تكوين IPSec بين موجه Cisco IOS وعميل Cisco VPN 4.x ل Windows الذي يستخدم RADIUS للمصادقة المستخدم

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين اتصال بين موجه وعميل VPN 4.x من Cisco باستخدام خدمة مصادقة طلب اتصال المستخدم البعيد (RADIUS) لمصادقة المستخدم. برنامج IOS® الإصدارات T(8)12.2 من Cisco واتصالات الدعم الأحدث من Cisco VPN Client 4.x. يستخدم عملاء VPN 3.x و x.4 سياسة مجموعة (DH) Diffie Hellman رقم 2. يتيح الأمر **isakmp policy # group 2** لعملاء VPN إمكانية الاتصال.

يوضح هذا المستند المصادقة على خادم RADIUS والتخويل (مثل تعيين خدمة تسمية إنترنت في Windows (WINS)) وخدمة تسمية المجال (DNS) محليا بواسطة الموجه. إذا كنت مهتما بالقيام بكل من المصادقة والتفويض من خلال خادم RADIUS، فارجع إلى تكوين IPSec بين موجه Cisco IOS وعميل Cisco VPN الإصدار x.4 ل Windows الذي يستخدم RADIUS.

ملاحظة: تتوفر الآن محاسبة IPSec VPN. راجع محاسبة IPSec VPN للحصول على مزيد من المعلومات وعينة التكوينات.

ارجع إلى نفق IPsec بين موجه IOS وزبون Cisco VPN 4.x ل Windows مع مثال تكوين مصادقة المستخدم TACACS+ للحصول على مزيد من المعلومات حول السيناريو الذي تحدث فيه مصادقة المستخدم خارجيا مع

بروتوكول TACACS+.

ارجع إلى تكوين عميل Cisco VPN الإصدار x.3 ل Windows إلى IOS باستخدام المصادقة الموسعة المحلية للحصول على مزيد من المعلومات حول السيناريو الذي تحدث فيه مصادقة المستخدم محليا في موجه Cisco IOS.

ارجع إلى مثال تكوين مصادقة PIX/ASA 7.x و Cisco VPN Client 4.x ل Windows مع Microsoft Windows 2003 IAS RADIUS للحصول على معلومات حول كيفية إعداد اتصال VPN للوصول عن بعد بين عميل Cisco VPN 4.x) ل Windows) وجهاز الأمان PIX 500 Series 7.x باستخدام خادم RADIUS لخدمة مصادقة الإنترنت (IAS) في Microsoft Windows 2003.

ارجع إلى IPSec - PIX إلى البطاقة البرية لعميل VPN، والتكوين المشترك مسبقا، والوضع مع المصادقة الموسعة للحصول على معلومات حول كيفية توصيل عميل VPN بجدار حماية PIX باستخدام البطاقات البدل، و mode-config، وأمر **sysopt connection allowed-ip**، والمصادقة الموسعة (Xauth).

ارجع إلى IPsec بين مركز VPN 3000 وزبون VPN 4.x ل Windows باستخدام RADIUS لمصادقة المستخدم ومثال تكوين المحاسبة للحصول على معلومات حول كيفية إنشاء نفق IPSec بين مركز Cisco VPN 3000 وزبون Cisco VPN 4.x ل Windows باستخدام RADIUS لمصادقة المستخدم ومحاسبته.

المتطلبات الأساسية

المتطلبات

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

- مجموعة من العناوين التي سيتم تعيينها ل IPSec
- مجموعة تسمى "3000 عميل" بكلمة مرور من "Cisco123"
- مصادقة المستخدم على خادم RADIUS

المكونات المستخدمة

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

- موجه 2621XM يعمل ببرنامج Cisco IOS Software، الإصدار T2(15)12.2
- مصدر المحتوى الإضافي الآمن من Cisco لنظام التشغيل Windows 2000 الإصدار 4.2 (يجب أن يعمل أي خادم RADIUS)
- عميل شبكة VPN من Cisco لنظام التشغيل Windows الإصدار 4.8 (يجب أن يعمل أي عميل لشبكة VPN الإصدار x.4 والإصدارات الأحدث)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

هذا إنتاج من **العرض صيغة** أمر على المسحاج تخديد:

```
vpn2621#show version
Cisco Internetwork Operating System Software
(IOS (tm) C2600 Software (C2600-IK9S-M), Version 12.2(15)T2,  RELEASE SOFTWARE (fc2
TAC Support: http://www.cisco.com/tac
.Copyright (c) 1986-2003 by cisco Systems, Inc
Compiled Thu 01-May-03 10:39 by nmasa
Image text-base: 0x80008098, data-base: 0x81BBB0BC
```

```
(ROM: System Bootstrap, Version 12.2(7r) [cmong 7r], RELEASE SOFTWARE (fc1

vpn2621 uptime is 1 hour, 34 minutes
System returned to ROM by reload
"System image file is "flash:c2600-ik9s-mz.122-15.T2.bin


This product contains cryptographic features and is subject to United
 States and local country laws governing import, export, transfer and
        use. Delivery of Cisco cryptographic products does not imply
.third-party authority to import, export, distribute or use encryption
     Importers, exporters, distributors and users are responsible for
 compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
   .to comply with U.S. and local laws, return this product immediately

:A summary of U.S. laws governing Cisco cryptographic products may be found at
                        http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
                                                        .export@cisco.com

.cisco 2621XM (MPC860P) processor (revision 0x100) with 125952K/5120K bytes of memory
                                        (Processor board ID JAD064503FK (64188517
                                            M860 processor: part number 5, mask 2
                                                    .Bridging software
                                                .X.25 software, Version 3.0.0
                                           (FastEthernet/IEEE 802.3 interface(s 2
                                        (Serial(sync/async) network interface(s 2
                                                    (terminal line(s 1
                                        (Virtual Private Network (VPN) Module(s 1
                                                    (cisco content engine(s 1
                                     .32K bytes of non-volatile configuration memory
                                  (32768K bytes of processor board System flash (Read/Write

                                                Configuration register is 0x2102
```

الاصطلاحات

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

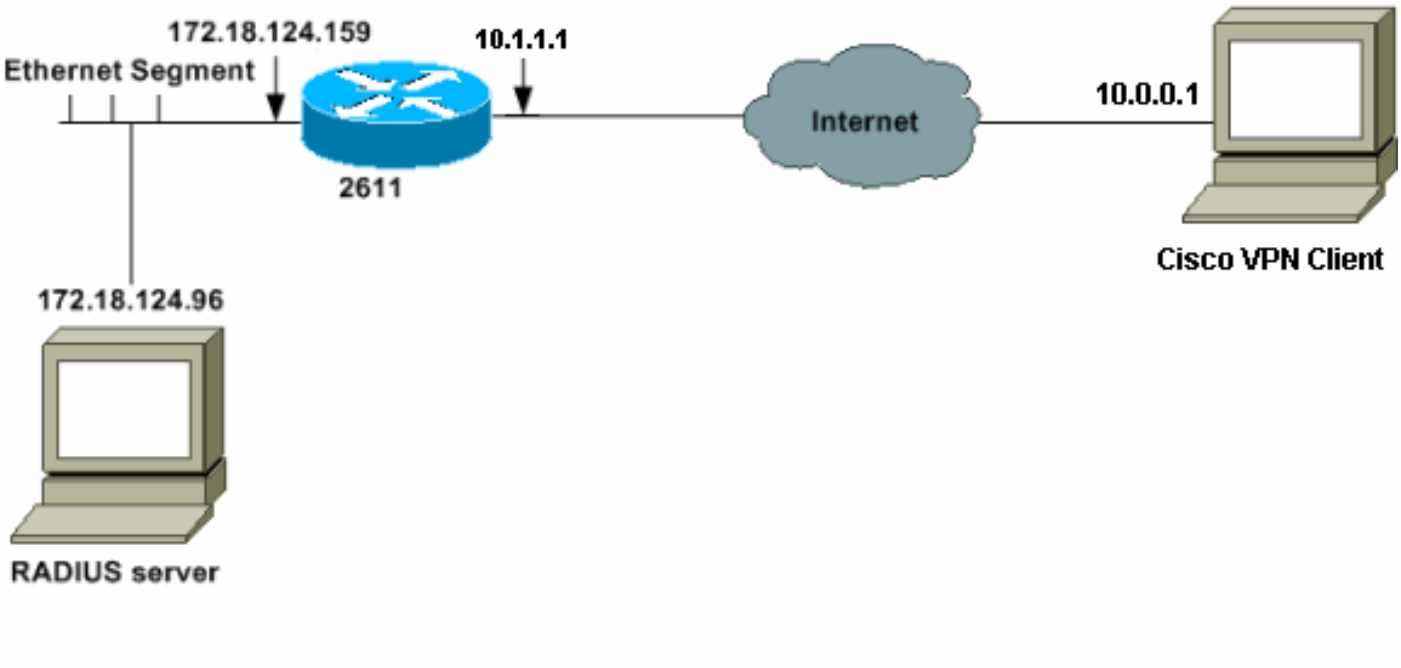
التكوين

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

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



تكوين الموجه 2621XM

الموجه 2621XM
Enable authentication, authorization and accounting ---! *(AAA) !--- for user authentication and group* *authorization.* **aaa new-model** ! *In order to enable extended authentication (Xauth) ---!* *for user authentication, !--- enable the* **aaa** **authentication** commands. !--- "Group radius local" specifies RADIUS user authentication !--- to be used by default and to use local database if RADIUS server is .not reachable **aaa authentication login userauthen group radius local** *In order to enable group authorization, !--- enable ---!* .*the* **aaa authorization** commands **aaa authorization network groupauthor local** *Create an Internet Security Association and !--- ---!* *Key Management Protocol (ISAKMP) policy for Phase 1* *negotiations.* **crypto isakmp policy 3** **encr 3des** **authentication pre-share** **group 2** ! *Create a group that will be used to specify the !-- ---!* *- Windows Internet Naming Service (WINS) and Domain* *Naming Service (DNS) server !--- addresses to the* *client, along with the pre-shared key for* *authentication.* **crypto isakmp client configuration group** **3000client** **key cisco123** **dns 10.1.1.10** **wins 10.1.1.20**

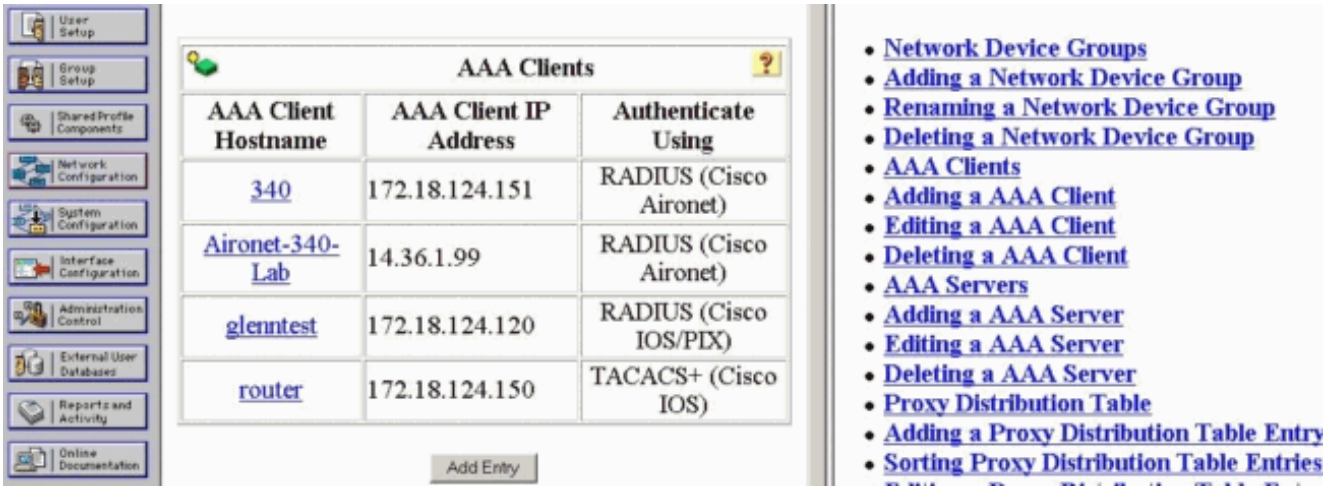
```
domain cisco.com
pool ippool
!
Create the Phase 2 policy for actual data ---!
encryption. crypto ipsec transform-set myset esp-3des
esp-sha-hmac
!

Create a dynamic map and !--- apply the transform ---!
set that was created. crypto dynamic-map dynmap 10
set transform-set myset
!
Create the actual crypto map, !--- and apply the ---!
AAA lists that were created earlier. crypto map
clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list
groupauthor
crypto map clientmap client configuration address
respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
Apply the crypto map on the outside interface. ---!
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
half-duplex
crypto map clientmap
interface Ethernet0/1

ip address 172.18.124.159 255.255.255.0
half-duplex
!

Create a pool of addresses to be assigned to the ---!
VPN Clients. ip local pool ippool  10.16.20.1
10.16.20.200
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
ip http server
ip pim bidir-enable
!
!
!
Specify the IP address of the RADIUS server, !--- ---!
along with the RADIUS shared secret key. radius-server
host 172.18.124.96 auth-port 1645 acct-port 1646 key
cisco123
radius-server retransmit 3
```

تكوين خادم RADIUS

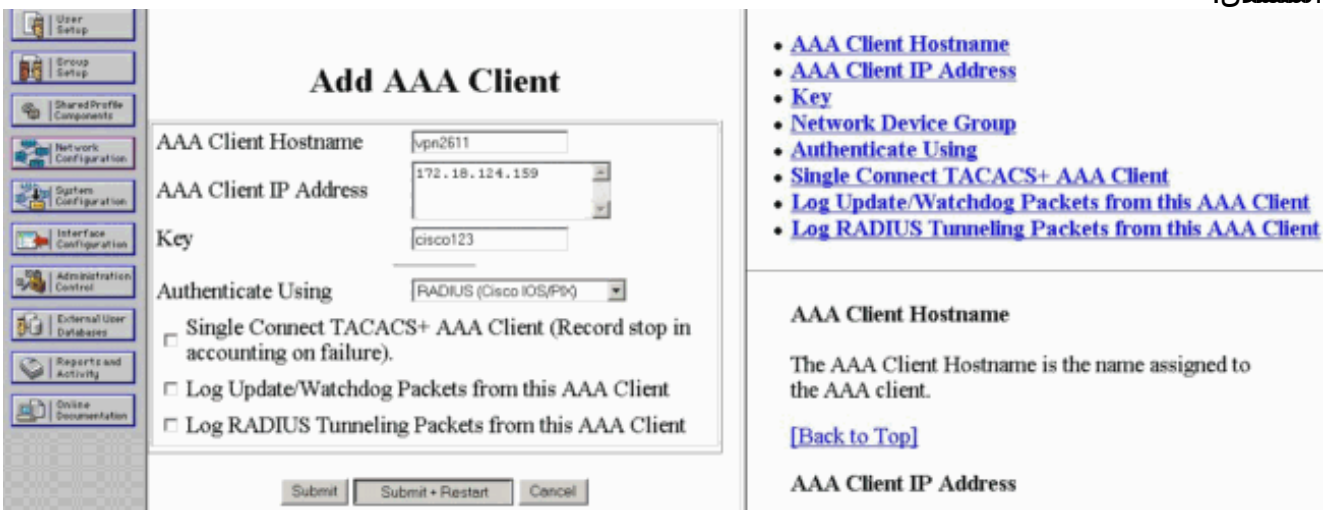
تكوين خادم RADIUS لمصادقة المستخدم

أكمل الخطوات التالية لتكوين خادم RADIUS:

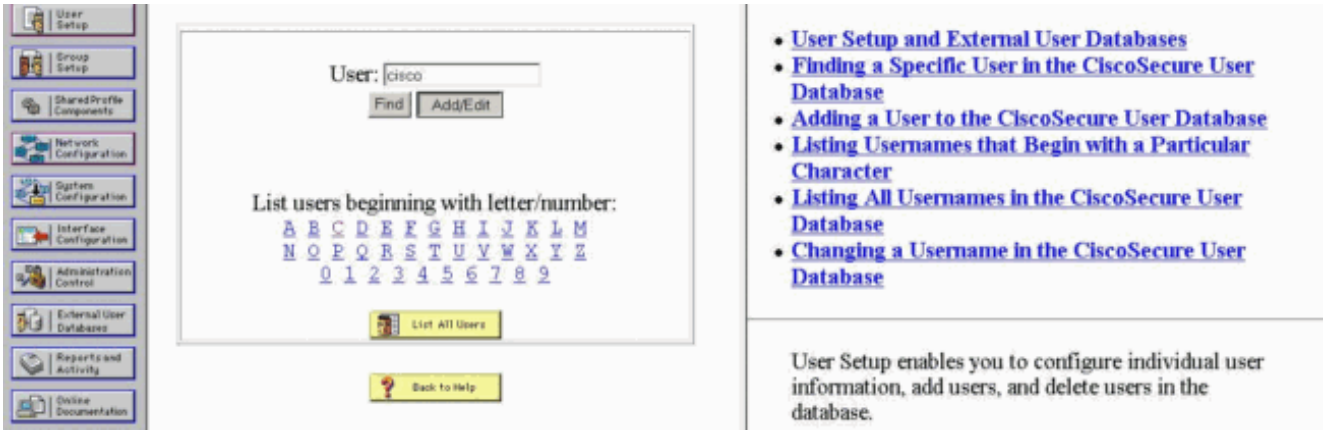
1. قم بإضافة إدخال للموجه في قاعدة بيانات خادم RADIUS.



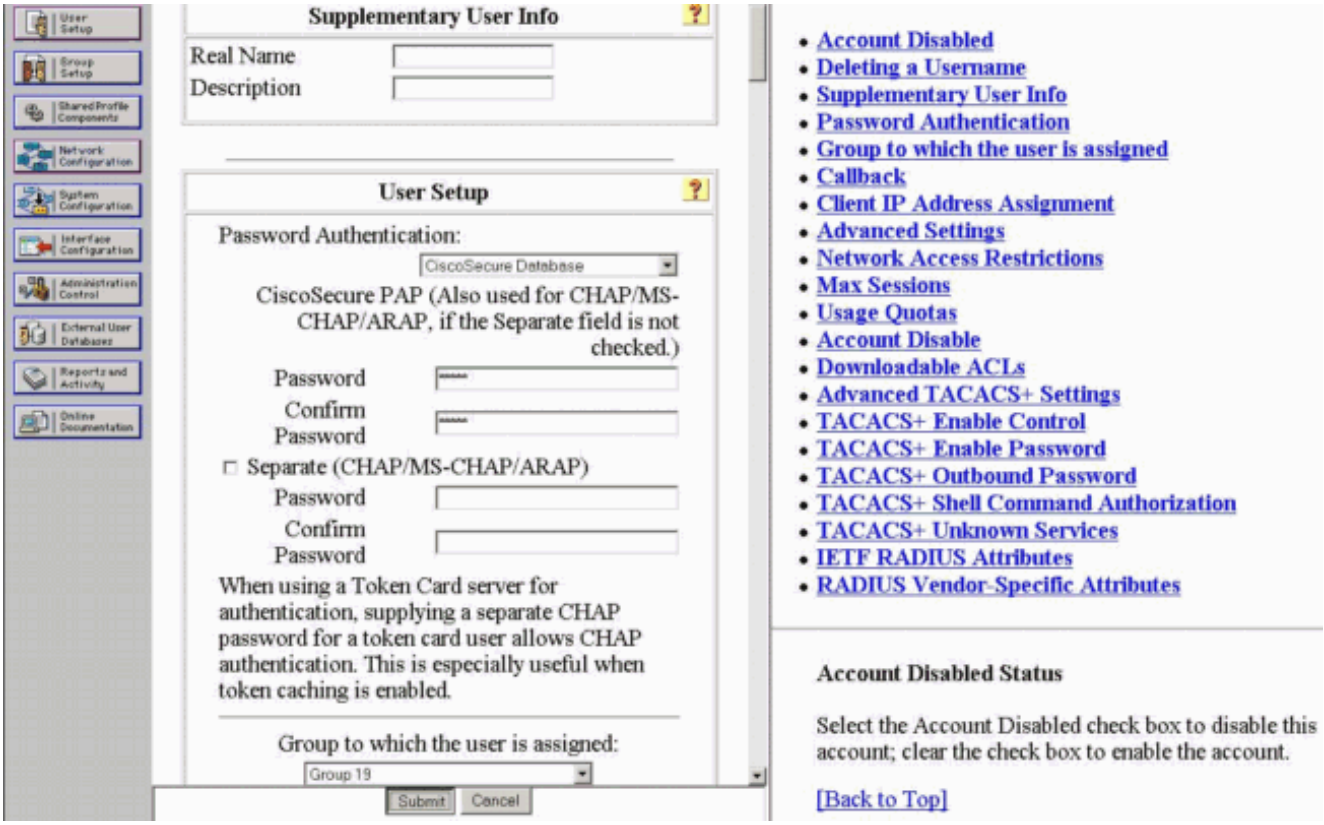
2. حدد عنوان IP الخاص بالموجه "172.18.124.159"، مع المفتاح السري المشترك "Cisco123". أختر **RADIUS** في المصادقة باستخدام المربع المنسدل.



3. أضفت ال username ل ال VPN مستعمل في ال ciscoSecure قاعدة معطيات. في المثال، اسم المستخدم هو Cisco.



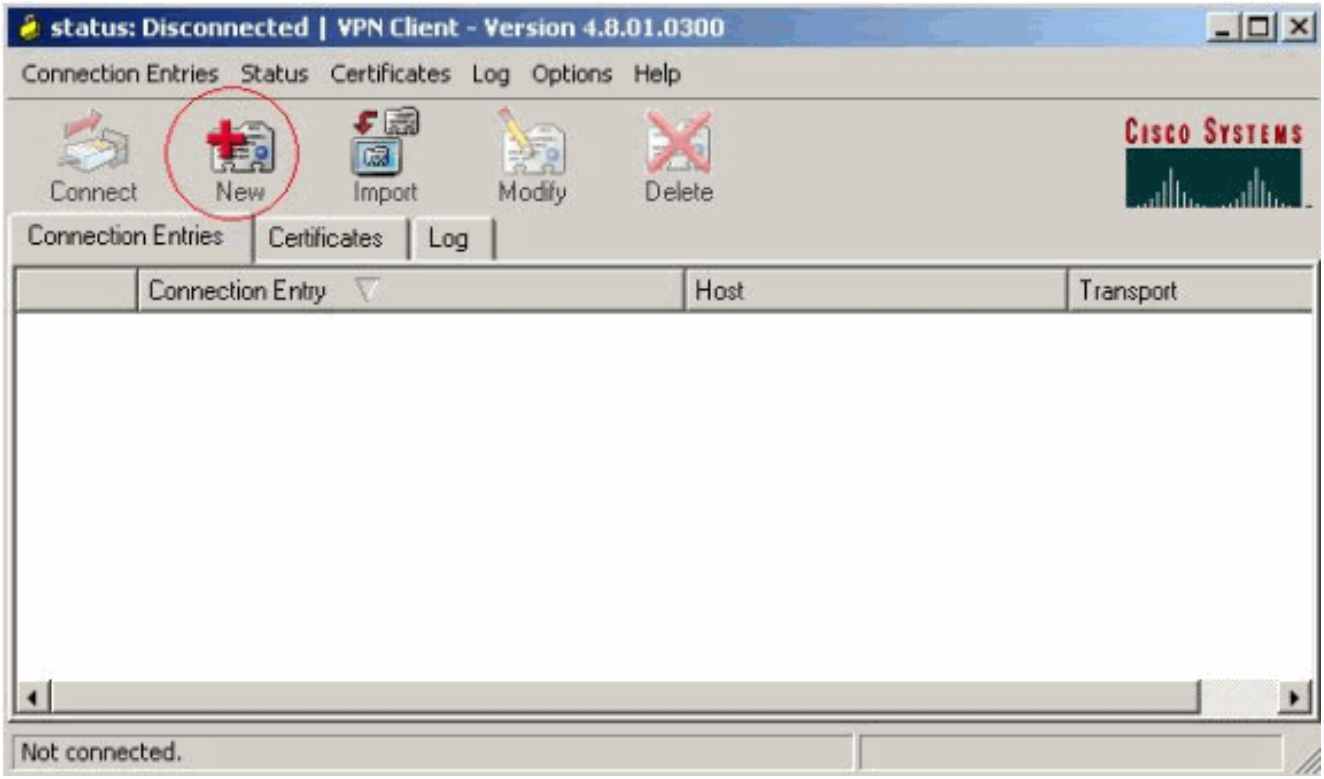
4. على الإطار التالي، عينت الكلمة للمستخدم cisco. في هذا مثال، الكلمة أيضا cisco. يمكنك تعيين حساب المستخدم إلى مجموعة. بمجرد الانتهاء، انقر فوق **إرسال**.



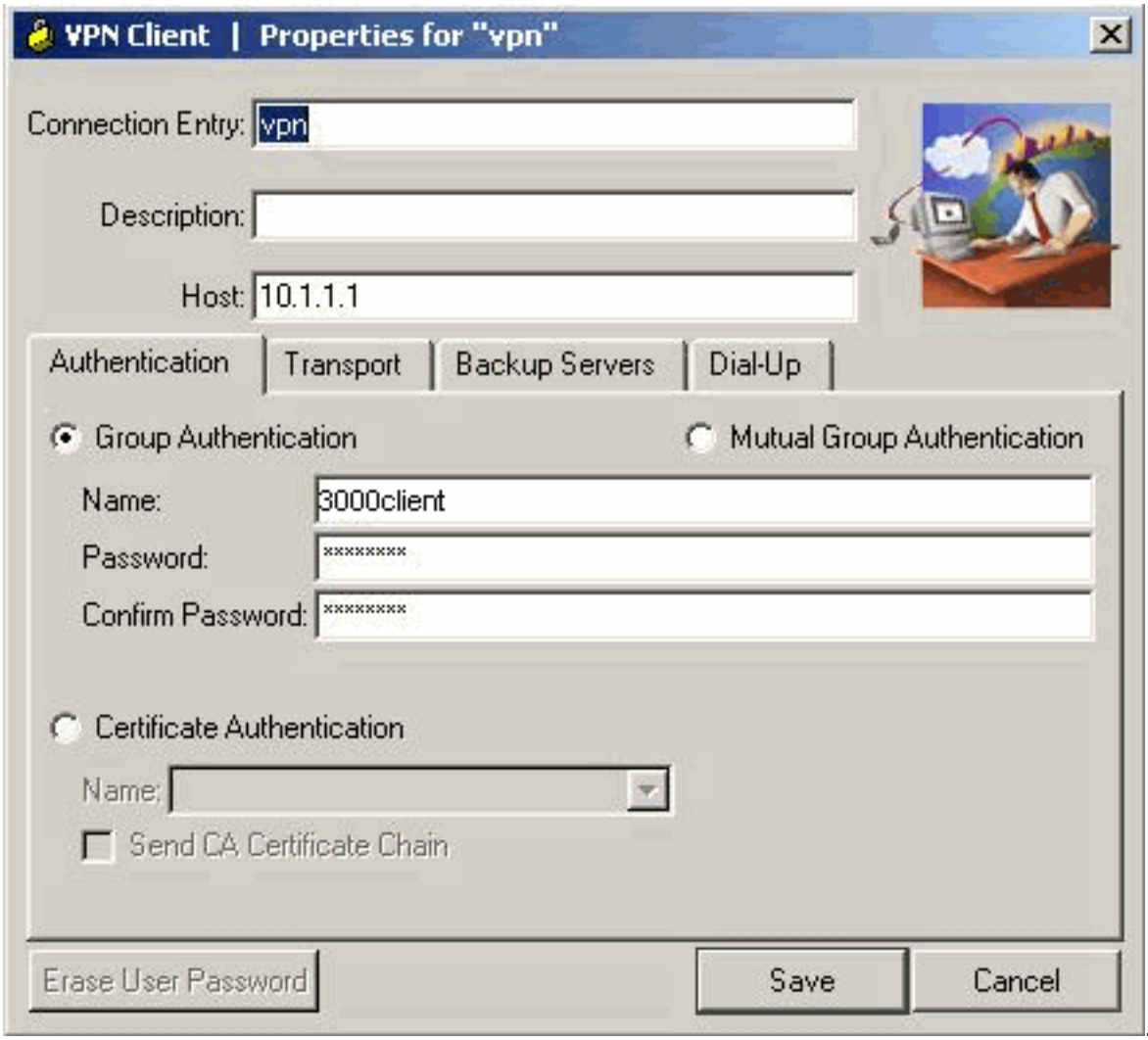
تكوين VPN Client 4.8

أتمت هذا steps in order to شكلت ال VPN زبون 4.8:

1. أخترت **بداية>برنامج>Cisco Systems VPN زبون>VPN زبون**.
2. انقر على **جديد** لتشغيل الإطار "إنشاء اتصال VPN جديد".

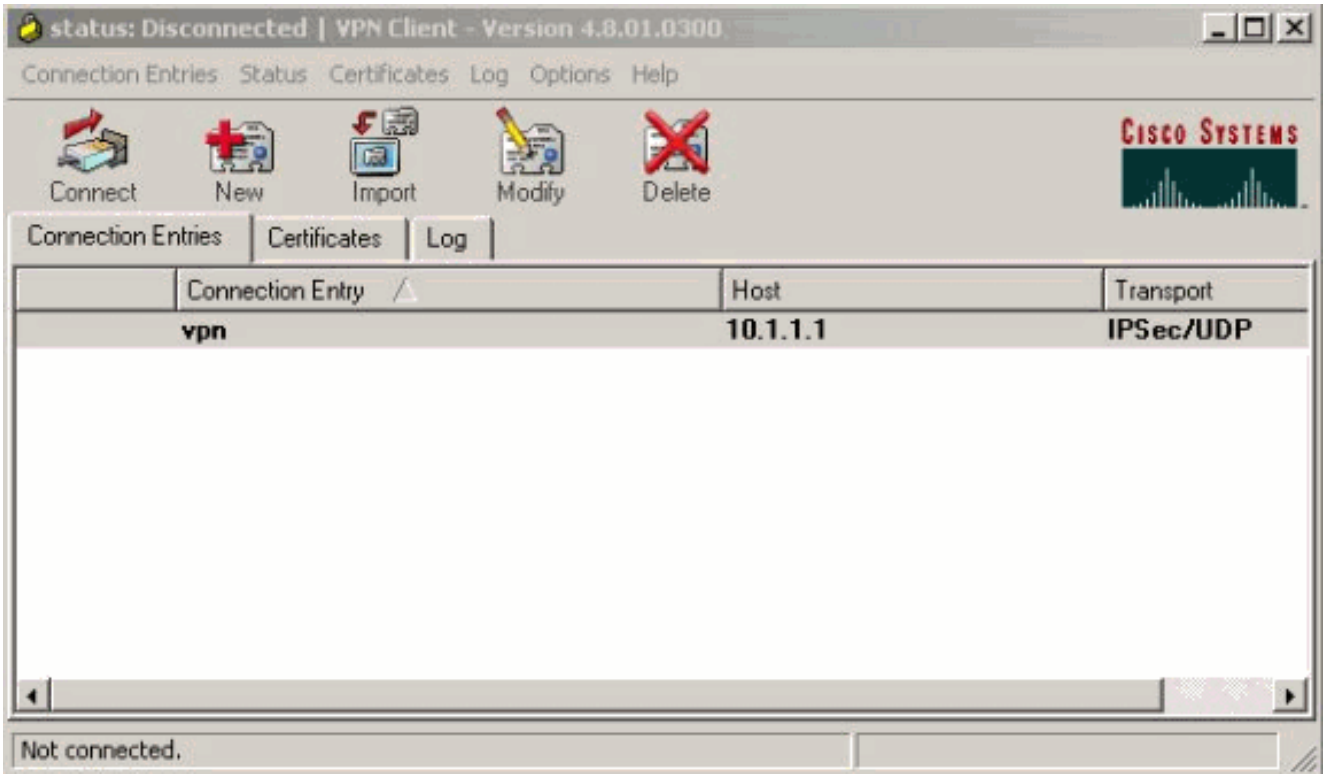


3. أدخل اسم "إدخال الاتصال" مع وصف. أدخل عنوان IP الخارجي للموجه في المربع المضيف. ثم أدخل اسم مجموعة VPN وكلمة المرور وانقر على

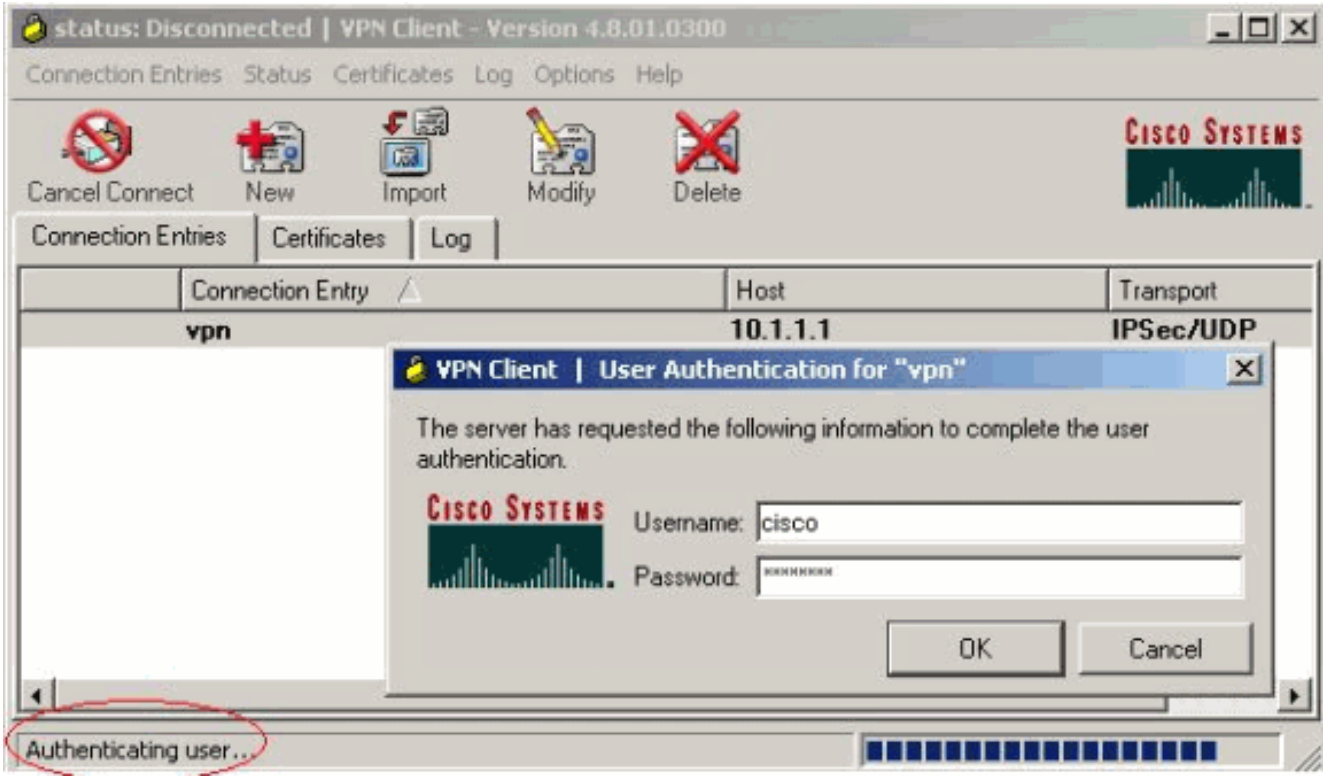


حفظ.

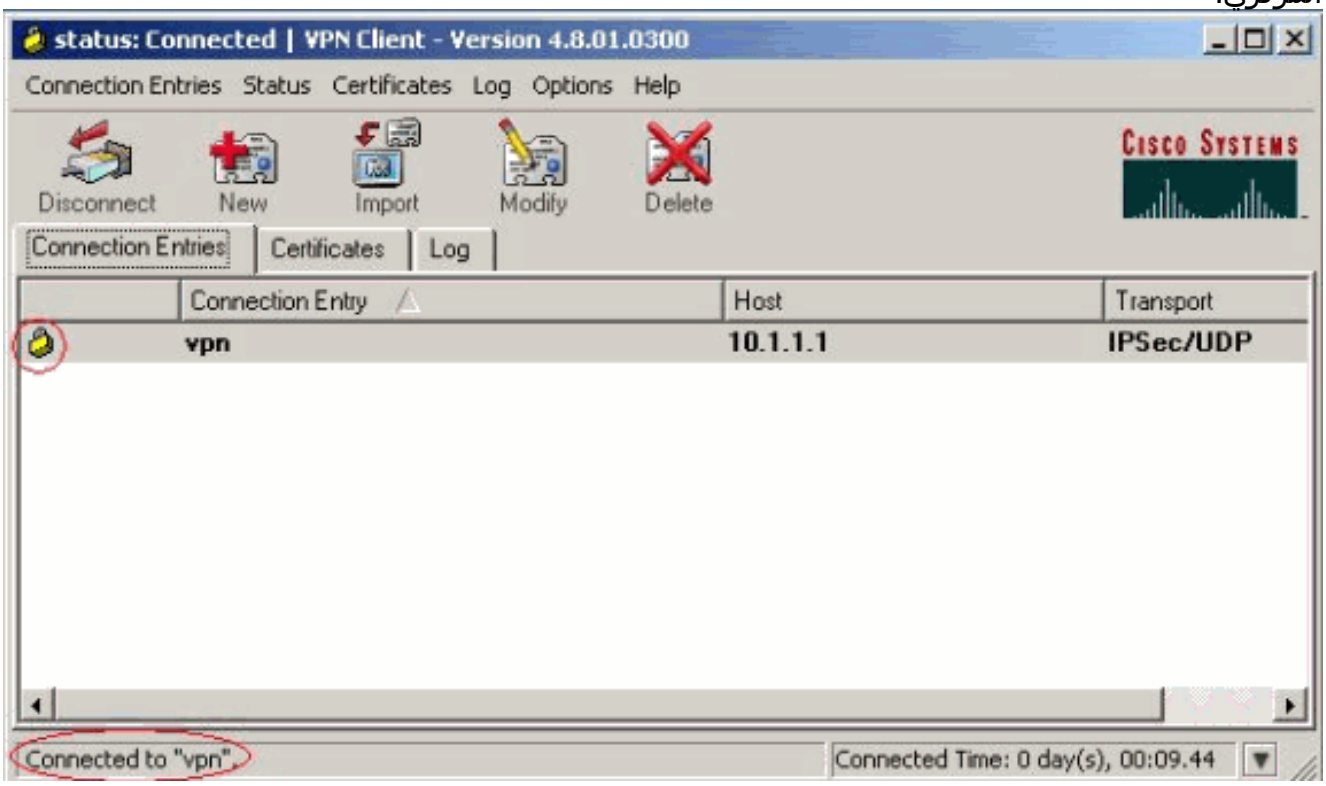
4. انقر على الاتصال الذي تريد إستخدامه وانقر فوق **الاتصال** من الإطار الرئيسي لعميل شبكة VPN.



5. عند المطالبة، أدخل معلومات اسم المستخدم وكلمة المرور للإرسال وانقر فوق **موافق** للاتصال بالشبكة البعيدة.



يتم اتصال عميل شبكة VPN بالموجه في الموقع المركزي.



تمكين الاتصال النفقي للتقسيم

لتمكين الاتصال النفقي المنقسم لاتصالات VPN، تأكد من أن لديك قائمة تحكم في الوصول (ACL) تم تكوينها على الموجه. في هذا المثال، يتم إقران الأمر **access-list 108** بالمجموعة لأغراض إنشاء قنوات اتصال عبر الاتصال النفقي، ويتم تكوين النفق لشبكة 16.14.38/ x.x. تتدفق حركة المرور غير مشفرة إلى الأجهزة غير الموجودة في قائمة التحكم في الوصول 108 (على سبيل المثال، الإنترنت).

```
access-list 108 permit ip 172.18.124.0 0.0.255.255 10.16.20.0 0.0.0.255
```

تطبيق قائمة التحكم في الوصول (ACL) على خصائص المجموعة.

```
crypto isakmp client configuration group 3000client
                                                key cisco123
                                              dns 10.1.1.10
                                             wins 10.1.1.20
                                           domain cisco.com
                                                pool ippool
                                                    acl 108
```

تكوين ميزة RADIUS Server الاحتياطية

عندما يصبح خادم RADIUS الأساسي غير متاح، سيتم تجاوز فشل الموجه إلى خادم RADIUS النشط التالي للنسخ الاحتياطي. سيستمر الموجه في إستخدام خادم RADIUS الثانوي إلى الأبد، حتى إذا كان الخادم الأساسي متوفرا. عادة ما يكون الخادم الرئيسي هو الخادم عالي الأداء والخادم المفضل. إذا لم يكن الخادم الثانوي متوفرا، يمكن إستخدام قاعدة البيانات المحلية للمصادقة باستخدام أمر **تسجيل دخول مصادقة AAA مستخدم** المجموعة radius المحلي.

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** .

هذا مخرج من أوامر **show** ذات الصلة:

```
                                                vpn2621#show crypto isakmp sa
                dst             src             state          conn-id    slot
                                 QM_IDLE           3       0   10.0.0.1  10.1.1.1


                                                vpn2621#show crypto ipsec sa interface: Ethernet0/0
                                                Crypto map tag: clientmap, local addr. 10.1.1.1

                  (local  ident (addr/mask/prot/port): (10.1.1.1/255.255.255.255/0/0
                (remote ident (addr/mask/prot/port): (10.16.20.2/255.255.255.255/0/0
                                                        current_peer: 10.0.0.1
                                                            {}=PERMIT, flags
                                                  pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5#
                                                  pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5#
                                                        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.: 10.1.1.1, remote crypto endpt.: 10.0.0.1
                                                        path mtu 1500, media mtu 1500
                                                      current outbound spi: 77AFCCFA

                                                                    :inbound esp sas
                                                             (spi: 0xC7AC22AB(3349947051
                                                  , transform: esp-3des esp-sha-hmac
```

{ ,in use settings ={Tunnel
slot: 0, conn id: 2000, flow_id: 1, crypto map: clientmap
(sa timing: remaining key lifetime (k/sec): (4608000/3444
IV size: 8 bytes
replay detection support: Y

:inbound ah sas

:inbound pcp sas

:outbound esp sas
(spi: 0x77AFCCFA(2008009978
, transform: esp-3des esp-sha-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 2001, flow_id: 2, crypto map: clientmap
(sa timing: remaining key lifetime (k/sec): (4608000/3444
IV size: 8 bytes
replay detection support: Y

:outbound ah sas

:outbound pcp sas

(local ident (addr/mask/prot/port): (172.18.124.0/255.255.255.0/0/0
(remote ident (addr/mask/prot/port): (10.16.20.2/255.255.255.255/0/0
current_peer: 10.0.0.1
{}=PERMIT, flags
pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4#
pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6#
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.: 10.1.1.1, remote crypto endpt.: 10.0.0.1
path mtu 1500, media mtu 1500
current outbound spi: 2EE5BF09

:inbound esp sas
(spi: 0x3565451F(895829279
, transform: esp-3des esp-sha-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 2002, flow_id: 3, crypto map: clientmap
(sa timing: remaining key lifetime (k/sec): (4607999/3469
IV size: 8 bytes
replay detection support: Y

:inbound ah sas

:inbound pcp sas

:outbound esp sas
(spi: 0x2EE5BF09(786808585
, transform: esp-3des esp-sha-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 2003, flow_id: 4, crypto map: clientmap
(sa timing: remaining key lifetime (k/sec): (4607999/3469
IV size: 8 bytes
replay detection support: Y

:outbound ah sas

:outbound pcp sas

```
vpn2621#show crypto engine connections active

ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
      Ethernet0/0     10.1.1.1  set    HMAC_SHA+3DES_56_C        0        0 3
      Ethernet0/0     10.1.1.1  set    HMAC_SHA+3DES_56_C        0        5 2000
      Ethernet0/0     10.1.1.1  set    HMAC_SHA+3DES_56_C        5        0 2001
      Ethernet0/0     10.1.1.1  set    HMAC_SHA+3DES_56_C        0        6 2002
      Ethernet0/0     10.1.1.1  set    HMAC_SHA+3DES_56_C        4        0 2003

vpn2621#show crypto engine accelerator statistic
                      Virtual Private Network (VPN) Module in aim slot : 0
                    Statistics for Hardware VPN Module since the last clear
                                                 of counters 5570 seconds ago
              packets in                         14 packets out 14
     packet overruns                   0 output packets dropped 0
         packets decompressed              0 packets compressed 0
       compressed bytes in               0 uncompressed bytes in 0
        decompressed bytes out            0 compressed bytes out 0
   packets bypass compression        0 packets abort compression 0
    packets fail decompression        0 packets fail compression 0
           packets decrypted                7 packets encrypted 7
             bytes decrypted                532 bytes encrypted 532
         bytes before decrypt          19200 bytes after encrypt 784
                paks/sec in                      0 paks/sec out 0
         Kbits/sec decrypted               0 Kbits/sec encrypted 0
                                                        :Last 5 minutes
                  packets in                       14 packets out 14
            packets decrypted                7 packets encrypted 7
              bytes decrypted                420 bytes encrypted 532
          bytes before decrypt             672 bytes after encrypt 784
                 paks/sec in                       0 paks/sec out 0
          Kbits/sec decrypted               0 Kbits/sec encrypted 0
rx_no_endp:          0  rx_hi_discards:       0    fw_failure:             0
invalid_sa:          0  invalid_flow:         0    cgx_errors              0
fw_qs_filled:        0  fw_resource_lock:     0    lotx_full_err:          0
null_ip_error:       0  pad_size_error:       0    out_bound_dh_acc:       0
esp_auth_fail:       0  ah_auth_failure:      0    crypto_pad_error:       0
ah_prot_absent:      0  ah_seq_failure:       0    ah_spi_failure:         0
esp_prot_absent:     0  esp_seq_fail:         0    esp_spi_failure:        0
obound_sa_acc:       0  invalid_sa:           0    out_bound_sa_flow:      0
invalid_dh:          0  bad_keygroup:         0    out_of_memory:          0
no_sh_secret:        0  no_skeys:             0    invalid_cmd:            0
dsp_coproc_err:      0  comp_unsupported:     0    pak_too_big:            0
                                                     null packets:        0
                   pak_mp_length_spec_fault:      0 cmd queue errors:      0
                       tx_lo_queue_size_max      0 cmd_unimplemented:      0
                      Interrupts:    439  Immed:      0  HiPri ints:      14
                        LoPri ints:    425  POST Errs:      0 Alerts:      0
                                       Unk Cmds:        0  UnexpCmds:      0
                  cgx_cmd_pending:0   packet_loop_max: 0packet_loop_limit: 0
                                        vpn2621#sh crypto engine configuration

               crypto engine name:  Virtual Private Network (VPN) Module
                                        crypto engine type:  hardware

                                       Product Name:  AIM-VPN/BP
                          Configuration:  0x000109010F00F00784000000
                          0x995FB1441BA279D5BD46CF6C  :
                          0xECE77614C30835CB0A000300  :
```

```
0x00000000000000000000000  :
                  CryptIC Version:  001.000
                  CGX Version:  001.009
                   CGX Reserved:  0x000F
      PCDB info:  0x07F0 0x0084 0x0000
   Serial Number:  0x5F9944B1A21BD57946BD
    0x6CCFE7EC14768C3CB35  :
                  DSP firmware version:  000.010
                  DSP Bootstrap Version:  000.003
                   DSP Bootstrap Info:  0x0000

                     Compression:  Yes
                     DES:  Yes
                     DES:  Yes 3
                      AES CBC:  No
                      AES CNTR:  No
                   Maximum buffer length:  4096
                   Maximum DH index:  0210
                   Maximum SA index:  0420
                   Maximum Flow index:  0840
                   Maximum RSA key size:  0000
                      crypto engine in slot:  0
platform:  VPN hardware accelerator

                        :Crypto Adjacency Counts
                     Lock Count:  0
                     Unlock Count:  0
               crypto lib version:  16.0.0
                ipsec lib version:  2.0.0
```

استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

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

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

- **debug crypto ipSec**—يعرض معلومات تصحيح الأخطاء حول إتصالات IPSec.
- **debug crypto isakmp**— يعرض معلومات تصحيح الأخطاء حول إتصالات IPSec، ويبدي المجموعة الأولى من السمات التي يتم رفضها بسبب عدم التوافق على كلا النهايتين.
- **debug crypto engine**—يعرض معلومات من محرك التشفير.
- **مصادقة AAA** Debug—يعرض معلومات حول مصادقة نظام التحكم في الوصول إلى وحدة التحكم في الوصول إلى المحطة الطرفية (AAA/Terminal Access Controller (+TACACS.
- **تصحيح أخطاء المصادقة والتفويض والمحاسبة (AAA)**—يعرض معلومات حول تفويض AAA/TACACS+.
- **debug radius**—يعرض معلومات حول أستكشاف أخطاء الاتصال وإصلاحها بين خادم RADIUS والموجه.

إخراج تصحيح الأخطاء

يوفر هذا القسم معلومات تصحيح الأخطاء من الموجه الذي يمكنك إستخدامه لاستكشاف أخطاء التكوين وإصلاحها.

سجلات الموجه

```
vpn2621#show debug
:General OS
  AAA Authentication debugging is on
  AAA Authorization debugging is on

  Radius protocol debugging is on
Radius packet protocol debugging is on


:Cryptographic Subsystem
  Crypto ISAKMP debugging is on
  Crypto Engine debugging is on
  Crypto IPSEC debugging is on


vpn2621#
ISAKMP (0:0): received packet from 10.0.0.1 dport 500 sport 500 Global (N) NEW SA*
                ISAKMP: Created a peer struct for 10.0.0.1, peer port 500*
              ISAKMP: Locking peer struct 0x83166B20, IKE refcount 1 for*
                                  crypto_ikmp_config_initialize_sa
                  ISAKMP (0:0): Setting client config settings 82F0F82C*
                ISAKMP (0:0): (Re)Setting client xauth list  and state*
                                 ISAKMP: local port 500, remote port 500*
                             ISAKMP: insert sa successfully sa = 83165694*
                   ISAKMP (0:1): processing SA payload. message ID = 0*
                   ISAKMP (0:1): processing ID payload. message ID = 0*
                     ISAKMP (0:1): peer matches *none* of the profiles*
                             ISAKMP (0:1): processing vendor id payload*
          ISAKMP (0:1): vendor ID seems Unity/DPD but major 215 mismatch*
                                          ISAKMP (0:1): vendor ID is XAUTH*
                             ISAKMP (0:1): processing vendor id payload*
                                           ISAKMP (0:1): vendor ID is DPD*
                             ISAKMP (0:1): processing vendor id payload*
          ISAKMP (0:1): vendor ID seems Unity/DPD but major 123 mismatch*
                                    ISAKMP (0:1): vendor ID is NAT-T v2*
                             ISAKMP (0:1): processing vendor id payload*
          ISAKMP (0:1): vendor ID seems Unity/DPD but major 194 mismatch*
                             ISAKMP (0:1): processing vendor id payload*
                                       ISAKMP (0:1): vendor ID is Unity*
                        ISAKMP (0:1) Authentication by xauth preshared*
        ISAKMP (0:1): Checking ISAKMP transform 1 against priority 3 policy*
                                      ISAKMP:      encryption AES-CBC*
                                           ISAKMP:      hash SHA*
                                        ISAKMP:      default group 2*
                                    ISAKMP:      auth XAUTHInitPreShared*
                                       ISAKMP:      life type in seconds*
                          ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                         ISAKMP:      keylength of 256*
            !ISAKMP (0:1): Encryption algorithm offered does not match policy*
     en/US/docs/net_mgmt/wan_service_administrator/1.1/administrator/guide/getstart.html/
snip/en/US/docs/net_mgmt/wan_service_administrator/1.1/administrator/guide/getstart.html-
     en/US/docs/net_mgmt/wan_service_administrator/1.1/administrator/guide/getstart.html/
     en/US/docs/net_mgmt/wan_service_administrator/1.1/administrator/guide/getstart.html/
```

ISAKMP values are acceptable and then the router continues with the !--- ISAKMP negotiation ---! process.

```
*ISAKMP (0:1): Checking ISAKMP transform 9 against priority 3 policy
                                      ISAKMP:      encryption 3DES-CBC*
                                           ISAKMP:      hash SHA*
                                        ISAKMP:      default group 2*
                                    ISAKMP:      auth XAUTHInitPreShared*
                                       ISAKMP:      life type in seconds*
                          ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B*
```

ISAKMP (0:1): atts are acceptable. Next payload is 3*
CryptoEngine0: generate alg parameter*
(CryptoEngine0: CRYPTO_ISA_DH_CREATE(hw)(ipsec*
CRYPTO_ENGINE: Dh phase 1 status: 0*
ISAKMP (0:1): processing KE payload. message ID = 0*
CryptoEngine0: generate alg parameter*
(CryptoEngine0: CRYPTO_ISA_DH_SHARE_SECRET(hw)(ipsec*
ISAKMP (0:1): processing NONCE payload. message ID = 0*
ISAKMP (0:1): vendor ID is NAT-T v2*
AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-1*
AAA/MEMORY: create_user (0x830E12E8) user='3000client' ruser='NULL' ds0=0*
port='ISAKMP-ID-AUTH' rem_addr='10.0.0.1' authen_type=NONE service=LOGIN
(priv=0 initial_task_id='0', vrf= (id=0
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH*
ISAKMP (0:1): Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT*

'ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): Port='ISAKMP-ID-AUTH*
list='groupauthor' service=NET
'AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(54534875) user='3000client*
ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): send AV service=ike*
ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): send AV protocol=ipsec*
"ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): found list "groupauthor*
ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(54534875): Method=LOCAL*
AAA/AUTHOR (54534875): Post authorization status = PASS_ADD*
ISAKMP: got callback 1*
*
AAA/AUTHOR/IKE: Processing AV service=ike
*
AAA/AUTHOR/IKE: Processing AV protocol=ipsec
*
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
*
AAA/AUTHOR/IKE: Processing AV default-domain*cisco.com
*
AAA/AUTHOR/IKE: Processing AV addr-pool*ippool
*
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
*
AAA/AUTHOR/IKE: Processing AV group-lock*0
*
AAA/AUTHOR/IKE: Processing AV timeout*0
*
AAA/AUTHOR/IKE: Processing AV idletime*0
*
AAA/AUTHOR/IKE: Processing AV inacl*108
*
AAA/AUTHOR/IKE: Processing AV dns-servers*10.1.1.10 0.0.0.0
*
AAA/AUTHOR/IKE: Processing AV wins-servers*10.1.1.20 0.0.0.0
CryptoEngine0: create ISAKMP SKEYID for conn id 1*
(CryptoEngine0: CRYPTO_ISA_SA_CREATE(hw)(ipsec*
ISAKMP (0:1): SKEYID state generated*
ISAKMP (0:1): constructed NAT-T vendor-02 ID*
ISAKMP (0:1): SA is doing pre-shared key authentication plus XAUTH using*
id type ID_IPV4_ADDR
ISAKMP (1): ID payload*
next-payload : 10
type : 1
addr : 10.1.1.1
protocol : 17
port : 0
length : 8
(ISAKMP (1): Toine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec*
ISAKMP (0:1): processing HASH payload. message ID = 0*

CryptoEngine0: generate hmac context for conn id 1*
CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)tal payload length: 12*
CryptoEngine0: generate hmac conte*
ISAKMP (0:1): processing NOTIFY INITIAL_CONTACT protocol 1*
spi 0, message ID = 0, sa = 83165694
,ISAKMP (0:1): Process initial contact*
bring down existing phase 1 and 2 SA's with local 10.1.1.1 remote
remote port 500 10.0.0.1
ISAKMP (0:1): returning IP addr to the address pool*
ISAKMP:received payload type 17*
ISAKMP (0:1): Detected NAT-D payload*
ISAKMP (0:1): recalc my hash for NAT-D*
ISAKMP (0:1): NAT match MINE hash*
ISAKMP:received payload type 17xt for conn id 1*
(CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec*
ISAKMP (0:1): constructed HIS NAT-D*
ISAKMP (0:1): constructed MINE NAT-D*
ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) AG_INIT_EXCH*
ISAKMP (0:1): Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY*
ISAKMP (0:1): Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2*

'AAA/MEMORY: free_user (0x830E12E8) user='3000client' ruser='NULL' port='ISAKMP-ID-AUTH*
(rem_addr='10.0.0.1' authen_type=NONE service=LOGIN priv=0 vrf= (id=0
ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) AG_INIT_EXCH*
CryptoEng*
ISAKMP (0:1): Detected NAT-D payload*
ISAKMP (0:1): recalc his hash for NAT-D*
ISAKMP (0:1): NAT match HIS hash*
ISAKMP (0:1): SA has been authenticated with 10.0.0.1*
CryptoEngine0: clear dh number for conn id 1*
.ISAKMP: Trying to insert a peer 10.0.0.1/500/, and inserted successfully*
ISAKMP (0:1): IKE_DPD is enabled, initializing timers*
ISAKMP: set new node 2011892843 to CONF_XAUTH*
CryptoEngine0: generate hmac context for conn id 1*
(CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec*
...IPSEC(key_engine): got a queue event*
(CryptoEngine0: CRYPTO_ISA_DH_DELETE(hw)(ipsec*
(CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec*
ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) QM_IDLE*
ISAKMP (0:1): purging node 2011892843*
ISAKMP: Sending phase 1 responder lifetime 86400*

ISAKMP (0:1): peer matches *none* of the profiles*
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH*
ISAKMP (0:1): Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE*

ISAKMP (0:1): Need XAUTH*
AAA: parse name=ISAKMP idb type=-1 tty=-1*
'AAA/MEMORY: create_user (0x830DE43C) user='NULL' ruser='NULL' ds0=0 port='ISAKMP*
,'rem_addr='10.0.0.1' authen_type=ASCII service=LOGIN priv=0 initial_task_id='0
(vrf= (id=0
ISAKMP (0:1): Input = IKE_MESG_INTERNAL, **IKE_PHASE1_COMPLETE***
ISAKMP (0:1): Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT*

AAA/AUTHEN/START (992119247): port='ISAKMP' list='userauthen' action=LOGIN service=LOGIN*
AAA/AUTHEN/START (992119247): found list userauthen*
(AAA/AUTHEN/START (992119247): Method=radius (radius*
AAA/AUTHEN(992119247): Status=GETUSER*
ISAKMP: got callback 1*
ISAKMP: set new node -883516238 to CONF_XAUTH*
ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2*
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2*
CryptoEngine0: generate hmac context for conn id 1*
(CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec*

```
                        ISAKMP (0:1): initiating peer config to 10.0.0.1. ID = -883516238*
                                              (CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec*
       ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) CONF_XAUTH*
                               ISAKMP (0:1): Input = IKE_MESG_FROM_AAA, IKE_AAA_START_LOGIN*
ISAKMP (0:1): Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT  New State = IKE_XAUTH_REQ_SENT*

                         ... ISAKMP (0:1): retransmitting phase 2 CONF_XAUTH    -883516238*
                        ISAKMP (0:1): incrementing error counter on sa: retransmit phase 2*
                        ISAKMP (0:1): incrementing error counter on sa: retransmit phase 2*
                                ISAKMP (0:1): retransmitting phase 2 -883516238 CONF_XAUTH*
       ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) CONF_XAUTH*
   ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) CONF_XAUTH*
                                              (CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec*
     ISAKMP (0:1): processing transaction payload from 10.0.0.1. message ID = -883516238*
                                          CryptoEngine0: generate hmac context for conn id 1*
                                               (CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec*
                                                        ISAKMP: Config payload REPLY*
                                          ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2*
                                       ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2*
                                    ISAKMP (0:1): deleting node -883516238 error FALSE reason*
                                        "done with xauth request/reply exchange"
                                     ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_CFG_REPLY*
 ISAKMP (0:1): Old State = IKE_XAUTH_REQ_SENT  New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT*

                                ('(AAA/AUTHEN/CONT (992119247): continue_login (user='(undef*
                                                    AAA/AUTHEN(992119247): Status=GETUSER*
                                                 (AAA/AUTHEN(992119247): Method=radius (radius*
                                                    AAA/AUTHEN(992119247): Status=GETPASS*
                                  ('AAA/AUTHEN/CONT (992119247): continue_login (user='cisco*
                                                    AAA/AUTHEN(992119247): Status=GETPASS*
                                                 (AAA/AUTHEN(992119247): Method=radius (radius*
       RADIUS: Pick NAS IP for u=0x830DE43C tableid=0 cfg_addr=0.0.0.0 best_addr=10.1.1.1*
                                                              RADIUS: ustruct sharecount=2*
                                       Radius: radius_port_info() success=0 radius_nas_port=1*
           RADIUS(00000000): Send Access-Request to 172.18.124.96:1645 id 21645/4, len 72*
                 RADIUS:  authenticator F2 7F ED 86 2B D9 80 1F - 74 D7 8F 90 3B EF F0 D5*
                                        RADIUS:  NAS-IP-Address      [4]   6   10.1.1.1*
                     [RADIUS:  NAS-Port-Type       [61]  6   Async                     [0*
                                         "RADIUS:  User-Name           [1]   9   "cisco*
                                       "RADIUS:  Calling-Station-Id  [31]  13  "10.0.0.1*
                                                *  RADIUS:  User-Password       [2]   18*
                              RADIUS: Retransmit to (172.18.124.96:1645,1646) for id 21645/4*
                  RADIUS: Received from id 21645/4 172.18.124.96:1645, Access-Accept, len 62*
                    RADIUS:  authenticator 97 DF CB C8 74 AC 92 D6 - 3B D8 D9 DC 9E 85 94 35*
                                      RADIUS:  Framed-IP-Address   [8]   6   172.17.8.123*
                                                    RADIUS:  Class               [25]  36*
             [RADIUS:   43 49 53 43 4F 41 43 53 3A 30 30 30 30 31 38 32  [CISCOACS:0000182*
             [RADIUS:   62 2F 61 63 31 32 37 63 39 66 2F 74 6E 65 75 62  [b/ac127c9f/cisco*
                                                                          RADIUS:   65 72*
                              RADIUS: saved authorization data for user 830DE43C at 830DB5FC*
                                                    AAA/AUTHEN(992119247): Status=PASS*
                                                             ISAKMP: got callback 1*
                                         ISAKMP: set new node -1874799558 to CONF_XAUTH*
                                          CryptoEngine0: generate hmac context for conn id 1*
                                               (CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec*
                        ISAKMP (0:1): initiating peer config to 10.0.0.1. ID = -1874799558*
                                              (CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec*
       ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) CONF_XAUTH*
                               ISAKMP (0:1): Input = IKE_MESG_FROM_AAA, IKE_AAA_CONT_LOGIN*
 ISAKMP (0:1): Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT  New State = IKE_XAUTH_SET_SENT*

                 'AAA/MEMORY: free_user (0x830DE43C) user='cisco' ruser='NULL' port='ISAKMP*
                    (rem_addr='10.0.0.1' authen_type=ASCII service=LOGIN priv=0 vrf= (id=0
   ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) CONF_XAUTH*
```

```
                                        (CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec*
ISAKMP (0:1): processing transaction payload from 10.0.0.1. message ID = -1874799558*
                                    CryptoEngine0: generate hmac context for conn id 1*
                                         (CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec*
                                                      ISAKMP: Config payload ACK*
                                               ISAKMP (0:1):        XAUTH ACK Processed*
  "ISAKMP (0:1): deleting node -1874799558 error FALSE reason "done with transaction*
                                  ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK*
           ISAKMP (0:1): Old State = IKE_XAUTH_SET_SENT  New State = IKE_P1_COMPLETE*

                            ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE*
                ISAKMP (0:1): Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE*

  ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE*
                                       ISAKMP: set new node -1474156599 to QM_IDLE*
                                        (CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec*
ISAKMP (0:1): processing transaction payload from 10.0.0.1. message ID = -1474156599*
                                    CryptoEngine0: generate hmac context for conn id 1*
                                         (CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec*
                                                      ISAKMP: Config payload REQUEST*
                                                    :ISAKMP (0:1): checking request*
                                                             ISAKMP:    IP4_ADDRESS*
                                                             ISAKMP:    IP4_NETMASK*
                                                                 ISAKMP:    IP4_DNS*
                                                                ISAKMP:    IP4_NBNS*
                                                            ISAKMP:    ADDRESS_EXPIRY*
                                                         ISAKMP:    APPLICATION_VERSION*
                                                ISAKMP:    UNKNOWN Unknown Attr: 0x7000*
                                                ISAKMP:    UNKNOWN Unknown Attr: 0x7001*
                                                   ISAKMP:    DEFAULT_DOMAIN*
                                                    ISAKMP:    SPLIT_INCLUDE*
                                                ISAKMP:    UNKNOWN Unknown Attr: 0x7003*
                                                ISAKMP:    UNKNOWN Unknown Attr: 0x7007*
                                                ISAKMP:    UNKNOWN Unknown Attr: 0x7008*
                                                ISAKMP:    UNKNOWN Unknown Attr: 0x7009*
                                                ISAKMP:    UNKNOWN Unknown Attr: 0x700A*
                                                ISAKMP:    UNKNOWN Unknown Attr: 0x7005*
                                  AAA: parse name=ISAKMP-GROUP-AUTH idb type=-1 tty=-1*
            AAA/MEMORY: create_user (0x831663A0) user='3000client' ruser='NULL' ds0=0*
          port='ISAKMP-GROUP-AUTH' rem_addr='10.0.0.1' authen_type=NONE service=LOGIN
                                                (priv=0 initial_task_id='0', vrf= (id=0
                               ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST*
  ISAKMP (0:1): Old State = IKE_P1_COMPLETE  New State = IKE_CONFIG_AUTHOR_AAA_AWAIT*

       'ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): Port='ISAKMP-GROUP-AUTH*
                                                       list='groupauthor' service=NET
             'AAA/AUTHOR/CRYPTO AAA: ISAKMP-GROUP-AUTH(3136771130) user='3000client*
           ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): send AV service=ike*
         ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): send AV protocol=ipsec*
       "ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): found list "groupauthor*
                    ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3136771130): Method=LOCAL*
                        AAA/AUTHOR (3136771130): Post authorization status = PASS_ADD*
                                                       ISAKMP: got callback 1*
                                          AAA/AUTHOR/IKE: Processing AV service=ike *
                                        AAA/AUTHOR/IKE: Processing AV protocol=ipsec *
                                                                                    *
                                    AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
                                                                                    *
                                    AAA/AUTHOR/IKE: Processing AV default-domain*cisco.com
                                                                                    *
                                          AAA/AUTHOR/IKE: Processing AV addr-pool*ippool
                                                                                    *
                                          AAA/AUTHOR/IKE: Processing AV key-exchange=ike
                                                                                    *
```

```
                                                AAA/AUTHOR/IKE: Processing AV group-lock*0
                                                                                        *
                                                   AAA/AUTHOR/IKE: Processing AV timeout*0
                                                                                        *
                                                 AAA/AUTHOR/IKE: Processing AV idletime*0
                                                                                        *
                                                   AAA/AUTHOR/IKE: Processing AV inacl*108
                                                                                        *
                                          AAA/AUTHOR/IKE: Processing AV dns-servers*10.1.1.10 0.0.0.0
                                                                                        *
                                         AAA/AUTHOR/IKE: Processing AV wins-servers*10.1.1.20 0.0.0.0
                                                  :ISAKMP (0:1): attributes sent in message*
                                                                 Address: 0.2.0.0        *
                                               ISAKMP (0:1): allocating address 10.16.20.1*
                                               ISAKMP: Sending private address: 10.16.20.1*
                                            ISAKMP: Sending IP4_DNS server address: 10.1.1.10*
                                           ISAKMP: Sending IP4_NBNS server address: 10.1.1.20*
                             ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address: 86388*
          ISAKMP: Sending APPLICATION_VERSION string: Cisco Internetwork Operating System Software*
                (IOS (tm) C2600 Software (C2600-IK9S-M), Version 12.2(15)T2,  RELEASE SOFTWARE (fc2
                                                    TAC Support: http://www.cisco.com/tac
                                             .Copyright (c) 1986-2003 by cisco Systems, Inc
                                                    Compiled Thu 01-May-03 10:39 by nmasa
                                             (ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7000*
                                             (ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7001*
                                  ISAKMP: Sending DEFAULT_DOMAIN default domain name: cisco.com*
                      ISAKMP: Sending split include name 108 network 172.18.124.0 mask 255.255.255.0*
                                                  protocol 0, src port 0, dst port 0

                                             (ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7003*
                                             (ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7007*
                                             (ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7008*
                                             (ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7009*
                                             (ISAKMP (0/1): Unknown Attr: UNKNOWN (0x700A*
                                             (ISAKMP (0/1): Unknown Attr: UNKNOWN (0x7005*
                                          CryptoEngine0: generate hmac context for conn id 1*
                                               (CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec*
                        ISAKMP (0:1): responding to peer config from 10.0.0.1. ID = -1474156599*
                          CryptoEngi*ISAKMP (0:1): deleting node -1474156599 error FALSE reason*
                                              (ne0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec""
                                          ISAKMP (0:1): sending packet to 10.0.0.1 my_por231*
                                 ISAKMP (0:1): processing SA payload. message ID = 2058744231*
                                              ISAKMP (0:1): Checking IPSec proposal 1*
                                                        ISAKMP: transform 1, ESP_AES*
                                                   :ISAKMP:   attributes in transform*
                                                ISAKMP:      authenticator is HMAC-MD5*
                                                          ISAKMP:      encaps is 1*
                                  ISAKMP:      key length is 256t 500 peer_port 500 (R) CONF_ADDR*

                                       ISAKMP (0:1): Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR*
                 ISAKMP (0:1): Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT  New State = IKE_P1_COMPLETE*

'AAA/MEMORY: free_user (0x831663A0) user='3000client' ruser='NULL' port='ISAKMP-GROUP-AUTH*
                              (rem_addr='10.0.0.1' authen_type=NONE service=LOGIN priv=0 vrf= (id=0
                 ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE*
                                              ISAKMP: set new node 2058744231 to QM_IDLE*
                                        (CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec*
                                          CryptoEngine0: generate hmac context for conn id 1*
                                               (CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec*
                                 ISAKMP (0:1): processing HASH payload. message ID = 2058744*
                                                          ISAKMP:      SA life type in seconds*
                                  ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                       CryptoEngine0: validate proposal*
                                                .ISAKMP (0:1): atts are acceptable*
```

```
                                                ISAKMP (0:1): Checking IPSec proposal 1*
                                                   ISAKMP (0:1): transform 1, IPPCP LZS*
                                                     :ISAKMP:   attributes in transform*
                                                              ISAKMP:      encaps is 1*
                                                   ISAKMP:      SA life type in seconds*
                                    ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                    .ISAKMP (0:1): atts are acceptable*
                                           ,IPSEC(validate_proposal_request): proposal part #1*
                                  ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                       ,(local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1
                                    ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                      , protocol= ESP, transform= esp-aes 256 esp-md5-hmac
                                                                ,lifedur= 0s and 0kb
                                         spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
                                          ,IPSEC(validate_proposal_request): proposal part #2*
                                  ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                       ,(local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1
                                    ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                                    , protocol= PCP, transform= comp-lzs
                                                                ,lifedur= 0s and 0kb
                                           spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
                                                  CryptoEngine0: validate proposal request*
                              = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
:IPSEC(validate_transform_proposal): transform proposal not supported for identity*
                                                    { esp-aes 256 esp-md5-hmac comp-lzs}
                                         ISAKMP (0:1): IPSec policy invalidated proposal*
                                                ISAKMP (0:1): Checking IPSec proposal 2*
                                                          ISAKMP: transform 1, ESP_AES*
                                                     :ISAKMP:   attributes in transform*
                                                      ISAKMP:      authenticator is HMAC-SHA*
                                                               ISAKMP:      encaps is 1*
                                                          ISAKMP:      key length is 256*
                                                   ISAKMP:      SA life type in seconds*
                                    ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                      CryptoEngine0: validate proposal*
                                                    .ISAKMP (0:1): atts are acceptable*
                                                ISAKMP (0:1): Checking IPSec proposal 2*
                                                   ISAKMP (0:1): transform 1, IPPCP LZS*
                                                     :ISAKMP:   attributes in transform*
                                                              ISAKMP:      encaps is 1*
                                                   ISAKMP:      SA life type in seconds*
                                    ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                    .ISAKMP (0:1): atts are acceptable*
                                           ,IPSEC(validate_proposal_request): proposal part #1*
                                  ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                       ,(local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1
                                    ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                      , protocol= ESP, transform= esp-aes 256 esp-sha-hmac
                                                                ,lifedur= 0s and 0kb
                                         spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
                                          ,IPSEC(validate_proposal_request): proposal part #2*
                                  ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                       ,(local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1
                                    ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                                    , protocol= PCP, transform= comp-lzs
                                                                ,lifedur= 0s and 0kb
                                           spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
                                                  CryptoEngine0: validate proposal request*
                              = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
:IPSEC(validate_transform_proposal): transform proposal not supported for identity*
                                                    { esp-aes 256 esp-sha-hmac comp-lzs}
                                         ISAKMP (0:1): IPSec policy invalidated proposal*
                                                ISAKMP (0:1): Checking IPSec proposal 3*
                                                          ISAKMP: transform 1, ESP_AES*
```

```
                                                :ISAKMP:   attributes in transform*
                                             ISAKMP:      authenticator is HMAC-MD5*
                                                          ISAKMP:      encaps is 1*
                                                       ISAKMP:      key length is 128*
                                                  ISAKMP:      SA life type in seconds*
                                    ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                        CryptoEngine0: validate proposal*
                                                    .ISAKMP (0:1): atts are acceptable*
                                                ISAKMP (0:1): Checking IPSec proposal 3*
                                                   ISAKMP (0:1): transform 1, IPPCP LZS*
                                                     :ISAKMP:   attributes in transform*
                                                              ISAKMP:      encaps is 1*
                                                  ISAKMP:      SA life type in seconds*
                                    ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                    .ISAKMP (0:1): atts are acceptable*
                                           ,IPSEC(validate_proposal_request): proposal part #1*
                                  ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                       ,(local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1
                                        ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                               , protocol= ESP, transform= esp-aes esp-md5-hmac
                                                                    ,lifedur= 0s and 0kb
                                             spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
                                           ,IPSEC(validate_proposal_request): proposal part #2*
                                  ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                       ,(local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1
                                        ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                                    , protocol= PCP, transform= comp-lzs
                                                                    ,lifedur= 0s and 0kb
                                              spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
                                                        CryptoEngine0: validate proposal request*
                                 = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
:IPSEC(validate_transform_proposal): transform proposal not supported for identity*
                                                     { esp-aes esp-md5-hmac comp-lzs}
                                          ISAKMP (0:1): IPSec policy invalidated proposal*
                                                  ISAKMP (0:1): Checking IPSec proposal 4*
                                                             ISAKMP: transform 1, ESP_AES*
                                                     :ISAKMP:   attributes in transform*
                                                   ISAKMP:      authenticator is HMAC-SHA*
                                                                ISAKMP:      encaps is 1*
                                                             ISAKMP:      key length is 128*
                                                     ISAKMP:      SA life type in seconds*
                                    ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                      CryptoEngine0: validate proposal*
                                                    .ISAKMP (0:1): atts are acceptable*
                                                ISAKMP (0:1): Checking IPSec proposal 4*
                                                   ISAKMP (0:1): transform 1, IPPCP LZS*
                                                     :ISAKMP:   attributes in transform*
                                                              ISAKMP:      encaps is 1*
                                                  ISAKMP:      SA life type in seconds*
                                    ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                    .ISAKMP (0:1): atts are acceptable*
                                           ,IPSEC(validate_proposal_request): proposal part #1*
                                  ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                       ,(local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1
                                        ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                               , protocol= ESP, transform= esp-aes esp-sha-hmac
                                                                    ,lifedur= 0s and 0kb
                                             spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
                                           ,IPSEC(validate_proposal_request): proposal part #2*
                                  ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                       ,(local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1
                                        ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                                    , protocol= PCP, transform= comp-lzs
                                                                    ,lifedur= 0s and 0kb
```

```
                                    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
                                                CryptoEngine0: validate proposal request*
                          = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
:IPSEC(validate_transform_proposal): transform proposal not supported for identity*
                                                  { esp-aes esp-sha-hmac comp-lzs}
                                        ISAKMP (0:1): IPSec policy invalidated proposal*
                                                ISAKMP (0:1): Checking IPSec proposal 5*
                                                           ISAKMP: transform 1, ESP_AES*
                                                     :ISAKMP:   attributes in transform*
                                                 ISAKMP:      authenticator is HMAC-MD5*
                                                               ISAKMP:      encaps is 1*
                                                          ISAKMP:      key length is 256*
                                                    ISAKMP:      SA life type in seconds*
                               ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                       CryptoEngine0: validate proposal*
                                                     .ISAKMP (0:1): atts are acceptable*
                                            ,IPSEC(validate_proposal_request): proposal part #1*
                                 ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                      ,(local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1
                                  ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                    , protocol= ESP, transform= esp-aes 256 esp-md5-hmac
                                                                ,lifedur= 0s and 0kb
                                       spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
                                                CryptoEngine0: validate proposal request*
                          = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
:IPSEC(validate_transform_proposal): transform proposal not supported for identity*
                                                  { esp-aes 256 esp-md5-hmac}
                                        ISAKMP (0:1): IPSec policy invalidated proposal*
                                                ISAKMP (0:1): Checking IPSec proposal 6*
                                                           ISAKMP: transform 1, ESP_AES*
                                                     :ISAKMP:   attributes in transform*
                                                 ISAKMP:      authenticator is HMAC-SHA*
                                                               ISAKMP:      encaps is 1*
                                                          ISAKMP:      key length is 256*
                                                    ISAKMP:      SA life type in seconds*
                               ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                       CryptoEngine0: validate proposal*
                                                     .ISAKMP (0:1): atts are acceptable*
                                            ,IPSEC(validate_proposal_request): proposal part #1*
                                 ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                      ,(local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1
                                  ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                    , protocol= ESP, transform= esp-aes 256 esp-sha-hmac
                                                                ,lifedur= 0s and 0kb
                                       spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
                                                CryptoEngine0: validate proposal request*
                          = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
:IPSEC(validate_transform_proposal): transform proposal not supported for identity*
                                                  { esp-aes 256 esp-sha-hmac}
                                        ISAKMP (0:1): IPSec policy invalidated proposal*
                                                ISAKMP (0:1): Checking IPSec proposal 7*
                                                           ISAKMP: transform 1, ESP_AES*
                                                     :ISAKMP:   attributes in transform*
                                                 ISAKMP:      authenticator is HMAC-MD5*
                                                               ISAKMP:      encaps is 1*
                                                          ISAKMP:      key length is 128*
                                                    ISAKMP:      SA life type in seconds*
                               ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                       CryptoEngine0: validate proposal*
                                                     .ISAKMP (0:1): atts are acceptable*
                                            ,IPSEC(validate_proposal_request): proposal part #1*
                                 ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                      ,(local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1
                                  ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
```

, protocol= ESP, transform= esp-aes esp-md5-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
CryptoEngine0: validate proposal request*
= IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
:IPSEC(validate_transform_proposal): transform proposal not supported for identity*
{ esp-aes esp-md5-hmac}
ISAKMP (0:1): IPSec policy invalidated proposal*
ISAKMP (0:1): Checking IPSec proposal 8*
ISAKMP: transform 1, ESP_AES*
:ISAKMP: attributes in transform*
ISAKMP: authenticator is HMAC-SHA*
ISAKMP: encaps is 1*
ISAKMP: key length is 128*
ISAKMP: SA life type in seconds*
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B*
CryptoEngine0: validate proposal*
.ISAKMP (0:1): atts are acceptable*
,IPSEC(validate_proposal_request): proposal part #1*
,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
,(local_proxy= 10.1.1.1/255.255.255.255/0/0 (type=1
,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
, protocol= ESP, transform= esp-aes esp-sha-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
CryptoEngine0: validate proposal request*
= IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
:IPSEC(validate_transform_proposal): transform proposal not supported for identity*
{ esp-aes esp-sha-hmac}
ISAKMP (0:1): IPSec policy invalidated proposal*
ISAKMP (0:1): Checking IPSec proposal 9*
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*
CryptoEngine0: validate proposal*
.ISAKMP (0:1): atts are acceptable*
ISAKMP (0:1): Checking IPSec proposal 9*
ISAKMP (0:1): transform 1, IPPCP LZS*
:ISAKMP: attributes in transform*
ISAKMP: encaps is 1*
ISAKMP: SA life type in seconds*
IPSEC(spi_response): getting spi 3233689542 for SA*
from 10.1.1.1 to 10.0.0.1 for prot 3
(ISAKMP: received ke message (2/1*
CryptoEngine0: generate hmac context for conn id 1*
(CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec*
(CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec*
ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) QM_IDLE*
ISAKMP (0:1): Node 2058744231, Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY*
ISAKMP (0:1): Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2*
ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE*
(CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec*
CryptoEngine0: generate hmac context for conn id 1*
(CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec*
CryptoEngine0: ipsec allocate flow*
CryptoEngine0: ipsec allocate flow*
(CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec*
(CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec*
ISAKMP: Locking peer struct 0x83166B20, IPSEC refcount 1 for for stuff_ke*

A matching IPSec policy has been negotiated and authenticated. !--- Next, the SA's are set ---!

up. ***ISAKMP (0:1): Creating IPSec SAs**

inbound SA from 10.0.0.1 to 10.1.1.1 (f/i) 0/ 0 *
(proxy 10.16.20.1 to 10.1.1.1)
has spi 0xC0BE2FC6 and conn_id 420 and flags 2 *
lifetime of 2147483 seconds *
has client flags 0x0 *
outbound SA from 10.1.1.1 to 10.0.0.1 (f/i) 0/ 0 *
(**proxy 10.1.1.1** to 10.16.20.1)
ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE*
ISAKMP: set new node 1101355775 to QM_IDLE*
(CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec*
CryptoEngine0: generate hmac context for conn id 1*
(CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec*
ISAKMP (0:1): processing HASH payload. message ID = 1101355775*
ISAKMP (0:1): processing SA payload. message ID = 1101355775*
ISAKMP (0:1): Checking IPSec proposal 1*
ISAKMP: transform 1, ESP_AES*
:ISAKMP: attributes in transform*
ISAKMP: authenticator is HMAC-MD5*
ISAKMP: encaps is 1*
ISAKMP: key length is 256*
ISAKMP: SA life type in seconds*
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B*
CryptoEngine0: validate proposal*
.ISAKMP (0:1): atts are acceptable*
ISAKMP (0:1): Checking IPSec proposal 1*
ISAKMP (0:1): transform 1, IPPCP LZS*
:ISAKMP: attributes in transform*
ISAKMP: encaps is 1*
ISAKMP: SA life type in seconds*
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B*
.ISAKMP (0:1): atts are acceptable*
,IPSEC(validate_proposal_request): proposal part #1*
,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
,(local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
, protocol= ESP, transform= esp-aes 256 esp-md5-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
,IPSEC(validate_proposal_request): proposal part #2*
,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
,(local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
, protocol= PCP, transform= comp-lzs
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
CryptoEngine0: validate proposal request*
= IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
= IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
:IPSEC(validate_transform_proposal): transform proposal not supported for identity*
{ esp-aes 256 esp-md5-hmac comp-lzs}
ISAKMP (0:1): IPSec policy invalidated proposal*
ISAKMP (0:1): Checking IPSec proposal 2*
ISAKMP: transform 1, ESP_AES*
:ISAKMP: attributes in transform*
ISAKMP: authenticator is HMAC-SHA*
ISAKMP: encaps is 1*
ISAKMP: key length is 256*
ISAKMP: SA life type in seconds*
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B*
CryptoEngine0: validate proposal*
.ISAKMP (0:1): atts are acceptable*
ISAKMP (0:1): Checking IPSec proposal 2*
ISAKMP (0:1): transform 1, IPPCP LZS*
:ISAKMP: attributes in transform*

```
                                                    ISAKMP:      encaps is 1*
                                                ISAKMP:      SA life type in seconds*
                          ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                .ISAKMP (0:1): atts are acceptable*
                                       ,IPSEC(validate_proposal_request): proposal part #1*
                                ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                   ,(local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4
                                  ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                    , protocol= ESP, transform= esp-aes 256 esp-sha-hmac
                                                    ,lifedur= 0s and 0kb
                                      spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
                                       ,IPSEC(validate_proposal_request): proposal part #2*
                                ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                   ,(local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4
                                  ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                                , protocol= PCP, transform= comp-lzs
                                                    ,lifedur= 0s and 0kb
                                         spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
                                                CryptoEngine0: validate proposal request*
                              = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
                              = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
:IPSEC(validate_transform_proposal): transform proposal not supported for identity*
                                                { esp-aes 256 esp-sha-hmac comp-lzs}
                                        ISAKMP (0:1): IPSec policy invalidated proposal*
                                                ISAKMP (0:1): Checking IPSec proposal 3*
                                                           ISAKMP: transform 1, ESP_AES*
                                                     :ISAKMP:   attributes in transform*
                                                 ISAKMP:      authenticator is HMAC-MD5*
                                                               ISAKMP:      encaps is 1*
                                                          ISAKMP:      key length is 128*
                                                    ISAKMP:      SA life type in seconds*
                          ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                      CryptoEngine0: validate proposal*
                                                .ISAKMP (0:1): atts are acceptable*
                                                ISAKMP (0:1): Checking IPSec proposal 3*
                                                   ISAKMP (0:1): transform 1, IPPCP LZS*
                                                     :ISAKMP:   attributes in transform*
                                                               ISAKMP:      encaps is 1*
                                                    ISAKMP:      SA life type in seconds*
                          ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                .ISAKMP (0:1): atts are acceptable*
                                       ,IPSEC(validate_proposal_request): proposal part #1*
                                ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                   ,(local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4
                                  ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                        , protocol= ESP, transform= esp-aes esp-md5-hmac
                                                    ,lifedur= 0s and 0kb
                                      spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
                                       ,IPSEC(validate_proposal_request): proposal part #2*
                                ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                   ,(local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4
                                  ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                                , protocol= PCP, transform= comp-lzs
                                                    ,lifedur= 0s and 0kb
                                         spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
                                                CryptoEngine0: validate proposal request*
                              = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
                              = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
:IPSEC(validate_transform_proposal): transform proposal not supported for identity*
                                                 { esp-aes esp-md5-hmac comp-lzs}
                                        ISAKMP (0:1): IPSec policy invalidated proposal*
                                                ISAKMP (0:1): Checking IPSec proposal 4*
                                                           ISAKMP: transform 1, ESP_AES*
                                                     :ISAKMP:   attributes in transform*
```

```
                                                ISAKMP:      authenticator is HMAC-SHA*
                                                             ISAKMP:      encaps is 1*
                                                        ISAKMP:      key length is 128*
                                                   ISAKMP:      SA life type in seconds*
                            ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                          CryptoEngine0: validate proposal*
                                                      .ISAKMP (0:1): atts are acceptable*
                                                 ISAKMP (0:1): Checking IPSec proposal 4*
                                                    ISAKMP (0:1): transform 1, IPPCP LZS*
                                                      :ISAKMP:   attributes in transform*
                                                             ISAKMP:      encaps is 1*
                                                   ISAKMP:      SA life type in seconds*
                            ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                      .ISAKMP (0:1): atts are acceptable*
                                    ,IPSEC(validate_proposal_request): proposal part #1*
                                ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                   ,(local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4
                                  ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                         , protocol= ESP, transform= esp-aes esp-sha-hmac
                                                                ,lifedur= 0s and 0kb
                                       spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
                                        ,IPSEC(validate_proposal_request): proposal part #2*
                                ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                   ,(local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4
                                  ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                                   , protocol= PCP, transform= comp-lzs
                                                                ,lifedur= 0s and 0kb
                                         spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
                                                      CryptoEngine0: validate proposal request*
                                = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
                                = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
:IPSEC(validate_transform_proposal): transform proposal not supported for identity*
                                                          { esp-aes esp-sha-hmac comp-lzs}
                                            ISAKMP (0:1): IPSec policy invalidated proposal*
                                                    ISAKMP (0:1): Checking IPSec proposal 5*
                                                       ISAKMP: transform 1, ESP_AES*
                                                    :ISAKMP:   attributes in transform*
                                                     ISAKMP:      authenticator is HMAC-MD5*
                                                             ISAKMP:      encaps is 1*
                                                        ISAKMP:      key length is 256*
                                                   ISAKMP:      SA life type in seconds*
                            ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                          CryptoEngine0: validate proposal*
                                                      .ISAKMP (0:1): atts are acceptable*
                                    ,IPSEC(validate_proposal_request): proposal part #1*
                                ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                   ,(local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4
                                  ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                    , protocol= ESP, transform= esp-aes 256 esp-md5-hmac
                                                                ,lifedur= 0s and 0kb
                                       spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
                                                      CryptoEngine0: validate proposal request*
                                = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
                                = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
:IPSEC(validate_transform_proposal): transform proposal not supported for identity*
                                                          { esp-aes 256 esp-md5-hmac}
                                            ISAKMP (0:1): IPSec policy invalidated proposal*
                                                    ISAKMP (0:1): Checking IPSec proposal 6*
                                                       ISAKMP: transform 1, ESP_AES*
                                                    :ISAKMP:   attributes in transform*
                                                     ISAKMP:      authenticator is HMAC-SHA*
                                                             ISAKMP:      encaps is 1*
                                                        ISAKMP:      key length is 256*
                                                   ISAKMP:      SA life type in seconds*
```

```
                          ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                 CryptoEngine0: validate proposal*
                                               .ISAKMP (0:1): atts are acceptable*
                                      ,IPSEC(validate_proposal_request): proposal part #1*
                                ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                   ,(local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4
                                  ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                    , protocol= ESP, transform= esp-aes 256 esp-sha-hmac
                                                          ,lifedur= 0s and 0kb
                                       spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
                                                 CryptoEngine0: validate proposal request*
                          = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
                          = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
:IPSEC(validate_transform_proposal): transform proposal not supported for identity*
                                                    { esp-aes 256 esp-sha-hmac}
                                        ISAKMP (0:1): IPSec policy invalidated proposal*
                                         ISAKMP (0:1): Checking IPSec proposal 7*
                                                   ISAKMP: transform 1, ESP_AES*
                                              :ISAKMP:   attributes in transform*
                                           ISAKMP:      authenticator is HMAC-MD5*
                                                        ISAKMP:      encaps is 1*
                                                     ISAKMP:      key length is 128*
                                                  ISAKMP:      SA life type in seconds*
                          ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                 CryptoEngine0: validate proposal*
                                               .ISAKMP (0:1): atts are acceptable*
                                      ,IPSEC(validate_proposal_request): proposal part #1*
                                ,key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1)
                                   ,(local_proxy= 172.18.124.0/255.255.255.0/0/0 (type=4
                                  ,(remote_proxy= 10.16.20.1/255.255.255.255/0/0 (type=1
                                        , protocol= ESP, transform= esp-aes esp-md5-hmac
                                                          ,lifedur= 0s and 0kb
                                       spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x2
                                                 CryptoEngine0: validate proposal request*
                          = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
                          = IPSEC(kei_proxy): head = clientmap, map->ivrf = , kei->ivrf*
:IPSEC(validate_transform_proposal): transform proposal not supported for identity*
                                                      { esp-aes esp-md5-hmac}
                                        ISAKMP (0:1): IPSec policy invalidated proposal*
                                         ISAKMP (0:1): Checking IPSec proposal 8*
                                                   ISAKMP: transform 1, ESP_AES*
                                              :ISAKMP:   attributes in transform*
                                           ISAKMP:      authenticator is HMAC-SHA*
                                                        ISAKMP:      encaps is 1*
                                                     ISAKMP:      key length is 128*
                                                  ISAKMP:      SA life type in seconds*
                          ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B*
                                                 CryptoEngine0: validate proposal*
                                               .ISAKMP (0:1): atts are acceptable*
                                     IPSEC(spi_response): getting spi 3438126624 for SA*
                                       from 10.1.1.1  to 10.0.0.1     for prot 3
                                                      (ISAKMP: received ke message (2/1*
                                     CryptoEngine0: generate hmac context for conn id 1*
                                          (CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec*
                                       (CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec*
    ISAKMP (0:1): sending packet to 10.0.0.1 my_port 500 peer_port 500 (R) QM_IDLE*
         ISAKMP (0:1): Node 1101355775, Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY*
             ISAKMP (0:1): Old State = IKE_QM_SPI_STARVE  New State = IKE_QM_R_QM2*
ISAKMP (0:1): received packet from 10.0.0.1 dport 500 sport 500 Global (R) QM_IDLE*
                                       (CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec*
                                     CryptoEngine0: generate hmac context for conn id 1*
                                          (CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec*
                                                     CryptoEngine0: ipsec allocate flow*
                                                     CryptoEngine0: ipsec allocate flow*
```

```
                                (CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec*
                                (CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec*
            ISAKMP: Locking peer struct 0x83166B20, IPSEC refcount 2 for for stuff_ke*
                                                    ISAKMP (0:1): Creating IPSec SAs*
                                inbound SA from 10.0.0.1 to 10.1.1.1 (f/i)  0/ 0        *
                                                (proxy 10.16.20.1 to 172.18.124.0)
                                  has spi 0xCCEDA620 and conn_id 422 and flags 2        *
                                                      lifetime of 2147483 seconds       *
                                                            has client flags 0x0        *
                              outbound SA from 10.1.1.1  to 10.0.0.1     (f/i)  0/ 0        *
                                      (     proxy 172.18.124.0          to 10.16.20.1)
```

سجلات العميل

قم بتشغيل LogViewer على عميل VPN لعرض السجلات. تأكد من تعيين عامل التصفية إلى "عالي" لجميع الفئات التي تم تكوينها. هذا نموذج لمخرجات السجل:

```
                                Sev=Info/6       DIALER/0x63300002  06/18/03  16:52:27.031      1
                                                                .Initiating connection

                                    Sev=Info/4       CM/0x63100002  06/18/03  16:52:27.041      2
                                                                Begin connection process

                                    Sev=Info/4       CM/0x63100004  06/18/03  16:52:27.051      3
                                                  Establish secure connection using Ethernet

                                    Sev=Info/4       CM/0x63100024  06/18/03  16:52:27.051      4
                                                     "Attempt connection with server "10.1.1.1

                                   Sev=Info/6       IKE/0x6300003B  06/18/03  16:52:27.101      5
                                              .Attempting to establish a connection with 10.1.1.1

                                    Sev=Info/4       IKE/0x63000013  06/18/03  16:52:27.481      6
                           (SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID, VID, VID
                                                                to 10.1.1.1

                                Sev=Info/4       IPSEC/0x63700014  06/18/03  16:52:27.612      7
                                                                   Deleted all keys

                                    Sev=Info/5       IKE/0x6300002F  06/18/03  16:52:27.722      8
                                                         Received ISAKMP packet: peer = 10.1.1.1

                                    Sev=Info/4       IKE/0x63000014  06/18/03  16:52:27.722      9
            (RECEIVING <<< ISAKMP OAK AG (SA, VID, VID, VID, VID, VID, KE, ID, NON, HASH, NAT-D, NAT-D
                                                                from 10.1.1.1

                                    Sev=Info/5       IKE/0x63000059  06/18/03  16:52:27.722     10
                                              Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

                                    Sev=Info/5       IKE/0x63000001  06/18/03  16:52:27.722     11
                                                         Peer is a Cisco-Unity compliant peer

                                    Sev=Info/5       IKE/0x63000059  06/18/03  16:52:27.722     12
                                              Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

                                    Sev=Info/5       IKE/0x63000001  06/18/03  16:52:27.722     13
                                                                   Peer supports DPD

                                    Sev=Info/5       IKE/0x63000059  06/18/03  16:52:27.722     14
                                              Vendor ID payload = 4F6CF9393C7749D894C6C92D2131AE04

                                    Sev=Info/5       IKE/0x63000059  06/18/03  16:52:27.722     15
```

```
                                        Vendor ID payload = 09002689DFD6B712

          Sev=Info/5       IKE/0x63000001  06/18/03  16:52:27.722     16
                                                  Peer supports XAUTH

          Sev=Info/5       IKE/0x63000059  06/18/03  16:52:27.722     17
                    Vendor ID payload = 90CB80913EBB696E086381B5EC427B1F

          Sev=Info/5       IKE/0x63000001  06/18/03  16:52:27.722     18
                                                  Peer supports NAT-T

          Sev=Info/4       IKE/0x63000013  06/18/03  16:52:27.782     19
(SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT, NAT-D, NAT-D
                                                    to 10.1.1.1

          Sev=Info/5       IKE/0x6300002F  06/18/03  16:52:27.822     20
                                 Received ISAKMP packet: peer = 10.1.1.1

          Sev=Info/4       IKE/0x63000014  06/18/03  16:52:27.822     21
(RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:STATUS_RESP_LIFETIME
                                             from 10.1.1.1

          Sev=Info/5       IKE/0x63000044  06/18/03  16:52:27.822     22
                    RESPONDER-LIFETIME notify has value of 86400 seconds

          Sev=Info/5       IKE/0x63000046  06/18/03  16:52:27.822     23
This SA has already been alive for 0 seconds, setting expiry to 86400 seconds from now

          Sev=Info/5       IKE/0x6300002F  06/18/03  16:52:27.842     24
                                 Received ISAKMP packet: peer = 10.1.1.1

          Sev=Info/4       IKE/0x63000014  06/18/03  16:52:27.842     25
              RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.1.1.1

           Sev=Info/4       CM/0x63100015  06/18/03  16:52:27.842     26
                                               Launch xAuth application

          Sev=Info/5       IKE/0x6300002F  06/18/03  16:52:32.449     27
                                 Received ISAKMP packet: peer = 10.1.1.1

          Sev=Info/4       IKE/0x63000014  06/18/03  16:52:32.449     28
          RECEIVING <<< ISAKMP OAK TRANS *(Retransmission) from 10.1.1.1

           Sev=Info/4       CM/0x63100017  06/18/03  16:52:32.809     29
                                             xAuth application returned

          Sev=Info/4       IKE/0x63000013  06/18/03  16:52:32.809     30
                  SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.1.1.1

          Sev=Info/5       IKE/0x6300002F  06/18/03  16:52:37.626     31
                                 Received ISAKMP packet: peer = 10.1.1.1

          Sev=Info/4       IKE/0x63000014  06/18/03  16:52:37.636     32
              RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.1.1.1

          Sev=Info/5       IKE/0x63000071  06/18/03  16:52:37.636     33
                                          :Automatic NAT Detection Status
                               Remote end is NOT behind a NAT device
                               This   end is NOT behind a NAT device

           Sev=Info/4       CM/0x6310000E  06/18/03  16:52:37.636     34
                     Established Phase 1 SA.  1 Phase 1 SA in the system

          Sev=Info/4       IKE/0x63000013  06/18/03  16:52:37.656     35
```

```
                                SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.1.1.1

                        Sev=Info/5       IKE/0x6300005D  06/18/03  16:52:37.987     36
                                    Client sending a firewall request to concentrator

                        Sev=Info/5       IKE/0x6300005C  06/18/03  16:52:37.987     37
                         =Firewall Policy: Product=Cisco Integrated Client, Capability
                                                  .(Centralized Protection Policy)

                        Sev=Info/4       IKE/0x63000013  06/18/03  16:52:38.007     38
                                SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.1.1.1

                        Sev=Info/5       IKE/0x6300002F  06/18/03  16:52:38.087     39
                                          Received ISAKMP packet: peer = 10.1.1.1

                        Sev=Info/4       IKE/0x63000014  06/18/03  16:52:38.087     40
                            RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.1.1.1

                        Sev=Info/5       IKE/0x63000010  06/18/03  16:52:38.097     41
                MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 10.16.20.1

                        Sev=Info/5       IKE/0x63000010  06/18/03  16:52:38.097     42
                  MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): , value = 10.1.1.10

                        Sev=Info/5       IKE/0x63000010  06/18/03  16:52:38.097     43
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1) (a.k.a. WINS) : , value = 10.1.1.20

                        Sev=Info/5       IKE/0xA3000017  06/18/03  16:52:38.097     44
   (MODE_CFG_REPLY: The received (INTERNAL_ADDRESS_EXPIRY) attribute and value (86388
                                                                  is not supported

                        Sev=Info/5       IKE/0x6300000E  06/18/03  16:52:38.097     45
          MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Internetwork
,Operating System Software IOS (tm) C2600 Software (C2600-IK9S-M), Version 12.2(15)T2
                                                          (RELEASE SOFTWARE (fc2
                                                TAC Support: http://www.cisco.com/tac
                                      .Copyright (c) 1986-2003 by cisco Systems, Inc
                                                Compiled Thu 01-May-03 10:39 by nmasa

                        Sev=Info/5       IKE/0x6300000E  06/18/03  16:52:38.097     46
              MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN: , value = cisco.com

                        Sev=Info/5       IKE/0x6300000D  06/18/03  16:52:38.097     47
             ,(MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets
                                                              value = 0x00000001

                        Sev=Info/5       IKE/0x6300000F  06/18/03  16:52:38.097     48
                                                                      SPLIT_NET #1
                                                         subnet = 172.18.124.0
                                                          mask = 255.255.255.0
                                                                  protocol = 0
                                                                  src port = 0
                                                                   dest port=0

                         Sev=Info/4       CM/0x63100019  06/18/03  16:52:38.097     49
                                                             Mode Config data received

                        Sev=Info/5       IKE/0x63000055  06/18/03  16:52:38.347     50
                           ,Received a key request from Driver for IP address 10.1.1.1
                                                                GW IP = 10.1.1.1

                        Sev=Info/4       IKE/0x63000013  06/18/03  16:52:38.347     51
                        SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 10.1.1.1
```

```
Sev=Info/5       IKE/0x6300002F  06/18/03  16:52:38.728     52
                                  Received ISAKMP packet: peer = 10.1.1.1

Sev=Info/4       IKE/0x63000014  06/18/03  16:52:38.728     53
(RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME
                                                  from 10.1.1.1

Sev=Info/5       IKE/0x63000044  06/18/03  16:52:38.738     54
                        RESPONDER-LIFETIME notify has value of 3600 seconds

Sev=Info/5       IKE/0x63000045  06/18/03  16:52:38.738     55
                      RESPONDER-LIFETIME notify has value of 4608000 kb

Sev=Info/4       IKE/0x63000013  06/18/03  16:52:38.738     56
                                  SENDING >>> ISAKMP OAK QM *(HASH) to 10.1.1.1

Sev=Info/5       IKE/0x63000058  06/18/03  16:52:38.738     57
          Loading IPsec SA (Message ID = 0x7AB5F1A7 OUTBOUND SPI = 0xC0BE2FC6
                                                (INBOUND SPI = 0x56FFC535

Sev=Info/5       IKE/0x63000025  06/18/03  16:52:38.788     58
                                       Loaded OUTBOUND ESP SPI: 0xC0BE2FC6

Sev=Info/5       IKE/0x63000026  06/18/03  16:52:38.798     59
                                     Loaded INBOUND ESP SPI: 0x56FFC535

Sev=Info/4       CM/0x6310001A  06/18/03  16:52:38.798     60
                                    One secure connection established

Sev=Info/6       DIALER/0x63300003  06/18/03  16:52:38.828     61
                                              .Connection established

Sev=Info/6       CVPND/0x63400011  06/18/03  16:52:38.868     62
                                             Found matching adapter

Sev=Info/6       CVPND/0x63400011  06/18/03  16:52:38.968     63
                                             Found matching adapter

Sev=Info/4       CM/0x63100037  06/18/03  16:52:39.819     64
.Address watch added for 10.0.0.1.  Current address(es): 10.0.0.1

Sev=Info/4       IPSEC/0x63700014  06/18/03  16:52:40.280     65
                                                 Deleted all keys

Sev=Info/4       IPSEC/0x63700010  06/18/03  16:52:40.280     66
                                           Created a new key structure

Sev=Info/4       IPSEC/0x6370000F  06/18/03  16:52:40.290     67
                                  Added key with SPI=0xc62fbec0 into key list

Sev=Info/4       IPSEC/0x63700010  06/18/03  16:52:40.290     68
                                           Created a new key structure

Sev=Info/4       IPSEC/0x6370000F  06/18/03  16:52:40.290     69
                                  Added key with SPI=0x35c5ff56 into key list

Sev=Info/6       DIALER/0x63300008  06/18/03  16:52:41.562     70
                        MAPI32 Information - Outlook not default mail client

Sev=Info/5       IKE/0x63000055  06/18/03  16:52:54.230     71
Received a key request from Driver for IP address 1.1.1.2, GW IP = 10.1.1.1

Sev=Info/4       IKE/0x63000013  06/18/03  16:52:54.250     72
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 10.1.1.1
```

```
Sev=Info/5       IKE/0x6300002F  06/18/03  16:52:54.731     73
                                Received ISAKMP packet: peer = 10.1.1.1

Sev=Info/4       IKE/0x63000014  06/18/03  16:52:54.731     74
(RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME
                                                  from 10.1.1.1

Sev=Info/5       IKE/0x63000044  06/18/03  16:52:54.741     75
                          RESPONDER-LIFETIME notify has value of 3600 seconds

Sev=Info/5       IKE/0x63000045  06/18/03  16:52:54.741     76
                        RESPONDER-LIFETIME notify has value of 4608000 kb

Sev=Info/4       IKE/0x63000013  06/18/03  16:52:54.741     77
                                SENDING >>> ISAKMP OAK QM *(HASH) to 10.1.1.1

Sev=Info/5       IKE/0x63000058  06/18/03  16:52:54.741     78
          Loading IPsec SA (Message ID = 0x41A55AFF OUTBOUND SPI = 0xCCEDA620
                                                  (INBOUND SPI = 0x0C5B3DB2

Sev=Info/5       IKE/0x63000025  06/18/03  16:52:54.771     79
                                          Loaded OUTBOUND ESP SPI: 0xCCEDA620

Sev=Info/5       IKE/0x63000026  06/18/03  16:52:54.781     80
                                        Loaded INBOUND ESP SPI: 0x0C5B3DB2

Sev=Info/4       CM/0x63100021  06/18/03  16:52:54.781     81
                                        .Additional Phase 2 SA established

Sev=Info/4       IPSEC/0x63700010  06/18/03  16:52:55.472     82
                                        Created a new key structure

Sev=Info/4       IPSEC/0x6370000F  06/18/03  16:52:55.472     83
                                    Added key with SPI=0x20a6edcc into key list

Sev=Info/4       IPSEC/0x63700010  06/18/03  16:52:55.472     84
                                        Created a new key structure

Sev=Info/4       IPSEC/0x6370000F  06/18/03  16:52:55.472     85
                                    Added key with SPI=0xb23d5b0c into key list

Sev=Info/4       IPSEC/0x63700019  06/18/03  16:52:55.472     86
Activate outbound key with SPI=0x20a6edcc for inbound key with SPI=0xb23d5b0c
```

معلومات ذات صلة

- صفحة دعم تقنية RADIUS
- صفحة دعم مفاوضة IPSec/بروتوكولات IKE
- صفحة دعم عميل شبكة VPN من Cisco
- طلب التعليقات (RFCs)
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).