جدار حماية PIX الآمن من Cisco وبرنامج عميل Cisco VPN الإصدار 3.5 لنظام التشغيل Microsoft Windows 2000 و Windows 2003 IAS RADIUS

المحتويات

المقدمة

يوضح هذا النموذج من التكوين كيفية تكوين الإصدار 3.5 من Cisco VPN Client ل Windows وجدار حماية PIX الآمن من Cisco للاستخدام مع خادم RADIUS لخدمة مصادقة الإنترنت (IAS) ل Microsoft Windows 2000 و 2003. ارجع إلى Microsoft - قائمة التحقق: تكوين IAS للطلب الهاتفي والوصول إلى VPN للحصول على مزيد من المعلومات حول IAS.

ارجع إلى PIX/ASA 7.x و Cisco VPN Client 4.x ل Windows مع مثال تكوين مصادقة Microsoft Windows 2003 IAS RADIUS لمعرفة المزيد حول نفس السيناريو في PIX/ASA 7.0 مع Cisco VPN Client 4.x.

المتطلبات الأساسية

المتطلبات

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

- يدعم برنامج جدار حماية PIX الآمن من Cisco، الإصدار 6.0 إتصالات VPN من عميل Cisco VPN الإصدار 3.5 ل Windows.
- يفترض هذا التكوين العينة أن PIX يعمل بالفعل باستخدام قوائم الوصول أو القنوات أو قوائم الوصول المناسبة.

لا ينوي المستند الحالي توضيح هذه المفاهيم الأساسية، ولكن لإظهار الاتصال ب PIX من عميل Cisco VPN.

المكونات المستخدمة

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

- برنامج جدار حماية PIX الإصدار 6.1.1**ملاحظة:** تم إختبار ذلك على برنامج PIX الإصدار 6.1.1، ولكنه يجب أن يعمل على جميع إصدارات الإصدار x.6.
- Cisco VPN Client، الإصدار 3.5 ل Windows
- Windows 2000 و Server 2003 مع IAS

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.

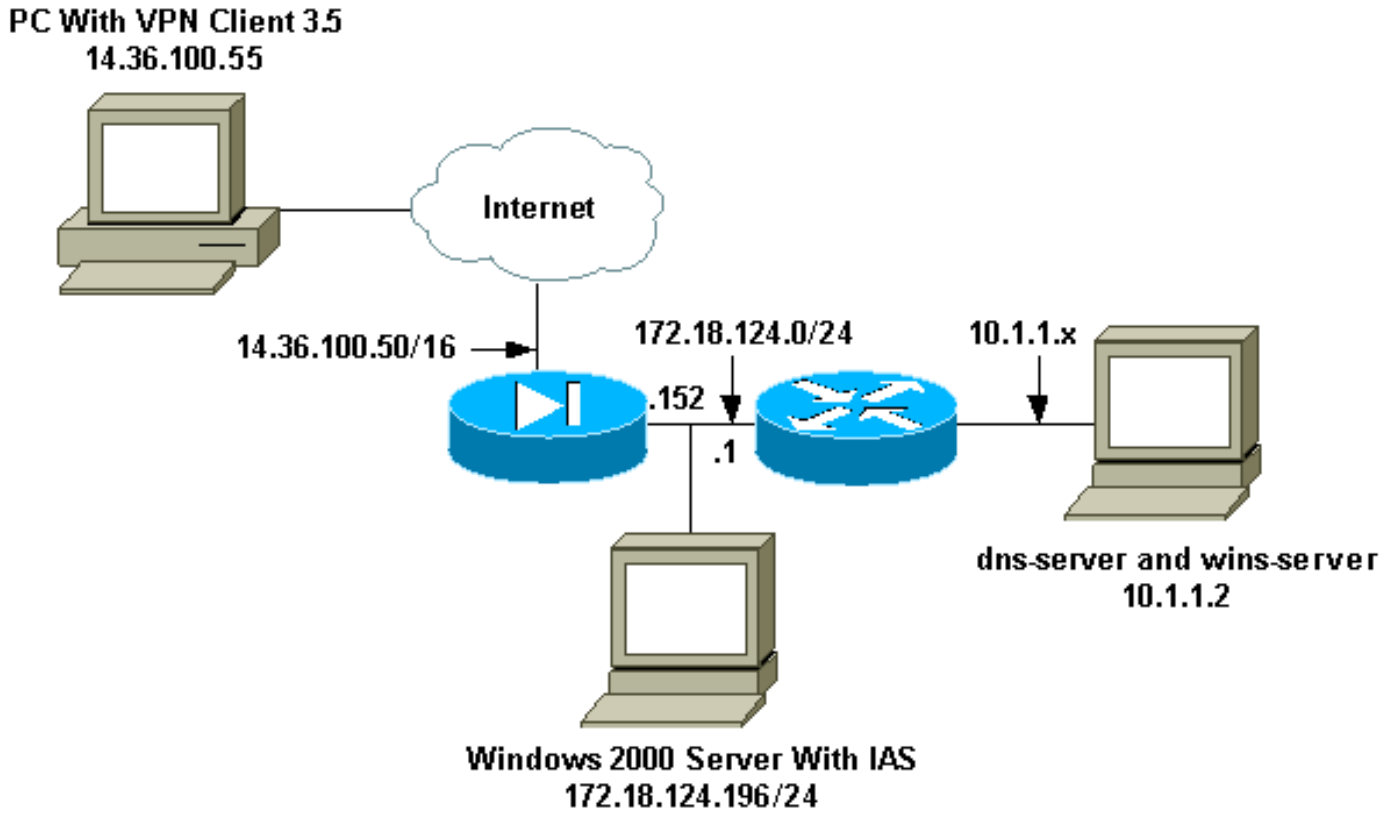
التكوين

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 هذه التكوينات.

- جدار حماية PIX
- Cisco VPN Client 3.5 ل Windows
- Microsoft Windows 2000 Server مع IAS
- Microsoft Windows 2003 Server مع IAS

جدار حماية PIX

جدار حماية PIX

```
pixfirewall(config)#write terminal
...Building configuration
Saved :
:
(PIX Version 6.1(1
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
```

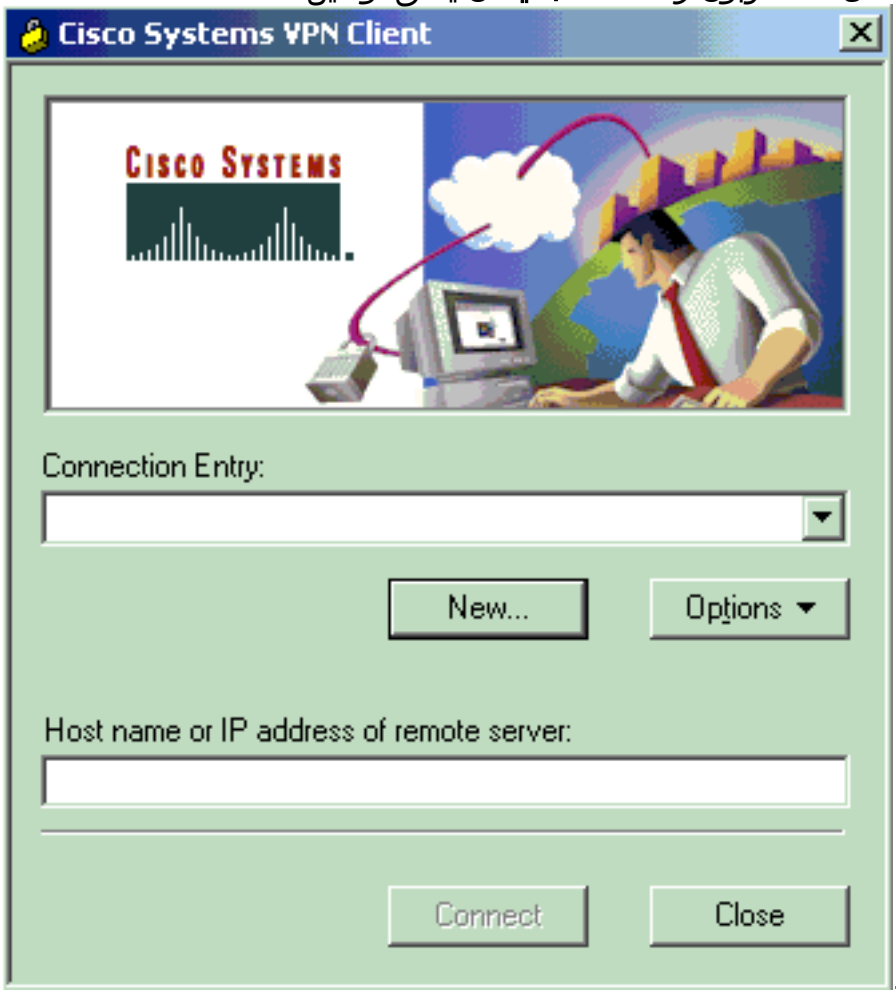
```
                                                                names
Issue the access-list command to avoid !--- Network ---!
        .Address Translation (NAT) on the IPsec packets

       access-list 101 permit ip 10.1.1.0 255.255.255.0
                                                  10.1.2.0
                                              255.255.255.0
                                               pager lines 24
                                    interface ethernet0 auto
                                    interface ethernet1 auto
                                            mtu outside 1500
                                             mtu inside 1500
           ip address outside 14.36.100.50 255.255.0.0
         ip address inside 172.18.124.152 255.255.255.0
                                 ip audit info action alarm
                               ip audit attack action alarm
              ip local pool ippool 10.1.2.1-10.1.2.254
                                         pdm history enable
                                          arp timeout 14400
                             global (outside) 1 14.36.100.51
    Binding access list 101 to the NAT statement to ---!
     avoid !--- NAT on the IPsec packets. nat (inside) 0
                                                access-list 101
                          Nat (inside) 1 0.0.0.0 0.0.0.0 0 0
                 route outside 0.0.0.0 0.0.0.0 14.36.1.1 1
          route inside 10.1.1.0 255.255.255.0 172.18.124.1
                                       timeout xlate 3:00:00
    timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
       rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media
                                                    0:02:00
                                timeout uauth 0:05:00 absolute
                .Enable access to the RADIUS protocol ---!
                                aaa-server RADIUS protocol radius
 Associate the partnerauth protocol to RADIUS. aaa- ---!
                                server partnerauth protocol radius
      aaa-server partnerauth (inside) host 172.18.124.196
                                                    cisco123
                                                  timeout 5
                                    no snmp-server location
                                     no snmp-server contact
                                snmp-server community public
                                 no snmp-server enable traps
                                                floodguard enable
Tell PIX to implicitly permit IPsec traffic. sysopt ---!
                                      connection permit-ipsec
                                        no sysopt route dnat
     Configure a transform set that defines how the ---!
   traffic is protected. crypto ipsec transform-set myset
                                          esp-des esp-md5-hmac
 Create a dynamic crypto map and specify which !--- ---!
   transform sets are allowed for this dynamic crypto map
     entry. crypto dynamic-map dynmap 10 set transform-set
                                                       myset
Add the dynamic crypto map set into a static crypto ---!
map set. crypto map mymap 10 ipsec-isakmp dynamic dynmap
   Enable the PIX to launch the Xauth application on ---!
   the VPN Client. crypto map mymap client authentication
                                                partnerauth
     Apply the crypto map to the outside interface. ---!
                                crypto map mymap interface outside
    IKE Policy Configuration. isakmp enable outside ---!
                                      isakmp identity address
                    isakmp policy 10 authentication pre-share
                                isakmp policy 10 encryption des
```

```
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
IPsec group configuration for VPN Client. vpngroup ---!
vpn3000 address-pool ippool
vpngroup vpn3000 dns-server 10.1.1.2
vpngroup vpn3000 wins-server 10.1.1.2
vpngroup vpn3000 default-domain cisco.com
vpngroup vpn3000 idle-time 1800
******** vpngroup vpn3000 password
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:3f9e31533911b8a6bb5c0f06900c2dbc
end :
[OK]
#(pixfirewall(config
```

Windows ل Cisco VPN Client 3.5

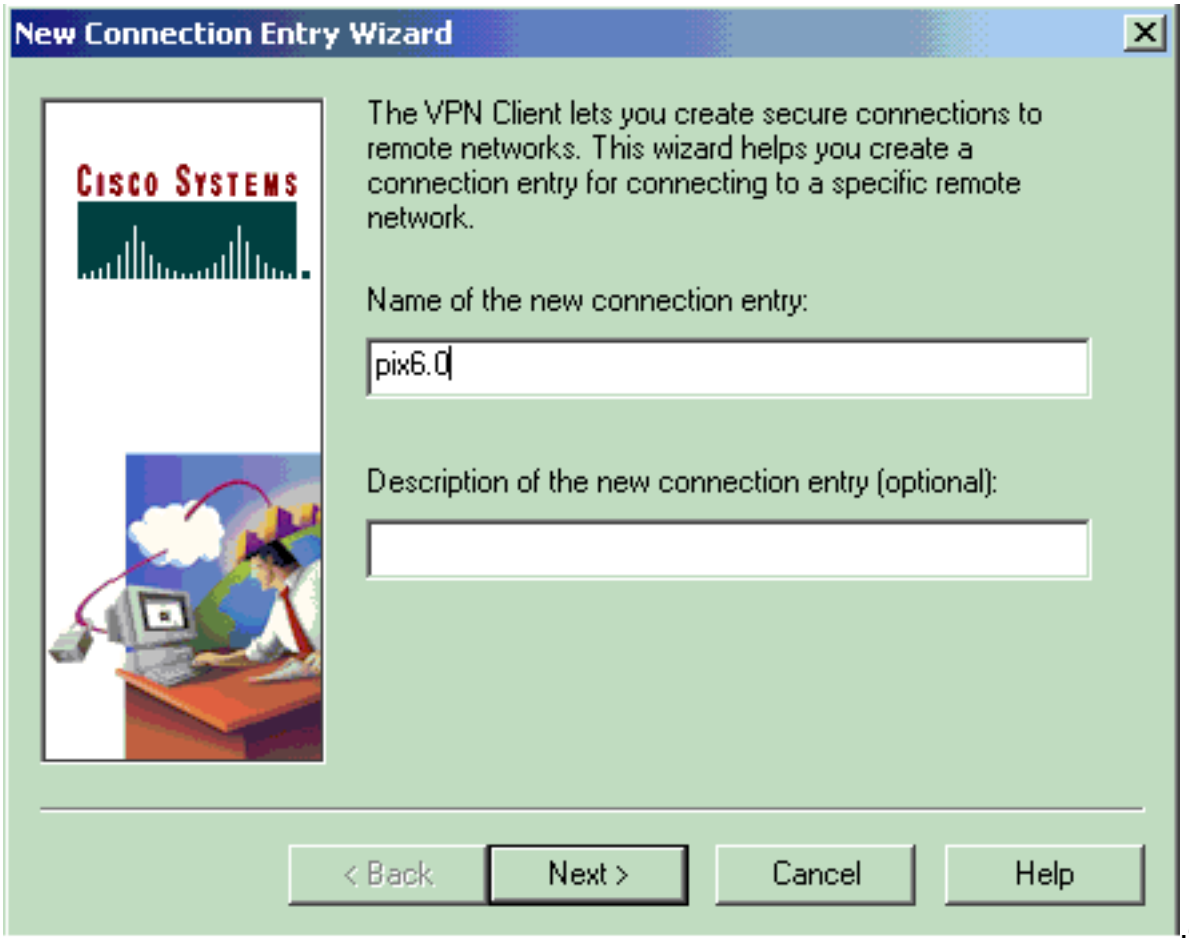
يشرح هذا القسم كيفية تكوين عميل Cisco VPN 3.5 ل Windows.

1. أطلقت ال VPN زبون وطقطقت **جديد** أن يخلق توصيل



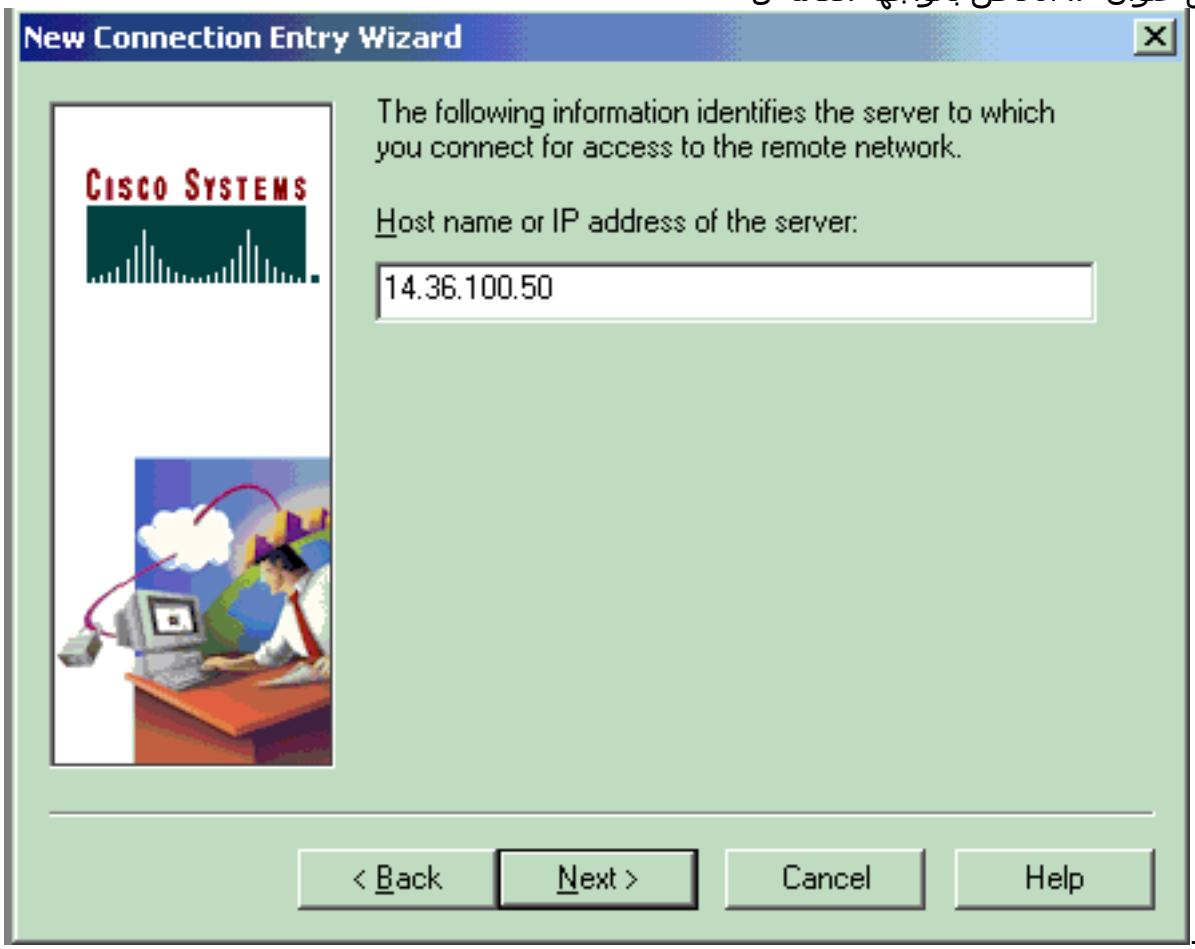
جديد.

2. في مربع **إدخال الاتصال**، قم بتعيين اسم للإدخال الخاص



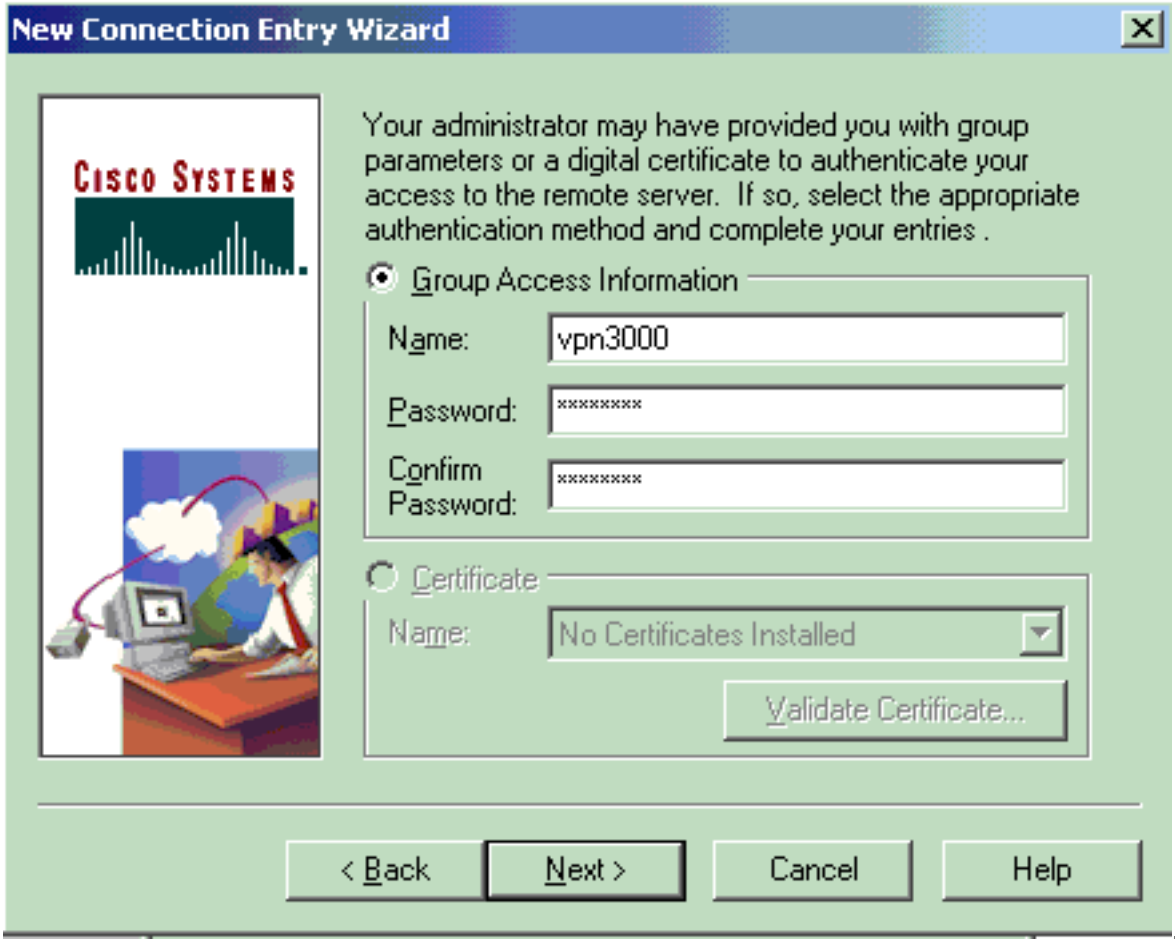
بك.

3. أدخل عنوان IP الخاص بالواجهة العامة ل



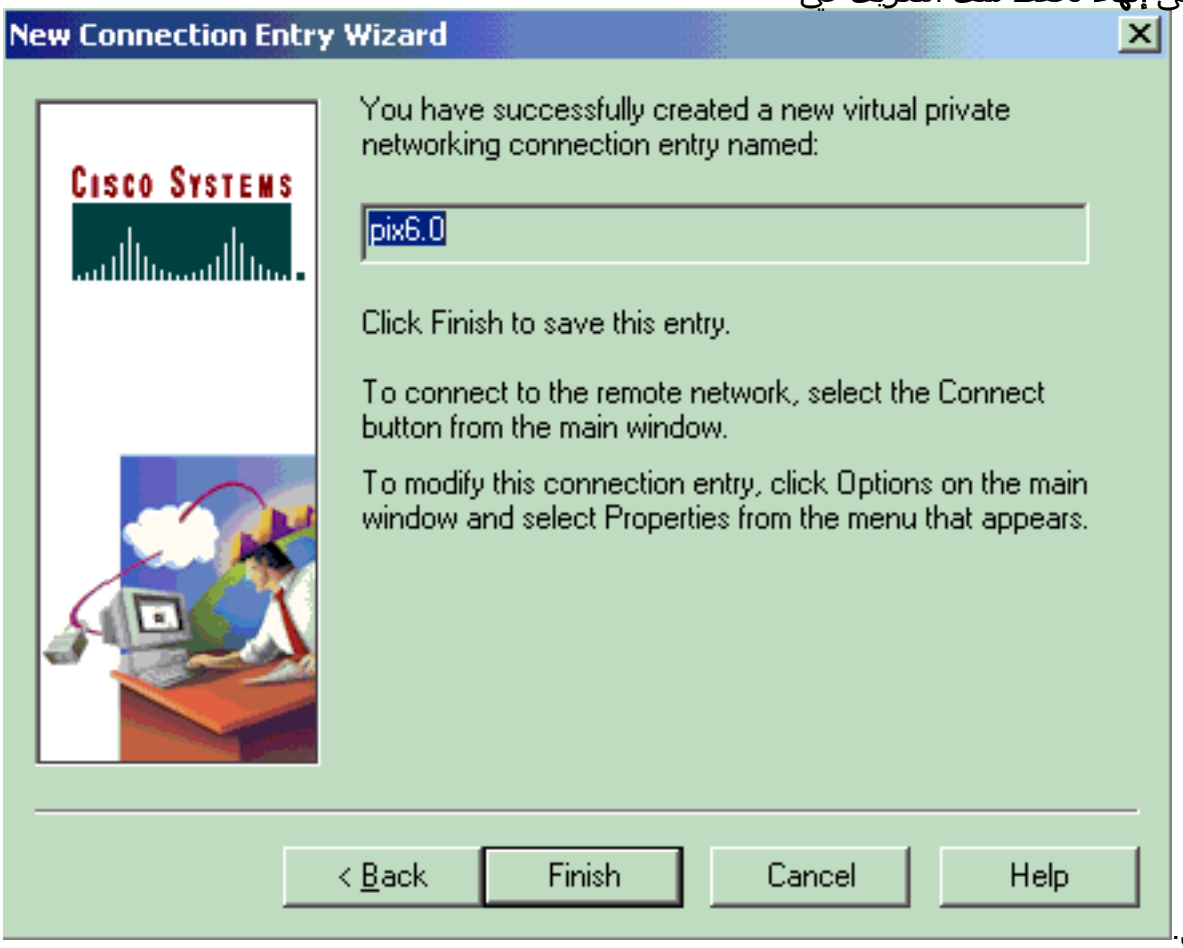
.PIX

4. تحت **معلومات الوصول إلى المجموعة**، أدخل اسم المجموعة وكلمة مرور

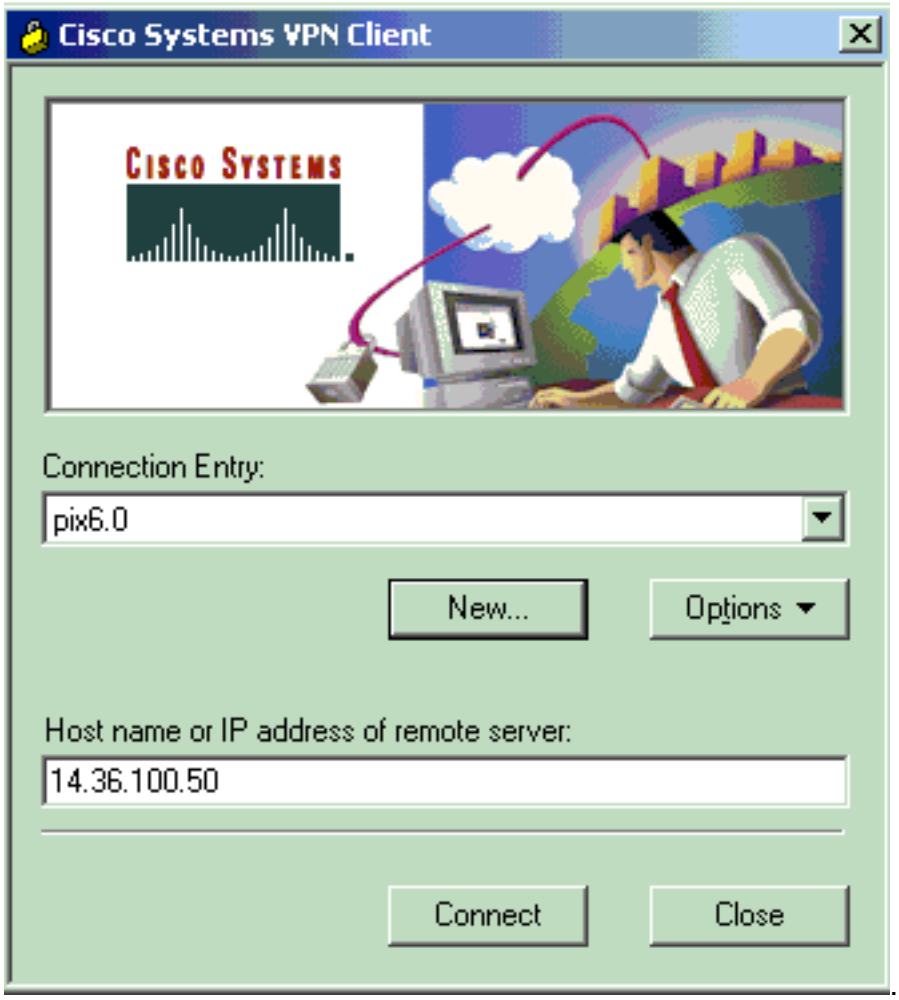


المجموعة.

5. انقر على **إنهاء** لحفظ ملف التعريف في



السجل.



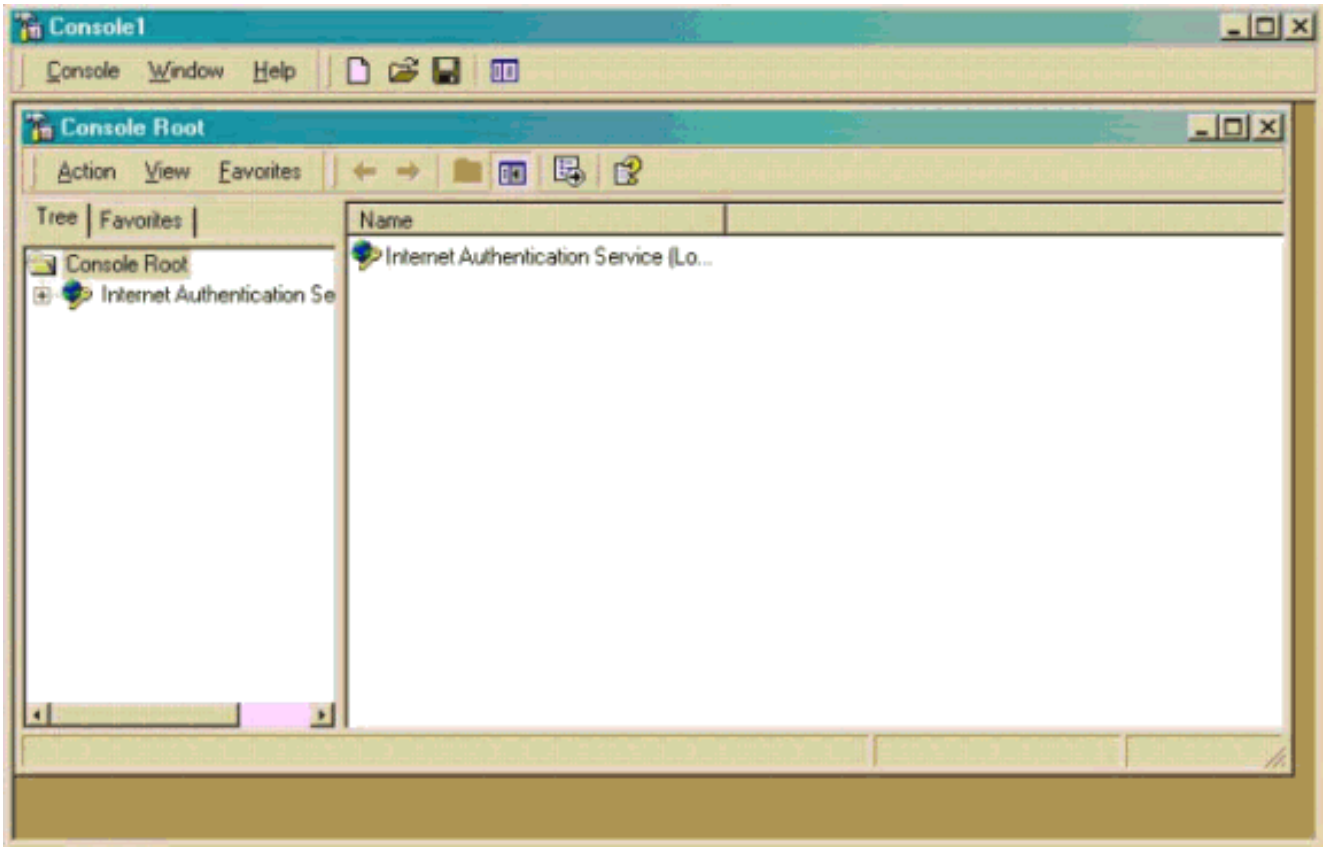
6. انقر فوق **توصيل"** للاتصال ب PIX.

Microsoft Windows 2000 Server مع IAS

أكمل الخطوات التالية لتكوين خادم Microsoft Windows 2000 باستخدام IAS. هذا إعداد أساسي للغاية لاستخدام خادم Windows 2000 IAS لمصادقة RADIUS الخاصة بمستخدمي VPN. إذا كنت بحاجة إلى تصميم أكثر تعقيدا، فاتصل ب Microsoft للحصول على المساعدة.

ملاحظة: تفترض هذه الخطوات أن المعايير الدولية للمحاسبة قد تم تثبيتها بالفعل على الجهاز المحلي. وإذا لم تكن هناك مساحة، فقم بإضافة هذا من خلال **لوحة التحكم > إضافة/إزالة البرامج**.

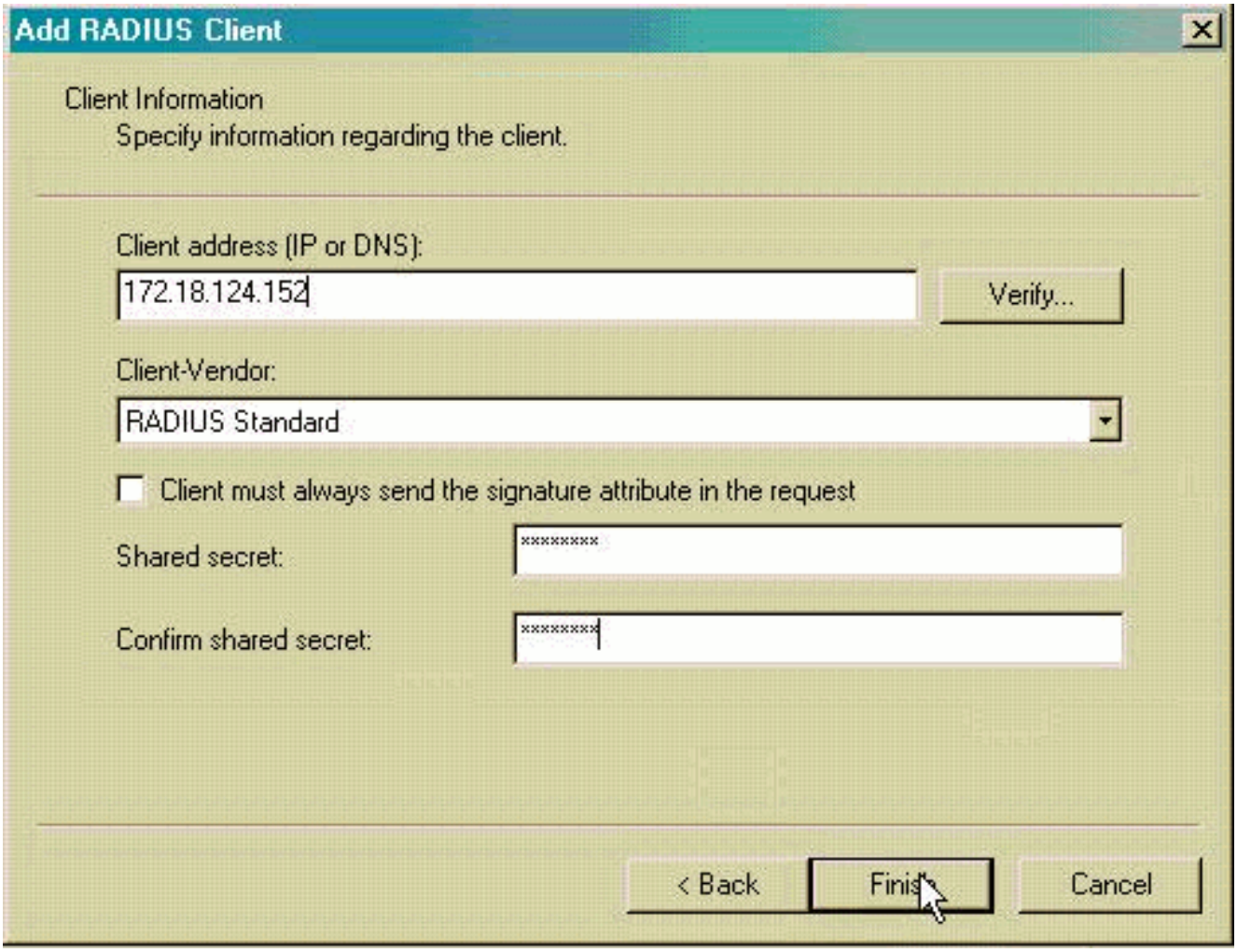
1. بدء تشغيل وحدة تحكم الإدارة من Microsoft. أختر **ابدأ > تشغيل** واكتب **MMC.** ثم انقر فوق **OK**.
2. أختر **وحدة التحكم > إضافة أداة إضافية لإزالة....** لإضافة خدمة IAS إلى وحدة التحكم هذه.
3. طقطقة **يضيف** in order to أطلقت نافذة جديد مع كل من يتوفر أداة إضافية مستقل. طقطقت **إنترنت صحة هوية خدمة (IAS)** وطقطقة **يضيف**.
4. تأكد من تحديد **الكمبيوتر المحلي** وانقر فوق **إنهاء**. ثم انقر فوق **إغلاق**".
5. لاحظ إضافة IAS الآن. انقر فوق **موافق** للتأكد من إضافته إلى جذر وحدة التحكم.



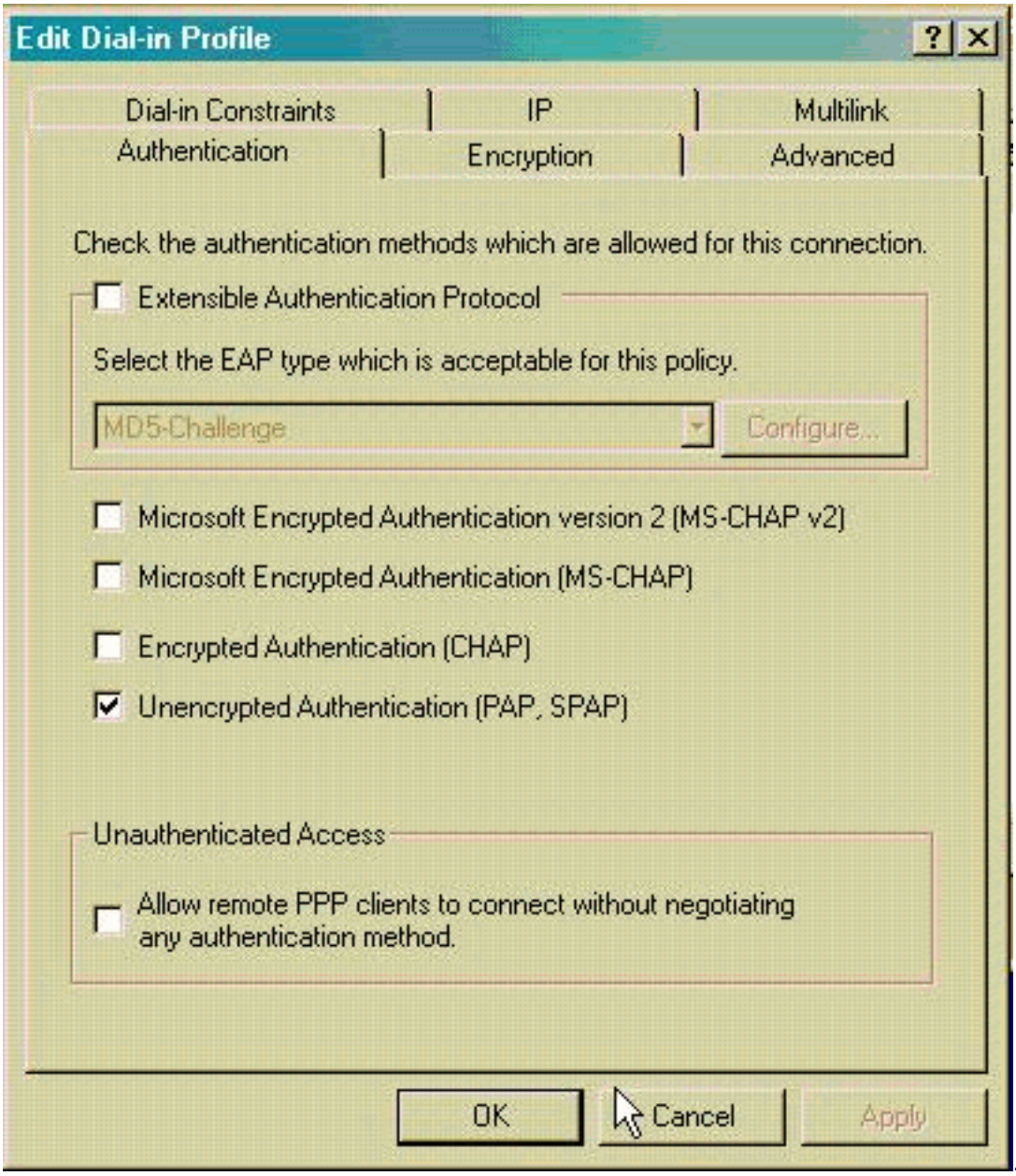
6. قم بتوسيع **خدمة مصادقة الإنترنت** وانقر بزر الماوس الأيمن فوق **العملاء**. انقر فوق **عميل جديد** وقم بإدخال اسم. ان إختيار الاسم ليس مهما حقا؛ فهو ما تراه في وجهة النظر هذه. تأكد من تحديد **RADIUS** وانقر **بعد ذلك**.
7. املأ **عنوان العميل** بعنوان واجهة PIX الذي يتم توصيل خادم IAS به. تأكد من تحديد **RADIUS Standard** وأضف السر المشترك لمطابقة الأمر الذي أدخلته على PIX:

```
aaa-server partnerauth (inside) host 172.18.124.196 cisco123 timeout 5
```

ملاحظة: في هذا المثال، "Cisco123" هي السر المشترك.

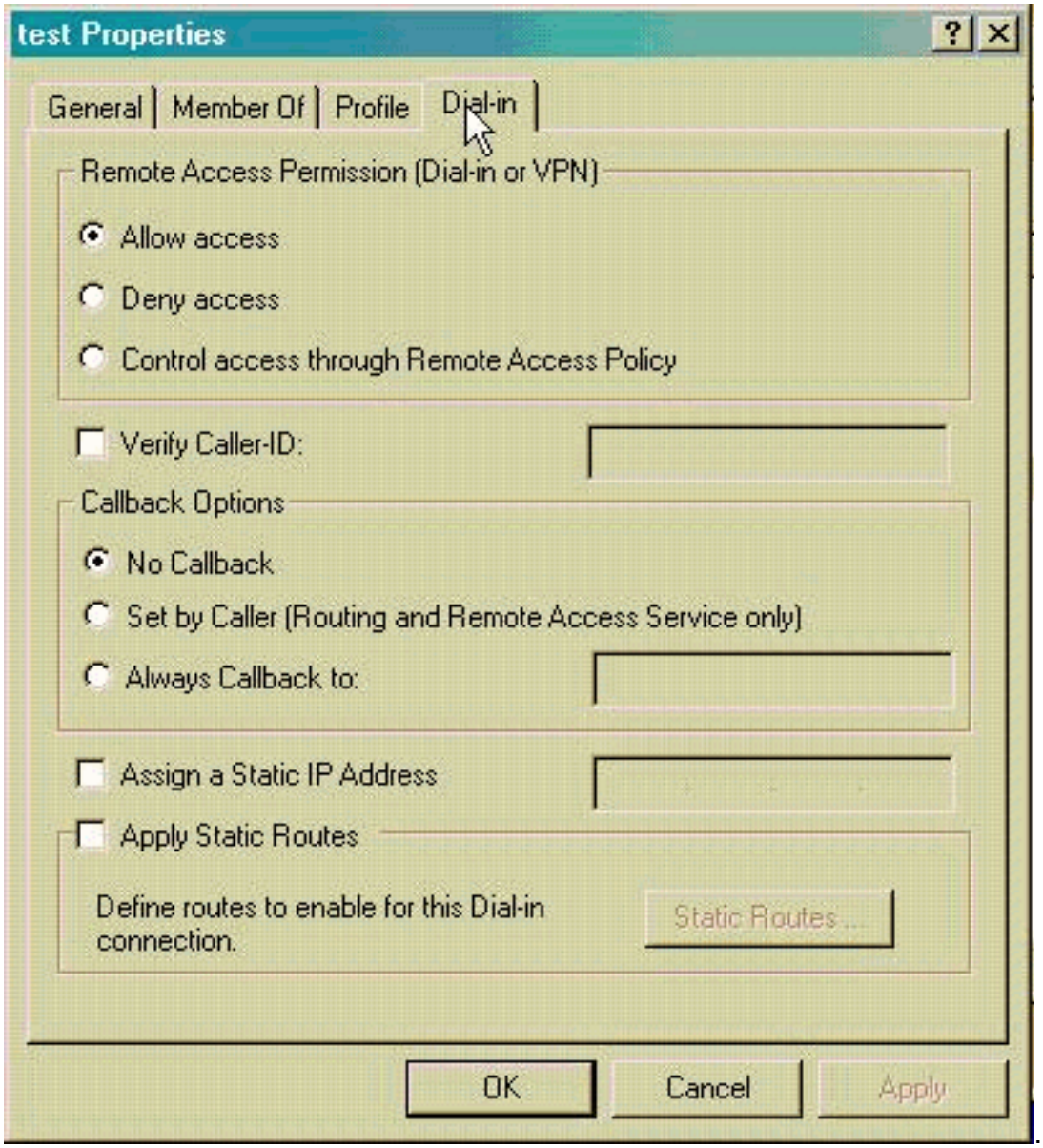


8. انقر فوق **إنهاء** للعودة إلى جذر وحدة التحكم.
9. انقر فوق **نهج الوصول عن بعد** في الجزء الأيسر وانقر نقرا مزدوجا فوق النهج المسمى **السماح بالوصول في حالة تمكين إذن الطلب الهاتفي**.
10. انقر على **تحرير التوصيف** وانتقل إلى علامة تبويب المصادقة. تحت **طرق المصادقة**، تأكد من **التحقق من المصادقة غير المشفرة (PAP، SPAP)** فقط.**ملاحظة:** يمكن لعميل شبكة VPN إستخدام هذه الطريقة فقط



للمصادقة.

11. طقطقة **يطبق** وبعد ذلك **ok** مرتين.
12. لتعديل المستخدمين للسماح بالاتصال، أختر **وحدة التحكم > إضافة/إزالة الأداة الإضافية**. انقر فوق **إضافة** ثم حدد الأداة الإضافية **المستخدمون المحليون والمجموعات المحلية**. انقر فوق **إضافة (Add)**. تأكد من تحديد **الكمبيوتر المحلي** وانقر فوق **إنهاء**. وانقر فوق OK.
13. قم بتوسيع **المستخدم المحلي والمجموعات المحلية** وانقر فوق مجلد **المستخدمين** في الجزء الأيسر. في الجزء الأيمن، انقر نقرا مزدوجا فوق المستخدم الذي تريد السماح بالوصول إليه.
14. انقر فوق علامة التبويب الطلب الهاتفي وحدد **السماح بالوصول** ضمن **إذن الوصول عن بعد (الطلب الهاتفي أو**



(VPN).

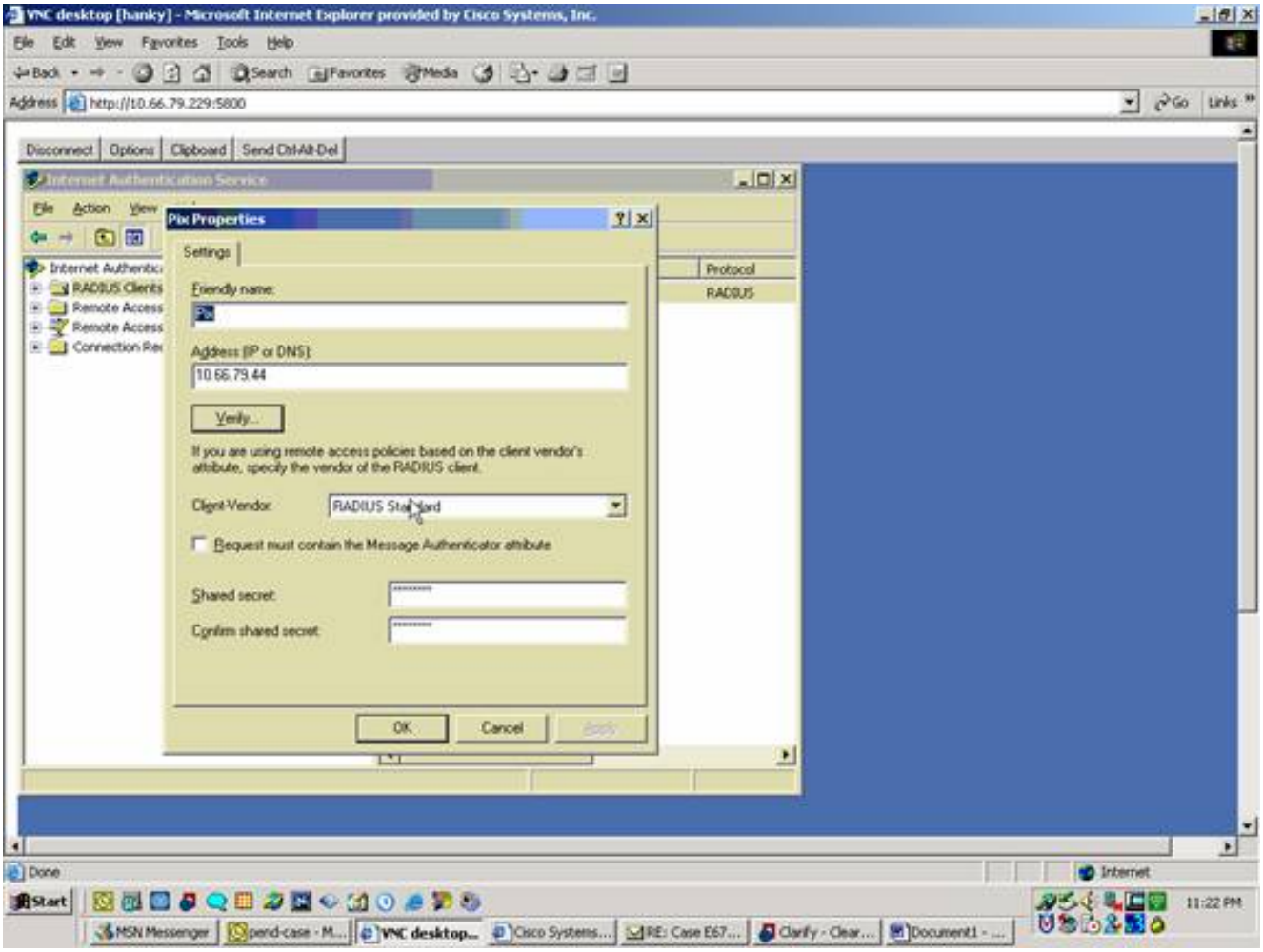
15. انقر فوق **تطبيق** و**موافق** لإكمال الإجراء. يمكنك إغلاق شاشة **إدارة وحدة التحكم** وحفظ الجلسة، إذا أردت.
16. يجب أن يكون المستخدمون الذين قمت بتعديلهم قادرين الآن على الوصول إلى PIX باستخدام عميل VPN 3.5. الرجاء مراعاة أن خادم IAS يقوم بمصادقة معلومات المستخدم فقط. لا يزال PIX يقوم بمصادقة المجموعة.

Microsoft Windows 2003 Server مع IAS

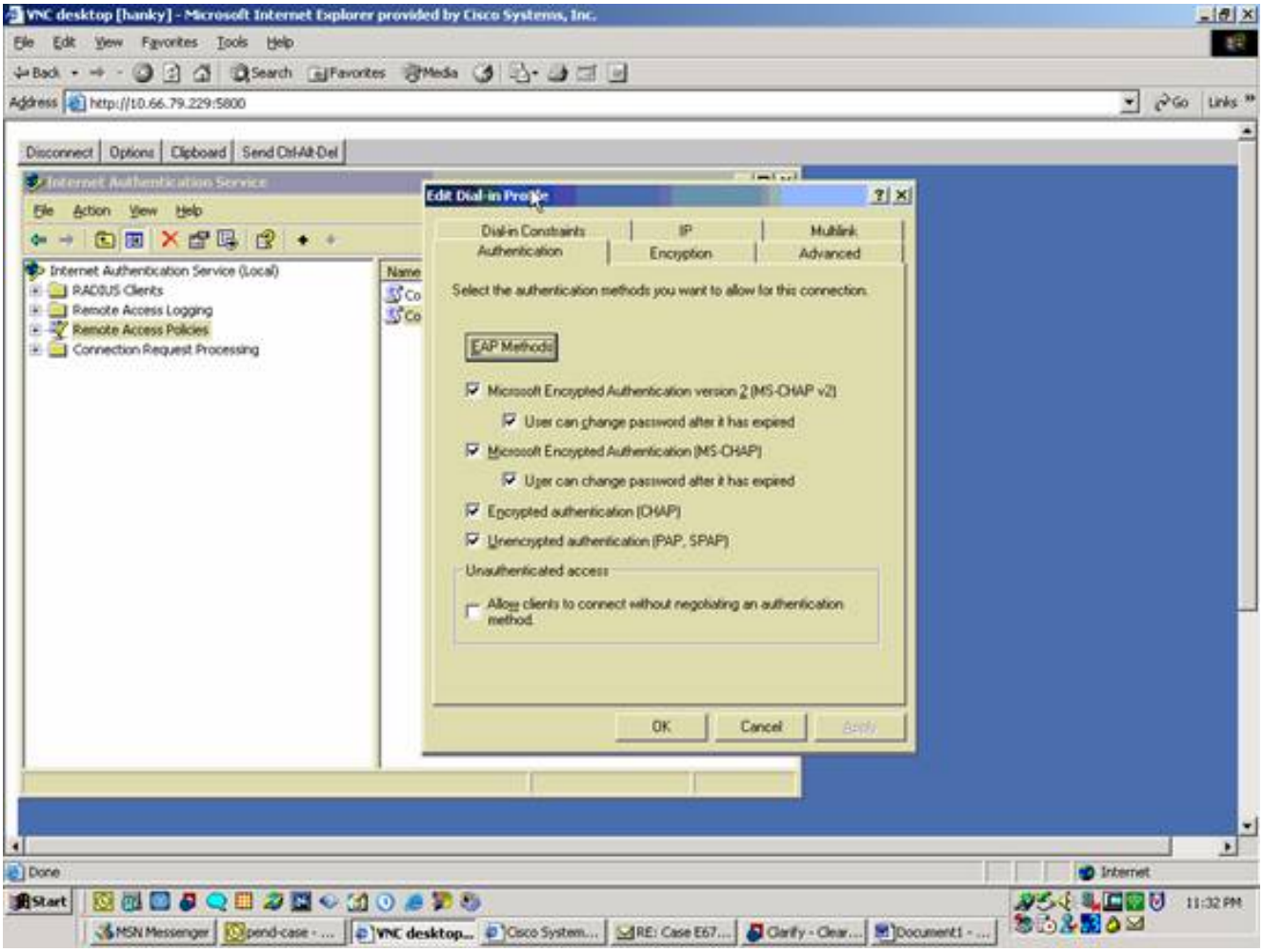
أكمل الخطوات التالية لتكوين خادم Microsoft Windows 2003 باستخدام IAS.

ملاحظة: تفترض هذه الخطوات أن المعايير الدولية للمحاسبة قد تم تثبيتها بالفعل على الجهاز المحلي. وإذا لم تكن هناك مساحة، فقم بإضافة هذا من خلال **لوحة التحكم > إضافة/إزالة البرامج**.

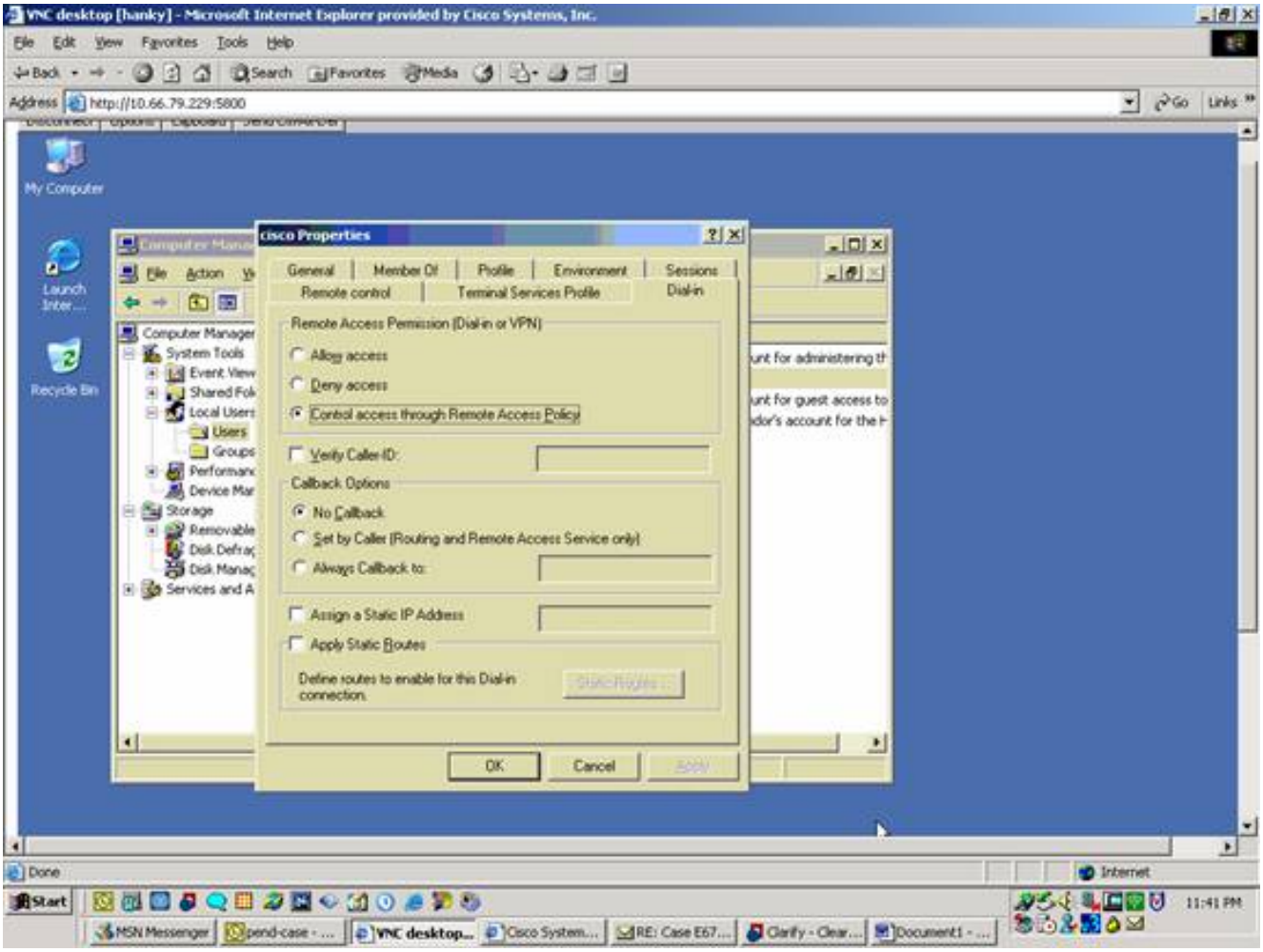
1. أختر **أدوات إدارية > خدمة مصادقة الإنترنت** وانقر بزر الماوس الأيمن فوق **عميل RADIUS** لإضافة عميل RADIUS جديد. بعد كتابة معلومات العميل، انقر فوق **موافق**.يوضح هذا المثال عميل مسمى "PIX" بعنوان IP بقيمة 10.66.79.44. تم تعيين العميل-المورد على معيار RADIUS، والسر المشترك هو "Cisco123".



2. انتقل إلى **نهج الوصول عن بعد**، وانقر بزر الماوس الأيمن فوق **الاتصالات بخوادم الوصول الأخرى**، وحدد **الخصائص**.
3. تأكد من تحديد خيار منح أذونات الوصول عن بعد.
4. انقر على **تحرير التوصيف** وتحقق من هذه الإعدادات.في علامة تبويب المصادقة، تحقق من **المصادقة غير المشفرة (PAP، SPAP)**.في علامة تبويب التشفير، تأكد من تحديد خيار عدم التشفير.طقطقت **ok** عندما أنت إنتهيت.



5. إضافة مستخدم إلى حساب الكمبيوتر المحلي. للقيام بذلك، أختر **الأدوات الإدارية > إدارة الكمبيوتر > أدوات النظام > المستخدمون المحليون والمجموعات المحلية.**. انقر بزر الماوس الأيمن فوق **المستخدمين** وحدد **المستخدمين الجدد**.
6. أضفت مستعمل مع cisco كلمة "cisco123" وفحصت هذا توصيف معلومة.على علامة التبويب "عام"، تأكد من تحديد خيار **كلمة المرور التي لا تنتهي صلاحيتها أبدا** بدلا من الخيار الخاص ب المستخدم الذي يجب عليه تغيير كلمة المرور.في علامة التبويب "الطلب الهاتفي"، حدد الخيار ل **السماح بالوصول** (أو أترك الإعداد الافتراضي ل Control Access من خلال نهج الوصول عن بعد).طقطقت **ok** عندما أنت إنتهيت.



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 isakmp sa**—يعرض جميع اقترانات أمان IKE الحالية (SAs) في نظير.
- **show crypto ipSec**—يعرض الإعدادات المستخدمة من قبل اقترانات الأمان الحالية.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها. لمزيد من المعلومات، ارجع إلى أستكشاف أخطاء PIX وإصلاحها لتمرير حركة مرور البيانات على نفق IPSec تم إنشاؤه.

أوامر استكشاف الأخطاء وإصلاحها

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

ملاحظة: ارجع إلى معلومات مهمة عن أوامر تصحيح الأخطاء قبل أن تستخدم أوامر **debug** ارجع إلى أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها.

- **debug crypto ipSec**—عرض مفاوضات IPSec للمرحلة 2.
- **debug crypto isakmp**—عرض مفاوضات ISAKMP للمرحلة 1.
- **debug crypto engine**—عرض حركة مرور البيانات التي يتم تشفيرها.

إخراج تصحيح الأخطاء للعينة

- جدار حماية PIX
- Windows ل VPN Client 3.5

جدار حماية PIX

```
                                                #(pixfirewall(config
   crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
VPN Peer: ISAKMP: Added new peer: ip:14.36.100.55 Total VPN Peers:1
    VPN Peer: ISAKMP: Peer ip:14.36.100.55 Ref cnt incremented to:1
                                                Total VPN Peers:1
                                                     OAK_AG exchange
                ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
                                     ISAKMP:      encryption 3DES-CBC
                                               ISAKMP:      hash SHA
                                         ISAKMP:      default group 2
                                    ISAKMP:      extended auth pre-share
                                       ISAKMP:      life type in seconds
           ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
            ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
                                     ISAKMP:      encryption 3DES-CBC
                                               ISAKMP:      hash MD5
                                         ISAKMP:      default group 2
                                    ISAKMP:      extended auth pre-share
                                       ISAKMP:      life type in seconds
           ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
            ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
                                     ISAKMP:      encryption 3DES-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 (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 10 policy
                                     ISAKMP:      encryption 3DES-CBC
                                               ISAKMP:      hash MD5
                                         ISAKMP:      default group 2
                                          ISAKMP:      auth pre-share
                                       ISAKMP:      life type in seconds
           ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
            ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy
                                      ISAKMP:      encryption DES-CBC
                                               ISAKMP:      hash SHA
                                         ISAKMP:      default group 2
                                    ISAKMP:      extended auth pre-share
                                       ISAKMP:      life type in seconds
           ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
```

```
                ISAKMP (0): atts are not acceptable. Next payload is 3
   ISAKMP (0): Checking ISAKMP transform 6 against priority 10 policy
                                      ISAKMP:      encryption DES-CBC
                                                ISAKMP:      hash MD5
                                             ISAKMP:      default group 2
                                       ISAKMP:      extended auth pre-share
                                          ISAKMP:      life type in seconds
                    ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
                         ISAKMP (0): atts are acceptable. Next payload is 3
                          ISAKMP (0): processing KE payload. message ID = 0

                       ISAKMP (0): processing NONCE payload. message ID = 0

                          ISAKMP (0): processing ID payload. message ID = 0
                                   ISAKMP (0): processing vendor id payload

                                   ISAKMP (0): processing vendor id payload

                       ISAKMP (0): remote peer supports dead peer detection

                                   ISAKMP (0): processing vendor id payload

                                     ISAKMP (0): speaking to a Unity client

                                ISAKMP: Created a peer node for 14.36.100.55
                                                    ISAKMP (0): ID payload
                                                  next-payload : 10
                                                  type         : 1
                                                 protocol     : 17
                                                port         : 500
                                                  length       : 8
                                     ISAKMP (0): Total payload length: 12
                                           return status is IKMP_NO_ERROR
    crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
                                                        OAK_AG exchange
                      ISAKMP (0): processing HASH payload. message ID = 0
                    ISAKMP (0): processing NOTIFY payload 24578 protocol 1
                                           spi 0, message ID = 0
  ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine): got
                                                     ...a queue event
        IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 14.36.100.55

                                    ISAKMP (0): SA has been authenticated
                                           return status is IKMP_NO_ERROR
                                 ISAKMP/xauth: request attribute XAUTH_TYPE
                             ISAKMP/xauth: request attribute XAUTH_USER_NAME
                         ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 14.36.100.55. ID = 3870616596
                                                        (0xe6b4ec14)
    crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
                                           ISAKMP_TRANSACTION exchange
     .ISAKMP (0:0): processing transaction payload from 14.36.100.55
                                                     message ID = 84
                                        ISAKMP: Config payload CFG_REPLY
                                      return status is IKMP_ERR_NO_RETRANS
ISAKMP (0:0): initiating peer config to 14.36.100.55. ID = 3612718114
                                                        (0xd755b422)
    crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
                                           ISAKMP_TRANSACTION exchange
     .ISAKMP (0:0): processing transaction payload from 14.36.100.55
                                                     message ID = 60
                                          ISAKMP: Config payload CFG_ACK
                                          return status is IKMP_NO_ERROR
```

```
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
                                        ISAKMP_TRANSACTION exchange
 .ISAKMP (0:0): processing transaction payload from 14.36.100.55
                                                  message ID = 0
                                    ISAKMP: Config payload CFG_REQUEST
                                       :ISAKMP (0:0): checking request
                                  (ISAKMP: attribute    IP4_ADDRESS (1
                                  (ISAKMP: attribute    IP4_NETMASK (2
                                      (ISAKMP: attribute    IP4_DNS (3
                                     (ISAKMP: attribute    IP4_NBNS (4
                                (ISAKMP: attribute    ADDRESS_EXPIRY (5
                                        Unsupported Attr: 5
                            (ISAKMP: attribute    APPLICATION_VERSION (7
                                        Unsupported Attr: 7
                                  (ISAKMP: attribute    UNKNOWN (28672
                                       Unsupported Attr: 28672
                                  (ISAKMP: attribute    UNKNOWN (28673
                                       Unsupported Attr: 28673
                                  (ISAKMP: attribute    UNKNOWN (28674
                                  (ISAKMP: attribute    UNKNOWN (28676
                                  (ISAKMP: attribute    UNKNOWN (28679
                                       Unsupported Attr: 28679
                                  (ISAKMP: attribute    UNKNOWN (28680
                                       Unsupported Attr: 28680
                                  (ISAKMP: attribute    UNKNOWN (28677
                                       Unsupported Attr: 28677
      .ISAKMP (0:0): responding to peer config from 14.36.100.55
                                                 ID = 3979868003
                                     return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
                                                  OAK_QM exchange
                                          :oakley_process_quick_mode
                                                       OAK_QM_IDLE
      ISAKMP (0): processing SA payload. message ID = 1527320241

                                    ISAKMP : Checking IPSec proposal 1

                                         ISAKMP: transform 1, ESP_3DES
                                      :ISAKMP:   attributes in transform
                                ISAKMP:      authenticator is HMAC-MD5
                                         ISAKMP:      encaps is 1
                                   ISAKMP:      SA life type in seconds
      ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
  IPSEC(validate_proposal): transform proposal (prot 3, trans
                                       hmac_alg 1) not supported ,3

                     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_3DES
                                      :ISAKMP:   attributes in transform
                                ISAKMP:      authenticator is HMAC-SHA
                                         ISAKMP:      encaps is 1
                                   ISAKMP:      SA life type in seconds
      ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
  IPSEC(validate_proposal): transform proposal (prot 3, trans
                                       hmac_alg 2) not supported ,3

                     ISAKMP (0): atts not acceptable. Next payload is 0
                           (ISAKMP (0): skipping next ANDed proposal (2
                                    ISAKMP : Checking IPSec proposal 3

                                         ISAKMP: transform 1, ESP_3DES
```

```
                                        :ISAKMP:   attributes in transform
                                    ISAKMP:      authenticator is HMAC-MD5
                                                  ISAKMP:      encaps is 1
                                      ISAKMP:      SA life type in seconds
        ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
    IPSEC(validate_proposal): transform proposal (prot 3, trans
                                            hmac_alg 1) not supported ,3

                    ISAKMP (0): atts not acceptable. Next payload is 0
                                    ISAKMP : Checking IPSec proposal 4

                                         ISAKMP: transform 1, ESP_3DES
                                        :ISAKMP:   attributes in transform
                                    ISAKMP:      authenticator is HMAC-SHA
                                                  ISAKMP:      encaps is 1
                                      ISAKMP:      SA life type in seconds
        ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
    IPSEC(validate_proposal): transform proposal (prot 3, trans
                                            hmac_alg 2) not supported ,3

                    ISAKMP (0): atts not acceptable. Next payload is 0
                                    ISAKMP : Checking IPSec proposal 5

                                         ISAKMP: transform 1, ESP_DES
                                        :ISAKMP:   attributes in transform
                                    ISAKMP:      authenticator is HMAC-MD5
                                                  ISAKMP:      encaps is 1
                                      ISAKMP:      SA life type in seconds
        ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
                                   .ISAKMP (0): atts are acceptable
                                !ISAKMP (0): bad SPI size of 2 octets
                                    ISAKMP : Checking IPSec proposal 6

                                         ISAKMP: transform 1, ESP_DES
                                        :ISAKMP:   attributes in transform
                                    ISAKMP:      authenticator is HMAC-SHA
                                                  ISAKMP:      encaps is 1
                                      ISAKMP:      SA life type in seconds
        ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
    IPSEC(validate_proposal): transform proposal (prot 3, trans
                                            hmac_alg 2) not supported ,2

                    ISAKMP (0): atts not acceptable. Next payload is 0
                          (ISAKMP (0): skipping next ANDed proposal (6
                                    ISAKMP : Checking IPSec proposal 7

                                         ISAKMP: transform 1, ESP_DES
                                        :ISAKMP:   attributes in transform
                                    ISAKMP:      authenticator is HMAC-MD5
                                                  ISAKMP:      encaps is 1
                                      ISAKMP:      SA life type in seconds
        ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
:(ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request
                                                 ,proposal part #1
          ,key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55)
        ,(dest_proxy= 14.36.100.50/255.255.255.255/0/0 (type=1
             ,(src_proxy= 10.1.2.1/255.255.255.255/0/0 (type=1
              , protocol= ESP, transform= esp-des esp-md5-hmac
                                              ,lifedur= 0s and 0kb
                spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

    ISAKMP (0): processing NONCE payload. message ID = 1527320241

        ISAKMP (0): processing ID payload. message ID = 1527320241
```

```
                                ISAKMP (0): ID_IPV4_ADDR src 10.1.2.1 prot 0 port 0
                            ISAKMP (0): processing ID payload. message ID = 1527320241
                                 ISAKMP (0): ID_IPV4_ADDR dst 14.36.100.50 prot 0 port
                                           ...0IPSEC(key_engine): got a queue event
                              IPSEC(spi_response): getting spi 0xf39c2217(4087095831) for SA
                                  from    14.36.100.55 to    14.36.100.50 for prot 3

                                                                  return status is IKMP_NO_ERROR
                                 crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
                                                                                OAK_QM exchange
                                                                       :oakley_process_quick_mode
                                                                                    OAK_QM_IDLE
                                      ISAKMP (0): processing SA payload. message ID = 3487980779

                                                                ISAKMP : Checking IPSec proposal 1

                                                                     ISAKMP: transform 1, ESP_3DES
                                                                   :ISAKMP:   attributes in transform
                                                                ISAKMP:      authenticator is HMAC-MD5
                                 crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
                                                                                OAK_QM exchange
                                                                       :oakley_process_quick_mode
                                                                              OAK_QM_AUTH_AWAIT
                                                                  ISAKMP (0): Creating IPSec SAs
                                      inbound SA from    14.36.100.55 to    14.36.100.50
                                         (proxy        10.1.2.1 to    14.36.100.50)
                                            has spi 4087095831 and conn_id 1 and flags 4
                                                                lifetime of 2147483 seconds
                                     outbound SA from    14.36.100.50 to    14.36.100.55
                                         (proxy    14.36.100.50 to        10.1.2.1)
                                            has spi 1929305241 and conn_id 2 and flags 4
                        ...lifetime of 2147483 secondsIPSEC(key_engine): got a queue event
                                                                          , :(IPSEC(initialize_sas
                                           ,key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55)
                                                 ,(dest_proxy= 14.36.100.50/0.0.0.0/0/0 (type=1
                                                      ,(src_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1
                                                 , protocol= ESP, transform= esp-des esp-md5-hmac
                                                                ,lifedur= 2147483s and 0kb
                                 spi= 0xf39c2217(4087095831), conn_id= 1, keysize= 0, flags= 0x4
                                                                          , :(IPSEC(initialize_sas
                                           ,key eng. msg.) src= 14.36.100.50, dest= 14.36.100.55)
                                                  ,(src_proxy= 14.36.100.50/0.0.0.0/0/0 (type=1
                                                     ,(dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1
                                                 , protocol= ESP, transform= esp-des esp-md5-hmac
                                                                ,lifedur= 2147483s and 0kb
                                 spi= 0x72fedc99(1929305241), conn_id= 2, keysize= 0, flags= 0x4

                                      VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:2
                                                                          Total VPN Peers:1
                                      VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:3
                                                                          Total VPN Peers:1
                                                                  return status is IKMP_NO_ERROR
                                 crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
                                                                                OAK_QM exchange
                                                                       :oakley_process_quick_mode
                                                                              OAK_QM_AUTH_AWAIT
                                                                  ISAKMP (0): Creating IPSec SAs
                                      inbound SA from    14.36.100.55 to    14.36.100.50
                                         (proxy        10.1.2.1 to         0.0.0.0)
                                            has spi 1791135440 and conn_id 3 and flags 4
                                                                lifetime of 2147483 seconds
                                     outbound SA from    14.36.100.50 to    14.36.100.55
                                         (proxy         0.0.0.0 to        10.1.2.1)
                                             has spi 173725574 and conn_id 4 and flags 4
```

```
...lifetime of 2147483 secondsIPSEC(key_engine): got a queue event
                                                , :(IPSEC(initialize_sas
                  ,key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55)
                                ,(dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
                                ,(src_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1
                     , protocol= ESP, transform= esp-des esp-md5-hmac
                                              ,lifedur= 2147483s and 0kb
        spi= 0x6ac28ed0(1791135440), conn_id= 3, keysize= 0, flags= 0x4
                                                , :(IPSEC(initialize_sas
                  ,key eng. msg.) src= 14.36.100.50, dest= 14.36.100.55)
                                 ,(src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
                                ,(dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1
                     , protocol= ESP, transform= esp-des esp-md5-hmac
                                              ,lifedur= 2147483s and 0kb
          spi= 0xa5ad786(173725574), conn_id= 4, keysize= 0, flags= 0x4

      VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:4
                                                 Total VPN Peers:1
      VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:5
                                                 Total VPN Peers:1
                                        return status is IKMP_NO_ERROR
       crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
                 ISAKMP (0): processing NOTIFY payload 36136 protocol 1
                                  spi 0, message ID = 3443334051
            ISAMKP (0): received DPD_R_U_THERE from peer 14.36.100.55
                  ISAKMP (0): sending NOTIFY message 36137 protocol 1
                                  return status is IKMP_NO_ERR_NO_TRANS
```

Windows „J VPN Client 3.5

```
    Sev=Info/6       DIALER/0x63300002  01/24/02  19:00:56.073    193
                                              .Initiating connection

        Sev=Info/4       CM/0x63100002  01/24/02  19:00:56.073    194
                                            Begin connection process

        Sev=Info/4       CM/0x63100004  01/24/02  19:00:56.083    195
                             Establish secure connection using Ethernet

        Sev=Info/4       CM/0x63100026  01/24/02  19:00:56.083    196
                           "Attempt connection with server "14.36.100.50

      Sev=Info/6       IKE/0x6300003B  01/24/02  19:00:56.083    197
             .Attempting to establish a connection with 14.36.100.50

      Sev=Info/4       IKE/0x63000013  01/24/02  19:00:56.124    198
          (SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID
                                                    to 14.36.100.50

       Sev=Info/4       IPSEC/0x63700014  01/24/02  19:00:56.774    199
                                                  Deleted all keys

      Sev=Info/5       IKE/0x6300002F  01/24/02  19:00:59.539    200
                             Received ISAKMP packet: peer = 14.36.100.50

      Sev=Info/4       IKE/0x63000014  01/24/02  19:00:59.539    201
    (RECEIVING <<< ISAKMP OAK AG (SA, VID, VID, VID, KE, ID, NON, HASH
                                                  from 14.36.100.50

      Sev=Info/5       IKE/0x63000059  01/24/02  19:00:59.539    202
                Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

      Sev=Info/5       IKE/0x63000001  01/24/02  19:00:59.539    203
```

```
                                    Peer is a Cisco-Unity compliant peer

  Sev=Info/5       IKE/0x63000059  01/24/02  19:00:59.539    204
           Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

  Sev=Info/5       IKE/0x63000001  01/24/02  19:00:59.539    205
                                                 Peer supports DPD

  Sev=Info/5       IKE/0x63000059  01/24/02  19:00:59.539    206
           Vendor ID payload = 6D761DDC26ACECA1B0ED11FABBB860C4

  Sev=Info/4       IKE/0x63000013  01/24/02  19:00:59.569    207
(SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT
                                                 to 14.36.100.50

  Sev=Info/5       IKE/0x6300002F  01/24/02  19:00:59.569    208
                     Received ISAKMP packet: peer = 14.36.100.50

  Sev=Info/4       IKE/0x63000014  01/24/02  19:00:59.569    209
  RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

   Sev=Info/4       CM/0x63100015  01/24/02  19:00:59.569    210
                                        Launch xAuth application

   Sev=Info/4       CM/0x63100017  01/24/02  19:01:04.236    211
                                      xAuth application returned

  Sev=Info/4       IKE/0x63000013  01/24/02  19:01:04.236    212
      SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

  Sev=Info/5       IKE/0x6300002F  01/24/02  19:01:04.496    213
                     Received ISAKMP packet: peer = 14.36.100.50

  Sev=Info/4       IKE/0x63000014  01/24/02  19:01:04.496    214
  RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

   Sev=Info/4       CM/0x6310000E  01/24/02  19:01:04.496    215
             Established Phase 1 SA.  1 Phase 1 SA in the system

  Sev=Info/4       IKE/0x63000013  01/24/02  19:01:04.506    216
      SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

  Sev=Info/5       IKE/0x6300005D  01/24/02  19:01:04.516    217
                Client sending a firewall request to concentrator

  Sev=Info/5       IKE/0x6300005C  01/24/02  19:01:04.516    218
   =Firewall Policy: Product=Cisco Integrated Client, Capability
                                      .(Centralized Policy Push)

  Sev=Info/4       IKE/0x63000013  01/24/02  19:01:04.516    219
      SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

  Sev=Info/5       IKE/0x6300002F  01/24/02  19:01:04.586    220
                     Received ISAKMP packet: peer = 14.36.100.50

  Sev=Info/4       IKE/0x63000014  01/24/02  19:01:04.586    221
  RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

  Sev=Info/5       IKE/0x63000010  01/24/02  19:01:04.586    222
            , :MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS
                                                 value = 10.1.2.1

  Sev=Info/5       IKE/0x63000010  01/24/02  19:01:04.586    223
             , :(MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1
```

```
                                                    value = 10.1.1.2

    Sev=Info/5       IKE/0x63000010  01/24/02  19:01:04.586    224
   (MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1) (a.k.a. WINS
                                                value = 10.1.1.2 , :

    Sev=Info/5       IKE/0x6300000E  01/24/02  19:01:04.586    225
            , :MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN
                                                  value = cisco.com

     Sev=Info/4       CM/0x63100019  01/24/02  19:01:04.586    226
                                           Mode Config data received

    Sev=Info/5       IKE/0x63000055  01/24/02  19:01:04.606    227
   ,Received a key request from Driver for IP address 14.36.100.50
                                                GW IP = 14.36.100.50

    Sev=Info/4       IKE/0x63000013  01/24/02  19:01:04.606    228
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 14.36.100.50

    Sev=Info/5       IKE/0x63000055  01/24/02  19:01:04.606    229
   ,Received a key request from Driver for IP address 10.10.10.255
                                                GW IP = 14.36.100.50

    Sev=Info/4       IKE/0x63000013  01/24/02  19:01:04.606    230
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 14.36.100.50

  Sev=Info/4       IPSEC/0x63700014  01/24/02  19:01:04.786    231
                                                   Deleted all keys

    Sev=Info/5       IKE/0x6300002F  01/24/02  19:01:05.948    232
                       Received ISAKMP packet: peer = 14.36.100.50

    Sev=Info/4       IKE/0x63000014  01/24/02  19:01:05.948    233
              ,RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID
                     NOTIFY:STATUS_RESP_LIFETIME) from 14.36.100.50

    Sev=Info/5       IKE/0x63000044  01/24/02  19:01:05.948    234
              RESPONDER-LIFETIME notify has value of 28800 seconds

    Sev=Info/5       IKE/0x63000045  01/24/02  19:01:05.948    235
                 RESPONDER-LIFETIME notify has value of 4608000 kb

    Sev=Info/4       IKE/0x63000013  01/24/02  19:01:05.948    236
                 SENDING >>> ISAKMP OAK QM *(HASH) to 14.36.100.50

    Sev=Info/5       IKE/0x63000058  01/24/02  19:01:05.948    237
          = Loading IPsec SA (Message ID = 0x5B090EB1 OUTBOUND SPI
                                (0xF39C2217 INBOUND SPI = 0x72FEDC99

    Sev=Info/5       IKE/0x63000025  01/24/02  19:01:05.948    238
                                   Loaded OUTBOUND ESP SPI: 0xF39C2217

    Sev=Info/5       IKE/0x63000026  01/24/02  19:01:05.948    239
                                    Loaded INBOUND ESP SPI: 0x72FEDC99

     Sev=Info/4       CM/0x6310001A  01/24/02  19:01:05.948    240
                                     One secure connection established

 Sev=Info/6       DIALER/0x63300003  01/24/02  19:01:05.988    241
                                           .Connection established

 Sev=Info/6       DIALER/0x63300008  01/24/02  19:01:06.078    242
              MAPI32 Information - Outlook not default mail client
```

```
  Sev=Info/5       IKE/0x6300002F  01/24/02  19:01:06.118    243
                     Received ISAKMP packet: peer = 14.36.100.50

  Sev=Info/4       IKE/0x63000014  01/24/02  19:01:06.118    244
           ,RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID
                 NOTIFY:STATUS_RESP_LIFETIME) from 14.36.100.50

  Sev=Info/5       IKE/0x63000044  01/24/02  19:01:06.118    245
           RESPONDER-LIFETIME notify has value of 28800 seconds

  Sev=Info/5       IKE/0x63000045  01/24/02  19:01:06.118    246
              RESPONDER-LIFETIME notify has value of 4608000 kb

  Sev=Info/4       IKE/0x63000013  01/24/02  19:01:06.118    247
              SENDING >>> ISAKMP OAK QM *(HASH) to 14.36.100.50

  Sev=Info/5       IKE/0x63000058  01/24/02  19:01:06.118    248
        = Loading IPsec SA (Message ID = 0xCFE65CEB OUTBOUND SPI
                           (0x6AC28ED0 INBOUND SPI = 0x0A5AD786

  Sev=Info/5       IKE/0x63000025  01/24/02  19:01:06.118    249
                             Loaded OUTBOUND ESP SPI: 0x6AC28ED0

  Sev=Info/5       IKE/0x63000026  01/24/02  19:01:06.118    250
                              Loaded INBOUND ESP SPI: 0x0A5AD786

   Sev=Info/4       CM/0x63100022  01/24/02  19:01:06.118    251
                              .Additional Phase 2 SA established

Sev=Info/4       IPSEC/0x63700010  01/24/02  19:01:07.020    252
                                   Created a new key structure

Sev=Info/4       IPSEC/0x6370000F  01/24/02  19:01:07.020    253
                     Added key with SPI=0x17229cf3 into key list

Sev=Info/4       IPSEC/0x63700010  01/24/02  19:01:07.020    254
                                   Created a new key structure

Sev=Info/4       IPSEC/0x6370000F  01/24/02  19:01:07.020    255
                     Added key with SPI=0x99dcfe72 into key list

Sev=Info/4       IPSEC/0x63700010  01/24/02  19:01:07.020    256
                                   Created a new key structure

Sev=Info/4       IPSEC/0x6370000F  01/24/02  19:01:07.020    257
                     Added key with SPI=0xd08ec26a into key list

Sev=Info/4       IPSEC/0x63700010  01/24/02  19:01:07.020    258
                                   Created a new key structure

Sev=Info/4       IPSEC/0x6370000F  01/24/02  19:01:07.020    259
                     Added key with SPI=0x86d75a0a into key list

  Sev=Info/6       IKE/0x6300003D  01/24/02  19:01:15.032    260
           Sending DPD request to 14.36.100.50, seq# = 152233542

  Sev=Info/4       IKE/0x63000013  01/24/02  19:01:15.032    261
         (SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST
                                                 to 14.36.100.50

  Sev=Info/5       IKE/0x6300002F  01/24/02  19:01:15.032    262
                     Received ISAKMP packet: peer = 14.36.100.50
```

```
Sev=Info/4       IKE/0x63000014  01/24/02  19:01:15.032    263
         (RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:DPD_ACK
                                                 from 14.36.100.50

Sev=Info/5       IKE/0x6300003F  01/24/02  19:01:15.032    264
,Received DPD ACK from 14.36.100.50, seq# received = 152233542
                                                 seq# expected = 152233542
```

معلومات ذات صلة

- صفحة دعم PIX
- مراجع أوامر PIX
- صفحة دعم RADIUS
- صفحة دعم مركز Cisco VPN 3000 Series
- صفحة دعم عميل Cisco VPN 3000 Series
- مفاوضة IPsec/صفحة دعم بروتوكول IKE
- طلبات التعليقات (RFCs)
- الدعم الفني - 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).