

Configuring the Cisco VPN 3000 Concentrator to a Cisco Router

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configuração do VPN Concentrator](#)

[Verificar](#)

[No roteador](#)

[No VPN Concentrator](#)

[Troubleshoot](#)

[No roteador](#)

[Problema - Não é possível iniciar o túnel](#)

[PFS](#)

[Informações Relacionadas](#)

[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(1)**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.](#)

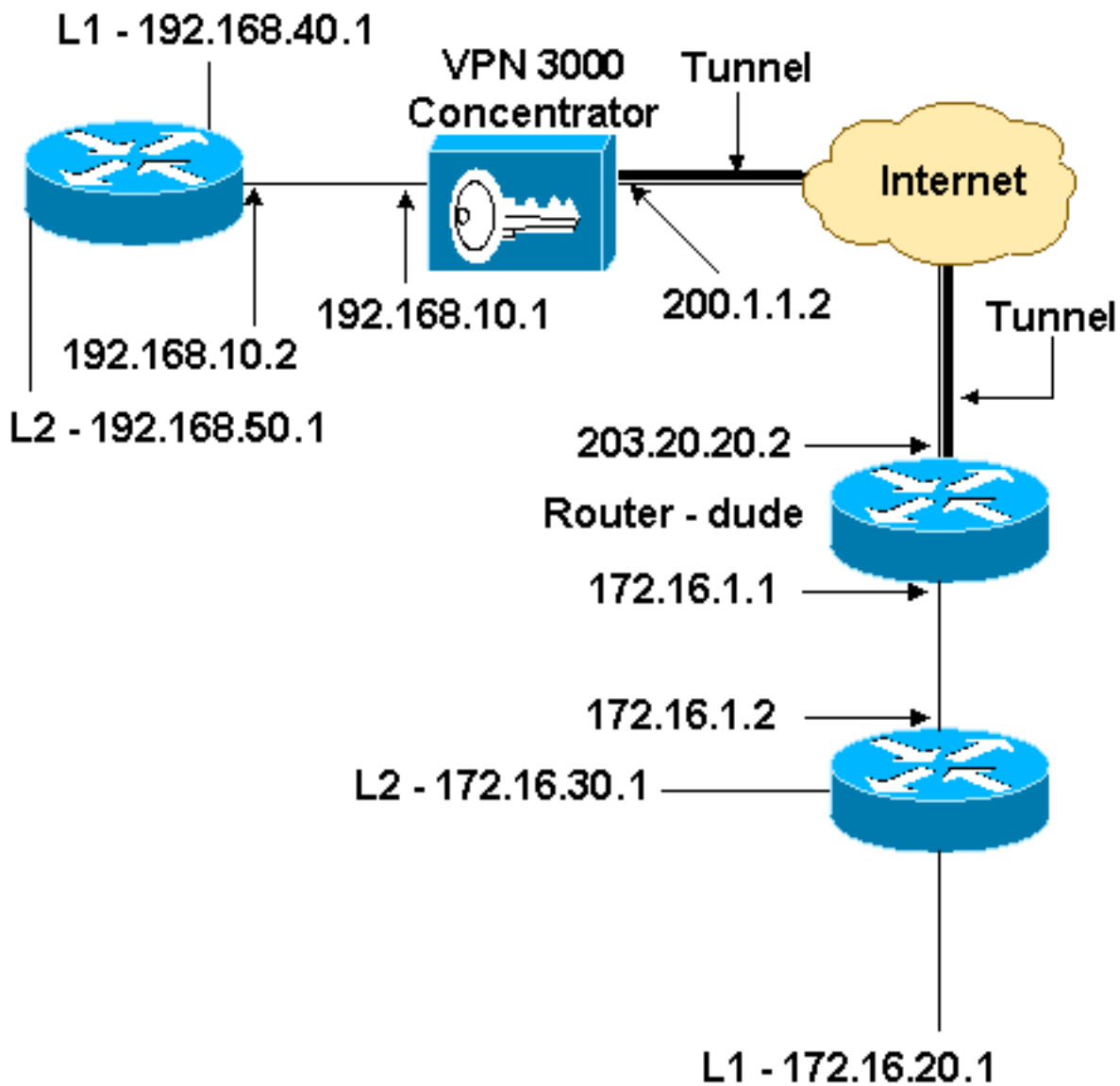
Configurar

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 Factory/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.

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. 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.

Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

Default Gateway Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.

Metric Enter the metric, from 1 to 16.

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

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 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.

Estas são as redes remotas:

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

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

- 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.

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
```

Apply Cancel Generate Local List

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.

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	Actions
VPN Client Local LAN (Default)	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
vpn_local_subnet	
router_subnet	

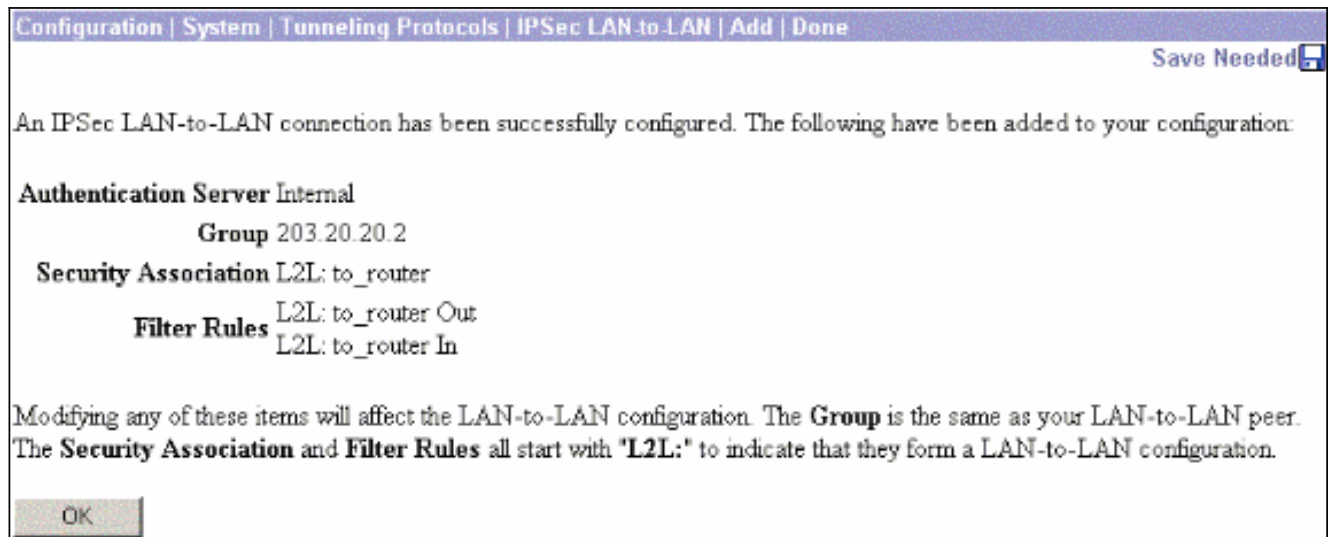
5. Escolha **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN** e defina o túnel de LAN para LAN.

Add a new IPSec LAN-to-LAN connection.

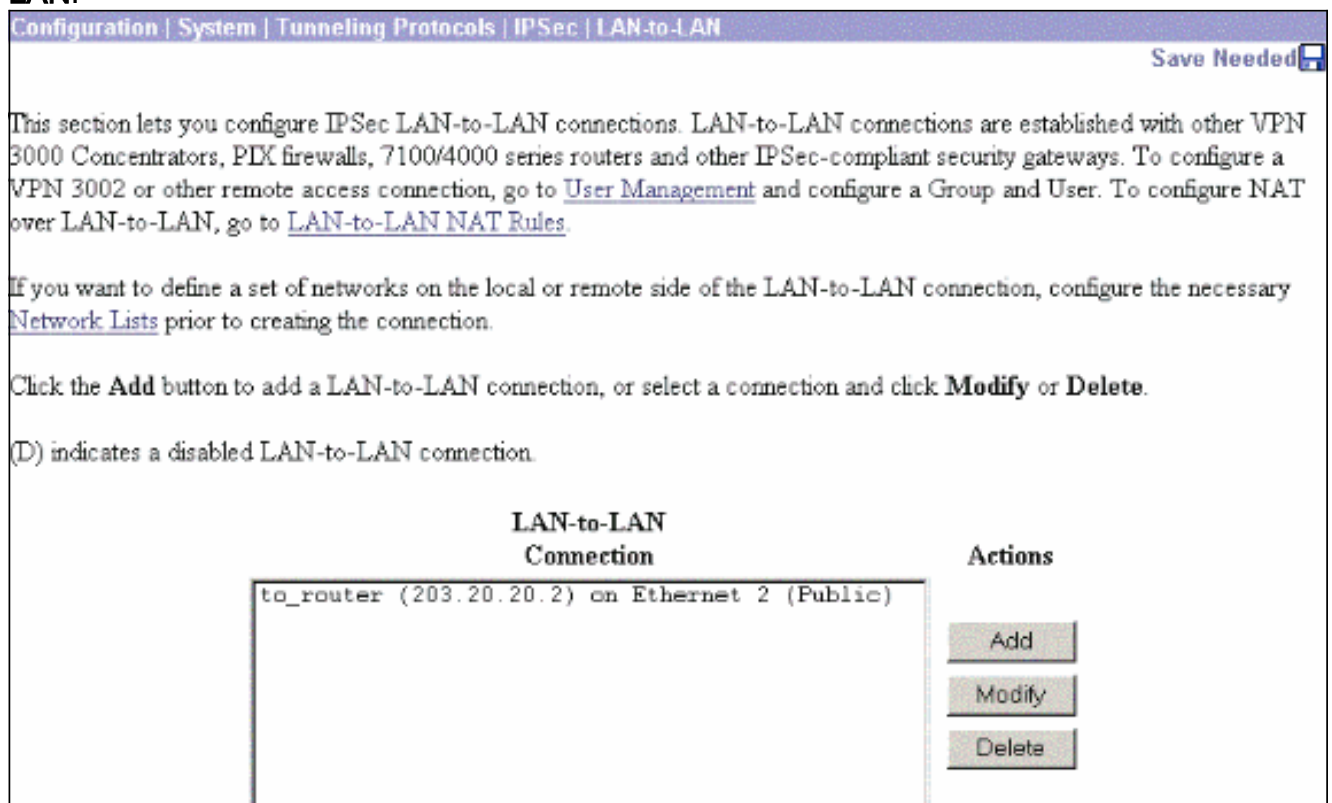
<p>Enable <input checked="" type="checkbox"/></p> <p>Name <input type="text" value="to_router"/></p> <p>Interface <input type="text" value="Ethernet 2 (Public) (200.1.1.2)"/></p> <p>Connection Type <input type="text" value="Bi-directional"/></p> <p>Peers</p> <div style="border: 1px solid gray; padding: 2px; min-height: 100px;"> <p>203.20.20.2</p> </div> <p>Digital Certificate <input type="text" value="None (Use Preshared Keys)"/></p> <p>Certificate <input type="radio"/> Entire certificate chain</p> <p>Transmission <input checked="" type="radio"/> Identity certificate only</p> <p>Preshared Key <input type="text" value="cisco123"/></p> <p>Authentication <input type="text" value="ESP/MD5/HMAC-128"/></p> <p>Encryption <input type="text" value="3DES-168"/></p> <p>IKE Proposal <input type="text" value="IKE-3DES-MD5"/></p>	<p>Check to enable this LAN-to-LAN connection.</p> <p>Enter the name for this LAN-to-LAN connection.</p> <p>Select the interface for this LAN-to-LAN connection.</p> <p>Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.</p> <p>Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses. Enter one IP address per line.</p> <p>Select the digital certificate to use.</p> <p>Choose how to send the digital certificate to the IKE peer.</p> <p>Enter the preshared key for this LAN-to-LAN connection.</p> <p>Specify the packet authentication mechanism to use.</p> <p>Specify the encryption mechanism to use.</p> <p>Select the IKE Proposal to use for this LAN-to-LAN connection.</p>
<p>Filter <input type="text" value="-None-"/></p> <p>IPSec NAT-T <input type="checkbox"/></p> <p>Bandwidth Policy <input type="text" value="-None-"/></p> <p>Routing <input type="text" value="None"/></p>	<p>Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.</p> <p>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.</p> <p>Choose the bandwidth policy to apply to this LAN-to-LAN connection.</p> <p>Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.</p>
<p>Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.</p> <p>Network List <input type="text" value="vpn_local_subnet"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	
<p>Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.</p> <p>Network List <input type="text" value="router_subnet"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	
<p><input type="button" value="Add"/> <input type="button" value="Cancel"/></p>	

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.



- Escolha Configuração > Sistema > Protocolos de tunelamento > IPsec > Propostas IKE para confirmar a Proposta IKE ativa.

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals Save Needed

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	Actions	Inactive 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	<< Activate Deactivate >> Move Up Move Down Add Modify Copy Delete	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. Escolha **Configuration > Policy Management > Traffic Management > Security Associations** para ver a lista de Security Associations.

Configuration | Policy Management | Traffic Management | Security Associations Save Needed

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	Actions
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	Add Modify Delete

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

SA Name	<input type="text" value="L2L: to_router"/>	Specify the name of this Security Association (SA).
Inheritance	<input type="text" value="From Rule"/>	Select the granularity of this SA.
IPSec Parameters		
Authentication Algorithm	<input type="text" value="ESP/MD5/HMAC-128"/>	Select the packet authentication algorithm to use.
Encryption Algorithm	<input type="text" value="3DES-168"/>	Select the ESP encryption algorithm to use.
Encapsulation Mode	<input type="text" value="Tunnel"/>	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy	<input type="text" value="Disabled"/>	Select the use of Perfect Forward Secrecy.
Lifetime Measurement	<input type="text" value="Time"/>	Select the lifetime measurement of the IPSec keys.
Data Lifetime	<input type="text" value="10000"/>	Specify the data lifetime in kilobytes (KB).
Time Lifetime	<input type="text" value="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	<input type="text" value="Main"/>	Select the IKE Negotiation mode to use.
Digital Certificate	<input type="text" value="None (Use Preshared Keys)"/>	Select the Digital Certificate to use.
Certificate Transmission	<input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
IKE Proposal	<input type="text" value="IKE-3DES-MD5"/>	Select the IKE Proposal to use as IKE initiator.

[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 active** — 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](#)