

# Configuring L2TP over IPSec from a Windows 2000 or XP Client to a Cisco VPN 3000 Series Concentrator Using Pre-Shared Keys

Document ID: 19260

---

## Introduction

### Before You Begin

- Conventions

- Prerequisites

- Components Used

- Network Diagram

### Configurations for the VPN Client and the VPN 3000 Concentrator

- VPN Client

- VPN 3000 Concentrator

- User Configuration on the VPN 3000 Concentrator

### Testing the Tunnel

### Verifying the Tunnel

### Debugs of Successful Connections from Both Clients

### Related Information

---

## Introduction

This document describes how to configure Layer 2 Tunneling Protocol (L2TP) over IP Security (IPSec) from remote Microsoft Windows 2000 and XP clients to a corporate site using an encrypted method.

In order to configure L2TP over IPSec between the PIX 6.x and Windows 2000, refer to [Configuring L2TP Over IPSec Between PIX Firewall and Windows 2000 PC Using Certificates](#).

In order to configure Layer 2 Tunneling Protocol (L2TP) over IPsec from remote Microsoft Windows 2000/2003 and XP clients to a PIX/ASA Security Appliance corporate office with pre-shared keys with Microsoft Windows 2003 Internet Authentication Service (IAS) RADIUS Server for user authentication, refer to [L2TP Over IPsec Between Windows 2000/XP PC and PIX/ASA 7.2 Using Pre-shared Key Configuration Example](#).

## Before You Begin

### Conventions

For more information on document conventions, see the [Cisco Technical Tips Conventions](#).

### Prerequisites

There are no specific prerequisites for this document.

### Components Used

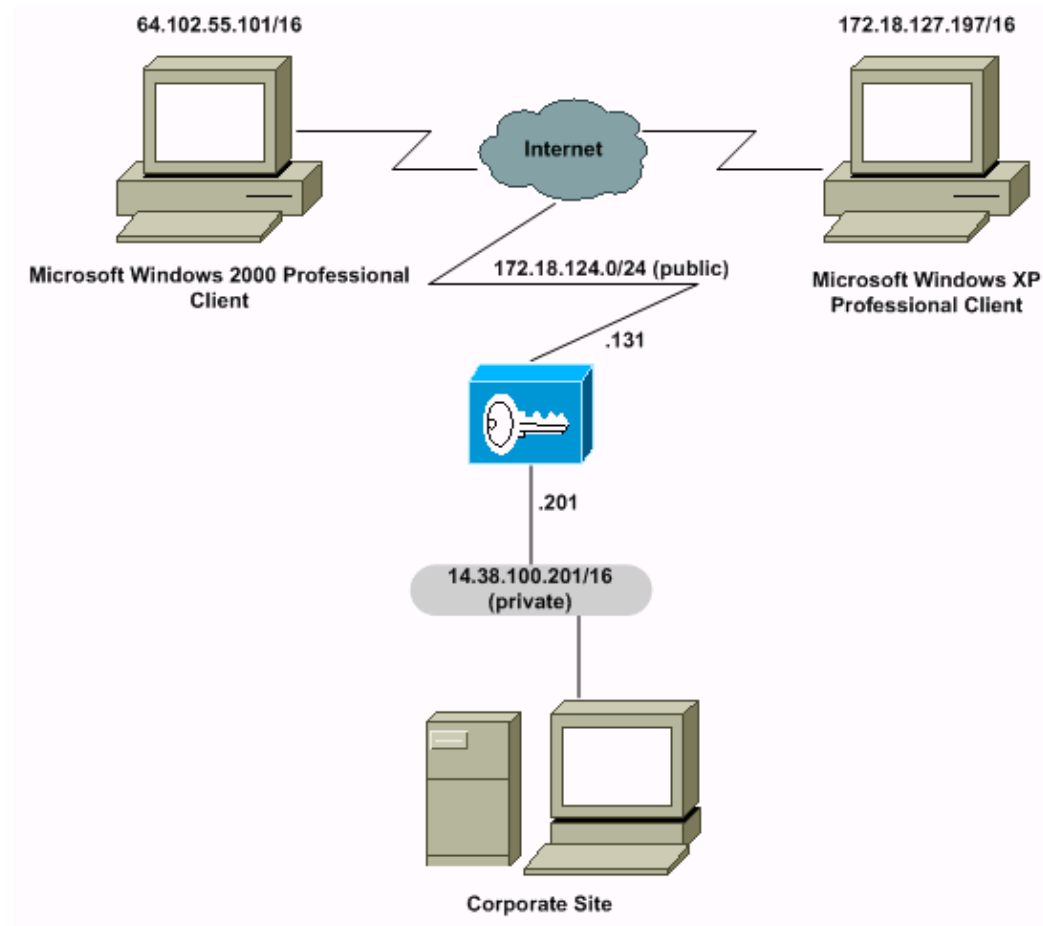
The information in this document is based on the software and hardware versions below.

- Microsoft Windows 2000 Professional
- Microsoft Windows XP Professional
- Cisco VPN 3000 Series Concentrator
- Cisco VPN Client for Windows v3.5

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

## Network Diagram

This document uses the network setup shown in the diagram below.



## IP Addresses

3000 Series Concentrator:

- Public Interface: 172.18.124.131
- Private Interface: 14.38.100.201

WIN XP Professional:

- Public IP Address: 172.18.127.197

WIN 2000 Professional:

- Public Interface: 64.102.55.101

# Configurations for the VPN Client and the VPN 3000 Concentrator

## VPN Client

In this section, you are presented with the information to configure the features described in this document.

### Configuring L2TP over the IPSec Feature on Windows 2000 and XP

Follow these instructions to configure L2TP over the IPSec feature on Windows 2000 and XP:

1. Add the following registry value to your Windows 2000 or XP machines:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
```

2. Add the following registry value to this key:

```
Value Name: ProhibitIpSec  
Data Type: REG_DWORD  
Value: 1
```

**Note:** You must restart Windows 2000 or XP for the changes to take effect.

In [How to Configure a L2TP/IPSec Connection Using Pre-shared Key Authentication \(Q240262\)](#) you will find the following statement:

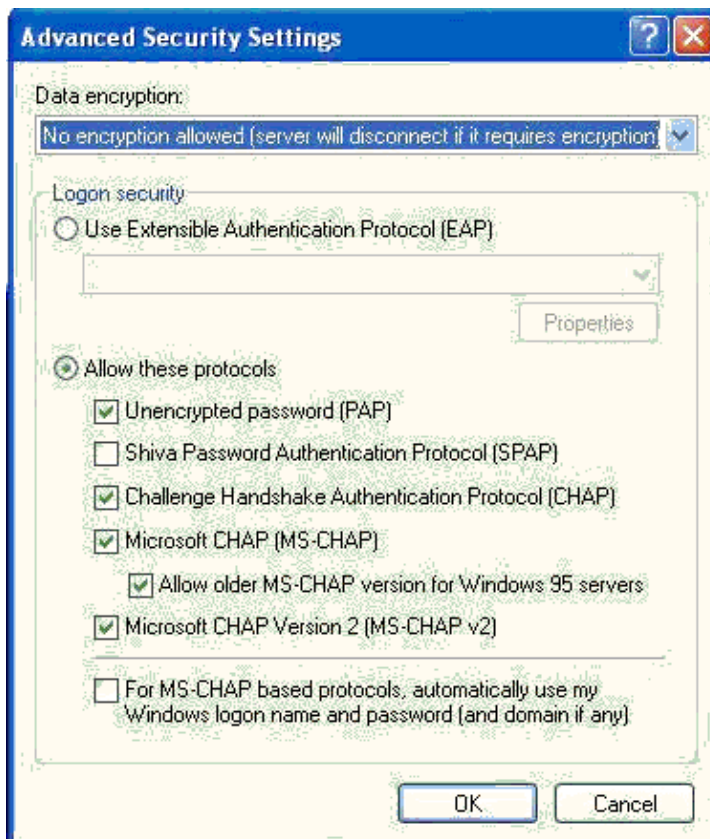
"Microsoft does support VPN L2TP/IPSec tunnels gateway-to-gateway with a preshared key because it must be configured locally on that gateway by a very knowledgeable gateway administrator on a per-static IP basis. IPSec tunnels are only supported where static IP addresses are used, and for address-based policy selectors only, not port and protocol. Microsoft recommends using L2TP/IPSec for gateway-to-gateway. Use IPSec tunnel mode for gateway-to-gateway only if L2TP/IPSec is not an option."

Please follow the Microsoft document linked below to configure your Windows 2000 and XP client for an IPSec policy. If any problems arise from the configuration of the client, please contact Microsoft for support.

[HOW TO: Configure a Preshared Key for Use with Layer 2 Tunneling Protocol Connections in Windows XP \(Q281555\)](#)

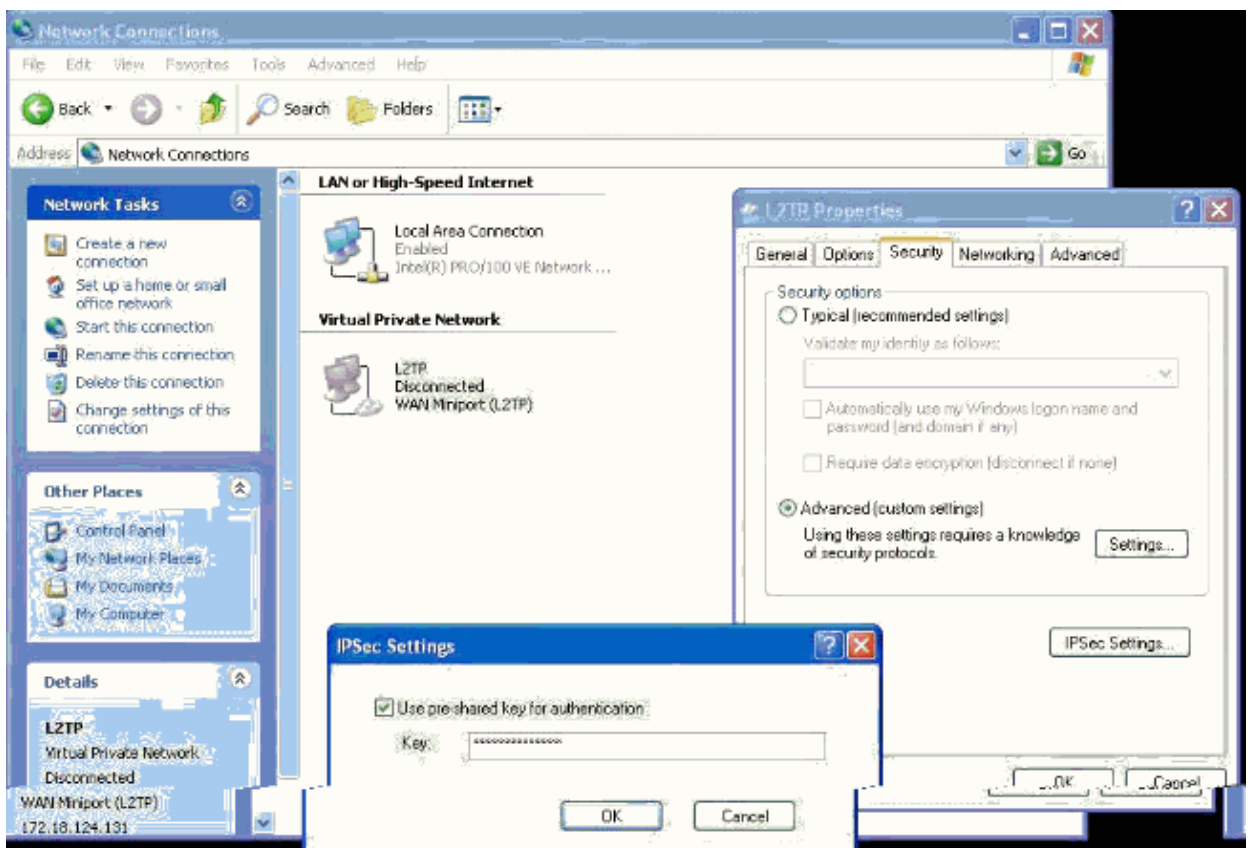
3. After creating your L2TP IPSec policy, create your connection.

Then, under **Network and Dial-up Connections**, right click on that connection and select **Properties**. On the **Security** tab, click on **Advanced**. Select the protocols as in the image below.



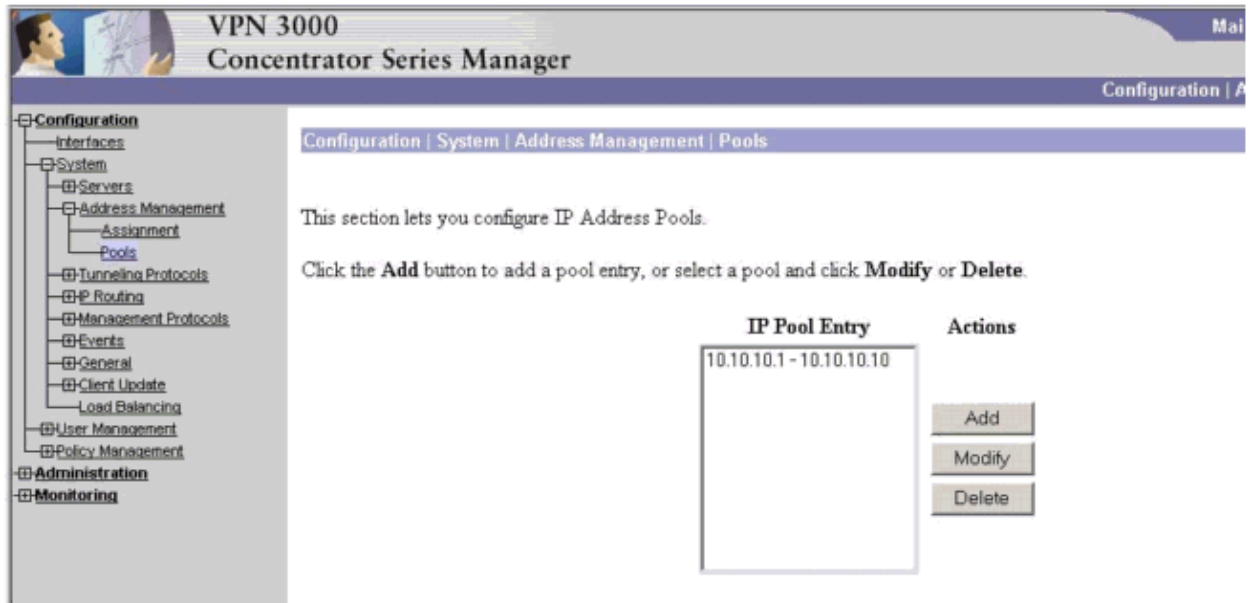
4. To set the pre-shared key, click on **IPSec Settings** and check **Use pre-shared key for authentication** and type in the pre-shared key.

In this example, "cisco123" is used.



# VPN 3000 Concentrator

On the VPN 3000 Concentrator you will need to configure an address pool for the remote users by going to **Configuration > System > Address Management > Pools**.



Next, make sure your base group has the default pre-shared key specified by going to **Configuration > User Management > Base Group**. In this example the pre-shared key is "cisco123."

Configuration | User Management | Base Group

General | IPsec | Mode Config | Client FW | HW Client | PPTP/L2TP

General Parameters		
Attribute	Value	Description
Access Hours	No Restrictions	Select the access hours for this group.
Simultaneous Logins	3	Enter the number of simultaneous logins for users in this group.
Minimum Password Length	8	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	(minutes) Enter the idle timeout for this group.
Maximum Connect time	0	(minutes) Enter the maximum connect time for this group.
Filter	-None-	Select the filter assigned to this group.
Primary DNS		Enter the IP address of the primary DNS server for this group.
Secondary DNS		Enter the IP address of the secondary DNS server.
Primary WINS		Enter the IP address of the primary WINS server for this group.
Secondary WINS		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	Select the SEP cards this group can be on.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input type="checkbox"/> IPsec <input checked="" type="checkbox"/> L2TP over IPsec	Select the tunneling protocols this group can connect with.
Strip Realm	<input type="checkbox"/>	Check to remove the realm qualifier of the user name during authentication.

IPsec Parameters		
Attribute	Value	Description
IPsec SA	ESP-3DES-MD5	Select the IPsec Security Association assigned to this group.
IKE Peer Identity Validation	If supported by certificate	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives for members of this group.
Reauthentication on Rekey	<input type="checkbox"/>	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Tunnel Type	Remote Access	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters		
Group Lock	<input type="checkbox"/>	Lock the users into this group.
Authentication	Internal	Select the authentication method for members of this group. This parameter does not apply to <b>Individual User Authentication</b> .
IPComp	None	Select the method of IP Compression for members of this group.
Default Preshared Key	cisco123	Enter the preshared key to be used with clients that do not support groups.
Mode Configuration	<input checked="" type="checkbox"/>	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the the Aliga/Cisco client are being used by members of this group.

PPTP/L2TP Parameters		
Attribute	Value	Description
Use Client Address	<input type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. <b>Unchecking all options means that no authentication is required.</b>
PPTP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	<input type="checkbox"/>	Check to enable MPPC compression for PPTP connections for this group.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. <b>Unchecking all options means that no authentication is required.</b>
L2TP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input type="checkbox"/> 40-bit <input type="checkbox"/> 128-bit	Select the allowed encryption methods for L2TP connections for this group.
L2TP Compression	<input type="checkbox"/>	Check to enable MPPC compression for L2TP connections for this group.

## User Configuration on the VPN 3000 Concentrator

In the examples below, L2TP\_user and L2TP2k\_users were defined. Both users have passwords "cisco123." The L2TP\_user is the XP Professional client, and L2TP2k\_user is the 2000 Professional client. Please follow the pictures exactly when configuring all users. The images list the XP user; however, the debugs will show both users connecting.

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

Identity Parameters		
Attribute	Value	Description
User Name	L2TP_user	Enter a unique user name.
Password	●●●●●●●●	Enter the user's password. The password must satisfy the group password requirements.
Verify	●●●●●●●●	Verify the user's password.
Group	-Base Group-	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.

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

General Parameters			
Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this user.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this user.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this user.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this user.
Filter	-None-	<input checked="" type="checkbox"/>	Enter the filter assigned to this user.
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 user can be assigned to.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input type="checkbox"/> IPSec <input checked="" type="checkbox"/> L2TP over IPSec	<input checked="" type="checkbox"/>	Select the tunneling protocols this user can connect with.

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

PPTP/L2TP Parameters			
Attribute	Value	Inherit?	Description
Use Client Address	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	<input checked="" type="checkbox"/>	Enter the authentication protocols this user is allowed to use. This is used to <i>remove</i> protocols from the list of acceptable authentication protocols. <b>Unchecking all options means that no authentication is required.</b>
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	<input checked="" type="checkbox"/>	Enter the authentication protocols this user is allowed to use. This is used to <i>remove</i> protocols from the list of acceptable authentication protocols. <b>Unchecking all options means that no authentication is required.</b>

## Testing the Tunnel

After connecting, ping the private interface's IP address for each client. Below is the expected response.

```

C:\ F:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

F:\Documents and Settings\Admin>ping 14.38.100.201

Pinging 14.38.100.201 with 32 bytes of data:

Reply from 14.38.100.201: bytes=32 time=1ms TTL=128
Reply from 14.38.100.201: bytes=32 time=1ms TTL=128
Reply from 14.38.100.201: bytes=32 time=1ms TTL=128
Reply from 14.38.100.201: bytes=32 time=2ms TTL=128

Ping statistics for 14.38.100.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

F:\Documents and Settings\Admin>

```

## Verifying the Tunnel

In order to view the session statistics from the VPN Concentrator GUI, go to Monitoring > Sessions and review the statistics of the "Remote Access Sessions."

Monitoring | Sessions Tuesday, 05 February 2002 13:17:27  
Reset Refresh

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name.

Group:

### Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Concurrent Sessions Limit	Total Cumulative Sessions
0	2	2	4	5	5000	1169

### LAN-to-LAN Sessions

[\[ Remote Access Sessions | Management Sessions \]](#)

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
No LAN-to-LAN Sessions							

### Remote Access Sessions

[\[ LAN-to-LAN Sessions | Management Sessions \]](#)

Username	Group	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
L2TP2k_user	Base Group	64.102.55.101	10.10.10.1	L2TP/IPSec	DES-56	Feb 05 13:07:54	0:09:32	1120	90032
L2TP_user	Base Group	172.18.124.197	10.10.10.2	L2TP/IPSec	DES-56	Feb 05 13:17:18	0:00:09	784	4664

## Debugs of Successful Connections from Both Clients

```

1 02/05/2002 13:20:23.460 SEV=4 L2TP/47 RPT=30 64.102.55.101
Session closed on tunnel 64.102.55.101 (peer 1, local 7074, serial 0), reason: L
2TP peer terminated connection

3 02/05/2002 13:20:23.460 SEV=9 IKEDBG/0 RPT=33085
sending delete message

4 02/05/2002 13:20:23.470 SEV=9 IKEDBG/0 RPT=33086 64.102.55.101
Group [VPNC_Base_Group]
constructing blank hash

```

5 02/05/2002 13:20:23.470 SEV=9 IKEDBG/0 RPT=33087  
constructing ipsec delete payload

6 02/05/2002 13:20:23.470 SEV=9 IKEDBG/0 RPT=33088 64.102.55.101  
Group [VPNC\_Base\_Group]  
constructing qm hash

7 02/05/2002 13:20:23.470 SEV=8 IKEDBG/0 RPT=33089 64.102.55.101  
SENDING Message (msgid=4371eb76) with payloads :  
HDR + HASH (8) + DELETE (12) + NONE (0) ... total length : 64

9 02/05/2002 13:20:23.470 SEV=7 IKEDBG/9 RPT=10 64.102.55.101  
Group [VPNC\_Base\_Group]  
IKE Deleting SA: Remote Proxy 64.102.55.101, Local Proxy 172.18.124.131

11 02/05/2002 13:20:23.470 SEV=9 IKEDBG/0 RPT=33090 64.102.55.101  
Group [VPNC\_Base\_Group]  
IKE SA MM:ba857ac8 rcv'd Terminate: state MM\_ACTIVE  
flags 0x00000042, refcnt 1, tuncnt 0

14 02/05/2002 13:20:23.470 SEV=9 IKEDBG/0 RPT=33091 64.102.55.101  
Group [VPNC\_Base\_Group]  
IKE SA MM:ba857ac8 terminating:  
flags 0x01000002, refcnt 0, tuncnt 0

16 02/05/2002 13:20:23.470 SEV=9 IKEDBG/0 RPT=33092  
sending delete message

17 02/05/2002 13:20:23.470 SEV=9 IKEDBG/0 RPT=33093 64.102.55.101  
Group [VPNC\_Base\_Group]  
constructing blank hash

18 02/05/2002 13:20:23.470 SEV=9 IKEDBG/0 RPT=33094  
constructing delete payload

19 02/05/2002 13:20:23.470 SEV=9 IKEDBG/0 RPT=33095 64.102.55.101  
Group [VPNC\_Base\_Group]  
constructing qm hash

20 02/05/2002 13:20:23.470 SEV=8 IKEDBG/0 RPT=33096 64.102.55.101  
SENDING Message (msgid=89b41alf) with payloads :  
HDR + HASH (8) + DELETE (12) + NONE (0) ... total length : 76

22 02/05/2002 13:20:23.470 SEV=9 IPSECDBG/6 RPT=52  
IPSEC key message parse - msgtype 2, len 266, vers 1, pid 00000000, seq 0, err 0  
, type 2, mode 0, state 32, label 0, pad 0, spi 0befc8ee, encrKeyLen 0, hashKeyL  
en 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 708648, lifetime2 0, dsId  
0

26 02/05/2002 13:20:23.470 SEV=9 IPSECDBG/1 RPT=202  
Processing KEY\_DELETE msg!

27 02/05/2002 13:20:23.470 SEV=4 AUTH/28 RPT=12 64.102.55.101  
User [L2TP2k\_user] disconnected:  
Duration: 0:12:28  
Bytes xmt: 1312  
Bytes rcv: 118624  
Reason: User Requested

29 02/05/2002 13:20:23.470 SEV=9 IPSECDBG/6 RPT=53  
IPSEC key message parse - msgtype 2, len 266, vers 1, pid 00000000, seq 0, err 0  
, type 2, mode 0, state 64, label 0, pad 0, spi 7alc77ec, encrKeyLen 0, hashKeyL  
en 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 708648, lifetime2 0, dsId  
0

33 02/05/2002 13:20:23.470 SEV=9 IPSECDBG/1 RPT=203

Processing KEY\_DELETE msg!

34 02/05/2002 13:20:23.470 SEV=9 IPSECDBG/1 RPT=204  
key\_msghdr2secassoc(): Enter

35 02/05/2002 13:20:23.470 SEV=7 IPSECDBG/1 RPT=205  
No USER filter configured

36 02/05/2002 13:20:23.470 SEV=8 IKEDBG/0 RPT=33097  
pitcher: received key delete msg, spi 0xbefc8ee

37 02/05/2002 13:20:23.470 SEV=8 IKEDBG/0 RPT=33098  
pitcher: received key delete msg, spi 0x7alc77ec

38 02/05/2002 13:20:23.470 SEV=4 L2TP/46 RPT=30 64.102.55.101  
Tunnel to peer 64.102.55.101 closed, reason: L2TP peer terminated connection

39 02/05/2002 13:20:24.590 SEV=6 IKE/38 RPT=6 64.102.55.101  
Header invalid, missing SA payload! (next payload = 8)

40 02/05/2002 13:20:29.650 SEV=8 IKEDBG/0 RPT=33099 64.102.55.101  
RECEIVED Message (msgid=0) with payloads :  
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 216

42 02/05/2002 13:20:29.650 SEV=9 IKEDBG/0 RPT=33100 64.102.55.101  
processing SA payload

43 02/05/2002 13:20:29.650 SEV=8 IKEDBG/0 RPT=33101 64.102.55.101  
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

48 02/05/2002 13:20:29.650 SEV=8 IKEDBG/0 RPT=33102 64.102.55.101  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

51 02/05/2002 13:20:29.650 SEV=8 IKEDBG/0 RPT=33103 64.102.55.101  
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

54 02/05/2002 13:20:29.650 SEV=8 IKEDBG/0 RPT=33104 64.102.55.101  
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

57 02/05/2002 13:20:29.650 SEV=8 IKEDBG/0 RPT=33105 64.102.55.101  
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

60 02/05/2002 13:20:29.650 SEV=8 IKEDBG/0 RPT=33106 64.102.55.101  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

63 02/05/2002 13:20:29.650 SEV=8 IKEDBG/0 RPT=33107 64.102.55.101

Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

66 02/05/2002 13:20:29.650 SEV=8 IKEDBG/0 RPT=33108 64.102.55.101  
Proposal # 1, Transform # 2, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

71 02/05/2002 13:20:29.650 SEV=8 IKEDBG/0 RPT=33109 64.102.55.101  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

74 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33110 64.102.55.101  
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

77 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33111 64.102.55.101  
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

80 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33112 64.102.55.101  
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

83 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33113 64.102.55.101  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

86 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33114 64.102.55.101  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

89 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33115 64.102.55.101  
Proposal # 1, Transform # 3, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

94 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33116 64.102.55.101  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 2

97 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33117 64.102.55.101  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class Encryption Alg:

Rcv'd: DES-CBC  
Cfg'd: Triple-DES

100 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33118 64.102.55.101  
Phase 1 failure against global IKE proposal # 4:  
Mismatched attr types for class Hash Alg:  
Rcv'd: SHA  
Cfg'd: MD5

102 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33119 64.102.55.101  
Phase 1 failure against global IKE proposal # 5:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 7

105 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33120 64.102.55.101  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 2

108 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33121 64.102.55.101  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 2

111 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33122 64.102.55.101  
Proposal # 1, Transform # 4, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

116 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33123 64.102.55.101  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 2

119 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33124 64.102.55.101  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

122 02/05/2002 13:20:29.660 SEV=7 IKEDBG/0 RPT=33125 64.102.55.101  
Oakley proposal is acceptable

123 02/05/2002 13:20:29.660 SEV=9 IKEDBG/47 RPT=1194 64.102.55.101  
processing VID payload

124 02/05/2002 13:20:29.660 SEV=9 IKEDBG/0 RPT=33126 64.102.55.101  
processing IKE SA

125 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33127 64.102.55.101  
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

130 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33128 64.102.55.101  
Phase 1 failure against global IKE proposal # 2:

Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

133 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33129 64.102.55.101  
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

136 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33130 64.102.55.101  
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

139 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33131 64.102.55.101  
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

142 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33132 64.102.55.101  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

145 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33133 64.102.55.101  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

148 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33134 64.102.55.101  
Proposal # 1, Transform # 2, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

153 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33135 64.102.55.101  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

156 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33136 64.102.55.101  
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

159 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33137 64.102.55.101  
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

162 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33138 64.102.55.101  
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

165 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33139 64.102.55.101  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

168 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33140 64.102.55.101  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

171 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33141 64.102.55.101  
Proposal # 1, Transform # 3, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

176 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33142 64.102.55.101  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 2

179 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33143 64.102.55.101  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

182 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33144 64.102.55.101  
Phase 1 failure against global IKE proposal # 4:  
Mismatched attr types for class Hash Alg:  
Rcv'd: SHA  
Cfg'd: MD5

184 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33145 64.102.55.101  
Phase 1 failure against global IKE proposal # 5:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 7

187 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33146 64.102.55.101  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 2

190 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33147 64.102.55.101  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 2

193 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33148 64.102.55.101  
Proposal # 1, Transform # 4, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

198 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33149 64.102.55.101  
Phase 1 failure against global IKE proposal # 2:

Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 2

201 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33150 64.102.55.101  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

204 02/05/2002 13:20:29.660 SEV=7 IKEDBG/28 RPT=1146 64.102.55.101  
IKE SA Proposal # 1, Transform # 4 acceptable  
Matches global IKE entry # 4

205 02/05/2002 13:20:29.660 SEV=9 IKEDBG/0 RPT=33151 64.102.55.101  
constructing ISA\_SA for isakmp

206 02/05/2002 13:20:29.660 SEV=8 IKEDBG/0 RPT=33152 64.102.55.101  
SENDING Message (msgid=0) with payloads :  
HDR + SA (1) + NONE (0) ... total length : 80

208 02/05/2002 13:20:29.710 SEV=8 IKEDBG/0 RPT=33153 64.102.55.101  
RECEIVED Message (msgid=0) with payloads :  
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

210 02/05/2002 13:20:29.710 SEV=8 IKEDBG/0 RPT=33154 64.102.55.101  
RECEIVED Message (msgid=0) with payloads :  
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

212 02/05/2002 13:20:29.710 SEV=9 IKEDBG/0 RPT=33155 64.102.55.101  
processing ke payload

213 02/05/2002 13:20:29.710 SEV=9 IKEDBG/0 RPT=33156 64.102.55.101  
processing ISA\_KE

214 02/05/2002 13:20:29.710 SEV=9 IKEDBG/1 RPT=8089 64.102.55.101  
processing nonce payload

215 02/05/2002 13:20:29.730 SEV=9 IKEDBG/0 RPT=33157 64.102.55.101  
constructing ke payload

216 02/05/2002 13:20:29.730 SEV=9 IKEDBG/1 RPT=8090 64.102.55.101  
constructing nonce payload

217 02/05/2002 13:20:29.730 SEV=9 IKEDBG/46 RPT=4580 64.102.55.101  
constructing Cisco Unity VID payload

218 02/05/2002 13:20:29.730 SEV=9 IKEDBG/46 RPT=4581 64.102.55.101  
constructing xauth V6 VID payload

219 02/05/2002 13:20:29.730 SEV=9 IKEDBG/48 RPT=2291 64.102.55.101  
Send IOS VID

220 02/05/2002 13:20:29.730 SEV=9 IKEDBG/38 RPT=1146 64.102.55.101  
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)

222 02/05/2002 13:20:29.730 SEV=9 IKEDBG/46 RPT=4582 64.102.55.101  
constructing VID payload

223 02/05/2002 13:20:29.730 SEV=9 IKEDBG/48 RPT=2292 64.102.55.101  
Send Altiga GW VID

224 02/05/2002 13:20:29.730 SEV=9 IKEDBG/0 RPT=33158 64.102.55.101  
Generating keys for Responder...

225 02/05/2002 13:20:29.730 SEV=6 IKE/139 RPT=1146 64.102.55.101  
Group 64.102.55.101 not found, using BASE GROUP default preshared key

226 02/05/2002 13:20:29.730 SEV=8 IKEDBG/0 RPT=33159 64.102.55.101  
SENDING Message (msgid=0) with payloads :  
HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13)  
+ NONE (0) ... total length : 224

229 02/05/2002 13:20:29.750 SEV=8 IKEDBG/0 RPT=33160 64.102.55.101  
RECEIVED Message (msgid=0) with payloads :  
HDR + ID (5) + HASH (8) + NONE (0) ... total length : 60

231 02/05/2002 13:20:29.750 SEV=9 IKEDBG/1 RPT=8091 64.102.55.101  
Group [VPNC\_Base\_Group]  
Processing ID

232 02/05/2002 13:20:29.750 SEV=9 IKEDBG/0 RPT=33161 64.102.55.101  
Group [VPNC\_Base\_Group]  
processing hash

233 02/05/2002 13:20:29.750 SEV=9 IKEDBG/0 RPT=33162 64.102.55.101  
Group [VPNC\_Base\_Group]  
computing hash

234 02/05/2002 13:20:29.750 SEV=9 IKEDBG/23 RPT=1162 64.102.55.101  
Group [VPNC\_Base\_Group]  
Starting group lookup for peer 64.102.55.101

235 02/05/2002 13:20:29.750 SEV=8 AUTHDBG/1 RPT=1194  
AUTH\_Open() returns 169

236 02/05/2002 13:20:29.750 SEV=7 AUTH/12 RPT=1194  
Authentication session opened: handle = 169

237 02/05/2002 13:20:29.750 SEV=8 AUTHDBG/3 RPT=1226  
AUTH\_PutAttrTable(169, 728a84)

238 02/05/2002 13:20:29.750 SEV=8 AUTHDBG/6 RPT=1162  
AUTH\_GroupAuthenticate(169, 5009f44, 482fb0)

239 02/05/2002 13:20:29.750 SEV=8 AUTHDBG/59 RPT=1226  
AUTH\_BindServer(9b1c418, 0, 0)

240 02/05/2002 13:20:29.750 SEV=9 AUTHDBG/69 RPT=1226  
Auth Server 16b7fa0 has been bound to ACB 9b1c418, sessions = 1

241 02/05/2002 13:20:29.750 SEV=8 AUTHDBG/65 RPT=1194  
AUTH\_CreateTimer(9b1c418, 0, 0)

242 02/05/2002 13:20:29.750 SEV=9 AUTHDBG/72 RPT=1194  
Reply timer created: handle = 15160016

243 02/05/2002 13:20:29.750 SEV=8 AUTHDBG/61 RPT=1194  
AUTH\_BuildMsg(9b1c418, 0, 0)

244 02/05/2002 13:20:29.750 SEV=8 AUTHDBG/64 RPT=1194  
AUTH\_StartTimer(9b1c418, 0, 0)

245 02/05/2002 13:20:29.750 SEV=9 AUTHDBG/73 RPT=1194  
Reply timer started: handle = 15160016, timestamp = 34949331, timeout = 30000

246 02/05/2002 13:20:29.750 SEV=8 AUTHDBG/62 RPT=1194  
AUTH\_SndRequest(9b1c418, 0, 0)

247 02/05/2002 13:20:29.750 SEV=8 AUTHDBG/50 RPT=2386  
IntDB\_Decode(62b53e8, 111)

248 02/05/2002 13:20:29.750 SEV=8 AUTHDBG/47 RPT=2387  
IntDB\_Xmt(9b1c418)

249 02/05/2002 13:20:29.750 SEV=9 AUTHDBG/71 RPT=1194  
xmit\_cnt = 1

250 02/05/2002 13:20:29.750 SEV=8 AUTHDBG/47 RPT=2388  
IntDB\_Xmt(9b1c418)

251 02/05/2002 13:20:29.850 SEV=8 AUTHDBG/49 RPT=1193  
IntDB\_Match(9b1c418, 9b20a7c)

252 02/05/2002 13:20:29.850 SEV=8 AUTHDBG/63 RPT=1193  
AUTH\_RcvReply(9b1c418, 0, 0)

253 02/05/2002 13:20:29.850 SEV=8 AUTHDBG/50 RPT=2387  
IntDB\_Decode(9b20a7c, 653)

254 02/05/2002 13:20:29.850 SEV=8 AUTHDBG/48 RPT=1193  
IntDB\_Rcv(9b1c418)

255 02/05/2002 13:20:29.850 SEV=8 AUTHDBG/66 RPT=1194  
AUTH\_DeleteTimer(9b1c418, 0, 0)

256 02/05/2002 13:20:29.850 SEV=9 AUTHDBG/74 RPT=1194  
Reply timer stopped: handle = 15160016, timestamp = 34949341

257 02/05/2002 13:20:29.850 SEV=8 AUTHDBG/58 RPT=1193  
AUTH\_Callback(9b1c418, 0, 0)

258 02/05/2002 13:20:29.850 SEV=6 AUTH/41 RPT=1161 64.102.55.101  
Authentication successful: handle = 169, server = Internal, group = VPNC\_Base\_Group

260 02/05/2002 13:20:29.850 SEV=7 IKEDBG/0 RPT=33163 64.102.55.101  
Group [VPNC\_Base\_Group]  
Found Phase 1 Group (VPNC\_Base\_Group)

261 02/05/2002 13:20:29.850 SEV=8 AUTHDBG/4 RPT=1174  
AUTH\_GetAttrTable(169, 728c4c)

262 02/05/2002 13:20:29.850 SEV=7 IKEDBG/14 RPT=1145 64.102.55.101  
Group [VPNC\_Base\_Group]  
Authentication configured for Internal

263 02/05/2002 13:20:29.850 SEV=8 AUTHDBG/2 RPT=1194  
AUTH\_Close(169)

264 02/05/2002 13:20:29.850 SEV=9 IKEDBG/1 RPT=8092 64.102.55.101  
Group [VPNC\_Base\_Group]  
constructing ID

265 02/05/2002 13:20:29.850 SEV=9 IKEDBG/0 RPT=33164  
Group [VPNC\_Base\_Group]  
construct hash payload

266 02/05/2002 13:20:29.850 SEV=9 IKEDBG/0 RPT=33165 64.102.55.101  
Group [VPNC\_Base\_Group]  
computing hash

267 02/05/2002 13:20:29.850 SEV=9 IKEDBG/46 RPT=4583 64.102.55.101  
Group [VPNC\_Base\_Group]  
constructing dpd vid payload

268 02/05/2002 13:20:29.850 SEV=8 IKEDBG/0 RPT=33166 64.102.55.101

SENDING Message (msgid=0) with payloads :  
HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) ... total length : 80

270 02/05/2002 13:20:29.850 SEV=4 IKE/119 RPT=1145 64.102.55.101  
Group [VPNC\_Base\_Group]  
PHASE 1 COMPLETED

271 02/05/2002 13:20:29.850 SEV=6 IKE/121 RPT=1145 64.102.55.101  
Keep-alive type for this connection: None

272 02/05/2002 13:20:29.850 SEV=6 IKE/122 RPT=1145 64.102.55.101  
Keep-alives configured on but peer does not support keep-alives (type = None)

273 02/05/2002 13:20:29.850 SEV=7 IKEDBG/0 RPT=33167 64.102.55.101  
Group [VPNC\_Base\_Group]  
Starting phase 1 rekey timer: 21600000 (ms)

274 02/05/2002 13:20:29.850 SEV=8 AUTHDBG/60 RPT=1194  
AUTH\_UnbindServer(9b1c418, 0, 0)

275 02/05/2002 13:20:29.850 SEV=9 AUTHDBG/70 RPT=1194  
Auth Server 16b7fa0 has been unbound from ACB 9b1c418, sessions = 0

276 02/05/2002 13:20:29.850 SEV=8 AUTHDBG/10 RPT=1194  
AUTH\_Int\_FreeAuthCB(9b1c418)

277 02/05/2002 13:20:29.850 SEV=7 AUTH/13 RPT=1194  
Authentication session closed: handle = 169

278 02/05/2002 13:20:29.850 SEV=8 IKEDBG/0 RPT=33168 64.102.55.101  
RECEIVED Message (msgid=10f9c9b7) with payloads :  
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total length : 160

281 02/05/2002 13:20:29.850 SEV=9 IKEDBG/0 RPT=33169 64.102.55.101  
Group [VPNC\_Base\_Group]  
processing hash

282 02/05/2002 13:20:29.850 SEV=9 IKEDBG/0 RPT=33170 64.102.55.101  
Group [VPNC\_Base\_Group]  
processing SA payload

283 02/05/2002 13:20:29.850 SEV=9 IKEDBG/1 RPT=8093 64.102.55.101  
Group [VPNC\_Base\_Group]  
processing nonce payload

284 02/05/2002 13:20:29.850 SEV=9 IKEDBG/1 RPT=8094 64.102.55.101  
Group [VPNC\_Base\_Group]  
Processing ID

285 02/05/2002 13:20:29.850 SEV=5 IKE/25 RPT=1145 64.102.55.101  
Group [VPNC\_Base\_Group]  
Received remote Proxy Host data in ID Payload:  
Address 64.102.55.101, Protocol 17, Port 1701

288 02/05/2002 13:20:29.850 SEV=9 IKEDBG/1 RPT=8095 64.102.55.101  
Group [VPNC\_Base\_Group]  
Processing ID

289 02/05/2002 13:20:29.850 SEV=5 IKE/24 RPT=1145 64.102.55.101  
Group [VPNC\_Base\_Group]  
Received local Proxy Host data in ID Payload:  
Address 172.18.124.131, Protocol 17, Port 1701

292 02/05/2002 13:20:29.850 SEV=8 IKEDBG/0 RPT=33171  
QM IsRekeyed old sa not found by addr

293 02/05/2002 13:20:29.850 SEV=5 IKE/66 RPT=1145 64.102.55.101  
Group [VPNC\_Base\_Group]  
IKE Remote Peer configured for SA: ESP-3DES-MD5

294 02/05/2002 13:20:29.850 SEV=9 IKEDBG/0 RPT=33172 64.102.55.101  
Group [VPNC\_Base\_Group]  
processing IPSEC SA

295 02/05/2002 13:20:29.850 SEV=7 IKEDBG/27 RPT=12 64.102.55.101  
Group [VPNC\_Base\_Group]  
IPSec SA Proposal # 1, Transform # 1 acceptable

296 02/05/2002 13:20:29.850 SEV=7 IKEDBG/0 RPT=33173 64.102.55.101  
Group [VPNC\_Base\_Group]  
IKE: requesting SPI!

297 02/05/2002 13:20:29.850 SEV=9 IPSECDBG/6 RPT=54  
IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000, seq 12, err  
0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKey  
Len 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 708648, lifetime2 0, dsI  
d 300

301 02/05/2002 13:20:29.850 SEV=9 IPSECDBG/1 RPT=206  
Processing KEY\_GETSPI msg!

302 02/05/2002 13:20:29.850 SEV=7 IPSECDBG/13 RPT=12  
Reserved SPI 543073072

303 02/05/2002 13:20:29.850 SEV=8 IKEDBG/6 RPT=12  
IKE got SPI from key engine: SPI = 0x205ea330

304 02/05/2002 13:20:29.850 SEV=9 IKEDBG/0 RPT=33174 64.102.55.101  
Group [VPNC\_Base\_Group]  
oakley constructing quick mode

305 02/05/2002 13:20:29.850 SEV=9 IKEDBG/0 RPT=33175 64.102.55.101  
Group [VPNC\_Base\_Group]  
constructing blank hash

306 02/05/2002 13:20:29.850 SEV=9 IKEDBG/0 RPT=33176 64.102.55.101  
Group [VPNC\_Base\_Group]  
constructing ISA\_SA for ipsec

307 02/05/2002 13:20:29.850 SEV=9 IKEDBG/1 RPT=8096 64.102.55.101  
Group [VPNC\_Base\_Group]  
constructing ipsec nonce payload

308 02/05/2002 13:20:29.850 SEV=9 IKEDBG/1 RPT=8097 64.102.55.101  
Group [VPNC\_Base\_Group]  
constructing proxy ID

309 02/05/2002 13:20:29.850 SEV=7 IKEDBG/0 RPT=33177 64.102.55.101  
Group [VPNC\_Base\_Group]  
Transmitting Proxy Id:  
Remote host: 64.102.55.101 Protocol 17 Port 1701  
Local host: 172.18.124.131 Protocol 17 Port 1701

313 02/05/2002 13:20:29.850 SEV=9 IKEDBG/0 RPT=33178 64.102.55.101  
Group [VPNC\_Base\_Group]  
constructing qm hash

314 02/05/2002 13:20:29.850 SEV=8 IKEDBG/0 RPT=33179 64.102.55.101  
SENDING Message (msgid=10f9c9b7) with payloads :  
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total leng  
th : 156

317 02/05/2002 13:20:29.860 SEV=4 IPSEC/7 RPT=23  
IPSec ESP Tunnel Inb: invalid direction in security association

318 02/05/2002 13:20:29.860 SEV=7 IPSECDBG/7 RPT=12  
IPSEC secassoc dump (from ipsec\_esp\_input) - type 2, state 0x04, spi 205ea330, algorithm 0, lifetype 0, lifetime1 0, lifetime2 0, src 000000f0, dst 00000000, from 00000000/40663765/ac127c83, to 00000000/00000000/00000000

321 02/05/2002 13:20:29.860 SEV=6 IPSEC/7 RPT=24  
IPSec ESP Tunnel Inb: Invalid SA or pre-parsing problem!

322 02/05/2002 13:20:29.860 SEV=8 IKEDBG/0 RPT=33180 64.102.55.101  
RECEIVED Message (msgid=10f9c9b7) with payloads :  
HDR + HASH (8) + NONE (0) ... total length : 48

324 02/05/2002 13:20:29.860 SEV=9 IKEDBG/0 RPT=33181 64.102.55.101  
Group [VPNC\_Base\_Group]  
processing hash

325 02/05/2002 13:20:29.860 SEV=9 IKEDBG/0 RPT=33182 64.102.55.101  
Group [VPNC\_Base\_Group]  
loading all IPSEC SAs

326 02/05/2002 13:20:29.860 SEV=9 IKEDBG/1 RPT=8098 64.102.55.101  
Group [VPNC\_Base\_Group]  
Generating Quick Mode Key!

327 02/05/2002 13:20:29.860 SEV=9 IKEDBG/1 RPT=8099 64.102.55.101  
Group [VPNC\_Base\_Group]  
Generating Quick Mode Key!

328 02/05/2002 13:20:29.860 SEV=7 IKEDBG/0 RPT=33183 64.102.55.101  
Group [VPNC\_Base\_Group]  
Loading host:  
  Dst: 172.18.124.131  
  Src: 64.102.55.101

329 02/05/2002 13:20:29.860 SEV=4 IKE/49 RPT=12 64.102.55.101  
Group [VPNC\_Base\_Group]  
Security negotiation complete for User ()  
Responder, Inbound SPI = 0x205ea330, Outbound SPI = 0xec82c01c

332 02/05/2002 13:20:29.860 SEV=9 IPSECDBG/6 RPT=55  
IPSEC key message parse - msgtype 1, len 592, vers 1, pid 00000000, seq 0, err 0, type 2, mode 2, state 64, label 0, pad 0, spi ec82c01c, encrKeyLen 8, hashKeyLen 16, ivlen 8, alg 1, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, dsid 95000000

336 02/05/2002 13:20:29.860 SEV=9 IPSECDBG/1 RPT=207  
Processing KEY\_ADD msg!

337 02/05/2002 13:20:29.860 SEV=9 IPSECDBG/1 RPT=208  
key\_msghdr2secassoc(): Enter

338 02/05/2002 13:20:29.860 SEV=7 IPSECDBG/1 RPT=209  
No USER filter configured

339 02/05/2002 13:20:29.860 SEV=9 IPSECDBG/1 RPT=210  
KeyProcessAdd: Enter

340 02/05/2002 13:20:29.860 SEV=8 IPSECDBG/1 RPT=211  
KeyProcessAdd: Adding outbound SA

341 02/05/2002 13:20:29.860 SEV=8 IPSECDBG/1 RPT=212  
KeyProcessAdd: src 172.18.124.131 mask 0.0.0.0, dst 64.102.55.101 mask 0.0.0.0

342 02/05/2002 13:20:29.860 SEV=8 IPSECDBG/1 RPT=213  
KeyProcessAdd: FilterIpsecAddIkeSa success

343 02/05/2002 13:20:29.860 SEV=9 IPSECDBG/6 RPT=56  
IPSEC key message parse - msgtype 3, len 312, vers 1, pid 00000000, seq 0, err 0  
, type 2, mode 2, state 32, label 0, pad 0, spi 205ea330, encrKeyLen 8, hashKeyL  
en 16, ivlen 8, alg 1, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, dsI  
d 95000000

347 02/05/2002 13:20:29.860 SEV=9 IPSECDBG/1 RPT=214  
Processing KEY\_UPDATE msg!

348 02/05/2002 13:20:29.860 SEV=9 IPSECDBG/1 RPT=215  
Update inbound SA addresses

349 02/05/2002 13:20:29.860 SEV=9 IPSECDBG/1 RPT=216  
key\_msghdr2secassoc(): Enter

350 02/05/2002 13:20:29.860 SEV=7 IPSECDBG/1 RPT=217  
No USER filter configured

351 02/05/2002 13:20:29.860 SEV=9 IPSECDBG/1 RPT=218  
KeyProcessUpdate: Enter

352 02/05/2002 13:20:29.860 SEV=8 IPSECDBG/1 RPT=219  
KeyProcessUpdate: success

353 02/05/2002 13:20:29.860 SEV=8 IKEDBG/7 RPT=12  
IKE got a KEY\_ADD msg for SA: SPI = 0xec82c01c

354 02/05/2002 13:20:29.860 SEV=8 IKEDBG/0 RPT=33184  
pitcher: rcv KEY\_UPDATE, spi 0x205ea330

355 02/05/2002 13:20:29.860 SEV=4 IKE/120 RPT=12 64.102.55.101  
Group [VPNC\_Base\_Group]  
PHASE 2 COMPLETED (msgid=10f9c9b7)

356 02/05/2002 13:20:30.650 SEV=7 IPSECDBG/1 RPT=220  
IPSec Inbound SA has received data!

357 02/05/2002 13:20:30.650 SEV=8 IKEDBG/0 RPT=33185  
pitcher: rcv KEY\_SA\_ACTIVE spi 0x205ea330

358 02/05/2002 13:20:30.650 SEV=8 IKEDBG/0 RPT=33186  
KEY\_SA\_ACTIVE no old rekey centry found with new spi 0x205ea330, mess\_id 0x0

359 02/05/2002 13:20:30.650 SEV=4 L2TP/57 RPT=32  
Tunnel to peer 64.102.55.101 established

360 02/05/2002 13:20:30.650 SEV=4 L2TP/53 RPT=32 64.102.55.101  
Session started on tunnel 64.102.55.101

361 02/05/2002 13:20:33.650 SEV=8 AUTHDBG/1 RPT=1195  
AUTH\_Open() returns 170

362 02/05/2002 13:20:33.650 SEV=7 AUTH/12 RPT=1195  
Authentication session opened: handle = 170

363 02/05/2002 13:20:33.650 SEV=8 AUTHDBG/9 RPT=65  
AUTH\_GetChallenge(170, 8aa, 8, 42a25c)

364 02/05/2002 13:20:33.650 SEV=8 AUTHDBG/3 RPT=1227  
AUTH\_PutAttrTable(170, 727bec)

365 02/05/2002 13:20:33.650 SEV=8 AUTHDBG/9 RPT=66

AUTH\_GetChallenge(170, 8aa, 8, 42a25c)

366 02/05/2002 13:20:33.650 SEV=8 AUTHDBG/59 RPT=1227  
AUTH\_BindServer(9b1d084, 0, 0)

367 02/05/2002 13:20:33.650 SEV=9 AUTHDBG/69 RPT=1227  
Auth Server 16b7fa0 has been bound to ACB 9b1d084, sessions = 1

368 02/05/2002 13:20:33.650 SEV=8 AUTHDBG/3 RPT=1228  
AUTH\_PutAttrTable(170, 727bec)

369 02/05/2002 13:20:33.650 SEV=8 AUTHDBG/5 RPT=33  
AUTH\_Authenticate(170, 8aa, 429df8)

370 02/05/2002 13:20:33.650 SEV=8 AUTHDBG/59 RPT=1228  
AUTH\_BindServer(9b1d084, 0, 0)

371 02/05/2002 13:20:33.650 SEV=9 AUTHDBG/69 RPT=1228  
Auth Server 16b7fa0 has been bound to ACB 9b1d084, sessions = 1

372 02/05/2002 13:20:33.650 SEV=8 AUTHDBG/65 RPT=1195  
AUTH\_CreateTimer(9b1d084, 0, 0)

373 02/05/2002 13:20:33.650 SEV=9 AUTHDBG/72 RPT=1195  
Reply timer created: handle = 15260018

374 02/05/2002 13:20:33.650 SEV=8 AUTHDBG/61 RPT=1195  
AUTH\_BuildMsg(9b1d084, 0, 0)

375 02/05/2002 13:20:33.650 SEV=8 AUTHDBG/64 RPT=1195  
AUTH\_StartTimer(9b1d084, 0, 0)

376 02/05/2002 13:20:33.650 SEV=9 AUTHDBG/73 RPT=1195  
Reply timer started: handle = 15260018, timestamp = 34949721, timeout = 30000

377 02/05/2002 13:20:33.650 SEV=8 AUTHDBG/62 RPT=1195  
AUTH\_SndRequest(9b1d084, 0, 0)

378 02/05/2002 13:20:33.650 SEV=8 AUTHDBG/50 RPT=2388  
IntDB\_Decode(62f6d48, 162)

379 02/05/2002 13:20:33.650 SEV=8 AUTHDBG/47 RPT=2389  
IntDB\_Xmt(9b1d084)

380 02/05/2002 13:20:33.650 SEV=9 AUTHDBG/71 RPT=1195  
xmit\_cnt = 1

381 02/05/2002 13:20:33.650 SEV=8 AUTHDBG/47 RPT=2390  
IntDB\_Xmt(9b1d084)

382 02/05/2002 13:20:33.750 SEV=8 AUTHDBG/49 RPT=1194  
IntDB\_Match(9b1d084, 62f70b4)

383 02/05/2002 13:20:33.750 SEV=8 AUTHDBG/63 RPT=1194  
AUTH\_RcvReply(9b1d084, 0, 0)

384 02/05/2002 13:20:33.750 SEV=8 AUTHDBG/50 RPT=2389  
IntDB\_Decode(62f70b4, 137)

385 02/05/2002 13:20:33.750 SEV=8 AUTHDBG/48 RPT=1194  
IntDB\_Rcv(9b1d084)

386 02/05/2002 13:20:33.750 SEV=8 AUTHDBG/66 RPT=1195  
AUTH\_DeleteTimer(9b1d084, 0, 0)

387 02/05/2002 13:20:33.750 SEV=9 AUTHDBG/74 RPT=1195

Reply timer stopped: handle = 15260018, timestamp = 34949731

388 02/05/2002 13:20:33.750 SEV=8 AUTHDBG/58 RPT=1194  
AUTH\_Callback(9b1d084, 0, 0)

389 02/05/2002 13:20:33.750 SEV=6 AUTH/4 RPT=14 64.102.55.101  
Authentication successful: handle = 170, server = Internal, user = L2TP2k\_user

390 02/05/2002 13:20:33.750 SEV=5 PPP/8 RPT=14 64.102.55.101  
User [L2TP2k\_user]  
Authenticated successfully with MSCHAP-V1

391 02/05/2002 13:20:33.750 SEV=8 AUTHDBG/60 RPT=1195  
AUTH\_UnbindServer(9b1d084, 0, 0)

392 02/05/2002 13:20:33.750 SEV=9 AUTHDBG/70 RPT=1195  
Auth Server 16b7fa0 has been unbound from ACB 9b1d084, sessions = 0

393 02/05/2002 13:20:33.750 SEV=8 AUTHDBG/4 RPT=1175  
AUTH\_GetAttrTable(170, 72796c)

394 02/05/2002 13:20:33.750 SEV=8 AUTHDBG/2 RPT=1195  
AUTH\_Close(170)

395 02/05/2002 13:20:33.750 SEV=8 AUTHDBG/10 RPT=1195  
AUTH\_Int\_FreeAuthCB(9b1d084)

396 02/05/2002 13:20:33.750 SEV=7 AUTH/13 RPT=1195  
Authentication session closed: handle = 170

397 02/05/2002 13:20:36.680 SEV=4 AUTH/22 RPT=34  
User L2TP2k\_user connected

398 02/05/2002 13:20:39.110 SEV=4 L2TP/47 RPT=31 172.18.124.197  
Session closed on tunnel 172.18.124.197 (peer 1, local 58700, serial 0), reason:  
L2TP peer terminated connection

400 02/05/2002 13:20:39.110 SEV=9 IKEDBG/0 RPT=33187  
sending delete message

401 02/05/2002 13:20:39.110 SEV=9 IKEDBG/0 RPT=33188 172.18.124.197  
Group [VPNC\_Base\_Group]  
constructing blank hash

402 02/05/2002 13:20:39.110 SEV=9 IKEDBG/0 RPT=33189  
constructing ipsec delete payload

403 02/05/2002 13:20:39.110 SEV=9 IKEDBG/0 RPT=33190 172.18.124.197  
Group [VPNC\_Base\_Group]  
constructing qm hash

404 02/05/2002 13:20:39.110 SEV=8 IKEDBG/0 RPT=33191 172.18.124.197  
SENDING Message (msgid=19e3b16b) with payloads :  
HDR + HASH (8) + DELETE (12) + NONE (0) ... total length : 64

406 02/05/2002 13:20:39.110 SEV=7 IKEDBG/9 RPT=11 172.18.124.197  
Group [VPNC\_Base\_Group]  
IKE Deleting SA: Remote Proxy 172.18.124.197, Local Proxy 172.18.124.131

408 02/05/2002 13:20:39.110 SEV=9 IKEDBG/0 RPT=33192 172.18.124.197  
Group [VPNC\_Base\_Group]  
IKE SA MM:1dceb39 rcv'd Terminate: state MM\_ACTIVE  
flags 0x00000042, refcnt 1, tuncnt 0

411 02/05/2002 13:20:39.110 SEV=9 IKEDBG/0 RPT=33193 172.18.124.197  
Group [VPNC\_Base\_Group]

IKE SA MM:1dcebf39 terminating:  
flags 0x01000002, refcnt 0, tuncnt 0

413 02/05/2002 13:20:39.110 SEV=9 IKEDBG/0 RPT=33194  
sending delete message

414 02/05/2002 13:20:39.110 SEV=9 IKEDBG/0 RPT=33195 172.18.124.197  
Group [VPNC\_Base\_Group]  
constructing blank hash

415 02/05/2002 13:20:39.110 SEV=9 IKEDBG/0 RPT=33196  
constructing delete payload

416 02/05/2002 13:20:39.110 SEV=9 IKEDBG/0 RPT=33197 172.18.124.197  
Group [VPNC\_Base\_Group]  
constructing qm hash

417 02/05/2002 13:20:39.110 SEV=8 IKEDBG/0 RPT=33198 172.18.124.197  
SENDING Message (msgid=f4c647aa) with payloads :  
HDR + HASH (8) + DELETE (12) + NONE (0) ... total length : 76

419 02/05/2002 13:20:39.110 SEV=9 IPSECDBG/6 RPT=57  
IPSEC key message parse - msgtype 2, len 266, vers 1, pid 00000000, seq 0, err 0  
, type 2, mode 0, state 32, label 0, pad 0, spi 13a0490f, encrKeyLen 0, hashKeyL  
en 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 708648, lifetime2 0, dsId  
0

423 02/05/2002 13:20:39.110 SEV=9 IPSECDBG/1 RPT=221  
Processing KEY\_DELETE msg!

424 02/05/2002 13:20:39.110 SEV=4 AUTH/28 RPT=13 172.18.124.197  
User [L2TP\_user] disconnected:  
Duration: 0:03:20  
Bytes xmt: 63880  
Bytes rcv: 72424  
Reason: User Requested

426 02/05/2002 13:20:39.110 SEV=9 IPSECDBG/6 RPT=58  
IPSEC key message parse - msgtype 2, len 266, vers 1, pid 00000000, seq 0, err 0  
, type 2, mode 0, state 64, label 0, pad 0, spi elb59da4, encrKeyLen 0, hashKeyL  
en 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 708648, lifetime2 0, dsId  
0

430 02/05/2002 13:20:39.110 SEV=9 IPSECDBG/1 RPT=222  
Processing KEY\_DELETE msg!

431 02/05/2002 13:20:39.110 SEV=9 IPSECDBG/1 RPT=223  
key\_msghdr2secassoc(): Enter

432 02/05/2002 13:20:39.110 SEV=7 IPSECDBG/1 RPT=224  
No USER filter configured

433 02/05/2002 13:20:39.110 SEV=8 IKEDBG/0 RPT=33199  
pitcher: received key delete msg, spi 0x13a0490f

434 02/05/2002 13:20:39.110 SEV=8 IKEDBG/0 RPT=33200  
pitcher: received key delete msg, spi 0xelb59da4

435 02/05/2002 13:20:39.110 SEV=4 L2TP/46 RPT=31 172.18.124.197  
Tunnel to peer 172.18.124.197 closed, reason: L2TP peer terminated connection

436 02/05/2002 13:20:41.940 SEV=8 IKEDBG/0 RPT=33201 172.18.124.197  
RECEIVED Message (msgid=0) with payloads :  
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 216

438 02/05/2002 13:20:41.940 SEV=9 IKEDBG/0 RPT=33202 172.18.124.197

processing SA payload

439 02/05/2002 13:20:41.940 SEV=8 IKEDBG/0 RPT=33203 172.18.124.197  
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE

Parsing received transform:

Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

444 02/05/2002 13:20:41.940 SEV=8 IKEDBG/0 RPT=33204 172.18.124.197  
Phase 1 failure against global IKE proposal # 2:

Mismatched attr types for class Hash Alg:  
Rcv'd: SHA  
Cfg'd: MD5

446 02/05/2002 13:20:41.940 SEV=8 IKEDBG/0 RPT=33205 172.18.124.197  
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

449 02/05/2002 13:20:41.940 SEV=8 IKEDBG/0 RPT=33206 172.18.124.197  
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

452 02/05/2002 13:20:41.940 SEV=8 IKEDBG/0 RPT=33207 172.18.124.197  
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

455 02/05/2002 13:20:41.940 SEV=8 IKEDBG/0 RPT=33208 172.18.124.197  
Phase 1 failure against global IKE proposal # 6:

Mismatched attr types for class Hash Alg:  
Rcv'd: SHA  
Cfg'd: MD5

457 02/05/2002 13:20:41.940 SEV=8 IKEDBG/0 RPT=33209 172.18.124.197  
Phase 1 failure against global IKE proposal # 7:

Mismatched attr types for class Hash Alg:  
Rcv'd: SHA  
Cfg'd: MD5

459 02/05/2002 13:20:41.940 SEV=8 IKEDBG/0 RPT=33210 172.18.124.197  
Proposal # 1, Transform # 2, Type ISAKMP, Id IKE

Parsing received transform:

Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

464 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33211 172.18.124.197  
Phase 1 failure against global IKE proposal # 2:

Mismatched attr types for class Auth Method:  
Rcv'd: Preshared Key  
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

468 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33212 172.18.124.197  
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

471 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33213 172.18.124.197  
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

474 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33214 172.18.124.197  
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

477 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33215 172.18.124.197  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class Auth Method:  
Rcv'd: Preshared Key  
Cfg'd: RSA signature with Certificates

480 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33216 172.18.124.197  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class Auth Method:  
Rcv'd: Preshared Key  
Cfg'd: XAUTH with RSA signatures (Initiator authenticated)

484 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33217 172.18.124.197  
Proposal # 1, Transform # 3, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

489 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33218 172.18.124.197  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 2

492 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33219 172.18.124.197  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

495 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33220 172.18.124.197  
Phase 1 failure against global IKE proposal # 4:  
Mismatched attr types for class Hash Alg:  
Rcv'd: SHA  
Cfg'd: MD5

497 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33221 172.18.124.197  
Phase 1 failure against global IKE proposal # 5:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 7

500 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33222 172.18.124.197  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 2

503 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33223 172.18.124.197  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1

Cfg'd: Oakley Group 2

506 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33224 172.18.124.197  
Proposal # 1, Transform # 4, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

511 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33225 172.18.124.197  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 2

514 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33226 172.18.124.197  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

517 02/05/2002 13:20:41.950 SEV=7 IKEDBG/0 RPT=33227 172.18.124.197  
Oakley proposal is acceptable

518 02/05/2002 13:20:41.950 SEV=9 IKEDBG/47 RPT=1195 172.18.124.197  
processing VID payload

519 02/05/2002 13:20:41.950 SEV=9 IKEDBG/0 RPT=33228 172.18.124.197  
processing IKE SA

520 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33229 172.18.124.197  
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

525 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33230 172.18.124.197  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class Hash Alg:  
Rcv'd: SHA  
Cfg'd: MD5

527 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33231 172.18.124.197  
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

530 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33232 172.18.124.197  
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

533 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33233 172.18.124.197  
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

536 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33234 172.18.124.197  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class Hash Alg:

Rcv'd: SHA  
Cfg'd: MD5

538 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33235 172.18.124.197  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class Hash Alg:  
Rcv'd: SHA  
Cfg'd: MD5

540 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33236 172.18.124.197  
Proposal # 1, Transform # 2, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

545 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33237 172.18.124.197  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class Auth Method:  
Rcv'd: Preshared Key  
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

549 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33238 172.18.124.197  
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

552 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33239 172.18.124.197  
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

555 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33240 172.18.124.197  
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

558 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33241 172.18.124.197  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class Auth Method:  
Rcv'd: Preshared Key  
Cfg'd: RSA signature with Certificates

561 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33242 172.18.124.197  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class Auth Method:  
Rcv'd: Preshared Key  
Cfg'd: XAUTH with RSA signatures (Initiator authenticated)

565 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33243 172.18.124.197  
Proposal # 1, Transform # 3, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

570 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33244 172.18.124.197  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 2

573 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33245 172.18.124.197  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

576 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33246 172.18.124.197  
Phase 1 failure against global IKE proposal # 4:  
Mismatched attr types for class Hash Alg:  
Rcv'd: SHA  
Cfg'd: MD5

578 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33247 172.18.124.197  
Phase 1 failure against global IKE proposal # 5:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 7

581 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33248 172.18.124.197  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 2

584 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33249 172.18.124.197  
Phase 1 failure against global IKE proposal # 7:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 2

587 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33250 172.18.124.197  
Proposal # 1, Transform # 4, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

592 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33251 172.18.124.197  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 1  
Cfg'd: Oakley Group 2

595 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33252 172.18.124.197  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class Encryption Alg:  
Rcv'd: DES-CBC  
Cfg'd: Triple-DES

598 02/05/2002 13:20:41.950 SEV=7 IKEDBG/28 RPT=1147 172.18.124.197  
IKE SA Proposal # 1, Transform # 4 acceptable  
Matches global IKE entry # 4

599 02/05/2002 13:20:41.950 SEV=9 IKEDBG/0 RPT=33253 172.18.124.197  
constructing ISA\_SA for isakmp

600 02/05/2002 13:20:41.950 SEV=8 IKEDBG/0 RPT=33254 172.18.124.197  
SENDING Message (msgid=0) with payloads :  
HDR + SA (1) + NONE (0) ... total length : 80

602 02/05/2002 13:20:41.990 SEV=8 IKEDBG/0 RPT=33255 172.18.124.197  
RECEIVED Message (msgid=0) with payloads :  
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

604 02/05/2002 13:20:41.990 SEV=8 IKEDBG/0 RPT=33256 172.18.124.197  
RECEIVED Message (msgid=0) with payloads :  
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

606 02/05/2002 13:20:41.990 SEV=9 IKEDBG/0 RPT=33257 172.18.124.197  
processing ke payload

607 02/05/2002 13:20:41.990 SEV=9 IKEDBG/0 RPT=33258 172.18.124.197  
processing ISA\_KE

608 02/05/2002 13:20:41.990 SEV=9 IKEDBG/1 RPT=8100 172.18.124.197  
processing nonce payload

609 02/05/2002 13:20:42.010 SEV=9 IKEDBG/0 RPT=33259 172.18.124.197  
constructing ke payload

610 02/05/2002 13:20:42.010 SEV=9 IKEDBG/1 RPT=8101 172.18.124.197  
constructing nonce payload

611 02/05/2002 13:20:42.010 SEV=9 IKEDBG/46 RPT=4584 172.18.124.197  
constructing Cisco Unity VID payload

612 02/05/2002 13:20:42.010 SEV=9 IKEDBG/46 RPT=4585 172.18.124.197  
constructing xauth V6 VID payload

613 02/05/2002 13:20:42.010 SEV=9 IKEDBG/48 RPT=2293 172.18.124.197  
Send IOS VID

614 02/05/2002 13:20:42.010 SEV=9 IKEDBG/38 RPT=1147 172.18.124.197  
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)

616 02/05/2002 13:20:42.010 SEV=9 IKEDBG/46 RPT=4586 172.18.124.197  
constructing VID payload

617 02/05/2002 13:20:42.010 SEV=9 IKEDBG/48 RPT=2294 172.18.124.197  
Send Altiga GW VID

618 02/05/2002 13:20:42.010 SEV=9 IKEDBG/0 RPT=33260 172.18.124.197  
Generating keys for Responder...

619 02/05/2002 13:20:42.010 SEV=6 IKE/139 RPT=1147 172.18.124.197  
Group 172.18.124.197 not found, using BASE GROUP default preshared key

620 02/05/2002 13:20:42.010 SEV=8 IKEDBG/0 RPT=33261 172.18.124.197  
SENDING Message (msgid=0) with payloads :  
HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13)  
+ NONE (0) ... total length : 224

623 02/05/2002 13:20:42.040 SEV=8 IKEDBG/0 RPT=33262 172.18.124.197  
RECEIVED Message (msgid=0) with payloads :  
HDR + ID (5) + HASH (8) + NONE (0) ... total length : 60

625 02/05/2002 13:20:42.040 SEV=9 IKEDBG/1 RPT=8102 172.18.124.197  
Group [VPNC\_Base\_Group]  
Processing ID

626 02/05/2002 13:20:42.040 SEV=9 IKEDBG/0 RPT=33263 172.18.124.197  
Group [VPNC\_Base\_Group]  
processing hash

627 02/05/2002 13:20:42.040 SEV=9 IKEDBG/0 RPT=33264 172.18.124.197  
Group [VPNC\_Base\_Group]  
computing hash

628 02/05/2002 13:20:42.040 SEV=9 IKEDBG/23 RPT=1163 172.18.124.197

Group [VPNC\_Base\_Group]  
Starting group lookup for peer 172.18.124.197

629 02/05/2002 13:20:42.040 SEV=8 AUTHDBG/1 RPT=1196  
AUTH\_Open() returns 171

630 02/05/2002 13:20:42.040 SEV=7 AUTH/12 RPT=1196  
Authentication session opened: handle = 171

631 02/05/2002 13:20:42.040 SEV=8 AUTHDBG/3 RPT=1229  
AUTH\_PutAttrTable(171, 728a84)

632 02/05/2002 13:20:42.040 SEV=8 AUTHDBG/6 RPT=1163  
AUTH\_GroupAuthenticate(171, 5009504, 482fb0)

633 02/05/2002 13:20:42.040 SEV=8 AUTHDBG/59 RPT=1229  
AUTH\_BindServer(9b19ab0, 0, 0)

634 02/05/2002 13:20:42.040 SEV=9 AUTHDBG/69 RPT=1229  
Auth Server 16b7fa0 has been bound to ACB 9b19ab0, sessions = 1

635 02/05/2002 13:20:42.040 SEV=8 AUTHDBG/65 RPT=1196  
AUTH\_CreateTimer(9b19ab0, 0, 0)

636 02/05/2002 13:20:42.040 SEV=9 AUTHDBG/72 RPT=1196  
Reply timer created: handle = 15320016

637 02/05/2002 13:20:42.040 SEV=8 AUTHDBG/61 RPT=1196  
AUTH\_BuildMsg(9b19ab0, 0, 0)

638 02/05/2002 13:20:42.040 SEV=8 AUTHDBG/64 RPT=1196  
AUTH\_StartTimer(9b19ab0, 0, 0)

639 02/05/2002 13:20:42.040 SEV=9 AUTHDBG/73 RPT=1196  
Reply timer started: handle = 15320016, timestamp = 34950560, timeout = 30000

640 02/05/2002 13:20:42.040 SEV=8 AUTHDBG/62 RPT=1196  
AUTH\_SndRequest(9b19ab0, 0, 0)

641 02/05/2002 13:20:42.040 SEV=8 AUTHDBG/50 RPT=2390  
IntDB\_Decode(62f60bc, 112)

642 02/05/2002 13:20:42.040 SEV=8 AUTHDBG/47 RPT=2391  
IntDB\_Xmt(9b19ab0)

643 02/05/2002 13:20:42.040 SEV=9 AUTHDBG/71 RPT=1196  
xmit\_cnt = 1

644 02/05/2002 13:20:42.040 SEV=8 AUTHDBG/47 RPT=2392  
IntDB\_Xmt(9b19ab0)

645 02/05/2002 13:20:42.140 SEV=8 AUTHDBG/49 RPT=1195  
IntDB\_Match(9b19ab0, 9b185fc)

646 02/05/2002 13:20:42.140 SEV=8 AUTHDBG/63 RPT=1195  
AUTH\_RcvReply(9b19ab0, 0, 0)

647 02/05/2002 13:20:42.140 SEV=8 AUTHDBG/50 RPT=2391  
IntDB\_Decode(9b185fc, 653)

648 02/05/2002 13:20:42.140 SEV=8 AUTHDBG/48 RPT=1195  
IntDB\_Rcv(9b19ab0)

649 02/05/2002 13:20:42.140 SEV=8 AUTHDBG/66 RPT=1196  
AUTH\_DeleteTimer(9b19ab0, 0, 0)

650 02/05/2002 13:20:42.140 SEV=9 AUTHDBG/74 RPT=1196  
Reply timer stopped: handle = 15320016, timestamp = 34950570

651 02/05/2002 13:20:42.140 SEV=8 AUTHDBG/58 RPT=1195  
AUTH\_Callback(9b19ab0, 0, 0)

652 02/05/2002 13:20:42.140 SEV=6 AUTH/41 RPT=1162 172.18.124.197  
Authentication successful: handle = 171, server = Internal, group = VPNC\_Base\_Group

654 02/05/2002 13:20:42.140 SEV=7 IKEDBG/0 RPT=33265 172.18.124.197  
Group [VPNC\_Base\_Group]  
Found Phase 1 Group (VPNC\_Base\_Group)

655 02/05/2002 13:20:42.140 SEV=8 AUTHDBG/4 RPT=1176  
AUTH\_GetAttrTable(171, 728c4c)

656 02/05/2002 13:20:42.140 SEV=7 IKEDBG/14 RPT=1146 172.18.124.197  
Group [VPNC\_Base\_Group]  
Authentication configured for Internal

657 02/05/2002 13:20:42.140 SEV=8 AUTHDBG/2 RPT=1196  
AUTH\_Close(171)

658 02/05/2002 13:20:42.140 SEV=9 IKEDBG/1 RPT=8103 172.18.124.197  
Group [VPNC\_Base\_Group]  
constructing ID

659 02/05/2002 13:20:42.140 SEV=9 IKEDBG/0 RPT=33266  
Group [VPNC\_Base\_Group]  
construct hash payload

660 02/05/2002 13:20:42.140 SEV=9 IKEDBG/0 RPT=33267 172.18.124.197  
Group [VPNC\_Base\_Group]  
computing hash

661 02/05/2002 13:20:42.140 SEV=9 IKEDBG/46 RPT=4587 172.18.124.197  
Group [VPNC\_Base\_Group]  
constructing dpd vid payload

662 02/05/2002 13:20:42.140 SEV=8 IKEDBG/0 RPT=33268 172.18.124.197  
SENDING Message (msgid=0) with payloads :  
HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) ... total length : 80

664 02/05/2002 13:20:42.140 SEV=4 IKE/119 RPT=1146 172.18.124.197  
Group [VPNC\_Base\_Group]  
PHASE 1 COMPLETED

665 02/05/2002 13:20:42.140 SEV=6 IKE/121 RPT=1146 172.18.124.197  
Keep-alive type for this connection: None

666 02/05/2002 13:20:42.140 SEV=6 IKE/122 RPT=1146 172.18.124.197  
Keep-alives configured on but peer does not support keep-alives (type = None)

667 02/05/2002 13:20:42.140 SEV=7 IKEDBG/0 RPT=33269 172.18.124.197  
Group [VPNC\_Base\_Group]  
Starting phase 1 rekey timer: 21600000 (ms)

668 02/05/2002 13:20:42.140 SEV=8 AUTHDBG/60 RPT=1196  
AUTH\_UnbindServer(9b19ab0, 0, 0)

669 02/05/2002 13:20:42.140 SEV=9 AUTHDBG/70 RPT=1196  
Auth Server 16b7fa0 has been unbound from ACB 9b19ab0, sessions = 0

670 02/05/2002 13:20:42.140 SEV=8 AUTHDBG/10 RPT=1196

AUTH\_Int\_FreeAuthCB(9b19ab0)

671 02/05/2002 13:20:42.140 SEV=7 AUTH/13 RPT=1196  
Authentication session closed: handle = 171

672 02/05/2002 13:20:42.150 SEV=8 IKEDBG/0 RPT=33270 172.18.124.197  
RECEIVED Message (msgid=dba7daa8) with payloads :  
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total length : 136

675 02/05/2002 13:20:42.150 SEV=9 IKEDBG/0 RPT=33271 172.18.124.197  
Group [VPNC\_Base\_Group]  
processing hash

676 02/05/2002 13:20:42.150 SEV=9 IKEDBG/0 RPT=33272 172.18.124.197  
Group [VPNC\_Base\_Group]  
processing SA payload

677 02/05/2002 13:20:42.150 SEV=9 IKEDBG/1 RPT=8104 172.18.124.197  
Group [VPNC\_Base\_Group]  
processing nonce payload

678 02/05/2002 13:20:42.150 SEV=9 IKEDBG/1 RPT=8105 172.18.124.197  
Group [VPNC\_Base\_Group]  
Processing ID

679 02/05/2002 13:20:42.150 SEV=5 IKE/25 RPT=1146 172.18.124.197  
Group [VPNC\_Base\_Group]  
Received remote Proxy Host data in ID Payload:  
Address 172.18.124.197, Protocol 17, Port 1701

682 02/05/2002 13:20:42.150 SEV=9 IKEDBG/1 RPT=8106 172.18.124.197  
Group [VPNC\_Base\_Group]  
Processing ID

683 02/05/2002 13:20:42.150 SEV=5 IKE/24 RPT=1146 172.18.124.197  
Group [VPNC\_Base\_Group]  
Received local Proxy Host data in ID Payload:  
Address 172.18.124.131, Protocol 17, Port 0

686 02/05/2002 13:20:42.150 SEV=8 IKEDBG/0 RPT=33273  
QM IsRekeyed old sa not found by addr

687 02/05/2002 13:20:42.150 SEV=5 IKE/66 RPT=1146 172.18.124.197  
Group [VPNC\_Base\_Group]  
IKE Remote Peer configured for SA: ESP-3DES-MD5

688 02/05/2002 13:20:42.150 SEV=9 IKEDBG/0 RPT=33274 172.18.124.197  
Group [VPNC\_Base\_Group]  
processing IPSEC SA

689 02/05/2002 13:20:42.150 SEV=7 IKEDBG/27 RPT=13 172.18.124.197  
Group [VPNC\_Base\_Group]  
IPSec SA Proposal # 1, Transform # 1 acceptable

690 02/05/2002 13:20:42.150 SEV=7 IKEDBG/0 RPT=33275 172.18.124.197  
Group [VPNC\_Base\_Group]  
IKE: requesting SPI!

691 02/05/2002 13:20:42.150 SEV=9 IPSECDBG/6 RPT=59  
IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000, seq 13, err 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 708648, lifetime2 0, dsid 300

695 02/05/2002 13:20:42.150 SEV=9 IPSECDBG/1 RPT=225

Processing KEY\_GETSPI msg!

696 02/05/2002 13:20:42.150 SEV=7 IPSECDBG/13 RPT=13  
Reserved SPI 1842824273

697 02/05/2002 13:20:42.150 SEV=8 IKEDBG/6 RPT=13  
IKE got SPI from key engine: SPI = 0x6dd74451

698 02/05/2002 13:20:42.150 SEV=9 IKEDBG/0 RPT=33276 172.18.124.197  
Group [VPNC\_Base\_Group]  
oakley constructing quick mode

699 02/05/2002 13:20:42.150 SEV=9 IKEDBG/0 RPT=33277 172.18.124.197  
Group [VPNC\_Base\_Group]  
constructing blank hash

700 02/05/2002 13:20:42.150 SEV=9 IKEDBG/0 RPT=33278 172.18.124.197  
Group [VPNC\_Base\_Group]  
constructing ISA\_SA for ipsec

701 02/05/2002 13:20:42.150 SEV=9 IKEDBG/1 RPT=8107 172.18.124.197  
Group [VPNC\_Base\_Group]  
constructing ipsec nonce payload

702 02/05/2002 13:20:42.150 SEV=9 IKEDBG/1 RPT=8108 172.18.124.197  
Group [VPNC\_Base\_Group]  
constructing proxy ID

703 02/05/2002 13:20:42.150 SEV=7 IKEDBG/0 RPT=33279 172.18.124.197  
Group [VPNC\_Base\_Group]  
Transmitting Proxy Id:  
Remote host: 172.18.124.197 Protocol 17 Port 1701  
Local host: 172.18.124.131 Protocol 17 Port 0

707 02/05/2002 13:20:42.150 SEV=9 IKEDBG/0 RPT=33280 172.18.124.197  
Group [VPNC\_Base\_Group]  
constructing qm hash

708 02/05/2002 13:20:42.150 SEV=8 IKEDBG/0 RPT=33281 172.18.124.197  
SENDING Message (msgid=dba7daa8) with payloads :  
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total length : 136

711 02/05/2002 13:20:42.160 SEV=4 IPSEC/7 RPT=25  
IPSec ESP Tunnel Inb: invalid direction in security association

712 02/05/2002 13:20:42.160 SEV=7 IPSECDBG/7 RPT=13  
IPSEC secassoc dump (from ipsec\_esp\_input) - type 2, state 0x04, spi 6dd74451, algorithm 0, lifetype 0, lifetime1 0, lifetime2 0, src 000000f0, dst 00000000, from 00000000/ac127cc5/ac127c83, to 00000000/00000000/00000000

715 02/05/2002 13:20:42.160 SEV=6 IPSEC/7 RPT=26  
IPSec ESP Tunnel Inb: Invalid SA or pre-parsing problem!

716 02/05/2002 13:20:42.160 SEV=8 IKEDBG/0 RPT=33282 172.18.124.197  
RECEIVED Message (msgid=dba7daa8) with payloads :  
HDR + HASH (8) + NONE (0) ... total length : 48

718 02/05/2002 13:20:42.160 SEV=9 IKEDBG/0 RPT=33283 172.18.124.197  
Group [VPNC\_Base\_Group]  
processing hash

719 02/05/2002 13:20:42.160 SEV=9 IKEDBG/0 RPT=33284 172.18.124.197  
Group [VPNC\_Base\_Group]  
loading all IPSEC SAs

720 02/05/2002 13:20:42.160 SEV=9 IKEDBG/1 RPT=8109 172.18.124.197  
Group [VPNC\_Base\_Group]  
Generating Quick Mode Key!

721 02/05/2002 13:20:42.170 SEV=9 IKEDBG/1 RPT=8110 172.18.124.197  
Group [VPNC\_Base\_Group]  
Generating Quick Mode Key!

722 02/05/2002 13:20:42.170 SEV=7 IKEDBG/0 RPT=33285 172.18.124.197  
Group [VPNC\_Base\_Group]  
Loading host:  
  Dst: 172.18.124.131  
  Src: 172.18.124.197

724 02/05/2002 13:20:42.170 SEV=4 IKE/49 RPT=13 172.18.124.197  
Group [VPNC\_Base\_Group]  
Security negotiation complete for User ()  
Responder, Inbound SPI = 0x6dd74451, Outbound SPI = 0x5151839b

727 02/05/2002 13:20:42.170 SEV=9 IPSECDBG/6 RPT=60  
IPSEC key message parse - msgtype 1, len 592, vers 1, pid 00000000, seq 0, err 0  
, type 2, mode 2, state 64, label 0, pad 0, spi 5151839b, encrKeyLen 8, hashKeyL  
en 16, ivlen 8, alg 1, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, dsI  
d 0

731 02/05/2002 13:20:42.170 SEV=9 IPSECDBG/1 RPT=226  
Processing KEY\_ADD msg!

732 02/05/2002 13:20:42.170 SEV=9 IPSECDBG/1 RPT=227  
key\_msghdr2secassoc(): Enter

733 02/05/2002 13:20:42.170 SEV=7 IPSECDBG/1 RPT=228  
No USER filter configured

734 02/05/2002 13:20:42.170 SEV=9 IPSECDBG/1 RPT=229  
KeyProcessAdd: Enter

735 02/05/2002 13:20:42.170 SEV=8 IPSECDBG/1 RPT=230  
KeyProcessAdd: Adding outbound SA

736 02/05/2002 13:20:42.170 SEV=8 IPSECDBG/1 RPT=231  
KeyProcessAdd: src 172.18.124.131 mask 0.0.0.0, dst 172.18.124.197 mask 0.0.0.0

737 02/05/2002 13:20:42.170 SEV=8 IPSECDBG/1 RPT=232  
KeyProcessAdd: FilterIpsecAddIkeSa success

738 02/05/2002 13:20:42.170 SEV=9 IPSECDBG/6 RPT=61  
IPSEC key message parse - msgtype 3, len 312, vers 1, pid 00000000, seq 0, err 0  
, type 2, mode 2, state 32, label 0, pad 0, spi 6dd74451, encrKeyLen 8, hashKeyL  
en 16, ivlen 8, alg 1, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, dsI  
d 0

742 02/05/2002 13:20:42.170 SEV=9 IPSECDBG/1 RPT=233  
Processing KEY\_UPDATE msg!

743 02/05/2002 13:20:42.170 SEV=9 IPSECDBG/1 RPT=234  
Update inbound SA addresses

744 02/05/2002 13:20:42.170 SEV=9 IPSECDBG/1 RPT=235  
key\_msghdr2secassoc(): Enter

745 02/05/2002 13:20:42.170 SEV=7 IPSECDBG/1 RPT=236  
No USER filter configured

746 02/05/2002 13:20:42.170 SEV=9 IPSECDBG/1 RPT=237  
KeyProcessUpdate: Enter

747 02/05/2002 13:20:42.170 SEV=8 IPSECDBG/1 RPT=238  
KeyProcessUpdate: success

748 02/05/2002 13:20:42.170 SEV=8 IKEDBG/7 RPT=13  
IKE got a KEY\_ADD msg for SA: SPI = 0x5151839b

749 02/05/2002 13:20:42.170 SEV=8 IKEDBG/0 RPT=33286  
pitcher: rcv KEY\_UPDATE, spi 0x6dd74451

750 02/05/2002 13:20:42.170 SEV=4 IKE/120 RPT=13 172.18.124.197  
Group [VPNC\_Base\_Group]  
PHASE 2 COMPLETED (msgid=dba7daa8)

751 02/05/2002 13:20:42.940 SEV=7 IPSECDBG/1 RPT=239  
IPSec Inbound SA has received data!

752 02/05/2002 13:20:42.940 SEV=8 IKEDBG/0 RPT=33287  
pitcher: recv KEY\_SA\_ACTIVE spi 0x6dd74451

753 02/05/2002 13:20:42.940 SEV=8 IKEDBG/0 RPT=33288  
KEY\_SA\_ACTIVE no old rekey centry found with new spi 0x6dd74451, mess\_id 0x0

754 02/05/2002 13:20:42.940 SEV=4 L2TP/57 RPT=33  
Tunnel to peer 172.18.124.197 established

755 02/05/2002 13:20:42.940 SEV=4 L2TP/53 RPT=33 172.18.124.197  
Session started on tunnel 172.18.124.197

756 02/05/2002 13:20:42.960 SEV=8 AUTHDBG/1 RPT=1197  
AUTH\_Open() returns 172

757 02/05/2002 13:20:42.960 SEV=7 AUTH/12 RPT=1197  
Authentication session opened: handle = 172

758 02/05/2002 13:20:42.960 SEV=8 AUTHDBG/9 RPT=67  
AUTH\_GetChallenge(172, 8ad, 8, 42a25c)

759 02/05/2002 13:20:42.960 SEV=8 AUTHDBG/3 RPT=1230  
AUTH\_PutAttrTable(172, 727bec)

760 02/05/2002 13:20:42.960 SEV=8 AUTHDBG/9 RPT=68  
AUTH\_GetChallenge(172, 8ad, 8, 42a25c)

761 02/05/2002 13:20:42.960 SEV=8 AUTHDBG/59 RPT=1230  
AUTH\_BindServer(9b181d8, 0, 0)

762 02/05/2002 13:20:42.960 SEV=9 AUTHDBG/69 RPT=1230  
Auth Server 16b7fa0 has been bound to ACB 9b181d8, sessions = 1

763 02/05/2002 13:20:42.960 SEV=8 AUTHDBG/3 RPT=1231  
AUTH\_PutAttrTable(172, 727bec)

764 02/05/2002 13:20:42.960 SEV=8 AUTHDBG/5 RPT=34  
AUTH\_Authenticate(172, 8ad, 429df8)

765 02/05/2002 13:20:42.960 SEV=8 AUTHDBG/59 RPT=1231  
AUTH\_BindServer(9b181d8, 0, 0)

766 02/05/2002 13:20:42.960 SEV=9 AUTHDBG/69 RPT=1231  
Auth Server 16b7fa0 has been bound to ACB 9b181d8, sessions = 1

767 02/05/2002 13:20:42.960 SEV=8 AUTHDBG/65 RPT=1197  
AUTH\_CreateTimer(9b181d8, 0, 0)

768 02/05/2002 13:20:42.960 SEV=9 AUTHDBG/72 RPT=1197

Reply timer created: handle = 15410018

769 02/05/2002 13:20:42.960 SEV=8 AUTHDBG/61 RPT=1197  
AUTH\_BuildMsg(9b181d8, 0, 0)

770 02/05/2002 13:20:42.960 SEV=8 AUTHDBG/64 RPT=1197  
AUTH\_StartTimer(9b181d8, 0, 0)

771 02/05/2002 13:20:42.960 SEV=9 AUTHDBG/73 RPT=1197  
Reply timer started: handle = 15410018, timestamp = 34950652, timeout = 30000

772 02/05/2002 13:20:42.960 SEV=8 AUTHDBG/62 RPT=1197  
AUTH\_SndRequest(9b181d8, 0, 0)

773 02/05/2002 13:20:42.960 SEV=8 AUTHDBG/50 RPT=2392  
IntDB\_Decode(62f61e0, 161)

774 02/05/2002 13:20:42.960 SEV=8 AUTHDBG/47 RPT=2393  
IntDB\_Xmt(9b181d8)

775 02/05/2002 13:20:42.960 SEV=9 AUTHDBG/71 RPT=1197  
xmit\_cnt = 1

776 02/05/2002 13:20:42.960 SEV=8 AUTHDBG/47 RPT=2394  
IntDB\_Xmt(9b181d8)

777 02/05/2002 13:20:43.060 SEV=8 AUTHDBG/49 RPT=1196  
IntDB\_Match(9b181d8, 62f6428)

778 02/05/2002 13:20:43.060 SEV=8 AUTHDBG/63 RPT=1196  
AUTH\_RcvReply(9b181d8, 0, 0)

779 02/05/2002 13:20:43.060 SEV=8 AUTHDBG/50 RPT=2393  
IntDB\_Decode(62f6428, 179)

780 02/05/2002 13:20:43.060 SEV=8 AUTHDBG/48 RPT=1196  
IntDB\_Rcv(9b181d8)

781 02/05/2002 13:20:43.060 SEV=8 AUTHDBG/66 RPT=1197  
AUTH\_DeleteTimer(9b181d8, 0, 0)

782 02/05/2002 13:20:43.060 SEV=9 AUTHDBG/74 RPT=1197  
Reply timer stopped: handle = 15410018, timestamp = 34950662

783 02/05/2002 13:20:43.060 SEV=8 AUTHDBG/58 RPT=1196  
AUTH\_Callback(9b181d8, 0, 0)

784 02/05/2002 13:20:43.060 SEV=6 AUTH/4 RPT=15 172.18.124.197  
Authentication successful: handle = 172, server = Internal, user = L2TP\_user

785 02/05/2002 13:20:43.060 SEV=5 PPP/8 RPT=15 172.18.124.197  
User [L2TP\_user]  
Authenticated successfully with MSCHAP-V1

786 02/05/2002 13:20:43.060 SEV=8 AUTHDBG/60 RPT=1197  
AUTH\_UnbindServer(9b181d8, 0, 0)

787 02/05/2002 13:20:43.060 SEV=9 AUTHDBG/70 RPT=1197  
Auth Server 16b7fa0 has been unbound from ACB 9b181d8, sessions = 0

788 02/05/2002 13:20:43.060 SEV=8 AUTHDBG/4 RPT=1177  
AUTH\_GetAttrTable(172, 72796c)

789 02/05/2002 13:20:43.060 SEV=8 AUTHDBG/2 RPT=1197  
AUTH\_Close(172)

790 02/05/2002 13:20:43.060 SEV=8 AUTHDBG/10 RPT=1197  
AUTH\_Int\_FreeAuthCB(9b181d8)

791 02/05/2002 13:20:43.060 SEV=7 AUTH/13 RPT=1197  
Authentication session closed: handle = 172

792 02/05/2002 13:20:44.950 SEV=4 AUTH/22 RPT=35  
User L2TP\_user connected

---

## Related Information

- **Technical Support – Cisco Systems**
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Oct 23, 2009

Document ID: 19260

---