Konfigurieren von redundantem Routing im VPN 3000-Konzentrator

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Konfigurieren
Netzwerkdiagramm
Router-Konfigurationen
Konfiguration des VPN 3080-Konzentrators
Konfiguration des VPN 3060a-Konzentrators
Konfiguration des VPN 3030b-Konzentrators
Überprüfen
Fehlerbehebung
Simulierter Fehler
Was kann schief gehen?
Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie ein redundantes VPN-Failover konfiguriert wird, wenn ein Remote-Standort den VPN 3000-Konzentrator oder die Internetverbindung verliert. In diesem Beispiel wird davon ausgegangen, dass das Unternehmensnetzwerk hinter dem VPN 3030B Open Shortest Path First (OSPF) als Standard-Routing-Protokoll verwendet.

Hinweis: Wenn Sie zwischen Routing-Protokollen neu verteilen, können Sie eine Routing-Schleife bilden, die im Netzwerk Probleme verursachen kann. OSPF wird in diesem Beispiel verwendet, es ist jedoch nicht das einzige Routing-Protokoll, das verwendet werden kann.

Ziel dieses Beispiels ist es, dass das Netzwerk 192.168.1.0 den roten Tunnel (unter normalen Betriebsbedingungen) verwendet, der im Abschnitt Netzwerkdiagramm dargestellt ist, um 192.168.3.x zu erreichen. Wenn der Tunnel, der VPN Concentrator oder der ISP verfällt, wird das Netzwerk 192.168.3.0 über ein dynamisches Routing-Protokoll über den grünen Tunnel erfasst. Außerdem geht die Verbindung zum 192.168.3.0-Standort nicht verloren. Sobald das Problem behoben ist, kehrt der Datenverkehr automatisch zum roten Tunnel zurück.

Hinweis: RIP verfügt über einen dreiminütigen Alterungs-Timer, bevor eine neue Route über eine ungültige Route akzeptiert werden kann. Gehen Sie außerdem davon aus, dass die Tunnel erstellt werden und der Datenverkehr zwischen den Peers übertragen werden kann.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Router 3620 und 3640
- Cisco VPN 3080 Concentrator - Version: Cisco Systems, Inc./VPN 300 Concentrator Version 4.7
- Cisco VPN 3060 Concentrator - Version: Cisco Systems, Inc./VPN Concentrator der Serie 3000 Version 4.7
- Cisco VPN 3030 Concentrator - Version: Cisco Systems, Inc./VPN Concentrator der Serie 3000 Version 4.7

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

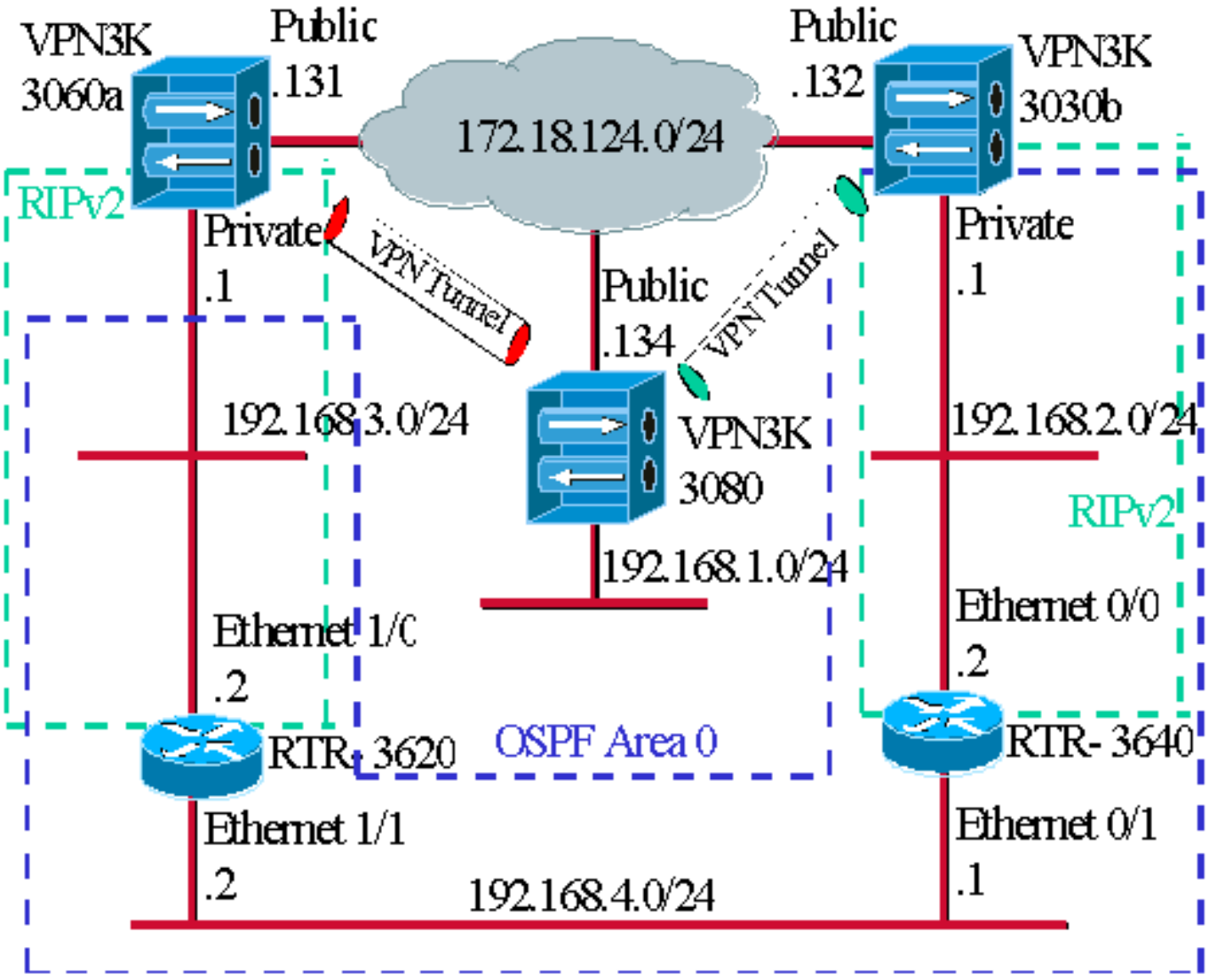
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das Command Lookup Tool (nur registrierte Kunden).

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Die blauen Bindestriche zeigen an, dass OSPF von VPN 3030b bis RTR-3640 und RTR-3620 aktiviert ist.

Die grünen Bindestriche zeigen an, dass RIPv2 vom privaten VPN 3060a zum RTR-3620, RTR-3640 und privaten VPN 3030b aktiviert ist.

RIPv2 ist auch in den roten und grünen VPN-Tunneln aktiviert, da die Netzwerkerkennung aktiviert ist. Die Aktivierung von RIP auf der privaten VPN 3080-Schnittstelle ist nicht erforderlich. Darüber hinaus gibt es im Netzwerk 192.168.4.x kein RIP, da OSPF alle Routen über diese Verbindung erfasst.

Hinweis: Bei PCs in den Netzwerken 192.168.2.x und 192.168.3.x müssen die Standard-Gateways auf die Router und nicht auf die VPN-Konzentratoren verweisen. Lassen Sie die Router entscheiden, wohin die Pakete weitergeleitet werden sollen.

Router-Konfigurationen

In diesem Dokument werden folgende Routerkonfigurationen verwendet:

- 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
```

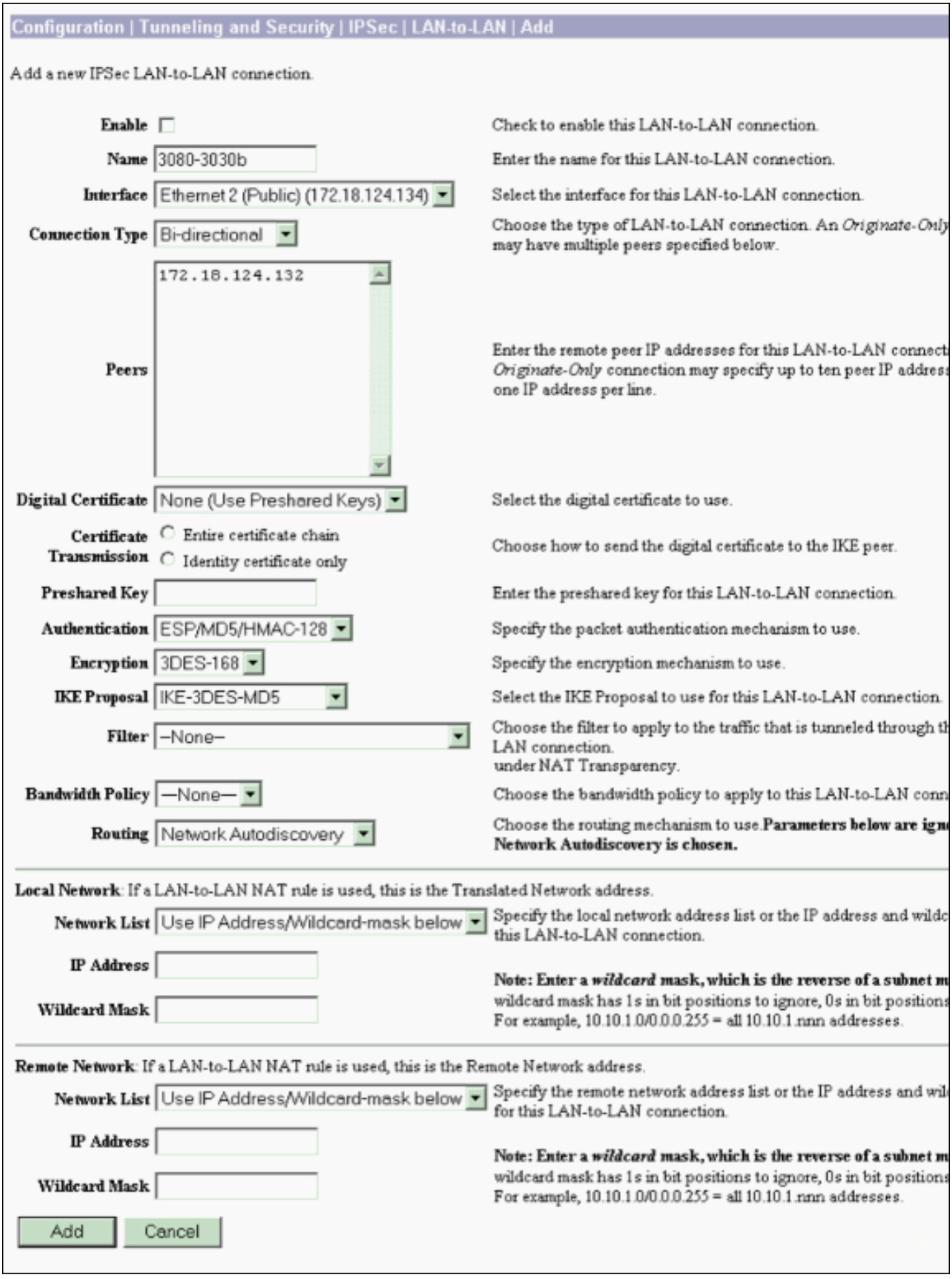
```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rtr-3640
!
ip subnet-zero
!
interface Ethernet0/0
 ip address 192.168.2.2 255.255.255.0
 half-duplex
!
interface Ethernet0/1
 ip address 192.168.4.1 255.255.255.0
 half-duplex
!
router ospf 1
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

Konfiguration des VPN 3080-Konzentrators

LAN-to-LAN VPN 3080 zu VPN 3030b

Wählen Sie **Configuration > Tunneling and Security > IPSec > IPSec LAN-to-LAN aus**. Da Network Autodiscovery verwendet wird, müssen die Listen für das lokale und das Remote-Netzwerk nicht ausgefüllt werden.

Hinweis: VPN Concentrators, die die Software Version 3.1 und früher ausführen, verfügen über ein Kontrollkästchen für die automatische Erkennung. Die Softwareversion 3.5 (für VPN 3080 verwendet) verwendet ein Dropdown-Menü, z. B. das hier abgebildete Menü.

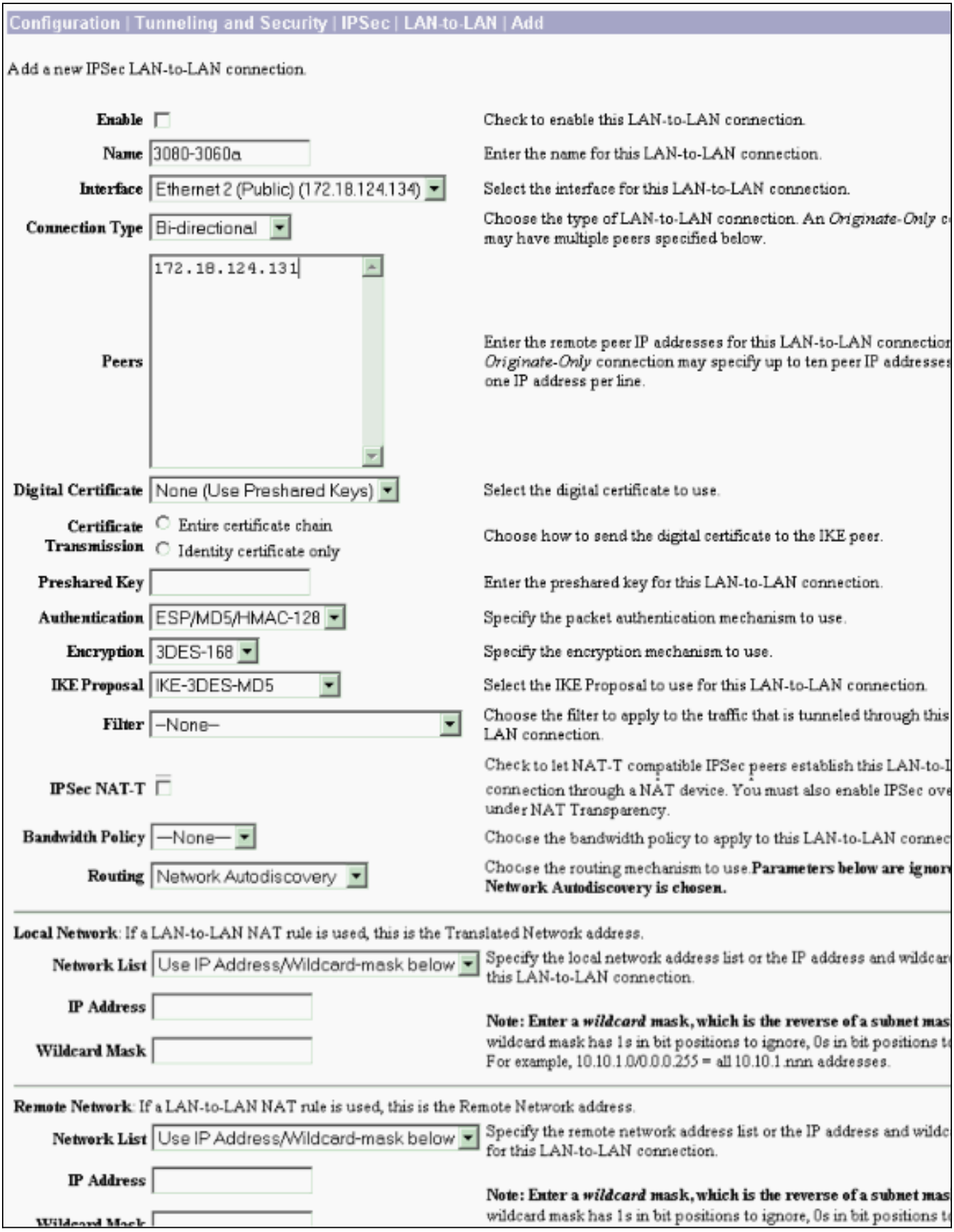


[LAN-to-LAN VPN 3080 zu VPN 3060a]

Wählen Sie **Configuration > Tunneling and Security > IPSec > IPSec LAN-to-LAN aus**. Da

Network Autodiscovery verwendet wird, müssen die Listen für das lokale und das Remote-Netzwerk nicht ausgefüllt werden.

Hinweis: VPN Concentrators, die die Software Version 3.1 und früher ausführen, verfügen über ein Kontrollkästchen für die automatische Erkennung. Die Softwareversion 3.5 (für VPN 3080 verwendet) verwendet ein Dropdown-Menü, z. B. das hier abgebildete Menü.

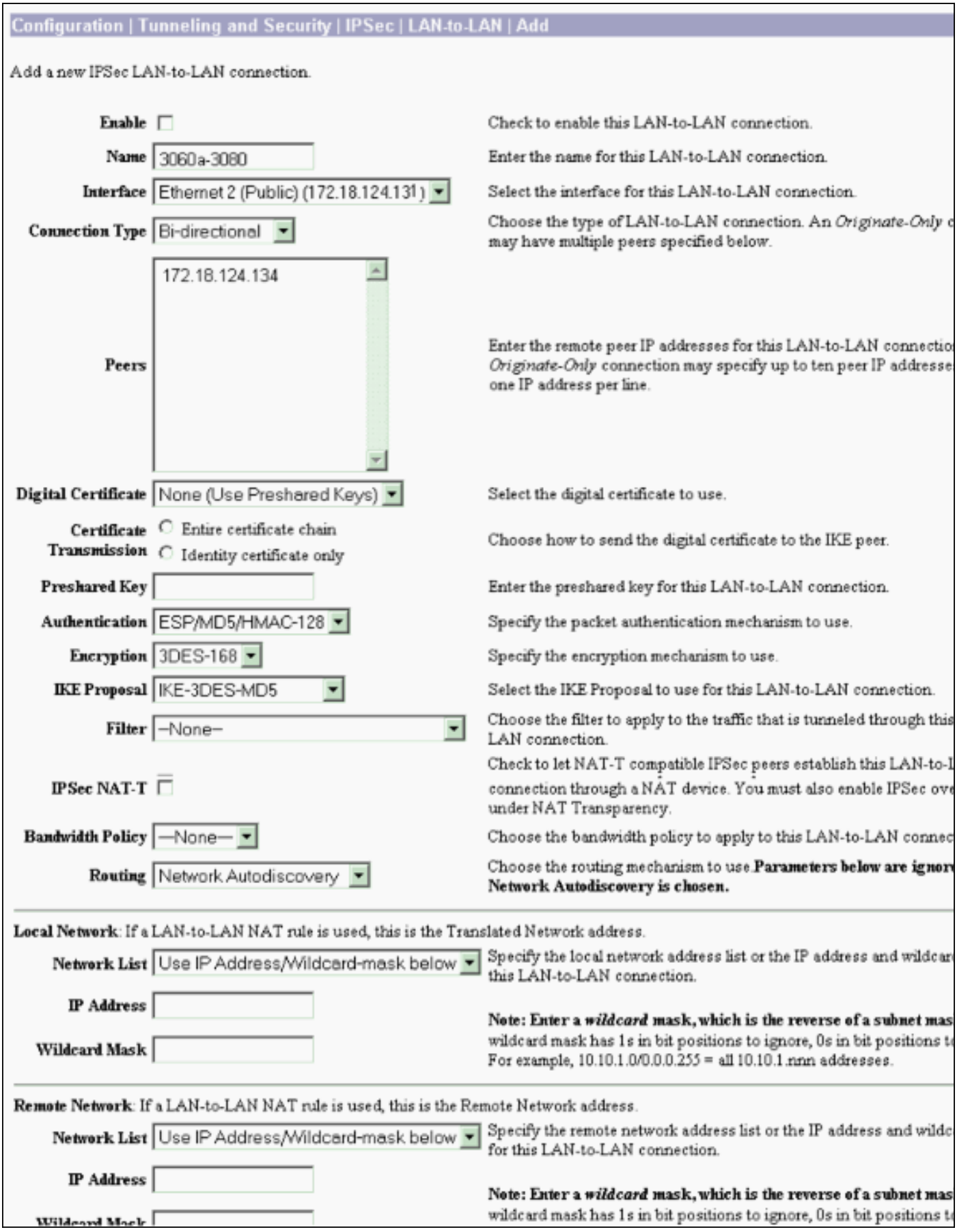


Konfiguration des VPN 3060a-Konzentrators

LAN-to-LAN VPN 3060a zu VPN 3080

Wählen Sie **Configuration > Tunneling and Security > IPSec > IPSec LAN-to-LAN aus**.

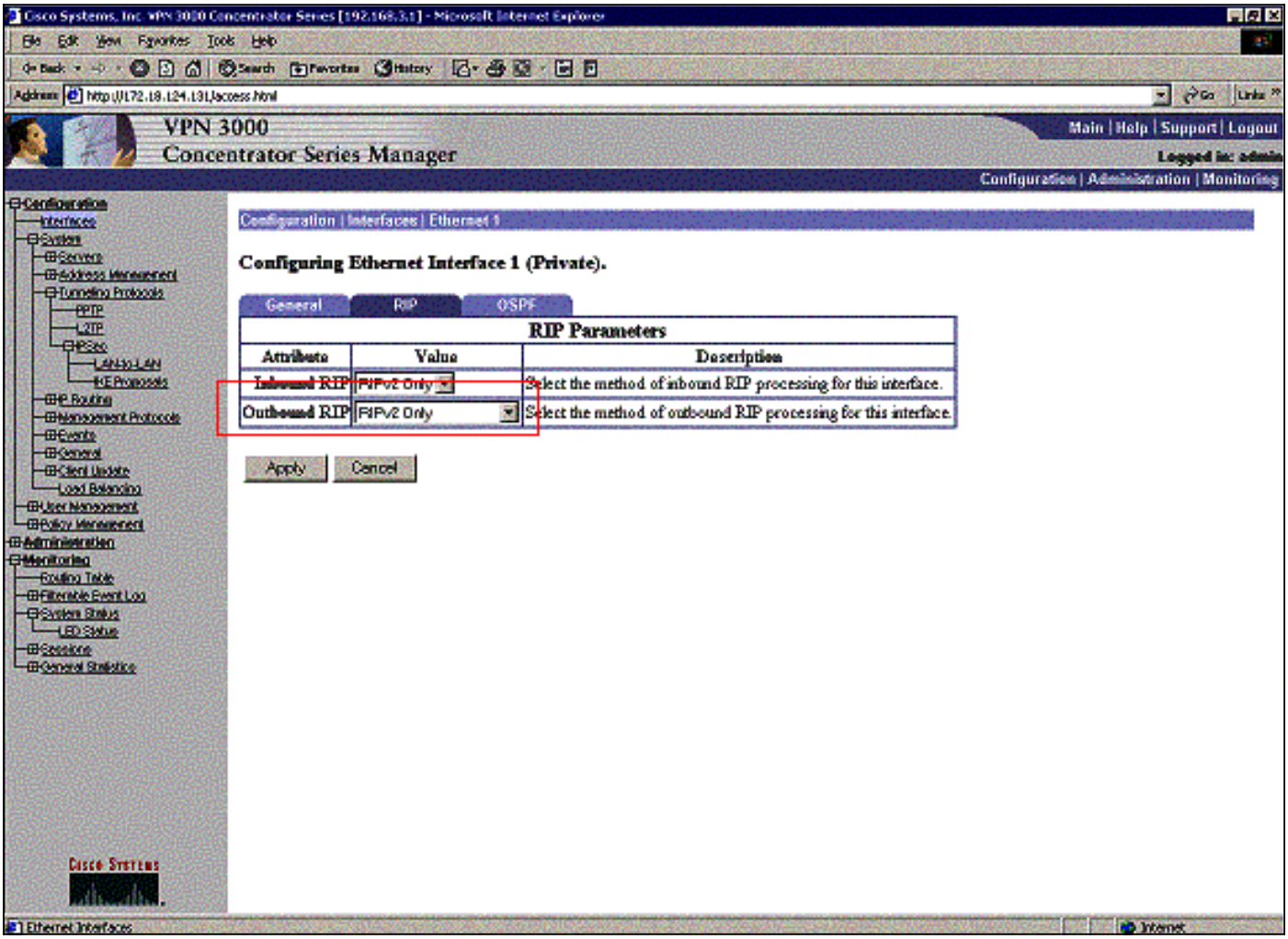
Hinweis: Auf dem VPN 3060 steht anstelle des Dropdown-Menüs ein Kontrollkästchen für "Network Autodiscovery" (für automatische Netzwerkerkennung), wie in der Softwareversion 3.5 und höher, zur Verfügung.



Aktivieren Sie RIP, um die Tunnel-gelernten Routen an den VPN 3620-Router zu übergeben.

Wählen Sie **Konfiguration > Schnittstellen > Privat > RIP aus**. Ändern Sie das Dropdown-Menü in **Nur RIPv2**, und klicken Sie auf **Übernehmen**. Wählen Sie dann **Configuration > System > Tunneling Protocols > IPSec > LAN-to-LAN aus**.

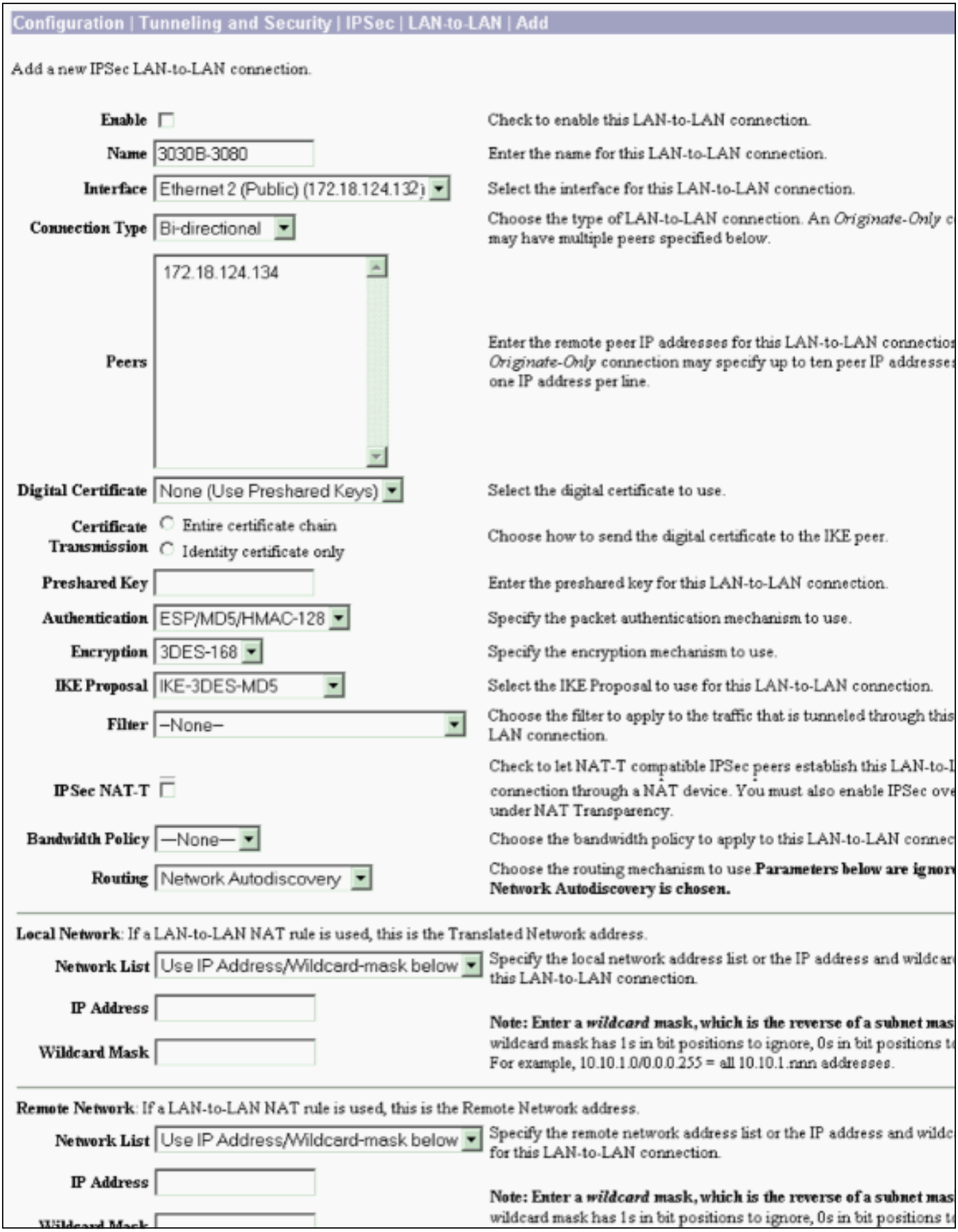
Hinweis: Der Standardwert ist "Outbound RIP" (Ausgehender RIP) und "Deaktiviert" (deaktiviert) für die private Schnittstelle.



Konfiguration des VPN 3030b-Konzentrators

LAN-to-LAN VPN 3030b zu VPN 3080

Wählen Sie **Configuration > Tunneling and Security > IPSec > LAN-to-LAN aus**.



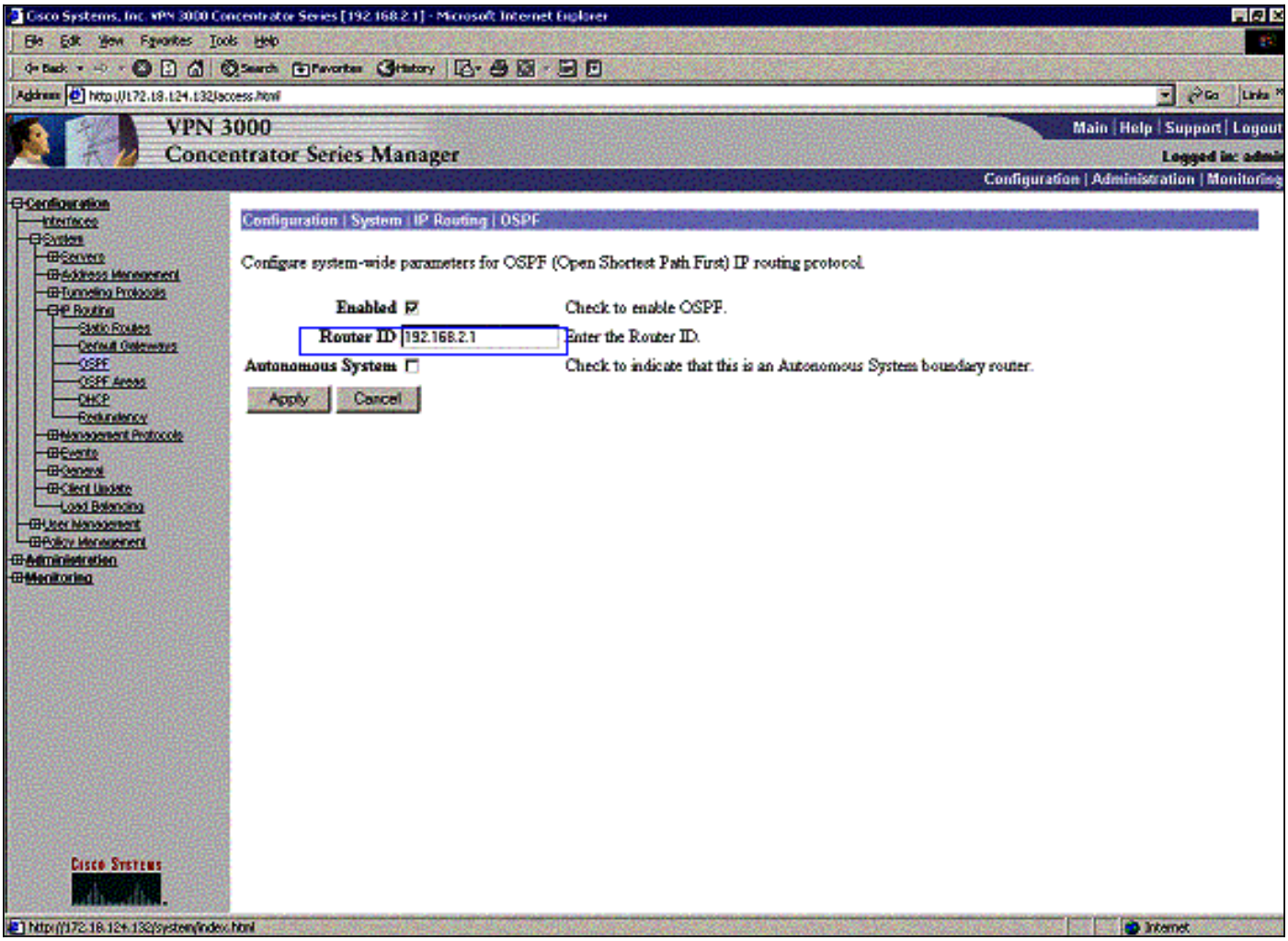
[Aktivieren Sie RIP, um die Tunnel-gelernten Routen an den VPN 3640-Router zu übergeben.]

Folgen Sie den oben in diesem Dokument aufgeführten Schritten für [VPN 3060a Concentrator].

[Aktivieren Sie OSPF, um die Backbone-gelernten Routen an den VPN 3030b-Concentrator]

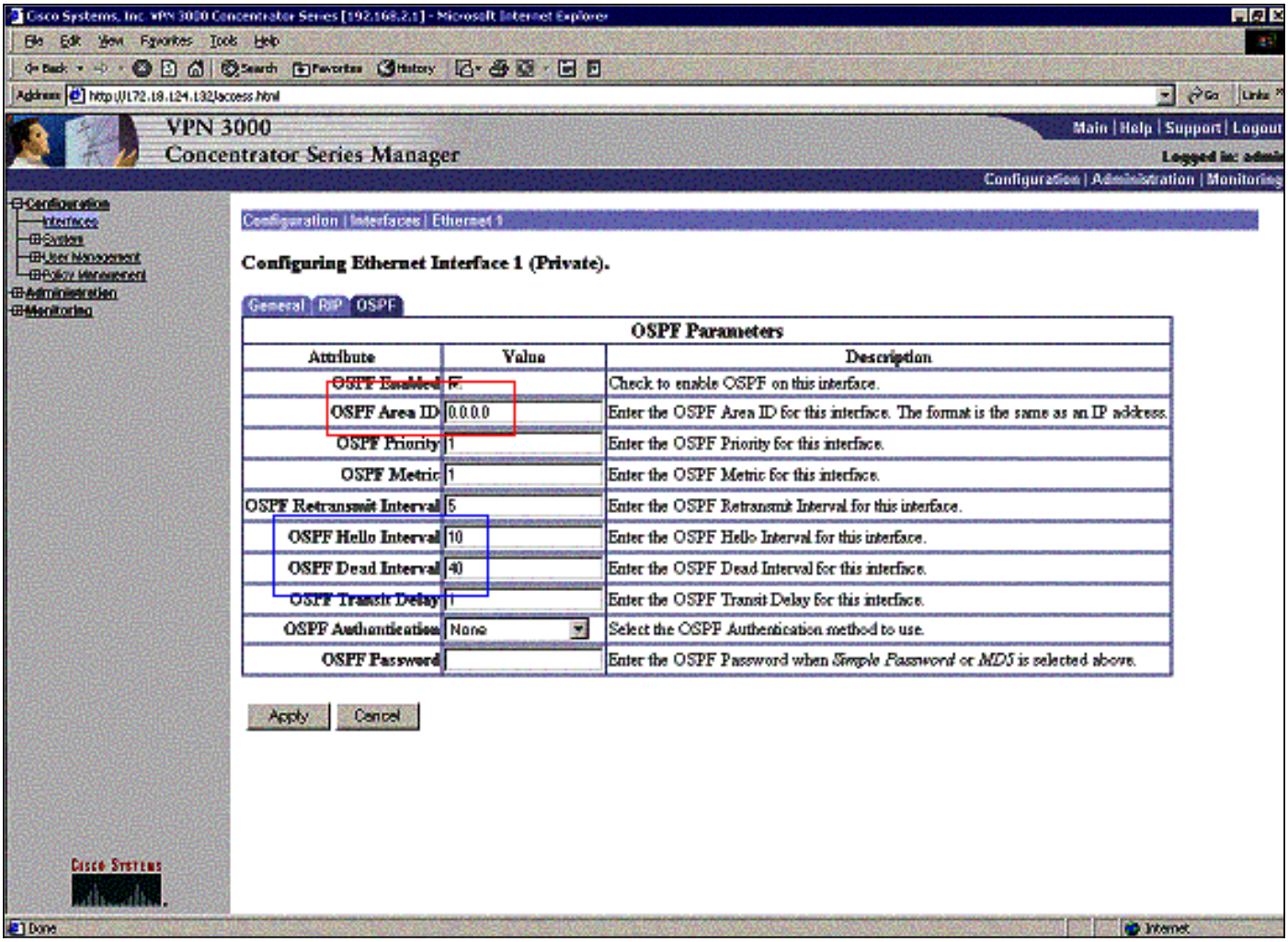
weiterzuleiten.

Wählen Sie **Configuration > System > IP Routing > OSPF aus,** und geben Sie die Router-ID ein.




```
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
```

Die Bereich-ID muss mit der ID auf der Leitung übereinstimmen. Da der Bereich in diesem Beispiel 0 ist, wird er durch 0.0.0.0 dargestellt. Aktivieren Sie außerdem das Kontrollkästchen **OSPF aktivieren**, und klicken Sie auf **Übernehmen**.



Stellen Sie sicher, dass Ihre OSPF-Timer mit denen des Routers übereinstimmen. Um die Router-Timer zu überprüfen, verwenden Sie den Befehl **show ip ospf interface *<Schnittstellenname>*.**

```
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)
```

Weitere Informationen zu OSPF finden Sie in RFC 1247 .

Überprüfen

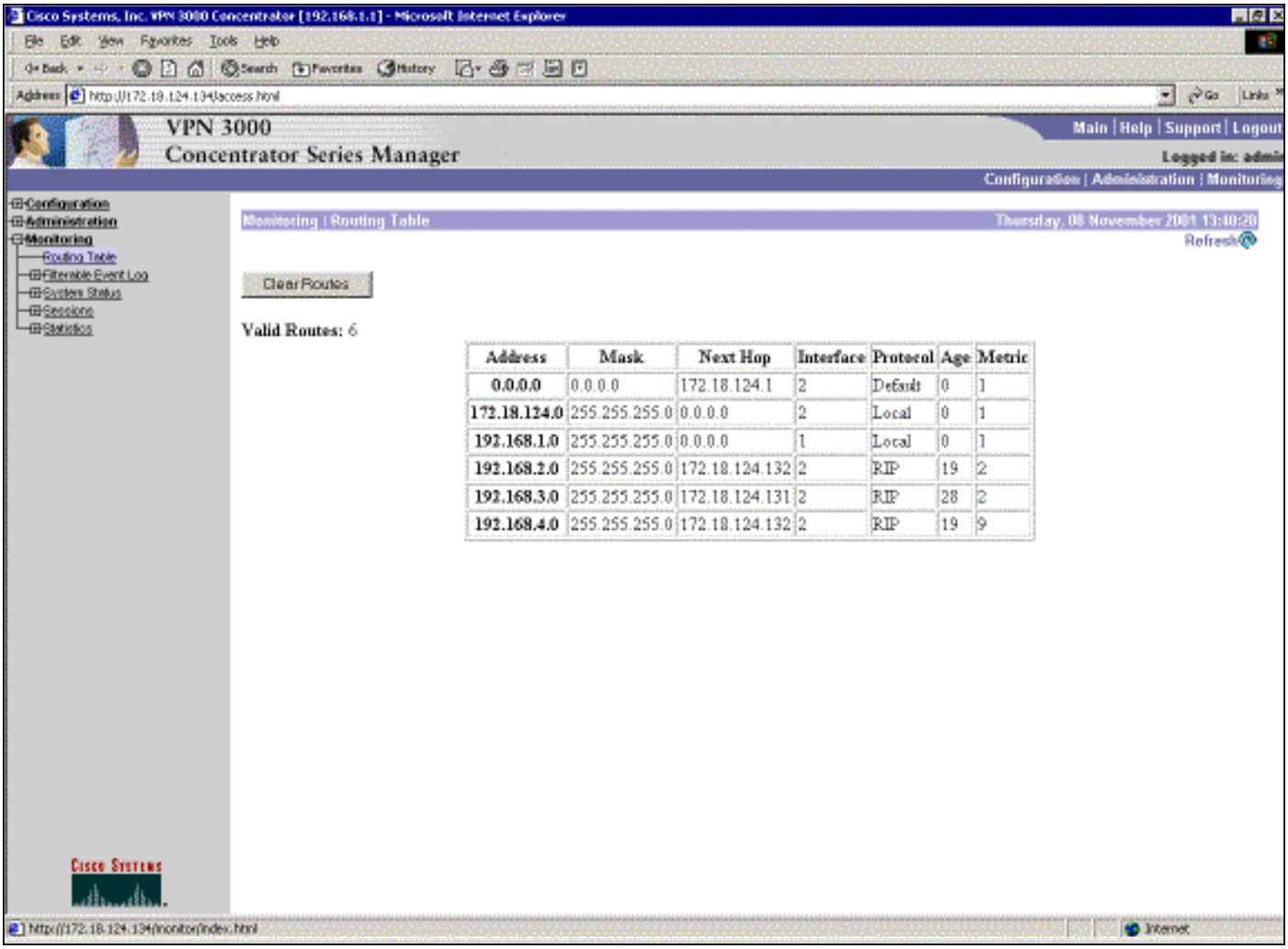
Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

Diese Befehlsausgabe zeigt genaue Routing-Tabellen an.

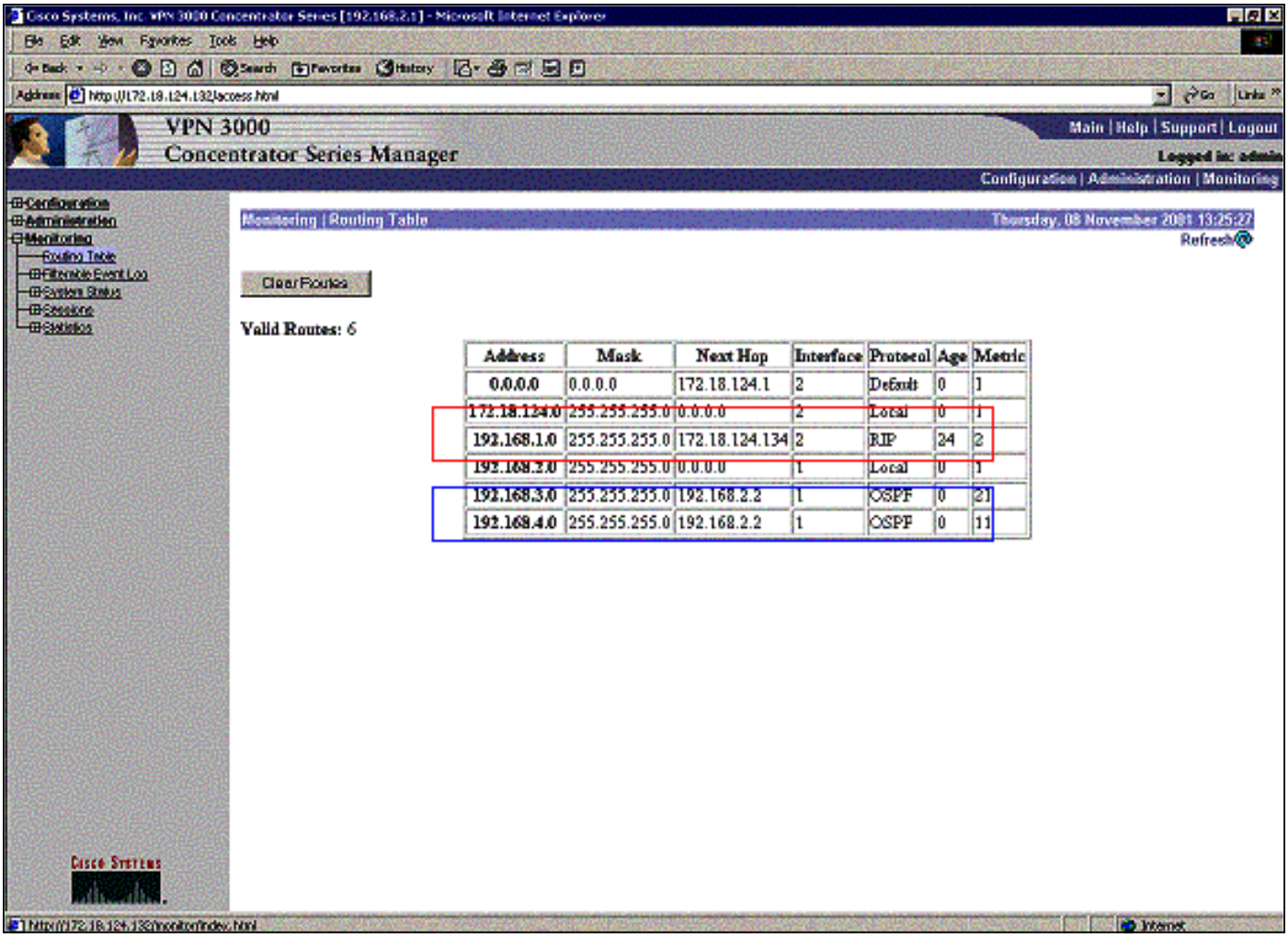
```
rtr-3620#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

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
```

Dies ist die VPN 3080 Concentrator-Routing-Tabelle unter normalen Umständen.



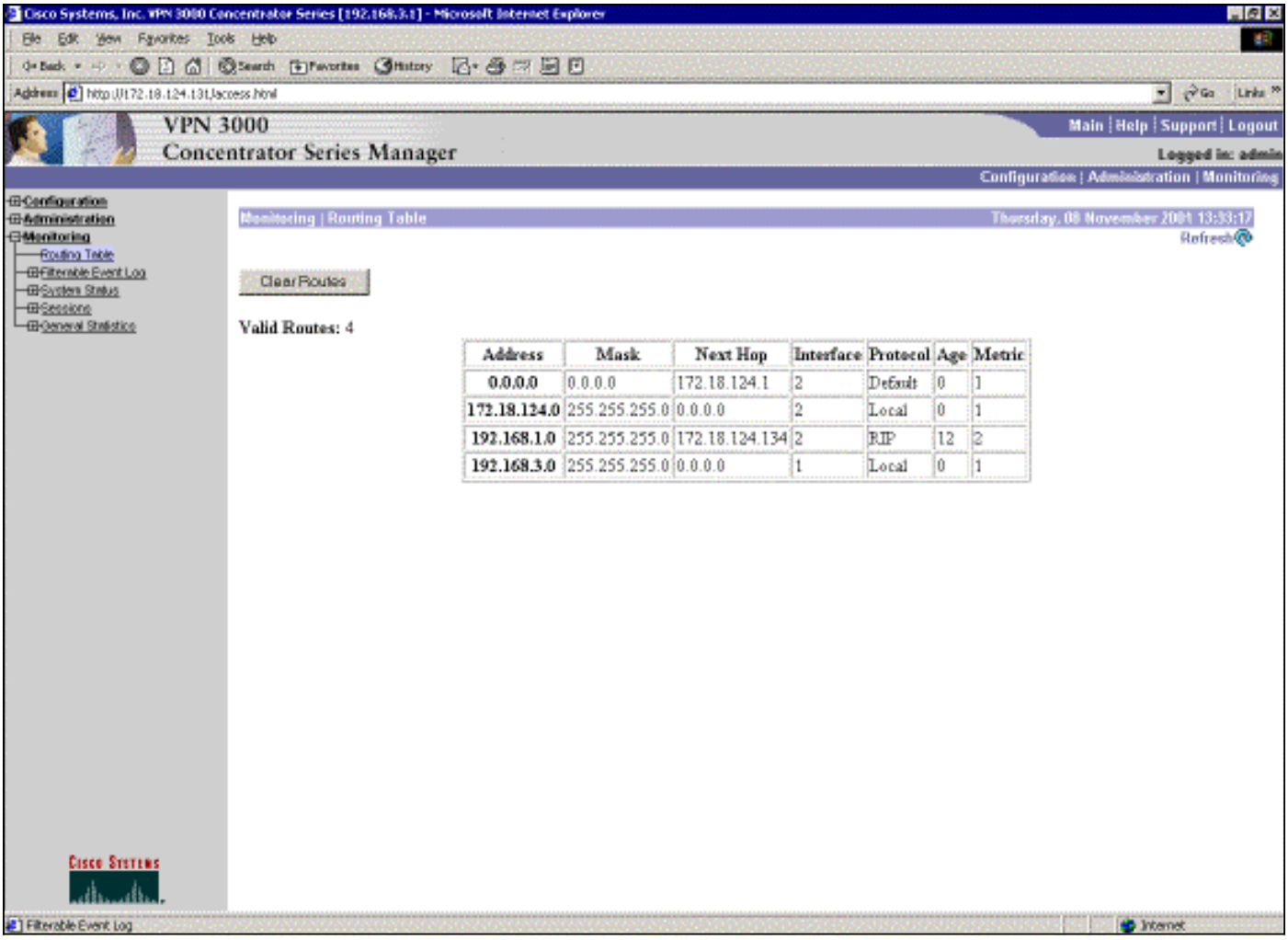
Die Netzwerke 192.168.2.x und 192.168.3.x werden beide durch die VPN-Tunnel 172.18.124.132 bzw. 172.18.124.131 erfasst. Das Netzwerk 192.168.4.x wird durch den Tunnel 172.18.124.132 erfasst, da die OSPF-Anzeigen des Routers in die Routing-Tabelle des VPN 3030b-Konzentrators eingefügt werden. Anschließend informiert die Routing-Tabelle die Remote-VPN-Peers über das Netzwerk.

Dies ist die VPN 3030b Concentrator-Routing-Tabelle unter normalen Umständen.



Das rote Kästchen zeigt an, dass das Netzwerk 192.168.1.x aus dem VPN-Tunnel gelernt wird. Die blaue Box zeigt, dass die Netzwerke 192.168.3.x und 192.168.4.x durch den OSPF-Kernprozess gelernt werden.

Dies ist die Routing-Tabelle des VPN-Concentrators 3060a unter normalen Umständen.

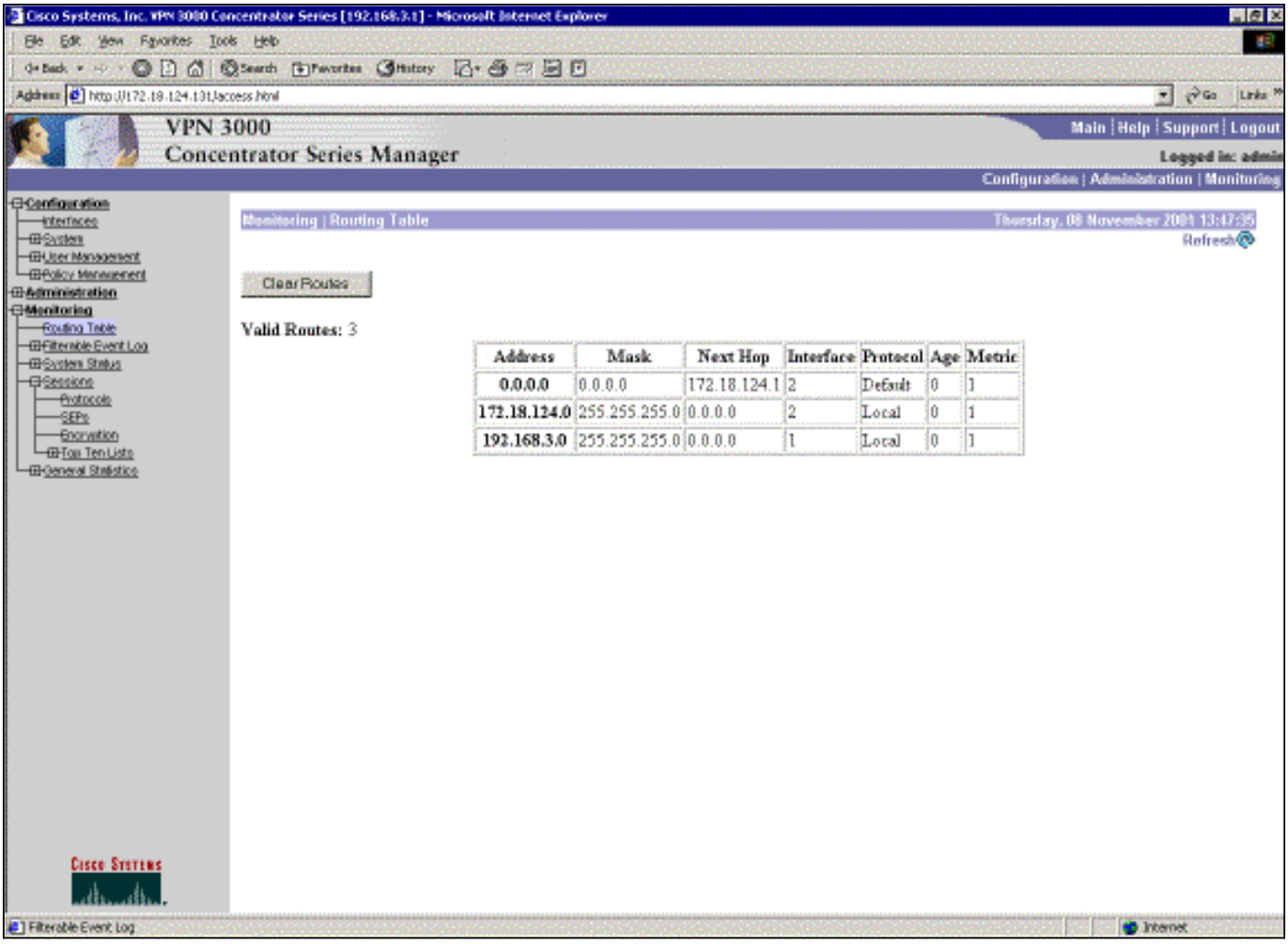


Das Netzwerk 192.168.1.x ist hier das einzige Netzwerk, das über den VPN-Tunnel erreicht werden kann. Es gibt kein 192.168.2.0-Netzwerk, da an dieser Route kein Prozess (z. B. RIP) verläuft. Es geht nichts verloren, solange die PCs im Netzwerk 192.168.3.x ihr Standard-Gateway nicht auf den VPN-Konzentrator verweisen. Sie können jederzeit eine statische Route hinzufügen. In diesem Beispiel muss der VPN-Konzentrator selbst jedoch nicht das Netzwerk 192.168.2.0 erreichen.

Fehlerbehebung

Simulierter Fehler

Dies ist ein simulierter Fehler in der Konfiguration. Wenn Sie den Filter zur öffentlichen Schnittstelle entfernen, wird der VPN-Tunnel verworfen. Dadurch wird auch die Route für den 192.168.1.0, der durch den Tunnel gelernt wurde, unterbrochen. Das Entfernen der Route durch den RIP-Prozess dauert etwa drei Minuten. Daher kann es zu einem Ausfall von drei Minuten kommen, bis die Route selbst das Zeitlimit überschreitet.



Nach Ablauf der RIP-Route erscheint die neue Routing-Tabelle auf den Routern ähnlich der folgenden:

```
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
```

Was kann schief gehen?

Wenn Sie vergessen, die Admin-Distanz zu 130 hinzuzufügen, dann können Sie diese Ausgabe möglicherweise sehen. Beachten Sie, dass beide VPN-Tunnel aktiv sind.

[VPN 3080 Concentrator](#)

Hinweis: Dies ist die nicht grafische Benutzeroberfläche (GUI)-Version der Routing-Tabelle.

```
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
```

Um zum Netzwerk 192.168.3.0 zu gelangen, muss die Route über 172.18.124.131 geleitet werden. Die Routing-Tabelle auf RTR-3620 zeigt jedoch Folgendes:

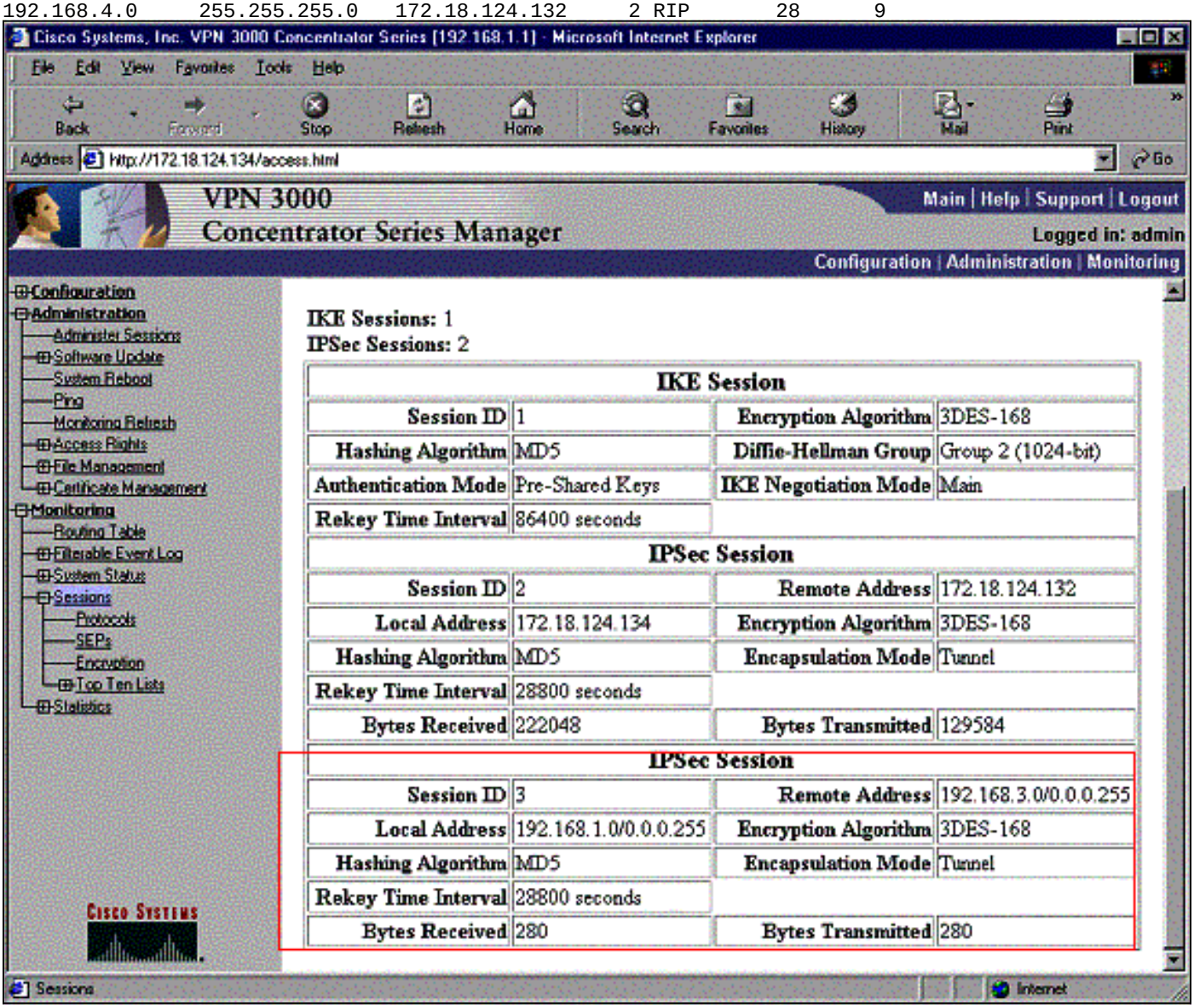
```
rtr-3620#show ip route

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
```

Um zum Netzwerk 192.168.1.0 zurückzukehren, muss die Route das Backbone-Netzwerk 192.168.4.x durchlaufen.

Der Datenverkehr funktioniert weiterhin, da die automatische Erkennung die richtigen SA-Informationen (Security Association) für den VPN 3030b-Konzentrator generiert. Beispiel:

```
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
```



Die Routing-Tabelle besagt, dass der Peer 172.18.124.131 sein soll, jedoch wird die tatsächliche SA (Datenverkehrsfluss) über den VPN 3030b-Konzentrator mit 172.18.124.132 geleitet. Die SA-Tabelle hat Vorrang vor der Routing-Tabelle. Nur eine genaue Untersuchung der Routing-Tabelle und der SA-Tabelle im VPN 3060a-Konzentrator zeigt, dass der Datenverkehr nicht in die richtige Richtung fließt.

Zugehörige Informationen

- Support-Seite für Cisco VPN Concentrator der Serie 3000
- IPSec-Support-Seite
- Technischer Support - Cisco Systems