كيفية تكوين عميل Cisco VPN إلى PIX باستخدام AES

المحتويات

المقدمة

يوضح هذا التكوين العينة كيفية إعداد اتصال VPN للوصول عن بعد من عميل Cisco VPN إلى جدار حماية PIX، باستخدام معيار التشفير المتقدم (AES) للتشفير. يستخدم هذا المثال شبكة VPN "سهلة من Cisco" لإعداد قناة الاتصال الآمنة وتم تكوين جدار حماية PIX كخادم VPN سهل.

في الإصدار 6.3 من برنامج جدار حماية PIX الآمن من Cisco والإصدارات الأحدث، يتم دعم معيار التشفير الدولي الجديد AES لتأمين إتصالات VPN للوصول من موقع إلى موقع والوصول عن بعد. هذا بالإضافة إلى معيار تشفير البيانات (DES) وخوارزميات تشفير 3DES. يدعم جدار حماية PIX أحجام مفاتيح AES التي تبلغ 128 و 192 و 256 بت.

يدعم عميل شبكة VPN AES كخوارزمية تشفير تبدأ مع الإصدار 3.6.1 من عميل Cisco VPN. يدعم عميل الشبكة الخاصة الظاهرية (VPN) أحجام المفاتيح التي تبلغ 128 بت و 256 بت فقط.

المتطلبات الأساسية

المتطلبات

يفترض هذا التكوين العينة أن PIX قيد التشغيل الكامل ويتم تكوينه باستخدام الأوامر الضرورية لمعالجة حركة مرور البيانات وفقا لسياسة الأمان الخاصة بالمؤسسة.

المكونات المستخدمة

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

- برنامج PIX الإصدار 6.3(1)**ملاحظة:** تم إختبار هذا الإعداد على برنامج PIX الإصدار 6.3(1) ومن المتوقع أن يعمل على جميع الإصدارات اللاحقة.
- عميل شبكة VPN الإصدار 4.0.3(a) من Cisco**ملاحظة:** تم إختبار هذا الإعداد على الإصدار 4.0.3(A) من عميل VPN، ولكنه يعمل على الإصدارات السابقة التي تعود إلى 3.6.1 وحتى الإصدار الحالي.

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.

معلومات أساسية

تلبي شبكات VPN الخاصة بالوصول عن بعد متطلبات الموظفين كثيري التنقل للاتصال بأمان بشبكة المؤسسة. يستطيع مستخدمو الأجهزة المحمولة إعداد اتصال آمن باستخدام برنامج عميل شبكة VPN المثبت على أجهزة الكمبيوتر الخاصة بهم. يقوم عميل شبكة VPN ببدء اتصال بجهاز موقع مركزي تم تكوينه لقبول هذه الطلبات. في هذا المثال، جهاز الموقع المركزي هو جدار حماية PIX تم تكوينه كخادم VPN سهل يستخدم خرائط التشفير الديناميكية.

تعمل الشبكة الخاصة الظاهرية (VPN) السهلة من Cisco على تبسيط نشر الشبكة الخاصة الظاهرية (VPN) من خلال تسهيل تكوين الشبكات الخاصة الظاهرية (VPN) وإدارتها. وهو يتكون من خادم Cisco Easy VPN وخادم Cisco Easy VPN Remote. يلزم توفر تكوين أقل على جهاز VPN Remote سهل. يقوم جهاز VPN البعيد السهل ببدء اتصال. إذا نجحت المصادقة، يدفع خادم VPN السهل تكوين VPN لأسفل إليه. يتوفر المزيد من المعلومات حول كيفية تكوين جدار حماية PIX كخادم VPN سهل في إدارة الوصول عن بعد إلى VPN.

يتم إستخدام خرائط التشفير الديناميكية لتكوين IPsec عندما لا يمكن تحديد بعض المعلمات المطلوبة لإعداد شبكة VPN مسبقا، كما هو الحال مع مستخدمي الأجهزة المحمولة الذين يحصلون على عناوين IP المعينة ديناميكيا. تعمل خريطة التشفير الديناميكية كقالب ويتم تحديد المعلمات المفقودة أثناء تفاوض IPsec. يتوفر المزيد من المعلومات حول خرائط التشفير الديناميكية في خرائط التشفير الديناميكية.

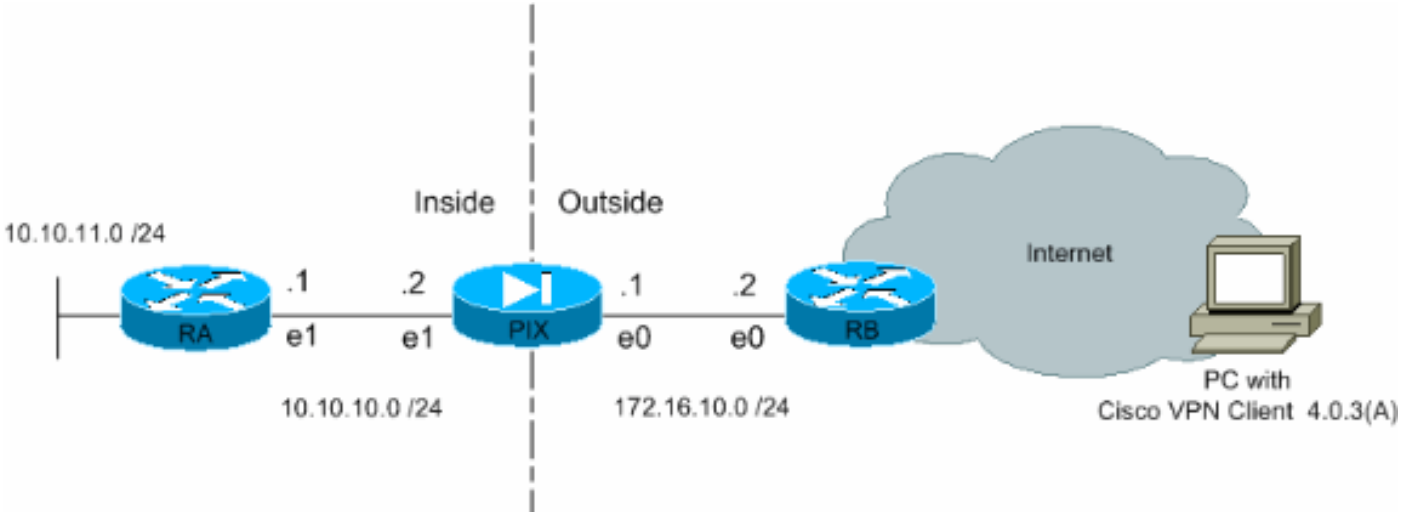
التكوينات

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:



تكوين PIX

يتم عرض التكوين اللازم على جدار حماية PIX في هذا الإخراج. التشكيل ل VPN فقط.

PIX

```
(PIX Version 6.3(1
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Pixfirewall
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
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
names

Define the access list to enable split tunneling. ---!
access-list 101 permit ip 10.10.10.0 255.255.255.0
10.10.8.0 255.255.255.0 access-list 101 permit ip
10.10.11.0 255.255.255.0 10.10.8.0 255.255.255.0 !---
Define the access list to avoid network address !---
translation (NAT) on IPsec packets. access-list 102
permit ip 10.10.10.0 255.255.255.0 10.10.8.0
255.255.255.0 access-list 102 permit ip 10.10.11.0
255.255.255.0 10.10.8.0 255.255.255.0 pager lines 24 mtu
outside 1500 mtu inside 1500 mtu intf2 1500 !---
Configure the IP address on the interfaces. ip address
outside 172.16.10.1 255.255.255.0 ip address inside
10.10.10.2 255.255.255.0 no ip address intf2 ip audit
info action alarm ip audit attack action alarm !---
```

```
Create a pool of addresses from which IP addresses are assigned !--- dynamically to the remote VPN Clients. ip local pool vpnpool1 10.10.8.1-10.10.8.254 pdm history enable arp timeout 14400 !--- Disable NAT for IPsec packets. nat (inside) 0 access-list 102 route outside 0.0.0.0 0.0.0.0 172.16.10.2 1 route inside 10.10.11.0 255.255.255.0 10.10.10.1 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 !--- Permit packet that came from an IPsec tunnel to pass through without !--- checking them against the configured conduits/access lists. sysopt connection permit-ipsec !--- Define the transform set to be used during IPsec !--- security association (SA) negotiation. Specify AES as the encryption algorithm. crypto ipsec transform-set trmset1 esp-aes-256 esp-sha-hmac !--- Create a dynamic crypto map entry !--- and add it to a static crypto map. crypto dynamic-map map2 10 set transform-set trmset1 crypto map map1 10 ipsec-isakmp dynamic map2 !--- Bind the crypto map to the outside interface. crypto map map1 interface outside !--- Enable Internet Security Association and Key Management !--- Protocol (ISAKMP) negotiation on the interface on which the IPsec !--- peer communicates with the PIX Firewall. isakmp enable outside isakmp identity address !--- Define an ISAKMP policy to be used while !--- negotiating the ISAKMP SA. Specify !--- AES as the encryption algorithm. The configurable AES !--- options are aes, aes-192 and aes-256. !--- Note: AES 192 is not .supported by the VPN Client

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
Create a VPN group and configure the policy ---! attributes which are !--- downloaded to the Easy VPN Clients. vpngroup groupmarketing address-pool vpnpool1 vpngroup groupmarketing dns-server 10.10.11.5 vpngroup groupmarketing wins-server 10.10.11.5 vpngroup groupmarketing default-domain org1.com vpngroup groupmarketing split-tunnel 101 vpngroup groupmarketing idle-time 1800 vpngroup groupmarketing password ******** telnet timeout 5 ssh timeout 5 console timeout 0
terminal width 80
Cryptochecksum:c064abce81996b132025e83e421ee1c3 : end
```

ملاحظة: في هذا الإعداد، يوصى بعدم تحديد AES-192 أثناء تكوين مجموعة التحويل أو نهج ISAKMP. لا يدعم عملاء شبكة VPN AES-192 للتشفير.

ملاحظة: باستخدام الإصدارات السابقة، كانت مطلوبة أوامر تكوين وضع IKE **وعنوان تكوين عميل isakmp** وعنوان **تكوين عميل خريطة التشفير**. ومع ذلك، باستخدام الإصدارات الأحدث (x.3 والإصدارات الأحدث)، لم تعد هذه الأوامر ضرورية. يمكن تحديد تجمعات عناوين متعددة الآن باستخدام الأمر **vpnGroup address-pool**.

ملاحظة: أسماء مجموعات VPN حساسة لحالة الأحرف. وهذا يعني أن مصادقة المستخدم تفشل إذا كان اسم المجموعة المحدد في PIX واسم المجموعة على عميل VPN مختلفين من حيث حالة الحرف (أحرف كبيرة أو

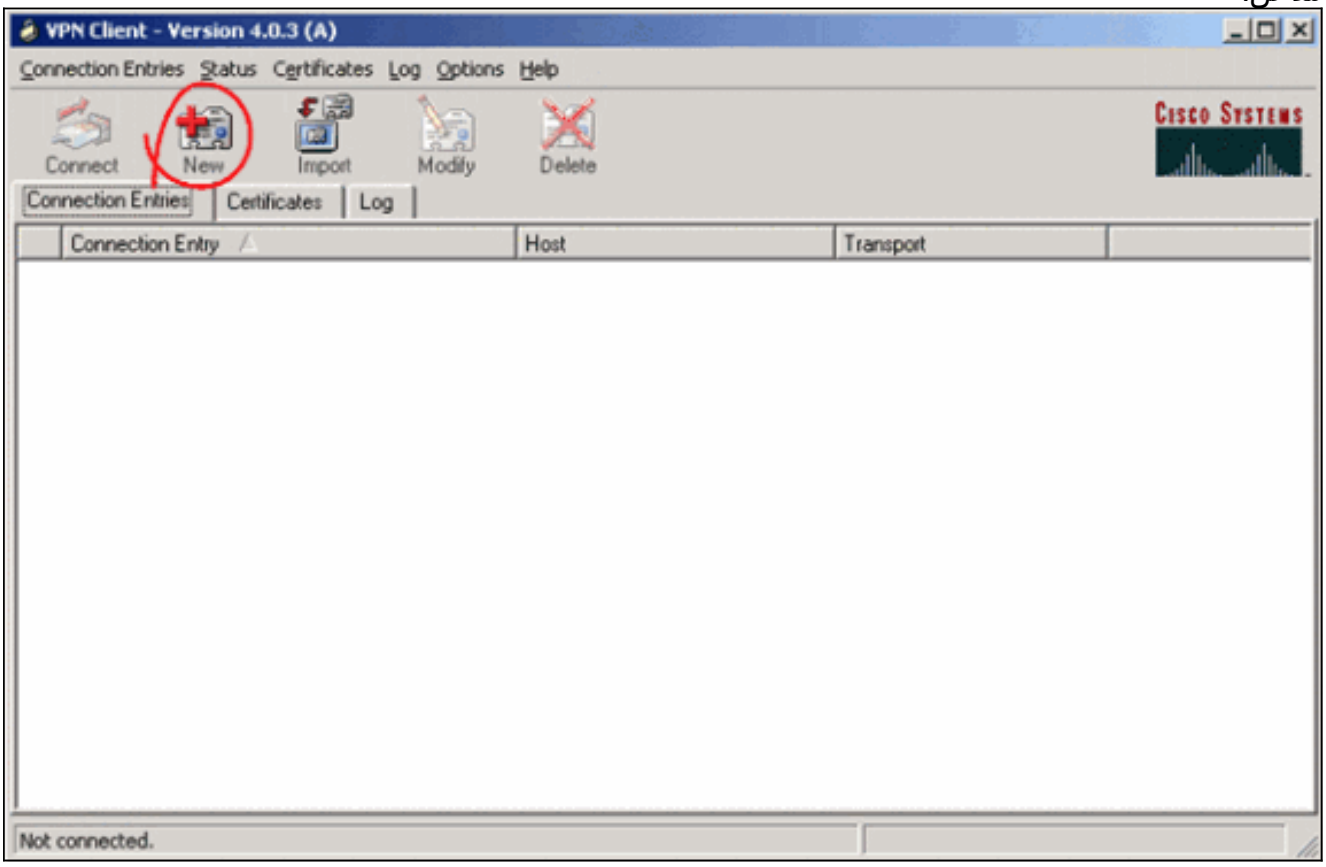
صغيرة).

ملاحظة: على سبيل المثال، عند إدخال اسم المجموعة ك **GroupMarketing** في جهاز واحد و**GroupMarketing** في جهاز آخر، لا يعمل الجهاز.

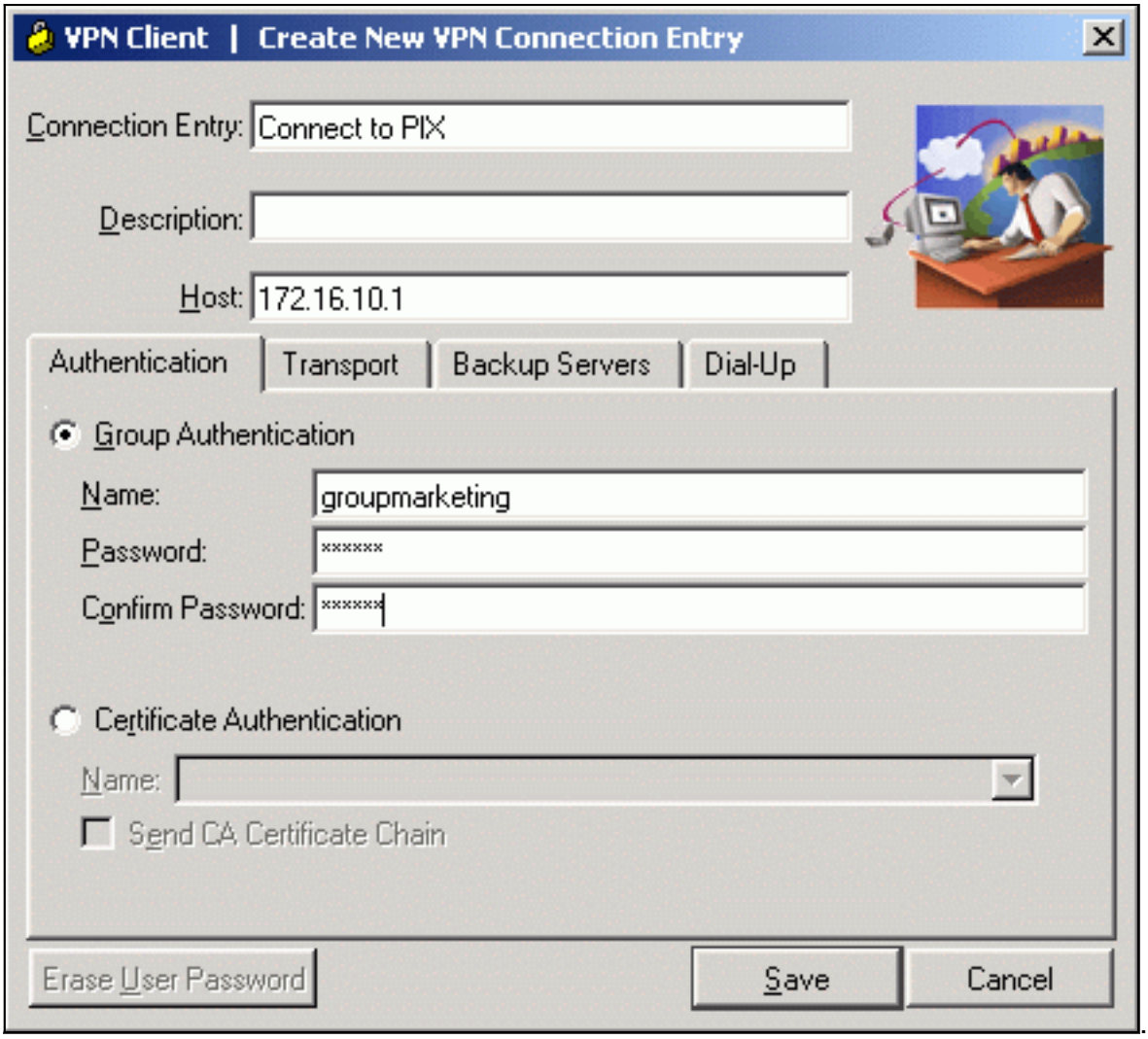
تكوين عميل VPN

بعد تثبيت عميل VPN على الكمبيوتر الشخصي، قم بإنشاء اتصال جديد كما هو موضح في هذه الخطوات:

1. أطلقت ال VPN زبون تطبيق وطقطقة **جديد** أن يخلق توصيل جديد مدخل.

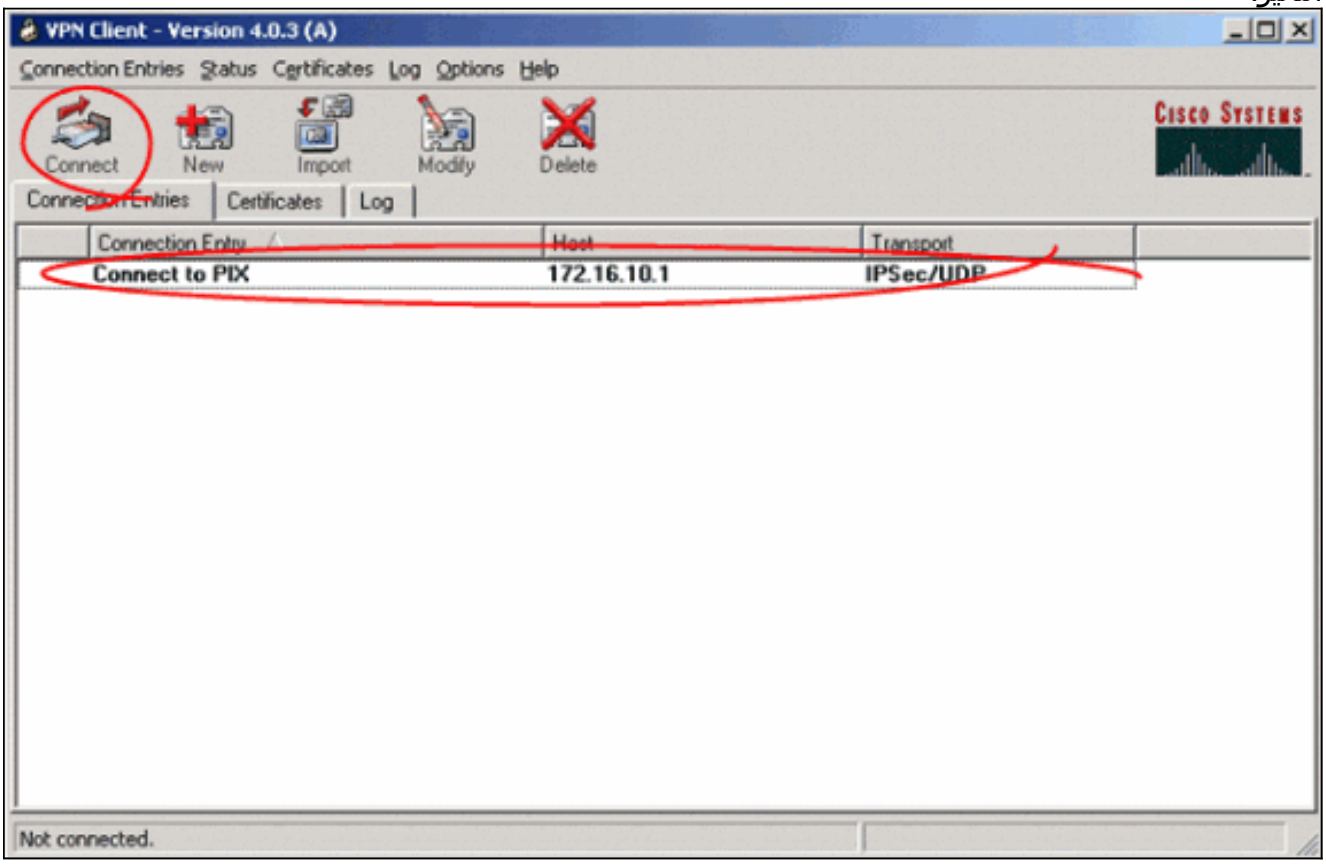


2. مربع حوار جديد بعنوان عميل VPN | ظهور إدخال اتصال VPN جديد. أدخل معلومات التكوين للاتصال الجديد.في حقل "إدخال الاتصال"، قم بتعيين اسم للإدخال الجديد الذي تم إنشاؤه.في حقل المضيف، اكتب عنوان IP الخاص بالواجهة العامة ل PIX.حدد علامة تبويب المصادقة، ثم اكتب اسم المجموعة وكلمة المرور (مرتين - للتأكيد). يحتاج هذا أن يطابق المعلومة دخلت على ال PIX يستعمل ال **vpnGroup كلمة** أمر.انقر فوق **حفظ** لحفظ المعلومات التي تم إدخالها. تم إنشاء الاتصال الجديد



الآن.

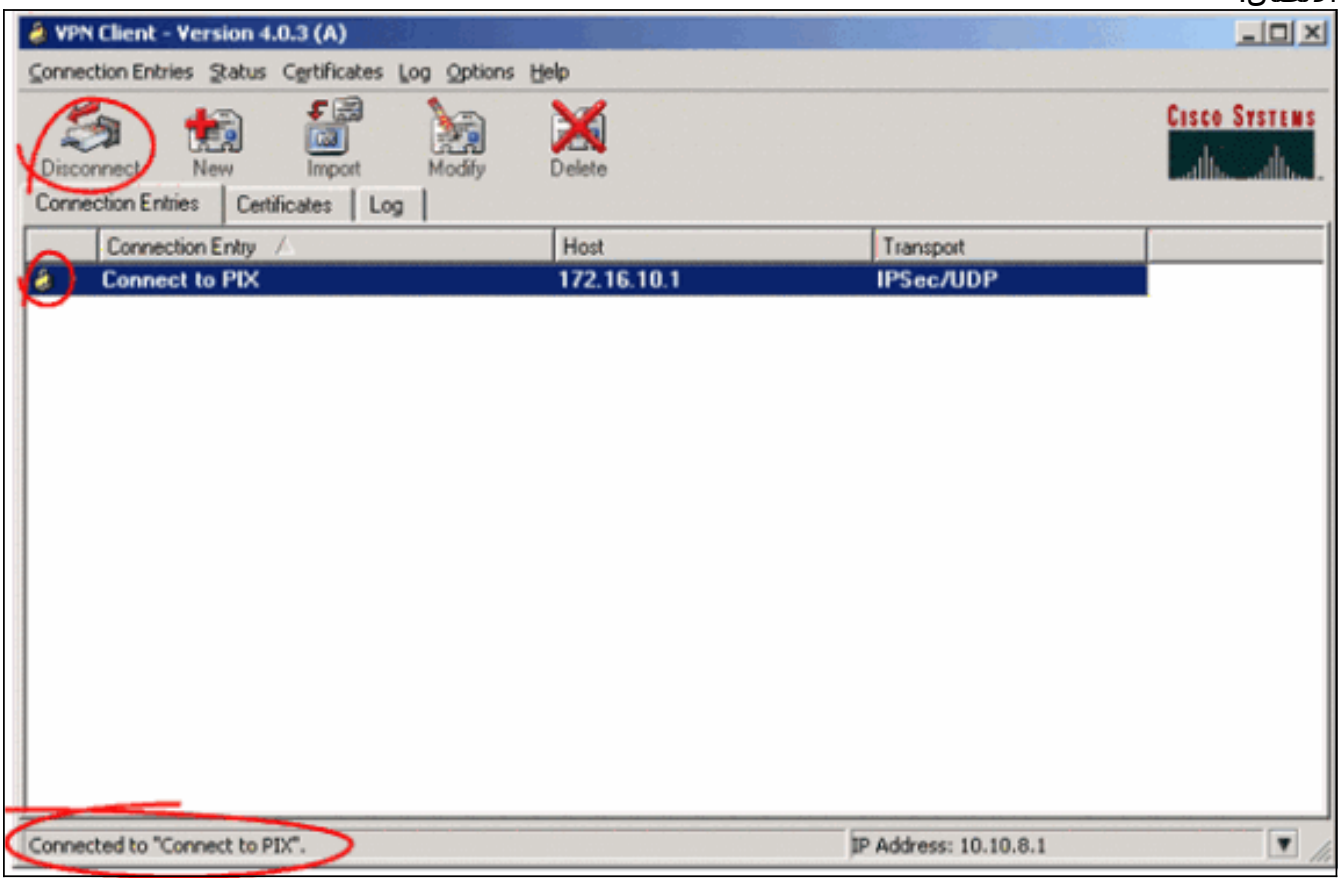
3. للاتصال بالبوابة باستخدام إدخال الاتصال الجديد، حدد إدخال الاتصال بالنقر عليه مرة واحدة ثم انقر على رمز **الاتصال**. يكون للنقرة المزدوجة على إدخال التوصيل نفس التأثير.



التحقق من الصحة

في عميل الشبكة الخاصة الظاهرية (VPN)، تشير هذه العناصر إلى اتصال تم إنشاؤه بنجاح للعبارة البعيدة:

- تظهر أيقونة إغلاق صفراء مقابل إدخال التوصيل النشط.
- يتغير رمز الاتصال الموجود على شريط الأدوات (بجوار علامة تبويب إدخالات الاتصال) إلى قطع الاتصال.
- يظهر سطر الحالة في نهاية الإطار الحالة ك "متصل ب" متبوعا باسم إدخال الاتصال.



ملاحظة: بشكل افتراضي، بمجرد تأسيس الاتصال، يتضاءل عميل VPN إلى رمز قفل مغلق في درج النظام، في الركن السفلي الأيمن من شريط مهام Windows. انقر نقرا مزدوجا على أيقونة القفل المغلق لجعل نافذة عميل VPN مرئية مرة أخرى.

على جدار حماية PIX، يمكن إستخدام أوامر **العرض** هذه للتحقق من حالة الاتصالات التي تم إنشاؤها.

ملاحظة: يتم دعم بعض أوامر **العرض** بواسطة أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

- **show crypto ipSec sa**— يعرض جميع رسائل IPsec الحالية على PIX. بالإضافة إلى ذلك، يعرض الإخراج عنوان IP الفعلي للنظير البعيد وعنوان IP المعين وعنوان IP المحلي والواجهة وخريطة التشفير المطبقة.

```
Pixfirewall#show crypto ipsec sa

                                interface: outside
                Crypto map tag: map1, local addr. 172.16.10.1

               (local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
            (remote ident (addr/mask/prot/port): (10.10.8.1/255.255.255.255/0/0
                                current_peer: 172.16.12.3:500
                            dynamic allocated peer ip: 10.10.8.1

                                              {}=PERMIT, flags
              pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0#
```

```
                                pkts decaps: 25, #pkts decrypt: 25, #pkts verify 25#
                                        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.: 172.16.10.1, remote crypto endpt.: 172.16.12.3
                                  path mtu 1500, ipsec overhead 64, media mtu 1500
                                             current outbound spi: cbabd0ce

                                                                  :inbound esp sas
                                                    (spi: 0x4d8a971d(1300928285
                                          , transform: esp-aes-256 esp-sha-hmac
                                                    { ,in use settings ={Tunnel
                                         slot: 0, conn id: 2, crypto map: map1
                        (sa timing: remaining key lifetime (k/sec): (4607996/28685
                                                               IV size: 16 bytes
                                                    replay detection support: Y


                                                                   :inbound ah sas


                                                                  :inbound pcp sas


                                                                 :outbound esp sas
                                                    (spi: 0xcbabd0ce(3417034958
                                          , transform: esp-aes-256 esp-sha-hmac
                                                    { ,in use settings ={Tunnel
                                         slot: 0, conn id: 1, crypto map: map1
                        (sa timing: remaining key lifetime (k/sec): (4608000/28676
                                                               IV size: 16 bytes
                                                    replay detection support: Y


                                                                   :outbound ah sas


                                                                  :outbound pcp sas
```

- **show crypto isakmp sa**— يعرض حالة ISAKMP SA التي تم إنشاؤها بين الأقران.

```
Pixfirewall#show crypto isakmp sa
                                                                  Total     : 1
                                                                  Embryonic : 0
      dst               src         state     pending     created
      QM_IDLE         0           1    172.16.12.3      172.16.10.1
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

يمكن أن تساعد أوامر تصحيح الأخطاء هذه في أستكشاف أخطاء إعداد VPN وإصلاحها.

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

- **debug crypto isakmp**— يعرض ISAKMP SA الذي تم إنشاؤه وسمات IPsec التي تم التفاوض عليها. وخلال مفاوضات ISAKMP SA، يمكن ل PIX أن يلغي عدة مقترحات باعتبارها "غير مقبولة" قبل أن يقبل واحدة منها. بمجرد الموافقة على ISAKMP SA، يتم التفاوض على سمات IPsec. ومرة أخرى، من الممكن رفض عدة اقتراحات قبل قبولها، كما هو موضح في ناتج **تصحيح الأخطاء** هذا.

```
crypto_isakmp_process_block:src:172.16.12.3, dest:172.16.10.1 spt:500 dpt:500
```

```
                                                                OAK_AG exchange
                                                ISAKMP (0): processing SA payload. message ID = 0

                                    ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
                                                                ISAKMP:      encryption AES-CBC
                                                                ISAKMP:      hash SHA
                                                                ISAKMP:      default group 2
                                                (ISAKMP:      extended auth pre-share (init
                                                                ISAKMP:      life type in seconds
                                                ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
                                                                ISAKMP:      keylength of 256
  Proposal is rejected since extended auth is not configured. ISAKMP (0): atts are not ---!
                                                                acceptable. Next payload is 3
                                    ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
                                                                ISAKMP:      encryption AES-CBC
                                                                ISAKMP:      hash MD5
                                                                ISAKMP:      default group 2
                                                (ISAKMP:      extended auth pre-share (init
                                                                ISAKMP:      life type in seconds
                                                ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
                                                                ISAKMP:      keylength of 256
Proposal is rejected since MD5 is not specified as the hash algorithm. ISAKMP (0): atts ---!
                                                                are not acceptable. Next payload is 3
                                    ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
                                                                ISAKMP:      encryption AES-CBC
                                                                ISAKMP:      hash SHA
                                                                ISAKMP:      default group 2
                                                                ISAKMP:      auth pre-share
                                                                ISAKMP:      life type in seconds
                                                ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
                                                                ISAKMP:      keylength of 256
    This proposal is accepted since it matches ISAKMP policy 10. ISAKMP (0): atts are ---!
                                                                acceptable. Next payload is 3
                                                ISAKMP (0): processing KE payload. message ID = 0
                                                        Output is suppressed. OAK_QM exchange ---!
                                                                :oakley_process_quick_mode
                                                                OAK_QM_IDLE
                                                ISAKMP (0): processing SA payload. message ID = 3348522173

                                                                ISAKMP : Checking IPSec proposal 1

                                                                ISAKMP: transform 1, ESP_AES
                                                                :ISAKMP:   attributes in transform
                                                                ISAKMP:      authenticator is HMAC-MD5
                                                                ISAKMP:      key length is 256
                                                                ISAKMP:      encaps is 1
                                                                ISAKMP:      SA life type in seconds
                                                ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
This proposal is not accepted since transform-set !--- trmset1 does not use MD5. ISAKMP ---!
                                                                (0): atts not acceptable. Next payload is 0
                                                (ISAKMP (0): skipping next ANDed proposal (1
                                                                ISAKMP : Checking IPSec proposal 2

                                                                ISAKMP: transform 1, ESP_AES
                                                                :ISAKMP:   attributes in transform
                                                                ISAKMP:      authenticator is HMAC-SHA
                                                                ISAKMP:      key length is 256
                                                                ISAKMP:      encaps is 1
                                                                ISAKMP:      SA life type in seconds
                                                ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
This proposal is accepted since it matches !--- transform-set trmset1. ISAKMP (0): atts ---!
                                                                .are acceptable
                                                !ISAKMP (0): bad SPI size of 2 octets
                                                                ISAKMP : Checking IPSec proposal 3
```

```
.Output is suppressed ---!
```

- **debug crypto ipSec**—يعرض معلومات حول مفاوضات IPsec SA.

```
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with     172.16.12.3
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
                                                                      supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
                                                                      supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 2) not
                                                                      supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
                                                                      supported
                          ,IPSEC(validate_proposal_request): proposal part #1
                        ,key eng. msg.) dest= 172.16.10.1, src= 172.16.12.3)
                                ,(dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
                        ,(src_proxy= 10.10.8.1/255.255.255.255/0/0 (type=1
                      , protocol= ESP, transform= esp-aes-256 esp-sha-hmac
                                                ,lifedur= 0s and 0kb
                         spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x4
                                    ...IPSEC(key_engine): got a queue event
                  IPSEC(spi_response): getting spi 0xfb0cb69(263244649) for SA
                    from     172.16.12.3 to     172.16.10.1 for prot 3
                                    ...IPSEC(key_engine): got a queue event
                                                , :(IPSEC(initialize_sas
                        ,key eng. msg.) dest= 172.16.10.1, src= 172.16.12.3)
                                ,(dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
                               ,(src_proxy= 10.10.8.1/0.0.0.0/0/0 (type=1
                      , protocol= ESP, transform= esp-aes-256 esp-sha-hmac
                                               ,lifedur= 2147483s and 0kb
          spi= 0xfb0cb69(263244649), conn_id= 2, keysize= 256, flags= 0x4
                                                , :(IPSEC(initialize_sas
                        ,key eng. msg.) src= 172.16.10.1, dest= 172.16.12.3)
                                 ,(src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
                              ,(dest_proxy= 10.10.8.1/0.0.0.0/0/0 (type=1
                      , protocol= ESP, transform= esp-aes-256 esp-sha-hmac
                                               ,lifedur= 2147483s and 0kb
        spi= 0xda6c054a(3664512330), conn_id= 1, keysize= 256, flags= 0x4
```

باستخدام التكوينات الموضحة في هذا المستند، يمكن لعميل شبكة VPN الاتصال بنجاح ب PIX الموقع الرئيسي باستخدام AES. يلاحظ في بعض الأحيان أنه على الرغم من إنشاء نفق الشبكة الخاصة الظاهرية (VPN) بنجاح، إلا أن المستخدمين غير قادرين على تنفيذ المهام الشائعة مثل موارد شبكة الاتصال، أو تسجيل الدخول إلى المجال، أو إستعراض جوار الشبكة. يتوفر المزيد من المعلومات حول أستكشاف أخطاء هذه المشاكل وإصلاحها في حي شبكة Microsoft بعد إنشاء نفق VPN مع عميل شبكة VPN من Cisco.

معلومات ذات صلة

- معيار التشفير المتقدم (AES)
- مقدمة عن تشفير أمان IP (IPSec)
- أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر التصحيح واستخدامها
- صفحة دعم مفاوضة IPsec/بروتوكولات IKE
- صفحة دعم PIX
- صفحة دعم عميل شبكة VPN من Cisco
- مرجع أوامر PIX
- 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).