

IPSec Between Two Cisco VPN 3000 Concentrators with Overlapping Private Networks

Document ID: 26286

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Network Diagram
- Conventions

Configure the VPN 3000 Concentrator A

Configure Cisco VPN 3000 Concentrator B

Verify

- Verify the VPN 3000 Concentrator A Configuration
- Verify the VPN 3000 Concentrator B Configuration

Troubleshoot

- Troubleshoot the VPN 3000 Concentrator A Configuration
- Troubleshoot the VPN 3000 Concentrator B Configuration

Related Information

Introduction

This document describes how to configure the Cisco VPN 3000 Concentrator in a site-to-site IPSec VPN with overlapping network addresses behind the VPN gateways. The enhanced Network Address Translation (NAT) feature introduced in VPN 3000 Concentrator version 3.6 was used in this example to translate the overlapping networks on each side of the IPSec VPN tunnel to change the addresses in the non-overlapping range.

Prerequisites

Requirements

Before attempting this configuration, ensure that you meet these requirements:

- Knowledge of the Cisco VPN 3000 Concentrator
- Knowledge of IPSec VPN

Components Used

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

- Cisco VPN 3000 Concentrator version 3.6 or later

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:



Both private LAN 1 and private LAN 2 have an IP subnet of 14.38.100.0/24. This simulates the overlapping address space behind each side of the IPsec tunnel.

In this example, the VPN 3000 Concentrator performs a bi-directional NAT translation so the two private LANs can communicate over the IPsec tunnel. The translation means that private LAN 1 "sees" private LAN 2 as 14.38.200.0/24 through the IPsec tunnel, and private LAN 2 "sees" Private LAN 1 as 14.38.80.0/24 through the IPsec tunnel.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configure the VPN 3000 Concentrator A

Use the following procedure to configure the VPN 3000 Concentrator A.

1. Configure the LAN-to-LAN session proposals and parameters for LAN-to-LAN on VPN Concentrator A under **Configuration > System > Tunneling Protocols > IPsec > LAN-to-LAN > Modify**.
 - ◆ Under the Local Network section, enter **14.38.80.0/24** in the IP Address field.
 - ◆ Under the Remote Network section, enter **14.38.200.0/24** in the IP Address field.Click **Apply** when you have finished.

Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN | Modify

Modify an IPSec LAN-to-LAN connection.

Name Enter the name for this LAN-to-LAN connection.

Interface Select the interface for this LAN-to-LAN connection.

Peer Enter the IP address of the remote peer for this LAN-to-LAN connection.

Digital Certificate Select the digital certificate to use.

Certificate Entire certificate chain
 Transmission Identity certificate only
 Choose how to send the digital certificate to the IKE peer.

Preshared Key Enter the preshared key for this LAN-to-LAN connection.

Authentication Specify the packet authentication mechanism to use.

Encryption Specify the encryption mechanism to use.

IKE Proposal Select the IKE Proposal to use for this LAN-to-LAN connection.

Filter Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.

IPSec NAT-T Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency.

Bandwidth Policy Choose the bandwidth policy to apply to this LAN-to-LAN connection.

Routing Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.

Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

Network List Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.

IP Address Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

Wildcard Mask

Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

Network List Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.

IP Address Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

Wildcard Mask

2. Create the static NAT for private LAN 2 destined for private LAN 1 by going to **Configuration > Policy Management > Traffic Management > NAT > LAN-to-LAN Rules > Modify**.

In the IP Address row, enter **14.38.100.0/24** in the Source Network field, **14.38.80.0/24** in the Translated Network field, **14.38.200.0/24** in the Remote Network field, and click **Apply**.

Configuration | Policy Management | Traffic Management | NAT | LAN-to-LAN Rules | Modify

Modify a LAN-to-LAN NAT rule.

Static Static: maps source IP addresses to translated IP addresses on a one-to-one basis. Static mappings apply to both inbound and outbound traffic.

NAT Type Dynamic Dynamic: maps source IP addresses to one of a pool of available translated IP addresses. Dynamic mappings apply to outbound traffic only.

PAT PAT: Dynamic mapping with Port Address Translation. PAT applies to outbound traffic only.

Source Network: specifies the source IP address and wildcard mask to be translated.

Translated Network: specifies the translated IP address and wildcard mask for the Local Network. It is the local address of the LAN-to-LAN connection.

Remote Network: specifies the destination IP address and wildcard mask for which this rule applies. To allow any remote network, set IP address/wildcard mask to 0.0.0.0/255.255.255.255. It is the remote address of the LAN-to-LAN connection.

Source Network	Translated Network	Remote Network
IP Address <input type="text" value="14.38.100.0"/>	: <input type="text" value="14.38.80.0"/>	-> <input type="text" value="14.38.200.0"/>
Wildcard Mask <input type="text" value="0.0.0.255"/>	: <input type="text" value="0.0.0.255"/>	-> <input type="text" value="0.0.0.255"/>

3. Select **Configuration > Policy Management > Traffic Management > NAT > Enable** and select **Check to enable NAT rules on LAN-to-LAN tunnels**. Click **Apply**.

Configuration | Policy Management | Traffic Management | NAT | Enable

This section lets you enable system-wide NAT rules.

Interface NAT Rules Enabled Check to enable NAT rules on interfaces.

LAN-to-LAN Tunnel NAT Rule Enabled Check to enable NAT rules on LAN-to-LAN tunnels.

Configure Cisco VPN 3000 Concentrator B

Use the following procedure to configure Cisco VPN 3000 Concentrator B.

1. Configure the LAN-to-LAN sessions proposals and parameters for LAN-to-LAN on VPN Concentrator B by selecting **Configuration > System > Tunneling Protocols > IPSec > LAN-to-LAN > Modify**.

- ◆ Under the Local Network section, enter **14.38.200.0/24** in the IP Address field.
- ◆ Under the Remote Network section, enter **14.38.80.0/24** in the IP Address field.

Click **Apply** when you have finished.

The screenshot shows the configuration page for modifying an IPSec LAN-to-LAN connection. The page is titled "Modify an IPSec LAN-to-LAN connection." and contains several sections for configuration:

- General Settings:** Name (FTP NAT TUNNEL), Interface (Ethernet 2 (Public) (172.18.124.131)), Peer (172.18.124.132), Digital Certificate (None (Use Preshared Keys)), Certificate (Entire certificate chain), Transmission (Identity certificate only), Preshared Key (ypvpa), Authentication (ESP:MD5+HMAC-128), Encryption (3DES-168), IKE Proposal (IKE-3DES-MD6), Filter (None), IPSec NAT-T (unchecked), Bandwidth Policy (None), and Routing (None).
- Local Network:** Network List (Use IP Address/Wildcard mask below), IP Address (14.38.200.0), and Wildcard Mask (0.0.0.255). Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.x addresses.
- Remote Network:** Network List (Use IP Address/Wildcard mask below), IP Address (14.38.80.0), and Wildcard Mask (0.0.0.255). Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.x addresses.

Buttons for "Apply" and "Cancel" are located at the bottom left of the form.

2. Create the static NAT for private LAN 1 destined for private LAN 2 by selecting **Configuration > Policy Management > Traffic Management > NAT > LAN-to-LAN Rules > Modify**.

In the IP Address row, enter **14.38.100.0/24** in the Source Network field, **14.38.200.0/24** in the Translated Network field, **14.38.80.0/24** in the Remote Network field, and click **Apply**.

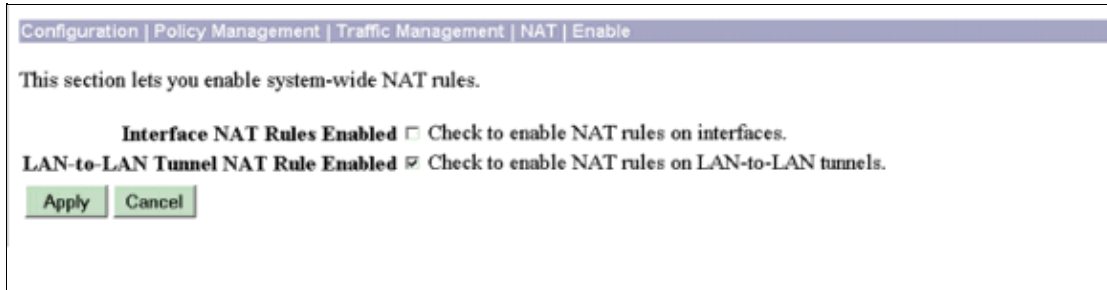
The screenshot shows the configuration page for modifying a LAN-to-LAN NAT rule. The page is titled "Modify a LAN-to-LAN NAT rule." and contains several sections for configuration:

- NAT Type:** Static (selected), Dynamic, and PAT.
- Source Network:** specifies the source IP address and wildcard mask to be translated.
- Translated Network:** specifies the translated IP address and wildcard mask for the Local Network. It is the local address of the LAN-to-LAN connection.
- Remote Network:** specifies the destination IP address and wildcard mask for which this rule applies. To allow any remote network, set IP address/wildcard mask to 0.0.0.0/255.255.255.255. It is the remote address of the LAN-to-LAN connection.

	Source Network	Translated Network	Remote Network
IP Address	14.38.100.0	14.38.200.0	14.38.80.0
Wildcard Mask	0.0.0.255	0.0.0.255	0.0.0.255

Buttons for "Apply" and "Cancel" are located at the bottom left of the form.

3. Select **Configuration > Policy Management > Traffic Management > NAT > Enable** and select **Check to enable NAT rules on LAN-to-LAN tunnels**. Click **Apply**.



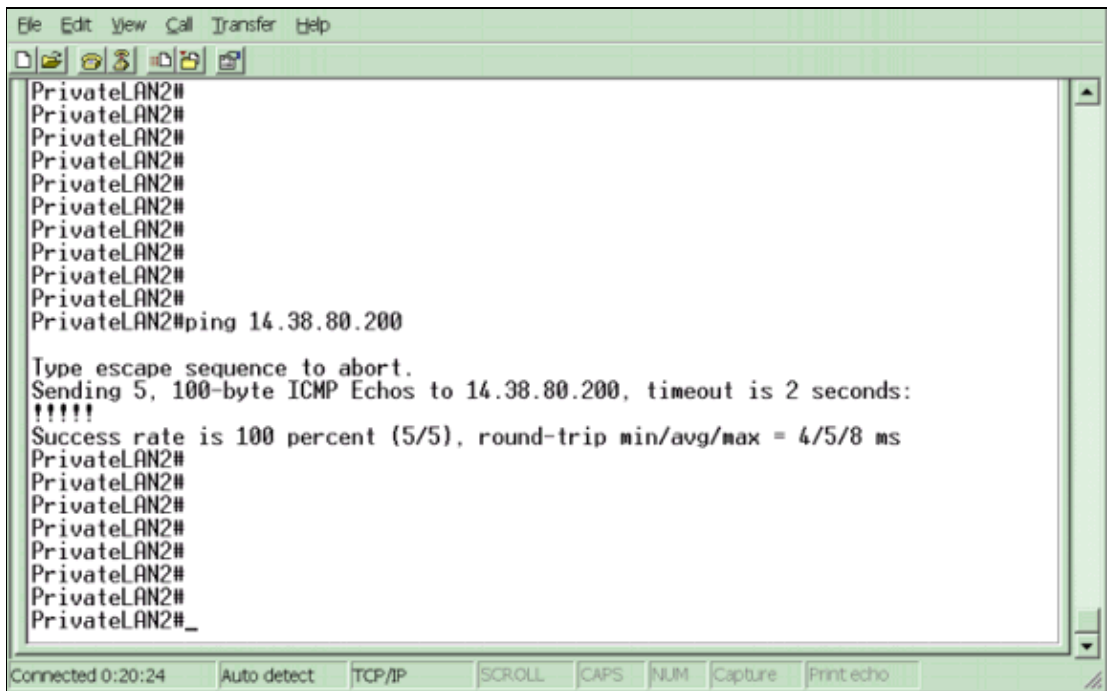
Verify

Verify the VPN 3000 Concentrator A Configuration

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- To initiate the tunnel, send a ping from a private LAN 2 device (14.38.200.10) to an IP address on private LAN 1 (14.38.80.200).



- Confirm that the Internet Key Exchange (IKE) and IPsec sessions show private LAN 1 and private LAN 2 with NAT by selecting **Administration > Administer Sessions > Detail**.

Administration Administer Sessions Detail		Wednesday, 07 August 2002 12:49:04					
Back to Sessions							
Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
VPN TUNNEL	172.18.124.131	IPSec/LAN-to-LAN	3DES-168	Aug 06 13:20:24	23:28:40	1456	1040
IKE Sessions: 1							
IPSec Sessions: 1							
IKE Session							
Session ID 1				Encryption Algorithm 3DES-168			
Hashing Algorithm MD5				Diffie-Hellman Group Group 2 (1024-bit)			
Authentication Mode Pre-Shared Keys				IKE Negotiation Mode Main			
Rekey Time Interval 86400 seconds							
IPSec Session							
Session ID 2				Remote Address 14.38.200.0/0.0.0.255			
Local Address 14.38.80.0/0.0.0.255				Encryption Algorithm 3DES-168			
Hashing Algorithm MD5				SEP 1			
Encapsulation Mode Tunnel				Rekey Time Interval 28800 seconds			
Bytes Received 1040				Bytes Transmitted 1456			

Verify the VPN 3000 Concentrator B Configuration

This section provides information you can use to confirm your configuration is working properly. For information on setting up and reviewing logs when troubleshooting connection problems with VPN 3000 Concentrator, refer to Troubleshooting Connection Problems on the VPN 3000 Concentrator.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only), which allows you to view an analysis of **show** command output.

Confirm that the IKE and IPSec sessions show the private LAN 2 and private LAN 1 with the NAT by selecting **Administration > Administer Sessions > Detail**.

Administration Administer Sessions Detail		Friday, 09 August 2002 12:36:39					
Back to Sessions							
Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
RTP NAT TUNNEL	172.18.124.132	IPSec/LAN-to-LAN	3DES-168	Aug 08 13:17:22	23:19:15	1040	1456
IKE Sessions: 1							
IPSec Sessions: 1							
IKE Session							
Session ID 1				Encryption Algorithm 3DES-168			
Hashing Algorithm MD5				Diffie-Hellman Group Group 2 (1024-bit)			
Authentication Mode Pre-Shared Keys				IKE Negotiation Mode Main			
Rekey Time Interval 86400 seconds							
IPSec Session							
Session ID 2				Remote Address 14.38.200.0/0.0.0.255			
Local Address 14.38.80.0/0.0.0.255				Encryption Algorithm 3DES-168			
Hashing Algorithm MD5				SEP 1			
Encapsulation Mode Tunnel				Rekey Time Interval 28800 seconds			
Bytes Received 1456				Bytes Transmitted 1040			

Troubleshoot

Troubleshoot the VPN 3000 Concentrator A Configuration

On the VPN Concentrator, turn on logging, select **Configuration > System > Events > Classes > Modify**. The following options are available:

- IKE
- IKEDBG
- IKEDECODE
- IPSEC

- IPSECDBG
- IPSECDECODE
- Severity to Log = 1–13
- Severity to Console = 1–3

You can retrieve the event log by selecting **Monitoring > Event Log**.

For additional information setting up and reviewing logs when troubleshooting connection problems with VPN 3000 Concentrator, refer to Troubleshooting Connection Problems on the VPN 3000 Concentrator.

```

1 08/09/2002 13:14:22.690 SEV=8 IKEDBG/0 RPT=52040 172.18.124.132
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 108

3 08/09/2002 13:14:22.690 SEV=9 IKEDBG/0 RPT=52041 172.18.124.132
processing SA payload

4 08/09/2002 13:14:22.690 SEV=8 IKEDBG/0 RPT=52042
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class Auth Method:
    Rcv'd: Preshared Key
    Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

10 08/09/2002 13:14:22.690 SEV=7 IKEDBG/0 RPT=52043 172.18.124.132
Oakley proposal is acceptable

11 08/09/2002 13:14:22.690 SEV=9 IKEDBG/47 RPT=28 172.18.124.132
processing VID payload

12 08/09/2002 13:14:22.690 SEV=9 IKEDBG/49 RPT=24 172.18.124.132
Received Fragmentation VID

13 08/09/2002 13:14:22.690 SEV=5 IKEDBG/64 RPT=6 172.18.124.132
IKE Peer included IKE fragmentation capability flags:
Main Mode:          True
Aggressive Mode:   True

15 08/09/2002 13:14:22.690 SEV=9 IKEDBG/0 RPT=52044 172.18.124.132
processing IKE SA

16 08/09/2002 13:14:22.690 SEV=8 IKEDBG/0 RPT=52045
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class Auth Method:
    Rcv'd: Preshared Key
    Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

22 08/09/2002 13:14:22.690 SEV=7 IKEDBG/28 RPT=5 172.18.124.132
IKE SA Proposal # 1, Transform # 1 acceptable
Matches global IKE entry # 2

```

23 08/09/2002 13:14:22.690 SEV=9 IKEDBG/0 RPT=52046 172.18.124.132
constructing ISA_SA for isakmp

24 08/09/2002 13:14:22.690 SEV=9 IKEDBG/46 RPT=26 172.18.124.132
constructing Fragmentation VID + extended capabilities payload

25 08/09/2002 13:14:22.690 SEV=8 IKEDBG/0 RPT=52047 172.18.124.132
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) ... total length : 108

27 08/09/2002 13:14:22.700 SEV=8 IKEDBG/0 RPT=52048 172.18.124.132
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13)
) + NONE (0) ... total length : 256

30 08/09/2002 13:14:22.700 SEV=8 IKEDBG/0 RPT=52049 172.18.124.132
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13)
) + NONE (0) ... total length : 256

33 08/09/2002 13:14:22.700 SEV=9 IKEDBG/0 RPT=52050 172.18.124.132
processing ke payload

34 08/09/2002 13:14:22.700 SEV=9 IKEDBG/0 RPT=52051 172.18.124.132
processing ISA_KE

35 08/09/2002 13:14:22.700 SEV=9 IKEDBG/1 RPT=83 172.18.124.132
processing nonce payload

36 08/09/2002 13:14:22.700 SEV=9 IKEDBG/47 RPT=29 172.18.124.132
processing VID payload

37 08/09/2002 13:14:22.700 SEV=9 IKEDBG/49 RPT=25 172.18.124.132
Received Cisco Unity client VID

38 08/09/2002 13:14:22.700 SEV=9 IKEDBG/47 RPT=30 172.18.124.132
processing VID payload

39 08/09/2002 13:14:22.700 SEV=9 IKEDBG/49 RPT=26 172.18.124.132
Received xauth V6 VID

40 08/09/2002 13:14:22.700 SEV=9 IKEDBG/47 RPT=31 172.18.124.132
processing VID payload

41 08/09/2002 13:14:22.700 SEV=9 IKEDBG/38 RPT=9 172.18.124.132
Processing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabilities
: 20000001)

43 08/09/2002 13:14:22.700 SEV=9 IKEDBG/47 RPT=32 172.18.124.132
processing VID payload

44 08/09/2002 13:14:22.700 SEV=9 IKEDBG/49 RPT=27 172.18.124.132
Received Altiga GW VID

45 08/09/2002 13:14:22.730 SEV=9 IKEDBG/0 RPT=52052 172.18.124.132
constructing ke payload

46 08/09/2002 13:14:22.730 SEV=9 IKEDBG/1 RPT=84 172.18.124.132
constructing nonce payload

47 08/09/2002 13:14:22.730 SEV=9 IKEDBG/46 RPT=27 172.18.124.132
constructing Cisco Unity VID payload

48 08/09/2002 13:14:22.730 SEV=9 IKEDBG/46 RPT=28 172.18.124.132
constructing xauth V6 VID payload

49 08/09/2002 13:14:22.730 SEV=9 IKEDBG/48 RPT=10 172.18.124.132
Send IOS VID

50 08/09/2002 13:14:22.730 SEV=9 IKEDBG/38 RPT=10 172.18.124.132
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)

52 08/09/2002 13:14:22.730 SEV=9 IKEDBG/46 RPT=29 172.18.124.132
constructing VID payload

53 08/09/2002 13:14:22.730 SEV=9 IKEDBG/48 RPT=11 172.18.124.132
Send Altiga GW VID

54 08/09/2002 13:14:22.730 SEV=9 IKEDBG/0 RPT=52053 172.18.124.132
Generating keys for Responder...

55 08/09/2002 13:14:22.730 SEV=8 IKEDBG/0 RPT=52054 172.18.124.132
SENDING Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) ... total length : 256

57 08/09/2002 13:14:22.770 SEV=8 IKEDBG/0 RPT=52055 172.18.124.132
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14) + VENDOR (13) + NONE (0) ... total
length : 92

60 08/09/2002 13:14:22.770 SEV=9 IKEDBG/1 RPT=85 172.18.124.132
Group [172.18.124.132]
Processing ID

61 08/09/2002 13:14:22.770 SEV=9 IKEDBG/0 RPT=52056 172.18.124.132
Group [172.18.124.132]
processing hash

62 08/09/2002 13:14:22.770 SEV=9 IKEDBG/0 RPT=52057 172.18.124.132
Group [172.18.124.132]
computing hash

63 08/09/2002 13:14:22.770 SEV=9 IKEDBG/34 RPT=9 172.18.124.132
Processing IOS keep alive payload: proposal=32767/32767 sec.

64 08/09/2002 13:14:22.770 SEV=9 IKEDBG/47 RPT=33 172.18.124.132
Group [172.18.124.132]
processing VID payload

65 08/09/2002 13:14:22.770 SEV=9 IKEDBG/49 RPT=28 172.18.124.132
Group [172.18.124.132]
Received DPD VID

66 08/09/2002 13:14:22.770 SEV=9 IKEDBG/23 RPT=6 172.18.124.132
Group [172.18.124.132]
Starting group lookup for peer 172.18.124.132

67 08/09/2002 13:14:22.770 SEV=8 AUTHDBG/1 RPT=7
AUTH_Open() returns 9

68 08/09/2002 13:14:22.770 SEV=7 AUTH/12 RPT=7
Authentication session opened: handle = 9

69 08/09/2002 13:14:22.770 SEV=8 AUTHDBG/3 RPT=9
AUTH_PutAttrTable(9, 8c6274)

70 08/09/2002 13:14:22.770 SEV=8 AUTHDBG/6 RPT=6
AUTH_GroupAuthenticate(9, 2f1c798, 599818)

71 08/09/2002 13:14:22.770 SEV=8 AUTHDBG/59 RPT=9
AUTH_BindServer(511c62c, 0, 0)

72 08/09/2002 13:14:22.770 SEV=9 AUTHDBG/69 RPT=9
Auth Server db1704 has been bound to ACB 511c62c, sessions = 1

73 08/09/2002 13:14:22.770 SEV=8 AUTHDBG/65 RPT=9
AUTH_CreateTimer(511c62c, 0, 0)

74 08/09/2002 13:14:22.770 SEV=9 AUTHDBG/72 RPT=9
Reply timer created: handle = 66001B

75 08/09/2002 13:14:22.770 SEV=8 AUTHDBG/179 RPT=9
AUTH_SyncToServer(511c62c, 0, 0)

76 08/09/2002 13:14:22.770 SEV=8 AUTHDBG/180 RPT=9
AUTH_SendLockReq(511c62c, 0, 0)

77 08/09/2002 13:14:22.770 SEV=8 AUTHDBG/61 RPT=9
AUTH_BuildMsg(511c62c, 0, 0)

78 08/09/2002 13:14:22.770 SEV=8 AUTHDBG/64 RPT=9
AUTH_StartTimer(511c62c, 0, 0)

79 08/09/2002 13:14:22.770 SEV=9 AUTHDBG/73 RPT=9
Reply timer started: handle = 66001B, timestamp = 17178934, timeout = 30000

80 08/09/2002 13:14:22.770 SEV=8 AUTHDBG/62 RPT=9
AUTH_SndRequest(511c62c, 0, 0)

81 08/09/2002 13:14:22.770 SEV=8 AUTHDBG/50 RPT=17
IntDB_Decode(37f1908, 149)

82 08/09/2002 13:14:22.770 SEV=8 AUTHDBG/47 RPT=17
IntDB_Xmt(511c62c)

83 08/09/2002 13:14:22.770 SEV=9 AUTHDBG/71 RPT=9
xmit_cnt = 1

84 08/09/2002 13:14:22.770 SEV=8 AUTHDBG/47 RPT=18
IntDB_Xmt(511c62c)

85 08/09/2002 13:14:22.870 SEV=8 AUTHDBG/49 RPT=9
IntDB_Match(511c62c, 5119cc4)

86 08/09/2002 13:14:22.870 SEV=8 AUTHDBG/63 RPT=9
AUTH_RcvReply(511c62c, 0, 0)

87 08/09/2002 13:14:22.870 SEV=8 AUTHDBG/50 RPT=18
IntDB_Decode(5119cc4, 835)

88 08/09/2002 13:14:22.870 SEV=8 AUTHDBG/48 RPT=9
IntDB_Rcv(511c62c)

89 08/09/2002 13:14:22.870 SEV=8 AUTHDBG/66 RPT=9
AUTH_DeleteTimer(511c62c, 0, 0)

90 08/09/2002 13:14:22.870 SEV=9 AUTHDBG/74 RPT=9
Reply timer stopped: handle = 66001B, timestamp = 17178944

91 08/09/2002 13:14:22.870 SEV=8 AUTHDBG/58 RPT=9
AUTH_Callback(511c62c, 0, 0)

**92 08/09/2002 13:14:22.870 SEV=6 AUTH/41 RPT=8 172.18.124.132
Authentication successful: handle = 9, server = Internal, group = 172.18.124.132**

93 08/09/2002 13:14:22.870 SEV=7 IKEDBG/0 RPT=52058 172.18.124.132
Group [172.18.124.132]
Found Phase 1 Group (172.18.124.132)

94 08/09/2002 13:14:22.870 SEV=8 AUTHDBG/4 RPT=8
AUTH_GetAttrTable(9, 8c6520)

95 08/09/2002 13:14:22.870 SEV=7 IKEDBG/14 RPT=7 172.18.124.132
Group [172.18.124.132]
Authentication configured for Internal

96 08/09/2002 13:14:22.870 SEV=8 AUTHDBG/2 RPT=7
AUTH_Close(9)

97 08/09/2002 13:14:22.870 SEV=9 IKEDBG/1 RPT=86 172.18.124.132
Group [172.18.124.132]
constructing ID

98 08/09/2002 13:14:22.870 SEV=9 IKEDBG/0 RPT=52059
Group [172.18.124.132]
construct hash payload

99 08/09/2002 13:14:22.870 SEV=9 IKEDBG/0 RPT=52060 172.18.124.132
Group [172.18.124.132]
computing hash

100 08/09/2002 13:14:22.870 SEV=9 IKEDBG/34 RPT=10 172.18.124.132
Constructing IOS keep alive payload: proposal=32767/32767 sec.

101 08/09/2002 13:14:22.870 SEV=9 IKEDBG/46 RPT=30 172.18.124.132
Group [172.18.124.132]
constructing dpd vid payload

102 08/09/2002 13:14:22.870 SEV=8 IKEDBG/0 RPT=52061 172.18.124.132
SENDING Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) ... total length : 92

104 08/09/2002 13:14:22.870 SEV=4 IKE/119 RPT=8 172.18.124.132
Group [172.18.124.132]
PHASE 1 COMPLETED

105 08/09/2002 13:14:22.870 SEV=6 IKE/121 RPT=6 172.18.124.132
Keep-alive type for this connection: DPD

106 08/09/2002 13:14:22.870 SEV=7 IKEDBG/0 RPT=52062 172.18.124.132
Group [172.18.124.132]
Starting phase 1 rekey timer: 73440000 (ms)

107 08/09/2002 13:14:22.870 SEV=4 AUTH/22 RPT=38
User 172.18.124.132 connected

108 08/09/2002 13:14:22.870 SEV=8 AUTHDBG/60 RPT=9
AUTH_UnbindServer(511c62c, 0, 0)

109 08/09/2002 13:14:22.870 SEV=9 AUTHDBG/70 RPT=9
Auth Server db1704 has been unbound from ACB 511c62c, sessions = 0

110 08/09/2002 13:14:22.870 SEV=8 AUTHDBG/10 RPT=7
AUTH_Int_FreeAuthCB(511c62c)

111 08/09/2002 13:14:22.870 SEV=7 AUTH/13 RPT=7
Authentication session closed: handle = 9

112 08/09/2002 13:14:22.970 SEV=8 IKEDBG/0 RPT=52063 172.18.124.132
RECEIVED Message (msgid=56fdca09) with payloads :

HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0)
... total length : 180

115 08/09/2002 13:14:22.970 SEV=9 IKEDBG/0 RPT=52064 172.18.124.132
Group [172.18.124.132]
processing hash

116 08/09/2002 13:14:22.970 SEV=9 IKEDBG/0 RPT=52065 172.18.124.132
Group [172.18.124.132]
processing SA payload

117 08/09/2002 13:14:22.970 SEV=9 IKEDBG/1 RPT=87 172.18.124.132
Group [172.18.124.132]
processing nonce payload

118 08/09/2002 13:14:22.970 SEV=9 IKEDBG/1 RPT=88 172.18.124.132
Group [172.18.124.132]
Processing ID

119 08/09/2002 13:14:22.970 SEV=5 IKE/35 RPT=4 172.18.124.132
Group [172.18.124.132]
Received remote IP Proxy Subnet data in ID Payload:
Address 14.38.80.0, Mask 255.255.255.0, Protocol 0, Port 0

122 08/09/2002 13:14:22.970 SEV=9 IKEDBG/1 RPT=89 172.18.124.132
Group [172.18.124.132]
Processing ID

123 08/09/2002 13:14:22.970 SEV=5 IKE/34 RPT=6 172.18.124.132
Group [172.18.124.132]
Received local IP Proxy Subnet data in ID Payload:
Address 14.38.200.0, Mask 255.255.255.0, Protocol 0, Port 0

126 08/09/2002 13:14:22.970 SEV=9 IKEDBG/0 RPT=52066 172.18.124.132
Group [172.18.124.132]
Processing Notify payload

127 08/09/2002 13:14:22.970 SEV=8 IKEDBG/0 RPT=52067
QM IsRekeyed old sa not found by addr

128 08/09/2002 13:14:22.970 SEV=5 IKE/66 RPT=8 172.18.124.132
Group [172.18.124.132]
IKE Remote Peer configured for SA: L2L: RTP NAT TUNNEL

129 08/09/2002 13:14:22.970 SEV=9 IKEDBG/0 RPT=52068 172.18.124.132
Group [172.18.124.132]
processing IPSEC SA

130 08/09/2002 13:14:22.970 SEV=7 IKEDBG/27 RPT=6 172.18.124.132
Group [172.18.124.132]
IPSec SA Proposal # 1, Transform # 1 acceptable

131 08/09/2002 13:14:22.970 SEV=7 IKEDBG/0 RPT=52069 172.18.124.132
Group [172.18.124.132]
IKE: requesting SPI!

132 08/09/2002 13:14:22.970 SEV=6 IKE/0 RPT=5
Received unexpected event EV_ACTIVATE_NEW_SA in state MM_ACTIVE

133 08/09/2002 13:14:22.970 SEV=9 IPSECDBG/6 RPT=41
IPSEC key message parse - msgtype 6, len 208, 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 21, lifetime2 0, dsId 30
0

137 08/09/2002 13:14:22.970 SEV=9 IPSECDBG/1 RPT=155

Processing KEY_GETSPI msg!

138 08/09/2002 13:14:22.970 SEV=7 IPSECDBG/13 RPT=9
Reserved SPI 840508266

139 08/09/2002 13:14:22.970 SEV=8 IKEDBG/6 RPT=9
IKE got SPI from key engine: SPI = 0x3219236a

140 08/09/2002 13:14:22.970 SEV=9 IKEDBG/0 RPT=52070 172.18.124.132
Group [172.18.124.132]
oakley constructing quick mode

141 08/09/2002 13:14:22.970 SEV=9 IKEDBG/0 RPT=52071 172.18.124.132
Group [172.18.124.132]
constructing blank hash

142 08/09/2002 13:14:22.970 SEV=9 IKEDBG/0 RPT=52072 172.18.124.132
Group [172.18.124.132]
constructing ISA_SA for ipsec

143 08/09/2002 13:14:22.970 SEV=9 IKEDBG/1 RPT=90 172.18.124.132
Group [172.18.124.132]
constructing ipsec nonce payload

144 08/09/2002 13:14:22.970 SEV=9 IKEDBG/1 RPT=91 172.18.124.132
Group [172.18.124.132]
constructing proxy ID

145 08/09/2002 13:14:22.970 SEV=7 IKEDBG/0 RPT=52073 172.18.124.132
Group [172.18.124.132]

Transmitting Proxy Id:

Remote subnet: 14.38.80.0 Mask 255.255.255.0 Protocol 0 Port 0

Local subnet: 14.38.200.0 mask 255.255.255.0 Protocol 0 Port 0

149 08/09/2002 13:14:22.970 SEV=9 IKEDBG/0 RPT=52074 172.18.124.132
Group [172.18.124.132]
constructing qm hash

150 08/09/2002 13:14:22.970 SEV=8 IKEDBG/0 RPT=52075 172.18.124.132
SENDING Message (msgid=56fdca09) with payloads :
HDR + HASH (8) + SA (1) ... total length : 152

152 08/09/2002 13:14:22.980 SEV=8 IKEDBG/0 RPT=52076 172.18.124.132
RECEIVED Message (msgid=56fdca09) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

154 08/09/2002 13:14:22.980 SEV=9 IKEDBG/0 RPT=52077 172.18.124.132
Group [172.18.124.132]
processing hash

155 08/09/2002 13:14:22.980 SEV=9 IKEDBG/0 RPT=52078 172.18.124.132
Group [172.18.124.132]
loading all IPSEC SAs

156 08/09/2002 13:14:22.980 SEV=9 IKEDBG/1 RPT=92 172.18.124.132
Group [172.18.124.132]
Generating Quick Mode Key!

157 08/09/2002 13:14:22.980 SEV=9 IKEDBG/1 RPT=93 172.18.124.132
Group [172.18.124.132]
Generating Quick Mode Key!

158 08/09/2002 13:14:22.980 SEV=7 IKEDBG/0 RPT=52079 172.18.124.132
Group [172.18.124.132]

Loading subnet:

Dst: 14.38.200.0 mask: 255.255.255.0

Src: 14.38.80.0 mask: 255.255.255.0

161 08/09/2002 13:14:22.980 SEV=4 IKE/49 RPT=12 172.18.124.132
Group [172.18.124.132]
Security negotiation complete for LAN-to-LAN Group (172.18.124.132)
Responder, Inbound SPI = 0x3219236a, Outbound SPI = 0x3607c2f4

164 08/09/2002 13:14:22.980 SEV=9 IPSECDBG/6 RPT=42
IPSEC key message parse - msgtype 1, len 622, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 64, label 0, pad 0, spi 3607c2f4, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 21, lifetime2 0, dsId 0

167 08/09/2002 13:14:22.980 SEV=9 IPSECDBG/1 RPT=156
Processing KEY_ADD msg!

168 08/09/2002 13:14:22.980 SEV=9 IPSECDBG/1 RPT=157
key_msghdr2secassoc(): Enter

169 08/09/2002 13:14:22.980 SEV=7 IPSECDBG/1 RPT=158
No USER filter configured

170 08/09/2002 13:14:22.980 SEV=9 IPSECDBG/1 RPT=159
KeyProcessAdd: Enter

171 08/09/2002 13:14:22.980 SEV=8 IPSECDBG/1 RPT=160
KeyProcessAdd: Adding outbound SA

172 08/09/2002 13:14:22.980 SEV=8 IPSECDBG/1 RPT=161
KeyProcessAdd: src 14.38.200.0 mask 0.0.0.255, dst 14.38.80.0 mask 0.0.0.255

173 08/09/2002 13:14:22.980 SEV=8 IPSECDBG/1 RPT=162
KeyProcessAdd: FilterIpssecAddIkeSa success

174 08/09/2002 13:14:22.980 SEV=9 IPSECDBG/6 RPT=43
IPSEC key message parse - msgtype 3, len 335, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 32, label 0, pad 0, spi 3219236a, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 21, lifetime2 0, dsId 0

177 08/09/2002 13:14:22.980 SEV=9 IPSECDBG/1 RPT=163
Processing KEY_UPDATE msg!

178 08/09/2002 13:14:22.980 SEV=9 IPSECDBG/1 RPT=164
Update inbound SA addresses

179 08/09/2002 13:14:22.980 SEV=9 IPSECDBG/1 RPT=165
key_msghdr2secassoc(): Enter

180 08/09/2002 13:14:22.980 SEV=7 IPSECDBG/1 RPT=166
No USER filter configured

181 08/09/2002 13:14:22.980 SEV=9 IPSECDBG/1 RPT=167
KeyProcessUpdate: Enter

182 08/09/2002 13:14:22.980 SEV=8 IPSECDBG/1 RPT=168
KeyProcessUpdate: success

183 08/09/2002 13:14:22.980 SEV=8 IKEDBG/7 RPT=9
IKE got a KEY_ADD msg for SA: SPI = 0x3607c2f4

184 08/09/2002 13:14:22.980 SEV=8 IKEDBG/0 RPT=52080
pitcher: rcv KEY_UPDATE, spi 0x3219236a

**185 08/09/2002 13:14:22.980 SEV=4 IKE/120 RPT=12 172.18.124.132
Group [172.18.124.132]
PHASE 2 COMPLETED (msgid=56fdca09)**

186 08/09/2002 13:14:24.690 SEV=7 IPSECDBG/1 RPT=169
IPSec Inbound SA has received data!

187 08/09/2002 13:14:24.690 SEV=8 IKEDBG/0 RPT=52081
pitcher: recv KEY_SA_ACTIVE spi 0x3219236a

188 08/09/2002 13:14:24.690 SEV=8 IKEDBG/0 RPT=52082
KEY_SA_ACTIVE no old rekey centry found with new spi 0x3219236a, mess_id 0x0

Troubleshoot the VPN 3000 Concentrator B Configuration

For information setting up and reviewing logs when troubleshooting connection problems with VPN 3000 Concentrator, refer to Troubleshooting Connection Problems on the VPN 3000 Concentrator. Before issuing **debug** commands, please see Important Information on Debug Commands.

1 08/07/2002 13:27:13.970 SEV=7 IPSECDBG/10 RPT=4
IPSEC ipsec_output() can call key_acquire() because 590 seconds have elapsed since last IKE negotiation began (src 0x0e265065, dst 0x01b99224)

3 08/07/2002 13:27:13.970 SEV=7 IPSECDBG/14 RPT=5
Sending KEY_ACQUIRE to IKE for src 14.38.80.101, dst 14.38.200.3

4 08/07/2002 13:27:13.970 SEV=8 IKEDBG/0 RPT=52300
pitcher: received a key acquire message!

5 08/07/2002 13:27:13.970 SEV=4 IKE/41 RPT=5 172.18.124.131
IKE Initiator: New Phase 1, Intf 2, IKE Peer 172.18.124.131
local Proxy Address 14.38.80.0, remote Proxy Address 14.38.200.0,
SA (L2L: VPN TUNNEL)

8 08/07/2002 13:27:13.970 SEV=9 IKEDBG/0 RPT=52301 172.18.124.131
constructing ISA_SA for isakmp

9 08/07/2002 13:27:13.970 SEV=9 IKEDBG/46 RPT=26 172.18.124.131
constructing Fragmentation VID + extended capabilities payload

10 08/07/2002 13:27:13.970 SEV=8 IKEDBG/0 RPT=52302 172.18.124.131
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) ... total length : 108

12 08/07/2002 13:27:13.970 SEV=8 IKEDBG/0 RPT=52303 172.18.124.131
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 108

14 08/07/2002 13:27:13.970 SEV=8 IKEDBG/0 RPT=52304 172.18.124.131
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 108

16 08/07/2002 13:27:13.970 SEV=9 IKEDBG/0 RPT=52305 172.18.124.131
processing SA payload

17 08/07/2002 13:27:13.970 SEV=7 IKEDBG/0 RPT=52306 172.18.124.131
Oakley proposal is acceptable

18 08/07/2002 13:27:13.970 SEV=9 IKEDBG/47 RPT=31 172.18.124.131
processing VID payload

19 08/07/2002 13:27:13.970 SEV=9 IKEDBG/49 RPT=26 172.18.124.131
Received Fragmentation VID

20 08/07/2002 13:27:13.970 SEV=5 IKEDBG/64 RPT=7 172.18.124.131
IKE Peer included IKE fragmentation capability flags:
Main Mode: True
Aggressive Mode: True

22 08/07/2002 13:27:13.970 SEV=9 IKEDBG/0 RPT=52307 172.18.124.131
constructing ke payload

23 08/07/2002 13:27:13.970 SEV=9 IKEDBG/1 RPT=70 172.18.124.131
constructing nonce payload

24 08/07/2002 13:27:13.970 SEV=9 IKEDBG/46 RPT=27 172.18.124.131
constructing Cisco Unity VID payload

25 08/07/2002 13:27:13.970 SEV=9 IKEDBG/46 RPT=28 172.18.124.131
constructing xauth V6 VID payload

26 08/07/2002 13:27:13.970 SEV=9 IKEDBG/48 RPT=11 172.18.124.131
Send IOS VID

27 08/07/2002 13:27:13.970 SEV=9 IKEDBG/38 RPT=11 172.18.124.131
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)

29 08/07/2002 13:27:13.970 SEV=9 IKEDBG/46 RPT=29 172.18.124.131
constructing VID payload

30 08/07/2002 13:27:13.970 SEV=9 IKEDBG/48 RPT=12 172.18.124.131
Send Altiga GW VID

31 08/07/2002 13:27:13.970 SEV=8 IKEDBG/0 RPT=52308 172.18.124.131
SENDING Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) ... total length : 256

33 08/07/2002 13:27:14.010 SEV=8 IKEDBG/0 RPT=52309 172.18.124.131
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) ... total length : 256

36 08/07/2002 13:27:14.010 SEV=8 IKEDBG/0 RPT=52310 172.18.124.131
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) ... total length : 256

39 08/07/2002 13:27:14.010 SEV=9 IKEDBG/0 RPT=52311 172.18.124.131
processing ke payload

40 08/07/2002 13:27:14.010 SEV=9 IKEDBG/0 RPT=52312 172.18.124.131
processing ISA_KE

41 08/07/2002 13:27:14.010 SEV=9 IKEDBG/1 RPT=71 172.18.124.131
processing nonce payload

42 08/07/2002 13:27:14.010 SEV=9 IKEDBG/47 RPT=32 172.18.124.131
processing VID payload

43 08/07/2002 13:27:14.010 SEV=9 IKEDBG/49 RPT=27 172.18.124.131
Received Cisco Unity client VID

44 08/07/2002 13:27:14.010 SEV=9 IKEDBG/47 RPT=33 172.18.124.131
processing VID payload

45 08/07/2002 13:27:14.010 SEV=9 IKEDBG/49 RPT=28 172.18.124.131
Received xauth V6 VID

46 08/07/2002 13:27:14.010 SEV=9 IKEDBG/47 RPT=34 172.18.124.131
processing VID payload

47 08/07/2002 13:27:14.010 SEV=9 IKEDBG/38 RPT=12 172.18.124.131
Processing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabilities
: 20000001)

49 08/07/2002 13:27:14.010 SEV=9 IKEDBG/47 RPT=35 172.18.124.131
processing VID payload

50 08/07/2002 13:27:14.010 SEV=9 IKEDBG/49 RPT=29 172.18.124.131
Received Altiga GW VID

51 08/07/2002 13:27:14.040 SEV=9 IKEDBG/0 RPT=52313 172.18.124.131
Generating keys for Initiator...

52 08/07/2002 13:27:14.040 SEV=9 IKEDBG/1 RPT=72 172.18.124.131
Group [172.18.124.131]
constructing ID

53 08/07/2002 13:27:14.040 SEV=9 IKEDBG/0 RPT=52314
Group [172.18.124.131]
construct hash payload

54 08/07/2002 13:27:14.040 SEV=9 IKEDBG/0 RPT=52315 172.18.124.131
Group [172.18.124.131]
computing hash

55 08/07/2002 13:27:14.040 SEV=9 IKEDBG/34 RPT=11 172.18.124.131
Constructing IOS keep alive payload: proposal=32767/32767 sec.

56 08/07/2002 13:27:14.040 SEV=9 IKEDBG/46 RPT=30 172.18.124.131
Group [172.18.124.131]
constructing dpd vid payload

57 08/07/2002 13:27:14.040 SEV=8 IKEDBG/0 RPT=52316 172.18.124.131
SENDING Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) ... total length : 92

59 08/07/2002 13:27:14.140 SEV=8 IKEDBG/0 RPT=52317 172.18.124.131
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14) + VENDOR (13) + NONE (0) ... total
length : 92

62 08/07/2002 13:27:14.140 SEV=9 IKEDBG/1 RPT=73 172.18.124.131
Group [172.18.124.131]
Processing ID

63 08/07/2002 13:27:14.140 SEV=9 IKEDBG/0 RPT=52318 172.18.124.131
Group [172.18.124.131]
processing hash

64 08/07/2002 13:27:14.140 SEV=9 IKEDBG/0 RPT=52319 172.18.124.131
Group [172.18.124.131]
computing hash

65 08/07/2002 13:27:14.140 SEV=9 IKEDBG/34 RPT=12 172.18.124.131
Processing IOS keep alive payload: proposal=32767/32767 sec.

66 08/07/2002 13:27:14.140 SEV=9 IKEDBG/47 RPT=36 172.18.124.131
Group [172.18.124.131]
processing VID payload

67 08/07/2002 13:27:14.140 SEV=9 IKEDBG/49 RPT=30 172.18.124.131
Group [172.18.124.131]
Received DPD VID

68 08/07/2002 13:27:14.140 SEV=9 IKEDBG/23 RPT=6 172.18.124.131
Group [172.18.124.131]
Starting group lookup for peer 172.18.124.131

69 08/07/2002 13:27:14.140 SEV=8 AUTHDBG/1 RPT=2
AUTH_Open() returns 6

70 08/07/2002 13:27:14.140 SEV=7 AUTH/12 RPT=2
Authentication session opened: handle = 6

71 08/07/2002 13:27:14.150 SEV=8 AUTHDBG/3 RPT=2
AUTH_PutAttrTable(6, 8c6274)

72 08/07/2002 13:27:14.150 SEV=8 AUTHDBG/6 RPT=2
AUTH_GroupAuthenticate(6, 50097dc, 599818)

73 08/07/2002 13:27:14.150 SEV=8 AUTHDBG/59 RPT=2
AUTH_BindServer(9a05c60, 0, 0)

74 08/07/2002 13:27:14.150 SEV=9 AUTHDBG/69 RPT=2
Auth Server 15dd704 has been bound to ACB 9a05c60, sessions = 1

75 08/07/2002 13:27:14.150 SEV=8 AUTHDBG/65 RPT=2
AUTH_CreateTimer(9a05c60, 0, 0)

76 08/07/2002 13:27:14.150 SEV=9 AUTHDBG/72 RPT=2
Reply timer created: handle = 4F0019

77 08/07/2002 13:27:14.150 SEV=8 AUTHDBG/179 RPT=2
AUTH_SyncToServer(9a05c60, 0, 0)

78 08/07/2002 13:27:14.150 SEV=8 AUTHDBG/180 RPT=2
AUTH_SendLockReq(9a05c60, 0, 0)

79 08/07/2002 13:27:14.150 SEV=8 AUTHDBG/61 RPT=2
AUTH_BuildMsg(9a05c60, 0, 0)

80 08/07/2002 13:27:14.150 SEV=8 AUTHDBG/64 RPT=2
AUTH_StartTimer(9a05c60, 0, 0)

81 08/07/2002 13:27:14.150 SEV=9 AUTHDBG/73 RPT=2
Reply timer started: handle = 4F0019, timestamp = 17231134, timeout = 30000

82 08/07/2002 13:27:14.150 SEV=8 AUTHDBG/62 RPT=2
AUTH_SndRequest(9a05c60, 0, 0)

83 08/07/2002 13:27:14.150 SEV=8 AUTHDBG/50 RPT=3
IntDB_Decode(62ea4f8, 149)

84 08/07/2002 13:27:14.150 SEV=8 AUTHDBG/47 RPT=3
IntDB_Xmt(9a05c60)

85 08/07/2002 13:27:14.150 SEV=9 AUTHDBG/71 RPT=2
xmit_cnt = 1

86 08/07/2002 13:27:14.150 SEV=8 AUTHDBG/47 RPT=4
IntDB_Xmt(9a05c60)

87 08/07/2002 13:27:14.250 SEV=8 AUTHDBG/49 RPT=2
IntDB_Match(9a05c60, 9a09658)

88 08/07/2002 13:27:14.250 SEV=8 AUTHDBG/63 RPT=2
AUTH_RcvReply(9a05c60, 0, 0)

89 08/07/2002 13:27:14.250 SEV=8 AUTHDBG/50 RPT=4
IntDB_Decode(9a09658, 636)

90 08/07/2002 13:27:14.250 SEV=8 AUTHDBG/48 RPT=2
IntDB_Rcv(9a05c60)

91 08/07/2002 13:27:14.250 SEV=8 AUTHDBG/66 RPT=2
AUTH_DeleteTimer(9a05c60, 0, 0)

92 08/07/2002 13:27:14.250 SEV=9 AUTHDBG/74 RPT=2
Reply timer stopped: handle = 4F0019, timestamp = 17231144

93 08/07/2002 13:27:14.250 SEV=8 AUTHDBG/58 RPT=2
AUTH_Callback(9a05c60, 0, 0)

94 08/07/2002 13:27:14.250 SEV=6 AUTH/41 RPT=2 172.18.124.131
Authentication successful: handle = 6, server = Internal, group = 172.18.124.131

95 08/07/2002 13:27:14.250 SEV=7 IKEDBG/0 RPT=52320 172.18.124.131
Group [172.18.124.131]
Found Phase 1 Group (172.18.124.131)

96 08/07/2002 13:27:14.250 SEV=8 AUTHDBG/4 RPT=2
AUTH_GetAttrTable(6, 8c6520)

97 08/07/2002 13:27:14.250 SEV=7 IKEDBG/14 RPT=6 172.18.124.131
Group [172.18.124.131]
Authentication configured for Internal

98 08/07/2002 13:27:14.250 SEV=8 AUTHDBG/2 RPT=2
AUTH_Close(6)

99 08/07/2002 13:27:14.250 SEV=9 IKEDBG/0 RPT=52321 172.18.124.131
Group [172.18.124.131]
Oakley begin quick mode

**100 08/07/2002 13:27:14.250 SEV=4 IKE/119 RPT=7 172.18.124.131
Group [172.18.124.131]
PHASE 1 COMPLETED**

101 08/07/2002 13:27:14.250 SEV=6 IKE/121 RPT=6 172.18.124.131
Keep-alive type for this connection: DPD

102 08/07/2002 13:27:14.250 SEV=7 IKEDBG/0 RPT=52322 172.18.124.131
Group [172.18.124.131]
Starting phase 1 rekey timer: 82080000 (ms)

103 08/07/2002 13:27:14.250 SEV=4 AUTH/22 RPT=27
User 172.18.124.131 connected

104 08/07/2002 13:27:14.250 SEV=9 IPSECDBG/6 RPT=36
IPSEC key message parse - msgtype 6, len 208, vers 1, pid 00000000, seq 9, 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, lifetimel 21, lifetime2 0, dsId 300

107 08/07/2002 13:27:14.250 SEV=9 IPSECDBG/1 RPT=135
Processing KEY_GETSPI msg!

108 08/07/2002 13:27:14.250 SEV=7 IPSECDBG/13 RPT=8
Reserved SPI 651287217

109 08/07/2002 13:27:14.250 SEV=8 IKEDBG/6 RPT=8
IKE got SPI from key engine: SPI = 0x26d1dab1

110 08/07/2002 13:27:14.250 SEV=9 IKEDBG/0 RPT=52323 172.18.124.131
Group [172.18.124.131]
oakley constructing quick mode

111 08/07/2002 13:27:14.250 SEV=9 IKEDBG/0 RPT=52324 172.18.124.131
Group [172.18.124.131]
constructing blank hash

112 08/07/2002 13:27:14.250 SEV=9 IKEDBG/0 RPT=52325 172.18.124.131
Group [172.18.124.131]
constructing ISA_SA for ipsec

113 08/07/2002 13:27:14.250 SEV=9 IKEDBG/1 RPT=74 172.18.124.131
Group [172.18.124.131]
constructing ipsec nonce payload

114 08/07/2002 13:27:14.250 SEV=9 IKEDBG/1 RPT=75 172.18.124.131
Group [172.18.124.131]
constructing proxy ID

115 08/07/2002 13:27:14.250 SEV=7 IKEDBG/0 RPT=52326 172.18.124.131
Group [172.18.124.131]
Transmitting Proxy Id:
Local subnet: 14.38.80.0 mask 255.255.255.0 Protocol 0 Port 0
Remote subnet: 14.38.200.0 Mask 255.255.255.0 Protocol 0 Port 0

119 08/07/2002 13:27:14.250 SEV=9 IKEDBG/0 RPT=52327 172.18.124.131
Group [172.18.124.131]
constructing qm hash

120 08/07/2002 13:27:14.250 SEV=8 IKEDBG/0 RPT=52328 172.18.124.131
SENDING Message (msgid=201d0d40) with payloads :
HDR + HASH (8) + SA (1) ... total length : 180

122 08/07/2002 13:27:14.250 SEV=8 AUTHDBG/60 RPT=2
AUTH_UnbindServer(9a05c60, 0, 0)

123 08/07/2002 13:27:14.250 SEV=9 AUTHDBG/70 RPT=2
Auth Server 15dd704 has been unbound from ACB 9a05c60, sessions = 0

124 08/07/2002 13:27:14.250 SEV=8 AUTHDBG/10 RPT=2
AUTH_Int_FreeAuthCB(9a05c60)

125 08/07/2002 13:27:14.250 SEV=7 AUTH/13 RPT=2
Authentication session closed: handle = 6

126 08/07/2002 13:27:14.250 SEV=8 IKEDBG/0 RPT=52329 172.18.124.131
RECEIVED Message (msgid=201d0d40) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total length : 152

129 08/07/2002 13:27:14.250 SEV=9 IKEDBG/0 RPT=52330 172.18.124.131
Group [172.18.124.131]
processing hash

130 08/07/2002 13:27:14.250 SEV=9 IKEDBG/0 RPT=52331 172.18.124.131
Group [172.18.124.131]
processing SA payload

131 08/07/2002 13:27:14.250 SEV=9 IKEDBG/1 RPT=76 172.18.124.131
Group [172.18.124.131]
processing nonce payload

132 08/07/2002 13:27:14.250 SEV=9 IKEDBG/1 RPT=77 172.18.124.131
Group [172.18.124.131]
Processing ID

133 08/07/2002 13:27:14.250 SEV=9 IKEDBG/1 RPT=78 172.18.124.131
Group [172.18.124.131]
Processing ID

134 08/07/2002 13:27:14.250 SEV=9 IKEDBG/0 RPT=52332 172.18.124.131
Group [172.18.124.131]
loading all IPSEC SAs

135 08/07/2002 13:27:14.250 SEV=9 IKEDBG/1 RPT=79 172.18.124.131
Group [172.18.124.131]
Generating Quick Mode Key!

136 08/07/2002 13:27:14.260 SEV=9 IKEDBG/1 RPT=80 172.18.124.131
Group [172.18.124.131]
Generating Quick Mode Key!

137 08/07/2002 13:27:14.260 SEV=7 IKEDBG/0 RPT=52333 172.18.124.131
Group [172.18.124.131]
Loading subnet:
Dst: 14.38.200.0 mask: 255.255.255.0
Src: 14.38.80.0 mask: 255.255.255.0

140 08/07/2002 13:27:14.260 SEV=4 IKE/49 RPT=9 172.18.124.131
Group [172.18.124.131]
Security negotiation complete for LAN-to-LAN Group (172.18.124.131)
Initiator, Inbound SPI = 0x26d1dab1, Outbound SPI = 0x2f285111

143 08/07/2002 13:27:14.260 SEV=9 IKEDBG/0 RPT=52334 172.18.124.131
Group [172.18.124.131]
oakley constructing final quick mode

144 08/07/2002 13:27:14.260 SEV=8 IKEDBG/0 RPT=52335 172.18.124.131
SENDING Message (msgid=201d0d40) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 72

146 08/07/2002 13:27:14.260 SEV=9 IPSECDBG/6 RPT=37
IPSEC key message parse - msgtype 1, len 622, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 64, label 0, pad 0, spi 2f285111, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 21, lifetime2 0, dsId 0

149 08/07/2002 13:27:14.260 SEV=9 IPSECDBG/1 RPT=136
Processing KEY_ADD msg!

150 08/07/2002 13:27:14.260 SEV=9 IPSECDBG/1 RPT=137
key_msghdr2secassoc(): Enter

151 08/07/2002 13:27:14.260 SEV=7 IPSECDBG/1 RPT=138
No USER filter configured

152 08/07/2002 13:27:14.260 SEV=9 IPSECDBG/1 RPT=139
KeyProcessAdd: Enter

153 08/07/2002 13:27:14.260 SEV=8 IPSECDBG/1 RPT=140
KeyProcessAdd: Adding outbound SA

154 08/07/2002 13:27:14.260 SEV=8 IPSECDBG/1 RPT=141
KeyProcessAdd: src 14.38.80.0 mask 0.0.0.255, dst 14.38.200.0 mask 0.0.0.255

155 08/07/2002 13:27:14.260 SEV=8 IPSECDBG/1 RPT=142
KeyProcessAdd: FilterIpssecAddIkeSa success

156 08/07/2002 13:27:14.260 SEV=9 IPSECDBG/6 RPT=38
IPSEC key message parse - msgtype 3, len 335, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 32, label 0, pad 0, spi 26d1dab1, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 21, lifetime2 0, dsId 0

159 08/07/2002 13:27:14.260 SEV=9 IPSECDBG/1 RPT=143
Processing KEY_UPDATE msg!

160 08/07/2002 13:27:14.260 SEV=9 IPSECDBG/1 RPT=144
Update inbound SA addresses

161 08/07/2002 13:27:14.260 SEV=9 IPSECDBG/1 RPT=145
key_msghdr2secassoc(): Enter

162 08/07/2002 13:27:14.260 SEV=7 IPSECDBG/1 RPT=146
No USER filter configured

163 08/07/2002 13:27:14.260 SEV=9 IPSECDBG/1 RPT=147
KeyProcessUpdate: Enter

164 08/07/2002 13:27:14.260 SEV=8 IPSECDBG/1 RPT=148
KeyProcessUpdate: success

165 08/07/2002 13:27:14.260 SEV=8 IKEDBG/7 RPT=8
IKE got a KEY_ADD msg for SA: SPI = 0x2f285111

166 08/07/2002 13:27:14.260 SEV=8 IKEDBG/0 RPT=52336
pitcher: rcv KEY_UPDATE, spi 0x26d1dab1

167 08/07/2002 13:27:14.260 SEV=4 IKE/120 RPT=9 172.18.124.131
Group [172.18.124.131]
PHASE 2 COMPLETED (msgid=201d0d40)

168 08/07/2002 13:27:15.970 SEV=7 IPSECDBG/1 RPT=149
IPSec Inbound SA has received data!

169 08/07/2002 13:27:15.970 SEV=8 IKEDBG/0 RPT=52337
pitcher: rcv KEY_SA_ACTIVE spi 0x26d1dab1

170 08/07/2002 13:27:15.970 SEV=8 IKEDBG/0 RPT=52338
KEY_SA_ACTIVE no old rekey centry found with new spi 0x26d1dab1, mess_id 0x0

Related Information

- [Cisco VPN 3000 Series Concentrator Support Page](#)
- [Cisco VPN 3000 Series Client Support Page](#)
- [IPSec Support Page](#)
- [Technical Support – Cisco Systems](#)

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

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 14, 2008

Document ID: 26286
