

GRE sobre o IPsec com o EIGRP a distribuir com um exemplo de configuração do hub e das sites remoto múltiplo

Índice

[Introdução](#)

[Pré-requisitos](#)

[Pré-requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Diagrama de Rede](#)

[Configurar](#)

[Configurar os túneis GRE](#)

[Configurar a criptografia para os túneis GRE](#)

[Configurar o protocolo de roteamento](#)

[Configurações de exemplo](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento explica como configurar o GRE sobre o roteamento do IPsec através de local de hub para vários locais remotos. O Cisco 7206 Router é o roteador de site central, a que todos os locais restantes conectam com o IPsec. O Cisco 2610, os 3620, e os 3640 Router são os roteadores remotos. Todos os locais podem alcançar a rede principal atrás do Cisco 7206 e todos locais remotos restantes através do túnel ao local principal, com as atualizações de roteamento que ocorrem automaticamente através do Enhanced Interior Gateway Routing Protocol (EIGRP).

[Pré-requisitos](#)

[Pré-requisitos](#)

Este documento foi desenvolvido e testado com uso das versões de software e hardware abaixo.

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 7206 Router que executa o Software Release 12.3(1) IK9S de Cisco IOS®

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

[Convenções](#)

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

[Diagrama de Rede](#)

Este documento utiliza a seguinte configuração de rede:

[Configurar](#)

Esse processo o orienta durante a configuração de um túnel de IPsec para rotear por um hub e vários locais remotos. O processo é separado nestas três etapas preliminares.

- [Configurar os túneis de encapsulamento de roteamento genéricos \(GRE\)](#)
- [Configurar a criptografia para os túneis GRE](#)
- [Configurar o protocolo de roteamento](#)

[Configurar os túneis GRE](#)

Siga estas etapas para configurar os túneis GRE:

1. Crie um túnel GRE de cada local remoto ao escritório principal. Configure uma interface de túnel no roteador Cisco 7206 para cada estação remota.

```
interface Tunnel0
 ip address 192.168.16.2 255.255.255.0
 tunnel source FastEthernet1/0
 tunnel destination 14.38.88.10
!
interface Tunnell
 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
```

A origem de túnel para cada túnel é a interface FastEthernet1/0 ou a interface que é a conexão de Internet. O destino do túnel é o endereço IP da interface de Internet do roteador remoto. Cada túnel deve ter um endereço IP de Um ou Mais Servidores Cisco ICM NT em um diferente, sub-rede não utilizada.

2. Configurar os túneis GRE no Cisco 2610, nos 3620, e nos 3640 Router. As configurações

são similares ao 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 roteador remoto usa sua interface local que conecta ao Internet como o origem de túnel. Os roteadores remotos correspondem aos endereços IP de destino na configuração do roteador Cisco 7206. O endereço IP de destino de túnel para cada roteador remoto corresponde ao endereço IP de Um ou Mais Servidores Cisco ICM NT da relação do Cisco 7206 Router que conecta ao Internet. O endereço IP da interface de túnel corresponde a um endereço IP na mesma sub-rede da interface de túnel do roteador Cisco 7206.

3. Assegure-se de que cada roteador remoto possa sibilhar o endereço IP de Um ou Mais Servidores Cisco ICM NT do destino de túnel e da interface de túnel correspondente do roteador principal. Também, assegure-se de que cada roteador seja processo de ping do roteador de site 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 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: Se não todo o Roteadores pode sibilar o roteador central (do hub), pesquisa defeitos cada conexão como necessário usando estas diretrizes. Pode o roteador remoto sibilar o roteador de hub do IP do público ao IP do público? Há algum dispositivo que obstrui o GRE entre os dois Roteadores? (Firewall, lista de acesso no roteador) O que os comandos show interface mostram para a interface de túnel?

[Configurar a criptografia para os túneis GRE](#)

Termine estas etapas para configurar a criptografia para os túneis GRE:

1. Se os túneis GRE vêm acima, continue com criptografia. Primeiramente, crie Listas de acesso para definir o tráfego para a criptografia. As Listas de acesso permitem o tráfego do endereço IP local em cada roteador ao endereço IP de Um ou Mais Servidores Cisco ICM NT no extremo oposto. Use o comando show version para exibir a versão de software que o Cache Engine está executando.

```
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. Configurar uma política do Internet Security Association and Key Management Protocol (ISAKMP), uma chave ISAKMP, e um IPsec transforma o grupo. A política ISAKMP, a chave e o comando transform-set ipsec devem corresponder nos dois lados de um único túnel. Não todos os túneis têm que usar a mesma política, chave, ou transforme o grupo. Neste exemplo, todos os túneis usam a mesma política, chave, e transformam o grupo para a simplicidade. **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#
```

3. Configurar o crypto map. O site central tem um número de seqüência separado para cada conexão.

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#
```

4. Aplique o crypto map. O mapa é aplicado às interfaces do tunel e física por onde saem os pacotes.

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#
```

[Configurar o protocolo de roteamento](#)

Para configurar o protocolo de roteamento, configurar todos os locais com o número de sistema autônomo e instruir o protocolo de roteamento (EIGRP) para compartilhar de rotas. Somente redes que estejam incluídas nas instruções de rede são compartilhadas com os outros roteadores pelo Routing Protocol. O número de sistema autônomo deve combinar em todo o Roteadores que participa na partilha das rotas. Neste exemplo, as redes que podem ser resumidas em uma instrução de rede são usadas para a simplicidade.

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#
```

Configurações de exemplo

Este documento usa estes exemplos de configurações:

- [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#
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **mostre a rota IP** — Use este comando assegurar-se de que as rotas sejam instruídas com o protocolo de roteamento.

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: Com um cartão do adaptador dos Serviços integrados (ISA) no Cisco 7206 Router, o Cisco Express Forwarding (CEF) pode ter que ser desabilitado para que as atualizações de roteamento passem.

[Troubleshooting](#)

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

[Informações Relacionadas](#)

- [Página de suporte do IPSec](#)
- [Suporte Técnico - Cisco Systems](#)