Configurazione del routing ridondante sul concentratore VPN 3000

Sommario

Introduzione

In questo documento viene descritto come configurare un failover VPN ridondante se un sito remoto perde il proprio concentratore VPN 3000 o la connettività Internet. Nell'esempio, si supponga che la rete aziendale situata dietro la VPN 3030B utilizzi Open Shortest Path First (OSPF) come protocollo di routing predefinito.

Nota: quando si esegue la ridistribuzione tra i protocolli di instradamento, è possibile creare un ciclo di instradamento che può causare problemi alla rete. Nell'esempio viene utilizzato OSPF, che non è tuttavia l'unico protocollo di routing utilizzabile.

L'obiettivo di questo esempio è che la rete 192.168.1.0 utilizzi il tunnel rosso (in normali circostanze operative), illustrato nella sezione Diagramma reticolare, per raggiungere il valore 192.168.3.x. Se il tunnel, VPN Concentrator o ISP viene interrotto, la rete 192.168.3.0 viene appresa tramite un protocollo di routing dinamico sul tunnel verde. Inoltre, la connettività con il sito 192.168.3.0 non viene persa. Una volta risolto il problema, il traffico torna automaticamente al tunnel rosso.

Nota: RIP dispone di un timer di aging di tre minuti prima di consentire l'accettazione di una nuova route su una route non valida. Si supponga inoltre che i tunnel siano stati creati e che il traffico possa passare tra i peer.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Router 3620 e 3640
- Cisco VPN 3080 Concentrator - Versione: Cisco Systems, Inc./VPN 3000 Concentrator versione 4.7
- Cisco VPN 3060 Concentrator - Versione: Cisco Systems, Inc./VPN 3000 Concentrator serie 4.7
- Cisco VPN 3030 Concentrator - Versione: Cisco Systems, Inc./VPN 3000 Concentrator serie 4.7

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

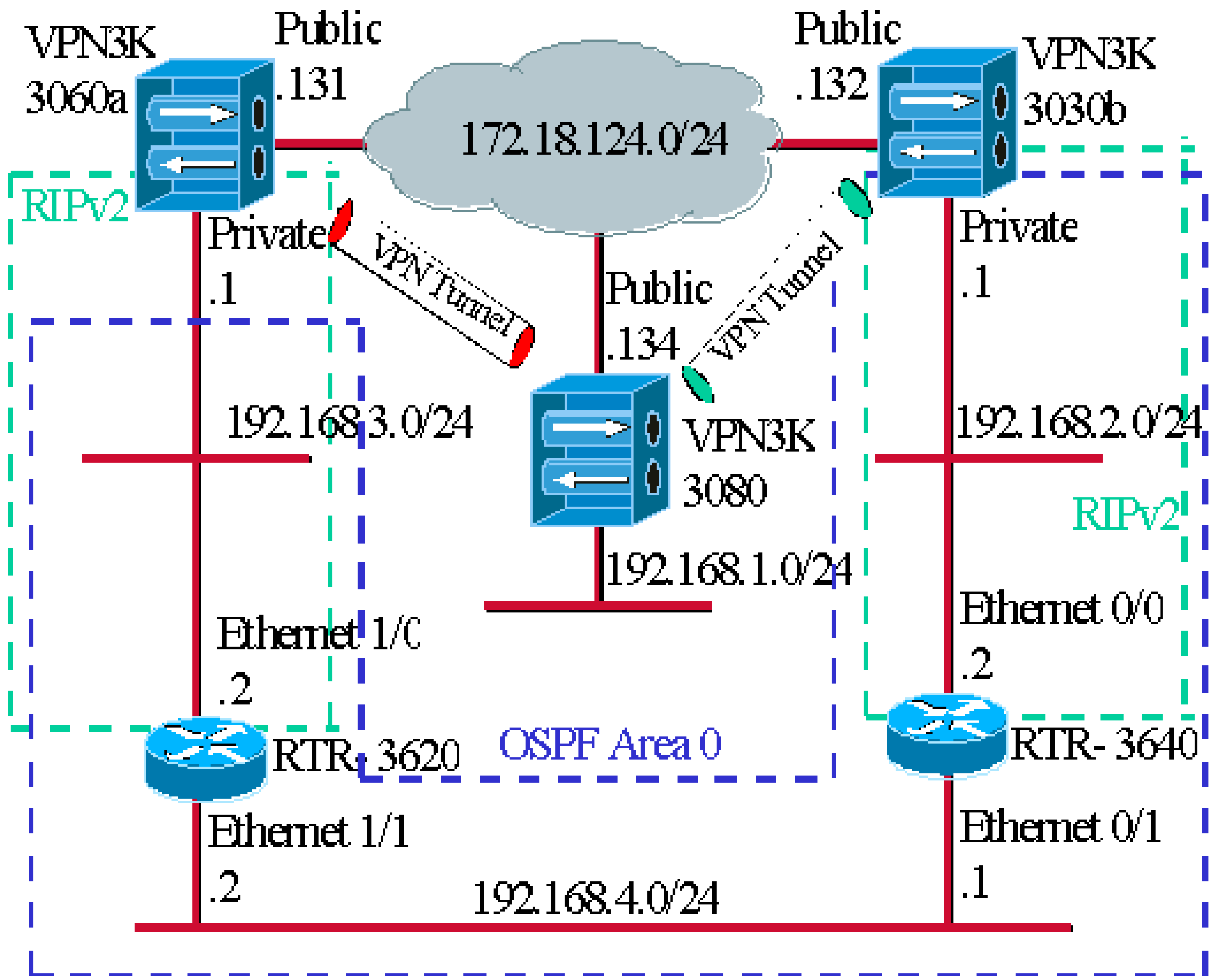
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



I trattini blu indicano che OSPF è abilitato da VPN 3030b a RTR-3640 e RTR-3620.

I trattini verdi indicano che RIPv2 è abilitato dalla VPN privata 3060a a RTR-3620, RTR-3640 e dalla VPN privata 3030b.

RIPv2 è abilitato anche nei tunnel VPN rosso e verde perché l'individuazione della rete è abilitata. Non è necessario abilitare RIP sull'interfaccia privata VPN 3080. Non è presente alcun RIP sulla rete 192.168.4.x perché tutte le route vengono apprese da OSPF tramite questo collegamento.

Nota: i PC sulle reti 192.168.2.x e 192.168.3.x devono avere i gateway predefiniti che puntano ai router e non ai concentratori VPN. Permettere ai router di decidere dove instradare i pacchetti.

Configurazioni router

Nel documento vengono usate queste configurazioni di router:

- 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
```

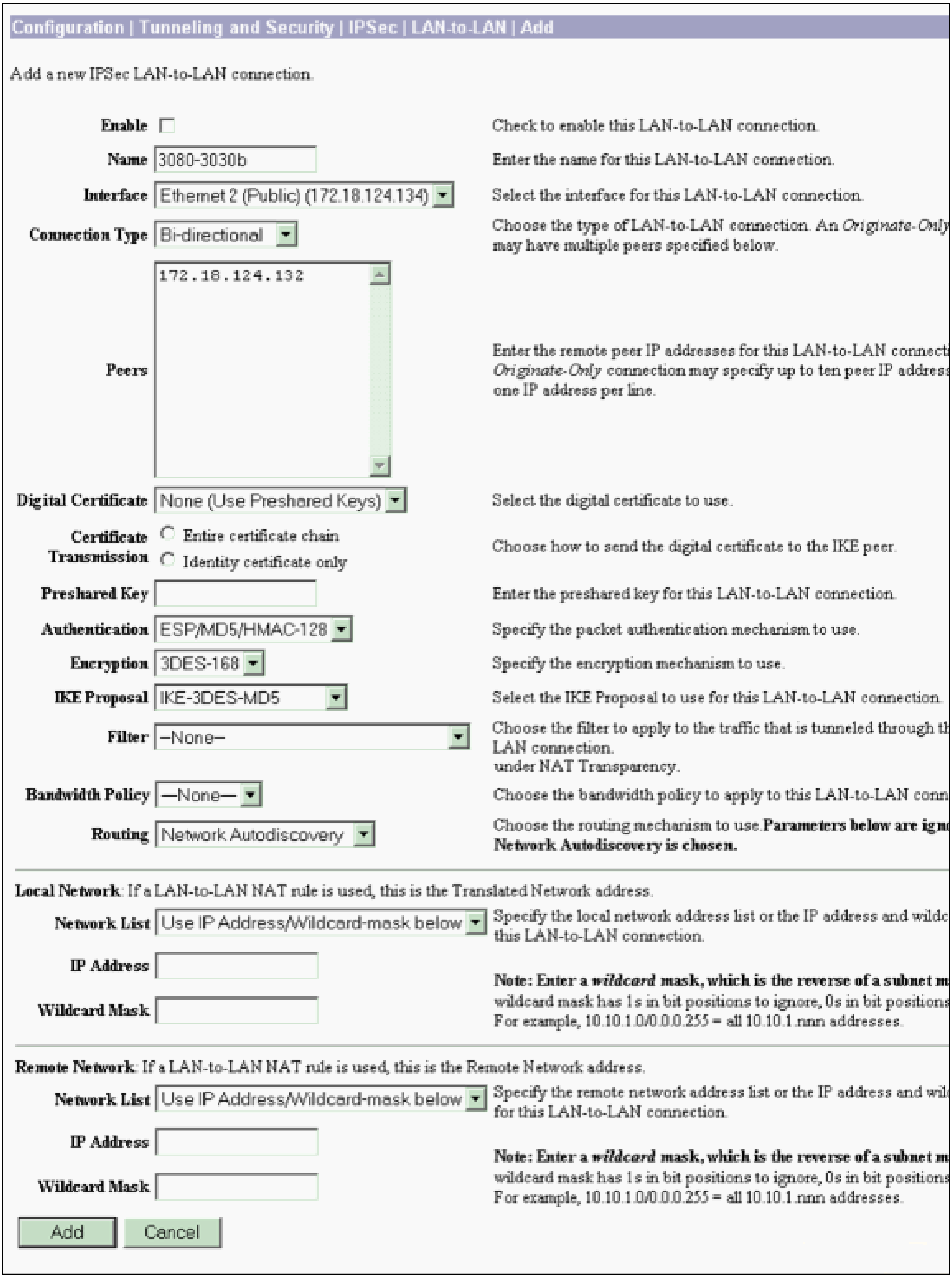
```
!
hostname rtr-3640
!
ip subnet-zero
!
interface Ethernet0/0
 ip address 192.168.2.2 255.255.255.0
 half-duplex
!
interface Ethernet0/1
 ip address 192.168.4.1 255.255.255.0
 half-duplex
!
router ospf 1
 log-adjacency-changes
!--- Use this command to push RIP learned routes into
OSPF. !--- You need 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
```

Configurazione VPN 3080 Concentrator

Da LAN-to-LAN VPN 3080 a VPN 3030b

Selezionare **Configurazione > Tunneling e sicurezza > IPSec > IPSec da LAN a LAN**. Poiché viene utilizzata l'individuazione automatica della rete, non è necessario compilare gli elenchi delle reti locali e remote.

Nota: i concentratori VPN con software versione 3.1 e precedenti dispongono di una casella di controllo per il rilevamento automatico. La versione software 3.5 (utilizzata sulla VPN 3080) utilizza un menu a discesa, come quello illustrato qui.



Configuration | Tunneling and Security | IPSec | LAN-to-LAN | Add

Add a new IPSec LAN-to-LAN connection.

Enable	□	Check to enable this LAN-to-LAN connection.
Name	3080-3030b	Enter the name for this LAN-to-LAN connection.
Interface	Ethernet 2 (Public) (172.18.124.134)	Select the interface for this LAN-to-LAN connection.
Connection Type	Bi-directional	Choose the type of LAN-to-LAN connection. An *Originate-Only* may have multiple peers specified below.
Peers	172.18.124.132	Enter the remote peer IP addresses for this LAN-to-LAN connecti *Originate-Only* connection may specify up to ten peer IP address one IP address per line.
Digital Certificate	None (Use Preshared Keys)	Select the digital certificate to use.
Certificate Transmission	○ Entire certificate chain ○ Identity certificate only	Choose how to send the digital certificate to the IKE peer.
Preshared Key		Enter the preshared key for this LAN-to-LAN connection.
Authentication	ESP/MD5/HMAC-128	Specify the packet authentication mechanism to use.
Encryption	3DES-168	Specify the encryption mechanism to use.
IKE Proposal	IKE-3DES-MD5	Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter	–None–	Choose the filter to apply to the traffic that is tunneled through th LAN connection. under NAT Transparency.
Bandwidth Policy	–None–	Choose the bandwidth policy to apply to this LAN-to-LAN conn
Routing	Network Autodiscovery	Choose the routing mechanism to use. **Parameters below are ign Network Autodiscovery is chosen.**

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

Network List	Use IP Address/Wildcard-mask below	Specify the local network address list or the IP address and wildc this LAN-to-LAN connection.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet m** wildcard mask has 1s in bit positions to ignore, 0s in bit positions For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask		

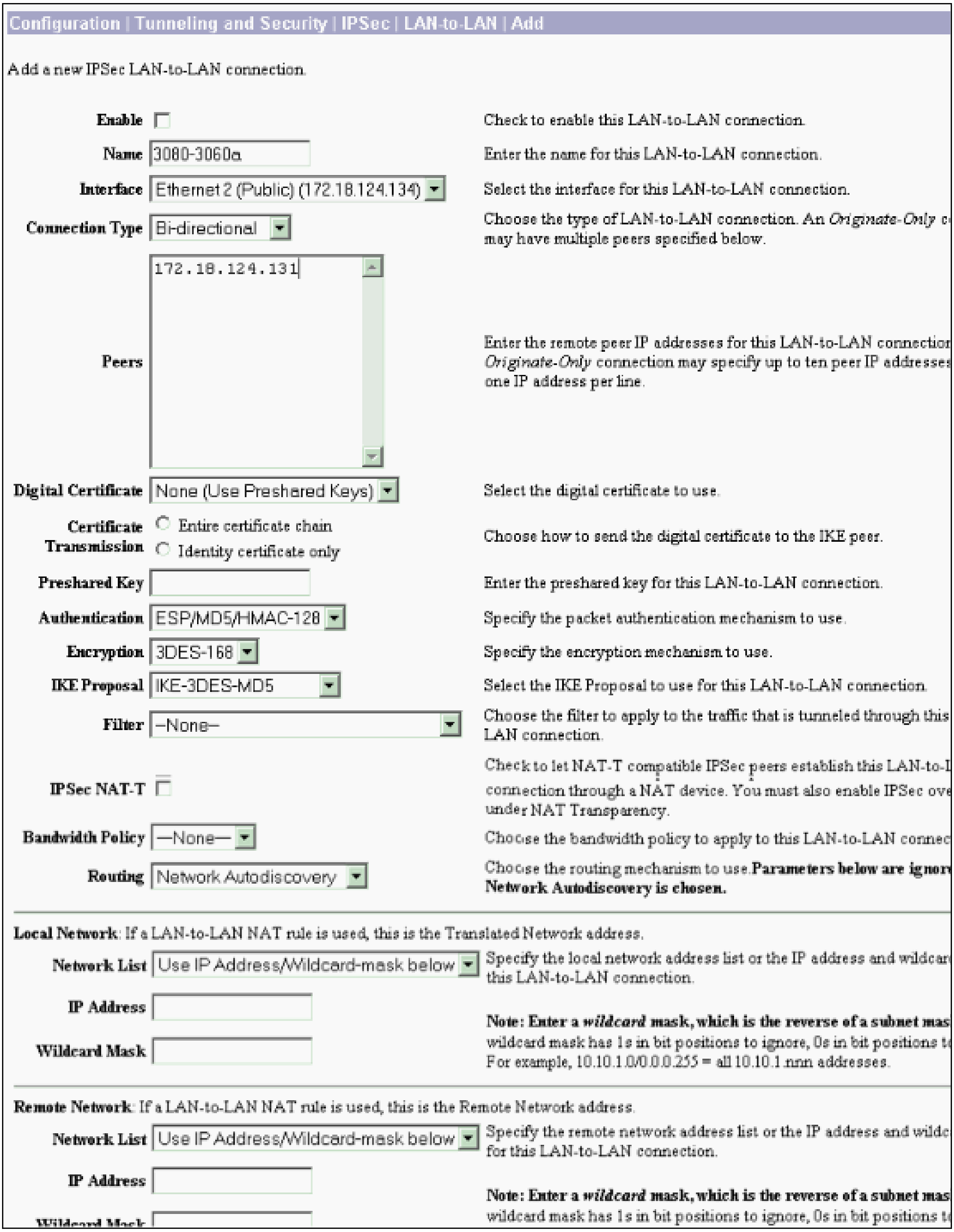
Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

Network List	Use IP Address/Wildcard-mask below	Specify the remote network address list or the IP address and wil for this LAN-to-LAN connection.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet m** wildcard mask has 1s in bit positions to ignore, 0s in bit positions For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask		

Da LAN-to-LAN VPN 3080 a VPN 3060a

Selezionare **Configurazione > Tunneling e sicurezza > IPSec > IPSec da LAN a LAN**. Poiché viene utilizzata l'individuazione automatica della rete, non è necessario compilare gli elenchi delle reti locali e remote.

Nota: i concentratori VPN con software versione 3.1 e precedenti dispongono di una casella di controllo per il rilevamento automatico. La versione software 3.5 (utilizzata sulla VPN 3080) utilizza un menu a discesa, come quello illustrato qui.



Configuration | Tunneling and Security | IPSec | LAN-to-LAN | Add

Add a new IPSec LAN-to-LAN connection.

Enable	□	Check to enable this LAN-to-LAN connection.
Name	3080-3060a	Enter the name for this LAN-to-LAN connection.
Interface	Ethernet 2 (Public) (172.18.124.134)	Select the interface for this LAN-to-LAN connection.
Connection Type	Bi-directional	Choose the type of LAN-to-LAN connection. An *Originate-Only* c may have multiple peers specified below.
Peers	172.18.124.131	Enter the remote peer IP addresses for this LAN-to-LAN connectio *Originate-Only* connection may specify up to ten peer IP addresses one IP address per line.
Digital Certificate	None (Use Preshared Keys)	Select the digital certificate to use.
Certificate Transmission	○ Entire certificate chain ○ Identity certificate only	Choose how to send the digital certificate to the IKE peer.
Preshared Key		Enter the preshared key for this LAN-to-LAN connection.
Authentication	ESP/MD5/HMAC-128	Specify the packet authentication mechanism to use.
Encryption	3DES-168	Specify the encryption mechanism to use.
IKE Proposal	IKE-3DES-MD5	Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter	--None--	Choose the filter to apply to the traffic that is tunneled through this LAN connection.
IPSec NAT-T	□	Check to let NAT-T compatible IPSec peers establish this LAN-to-L connection through a NAT device. You must also enable IPSec ove under NAT Transparency.
Bandwidth Policy	--None--	Choose the bandwidth policy to apply to this LAN-to-LAN connec
Routing	Network Autodiscovery	Choose the routing mechanism to use. **Parameters below are ignor Network Autodiscovery is chosen.**

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

Network List	Use IP Address/Wildcard-mask below	Specify the local network address list or the IP address and wildcar this LAN-to-LAN connection.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet mas** wildcard mask has 1s in bit positions to ignore, 0s in bit positions to For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask		

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

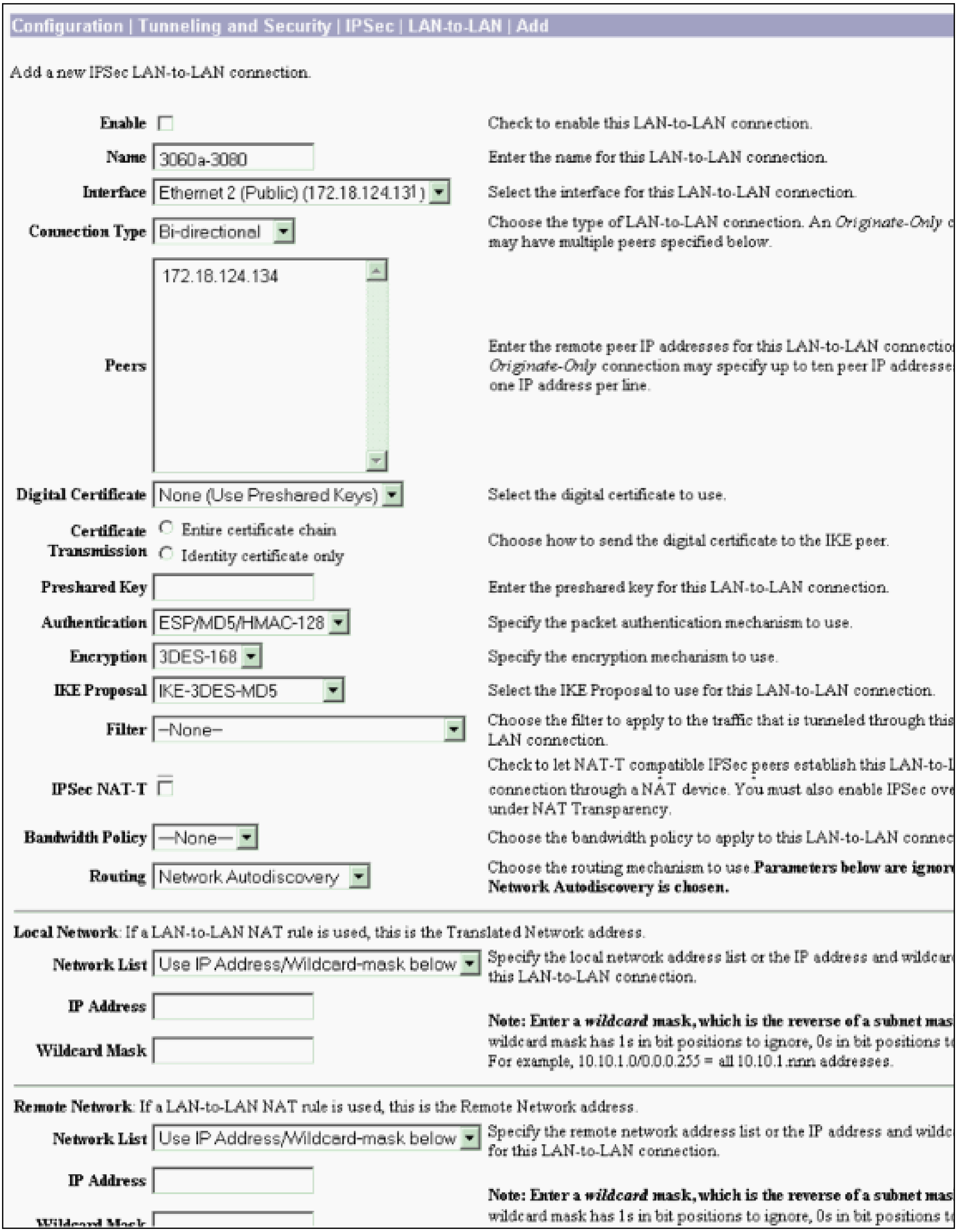
Network List	Use IP Address/Wildcard-mask below	Specify the remote network address list or the IP address and wildc for this LAN-to-LAN connection.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet mas** wildcard mask has 1s in bit positions to ignore, 0s in bit positions to
Wildcard Mask		

Configurazione VPN 3060a Concentrator

Da LAN a LAN VPN 3060a a VPN 3080

Selezionare **Configurazione > Tunneling e sicurezza > IPSec > IPSec da LAN a LAN**.

Nota: sulla VPN 3060 è presente una casella di controllo per l'individuazione automatica della rete anziché il menu a discesa come nella versione software 3.5 e successive.



Configuration | Tunneling and Security | IPSec | LAN-to-LAN | Add

Add a new IPSec LAN-to-LAN connection.

Enable	□	Check to enable this LAN-to-LAN connection.
Name	3060a-3080	Enter the name for this LAN-to-LAN connection.
Interface	Ethernet 2 (Public) (172.18.124.131) ▾	Select the interface for this LAN-to-LAN connection.
Connection Type	Bi-directional ▾	Choose the type of LAN-to-LAN connection. An *Originate-Only* c may have multiple peers specified below.
Peers	172.18.124.134	Enter the remote peer IP addresses for this LAN-to-LAN connectio *Originate-Only* connection may specify up to ten peer IP addresse one IP address per line.
Digital Certificate	None (Use Preshared Keys) ▾	Select the digital certificate to use.
Certificate Transmission	○ Entire certificate chain ○ Identity certificate only	Choose how to send the digital certificate to the IKE peer.
Preshared Key		Enter the preshared key for this LAN-to-LAN connection.
Authentication	ESP/MD5/HMAC-128 ▾	Specify the packet authentication mechanism to use.
Encryption	3DES-168 ▾	Specify the encryption mechanism to use.
IKE Proposal	IKE-3DES-MD5 ▾	Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter	--None-- ▾	Choose the filter to apply to the traffic that is tunneled through this LAN connection.
IPSec NAT-T	□	Check to let NAT-T compatible IPSec peers establish this LAN-to-L connection through a NAT device. You must also enable IPSec ove under NAT Transparency.
Bandwidth Policy	--None-- ▾	Choose the bandwidth policy to apply to this LAN-to-LAN connec
Routing	Network Autodiscovery ▾	Choose the routing mechanism to use. **Parameters below are ignor Network Autodiscovery is chosen.**

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

Network List	Use IP Address/Wildcard-mask below ▾	Specify the local network address list or the IP address and wildcar this LAN-to-LAN connection.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet mas** wildcard mask has 1s in bit positions to ignore, 0s in bit positions t For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask		

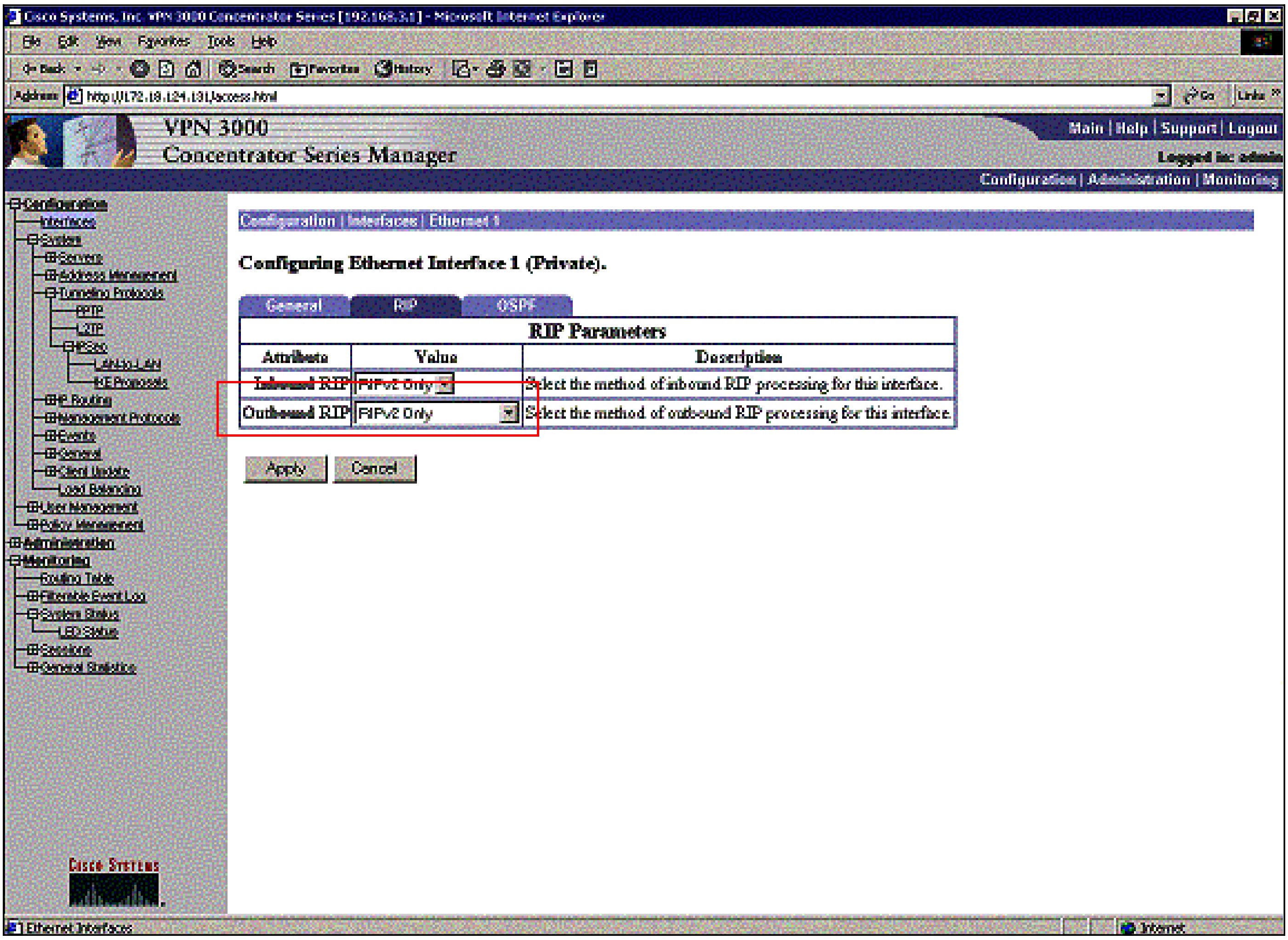
Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

Network List	Use IP Address/Wildcard-mask below ▾	Specify the remote network address list or the IP address and wildc for this LAN-to-LAN connection.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet mas** wildcard mask has 1s in bit positions to ignore, 0s in bit positions t
Wildcard Mask		

Abilitare RIP per passare le route apprese dal tunnel al router VPN 3620

Selezionare **Configurazione > Interfacce > Private > RIP**. Modificare il menu a discesa in **RIPv2 Only** e fare clic su **Applica**. Quindi selezionare **Configurazione > Sistema > Protocolli di tunneling > IPSec > Da LAN a LAN**.

Nota: il valore predefinito è RIP in uscita ed è disabilitato per l'interfaccia privata.



Configuration | Interfaces | Ethernet 1

Configuring Ethernet Interface 1 (Private).

General | RIP | OSPF

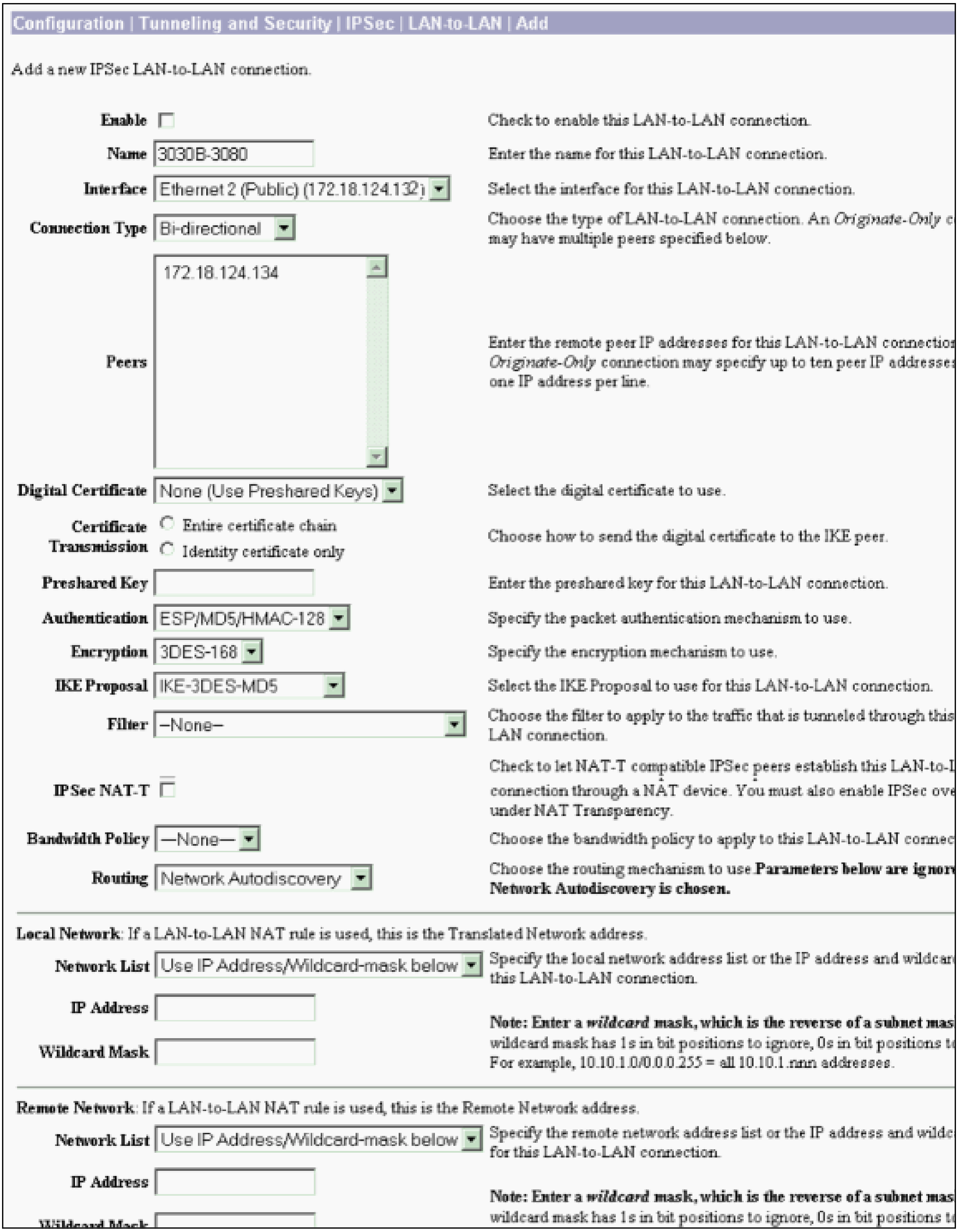
RIP Parameters		
Attribute	**Value**	**Description**
Inbound RIP	RIPv2 Only	Select the method of inbound RIP processing for this interface.
Outbound RIP	RIPv2 Only	Select the method of outbound RIP processing for this interface.

Apply | Cancel

Configurazione VPN 3030b Concentrator

Da LAN-to-LAN VPN 3030b a VPN 3080

Selezionare **Configurazione > Tunneling e sicurezza > IPSec > Da LAN a LAN**.



Configuration | Tunneling and Security | IPSec | LAN-to-LAN | Add

Add a new IPSec LAN-to-LAN connection.

Enable	□	Check to enable this LAN-to-LAN connection.
Name	3030B-3080	Enter the name for this LAN-to-LAN connection.
Interface	Ethernet 2 (Public) (172.18.124.132)	Select the interface for this LAN-to-LAN connection.
Connection Type	Bi-directional	Choose the type of LAN-to-LAN connection. An *Originate-Only* c may have multiple peers specified below.
Peers	172.18.124.134	Enter the remote peer IP addresses for this LAN-to-LAN connectio *Originate-Only* connection may specify up to ten peer IP addresses one IP address per line.
Digital Certificate	None (Use Preshared Keys)	Select the digital certificate to use.
Certificate Transmission	○ Entire certificate chain ○ Identity certificate only	Choose how to send the digital certificate to the IKE peer.
Preshared Key		Enter the preshared key for this LAN-to-LAN connection.
Authentication	ESP/MD5/HMAC-128	Specify the packet authentication mechanism to use.
Encryption	3DES-168	Specify the encryption mechanism to use.
IKE Proposal	IKE-3DES-MD5	Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter	–None–	Choose the filter to apply to the traffic that is tunneled through this LAN connection.
IPSec NAT-T	□	Check to let NAT-T compatible IPSec peers establish this LAN-to-L connection through a NAT device. You must also enable IPSec ove under NAT Transparency.
Bandwidth Policy	–None–	Choose the bandwidth policy to apply to this LAN-to-LAN connec
Routing	Network Autodiscovery	Choose the routing mechanism to use. **Parameters below are ignor Network Autodiscovery is chosen.**

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

Network List	Use IP Address/Wildcard-mask below	Specify the local network address list or the IP address and wildcar this LAN-to-LAN connection.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet mas** wildcard mask has 1s in bit positions to ignore, 0s in bit positions t For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask		

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

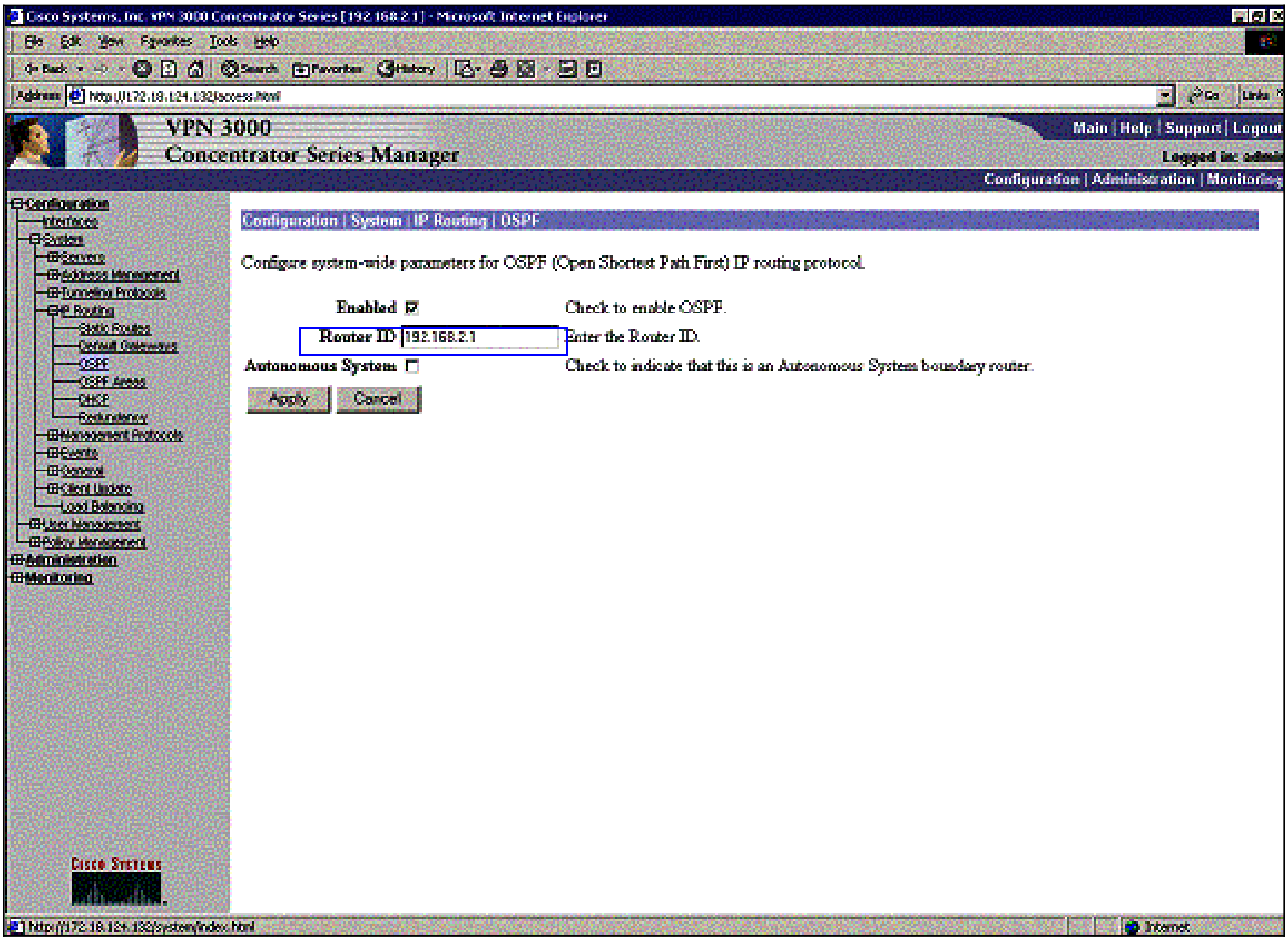
Network List	Use IP Address/Wildcard-mask below	Specify the remote network address list or the IP address and wildc for this LAN-to-LAN connection.
IP Address		**Note: Enter a *wildcard* mask, which is the reverse of a subnet mas** wildcard mask has 1s in bit positions to ignore, 0s in bit positions t
Wildcard Mask		

Abilitare RIP per passare le route apprese dal tunnel al router VPN 3640

Attenersi alla procedura descritta in precedenza in questo documento per i concentratori VPN 3060a.

Abilitare OSPF per passare le route apprese dalla backbone al concentratore VPN 3030b

Selezionare **Configuration > System > IP Routing > OSPF** e immettere l'ID del router.


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.2.1] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.18.124.132/access.html
Go Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
Servers
Address Management
Tunneling Protocols
IP Routing
Static Routes
Default Gateways
OSPF
OSPF Areas
DHCP
Redundancy
Management Protocols
Events
General
Client Update
Load Balancing
User Management
Policy Management
Administration
Monitoring
Cisco Systems
http://172.18.124.132/system/index.html
Internet

Configuration | System | IP Routing | OSPF

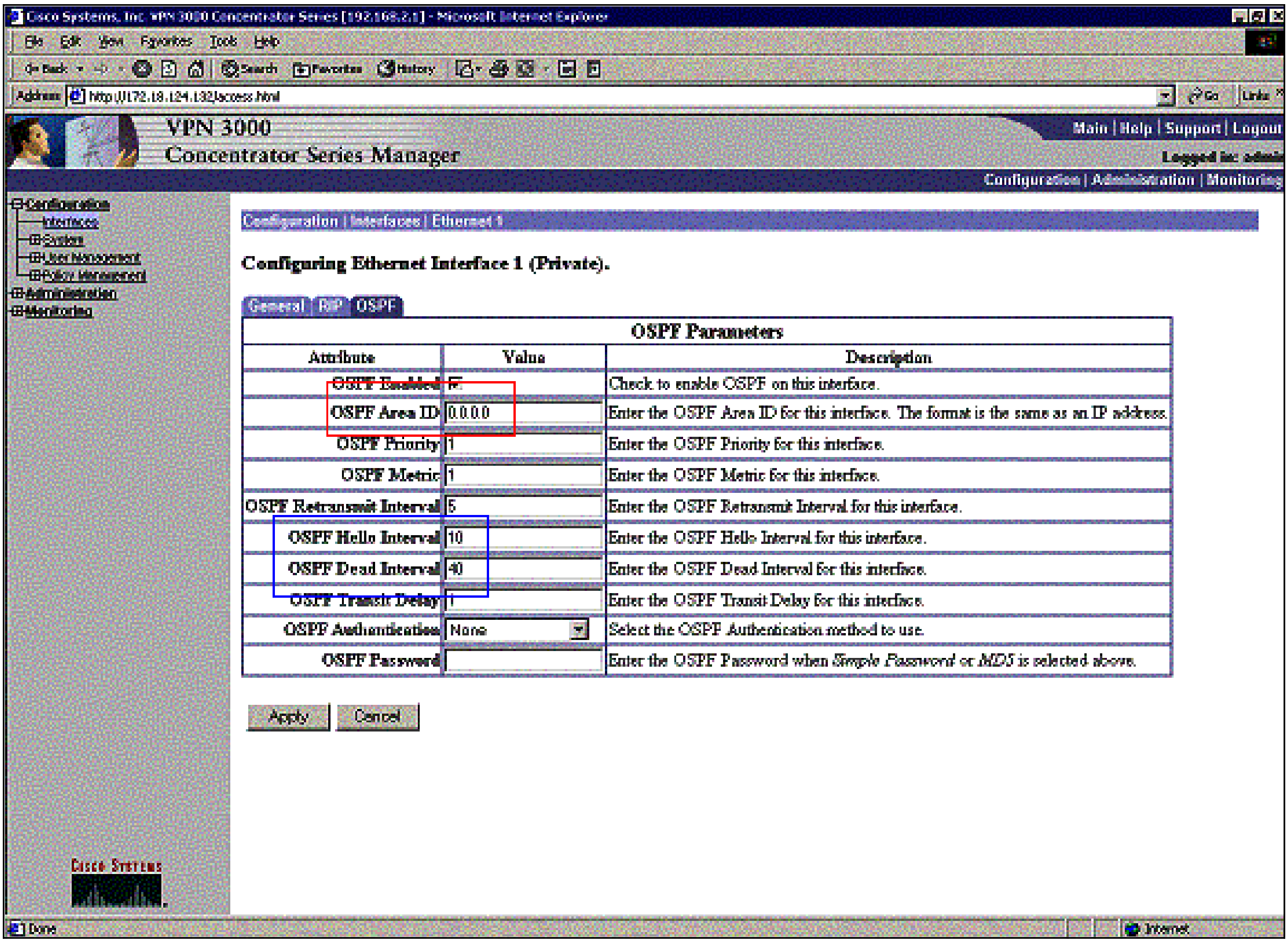
Configure system-wide parameters for OSPF (Open Shortest Path First) IP routing protocol.

Enabled	☑	Check to enable OSPF.
Router ID	192.168.2.1	Enter the Router ID.
Autonomous System	□	Check to indicate that this is an Autonomous System boundary router.

Apply Cancel

```
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
```

L'ID area deve corrispondere all'ID sul cavo. Poiché l'area in questo esempio è 0, è rappresentata da 0.0.0.0. Selezionare inoltre la casella **Abilita OSPF** e fare clic su **Applica**.



Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.2.1] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.18.124.132/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Administration
Monitoring
Configuration | Interfaces | Ethernet 1
General RIP OSPF
Apply Cancel
Done
Internet

Configuring Ethernet Interface 1 (Private).

OSPF Parameters		
Attribute	Value	Description
OSPF Enabled	☑	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.

Verificare che i timer OSPF corrispondano a quelli del router. Per verificare i timer dei router, usare il comando **show ip ospf interface *<nome interfaccia>*** .

```
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)
```

Per ulteriori informazioni su OSPF, fare riferimento alla RFC 1247 .

Verifica

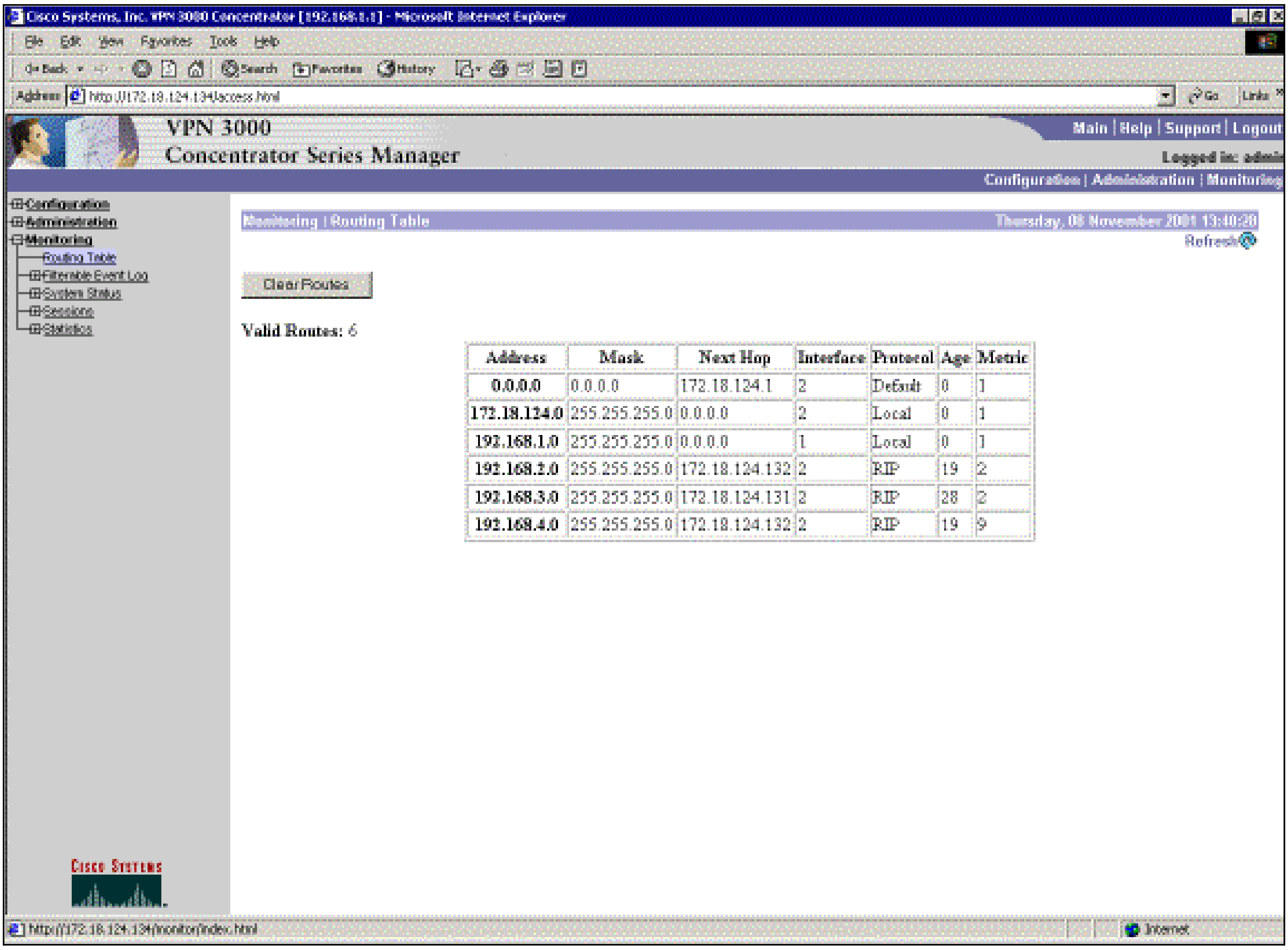
Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

Questo output del comando mostra tabelle di routing precise.

```
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
```

Questa è la tabella di routing di VPN 3080 Concentrator in circostanze normali.

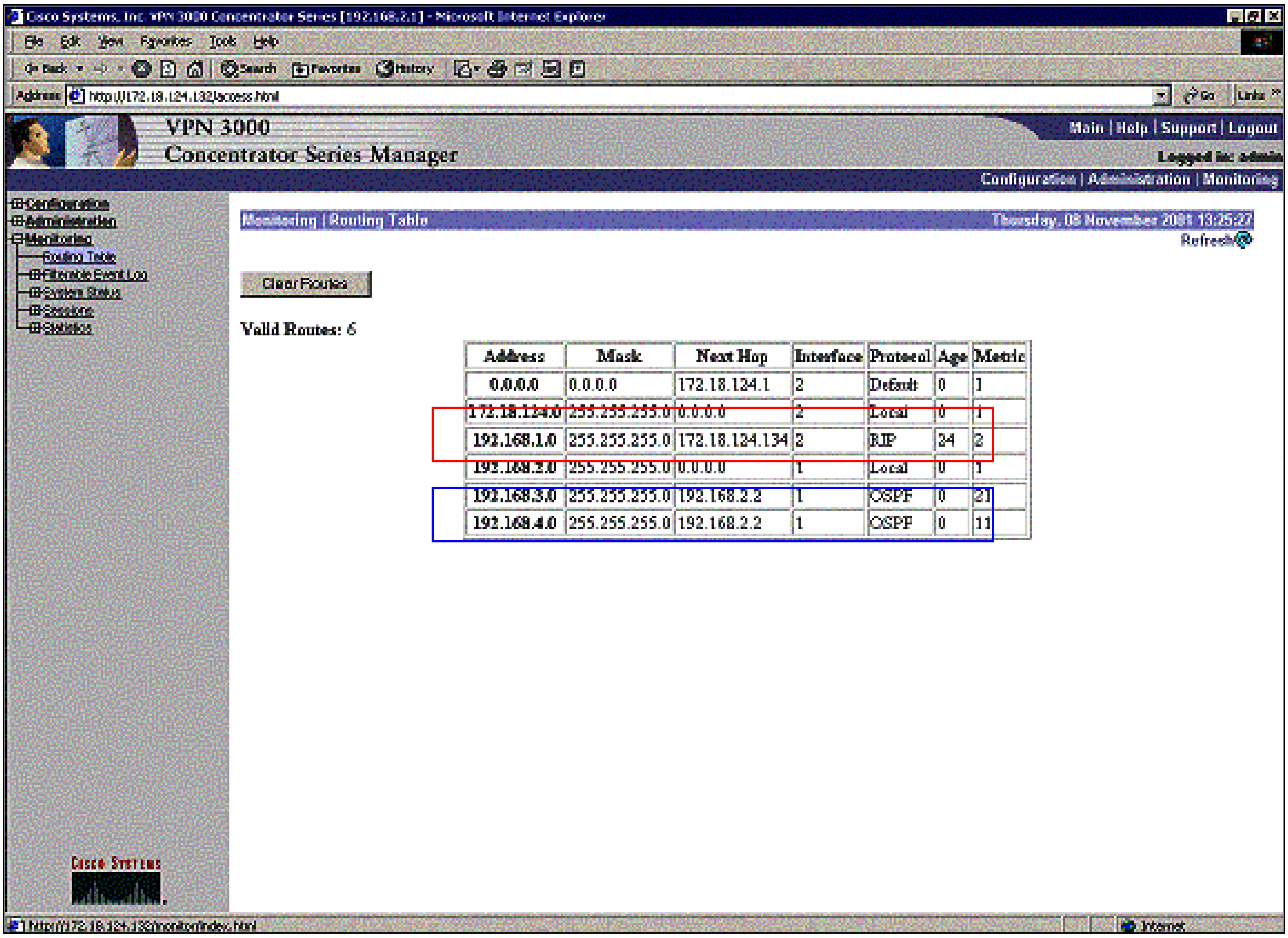

Cisco Systems, Inc. VPN 3000 Concentrator [192.168.1.1] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.18.124.134/access.html
Go Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Monitoring
Routing Table
Filterable Event Log
System Status
Sessions
Statistics
Monitoring | Routing Table
Thursday, 08 November 2001 13:40:28
Refresh
Clear Routes
Cisco Systems
http://172.18.124.134/monitor/index.html
Internet

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	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

Le reti 192.168.2.x e 192.168.3.x vengono entrambe imparate tramite i tunnel VPN, rispettivamente 172.18.124.132 e 172.18.124.131. La rete 192.168.4.x viene appresa tramite il tunnel 172.18.124.132 perché gli annunci OSPF del router vengono inseriti nella tabella di routing del concentratore VPN 3030b. Quindi, la tabella di routing annuncia la rete ai peer VPN remoti.

Questa è la tabella di routing di VPN 3030b Concentrator in circostanze normali.
]


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.2.1] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.18.124.132/access.html
Go Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Monitoring
Routing Table
Filterable Event Log
System Status
Sessions
Statistics
Refresh
CISCO SYSTEMS
http://172.18.124.132/monitorindex.html
Internet

Monitoring | Routing Table Thursday, 08 November 2001 13:25:27

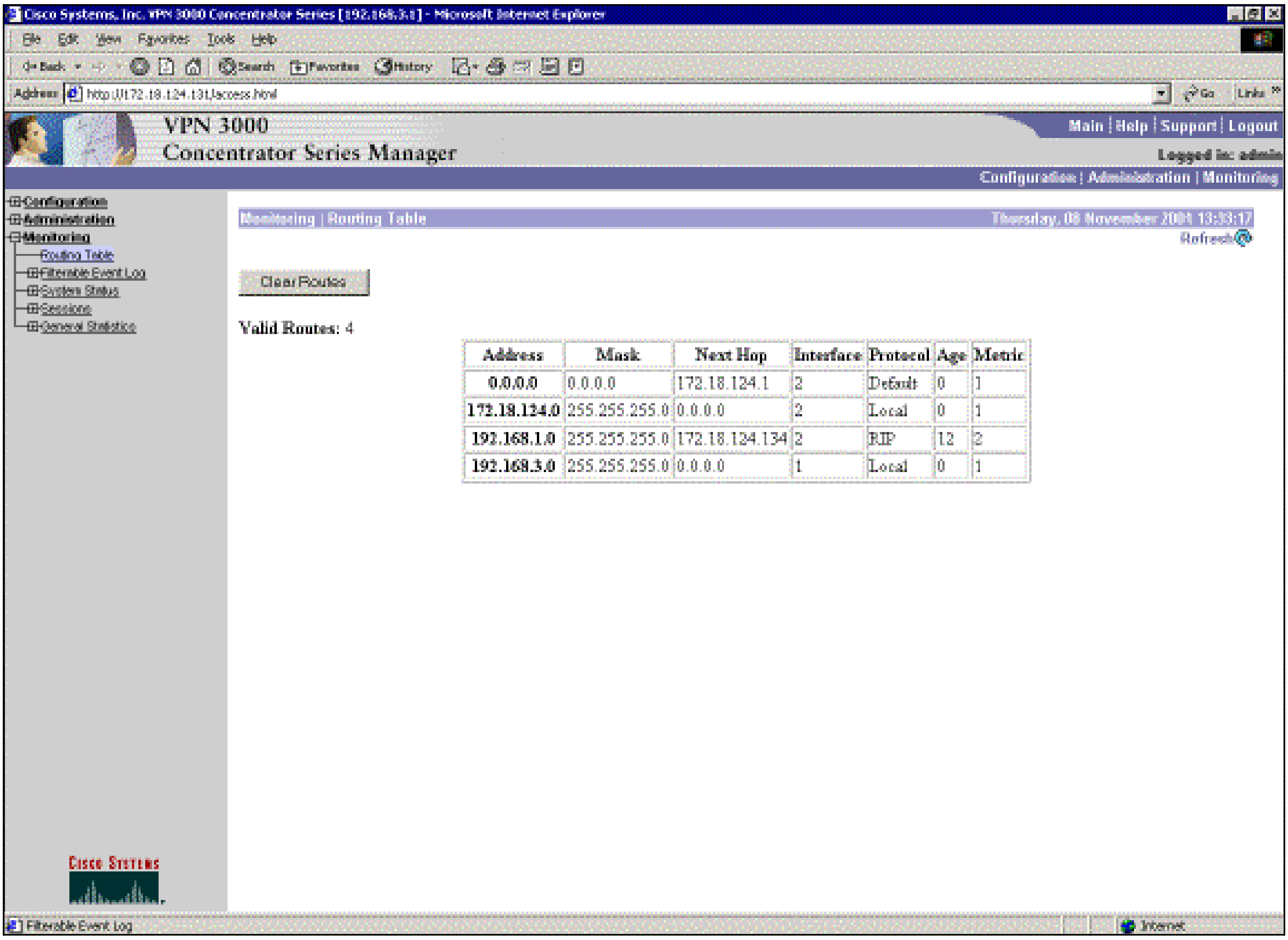
Clear Routes

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

Il riquadro rosso indica che la rete 192.168.1.x viene appresa dal tunnel VPN. La scatola blu evidenzia che le reti 192.168.3.x e 192.168.4.x vengono apprese tramite il processo OSPF principale.

Questa è la tabella di routing di VPN 3060a Concentrator in circostanze normali.


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.3.1] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.18.124.131/access.html
Go Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Monitoring
Routing Table
Filterable Event Log
System Status
Sessions
General Statistics
Refresh
Clear Routes
Filterable Event Log
Internet

Monitoring | Routing Table Thursday, 08 November 2001 13:33:17

Valid Routes: 4

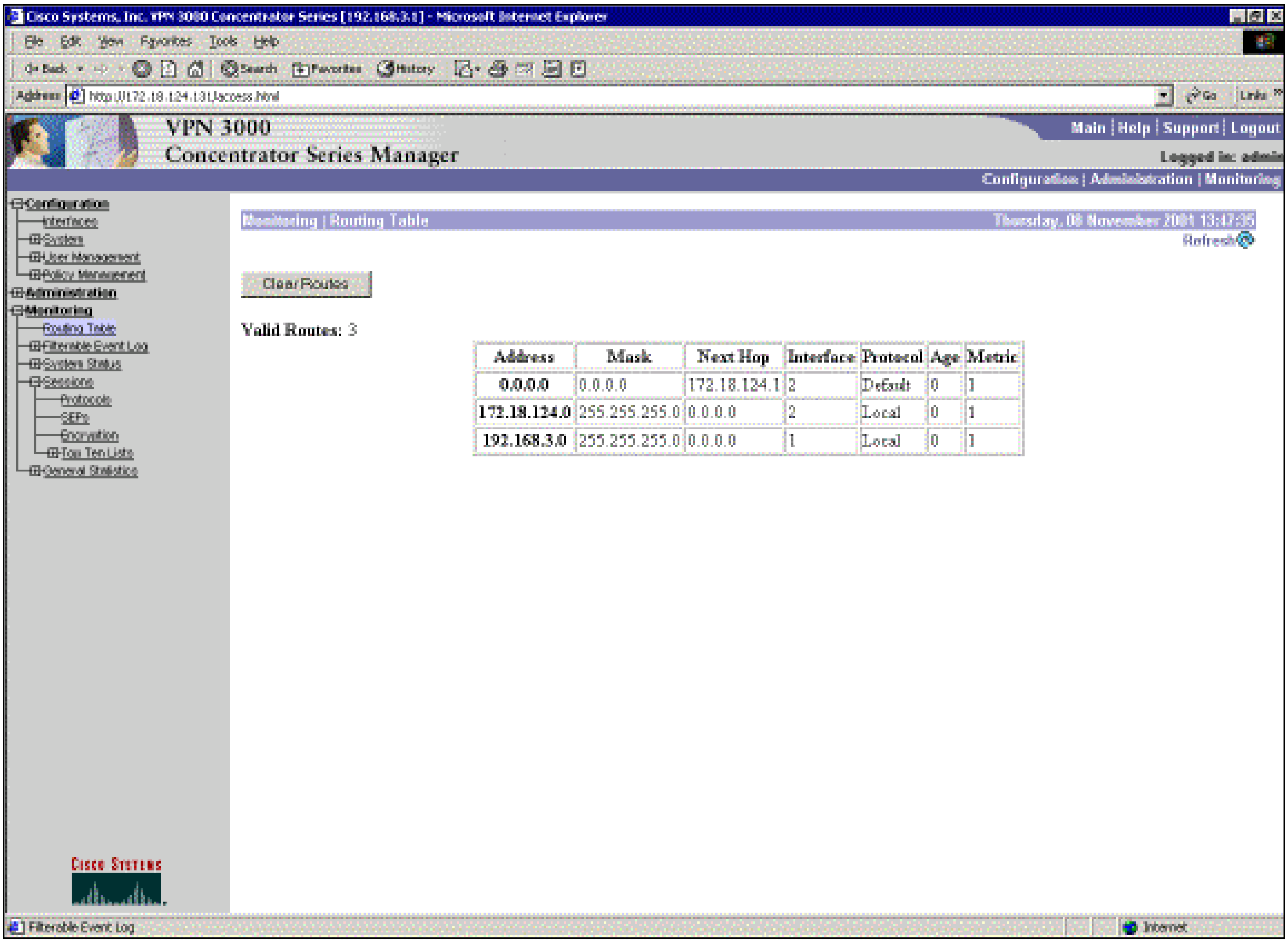
Address	Mask	Next Hop	Interface	Protocol	Age	Metric
0.0.0.0	0.0.0.0	172.18.124.1	2	Default	0	1
172.18.124.0	255.255.255.0	0.0.0.0	2	Local	0	1
192.168.1.0	255.255.255.0	172.18.124.134	2	RIP	12	2
192.168.3.0	255.255.255.0	0.0.0.0	1	Local	0	1

La rete 192.168.1.x è l'unica rete qui e può essere raggiunta tramite il tunnel VPN. Non esiste una rete 192.168.2.0 poiché nessun processo (ad esempio RIP) passa lungo tale percorso. Non si perde nulla finché i PC sulla rete 192.168.3.x non puntano il gateway predefinito al VPN Concentrator. Se lo si desidera, è sempre possibile aggiungere una route statica. Tuttavia, per questo esempio, il VPN Concentrator stesso non deve raggiungere la rete 192.168.2.0.

Risoluzione dei problemi

Errore simulato

Si tratta di un errore simulato nella configurazione. Se si rimuove il filtro dall'interfaccia pubblica, il tunnel VPN viene eliminato. In questo modo, cade anche il percorso per la 192.168.1.0 appresa attraverso il tunnel. Il processo RIP impiega circa tre minuti per eliminare la route. Pertanto, è possibile che si verifichi un'interruzione di tre minuti fino a quando il ciclo di lavorazione non si interrompe.


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.3.1] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.18.124.131/access.html
Go Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Administration
Monitoring
Routing Table
Filterable Event Log
System Status
Sessions
Protocols
SEPs
Encryption
Top Ten Lists
General Statistics
Cisco Systems
Filterable Event Log
Internet

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

Dopo la scadenza della route RIP, la nuova tabella di routing sui router sarà simile alla seguente:

```
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
```

Problemi che possono verificarsi

Se si dimentica di aggiungere la modifica della distanza di amministrazione a 130, è possibile che venga visualizzato questo output. Notare che entrambi i tunnel VPN sono attivi.

VPN 3080 Concentrator

Nota: si tratta della versione dell'interfaccia utente non grafica (GUI) della tabella di routing.

```
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
```

Per raggiungere la rete 192.168.3.0, il percorso deve passare attraverso 172.18.124.131. Tuttavia, la tabella di routing su RTR-3620 mostra:

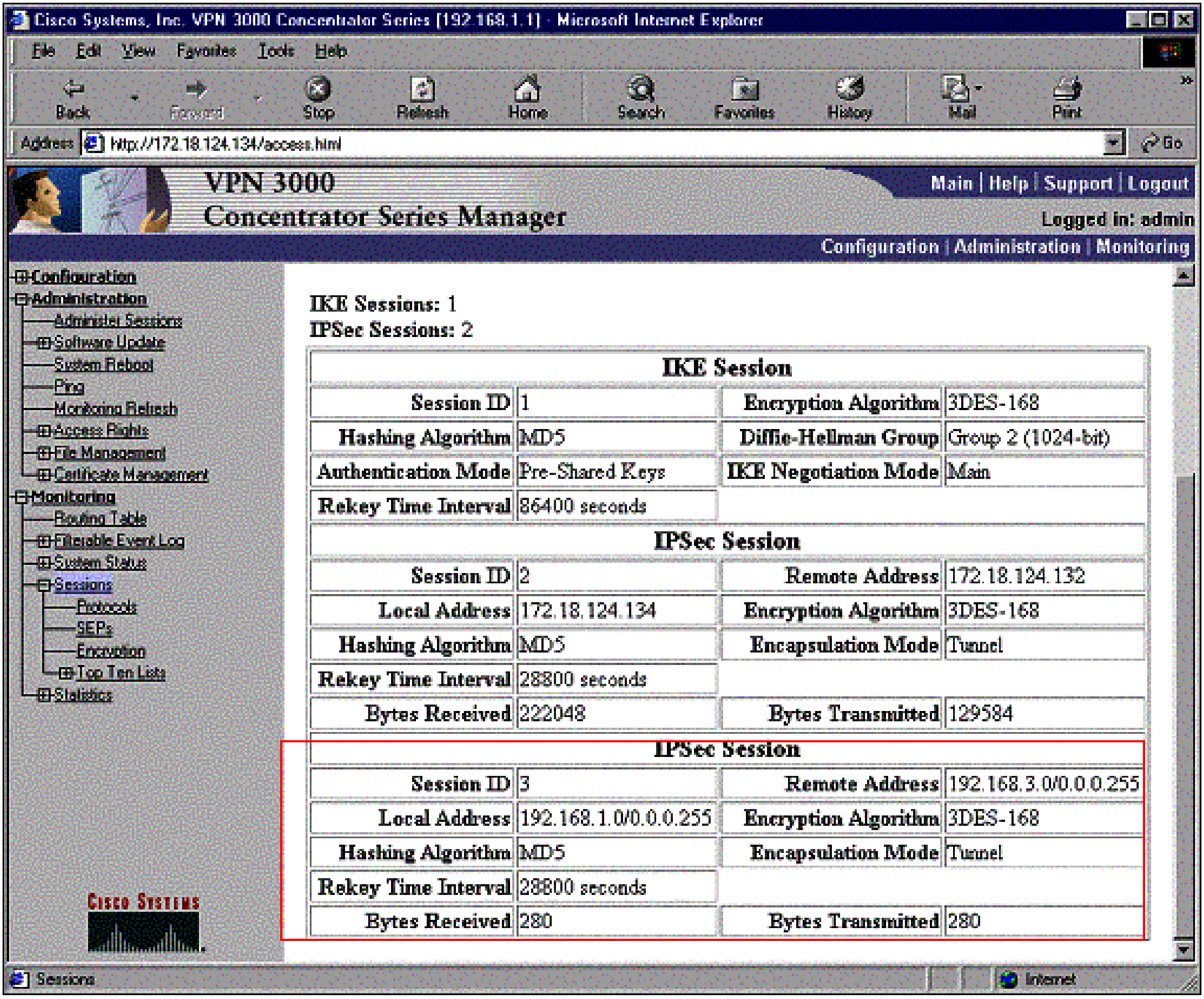
```
rtr-3620#show ip route

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
```

Per tornare alla rete 192.168.1.0, il percorso deve passare attraverso la rete 192.168.4.x della backbone.

Il traffico continua a funzionare perché il rilevamento automatico genera le informazioni corrette sulle associazioni di sicurezza (SA) sul concentratore VPN 3030b. Ad esempio:

```
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
```


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://172.18.124.134/access.html
Go
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
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
Cisco Systems
Sessions
Internet

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

Anche se la tabella di routing indica che il peer deve essere 172.18.124.131, l'SA (flusso del traffico) effettivo viene trasmesso dal concentratore VPN 3030b al numero 172.18.124.132. La tabella SA ha la precedenza sulla tabella di routing. Solo un esame approfondito della tabella dei percorsi e della tabella SA sul concentratore VPN 3060a indica che il traffico non scorre nella direzione corretta.

Informazioni correlate

- Cisco VPN serie 3000 Concentrator Support Page
- Pagina di supporto per IPSec
- Supporto tecnico – Cisco Systems