

Configurando o roteamento redundante no VPN 3000 concentrator

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações do Roteador](#)

[Configuração de concentrador VPN 3080](#)

[Configuração de concentrador VPN 3060a](#)

[Configuração de concentrador VPN 3030b](#)

[Verificar](#)

[Troubleshooting](#)

[Falha simulada](#)

[Que pode ir mal?](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento descreve como configurar um failover de VPN redundante se um local remoto perde sua VPN 3000 concentrator ou conectividade de Internet. Neste exemplo, supõe que a rede corporativa situada atrás do VPN 3030B usa o Open Shortest Path First (OSPF) como seu protocolo do roteamento padrão.

Note: Quando você redistribui entre protocolos de roteamento, você pode formar um loop de roteamento que possa causar o problema na rede. O OSPF é usado neste exemplo, mas não é o único protocolo de roteamento que pode ser usado.

O objetivo deste exemplo é ter o uso da rede de 192.168.1.0 o túnel vermelho (sob circunstâncias normal de operação), descrito na seção do diagrama da rede, para alcançar 192.168.3.x. Se o túnel, o concentrador VPN, ou as gotas ISP, então a rede the192.168.3.0 são instruídos sobre um protocolo de roteamento dinâmico sobre o túnel verde. Também, a Conectividade não é perdida ao local de 192.168.3.0. Uma vez que a edição é resolved, o tráfego reverte automaticamente de volta ao túnel vermelho.

Note: O RASGO tem um aging timer três minuto antes que permita que uma rota nova seja aceita sobre uma rota inválida. Também, supõe que os túneis estão criados e que o tráfego pode passar entre os pares.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Roteadores Cisco 3620 e 3640
- Concentrador Cisco VPN 3080 - Versão: Cisco Systems, versão do concentrador 4.7 Inc. /VPN 3000
- Concentrador Cisco VPN 3060 - Versão: Cisco Systems, Inc. /VPN 3000 Concentrator Series da versão 4.7
- Concentrador Cisco VPN 3030 - Versão: Cisco Systems, Inc. /VPN 3000 Concentrator Series da versão 4.7

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 a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Note: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes [registrados](#)).

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Os traços azuis indicam que o OSPF está permitido de VPN 3030b ao RTR-3640 e ao RTR-3620.

Os traços verdes indicam que o RIPv2 está permitido de VPN privado 3060a ao RTR-3620, ao RTR-3640, e a VPN privado 3030b.

O RIPv2 é permitido igualmente nos túneis vermelhos e verdes VPN porque a descoberta da rede é permitida. Não é necessário permitir o RASGO na interface confidencial VPN 3080. Não há igualmente nenhum RASGO na rede 192.168.4.x porque todas as rotas são aprendidas pelo OSPF sobre este link.

Note: Os PC nas redes 192.168.2.x e 192.168.3.x precisam de ter seus gateways padrão que apontam ao Roteadores e não aos concentradores VPN. Permita que o Roteadores decida em onde distribuir os pacotes.

Configurações do Roteador

Este documento usa estas configurações de roteador:

- [Roteador 3620](#)
- [Roteador 3640](#)

Roteador 3620

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

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

 redistribute rip subnets route-map block192.168.1.0
!--- To enable the OSPF process for the interfaces that
are included !--- in the 192.168.x.x networks: network
192.168.0.0 0.0.255.255 area 0 !--- Since RIP's default
admin distance is 120 and OSPF's is 110, !--- make RIP a
preferable metric for communications !--- over the
"backup" network. !--- Change any learned OSPF routes
from neighbor 192.168.4.1 !--- to an admin distance of
130. distance 130 192.168.4.1 0.0.0.0 ! !--- To enable
RIP on the Ethernet 1/0 interface and set it to !--- use
```

```
version 2: router rip version 2 network 192.168.3.0 ! ip
classless ! ! access-list 1 deny 192.168.1.0 0.0.0.255
access-list 1 permit any route-map block192.168.1.0
permit 10 match ip address 1 ! line con 0 exec-timeout 0
0 line aux 0 line vty 0 4 ! end
```

Roteador 3640

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

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

[Configuração de concentrador VPN 3080](#)

[LAN para LAN VPN 3080 a VPN 3030b](#)

Selecione a **configuração > o Tunelamento e a Segurança > o IPsec > o LAN para LAN do IPsec**. Desde que a descoberta automática de rede é usada, não há nenhuma necessidade de completar as lista da rede remota e local.

Note: Os concentradores VPN que executam a versão de software 3.1 e mais adiantado têm uma caixa de verificação para a descoberta automática. A versão de software 3.5 (usada no VPN 3080) usa um menu suspenso, tal como esse representado aqui.

[LAN para LAN VPN 3080 a VPN 3060a](#)

Selecione a **configuração > o Tunelamento e a Segurança > o IPsec > o LAN para LAN do IPsec**. Desde que a descoberta automática de rede é usada, não há nenhuma necessidade de completar as lista da rede remota e local.

Note: Os concentradores VPN que executam a versão de software 3.1 e mais adiantado têm uma caixa de verificação para a descoberta automática. A versão de software 3.5 (usada no VPN 3080) usa um menu suspenso, tal como esse representado aqui.

[Configuração de concentrador VPN 3060a](#)

[LAN para LAN VPN 3060a a VPN 3080](#)

Selecione a **configuração > o Tunelamento e a Segurança > o IPsec > o LAN para LAN do IPsec**.

Note: Há uma caixa de verificação no VPN 3060 para a descoberta automática de rede em vez do menu suspenso como na versão de software 3.5 e mais atrasado.

[Permita o RASGO de passar as rotas aprendidas de túnel ao 3620 Router VPN](#)

Selecione o **configuração > interfaces > privado > RASGO**. Mude o menu suspenso ao **RIPv2 somente** e o clique **aplica-se**. Selecione então o **Configuration > System > Tunneling Protocols > IPsec > LAN para LAN**.

Note: O padrão é RASGO de partida, e é desabilitado para a interface confidencial.

[Configuração de concentrador VPN 3030b](#)

[LAN para LAN VPN 3030b a VPN 3080](#)

Selecione a **configuração > o Tunelamento e a Segurança > o IPsec > o LAN para LAN**.

[Permita o RASGO de passar as rotas aprendidas de túnel ao 3640 Router VPN](#)

Siga as etapas alistadas mais cedo neste documento para o [concentrador VPN 3060a](#).

[Permita o OSPF de passar as rotas Backbone-instruídas ao concentrador VPN 3030b](#)

Selecione o **Configuração > Sistema > IP routing > OSPF** e incorpore o Router ID.

```
rtr-3640#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.4.2	1	FULL/DR	00:00:39	192.168.4.2	Ethernet0/1
<i>!--- For troubleshooting purposes, it helps to make the router ID the !--- IP address of the private interface.</i>					
192.168.2.1	1	FULL/BDR	00:00:36	192.168.2.1	Ethernet0/0

O ID da área precisa de combinar o ID no fio. Desde que a área neste exemplo é 0, é representada por 0.0.0.0. Também, verifique a caixa da **possibilidade OSPF** e o clique **aplica-se**.

Certifique-se de que seus temporizadores OSPF combinam aquele do roteador. Para verificar os temporizadores de roteadores, use o comando **show ip ospf interface <interface name>**.

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

Para obter mais informações sobre do OSPF, refira o [RFC 1247](#) .

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.

Esta saída do comando mostra tabelas de roteamento exatas.

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

Gateway of last resort is not set

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

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

Gateway of last resort is not set

    172.18.0.0/24 is subnetted, 1 subnets
```

```

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

```

Esta é a tabela de roteamento de concentrador VPN 3080 em circunstâncias normais.

As redes 192.168.2.x e 192.168.3.x são ambas instruídas através dos túneis 172.18.124.132 e 172.18.124.131 VPN, respectivamente. A rede 192.168.4.x é instruída através do túnel de 172.18.124.132 porque os anúncios de OSPF do roteador são colocados na tabela de roteamento do concentrador VPN 3030b. Então a tabela de roteamento anuncia a rede para fora aos pares remotos VPN.

Esta é a tabela de roteamento de concentrador VPN 3030b em circunstâncias normais.

Os destaques vermelhos da caixa que a rede 192.168.1.x é instruída do túnel VPN. Os destaques da caixa azul que as redes 192.168.3.x e 192.168.4.x são instruídas com o processo de OSPF do núcleo.

Esta é a tabela de roteamento de concentrador VPN 3060a em circunstâncias normais.

A rede 192.168.1.x é a única rede aqui, e pode ser alcançada através do túnel VPN. Não há nenhuma rede de 192.168.2.0 desde que nenhum processo (tal como o RASGO) passa ao longo dessa rota. Não há nada perdido enquanto os PC na rede 192.168.3.x não apontam seu gateway padrão ao concentrador VPN. Você pode sempre adicionar uma rota estática se você escolher. Contudo, para este exemplo, o concentrador VPN próprio não precisa de alcançar a rede de 192.168.2.0.

Troubleshooting

Falha simulada

Esta é uma falha simulada na configuração. Se você remove o filtro à interface pública, a seguir o túnel VPN deixa cair. Isto causa a rota para 192.168.1.0 aprendido através do túnel deixar cair também. Toma aproximadamente três minutos para que o processo do RASGO remova para fora a rota. Conseqüentemente, você pode potencialmente ter uma indisponibilidade de três-minuto até a rota cronometra-se para fora.

Uma vez que a rota RIP expira, a tabela de roteamento nova no Roteadores parece similar a esta:

```
rtr-3620#show ip route
```

```

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

```

Gateway of last resort is not set

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

Que pode ir mal?

Se você esquece adicionar na mudança da distância administrativa a 130, a seguir você pode possivelmente ver esta saída. Note que ambos os túneis VPN estão acima.

Concentrador VPN 3080

Note: Esta é a versão NON-gráfica da interface do utilizador (GUI) da tabela de roteamento.

```
rtr-3620#show ip route
```

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

Gateway of last resort is not set

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

Para obter à rede de 192.168.3.0, as necessidades da rota de atravessar 172.18.124.131. Contudo, a tabela de roteamento em mostras do RTR-3620:

```
rtr-3620#show ip route
```

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

Gateway of last resort is not set

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


00:03:16, Ethernet1/1

O 192.168.2.0/24 [110/20] via 192.168.4.1, 00:03:16, Ethernet1/1

C 192.168.3.0/24 is directly connected, Ethernet1/0

Para receber de volta à rede de 192.168.1.0, as necessidades da rota de atravessar a rede do backbone 192.168.4.x.

O tráfego ainda trabalha desde que a descoberta automática gerencie a informação da associação da segurança adequada (SA) no concentrador VPN 3030b. Por exemplo:

```
rtr-3620#show ip route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

172.18.0.0/24 is subnetted, 1 subnets

O E2 172.18.124.0 [110/20] via 192.168.4.1, 00:03:16, Ethernet1/1

C 192.168.4.0/24 is directly connected, Ethernet1/1

!--- This is an example of asymmetric routing. O E2 192.168.1.0/24 [110/20] via 192.168.4.1, 00:03:16, Ethernet1/1

O 192.168.2.0/24 [110/20] via 192.168.4.1, 00:03:16, Ethernet1/1

C 192.168.3.0/24 is directly connected, Ethernet1/0

Mesmo que a tabela de roteamento diga o par deve ser 172.18.124.131, o SA real (fluxo de tráfego) é através do concentrador VPN 3030b em 172.18.124.132. A tabela SA toma a precedência sobre a tabela de rota. Somente a examinação precisa da tabela de rota e da tabela SA no concentrador VPN 3060a mostra que o tráfego não flui no sentido correto.

[Informações Relacionadas](#)

- [Página de suporte do Cisco VPN 3000 Series Concentrator](#)
- [Página de suporte do IPsec](#)
- [Suporte Técnico - Cisco Systems](#)