Configuring the Cisco VPN 3000 Concentrator to a Cisco Router

Contents

Introduction

Este exemplo de configuração mostra como conectar uma rede privada atrás de um roteador que executa o software Cisco IOS® a uma rede privada atrás do Cisco VPN 3000 Concentrator. Os dispositivos nas redes se reconhecem por seus endereços privados.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Roteador Cisco 2611 com Software Cisco IOS versão 12.3.1(1a**Observação:** certifique-se de que os roteadores Cisco 2600 Series estejam instalados com uma imagem criptografada do

IPsec VPN IOS que suporte o recurso VPN.
- Concentrador Cisco VPN 3000 com 4.0.1 B

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

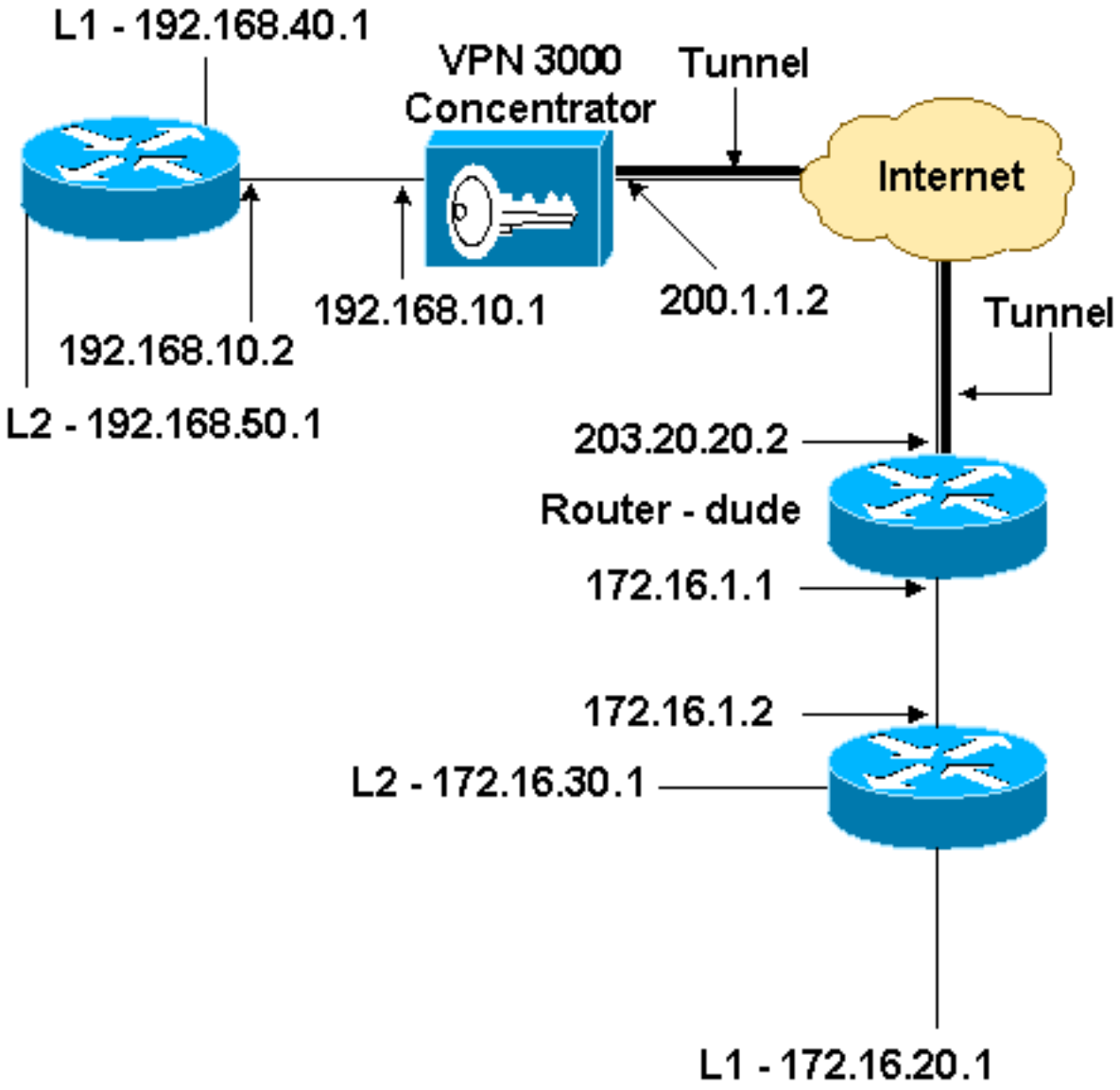
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede.



Configurações

Este documento utiliza esta configuração.

Configuração do roteador

```
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
```

Configuração do VPN Concentrator

Nesta configuração de laboratório, o VPN Concentrator é acessado pela porta do console e uma configuração mínima é adicionada para que a configuração adicional possa ser feita através da interface gráfica do usuário (GUI).

Escolha **Administration > System Reboot > Schedule reboot > Reboot with Fatory/Default Configuration** para garantir que não haja nenhuma configuração existente no VPN Concentrator.

O VPN Concentrator aparece na Configuração rápida e estes itens são configurados após a reinicialização:

- Hora/Data
- Interfaces/Máscaras em Configuration > Interfaces (pública=200.1.1.2/24, privada=192.168.10.1/24)
- Gateway padrão em Configuration > System > IP routing > Default_Gateway (200.1.1.1)

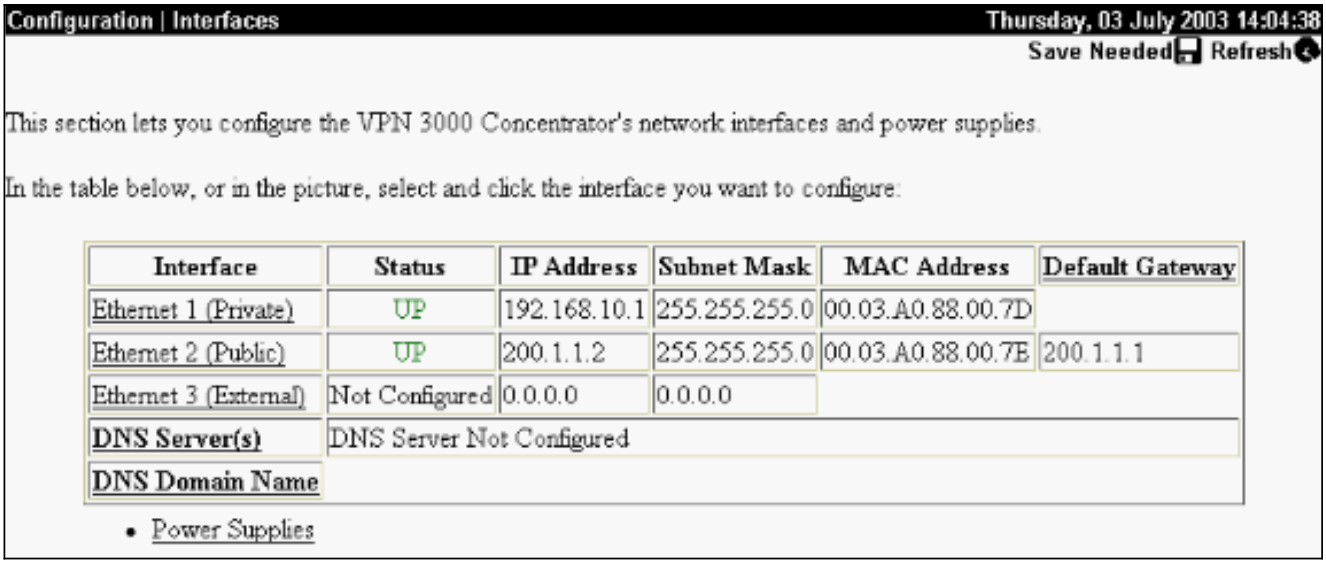
Neste ponto, o VPN Concentrator é acessível por meio de HTML da rede interna.

Observação: como o VPN Concentrator é gerenciado de fora, você também deve selecionar:

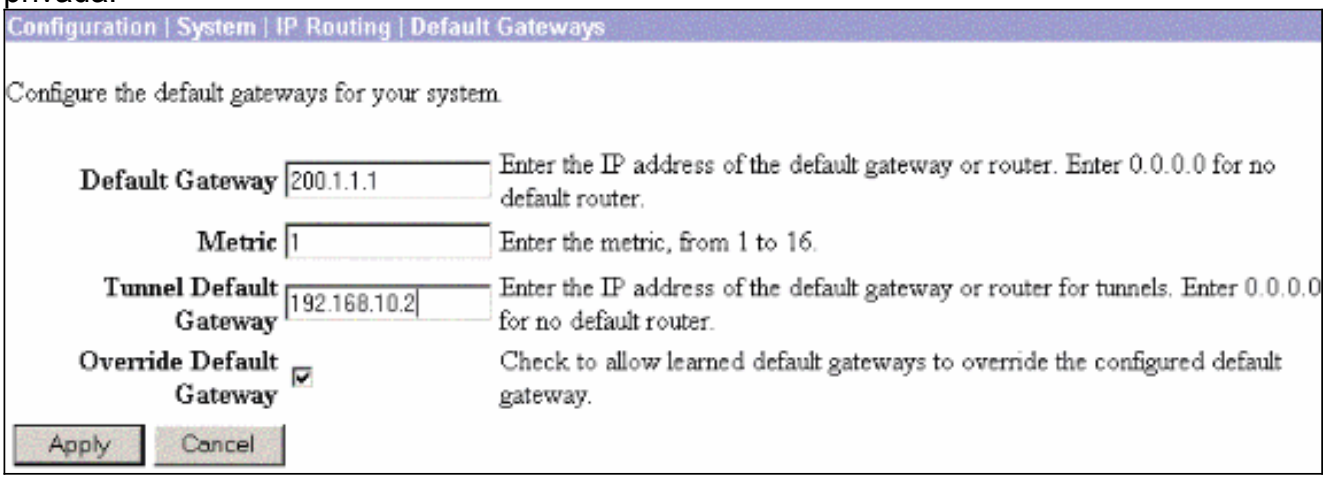
- **Configuração > Interfaces > 2-public > Selecionar filtro IP > 1. Privado (Padrão)**.
- **Administration > Access Rights > Access Control List > Add Manager Workstation** para adicionar o endereço IP do *externo* manager.

Isso não é necessário a menos que você gerencie o VPN Concentrator de *fora*.

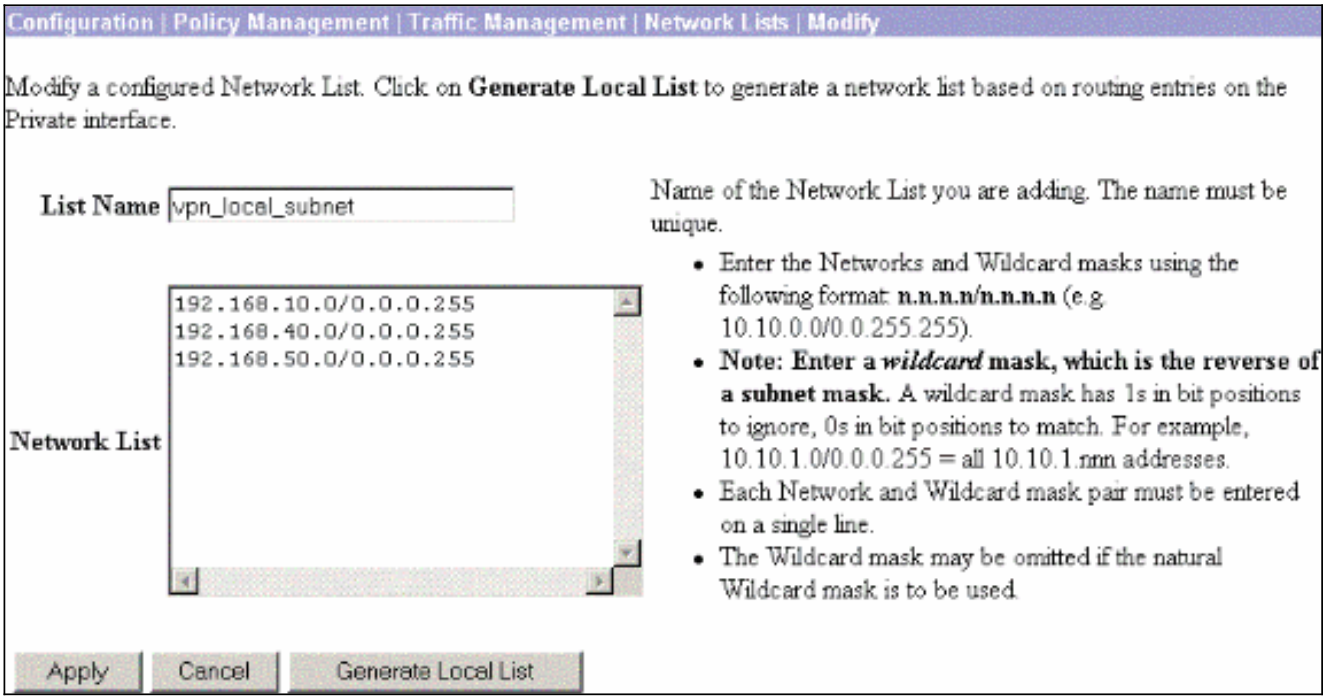
1. Escolha **Configuration > Interfaces** para verificar novamente as interfaces depois de ativar a GUI.



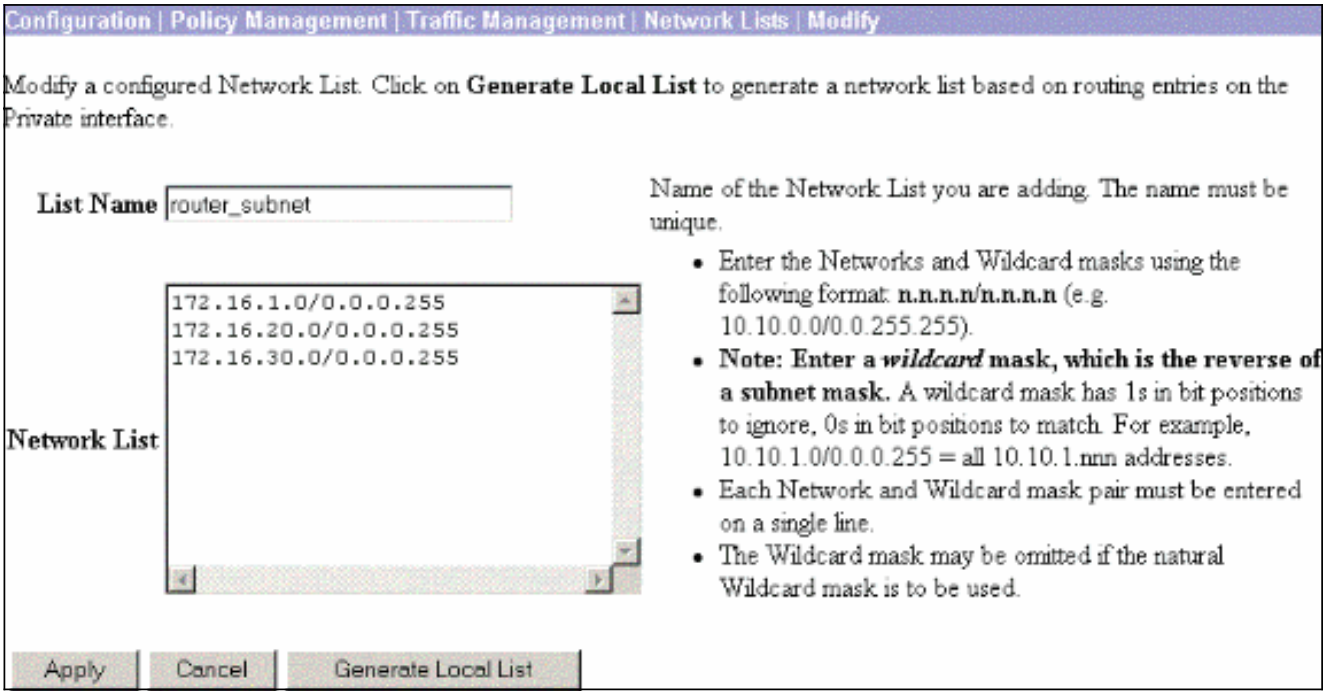
2. Escolha Configuration > System > IP Routing > Default Gateways para configurar o Gateway Padrão (Internet) e o Gateway Padrão de Túnel(interno) **Gateway** para IPsec para acessar as outras sub-redes na rede privada.



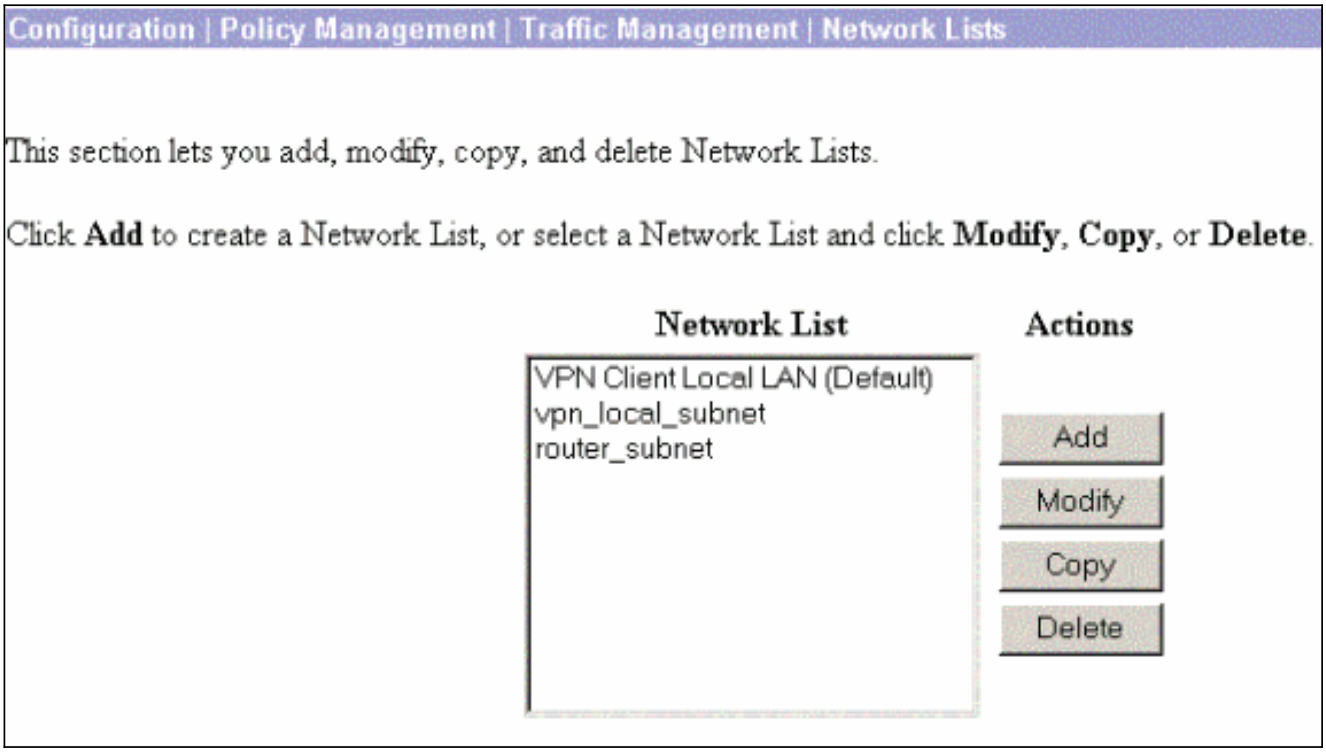
3. Escolha **Configuration > Policy Management > Network Lists** para criar as listas de rede que definem o tráfego a ser criptografado.Estas são as redes locais:



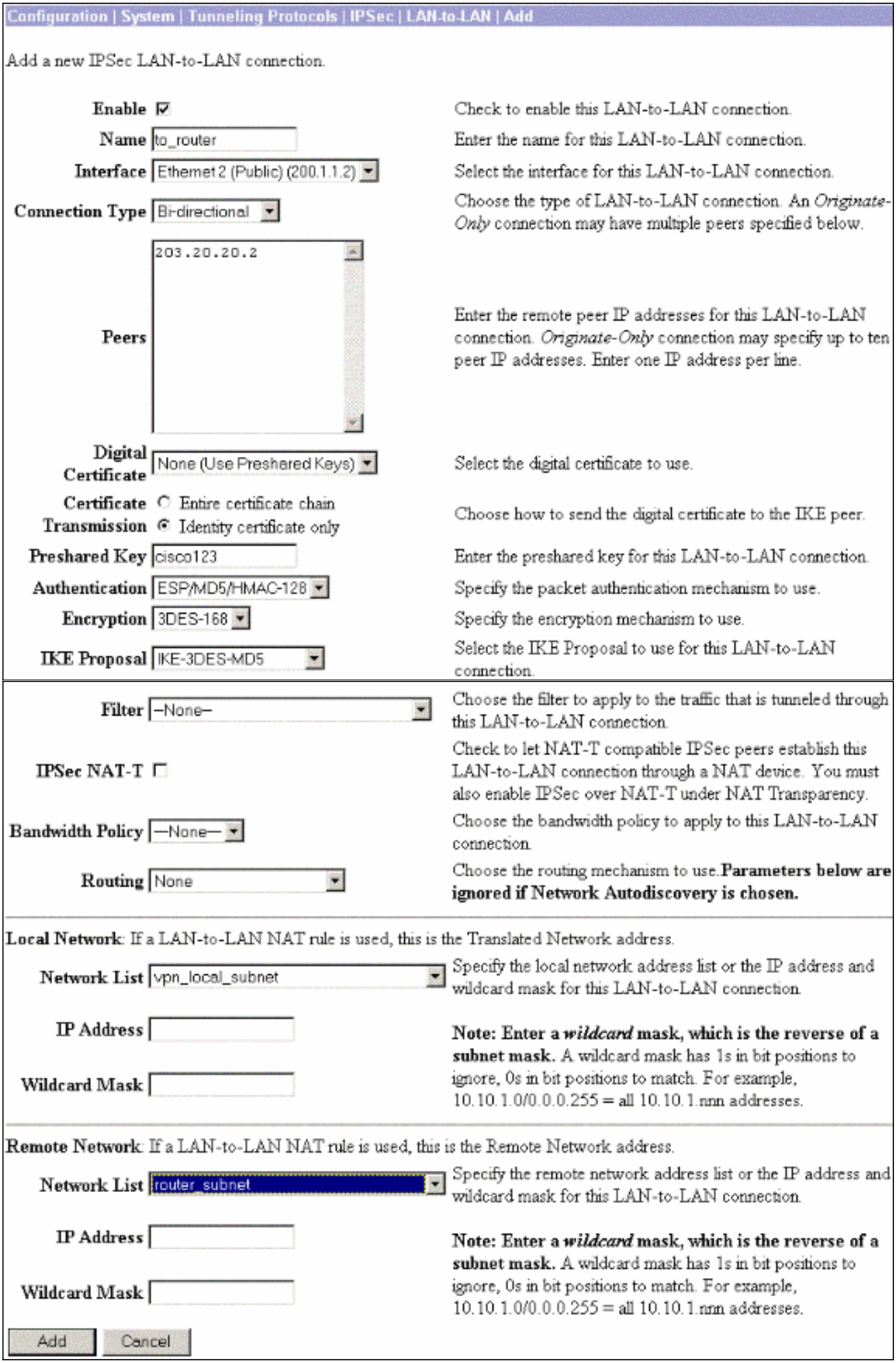
Estas são as redes
remotas:



4. Quando concluídas, estas são as duas listas de rede:**Observação:** se o túnel IPsec não aparecer, verifique se o tráfego interessante corresponde em ambos os lados. O tráfego interessante é definido pela lista de acesso no roteador e nas caixas PIX. Eles são definidos por listas de rede nos VPN
Concentrators.

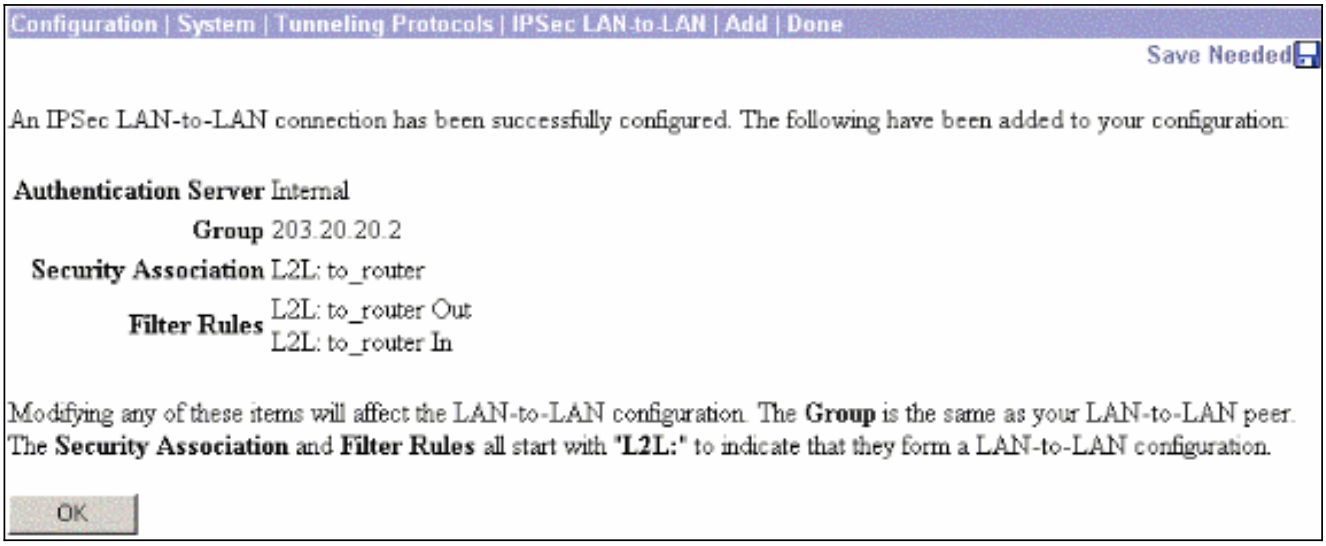


5. Escolha **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN** e defina o túnel de LAN para
LAN.

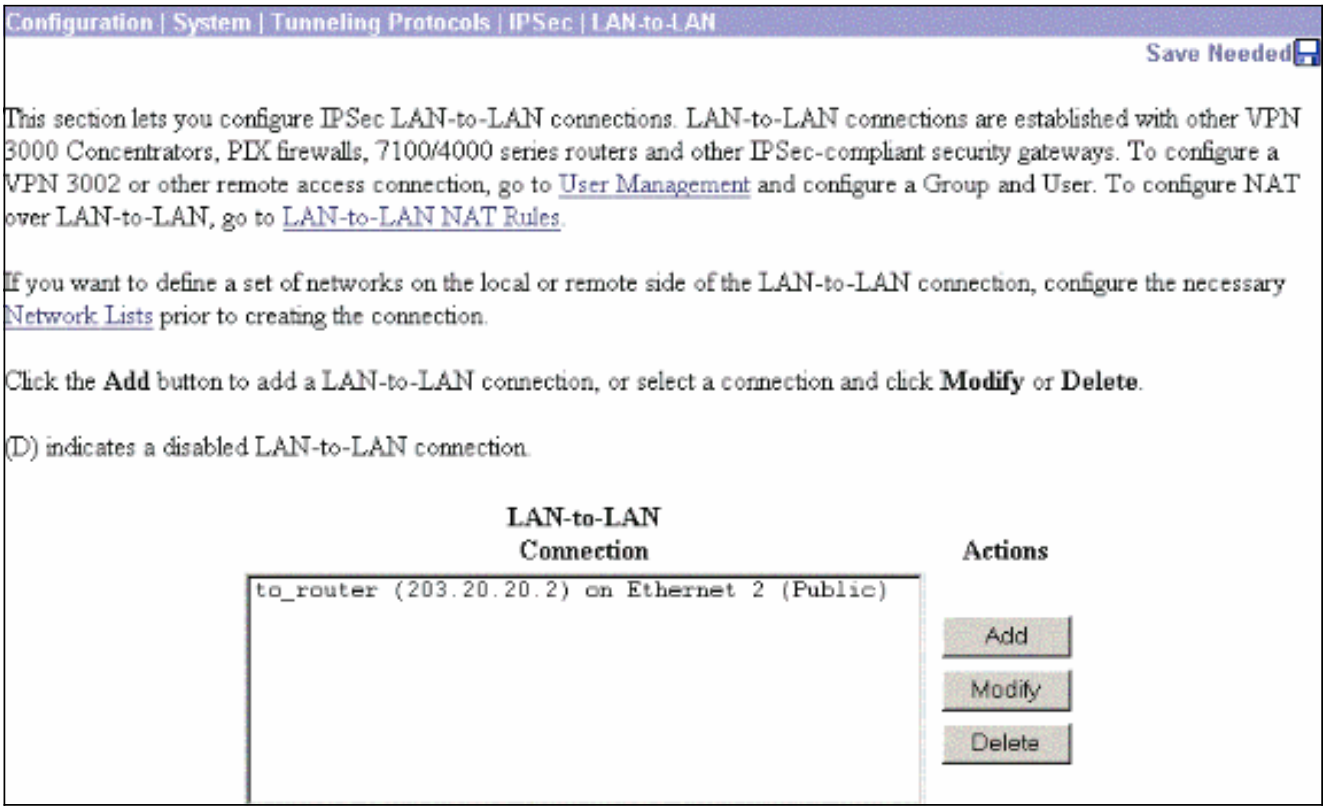


6. Depois de clicar em **Apply**, esta janela é exibida com a outra configuração que é criada

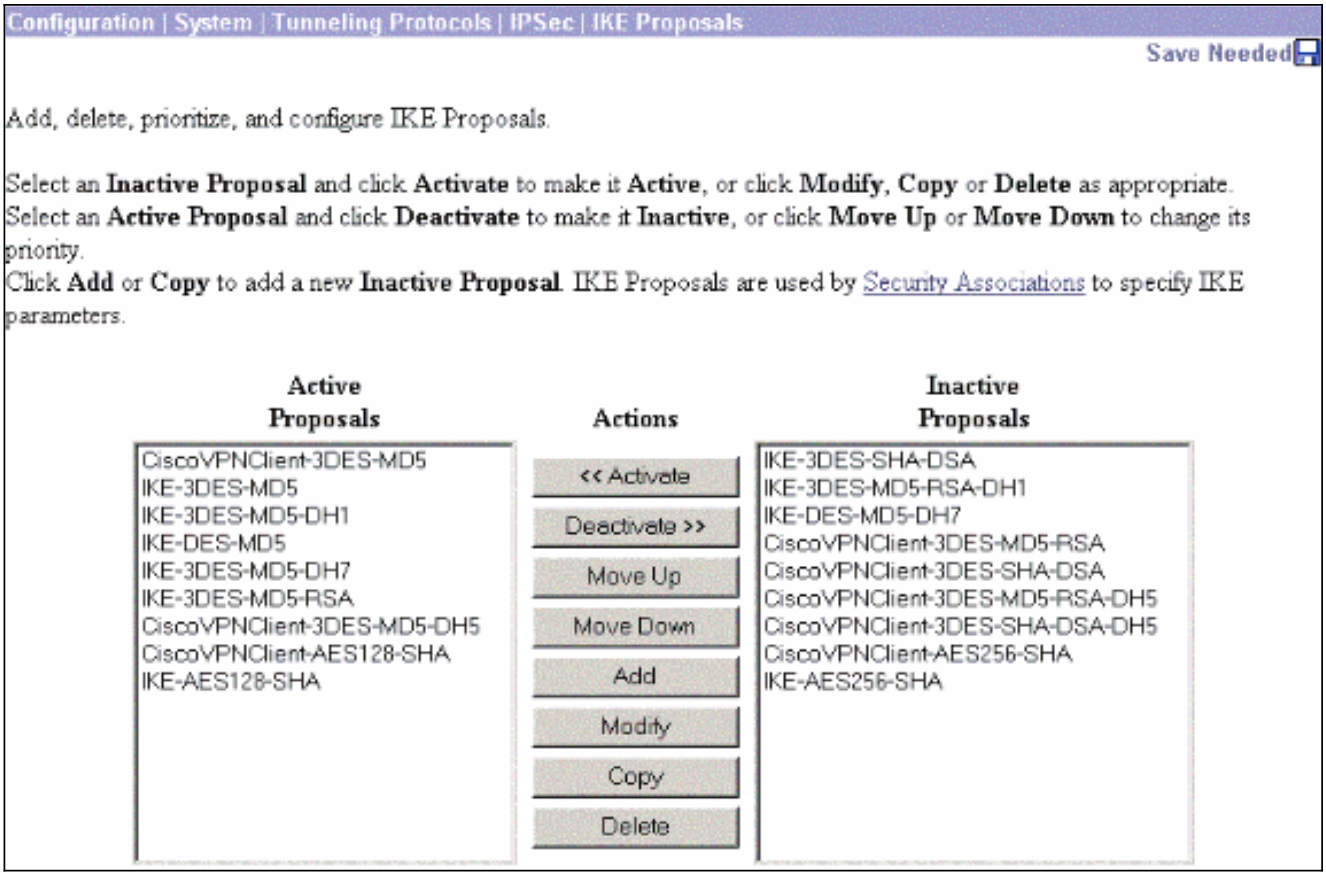
automaticamente como resultado da configuração do túnel LAN para LAN.



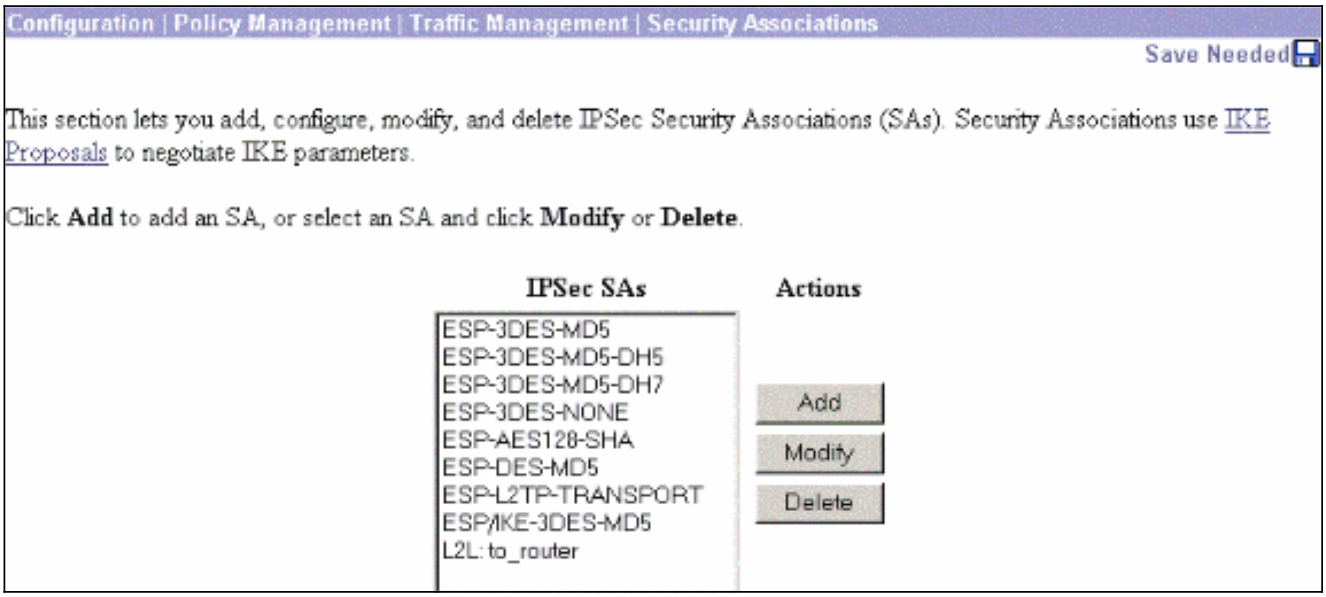
Os parâmetros IPsec LAN a LAN criados anteriormente podem ser exibidos ou modificados em **Configuração > Sistema > Protocolos de encapsulamento > IPSec LAN a LAN**.



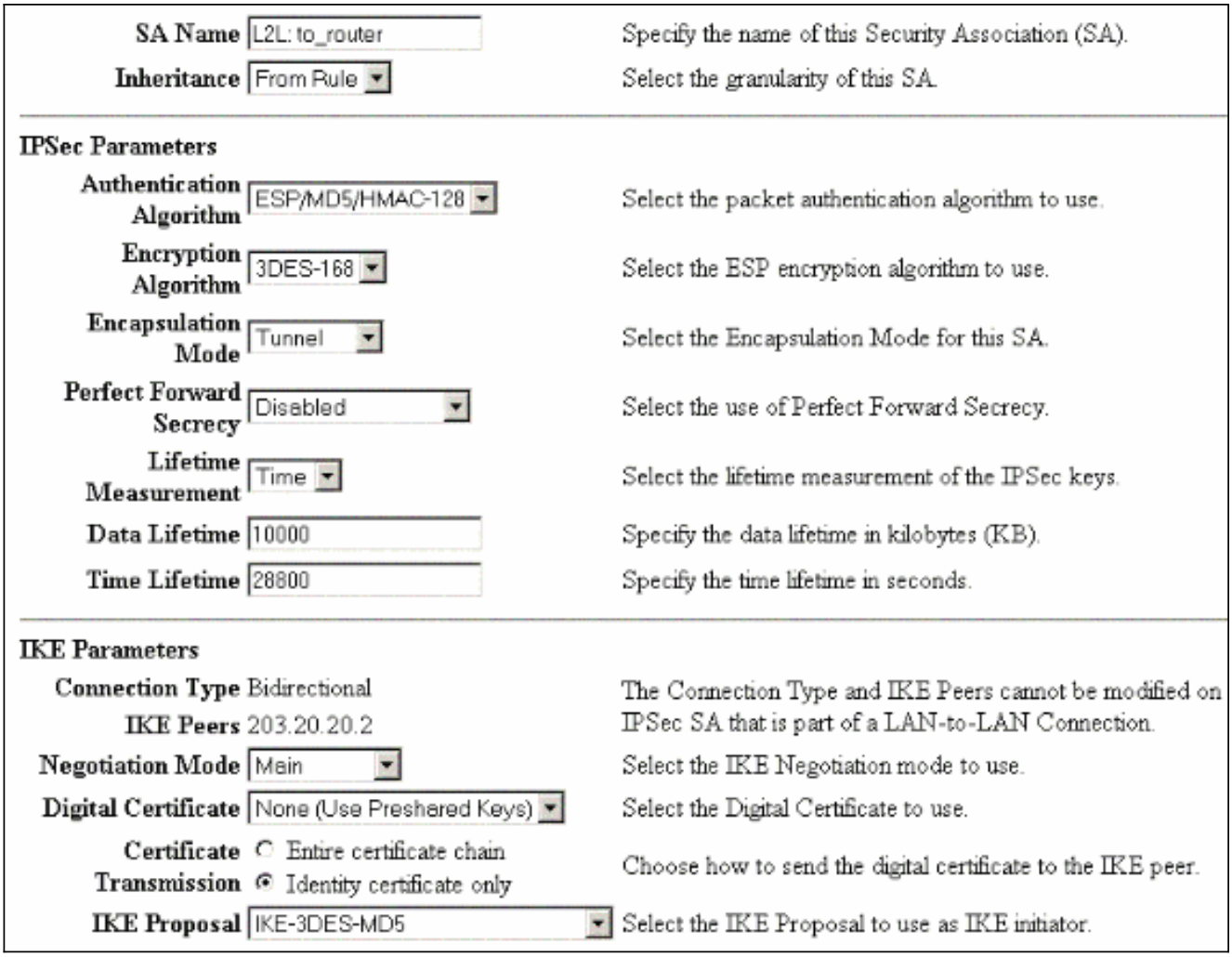
7. Escolha Configuração > **Sistema > Protocolos de tunelamento > IPSec > Propostas IKE** para confirmar a Proposta IKE ativa.



8. Escolha **Configuration > Policy Management > Traffic Management > Security Associations** para ver a lista de Security Associations.



9. Clique no nome da associação de segurança e, em seguida, clique em **Modificar** para verificar as associações de segurança.



Verificar

Esta seção lista os comandos **show** usados nesta configuração.

No roteador

Esta seção fornece informações que você pode usar para confirmar se sua configuração funciona adequadamente.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **show crypto ipsec sa** — Mostra as configurações usadas pelas Associações de Segurança atuais.
- **show crypto isakmp sa** — Mostra todas as associações de segurança atuais do Internet Key Exchange em um peer.
- **show crypto engine connection ative** —Mostra as conexões de sessão criptografada ativas atuais para todos os mecanismos de criptografia.

Você pode usar a IOS Command Lookup Tool (clientes registrados somente) para ver mais informações sobre comandos específicos.

No VPN Concentrator

Escolha Configuration > **System** > **Events** > **Classes** > **Modify** para ativar o registro. Essas opções estão disponíveis:

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

Gravidade para registro = 1-13

Severidade para console = 1-3

Selecione **Monitoring** > **Event Log** para recuperar o log de eventos.

Troubleshoot

No roteador

Consulte Informações Importantes sobre Comandos de Depuração antes de tentar qualquer comando de depuração.

- **debug crypto engine — Exibe o tráfego que está criptografado.**
- **debug crypto ipsec — Exibe as negociações de IPSec de fase 2**
- **debug crypto isakmp — Exibe as negociações ISAKMP da Fase 1.**

Problema - Não é possível iniciar o túnel

Mensagem de erro

```
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>
```

Solução

Conclua esta ação para configurar o número desejado de logins simultâneos ou defina os logins simultâneos para 5 para esta SA:

Vá para **Configuration > User Management > Groups > Modify 10.19.187.229 > General > Simultaneouts Logins** e altere o número de logins para 5.

PFS

Nas negociações de IPsec, o Perfect Forward Secrecy (PFS) garante que cada nova chave criptográfica não tenha relação com nenhuma chave anterior. Habilite ou desabilite o PFS em ambos os tuneis peer. Caso contrário, o túnel IPsec de LAN para LAN (L2L) não é estabelecido nos roteadores.

Para especificar que o IPsec deve pedir PFS quando novas Associações de Segurança forem solicitadas para esta entrada de mapa de criptografia ou que o IPsec exige PFS quando recebe solicitações para novas Associações de Segurança, use o comando **set pfs** no modo de configuração de mapa de criptografia. Para especificar que o IPsec não deve solicitar o PFS, use a forma **no** desse comando.

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

Para o comando set pfs:

- *group1* —Especifica que o IPsec deve usar o grupo Diffie-Hellman prime modulus de 768 bits quando a nova troca Diffie-Hellman é executada.
- *group2* —Especifica que o IPsec deve usar o grupo Diffie-Hellman prime modulus de 1024 bits quando a nova troca Diffie-Hellman é executada.

Por padrão, o PFS não é solicitado. Se nenhum grupo for especificado com este comando, group1 será usado como o padrão.

Exemplo:

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

Consulte a Referência de Comandos de Segurança do Cisco IOS para obter mais informações sobre o comando **set pfs**.

Informações Relacionadas

- Soluções de Troubleshooting Mais Comuns de VPN IPsec L2L e de Acesso Remoto
- Cisco VPN 3000 Series Concentrators
- Cisco VPN 3002 Hardware Clients
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems