تكوين PIX-to-PIX-to-PIX IPSec (العزوم والمتكامل)

المحتويات

المقدمة

يتيح هذا التكوين لجدار حماية PIX الآمن من Cisco الاتصال بالشبكات خلف مربعي جدار حماية PIX الآخرين من خلال أنفاق VPN عبر الإنترنت أو أي شبكة عامة باستخدام IPsec. لا تحتاج الشبكتين النهائيتين إلى الاتصال ببعضها البعض، ولكن هناك اتصال بالشبكة المركزية. لا يمكن للشبكتين البعيدتين الاتصال ببعضها البعض من خلال المرور عبر PIX المركزي لأن PIX لا يقوم بتوجيه حركة مرور البيانات التي يتم استقبالها على واجهة واحدة إلى خارج الواجهة نفسها. إذا كانت هناك حاجة للشبكات البعيدة للتواصل مع بعضها البعض، فأنت بحاجة إلى تكوين متكامل، بدلا من تكوين الصرة والمحور الموضح في هذا المستند. قد يكون هناك بالفعل **nat 1**، **عالمي**، **ثابت**، و**بيانات قناة** موجودة على PIXs. يوضح هذا المثال إضافة التشفير فقط.

المتطلبات الأساسية

المتطلبات

لكي يعمل IPsec، يجب *عليك* إنشاء اتصال بين نقاط النهاية للنفق قبل بدء هذا التكوين.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات جدار حماية PIX 5.1.x و x.5.2 و 6.3.3.

ملاحظة: يجب أن يوضح الأمر **show version** أن التشفير ممكن.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة

المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

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

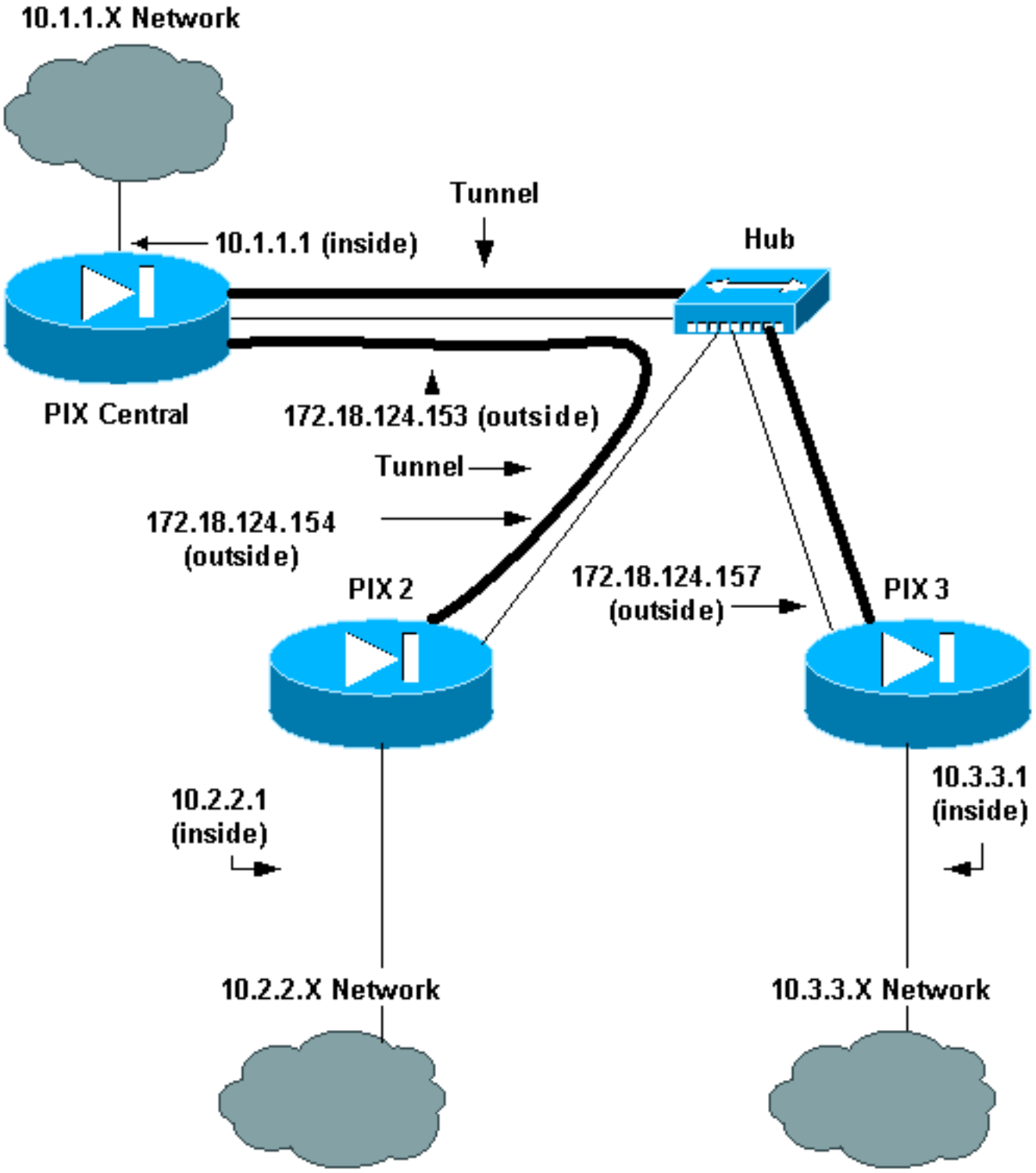
التكوين

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

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

يستخدم هذا المستند التكوينات التالية:

- PIX Central
- PIX 2
- PIX 3

PIX Central
...Building configuration Saved :

```
:
(PIX Version 6.3(3
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix-central
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
This is traffic to PIX 2. access-list 120 permit ip ---!
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
This is traffic to PIX 3. access-list 130 permit ip ---!
10.1.1.0 255.255.255.0 10.3.3.0 255.255.255.0
Do not do Network Address Translation (NAT) on ---!
traffic to other PIXes. access-list 100 permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
access-list 100 permit ip 10.1.1.0 255.255.255.0
10.3.3.0 255.255.255.0
pager lines 24
logging on
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.153 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
Do not do NAT on traffic to other PIXes. nat ---!
(inside) 0 access-list 100
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 h225 1:00:00
timeout h323 0:05:00 mgcp 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
snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-des esp-md5-hmac
This is traffic to PIX 2. crypto map newmap 20 ---!
ipsec-isakmp
crypto map newmap 20 match address 120
```

```
crypto map newmap 20 set peer 172.18.124.154
crypto map newmap 20 set transform-set myset
This is traffic to PIX 3. crypto map newmap 30 ---!
ipsec-isakmp
crypto map newmap 30 match address 130
crypto map newmap 30 set peer 172.18.124.157
crypto map newmap 30 set transform-set myset
crypto map newmap interface outside
isakmp enable outside
isakmp key ******** address 172.18.124.154 netmask
255.255.255.255
no-xauth no-config-mode
isakmp key ******** address 172.18.124.157 netmask
255.255.255.255
no-xauth no-config-mode
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
end :
```

PIX 2

```
...Building configuration
Saved :
:
(PIX Version 6.3(3
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix2
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
This is traffic to PIX Central. access-list 110 ---!
permit ip 10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0
Do not do NAT on traffic to PIX Central. access- ---!
list 100 permit ip 10.2.2.0 255.255.255.0 10.1.1.0
255.255.255.0
pager lines 24
logging on
mtu outside 1500
```

```
                                        mtu inside 1500
          ip address outside 172.18.124.154 255.255.255.0
                 ip address inside 10.2.2.1 255.255.255.0
                                ip audit info action alarm
                             ip audit attack action alarm
                                                no failover
                                  failover timeout 0:00:00
                                           failover poll 15
                              no failover ip address outside
                               no failover ip address inside
                                        pdm history enable
                                         arp timeout 14400
        Do not do NAT on traffic to PIX Central. nat ---!
                                      (inside) 0 access-list 100
             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 h225 1:00:00
 timeout h323 0:05:00 mgcp 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
                                sysopt connection permit-ipsec
    crypto ipsec transform-set myset esp-des esp-md5-hmac
  This is traffic to PIX Central. crypto map newmap ---!
                                                10 ipsec-isakmp
                      crypto map newmap 10 match address 110
                  crypto map newmap 10 set peer 172.18.124.153
                  crypto map newmap 10 set transform-set myset
                           crypto map newmap interface outside
                                    isakmp enable outside
      isakmp key ******** address 172.18.124.153 netmask
                                                255.255.255.255
                                    no-xauth no-config-mode
                                       isakmp identity address
                isakmp policy 10 authentication pre-share
                           isakmp policy 10 encryption des
                                 isakmp policy 10 hash md5
                                  isakmp policy 10 group 1
                               isakmp policy 10 lifetime 1000
                                        telnet timeout 5
                                           ssh timeout 5
                                      console timeout 0
                                      terminal width 80
          Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
                                                    end :
```

PIX 3

```
                                  ...Building configuration
                                                  Saved :
                                                        :
                                        (PIX Version 6.3(3
                                   interface ethernet0 auto
                                   interface ethernet1 auto
                          nameif ethernet0 outside security0
```

```
                    nameif ethernet1 inside security100
               enable password 8Ry2YjIyt7RRXU24 encrypted
                  passwd 2KFQnbNIdI.2KYOU encrypted
                                        hostname pix3
              fixup protocol dns maximum-length 512
                                fixup protocol ftp 21
                    fixup protocol h323 h225 1720
                 fixup protocol h323 ras 1718-1719
                            fixup protocol http 80
                            fixup protocol rsh 514
                          fixup protocol rtsp 554
                          fixup protocol sip 5060
                     fixup protocol sip udp 5060
                     fixup protocol skinny 2000
                          fixup protocol smtp 25
                    fixup protocol sqlnet 1521
                          fixup protocol tftp 69
                                              names
    This is traffic to PIX Central. access-list 110 ---!
permit ip 10.3.3.0 255.255.255.0 10.1.1.0 255.255.255.0
  Do not do NAT on traffic to PIX Central. access- ---!
      list 100 permit ip 10.3.3.0 255.255.255.0 10.1.1.0
                                      255.255.255.0
                                       pager lines 24
                                           logging on
                                    mtu outside 1500
                                     mtu inside 1500
         ip address outside 172.18.124.157 255.255.255.0
               ip address inside 10.3.3.1 255.255.255.0
                                ip audit info action alarm
                            ip audit attack action alarm
                                              no failover
                          failover timeout 0:00:00
                                   failover poll 15
                       no failover ip address outside
                        no failover ip address inside
                                  pdm history enable
                                   arp timeout 14400
      Do not do NAT on traffic to PIX Central. nat ---!
                                (inside) 0 access-list 100
            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 h225 1:00:00
 timeout h323 0:05:00 mgcp 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
                      sysopt connection permit-ipsec
  crypto ipsec transform-set myset esp-des esp-md5-hmac
  This is traffic to PIX Central. crypto map newmap ---!
                                    10 ipsec-isakmp
                 crypto map newmap 10 match address 110
               crypto map newmap 10 set peer 172.18.124.153
               crypto map newmap 10 set transform-set myset
                      crypto map newmap interface outside
                                isakmp enable outside
```

```
isakmp key ******** address 172.18.124.153 netmask
255.255.255.255
no-xauth no-config-mode
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:aa3bbd8c6275d214b153e1e0bc0173e4
end :
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

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

- **show crypto ipSec**—يعرض الحالة الحالية لاقترانات أمان IPsec (SAs) ويكون مفيدا في تحديد ما إذا تم تشفير حركة مرور البيانات.

```
pix-central#show crypto ipsec sa

interface: outside
Crypto map tag: newmap, local addr. 172.18.124.153

(local  ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0
(remote ident (addr/mask/prot/port): (10.3.3.0/255.255.255.0/0/0
current_peer: 172.18.124.157:500
{,PERMIT, flags={origin_is_acl
This verifies that encrypted packets are sent !--- and received without any errors. ---!
#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 0, #recv errors 0#

,local crypto endpt.: 172.18.124.153
remote crypto endpt.: 172.18.124.157
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 3bcb6913
:Shows inbound SAs that are established. inbound esp sas ---!
(spi: 0x3efbe540(1056695616
, transform: esp-des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 3, crypto map: newmap
(sa timing: remaining key lifetime (k/sec): (4607999/27330
IV size: 8 bytes
replay detection support: Y

:inbound ah sas
:inbound pcp sas
:Shows outbound SAs that are established. outbound esp sas ---!
(spi: 0x3bcb6913(1003186451
, transform: esp-des esp-md5-hmac
{ ,in use settings ={Tunnel
```

```
                                slot: 0, conn id: 4, crypto map: newmap
                (sa timing: remaining key lifetime (k/sec): (4607999/27321
                                                        IV size: 8 bytes
                                                replay detection support: Y

                                                                :outbound ah sas

                                                               :outbound pcp sas

                        (local  ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0
                        (remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0
                                                    current_peer: 172.18.124.154:500
                                                    {,PERMIT, flags={origin_is_acl
    This verifies that encrypted packets are sent !--- and received without any errors. ---!
                                  #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 0, #recv errors 0#

                                                ,local crypto endpt.: 172.18.124.153
                                                remote crypto endpt.: 172.18.124.154
                                    path mtu 1500, ipsec overhead 56, media mtu 1500
                                                    current outbound spi: da8d556
    Shows inbound SAs that are established. inbound esp sas: spi: 0x53835c96(1401117846) ---!
                                                  , transform: esp-des esp-md5-hmac
                                                 { ,in use settings ={Tunnel
                                        slot: 0, conn id: 1, crypto map: newmap
                        (sa timing: remaining key lifetime (k/sec): (4607999/27319
                                                        IV size: 8 bytes
                                                replay detection support: Y

                                                                 :inbound ah sas

                                                                :inbound pcp sas
    Shows outbound SAs that are established. outbound esp sas: spi: 0xda8d556c(3666695532) ---!
                                                  , transform: esp-des esp-md5-hmac
                                                { ,in use settings ={Tunnel
                                        slot: 0, conn id: 2, crypto map: newmap
                        (sa timing: remaining key lifetime (k/sec): (4607999/27319
                                                        IV size: 8 bytes
                                                replay detection support: Y

                                                                :outbound ah sas

                                                               :outbound pcp sas
```

- **show crypto isakmp sa**— يعرض الحالة الحالية لاتصالات IKE (تبادل مفتاح الإنترنت).

```
                                                pix-central#show crypto isakmp sa
                                                                Total     : 2
                                                                Embryonic : 0
      dst               src       state     pending   created

      QM_IDLE         0         0   172.18.124.154   172.18.124.153
      QM_IDLE         0         0   172.18.124.157   172.18.124.153
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

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

على PIX (مع تشغيل أوامر **تصحيح أخطاء مراقبة التسجيل** أو **تصحيح أخطاء وحدة التحكم في** التسجيل):

- **debug crypto ipSec**—معالجة IPsec للتصحيح.
- **debug crypto isakmp**—debugs إنترنت security association and key management protocol processing (ISAKMP).
- **debug crypto engine**—يعرض رسائل تصحيح الأخطاء حول محركات التشفير، التي تقوم بالتشفير وفك التشفير.

مسح الاقترانات الأمنية

استعملت هذا أمر في ال config أسلوب من ال PIX:

- **مسح [crypto] ipSec sa**—يحذف شبكات IPsec النشطة. الكلمة الأساسية **تشفير** إختيارية.
- **مسح [crypto] isakmp sa**— يحذف شبكات IKE النشطة. الكلمة الأساسية **تشفير** إختيارية.

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)
- مفاوضة IPSec/بروتوكولات IKE
- 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).