

# 使用RADIUS配置Cisco IOS路由器與Cisco VPN客戶端4.x for Windows之間的IPSec

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

### [背景理論](#)

### [設定](#)

#### [網路圖表](#)

#### [組態](#)

#### [RADIUS伺服器配置](#)

[為AAA客戶端（路由器）配置RADIUS伺服器](#)

[配置RADIUS伺服器以進行組身份驗證和授權](#)

[配置RADIUS伺服器以進行使用者身份驗證](#)

[VPN客戶端4.8配置](#)

### [驗證](#)

### [疑難排解](#)

#### [疑難排解指令](#)

#### [調試輸出](#)

[路由器日誌](#)

[客戶端日誌](#)

### [相關資訊](#)

---

## 簡介

本文檔演示如何使用RADIUS進行組授權和使用者身份驗證，在Cisco IOS路由器和Cisco VPN客戶端4.x之間配置連線。Cisco IOS<sup>®</sup>軟體版本12.2(8)T及更高版本支援從Cisco VPN Client 3.x建立的連線。VPN客戶端3.x和4.x使用Diffie Hellman (DH)第2組策略。isakmp policy # group 2命令使VPN客戶端可以進行連線。



注意：IPSec VPN記賬現在可用。有關更多資訊和配置示例，請參閱[IPSec VPN記賬](#)。

---

## 必要條件


### 需求

嘗試此組態之前，請確保符合以下要求：

- 要分配給IPSec的地址池

- 名為「3000clients」的組使用預共用金鑰「cisco123」
- RADIUS伺服器上的群組授權和使用者驗證

---

 注意：目前不支援RADIUS記帳。

---

## 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行Cisco IOS軟體版本12.2(8)T的2611路由器。
- 適用於Windows的Cisco Secure ACS (任何RADIUS伺服器都應該工作)。
- 適用於Windows的Cisco VPN Client版本4.8 (任何VPN Client 4.x都應該起作用)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

路由器上show version命令的輸出如下：

```
<#root>
vpn2611#
show version

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-JK903S-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
```

## 背景理論

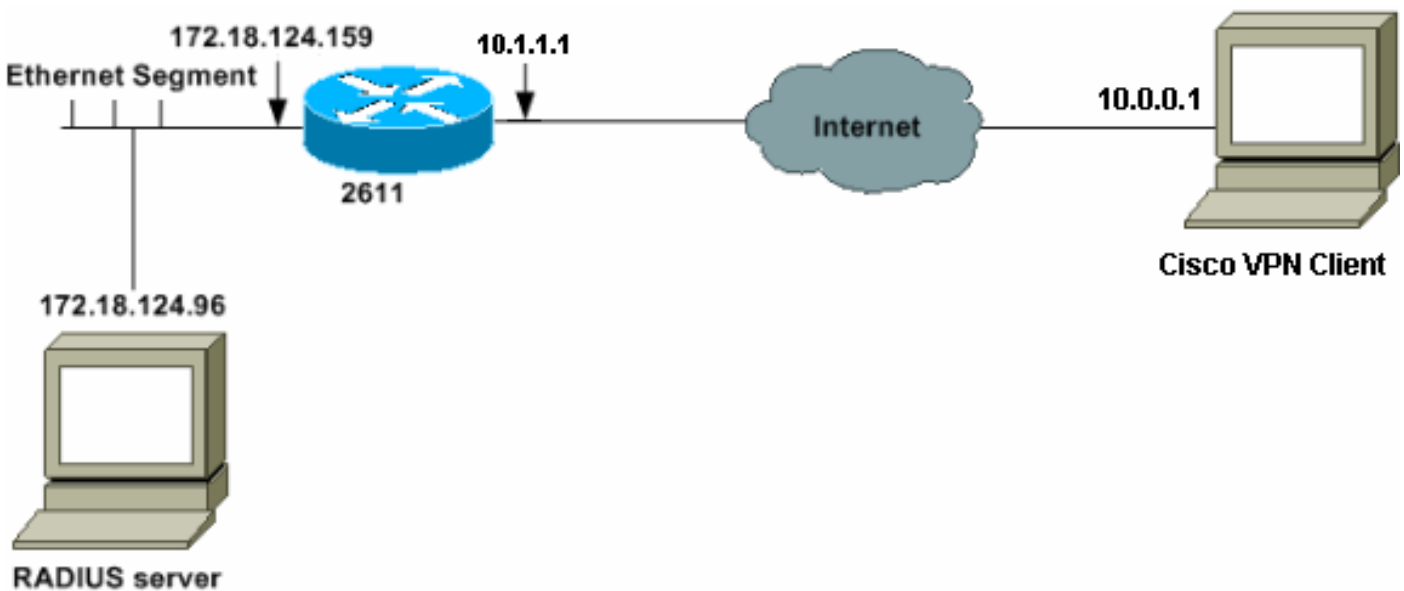
本檔案顯示RADIUS伺服器的驗證與授權，例如指派Windows Internet命名服務(WINS)和網域命名服務(DNS)。如果您感興趣的是由RADIUS伺服器進行身份驗證並由路由器進行本地授權，請參閱[使用RADIUS進行使用者身份驗證以配置Cisco IOS路由器與Cisco VPN客戶端4.x for Windows之間的IPSec。](#)


## 設定

本節提供用於設定本文件中所述功能的資訊。

### 網路圖表

此文件使用以下網路設定：



 注意：本示例網路中的IP地址在全局網際網路中不可路由，因為它們是實驗網路中的專用IP地址。

### 組態

#### 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伺服器配置

為AAA客戶端 ( 路由器 ) 配置RADIUS伺服器

請完成以下步驟：

1. 按一下Add Entry將路由器增加到RADIUS伺服器資料庫。

AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">340</a>	172.18.124.151	RADIUS (Cisco Aironet)
<a href="#">Aironet-340-Lab</a>	14.36.1.99	RADIUS (Cisco Aironet)
<a href="#">glennitest</a>	172.18.124.120	RADIUS (Cisco IOS/PIX)
<a href="#">router</a>	172.18.124.150	TACACS+ (Cisco IOS)

- [Network Device Groups](#)
- [Adding a Network Device Group](#)
- [Renaming a Network Device Group](#)
- [Deleting a Network Device Group](#)
- [AAA Clients](#)
- [Adding a AAA Client](#)
- [Editing a AAA Client](#)
- [Deleting a AAA Client](#)
- [AAA Servers](#)
- [Adding a AAA Server](#)
- [Editing a AAA Server](#)
- [Deleting a AAA Server](#)
- [Proxy Distribution Table](#)
- [Adding a Proxy Distribution Table Entry](#)
- [Sorting Proxy Distribution Table Entries](#)

- 指定路由器的IP地址「172.18.124.159」以及共用金鑰「cisco123」，並在「Authenticate Using」下拉框中選擇RADIUS。

**Add AAA Client**

AAA Client Hostname:

AAA Client IP Address:

Key:

Authenticate Using:

Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

- [AAA Client Hostname](#)
- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[\[Back to Top\]](#)

AAA Client IP Address

配置RADIUS伺服器以進行組身份驗證和授權

請完成以下步驟：

- 按一下Add/Edit將一個名為3000client的使用者增加到RADIUS伺服器。

User:

List users beginning with letter/number:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0 1 2 3 4 5 6 7 8 9

- [User Setup and External User Databases](#)
- [Finding a Specific User in the CiscoSecure User Database](#)
- [Adding a User to the CiscoSecure User Database](#)
- [Listing Usernames that Begin with a Particular Character](#)
- [Listing All Usernames in the CiscoSecure User Database](#)
- [Changing a Username in the CiscoSecure User Database](#)

User Setup enables you to configure individual user information, delete users in the database.

**User Setup and External User Databases**

Before Cisco Secure ACS can authenticate users with an external database, you must:

- You must have the database up and running on the external server.
- You must have configured the applicable parameters in the Cisco Secure ACS configuration.


- 在Cisco IOS軟體版本15.8.3和Cisco IOS XE軟體版本16.9.1之前，此密碼是Cisco IOS的一個特殊關鍵字，表示必須引用組配置檔案。您可以根據需要將使用者對映到Cisco Secure組。確

保未選擇任何IP地址分配。

在Cisco IOS軟體版本15.8.3和Cisco IOS XE軟體版本16.9.1之後，AAA授權需要密碼並且是必需的。建議定義透過isakmp authorization list aaa\_list1 password <secret>命令使用的口令。

然後，管理員將在RADIUS伺服器上配置<secret>匹配密碼。





# User Setup

**User Setup** ?

Password Authentication:

CiscoSecure Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

    Password

    Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

    Password

    Confirm Password

When using a Token Card server for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

---

Group to which the user is assigned:

Group 20

---

Callback

Use group setting

No callback allowed

Callback using this number

Dialup client specifies callback number

Use Microsoft NT callback settings

---

Client IP Address Assignment

Use group settings

No IP address assignment

Assigned by dialup client

Assign static IP address

Assigned by AAA client pool

3. 指定將由此使用者帳戶傳回VPN客戶端的組授權引數。

確保已啟用cisco-av-pair並具有下列屬性：

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

- ipsec : addr-pool=ippool
- ipsec : inacl=108 ( 僅在路由器上使用分割隧道時需要 )

此外，請確保已啟用IETF RADIUS屬性等：

- 屬性6 : Service-Type=Outbound
- 屬性64 : Tunnel-Type=IP ESP
- 屬性69 : Tunnel-Password=cisco123 ( 這是VPN客戶端上的組口令 )

完成後，按一下Submit。

**Checking this option will PERMIT all UNKNOWN Services**

Default (Undefined) Services

---

**Cisco IOS/PIX RADIUS Attributes** ?

[009\001] cisco-av-pair

```
ipsec:key-exchange=ike
ipsec:key-exchange=preshared-key
ipsec:addr-pool=ippool
ipsec:inac1=100
```

---

**IETF RADIUS Attributes** ?

[006] Service-Type Outbound

[007] Framed-Protocol PPP

[027] Session-Timeout 0

[028] Idle-Timeout 0

[064] Tunnel-Type

Tag 1 Value IP ESP

Tag 2 Value

[069] Tunnel-Password

Tag 1 Value cisco123

Tag 2 Value

Submit Delete Cancel

在Vendor Specific Attributes下，您還可以啟用以下可選屬性：

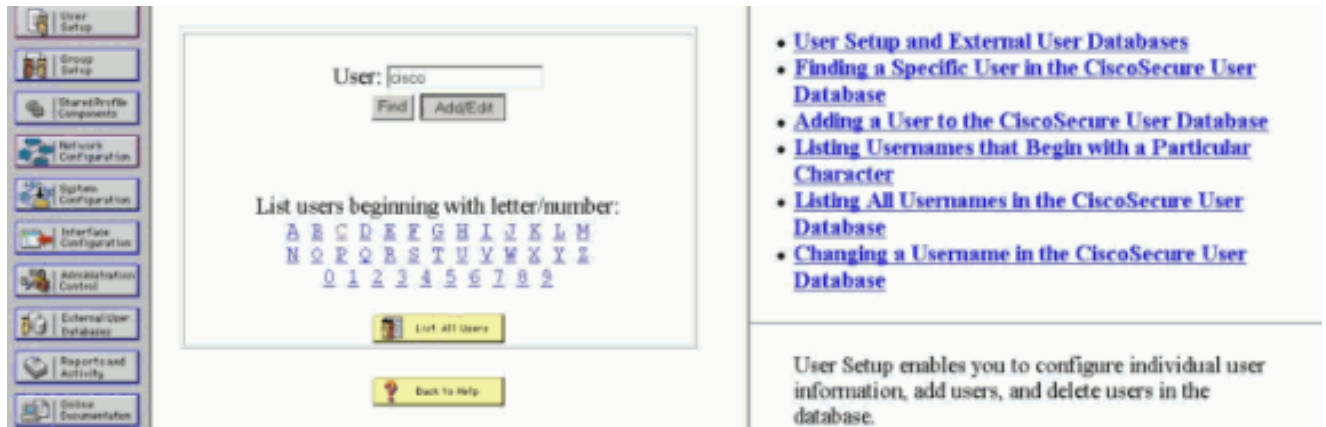
- ipsec : default-domain=
- ipsec : timeout=
- ipsec : idletime=
- ipsec : dns-servers=
- ipsec : wins-servers=

## 配置RADIUS伺服器以進行使用者身份驗證

請完成以下步驟：

1. 按一下Add/Edit在Cisco Secure資料庫中增加VPN使用者。

在本示例中，使用者名稱是cisco。

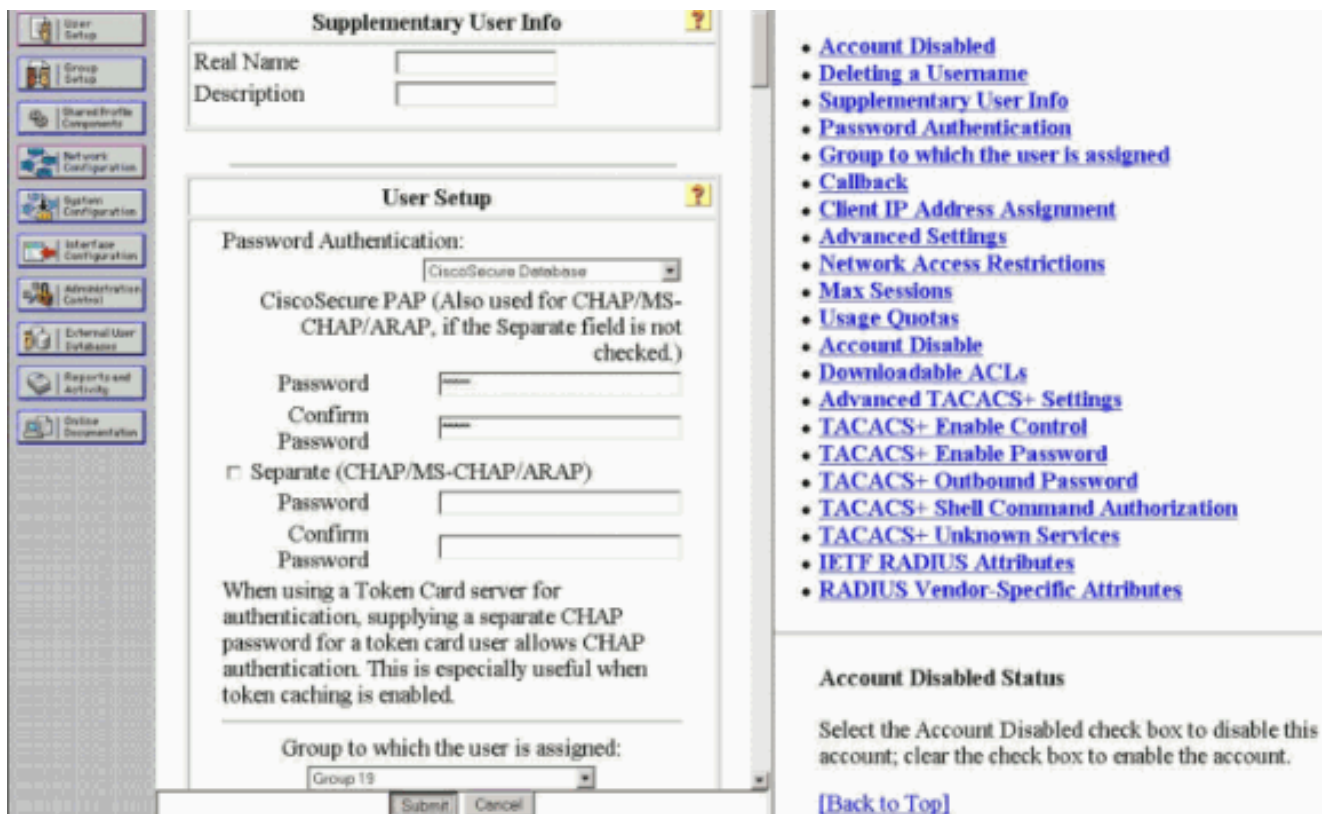


- [User Setup and External User Databases](#)
- [Finding a Specific User in the CiscoSecure User Database](#)
- [Adding a User to the CiscoSecure User Database](#)
- [Listing Usernames that Begin with a Particular Character](#)
- [Listing All Usernames in the CiscoSecure User Database](#)
- [Changing a Username in the CiscoSecure User Database](#)

User Setup enables you to configure individual user information, add users, and delete users in the database.

2. 在下一個窗口中，為使用者cisco指定口令。口令也是cisco。

您可以將使用者帳戶對映至群組。完成後，按一下Submit。



- [Account Disabled](#)
- [Deleting a Username](#)
- [Supplementary User Info](#)
- [Password Authentication](#)
- [Group to which the user is assigned](#)
- [Callback](#)
- [Client IP Address Assignment](#)
- [Advanced Settings](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Account Disable](#)
- [Downloadable ACLs](#)
- [Advanced TACACS+ Settings](#)
- [TACACS+ Enable Control](#)
- [TACACS+ Enable Password](#)
- [TACACS+ Outbound Password](#)
- [TACACS+ Shell Command Authorization](#)
- [TACACS+ Unknown Services](#)
- [IETF RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

**Account Disabled Status**

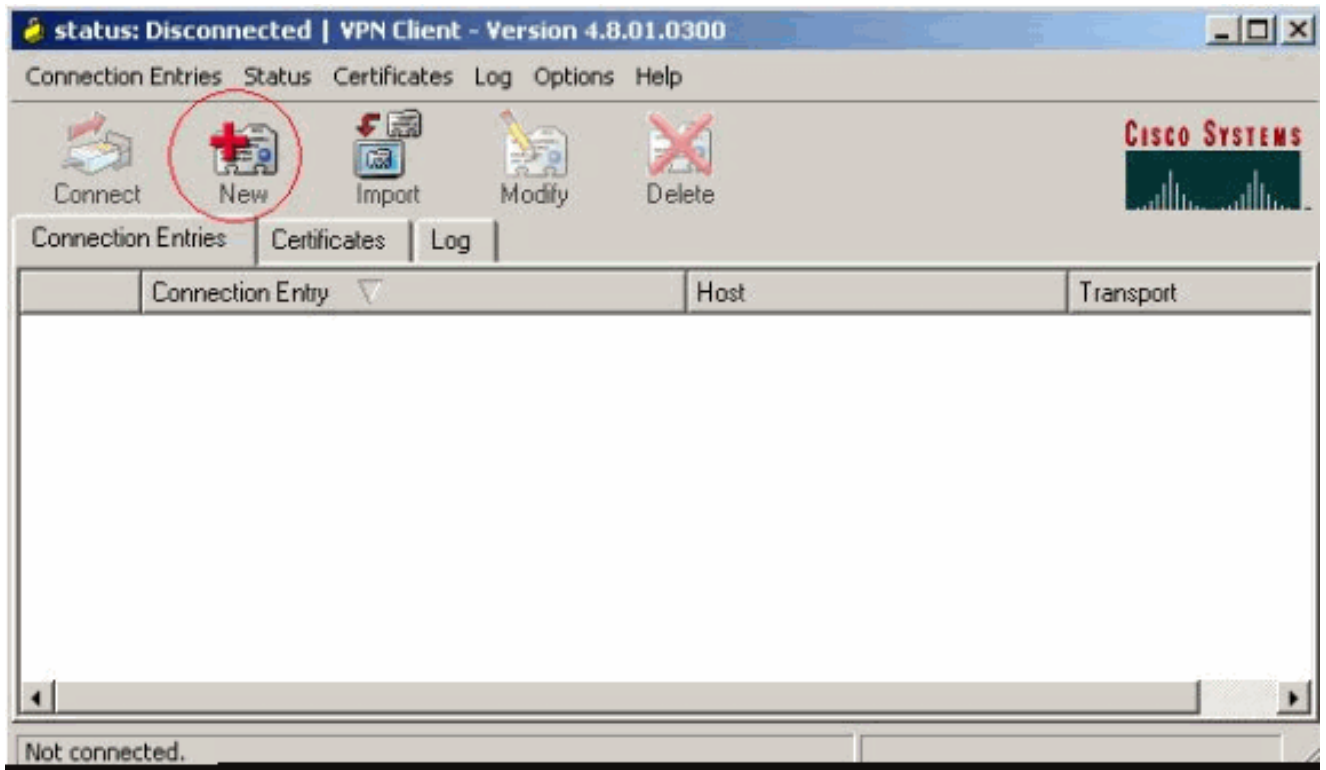
Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[\[Back to Top\]](#)

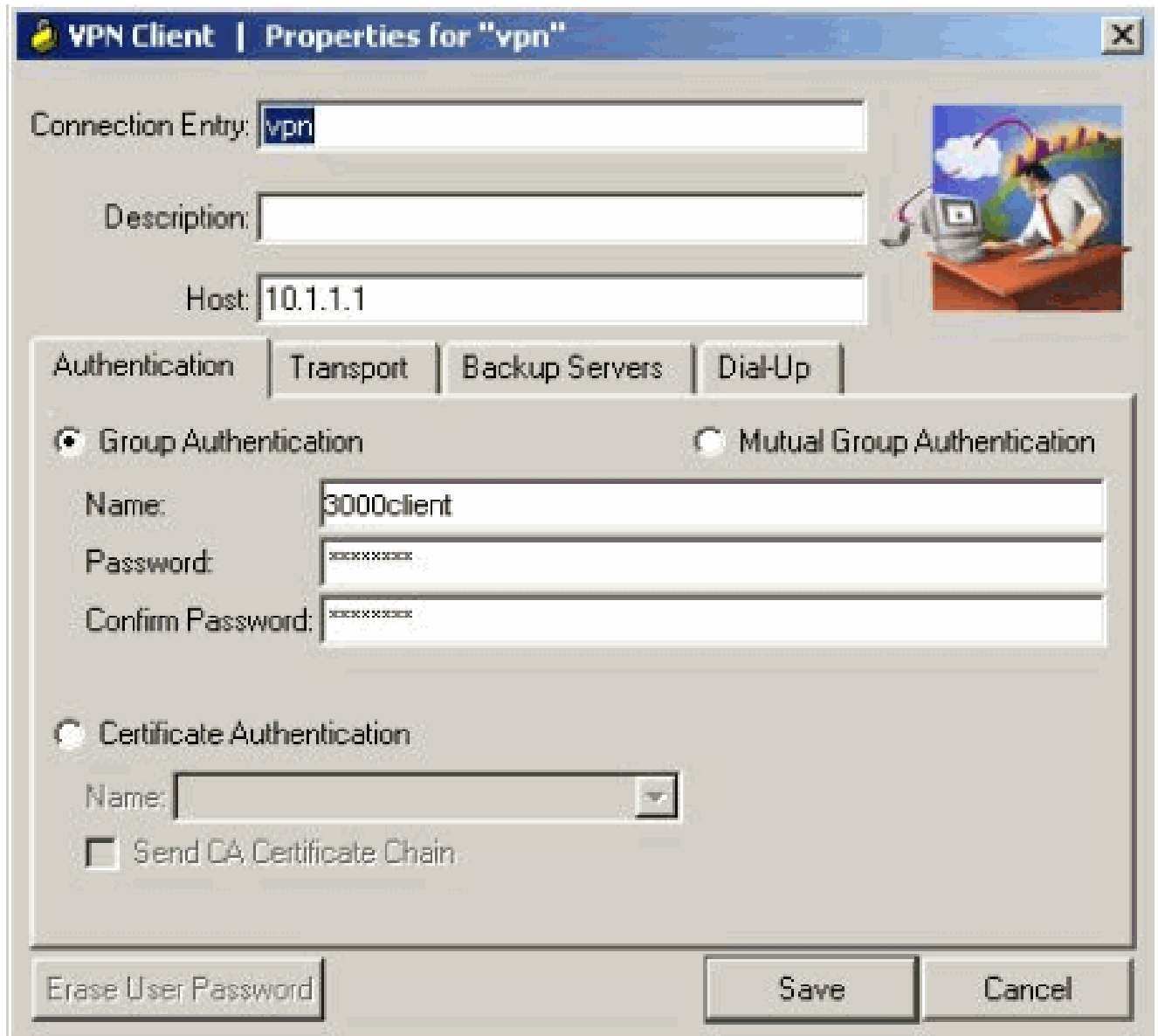
## VPN客戶端4.8配置

要配置VPN客戶端4.8，請完成以下步驟：

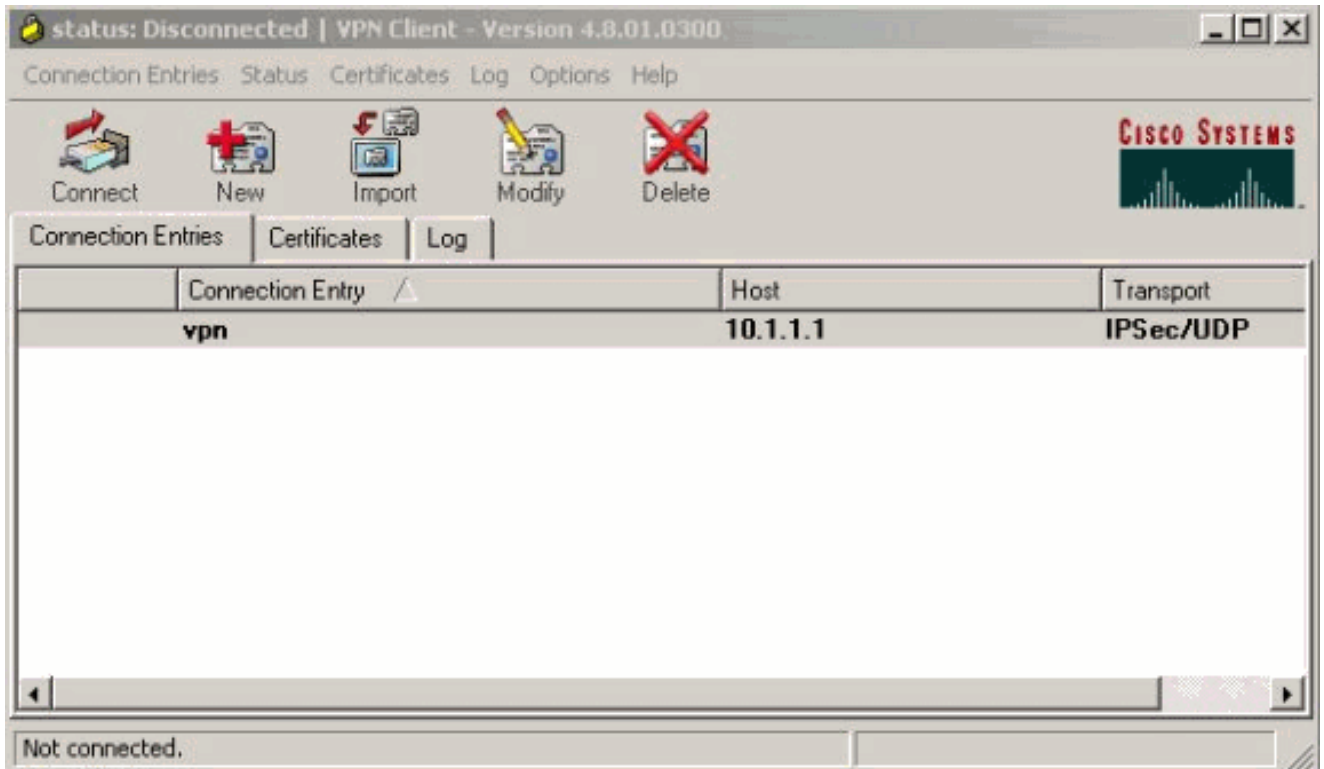
1. 選擇開始>程式> Cisco Systems VPN客戶端> VPN客戶端。
2. 按一下New以啟動Create New VPN Connection Entry窗口。



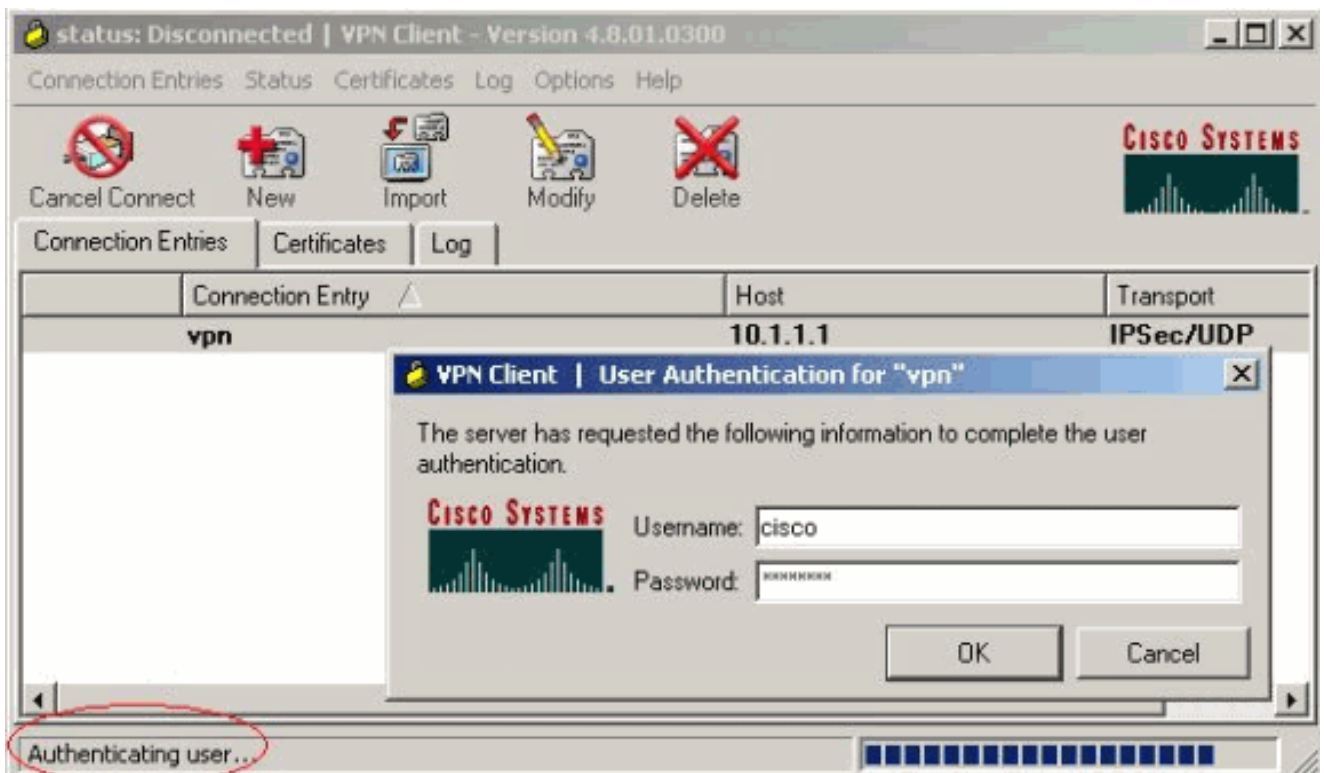
3. 輸入連線條目的名稱和說明。在Host框中輸入路由器的外部IP地址。然後輸入VPN組的名稱和口令，並按一下Save。



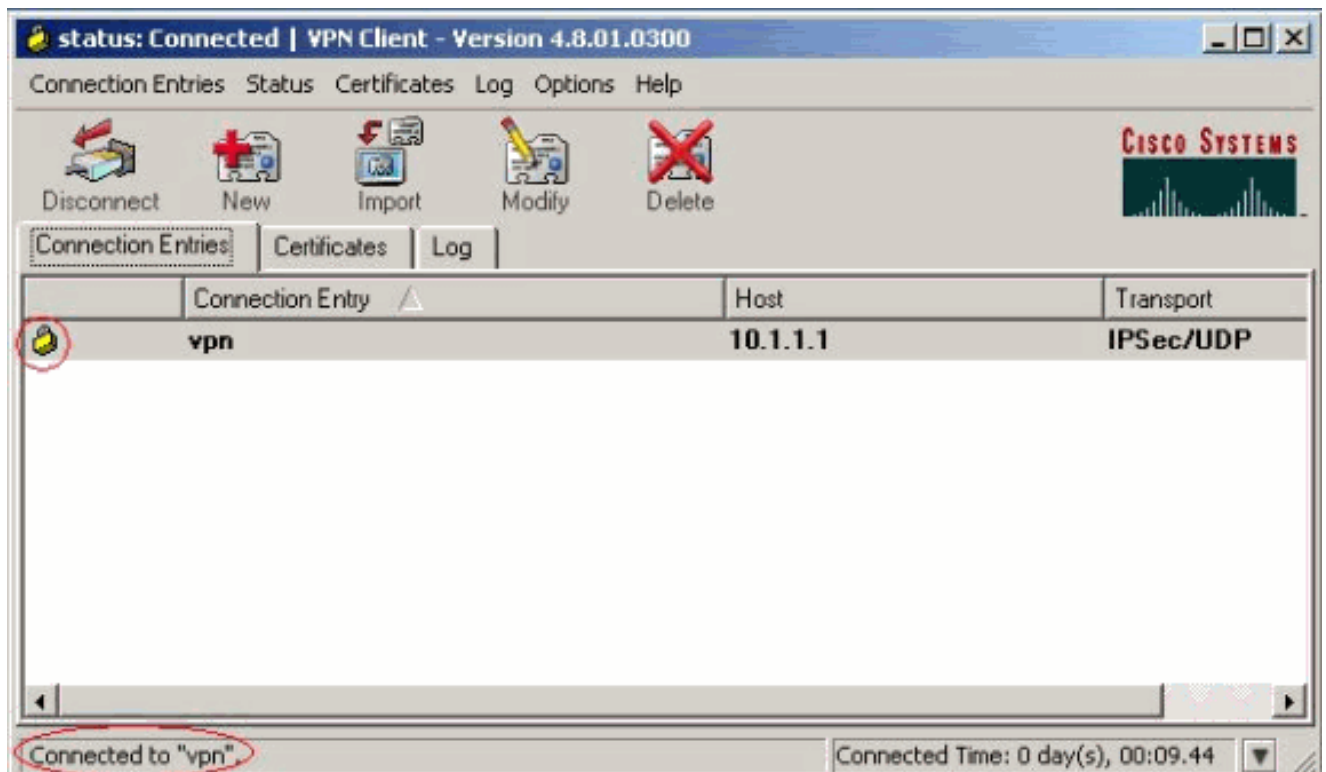
4. 按一下要使用的連線，然後在VPN客戶端主窗口中按一下Connect。



5. 出現提示時，輸入xauth的使用者名稱和口令資訊，然後按一下OK 以連線遠端網路。



VPN客戶端與中心站點的路由器連線。



## 驗證

使用本節內容，確認您的組態是否正常運作。

```
<#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

## 疑難排解

使用本節內容，對組態進行疑難排解。

### 疑難排解指令

使用 debug 指令之前，請先參閱[有關 Debug 指令的重要資訊。](#)

- debug crypto ipsec -顯示有關IPSec連線的調試資訊。
- debug crypto isakmp— 顯示有關IPSec連線的調試資訊，並顯示由於兩端不相容而被拒絕的第一組屬性。
- debug crypto engine -顯示來自加密引擎的資訊。
- debug aaa authentication -顯示有關AAA/TACACS+身份驗證的資訊。
- debug aaa authorization radius -顯示有關AAA/TACACS+授權的資訊。
- debug radius— 顯示有關RADIUS伺服器與路由器之間通訊故障排除的資訊。

### 調試輸出

本部分提供來自路由器的調試資訊，可用於排除配置故障。

### 路由器日誌

<#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:inac1=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:inac1=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 inac1=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_MSG_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_MSG_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_MSG_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_MSG_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  
0ld 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  
0ld 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  
0ld State = IKE\_XAUTH\_SET\_SENT New State = IKE\_P1\_COMPLETE

1w0d: ISAKMP (0:2): Input = IKE\_MESG\_INTERNAL, IKE\_PHASE1\_COMPLETE  
0ld 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
01d 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:inac1=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:inac1=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-JK903S-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\_MSG\_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, keysiz= 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-sh11
All possible debugging has been turned off
vpn2611#a-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x42FC1D6A(1123818858), conn_id= 2003, keysiz= 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
```

## 客戶端日誌

在VPN客戶端上啟動LogViewer以檢視日誌。確保所有已配置類的過濾器都設定為「高」。以下是日誌輸出示例：

```
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) 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-JK903S-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.

## 相關資訊

- [IPSec協商/IKE通訊協定支援](#)
- [要求建議\(RFC\)](#)
- [技術支援與文件 - Cisco Systems](#)



## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。