PIX/ASA 7.x وأعلى: مثال تكوين نفق PIX-to-PIX VPN

المحتويات

المقدمة

يصف هذا المستند إجراء تكوين أنفاق VPN بين جدران حماية PIX باستخدام مدير أجهزة الأمان المعدلة (ASDM) من Cisco. ASDM هي أداة تكوين قائمة على التطبيقات تم تصميمها لمساعدتك في إعداد جدار حماية PIX وتكوينه ومراقبته باستخدام واجهة المستخدم الرسومية (GUI). يتم وضع جداران الحماية من طراز PIX في موقعين مختلفين.

يتم تكوين نفق باستخدام IPsec. IPsec هو مجموعة من المعايير المفتوحة التي توفر سرية البيانات وسلامة البيانات وأصالة البيانات بين نظراء IPsec.

ملاحظة: في PIX 7.1 والإصدارات الأحدث، يتم تغيير الأمر sysopt connection allowed-ips إلى sysopt connection permit-vpn. يسمح هذا الأمر لحركة المرور التي تدخل جهاز الأمان من خلال نفق VPN ثم يتم فك تشفيرها، لتخطي قوائم الوصول إلى الواجهة. لا تزال نهج المجموعة وقوائم الوصول إلى التخويل لكل مستخدم يتم تطبيقها على حركة المرور. invalider in order to أمر. لا يكون هذا الأمر في وضع التكوين العام. لا يمكن استخدام هذا الأمر في تكوين الواجهة. to قم بتعطيل هذه الميزة، استخدم no من هذا الأمر.

ارجع إلى PIX 6.x: مثال تكوين نفق VPN البسيط من PIX إلى PIX لمعرفة المزيد حول نفس السيناريو حيث يشغل جهاز أمان Cisco PIX الإصدار 6.x من البرنامج.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تحدد المعلومات الواردة في هذا المستند أن هذا النظير يهيئ أولا تبادل خاص لتحديد النظير المناسب الذي يتم الاتصال به.

- جهاز الأمان Cisco PIX 500 Series Security Appliance مع الإصدار 7.x والإصدارات الأحدث
- ASDM الإصدار 5.x والإصدارات الأحدث

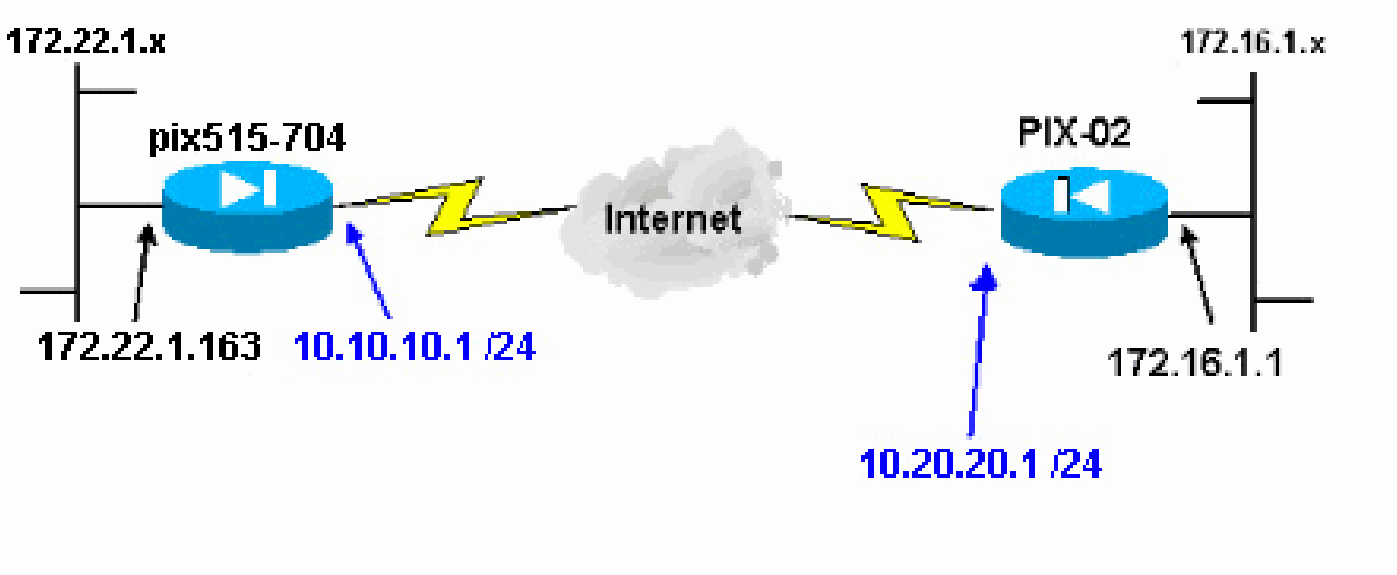
ملاحظة: ارجع إلى السماح بوصول HTTPS إلى ASDM للسماح بتكوين ASA بواسطة ASDM.

ملاحظة: تقوم سلسلة ASA 5500 الإصدار 7.x/8.x بتشغيل نفس البرنامج الموجود في الإصدار 7.x/8.x من PIX. تنطبق التكوينات الواردة في هذا المستند على كل من سطور المنتجات.

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.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



الاصطلاحات

ارجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات

المستندات.

معلومات أساسية

يمكن تقسيم مفاوضات IPsec إلى خمس خطوات، وتتضمن مرحلتين من عملية تبادل مفاتيح الإنترنت (IKE).

1. يتم بدء نفق IPsec بواسطة حركة مرور مثيرة. تعتبر حركة المرور مثيرة للاهتمام عندما تنتقل بين نظائر IPsec.
2. في المرحلة الأولى من IKE، يتفاوض نظراء IPsec على سياسة اقتران أمان IKE (SA) التي تم إنشاؤها. بمجرد مصادقة النظراء، يتم إنشاء نفق آمن باستخدام بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP).
3. 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.
4. يتم إنشاء نفق IPsec ويتم نقل البيانات بين نظائر IPsec استنادا إلى معلمات IPsec التي تم تكوينها في مجموعات تحويل IPsec.
5. ينتهي نفق IPsec عند حذف وحدات IPsec SAs أو عند انتهاء صلاحية مدة حياتها.

ملاحظة: يفشل مفاوضة IPsec بين PIXs إذا لم تتطابق عمليات SAs على كل من مرحلتي IKE مع عمليات النظير.

التكوين

- تكوين ASDM
- تكوينات PIX CLI

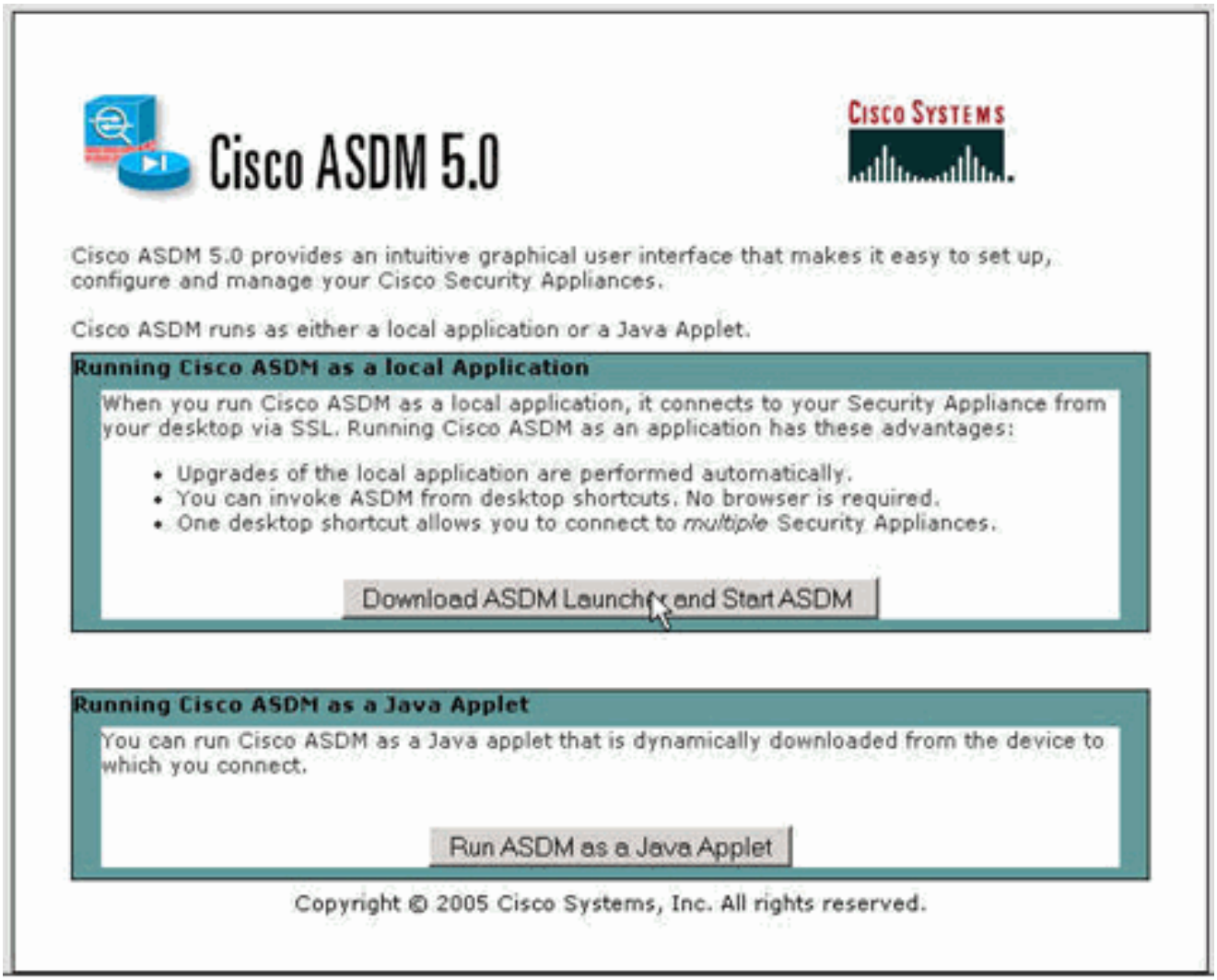
تكوين ASDM

أكمل الخطوات التالية:

1. افتح المستعرض واكتب https://<inside_ip_address_of_pix> للوصول إلى ASDM على PIX.

   تأكد من تخويل أية تحذيرات يعطيك المستعرض لها علاقة بموثوقية شهادة SSL. اترك حقلي username وكلمة السر فارغين.

   يقدم PIX هذه النافذة للسماح بتنزيل تطبيق ASDM. يقوم هذا المثال بتحميل التطبيق على الكمبيوتر المحلي والا يعمل في تطبيق Java.

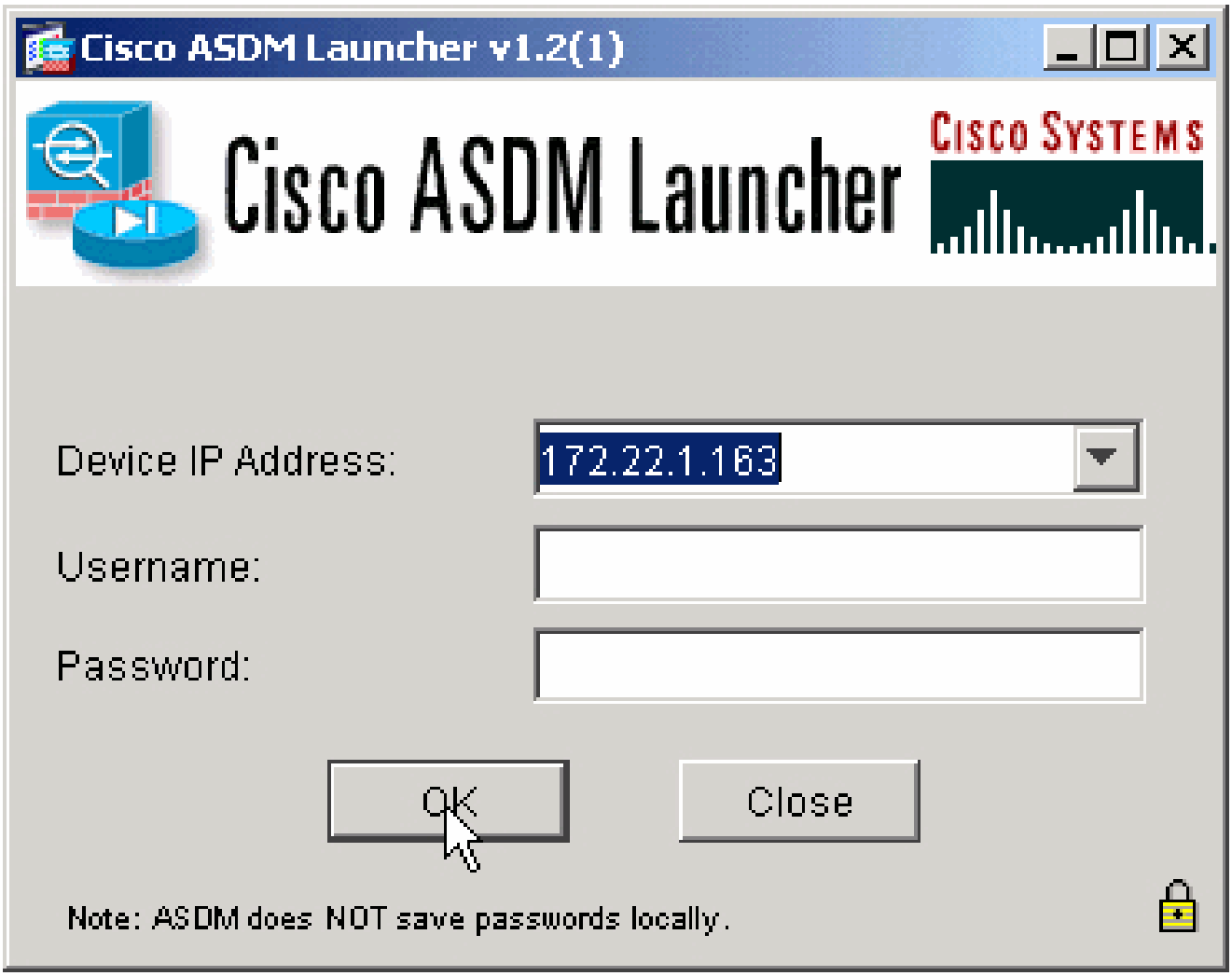


2. انقر على تنزيل مشغل ASDM وابدأ ASDM لتنزيل المثبت الخاص بتطبيق ASDM.

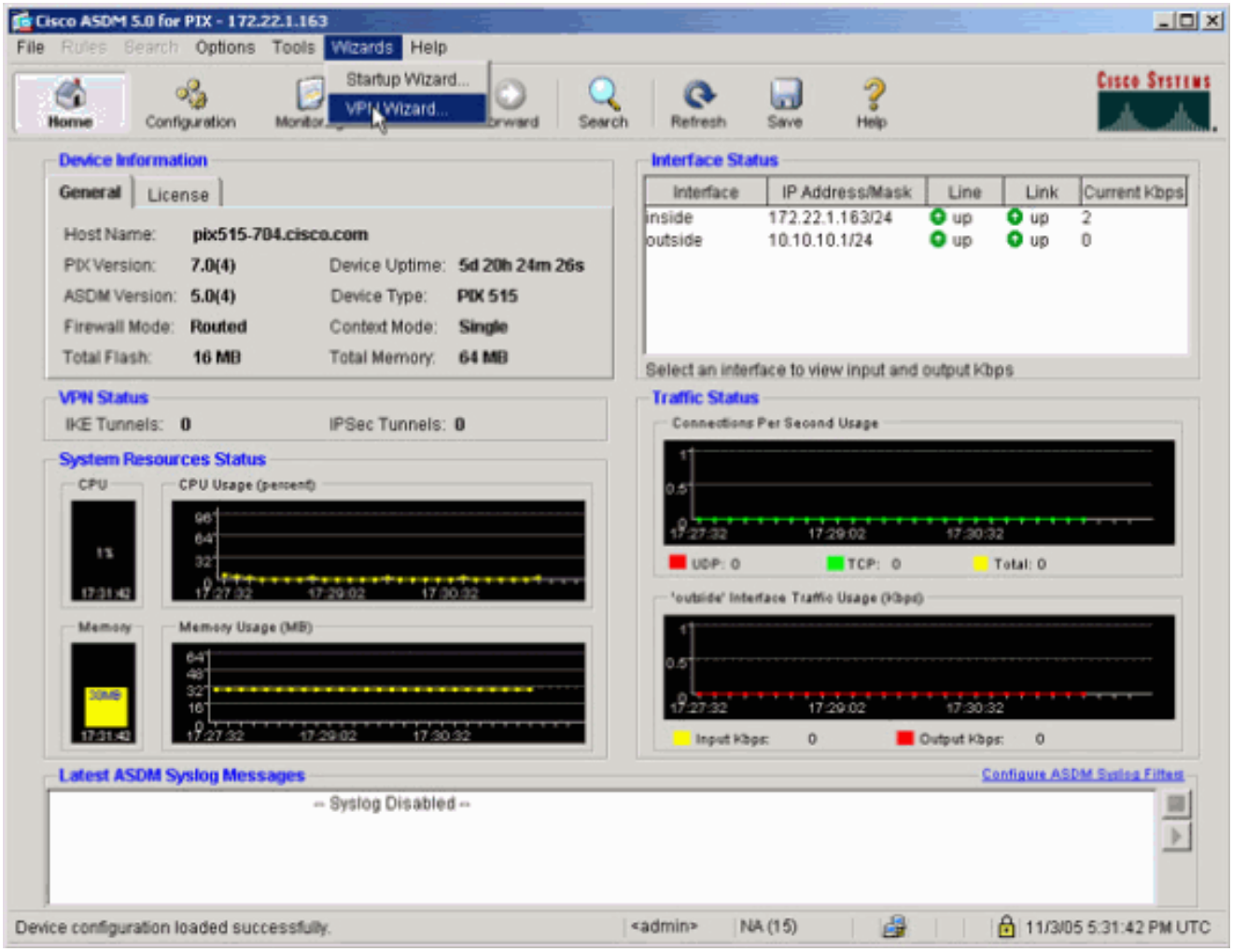
3. بمجرد تنزيل مشغل ASDM، اتبع المطالبات لتثبيت البرنامج وتشغيل مشغل ASDM من Cisco.

4. أدخل عنوان IP للواجهة التي قمت بتكوينها باستخدام الأمر http - واسم مستخدم وكلمة مرور إذا قمت بتحديد واحد.

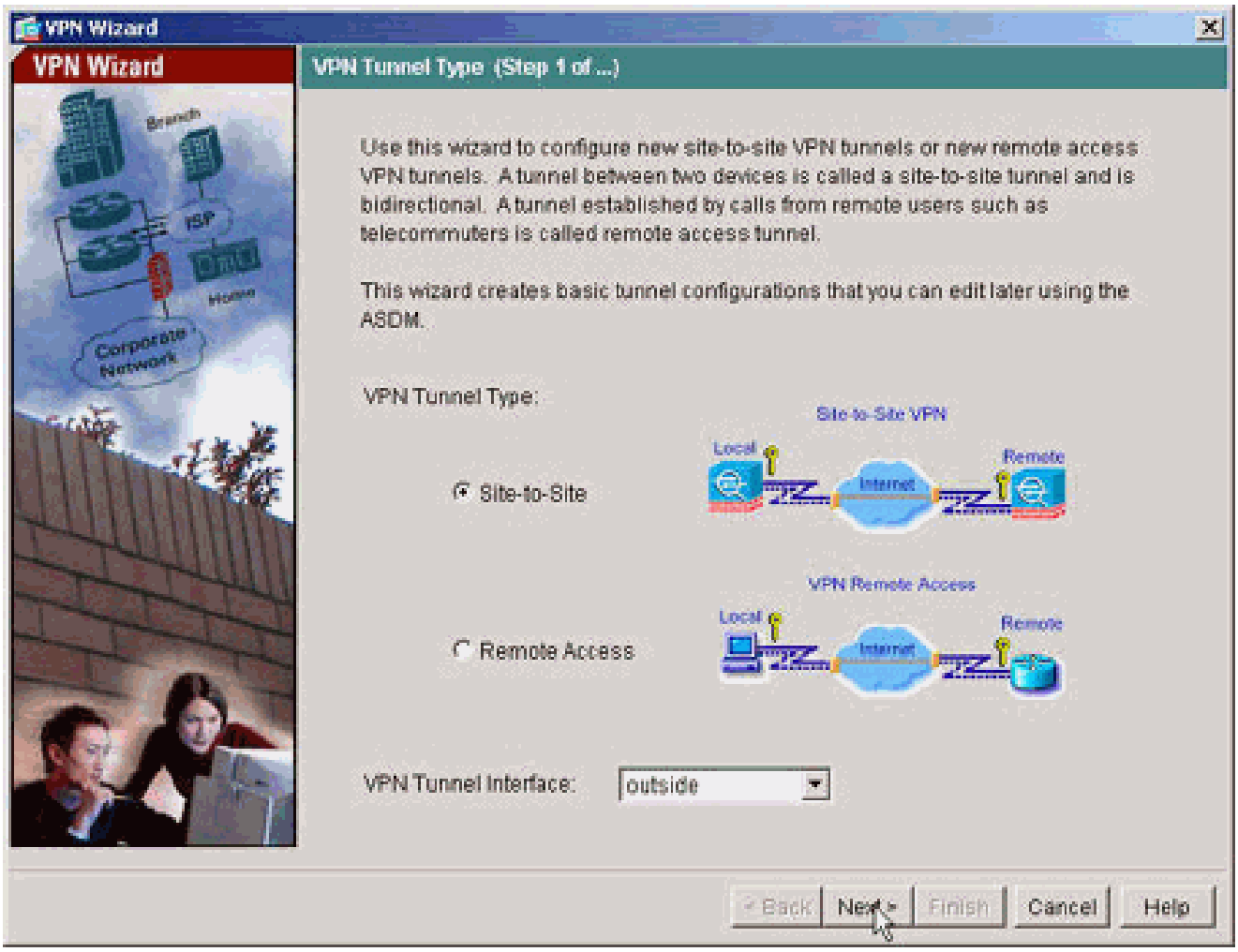
يستعمل هذا مثال التقصير فارغ username وكلمة.



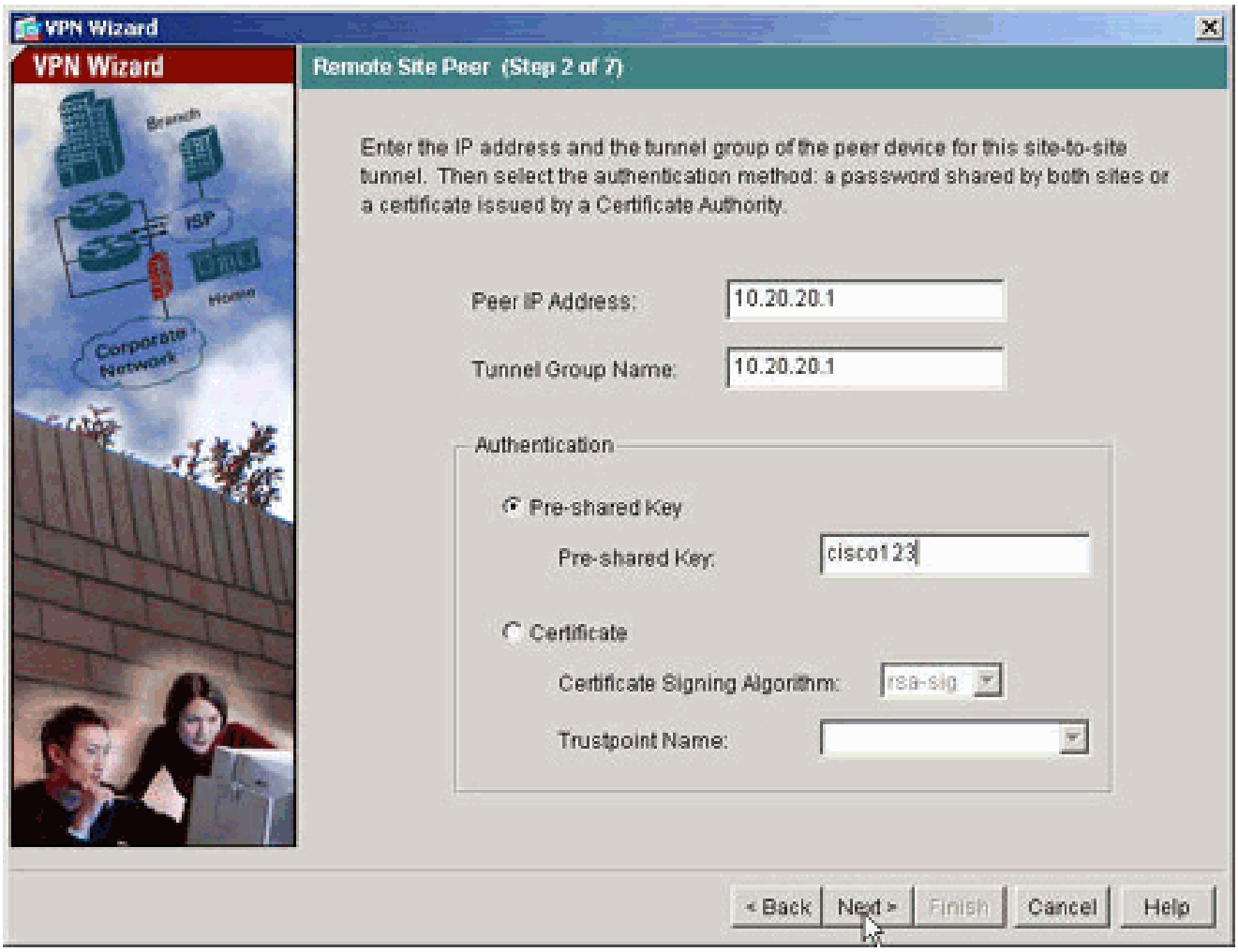
قم بتشغيل معالج VPN بمجرد اتصال تطبيق ASDM ب PIX.5.



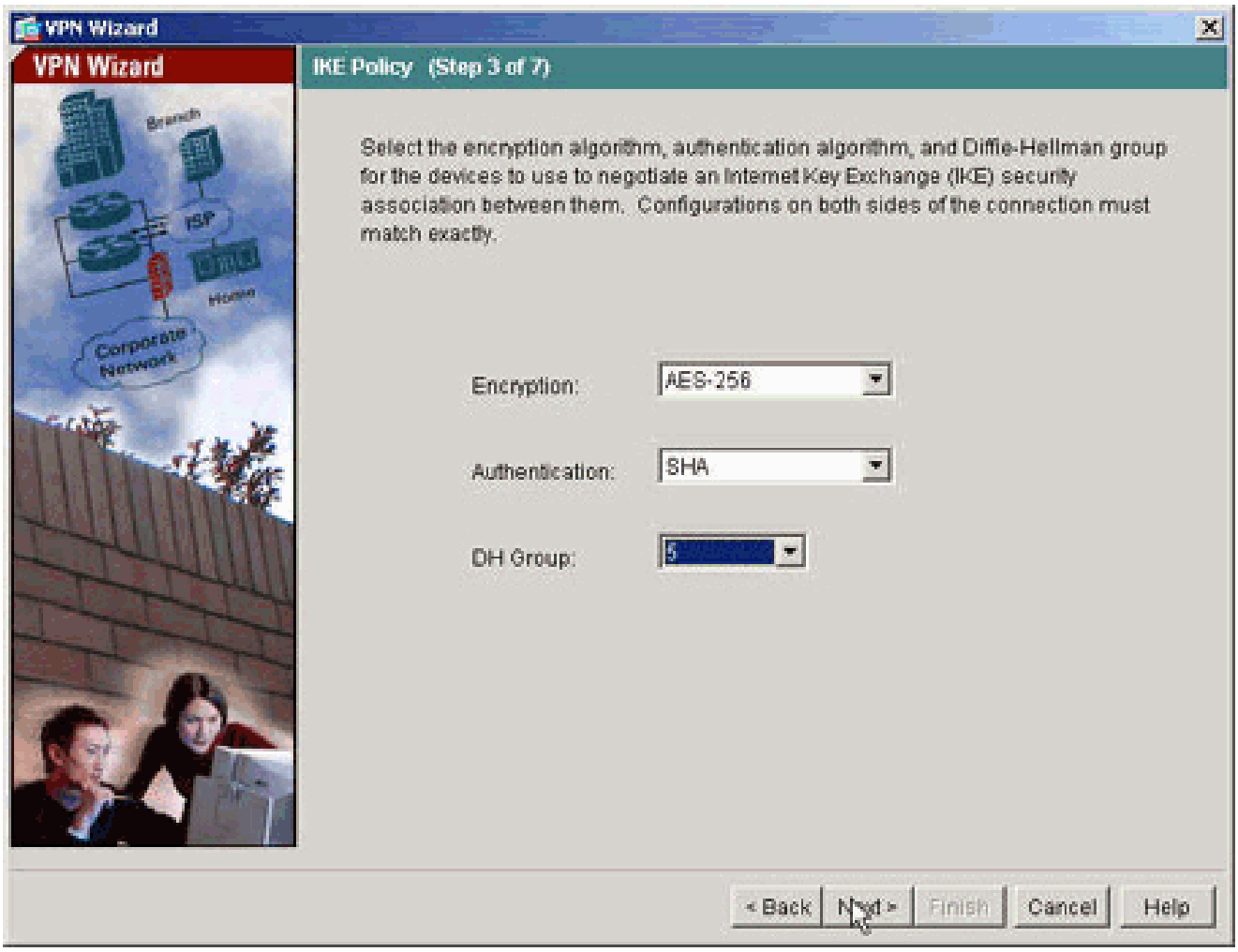
6. أختر نوع نفق VPN من موقع إلى موقع.



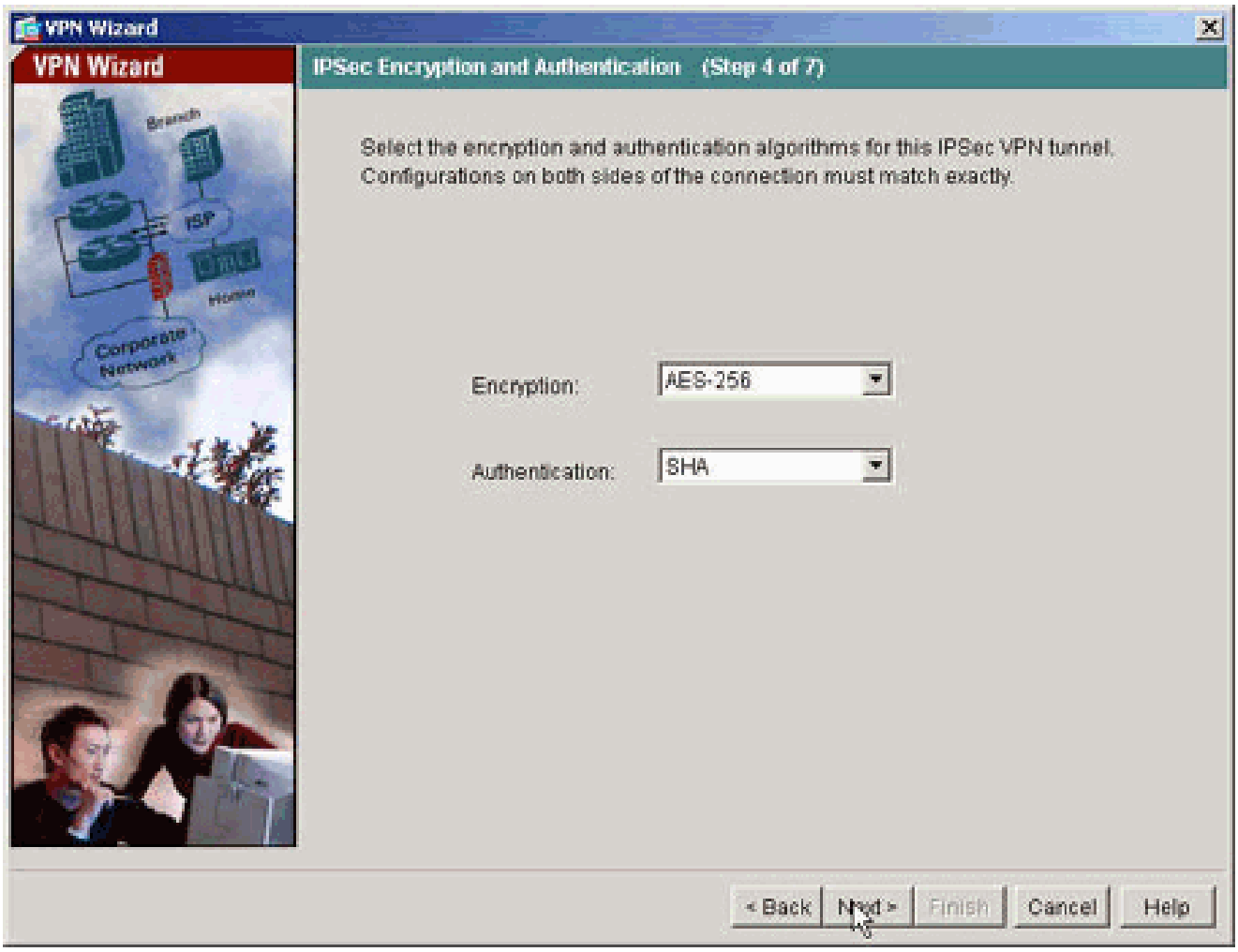
حدد عنوان IP الخارجي للنظير البعيد. أدخل معلومات المصادقة المراد إستخدامها (مفتاح7. مشترك مسبقا في هذا المثال).



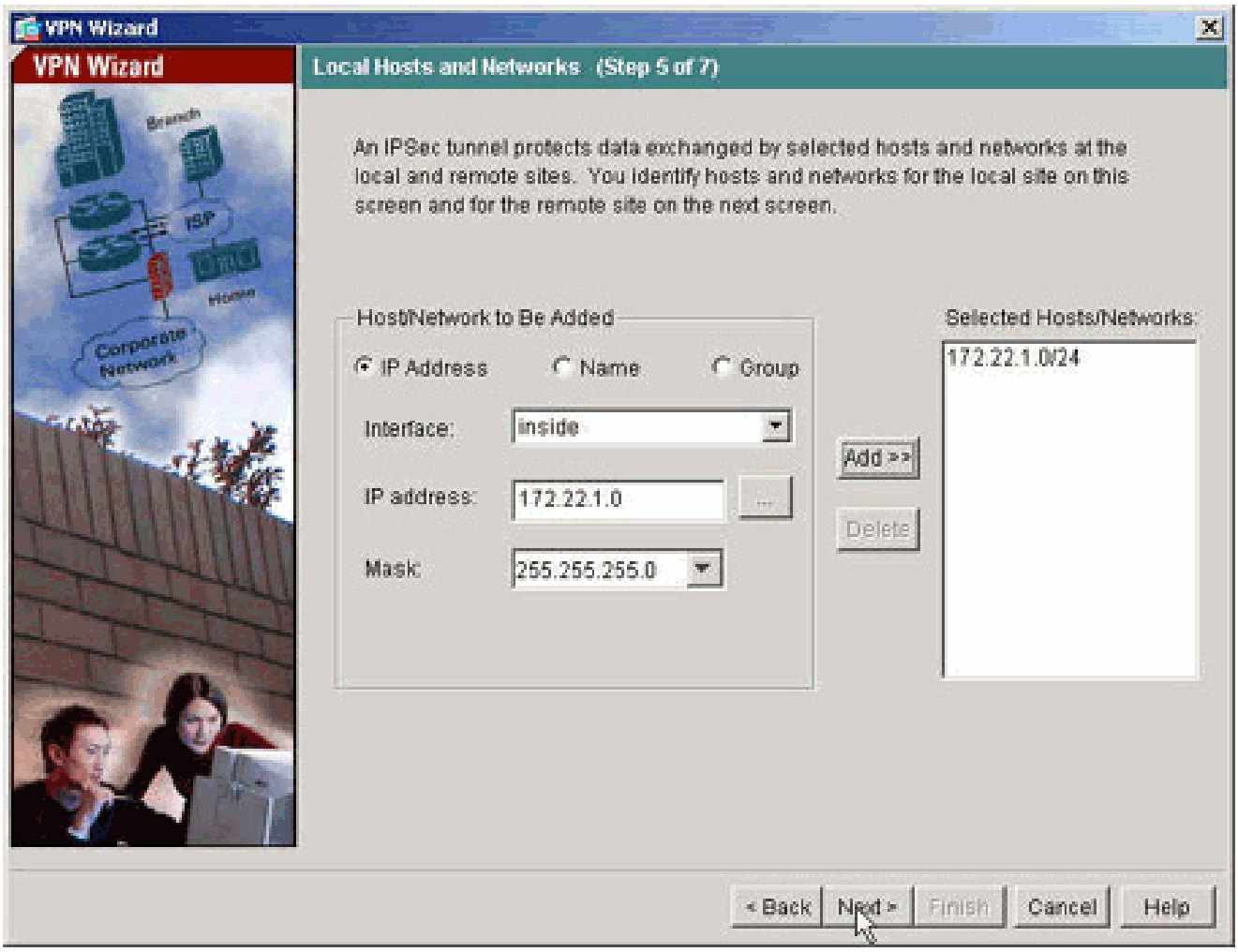
8. حدد السمات التي سيتم إستخدامها ل IKE، المعروفة أيضا باسم "المرحلة 1". يجب أن تكون هذه السمات واحدة على كل جانبي النفق.



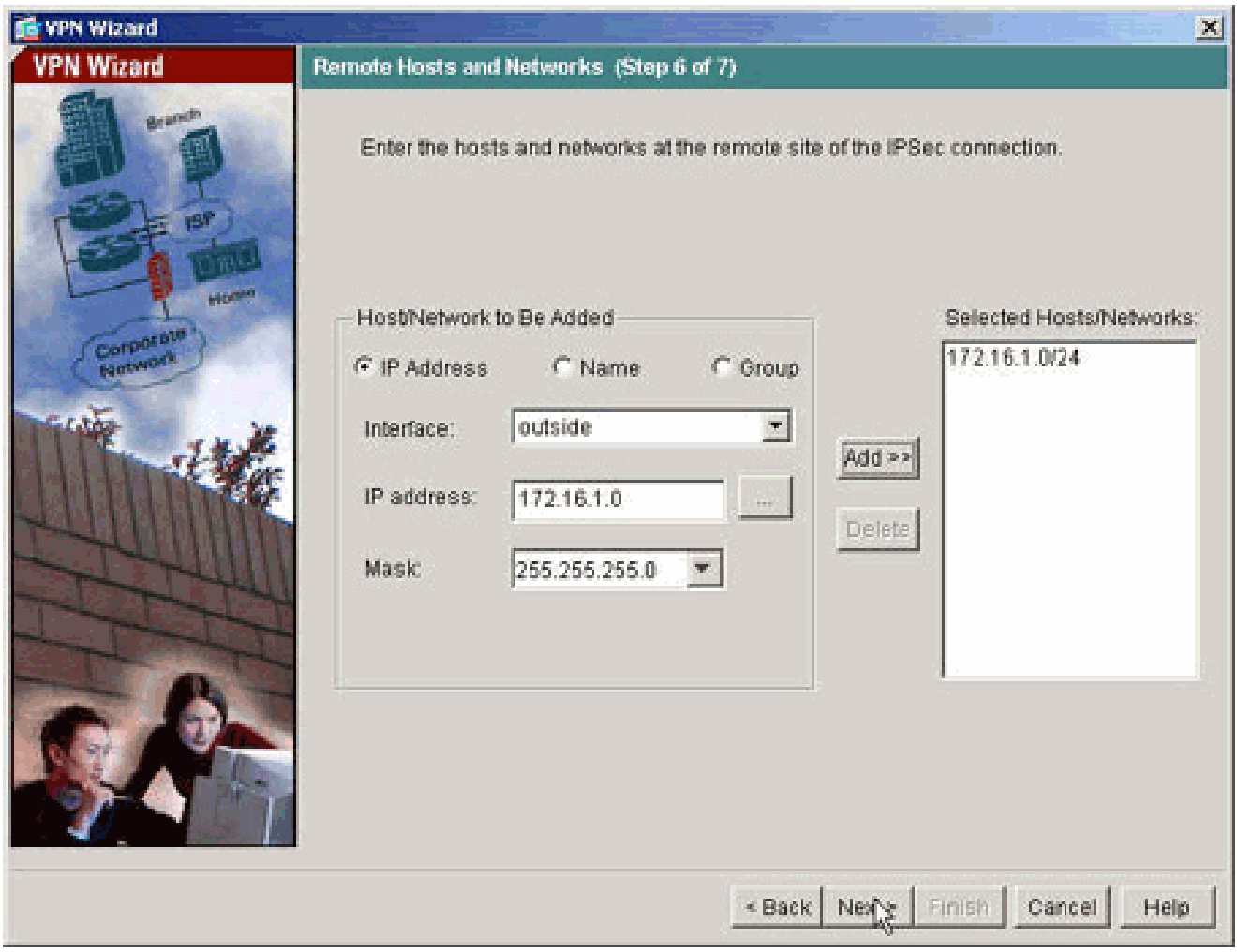
9. حدد السمات التي سيتم إستخدامها ل IPsec، المعروفة أيضا باسم "المرحلة 2". يجب أن تتطابق هذه السمات على كل الجانبين.



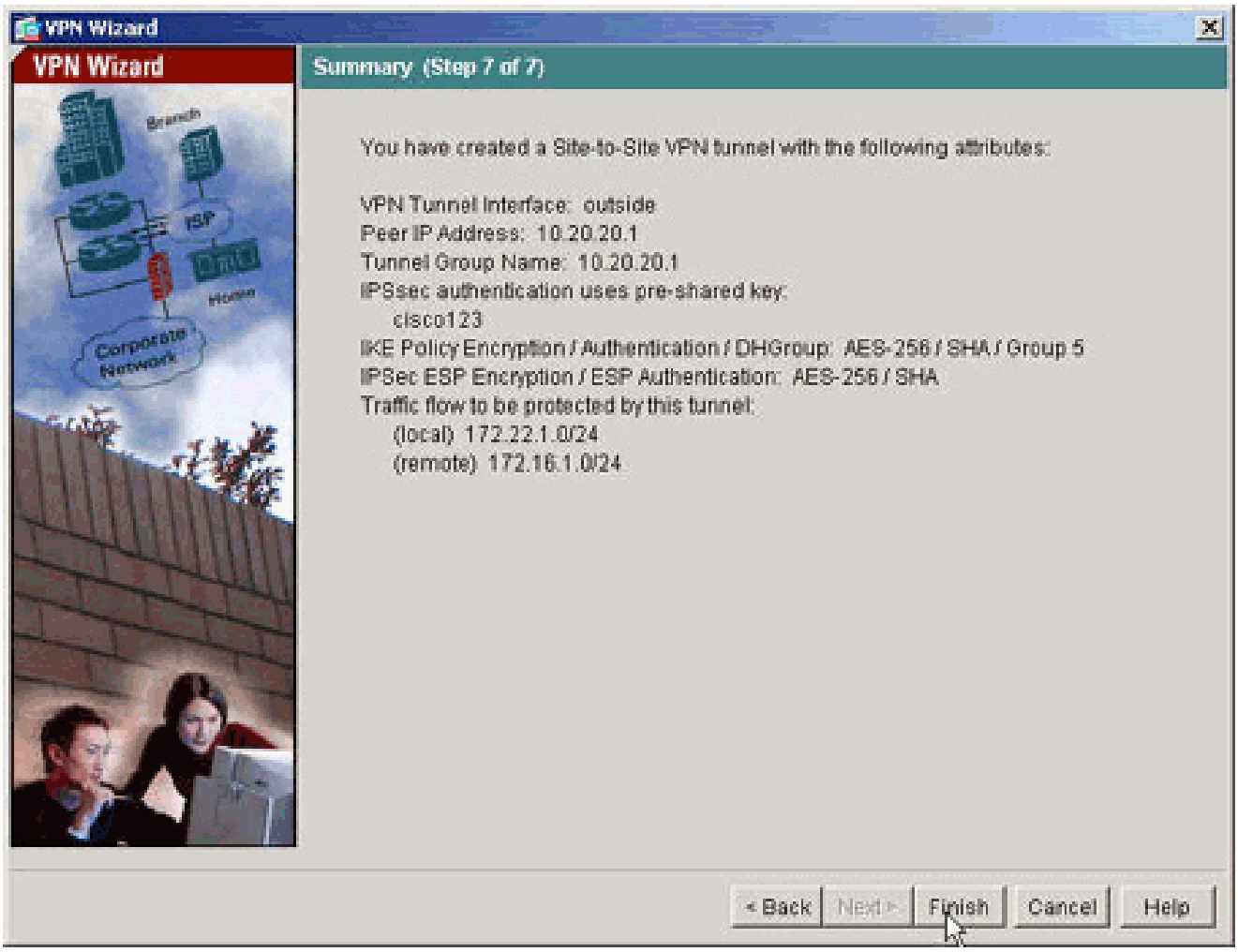
10. حدد البيئات المضيفة التي يجب السماح لحركة مرور البيانات الخاصة بها بالمرور من خلال نفق VPN. في هذه الخطوة، عينت المضيف محلي إلى PIX515-704.



11. يتم تحديد البيئات المضيفة والشبكات الموجودة على الجانب البعيد من النفق.



12. يتم عرض السمات التي تم تعريفها بواسطة معالج الشبكة الخاصة الظاهرية (VPN) في هذا الملخص. تحقق مرة أخرى من التكوين وانقر فوق إنهاء عندما ترضى بأن الإعدادات صحيحة.



تكوين PIX CLI

command. !--- This prevents traffic which matches the access list from undergoing !--- network addres

```
!--- PHASE 1 CONFIGURATION ---! !--- This configuratio
```

PIX-02

```
<#root>

PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 10.20.20.1 255.255.255.0
!
interface Ethernet1
nameif inside
security-level 100
ip address 172.16.1.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name default.domain.invalid

access-list inside_nat0_outbound extended permit ip 172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0

!--- Note that this ACL is a mirror of the

inside_nat0_outbound

!--- ACL on pix515-704.

access-list outside_cryptomap_20 extended permit ip 172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0

!--- Note that this ACL is a mirror of the

outside_cryptomap_20

!--- ACL on pix515-704.

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image flash:/asdm-511.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list inside_nat0_outbound
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 inside
```

```
no snmp-server location
no snmp-server contact
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto map outside_map 20 match address outside_cryptomap_20
crypto map outside_map 20 set peer 10.10.10.1
crypto map outside_map 20 set transform-set ESP-AES-256-SHA
crypto map outside_map interface outside
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 5
isakmp policy 10 lifetime 86400
tunnel-group 10.10.10.1 type ipsec-l2l
tunnel-group 10.10.10.1 ipsec-attributes
pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:6774691244870705f858ad4e9b810874
: end
pixfirewall#
```

نفق موقع النسخة الاحتياطية

لتحديد نوع الاتصال لميزة "موقع النسخة الاحتياطية إلى موقع" لإدخال خريطة التشفير crypto map set connection-type في وضع التكوين العام. أستخدم الصيغة هذه، أستخدم الأمر no من هذه الأمر للعودة إلى الإعداد الافتراضي.

الصيغة:

<#root>

crypto map *map-name seq-num set* **connection-type {answer-only | originate-only | bidirectional}**

- الإجابة فقط—يحدد هذا أن هذا النظير يستجيب فقط الاتصالات IKE الواردة أولا أثناء البادئ الأولي لحقوق الملكية لتحديد النظير المناسب الذي يتم الاتصال به.
- ثنائي الإتجاه—يحدد هذا أن هذا النظير يمكنه قبول الاتصالات وإنشاؤها استنادا إلى إدخال خريطة التشفير هذه. هذا هو نوع الاتصال الافتراضي لكافة إتصالات الموقع إلى الموقع.
- الإنشاء فقط—يحدد هذا أن يقوم هذا النظير بتهيئة أول تبادل خاص لتحديد النظير المناسب الذي يتم الاتصال به.

يحدد الأمر crypto map set connection-type أنواع الاتصال لميزة Backup LAN-to-LAN. وهو يسمح بتحديد نظائر نسخ إحتياطي متعددة في نهاية واحدة من الاتصال. تعمل هذه الميزة فقط بين هذه الأنظمة الأساسية:

- Cisco ASA 5500 سلسلة من أمان أجهزة
- Cisco VPN 3000 Concentrator ومجمع Cisco ASA 5500 Series الأمان جهاز
- Cisco PIX Security Appliance Software، الإصدار 7.0 أو إصدار أحدث برنامج جهاز الأمان الذي يشغل Cisco ASA 5500 Series وجهاز الأمان

in order to شكلت نسخة إحتياطية lan اتصال إلى LAN، cisco يوصي أن أنت تشكل واحد نهاية مع طرف مصدر فقط الأصلي مع ال المفتاح ملكية، والنهايات مع يتعدد نهاية الأصلية في طرف فقط مع ال المفتاح ملكية جواب كإجابة نظير نسخ إحتياطية جهاز واحد الأقران. أو الأولوية لترتيب التشفير خريطة القران مجموعة الأمر مستخدم أمر، فقط النظير الأول في القائمة. وإذا لم يستجب ذلك النظير، الأصلي يتوافق مع النظير فقط الأمان نم المزيد لا يوجد أو نظير أي يستجيب أن إلى القائمة خفض على يعمل الأمان جهاز فإن القائمة في نظراء.

عند تكوينها بهذه الطريقة، يحاول النظير الأصلي في البداية فقط إنشاء نفق خاص إلى LAN شبكة من داخل اتصال إنشاء النظير من أي نظير. وبعد ذلك، يمكن مع يتوافق النظير عبر اتصال النفق من أي من البيانات ويمكن LAN شبكة.

ملاحظة: إذا قمت بتكوين شبكة VPN باستخدام عناوين IP نظيرة متعددة للإدخال التشفير، فسيتم إنشاء شبكة VPN باستخدام بروتوكول IP للنظير الاحتياطي بمجرد انخفاض النظير الأساسي. ومع ذلك، بمجرد عودة النظير الأساسي، لا تستبق الشبكة الخاصة الظاهرية (VPN) عنوان IP الأساسي. أنت ينبغي يدويا حامت ال SA موجود in order to restartup ال VPN مفاوضة أن يحول هو إلى العنوان أساسي. وكما يقول الاستنتاج، ال يتم دعم ميزة "الحماية الاستباقية للشبكات الخاصة الظاهرية (VPN)" في النفق من موقع إلى موقع.

أنواع اتصال شبكة LAN إلى شبكة LAN الاحتياطية المدعومة

الجانب البعيد	طرف مركزي
`Originate-Only`	`Answer-Only`

Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

مثال

يقوم هذا المثال، الذي تم إدخاله في وضع التكوين العام، بتكوين خريطة التشفير ويعين نوع الاتصال على الإنشاء فقط.

```
<#root>

hostname(config)#

crypto map outside_map 20 connection-type originate-only
```

مسح اقترانات الأمان (SAs)

في وضع الامتيازات ل PIX، أستخدم الأوامر التالية:

- مسح [crypto] ipSec sa—يحذف شبكات IPsec النشطة. كلمة التشفير الرئيسية إختيارية.
- مسح [crypto] isakmp sa— يحذف شبكات IKE النشطة. كلمة التشفير الرئيسية إختيارية.

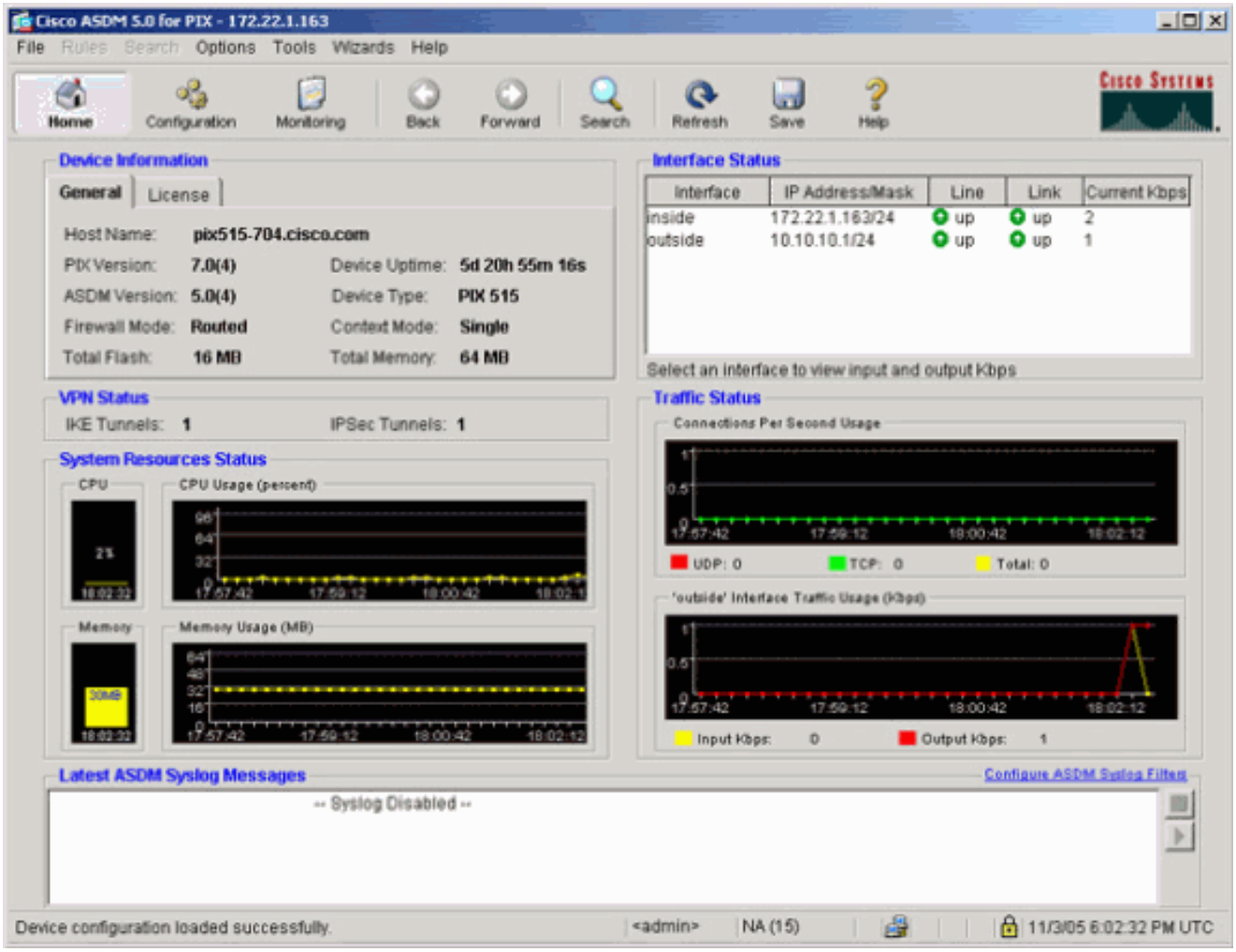
التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

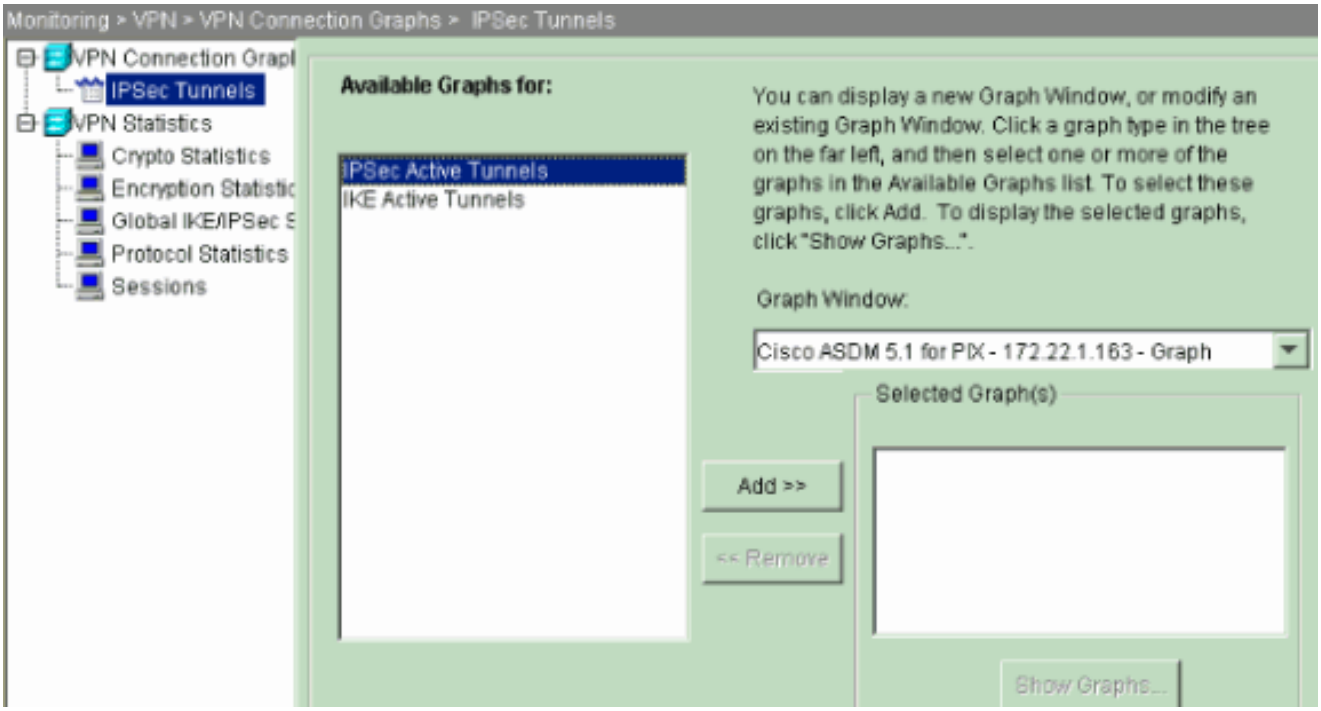
تدعم [أداة مترجم الإخراج (للعملاء المسجلين فقط)](#) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر show .

إذا كان هناك حركة مرور مثيرة للاهتمام إلى النظير، يتم إنشاء النفق بين PIX515-704 و PIX-02.

1. تكوين1 للتحقق من ASDM في الصفحة الرئيسية ضمن VPN عرض حالة شبكة النفق.

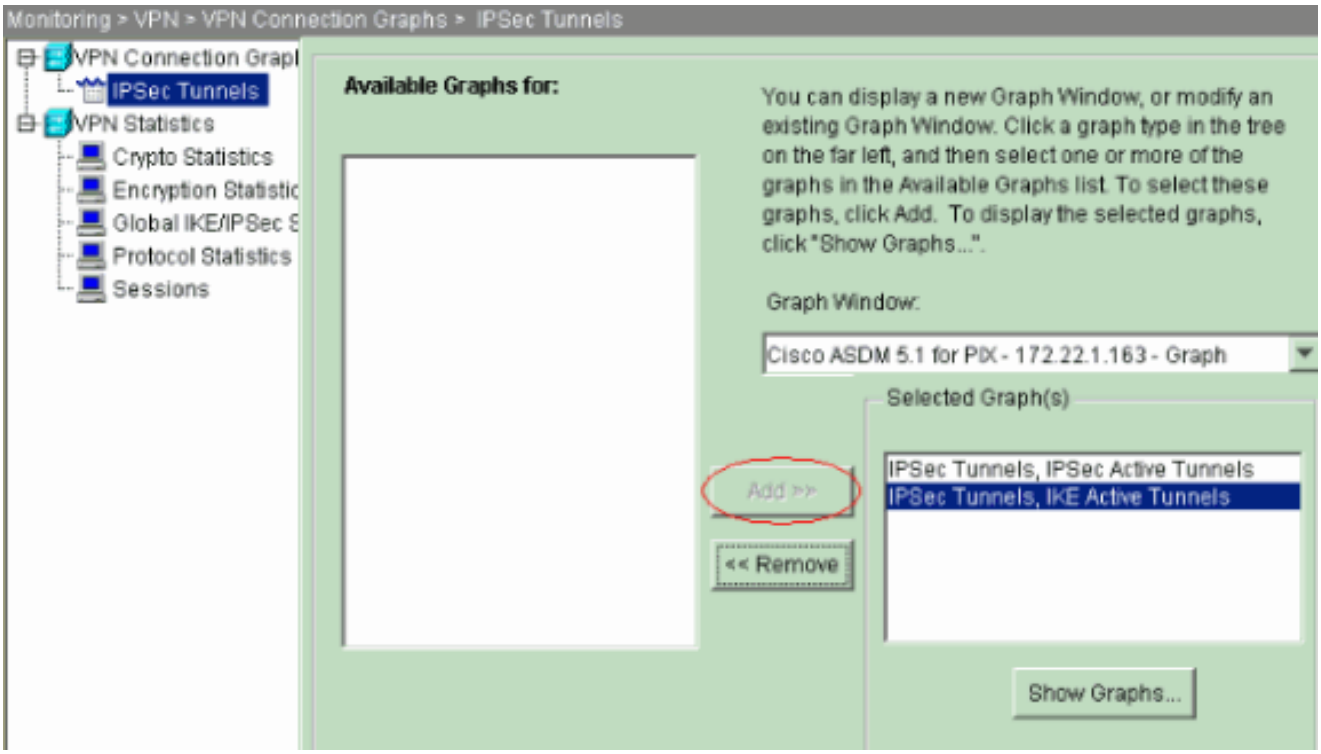


2. أخترت monitore>VPN>VPN توصيل رسم بياني > IPSec نفق in order to دقق
التفاصيل حول إنشاء النفق.

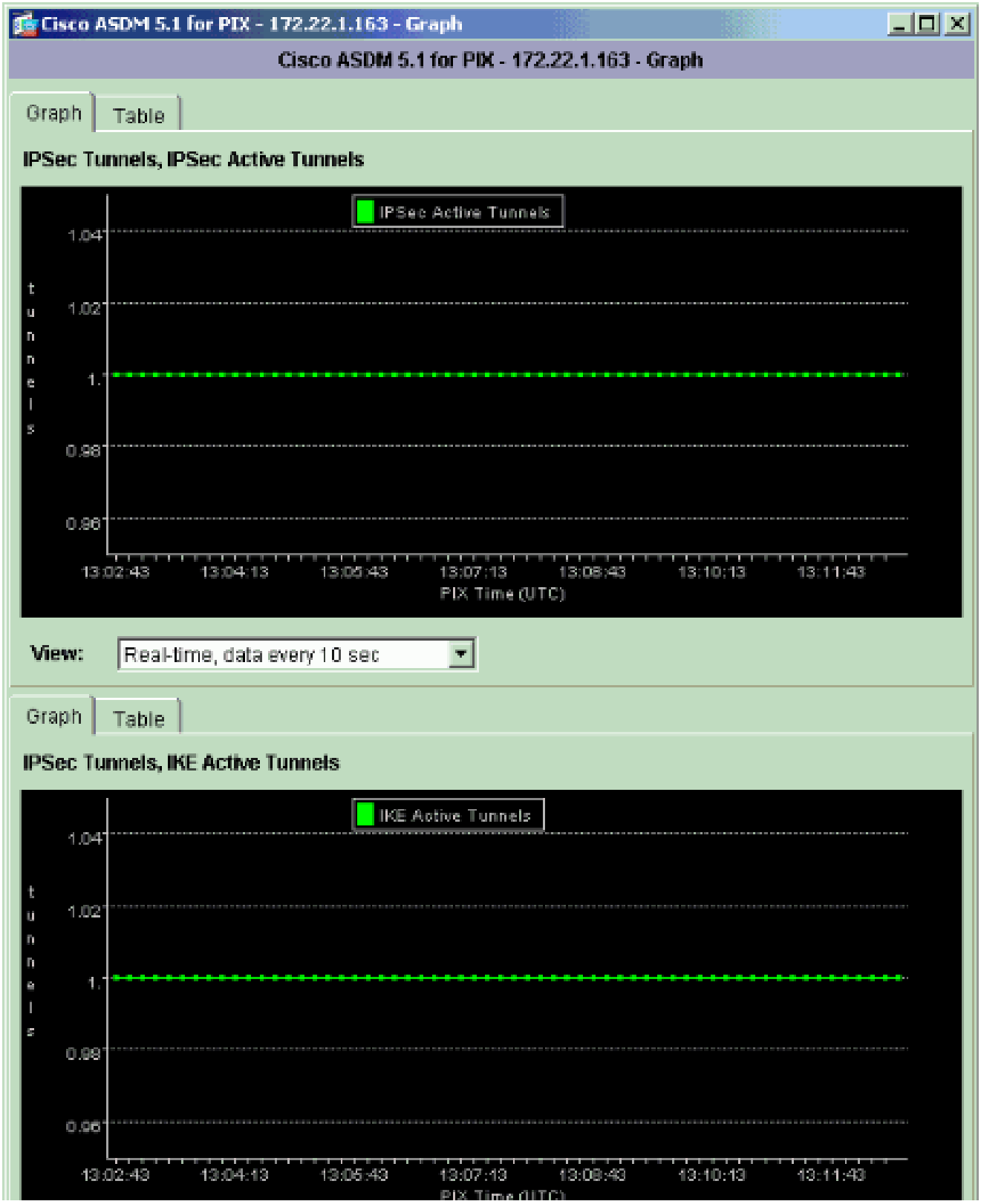


3. انقر فوق إضافة لتحديد الرسومات البيانية المتوفرة للعرض في نافذة الرسم

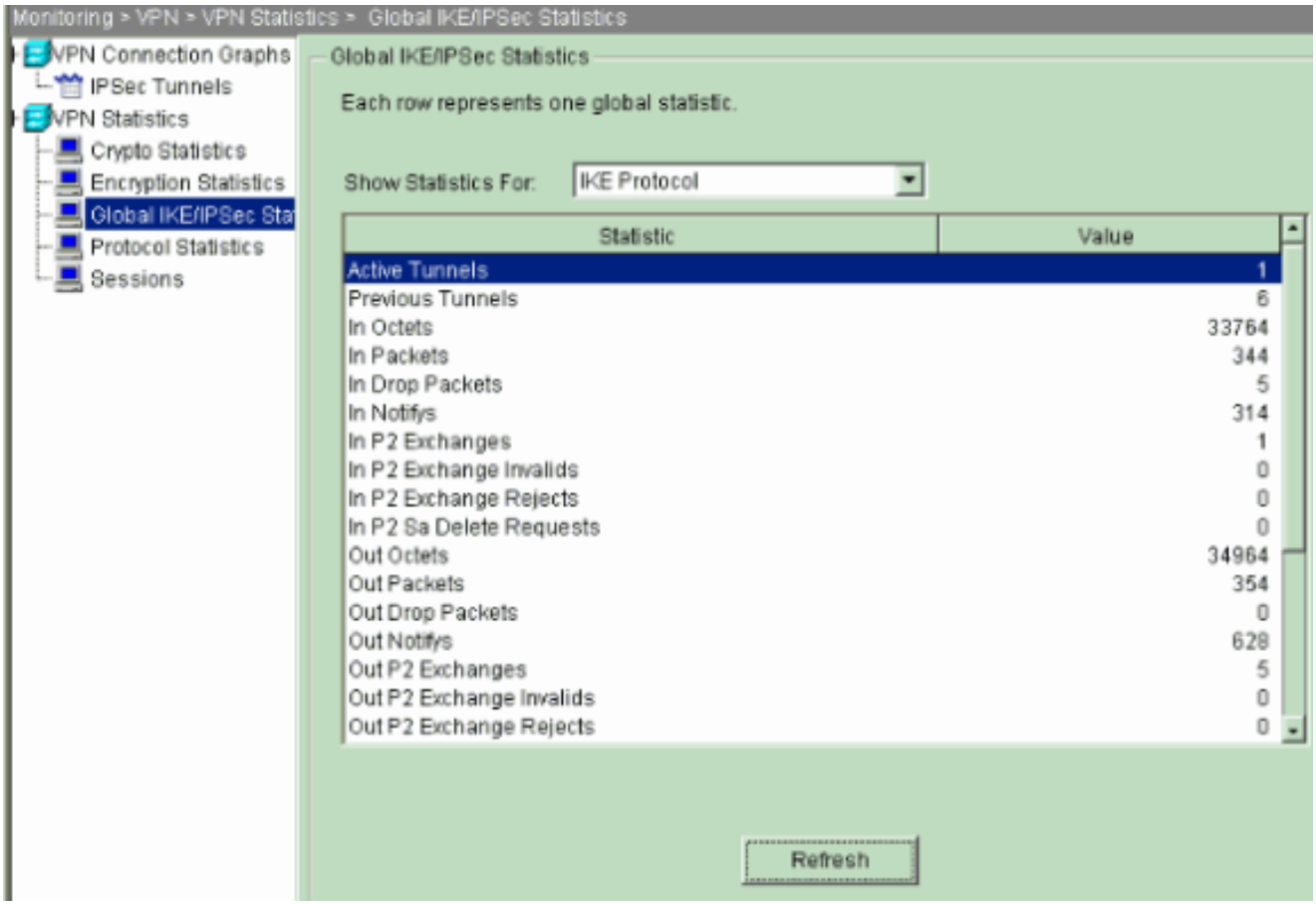
البياني.



4. انقر فوق إظهار الرسومات البيانية لعرض الرسومات البيانية لكل من الأنفاق النشطة IKE و IPsec.



5. أخترت monitore>VPN>VPN إحصائيات>شامل IKE/IPSec إحصائيات in order to عرفت حول المعلومة الإحصائية من ال VPN نفق.



يمكنك أيضا التحقق من تكوين أنفاق باستخدام CLI (واجهة سطر الأوامر). قم بإصدار الأمر show crypto ipSec لمراقبة الأنفاق وأصدر الأمر show crypto isakmp sa للتحقق من تكوين عدد الحزم التي تم تكوينها، وتشفيرها، وما إلى ذلك.

سلسلة PIX 515-704
<#root> pixfirewall(config)# **show crypto isakmp sa** Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 10.20.20.1 Type : **L2L** Role : initiator Rekey : no State : **MM_ACTIVE**

سلسلة PIX 515-704

```
<#root>

pixfirewall(config)#

show crypto ipsec sa

                                                interface: outside
      Crypto map tag: outside_map, seq num: 20, local addr: 10.10.10.1

                  access-list outside_cryptomap_20 permit ip 172.22.1.0
                                  255.255.255.0 172.16.1.0 255.255.255.0
                                      local ident (addr/mask/prot/port):

                                          (172.22.1.0/255.255.255.0/0/0)

                                     remote ident (addr/mask/prot/port):

                                          (172.16.1.0/255.255.255.0/0/0)

                                               current_peer: 10.20.20.1

                    #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20
                    #pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20
                                #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp failed: 0
                                        #send errors: 0, #recv errors: 0

                                                   local crypto endpt.:

                                                               10.10.10.1

                                                 , remote crypto endpt.:

                                                               10.20.20.1


                          path mtu 1500, ipsec overhead 76, media mtu 1500
                                        current outbound spi: 44532974

                                                       inbound esp sas:
                                              spi: 0xA87AD6FA (2826622714)
                                         transform: esp-aes-256 esp-sha-hmac
                                            in use settings ={L2L, Tunnel, }
                                    slot: 0, conn_id: 1, crypto-map: outside_map
                  sa timing: remaining key lifetime (kB/sec): (3824998/28246)
                                                       IV size: 16 bytes
                                          replay detection support: Y
                                                       outbound esp sas:
                                              spi: 0x44532974 (1146300788)
                                         transform: esp-aes-256 esp-sha-hmac
                                            in use settings ={L2L, Tunnel, }
                                    slot: 0, conn_id: 1, crypto-map: outside_map
                  sa timing: remaining key lifetime (kB/sec): (3824998/28245)
                                                       IV size: 16 bytes
                                          replay detection support: Y
```

استكشاف الأخطاء وإصلاحها

PFS

في مفاوضات IPsec، تضمن سرية إعادة التوجيه الكاملة (PFS) عدم إرتباط كل مفتاح جديد بأي مفتاح سابق. إما أن يمكن أو أعجزت PFS على الك من نظائر النفق، والإ فإن نفق L2L IPsec ال يتم إنشاؤه في PIX/ASA.

ليتم تعطيل PFS بشكل افتراضي. لتمكين PFS، أستخدم الأمر pfs مع الكلمة الأساسية enable في وضع تكوين نهج المجموعة. تدخل in order to أعجزت PFS، ال disable الكلمة المفتاح.

<#root>

```
hostname(config-group-policy)#

pfs {enable | disable}
```

تدخل in order to أزلت ال PFS سمة من التشكيل جار، ال ما من شكل من اذه أمر. يمكن أن يرث نهج المجموعة قيمة ل PFS من نهج مجموعة آخر. أدخل الصيغة no من اذه الأمر لمنع توريث قيمة.

<#root>

```
hostname(config-group-policy)#

no pfs
```

الوصول إلى الإدارة

يوفر اذه القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

ال يمكن بحس الواجهة الداخلية ل PIX من الطرف الآخر من النفق ما لم يتم تكوين الأمر management-access في وضع التكوين العام.

<#root>

```
PIX-02(config)#

management-access inside

PIX-02(config)#

show management-access

management-access inside
```

أوامر التصحيح

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

debug crypto isakmp — يعرض معلومات تصحيح الأخطاء حول إتصالات IPsec، ويبدي المجموعة الأولى من السمات التي يتم رفضها بسبب عدم التوافق على كل النهايتين.

debug crypto isakmp

```
<#root>

pixfirewall(config)#

debug crypto isakmp 7

Nov 27 12:01:59 [IKEv1 DEBUG]: Pitcher: received a key acquire message,
                                                                spi 0x0
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE Initiator: New Phase 1,
Intf 2, IKE Peer 10.20.20.1  local Proxy Address 172.22.1.0, remote
                                Proxy Address 172.16.1.0,  Crypto map (outside_map)
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing ISAKMP SA payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing Fragmentation
                                                VID + extended capabilities payload
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message
                                                (msgid=0) with payloads : HDR +
                                        SA (1) + VENDOR (13) + NONE (0) total length : 148
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 112
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, processing SA payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Oakley proposal is acceptable
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Fragmentation VID
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, IKE Peer included
                                                IKE fragmentation capability flags
                                                                              :

                                                                    Main Mode

                                                :        True  Aggressive Mode:  True
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing ke payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing Cisco Unity VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing xauth V6 VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send IOS VID
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Constructing ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send Altiga/
                                                Cisco VPN3000/Cisco ASA GW VID
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13)
                                        + VENDOR (13) + NONE (0) total length
                                                                        : 320
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message
                                                (msgid=0) with payloads : HDR
+ KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
                                                NONE (0) total length : 320
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing ke payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing ISA_KE payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Cisco Unity client VID
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received xauth V6 VID
```

```
                Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload
                Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Processing VPN3000/ASA
               spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)
                Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Altiga/Cisco VPN3000/Cisco ASA
                                                                                GW VID
 Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection landed on tunnel_group 10.20.20.1
    Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Generating keys
                                                                      for Initiator...
                   Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                                            constructing ID payload
                   Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                                          constructing hash payload
                   Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                                          Computing hash for ISAKMP
                                       Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
                        Constructing IOS keep alive payload: proposal=32767/32767 sec.
                   Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                                        constructing dpd vid payload
         Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message (msgid=0)
           with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14) + VENDOR (13) +
                                                          NONE (0) total length : 119
        Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message (msgid=0)
           with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14) + VENDOR (13) +
                                                           NONE (0) total length : 96
                   Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                                              processing ID payload
                   Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                                            processing hash payload
                   Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                                            Computing hash for ISAKMP
                                       Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
                          Processing IOS keep alive payload: proposal=32767/32767 sec.
                   Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                                              processing VID payload
                   Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                                                  Received DPD VID
 Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection landed on tunnel_group 10.20.20.1
                   Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                                            Oakley begin quick mode
                         Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1,

                                                                  PHASE 1 COMPLETED

    Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Keep-alive type for this connection: DPD
                   Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                            Starting phase 1 rekey timer: 73440000 (ms)
           Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, IKE got
                                          SPI from key engine: SPI = 0x44ae0956
                   Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                                      oakley constucting quick mode
                   Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                                    constructing blank hash payload
                   Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                                    constructing IPSec SA payload
                   Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                                  constructing IPSec nonce payload
                   Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                                        constructing proxy ID
                   Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                                      Transmitting Proxy Id:
                      Local subnet:  172.22.1.0  mask 255.255.255.0 Protocol 0  Port 0
```

```
   Remote subnet: 172.16.1.0  Mask 255.255.255.0 Protocol 0  Port 0
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                        constructing qm hash payload
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message
                                        (msgid=d723766b) with payloads
: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) +
                                        NONE (0) total length : 200
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message
                                        (msgid=d723766b) with payloads
: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
                                        total length : 172
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                        processing hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                        processing SA payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                        processing nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                        processing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                        processing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                        loading all IPSEC SAs
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                        Generating Quick Mode Key!
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                        Generating Quick Mode Key!
      Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1,
    Security negotiation complete for LAN-to-LAN Group (10.20.20.1)
     Initiator, Inbound SPI = 0x44ae0956, Outbound SPI = 0x4a6429ba
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                        oakley constructing final quick mode
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message
                                        (msgid=d723766b) with payloads
                                : HDR + HASH (8) + NONE (0) total length : 76
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                               IKE got a KEY_ADD msg for SA: SPI = 0x4a6429ba
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
                                Pitcher: received KEY_UPDATE, spi 0x44ae0956
      Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1,
                    Starting P2 Rekey timer to expire in 24480 seconds
      Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1,

                                                    PHASE 2 COMPLETED

                                                    (msgid=d723766b)
```

debug crypto ipSec—يعرض معلومات تصحيح الأخطاء حول إتصالات IPsec.

debug crypto ipSec
<#root> pix1(config)# **debug crypto ipsec 7**

```
                                        exec mode commands/options:
       <1-255>  Specify an optional debug level (default is 1)
                                                              <cr>
                                pix1(config)# debug crypto ipsec 7
    pix1(config)# IPSEC: New embryonic SA created @ 0x024211B0,
                                                SCB: 0x0240AEB0,
                                              Direction: inbound
                                           SPI      : 0x2A3E12BE
                                         Session ID: 0x00000001
                                         VPIF num  : 0x00000001
                                               Tunnel type: l2l
                                               Protocol   : esp
                                        Lifetime   : 240 seconds
                  IPSEC: New embryonic SA created @ 0x0240B7A0,
                                                SCB: 0x0240B710,
                                             Direction: outbound
                                           SPI      : 0xB283D32F
                                         Session ID: 0x00000001
                                         VPIF num  : 0x00000001
                                               Tunnel type: l2l
                                               Protocol   : esp
                                        Lifetime   : 240 seconds
               IPSEC: Completed host OBSA update, SPI 0xB283D32F
IPSEC: Updating outbound VPN context 0x02422618, SPI 0xB283D32F
                                                Flags: 0x00000005
                                                SA   : 0x0240B7A0
                                                SPI  : 0xB283D32F
                                                MTU  : 1500 bytes
                                                VCID : 0x00000000
                                                Peer : 0x00000000
                                                SCB  : 0x0240B710
                                              Channel: 0x014A45B0
          IPSEC: Completed outbound VPN context, SPI 0xB283D32F
                                              VPN handle: 0x02422618
           IPSEC: Completed outbound inner rule, SPI 0xB283D32F
                                                Rule ID: 0x01FA0290
                IPSEC: New outbound permit rule, SPI 0xB283D32F
                                              Src addr: 10.10.10.1
                                         Src mask: 255.255.255.255
                                              Dst addr: 10.20.20.1
                                         Dst mask: 255.255.255.255
                                                          Src ports
                                                           Upper: 0
                                                           Lower: 0
                                                       Op   : ignore
                                                          Dst ports
                                                           Upper: 0
                                                           Lower: 0
                                                       Op   : ignore
                                                        Protocol: 50
                                                Use protocol: true
                                                   SPI: 0xB283D32F
                                                     Use SPI: true
          IPSEC: Completed outbound permit rule, SPI 0xB283D32F
                                                Rule ID: 0x0240AF40
              IPSEC: Completed host IBSA update, SPI 0x2A3E12BE
            IPSEC: Creating inbound VPN context, SPI 0x2A3E12BE
                                                Flags: 0x00000006
                                                SA   : 0x024211B0
                                                SPI  : 0x2A3E12BE
                                                   MTU  : 0 bytes
                                                VCID : 0x00000000
```

```
                                                Peer : 0x02422618
                                                SCB  : 0x0240AEB0
                                             Channel: 0x014A45B0
          IPSEC: Completed inbound VPN context, SPI 0x2A3E12BE
                                          VPN handle: 0x0240BF80
IPSEC: Updating outbound VPN context 0x02422618, SPI 0xB283D32F
                                                Flags: 0x00000005
                                                SA   : 0x0240B7A0
                                                SPI  : 0xB283D32F
                                                MTU  : 1500 bytes
                                                VCID : 0x00000000
                                                Peer : 0x0240BF80
                                                SCB  : 0x0240B710
                                             Channel: 0x014A45B0
         IPSEC: Completed outbound VPN context, SPI 0xB283D32F
                                          VPN handle: 0x02422618
          IPSEC: Completed outbound inner rule, SPI 0xB283D32F
                                           Rule ID: 0x01FA0290
       IPSEC: Completed outbound outer SPD rule, SPI 0xB283D32F
                                           Rule ID: 0x0240AF40
           IPSEC: New inbound tunnel flow rule, SPI 0x2A3E12BE
                                        Src addr: 172.16.1.0
                                      Src mask: 255.255.255.0
                                        Dst addr: 172.22.1.0
                                      Dst mask: 255.255.255.0
                                                     Src ports
                                                      Upper: 0
                                                      Lower: 0
                                                Op   : ignore
                                                     Dst ports
                                                      Upper: 0
                                                      Lower: 0
                                                Op   : ignore
                                                  Protocol: 0
                                             Use protocol: false
                                                 SPI: 0x00000000
                                                  Use SPI: false
      IPSEC: Completed inbound tunnel flow rule, SPI 0x2A3E12BE
                                           Rule ID: 0x0240B108
               IPSEC: New inbound decrypt rule, SPI 0x2A3E12BE
                                        Src addr: 10.20.20.1
                                   Src mask: 255.255.255.255
                                        Dst addr: 10.10.10.1
                                   Dst mask: 255.255.255.255
                                                     Src ports
                                                      Upper: 0
                                                      Lower: 0
                                                Op   : ignore
                                                     Dst ports
                                                      Upper: 0
                                                      Lower: 0
                                                Op   : ignore
                                                   Protocol: 50
                                            Use protocol: true
                                               SPI: 0x2A3E12BE
                                                 Use SPI: true
         IPSEC: Completed inbound decrypt rule, SPI 0x2A3E12BE
                                           Rule ID: 0x02406E98
                 IPSEC: New inbound permit rule, SPI 0x2A3E12BE
                                        Src addr: 10.20.20.1
                                   Src mask: 255.255.255.255
                                        Dst addr: 10.10.10.1
```

```
                                                Dst mask: 255.255.255.255
                                                                Src ports
                                                                 Upper: 0
                                                                 Lower: 0
                                                              Op   : ignore
                                                                Dst ports
                                                                 Upper: 0
                                                                 Lower: 0
                                                              Op   : ignore
                                                               Protocol: 50
                                                          Use protocol: true
                                                             SPI: 0x2A3E12BE
                                                              Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x2A3E12BE
                                                          Rule ID: 0x02422C78
```

معلومات ذات صلة

- إنشاء نفق متكرر بين جدران الحماية باستخدام PDM
- برنامج جدار حماية Cisco PIX
- مدير أجهزة حلول الأمان المعدلة من Cisco
- أجهزة الأمان Cisco ASA 5500 Series Adaptive Security Appliances
- جدار حماية PIX الآمن من Cisco وأوامر مرجع
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- طلبات التعليقات (RFCs)
- 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).