通过 IPSec SDI Authentication 5.0 及以上版本配置 Cisco VPN Client到 VPN 3000 集中器的连接

目录

简介

亦称Cisco VPN 3000集中器可以配置通过RSA ACE服务器， Security Dynamics International (SDI)服务器验证Cisco VPN Client。本文可互换使用期限SDI和ACE。

VPN 3000集中器作为ACE客户端。它与在用户数据报协议(UDP)端口5500的ACE服务器联络。本文显示您如何保证ACE服务器、VPN 3000集中器和Cisco VPN Client一起正常运转。如果您的VPN 3000集中器未配置，推荐您首先配置它，不用ACE服务器，并且确保，工作。

Cisco VPN Client的配置和故障排除VPN 3000集中器的是超出本文的范围之外。为了保证配置工作，不用ACE服务器，参考其他文档，例如配置Ipsec- Cisco VPN 3000客户端到VPN 3000集中器。

如果您的VPN 3000集中器以前配置，请使用本文为了修改您的当前配置(工作有或没有SDI)。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本。

- RSA ACE服务器5.0.1 (Windows 2000/NT)
- VPN 3000集中器(3.6.7)
- VPN客户端3.6.3A

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络实际，请保证您了解所有命令潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景理论

本文适用于Cisco VPN 3000客户端(3.6.x)和Cisco VPN Client (3.x)。使用3.0及以上版本版本，您能当前配置单个组的服务器与一个ACE服务器相对定义全局和使用由所有组的单个ACE。不安排单个ACE服务器配置的组，使用定义的ACE服务器全局。

有新的personal identification number (PIN)模式的三种类型在ACE的。VPN 3000集中器支持两第一选择如显示此处。

- 用户选择New PIN。
- 服务器选择New PIN并且通知用户。
- 服务器选择New PIN并且通知用户;用户能更改PIN。

配置

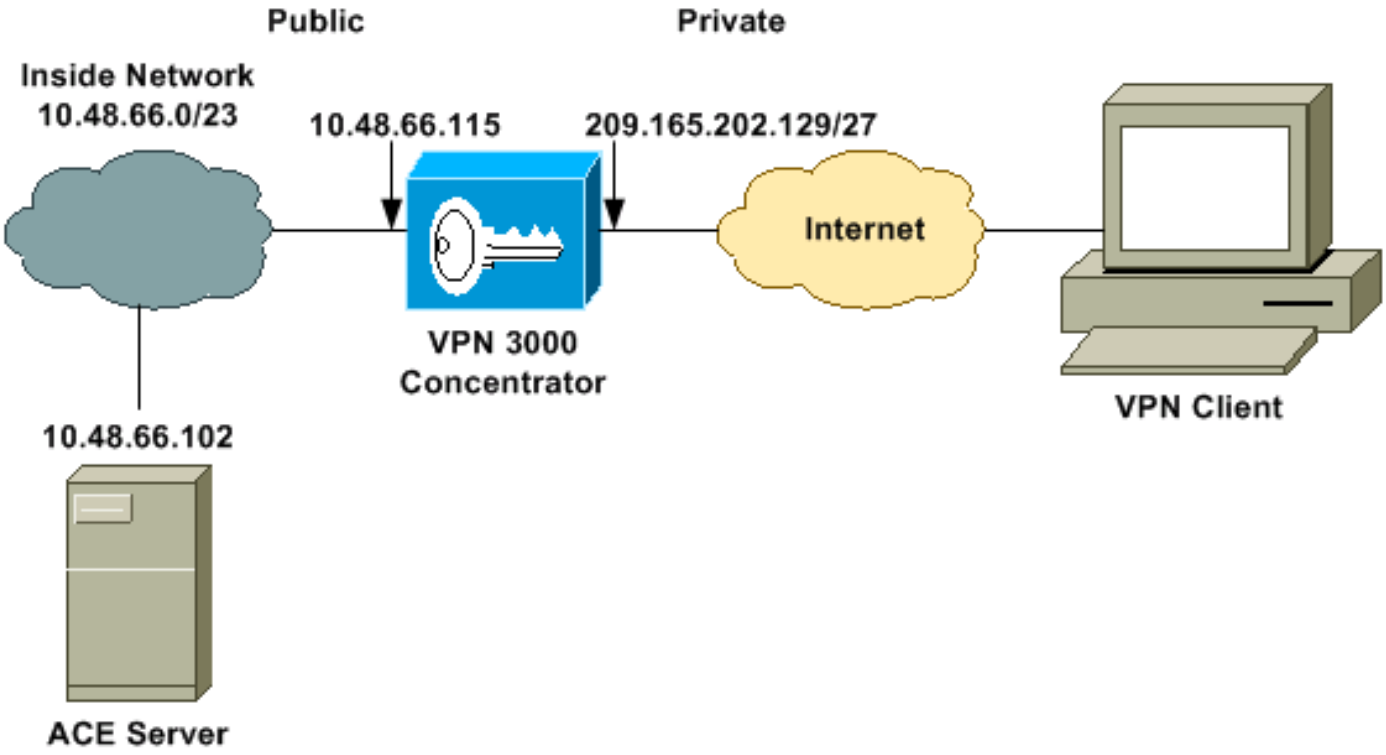
本部分提供用于配置本文档所述功能的信息。

本文档使用以下配置。

- 配置ACE服务器与Cisco VPN 3000集中器谈
- 配置Cisco VPN 3000集中器与ACE服务器谈

网络图

本文档使用此网络设置。



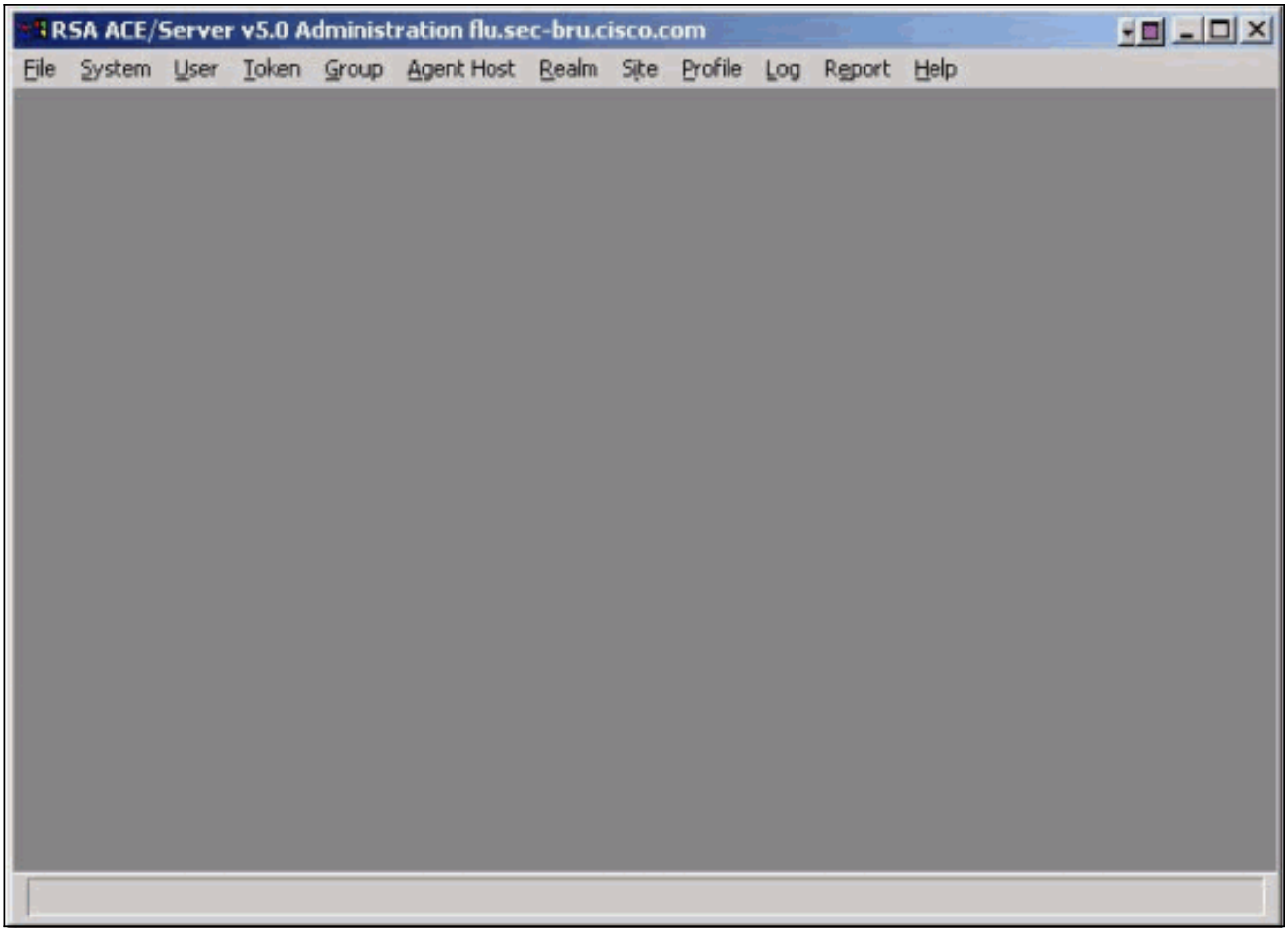
配置 ACE

配置ACE服务器与Cisco VPN 3000集中器谈

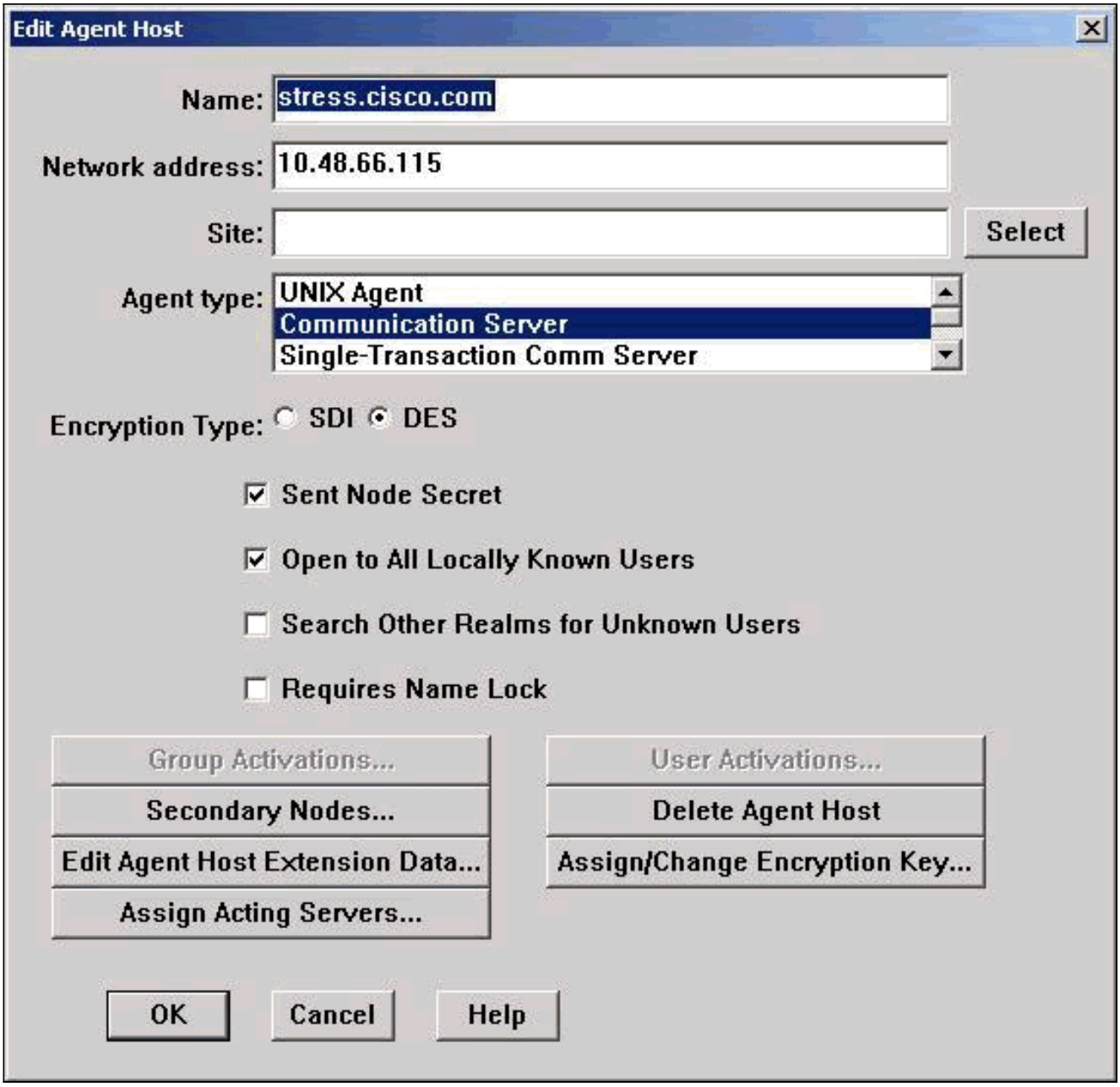
注意： 确保VPN客户端对VPN集中器通信工作(如在介绍上建议)，在您配置ACE服务器到VPN集中器前。

完成这些步骤为了配置ACE服务器与VPN 3000集中器谈。

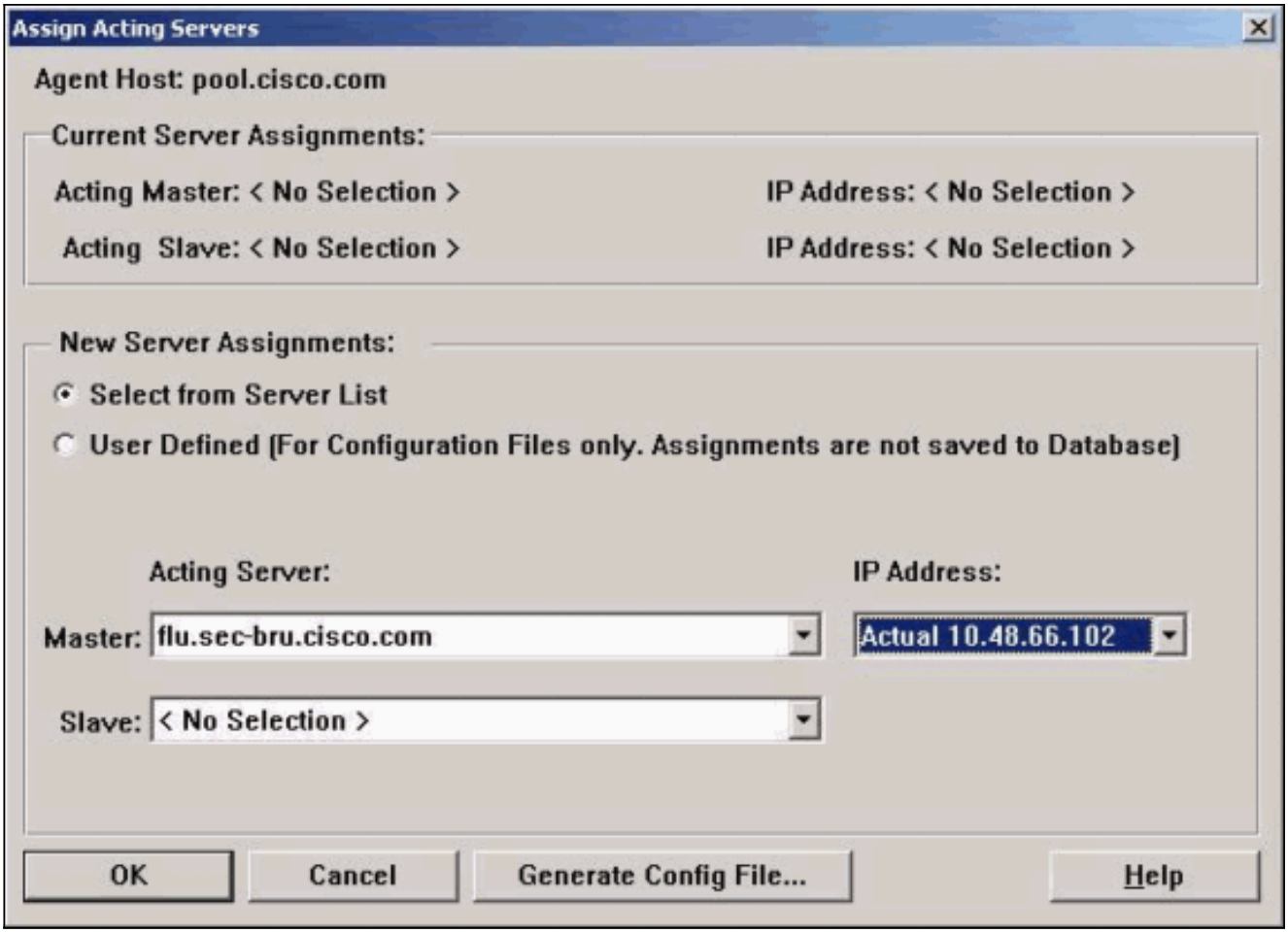
1. 启动ACE管理主机模式应用程序。



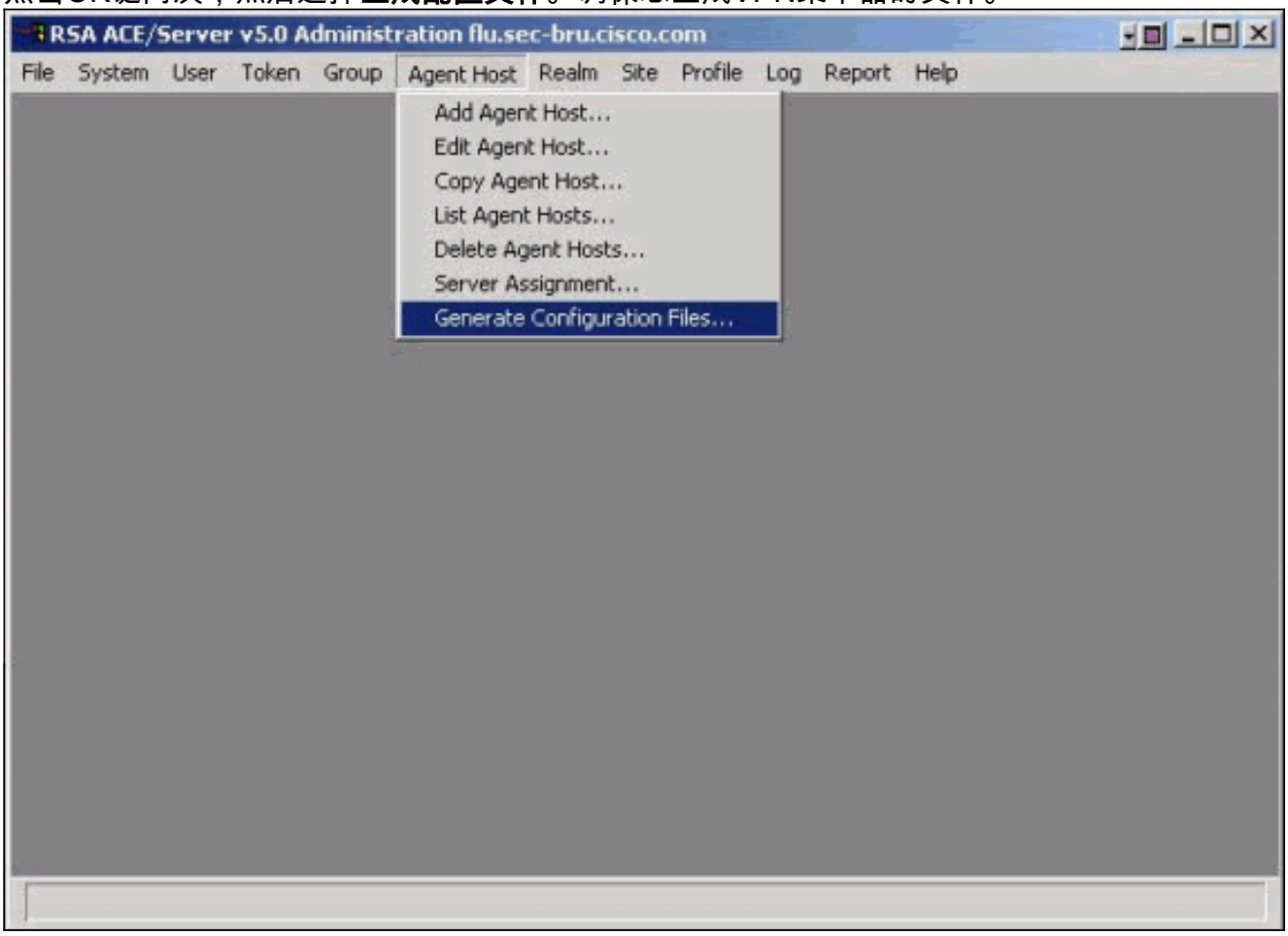
2. 选择**Agent Host > Add Agent Host**。配置主机名，网络地址，代理程序类型(请选择**通信服务器**)，并且选择**开放对所有本地已知用户，**如果希望所有ACE用户能用VPN集中器验证。



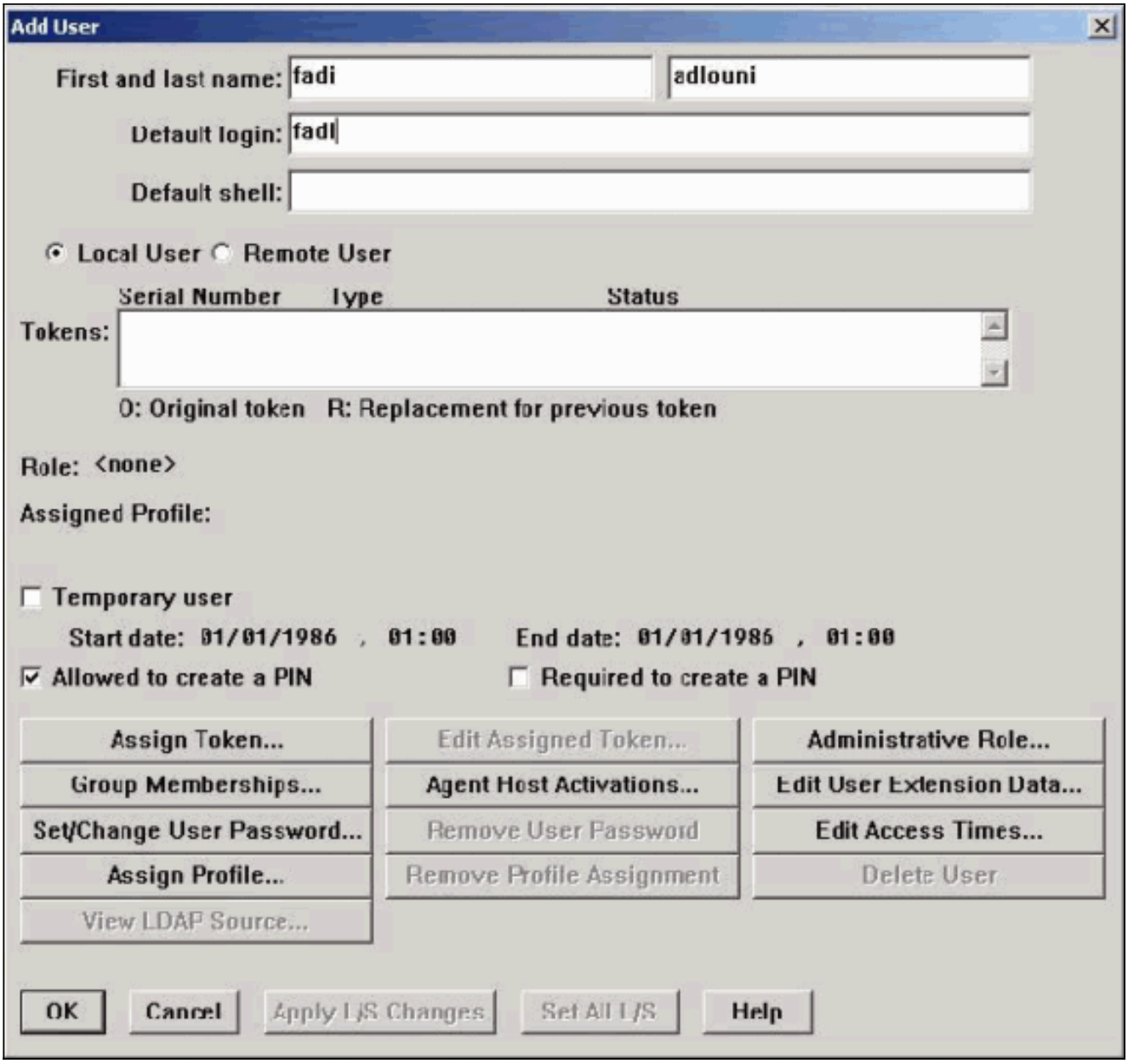
3. 单击**分配代理服务器**并且选择**重要的服务器**(在本例中它是同一个本地ACE服务器)。



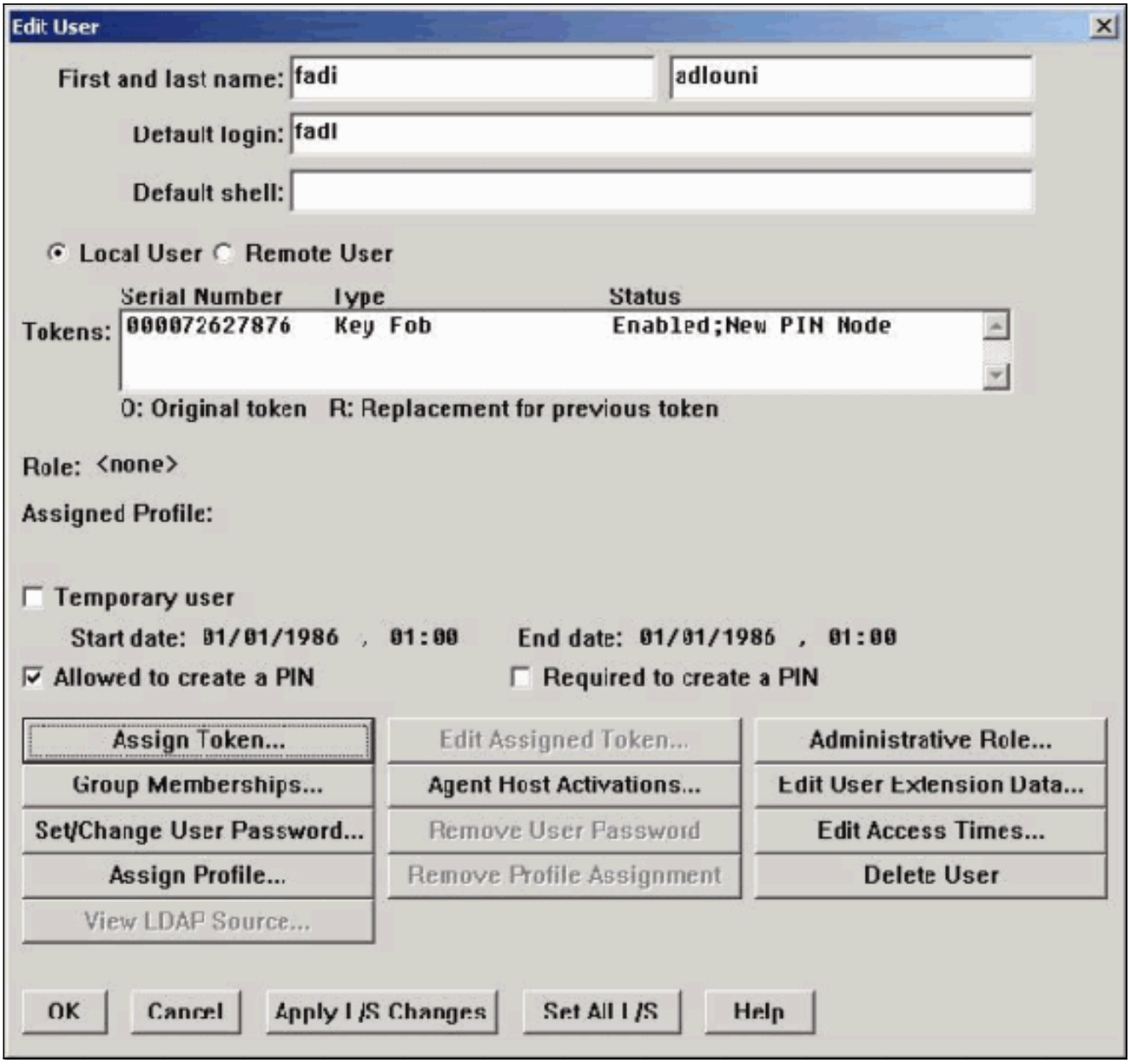
4. 点击OK键两次，然后选择**生成配置文件**。确保您生成VPN集中器的文件。



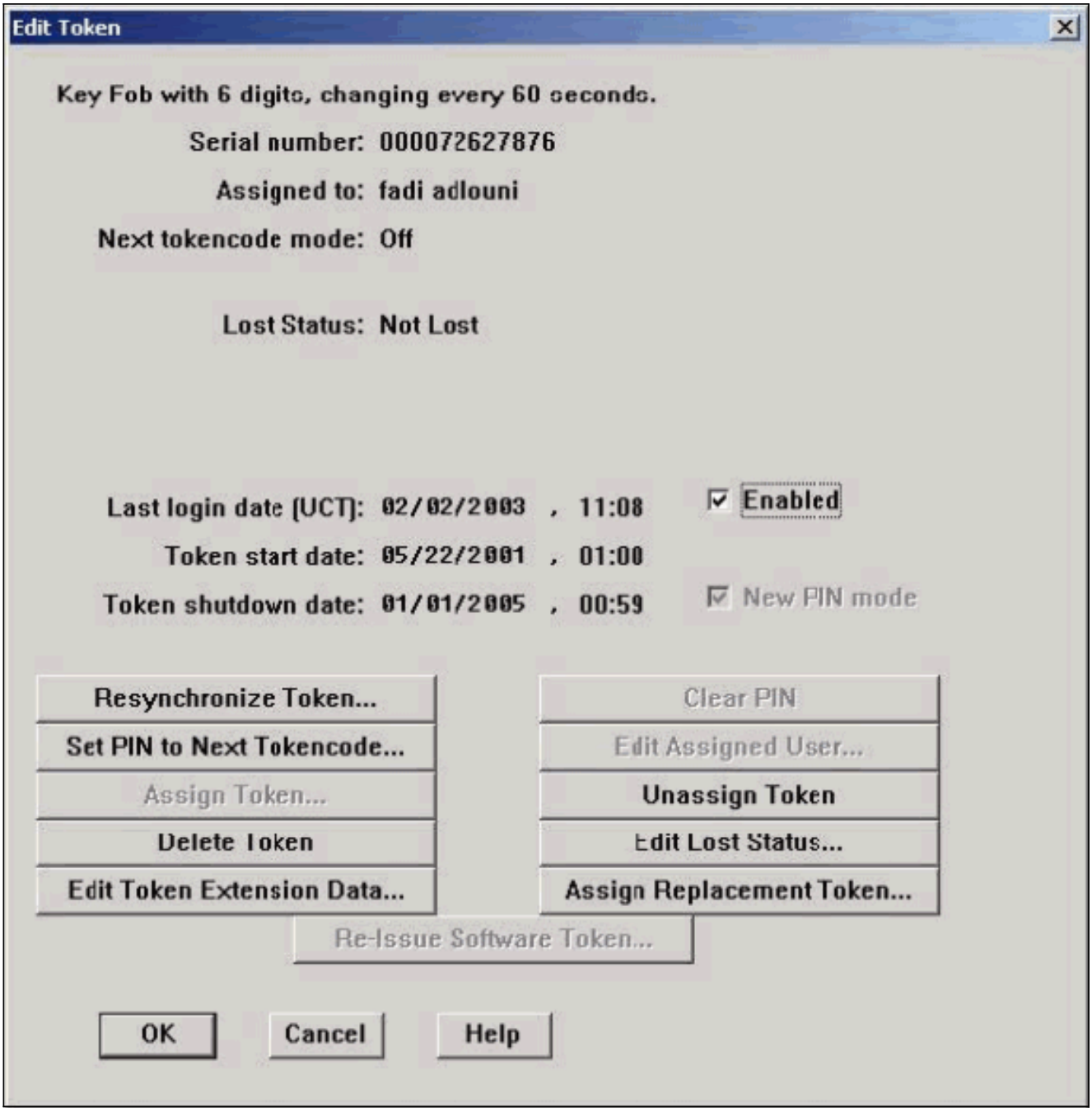
5. 选择**User > Add User**，并且填写字段为了配置用户。



6. 单击**分配标记**并且选择标记。按**OK**，并且您看到一个编号类似那个在此镜像。



7. 选择在令牌方框的标记并且单击**编辑已分配标记**。



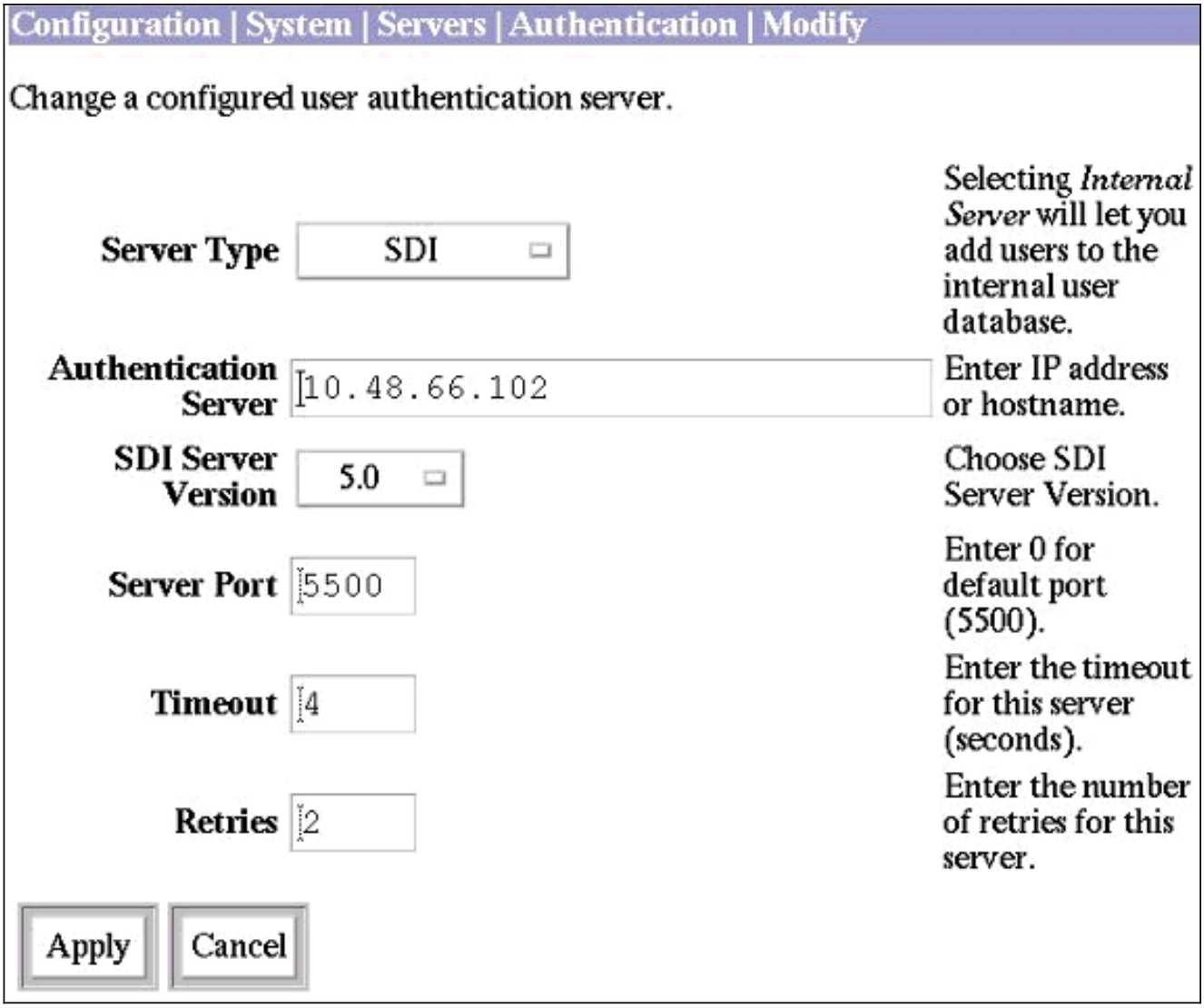
8. 同步标记。如果希望请配置它，则选择**集合PIN对下Tokencode**。

配置Cisco VPN 3000集中器与ACE服务器谈

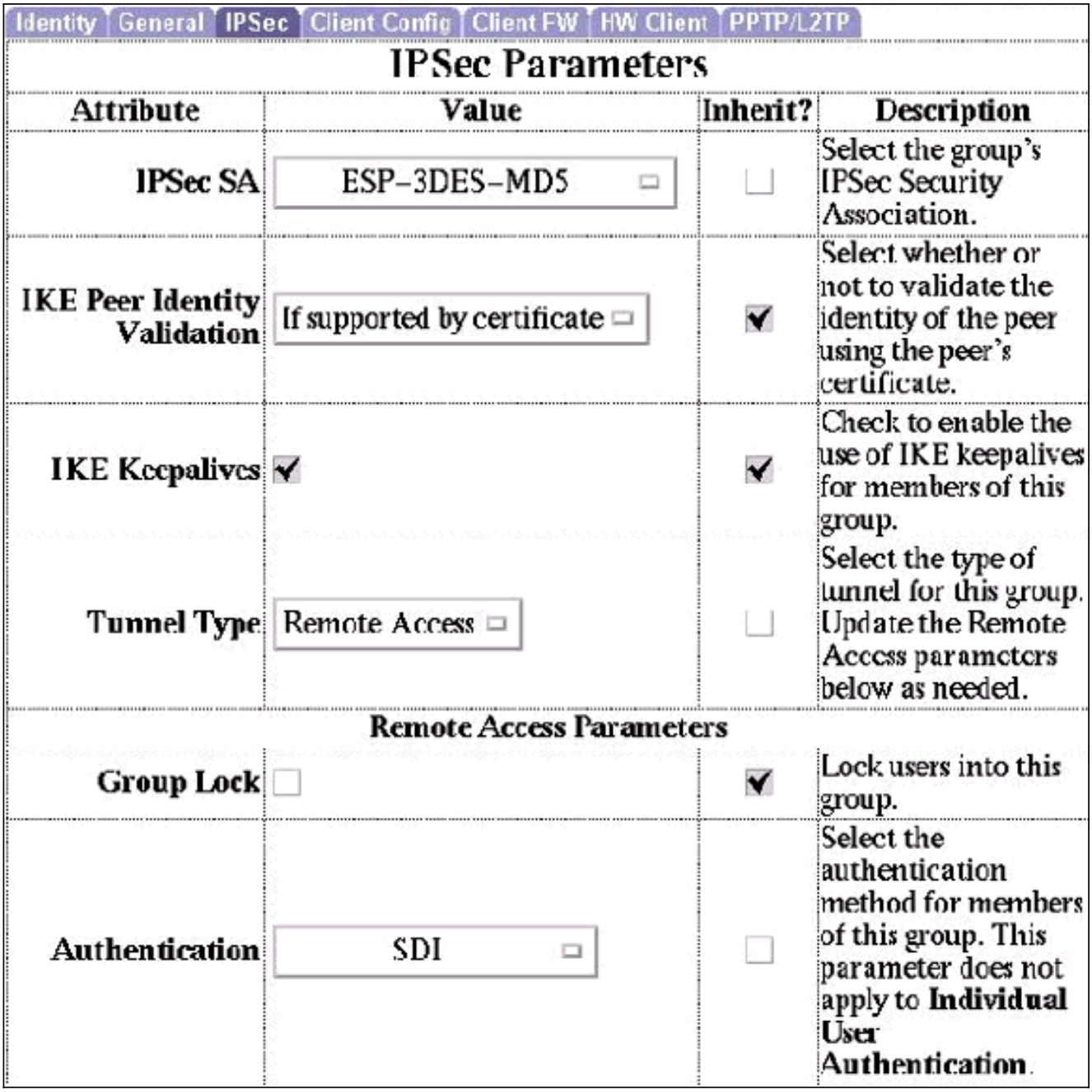
注意： (如果使用ACE 5.0及以上版本)，您能有每组配置的ACE服务器。然而，此示例使用配置的一个ACE服务器全局。

完成这些步骤为了配置Cisco VPN 3000集中器与ACE服务器谈。

1. 选择**Configuration > System > Servers > Authentication**，单击添加，并且配置服务器如执行在此镜像。**注意：** 因为本文讨论SDI 5.0及以上版本，请确保选择SDI服务器版本**5.0**。



2. 单击**应用**，然后选择Configuration > User Management，并且选择用户使用的组。选择**修改组**，然后选择IPSec选项。配置验证对**SDI**。

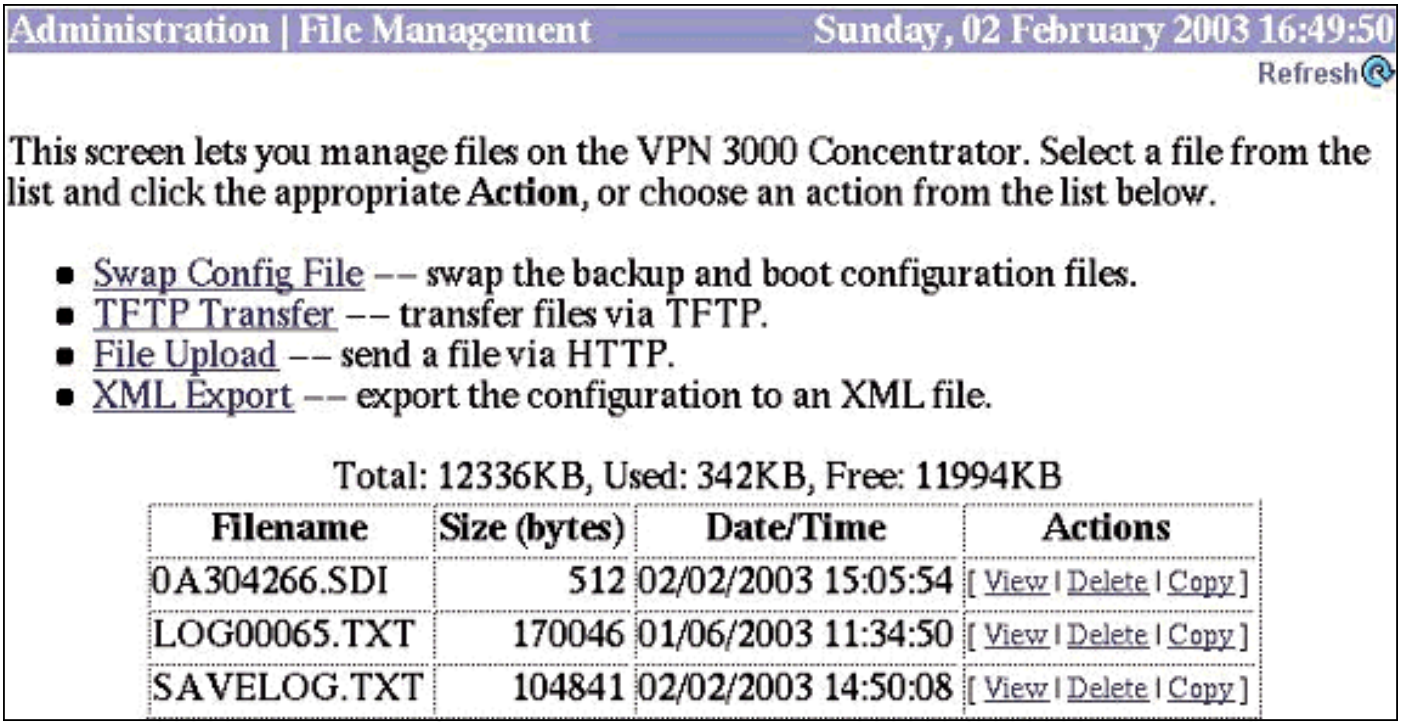


验证

本部分提供可用于确认您的配置是否正常运行的信息。

请使用您为SDI以前配置的同一组，通过VPN客户端连接。

第一次您在VPN客户端帮助下验证， VPN集中器连接对SDI服务器并且创建在其闪存的一个文件与.SDI分机。选择**Administration > File Management**为了检查此文件。



故障排除

本部分提供的信息可用于对配置进行故障排除。

注意： 在发出 **debug** 命令之前，请参阅有关 debug 命令的重要信息。

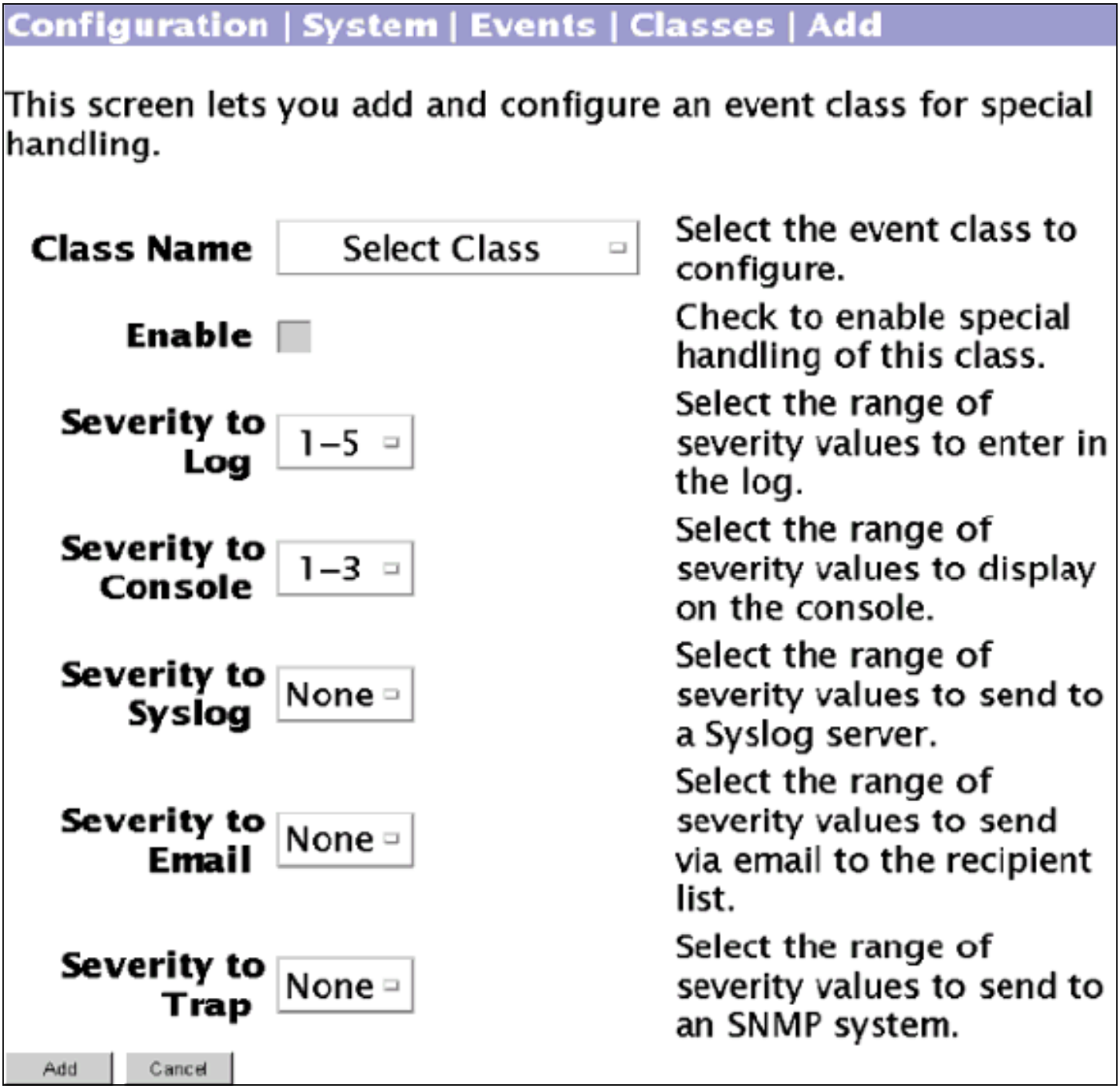
启用调试在VPN 3000集中器

类名称对于验证：

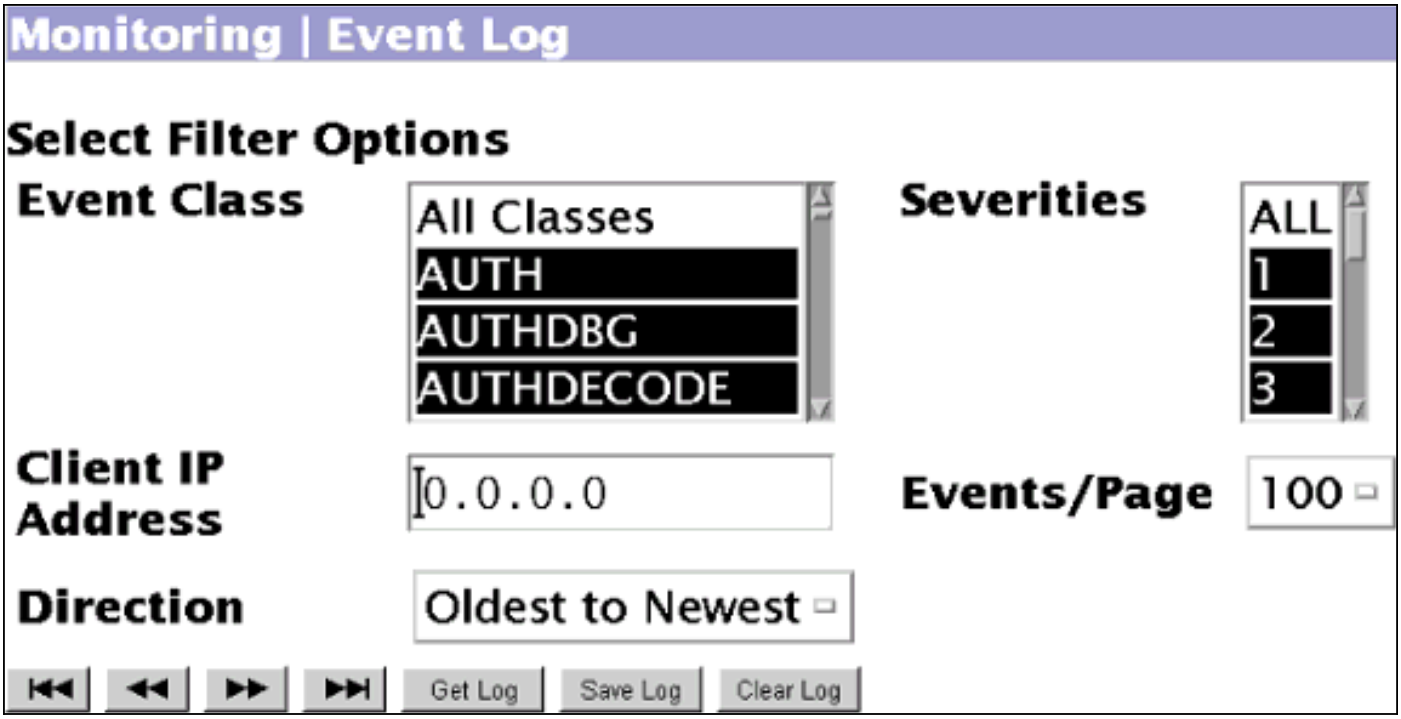
- AUTH
- AUTHDBG
- AUTHDECODE

类名称对于IPSec ：

- IKE， IKEDBG， IKEDECODE
- IPSEC， IPSECDBG， IPSECDECODE
- 对Log=1-9的严重性
- Console的严重性=1-3



选择**获得洛金**命令查看**调试**操作的结果。



与ACE验证的成功调试

```
1 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=1 209.165.202.130
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  5D 2F CC 82 FF 58 F1 18
  Responder Cookie(8):  00 00 00 00 00 00 00 00
  Next Payload  :       SA (1)
  Exchange Type :       Oakley Aggressive Mode
  Flags         :       0
  Message ID    :       0
  Length        :       853

7 02/02/2003 18:14:47.150 SEV=8 IKEDBG/0 RPT=1 209.165.202.130
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + VENDOR (13) + VENDOR
 (13) + VENDOR (13) + VENDOR (13) + NONE (0)
total length : 853

10 02/02/2003 18:14:47.150 SEV=9 IKEDBG/0 RPT=2 209.165.202.130
processing SA payload

11 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=2 209.165.202.130
SA Payload Decode :
  DOI           :       IPSEC (1)
  Situation     :       Identity Only (1)
  Length        :       556

14 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=3 209.165.202.130
Proposal Decode:
  Proposal #    :       1
  Protocol ID   :       ISAKMP (1)
  #of Transforms:       14
  Length        :       544

17 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=4 209.165.202.130
Transform # 1 Decode for Proposal # 1:
  Transform #   :       1
  Transform ID  :       IKE (1)
  Length        :       40
```

```
19 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=5 209.165.202.130
Phase 1 SA Attribute Decode for Transform # 1:
  Encryption Alg:       AES (7)
  Hash Alg      :       SHA (2)
  DH Group      :       Oakley Group 2 (2)
  Auth Method   :       XAUTH with Preshared Key (Initiator authenticated) (65001)
  Life Time     :       2147483 seconds
  Key Length    :       256 Bits (256)

25 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=6 209.165.202.130
Transform # 2 Decode for Proposal # 1:
  Transform #   :       2
  Transform ID  :       IKE (1)
  Length        :       40

27 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=7 209.165.202.130
Phase 1 SA Attribute Decode for Transform # 2:
  Encryption Alg:       AES (7)
  Hash Alg      :       MD5 (1)
  DH Group      :       Oakley Group 2 (2)
  Auth Method   :       XAUTH with Preshared Key (Initiator authenticated) (65001)
  Life Time     :       2147483 seconds
  Key Length    :       256 Bits (256)

33 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=8 209.165.202.130
Transform # 3 Decode for Proposal # 1:
  Transform #   :       3
  Transform ID  :       IKE (1)
  Length        :       40

35 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=9 209.165.202.130
Phase 1 SA Attribute Decode for Transform # 3:
  Encryption Alg:       AES (7)
  Hash Alg      :       SHA (2)
  DH Group      :       Oakley Group 2 (2)
  Auth Method   :       Preshared Key (1)
  Life Time     :       2147483 seconds
  Key Length    :       256 Bits (256)

41 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=10 209.165.202.130
Transform # 4 Decode for Proposal # 1:
  Transform #   :       4
  Transform ID  :       IKE (1)
  Length        :       40

43 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=11 209.165.202.130
Phase 1 SA Attribute Decode for Transform # 4:
  Encryption Alg:       AES (7)
  Hash Alg      :       MD5 (1)
  DH Group      :       Oakley Group 2 (2)
  Auth Method   :       Preshared Key (1)
  Life Time     :       2147483 seconds
  Key Length    :       256 Bits (256)

49 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=12 209.165.202.130
Transform # 5 Decode for Proposal # 1:
  Transform #   :       5
  Transform ID  :       IKE (1)
  Length        :       40

51 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=13 209.165.202.130
Phase 1 SA Attribute Decode for Transform # 5:
  Encryption Alg:       AES (7)
```

```
  Hash Alg      :       SHA (2)
  DH Group      :       Oakley Group 2 (2)
  Auth Method   :       XAUTH with Preshared Key (Initiator authenticated) (65001)
  Life Time     :       2147483 seconds
  Key Length    :       128 Bits (128)

57 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=14 209.165.202.130
Transform # 6 Decode for Proposal # 1:
  Transform #   :       6
  Transform ID  :       IKE (1)
  Length        :       40

59 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=15 209.165.202.130
Phase 1 SA Attribute Decode for Transform # 6:
  Encryption Alg:       AES (7)
  Hash Alg      :       MD5 (1)
  DH Group      :       Oakley Group 2 (2)
  Auth Method   :       XAUTH with Preshared Key (Initiator authenticated) (65001)
  Life Time     :       2147483 seconds
  Key Length    :       128 Bits (128)

65 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=16 209.165.202.130
Transform # 7 Decode for Proposal # 1:
  Transform #   :       7
  Transform ID  :       IKE (1)
  Length        :       40

67 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=17 209.165.202.130
Phase 1 SA Attribute Decode for Transform # 7:
  Encryption Alg:       AES (7)
  Hash Alg      :       SHA (2)
  DH Group      :       Oakley Group 2 (2)
  Auth Method   :       Preshared Key (1)
  Life Time     :       2147483 seconds
  Key Length    :       128 Bits (128)

73 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=18 209.165.202.130
Transform # 8 Decode for Proposal # 1:
  Transform #   :       8
  Transform ID  :       IKE (1)
  Length        :       40

75 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=19 209.165.202.130
Phase 1 SA Attribute Decode for Transform # 8:
  Encryption Alg:       AES (7)
  Hash Alg      :       MD5 (1)
  DH Group      :       Oakley Group 2 (2)
  Auth Method   :       Preshared Key (1)
  Life Time     :       2147483 seconds
  Key Length    :       128 Bits (128)

81 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=20 209.165.202.130
Transform # 9 Decode for Proposal # 1:
  Transform #   :       9
  Transform ID  :       IKE (1)
  Length        :       36

83 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=21 209.165.202.130
Phase 1 SA Attribute Decode for Transform # 9:
  Encryption Alg:       Triple-DES (5)
  Hash Alg      :       SHA (2)
  DH Group      :       Oakley Group 2 (2)
  Auth Method   :       XAUTH with Preshared Key (Initiator authenticated) (65001)
  Life Time     :       2147483 seconds
```

```
89 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=22 209.165.202.130
Transform # 10 Decode for Proposal # 1:
  Transform #   :       10
  Transform ID  :       IKE (1)
  Length        :       36

91 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=23 209.165.202.130
Phase 1 SA Attribute Decode for Transform # 10:
  Encryption Alg:       Triple-DES (5)
  Hash Alg      :       MD5 (1)
  DH Group      :       Oakley Group 2 (2)
  Auth Method   :       XAUTH with Preshared Key (Initiator authenticated) (65001)
  Life Time     :       2147483 seconds

97 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=24 209.165.202.130
Transform # 11 Decode for Proposal # 1:
  Transform #   :       11
  Transform ID  :       IKE (1)
  Length        :       36

99 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=25 209.165.202.130
Phase 1 SA Attribute Decode for Transform # 11:
  Encryption Alg:       Triple-DES (5)
  Hash Alg      :       SHA (2)
  DH Group      :       Oakley Group 2 (2)
  Auth Method   :       Preshared Key (1)
  Life Time     :       2147483 seconds

104 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=26 209.165.202.130
Transform # 12 Decode for Proposal # 1:
  Transform #   :       12
  Transform ID  :       IKE (1)
  Length        :       36

106 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=27 209.165.202.130
Phase 1 SA Attribute Decode for Transform # 12:
  Encryption Alg:       Triple-DES (5)
  Hash Alg      :       MD5 (1)
  DH Group      :       Oakley Group 2 (2)
  Auth Method   :       Preshared Key (1)
  Life Time     :       2147483 seconds

111 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=28 209.165.202.130
Transform # 13 Decode for Proposal # 1:
  Transform #   :       13
  Transform ID  :       IKE (1)
  Length        :       36

113 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=29 209.165.202.130
Phase 1 SA Attribute Decode for Transform # 13:
  Encryption Alg:       DES-CBC (1)
  Hash Alg      :       MD5 (1)
  DH Group      :       Oakley Group 2 (2)
  Auth Method   :       XAUTH with Preshared Key (Initiator authenticated) (65001)
  Life Time     :       2147483 seconds

119 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=30 209.165.202.130
Transform # 14 Decode for Proposal # 1:
  Transform #   :       14
  Transform ID  :       IKE (1)
  Length        :       36

121 02/02/2003 18:14:47.150 SEV=8 IKEDECODE/0 RPT=31 209.165.202.130
```

```
Phase 1 SA Attribute Decode for Transform # 14:
  Encryption Alg:       DES-CBC (1)
  Hash Alg      :       MD5 (1)
  DH Group      :       Oakley Group 2 (2)
  Auth Method   :       Preshared Key (1)
  Life Time     :       2147483 seconds

126 02/02/2003 18:14:47.150 SEV=9 IKEDBG/0 RPT=3 209.165.202.130
processing ke payload

127 02/02/2003 18:14:47.150 SEV=9 IKEDBG/0 RPT=4 209.165.202.130
processing ISA_KE

128 02/02/2003 18:14:47.150 SEV=9 IKEDBG/1 RPT=1 209.165.202.130
processing nonce payload

129 02/02/2003 18:14:47.150 SEV=9 IKEDBG/1 RPT=2 209.165.202.130
Processing ID

130 02/02/2003 18:14:47.150 SEV=9 IKEDBG/47 RPT=1 209.165.202.130
processing VID payload

131 02/02/2003 18:14:47.150 SEV=9 IKEDBG/49 RPT=1 209.165.202.130
Received xauth V6 VID

132 02/02/2003 18:14:47.150 SEV=9 IKEDBG/47 RPT=2 209.165.202.130
processing VID payload

133 02/02/2003 18:14:47.150 SEV=9 IKEDBG/49 RPT=2 209.165.202.130
Received DPD VID

134 02/02/2003 18:14:47.150 SEV=9 IKEDBG/47 RPT=3 209.165.202.130
processing VID payload

135 02/02/2003 18:14:47.150 SEV=9 IKEDBG/49 RPT=3 209.165.202.130
Received NAT-Traversal ver 02 VID

136 02/02/2003 18:14:47.150 SEV=9 IKEDBG/47 RPT=4 209.165.202.130
processing VID payload

137 02/02/2003 18:14:47.150 SEV=9 IKEDBG/49 RPT=4 209.165.202.130
Received Fragmentation VID

138 02/02/2003 18:14:47.150 SEV=5 IKEDBG/64 RPT=2 209.165.202.130
IKE Peer included IKE fragmentation capability flags:
Main Mode:        True
Aggressive Mode:  False

140 02/02/2003 18:14:47.150 SEV=9 IKEDBG/47 RPT=5 209.165.202.130
processing VID payload

141 02/02/2003 18:14:47.150 SEV=9 IKEDBG/49 RPT=5 209.165.202.130
Received Cisco Unity client VID

142 02/02/2003 18:14:47.150 SEV=9 IKEDBG/23 RPT=1 209.165.202.130
Starting group lookup for peer 209.165.202.130

143 02/02/2003 18:14:47.150 SEV=8 AUTHDBG/1 RPT=3
AUTH_Open() returns 2

144 02/02/2003 18:14:47.150 SEV=7 AUTH/12 RPT=3
Authentication session opened: handle = 2

145 02/02/2003 18:14:47.150 SEV=8 AUTHDBG/3 RPT=7
```

```
AUTH_PutAttrTable(2, 8aa824)

146 02/02/2003 18:14:47.150 SEV=8 AUTHDBG/6 RPT=2
AUTH_GroupAuthenticate(2, 55322fc, 578090)

147 02/02/2003 18:14:47.160 SEV=8 AUTHDBG/59 RPT=7
AUTH_BindServer(553ede0, 0, 0)

148 02/02/2003 18:14:47.160 SEV=9 AUTHDBG/69 RPT=7
Auth Server 142f704 has been bound to ACB 553ede0, sessions = 1

149 02/02/2003 18:14:47.160 SEV=8 AUTHDBG/65 RPT=7
AUTH_CreateTimer(553ede0, 0, 0)

150 02/02/2003 18:14:47.160 SEV=9 AUTHDBG/72 RPT=7
Reply timer created: handle = 340019

151 02/02/2003 18:14:47.160 SEV=8 AUTHDBG/179 RPT=7
AUTH_SyncToServer(553ede0, 0, 0)

152 02/02/2003 18:14:47.160 SEV=8 AUTHDBG/180 RPT=6
AUTH_SendLockReq(553ede0, 0, 0)

153 02/02/2003 18:14:47.160 SEV=8 AUTHDBG/61 RPT=7
AUTH_BuildMsg(553ede0, 0, 0)

154 02/02/2003 18:14:47.160 SEV=8 AUTHDBG/64 RPT=7
AUTH_StartTimer(553ede0, 0, 0)

155 02/02/2003 18:14:47.160 SEV=9 AUTHDBG/73 RPT=7
Reply timer started: handle = 340019, timestamp = 93512, timeout = 30000

156 02/02/2003 18:14:47.160 SEV=8 AUTHDBG/62 RPT=7
AUTH_SndRequest(553ede0, 0, 0)

157 02/02/2003 18:14:47.160 SEV=8 AUTHDBG/50 RPT=7
IntDB_Decode(3a38b2c, 144)

158 02/02/2003 18:14:47.160 SEV=8 AUTHDBG/47 RPT=4
IntDB_Xmt(553ede0)

159 02/02/2003 18:14:47.160 SEV=9 AUTHDBG/71 RPT=7
xmit_cnt = 1

160 02/02/2003 18:14:47.160 SEV=8 AUTHDBG/182 RPT=4
IntDB_ServiceRequest(553ede0)

161 02/02/2003 18:14:47.260 SEV=8 AUTHDBG/49 RPT=4
IntDB_Match(553ede0, 3a38d74)

162 02/02/2003 18:14:47.260 SEV=8 AUTHDBG/63 RPT=7
AUTH_RcvReply(553ede0, 0, 0)

163 02/02/2003 18:14:47.260 SEV=8 AUTHDBG/50 RPT=8
IntDB_Decode(3a38d74, 163)

164 02/02/2003 18:14:47.260 SEV=8 AUTHDBG/48 RPT=4
IntDB_Rcv(553ede0)

165 02/02/2003 18:14:47.260 SEV=8 AUTHDBG/66 RPT=7
AUTH_DeleteTimer(553ede0, 0, 0)

166 02/02/2003 18:14:47.260 SEV=9 AUTHDBG/74 RPT=7
Reply timer stopped: handle = 340019, timestamp = 93522
```

167 02/02/2003 18:14:47.260 SEV=8 AUTHDBG/58 RPT=7
AUTH_Callback(553ede0, 0, 0)

!--- Group name . **168 02/02/2003 18:14:47.260 SEV=6 AUTH/41 RPT=4 209.165.202.130 Authentication successful: handle = 2, server = Internal, group = fadigroup 169 02/02/2003 18:14:47.260 SEV=7 IKEDBG/0 RPT=5 209.165.202.130 Group [fadigroup] Found Phase 1 Group (fadigroup) 170 02/02/2003 18:14:47.260 SEV=8 AUTHDBG/4 RPT=8 AUTH_GetAttrTable(2, 8aaad0) 171 02/02/2003 18:14:47.260 SEV=7 IKEDBG/14 RPT=1 209.165.202.130 Group [fadigroup] Authentication configured for SDI 172 02/02/2003 18:14:47.260 SEV=9 IKEDBG/19 RPT=1 209.165.202.130 Group [fadigroup] IKEGetUserAttributes: default domain = cisco.com 173 02/02/2003 18:14:47.260 SEV=9 IKEDBG/19 RPT=2 209.165.202.130 Group [fadigroup] IKEGetUserAttributes: IP Compression = reset 174 02/02/2003 18:14:47.260 SEV=8 AUTHDBG/2 RPT=3 AUTH_Close(2) 175 02/02/2003 18:14:47.260 SEV=9 IKEDBG/0 RPT=6 209.165.202.130 Group [fadigroup] processing IKE SA** 176 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=7 Proposal # 1, Transform # 1, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Rcv'd Key Length attr class, but class is not cfg'd 180 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=8 Phase 1 failure against global IKE proposal # 2: Rcv'd Key Length attr class, but class is not cfg'd 182 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=9 Phase 1 failure against global IKE proposal # 3: Rcv'd Key Length attr class, but class is not cfg'd 184 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=10 Phase 1 failure against global IKE proposal # 4: Rcv'd Key Length attr class, but class is not cfg'd 186 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=11 Phase 1 failure against global IKE proposal # 5: Rcv'd Key Length attr class, but class is not cfg'd 188 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=12 Phase 1 failure against global IKE proposal # 6: Rcv'd Key Length attr class, but class is not cfg'd 190 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=13 Phase 1 failure against global IKE proposal # 7: Rcv'd Key Length attr class, but class is not cfg'd 192 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=14 Phase 1 failure against global IKE proposal # 8: Mismatched attr types for class Key Length: Rcv'd: 256 Bits Cfg'd: 128 Bits 195 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=15 Phase 1 failure against global IKE proposal # 9: Mismatched attr types for class Key Length: Rcv'd: 256 Bits Cfg'd: 128 Bits 198 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=16 Proposal # 1, Transform # 2, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Rcv'd Key Length attr class, but class is not cfg'd 202 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=17 Phase 1 failure against global IKE proposal # 2: Rcv'd Key Length attr class, but class is not cfg'd 204 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=18 Phase 1 failure against global IKE proposal # 3: Rcv'd Key Length attr class, but class is not cfg'd 206 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=19 Phase 1 failure against global IKE proposal # 4: Rcv'd Key Length attr class, but class is not cfg'd 208 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=20 Phase 1 failure against global IKE proposal # 5: Rcv'd Key Length attr class, but class is not cfg'd 210 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=21 Phase 1 failure against global IKE proposal # 6: Rcv'd Key Length attr class, but class is not cfg'd 212 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=22 Phase 1 failure against global IKE proposal # 7: Rcv'd Key Length attr class, but class is not cfg'd 214 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=23 Phase 1 failure against global IKE proposal # 8: Mismatched attr types for class Key Length: Rcv'd: 256 Bits Cfg'd: 128 Bits 217 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=24 Phase 1 failure against global IKE proposal # 9: Mismatched attr types for class Key Length: Rcv'd: 256 Bits Cfg'd: 128 Bits 220 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=25 Proposal # 1, Transform # 3, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Rcv'd Key Length attr class, but class is not cfg'd 224 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=26 Phase 1 failure against global IKE proposal # 2: Rcv'd Key Length attr class, but class is not cfg'd 226 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=27 Phase 1 failure against global IKE proposal # 3: Rcv'd Key Length attr class, but class is not cfg'd 228 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=28 Phase 1 failure against global IKE proposal # 4: Rcv'd Key Length attr class, but class is not cfg'd 230 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=29 Phase 1 failure against global IKE proposal # 5: Rcv'd Key Length attr class, but class is not cfg'd 232 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=30 Phase 1 failure against global IKE proposal # 6: Rcv'd Key Length attr class, but class is not cfg'd 234 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=31 Phase 1 failure against global IKE proposal # 7: Rcv'd Key Length attr class, but class is not cfg'd 236 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=32 Phase 1 failure against global IKE proposal # 8: Mismatched attr types for class Key Length: Rcv'd: 256 Bits Cfg'd: 128 Bits 239 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=33 Phase 1 failure against global IKE proposal # 9: Mismatched attr types for class Key Length: Rcv'd: 256 Bits Cfg'd: 128 Bits 242 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=34 Proposal # 1, Transform # 4, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Rcv'd Key Length attr class, but

class is not cfg'd 246 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=35 Phase 1 failure against global IKE proposal # 2: Rcv'd Key Length attr class, but class is not cfg'd 248 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=36 Phase 1 failure against global IKE proposal # 3: Rcv'd Key Length attr class, but class is not cfg'd 250 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=37 Phase 1 failure against global IKE proposal # 4: Rcv'd Key Length attr class, but class is not cfg'd 252 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=38 Phase 1 failure against global IKE proposal # 5: Rcv'd Key Length attr class, but class is not cfg'd 254 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=39 Phase 1 failure against global IKE proposal # 6: Rcv'd Key Length attr class, but class is not cfg'd 256 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=40 Phase 1 failure against global IKE proposal # 7: Rcv'd Key Length attr class, but class is not cfg'd 258 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=41 Phase 1 failure against global IKE proposal # 8: Mismatched attr types for class Key Length: Rcv'd: 256 Bits Cfg'd: 128 Bits 261 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=42 Phase 1 failure against global IKE proposal # 9: Mismatched attr types for class Key Length: Rcv'd: 256 Bits Cfg'd: 128 Bits 264 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=43 Proposal # 1, Transform # 5, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Rcv'd Key Length attr class, but class is not cfg'd 268 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=44 Phase 1 failure against global IKE proposal # 2: Rcv'd Key Length attr class, but class is not cfg'd 270 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=45 Phase 1 failure against global IKE proposal # 3: Rcv'd Key Length attr class, but class is not cfg'd 272 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=46 Phase 1 failure against global IKE proposal # 4: Rcv'd Key Length attr class, but class is not cfg'd 274 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=47 Phase 1 failure against global IKE proposal # 5: Rcv'd Key Length attr class, but class is not cfg'd 276 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=48 Phase 1 failure against global IKE proposal # 6: Rcv'd Key Length attr class, but class is not cfg'd 278 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=49 Phase 1 failure against global IKE proposal # 7: Rcv'd Key Length attr class, but class is not cfg'd 280 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=50 Proposal # 1, Transform # 6, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Rcv'd Key Length attr class, but class is not cfg'd 284 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=51 Phase 1 failure against global IKE proposal # 2: Rcv'd Key Length attr class, but class is not cfg'd 286 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=52 Phase 1 failure against global IKE proposal # 3: Rcv'd Key Length attr class, but class is not cfg'd 288 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=53 Phase 1 failure against global IKE proposal # 4: Rcv'd Key Length attr class, but class is not cfg'd 290 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=54 Phase 1 failure against global IKE proposal # 5: Rcv'd Key Length attr class, but class is not cfg'd 292 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=55 Phase 1 failure against global IKE proposal # 6: Rcv'd Key Length attr class, but class is not cfg'd 294 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=56 Phase 1 failure against global IKE proposal # 7: Rcv'd Key Length attr class, but class is not cfg'd 296 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=57 Phase 1 failure against global IKE proposal # 8: Mismatched attr types for class Hash Alg: Rcv'd: MD5 Cfg'd: SHA 298 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=58 Phase 1 failure against global IKE proposal # 9: Mismatched attr types for class Hash Alg: Rcv'd: MD5 Cfg'd: SHA 300 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=59 Proposal # 1, Transform # 7, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Rcv'd Key Length attr class, but class is not cfg'd 304 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=60 Phase 1 failure against global IKE proposal # 2: Rcv'd Key Length attr class, but class is not cfg'd 306 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=61 Phase 1 failure against global IKE proposal # 3: Rcv'd Key Length attr class, but class is not cfg'd 308 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=62 Phase 1 failure against global IKE proposal # 4: Rcv'd Key Length attr class, but class is not cfg'd 310 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=63 Phase 1 failure against global IKE proposal # 5: Rcv'd Key Length attr class, but class is not cfg'd 312 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=64 Phase 1 failure against global IKE proposal # 6: Rcv'd Key Length attr class, but class is not cfg'd 314 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=65 Phase 1 failure against global IKE proposal # 7: Rcv'd Key Length attr class, but class is not cfg'd 316 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=66 Phase 1 failure against global IKE proposal # 8: Mismatched attr types for class Auth Method: Rcv'd: Preshared Key Cfg'd: XAUTH with Preshared Key (Initiator authenticated) 320 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=67 Proposal # 1, Transform # 8, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Rcv'd Key Length attr class, but class is not cfg'd 324 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=68 Phase 1 failure against global IKE proposal # 2: Rcv'd Key Length attr class, but class is not cfg'd 326 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=69 Phase 1 failure against global IKE proposal # 3: Rcv'd Key Length attr class, but class is not cfg'd 328 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=70 Phase 1 failure against global IKE proposal # 4: Rcv'd Key Length attr class, but class is not cfg'd 330 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=71

Phase 1 failure against global IKE proposal # 5: Rcv'd Key Length attr class, but class is not cfg'd 332 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=72 Phase 1 failure against global IKE proposal # 6: Rcv'd Key Length attr class, but class is not cfg'd 334 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=73 Phase 1 failure against global IKE proposal # 7: Rcv'd Key Length attr class, but class is not cfg'd 336 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=74 Phase 1 failure against global IKE proposal # 8: Mismatched attr types for class Hash Alg: Rcv'd: MD5 Cfg'd: SHA 338 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=75 Phase 1 failure against global IKE proposal # 9: Mismatched attr types for class Hash Alg: Rcv'd: MD5 Cfg'd: SHA 340 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=76 Proposal # 1, Transform # 9, 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 344 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=77 Phase 1 failure against global IKE proposal # 2: Mismatched attr types for class Hash Alg: Rcv'd: SHA Cfg'd: MD5 346 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=78 Phase 1 failure against global IKE proposal # 3: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1 349 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=79 Phase 1 failure against global IKE proposal # 4: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1 352 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=80 Phase 1 failure against global IKE proposal # 5: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 7 355 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=81 Phase 1 failure against global IKE proposal # 6: Mismatched attr types for class Hash Alg: Rcv'd: SHA Cfg'd: MD5 357 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=82 Phase 1 failure against global IKE proposal # 7: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 5 360 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=83 Phase 1 failure against global IKE proposal # 8: Mismatched attr types for class Encryption Alg: Rcv'd: Triple-DES Cfg'd: AES 363 02/02/2003 18:14:47.260 SEV=8 IKEDBG/0 RPT=84 Phase 1 failure against global IKE proposal # 9: Mismatched attr types for class Encryption Alg: Rcv'd: Triple-DES Cfg'd: AES 366 02/02/2003 18:14:47.260 SEV=7 IKEDBG/28 RPT=1 209.165.202.130 Group [fadigroup] IKE SA Proposal # 1, Transform # 10 acceptable Matches global IKE entry # 1 368 02/02/2003 18:14:47.260 SEV=8 AUTHDBG/60 RPT=7 AUTH_UnbindServer(553ede0, 0, 0) 369 02/02/2003 18:14:47.260 SEV=9 AUTHDBG/70 RPT=7 Auth Server 142f704 has been unbound from ACB 553ede0, sessions = 0 370 02/02/2003 18:14:47.260 SEV=8 AUTHDBG/10 RPT=3 AUTH_Int_FreeAuthCB(553ede0) 371 02/02/2003 18:14:47.260 SEV=7 AUTH/13 RPT=3 Authentication session closed: handle = 2 372 02/02/2003 18:14:47.290 SEV=9 IKEDBG/0 RPT=85 209.165.202.130 Group [fadigroup] constructing ISA_SA for isakmp 373 02/02/2003 18:14:47.290 SEV=9 IKEDBG/0 RPT=86 209.165.202.130 Group [fadigroup] constructing ke payload 374 02/02/2003 18:14:47.290 SEV=9 IKEDBG/1 RPT=3 209.165.202.130 Group [fadigroup] constructing nonce payload 375 02/02/2003 18:14:47.290 SEV=9 IKEDBG/0 RPT=87 209.165.202.130 Group [fadigroup] Generating keys for Responder... 376 02/02/2003 18:14:47.300 SEV=9 IKEDBG/1 RPT=4 209.165.202.130 Group [fadigroup] constructing ID 377 02/02/2003 18:14:47.300 SEV=9 IKEDBG/0 RPT=88 Group [fadigroup] construct hash payload 378 02/02/2003 18:14:47.300 SEV=9 IKEDBG/0 RPT=89 209.165.202.130 Group [fadigroup] computing hash 379 02/02/2003 18:14:47.300 SEV=9 IKEDBG/46 RPT=1 209.165.202.130 Group [fadigroup] constructing Cisco Unity VID payload 380 02/02/2003 18:14:47.300 SEV=9 IKEDBG/46 RPT=2 209.165.202.130 Group [fadigroup] constructing xauth V6 VID payload 381 02/02/2003 18:14:47.300 SEV=9 IKEDBG/46 RPT=3 209.165.202.130 Group [fadigroup] constructing dpd vid payload 382 02/02/2003 18:14:47.300 SEV=9 IKEDBG/46 RPT=4 209.165.202.130 Group [fadigroup] constructing Fragmentation VID + extended capabilities payload 383 02/02/2003 18:14:47.300 SEV=9 IKEDBG/46 RPT=5 209.165.202.130 Group [fadigroup] constructing VID payload 384 02/02/2003 18:14:47.300 SEV=9 IKEDBG/48 RPT=1 209.165.202.130 Group [fadigroup] Send Altiga GW VID 385 02/02/2003 18:14:47.300 SEV=8 IKEDBG/0 RPT=90 209.165.202.130 SENDING Message (msgid=0) with payloads : HDR + SA (1) + KE (4) total length : 368 387 02/02/2003 18:14:47.340 SEV=8 IKEDECODE/0 RPT=32 209.165.202.130 ISAKMP HEADER : (Version 1.0) Initiator Cookie(8): 5D 2F CC 82 FF 58 F1 18 Responder Cookie(8): 91 AC 22 89 C5 69 60 92 Next Payload : HASH (8) Exchange Type : Oakley Aggressive Mode Flags : 1 (ENCRYPT) Message ID : 0 Length : 76 393 02/02/2003 18:14:47.340 SEV=8 IKEDBG/0 RPT=91 209.165.202.130 RECEIVED Message (msgid=0) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 76 395 02/02/2003 18:14:47.340 SEV=9 IKEDBG/0 RPT=92 209.165.202.130 Group [fadigroup] processing hash 396 02/02/2003 18:14:47.340 SEV=9 IKEDBG/0 RPT=93 209.165.202.130 Group [fadigroup] computing hash 397 02/02/2003 18:14:47.340 SEV=9 IKEDBG/0 RPT=94 209.165.202.130 Group [fadigroup] Processing Notify payload 398 02/02/2003 18:14:47.340 SEV=8 IKEDECODE/0 RPT=33 209.165.202.130 Notify Payload Decode : DOI : IPSEC (1) Protocol : ISAKMP (1) Message : Initial contact (24578) Spi : 5D 2F CC 82 FF 58 F1 18 91 AC 22 89 C5 69 60 92 Length : 28 404 02/02/2003 18:14:47.340 SEV=9 IKEDBG/0 RPT=95 209.165.202.130 Group [fadigroup] constructing blank hash 405 02/02/2003 18:14:47.340 SEV=9 IKEDBG/0 RPT=96 209.165.202.130 Group [fadigroup] constructing qm hash 406 02/02/2003 18:14:47.340 SEV=8 IKEDBG/0 RPT=97 209.165.202.130 SENDING Message (msgid=b1fa6c1c) with payloads : HDR + HASH (8) + ATTR (14) total length : 104 408 02/02/2003 18:14:54.890 SEV=8

IKEDECODE/0 RPT=34 209.165.202.130 ISAKMP HEADER : (Version 1.0) Initiator Cookie(8): 5D 2F CC 82 FF 58 F1 18 Responder Cookie(8): 91 AC 22 89 C5 69 60 92 Next Payload : HASH (8) Exchange Type : Oakley Transactional Flags : 1 (ENCRYPT) Message ID : b1fa6c1c Length : 92 415 02/02/2003 18:14:54.890 SEV=8 IKEDBG/0 RPT=98 209.165.202.130 RECEIVED Message (msgid=b1fa6c1c) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 86 417 02/02/2003 18:14:54.890 SEV=9 IKEDBG/1 RPT=5 process_attr(): Enter! 418 02/02/2003 18:14:54.890 SEV=9 IKEDBG/1 RPT=6 Processing MODE_CFG Reply attributes. 419 02/02/2003 18:14:54.890 SEV=8 AUTHDBG/1 RPT=4 AUTH_Open() returns 3 420 02/02/2003 18:14:54.890 SEV=7 AUTH/12 RPT=4 Authentication session opened: handle = 3 421 02/02/2003 18:14:54.890 SEV=8 AUTHDBG/3 RPT=8 AUTH_PutAttrTable(3, 8aa824) 422 02/02/2003 18:14:54.890 SEV=8 AUTHDBG/5 RPT=4 AUTH_Authenticate(3, 30594a4, 5b15c4) 423 02/02/2003 18:14:54.890 SEV=8 AUTHDBG/59 RPT=8 AUTH_BindServer(5566340, 0, 0) 424 02/02/2003 18:14:54.890 SEV=9 AUTHDBG/69 RPT=8 Auth Server 142f914 has been bound to ACB 5566340, sessions = 1 425 02/02/2003 18:14:54.890 SEV=8 AUTHDBG/65 RPT=8 AUTH_CreateTimer(5566340, 0, 0) 426 02/02/2003 18:14:54.890 SEV=9 AUTHDBG/72 RPT=8 Reply timer created: handle = 360016 427 02/02/2003 18:14:54.890 SEV=8 AUTHDBG/179 RPT=8 AUTH_SyncToServer(5566340, 0, 0) *!--- Initializes SDI.* **428 02/02/2003 18:14:54.890 SEV=8 AUTHDBG/177 RPT=4 Sdi_init(5566340)** 429 02/02/2003 18:14:54.890 SEV=8 AUTHDBG/180 RPT=7 AUTH_SendLockReq(5566340, 0, 0) 430 02/02/2003 18:14:54.890 SEV=8 AUTHDBG/178 RPT=3 Sdi_lock(5566340) 431 02/02/2003 18:14:54.890 SEV=9 AUTHDBG/169 RPT=2 Ace Agent building lock name request pkt ... 432 02/02/2003 18:14:54.890 SEV=5 AUTH/72 RPT=1 Setting server priority: idx: 0, addr: 10.48.66.102, priority: 7, proximity: 2 433 02/02/2003 18:14:54.890 SEV=5 AUTH/70 RPT=1 Adding ACE server 10.48.66.102 in the select table, idx : 0, priority : 7 434 02/02/2003 18:14:54.890 SEV=9 AUTHDBG/174 RPT=6 Ace Agent transmitting to server 10.48.66.102 435 02/02/2003 18:14:54.900 SEV=8 AUTHDBG/61 RPT=8 AUTH_BuildMsg(5566340, 0, 0) 436 02/02/2003 18:14:54.900 SEV=8 AUTHDBG/51 RPT=4 Sdi_Build(5566340) 437 02/02/2003 18:14:54.900 SEV=8 AUTHDBG/64 RPT=8 AUTH_StartTimer(5566340, 0, 0) 438 02/02/2003 18:14:54.900 SEV=9 AUTHDBG/73 RPT=8 Reply timer started: handle = 360016, timestamp = 94286, timeout = 4000 439 02/02/2003 18:14:54.900 SEV=8 AUTHDBG/62 RPT=8 AUTH_SndRequest(5566340, 0, 0) 440 02/02/2003 18:14:54.900 SEV=8 AUTHDBG/52 RPT=4 Sdi_Xmt(5566340) 441 02/02/2003 18:14:54.900 SEV=9 AUTHDBG/71 RPT=8 xmit_cnt = 2 442 02/02/2003 18:14:54.900 SEV=9 AUTHDBG/170 RPT=3 Ace Agent building auth request pkt ... *!--- Sends authentication request to the ACE server.* **443 02/02/2003 18:14:54.910 SEV=9 AUTHDBG/174 RPT=7 Ace Agent transmitting to server 10.48.66.102 444 02/02/2003 18:14:56.910 SEV=8 AUTHDBG/63 RPT=8 AUTH_RcvReply(5566340, 0, 0) 445 02/02/2003 18:14:56.910 SEV=8 AUTHDBG/53 RPT=4 Sdi_Rcv(5566340) 446 02/02/2003 18:14:56.910 SEV=8 AUTHDBG/66 RPT=8 AUTH_DeleteTimer(5566340, 0, 0) 447 02/02/2003 18:14:56.910 SEV=9 AUTHDBG/74 RPT=8 Reply timer stopped: handle = 360016, timestamp = 94487 448 02/02/2003 18:14:56.910 SEV=8 AUTHDBG/58 RPT=8 AUTH_Callback(5566340, 0, 0) 449 02/02/2003 18:14:56.910 SEV=5 AUTH/77 RPT=4 Primary server: 10.48.66.102, Authenticator: 10.48.66.102** *!--- The authentication is successful* . **450 02/02/2003 18:14:56.910 SEV=6 AUTH/4 RPT=2 209.165.202.130 Authentication successful: handle = 3, server = 10.48.66.102, user = fadi** 451 02/02/2003 18:14:56.910 SEV=8 AUTHDBG/3 RPT=9 AUTH_PutAttrTable(3, 15293d4) 452 02/02/2003 18:14:56.910 SEV=8 AUTHDBG/60 RPT=8 AUTH_UnbindServer(5566340, 0, 0) 453 02/02/2003 18:14:56.910 SEV=9 AUTHDBG/70 RPT=8 Auth Server 142f914 has been unbound from ACB 5566340, sessions = 0 454 02/02/2003 18:14:56.910 SEV=8 AUTHDBG/59 RPT=9 AUTH_BindServer(5566340, 0, 0) 455 02/02/2003 18:14:56.910 SEV=9 AUTHDBG/69 RPT=9 Auth Server 142f704 has been bound to ACB 5566340, sessions = 1 456 02/02/2003 18:14:56.910 SEV=8 AUTHDBG/65 RPT=9 AUTH_CreateTimer(5566340, 0, 0) 457 02/02/2003 18:14:56.910 SEV=9 AUTHDBG/72 RPT=9 Reply timer created: handle = 370016 458 02/02/2003 18:14:56.910 SEV=8 AUTHDBG/179 RPT=9 AUTH_SyncToServer(5566340, 0, 0) 459 02/02/2003 18:14:56.910 SEV=8 AUTHDBG/180 RPT=8 AUTH_SendLockReq(5566340, 0, 0) 460 02/02/2003 18:14:56.910 SEV=8 AUTHDBG/61 RPT=9 AUTH_BuildMsg(5566340, 0, 0) 461 02/02/2003 18:14:56.910 SEV=8 AUTHDBG/64 RPT=9 AUTH_StartTimer(5566340, 0, 0) 462 02/02/2003 18:14:56.910 SEV=9 AUTHDBG/73 RPT=9 Reply timer started: handle = 370016, timestamp = 94487, timeout = 30000 463 02/02/2003 18:14:56.910 SEV=8 AUTHDBG/62 RPT=9 AUTH_SndRequest(5566340, 0, 0) 464 02/02/2003 18:14:56.910 SEV=8 AUTHDBG/50 RPT=9 IntDB_Decode(28305c8, 52) 465 02/02/2003 18:14:56.910 SEV=8 AUTHDBG/47 RPT=5 IntDB_Xmt(5566340) 466 02/02/2003 18:14:56.910 SEV=9 AUTHDBG/71 RPT=9 xmit_cnt = 1 467 02/02/2003 18:14:56.910 SEV=8 AUTHDBG/182 RPT=5 IntDB_ServiceRequest(5566340) 468 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/49 RPT=5 IntDB_Match(5566340, 3a3944c) 469 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/63 RPT=9 AUTH_RcvReply(5566340, 0, 0) 470 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/50 RPT=10 IntDB_Decode(3a3944c, 163) 471 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/48 RPT=5 IntDB_Rcv(5566340) 472 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/66 RPT=9 AUTH_DeleteTimer(5566340, 0, 0) 473 02/02/2003 18:14:57.010 SEV=9 AUTHDBG/74 RPT=9 Reply timer stopped: handle = 370016, timestamp = 94497 474 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/58 RPT=9 AUTH_Callback(5566340, 0, 0) 475 02/02/2003 18:14:57.010 SEV=6 AUTH/41 RPT=5 209.165.202.130 Authentication successful: handle = 3, server = Internal, group = fadigroup 476 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/3

RPT=10 AUTH_PutAttrTable(3, 1529394) 477 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/60 RPT=9 AUTH_UnbindServer(5566340, 0, 0) 478 02/02/2003 18:14:57.010 SEV=9 AUTHDBG/70 RPT=9 Auth Server 142f704 has been unbound from ACB 5566340, sessions = 0 479 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/59 RPT=10 AUTH_BindServer(5566340, 0, 0) 480 02/02/2003 18:14:57.010 SEV=9 AUTHDBG/69 RPT=10 Auth Server 142f704 has been bound to ACB 5566340, sessions = 1 481 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/65 RPT=10 AUTH_CreateTimer(5566340, 0, 0) 482 02/02/2003 18:14:57.010 SEV=9 AUTHDBG/72 RPT=10 Reply timer created: handle = 380016 483 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/179 RPT=10 AUTH_SyncToServer(5566340, 0, 0) 484 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/180 RPT=9 AUTH_SendLockReq(5566340, 0, 0) 485 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/61 RPT=10 AUTH_BuildMsg(5566340, 0, 0) 486 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/64 RPT=10 AUTH_StartTimer(5566340, 0, 0) 487 02/02/2003 18:14:57.010 SEV=9 AUTHDBG/73 RPT=10 Reply timer started: handle = 380016, timestamp = 94497, timeout = 30000 488 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/62 RPT=10 AUTH_SndRequest(5566340, 0, 0) 489 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/50 RPT=11 IntDB_Decode(28306f4, 52) 490 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/47 RPT=6 IntDB_Xmt(5566340) 491 02/02/2003 18:14:57.010 SEV=9 AUTHDBG/71 RPT=10 xmit_cnt = 1 492 02/02/2003 18:14:57.010 SEV=8 AUTHDBG/182 RPT=6 IntDB_ServiceRequest(5566340) 493 02/02/2003 18:14:57.110 SEV=8 AUTHDBG/49 RPT=6 IntDB_Match(5566340, 3a39694) 494 02/02/2003 18:14:57.110 SEV=8 AUTHDBG/63 RPT=10 AUTH_RcvReply(5566340, 0, 0) 495 02/02/2003 18:14:57.110 SEV=8 AUTHDBG/50 RPT=12 IntDB_Decode(3a39694, 163) 496 02/02/2003 18:14:57.110 SEV=8 AUTHDBG/48 RPT=6 IntDB_Rcv(5566340) 497 02/02/2003 18:14:57.110 SEV=8 AUTHDBG/66 RPT=10 AUTH_DeleteTimer(5566340, 0, 0) 498 02/02/2003 18:14:57.110 SEV=9 AUTHDBG/74 RPT=10 Reply timer stopped: handle = 380016, timestamp = 94507 499 02/02/2003 18:14:57.110 SEV=8 AUTHDBG/58 RPT=10 AUTH_Callback(5566340, 0, 0) 500 02/02/2003 18:14:57.110 SEV=6 AUTH/41 RPT=6 209.165.202.130 Authentication successful: handle = 3, server = Internal, group = fadigroup 501 02/02/2003 18:14:57.110 SEV=8 AUTHDBG/4 RPT=9 AUTH_GetAttrTable(3, 8abec8) 502 02/02/2003 18:14:57.110 SEV=8 AUTHDBG/4 RPT=10 AUTH_GetAttrTable(3, 8aaad0) *!--- The group name and user name.* **503 02/02/2003 18:14:57.110 SEV=7 IKEDBG/14 RPT=2 209.165.202.130 Group [fadigroup] User [fadi] Authentication configured for SDI 504 02/02/2003 18:14:57.110 SEV=9 IKEDBG/19 RPT=3 209.165.202.130 Group [fadigroup] User [fadi] IKEGetUserAttributes: default domain = cisco.com 505 02/02/2003 18:14:57.110 SEV=9 IKEDBG/19 RPT=4 209.165.202.130 Group [fadigroup] User [fadi] IKEGetUserAttributes: IP Compression = reset 506 02/02/2003 18:14:57.110 SEV=8 AUTHDBG/2 RPT=4 AUTH_Close(3) 507 02/02/2003 18:14:57.110 SEV=4 IKE/52 RPT=2 209.165.202.130 Group [fadigroup] User [fadi] User (fadi) authenticated. 508 02/02/2003 18:14:57.110 SEV=9 IKEDBG/0 RPT=99 209.165.202.130 Group [fadigroup] User [fadi] constructing blank hash 509 02/02/2003 18:14:57.110 SEV=9 IKEDBG/0 RPT=100 209.165.202.130 Group [fadigroup] User [fadi] constructing qm hash 510 02/02/2003 18:14:57.110 SEV=8 IKEDBG/0 RPT=101 209.165.202.130 SENDING Message (msgid=aee2a5e1) with payloads : HDR + HASH (8) + ATTR (14) total length : 60** 512 02/02/2003 18:14:57.110 SEV=8 AUTHDBG/60 RPT=10 AUTH_UnbindServer(5566340, 0, 0) 513 02/02/2003 18:14:57.110 SEV=9 AUTHDBG/70 RPT=10 Auth Server 142f704 has been unbound from ACB 5566340, sessions = 0 514 02/02/2003 18:14:57.110 SEV=8 AUTHDBG/10 RPT=4 AUTH_Int_FreeAuthCB(5566340) 515 02/02/2003 18:14:57.110 SEV=7 AUTH/13 RPT=4 Authentication session closed: handle = 3 516 02/02/2003 18:14:57.120 SEV=8 IKEDECODE/0 RPT=35 209.165.202.130 ISAKMP HEADER : (Version 1.0) Initiator Cookie(8): 5D 2F CC 82 FF 58 F1 18 Responder Cookie(8): 91 AC 22 89 C5 69 60 92 Next Payload : HASH (8) Exchange Type : Oakley Transactional Flags : 1 (ENCRYPT) Message ID : aee2a5e1 Length : 60 523 02/02/2003 18:14:57.120 SEV=8 IKEDBG/0 RPT=102 209.165.202.130 RECEIVED Message (msgid=aee2a5e1) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 56 525 02/02/2003 18:14:57.120 SEV=9 IKEDBG/1 RPT=7 process_attr(): Enter! 526 02/02/2003 18:14:57.120 SEV=9 IKEDBG/1 RPT=8 Processing cfg ACK attributes 527 02/02/2003 18:14:57.160 SEV=8 IKEDECODE/0 RPT=36 209.165.202.130 ISAKMP HEADER : (Version 1.0) Initiator Cookie(8): 5D 2F CC 82 FF 58 F1 18 Responder Cookie(8): 91 AC 22 89 C5 69 60 92 Next Payload : HASH (8) Exchange Type : Oakley Transactional Flags : 1 (ENCRYPT) Message ID : fa72a23b Length : 180 534 02/02/2003 18:14:57.160 SEV=8 IKEDBG/0 RPT=103 209.165.202.130 RECEIVED Message (msgid=fa72a23b) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 176 536 02/02/2003 18:14:57.160 SEV=9 IKEDBG/1 RPT=9 process_attr(): Enter! 537 02/02/2003 18:14:57.160 SEV=9 IKEDBG/1 RPT=10 Processing cfg Request attributes 538 02/02/2003 18:14:57.160 SEV=9 IKEDBG/53 RPT=1 MODE_CFG: Received request for IPV4 address! 539 02/02/2003 18:14:57.160 SEV=9 IKEDBG/53 RPT=2 MODE_CFG: Received request for IPV4 net mask! 540 02/02/2003 18:14:57.160 SEV=9 IKEDBG/53 RPT=3 MODE_CFG: Received request for DNS server address! 541 02/02/2003 18:14:57.160 SEV=9 IKEDBG/53 RPT=4 MODE_CFG: Received request for WINS server address! 542 02/02/2003 18:14:57.160 SEV=6 IKE/130 RPT=1 209.165.202.130 Group [fadigroup] User [fadi] Received unsupported transaction mode attribute: 5 543 02/02/2003 18:14:57.160 SEV=9 IKEDBG/53 RPT=5 MODE_CFG: Received request for Application Version! 544 02/02/2003 18:14:57.160 SEV=5 IKE/184 RPT=2 209.165.202.130 Group [fadigroup] User [fadi] Client OS: WinNT Client Application Version: 3.6.3 (A) 546 02/02/2003 18:14:57.160 SEV=9 IKEDBG/53 RPT=6 MODE_CFG: Received request for Banner! 547 02/02/2003

18:14:57.160 SEV=9 IKEDBG/53 RPT=7 MODE_CFG: Received request for Save PW setting! 548 02/02/2003 18:14:57.160 SEV=9 IKEDBG/53 RPT=8 MODE_CFG: Received request for Default Domain Name! 549 02/02/2003 18:14:57.160 SEV=9 IKEDBG/53 RPT=9 MODE_CFG: Received request for Split Tunnel List! 550 02/02/2003 18:14:57.160 SEV=9 IKEDBG/53 RPT=10 MODE_CFG: Received request for Split DNS! 551 02/02/2003 18:14:57.160 SEV=9 IKEDBG/53 RPT=11 MODE_CFG: Received request for PFS setting! 552 02/02/2003 18:14:57.160 SEV=9 IKEDBG/53 RPT=12 MODE_CFG: Received request for FWTYPE! 553 02/02/2003 18:14:57.160 SEV=9 IKEDBG/53 RPT=13 MODE_CFG: Received request for backup ip-sec peer list! 554 02/02/2003 18:14:57.160 SEV=9 IKEDBG/53 RPT=14 MODE_CFG: Received request for DHCP hostname for DDNS is: dire! 555 02/02/2003 18:14:57.160 SEV=9 IKEDBG/53 RPT=15 MODE_CFG: Received request for UDP Port! 556 02/02/2003 18:14:58.030 SEV=9 IKEDBG/31 RPT=1 209.165.202.130 Group [fadigroup] User [fadi] Obtained IP addr (10.48.67.100) prior to initiating Mode Cfg (XAuth enabled) 558 02/02/2003 18:14:58.030 SEV=7 IKEDBG/32 RPT=1 209.165.202.130 Group [fadigroup] User [fadi] Sending subnet mask (255.255.254.0) to remote client 560 02/02/2003 18:14:58.030 SEV=9 IKEDBG/0 RPT=104 209.165.202.130 Group [fadigroup] User [fadi] constructing blank hash 561 02/02/2003 18:14:58.030 SEV=9 IKEDBG/20 RPT=1 209.165.202.130 Group [fadigroup] User [fadi] construct_cfg_set: default domain = cisco.com 562 02/02/2003 18:14:58.030 SEV=9 IKEDBG/0 RPT=105 209.165.202.130 0000: 00010004 0A304364 00020004 FFFFFE00 .....0Cd........ 0010: F0010000 70020009 63697363 6F2E636F ....p...cisco.co 0020: 6DF00700 00000700 64436973 636F2053 m.......dCisco S 0030: 79737465 6D732C20 496E632E 2F56504E ystems, Inc./VPN 0040: 20333030 3020436F 6E63656E 74726174 3000 Concentrat 0050: 6F722056 65727369 6F6E2033 2E362E37 or Version 3.6.7 568 02/02/2003 18:14:58.030 SEV=9 IKEDBG/0 RPT=106 209.165.202.130 0000: 2E52656C 20627569 6C742062 7920766D .Rel built by vm 0010: 75727068 79206F6E 20446563 20313820 urphy on Dec 18 0020: 32303032 2031333A 31313A32 30 2002 13:11:20 571 02/02/2003 18:14:58.030 SEV=9 IKEDBG/0 RPT=107 209.165.202.130 Group [fadigroup] User [fadi] constructing qm hash 572 02/02/2003 18:14:58.030 SEV=8 IKEDBG/0 RPT=108 209.165.202.130 SENDING Message (msgid=fa72a23b) with payloads : HDR + HASH (8) + ATTR (14) total length : 197 574 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=37 209.165.202.130 ISAKMP HEADER : (Version 1.0) Initiator Cookie(8): 5D 2F CC 82 FF 58 F1 18 Responder Cookie(8): 91 AC 22 89 C5 69 60 92 Next Payload : HASH (8) Exchange Type : Oakley Quick Mode Flags : 1 (ENCRYPT) Message ID : c7b34e48 Length : 1020 581 02/02/2003 18:14:58.090 SEV=9 IKEDBG/21 RPT=1 209.165.202.130 Group [fadigroup] User [fadi] Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress 583 02/02/2003 18:14:58.090 SEV=4 AUTH/22 RPT=3 User fadi connected 584 02/02/2003 18:14:58.090 SEV=7 IKEDBG/22 RPT=1 209.165.202.130 Group [fadigroup] User [fadi] Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed 586 02/02/2003 18:14:58.090 SEV=4 IKE/119 RPT=2 209.165.202.130 Group [fadigroup] User [fadi] PHASE 1 COMPLETED 587 02/02/2003 18:14:58.090 SEV=6 IKE/121 RPT=1 209.165.202.130 Keep-alive type for this connection: DPD 588 02/02/2003 18:14:58.090 SEV=7 IKEDBG/0 RPT=109 209.165.202.130 Group [fadigroup] User [fadi] Starting phase 1 rekey timer: 82080000 (ms) 589 02/02/2003 18:14:58.090 SEV=9 IKEDBG/0 RPT=110 209.165.202.130 Group [fadigroup] User [fadi] sending notify message 590 02/02/2003 18:14:58.090 SEV=9 IKEDBG/0 RPT=111 209.165.202.130 Group [fadigroup] User [fadi] constructing blank hash 591 02/02/2003 18:14:58.090 SEV=9 IKEDBG/0 RPT=112 209.165.202.130 Group [fadigroup] User [fadi] constructing qm hash 592 02/02/2003 18:14:58.090 SEV=8 IKEDBG/0 RPT=113 209.165.202.130 SENDING Message (msgid=aa498927) with payloads : HDR + HASH (8) + NOTIFY (11) total length : 88 594 02/02/2003 18:14:58.090 SEV=8 IKEDBG/0 RPT=114 209.165.202.130 RECEIVED Message (msgid=c7b34e48) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 1018 597 02/02/2003 18:14:58.090 SEV=9 IKEDBG/0 RPT=115 209.165.202.130 Group [fadigroup] User [fadi] processing hash 598 02/02/2003 18:14:58.090 SEV=9 IKEDBG/0 RPT=116 209.165.202.130 Group [fadigroup] User [fadi] processing SA payload 599 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=38 209.165.202.130 SA Payload Decode : DOI : IPSEC (1) Situation : Identity Only (1) Length : 922 602 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=39 209.165.202.130 Proposal Decode: Proposal # : 1 Protocol ID : ESP (3) #of Transforms: 1 Spi : D8 A3 F8 09 Length : 44 606 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=40 209.165.202.130 Transform # 1 Decode for Proposal # 1: Transform # : 1 Transform ID : AES (12) Length : 32 608 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=41 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Key Length : 256 Bits (256) Life Time : 2147483 seconds 612 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=42 209.165.202.130 Proposal Decode: Proposal # : 1 Protocol ID : IPCOMP (4) #of Transforms: 1 Spi : 05 05 Length : 34 616 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=43 209.165.202.130 Transform # 1 Decode for Proposal # 1: Transform # : 1 Transform ID : LZS (3) Length : 24 618 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=44 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: Encapsulation : Tunnel (1) Life Time : 2147483 seconds 620 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=45 209.165.202.130 Proposal Decode: Proposal # : 2 Protocol ID : ESP (3) #of Transforms: 1 Spi : D8 A3 F8 09 Length : 44 624 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=46 209.165.202.130 Transform # 1 Decode for Proposal # 2: Transform # : 1 Transform ID : AES (12) Length : 32 626 02/02/2003

18:14:58.090 SEV=8 IKEDECODE/0 RPT=47 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: SHA (2) Encapsulation : Tunnel (1) Key Length : 256 Bits (256) Life Time : 2147483 seconds 630 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=48 209.165.202.130 Proposal Decode: Proposal # : 2 Protocol ID : IPCOMP (4) #of Transforms: 1 Spi : 21 F6 Length : 34 634 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=49 209.165.202.130 Transform # 1 Decode for Proposal # 2: Transform # : 1 Transform ID : LZS (3) Length : 24 636 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=50 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: Encapsulation : Tunnel (1) Life Time : 2147483 seconds 638 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=51 209.165.202.130 Proposal Decode: Proposal # : 3 Protocol ID : ESP (3) #of Transforms: 1 Spi : D8 A3 F8 09 Length : 44 642 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=52 209.165.202.130 Transform # 1 Decode for Proposal # 3: Transform # : 1 Transform ID : AES (12) Length : 32 644 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=53 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Key Length : 128 Bits (128) Life Time : 2147483 seconds 648 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=54 209.165.202.130 Proposal Decode: Proposal # : 3 Protocol ID : IPCOMP (4) #of Transforms: 1 Spi : 01 CC Length : 34 652 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=55 209.165.202.130 Transform # 1 Decode for Proposal # 3: Transform # : 1 Transform ID : LZS (3) Length : 24 654 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=56 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: Encapsulation : Tunnel (1) Life Time : 2147483 seconds 656 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=57 209.165.202.130 Proposal Decode: Proposal # : 4 Protocol ID : ESP (3) #of Transforms: 1 Spi : D8 A3 F8 09 Length : 44 660 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=58 209.165.202.130 Transform # 1 Decode for Proposal # 4: Transform # : 1 Transform ID : AES (12) Length : 32 662 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=59 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: SHA (2) Encapsulation : Tunnel (1) Key Length : 128 Bits (128) Life Time : 2147483 seconds 666 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=60 209.165.202.130 Proposal Decode: Proposal # : 4 Protocol ID : IPCOMP (4) #of Transforms: 1 Spi : 43 36 Length : 34 670 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=61 209.165.202.130 Transform # 1 Decode for Proposal # 4: Transform # : 1 Transform ID : LZS (3) Length : 24 672 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=62 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: Encapsulation : Tunnel (1) Life Time : 2147483 seconds 674 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=63 209.165.202.130 Proposal Decode: Proposal # : 5 Protocol ID : ESP (3) #of Transforms: 1 Spi : D8 A3 F8 09 Length : 44 678 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=64 209.165.202.130 Transform # 1 Decode for Proposal # 5: Transform # : 1 Transform ID : AES (12) Length : 32 680 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=65 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Key Length : 256 Bits (256) Life Time : 2147483 seconds 684 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=66 209.165.202.130 Proposal Decode: Proposal # : 6 Protocol ID : ESP (3) #of Transforms: 1 Spi : D8 A3 F8 09 Length : 44 688 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=67 209.165.202.130 Transform # 1 Decode for Proposal # 6: Transform # : 1 Transform ID : AES (12) Length : 32 690 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=68 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: SHA (2) Encapsulation : Tunnel (1) Key Length : 256 Bits (256) Life Time : 2147483 seconds 694 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=69 209.165.202.130 Proposal Decode: Proposal # : 7 Protocol ID : ESP (3) #of Transforms: 1 Spi : D8 A3 F8 09 Length : 44 698 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=70 209.165.202.130 Transform # 1 Decode for Proposal # 7: Transform # : 1 Transform ID : AES (12) Length : 32 700 02/02/2003 18:14:58.090 SEV=8 IKEDECODE/0 RPT=71 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Key Length : 128 Bits (128) Life Time : 2147483 seconds 704 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=72 209.165.202.130 Proposal Decode: Proposal # : 8 Protocol ID : ESP (3) #of Transforms: 1 Spi : D8 A3 F8 09 Length : 44 708 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=73 209.165.202.130 Transform # 1 Decode for Proposal # 8: Transform # : 1 Transform ID : AES (12) Length : 32 710 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=74 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: SHA (2) Encapsulation : Tunnel (1) Key Length : 128 Bits (128) Life Time : 2147483 seconds 714 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=75 209.165.202.130 Proposal Decode: Proposal # : 9 Protocol ID : ESP (3) #of Transforms: 1 Spi : D8 A3 F8 09 Length : 40 718 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=76 209.165.202.130 Transform # 1 Decode for Proposal # 9: Transform # : 1 Transform ID : Triple-DES (3) Length : 28 720 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=77 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Life Time : 2147483 seconds 723 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=78 209.165.202.130 Proposal Decode: Proposal # : 9 Protocol ID : IPCOMP (4) #of Transforms: 1 Spi : 87 69 Length : 34 727 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=79 209.165.202.130 Transform # 1 Decode for Proposal # 9: Transform # : 1 Transform ID : LZS (3) Length : 24 729 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=80

209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: Encapsulation : Tunnel (1) Life Time : 2147483 seconds 731 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=81 209.165.202.130 Proposal Decode: Proposal # : 10 Protocol ID : ESP (3) #of Transforms: 1 Spi : D8 A3 F8 09 Length : 40 735 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=82 209.165.202.130 Transform # 1 Decode for Proposal # 10: Transform # : 1 Transform ID : Triple-DES (3) Length : 28 737 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=83 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: SHA (2) Encapsulation : Tunnel (1) Life Time : 2147483 seconds 740 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=84 209.165.202.130 Proposal Decode: Proposal # : 10 Protocol ID : IPCOMP (4) #of Transforms: 1 Spi : 59 91 Length : 34 744 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=85 209.165.202.130 Transform # 1 Decode for Proposal # 10: Transform # : 1 Transform ID : LZS (3) Length : 24 746 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=86 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: Encapsulation : Tunnel (1) Life Time : 2147483 seconds 748 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=87 209.165.202.130 Proposal Decode: Proposal # : 11 Protocol ID : ESP (3) #of Transforms: 1 Spi : D8 A3 F8 09 Length : 40 752 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=88 209.165.202.130 Transform # 1 Decode for Proposal # 11: Transform # : 1 Transform ID : Triple-DES (3) Length : 28 754 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=89 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Life Time : 2147483 seconds 757 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=90 209.165.202.130 Proposal Decode: Proposal # : 12 Protocol ID : ESP (3) #of Transforms: 1 Spi : D8 A3 F8 09 Length : 40 761 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=91 209.165.202.130 Transform # 1 Decode for Proposal # 12: Transform # : 1 Transform ID : Triple-DES (3) Length : 28 763 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=92 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: SHA (2) Encapsulation : Tunnel (1) Life Time : 2147483 seconds 766 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=93 209.165.202.130 Proposal Decode: Proposal # : 13 Protocol ID : ESP (3) #of Transforms: 1 Spi : D8 A3 F8 09 Length : 40 770 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=94 209.165.202.130 Transform # 1 Decode for Proposal # 13: Transform # : 1 Transform ID : DES-CBC (2) Length : 28 772 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=95 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Life Time : 2147483 seconds 775 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=96 209.165.202.130 Proposal Decode: Proposal # : 13 Protocol ID : IPCOMP (4) #of Transforms: 1 Spi : 8E 66 Length : 34 779 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=97 209.165.202.130 Transform # 1 Decode for Proposal # 13: Transform # : 1 Transform ID : LZS (3) Length : 24 781 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=98 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: Encapsulation : Tunnel (1) Life Time : 2147483 seconds 783 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=99 209.165.202.130 Proposal Decode: Proposal # : 14 Protocol ID : ESP (3) #of Transforms: 1 Spi : D8 A3 F8 09 Length : 40 787 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=100 209.165.202.130 Transform # 1 Decode for Proposal # 14: Transform # : 1 Transform ID : DES-CBC (2) Length : 28 789 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=101 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Life Time : 2147483 seconds 792 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=102 209.165.202.130 Proposal Decode: Proposal # : 15 Protocol ID : ESP (3) #of Transforms: 1 Spi : D8 A3 F8 09 Length : 40 796 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=103 209.165.202.130 Transform # 1 Decode for Proposal # 15: Transform # : 1 Transform ID : NULL (11) Length : 28 798 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=104 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Life Time : 2147483 seconds 801 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=105 209.165.202.130 Proposal Decode: Proposal # : 16 Protocol ID : ESP (3) #of Transforms: 1 Spi : D8 A3 F8 09 Length : 40 805 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=106 209.165.202.130 Transform # 1 Decode for Proposal # 16: Transform # : 1 Transform ID : NULL (11) Length : 28 807 02/02/2003 18:14:58.100 SEV=8 IKEDECODE/0 RPT=107 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: SHA (2) Encapsulation : Tunnel (1) Life Time : 2147483 seconds 810 02/02/2003 18:14:58.100 SEV=9 IKEDBG/1 RPT=11 209.165.202.130 Group [fadigroup] User [fadi] processing nonce payload 811 02/02/2003 18:14:58.100 SEV=9 IKEDBG/1 RPT=12 209.165.202.130 Group [fadigroup] User [fadi] Processing ID 812 02/02/2003 18:14:58.100 SEV=5 IKE/25 RPT=3 209.165.202.130 Group [fadigroup] User [fadi] Received remote Proxy Host data in ID Payload: Address 10.48.67.100, Protocol 0, Port 0 815 02/02/2003 18:14:58.100 SEV=9 IKEDBG/1 RPT=13 209.165.202.130 Group [fadigroup] User [fadi] Processing ID 816 02/02/2003 18:14:58.100 SEV=5 IKE/24 RPT=2 209.165.202.130 Group [fadigroup] User [fadi] Received local Proxy Host data in ID Payload: Address 209.165.202.129, Protocol 0, Port 0 819 02/02/2003 18:14:58.100 SEV=8 IKEDBG/0 RPT=117 QM IsRekeyed old sa not found by addr 820 02/02/2003 18:14:58.100 SEV=5 IKE/66 RPT=3 209.165.202.130 Group [fadigroup] User [fadi] IKE Remote Peer configured for SA: ESP-3DES-MD5 821 02/02/2003 18:14:58.100 SEV=9 IKEDBG/0 RPT=118 209.165.202.130 Group [fadigroup] User [fadi] processing IPSEC SA 822 02/02/2003 18:14:58.100

SEV=8 IKEDBG/0 RPT=119 Proposal # 1, Transform # 1, Type ESP, Id AES Parsing received transform: Phase 2 failure: Mismatched transform IDs for protocol ESP: Rcv'd: AES Cfg'd: Triple-DES 827 02/02/2003 18:14:58.100 SEV=8 IKEDBG/0 RPT=120 Proposal # 2, Transform # 1, Type ESP, Id AES Parsing received transform: Phase 2 failure: Mismatched transform IDs for protocol ESP: Rcv'd: AES Cfg'd: Triple-DES 832 02/02/2003 18:14:58.100 SEV=8 IKEDBG/0 RPT=121 Proposal # 3, Transform # 1, Type ESP, Id AES Parsing received transform: Phase 2 failure: Mismatched transform IDs for protocol ESP: Rcv'd: AES Cfg'd: Triple-DES 837 02/02/2003 18:14:58.100 SEV=8 IKEDBG/0 RPT=122 Proposal # 4, Transform # 1, Type ESP, Id AES Parsing received transform: Phase 2 failure: Mismatched transform IDs for protocol ESP: Rcv'd: AES Cfg'd: Triple-DES 842 02/02/2003 18:14:58.100 SEV=8 IKEDBG/0 RPT=123 Proposal # 5, Transform # 1, Type ESP, Id AES Parsing received transform: Phase 2 failure: Mismatched transform IDs for protocol ESP: Rcv'd: AES Cfg'd: Triple-DES 847 02/02/2003 18:14:58.100 SEV=8 IKEDBG/0 RPT=124 Proposal # 6, Transform # 1, Type ESP, Id AES Parsing received transform: Phase 2 failure: Mismatched transform IDs for protocol ESP: Rcv'd: AES Cfg'd: Triple-DES 852 02/02/2003 18:14:58.100 SEV=8 IKEDBG/0 RPT=125 Proposal # 7, Transform # 1, Type ESP, Id AES Parsing received transform: Phase 2 failure: Mismatched transform IDs for protocol ESP: Rcv'd: AES Cfg'd: Triple-DES 857 02/02/2003 18:14:58.100 SEV=8 IKEDBG/0 RPT=126 Proposal # 8, Transform # 1, Type ESP, Id AES Parsing received transform: Phase 2 failure: Mismatched transform IDs for protocol ESP: Rcv'd: AES Cfg'd: Triple-DES 862 02/02/2003 18:14:58.100 SEV=8 IKEDBG/0 RPT=127 Proposal # 10, 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 866 02/02/2003 18:14:58.100 SEV=7 IKEDBG/27 RPT=1 209.165.202.130 Group [fadigroup] User [fadi] IPSec SA Proposal # 11, Transform # 1 acceptable 867 02/02/2003 18:14:58.100 SEV=7 IKEDBG/0 RPT=128 209.165.202.130 Group [fadigroup] User [fadi] IKE: requesting SPI! 868 02/02/2003 18:14:58.100 SEV=9 IPSECDBG/6 RPT=1 IPSEC key message parse - msgtype 6, len 208, vers 1, pid 00000000, seq 3, err 0 , type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKeyL en 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 21, lifetime2 0, dsId 300 871 02/02/2003 18:14:58.100 SEV=9 IPSECDBG/1 RPT=1 Processing KEY_GETSPI msg! 872 02/02/2003 18:14:58.100 SEV=7 IPSECDBG/13 RPT=1 Reserved SPI 1937253276 873 02/02/2003 18:14:58.100 SEV=8 IKEDBG/6 RPT=1 IKE got SPI from key engine: SPI = 0x7378239c 874 02/02/2003 18:14:58.100 SEV=9 IKEDBG/0 RPT=129 209.165.202.130 Group [fadigroup] User [fadi] oakley constucting quick mode 875 02/02/2003 18:14:58.100 SEV=9 IKEDBG/0 RPT=130 209.165.202.130 Group [fadigroup] User [fadi] constructing blank hash 876 02/02/2003 18:14:58.100 SEV=9 IKEDBG/0 RPT=131 209.165.202.130 Group [fadigroup] User [fadi] constructing ISA_SA for ipsec 877 02/02/2003 18:14:58.100 SEV=5 IKE/75 RPT=3 209.165.202.130 Group [fadigroup] User [fadi] Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 seconds 879 02/02/2003 18:14:58.100 SEV=9 IKEDBG/1 RPT=14 209.165.202.130 Group [fadigroup] User [fadi] constructing ipsec nonce payload 880 02/02/2003 18:14:58.100 SEV=9 IKEDBG/1 RPT=15 209.165.202.130 Group [fadigroup] User [fadi] constructing proxy ID 881 02/02/2003 18:14:58.100 SEV=7 IKEDBG/0 RPT=132 209.165.202.130 Group [fadigroup] User [fadi] Transmitting Proxy Id: Remote host: 10.48.67.100 Protocol 0 Port 0 Local host: 209.165.202.129 Protocol 0 Port 0 885 02/02/2003 18:14:58.100 SEV=7 IKEDBG/0 RPT=133 209.165.202.130 Group [fadigroup] User [fadi] Sending RESPONDER LIFETIME notification to Initiator 887 02/02/2003 18:14:58.100 SEV=9 IKEDBG/0 RPT=134 209.165.202.130 Group [fadigroup] User [fadi] constructing qm hash 888 02/02/2003 18:14:58.100 SEV=8 IKEDBG/0 RPT=135 209.165.202.130 SENDING Message (msgid=c7b34e48) with payloads : HDR + HASH (8) + SA (1) total length : 172 890 02/02/2003 18:14:58.120 SEV=8 IKEDECODE/0 RPT=108 209.165.202.130 ISAKMP HEADER : (Version 1.0) Initiator Cookie(8): 5D 2F CC 82 FF 58 F1 18 Responder Cookie(8): 91 AC 22 89 C5 69 60 92 Next Payload : HASH (8) Exchange Type : Oakley Quick Mode Flags : 1 (ENCRYPT) Message ID : c0349619 Length : 1028 897 02/02/2003 18:14:58.120 SEV=8 IKEDBG/0 RPT=136 209.165.202.130 RECEIVED Message (msgid=c0349619) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 1022 900 02/02/2003 18:14:58.120 SEV=9 IKEDBG/0 RPT=137 209.165.202.130 Group [fadigroup] User [fadi] processing hash 901 02/02/2003 18:14:58.120 SEV=9 IKEDBG/0 RPT=138 209.165.202.130 Group [fadigroup] User [fadi] processing SA payload 902 02/02/2003 18:14:58.120 SEV=8 IKEDECODE/0 RPT=109 209.165.202.130 SA Payload Decode : DOI : IPSEC (1) Situation : Identity Only (1) Length : 922 905 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=110 209.165.202.130 Proposal Decode: Proposal # : 1 Protocol ID : ESP (3) #of Transforms: 1 Spi : 8F 00 50 92 Length : 44 909 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=111 209.165.202.130 Transform # 1 Decode for Proposal # 1: Transform # : 1 Transform ID : AES (12) Length : 32 911 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=112 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Key Length : 256 Bits (256) Life Time : 2147483 seconds 915 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=113 209.165.202.130 Proposal Decode: Proposal # : 1 Protocol ID : IPCOMP (4) #of Transforms: 1 Spi : C4 EA Length : 34 919 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=114 209.165.202.130 Transform # 1 Decode for Proposal # 1: Transform # : 1 Transform ID : LZS (3) Length : 24 921 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0

RPT=115 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: Encapsulation : Tunnel (1) Life Time : 2147483 seconds 923 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=116 209.165.202.130 Proposal Decode: Proposal # : 2 Protocol ID : ESP (3) #of Transforms: 1 Spi : 8F 00 50 92 Length : 44 927 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=117 209.165.202.130 Transform # 1 Decode for Proposal # 2: Transform # : 1 Transform ID : AES (12) Length : 32 929 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=118 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: SHA (2) Encapsulation : Tunnel (1) Key Length : 256 Bits (256) Life Time : 2147483 seconds 933 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=119 209.165.202.130 Proposal Decode: Proposal # : 2 Protocol ID : IPCOMP (4) #of Transforms: 1 Spi : 5F 1D Length : 34 937 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=120 209.165.202.130 Transform # 1 Decode for Proposal # 2: Transform # : 1 Transform ID : LZS (3) Length : 24 939 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=121 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: Encapsulation : Tunnel (1) Life Time : 2147483 seconds 941 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=122 209.165.202.130 Proposal Decode: Proposal # : 3 Protocol ID : ESP (3) #of Transforms: 1 Spi : 8F 00 50 92 Length : 44 945 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=123 209.165.202.130 Transform # 1 Decode for Proposal # 3: Transform # : 1 Transform ID : AES (12) Length : 32 947 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=124 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Key Length : 128 Bits (128) Life Time : 2147483 seconds 951 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=125 209.165.202.130 Proposal Decode: Proposal # : 3 Protocol ID : IPCOMP (4) #of Transforms: 1 Spi : 7E 6E Length : 34 955 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=126 209.165.202.130 Transform # 1 Decode for Proposal # 3: Transform # : 1 Transform ID : LZS (3) Length : 24 957 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=127 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: Encapsulation : Tunnel (1) Life Time : 2147483 seconds 959 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=128 209.165.202.130 Proposal Decode: Proposal # : 4 Protocol ID : ESP (3) #of Transforms: 1 Spi : 8F 00 50 92 Length : 44 963 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=129 209.165.202.130 Transform # 1 Decode for Proposal # 4: Transform # : 1 Transform ID : AES (12) Length : 32 965 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=130 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: SHA (2) Encapsulation : Tunnel (1) Key Length : 128 Bits (128) Life Time : 2147483 seconds 969 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=131 209.165.202.130 Proposal Decode: Proposal # : 4 Protocol ID : IPCOMP (4) #of Transforms: 1 Spi : 09 0D Length : 34 973 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=132 209.165.202.130 Transform # 1 Decode for Proposal # 4: Transform # : 1 Transform ID : LZS (3) Length : 24 975 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=133 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: Encapsulation : Tunnel (1) Life Time : 2147483 seconds 977 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=134 209.165.202.130 Proposal Decode: Proposal # : 5 Protocol ID : ESP (3) #of Transforms: 1 Spi : 8F 00 50 92 Length : 44 981 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=135 209.165.202.130 Transform # 1 Decode for Proposal # 5: Transform # : 1 Transform ID : AES (12) Length : 32 983 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=136 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Key Length : 256 Bits (256) Life Time : 2147483 seconds 987 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=137 209.165.202.130 Proposal Decode: Proposal # : 6 Protocol ID : ESP (3) #of Transforms: 1 Spi : 8F 00 50 92 Length : 44 991 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=138 209.165.202.130 Transform # 1 Decode for Proposal # 6: Transform # : 1 Transform ID : AES (12) Length : 32 993 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=139 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: SHA (2) Encapsulation : Tunnel (1) Key Length : 256 Bits (256) Life Time : 2147483 seconds 997 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=140 209.165.202.130 Proposal Decode: Proposal # : 7 Protocol ID : ESP (3) #of Transforms: 1 Spi : 8F 00 50 92 Length : 44 1001 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=141 209.165.202.130 Transform # 1 Decode for Proposal # 7: Transform # : 1 Transform ID : AES (12) Length : 32 1003 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=142 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Key Length : 128 Bits (128) Life Time : 2147483 seconds 1007 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=143 209.165.202.130 Proposal Decode: Proposal # : 8 Protocol ID : ESP (3) #of Transforms: 1 Spi : 8F 00 50 92 Length : 44 1011 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=144 209.165.202.130 Transform # 1 Decode for Proposal # 8: Transform # : 1 Transform ID : AES (12) Length : 32 1013 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=145 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: SHA (2) Encapsulation : Tunnel (1) Key Length : 128 Bits (128) Life Time : 2147483 seconds 1017 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=146 209.165.202.130 Proposal Decode: Proposal # : 9 Protocol ID : ESP (3) #of Transforms: 1 Spi : 8F 00 50 92 Length : 40 1021 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=147 209.165.202.130 Transform # 1 Decode for Proposal # 9: Transform # : 1 Transform ID : Triple-DES (3) Length : 28 1023 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=148

209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Life Time : 2147483 seconds 1026 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=149 209.165.202.130 Proposal Decode: Proposal # : 9 Protocol ID : IPCOMP (4) #of Transforms: 1 Spi : 33 4A Length : 34 1030 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=150 209.165.202.130 Transform # 1 Decode for Proposal # 9: Transform # : 1 Transform ID : LZS (3) Length : 24 1032 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=151 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: Encapsulation : Tunnel (1) Life Time : 2147483 seconds 1034 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=152 209.165.202.130 Proposal Decode: Proposal # : 10 Protocol ID : ESP (3) #of Transforms: 1 Spi : 8F 00 50 92 Length : 40 1038 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=153 209.165.202.130 Transform # 1 Decode for Proposal # 10: Transform # : 1 Transform ID : Triple-DES (3) Length : 28 1040 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=154 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: SHA (2) Encapsulation : Tunnel (1) Life Time : 2147483 seconds 1043 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=155 209.165.202.130 Proposal Decode: Proposal # : 10 Protocol ID : IPCOMP (4) #of Transforms: 1 Spi : A5 E9 Length : 34 1047 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=156 209.165.202.130 Transform # 1 Decode for Proposal # 10: Transform # : 1 Transform ID : LZS (3) Length : 24 1049 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=157 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: Encapsulation : Tunnel (1) Life Time : 2147483 seconds 1051 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=158 209.165.202.130 Proposal Decode: Proposal # : 11 Protocol ID : ESP (3) #of Transforms: 1 Spi : 8F 00 50 92 Length : 40 1055 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=159 209.165.202.130 Transform # 1 Decode for Proposal # 11: Transform # : 1 Transform ID : Triple-DES (3) Length : 28 1057 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=160 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Life Time : 2147483 seconds 1060 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=161 209.165.202.130 Proposal Decode: Proposal # : 12 Protocol ID : ESP (3) #of Transforms: 1 Spi : 8F 00 50 92 Length : 40 1064 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=162 209.165.202.130 Transform # 1 Decode for Proposal # 12: Transform # : 1 Transform ID : Triple-DES (3) Length : 28 1066 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=163 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: SHA (2) Encapsulation : Tunnel (1) Life Time : 2147483 seconds 1069 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=164 209.165.202.130 Proposal Decode: Proposal # : 13 Protocol ID : ESP (3) #of Transforms: 1 Spi : 8F 00 50 92 Length : 40 1073 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=165 209.165.202.130 Transform # 1 Decode for Proposal # 13: Transform # : 1 Transform ID : DES-CBC (2) Length : 28 1075 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=166 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Life Time : 2147483 seconds 1078 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=167 209.165.202.130 Proposal Decode: Proposal # : 13 Protocol ID : IPCOMP (4) #of Transforms: 1 Spi : 11 76 Length : 34 1082 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=168 209.165.202.130 Transform # 1 Decode for Proposal # 13: Transform # : 1 Transform ID : LZS (3) Length : 24 1084 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=169 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: Encapsulation : Tunnel (1) Life Time : 2147483 seconds 1086 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=170 209.165.202.130 Proposal Decode: Proposal # : 14 Protocol ID : ESP (3) #of Transforms: 1 Spi : 8F 00 50 92 Length : 40 1090 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=171 209.165.202.130 Transform # 1 Decode for Proposal # 14: Transform # : 1 Transform ID : DES-CBC (2) Length : 28 1092 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=172 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Life Time : 2147483 seconds 1095 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=173 209.165.202.130 Proposal Decode: Proposal # : 15 Protocol ID : ESP (3) #of Transforms: 1 Spi : 8F 00 50 92 Length : 40 1099 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=174 209.165.202.130 Transform # 1 Decode for Proposal # 15: Transform # : 1 Transform ID : NULL (11) Length : 28 1101 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=175 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: MD5 (1) Encapsulation : Tunnel (1) Life Time : 2147483 seconds 1104 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=176 209.165.202.130 Proposal Decode: Proposal # : 16 Protocol ID : ESP (3) #of Transforms: 1 Spi : 8F 00 50 92 Length : 40 1108 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=177 209.165.202.130 Transform # 1 Decode for Proposal # 16: Transform # : 1 Transform ID : NULL (11) Length : 28 1110 02/02/2003 18:14:58.130 SEV=8 IKEDECODE/0 RPT=178 209.165.202.130 Phase 2 SA Attribute Decode for Transform # 1: HMAC Algorithm: SHA (2) Encapsulation : Tunnel (1) Life Time : 2147483 seconds 1113 02/02/2003 18:14:58.130 SEV=9 IKEDBG/1 RPT=16 209.165.202.130 Group [fadigroup] User [fadi] processing nonce payload 1114 02/02/2003 18:14:58.130 SEV=9 IKEDBG/1 RPT=17 209.165.202.130 Group [fadigroup] User [fadi] Processing ID 1115 02/02/2003 18:14:58.130 SEV=5 IKE/25 RPT=4 209.165.202.130 Group [fadigroup] User [fadi] Received remote Proxy Host data in ID Payload: Address 10.48.67.100, Protocol 0, Port 0 1118 02/02/2003 18:14:58.130 SEV=9 IKEDBG/1 RPT=18 209.165.202.130 Group [fadigroup] User

[fadi] Processing ID 1119 02/02/2003 18:14:58.130 SEV=5 IKE/34 RPT=2 209.165.202.130 Group [fadigroup] User [fadi] Received local IP Proxy Subnet data in ID Payload: Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0 1122 02/02/2003 18:14:58.130 SEV=8 IKEDBG/0 RPT=139 QM IsRekeyed old sa not found by addr 1123 02/02/2003 18:14:58.130 SEV=5 IKE/66 RPT=4 209.165.202.130 Group [fadigroup] User [fadi] IKE Remote Peer configured for SA: ESP-3DES-MD5 1124 02/02/2003 18:14:58.130 SEV=9 IKEDBG/0 RPT=140 209.165.202.130 Group [fadigroup] User [fadi] processing IPSEC SA 1125 02/02/2003 18:14:58.130 SEV=8 IKEDBG/0 RPT=141 Proposal # 1, Transform # 1, Type ESP, Id AES Parsing received transform: Phase 2 failure: Mismatched transform IDs for protocol ESP: Rcv'd: AES Cfg'd: Triple-DES 1130 02/02/2003 18:14:58.130 SEV=8 IKEDBG/0 RPT=142 Proposal # 2, Transform # 1, Type ESP, Id AES Parsing received transform: Phase 2 failure: Mismatched transform IDs for protocol ESP: Rcv'd: AES Cfg'd: Triple-DES 1135 02/02/2003 18:14:58.130 SEV=8 IKEDBG/0 RPT=143 Proposal # 3, Transform # 1, Type ESP, Id AES Parsing received transform: Phase 2 failure: Mismatched transform IDs for protocol ESP: Rcv'd: AES Cfg'd: Triple-DES 1140 02/02/2003 18:14:58.130 SEV=8 IKEDBG/0 RPT=144 Proposal # 4, Transform # 1, Type ESP, Id AES Parsing received transform: Phase 2 failure: Mismatched transform IDs for protocol ESP: Rcv'd: AES Cfg'd: Triple-DES 1145 02/02/2003 18:14:58.130 SEV=8 IKEDBG/0 RPT=145 Proposal # 5, Transform # 1, Type ESP, Id AES Parsing received transform: Phase 2 failure: Mismatched transform IDs for protocol ESP: Rcv'd: AES Cfg'd: Triple-DES 1150 02/02/2003 18:14:58.130 SEV=8 IKEDBG/0 RPT=146 Proposal # 6, Transform # 1, Type ESP, Id AES Parsing received transform: Phase 2 failure: Mismatched transform IDs for protocol ESP: Rcv'd: AES Cfg'd: Triple-DES 1155 02/02/2003 18:14:58.130 SEV=8 IKEDBG/0 RPT=147 Proposal # 7, Transform # 1, Type ESP, Id AES Parsing received transform: Phase 2 failure: Mismatched transform IDs for protocol ESP: Rcv'd: AES Cfg'd: Triple-DES 1160 02/02/2003 18:14:58.130 SEV=8 IKEDBG/0 RPT=148 Proposal # 8, Transform # 1, Type ESP, Id AES Parsing received transform: Phase 2 failure: Mismatched transform IDs for protocol ESP: Rcv'd: AES Cfg'd: Triple-DES 1165 02/02/2003 18:14:58.130 SEV=8 IKEDBG/0 RPT=149 Proposal # 10, 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 1169 02/02/2003 18:14:58.130 SEV=7 IKEDBG/27 RPT=2 209.165.202.130 Group [fadigroup] User [fadi] IPSec SA Proposal # 11, Transform # 1 acceptable 1170 02/02/2003 18:14:58.130 SEV=7 IKEDBG/0 RPT=150 209.165.202.130 Group [fadigroup] User [fadi] IKE: requesting SPI! 1171 02/02/2003 18:14:58.130 SEV=9 IPSECDBG/6 RPT=2 IPSEC key message parse - msgtype 6, len 208, vers 1, pid 00000000, seq 4, err 0 , type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKeyL en 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 21, lifetime2 0, dsId 300 1174 02/02/2003 18:14:58.130 SEV=9 IPSECDBG/1 RPT=2 Processing KEY_GETSPI msg! 1175 02/02/2003 18:14:58.130 SEV=7 IPSECDBG/13 RPT=2 Reserved SPI 10677127 1176 02/02/2003 18:14:58.130 SEV=8 IKEDBG/6 RPT=2 IKE got SPI from key engine: SPI = 0x00a2eb87 1177 02/02/2003 18:14:58.130 SEV=9 IKEDBG/0 RPT=151 209.165.202.130 Group [fadigroup] User [fadi] oakley constucting quick mode 1178 02/02/2003 18:14:58.130 SEV=9 IKEDBG/0 RPT=152 209.165.202.130 Group [fadigroup] User [fadi] constructing blank hash 1179 02/02/2003 18:14:58.130 SEV=9 IKEDBG/0 RPT=153 209.165.202.130 Group [fadigroup] User [fadi] constructing ISA_SA for ipsec 1180 02/02/2003 18:14:58.130 SEV=5 IKE/75 RPT=4 209.165.202.130 Group [fadigroup] User [fadi] Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 seconds 1182 02/02/2003 18:14:58.130 SEV=9 IKEDBG/1 RPT=19 209.165.202.130 Group [fadigroup] User [fadi] constructing ipsec nonce payload 1183 02/02/2003 18:14:58.130 SEV=9 IKEDBG/1 RPT=20 209.165.202.130 Group [fadigroup] User [fadi] constructing proxy ID 1184 02/02/2003 18:14:58.140 SEV=7 IKEDBG/0 RPT=154 209.165.202.130 Group [fadigroup] User [fadi] Transmitting Proxy Id: Remote host: 10.48.67.100 Protocol 0 Port 0 Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0 1188 02/02/2003 18:14:58.140 SEV=7 IKEDBG/0 RPT=155 209.165.202.130 Group [fadigroup] User [fadi] Sending RESPONDER LIFETIME notification to Initiator 1190 02/02/2003 18:14:58.140 SEV=9 IKEDBG/0 RPT=156 209.165.202.130 Group [fadigroup] User [fadi] constructing qm hash 1191 02/02/2003 18:14:58.140 SEV=8 IKEDBG/0 RPT=157 209.165.202.130 SENDING Message (msgid=c0349619) with payloads : HDR + HASH (8) + SA (1) total length : 176 1193 02/02/2003 18:14:58.150 SEV=8 IKEDECODE/0 RPT=179 209.165.202.130 ISAKMP HEADER : (Version 1.0) Initiator Cookie(8): 5D 2F CC 82 FF 58 F1 18 Responder Cookie(8): 91 AC 22 89 C5 69 60 92 Next Payload : HASH (8) Exchange Type : Oakley Quick Mode Flags : 1 (ENCRYPT) Message ID : c7b34e48 Length : 52 1200 02/02/2003 18:14:58.160 SEV=8 IKEDBG/0 RPT=158 209.165.202.130 RECEIVED Message (msgid=c7b34e48) with payloads : HDR + HASH (8) + NONE (0) total length : 48 1202 02/02/2003 18:14:58.160 SEV=9 IKEDBG/0 RPT=159 209.165.202.130 Group [fadigroup] User [fadi] processing hash 1203 02/02/2003 18:14:58.160 SEV=9 IKEDBG/0 RPT=160 209.165.202.130 Group [fadigroup] User [fadi] loading all IPSEC SAs 1204 02/02/2003 18:14:58.160 SEV=9 IKEDBG/1 RPT=21 209.165.202.130 Group [fadigroup] User [fadi] Generating Quick Mode Key! 1205 02/02/2003 18:14:58.160 SEV=9 IKEDBG/1 RPT=22 209.165.202.130 Group [fadigroup] User [fadi] Generating Quick Mode Key! 1206 02/02/2003 18:14:58.160 SEV=7 IKEDBG/0 RPT=161 209.165.202.130 Group [fadigroup] User [fadi] Loading host: Dst: 209.165.202.129 Src: 10.48.67.100 1208 02/02/2003 18:14:58.160 SEV=4 IKE/49 RPT=3

```
209.165.202.130 Group [fadigroup] User [fadi] Security negotiation complete for User (fadi)
Responder, Inbound SPI = 0x7378239c, Outbound SPI = 0xd8a3f809 1211 02/02/2003 18:14:58.160
SEV=9 IPSECDBG/6 RPT=3 IPSEC key message parse - msgtype 1, len 696, vers 1, pid 00000000, seq
0, err 0 , type 2, mode 1, state 64, label 0, pad 0, spi d8a3f809, encrKeyLen 24, hashKey Len
16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 21, lifetime2 0, dsId 0 1214 02/02/2003
18:14:58.160 SEV=9 IPSECDBG/1 RPT=3 Processing KEY_ADD msg! 1215 02/02/2003 18:14:58.160 SEV=9
IPSECDBG/1 RPT=4 key_msghdr2secassoc(): Enter 1216 02/02/2003 18:14:58.160 SEV=7 IPSECDBG/1
RPT=5 No USER filter configured 1217 02/02/2003 18:14:58.160 SEV=9 IPSECDBG/1 RPT=6
KeyProcessAdd: Enter 1218 02/02/2003 18:14:58.160 SEV=8 IPSECDBG/1 RPT=7 KeyProcessAdd: Adding
outbound SA 1219 02/02/2003 18:14:58.160 SEV=8 IPSECDBG/1 RPT=8 KeyProcessAdd: src
209.165.202.129 mask 0.0.0.0, dst 10.48.67.100 mask 0.0.0.0 1220 02/02/2003 18:14:58.160 SEV=8
IPSECDBG/1 RPT=9 KeyProcessAdd: FilterIpsecAddIkeSa success 1221 02/02/2003 18:14:58.160 SEV=9
IPSECDBG/6 RPT=4 IPSEC key message parse - msgtype 3, len 372, vers 1, pid 00000000, seq 0, err
0 , type 2, mode 1, state 32, label 0, pad 0, spi 7378239c, encrKeyLen 24, hashKey Len 16, ivlen
8, alg 2, hmacAlg 3, lifetype 0, lifetime1 21, lifetime2 0, dsId 0 1224 02/02/2003 18:14:58.160
SEV=9 IPSECDBG/1 RPT=10 Processing KEY_UPDATE msg! 1225 02/02/2003 18:14:58.160 SEV=9 IPSECDBG/1
RPT=11 Update inbound SA addresses 1226 02/02/2003 18:14:58.160 SEV=9 IPSECDBG/1 RPT=12
key_msghdr2secassoc(): Enter 1227 02/02/2003 18:14:58.160 SEV=7 IPSECDBG/1 RPT=13 No USER filter
configured 1228 02/02/2003 18:14:58.160 SEV=9 IPSECDBG/1 RPT=14 KeyProcessUpdate: Enter 1229
02/02/2003 18:14:58.160 SEV=8 IPSECDBG/1 RPT=15 KeyProcessUpdate: success 1230 02/02/2003
18:14:58.160 SEV=8 IKEDBG/7 RPT=1 IKE got a KEY_ADD msg for SA: SPI = 0xd8a3f809 1231 02/02/2003
18:14:58.160 SEV=8 IKEDBG/0 RPT=162 pitcher: rcv KEY_UPDATE, spi 0x7378239c 1232 02/02/2003
18:14:58.160 SEV=4 IKE/120 RPT=3 209.165.202.130 Group [fadigroup] User [fadi] PHASE 2 COMPLETED
(msgid=c7b34e48) 1233 02/02/2003 18:14:58.280 SEV=8 IKEDECODE/0 RPT=180 209.165.202.130 ISAKMP
HEADER : ( Version 1.0 ) Initiator Cookie(8): 5D 2F CC 82 FF 58 F1 18 Responder Cookie(8): 91 AC
22 89 C5 69 60 92 Next Payload : HASH (8) Exchange Type : Oakley Quick Mode Flags : 1 (ENCRYPT )
Message ID : c0349619 Length : 52 1240 02/02/2003 18:14:58.280 SEV=8 IKEDBG/0 RPT=163
209.165.202.130 RECEIVED Message (msgid=c0349619) with payloads : HDR + HASH (8) + NONE (0)
total length : 48 1242 02/02/2003 18:14:58.280 SEV=9 IKEDBG/0 RPT=164 209.165.202.130 Group
[fadigroup] User [fadi] processing hash 1243 02/02/2003 18:14:58.280 SEV=9 IKEDBG/0 RPT=165
209.165.202.130 Group [fadigroup] User [fadi] loading all IPSEC SAs 1244 02/02/2003 18:14:58.280
SEV=9 IKEDBG/1 RPT=23 209.165.202.130 Group [fadigroup] User [fadi] Generating Quick Mode Key!
1245 02/02/2003 18:14:58.280 SEV=9 IKEDBG/1 RPT=24 209.165.202.130 Group [fadigroup] User [fadi]
Generating Quick Mode Key! 1246 02/02/2003 18:14:58.280 SEV=7 IKEDBG/0 RPT=166 209.165.202.130
Group [fadigroup] User [fadi] Loading subnet: Dst: 0.0.0.0 mask: 0.0.0.0 Src: 10.48.67.100 1248
02/02/2003 18:14:58.280 SEV=4 IKE/49 RPT=4 209.165.202.130 Group [fadigroup] User [fadi]
Security negotiation complete for User (fadi) Responder, Inbound SPI = 0x00a2eb87, Outbound SPI
= 0x8f005092 1251 02/02/2003 18:14:58.280 SEV=9 IPSECDBG/6 RPT=5 IPSEC key message parse -
msgtype 1, len 696, vers 1, pid 00000000, seq 0, err 0 , type 2, mode 1, state 64, label 0, pad
0, spi 8f005092, encrKeyLen 24, hashKey Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1
21, lifetime2 0, dsId 0 1254 02/02/2003 18:14:58.280 SEV=9 IPSECDBG/1 RPT=16 Processing KEY_ADD
msg! 1255 02/02/2003 18:14:58.280 SEV=9 IPSECDBG/1 RPT=17 key_msghdr2secassoc(): Enter 1256
02/02/2003 18:14:58.280 SEV=7 IPSECDBG/1 RPT=18 No USER filter configured 1257 02/02/2003
18:14:58.280 SEV=9 IPSECDBG/1 RPT=19 KeyProcessAdd: Enter 1258 02/02/2003 18:14:58.280 SEV=8
IPSECDBG/1 RPT=20 KeyProcessAdd: Adding outbound SA 1259 02/02/2003 18:14:58.280 SEV=8
IPSECDBG/1 RPT=21 KeyProcessAdd: src 0.0.0.0 mask 255.255.255.255, dst 10.48.67.100 mask 0.0.0.0
1260 02/02/2003 18:14:58.280 SEV=8 IPSECDBG/1 RPT=22 KeyProcessAdd: FilterIpsecAddIkeSa success
1261 02/02/2003 18:14:58.280 SEV=9 IPSECDBG/6 RPT=6 IPSEC key message parse - msgtype 3, len
372, vers 1, pid 00000000, seq 0, err 0 , type 2, mode 1, state 32, label 0, pad 0, spi
00a2eb87, encrKeyLen 24, hashKey Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 21,
lifetime2 0, dsId 0 1264 02/02/2003 18:14:58.280 SEV=9 IPSECDBG/1 RPT=23 Processing KEY_UPDATE
msg! 1265 02/02/2003 18:14:58.280 SEV=9 IPSECDBG/1 RPT=24 Update inbound SA addresses 1266
02/02/2003 18:14:58.280 SEV=9 IPSECDBG/1 RPT=25 key_msghdr2secassoc(): Enter 1267 02/02/2003
18:14:58.280 SEV=7 IPSECDBG/1 RPT=26 No USER filter configured 1268 02/02/2003 18:14:58.280
SEV=9 IPSECDBG/1 RPT=27 KeyProcessUpdate: Enter 1269 02/02/2003 18:14:58.280 SEV=8 IPSECDBG/1
RPT=28 KeyProcessUpdate: success 1270 02/02/2003 18:14:58.280 SEV=8 IKEDBG/7 RPT=2 IKE got a
KEY_ADD msg for SA: SPI = 0x8f005092 1271 02/02/2003 18:14:58.280 SEV=8 IKEDBG/0 RPT=167
pitcher: rcv KEY_UPDATE, spi 0xa2eb87 1272 02/02/2003 18:14:58.280 SEV=4 IKE/120 RPT=4
209.165.202.130 Group [fadigroup] User [fadi] PHASE 2 COMPLETED (msgid=c0349619)
```

常见问题

- 如果不删除从Cisco VPN 3000集中器的.SDI文件，当您删除(然后时重新加写)在SDI服务器的

VPN集中器，您收到在VPN集中器调试的此错误：`Node Verification Failed`为了解决此错误，请删除从VPN 3000集中器的.SDI文件。然后，在ACE服务器，请编辑代理主机集中器并且非选定**发送的节点秘密**方框。

- 当代理主机没有配置为“时请打开给所有本地已知用户” ACE服务器的，并且用户在该代理主机没有激活，您在VPN 3000集中器**debug输出中**获得一个在SDI日志的和此消息的。

```
Authentication rejected:
Reason = Unspecified handle = 15, server = 10.48.66.102, user = junk
```

- 如果有一个好用户名，但是一个坏密码，您收到一个错误在SDI日志和一个错误在集中器**debug输出中**。

相关信息

- 配置Cisco VPN Client对有IPSec SDI Authentication的(服务器版本3.3) VPN 3000集中器
- Cisco VPN 3000 系列集中器支持页
- Cisco VPN 3000 系列客户端支持页
- IPSec 支持页面
- 技术支持 - Cisco Systems