

# IPSec与VPN客户端(静态或动态分配IP地址)到VPN 3000集中器的配置示例

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[网络图](#)

[规则](#)

[配置VPN 3000集中器](#)

[分配静态IP地址到用户](#)

[配置 VPN 客户端](#)

[验证](#)

[故障排除](#)

[可能出现的错误](#)

[VPN 客户](#)

[VPN 集中器](#)

[VPN 3000 集中器 – 好的调试示例](#)

[相关信息](#)

## [简介](#)

此配置示例展示如何形成从运行Cisco VPN Client的PC的一个IPSec隧道(4.x和以后) (静态/动态指定的IP地址)到Cisco VPN 3000集中器为了使用户安全地访问网络在VPN集中器里面。

参考[使用Cisco Secure ACS for Windows用VPN 3000集中器-使用Cisco ACS](#) , [IPSec](#)为了学习与RADIUS验证的更加大致同样的方案。参考[配置有MS RADIUS的Cisco VPN 3000集中器](#)为了认识与MS-RADIUS验证的更加大致同样的方案。

## [先决条件](#)

### [要求](#)

本文档没有任何特定的要求。

### [使用的组件](#)

本文档中的信息基于以下软件和硬件版本：

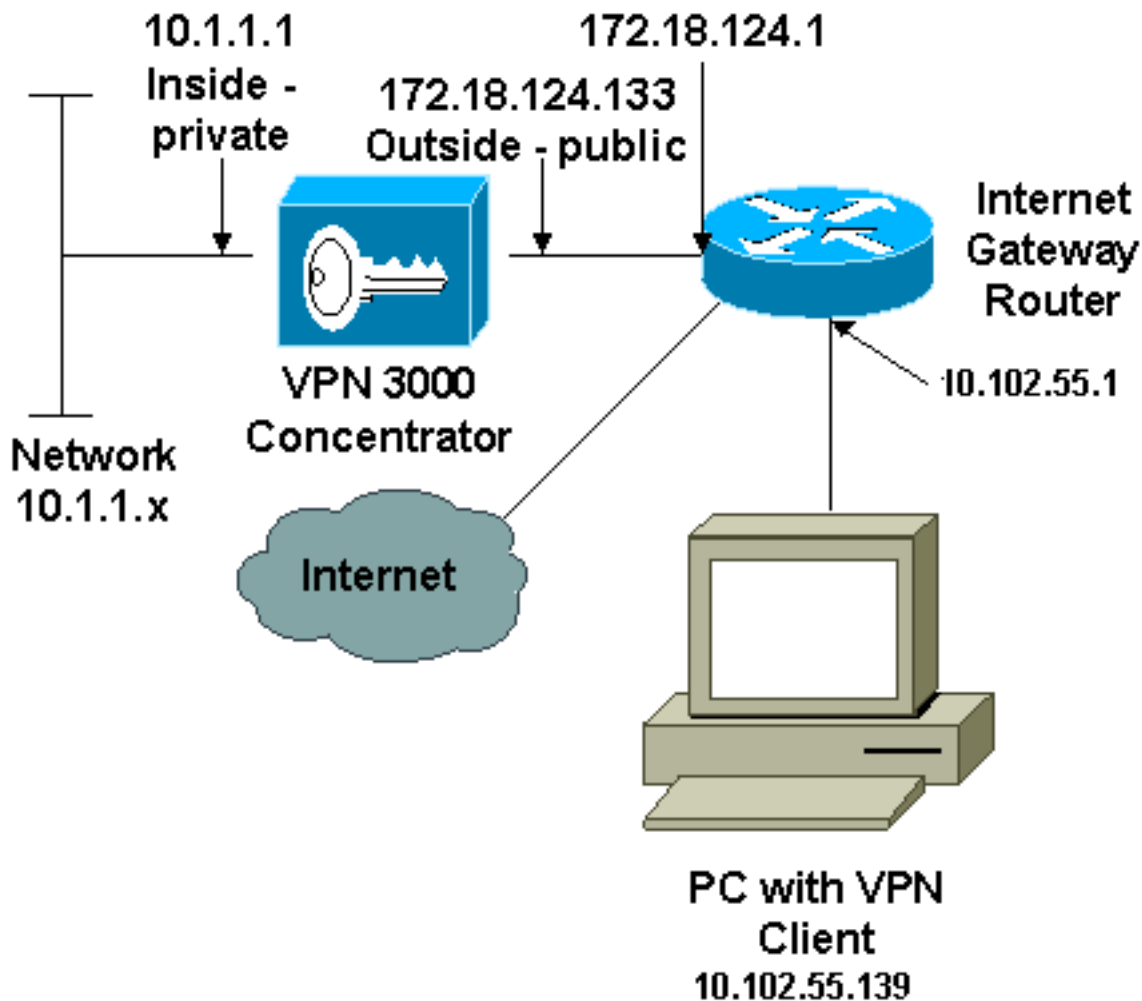
- Cisco VPN 3030集中器版本4.1.7.A
- Cisco VPN 客户端 4.x 及更高版本

**注意：** 使用Cisco VPN集中器版本4.7.2.H，此配置最近再测试。

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。

## 网络图

本文档使用以下网络设置：



**注意：** 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

## 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## 配置VPN 3000集中器

完成这些步骤为了配置VPN 3000集中器。

**注意：** 由于空间限制，一些屏幕截图显示仅部分屏幕。

1. 连接到VPN集中器控制台端口并且验证有IP地址分配到私有(里面)和公共(从外部)接口。另外，请验证有默认网关分配，因此VPN集中器能转发不知道到默认网关的目的地的数据包(通常互联网网关路由器)

```
97 01/21/2005 12:18:50.300 SEV=3 PSH/23 RPT=1
PSH - Console user "admin" failed login
Login: admin
Password:
```

```
                Welcome to
                Cisco Systems
        VPN 3000 Concentrator Series
        Command Line Interface
Copyright (C) 1998-2004 Cisco Systems, Inc.
```

- 1) Configuration
- 2) Administration
- 3) Monitoring
- 4) Save changes to Config file
- 5) Help Information
- 6) Exit

```
Main -> _
```

```
                Cisco Systems
        VPN 3000 Concentrator Series
        Command Line Interface
Copyright (C) 1998-2004 Cisco Systems, Inc.
```

- 1) Configuration
- 2) Administration
- 3) Monitoring
- 4) Save changes to Config file
- 5) Help Information
- 6) Exit

```
Main -> 1
```

- 1) Interface Configuration
- 2) System Management
- 3) User Management
- 4) Policy Management
- 5) Tunneling and Security
- 6) Back

```
Config -> 1
```

此表显示当前IP地址。

5) Tunneling and Security

6) Back

Config -> 1

This table shows current IP addresses.

Intf	Status	IP Address/Subnet Mask	MAC Address
Ether1-Pri	UP	10.1.1.1/255.255.255.0	00.90.A4.00.06.94
Ether2-Pub	UP	172.18.124.133/255.255.255.0	00.90.A4.00.06.95
Ether3-Ext	Not Configured	0.0.0.0/0.0.0.0	

DNS Server(s): 10.1.0.121, 10.1.0.122

DNS Domain Name:

Default Gateway: 172.18.124.1

- 1) Configure Ethernet #1 (Private)
- 2) Configure Ethernet #2 (Public)
- 3) Configure Ethernet #3 (External)
- 4) Configure Power Supplies
- 5) Back

Interfaces ->

DNS Domain Name:

Default Gateway: 172.18.124.1

- 1) Configure Ethernet #1 (Private)
- 2) Configure Ethernet #2 (Public)
- 3) Configure Ethernet #3 (External)
- 4) Configure Power Supplies

5) Back

Interfaces -> 5

- 1) Interface Configuration
- 2) System Management
- 3) User Management
- 4) Policy Management
- 5) Tunneling and Security
- 6) Back

Config -> 2

- 1) Servers (Authentication, Authorization, Accounting, DNS, DHCP, etc.)
- 2) Address Management
- 3) IP Routing (static routes, OSPF, etc.)
- 4) Management Protocols (Telnet, TFTP, FTP, etc.)
- 5) Event Configuration
- 6) General Config (system name, time, etc.)
- 7) Client Update
- 8) Load Balancing Configuration
- 9) Back

System -> 3\_

8) Load Balancing Configuration  
9) Back

System -> 3

1) Static Routes  
2) Default Gateways

3) OSPF  
4) OSPF Areas  
5) DHCP Parameters  
6) Redundancy  
7) Reverse Route Injection  
8) DHCP Relay  
9) Back

Routing -> 1

Static Routes

Destination	Mask	Metric	Destination
0.0.0.0	0.0.0.0	1	172.18.124.1
10.0.0.0	255.0.0.0	10	10.1.16.111
192.168.0.0	255.255.0.0	10	10.1.16.111

1) Add Static Route  
2) Modify Static Route  
3) Delete Static Route  
4) Back

Routing ->

8) Load Balancing Configuration  
9) Back

System -> 3

1) Static Routes  
2) Default Gateways

3) OSPF  
4) OSPF Areas  
5) DHCP Parameters  
6) Redundancy  
7) Reverse Route Injection  
8) DHCP Relay  
9) Back

Routing -> 1

Static Routes

Destination	Mask	Metric	Destination
0.0.0.0	0.0.0.0	1	172.18.124.1

1) Add Static Route  
2) Modify Static Route  
3) Delete Static Route  
4) Back

Routing ->

2. 确保您选择公共接口的公共过滤器选项。



You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.

## Configuring Ethernet Interface 2 (Public).

General Parameters			
Sel	Attribute	Value	Description
<input type="radio"/>	Disabled		Select to disable this interface.
<input type="radio"/>	DHCP Client		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.
<input checked="" type="radio"/>	Static IP Addressing		Select to configure the IP Address and Subnet Mask.
	IP Address	192.168.1.2	Enter the IP Address and Subnet Mask for this interface.
	Subnet Mask	255.255.255.0	
	Public Interface	<input checked="" type="checkbox"/>	Check to make this interface a "public" interface.
	MAC Address	00.03.A0.89.BF.D1	The MAC address for this interface.
	Filter	2. Public (Default)	Select the filter for this interface.
	Speed	10/100 auto	Select the speed for this interface.

3. 点一个浏览器VPN集中器的内部接口并且选择**Configuration > System > Address Management > 地址池>Add**为了分配一可用的IP地址范围。指定与在网络内部的任何其它设备不相冲突的IP地址范围：**注意**：因为过滤器在仅，实验室设置被添加允许此这些屏幕截图显示外部公共接口管理。

VPN 3000  
Concentrator Series Manager

Configuration | System | Address Management | Pools | Add

Add an address pool.

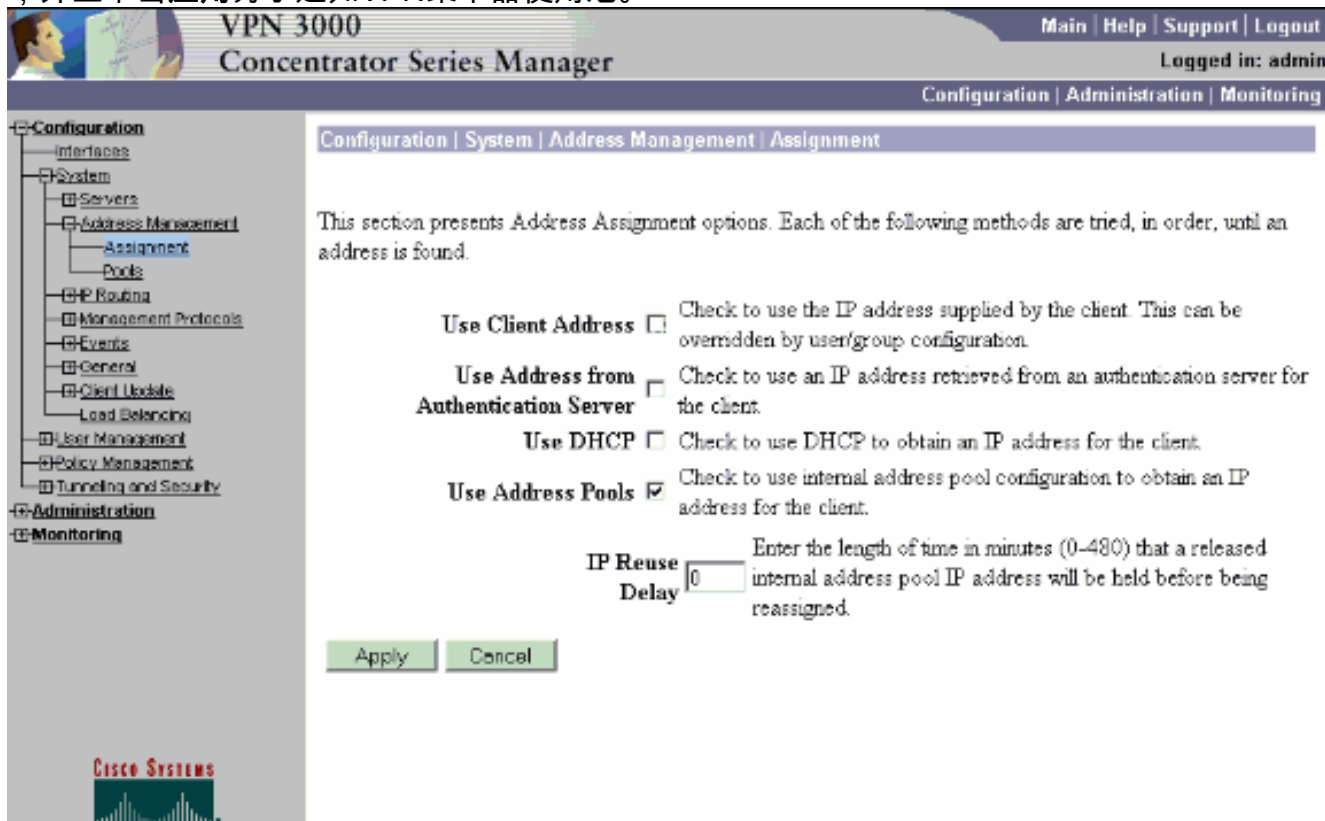
Range Start  Enter the start of the IP pool address range.

Range End  Enter the end of the IP pool address range.

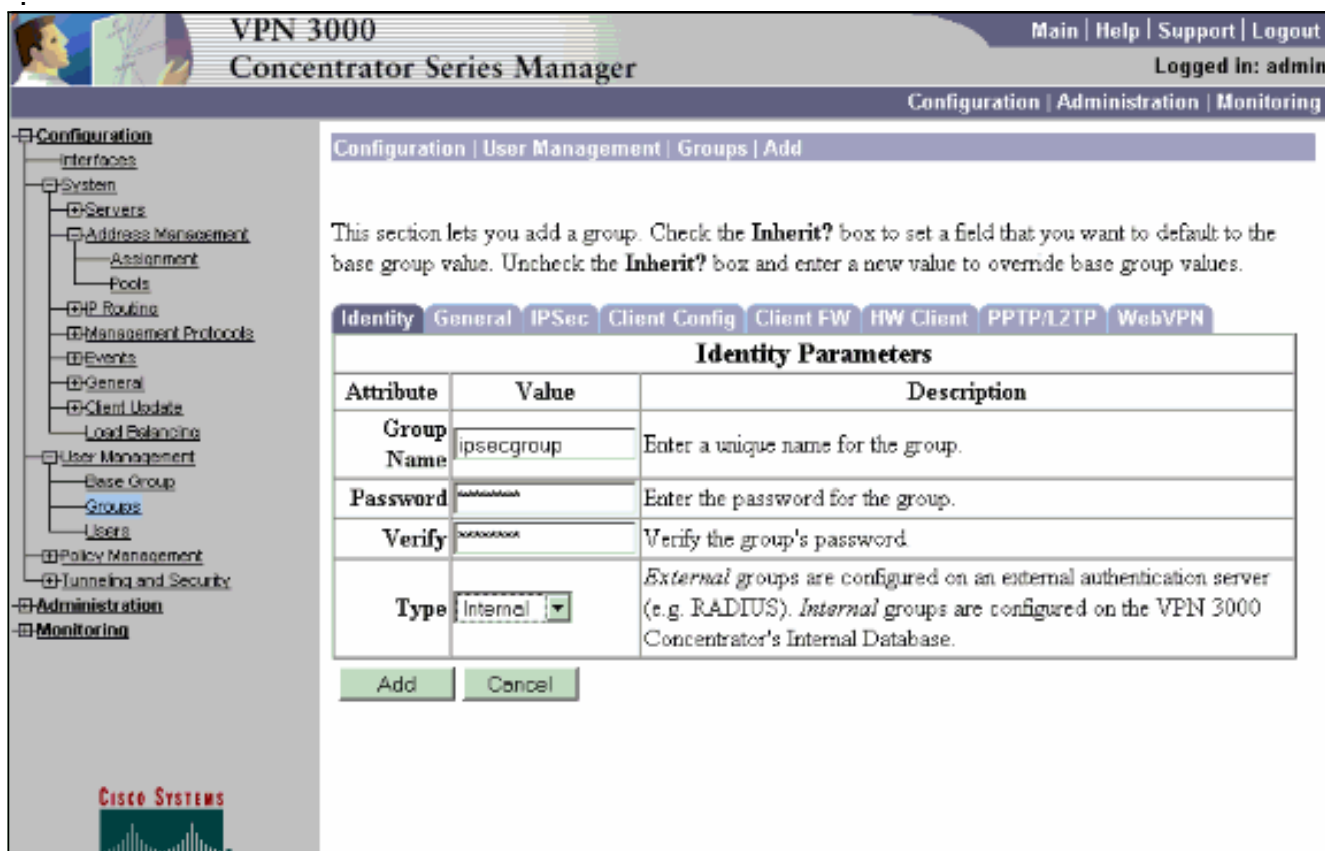
Subnet Mask  Enter the subnet mask of the IP pool address range.  
Enter 0.0.0.0 to use default behavior.

4. 选择**Configuration > System > Address Management > Assignment**，检查使用地址池方框

，并且单击应用为了通知VPN集中器使用池。



5. 选择Configuration > User Management > Groups > Add组为了配置用户的一个IPSec组和定义组名和密码。此示例以password/verify="cisco123"使用group= " ipsecgroup"



6. 在组的常规选项卡，请验证IPSec选择。

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration

- Interfaces
- System
  - Servers
  - Address Management
    - Assignment
    - Pools
  - IP Routing
  - Management Protocols
  - Events
  - General
  - Client Update
  - Load Balancing
- User Management
  - Base Group
  - Groups
  - Users
- Policy Management
- Tunneling and Security

Administration

Monitoring

Secondary DNS	<input type="text"/>	<input checked="" type="checkbox"/>	secondary DNS server.
Primary WINS	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the IP address of the primary WINS server.
Secondary WINS	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the IP address of the secondary WINS server.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select the SEP cards this group can be assigned to.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec <input checked="" type="checkbox"/> WebVPN	<input checked="" type="checkbox"/>	Select the tunneling protocols this group can connect with.
Strip Realm	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to remove the realm qualifier of the username during authentication.
DHCP Network Scope	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the IP sub-network to which users within this group will be assigned when using the concentrator as a DHCP Proxy.

Apply Cancel

CISCO SYSTEMS

7. 在组的IPSec选项，请验证验证设置对内部。从当前组选项选择Configuration > User Management > Groups > modify group和挑选ipsecgroup为了执行此。

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration

- Interfaces
- System
  - Servers
  - Address Management
    - Assignment
    - Pools
  - IP Routing
  - Management Protocols
  - Events
  - General
  - Client Update
  - Load Balancing
- User Management
  - Base Group
  - Groups
  - Users
- Policy Management
- Tunneling and Security

Administration

Monitoring

Confidence Interval	300	<input checked="" type="checkbox"/>	When a peer is permitted to idle before the VPN Concentrator checks to see if it is still connected.
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
<b>Remote Access Parameters</b>			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	Internal	<input checked="" type="checkbox"/>	Select the authentication method for members of this group. This parameter does not apply to <b>Individual User Authentication</b> .
Authorization Type	None	<input checked="" type="checkbox"/>	If members of this group need authorization in addition to authentication, select an authorization method. If you configure

CISCO SYSTEMS

8. 选择Configuration > User Management > Users > Add，并且以前添加用户到定义的组。在本例中，用户是“ipsecuser”用密码“xyz12345”在组“ipsecgroup”中

:



VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity | General | IPsec | PPTP/L2TP

Identity Parameters		
Attribute	Value	Description
Username	ipseccuser	Enter a unique username.
Password	*****	Enter the user's password. The password must satisfy the group password requirements.
Verify	*****	Verify the user's password.
Group	ipseccgroup	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Add Cancel

CISCO SYSTEMS

## 分配静态IP地址到用户

为了为远程VPN用户分配静态IP地址，在他们连接到VPN 3000系列集中器时候，请选择 **Configuration > User Management > Users > Modify ipsecuser2 > 标识**。在用户的(ipsecuser2)此配置中，静态IP地址10.2.2.1/24分配，在用户连接时候。

Configuration | User Management | Users | Modify ipsecuser2

Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inherit?** box and enter values.

Identity | General | IPsec | PPTP/L2TP

Identity Parameters		
Attribute	Value	Description
Username	ipseccuser2	Enter a unique username.
Password	*****	Enter the user's password. The password must satisfy the group password re.
Verify	*****	Verify the user's password.
Group	ipseccgroup	Enter the group to which this user belongs.
IP Address	10.2.2.1	Enter the IP address assigned to this user.
Subnet Mask	255.255.255.0	Enter the subnet mask assigned to this user.

Apply Cancel

**注意：**请务必去**Configuration > System > Address Management > Assignment**为了保证VPN集中器设置指定的IP地址。检查从认证服务器从认证服务器逐个用户检索的分配IP地址的**使用地址**。在**用户管理 > Users > Add或Modify窗口**的标识参数选项卡和子网掩码输入的IP地址认为在内部认证服务器。

This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.

**Use Client Address**  Check to use the IP address supplied by the client. This can be overridden by user/group configuration.

**Use Address from Authentication Server**  Check to use an IP address retrieved from an authentication server for the client.

**Use DHCP**  Check to use DHCP to obtain an IP address for the client.

**Use Address Pools**  Check to use internal address pool configuration to obtain an IP address for the client.

**IP Reuse Delay**  Enter the length of time in minutes (0-480) that a released internal address pool IP address will be held before being reassigned.

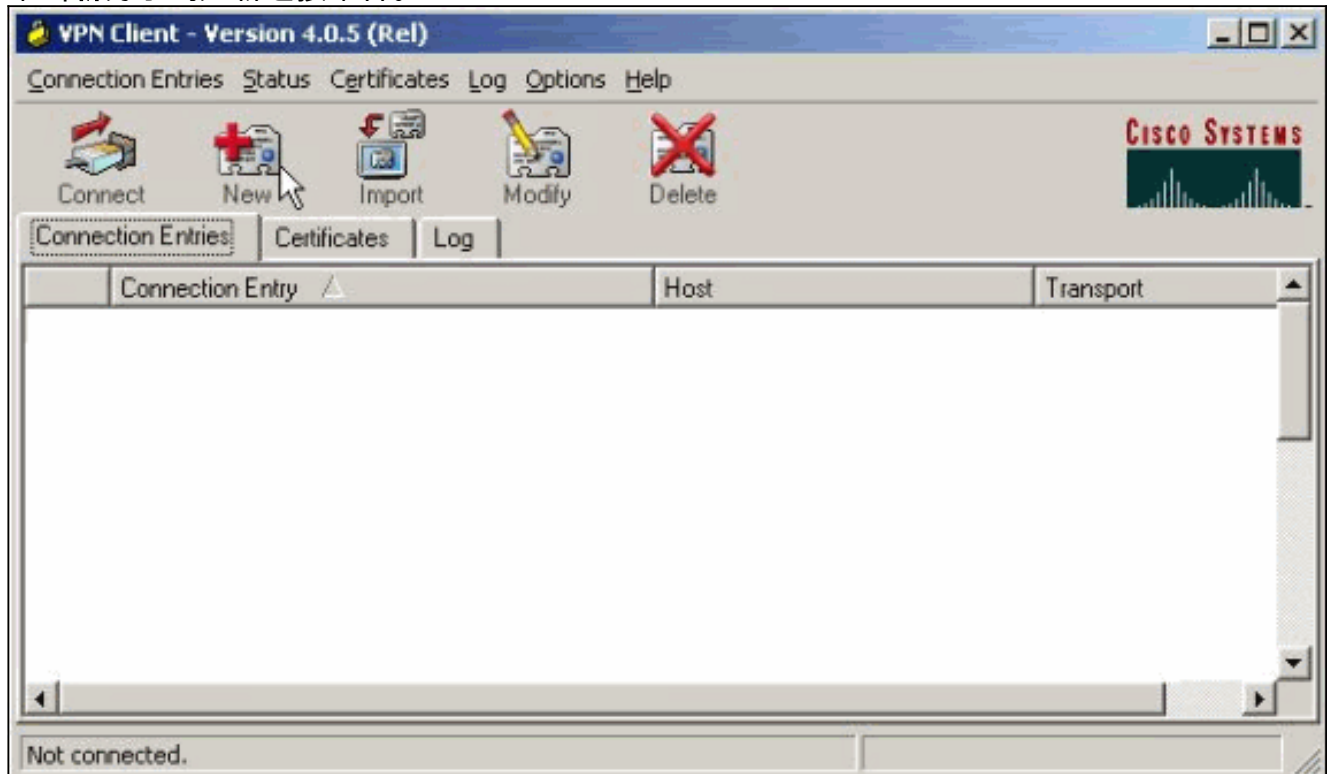
Apply

Cancel

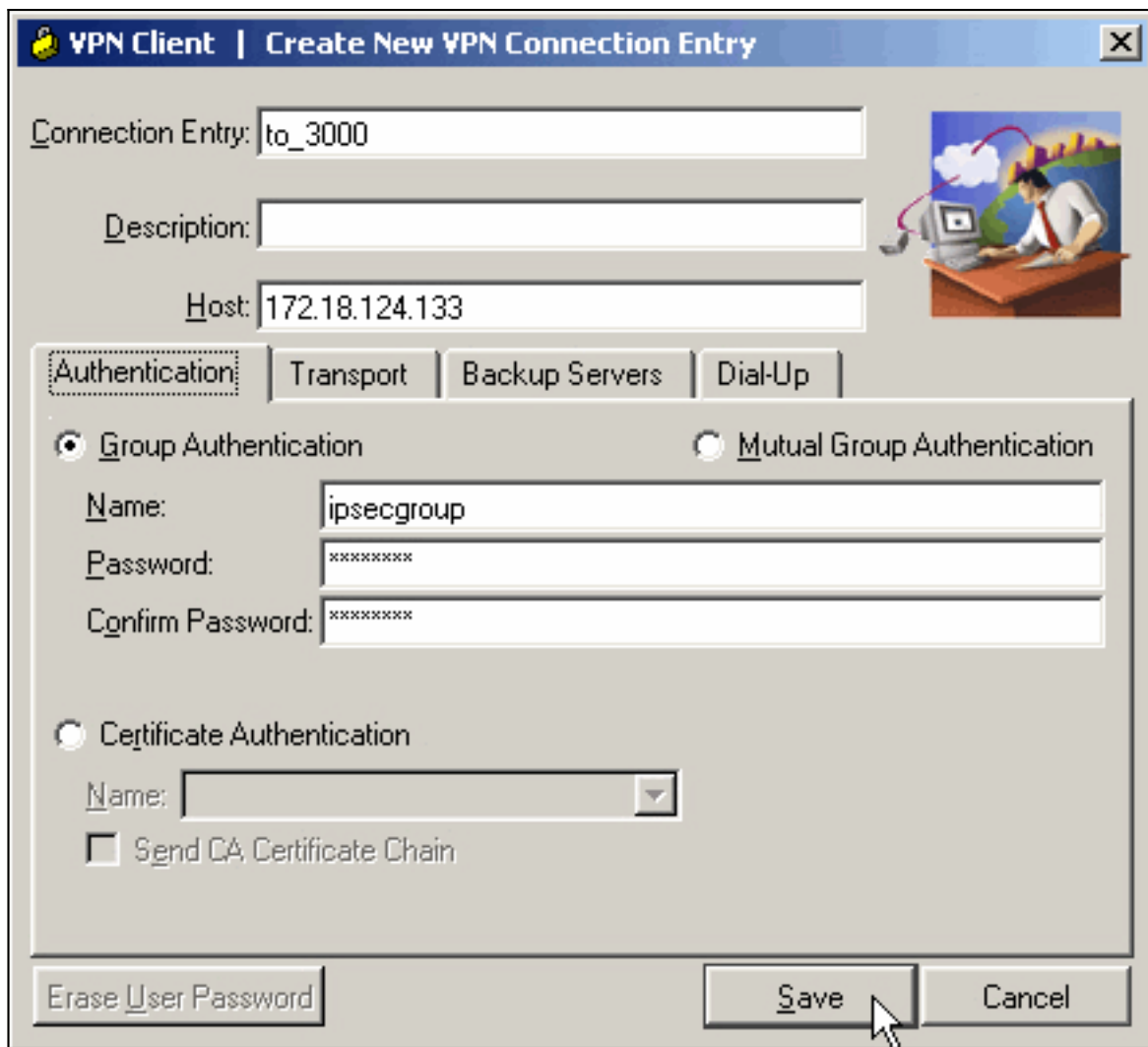
## 配置 VPN 客户端

执行下列步骤以配置 VPN 客户端。

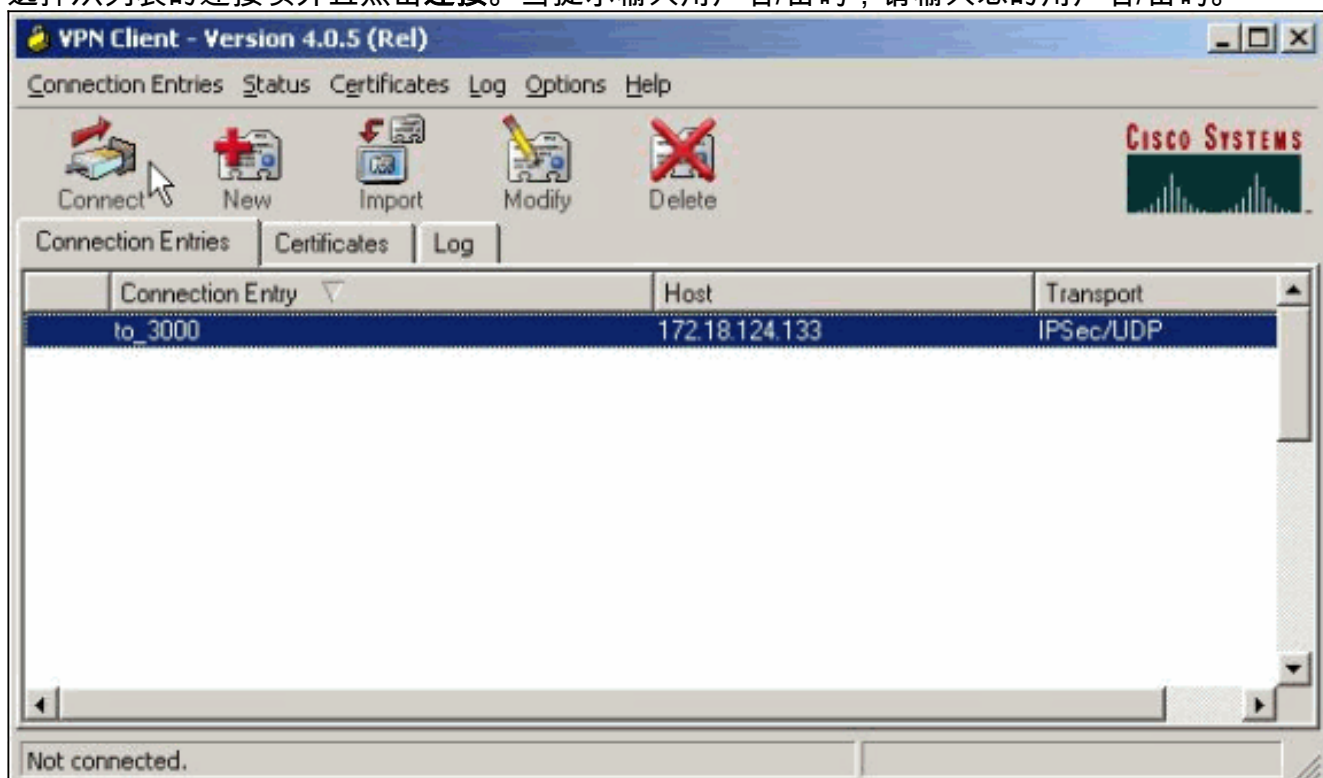
1. 单击新为了创建新连接条目。



2. 给出连接，输入VPN集中器的公共接口的IP地址并且提供组凭证。在这种情况下，名称是 ipsecgroup，并且密码是cisco123。点击“Save”，当完成。



3. 选择从列表的连接项并且点击**连接**。当提示输入用户名/密码，请输入您的用户名/密码。



[验证](#)

当前没有可用于此配置的验证过程。

## 故障排除

您可以使用这些部分提供的信息对您的配置进行故障排除。

[命令输出解释程序 \(仅限注册用户\)](#) (OIT) 支持某些 **show** 命令。使用 OIT 可查看对 **show** 命令输出的分析。

**注意：** 发出 **debug** 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

## 可能出现的错误

这些是能生成的潜在的错误。请参阅[VPN客户端](#)和[VPN集中器](#)部分关于解决方法对这些错误。

- 用户收到消息IPSec。VPN 3000 Debug显示：`14 02/20/2001 08:59:29.100 SEV=4 IKE/22 RPT=5 10.102.55.139`  
No Group found matching badgroup for Pre-shared key peer 10.102.55.139**通常原因：**用户尝试连接没有配置的组名。
- 用户不能连接，并且VPN 3000 Debug显示：`Filter missing on interface 2, IKE data from Peer x.x.x.x dropped`**通常原因：**过滤器从公共接口未命中。它通常是“公共”过滤器(但是可以是专用过滤器;“什么都”不无效)。选择**Configuration > Interfaces > Ethernet 2 > Filter**并且做过滤器“公共”或别的值(即不是“无”)。请参阅本文[配置部分](#)关于如何配置过滤器的更多信息。
- 用户不能连接并且看见IPSec。VPN 3000 Debug显示：`Terminating connection attempt: IPSEC not permitted for group >group<`**通常原因：**IPsec在组没有选择。选择**Configuration > User Management > Groups ><group>>Modify>常规**并且验证IPSec选择在隧道协议下。
- 用户不能在许多尝试以后连接并且看到VPN 3000 Debug显示：`Authentication rejected: Reason = User was not found handle = 14, server = Internal, user = <user>`**通常原因：**用户在用户数据库不存在。确保您输入正确用户名，当用户认证窗口显示。
- 用户不能连接，并且VPN 3000 Debug显示：`Filter missing on interface 0, IKE data from Peer x.x.x.x dropped`**通常原因：**默认路由未命中。确保那里是一个默认路由在配置里。选择**Configuration > System > IP routing > Default Gateway**并且指定默认网关。
- 用户不能连接并且看见IPSec。VPN 3000 Debug显示：`User [ <user> ] IKE rcv'd FAILED IP Addr status!`**通常原因：**没有被检查的选项给VPN客户端IP地址。选择**Configuration > System > Address Management >地址分配**并且选择选项。
- 用户不能连接并且看到VPN 3000 Debug显示：`The calculated HASH doesn't match the received value`**通常原因：**在VPN客户端的组密码跟在VPN集中器配置的密码不同。检查在VPN客户端和集中器的密码。
- 您设置资源的VPN池在VPN集中器背后。您能访问资源，但是不能ping他们。**通常原因：**有PIX在阻塞ICMP数据包的VPN集中器背后。登陆对该PIX并且应用**access-list**启用ICMP数据包。
- 没有VPN集中器调试，并且所有或一些用户不能连接。默认VPN集中器公共过滤器包含规则允许此流量：`协议= UDP, port= 500协议= UDP, port= 10000协议= ESP协议= AH`如果VPN集中器的过滤器允许此流量，则在VPN客户端和VPN集中器之间的一个设备可以阻塞其中一些端口(或许防火墙)。为了验证，请设法连接到从网络的VPN集中器立即VPN集中器的外部。如果那工作，在VPN客户端PC和VPN集中器之间的一个设备阻塞流量。
- 用户不能连接并且看到这些日志：`07/10/2006 11:48:59.280 SEV=4 IKE/0 RPT=141 10.86.190.92`

Group [NYMVPN]

received an unencrypted packet when crypto active!! Dropping packet **通常原因**：一个不正确地定义的组名或密码。再创新的组名和密码在VPN 3000集中器VPN客户端的。

- 用户能ping或远程登录到一台主机在VPN集中器背后，但是用户不能使用远程桌面(RDP)或相似的应用程序。**通常原因**：公共过滤器在公共接口没有启用。请参阅在[配置的步骤2](#)本文的[VPN 3000集中器](#)部分。
- 用户能连接，但是流量没有通过VPN通道通过。**通常原因**：NAT-Transparency没有启用。在许多情况下VPN客户端是在PAT设备后。PAT依靠TCP和UDP端口号保存地址空间。但是ESP，封装VPN流量，是从TCP或UDP的一份分开的协议。这意味着许多PAT设备不能处理ESP流量。NAT-T封装在给他们的UDP数据包的ESP数据包容易地穿过PAT设备。因此，为了允许ESP流量流经PAT设备，您需要启用在集中器的NAT-T。参考[配置IPSec的NAT透明模式在VPN 3000集中器](#)欲知更多信息。

## [VPN 客户](#)

选择Start > Programs > Cisco系统VPN 3000客户端>日志查看器为了启动日志查看器。

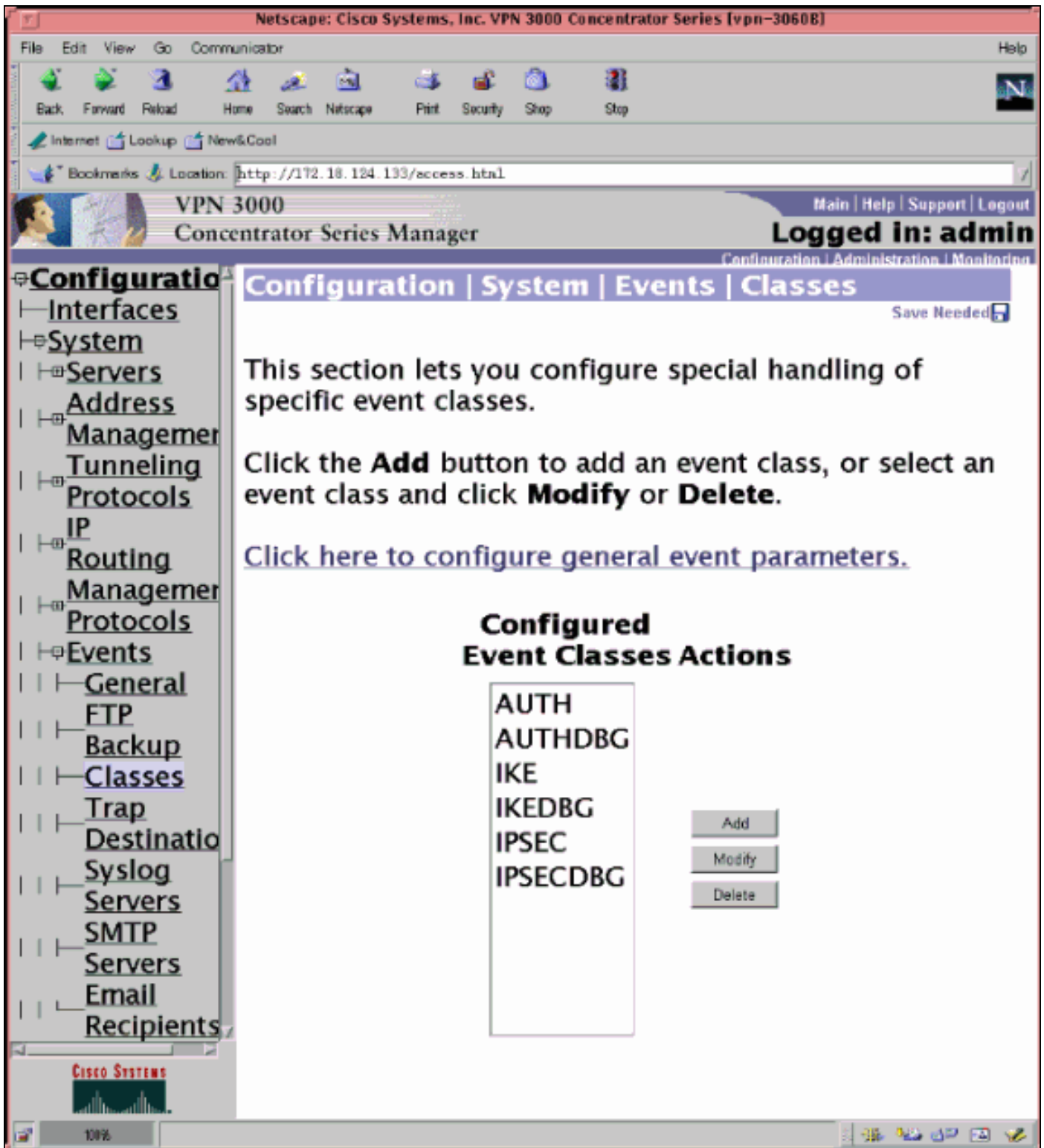
## [VPN 集中器](#)

如果有事件连接故障，请选择Configuration > System > Events > Classes为了打开此调试：

- 验证-记录1-13的严重性
- AUTHDBG -记录1-13的严重性
- IKE -记录1-13的严重性
- IKEDBG -记录1-13的严重性
- IPSEC-记录1-13的严重性
- IPSECDBG -记录1-13的严重性

**注意**：如果需要，AUTHDECODE，IKEDECODE，IPSECDECODE可以被添加的以后。

参考[在VPN 3000集中器的故障排除连接问题](#)关于其他故障排除详细信息。



选择Monitoring>可过滤的事件洛金定货查看日志。

## VPN 3000 集中器 – 好的调试示例

```

1 02/07/2002 08:00:13.320 SEV=8 IKEDBG/0 RPT=69 172.18.124.241
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + NONE (0) ... total length : 562

4 02/07/2002 08:00:13.320 SEV=9 IKEDBG/0 RPT=70 172.18.124.241
processing SA payload

5 02/07/2002 08:00:13.320 SEV=9 IKEDBG/0 RPT=71 172.18.124.241

```

processing ke payload

6 02/07/2002 08:00:13.320 SEV=9 IKEDBG/0 RPT=72 172.18.124.241  
processing ISA\_KE

7 02/07/2002 08:00:13.320 SEV=9 IKEDBG/1 RPT=7 172.18.124.241  
processing nonce payload

8 02/07/2002 08:00:13.320 SEV=9 IKEDBG/1 RPT=8 172.18.124.241  
Processing ID

9 02/07/2002 08:00:13.320 SEV=9 IKEDBG/47 RPT=4 172.18.124.241  
processing VID payload

10 02/07/2002 08:00:13.320 SEV=9 IKEDBG/49 RPT=4 172.18.124.241  
Received xauth V6 VID

11 02/07/2002 08:00:13.320 SEV=9 IKEDBG/47 RPT=5 172.18.124.241  
processing VID payload

12 02/07/2002 08:00:13.320 SEV=9 IKEDBG/49 RPT=5 172.18.124.241  
Received DPD VID

13 02/07/2002 08:00:13.320 SEV=9 IKEDBG/47 RPT=6 172.18.124.241  
processing VID payload

14 02/07/2002 08:00:13.320 SEV=9 IKEDBG/49 RPT=6 172.18.124.241  
Received Cisco Unity client VID

15 02/07/2002 08:00:13.320 SEV=9 IKEDBG/23 RPT=2 172.18.124.241  
Starting group lookup for peer 172.18.124.241

16 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/1 RPT=2  
AUTH\_Open() returns 136

17 02/07/2002 08:00:13.320 SEV=7 AUTH/12 RPT=2  
Authentication session opened: handle = 136

18 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/3 RPT=2  
AUTH\_PutAttrTable(136, 728a84)

19 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/6 RPT=2  
AUTH\_GroupAuthenticate(136, 9b143bc, 482fb0)

20 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/59 RPT=2  
AUTH\_BindServer(9a08630, 0, 0)

21 02/07/2002 08:00:13.320 SEV=9 AUTHDBG/69 RPT=2  
Auth Server 16b3fa0 has been bound to ACB 9a08630, sessions = 1

22 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/65 RPT=2  
AUTH\_CreateTimer(9a08630, 0, 0)

23 02/07/2002 08:00:13.320 SEV=9 AUTHDBG/72 RPT=2  
Reply timer created: handle = 3B2001B

24 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/61 RPT=2  
AUTH\_BuildMsg(9a08630, 0, 0)

25 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/64 RPT=2  
AUTH\_StartTimer(9a08630, 0, 0)

26 02/07/2002 08:00:13.320 SEV=9 AUTHDBG/73 RPT=2  
Reply timer started: handle = 3B2001B, timestamp = 10085308, timeout = 30000

27 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/62 RPT=2  
AUTH\_SndRequest(9a08630, 0, 0)

28 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/50 RPT=3  
IntDB\_Decode(62b6d00, 115)

29 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/47 RPT=3  
IntDB\_Xmt(9a08630)

30 02/07/2002 08:00:13.320 SEV=9 AUTHDBG/71 RPT=2  
xmit\_cnt = 1

31 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/47 RPT=4  
IntDB\_Xmt(9a08630)

32 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/49 RPT=2  
IntDB\_Match(9a08630, 2ebe71c)

33 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/63 RPT=2  
AUTH\_RcvReply(9a08630, 0, 0)

34 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/50 RPT=4  
IntDB\_Decode(2ebe71c, 44)

35 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/48 RPT=2  
IntDB\_Rcv(9a08630)

36 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/66 RPT=2  
AUTH\_DeleteTimer(9a08630, 0, 0)

37 02/07/2002 08:00:13.420 SEV=9 AUTHDBG/74 RPT=2  
Reply timer stopped: handle = 3B2001B, timestamp = 10085318

38 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/58 RPT=2  
AUTH\_Callback(9a08630, 0, 0)

39 02/07/2002 08:00:13.420 SEV=6 AUTH/41 RPT=2 172.18.124.241  
Authentication successful: handle = 136, server = Internal, group = ipsecgroup

40 02/07/2002 08:00:13.420 SEV=7 IKEDBG/0 RPT=73 172.18.124.241  
Group [ipsecgroup]  
Found Phase 1 Group (ipsecgroup)

41 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/4 RPT=2  
AUTH\_GetAttrTable(136, 728c4c)

42 02/07/2002 08:00:13.420 SEV=7 IKEDBG/14 RPT=2 172.18.124.241  
Group [ipsecgroup]  
Authentication configured for Internal

43 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/2 RPT=2  
AUTH\_Close(136)

44 02/07/2002 08:00:13.420 SEV=9 IKEDBG/0 RPT=74 172.18.124.241  
Group [ipsecgroup]  
processing IKE SA

45 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=75 172.18.124.241  
Group [ipsecgroup]  
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class Hash Alg:



Rcv'd: SHA  
Cfg'd: MD5

50 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=76 172.18.124.241

Group [ipsecgroup]

Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class Hash Alg:

Rcv'd: SHA  
Cfg'd: MD5

53 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=77 172.18.124.241

Group [ipsecgroup]

Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class DH Group:

Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

57 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=78 172.18.124.241

Group [ipsecgroup]

Phase 1 failure against global IKE proposal # 4:  
Mismatched attr types for class DH Group:

Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

61 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=79 172.18.124.241

Group [ipsecgroup]

Phase 1 failure against global IKE proposal # 5:  
Mismatched attr types for class DH Group:

Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 7

65 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=80 172.18.124.241

Group [ipsecgroup]

Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class Hash Alg:

Rcv'd: SHA  
Cfg'd: MD5

68 02/07/2002 08:00:13.420 SEV=7 IKEDBG/28 RPT=2 172.18.124.241

Group [ipsecgroup]

IKE SA Proposal # 1, Transform # 2 acceptable  
Matches global IKE entry # 1

70 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/60 RPT=2

AUTH\_UnbindServer(9a08630, 0, 0)

71 02/07/2002 08:00:13.420 SEV=9 AUTHDBG/70 RPT=2

Auth Server 16b3fa0 has been unbound from ACB 9a08630, sessions = 0

72 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/10 RPT=2

AUTH\_Int\_FreeAuthCB(9a08630)

73 02/07/2002 08:00:13.420 SEV=7 AUTH/13 RPT=2

Authentication session closed: handle = 136

74 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=81 172.18.124.241

Group [ipsecgroup]

constructing ISA\_SA for isakmp

75 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=82 172.18.124.241

Group [ipsecgroup]

constructing ke payload

76 02/07/2002 08:00:13.450 SEV=9 IKEDBG/1 RPT=9 172.18.124.241  
Group [ipsecgroup]  
constructing nonce payload

77 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=83 172.18.124.241  
Group [ipsecgroup]  
Generating keys for Responder...

78 02/07/2002 08:00:13.450 SEV=9 IKEDBG/1 RPT=10 172.18.124.241  
Group [ipsecgroup]  
constructing ID

79 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=84  
Group [ipsecgroup]  
construct hash payload

80 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=85 172.18.124.241  
Group [ipsecgroup]  
computing hash

81 02/07/2002 08:00:13.450 SEV=9 IKEDBG/46 RPT=5 172.18.124.241  
Group [ipsecgroup]  
constructing Cisco Unity VID payload

82 02/07/2002 08:00:13.450 SEV=9 IKEDBG/46 RPT=6 172.18.124.241  
Group [ipsecgroup]  
constructing xauth V6 VID payload

83 02/07/2002 08:00:13.450 SEV=9 IKEDBG/46 RPT=7 172.18.124.241  
Group [ipsecgroup]  
constructing dpd vid payload

84 02/07/2002 08:00:13.450 SEV=9 IKEDBG/46 RPT=8 172.18.124.241  
Group [ipsecgroup]  
constructing VID payload

85 02/07/2002 08:00:13.450 SEV=9 IKEDBG/48 RPT=2 172.18.124.241  
Group [ipsecgroup]  
Send Altiga GW VID

86 02/07/2002 08:00:13.450 SEV=8 IKEDBG/0 RPT=86 172.18.124.241  
SENDING Message (msgid=0) with payloads :  
HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) ... total length : 344

89 02/07/2002 08:00:13.480 SEV=8 IKEDBG/0 RPT=87 172.18.124.241  
RECEIVED Message (msgid=0) with payloads :  
HDR + HASH (8) + NOTIFY (11) + NONE (0) ... total length : 76

91 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=88 172.18.124.241  
Group [ipsecgroup]  
processing hash

92 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=89 172.18.124.241  
Group [ipsecgroup]  
computing hash

93 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=90 172.18.124.241  
Group [ipsecgroup]  
Processing Notify payload

94 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=91 172.18.124.241  
Group [ipsecgroup]  
constructing blank hash

95 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=92 172.18.124.241  
Group [ipsecgroup]  
constructing qm hash

96 02/07/2002 08:00:13.480 SEV=8 IKEDBG/0 RPT=93 172.18.124.241  
SENDING Message (msgid=ec88ba81) with payloads :  
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 100

98 02/07/2002 08:00:21.810 SEV=8 IKEDBG/0 RPT=94 172.18.124.241  
RECEIVED Message (msgid=ec88ba81) with payloads :  
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 85

100 02/07/2002 08:00:21.810 SEV=9 IKEDBG/1 RPT=11  
process\_attr(): Enter!

101 02/07/2002 08:00:21.810 SEV=9 IKEDBG/1 RPT=12  
Processing MODE\_CFG Reply attributes.

102 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/1 RPT=3  
AUTH\_Open() returns 137

103 02/07/2002 08:00:21.810 SEV=7 AUTH/12 RPT=3  
Authentication session opened: handle = 137

104 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/3 RPT=3  
AUTH\_PutAttrTable(137, 728a84)

105 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/5 RPT=1  
AUTH\_Authenticate(137, 50093bc, 4b5708)

106 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/59 RPT=3  
AUTH\_BindServer(9b1544c, 0, 0)

107 02/07/2002 08:00:21.810 SEV=9 AUTHDBG/69 RPT=3  
Auth Server 16b3fa0 has been bound to ACB 9b1544c, sessions = 1

108 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/65 RPT=3  
AUTH\_CreateTimer(9b1544c, 0, 0)

109 02/07/2002 08:00:21.810 SEV=9 AUTHDBG/72 RPT=3  
Reply timer created: handle = 3B4001A

110 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/61 RPT=3  
AUTH\_BuildMsg(9b1544c, 0, 0)

111 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/64 RPT=3  
AUTH\_StartTimer(9b1544c, 0, 0)

112 02/07/2002 08:00:21.810 SEV=9 AUTHDBG/73 RPT=3  
Reply timer started: handle = 3B4001A, timestamp = 10086157, timeout = 30000

113 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/62 RPT=3  
AUTH\_SndRequest(9b1544c, 0, 0)

114 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/50 RPT=5  
IntDB\_Decode(62b6d00, 102)

115 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/47 RPT=5  
IntDB\_Xmt(9b1544c)

116 02/07/2002 08:00:21.810 SEV=9 AUTHDBG/71 RPT=3  
xmit\_cnt = 1

117 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/47 RPT=6  
IntDB\_Xmt(9b1544c)

118 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/49 RPT=3  
IntDB\_Match(9b1544c, 2ebe71c)

119 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/63 RPT=3  
AUTH\_RcvReply(9b1544c, 0, 0)

120 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/50 RPT=6  
IntDB\_Decode(2ebe71c, 62)

121 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/48 RPT=3  
IntDB\_Rcv(9b1544c)

122 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/66 RPT=3  
AUTH\_DeleteTimer(9b1544c, 0, 0)

123 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/74 RPT=3  
Reply timer stopped: handle = 3B4001A, timestamp = 10086167

124 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/58 RPT=3  
AUTH\_Callback(9b1544c, 0, 0)

125 02/07/2002 08:00:21.910 SEV=6 AUTH/4 RPT=1 172.18.124.241  
Authentication successful: handle = 137, server = Internal, user = ipsecuser

126 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/3 RPT=4  
AUTH\_PutAttrTable(137, 1861c60)

127 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/60 RPT=3  
AUTH\_UnbindServer(9b1544c, 0, 0)

128 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/70 RPT=3  
Auth Server 16b3fa0 has been unbound from ACB 9b1544c, sessions = 0

129 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/59 RPT=4  
AUTH\_BindServer(9b1544c, 0, 0)

130 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/69 RPT=4  
Auth Server 16b3fa0 has been bound to ACB 9b1544c, sessions = 1

131 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/65 RPT=4  
AUTH\_CreateTimer(9b1544c, 0, 0)

132 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/72 RPT=4  
Reply timer created: handle = 3B5001A

133 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/61 RPT=4  
AUTH\_BuildMsg(9b1544c, 0, 0)

134 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/64 RPT=4  
AUTH\_StartTimer(9b1544c, 0, 0)

135 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/73 RPT=4  
Reply timer started: handle = 3B5001A, timestamp = 10086167, timeout = 30000

136 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/62 RPT=4  
AUTH\_SndRequest(9b1544c, 0, 0)

137 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/50 RPT=7  
IntDB\_Decode(2ec5350, 44)

138 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/47 RPT=7  
IntDB\_Xmt(9b1544c)

139 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/71 RPT=4  
xmit\_cnt = 1

140 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/47 RPT=8  
IntDB\_Xmt(9b1544c)

141 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/49 RPT=4  
IntDB\_Match(9b1544c, 2ec3f64)

142 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/63 RPT=4  
AUTH\_RcvReply(9b1544c, 0, 0)

143 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/50 RPT=8  
IntDB\_Decode(2ec3f64, 44)

144 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/48 RPT=4  
IntDB\_Rcv(9b1544c)

145 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/66 RPT=4  
AUTH\_DeleteTimer(9b1544c, 0, 0)

146 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/74 RPT=4  
Reply timer stopped: handle = 3B5001A, timestamp = 10086177

147 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/58 RPT=4  
AUTH\_Callback(9b1544c, 0, 0)

148 02/07/2002 08:00:22.010 SEV=6 AUTH/41 RPT=3 172.18.124.241  
Authentication successful: handle = 137, server = Internal, group = ipsecgroup

149 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/3 RPT=5  
AUTH\_PutAttrTable(137, 1861c60)

150 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/60 RPT=4  
AUTH\_UnbindServer(9b1544c, 0, 0)

151 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/70 RPT=4  
Auth Server 16b3fa0 has been unbound from ACB 9b1544c, sessions = 0

152 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/59 RPT=5  
AUTH\_BindServer(9b1544c, 0, 0)

153 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/69 RPT=5  
Auth Server 16b3fa0 has been bound to ACB 9b1544c, sessions = 1

154 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/65 RPT=5  
AUTH\_CreateTimer(9b1544c, 0, 0)

155 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/72 RPT=5  
Reply timer created: handle = 3B6001A

156 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/61 RPT=5  
AUTH\_BuildMsg(9b1544c, 0, 0)

157 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/64 RPT=5  
AUTH\_StartTimer(9b1544c, 0, 0)

158 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/73 RPT=5  
Reply timer started: handle = 3B6001A, timestamp = 10086177, timeout = 30000

159 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/62 RPT=5

AUTH\_SndRequest(9b1544c, 0, 0)

160 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/50 RPT=9  
IntDB\_Decode(2ec39ec, 44)

161 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/47 RPT=9  
IntDB\_Xmt(9b1544c)

162 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/71 RPT=5  
xmit\_cnt = 1

163 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/47 RPT=10  
IntDB\_Xmt(9b1544c)

164 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/49 RPT=5  
IntDB\_Match(9b1544c, 2ec5350)

165 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/63 RPT=5  
AUTH\_RcvReply(9b1544c, 0, 0)

166 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/50 RPT=10  
IntDB\_Decode(2ec5350, 44)

167 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/48 RPT=5  
IntDB\_Rcv(9b1544c)

168 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/66 RPT=5  
AUTH\_DeleteTimer(9b1544c, 0, 0)

169 02/07/2002 08:00:22.110 SEV=9 AUTHDBG/74 RPT=5  
Reply timer stopped: handle = 3B6001A, timestamp = 10086187

170 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/58 RPT=5  
AUTH\_Callback(9b1544c, 0, 0)

171 02/07/2002 08:00:22.110 SEV=6 AUTH/41 RPT=4 172.18.124.241  
Authentication successful: handle = 137, server = Internal, group = ipsecgroup

172 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/4 RPT=3  
AUTH\_GetAttrTable(137, 729c04)

173 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/4 RPT=4  
AUTH\_GetAttrTable(137, 728c4c)

174 02/07/2002 08:00:22.110 SEV=7 IKEDBG/14 RPT=3 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Authentication configured for Internal

175 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/2 RPT=3  
AUTH\_Close(137)

176 02/07/2002 08:00:22.110 SEV=4 IKE/52 RPT=61 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
User (ipsecuser) authenticated.

177 02/07/2002 08:00:22.110 SEV=9 IKEDBG/0 RPT=95 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing blank hash

178 02/07/2002 08:00:22.110 SEV=9 IKEDBG/0 RPT=96 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing qm hash

179 02/07/2002 08:00:22.110 SEV=8 IKEDBG/0 RPT=97 172.18.124.241

SENDING Message (msgid=4cc78f4e) with payloads :  
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 60

181 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/60 RPT=5  
AUTH\_UnbindServer(9b1544c, 0, 0)

182 02/07/2002 08:00:22.110 SEV=9 AUTHDBG/70 RPT=5  
Auth Server 16b3fa0 has been unbound from ACB 9b1544c, sessions = 0

183 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/10 RPT=3  
AUTH\_Int\_FreeAuthCB(9b1544c)

184 02/07/2002 08:00:22.110 SEV=7 AUTH/13 RPT=3  
Authentication session closed: handle = 137

185 02/07/2002 08:00:22.110 SEV=8 IKEDBG/0 RPT=98 172.18.124.241  
RECEIVED Message (msgid=4cc78f4e) with payloads :  
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 56

187 02/07/2002 08:00:22.110 SEV=9 IKEDBG/1 RPT=13  
process\_attr(): Enter!

188 02/07/2002 08:00:22.110 SEV=9 IKEDBG/1 RPT=14  
Processing cfg ACK attributes

189 02/07/2002 08:00:22.180 SEV=8 IKEDBG/0 RPT=99 172.18.124.241  
RECEIVED Message (msgid=38a7c320) with payloads :  
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 154

191 02/07/2002 08:00:22.180 SEV=9 IKEDBG/1 RPT=15  
process\_attr(): Enter!

192 02/07/2002 08:00:22.180 SEV=9 IKEDBG/1 RPT=16  
Processing cfg Request attributes

193 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=1  
MODE\_CFG: Received request for IPV4 address!

194 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=2  
MODE\_CFG: Received request for IPV4 net mask!

195 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=3  
MODE\_CFG: Received request for DNS server address!

196 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=4  
MODE\_CFG: Received request for WINS server address!

197 02/07/2002 08:00:22.180 SEV=6 IKE/130 RPT=1 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Received unsupported transaction mode attribute: 5

199 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=5  
MODE\_CFG: Received request for Application Version!

200 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=6  
MODE\_CFG: Received request for Banner!

201 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=7  
MODE\_CFG: Received request for Save PW setting!

202 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=8  
MODE\_CFG: Received request for Default Domain Name!

203 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=9

MODE\_CFG: Received request for Split Tunnel List!

204 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=10  
MODE\_CFG: Received request for PFS setting!

205 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=11  
MODE\_CFG: Received request for FWTYPE!

206 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=12  
MODE\_CFG: Received request for UDP Port!

207 02/07/2002 08:00:22.180 SEV=9 IKEDBG/31 RPT=1 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Obtained IP addr (10.1.1.100) prior to initiating Mode Cfg (XAuth enabled)

209 02/07/2002 08:00:22.180 SEV=9 IKEDBG/0 RPT=100 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing blank hash

210 02/07/2002 08:00:22.180 SEV=9 IKEDBG/0 RPT=101 172.18.124.241  
0000: 00010004 0A010164 F0010000 F0070000 .....d.....  
0010: 00070062 43697363 6F205379 7374656D ...bCisco System  
0020: 732C2049 6E632E2F 56504E20 33303030 s, Inc./VPN 3000  
0030: 20436F6E 63656E74 7261746F 72205665 Concentrator Ve  
0040: 7273696F 6E20332E 352E5265 6C206275 rsion 3.5.Rel bu  
0050: 696C7420 62792076 6D757270 6879206F ilt by vmurphy o

216 02/07/2002 08:00:22.180 SEV=9 IKEDBG/0 RPT=102 172.18.124.241  
0000: 6E204E6F 76203237 20323030 31203131 n Nov 27 2001 11  
0010: 3A32323A 3331 :22:31

218 02/07/2002 08:00:22.180 SEV=9 IKEDBG/0 RPT=103 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing qm hash

219 02/07/2002 08:00:22.180 SEV=8 IKEDBG/0 RPT=104 172.18.124.241  
SENDING Message (msgid=38a7c320) with payloads :  
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 174

221 02/07/2002 08:00:22.190 SEV=9 IKEDBG/21 RPT=1 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

223 02/07/2002 08:00:22.190 SEV=4 AUTH/22 RPT=86  
User ipsecuser connected

224 02/07/2002 08:00:22.190 SEV=7 IKEDBG/22 RPT=1 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

226 02/07/2002 08:00:22.200 SEV=4 IKE/119 RPT=68 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
PHASE 1 COMPLETED

227 02/07/2002 08:00:22.200 SEV=6 IKE/121 RPT=1 172.18.124.241  
Keep-alive type for this connection: DPD

228 02/07/2002 08:00:22.200 SEV=7 IKEDBG/0 RPT=105 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Starting phase 1 rekey timer: 82080000 (ms)

229 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=106 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
sending notify message



230 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=107 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing blank hash

231 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=108 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing qm hash

232 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=109 172.18.124.241  
SENDING Message (msgid=be237358) with payloads :  
HDR + HASH (8) + NOTIFY (11) + NONE (0) ... total length : 88

234 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=110 172.18.124.241  
RECEIVED Message (msgid=472c326b) with payloads :  
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total length : 792

237 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=111 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing hash

238 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=112 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing SA payload

239 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=17 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing nonce payload

240 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=18 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Processing ID

241 02/07/2002 08:00:22.200 SEV=5 IKE/25 RPT=62 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Received remote Proxy Host data in ID Payload:  
Address 10.1.1.100, Protocol 0, Port 0

244 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=19 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Processing ID

245 02/07/2002 08:00:22.200 SEV=5 IKE/24 RPT=61 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Received local Proxy Host data in ID Payload:  
Address 172.18.124.133, Protocol 0, Port 0

248 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=113  
QM IsRekeyed old sa not found by addr

249 02/07/2002 08:00:22.200 SEV=5 IKE/66 RPT=121 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
IKE Remote Peer configured for SA: ESP-3DES-MD5

251 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=114 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing IPSEC SA

252 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=115  
Proposal # 2, Transform # 1, Type ESP, Id Triple-DES  
Parsing received transform:  
Phase 2 failure:  
Mismatched attr types for class HMAC Algorithm:

Rcv'd: SHA  
Cfg'd: MD5

256 02/07/2002 08:00:22.200 SEV=7 IKEDBG/27 RPT=1 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
IPSec SA Proposal # 3, Transform # 1 acceptable

258 02/07/2002 08:00:22.200 SEV=7 IKEDBG/0 RPT=116 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
IKE: requesting SPI!

259 02/07/2002 08:00:22.200 SEV=9 IPSECDBG/6 RPT=1  
IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000, seq 129, err  
0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKe  
yLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 708648, lifetime2 0, ds  
Id 300

263 02/07/2002 08:00:22.200 SEV=9 IPSECDBG/1 RPT=1  
Processing KEY\_GETSPI msg!

264 02/07/2002 08:00:22.200 SEV=7 IPSECDBG/13 RPT=1  
Reserved SPI 1037485220

265 02/07/2002 08:00:22.200 SEV=8 IKEDBG/6 RPT=1  
IKE got SPI from key engine: SPI = 0x3dd6c4a4

266 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=117 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
oakley constructing quick mode

267 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=118 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing blank hash

268 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=119 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing ISA\_SA for ipsec

269 02/07/2002 08:00:22.200 SEV=5 IKE/75 RPT=121 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 seconds

271 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=20 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing ipsec nonce payload

272 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=21 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing proxy ID

273 02/07/2002 08:00:22.200 SEV=7 IKEDBG/0 RPT=120 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Transmitting Proxy Id:  
Remote host: 10.1.1.100 Protocol 0 Port 0  
Local host: 172.18.124.133 Protocol 0 Port 0

277 02/07/2002 08:00:22.200 SEV=7 IKEDBG/0 RPT=121 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Sending RESPONDER LIFETIME notification to Initiator

279 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=122 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing qm hash

280 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=123 172.18.124.241  
SENDING Message (msgid=472c326b) with payloads :  
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0)  
... total length : 172

283 02/07/2002 08:00:22.210 SEV=8 IKEDBG/0 RPT=124 172.18.124.241  
RECEIVED Message (msgid=64c59a32) with payloads :  
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total length : 796

286 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=125 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing hash

287 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=126 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing SA payload

288 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=22 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing nonce payload

289 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=23 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Processing ID

290 02/07/2002 08:00:22.210 SEV=5 IKE/25 RPT=63 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Received remote Proxy Host data in ID Payload:  
Address 10.1.1.100, Protocol 0, Port 0

293 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=24 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Processing ID

294 02/07/2002 08:00:22.210 SEV=5 IKE/34 RPT=61 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Received local IP Proxy Subnet data in ID Payload:  
Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0

297 02/07/2002 08:00:22.210 SEV=8 IKEDBG/0 RPT=127  
QM IsRekeyed old sa not found by addr

298 02/07/2002 08:00:22.210 SEV=5 IKE/66 RPT=122 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
IKE Remote Peer configured for SA: ESP-3DES-MD5

300 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=128 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing IPSEC SA

301 02/07/2002 08:00:22.210 SEV=8 IKEDBG/0 RPT=129  
Proposal # 2, Transform # 1, Type ESP, Id Triple-DES  
Parsing received transform:  
Phase 2 failure:  
Mismatched attr types for class HMAC Algorithm:  
Rcv'd: SHA  
Cfg'd: MD5

305 02/07/2002 08:00:22.210 SEV=7 IKEDBG/27 RPT=2 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
IPSec SA Proposal # 3, Transform # 1 acceptable

307 02/07/2002 08:00:22.210 SEV=7 IKEDBG/0 RPT=130 172.18.124.241

Group [ipsecgroup] User [ipsecuser]  
IKE: requesting SPI!

308 02/07/2002 08:00:22.210 SEV=9 IPSECDBG/6 RPT=2  
IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000, seq 130, err  
0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKe  
yLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 708648, lifetime2 0, ds  
Id 300

312 02/07/2002 08:00:22.210 SEV=9 IPSECDBG/1 RPT=2  
Processing KEY\_GETSPI msg!

313 02/07/2002 08:00:22.210 SEV=7 IPSECDBG/13 RPT=2  
Reserved SPI 1517437317

314 02/07/2002 08:00:22.210 SEV=8 IKEDBG/6 RPT=2  
IKE got SPI from key engine: SPI = 0x5a724185

315 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=131 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
oakley constructing quick mode

316 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=132 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing blank hash

317 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=133 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing ISA\_SA for ipsec

318 02/07/2002 08:00:22.210 SEV=5 IKE/75 RPT=122 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 seconds

320 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=25 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing ipsec nonce payload

321 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=26 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing proxy ID

322 02/07/2002 08:00:22.210 SEV=7 IKEDBG/0 RPT=134 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Transmitting Proxy Id:  
Remote host: 10.1.1.100 Protocol 0 Port 0  
Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0

326 02/07/2002 08:00:22.210 SEV=7 IKEDBG/0 RPT=135 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Sending RESPONDER LIFETIME notification to Initiator

328 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=136 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing qm hash

329 02/07/2002 08:00:22.220 SEV=8 IKEDBG/0 RPT=137 172.18.124.241  
SENDING Message (msgid=64c59a32) with payloads :  
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0)  
... total length : 176

332 02/07/2002 08:00:22.220 SEV=8 IKEDBG/0 RPT=138 172.18.124.241  
RECEIVED Message (msgid=472c326b) with payloads :  
HDR + HASH (8) + NONE (0) ... total length : 48

334 02/07/2002 08:00:22.220 SEV=9 IKEDBG/0 RPT=139 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing hash

335 02/07/2002 08:00:22.220 SEV=9 IKEDBG/0 RPT=140 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
loading all IPSEC SAs

336 02/07/2002 08:00:22.220 SEV=9 IKEDBG/1 RPT=27 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Generating Quick Mode Key!

337 02/07/2002 08:00:22.220 SEV=9 IKEDBG/1 RPT=28 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Generating Quick Mode Key!

338 02/07/2002 08:00:22.220 SEV=7 IKEDBG/0 RPT=141 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Loading host:  
Dst: 172.18.124.133  
Src: 10.1.1.100

340 02/07/2002 08:00:22.220 SEV=4 IKE/49 RPT=129 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Security negotiation complete for User (ipsecuser)  
Responder, Inbound SPI = 0x3dd6c4a4, Outbound SPI = 0x8104887e

343 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/6 RPT=3  
IPSEC key message parse - msgtype 1, len 624, vers 1, pid 00000000, seq 0, err 0  
, type 2, mode 1, state 64, label 0, pad 0, spi 8104887e, encrKeyLen 24, hashKey  
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, ds  
Id 0

347 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=3  
Processing KEY\_ADD msg!

348 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=4  
key\_msghdr2secassoc(): Enter

349 02/07/2002 08:00:22.220 SEV=7 IPSECDBG/1 RPT=5  
No USER filter configured

350 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=6  
KeyProcessAdd: Enter

351 02/07/2002 08:00:22.220 SEV=8 IPSECDBG/1 RPT=7  
KeyProcessAdd: Adding outbound SA

352 02/07/2002 08:00:22.220 SEV=8 IPSECDBG/1 RPT=8  
KeyProcessAdd: src 172.18.124.133 mask 0.0.0.0, dst 10.1.1.100 mask 0.0.0.0

353 02/07/2002 08:00:22.220 SEV=8 IPSECDBG/1 RPT=9  
KeyProcessAdd: FilterIpsecAddIkeSa success

354 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/6 RPT=4  
IPSEC key message parse - msgtype 3, len 336, vers 1, pid 00000000, seq 0, err 0  
, type 2, mode 1, state 32, label 0, pad 0, spi 3dd6c4a4, encrKeyLen 24, hashKey  
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, ds  
Id 0

358 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=10  
Processing KEY\_UPDATE msg!

359 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=11  
Update inbound SA addresses

360 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=12  
key\_msghdr2secassoc(): Enter

361 02/07/2002 08:00:22.220 SEV=7 IPSECDBG/1 RPT=13  
No USER filter configured

362 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=14  
KeyProcessUpdate: Enter

363 02/07/2002 08:00:22.220 SEV=8 IPSECDBG/1 RPT=15  
KeyProcessUpdate: success

364 02/07/2002 08:00:22.220 SEV=8 IKEDBG/7 RPT=1  
IKE got a KEY\_ADD msg for SA: SPI = 0x8104887e

365 02/07/2002 08:00:22.220 SEV=8 IKEDBG/0 RPT=142  
pitcher: rcv KEY\_UPDATE, spi 0x3dd6c4a4

366 02/07/2002 08:00:22.220 SEV=4 IKE/120 RPT=129 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
PHASE 2 COMPLETED (msgid=472c326b)

367 02/07/2002 08:00:22.280 SEV=8 IKEDBG/0 RPT=143 172.18.124.241  
RECEIVED Message (msgid=64c59a32) with payloads :  
HDR + HASH (8) + NONE (0) ... total length : 48

369 02/07/2002 08:00:22.280 SEV=9 IKEDBG/0 RPT=144 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing hash

370 02/07/2002 08:00:22.280 SEV=9 IKEDBG/0 RPT=145 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
loading all IPSEC SAs

371 02/07/2002 08:00:22.280 SEV=9 IKEDBG/1 RPT=29 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Generating Quick Mode Key!

372 02/07/2002 08:00:22.280 SEV=9 IKEDBG/1 RPT=30 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Generating Quick Mode Key!

373 02/07/2002 08:00:22.280 SEV=7 IKEDBG/0 RPT=146 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Loading subnet:  
 Dst: 0.0.0.0 mask: 0.0.0.0  
 Src: 10.1.1.100

375 02/07/2002 08:00:22.280 SEV=4 IKE/49 RPT=130 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Security negotiation complete for User (ipsecuser)  
Responder, Inbound SPI = 0x5a724185, Outbound SPI = 0x285e6ed0

378 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/6 RPT=5  
IPSEC key message parse - msgtype 1, len 624, vers 1, pid 00000000, seq 0, err 0  
, type 2, mode 1, state 64, label 0, pad 0, spi 285e6ed0, encrKeyLen 24, hashKey  
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, ds  
Id 0

382 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=16  
Processing KEY\_ADD msg!

383 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=17  
key\_msghdr2secassoc(): Enter

384 02/07/2002 08:00:22.280 SEV=7 IPSECDBG/1 RPT=18  
No USER filter configured

385 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=19  
KeyProcessAdd: Enter

386 02/07/2002 08:00:22.280 SEV=8 IPSECDBG/1 RPT=20  
KeyProcessAdd: Adding outbound SA

387 02/07/2002 08:00:22.280 SEV=8 IPSECDBG/1 RPT=21  
KeyProcessAdd: src 0.0.0.0 mask 255.255.255.255, dst 10.1.1.100 mask 0.0.0.0

388 02/07/2002 08:00:22.280 SEV=8 IPSECDBG/1 RPT=22  
KeyProcessAdd: FilterIpssecAddIkeSa success

389 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/6 RPT=6  
IPSEC key message parse - msgtype 3, len 336, vers 1, pid 00000000, seq 0, err 0  
, type 2, mode 1, state 32, label 0, pad 0, spi 5a724185, encrKeyLen 24, hashKey  
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, ds  
Id 0

393 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=23  
Processing KEY\_UPDATE msg!

394 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=24  
Update inbound SA addresses

395 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=25  
key\_msghdr2secassoc(): Enter

396 02/07/2002 08:00:22.280 SEV=7 IPSECDBG/1 RPT=26  
No USER filter configured

397 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=27  
KeyProcessUpdate: Enter

398 02/07/2002 08:00:22.280 SEV=8 IPSECDBG/1 RPT=28  
KeyProcessUpdate: success

399 02/07/2002 08:00:22.280 SEV=8 IKEDBG/7 RPT=2  
IKE got a KEY\_ADD msg for SA: SPI = 0x285e6ed0

400 02/07/2002 08:00:22.280 SEV=8 IKEDBG/0 RPT=147  
pitcher: rcv KEY\_UPDATE, spi 0x5a724185

401 02/07/2002 08:00:22.280 SEV=4 IKE/120 RPT=130 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
PHASE 2 COMPLETED (msgid=64c59a32)

## [相关信息](#)

- [Cisco VPN 3000 系列集中器支持页](#)
- [Cisco VPN 3000 系列客户端支持页](#)
- [IPsec 协商/IKE 协议](#)
- [技术支持和文档 - Cisco Systems](#)