

VPN 3000 زكرم ىلع رركتم لا هيچوت لا نيوكت

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[التكوين](#)

[الرسم التخطيطي للشبكة](#)

[تكوينات الموجه](#)

[تكوين مركز VPN 3080](#)

[تكوين مركز VPN 3060A](#)

[تكوين مركز VPN 3030B](#)

[التحقق من الصحة](#)

[استكشاف الأخطاء وإصلاحها](#)

[صدع محاكي](#)

[ما الذي يمكن أن يحدث بشكل خاطئ؟](#)

[معلومات ذات صلة](#)

المقدمة

يصف هذا المستند كيفية تكوين تجاوز فشل الشبكة الخاصة الظاهرية (VPN) المكررة إذا فقد موقع بعيد مركز VPN 3000 أو الاتصال بالإنترنت الخاص به. في هذا المثال، لنفترض أن شبكة الشركة الموجودة خلف شبكة VPN 3030B تستخدم بروتوكول فتح أقصر مسار أولا (OSPF) كبروتوكول توجيه افتراضي لها.

ملاحظة: عند إعادة التوزيع بين بروتوكولات التوجيه، يمكنك تكوين حلقة توجيه قد تسبب في حدوث مشكلة على الشبكة. يتم استخدام OSPF في هذا المثال، ولكنه ليس بروتوكول التوجيه الوحيد الذي يمكن استخدامه.

الهدف من هذا المثال هو أن تستخدم شبكة 192.168.1.0 النفق الأحمر (في ظروف التشغيل العادية)، كما هو موضح في قسم رسم بياني للشبكة، للوصول إلى 3.192.168.x. إذا كان النفق أو مركز الشبكة الخاصة الظاهرية (VPN) أو نقاط ISP تسقط، فسيتم تعلم شبكة 192.168.3.0 عبر بروتوكول توجيه ديناميكي عبر النفق الأخضر. كما أن إمكانية الاتصال لم تفقد في الموقع 192.168.3.0. ما إن حلت الإصدار، الحركة مرور تلقائيا رجعت إلى النفق الأحمر.

ملاحظة: يحتوي بروتوكول معلومات التوجيه (RIP) على مؤقت تأخر لمدة ثلاث دقائق قبل أن يسمح بقبول مسار جديد عبر مسار غير صالح. افترض أيضا ان الانفاق تتشأن حركة المرور يمكن ان تمر بين النظراء.

المتطلبات الأساسية

[المتطلبات](#)

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- الموجهات من Cisco طراز 3620 و 3640
 - مركز Cisco VPN 3080 - الإصدار: Cisco Systems، Inc./VPN 3000 Concentrator، الإصدار 4.7
 - مركز Cisco VPN 3060 - الإصدار: Cisco Systems، Inc./VPN 3000 Concentrator Series، الإصدار 4.7
 - مركز Cisco VPN 3030 - الإصدار: Cisco Systems، Inc./VPN 3000 Concentrator Series، الإصدار 4.7
- تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين مسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى [اصطلاحات تلمحات Cisco التقنية](#).

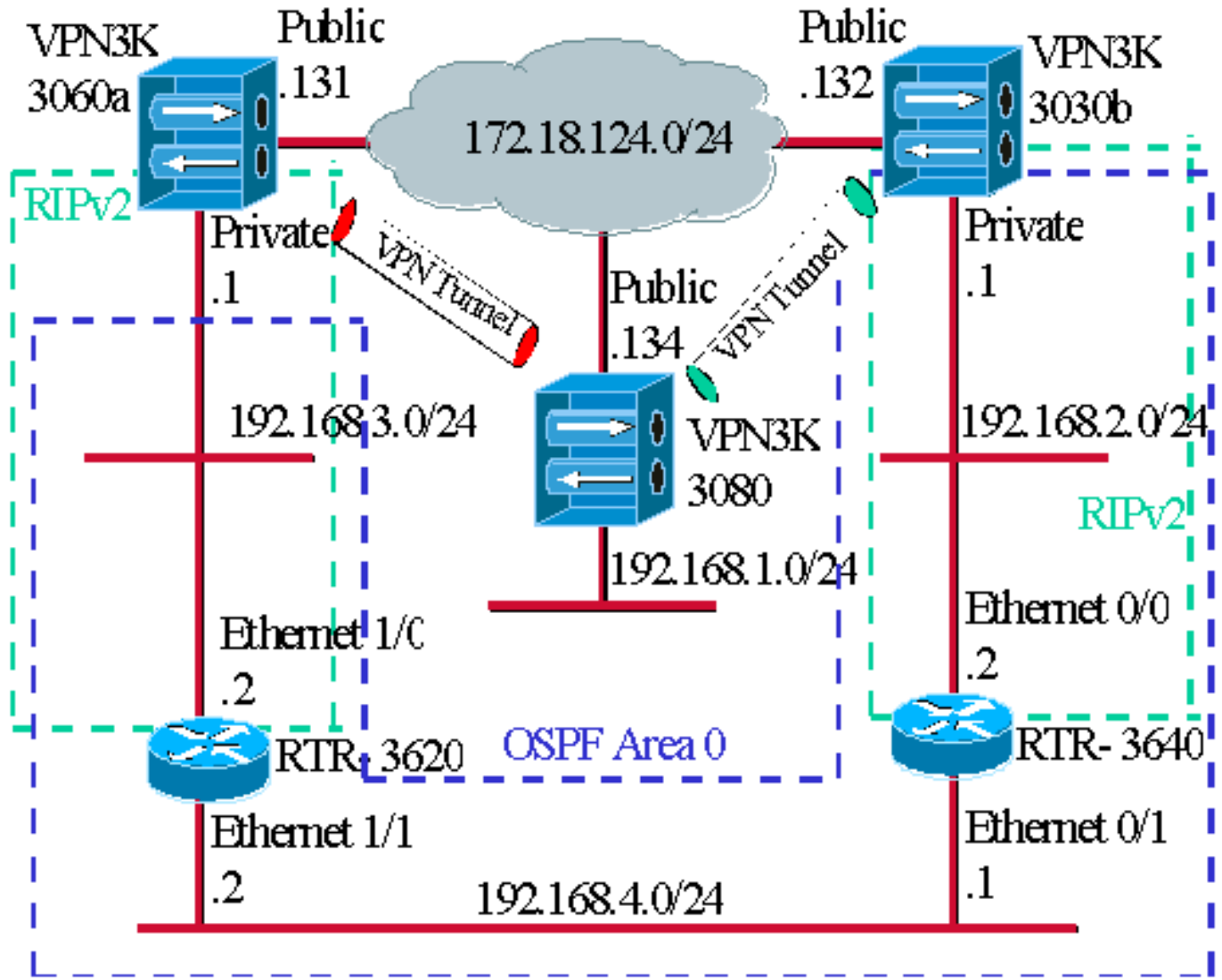
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، استخدم [أداة بحث الأوامر \(للعلماء المسجلين فقط\)](#).

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



تشير الشرطات الزرقاء إلى تمكين OSPF من VPN 3030b إلى RTR-3620 و RTR-3640.

تشير الشرطات الخضراء إلى أنه يتم تمكين RIPv2 من الشبكة الخاصة VPN 3060a إلى RTR- و RTR-3620 و VPN 3640 الخاصة بـ 3030b.

كما يتم تمكين RIPv2 على أنفاق الشبكة الخاصة الظاهرية (VPN) الحمراء والخضراء نظرا لتمكين اكتشاف الشبكة. ليس ضروري أن يمكن RIP على الـ VPN 3080 خاص قارن. لا يوجد أيضا بروتوكول معلومات التوجيه (RIP) على شبكة 192.168.4.x لأن جميع المسارات يتم التعرف عليها بواسطة OSPF عبر هذا الارتباط.

ملاحظة: تحتاج أجهزة الكمبيوتر الموجودة على شبكتي 192.168.2.x و 192.168.3.x إلى أن تكون لها بواباتها الافتراضية التي تشير إلى الموجهات وليس إلى مراكز الشبكات الخاصة الظاهرية (VPN). السماح للموجهات بتحديد مكان توجيه الحزم.

تكوينات الموجه

يستخدم هذا المستند تكوينات الموجه التالية:

- الموجه 3620
- الموجه 3640

الموجه 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

```

الموجه 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

```

تكوين مركز VPN 3080

شبكة VPN 3080 إلى VPN 3030b لشبكة LAN-to-LAN

حدد التكوين < الاتصال النفقي والأمان > IPsec LAN-to-LAN > IPsec. منذ إستخدام الاكتشاف التلقائي للشبكة، لا توجد حاجة لتعبئة قوائم الشبكة المحلية والبعيدة.

ملاحظة: تحتوي تركيزات الشبكة الخاصة الظاهرية (VPN) التي تشغل الإصدار 3.1 من البرنامج والإصدارات الأقدم على خانة إختيار للاكتشاف التلقائي. يستخدم إصدار البرنامج 3.5 (المستخدم على الشبكة الخاصة الظاهرية (VPN)) (3080) قائمة منسدلة، مثل القائمة الموضحة هنا.

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>Note: Enter a <i>wildcard</i> mask, 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>	
<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>Note: Enter a <i>wildcard</i> mask, 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>	
<p><input type="button" value="Add"/> <input type="button" value="Cancel"/></p>	

[شبكة VPN 3080 إلى VPN 3060a من LAN-to-LAN](#)

حدد التكوين < الاتصال النفقي والأمان > IPSec LAN-to-LAN > IPSec. منذ استخدام الاكتشاف التلقائي للشبكة، لا

توجد حاجة لتعبئة قوائم الشبكة المحلية والبعيدة.

ملاحظة: تحتوي تركيبات الشبكة الخاصة الظاهرية (VPN) التي تشغل الإصدار 3.1 من البرنامج والإصدارات الأقدم على خانة إختيار للاكتشاف التلقائي. يستخدم إصدار البرنامج 3.5 (المستخدم على الشبكة الخاصة الظاهرية (VPN)) قائمة منسدلة، مثل القائمة الموضحة هنا.

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="3080-3060a"/>	Enter the name for this LAN-to-LAN connection.
Interface <input type="text" value="Ethernet 2 (Public) (172.18.124.134)"/>	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="172.18.124.131"/>	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 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 if 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"/>	
Wildcard Mask <input type="text"/>	Note: Enter a <i>wildcard</i> mask, 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.

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"/>	
Wildcard Mask <input type="text"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match.

تكوين مركز VPN 3060A

شبكة VPN 3060a إلى VPN 3080 من LAN إلى LAN

حدد التكوين < الاتصال النفقي والأمان > IPsec LAN-to-LAN > IPsec.

ملاحظة: هناك خانة إختيار على شبكة VPN 3060 للاكتشاف التلقائي للشبكة بدلا من القائمة المنسدلة كما هو الحال في إصدار البرنامج 3.5 والإصدارات الأحدث.

Add a new IPSec LAN-to-LAN connection.

<p>Enable <input type="checkbox"/></p> <p>Name <input type="text" value="3060a-3080"/></p> <p>Interface <input type="text" value="Ethernet 2 (Public) (172.18.124.131)"/></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>172.18.124.134</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 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</i> mask, 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</i> mask, 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>
---	--

[قم بتمكين RIP من تمرير المسارات التي تم التعرف عليها عبر النفق إلى موجه VPN 3620](#)

حدد تشكيل < واجهات > خاص < RIP. قم بتغيير القائمة المنسدلة إلى RIPv2 فقط وانقر تطبيق. ثم حدد التكوين < النظام > بروتوكولات الاتصال النفقي < IPSec > الشبكة المحلية (LAN) إلى الشبكة المحلية (LAN).

ملاحظة: الافتراضي هو RIP الصادر، وهو معطل للواجهة الخاصة.

Configuration | Interfaces | Ethernet 1

Configuring Ethernet Interface 1 (Private).

General RIP OSPF

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

[تكوين مركز VPN 3030B](#)

[شبكة VPN من LAN إلى LAN طراز 3030b إلى 3080](#)

حدد التكوين < الاتصال النفقي والأمان < IPSec < الشبكة المحلية (LAN) إلى الشبكة المحلية (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 NAT 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>
--	--

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.

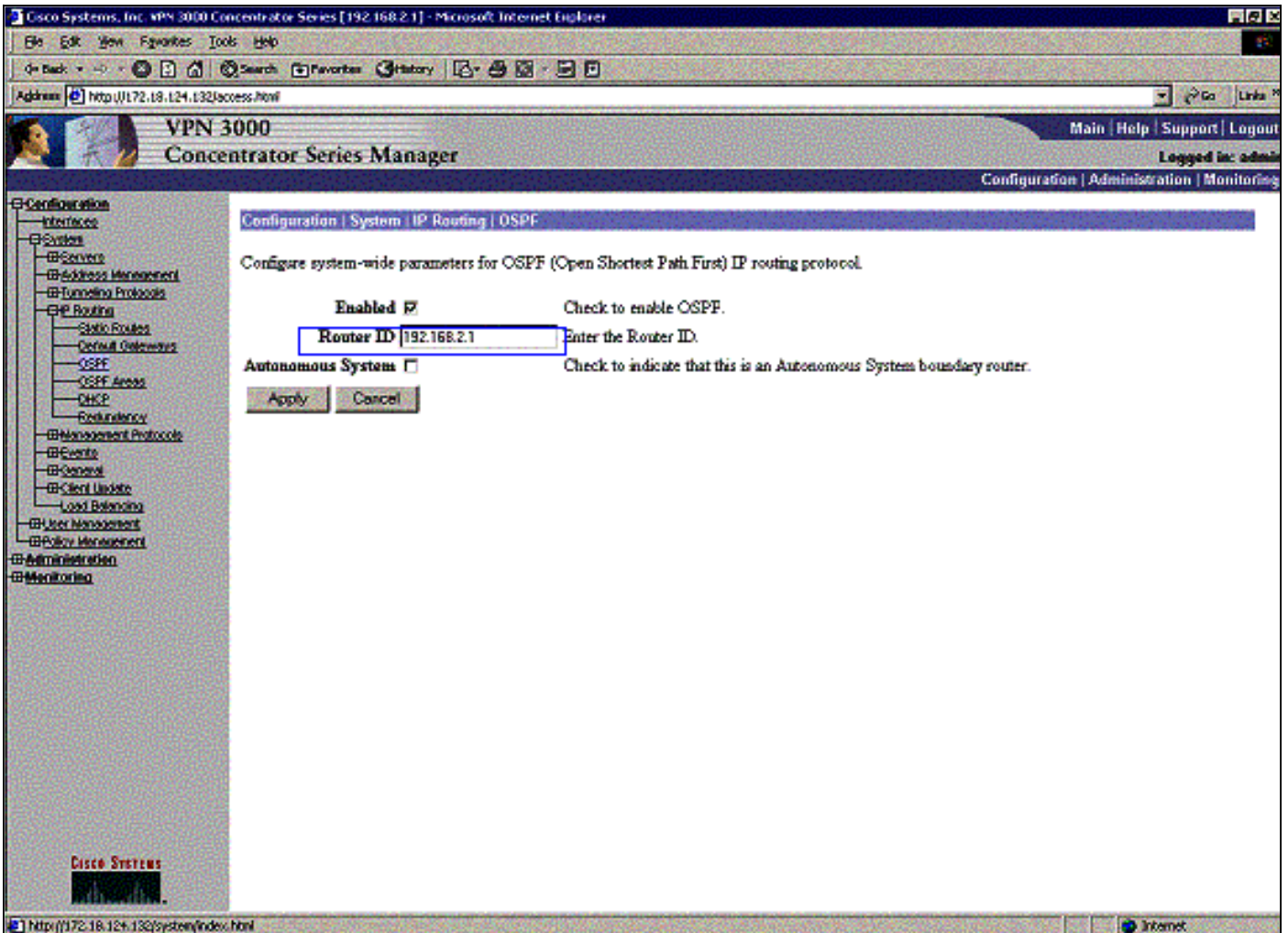
<p>Network List <input type="text" value="Use IP Address/Wildcard-mask below"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	<p>Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.</p> <p>Note: Enter a <i>wildcard 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>
---	--

[قم بتكوين RIP من تمرير المسارات التي تم التعرف عليها عبر النفق إلى موجه VPN 3640](#)

اتبع الخطوات المذكورة سابقا في هذا المستند لمحرك [VPN 3060A](#).

[تمكين OSPF من تمرير المسارات التي تم التعرف عليها عبر العمود الفقري إلى مركز VPN 3030B](#)

حدد تكوين < نظام > توجيه OSPF > IP وأدخل معرف الموجه.



```
rtr-3640#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
FULL/DR	00:00:39	192.168.4.2	Ethernet0/1	1	192.168.4.2

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
---	----------	----------	-------------	-------------

يجب أن يتطابق معرف المنطقة مع معرف السلك. بما أن المساحة في هذا المثال هي 0، فإنها تمثل ب 0.0.0.0. حدد أيضا مربع تمكين OSPF وانقر تطبيق.

تأكد من تطابق مؤقتات OSPF مع تلك الخاصة بالموجه. للتحقق من وحدات توقيت الموجهات، أستخدم الأمر `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)
لمزيد من المعلومات حول OSPF، ارجع إلى RFC 1247.
```

[التحقق من الصحة](#)

يوفر هذا القسم معلومات يمكنك استخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر العرض بواسطة [أداة مترجم الإخراج \(العملاء المسجلون فقط\)](#)، والتي تتيح لك عرض تحليل

إخراج أمر العرض.

تعرض مخرجات الأمر هذه جداول توجيه دقيقة.

```
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

          is subnetted, 1 subnets 172.18.0.0/24
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

          is subnetted, 1 subnets 172.18.0.0/24
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
```

هذا هو جدول توجيه مركز VPN 3080 في الظروف العادية.

Cisco Systems, Inc. VPN 3000 Concentrator [192.168.1.1] - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://172.18.124.134/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Configuration | Administration | Monitoring

Thursday, 08 November 2001 13:40:20

Refresh

Monitoring | Routing Table

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	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

Internet

يتم تعلم الشبكات x.192.168.2 و x.192.168.3 من خلال أنفاق الشبكة الخاصة الظاهرية (VPN) أرقام 172.18.124.131 و 172.18.124.132 على التوالي. يتم تعلم شبكة x.192.168.4 من خلال نفق 172.18.124.132 لأن إعلانات OSPF الخاصة بالموجه يتم وضعها في جدول توجيه مركز VPN 3030b. ثم يعلن جدول التوجيه عن خروج الشبكة إلى أقران شبكات VPN البعيدة.

هذا هو جدول توجيه مركز VPN 3030B في الظروف العادية.

Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.2.1] - Microsoft Internet Explorer

Address: http://172.18.124.132/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Configuration | Administration | Monitoring

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
172.18.134.0	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
192.168.3.0	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

DISCO SYSTEMS

http://172.18.124.132/monitor/index.html

يسلط المربع الأحمر الضوء على أنه قد تم تعلم شبكة x.192.168.1 من نفق الشبكة الخاصة الظاهرية (VPN).
يسلط المربع الأزرق الضوء على أنه يتم التعرف على الشبكات x.192.168.3 و x.192.168.4 من خلال عملية
OSPF الأساسية.

هذا هو جدول توجيه مركز VPN 3060A في الظروف العادية.

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

الشبكة x.192.168.1 هي الشبكة الوحيدة هنا، ويمكن الوصول إليها من خلال نفق VPN. لا توجد شبكة 192.168.2.0 نظراً لعدم مرور أي عملية (مثل RIP) على هذا المسار. لا يوجد شيء مفقود ما دامت أجهزة الكمبيوتر على شبكة x.192.168.3 لا تشير إلى العبارة الافتراضية الخاصة بها إلى مركز الشبكة الخاصة الظاهرية (VPN). يمكنك دائماً إضافة مسار ثابت إذا اخترت. ومع ذلك، على سبيل المثال، لا يحتاج مركز الشبكة الخاصة الظاهرية (VPN) نفسه إلى الوصول إلى شبكة 192.168.2.0.

استكشاف الأخطاء وإصلاحها

صدع محاكي

هذا خطأ محاكاة في التكوين. إن يزيل أنت المرشح إلى القارن عام، بعد ذلك ال VPN نفق يسقط. وهذا يتسبب أيضاً في إنزال المسار ل 192.168.1.0 الذي تم تعلمه عبر النفق. تحتاج عملية مجموعة إعادة التوجيه السريع (RIP) إلى حوالي ثلاث دقائق لتطهير الطريق. وبالتالي، من المحتمل أن يكون لديك انقطاع لمدة ثلاث دقائق حتى يعرض المسار نفسه للأعلى.

بمجرد انتهاء صلاحية مسار بروتوكول معلومات التوجيه (RIP)، يظهر جدول التوجيه الجديد على الموجهات مشابهًا لهذا:

```
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
```

```
is subnetted, 1 subnets 172.18.0.0/24
```

```
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 ---!

```
       O       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
```

ما الذي يمكن أن يحدث بشكل خاطئ؟

إذا نسيت إضافة تغيير مسافة المسؤول إلى 130، يمكنك عندئذ رؤية هذا الإخراج. لاحظ أن كلا النفقي عبر الشبكة الخاصة الظاهرية (VPN) قيد التشغيل.

ملاحظة: هذا هو إصدار واجهة المستخدم (GUI) غير الرسومية لجدول التوجيه.

Monitor -> 1

Routing Table

Number of Routes: 6

IP Address	Mask	Next Hop	Intf	Protocol	Age	Metric
Default	0	1 2	172.18.124.1	0.0.0.0		0.0.0.0
Local	0	1 2	0.0.0.0	255.255.255.0		172.18.124.0
Local	0	1 1	0.0.0.0	255.255.255.0		192.168.1.0
RIP	10	2 2	172.18.124.132	255.255.255.0		192.168.2.0
RIP	2	2 2	172.18.124.131	255.255.255.0		192.168.3.0
RIP	10	9 2	172.18.124.132	255.255.255.0		192.168.4.0

للوصول إلى شبكة 192.168.3.0، يجب أن يمر المسار عبر 172.18.124.131. ومع ذلك، يوضح جدول التوجيه على RTR-3620:

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

is subnetted, 1 subnets 172.18.0.0/24

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

للعودة إلى شبكة 192.168.1.0، يجب أن يمر المسار عبر الشبكة الأساسية 192.168.4.x.

لا تزال حركة المرور تعمل منذ أن يعمل الاكتشاف التلقائي على إنشاء معلومات اقتران الأمان المناسب (SA) على مركز VPN 3030B. على سبيل المثال:

Routing -> 1

Routing Table

Number of Routes: 6

IP Address	Mask	Next Hop	Intf	Protocol	Age	Metric
Default	0	1 2	172.18.124.1	0.0.0.0		0.0.0.0
Local	0	1 2	0.0.0.0	255.255.255.0		172.18.124.0
Local	0	1 1	0.0.0.0	255.255.255.0		192.168.1.0
RIP	28	2 2	172.18.124.132	255.255.255.0		192.168.2.0
RIP	20	2 2	172.18.124.131	255.255.255.0		192.168.3.0

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

VPN 3000 Concentrator Series Manager Main | Help | Support | Logout

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

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

CISCO SYSTEMS

Sessions Internet

على الرغم من أن جدول التوجيه يقول إن النظير يجب أن يكون 172.18.124.131، فإن SA (تدفق حركة المرور) الفعلي هو من خلال مركز VPN 3030b على 172.18.124.132. يعطي جدول SA الأولوية على جدول المسار. لا يظهر إلا الفحص الدقيق لجدول المسار و جدول SA على مركز VPN 3060A أن حركة المرور لا تتدفق في الاتجاه الصحيح.

معلومات ذات صلة

- [صفحة دعم مركز Cisco VPN 3000 Series](#)
- [صفحة دعم IPSec](#)
- [الدعم الفني - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل اء ان ا ع مچ ي ف ن م دخت س م ل ل م عد و ت م م م دقت ل ة يرش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا