Configurando o roteamento redundante no VPN 3000 Concentrator

Contents

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.

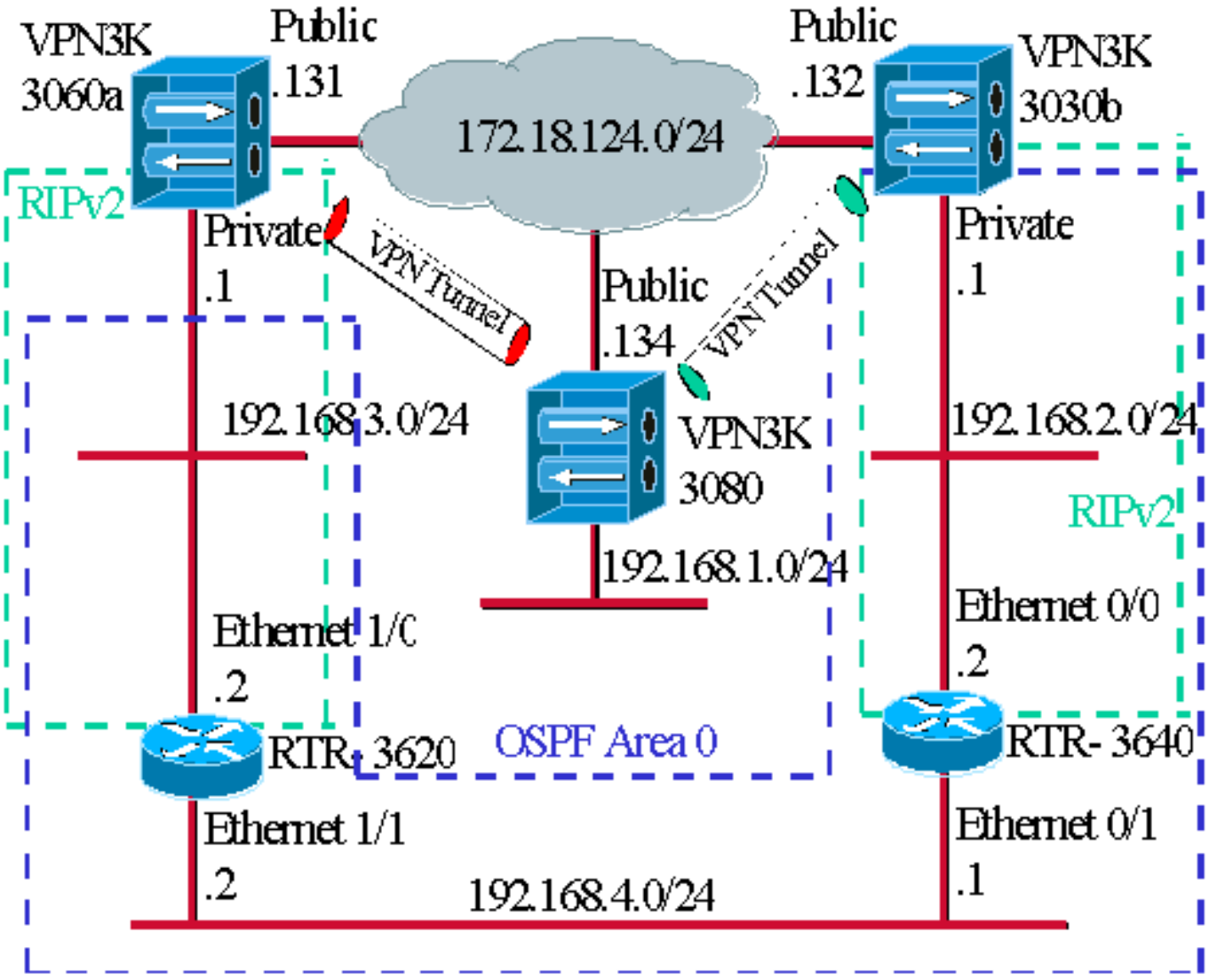
Configurar

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
```

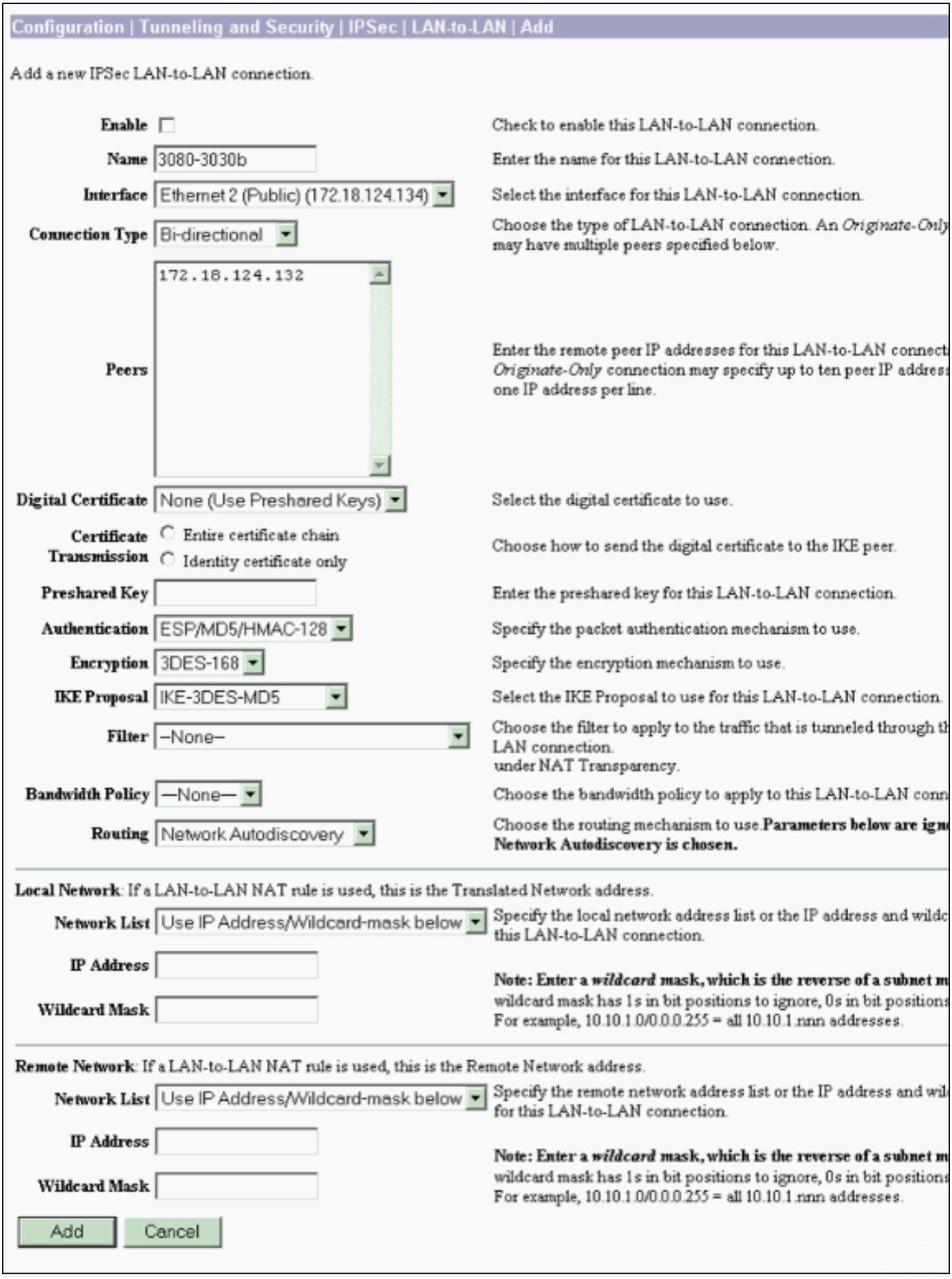
```
service timestamps log uptime
no service password-encryption
!
hostname rtr-3640
!
ip subnet-zero
!
interface Ethernet0/0
 ip address 192.168.2.2 255.255.255.0
 half-duplex
!
interface Ethernet0/1
 ip address 192.168.4.1 255.255.255.0
 half-duplex
!
router ospf 1
 log-adjacency-changes
!--- Use this 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.

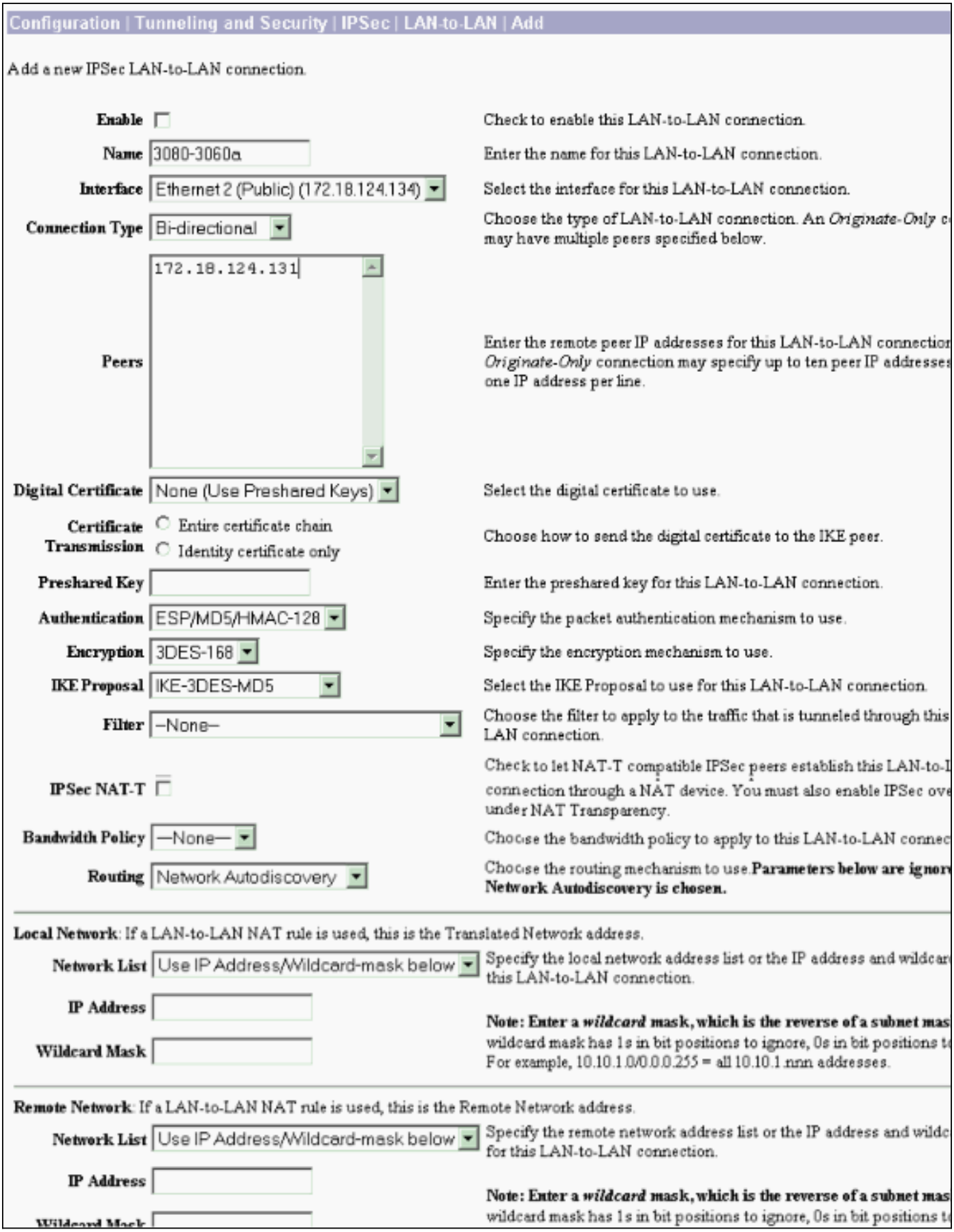


LAN-to-LAN VPN 3080 a VPN 3060a

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.

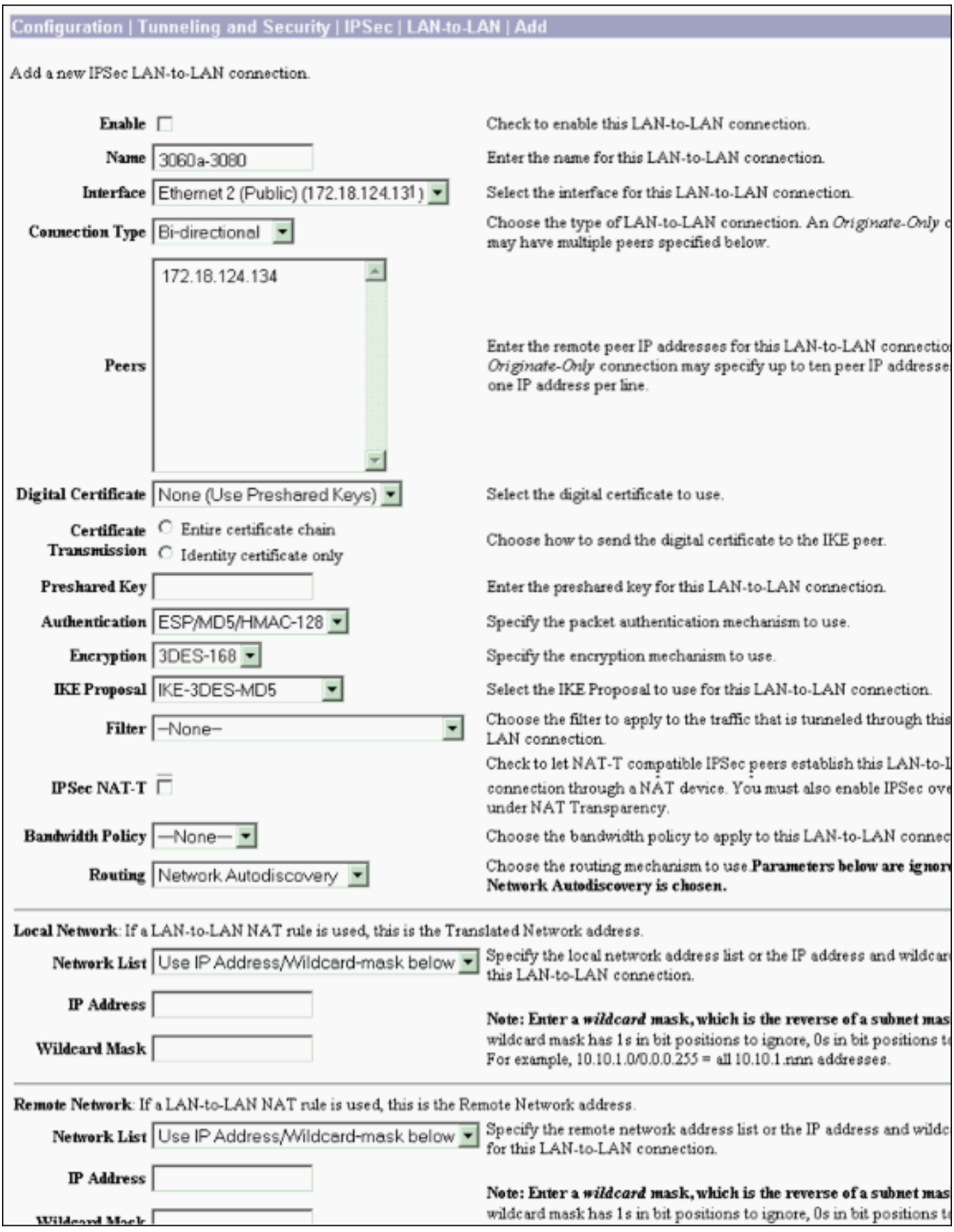


Configuração do VPN 3060a Concentrator

VPN 3060a para VPN 3080 de LAN para LAN

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

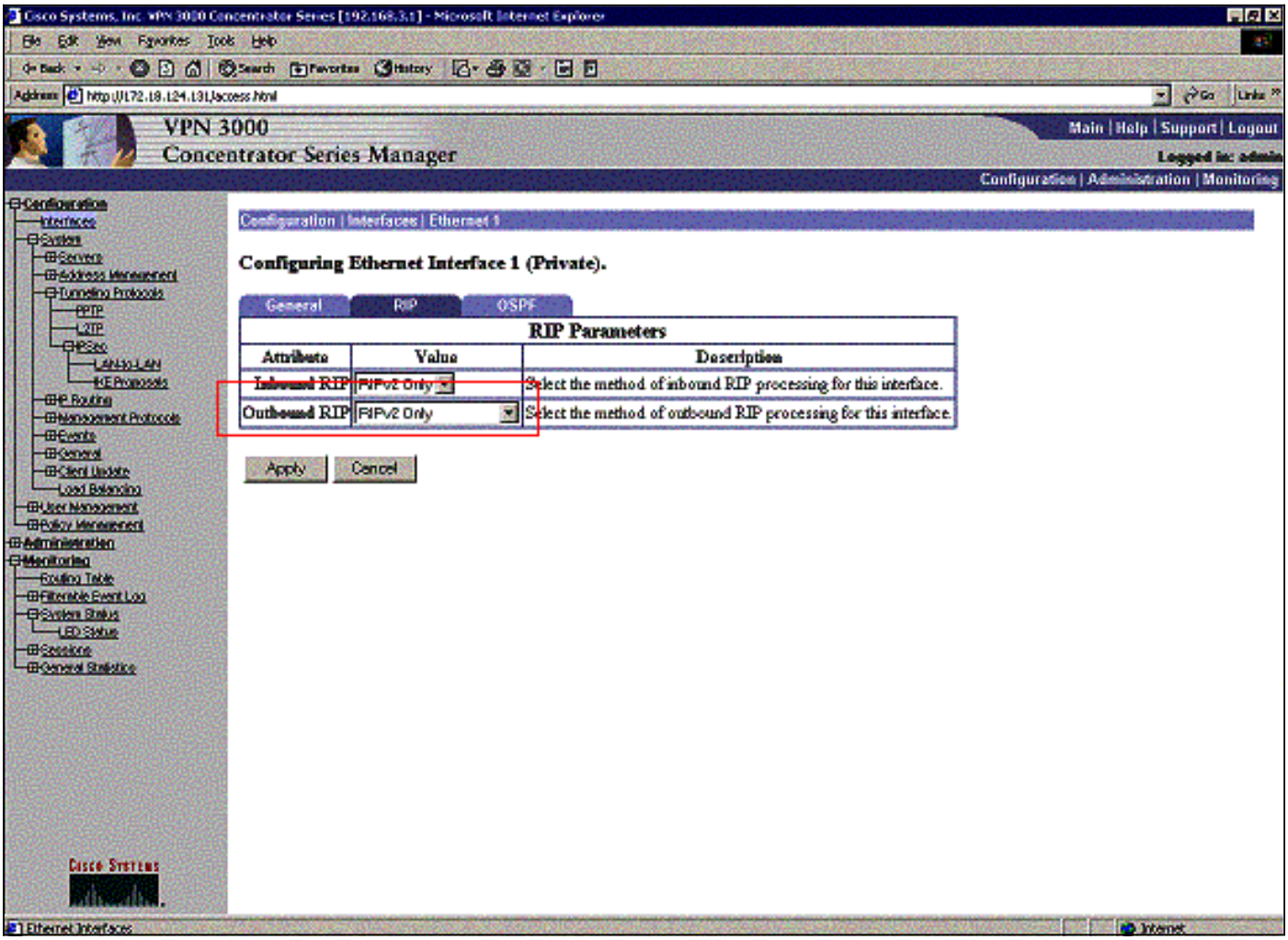
Observação: há uma caixa de seleção no VPN 3060 para a descoberta automática de rede em vez do menu suspenso como na versão de software 3.5 e posterior.



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**.

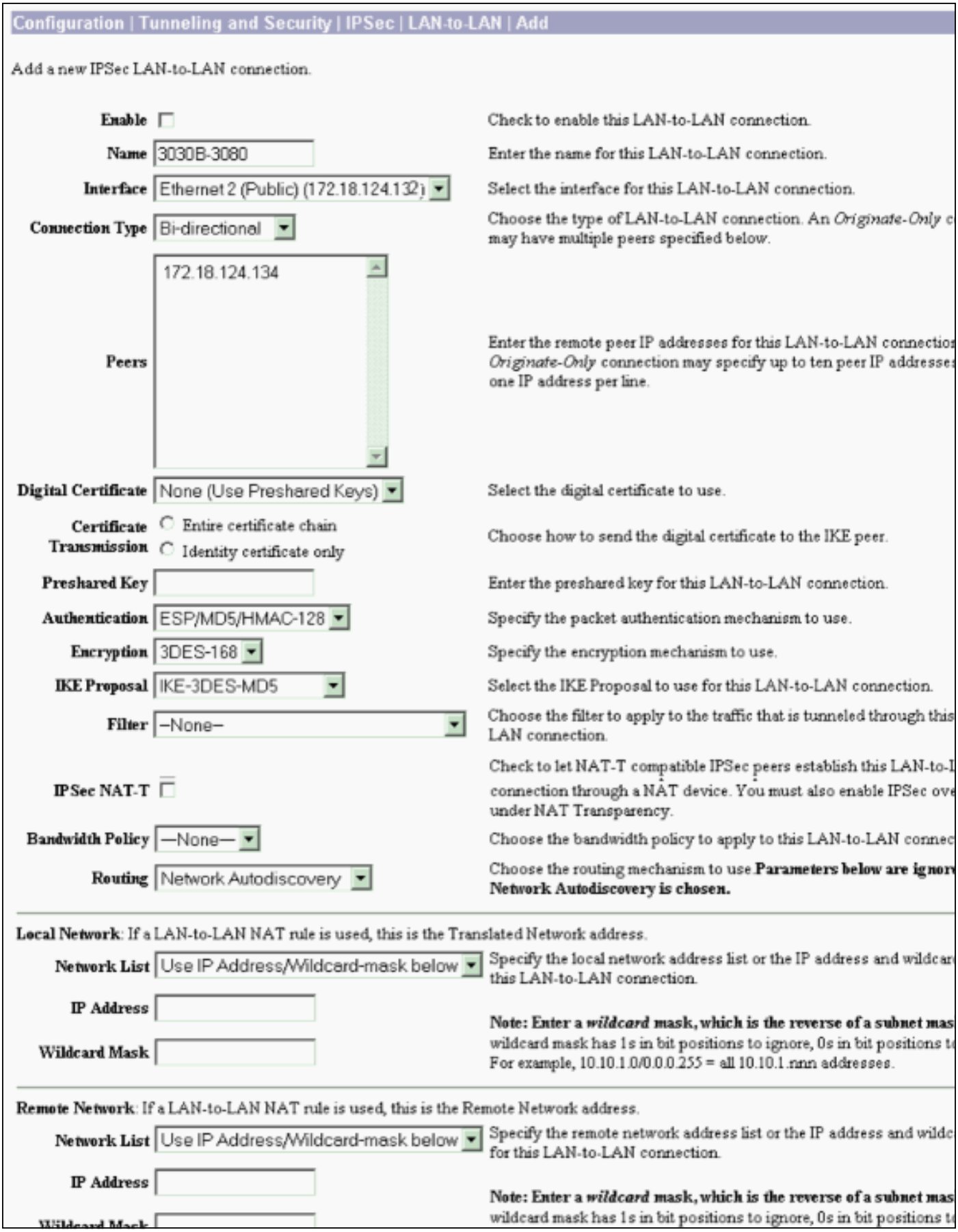
Observação: o padrão é o RIP de saída e é desativado para a interface privada.



Configuração do VPN 3030b Concentrator

VPN 3030b para VPN 3080 de LAN para LAN

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

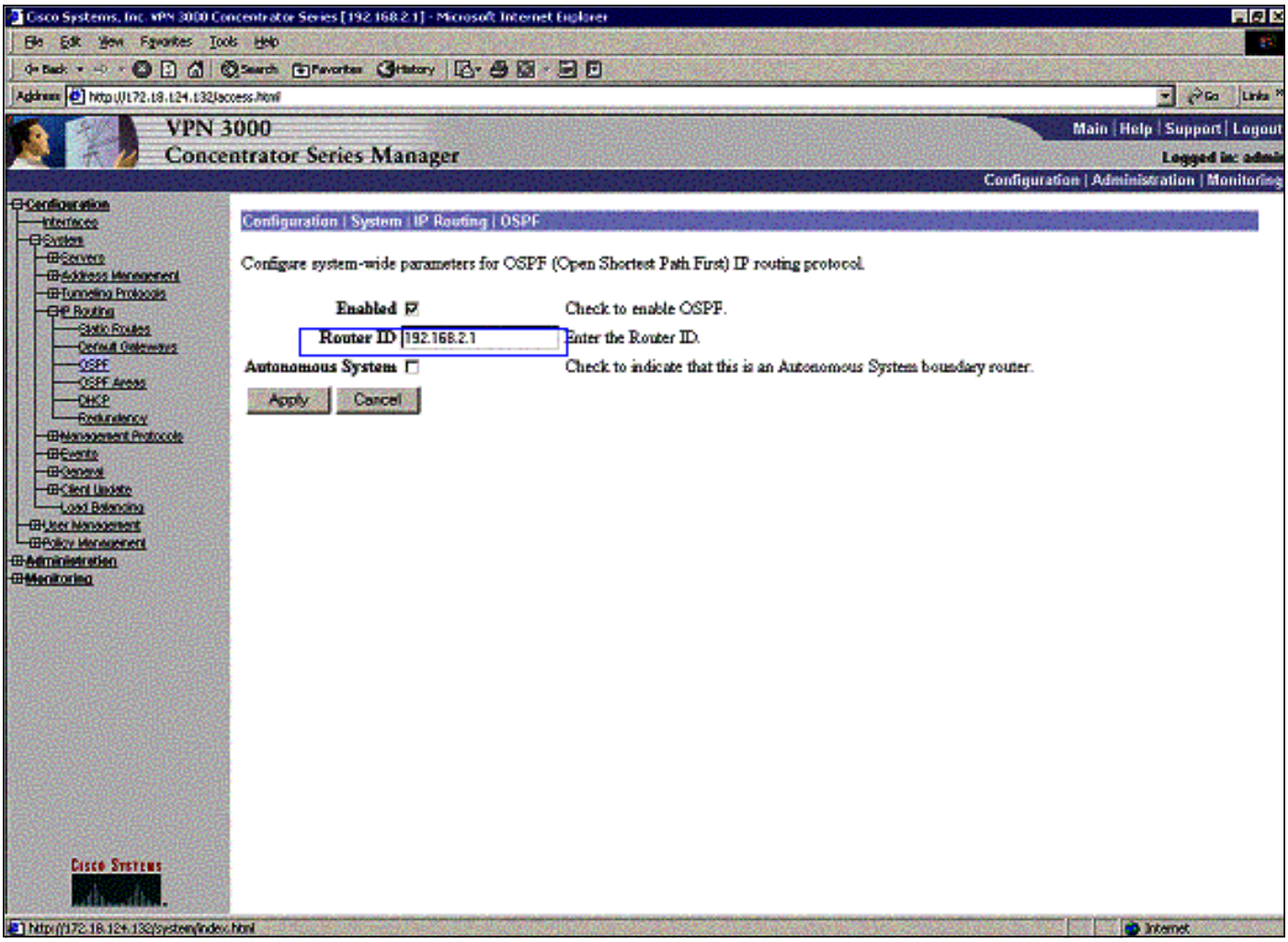


Ative o RIP para passar as rotas aprendidas pelo túnel para o roteador VPN 3640

Siga as etapas listadas anteriormente neste documento para o VPN 3060a Concentrator.

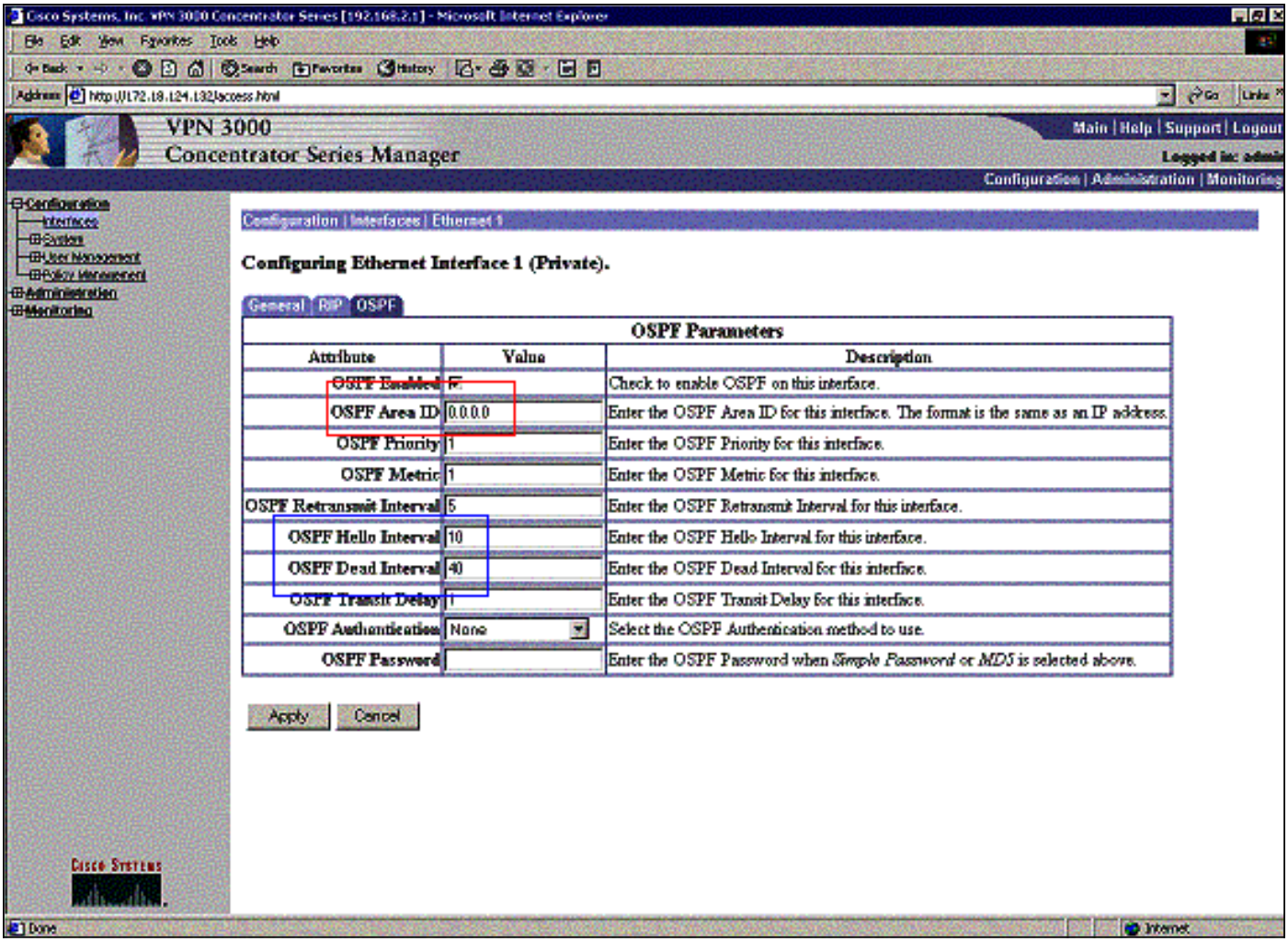
Habilite o OSPF para passar as rotas aprendidas por backbone para o VPN 3030b Concentrator

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
!--- For troubleshooting purposes, it helps to make the router ID the !--- IP address of the
private interface. 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**.



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

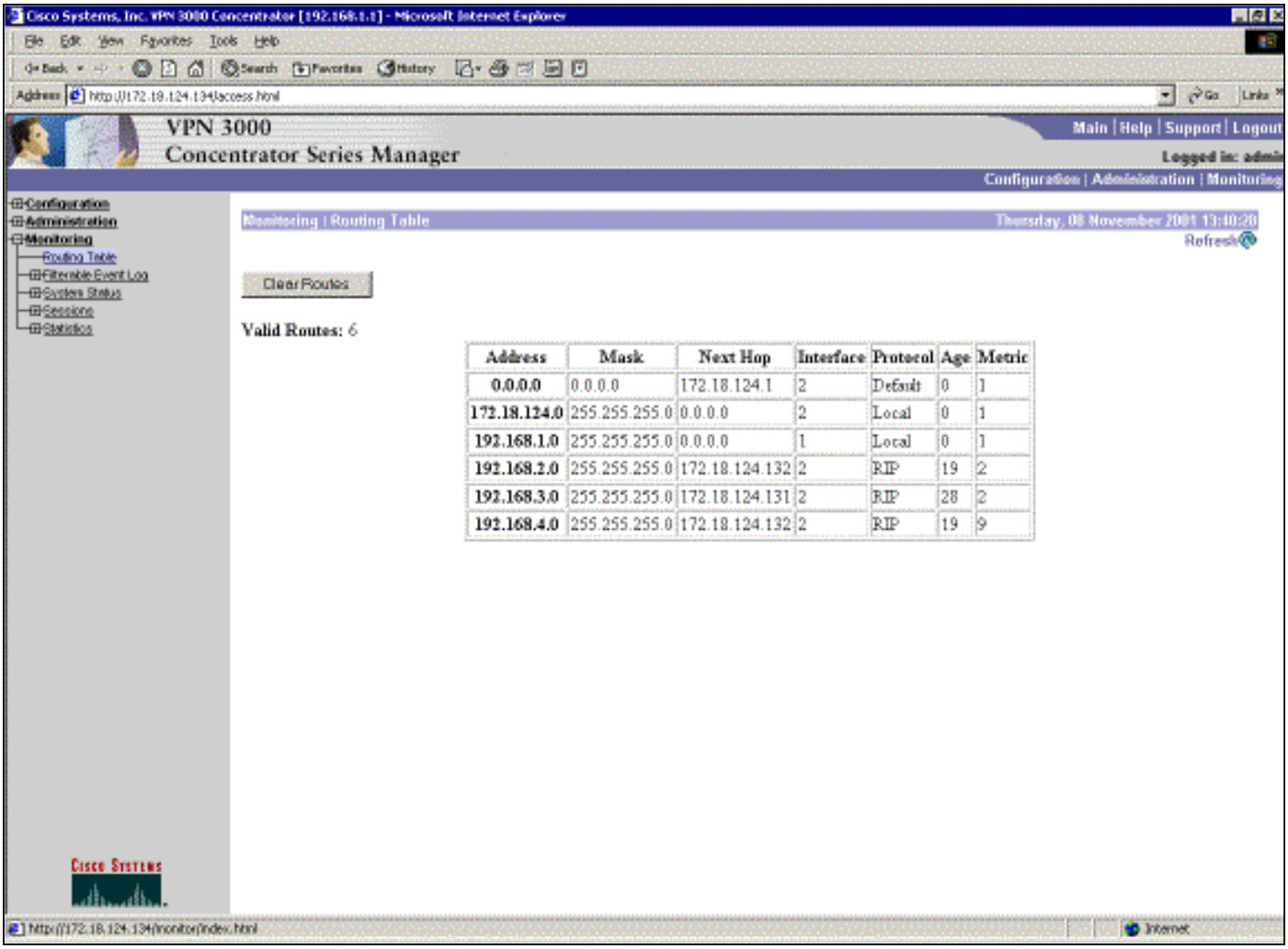
Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

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.

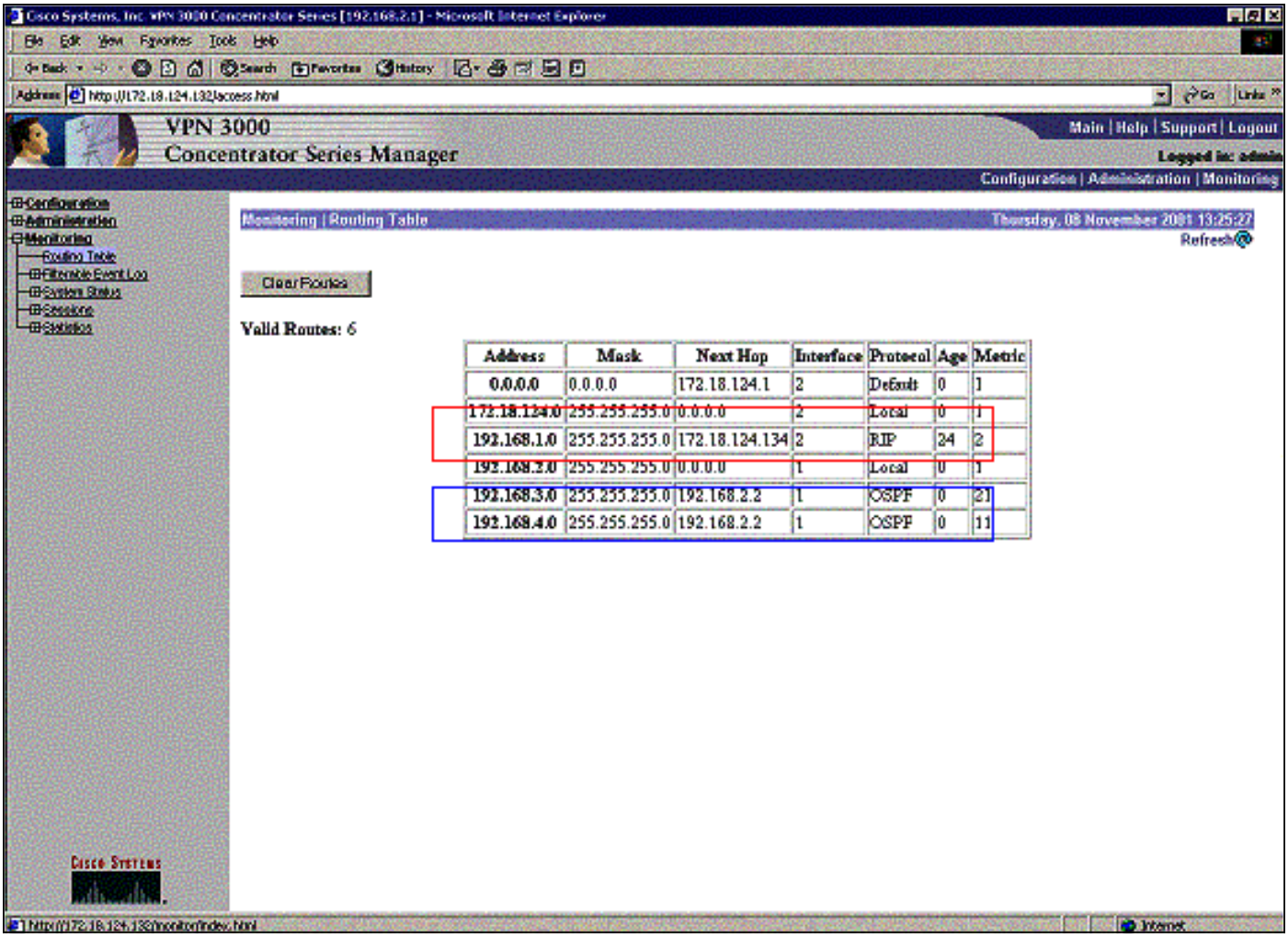
```
rtr-3620#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

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.



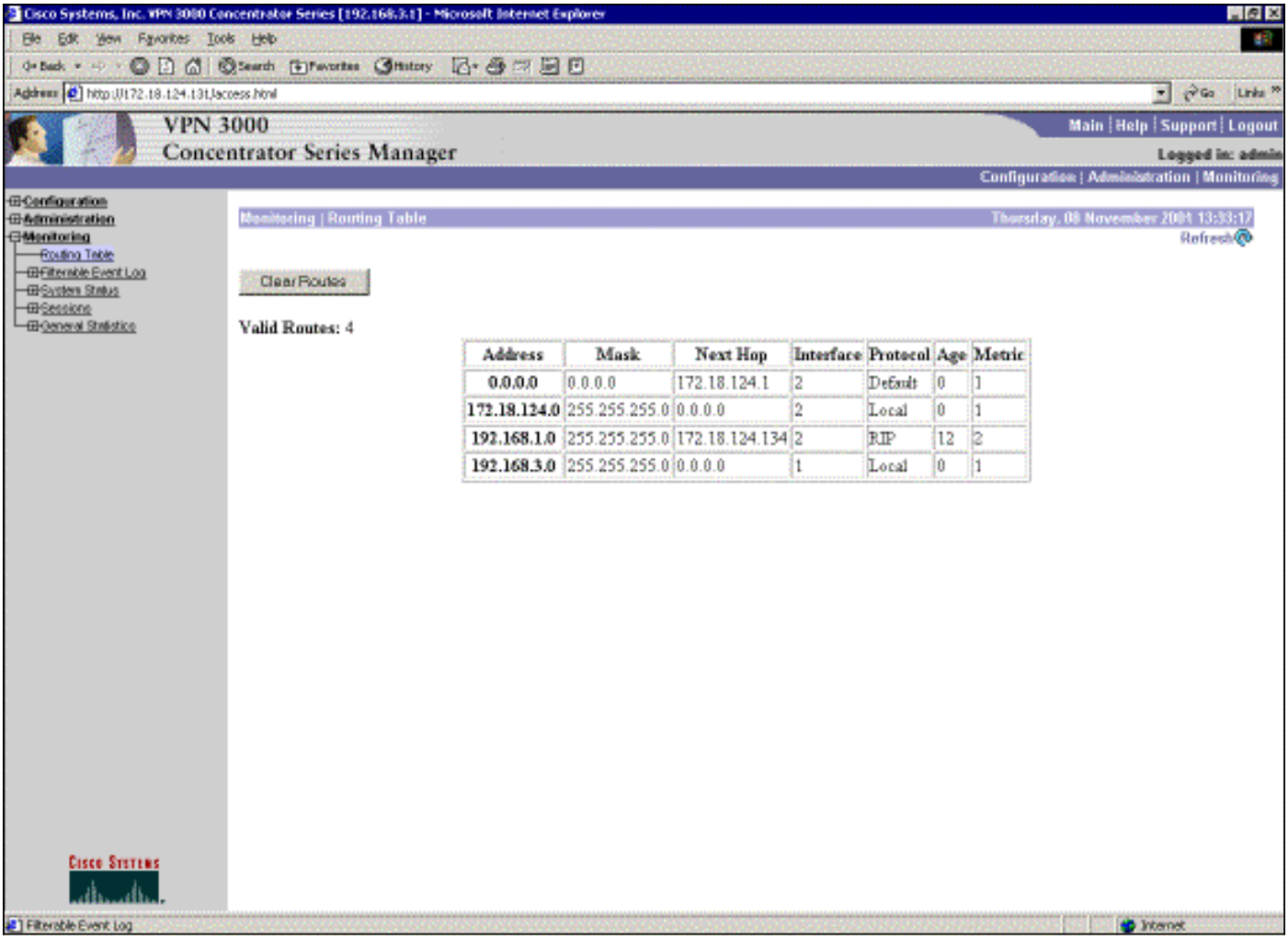
As redes 192.168.2.x e 192.168.3.x são aprendidas através dos túneis VPN 172.18.124.132 e 172.18.124.131, respectivamente. A rede 192.168.4.x é aprendida através do túnel 172.18.124.132 porque os anúncios OSPF do roteador são colocados na tabela de roteamento do VPN 3030b Concentrator. Em seguida, a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

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



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.

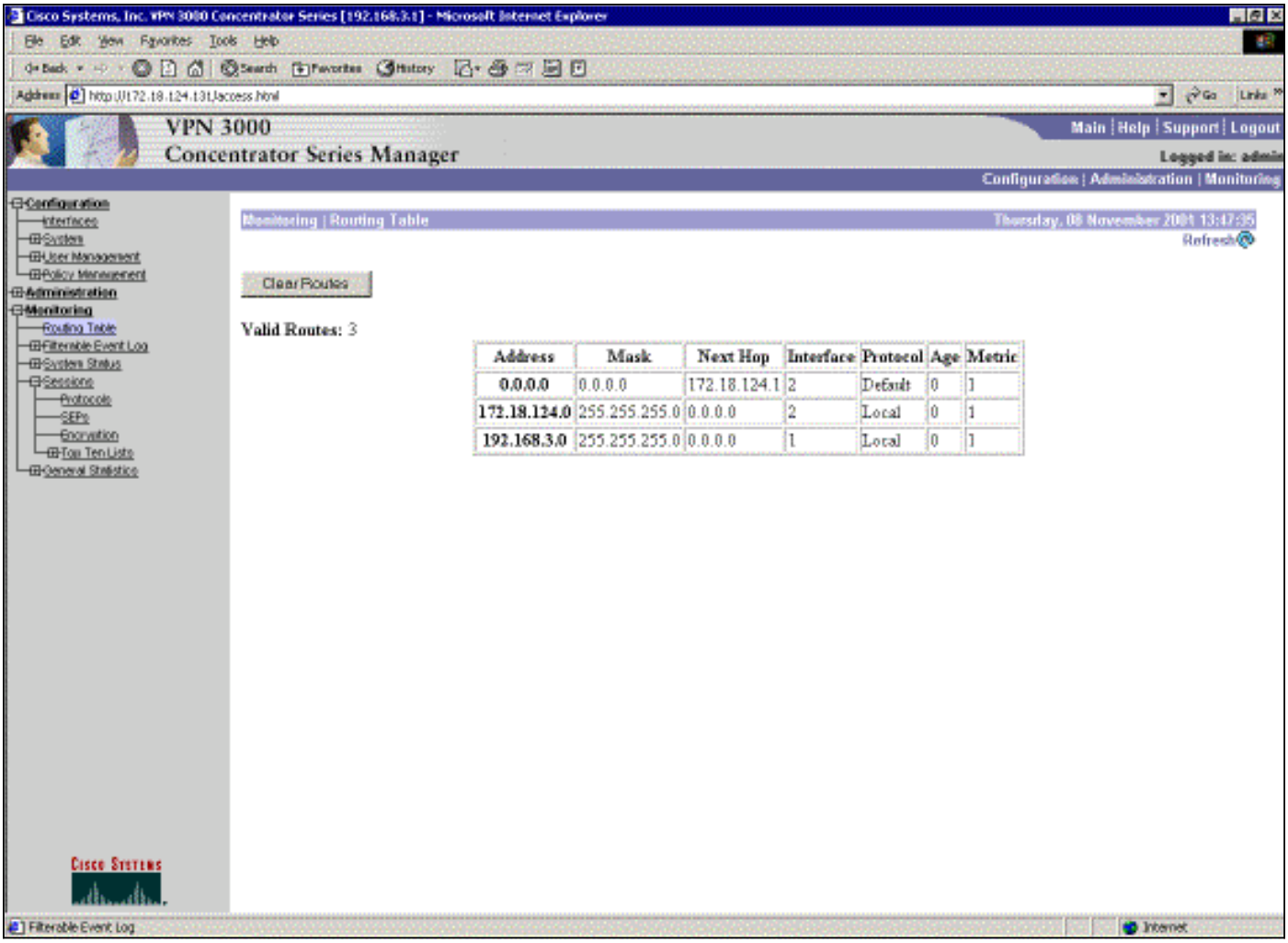


A rede 192.168.1.x é a única rede aqui e pode ser acessada através do túnel VPN. Não há rede 192.168.2.0, pois nenhum processo (como o RIP) passa por essa rota. Não há nada perdido enquanto os PCs na rede 192.168.3.x não apontarem seu gateway padrão para o VPN Concentrator. Você sempre pode adicionar 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.



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:

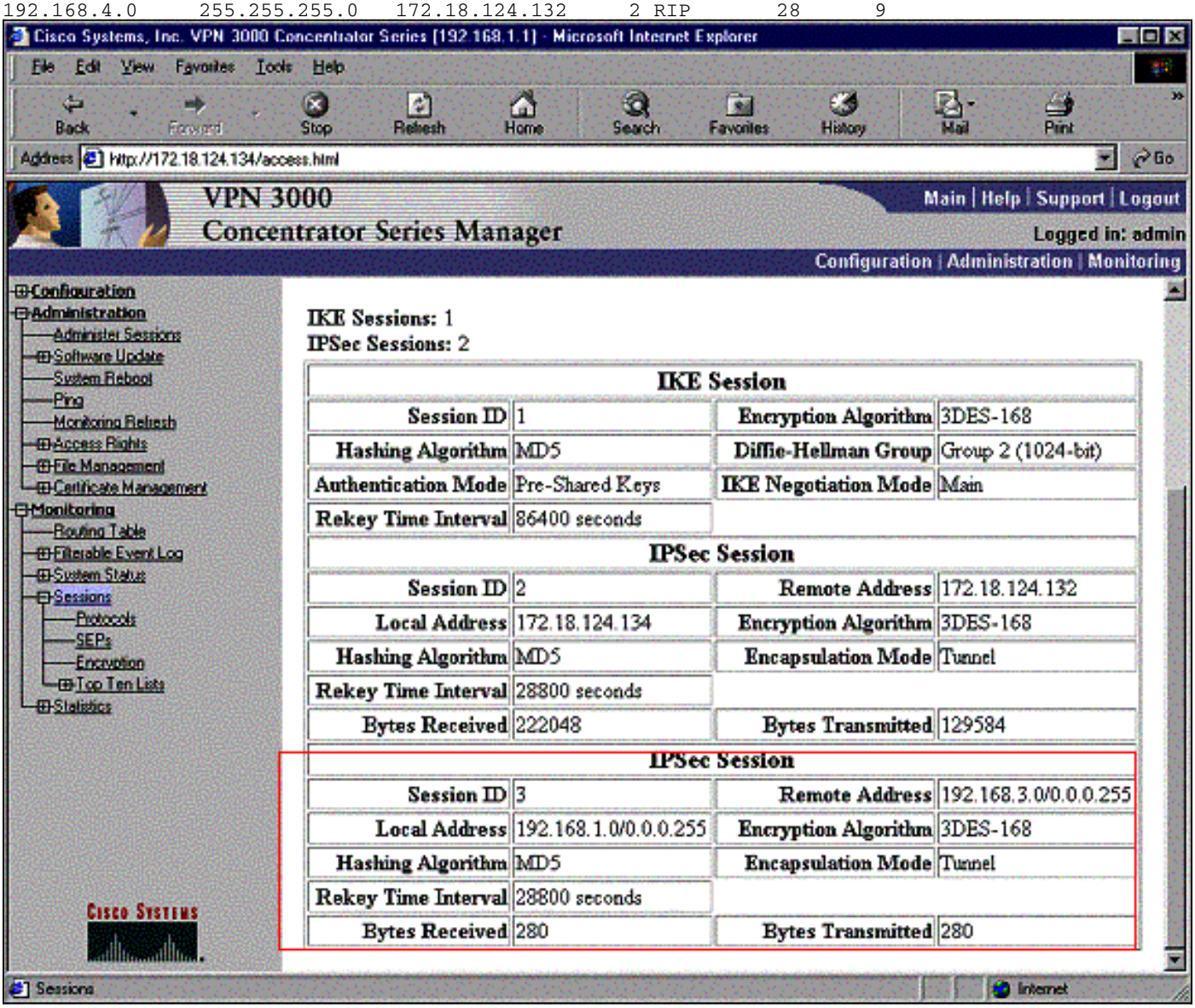
```
rtr-3620#show ip route

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
```

```
192.168.4.0     255.255.255.0   172.18.124.132     2 RIP       28       9
```



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