تكوين نفق IPsec - موجه إلى جدار حماية نقطة التفتيش 4.1 من Cisco

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين نفق IPsec بمفاتيح مشتركة مسبقا للانضمام إلى شبكتين خاصتين: الشبكة الخاصة x.192.168.1 داخل موجه Cisco والشبكة الخاصة x.10.32.50 داخل جدار حماية نقطة التفتيش.

المتطلبات الأساسية

المتطلبات

يفترض هذا التكوين أن حركة المرور من داخل الموجه وداخل نقطة التفتيش إلى الإنترنت (ممثلة هنا في شبكات x.172.18.124) تتدفق قبل بدء التكوين.

المكونات المستخدمة

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

- موجّه Cisco 3600
- برنامج Cisco IOS® (C3640-JO3S56I-M)، الإصدار 12.1(5)T، برنامج الإصدار (FC1)
- جدار حماية نقطة التفتيش 4.1

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.

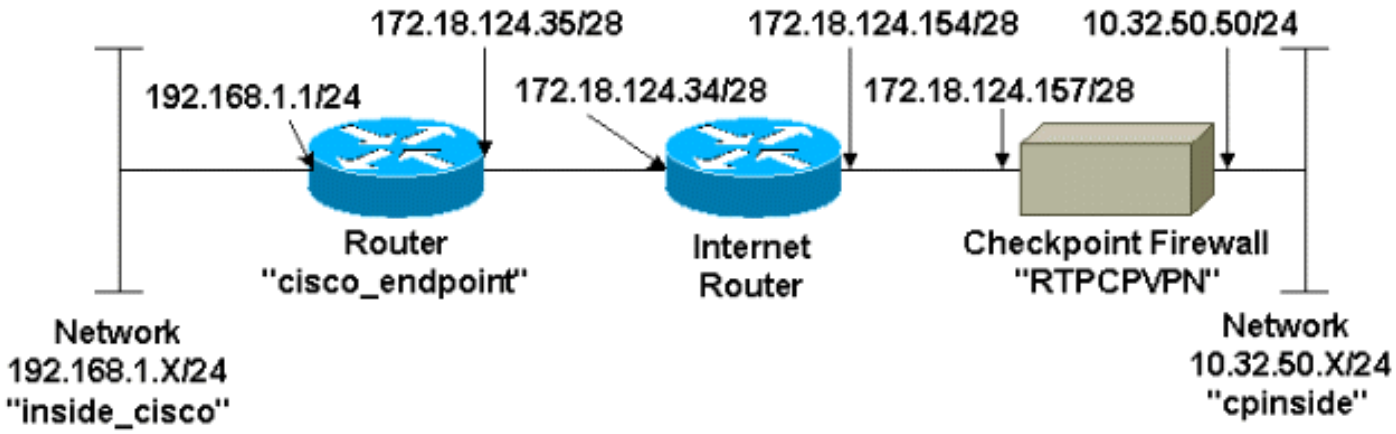
التكوين

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 هذه التكوينات.

- تكوين الموجّه
- تكوين جدار حماية نقطة الوصول

تكوين الموجّه

تكوين الموجه Cisco 3600
Current configuration : 1608 bytes ! version 12.1 no service single-slot-reload-enable service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname cisco_endpoint !

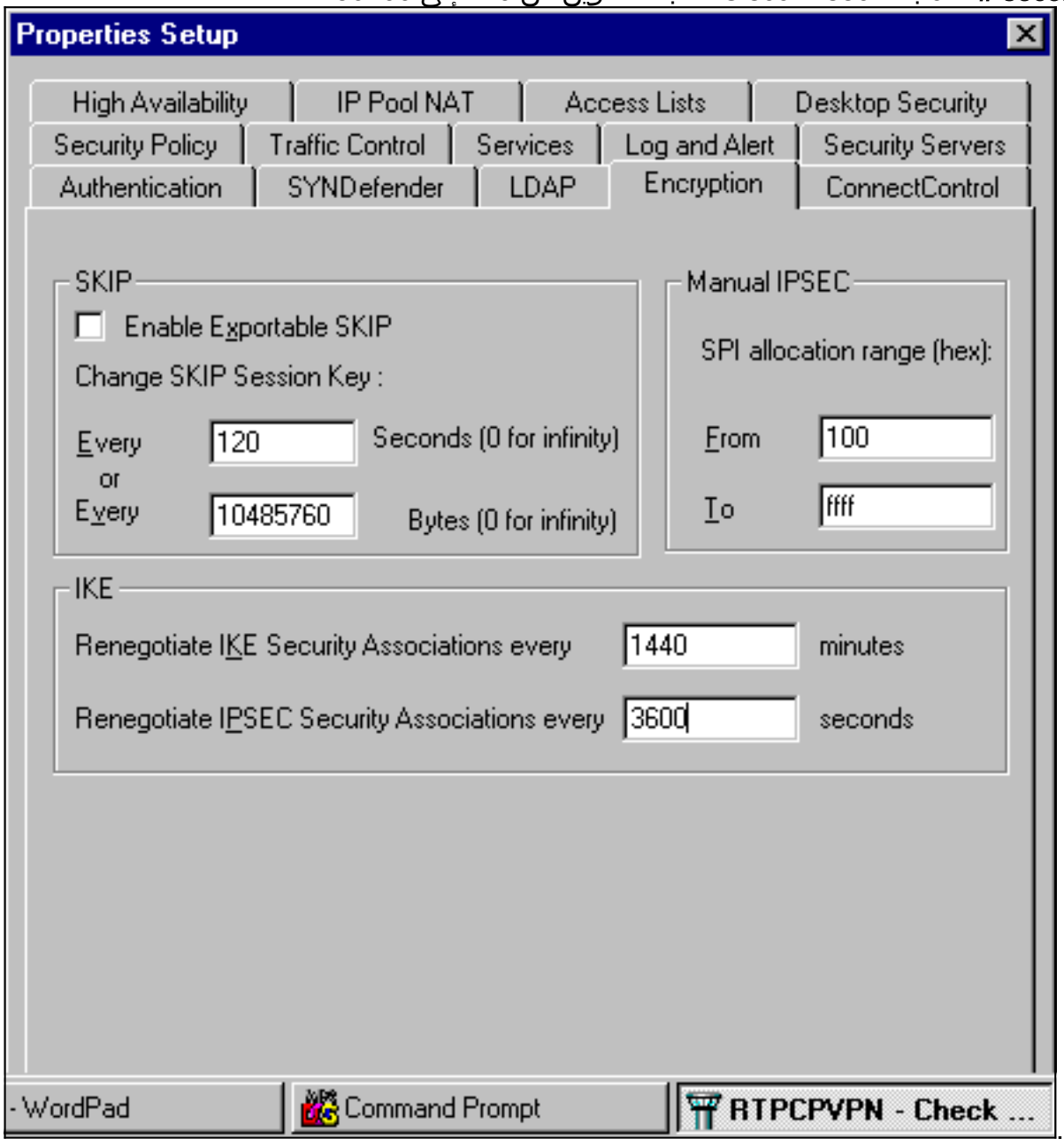
```
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
Internet Key Exchange (IKE) configuration crypto ---!
isakmp policy 1
authentication pre-share
crypto isakmp key ciscorules address 172.18.124.157
!
IPsec configuration crypto ipsec transform-set ---!
rtpset esp-des esp-sha-hmac
!
crypto map rtp 1 ipsec-isakmp
set peer 172.18.124.157
set transform-set rtpset
match address 115
!
call rsvp-sync
cns event-service server
!
controller T1 1/0
!
controller T1 1/1
!
interface Ethernet0/0
ip address 172.18.124.35 255.255.255.240
ip nat outside
no ip mroute-cache
half-duplex
crypto map rtp
!
interface Ethernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
ip kerberos source-interface any
ip nat pool INTERNET 172.18.124.36 172.18.124.36 netmask
255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.34
no ip http server
!
access-list 101 deny ip 192.168.1.0 0.0.0.255 10.32.50.0
0.0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
access-list 115 permit ip 192.168.1.0 0.0.0.255
10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any
route-map nonat permit 10
match ip address 101
!
```

```
dial-peer cor custom
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

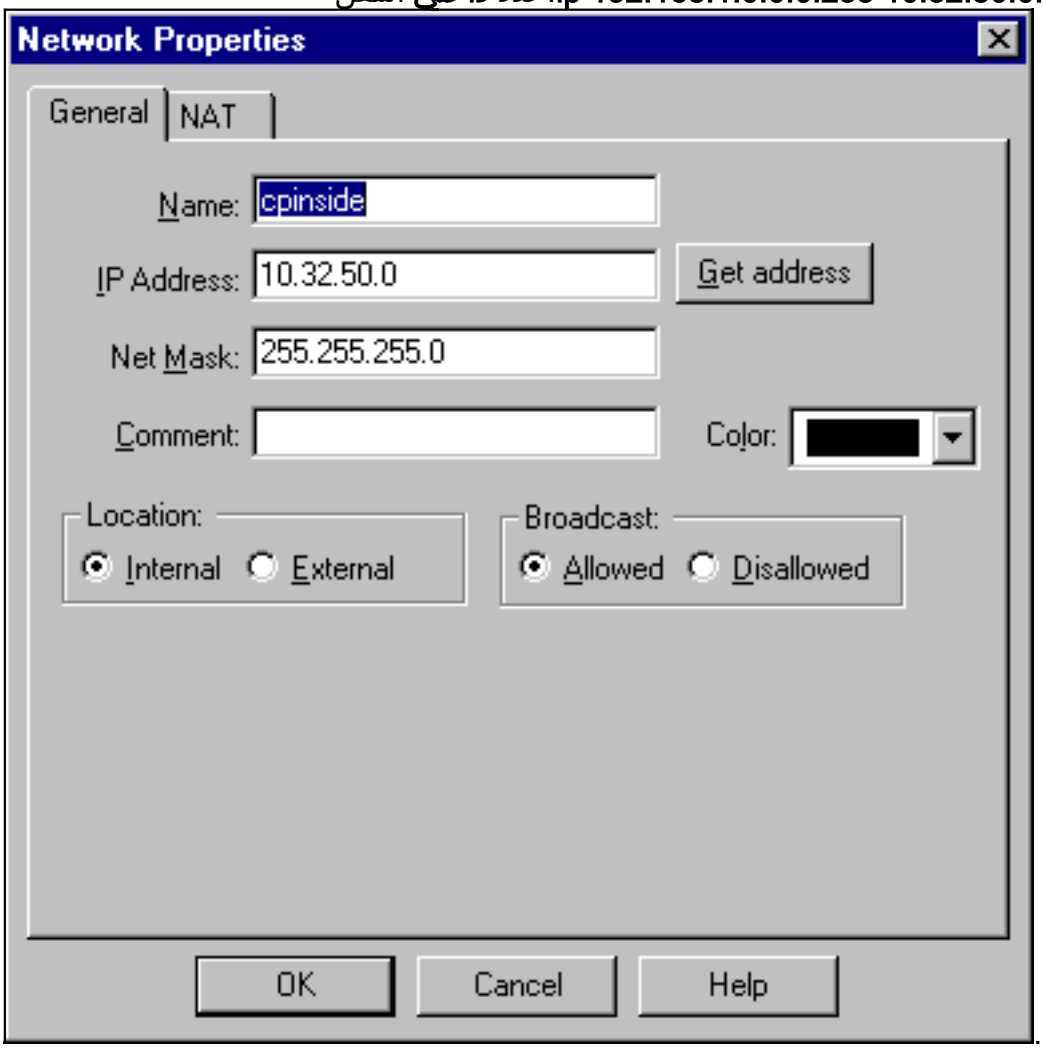
تكوين جدار حماية نقطة الوصول

أكمل الخطوات التالية لتكوين جدار حماية نقطة التحقق.

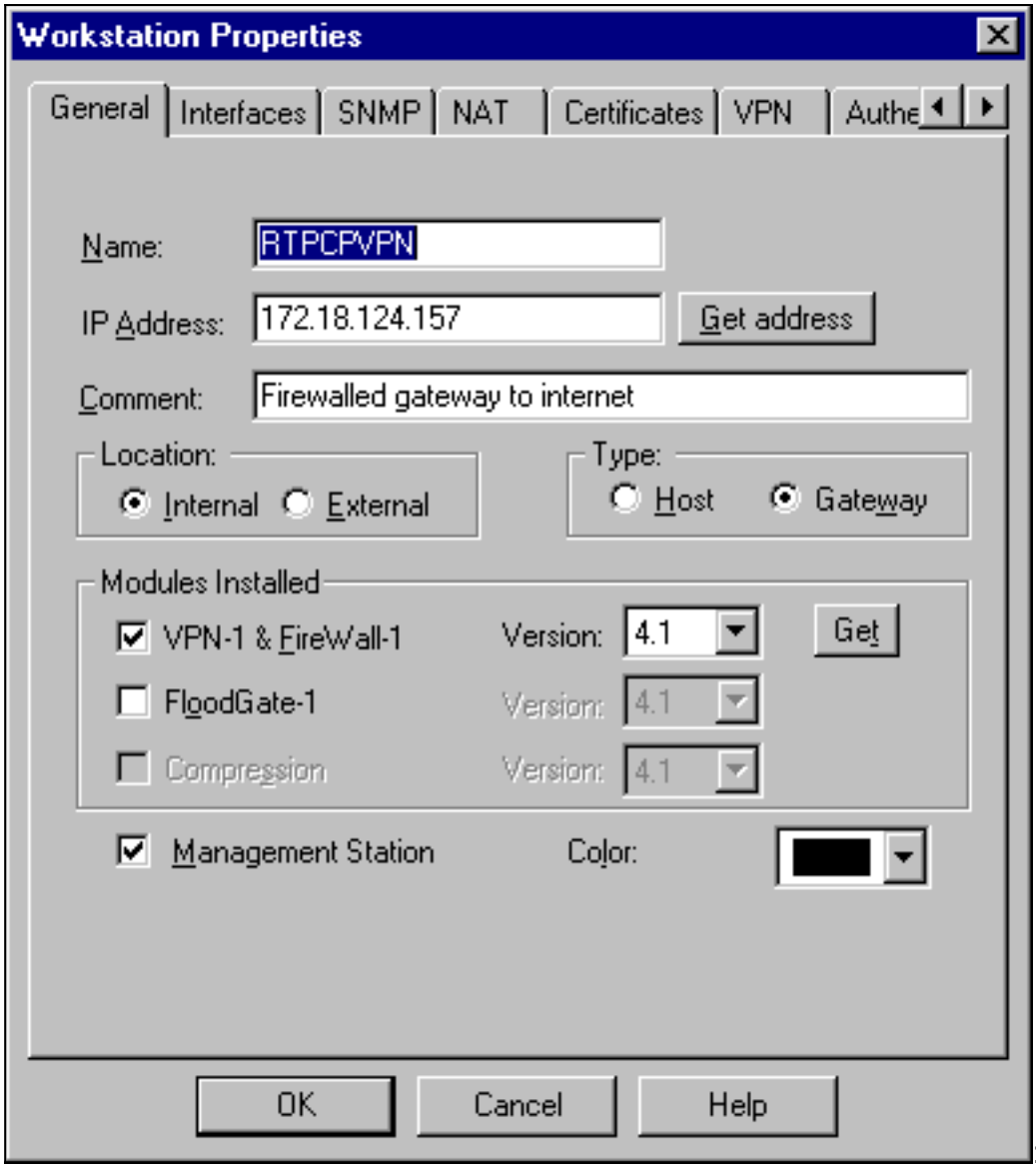
1. ونظرا لاختلاف مدد الحياة الافتراضية لكل من IKE و IPsec بين الموردين، حدد **خصائص > تشفير** لتعيين فترات حياة نقطة التحقق للاتفاق مع إعدادات Cisco الافتراضية.مدة بقاء IKE الافتراضية من Cisco هي 86400 ثانية (= 1440 دقيقة)، ويمكن تعديلها باستخدام الأوامر التالية:**سياسة التشفير ISAKMP #رقم العمر**تتراوح مدة بقاء Cisco IKE القابلة للتكوين من 60 إلى 86400 ثانية. مدة بقاء IPsec الافتراضية من Cisco هي 3600 ثانية، ويمكن تعديلها بواسطة الأمر **crypto ipsEc security-association lifetime seconds #**.مدة بقاء Cisco IPsec القابلة للتكوين من 120 إلى 86400 ثانية.



2. حدد **إدارة > كائنات الشبكة > جديد (أو تحرير) > الشبكة** لتكوين الكائن للشبكة الداخلية (يسمى "CPINSIDE") خلف نقطة التفتيش.يجب أن يتوافق هذا مع شبكة الوجهة (الثانية) في **الأمر** Cisco **access-list 115 allowed ip 192.168.1.0.0.0.255 10.32.50.0.0.255**.حدد **داخلي** أسفل الموقع.

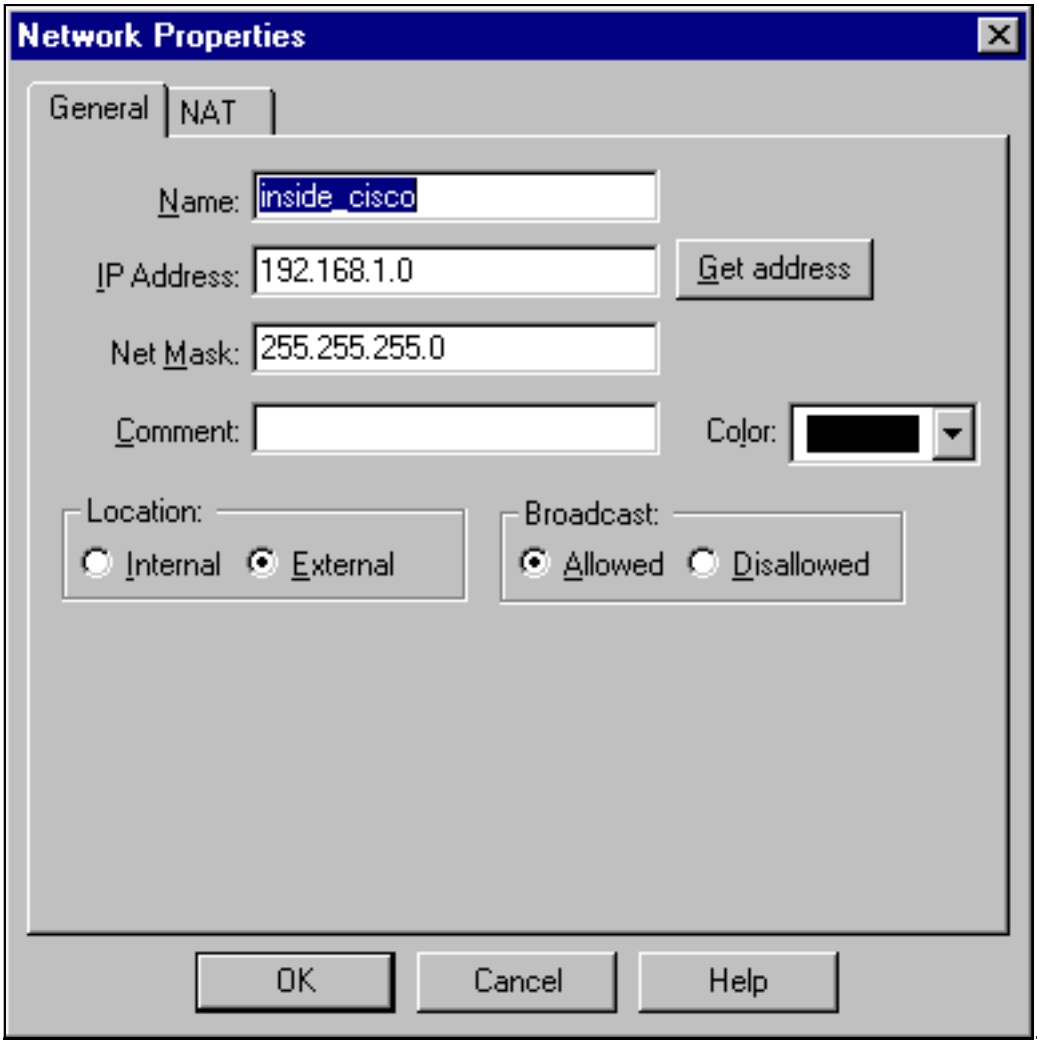


3. حدد **إدارة > كائنات الشبكة > تحرير** لتحرير الكائن لنقطة نهاية (بوابة) RTPCPVPN التي يشير إليها موجه Cisco في الأمر **set peer 172.18.124.157**.حدد **داخلي** أسفل الموقع. للنوع، حدد **البوابة**. تحت الوحدات المثبتة، حدد خانة الاختيار **VPN-1 و FireWall-1**، ثم حدد أيضا خانة الاختيار **محطة**



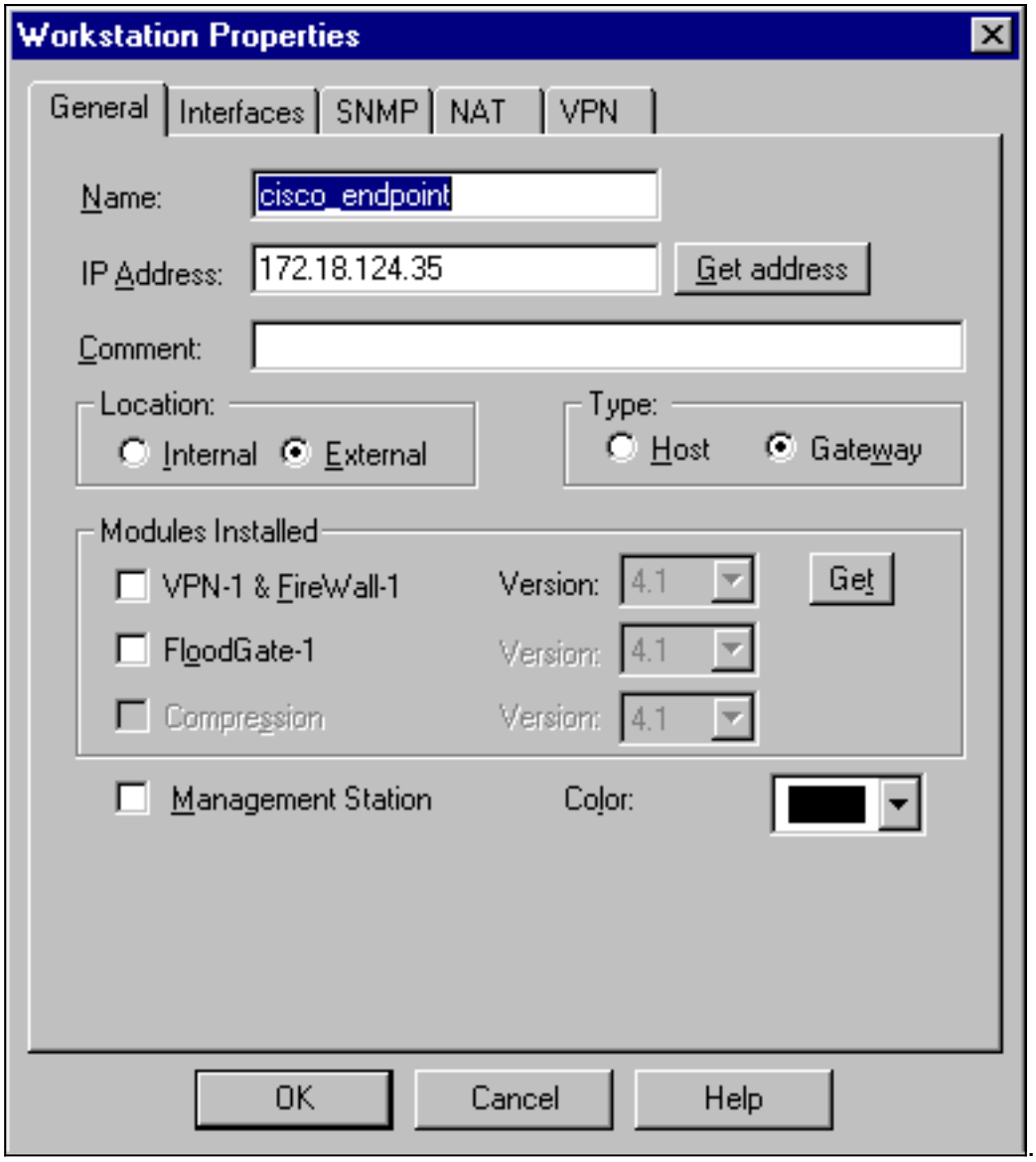
الإدارة:

4. حدد **إدارة > كائنات الشبكة > جديد > الشبكة** لتكوين الكائن للشبكة الخارجية (تسمى "inside_cisco") خلف موجه Cisco.يجب أن يتوافق هذا مع شبكة المصدر (أولا) في **الأمر access-list 115 allowed ip** Cisco **10.32.50.0.0.255 192.168.1.0.0.0.255**.حدد **خارجي** أسفل



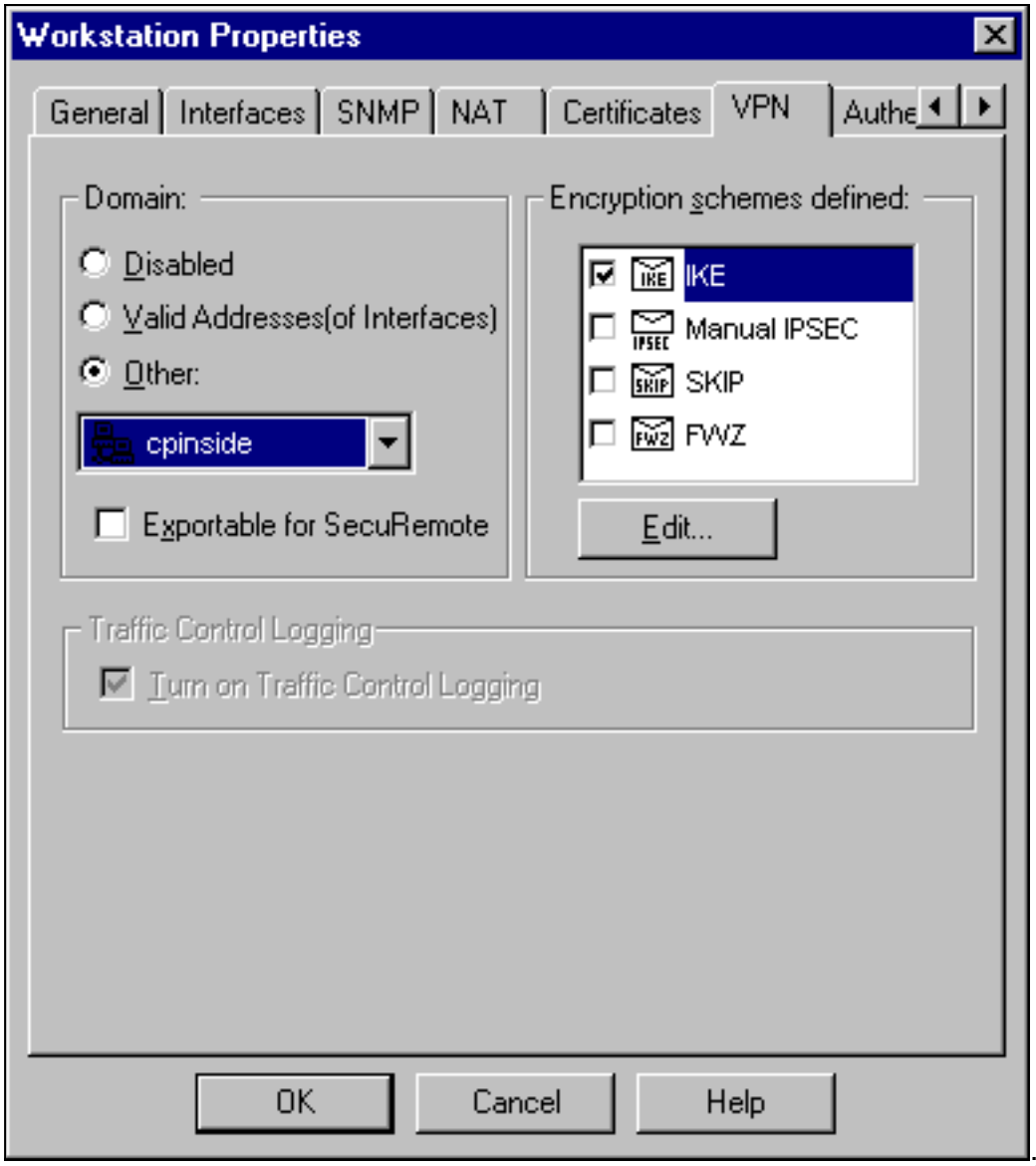
الموقع.

5. حدد **إدارة > كائنات الشبكة > جديد > محطة عمل** لإضافة كائن لبوابة موجه Cisco الخارجية (التي تسمى "cisco_endpoint"). هذه هي واجهة Cisco التي يتم تطبيق الأمر **crypto map** name عليها.حدد **خارجي** أسفل الموقع. للنوع، حدد **البوابة.ملاحظة:** لا تحدد خانة الاختيار -VPN-1/FireWall



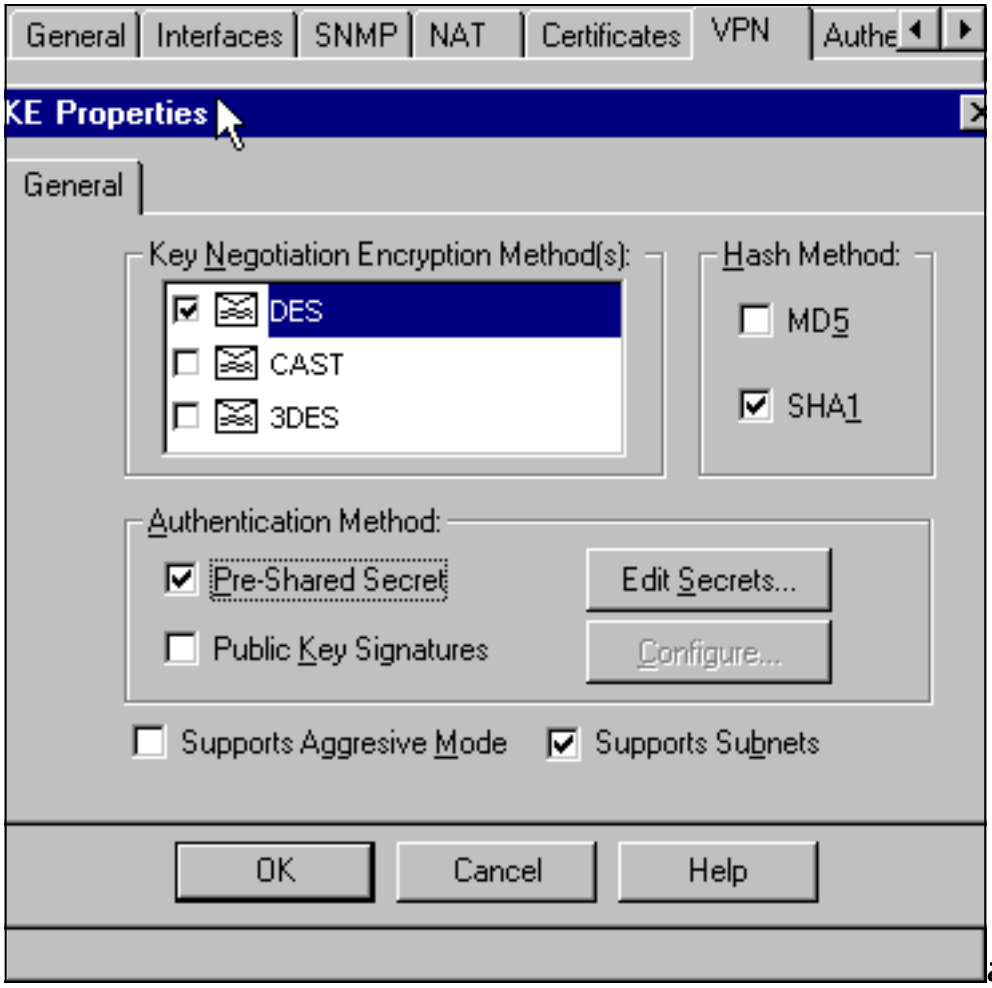
1.

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



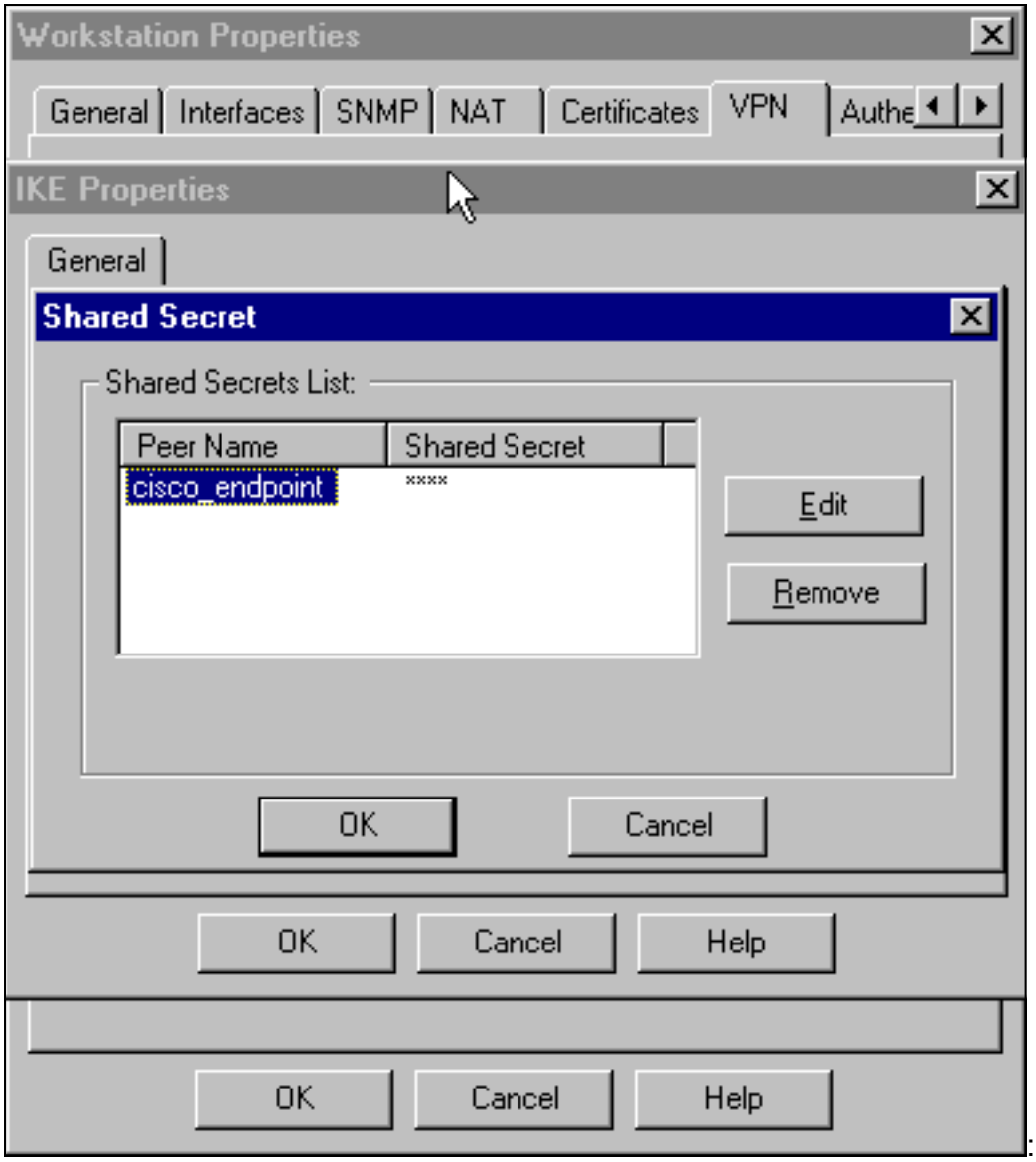
تحرير.

7. قم بتغيير خصائص IKE لتشفير DES لتوافق مع الأوامر التالية:**سياسة التشفير ISAKMP #تشفير DES**
ملاحظة: تشفير DES هو الإعداد الافتراضي لذلك لا يكون مرئيا في تكوين Cisco.
8. قم بتغيير خصائص IKE إلى تجزئة SHA1 للاتفاق مع الأوامر التالية:**سياسة التشفير ISAKMP #تجزئة**
ملاحظة: خوارزمية تجزئة SHA هي الإعداد الافتراضي لذلك لا تكون مرئية في تكوين Cisco.تغيير هذه الإعدادات:عدم تحديد **الوضع المتداخل**.تحقق من **دعم الشبكات الفرعية**.تحقق من **سر مشترك مسبقا** تحت أسلوب المصادقة.
هذا يوافق مع هذا أمر:**سياسة التشفير ISAKMP #مشاركة مسبقة**



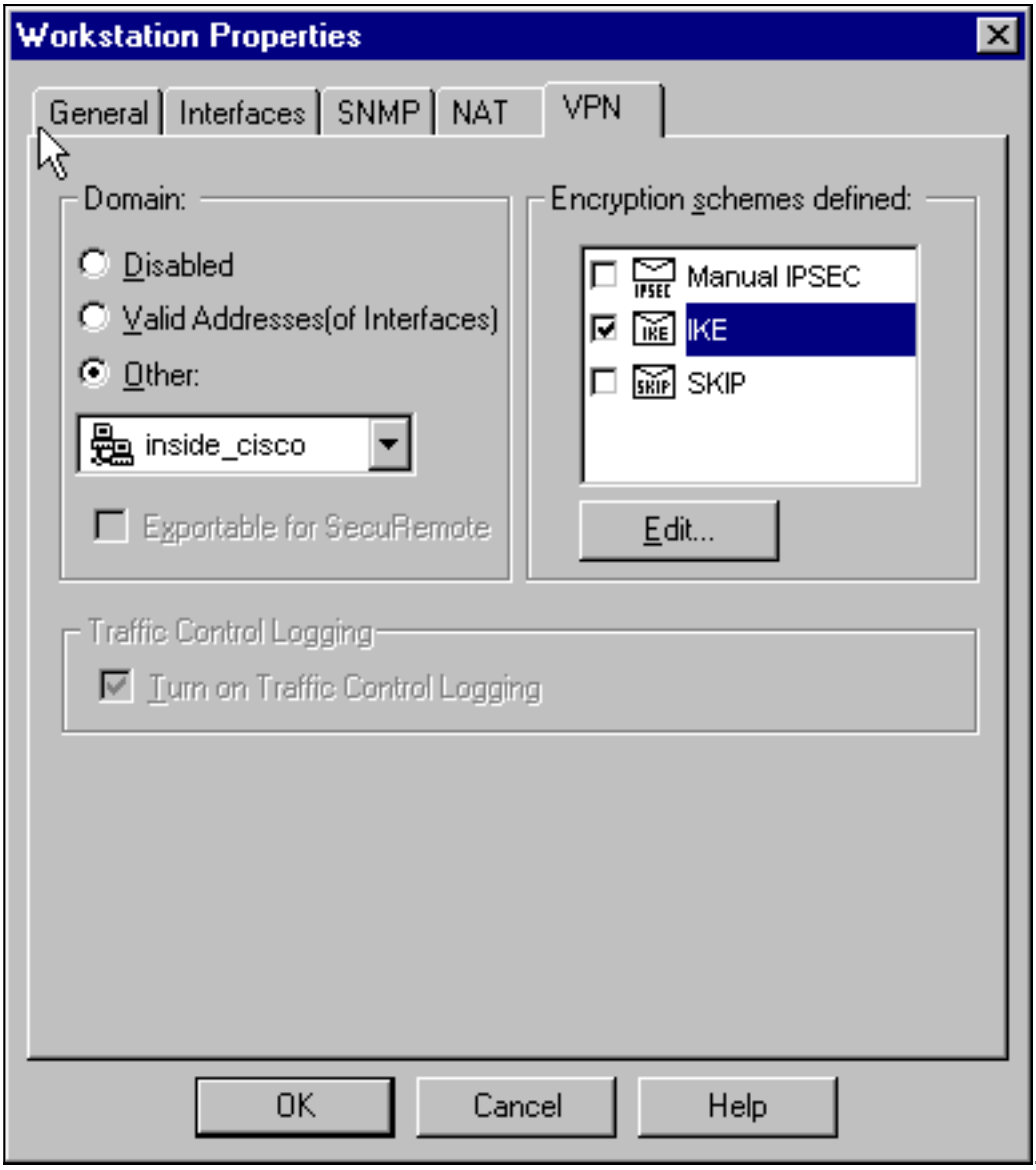
للمصادقة

9. انقر فوق **تحرير الأسرار** لتعيين المفتاح المشترك مسبقا للاتفاق مع **أمر عنوان** مفتاح *تشفير* ***isakmp من***



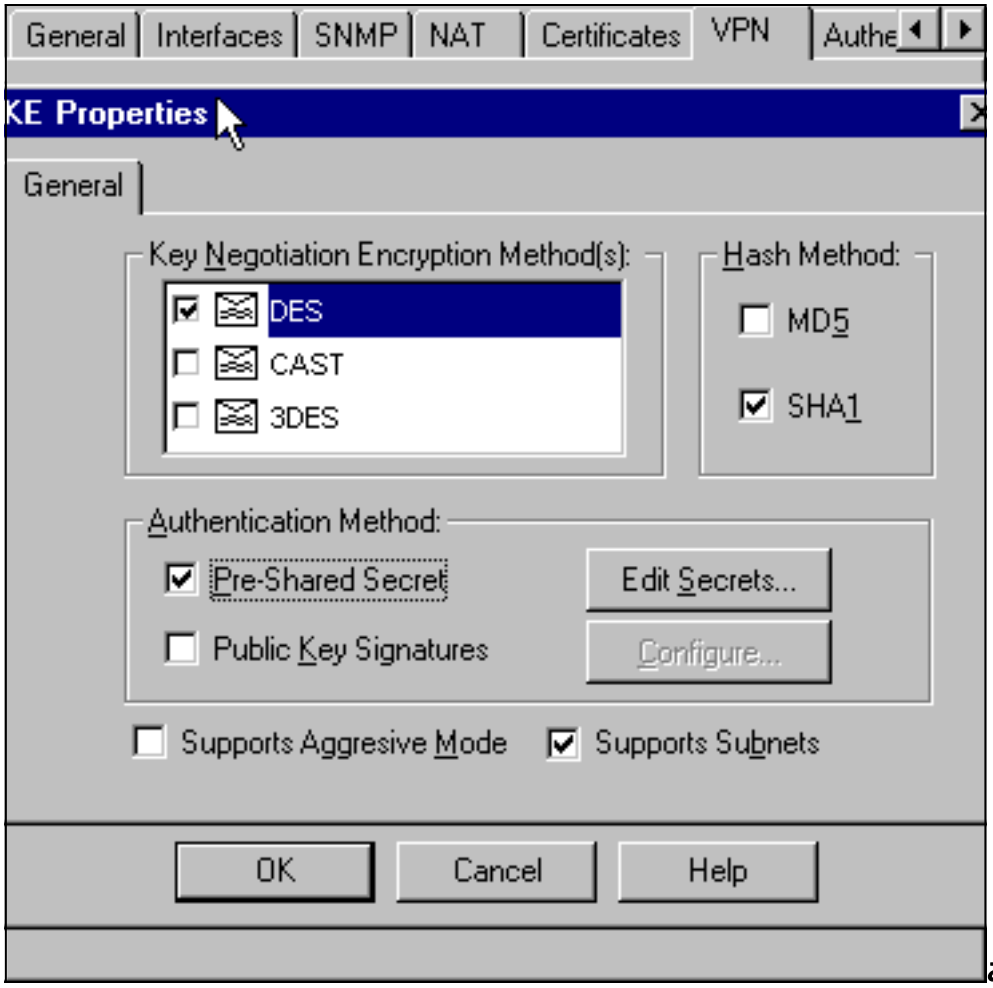
Cisco:

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



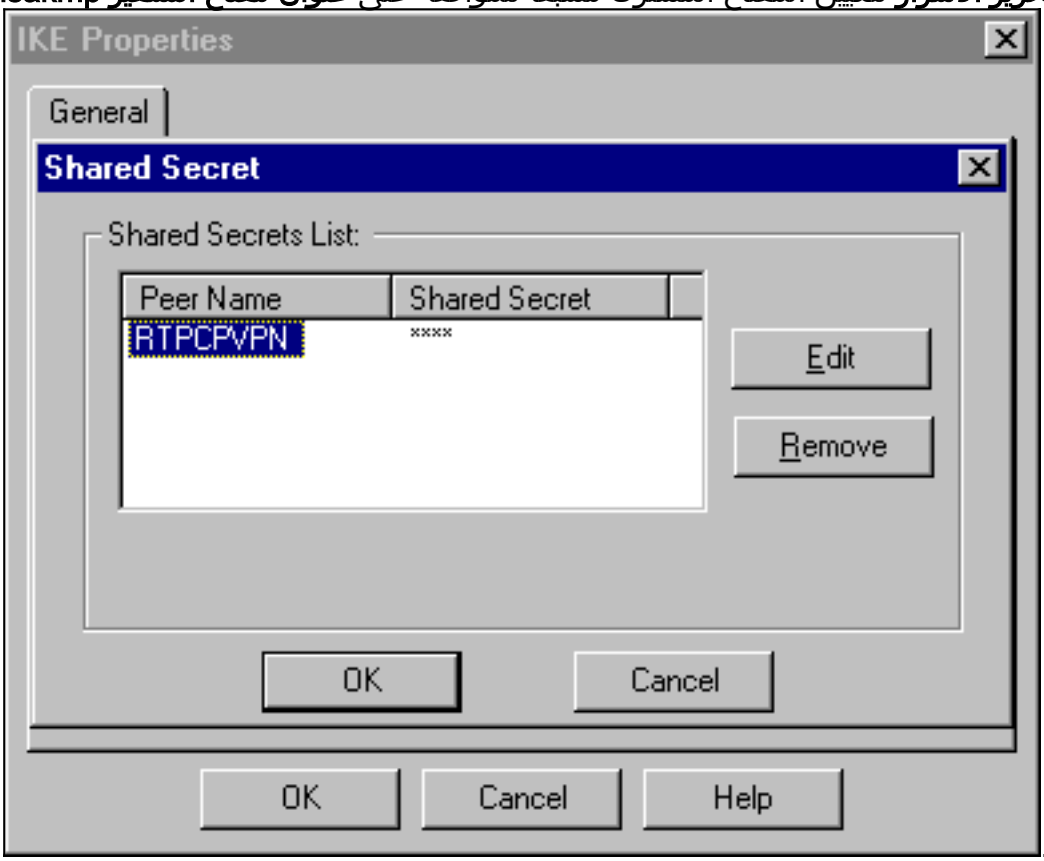
تحرير.

11. قم بتغيير تشفير DES لخصائص IKE للاتفاق مع الأوامر التالية:**سياسة التشفير ISAKMP #تشفير DES**
ملاحظة: تشفير DES هو الإعداد الافتراضي لذلك لا يكون مرئيا في تكوين Cisco.
12. قم بتغيير خصائص IKE إلى تجزئة SHA1 للاتفاق مع الأوامر التالية:**سياسة التشفير ISAKMP #تجزئة**
ملاحظة: خوارزمية تجزئة SHA هي الإعداد الافتراضي لذلك لا تكون مرئية في تكوين Cisco.تغيير هذه الإعدادات:عدم تحديد **الوضع المتداخل**.تحقق من **دعم الشبكات الفرعية**.تحقق من **سر مشترك مسبقا** تحت أسلوب المصادقة. هذا يوافق مع هذا أمر:**سياسة التشفير ISAKMP #مشاركة مسبقة**



للمصادقة

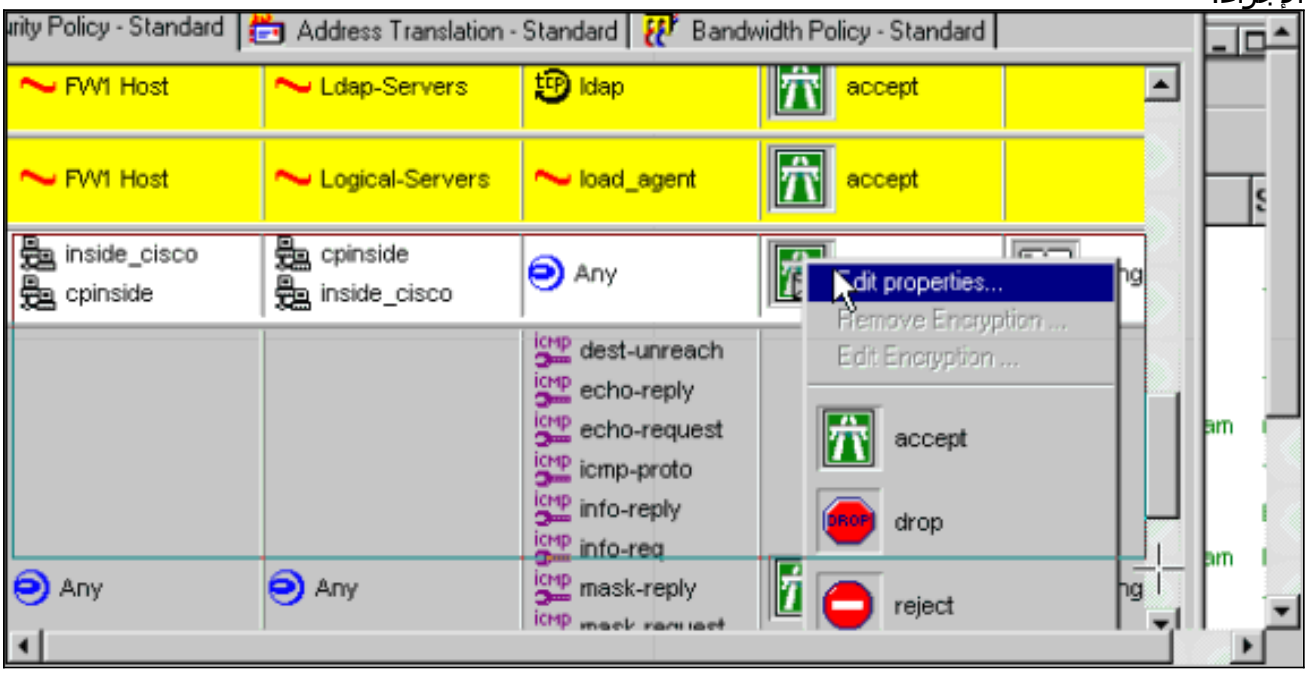
13. انقر فوق **تحرير الأسرار** لتعيين المفتاح المشترك مسبقا للموافقة على **عنوان مفتاح التشفير isakmp عنوان**



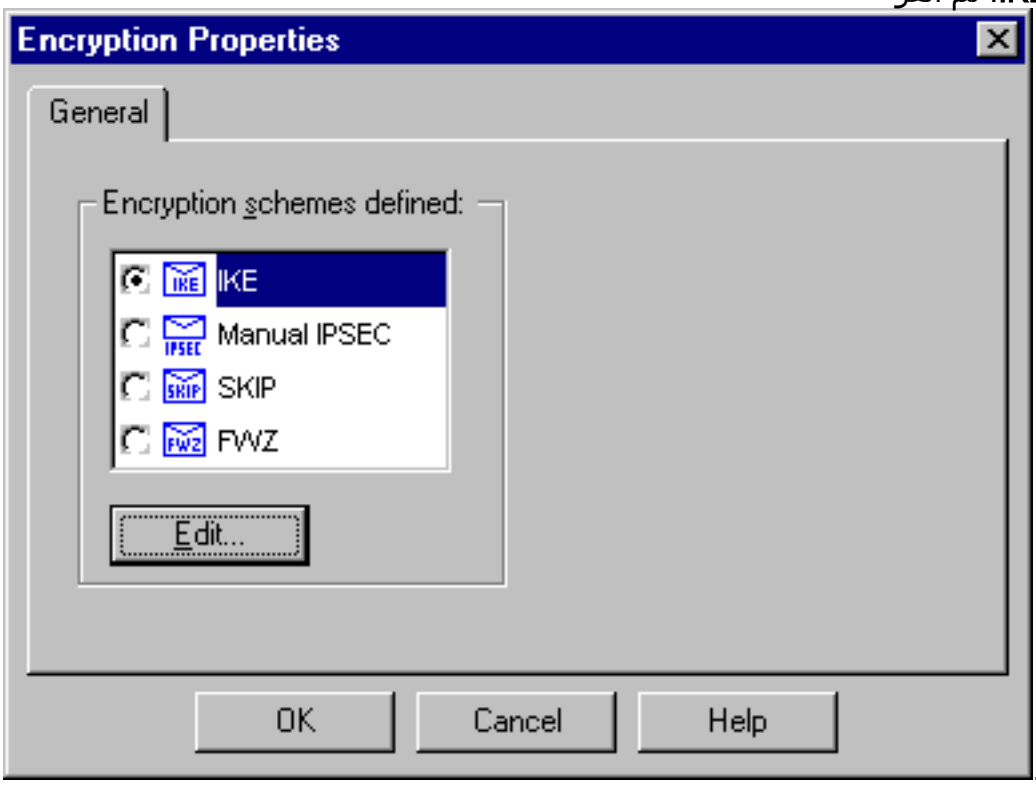
أمر Cisco.

14. 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**.

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

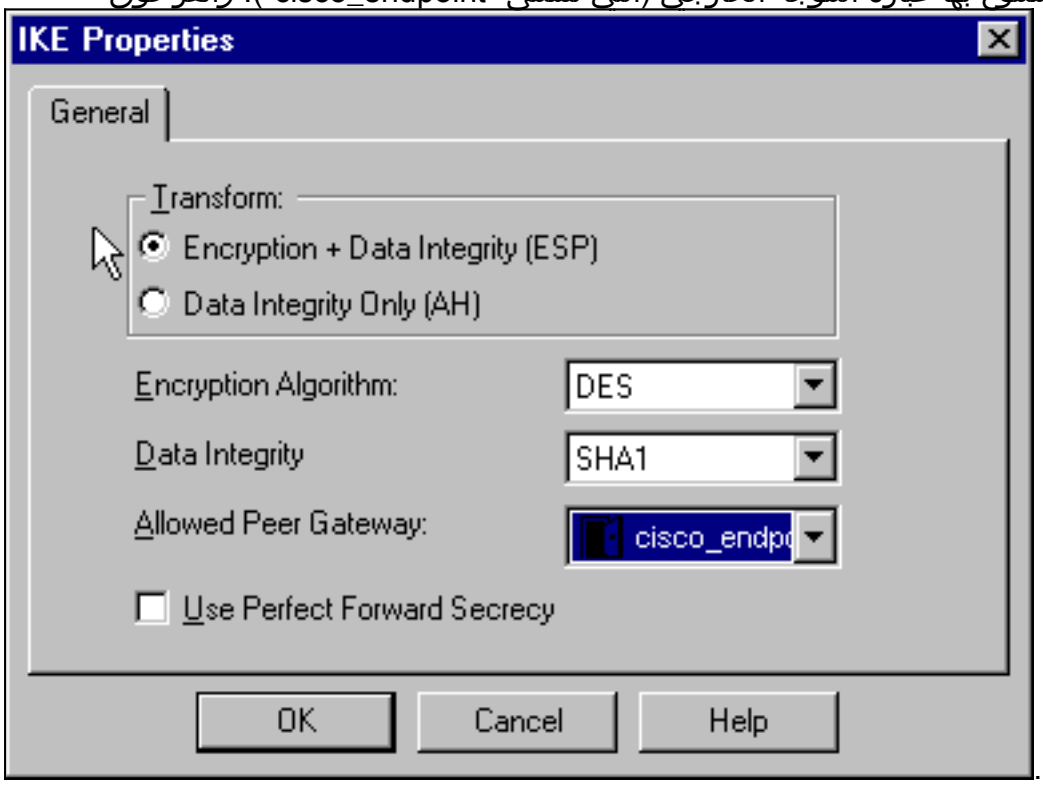


16. حدد **IKE**، ثم انقر



تحرير.

17. على نافذة خصائص IKE، قم بتغيير هذه الخصائص لتوافق مع تحويلات Cisco IPsec في أمر **crypto ips transform-set rtpset esp-des esp-sha-hmac**: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 الموجه الخارجي (التي تسمى "cisco_endpoint"). وانقر فوق OK.



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

التحقق من الصحة

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 isakmp sa**—عرض جميع اقترانات أمان IKE الحالية (SAs) في نظير.
- **show crypto ipSec**—عرض الإعدادات المستخدمة من قبل SAs الحالية.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

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

- **debug crypto engine**—يعرض رسائل تصحيح الأخطاء حول محركات التشفير، التي تقوم بالتشفير وفك التشفير.
- **debug crypto isakmp**—يعرض الرسائل المتعلقة بأحداث IKE.
- **debug crypto ipSec**—يعرض أحداث IPsec.
- **مسح التشفير isakmp**—مسح جميع إتصالات IKE النشطة.

- **مسح التشفير sa**—مسح جميع معرفات فئات المورد (SAs) ل IPsec.

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 الموجه 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.

نقطة تفتيش

نظرا لتعيين التعقب لفترة طويلة في نافذة محرر النهج، يجب أن تظهر حركة المرور المرفوضة باللون الأحمر في عارض السجل. يمكن الحصول على المزيد من تصحيح الأخطاء المطبعية مع:

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

وفي نافذة تانية:

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

ملاحظة: كان هذا تثبيت Microsoft Windows NT.

أصدرت هذا أمر أن يمسح SAs على 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** على السؤال هل أنت متأكد؟

إخراج تصحيح الأخطاء للعينة

```
Configuration register is 0x2102

cisco_endpoint#debug crypto isakmp
Crypto ISAKMP debugging is on
cisco_endpoint#debug crypto isakmp
Crypto IPSEC debugging is on
cisco_endpoint#debug crypto engine
Crypto Engine debugging is on
#cisco_endpoint
, :(IPSEC(sa_request :20:54:06
,key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157)
,(src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4
,(dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-des esp-sha-hmac
,lifedur= 3600s and 4608000kb
spi= 0xA29984CA(2727969994), conn_id= 0, keysize= 0, flags= 0x4004
(ISAKMP: received ke message (1/1 :20:54:06
ISAKMP: local port 500, remote port 500 :20:54:06
ISAKMP (0:1): beginning Main Mode exchange :20:54:06
ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_NO_STATE :20:54:06
ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_NO_STATE :20:54:06
```

```
                    ISAKMP (0:1): processing SA payload. message ID = 0 :20:54:06
      ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157 :20:54:06
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy :20:54:06
                                        ISAKMP:      encryption DES-CBC :20:54:06
                                                ISAKMP:      hash SHA :20:54:06
                                             ISAKMP:      default group 1 :20:54:06
                                              ISAKMP:      auth pre-share :20:54:06
                  ISAKMP (0:1): atts are acceptable. Next payload is 0 :20:54:06
                                    CryptoEngine0: generate alg parameter :20:54:06
                                      CRYPTO_ENGINE: Dh phase 1 status: 0 :20:54:06
                                      CRYPTO_ENGINE: Dh phase 1 status: 0 :20:54:06
             ISAKMP (0:1): SA is doing pre-shared key authentication :20:54:06
                                                  using id type ID_IPV4_ADDR
      ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_SA_SETUP :20:54:06
    ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_SA_SETUP :20:54:06
                    ISAKMP (0:1): processing KE payload. message ID = 0 :20:54:06
                                    CryptoEngine0: generate alg parameter :20:54:06
              ISAKMP (0:1): processing NONCE payload. message ID = 0 :20:54:06
    ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157 :20:54:06
                  CryptoEngine0: create ISAKMP SKEYID for conn id 1 :20:54:06
                                ISAKMP (0:1): SKEYID state generated :20:54:06
                                            ISAKMP (1): ID payload :20:54:06
                                                    next-payload : 8
                                                    type         : 1
                                                  protocol     : 17
                                                 port         : 500
                                                   length       : 8
                                ISAKMP (1): Total payload length: 12 :20:54:06
                    CryptoEngine0: generate hmac context for conn id 1 :20:54:06
      ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_KEY_EXCH :20:54:06
    ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_KEY_EXCH :20:54:06
                    ISAKMP (0:1): processing ID payload. message ID = 0 :20:54:06
                ISAKMP (0:1): processing HASH payload. message ID = 0 :20:54:06
                    CryptoEngine0: generate hmac context for conn id 1 :20:54:06
         ISAKMP (0:1): SA has been authenticated with 172.18.124.157 :20:54:06
    ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1855173267 :20:54:06
                    CryptoEngine0: generate hmac context for conn id 1 :20:54:06
          ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE :20:54:06
                            CryptoEngine0: clear dh number for conn id 1 :20:54:06
        ISAKMP (0:1): received packet from 172.18.124.157 (I) QM_IDLE :20:54:06
                    CryptoEngine0: generate hmac context for conn id 1 :20:54:06
      ISAKMP (0:1): processing HASH payload. message ID = 1855173267 :20:54:06
        ISAKMP (0:1): processing SA payload. message ID = 1855173267 :20:54:06
                                ISAKMP (0:1): Checking IPSec proposal 1 :20:54:06
                                            ISAKMP: transform 1, ESP_DES :20:54:06
                                       :ISAKMP:   attributes in transform :20:54:06
                                                  ISAKMP:      encaps is 1 :20:54:06
                                     ISAKMP:      SA life type in seconds :20:54:06
                           ISAKMP:      SA life duration (basic) of 3600 :20:54:06
                                    ISAKMP:      SA life type in kilobytes :20:54:06
               ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0 :20:54:06
                                    ISAKMP:      authenticator is HMAC-SHA :20:54:06
                                                  validate proposal 0 :20:54:06
                                       .ISAKMP (0:1): atts are acceptable :20:54:06
                    ,IPSEC(validate_proposal_request): proposal part #1 :20:54:06
                      ,key eng. msg.) dest= 172.18.124.157, src= 172.18.124.35)
                           ,(dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4
                           ,(src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4
                             , protocol= ESP, transform= esp-des esp-sha-hmac
                                                    ,lifedur= 0s and 0kb
                              spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
                                           validate proposal request 0 :20:54:06
      ISAKMP (0:1): processing NONCE payload. message ID = 1855173267 :20:54:06
        ISAKMP (0:1): processing ID payload. message ID = 1855173267 :20:54:06
```

```
ISAKMP (0:1): processing ID payload. message ID = 1855173267 :20:54:06
          CryptoEngine0: generate hmac context for conn id 1 :20:54:06
                                    ipsec allocate flow 0 :20:54:06
                                    ipsec allocate flow 0 :20:54:06
                           ISAKMP (0:1): Creating IPSec SAs :20:54:06
    inbound SA from 172.18.124.157 to 172.18.124.35         :20:54:06
                            (proxy 10.32.50.0 to 192.168.1.0)
    has spi 0xA29984CA and conn_id 2000 and flags 4         :20:54:06
                           lifetime of 3600 seconds         :20:54:06
                       lifetime of 4608000 kilobytes        :20:54:06
  outbound SA from 172.18.124.35   to 172.18.124.157        :20:54:06
                                 (proxy 192.168.1.0 to 10.32.50.0)
     has spi 404516441 and conn_id 2001 and flags 4         :20:54:06
                           lifetime of 3600 seconds         :20:54:06
                       lifetime of 4608000 kilobytes        :20:54:06
  ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE :20:54:06
"" ISAKMP (0:1): deleting node 1855173267 error FALSE reason :20:54:06
                    ...IPSEC(key_engine): got a queue event :20:54:06
                                    , :(IPSEC(initialize_sas :20:54:06
           ,key eng. msg.) dest= 172.18.124.35, src= 172.18.124.157)
               ,(dest_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4
                 ,(src_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4
                  , protocol= ESP, transform= esp-des esp-sha-hmac
                                    ,lifedur= 3600s and 4608000kb
spi= 0xA29984CA(2727969994), conn_id= 2000, keysize= 0, flags= 0x4
                                    , :(IPSEC(initialize_sas :20:54:06
           ,key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157)
                ,(src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4
                ,(dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4
                  , protocol= ESP, transform= esp-des esp-sha-hmac
                                    ,lifedur= 3600s and 4608000kb
 spi= 0x181C6E59(404516441), conn_id= 2001, keysize= 0, flags= 0x4
                                ,IPSEC(create_sa): sa created :20:54:06
                             ,sa) sa_dest= 172.18.124.35, sa_prot= 50)
                                    ,(sa_spi= 0xA29984CA(2727969994
                  sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2000
                                ,IPSEC(create_sa): sa created :20:54:06
                            ,sa) sa_dest= 172.18.124.157, sa_prot= 50)
                                    ,(sa_spi= 0x181C6E59(404516441
                  sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2001
                                       cisco_endpoint#sho cry ips sa

                                                interface: Ethernet0/0
                      Crypto map tag: rtp, local addr. 172.18.124.35

(local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0
 (remote ident (addr/mask/prot/port): (10.32.50.0/255.255.255.0/0/0
                                       current_peer: 172.18.124.157
                                    {,PERMIT, flags={origin_is_acl
                pkts encaps: 14, #pkts encrypt: 14, #pkts digest 14#
                pkts decaps: 14, #pkts decrypt: 14, #pkts verify 14#
                          pkts compressed: 0, #pkts decompressed: 0#
                     ,pkts not compressed: 0, #pkts compr. failed: 0#
           pkts decompress failed: 0, #send errors 1, #recv errors 0#

local crypto endpt.: 172.18.124.35, remote crypto endpt.: 172.18.124.157
                                    path mtu 1500, media mtu 1500
                                   current outbound spi: 181C6E59

                                                 :inbound esp sas
                                     (spi: 0xA29984CA(2727969994
                                , transform: esp-des esp-sha-hmac
                                     { ,in use settings ={Tunnel
                slot: 0, conn id: 2000, flow_id: 1, crypto map: rtp
```

```
:(More--                sa timing: remaining key lifetime (k/sec--
                                                (4607998/3447)
                                        IV size: 8 bytes
                                replay detection support: Y

                                                :inbound ah sas

                                                :inbound pcp sas

                                                :outbound esp sas
                                            (spi: 0x181C6E59(404516441
                                    , transform: esp-des esp-sha-hmac
                                        { ,in use settings ={Tunnel
              slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp
        (sa timing: remaining key lifetime (k/sec): (4607997/3447
                                        IV size: 8 bytes
                                replay detection support: Y

                                                :outbound ah sas

                                                :outbound pcp sas


                                    cisco_endpoint#show crypto isakmp sa
          dst             src             state          conn-id   slot
           QM_IDLE           1       0  172.18.124.35 172.18.124.157

                                                cisco_endpoint#exit
```

معلومات ذات صلة

- مفاوضة IPSec/بروتوكولات IKE
- تكوين أمان شبكة IPsec
- تكوين بروتوكول أمان Internet Key Exchange
- 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).