Cisco ルータへの Cisco VPN 3000 コンセントレータの設定

内容

概要

この設定例では、Cisco IOS® ソフトウェアを実行するルータの背後にあるプライベート ネットワークを Cisco VPN 3000 コンセントレータの背後にあるプライベート ネットワークに接続する方法を示します。ネットワーク上のデバイスは、プライベート アドレスによって互いを認識します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOSソフトウェアリリース12.3.(1)aが稼働するCisco 2611ルータ**注**：Cisco 2600シリー

ズルータに、VPN機能をサポートする暗号化IPsec VPN IOSイメージがインストールされていることを確認してください。

- Cisco VPN 3000コンセントレータ(4.0.1 B)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

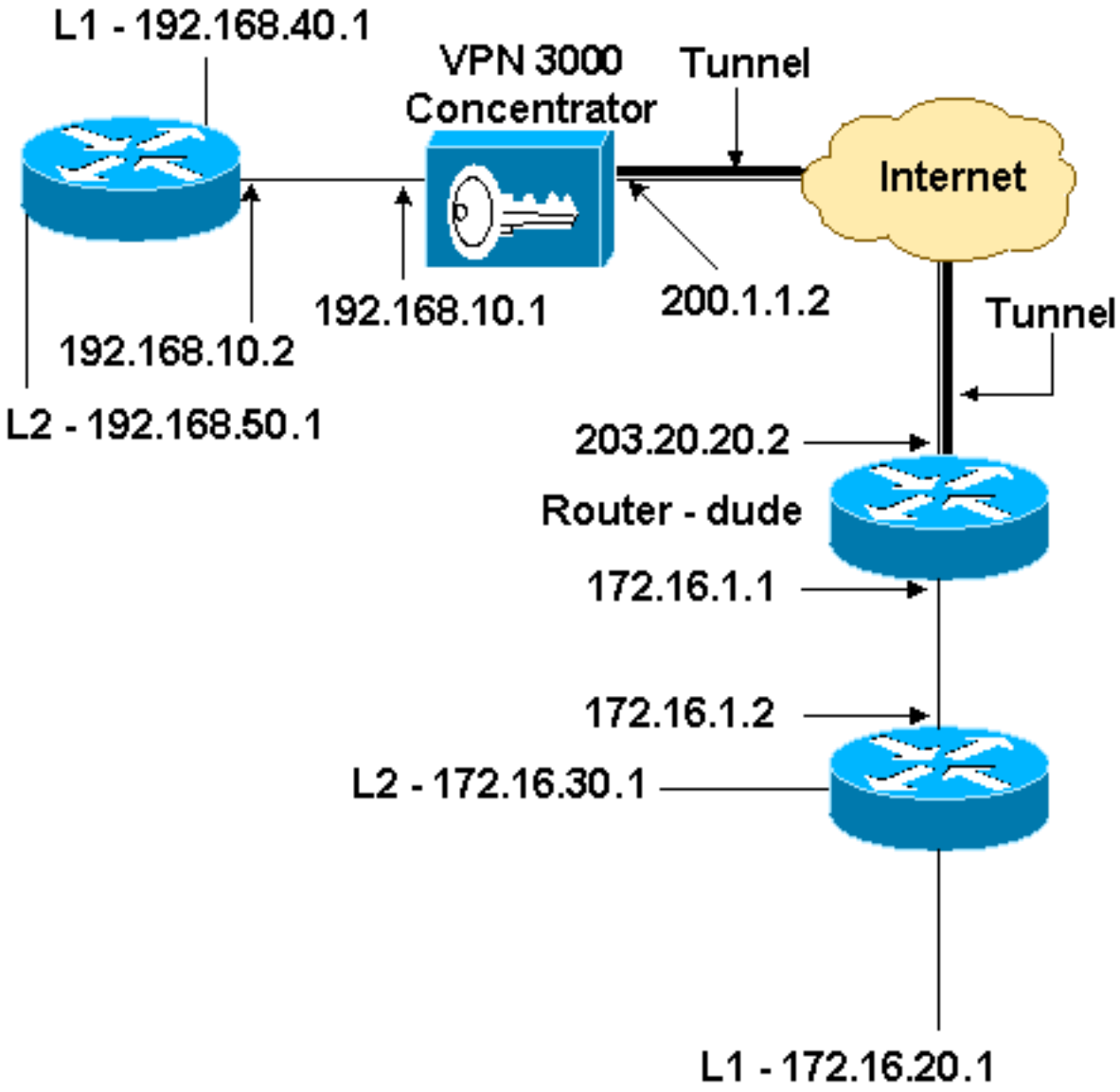
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注： このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク設定を使用します。



設定

このドキュメントでは次の設定を使用します。

ルータの設定

```
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 コンセントレータの設定

このラボ設定では、最初にコンソールポートからVPNコンセントレータにアクセスし、最小限の設定を追加して、さらに詳細な設定をグラフィカルユーザインターフェイス(GUI)で行うことができます。

[Administration] > [System Reboot] > [Schedule reboot] > [Reboot with Factory/Default Configuration] を選択して、VPNコンセントレータに既存の設定がないことを確認します。

VPNコンセントレータが[Quick Configuration]に表示され、リブート後に次の項目が設定されます。

- 時間/日付
- Configuration Interfaces（パブリック アドレス = 200.1.1.2/24、プライベート アドレス = 192.168.10.1/24）でのインターフェイス/マスク
- Configuration > System > IP routing > Default_Gateway（200.1.1.1）のデフォルト ゲートウェイ

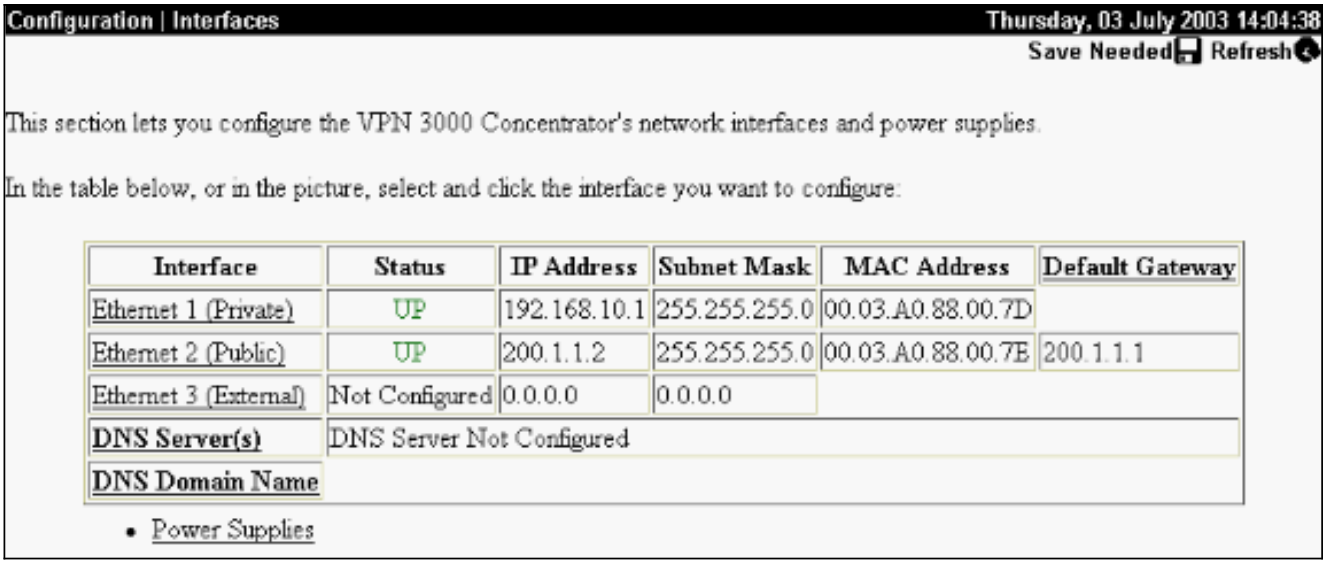
この段階で、VPN コンセントレータは、内部ネットワークから HTML を介してアクセスできます。

注：VPNコンセントレータは外部から管理されているため、次の項目も選択する必要があります。

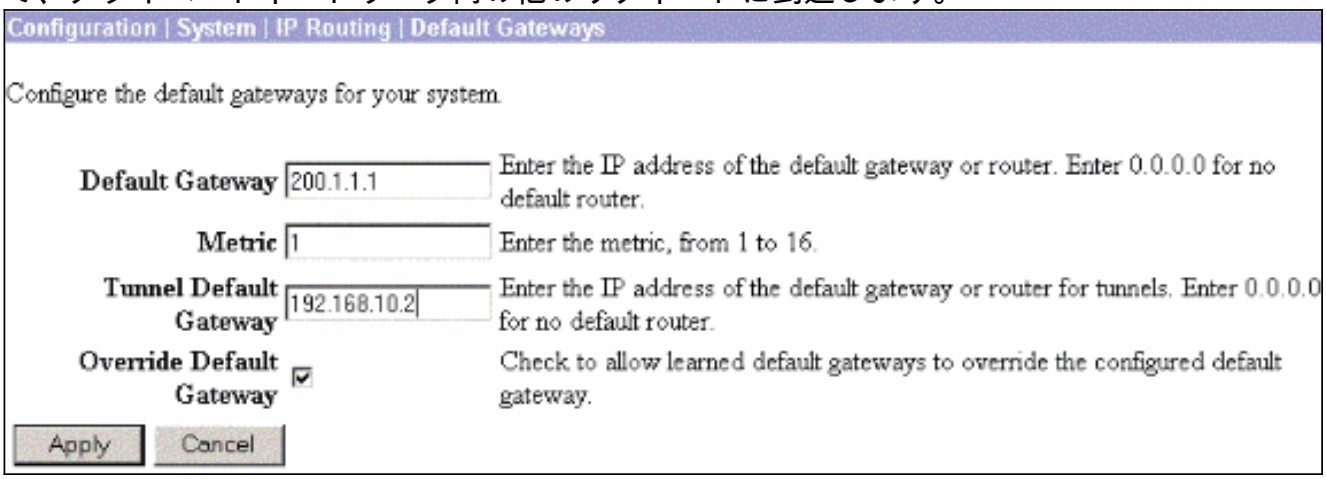
- [Configuration] **> [Interfaces] > 2-public > [Select IP Filter] > [1. Private (Default)]**。
- **[Administration] > [Access Rights]** > [Access Control List] > [Add Manager Workstation] を選択して、外部マネージャのIPアドレスを追加します。

これは、外部からVPNコンセントレータを管理しない限り必要*ありません*。

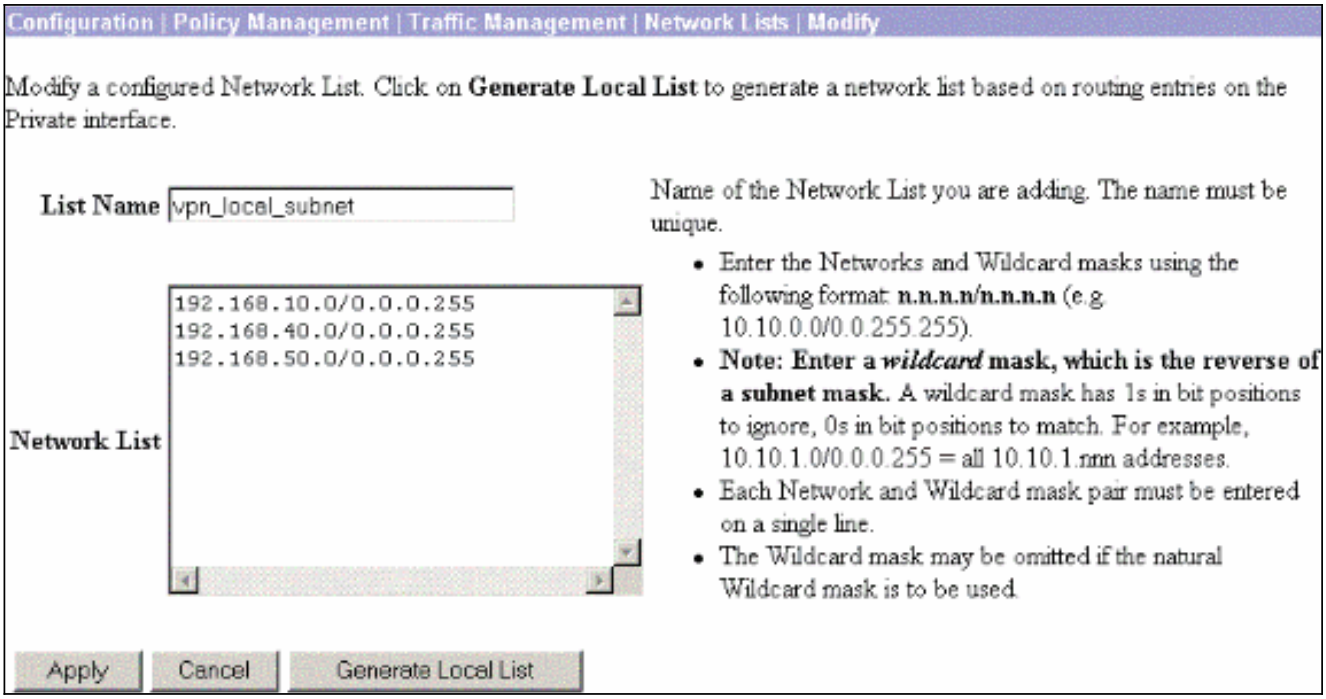
1. GUIを起動した後にインターフェイスを再確認するには、[Configuration] > [Interfaces] を選択します。



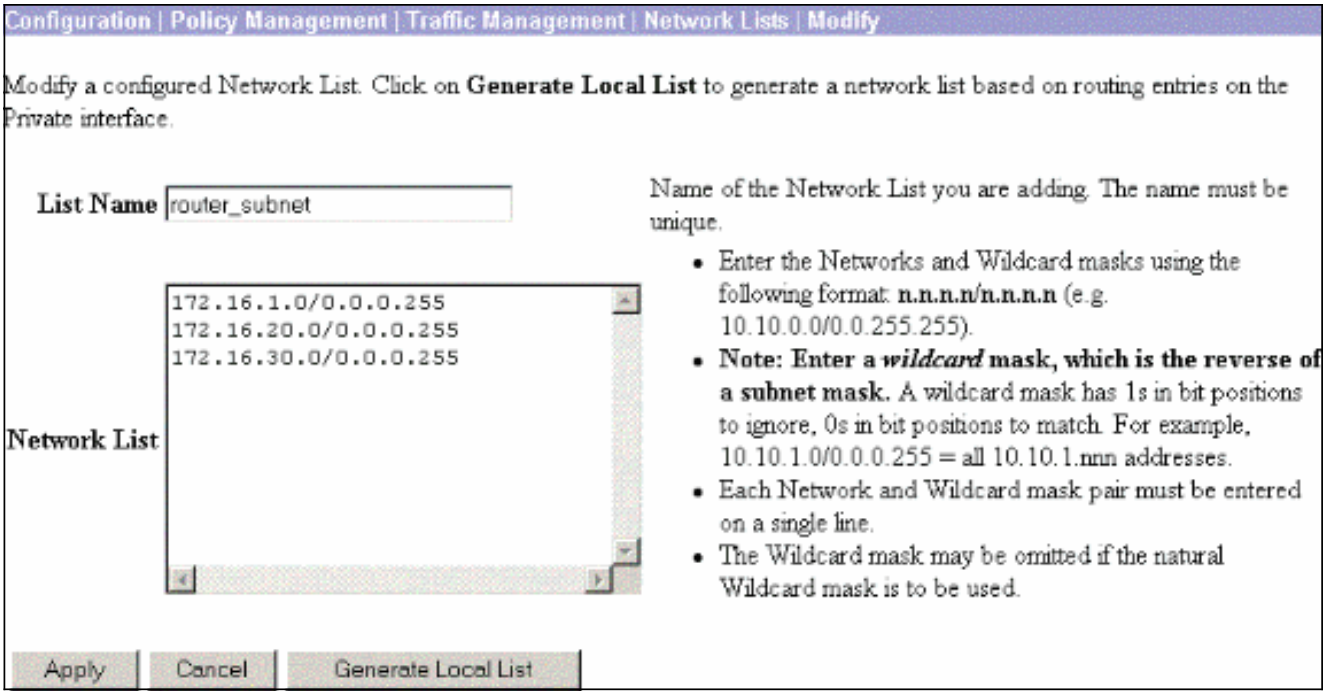
2. [Configuration] > [System] > [IP Routing] > [Default Gateways] を選択し、IPSecのデフォルト（インターネット）ゲートウェイとトンネルデフォルト（内部）ゲートウェイを設定して、プライベートネットワーク内の他のサブネットに到達します。



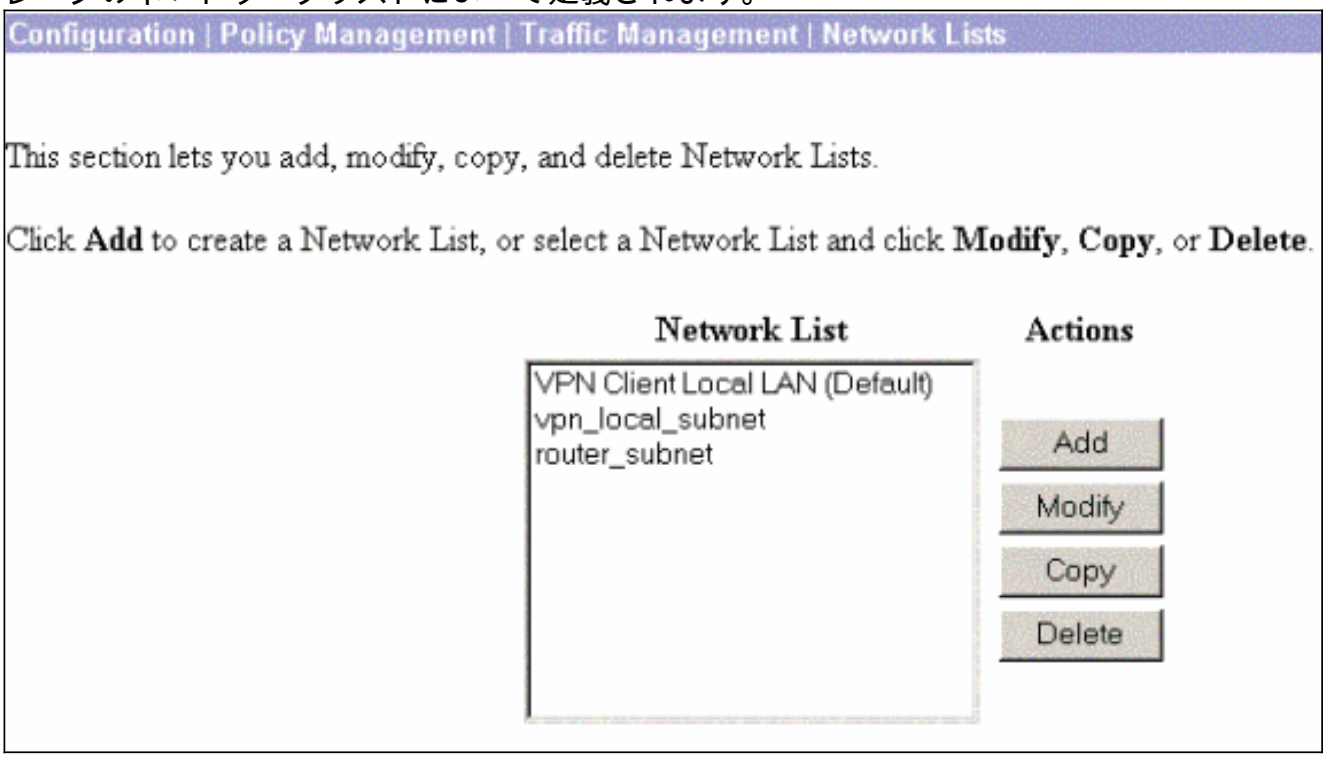
3. [Configuration] > [Policy Management] > [Network Lists] を選択し、暗号化するトラフィックを定義するネットワークリストを作成します。ローカルネットワークは次のとおりです。



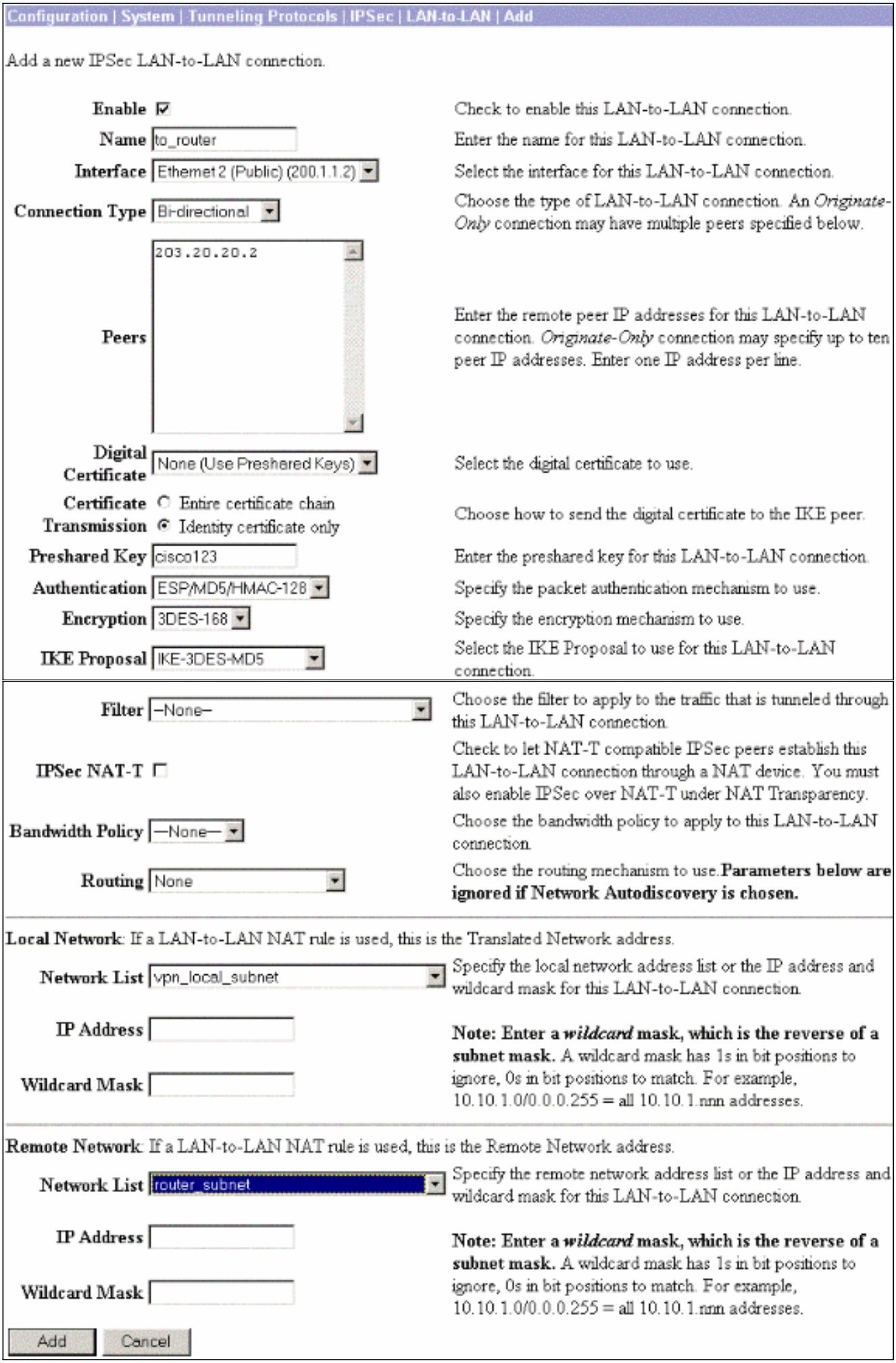
リモートネットワークは次のとおりです。



4. 完了時の 2 つのネットワーク リストは次のとおりです。**注**：IPSecトンネルがアップしない場合は、対象トラフィックが両側で一致するかどうかを確認します。対象トラフィックは、ルータとPIXボックスのアクセスリストによって定義されます。これらは、VPNコンセントレータのネットワークリストによって定義されます。

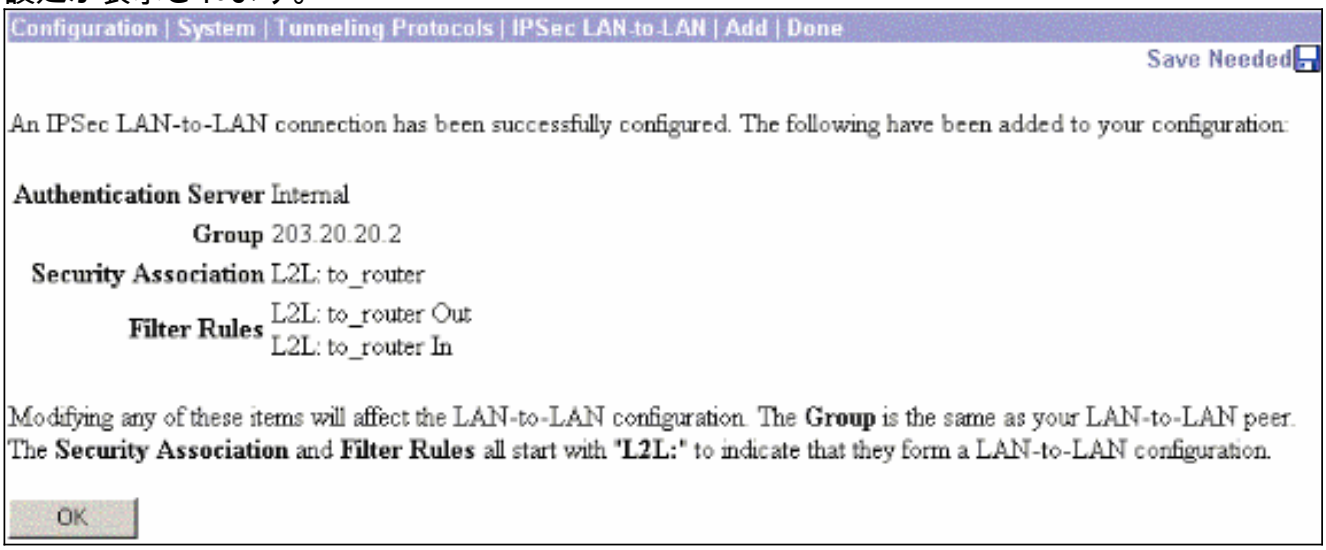


5. [Configuration] > [System] > [Tunneling Protocols] > [IPSec LAN-to-LAN]の順に選択し、LAN-to-LANトンネルを定義します。

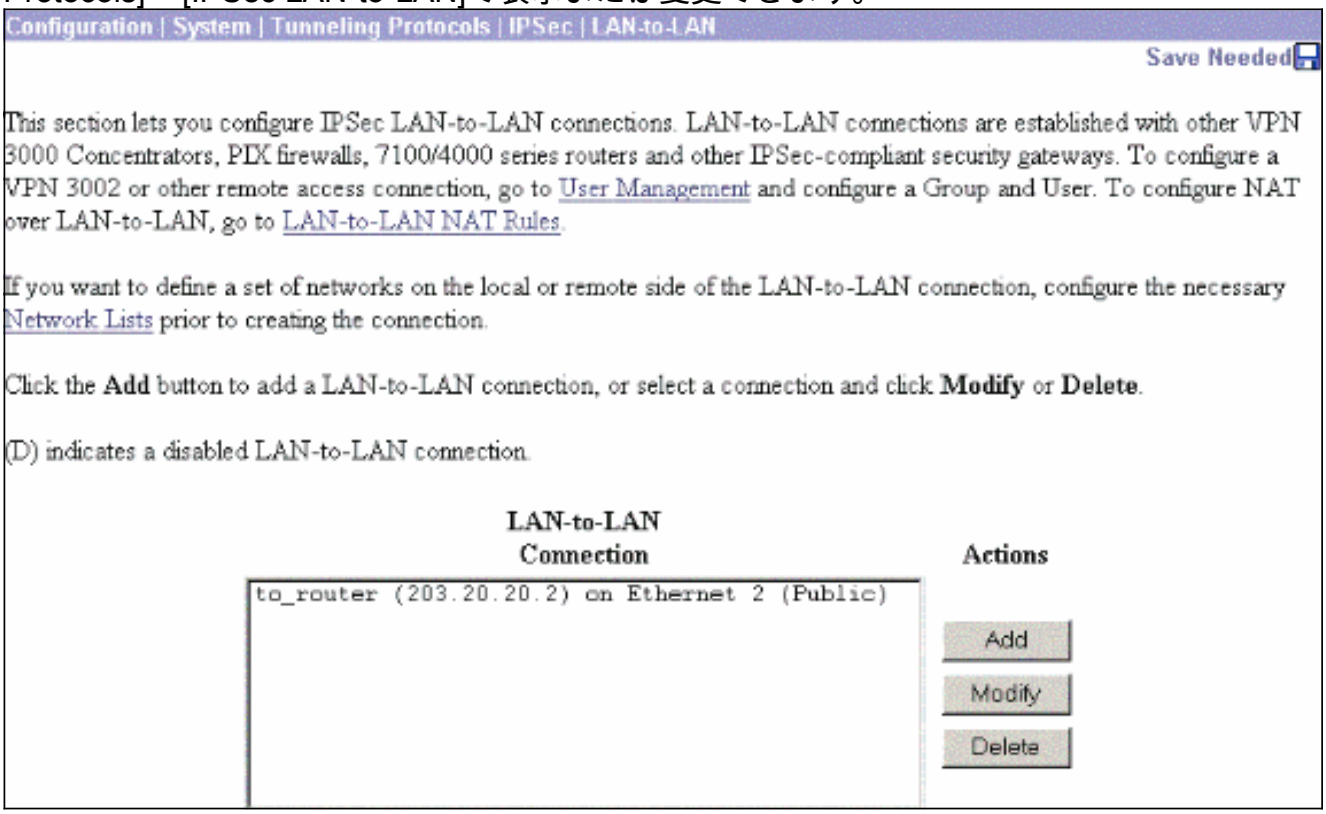


6. [Apply] をクリックすると、LAN-to-LANトンネル設定の結果として自動的に作成される他の

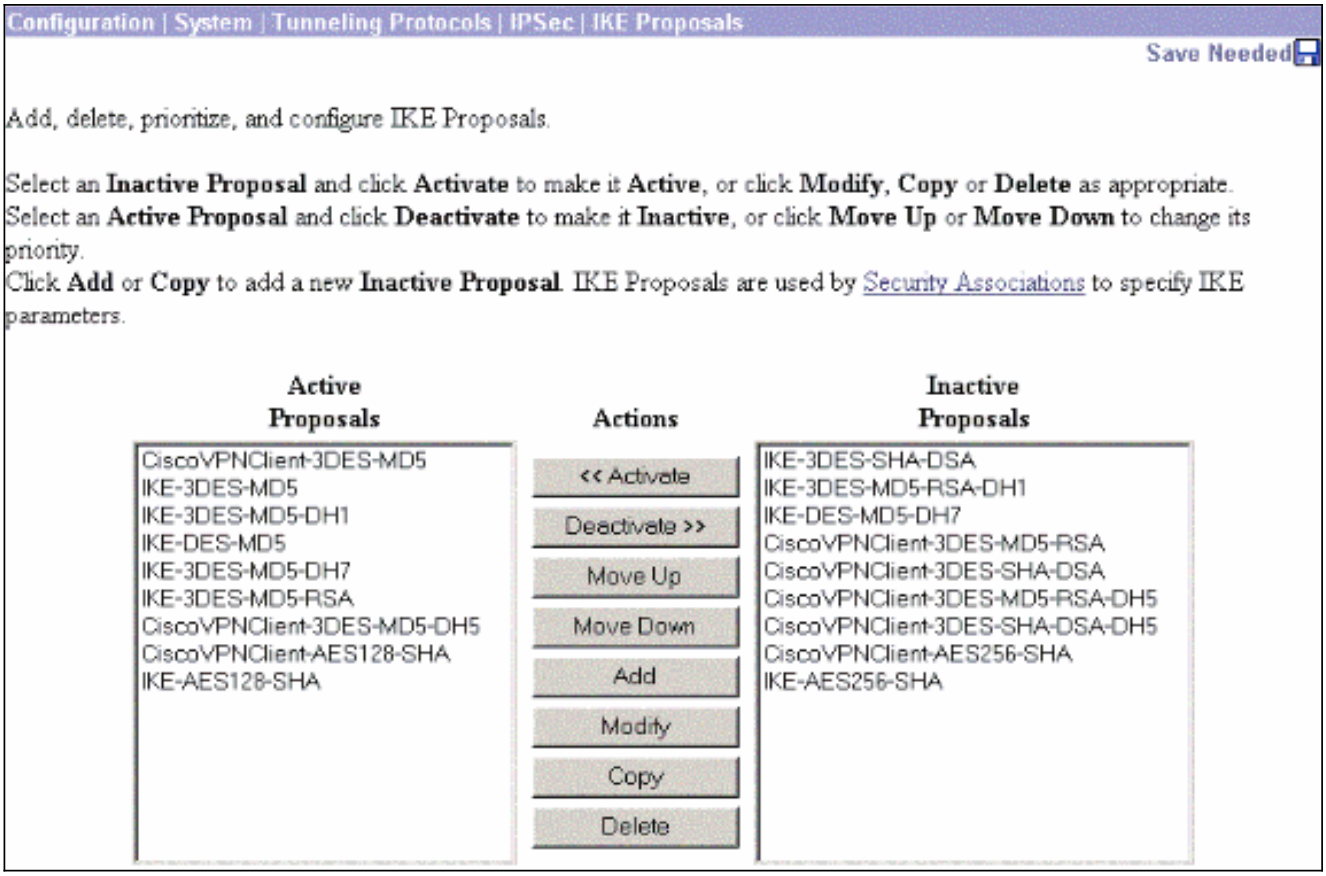
設定が表示されます。



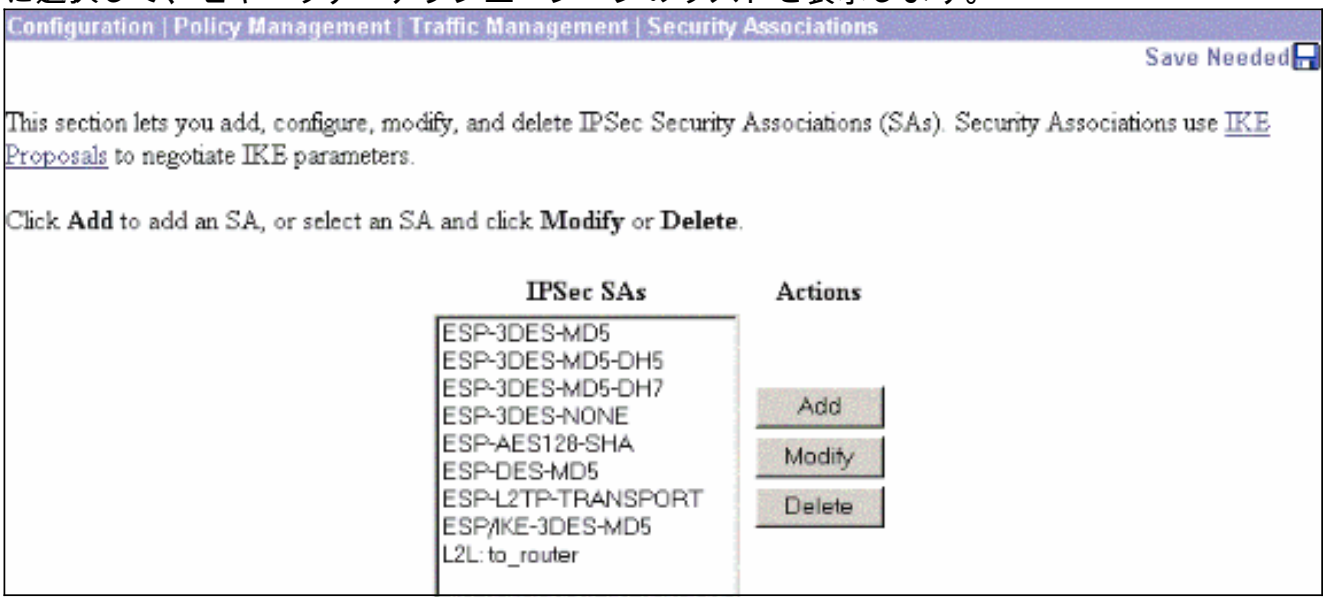
以前に作成したLAN-to-LAN IPsecパラメータは、[Configuration] > [System] > [Tunneling Protocols] > [IPSec LAN-to-LAN]で表示または変更できます。



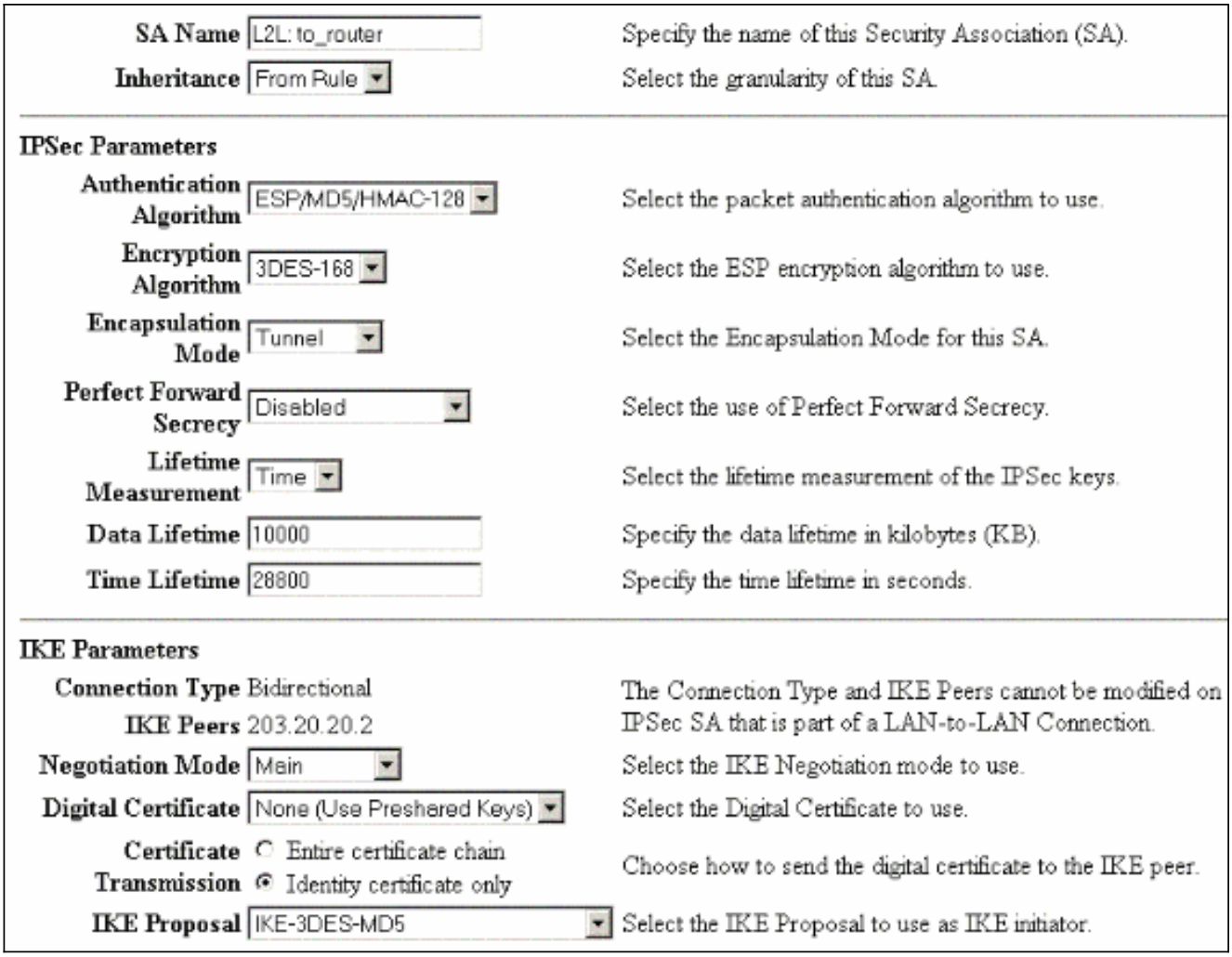
7. [Configuration] > [System] > [Tunneling Protocols] > [IPSec] > [IKE Proposals] を選択して、アクティブなIKEプロポーザルを確認します。



8. [Configuration] > [Policy Management] > [Traffic Management] > [Security Associations] の順に選択して、セキュリティアソシエーションのリストを表示します。



9. セキュリティアソシエーション名をクリックし、次に[Modify]をクリックしてセキュリティアソシエーションを確認します。



確認

このセクションでは、この設定で使用されるshowコマンドをリストします。

インターフェイス設定です。

この項では、設定が正常に動作しているかどうかを確認する際に役立つ情報を紹介しています。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- **show crypto ipsec sa**：現在のセキュリティアソシエーションで使用されている設定を表示します。
- **show crypto isakmp sa**：ピアにおける現在のInternet Key Exchange（IKE；インターネット鍵交換）セキュリティアソシエーション(SA)をすべて表示します。
- **show crypto engine connection active**：すべての暗号化エンジンの現在アクティブな暗号化セッション接続を表示します。

IOS Command Lookup Tool（登録ユーザ専用）を使用して、特定のコマンドに関する詳細情報を確認できます。

VPN コンセントレータ上で使用する場合

[Configuration] > [**System**] > [**Events**] > [**Classes**] > [Modify]の順に選択して、ロギングをオンにし

ます。次のオプションを使用できます。

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

ログに対する重大度 = 1 ~ 13

コンソールに対する重大度 = 1 ~ 3

[Monitoring] > [Event Log]を選択し、イベントログを取得します。

トラブルシュート

インターフェイス設定です。

debugコマンドを試す前に、『debugコマンドの重要な情報』を参照してください。

- **debug crypto engine - 暗号化されたトラフィックを表示します。**
- **debug crypto ipsec：フェーズ 2 の IPsec ネゴシエーションを表示します。**
- **debug crypto isakmp**：フェーズ 1 の ISAKMP ネゴシエーションを表示します。

問題：トンネルを開始できない

エラー メッセージ

```
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>
```

解決方法

このSAに対して必要な同時ログイン数を設定するか、同時ログイン数を5に設定するには、次の操作を実行します。

[Configuration] > [User Management] > [Groups] > [Modify 10.19.187.229] > [General] > [Simultaneouts Logins]に移動し、ログイン数を5に変更します。

PFS

IPSec のネゴシエーションでは、Perfect Forward Secrecy（PFS; 完全転送秘密）によって、それぞれの新しい暗号鍵が以前の鍵とは独立したものであることが保証されます。両方のトンネルピアでPFSを有効または無効にします。そうでない場合、LAN-to-LAN(L2L)IPsecトンネルはルータで確立されません。

この暗号マップエントリに対して新しいセキュリティアソシエーション(SA)が要求されたときに、IPSecがPFSを要求するように指定するには、暗号マップ設定モードで**set pfsコマンドを使用し**

ます。IPSecがPFSを要求しないように指定するには、このコマンドのno形式を使用します。

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

set pfs コマンドについて：

- *group1*：新しいDiffie-Hellman交換の実行時に、IPSecで768ビットのDiffie-Hellmanプライムモジュラスグループを使用するように指定します。
- *group2*：新しいDiffie-Hellman交換の実行時に、IPsecが1024ビットのDiffie-Hellmanプライムモジュラスグループを使用することを指定します。

デフォルトでは、PFS は要求されません。このコマンドでグループが指定されていない場合は、*group1*がデフォルトとして使用されます。

例：

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

set pfsコマンドの詳細については、『Cisco IOS Security Command Reference』を参照してください。

関連情報

- 一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について
- Cisco VPN 3000 シリーズ コンセントレータ
- Cisco VPN 3002 Hardware Client
- IPSec ネゴシエーション/IKE プロトコル
- テクニカル サポートとドキュメント – Cisco Systems