نفق IPsec من شبكة LAN إلى شبكة LAN مع موجه وCisco VPN 3000 مركز بين مثال تكوين AES

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين نفق IPsec بين مركز Cisco VPN 3000 وموجه Cisco مع معيار التشفير المتقدم (AES) كخوارزمية التشفير.

AES هو منشور جديد عن "معيار معالجة المعلومات الاتحادي" (FIPS) تم إنشاؤه بواسطة المعهد الوطني للمعايير والتكنولوجيا (NIST) لاستخدامه كطريقة تشفير. يحدد هذا المعيار خوارزمية تشفير AES المتماثل التي تستبدل معيار تشفير البيانات (DES) كتحويل للخصوصية لكل من IPsec و IKE (Internet Key Exchange). يحتوي AES على ثلاثة أطوال مفاتيح مختلفة، ومفتاح 128-بت (الافتراضي)، ومفتاح 192-بت، ومفتاح 256-بت. تضيف ميزة AES في Cisco IOS® دعم لمعيار التشفير الجديد AES، مع وضع توصيل كتل التشفير (CBC)، إلى IPsec.

ارجع إلى موقع مركز موارد أمان الكمبيوتر ل NIST للحصول على مزيد من المعلومات حول AES.

ارجع إلى نفق IPsec من شبكة LAN إلى شبكة LAN بين مركز VPN 3000 من Cisco ومثال تكوين جدار حماية PIX للحصول على مزيد من المعلومات حول تكوين نفق من شبكة LAN إلى شبكة LAN بين مركز VPN 3000 وجدار حماية PIX.

ارجع إلى مثال تكوين مركز VPN 3000 ل IPsec Tunnel بين PIX 7.x و VPN 3000 للحصول على مزيد من المعلومات عندما يحتوي PIX على إصدار برنامج 7.1.

المتطلبات الأساسية

المتطلبات

يتطلب هذا المستند فهما أساسيا لبروتوكول IPsec. ارجع إلى مقدمة عن تشفير IPSec لمعرفة المزيد حول IPsec.

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- **متطلبات الموجه** - تم إدخال ميزة AES في البرنامج Cisco IOS Software، الإصدار 12.2(13)T. لتمكين AES، يجب أن يدعم الموجه لديك IPsec ويشغل صورة IOS باستخدام المفاتيح الطويلة "k9" (النظام الفرعي "k9").**ملاحظة:** يتوفر أيضا دعم الأجهزة ل AES على الوحدات النمطية VPN للتعجيل Cisco 2600XM و 2691 و 3725 و 3745 AES. لا تتضمن هذه الميزة أي تأثيرات في التكوين ويتم تحديد وحدة الجهاز النمطية تلقائيا إذا كان كلاهما متوفرا.
- **متطلبات مركز الشبكة الخاصة الظاهرية (VPN)** - تم تقديم دعم البرنامج لميزة AES في الإصدار 3.6. يتم توفير دعم الأجهزة من خلال معالج التشفير الجديد المحسن والقابل للتطوير (SEP-E). لا تتضمن هذه الميزة أي تأثيرات تكوين.**ملاحظة:** في الإصدار 3.6.3 من مركز Cisco VPN 3000، لا تتفاوض الأنفاق إلى AES بسبب معرف تصحيح الأخطاء من Cisco CSCdy88797 (للعملاء المسجلين فقط). تم حل هذا من الإصدار 3.6.4.**ملاحظة:** يستخدم مركز Cisco VPN 3000 إما وحدات SEP أو SEP-E، وليس كلاهما. لا تقم بتثبيت كليهما على نفس الجهاز. إذا قمت بتثبيت وحدة SEP-E على مركز VPN يحتوي بالفعل على وحدة SEP، فإن مركز VPN يعجز وحدة SEP ويستخدم وحدة SEP فقط.

المكونات المستخدمة

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

- cisco 3600 sery مسحاج تخديد مع cisco ios برمجية إطلاق 12.3(5)
- مركز Cisco VPN 3060 مع برنامج الإصدار 4.0.3

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

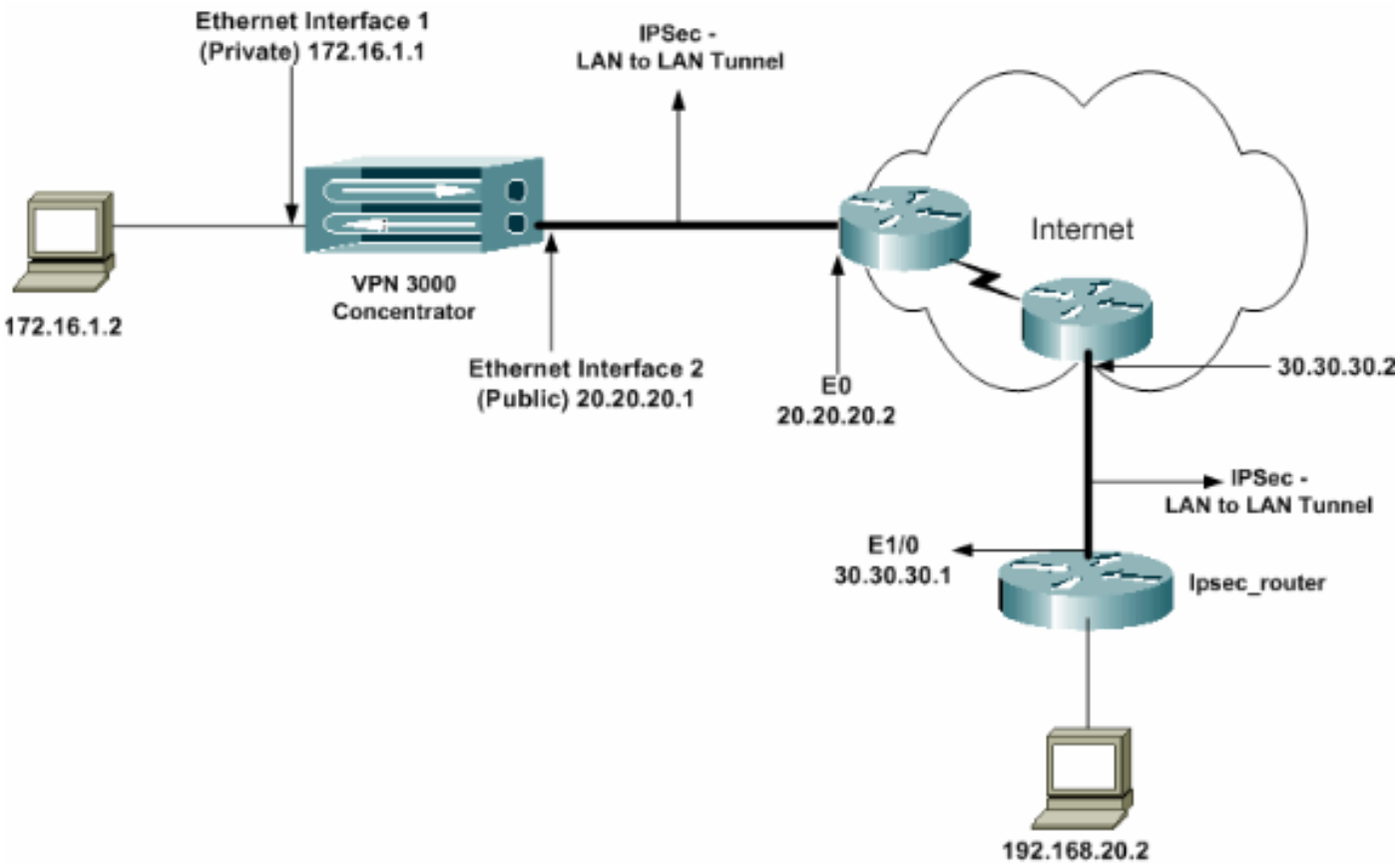
التكوين

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

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

يستخدم هذا المستند التكوينات التالية:

- موجه IPsec
- مركز VPN

تكوين IPSec_Router

```
version 12.3
service timestamps debug uptime
service timestamps log datetime msec
no service password-encryption
!
hostname ipsec_router
!
memory-size iomem 10
no aaa new-model
ip subnet-zero
!
Configuration for IKE policies. crypto isakmp ---!
policy 1
Enables the IKE policy configuration (config- ---!
isakmp) command mode, !--- where you can specify the
parameters to be used during !--- an IKE negotiation.
encryption aes 256
Specifies the encryption algorithm as AES with a ---!
256 !--- bit key within an IKE policy. authentication
pre-share
group 2
crypto isakmp key cisco123 address 20.20.20.1
Specifies the preshared key "cisco123" which !--- ---!
```

```
! .should be identical at both peers
Configuration for IPsec policies. crypto ipsec ---!
security-association lifetime seconds 28800
Specifies the lifetime of the IPsec security ---!
association (SA). ! crypto ipsec transform-set vpn esp-
aes 256 esp-md5-hmac
Enables the crypto transform configuration mode, ---!
where you can !--- specify the transform sets to be used
during an IPsec negotiation. ! crypto map vpn 10 ipsec-
isakmp
Indicates that IKE is used to establish the IPsec ---!
SA for protecting !--- the traffic specified by this
crypto map entry. set peer 20.20.20.1
Sets the IP address of the remote end (VPN ---!
Concentrator). set transform-set vpn
Configures IPsec to use the transform-set "vpn" ---!
defined earlier. ! !--- Specifies the traffic to be
encrypted. match address 110
!
interface Ethernet1/0
ip address 30.30.30.1 255.255.255.0
ip nat outside
half-duplex
crypto map vpn
Configures the interface to use the crypto map ---!
! ."vpn" for IPsec
interface FastEthernet2/0
ip address 192.168.20.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
ip nat pool mypool 30.30.30.3 30.30.30.3 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 30.30.30.2
!
access-list 110 permit ip 192.168.20.0 0.0.0.255
172.16.0.0 0.0.255.255
This crypto ACL-permit identifies the matching ---!
traffic !--- flows to be protected via encryption. !---
Specifies the traffic not to be encrypted. access-list
120 deny ip 192.168.20.0 0.0.0.255 172.16.0.0
0.0.255.255
This crypto ACL-deny identifies the matching ---!
! .traffic flows not to be encrypted
access-list 120 permit ip 192.168.20.0 0.0.0.255 any
The access control list (ACL) used in the NAT ---!
configuration exempts !--- the LAN-to-LAN traffic from
the NAT process, !--- but allows all traffic going to
! .the Internet to be translated
route-map nonat permit 10
The traffic flows not encrypted from the !--- peer ---!
network are allowed. match ip address 120
!
line con 0
line aux 0
line vty 0 4
login
!
```

```
end
```

ملاحظة: على الرغم من أن صياغة قائمة التحكم في الوصول (ACL) لم تتغير، إلا أن المعاني مختلفة قليلا لقوائم التحكم في الوصول (ACL) المشفرة. في قوائم التحكم في الوصول (ACL) المشفرة، يحدد **السماح** أنه يجب تشفير الحزم المطابقة، بينما **يحدد الرفض** أن الحزم المطابقة لا تحتاج إلى التشفير.

تكوين مركز VPN

لا يتم برمجة مركزات VPN مسبقا باستخدام عناوين IP في إعدادات المصنع الخاصة بها. أنت يضطر استعملت الوحدة طرفية للتحكم ميناء أن يشكل التشكيل أولي أي يكون baser أمر خط قارن (CLI). ارجع إلى تكوين مركزات VPN من خلال وحدة التحكم للحصول على معلومات حول كيفية التكوين من خلال وحدة التحكم.

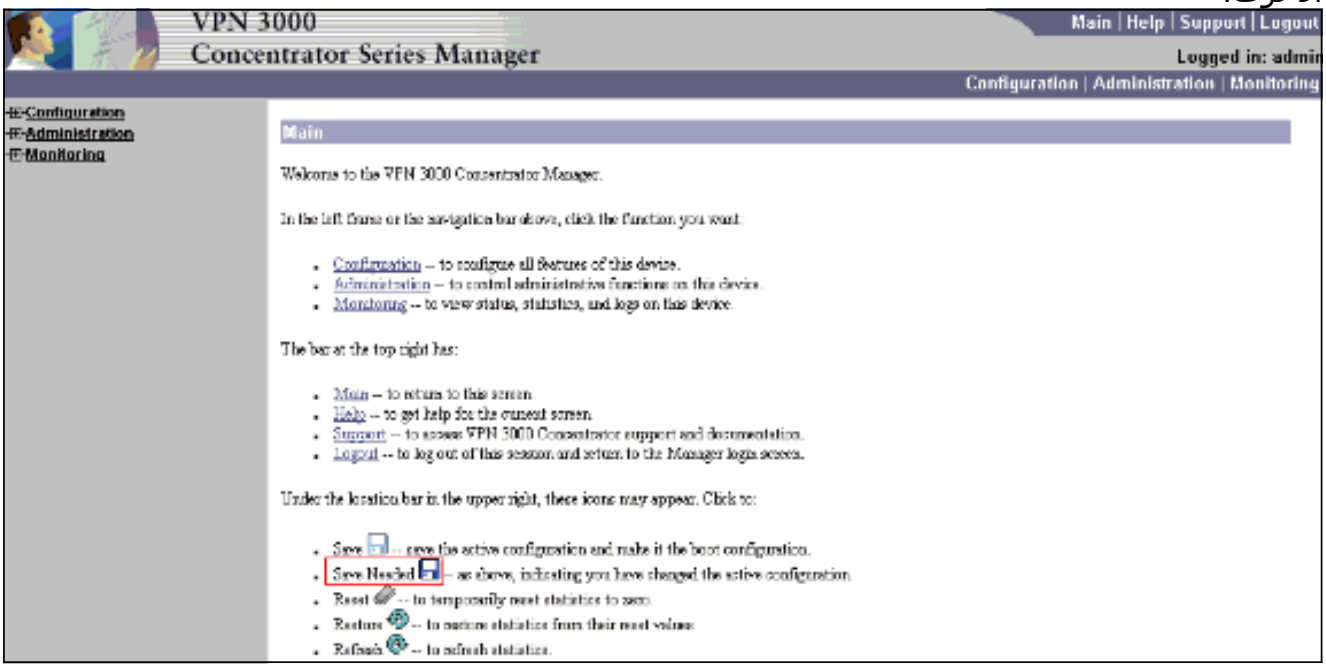
بعد تكوين عنوان IP على واجهة إيثرنت 1 (الخاصة)، يمكن تكوين الباقي إما باستخدام CLI أو من خلال واجهة المستعرض. تدعم واجهة المستعرض كلا من HTTP و HTTP عبر طبقة مأخذ التوصيل الآمنة (SSL).

يتم تكوين هذه المعلمات من خلال وحدة التحكم:

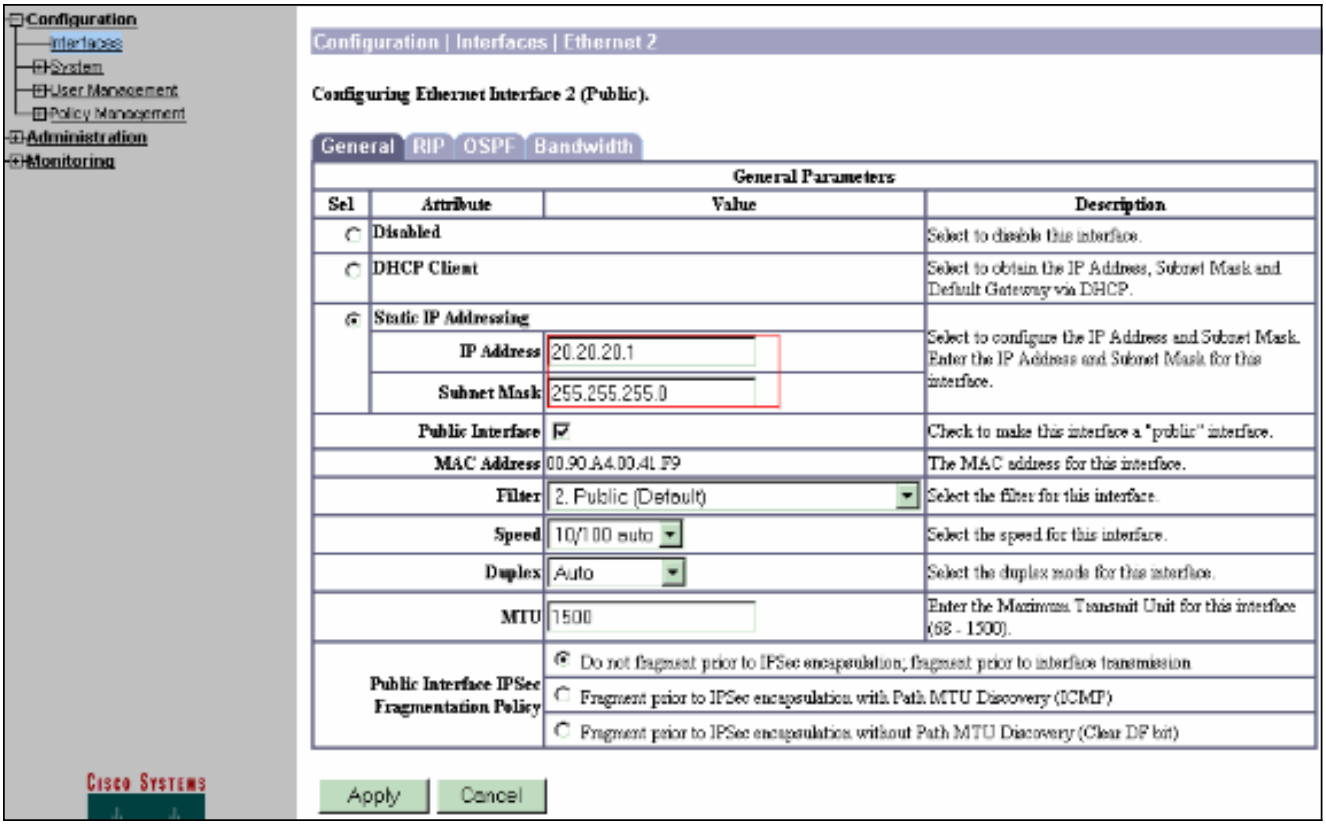
- **الوقت/التاريخ** - الوقت والتاريخ الصحيحان مهمان للغاية. فهي تساعد على ضمان دقة إدخالات التسجيل والمحاسبة، وأن النظام يمكنه إنشاء شهادة أمان صالحة.
- **واجهة Ethernet 1 (الخاصة)** - عنوان IP وقناع (من مخطط الشبكة 24/172.16.1.1).

عند هذه النقطة، يمكن الوصول إلى مركز الشبكة الخاصة الظاهرية (VPN) من خلال متصفح HTML من الشبكة الداخلية. أحلت لمعلومة على يشكل ال VPN مركز في CLI أسلوب، تشكيل سريع يستعمل CLI.

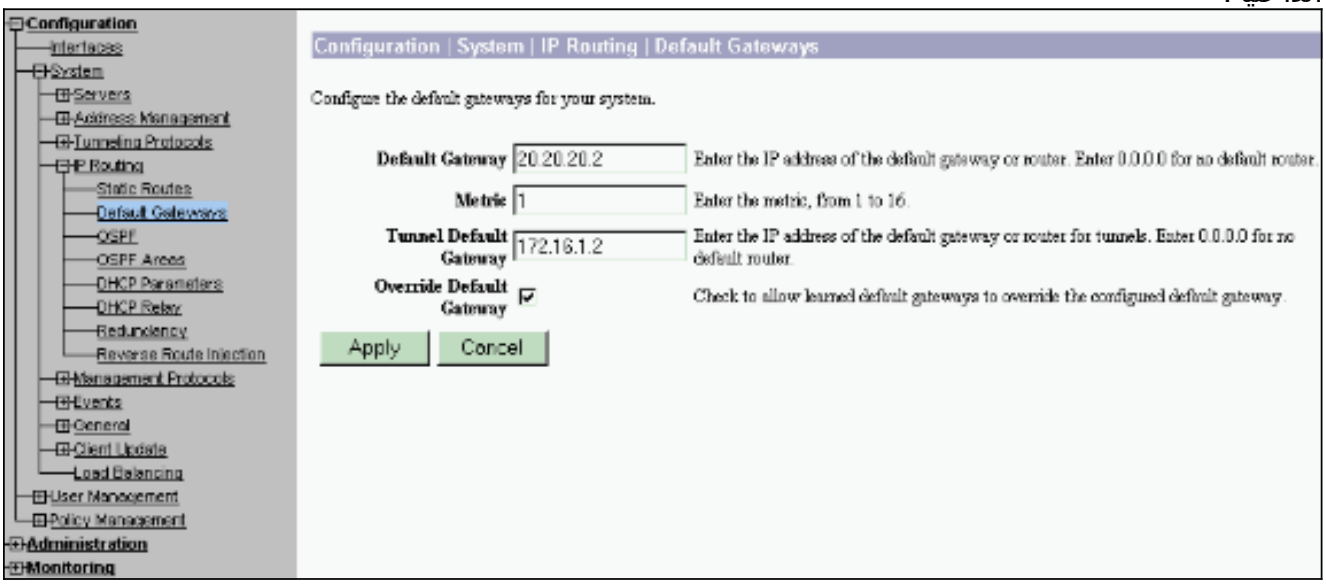
1. اكتب عنوان IP الخاص بالواجهة الخاصة من مستعرض الويب لتمكين واجهة واجهة المستخدم الرسومية (GUI).انقر على أيقونة **حفظ ما يلزم** لحفظ التغييرات في الذاكرة. اسم المستخدم وكلمة المرور الافتراضيان في المصنع هما "admin" وهو أمر حساس لحالة الأحرف.



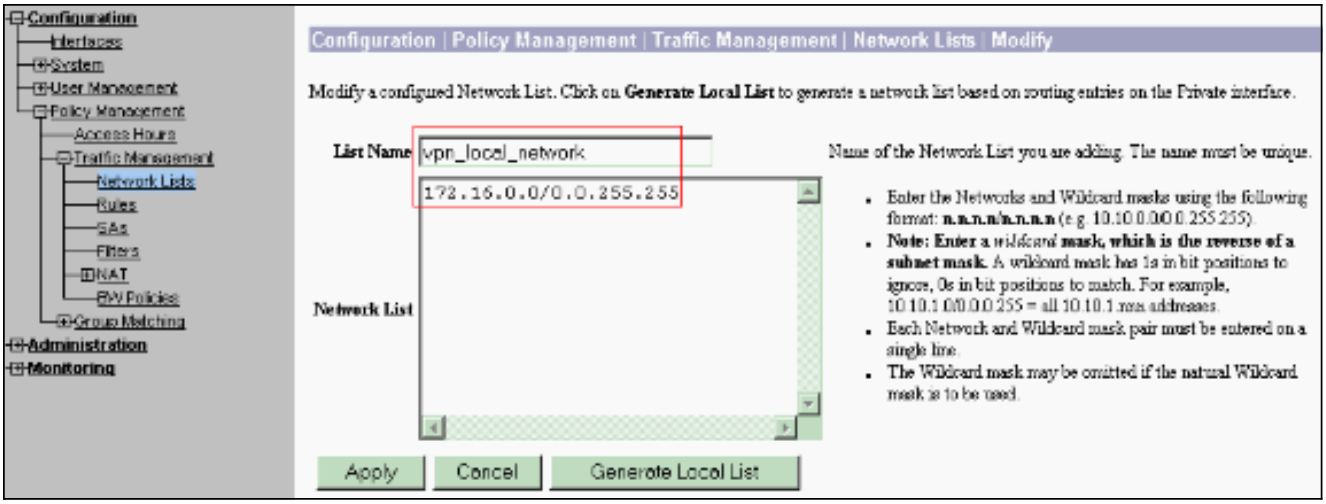
2. بعد إضافة واجهة المستخدم الرسومية، حدد **التكوين>الواجهات > إيثرنت 2 (عام)** لتكوين واجهة إيثرنت 2.



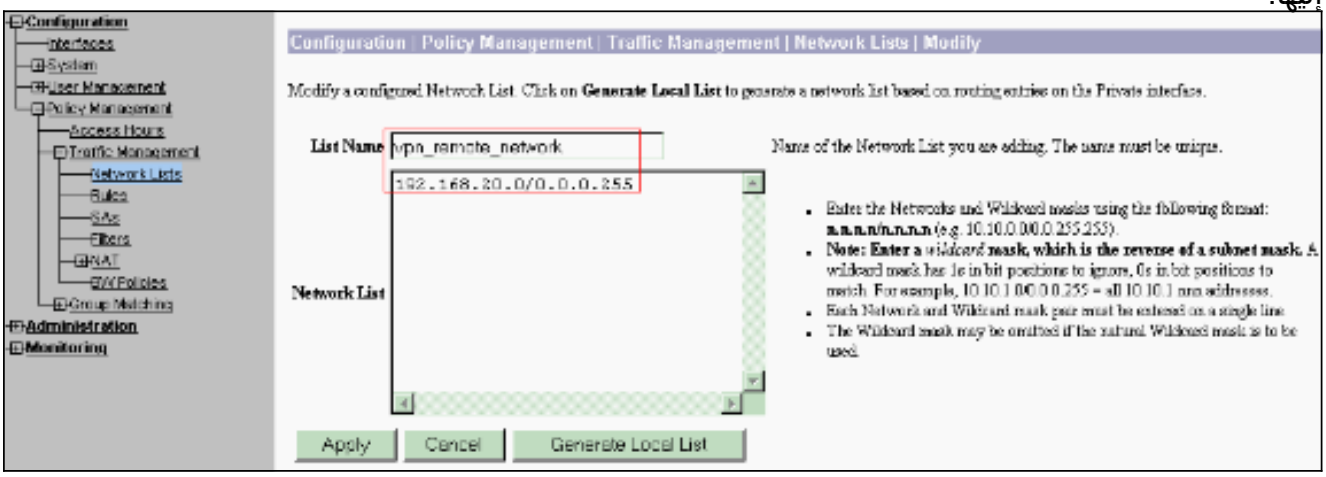
3. حدد **تكوين>نظام>توجيه IP>البوابات الافتراضية** تكوين البوابة الافتراضية (الإنترنت) وبوابة النفق الافتراضية (الداخلية) ل IPsec للوصول إلى الشبكات الفرعية الأخرى في الشبكة الخاصة.في هذا السيناريو، هناك شبكة فرعية واحدة فقط متوفرة على الشبكة الداخلية.



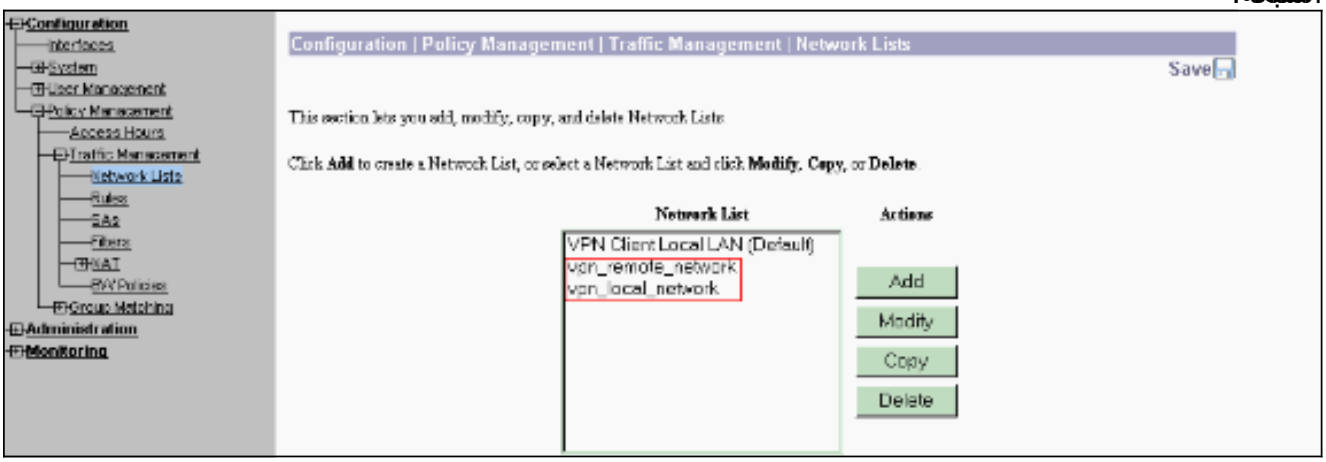
4. حدد تكوين > **إدارة السياسة>إدارة حركة مرور البيانات > قوائم الشبكة>**إضافة لإنشاء قوائم الشبكة التي تحدد حركة المرور التي سيتم تشفيرها.يمكن الوصول إلى الشبكات المذكورة في القائمة إلى الشبكة البعيدة.
الشبكات الموضحة في القائمة أدناه هي شبكات محلية. يمكنك أيضا إنشاء قائمة الشبكة المحلية تلقائيا من خلال RIP عند النقر فوق **إنشاء قائمة محلية**.



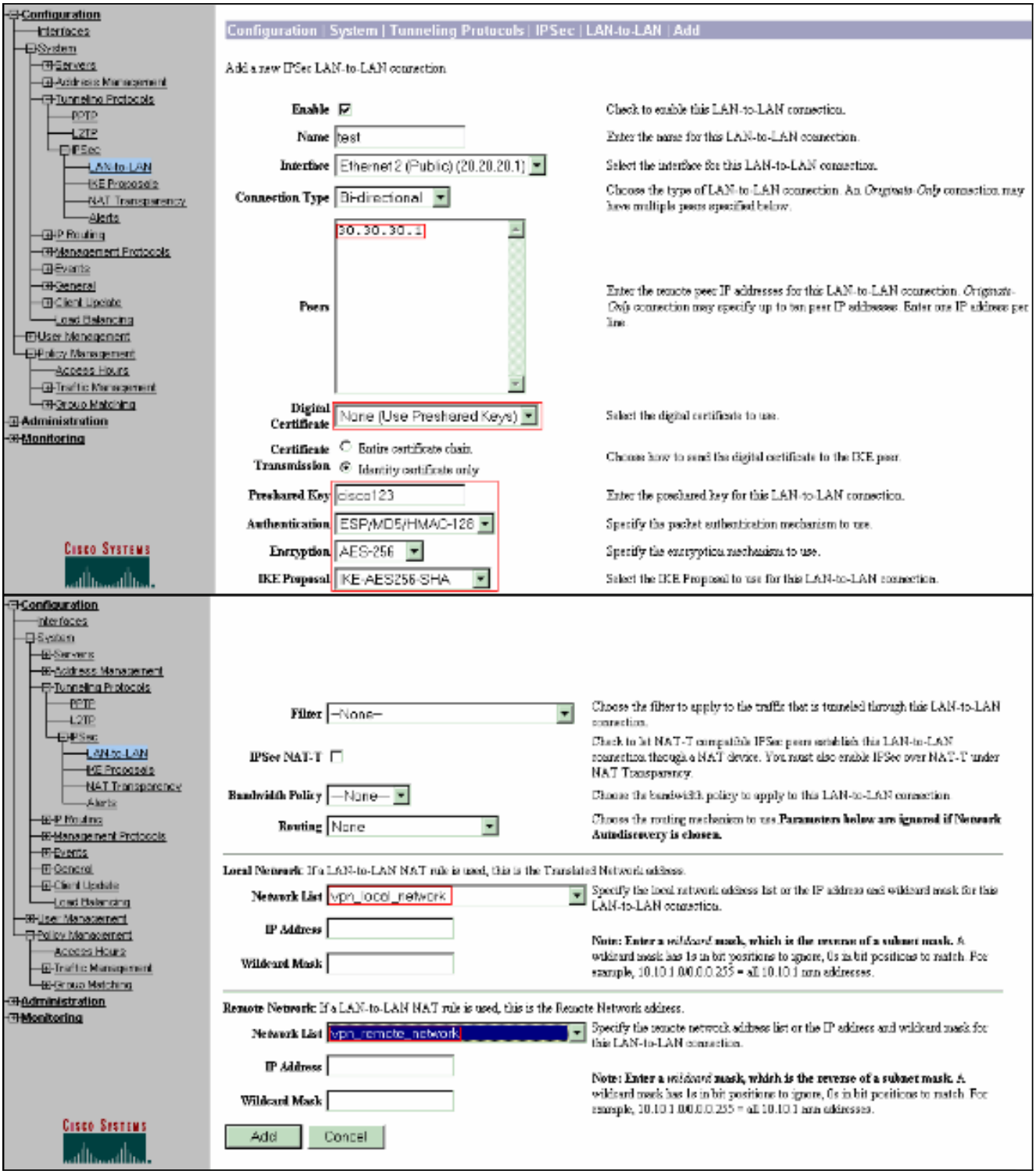
5. الشبكات الموجودة في هذه القائمة هي شبكات بعيدة وتحتاج إلى تكوينها يدويا. للقيام بهذا الإجراء، أدخل الشبكة/حرف البدل لكل شبكة فرعية يمكن الوصول إليها.



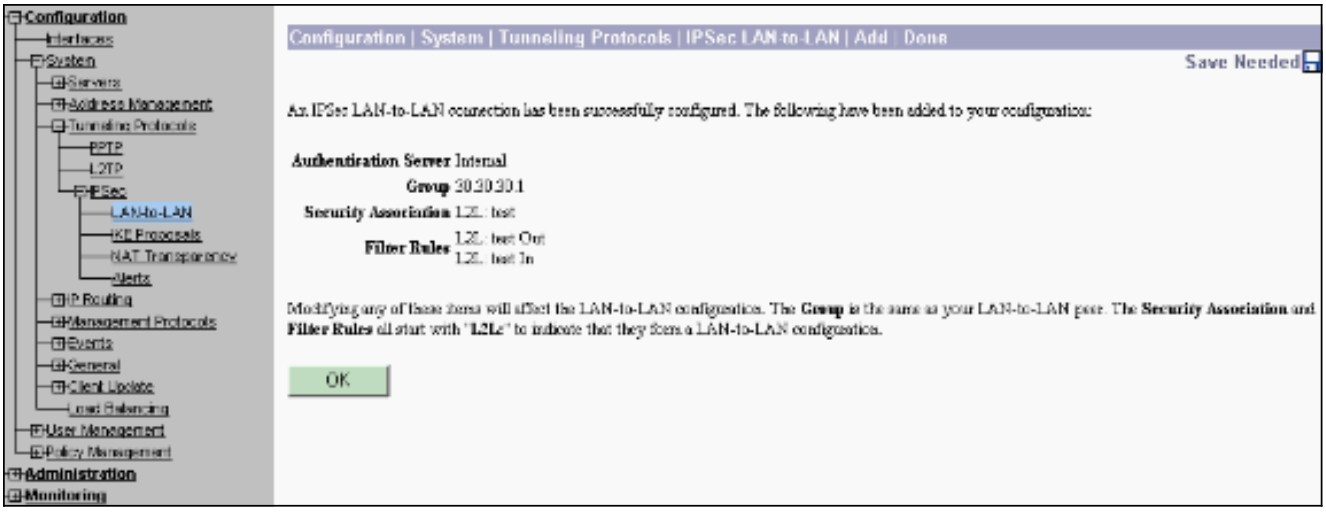
عند اكتمالها، هذان هما قائمتا الشبكة:



6. حدد تكوين > **نظام** > **بروتوكولات إنشاء قنوات** > **IPSec LAN إلى شبكة LAN** > إضافة وتعريف نفق شبكة LAN إلى شبكة LAN.هذه النافذة لها ثلاثة أقسام. القسم العلوي خاص بمعلومات الشبكة والقسمين الأسفل مخصص لقوائم الشبكة المحلية والبعيدة. في قسم معلومات الشبكة، حدد تشفير AES ونوع المصادقة ومقترح IKE واكتب المفتاح المشترك مسبقا. في الأقسام السفلى، أشر إلى قوائم الشبكة التي قمت بإنشائها بالفعل، على كل من القوائم المحلية والقوائم البعيدة على التوالي.

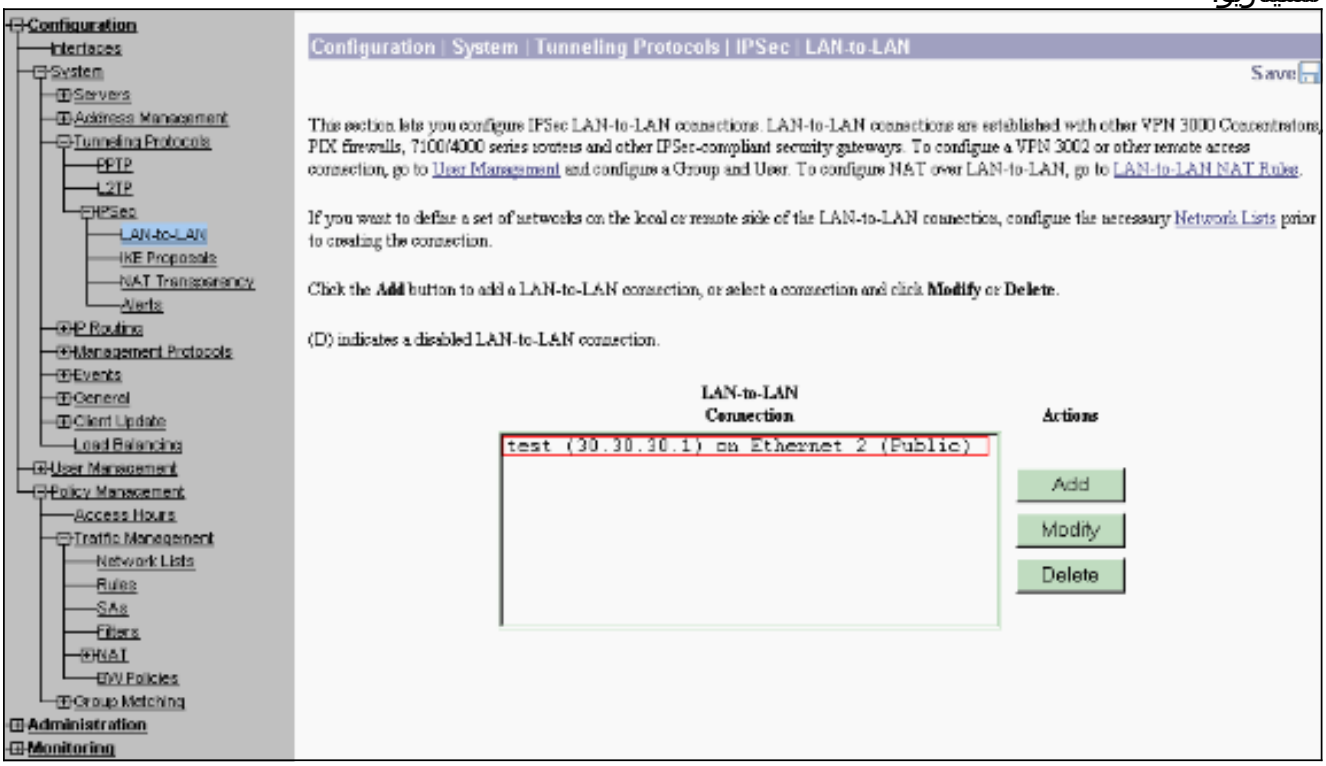


7. بعد النقر فوق **إضافة**، إذا كان إتصالك صحيحا، يتم تقديمك مع نافذة IPSec LAN-to-LAN-Add-Done.يقدم هذا نافذة خلاصة من النفق تشكيل معلومة. كما أنه يقوم بتكوين اسم المجموعة واسم SA واسم عامل التصفية تلقائيا. يمكنك تحرير أية معلمات في هذا الجدول.

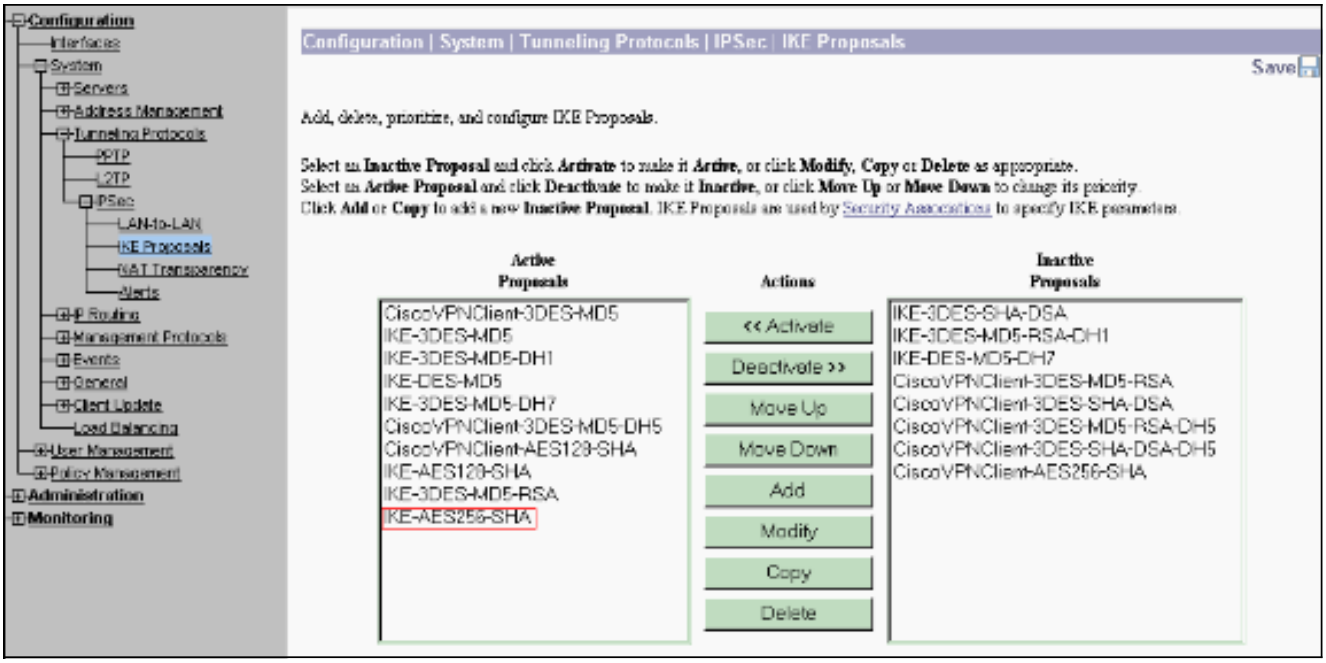


عند هذه النقطة، تم إعداد نفق IPsec LAN إلى LAN ويمكنك بدء العمل. إذا، لسبب ما، لم يعمل النفق، يمكنك التحقق من التكوينات الخاطئة.

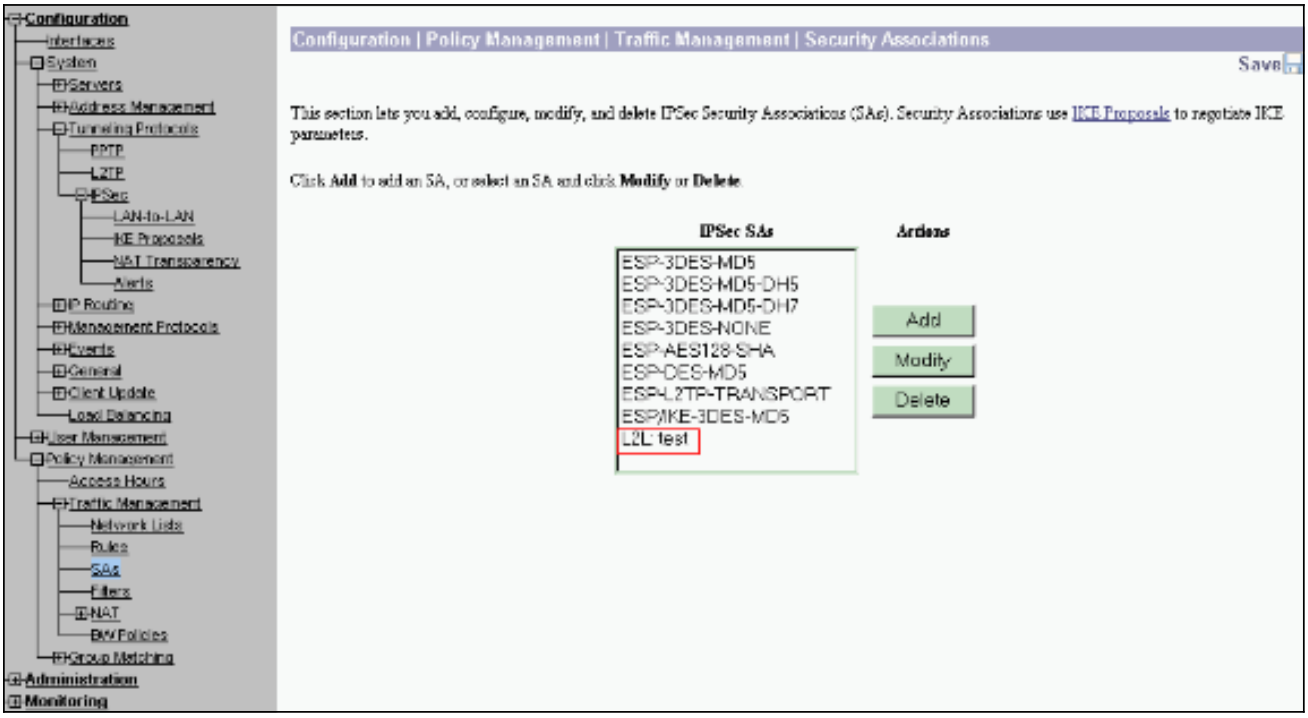
8. يمكنك عرض معلمات IPsec التي تم إنشاؤها مسبقا من شبكة LAN إلى شبكة LAN أو تعديلها عند تحديد **التكوين > النظام > بروتوكولات الاتصال النفقي>IPSec من شبكة LAN إلى شبكة LAN**.يوضح هذا الرسم "test" كاسم النفق والواجهة العامة للطرف البعيد هو 30.30.30.1 وفقا للسيناريو.



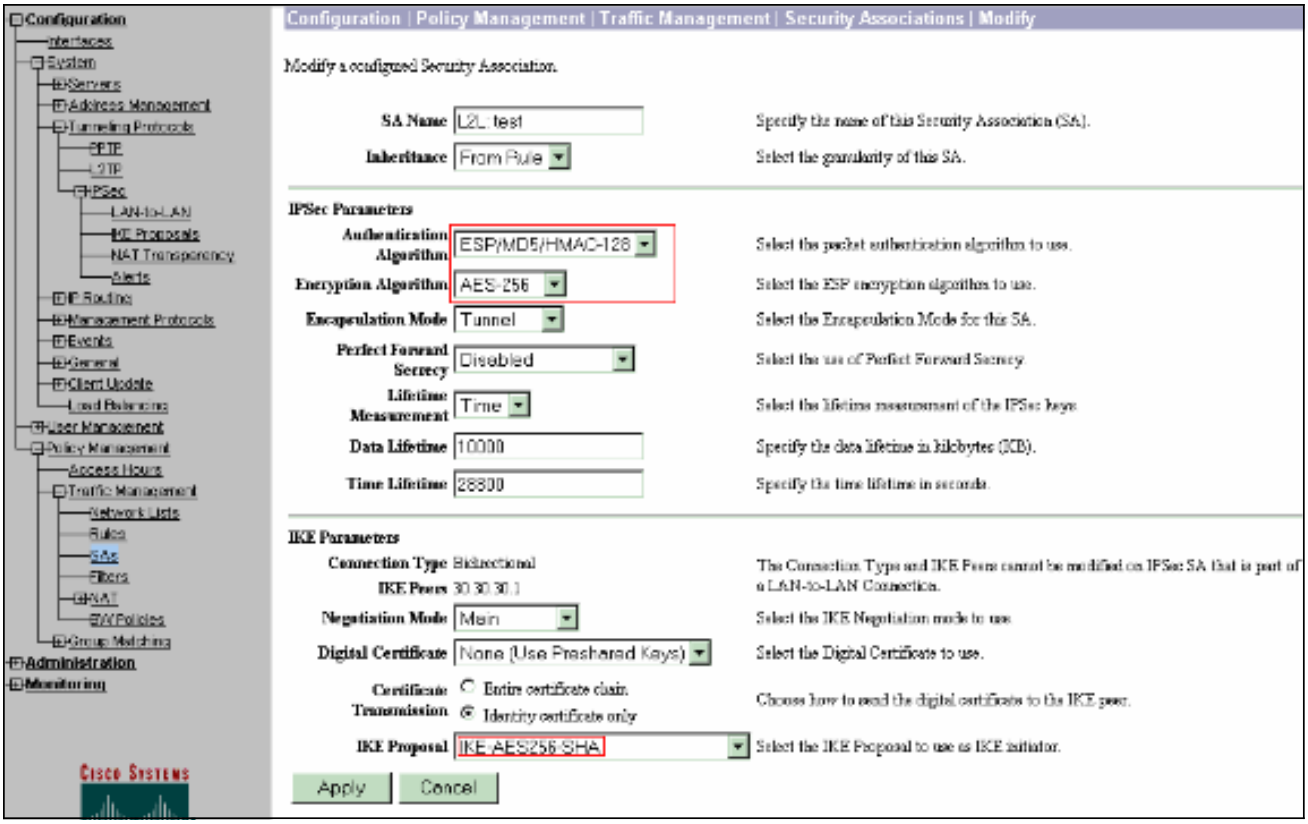
9. وفي بعض الأحيان، قد لا يظهر النفق الخاص بك إذا كان اقتراح IKE الخاص بك مدرجا في قائمة الاقتراحات غير النشطة. حدد تكوين > **نظام > بروتوكولات إنشاء قنوات الاتصال النفقي>IPSec**مقترحات IKE لتكوين مقترح IKE النشط.إذا كان عرض IKE الخاص بك مدرجا في قائمة "الاقتراحات غير النشطة"، يمكنك تمكينه عند تحديد عرض IKE والنقر فوق الزر **تنشيط**. في هذا الرسم، يوجد الاقتراح المحدد "IKE-AES256-SHA" في قائمة الاقتراحات النشطة.



10. حدد **تكوين>إدارة السياسة>إدارة حركة مرور البيانات>اقترانات الأمان** للتحقق من صحة معلمات SA.



11. طقطقت ال sa إسم (في هذه الحالة، **L2L: إختبار**)، وبعد ذلك طقطقت **يعدل** أن يدقق ال SAs.إذا لم تتطابق أي من المعلمات مع تكوين النظير البعيد، يمكن تغييرها هنا.



التحقق من الصحة

التحقق من تكوين الموجه

يوفر هذا القسم معلومات يمكنك إستخدامها 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**.

- **show crypto isakmp sa**— يعرض جميع شبكات IKE الحالية في نظير. تشير QM_IDLE إلى أن SA لا يزال مصدقا عليه مع نظيره ويمكن إستخدامه لمبادلات الوضع السريع اللاحقة. وهي في حالة من الهدوء والسكون.

```
ipsec_router#show crypto isakmp sa

dst             src             state          conn-id  slot

QM_IDLE           1        0    30.30.30.1      20.20.20.1
```

- **show crypto ipSec** — يعرض الإعدادات المستخدمة من قبل موجهات الخدمات (SAs) الحالية. تحقق من عناوين IP النظيرة والشبكات التي يمكن الوصول إليها عند كل من النهايات المحلية والبعيدة ومجموعة التحويل التي يتم إستخدامها. يوجد إثنان من ESP SAs، واحد في كل إتجاه. بما أن مجموعات تحويل AH يتم إستخدامها، فهي فارغة.

```
ipsec_router#show crypto ipsec sa

interface: Ethernet1/0

Crypto map tag: vpn, local addr. 30.30.30.1

:protected vrf

(local ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0

(remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0
```

```
                                        current_peer: 20.20.20.1:500

                                      {,PERMIT, flags={origin_is_acl

                    pkts encaps: 145, #pkts encrypt: 145, #pkts digest 145#

                      pkts decaps: 51, #pkts decrypt: 51, #pkts verify 51#

                               pkts compressed: 0, #pkts decompressed: 0#

                          pkts not compressed: 0, #pkts compr. failed: 0#

                    pkts not decompressed: 0, #pkts decompress failed: 0#

                                      send errors 6, #recv errors 0#

local crypto endpt.: 30.30.30.1, remote crypto endpt.: 20.20.20.1

                                       path mtu 1500, media mtu 1500

                                      current outbound spi: 54FA9805

                                                   :inbound esp sas

                                                (spi: 0x4091292(67703442

                                    , transform: esp-256-aes esp-md5-hmac

                                                { ,in use settings ={Tunnel

                            slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn

                  (sa timing: remaining key lifetime (k/sec): (4471883/28110

                                                     IV size: 16 bytes

                                                replay detection support: Y

                                                    :inbound ah sas

                                                   :inbound pcp sas

                                                  :outbound esp sas

                                                 (spi: 0x54FA9805(1425709061

                                    , transform: esp-256-aes esp-md5-hmac

                                                { ,in use settings ={Tunnel

                            slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn

                  (sa timing: remaining key lifetime (k/sec): (4471883/28110

                                                     IV size: 16 bytes

                                                replay detection support: Y

                                                   :outbound ah sas

                                                  :outbound pcp sas
```

• **show crypto engine connections active**—يعرض إتصالات الجلسة المشفرة النشطة الحالية لجميع محركات التشفير. كل معرف اتصال فريد. يتم عرض عدد الحزم التي يتم تشفيرها وفك تشفيرها في العمودين

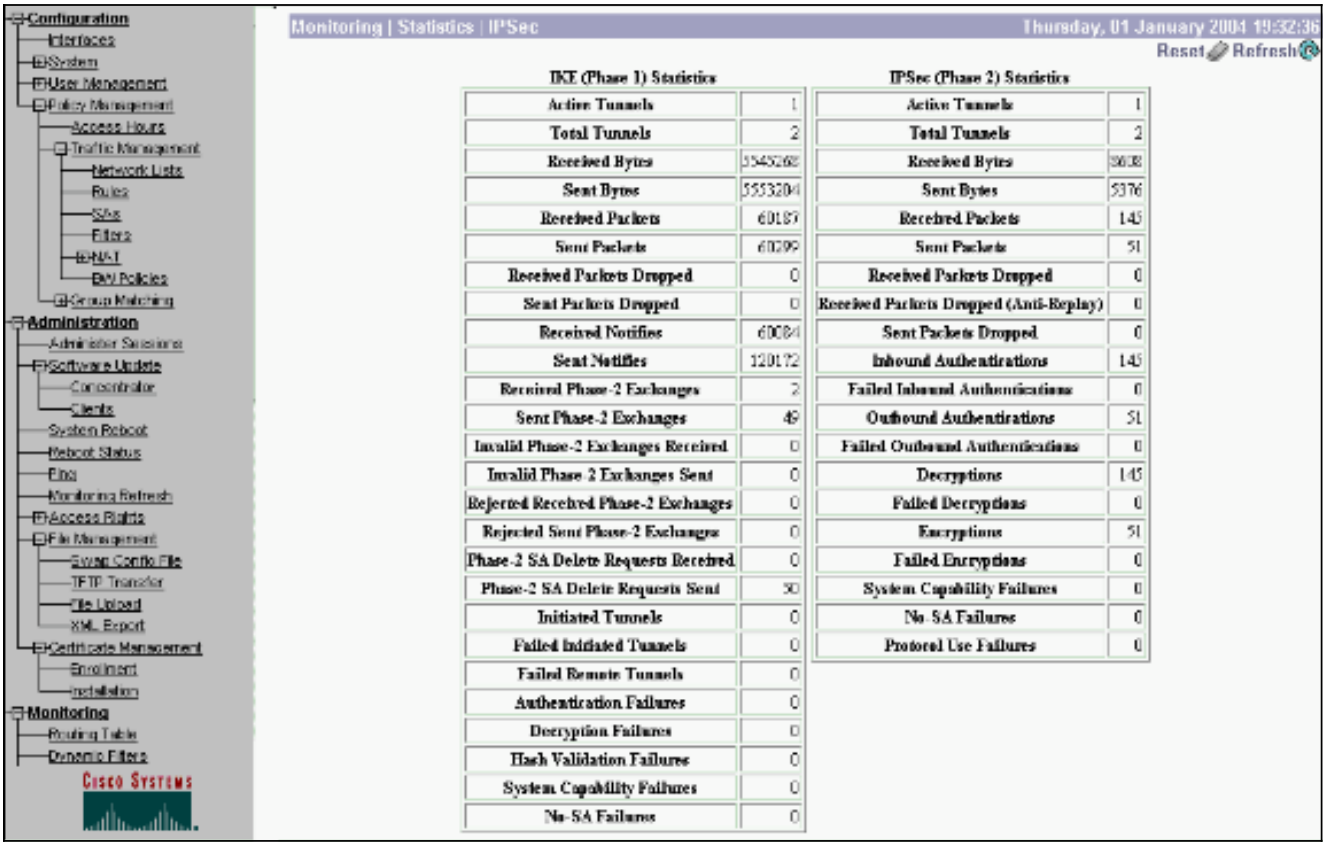
الأخيرين.

```
ipsec_router#show crypto engine connections active
ID     Interface     IP-Address   State   Algorithm           Encrypt Decrypt

Ethernet1/0   30.30.30.1   set     HMAC_SHA+AES_256_C       0       0      1

Ethernet1/0   30.30.30.1   set     HMAC_MD5+AES_256_C       0       19     2000

Ethernet1/0   30.30.30.1   set     HMAC_MD5+AES_256_C       19      0      2001
```

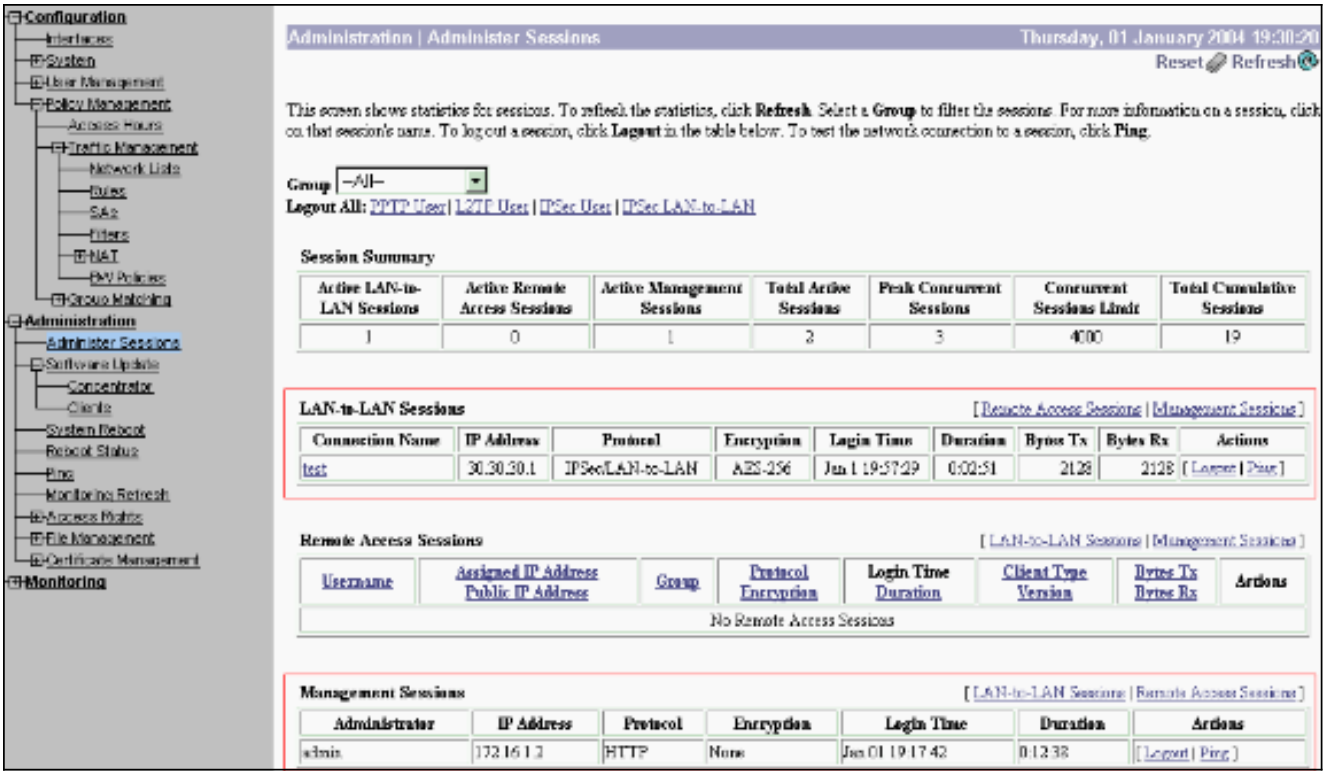
التحقق من تكوين مركز VPN

أكمل هذه الخطوات للتحقق من تكوين مركز VPN.

1. كما هو الحال لإظهار أوامر crypto ips sa و**show crypto isakmp sa** على الموجهات، يمكنك عرض إحصائيات IPsec و IKE عند تحديد **المراقبة > الإحصائيات>IPSec** على **مركزات** VPN.



2. وكما هو الحال مع الأمر **show crypto engine connections active** على الموجهات، يمكنك إستخدام نافذة Administration-Sessions على مركز VPN لعرض المعلمات والإحصائيات لجميع إتصالات LAN إلى شبكة LAN النشطة عبر بروتوكول IPsec أو الأنفاق.



استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أستكشاف أخطاء الموجه وإصلاحها

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

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

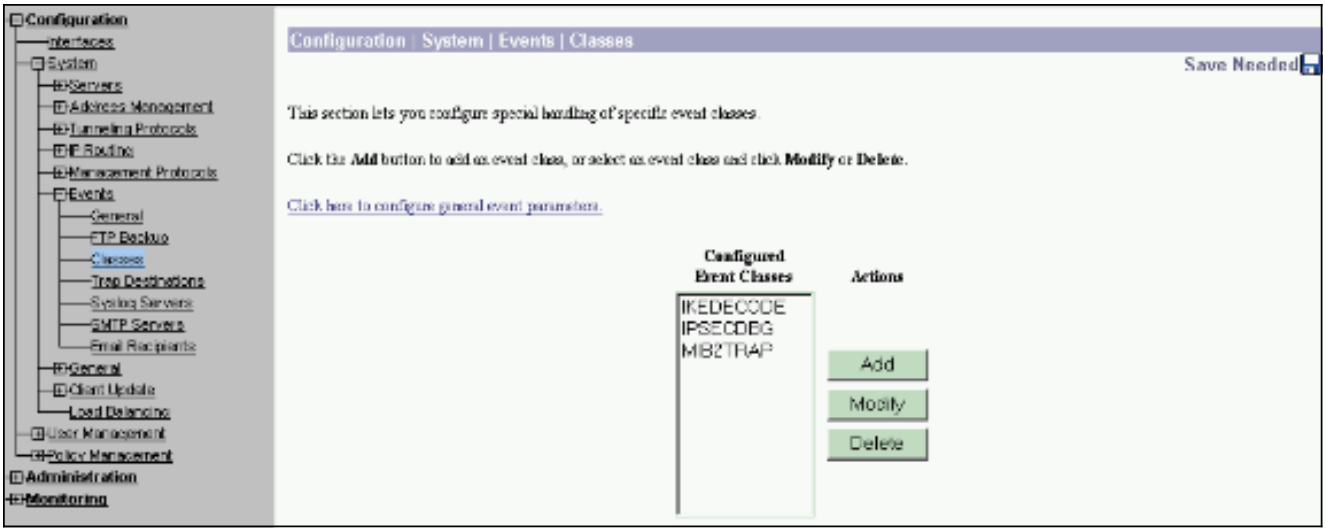
- **debug crypto engine**—يعرض حركة مرور البيانات التي يتم تشفيرها. محرك التشفير هو الآلية الفعلية التي تقوم بتنفيذ التشفير وفك التشفير. يمكن أن يكون محرك التشفير برنامج أو مسرع أجهزة.
- **debug crypto isakmp**—يعرض مفاوضات بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP) للمرحلة 1 من IKE.
- **debug crypto ips**—يعرض مفاوضات IPsec للمرحلة 2 من IKE.

راجع أستكشاف أخطاء IPSec وإصلاحها - فهم أوامر **debug** واستخدامها للحصول على معلومات أكثر تفصيلا وعينة إخراج.

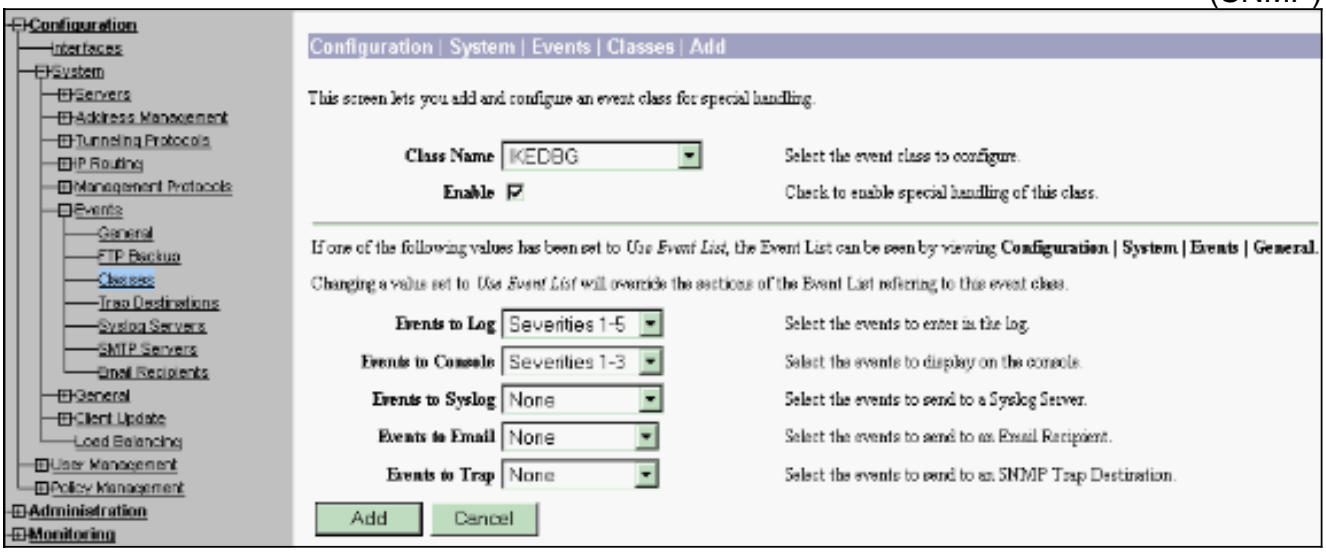
أستكشاف أخطاء مركز الشبكة الخاصة الظاهرية (VPN) وإصلاحها

يمكنك تكوين فئات الأحداث لعرض جميع الإنذارات، وذلك على غرار أوامر **تصحيح الأخطاء** على موجهات Cisco.

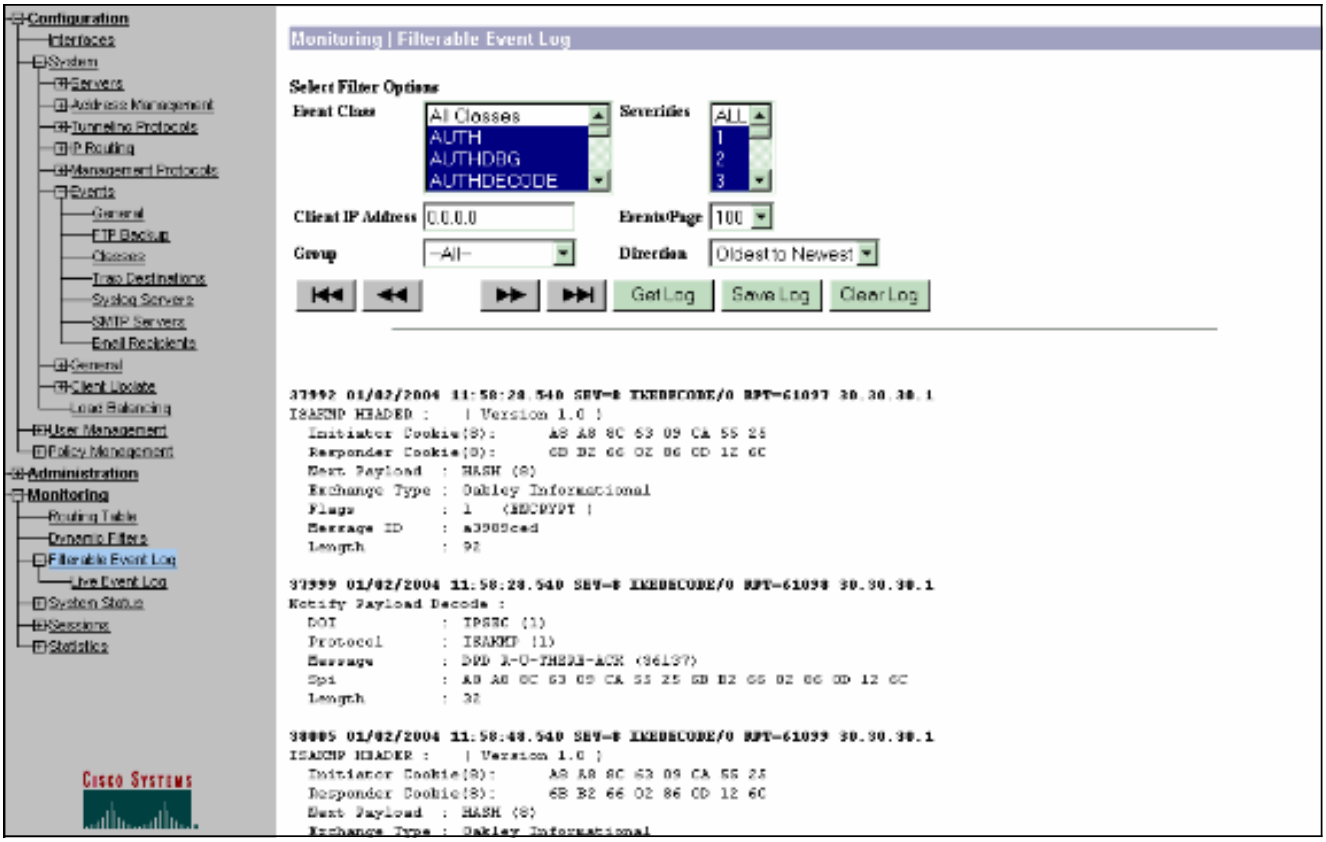
1. حدد تكوين > **نظام** > **أحداث** > **فئات** > إضافة لتشغيل تسجيل فئات الحدث.تتوفر هذه الفئات ل IPsec:آيكIkedbgإيكيديكودIPSECIPSECDBGإبسيديكوده



2. أثناء الإضافة، يمكنك أيضا تحديد مستوى الخطورة لكل فئة، استنادا إلى مستوى الخطورة الذي يتم إرسال التنبيه إليه.يمكن التعامل مع الإنذارات باستخدام إحدى هذه الأساليب:حسب السجلمعروض على وحدة التحكمتم الإرسال إلى خادم UNIX Syslogتم الإرسال كبريد إلكترونييتم إرسالها كفخ إلى خادم بروتوكول إدارة الشبكة البسيط
(SNMP)



3. حدد **مراقبة > سجل أحداث قابل للتصفية** لمراقبة الإنذارات التي تم تمكينها.



معلومات ذات صلة

- معيار التشفير المتقدم (AES)
- وحدة تشفير DES/3DES/AES VPN
- عمليات تكوين نموذج IPSec
- صفحة دعم عميل Cisco VPN 3000 Series
- صفحة دعم مفاوضة IPSec/بروتوكولات IKE

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).