نفق IPsec بين موجه IOS وزبون Cisco VPN 4.x ل Windows مع مثال تكوين مصادقة المستخدم TACACS+

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
التكوين
الرسم التخطيطي للشبكة
التكوينات
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
أوامر استكشاف الأخطاء وإصلاحها
سجلات الموجه
سجلات العميل
معلومات ذات صلة

المقدمة

يصف هذا المستند كيفية تكوين اتصال IPsec بين موجه وعميل الشبكة الخاصة الظاهرية (VPN) 4.x من Cisco باستخدام نظام التحكم في الوصول إلى وحدة تحكم الوصول إلى المحطة الطرفية (TACACS+) لمصادقة المستخدم. برنامج Cisco IOS® الإصدار T(8)12.2 والإصدارات الأحدث إتصالات الدعم من Cisco VPN Client 4.x. يستخدم عميل شبكة VPN 4.x سياسة المجموعة 2 (Diffie-Hellman (D-H. يتيح الأمر **isakmp policy # group 2** لعملاء x.4 إمكانية الاتصال.

يوضح هذا المستند المصادقة على خادم TACACS+ باستخدام التخويل، مثل تعيينات خدمة تسمية الإنترنت في Windows (WINS) وخدمة تسمية المجال (DNS)، التي يتم تنفيذها محليا بواسطة الموجه.

ارجع إلى تكوين عميل Cisco VPN الإصدار x.3 ل Windows to IOS باستخدام المصادقة الموسعة المحلية لمعرفة المزيد حول السيناريو الذي تحدث فيه مصادقة المستخدم محليا في موجه Cisco IOS.

ارجع إلى تكوين IPSec بين موجه Cisco IOS وعميل Cisco VPN 4.x ل Windows الذي يستخدم RADIUS لمصادقة المستخدم لمعرفة المزيد حول السيناريو الذي تحدث فيه مصادقة المستخدم خارجيا مع بروتوكول RADIUS.

المتطلبات الأساسية

المتطلبات

قبل أن تحاول إجراء هذا التكوين، فتأكد من استيفاء المتطلبات التالية:

- مجموعة من العناوين التي سيتم تعيينها ل IPsec
- مجموعة مسماة "vpnGroup" بكلمة مرور من "cisco123"
- مصادقة المستخدم على خادم TACACS+

المكونات المستخدمة

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

- عميل شبكة VPN من Cisco لنظام التشغيل Windows الإصدار 4.0.2D (يجب أن يعمل أي عميل لشبكة VPN الإصدار x.3 أو إصدار أحدث.)
- Cisco Secure ل Windows الإصدار 3.0 (يجب أن يعمل أي خادم TACACS+)
- الإصدار T1(8)12.2 من موجه IOS 1710 من Cisco الذي تم تحميله مع مجموعة ميزات IPsecيتم عرض الإخراج من الأمر **show version** على الموجه هنا.

```
1710#show version
Cisco Internetwork Operating System Software
,(IOS (tm) C1700 Software (C1710-K9O3SY-M
(Version 12.2(8)T1, RELEASE SOFTWARE (fc2
TAC Support: http://www.cisco.com/tac
.Copyright (c) 1986-2002 by cisco Systems, Inc
Compiled Sat 30-Mar-02 13:30 by ccai
Image text-base: 0x80008108, data-base: 0x80C1E054

(ROM: System Bootstrap, Version 12.2(1r)XE1, RELEASE SOFTWARE (fc1

uptime is 1 week, 6 days, 22 hours, 30 minutes 1710
System returned to ROM by reload
"System image file is "flash:c1710-k9o3sy-mz.122-8.T1

(cisco 1710 (MPC855T) processor (revision 0x200
.with 27853K/4915K bytes of memory
Processor board ID JAD052706CX (3234866109), with hardware revision 0000
MPC855T processor: part number 5, mask 2
.Bridging software
.X.25 software, Version 3.0.0
(Ethernet/IEEE 802.3 interface(s 1
(FastEthernet/IEEE 802.3 interface(s 1
(Virtual Private Network (VPN) Module(s 1
.32K bytes of non-volatile configuration memory
(16384K bytes of processor board System flash (Read/Write

Configuration register is 0x2102
```

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.

الاصطلاحات

أحلت cisco فني طرف إتفاق لمعلومة على وثيقة إتفاق.

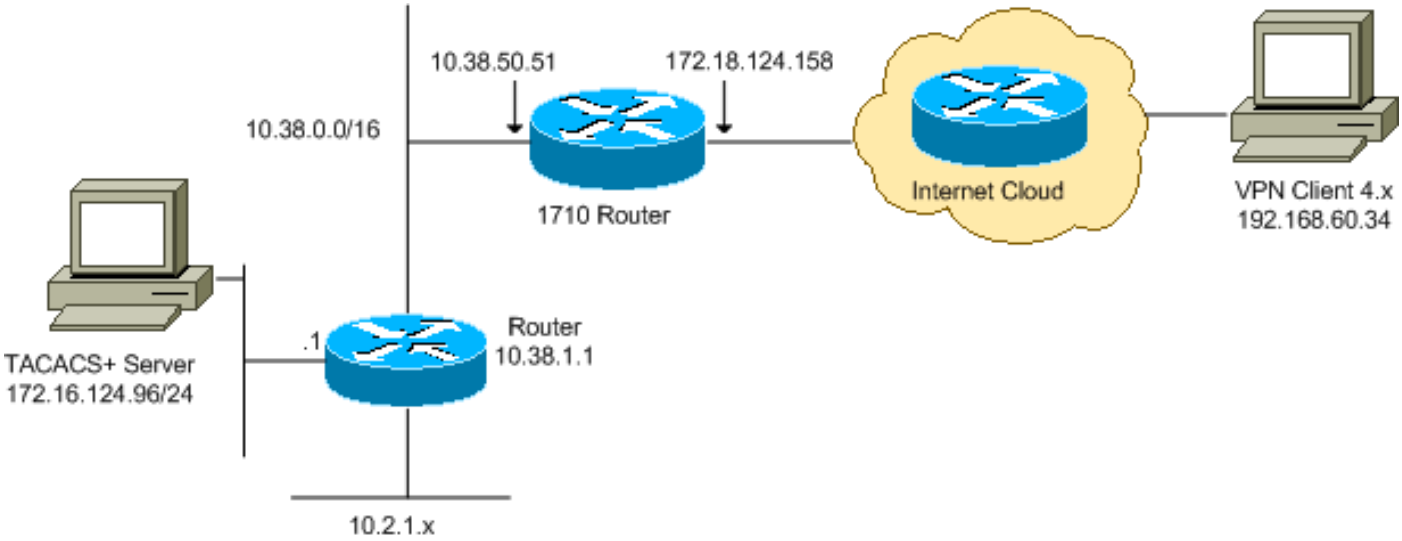
التكوين

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:



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان أن يتلقى يكون استعملت في مختبر بيئة.

التكوينات

يستخدم هذا المستند التكوينات التالية:

- موجّه Cisco 1710
- خادم TACACS+
- عميل VPN 4.x
- تقسيم الاتصال النفقي

موجّه Cisco 1710

موجّه Cisco 1710
1710#**show run** ...Building configuration Current configuration : 1884 bytes ! version 12.2 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname 1710 ! *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. !--- The group TACACS+ command
.specifies TACACS+ user authentication

+aaa authentication login userauthen group tacacs
In order to enable group authorization, !--- enable ---!
.the aaa authorization commands

aaa authorization network groupauthor local
!
!
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
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 in order to specify the !--- WINS ---!
and DNS server addresses to the VPN Client, !--- along
with the pre-shared key for authentication. crypto
isakmp client configuration group vpngroup
key cisco123
dns 10.2.1.10
wins 10.2.1.20
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 previously 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
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
!
!
```

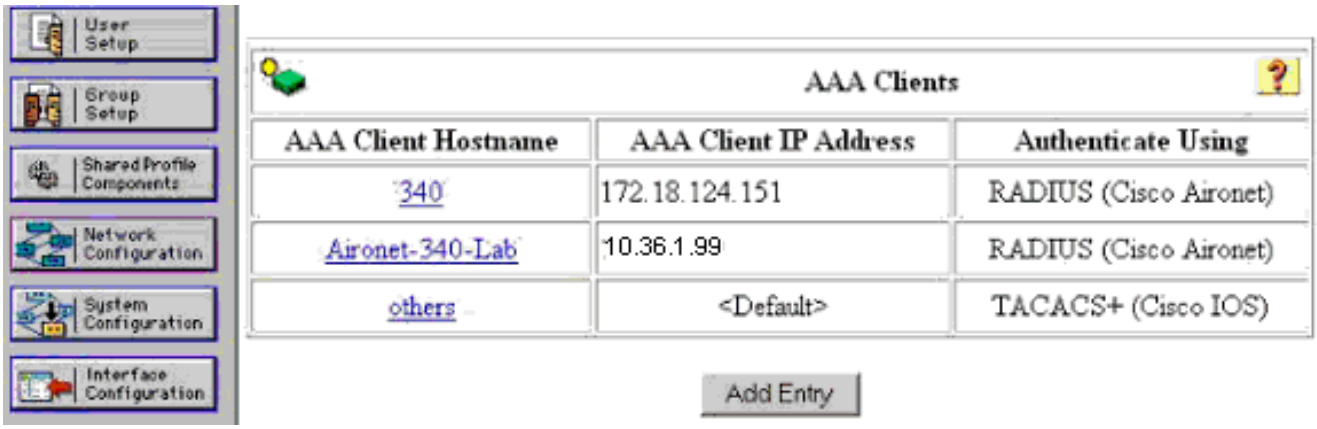
```
Apply the crypto map on the outside interface. ---!
interface FastEthernet0
ip address 172.18.124.158 255.255.255.0
crypto map clientmap
!
interface Ethernet0
ip address 10.38.50.51 255.255.0.0
!

Create a pool of addresses to be assigned to the ---!
VPN Clients. ip local pool ippool 10.1.1.100 10.1.1.200
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1
ip route 172.16.124.0 255.255.255.0 10.38.1.1
ip route 10.2.1.0 255.255.255.0 10.38.1.1
ip http server
ip pim bidir-enable
!
!
!
Specify the IP address of the TACACS+ server, !--- ---!
along with the TACACS+ shared secret key. tacacs-server
host 172.16.124.96 key cisco123
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
!
!
end
```

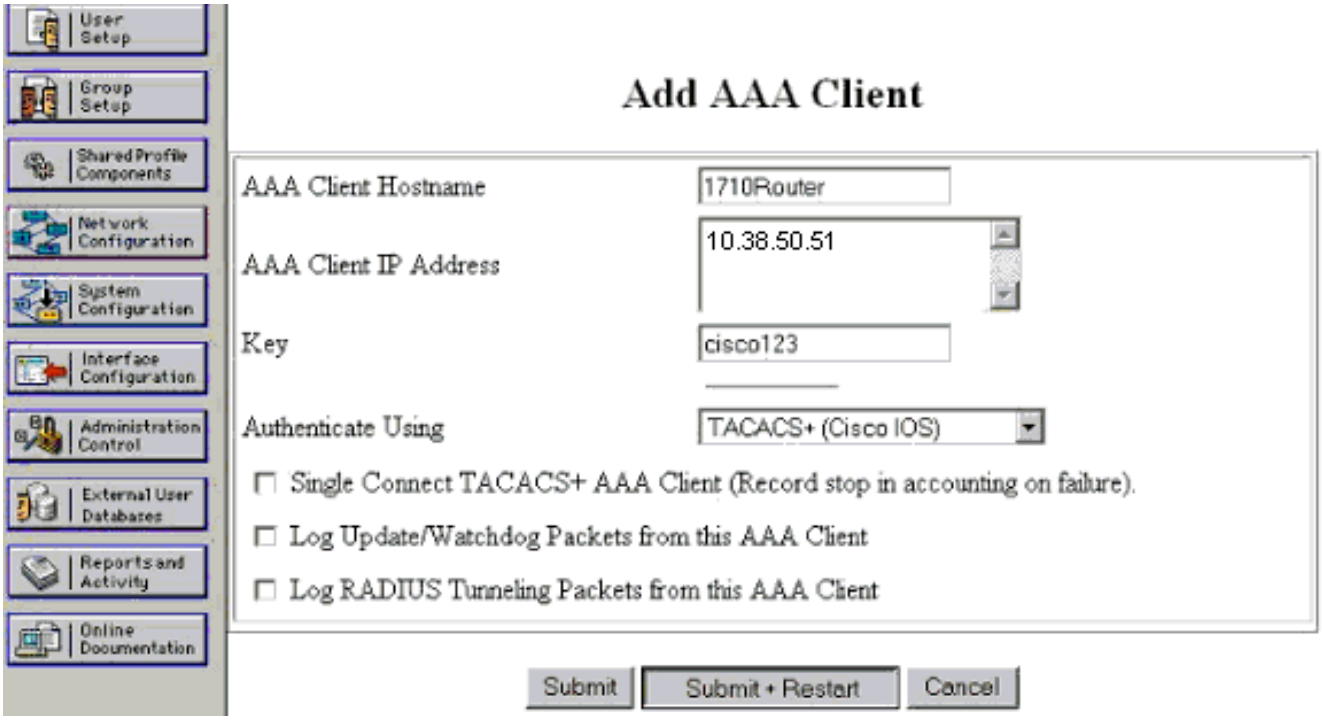
خادم TACACS+

لتكوين خادم TACACS+، أكمل الخطوات التالية:

1. انقر فوق **إضافة إدخال** لإضافة إدخال للموجه في قاعدة بيانات خادم TACACS+.

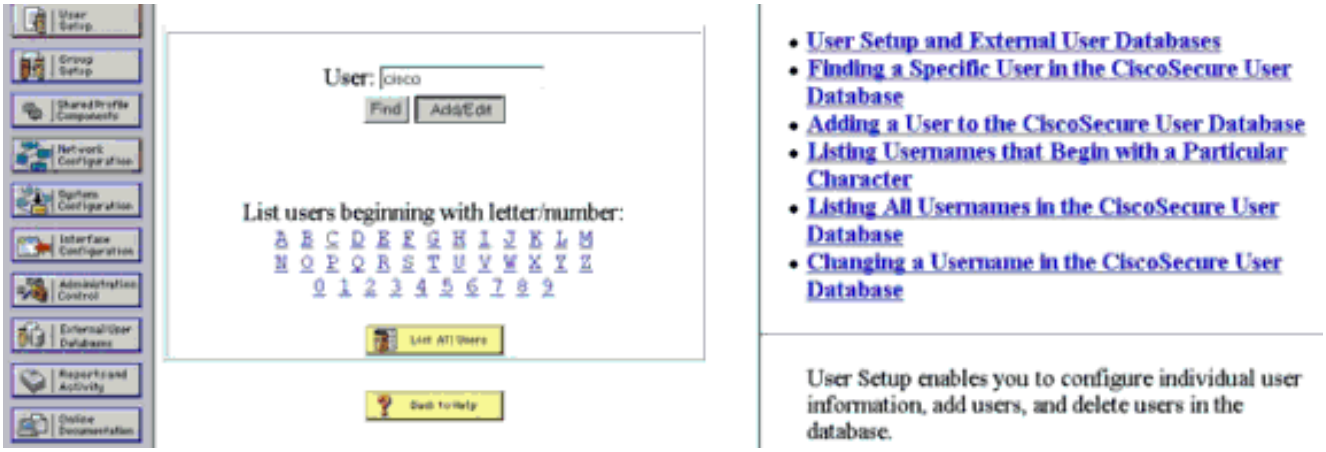


2. في صفحة إضافة عميل AAA، أدخل معلومات الموجه كما هو موضح في هذه الصورة:

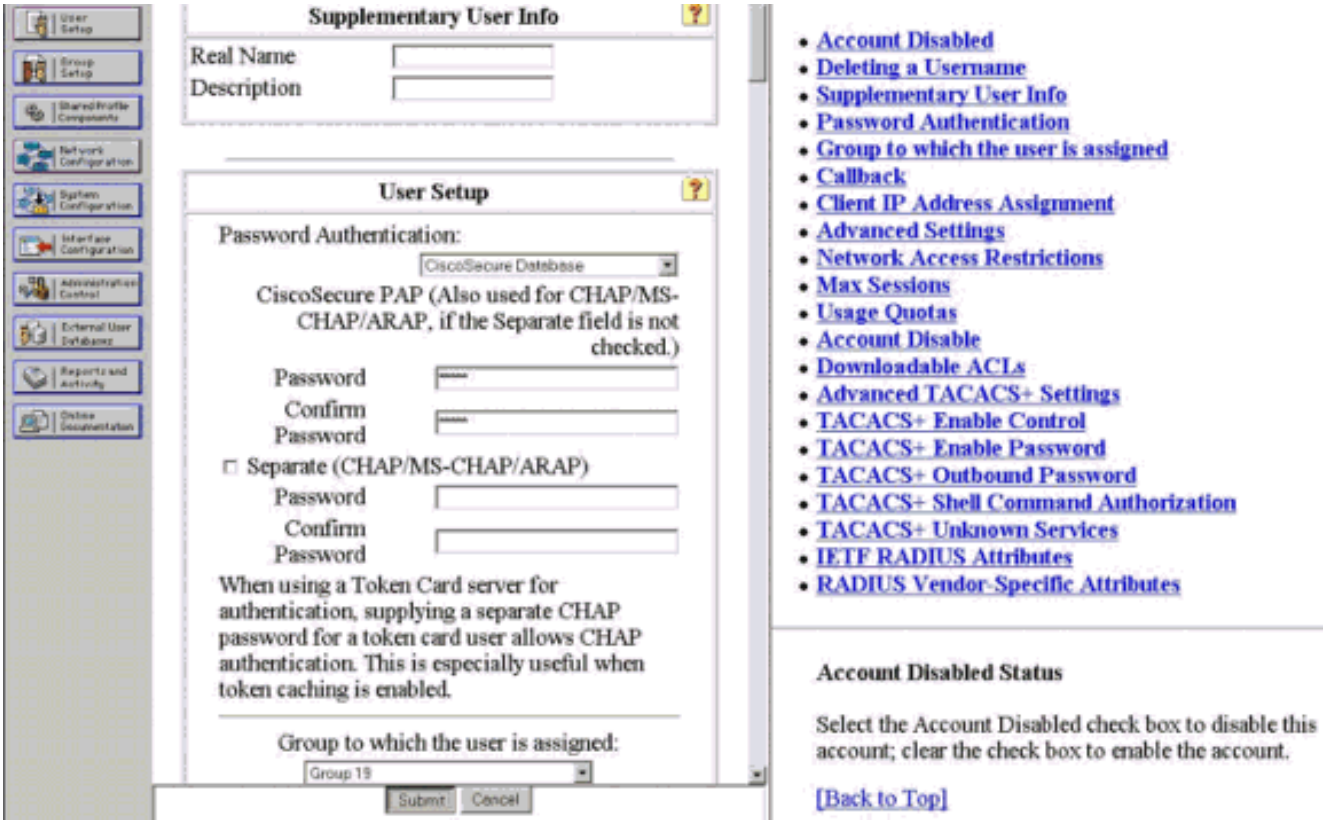


في حقل اسم المضيف لعميل AAA، أدخل اسما للموجه.في حقل عنوان IP لعميل AAA، أدخل **10.38.50.51**.دخلت في المفتاح مجال، **cisco123** بما أن ال يشارك سر مفتاح.من القائمة المنسدلة مصادقة باستخدام، أختر **TACACS+ (Cisco IOS)**، وانقر فوق **إرسال**.

3. دخلت في المستعمل مجال، المستعمل إسم ل ال VPN مستعمل في ال cisco يأمن قاعدة معطيات، وطقطقة **يضيف/يحرر**.في هذا مثال، المستعمل إسم *cisco*.



4. في الصفحة التالية، أدخل كلمة المرور وأكدها للمستخدم *cisco*.في هذا مثال، الكلمة أيضا *cisco*.

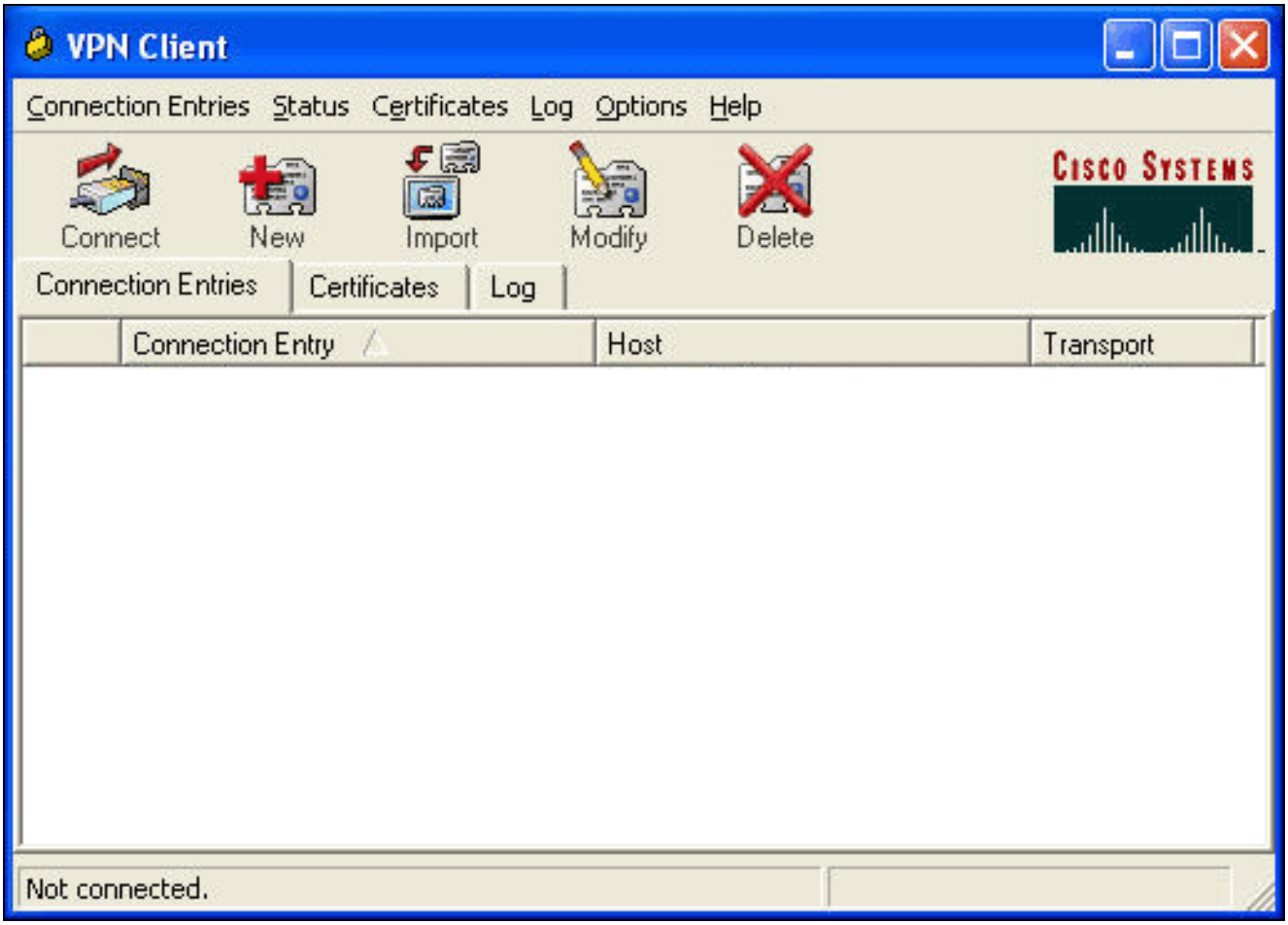


5. إذا كنت ترغب في تعيين حساب المستخدم إلى مجموعة، أكمل هذه الخطوة الآن. عند الانتهاء، انقر فوق **إرسال**.

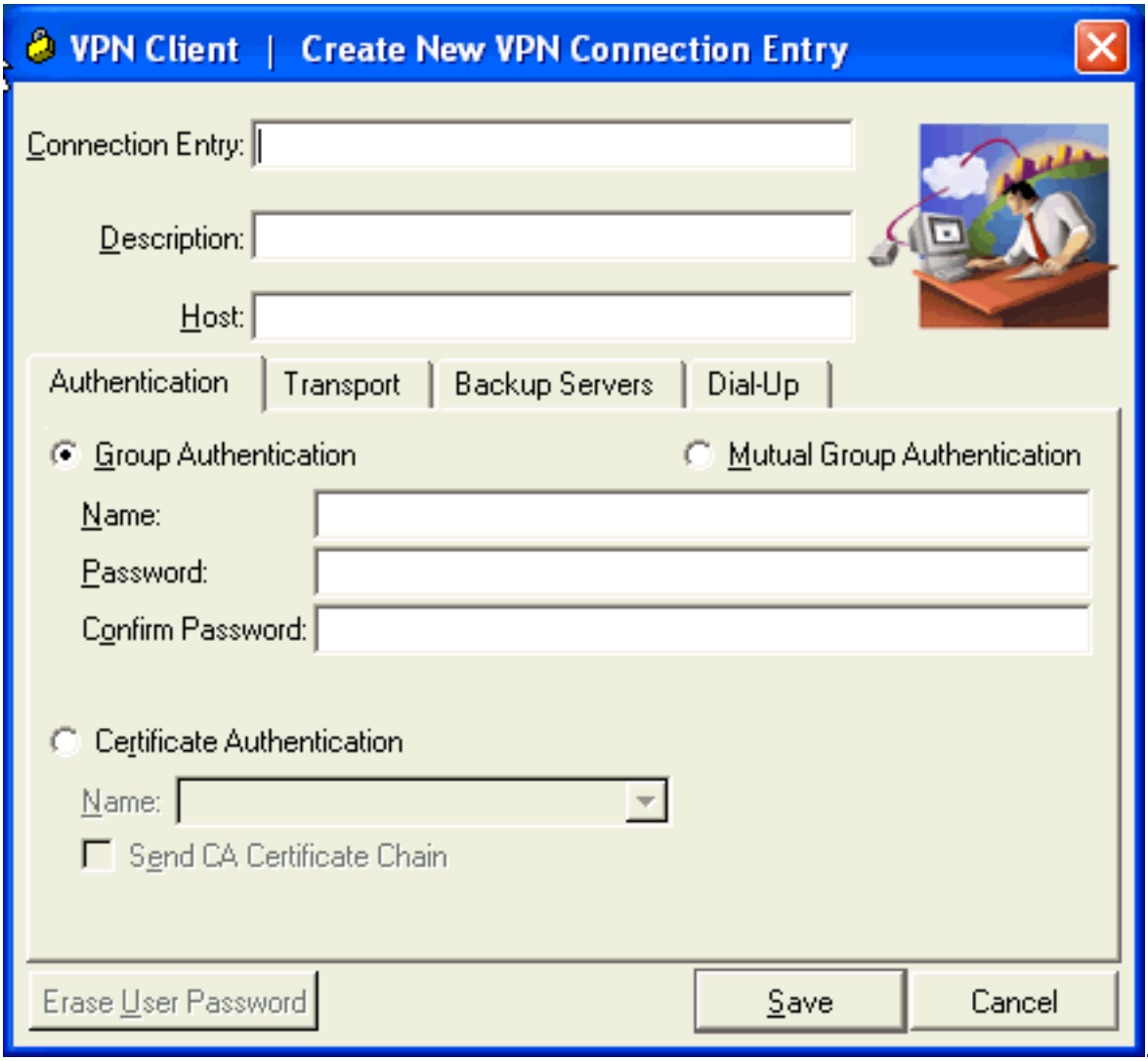
عميل VPN 4.x

لتكوين عميل VPN 4.x، أكمل الخطوات التالية:

1. أطلقت ال VPN زبون، وطقطقة **جديد** in order to خلقت توصيل جديد.

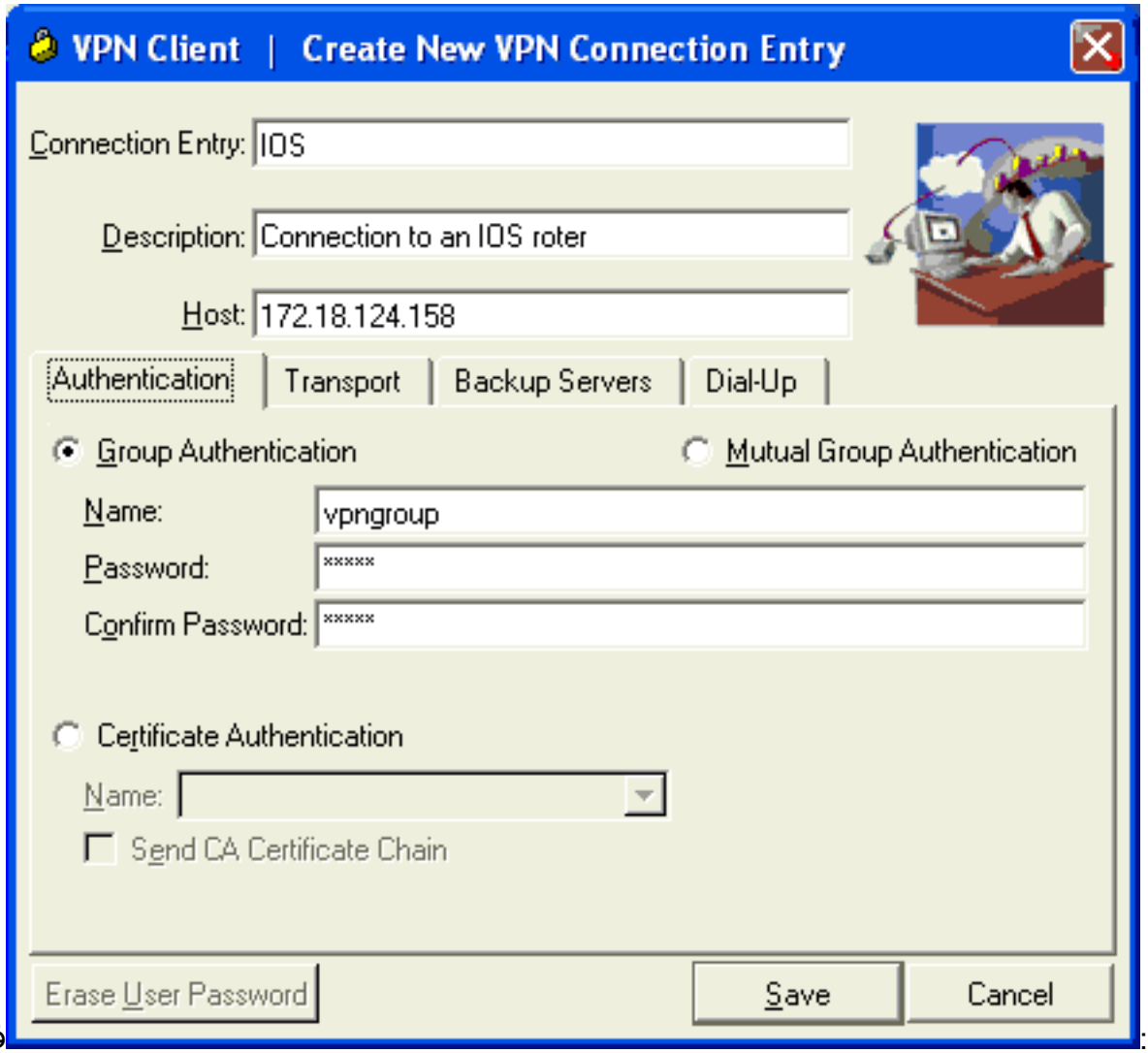


يظهر مربع الحوار "إنشاء اتصال VPN جديد ل



."VPN

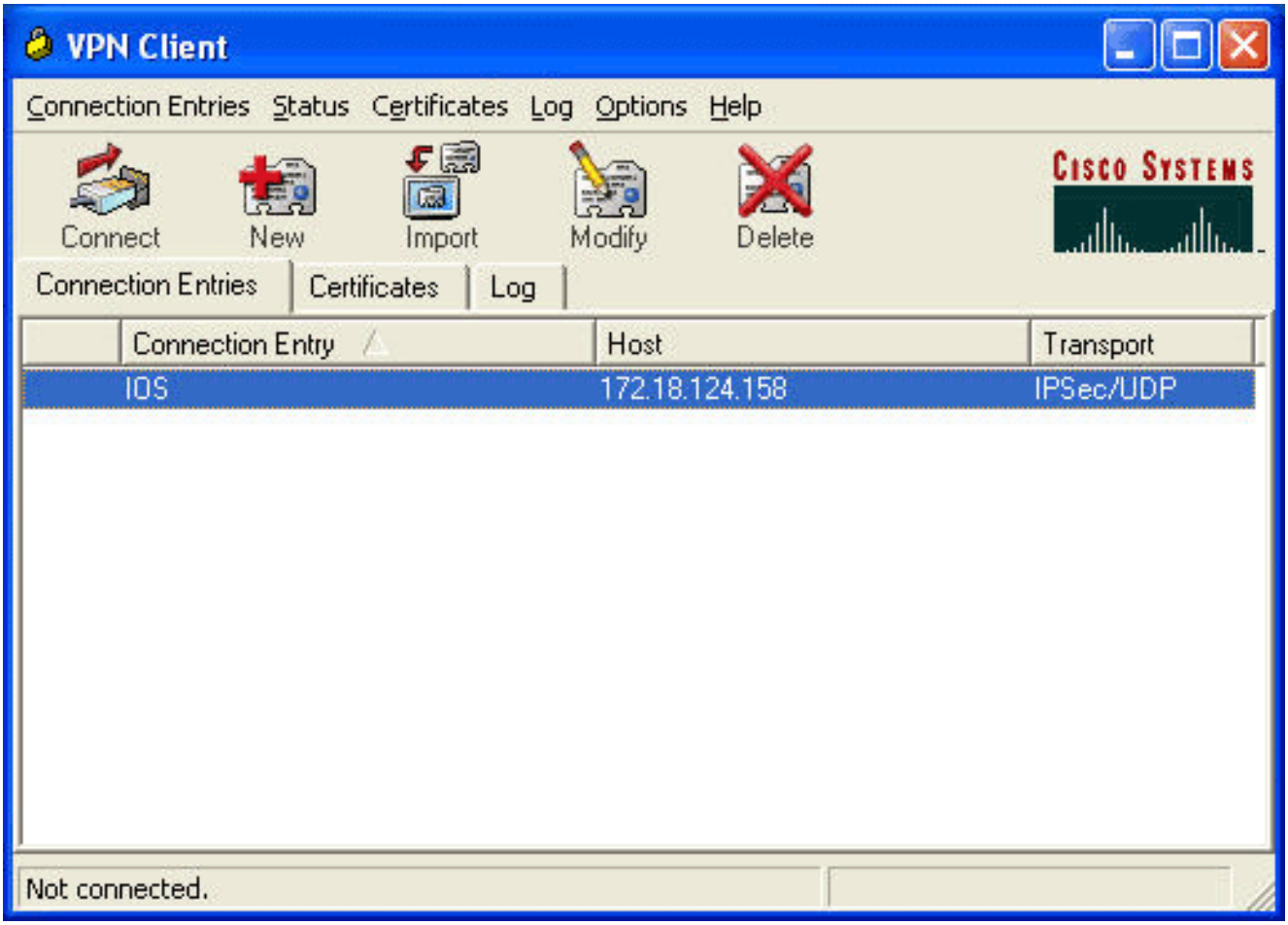
2. في مربع الحوار "إنشاء اتصال VPN جديد"، أدخل معلومات الاتصال كما هو موضح في هذه



في الصورة:

حقل "إدخال الاتصال"، أدخل اسما للاتصال.في حقلي الوصف والمضيف، أدخل وصفا وعنوان IP للمضيف لإدخال الاتصال.في علامة تبويب المصادقة، انقر على زر راديو **مصادقة المجموعة**، وأدخل اسم المستخدم وكلمة المرور الخاصة به.طقطقة **حفظ** in order to أنقذت التوصيل.

3. في نافذة عميل شبكة VPN، حدد إدخال الاتصال الذي قمت بإنشائه، وانقر فوق **توصيل** للاتصال بالموجه.



4. بينما يقوم IPsec بالتفاوض، تتم مطالبتك باسم مستخدم وكلمة مرور. أدخل اسم مستخدم وكلمة مرور.يعرض الإطار الرسائل التالية:"التفاوض على ملفات الأمن.""الارتباط الخاص بك آمن الآن."

تقسيم الاتصال النفقي

لتمكين الاتصال النفقي المنقسم لاتصالات VPN، تأكد من تكوين قائمة تحكم في الوصول (ACL) على الموجه. في هذا المثال، يتم إقران الأمر 102 **access-list** بالمجموعة لأغراض تقسيم الاتصال النفقي، ويتم تكوين النفق لشبكات x.16.10.38 و x.x.10.2. تتدفق حركة المرور غير مشفرة إلى الأجهزة غير الموجودة في قائمة التحكم في الوصول 102 (على سبيل المثال، الإنترنت).

```
access-list 102 permit ip 10.38.0.0 0.0.255.255 10.1.1.0 0.0.0.255
access-list 102 permit ip 10.2.0.0 0.0.255.255 10.1.1.0 0.0.0.255
```

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

```
crypto isakmp client configuration group vpngroup
        key cisco123
        dns 10.2.1.10
        wins 10.2.1.20
        domain cisco.com
        pool ippool
        acl 102
```

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك استخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر **العرض** بواسطة أداة مترجم الإخراج (العملاء المسجلون فقط). تتيح لك هذه الأداة عرض تحليل مخرج الأمر **show**.

```
1710#show crypto isakmp sa
dst             src             state          conn-id    slot
QM_IDLE              3       0   192.168.60.34  172.18.124.158


1710#show crypto ipsec sa

interface: FastEthernet0
Crypto map tag: clientmap, local addr. 172.18.124.158

(local ident (addr/mask/prot/port): (172.18.124.158/255.255.255.255/0/0
(remote ident (addr/mask/prot/port): (10.1.1.114/255.255.255.255/0/0
current_peer: 192.168.60.34
{}=PERMIT, flags
pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0#
pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0#
pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0#
send errors 0, #recv errors 0#

local crypto endpt.: 172.18.124.158, remote crypto endpt.: 192.168.60.34
path mtu 1500, media mtu 1500
current outbound spi: 8F9BB05F

:inbound esp sas
(spi: 0x61C53A64(1640315492
, transform: esp-3des esp-sha-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 200, flow_id: 1, crypto map: clientmap
(sa timing: remaining key lifetime (k/sec): (4608000/3294
IV size: 8 bytes
replay detection support: Y

:inbound ah sas

:inbound pcp sas

:outbound esp sas
(spi: 0x8F9BB05F(2409345119
, transform: esp-3des esp-sha-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 201, flow_id: 2, crypto map: clientmap
(sa timing: remaining key lifetime (k/sec): (4608000/3294
IV size: 8 bytes
replay detection support: Y

:outbound ah sas

:outbound pcp sas


(local ident (addr/mask/prot/port): (10.38.0.0/255.255.0.0/0/0
(remote ident (addr/mask/prot/port): (10.1.1.114/255.255.255.255/0/0
current_peer: 192.168.60.34
{}=PERMIT, flags
pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3#
```

```
pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3#
                pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0#
                send errors 0, #recv errors 0#

local crypto endpt.: 172.18.124.158, remote crypto endpt.: 192.168.60.34
                path mtu 1500, media mtu 1500
                current outbound spi: 8B57E45E

                                :inbound esp sas
                        (spi: 0x89898D1A(2307493146
                , transform: esp-3des esp-sha-hmac
                        { ,in use settings ={Tunnel
        slot: 0, conn id: 202, flow_id: 3, crypto map: clientmap
        (sa timing: remaining key lifetime (k/sec): (4607999/3452
                                IV size: 8 bytes
                        replay detection support: Y

                                 :inbound ah sas

                                :inbound pcp sas

                               :outbound esp sas
                        (spi: 0x8B57E45E(2337793118
                , transform: esp-3des esp-sha-hmac
                        { ,in use settings ={Tunnel
        slot: 0, conn id: 203, flow_id: 4, crypto map: clientmap
        (sa timing: remaining key lifetime (k/sec): (4607999/3452
                                IV size: 8 bytes
                        replay detection support: Y

                                :outbound ah sas

                               :outbound pcp sas


                        1710#show crypto engine connections active

ID    Interface      IP-Address      State  Algorithm           Encrypt  Decrypt
      FastEthernet0  172.18.124.158  set    HMAC_SHA+3DES_56_C  0        0     2
      FastEthernet0  172.18.124.158  set    HMAC_SHA+3DES_56_C  0        0   200
      FastEthernet0  172.18.124.158  set    HMAC_SHA+3DES_56_C  0        0   201
      FastEthernet0  172.18.124.158  set    HMAC_SHA+3DES_56_C  0        3   202
      FastEthernet0  172.18.124.158  set    HMAC_SHA+3DES_56_C  3        0   203
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استعملت ال OIT in order to شاهدت تحليل من **عرض** أمر إنتاج.

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 ويظهر المجموعة الأولى من

السمات التي يتم رفضها بسبب عدم التوافق على كلا النهايتين.

- **debug crypto engine**—يعرض معلومات من محرك التشفير.
- **debug aaa authentication**— يعرض معلومات حول مصادقة AAA/TACACS+.
- **تصحيح أخطاء تفويض المصادقة والتفويض والمحاسبة (AAA)**—يعرض معلومات حول تفويض AAA/TACACS+.
- **debug tacacs**— يعرض المعلومات التي تتيح لك أستكشاف أخطاء الاتصال بين خادم TACACS+ والموجه وإصلاحها.

سجلات الموجه

```
1710#show debug
General OS:
  TACACS access control debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
Cryptographic Subsystem:
  Crypto ISAKMP debugging is on
  Crypto Engine debugging is on
  Crypto IPSEC debugging is on


1710#
1w6d: ISAKMP (0:0): received packet from 192.168.60.34 (N) NEW SA
1w6d: ISAKMP: local port 500, remote port 500
1w6d: ISAKMP (0:2): (Re)Setting client xauth list userauthen and state
1w6d: ISAKMP: Locking CONFIG struct 0x8158B894 from
 crypto_ikmp_config_initialize_sa, count 2
1w6d: ISAKMP (0:2): processing SA payload. message ID = 0
1w6d: ISAKMP (0:2): processing ID payload. message ID = 0
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): vendor ID seems Unity/DPD but bad major
1w6d: ISAKMP (0:2): vendor ID is XAUTH
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): vendor ID is DPD
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): vendor ID is Unity
1w6d: ISAKMP (0:2): Checking ISAKMP transform 1 against priority 3 policy
1w6d: ISAKMP: encryption 3DES-CBC
1w6d: ISAKMP: hash SHA
1w6d: ISAKMP: default group 2
1w6d: ISAKMP: auth XAUTHInitPreShared
1w6d: ISAKMP: life type in seconds
1w6d: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w6d: ISAKMP (0:2): atts are acceptable. Next payload is 3
1w6d: CryptoEngine0: generate alg parameter
(1w6d: CryptoEngine0: CRYPTO_ISA_DH_CREATE(hw)(ipsec
1w6d: CRYPTO_ENGINE: Dh phase 1 status: 0
1w6d: ISAKMP (0:2): processing KE payload. message ID = 0
1w6d: CryptoEngine0: generate alg parameter
(1w6d: CryptoEngine0: CRYPTO_ISA_DH_SHARE_SECRET(hw)(ipsec
1w6d: ISAKMP (0:2): processing NONCE payload. message ID = 0
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: ISAKMP (0:2): processing vendor id payload
1w6d: AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-1
1w6d: AAA/MEMORY: create_user (0x817F63F4) user='vpngroup' ruser='NULL' ds0=0
 port='ISAKMP-ID-AUTH' rem_addr='192.168.60.34' authen_type=NONE
 'service=LOGIN priv=0 initial_task_id='0
1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
```

```
                                Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT

                               :(1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894
                              Port='ISAKMP-ID-AUTH' list='groupauthor' service=NET
              '1w6d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(1472763894) user='vpngroup
         1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): send AV service=ike
       1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): send AV protocol=ipsec
     "1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): found list "groupauthor
                 1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): Method=LOCAL
                  1w6d: AAA/AUTHOR (1472763894): Post authorization status = PASS_ADD
                                                      1w6d: 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 timeout*0
                                             AAA/AUTHOR/IKE: Processing AV idletime*0
                                              AAA/AUTHOR/IKE: Processing AV inacl*102
                          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
                               1w6d: CryptoEngine0: create ISAKMP SKEYID for conn id 2
                                  (1w6d: CryptoEngine0: CRYPTO_ISA_SA_CREATE(hw)(ipsec
                                        1w6d: ISAKMP (0:2): SKEYID state generated
                    1w6d: ISAKMP (0:2): SA is doing pre-shared key authentication plux
                                             XAUTH using id type ID_IPV4_ADDR
                                                    1w6d: ISAKMP (2): ID payload
                                                                next-payload : 10
                                                                        type : 1
                                                                    protocol : 17
                                                                       port : 500
                                                                       length : 8
                                                  1w6d: ISAKMP (2): Total payload length: 12
                                      1w6d: CryptoEngine0: generate hmac context for conn id 2
                                           (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec
                       1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) AG_INIT_EXCH
                         1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY
                                        Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2

                                       '1w6d: AAA/MEMORY: free_user (0x817F63F4) user='vpngroup
                           'ruser='NULL' port='ISAK MP-ID-AUTH' rem_addr='192.168.60.34
                                                 authen_type=NONE service=LOGIN priv=0
                    1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) AG_INIT_EXCH
                                     (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec
                           1w6d: ISAKMP (0:2): processing HASH payload. message ID = 0
                                      1w6d: CryptoEngine0: generate hmac context for conn id 2
                                           (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec
                             1w6d: ISAKMP (0:2): processing NOTIFY INITIAL_CONTACT protocol 1
                                                 spi 0, message ID = 0, sa = 81673884
                                       1w6d: ISAKMP (0:2): Process initial contact, bring down
                                                           existing phase 1 and 2 SA's
                        1w6d: ISAKMP (0:2): returning IP addr to the address pool: 10.1.1.113
                                       1w6d: ISAKMP (0:2): returning address 10.1.1.113 to pool
                                     .1w6d: ISAKMP (0:2): peer does not do paranoid keepalives

                             1w6d: ISAKMP (0:2): SA has been authenticated with 192.168.60.34
                                       1w6d: CryptoEngine0: clear dh number for conn id 1
                                      (1w6d: CryptoEngine0: CRYPTO_ISA_DH_DELETE(hw)(ipsec
                                            ...1w6d: IPSEC(key_engine): got a queue event
                          1w6d: IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
                 1w6d: IPSEC(key_engine_delete_sas): delete all SAs shared with 192.168.60.34
                                      1w6d: CryptoEngine0: generate hmac context for conn id 2
                                           (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec
```

```
                                (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec
                        1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) QM_IDLE
                                        1w6d: ISAKMP (0:2): purging node 1324880791
                                1w6d: ISAKMP: Sending phase 1 responder lifetime 86400

                            1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
                                    Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE

                                                        1w6d: ISAKMP (0:2): Need XAUTH
                                            1w6d: AAA: parse name=ISAKMP idb type=-1 tty=-1
                                '1w6d: AAA/MEMORY: create_user (0x812F79FC) user='NULL
                                                    '=ruser='NULL' ds0=0 port
                            ISAKMP' rem_addr='192.168.60.34' authen_type=ASCII service=LOGIN
                                                    'priv=0 initial_task_id='0
                                1w6d: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
                        Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT

                            '1w6d: AAA/AUTHEN/START (2017610393): port='ISAKMP' list='userauthen
                                                    action=LOGIN service=LOGIN
                                    1w6d: AAA/AUTHEN/START (2017610393): found list userauthen
                                (+1w6d: AAA/AUTHEN/START (2017610393): Method=tacacs+ (tacacs
                                   1w6d: TAC+: send AUTHEN/START packet ver=192 id=2017610393
                                  .1w6d: TAC+: Using default tacacs server-group "tacacs+" list
                                       1w6d: TAC+: Opening TCP/IP to 172.16.124.96/49 timeout=5
                                  1w6d: TAC+: Opened TCP/IP handle 0x8183D638 to 172.16.124.96/49
                            1w6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/START/LOGIN/ASCII queued
                                       1w6d: TAC+: (2017610393) AUTHEN/START/LOGIN/ASCII processed
                                  1w6d: TAC+: ver=192 id=2017610393 received AUTHEN status = GETUSER
                                                    1w6d: AAA/AUTHEN(2017610393): Status=GETUSER
                                                        1w6d: ISAKMP: got callback 1
                                            1w6d: ISAKMP/xauth: request attribute XAUTH_TYPE_V2
                                          1w6d: ISAKMP/xauth: request attribute XAUTH_MESSAGE_V2
                                        1w6d: ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
                                    1w6d: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
                                        1w6d: CryptoEngine0: generate hmac context for conn id 2
                                             (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec
                    1w6d: ISAKMP (0:2): initiating peer config to 192.168.60.34. ID = 1641488057
                                          (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec
                                1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF_XAUTH
                                1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, IKE_AAA_START_LOGIN
                                                    Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT
                                                              New State = IKE_XAUTH_REQ_SENT

                                 1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) CONF_XAUTH
                                          (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec
                                .1w6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34
                                                                message ID = 1641488057
                                        1w6d: CryptoEngine0: generate hmac context for conn id 2
                                             (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec
                                                        1w6d: ISAKMP: Config payload REPLY
                                    1w6d: ISAKMP/xauth: reply attribute XAUTH_TYPE_V2 unexpected
                                          1w6d: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2
                                      1w6d: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
                                        1w6d: ISAKMP (0:2): deleting node 1641488057 error FALSE
                                              "reason "done with xauth request/reply exchange
                                1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_CFG_REPLY
                                                        Old State = IKE_XAUTH_REQ_SENT
                                                    New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT

                                ('(1w6d: AAA/AUTHEN/CONT (2017610393): continue_login (user='(undef
                                                    1w6d: AAA/AUTHEN(2017610393): Status=GETUSER
                                        (+1w6d: AAA/AUTHEN(2017610393): Method=tacacs+ (tacacs
                                             1w6d: TAC+: send AUTHEN/CONT packet id=2017610393
                                    1w6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/CONT queued
```

```
                                1w6d: TAC+: (2017610393) AUTHEN/CONT processed
            1w6d: TAC+: ver=192 id=2017610393 received AUTHEN status = GETPASS
                                1w6d: AAA/AUTHEN(2017610393): Status=GETPASS
             ('1w6d: AAA/AUTHEN/CONT (2017610393): continue_login (user='cisco
                                1w6d: AAA/AUTHEN(2017610393): Status=GETPASS
                        (+1w6d: AAA/AUTHEN(2017610393): Method=tacacs+ (tacacs
                             1w6d: TAC+: send AUTHEN/CONT packet id=2017610393
                      1w6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/CONT queued
                                1w6d: TAC+: (2017610393) AUTHEN/CONT processed
              1w6d: TAC+: ver=192 id=2017610393 received AUTHEN status = PASS
                                     1w6d: AAA/AUTHEN(2017610393): Status=PASS
                                                1w6d: ISAKMP: got callback 1
         1w6d: TAC+: Closing TCP/IP 0x8183D638 connection to 172.16.124.96/49
                             1w6d: CryptoEngine0: generate hmac context for conn id 2
                                  (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec
1w6d: ISAKMP (0:2): initiating peer config to 192.168.60.34. ID = 1736579999
                                  (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec
            1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF_XAUTH
             1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, IKE_AAA_CONT_LOGIN
                                      Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT
                                              New State = IKE_XAUTH_SET_SENT

                '1w6d: AAA/MEMORY: free_user (0x812F79FC) user='cisco' ruser='NULL
                       port='ISAKMP' rem_addr='192.168.60.34' authen_type=ASCII
                                                       service=LOGIN priv=0
             1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) CONF_XAUTH
                                  (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec
           .1w6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34
                                                    message ID = 1736579999
                             1w6d: CryptoEngine0: generate hmac context for conn id 2
                                  (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec
                                           1w6d: ISAKMP: Config payload ACK
                                      1w6d: ISAKMP (0:2): XAUTH ACK Processed
                             1w6d: ISAKMP (0:2): deleting node 1736579999 error FALSE
                                              "reason "done with transaction
                          1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK
                           Old State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE

                1w6d: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
                            Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

                1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM_IDLE
                                  (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec
           .1w6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34
                                                     message ID = 398811763
                             1w6d: CryptoEngine0: generate hmac context for conn id 2
                                  (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec
                                           1w6d: ISAKMP: Config payload REQUEST
                                        :1w6d: ISAKMP (0:2): checking request
                                                1w6d: ISAKMP: IP4_ADDRESS
                                                1w6d: ISAKMP: IP4_NETMASK
                                                    1w6d: ISAKMP: IP4_DNS
                                                   1w6d: ISAKMP: IP4_NBNS
                                               1w6d: ISAKMP: ADDRESS_EXPIRY
                                            1w6d: ISAKMP: APPLICATION_VERSION
                                      1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7000
                                      1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7001
                                                1w6d: ISAKMP: DEFAULT_DOMAIN
                                                 1w6d: ISAKMP: SPLIT_INCLUDE
                                      1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7007
                                      1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7008
                                      1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7005
                          1w6d: AAA: parse name=ISAKMP-GROUP-AUTH idb type=-1 tty=-1
1w6d: AAA/MEMORY: create_user (0x812F79FC) user='vpngroup' ruser='NULL' ds0=0 po
```

```
rt='ISAKMP-GROUP-AUTH' rem_addr='192.168.60.34' authen_type=NONE service=LOGIN pr
                                                    'iv=0 initial_task_id='0
                    1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST
                Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT

                          :(1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615
                          Port='ISAKMP-GROUP-AUTH' list='groupauthor' service=NET
                          (1w6d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-GROUP-AUTH(1059453615
                                                          'user='vpngroup
                          :(1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615
                                                        send AV service=ike
                          :(1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615
                                                      send AV protocol=ipsec
                          :(1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615
                                                     "found list "groupauthor
                          :(1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615
                                                          Method=LOCAL
                1w6d: AAA/AUTHOR (1059453615): Post authorization status = PASS_ADD
                                                    1w6d: 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 timeout*0
                                               AAA/AUTHOR/IKE: Processing AV idletime*0
                                                 AAA/AUTHOR/IKE: Processing AV inacl*102
                           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
                                        :1w6d: ISAKMP (0:2): attributes sent in message
                                                      1w6d: Address: 0.2.0.0
                                     1w6d: ISAKMP (0:2): allocating address 10.1.1.114
                                     1w6d: ISAKMP: Sending private address: 10.1.1.114
                                         (1w6d: ISAKMP: Unknown Attr: IP4_NETMASK (0x2
                                1w6d: ISAKMP: Sending IP4_DNS server address: 10.1.1.10
                               1w6d: ISAKMP: Sending IP4_NBNS server address: 10.1.1.20
     1w6d: ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address: 86396
                                        :1w6d: ISAKMP: Sending APPLICATION_VERSION string
         Cisco Internetwork Operating System Software IOS (tm) C1700 Software
                  (C1710-K9O3SY-M), Version 12.2(8)T1, RELEASE SOFTWARE (fc2)
                                           TAC Support: http://www.cisco.com/tac
                                    .Copyright (c) 1986-2002 by cisco Systems, Inc
                                             Compiled Sat 30-Mar-02 13:30 by ccai
                                         (1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7000
                                         (1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7001
                1w6d: ISAKMP: Sending DEFAULT_DOMAIN default domain name: cisco.com
                     1w6d: ISAKMP: Sending split include name 102 network 10.38.0.0
                             mask 255.255.0.0 protocol 0, src port 0, dst port 0

                                         (1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7007
                                         (1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7008
                                         (1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7005
                                1w6d: CryptoEngine0: generate hmac context for conn id 2
                                     (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec
 1w6d: ISAKMP (0:2): responding to peer config from 192.168.60.34. ID = 398811763
                                    (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec
                  1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF_ADDR
                  "" 1w6d: ISAKMP (0:2): deleting node 398811763 error FALSE reason
                  1w6d: ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR
                Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE

                          '1w6d: AAA/MEMORY: free_user (0x812F79FC) user='vpngroup
                   'ruser='NULL' port='ISAKMP-GROUP-AUTH' rem_addr='192.168.60.34
```

```
                                        authen_type=NONE service=LOGIN priv=0
          1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM_IDLE
                      (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec
                    1w6d: CryptoEngine0: generate hmac context for conn id 2
                         (1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec
     1w6d: ISAKMP (0:2): processing HASH payload. message ID = 1369459046
          1w6d: ISAKMP (0:2): processing SA payload. message ID = 1369459046
                               1w6d: ISAKMP (0:2): Checking IPSec proposal 1
                                        1w6d: ISAKMP: transform 1, ESP_3DES
                                      :1w6d: ISAKMP: attributes in transform
                                     1w6d: ISAKMP: authenticator is HMAC-MD5
                                                1w6d: ISAKMP: encaps is 1
                                       1w6d: ISAKMP: SA life type in seconds
                    1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
                                                1w6d: validate proposal 0
                             1w6d: IPSEC(validate_proposal): transform proposal
                                 prot 3, trans 3, hmac_alg 1) not supported)
                    1w6d: ISAKMP (0:2): atts not acceptable. Next payload is 0
                           (1w6d: ISAKMP (0:2): skipping next ANDed proposal (1
                                1w6d: ISAKMP (0:2): Checking IPSec proposal 2
                                        1w6d: ISAKMP: transform 1, ESP_3DES
                                      :1w6d: ISAKMP: attributes in transform
                                     1w6d: ISAKMP: authenticator is HMAC-SHA
                                                1w6d: ISAKMP: encaps is 1
                                       1w6d: ISAKMP: SA life type in seconds
                    1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
                                                1w6d: validate proposal 0
                                    .1w6d: ISAKMP (0:2): atts are acceptable
                               1w6d: ISAKMP (0:2): Checking IPSec proposal 2
                                  1w6d: ISAKMP (0:2): transform 1, IPPCP LZS
                                      :1w6d: ISAKMP: attributes in transform
                                                1w6d: ISAKMP: encaps is 1
                                       1w6d: ISAKMP: SA life type in seconds
                    1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
                             1w6d: IPSEC(validate_proposal): transform proposal
                                 prot 4, trans 3, hmac_alg 0) not supported)
                    1w6d: ISAKMP (0:2): atts not acceptable. Next payload is 0
                                1w6d: ISAKMP (0:2): Checking IPSec proposal 3
                                        1w6d: ISAKMP: transform 1, ESP_3DES
                                      :1w6d: ISAKMP: attributes in transform
                                     1w6d: ISAKMP: authenticator is HMAC-MD5
                                                1w6d: ISAKMP: encaps is 1
                                       1w6d: ISAKMP: SA life type in seconds
                    1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
                                                1w6d: validate proposal 0
                             1w6d: IPSEC(validate_proposal): transform proposal
                                 prot 3, trans 3, hmac_alg 1) not supported)
                    1w6d: ISAKMP (0:2): atts not acceptable. Next payload is 0
                                1w6d: ISAKMP (0:2): Checking IPSec proposal 4
                                        1w6d: ISAKMP: transform 1, ESP_3DES
                                      :1w6d: ISAKMP: attributes in transform
                                     1w6d: ISAKMP: authenticator is HMAC-SHA
                                                1w6d: ISAKMP: encaps is 1
                                       1w6d: ISAKMP: SA life type in seconds
                    1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
                                                1w6d: validate proposal 0
                                    .1w6d: ISAKMP (0:2): atts are acceptable
                     ,1w6d: IPSEC(validate_proposal_request): proposal part #1
                              ,key eng. msg.) INBOUND local= 172.18.124.158)
    remote= 192.168.60.34, local_proxy= 172.18.124.158/255.255.255.255/0/0
          ,(type=1), remote_proxy= 10.1.1.114/255.255.255.255/0/0 (type=1)
    ,protocol= ESP, transform= esp-3des esp-sha-hmac , lifedur= 0s and 0kb
                            spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
                                                1w6d: validate proposal request 0
```

```
1w6d: ISAKMP (0:2): processing NONCE payload. message ID = 1369459046
1w6d: ISAKMP (0:2): processing ID payload. message ID = 1369459046
1w6d: ISAKMP (0:2): processing ID payload. message ID = 1369459046
1w6d: ISAKMP (0:2): asking for 1 spis from ipsec
1w6d: ISAKMP (0:2): Node 1369459046, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE

...1w6d: IPSEC(key_engine): got a queue event
1w6d: IPSEC(spi_response): getting spi 1640315492 for SA
from 172.18.124.158 to 192.168.60.34 for prot 3
(1w6d: ISAKMP: received ke message (2/1
1w6d: CryptoEngine0: generate hmac context for conn id 2
(1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec
(1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) QM_IDLE
,1w6d: ISAKMP (0:2): Node 1369459046
Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2

1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM_IDLE
(1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec
1w6d: CryptoEngine0: generate hmac context for conn id 2
(1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec
1w6d: ipsec allocate flow 0
1w6d: ipsec allocate flow 0
(1w6d: CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec
(1w6d: CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec
1w6d: ISAKMP (0:2): Creating IPSec SAs
1w6d: inbound SA from 192.168.60.34 to 172.18.124.158
(proxy 10.1.1.114 to 172.18.124.158)
1w6d: has spi 0x61C53A64 and conn_id 200 and flags 4
1w6d: lifetime of 2147483 seconds
1w6d: outbound SA from 172.18.124.158 to 192.168.60.34
( proxy 172.18.124.158 to 10.1.1.114)
1w6d: has spi -1885622177 and conn_id 201 and flags C
1w6d: lifetime of 2147483 seconds
1w6d: ISAKMP (0:2): deleting node 1369459046 error FALSE
"()reason "quick mode done (await
,1w6d: ISAKMP (0:2): Node 1369459046
Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE

...1w6d: IPSEC(key_engine): got a queue event
, :(1w6d: IPSEC(initialize_sas
,key eng. msg.) INBOUND local= 172.18.124.158)
remote= 192.168.60.34, local_proxy= 172.18.124.158/0.0.0.0/0/0
,(type=1), remote_proxy= 10.1.1.114/0.0.0.0/0/0 (type=1)
, protocol= ESP, transform= esp-3des esp-sha-hmac
,(lifedur= 2147483s and 0kb, spi= 0x61C53A64(1640315492
conn_id= 200, keysize= 0, flags= 0x4
(.1w6d: IPSEC(initialize_sas): , (key eng. msg
,OUTBOUND local= 172.18.124.158, remote= 192.168.60.34
,(local_proxy= 172.18.124.158/0.0.0.0/0/0 (type=1
,(remote_proxy= 10.1.1.114/0.0.0.0/0/0 (type=1
, protocol= ESP, transform= esp-3des esp-sha-hmac
,(lifedur= 2147483s and 0kb, spi= 0x8F9BB05F(2409345119
conn_id= 201, keysize= 0, flags= 0xC
,1w6d: IPSEC(create_sa): sa created, (sa) sa_dest= 172.18.124.158
,(sa_prot= 50, sa_spi= 0x61C53A64(1640315492
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 200
,1w6d: IPSEC(create_sa): sa created, (sa) sa_dest= 192.168.60.34
,(sa_prot= 50, sa_spi= 0x8F9BB05F(2409345119
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 201
```

سجلات العميل

لعرض السجلات، قم بتشغيل "عارض السجل" على عميل VPN، وقم بتعيين عامل التصفية إلى *High* لجميع الفئات التي تم تكوينها.

يتم عرض إخراج نموذج السجل هنا.

```
Sev=Info/6 DIALER/0x63300002 06/05/02 11:56:06.609 1
.Initiating connection

Sev=Info/4 CM/0x63100002 06/05/02 11:56:06.609 2
Begin connection process

Sev=Info/4 CM/0x63100004 06/05/02 11:56:06.609 3
      Establish secure connection using Ethernet

Sev=Info/4 CM/0x63100026 06/05/02 11:56:06.609 4
 "Attempt connection with server "172.18.124.158

Sev=Info/6 IKE/0x6300003B 06/05/02 11:56:06.609 5
.Attempting to establish a connection with 172.18.124.158

Sev=Info/4 IKE/0x63000013 06/05/02 11:56:06.669 6
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID) to 172.18.124.158

Sev=Info/5 IKE/0x6300002F 06/05/02 11:56:07.250 7
    Received ISAKMP packet: peer = 172.18.124.158

Sev=Info/4 IKE/0x63000014 06/05/02 11:56:07.250 8
RECEIVING <<< ISAKMP OAK AG (SA, VID, VID, VID, VID, KE, ID, NON, HASH) from
                                                        172.18.124.158

Sev=Info/5 IKE/0x63000059 06/05/02 11:56:07.250 9
Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

Sev=Info/5 IKE/0x63000001 06/05/02 11:56:07.250 10
              Peer is a Cisco-Unity compliant peer

Sev=Info/5 IKE/0x63000059 06/05/02 11:56:07.250 11
Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

Sev=Info/5 IKE/0x63000001 06/05/02 11:56:07.250 12
                                          Peer supports DPD

Sev=Info/5 IKE/0x63000059 06/05/02 11:56:07.250 13
Vendor ID payload = 0A0E5F2A15C0B2F2A41B00897B816B3C

Sev=Info/5 IKE/0x63000059 06/05/02 11:56:07.250 14
              Vendor ID payload = 09002689DFD6B712

Sev=Info/4 IKE/0x63000013 06/05/02 11:56:07.280 15
SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT) to
                                                        172.18.124.158

Sev=Info/5 IKE/0x6300002F 06/05/02 11:56:07.320 16
    Received ISAKMP packet: peer = 172.18.124.158

Sev=Info/4 IKE/0x63000014 06/05/02 11:56:07.320 17
RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:STATUS_RESP_LIFETIME) from
```

```
                                                                  172.18.124.158

                                  Sev=Info/5 IKE/0x63000044 06/05/02 11:56:07.320 18
                                RESPONDER-LIFETIME notify has value of 86400 seconds

                                  Sev=Info/5 IKE/0x63000046 06/05/02 11:56:07.320 19
This SA has already been alive for 1 seconds, setting expiry to 86399 seconds
                                                                       from now

                                  Sev=Info/5 IKE/0x6300002F 06/05/02 11:56:07.561 20
                                       Received ISAKMP packet: peer = 172.18.124.158

                                  Sev=Info/4 IKE/0x63000014 06/05/02 11:56:07.561 21
                    RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.18.124.158

                                   Sev=Info/4 CM/0x63100015 06/05/02 11:56:07.561 22
                                                  Launch xAuth application

                                Sev=Info/4 IPSEC/0x63700014 06/05/02 11:56:07.571 23
                                                            Deleted all keys

                                   Sev=Info/4 CM/0x63100017 06/05/02 11:56:09.734 24
                                                 xAuth application returned

                                  Sev=Info/4 IKE/0x63000013 06/05/02 11:56:09.734 25
                       SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.18.124.158

                                  Sev=Info/5 IKE/0x6300002F 06/05/02 11:56:10.174 26
                                       Received ISAKMP packet: peer = 172.18.124.158

                                  Sev=Info/4 IKE/0x63000014 06/05/02 11:56:10.184 27
                    RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.18.124.158

                                   Sev=Info/4 CM/0x6310000E 06/05/02 11:56:10.184 28
                                  Established Phase 1 SA. 1 Phase 1 SA in the system

                                  Sev=Info/4 IKE/0x63000013 06/05/02 11:56:10.184 29
                       SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.18.124.158

                                  Sev=Info/5 IKE/0x6300005D 06/05/02 11:56:10.204 30
                                   Client sending a firewall request to concentrator

                                  Sev=Info/5 IKE/0x6300005C 06/05/02 11:56:10.204 31
   Firewall Policy: Product=Cisco Integrated Client, Capability= (Centralized
                                                                  .(Policy Push

                                  Sev=Info/4 IKE/0x63000013 06/05/02 11:56:10.204 32
                       SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.18.124.158

                                  Sev=Info/5 IKE/0x6300002F 06/05/02 11:56:10.265 33
                                       Received ISAKMP packet: peer = 172.18.124.158

                                  Sev=Info/4 IKE/0x63000014 06/05/02 11:56:10.265 34
                    RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.18.124.158

                                  Sev=Info/5 IKE/0x63000010 06/05/02 11:56:10.265 35
      MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 10.1.1.114

                                  Sev=Info/5 IKE/0x63000010 06/05/02 11:56:10.265 36
        MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): , value = 10.1.1.10

                                  Sev=Info/5 IKE/0x63000010 06/05/02 11:56:10.265 37
    = MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1) (a.k.a. WINS) : , value
                                                                       10.1.1.20
```

```
                          Sev=Info/5 IKE/0xA3000017 06/05/02 11:56:10.265 38
MODE_CFG_REPLY: The received (INTERNAL_ADDRESS_EXPIRY) attribute and value
                                                    is not supported (86396)

                          Sev=Info/5 IKE/0x6300000E 06/05/02 11:56:10.265 39
                            ,MODE_CFG_REPLY: Attribute = APPLICATION_VERSION
                       value = Cisco Internetwork Operating System Software
              ,IOS (tm) C1700 Software (C1710-K9O3SY-M), Version 12.2(8)T1
                                                    (RELEASE SOFTWARE (fc2
                                          TAC Support: http://www.cisco.com/tac
                               .Copyright (c) 1986-2002 by cisco Systems, Inc
                                          Compiled Sat 30-Mar-02 13:30 by ccai

                          Sev=Info/5 IKE/0x6300000E 06/05/02 11:56:10.265 40
  MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN: , value = cisco.com

                          Sev=Info/5 IKE/0x6300000D 06/05/02 11:56:10.265 41
,(MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets
                                                    value = 0x00000001

                          Sev=Info/5 IKE/0x6300000F 06/05/02 11:56:10.265 42
                                                          SPLIT_NET #1
                                                    subnet = 10.38.0.0
                                                    mask = 255.255.0.0
                                                          protocol = 0
                                                          src port = 0
                                                           dest port=0

                           Sev=Info/4 CM/0x63100019 06/05/02 11:56:10.265 43
                                                 Mode Config data received

                          Sev=Info/5 IKE/0x63000055 06/05/02 11:56:10.275 44
 = Received a key request from Driver for IP address 172.18.124.158, GW IP
                                                              172.18.124.158

                          Sev=Info/4 IKE/0x63000013 06/05/02 11:56:10.275 45
       SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 172.18.124.158

                        Sev=Info/4 IPSEC/0x63700014 06/05/02 11:56:10.575 46
                                                       Deleted all keys

                          Sev=Info/5 IKE/0x6300002F 06/05/02 11:56:10.605 47
                               Received ISAKMP packet: peer = 172.18.124.158

                          Sev=Info/4 IKE/0x63000014 06/05/02 11:56:10.605 48
                        ,RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID
                            NOTIFY:STATUS_RESP_LIFETIME) from 172.18.124.158

                          Sev=Info/5 IKE/0x63000044 06/05/02 11:56:10.605 49
                         RESPONDER-LIFETIME notify has value of 3600 seconds

                          Sev=Info/5 IKE/0x63000045 06/05/02 11:56:10.605 50
                          RESPONDER-LIFETIME notify has value of 4608000 kb

                          Sev=Info/4 IKE/0x63000013 06/05/02 11:56:10.605 51
                         SENDING >>> ISAKMP OAK QM *(HASH) to 172.18.124.158

                          Sev=Info/5 IKE/0x63000058 06/05/02 11:56:10.605 52
Loading IPsec SA (Message ID = 0x51A04966 OUTBOUND SPI = 0x61C53A64 INBOUND
                                                    (SPI = 0x8F9BB05F

                          Sev=Info/5 IKE/0x63000025 06/05/02 11:56:10.605 53
                                                 Loaded OUTBOUND ESP SPI: 0x61C53A64
```

```
Sev=Info/5 IKE/0x63000026 06/05/02 11:56:10.605 54
                Loaded INBOUND ESP SPI: 0x8F9BB05F

Sev=Info/4 CM/0x6310001A 06/05/02 11:56:10.605 55
                One secure connection established

Sev=Info/6 DIALER/0x63300003 06/05/02 11:56:10.625 56
                            .Connection established

Sev=Info/6 DIALER/0x63300008 06/05/02 11:56:10.735 57
 MAPI32 Information - Outlook not default mail client

 Sev=Info/4 IPSEC/0x63700010 06/05/02 11:56:11.677 58
                        Created a new key structure

 Sev=Info/4 IPSEC/0x6370000F 06/05/02 11:56:11.677 59
         Added key with SPI=0x643ac561 into key list

 Sev=Info/4 IPSEC/0x63700010 06/05/02 11:56:11.677 60
                        Created a new key structure

 Sev=Info/4 IPSEC/0x6370000F 06/05/02 11:56:11.677 61
         Added key with SPI=0x5fb09b8f into key list
```

معلومات ذات صلة

- دعم نظام مراقبة الدخول إلى وحدة تحكم الوصول إلى المحطة الطرفية (TACACS+)
- خادم التحكم في الوصول الآمن من Cisco لدعم UNIX
- مصدر المحتوى الإضافي الآمن من Cisco لدعم Windows
- دعم عميل شبكة VPN من Cisco
- دعم مفاوضة IPSec/بروتوكولات IKE
- الدعم التقني والمستندات - Cisco Systems

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