نفق IPsec بين مثال تكوين مركز PIX 7.x و VPN 3000

المحتويات

المقدمة

يقدم هذا المستند نموذجا لتكوين كيفية إنشاء نفق VPN من LAN إلى LAN IPsec بين جدار حماية PIX 7.x ومجمع Cisco VPN 3000.

ارجع إلى PIX/ASA 7.x Enhanced Talk-To-Client VPN مع مثال تكوين مصادقة TACACS+ لمعرفة المزيد حول السيناريو الذي يسمح فيه نفق شبكة LAN إلى شبكة LAN بين PIXs أيضا لعميل VPN بالوصول إلى PIX الذي يتم التحدث به من خلال PIX في الصرة.

ارجع إلى جهاز الأمان PIX/ASA 7.x إلى مثال تكوين نفق IPsec لموجه IOS إلى شبكة LAN لمعرفة المزيد حول السيناريو الذي يؤدي إلى نفق شبكة LAN إلى شبكة LAN بين جهاز PIX/ASA وموجه IOS.

المتطلبات الأساسية

المتطلبات

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

- يتطلب هذا المستند فهما أساسيا لبروتوكول IPsec. ارجع إلى مقدمة عن تشفير IPsec لمعرفة المزيد حول

.IPsec

المكونات المستخدمة

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

- جهاز الأمان Cisco PIX 500 Series Security Appliance مع إصدار البرنامج 7.1(1)
- مركز Cisco VPN 3060 مع إصدار البرنامج 4.7.2(B)

ملاحظة: لا يدعم المعيار PIX 506/506E الإصدار x.7.

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.

لتكوين PIX 6.x، ارجع إلى نفق IPSec من شبكة LAN إلى شبكة LAN بين مركز Cisco VPN 3000 ومثال تكوين جدار حماية PIX.

الاصطلاحات

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

التكوين

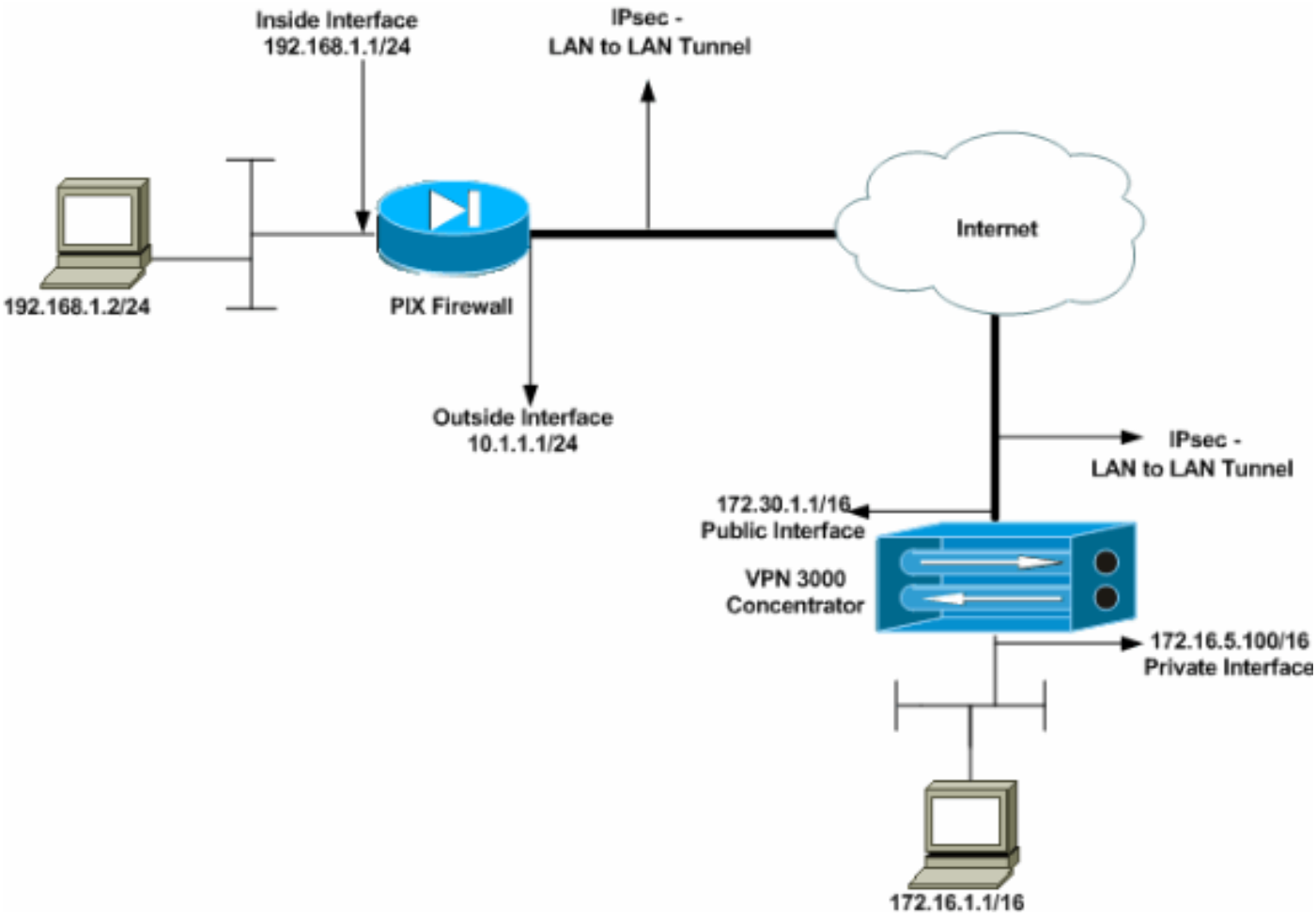
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

- تكوين PIX
- تكوين مركز VPN 3000

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



تكوين PIX

PIX

```
PIX7#show running-config
Saved :
:
(PIX Version 7.1(1
!
hostname PIX7
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
 Configures the outside interface of the PIX. !--- ---!
By default, the security level for the outside interface
is 0. interface Ethernet0
nameif outside
security-level 0
ip address 10.1.1.1 255.255.255.0
!
Configures the inside interface of the PIX. !--- By ---!
 default, the security level for the inside interface is
100. interface Ethernet1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
 Defines the IP addresses that should not be NATed. ---!
access-list nonat extended permit ip 192.168.1.0
255.255.255.0 172.16.0.0 255.255.0.0
access-list outside extended permit icmp any any
```

```
Defines the IP addresses that can communicate via ---!
the IPsec tunnel. access-list 101 extended permit ip
192.168.1.0 255.255.255.0 172.16.0.0 255.255.0.0
access-list OUT extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
asdm image flash:/asdm-504.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list nonat
access-group OUT in interface outside
route outside 0.0.0.0 0.0.0.0 10.1.1.2 1
Output is suppressed. !--- These are the IPsec ---!
parameters that are negotiated with the client. crypto
ipsec transform-set my-set esp-aes-256 esp-sha-hmac
crypto map mymap 20 match address 101
crypto map mymap 20 set peer 172.30.1.1
crypto map mymap 20 set transform-set my-set
crypto map mymap interface outside
These are the Phase I parameters negotiated by the ---!
two peers. isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
A tunnel group consists of a set of records !--- ---!
that contain tunnel connection policies. The two
attributes !--- are General and IPsec. Use the remote
peer IP address as the !--- name of the Tunnel group. In
this example 172.30.1.1 is the peer IP address. !---
Refer to Tunnel Group for more information. tunnel-group
172.30.1.1 type ipsec-121
tunnel-group 172.30.1.1 ipsec-attributes
* pre-shared-key
Output is suppressed. ! : end PIX7# ---!
```

تكوين مركز VPN 3000

لا يتم برمجة مركزات VPN مسبقا باستخدام عناوين IP في إعدادات المصنع الخاصة بها. أنت يضطر استعملت الوحدة طرفية للتحكم ميناء in order to شكلت التشكيل أولي أي يكون baser أمر خط قارن (CLI). ارجع إلى تكوين مركزات VPN من خلال وحدة التحكم للحصول على معلومات حول كيفية التكوين من خلال وحدة التحكم.

عقب يشكل أنت العنوان على الإثرنيت 1 (خاص) قارن، أنت يستطيع شكلت الإستراحة مع إما ال CLI أو من خلال المتصفح قارن. تدعم واجهة المستعرض كلا من HTTP و HTTP عبر طبقة مأخذ التوصيل الآمنة (SSL).

يتم تكوين هذه المعلمات من خلال وحدة التحكم:

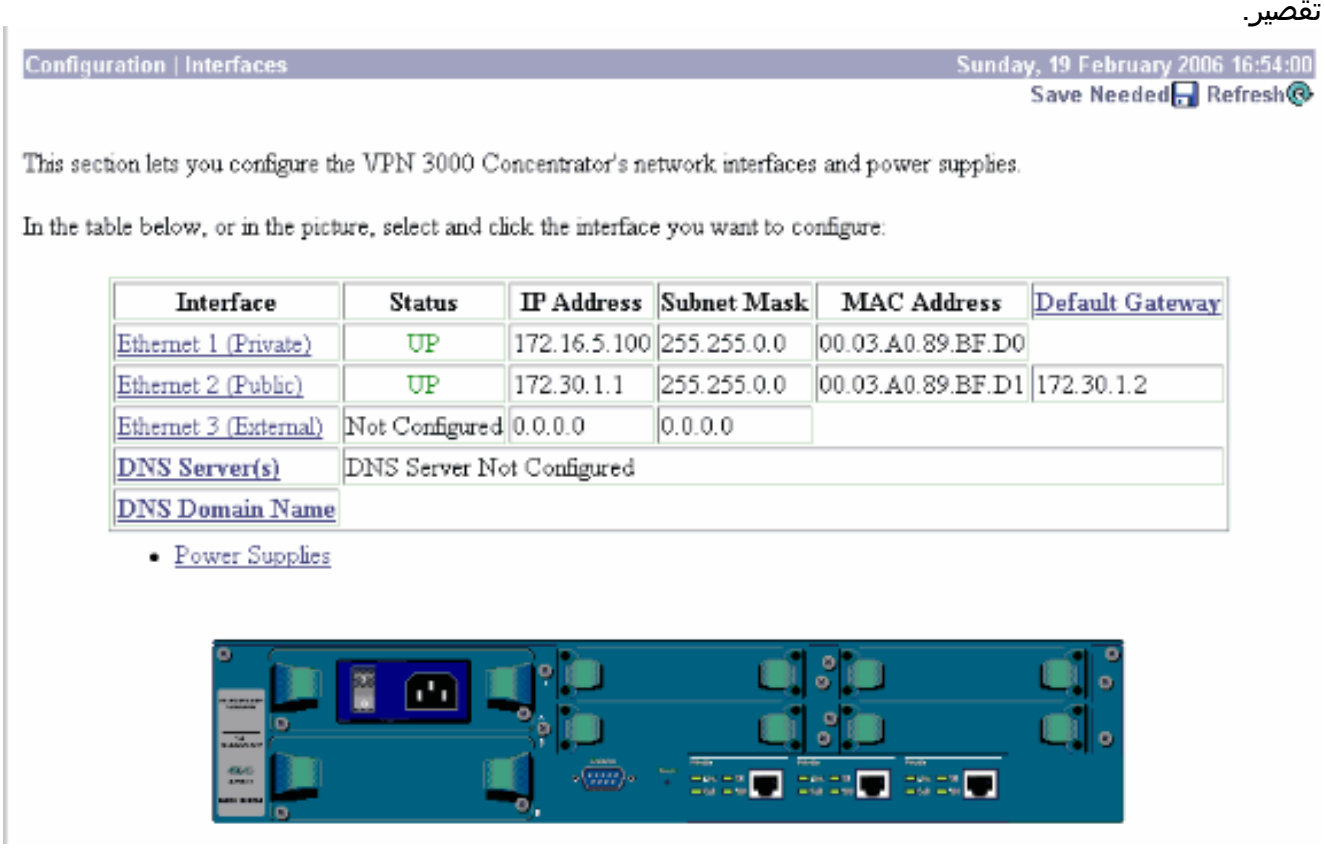
- **الوقت/التاريخ** — الوقت والتاريخ الصحيحان مهمان جدا. فهي تساعد على ضمان دقة إدخالات التسجيل والمحاسبة، وأن النظام يمكنه إنشاء شهادة أمان صالحة.
- **واجهة Ethernet 1 (الخاصة)** — عنوان IP وقناع (من مخطط الشبكة 16/172.16.5.100).

يمكن الوصول الآن إلى مركز الشبكة الخاصة الظاهرية (VPN) من خلال متصفح HTML من الشبكة الداخلية. ارجع إلى إستخدام واجهة سطر الأوامر للتكوين السريع للحصول على معلومات حول كيفية تكوين مركز VPN في وضع CLI.

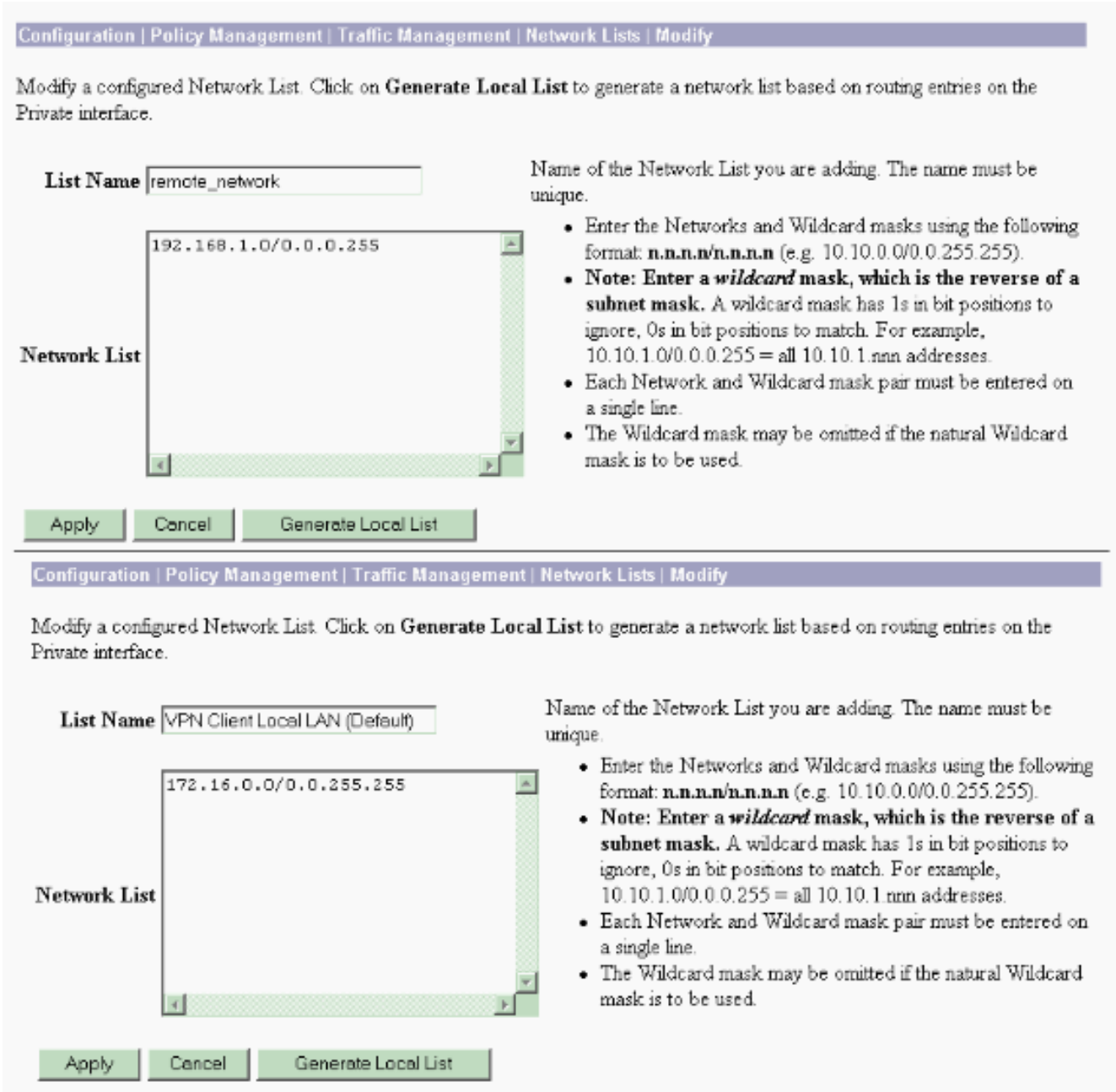
اكتب عنوان IP للواجهة الخاصة من مستعرض الويب لتمكين واجهة واجهة المستخدم الرسومية (GUI).

انقر فوق أيقونة **حفظ المطلوب** لحفظ التغييرات في الذاكرة. اسم المستخدم وكلمة المرور الافتراضيان في المصنع هما **admin**، وهو حساس لحالة الأحرف.

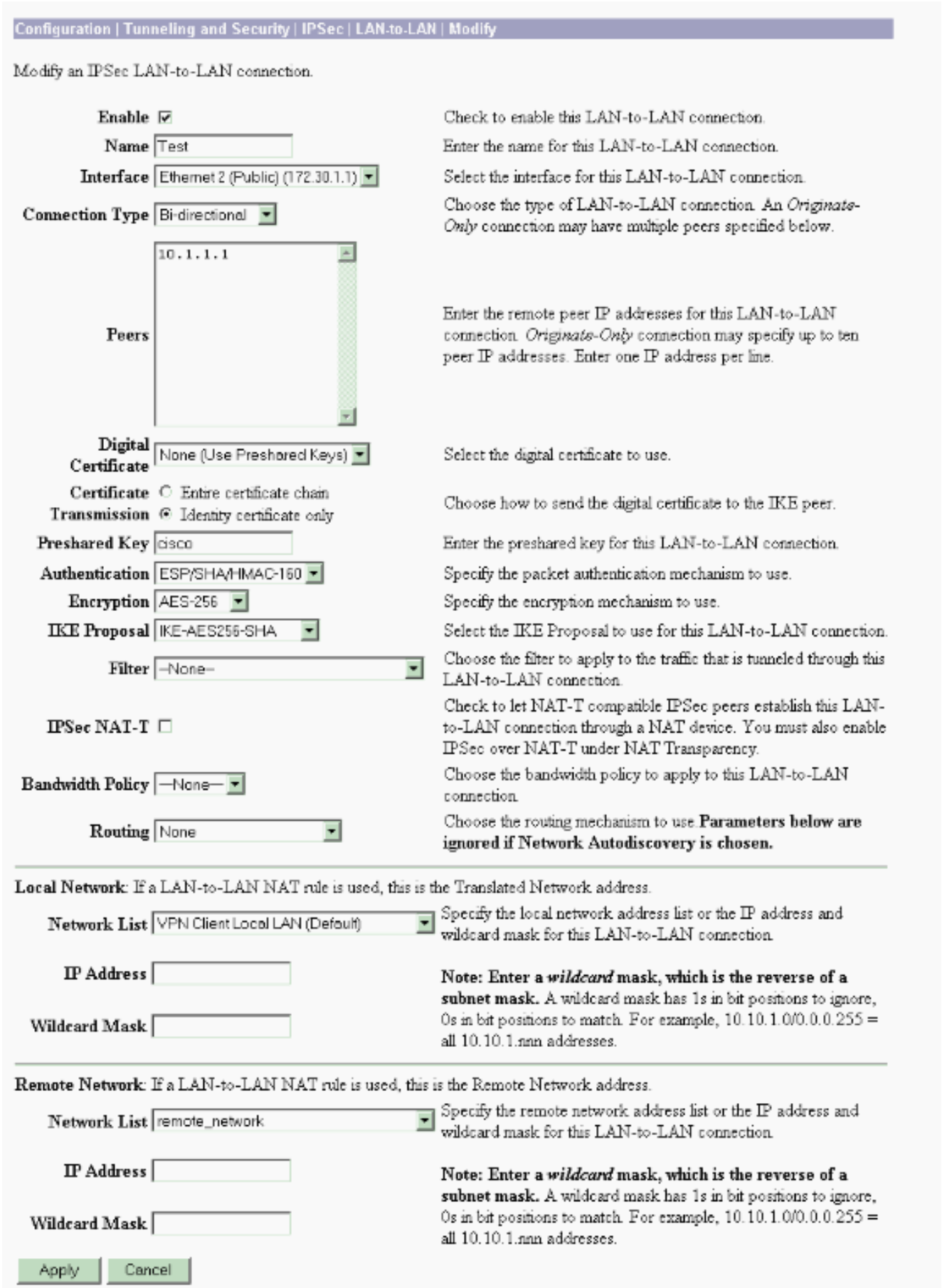
1. أطلقت ال gui وحدد **تشكيل>قارن** أن يشكل العنوان للقارن عام والقارن تقصير.



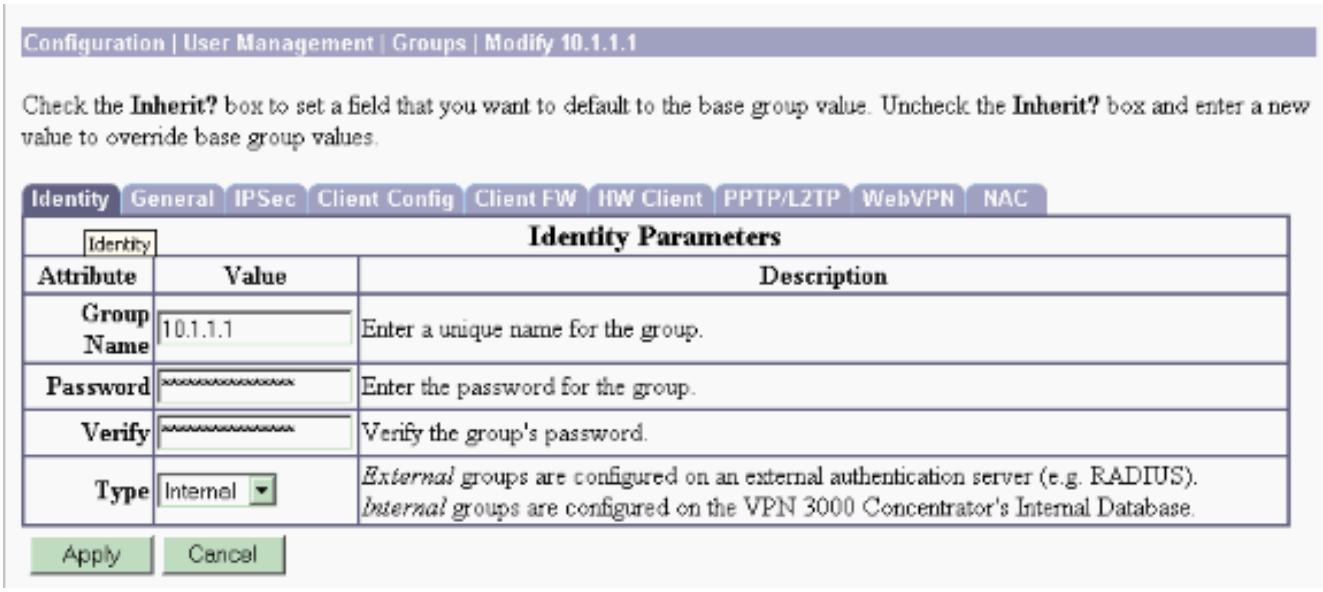
2. حدد **تكوين > إدارة السياسة > إدارة حركة المرور > قوائم الشبكة > إضافة أو تعديل** لإنشاء قوائم الشبكة التي تحدد حركة المرور التي سيتم تشفيرها.أضف كلا من الشبكات المحلية والبعيدة هنا. يجب أن تعكس عناوين IP العناوين الموجودة في قائمة الوصول التي تم تكوينها على PIX البعيد.في هذا المثال، تكون قائمتا الشبكة هي **remote_network** و**شبكة VPN Client Local** **LAN**.



3. حدد **Configuration (التكوين) > System (النظام) > بروتوكولات الاتصال النفقي > IPSec LAN إلى شبكة LAN > Add** لتكوين نفق IPsec LAN إلى LAN. انقر فوق **تطبيق** عند الانتهاء.أدخل عنوان IP النظير وقوائم الشبكة التي تم إنشاؤها في الخطوة 2 ومعلمات IPsec و ISAKMP والمفتاح المشترك مسبقا.في هذا المثال، يكون عنوان IP النظير هو **10.1.1.1**، وقوائم الشبكة هي **remote_network** و**شبكة VPN Client Local LAN**، و**Cisco** هو المفتاح المشترك مسبقا.



4. حدد **تكوين > إدارة المستخدم > مجموعات > تعديل 10.1.1.1** لعرض معلومات المجموعة التي تم إنشاؤها تلقائيا.**ملاحظة:** لا تعدل إعدادات المجموعة هذه.



التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

- التحقق من PIX
- التحقق من مركز VPN 3000

التحقق من PIX

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

- show isakmp sa — يعرض جميع اقترانات أمان IKE (SAs) الحالية في نظير. تشير الحالة MM_ACTIVE إلى إستخدام الوضع الرئيسي لإعداد نفق VPN ل IPsec.في هذا المثال، يقوم جدار حماية PIX ببدء اتصال IPsec. عنوان IP للنظير هو 172.30.1.1 ويستخدم الوضع الرئيسي لإنشاء الاتصال.

```
PIX7#show isakmp sa

                                     Active SA: 1
(Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey
                                     Total IKE SA: 1

                                  IKE Peer: 172.30.1.1   1
Type    : L2L                      Role    : initiator
Rekey   : no                       State   : MM_ACTIVE
```

- show ipsEc sa — يعرض الإعدادات المستخدمة من قبل موجهات الخدمات (SAs) الحالية. تحقق من عناوين IP النظيرة والشبكات التي يمكن الوصول إليها عند كل من النهايات المحلية والبعيدة ومجموعة التحويل التي يتم إستخدامها. يوجد إثنان من ESP SAs، واحد في كل إتجاه.

```
PIX7#show ipsec sa
                                     interface: outside
                Crypto map tag: mymap, seq num: 20, local addr: 10.1.1.1

        access-list 101 permit ip 192.168.1.0 255.255.255.0 172.16.0.0 255.255.0.0

          (local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0
            (remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0
                                     current_peer: 172.30.1.1
```

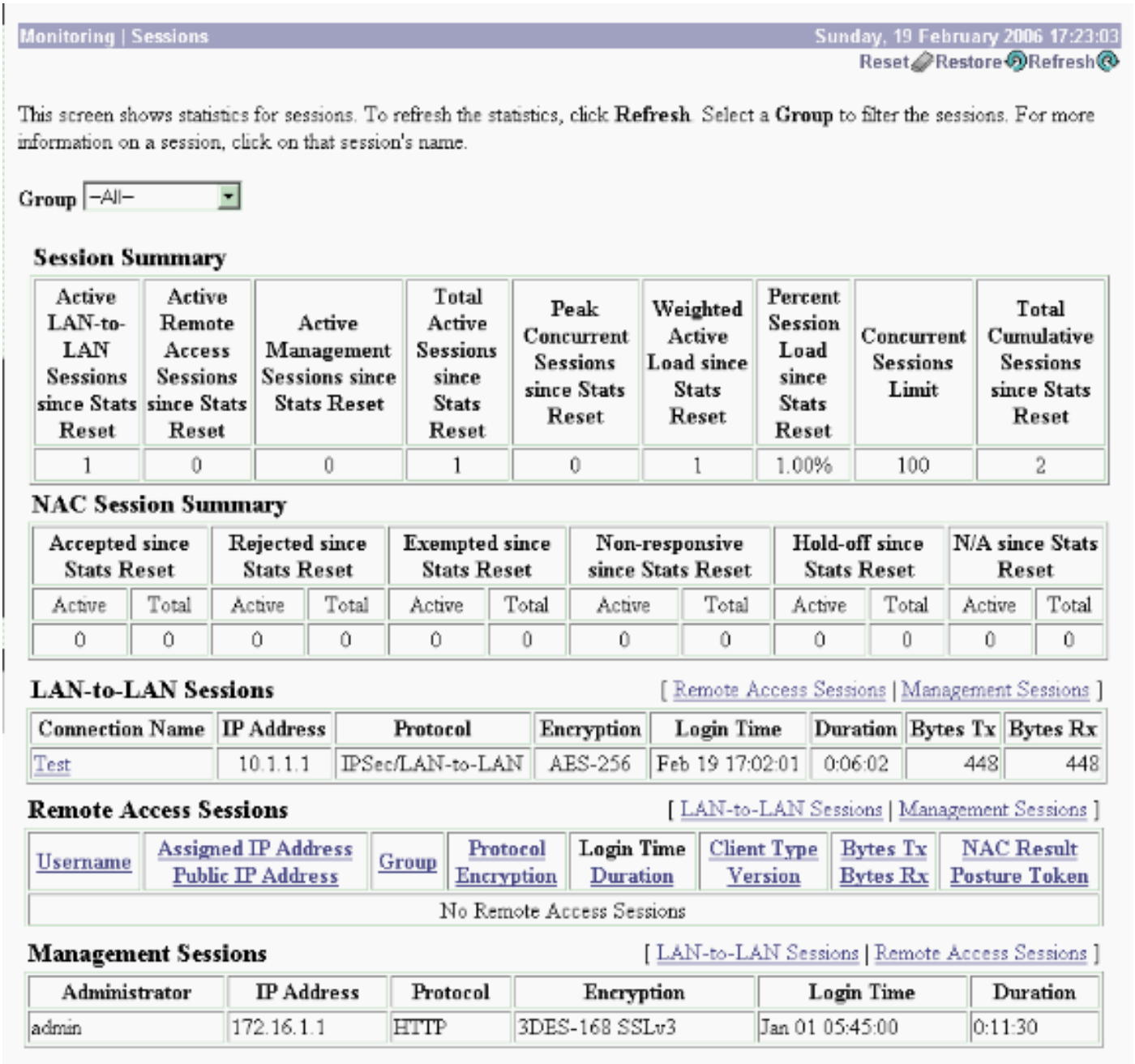
```
                    pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4#
                    pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4#
                            pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0#
                                send errors: 0, #recv errors: 0#

      local crypto endpt.: 10.1.1.1, remote crypto endpt.: 172.30.1.1

                  path mtu 1500, ipsec overhead 76, media mtu 1500
                                current outbound spi: 136580F6

                                                     :inbound esp sas
                                          (spi: 0xF24F4675 (4065281653
                                transform: esp-aes-256 esp-sha-hmac
                                    {,in use settings ={L2L, Tunnel
                            slot: 0, conn_id: 1, crypto-map: mymap
 (sa timing: remaining key lifetime (kB/sec): (3824999/28747
                                                   IV size: 16 bytes
                                        replay detection support: Y
                                                    :outbound esp sas
                                           (spi: 0x136580F6 (325419254
                                transform: esp-aes-256 esp-sha-hmac
                                    {,in use settings ={L2L, Tunnel
                            slot: 0, conn_id: 1, crypto-map: mymap
 (sa timing: remaining key lifetime (kB/sec): (3824999/28745
                                                   IV size: 16 bytes
                                        replay detection support: Y
```

أستخدم أوامر clear ipSec sa وclear isakmp sa لإعادة ضبط النفق.

التحقق من مركز VPN 3000

حدد **مراقبة > إحصائيات > IPsec** للتحقق من ظهور النفق في مركز VPN 3000. يحتوي هذا على إحصائيات لكل من معلمات IKE و IPsec.

أنت يستطيع راقبت بنشاط الجلسة في **monitore > جلسة**. يمكنك إعادة ضبط نفق IPsec هنا.



Monitoring | Sessions — Sunday, 19 February 2006 17:23:03

Reset Restore Refresh

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name.

Group –All–

Session Summary

Active LAN-to-LAN Sessions since Stats Reset	Active Remote Access Sessions since Stats Reset	Active Management Sessions since Stats Reset	Total Active Sessions since Stats Reset	Peak Concurrent Sessions since Stats Reset	Weighted Active Load since Stats Reset	Percent Session Load since Stats Reset	Concurrent Sessions Limit	Total Cumulative Sessions since Stats Reset
1	0	0	1	0	1	1.00%	100	2

NAC Session Summary

Accepted since Stats Reset		Rejected since Stats Reset		Exempted since Stats Reset		Non-responsive since Stats Reset		Hold-off since Stats Reset		N/A since Stats Reset	
Active	Total	Active	Total	Active	Total	Active	Total	Active	Total	Active	Total
0	0	0	0	0	0	0	0	0	0	0	0

LAN-to-LAN Sessions [Remote Access Sessions | Management Sessions]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
Test	10.1.1.1	IPSec/LAN-to-LAN	AES-256	Feb 19 17:02:01	0:06:02	448	448

Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token
No Remote Access Sessions							

Management Sessions [LAN-to-LAN Sessions | Remote Access Sessions]

Administrator	IP Address	Protocol	Encryption	Login Time	Duration
admin	172.16.1.1	HTTP	3DES-168 SSLv3	Jan 01 05:45:00	0:11:30

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

- أستكشاف أخطاء PIX وإصلاحها
- أستكشاف أخطاء مركز VPN 3000 وإصلاحها
- PFS

أستكشاف أخطاء PIX وإصلاحها

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

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

ال **debug** أمر على PIX ل VPN نفق:

- debug crypto isakmp — debugs ISAKMP SA تفاوض.
- debug crypto ipSec — تصحيح أخطاء مفاوضات IPsec SA.

أستكشاف أخطاء مركز VPN 3000 وإصلاحها

مماثل لأوامر تصحيح الأخطاء على موجهات Cisco، يمكنك تكوين فئات الحدث لعرض جميع التنبيهات. حدد **تكوين > نظام > أحداث > فئات > إضافة** لتشغيل تسجيل فئات الحدث.

حدد **مراقبة > سجل أحداث قابل للتصفية** لمراقبة الأحداث التي تم تمكينها.

PFS

في مفاوضات IPsec، تضمن سرية إعادة التوجيه الكاملة (PFS) عدم إرتباط كل مفتاح تشفير جديد بأي مفتاح سابق.

إما أن يمكن أو أعجزت PFS على كلا من نظائر النفق، وإلا فإن نفق LAN إلى LAN (L2L) IPsec لم يتم إنشاؤه في PIX/ASA.

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

```
{hostname(config-group-policy)#pfs {enable | disable
```

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

```
hostname(config-group-policy)#no pfs
```

معلومات ذات صلة

- أجهزة الأمان Cisco PIX 500 Series Security Appliances - صفحة الدعم
- مركز Cisco VPN 3000 Series - صفحة الدعم
- مرجع أوامر جهاز الأمان Cisco PIX 500 Series Security Appliance Command Reference
- 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).