

Configuration du routage redondant sur le concentrateur VPN 3000

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations du routeur](#)

[Configuration du concentrateur VPN 3080](#)

[Configuration du concentrateur VPN 3060a](#)

[Configuration du concentrateur VPN 3030b](#)

[Vérification](#)

[Dépannage](#)

[Erreur simulée](#)

[Qu'est-ce qui peut mal tourner ?](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit comment configurer un basculement VPN redondant si un site distant perd son concentrateur VPN 3000 ou sa connectivité Internet. Dans cet exemple, supposons que le réseau d'entreprise situé derrière le VPN 3030B utilise le protocole de routage OSPF (Open Shortest Path First) comme protocole de routage par défaut.

Remarque : lorsque vous redistribuez les protocoles de routage, vous pouvez former une boucle de routage qui peut causer des problèmes sur le réseau. Le protocole OSPF est utilisé dans cet exemple, mais il n'est pas le seul protocole de routage à pouvoir être utilisé.

L'objectif de cet exemple est de faire en sorte que le réseau 192.168.1.0 utilise le tunnel rouge (dans des conditions normales de fonctionnement), représenté dans la section Network Diagram, pour atteindre 192.168.3.x. Si le tunnel, le concentrateur VPN ou le FAI est abandonné, le réseau 192.168.3.0 est appris via un protocole de routage dynamique via le tunnel vert. En outre, la connectivité n'est pas perdue par le site 192.168.3.0. Une fois le problème résolu, le trafic revient automatiquement au tunnel rouge.

Remarque : RIP dispose d'un compteur d'obsolescence de trois minutes avant de permettre l'acceptation d'une nouvelle route sur une route non valide. Supposons également que les tunnels sont créés et que le trafic peut circuler entre les homologues.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeurs Cisco 3620 et 3640
- Concentrateur VPN Cisco 3080 - Version : Cisco Systems, Inc./VPN 3000 Concentrator Version 4.7
- Concentrateur VPN Cisco 3060 - Version : Cisco Systems, Inc./VPN série 3000 Concentrator Version 4.7
- Concentrateur Cisco VPN 3030 - Version : Cisco Systems, Inc./VPN série 3000 Concentrator Version 4.7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

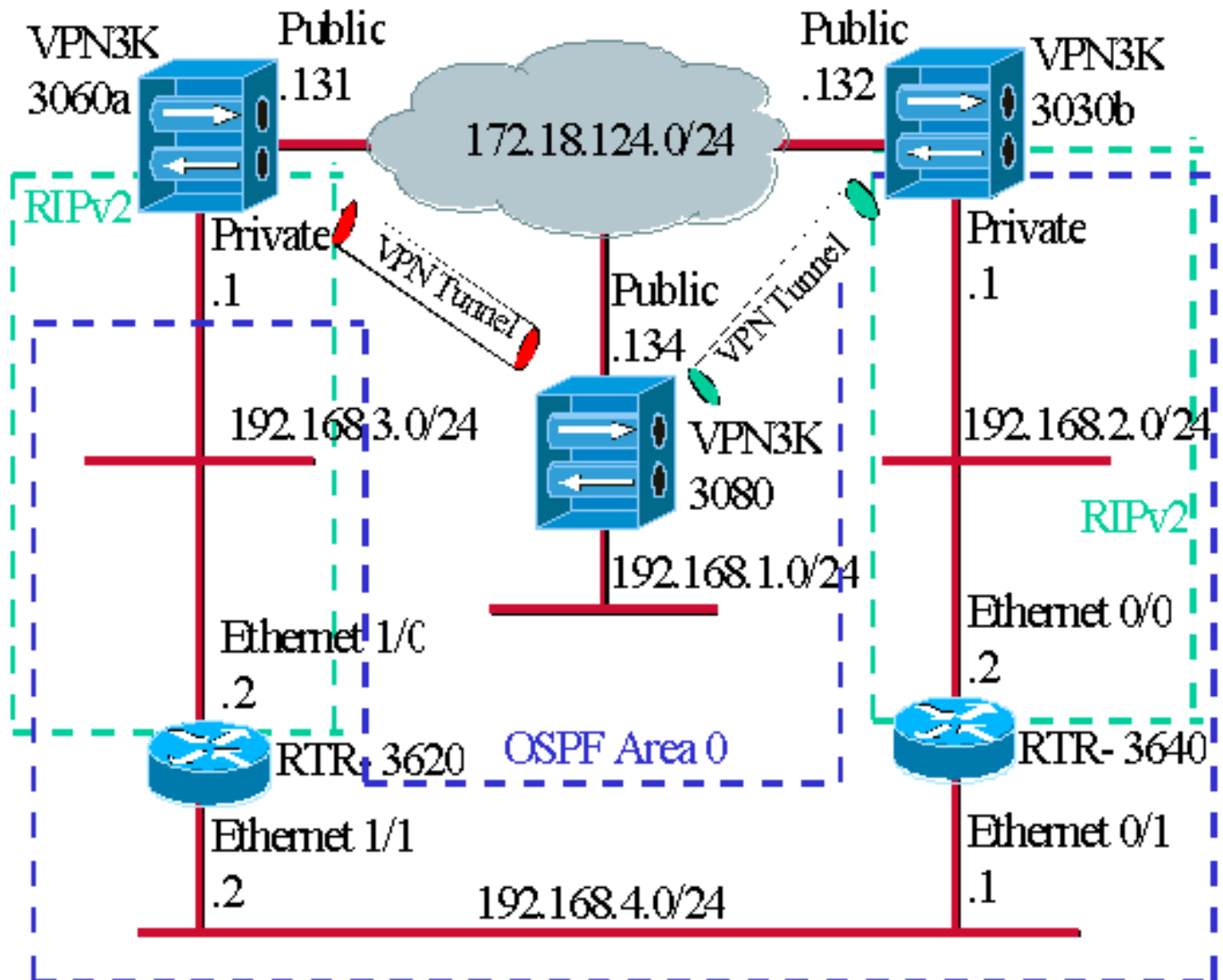
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez [l'outil de recherche de commandes](#) (clients [inscrits](#) seulement).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Les tirets bleus indiquent que le protocole OSPF est activé de VPN 3030b à RTR-3640 et RTR-3620.

Les tirets verts indiquent que RIPv2 est activé à partir de VPN privé 3060a vers RTR-3620, RTR-3640 et VPN privé 3030b.

RIPv2 est également activé sur les tunnels VPN rouges et verts, car la découverte de réseau est activée. Il n'est pas nécessaire d'activer le protocole RIP sur l'interface privée VPN 3080. Il n'existe pas non plus de protocole RIP sur le réseau 192.168.4.x, car toutes les routes sont apprises par le protocole OSPF sur cette liaison.

Remarque : les PC des réseaux 192.168.2.x et 192.168.3.x doivent avoir leurs passerelles par défaut pointant vers les routeurs et non vers les concentrateurs VPN. Autoriser les routeurs à décider où acheminer les paquets.

Configurations du routeur

Ce document utilise les configurations de routeur suivantes :

- [Routeur 3620](#)
- [Routeur 3640](#)

Routeur 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
```

Routeur 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 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

```

[Configuration du concentrateur VPN 3080](#)

[VPN LAN à LAN 3080 à VPN 3030b](#)

Sélectionnez **Configuration > Tunneling and Security > IPSec > IPSec LAN-to-LAN**. Puisque la découverte automatique du réseau est utilisée, il n'est pas nécessaire de remplir les listes de réseau local et distant.

Remarque : les concentrateurs VPN qui exécutent le logiciel version 3.1 et antérieure ont une case à cocher pour la détection automatique. La version 3.5 du logiciel (utilisée sur le VPN 3080) utilise un menu déroulant, tel que celui illustré ici.

Add a new IPSec LAN-to-LAN connection.

<p>Enable <input type="checkbox"/></p> <p>Name <input type="text" value="3080-3030b"/></p> <p>Interface <input type="text" value="Ethernet 2 (Public) (172.18.124.134)"/></p> <p>Connection Type <input type="text" value="Bi-directional"/></p> <p>Peers</p> <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> <p>172.18.124.132</p> </div> <p>Digital Certificate <input type="text" value="None (Use Preshared Keys)"/></p> <p>Certificate Transmission <input type="radio"/> Entire certificate chain <input type="radio"/> Identity certificate only</p> <p>Preshared Key <input type="text"/></p> <p>Authentication <input type="text" value="ESP/MD5/HMAC-128"/></p> <p>Encryption <input type="text" value="3DES-168"/></p> <p>IKE Proposal <input type="text" value="IKE-3DES-MD5"/></p> <p>Filter <input type="text" value="-None-"/></p> <p>Bandwidth Policy <input type="text" value="-None-"/></p> <p>Routing <input type="text" value="Network Autodiscovery"/></p>	<p>Check to enable this LAN-to-LAN connection.</p> <p>Enter the name for this LAN-to-LAN connection.</p> <p>Select the interface for this LAN-to-LAN connection.</p> <p>Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> may have multiple peers specified below.</p> <p>Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses, one IP address per line.</p> <p>Select the digital certificate to use.</p> <p>Choose how to send the digital certificate to the IKE peer.</p> <p>Enter the preshared key for this LAN-to-LAN connection.</p> <p>Specify the packet authentication mechanism to use.</p> <p>Specify the encryption mechanism to use.</p> <p>Select the IKE Proposal to use for this LAN-to-LAN connection.</p> <p>Choose the filter to apply to the traffic that is tunneled through the LAN connection, under NAT Transparency.</p> <p>Choose the bandwidth policy to apply to this LAN-to-LAN connection.</p> <p>Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.</p>
<p>Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.</p> <p>Network List <input type="text" value="Use IP Address/Wildcard-mask below"/> Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.</p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p> <p>Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.</p> <p>Network List <input type="text" value="Use IP Address/Wildcard-mask below"/> Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.</p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	
<p><input type="button" value="Add"/> <input type="button" value="Cancel"/></p>	

[VPN LAN à LAN 3080 à VPN 3060a](#)

Sélectionnez Configuration > Tunneling and Security > IPSec > IPSec LAN-to-LAN. Puisque la

découverte automatique du réseau est utilisée, il n'est pas nécessaire de remplir les listes de réseau local et distant.

Remarque : les concentrateurs VPN qui exécutent le logiciel version 3.1 et antérieure ont une case à cocher pour la détection automatique. La version 3.5 du logiciel (utilisée sur le VPN 3080) utilise un menu déroulant, tel que celui illustré ici.

Add a new IPsec LAN-to-LAN connection.

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

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

<p>Network List <input type="text" value="Use IP Address/Wildcard-mask below"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	<p>Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.</p> <p>Note: Enter a <i>wildcard mask</i>, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.</p>
---	---

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

<p>Network List <input type="text" value="Use IP Address/Wildcard-mask below"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	<p>Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.</p> <p>Note: Enter a <i>wildcard mask</i>, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match.</p>
---	--

[Configuration du concentrateur VPN 3060a](#)

[VPN LAN à LAN 3060a à VPN 3080](#)

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

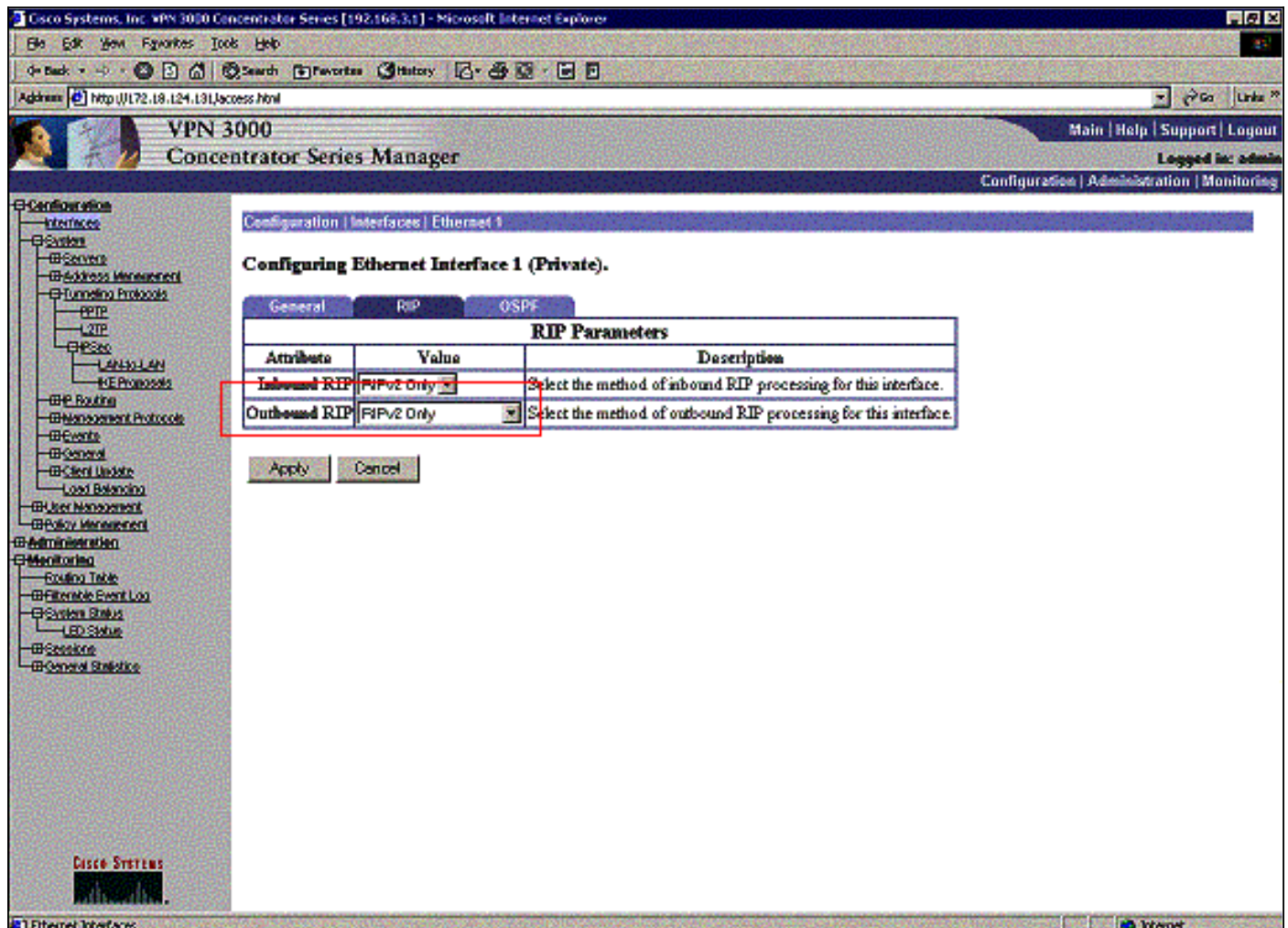
Remarque : Il existe une case à cocher sur le VPN 3060 pour la découverte automatique de réseau au lieu du menu déroulant comme dans les versions 3.5 et ultérieures du logiciel.

Configuration Tunneling and Security IPSec LAN-to-LAN Add	
Add a new IPSec LAN-to-LAN connection.	
Enable <input type="checkbox"/>	Check to enable this LAN-to-LAN connection.
Name <input type="text" value="3060a-3080"/>	Enter the name for this LAN-to-LAN connection.
Interface <input type="text" value="Ethernet 2 (Public) (172.18.124.131)"/>	Select the interface for this LAN-to-LAN connection.
Connection Type <input type="text" value="Bi-directional"/>	Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.
Peers <input type="text" value="172.18.124.134"/>	Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses, one IP address per line.
Digital Certificate <input type="text" value="None (Use Preshared Keys)"/>	Select the digital certificate to use.
Certificate Transmission <input type="radio"/> Entire certificate chain <input type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
Preshared Key <input type="text"/>	Enter the preshared key for this LAN-to-LAN connection.
Authentication <input type="text" value="ESP/MD5/HMAC-128"/>	Specify the packet authentication mechanism to use.
Encryption <input type="text" value="3DES-168"/>	Specify the encryption mechanism to use.
IKE Proposal <input type="text" value="IKE-3DES-MD5"/>	Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter <input type="text" value="-None-"/>	Choose the filter to apply to the traffic that is tunneled through this LAN connection.
IPSec NAT-T <input type="checkbox"/>	Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over under NAT Transparency.
Bandwidth Policy <input type="text" value="-None-"/>	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Routing <input type="text" value="Network Autodiscovery"/>	Choose the routing mechanism to use. Parameters below are ignored. Network Autodiscovery is chosen.
Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.	
Network List <input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address <input type="text"/>	Note: Enter a <i>wildcard mask</i> , which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to use. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask <input type="text"/>	
Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.	
Network List <input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address <input type="text"/>	Note: Enter a <i>wildcard mask</i> , which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to use.
Wildcard Mask <input type="text"/>	

[Activez le protocole RIP pour transmettre les routes apprises par le tunnel au routeur VPN 3620](#)

Sélectionnez **Configuration > Interfaces > Private > RIP**. Remplacez le menu déroulant par **RIPv2 Only** et cliquez sur **Apply**. Sélectionnez ensuite **Configuration > System > Tunneling Protocols > IPSec > LAN-to-LAN**.

Remarque : La valeur par défaut est le protocole RIP sortant et il est désactivé pour l'interface privée.



The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The left sidebar contains a navigation tree with categories like Configuration, Administration, and Monitoring. The main content area is titled "Configuring Ethernet Interface 1 (Private)" and has tabs for General, RIP, and OSPF. The RIP tab is active, displaying a table of RIP Parameters. The table has three columns: Attribute, Value, and Description. Two rows are visible: "Inbound RIP" and "Outbound RIP", both with "RIPv2 Only" selected in the Value column. Below the table are "Apply" and "Cancel" buttons.

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.

[Configuration du concentrateur VPN 3030b](#)

[VPN LAN à LAN 3030b à VPN 3080](#)

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

Add a new IPSec LAN-to-LAN connection.

<p>Enable <input type="checkbox"/></p> <p>Name <input type="text" value="3030B-3080"/></p> <p>Interface <input type="text" value="Ethernet 2 (Public) (172.18.124.132)"/></p> <p>Connection Type <input type="text" value="Bi-directional"/></p> <p>Peers</p> <div style="border: 1px solid black; padding: 5px; min-height: 100px;"> <p>172.18.124.134</p> </div> <p>Digital Certificate <input type="text" value="None (Use Preshared Keys)"/></p> <p>Certificate Transmission <input type="radio"/> Entire certificate chain <input type="radio"/> Identity certificate only</p> <p>Preshared Key <input type="text"/></p> <p>Authentication <input type="text" value="ESP/MD5/HMAC-128"/></p> <p>Encryption <input type="text" value="3DES-168"/></p> <p>IKE Proposal <input type="text" value="IKE-3DES-MD5"/></p> <p>Filter <input type="text" value="-None-"/></p> <p>IPSec NAT-T <input type="checkbox"/></p> <p>Bandwidth Policy <input type="text" value="-None-"/></p> <p>Routing <input type="text" value="Network Autodiscovery"/></p>	<p>Check to enable this LAN-to-LAN connection.</p> <p>Enter the name for this LAN-to-LAN connection.</p> <p>Select the interface for this LAN-to-LAN connection.</p> <p>Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.</p> <p>Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses, one IP address per line.</p> <p>Select the digital certificate to use.</p> <p>Choose how to send the digital certificate to the IKE peer.</p> <p>Enter the preshared key for this LAN-to-LAN connection.</p> <p>Specify the packet authentication mechanism to use.</p> <p>Specify the encryption mechanism to use.</p> <p>Select the IKE Proposal to use for this LAN-to-LAN connection.</p> <p>Choose the filter to apply to the traffic that is tunneled through this LAN connection.</p> <p>Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over under NAT Transparency.</p> <p>Choose the bandwidth policy to apply to this LAN-to-LAN connection.</p> <p>Choose the routing mechanism to use. Parameters below are ignored. Network Autodiscovery is chosen.</p>
<p>Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.</p> <p>Network List <input type="text" value="Use IP Address/Wildcard-mask below"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	
<p>Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.</p> <p>Network List <input type="text" value="Use IP Address/Wildcard-mask below"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	

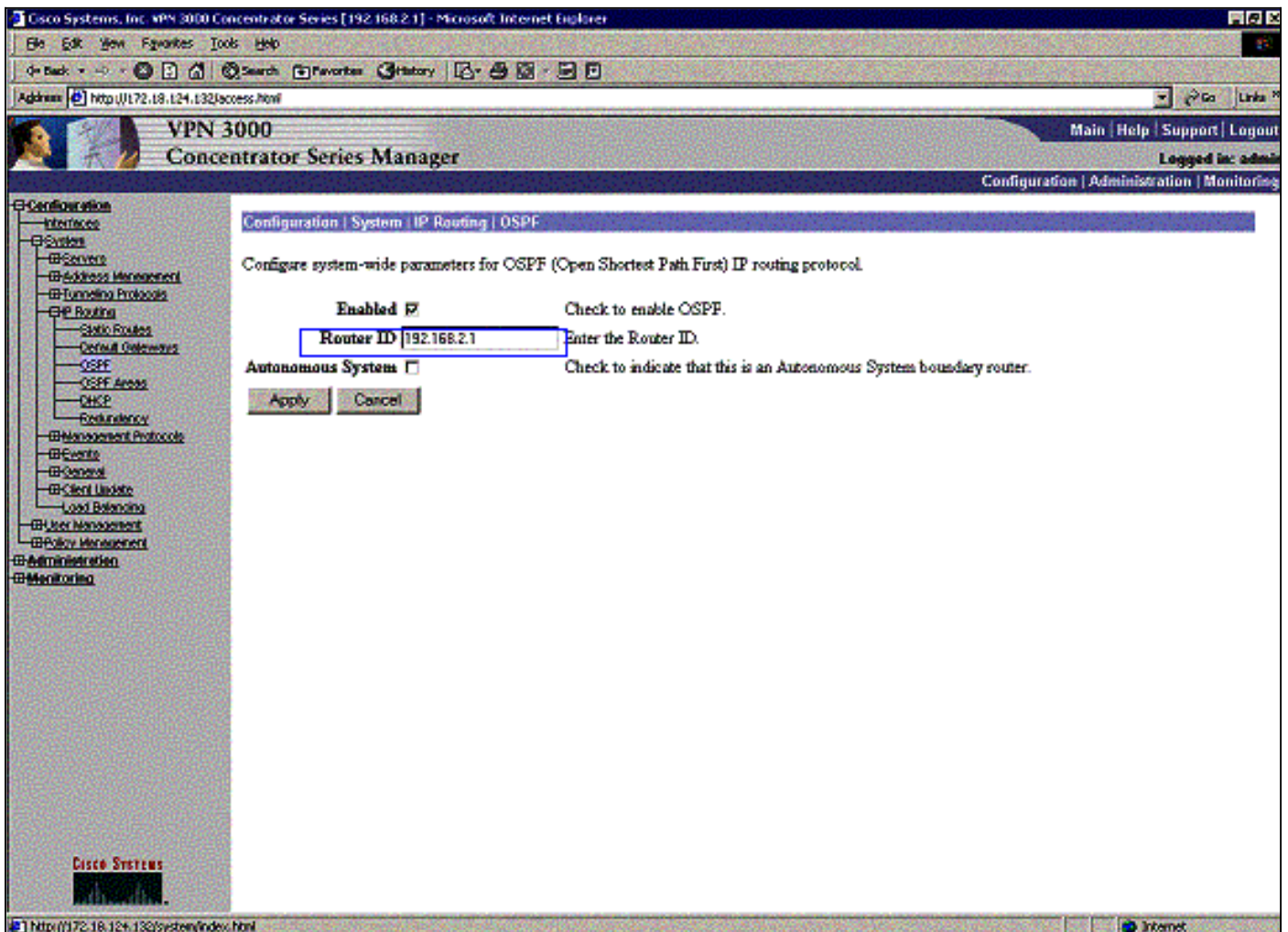
[Activez le protocole RIP pour transmettre les routes apprises par le tunnel au routeur VPN 3640](#)

Suivez les étapes indiquées précédemment dans ce document pour [le concentrateur VPN 3060a](#).

[Permettre au protocole OSPF de transmettre les routes apprises par le réseau fédérateur au](#)

concentrateur VPN 3030b

Sélectionnez **Configuration > System > IP Routing > OSPF** et saisissez l'ID de routeur.



```
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 de zone doit correspondre à l'ID du câble. Puisque la zone de cet exemple est 0, elle est représentée par 0.0.0.0. Cochez également la case **Enable OSPF** et cliquez sur **Apply**.

Configuration | Interfaces | Ethernet 1

Configuring Ethernet Interface 1 (Private).

General RIP OSPF

OSPF Parameters		
Attribute	Value	Description
OSPF Enabled	<input checked="" type="checkbox"/>	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.

Apply Cancel

Assurez-vous que vos compteurs OSPF correspondent à ceux du routeur. Pour vérifier les compteurs des routeurs, utilisez la commande **show ip ospf interface <interface name>**.

```
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)
```

Pour plus d'informations sur OSPF, référez-vous à [RFC 1247](#).

Vérification

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Cette sortie de commande affiche des tables de routage précises.

```
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
```

Il s'agit de la table de routage du concentrateur VPN 3080 dans des circonstances normales.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The page title is "VPN 3000 Concentrator Series Manager". The navigation menu on the left includes Configuration, Administration, and Monitoring. The Monitoring section is expanded, showing Routing Table, Filterable Event Log, System Status, Sessions, and Statistics. The Routing Table page is active, displaying a "Clear Routes" button and a table of valid routes. The table has 7 columns: Address, Mask, Next Hop, Interface, Protocol, Age, and Metric. There are 6 rows of data.

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

Les réseaux 192.168.2.x et 192.168.3.x sont tous deux appris via les tunnels VPN 172.18.124.132 et 172.18.124.131, respectivement. Le réseau 192.168.4.x est appris via le tunnel 172.18.124.132 car les annonces OSPF du routeur sont placées dans la table de routage du concentrateur VPN 3030b. Ensuite, la table de routage annonce le réseau aux homologues VPN distants.

Il s'agit de la table de routage du concentrateur VPN 3030b dans des circonstances normales.

VPN 3000 Concentrator Series Manager

Monitoring | Routing Table

Thursday, 08 November 2001 13:25:27

Refresh

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

La zone rouge indique que le réseau 192.168.1.x est appris à partir du tunnel VPN. La zone bleue indique que les réseaux 192.168.3.x et 192.168.4.x sont appris via le processus OSPF principal.

Il s'agit de la table de routage du concentrateur VPN 3060a dans des circonstances normales.

Monitoring | Routing Table

Thursday, 08 November 2001 13:33:17

Refresh

Clear Routes

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

Le réseau 192.168.1.x est le seul réseau ici, et il peut être atteint via le tunnel VPN. Il n'y a pas de réseau 192.168.2.0, car aucun processus (tel que RIP) ne passe le long de cette route. Il n'y a rien de perdu tant que les PC du réseau 192.168.3.x ne pointent pas leur passerelle par défaut vers le concentrateur VPN. Vous pouvez toujours ajouter une route statique si vous le souhaitez. Cependant, pour cet exemple, le concentrateur VPN lui-même n'a pas besoin d'atteindre le réseau 192.168.2.0.

Dépannage

Erreur simulée

Il s'agit d'une erreur simulée dans la configuration. Si vous supprimez le filtre vers l'interface publique, le tunnel VPN est abandonné. Cela entraîne également la perte de la route pour 192.168.1.0 apprise via le tunnel. Il faut environ trois minutes au processus RIP pour supprimer la route. Par conséquent, vous pouvez avoir une panne de trois minutes jusqu'à ce que la route expire elle-même.

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

Une fois la route RIP expirée, la nouvelle table de routage sur les routeurs apparaît comme suit :

```
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
```

Qu'est-ce qui peut mal tourner ?

Si vous oubliez d'ajouter la distance admin à 130, vous pouvez peut-être voir cette sortie. Notez que les deux tunnels VPN sont activés.

Concentrateur VPN 3080

Remarque : Il s'agit de la version de l'interface utilisateur graphique (GUI) non graphique de la table de routage.

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

Pour accéder au réseau 192.168.3.0, la route doit passer par 172.18.124.131. Cependant, la table de routage sur RTR-3620 affiche :

```
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

Pour revenir au réseau 192.168.1.0, la route doit passer par le réseau fédérateur 192.168.4.x.

Le trafic fonctionne toujours puisque la détection automatique génère les informations d'association de sécurité (SA) appropriées sur le concentrateur VPN 3030b. Exemple :

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

```

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout
 Logged in: admin
 Configuration | Administration | Monitoring

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

Même si la table de routage indique que l'homologue doit être 172.18.124.131, la SA réelle (flux de trafic) passe par le concentrateur VPN 3030b à 172.18.124.132. La table SA prime sur la table de routage. Seul un examen approfondi de la table de routage et de la table SA sur le concentrateur VPN 3060a montre que le trafic ne circule pas dans la bonne direction.

Informations connexes

- [Page d'assistance des concentrateurs VPN Cisco 3000](#)
- [Page d'assistance IPsec](#)
- [Support technique - Cisco Systems](#)