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

المحتويات

المقدمة

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

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

المتطلبات الأساسية

المتطلبات

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

- مجموعة من العناوين التي سيتم تعيينها ل IPSec
- مجموعة تسمى "3000 عميل" باستخدام مفتاح مشترك مسبقا من "Cisco123"
- تفويض المجموعة ومصادقة المستخدم على خادم RADIUS

ملاحظة: ال يتم اعتماد محاسبة RADIUS في الوقت الحالي.

المكونات المستخدمة

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

- موجه 2611 الذي يشغل برنامج Cisco IOS، الإصدار 12.2(8)T.
- مصدر المحتوى الإضافي الآمن من Cisco لنظام التشغيل Windows (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 4.x).

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

هذا إنتاج من العرض صيغة أمر على المسحاج تخدي:

<#root>

vpn2611#

show version

```
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-JK9O3S-M), Version 12.2(8)T,
   RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 14-Feb-02 16:50 by ccai
Image text-base: 0x80008070, data-base: 0x81816184

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

vpn2611 uptime is 1 hour, 15 minutes
System returned to ROM by reload
System image file is "flash:c2600-jk9o3s-mz.122-8.T"

cisco 2611 (MPC860) processor (revision 0x203)
   with 61440K/4096K bytes of memory.
Processor board ID JAD04370EEG (2285146560)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
```

```
TN3270 Emulation software.
2 Ethernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

النظرية الأساسية

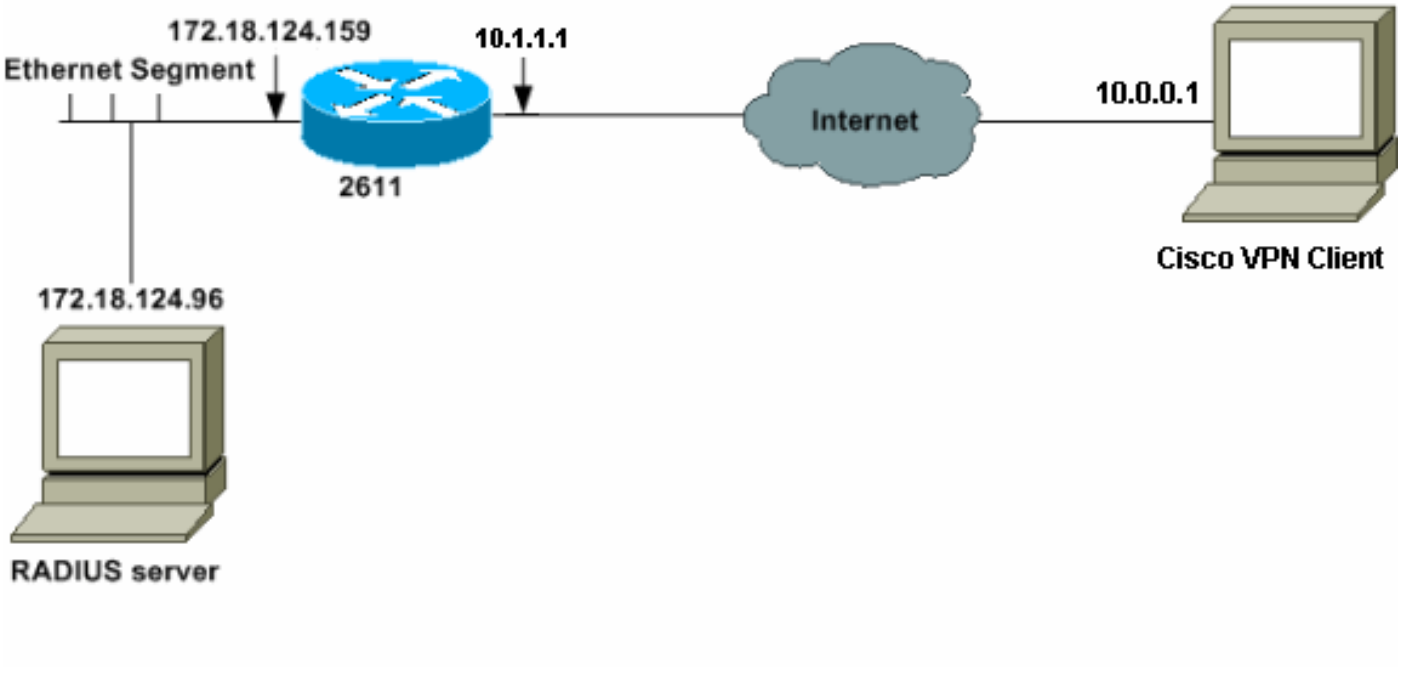
يوضح هذا المستند المصادقة والتفويض، مثل تعيين خدمة تسمية إنترنت في Windows (WINS) وخدمة تسمية المجال (DNS)، بواسطة خادم RADIUS. إذا كنت مهتما بتنفيذ تكوين IPSec بواسطة خادم RADIUS والتخويل المحلي بواسطة الموجه، فارجع إلى مصادقة المستخدم بين موجه Cisco IOS وعميل Cisco VPN الإصدار 4.x ل Windows الذي يستخدم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

التكوين

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



ملاحظة: عناوين IP في هذا المثال ليست قابلة للتوجيه في الإنترنت العالمية لأنها عناوين IP خاصة في شبكة معملية.

التكوينات

الموجه 2611

<#root>

```
vpn2611#
show run

Building configuration...

Current configuration : 1884 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname vpn2611
!

!--- Enable 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" specifies RADIUS user authentication.


aaa authentication login userauthen group radius




!--- In order to enable group authorization,
!--- enable the

aaa authorization

 commands.


aaa authorization network groupauthor group radius


!
!
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 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

!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
!
!

!--- 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 Serial0/0
 no ip address
 shutdown
!
interface Ethernet0/1
 ip address 172.18.124.159 255.255.255.0
 no keepalive
 half-duplex
!
```

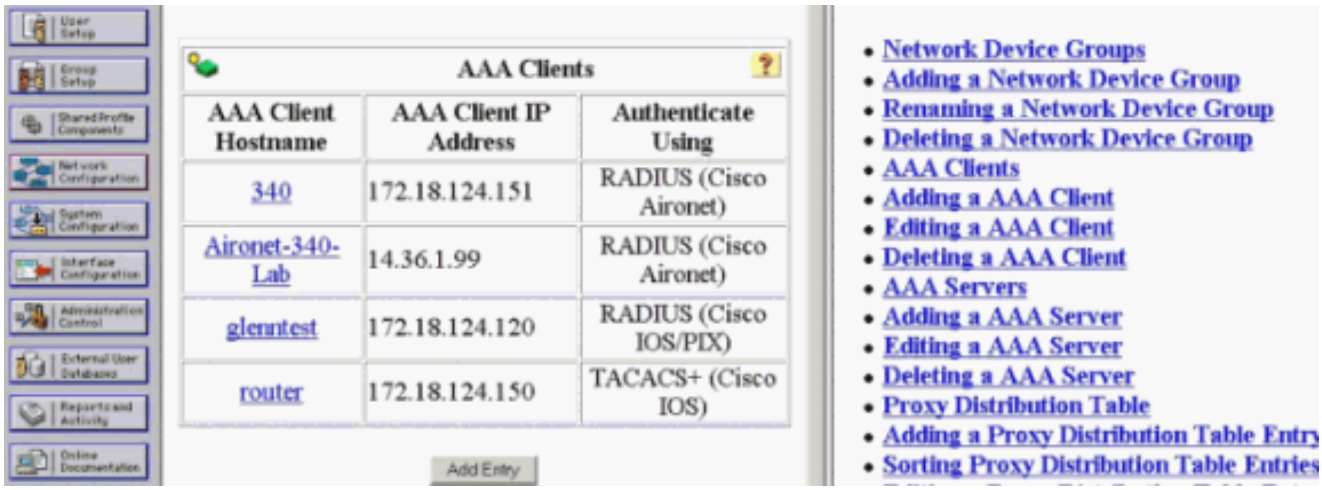
```
!--- Create a pool of addresses to be assigned to the VPN Clients.


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
!

!--- Create an access control list (ACL) if you want to do split tunneling.
!--- This ACL is referenced in the RADIUS profile.



access-list 108 permit ip 172.18.124.0 0.0.255.255 10.16.20.0 0.0.0.255

!

!--- 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
call rsvp-sync

!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
!
end

vpn2611#
```

تكوين خادم RADIUS

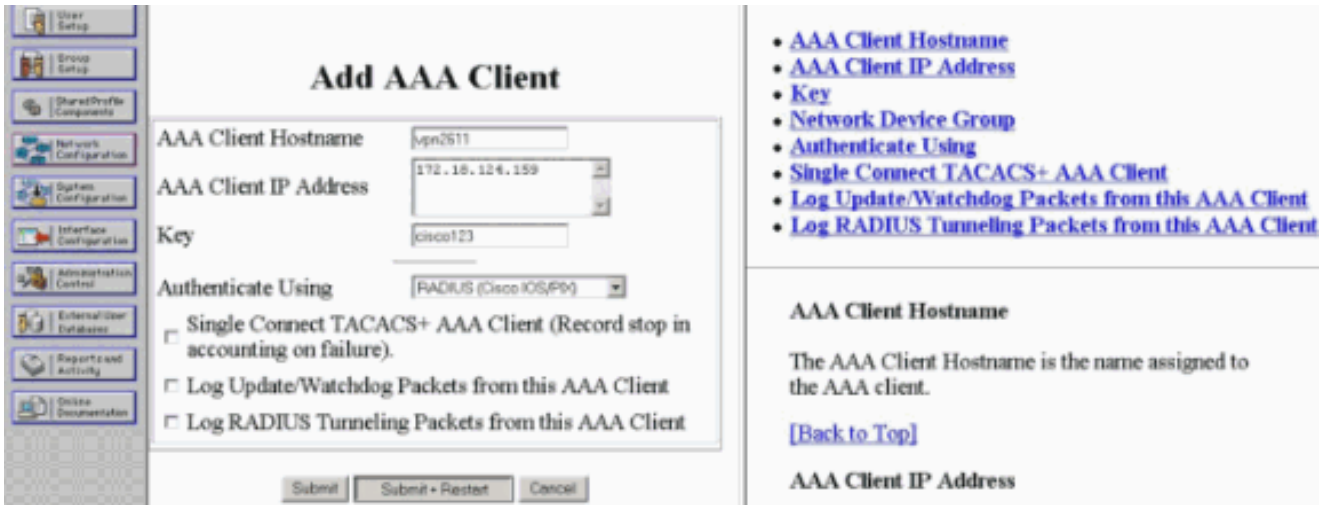
تكوين خادم RADIUS لعملاء AAA (الموجه)

أكمل الخطوات التالية:

1. انقر فوق إضافة إدخال للإضافة الموجه إلى قاعدة بيانات خادم RADIUS.



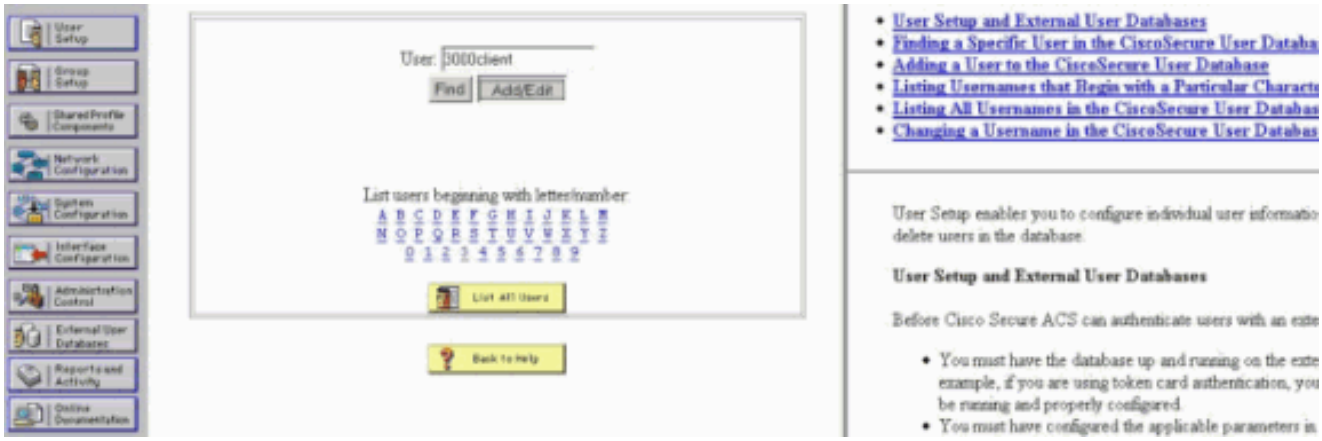
2. حدد عنوان IP الخاص بالموجه "172.18.124.159" مع المفتاح السري المشترك "Cisco123" واختر RADIUS في المربع المنسدل Authenticate باستخدام.



تكوين خادم RADIUS لمصادقة المجموعة وترخيصها

أكمل الخطوات التالية:

1. انقر فوق إضافة/تحرير لإضافة مستخدم باسم 3000 عميل إلى خادم RADIUS.

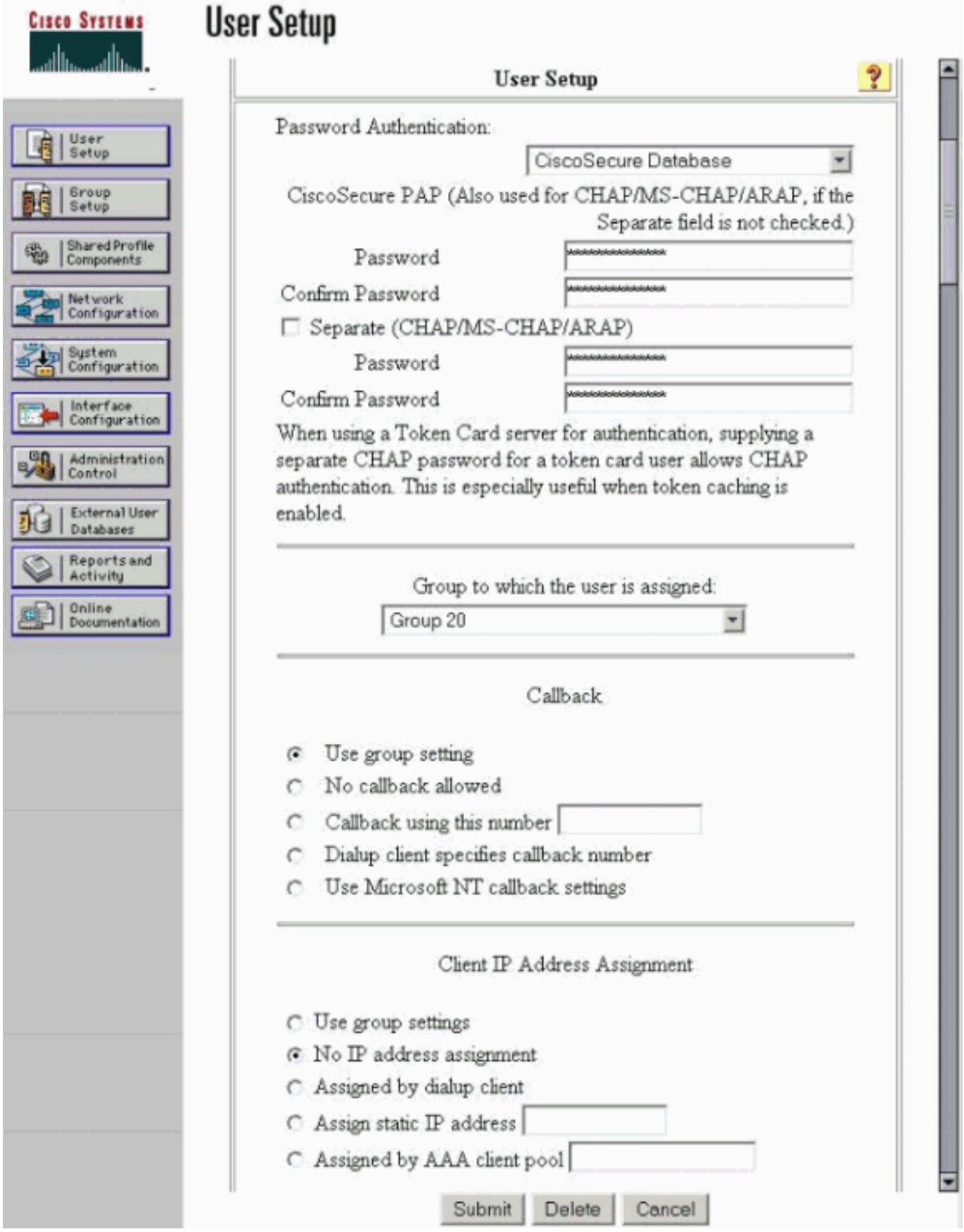


2. قبل الإصدار 15.8.3 من برنامج Cisco IOS Software والإصدار 16.9.1 من برنامج Cisco IOS XE Software، كانت كلمة المرور هذه كلمة أساسية خاصة ل Cisco IOS، والتي تشير إلى

ملف تعريف مجموعة يجب الإشارة إليها. يمكنك تعيين المستخدم إلى مجموعة Cisco
الآمنة إذا كنت تفضل ذلك. تأكد من عدم إختيار تعيين عنوان IP.

بعد الإصدار 15.8.3 من برنامج Cisco IOS Software وبرنامج Cisco IOS XE الإصدار 16.9.1،
يحتاج تفويض AAA إلى كلمة مرور ويكون إلزامي. يوصى بتعريف كلمة المرور
المستخدمة عبر الأمر <secret>isakmp authorization list aaa_list1 password.

ثم يقوم المسؤول بتكوين كلمة المرور <secret> المطابقة على خادم RADIUS.



3. حدد معلمات تخويل المجموعة التي سيتم تمريرها بواسطة حساب المستخدم هذا مرة أخرى إلى عميل VPN.

تأكد من تمكين زوج Cisco-AV مع هذه السمات:

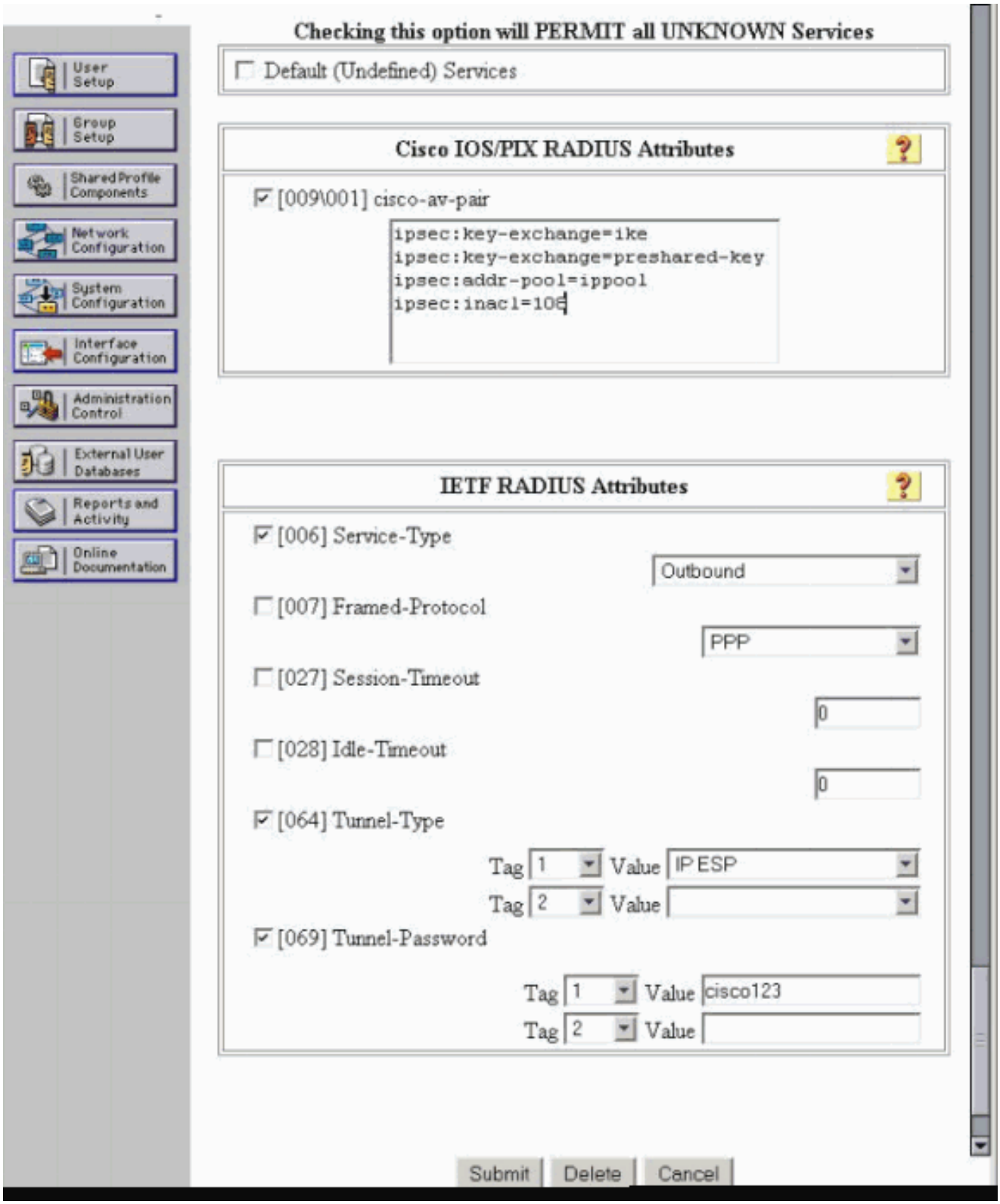
- ipsSec:Key-exchange=ike

- ips:key-exchange=preshared-key
- ipsSec:addr-pool=ippool
- ipsSec:inacl=108 (يلزم فقط إذا كنت تستخدم تقسيم الاتصال النفقي على الموجه)

أيضا، تأكد من أن لديك خصائص IETF RADIUS هذه ممكنة:

- السمة 6: service-type=outbound
- السمة 64: نوع النفق=ip esp
- السمة 69: tunnel-password=cisco123 (هذه هي كلمة مرور مجموعتك على عميل VPN)

بمجرد الانتهاء، انقر فوق إرسال.



تحت سمات محددة للمورد، يمكنك أيضا تمكين هذه السمات الاختيارية:

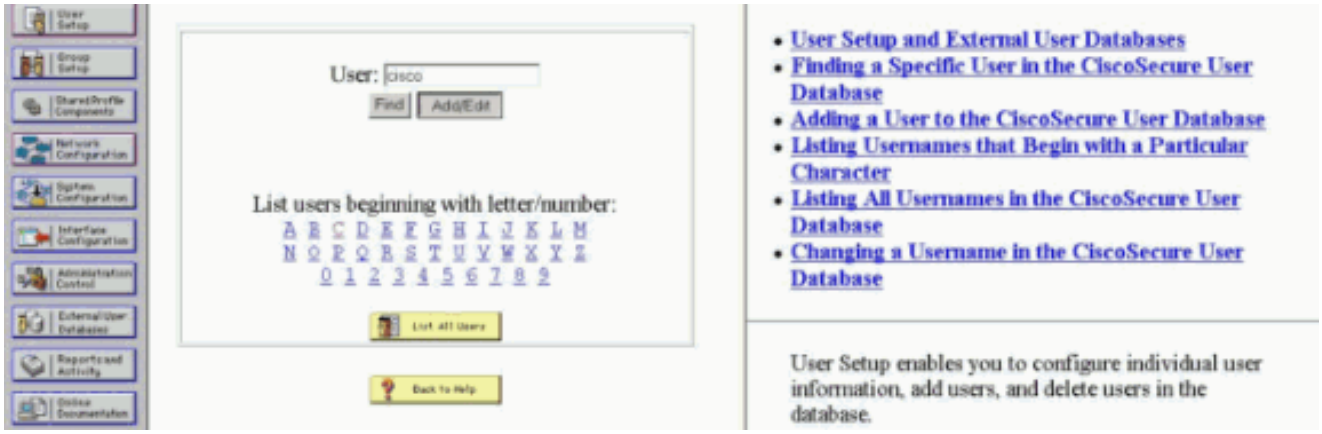
- ipsSec:default-domain=
- ipsEc:المجال=
- ipsSec:idletime=
- IPSec:خوادم DNS=
- ipsSec:wins-servers=

تكوين خادم RADIUS لمصادقة المستخدم

أكمل الخطوات التالية:

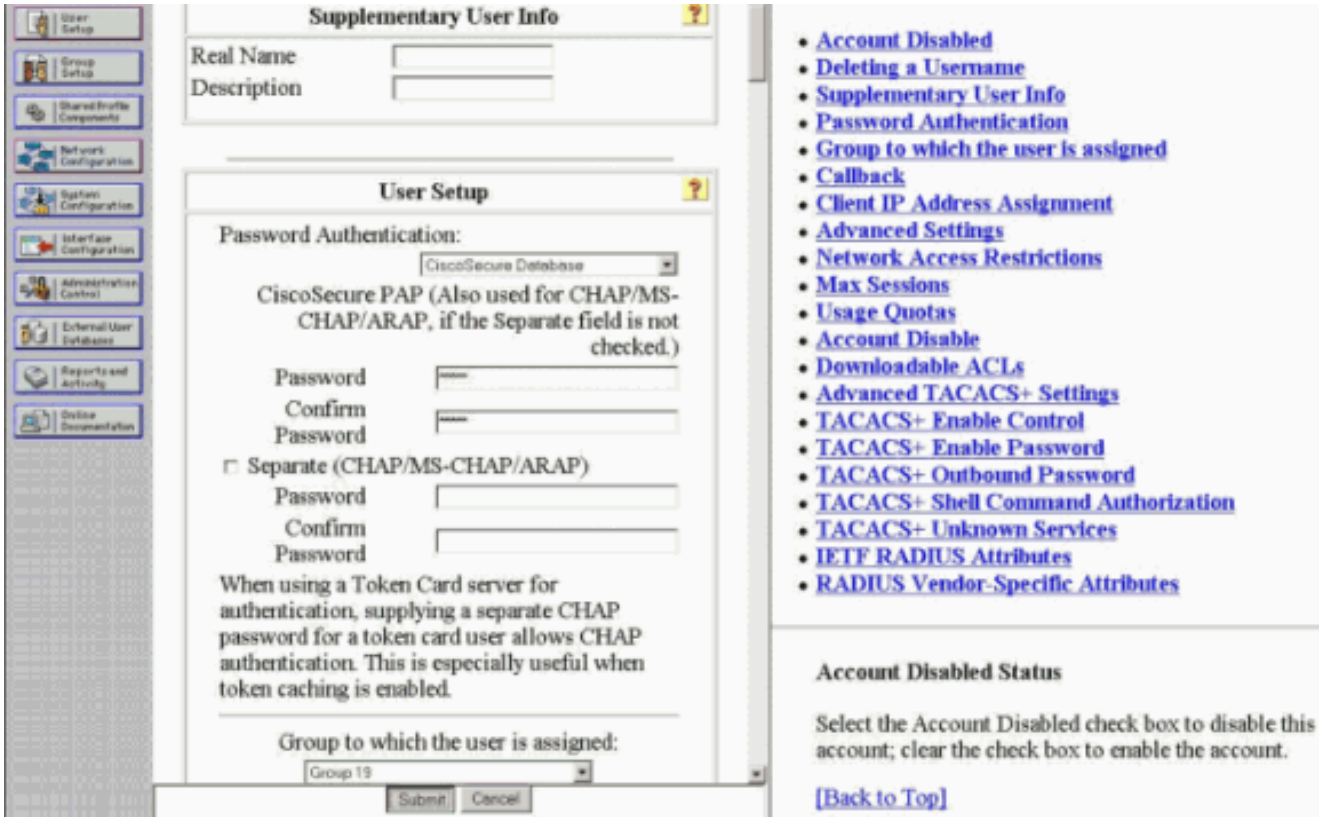
1. طقطقة يضيف/يحرر أن يضيف ال VPN مستعمل في ال cisco أمن قاعدة معطيات.

   في هذا مثال، ال username cisco.



2. على الإطار التالي، عينت الكلمة للمستخدم cisco. كلمة أيضا cisco.

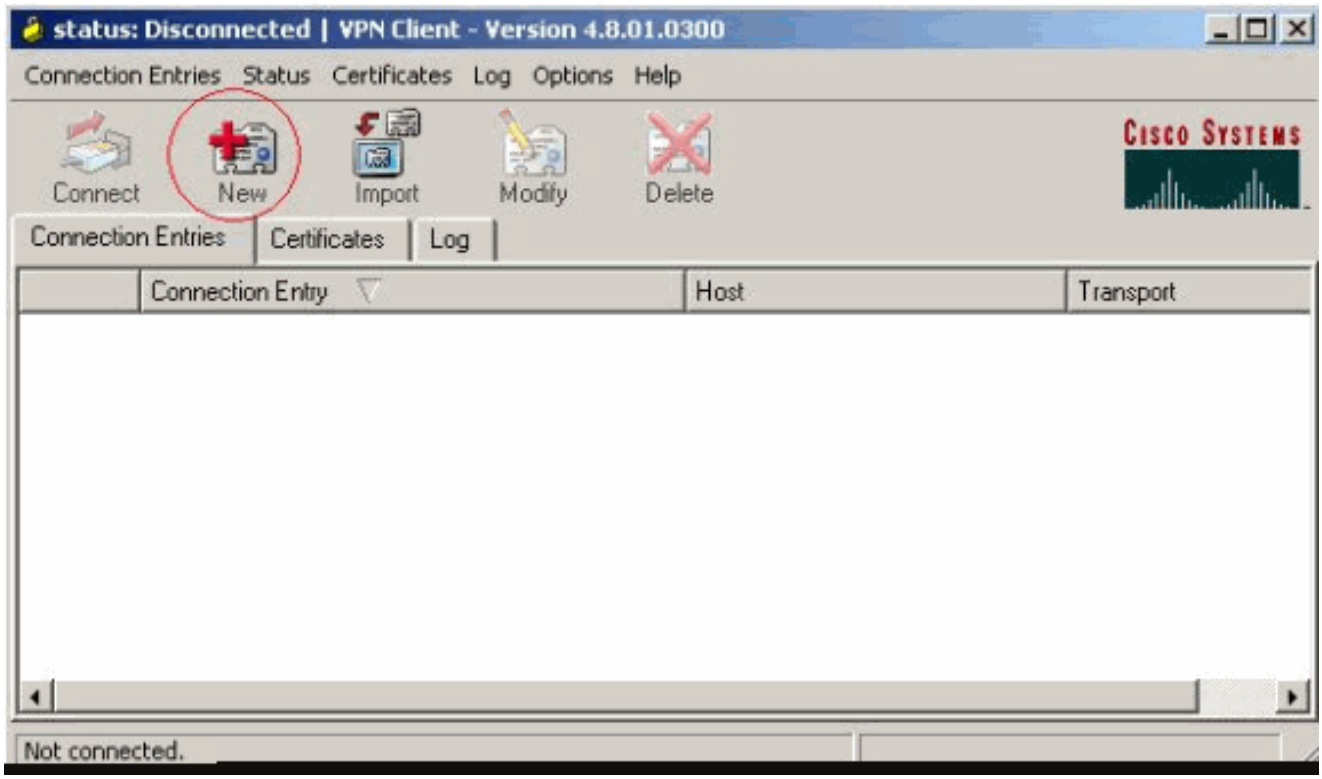
   يمكنك تعيين حساب المستخدم إلى مجموعة. بمجرد الانتهاء، انقر فوق إرسال.



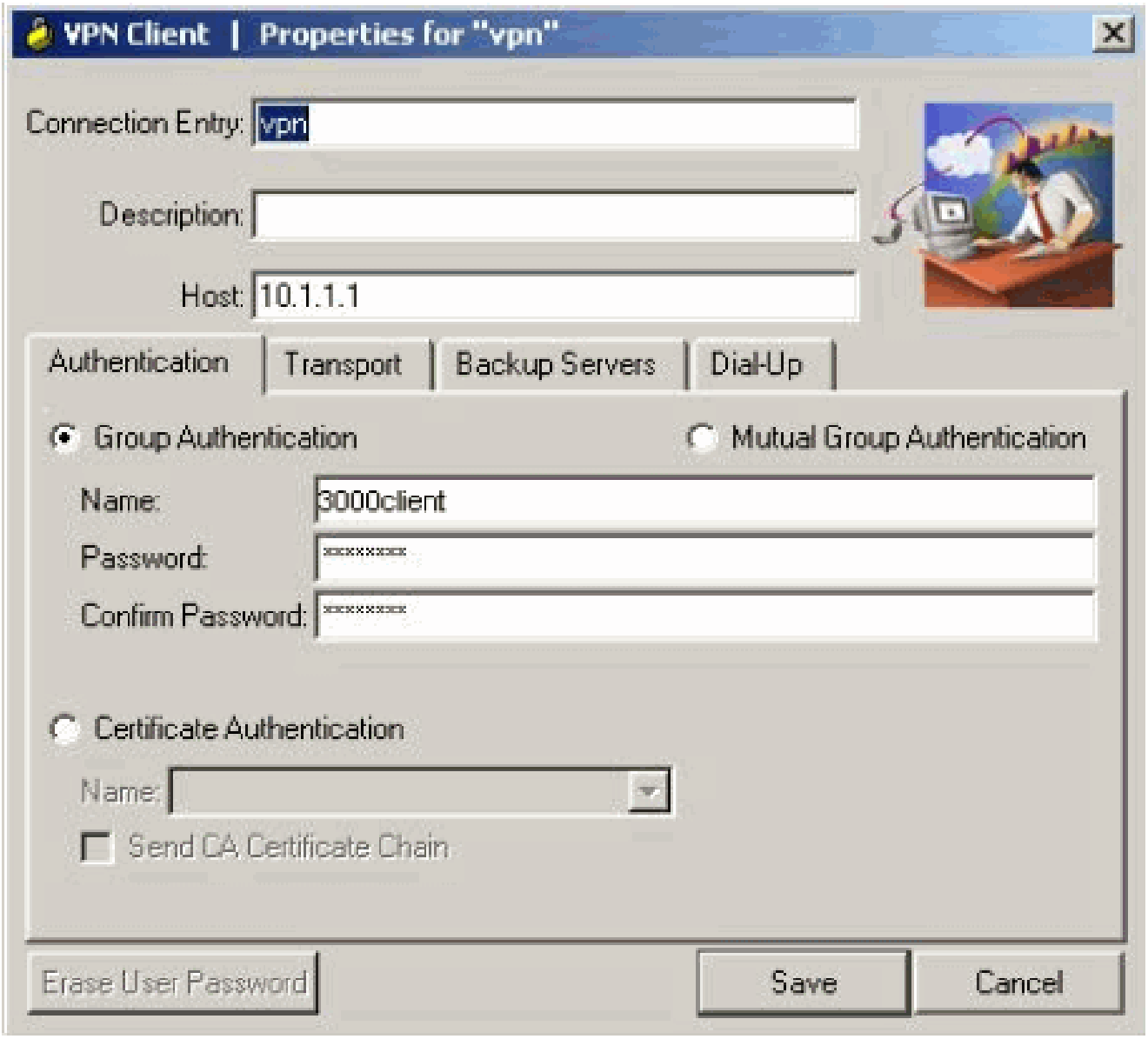
تكوين VPN Client 4.8

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

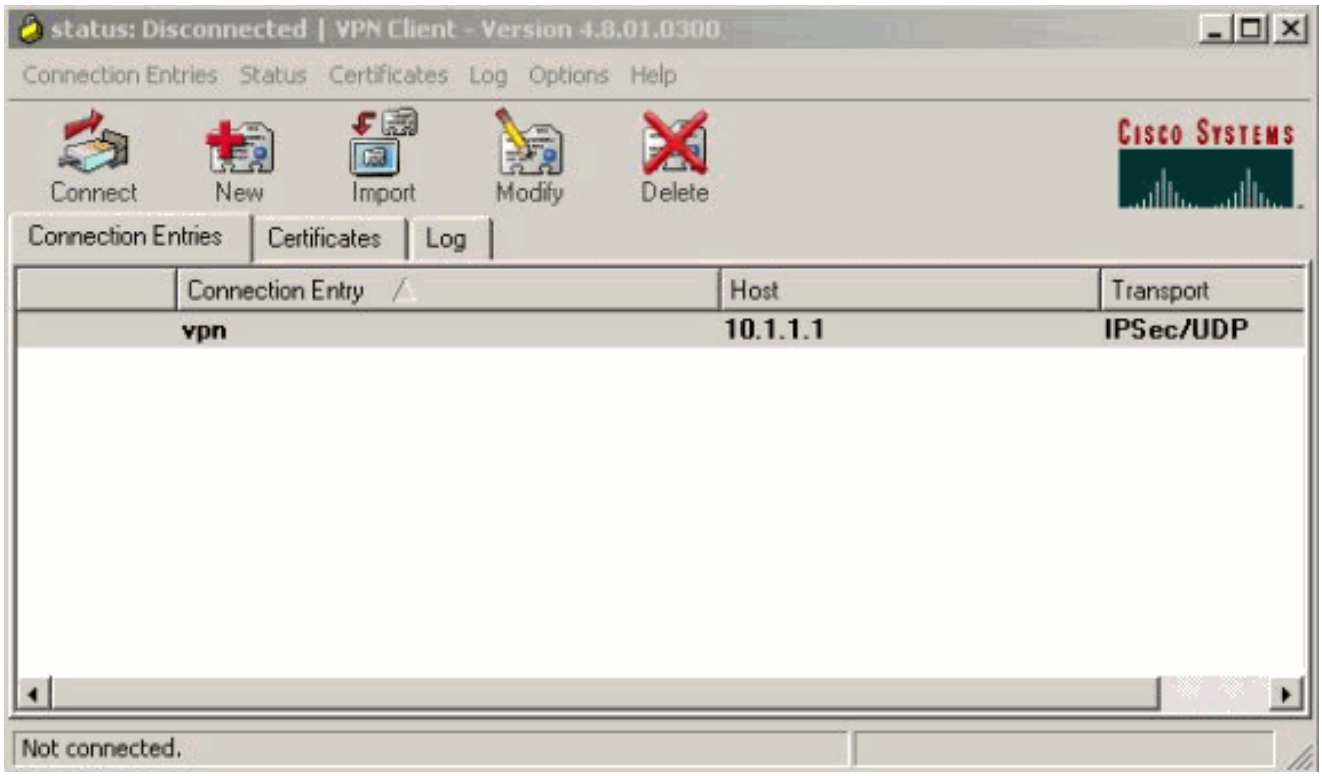
1. أخترت بداية>برنامج>Cisco Systems VPN زبون>VPN زبون.
2. انقر على جديد لتشغيل الإطار "إنشاء اتصال VPN جديد".



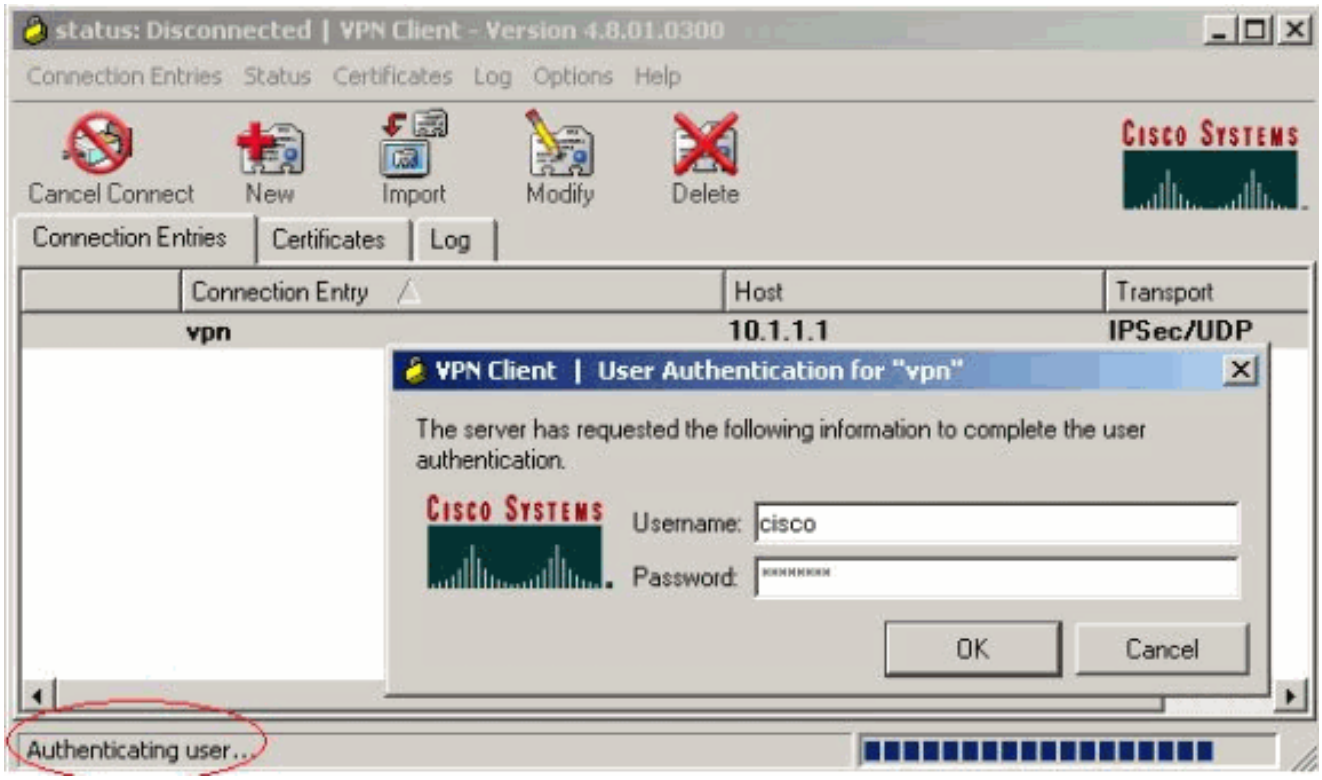
3. أدخل اسم "إدخال الاتصال" مع وصف. أدخل عنوان IP الخارجي للموجه في المربع المضيف. بعد ذلك، أدخل اسم مجموعة VPN وكلمة المرور وانقر على حفظ.



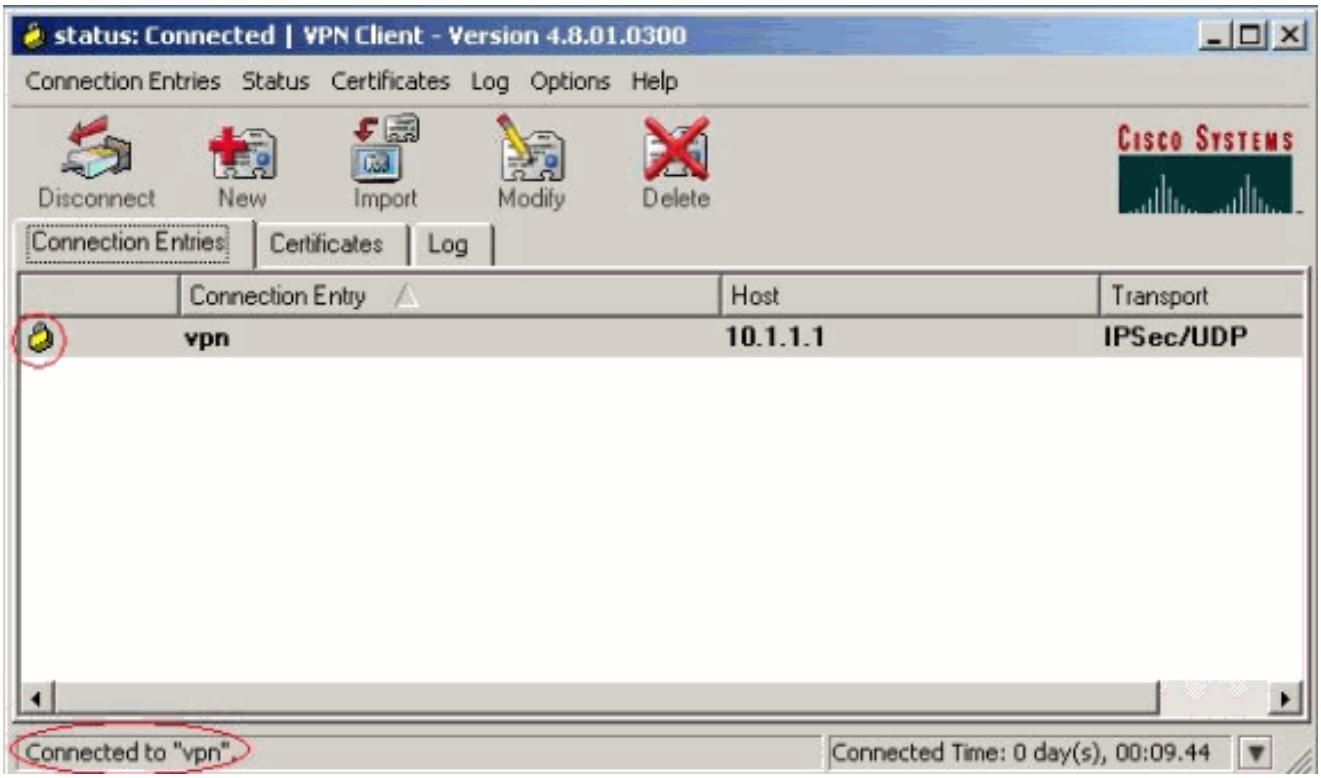
4. انقر على الاتصال الذي تريد إستخدامه وانقر فوق الاتصال من الإطار الرئيسي لعميل شبكة VPN.



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



يتم اتصال عميل شبكة VPN بالموجه في الموقع المركزي.



التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

<#root>

vpn2611#

show crypto isakmp sa

dst src state conn-id slot
10.1.1.1 10.0.0.1

QM_IDLE

3 0

vpn2611#

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:


vpn2611#
show crypto engine connections active

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

استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

ارجع إلى معلومات مهمة عن أوامر تصحيح الأخطاء قبل أن تستخدم 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 كل النهايتين.
- debug crypto engine—يعرض معلومات من محرك التشفير.
- debug aaa authentication— يعرض معلومات حول مصادقة AAA/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

<#root>

vpn2611#

show debug

General OS:

AAA Authorization debugging is on
Radius protocol debugging is on
Radius packet protocol debugging is on

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

vpn2611#

1w0d: ISAKMP (0:0): received packet from 10.0.0.1 (N) NEW SA

1w0d: ISAKMP: local port 500, remote port 500
1w0d: ISAKMP (0:2): (Re)Setting client xauth list userauthen and state
1w0d: ISAKMP: Locking CONFIG struct 0x830BF118 from
crypto_ikmp_config_initialize_sa, count 2
1w0d: ISAKMP (0:2): processing SA payload. message ID = 0
1w0d: ISAKMP (0:2): processing ID payload. message ID = 0
1w0d: ISAKMP (0:2): processing vendor id payload
1w0d: ISAKMP (0:2): vendor ID seems Unity/DPD but bad major
1w0d: ISAKMP (0:2): vendor ID is XAUTH
1w0d: ISAKMP (0:2): processing vendor id payload
1w0d: ISAKMP (0:2): vendor ID is DPD
1w0d: ISAKMP (0:2): processing vendor id payload
1w0d: ISAKMP (0:2): vendor ID is Unity
1w0d: ISAKMP (0:2): Checking ISAKMP transform 1 against priority 3 policy
1w0d: ISAKMP: encryption 3DES-CBC
1w0d: ISAKMP: hash SHA
1w0d: ISAKMP: default group 2
1w0d: ISAKMP: auth XAUTHInitPreShared
1w0d: ISAKMP: life type in seconds
1w0d: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B

1w0d: ISAKMP (0:2): atts are acceptable. Next payload is 3

1w0d: ISAKMP (0:2): processing KE payload. message ID = 0
1w0d: ISAKMP (0:2): processing NONCE payload. message ID = 0
1w0d: ISAKMP (0:2): processing vendor id payload
1w0d: ISAKMP (0:2): processing vendor id payload
1w0d: ISAKMP (0:2): processing vendor id payload
1w0d: AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-1
1w0d: AAA/MEMORY: create_user (0x830CAF28) 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'
1w0d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT

1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552):

```
Port='ISAKMP-ID-AUTH' list='groupauthor' service=NET
1w0d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(66832552) user='3000client'
1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): send AV service=ike
1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): send AV
protocol=ipsec

1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): found list
"groupauthor"
1w0d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(66832552): Method=radius

(radius)
1w0d: RADIUS: authenticating to get author data
1w0d: RADIUS: ustruct sharecount=3
1w0d: Radius: radius_port_info() success=0 radius_nas_port=1

1w0d: RADIUS: Send to ISAKMP-ID-AUTH id 60 172.18.124.96:1645,
Access-Request, len 83

1w0d: RADIUS: authenticator AF EC D3 AD D6 39 4F 7D - A0 5E FC 64 F5 DE
A7 3B
1w0d: RADIUS: NAS-IP-Address [4] 6 172.18.124.159
1w0d: RADIUS: NAS-Port-Type [61] 6 Async [0]

1w0d: RADIUS: User-Name [1] 12 "3000client"

1w0d: RADIUS: Calling-Station-Id [31] 15 "10.0.0.1"
1w0d: RADIUS: User-Password [2] 18 *
1w0d: RADIUS: Service-Type [6] 6 Outbound [5]

1w0d: RADIUS: Received from id 60 172.18.124.96:1645, Access-Accept, len
176

1w0d: RADIUS: authenticator 52 BA 0A 38 AC C2 2B 6F - A0 77 64 93 D6 19
78 CF
1w0d: RADIUS: Service-Type [6] 6 Outbound [5]
1w0d: RADIUS: Vendor, Cisco [26] 30
1w0d: RADIUS: Cisco AVpair [1] 24 "ipsec:key-exchange=ike"
1w0d: RADIUS: Vendor, Cisco [26] 40
1w0d: RADIUS: Cisco AVpair [1] 34 "ipsec:key-exchange=preshared-key"
1w0d: RADIUS: Vendor, Cisco [26] 30
1w0d: RADIUS: Cisco AVpair [1] 24 "ipsec:addr-pool=ippool"
1w0d: RADIUS: Vendor, Cisco [26] 23
1w0d: RADIUS: Cisco AVpair [1] 17 "ipsec:inacl=108"
1w0d: RADIUS: Tunnel-Type [64] 6 01:ESP [9]
1w0d: RADIUS: Tunnel-Password [69] 21 *
1w0d: RADIUS: saved authorization data for user 830CAF28 at 83198648

1w0d: RADIUS: cisco AVPair "ipsec:key-exchange=ike"
1w0d: RADIUS: cisco AVPair "ipsec:key-exchange=preshared-key"
1w0d: RADIUS: cisco AVPair "ipsec:addr-pool=ippool"
1w0d: RADIUS: cisco AVPair "ipsec:inacl=108"
1w0d: RADIUS: Tunnel-Type, [01] 00 00 09
1w0d: RADIUS: TAS(1) created and enqueued.
1w0d: RADIUS: Tunnel-Password decrypted, [01] cisco123

1w0d: RADIUS: TAS(1) takes precedence over tagged attributes,
tunnel_type=esp
1w0d: RADIUS: free TAS(1)
1w0d: AAA/AUTHOR (66832552): Post authorization status = PASS_REPL
1w0d: ISAKMP: got callback 1
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
AAA/AUTHOR/IKE: Processing AV key-exchange=preshared-key
AAA/AUTHOR/IKE: Processing AV addr-pool=ippool
AAA/AUTHOR/IKE: Processing AV inacl=108
AAA/AUTHOR/IKE: Processing AV tunnel-type*esp
```

```
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
AAA/AUTHOR/IKE: Processing AV tunnel-tag*1
1w0d: ISAKMP (0:2): SKEYID state generated
1w0d: ISAKMP (0:2): SA is doing pre-shared key authentication plux XAUTH
using id type ID_IPV4_ADDR
1w0d: ISAKMP (2): ID payload
next-payload : 10
type : 1
protocol : 17
port : 500
length : 8
1w0d: ISAKMP (2): Total payload length: 12
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) AG_INIT_EXCH
1w0d: ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY
Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2

1w0d: AAA/MEMORY: free_user (0x830CAF28) user='3000client' ruser='NULL'
port='ISAKMP-ID-AUTH' rem_addr='10.0.0.1' authen_type=NONE
service=LOGIN priv=0
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) AG_INIT_EXCH
1w0d: ISAKMP (0:2): processing HASH payload. message ID = 0
1w0d: ISAKMP (0:2): processing NOTIFY INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 831938B0
1w0d: ISAKMP (0:2): Process initial contact, bring down existing phase 1
and 2 SA's
1w0d: ISAKMP (0:2): returning IP addr to the address pool: 10.16.20.1
1w0d: ISAKMP (0:2): returning address 10.16.20.1 to pool
1w0d: ISAKMP (0:2): peer does not do paranoid keepalives.

1w0d: ISAKMP (0:2): SA has been authenticated with 10.0.0.1
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) QM_IDLE
1w0d: ISAKMP (0:2): purging node -1377537628
1w0d: ISAKMP: Sending phase 1 responder lifetime 86400

1w0d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE

1w0d: IPSEC(key_engine): got a queue event...
1w0d: IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
1w0d: IPSEC(key_engine_delete_sas): delete all SAs shared with
10.0.0.1
1w0d: ISAKMP (0:2): Need XAUTH
1w0d: AAA: parse name=ISAKMP idb type=-1 tty=-1
1w0d: AAA/MEMORY: create_user (0x830CAF28) 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'
1w0d: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT

1w0d: ISAKMP: got callback 1
1w0d: ISAKMP/xauth: request attribute XAUTH_TYPE_V2
1w0d: ISAKMP/xauth: request attribute XAUTH_MESSAGE_V2
1w0d: ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
1w0d: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
1w0d: ISAKMP (0:2): initiating peer config to 10.0.0.1. ID =
-1021889193
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) CONF_XAUTH
1w0d: 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

1w0d: ISAKMP (0:1): purging node 832238598
```

```
1w0d: ISAKMP (0:1): purging node 1913225491
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) CONF_XAUTH
1w0d: ISAKMP (0:2): processing transaction payload from 10.0.0.1.
message ID = -1021889193
1w0d: ISAKMP: Config payload REPLY
1w0d: ISAKMP/xauth: reply attribute XAUTH_TYPE_V2 unexpected
1w0d: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2
1w0d: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
1w0d: ISAKMP (0:2): deleting node -1021889193 error FALSE reason "done
with xauth request/reply exchange"
1w0d: 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

1w0d: RADIUS: ustruct sharecount=2
1w0d: Radius: radius_port_info() success=0 radius_nas_port=1

1w0d: RADIUS: Send to ISAKMP id 61 172.18.124.96:1645, Access-Request, len 72

1w0d: RADIUS: authenticator 98 12 4F C0 DA B9 48 B8 - 58 00 BA 14 08 8E
87 C0
1w0d: RADIUS: NAS-IP-Address [4] 6 172.18.124.159
1w0d: RADIUS: NAS-Port-Type [61] 6 Async [0]

1w0d: RADIUS: User-Name [1] 7 "cisco"

1w0d: RADIUS: Calling-Station-Id [31] 15 "10.0.0.1"
1w0d: RADIUS: User-Password [2] 18 *

1w0d: RADIUS: Received from id 61 172.18.124.96:1645, Access-Accept, len 26

1w0d: RADIUS: authenticator 00 03 F4 E1 9C 61 3F 03 - 54 83 E8 27 5C 6A
7B 6E
1w0d: RADIUS: Framed-IP-Address [8] 6 255.255.255.255
1w0d: RADIUS: saved authorization data for user 830CAF28 at 830F89F8
1w0d: ISAKMP: got callback 1
1w0d: ISAKMP (0:2): initiating peer config to 10.0.0.1. ID =
-547189328
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) CONF_XAUTH
1w0d: 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

1w0d: AAA/MEMORY: free_user (0x830CAF28) user='cisco' ruser='NULL'
port='ISAKMP' rem_addr='10.0.0.1' authen_type=ASCII service=LOGIN
priv=0
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) CONF_XAUTH
1w0d: ISAKMP (0:2): processing transaction payload from 10.0.0.1.
message ID = -547189328
1w0d: ISAKMP: Config payload ACK
1w0d: ISAKMP (0:2): XAUTH ACK Processed
1w0d: ISAKMP (0:2): deleting node -547189328 error FALSE reason "done with
transaction"
1w0d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK
Old State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE

1w0d: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM_IDLE
1w0d: ISAKMP (0:2): processing transaction payload from 10.0.0.1.
message ID = -1911189201
1w0d: ISAKMP: Config payload REQUEST
1w0d: ISAKMP (0:2): checking request:
1w0d: ISAKMP: IP4_ADDRESS
1w0d: ISAKMP: IP4_NETMASK
```

```
1w0d: ISAKMP: IP4_DNS
1w0d: ISAKMP: IP4_NBNS
1w0d: ISAKMP: ADDRESS_EXPIRY
1w0d: ISAKMP: APPLICATION_VERSION
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7000
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7001
1w0d: ISAKMP: DEFAULT_DOMAIN
1w0d: ISAKMP: SPLIT_INCLUDE
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7007
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7008
1w0d: ISAKMP: UNKNOWN Unknown Attr: 0x7005
1w0d: AAA: parse name=ISAKMP-GROUP-AUTH idb type=-1 tty=-1
1w0d: AAA/MEMORY: create_user (0x830CAF28) 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'
1w0d: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST
Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT

1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746):
Port='ISAKMP-GROUP-AUTH' list='groupauthor' service=NET
1w0d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-GROUP-AUTH(3098118746)
user='3000client'
1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): send AV
service=ike
1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): send AV
protocol=ipsec
1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): found list
"groupauthor"
1w0d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(3098118746): Method=radius
(radius)
1w0d: RADIUS: authenticating to get author data
1w0d: RADIUS: ustruct sharecount=3
1w0d: Radius: radius_port_info() success=0 radius_nas_port=1
1w0d: RADIUS: Send to ISAKMP-GROUP-AUTH id 62 172.18.124.96:1645,
Access-Request, len 83
1w0d: RADIUS: authenticator 32 C5 32 FF AB B7 E4 68 - 9A 68 5A DE D5 56
0C BE
1w0d: RADIUS: NAS-IP-Address [4] 6 172.18.124.159
1w0d: RADIUS: NAS-Port-Type [61] 6 Async [0]
1w0d: RADIUS: User-Name [1] 12 "3000client"
1w0d: RADIUS: Calling-Station-Id [31] 15 "10.0.0.1"
1w0d: RADIUS: User-Password [2] 18 *
1w0d: RADIUS: Service-Type [6] 6 Outbound [5]
1w0d: RADIUS: Received from id 62 172.18.124.96:1645, Access-Accept, len
176
1w0d: RADIUS: authenticator DF FA FE 21 07 92 4F 10 - 75 5E D6 96 66 70
19 27
1w0d: RADIUS: Service-Type [6] 6 Outbound [5]
1w0d: RADIUS: Vendor, Cisco [26] 30
1w0d: RADIUS: Cisco AVpair [1] 24 "ipsec:key-exchange=ike"
1w0d: RADIUS: Vendor, Cisco [26] 40
1w0d: RADIUS: Cisco AVpair [1] 34
"ipsec:key-exchange=preshared-key"
1w0d: RADIUS: Vendor, Cisco [26] 30
1w0d: RADIUS: Cisco AVpair [1] 24 "ipsec:addr-pool=ippool"
1w0d: RADIUS: Vendor, Cisco [26] 23
1w0d: RADIUS: Cisco AVpair [1] 17 "ipsec:inacl=108"
1w0d: RADIUS: Tunnel-Type [64] 6 01:ESP [9]
1w0d: RADIUS: Tunnel-Password [69] 21 *
1w0d: RADIUS: saved authorization data for user 830CAF28 at 83143E64
1w0d: RADIUS: cisco AVPair "ipsec:key-exchange=ike"
1w0d: RADIUS: cisco AVPair "ipsec:key-exchange=preshared-key"
```

```
1w0d: RADIUS: cisco AVPair "ipsec:addr-pool=ippool"
1w0d: RADIUS: cisco AVPair "ipsec:inacl=108"
1w0d: RADIUS: Tunnel-Type, [01] 00 00 09
1w0d: RADIUS: TAS(1) created and enqueued.
1w0d: RADIUS: Tunnel-Password decrypted, [01] cisco123
1w0d: RADIUS: TAS(1) takes precedence over tagged attributes,
tunnel_type=esp
1w0d: RADIUS: free TAS(1)
1w0d: AAA/AUTHOR (3098118746): Post authorization status = PASS_REPL
1w0d: ISAKMP: got callback 1
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
AAA/AUTHOR/IKE: Processing AV key-exchange=preshared-key
AAA/AUTHOR/IKE: Processing AV addr-pool=ippool
AAA/AUTHOR/IKE: Processing AV inacl=108
AAA/AUTHOR/IKE: Processing AV tunnel-type*esp
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
AAA/AUTHOR/IKE: Processing AV tunnel-tag*1
1w0d: ISAKMP (0:2): attributes sent in message:
1w0d: Address: 0.2.0.0
1w0d: ISAKMP (0:2): allocating address 10.16.20.2
1w0d: ISAKMP: Sending private address: 10.16.20.2
1w0d: ISAKMP: Unknown Attr: IP4_NETMASK (0x2)
1w0d: ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address:
86395
1w0d: ISAKMP: Sending APPLICATION_VERSION string: Cisco Internetwork
Operating System Software
IOS (tm) C2600 Software (C2600-JK9O3S-M), Version 12.2(8)T, RELEASE
SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 14-Feb-02 16:50 by ccai
1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7000)
1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7001)
1w0d: ISAKMP: Sending split include name 108 network 14.38.0.0 mask
255.255.0.0 protocol 0, src port 0, dst port 0

1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7007)
1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7008)
1w0d: ISAKMP: Unknown Attr: UNKNOWN (0x7005)
1w0d: ISAKMP (0:2): responding to peer config from 10.0.0.1. ID =
-1911189201
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) CONF_ADDR
1w0d: ISAKMP (0:2): deleting node -1911189201 error FALSE reason ""
1w0d: ISAKMP (0:2): Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR
Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE

1w0d: AAA/MEMORY: free_user (0x830CAF28) user='3000client' ruser='NULL'
port='ISAKMP-GROUP-AUTH' rem_addr='10.0.0.1' authen_type=NONE
service=LOGIN priv=0
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM_IDLE
1w0d: ISAKMP (0:2): processing HASH payload. message ID = 132557281
1w0d: ISAKMP (0:2): processing SA payload. message ID = 132557281
1w0d: ISAKMP (0:2): Checking IPSec proposal 1
1w0d: ISAKMP: transform 1, ESP_3DES
1w0d: ISAKMP: attributes in transform:
1w0d: ISAKMP: authenticator is HMAC-MD5
1w0d: ISAKMP: encaps is 1
1w0d: ISAKMP: SA life type in seconds
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w0d: IPSEC(validate_proposal): transform proposal (prot 3, trans 3,
hmac_alg 1) not supported
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0
```

```
1w0d: ISAKMP (0:2): skipping next ANDed proposal (1)
1w0d: ISAKMP (0:2): Checking IPSec proposal 2
1w0d: ISAKMP: transform 1, ESP_3DES
1w0d: ISAKMP: attributes in transform:
1w0d: ISAKMP: authenticator is HMAC-SHA
1w0d: ISAKMP: encaps is 1
1w0d: ISAKMP: SA life type in seconds
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w0d: ISAKMP (0:2): atts are acceptable.
1w0d: ISAKMP (0:2): Checking IPSec proposal 2
1w0d: ISAKMP (0:2): transform 1, IPPCP LZS
1w0d: ISAKMP: attributes in transform:
1w0d: ISAKMP: encaps is 1
1w0d: ISAKMP: SA life type in seconds
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w0d: IPSEC(validate_proposal): transform proposal (prot 4, trans 3,
hmac_alg 0) not supported
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0
1w0d: ISAKMP (0:2): Checking IPSec proposal 3
1w0d: ISAKMP: transform 1, ESP_3DES
1w0d: ISAKMP: attributes in transform:
1w0d: ISAKMP: authenticator is HMAC-MD5
1w0d: ISAKMP: encaps is 1
1w0d: ISAKMP: SA life type in seconds
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w0d: IPSEC(validate_proposal): transform proposal (prot 3, trans 3,
hmac_alg 1) not supported
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0
1w0d: ISAKMP (0:2): Checking IPSec proposal 4
1w0d: ISAKMP: transform 1, ESP_3DES
1w0d: ISAKMP: attributes in transform:
1w0d: ISAKMP: authenticator is HMAC-SHA
1w0d: ISAKMP: encaps is 1
1w0d: ISAKMP: SA life type in seconds
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
```

1w0d: ISAKMP (0:2): atts are acceptable.

```
1w0d: 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= 10.16.20.2/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
1w0d: ISAKMP (0:2): processing NONCE payload. message ID = 132557281
1w0d: ISAKMP (0:2): processing ID payload. message ID = 132557281
1w0d: ISAKMP (0:2): processing ID payload. message ID = 132557281
1w0d: ISAKMP (0:2): asking for 1 spis from ipsec
1w0d: ISAKMP (0:2): Node 132557281, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE

1w0d: IPSEC(key_engine): got a queue event...
1w0d: IPSEC(spi_response): getting spi 245824456 for SA
from 10.1.1.1 to 10.0.0.1 for prot 3
1w0d: ISAKMP: received ke message (2/1)
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) QM_IDLE
1w0d: ISAKMP (0:2): Node 132557281, Input = IKE_MESG_FROM_IPSEC,
IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2

1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM_IDLE
```

1w0d: ISAKMP (0:2): Creating IPSec SAs
1w0d: inbound SA from 10.0.0.1 to 10.1.1.1
(proxy 10.16.20.2 to 10.1.1.1)
1w0d: has spi 0xEA6FBC8 and conn_id 2000 and flags 4
1w0d: lifetime of 2147483 seconds
1w0d: outbound SA from 10.1.1.1 to 10.0.0.1 (proxy
10.1.1.1 to 10.16.20.2)
1w0d: has spi 1009463339 and conn_id 2001 and flags C
1w0d: lifetime of 2147483 seconds

1w0d: ISAKMP (0:2): deleting node 132557281 error FALSE reason "quick mode
done (await()"
1w0d: ISAKMP (0:2): Node 132557281, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE

1w0d: IPSEC(key_engine): got a queue event...
1w0d: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1,
local_proxy= 10.1.1.1/0.0.0.0/0/0 (type=1),
remote_proxy= 10.16.20.2/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac ,
lifedur= 2147483s and 0kb,
spi= 0xEA6FBC8(245824456), conn_id= 2000, keysize= 0, flags= 0x4
1w0d: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 10.1.1.1, remote= 10.0.0.1,
local_proxy= 10.1.1.1/0.0.0.0/0/0 (type=1),
remote_proxy= 10.16.20.2/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x3C2B302B(1009463339), conn_id= 2001, keysize= 0, flags= 0xC
1w0d: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.1.1.1, sa_prot= 50,
sa_spi= 0xEA6FBC8(245824456),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2000
1w0d: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.0.0.1, sa_prot= 50,
sa_spi= 0x3C2B302B(1009463339),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2001
1w0d: ISAKMP: received ke message (4/1)
1w0d: ISAKMP: Locking CONFIG struct 0x830BF118 for
crypto_ikmp_config_handle_kei_mess, count 3
1w0d: ISAKMP (0:1): purging SA., sa=83196748, delme=83196748
1w0d: ISAKMP: Unlocking CONFIG struct 0x830BF118 on return of attributes,
count 2
1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM_IDLE
1w0d: ISAKMP (0:2): processing HASH payload. message ID = -1273332908
1w0d: ISAKMP (0:2): processing SA payload. message ID = -1273332908
1w0d: ISAKMP (0:2): Checking IPSec proposal 1
1w0d: ISAKMP: transform 1, ESP_3DES
1w0d: ISAKMP: attributes in transform:
1w0d: ISAKMP: authenticator is HMAC-MD5
1w0d: ISAKMP: encaps is 1
1w0d: ISAKMP: SA life type in seconds
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w0d: IPSEC(validate_proposal): transform proposal (prot 3, trans 3,
hmac_alg 1) not supported
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0
1w0d: ISAKMP (0:2): skipping next ANDed proposal (1)
1w0d: ISAKMP (0:2): Checking IPSec proposal 2
1w0d: ISAKMP: transform 1, ESP_3DES
1w0d: ISAKMP: attributes in transform:
1w0d: ISAKMP: authenticator is HMAC-SHA

```
1w0d: ISAKMP: encaps is 1
1w0d: ISAKMP: SA life type in seconds
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w0d: ISAKMP (0:2): atts are acceptable.
1w0d: ISAKMP (0:2): Checking IPSec proposal 2
1w0d: ISAKMP (0:2): transform 1, IPPCP LZS
1w0d: ISAKMP: attributes in transform:
1w0d: ISAKMP: encaps is 1
1w0d: ISAKMP: SA life type in seconds
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w0d: IPSEC(validate_proposal): transform proposal (prot 4, trans 3,
hmac_alg 0) not supported
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0
1w0d: ISAKMP (0:2): Checking IPSec proposal 3
1w0d: ISAKMP: transform 1, ESP_3DES
1w0d: ISAKMP: attributes in transform:
1w0d: ISAKMP: authenticator is HMAC-MD5
1w0d: ISAKMP: encaps is 1
1w0d: ISAKMP: SA life type in seconds
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w0d: IPSEC(validate_proposal): transform proposal (prot 3, trans 3,
hmac_alg 1) not supported
1w0d: ISAKMP (0:2): atts not acceptable. Next payload is 0
1w0d: ISAKMP (0:2): Checking IPSec proposal 4
1w0d: ISAKMP: transform 1, ESP_3DES
1w0d: ISAKMP: attributes in transform:
1w0d: ISAKMP: authenticator is HMAC-SHA
1w0d: ISAKMP: encaps is 1
1w0d: ISAKMP: SA life type in seconds
1w0d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
1w0d: ISAKMP (0:2): atts are acceptable.
1w0d: IPSEC(validate_proposal_request): proposal part #
vpn2611#1,
(key eng. msg.) INBOUND local= 10.1.1.1, remote= 10.0.0.1,
local_proxy= 14.38.0.0/255.255.0.0/0/0 (type=4),
remote_proxy= 10.16.20.2/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
1w0d: ISAKMP (0:2): processing NONCE payload. message ID = -1273332908
1w0d: ISAKMP (0:2): processing ID payload. message ID = -1273332908
1w0d: ISAKMP (0:2): processing ID payload. message ID = -1273332908
1w0d: ISAKMP (0:2): asking for 1 spis from ipsec
1w0d: ISAKMP (0:2): Node -1273332908, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE

1w0d: IPSEC(key_engine): got a queue event...
1w0d: IPSEC(spi_response): getting spi 593097454 for SA
from 10.1.1.1 to 10.0.0.1
vpn2611#
vpn2611#2 for prot 3
1w0d: ISAKMP: received ke message (2/1)
1w0d: ISAKMP (0:2): sending packet to 10.0.0.1 (R) QM_IDLE
1w0d: ISAKMP (0:2): Node -1273332908, Input = IKE_MESG_FROM_IPSEC,
IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2

1w0d: ISAKMP (0:2): received packet from 10.0.0.1 (R) QM_IDLE

1w0d: ISAKMP (0:2): Creating IPSec SAs
1w0d: inbound SA from 10.0.0.1 to 10.1.1.1
(proxy 10.16.20.2 to 14.38.0.0)
```

```
1w0d: has spi 0x2359F2EE and conn_id 2002 and flags 4
1w0d: lifetime of 2147483 seconds
1w0d: outbound SA from 10.1.1.1 to 10.0.0.1 (proxy
14.38.0.0 to 10.16.20.2 )
1w0d: has spi 1123818858 and conn_id 2003 and flags C
1w0d: lifetime of 2147483 seconds

1w0d: ISAKMP (0:2): deleting node -1273332908 erro
vpn2611#un ar FALSE reason "quick mode done (await()"
1w0d: ISAKMP (0:2): Node -1273332908, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE

1w0d: IPSEC(key_engine): got a queue event...
1w0d: IPSEC(initialize_sas): ,
(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= 10.16.20.2/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x2359F2EE(593097454), conn_id= 2002, keysize= 0, flags= 0x4
1w0d: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND 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= 10.16.20.2/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-shll
All possible debugging has been turned off
vpn2611#a-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x42FC1D6A(1123818858), conn_id= 2003, keysize= 0, flags= 0xC
1w0d: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.1.1.1, sa_prot= 50,
sa_spi= 0x2359F2EE(593097454),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2002
1w0d: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.0.0.1, sa_prot= 50,
sa_spi= 0x42FC1D6A(1123818858),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2003
```

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:

```
1 16:48:10.203 03/05/02 Sev=Info/6 DIALER/0x63300002
Initiating connection.

2 16:48:10.203 03/05/02 Sev=Info/4 CM/0x63100002
Begin connection process

3 16:48:10.223 03/05/02 Sev=Info/4 CM/0x63100004
Establish secure connection using Ethernet

4 16:48:10.223 03/05/02 Sev=Info/4 CM/0x63100026
Attempt connection with server "10.1.1.1"

5 16:48:10.223 03/05/02 Sev=Info/6 IKE/0x6300003B
```

```
Attempting to establish a connection with 10.1.1.1.

6 16:48:10.273 03/05/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID) to 10.1.1.1

7 16:48:10.273 03/05/02 Sev=Info/4 IPSEC/0x63700014
Deleted all keys

8 16:48:10.994 03/05/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 10.1.1.1

9 16:48:10.994 03/05/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK AG (SA, VID, VID, VID, VID, KE, ID, NON, HASH)
from 10.1.1.1

10 16:48:10.994 03/05/02 Sev=Info/5 IKE/0x63000059
Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

11 16:48:10.994 03/05/02 Sev=Info/5 IKE/0x63000001
Peer is a Cisco-Unity compliant peer

12 16:48:10.994 03/05/02 Sev=Info/5 IKE/0x63000059
Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

13 16:48:10.994 03/05/02 Sev=Info/5 IKE/0x63000001
Peer supports DPD

14 16:48:10.994 03/05/02 Sev=Info/5 IKE/0x63000059
Vendor ID payload = 2D275A044215F48F531958AB2578EB2D

15 16:48:10.994 03/05/02 Sev=Info/5 IKE/0x63000059
Vendor ID payload = 09002689DFD6B712

16 16:48:11.025 03/05/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT) to 10.1.1.1

17 16:48:11.045 03/05/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 10.1.1.1

18 16:48:11.045 03/05/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:STATUS_RESP_LIFETIME)
from 10.1.1.1

19 16:48:11.045 03/05/02 Sev=Info/5 IKE/0x63000044
RESPONDER-LIFETIME notify has value of 86400 seconds

20 16:48:11.045 03/05/02 Sev=Info/5 IKE/0x63000046
This SA has already been alive for 1 seconds,
setting expiry to 86399 seconds from now

21 16:48:11.075 03/05/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 10.1.1.1

22 16:48:11.075 03/05/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.1.1.1

23 16:48:11.075 03/05/02 Sev=Info/4 CM/0x63100015
Launch xAuth application

24 16:48:14.920 03/05/02 Sev=Info/4 CM/0x63100017
xAuth application returned
```

```
25 16:48:14.920 03/05/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.1.1.1

26 16:48:14.990 03/05/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 10.1.1.1

27 16:48:14.990 03/05/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.1.1.1

28 16:48:14.990 03/05/02 Sev=Info/4 CM/0x6310000E
Established Phase 1 SA. 1 Phase 1 SA in the system

29 16:48:15.000 03/05/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.1.1.1

30 16:48:15.010 03/05/02 Sev=Info/5 IKE/0x6300005D
Client sending a firewall request to concentrator

31 16:48:15.010 03/05/02 Sev=Info/5 IKE/0x6300005C
Firewall Policy: Product=Cisco Integrated Client,
Capability= (Centralized Policy Push).

32 16:48:15.010 03/05/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.1.1.1

33 16:48:15.141 03/05/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 10.1.1.1

34 16:48:15.141 03/05/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.1.1.1

35 16:48:15.141 03/05/02 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 10.16.20.2

36 16:48:15.141 03/05/02 Sev=Info/5 IKE/0xA3000017
MODE_CFG_REPLY: The received (INTERNAL_ADDRESS_EXPIRY) attribute and value
(86395) is not supported

37 16:48:15.141 03/05/02 Sev=Info/5 IKE/0x6300000E
MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Internetwork
Operating System Software IOS (tm) C2600 Software (C2600-JK9O3S-M),
Version 12.2(8)T, RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 14-Feb-02 16:50 by ccai

38 16:48:15.141 03/05/02 Sev=Info/5 IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets),
value = 0x00000001

39 16:48:15.141 03/05/02 Sev=Info/5 IKE/0x6300000F
SPLIT_NET #1
subnet = 172.18.124.0
mask = 255.255.255.0
protocol = 0
src port = 0
dest port=0

40 16:48:15.141 03/05/02 Sev=Info/4 CM/0x63100019
Mode Config data received

41 16:48:15.151 03/05/02 Sev=Info/5 IKE/0x63000055
```

```
Received a key request from Driver for IP address 10.1.1.1,
GW IP = 10.1.1.1

42 16:48:15.151 03/05/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 10.1.1.1

43 16:48:15.361 03/05/02 Sev=Info/4 IPSEC/0x63700014
Deleted all keys

44 16:48:15.461 03/05/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 10.1.1.1

45 16:48:15.461 03/05/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME) from 10.1.1.1

46 16:48:15.461 03/05/02 Sev=Info/5 IKE/0x63000044
RESPONDER-LIFETIME notify has value of 3600 seconds

47 16:48:15.461 03/05/02 Sev=Info/5 IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

48 16:48:15.461 03/05/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 10.1.1.1

49 16:48:15.461 03/05/02 Sev=Info/5 IKE/0x63000058
Loading IPsec SA (Message ID = 0x07E6A9E1 OUTBOUND SPI = 0x0EA6FBC8
INBOUND SPI = 0x3C2B302B)

50 16:48:15.461 03/05/02 Sev=Info/5 IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0x0EA6FBC8

51 16:48:15.471 03/05/02 Sev=Info/5 IKE/0x63000026
Loaded INBOUND ESP SPI: 0x3C2B302B

52 16:48:15.471 03/05/02 Sev=Info/4 CM/0x6310001A
One secure connection established

53 16:48:15.511 03/05/02 Sev=Info/6 DIALER/0x63300003
Connection established.

54 16:48:15.581 03/05/02 Sev=Info/6 DIALER/0x63300008
MAPI32 Information - Outlook not default mail client

55 16:48:16.553 03/05/02 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

56 16:48:16.553 03/05/02 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0xc8fba60e into key list

57 16:48:16.553 03/05/02 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

58 16:48:16.553 03/05/02 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0x2b302b3c into key list

59 16:48:26.357 03/05/02 Sev=Info/5 IKE/0x63000055
Received a key request from Driver for IP address 172.18.124.159,
GW IP = 10.1.1.1

60 16:48:26.357 03/05/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 10.1.1.1
```

```
61 16:48:26.668 03/05/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 10.1.1.1

62 16:48:26.668 03/05/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME) from 10.1.1.1

63 16:48:26.668 03/05/02 Sev=Info/5 IKE/0x63000044
RESPONDER-LIFETIME notify has value of 3600 seconds

64 16:48:26.668 03/05/02 Sev=Info/5 IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

65 16:48:26.668 03/05/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 10.1.1.1

66 16:48:26.668 03/05/02 Sev=Info/5 IKE/0x63000058
Loading IPsec SA (Message ID = 0xB41A7B54 OUTBOUND SPI = 0x2359F2EE
INBOUND SPI = 0x42FC1D6A)

67 16:48:26.668 03/05/02 Sev=Info/5 IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0x2359F2EE

68 16:48:26.668 03/05/02 Sev=Info/5 IKE/0x63000026
Loaded INBOUND ESP SPI: 0x42FC1D6A

69 16:48:26.668 03/05/02 Sev=Info/4 CM/0x63100022
Additional Phase 2 SA established.
```

معلومات ذات صلة

- دعم مفاوضة IPSec/بروتوكولات IKE
- 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).