

Configuración del concentrador Cisco VPN 3000 en un router Cisco

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración del concentrador VPN](#)

[Verificación](#)

[En el router](#)

[En el concentrador VPN](#)

[Troubleshoot](#)

[En el router](#)

[Problema - No se puede iniciar el túnel](#)

[PFS](#)

[Información Relacionada](#)

[Introducción](#)

Este ejemplo de configuración muestra cómo conectar una red privada detrás de un router que ejecuta el software Cisco IOS[®] a una red privada detrás del concentrador Cisco VPN 3000. Los dispositivos de las redes se reconocen entre sí por las direcciones privadas.

[Prerequisites](#)

[Requirements](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 2611 Router con Cisco IOS Software Release 12.3.1(1)**Nota:** Asegúrese de que los

routers Cisco serie 2600 estén instalados con una imagen de IPsec VPN IOS crypto que soporte la función VPN.

- Concentrador Cisco VPN 3000 con 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.

Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco para obtener más información sobre las convenciones del documento.](#)

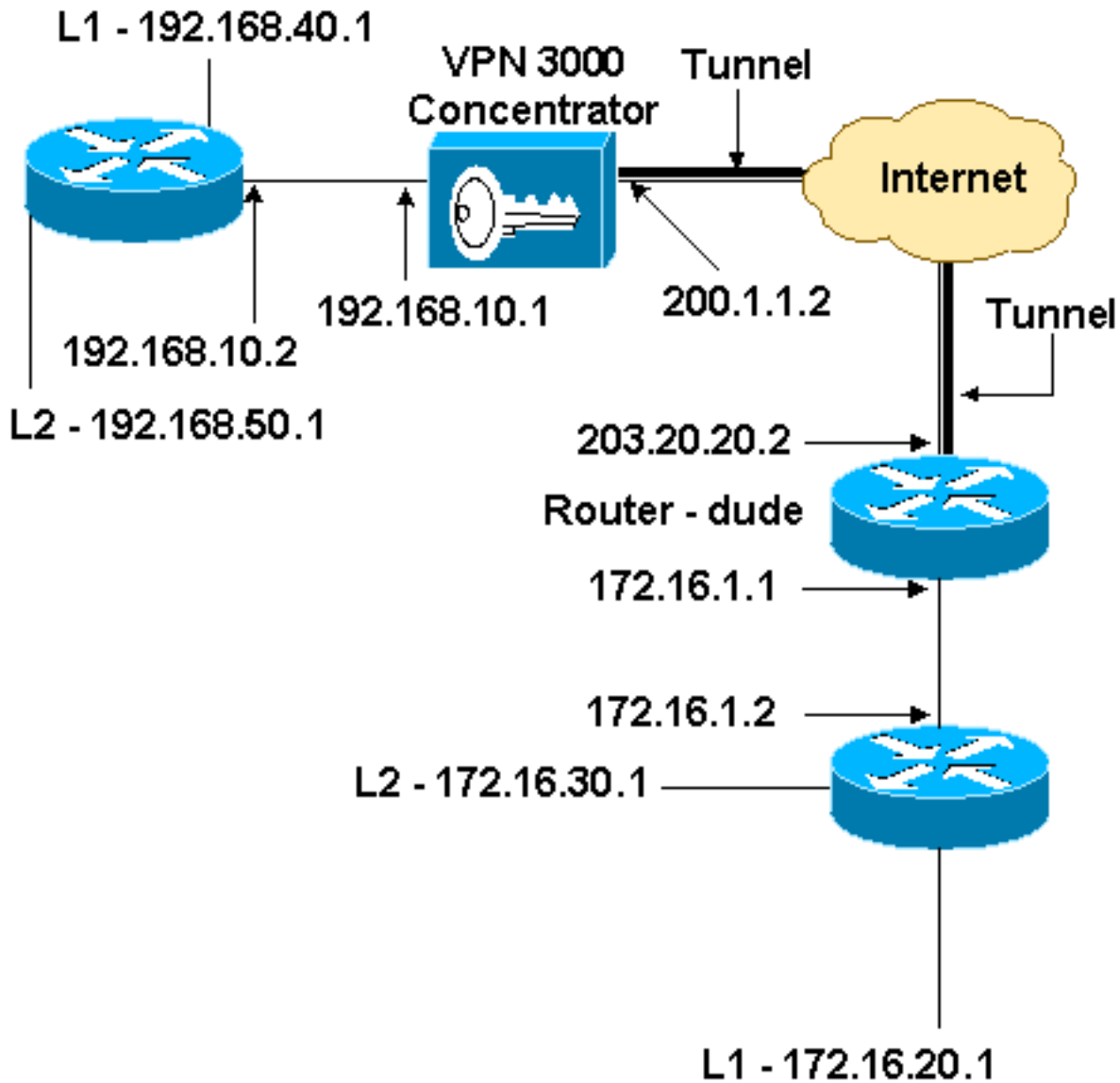
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la [Command Lookup Tool](#) (sólo [clientes registrados](#)) para obtener más información sobre los comandos utilizados en este documento.

Diagrama de la red

Este documento utiliza esta configuración de red:



Configuraciones

Este documento usa esta configuración.

Configuración del router

```

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
```

Configuración del concentrador VPN

En esta configuración de laboratorio, se accede primero al concentrador VPN a través del puerto de la consola y se agrega una configuración mínima para que se pueda realizar la configuración adicional a través de la interfaz gráfica de usuario (GUI).

Elija **Administration > System Reboot > Schedule reboot > Reboot with Factory/Default Configuration** para asegurarse de que no haya una configuración existente en el VPN Concentrator.

El concentrador VPN aparece en Configuración rápida y estos elementos se configuran después del reinicio:

- Fecha/hora
- Interfaces/Masks in Configuration > Interfaces (public=200.1.1.2/24, private=192.168.10.1/24)
- Gateway predeterminada en Configuration (Configuración) > System (Sistema) > ip routing (Ruteo de IP) > Default_Gateway (200.1.1.1) (Gateway predeterminada [200.1.1.1])

En este momento, el VPN Concentrator es accesible a través de HTML desde la red interna.

Nota: Debido a que el concentrador VPN se administra desde afuera, también debe seleccionar:

- **Configuration > Interfaces > 2-public > Select IP Filter > 1. Private (Default).**
- **Administration > Access Rights > Access Control List > Add Manager Workstation** para agregar la dirección IP del administrador externo.

Esto no es necesario a menos que administre el VPN Concentrator desde *afuera*.

1. Elija **Configuration > Interfaces** para volver a verificar las interfaces después de activar la GUI.

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. Elija Configuration > System > IP Routing > Default Gateways para configurar la gateway predeterminada(Internet) y la gateway predeterminada del túnel (interior) para IPsec para alcanzar las otras subredes en la red privada.

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.

Apply

Cancel

3. Elija Configuration > Policy Management > Network Lists para crear las listas de red que definen el tráfico que se cifrará. Estas son las redes locales:

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.

Apply

Cancel

Generate Local List

Estas son las 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. Una vez terminado, estas son las dos listas de red: **Nota:** Si el túnel IPsec no se activa, verifique si el tráfico interesante coincide con ambos lados. El tráfico interesante se define por la lista de acceso en el router y los cuadros PIX. Se definen mediante listas de red en los concentradores VPN.

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) vpn_local_subnet router_subnet	Add Modify Copy Delete

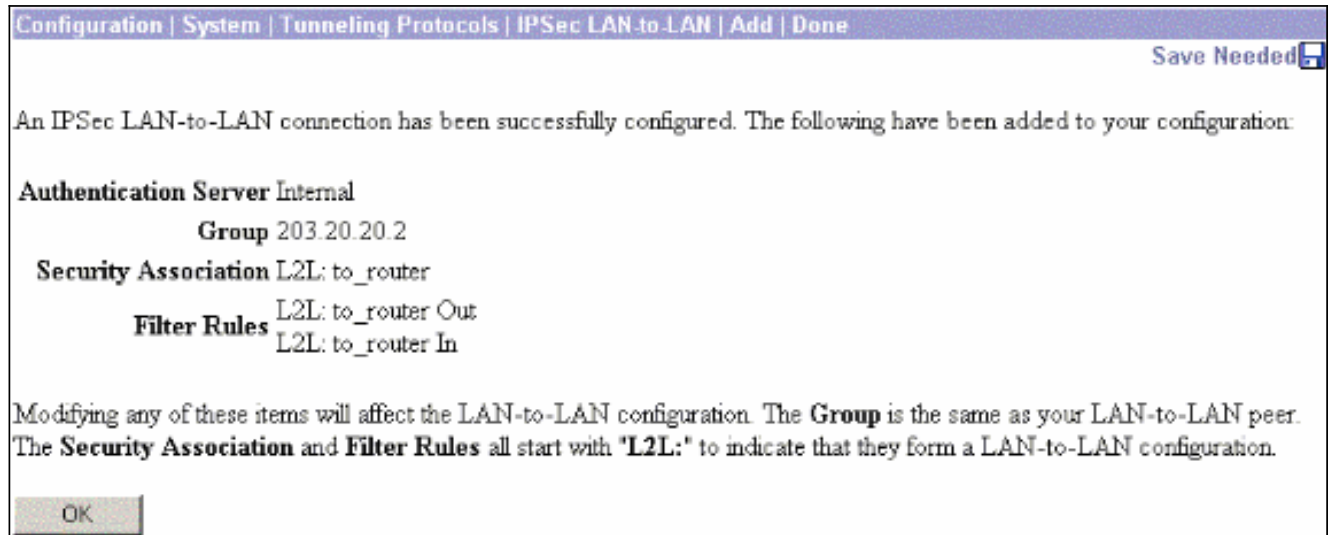
5. Elija Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN y defina el túnel de LAN a LAN.

Add a new IPSec LAN-to-LAN connection.

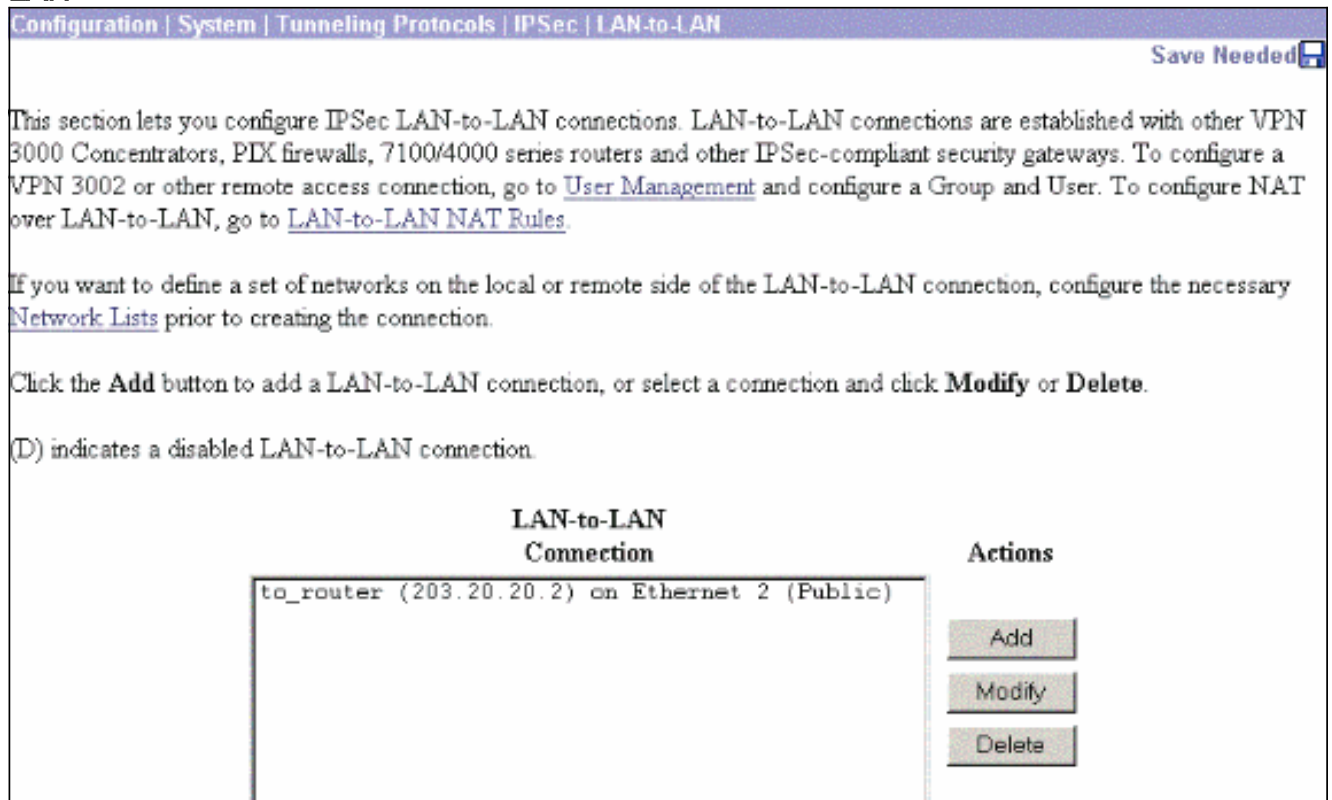
<p>Enable <input checked="" type="checkbox"/></p> <p>Name <input type="text" value="to_router"/></p> <p>Interface <input type="text" value="Ethernet2 (Public) (200.1.1.2)"/></p> <p>Connection Type <input type="text" value="Bi-directional"/></p> <p>Peers</p> <div style="border: 1px solid gray; padding: 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. Después de hacer clic en **Aplicar**, esta ventana se muestra con la otra configuración que se

crea automáticamente como resultado de la configuración del túnel de LAN a LAN.



Los parámetros IPsec de LAN a LAN creados anteriormente se pueden ver o modificar en Configuración > Sistema > Tunelización de los Protocolos > IPsec LAN a LAN.



7. Elija Configuration > System > Tunneling Protocols > IPsec > IKE Proposals para confirmar la propuesta IKE activa.

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	<input type="button" value="« Activate"/> <input type="button" value="Deactivate »"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="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. Elija **Configuration > Policy Management > Traffic Management > Security Associations** para ver la 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	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>

9. Haga clic en el nombre de la asociación de seguridad y, a continuación, haga clic en **Modificar** para verificar las asociaciones de seguridad.

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	<input type="text" value="Bidirectional"/>	The Connection Type and IKE Peers cannot be modified on IPSec SA that is part of a LAN-to-LAN Connection.
IKE Peers	<input type="text" value="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.

Verificación

Esta sección enumera los comandos **show** utilizados en esta configuración.

En el router

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

- **show crypto ipsec sa:** muestra la configuración utilizada por las asociaciones de seguridad actuales.
- **show crypto isakmp sa:** muestra todas las asociaciones de seguridad de intercambio de claves de Internet actuales en un par.
- **show crypto engine connection active:** muestra las conexiones de sesión cifradas activas actuales para todos los motores criptográficos.

Puede utilizar la [Herramienta de Búsqueda de Comandos de IOS \(sólo clientes registrados\)](#) para ver más información sobre comandos específicos.

En el concentrador VPN

Elija Configuration > **System** > **Events** > **Classes** > Modify para activar el registro. Estas opciones están disponibles:

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

Gravedad de registro = 1-13

Gravedad en la consola = 1-3

Seleccione **Monitoring** > **Event Log** para recuperar el registro de eventos.

Troubleshoot

En el router

Consulte [Información Importante sobre Comandos Debug](#) antes de intentar cualquier comando debug.

- **debug crypto engine**: muestra el tráfico cifrado.
- **debug crypto ipsec** — Muestra los IPsec Negotiations de la Fase 2.
- **debug crypto isakmp** — Muestra las negociaciones ISAKMP para la fase 1.

Problema - No se puede iniciar el túnel

Mensaje de error

```
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>
```

Solución

Complete esta acción para configurar el número deseado de inicios de sesión simultáneos o establezca los inicios de sesión simultáneos en 5 para esta SA:

Vaya a **Configuration** > **User Management** > **Groups** > **Modify 10.19.187.229** > **General** > **Simultaneouts Logins** y cambie el número de logins a 5.

PFS

En las negociaciones de IPsec, Perfect Forward Secrecy (PFS) garantiza que cada clave criptográfica nueva no esté relacionada a cualquier clave anterior. Habilite o inhabilite PFS en ambos peers de túnel. De lo contrario, el túnel IPsec de LAN a LAN (L2L) no se establece en los routers.

Para especificar que IPsec debe solicitar PFS cuando se solicitan nuevas Asociaciones de Seguridad para esta entrada de mapa crypto, o que IPsec requiere PFS cuando recibe solicitudes de nuevas Asociaciones de Seguridad, utilice el comando **set pfs** en el modo de configuración de mapa crypto. Para especificar que IPsec no debe solicitar PFS, utilice la forma **no** de este comando.

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

Para el comando set pfs:

- *group1* : especifica que IPsec debe utilizar el grupo de módulos primos Diffie-Hellman de 768 bits cuando se realiza el nuevo intercambio Diffie-Hellman.
- *group2* : especifica que IPsec debe utilizar el grupo de módulos primos Diffie-Hellman de 1024 bits cuando se realiza el nuevo intercambio Diffie-Hellman.

De forma predeterminada, PFS no se solicita. Si no se especifica ningún grupo con este comando, como valor predeterminado se utiliza group1.

Ejemplo:

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

Consulte [Referencia de Comandos de Seguridad de Cisco IOS](#) para obtener más información sobre el comando **set pfs**.

Información Relacionada

- [Soluciones a los Problemas más frecuentes de IPsec VPN L2L y de Acceso Remoto](#)
- [Cisco VPN 3000 Series Concentrators](#)
- [Cisco VPN 3002 Hardware Clients](#)
- [Negociación IPsec/Protocolos IKE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)