VPN 3000 Concentrator 冗長なルーティング設定

目次

[はじめに](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[設定](#)
[ネットワーク図](#)
[ルータの設定](#)
[VPN 3080 コンセントレータの設定](#)
[VPN 3060a コンセントレータの設定](#)
[VPN 3030b コンセントレータの設定](#)
[確認](#)
[トラブルシューティング](#)
[シミュレートされた欠陥](#)
[不具合の原因](#)
[関連情報](#)

はじめに

このドキュメントでは、リモート サイトの VPN 3000 コンセントレータまたはインターネット接続が失われた場合の冗長 VPN フェールオーバーを設定する方法について説明します。 この例では、VPN 3030B の背後にある企業ネットワークがデフォルトのルーティング プロトコルとして Open Shortest Path First（OSPF）を使用すると仮定します。

注: ルーティング プロトコル間で再配布を行う場合、ネットワークで問題を引き起こす可能性があるルーティング ループを形成することがあります。 OSPF がこの例で使用されますが、使用できる唯一のルーティング プロトコルではありません。

この例の目的は、192.168.1.0 のネットワークで、「ネットワーク図」セクションに示されている赤色のトンネル（通常の稼働状況で）を使用して 192.168.3.x に到達させることです。 トンネル、VPN コンセントレータ、または ISP がドロップした場合、192.168.3.0 ネットワークは緑色のトンネル上でダイナミック ルーティング プロトコルを学習します。 また、192.168.3.0 サイトへの接続は失われません。 問題が解決されると、トラフィックは赤色のトンネルに自動的に戻ります。

注: 無効なルートから新しいルートを受け入れ可能な状態にするまで、RIP には 3 分間のエージング タイマーがあります。 また、トンネルが作成され、トラフィックがピア間を経過できると仮定します。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Nexus 3620 および 3640
- Cisco VPN 3080 コンセントレータ - バージョン： Cisco Systems, Inc./VPN 3000 コンセントレータ バージョン 4.7
- Cisco VPN 3060 コンセントレータ - バージョン： Cisco Systems, Inc./VPN 3000 コンセントレータ シリーズ バージョン 4.7
- Cisco VPN 3030 コンセントレータ - バージョン： Cisco Systems, Inc./VPN 3000 コンセントレータ シリーズ バージョン 4.7

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

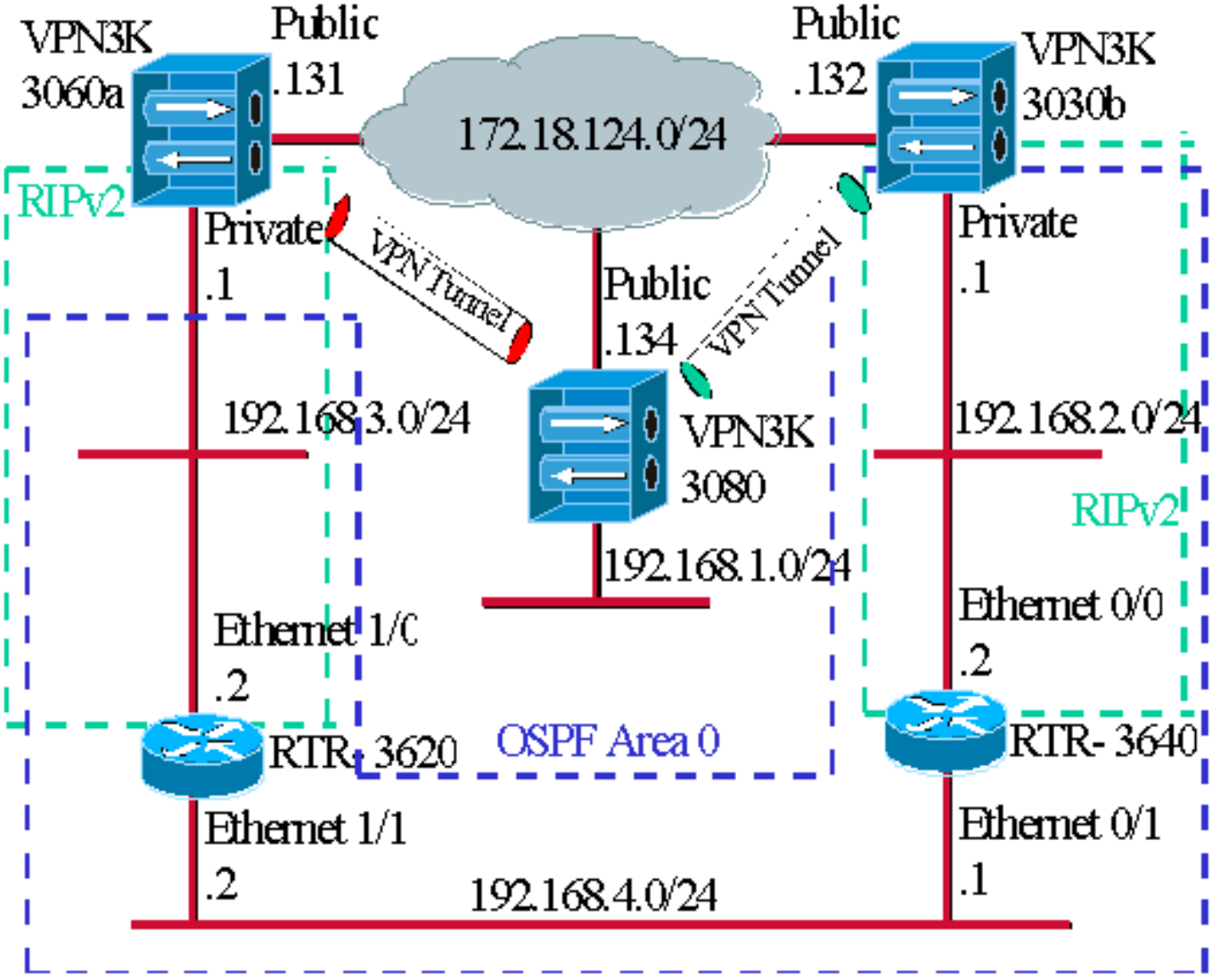
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



青色の点線は、OSPF が VPN 3030b から RTR-3640、RTR-3620 まで有効であることを示します。

緑色の点線は、RIPv2 がプライベート VPN 3060a から RTR-3620、RTR-3640、プライベート VPN 3030b まで有効であることを示します。

また、ネットワーク検出が有効になっているため、赤色と緑色の VPN トンネルで RIPv2 が有効になっています。 VPN 3080 プライベート インターフェイスで RIP を有効にする必要はありません。 このリンク上の OSPF によってすべてのルートが学習されているため、192.168.4.x ネットワークには RIP はありません。

注: 192.168.2.x と 192.168.3.x のネットワーク上の PC に、VPN コンセントレータではなく、ルータを指すデフォルト ゲートウェイが必要になります。 ルータがパケットをどこにルーティングするか決定できるようにします。

ルータの設定

このドキュメントでは、次のルータ設定を使用します。

- ルータ 3620
- ルータ 3640

ルータ 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
```

ルータ 3640

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

Current configuration : 1129 bytes
!
version 12.2
```

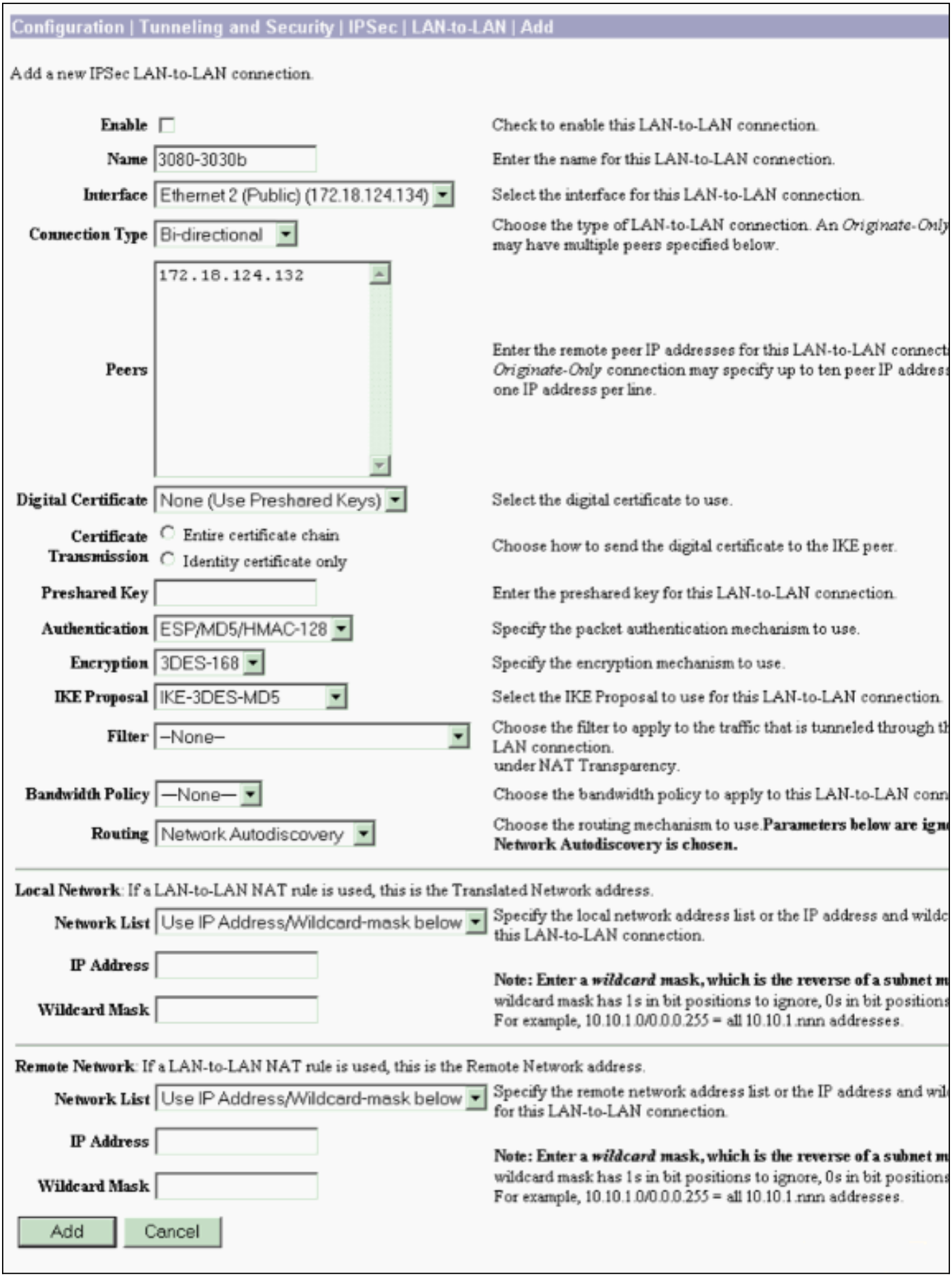
```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rtr-3640
!
ip subnet-zero
!
interface Ethernet0/0
 ip address 192.168.2.2 255.255.255.0
 half-duplex
!
interface Ethernet0/1
 ip address 192.168.4.1 255.255.255.0
 half-duplex
!
router ospf 1
 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 3080 コンセントレータの設定

VPN 3080 から VPN 3030b への LAN-to-LAN

[Configuration] > [Tunneling and Security] > [IPSec] > [IPSec LAN-to-LAN] の順に選択します。 ネットワーク自動検出が使用されているため、ローカルおよびリモート ネットワークのリストに入力する必要はありません。

注: ソフトウェア バージョン 3.1 以前を実行する VPN コンセントレータには自動検出のチェックボックスがあります。 ソフトウェア バージョン 3.5 (VPN 3080 で使用) では、次に示すようなドロップダウン メニューが使用されます。

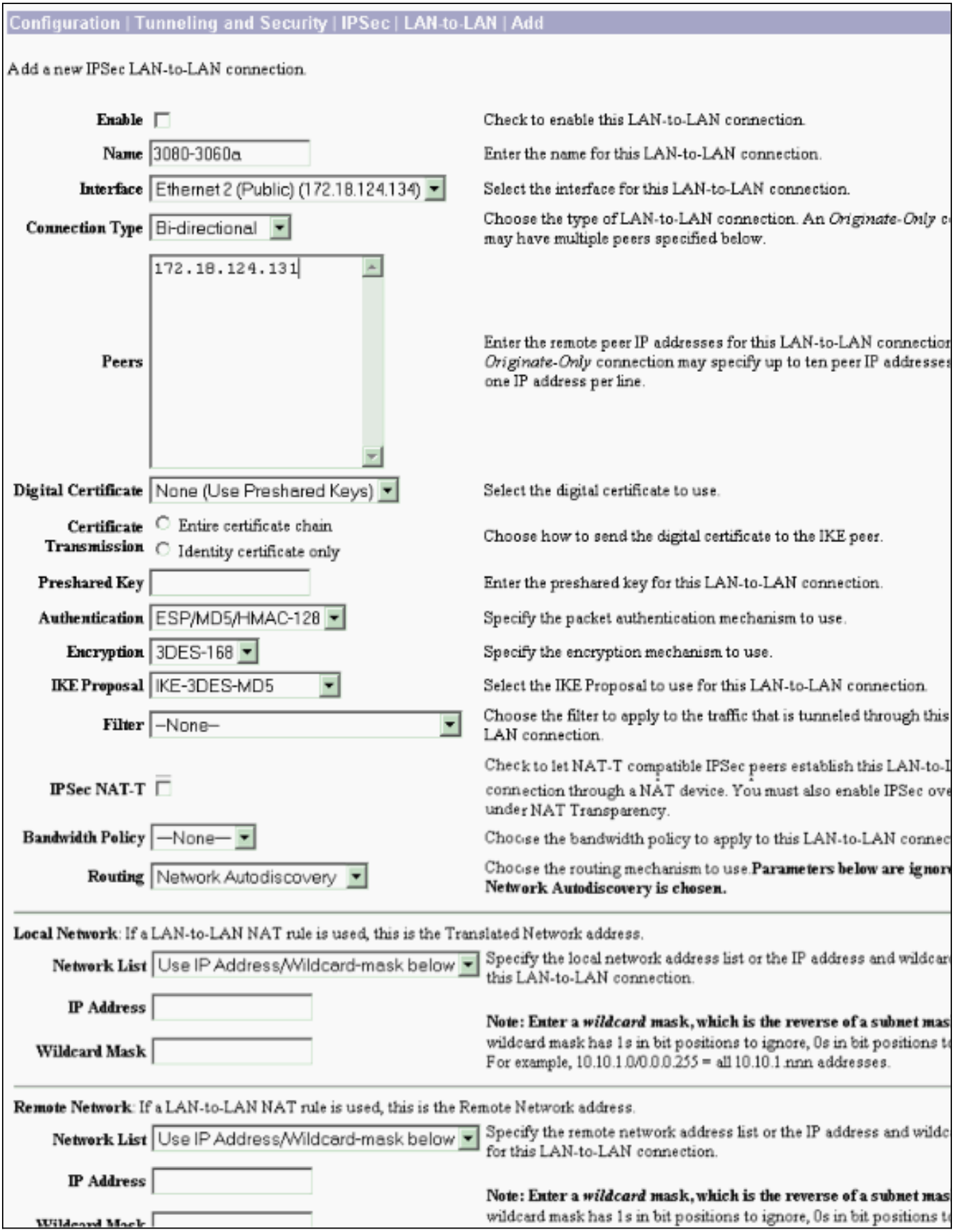


VPN 3080 から VPN 3060a への LAN-to-LAN

[Configuration] > [Tunneling and Security] > [IPSec] > [IPSec LAN-to-LAN] の順に選択します。 ネ

ットワーク自動検出が使用されているため、ローカルおよびリモート ネットワークのリストに入力する必要はありません。

注: ソフトウェア バージョン 3.1 以前を実行する VPN コンセントレータには自動検出のチェックボックスがあります。 ソフトウェア バージョン 3.5（VPN 3080 で使用）では、次に示すようなドロップダウン メニューが使用されます。

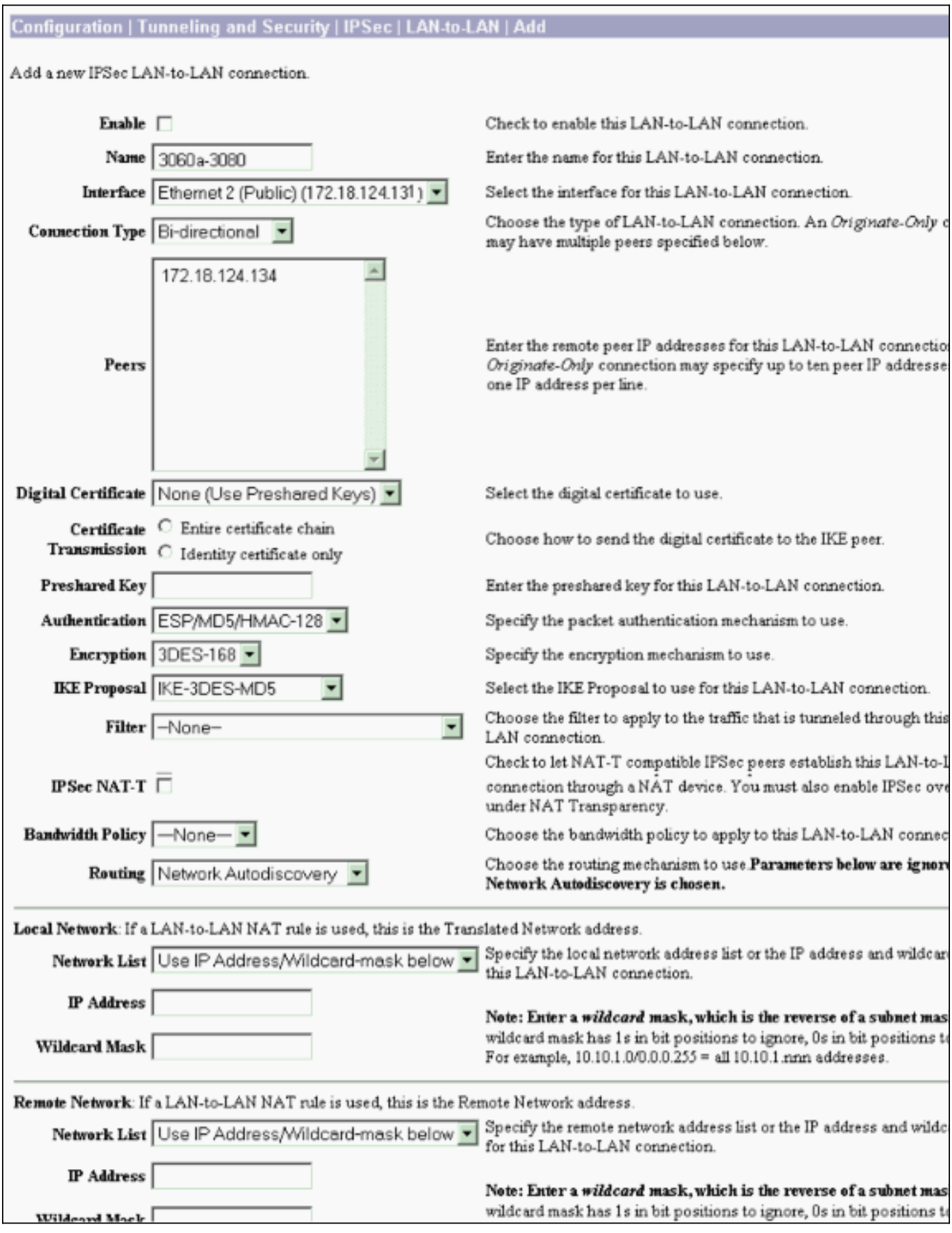


VPN 3060a コンセントレータの設定

VPN 3060a から VPN 3080 への LAN-to-LAN

[Configuration] > [Tunneling and Security] > [IPSec] > [IPSec LAN-to-LAN] の順に選択します。

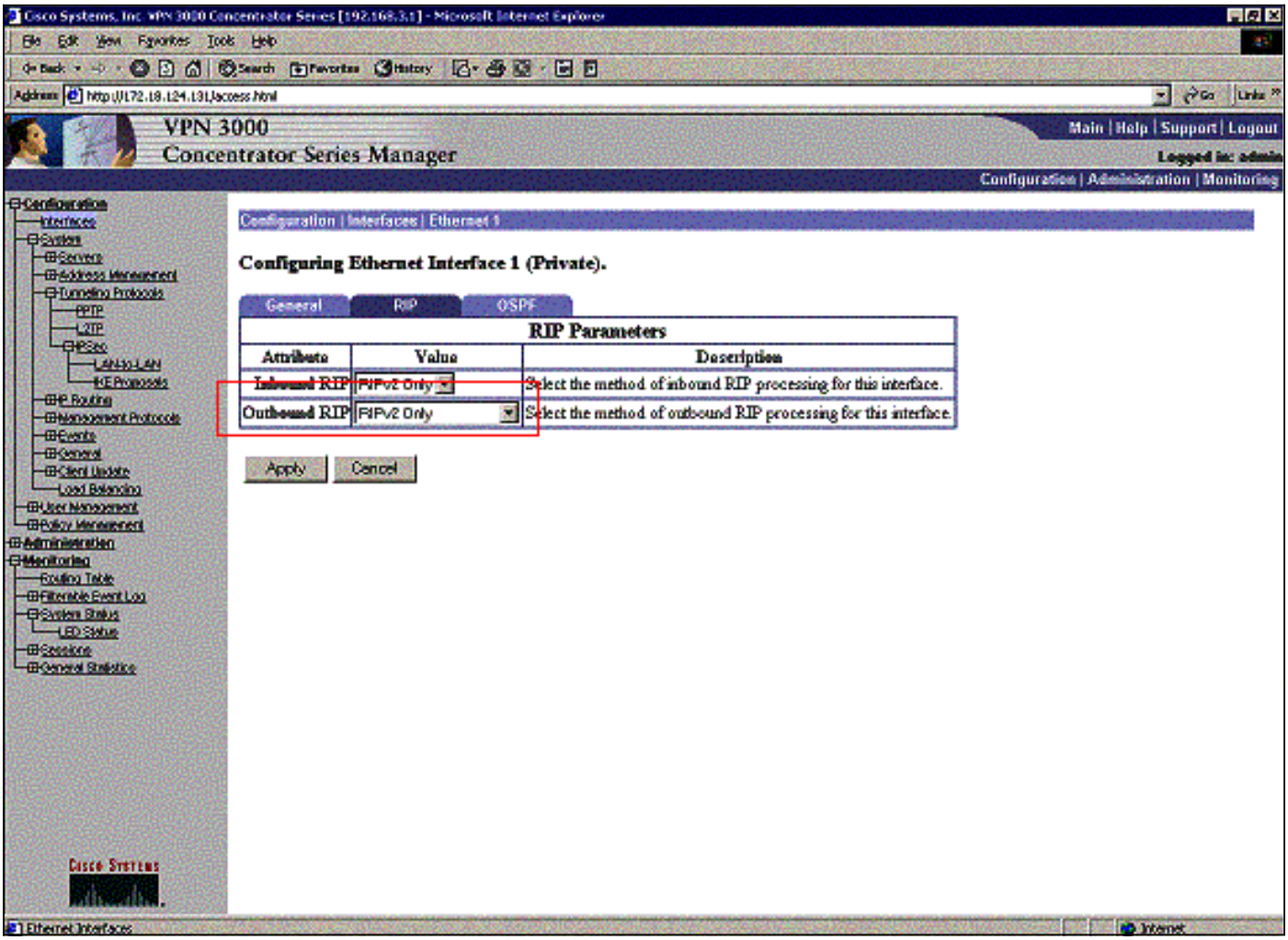
注: VPN 3060 では、ソフトウェア バージョン 3.5 以降にあるようなドロップダウン メニューの代わりに、ネットワーク自動検出に関するチェックボックスがあります。



RIP でトンネル学習ルートから VPN 3620 ルータに通過できるようにする

[Configuration] > [Interfaces] > [Private] > [RIP] の順に選択します。 ドロップダウン メニューを [RIPv2 Only] に変更し、[Apply] をクリックします。 [Configuration] > [System] > [Tunneling Protocols] > [IPSec] > [LAN-to-LAN] の順に選択します。

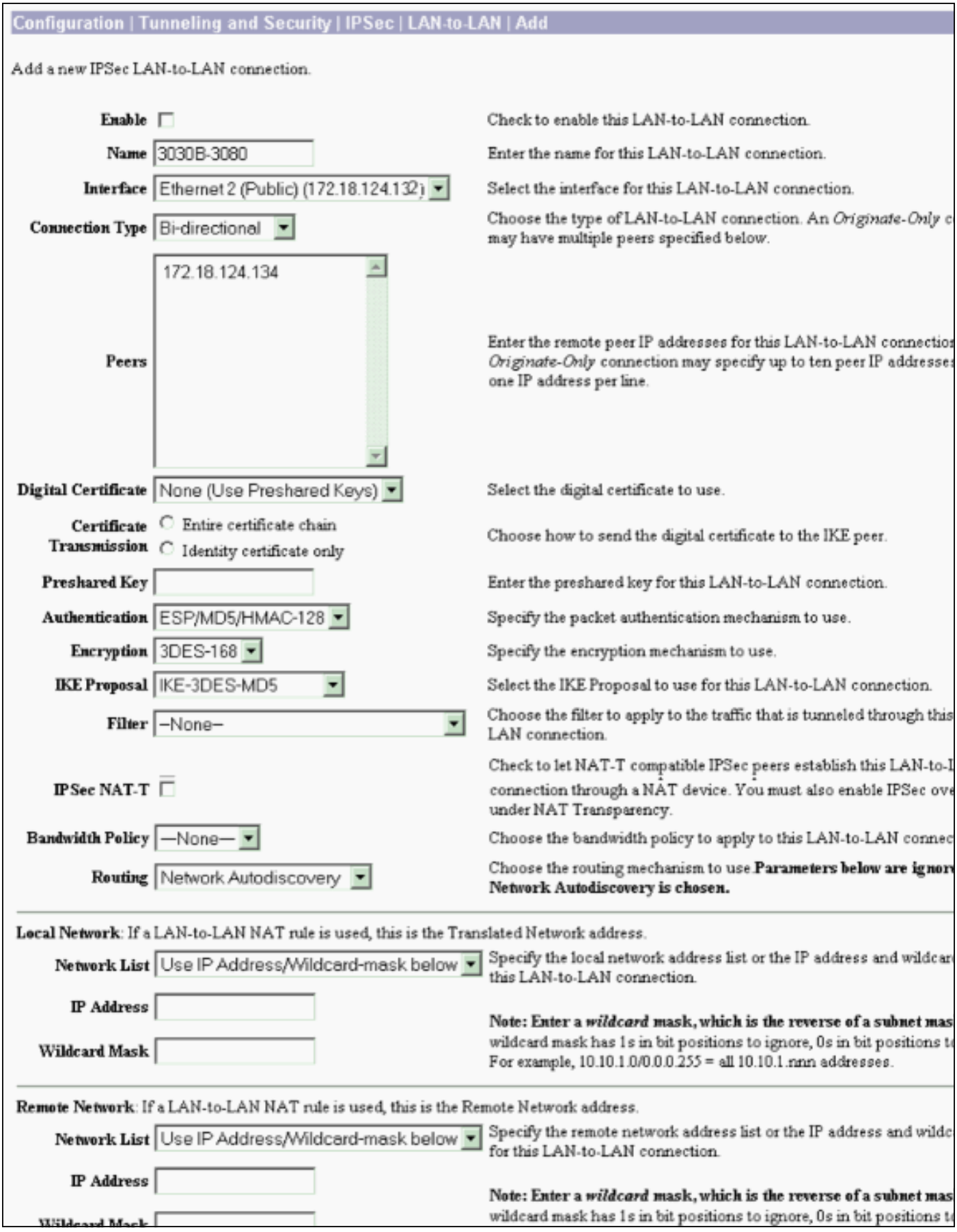
注: デフォルトは発信 RIP で、プライベート インターフェイスでは無効です。



VPN 3030b コンセントレータの設定

VPN 3030b から VPN 3080 への LAN-to-LAN

[Configuration] > [Tunneling and Security] > [IPSec] > [LAN-to-LAN] の順に選択します。

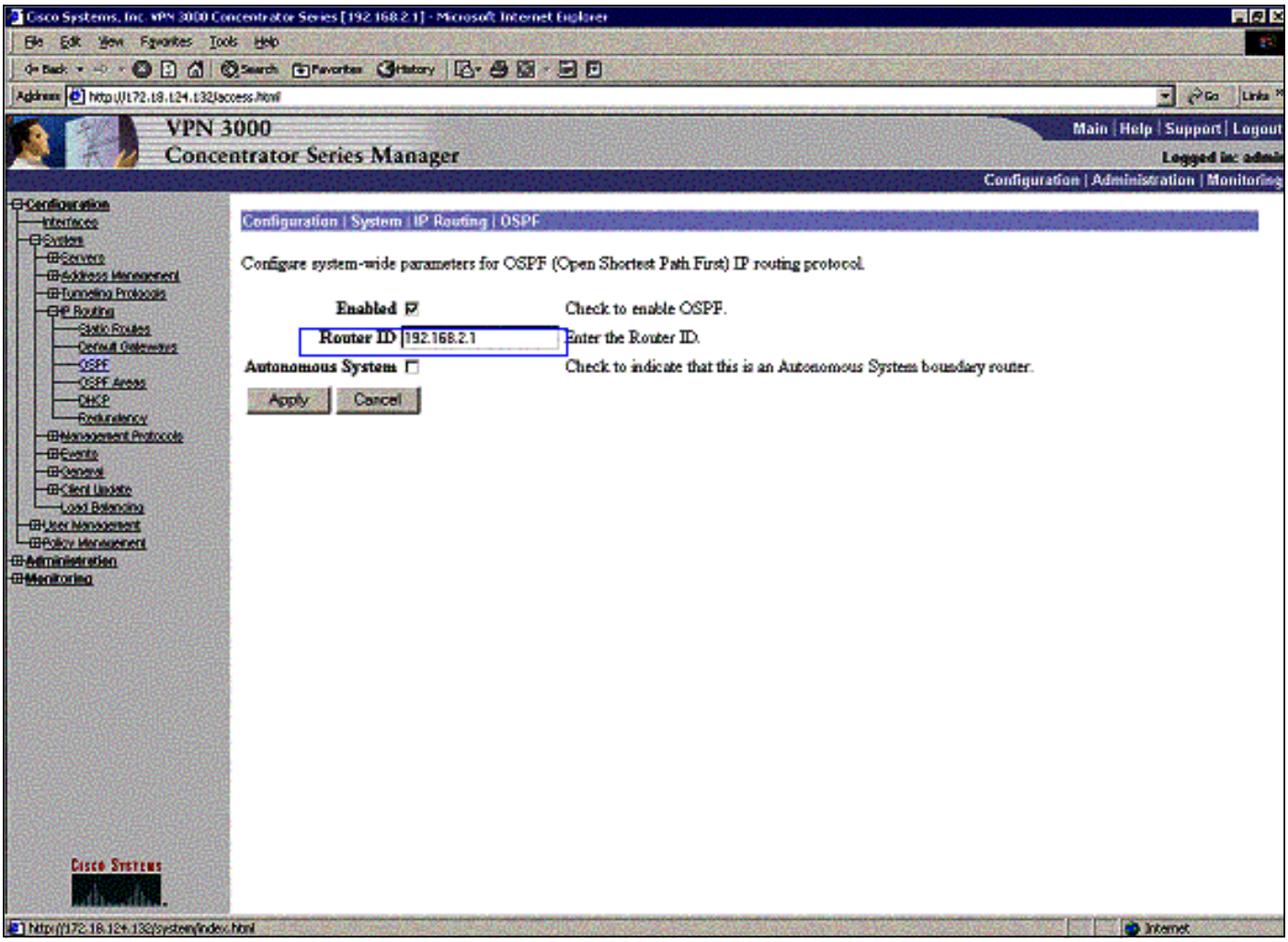


[RIP でトンネル学習ルートから VPN 3640 ルータに通過できるようにする]

このドキュメントの VPN 3060a コンセントレータに示されている手順に従ってください。

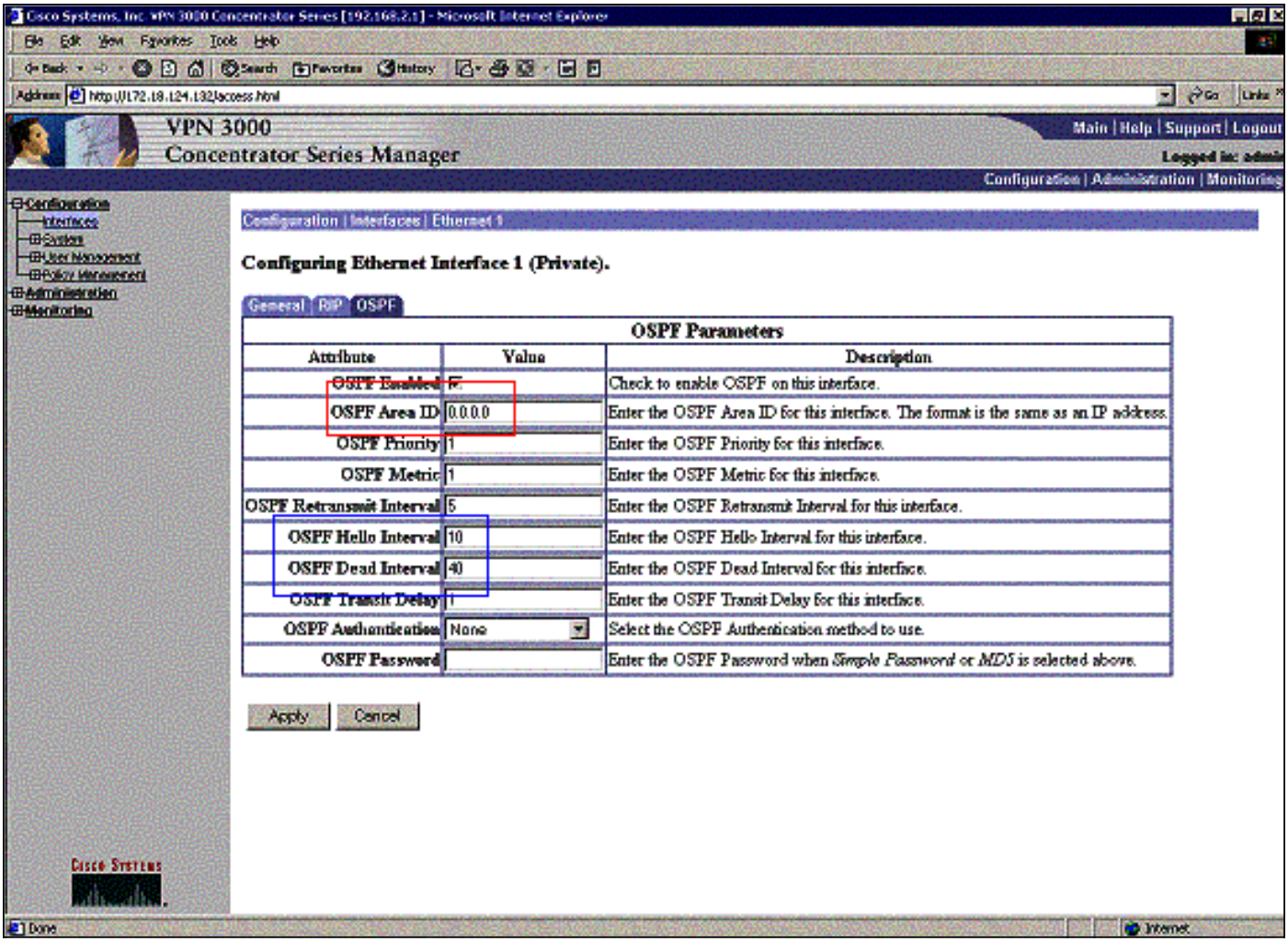
[OSPF でトンネル学習ルートから VPN 3030b コンセントレータに通過できるようにする]

[Configuration] > [System] > [IP Routing] > [OSPF] の順に選択し、ルート ID を入力します。




```
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
```

エリア ID はワイヤの ID と一致する必要があります。 この例ではエリア 0 にあるため、0.0.0.0 で表されます。 また **[Enable OSPF]** ボックスをオンにしてから、**[Apply]** をクリックします。



OSPF タイマーがルータのものと一致していることを確認します。 ルータのタイマーを確認するには、**show ip ospf interface <interface name>** コマンドを使用します。

```
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)
```

OSPF の詳細については、RFC 1247 を参照してください。

確認

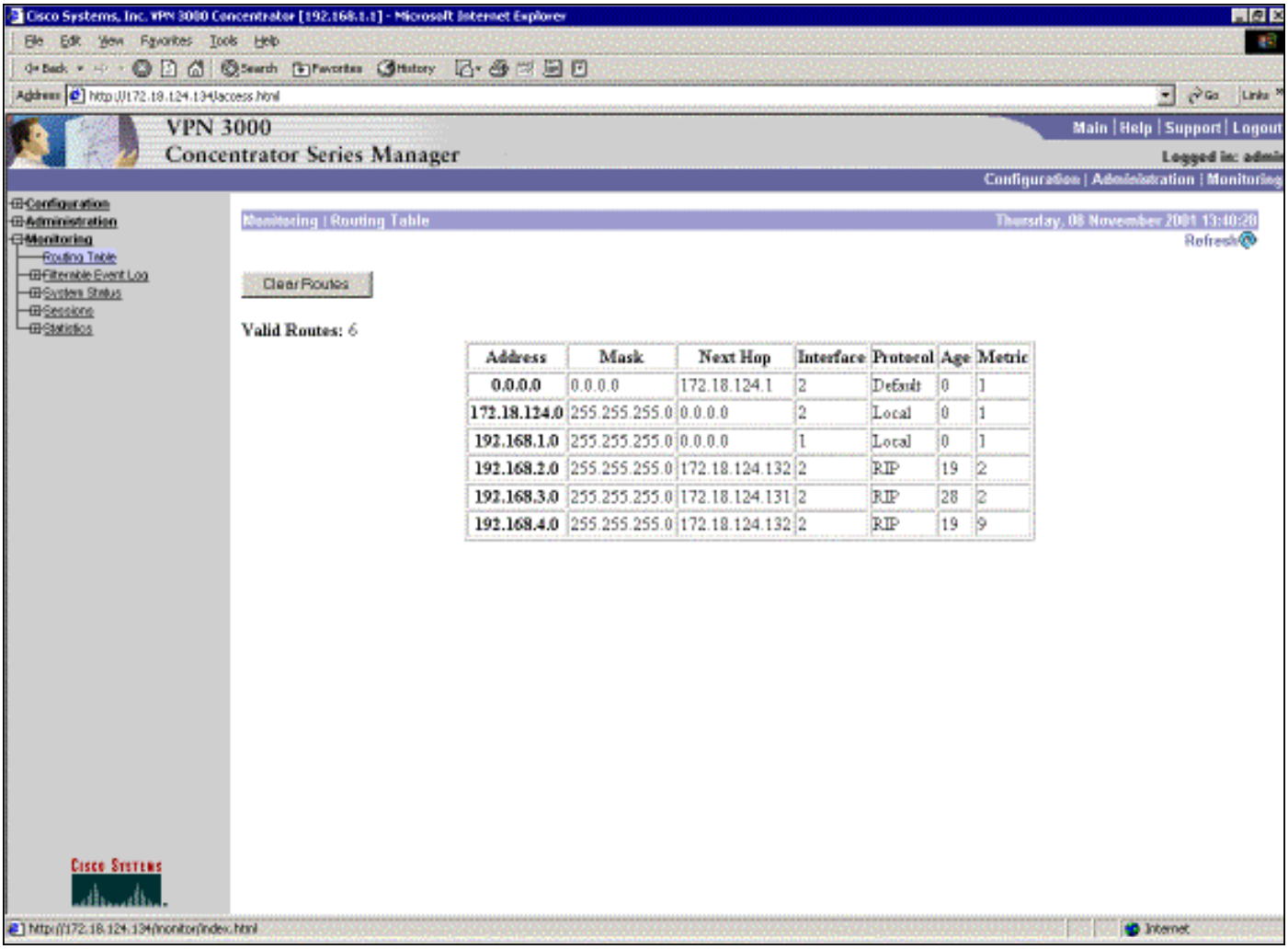
このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

このコマンド出力には、正確なルーティング テーブルが示されます。

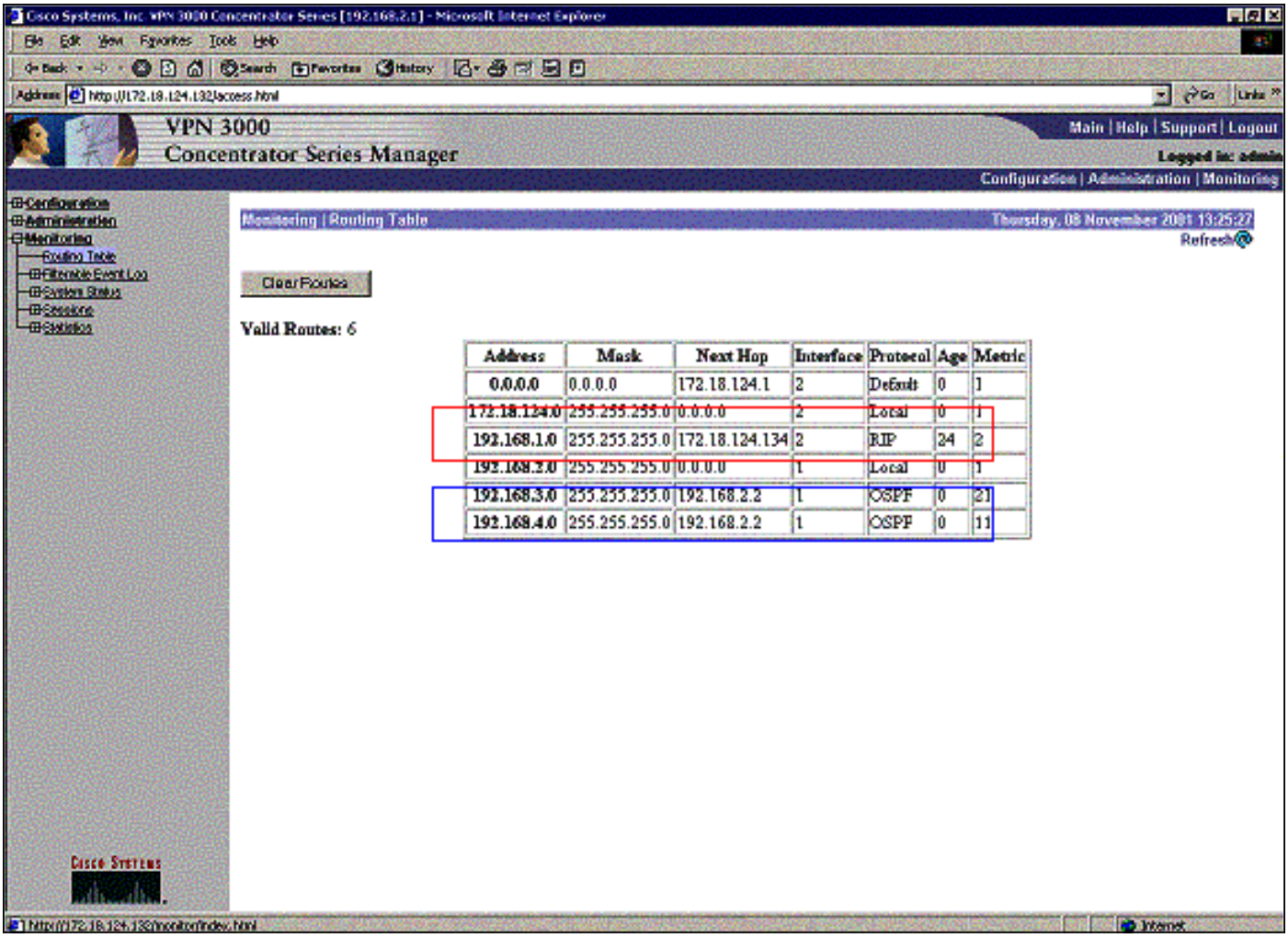
```
rtr-3620#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

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
```

次は、通常の状況の VPN 3080 コンセントレータのルーティング テーブルです。



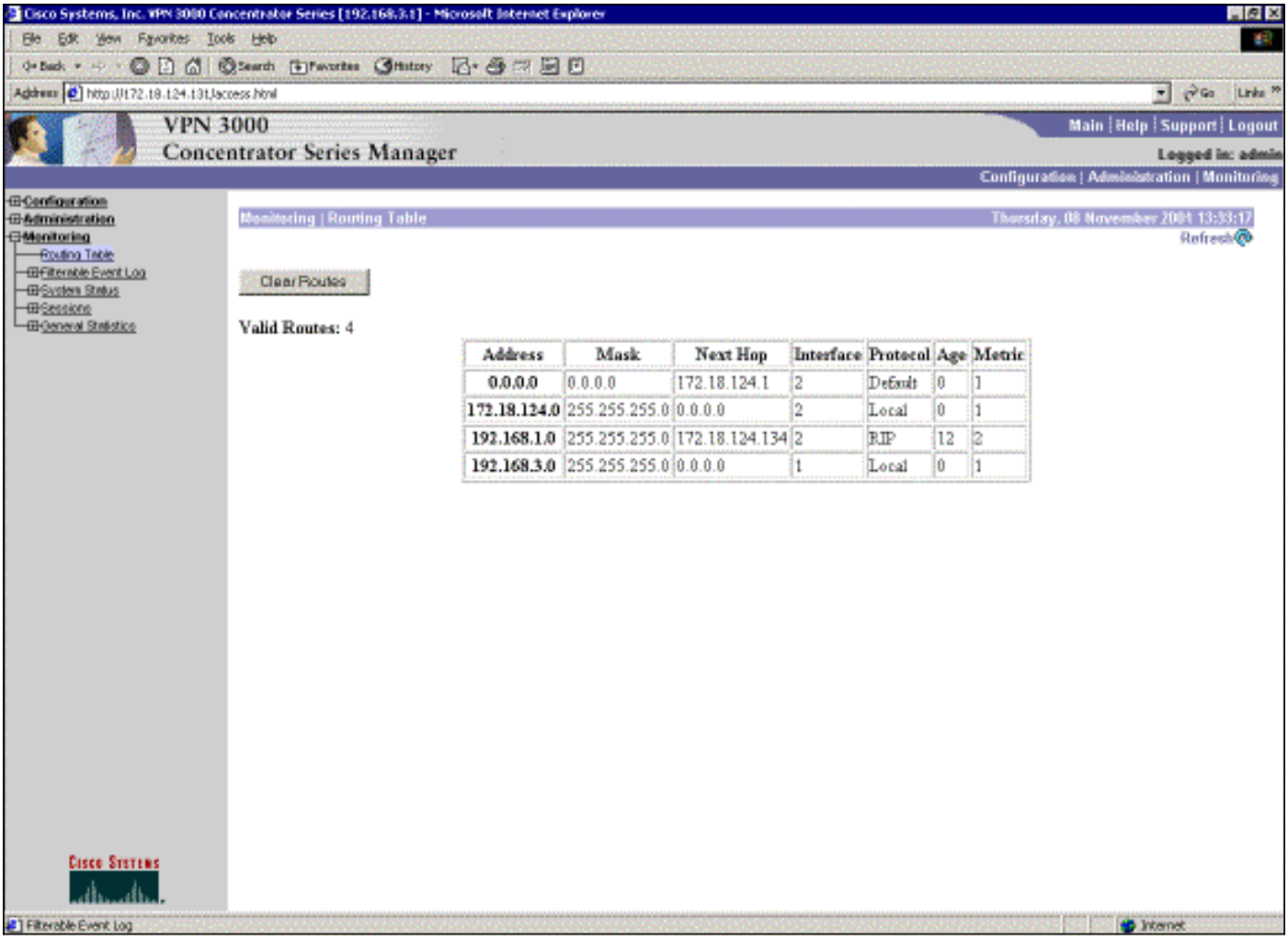
ネットワーク 192.168.2.x と 192.168.3.x は、それぞれ VPN トンネル 172.18.124.132 と 172.18.124.131 を通じて学習されます。 ルータの OSPF アドバタイズメントが VPN 3030b コンセントレータのルーティング テーブルに配置されるため、192.168.4.x ネットワークは 172.18.124.132 トンネルを介して学習されます。 ルーティング テーブルは、リモート VPN ピアにネットワークをアドバタイズします。

次は、通常の状況の VPN 3030b コンセントレータのルーティング テーブルです。



赤色で四角く囲った箇所は、192.168.1.x ネットワークが VPN トンネルから学習していることを示しています。 青色で四角く囲った箇所は、192.168.3.x と 192.168.4.x のネットワークがコア OSPF プロセスから学習していることを示しています。

次は、通常の状況の VPN 3060a コンセントレータのルーティング テーブルです。

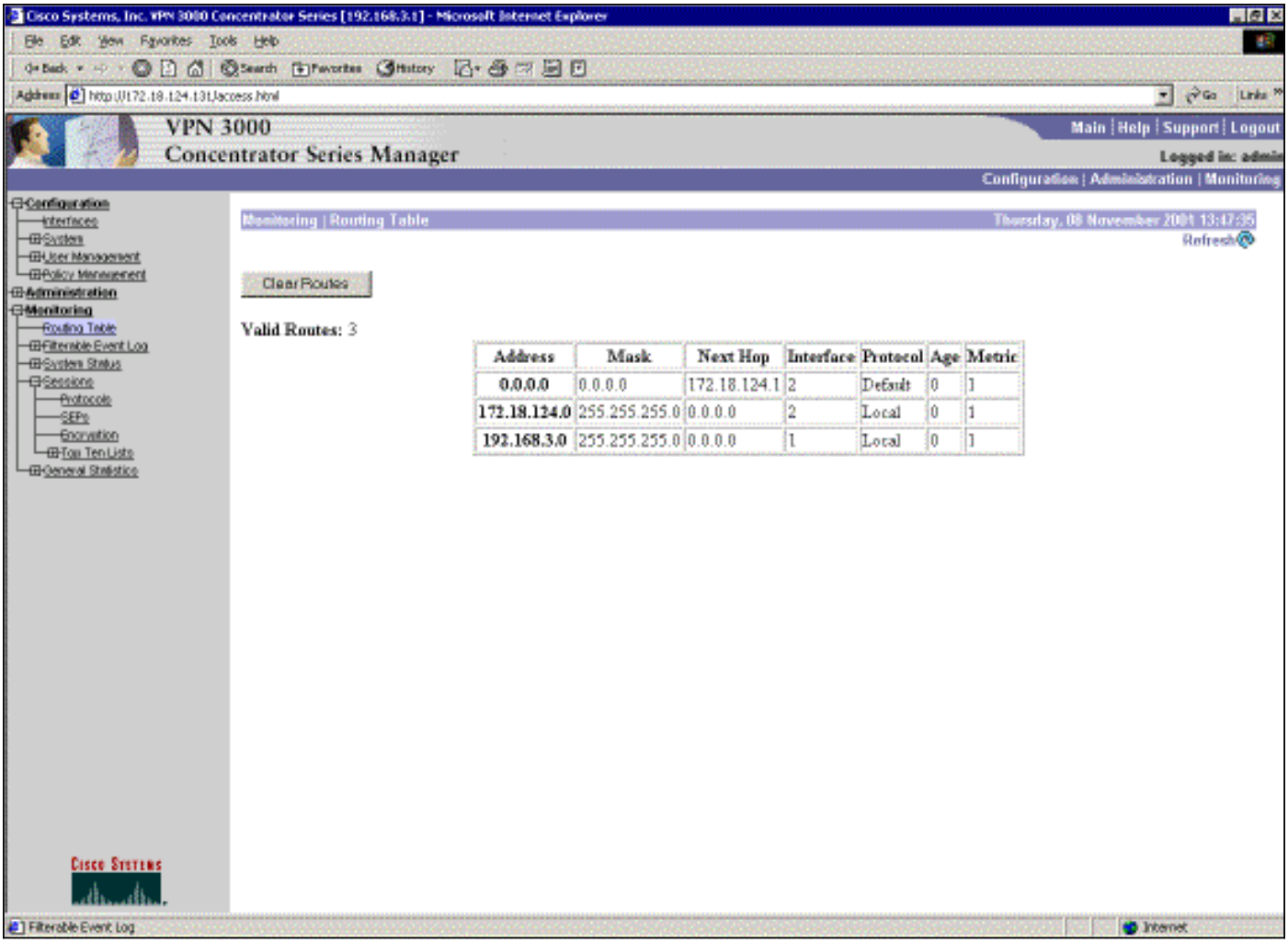


ネットワーク 192.168.1.x は、ここで唯一のネットワークで、VPN トンネルを介して到達できます。 192.168.2.0 ネットワークは、そのルートに沿って通過するプロセス (RIP など) が存在しないため、存在していません。 192.168.3.x ネットワーク上の PC が VPN コンセントレータへのデフォルト ゲートウェイを指していない限り、何も失われません。 必要に応じて、いつでもスタティック ルートを追加できます。 ただし、この例では、VPN コンセントレータ自体が 192.168.2.0 ネットワークに到達する必要はありません。

トラブルシューティング

シミュレートされた欠陥

これは、設定におけるシミュレートされた欠陥です。 パブリック インターフェイスへのフィルタを削除すると、VPN トンネルがドロップされます。 これにより、トンネルを介して学習された 192.168.1.0 のルートも同様にドロップされます。 RIP プロセスの場合、ルートを消去するのに約 3 分かかります。 したがって、ルート自体がタイムアウトするまで、3 分間停止する可能性があります。



RIP ルートの期限が切れると、以下のようなルータの新しいルーティング テーブルが表示されます。

```
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
```

不具合の原因

アドミニストレーティブ ディスタンスを 130 に変更するのを忘れた場合、次の出力が表示される可能性があります。 VPN トンネルはいずれも起動しています。

VPN 3080 コンセントレータ

注: これは、ルーティング テーブルのグラフィカル ユーザ インターフェイス (GUI) ではないバージョンです。

```
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
```

192.168.3.0 ネットワークに到達するには、172.18.124.131 を経由する必要があります。 ただし、RTR-3620 ルーティング テーブルは、次のようになります。

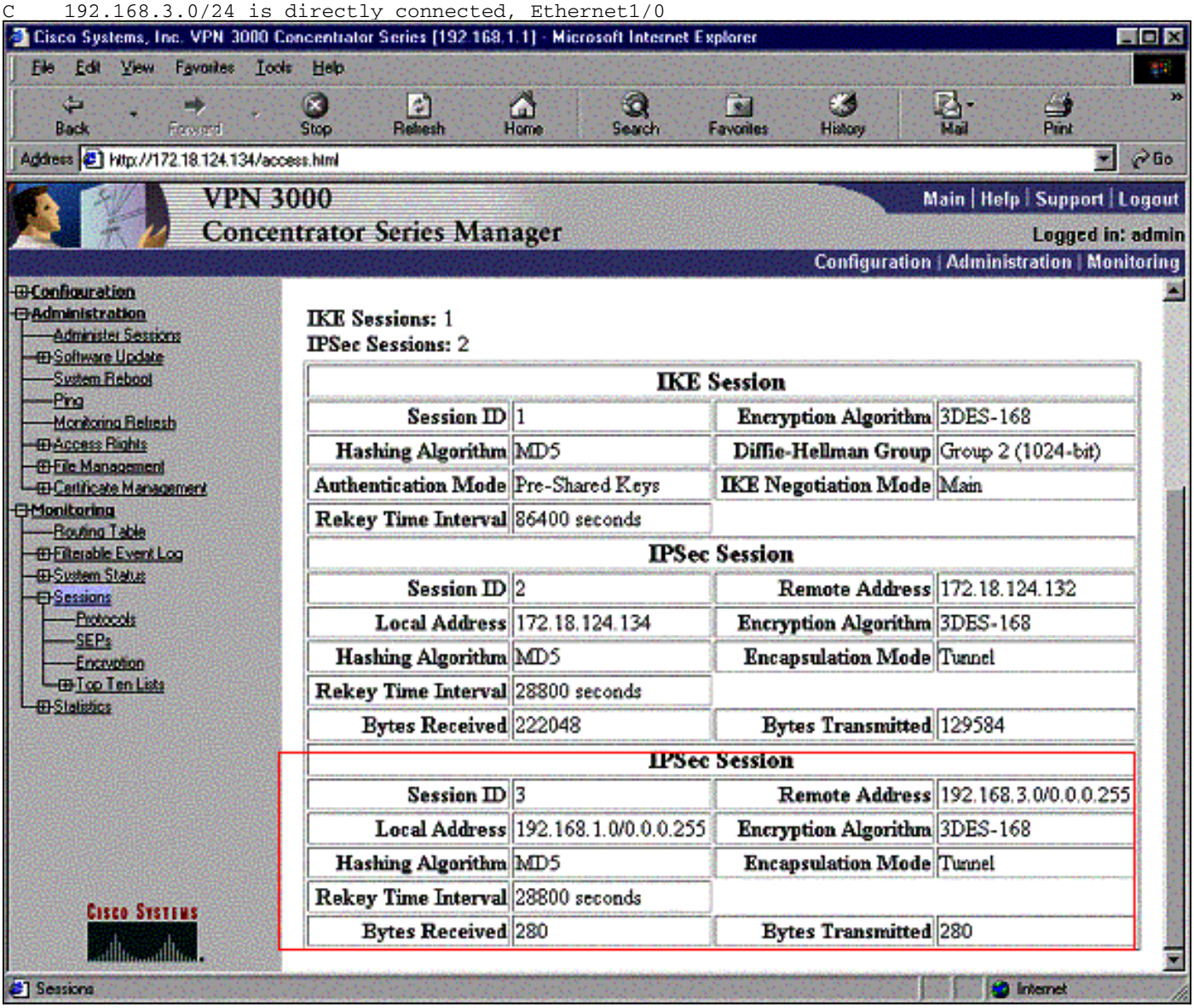
```
rtr-3620#show ip route

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
```

192.168.1.0 ネットワークに戻るには、ルートはバックボーン 192.168.4.x ネットワークを経由する必要があります。

自動検出によって VPN 3030b コンセントレータ上に適切なセキュリティ アソシエーション (SA) 情報が生成されているため、トラフィックは機能します。 次に、例を示します。

```
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
```



ルーティング テーブルにはピアが 172.18.124.132 であると示されていますが、実際の SA (トラフィック フロー) は 172.18.124.131 の VPN 3030b コンセントレータを経由します。 SA は、ルート テーブルより優先されます。 VPN 3060a コンセントレータのルート テーブルと SA テーブルを詳しく調べてみないと、トラフィックが正しい方向に流れていないことは判明しないかもしれません。

関連情報

- Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ

- IPSec に関するサポート ページ
- テクニカルサポート - Cisco Systems