

# نم آلا PIX ةيامح رادج نيب IPsec ق فن نيوكت ققحتلا ةطقنل NG ةيامح رادجو Cisco نم

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الرسم التخطيطي للشبكة](#)
- [الاصطلاحات](#)
- [تكوين PIX](#)
- [تكوين NG لنقطة التحقق](#)
- [التحقق من الصحة](#)
- [التحقق من تكوين PIX](#)
- [عرض حالة النفق على نقطة التحقق NG](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [أستكشاف أخطاء تكوين PIX وإصلاحها](#)
- [تلخيص الشبكة](#)
- [عرض سجلات NG لنقطة التحقق](#)
- [معلومات ذات صلة](#)

## المقدمة

يوضح هذا المستند كيفية تكوين نفق IPsec بمفاتيح مشتركة مسبقا للاتصال بين شبكتين خاصتين. في هذا المثال، شبكات الاتصال هي الشبكة الخاصة 192.168.10.x داخل جدار حماية Cisco Secure PIX والشبكة الخاصة 10.32.x.x داخل جدار حماية Checkpoint<sup>TM</sup> من الجيل التالي (NG).

## المتطلبات الأساسية

### المتطلبات

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

- يجب تدفق حركة المرور من داخل PIX ومن داخل NG Checkpoint<sup>TM</sup> إلى الإنترنت (ممثلة هنا بشبكات 172.18.124.x) 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 بدء نفق IPsec بواسطة حركة مرور مثيرة للاهتمام. تعتبر حركة المرور مثيرة للاهتمام عندما تنتقل بين نظائر IPsec. في المرحلة الأولى من IKE، يتفاوض نظراء IPsec على سياسة اقتران أمان (SA) IKE التي تم إنشاؤها. 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 والمصدع للتفاوض على تحويلات 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 وحدات IPsec SAs أو عند انتهاء صلاحية مدة حياتها.

## المكونات المستخدمة

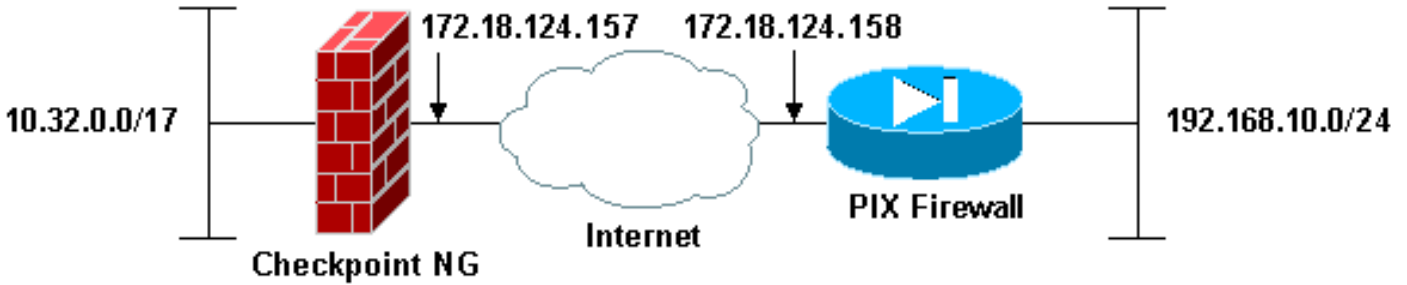
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج PIX الإصدار 6.2.1
- جدار حماية Checkpoint™ NG

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.

## الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



## الاصطلاحات

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

## تكوين PIX

يقدم لك هذا القسم معلومات تكوين الميزات الموضحة في هذا المستند.

```
PIX تكوين
(PIX Version 6.2(1
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIXRTPVPN
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
```

```

fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
  Interesting traffic to be encrypted to the ---!
Checkpoint™ NG. access-list 101 permit ip 192.168.10.0
255.255.255.0 10.32.0.0 255.255.128.0
Do not perform Network Address Translation (NAT) on ---!
traffic to the Checkpoint™ NG. access-list nonat permit
ip 192.168.10.0 255.255.255.0 10.32.0.0 255.255.128.0
  pager lines 24
  interface ethernet0 10baset
  interface ethernet1 10full
  mtu outside 1500
  mtu inside 1500
ip address outside 172.18.124.158 255.255.255.0
ip address inside 192.168.10.1 255.255.255.0
  ip audit info action alarm
  ip audit attack action alarm
  pdm history enable
  arp timeout 14400
  global (outside) 1 interface
  Do not perform NAT on traffic to the Checkpoint™ ---!
  NG. nat (inside) 0 access-list nonat
  nat (inside) 1 0.0.0.0 0.0.0.0 0 0
  route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
  timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00
h323 0:05:00 sip 0:30:00 sip_media 0:02:00
  timeout uauth 0:05:00 absolute
+aaa-server TACACS+ protocol tacacs
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
  no snmp-server location
  no snmp-server contact
snmp-server community public
  no snmp-server enable traps
  floodguard enable
  Permit all inbound IPsec authenticated cipher ---!
  sessions. sysopt connection permit-ipsec
  no sysopt route dnat
  Defines IPsec encryption and authentication ---!
  algorithms. crypto ipsec transform-set rtptac esp-3des
  esp-md5-hmac
  Defines crypto map. crypto map rtprules 10 ipsec- ---!
  isakmp
  crypto map rtprules 10 match address 101
  crypto map rtprules 10 set peer 172.18.124.157
  crypto map rtprules 10 set transform-set rtptac
  Apply crypto map on the outside interface. crypto ---!
  map rtprules interface outside
  isakmp enable outside
  Defines pre-shared secret used for IKE ---!
  authentication. isakmp key ***** address
  172.18.124.157 netmask 255.255.255.255
  Defines ISAKMP policy. isakmp policy 1 ---!
  authentication pre-share
  isakmp policy 1 encryption 3des
  isakmp policy 1 hash md5
  isakmp policy 1 group 2
  isakmp policy 1 lifetime 86400
  telnet timeout 5
  ssh timeout 5

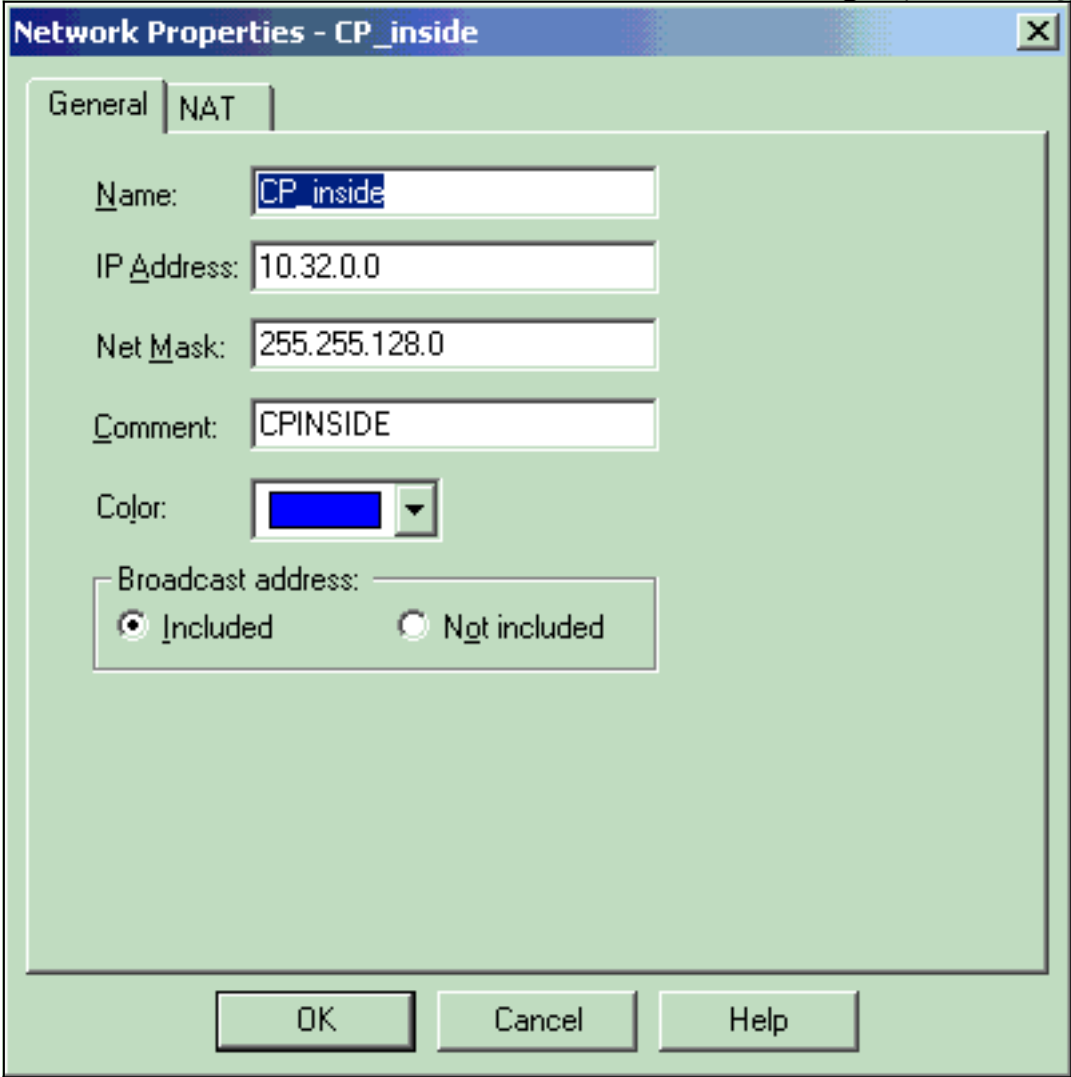
```

```
terminal width 80
Cryptochecksum: 089b038c8e0dbc38d8ce5ca72cf920a5
end :
```

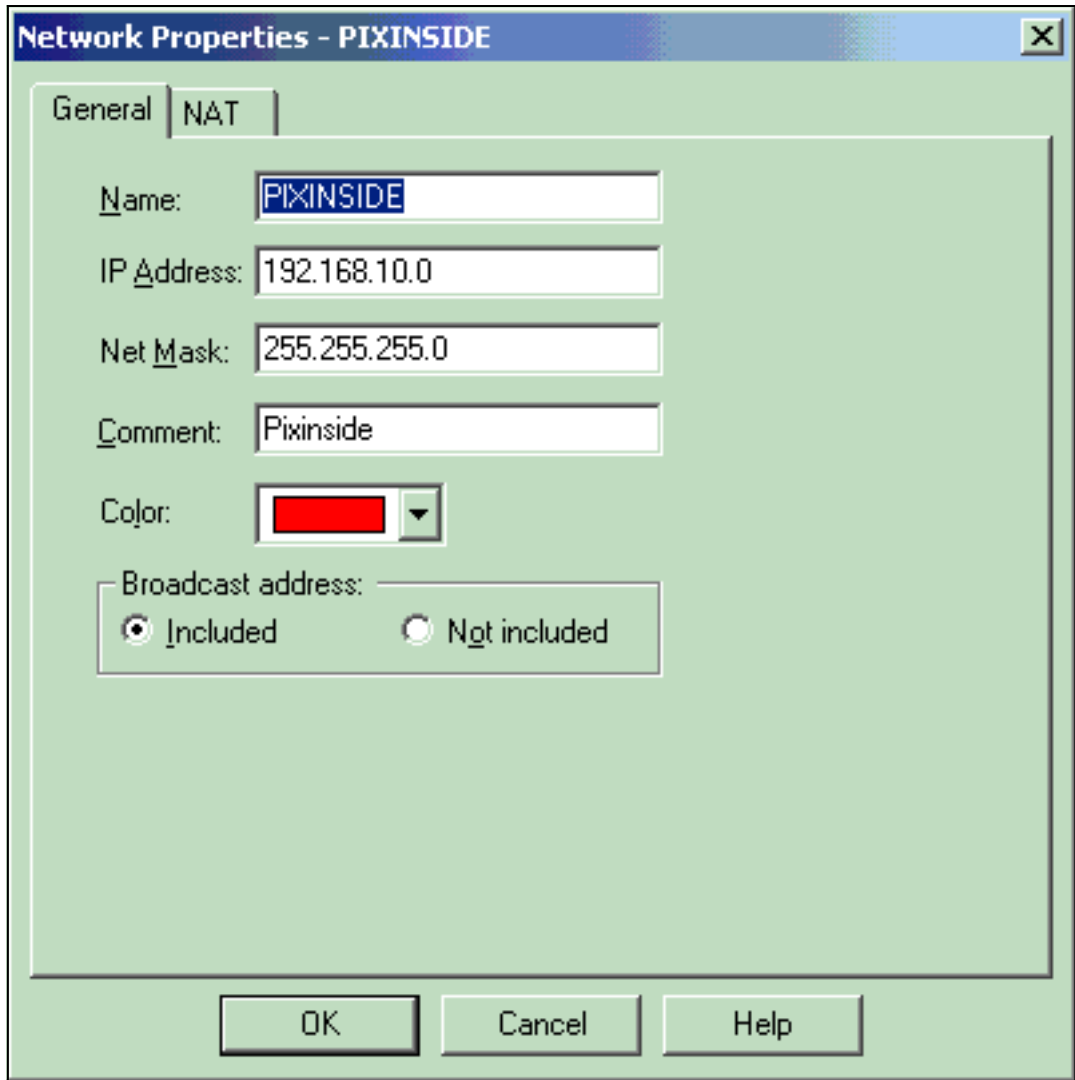
## تكوين NG لنقطة التحقق

يتم تحديد كائنات الشبكة وقواعدها على NG CheckpointTM لتكوين السياسة المتعلقة بتكوين VPN الذي سيتم إعدادها. يتم بعد ذلك تثبيت هذا النهج باستخدام محرر نهج CheckpointTM لـ NG لإكمال جانب CheckpointTM من NG من التكوين.

1. قم بإنشاء كائن الشبكة لشبكة نقطة التفتيش وشبكة جدار حماية PIX التي تقوم بتشفير حركة المرور المفيدة. للقيام بذلك، حدد إدارة < كائنات الشبكة، ثم حدد جديد < الشبكة. أدخل معلومات الشبكة المناسبة، ثم انقر على موافق. تظهر هذه الأمثلة مجموعة من كائنات الشبكة تسمى CP\_Inside (داخل شبكة CheckpointTM (NG و Pixinside (داخل شبكة



(PIX)



2. إنشاء كائنات محطة العمل ل NG Checkpoint<sup>TM</sup> و PIX. للقيام بذلك، حدد إدارة < كائنات الشبكة > جديد < محطة العمل. لاحظ أنه يمكنك استخدام كائن محطة العمل NG Checkpoint<sup>TM</sup> الذي تم إنشاؤه أثناء إعداد Checkpoint<sup>TM</sup> الأولي. حدد الخيارات لتعيين محطة العمل كبوابة وجهاز VPN قابل للتشغيل البيئي، ثم انقر فوق موافق. تظهر هذه الأمثلة مجموعة من الكائنات تسمى NG Checkpoint<sup>TM</sup> (CiscoCCP) و PIX (جدار حماية PIX).

## General

Topology

NAT

VPN

Authentication

Management

+ Advanced

## General

Name: ciscocp

IP Address: 172.18.124.157 

Comment: Checkpoint External IP

Color: Type:  Host  Gateway

## Check Point Products

 Check Point products installed: Version NG 

- 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

**Workstation Properties - PIX**

**General**

**Name:**

**IP Address:**

**Comment:**

**Color:**

**Type:**  Host  Gateway

**Check Point Products**

Check Point products installed: Version

VPN-1 & FireWall-1

FloodGate-1

Policy Server

Management Station

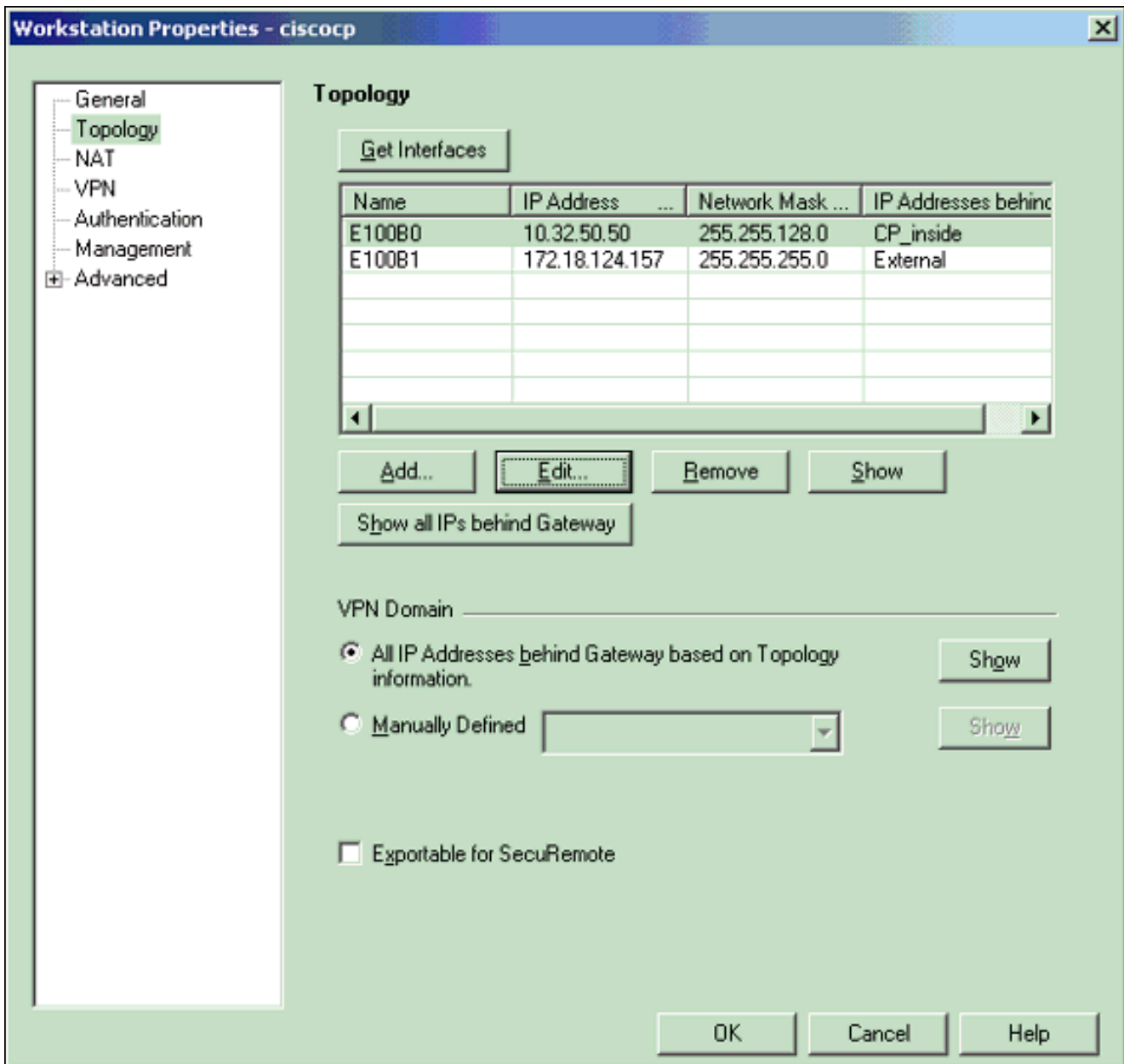
**Object Management**

Managed by this Management Server (Internal)

Managed by another Management Server (External)

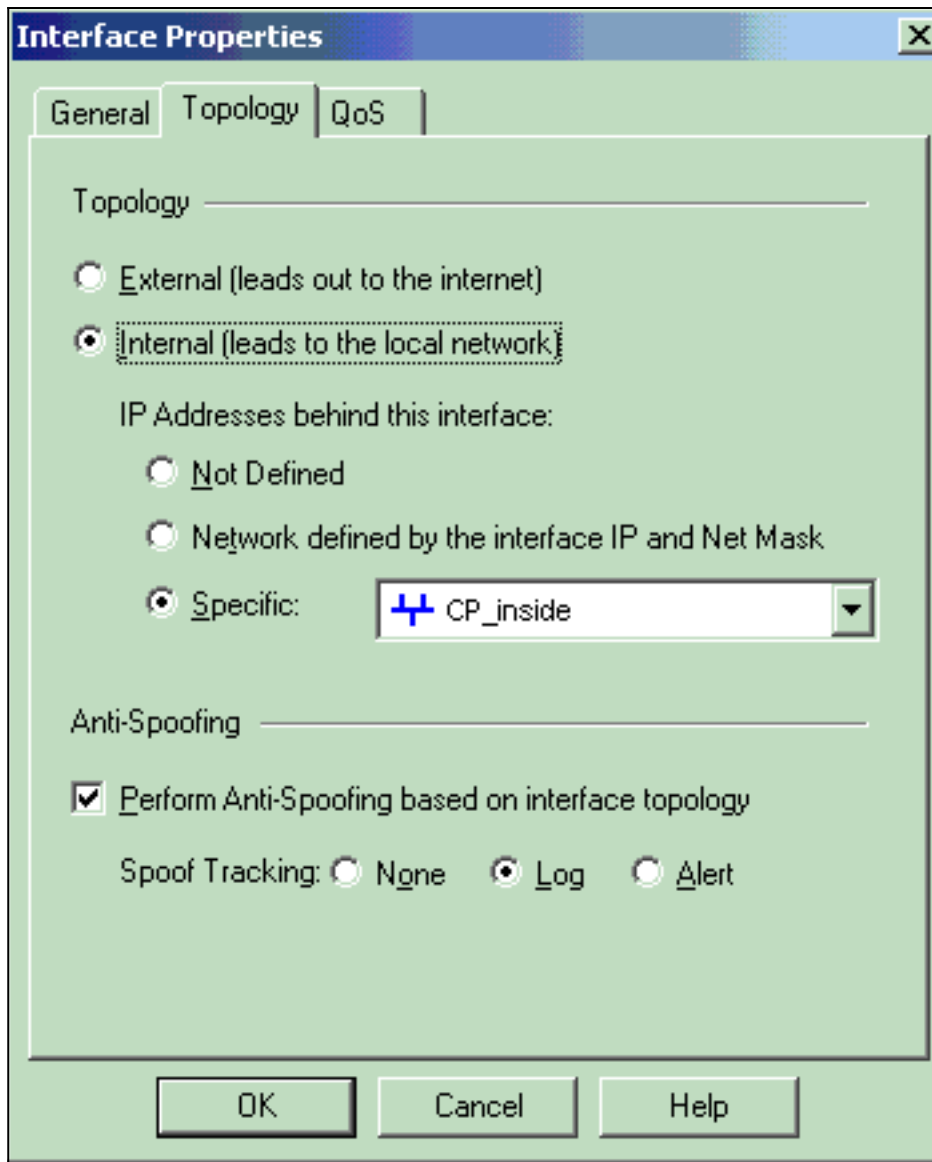
Interoperable VPN Device

3. حدد إدارة <كائنات الشبكة> تحرير لفتح نافذة خصائص محطة العمل ل Checkpoint™ NG Workstation (في هذا المثال). حدد المخطط من الخيارات الموجودة على الجانب الأيسر من النافذة، ثم حدد الشبكة التي سيتم تشفيرها. انقر فوق تحرير لتعيين خصائص الواجهة.



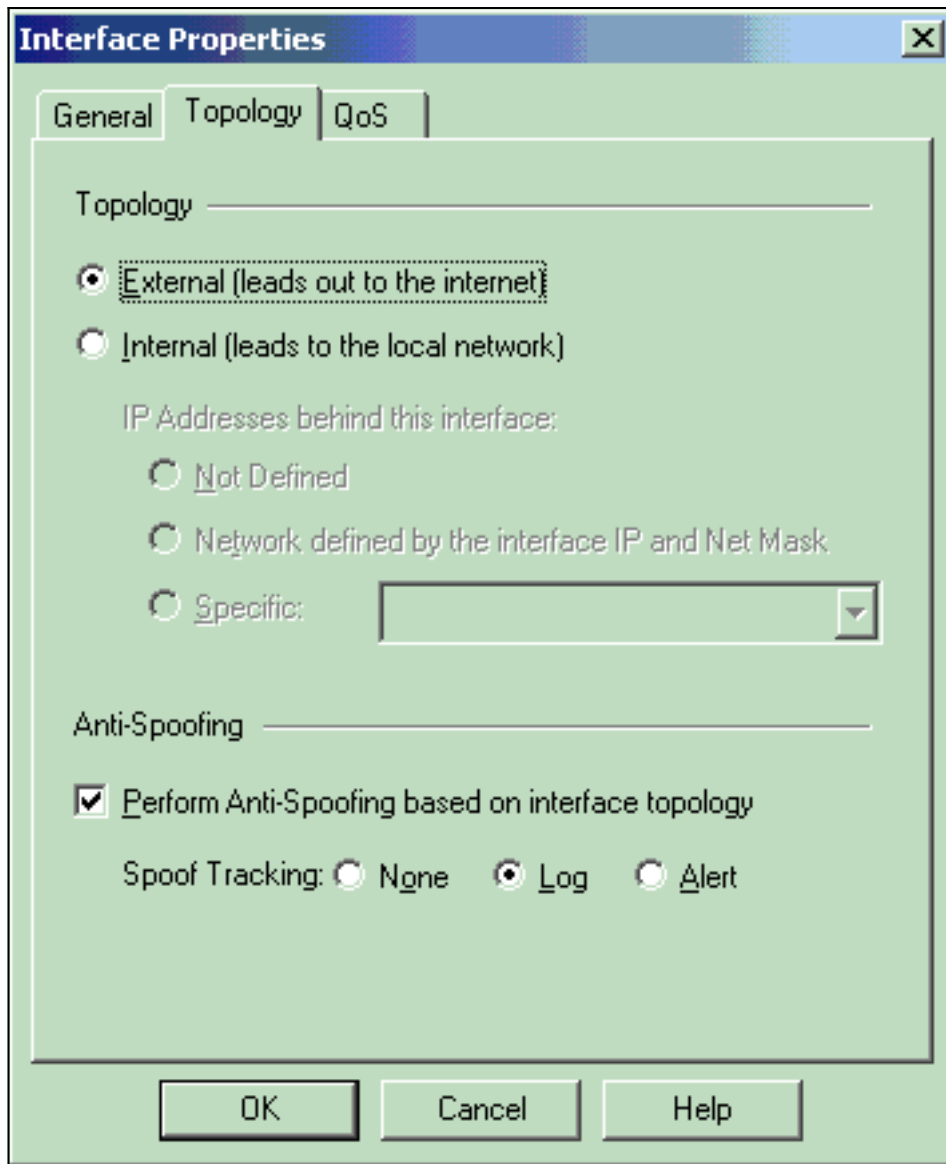
4. حدد الخيار الخاص بتعيين محطة العمل كمحطة عمل داخلية، ثم حدد عنوان IP المناسب. وانقر فوق OK. في هذا تشكيل، cp\_inside هو الشبكة الداخلية من ال NG Checkpoint™. تعيين تحديثات المخطط الموضحة هنا محطة العمل كمحطة عمل داخلية وتحدد العنوان كبروتوكول



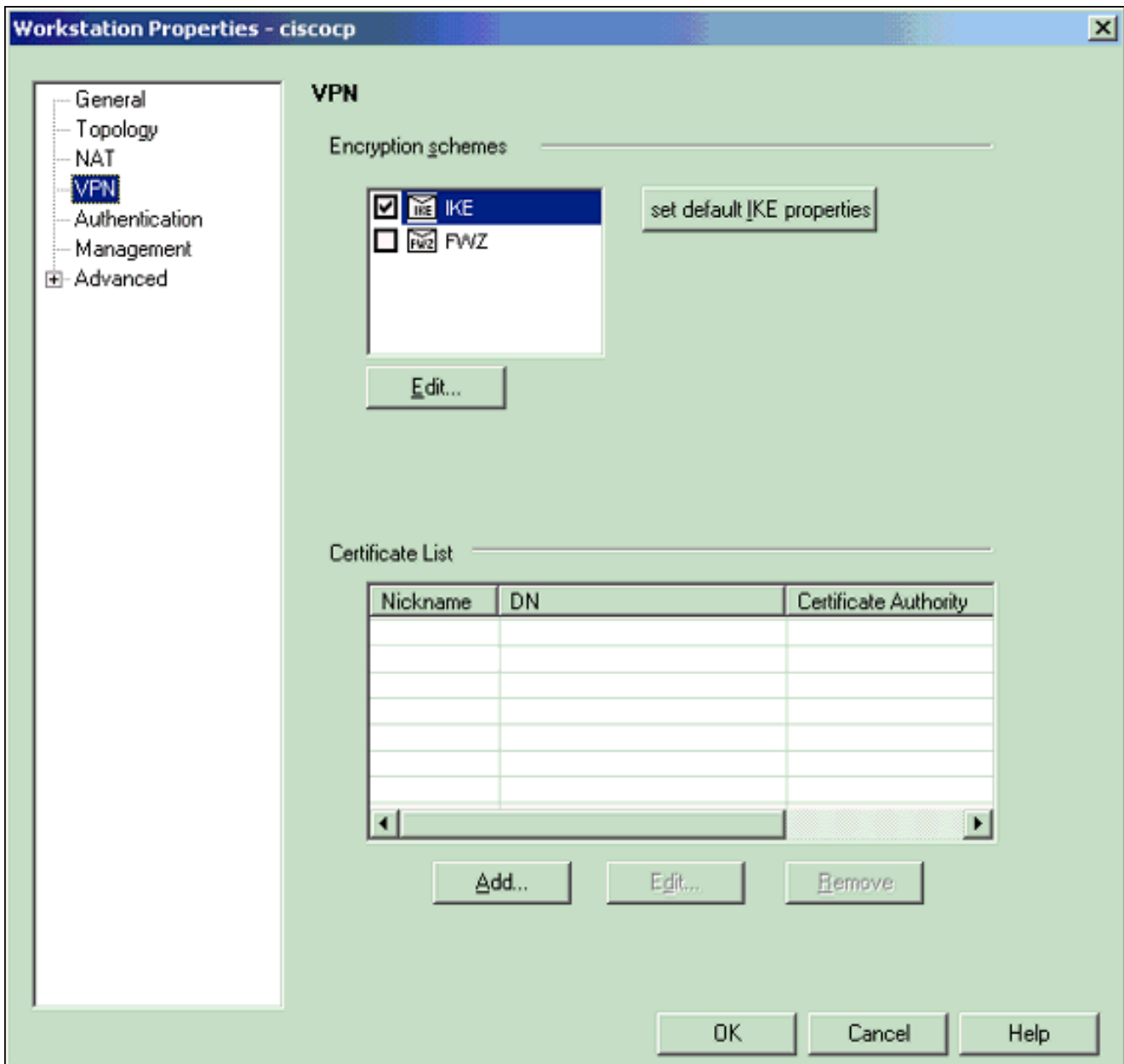


.CP\_Inside

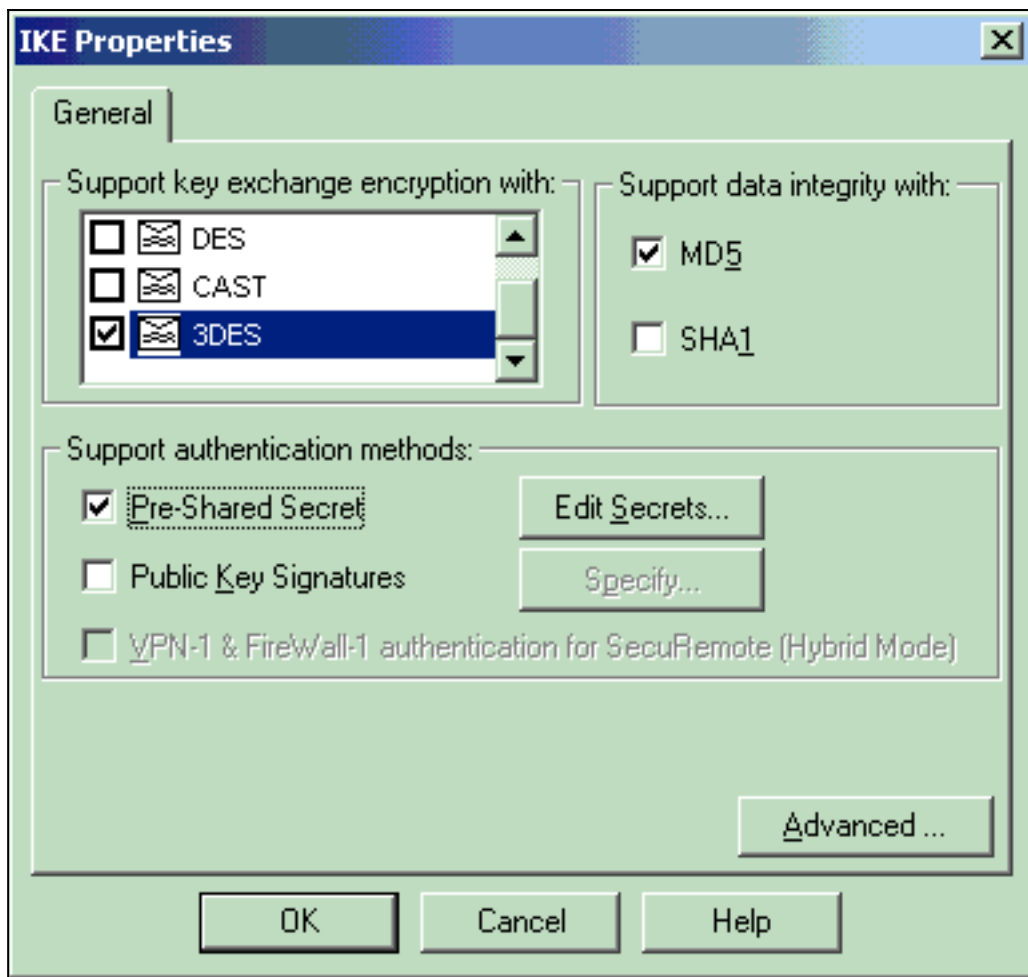
5. من نافذة "خصائص محطة العمل"، حدد الواجهة الخارجية الموجودة على NG CheckpointTM التي تؤدي إلى الإنترنت، ثم انقر فوق "Edit" لتعيين خصائص الواجهة. حدد الخيار لتعيين المخطط كمخطط خارجي، ثم انقر



فوق موافق.  
6. من نافذة خصائص محطة العمل على NG Checkpoint<sup>TM</sup>، حدد VPN من الخيارات الموجودة على الجانب الأيسر من النافذة، ثم حدد معلمات IKE لخوارزميات التشفير والمصادقة. انقر فوق تحرير لتكوين خصائص IKE.

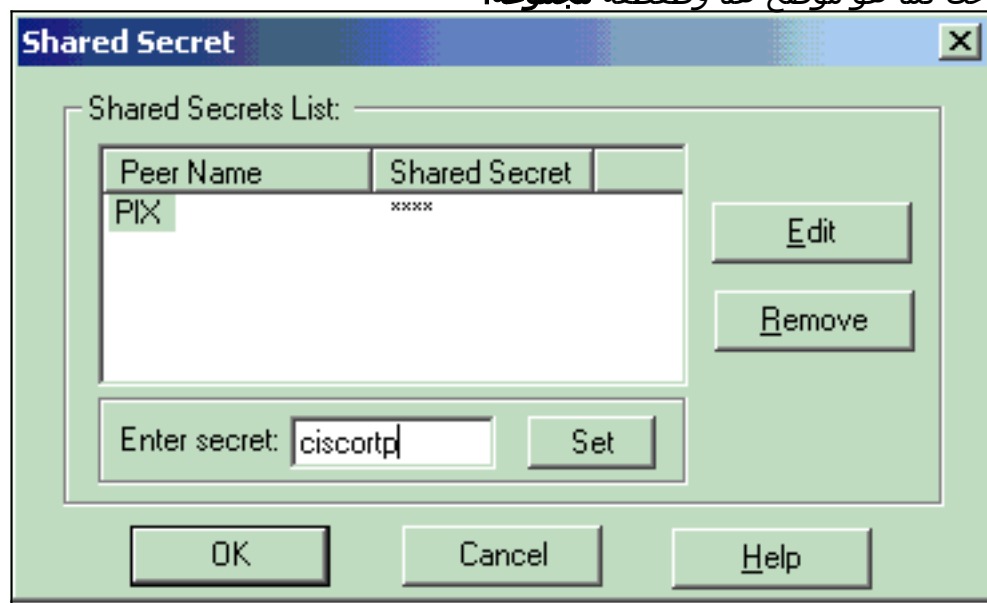


7. تكوين خصائص IKE: حدد الخيار لتشفير 3DES بحيث تكون خصائص IKE متوافقة مع الأمر # isakmp policy encryption 3des. حدد الخيار ل MD5 حتى تكون خصائص IKE متوافقة مع الأمر # crypto isakmp policy



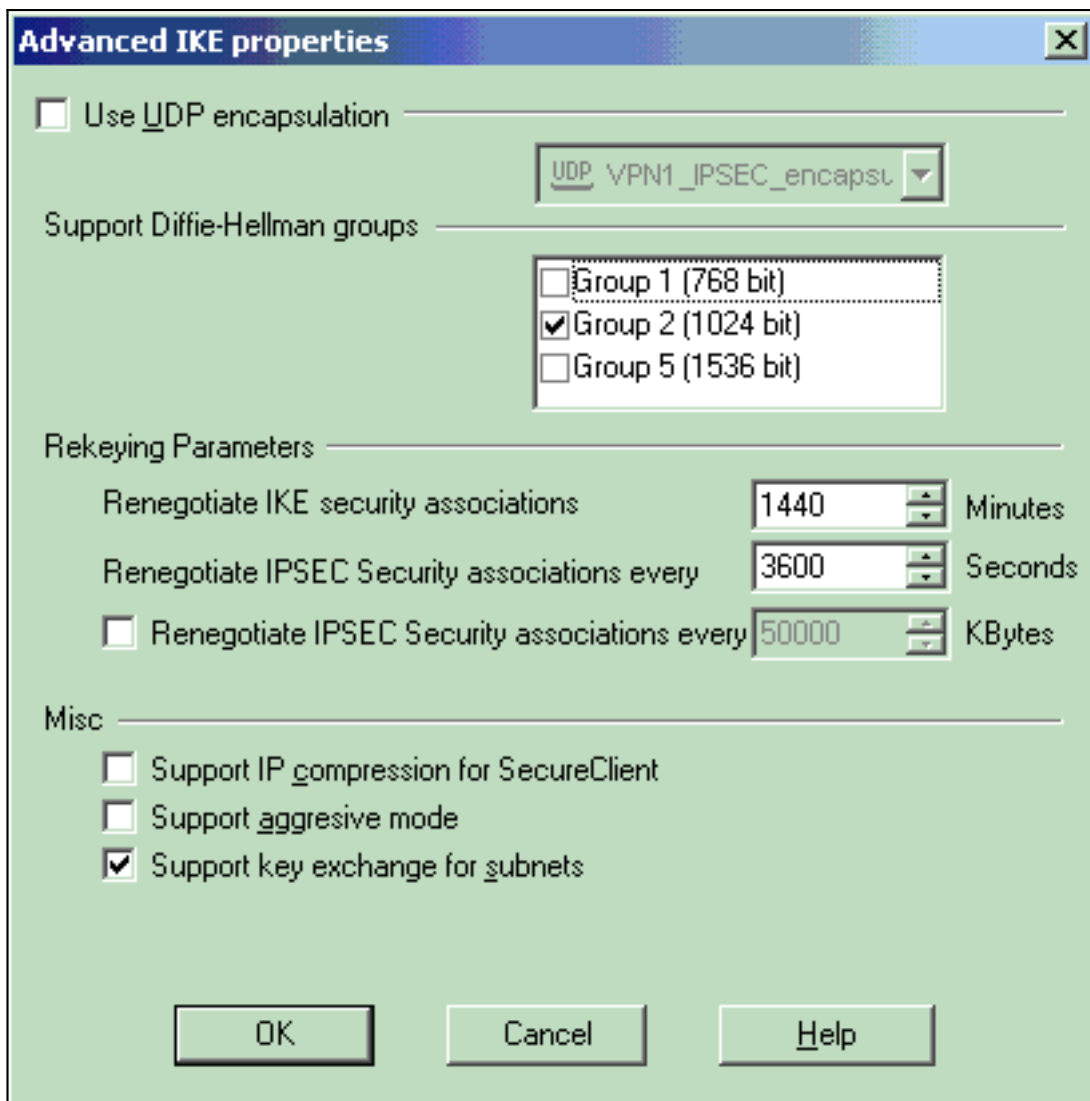
hash MD5

8. حدد خيار المصادقة للأسرار المشتركة مسبقا، ثم انقر فوق تحرير الأسرار لتعيين المفتاح المشترك مسبقا على أنه متوافق مع أمر PIX عنوان مفتاح ISAKMP لعنوان قناع الشبكة قناع الشبكة. طقطقة يحرر أن يدخل مفتاحك كما هو موضح هنا وطقطقة مجموعة،



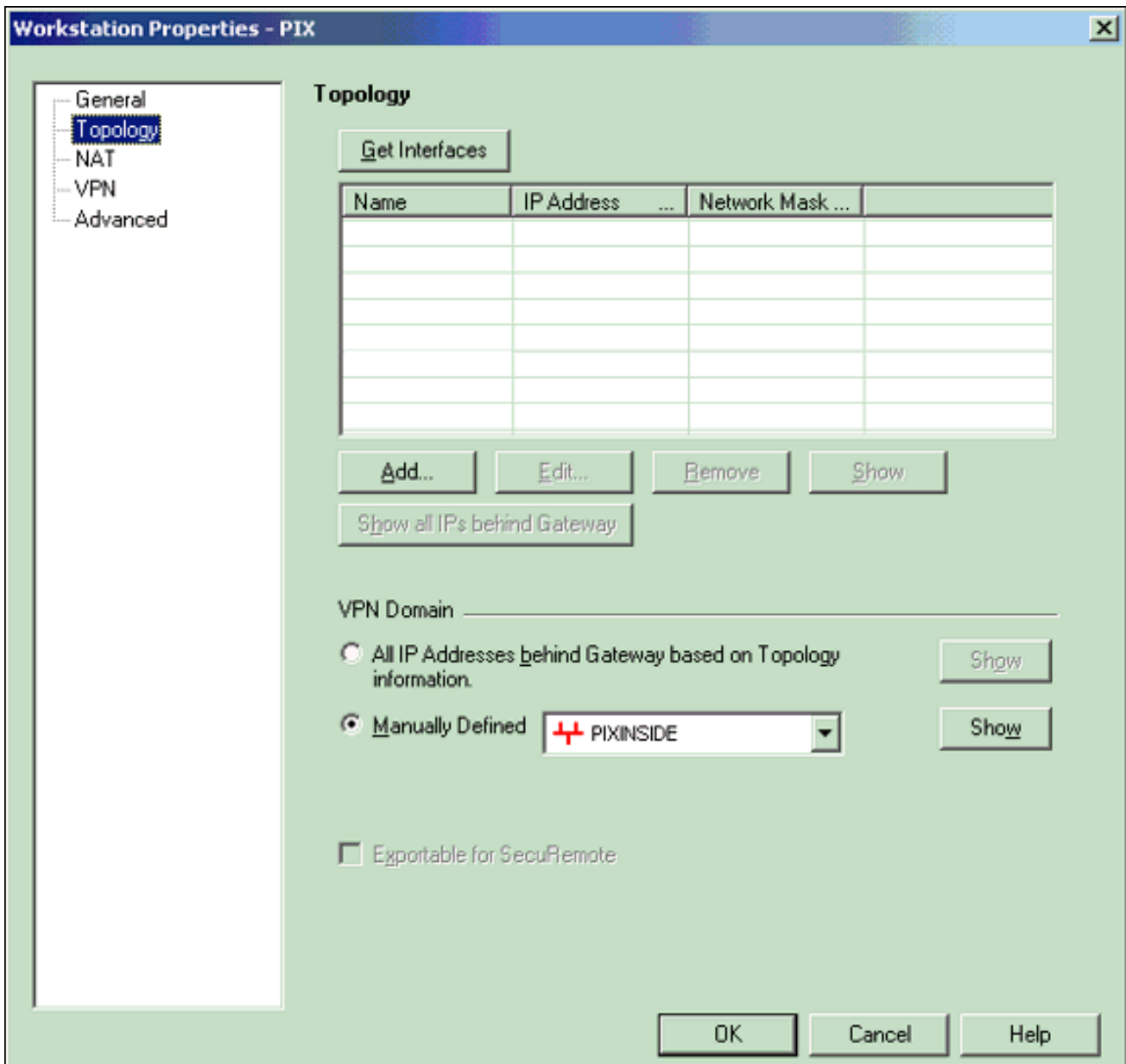
.ok

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. انقر فوق موافق عند

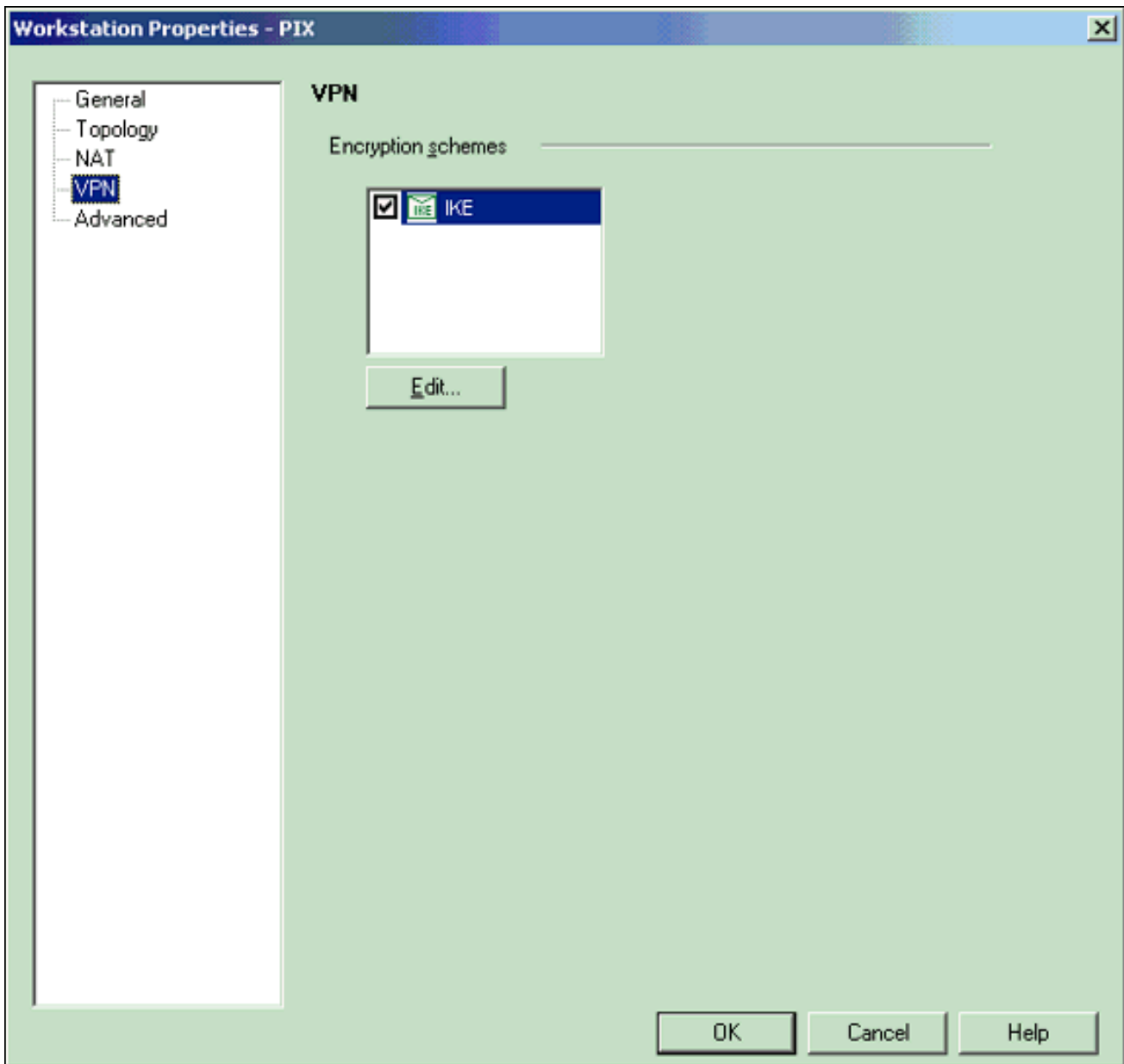


الانتهاء.

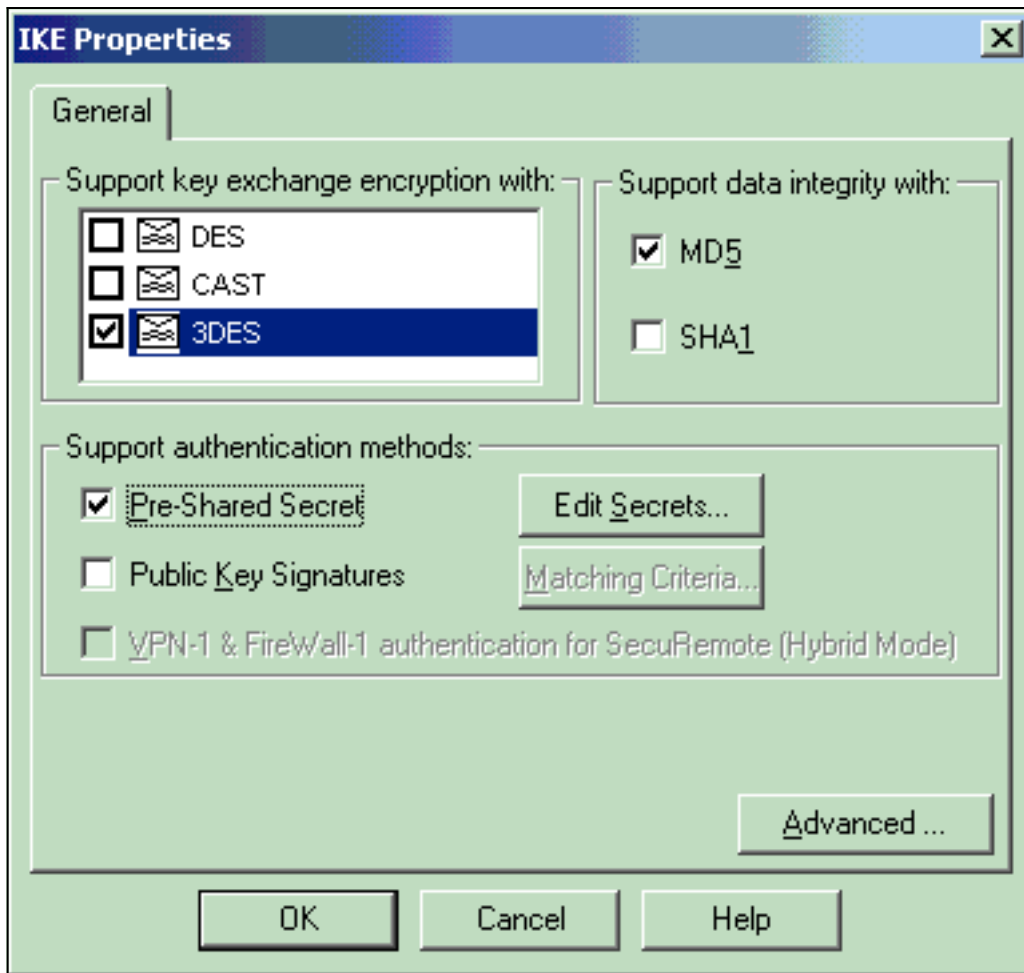
10. حدد إدارة < كائنات الشبكة > تحرير لفتح نافذة خصائص محطة العمل ل PIX. حدد طوبولوجيا من الخيارات الموجودة على الجانب الأيسر من النافذة لتعريف مجال VPN يدويا. في هذا التكوين، يتم تعريف Pixinside (داخل شبكة PIX) على أنه مجال .VPN



11. حدد VPN من الخيارات الموجودة على الجانب الأيسر من النافذة، ثم حدد IKE كمخطط تشفير. انقر فوق تحرير لتكوين خصائص IKE.

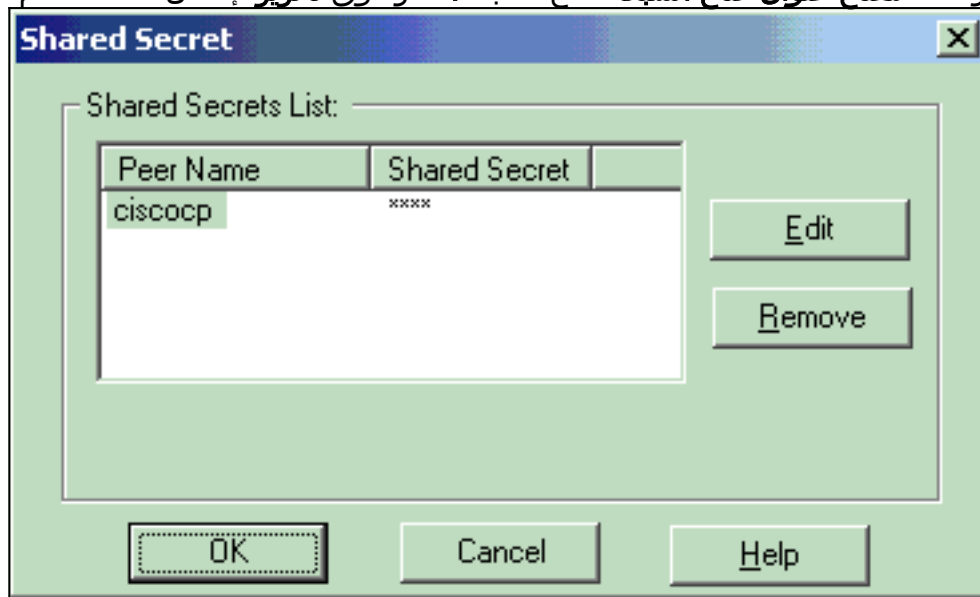


12. قم بتكوين خصائص IKE كما هو موضح هنا: حدد الخيار لتشفير 3DES بحيث تكون خصائص IKE متوافقة مع الأمر `isakmp policy # encryption 3des`. حدد الخيار ل MD5 حتى تكون خصائص IKE متوافقة مع الأمر `crypto isakmp policy # hash`



.MD5

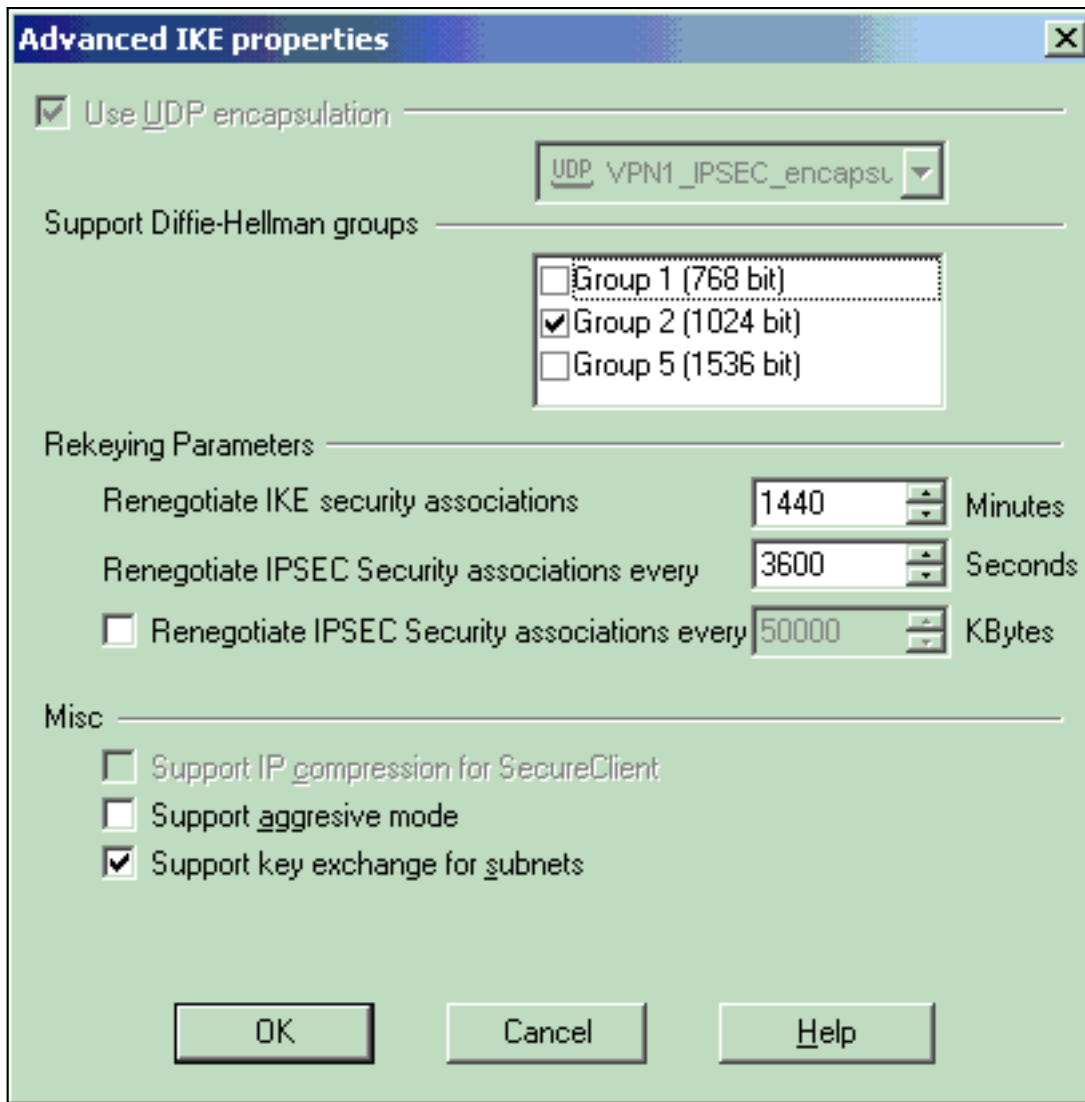
13. حدد خيار المصادقة للأسرار المشتركة مسبقا، ثم انقر فوق تحرير الأسرار لتعيين المفتاح المشترك مسبقا كمتوافق مع أمر PIX مفتاح عنوان قناع الشبكة قناع الشبكة. انقر فوق تحرير لإدخال مفتاحك، ثم انقر فوق



تعيين، موافق.

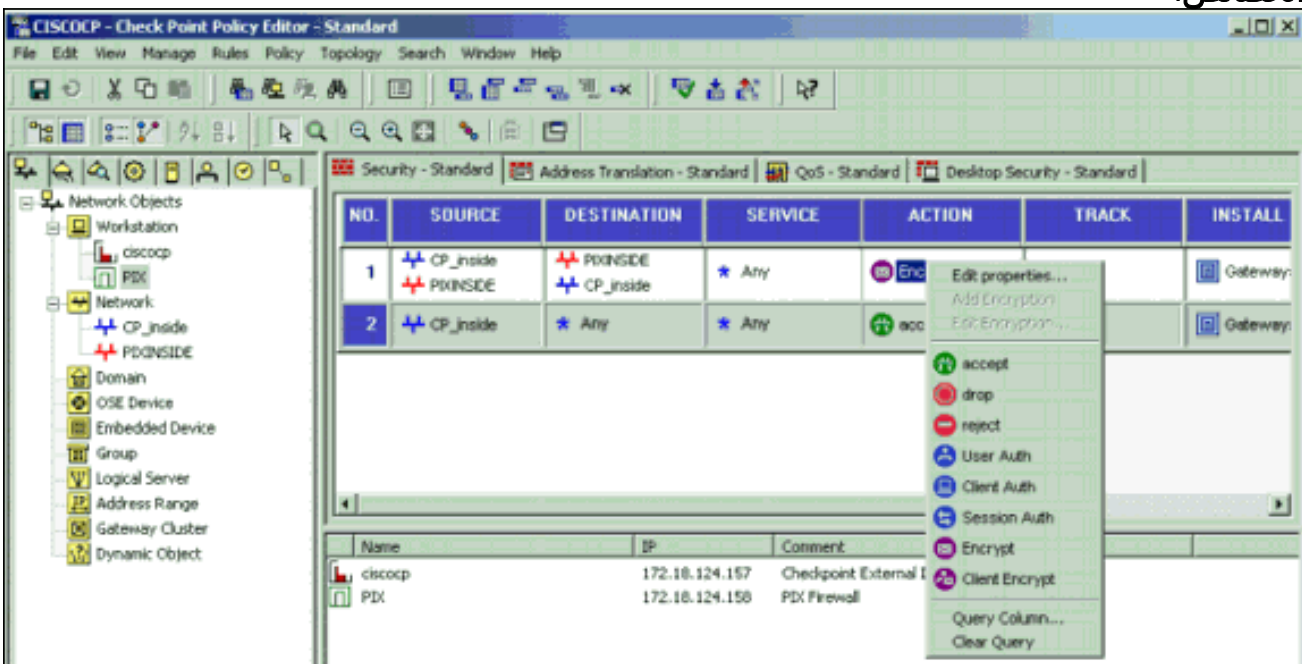
14. من نافذة خصائص IKE، انقر على خيارات متقدمة... وقم بتغيير هذه الإعدادات. حدد مجموعة Diffie-Hellman المناسبة لخصائص IKE. قم بإلغاء تحديد خيار دعم الوضع المتداخل. حدد الخيار لتبادل مفتاح الدعم للشبكات الفرعية. وانقر فوق موافق، موافق عند



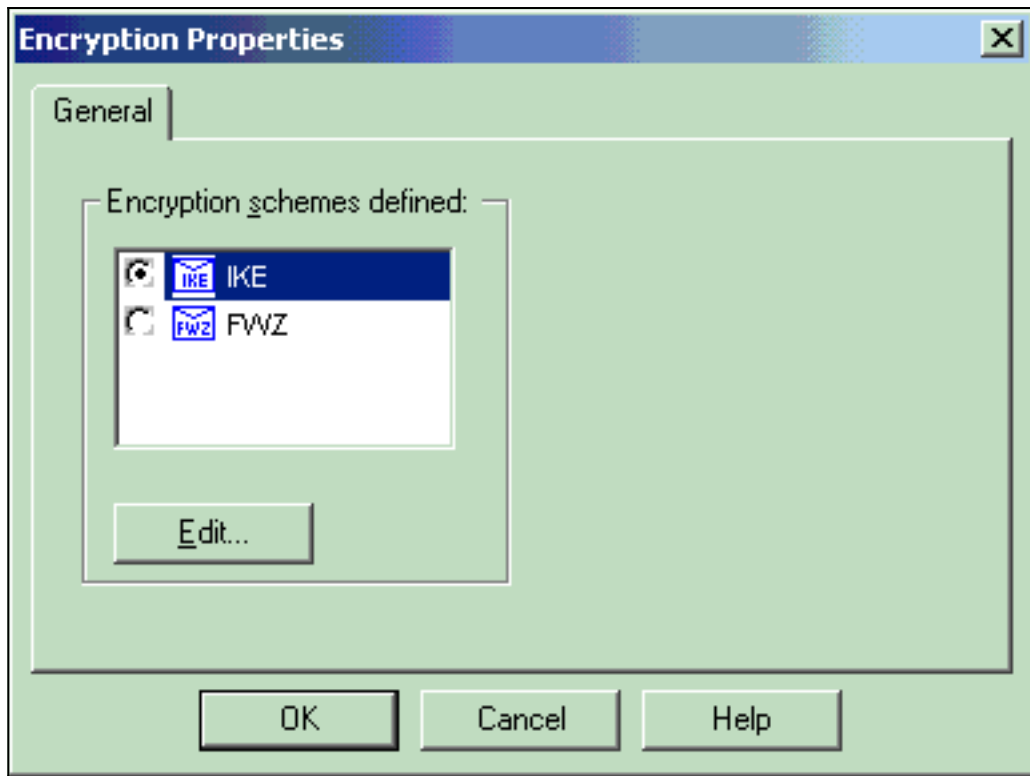


الانتهاء.

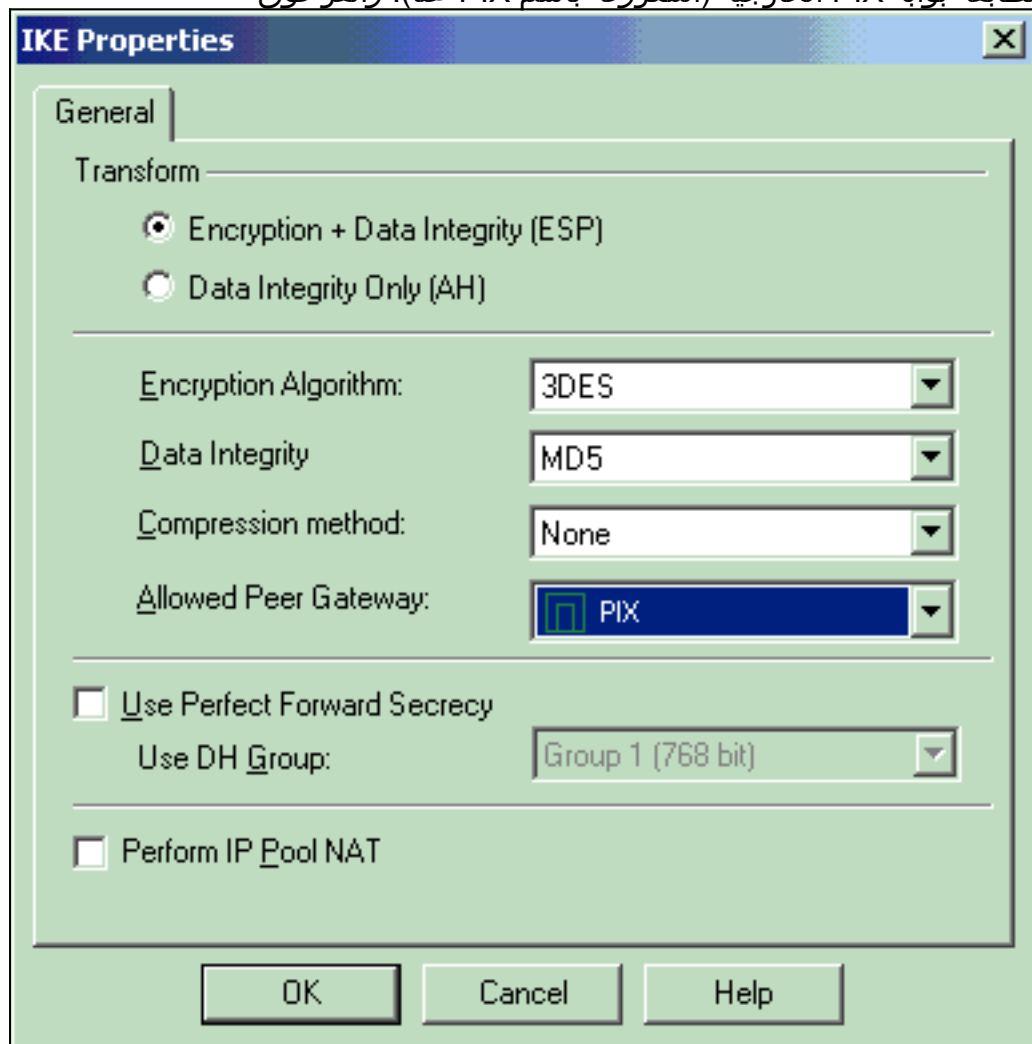
15. حدد قواعد <إضافة قواعد> Top لتكوين قواعد التشفير للنهج. في نافذة محرر النهج، قم بإدراج قاعدة بمصدر CP\_Inside (داخل شبكة من نقطة التفتيش NG<sup>TM</sup>) و Pixinside (داخل شبكة PIX) على كل من أعمدة المصدر والوجهة. قم بتعيين قيم للخدمة = أي، الإجراء = تشفير، والمسار = السجل. عندما تقوم بإضافة قسم إجراء التشفير من القاعدة، انقر بزر الماوس الأيمن فوق الإجراء وحدد تحرير الخصائص.



16. مع تحديد IKE وإبرازه، انقر

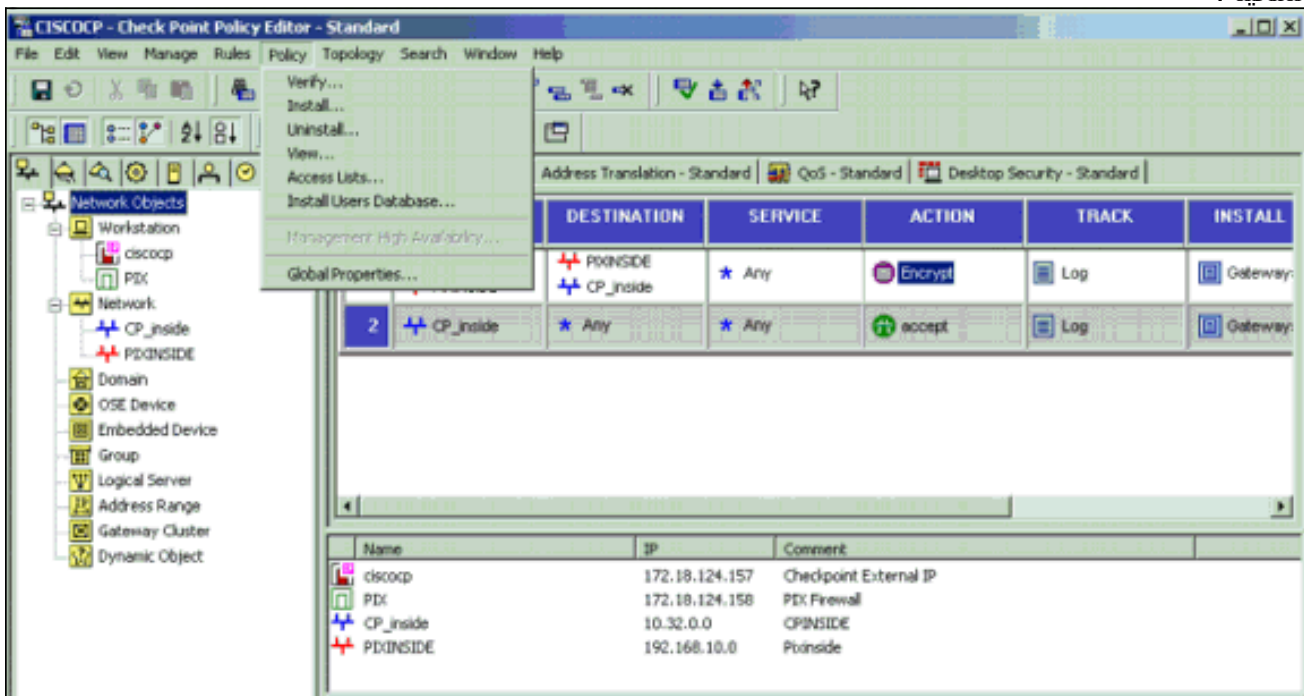


17. تحرير. على نافذة خصائص IKE، قم بتغيير الخصائص لتوافق مع تحويلات PIX IPsec في أمر crypto ipsec transform-set rtpac esp-3des esp-md5-hmac (ESP)، وتعيين خوارزمية التشفير إلى 3DES، وتعيين تكامل البيانات إلى MD5، وتعيين بوابة النظير المسموح بها لمطابقة بوابة PIX الخارجية (المعروفة باسم PIX هنا). وانقر فوق

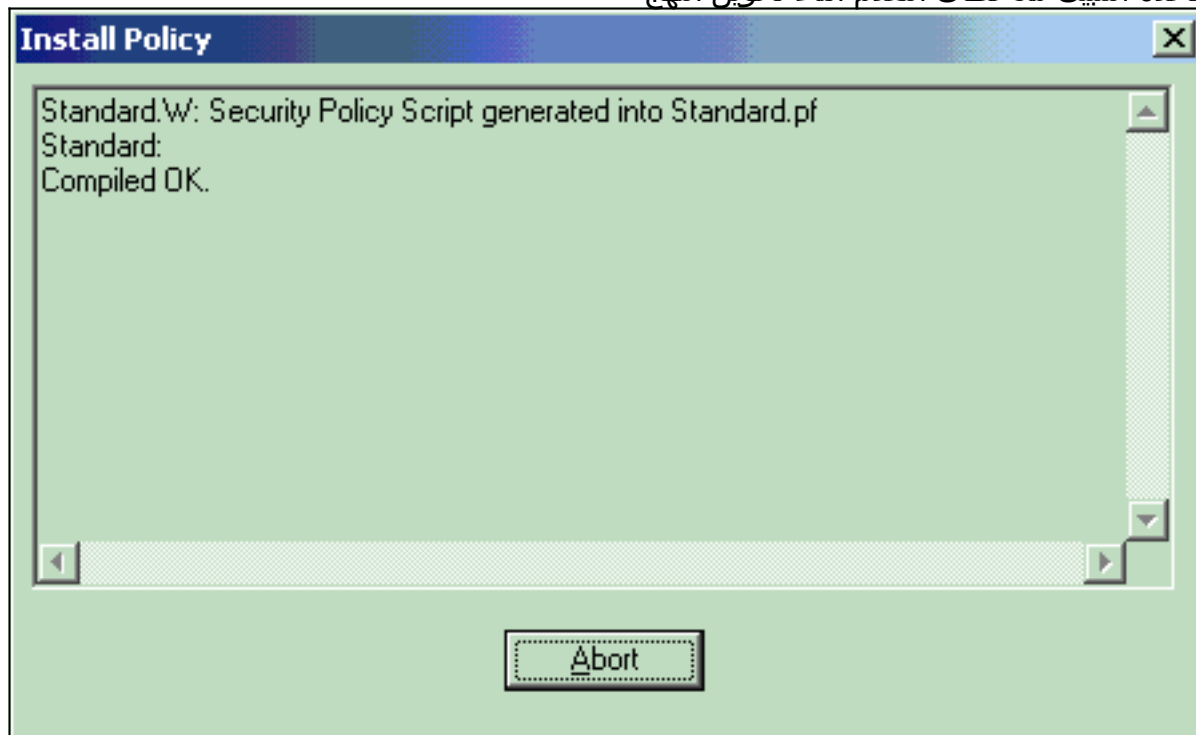


18. OK بعد تكوين NG CheckpointTM، احفظ النهج وحدد النهج < Install

تمكينه.

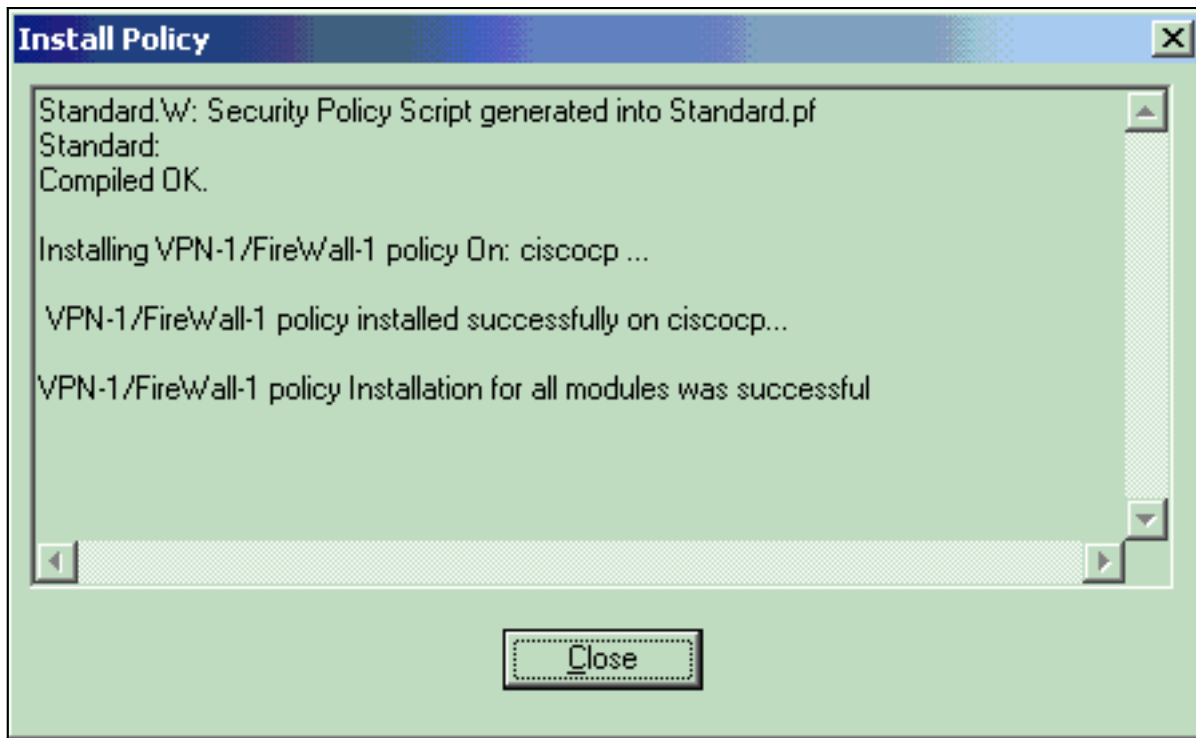


تعرض نافذة التثبيت ملاحظات التقدم أثناء تحويل النهج



برمجيا.

عندما تشير نافذة التثبيت إلى اكتمال تثبيت النهج. انقر فوق إغلاق " لإنهاء



الإجراء.

## التحقق من الصحة

### التحقق من تكوين PIX

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرج الأمر **show**.

بدء اختبار اتصال من إحدى الشبكات الخاصة إلى الشبكة الخاصة الأخرى لاختبار الاتصال بين الشبكتين الخاصتين. في هذا التكوين، تم إرسال اختبار اتصال من جانب (PIX (192.168.10.2 إلى الشبكة الداخلية NG Checkpoint™ (10.32.50.51).

• **show crypto isakmp sa** — يعرض جميع شبكات IKE الحالية في نظير.

```

show crypto isakmp sa
      Total      : 1
      Embryonic  : 0
dst          src          state    pending  created
QM_IDLE     0            1       172.18.124.158  172.18.124.157

```

• **show crypto ipSec** — يعرض الإعدادات المستخدمة من قبل SAs الحالية.

```

PIX501A#show cry ipsec sa
      interface: outside
      Crypto map tag: rtprules, local addr. 172.18.124.158
      (local ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
      (remote ident (addr/mask/prot/port): (10.32.0.0/255.255.128.0/0/0)
      current_peer: 172.18.124.157
      {,PERMIT, flags={origin_is_acl
      pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19#
      pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19#
      pkts compressed: 0, #pkts decompressed: 0#
      pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0#
      send errors 1, #rcv errors 0#

```

```

local crypto endpt.: 172.18.124.158, remote crypto endpt.: 172.18.124.157
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 6b15a355

```

```

:inbound esp sas
(spi: 0xcd238c7(3469883591)
, transform: esp-3des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 3, crypto map: rtprules
(sa timing: remaining key lifetime (k/sec): (4607998/27019
IV size: 8 bytes
replay detection support: Y

```

```

:inbound ah sas
:inbound pcsp sas

```

```

:outbound esp sas
(spi: 0x6b15a355(1796580181)
, transform: esp-3des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 4, crypto map: rtprules
(sa timing: remaining key lifetime (k/sec): (4607998/27019
IV size: 8 bytes
replay detection support: Y

```

```

:outbound ah sas

```

```

:outbound pcsp sas

```

## عرض حالة النفق على نقطة التحقق NG

انتقل إلى "محرر النهج" وحدد نافذة < حالة النظام لعرض حالة النفق.

Modules	IP Address	VPN-1 Details
CISCOCP		Status: OK
ciscocp	172.18.124.157	Packets
FireWall-1		Encrypted: 20
FloodGate-1		Decrypted: 20
Management		Errors
SVN Foundation		Encryption errors: 0
VPN-1		Decryption errors: 0
		IKE events errors: 0
		Hardware
		HW Vendor Name: none
		HW Status: none

# استكشاف الأخطاء وإصلاحها

## استكشاف أخطاء تكوين PIX وإصلاحها

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرج الأمر `show`.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل استخدام أوامر `debug`.

أستخدم هذه الأوامر لتمكين تصحيح الأخطاء على جدار حماية PIX.

• **debug crypto engine**—يعرض رسائل تصحيح الأخطاء حول محركات التشفير، التي تقوم بالتشفير وفك التشفير.

• **debug crypto isakmp**—يعرض الرسائل المتعلقة بأحداث IKE.

```
VPN Peer: ISAKMP: Added new peer: ip:172.18.124.157 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:172.18.124.157 Ref cnt incremented to:1 Total VPN Peers:1
      ISAKMP (0): beginning Main Mode exchange
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
      OAK_MM exchange
      ISAKMP (0): processing SA payload. message ID = 0
      ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
      ISAKMP: encryption 3DES-CBC
      ISAKMP: hash MD5
      ISAKMP: default group 2
      ISAKMP: auth pre-share
      ISAKMP: life type in seconds
      ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
      ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
      return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
      OAK_MM exchange
      ISAKMP (0): processing KE payload. message ID = 0
      ISAKMP (0): processing NONCE payload. message ID = 0
      ISAKMP (0): ID payload
      next-payload : 8
      type : 1
      protocol : 17
      port : 500
      length : 8
      ISAKMP (0): Total payload length: 12
      return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
      OAK_MM exchange
      ISAKMP (0): processing ID payload. message ID = 0
      ISAKMP (0): processing HASH payload. message ID = 0
      ISAKMP (0): SA has been authenticated
ISAKMP (0): beginning Quick Mode exchange, M-ID of 322868148:133e93b4 IPSEC(key_engine): got a
      ...queue event
      IPSEC(spi_response): getting spi 0xcd238c7(3469883591) for SA
      from 172.18.124.157 to 172.18.124.158 for prot 3
      return status is IKMP_NO_ERROR
      ISAKMP (0): sending INITIAL_CONTACT notify
      ISAKMP (0): sending NOTIFY message 24578 protocol 1
      ISAKMP (0): sending INITIAL_CONTACT notify
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
      OAK_QM exchange
```

```

: oakley_process_quick_mode
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 322868148
ISAKMP : Checking IPsec proposal 1
ISAKMP: transform 1, ESP_3DES
: 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-MD5
, ISAKMP (0): atts are acceptable. IPSEC(validate_proposal_request): proposal part #1
, key eng. msg.) dest= 172.18.124.157, src= 172.18.124.158)
, (dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4
, (src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-3des esp-md5-hmac
, lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
ISAKMP (0): processing NONCE payload. message ID = 322868148
ISAKMP (0): processing ID payload. message ID = 322868148
ISAKMP (0): processing ID payload. message ID = 322868148
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
spi 3469883591, message ID = 322868148
ISAKMP (0): processing responder lifetime
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
spi 3469883591, message ID = 322868148
ISAKMP (0): processing responder lifetime
ISAKMP (0): Creating IPsec SAs
(inbound SA from 172.18.124.157 to 172.18.124.158 (proxy 10.32.0.0 to 192.168.10.0
has spi 3469883591 and conn_id 3 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytes
(outbound SA from 172.18.124.158 to 172.18.124.157 (proxy 192.168.10.0 to 10.32.0.0
has spi 1796580181 and conn_id 4 and flags 4
lifetime of 28800 seconds
...lifetime of 4608000 kilobytes IPSEC(key_engine): got a queue event
, : (IPSEC(initialize_sas
, key eng. msg.) dest= 172.18.124.158, src= 172.18.124.157)
, (dest_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4
, (src_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4
, protocol= ESP, transform= esp-3des esp-md5-hmac
, lifedur= 28800s and 4608000kb
spi= 0xc3d238c7(3469883591), conn_id= 3, keysize= 0, flags= 0x4
, : (IPSEC(initialize_sas
, key eng. msg.) src= 172.18.124.158, dest= 172.18.124.157)
, (src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4
, (dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4
, protocol= ESP, transform= esp-3des esp-md5-hmac
, lifedur= 28800s and 4608000kb
spi= 0x6b15a355(1796580181), conn_id= 4, keysize= 0, flags= 0x4
VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:2 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:3 Total VPN Peers:1
return status is IKMP_NO_ERROR

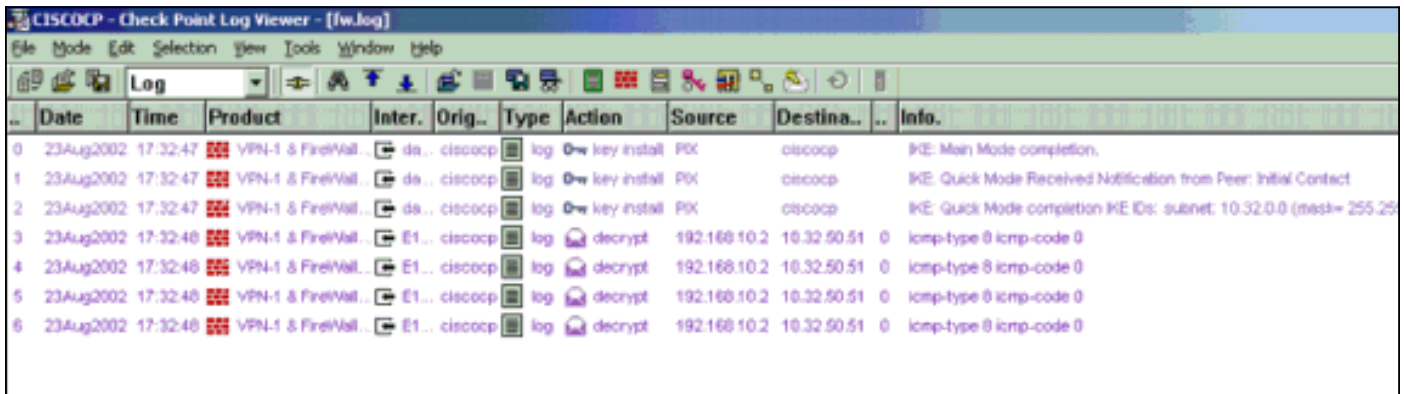
```

## تلخيص الشبكة

عندما يتم تكوين شبكات داخلية متجاوزة متعددة في مجال التشفير على نقطة التحقق، قد يقوم الجهاز بتلخيصها تلقائياً فيما يتعلق بحركة المرور المفيدة. إذا لم يتم تكوين قائمة التحكم في الوصول إلى التشفير (ACL) 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 تلخيصها إلى 23/ 10.0.0.0.

## عرض سجلات NG لنقطة التحقق

حدد نافذة > عارض السجل لعرض السجلات.



Date	Time	Product	Inter.	Orig..	Type	Action	Source	Destina...	Info.
23Aug2002	17:32:47	VPN-1 & FireWall...	da...	ciscocp	log	key install	PIX	ciscocp	IKE: Main Mode completion.
23Aug2002	17:32:47	VPN-1 & FireWall...	da...	ciscocp	log	key install	PIX	ciscocp	IKE: Quick Mode Received Notification from Peer: Initial Contact
23Aug2002	17:32:47	VPN-1 & FireWall...	da...	ciscocp	log	key install	PIX	ciscocp	IKE: Quick Mode completion IKE IDs: subnet: 10.32.0.0 (mesh= 255.25
23Aug2002	17:32:48	VPN-1 & FireWall...	E1...	ciscocp	log	decrypt	192.168.10.2	10.32.50.51 0	icmp-type 0 icmp-code 0
23Aug2002	17:32:48	VPN-1 & FireWall...	E1...	ciscocp	log	decrypt	192.168.10.2	10.32.50.51 0	icmp-type 0 icmp-code 0
23Aug2002	17:32:48	VPN-1 & FireWall...	E1...	ciscocp	log	decrypt	192.168.10.2	10.32.50.51 0	icmp-type 0 icmp-code 0
23Aug2002	17:32:48	VPN-1 & FireWall...	E1...	ciscocp	log	decrypt	192.168.10.2	10.32.50.51 0	icmp-type 0 icmp-code 0

## معلومات ذات صلة

- [برنامج جدار حماية Cisco PIX](#)
- [مراجع أوامر جدار حماية PIX الآمن من Cisco](#)
- [الإعلامات الميدانية لمنتج الأمان \(بما في ذلك PIX\)](#)
- [طلبات التعليقات \(RFCs\)](#)
- [الدعم التقني والمستندات - Cisco Systems](#)



ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نء مء دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءء. ةصاأل مء تءل ب  
Cisco ةلخت. فرتمة مچرت مء مء دق ةل ةل ةل فارتحال ةمچرتل عم لال او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزىل ءن إال دن تسمل