Configuración del ruteo redundante en el concentrador VPN 3000

Contenido

Introducción

Este documento describe cómo configurar un failover VPN redundante si un sitio remoto pierde su concentrador VPN 3000 o conectividad a Internet. En este ejemplo, suponga que la red corporativa situada detrás de la VPN 3030B utiliza Open Shortest Path First (OSPF) como su protocolo de routing predeterminado.

Nota: Cuando se redistribuye entre los protocolos de ruteo, puede formar un loop de ruteo que puede causar problemas en la red. OSPF se utiliza en este ejemplo, pero no es el único protocolo de ruteo que se puede utilizar.

El objetivo de este ejemplo es que la red 192.168.1.0 utilice el túnel rojo (en circunstancias de funcionamiento normales), representado en la sección Diagrama de red, para alcanzar 192.168.3.x. Si el túnel, el concentrador VPN o el ISP se descartan, la red 192.168.3.0 se aprende a través de un protocolo de ruteo dinámico sobre el túnel verde. Además, la conectividad no se pierde en el sitio 192.168.3.0. Una vez resuelto el problema, el tráfico vuelve automáticamente al túnel rojo.

Nota: RIP tiene un temporizador de envejecimiento de tres minutos antes de permitir que se acepte una nueva ruta sobre una ruta no válida. Además, supongamos que se crean los túneles y que el tráfico puede pasar entre los pares.

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.

- Routers de Cisco 3620 y 3640
- Concentrador Cisco VPN 3080 - Versión: Concentrador Cisco Systems, Inc./VPN 3000 Versión 4.7
- Concentrador Cisco VPN 3060 - Versión: Cisco Systems, Inc./VPN 3000 Concentrator Series Versión 4.7
- Concentrador Cisco VPN 3030 - Versión: Cisco Systems, Inc./VPN 3000 Concentrator Series Versión 4.7

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

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

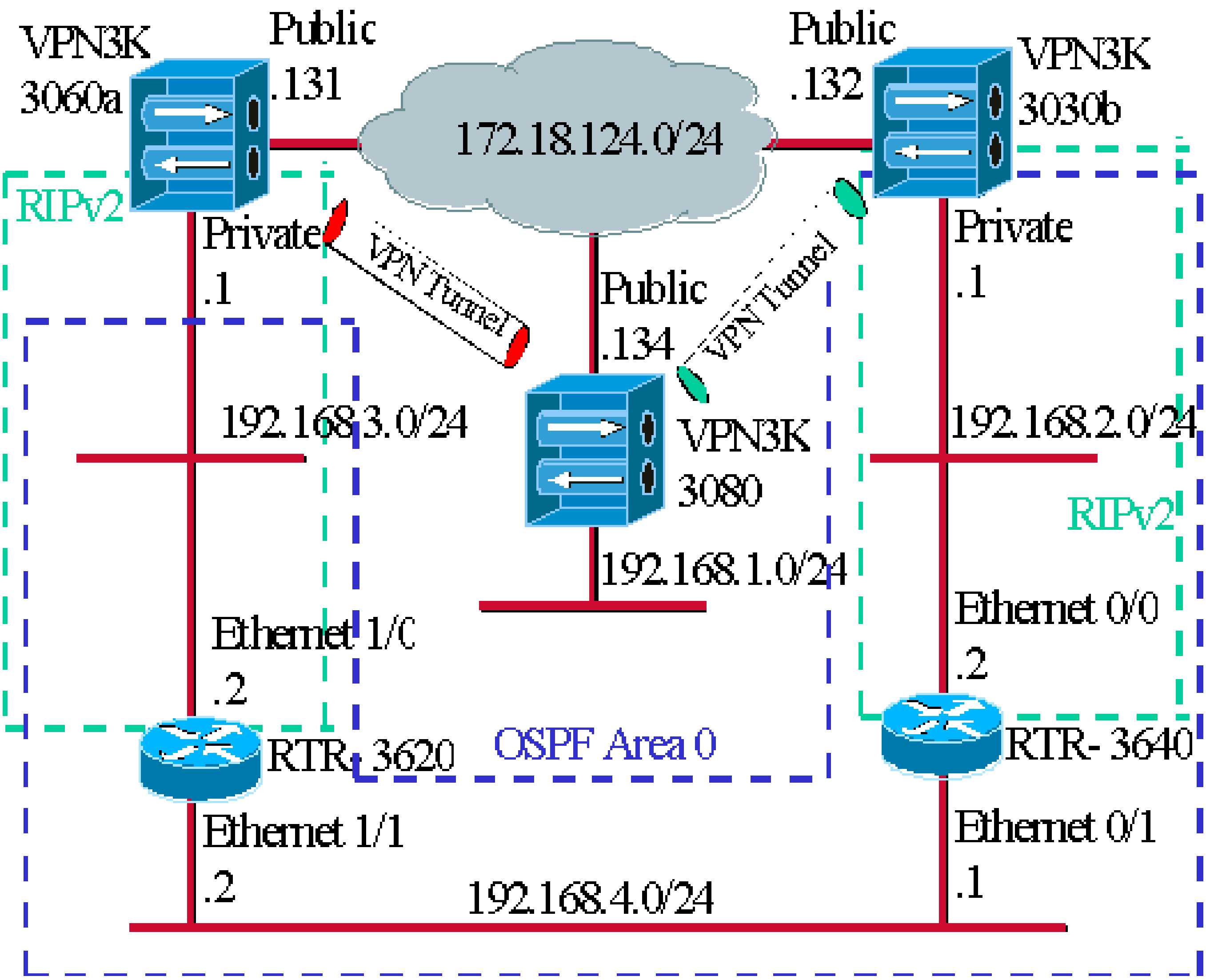
Configurar

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

Nota: Para encontrar información adicional sobre los comandos usados en este documento, utilice la Command Lookup Tool (sólo clientes registrados) .

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Los guiones azules indican que OSPF está habilitado desde VPN 3030b a RTR-3640 y RTR-3620.

Los guiones verdes indican que RIPv2 está habilitado desde VPN privada 3060a a RTR-3620, RTR-3640 y VPN privada 3030b.

RIPv2 también está habilitado en los túneles VPN rojo y verde porque la detección de red está habilitada. No es necesario habilitar RIP en la interfaz privada VPN 3080. Tampoco hay RIP en la red 192.168.4.x porque todas las rutas son aprendidas por OSPF a través de este link.

Nota: Los PC de las redes 192.168.2.x y 192.168.3.x necesitan que sus gateways predeterminados apunten a los routers y no a los concentradores VPN. Permita que los routers decidan dónde enrutar los paquetes.

Configuración del router

Este documento utiliza estas configuraciones de router:

- Router 3620
- Router 3640

Router 3620

```
rtr-3620#write  terminal
Building configuration...

Current configuration : 873 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rtr-3620
!
ip subnet-zero
!
interface Ethernet1/0
 ip address 192.168.3.2 255.255.255.0
 half-duplex
!
interface Ethernet1/1
 ip address 192.168.4.2 255.255.255.0
 half-duplex
!
router ospf 1
 log-adjacency-changes
!--- To pass the routes learned through RIP into the
OSPF process, !--- use the redistribute command. !--- To
prevent a routing loop, block the 192.168.1.0 network !-
-- from entering the OSPF process. It should only be
learned !--- through the RIP process. No two different
routing processes !--- exchange information unless you
implicitly use the !--- redistribute command. !--- The
192.168.1.x network is learned through OSPF from the !--
- 192.168.2.x side. However, since the admin distance is
changed, !--- it is not installed into the table !---
because RIP has an administrative distance of 120, !---
and all of the OSPF distances are 130.

 redistribute rip subnets route-map block192.168.1.0
!--- To enable the OSPF process for the interfaces that
are included !--- in the 192.168.x.x networks: network
192.168.0.0 0.0.255.255 area 0 !--- Since RIP's default
admin distance is 120 and OSPF's is 110, !--- make RIP a
preferable metric for communications !--- over the
"backup" network. !--- Change any learned OSPF routes
from neighbor 192.168.4.1 !--- to an admin distance of
130. distance 130 192.168.4.1 0.0.0.0 ! !--- To enable
RIP on the Ethernet 1/0 interface and set it to !--- use
version 2: router rip version 2 network 192.168.3.0 ! ip
classless ! ! access-list 1 deny 192.168.1.0 0.0.0.255
access-list 1 permit any route-map block192.168.1.0
permit 10 match ip address 1 ! line con 0 exec-timeout 0
0 line aux 0 line vty 0 4 ! end
```

Router 3640

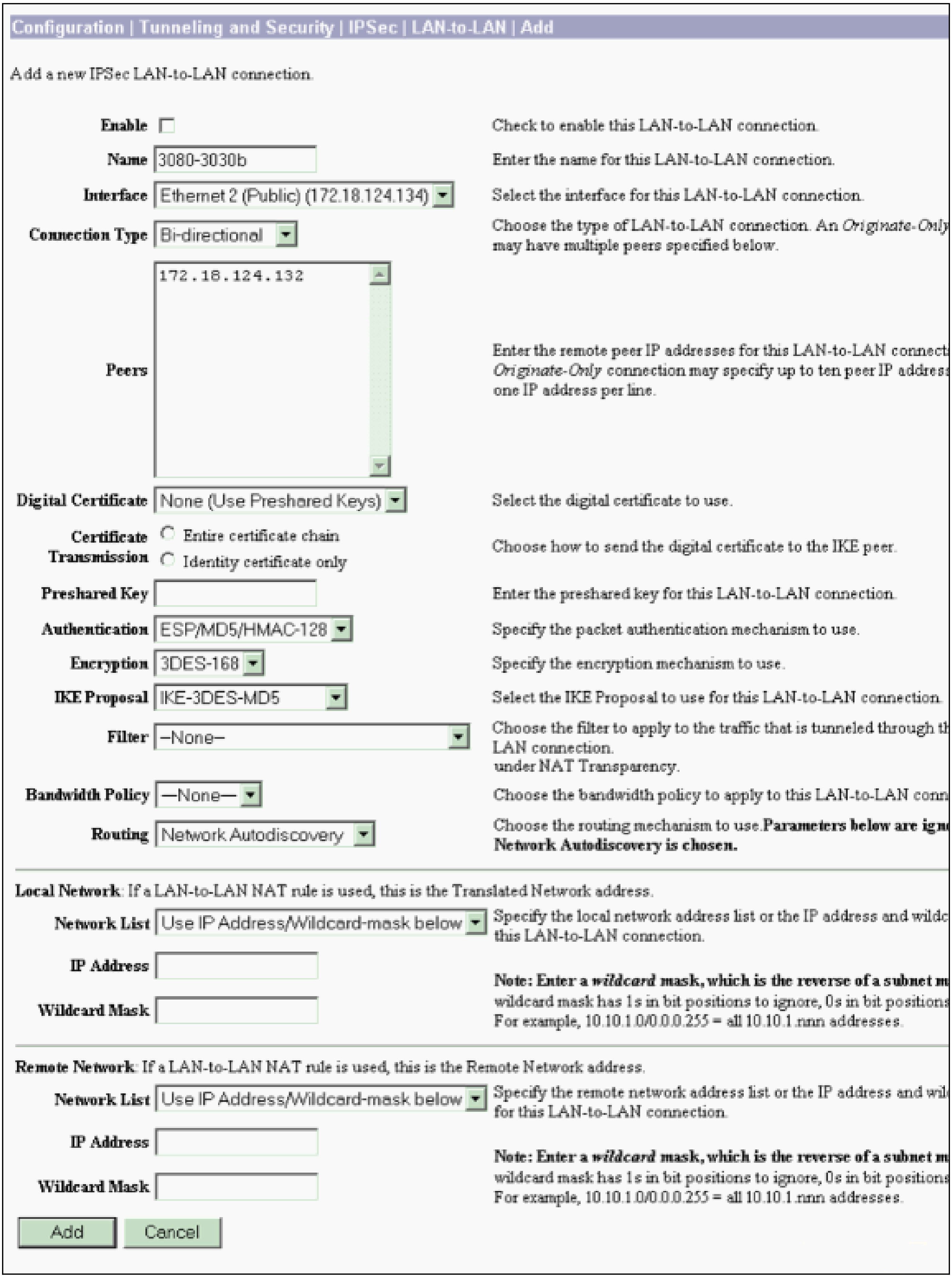
```
rtr-3640#write terminal
Building configuration...

Current configuration : 1129 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rtr-3640
!
ip subnet-zero
!
interface Ethernet0/0
 ip address 192.168.2.2 255.255.255.0
 half-duplex
!
interface Ethernet0/1
 ip address 192.168.4.1 255.255.255.0
 half-duplex
!
router ospf 1
 log-adjacency-changes
!--- Use this command to push RIP learned routes into
OSPF. !--- You need this when the VPN 3060a or the
connection drops and !--- the 192.168.3.0 route needs to
be injected into the OSPF backbone. redistribute rip
subnets !--- Place all 192.168.x.x networks into area 0.
network 192.168.0.0 0.0.255.255 area 0 !--- Since RIP's
default admin distance is 120 and OSPF's is 110, !---
make RIP a preferable metric for communications !---
over the "backup" network. !--- Change any learned OSPF
routes from neighbor 192.168.4.2 !--- to an admin
distance of 130. distance 130 192.168.4.2 0.0.0.0 ! !---
To enable RIP on the Ethernet 0/0 interface and set it
to !--- use version 2: router rip version 2 network
192.168.2.0 ! ip classless ! line con 0 exec-timeout 0 0
line aux 0 line vty 0 4 ! end
```

Configuración del concentrador de la VPN 3080

VPN de LAN a LAN 3080 a VPN 3030b

Seleccione **Configuration > Tunneling and Security > IPSec > IPSec LAN a LAN**. Dado que se utiliza Network Autodiscovery, no es necesario rellenar las listas de red locales y remotas.

Nota: Los concentradores VPN que ejecutan la versión de software 3.1 y anteriores tienen una casilla de verificación para la detección automática. La versión de software 3.5 (utilizada en la VPN 3080) utiliza un menú desplegable, como el que se muestra aquí.



Configuration | Tunneling and Security | IPSec | LAN-to-LAN | Add

Add a new IPSec LAN-to-LAN connection.

Enable	□	Check to enable this LAN-to-LAN connection.
Name	3080-3030b	Enter the name for this LAN-to-LAN connection.
Interface	Ethernet 2 (Public) (172.18.124.134)	Select the interface for this LAN-to-LAN connection.
Connection Type	Bi-directional	Choose the type of LAN-to-LAN connection. An *Originate-Only* may have multiple peers specified below.
Peers	172.18.124.132	Enter the remote peer IP addresses for this LAN-to-LAN connecti *Originate-Only* connection may specify up to ten peer IP address 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		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 th LAN connection. under NAT Transparency.
Bandwidth Policy	–None–	Choose the bandwidth policy to apply to this LAN-to-LAN conn
Routing	Network Autodiscovery	Choose the routing mechanism to use. **Parameters below are ign Network Autodiscovery is chosen.**

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

Network List	Use IP Address/Wildcard-mask below	Specify the local network address list or the IP address and wildc this LAN-to-LAN connection.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet m** wildcard mask has 1s in bit positions to ignore, 0s in bit positions For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask		

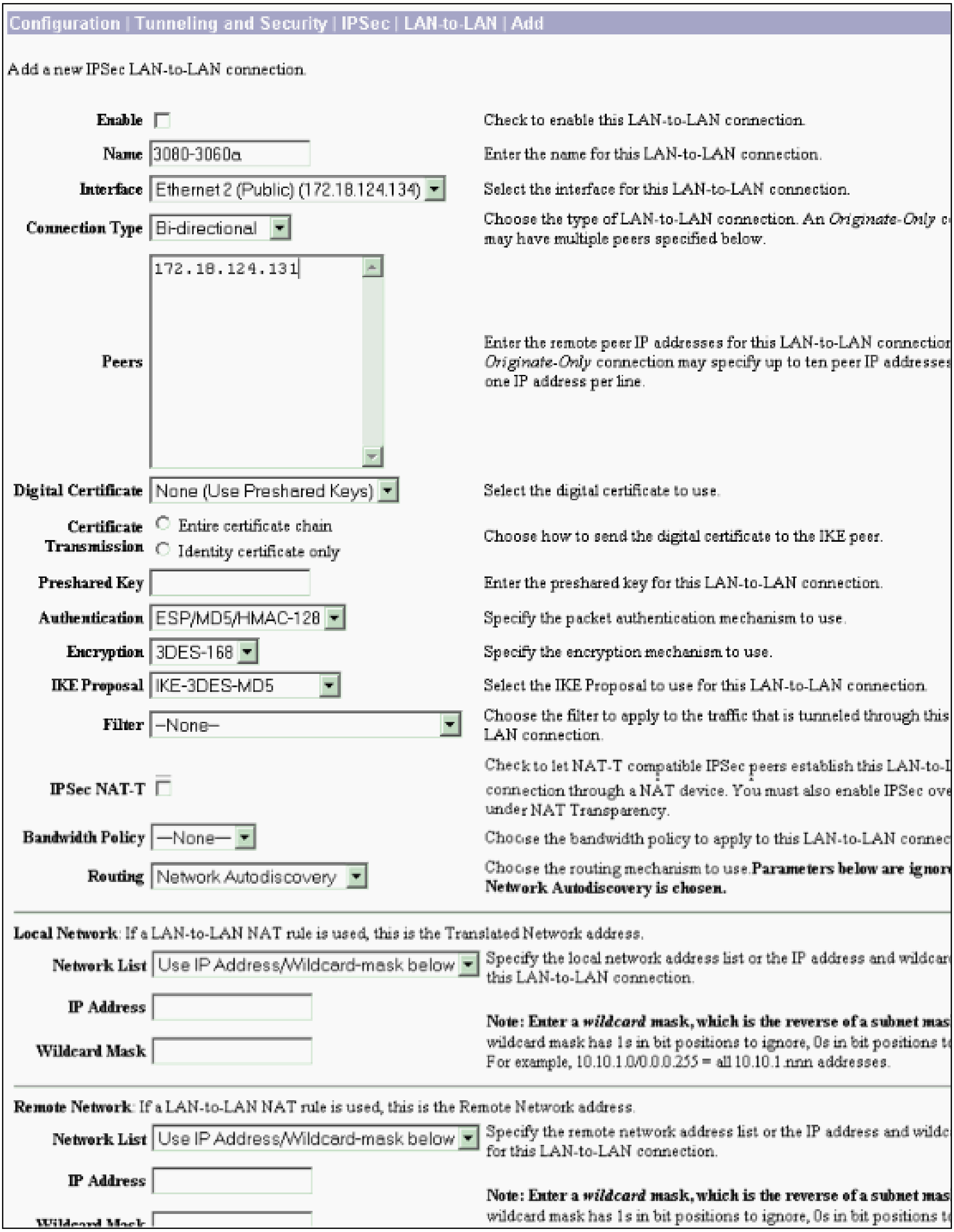
Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

Network List	Use IP Address/Wildcard-mask below	Specify the remote network address list or the IP address and wil for this LAN-to-LAN connection.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet m** wildcard mask has 1s in bit positions to ignore, 0s in bit positions For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask		

VPN de LAN a LAN 3080 a VPN 3060a

Seleccione **Configuration > Tunneling and Security > IPSec > IPSec LAN a LAN.** Dado que se utiliza Network Autodiscovery, no es necesario rellenar las listas de red locales y remotas.

Nota: Los concentradores VPN que ejecutan la versión de software 3.1 y anteriores tienen una casilla de verificación para la detección automática. La versión de software 3.5 (utilizada en la VPN 3080) utiliza un menú desplegable, como el que se muestra aquí.



Configuration | Tunneling and Security | IPSec | LAN-to-LAN | Add

Add a new IPSec LAN-to-LAN connection.

Enable	□	Check to enable this LAN-to-LAN connection.
Name	3080-3060a	Enter the name for this LAN-to-LAN connection.
Interface	Ethernet 2 (Public) (172.18.124.134) ▾	Select the interface for this LAN-to-LAN connection.
Connection Type	Bi-directional ▾	Choose the type of LAN-to-LAN connection. An *Originate-Only* c may have multiple peers specified below.
Peers	172.18.124.131	Enter the remote peer IP addresses for this LAN-to-LAN connection *Originate-Only* connection may specify up to ten peer IP addresses 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		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 connection.
IPSec NAT-T	□	Check to let NAT-T compatible IPSec peers establish this LAN-to-L connection through a NAT device. You must also enable IPSec ove under NAT Transparency.
Bandwidth Policy	--None-- ▾	Choose the bandwidth policy to apply to this LAN-to-LAN connec
Routing	Network Autodiscovery ▾	Choose the routing mechanism to use. **Parameters below are ignor Network Autodiscovery is chosen.**

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

Network List	Use IP Address/Wildcard-mask below ▾	Specify the local network address list or the IP address and wildcar this LAN-to-LAN connection.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet mas** wildcard mask has 1s in bit positions to ignore, 0s in bit positions t 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.

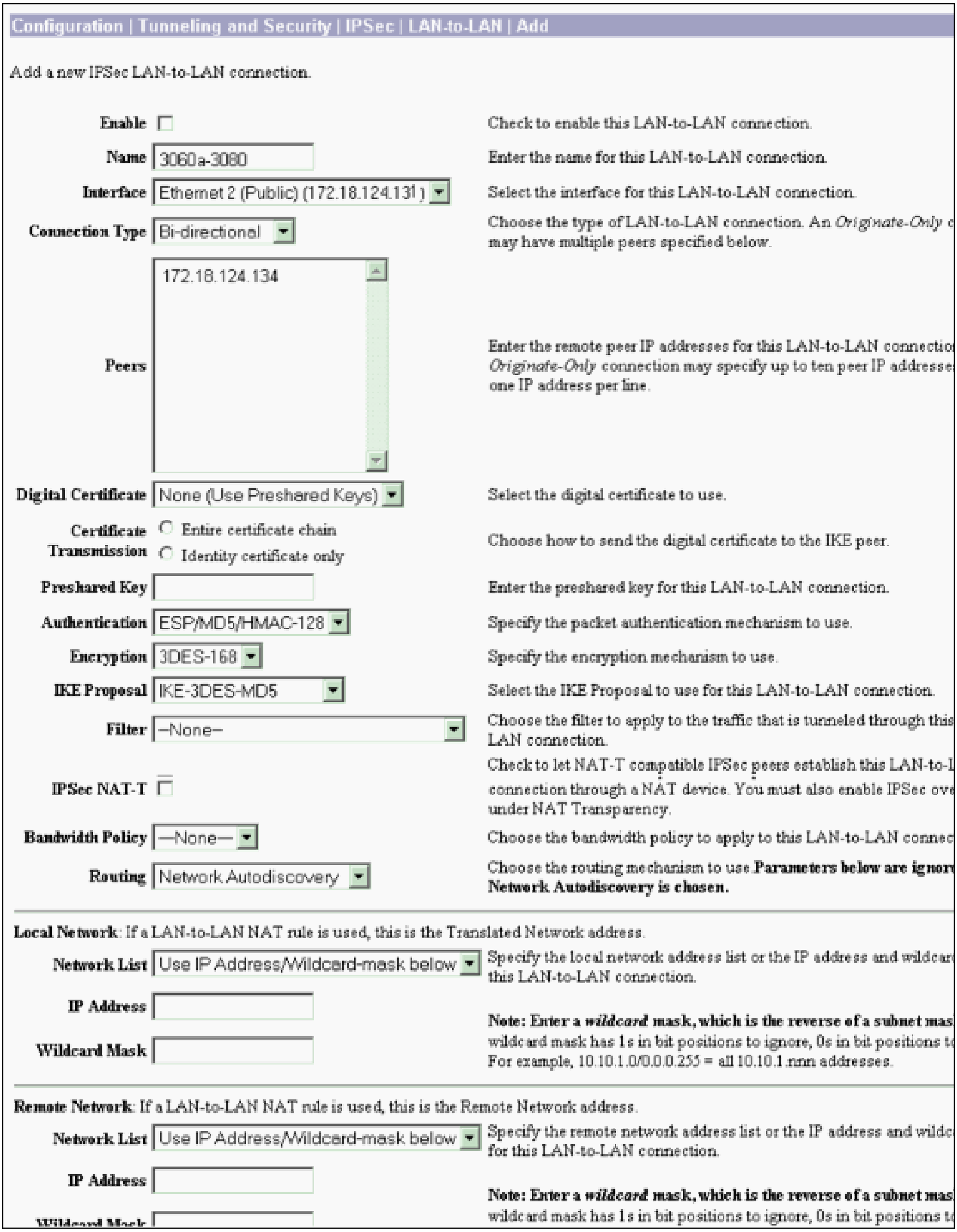
Network List	Use IP Address/Wildcard-mask below ▾	Specify the remote network address list or the IP address and wildc for this LAN-to-LAN connection.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet mas** wildcard mask has 1s in bit positions to ignore, 0s in bit positions t
Wildcard Mask		

Configuración del concentrador VPN 3060a

VPN de LAN a LAN 3060a a VPN 3080

Seleccione **Configuration > Tunneling and Security > IPSec > IPSec LAN a LAN**.

Nota: Hay una casilla de verificación en el VPN 3060 para Network Autodiscovery en lugar del menú desplegable como en la versión de software 3.5 y posteriores.



Configuration | Tunneling and Security | IPSec | LAN-to-LAN | Add

Add a new IPSec LAN-to-LAN connection.

Enable	□	Check to enable this LAN-to-LAN connection.
Name	3060a-3080	Enter the name for this LAN-to-LAN connection.
Interface	Ethernet 2 (Public) (172.18.124.131)	Select the interface for this LAN-to-LAN connection.
Connection Type	Bi-directional	Choose the type of LAN-to-LAN connection. An *Originate-Only* c may have multiple peers specified below.
Peers	172.18.124.134	Enter the remote peer IP addresses for this LAN-to-LAN connectio *Originate-Only* connection may specify up to ten peer IP addresse 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		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 connection.
IPSec NAT-T	□	Check to let NAT-T compatible IPSec peers establish this LAN-to-L connection through a NAT device. You must also enable IPSec ove under NAT Transparency.
Bandwidth Policy	--None--	Choose the bandwidth policy to apply to this LAN-to-LAN connec
Routing	Network Autodiscovery	Choose the routing mechanism to use. **Parameters below are ignor** **Network Autodiscovery is chosen.**

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

Network List	Use IP Address/Wildcard-mask below	Specify the local network address list or the IP address and wildcar this LAN-to-LAN connection.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet mas** wildcard mask has 1s in bit positions to ignore, 0s in bit positions t For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask		

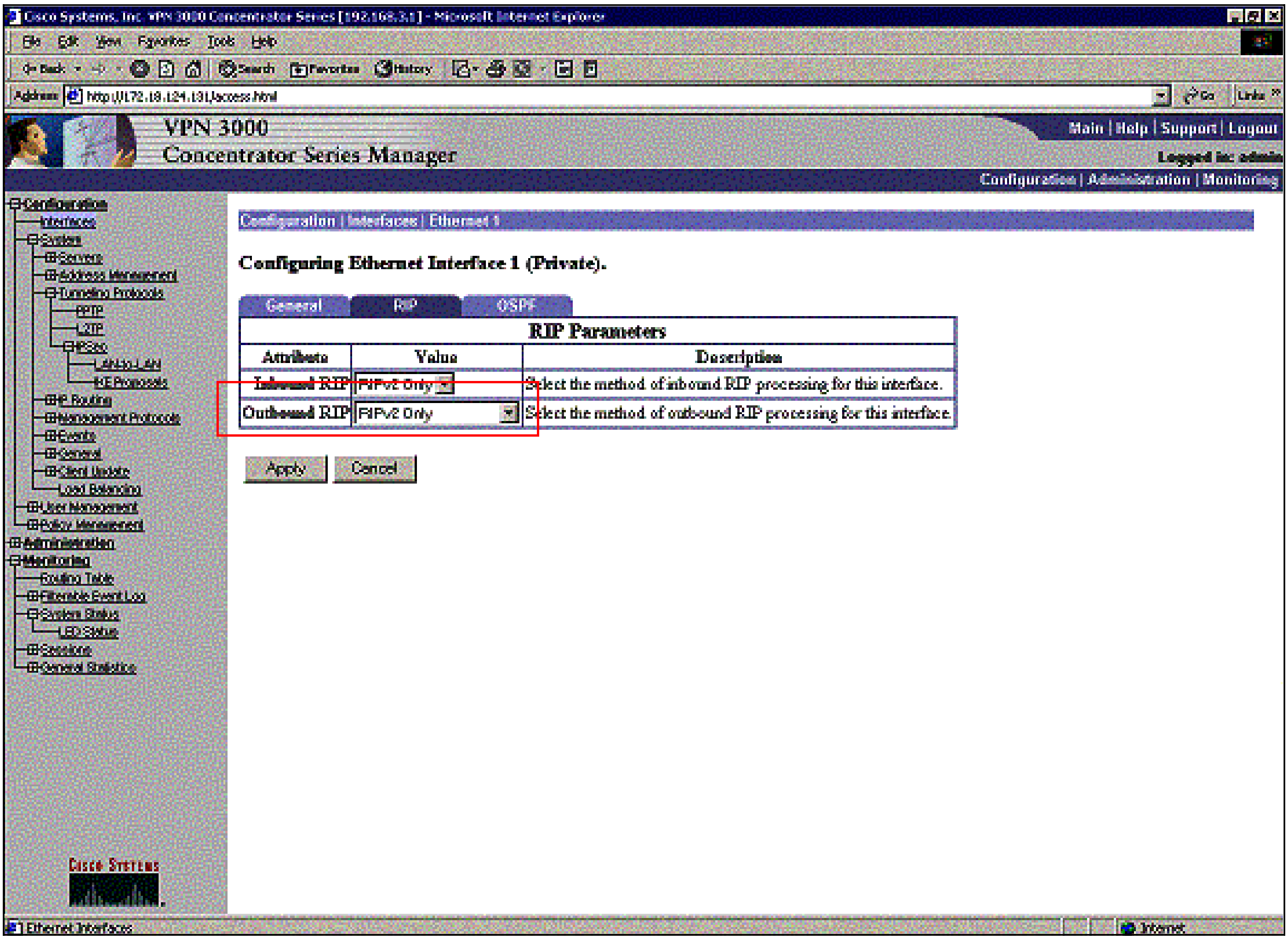
Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

Network List	Use IP Address/Wildcard-mask below	Specify the remote network address list or the IP address and wildc for this LAN-to-LAN connection.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet mas** wildcard mask has 1s in bit positions to ignore, 0s in bit positions t
Wildcard Mask		

Habilitación de RIP para Pasar las Rutas Aprendidas por Túnel al Router VPN 3620

Seleccione **Configuration > Interfaces > Private > RIP**. Cambie el menú desplegable a **Sólo RIPv2** y haga clic en **Aplicar**. A continuación, seleccione **Configuration > System > Tunneling Protocols > IPSec > LAN a LAN**.

Nota: El valor predeterminado es RIP saliente y está desactivado para la interfaz privada.



Configuration | Interfaces | Ethernet 1

Configuring Ethernet Interface 1 (Private).

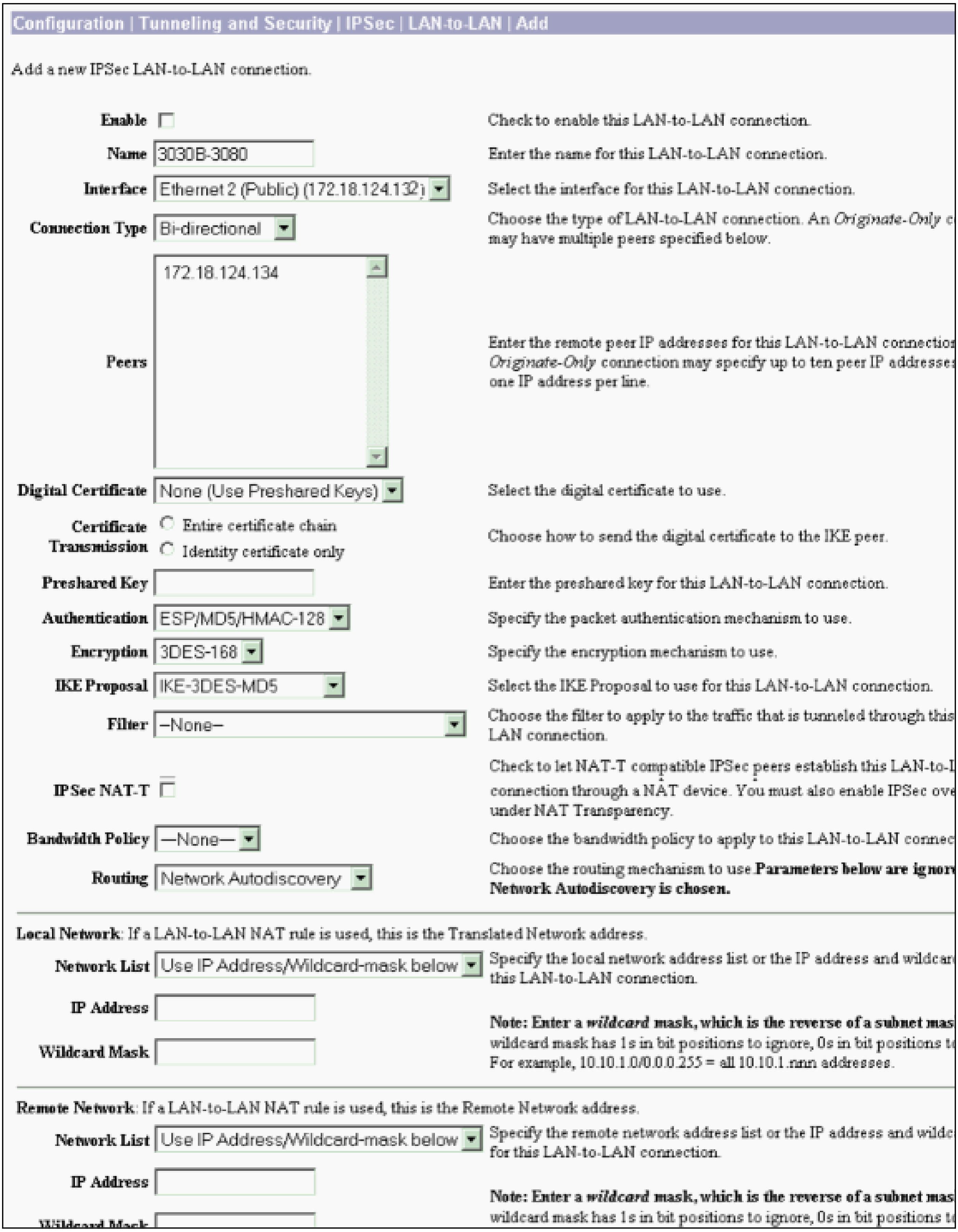
RIP Parameters

Attribute	Value	Description
Inbound RIP	RIPv2 Only	Select the method of inbound RIP processing for this interface.
Outbound RIP	RIPv2 Only	Select the method of outbound RIP processing for this interface.

Configuración del concentrador VPN 3030b

VPN de LAN a LAN 3030b a VPN 3080

Seleccione **Configuration > Tunneling and Security > IPSec > LAN-to-LAN**.



Configuration | Tunneling and Security | IPSec | LAN-to-LAN | Add

Add a new IPSec LAN-to-LAN connection.

Enable	□	Check to enable this LAN-to-LAN connection.
Name	3030B-3080	Enter the name for this LAN-to-LAN connection.
Interface	Ethernet 2 (Public) (172.18.124.132) ▾	Select the interface for this LAN-to-LAN connection.
Connection Type	Bi-directional ▾	Choose the type of LAN-to-LAN connection. An *Originate-Only* c may have multiple peers specified below.
Peers	172.18.124.134	Enter the remote peer IP addresses for this LAN-to-LAN connectio *Originate-Only* connection may specify up to ten peer IP addresse 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		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 connection.
IPSec NAT-T	□	Check to let NAT-T compatible IPSec peers establish this LAN-to-L connection through a NAT device. You must also enable IPSec ove under NAT Transparency.
Bandwidth Policy	–None– ▾	Choose the bandwidth policy to apply to this LAN-to-LAN connec
Routing	Network Autodiscovery ▾	Choose the routing mechanism to use. **Parameters below are ignor Network Autodiscovery is chosen.**

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

Network List	Use IP Address/Wildcard-mask below ▾	Specify the local network address list or the IP address and wildcar this LAN-to-LAN connection.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet mas** wildcard mask has 1s in bit positions to ignore, 0s in bit positions t 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	Use IP Address/Wildcard-mask below ▾	Specify the remote network address list or the IP address and wildc for this LAN-to-LAN connection.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet mas** wildcard mask has 1s in bit positions to ignore, 0s in bit positions t
Wildcard Mask		

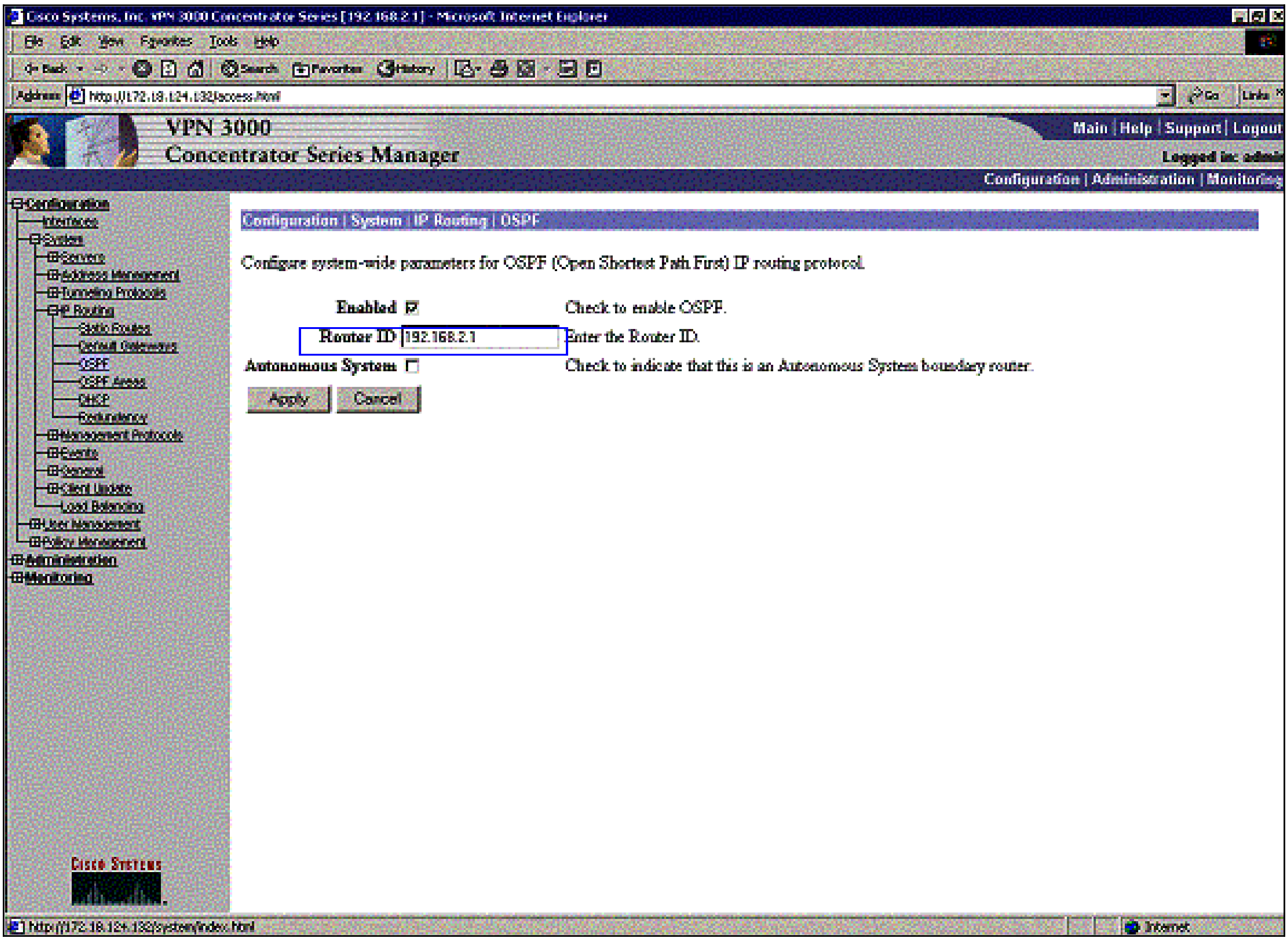
Habilitación de RIP para Pasar las Rutas Aprendidas por Túnel al Router VPN 3640

Siga los pasos enumerados anteriormente en este documento para el concentrador VPN 3060a.

Habilitación de OSPF para Pasar las Rutas Aprendidas de la Estructura Básica al Concentrador

VPN 3030b

Seleccione **Configuration > System > IP Routing > OSPF** e ingrese el ID del router.


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.2.1] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.18.124.132/access.html
Go Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
Servers
Address Management
Tunneling Protocols
IP Routing
Static Routes
Default Gateways
OSPF
OSPF Areas
DHCP
Redundancy
Management Protocols
Events
General
Client Update
Load Balancing
User Management
Policy Management
Administration
Monitoring
Cisco Systems
http://172.18.124.132/system/index.html
Internet

Configuration | System | IP Routing | OSPF

Configure system-wide parameters for OSPF (Open Shortest Path First) IP routing protocol.

Enabled ☑ Check to enable OSPF.

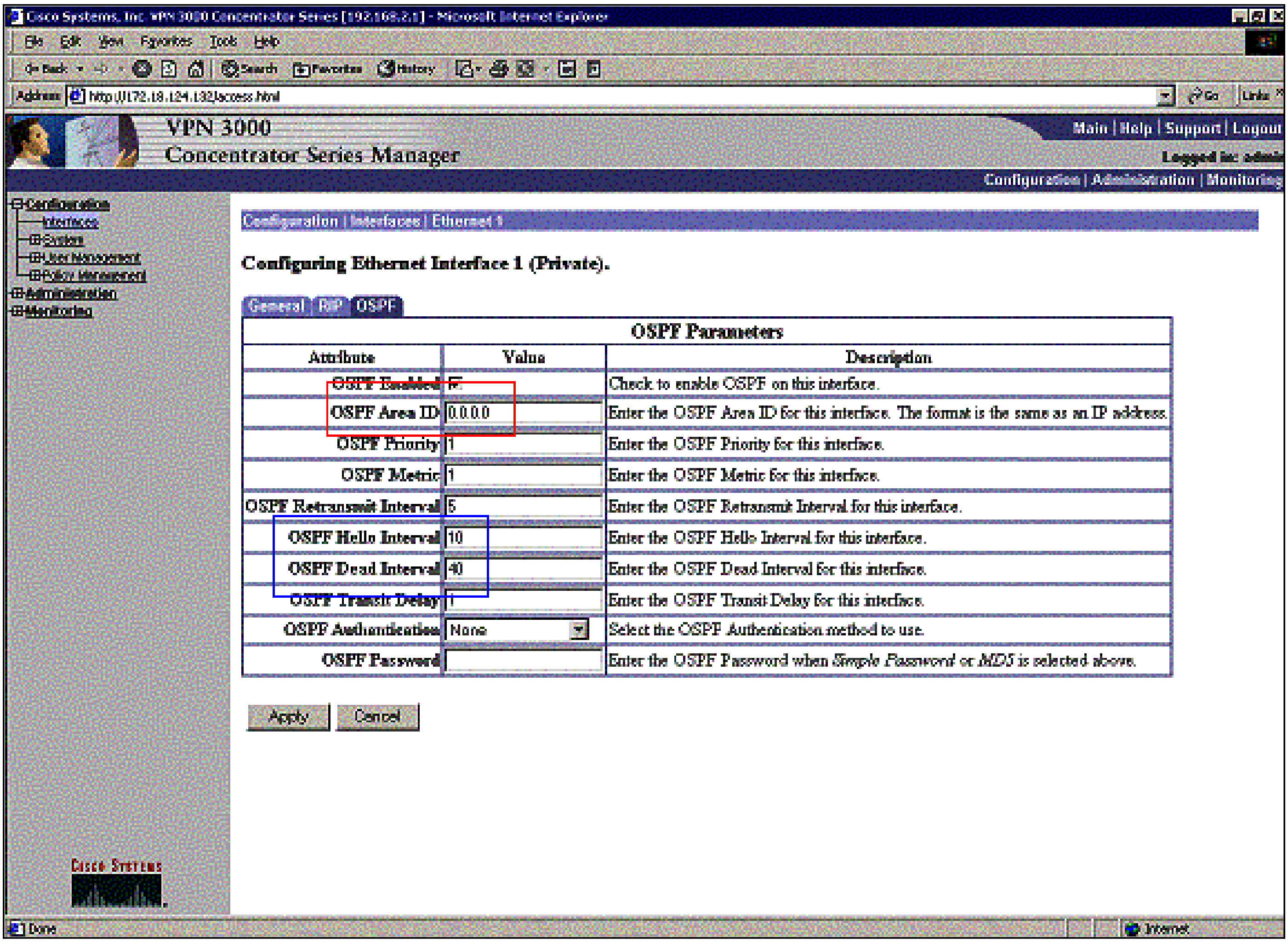
Router ID 192.168.2.1 Enter the Router ID.

Autonomous System □ Check to indicate that this is an Autonomous System boundary router.

Apply Cancel

```
rtr-3640#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface

192.168.4.2       1   FULL/DR         00:00:39    192.168.4.2     Ethernet0/1
!--- For troubleshooting purposes, it helps to make the router ID the !--- IP address of the
private interface. 192.168.2.1       1   FULL/BDR        00:00:36    192.168.2.1     Ethernet0/0
```

El ID de área debe coincidir con el ID del cable. Dado que el área en este ejemplo es 0, está representada por 0.0.0.0. Además, marque la casilla **Enable OSPF** y haga clic en **Apply**.


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.2.1] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.18.124.132/access.html
Go Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Administration
Monitoring
Configuration | Interfaces | Ethernet 1
General
RIP
OSPF
Apply
Cancel
Cisco Systems
Done
Internet

Configuring Ethernet Interface 1 (Private).

OSPF Parameters		
Attribute	Value	Description
OSPF Enabled	☑	Check to enable OSPF on this interface.
OSPF Area ID	0.0.0.0	Enter the OSPF Area ID for this interface. The format is the same as an IP address.
OSPF Priority	1	Enter the OSPF Priority for this interface.
OSPF Metric	1	Enter the OSPF Metric for this interface.
OSPF Retransmit Interval	5	Enter the OSPF Retransmit Interval for this interface.
OSPF Hello Interval	10	Enter the OSPF Hello Interval for this interface.
OSPF Dead Interval	40	Enter the OSPF Dead Interval for this interface.
OSPF Transit Delay	1	Enter the OSPF Transit Delay for this interface.
OSPF Authentication	None	Select the OSPF Authentication method to use.
OSPF Password		Enter the OSPF Password when *Simple Password* or *MD5* is selected above.

Asegúrese de que los temporizadores OSPF coinciden con los del router. Para verificar los temporizadores de los routers, utilice el comando **show ip ospf interface *<interface name>*** .

```
rtr-3640#show ip ospf interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  Internet Address 192.168.2.2/24, Area 0
  Process ID 1, Router ID 192.168.4.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.4.1, Interface address 192.168.2.2
  Backup Designated router (ID) 192.168.2.1, Interface address 192.168.2.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.2.1  (Backup Designated Router)
Suppress hello for 0 neighbor(s)
```

Para obtener más información sobre OSPF, consulte RFC 1247 .

Verificación

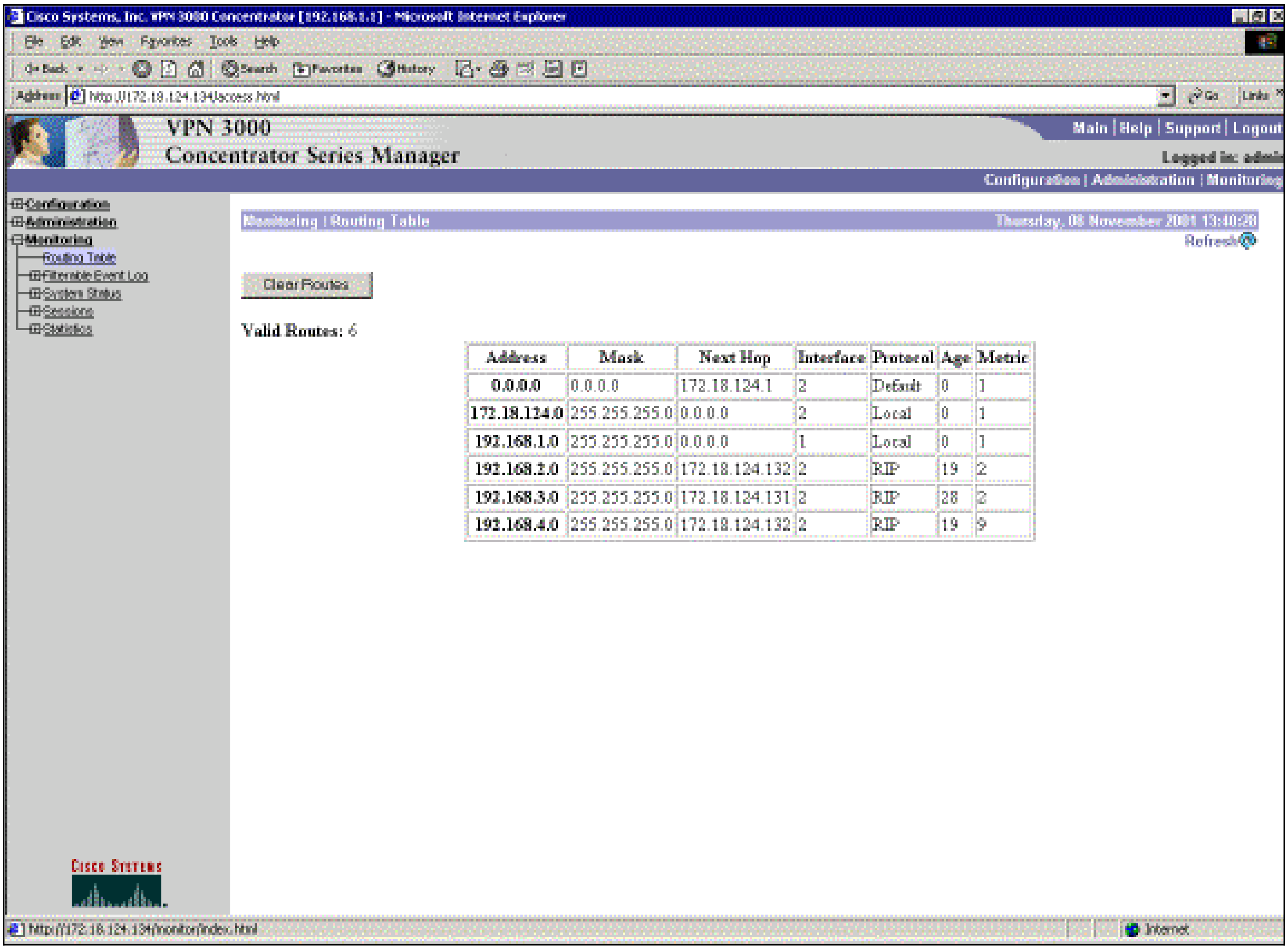
En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

Este resultado del comando muestra tablas de ruteo precisas.

```
rtr-3620#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

Gateway of last resort is not set

     172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.3.1, 00:00:11, Ethernet1/0
C    192.168.4.0/24 is directly connected, Ethernet1/1
!--- The 192.168.1.x network is learned from the !--- VPN 3060a Concentrator. R
192.168.1.0/24 [120/2] via 192.168.3.1, 00:00:11, Ethernet1/0
!--- The 192.168.3.x network traverses the 192.168.4.x network !--- to get to the 192.168.2.x
network. O    192.168.2.0/24 [130/20] via 192.168.4.1, 00:01:07, Ethernet1/1
C    192.168.3.0/24 is directly connected, Ethernet1/0

rtr-3640#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

Gateway of last resort is not set

     172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.2.1, 00:00:23, Ethernet0/0
C    192.168.4.0/24 is directly connected, Ethernet0/1
!--- The 192.168.1.x network is learned from the !--- VPN 3030b Concentrator. R
192.168.1.0/24 [120/2] via 192.168.2.1, 00:00:23, Ethernet0/0
C    192.168.2.0/24 is directly connected, Ethernet0/0
!--- The 192.168.2.x network traverses the 192.168.4.x network !--- to get to the 192.168.3.x
network. !--- This is an example of perfect symmetrical routing. O    192.168.3.0/24 [130/20]
via 192.168.4.2, 00:00:58, Ethernet0/1
```

Esta es la tabla de ruteo del concentrador VPN 3080 en circunstancias normales.


Cisco Systems, Inc. VPN 3000 Concentrator [192.168.1.1] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.18.124.134/access.html
Go Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Monitoring
Routing Table
Filterable Event Log
System Status
Sessions
Statistics
Cisco Systems
http://172.18.124.134/monitor/index.html
Internet

Monitoring | Routing Table

Thursday, 08 November 2001 13:40:20

Refresh

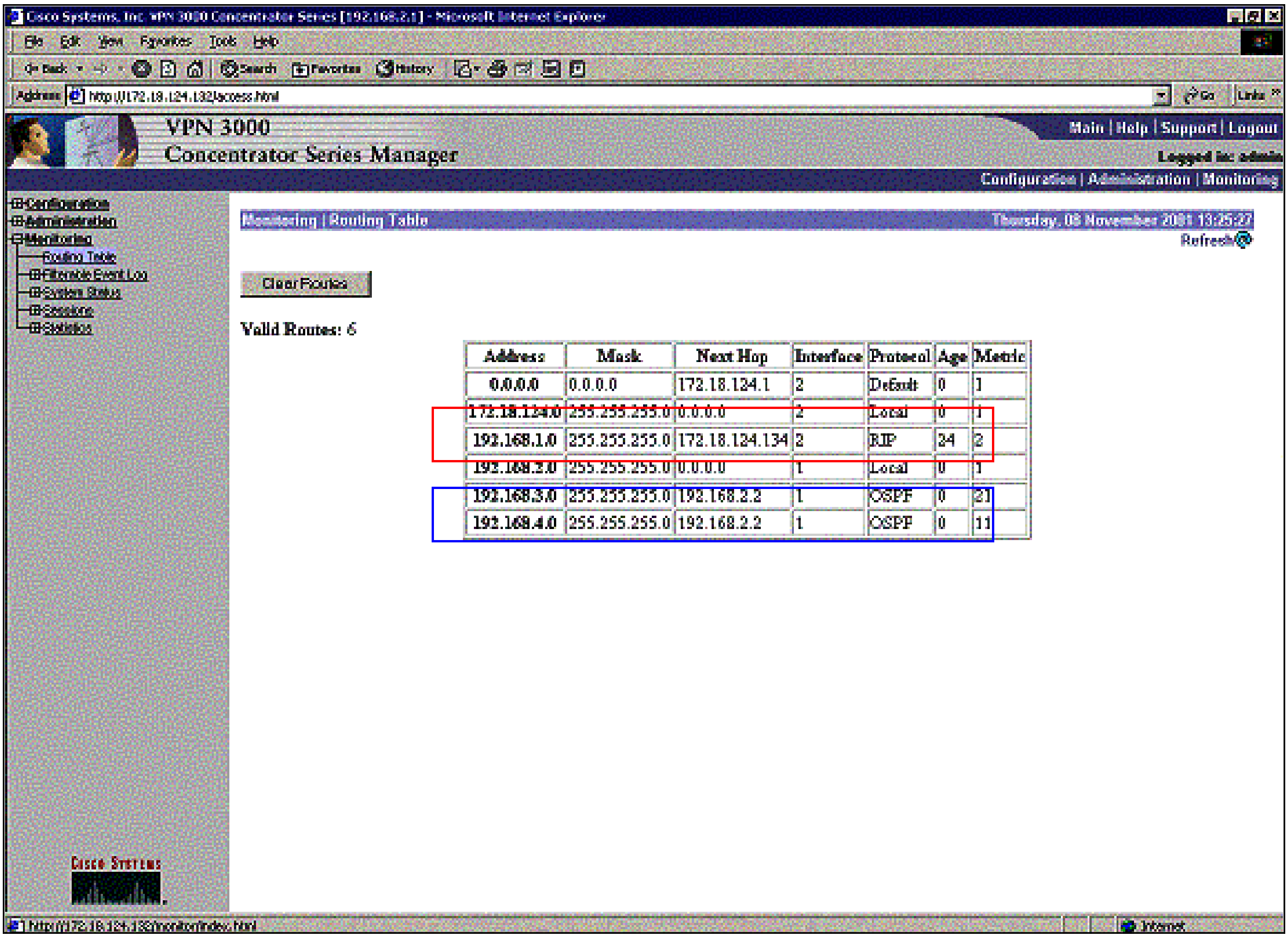
Clear Routes

Valid Routes: 6

Address	Mask	Next Hop	Interface	Protocol	Age	Metric
0.0.0.0	0.0.0.0	172.18.124.1	2	Default	0	1
172.18.124.0	255.255.255.0	0.0.0.0	2	Local	0	1
192.168.1.0	255.255.255.0	0.0.0.0	1	Local	0	1
192.168.2.0	255.255.255.0	172.18.124.132	2	RIP	19	2
192.168.3.0	255.255.255.0	172.18.124.131	2	RIP	28	2
192.168.4.0	255.255.255.0	172.18.124.132	2	RIP	19	9

Las redes 192.168.2.x y 192.168.3.x se aprenden a través de los túneles VPN 172.18.124.132 y 172.18.124.131, respectivamente. La red 192.168.4.x se aprende a través del túnel 172.18.124.132 porque los anuncios OSPF del router se colocan en la tabla de ruteo del concentrador VPN 3030b. A continuación, la tabla de ruteo anuncia la red a los pares VPN remotos.

Esta es la tabla de ruteo del concentrador VPN 3030b en circunstancias normales.



Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.2.1] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.18.124.132/access.html
Go Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Monitoring
Routing Table
Filterable Event Log
System Status
Sessions
Statistics
Cisco Systems
http://172.18.124.132/monitorindex.html
Internet

Monitoring | Routing Table

Thursday, 08 November 2001 13:25:27

Refresh

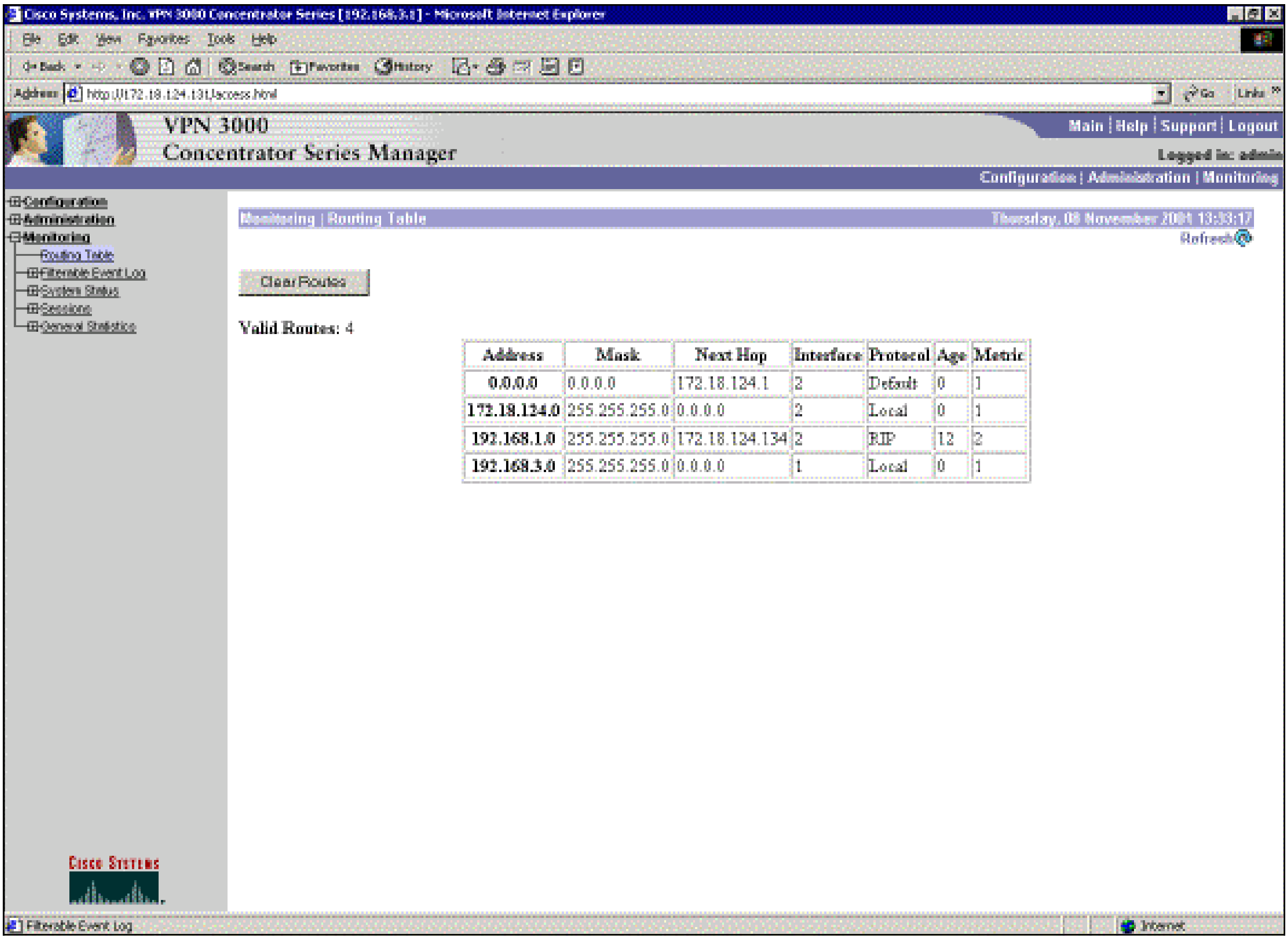
Clear Routes

Valid Routes: 6

Address	Mask	Next Hop	Interface	Protocol	Age	Metric
0.0.0.0	0.0.0.0	172.18.124.1	2	Default	0	1
172.18.124.0	255.255.255.0	0.0.0.0	2	Local	0	1
192.168.1.0	255.255.255.0	172.18.124.134	2	RIP	24	2
192.168.2.0	255.255.255.0	0.0.0.0	1	Local	0	1
192.168.3.0	255.255.255.0	192.168.2.2	1	OSPF	0	21
192.168.4.0	255.255.255.0	192.168.2.2	1	OSPF	0	11

El cuadro rojo destaca que la red 192.168.1.x se aprende del túnel VPN. El cuadro azul destaca que las redes 192.168.3.x y 192.168.4.x se aprenden a través del proceso OSPF de núcleo.

Esta es la tabla de ruteo del concentrador VPN 3060a en circunstancias normales.



Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.3.1] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.18.124.131/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Monitoring
Routing Table
Filterable Event Log
System Status
Sessions
General Statistics
Monitoring | Routing Table
Thursday, 08 November 2001 13:33:17
Refresh
Clear Routes
Filterable Event Log
Internet

Valid Routes: 4

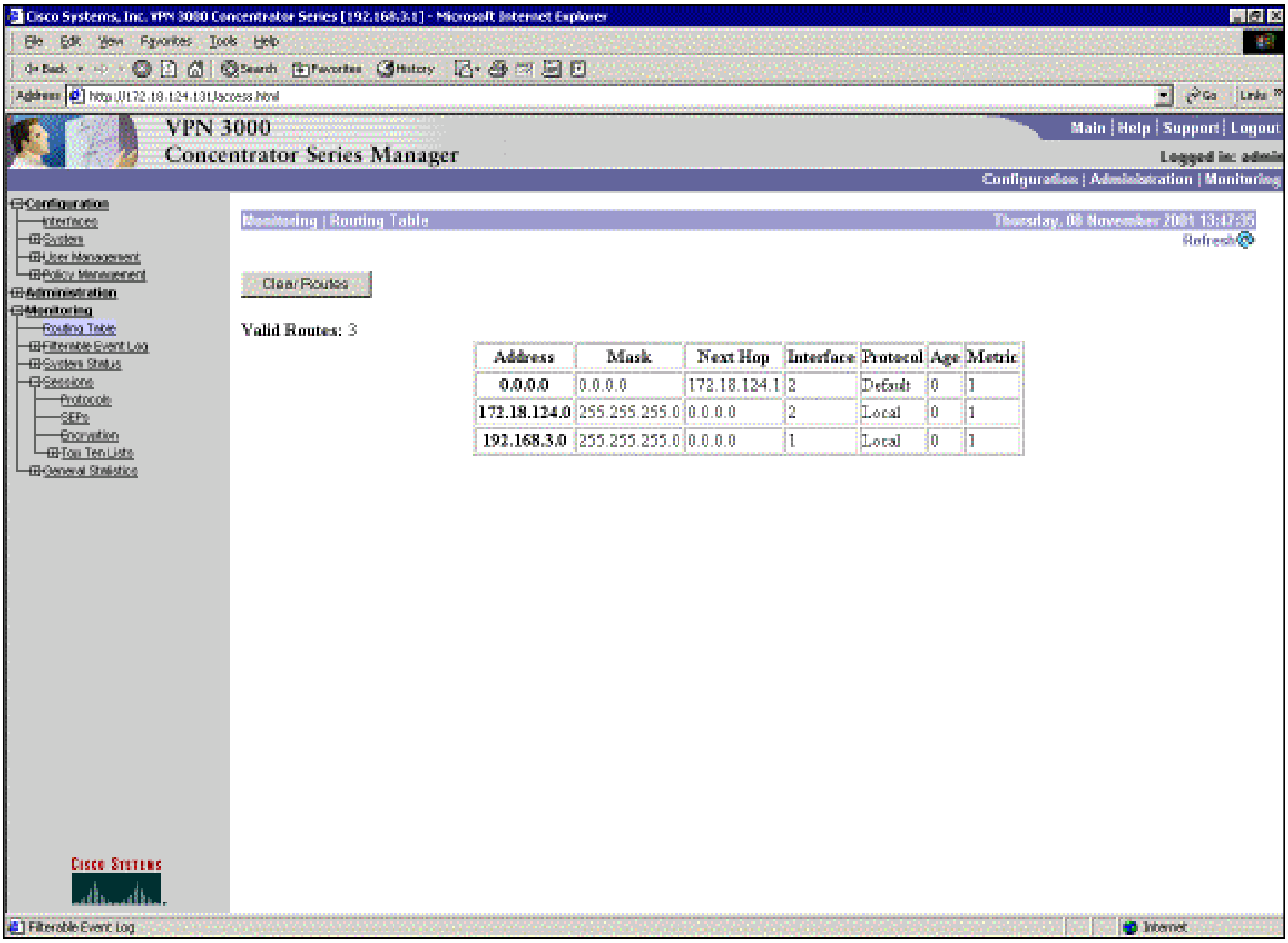
Address	Mask	Next Hop	Interface	Protocol	Age	Metric
0.0.0.0	0.0.0.0	172.18.124.1	2	Default	0	1
172.18.124.0	255.255.255.0	0.0.0.0	2	Local	0	1
192.168.1.0	255.255.255.0	172.18.124.134	2	RIP	12	2
192.168.3.0	255.255.255.0	0.0.0.0	1	Local	0	1

La red 192.168.1.x es la única red aquí y se puede alcanzar a través del túnel VPN. No hay red 192.168.2.0 ya que ningún proceso (como RIP) pasa a lo largo de esa ruta. No se pierde nada mientras los PC de la red 192.168.3.x no apunten su gateway predeterminado al concentrador VPN. Siempre puede agregar una ruta estática si así lo desea. Sin embargo, para este ejemplo, el propio VPN Concentrator no necesita alcanzar la red 192.168.2.0.

Troubleshoot

Falla simulada

Este es un error simulado en la configuración. Si quita el filtro a la interfaz pública, el túnel VPN se descarta. Esto hace que la ruta para el 192.168.1.0 aprendida a través del túnel también caiga. El proceso RIP tarda aproximadamente tres minutos en purgar la ruta. Por lo tanto, puede tener una interrupción de tres minutos hasta que la ruta se agote.


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.3.1] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.18.124.131/access.html
Go Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Administration
Monitoring
Routing Table
Filterable Event Log
System Status
Sessions
Protocols
SEPs
Encryption
Top Ten Lists
General Statistics
Cisco Systems
Filterable Event Log
Internet

Monitoring | Routing Table   Thursday, 08 November 2001 13:47:35

Refresh

Clear Routes

Valid Routes: 3

Address	Mask	Next Hop	Interface	Protocol	Age	Metric
0.0.0.0	0.0.0.0	172.18.124.1	2	Default	0	1
172.18.124.0	255.255.255.0	0.0.0.0	2	Local	0	1
192.168.3.0	255.255.255.0	0.0.0.0	1	Local	0	1

Una vez que caduca la ruta RIP, la nueva tabla de ruteo en los routers aparece de la misma manera:

```
rtr-3620#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.3.1, 00:00:05, Ethernet1/0
C    192.168.4.0/24 is directly connected, Ethernet1/1
!--- Now the 192.168.1.0 route is learned properly !--- through the OSPF backbone. O E2
192.168.1.0/24 [130/20] via 192.168.4.1, 00:00:05, Ethernet1/1
O    192.168.2.0/24 [130/20] via 192.168.4.1, 19:55:48, Ethernet1/1
C    192.168.3.0/24 is directly connected, Ethernet1/0
```

Qué Puede Salir Mal?

Si olvida agregar el cambio de distancia de administración a 130, es posible que vea este resultado. Observe que ambos túneles VPN están activos.

Concentrador VPN 3080

Nota: Esta es la versión de interfaz de usuario (GUI) no gráfica de la tabla de routing.

```
Monitor -> 1

Routing Table
-------------

Number of Routes: 6

   IP Address         Mask          Next Hop    Intf Protocol Age Metric
------------------------------------------------------------------------
0.0.0.0         0.0.0.0         172.18.124.1       2 Default    0      1
172.18.124.0    255.255.255.0   0.0.0.0            2 Local      0      1
192.168.1.0     255.255.255.0   0.0.0.0            1 Local      0      1
192.168.2.0     255.255.255.0   172.18.124.132     2 RIP       10      2
192.168.3.0     255.255.255.0   172.18.124.131     2 RIP        2      2
192.168.4.0     255.255.255.0   172.18.124.132     2 RIP       10      9
```

Para llegar a la red 192.168.3.0, la ruta debe atravesar 172.18.124.131. Sin embargo, la tabla de ruteo en RTR-3620 muestra:

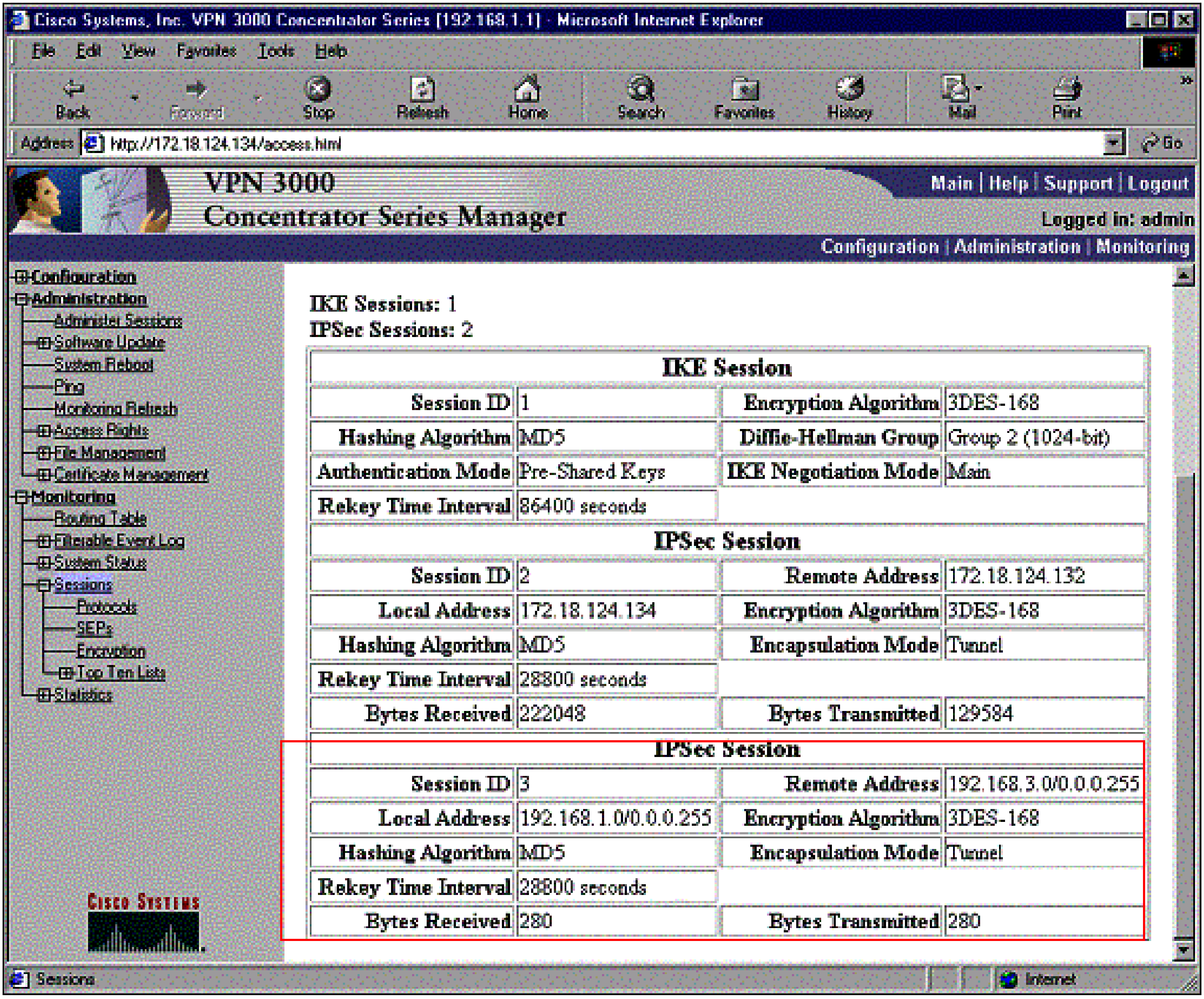
```
rtr-3620#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.18.0.0/24 is subnetted, 1 subnets
O E2    172.18.124.0 [110/20] via 192.168.4.1, 00:03:16, Ethernet1/1
C    192.168.4.0/24 is directly connected, Ethernet1/1
!--- This is an example of asymmetric routing. O E2 192.168.1.0/24 [110/20] via 192.168.4.1,
00:03:16, Ethernet1/1
O    192.168.2.0/24 [110/20] via 192.168.4.1, 00:03:16, Ethernet1/1
C    192.168.3.0/24 is directly connected, Ethernet1/0
```

Para volver a la red 192.168.1.0, la ruta debe atravesar la red de estructura básica 192.168.4.x.

El tráfico sigue funcionando desde que la detección automática genera la información de asociación de seguridad (SA) adecuada en el concentrador VPN 3030b. Por ejemplo:

```
Routing -> 1

Routing Table

-------------
Number of Routes: 6
   IP Address         Mask          Next Hop    Intf Protocol Age Metric

------------------------------------------------------------------------
0.0.0.0         0.0.0.0         172.18.124.1       2 Default    0      1
172.18.124.0    255.255.255.0   0.0.0.0            2 Local      0      1
```

```
192.168.1.0      255.255.255.0    0.0.0.0            1 Local      0       1
192.168.2.0      255.255.255.0    172.18.124.132     2 RIP       28       2
192.168.3.0      255.255.255.0    172.18.124.131     2 RIP       20       2
192.168.4.0      255.255.255.0    172.18.124.132     2 RIP       28       9
```


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://172.18.124.134/access.html
Go
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Administer Sessions
Software Update
System Reboot
Ping
Monitoring Refresh
Access Rights
File Management
Certificate Management
Monitoring
Routing Table
Filterable Event Log
System Status
Sessions
Protocols
SEPs
Encryption
Top Ten Lists
Statistics
Cisco Systems
Sessions
Internet

IKE Sessions: 1
IPSec Sessions: 2

IKE Session			
Session ID	1	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 2 (1024-bit)
Authentication Mode	Pre-Shared Keys	IKE Negotiation Mode	Main
Rekey Time Interval	86400 seconds		

IPSec Session			
Session ID	2	Remote Address	172.18.124.132
Local Address	172.18.124.134	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Encapsulation Mode	Tunnel
Rekey Time Interval	28800 seconds		
Bytes Received	222048	Bytes Transmitted	129584

IPSec Session			
Session ID	3	Remote Address	192.168.3.0/0.0.0.255
Local Address	192.168.1.0/0.0.0.255	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Encapsulation Mode	Tunnel
Rekey Time Interval	28800 seconds		
Bytes Received	280	Bytes Transmitted	280

Aunque la tabla de ruteo dice que el par debe ser 172.18.124.131, el SA real (flujo de tráfico) es a través del VPN 3030b Concentrator a 172.18.124.132. La tabla SA tiene prioridad sobre la tabla de ruta. Sólo un examen minucioso de la tabla de rutas y la tabla SA en el concentrador VPN 3060a muestra que el tráfico no fluye en la dirección correcta.

Información Relacionada

- Página de soporte del concentrador de la serie Cisco VPN 3000
- Página de soporte de IPSec
- Soporte Técnico - Cisco Systems