使用 RADIUS 在 Cisco IOS 路由器和 Cisco VPN 客户端 4.x for Windows 之间配置 IPSec

目录

简介

本文档展示如何使用 RADIUS 进行组授权和用户身份验证来配置 Cisco IOS 路由器与 Cisco VPN Client 4.x 之间的连接。Cisco IOS® 软件版本 12.2(8)T 和更高版本支持 Cisco VPN Client 3.x 及以上的连接。VPN 客户端 3.x 和 VPN 客户端 4.x 使用 Diffie Hellman (DH) 第 2 组策略。isakmp policy # group 2 命令使 VPN 客户端能够进行连接。

注意：IPSec VPN记账现在可用。有关更多信息和配置示例，请参阅 IPSec VPN 记账。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 要分配给 IPSec 的地址的池

- 具有预共享密钥“cisco123”的称为“3000clients”的组
- RADIUS 服务器上的组授权和用户身份验证

注意：目前不支持RADIUS记帐。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行 Cisco IOS 软件版本 12.2(8)T 的 2611 路由器。
- Cisco Secure ACS for Windows（任何RADIUS服务器都应工作）。
- 适用于Windows的Cisco VPN Client版本4.8（任何VPN Client 4.x都应该适用）。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

路由器上 show version 命令的输出如下：

<#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
```

背景理论

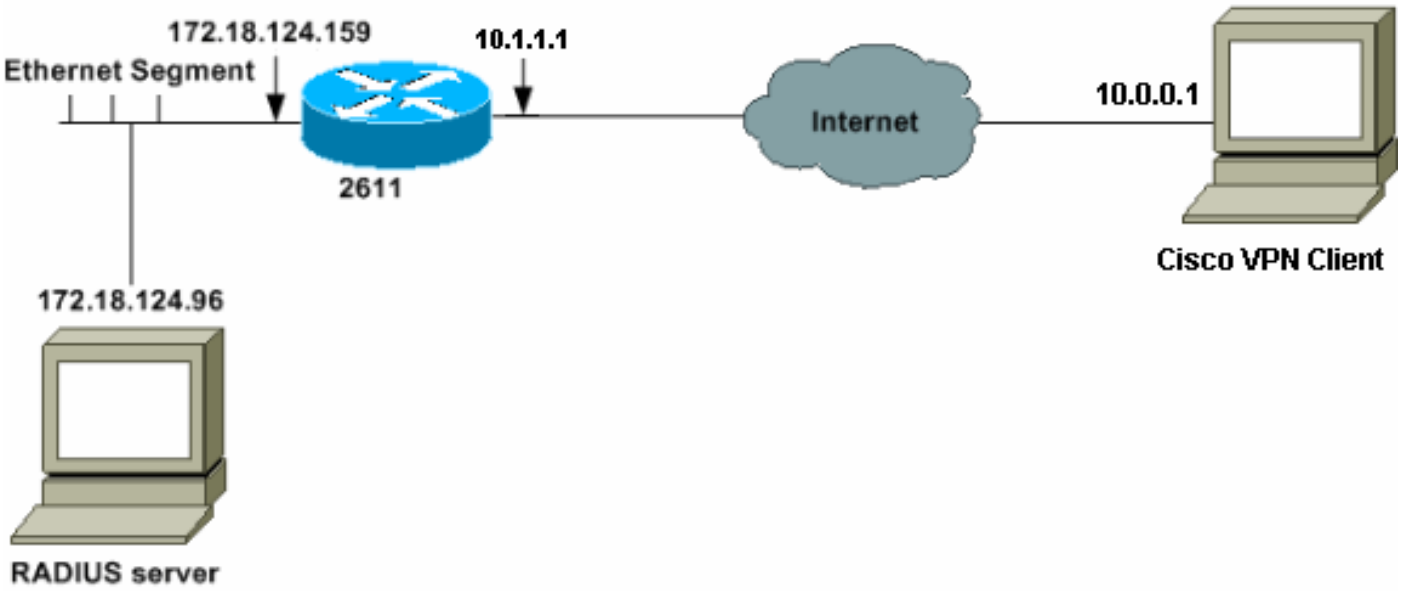
本文档显示身份验证和授权，例如由RADIUS服务器分配Windows Internet命名服务(WINS)和域名服务(DNS)。如果您感兴趣的是由 RADIUS 服务器进行身份验证并由路由器进行本地授权，请参阅使用 RADIUS 进行用户身份验证以配置 Cisco IOS 路由器与 Cisco VPN Client 4.x for Windows 之间的 IPSec。

配置

本部分提供有关如何配置本文档所述功能的信息。

网络图

本文档使用以下网络设置：



注意：本示例网络中的IP地址在全球Internet中不可路由，因为它们是实验网络中的专用IP地址。

配置

2611 路由器

```
<#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
!
```

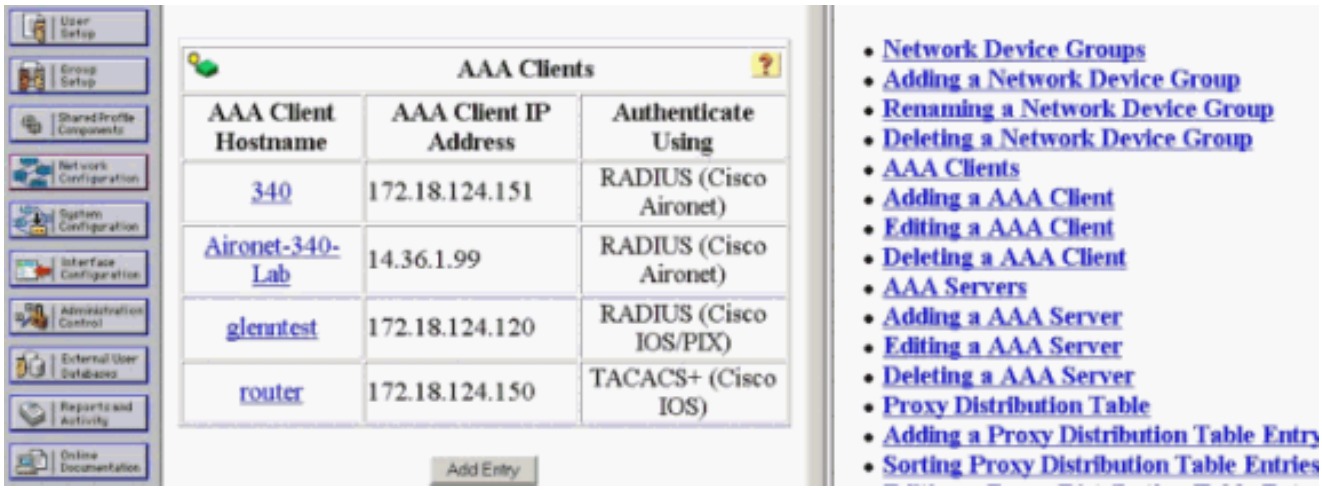
```
!--- Create an access control list (ACL) if you want to do split tunneling.
!--- This ACL is referenced in the RADIUS profile.


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#
```

RADIUS 服务器配置

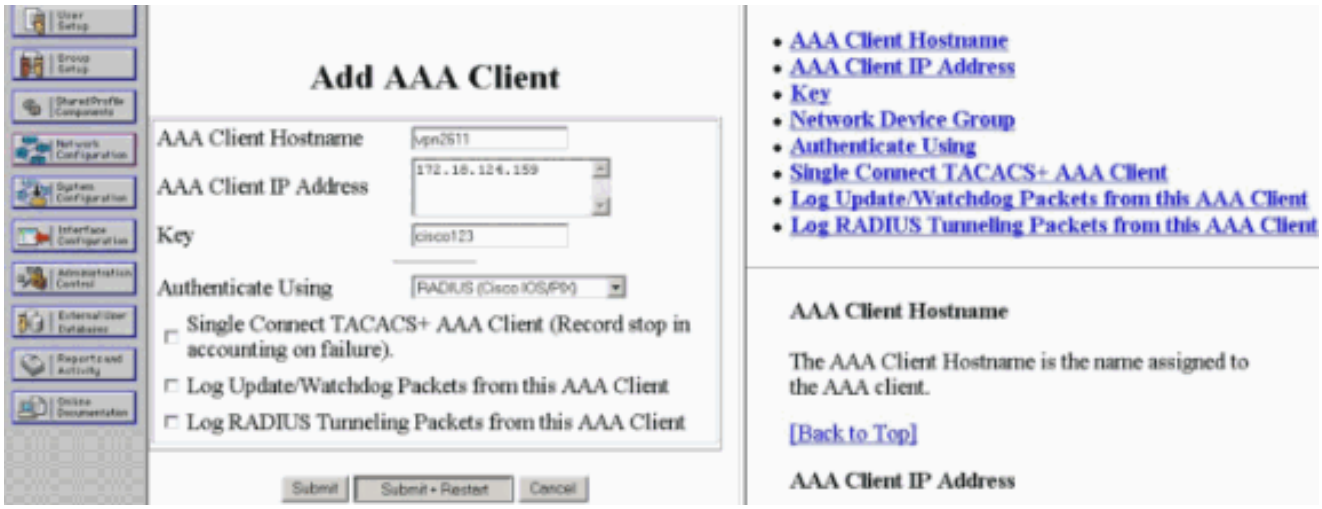
配置用于 AAA 客户端（路由器）的 RADIUS 服务器

请完成以下步骤：

1. 单击 Add Entry 将路由器添加到 RADIUS 服务器数据库。



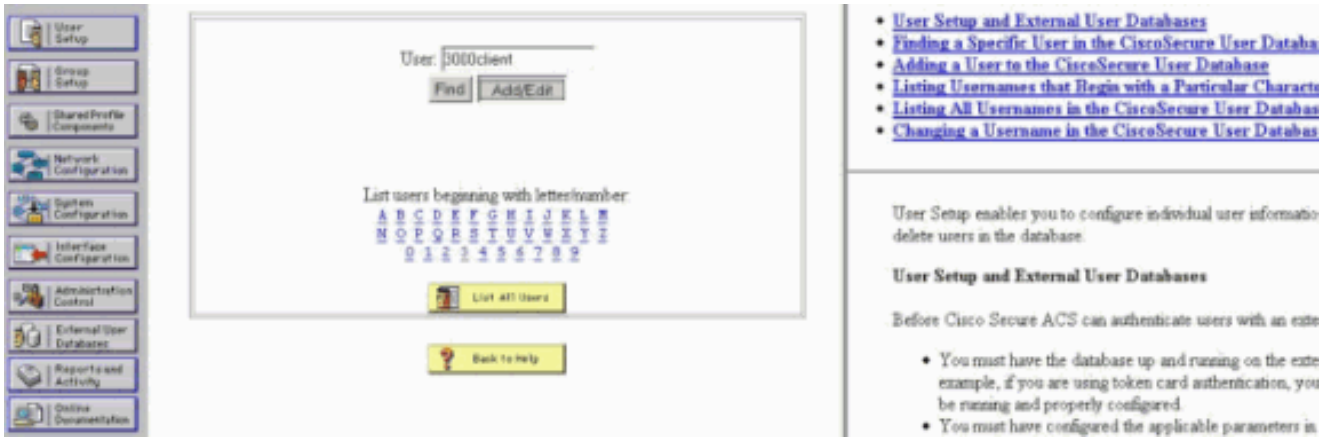
2. 指定路由器的 IP 地址“172.18.124.159”以及共享密钥“cisco123”，并在“Authenticate Using”下拉框中选择 RADIUS。



配置 RADIUS 服务器以进行组身份验证和授权

请完成以下步骤：

1. 单击 Add/Edit 将一个名为“3000client”的用户添加到 RADIUS 服务器。

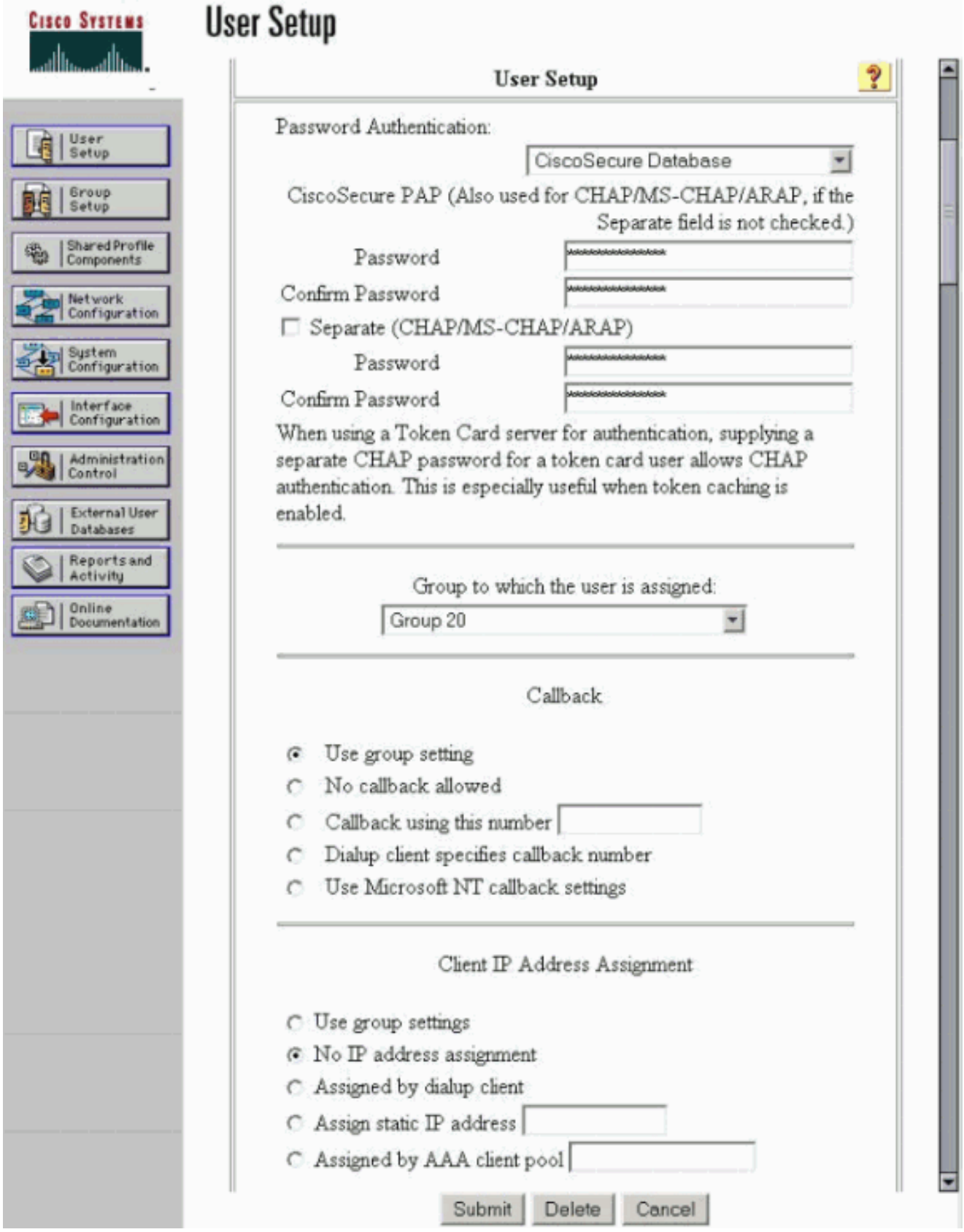


2. 在Cisco IOS软件版本15.8.3和Cisco IOS XE软件版本16.9.1之前，此密码是Cisco IOS的特殊关键字，表示必须引用组配置文件。如果需要，可以将用户映射到 Cisco Secure 组。请确保

选中 No IP address assignment。

在Cisco IOS软件版本15.8.3和Cisco IOS XE软件版本16.9.1之后，AAA授权需要密码并且是必需的。建议定义通过isakmp authorization list aaa_list1 password <secret>命令使用的口令。

然后，管理员将在RADIUS服务器上配置<secret>匹配密码。



3. 指定将由此用户帐户向下传递回 VPN 客户端的组授权参数。

   确保已启用 cisco-av-pair 并具有下列属性：

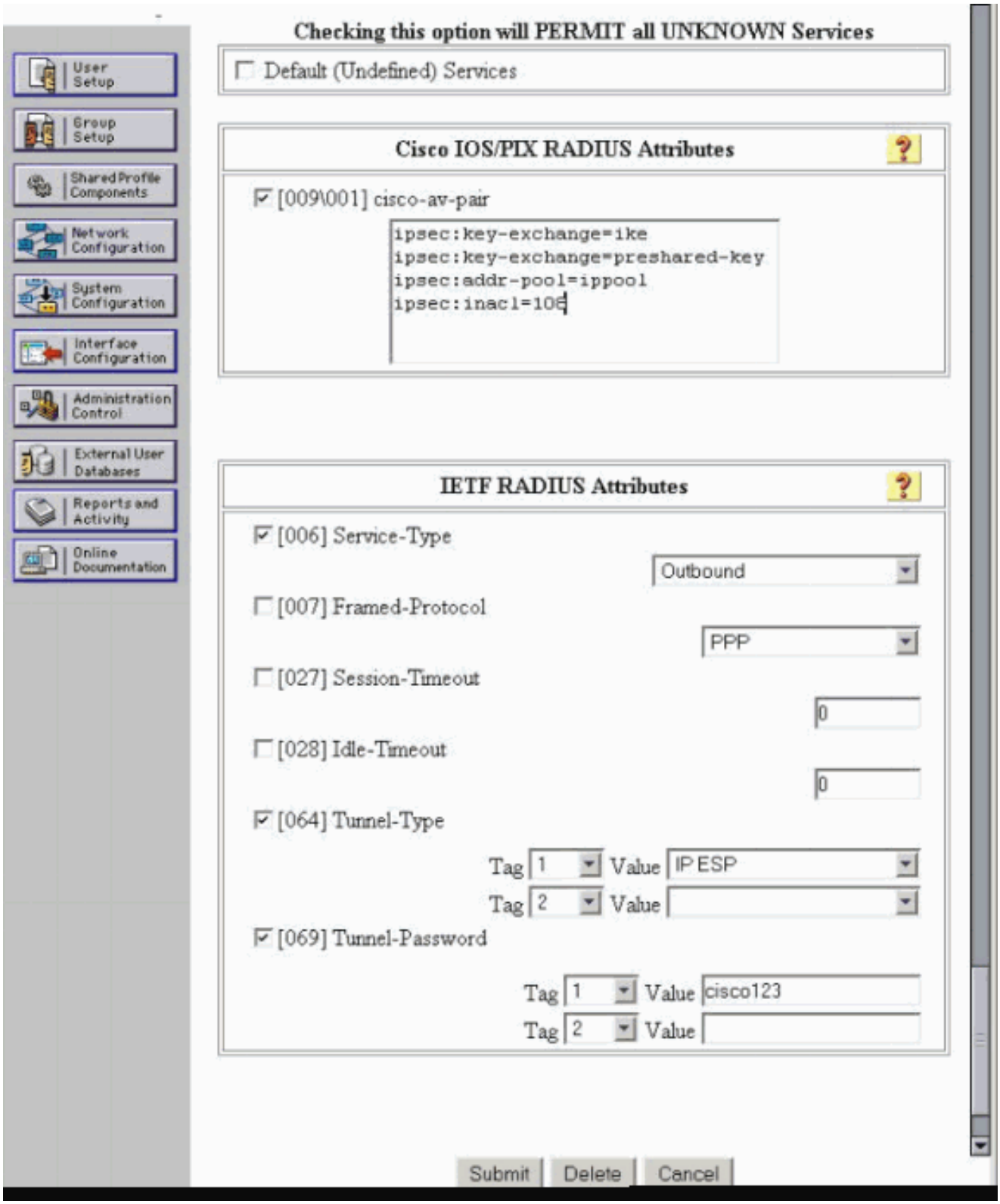
   - ipsec：key-exchange=ike
   - ipsec：key-exchange=preshared-key

- ipsec：addr-pool=ippool
- ipsec：inacl=108（仅当在路由器上使用分割隧道时才需要）

另外，请确保启用以下 IETF RADIUS 属性：

- 属性6：Service-Type=Outbound
- 属性64：Tunnel-Type=IP ESP
- 属性69：Tunnel-Password=cisco123（这是VPN客户端上的组密码）

完成后，单击 Submit。



在“Vendor Specific Attributes”下，还可以启用下列可选属性：

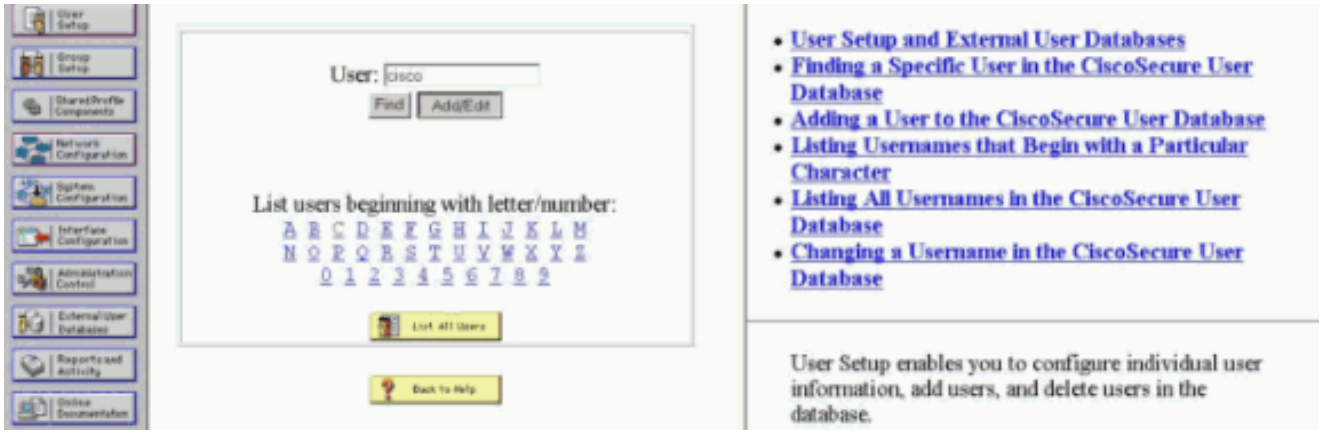
- ipsec：default-domain=
- ipsec：timeout=
- ipsec：idletime=
- ipsec：dns-servers=
- ipsec：wins-servers=

配置 RADIUS 服务器以进行用户身份验证

请完成以下步骤：

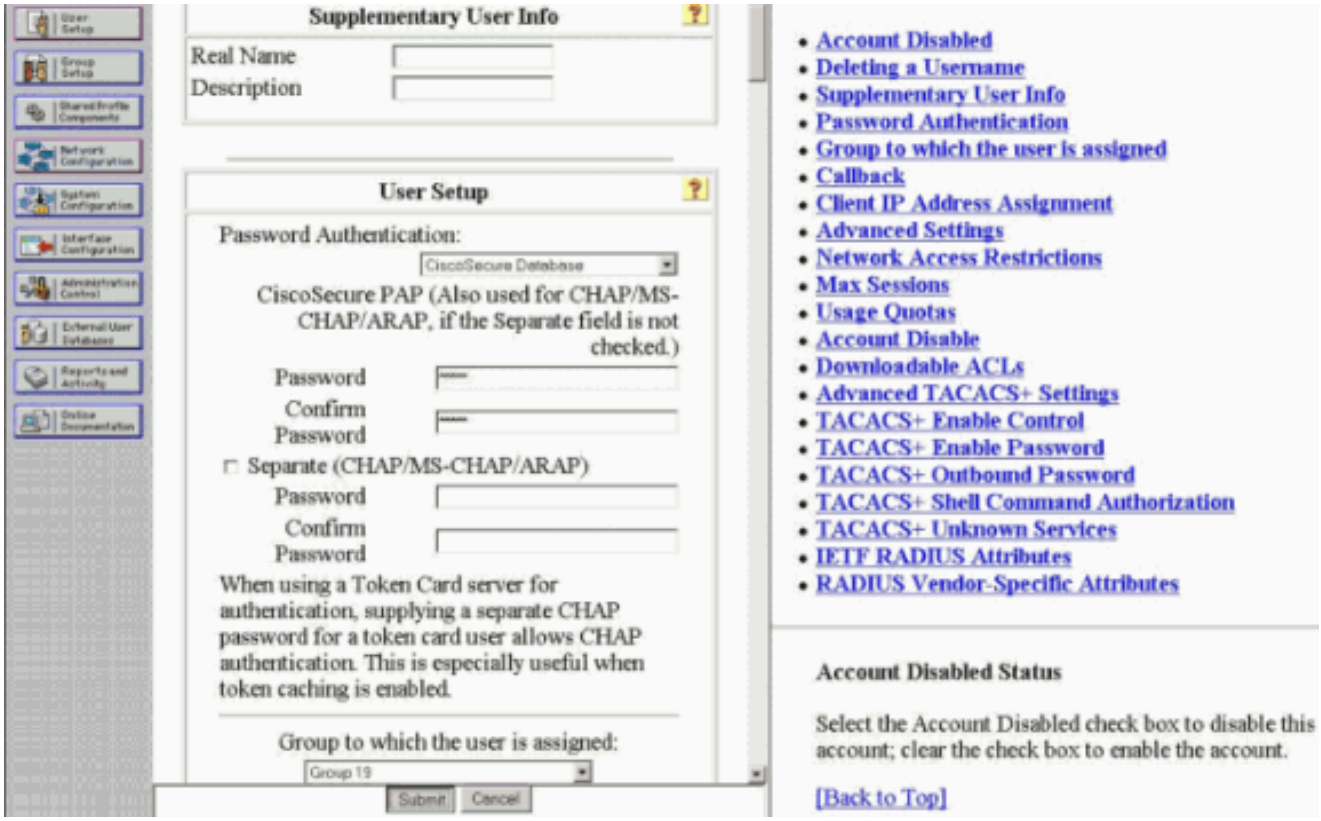
1. 单击 Add/Edit 在 Cisco Secure 数据库中添加 VPN 用户。

   在本示例中，用户名为 cisco。



2. 在下一个窗口中，为用户 cisco 指定口令。口令也是 cisco。

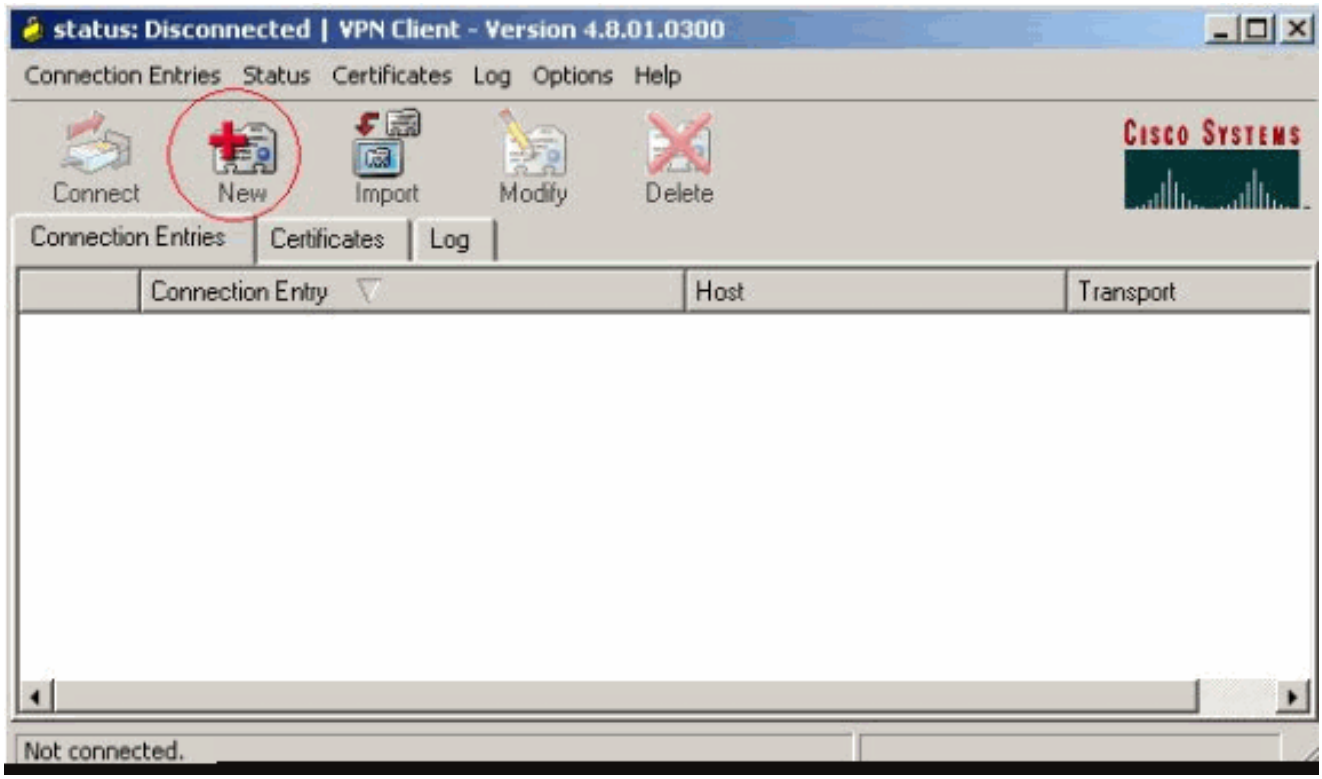
   可以将用户帐户映射到组。完成后，单击 Submit。



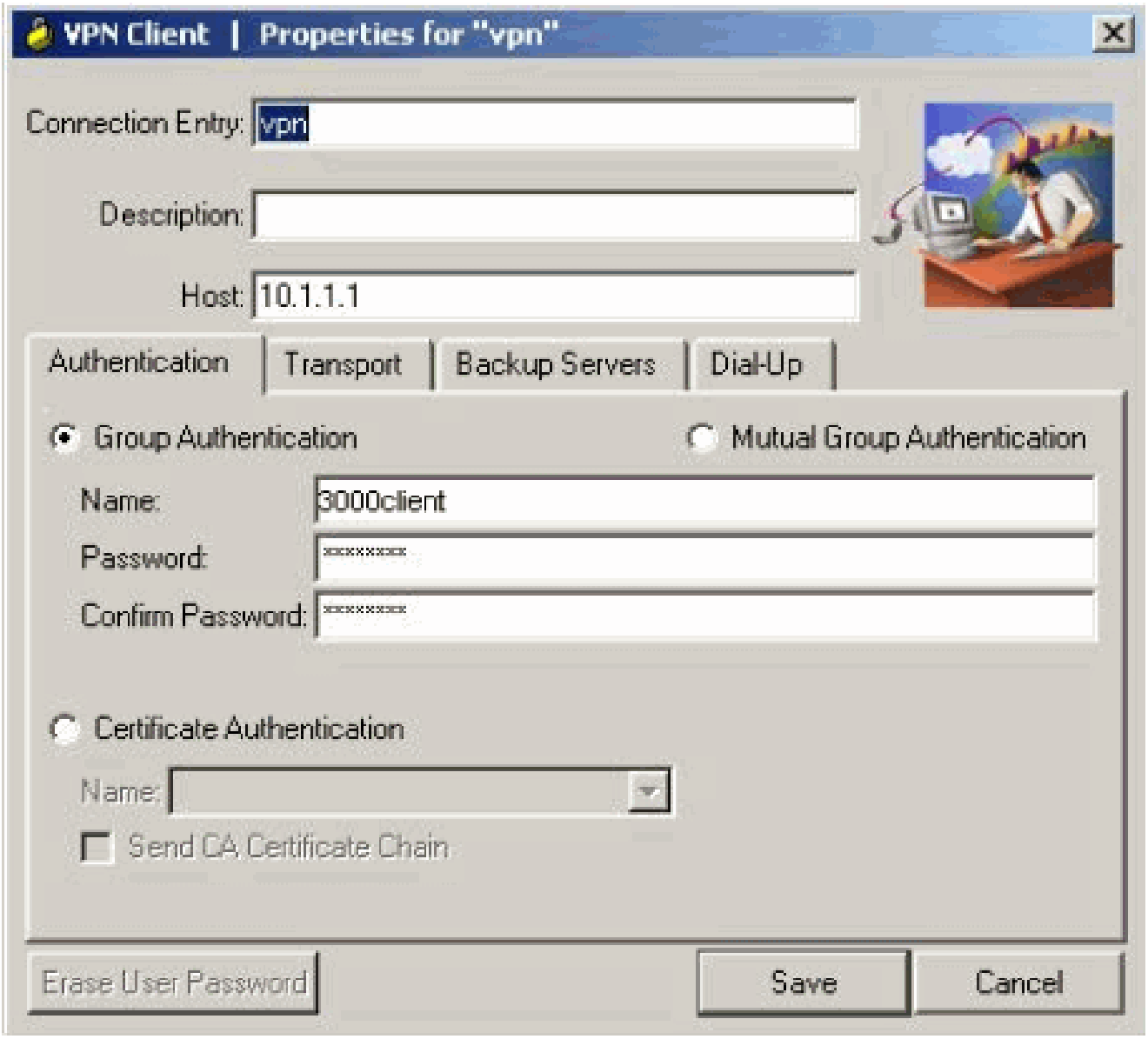
VPN 客户端 4.8 配置

完成下列步骤以配置 VPN Client 4.8：

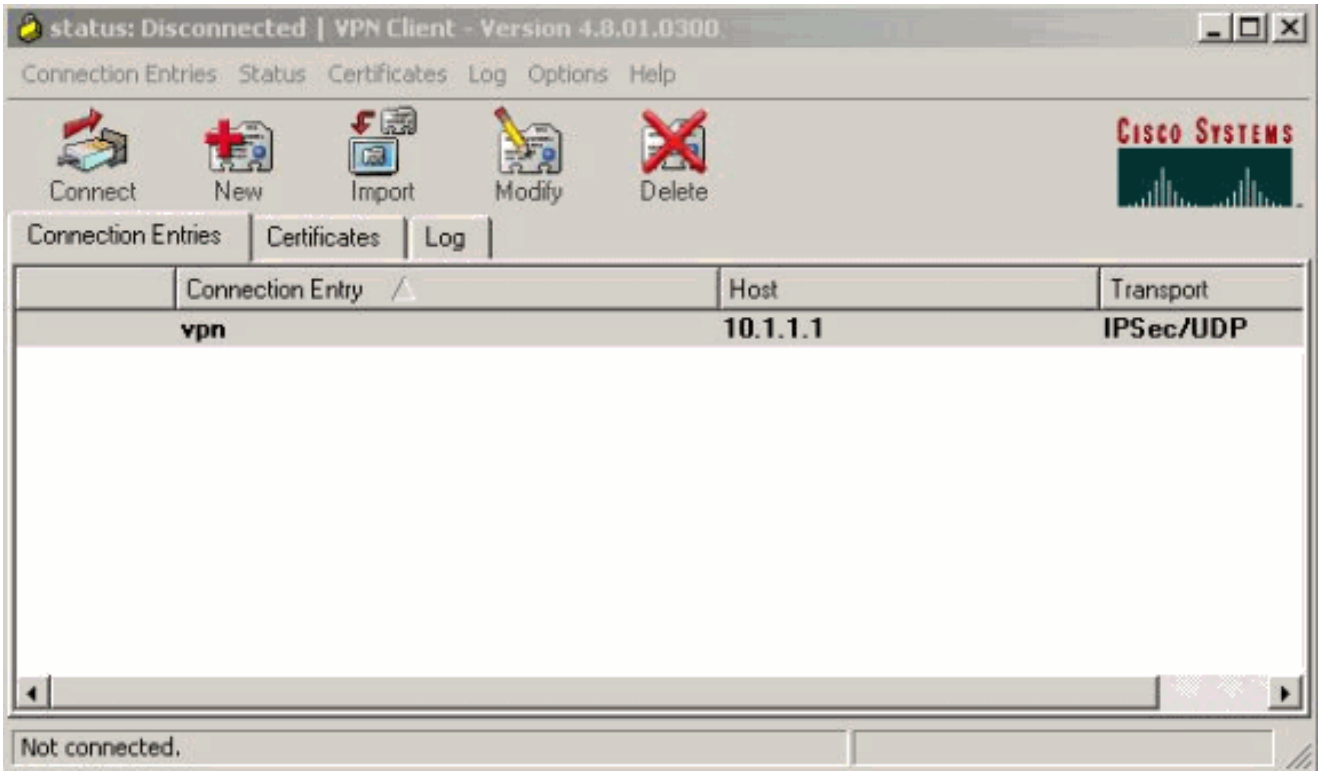
1. 选择开始 > 程序 > Cisco Systems VPN 客户端 > VPN 客户端。
2. 单击 New 以启动 Create New VPN Connection Entry 窗口。



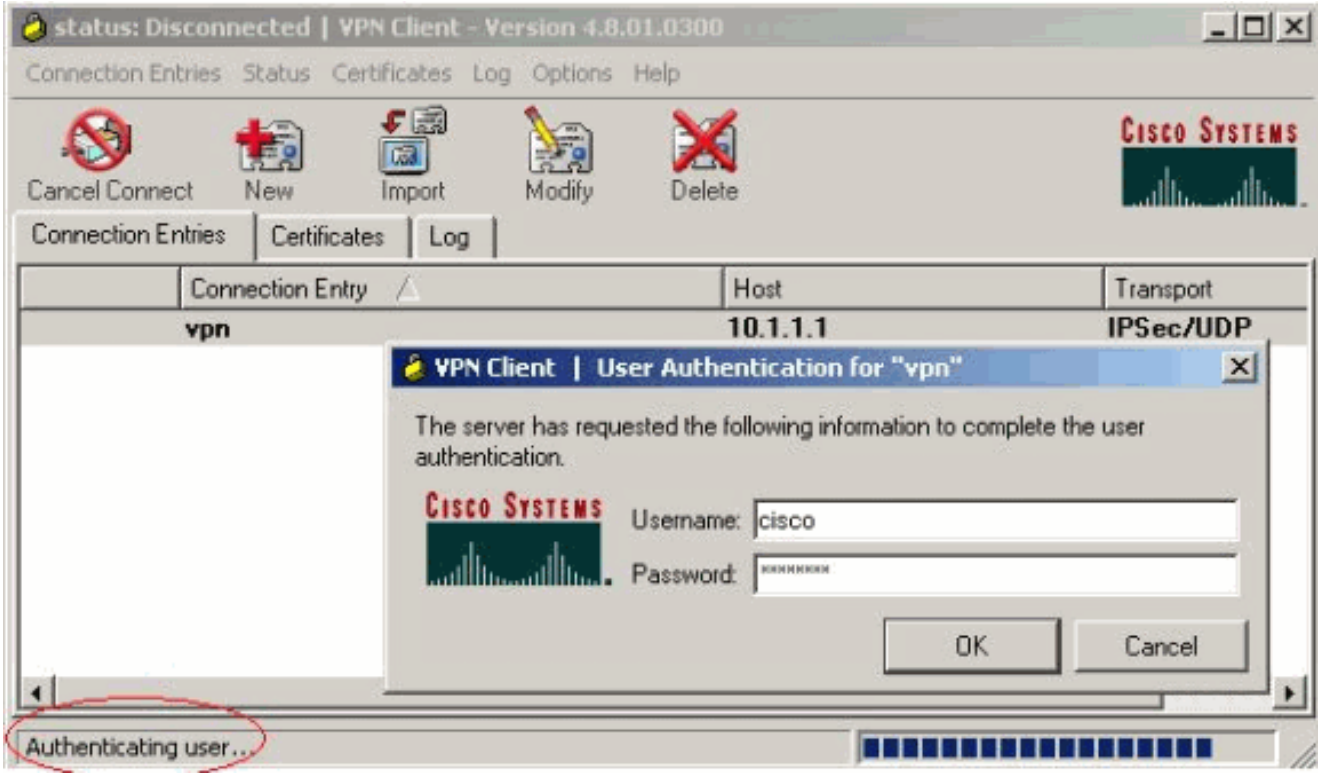
3. 输入 Connection Entry 的名称与说明。在“Host”框中输入路由器的外部 IP 地址。然后输入 VPN 组的名称和口令，并单击 Save。



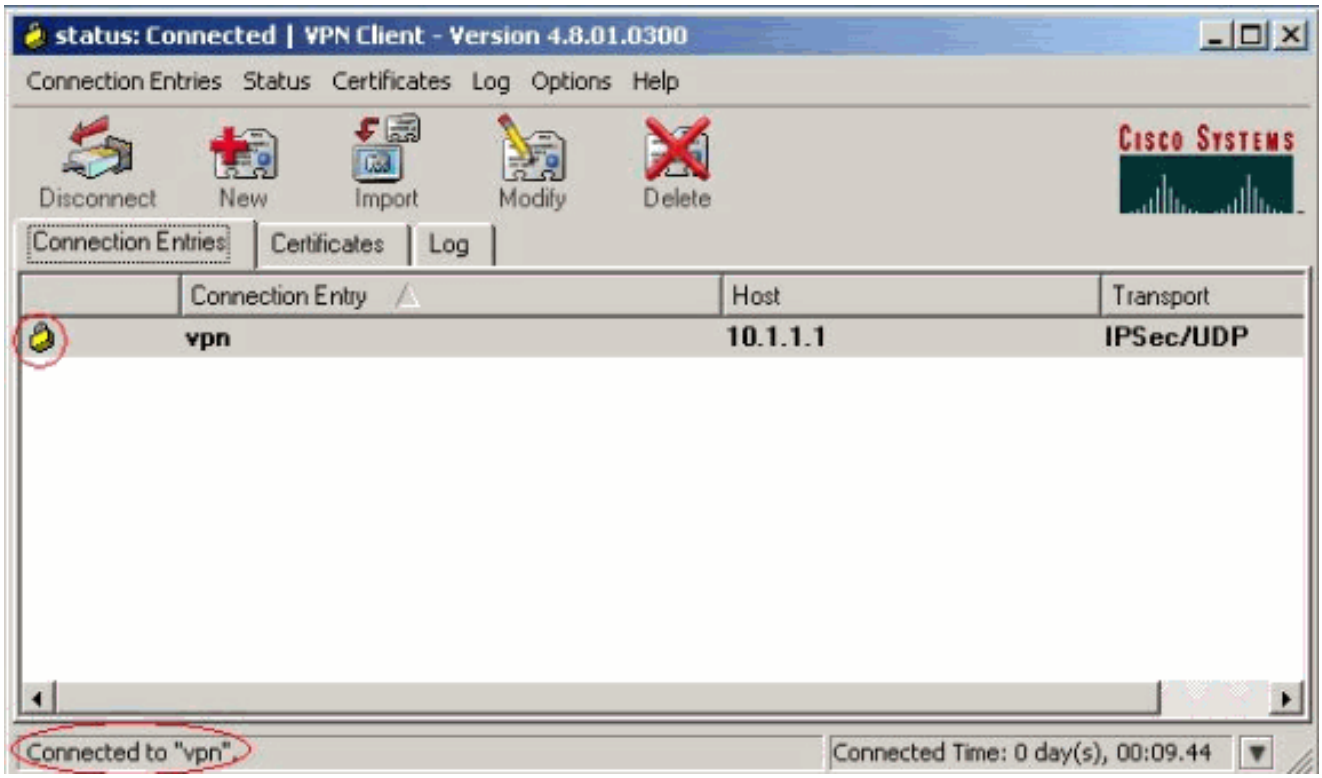
4. 单击要使用的连接，然后在 VPN 客户端主窗口中单击 Connect。



5. 出现提示时，输入用于 xauth 的 Username 和 Password 信息，然后单击 OK 以连接远程网络。



VPN客户端与中心站点的路由器连接。



验证

使用本部分可确认配置能否正常运行。

<#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
```

故障排除

使用本部分可排除配置故障。

故障排除命令

使用 debug 命令之前，请参阅有关 Debug 命令的重要信息。

- debug crypto ipsec - 显示有关 IPsec 连接的调试信息。
- debug crypto isakmp - 显示有关 IPsec 连接的调试信息，并显示由于两端不兼容而被拒绝的第一组属性。
- debug crypto engine - 显示来自加密引擎的信息。
- debug aaa authentication — 显示有关 AAA/TACACS+ 身份验证的信息。
- debug aaa authorization raduis — 显示有关 AAA/TACACS+ 授权的信息。
- debug radius — 显示有关 RADIUS 服务器与路由器之间通信故障排除的信息。

调试输出

本部分提供来自路由器的调试信息，这些信息可用于对您的配置进行故障排除。

路由器日志

<#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
```

客户端日志

在 VPN 客户端上启动 LogViewer 以查看日志。确保对于所有已配置的类，过滤器均设置为 High。以下是日志输出示例：

```
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.
```

相关信息

- IPSec 协商/IKE 协议技术支持
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。