Cisco مجوم ىلإ Cisco VPN 3000 زكرم نيوكت

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
التكوين
الرسم التخطيطي للشبكة
التكوينات
تكوين مركز VPN
التحقق من الصحة
على الموجه
على مركز الشبكة الخاصة الظاهرية (VPN)
استكشاف الأخطاء وإصلاحها
على الموجه
مشكلة - يتعذر بدء النفق
PFS
معلومات ذات صلة

المقدمة

يوضح هذا التكوين النموذجي كيفية توصيل شبكة خاصة خلف موجه يعمل ببرنامج Cisco IOS®Software بشبكة خاصة خلف مركز Cisco VPN 3000. تعرف الأجهزة الموجودة على الشبكات بعضها البعض من خلال العناوين الخاصة بها.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- cisco 2611 مسحاج تخديد مع cisco ios برمجية إطلاق a(1).12.3**ملاحظة:** تأكد من تثبيت موجهات سلسلة 2600 من Cisco باستخدام صورة VPN VPN IPsec التي تدعم ميزة VPN.
- مركز Cisco VPN 3000 مع b 4.0.1

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة

المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

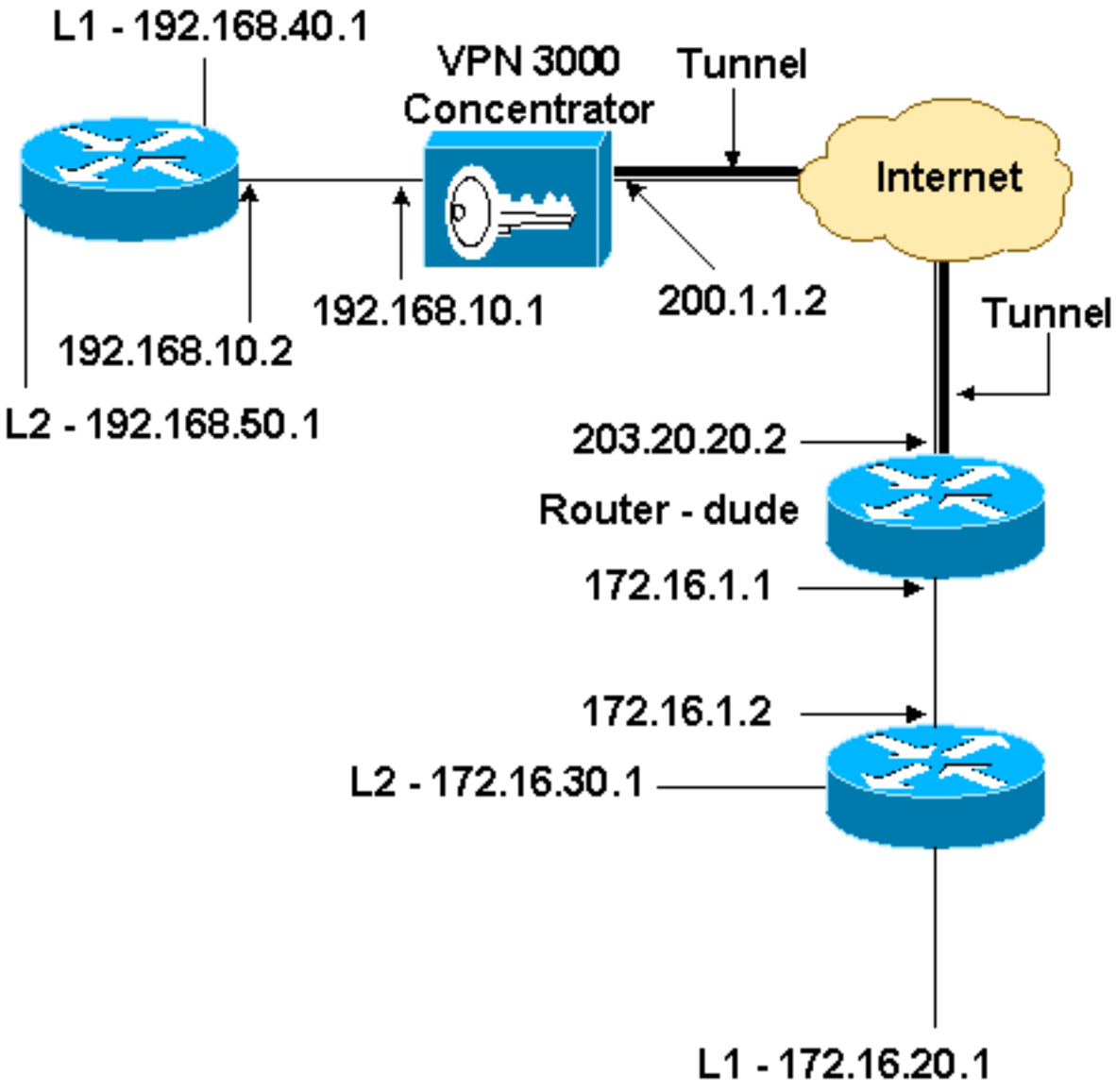
التكوين

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

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للعثور على مزيد من المعلومات حول الأوامر المستخدمة في هذا المستند.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي.



التكوينات

يستخدم هذا المستند هذا التكوين.

تكوين الموجّه

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
IKE policies. crypto isakmp policy 1 ---!!
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 200.1.1.2
IPsec policies. crypto ipsec transform-set to_vpn ---!!
 esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set to_vpn
Traffic to encrypt. match address 101 ---!
!
interface Ethernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 half-duplex
 crypto map to_vpn
!
interface Ethernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask
 255.255.255.0
ip nat inside source route-map nonat pool mypool
 overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
Traffic to encrypt. access-list 101 permit ip ---!!
 172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
 192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
```

```
                                    192.168.50.0 0.0.0.255
          access-list 101 permit ip 172.16.30.0 0.0.0.255
                                    192.168.10.0 0.0.0.255
          access-list 101 permit ip 172.16.30.0 0.0.0.255
                                    192.168.40.0 0.0.0.255
          access-list 101 permit ip 172.16.30.0 0.0.0.255
                                    192.168.50.0 0.0.0.255
Traffic to except from the NAT process. access-list ---!
          110 deny   ip 172.16.1.0 0.0.0.255 192.168.10.0
                                                 0.0.0.255
           access-list 110 deny   ip 172.16.1.0 0.0.0.255
                                    192.168.40.0 0.0.0.255
           access-list 110 deny   ip 172.16.1.0 0.0.0.255
                                    192.168.50.0 0.0.0.255
          access-list 110 deny   ip 172.16.20.0 0.0.0.255
                                    192.168.10.0 0.0.0.255
          access-list 110 deny   ip 172.16.20.0 0.0.0.255
                                    192.168.40.0 0.0.0.255
          access-list 110 deny   ip 172.16.20.0 0.0.0.255
                                    192.168.50.0 0.0.0.255
          access-list 110 deny   ip 172.16.30.0 0.0.0.255
                                    192.168.10.0 0.0.0.255
          access-list 110 deny   ip 172.16.30.0 0.0.0.255
                                    192.168.40.0 0.0.0.255
          access-list 110 deny   ip 172.16.30.0 0.0.0.255
                                    192.168.50.0 0.0.0.255
      access-list 110 permit ip 172.16.1.0 0.0.0.255 any
                                                       !
                                route-map nonat permit 10
                                    match ip address 110
                                                       !
                                                 line con 0
                                                 line aux 0
                                               line vty 0 4
                                                       !
                                                     end
```

تكوين مركز VPN

في هذا الإعداد المعملي، يتم الوصول إلى مركز الشبكة الخاصة الظاهرية (VPN) أولا من خلال منفذ وحدة التحكم ويتم إضافة تكوين أدنى حتى يمكن إجراء التكوين الإضافي من خلال واجهة المستخدم الرسومية (GUI).

أخترت **إدارة>نظام reboot>جدول reboot>يعيد مع مصنع/تقصير تشكيل** أن يضمن أن هناك ما من تشكيل حالي في ال VPN مركز.

يظهر مركز VPN في التكوين السريع، ويتم تكوين هذه العناصر بعد إعادة التمهيد:

- الوقت/التاريخ
- الواجهات/الأقنعة في **التكوين > الواجهات** (عام=24/200.1.1.2، خاص=24/192.168.10.1)
- البوابة الافتراضية في **التكوين>النظام** (200.1.1.1) **ip routing > default_gateway**

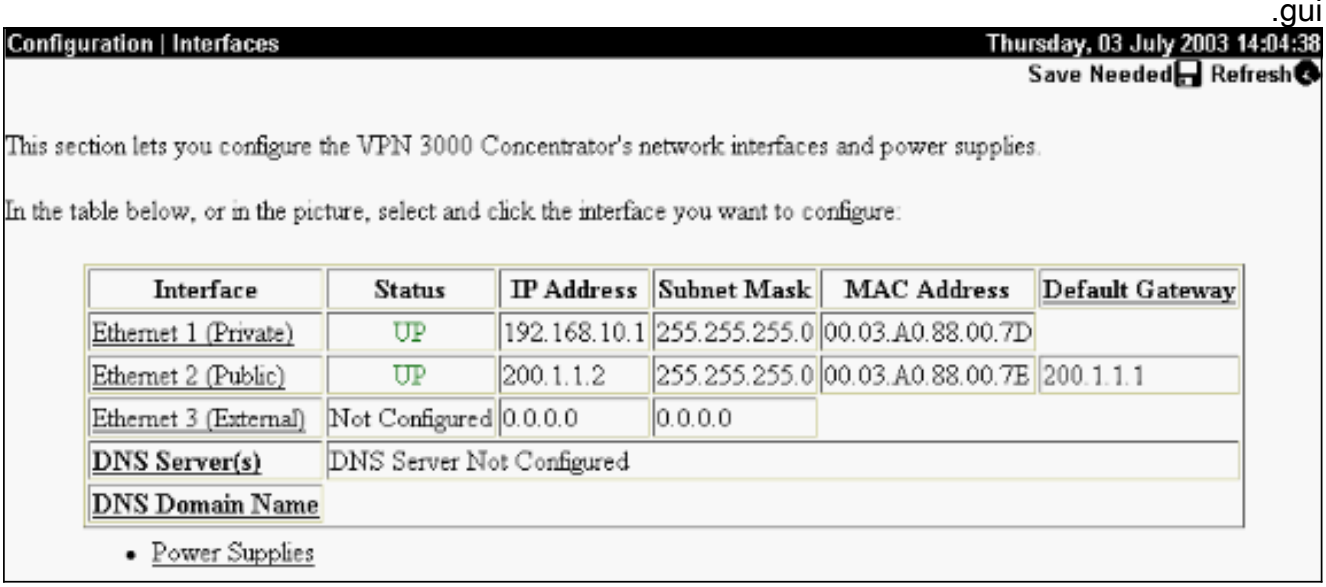
عند هذه النقطة، يمكن الوصول إلى مركز الشبكة الخاصة الظاهرية (VPN) من خلال HTML من الشبكة الداخلية.

ملاحظة: نظرا لأن مركز الشبكة الخاصة الظاهرية (VPN) تتم إدارته من الخارج، فيجب عليك أيضا تحديد:

- **تكوين > واجهات > 2-عام > تحديد عامل تصفية 1 > IP. خاص (افتراضي)**.
- **إدارة > حقوق الوصول >قائمة التحكم في الوصول > إضافة مدير محطة عمل** لإضافة عنوان IP الخاص ب المدير **الخارجي**.

لا يكون هذا ضروريا ما لم تقم بإدارة مركز VPN من *الخارج*.

1. أخترت **تشكيل>قارن** أن يعيد فحصت القارن بعد أن يشكل أنت ال gui.


Configuration | Interfaces — Thursday, 03 July 2003 14:04:38

Save Needed | Refresh

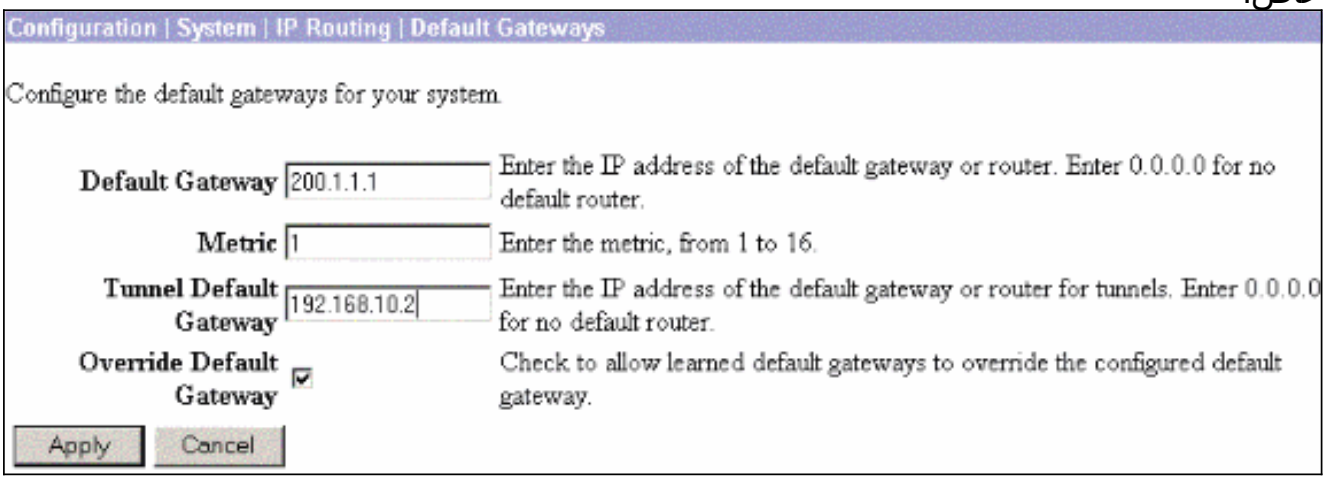
This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.10.1	255.255.255.0	00.03.A0.88.00.7D	
Ethernet 2 (Public)	UP	200.1.1.2	255.255.255.0	00.03.A0.88.00.7E	200.1.1.1
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

- Power Supplies

2. أخترت تشكيل>نظام>ip routing>تقصير مدخل أن يشكل التقصير (إنترنت) مدخل والقصير نفق (داخل) مدخل ل IPsec أن يبلغ الآخر شبكة فرعية في خاص.

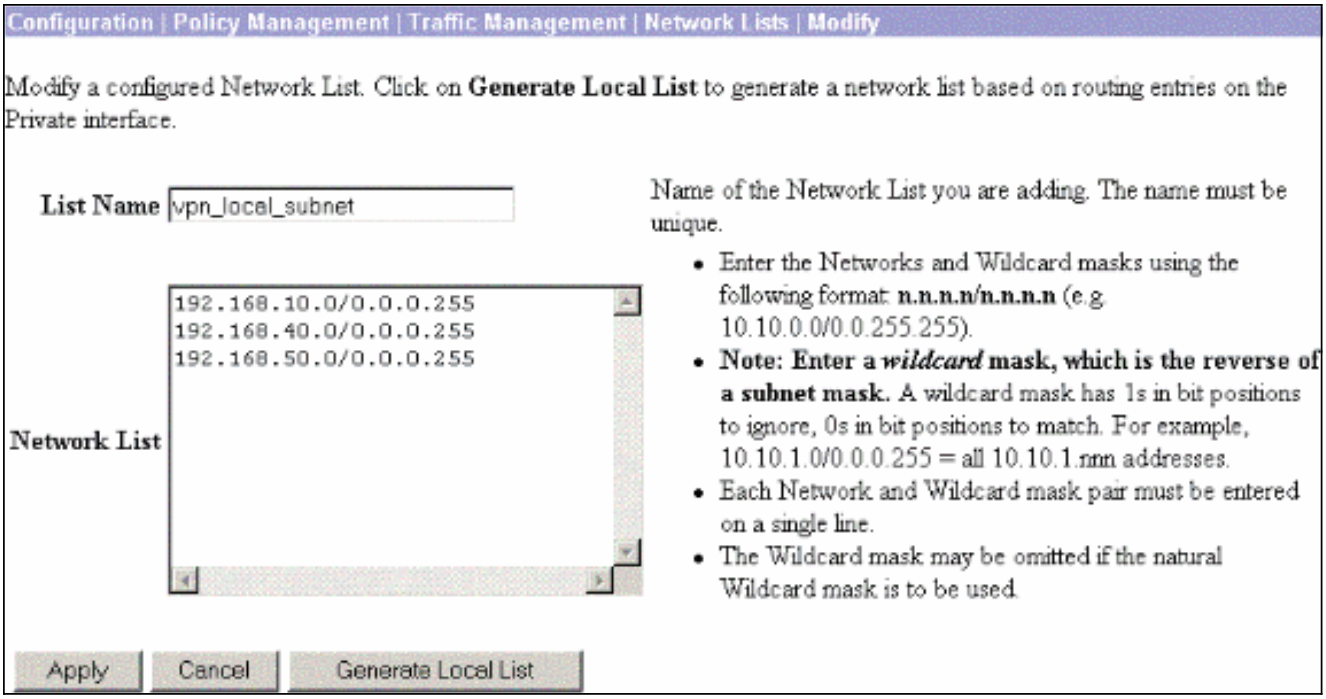

Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

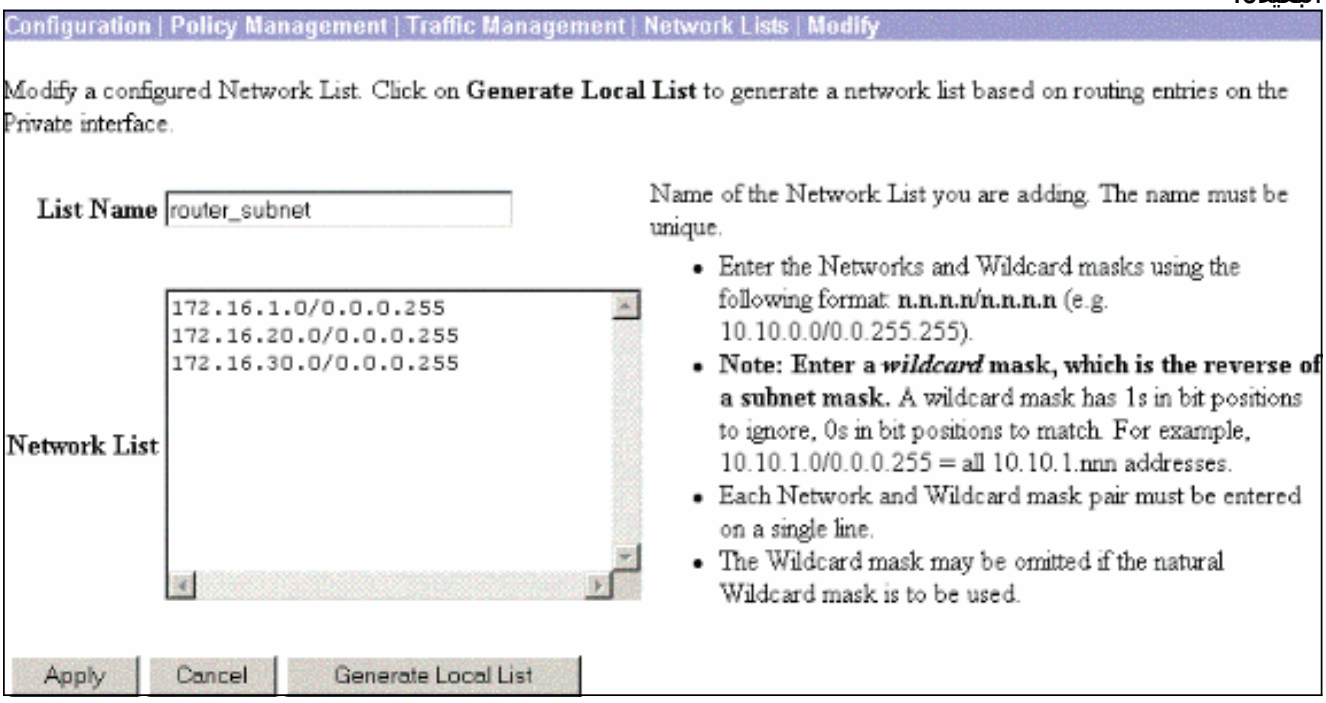
Default Gateway	200.1.1.1	Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.
Metric	1	Enter the metric, from 1 to 16.
Tunnel Default Gateway	192.168.10.2	Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router.
Override Default Gateway	☑	Check to allow learned default gateways to override the configured default gateway.

Apply | Cancel

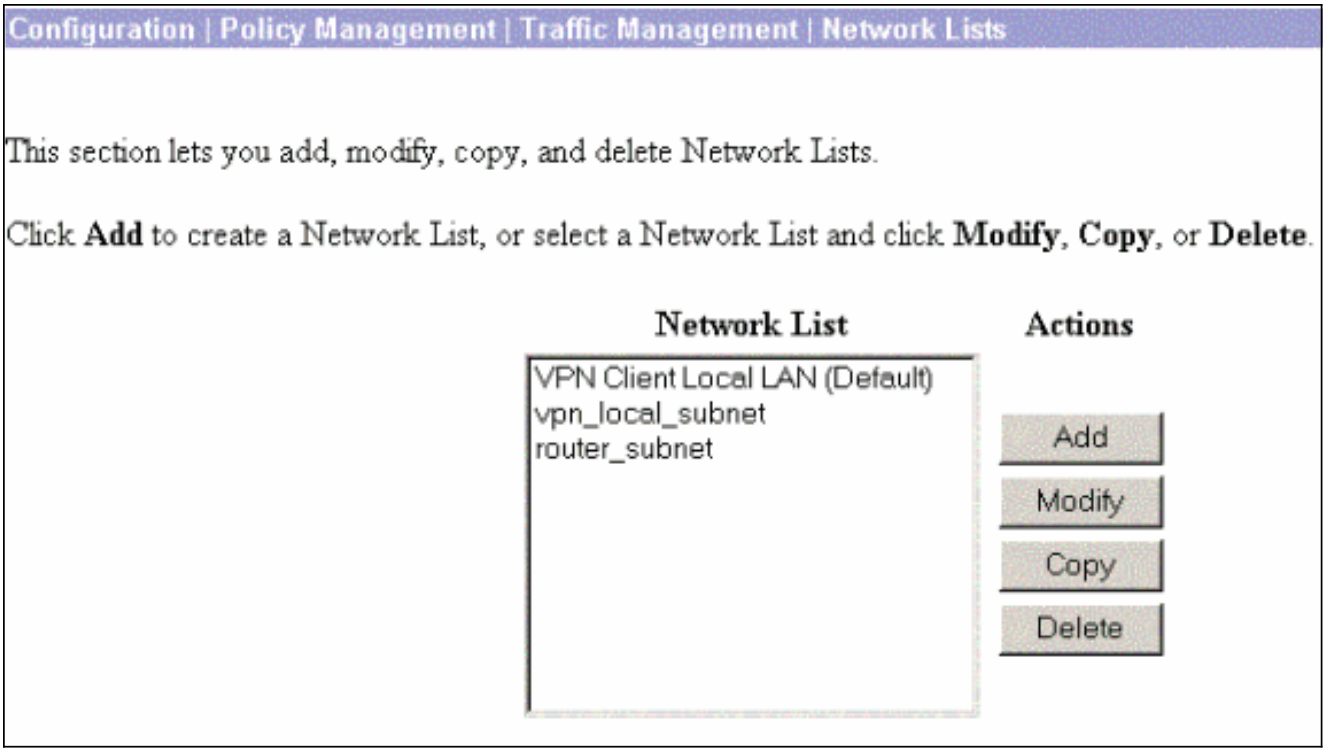
3. أخترت **تشكيل>سياسة إدارة>شبكة قائمة** أن يخلق الشبكة قائمة أن يعين الحركة مرور أن يكون يشفر.هذه هي الشبكات المحلية:



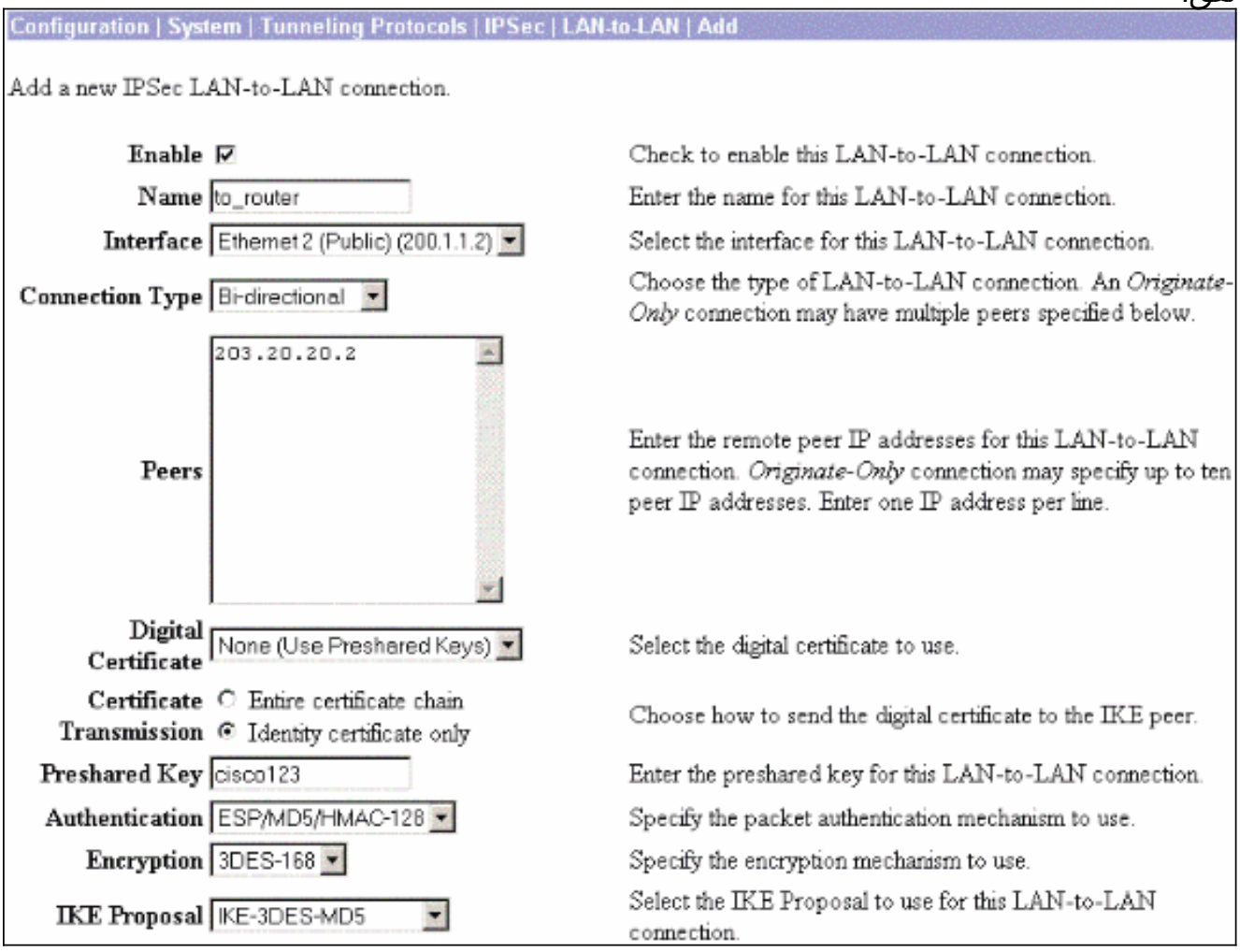
هذه هي الشبكات البعيدة:

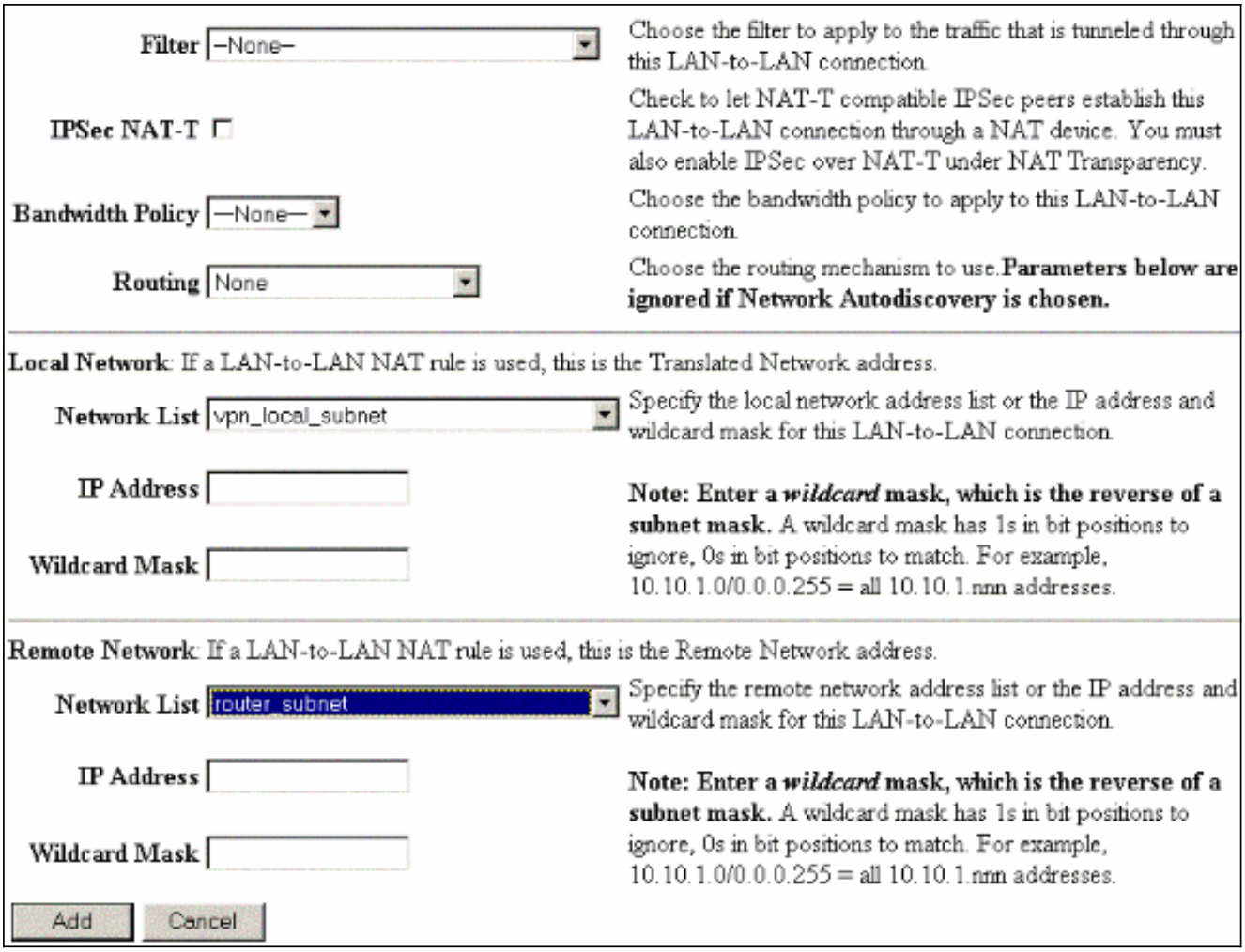


4. عند اكتمالها، هذان هما قائمتا الشبكة:**ملاحظة:** إذا لم يظهر نفق IPsec، فتحقق لمعرفة ما إذا كانت حركة المرور المفيدة تتطابق على كلا الجانبين. يتم تحديد حركة المرور المثيرة للاهتمام بواسطة قائمة الوصول على مربعات Router و PIX. ويتم تعريفها بواسطة قوائم الشبكة في مركزات الشبكة الخاصة الظاهرية (VPN).

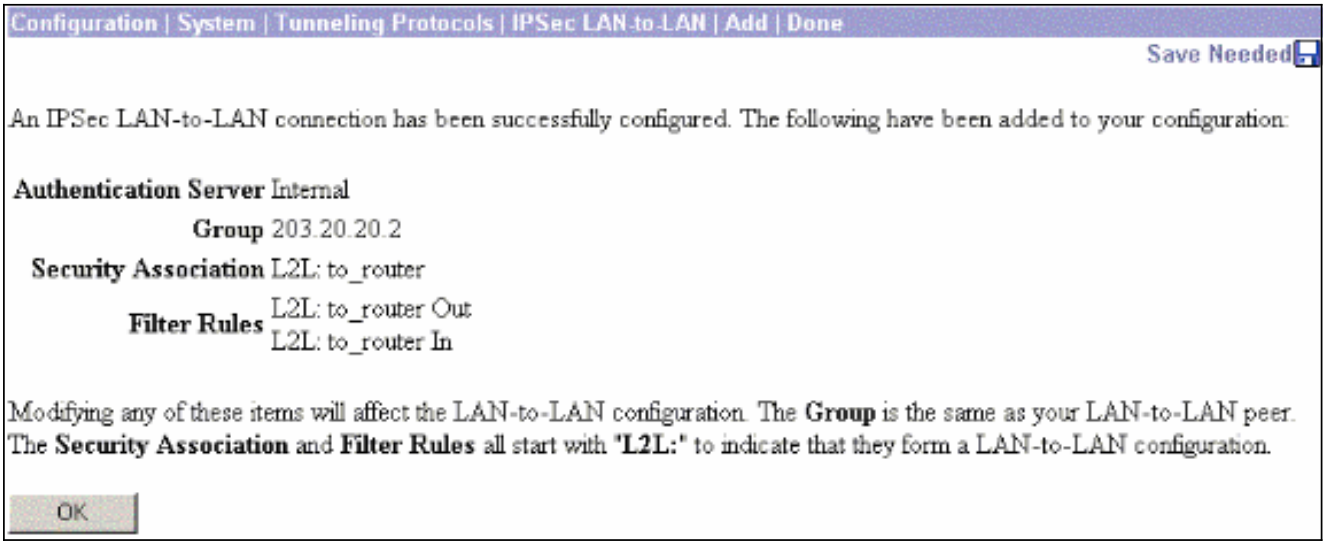


5. أخترت **تشكيل>نظام>tunneling بروتوكول>IPSec lan-to-LAN** وعينت ال LAN-to-LAN نفق.

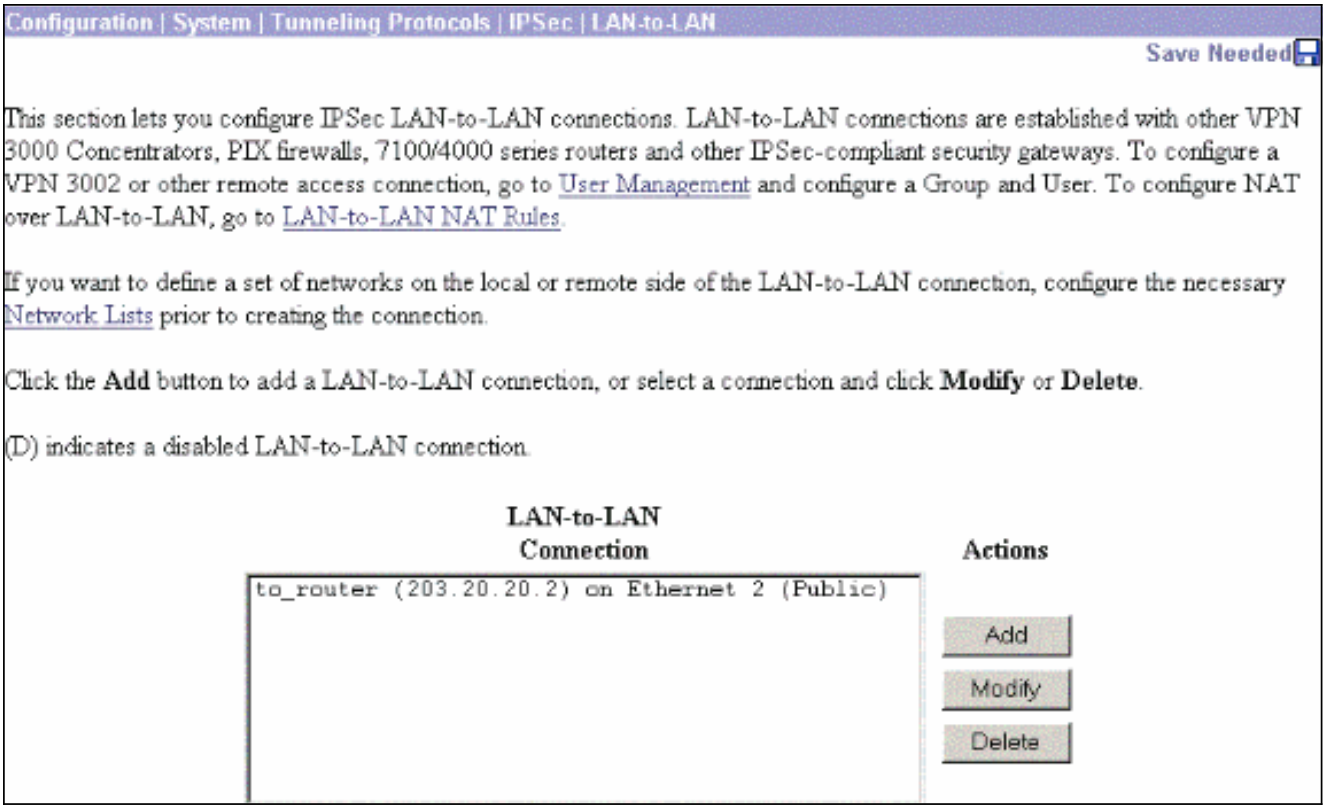




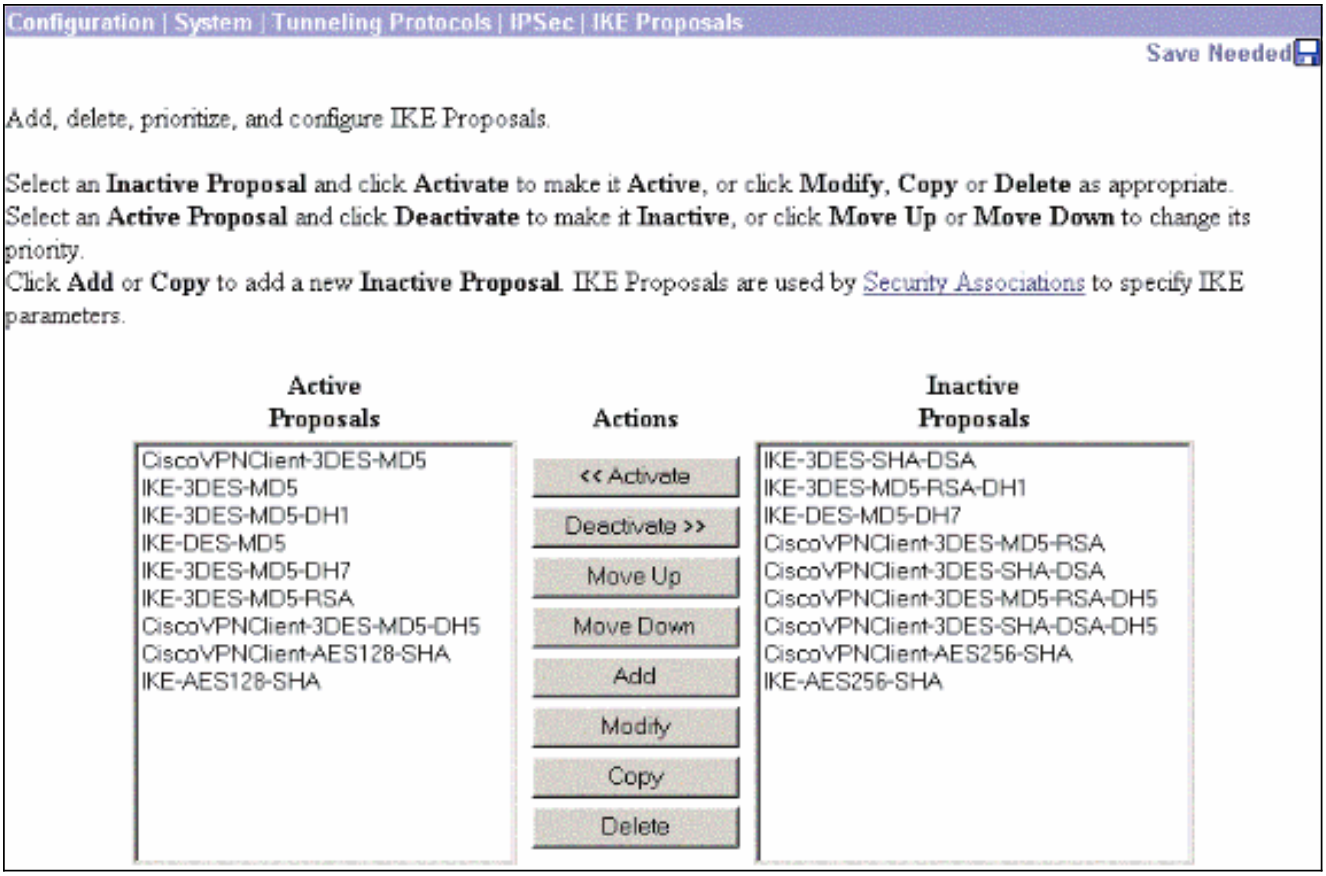
6. بعد النقر فوق **تطبيق**، يتم عرض هذا الإطار مع التكوين الآخر الذي يتم إنشاؤه تلقائيا كنتيجة لتكوين نفق شبكة LAN إلى شبكة LAN.



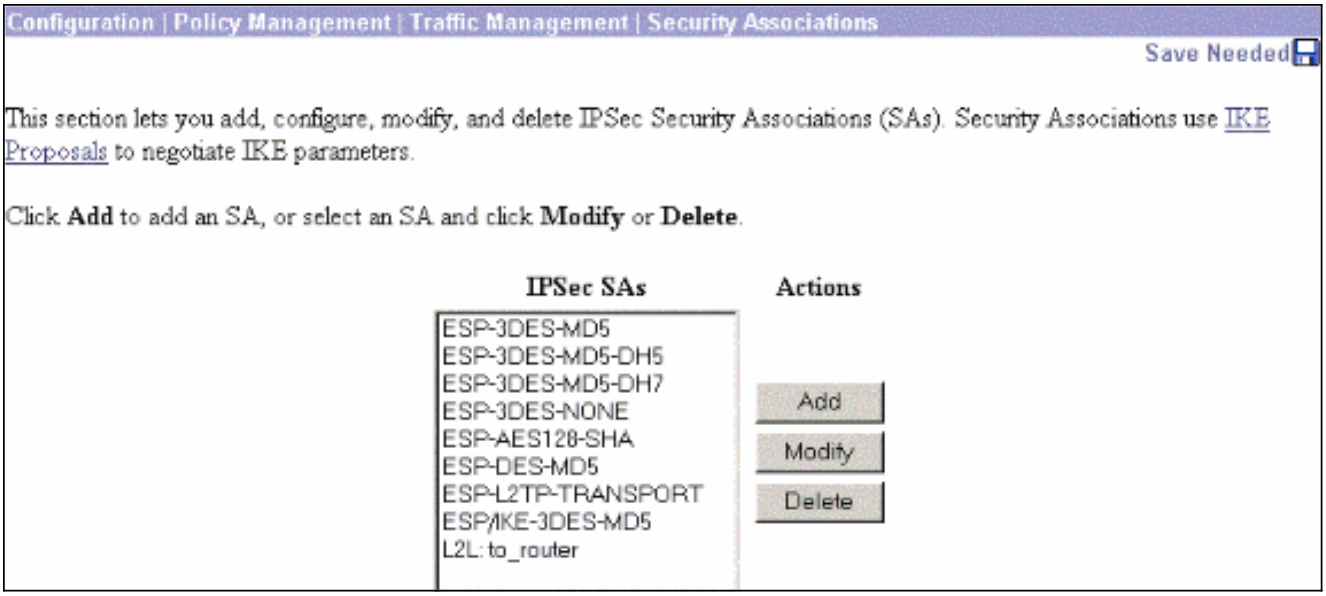
يمكن عرض معلمات IPsec من شبكة LAN إلى شبكة LAN التي تم إنشاؤها مسبقا أو تعديلها في **التكوين > النظام>إنشاء قنوات** البروتوكولات>IPSec من شبكة LAN إلى شبكة LAN.



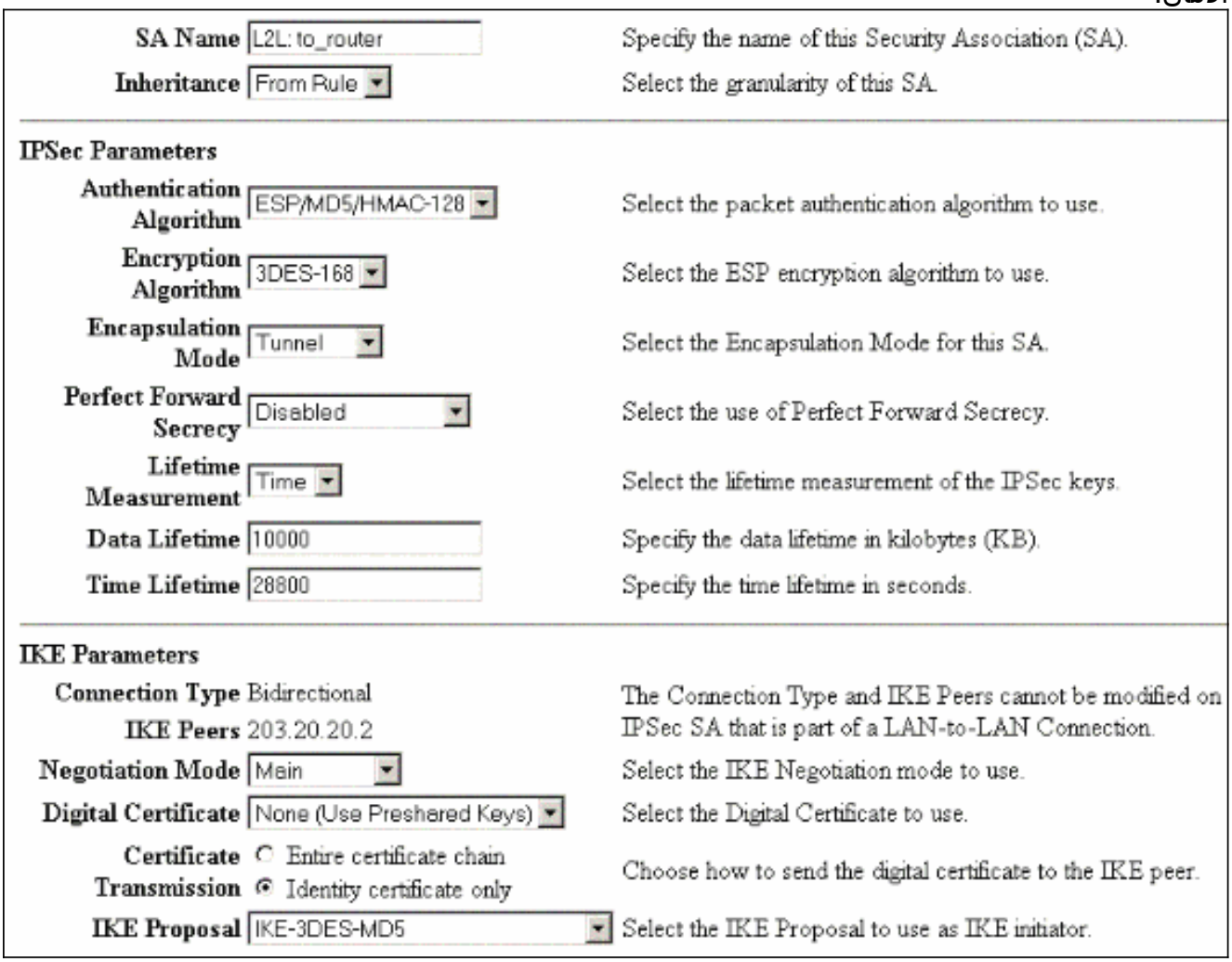
7. أخترت تشكيل>**نظام**>tunneling **بروتوكول**>IKE>**IPSec** مقترح أن يؤكد النشط IKE.



8. أخترت **تشكيل**>**سياسة إدارة**>**حركة مرور إدارة**>**أمن إتحاد** أن يشاهد القائمة ميلان إلى جانب من أمن اقترانات.



9. انقر على اسم اقتران الأمان، ثم انقر على **تعديل** للتحقق من اقترانات الأمان.



التحقق من الصحة

يسرد هذا القسم أوامر **show** المستخدمة في هذا التكوين.

على الموجه

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

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

- **show crypto ipSec**—يعرض الإعدادات المستخدمة من قبل اقترانات الأمان الحالية.
- **show crypto isakmp sa**— يعرض جميع اقترانات أمان تبادل مفتاح الإنترنت الحالية في نظير.
- **show crypto engine connection active**—يعرض إتصالات الجلسة المشفرة النشطة الحالية لجميع محركات التشفير.

يمكنك إستخدام أداة بحث أوامر IOS (للعملاء المسجلين فقط) للاطلاع على مزيد من المعلومات حول أوامر معينة.

على مركز الشبكة الخاصة الظاهرية (VPN)

أخترت تشكيل>**نظام>حدث>صنف**>يعدلأن يركض تسجيل. تتوفر هذه الخيارات:

- آيك
- Ikedbg
- إيكيديكود
- IPSEC
- IPSECDBG
- إبسيديكوده

الخطورة إلى السجل = 1-13

الخطورة بالنسبة لوحدة التحكم = 1-3

حدد **مراقبة > سجل الأحداث** لاسترداد سجل الأحداث.

استكشاف الأخطاء وإصلاحها

على الموجه

أحلت معلومة مهم على Debug أمر قبل أن يحاول أنت أي يضبط أمر.

- **debug crypto engine**—يعرض حركة مرور البيانات التي يتم تشفيرها.
- **debug crypto ipSec**—يعرض مفاوضات IPsec للمرحلة 2.
- **debug crypto isakmp**—يعرض مفاوضات ISAKMP للمرحلة 1.

مشكلة - يتعذر بدء النفق

رسالة خطأ

```
SEV=3 AUTH/5 RPT=1863 10.19.187.229 14:37:45.430 10/26/2007 20932
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
<specified
```

الحل

أتمت هذا الإجراء in order to شكلت العدد المرغوب من عمليات تسجيل الدخول المتزامنة أو ثبتت ال login متزامن

إلى 5 ل هذا SA:

انتقل إلى **التكوين > إدارة المستخدم > مجموعات > تعديل 10.19.187.229 > عام > عمليات تسجيل الدخول المتزامنة** وتغيير عدد عمليات تسجيل الدخول إلى 5.

PFS

في مفاوضات IPsec، تضمن سرية إعادة التوجيه الكاملة (PFS) عدم إرتباط كل مفتاح تشفير جديد بأي مفتاح سابق. إما أن تقوم بتمكين أو تعطيل PFS على كل من نظائر النفق. وإلا، لا يتم إنشاء نفق IPsec الخاص بشبكة LAN إلى شبكة LAN (L2L) في الموجهات.

لتحديد أنه يجب على IPsec طلب PFS عند طلب اقترانات أمان جديدة لإدخال خريطة التشفير هذا، أو أن IPsec يتطلب PFS عندما يستلم طلبات اقترانات أمان جديدة، أستخدم الأمر **set pfs** في وضع تكوين خريطة التشفير. لتحديد أنه لا يجب على IPsec طلب PFS، أستخدم الصيغة **no** من هذا الأمر.

```
[set pfs [group1 | group2
no set pfs
```

بالنسبة لأمر **مجموعة ملفات PFS**:

- *المجموعة 1* — يحدد أن IPsec يجب أن يستخدم مجموعة وحدات Diffie-Hellman الرئيسية ذات 768 بت عند إجراء تبادل Diffie-Hellman جديد.
- *المجموعة 2* — يحدد أن IPsec يجب أن يستخدم مجموعة وحدات Diffie-Hellman الرئيسية ذات 1024 بت عند إجراء تبادل Diffie-Hellman جديد.

بشكل افتراضي، لا يتم طلب ملفات PFS. إذا لم يتم تحديد مجموعة باستخدام هذا الأمر، فسيتم إستخدام *المجموعة 1* كافتراضي.

مثال:

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

راجع مرجع أمر أمان Cisco IOS للحصول على مزيد من المعلومات حول الأمر **set pfs**.

معلومات ذات صلة

- حلول أستكشاف أخطاء الشبكة الخاصة الظاهرية (VPN) عبر بروتوكول IPSec للوصول عن بعد و L2L الأكثر شيوعا
- مركزات Cisco VPN 3000 Series
- أجهزة Cisco VPN 3002 العميلة
- مفاوضة IPSec/بروتوكولات IKE
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).