Redundant routing configureren op de VPN-concentratie 3000

Inhoud

Inleiding

Dit document beschrijft hoe u een redundante VPN-failover kunt configureren als een externe site de VPN-concentratie 3000 of de internetverbinding verliest. In dit voorbeeld, neem aan dat het bedrijfsnetwerk achter VPN 3030B Open Kortste Pad Eerst (OSPF) als zijn standaard routingprotocol gebruikt.

Opmerking: wanneer u opnieuw verdeelt tussen het routeren van protocollen, kunt u een routinglus vormen die problemen op het netwerk kan veroorzaken. OSPF wordt in dit voorbeeld gebruikt, maar het is niet het enige routingprotocol dat kan worden gebruikt.

Het doel van dit voorbeeld is om het 192.168.1.0 netwerk gebruik te maken van de rode tunnel (onder normale bedrijfsomstandigheden), afgebeeld in het gedeelte Netwerkdiagram, om 192.168.3.x te bereiken. Als de tunnel, VPN Concentrator of ISP zakt, dan wordt het netwerk van 192.168.3.0 geleerd via een dynamisch routingprotocol via de groene tunnel. Bovendien is de connectiviteit niet verloren aan de 192.168.3.0 plaats. Als de kwestie is opgelost, keert het verkeer automatisch terug naar de rode tunnel.

Opmerking: RIP heeft een veroudering-timer van drie minuten voordat een nieuwe route op een ongeldige route wordt geaccepteerd. Ga er ook van uit dat de tunnels gecreëerd worden en dat er verkeer tussen de peers heen kan.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco-routers 3620 en 3640
- Cisco VPN 3800 Concentrator - versie: Cisco Systems, Inc./VPN 3000 Concentrator versie 4.7
- Cisco VPN 3060 Concentrator - versie: Cisco Systems, Inc./VPN 3000 Concentrator Series versie 4.7
- Cisco VPN 3030 Concentrator - versie: Cisco Systems, Inc./VPN 3000 Concentrator Series versie 4.7

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

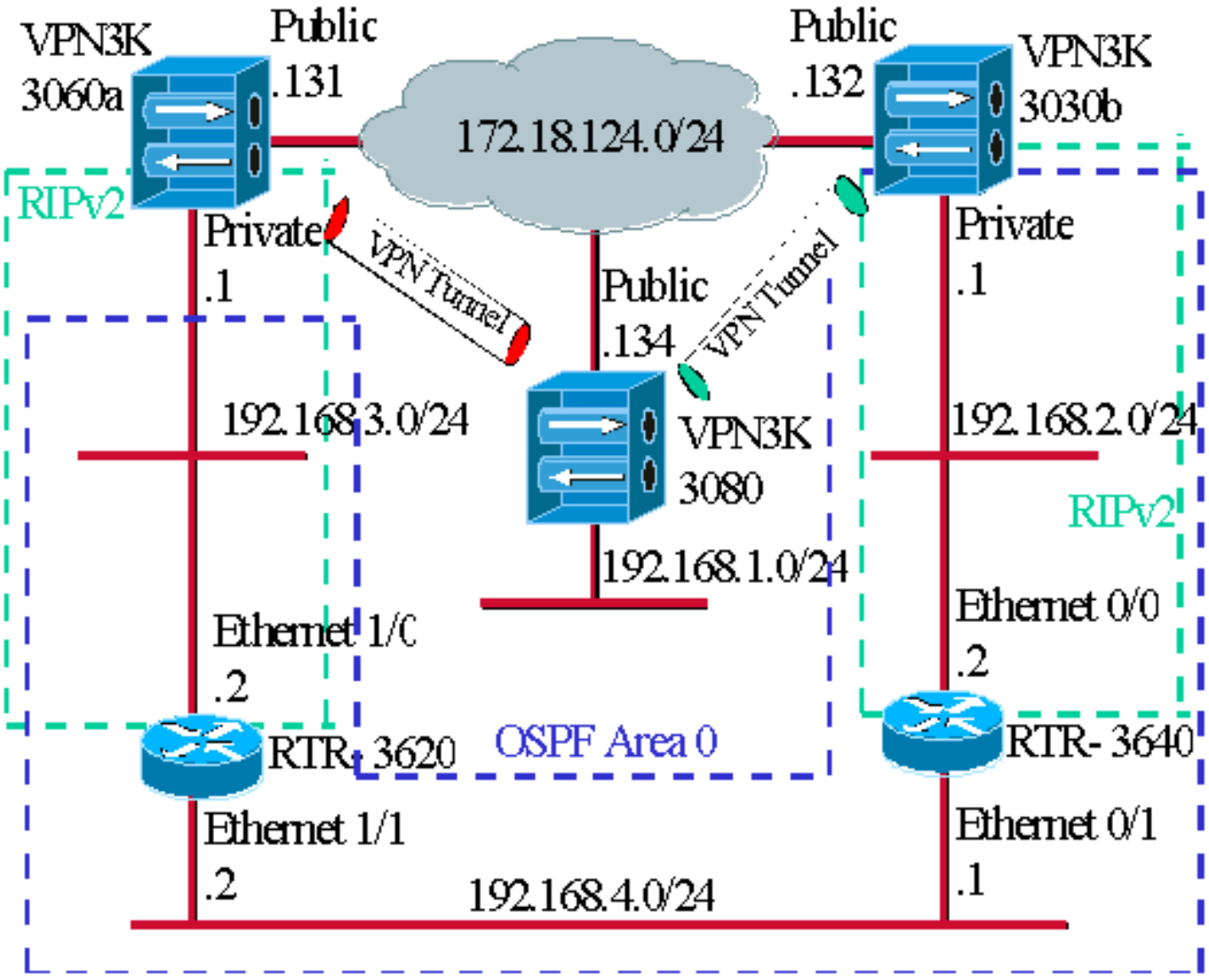
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Als u aanvullende informatie wilt vinden over de opdrachten in dit document, gebruikt u het Opdrachtplanningprogramma (alleen geregistreerd klanten).

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



De blauwe streepjes geven aan dat OSPF-ingeschakeld is van VPN 3030b naar RTR-3640 en RTR-3620.

De groene streepjes geven aan dat RIPv2 van privé VPN 3060a aan RTR-3620, RTR-3640, en privé VPN 3030b wordt ingeschakeld.

RIPv2 wordt ook ingeschakeld in de rode en groene VPN-tunnels omdat de netwerkontdekking is ingeschakeld. Het is niet nodig om RIP op de VPN 3080 privé interface in te schakelen. Er is ook geen RIP op het netwerk 192.168.4.x omdat alle routes door OSPF over deze link worden geleerd.

Opmerking: Voor PC's op de netwerken 192.168.2.x en 192.168.3.x moeten hun standaardgateways zijn gericht op de routers en niet op de VPN-concentrators. Laat de routers beslissen waar u de pakketten wilt verzenden.

Routerconfiguratie

Dit document gebruikt deze routerconfiguraties:

- router 3620
- router 3640

router 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
```

router 3640

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

Current configuration : 1129 bytes
!
version 12.2
```

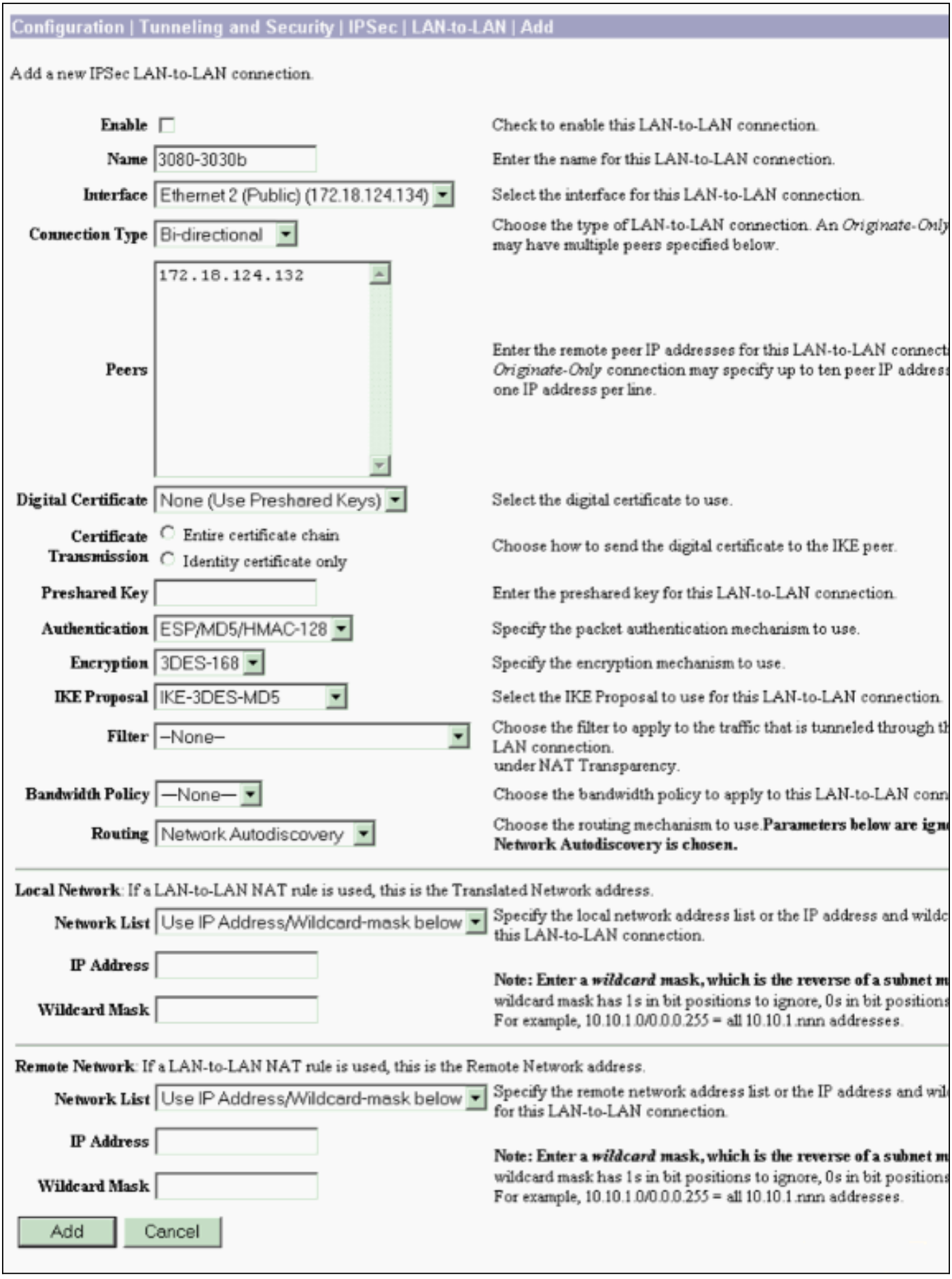
```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rtr-3640
!
ip subnet-zero
!
interface Ethernet0/0
 ip address 192.168.2.2 255.255.255.0
 half-duplex
!
interface Ethernet0/1
 ip address 192.168.4.1 255.255.255.0
 half-duplex
!
router ospf 1
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

VPN 3800 Concentrator-configuratie

LAN-to-LAN VPN 3080 tot VPN 3030b

Selecteer **Configuration > Tunneling en Security > IPSec > IPSec LAN-to-LAN**. Aangezien Network Automatisch discovery wordt gebruikt, hoeven de lokale en externe netwerklijsten niet in te vullen.

Opmerking: VPN Concentrators die softwareversie 3.1 uitvoeren en eerder beschikken over een aankruisvakje voor automatische ontdekking. Software versie 3.5 (gebruikt op VPN 3080) gebruikt een vervolgkeuzemenu, zoals het menu dat hier wordt weergegeven.

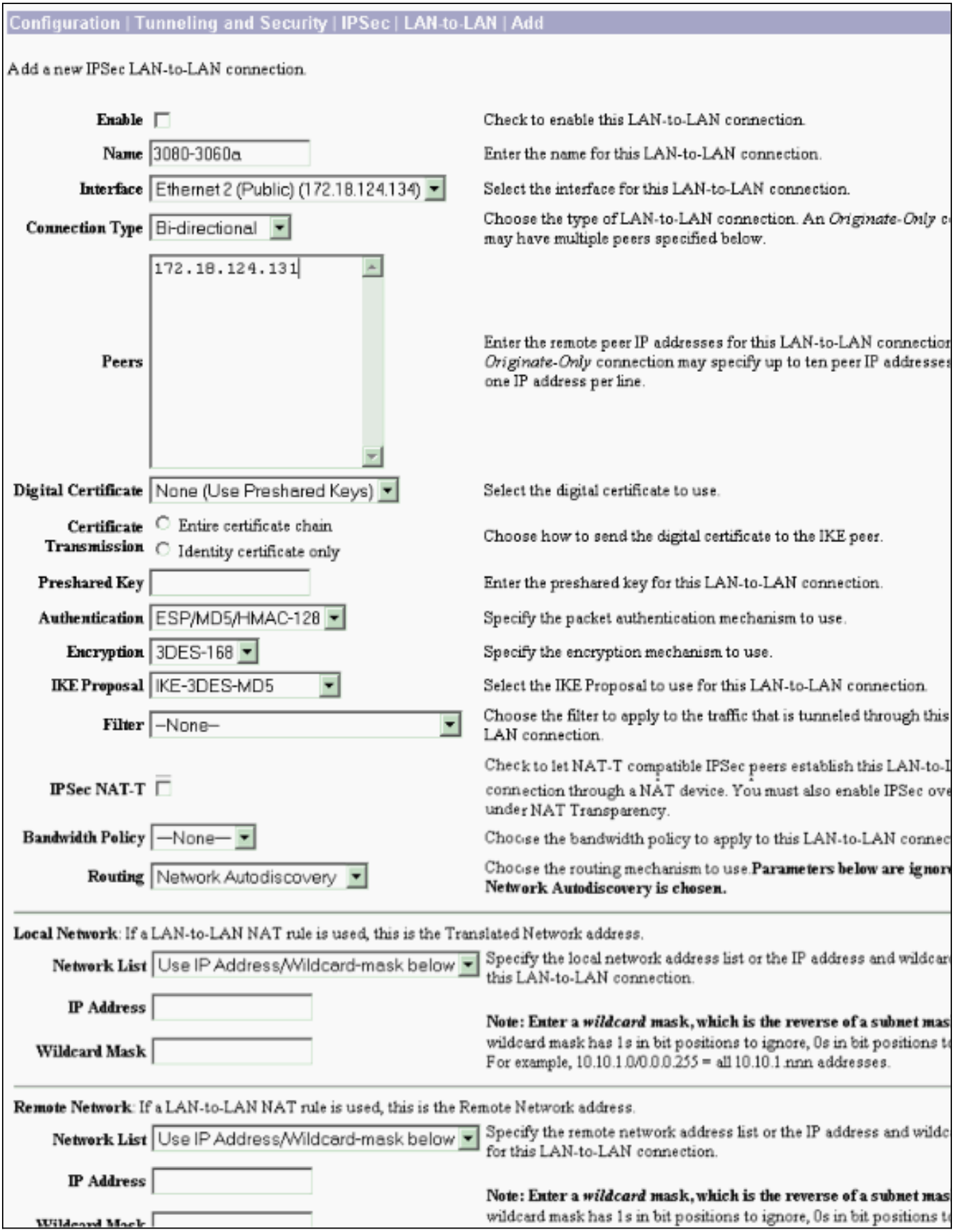


[LAN-to-LAN VPN 3080 tot VPN 3060a]

Selecteer **Configuration > Tunneling en Security > IPSec > IPSec LAN-to-LAN**. Aangezien

Network Automatisch discovery wordt gebruikt, hoeven de lokale en externe netwerklijsten niet in te vullen.

Opmerking: VPN Concentrators die softwareversie 3.1 uitvoeren en eerder beschikken over een aankruisvakje voor automatische ontdekking. Software versie 3.5 (gebruikt op VPN 3080) gebruikt een vervolgkeuzemenu, zoals het menu dat hier wordt weergegeven.

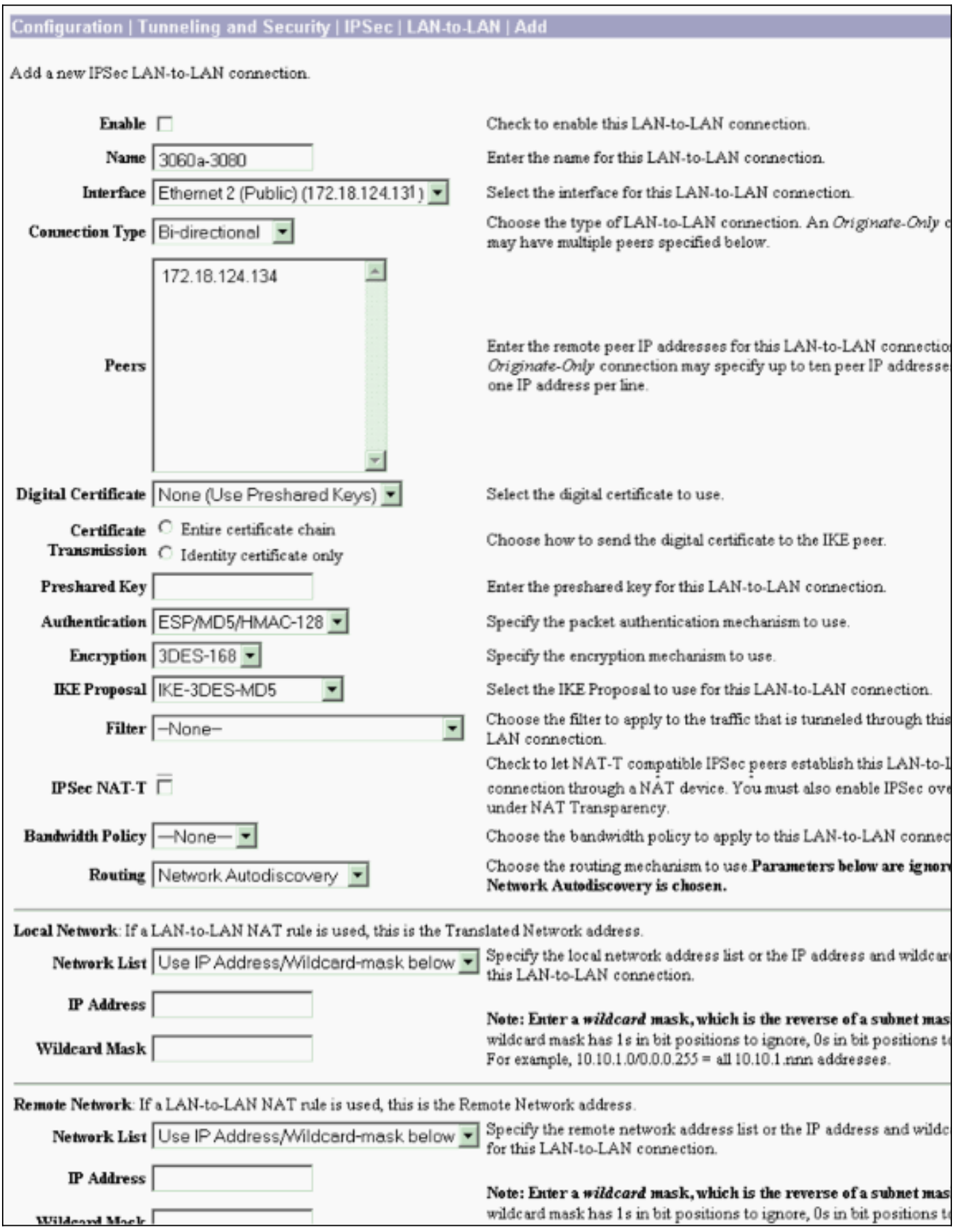


VPN 3060a Concentrator-configuratie

LAN-to-LAN VPN 3060a naar VPN 3080

Selecteer **Configuration > Tunneling en Security > IPSec > IPSec LAN-to-LAN**.

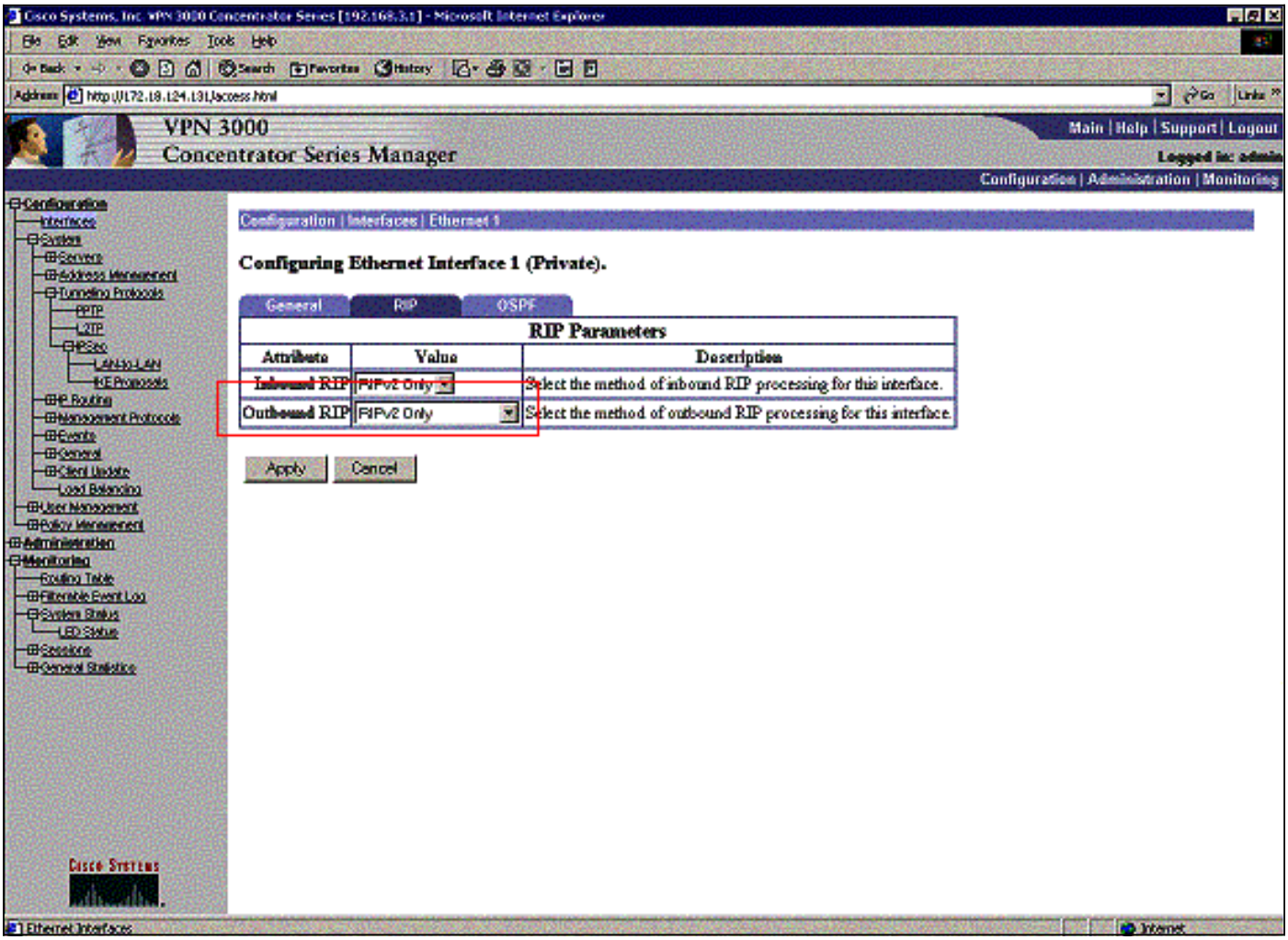
Opmerking: Er is een aankruisvakje in VPN 3060 voor Network Automatisch discovery in plaats van het uitrolmenu zoals in softwareversie 3.5 en hoger.



Laat RIP toe om de Tunnel-Leerde Routes aan de VPN 3620 router door te geven

Selecteer **Configuration > Interfaces > Private > RIP**. Verander het vervolgkeuzemenu naar **RIPv2 Alleen** en klik op **Toepassen**. Selecteer vervolgens **Configuration > System > Tunneling Protocols > IPSec > LAN-to-LAN**.

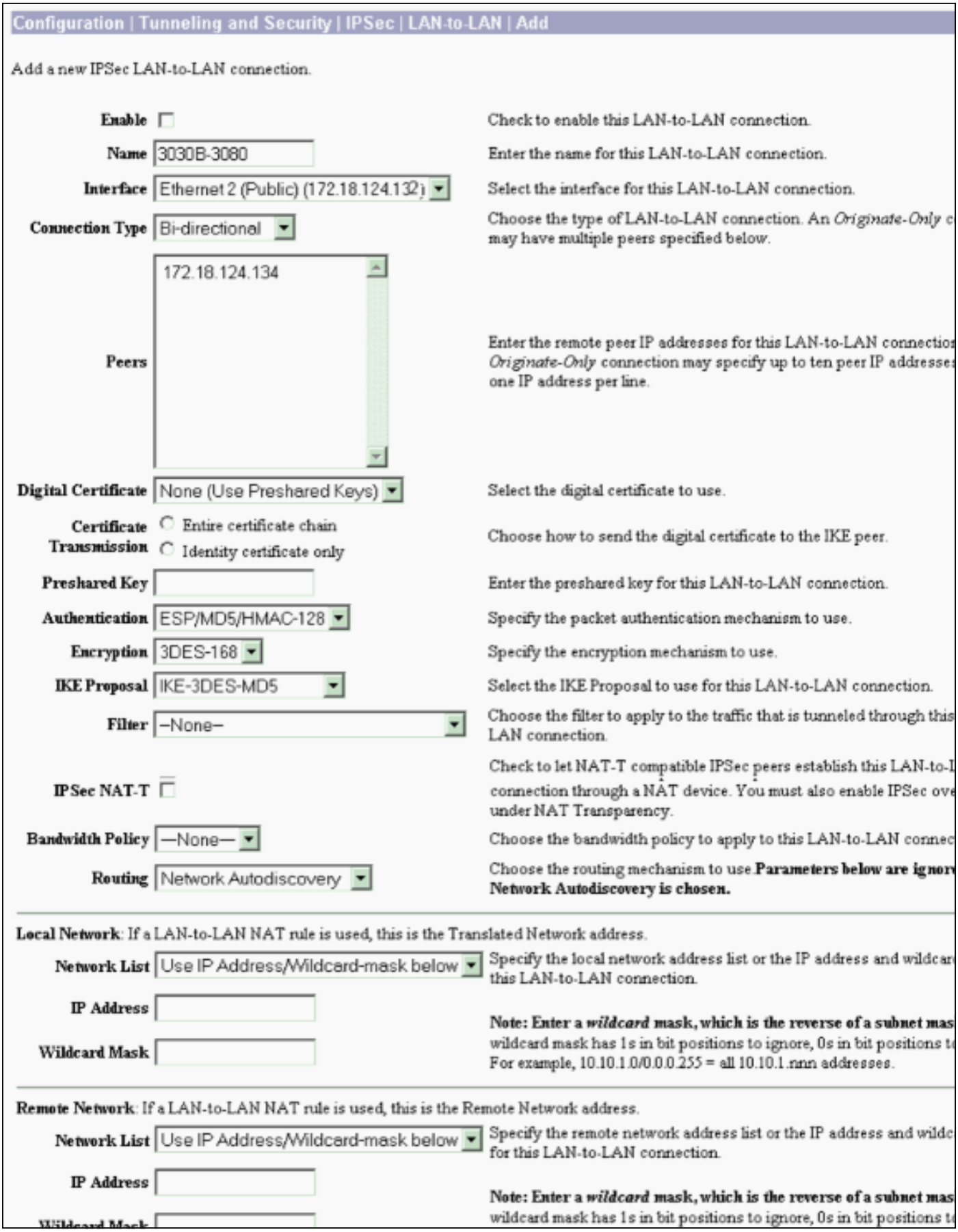
Opmerking: de standaard is uitgaande RIP en is uitgeschakeld voor de privé-interface.



VPN 3030b Concentrator-configuratie

LAN-to-LAN VPN 3030b naar VPN 3080

Selecteer **Configuration > Tunneling en Security > IPSec > LAN-to-LAN**.

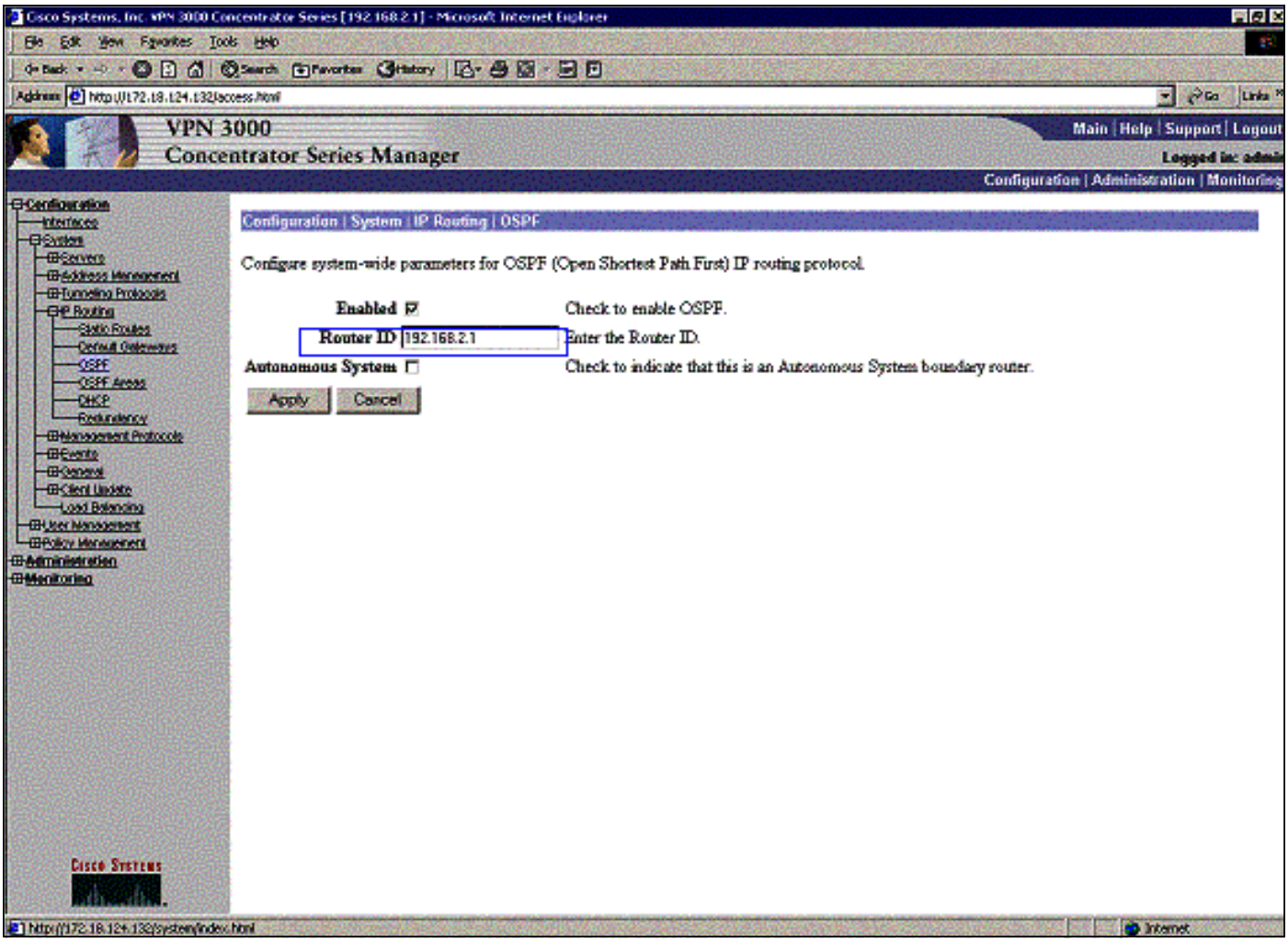


Laat RIP toe om de Tunnel-Leerde Routes aan de VPN 3640 router door te geven

Volg de stappen die eerder in dit document zijn opgesomd voor VPN 3060a Concentrator.

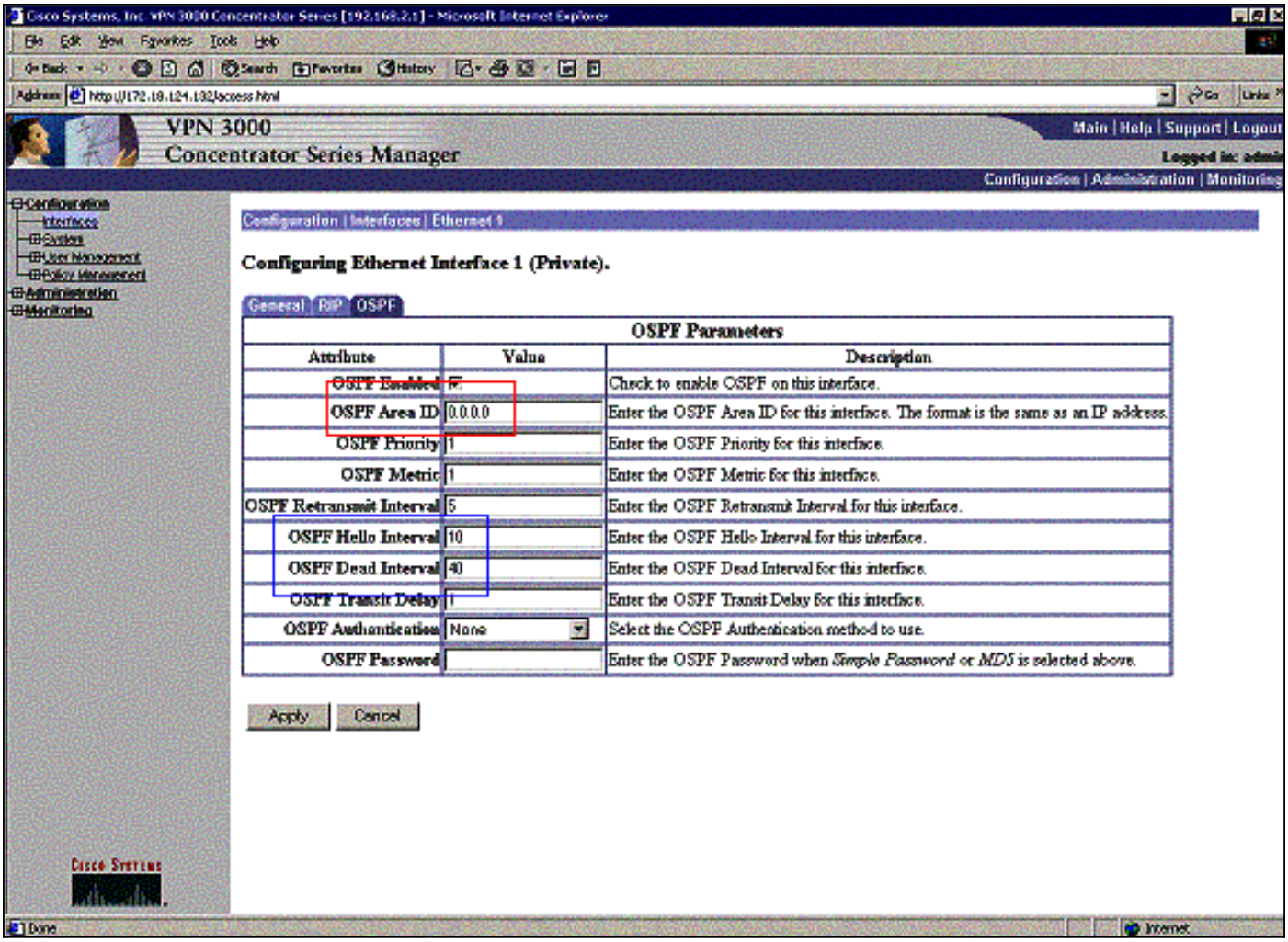
OSPF-inschakelen om de backbone-learning-routers uit te voeren naar VPN-Concentrator 3030b

Selecteer **Configuratie > Systeem > IP Routing > OSPF** en voer de router-ID in.




```
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
```

Het gebied-ID moet overeenkomen met de ID op de draad. Aangezien het gebied in dit voorbeeld 0 is, wordt het vertegenwoordigd door 0.0.0.0. Controleer ook het vakje **OSPF** inschakelen en klik op **Toepassen**.



Zorg dat uw OSPF-timers overeenkomen met die van de router. Om de routers te controleren gebruikt u de opdracht **tonen IP Ospf-interface *<interface-naam>*.**

```
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)
```

Raadpleeg voor meer informatie over OSPF RFC 1247 .

Verifiëren

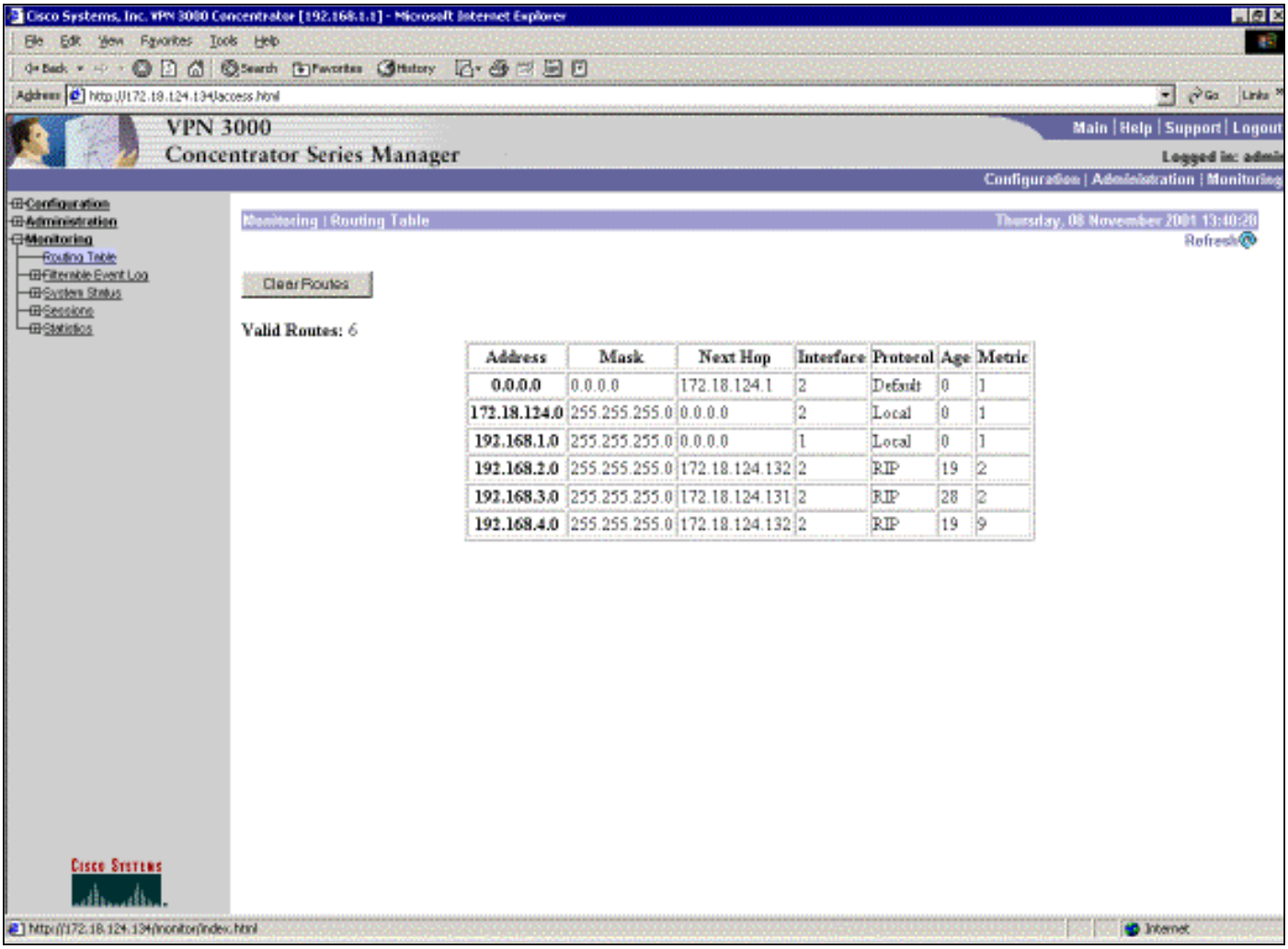
Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

Deze opdrachtoutput toont nauwkeurige routingtabellen.

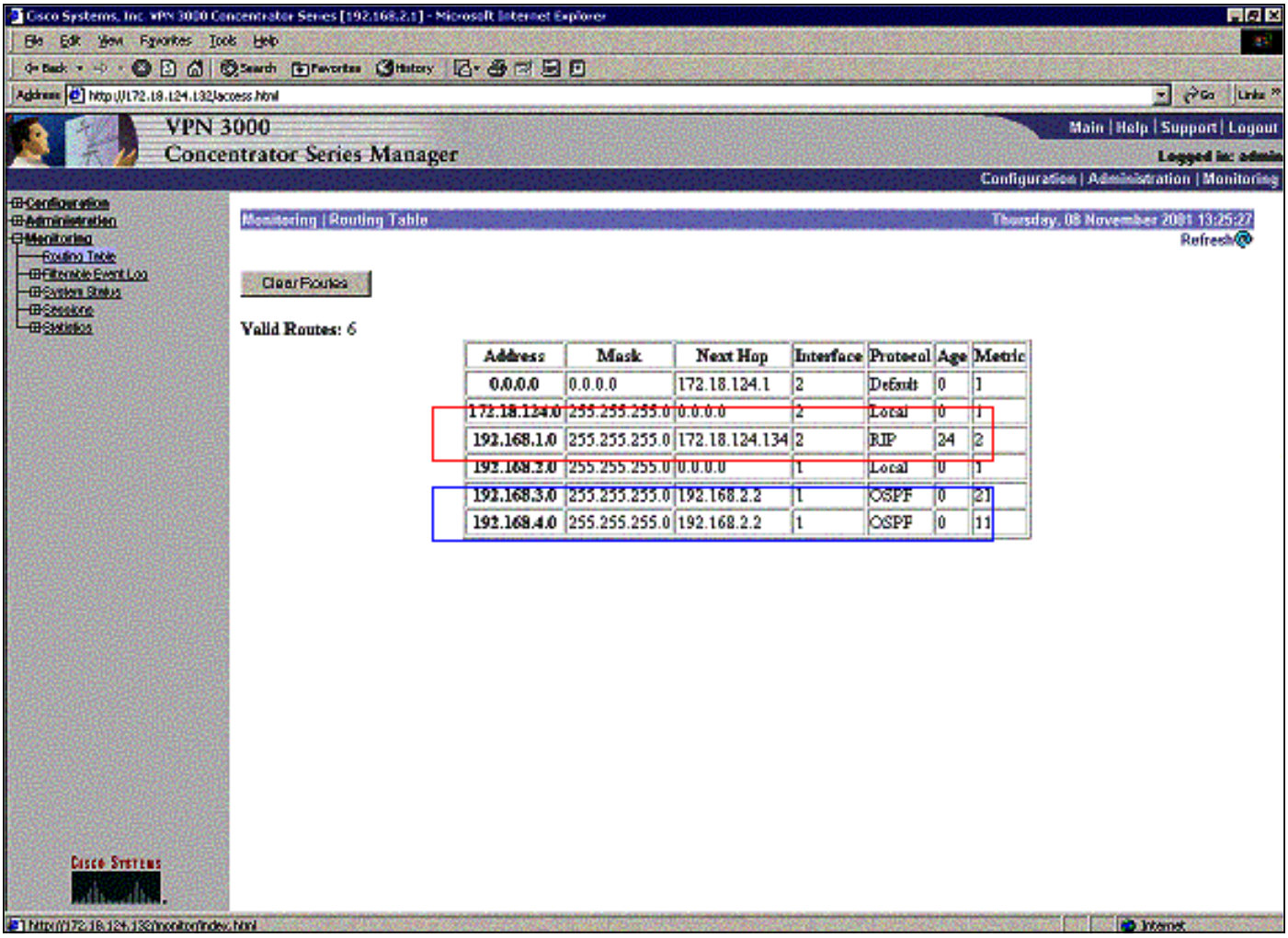
```
rtr-3620#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

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
```

Dit is de VPN 3080 Concentrator-routingtabel onder normale omstandigheden.



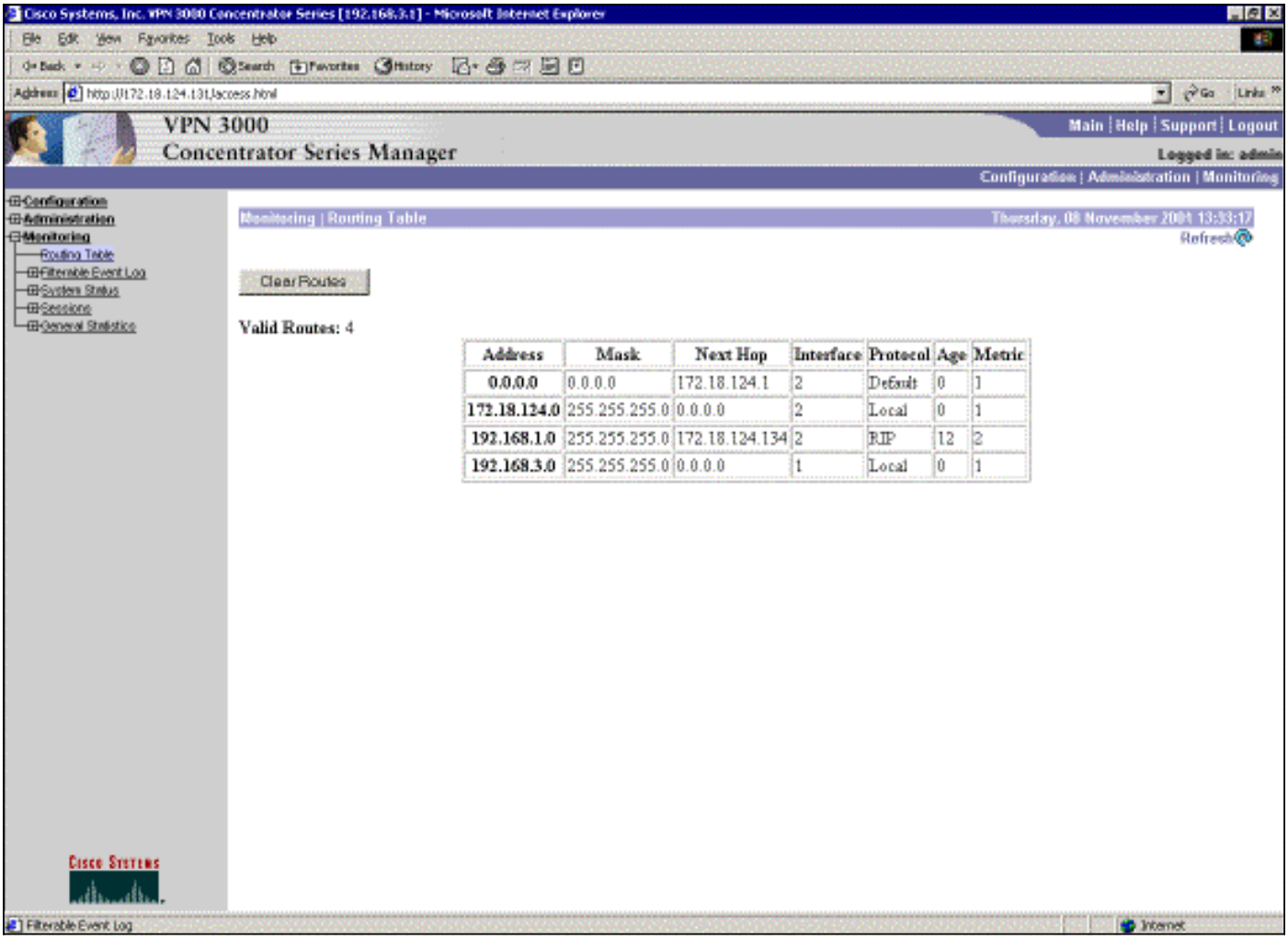
Networks 192.168.2.x en 192.168.3.x worden beide geleerd via de VPN-tunnels van respectievelijk 172.18.124.132 en 172.18.124.131. Het 192.168.4.x-netwerk wordt geleerd door de 172.18.124.132 tunnel omdat de OSPF-advertenties van de router in de VPN 3030b routeringstabel van Concentrator worden geplaatst. Dan adverteert de routingtabel het netwerk naar de externe VPN-peers.

Dit is de VPN 3030b Concentrator-routingtabel onder normale omstandigheden.



De rode doos benadrukt dat het 192.168.1.x netwerk uit de VPN tunnel wordt geleerd. De blauwe doos benadrukt dat netwerken 192.168.3.x en 192.168.4.x door het kern OSPF-proces worden geleerd.

Dit is de VPN 3060a Concentrator-routingtabel onder normale omstandigheden.

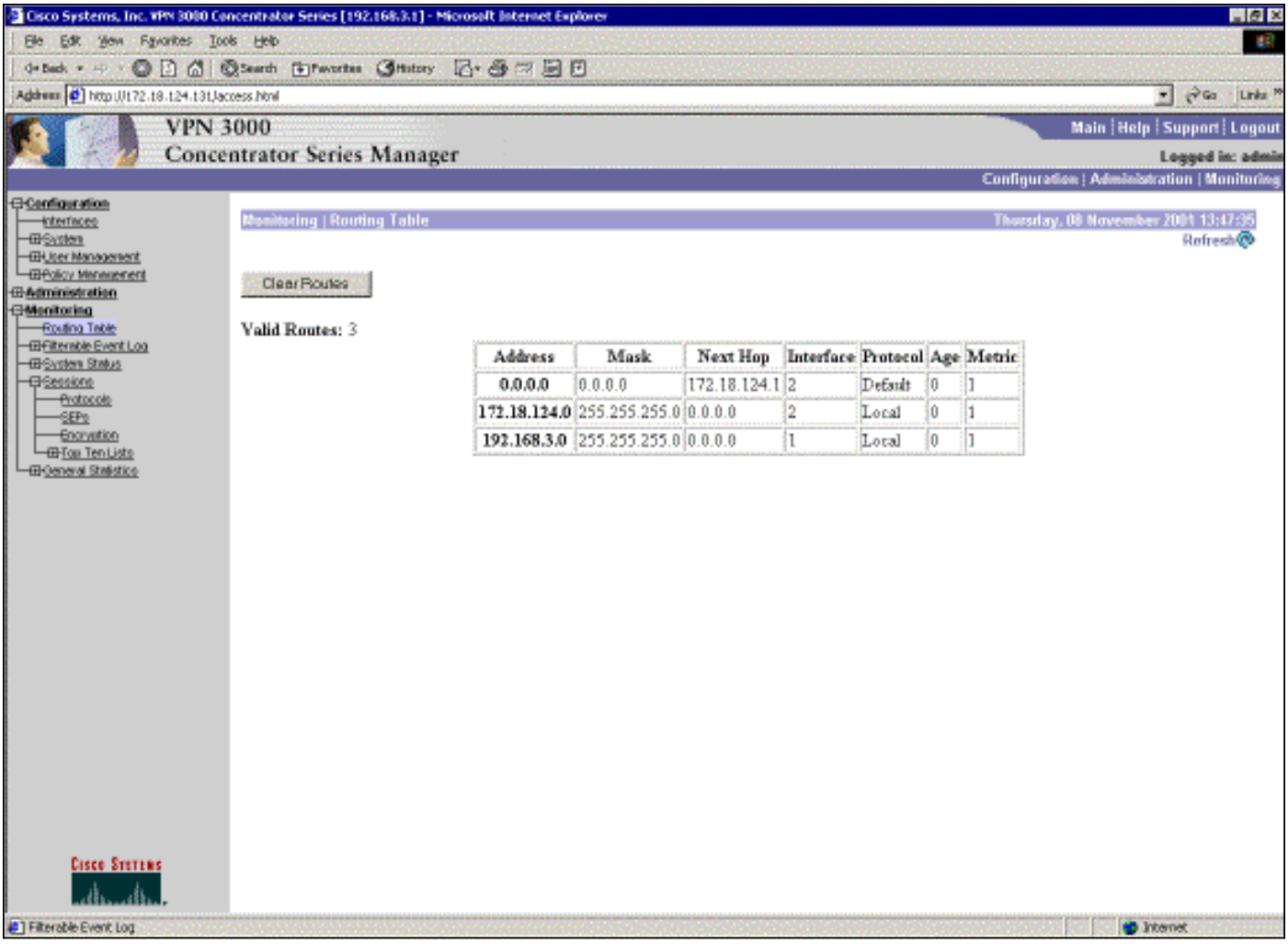


Netwerk 192.168.1.x is het enige netwerk hier en kan via de VPN-tunnel worden bereikt. Er is geen netwerk van 192.168.2.0 aangezien geen proces (zoals RIP) langs die route loopt. Er gaat niets verloren zolang de PC's op het 192.168.3.x netwerk hun standaardgateway naar de VPN Concentrator niet richten. U kunt altijd een statische route toevoegen als u kiest. Echter, bij dit voorbeeld hoeft de VPN Concentrator zelf niet het 192.168.2.0-netwerk te bereiken.

Problemen oplossen

Gesimuleerde fout

Dit is een gesimuleerde fout in de configuratie. Als u het filter naar de openbare interface verwijdert, daalt de VPN-tunnel. Dit zorgt ervoor dat de route voor de 192.168.1.0 die door de tunnel is geleerd ook daalt. Het TNO-proces duurt ongeveer drie minuten om de route te verwijderen. Daarom kan je mogelijk een drie minuten vertraging hebben tot de route zelf uitkomt.



Zodra de route van RIP verloopt, lijkt de nieuwe routingtabel op de routers gelijkaardig aan dit:

```
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
```

Wat kan er fout gaan?

Als u vergeet de afstand voor de beheerder toe te voegen op 130, dan kunt u deze uitvoer zichtbaar maken. Merk op dat beide VPN tunnels omhoog zijn.

VPN 3800-concentratie

Opmerking: dit is de niet-grafische gebruikersinterface (GUI) versie van de routingtabel.

```
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
```

Om op het 192.168.3.0 netwerk te komen moet de route door 172.18.124.131 gaan. Echter, de routingtabel op RTR-3620 toont:

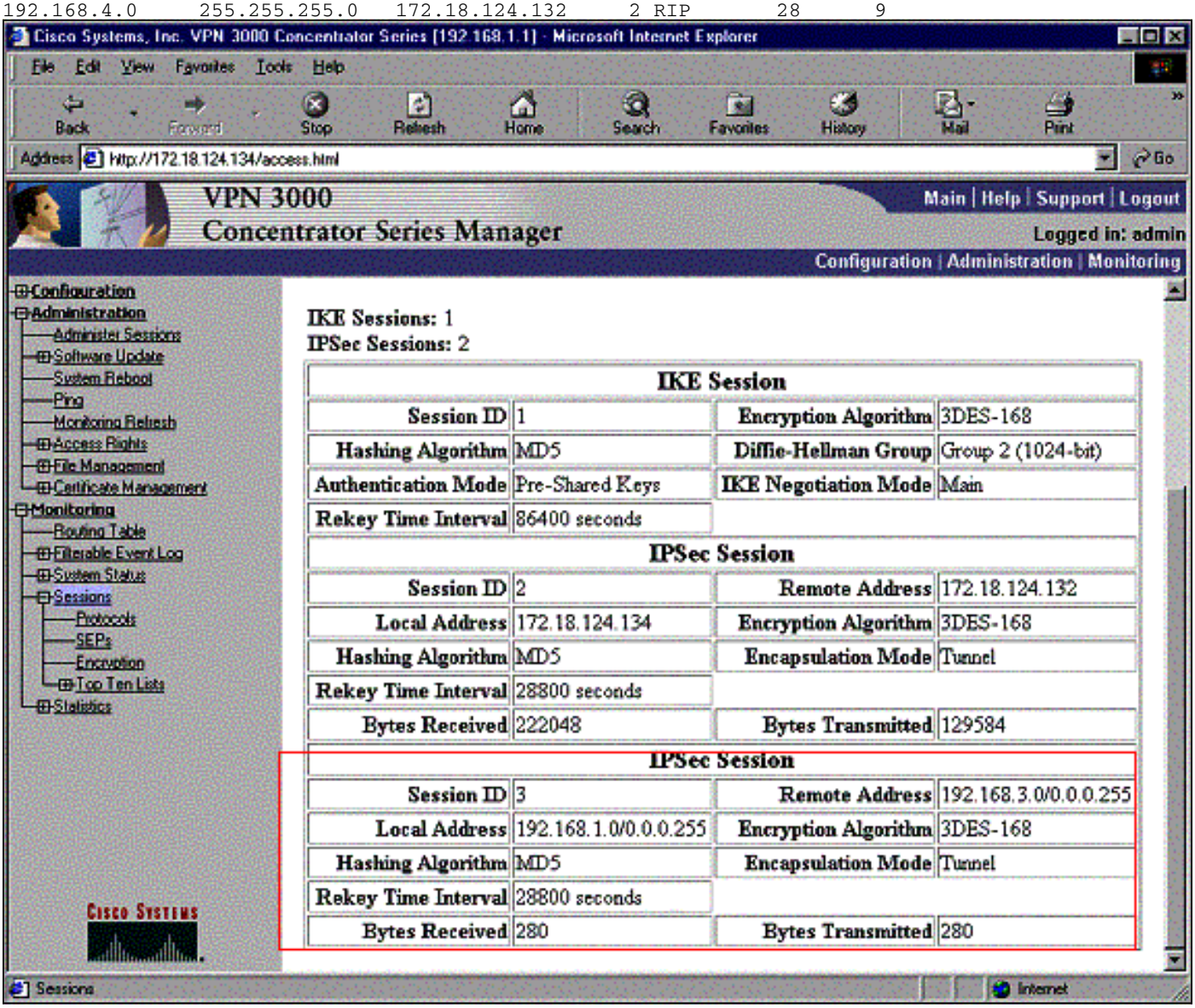
```
rtr-3620#show ip route

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
```

Om terug te keren naar het 192.168.1.0 netwerk, moet de route door het backbone 192.168.4.x netwerk gaan.

Het verkeer werkt nog steeds sinds de autodiscovery de juiste security associatie (SA) informatie over de VPN 3030b Concentrator genereren. Bijvoorbeeld:

```
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
```



Hoewel de routingtabel zegt dat de peer 172.18.124.131 moet zijn, is de echte SA (traffic flow) via de VPN 3030b-concentratie op 172.18.124.132. De SA-tabel heeft voorrang op de routeswittabel. Alleen nauwkeurig onderzoek van de routetabel en de SA-tabel in VPN 3060a Concentrator laat zien dat er geen verkeer in de juiste richting stroomt.

Gerelateerde informatie

- Ondersteuning van Cisco VPN 3000 Series Concentrator-pagina
- IPsec-ondersteuningspagina
- Technische ondersteuning - Cisco-systemen