

Configurando o roteamento redundante no VPN 3000 Concentrator

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações do Roteador](#)

[Configuração do VPN 3080 Concentrator](#)

[Configuração do VPN 3060a Concentrator](#)

[Configuração do VPN 3030b Concentrator](#)

[Verificar](#)

[Troubleshoot](#)

[Falha simulada](#)

[O que pode dar errado?](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento descreve como configurar um failover de VPN redundante se um site remoto perder seu VPN 3000 Concentrator ou conectividade com a Internet. Neste exemplo, suponha que a rede corporativa localizada atrás do VPN 3030B use o OSPF (Open Shortest Path First) como seu protocolo de roteamento padrão.

Observação: ao redistribuir entre protocolos de roteamento, você pode formar um loop de roteamento que pode causar problemas 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 fazer com que a rede 192.168.1.0 use o túnel vermelho (sob circunstâncias normais de operação), representado na seção Diagrama de Rede, para alcançar 192.168.3.x. Se o túnel, o VPN Concentrator ou o ISP cair, a rede 192.168.3.0 será aprendida sobre um protocolo de roteamento dinâmico sobre o túnel verde. Além disso, a conectividade não é perdida para o site 192.168.3.0. Quando o problema for resolvido, o tráfego reverterá automaticamente para o túnel vermelho.

Observação: o RIP tem um temporizador de envelhecimento de três minutos antes de permitir que uma nova rota seja aceita em uma rota inválida. Além disso, suponha que os túneis sejam criados e que o tráfego possa passar entre os pares.

Prerequisites

Requirements

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, Inc./VPN 3000 Concentrator versão 4.7
- Concentrador Cisco VPN 3060 - Versão: Cisco Systems, Inc./VPN 3000 Concentrator Series versão 4.7
- Cisco VPN 3030 Concentrator - Versão: Cisco Systems, Inc./VPN 3000 Concentrator Series versão 4.7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

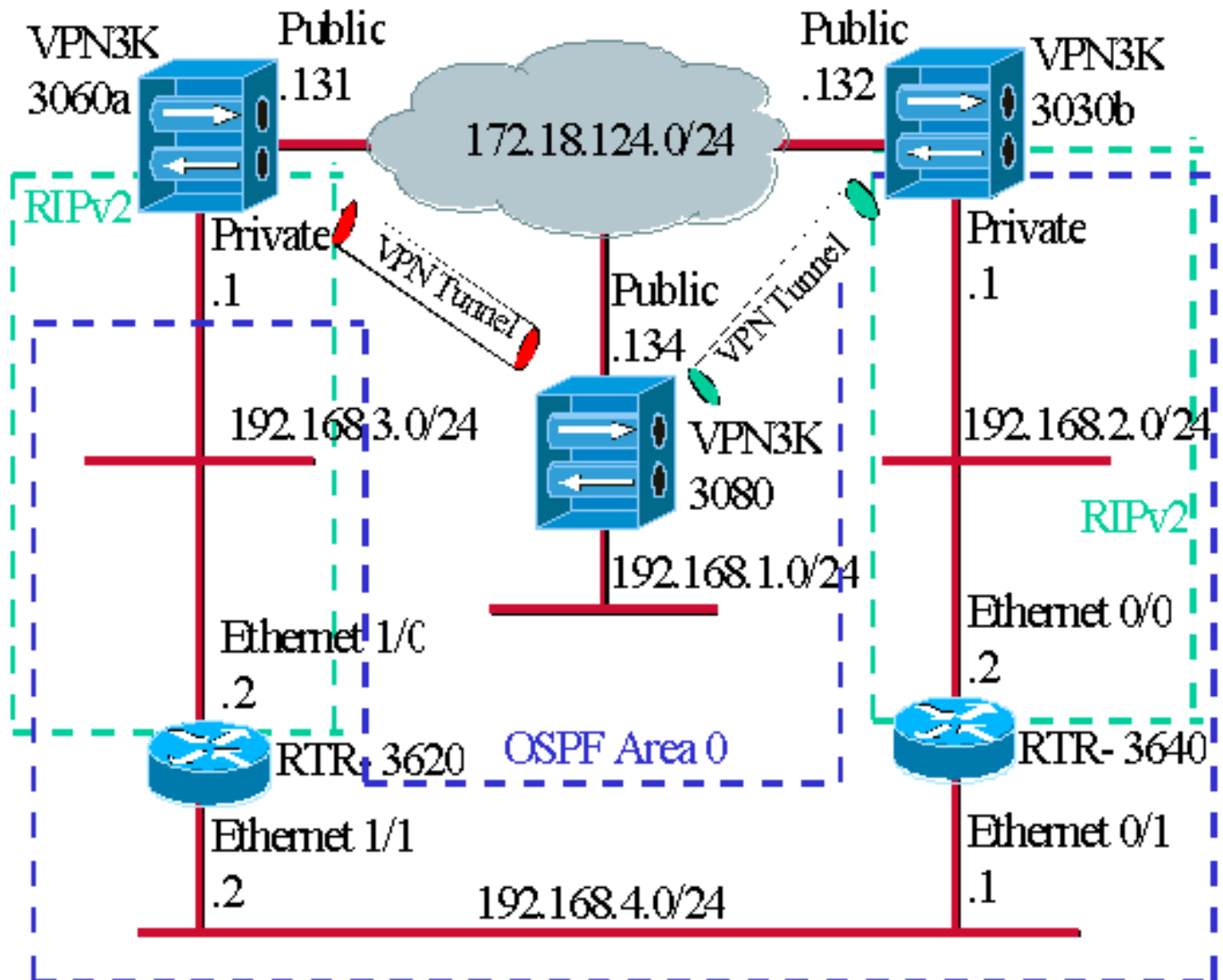
Configurar

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

Observação: para encontrar informações adicionais sobre os comandos usados neste documento, use a [ferramenta Command Lookup Tool](#) (somente clientes [registrados](#)).

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Os traços azuis indicam que o OSPF está ativado do VPN 3030b para o RTR-3640 e do RTR-3620.

Os traços verdes indicam que o RIPv2 está ativado do VPN 3060a privado para o RTR-3620, o RTR-3640 e o VPN 3030b privado.

O RIPv2 também está ativado nos túneis VPN vermelhos e verdes porque a descoberta de rede está habilitada. Não é necessário ativar o RIP na interface privada do VPN 3080. Também não há RIP na rede 192.168.4.x porque todas as rotas são aprendidas pelo OSPF sobre esse link.

Observação: os PCs nas redes 192.168.2.x e 192.168.3.x precisam ter seus gateways padrão apontando para os roteadores e não para os VPN Concentrators. Permita que os roteadores decidam para onde rotear 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 do VPN 3080 Concentrator

LAN-to-LAN VPN 3080 a VPN 3030b

Selecione **Configuration > Tunneling and Security > IPSec > IPSec LAN-to-LAN**. Como a descoberta automática de rede é usada, não há necessidade de preencher as listas de rede local e remota.

Observação: os VPN Concentrators que executam o software versão 3.1 e anterior têm uma caixa de seleção para descoberta automática. A versão de software 3.5 (usada no VPN 3080) usa um menu suspenso, como o mostrado aqui.

Add a new IPSec LAN-to-LAN connection.

<p>Enable <input type="checkbox"/></p> <p>Name <input type="text" value="3080-3030b"/></p> <p>Interface <input type="text" value="Ethernet 2 (Public) (172.18.124.134)"/></p> <p>Connection Type <input type="text" value="Bi-directional"/></p> <p>Peers</p> <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> <p>172.18.124.132</p> </div> <p>Digital Certificate <input type="text" value="None (Use Preshared Keys)"/></p> <p>Certificate Transmission <input type="radio"/> Entire certificate chain <input type="radio"/> Identity certificate only</p> <p>Preshared Key <input type="text"/></p> <p>Authentication <input type="text" value="ESP/MD5/HMAC-128"/></p> <p>Encryption <input type="text" value="3DES-168"/></p> <p>IKE Proposal <input type="text" value="IKE-3DES-MD5"/></p> <p>Filter <input type="text" value="-None-"/></p> <p>Bandwidth Policy <input type="text" value="-None-"/></p> <p>Routing <input type="text" value="Network Autodiscovery"/></p>	<p>Check to enable this LAN-to-LAN connection.</p> <p>Enter the name for this LAN-to-LAN connection.</p> <p>Select the interface for this LAN-to-LAN connection.</p> <p>Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> may have multiple peers specified below.</p> <p>Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses, one IP address per line.</p> <p>Select the digital certificate to use.</p> <p>Choose how to send the digital certificate to the IKE peer.</p> <p>Enter the preshared key for this LAN-to-LAN connection.</p> <p>Specify the packet authentication mechanism to use.</p> <p>Specify the encryption mechanism to use.</p> <p>Select the IKE Proposal to use for this LAN-to-LAN connection.</p> <p>Choose the filter to apply to the traffic that is tunneled through the LAN connection, under NAT Transparency.</p> <p>Choose the bandwidth policy to apply to this LAN-to-LAN connection.</p> <p>Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.</p>
<p>Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.</p> <p>Network List <input type="text" value="Use IP Address/Wildcard-mask below"/> Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.</p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p> <p>Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.</p>	
<p>Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.</p> <p>Network List <input type="text" value="Use IP Address/Wildcard-mask below"/> Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.</p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p> <p>Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.</p>	
<p><input type="button" value="Add"/> <input type="button" value="Cancel"/></p>	

[LAN-to-LAN VPN 3080 a VPN 3060a](#)

Selezione Configuration > Tunneling and Security > IPSec > IPSec LAN-to-LAN. Como a

descoberta automática de rede é usada, não há necessidade de preencher as listas de rede local e remota.

Observação: os VPN Concentrators que executam o software versão 3.1 e anterior têm uma caixa de seleção para descoberta automática. A versão de software 3.5 (usada no VPN 3080) usa um menu suspenso, como o mostrado aqui.

Add a new IPsec LAN-to-LAN connection.

<p>Enable <input type="checkbox"/></p> <p>Name <input type="text" value="3080-3060a"/></p> <p>Interface <input type="text" value="Ethernet 2 (Public) (172.18.124.134)"/></p> <p>Connection Type <input type="text" value="Bi-directional"/></p> <p>Peers</p> <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> <p>172.18.124.131</p> </div> <p>Digital Certificate <input type="text" value="None (Use Preshared Keys)"/></p> <p>Certificate Transmission <input type="radio"/> Entire certificate chain <input type="radio"/> Identity certificate only</p> <p>Preshared Key <input type="text"/></p> <p>Authentication <input type="text" value="ESP/MD5/HMAC-128"/></p> <p>Encryption <input type="text" value="3DES-168"/></p> <p>IKE Proposal <input type="text" value="IKE-3DES-MD5"/></p> <p>Filter <input type="text" value="-None-"/></p> <p>IPsec NAT-T <input type="checkbox"/></p> <p>Bandwidth Policy <input type="text" value="-None-"/></p> <p>Routing <input type="text" value="Network Autodiscovery"/></p>	<p>Check to enable this LAN-to-LAN connection.</p> <p>Enter the name for this LAN-to-LAN connection.</p> <p>Select the interface for this LAN-to-LAN connection.</p> <p>Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.</p> <p>Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses, one IP address per line.</p> <p>Select the digital certificate to use.</p> <p>Choose how to send the digital certificate to the IKE peer.</p> <p>Enter the preshared key for this LAN-to-LAN connection.</p> <p>Specify the packet authentication mechanism to use.</p> <p>Specify the encryption mechanism to use.</p> <p>Select the IKE Proposal to use for this LAN-to-LAN connection.</p> <p>Choose the filter to apply to the traffic that is tunneled through this LAN connection.</p> <p>Check to let NAT-T compatible IPsec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPsec over NAT Transparency.</p> <p>Choose the bandwidth policy to apply to this LAN-to-LAN connection.</p> <p>Choose the routing mechanism to use. Parameters below are ignored. Network Autodiscovery is chosen.</p>
---	--

Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

<p>Network List <input type="text" value="Use IP Address/Wildcard-mask below"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	<p>Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.</p> <p>Note: Enter a <i>wildcard mask</i>, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.</p>
---	---

Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

<p>Network List <input type="text" value="Use IP Address/Wildcard-mask below"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	<p>Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.</p> <p>Note: Enter a <i>wildcard mask</i>, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match.</p>
---	--

Configuração do VPN 3060a Concentrador

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

Selecione **Configuration > Tunneling and Security > IPSec > IPSec LAN-to-LAN**.

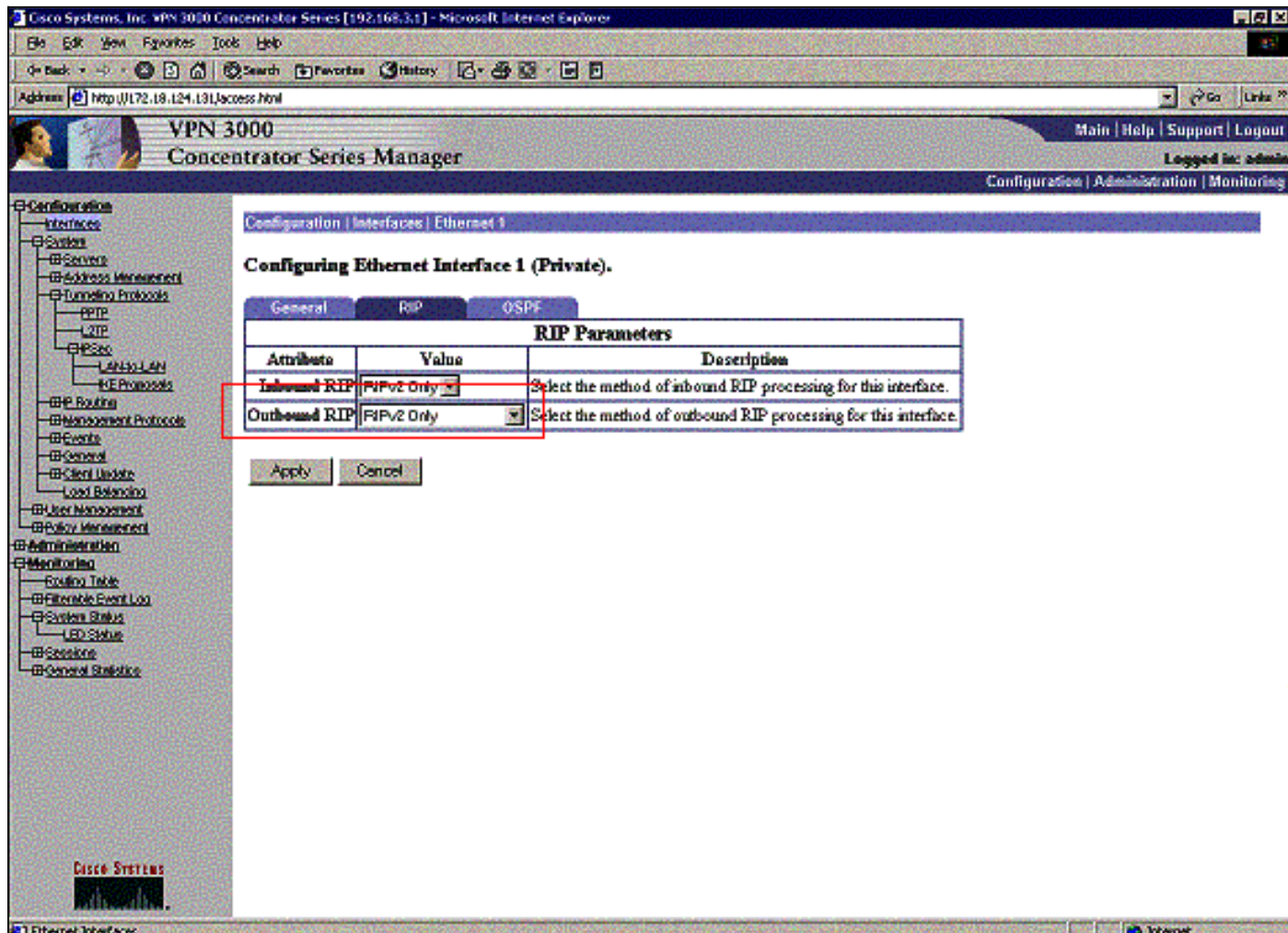
Observação: há uma caixa de seleção no VPN 3060 para a descoberta automática de rede em vez do menu suspenso como na versão de software 3.5 e posterior.

Configuration Tunneling and Security IPSec LAN-to-LAN Add	
Add a new IPSec LAN-to-LAN connection.	
Enable <input type="checkbox"/>	Check to enable this LAN-to-LAN connection.
Name <input type="text" value="3060a-3080"/>	Enter the name for this LAN-to-LAN connection.
Interface <input type="text" value="Ethernet 2 (Public) (172.18.124.131)"/>	Select the interface for this LAN-to-LAN connection.
Connection Type <input type="text" value="Bi-directional"/>	Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.
Peers <input type="text" value="172.18.124.134"/>	Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses, one IP address per line.
Digital Certificate <input type="text" value="None (Use Preshared Keys)"/>	Select the digital certificate to use.
Certificate Transmission <input type="radio"/> Entire certificate chain <input type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
Preshared Key <input type="text"/>	Enter the preshared key for this LAN-to-LAN connection.
Authentication <input type="text" value="ESP/MD5/HMAC-128"/>	Specify the packet authentication mechanism to use.
Encryption <input type="text" value="3DES-168"/>	Specify the encryption mechanism to use.
IKE Proposal <input type="text" value="IKE-3DES-MD5"/>	Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter <input type="text" value="-None-"/>	Choose the filter to apply to the traffic that is tunneled through this LAN connection.
IPSec NAT-T <input type="checkbox"/>	Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over under NAT Transparency.
Bandwidth Policy <input type="text" value="-None-"/>	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Routing <input type="text" value="Network Autodiscovery"/>	Choose the routing mechanism to use. Parameters below are ignored. Network Autodiscovery is chosen.
Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.	
Network List <input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address <input type="text"/>	Note: Enter a <i>wildcard mask</i> , which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask <input type="text"/>	
Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.	
Network List <input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address <input type="text"/>	Note: Enter a <i>wildcard mask</i> , which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match.
Wildcard Mask <input type="text"/>	

[Ative o RIP para passar as rotas aprendidas pelo túnel para o roteador VPN 3620](#)

Selecione **Configuration > Interfaces > Private > RIP**. Altere o menu suspenso para somente **RIPv2** e clique em **Aplicar**. Em seguida, selecione **Configuration > System > Tunneling Protocols > IPSec > LAN-to-LAN**.

Observação: o padrão é o RIP de saída e é desativado para a interface privada.



The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The left sidebar contains a navigation tree with categories like Configuration, System, Security, and Administration. The main content area is titled "Configuring Ethernet Interface 1 (Private)" and has tabs for General, RIP, and OSPF. The RIP Parameters table is highlighted with a red box:

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

Below the table are "Apply" and "Cancel" buttons.

[Configuração do VPN 3030b Concentrator](#)

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

Selecione **Configuration > Tunneling and Security > IPSec > LAN-to-LAN**.

Add a new IPSec LAN-to-LAN connection.

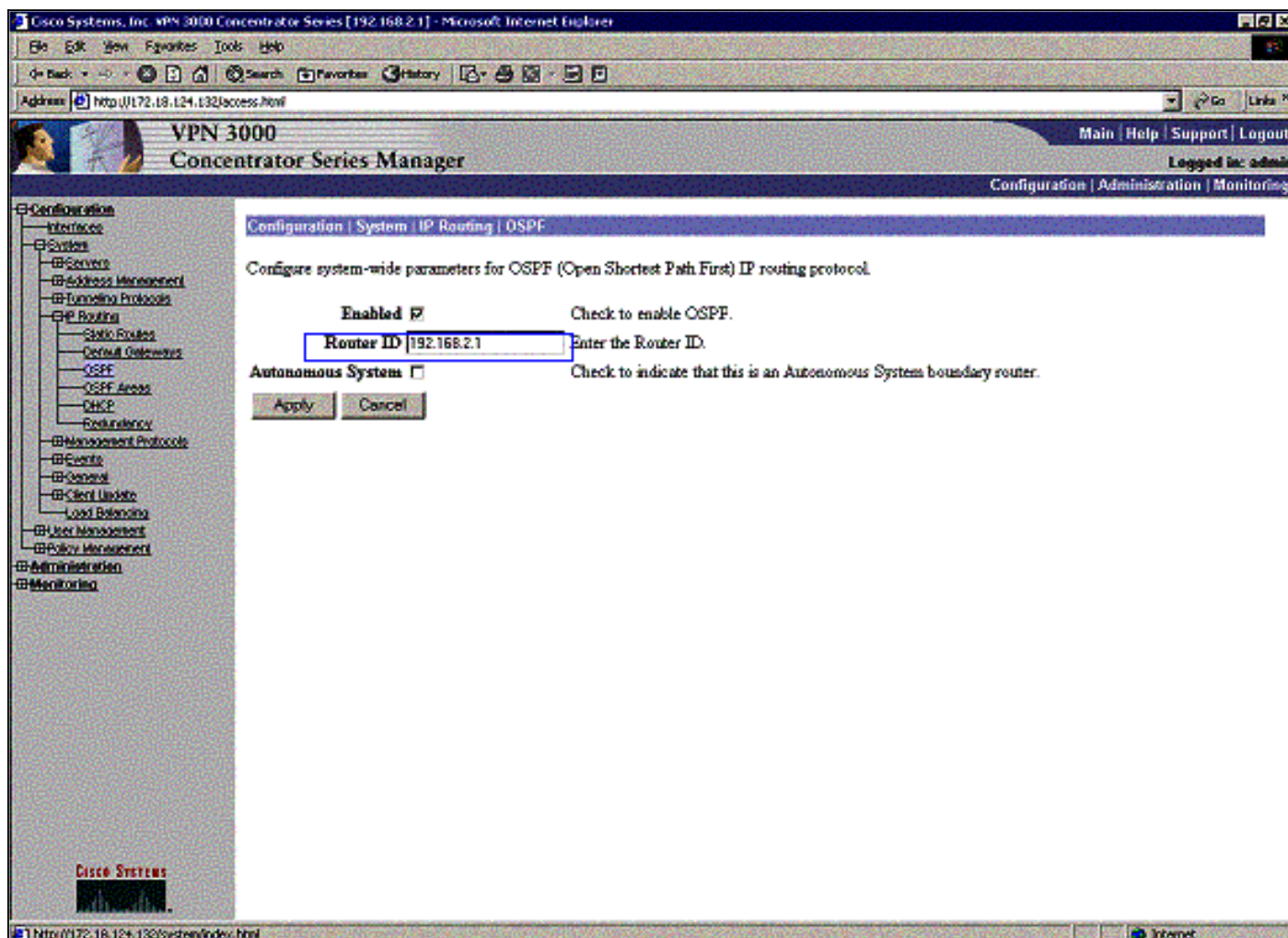
<p>Enable <input type="checkbox"/></p> <p>Name <input type="text" value="3030B-3080"/></p> <p>Interface <input type="text" value="Ethernet 2 (Public) (172.18.124.132)"/></p> <p>Connection Type <input type="text" value="Bi-directional"/></p> <p>Peers</p> <div style="border: 1px solid black; padding: 5px; min-height: 100px;"> <p>172.18.124.134</p> </div> <p>Digital Certificate <input type="text" value="None (Use Preshared Keys)"/></p> <p>Certificate Transmission <input type="radio"/> Entire certificate chain <input type="radio"/> Identity certificate only</p> <p>Preshared Key <input type="text"/></p> <p>Authentication <input type="text" value="ESP/MD5/HMAC-128"/></p> <p>Encryption <input type="text" value="3DES-168"/></p> <p>IKE Proposal <input type="text" value="IKE-3DES-MD5"/></p> <p>Filter <input type="text" value="-None-"/></p> <p>IPSec NAT-T <input type="checkbox"/></p> <p>Bandwidth Policy <input type="text" value="-None-"/></p> <p>Routing <input type="text" value="Network Autodiscovery"/></p>	<p>Check to enable this LAN-to-LAN connection.</p> <p>Enter the name for this LAN-to-LAN connection.</p> <p>Select the interface for this LAN-to-LAN connection.</p> <p>Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.</p> <p>Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses, one IP address per line.</p> <p>Select the digital certificate to use.</p> <p>Choose how to send the digital certificate to the IKE peer.</p> <p>Enter the preshared key for this LAN-to-LAN connection.</p> <p>Specify the packet authentication mechanism to use.</p> <p>Specify the encryption mechanism to use.</p> <p>Select the IKE Proposal to use for this LAN-to-LAN connection.</p> <p>Choose the filter to apply to the traffic that is tunneled through this LAN connection.</p> <p>Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over under NAT Transparency.</p> <p>Choose the bandwidth policy to apply to this LAN-to-LAN connection.</p> <p>Choose the routing mechanism to use. Parameters below are ignored. Network Autodiscovery is chosen.</p>
<p>Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.</p> <p>Network List <input type="text" value="Use IP Address/Wildcard-mask below"/> Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.</p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p> <p>Note: Enter a <i>wildcard mask</i>, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to use. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.</p>	
<p>Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.</p> <p>Network List <input type="text" value="Use IP Address/Wildcard-mask below"/> Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.</p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p> <p>Note: Enter a <i>wildcard mask</i>, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to use.</p>	

[Ative o RIP para passar as rotas aprendidas pelo túnel para o roteador VPN 3640](#)

Siga as etapas listadas anteriormente neste documento para o [VPN 3060a Concentrador](#).

[Habilite o OSPF para passar as rotas aprendidas por backbone para o VPN 3030b Concentrador](#)

Selecione Configuration > System > IP Routing > OSPF e insira o ID do roteador.



```
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 corresponder ao ID no fio. Como a área neste exemplo é 0, ela é representada por 0.0.0.0. Além disso, marque a caixa **Ativar OSPF** e clique em **Aplicar**.

Configuration | Interfaces | Ethernet 1

Configuring Ethernet Interface 1 (Private).

General RIP OSPF

OSPF Parameters		
Attribute	Value	Description
OSPF Enabled	<input checked="" type="checkbox"/>	Check to enable OSPF on this interface.
OSPF Area ID	0.0.0.0	Enter the OSPF Area ID for this interface. The format is the same as an IP address.
OSPF Priority	1	Enter the OSPF Priority for this interface.
OSPF Metric	1	Enter the OSPF Metric for this interface.
OSPF Retransmit Interval	5	Enter the OSPF Retransmit Interval for this interface.
OSPF Hello Interval	10	Enter the OSPF Hello Interval for this interface.
OSPF Dead Interval	40	Enter the OSPF Dead Interval for this interface.
OSPF Transit Delay	1	Enter the OSPF Transit Delay for this interface.
OSPF Authentication	None	Select the OSPF Authentication method to use.
OSPF Password		Enter the OSPF Password when Simple Password or MD5 is selected above.

Apply Cancel

Verifique se os temporizadores OSPF correspondem aos do roteador. Para verificar os temporizadores dos roteadores, use o comando **show ip ospf interface <nome da interface>**.

```
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 OSPF, consulte [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 de comando mostra tabelas de roteamento precisas.

```
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 do VPN 3080 Concentrator em circunstâncias normais.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The browser title is "Cisco Systems, Inc. VPN 3000 Concentrator [192.168.1.1] - Microsoft Internet Explorer". The address bar shows "http://172.18.124.134/access.html". The page title is "VPN 3000 Concentrator Series Manager". The navigation menu on the left includes Configuration, Administration, and Monitoring. The Monitoring section is expanded, showing Routing Table, Filterable Event Log, System Status, Sessions, and Statistics. The Routing Table page is displayed, showing a "Clear Routes" button and "Valid Routes: 6". The routing table is as follows:

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	RIP	19	2
192.168.3.0	255.255.255.0	172.18.124.131	2	RIP	28	2
192.168.4.0	255.255.255.0	172.18.124.132	2	RIP	19	9

As redes 192.168.2.x e 192.168.3.x são aprendidas através dos túneis VPN 172.18.124.132 e 172.18.124.131, respectivamente. A rede 192.168.4.x é aprendida através do túnel 172.18.124.132 porque os anúncios OSPF do roteador são colocados na tabela de roteamento do VPN 3030b Concentrator. Em seguida, a tabela de roteamento anuncia a rede para os peers VPN remotos.

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

Monitoring | Routing Table

Thursday, 08 November 2001 13:25:22

Refresh

Clear Routes

Valid Routes: 6

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	172.18.124.134	2	RIP	24	2
192.168.2.0	255.255.255.0	0.0.0.0	1	Local	0	1
192.168.3.0	255.255.255.0	192.168.2.2	1	OSPF	0	21
192.168.4.0	255.255.255.0	192.168.2.2	1	OSPF	0	11

A caixa vermelha destaca que a rede 192.168.1.x é aprendida do túnel VPN. A caixa azul destaca que as redes 192.168.3.x e 192.168.4.x são aprendidas através do processo principal do OSPF.

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

VPN 3000 Concentrator Series Manager

Monitoring | Routing Table

Thursday, 08 November 2001 13:33:17

Clear Routes

Valid Routes: 4

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	172.18.124.134	2	RIP	12	2
192.168.3.0	255.255.255.0	0.0.0.0	1	Local	0	1

A rede 192.168.1.x é a única rede aqui e pode ser acessada através do túnel VPN. Não há rede 192.168.2.0, pois nenhum processo (como o RIP) passa por essa rota. Não há nada perdido enquanto os PCs na rede 192.168.3.x não apontarem seu gateway padrão para o VPN Concentrator. Você sempre pode adicionar uma rota estática se escolher. No entanto, para esse exemplo, o VPN Concentrator em si não precisa acessar a rede 192.168.2.0.

Troubleshoot

Falha simulada

Essa é uma falha simulada na configuração. Se você remover o filtro para a interface pública, o túnel VPN será descartado. Isso faz com que a rota para 192.168.1.0 aprendida através do túnel também caia. O processo RIP leva aproximadamente três minutos para eliminar a rota. Portanto, é possível ter uma interrupção de três minutos até que a rota atinja o tempo limite.

VPN 3000 Concentrator Series Manager

Monitoring | Routing Table

Thursday, 08 November 2001 13:47:35

Refresh

Clear Routes

Valid Routes: 3

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
192.168.3.0	255.255.255.0	0.0.0.0	1	Local	0	1

Quando a rota RIP expira, a nova tabela de roteamento nos roteadores é semelhante 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
```

O que pode dar errado?

Se você esquecer de adicionar a distância do administrador como 130, é possível ver essa saída. Observe que ambos os túneis VPN estão ativados.

Concentrador VPN 3080

Observação: esta é a versão da interface gráfica do usuário (GUI) da tabela de roteamento.

Monitor -> 1

Routing Table

Number of Routes: 6

IP Address	Mask	Next Hop	Intf	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	RIP	10	2
192.168.3.0	255.255.255.0	172.18.124.131	2	RIP	2	2
192.168.4.0	255.255.255.0	172.18.124.132	2	RIP	10	9

Para chegar à rede 192.168.3.0, a rota precisa passar por 172.18.124.131. No entanto, a tabela de roteamento no RTR-3620 mostra:

```
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 voltar à rede 192.168.1.0, a rota precisa passar pela rede de backbone 192.168.4.x.

O tráfego ainda funciona desde que a descoberta automática gera as informações de associação de segurança (SA) apropriadas no VPN 3030b Concentrator. Por exemplo:

Routing -> 1

Routing Table

Number of Routes: 6

IP Address	Mask	Next Hop	Intf	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	RIP	28	2
192.168.3.0	255.255.255.0	172.18.124.131	2	RIP	20	2

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring

IKE Sessions: 1
IPSec Sessions: 2

IKE Session			
Session ID	1	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 2 (1024-bit)
Authentication Mode	Pre-Shared Keys	IKE Negotiation Mode	Main
Rekey Time Interval	86400 seconds		

IPSec Session			
Session ID	2	Remote Address	172.18.124.132
Local Address	172.18.124.134	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Encapsulation Mode	Tunnel
Rekey Time Interval	28800 seconds		
Bytes Received	222048	Bytes Transmitted	129584

IPSec Session			
Session ID	3	Remote Address	192.168.3.0/0.0.0.255
Local Address	192.168.1.0/0.0.0.255	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Encapsulation Mode	Tunnel
Rekey Time Interval	28800 seconds		
Bytes Received	280	Bytes Transmitted	280

Navigation Menu:

- Configuration
 - Administration
 - Administer Sessions
 - Software Update
 - System Reboot
 - Ping
 - Monitoring Refresh
 - Access Rights
 - File Management
 - Certificate Management
- Monitoring
 - Routing Table
 - Filterable Event Log
 - System Status
 - Sessions
 - Protocols
 - SEPs
 - Encryption
 - Top Ten Lists
 - Statistics

Embora a tabela de roteamento diga que o peer deve ser 172.18.124.131, o SA (fluxo de tráfego) real é através do VPN 3030b Concentrator em 172.18.124.132. A tabela SA tem precedência sobre a tabela de rotas. Apenas um exame mais detalhado da tabela de rotas e da tabela SA no VPN 3060a Concentrator mostra que o tráfego não flui na direção correta.

Informações Relacionadas

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