE-3DES-MD5-DH1** = Use preshared keys and MD5/HMAC-128 for authentication. Use 3DES-168 encryption. Use D-H Group 1 to generate SA keys. This selection is compatible with the Cisco VPN 3000 Client.
- **IKE-DES-MD5** = Use preshared keys and MD5/HMAC-128 for authentication. Use DES-56 encryption. Use D-H Group 1 to generate SA keys. This selection is compatible with the Cisco VPN 3000 Client.
- **IKE-3DES-MD5-DH7** = Use preshared keys and MD5/HMAC-128 for authentication. Use 3DES-168 encryption. Use D-H Group 7 (ECC) to generate SA keys. This IKE proposal is intended for use with the movianVPN client; it can also be used with any peer that supports ECC groups for D-H.

Network Autodiscovery

Check this box to use the VPN Concentrator network autodiscovery feature that dynamically discovers and continuously updates the private network addresses on each side of the LAN-to-LAN connection. This feature uses RIP, and **Inbound RIP RIPv2/v1** must be enabled on the Ethernet 1 (Private) interface of both VPN Concentrators. See **Configuration | Interfaces**. If you check this box, skip the **Local** and **Remote Network** parameters below; they are ignored.

Network autodiscovery is not allowed on a WAN interface.

Local Network

These entries identify the private network—*on this VPN Concentrator*—whose hosts can use the LAN-to-LAN connection. These entries must match those in the **Remote Network** section on the peer VPN Concentrator.

Network List

Click the drop-down menu button and select the configured network list that specifies the local network addresses. A network list is a list of network addresses that are treated as a single object. See the **Configuration | Policy Management | Traffic Management | Network Lists** screens. Otherwise, you can select:

- **Use IP Address/Wildcard-mask below**, which lets you enter a network address.
- **Create new Network List** (on **Add** screen only), which lets you create a network list of local network addresses. The Manager automatically opens the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Local Network List** screen when you click **Add**; see description below.

If you select a configured network list, the Manager ignores entries in the **IP Address** and **Wildcard Mask** fields.

Note An IP address is used with a *wildcard mask* to provide the desired granularity. *A wildcard mask is the reverse of a subnet mask*; i.e., the wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example:
`0.0.0.0/255.255.255.255` = any address
`10.10.1.35/0.0.0.0` = only `10.10.1.35`
`10.10.1.35/0.0.0.255` = all `10.10.1.nnn` addresses

IP Address

Enter the IP address of the private local network on this VPN Concentrator. Use dotted decimal notation; e.g., `10.10.0.0`.

Wildcard Mask

Enter the wildcard mask for the private local network. Use dotted decimal notation; e.g., `0.0.255.255`. The system supplies a default wildcard mask appropriate to the IP address class.

Remote Network

These entries identify the private network—*on the remote peer VPN Concentrator*—whose hosts can use the LAN-to-LAN connection. These entries must match those in the **Local Network** section on the peer VPN Concentrator.

Network List

Click the drop-down menu button and select the configured network list that specifies the remote network addresses. A network list is a list of network addresses that are treated as a single object. See the **Configuration | Policy Management | Traffic Management | Network Lists** screens. Otherwise, you can select:

- **Use IP Address/Wildcard-mask below**, which lets you enter a network address.
- **Create new Network List** (on **Add** screen only), which lets you create a network list of remote network addresses. The Manager automatically opens the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Remote Network List** screen when you click **Add**; see description below.

If you select a configured network list, the Manager ignores entries in the **IP Address** and **Wildcard-mask** fields.

See the *wildcard mask* note above.

IP Address

Enter the IP address of the private network on the remote peer VPN Concentrator. Use dotted decimal notation; e.g. `11.0.0.1`.

Wildcard Mask

Enter the wildcard mask for the private remote network. Use dotted decimal notation; e.g., `0.255.255.255`. The system supplies a default wildcard mask appropriate to the IP address class.

Add or Apply / Cancel

- **Add** screen: To add this connection to the list of configured LAN-to-LAN connections, click **Add**. If you are creating new network lists, the Manager automatically displays the appropriate **Local** or **Remote Network List** screens. Otherwise, the Manager displays the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done** screen.
- **Modify** screen: To apply your changes to this LAN-to-LAN connection, click **Apply**. *Any changes take effect as soon as you click* **Apply**. *If client sessions are using this connection, changes delete the tunnel—and the sessions—without warning. The* Manager returns to the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN** screen.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN** screen, and the **LAN-to-LAN Connection** list is unchanged.

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Local or Remote Network List

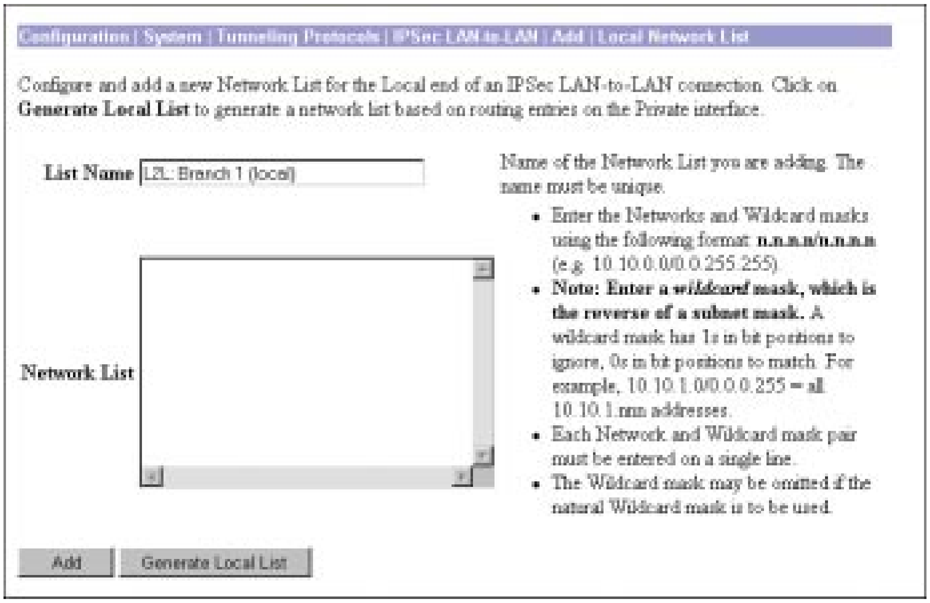
These screens let you configure and add network lists for the **Local Network** or **Remote Network** of a new IPSec LAN-to-LAN connection. The Manager automatically opens these screens if you select **Create new Network List** under **Network List** on the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add** screen.

A network list is a list of network addresses that are treated as a single object. See the **Configuration | Policy Management | Traffic Management | Network Lists** screens also.

On the **Local Network List** screen, the Manager can automatically generate a network list using the valid network routes in the routing table for the Ethernet 1 (Private) interface of this VPN Concentrator. (See **Monitoring | Routing Table**.)

A single network list can contain a maximum of 200 network entries.

Figure 8 Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Local or Remote Network List screen



Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Local Network List

Configure and add a new Network List for the Local end of an IPSec LAN-to-LAN connection. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name L2L: Branch 1 (local)

Name of the Network List you are adding. The name must be unique.

Network List

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a *wildcard* mask, which is the reverse of a subnet mask.** 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.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

List Name

The Manager supplies a default name that identifies the list as a LAN-to-LAN local or remote list, which we recommend you keep. Otherwise, enter a unique name for this network list. Maximum 48 characters, case-sensitive. Spaces are allowed.

If you use the **Generate Local List** feature on the **Local Network List** screen, edit this name *after* the system generates the network list.

Network List

Enter the networks in this network list. Enter each network on a single line using the format `n.n.n.n/w.w.w.w`, where `n.n.n.n` is a network IP address and `w.w.w.w` is a wildcard mask.

Note Enter a *wildcard mask*, which is the reverse of a subnet mask. 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.nnn` addresses.

If you omit the wildcard mask, the Manager supplies the default wildcard mask for the class of the network address. For example, `192.168.12.0` is a Class C address, and default wildcard mask is `0.0.0.255`.

You can enter a maximum of 200 networks in a single network list.

Generate Local List

On the **Local Network List** screen, click this button to have the Manager automatically generate a network list using the first 200 valid network routes in the routing table for the Ethernet 1 (Private) interface of this VPN Concentrator. (See **Monitoring | Routing Table**.) The Manager refreshes the screen after it generates the list, and you can then edit the **Network List** and the **List Name**.

Add

To add this network list to the configured network lists, click **Add**. The Manager displays either the **Remote Network List** screen or the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done** screen.

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

The Manager displays this screen when you have finished configuring all parameters for a new IPSec LAN-to-LAN connection. It documents the added configuration entities.

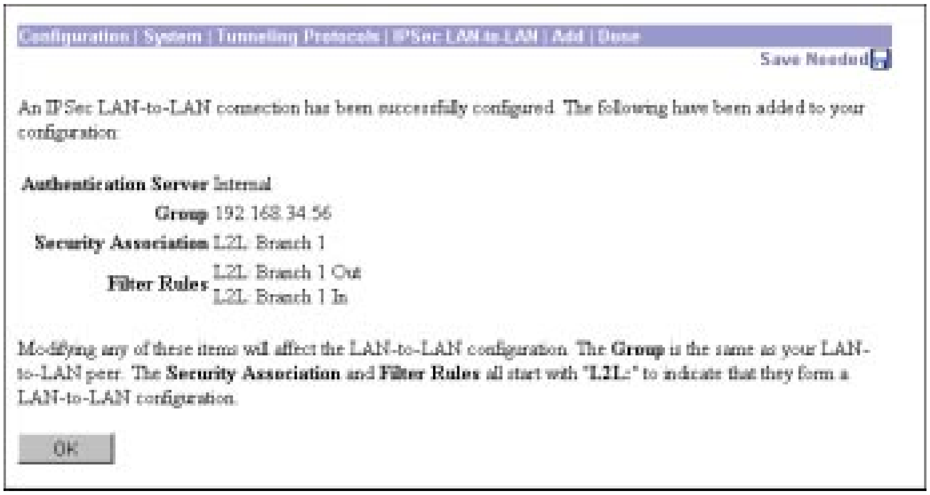
The Manager displays this screen only once. We suggest you print a copy of the screen to save it for your records.

To examine or modify an entity, see the appropriate screen:

- **Group**: See **Configuration | User Management | Groups**.
- **Security Association**: See **Configuration | Policy Management | Traffic Management | Security Associations**.
- **Filter Rules**: See **Configuration | Policy Management | Traffic Management | Rules**.

You cannot delete the group, SA, or rules individually, nor can you remove the rules from their filter. The system automatically deletes them when you delete the LAN-to-LAN connection.

Figure 9 Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done screen



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

Save Needed

An IPSec LAN-to-LAN connection has been successfully configured. The following have been added to your configuration:

Authentication Server Internal
Group 192.168.34.56
Security Association L2L: Branch 1
Filter Rules L2L: Branch 1 Out
L2L: Branch 1 In

Modifying any of these items will affect the LAN-to-LAN configuration. The **Group** is the same as your LAN-to-LAN peer. The **Security Association** and **Filter Rules** all start with "**L2L:**" to indicate that they form a LAN-to-LAN configuration.

OK

To close this screen and return to the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN** screen, click **OK**. The **LAN-to-LAN Connection** list shows the new connection, and the Manager includes all the new settings in the active configuration.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals

This section of the Manager lets you configure, add, modify, activate, deactivate, delete, and prioritize IKE proposals, which are sets of parameters for Phase 1 IPSec negotiations. During Phase 1, the two peers establish a secure tunnel within which they then negotiate the Phase 2 parameters.

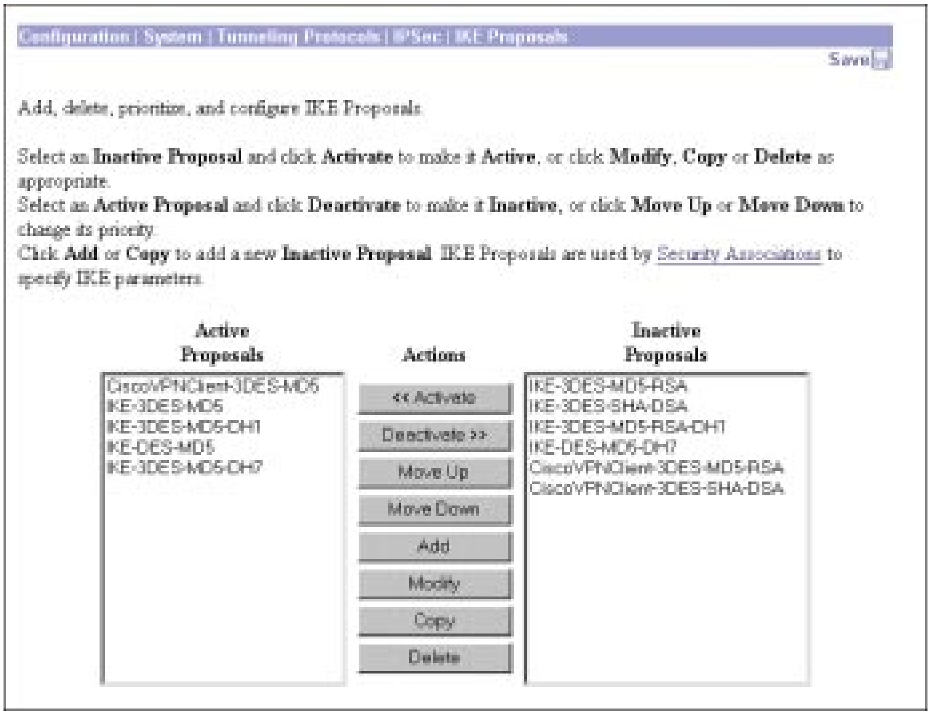
The VPN Concentrator uses IKE proposals both as initiator and responder in IPSec negotiations. In LAN-to-LAN connections, the VPN Concentrator can function as initiator or responder. In client-to-LAN connections, the VPN Concentrator functions only as responder.

You must configure, activate, and prioritize IKE proposals before you configure IPSec Security Associations. See **Configuration | Policy Management | Traffic Management | Security Associations**, or click the *Security Associations* link on this screen.

You must also configure and activate IKE proposals before configuring IPSec LAN-to-LAN connections. See **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN** above.

You can configure a maximum of 72 IKE proposals total (active and inactive).

Figure 10 Configuration | System | Tunneling Protocols | IPSec | IKE Proposals screen



Configuration | System | Tunneling Protocols | IPSec | IKE Proposals

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate.
Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority.
Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by Security Associations to specify IKE parameters.

Active Proposals

CiscoVPNClient-3DES-MD5
IKE-3DES-MD5
IKE-3DES-MD5-DH1
IKE-DES-MD5
IKE-3DES-MD5-DH7

Inactive Proposals

IKE-3DES-MD5-RSA
IKE-3DES-SHA-DSA
IKE-3DES-MD5-RSA-DH1
IKE-DES-MD5-DH7
CiscoVPNClient-3DES-MD5-RSA
CiscoVPNClient-3DES-SHA-DSA

Cisco supplies default IKE proposals that you can use or modify; see Table 2. See **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add** for explanations of the parameters.

Table 2 Cisco-supplied default IKE Proposals

Proposal Name	Authen. Mode	Authen. Algorithm	Encryption Algorithm	Diffie-Hellman Group	Lifetime Measure-ments	Data Lifetime	Time Lifetime
Proposals Active by Default							
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

Proposal Name	Authen. Mode	Authen. Algorithm	Encryption Algorithm	Diffie-Hellman Group	Lifetime Measure-ments	Data Lifetime	Time Lifetime
Proposals Inactive by Default							
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

The field shows the names of IKE proposals that have been configured, activated, and prioritized. As an IPSec responder, the VPN Concentrator checks these proposals in priority order, to see if it can find one that agrees with parameters in the initiator’s proposed SA.

Activating a proposal also makes it available for use wherever the Manager displays an **IKE Proposal** list, and the first active proposal appears as the default selection.

Inactive Proposals

The field shows the names of IKE proposals that have been configured but are inactive. New proposals appear in this list when you first configure and add them. The VPN Concentrator does not use these proposals in any IPSec negotiations, nor do they appear in **IKE Proposal** lists.

Note To configure L2TP over IPSec, you must activate **IKE-3DES-MD5-RSA**. Also see the **Configuration | User Management** screens.

<< Activate

To activate an inactive IKE proposal, select it from the **Inactive Proposals** list and click this button. The Manager moves the proposal to the **Active Proposals** list and refreshes the screen.

>> Deactivate

To deactivate an active IKE proposal, select it from the **Active Proposals** list and click this button. If the active proposal is configured on a Security Association, the Manager displays an error message; and you must remove it from the SA before you can deactivate it. Otherwise, the Manager moves the proposal to the **Inactive Proposals** list and refreshes the screen.

Move Up / Move Down

To change the priority order of an active IKE proposal, select it from the **Active Proposals** list and click **Move Up** or **Move Down**. The Manager refreshes the screen and shows the reordered **Active Proposals** list. These actions move the proposal up or down one position.

Add

To configure and add a new IKE proposal to the list of **Inactive Proposals**, click this button. See **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add**.

Modify

To modify a configured IKE proposal, select it from either **Active Proposals** or **Inactive Proposals** and click this button. See **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Modify**. Modifying an active proposal does not affect connections currently using it, but changes do affect subsequent connections.

Copy

To use a configured IKE proposal as the basis for configuring and adding a new one, select it from either **Active Proposals** or **Inactive Proposals** and click this button. See **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Copy**. The new proposal appears in the **Inactive Proposals** list.

Delete

To delete a configured IKE proposal, select it from either **Active Proposals** or **Inactive Proposals** and click this button. If an active proposal is configured on a Security Association, the Manager displays an error message; and you must remove it from the SA before you can delete it. *Otherwise, there is no confirmation or undo.* The Manager refreshes the screen and shows the remaining IKE proposals in the list.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

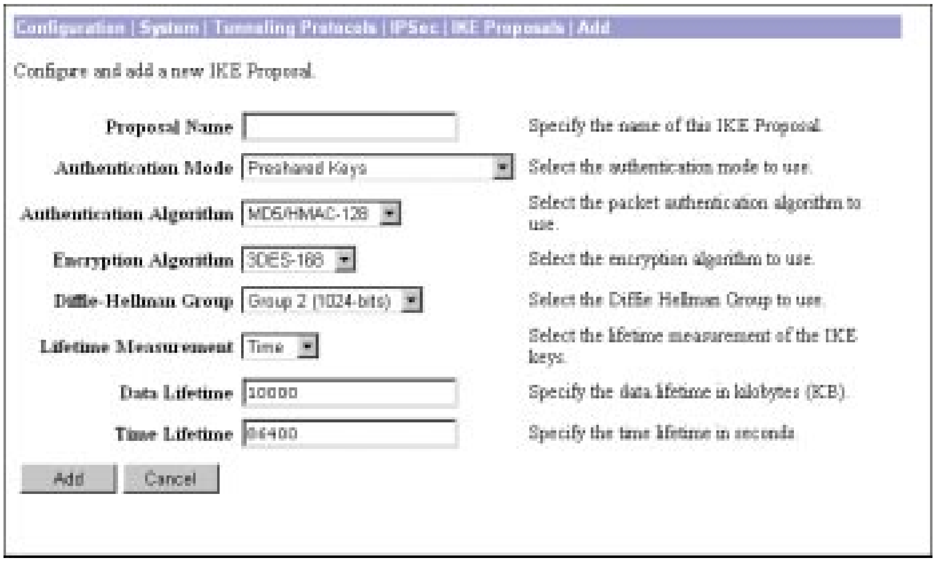
Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add, Modify, or Copy

These screens let you:

- **Add**: Configure and add a new inactive IKE proposal.
- **Modify**: Modify a previously configured IKE proposal.
- **Copy**: Copy a configured IKE proposal, modify its parameters, save it with a new name, and add it to the configured inactive IKE proposals.

You can configure a maximum of 25 IKE proposals total (active and inactive).

Figure 11 Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add, Modify, or Copy screen



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

Configure and add a new IKE Proposal.

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

Proposal Name

Enter a unique name for this IKE proposal. Maximum is 48 characters, case-sensitive. Spaces are allowed.

Authentication Mode

This parameter specifies how to authenticate the remote client or peer. Authentication proves that the connecting entity is who you think it is. If you select one of the digital certificate modes, an appropriate digital certificate must be installed on this VPN Concentrator and the remote client or peer. See the discussion under **Administration | Certificate Management**.

Click the drop-down menu button and select the method:

- **Preshared Keys** = Use preshared keys (the default). The keys are derived from the password of the user's or peer's group.
- **RSA Digital Certificate** = Use a digital certificate with keys generated by the RSA algorithm.

- **DSA Digital Certificate** = Use a digital certificate with keys generated by the DSA algorithm.
- **Preshared Keys (XAUTH)** = Use preshared keys (the default). The keys are derived from the password of the user's or peer's group. Require user-based authentication via XAUTH.
- **RSA Digital Certificate (XAUTH)** = Use a digital certificate with keys generated by the RSA algorithm. Require user-based authentication via XAUTH.
- **DSA Digital Certificate (XAUTH)** = Use a digital certificate with keys generated by the DSA algorithm. Require user-based authentication via XAUTH.

User-Based Authentication

You configure user-based authentication differently for VPN 3000 Clients and VPN Clients. For VPN 3000 Clients, configure user-based authentication in **Configuration | User Management | Groups | Add or Modify**. To configure user-based authentication for VPN Clients, follow these steps.

First, in **Configuration | User Management | Groups Add or Modify (IP Sec tab),** select an **Authentication** option.

Then, in **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals,** select a compatible IKE proposal and position it high in the list of active IKE proposals.

Compatible IKE proposals are any of those whose names begin with **CiscoVPNClient**. You can also create compatible IKE proposals of your own. If you would rather create a new IKE proposal, in **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add or Modify**, select one of the following **Authentication Mode** options: **Preshared Keys (XAUTH)**, **RSA Digital Certificate (XAUTH)**, or **DSA Digital Certificate (XAUTH)**.

Authentication Algorithm

This parameter specifies the data, or packet, authentication algorithm. Packet authentication proves that data comes from whom you think it comes from.

Click the drop-down menu button and select the algorithm:

- **MD5/HMAC-128** = HMAC (Hashed Message Authentication Coding) with the MD5 hash function using a 128-bit key. This is the default selection.
- **SHA/HMAC-160** = HMAC with the SHA-1 hash function using a 160-bit key. This selection is more secure but requires more processing overhead.

Encryption Algorithm

This parameter specifies the data, or packet, encryption algorithm. Data encryption makes the data unreadable if intercepted.

Click the drop-down menu button and select the algorithm:

- **DES-56** = DES encryption with a 56-bit key.
- **3DES-168** = Triple-DES encryption with a 168-bit key. This is the default selection, and it is the most secure.

Diffie-Hellman Group

This parameter specifies the Diffie-Hellman group used to generate IPSec SA keys. The Diffie-Hellman technique generates keys using prime numbers and "generator" numbers in a mathematical relationship.

Click the drop-down menu button and select the group:

- **Group 1 (768-bits)** = Use Diffie-Hellman Group 1 to generate IPSec SA keys, where the prime and generator numbers are 768 bits. Select this option if you select **DES-56** under **Encryption Algorithm** above.
- **Group 2 (1024-bits)** = use Diffie-Hellman Group 2 to generate IPSec SA keys, where the prime and generator numbers are 1024 bits. This is the default selection for use with the **3DES-168 Encryption Algorithm** above.
- **Group 7 (ECC)** = Use Diffie-Hellman Group 7 to generate IPSec SA keys, where the elliptical curve field size is 163 bits. You can use this option with any encryption algorithm. This option is intended for use with the movianVPN client, but you can use it with any peers that support Group 7 (ECC).

Lifetime Measurement

This parameter specifies how to measure the lifetime of the IKE SA keys, which is how long the IKE SA lasts until it expires and must be renegotiated with new keys. It is used with the **Data Lifetime** or **Time Lifetime** parameters below.

Note If the peer proposes a shorter lifetime measurement, the VPN Concentrator uses that lifetime measurement instead.

Click the drop-down menu button and select the measurement method:

- **Time** = Use time (seconds) to measure the lifetime of the SA (the default). Configure the **Time Lifetime** parameter below.
- **Data** = Use data (number of kilobytes) to measure the lifetime of the SA. Configure the **Data Lifetime** parameter below.
- **Both** = Use both time and data, whichever occurs first, to measure the lifetime. Configure both **Time Lifetime** and **Data Lifetime** parameters.
- **None** = No lifetime measurement. The SA lasts until terminated for other reasons. It lasts a maximum of 86400 seconds (24 hours).

Data Lifetime

If you select **Data** or **Both** under **Lifetime Measurement** above, enter the number of kilobytes of payload data after which the IKE SA expires. Minimum is `100` KB, default is `10000` KB, maximum is `2147483647` KB.

Time Lifetime

If you select **Time** or **Both** under **Lifetime Measurement** above, enter the number of seconds after which the IKE SA expires. Minimum is `60` seconds, default is `86400` seconds (24 hours), maximum is `2147483647` seconds (about 68 years).

Add or Apply / Cancel

Add or **Copy** screen:

- To add this IKE proposal to the list of **Inactive Proposals**, click **Add** or **Apply**. The Manager returns to the **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals** screen. To use the new proposal, you must activate and prioritize it as explained for that screen.

Modify screen:

- To apply your changes to this IKE proposal, click Apply. The Manager returns to the **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals** screen. If you modify an active proposal, changes do not affect connections currently using it, but they do affect subsequent connections.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals** screen, and the IKE proposals lists are unchanged.