IPSec with VPN client (Static/Dynamic assigned IP address) to VPN 3000 Concentrator Configuration Example

Document ID: 60141

Contents

Introduction
Prerequisites
Requirements
Components Used
Network Diagram
Conventions
Configure the VPN 3000 Concentrator
Assign a Static IP Address to a User
Configure the VPN Client
Verify
Troubleshoot
What Can Go Wrong
VPN Client
VPN Concentrator
VPN 3000 Concentrator − Good Sample Debug

Related Information

Introduction

This sample configuration demonstrates how to form an IPsec tunnel from a PC that runs the Cisco VPN Client (4.x and later) (Static/Dynamic assigned IP address) to a Cisco VPN 3000 Concentrator in order to enable the user to securely access the network inside the VPN Concentrator.

Refer to Using Cisco Secure ACS for Windows with the VPN 3000 Concentrator – IPSec in order to learn more about the same scenario with RADIUS Authentication using Cisco ACS. Refer to Configuring the Cisco VPN 3000 Concentrator with MS RADIUS in order to know more about the same scenario with MS–RADIUS Authentication.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco VPN 3030 Concentrator version 4.1.7.A
- Cisco VPN Client version 4.x and later
Note: This configuration was recently re-tested using Cisco VPN Concentrator version 4.7.2.H.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Network Diagram

This document uses this network setup:

![Network Diagram]

Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses that were used in a lab environment.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure the VPN 3000 Concentrator

Complete these steps in order to configure the VPN 3000 Concentrator.

Note: Due to space limitations, some screen captures show only partial screens.

1. Connect to the VPN Concentrator console port and verify that there are IP addresses assigned to the Private (inside) and Public (outside) interfaces.

   In addition, verify that there is a default gateway assigned so the VPN Concentrator can forward the packets for the destinations that it does not know about to the default gateway (normally the Internet Gateway Router):
This table shows the current IP addresses.
5) Tunneling and Security
6) Back

Config → 1

This table shows current IP addresses.

<table>
<thead>
<tr>
<th>Intf</th>
<th>Status</th>
<th>IP Address/Subnet Mask</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ether1-Pr1</td>
<td>UP</td>
<td>10.1.1.1/255.255.255.0</td>
<td>00.90.04.00.06.99</td>
</tr>
<tr>
<td>Ether2-Pub</td>
<td>UP</td>
<td>172.18.124.133/255.255.255.0</td>
<td>00.90.04.00.06.95</td>
</tr>
<tr>
<td>Ether3-Ext</td>
<td>Not Configured</td>
<td>0.0.0.0/0.0.0.0</td>
<td></td>
</tr>
</tbody>
</table>

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
2. Make sure that you choose the **Public** filter option for the Public interface.
Point a browser to the inside interface of the VPN Concentrator and choose Configuration > System > Address Management > Address Pools > Add in order to assign an available range of IP addresses.

Specify a range of IP addresses that do not conflict with any other devices on the inside network:

Note: These screen captures show outside-public interface management because filters were added to allow this in a lab setting only.
4. Choose **Configuration > System > Address Management > Assignment**, check the **Use Address Pools** box, and click **Apply** in order to tell the VPN Concentrator to use the pool.

5. Choose **Configuration > User Management > Groups > Add Group** in order to configure an IPsec group for the users and define a group name and password.

   This example uses `group="ipsecgroup"` with `password/verify="cisco123"`:

6. On the **General** tab of the group, verify that **IPSec** is selected.
7. On the IPSec tab of the group, verify that authentication is set to **Internal**. Choose **Configuration > User Management > Groups > Modify Group** and select **ipsecgroup** from the Current Groups option in order to do this.

8. Choose **Configuration > User Management > Users > Add**, and add a user to the previously defined group.

   In this example, the user is "ipsecuser" with password "xyz12345" in group "ipsecgroup":
Assign a Static IP Address to a User

In order to assign a static IP address for the remote VPN user every time they connect to the VPN 3000 Series Concentrator, choose Configuration > User Management > Users > Modify ipsecuser2 > identity. In this configuration for the user (ipsecuser2), the static IP address 10.2.2.1/24 is assigned every time the user connects.

Note: Be sure to go to Configuration > System > Address Management > Assignment in order to ensure that the VPN Concentrator provisions the assigned IP address. Check Use Address from Authentication Server to assign IP addresses retrieved from an authentication server on a per−user basis. The IP address and subnet mask entered on the Identity Parameters tab on the User Management > Users > Add or Modify window is considered to be in the internal authentication server.
Configure the VPN Client

Complete these steps in order to configure the VPN Client.

1. Click **New** in order to create a new connection entry.

2. Name the connection, enter the IP address of the public interface of the VPN Concentrator and provide the Group credentials. In this case, the Name is **ipsecgroup** and the Password is **cisco123**. Click **Save** when finished.
3. Select the connection entry from the list and click **Connect**. When prompted for the username/password, enter your username/password.

**Verify**

There is currently no verification procedure available for this configuration.

**Troubleshoot**

These sections provide information you can use to troubleshoot your configuration.
The Output Interpreter Tool (registered customers only) (OIT) supports certain show commands. Use the OIT to view an analysis of show command output.

**Note:** Refer to Important Information on Debug Commands before you issue debug commands.

**What Can Go Wrong**

These are potential errors that can occur. See the VPN Client and VPN Concentrator sections for the resolutions to these errors.

- A user receives the message Unable to negotiate IPSec or host did not respond.
  
  The VPN 3000 debug shows:

  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

**Usual cause:** The user attempts to connect with a group name that is not configured.

- A user cannot connect and the VPN 3000 debug shows:

  Filter missing on interface 2, IKE data from Peer x.x.x.x dropped

**Usual cause:** The filter is missing from the public interface. It is usually the "public" filter (but can be the private filter; "none" is not valid). Choose Configuration > Interfaces > Ethernet 2 > Filter and make the filter "public" or another value (that is, not "none"). See the configuration section of this document for more information on how to configure the filter.

- A user cannot connect and sees Unable to negotiate IPSec or host did not respond.
  
  The VPN 3000 debug shows:

  Terminating connection attempt: IPSEC not permitted for group >group<

**Usual cause:** IPsec is not selected on the group. Choose Configuration > User Management > Groups > <group> > Modify > General and verify that IPSec is selected under Tunneling Protocols.

- A user cannot connect after numerous tries and sees User Authentication Failed.
  
  The VPN 3000 debug shows:

  Authentication rejected: Reason = User was not found handle = 14, server = Internal, user = <user>

**Usual cause:** The user does not exist in the user database. Make sure that you enter the correct username when the user authentication window displays.

- Users cannot connect and the VPN 3000 debug shows:

  Filter missing on interface 0, IKE data from Peer x.x.x.x dropped

**Usual cause:** The default route is missing. Make sure there is a default route in the configuration. Choose Configuration > System > IP routing > Default Gateway and specify the default gateway.

- A user cannot connect and sees Your IPSec connection has been terminated by the remote peer.

  The VPN 3000 debug shows:
User [ <user> ]
IKE rcv'd FAILED IP Addr status!

**Usual cause:** There is no option checked to give the VPN Client an IP address. Choose **Configuration > System > Address Management > Address Assignment** and select an option.

- A user cannot connect and sees User authentication failed.

The VPN 3000 debug shows:

```
The calculated HASH doesn't match the received value
```

**Usual cause:** The group password on the VPN Client is different than the password configured on the VPN Concentrator. Check the password on both the VPN Client and the Concentrator.

- You have set up the VPN pool for the resources behind the VPN Concentrator. You are able to access the resources but cannot ping them.

**Usual cause:** There is a PIX behind the VPN Concentrator which blocks the ICMP packets. Login to that PIX and apply an `access-list` to enable ICMP packets.

- There are no VPN Concentrator debugs and all or some users cannot connect.

The default VPN Concentrator Public filter contains rules to allow this traffic:

- Protocol = UDP, port = 500
- Protocol = UDP, port = 10000
- Protocol = ESP
- Protocol = AH

If the filters of the VPN Concentrator allow this traffic, then a device between the VPN Client and the VPN Concentrator can be blocking some of these ports (perhaps a firewall). In order to verify, try to connect to the VPN Concentrator from the network immediately outside the VPN Concentrator. If that works, a device between the VPN Client PC and VPN Concentrator is blocking the traffic.

- A user cannot connect and sees these logs:

```
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
```

**Usual cause:** An incorrectly defined group name or password. Recreate the new group name and password on the VPN 3000 Concentrator for the VPN Client.

- A user can ping or Telnet to a host behind the VPN Concentrator, but the user cannot use the Remote Desktop 9RDP) or similar applications.

**Usual cause:** The Public filter is not enabled on the Public interface. See step 2 in the Configure the VPN 3000 Concentrator section of this document.

- A user can connect, but no traffic is passed through the VPN tunnel.

**Usual cause:** NAT–Transparency is not enabled. In many cases the VPN Client is behind a PAT device. PAT relies on TCP and UDP port numbers to conserve address space. But ESP, which encapsulates VPN traffic, is a separate protocol from TCP or UDP. This means that many PAT devices cannot handle ESP traffic. NAT–T encapsulates ESP packets in UDP packets allowing them to pass easily through a PAT device. Thus, in order to allow ESP traffic to flow through a PAT device, you need to enable NAT–T on the concentrator. Refer to Configuring NAT Transparent Mode for IPSec on the VPN 3000 Concentrator for more information.
VPN Client

Choose Start > Programs > Cisco Systems VPN 3000 Client > Log Viewer in order to bring up the log viewer.

VPN Concentrator

Choose Configuration > System > Events > Classes in order to turn on this debug if there are event connection failures:

- AUTH – Severity to log 1–13
- AUTHDBG – Severity to log 1–13
- IKE – Severity to log 1–13
- IKEDBG – Severity to log 1–13
- IPSEC – Severity to log 1–13
- IPSECDBG – Severity to log 1–13

Note: If necessary, AUTHDECODE, IKEDECODE, IPSECDECODE can be added later.

Refer to Troubleshooting Connection Problems on the VPN 3000 Concentrator for additional troubleshooting details.
Choose Monitoring > Filterable Event Log in order to view the log.

**VPN 3000 Concentrator – Good Sample Debug**

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_BldMsg(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 Altiaga 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 (1)
3 + 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)
AUTH_DeleteTimer(9b1544c, 0, 0)

Reply timer stopped: handle = 3B5001A, timestamp = 10086177

AUTH_Callback(9b1544c, 0, 0)

Authentication successful: handle = 137, server = Internal, group = ipsecgroup

AUTH_PutAttrTable(137, 1861c60)

AUTH_UnbindServer(9b1544c, 0, 0)

Auth Server 16b3fa0 has been unbound from ACB 9b1544c, sessions = 0

AUTH_BindServer(9b1544c, 0, 0)

Auth Server 16b3fa0 has been bound to ACB 9b1544c, sessions = 1

AUTH_CreateTimer(9b1544c, 0, 0)

Reply timer created: handle = 3B6001A

AUTH_BuildMsg(9b1544c, 0, 0)

AUTH_StartTimer(9b1544c, 0, 0)

Reply timer started: handle = 3B6001A, timestamp = 10086177, timeout = 30000

AUTH_SndRequest(9b1544c, 0, 0)

IntDB_Decode(2ec39ec, 44)

IntDB_Xmt(9b1544c)

xmit_cnt = 1

IntDB_Match(9b1544c, 2ec5350)

AUTH_RcvReply(9b1544c, 0, 0)

IntDB_Decode(2ec5350, 44)
AUTH_Recv(9b1544c)

AUTH_DeleteTimer(9b1544c, 0, 0)

Reply timer stopped: handle = 3B6001A, timestamp = 10086187

AUTH_Callback(9b1544c, 0, 0)

Authentication successful: handle = 137, server = Internal, group = ipsecgroup

AUTH_GetAttrTable(137, 729c04)

AUTH_GetAttrTable(137, 728c4c)

Group [ipsecgroup] User [ipsecuser]
Authentication configured for Internal

AUTH_Close(137)

User (ipsecuser) authenticated.

Group [ipsecgroup] User [ipsecuser]
constructing blank hash

Group [ipsecgroup] User [ipsecuser]
constructing qm hash

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

AUTH_UnbindServer(9b1544c, 0, 0)

Auth Server 16b3fa0 has been unbound from ACB 9b1544c, sessions = 0

AUTH_Int_FreeAuthCB(9b1544c)

Authentication session closed: handle = 137

RECEIVED Message (msgid=4cc78f4e) with payloads:
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 56

process_attr(): Enter!

Processing cfg ACK attributes
RECEIVED Message (msgid=38a7c320) with payloads:
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 154

process_attr(): Enter!

Processing cfg Request attributes

MODE_CFG: Received request for IPV4 address!

MODE_CFG: Received request for IPV4 net mask!

MODE_CFG: Received request for DNS server address!

MODE_CFG: Received request for WINS server address!

Received unsupported transaction mode attribute: 5

MODE_CFG: Received request for Application Version!

MODE_CFG: Received request for Banner!

MODE_CFG: Received request for Save PW setting!

MODE_CFG: Received request for Default Domain Name!

MODE_CFG: Received request for Split Tunnel List!

MODE_CFG: Received request for PFS setting!

MODE_CFG: Received request for FWTYPE!

MODE_CFG: Received request for UDP Port!

Obtained IP addr (10.1.1.100) prior to initiating Mode Cfg (XAuth enabled)

constructing blank hash

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
Group [ipsecgroup] User [ipsecuser] constructing qm hash

Group [ipsecgroup] User [ipsecuser] sending notify message

Group [ipsecgroup] User [ipsecuser] constructing blank hash

Group [ipsecgroup] User [ipsecuser] constructing qm hash

Group [ipsecgroup] User [ipsecuser] processing hash

Group [ipsecgroup] User [ipsecuser] processing SA payload

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, hashKeylen 0, ivlen 0, alg 0, hmacAlg 0, lifetime 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 constucting 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, lifetime 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!
key_hdr2secassoc(): Enter

No USER filter configured

KeyProcessAdd: Enter

KeyProcessAdd: Adding outbound SA

KeyProcessAdd: src 172.18.124.133 mask 0.0.0.0, dst 10.1.1.100 mask 0.0.0.0

KeyProcessAdd: FilterIpsecAddIkeSa success

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

Processing KEY_UPDATE msg!

Update inbound SA addresses

key_hdr2secassoc(): Enter

No USER filter configured

KeyProcessUpdate: Enter

KeyProcessUpdate: success

IKE got a KEY_ADD msg for SA: SPI = 0x8104887e

pitcher: rcv KEY_UPDATE, spi 0x3dd6c4a4

Group [ipsecgroup] User [ipsecuser]

PHASE 2 COMPLETED (msgid=472c326b)

Group [ipsecgroup] User [ipsecuser]

Group [ipsecgroup] User [ipsecuser]

Group [ipsecgroup] User [ipsecuser]

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: FilterIpsecAddIkeSa 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=8 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)

Related Information

- Cisco VPN 3000 Series Concentrator Support Page
- Cisco VPN 3000 Series Client Support Page
- IPsec Negotiation/IKE Protocols
- Technical Support & Documentation – Cisco Systems