配置 Cisco VPN 3000 集中器到 Cisco 路由器的连接

目录

简介

此示例配置显示如何将运行Cisco IOS®软件的路由器后面的专用网络连接到Cisco VPN 3000集中器后面的专用网络。网络上的设备通过专用地址互相通信。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 带Cisco IOS软件版本12.3.(1)a的Cisco 2611路由器**注意：**确保Cisco 2600系列路由器安装有支持VPN功能的加密IPsec VPN IOS映像。
- 带4.0.1 B的思科VPN 3000集中器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

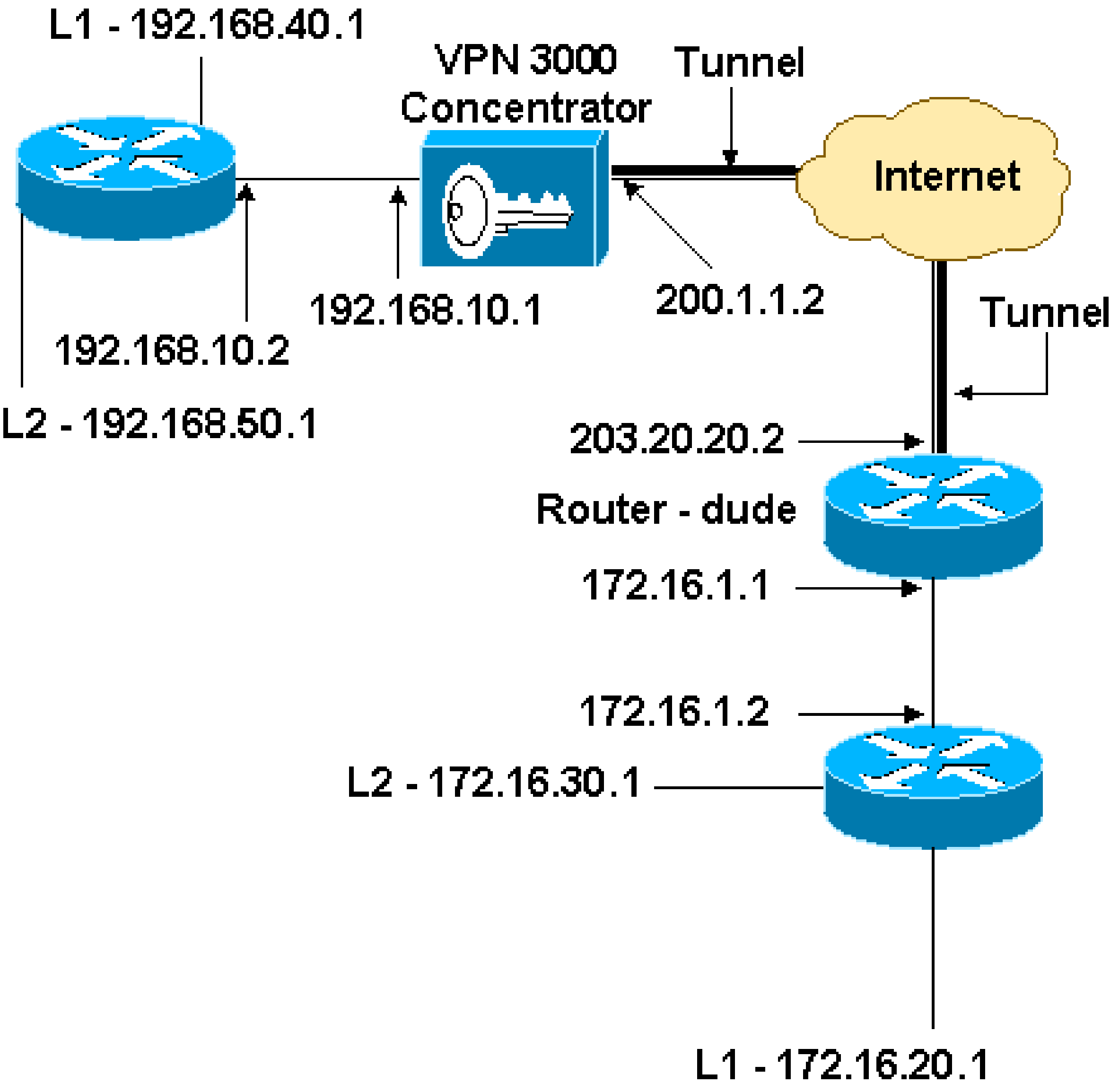
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具(仅限注册客户)可查找有关本文档中使用的命令的详细信息。

网络图

本文档使用此网络设置。



配置

本文档使用以下配置。

路由器配置

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 200.1.1.2
!!--- IPsec policies. crypto ipsec transform-set to_vpn
esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set to_vpn
!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 half-duplex
 crypto map to_vpn
!
interface Ethernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip
172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
```

```
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list
110 deny   ip 172.16.1.0 0.0.0.255 192.168.10.0
0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end
```

VPN 集中器配置

在本实验设置中，VPN集中器首先通过控制台端口访问，并添加最小配置，以便通过图形用户界面(GUI)完成进一步配置。

选择**Administration** > **System Reboot** > **Schedule reboot** > **Reboot with Factory/Default Configuration**以确保VPN集中器中不存在现有配置。

VPN集中器显示在快速配置中，这些项在重新启动后进行配置：

- 时间/日期
- “Configuration > Interfaces”中的接口/掩码（public=200.1.1.2/24，private=192.168.10.1/24）
- 配置> **系统** > **IP路由** > **Default_Gateway**(200.1.1.1)中的默认网关

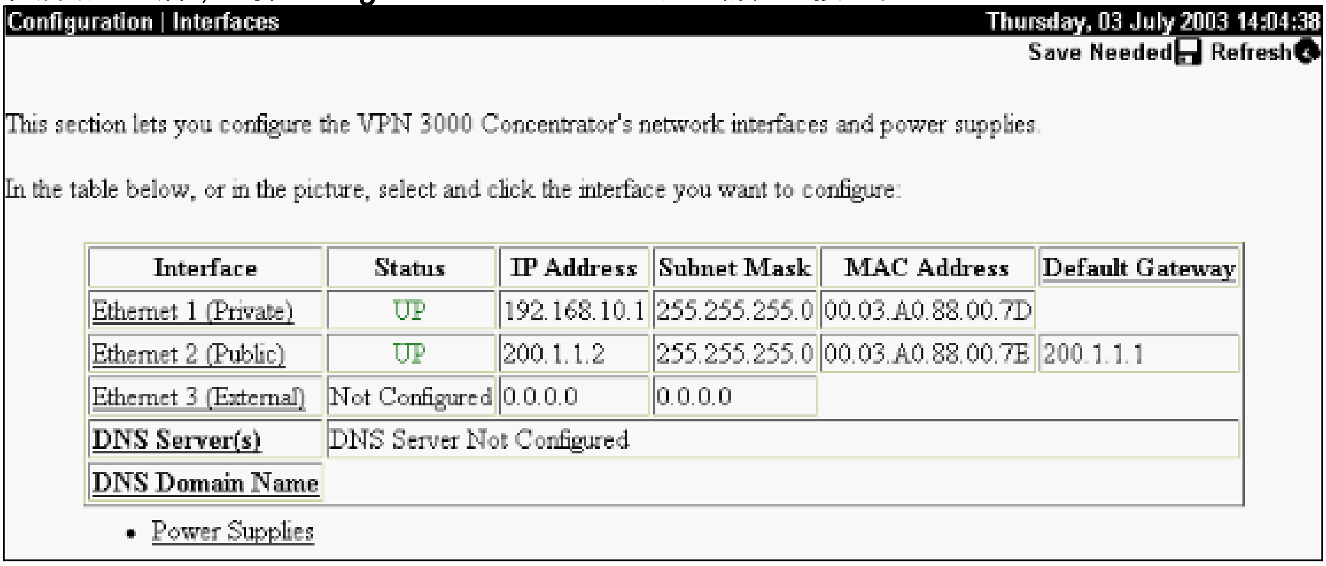
此时，VPN集中器可通过HTML从内部网络访问。

注意：由于VPN集中器是从外部管理的，因此您还必须选择：

- **Configuration** > **Interfaces** > 2-public > **Select IP Filter** > **1。 Private（默认）**。
- **管理**> **访问权**限> **访问控制列表**> **添加Manager Workstation**以添加外部管理器的IP地**址**。

除非您从外部管理VPN集中器，否则不*必执行此*。

1. 在启动GUI后，选择**Configuration** > **Interfaces**以重新检查接口。



Configuration | Interfaces

Thursday, 03 July 2003 14:04:38

Save Needed Refresh

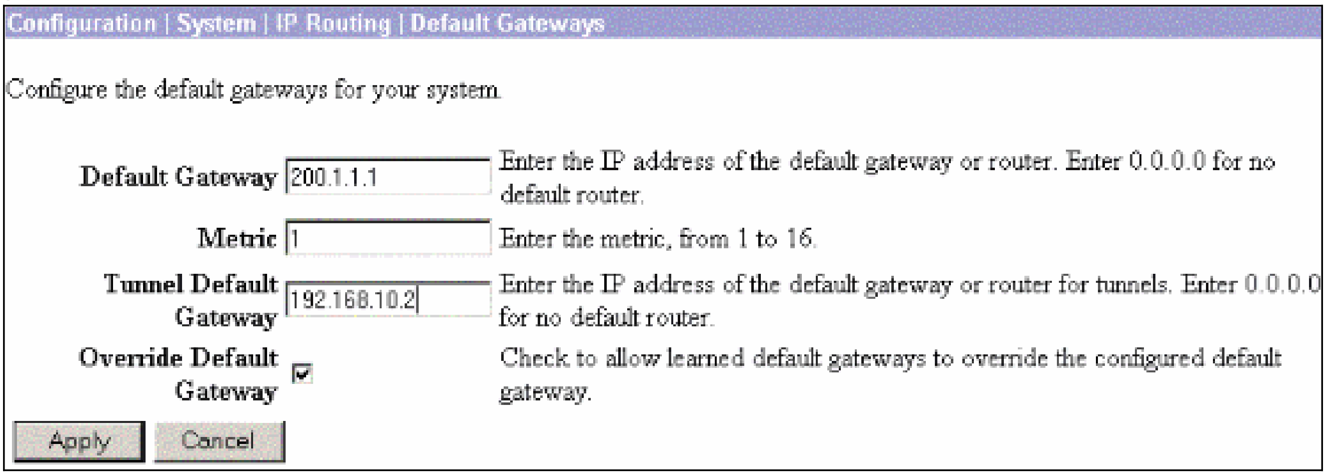
This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.10.1	255.255.255.0	00.03.A0.88.00.7D	
Ethernet 2 (Public)	UP	200.1.1.2	255.255.255.0	00.03.A0.88.00.7E	200.1.1.1
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

- Power Supplies

2. 选择Configuration > System > IP Routing > Default Gateways ，以配置Default (Internet)Gateway和Tunnel Default (inside)Gateway ，使IPsec能够到达专用网络中的其他子网。

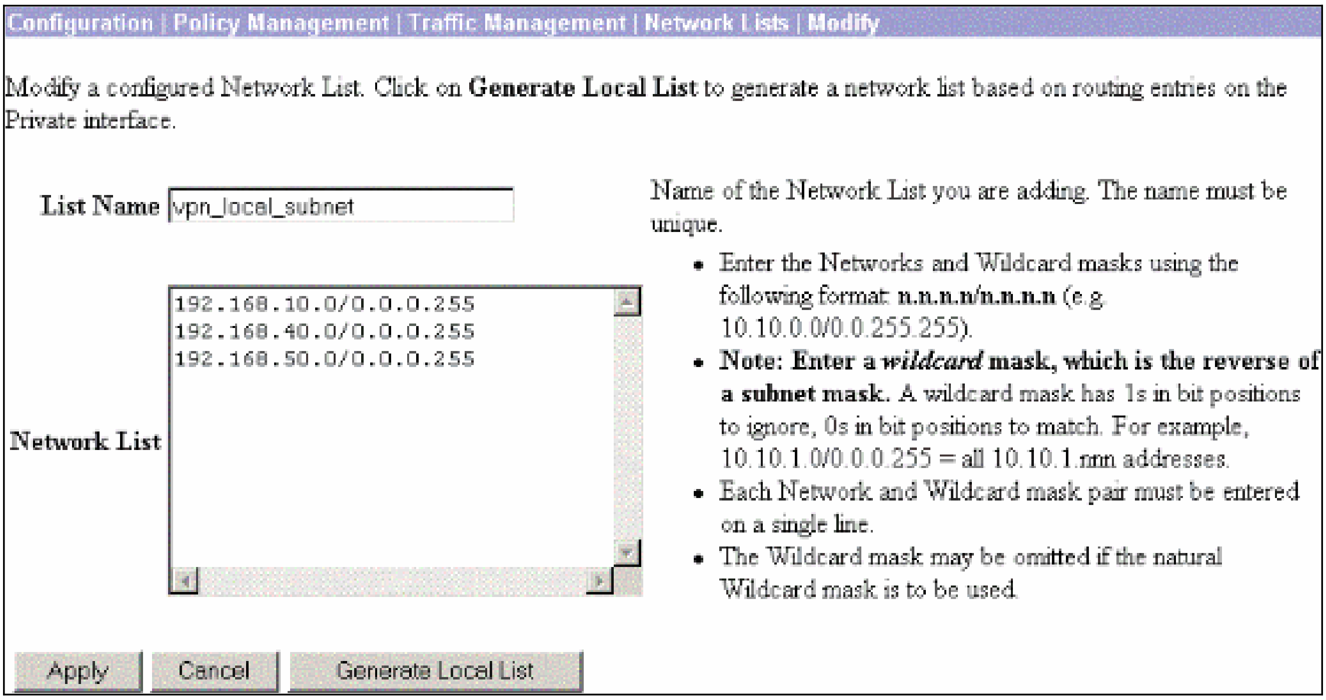


Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

Default Gateway	200.1.1.1	Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.
Metric	1	Enter the metric, from 1 to 16.
Tunnel Default Gateway	192.168.10.2	Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router.
Override Default Gateway	☑	Check to allow learned default gateways to override the configured default gateway.

3. 选择**Configuration** > **Policy Management** > **Network Lists**以创建定义要加密的流量的网络列表。以下是本地网络
：



Configuration | Policy Management | Traffic Management | Network Lists | Modify

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name vpn_local_subnet

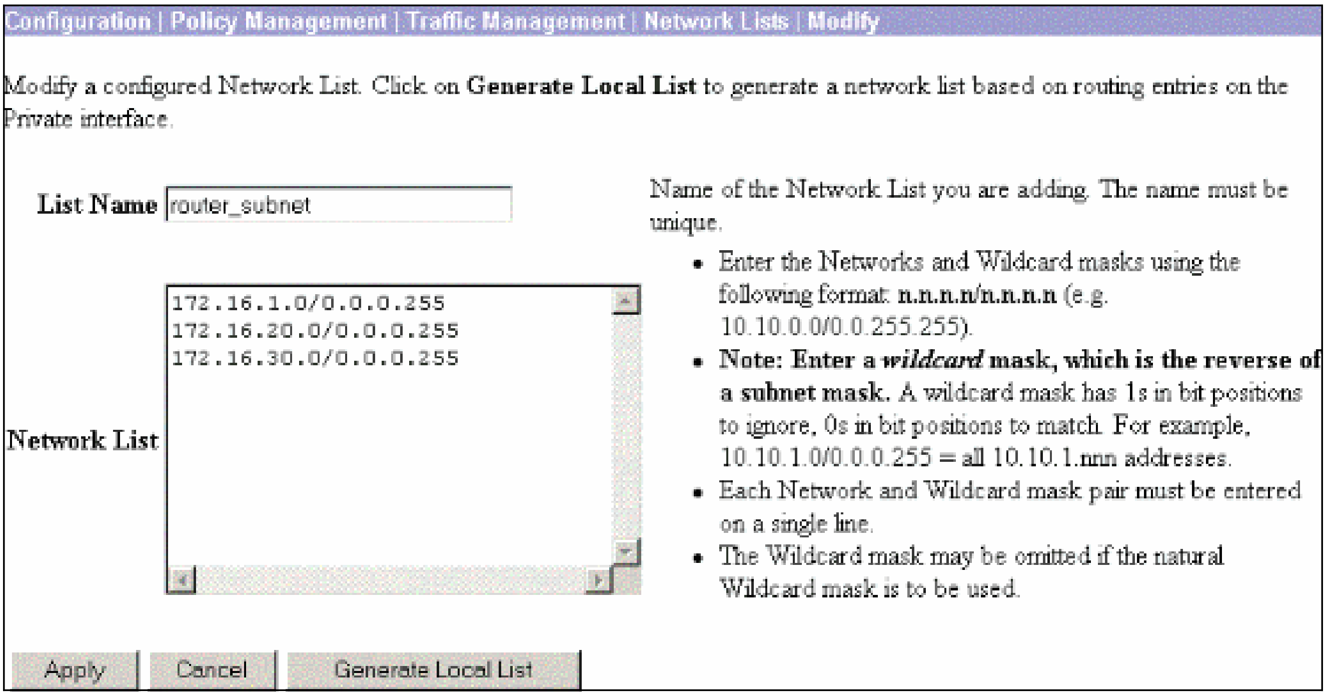
Name of the Network List you are adding. The name must be unique.

Network List

```
192.168.10.0/0.0.0.255
192.168.40.0/0.0.0.255
192.168.50.0/0.0.0.255
```

- 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.

以下是远程网络
：



Configuration | Policy Management | Traffic Management | Network Lists | Modify

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name router_subnet

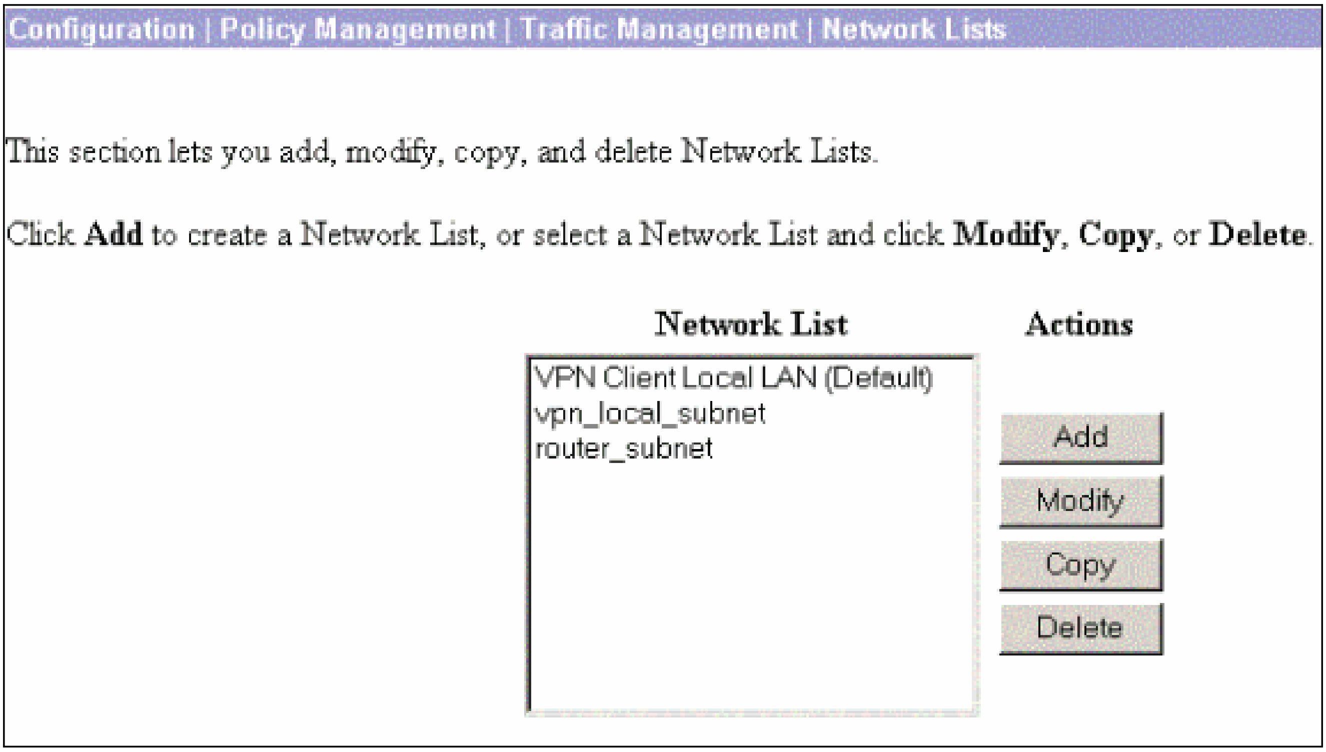
Name of the Network List you are adding. The name must be unique.

Network List

```
172.16.1.0/0.0.0.255
172.16.20.0/0.0.0.255
172.16.30.0/0.0.0.255
```

- 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.

4. 完成后，以下是两个网络列表：**注意：**如果IPsec隧道未启动，请检查相关流量是否在两端匹配。相关流量由路由器和PIX框中的访问列表定义。它们由VPN集中器中的网络列表定义。



Configuration | Policy Management | Traffic Management | Network Lists

This section lets you add, modify, copy, and delete Network Lists.

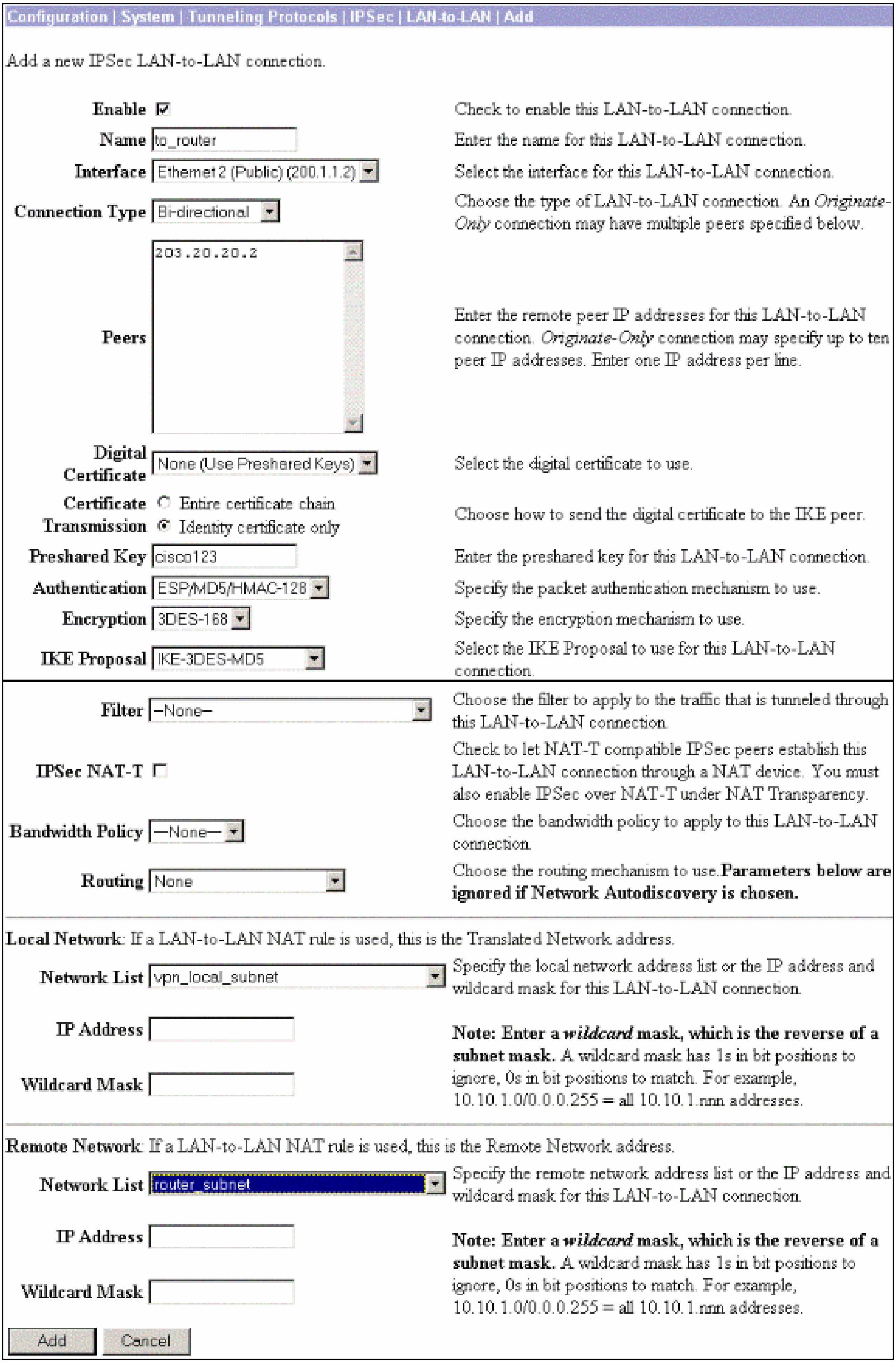
Click **Add** to create a Network List, or select a Network List and click **Modify**, **Copy**, or **Delete**.

Network List

VPN Client Local LAN (Default)
vpn_local_subnet
router_subnet

Actions

5. 选择**Configuration** > **System** > **Tunneling Protocols** > **IPSec LAN-to-LAN**并定义LAN到LAN隧道。



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

Add a new IPSec LAN-to-LAN connection.

Enable	☑	Check to enable this LAN-to-LAN connection.
Name	to_router	Enter the name for this LAN-to-LAN connection.
Interface	Ethernet 2 (Public) (200.1.1.2)	Select the interface for this LAN-to-LAN connection.
Connection Type	Bi-directional	Choose the type of LAN-to-LAN connection. An *Originate-Only* connection may have multiple peers specified below.
Peers	203.20.20.2	Enter the remote peer IP addresses for this LAN-to-LAN connection. *Originate-Only* connection may specify up to ten peer IP addresses. Enter one IP address per line.
Digital Certificate	None (Use Preshared Keys)	Select the digital certificate to use.
Certificate Transmission	○ Entire certificate chain ● Identity certificate only	Choose how to send the digital certificate to the IKE peer.
Preshared Key	cisco123	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.
Filter	-None-	Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
IPSec NAT-T	□	Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency.
Bandwidth Policy	--None--	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Routing	None	Choose the routing mechanism to use. **Parameters below are ignored if Network Autodiscovery is chosen.**

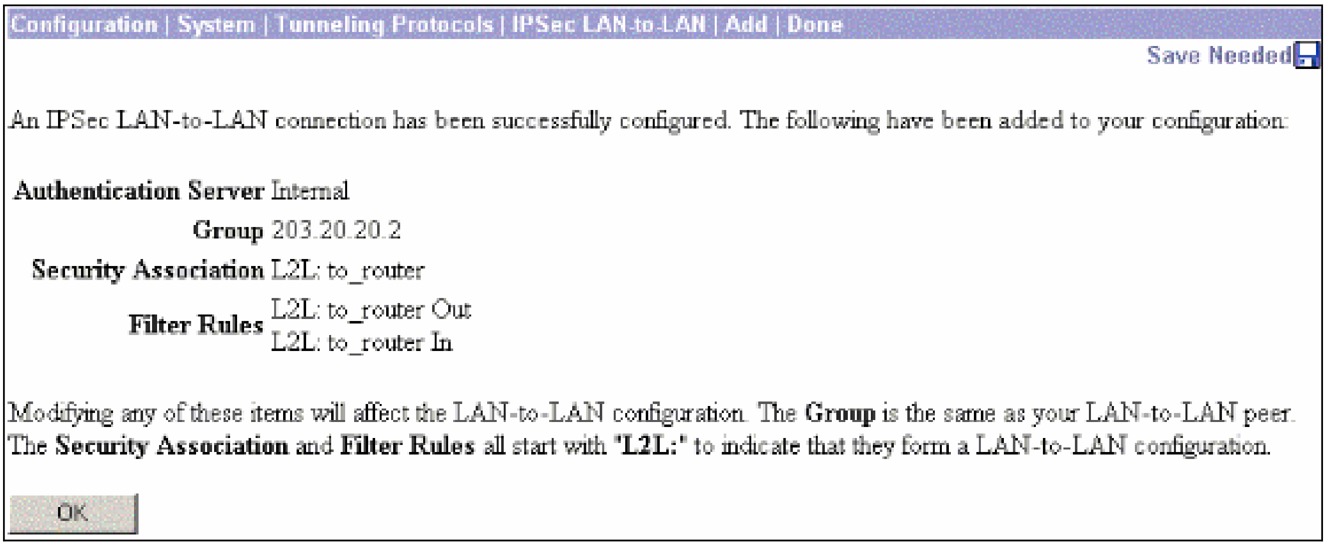
Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

Network List	vpn_local_subnet	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: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

Network List	router_subnet	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		

6. 单击**Apply**后，此窗口将显示为由LAN到LAN隧道配置自动创建的其他配置。

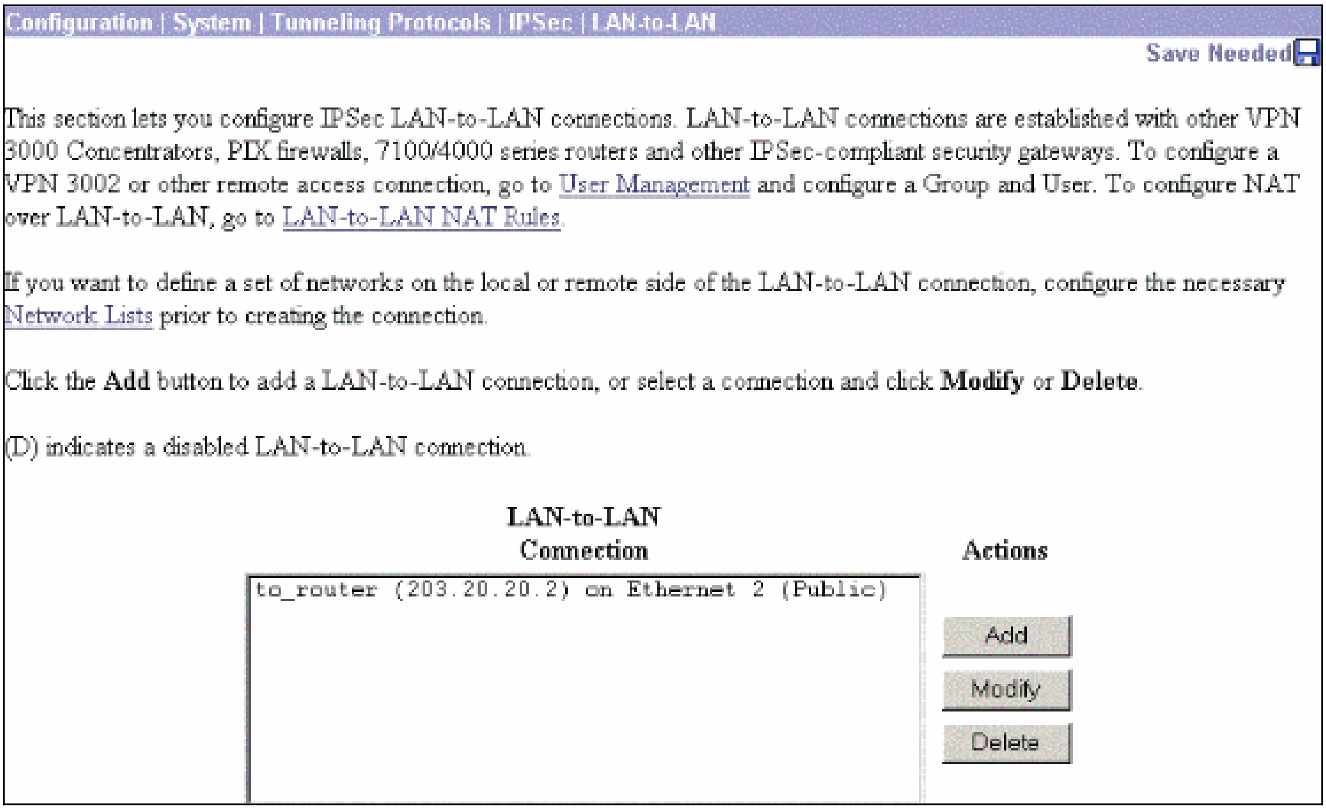

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done
Save Needed
OK

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

Authentication Server	Internal
Group	203.20.20.2
Security Association	L2L: to_router
Filter Rules	L2L: to_router Out L2L: to_router 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.

可以在**Configuration** > **System** > **Tunneling** Protocols **>** IPSec LAN到LAN中查看或修改以前创建的LAN到LAN IPsec参数。


Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN
Save Needed
LAN-to-LAN Connection
Actions
Add
Modify
Delete

This section lets you configure IPSec LAN-to-LAN connections. LAN-to-LAN connections are established with other VPN 3000 Concentrators, PIX firewalls, 7100/4000 series routers and other IPSec-compliant security gateways. To configure a VPN 3002 or other remote access connection, go to User Management and configure a Group and User. To configure NAT over LAN-to-LAN, go to LAN-to-LAN NAT Rules.

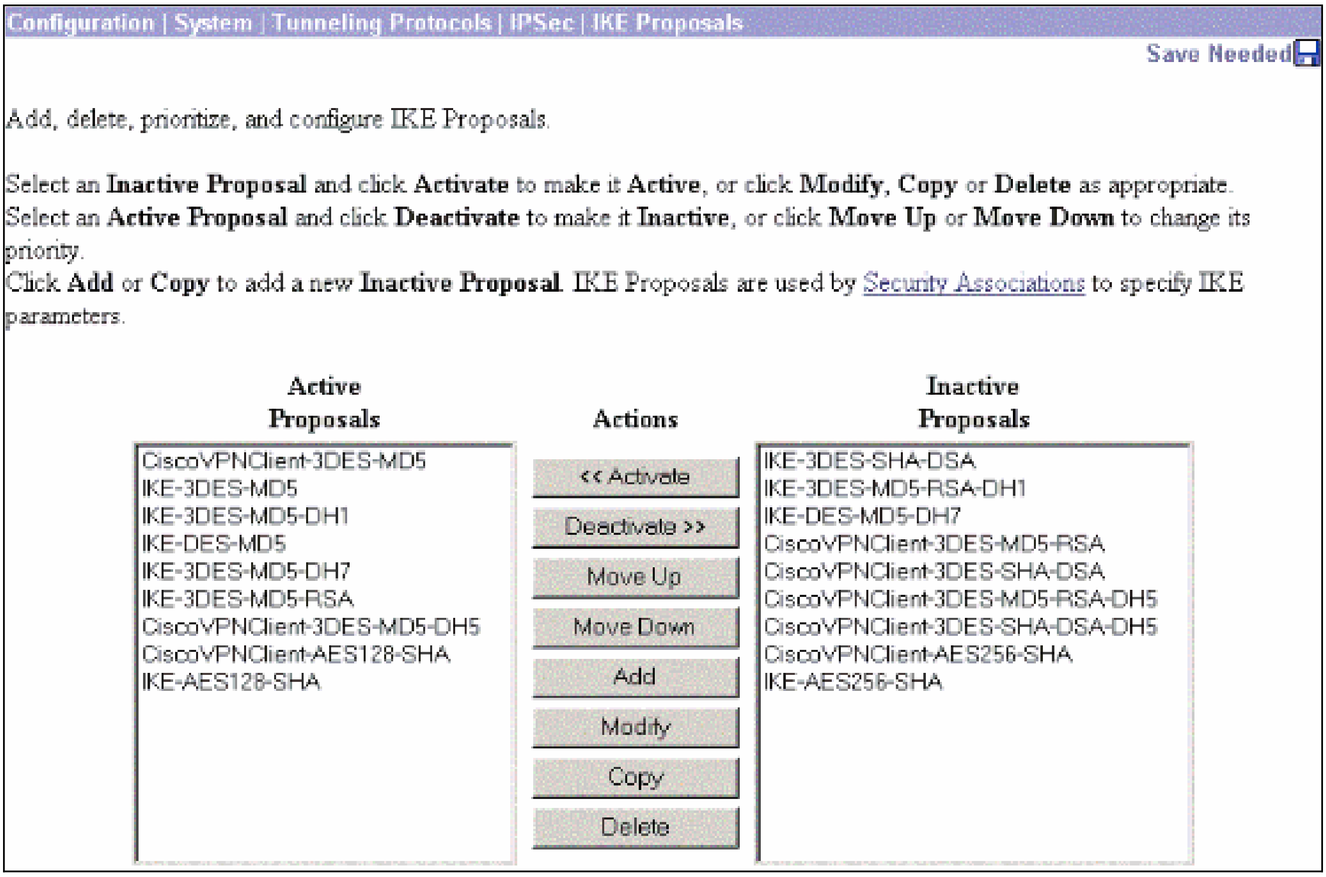
If you want to define a set of networks on the local or remote side of the LAN-to-LAN connection, configure the necessary Network Lists prior to creating the connection.

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

(D) indicates a disabled LAN-to-LAN connection.

to_router (203.20.20.2) on Ethernet 2 (Public)

7. 选择Configuration > **System >** Tunneling Protocols > **IPSec** > IKE Proposals，以确认活动的IKE Proposal。



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

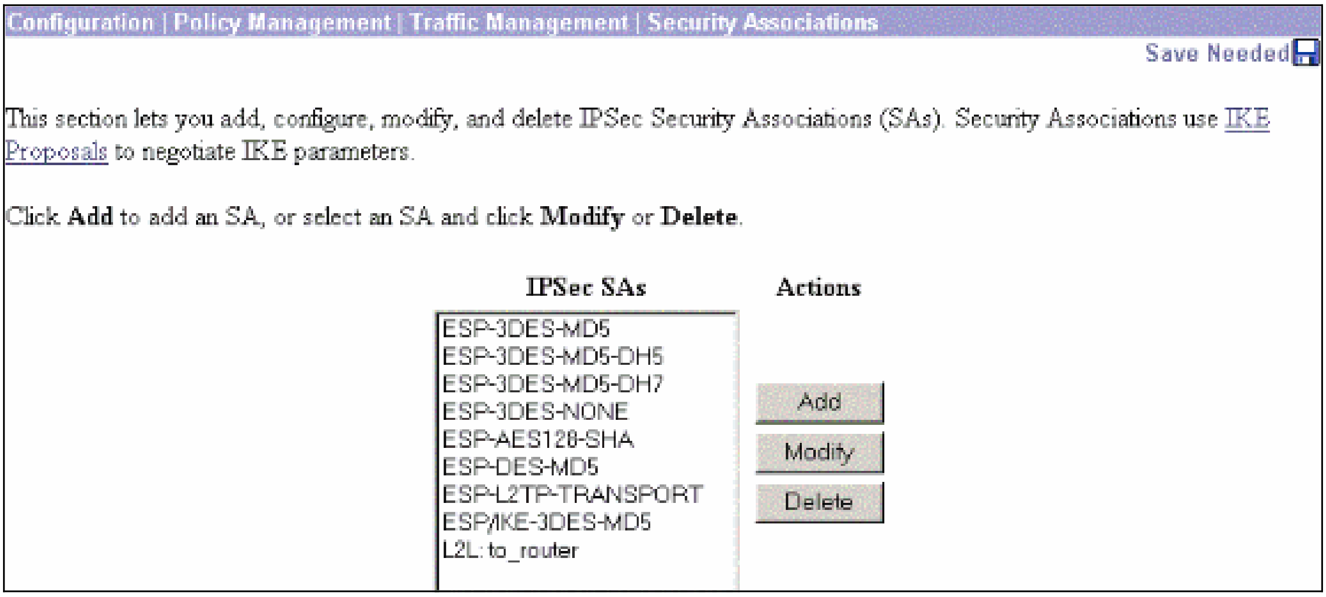
- CiscoVPNClient-3DES-MD5
- IKE-3DES-MD5
- IKE-3DES-MD5-DH1
- IKE-DES-MD5
- IKE-3DES-MD5-DH7
- IKE-3DES-MD5-RSA
- CiscoVPNClient-3DES-MD5-DH5
- CiscoVPNClient-AES128-SHA
- IKE-AES128-SHA

Actions

Inactive Proposals

- IKE-3DES-SHA-DSA
- IKE-3DES-MD5-RSA-DH1
- IKE-DES-MD5-DH7
- CiscoVPNClient-3DES-MD5-RSA
- CiscoVPNClient-3DES-SHA-DSA
- CiscoVPNClient-3DES-MD5-RSA-DH5
- CiscoVPNClient-3DES-SHA-DSA-DH5
- CiscoVPNClient-AES256-SHA
- IKE-AES256-SHA

8. 选择**Configuration** > **Policy Management** > **Traffic Management** > **Security Associations**以查看安全关联列表。



Configuration | Policy Management | Traffic Management | Security Associations

This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security Associations use IKE Proposals to negotiate IKE parameters.

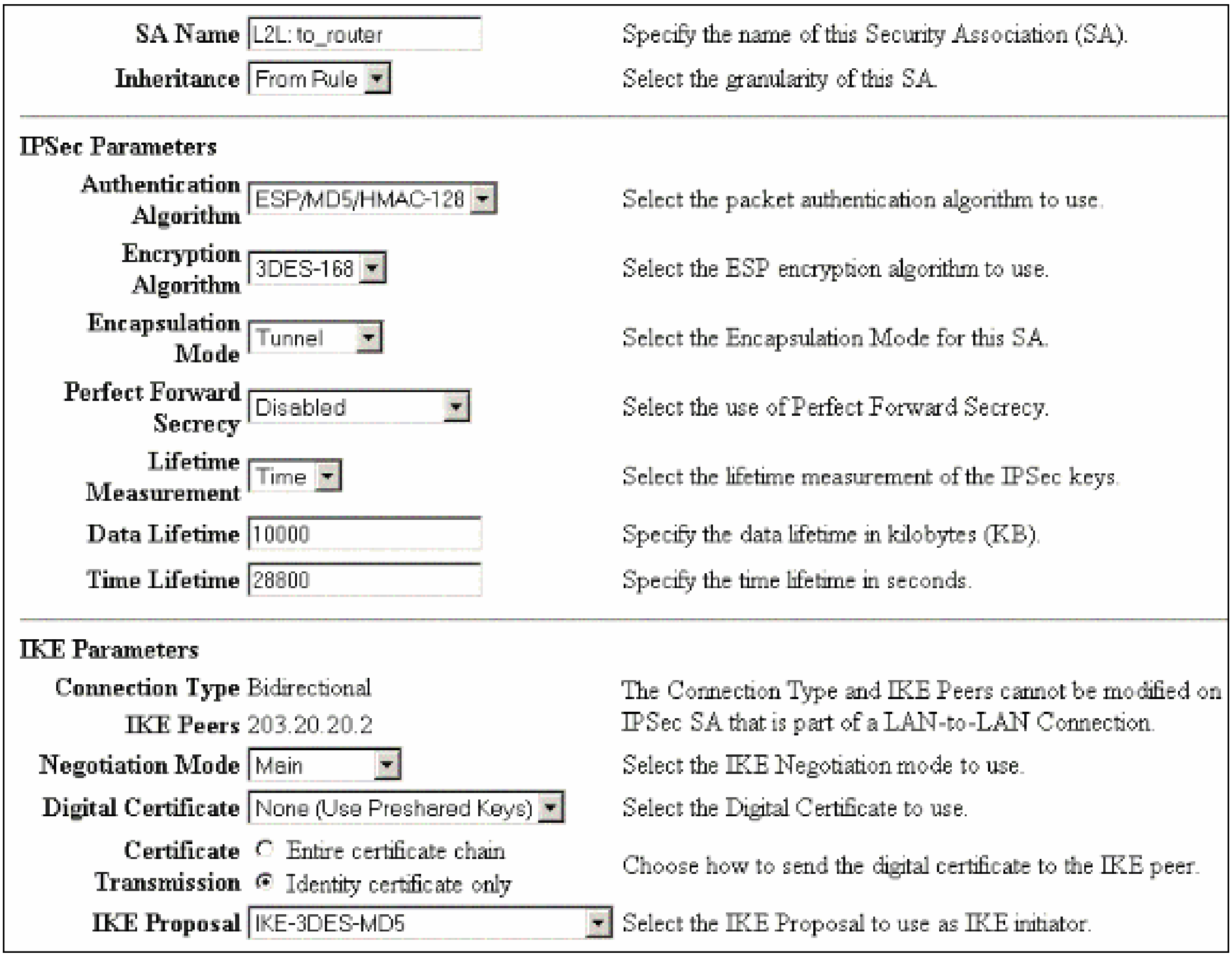
Click **Add** to add an SA, or select an SA and click **Modify** or **Delete**.

IPSec SAs

- ESP-3DES-MD5
- ESP-3DES-MD5-DH5
- ESP-3DES-MD5-DH7
- ESP-3DES-NONE
- ESP-AES128-SHA
- ESP-DES-MD5
- ESP-L2TP-TRANSPORT
- ESP/IKE-3DES-MD5
- L2L: to_router

Actions

9. 单击安全关联名称，然后单击**修改**以验证安全关联。



SA Name	L2L: to_router	Specify the name of this Security Association (SA).
Inheritance	From Rule	Select the granularity of this SA.
IPSec Parameters		
Authentication Algorithm	ESP/MD5/HMAC-128	Select the packet authentication algorithm to use.
Encryption Algorithm	3DES-168	Select the ESP encryption algorithm to use.
Encapsulation Mode	Tunnel	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy	Disabled	Select the use of Perfect Forward Secrecy.
Lifetime Measurement	Time	Select the lifetime measurement of the IPSec keys.
Data Lifetime	10000	Specify the data lifetime in kilobytes (KB).
Time Lifetime	28800	Specify the time lifetime in seconds.
IKE Parameters		
Connection Type	Bidirectional	The Connection Type and IKE Peers cannot be modified on IPSec SA that is part of a LAN-to-LAN Connection.
IKE Peers	203.20.20.2	
Negotiation Mode	Main	Select the IKE Negotiation mode to use.
Digital Certificate	None (Use Preshared Keys)	Select the Digital Certificate to use.
Certificate Transmission	○ Entire certificate chain ● Identity certificate only	Choose how to send the digital certificate to the IKE peer.
IKE Proposal	IKE-3DES-MD5	Select the IKE Proposal to use as IKE initiator.

验证

本部分列出此配置中使用的show命令。

在路由器上

本部分提供的信息可帮助您确认您的配置是否可正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show crypto ipsec sa — 显示当前安全关联所使用的设置。**
- **show crypto isakmp sa - 显示对等体上的所有当前 Internet 密钥交换安全关联。**
- **show crypto engine connection active** — 显示所有加密引擎的当前活动加密会话连接。

您可以使用IOS命令查找工具(仅注册客户)查看有关特定命令的详细信息。

在 VPN 集中器上

选择Configuration > **System >** Events > **Classes** > Modify 以打开日志记录。这些选项是可用的：

- IKE
- IKEDBG
- IKEDECODE

- IPSEC
- IPSECDBG
- IPSECDECODE

日志严重性= 1-13

Console的严重性=1-3

选择**Monitoring** > **Event Log**以检索事件日志。

故障排除

在路由器上

在尝试任何debug命令之前，请参阅有关debug命令的重要信息。

- **debug crypto engine - 显示已加密的流量。**
- **debug crypto ipsec - 显示第 2 阶段的 IPsec 协商。**
- **debug crypto isakmp - 显示第 1 阶段的 ISAKMP 协商。**

问题 — 无法启动隧道

错误消息

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

解决方案

要配置所需的同时登录数或将此SA的同时登录数设置为5，请完成此操作：

转至**Configuration > User Management > Groups > Modify 10.19.187.229 > General > Simultaneouts Logins**，并将登录数更改为5。

PFS

在 IPsec 协商中，完全转发保密 (PFS) 可确保每个新的加密密钥与任何先前密钥不相关。在两个隧道对等体上启用或禁用PFS。否则，路由器中不会建立LAN到LAN(L2L)IPsec隧道。

要指定当为此加密映射条目请求新的安全关联时IPsec应请求PFS，或当IPsec收到新安全关联请求时需要PFS，请在加密映射配置模式下使用**set pfs**命令。要指定IPsec不应请求PFS，请使用此命令的**no**形式。

```
set pfs [group1 | group2]
no set pfs
```

对于 set pfs 命令：

- *group1* — 指定IPsec在执行新的Diffie-Hellman交换时应使用768位Diffie-Hellman主模组。

- *group2* — 指定IPsec在执行新的Diffie-Hellman交换时应使用1024位Diffie-Hellman主模组。

默认情况下，不会请求 PFS。如果未使用此命令指定组，*则将*组1用作默认值。

示例：

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

有关set pfs命令的详细信息，请参阅《Cisco IOS安**全命令**参考》。

相关信息

- **最常见的L2L和远程访问IPSec VPN故障排除解决方案**
- Cisco VPN 3000 系列集中器
- Cisco VPN 3002 硬件客户端
- IPsec 协商/IKE 协议
- 技术支持和文档 - Cisco Systems