

Ejemplo de Configuración de GRE sobre IPSec con EIGRP para Rutear a través de un Hub y Múltiples Sitios Remotos

Contenido

[Introducción](#)

[prerrequisitos](#)

[prerrequisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Diagrama de la red](#)

[Configurar](#)

[Configure los túneles GRE](#)

[Configure el cifrado para los túneles GRE](#)

[Configure el Routing Protocol](#)

[Configuraciones de Ejemplo](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento explica cómo configurar GRE sobre IPSec para rutear a través de un sitio hub a varios sitios remotos. El Cisco 7206 Router es el router del sitio central, con quien el resto de sitios conectan con el IPSec. El Routers del 2610, 3620 y 3640 de Cisco es los routers remotos. Todos los sitios pueden alcanzar la red principal detrás del Cisco 7206 y el resto de los sitios remotos a través del túnel al sitio principal, con las actualizaciones de ruteo ocurriendo automáticamente vía el Enhanced Interior Gateway Routing Protocol (EIGRP).

[prerrequisitos](#)

[prerrequisitos](#)

Este documento fue desarrollado y probado utilizando el hardware y las versiones de software indicados a continuación.

[Componentes Utilizados](#)

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

- Cisco 7206 Router que funciona con el Software Release 12.3(1) IK9S de Cisco IOS®
- Cisco IOS Software Release 12.3(1) corriente IK9S del Cisco 2621XM Router
- Cisco IOS Software Release 12.3(1) corriente IK9S del Cisco 3640 Router
- Cisco IOS Software Release 12.3(1) corriente IK9S del Cisco 3640 Router

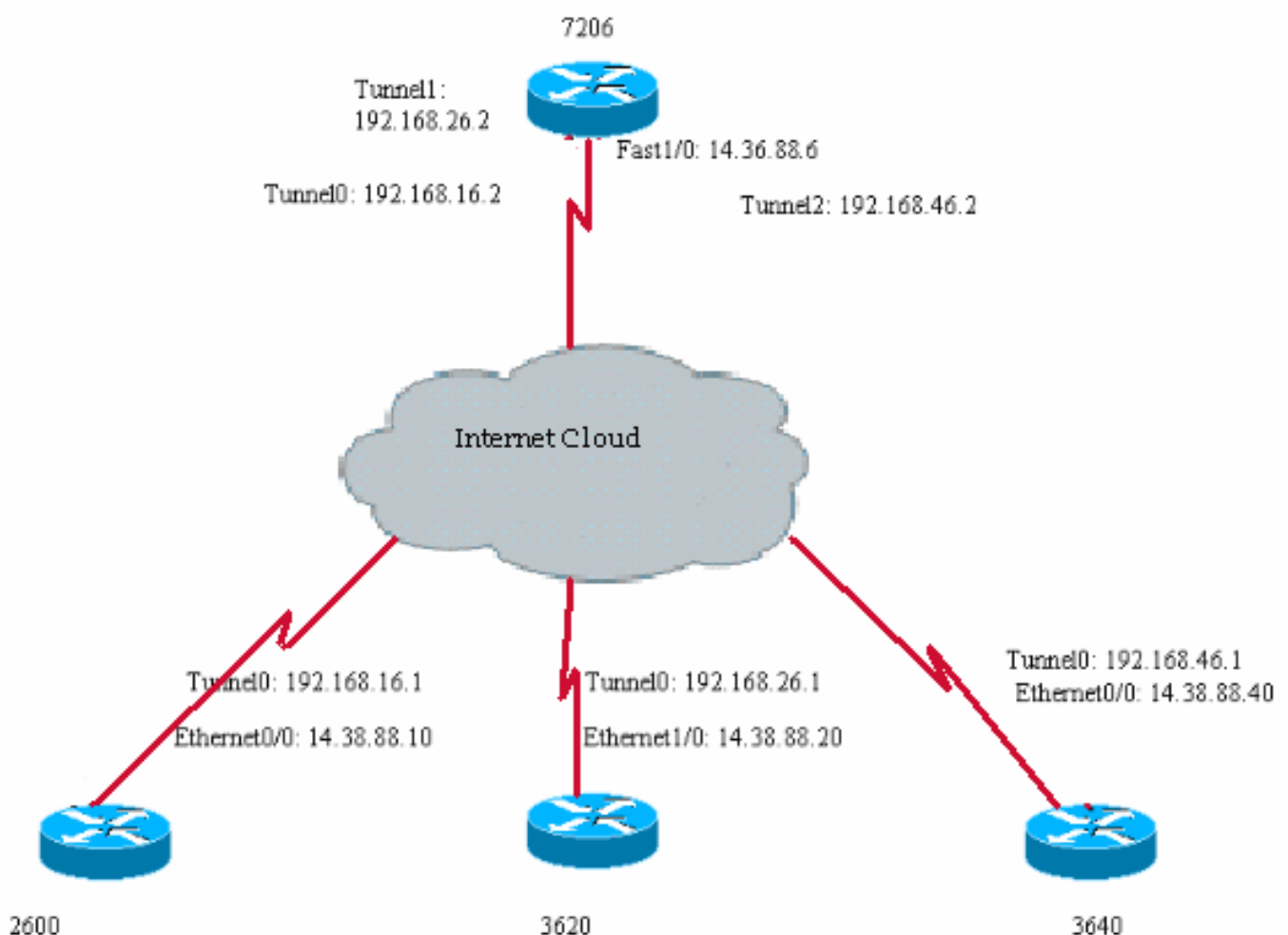
La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese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

Convenciones

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

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configurar

Este proceso lo llevará a través del proceso de configuración de un túnel IPsec a una ruta

mediante un hub y varios sitios remotos. El proceso se separa en estos tres pasos primarios.

- [Configure los túneles del Generic Routing Encapsulation \(GRE\)](#)
- [Configure el cifrado para los túneles GRE](#)
- [Configure el Routing Protocol](#)

Configure los túneles GRE

Siga los siguientes pasos para configurar los túneles GRE:

1. Cree un túnel GRE de cada sitio remoto a la oficina principal. Configure una interfaz de túnel en el router 7206 de Cisco para cada sitio remoto.

```
interface Tunnel0
 ip address 192.168.16.2 255.255.255.0
 tunnel source FastEthernet1/0
 tunnel destination 14.38.88.10
!
interface Tunnel1
 ip address 192.168.46.2 255.255.255.0
 tunnel source FastEthernet1/0
 tunnel destination 14.38.88.40
!
interface Tunnel2
 ip address 192.168.26.2 255.255.255.0
 tunnel source FastEthernet1/0
```

El origen de cada túnel es la interfaz FastEthernet1/0 o la interfaz que representa la conexión a Internet. El destino del túnel es la dirección IP de la interfaz de Internet del router remoto. Cada túnel debe tener una dirección IP en un diferente, subred sin utilizar.

2. Configure los túneles GRE en el Routers del 2610, 3620 y 3640 de Cisco. Las configuraciones son similares al Cisco 7206 Router.

```
Cisco 2610 Router interface Tunnel0
 ip address 192.168.16.1 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 14.36.88.6
Cisco 3620 Router interface Tunnel0
 ip address 192.168.26.1 255.255.255.0
 tunnel source Ethernet1/0
 tunnel destination 14.36.88.6
Cisco 3640 Router interface Tunnel0
 ip address 192.168.46.1 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 14.36.88.6
```

Cada router remoto utiliza su interfaz local que conecte con Internet como el origen de túnel. Los routers remotos corresponden a las direcciones IP de destino del túnel en la configuración del router Cisco 7206. El IP Address de destino del túnel para cada router remoto corresponde a la dirección IP de la interfaz del Cisco 7206 Router que conecta con Internet. La dirección IP de la interfaz de túnel corresponde a una dirección IP en la misma subred que la interfaz de túnel del router 7206 de Cisco.

3. Asegúrese de que cada router remoto pueda hacer ping la dirección IP del destino del túnel y de la interfaz del túnel correspondiente del router principal. También, asegúrese de que cada router sea pingable del router del sitio central.

```
Cisco 2610 Router vpn2610#ping
14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
vpn2610#ping 192.168.16.2
Type escape sequence to abort.
```

```

Sending 5, 100-byte ICMP Echos to 192.168.16.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/12 ms
vpn2610#Cisco 3620 Routervpn3620#ping 14.38.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.38.88.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3620#ping 192.168.26.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.26.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms
vpn3620#Cisco 3640 Routervpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#Nota: Si no todo el Routers puede hacer ping al router central (del concentrador),
resuelve problemas cada conexión según las necesidades usando estas guías de
consulta.¿Puede el router remoto hacer ping al router de eje de conexión del IP del público
al IP del público?¿Hay dispositivo que bloquea el GRE entre el dos Routers? (Firewall, lista
de acceso en el router)¿Qué muestra para la interfaz de túnel el comando show interface?

```

[Configure el cifrado para los túneles GRE](#)

Complete estos pasos para configurar el cifrado para los túneles GRE:

1. Si suben los túneles GRE, proceda con cifrar. Primero, cree las Listas de acceso para definir el tráfico para el cifrado.Las Listas de acceso permiten el tráfico del IP Address local en cada router a la dirección IP en el extremo contrario. Utilice el comando show version para mostrar la versión de software que el Motor de memoria de caché está

```

ejecutando.vpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#

```

2. Configure una directiva del Internet Security Association and Key Management Protocol (ISAKMP), una clave ISAKMP, y un IPSec transforma el conjunto.La política ISAKMP, la clave y el conjunto de transformación IPSec deben coincidir en ambos lados de un mismo túnel. No todos los túneles tienen que utilizar la misma directiva, clave, o transforme el conjunto. En este ejemplo, todos los túneles utilizan la misma directiva, clave, y transforman el conjunto para la simplicidad.**Cisco 7206 Router**vpn3640#ping 14.36.88.6

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:

```

```
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#Cisco 2610 Routervpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#Cisco 3620 Routervpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#Cisco 3640 Routervpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#
```

3. Configure la correspondencia de criptografía. El sitio central tiene un número de secuencia distinto para cada conexión.

```
Cisco 7206 Routervpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#Cisco 2610 Routervpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#Cisco 3620 Routervpn3640#ping 14.36.88.6
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#Cisco 3640 Routervpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#
```

4. Aplique la correspondencia de criptografía. El mapa debe aplicarse a la interfaz de túnel y a la interfaz física que los paquetes terminan.Cisco 7206 Routervpn3640#ping 14.36.88.6

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#Cisco 2610 Routervpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#Cisco 3620 Routervpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#Cisco 3640 Routervpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#
```

[Configure el Routing Protocol](#)

Para configurar el Routing Protocol, configurar todos los sitios con el número del sistema autónomo y dar instrucciones el (EIGRP) del Routing Protocol para compartir las rutas. Sólo las redes que están incluidas en las sentencias de red se comparten con otros routers por el protocolo de ruteo. El número del sistema autónomo debe hacer juego en todo el Routers que participe en la distribución de las rutas. En este ejemplo, las redes que se pueden resumir en una declaración de la red se utilizan para la simplicidad.

Cisco 7206 Router

```
vpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#
```

Cisco 2610 Router

```
vpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#
```

Cisco 3620 Router

```
vpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#
```

Cisco 3640 Router

```
vpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is 2 seconds:
!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
vpn3640#

[Configuraciones de Ejemplo](#)

Este documento utiliza las siguientes configuraciones de ejemplo:

- [Cisco 7206 Router](#)
- [Cisco 2610 Router](#)
- [Cisco 3620 Router](#)
- [Cisco 3640 Router](#)

Cisco 7206 Router

```
vpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is
2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout
is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 4/6/8 ms
vpn3640#
```

Cisco 2610 Router

```
vpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is
2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout
is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 4/6/8 ms
vpn3640#
```

Cisco 3620 Router

```
vpn3640#ping 14.36.88.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is
2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 1/2/4 ms
vpn3640#ping 192.168.46.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout
is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 4/6/8 ms
```



```
vpn3640#  
Cisco 3640 Router  
vpn3640#ping 14.36.88.6  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 14.36.88.6, timeout is  
2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip  
min/avg/max = 1/2/4 ms  
vpn3640#ping 192.168.46.2  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.46.2, timeout is  
2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip  
min/avg/max = 4/6/8 ms  
vpn3640#
```

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.

- **ruta de IP de la demostración** — Utilice este comando de asegurarse de que las rutas son doctas con el Routing Protocol.

Cisco 7206 Router

```
sec-7206#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 14.36.1.1 to network 0.0.0.0  
C 192.168.46.0/24 is directly connected, Tunnel1  
D 192.168.10.0/24 [90/297372416] via 192.168.16.1, 05:53:23, Tunnel0  
D 192.168.40.0/24 [90/297372416] via 192.168.46.1, 05:53:23, Tunnel1  
C 192.168.26.0/24 is directly connected, Tunnel2  
D 192.168.20.0/24 [90/297372416] via 192.168.26.1, 05:53:21, Tunnel2  
C 192.168.16.0/24 is directly connected, Tunnel0  
14.0.0.0/16 is subnetted, 1 subnets  
C 14.36.0.0 is directly connected, FastEthernet1/0  
S* 0.0.0.0/0 [1/0] via 14.36.1.1  
sec-7206#
```

Cisco 2610 Router

```
vpn2610#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 14.38.1.1 to network 0.0.0.0
D 192.168.46.0/24 [90/310044416] via 192.168.16.2, 05:53:55, Tunnel0
C 192.168.10.0/24 is directly connected, Loopback0
D 192.168.40.0/24 [90/310172416] via 192.168.16.2, 05:53:55, Tunnel0
D 192.168.26.0/24 [90/310044416] via 192.168.16.2, 05:53:55, Tunnel0
D 192.168.20.0/24 [90/310172416] via 192.168.16.2, 05:53:53, Tunnel0
C 192.168.16.0/24 is directly connected, Tunnel0
14.0.0.0/16 is subnetted, 1 subnets
C 14.38.0.0 is directly connected, Ethernet0/0
S* 0.0.0.0/0 [1/0] via 14.38.1.1
vpn2610#

```

Cisco 3620 Router

```

vpn3620#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 14.38.1.1 to network 0.0.0.0
D 192.168.46.0/24 [90/310044416] via 192.168.26.2, 05:54:15, Tunnel0
D 192.168.10.0/24 [90/310172416] via 192.168.26.2, 05:54:15, Tunnel0
D 192.168.40.0/24 [90/310172416] via 192.168.26.2, 05:54:15, Tunnel0
C 192.168.26.0/24 is directly connected, Tunnel0
C 192.168.20.0/24 is directly connected, Loopback0
D 192.168.16.0/24 [90/310044416] via 192.168.26.2, 05:54:15, Tunnel0
14.0.0.0/16 is subnetted, 1 subnets
C 14.38.0.0 is directly connected, Ethernet1/0
S* 0.0.0.0/0 [1/0] via 14.38.1.1
vpn3620#

```

Cisco 3640 Router

```

vpn3640#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 14.38.1.1 to network 0.0.0.0
C 192.168.46.0/24 is directly connected, Tunnel0
D 192.168.10.0/24 [90/310172416] via 192.168.46.2, 05:54:32, Tunnel0
C 192.168.40.0/24 is directly connected, Loopback0
D 192.168.26.0/24 [90/310044416] via 192.168.46.2, 05:54:32, Tunnel0
D 192.168.20.0/24 [90/310172416] via 192.168.46.2, 05:54:30, Tunnel0
D 192.168.16.0/24 [90/310044416] via 192.168.46.2, 05:54:32, Tunnel0
14.0.0.0/16 is subnetted, 1 subnets
C 14.38.0.0 is directly connected, Ethernet0/0
S* 0.0.0.0/0 [1/0] via 14.38.1.1
vpn3640#

```

Nota: Con un indicador luminoso LED amarillo de la placa muestra gravedad menor del adaptador de los Servicios integrados (ISA) en el Cisco 7206 Router, el Cisco Express Forwarding (CEF) puede tener que ser inhabilitado para que las actualizaciones de ruteo pasen.

[Troubleshooting](#)

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

[Información Relacionada](#)

- [Página de soporte de IPSec](#)
- [Soporte Técnico - Cisco Systems](#)