تكوين نفق IPSec بين مركز Cisco VPN 3000 وجدار حماية NG لنقطة التحقق

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين نفق IPSec بمفاتيح مشتركة مسبقا للاتصال بين شبكتين خاصتين. في هذا المثال، شبكات الاتصال هي الشبكة الخاصة x.192.168.10 داخل مركز Cisco VPN 3000 والشبكة الخاصة x.x.10.32 داخل جدار حماية الجيل التالي لنقطة الوصول.

المتطلبات الأساسية

المتطلبات

- يجب أن تتدفق حركة المرور من داخل مركز الشبكة الخاصة الظاهرية (VPN) ومن داخل نقطة التفتيش NG إلى الإنترنت - الممثلة هنا بشبكات x.172.18.124 - قبل بدء هذا التكوين.
- يجب أن يكون المستخدمون على دراية بتفاوض IPSec. يمكن تقسيم هذه العملية إلى خمس خطوات، تتضمن مرحلتين من عملية تبادل مفتاح الإنترنت (IKE).يتم إنشاء نفق IPSec بواسطة حركة مرور مثيرة للاهتمام. تعتبر حركة المرور مثيرة للاهتمام عندما تنتقل بين أقران IPSec.في المرحلة الأولى من IKE، يتفاوض نظراء IPSec على سياسة اقتران أمان IKE (SA) الراسخة. بمجرد مصادقة النظراء، يتم إنشاء نفق آمن باستخدام بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP).في المرحلة 2 من IKE، يستخدم نظراء IPSec النفق الآمن

والمصدق من أجل التفاوض على عمليات تحويل IPSec SA. يحدد التفاوض على السياسة المشتركة كيفية إنشاء نفق IPSec.يتم إنشاء نفق IPSec، ويتم نقل البيانات بين نظائر IPSec استنادا إلى معلمات IPSec التي تم تكوينها في مجموعات تحويل IPSec.ينتهي نفق IPSec عند حذف أسماء IPSec أو عند انتهاء صلاحية عمرها الافتراضي.

المكونات المستخدمة

تم تطوير هذه التهيئة واختبارها باستخدام إصدارات البرامج والمكونات المادية التالية:

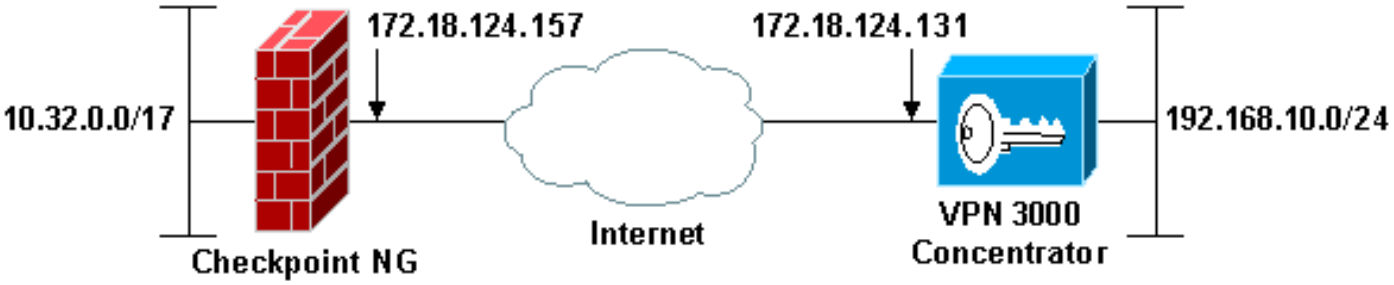
- مركز VPN 3000 Series Concentrator 3.5.2
- جدار حماية NG لنقطة التحقق

الاصطلاحات

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



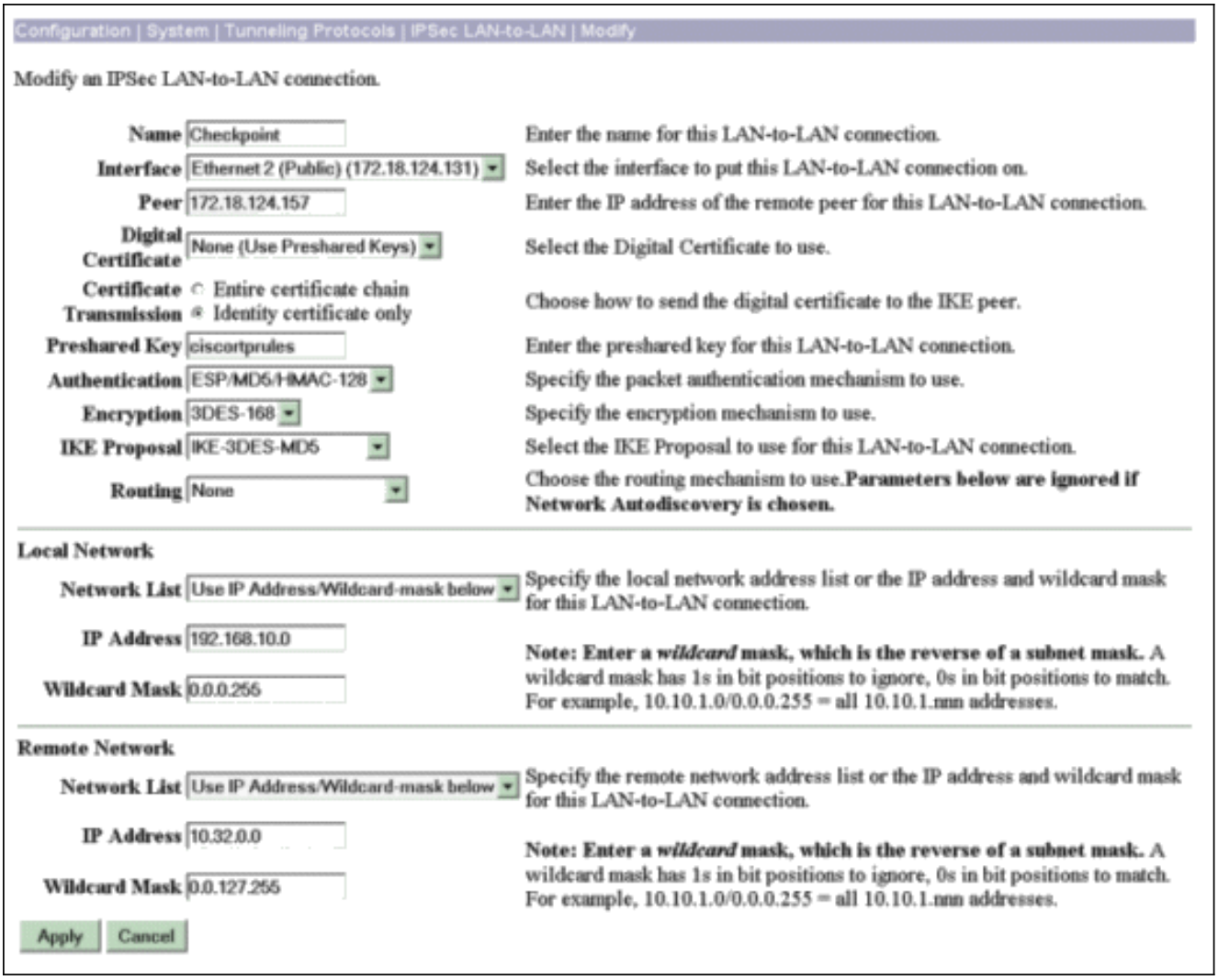
ملاحظة: مخطط عنونة IP المستخدم في هذا التكوين غير قابل للتوجيه بشكل قانوني على الإنترنت. هم rfc 1918 عنوان، أي يتلقى يكون استعملت في مختبر بيئة.

التكوينات

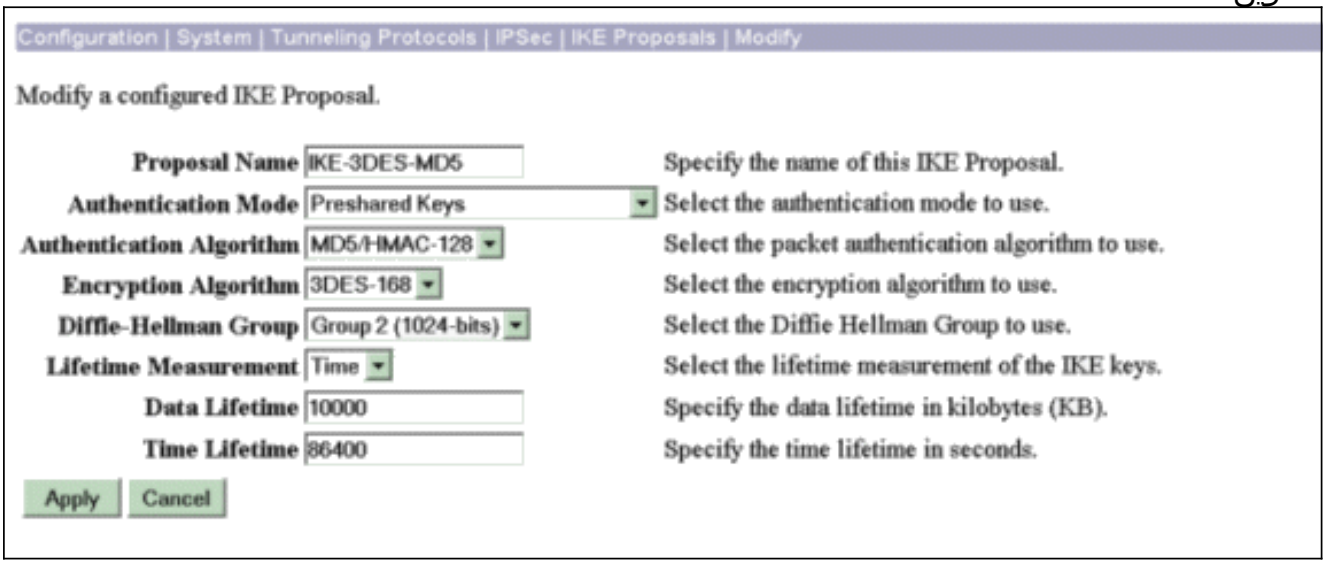
تكوين مركز VPN 3000

أتمت هذا steps in order to شكلت ال VPN 3000 مركز:

1. انتقل إلى **التكوين > النظام > بروتوكولات الاتصال النفقي > IPSec LAN إلى LAN** لتكوين جلسة عمل الشبكة المحلية (LAN) إلى الشبكة المحلية (LAN). قم بتعيين الخيارات الخاصة بخوارزميات المصادقة والتشغيل الفوري للبروتوكول IKE والمفتاح المشترك مسبقا وعنوان IP للنظير والمعلمات المحلية والبعيدة للشبكة. طقطقة **يطبق**.في هذا التكوين، تم تعيين المصادقة على أنها ESP-MD5-HMAC وتم تعيين التشفير على 3DES.

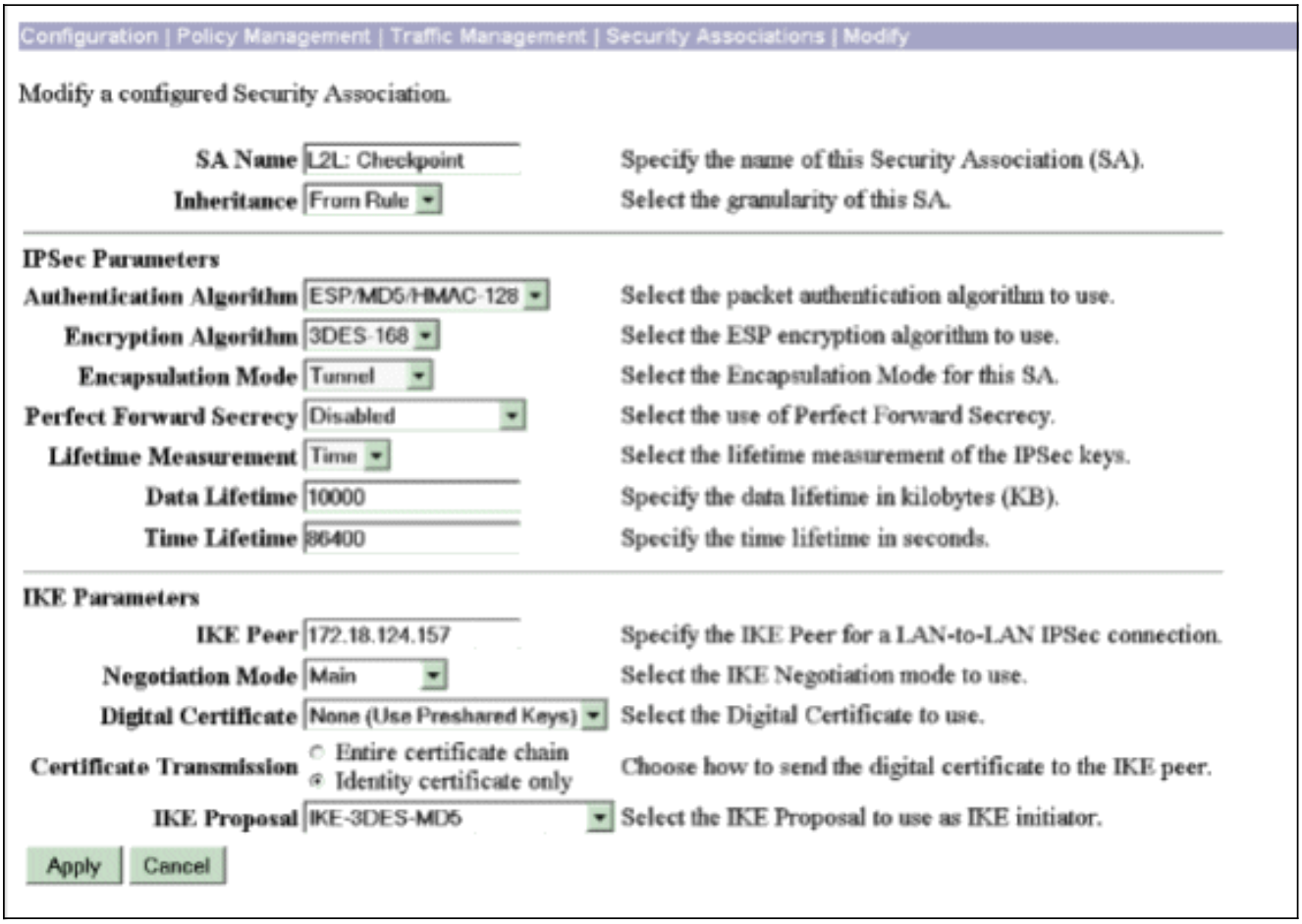


2. انتقل إلى **التكوين > النظام > بروتوكولات الاتصال النفقي > IPSec > مقترحات IKE** وقم بتعيين المعلمات المطلوبة.حدد مقترح IKE-3DES-MD5 وتحقق من المعلمات المحددة للمقترح. طقطقة **يطبق** in order to شكلت ال LAN إلى LAN جلسة.هذه هي معلمات هذا التكوين:



3. انتقل إلى **التكوين > إدارة السياسة > إدارة حركة المرور > اقترانات الأمان،** وحدد IPSec SA الذي تم إنشاؤه للجلسة، وتحقق من معلمات IPSec SA التي تم إختيارها لجلسة عمل الشبكة المحلية (LAN) إلى الشبكة المحلية (LAN).في هذا التكوين، كان اسم جلسة عمل الشبكة المحلية (LAN) إلى الشبكة المحلية (LAN) هو "Checkpoint"، لذلك تم إنشاء IPSec SA تلقائيا ك "L2L:Checkpoint".

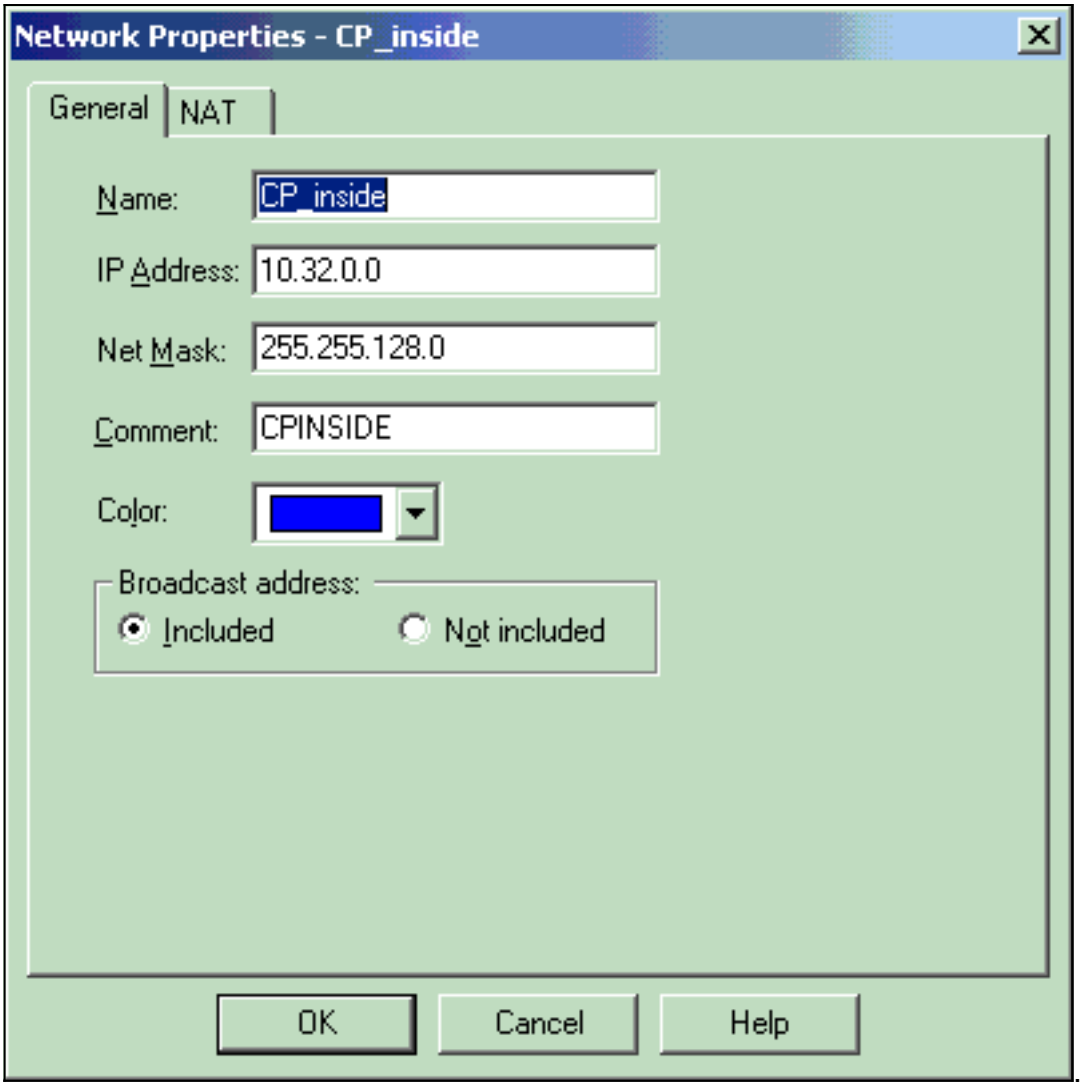
هذه هي المعلمات ل
:SA

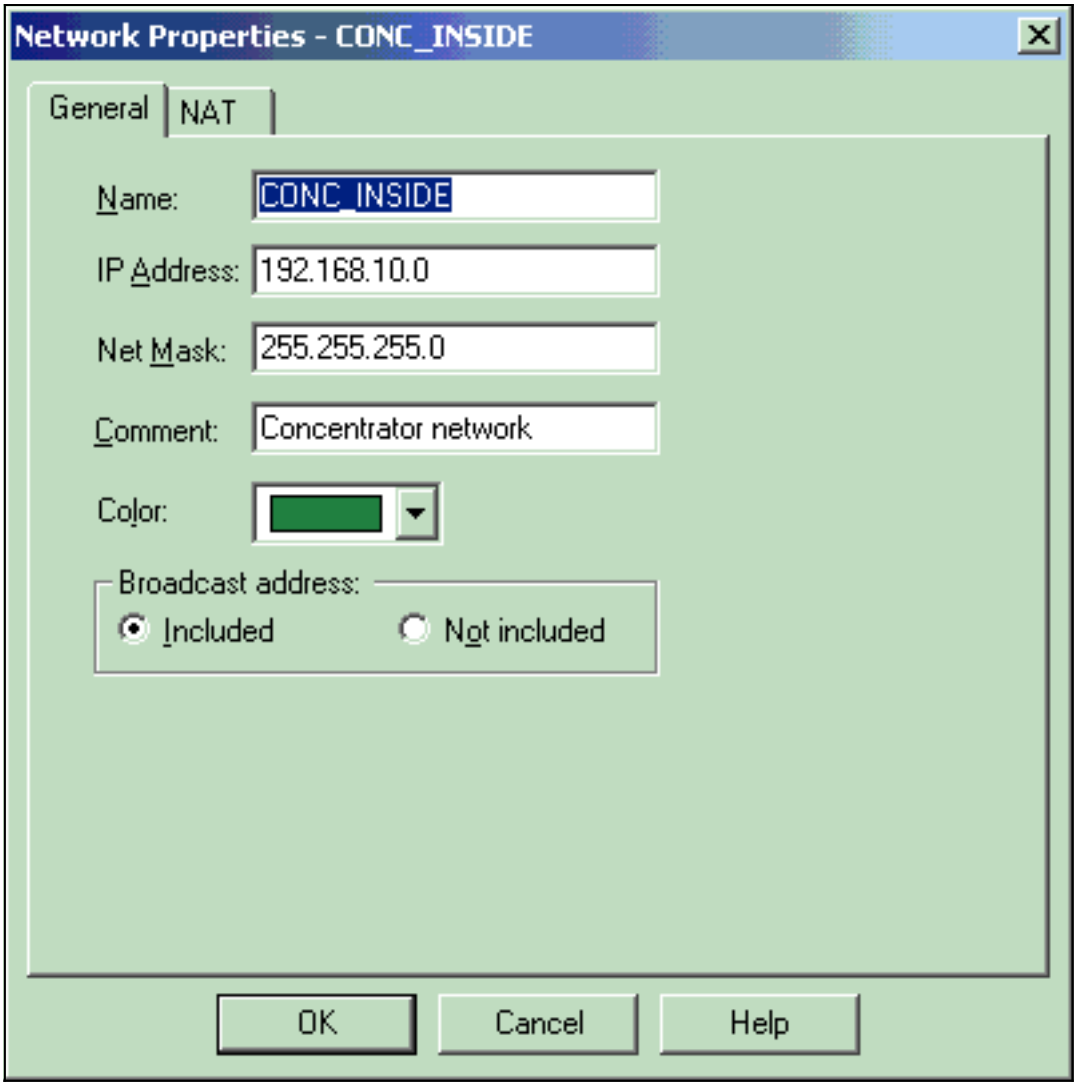


تكوين NG لنقطة التحقق

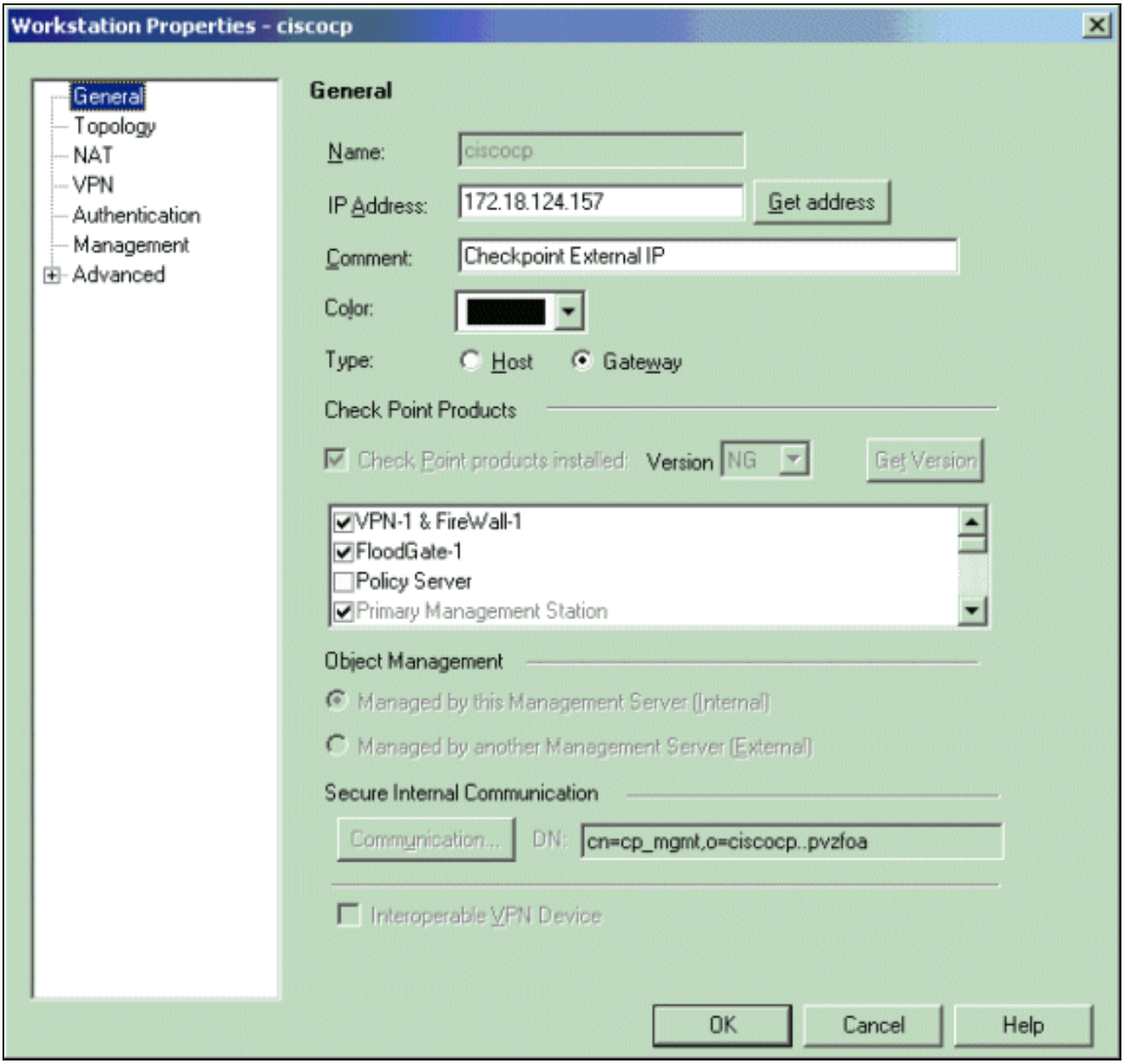
يتم تحديد كائنات الشبكة وقواعدها على نقطة الوصول NG لإنشاء السياسة المتعلقة بتكوين شبكة VPN الذي سيتم إعداده. يتم بعد ذلك تثبيت هذا النهج مع محرر نهج NG الخاص بنقطة التحقق لإكمال جانب NG لنقطة التحقق من التكوين.

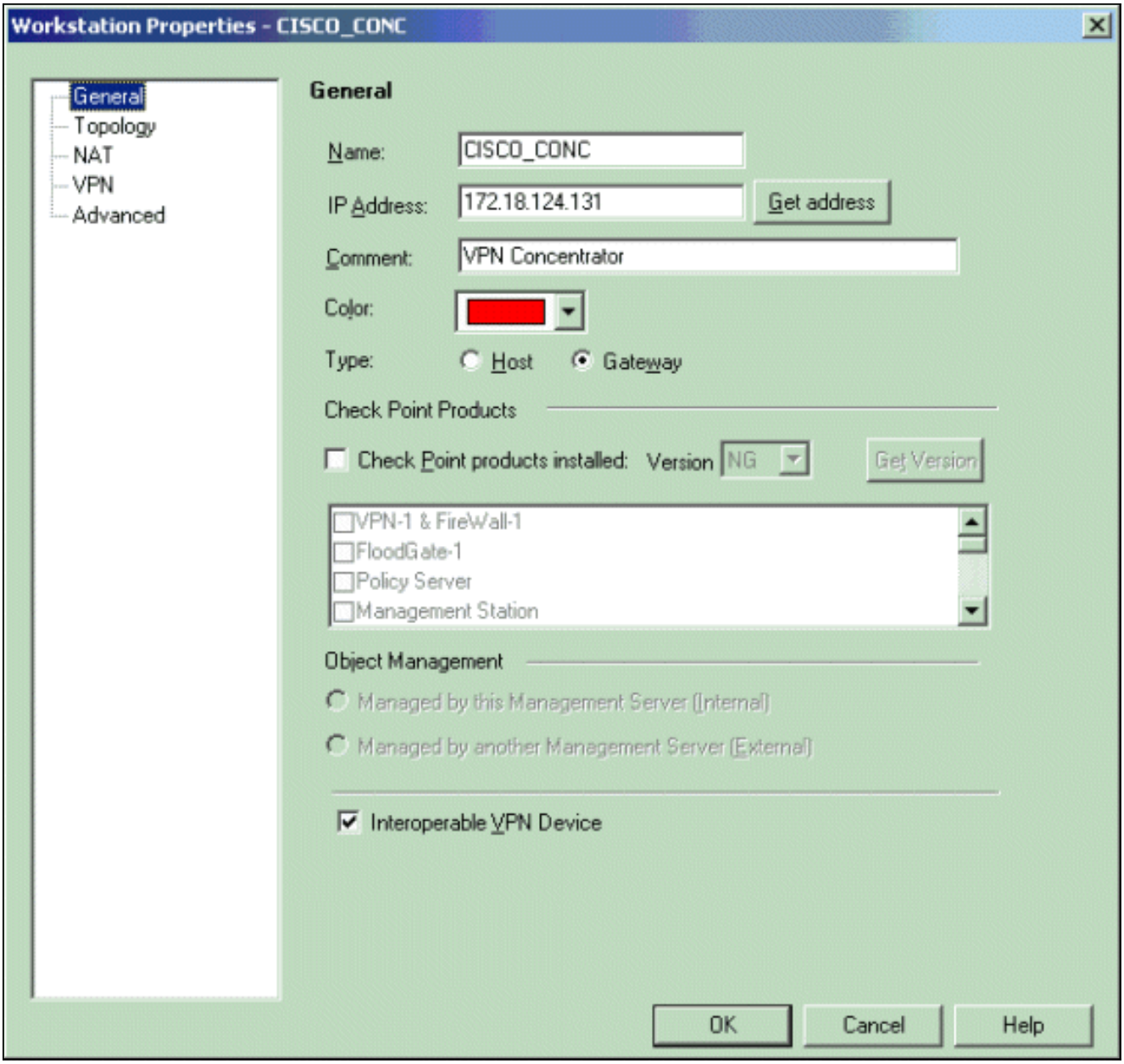
1. قم بإنشاء كائني الشبكة لشبكة NG نقطة الوصول وشبكة مركز VPN التي ستقوم بتشفير حركة المرور المفيدة.لإنشاء كائنات، حدد **إدارة > كائنات الشبكة**، ثم حدد **جديد > شبكة**. أدخل معلومات الشبكة المناسبة، ثم انقر على موافق.تظهر هذه الأمثلة مجموعة من كائنات الشبكة تسمى CP_Inside (الشبكة الداخلية لنقطة التحكم NG) و CONC_INSIDE (الشبكة الداخلية لمركز


Network Properties - CP_inside
General
NAT
Name:
CP_inside
IP Address:
10.32.0.0
Net Mask:
255.255.128.0
Comment:
CPINSIDE
Color:
Broadcast address:
Included
Not included
OK
Cancel
Help
.(VPN

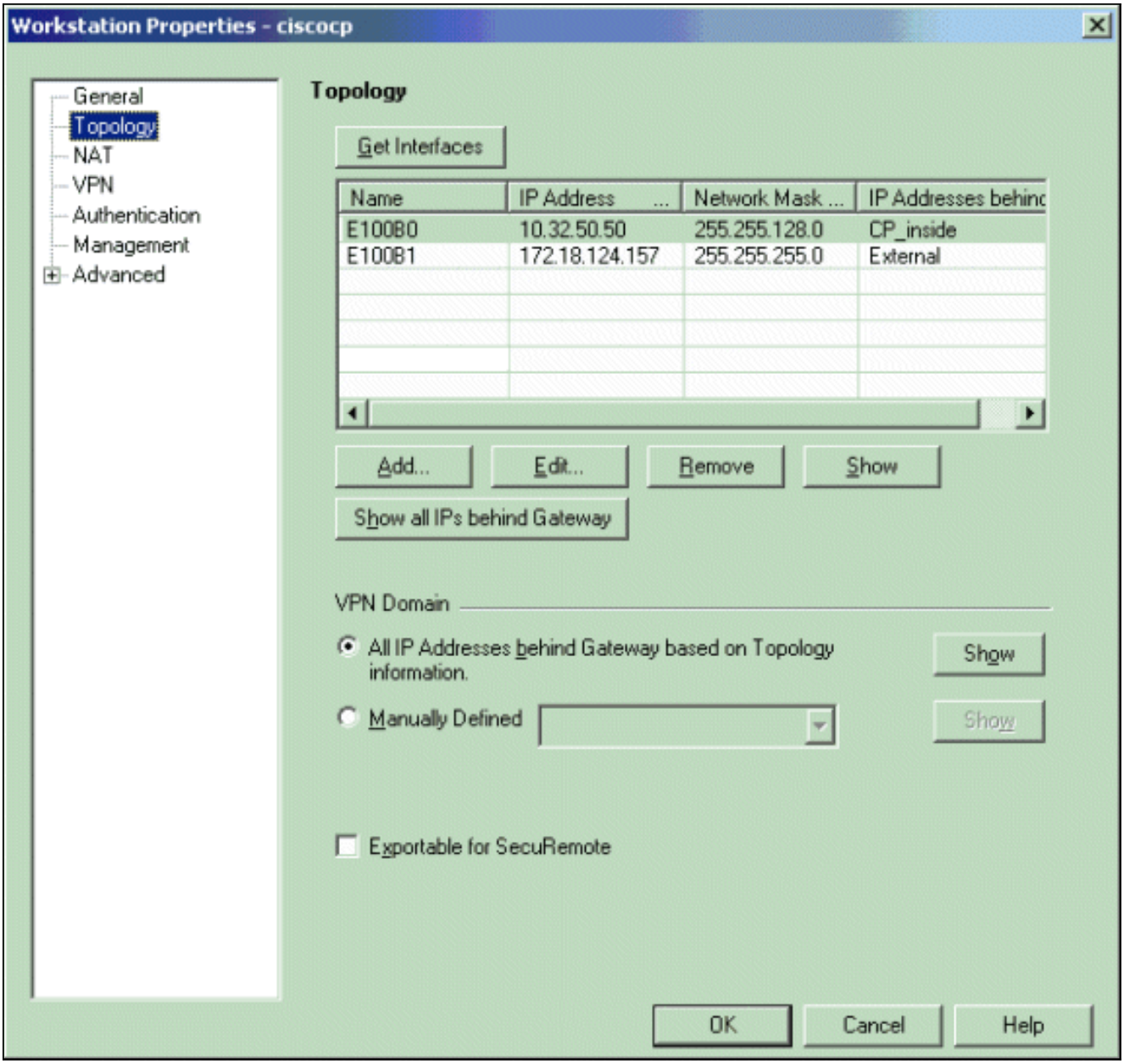


2. انتقل إلى **إدارة > كائنات الشبكة** وحدد **جديد > محطة عمل** لإنشاء كائنات محطة عمل لأجهزة الشبكة الخاصة الظاهرية (VPN)، نقطة الوصول NG ومركز الشبكة الخاصة الظاهرية (VPN).**ملاحظة:** يمكنك إستخدام كائن محطة العمل NG لنقطة الوصول الذي تم إنشاؤه أثناء إعداد NG لنقطة الوصول الأولية. حدد الخيارات لتعيين محطة العمل كبوابة وجهاز VPN قابل للتشغيل البيني، ثم انقر فوق **موافق**.تظهر هذه الأمثلة مجموعة الكائنات التي تسمى CiscoCcp (نقطة الوصول NG) و Cisco_CONC (مركز VPN 3000):

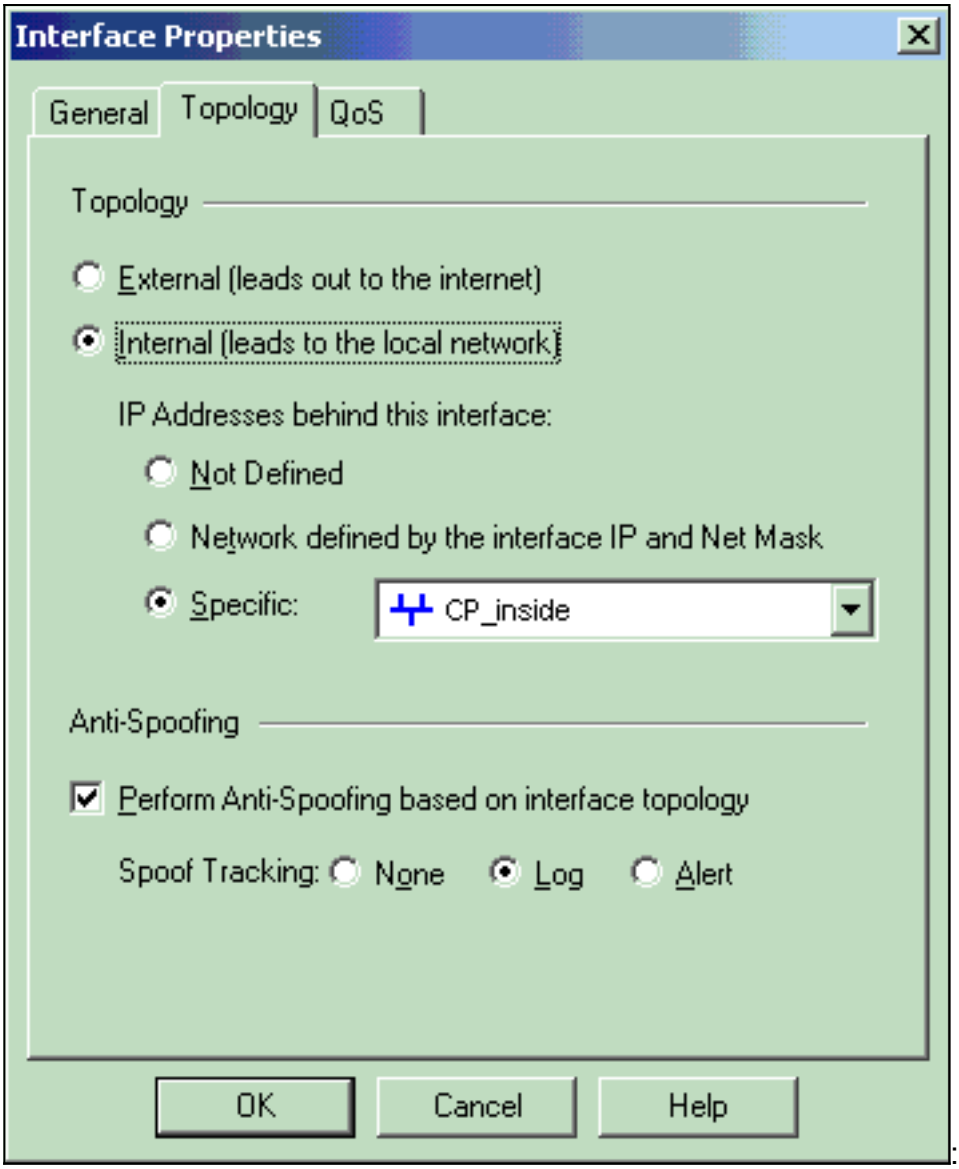

Workstation Properties - ciscocp
General
Topology
NAT
VPN
Authentication
Management
Advanced
General
Name:
ciscocp
IP Address:
172.18.124.157
Get address
Comment:
Checkpoint External IP
Color:
Type:
Host
Gateway
Check Point Products
Check Point products installed:
Version
NG
Get Version
VPN-1 & FireWall-1
FloodGate-1
Policy Server
Primary Management Station
Object Management
Managed by this Management Server (Internal)
Managed by another Management Server (External)
Secure Internal Communication
Communication...
DN:
cn=cp_mgmt,o=ciscocp..pvzfoa
Interoperable VPN Device
OK
Cancel
Help



3. انتقل إلى **إدارة > كائنات الشبكة > تحرير** لفتح نافذة خصائص محطة العمل الخاصة بمحطة العمل NG نقطة التحقق (CiscoPlug في هذا المثال). حدد **المخطط** من الخيارات الموجودة على الجانب الأيسر من النافذة، ثم حدد الشبكة التي سيتم تشفيرها. طقطقة **يحرر** in order to ثبت القارن خاصية.في هذا المثال، CP_Inside هو الشبكة الداخلية ل NG لنقطة التحقق.

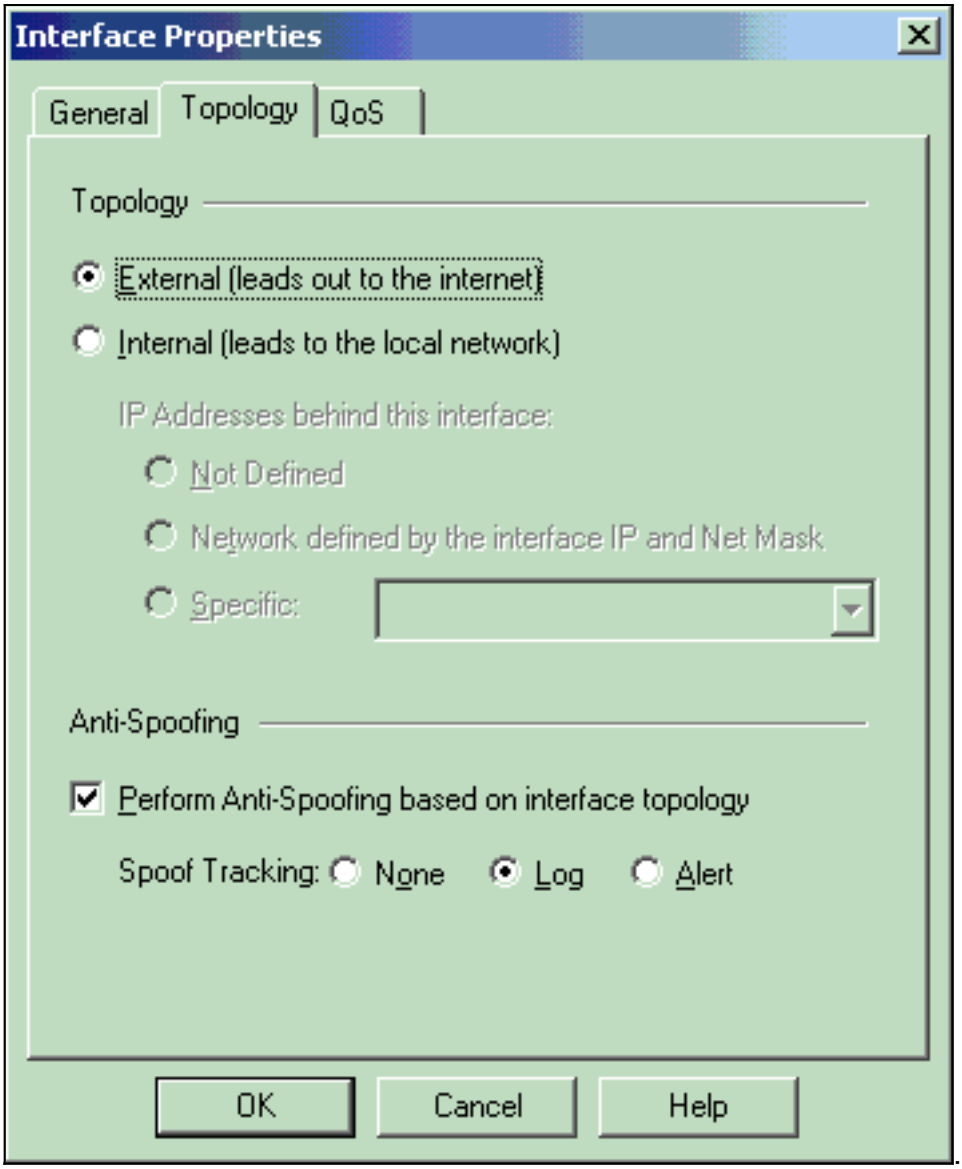


4. في نافذة خصائص الواجهة، حدد الخيار لتعيين محطة العمل كمحطة عمل داخلية، ثم حدد عنوان IP المناسب. وانقر فوق OK.تعين تحديدات المخطط المعروضة محطة العمل كمحطة عمل داخلية وتحدد عناوين IP خلف



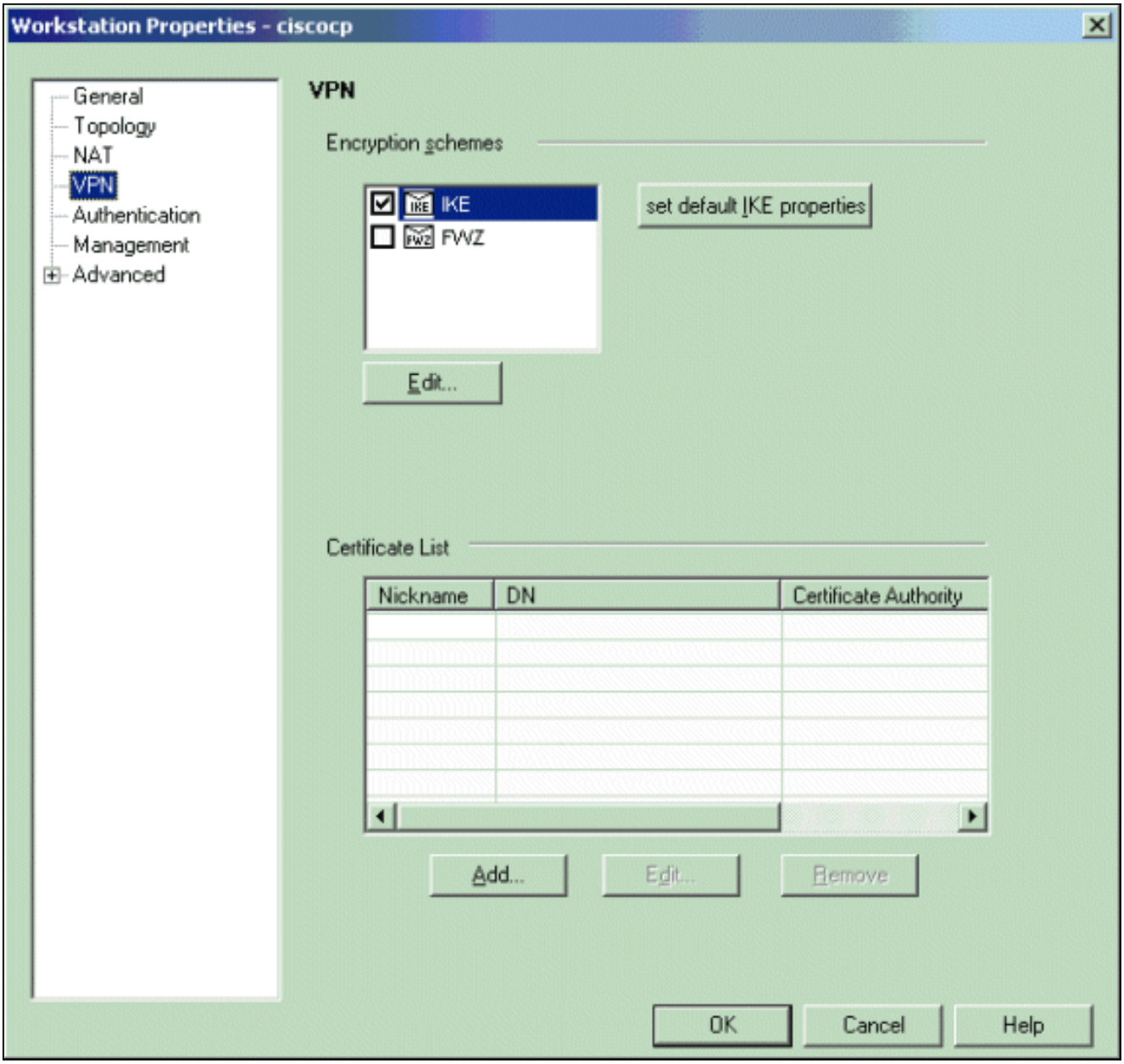
واجهة CP_Inside:

5. من نافذة "خصائص محطة العمل"، حدد الواجهة الخارجية على نقطة التفتيش NG التي تؤدي إلى الإنترنت، ثم انقر فوق **تحرير** لتعيين خصائص الواجهة. حدد الخيار لتعيين المخطط كمخطط خارجي، ثم انقر فوق

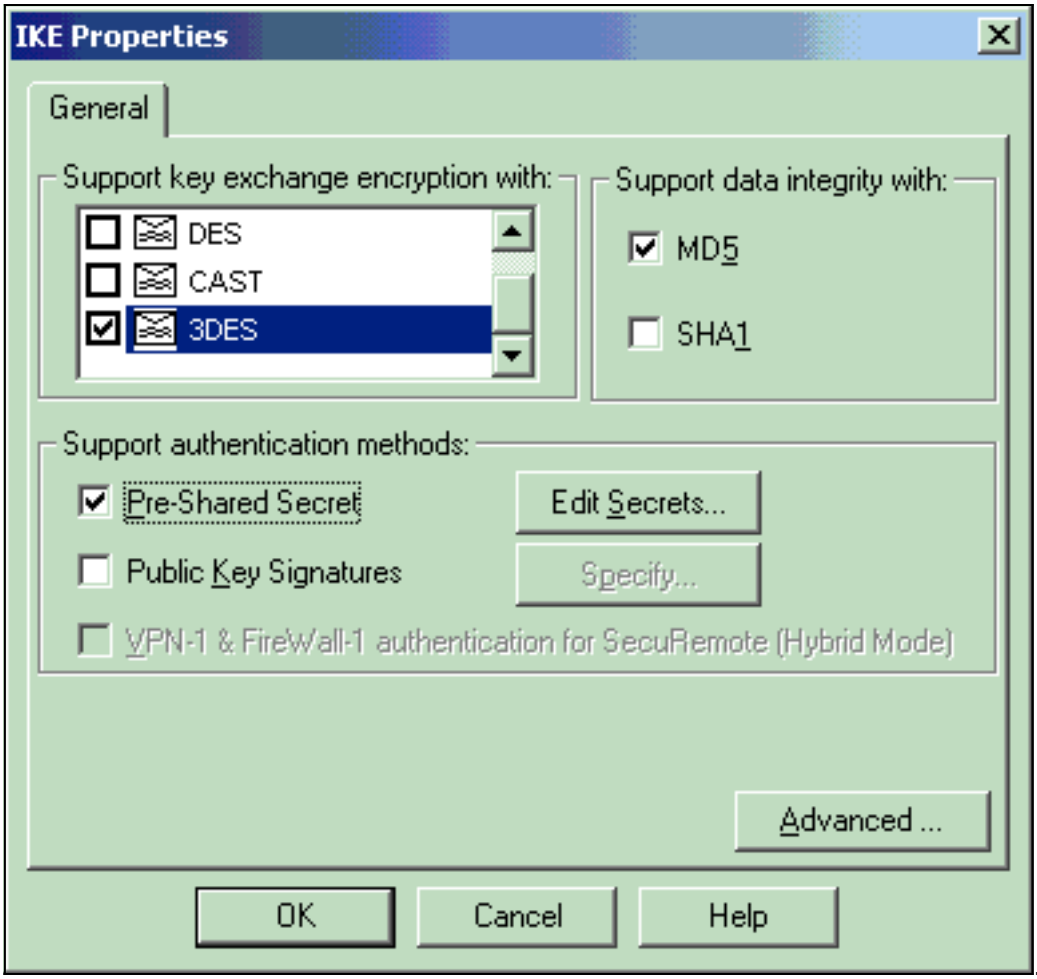


موافق.

6. من نافذة خصائص محطة العمل الموجودة على نقطة التفتيش NG، حدد **VPN** من الخيارات الموجودة على الجانب الأيسر من النافذة، ثم حدد معلمات IKE لخوارزميات التشفير والمصادقة. طقطقة **يحرر** in order to شكلت ال ike
خاصية.

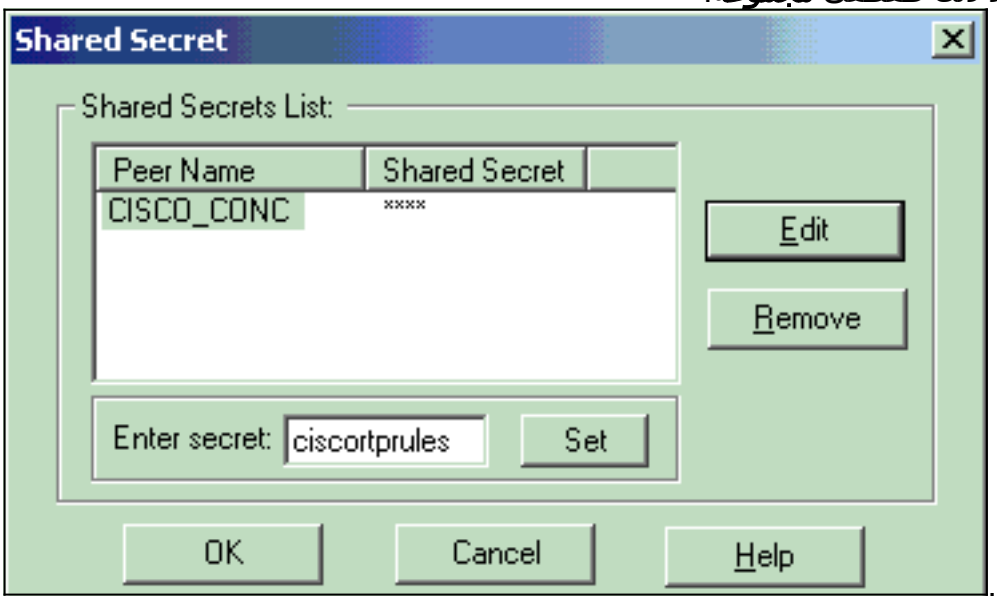


7. اضبط خصائص IKE لتطابق الخصائص على مركز VPN.في هذا المثال، حدد خيار التشفير ل **3DES** وخيار



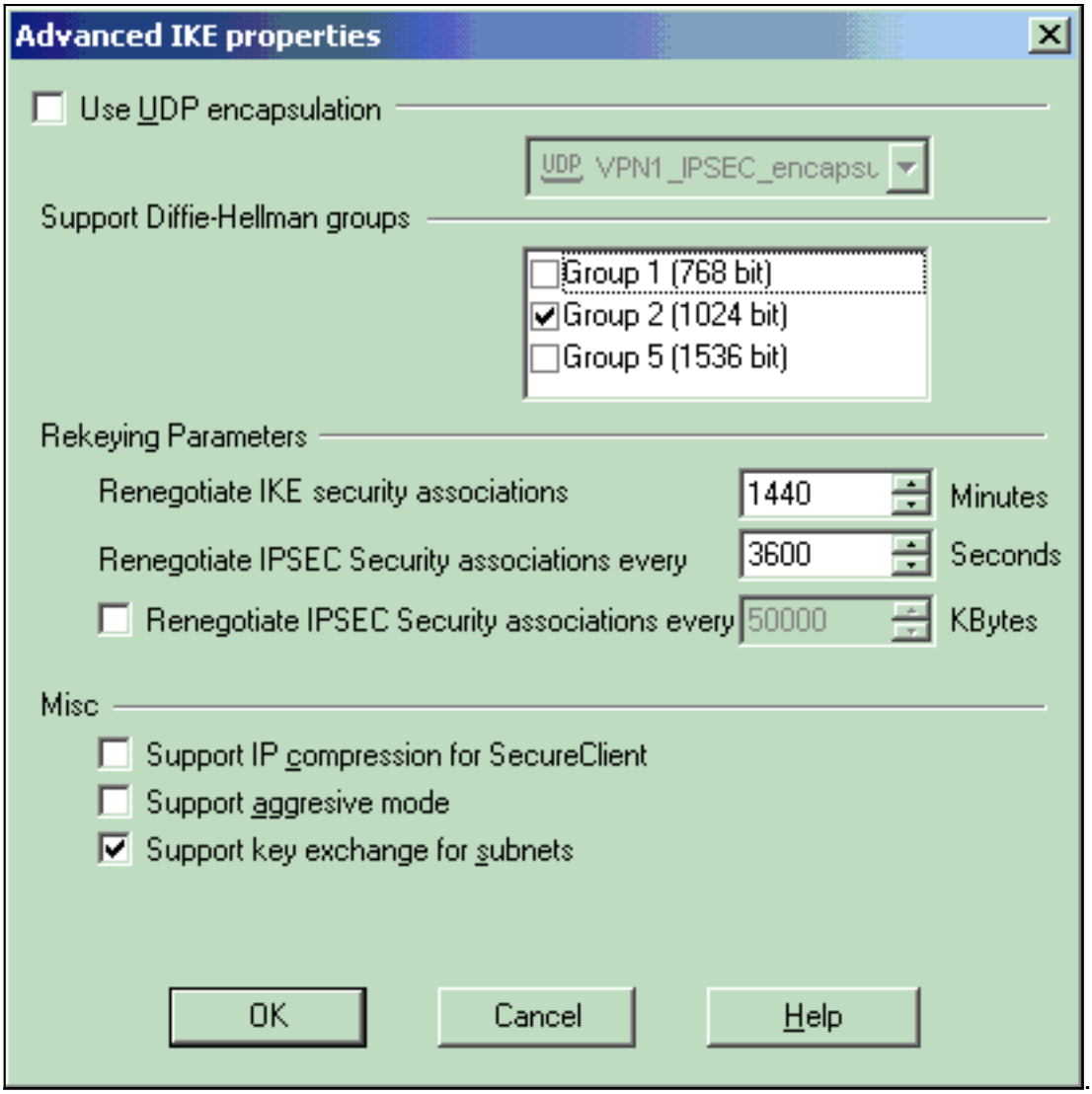
التجزئة ل **MD5**.

8. حدد خيار المصادقة **للأسرار المشتركة مسبقا**، ثم انقر **تحرير الأسرار** لتعيين المفتاح المشترك مسبقا ليكون متوافقا مع المفتاح المشترك مسبقا على مركز VPN. طقطقة **يحرر** in order to دخلت مفتاحك كما هو موضح، بعد ذلك طقطقت **مجموعة**،



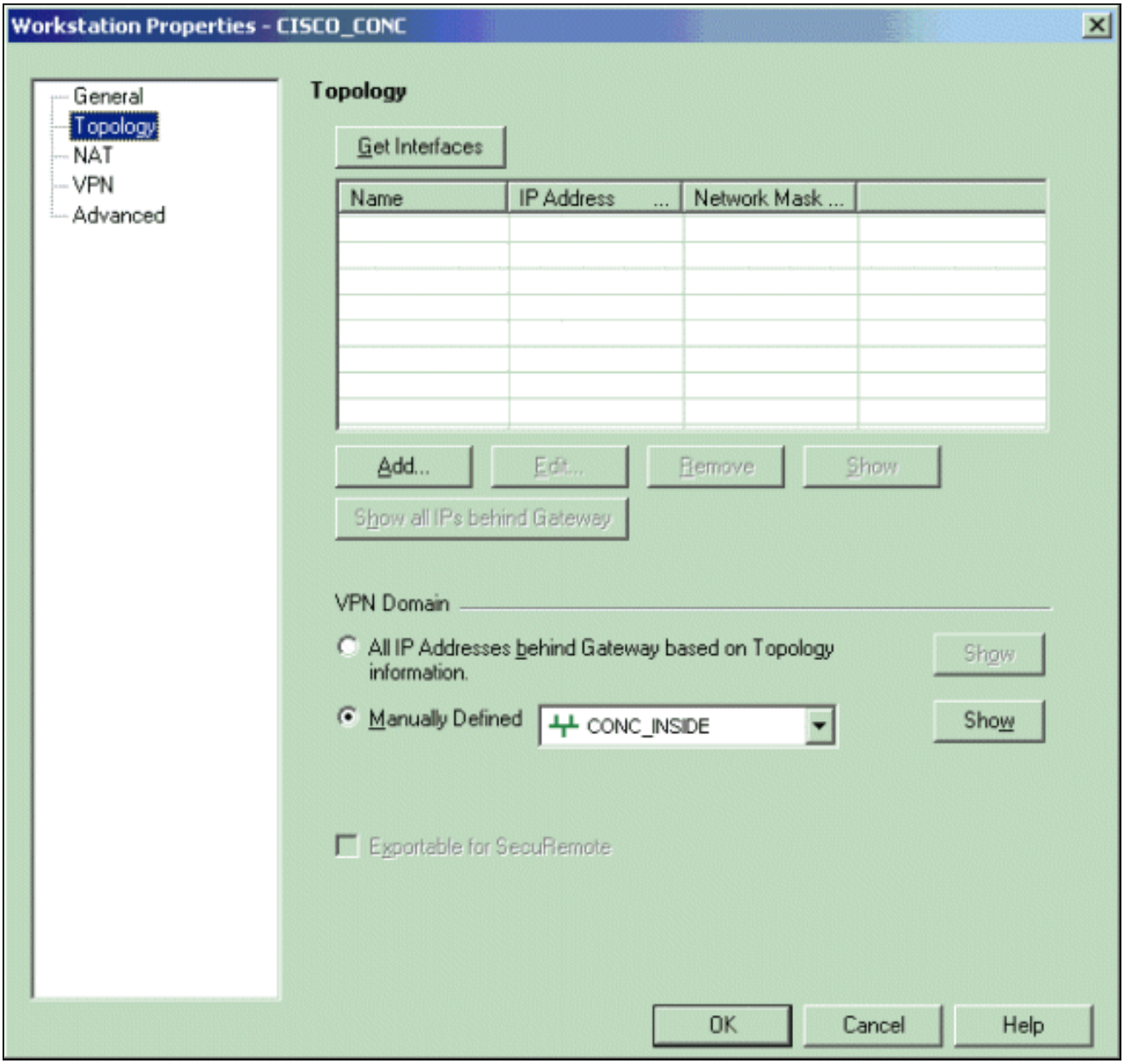
ok.

9. من نافذة خصائص IKE، انقر على **خيارات متقدمة**... وقم بتغيير هذه الإعدادات:قم بإلغاء تحديد خيار **دعم الوضع المتداخل**.حدد الخيار **لتبادل مفتاح الدعم للشبكات الفرعية**.عندما تنتهي، انقر **موافق**،

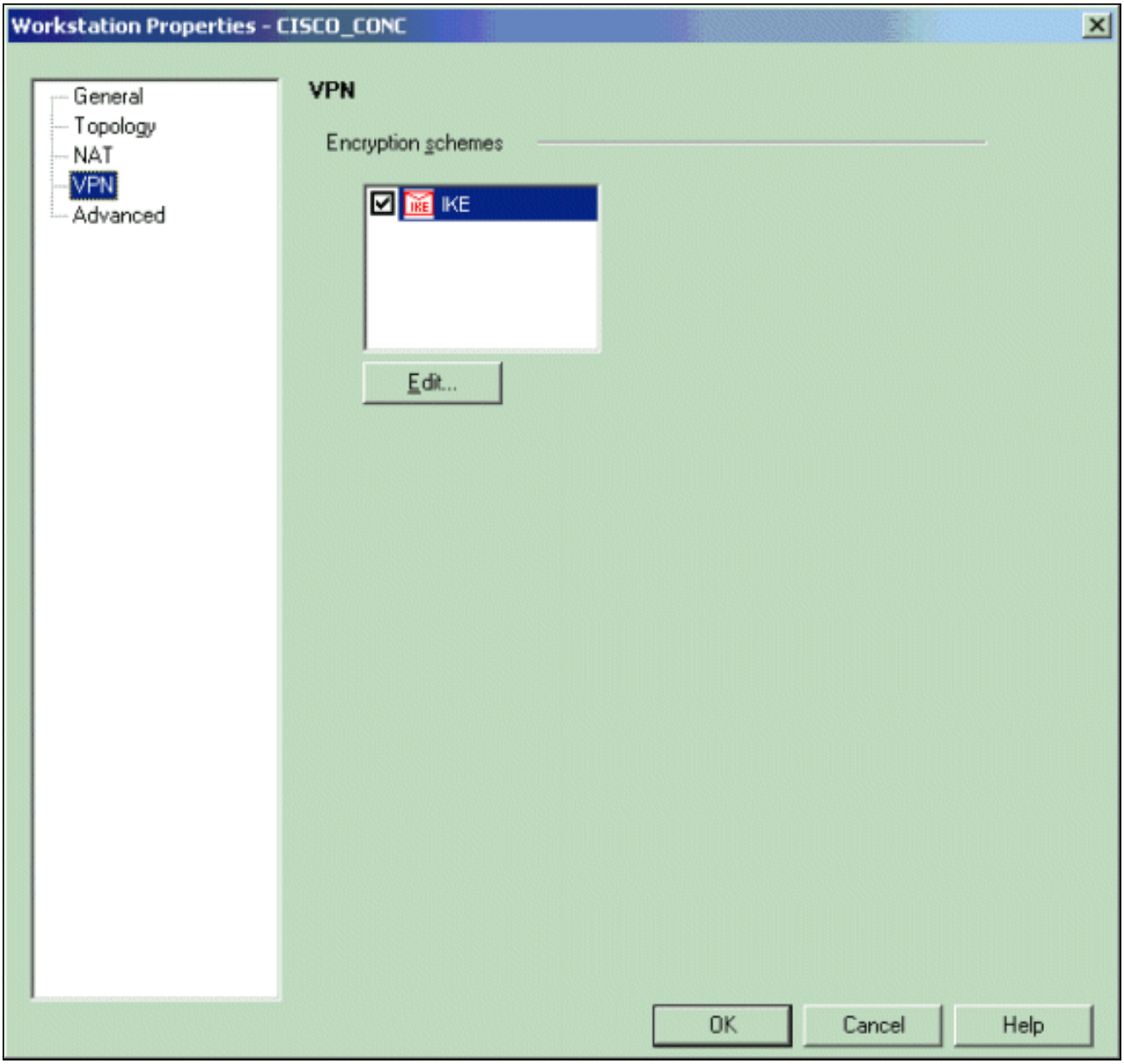


موافق.

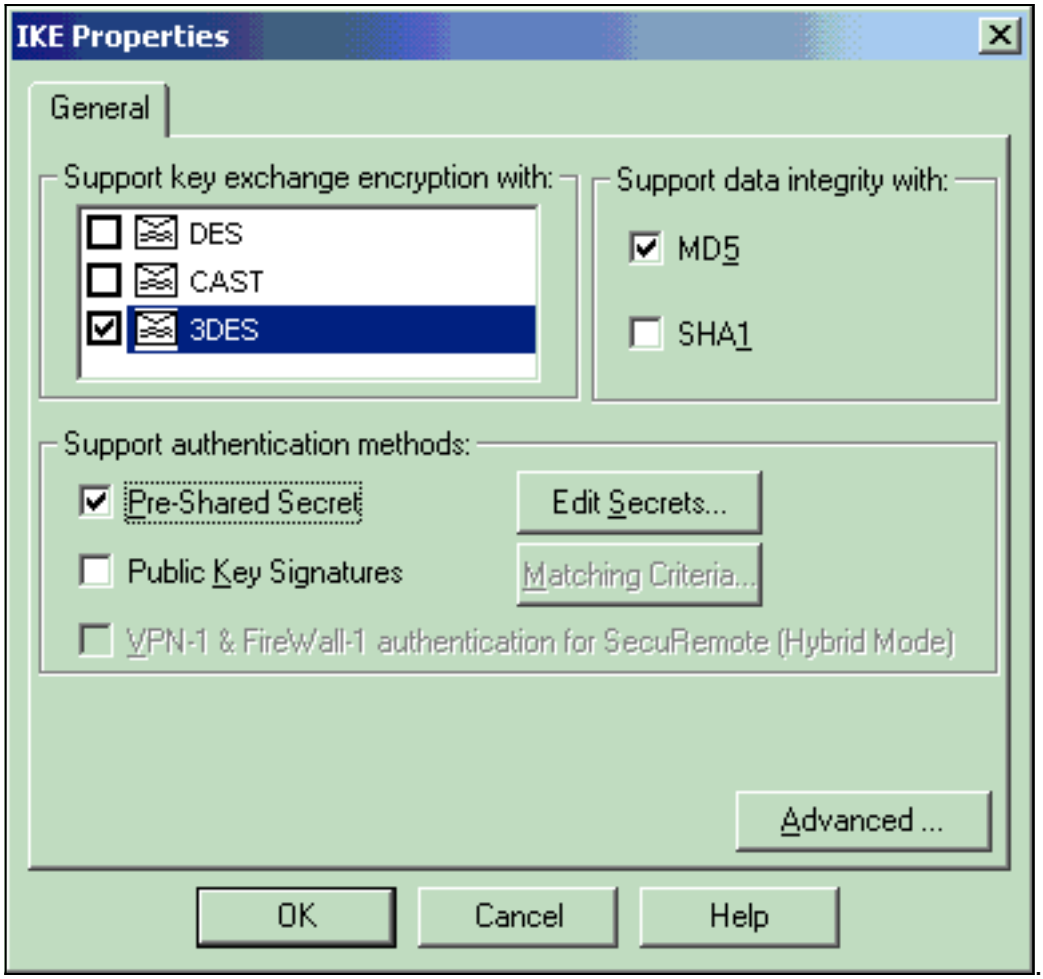
10. انتقل إلى **إدارة > كائنات الشبكة > تحرير** لفتح نافذة خصائص محطة العمل لتركيز الشبكة الخاصة الظاهرية (VPN). أخترت **طوبولوجيا** من الخيار على الجانب الأيسر من النافذة in order to عينت يدويا ال VPN مجال.في هذا المثال، يتم تعريف CONC_INSIDE (الشبكة الداخلية من مركز VPN) على أنها مجال شبكة VPN.



11. حدد **VPN** من الخيارات الموجودة على الجانب الأيسر من النافذة، ثم حدد **IKE** كمخطط تشفير. طقطقة **يحرر** in order to شكلت ال ike خاصية.

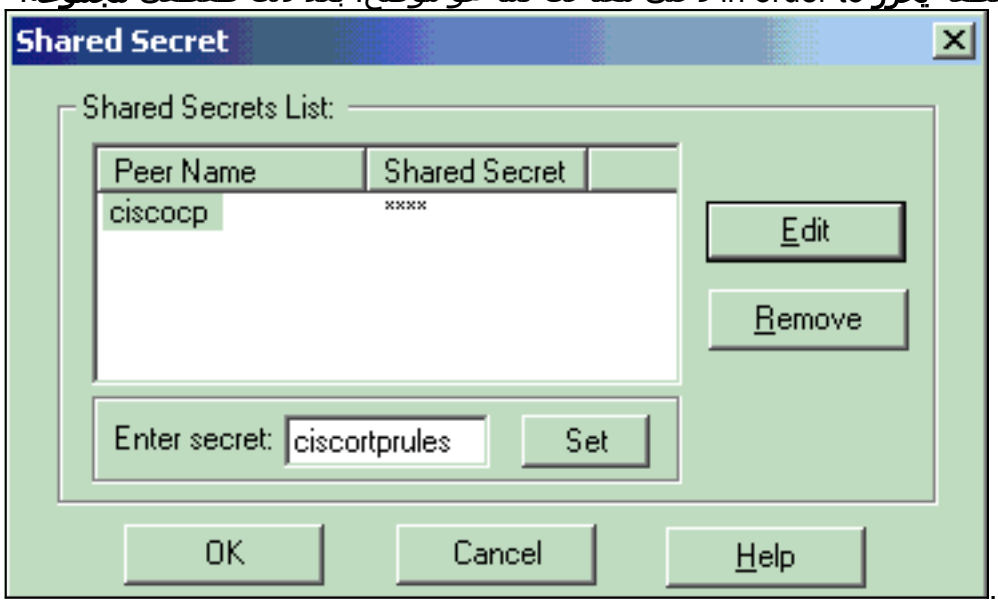


12. قم بتعيين خصائص IKE لتعكس التكوين الحالي على مركز VPN.في هذا المثال، قم بتعيين خيار التشفير ل 3DES وخيار التجزئة ل



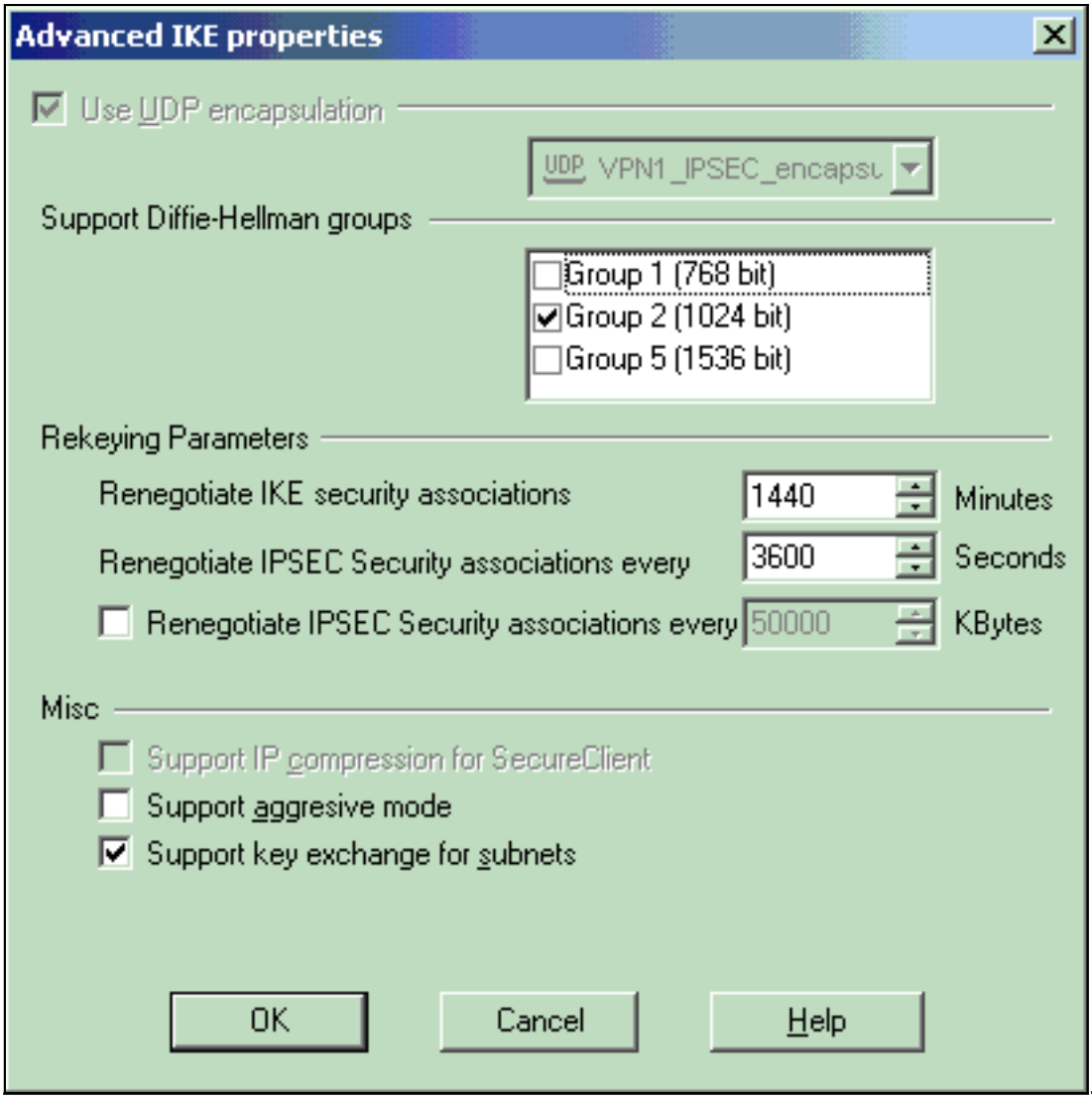
MD5.

13. حدد خيار المصادقة **للأسرار المشتركة مسبقا**، ثم انقر فوق **تحرير الأسرار** لتعيين المفتاح المشترك مسبقا. طقطقة **يحرر** in order to دخلت مفتاحك كما هو موضح، بعد ذلك طقطقت **مجموعة**،



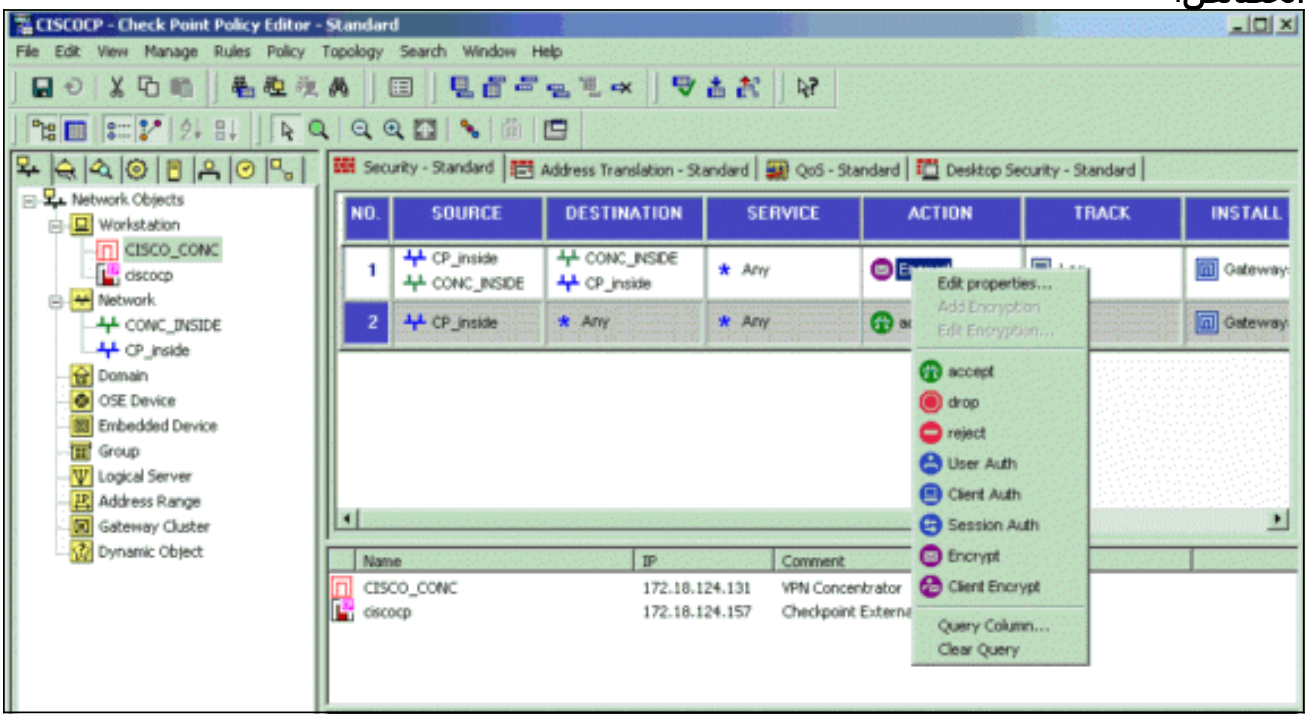
ok.

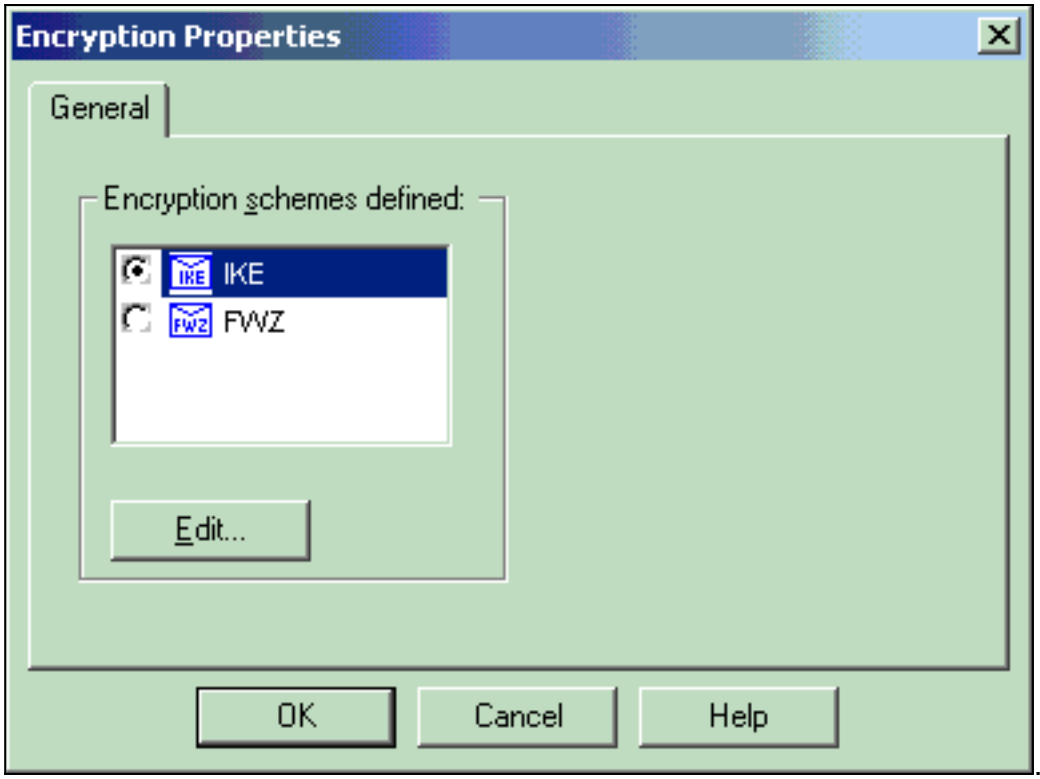
14. من نافذة خصائص IKE، انقر على **خيارات متقدمة**... وقم بتغيير هذه الإعدادات:حدد مجموعة Diffie-Hellman المناسبة لخصائص IKE.قم بإلغاء تحديد خيار **دعم الوضع المتداخل**.حدد الخيار **لتبادل مفتاح الدعم للشبكات الفرعية**.عندما تنتهي، انقر **موافق**،



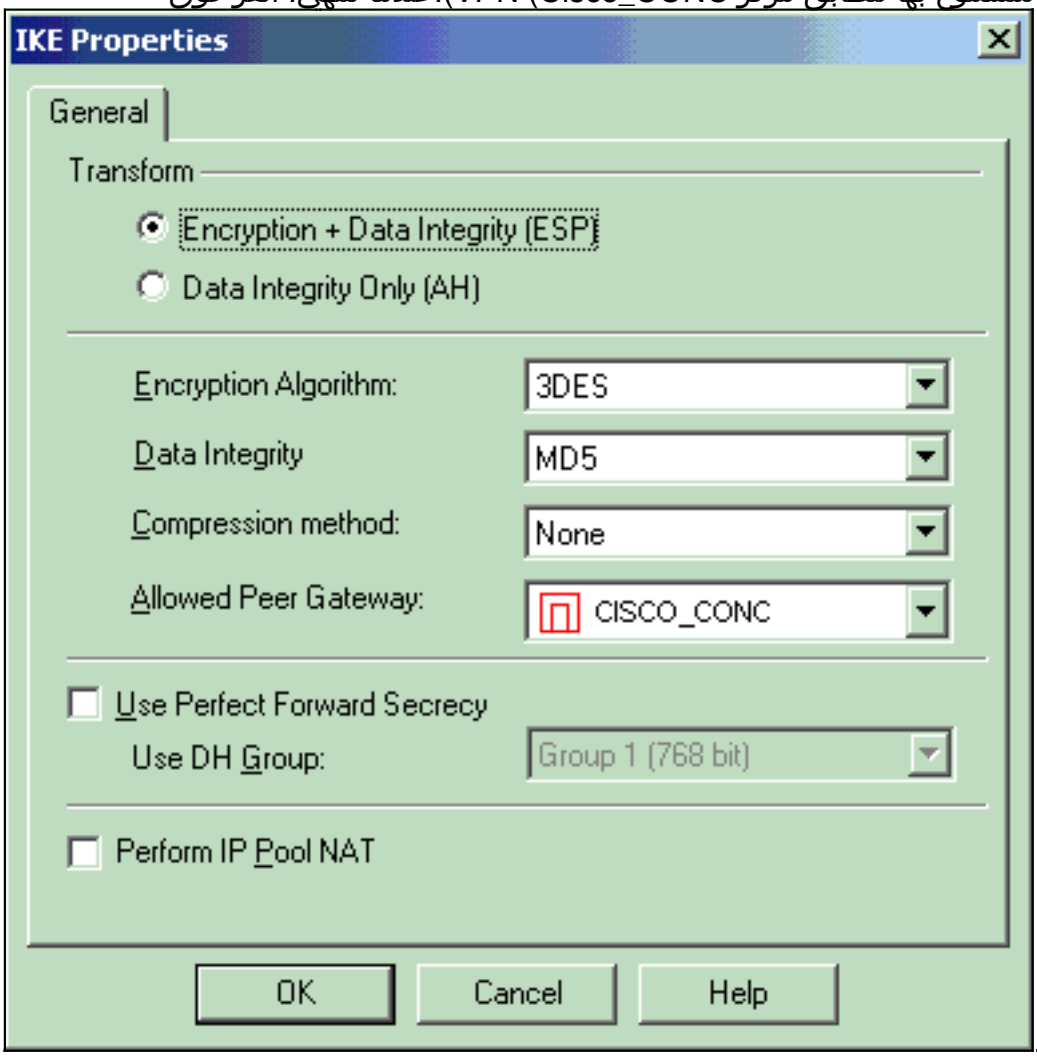
موافق.

15. حدد **قواعد > إضافة قواعد > أعلى** لتكوين قواعد التشفير للنهج. في نافذة "محرر النهج"، قم بإدراج قاعدة بمصدر على هيئة CP_Inside (داخل شبكة من NG لنقطة التفتيش) والوجهة على هيئة CONC_INSIDE (داخل الشبكة من مركز VPN). قم بتعيين قيم **للخدمة = أي**، **الإجراء = تشفير**، و**المسار = السجل**. عندما تقوم بإضافة قسم إجراء التشفير من القاعدة، انقر بزر الماوس الأيمن فوق **الإجراء** وحدد **تحرير الخصائص**.

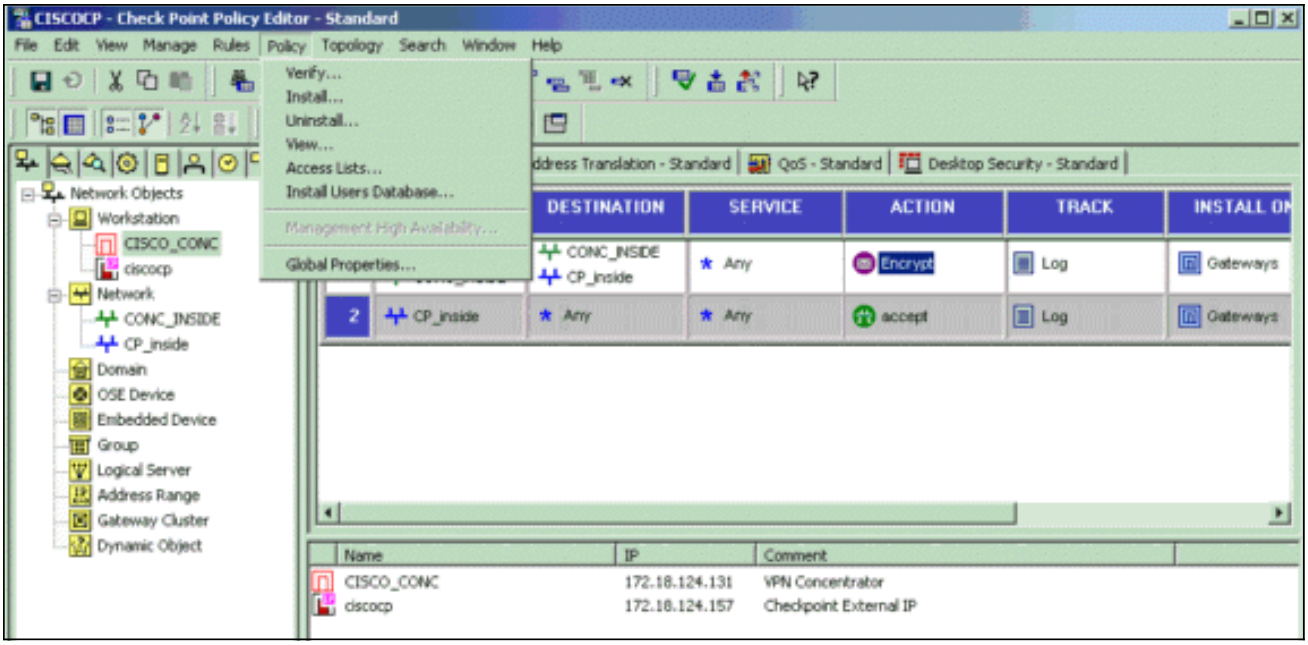




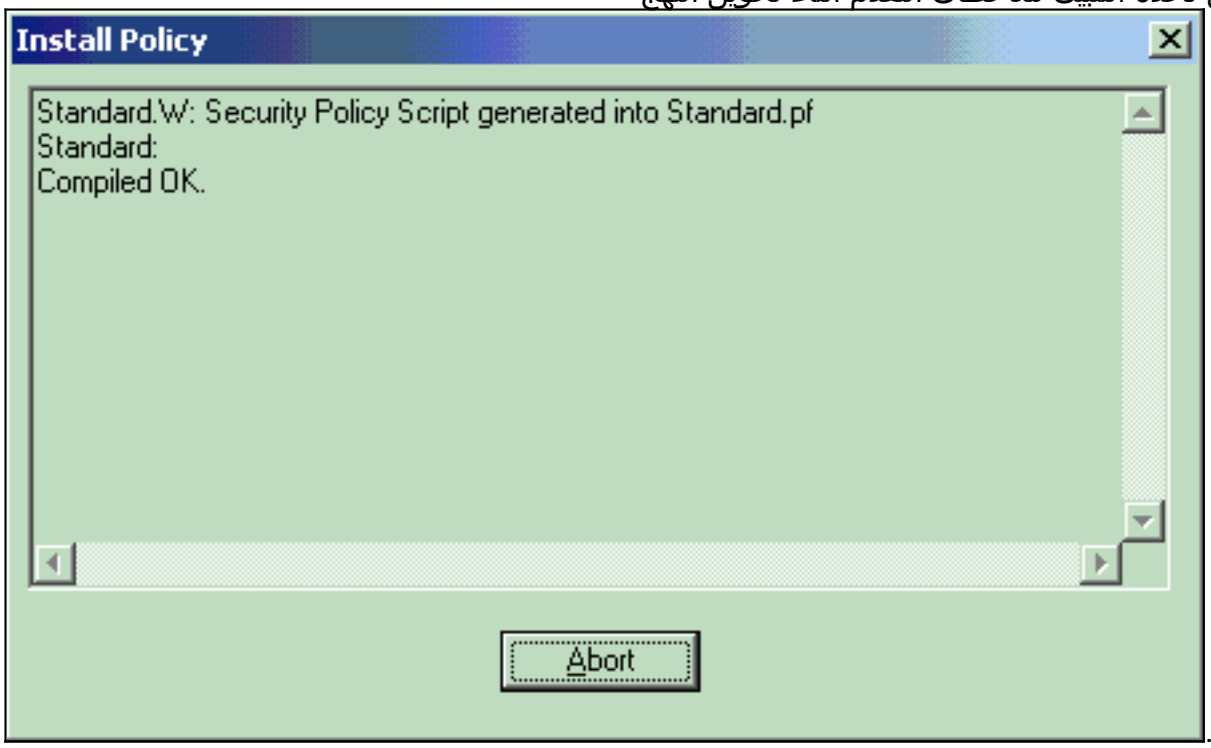
16. حدد **IKE** وانقر **تحرير**.
17. في نافذة خصائص IKE، قم بتغيير الخصائص لتوافق مع تحويل مركز VPN.اضبط خيار التحويل على **التشفير + تكامل البيانات (ESP)**.تعيين خوارزمية التشفير على **3DES**.تعيين تكامل البيانات على **MD5**.قم بتعيين بوابة النظير المسموح بها لتطابق مركز VPN (Cisco_CONC).عندما تنتهي، انقر فوق **موافق**.



18. بعد تكوين NG لنقطة التحقق، احفظ النهج وحدد **نهج > تثبيت** لتمكينه.

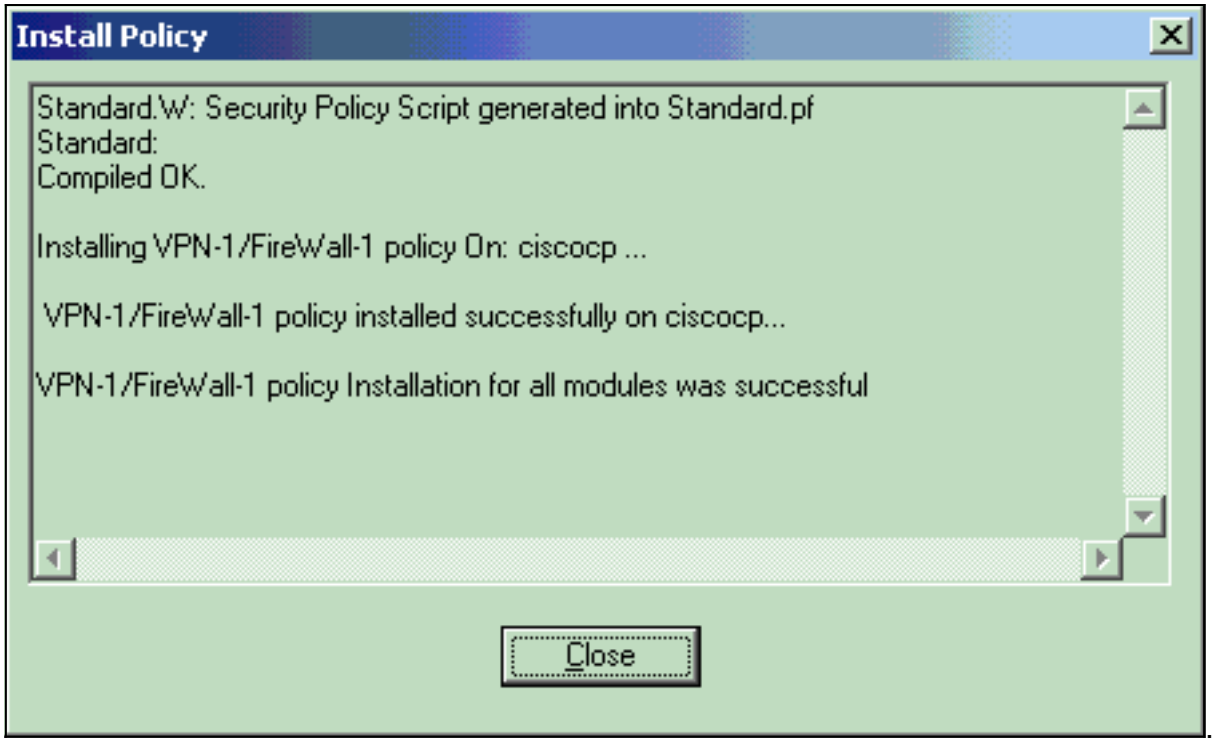


تعرض نافذة التثبيت ملاحظات التقدم أثناء تحويل النهج



برمجيا.

عندما تشير نافذة التثبيت إلى اكتمال تثبيت النهج، انقر فوق **إغلاق** لإنهاء



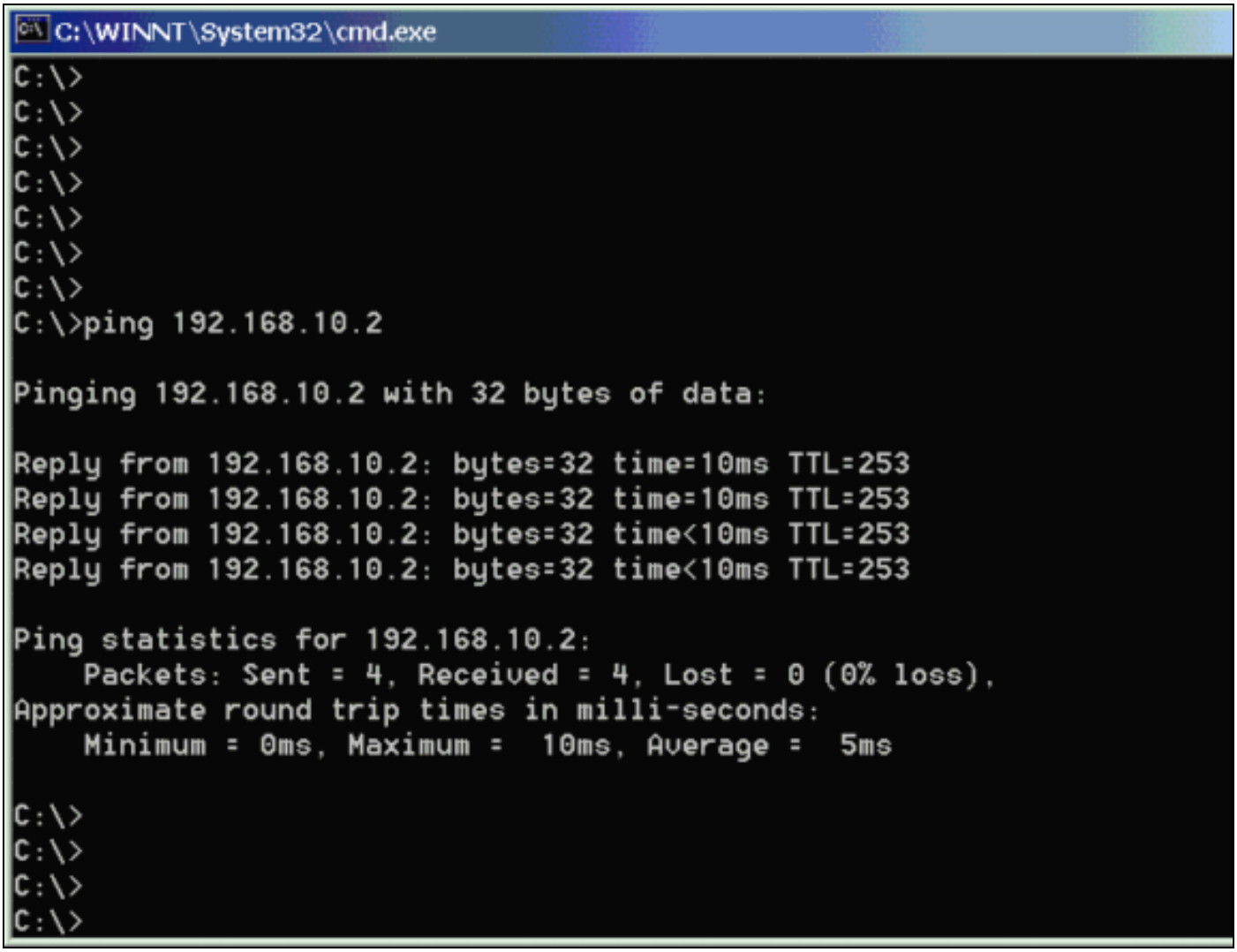
الإجراء.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

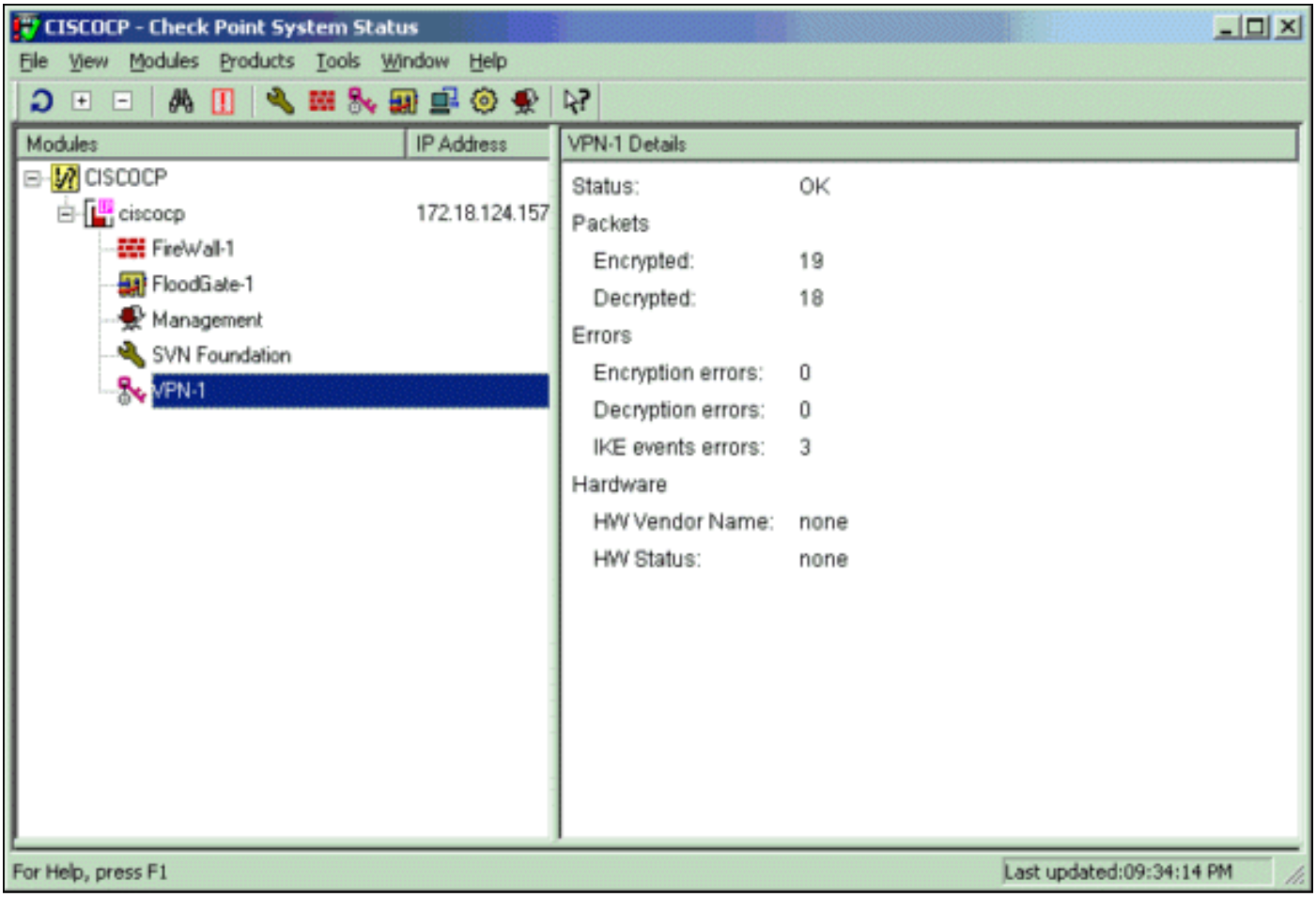
التحقق من اتصال الشبكة

لاختبار الاتصال بين الشبكتين الخاصتين، يمكنك بدء إختبار اتصال من إحدى الشبكات الخاصة إلى الشبكة الخاصة الأخرى. في هذا التكوين، تم إرسال إختبار اتصال من جانب NG في نقطة التفتيش (10.32.50.51) إلى شبكة مركز VPN (192.168.10.2).



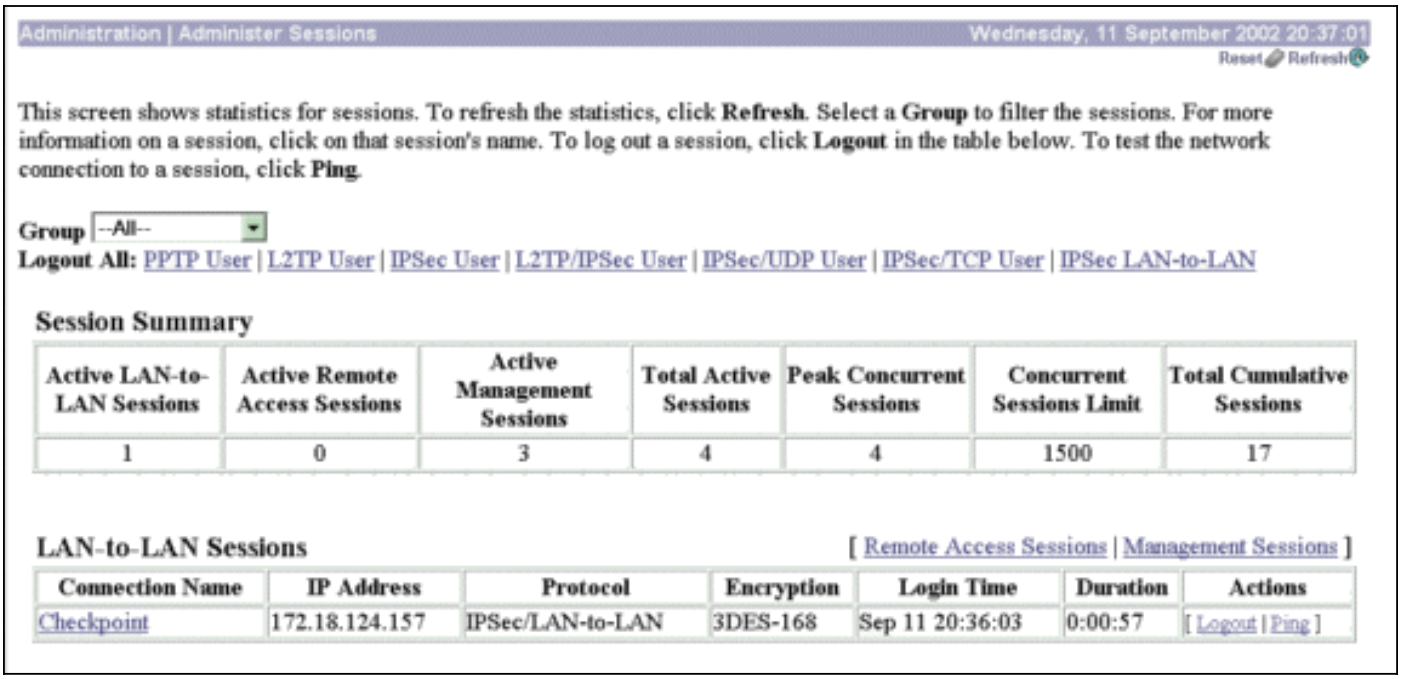
عرض حالة النفق على نقطة التفتيش NG

لعرض حالة النفق، انتقل إلى محرر النهج وحدد **نافذة > حالة النظام**.



عرض حالة النفق على مركز VPN

للتحقق من حالة النفق على مركز VPN، انتقل إلى **الإدارة > جلسات الإدارة**.



تحت جلسات عمل الشبكة المحلية (LAN) إلى الشبكة المحلية (LAN)، حدد اسم الاتصال لنقطة التفتيش لعرض التفاصيل حول شبكات SA التي تم إنشاؤها وعدد الحزم التي تم إرسالها/استقبالها.

Administration | Administer Sessions | Detail — Wednesday, 11 September 2002 20:37:59
Reset Refresh

Back to Sessions

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
Checkpoint	172.18.124.157	IPSec/LAN-to-LAN	3DES-168	Sep 11 20:36:03	0:01:55	256	256

IKE Sessions: 1
IPSec Sessions: 1

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**	10.32.0.0/0.0.127.255
Local Address	192.168.10.0/0.0.0.255	**Encryption Algorithm**	3DES-168
Hashing Algorithm	MD5	**SEP**	1
Encapsulation Mode	Tunnel	**Rekey Time Interval**	28800 seconds
Bytes Received	256	**Bytes Transmitted**	256

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

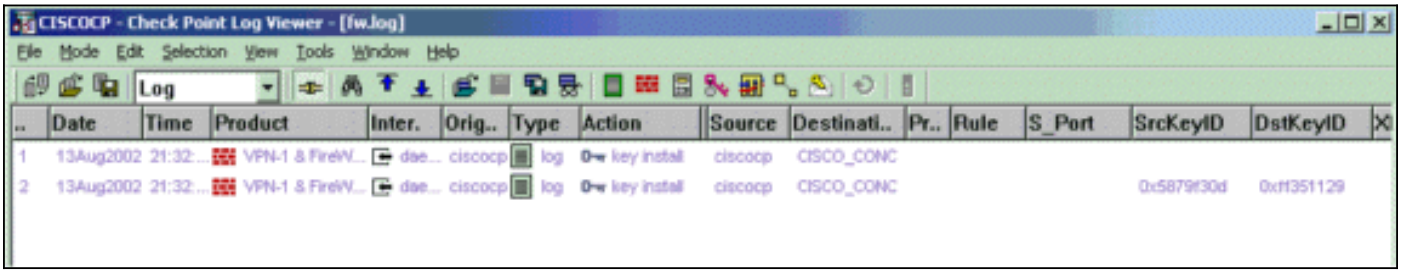
ملاحظة: يجب ألا يتم تحديد حركة المرور عبر نفق IPSec باستخدام عنوان IP العام لمركز بيانات الشبكة الخاصة الظاهرية (الواجهة الخارجية). وإلا فسيفشل النفق. لذلك، العنوان يستعمل ل PATing ينبغي كنت عنوان غير العنوان يشكل على القارن خارجي.

تلخيص الشبكة

عندما يتم تكوين شبكات متعددة متجاورة، داخل الشبكات في مجال التشفير على نقطة التحقق، يمكن للجهاز تلخيص الشبكات تلقائيا فيما يتعلق بحركة المرور المفيدة. إذا لم يتم تكوين مركز الشبكة الخاصة الظاهرية (VPN) ليتطابق، فمن المحتمل أن يفشل النفق. على سبيل المثال، إذا تم تكوين الشبكات الداخلية من 10.0.0.0 /24 و 10.0.1.0 /24 لتضمينها في النفق، فيمكن تلخيص هذه الشبكات إلى 10.0.0.0 /23.

تصحيح أخطاء NG لنقطة التفتيش

لعرض السجلات، حدد **نافذة > عارض السجل**.



تصحيح أخطاء مركز VPN

لتمكين تصحيح الأخطاء على مركز VPN، انتقل إلى **التكوين > النظام > الأحداث > الفئات**. قم بتمكين المصادقة و

authdbg و ike و ikedbg و IPSec و IPSECDBG من حيث الخطورة للتسجيل من 1 إلى 13. لعرض تصحيح الأخطاء، حدد **مراقبة > سجل أحداث قابل للتصفية**.

```
SEV=8 IKEDBG/0 RPT=506 172.18.124.157 20:36:03.610 09/11/2002 1
                        : RECEIVED Message (msgid=0) with payloads
   HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 128

SEV=9 IKEDBG/0 RPT=507 172.18.124.157 20:36:03.610 09/11/2002 3
                                            processing SA payload

                SEV=8 IKEDBG/0 RPT=508 20:36:03.610 09/11/2002 4
                Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
                                        :Parsing received transform
                :Phase 1 failure against global IKE proposal # 1
                    :Mismatched attr types for class Auth Method
                                            Rcv'd: Preshared Key
       (Cfg'd: XAUTH with Preshared Key (Initiator authenticated

               SEV=8 IKEDBG/0 RPT=509 20:36:03.610 09/11/2002 10
                :Phase 1 failure against global IKE proposal # 2
                       :Mismatched attr types for class DH Group
                                            Rcv'd: Oakley Group 2
                                            Cfg'd: Oakley Group 1

SEV=7 IKEDBG/0 RPT=510 172.18.124.157 20:36:03.610 09/11/2002 13
                                        Oakley proposal is acceptable

SEV=9 IKEDBG/47 RPT=9 172.18.124.157 20:36:03.610 09/11/2002 14
                                          processing VID payload

SEV=9 IKEDBG/0 RPT=511 172.18.124.157 20:36:03.610 09/11/2002 15
                                                processing IKE SA

               SEV=8 IKEDBG/0 RPT=512 20:36:03.610 09/11/2002 16
                Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
                                        :Parsing received transform
                :Phase 1 failure against global IKE proposal # 1
                    :Mismatched attr types for class Auth Method
                                            Rcv'd: Preshared Key
       (Cfg'd: XAUTH with Preshared Key (Initiator authenticated

               SEV=8 IKEDBG/0 RPT=513 20:36:03.610 09/11/2002 22
                :Phase 1 failure against global IKE proposal # 2
                       :Mismatched attr types for class DH Group
                                            Rcv'd: Oakley Group 2
                                            Cfg'd: Oakley Group 1

SEV=7 IKEDBG/28 RPT=9 172.18.124.157 20:36:03.610 09/11/2002 25
                    IKE SA Proposal # 1, Transform # 1 acceptable
                                    Matches global IKE entry # 3

SEV=9 IKEDBG/0 RPT=514 172.18.124.157 20:36:03.610 09/11/2002 26
                                        constructing ISA_SA for isakmp

SEV=8 IKEDBG/0 RPT=515 172.18.124.157 20:36:03.610 09/11/2002 27
                        : SENDING Message (msgid=0) with payloads
                   HDR + SA (1) + NONE (0) ... total length : 84

SEV=8 IKEDBG/0 RPT=516 172.18.124.157 20:36:03.630 09/11/2002 29
                        : RECEIVED Message (msgid=0) with payloads
     HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184
```

```
SEV=8 IKEDBG/0 RPT=517 172.18.124.157 20:36:03.630 09/11/2002 31
                          : RECEIVED Message (msgid=0) with payloads
     HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

SEV=9 IKEDBG/0 RPT=518 172.18.124.157 20:36:03.630 09/11/2002 33
                                                processing ke payload

SEV=9 IKEDBG/0 RPT=519 172.18.124.157 20:36:03.630 09/11/2002 34
                                                    processing ISA_KE

 SEV=9 IKEDBG/1 RPT=91 172.18.124.157 20:36:03.630 09/11/2002 35
                                               processing nonce payload

SEV=9 IKEDBG/0 RPT=520 172.18.124.157 20:36:03.660 09/11/2002 36
                                               constructing ke payload

 SEV=9 IKEDBG/1 RPT=92 172.18.124.157 20:36:03.660 09/11/2002 37
                                             constructing nonce payload

SEV=9 IKEDBG/46 RPT=37 172.18.124.157 20:36:03.660 09/11/2002 38
                                    constructing Cisco Unity VID payload

SEV=9 IKEDBG/46 RPT=38 172.18.124.157 20:36:03.660 09/11/2002 39
                                       constructing xauth V6 VID payload

SEV=9 IKEDBG/48 RPT=19 172.18.124.157 20:36:03.660 09/11/2002 40
                                                        Send IOS VID

SEV=9 IKEDBG/38 RPT=10 172.18.124.157 20:36:03.660 09/11/2002 41
,Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0
                                               (capabilities: 20000001

SEV=9 IKEDBG/46 RPT=39 172.18.124.157 20:36:03.660 09/11/2002 43
                                               constructing VID payload

SEV=9 IKEDBG/48 RPT=20 172.18.124.157 20:36:03.660 09/11/2002 44
                                                    Send Altiga GW VID

SEV=9 IKEDBG/0 RPT=521 172.18.124.157 20:36:03.660 09/11/2002 45
                                       ...Generating keys for Responder

SEV=8 IKEDBG/0 RPT=522 172.18.124.157 20:36:03.670 09/11/2002 46
                          : SENDING Message (msgid=0) with payloads
                  HDR + KE (4) + NONCE (10) ... total length : 256

SEV=8 IKEDBG/0 RPT=523 172.18.124.157 20:36:03.690 09/11/2002 48
                          : RECEIVED Message (msgid=0) with payloads
        HDR + ID (5) + HASH (8) + NONE (0) ... total length : 60

 SEV=9 IKEDBG/1 RPT=93 172.18.124.157 20:36:03.690 09/11/2002 50
                                                   [Group [172.18.124.157
                                                     Processing ID

SEV=9 IKEDBG/0 RPT=524 172.18.124.157 20:36:03.690 09/11/2002 51
                                                   [Group [172.18.124.157
                                                    processing hash

SEV=9 IKEDBG/0 RPT=525 172.18.124.157 20:36:03.690 09/11/2002 52
                                                   [Group [172.18.124.157
                                                    computing hash

SEV=9 IKEDBG/23 RPT=10 172.18.124.157 20:36:03.690 09/11/2002 53
                                                   [Group [172.18.124.157
                          Starting group lookup for peer 172.18.124.157
```

```
                                    SEV=8 AUTHDBG/1 RPT=10 20:36:03.690 09/11/2002 54
                                                          AUTH_Open() returns 9

                                      SEV=7 AUTH/12 RPT=10 20:36:03.690 09/11/2002 55
                                            Authentication session opened: handle = 9

                                    SEV=8 AUTHDBG/3 RPT=10 20:36:03.690 09/11/2002 56
                                                     (AUTH_PutAttrTable(9, 748174

                                    SEV=8 AUTHDBG/6 RPT=10 20:36:03.690 09/11/2002 57
                                             (AUTH_GroupAuthenticate(9, 2f1b19c, 49c648

                                   SEV=8 AUTHDBG/59 RPT=10 20:36:03.690 09/11/2002 58
                                                     (AUTH_BindServer(51a6b48, 0, 0

                                   SEV=9 AUTHDBG/69 RPT=10 20:36:03.690 09/11/2002 59
                          Auth Server e054d4 has been bound to ACB 51a6b48, sessions = 1

                                   SEV=8 AUTHDBG/65 RPT=10 20:36:03.690 09/11/2002 60
                                                    (AUTH_CreateTimer(51a6b48, 0, 0

                                   SEV=9 AUTHDBG/72 RPT=10 20:36:03.690 09/11/2002 61
                                                Reply timer created: handle = 4B0018

                                   SEV=8 AUTHDBG/61 RPT=10 20:36:03.690 09/11/2002 62
                                                     (AUTH_BuildMsg(51a6b48, 0, 0

                                   SEV=8 AUTHDBG/64 RPT=10 20:36:03.690 09/11/2002 63
                                                     (AUTH_StartTimer(51a6b48, 0, 0

                                   SEV=9 AUTHDBG/73 RPT=10 20:36:03.690 09/11/2002 64
                        ,Reply timer started: handle = 4B0018, timestamp = 1163319
                                                                    timeout = 30000

                                   SEV=8 AUTHDBG/62 RPT=10 20:36:03.690 09/11/2002 65
                                                     (AUTH_SndRequest(51a6b48, 0, 0

                                   SEV=8 AUTHDBG/50 RPT=19 20:36:03.690 09/11/2002 66
                                                       (IntDB_Decode(3825300, 156

                                   SEV=8 AUTHDBG/47 RPT=19 20:36:03.690 09/11/2002 67
                                                            (IntDB_Xmt(51a6b48

                                   SEV=9 AUTHDBG/71 RPT=10 20:36:03.690 09/11/2002 68
                                                                  xmit_cnt = 1

                                   SEV=8 AUTHDBG/47 RPT=20 20:36:03.690 09/11/2002 69
                                                            (IntDB_Xmt(51a6b48

                                   SEV=8 AUTHDBG/49 RPT=10 20:36:03.790 09/11/2002 70
                                                     (IntDB_Match(51a6b48, 3eb7ab0

                                   SEV=8 AUTHDBG/63 RPT=10 20:36:03.790 09/11/2002 71
                                                     (AUTH_RcvReply(51a6b48, 0, 0

                                   SEV=8 AUTHDBG/50 RPT=20 20:36:03.790 09/11/2002 72
                                                       (IntDB_Decode(3eb7ab0, 298

                                   SEV=8 AUTHDBG/48 RPT=10 20:36:03.790 09/11/2002 73
                                                            (IntDB_Rcv(51a6b48

                                   SEV=8 AUTHDBG/66 RPT=10 20:36:03.790 09/11/2002 74
                                                    (AUTH_DeleteTimer(51a6b48, 0, 0
```

```
                SEV=9 AUTHDBG/74 RPT=10 20:36:03.790 09/11/2002 75
      Reply timer stopped: handle = 4B0018, timestamp = 1163329

                SEV=8 AUTHDBG/58 RPT=10 20:36:03.790 09/11/2002 76
                                      (AUTH_Callback(51a6b48, 0, 0

  SEV=6 AUTH/41 RPT=10 172.18.124.157 20:36:03.790 09/11/2002 77
       ,Authentication successful: handle = 9, server = Internal
                                    group = 172.18.124.157

SEV=7 IKEDBG/0 RPT=526 172.18.124.157 20:36:03.790 09/11/2002 78
                                    [Group [172.18.124.157
                          (Found Phase 1 Group (172.18.124.157

                SEV=8 AUTHDBG/4 RPT=10 20:36:03.790 09/11/2002 79
                                      (AUTH_GetAttrTable(9, 748420

SEV=7 IKEDBG/14 RPT=10 172.18.124.157 20:36:03.790 09/11/2002 80
                                    [Group [172.18.124.157
                        Authentication configured for Internal

SEV=9 IKEDBG/19 RPT=19 172.18.124.157 20:36:03.790 09/11/2002 81
                                    [Group [172.18.124.157
                  IKEGetUserAttributes: IP Compression = disabled

SEV=9 IKEDBG/19 RPT=20 172.18.124.157 20:36:03.790 09/11/2002 82
                                    [Group [172.18.124.157
          IKEGetUserAttributes: Split Tunneling Policy = Disabled

                SEV=8 AUTHDBG/2 RPT=10 20:36:03.790 09/11/2002 83
                                        (AUTH_Close(9

 SEV=9 IKEDBG/1 RPT=94 172.18.124.157 20:36:03.790 09/11/2002 84
                                    [Group [172.18.124.157
                                      constructing ID

                SEV=9 IKEDBG/0 RPT=527 20:36:03.790 09/11/2002 85
                                    [Group [172.18.124.157
                                    construct hash payload

SEV=9 IKEDBG/0 RPT=528 172.18.124.157 20:36:03.790 09/11/2002 86
                                    [Group [172.18.124.157
                                      computing hash

SEV=9 IKEDBG/46 RPT=40 172.18.124.157 20:36:03.790 09/11/2002 87
                                    [Group [172.18.124.157
                                constructing dpd vid payload

SEV=8 IKEDBG/0 RPT=529 172.18.124.157 20:36:03.790 09/11/2002 88
                          : SENDING Message (msgid=0) with payloads
                    HDR + ID (5) + HASH (8) ... total length : 80

  SEV=4 IKE/119 RPT=10 172.18.124.157 20:36:03.790 09/11/2002 90
                                    [Group [172.18.124.157
                                         PHASE 1 COMPLETED

  SEV=6 IKE/121 RPT=10 172.18.124.157 20:36:03.790 09/11/2002 91
                        Keep-alive type for this connection: None

  SEV=6 IKE/122 RPT=10 172.18.124.157 20:36:03.790 09/11/2002 92
                      Keep-alives configured on but peer does not
                                (support keep-alives (type = None
```

```
SEV=7 IKEDBG/0 RPT=530 172.18.124.157 20:36:03.790 09/11/2002 93
                                                [Group [172.18.124.157
                          (Starting phase 1 rekey timer: 64800000 (ms

                     SEV=4 AUTH/22 RPT=16 20:36:03.790 09/11/2002 94
                                     User 172.18.124.157 connected

                   SEV=8 AUTHDBG/60 RPT=10 20:36:03.790 09/11/2002 95
                                    (AUTH_UnbindServer(51a6b48, 0, 0

                   SEV=9 AUTHDBG/70 RPT=10 20:36:03.790 09/11/2002 96
Auth Server e054d4 has been unbound from ACB 51a6b48, sessions = 0

                   SEV=8 AUTHDBG/10 RPT=10 20:36:03.790 09/11/2002 97
                                    (AUTH_Int_FreeAuthCB(51a6b48

                     SEV=7 AUTH/13 RPT=10 20:36:03.790 09/11/2002 98
                           Authentication session closed: handle = 9

 SEV=8 IKEDBG/0 RPT=531 172.18.124.157 20:36:03.790 09/11/2002 99
                : RECEIVED Message (msgid=54796f76) with payloads
(HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0
                                                total length : 156 ...

SEV=9 IKEDBG/0 RPT=532 172.18.124.157 20:36:03.790 09/11/2002 102
                                                [Group [172.18.124.157
                                                       processing hash

SEV=9 IKEDBG/0 RPT=533 172.18.124.157 20:36:03.790 09/11/2002 103
                                                [Group [172.18.124.157
                                                 processing SA payload

 SEV=9 IKEDBG/1 RPT=95 172.18.124.157 20:36:03.790 09/11/2002 104
                                                [Group [172.18.124.157
                                              processing nonce payload

 SEV=9 IKEDBG/1 RPT=96 172.18.124.157 20:36:03.790 09/11/2002 105
                                                [Group [172.18.124.157
                                                         Processing ID

    SEV=5 IKE/35 RPT=6 172.18.124.157 20:36:03.790 09/11/2002 106
                                                [Group [172.18.124.157
                    :Received remote IP Proxy Subnet data in ID Payload
        Address 10.32.0.0, Mask 255.255.128.0, Protocol 0, Port 0

 SEV=9 IKEDBG/1 RPT=97 172.18.124.157 20:36:03.790 09/11/2002 109
                                                [Group [172.18.124.157
                                                         Processing ID

    SEV=5 IKE/34 RPT=6 172.18.124.157 20:36:03.790 09/11/2002 110
                                                [Group [172.18.124.157
                    :Received local IP Proxy Subnet data in ID Payload
     Address 192.168.10.0, Mask 255.255.255.0, Protocol 0, Port 0

                SEV=8 IKEDBG/0 RPT=534 20:36:03.790 09/11/2002 113
                                 QM IsRekeyed old sa not found by addr

    SEV=5 IKE/66 RPT=8 172.18.124.157 20:36:03.790 09/11/2002 114
                                                [Group [172.18.124.157
                IKE Remote Peer configured for SA: L2L: Checkpoint

SEV=9 IKEDBG/0 RPT=535 172.18.124.157 20:36:03.790 09/11/2002 115
                                                [Group [172.18.124.157
                                                   processing IPSEC SA
```

SEV=7 IKEDBG/27 RPT=8 172.18.124.157 20:36:03.790 09/11/2002 116
[Group [172.18.124.157
IPSec SA Proposal # 1, Transform # 1 acceptable

SEV=7 IKEDBG/0 RPT=536 172.18.124.157 20:36:03.790 09/11/2002 117
[Group [172.18.124.157
!IKE: requesting SPI

SEV=9 IPSECDBG/6 RPT=39 20:36:03.790 09/11/2002 118
,IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000
,seq 10, err 0, type 2, mode 0, state 32, label 0, pad 0
,spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0
lifetype 0, lifetime1 17248580, lifetime2 0, dsId 300

SEV=9 IPSECDBG/1 RPT=139 20:36:03.790 09/11/2002 122
!Processing KEY_GETSPI msg

SEV=7 IPSECDBG/13 RPT=10 20:36:03.790 09/11/2002 123
Reserved SPI 305440147

SEV=8 IKEDBG/6 RPT=10 20:36:03.790 09/11/2002 124
IKE got SPI from key engine: SPI = 0x1234a593

SEV=9 IKEDBG/0 RPT=537 172.18.124.157 20:36:03.790 09/11/2002 125
[Group [172.18.124.157
oakley constucting quick mode

SEV=9 IKEDBG/0 RPT=538 172.18.124.157 20:36:03.800 09/11/2002 126
[Group [172.18.124.157
constructing blank hash

SEV=9 IKEDBG/0 RPT=539 172.18.124.157 20:36:03.800 09/11/2002 127
[Group [172.18.124.157
constructing ISA_SA for ipsec

SEV=9 IKEDBG/1 RPT=98 172.18.124.157 20:36:03.800 09/11/2002 128
[Group [172.18.124.157
constructing ipsec nonce payload

SEV=9 IKEDBG/1 RPT=99 172.18.124.157 20:36:03.800 09/11/2002 129
[Group [172.18.124.157
constructing proxy ID

SEV=7 IKEDBG/0 RPT=540 172.18.124.157 20:36:03.800 09/11/2002 130
[Group [172.18.124.157
:Transmitting Proxy Id
Remote subnet: 10.32.0.0 Mask 255.255.128.0 Protocol 0 Port 0
Local subnet: 192.168.10.0 mask 255.255.255.0 Protocol 0 Port 0

SEV=9 IKEDBG/0 RPT=541 172.18.124.157 20:36:03.800 09/11/2002 134
[Group [172.18.124.157
constructing qm hash

SEV=8 IKEDBG/0 RPT=542 172.18.124.157 20:36:03.800 09/11/2002 135
: SENDING Message (msgid=54796f76) with payloads
HDR + HASH (8) + SA (1) ... total length : 152

SEV=8 IKEDBG/0 RPT=543 172.18.124.157 20:36:03.800 09/11/2002 137
: RECEIVED Message (msgid=54796f76) with payloads
HDR + HASH (8) + NONE (0) ... total length : 48

SEV=9 IKEDBG/0 RPT=544 172.18.124.157 20:36:03.800 09/11/2002 139
[Group [172.18.124.157

```
                                                                processing hash

     SEV=9 IKEDBG/0 RPT=545 172.18.124.157 20:36:03.800 09/11/2002 140
                                                        [Group [172.18.124.157
                                                         loading all IPSEC SAs

     SEV=9 IKEDBG/1 RPT=100 172.18.124.157 20:36:03.800 09/11/2002 141
                                                        [Group [172.18.124.157
                                                    !Generating Quick Mode Key

     SEV=9 IKEDBG/1 RPT=101 172.18.124.157 20:36:03.800 09/11/2002 142
                                                        [Group [172.18.124.157
                                                    !Generating Quick Mode Key

     SEV=7 IKEDBG/0 RPT=546 172.18.124.157 20:36:03.800 09/11/2002 143
                                                        [Group [172.18.124.157
                                                               :Loading subnet
                                          Dst: 192.168.10.0 mask: 255.255.255.0
                                            Src: 10.32.0.0 mask: 255.255.128.0

          SEV=4 IKE/49 RPT=7 172.18.124.157 20:36:03.800 09/11/2002 146
                                                        [Group [172.18.124.157
   (Security negotiation complete for LAN-to-LAN Group (172.18.124.157
        Responder, Inbound SPI = 0x1234a593, Outbound SPI = 0x0df37959

                         SEV=9 IPSECDBG/6 RPT=40 20:36:03.800 09/11/2002 149
   ,IPSEC key message parse - msgtype 1, len 606, vers 1, pid 00000000
                ,seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0
,spi 0df37959, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3
                         lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0

                        SEV=9 IPSECDBG/1 RPT=140 20:36:03.800 09/11/2002 153
                                                    !Processing KEY_ADD msg

                        SEV=9 IPSECDBG/1 RPT=141 20:36:03.800 09/11/2002 154
                                              key_msghdr2secassoc(): Enter

                        SEV=7 IPSECDBG/1 RPT=142 20:36:03.800 09/11/2002 155
                                                No USER filter configured

                        SEV=9 IPSECDBG/1 RPT=143 20:36:03.800 09/11/2002 156
                                                   KeyProcessAdd: Enter

                        SEV=8 IPSECDBG/1 RPT=144 20:36:03.800 09/11/2002 157
                                           KeyProcessAdd: Adding outbound SA

                        SEV=8 IPSECDBG/1 RPT=145 20:36:03.800 09/11/2002 158
                             ,KeyProcessAdd: src 192.168.10.0 mask 0.0.0.255
                                           dst 10.32.0.0 mask 0.0.127.255

                        SEV=8 IPSECDBG/1 RPT=146 20:36:03.810 09/11/2002 159
                                     KeyProcessAdd: FilterIpsecAddIkeSa success

                         SEV=9 IPSECDBG/6 RPT=41 20:36:03.810 09/11/2002 160
   ,IPSEC key message parse - msgtype 3, len 327, vers 1, pid 00000000
                ,seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0
,spi 1234a593, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3
                         lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0

                        SEV=9 IPSECDBG/1 RPT=147 20:36:03.810 09/11/2002 164
                                                    !Processing KEY_UPDATE msg

                        SEV=9 IPSECDBG/1 RPT=148 20:36:03.810 09/11/2002 165
                                                  Update inbound SA addresses
```

```
SEV=9 IPSECDBG/1 RPT=149 20:36:03.810 09/11/2002 166
                                key_msghdr2secassoc(): Enter

SEV=7 IPSECDBG/1 RPT=150 20:36:03.810 09/11/2002 167
                                No USER filter configured

SEV=9 IPSECDBG/1 RPT=151 20:36:03.810 09/11/2002 168
                                    KeyProcessUpdate: Enter

SEV=8 IPSECDBG/1 RPT=152 20:36:03.810 09/11/2002 169
                                KeyProcessUpdate: success

    SEV=8 IKEDBG/7 RPT=7 20:36:03.810 09/11/2002 170
      IKE got a KEY_ADD msg for SA: SPI = 0x0df37959

  SEV=8 IKEDBG/0 RPT=547 20:36:03.810 09/11/2002 171
            pitcher: rcv KEY_UPDATE, spi 0x1234a593

SEV=4 IKE/120 RPT=7 172.18.124.157 20:36:03.810 09/11/2002 172
                                        [Group [172.18.124.157
                                (PHASE 2 COMPLETED (msgid=54796f76
```

معلومات ذات صلة

- صفحة دعم مركز Cisco VPN 3000 Series
- صفحة دعم عميل Cisco VPN 3000 Series
- صفحة دعم IPSec
- الدعم الفني - 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).