

Cómo Alimentar rutas dinámicas mediante la inyección de ruta inversa.

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración del concentrador VPN 3000 mediante RIPv2](#)

[Cliente Reverse Route Injection](#)

[Extensión de red RRI \(Cliente VPN 3002 en NEM únicamente\)](#)

[Detección automática de red del LAN a LAN](#)

[Red RRI del LAN a LAN](#)

[Rutas retenidas](#)

[Utilice el OSPF con el RRI](#)

[Verificación](#)

[Verifique/RIPv2 de la prueba](#)

[Verifique/detección automática de red del LAN a LAN de la prueba](#)

[Verifique/la red RRI del LAN a LAN de la prueba](#)

[Verifique/las rutas del asentamiento de la prueba](#)

[Verifique/la prueba OSPF con el RRI](#)

[Verifique la información de la tabla de ruteo en el concentrador VPN](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

El Reverse Route Injection (RRI) se utiliza para poblar la tabla de ruteo de un protocolo corriente o de Routing Information Protocol (RIP) del Open Shortest Path First (OSPF) del router interno para los clientes VPN remotos o las sesiones LAN a LAN. RRI se introdujo en las versiones 3.5 y posteriores del concentrador series VPN 3000 (3005 – 3080). RRI no se incluye en el VPN 3002 Hardware Client puesto que se trata como un Cliente VPN y no un Concentrador VPN. Solo los Concentradores VPN pueden anunciar rutas RRI. El VPN 3002 Hardware Client debe ejecutar las versiones 3.5 o posteriores del código para poder volver a inyectar Rutas de Extensión de Red al Concentrador VPN principal.

prerrequisitos

Requisitos

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 VPN 3000 Concentrator con la versión de software 3.5
- Cisco 2514 Router que funciona con el Software Release 12.2.3 de Cisco IOS®
- Cliente de hardware de Cisco VPN 3002 con versión de software 3.5 o posterior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las [Convenciones de Consejos Técnicos de Cisco](#).

Antecedentes

Hay cuatro maneras de utilizar la función RRI:

- Los clientes del software VPN inyectan sus direcciones de IP asignadas como rutas de hosts.
- Un cliente de hardware VPN 3002 se conecta usando el Modo de extensión de red (NEM) e inyecta su dirección de red protegida. (Observe que a un cliente del hardware VPN 3002 en modo de Traducción de dirección de puerto (PAT) se lo trata como a un cliente VPN.)
- Las definiciones de red remota del LAN a LAN son las rutas inyectadas. (Puede ser una única red o lista de red).
- RRI otorga una ruta detenida para las agrupaciones de VPN Client.

Cuando se utiliza el RRI, el RIP o el OSPF se puede utilizar para hacer publicidad de estas rutas. Con las versiones anteriores del código del concentrador VPN, las sesiones LAN a LAN pueden utilizar la detección automática de red. Sin embargo, este proceso puede utilizar solamente el RIP como su Routing Protocol de la publicidad.

Nota: El RRI no se puede utilizar con el Virtual Router Redundancy Protocol (VRRP) puesto que el ambo el master y servidores de backup hacen publicidad de las rutas RRI. Esto puede causar los problemas de ruteo. Los clientes registrados pueden conseguir más detalles en este problema en el Id. de bug Cisco [CSCdw30156](#) ([clientes registrados solamente](#)).

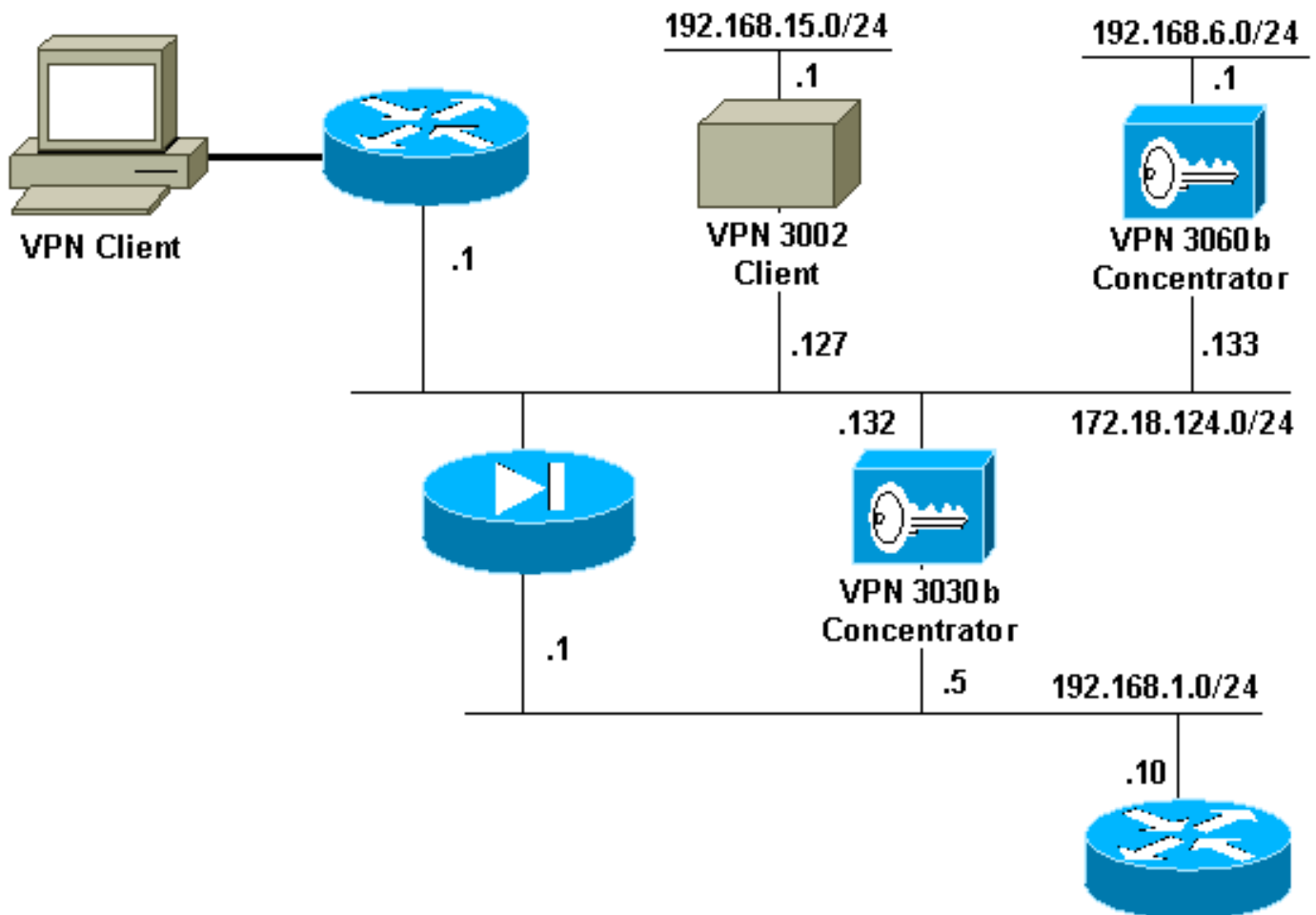
Configurar

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

Nota: Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

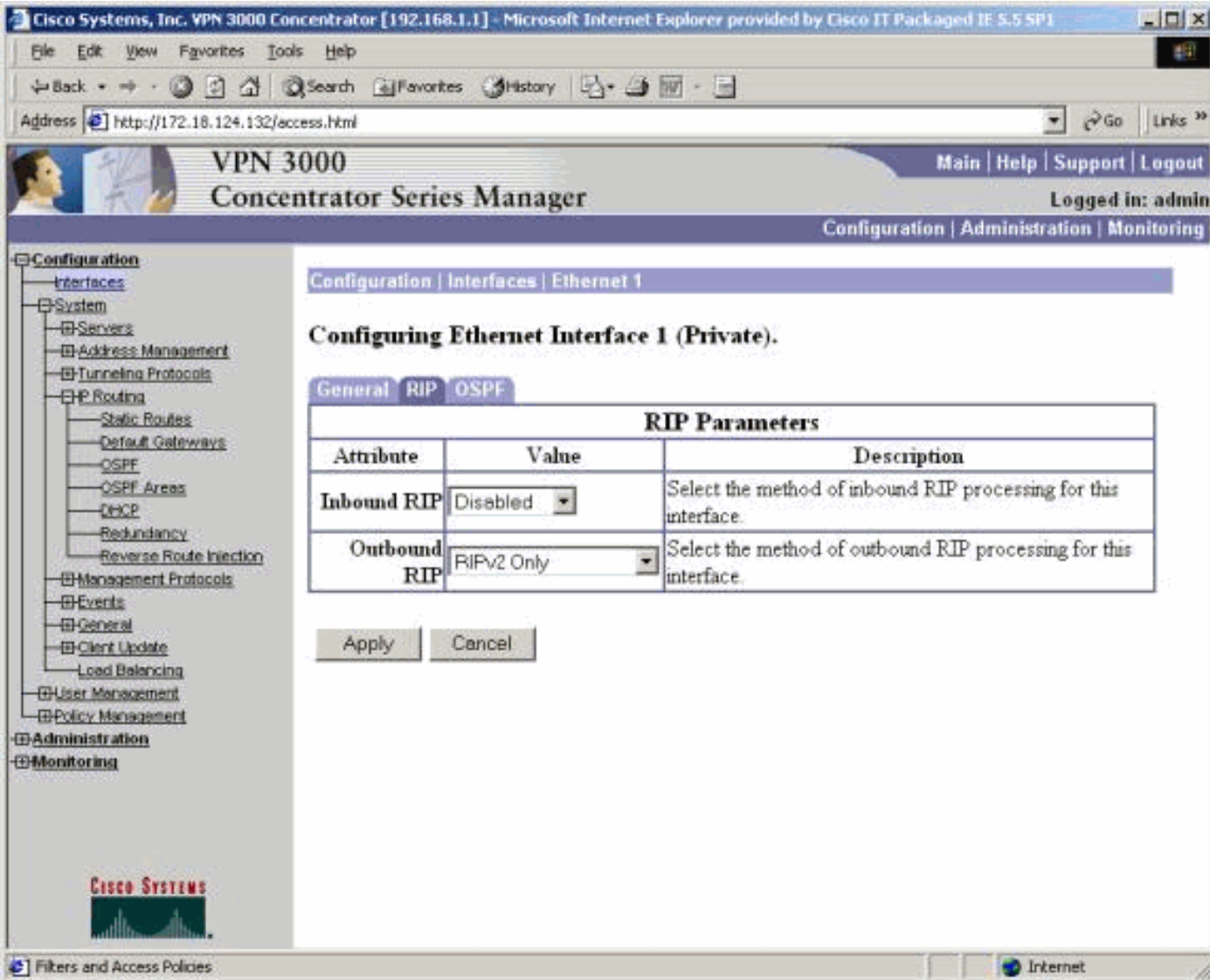
Configuración del router

```
2514-b#show version Cisco Internetwork Operating System
Software IOS (tm) 2500 Software (C2500-IK80S-L), Version
12.2(3), RELEASE SOFTWARE (fc1) Copyright (c) 1986-2001
by cisco Systems, Inc. Compiled Wed 18-Jul-01 20:14 by
pwade Image text-base: 0x0306B450, data-base: 0x00001000
2514-b#write terminal Building configuration... Current
configuration : 561 bytes ! version 12.2 service
timestamps debug uptime service timestamps log uptime no
service password-encryption ! hostname 2514-b ! ip
subnet-zero ! ip ssh time-out 120 ip ssh authentication-
retries 3 ! interface Ethernet0 ip address 192.168.1.10
255.255.255.0 ! interface Ethernet1 no ip address
```

```
shutdown ! router rip version 2 network 192.168.1.0 ! ip
classless ip route 0.0.0.0 0.0.0.0 192.168.1.1 ip http
server ! line con 0 line aux 0 line vty 0 4 ! end
```

[Configuración del concentrador VPN 3000 mediante RIPv2](#)

Para hacer publicidad de las rutas aprendido RRI, usted debe tener RIP saliente (en un mínimo) habilitado en la interfaz privada del concentrador VPN local (representado por VPN 3030b en el [diagrama de la red](#)). La detección automática de red requiere el RIP entrante y saliente que se habilitará. El cliente RRI puede ser utilizado en todos los clientes VPN que conecten con el concentrador VPN (tal como VPN, acode 2 Tunnel Protocol (L2TP), el Point-to-Point Tunneling Protocol (PPTP), y así sucesivamente).



The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The browser address bar shows `http://172.18.124.132/access.html`. The page title is "VPN 3000 Concentrator Series Manager" and the user is logged in as "admin". The navigation menu includes Configuration, Administration, and Monitoring. The left sidebar shows a tree view with "IP Routing" expanded to "RIP". The main content area is titled "Configuring Ethernet Interface 1 (Private)" and has tabs for "General", "RIP", and "OSPF". The "RIP Parameters" table is as follows:

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

Buttons for "Apply" and "Cancel" are visible below the table.

[Cliente Reverse Route Injection](#)

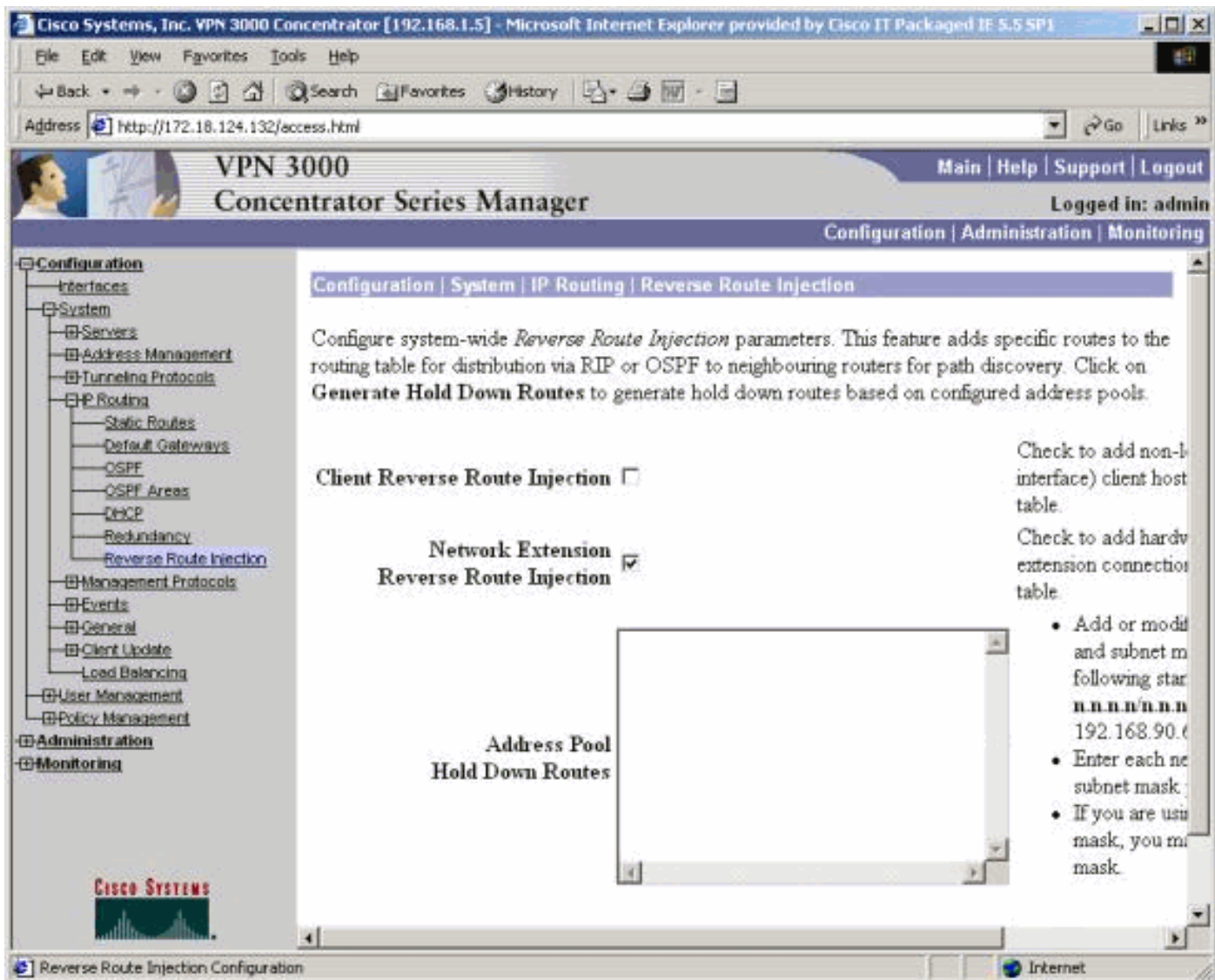
La RRI de cliente puede utilizarse en todos los clientes VPN que se conectan con el concentrador VPN. Para configurar al cliente RRI, vaya al **configuration > system > ip routing > reverse routeinjection** y seleccione el **Reverse Route Injection** de la opción para el cliente.

Nota: El concentrador VPN tiene definido un grupo y un usuario además de un grupo de clientes de 192.168.3.1 - 192.168.3.254. Vea [para verificar/RIPv2 de la prueba](#) para más información de la tabla de ruteo.

[Extensión de red RRI \(Cliente VPN 3002 en NEM únicamente\)](#)

Para configurar la Extensión de la red RRI para el cliente del VPN 3002, vaya al **configuration > system > ip routing > reverse routeinjection** y seleccione la opción para el **Reverse Route Injection** de la extensión de la red.

Nota: El cliente del VPN 3002 debe funcionar con 3.5 o el código más reciente para que la Extensión de la red RRI trabaje. Vea [verificar/prueba NEM RRI](#) para la información de la tabla de ruteo.



[Detección automática de red del LAN a LAN](#)

Esto es una sesión LAN a LAN con un peer remoto de 172.18.124.133 que cubra la red 192.168.6.0/24 en el LAN local. Dentro de la definición del LAN a LAN, (**Configuration > System > Tunneling Protocols > IPSec > LAN-to-LAN > Routing** selecto), la detección automática de red se utiliza en vez de las listas de red.

Nota: Recuerde que sólo se puede usar RIP para anunciar la dirección de redes remotas al utilizar la detección automática de red. En este caso, la detección automática normal se utiliza en vez del RRI. Vea [para verificar/detección automática de red del LAN a LAN de la prueba](#) para la información de la tabla de ruteo.

[Red RRI del LAN a LAN](#)

Para configurar para el RRI, vaya al **Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec**. En la definición del LAN a LAN, utilice el menú desplegable para fijar el campo de la encaminamiento al **Reverse Route Injection** para pasar las rutas definidas en la sesión LAN a LAN encendido al RIP o al proceso OSPF. Haga clic en Apply (Aplicar) para guardar la configuración.

Nota: Cuando la definición del LAN a LAN se fija para utilizar el RRI, el concentrador VPN 3000 hace publicidad hacia fuera de las redes remotas (red única o lista de red) de modo que el router

interno esté lejos de la red remota. Vea [para verificar/la red RRI del LAN a LAN de la prueba](#) para la información de la tabla de ruteo.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The browser window displays the URL <http://172.168.124.132/access.html>. The page title is "VPN 3000 Concentrator Series Manager" and the user is logged in as "admin". The left sidebar shows a navigation tree with "Configuration" expanded to "LAN-to-LAN". The main content area displays configuration fields for a LAN-to-LAN connection:

- Name:** to_3060b
- Interface:** Ethernet 2 (Public) (172.168.124.132)
- Peer:** 172.168.124.133
- Digital Certificate:** None (Use Preshared Keys)
- Certificate:** Entire certificate chain
- Transmission:** Identity certificate only
- Preshared Key:** cisco123
- Authentication:** ESP/MD5/HMAC-128
- Encryption:** 3DES-168
- IKE Proposal:** IKE-3DES-MD5
- Routing:** Reverse Route Injection

Each field has a corresponding help text on the right:

- Name:** Enter the name for this LAN-to-LAN connection.
- Interface:** Select the interface to put this LAN-to-LAN connection on.
- Peer:** Enter the IP address of the remote peer for this LAN-to-LAN connection.
- Digital Certificate:** Select the Digital Certificate to use.
- Certificate:** Choose how to send the digital certificate to the IKE peer.
- Transmission:** Enter the preshared key for this LAN-to-LAN connection.
- Authentication:** Specify the packet authentication mechanism to use.
- Encryption:** Specify the encryption mechanism to use.
- IKE Proposal:** Select the IKE Proposal to use for this LAN-to-LAN connection.
- Routing:** Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.

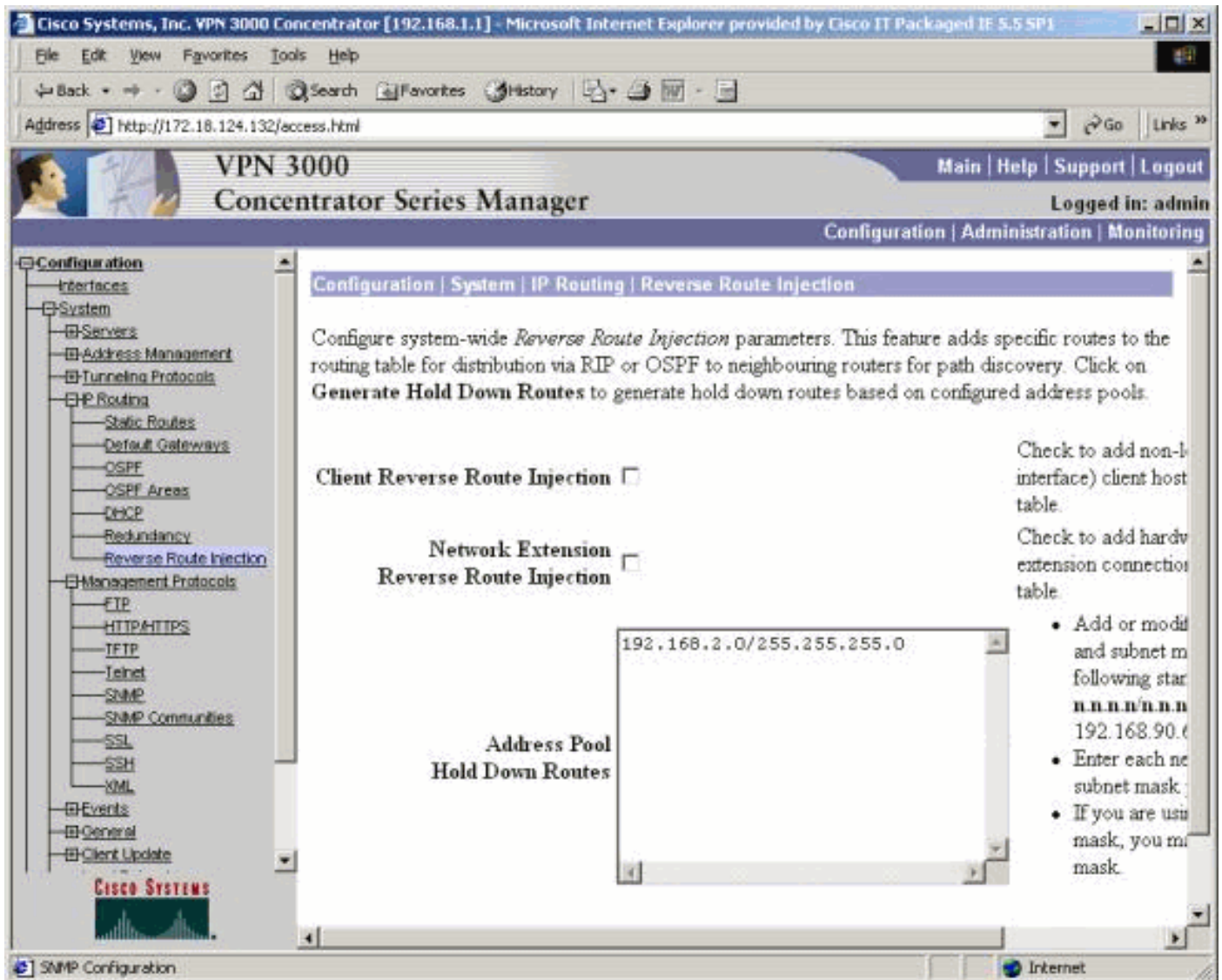
Para configurar en el modo CLI, refiérase [verifican que el rutear está correcto](#) para inyectar la información de las redes VPN remotas del LAN a LAN en la red corriente OSPF.

[Rutas retenidas](#)

Las rutas retenidas se utilizan como marcadores de posición para las rutas a las redes remotas o a grupos del cliente VPN. Por ejemplo, si un par del telecontrol VPN afronta la red 192.168.2.0/24, hay solamente algunas maneras que el LAN local puede considerar esa red:

- El router interno (tal como 2514-b en Esta es una solución aceptable si no desea ejecutar RRI o si el Concentrador VPN no admite esta característica.
- Usted puede utilizar la detección automática de red. Sin embargo, esto avanza la red 192.168.2.0/24 en la red local solamente cuando el túnel VPN está para arriba. En resumen, la red local no puede comenzar el túnel dado que no tiene conocimiento del ruteo de la red remota. Una vez que la red remota 192.168.2.0 activa el túnel, éste atraviesa la red mediante autodiscovery y luego se inserta en el proceso de ruteo. Recuerde que esto se aplica PARA RASGAR solamente; El OSPF no se puede utilizar en este caso.
- La utilización de las rutas retenidas de la agrupación de direcciones siempre anuncia las

redes definidas así las redes locales y remotas pueden encender el túnel si el túnel no existe. Para configurar a la **agrupación de direcciones mantenga las rutas**, vaya al **configuration > system > ip routing > reverse routeinjection** y entre a la agrupación de direcciones, como se muestra aquí. Vea [para verificar/las rutas del asentamiento de la prueba](#) para la información de la tabla de ruteo.



[Utilice el OSPF con el RRI](#)

Para utilizar el OSPF, vaya al **configuration > system > ip routing > ospf**, después ingrese el **Router ID** (IP Address). Marque las opciones **Autonomous System** (Sistema autónomo) y **Enabled** (Habilitado). Tenga en cuenta que, para colocar las rutas RPI en la tabla de OSPF, necesita convertir el proceso OSPF del concentrador VPN 3000 en un sistema autónomo.

Vea [verificar/prueba OSPF con el RRI](#) para la información de la tabla de ruteo.

Cisco Systems, Inc. VPN 3000 Concentrator [192.168.1.5] - Microsoft Internet Explorer provided by Cisco IT Packaged IE 5.5 SP1

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Print

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
 - Reverse Route Injection
 - Management Protocols
 - Events
 - General
 - Client Update
 - Load Balancing
 - User Management
 - Policy Management
- Administration
- Monitoring

Configuration | System | IP Routing | OSPF


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

Enabled Check to enable OSPF.

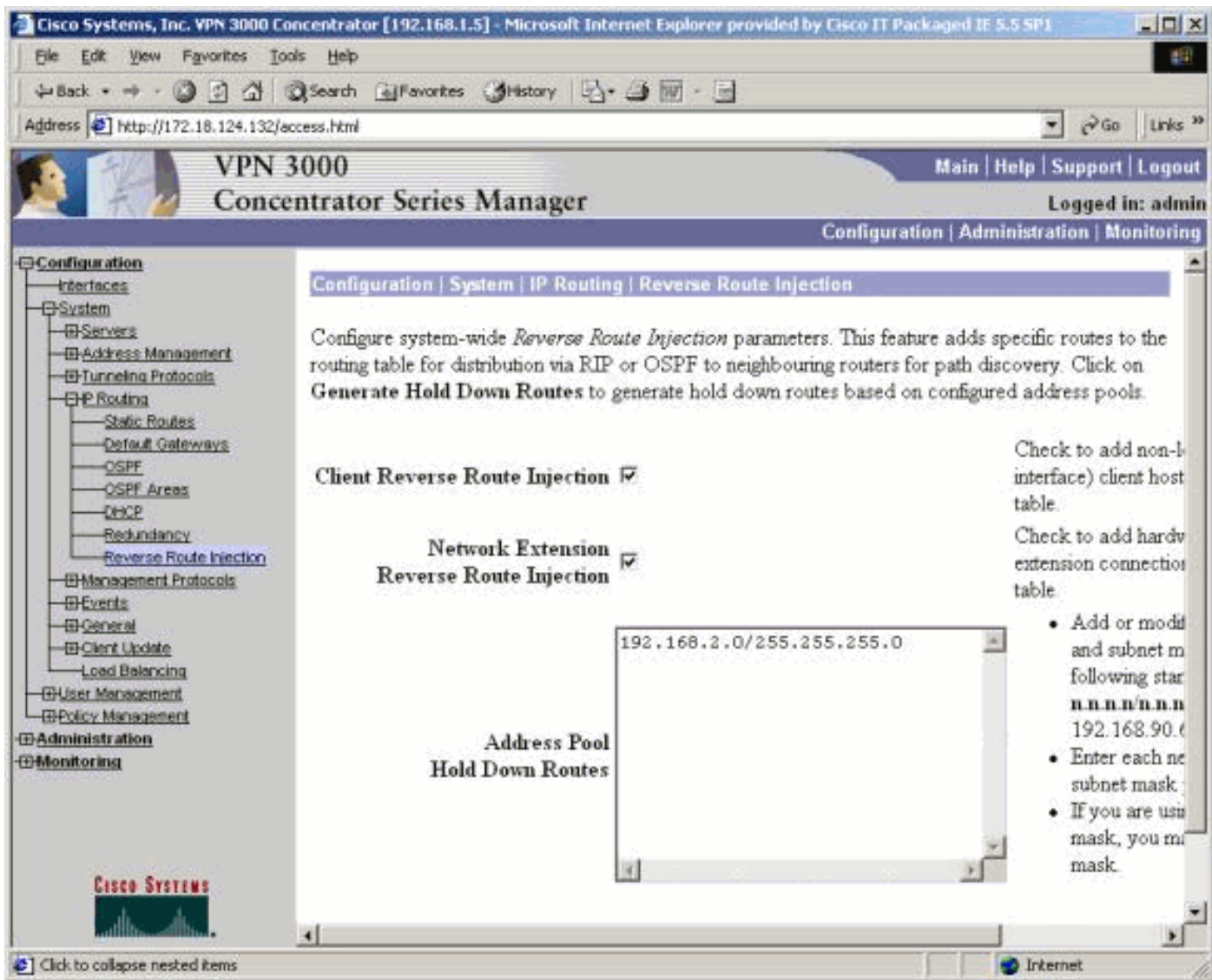
Router ID Enter the Router ID.

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

Apply Cancel



Click to expand nested items Internet



Verificación

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

Verifique/RIPv2 de la prueba

Tabla de ruteo antes de la conexión del cliente VPN

El concentrador VPN tiene definido un grupo y un usuario, además de un grupo de clientes de 192.168.3.1 - 192.168.3.254.

```
2514-b#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
192.168.1.1 to network 0.0.0.0 C 192.168.1.0/24 is directly connected, Ethernet0 S* 0.0.0.0/0
[1/0] via 192.168.1.1
```

Tabla de ruteo durante conexión de cliente VPN

```
2514-b#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
192.168.1.1 to network 0.0.0.0 172.18.0.0/24 is subnetted, 1 subnets R 172.18.124.0 [120/1] via
192.168.1.5, 00:00:21, Ethernet0 C 192.168.1.0/24 is directly connected, Ethernet0
192.168.3.0/32 is subnetted, 1 subnets R 192.168.3.1 [120/1] via 192.168.1.5, 00:00:21,
Ethernet0 !--- 192.168.3.1 is the client-assigned IP address !--- for the newly connected VPN
Client. S* 0.0.0.0/0 [1/0] via 192.168.1.1
```

Tabla de ruteo cuando dos clientes están conectados

```
2514-b#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
192.168.1.1 to network 0.0.0.0 172.18.0.0/24 is subnetted, 1 subnets R 172.18.124.0 [120/1] via
192.168.1.5, 00:00:05, Ethernet0 C 192.168.1.0/24 is directly connected, Ethernet0
192.168.3.0/32 is subnetted, 2 subnets R 192.168.3.2 [120/1] via 192.168.1.5, 00:00:05,
Ethernet0 R 192.168.3.1 [120/1] via 192.168.1.5, 00:00:05, Ethernet0 S* 0.0.0.0/0 [1/0] via
192.168.1.1
```

Con las rutas del host agregadas para cada cliente VPN, puede ser más fácil en la tabla de ruteo utilizar una [ruta del asentamiento](#) para 192.168.3.0/24. Es decir se convierte en una opción entre 250 rutas del host que utilicen al cliente RRI contra una ruta del asentamiento de la red.

Aquí está un ejemplo que muestra el uso de una ruta del asentamiento:

```
Gateway of last resort is 192.168.1.1 to network 0.0.0.0

    172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.1.5, 00:00:13, Ethernet0
C       192.168.1.0/24 is directly connected, Ethernet0
    192.168.3.0/24 is subnetted, 1 subnets
R 192.168.3.0 [120/1] via 192.168.1.5, 00:00:14, Ethernet0 !--- There is one entry for the
192.168.3.x network, !--- rather than 1 for each host for the VPN pool. S* 0.0.0.0/0 [1/0] via
192.168.1.1
```

Verifique/la prueba NEM RRI

Aquí está la tabla de ruteo del router:

```
2514-b#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
192.168.1.1 to network 0.0.0.0 R 192.168.15.0/24 [120/1] via 192.168.1.5, 00:00:05, Ethernet0 !-
-- This is the network behind the VPN 3002 Client. 172.18.0.0/24 is subnetted, 1 subnets R
172.18.124.0 [120/1] via 192.168.1.5, 00:00:05, Ethernet0 C 192.168.1.0/24 is directly
connected, Ethernet0 S* 0.0.0.0/0 [1/0] via 192.168.1.1
```

Verifique/detección automática de red del LAN a LAN de la prueba

Tabla de ruteo antes de la conexión de LAN a LAN (detección automática de red)

```
2514-b#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 192.168.1.1 to network 0.0.0.0 172.18.0.0/24 is subnetted, 1 subnets R 172.18.124.0 [120/1] via 192.168.1.5, 00:00:07, Ethernet0 C 192.168.1.0/24 is directly connected, Ethernet0 S* 0.0.0.0/0 [1/0] via 192.168.1.1

Tabla de ruteo (router interno) durante el LAN a LAN (detección automática de red)

```
2514-b#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
192.168.1.1 to network 0.0.0.0 172.18.0.0/24 is subnetted, 1 subnets R 172.18.124.0 [120/1] via
192.168.1.5, 00:00:04, Ethernet0 R 192.168.6.0/24 [120/2] via 192.168.1.5, 00:00:04, Ethernet0 C
192.168.1.0/24 is directly connected, Ethernet0 S* 0.0.0.0/0 [1/0] via 192.168.1.1
```

Nota: El RIP tiene un temporizador del asentamiento del tres-minuto. Aunque la sesión LAN a LAN cayó, tarda aproximadamente tres minutos para que la ruta mida el tiempo realmente hacia fuera.

Verifique/la red RRI del LAN a LAN de la prueba

Aquí está la tabla de ruteo del router:

```
Gateway of last resort is 192.168.1.1 to network 0.0.0.0

 172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.1.5, 00:00:11, Ethernet0
R       192.168.6.0/24 [120/1] via 192.168.1.5, 00:00:11, Ethernet0
C       192.168.1.0/24 is directly connected, Ethernet0
S*     0.0.0.0/0 [1/0] via 192.168.1.1
```

Porque 192.168.6.0/24 fueron utilizados en la lista de redes remotas del LAN a LAN, esta información se pasa apagado al proceso de ruteo. Si hubiera una lista de red de 192.168.6.x, de .7.x, y de .8.x (el /24), después la tabla de ruteo del router parecería esto:

```
R       192.168.8.0/24 [120/1] via 192.168.1.5, 00:00:02, Ethernet0
 172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.1.5, 00:00:02, Ethernet0
R       192.168.6.0/24 [120/1] via 192.168.1.5, 00:00:02, Ethernet0
R       192.168.7.0/24 [120/1] via 192.168.1.5, 00:00:02, Ethernet0
C       192.168.1.0/24 is directly connected, Ethernet0
S*     0.0.0.0/0 [1/0] via 192.168.1.1
...
```

Verifique/las rutas del asentamiento de la prueba

En este ejemplo, 192.168.2.0 es la red remota que usted quiere como tenedor del lugar. Por abandono, la tabla de ruteo en el router interno después de habilitar el pool del asentamiento muestra:

```
2514-b#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
192.168.1.1 to network 0.0.0.0 172.18.0.0/24 is subnetted, 1 subnets R 172.18.124.0 [120/1] via
192.168.1.5, 00:00:05, Ethernet0 C 192.168.1.0/24 is directly connected, Ethernet0 R
```

192.168.2.0/24 [120/1] via 192.168.1.5, 00:00:06, Ethernet0 S* 0.0.0.0/0 [1/0] via 192.168.1.1
Observe que la ruta 172.18.124.0 es de hecho la red de interfaz pública externa del concentrador VPN 3000. Si usted no quisiera que esta ruta fuera aprendida vía la interfaz privada del concentrador VPN, agregue una Static ruta o reescribir/bloque del filtro de la ruta esta ruta aprendido.

Usando una Static ruta que ahora señale al escurdo de protección corporativo en 192.168.1.1 muestra la tabla de ruteo como usando la ruta de IP 172.18.124.0 255.255.255.0 192.168.1.1, como se muestra aquí:

```
2514-b#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
192.168.1.1 to network 0.0.0.0 172.18.0.0/24 is subnetted, 1 subnets S 172.18.124.0 [1/0] via
192.168.1.1 C 192.168.1.0/24 is directly connected, Ethernet0 R 192.168.2.0/24 [120/1] via
192.168.1.5, 00:00:28, Ethernet0 S* 0.0.0.0/0 [1/0] via 192.168.1.1
```

[Verifique/la prueba OSPF con el RRI](#)

```
2514-b#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
192.168.1.1 to network 0.0.0.0 O E2 192.168.15.0/24 [110/20] via 192.168.1.5, 00:07:33,
Ethernet0 O E2 192.168.6.0/24 [110/20] via 192.168.1.5, 00:07:33, Ethernet0 C 192.168.1.0/24 is
directly connected, Ethernet0 O E2 192.168.2.0/24 [110/20] via 192.168.1.5, 00:07:33, Ethernet0
192.168.3.0/32 is subnetted, 1 subnets O E2 192.168.3.1 [110/20] via 192.168.1.5, 00:00:08,
Ethernet0 S* 0.0.0.0/0 [1/0] via 192.168.1.1
```

Aquí están los valores por este ejemplo:

- 192.168.15.0 es el modo de extensión de red para el concentrador VPN 3002.
- 192.168.6.0 es la red para la sesión LAN a LAN.
- 192.168.3.1 es una ruta retenida.
- 192.168.3.1 es una ruta ingresada por el cliente.

[Verifique la información de la tabla de ruteo en el concentrador VPN](#)

Asegúrese de que las rutas aparezcan en la tabla de ruteo en el Concentrador VPN local. Para marcar esto, vaya al **Monitoring > Routing Table**.

Usted puede ver las rutas aprendidas vía el RRI como Static rutas de la interfaz pública (interfaz #2). En este ejemplo, las rutas son:

- La ruta retenida, 192.168.2.0, muestra el siguiente salto que será la dirección IP de la interfaz pública, 172.18.124.132.
- El cliente VPN al que se le asignó la dirección 192.168.3.1 tiene su salto siguiente en el gateway predeterminado para el Concentrador VPN en la red pública (172.18.124.1).
- La conexión de LAN a LAN en 192.168.6.0 muestra a su dirección de peer de 172.18.124.133, y lo mismo es verdad para el concentrador del VPN 3002 en el modo de ampliación de la red.

Monitoring | Routing Table Thursday, 20 December 2001 08:50:55 Refresh

Clear Routes

Valid Routes: 7

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	Static	0	1
192.168.3.1	255.255.255.255	172.18.124.1	2	Static	0	1
192.168.6.0	255.255.255.0	172.18.124.133	2	Static	0	1
192.168.15.0	255.255.255.0	172.18.124.127	2	Static	0	1

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Soluciones a los Problemas más frecuentes de IPSec VPN L2L y de Acceso Remoto](#)
- [Concentrador soporta del Cisco VPN de la serie 3000](#)
- [Soporte de cliente del Cisco VPN de la serie 3000](#)
- [Soporte de la Negociación IPSec/Protocolos IKE](#)
- [Soporte OSPF](#)
- [Soporte del RIP](#)
- [Soporte Técnico - Cisco Systems](#)