تكوين نفق IPsec - مركز VPN 5000 من Cisco إلى جدار حماية 4.1 لنقطة الوصول

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين نفق IPsec بمفاتيح مشتركة مسبقا للانضمام إلى شبكتين خاصتين. وهو ينضم إلى شبكة خاصة داخل مركز Cisco VPN 5000 (192.168.1.x) إلى شبكة خاصة داخل جدار حماية نقطة التفتيش 4.1 (x.10.32.50). يفترض أن حركة المرور من داخل مركز الشبكة الخاصة الظاهرية (VPN) وداخل نقطة التفتيش إلى الإنترنت (ممثلة في هذا المستند بشبكات x.172.18.124) تتدفق قبل أن تبدأ هذا التكوين.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- مركز Cisco VPN 5000
- برنامج مركز Cisco VPN 5000 نسخة 5.2.19.0001

- جدار حماية نقطة التفتيش 4.1

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.

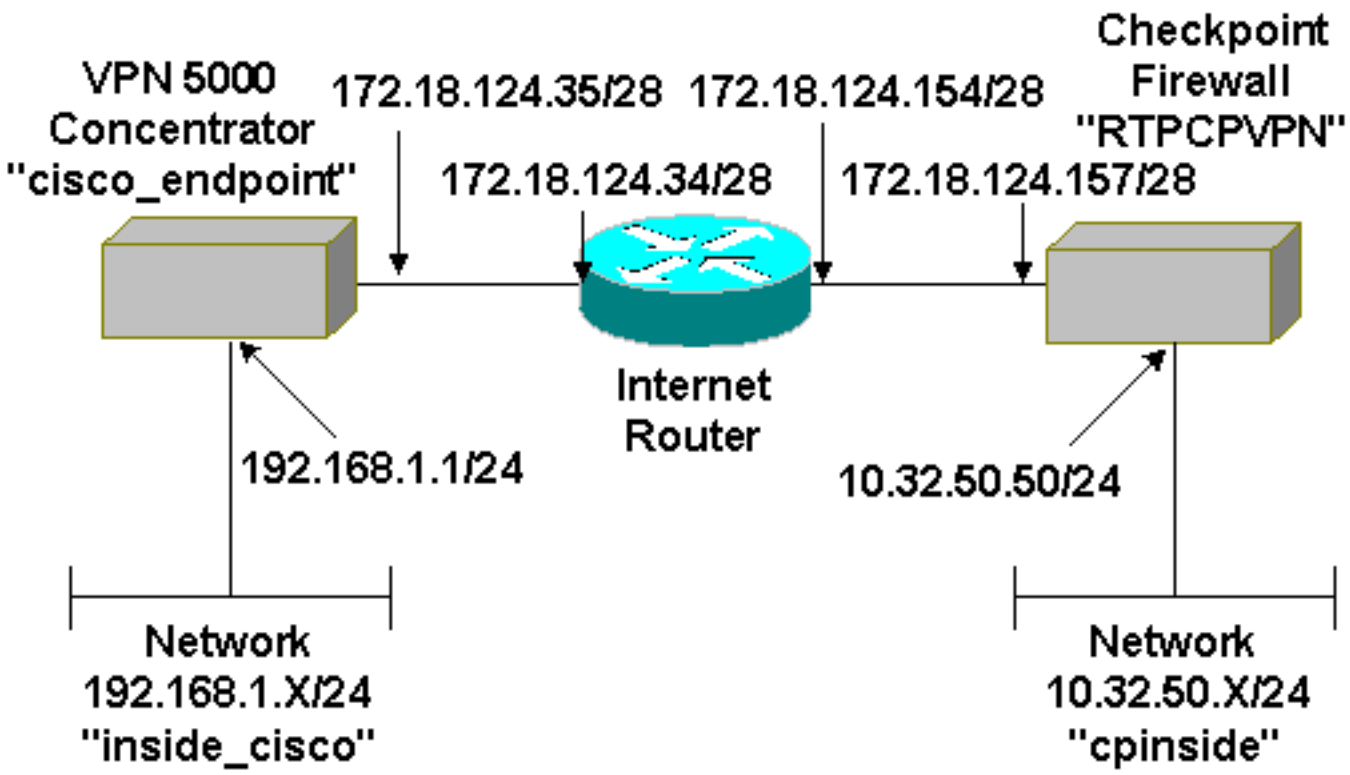
التكوين

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

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) 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.

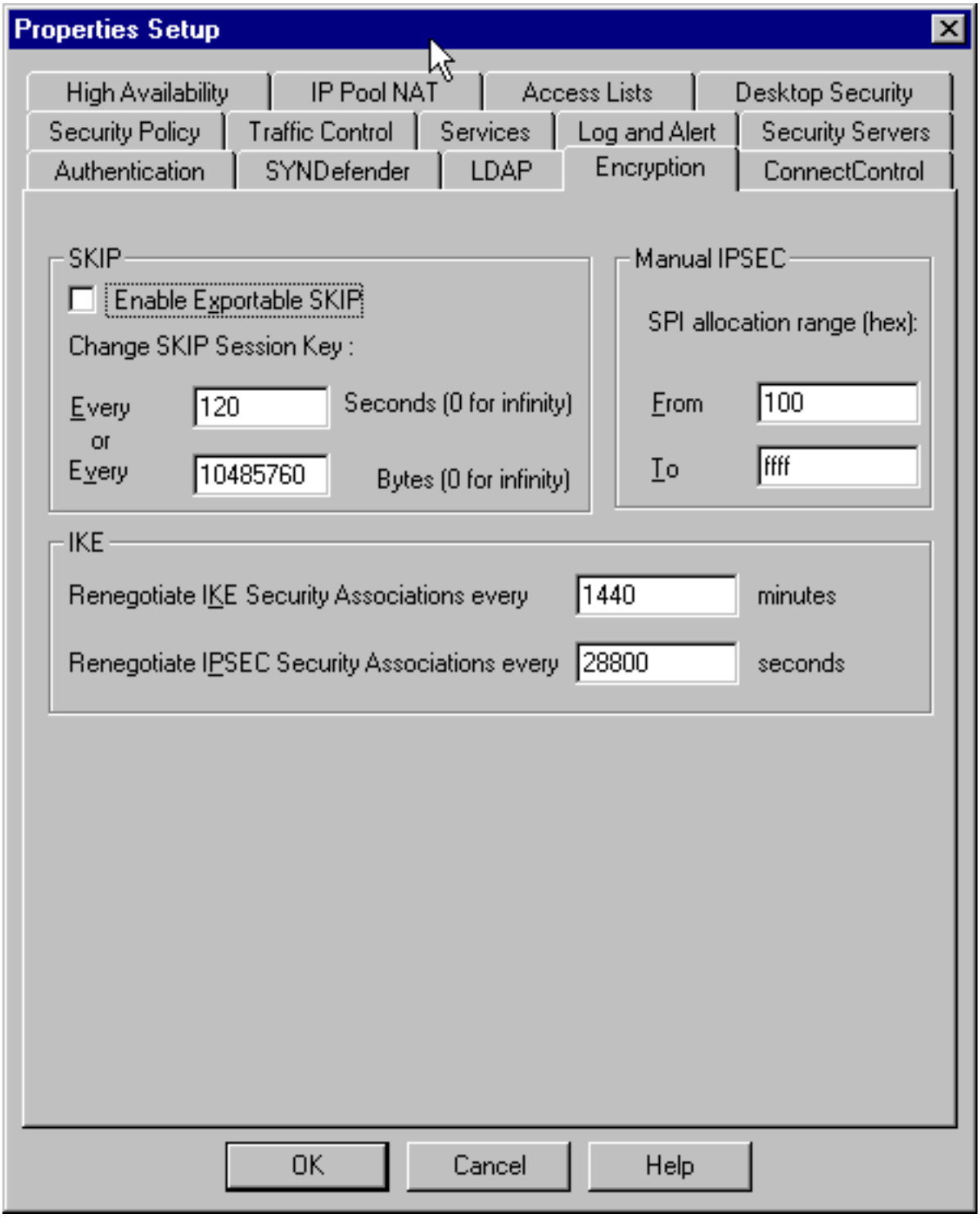
مركز Cisco VPN 5000
[IP Ethernet 0:0] Mode = Routed SubnetMask = 255.255.255.0

```
                IPAddress                = 192.168.1.1

                                                [ General ]
        EthernetAddress          = 00:00:a5:e9:c8:00
   DeviceType               = VPN 5002/8 Concentrator
 ConfiguredOn             = Timeserver not configured
ConfiguredFrom           = Command Line, from Console
         "DeviceName               = "cisco_endpoint
            IPSecGateway             = 172.18.124.34

                                             [ IKE Policy ]
              Protection               = SHA_DES_G2

                                  [ Tunnel Partner VPN 1 ]
                    KeyLifeSecs              = 28800
          "LocalAccess             = "192.168.1.0/24
           "Peer                    = "10.32.50.0/24
            "BindTo                  = "ethernet 1:0
              "SharedKey               = "ciscorules
                       KeyManage               = Auto
              (Transform               = esp(sha,des
            Partner                  = 172.18.124.157
                      Mode                    = Main

                                          [ IP VPN 1 ]
                 Numbered                 = Off
               Mode                     = Routed

                                     [ IP Ethernet 1:0 ]
          IPAddress                = 172.18.124.35
        SubnetMask               = 255.255.255.240
                  Mode                     = Routed

                                        [ IP Static ]
                VPN 1 1 255.255.255.0 10.32.50.0

        .Configuration size is 1131 out of 65500 bytes
```

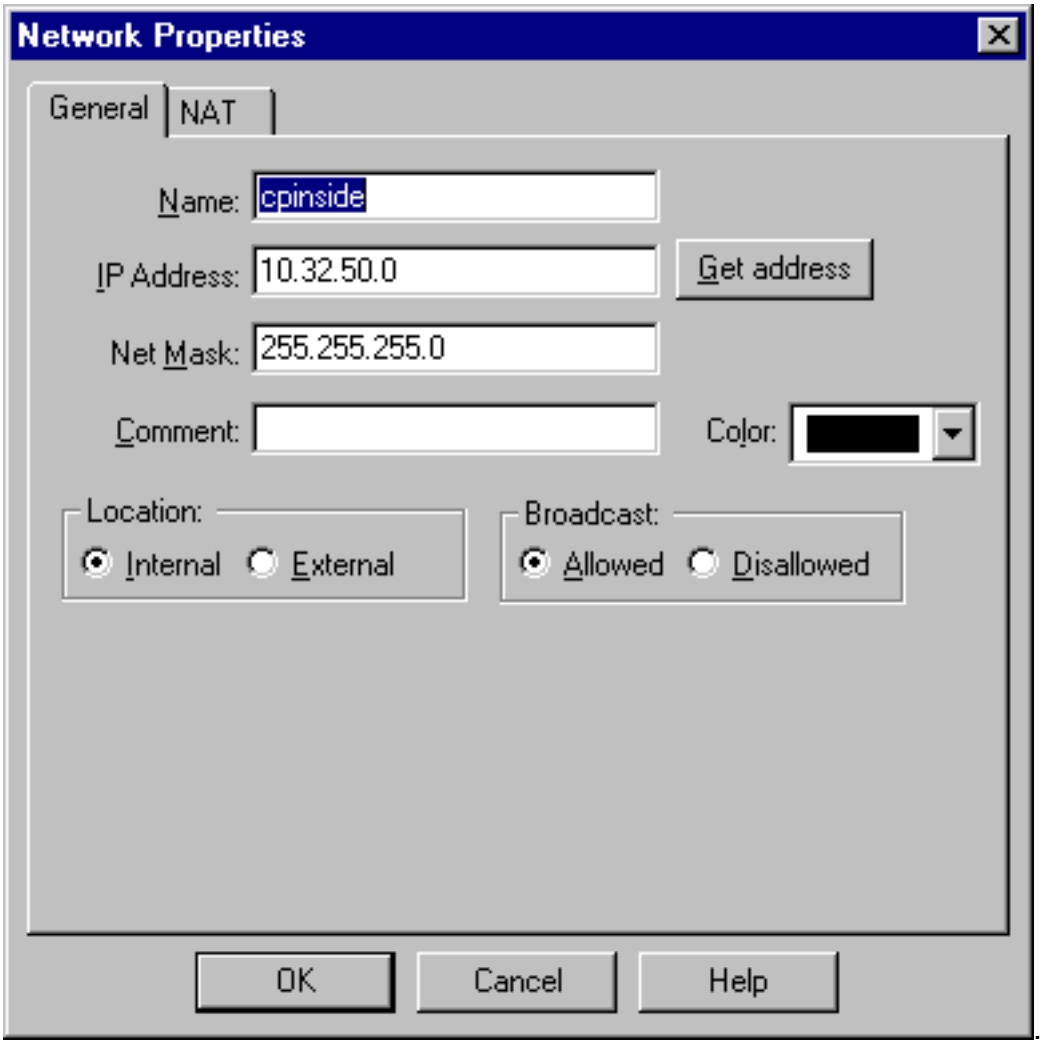
جدار حماية نقطة التفتيش 4.1

أكمل الخطوات التالية لتكوين جدار حماية نقطة الوصول 4.1.

1. حدد **خصائص > تشفير** لتعيين فترات حياة IPsec لنقطة التحقق للاتفاق مع **KeyLifeSeconds = 28800** أمر مركز VPN.**ملاحظة:** أترك نقاط التفتيش فترات حياة تبادل مفاتيح الإنترنت (IKE) في الوضع الافتراضي.

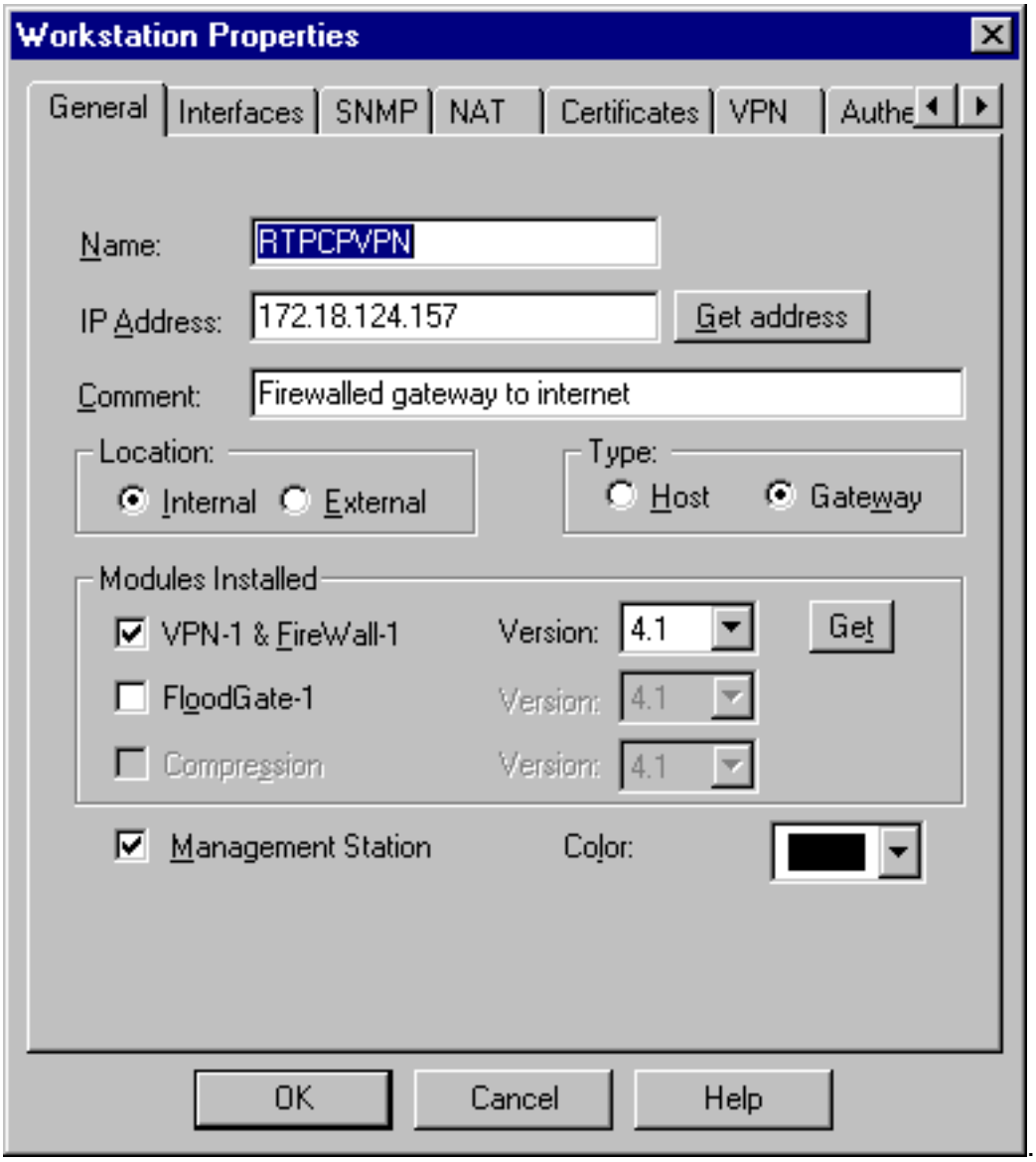


2. حدد **إدارة > كائنات الشبكة > جديد (أو تحرير) > الشبكة** لتكوين الكائن للشبكة الداخلية ("CPINSIDE") خلف نقطة التفتيش. يجب أن يتوافق هذا مع **النظير =** أمر **مركز** الشبكة الخاصة الظاهرية ((VPN



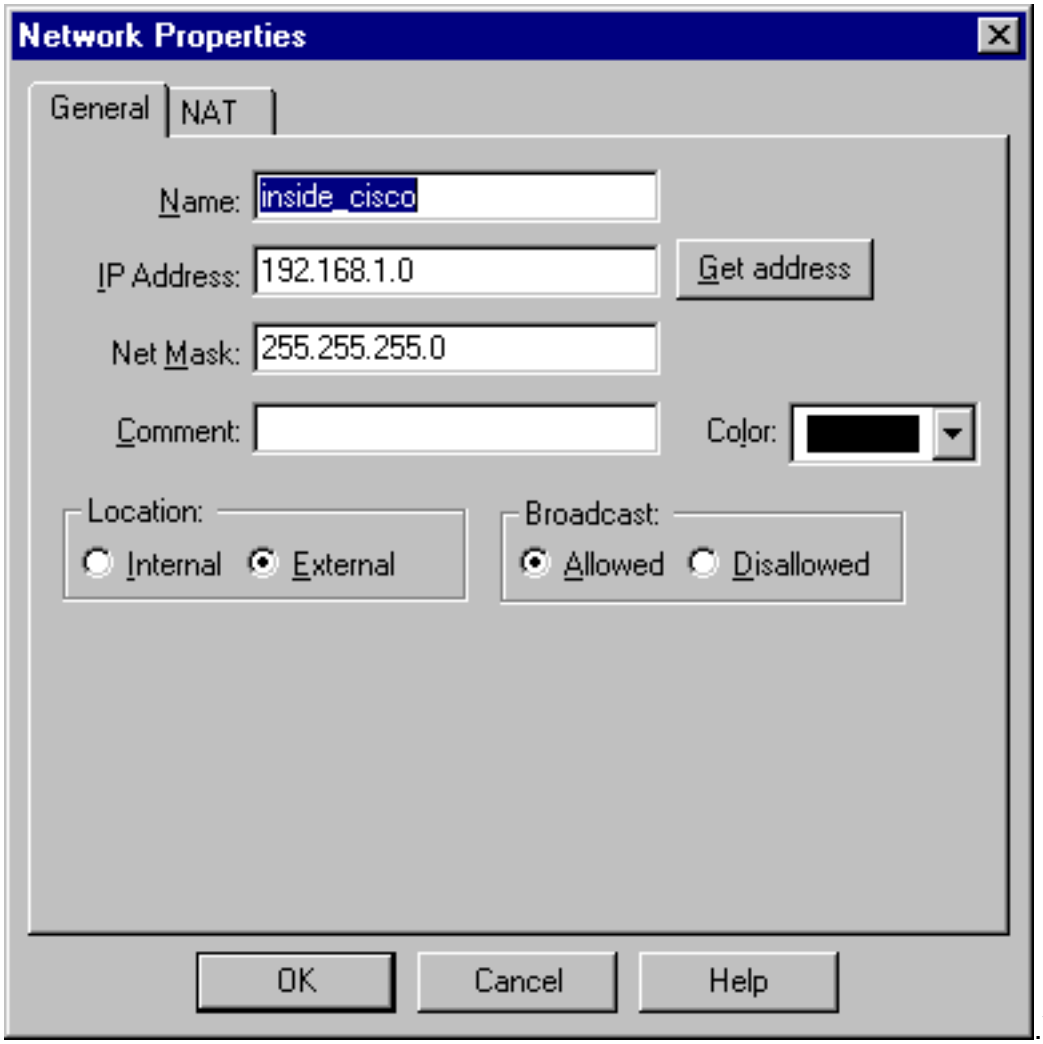
10.32.50.0/24"".

3. حدد **إدارة > كائنات الشبكة > تحرير** لتحرير الكائن لنقطة نهاية العبارة ("نقطة تفتيش RTPCPVPN") التي يشير إليها مركز VPN في الأمر **ip> = partner<**.حدد **داخلي** أسفل الموقع.حدد **عبارة** للنوع.تحقق من **VPN-1 و FireWALL-1** و**محطة الإدارة** ضمن الوحدات



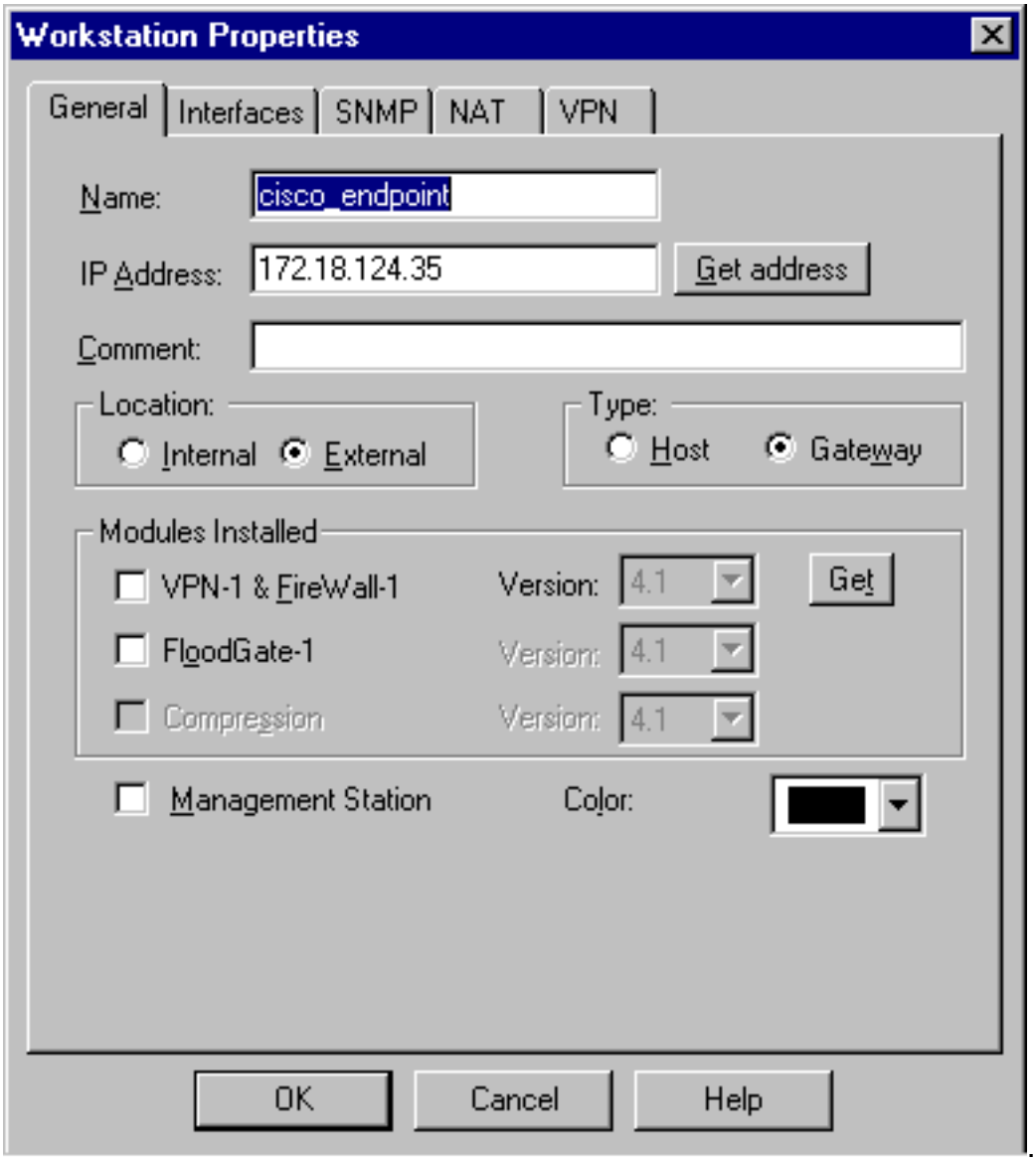
المثبتة.

4. حدد **إدارة > كائنات الشبكة > جديد (أو تحرير) > الشبكة** لتكوين الكائن للشبكة الخارجية ("inside_cisco") خلف مركز VPN.يجب أن يتوافق هذا مع **192.168.1.0/24> = LocalAccess<**أمر مركز



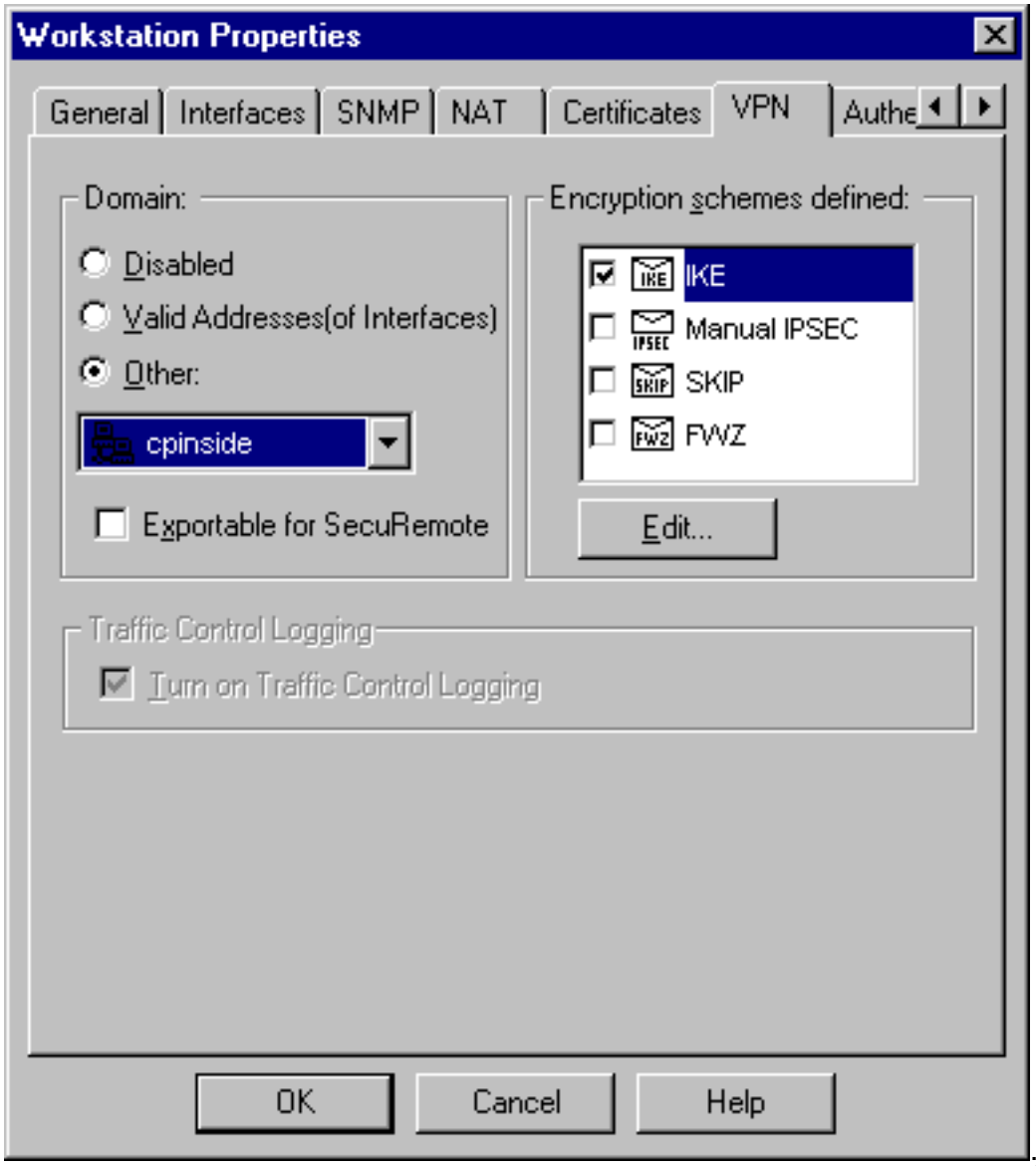
VPN.

5. حدد **إدارة > كائنات الشبكة > جديد > محطة عمل** لإضافة كائن لبوابة مركز VPN الخارجية ("Cisco_Endpoint").هذا هو الواجهة "الخارجية" من مركز VPN مع الاتصال بنقطة التفتيش (في هذا المستند، يمثل 172.18.124.35 عنوان IP في **الأمر** ip> =IPAddress**>**).حدد **خارجي** أسفل الموقع. حدد **عبارة** للنوع.**ملاحظة:** عدم التحقق من -VPN-1/FireWall



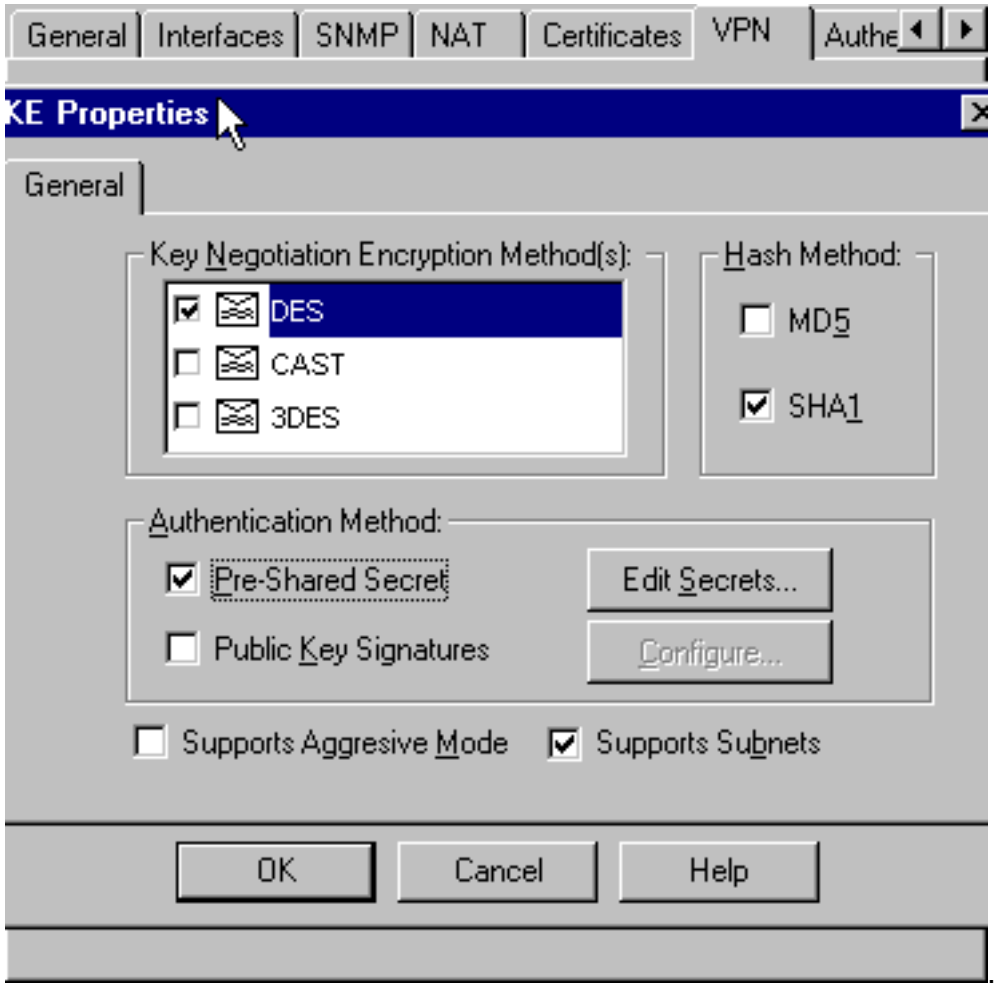
1.

6. حدد **إدارة > كائنات الشبكة > تحرير** لتحرير نقطة نهاية عبارة نقطة النهاية (تسمى "RTPCPVPN") لعلامة التبويب VPN. تحت المجال، حدد **آخر** ثم حدد داخل شبكة نقطة التفتيش (والتي تسمى "cpinside") من القائمة المنسدلة. تحت تشفير نظام يعين، حدد **IKE**، ثم انقر



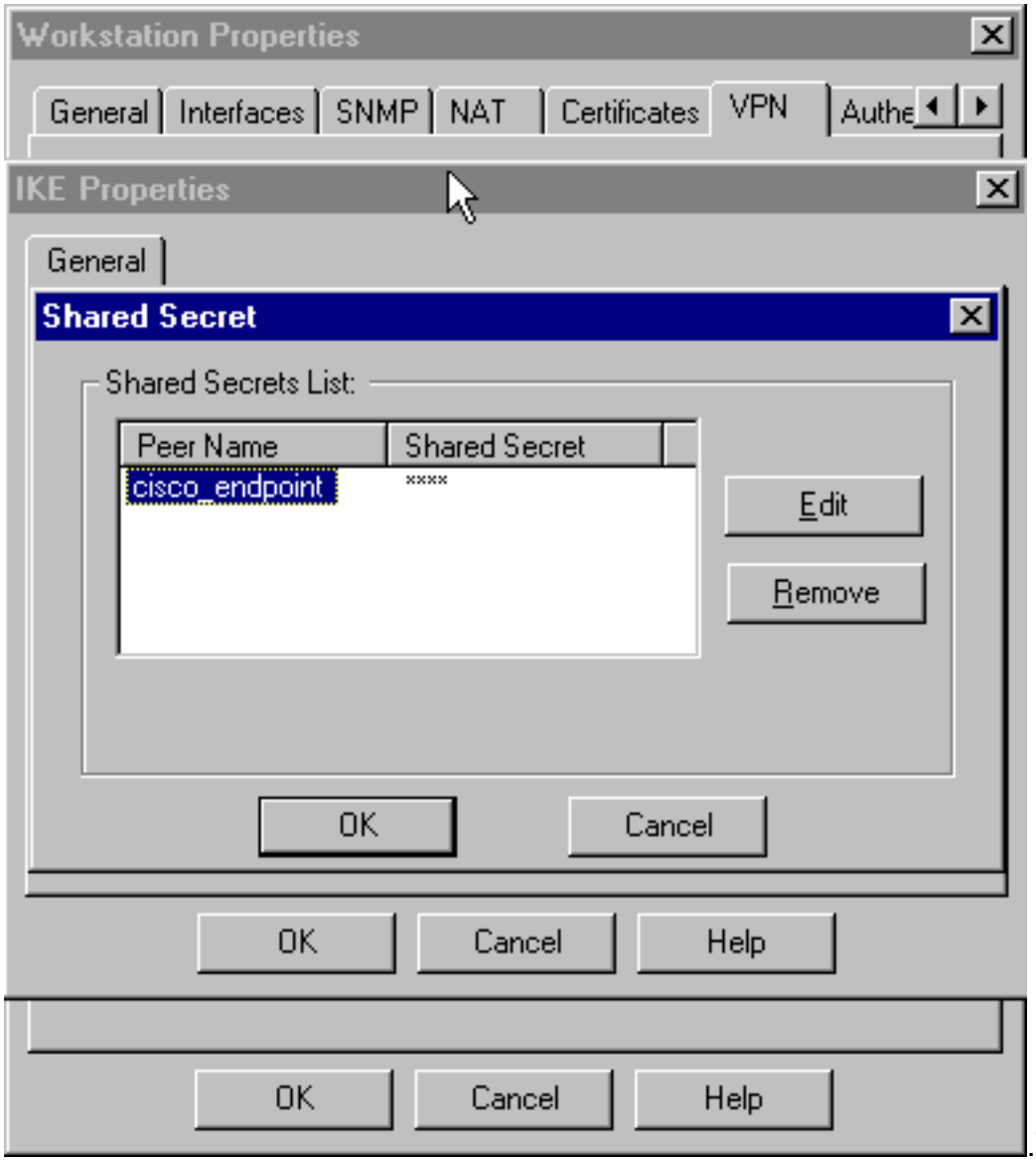
تحرير.

7. قم بتغيير خصائص IKE إلى تشفير **DES** وتجزئة **SHA1** للاتفاق مع أمر مركز **SHA_DES_G2** VPN.**ملاحظة:** تشير "G2" إلى مجموعة Diffie-Hellman رقم 1 أو 2. وفي الاختبار، اكتشف أن نقطة التفتيش تقبل إما "G2" أو "G1".تغيير هذه الإعدادات:عدم تحديد **الوضع المتداخل**.تحقق من **دعم الشبكات الفرعية**.تحقق من **سر مشترك مسبقا** تحت أسلوب



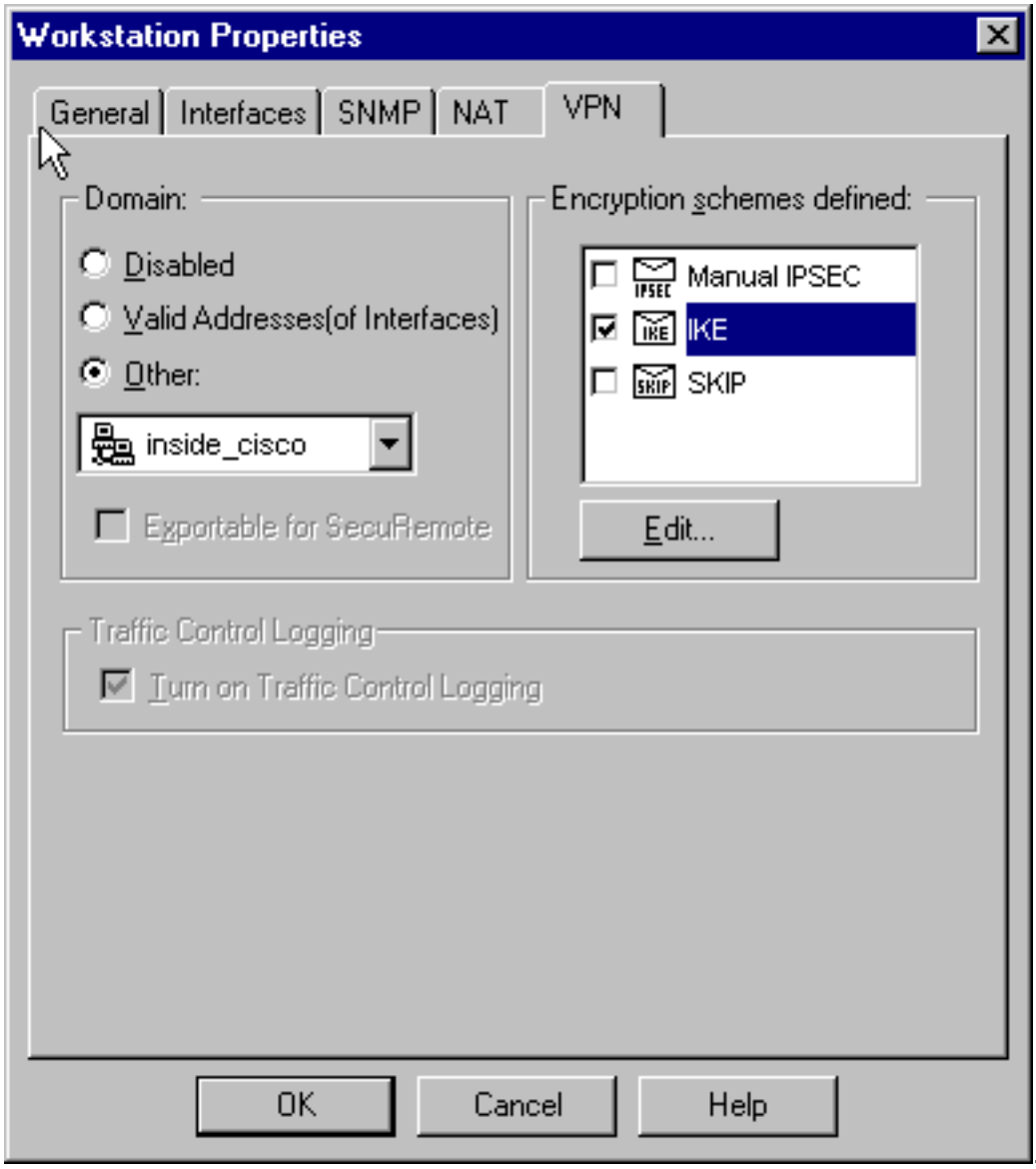
المصادقة.

8. انقر فوق **تحرير الأسرار** لتعيين المفتاح المشترك مسبقا للاتفاق مع **<SharedKey = <key**أمر مركز



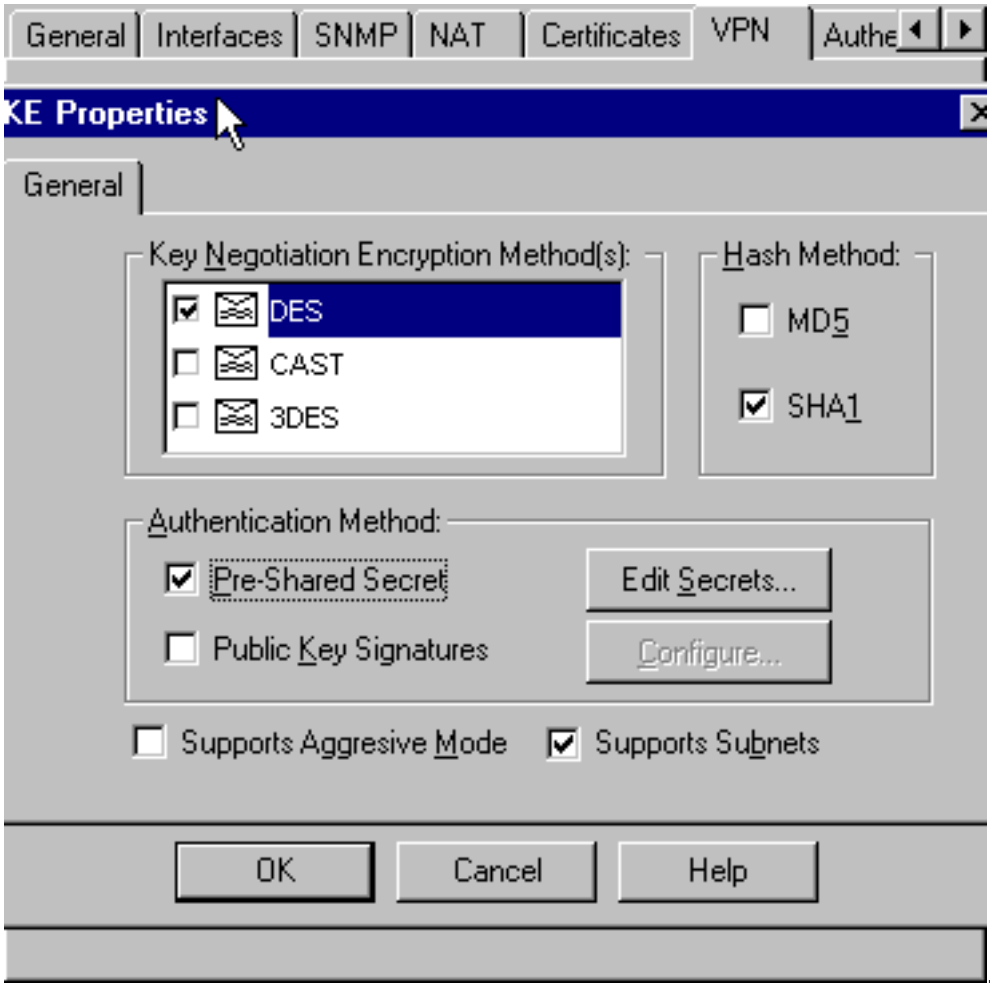
.VPN

9. حدد **إدارة > كائنات الشبكة > تحرير** لتحرير علامة التبويب VPN "cisco_endpoint". تحت المجال، حدد **آخر**، ثم حدد داخل شبكة مركز VPN (تسمى "inside_cisco"). تحت تشفير نظام يعين، حدد **IKE**، ثم انقر



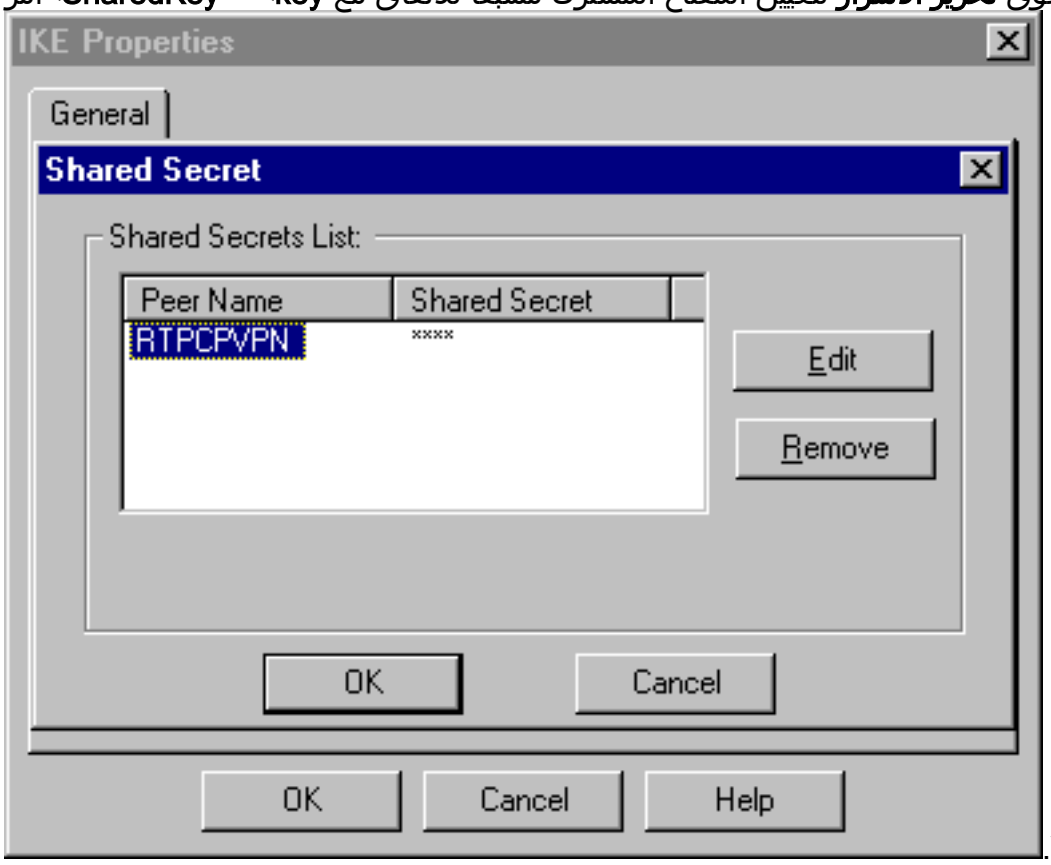
تحرير.

10. قم بتغيير خصائص IKE إلى تشفير **DES** وتجزئة **SHA1** للاتفاق مع أمر مركز **SHA_DES_G2** VPN.**ملاحظة:** تشير "G2" إلى مجموعة Diffie-Hellman رقم 1 أو 2. وعند الاختبار، تبين أن نقطة التفتيش تقبل إما "G2" أو "G1".تغيير هذه الإعدادات:عدم تحديد **الوضع المتداخل**.تحقق من **دعم الشبكات الفرعية**.تحقق من **سر مشترك مسبقا** تحت أسلوب



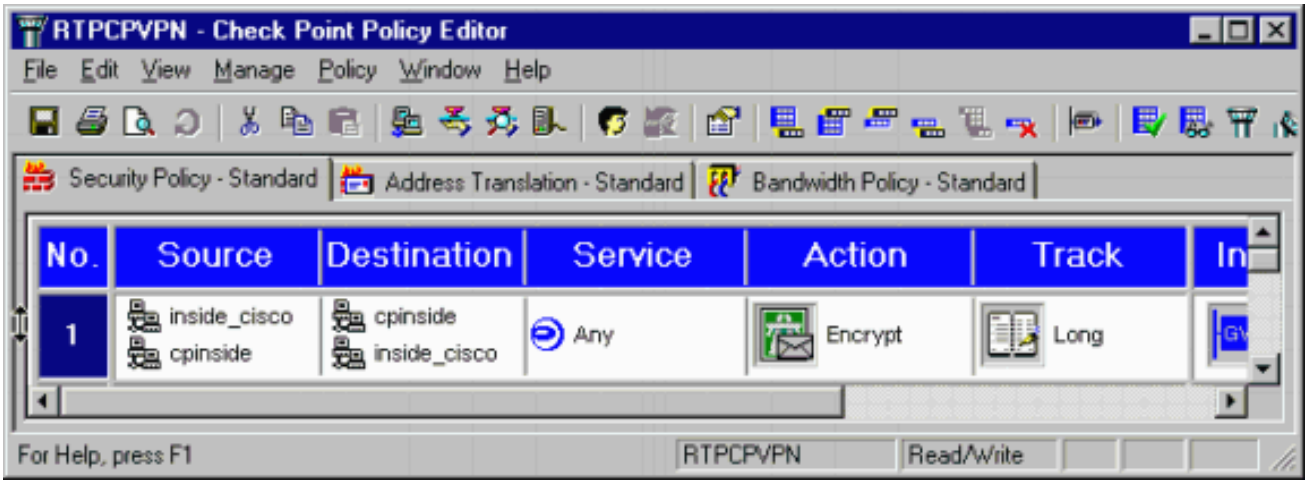
المصادقة.

11. انقر فوق **تحرير الأسرار** لتعيين المفتاح المشترك مسبقا للاتفاق مع **<SharedKey = <key**أمر مركز

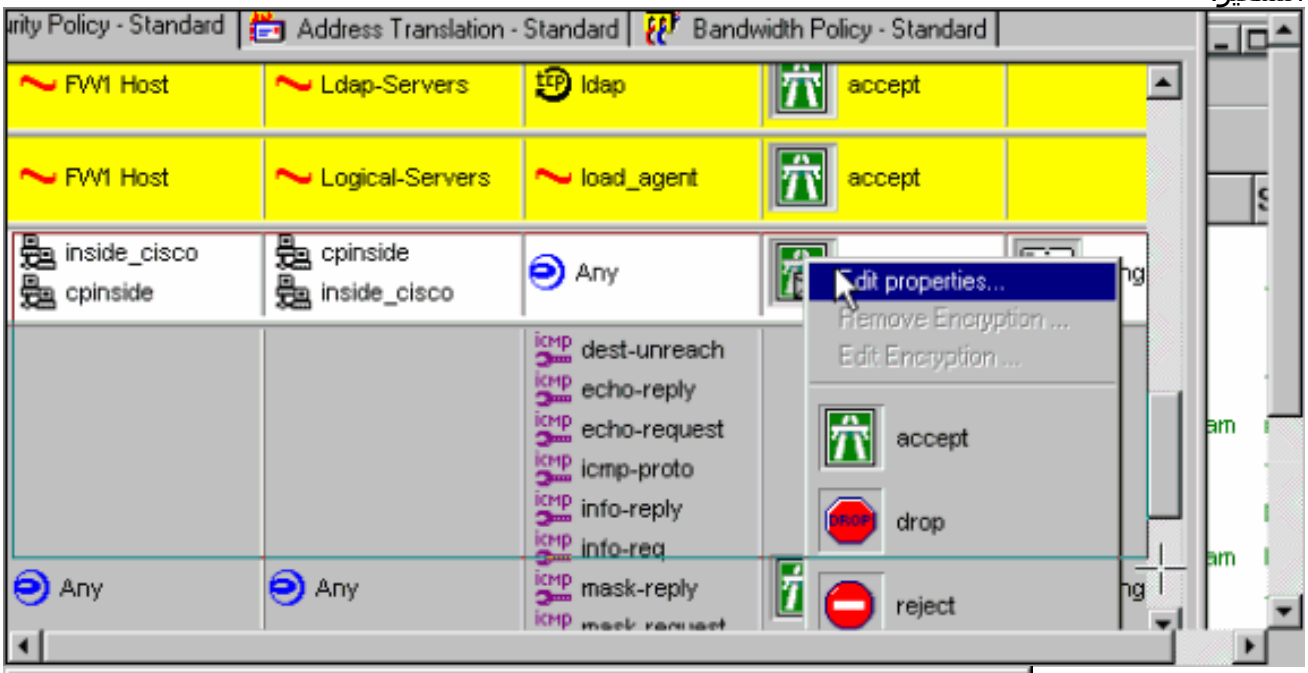


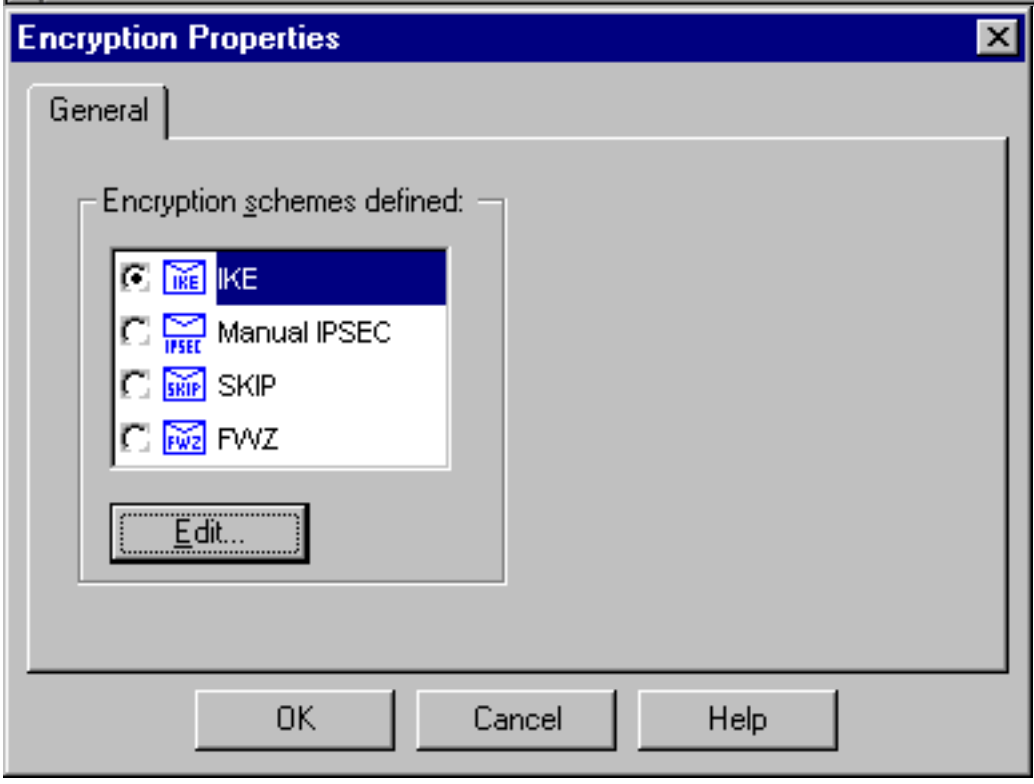
VPN.

12. في نافذة "محرر النهج"، قم بإدراج قاعدة بكل من "المصدر والوجهة" و"inside_cisco" و"cpinside" (ثنائي الإتجاه). **action=encrypt**، set **service=any**،
و**track=long**.



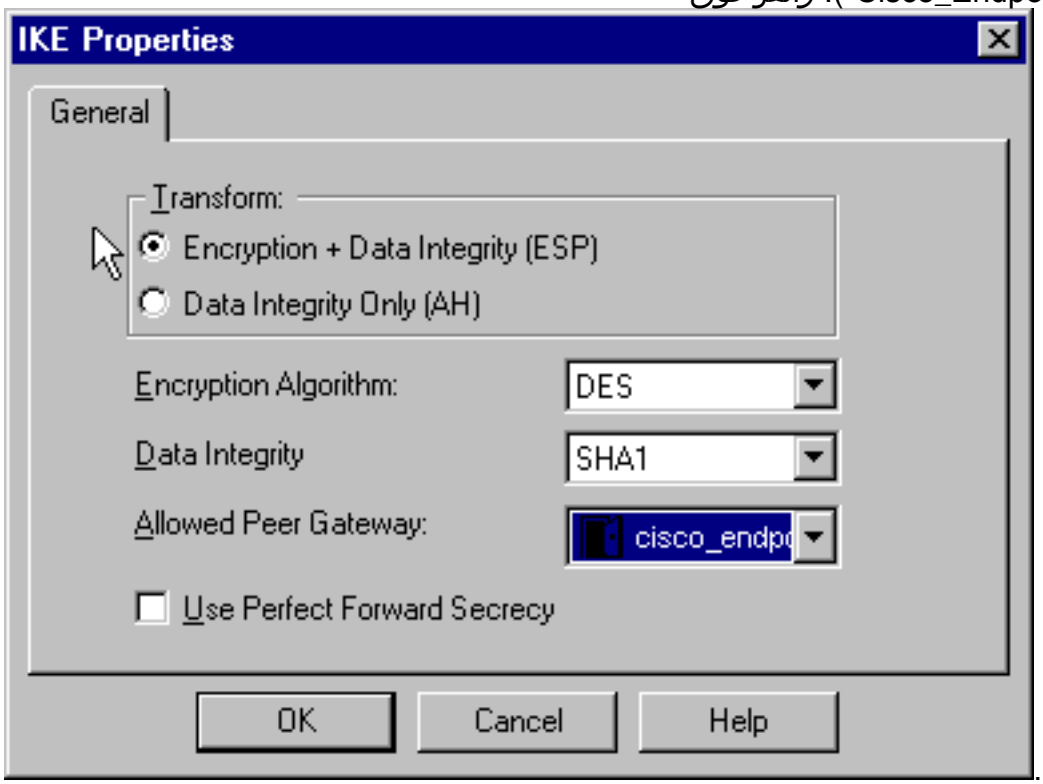
13. تحت عنوان الإجراء، انقر على أيقونة **التشفير** الأخضر وحدد **تحرير الخصائص** لتكوين سياسات التشفير.





14. حدد **IKE**، وانقر **تحرير**.
15. في نافذة خصائص IKE، قم بتغيير هذه الخصائص لتوافق مع أمر مركز **التحويل = esp(sha،des)**

VPN.تحت التحويل، حدد **التشفير + تكامل البيانات (ESP)**. يجب أن تكون خوارزمية التشفير **DES**، ويجب أن تكون تكامل البيانات **SHA1**، ويجب أن تكون بوابة النظير المسموح بها عبارة مركز VPN الخارجية (تسمى "Cisco_Endpoint"). وانقر فوق



.OK

16. بعد تكوين نقطة التحقق، حدد **نهج > تثبيت** في قائمة نقطة التفتيش لتفعيل التغييرات.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

أوامر أستكشاف أخطاء مركز VPN 5000 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**.

- **VPN Trace Dump all** —يعرض معلومات حول جميع إتصالات VPN المطابقة، بما في ذلك معلومات حول الوقت، ورقم VPN، وعنوان IP الحقيقي للنظير، والذي تم تشغيل البرامج النصية، وفي حالة حدوث خطأ، الروتين ورقم سطر رمز البرنامج حيث حدث الخطأ.
- **show system log buffer**— يعرض محتويات المخزن المؤقت للسجل الداخلي.
- **show vpn statistics** — يعرض هذه المعلومات للمستخدمين والشركاء والإجمالي لكل من. (للطرز النمطية، يتضمن العرض قسما لكل فتحة وحدة نمطية. ارجع إلى قسم إخراج تصحيح الأخطاء للعينة.) — الاتصالات النشطة الحالية. - الاتصالات التفاوضية الحالية. —أعلى عدد من الاتصالات النشطة المتزامنة منذ آخر إعادة تشغيل. —إجمالي عدد الاتصالات الناجحة منذ آخر إعادة تشغيل."OK — عدد الانفاق التي لم تكن هنالك أخطاء فيها. — يبدأ عدد النفق. - عدد الأنفاق التي بها أخطاء.
- **show vpn statistics verbose**— يعرض إحصائيات تفاوض ISAKMP، وإحصاءات اتصال أكثر نشاطا.

تلخيص الشبكة

عندما يتم تكوين شبكات داخلية متجاورة متعددة في مجال التشفير على نقطة التحقق، قد يقوم الجهاز بتلخيصها 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، فقد يتم تلخيصها إلى 10.0.0.0 /23.

تصحيح أخطاء جدار الحماية Checkpoint 4.1

كان هذا تثبيت Microsoft Windows NT. نظرا لتعيين التعقب في نافذة محرر النهج (كما هو موضح في الخطوة 12)، يجب أن تظهر حركة المرور المرفوضة باللون الأحمر في عارض السجل. يمكن الحصول على المزيد من تصحيح الأخطاء المطبعية من خلال:

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

وفي نافذة تانية:

```
C:\WINNT\FW1\4.1\fwstart
```

قم بإصدار هذه الأوامر لمسح اقترانات الأمان (SAs) على نقطة التفتيش:

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

أجب **بنعم** في ؟

إخراج تصحيح الأخطاء للعينة

```
cisco_endpoint#vpn trac dump all
                                        -- seconds -- stepmngr trace enabled 4
                                (new script: lan-lan primary initiator for <no id> (start
                               (manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start
                                                (seconds doing l2lp_init, (0 @ 0 38
                                            (seconds doing l2lp_do_negotiation, (0 @ 0 38
                        (new script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157] (start
                                             (seconds doing isa_i_main_init, (0 @ 0 38
                                (manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done
                               (manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start
                                  (seconds doing isa_i_main_process_pkt_2, (0 @ 0 38
                                (manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done
                               (manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start
                                  (seconds doing isa_i_main_process_pkt_4, (0 @ 0 38
                                (manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done
                               (manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start
                                  (seconds doing isa_i_main_process_pkt_6, (0 @ 0 39
                                        (seconds doing isa_i_main_last_op, (0 @ 0 39
                    (end script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0
               (next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0
                                         (seconds doing l2lp_phase_1_done, (0 @ 0 39
                                        (seconds doing l2lp_start_phase_2, (0 @ 0 39
                            (new script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157] (start
                                                 (seconds doing iph2_init, (0 @ 0 39
                                           (seconds doing iph2_build_pkt_1, (0 @ 0 39
```

```
                                    (seconds doing iph2_send_pkt_1, (0 @ 0 39
                           (manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done
                          (manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start
                                    (seconds doing iph2_pkt_2_wait, (0 @ 0 39
                                  (seconds doing ihp2_process_pkt_2, (0 @ 0 39
                                    (seconds doing iph2_build_pkt_3, (0 @ 0 39
                                    (seconds doing iph2_config_SAs, (0 @ 0 39
                                    (seconds doing iph2_send_pkt_3, (0 @ 0 39
                                       (seconds doing iph2_last_op, (0 @ 0 39
            (end script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0
    (next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0
                                    (seconds doing l2lp_open_tunnel, (0 @ 0 39
                                  (seconds doing l2lp_start_i_maint, (0 @ 0 39
          (new script: initiator maintenance for lan-lan-VPN0:1:[172.18.124.157] (start
                                       (seconds doing imnt_init, (0 @ 0 39
                           (manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done


                                                    cisco_endpoint#show vpn stat

  Current  In       High     Running  Tunnel   Tunnel   Tunnel
   Active   Negot    Water    Total    Starts   OK       Error
 ------------------------------------------------------------------
       Users     0        0        0        0        0        0        0
       Partners  1        0        1        1        1        0        0
       Total     1        0        1        1        1        0        0

                                                                 :IOP slot 1

  Current  In       High     Running  Tunnel   Tunnel   Tunnel
   Active   Negot    Water    Total    Starts   OK       Error
 ------------------------------------------------------------------
       Users     0        0        0        0        0        0        0
       Partners  0        0        0        0        0        0        0
       Total     0        0        0        0        0        0        0

                                                cisco_endpoint#show vpn stat verb

  Current  In       High     Running  Tunnel   Tunnel   Tunnel
   Active   Negot    Water    Total    Starts   OK       Error
 ------------------------------------------------------------------
       Users     0        0        0        0        0        0        0
       Partners  1        0        1        1        1        0        0
       Total     1        0        1        1        1        0        0

                                                    Stats             VPN0:1
                                                    Wrapped              13
                                                    Unwrapped             9
                                                    BadEncap              0
                                                    BadAuth               0
                                                    BadEncrypt            0
                                                    rx IP                 9
                                                    rx IPX                0
                                                    rx Other              0
                                                    tx IP                13
                                                    tx IPX                0
                                                    tx Other              0
                                                    IKE rekey             0

                                          Input VPN pkts dropped due to no SA: 0

                                 Input VPN pkts dropped due to no free queue entries: 0

                                                    ISAKMP Negotiation stats
```

Admin packets in	4
Fastswitch packets in	0
No cookie found	0
Can't insert cookie	0
Inserted cookie(L)	1
Inserted cookie(R)	0
Cookie not inserted(L)	0
Cookie not inserted(R)	0
Cookie conn changed	0
Cookie already inserted	0
Deleted cookie(L)	0
Deleted cookie(R)	0
Cookie not deleted(L)	0
Cookie not deleted(R)	0
Forwarded to RP	0
Forwarded to IOP	0
Bad UDP checksum	0
Not fastswitched	0
Bad Initiator cookie	0
Bad Responder cookie	0
Has Responder cookie	0
No Responder cookie	0
No SA	0
Bad find conn	0
Admin queue full	0
Priority queue full	0
Bad IKE packet	0
No memory	0
Bad Admin Put	0
IKE pkt dropped	0
No UDP PBuf	0
No Manager	0
Mgr w/ no cookie	0
Cookie Scavenge Add	1
Cookie Scavenge Rem	0
Cookie Scavenged	0
Cookie has mgr err	0
New conn limited	0

:IOP slot 1

	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error	
Users	0	0	0	0	0	0	0	
Partners	0	0	0	0	0	0	0	
Total	0	0	0	0	0	0	0	

Stats
Wrapped
Unwrapped
BadEncap
BadAuth
BadEncrypt
rx IP
rx IPX
rx Other
tx IP
tx IPX
tx Other
IKE rekey

Input VPN pkts dropped due to no SA: 0

```
Input VPN pkts dropped due to no free queue entries: 0

                ISAKMP Negotiation stats
 Admin packets in                   0
 Fastswitch packets in              3
 No cookie found                    0
 Can't insert cookie                0
 Inserted cookie(L)                 0
 Inserted cookie(R)                 1
 Cookie not inserted(L)             0
 Cookie not inserted(R)             0
 Cookie conn changed                0
Cookie already inserted             0
 Deleted cookie(L)                  0
 Deleted cookie(R)                  0
 Cookie not deleted(L)              0
 Cookie not deleted(R)              0
 Forwarded to RP                    0
 Forwarded to IOP                   3
 Bad UDP checksum                   0
 Not fastswitched                   0
 Bad Initiator cookie               0
 Bad Responder cookie               0
 Has Responder cookie               0
 No Responder cookie                0
 No SA                              0
 Bad find conn                      0
 Admin queue full                   0
 Priority queue full                0
 Bad IKE packet                     0
 No memory                          0
 Bad Admin Put                      0
 IKE pkt dropped                    0
 No UDP PBuf                        0
 No Manager                         0
 Mgr w/ no cookie                   0
 Cookie Scavenge Add                1
 Cookie Scavenge Rem                0
 Cookie Scavenged                   0
 Cookie has mgr err                 0
 New conn limited                   0
```

معلومات ذات صلة

- إعلان نهاية المبيعات لسلسلة Cisco VPN 5000
- 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).