

# GRE over IPsec with EIGRP to Route Through a Hub and Multiple Remote Sites Configuration Example

Document ID: 17868

---

## Introduction

### Prerequisites

Prerequisites

Components Used

Conventions

Network Diagram

### Configure

Configure the GRE Tunnels

Configure the Encryption for the GRE Tunnels

Configure the Routing Protocol

### Sample Configurations

### Verify

### Troubleshoot

### Related Information

---

## Introduction

This document explains how to configure GRE over IPsec routing through a hub site to multiple remote sites. The Cisco 7206 router is the central site router, to which all the other sites connect through IPsec. The Cisco 2610, 3620, and 3640 routers are the remote routers. All sites are able to reach the main network behind the Cisco 7206 and all other remote sites through the tunnel to the main site, with routing updates taking place automatically via Enhanced Interior Gateway Routing Protocol (EIGRP).

## Prerequisites

### Prerequisites

This document was developed and tested using the software and hardware versions below.

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco 7206 Router running Cisco IOS® Software Release 12.3(1) IK9S
- Cisco 2621XM Router running Cisco IOS Software Release 12.3(1) IK9S
- Cisco 3640 Router running Cisco IOS Software Release 12.3(1) IK9S
- Cisco 3640 Router running Cisco IOS Software Release 12.3(1) IK9S

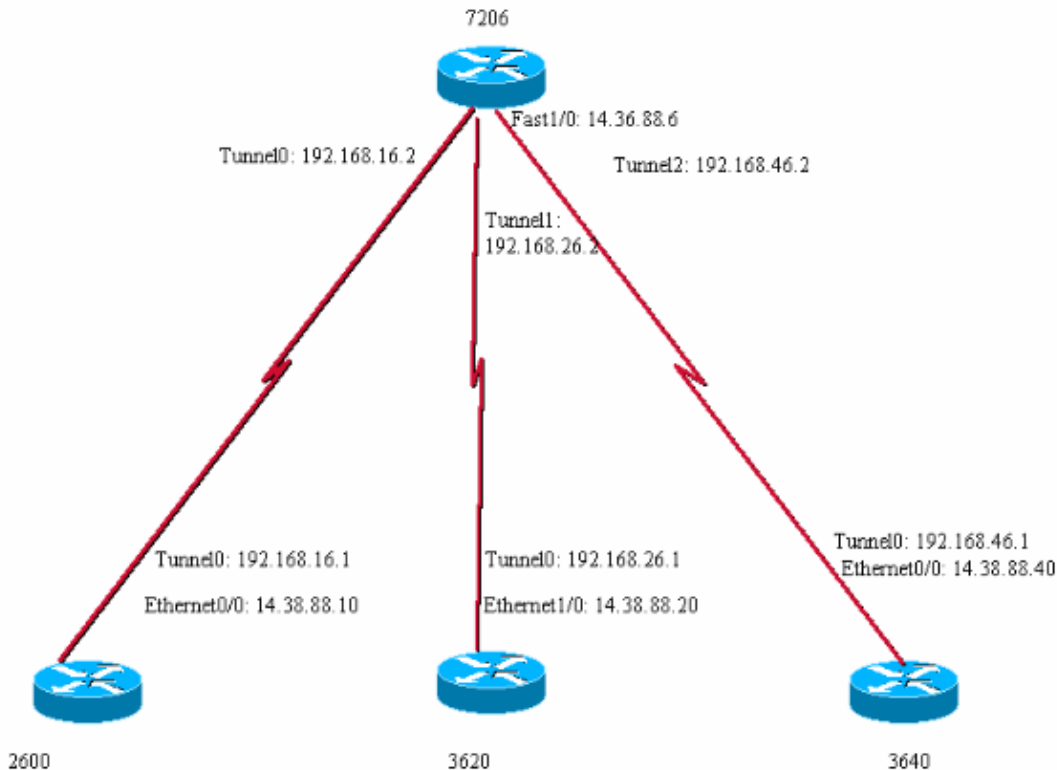
The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

## Conventions

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

## Network Diagram

This document uses this network setup:



## Configure

This process guides you through configuring an IPSec tunnel to route through a hub and multiple remote sites. The process is separated into these three primary steps.

- Configure the Generic Routing Encapsulation (GRE) Tunnels
- Configure Encryption for the GRE Tunnels
- Configure the Routing Protocol

### Configure the GRE Tunnels

Follow these steps to configure the GRE tunnels:

1. Create a GRE tunnel from each remote site to the main office. Set up a tunnel interface on the Cisco 7206 router for each remote site.

```
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
tunnel destination 14.38.88.20

```

The tunnel source for each tunnel is the FastEthernet1/0 interface, or the interface that is the Internet connection. The tunnel destination is the IP address of the remote router's Internet interface. Each tunnel should have an IP address on a different, unused subnet.

2. Configure the GRE tunnels on the Cisco 2610, 3620, and 3640 routers. The configurations are similar to the 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

```

Each remote router uses its local interface that connects to the Internet as the tunnel source. The remote routers correspond to the tunnel destination IP addresses in the configuration on the Cisco 7206 router. The tunnel destination IP address for each remote router corresponds to the IP address of the interface of the Cisco 7206 router that connects to the Internet. The IP address of the tunnel interface corresponds to an IP address on the same subnet as the tunnel interface of the Cisco 7206 router.

3. Ensure that each remote router can ping the IP address of the tunnel destination and the main router's corresponding tunnel interface.

Also, ensure that each router is pingable from the central site router.

### 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 Router

```
vpn3620#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 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#
```

**Note:** If not all routers can ping the central (hub) router, troubleshoot each connection as needed using these guidelines.

- ◆ Can the remote router ping the hub router from public IP to public IP?
- ◆ Is there any device blocking GRE between the two routers? (Firewall, access-list on router)
- ◆ What does a **show interface** command show for the tunnel interface?

## Configure the Encryption for the GRE Tunnels

Complete these steps to configure the encryption for the GRE tunnels:

1. If the GRE tunnels come up, proceed with encrypting. First, create access lists to define the traffic for encryption.

The access lists permit traffic from the local IP address on each router to the IP address on the opposite end. Use the **show version** command to display the software version the Cache Engine is running.

```
7206:
access-list 130 permit gre host 14.36.88.6 host 14.38.88.40
access-list 140 permit gre host 14.36.88.6 host 14.38.88.20
access-list 150 permit gre host 14.36.88.6 host 14.38.88.10

2610:
access-list 120 permit gre host 14.38.88.10 host 14.36.88.6

3620:
access-list 110 permit gre host 14.38.88.20 host 14.36.88.6

3640:
access-list 100 permit gre host 14.38.88.40 host 14.36.88.6
```

2. Configure an Internet Security Association and Key Management Protocol (ISAKMP) policy, an ISAKMP key, and an IPsec transform set.

The ISAKMP policy, key, and IPsec transform set must match on both sides of a single tunnel. Not all tunnels have to use the same policy, key, or transform set. In this example, all tunnels use the same policy, key, and transform set for simplicity.

### **Cisco 7206 Router**

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
 mode transport
```

### **Cisco 2610 Router**

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
 mode transport
```

### **Cisco 3620 Router**

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
 mode transport
```

### **Cisco 3640 Router**

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
 mode transport
```

3. Configure the crypto map. The central site has a separate sequence number for each connection.

### **Cisco 7206 Router**

```
crypto map vpn 10 ipsec-isakmp
 set peer 14.38.88.40
 set transform-set strong
 match address 130
crypto map vpn 20 ipsec-isakmp
 set peer 14.38.88.20
 set transform-set strong
 match address 140
crypto map vpn 30 ipsec-isakmp
 set peer 14.38.88.10
 set transform-set strong
 match address 150
```

### **Cisco 2610 Router**

```
crypto map vpn 10 ipsec-isakmp
set peer 14.36.88.6
set transform-set strong
match address 120
```

### **Cisco 3620 Router**

```
crypto map vpn 10 ipsec-isakmp
set peer 14.36.88.6
set transform-set strong
match address 110
```

### **Cisco 3640 Router**

```
crypto map vpn 10 ipsec-isakmp
set peer 14.36.88.6
set transform-set strong
match address 100
```

4. Apply the crypto map. The map should be applied to the tunnel interface and the physical interface that the packets exit.

### **Cisco 7206 Router**

```
interface Tunnel0
crypto map vpn
interface Tunnel1
crypto map vpn
interface Tunnel2
crypto map vpn
interface FastEthernet1/0
crypto map vpn
```

### **Cisco 2610 Router**

```
interface Tunnel0
crypto map vpn
interface Ethernet0/0
crypto map vpn
```

### **Cisco 3620 Router**

```
interface Tunnel0
crypto map vpn
interface Ethernet1/0
crypto map vpn
```

### **Cisco 3640 Router**

```
interface Tunnel0
crypto map vpn
interface Ethernet0/0
crypto map vpn
```

## **Configure the Routing Protocol**

To configure the routing protocol, configure all sites with the autonomous system number and instruct the routing protocol (EIGRP) to share routes. Only networks that are included in the network statements are shared with the other routers by the routing protocol. The autonomous system number must match in all routers that participate in the sharing of routes. In this example, networks that can be summarized into one network statement are used for simplicity.

## Cisco 7206 Router

```
router eigrp 60
 network 192.168.0.0 0.0.255.255
 auto-summary
 no eigrp log-neighbor-changes
```

## Cisco 2610 Router

```
router eigrp 60
 network 192.168.0.0 0.0.255.255
 auto-summary
 no eigrp log-neighbor-changes
```

## Cisco 3620 Router

```
router eigrp 60
 network 192.168.0.0 0.0.255.255
 auto-summary
 no eigrp log-neighbor-changes
```

## Cisco 3640 Router

```
router eigrp 60
 network 192.168.0.0 0.0.255.255
 auto-summary
 no eigrp log-neighbor-changes
```

# Sample Configurations

This document uses these sample configurations:

- Cisco 7206 Router
- Cisco 2610 Router
- Cisco 3620 Router
- Cisco 3640 Router

### Cisco 7206 Router

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname sec-7206
!
aaa new-model
aaa authentication ppp default local
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip cef
!
ip audit notify log
ip audit po max-events 100
vpdn enable
!
```

```
vpdn-group 1
! Default L2TP VPDN group
accept-dialin
  protocol l2tp
  virtual-template 1
no l2tp tunnel authentication
!
!
!
crypto isakmp policy 1
  authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
!
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
  mode transport
!
crypto map vpn 10 ipsec-isakmp
  set peer 14.38.88.40
  set transform-set strong
  match address 130
crypto map vpn 20 ipsec-isakmp
  set peer 14.38.88.20
  set transform-set strong
  match address 140
crypto map vpn 30 ipsec-isakmp
  set peer 14.38.88.10
  set transform-set strong
  match address 150
!
!
!
!
!
!
interface Tunnel0
  ip address 192.168.16.2 255.255.255.0
  tunnel source FastEthernet1/0
  tunnel destination 14.38.88.10
  crypto map vpn
!
interface Tunnel1
  ip address 192.168.46.2 255.255.255.0
  tunnel source FastEthernet1/0
  tunnel destination 14.38.88.40
  crypto map vpn
!
interface Tunnel2
  ip address 192.168.26.2 255.255.255.0
  tunnel source FastEthernet1/0
  tunnel destination 14.38.88.20
  crypto map vpn
!
interface FastEthernet0/0
  no ip address
  no ip mroute-cache
  shutdown
  media-type MII
  half-duplex
!
interface FastEthernet1/0
  ip address 14.36.88.6 255.255.0.0
  no ip mroute-cache
  half-duplex
  crypto map vpn
!
```

```

interface Virtual-Templat1
 ip unnumbered FastEthernet1/0
 peer default ip address pool test
 ppp authentication ms-chap
!
router eigrp 60
 network 192.168.0.0 0.0.255.255
 auto-summary
 no eigrp log-neighbor-changes
!
ip local pool test 10.0.7.1 10.0.7.254
ip default-gateway 14.36.1.1
ip classless
ip route 0.0.0.0 0.0.0.0 14.36.1.1
no ip http server
!
access-list 130 permit gre host 14.36.88.6 host 14.38.88.40
access-list 140 permit gre host 14.36.88.6 host 14.38.88.20
access-list 150 permit gre host 14.36.88.6 host 14.38.88.10
radius-server host 172.18.124.197 auth-port 1645 acct-port
1646 key cisco123
radius-server retransmit 3
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
end

sec-7206#

```

### Cisco 2610 Router

```

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname vpn2610
!
!
ip subnet-zero
ip cef
!
!
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
 mode transport
!
crypto map vpn 10 ipsec-isakmp
 set peer 14.36.88.6
 set transform-set strong
 match address 120
!
call rsvp-sync
!
!

```

```
!  
!  
!  
!  
!  
!  
interface Loopback0  
 ip address 192.168.10.1 255.255.255.0  
!  
interface Tunnel0  
 ip address 192.168.16.1 255.255.255.0  
 tunnel source Ethernet0/0  
 tunnel destination 14.36.88.6  
 crypto map vpn  
!  
interface Ethernet0/0  
 ip address 14.38.88.10 255.255.0.0  
 half-duplex  
 crypto map vpn  
!  
interface Serial0/0  
 no ip address  
 shutdown  
 no fair-queue  
!  
interface Ethernet0/1  
 ip address dhcp  
 half-duplex  
!  
interface Serial1/0  
 no ip address  
 shutdown  
!  
interface Serial1/1  
 no ip address  
 shutdown  
!  
interface Serial1/2  
 no ip address  
 shutdown  
!  
interface Serial1/3  
 no ip address  
 shutdown  
!  
interface Serial1/4  
 no ip address  
 shutdown  
!  
interface Serial1/5  
 no ip address  
 shutdown  
!  
interface Serial1/6  
 no ip address  
 shutdown  
!  
interface Serial1/7  
 no ip address  
 shutdown  
!  
router eigrp 60  
 network 192.168.0.0 0.0.255.255  
 auto-summary  
 no eigrp log-neighbor-changes  
!
```

```
ip classless
ip route 0.0.0.0 0.0.0.0 14.38.1.1
ip http server
!
access-list 120 permit gre host 14.38.88.10 host 14.36.88.6
!
dial-peer cor custom
!
!
!
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  login
line vty 5 15
  login
!
end
vpn2610#
```

### Cisco 3620 Router

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname vpn3620
!
!
ip subnet-zero
ip cef
!
!
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1
  authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
  mode transport
!
crypto map vpn 10 ipsec-isakmp
  set peer 14.36.88.6
  set transform-set strong
  match address 110
!
call rsvp-sync
!
!
!
!
!
!
!
!
interface Loopback0
  ip address 192.168.20.1 255.255.255.0
```

```

!
interface Tunnel0
 ip address 192.168.26.1 255.255.255.0
 tunnel source Ethernet1/0
 tunnel destination 14.36.88.6
 crypto map vpn
!
interface Ethernet1/0
 ip address 14.38.88.20 255.255.0.0
 half-duplex
 crypto map vpn
!
interface TokenRing1/0
 no ip address
 shutdown
 ring-speed 16
!
router eigrp 60
 network 192.168.0.0 0.0.255.255
 auto-summary
 no eigrp log-neighbor-changes
!
ip classless
ip route 0.0.0.0 0.0.0.0 14.38.1.1
ip http server
!
access-list 110 permit gre host 14.38.88.20 host 14.36.88.6
!
dial-peer cor custom
!
!
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
vpn3620#

```

### Cisco 3640 Router

```

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname vpn3640
!
!
ip subnet-zero
ip cef
!
!
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!

```

```
!  
crypto ipsec transform-set strong esp-3des esp-md5-hmac  
mode transport  
!  
crypto map vpn 10 ipsec-isakmp  
set peer 14.36.88.6  
set transform-set strong  
match address 100  
!  
call rsvp-sync  
!  
!  
!  
!  
!  
!  
!  
interface Loopback0  
ip address 192.168.40.1 255.255.255.0  
!  
interface Tunnel0  
ip address 192.168.46.1 255.255.255.0  
tunnel source Ethernet0/0  
tunnel destination 14.36.88.6  
crypto map vpn  
!  
interface Ethernet0/0  
ip address 14.38.88.40 255.255.0.0  
half-duplex  
crypto map vpn  
!  
interface Ethernet0/1  
no ip address  
shutdown  
half-duplex  
!  
interface Ethernet1/0  
no ip address  
shutdown  
half-duplex  
!  
interface Ethernet1/1  
no ip address  
shutdown  
half-duplex  
!  
interface Ethernet1/2  
no ip address  
shutdown  
half-duplex  
!  
interface Ethernet1/3  
no ip address  
shutdown  
half-duplex  
!  
interface Ethernet3/0  
no ip address  
shutdown  
half-duplex  
!  
interface TokenRing3/0  
no ip address  
shutdown  
ring-speed 16
```

```

!
router eigrp 60
 network 192.168.0.0 0.0.255.255
 auto-summary
 no eigrp log-neighbor-changes
!
ip classless
ip route 0.0.0.0 0.0.0.0 14.38.1.1
ip http server
!
access-list 100 permit gre host 14.38.88.40 host 14.36.88.6
!
dial-peer cor custom
!
!
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
end
vpn3640#

```

## Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only), which allows you to view an analysis of **show** command output.

- **show ip route** Use this command to ensure that routes are learned through the 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#

```

**Note:** With an Integrated Services Adapter (ISA) card in the Cisco 7206 router, Cisco Express Forwarding (CEF) may have to be disabled for the routing updates to pass.

# Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

---

## Related Information

- [IPSec Support Page](#)
  - [Technical Support – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jan 14, 2008

Document ID: 17868

---