

# نم نم آل PIX ةي امح راج - IPsec ق فن ني وكت 4.1 لوصول ا ةطقن ةي امح راج ل Cisco

## المحتويات

<a href="#">المقدمة</a>
<a href="#">المتطلبات الأساسية</a>
<a href="#">المتطلبات</a>
<a href="#">المكونات المستخدمة</a>
<a href="#">الاصطلاحات</a>
<a href="#">التكوين</a>
<a href="#">الرسم التخطيطي للشبكة</a>
<a href="#">التكوينات</a>
<a href="#">جدار حماية نقطة التحقق</a>
<a href="#">أوامر show و clear debug</a>
<a href="#">جدار حماية Cisco PIX</a>
<a href="#">نقطة التفتيش:</a>
<a href="#">استكشاف الأخطاء وإصلاحها</a>
<a href="#">تلخيص الشبكة</a>
<a href="#">إخراج تصحيح الأخطاء للعبئة من PIX</a>
<a href="#">معلومات ذات صلة</a>

## المقدمة

يوضح هذا التكوين النموذجي كيفية تكوين نفق IPsec بمفاتيح مشتركة مسبقا للانضمام إلى شبكتين خاصتين. في مثالنا، الشبكات المرتبطة هي الشبكة الخاصة x.192.168.1 داخل جدار حماية PIX الآمن من Cisco (PIX) والشبكة الخاصة x.10.32.50 داخل نقطة التفتيش. من المفترض أن حركة المرور من داخل PIX وداخل جدار حماية نقطة التفتيش 4.1 إلى الإنترنت (ممثلة هنا بشبكات x.172.18.124) تتدفق قبل بدء 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:

- برنامج PIX الإصدار 5.3.1
- 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.](#)

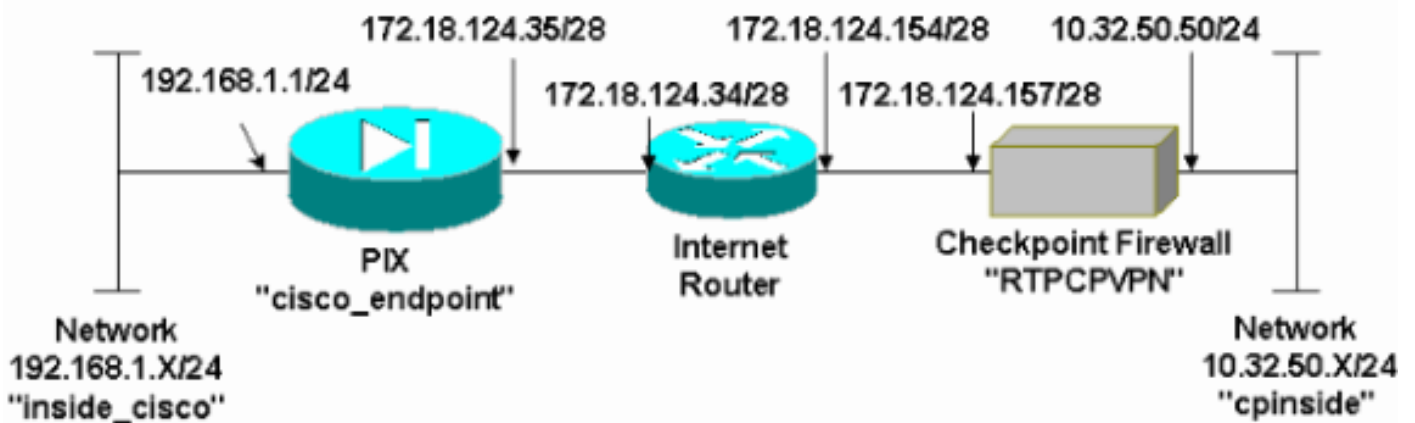
## التكوين

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

**ملاحظة:** للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، استخدم [أداة بحث الأوامر \(للعلماء المسجلين فقط\)](#).

## الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في هذا الرسم التخطيطي:



## التكوينات

يستخدم هذا المستند التكوينات الموضحة في هذا القسم.

```
تكوين PIX

(PIX Version 5.3(1
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname cisco_endpoint
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
access-list 115 permit ip 192.168.1.0 255.255.255.0
```

```

255.255.255.0 10.32.50.0
access-list 115 deny ip 192.168.1.0 255.255.255.0 any
    pager lines 24
    logging on
    no logging timestamp
    no logging standby
    no logging console
    logging monitor debugging
    no logging buffered
    logging trap debugging
    no logging history
    logging facility 20
    logging queue 512
    interface ethernet0 auto
    interface ethernet1 auto
    mtu outside 1500
    mtu inside 1500
    ip address outside 172.18.124.35 255.255.255.240
    ip address inside 192.168.1.1 255.255.255.0
    ip audit info action alarm
    ip audit attack action alarm
    no failover
    failover timeout 0:00:00
    failover poll 15
    failover ip address outside 0.0.0.0
    failover ip address inside 0.0.0.0
    arp timeout 14400
    global (outside) 1 172.18.124.36
    nat (inside) 0 access-list 115
    nat (inside) 1 0.0.0.0 0.0.0.0 0 0
    route outside 0.0.0.0 0.0.0.0 172.18.124.34 1
    timeout xlate 3:00:00g SA 0x80bd6a10, conn_id = 0
    timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
        0:10:00 h323
    sip 0:30:00 sip_media 0:02:00 0:05:00
    timeout uauth 0:05:00 absolute
    +aaa-server TACACS+ protocol tacacs
    aaa-server RADIUS protocol radius
    no snmp-server location
    no snmp-server contact
    snmp-server community public
    no snmp-server enable traps
    floodguard enable
IPSec configuration sysopt connection permit-ipsec ---!
    no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-sha-hmac
    crypto map rtpmap 10 ipsec-isakmp
    crypto map rtpmap 10 match address 115
    crypto map rtpmap 10 set peer 172.18.124.157
    crypto map rtpmap 10 set transform-set myset
crypto map rtpmap 10 set security-association lifetime
    seconds
    kilobytes 4608000 3600
    crypto map rtpmap interface outside
IKE configuration isakmp enable outside ---!
isakmp key ***** address 172.18.124.157 netmask
    255.255.255.240
    isakmp identity address
isakmp policy 10 authentication pre-share
    isakmp policy 10 encryption des
    isakmp policy 10 hash sha
    isakmp policy 10 group 1
    isakmp policy 10 lifetime 86400
    telnet timeout 5

```

```
ssh timeout 5
terminal width 80
Cryptochecksum:dc43c44e4513d3633a3fc7b1c3802c79
end :
[OK]
```

## جدار حماية نقطة التحقق

1. ونظرا لأن فترات الحياة الافتراضية لكل من IKE و IPsec تختلف بين الموردين، فحدد خصائص < تشفير لتعيين فترات الحياة الافتراضية لنقطة الوصول للاتفاق مع إعدادات PIX الافتراضية. مدة بقاء IKE الافتراضية ل PIX هي 86400 ثانية (=1440 دقيقة)، قابلة للتعديل بواسطة هذا الأمر: نهج ISAKMP # مدى الحياة 86400 يمكن تكوين العمر الافتراضي ل PIX IKE بين 60 و 86400 ثانية. مدة بقاء IPsec الافتراضية ل PIX هي 28800 ثانية، قابلة للتعديل بواسطة هذا الأمر: ثواني العمر الافتراضي لاقتران أمان IPsec ل crypto ipsec # يمكنك تكوين عمر PIX IPsec بين 120 و 86400

**Properties Setup**

High Availability | IP Pool NAT | Access Lists | Desktop Security

Security Policy | Traffic Control | Services | Log and Alert | Security Servers

Authentication | SYNDefender | LDAP | Encryption | ConnectControl

SKIP

Enable Exportable SKIP

Change SKIP Session Key :

Every 120 Seconds (0 for infinity)

or

Every 10485760 Bytes (0 for infinity)

Manual IPSEC

SPI allocation range (hex):

From 100

To ffff

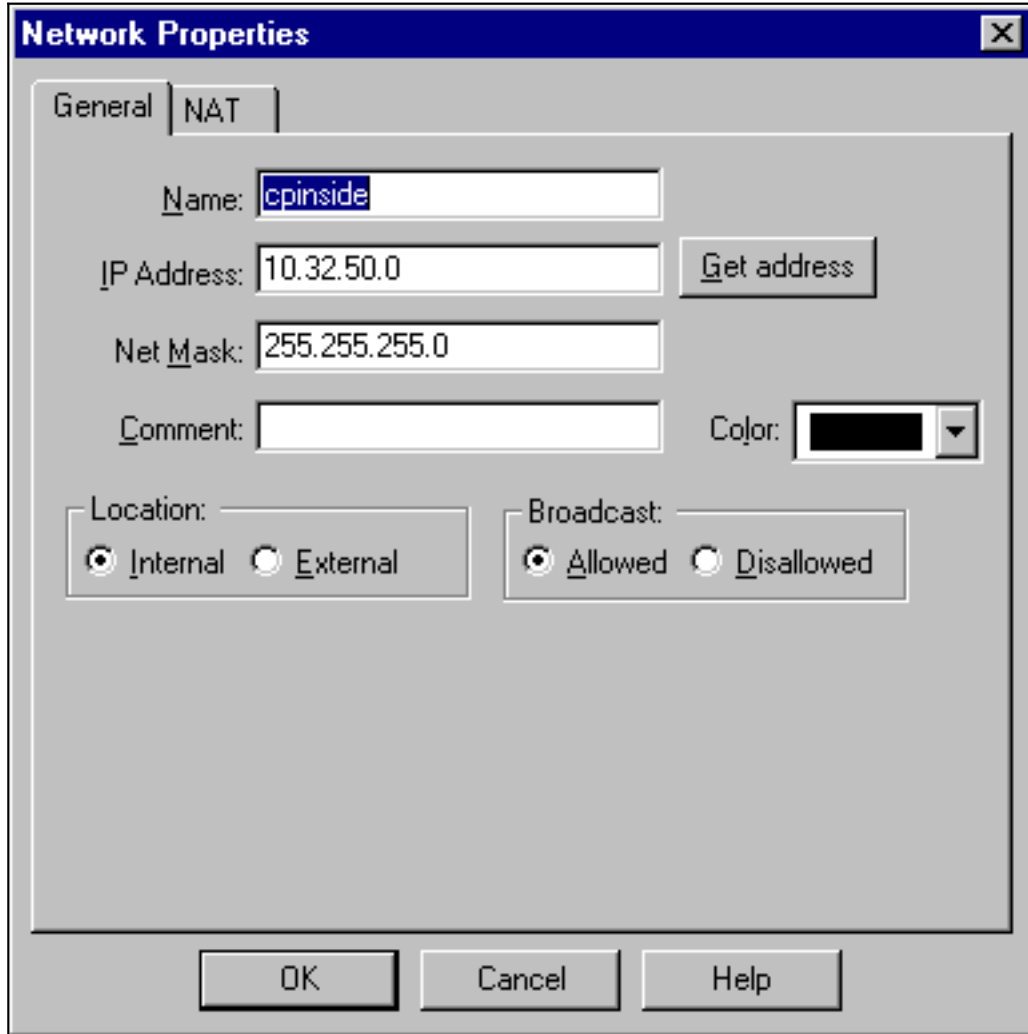
IKE

Renegotiate IKE Security Associations every 1440 minutes

Renegotiate IPSEC Security Associations every 28800 seconds

OK Cancel Help

2. حدد إدارة<كائنات الشبكة>جديد (أو تحرير)<الشبكة لتكوين الكائن لشبكة ("CPINSIDE") الداخلية خلف نقطة التفتيش. يجب أن يتوافق هذا مع شبكة الوجهة (الثانية) في الأمر PIX: access-list 115 allowed ip 192.168.1.0 255.255.255.0 10.32.50.0



The screenshot shows the 'Network Properties' dialog box with the 'NAT' tab selected. The 'Name' field contains 'cpinside'. The 'IP Address' field contains '10.32.50.0' and the 'Net Mask' field contains '255.255.255.0'. The 'Location' section has 'Internal' selected with a radio button. The 'Broadcast' section has 'Allowed' selected with a radio button. There are 'OK', 'Cancel', and 'Help' buttons at the bottom.

255.255.255.0

3. حدد إدارة<كائنات الشبكة>تحرير لتحرير الكائن لنقطة النهاية للبوابة ("RTPCPVPN") التي يشير إليها PIX في هذا الأمر: اسم خريطة التشفير # تعيين النظير ip\_address تحت الموقع، حدد داخلي. للنوع، حدد البوابة. تحت الوحدات المثبتة، حدد خانة الاختيار VPN-1 و Firewall-1، ثم حدد أيضا خانة الاختيار محطة

**Workstation Properties**

General | Interfaces | SNMP | NAT | Certificates | VPN | Auth

Name:

IP Address:

Comment:

Location:  Internal  External

Type:  Host  Gateway

Modules Installed

<input checked="" type="checkbox"/> VPN-1 & FireWall-1	Version: <input type="text" value="4.1"/>	<input type="button" value="Get"/>
<input type="checkbox"/> FloodGate-1	Version: <input type="text" value="4.1"/>	
<input type="checkbox"/> Compression	Version: <input type="text" value="4.1"/>	

Management Station      Color:

الإدارة:

4. حدد إدارة <كائنات الشبكة> <جديد> الشبكة لتكوين الكائن للشبكة الخارجية ("inside\_cisco") خلف PIX. يجب أن يتوافق هذا مع شبكة المصدر (أولا) في هذا الأمر PIX: `access-list 115 ip 192.168.1.0 255.255.255.0 10.32.50.0`

**Network Properties**

General | NAT

Name:

IP Address:

Net Mask:

Comment:

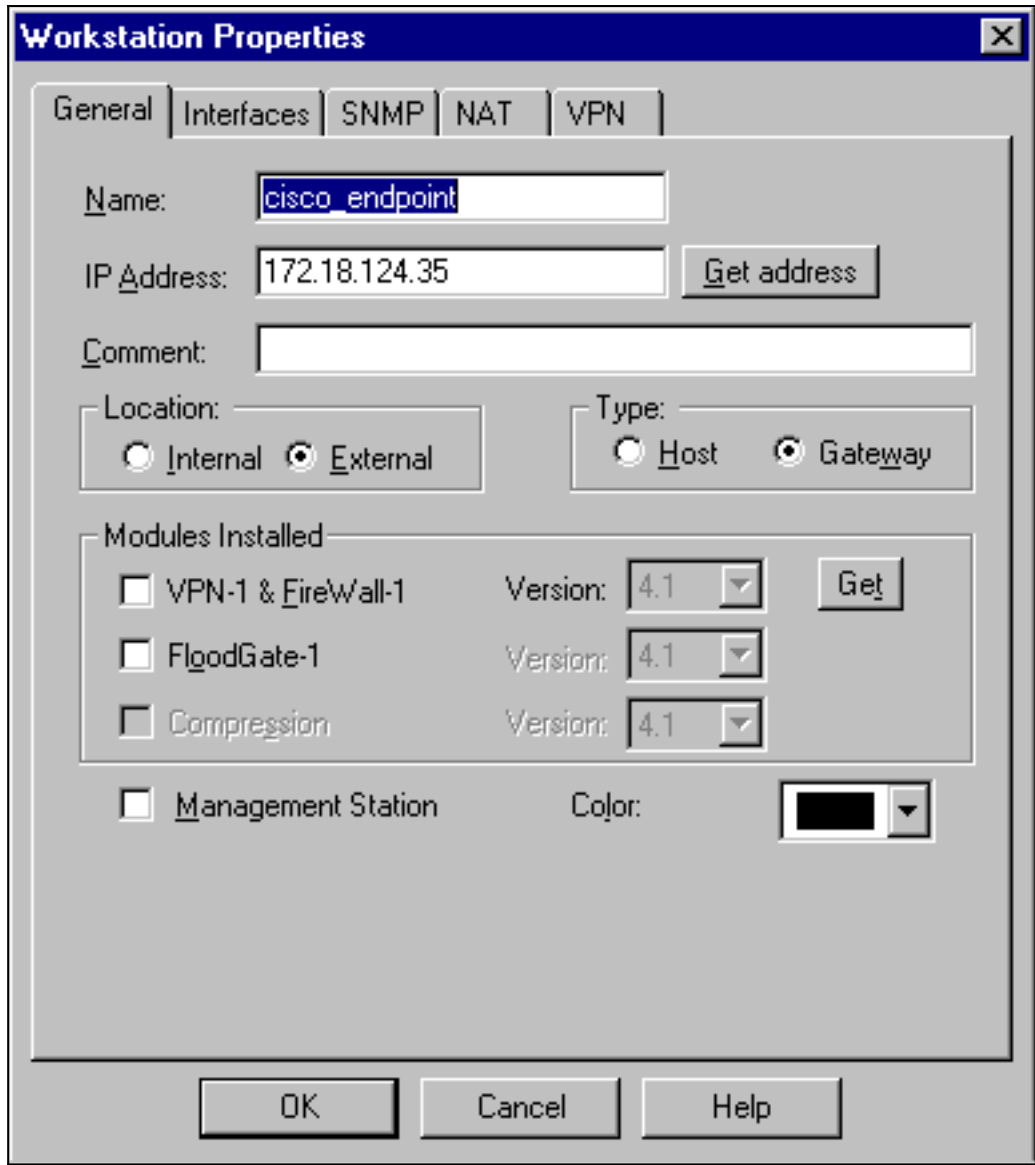
Color:

Location:  Internal  External

Broadcast:  Allowed  Disallowed

255.255.255.0

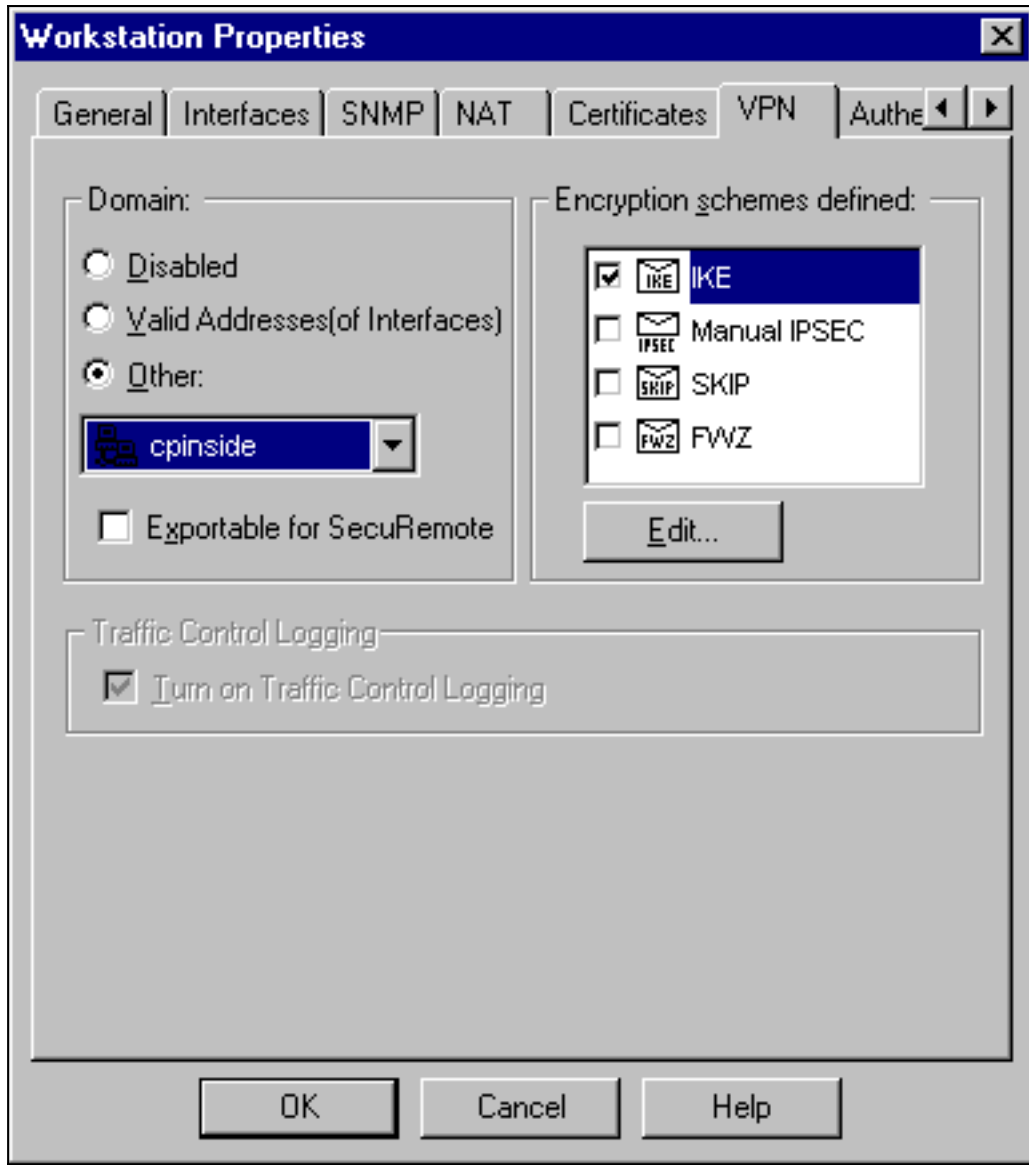
5. حدد إدارة <كائنات الشبكة> جديد <محطة عمل لإضافة كائن لبوابة PIX الخارجية ("Cisco\_endpoint"). هذه هي واجهة PIX التي يتم تطبيق هذا الأمر عليها: واجهة اسم خريطة التشفير الخارجية تحت الموقع، حدد خارجي. للنوع، حدد البوابة. ملاحظة: لا تحدد خانة الاختيار -VPN-1/FireWall



.1

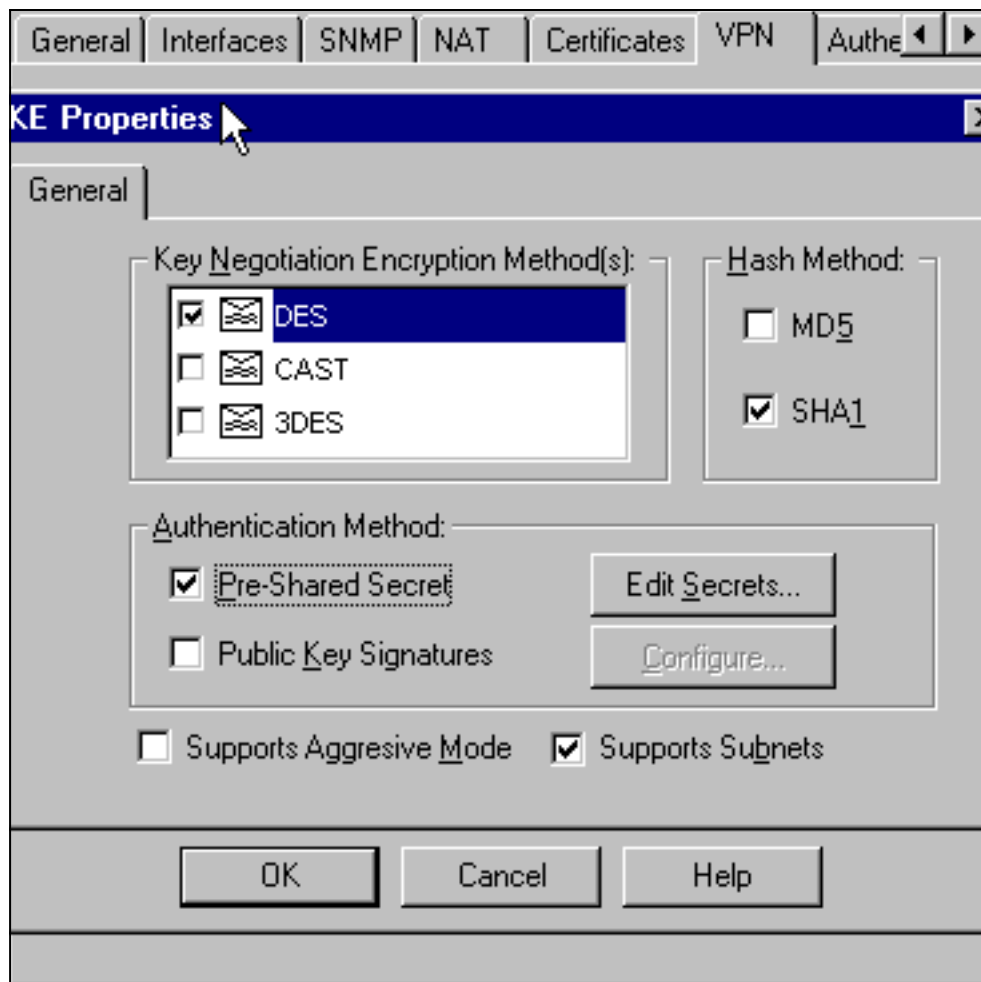
6. حدد إدارة < كائنات الشبكة > تحرير لتحرير نقطة نهاية عبارة نقطة التحقق (تسمى "RTPCPVPN") لعلامة التويب VPN. تحت المجال، حدد آخر ثم حدد داخل شبكة نقطة التفتيش (والتي تسمى "cpinside") من القائمة المنسدلة. تحت تشفير نظام يعين، حدد IKE، ثم انقر





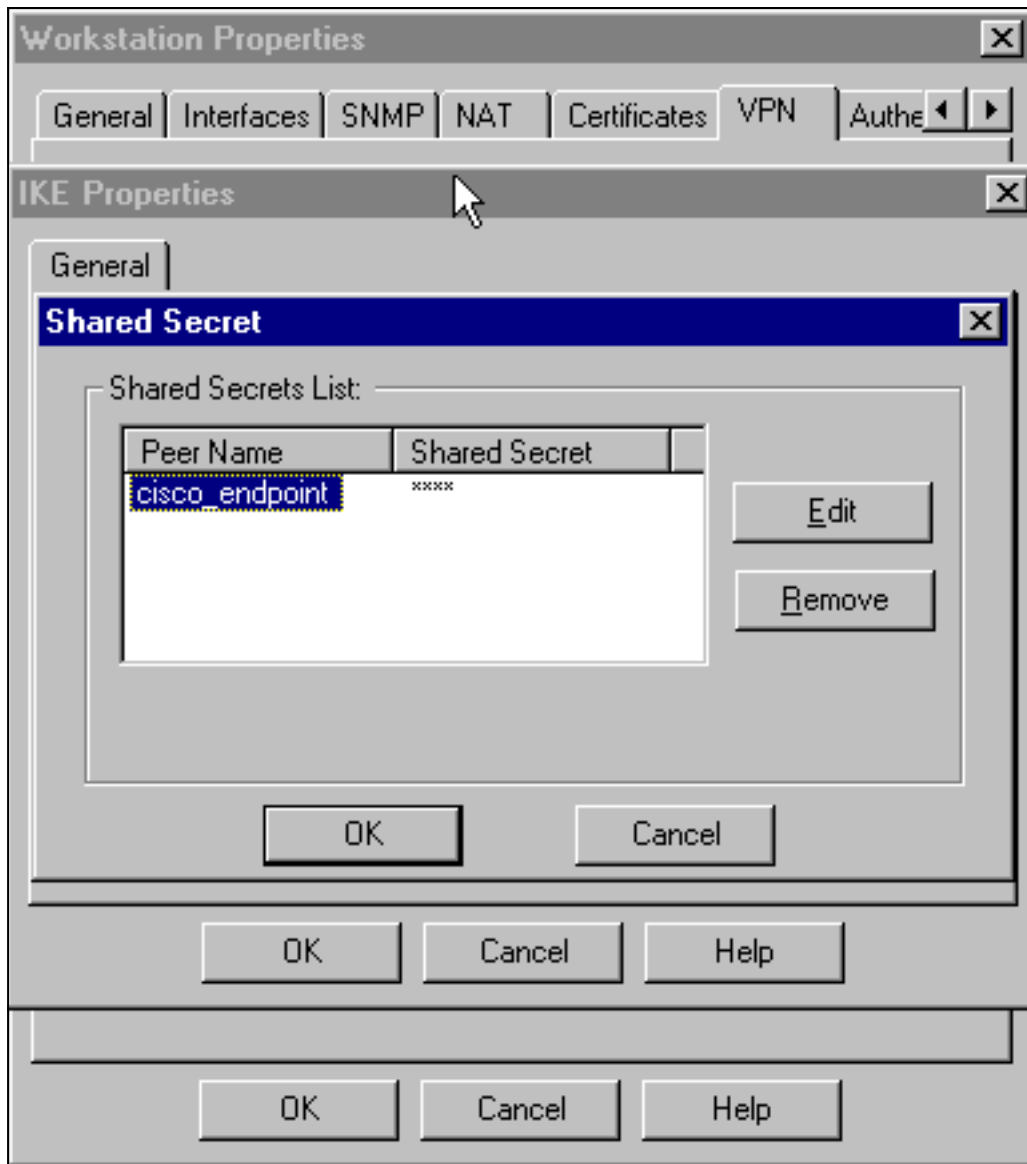
تحرير.

7. قم بتغيير خصائص IKE لتشفير DES لتوافق مع هذا الأمر: سياسة ISAKMP # تشفير des
8. قم بتغيير خصائص IKE إلى تجزئة SHA1 للاتفاق مع هذا الأمر: سياسة ISAKMP # hash SHA لتغيير هذه الإعدادات: عدم تحديد الوضع المتداخل. حدد خانة الاختيار شبكات الدعم الفرعية. تحت أسلوب المصادقة، حدد خانة الاختيار سر مشترك مسبقا. وهذا يتفق مع هذا الأمر: المشاركة المسبقة لسياسة # مصادقة



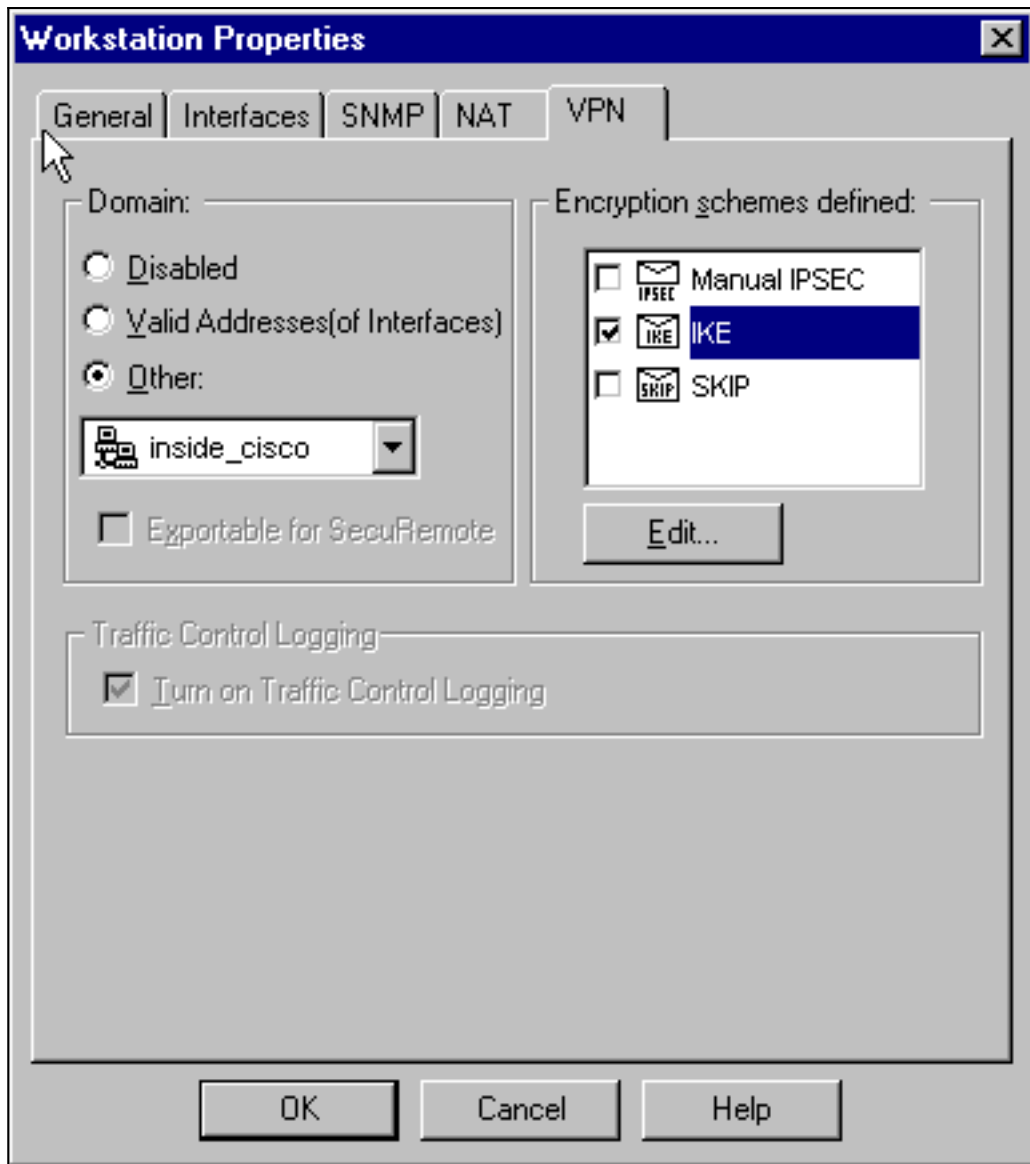
ISAKMP

9. انقر على تحرير الأسرار لتعيين المفتاح المشترك مسبقا للاتفاق مع أمر PIX: قناع الشبكة الخاص بعنوان مفتاح



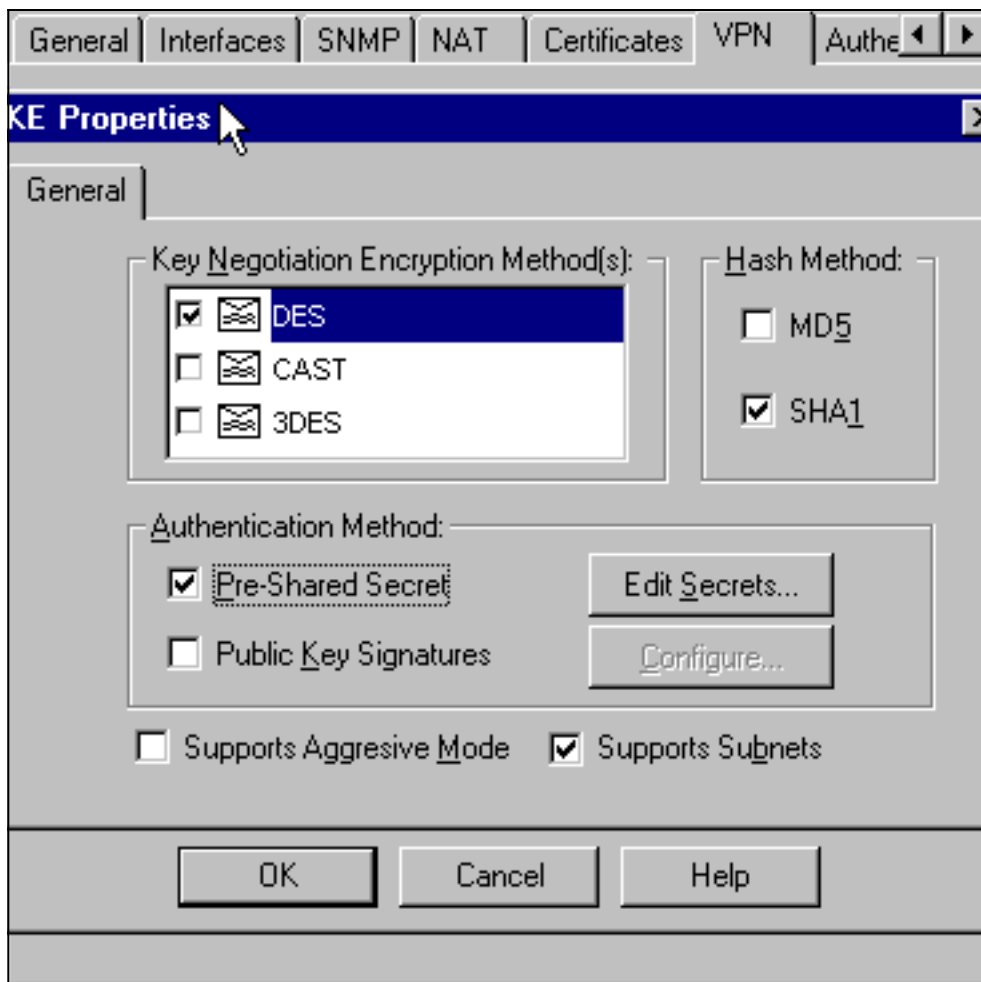
ISAKMP

10. حدد إدارة < كائنات الشبكة > تحرير لتحرير علامة التوبيو "VPN" Cisco\_Endpoint. تحت المجال، حدد آخر، ثم حدد داخل شبكة PIX (المسماة "inside\_cisco"). تحت تشفير نظام يعين، حدد IKE، ثم انقر



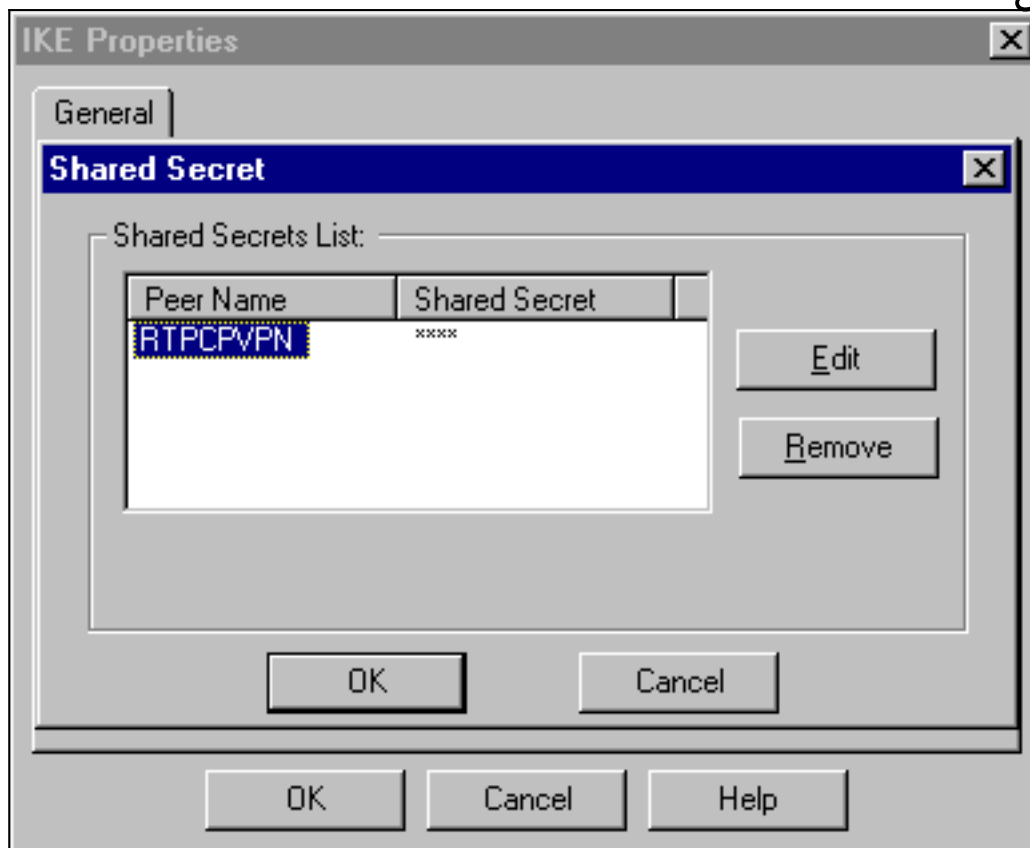
تحرير.

11. تغيير تشفير DES لخصائص IKE للاتفاق مع هذا الأمر: سياسة ISAKMP # تشفير des
12. قم بتغيير خصائص IKE إلى تجزئة SHA1 للاتفاق مع هذا الأمر: نهج التشفير SHA # hash ISAKMP تغيير  
هذه الإعدادات: عدم تحديد الوضع المتداخل. حدد خانة الاختيار شبكات الدعم الفرعية. تحت أسلوب المصادقة،  
حدد خانة الاختيار سر مشترك مسبقا. يتوافق هذا الإجراء مع هذا الأمر: المشاركة المسبقة لسياسة # مصادقة



ISAKMP

13. انقر فوق تحرير الأسرار لتعيين المفتاح المشترك مسبقا للموافقة على أمر PIX هذا: قناع الشبكة الخاص بعنوان مفتاح

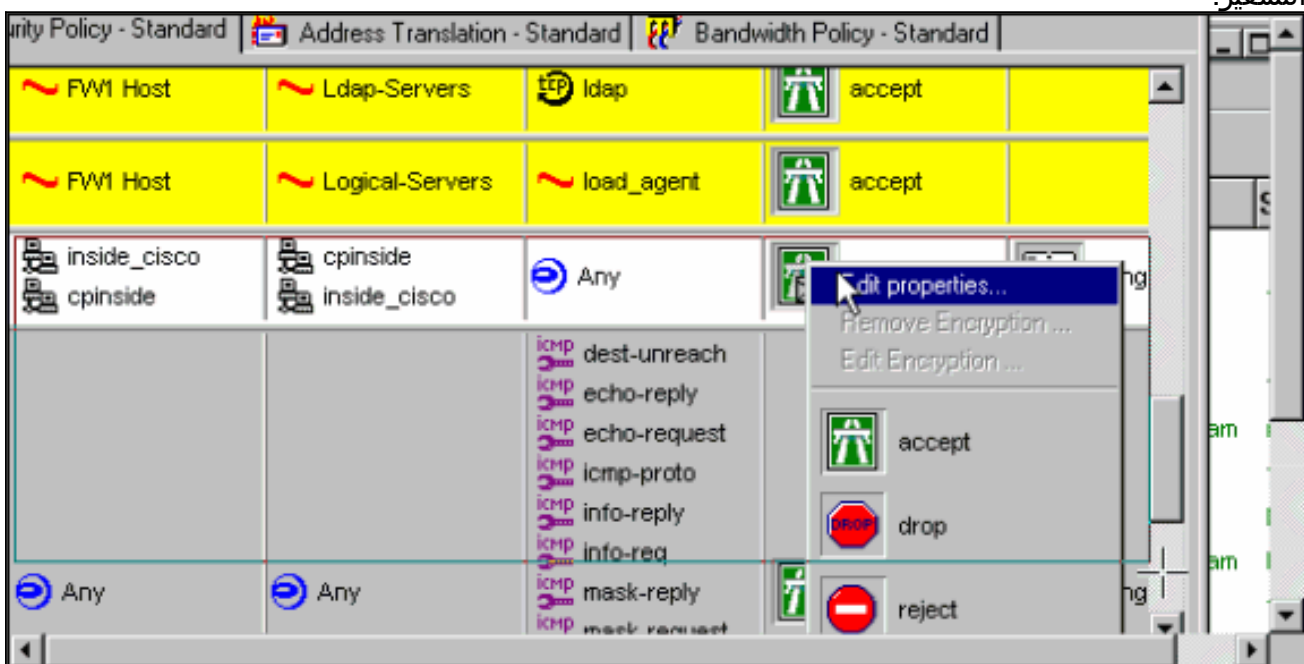


ISAKMP

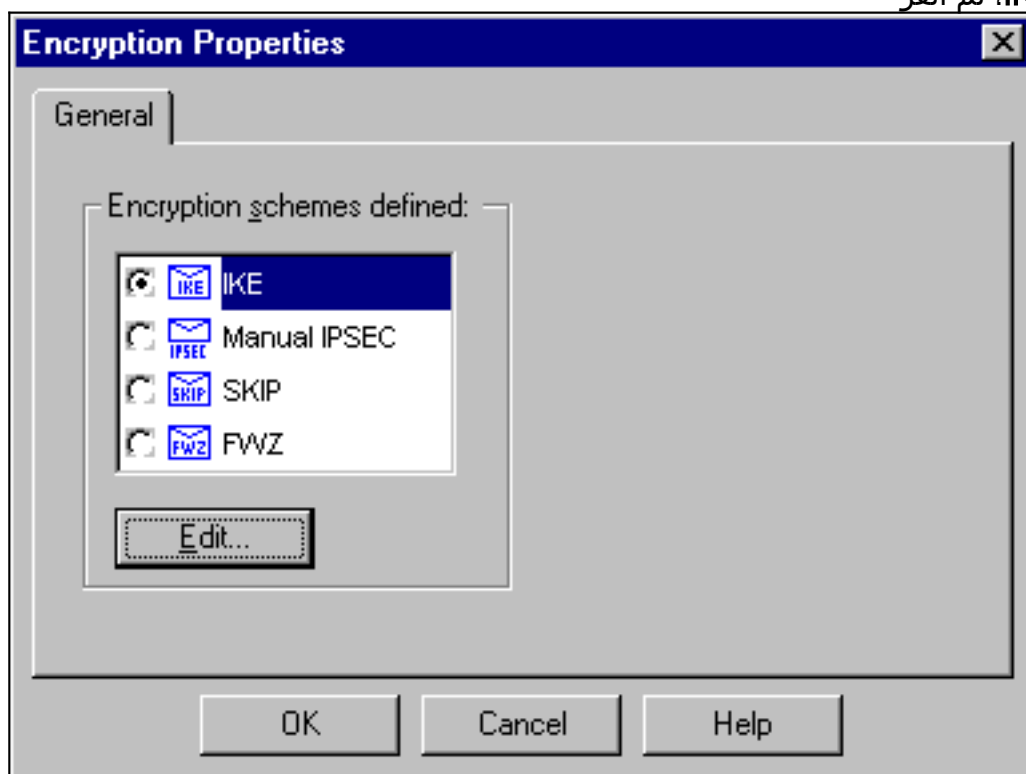
14. في نافذة "محرر النهج"، قم بإدراج قاعدة بكل من "المصدر والوجهة" و"inside\_cisco" و"cpinside" (ثاني الإتيان).  
 ،set service=any، action=encrypt، track=longo.



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

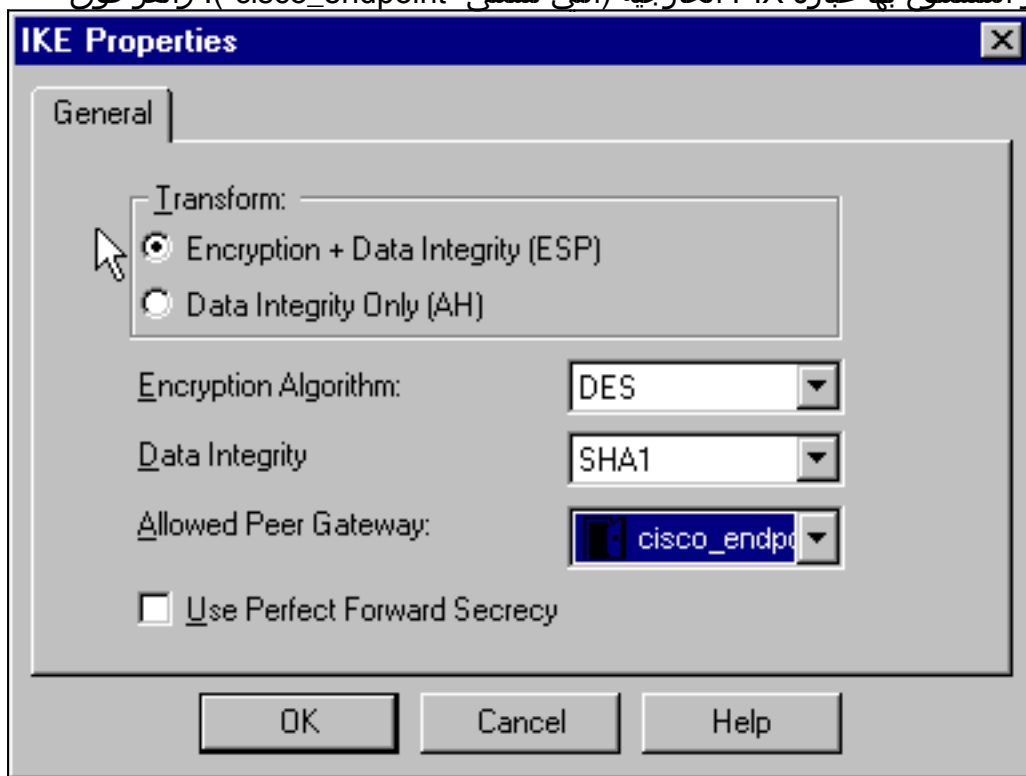


16. حدد IKE، ثم انقر



تحرير

17. على شاشة خصائص IKE، قم بتغيير هذه الخصائص لتوافق مع تحويلات PIX IPsec في هذا الأمر: `crypto ipsec transform-set myset esp-des esp-sha-hmac` حدد التشفير + تكامل البيانات (ESP). يجب أن تكون خوارزمية التشفير DES، ويجب أن تكون تكامل البيانات SHA1، ويجب أن تكون عبارة النظير المسموح بها عبارة PIX الخارجية (التي تسمى "cisco\_endpoint"). وانقر فوق



OK

18. بعد تكوين نقطة التحقق، حدد نهج < تثبيت في قائمة نقطة التفتيش لكي تصبح التغييرات نافذة المفعول.

## أوامر show و clear debug

يوفر هذا القسم معلومات يمكنك استخدامها 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.

قبل إصدار أوامر تصحيح الأخطاء، راجع المعلومات المهمة في أوامر تصحيح الأخطاء.

## جدار حماية Cisco PIX

- `debug crypto engine`—عرض رسائل تصحيح الأخطاء حول محركات التشفير، التي تقوم بالتشفير وفك التشفير.
- `debug crypto isakmp`—عرض الرسائل حول أحداث IKE.
- `debug crypto ipsec`—عرض أحداث IPsec.
- `show crypto isakmp sa`—عرض جميع اقترانات أمان IKE الحالية (SAs) في نظير.
- `show crypto ipsec`—عرض الإعدادات المستخدمة من قبل اقترانات الأمان الحالية.
- مسح التشفير `isakmp sa`—(من وضع التكوين) مسح جميع اتصالات IKE النشطة.
- مسح تشفير IPsec—(من وضع التكوين) احذف جميع اقترانات أمان IPsec.

## نقطة التفتيش:

نظرا لتعيين التعقب لمدة طويلة في نافذة محرر النهج الموضحة في الخطوة 14، تظهر حركة المرور المرفوضة باللون

الأحمر في عارض السجل. يمكن الحصول على تصحيح أخطاء أكثر تفصيلا من خلال إدخال:

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

وفي نافذة ثانية:

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

**ملاحظة:** كان هذا تثبيت Microsoft Windows NT.

يمكنك مسح أسماء المجالات (SAs) على نقطة التفتيش باستخدام الأوامر التالية:

```
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
```

و عم يرد بنعم عند هل انت متأكد ؟ متأهب.

## استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

### تليخيص الشبكة

عند تكوين شبكات داخلية متعددة متجاورة في مجال التشفير على نقطة التحقق، يمكن للجهاز تليخيصها تلقائيا فيما يتعلق بحركة المرور المفيدة. إذا لم يتم تكوين قائمة التحكم في الوصول للتشفير على PIX للمطابقة، فمن المحتمل أن يفشل النفق. على سبيل المثال، إذا تم تكوين الشبكات الداخلية من 24/ 10.0.0.0 و 24/ 10.0.1.0 لتضمينها في النفق، فيمكن تليخيصها إلى 23/ 10.0.0.0.

### إخراج تصحيح الأخطاء للعبئة من PIX

```
cisco_endpoint# show debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
debug fover status
tx Off
rx Off
open Off
cable Off
txdmp Off
rxdmp Off
ifc Off
rxip Off
txip Off
get Off
put Off
verify Off
```



```

switch Off
fail Off
fmsg Off
cisco_endpoint# term mon
#cisco_endpoint
,ISAKMP (0): beginning Quick Mode exchange
:(M-ID of 2112882468:7df00724IPSEC(key_engine
...got a queue event
IPSEC(spi_response): getting spi 0x9d71f29c(2641490588) for SA
from 172.18.124.157 to 172.18.124.35 for prot 3
70
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.35
OAK_QM exchange
:oakley_process_quick_mode
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 2112882468

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_DES
:ISAKMP: attributes in transform
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 28800
ISAKMP: SA life type in kilobytes
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP: authenticator is HMAC-SHA
:(ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request
,proposal part #1
,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

ISAKMP (0): processing NONCE payload. message ID = 2112882468

ISAKMP (0): processing ID payload. message ID = 2112882468
:ISAKMP (0): processing ID payload. message ID = 2112882468map_alloc_entry
allocating entry 3
map_alloc_entry: allocating entry 4

ISAKMP (0): Creating IPsec SAs
inbound SA from 172.18.124.157 to 172.18.124.35 (proxy
(to 192.168.1.0 10.32.50.0
has spi 2641490588 and conn_id 3 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytes
outbound SA from 172.18.124.35 to 172.18.124.157 (proxy
(to 10.32.50.0 192.168.1.0
has spi 3955804195 and conn_id 4 and flags 4
lifetime of 28800 seconds
...lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event
, :(IPSEC(initialize_sas
,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= 28800s and 4608000kb
spi= 0x9d71f29c(2641490588), conn_id= 3, keysize= 0, flags= 0x4
, :(IPSEC(initialize_sas
,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= 28800s and 4608000kb
spi= 0xebc8c823(3955804195), conn_id= 4, keysize= 0, flags= 0x4

(.return status is IKMP_NO_ERROR2303: sa_request, (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
, (type=4) 10.32.50.0/255.255.255.0/0/0
, protocol= ESP
, transform= esp-des esp-sha-hmac , lifedur= 28800s and 4608000kb
, spi= 0x0(0), conn_id= 0, keysize= 0
flags= 0x4004

=sa created, (sa) sa_dest= 172.18.124.35, sa_prot= 50, sa_spi :602301
, (0x9d71f29c(2641490588
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 3

=sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50, sa_spi :602301
, (0xebc8c823(3955804195
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 4

cisco_endpoint# sho cry ips sa

interface: outside
Crypto map tag: rtpmap, 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): (0.0.0.0/0.0.0.0/0/0
current_peer: 172.18.124.157
{, PERMIT, flags={origin_is_acl
pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0#
pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0#
pkts compressed: 0, #pkts decompressed: 0#
, pkts not compressed: 0, #pkts compr. failed: 0#
pkts decompress failed: 0 #send errors 0, #recv errors 0#

, local crypto endpt.: 172.18.124.35
remote crypto endpt.: 172.18.124.157
path mtu 1500, ipsec overhead 0, media mtu 1500
current outbound spi: 0

:inbound esp sas

:inbound ah sas

:inbound pcp sas

:outbound esp sas

:outbound ah sas

:outbound pcp sas

(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: 4, #pkts encrypt: 4, #pkts digest 4#
pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4#
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, ipsec overhead 56, media mtu 1500
current outbound spi: ebc8c823
```

```
      :inbound esp sas
      (spi: 0x9d71f29c(2641490588
      , transform: esp-des esp-sha-hmac
      { ,in use settings ={Tunnel
      slot: 0, conn id: 3, crypto map: rtpmap
(sa timing: remaining key lifetime (k/sec): (4607999/28777
      IV size: 8 bytes
      replay detection support: Y
```

```
      :inbound ah sas
```

```
      :inbound pcsp sas
```

```
      :outbound esp sas
      (spi: 0xebc8c823(3955804195
      , transform: esp-des esp-sha-hmac
      { ,in use settings ={Tunnel
      slot: 0, conn id: 4, crypto map: rtpmap
(sa timing: remaining key lifetime (k/sec): (4607999/28777
      IV size: 8 bytes
      replay detection support: Y
```

```
      :outbound ah sas
```

```
      :outbound pcsp sas
```

```
                                cisco_endpoint# sho cry is sa
dst          src          state    pending    created
QM_IDLE     0              2       172.18.124.35  172.18.124.157
```

## [معلومات ذات صلة](#)

- [صفحة دعم PIX](#)
- [مرجع أوامر PIX](#)
- [طلبات التعليقات \(RFCs\)](#)
- [تكوين أمان شبكة IPsec](#)
- [تكوين بروتوكول أمان Internet Key Exchange](#)
- [PIX 5.2: تكوين IPsec](#)
- [PIX 5.3: تكوين IPsec](#)
- [صفحة دعم IPsec](#)
- [الدعم الفني - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت  
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو  
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئى. ةصاغل مهتغب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىلإ أمئاد ةوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco  
Systems (رفوتم طبارلا) يلصلأل يزيلچنلإل دن تسمل