

有IPSec SDI 认证(服务器版本3.3)的Cisco VPN客户端到VPN 3000集中器

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[测试使用 SDI 时的 Cisco VPN 客户端到VPN 3000 集中器](#)

[故障排除](#)

[启用 VPN 3000 集中器上的调试](#)

[成功的使用本地认证的 IPsec 调试](#)

[成功的使用本地认证的 IPsec 调试](#)

[成功的使用 SDI 时的调试](#)

[错误调试](#)

[相关信息](#)

简介

Cisco VPN 3000集中器可以配置通过Security Dynamics International (SDI)服务器验证Cisco VPN Client。VPN 3000集中器用作SDI客户端，与用户数据包协议(UDP)端口5500上的SDI服务器进行通信。以下文件显示如何确保SDI服务器、VPN 3000集中器和Cisco VPN客户端正常运行，以及如何结合使用上述组件。如果您的VPN 3000集中器未配置，使用初始安装和配置的，命令行界面(CLI)请使用从[安装的步骤并且配置VPN 3000集中器，不用SDI](#)。如果早先配置了您的VPN 3000集中器，则遵从[“修改现有配置”的步骤\(没有SDI\)](#)。

先决条件

要求

本文档没有任何特定的前提条件。

使用的组件

此配置使用下面软件和硬件版本开发并且被测试。

- SDI服务器3.3 (UNIX和NT)
- VPN 3000集中器(2.5.2)
- VPN Client 2.5.2.A

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。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

[规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[背景信息](#)

本文适用于Cisco VPN 3000客户端(2.5.x)或Cisco VPN Client (3.x)。使用3.0及以上版本，您现在可以为单个组配置单个SDI服务器，单个SDI服务器与全局定义的供全部组使用的SDI服务器正好相反。没有配置各自的SDI服务器的那些组将使用全局定义的SDI服务器。

有新的personal identification number (PIN)模式的三种类型在SDI的。VPN 3000集中器支持两第一选择如下所示。

- 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。

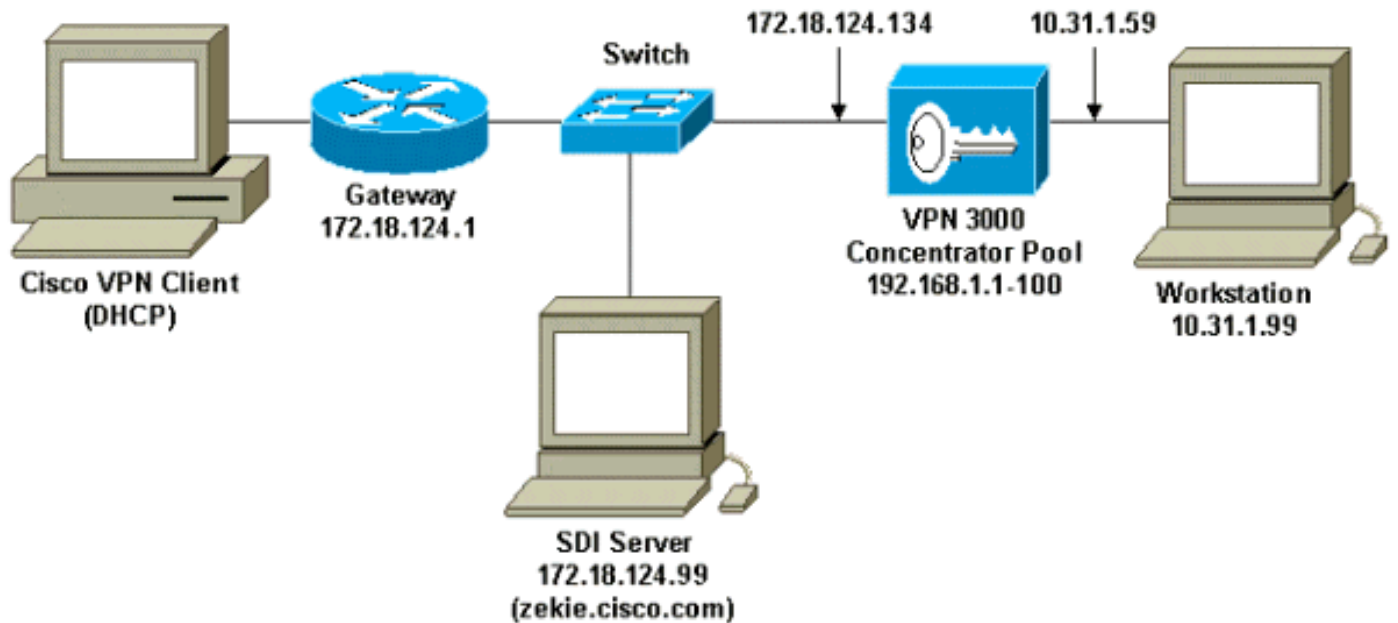
[配置](#)

本部分提供有关如何配置本文档所述功能的信息。

注意：要查找本文档所用命令的其他信息，请使用[命令查找工具](#)（[仅限注册用户](#)）。

[网络图](#)

本文档使用下图所示的网络设置。



配置

安装并且配置VPN 3000集中器，不用SDI

我们在组中配置VPN 3000集中器本地验证一个用户;通过在添加SDI之前执行该操作，我们能够确定思科VPN客户端和VPN 3000集中器之间的IPSec正在运行。我们清除了控制台端口上的VPN 3000集中器，方法是选择Administration>System Reboot>Schedule reboot>Reboot with Factory/Default Configuration。

在重新启动以后，以下初始配置被执行了：

VPN 3000集中器集中器配置

```

Login: admin Password: Welcome to Cisco Systems VPN 3000
Concentrator Series Command Line Interface Copyright (C)
1998-2000 Cisco Systems, Inc. -- : Set the time on your
device. The correct time is very important, -- : so that
logging and accounting entries are accurate. -- : Enter
the system time in the following format: -- : HH:MM:SS.
Example 21:30:00 for 9:30 PM > Time Quick -> [ 13:02:39
] -- : Enter the date in the following format. -- :
MM/DD/YYYY Example 06/12/1999 for June 12th 1999. > Date
Quick -> [ 10/09/2000 ] -- : Set the time zone on your
device. The correct time zone is very -- : important so
that logging and accounting entries are accurate. -- :
Enter the time zone using the hour offset from GMT: -- :
-12 : Kwajalein -11 : Samoa -10 : Hawaii -9 : Alaska --
: -8 : PST -7 : MST -6 : CST -5 : EST -- : -4 : Atlantic
-3 : Brasilia -2 : Mid-Atlantic -1 : Azores -- : 0 : GMT
+1 : Paris +2 : Cairo +3 : Kuwait -- : +4 : Abu Dhabi +5
: Karachi +6 : Almaty +7 : Bangkok -- : +8 : Singapore
+9 : Tokyo +10 : Sydney +11 : Solomon Is. -- : +12 :
Marshall Is. > Time Zone Quick -> [ -5 ] -5 1) Enable
DST Support 2) Disable DST Support Quick -> [ 1 ] This
table shows current IP addresses. Interface IP
Address/Subnet Mask MAC Address -----
-----
| Ethernet 1 - Private | 0.0.0.0/0.0.0.0 | | Ethernet 2
- Public | 0.0.0.0/0.0.0.0 | | Ethernet 3 - External |
0.0.0.0/0.0.0.0 | -----

```

```

----- ** An address
is required for the private interface. ** > Enter IP
Address Quick Ethernet 1 -> [ 0.0.0.0 ] 10.31.1.59
Waiting for Network Initialization... > Enter Subnet
Mask Quick Ethernet 1 -> [ 255.0.0.0 ] 255.255.255.0 1)
Ethernet Speed 10 Mbps 2) Ethernet Speed 100 Mbps 3)
Ethernet Speed 10/100 Mbps Auto Detect Quick Ethernet 1
-> [ 3 ] 1) Enter Duplex - Half/Full/Auto 2) Enter
Duplex - Full Duplex 3) Enter Duplex - Half Duplex Quick
Ethernet 1 -> [ 1 ] 1) Modify Ethernet 1 IP Address
(Private) 2) Modify Ethernet 2 IP Address (Public) 3)
Modify Ethernet 3 IP Address (External) 4) Configure
Expansion Cards 5) Save changes to Config file 6)
Continue 7) Exit Quick -> 2 This table shows current IP
addresses. Interface IP Address/Subnet Mask MAC Address
-----
----- | Ethernet 1 - Private |
10.31.1.59/255.255.255.0 | 00.90.A4.00.1C.B4 | Ethernet
2 - Public | 0.0.0.0/0.0.0.0 | | Ethernet 3 - External |
0.0.0.0/0.0.0.0 | -----
----- > Enter IP
Address Quick Ethernet 2 -> [ 0.0.0.0 ] 172.18.124.134 >
Enter Subnet Mask Quick Ethernet 2 -> [ 255.255.0.0 ]
255.255.255.0 1) Ethernet Speed 10 Mbps 2) Ethernet
Speed 100 Mbps 3) Ethernet Speed 10/100 Mbps Auto Detect
Quick Ethernet 2 -> [ 3 ] 1) Enter Duplex -
Half/Full/Auto 2) Enter Duplex - Full Duplex 3) Enter
Duplex - Half Duplex Quick Ethernet 2 -> [ 1 ] 1) Modify
Ethernet 1 IP Address (Private) 2) Modify Ethernet 2 IP
Address (Public) 3) Modify Ethernet 3 IP Address
(External) 4) Configure Expansion Cards 5) Save changes
to Config file 6) Continue 7) Exit Quick -> 6 -- :
Assign a system name to this device. > System Name Quick
-> vpn3000 -- : Specify a local DNS server, which lets
you enter hostnames -- : rather than IP addresses while
configuring. > DNS Server Quick -> [ 0.0.0.0 ] -- :
Enter your Internet domain name; e.g., yourcompany.com >
Domain Quick -> > Default Gateway Quick -> 172.18.124.1
-- : Configure protocols and encryption options. -- :
This table shows current protocol settings PPTP | L2TP |
----- | Enabled
| Enabled | | No Encryption Req | No Encryption Req | --
----- 1) Enable
PPTP 2) Disable PPTP Quick -> [ 1 ] 1) PPTP Encryption
Required 2) No Encryption Required Quick -> [ 2 ] 1)
Enable L2TP 2) Disable L2TP Quick -> [ 1 ] 1) L2TP
Encryption Required 2) No Encryption Required Quick -> [
2 ] 1) Enable IPsec 2) Disable IPsec Quick -> [ 1 ] -- :
Configure address assignment for PPTP, L2TP and IPsec.
1) Enable Client Specified Address Assignment 2) Disable
Client Specified Address Assignment Quick -> [ 2 ] 1)
Enable Per User Address Assignment 2) Disable Per User
Address Assignment Quick -> [ 2 ] 1) Enable DHCP Address
Assignment 2) Disable DHCP Address Assignment Quick -> [
2 ] 1) Enable Configured Pool Address Assignment 2)
Disable Configured Pool Address Assignment Quick -> [ 2
] 1 > Configured Pool Range Start Address Quick ->
192.168.1.1 > Configured Pool Range End Address Quick ->
[ 0.0.0.0 ] 192.168.1.100 -- : Specify how to
authenticate users 1) Internal Authentication Server 2)
RADIUS Authentication Server 3) NT Domain Authentication
Server 4) SDI Authentication Server 5) Continue Quick ->
[ 1 ] 1 Current Users -----
----- No Users -

```

```

----- 1) Add a User 2) Delete a User 3)
Continue Quick -> 1 > User Name Quick -> 37297304 >
Password Quick -> ***** Verify -> ***** Current
Users ----- | 1. 37297304 | | -----
----- 1) Add a User 2) Delete a User 3)
Continue Quick -> 3 > IPsec Group Name Quick -> vpn3000
> IPsec Group Password Quick -> ***** Verify ->
***** -- : We strongly recommend that you change the
password for user admin. > Reset Admin Password Quick ->
[ ***** ] Verify -> 1) Goto Main Configuration Menu 2)
Save changes to Config file 3) Exit Quick -> 2 1) Goto
Main Configuration Menu 2) Save changes to Config file
3) Exit Quick -> 3 Done

```

修改现有配置(没有SDI)

如果早先配置了VPN 3000集中器，则使用以下屏幕检验组、用户和IPSec/IKE设置：

1. 以本地认证使用此屏幕添加每组

:

Configuration | User Management | Groups | Modify
vpn3000

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

Identity
General
IPSec
PPTP/L2TP

| Identity Parameters | | |
|---------------------|-----------------------------------|--|
| Attribute | Value | Description |
| Group Name | vpn3000 | Enter a unique name for the group. |
| Password | ***** | Enter the password for the group. |
| Verify | ***** | Verify the group's password. |
| Type | Internal <input type="checkbox"/> | <i>External</i> groups are configured on an external authentication server (e.g. RADIUS). <i>Internal</i> groups are configured on the VPN 3000 Concentrator Series's Internal Database. |

Apply
Cancel

2. 请使用此屏幕添加用户给组与本地认证

Configuration | User Management | Users | Modify
37297304

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

Identity General IPsec PPTP/L2TP

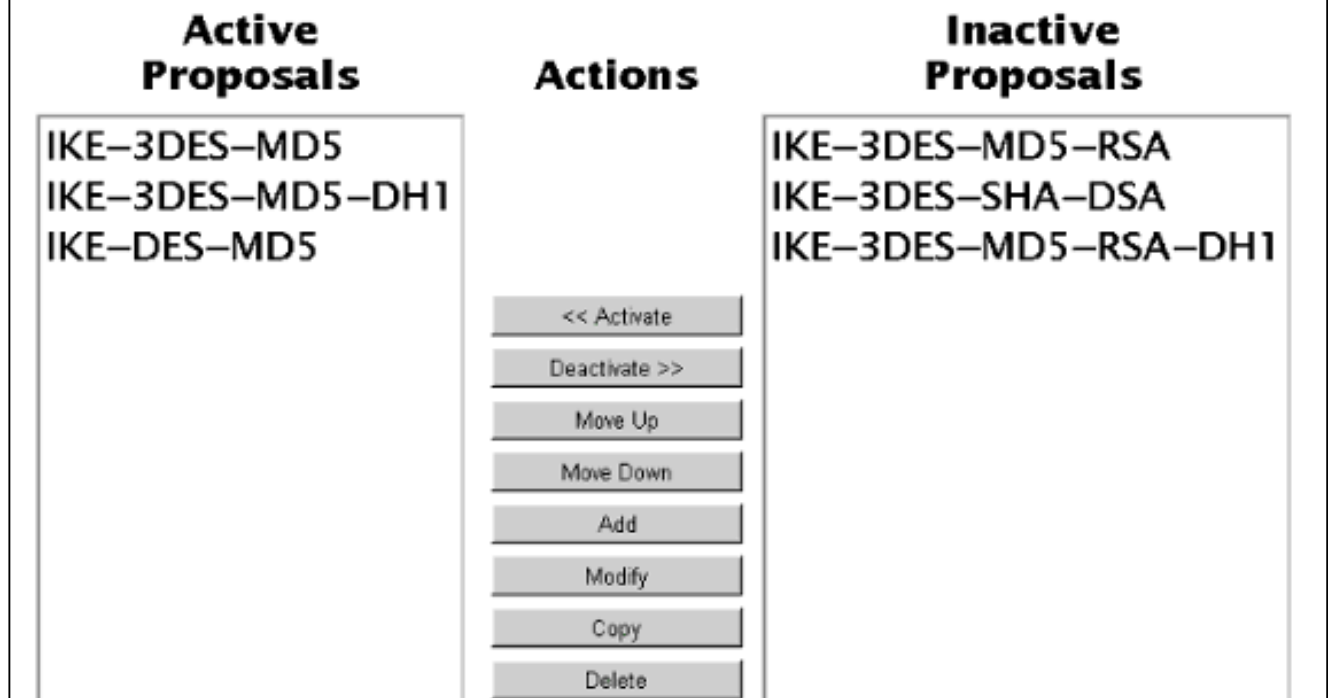
Identity Parameters

| Attribute | Value | Description |
|--------------------|--|---|
| User Name | <input type="text" value="37297304"/> | Enter a unique user name. |
| Password | <input type="password" value="*****"/> | Enter the user's password. The password must satisfy the group password requirements. |
| Verify | <input type="password" value="*****"/> | Verify the user's password. |
| Group | <input type="text" value="vpn3000"/> | Enter the group to which this user belongs. |
| IP Address | <input type="text"/> | Enter the IP address assigned to this user. |
| Subnet Mask | <input type="text"/> | Enter the subnet mask assigned to this user. |

3. 使用IPSec > IKE建议屏幕添加IKE设置(显示的设置是系统默认值):

Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority.

Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by [Security Associations](#) to specify IKE parameters.



[测试Cisco VPN Client和VPN 3000集中器，不用SDI](#)

修改完VPN 3000集中器上的现有配置后，我们安装Cisco VPN客户端，并配置终止在172.18.124.134(集中器的公共接口)的新连接。我们的组访问信息是“vpn3000”(组名称)，组密码则是该组的密码。当我们点击Connect时，username是“37297304”(用户的名称)，user password是用户的密码(存储在本地VPN 3000集中器中;SDI没有介入)。请参阅[成功的使用本地认证的IPSec调试](#)关于IKE，IKEDBG，IKEDECODE，IPSEC，IPSECDBG，IPSECDECODE调试。

[没有VPN 3000集中器的测试SDI服务器操作](#)

UNIX (Solaris)

1. 使用Solaris admintool，在SDI服务器上，请创建sditest帐户。/etc/passwd条目应该看起来象：
sditest:x:76:10::/local/0/sditest:/local/0/opt/ace/prog/sdshell **注意：**数值、到用户主目录的路径和“sdshell”取决于系统。
2. 分配标记到sditest。
3. 尝试远程登录到UNIX主机作为sditest。主机提示您输入UNIX密码和密码。在验证以后，它让您进来作为在该主机的sditest。

Microsoft Windows NT

1. 安装SecurSight代理程序。
2. 选择Programs> SecurSight >测验验证。

配置SDI/User与VPN 3000集中器谈

请使用以下步骤配置SDI/User与VPN 3000集中器谈：

1. 在SDI Server Edit Token屏幕上，确认token为“Enabled”，而不是“New PIN”模式。
2. 单击再同步标记和集合PIN对下Tokencode。



3. 在Edit User屏幕上，将令牌分配给用户，并检验“允许创建PIN”是否未被检查。
4. 点击客户端激活并且验证VPN 3000集中器包括。

Edit User

First and last name:

Default login:

Default shell:

Local User Remote User

| Serial Number | Type | Status |
|---------------|---------|---------|
| 000037297304 | Key Fob | Enabled |

O: Original token R: Replacement for previous token

Role: <none>

Assigned Profile:

Temporary user
 Start date: 12/31/1985 , 19:00 End date: 12/31/1985 , 19:00

Allowed to create a PIN Required to create a PIN

| | | |
|-----------------------------|---------------------------|-----------------------------|
| Assign Token... | Edit Assigned Token... | Administrative Role... |
| Group Memberships... | Client Activations... | Edit User Extension Data... |
| Set/Change User Password... | Remove User Password | Edit Access Times... |
| Assign Profile... | Remove Profile Assignment | Delete User |

OK Cancel Apply L/S Changes Set All L/S Help

注意：VPN 3000集中器认为SDI服务器的客户端;下面的屏幕是SDI服务器Add/Edit Client屏幕。由于这是一个新的客户端，“发送的节点秘密”方框变灰。SDI服务器没有机会发送“节点秘密”文件到集中器(此文件在集中器的Administration > File Management > Files部分显示为“SECURID”)。从VPN 3000进行成功验证之后，“节点秘密”文件将显示在VPN 3000集中器上，“被发送的节点秘密”机箱将被检查。

5. 点击**用户激活**并且验证用户包括。

[配置并且测试VPN 3000集中器对SDI](#)

请使用以下步骤配置和测试VPN 3000集中器到SDI。

1. 请使用以下屏幕配置VPN 3000集中器验证到SDI
：

Change a configured user authentication server.

Server Type

Selecting *Internal Server* will let you add users to the internal user database.

Authentication Server

Enter IP address or hostname.

Server Port

Enter 0 for default port (5500).

Timeout

Enter the timeout for this server (seconds).

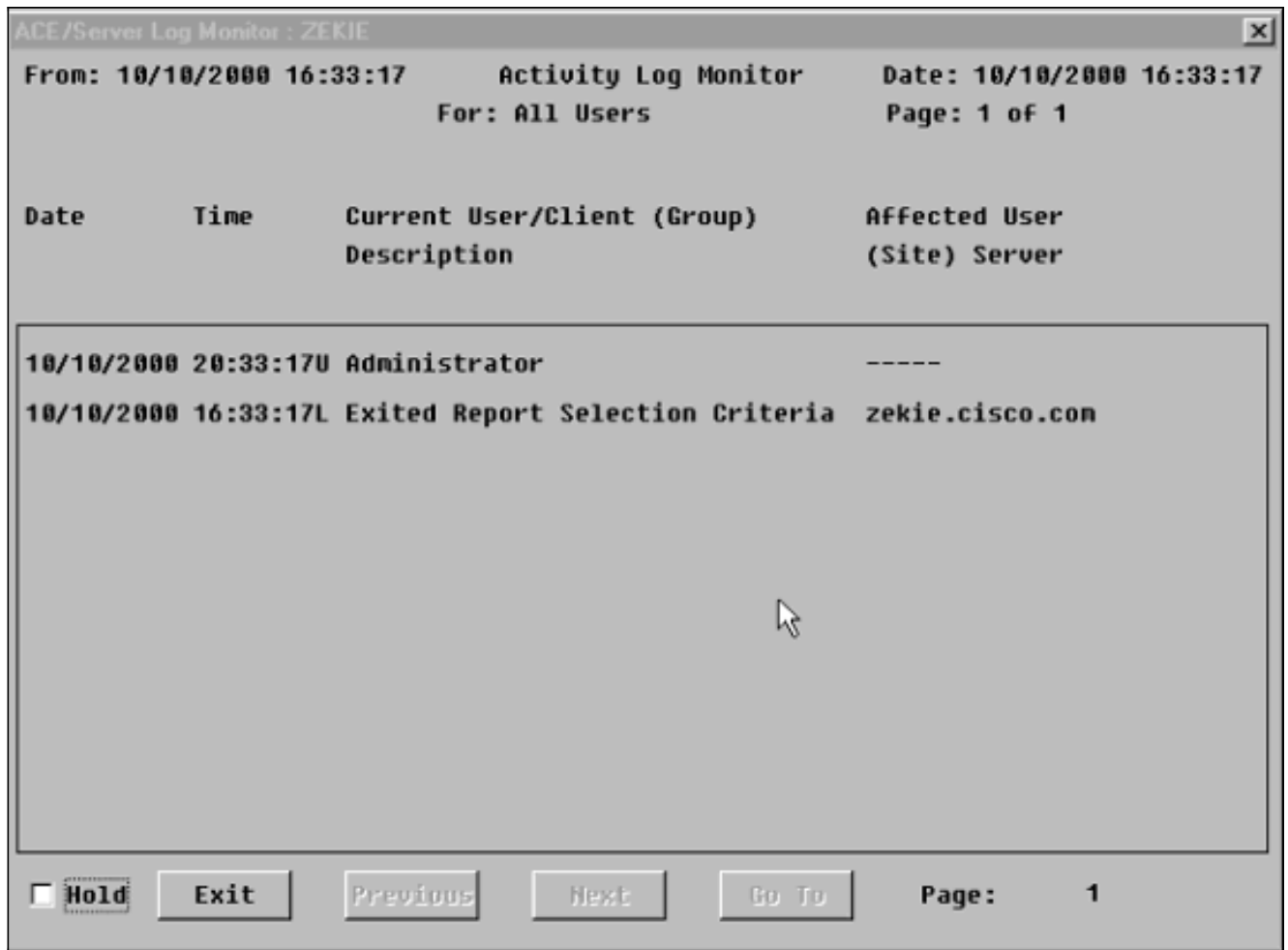
Retries

Enter the number of retries for this server.

Apply

Cancel

2. 从SDI选择Report>Log Monitor>Activity Monitor，并点击OK，遵守流入请求。



3. 在VPN 3000集中器上，请点击**测验**测试连接。

This section lets you configure parameters for servers that authenticate users.

You should have a properly configured RADIUS, NT Domain, or SDI server to access, or you can configure the internal server and [add users to the internal database](#).

Click the **Add** button to add a server, or select a server and click **Modify**, **Delete**, **Move**, or **Test**.

| Authentication Servers | Actions |
|--|---|
| Internal (Internal) 172.18.124.99 (SDI) | <input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Test"/> |

4. 如果验证是好，VPN 3000集中器显示：**成功的验证**

在上述示例中，我们定义一个全局SDI服务器。我们也可以为每组选择性定义各自的SDI服务器，方法是选择Configuration >User Management>Groups，突出显示各自的组，并选择Modify Auth Server。

调试信息，参考本文的以下部分：

- [启用 VPN 3000 集中器上的调试](#)
- [成功的使用 SDI 时的调试](#)
- [错误调试](#)

[验证](#)

本部分所提供的信息可用于确认您的配置是否正常工作。

[测试使用 SDI 时的 Cisco VPN 客户端到VPN 3000 集中器](#)

如果到此点的一切正常运行，便需要结合使用Cisco VPN客户端、VPN 3000集中器和SDI服务器。通过修改我们称之为“vpn3000”的工作组，来发送请求到SDI服务器，我们需要在VPN 3000集中器

上做某种更改。

Configuration | User Management | Groups | Modify vpn3000

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

Identity General **IPSec** PPTP/L2TP

| IPSec Parameters | | | |
|-------------------------------|-------------------------------------|-------------------------------------|---|
| Attribute | Value | Inherit? | Description |
| IPSec SA | ESP-3DES-MD5 | <input checked="" type="checkbox"/> | Select the group's IPSec Security Association. |
| Tunnel Type | Remote Access | <input checked="" type="checkbox"/> | Select the type of tunnel for this group. Update the Remote Access parameters below as needed |
| Remote Access Parameters | | | |
| Group Lock | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Lock users into this group. |
| Authentication | SDI | <input type="checkbox"/> | Select the authentication method for users in this group. |
| Mode Configuration | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Check to use Mode Configuration for users of this group. Update parameters below if checked. |
| Mode Configuration Parameters | | | |
| Banner | <input type="text"/> | <input checked="" type="checkbox"/> | Enter the banner for this group. |

故障排除

本部分提供的信息可用于对配置进行故障排除。

启用 VPN 3000 集中器上的调试

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

This screen lets you add and configure an event class for special handling.

| | | |
|----------------------------|---|--|
| Class Name | <input type="text" value="Select Class"/> | Select the event class to configure. |
| Enable | <input type="checkbox"/> | Check to enable special handling of this class. |
| Severity to Log | <input type="text" value="1-5"/> | Select the range of severity values to enter in the log. |
| Severity to Console | <input type="text" value="1-3"/> | Select the range of severity values to display on the console. |
| Severity to Syslog | <input type="text" value="None"/> | Select the range of severity values to send to a Syslog server. |
| Severity to Email | <input type="text" value="None"/> | Select the range of severity values to send via email to the recipient list. |
| Severity to Trap | <input type="text" value="None"/> | Select the range of severity values to send to an SNMP system. |

单击获得日志查看调试操作的结果。

Monitoring | Event Log

Select Filter Options

Event Class

AUTH
AUTHDBG
AUTHDECODE

Severities

1
2
3

Client IP Address

Events/Page

Direction

[成功的使用本地认证的 IPsec 调试](#)

1 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=1 161.44.17.135

```
ISAKMP HEADER :      ( Version 1.0 )
  Initiator Cookie(8): 9D F3 34 FE 89 BF AA B2
  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 :             307
```

7 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=1 161.44.17.135

```
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + NONE (0)
... total length : 307
```

10 10/10/2000 17:12:32.560 SEV=9 IKEDBG/0 RPT=2 161.44.17.135
processing SA payload

11 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=2 161.44.17.135

```
SA Payload Decode :
  DOI :                IPSEC (1)
  Situation :          Identity Only (1)
  Length :             120
```

14 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=3 161.44.17.135

```
Proposal Decode:
  Proposal # :          1
  Protocol ID :         ISAKMP (1)
  #of Transforms:      4
  Spi :               00 00 00 00
  Length :            108
```

18 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=4 161.44.17.135

```
Transform # 1 Decode for Proposal # 1:
  Transform # :         1
  Transform ID :        IKE (1)
  Length :            24
```

20 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=5 161.44.17.135

Phase 1 SA Attribute Decode for Transform # 1:

Encryption Alg: DES-CBC (1)
Hash Alg : MD5 (1)
DH Group : Oakley Group 1 (1)
Auth Method : Preshared Key (1)

24 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=6 161.44.17.135

Transform # 2 Decode for Proposal # 1:

Transform # : 2
Transform ID : IKE (1)
Length : 24

26 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=7 161.44.17.135

Phase 1 SA Attribute Decode for Transform # 2:

Encryption Alg: Triple-DES (5)
Hash Alg : MD5 (1)
DH Group : Oakley Group 1 (1)
Auth Method : Preshared Key (1)

30 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=8 161.44.17.135

Transform # 3 Decode for Proposal # 1:

Transform # : 3
Transform ID : IKE (1)
Length : 24

32 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=9 161.44.17.135

Phase 1 SA Attribute Decode for Transform # 3:

Encryption Alg: Triple-DES (5)
Hash Alg : SHA (2)
DH Group : Oakley Group 1 (1)
Auth Method : Preshared Key (1)

36 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=10 161.44.17.135

Transform # 4 Decode for Proposal # 1:

Transform # : 4
Transform ID : IKE (1)
Length : 24

38 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=11 161.44.17.135

Phase 1 SA Attribute Decode for Transform # 4:

Encryption Alg: DES-CBC (1)
Hash Alg : SHA (2)
DH Group : Oakley Group 1 (1)
Auth Method : Preshared Key (1)

42 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=3 161.44.17.135

Proposal # 1, Transform # 1, Type ISAKMP, Id IKE

Parsing received transform:

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

47 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=4 161.44.17.135

Phase 1 failure against global IKE proposal # 2:

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

50 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=5 161.44.17.135

Proposal # 1, Transform # 2, Type ISAKMP, Id IKE

Parsing received transform:

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

55 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=6 161.44.17.135
Proposal # 1, Transform # 3, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

60 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=7 161.44.17.135
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class Hash Alg:
Rcv'd: SHA
Cfg'd: MD5

62 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=8 161.44.17.135
Phase 1 failure against global IKE proposal # 3:
Mismatched attr types for class Encryption Alg:
Rcv'd: Triple-DES
Cfg'd: DES-CBC

65 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=9 161.44.17.135
Proposal # 1, Transform # 4, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

70 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=10 161.44.17.135
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

73 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=11 161.44.17.135
Phase 1 failure against global IKE proposal # 3:
Mismatched attr types for class Hash Alg:
Rcv'd: SHA
Cfg'd: MD5

75 10/10/2000 17:12:32.560 SEV=7 IKEDBG/0 RPT=12 161.44.17.135
Oakley proposal is acceptable

76 10/10/2000 17:12:32.560 SEV=9 IKEDBG/0 RPT=13 161.44.17.135
processing ke payload

77 10/10/2000 17:12:32.560 SEV=9 IKEDBG/0 RPT=14 161.44.17.135
processing ISA_KE

78 10/10/2000 17:12:32.560 SEV=9 IKEDBG/1 RPT=1 161.44.17.135
processing nonce payload

79 10/10/2000 17:12:32.560 SEV=9 IKEDBG/1 RPT=2 161.44.17.135
Processing ID

80 10/10/2000 17:12:32.560 SEV=9 IKEDBG/1 RPT=3 161.44.17.135
processing vid payload

81 10/10/2000 17:12:32.580 SEV=9 IKEDBG/23 RPT=1 161.44.17.135

Starting group lookup for peer 161.44.17.135

82 10/10/2000 17:12:32.680 SEV=7 IKEDBG/0 RPT=15 161.44.17.135
Found Phase 1 Group (vpn3000)

83 10/10/2000 17:12:32.680 SEV=7 IKEDBG/14 RPT=1 161.44.17.135
Authentication configured for Internal

84 10/10/2000 17:12:32.680 SEV=9 IKEDBG/0 RPT=16 161.44.17.135
constructing ISA_SA for isakmp

85 10/10/2000 17:12:32.680 SEV=9 IKEDBG/0 RPT=17 161.44.17.135
constructing ke payload

86 10/10/2000 17:12:32.680 SEV=9 IKEDBG/1 RPT=4 161.44.17.135
constructing nonce payload

87 10/10/2000 17:12:32.680 SEV=9 IKE/0 RPT=1 161.44.17.135
Generating keys for Responder...

88 10/10/2000 17:12:32.680 SEV=9 IKEDBG/1 RPT=5 161.44.17.135
constructing ID

89 10/10/2000 17:12:32.680 SEV=9 IKEDBG/0 RPT=18
construct hash payload

90 10/10/2000 17:12:32.680 SEV=9 IKEDBG/0 RPT=19 161.44.17.135
computing hash

91 10/10/2000 17:12:32.680 SEV=9 IKEDBG/1 RPT=6 161.44.17.135
constructing vid payload

92 10/10/2000 17:12:32.680 SEV=8 IKEDBG/0 RPT=20 161.44.17.135
SENDING Message (msgid=0) with payloads :
HDR + SA (1) ... total length : 248

93 10/10/2000 17:12:32.730 SEV=8 IKEDECODE/0 RPT=12 161.44.17.135
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): 9D F3 34 FE 89 BF AA B2
Responder Cookie(8): B7 AD 34 D2 74 4D 05 DA
Next Payload : HASH (8)
Exchange Type : Oakley Aggressive Mode
Flags : 1 (ENCRYPT)
Message ID : 0
Length : 52

99 10/10/2000 17:12:32.730 SEV=8 IKEDBG/0 RPT=21 161.44.17.135
RECEIVED Message (msgid=0) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

101 10/10/2000 17:12:32.730 SEV=9 IKEDBG/0 RPT=22 161.44.17.135
processing hash

102 10/10/2000 17:12:32.730 SEV=9 IKEDBG/0 RPT=23 161.44.17.135
computing hash

103 10/10/2000 17:12:33.410 SEV=8 IKEDECODE/0 RPT=13 161.44.17.135
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): 9D F3 34 FE 89 BF AA B2
Responder Cookie(8): B7 AD 34 D2 74 4D 05 DA
Next Payload : HASH (8)
Exchange Type : Oakley Quick Mode
Flags : 1 (ENCRYPT)
Message ID : 48687ca1

Length : 308

110 10/10/2000 17:12:33.410 SEV=9 IKEDBG/21 RPT=1 161.44.17.135
Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

111 10/10/2000 17:12:33.410 SEV=9 IKEDBG/0 RPT=24 161.44.17.135
constructing blank hash

112 10/10/2000 17:12:33.410 SEV=9 IKEDBG/0 RPT=25 161.44.17.135
constructing qm hash

113 10/10/2000 17:12:33.410 SEV=8 IKEDBG/0 RPT=26 161.44.17.135
SENDING Message (msgid=fc2ce5eb) with payloads :
HDR + HASH (8) ... total length : 68

115 10/10/2000 17:12:44.680 SEV=8 IKEDECODE/0 RPT=14 161.44.17.135
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): 9D F3 34 FE 89 BF AA B2
Responder Cookie(8): B7 AD 34 D2 74 4D 05 DA
Next Payload : HASH (8)
Exchange Type : Oakley Transactional
Flags : 1 (ENCRYPT)
Message ID : fc2ce5eb
Length : 92

122 10/10/2000 17:12:44.680 SEV=8 IKEDBG/0 RPT=27 161.44.17.135
RECEIVED Message (msgid=fc2ce5eb) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 85

124 10/10/2000 17:12:44.680 SEV=9 IKEDBG/1 RPT=7
process_attr(): Enter!

125 10/10/2000 17:12:44.680 SEV=9 IKEDBG/1 RPT=8
Processing cfg reply attributes.

126 10/10/2000 17:12:44.980 SEV=7 IKEDBG/14 RPT=2 161.44.17.135
User [37297304]
Authentication configured for Internal

127 10/10/2000 17:12:44.980 SEV=4 IKE/52 RPT=7 161.44.17.135
User [37297304]
User (37297304) authenticated.

128 10/10/2000 17:12:44.980 SEV=9 IKEDBG/31 RPT=1 161.44.17.135
User [37297304]
Obtained IP addr (192.168.1.1) prior to initiating Mode Cfg (XAuth enabled)

130 10/10/2000 17:12:44.980 SEV=9 IKEDBG/0 RPT=28 161.44.17.135
User [37297304]
constructing blank hash

131 10/10/2000 17:12:44.980 SEV=9 IKEDBG/0 RPT=29 161.44.17.135
0000: 00010004 C0A80101 F0010000

132 10/10/2000 17:12:44.980 SEV=9 IKEDBG/0 RPT=30 161.44.17.135
User [37297304]
constructing QM hash

133 10/10/2000 17:12:44.980 SEV=8 IKEDBG/0 RPT=31 161.44.17.135
SENDING Message (msgid=fc2ce5eb) with payloads :
HDR + HASH (8) ... total length : 80

135 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=15 161.44.17.135
ISAKMP HEADER : (Version 1.0)

Initiator Cookie(8): 9D F3 34 FE 89 BF AA B2
Responder Cookie(8): B7 AD 34 D2 74 4D 05 DA
Next Payload : HASH (8)
Exchange Type : Oakley Transactional
Flags : 1 (ENCRYPT)
Message ID : fc2ce5eb
Length : 68

142 10/10/2000 17:12:44.990 SEV=8 IKEDBG/0 RPT=32 161.44.17.135
RECEIVED Message (msgid=fc2ce5eb) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 64

144 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=9
process_attr(): Enter!

145 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=10
Processing cfg ACK attributes

146 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=11
Received IPV4 address ack!

147 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=12
Received Save PW ack!

148 10/10/2000 17:12:44.990 SEV=4 AUTH/21 RPT=18
User 37297304 connected

149 10/10/2000 17:12:44.990 SEV=7 IKEDBG/22 RPT=1 161.44.17.135
User [37297304]
Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

151 10/10/2000 17:12:44.990 SEV=8 IKEDBG/0 RPT=33 161.44.17.135
RECEIVED Message (msgid=48687ca1) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0)
... total length : 304

154 10/10/2000 17:12:44.990 SEV=9 IKEDBG/0 RPT=34 161.44.17.135
User [37297304]
processing hash

155 10/10/2000 17:12:44.990 SEV=9 IKEDBG/0 RPT=35 161.44.17.135
User [37297304]
processing SA payload

156 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=16 161.44.17.135
SA Payload Decode :
DOI : IPSEC (1)
Situation : Identity Only (1)
Length : 180

159 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=17 161.44.17.135
Proposal Decode:
Proposal # : 1
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 99 15 18 B4
Length : 28

163 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=18 161.44.17.135
Transform # 1 Decode for Proposal # 1:
Transform # : 1
Transform ID : DES-CBC (2)
Length : 16

165 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=19 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
HMAC Algorithm: MD5 (1)
Encapsulation : Tunnel (1)

167 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=20 161.44.17.135
Proposal Decode:
Proposal # : 2
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 99 15 18 B4
Length : 28

171 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=21 161.44.17.135
Transform # 1 Decode for Proposal # 2:
Transform # : 1
Transform ID : Triple-DES (3)
Length : 16

173 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=22 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
HMAC Algorithm: MD5 (1)
Encapsulation : Tunnel (1)

175 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=23 161.44.17.135
Proposal Decode:
Proposal # : 3
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 99 15 18 B4
Length : 28

179 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=24 161.44.17.135
Transform # 1 Decode for Proposal # 3:
Transform # : 1
Transform ID : DES-CBC (2)
Length : 16

181 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=25 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
HMAC Algorithm: SHA (2)
Encapsulation : Tunnel (1)

183 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=26 161.44.17.135
Proposal Decode:
Proposal # : 4
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 99 15 18 B4
Length : 28

187 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=27 161.44.17.135
Transform # 1 Decode for Proposal # 4:
Transform # : 1
Transform ID : Triple-DES (3)
Length : 16

189 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=28 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
HMAC Algorithm: SHA (2)
Encapsulation : Tunnel (1)

191 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=29 161.44.17.135
Proposal Decode:

Proposal # : 5
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 99 15 18 B4
Length : 28

195 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=30 161.44.17.135

Transform # 1 Decode for Proposal # 5:

Transform # : 1
Transform ID : NULL (11)
Length : 16

197 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=31 161.44.17.135

Phase 2 SA Attribute Decode for Transform # 1:

HMAC Algorithm: MD5 (1)
Encapsulation : Tunnel (1)

199 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=32 161.44.17.135

Proposal Decode:

Proposal # : 6
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 99 15 18 B4
Length : 28

203 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=33 161.44.17.135

Transform # 1 Decode for Proposal # 6:

Transform # : 1
Transform ID : NULL (11)
Length : 16

205 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=34 161.44.17.135

Phase 2 SA Attribute Decode for Transform # 1:

HMAC Algorithm: SHA (2)
Encapsulation : Tunnel (1)

207 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=13 161.44.17.135

User [37297304]

processing nonce payload

208 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=14 161.44.17.135

User [37297304]

Processing ID

209 10/10/2000 17:12:44.990 SEV=5 IKE/25 RPT=13 161.44.17.135

User [37297304]

Received remote Proxy Host data in ID Payload:

Address 161.44.17.135, Protocol 0, Port 0

212 10/10/2000 17:12:44.990 SEV=7 IKEDBG/1 RPT=15 161.44.17.135

User [37297304]

Modifying client proxy src address!

213 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=16 161.44.17.135

User [37297304]

Processing ID

214 10/10/2000 17:12:44.990 SEV=5 IKE/24 RPT=7 161.44.17.135

User [37297304]

Received local Proxy Host data in ID Payload:

Address 172.18.124.134, Protocol 0, Port 0

217 10/10/2000 17:12:44.990 SEV=9 IKEDBG/0 RPT=36 161.44.17.135

User [37297304]

Processing Notify payload

218 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=35 161.44.17.135

Notify Payload Decode :

DOI : IPSEC (1)
Protocol : ISAKMP (1)
Message : Initial contact (24578)
Spi : 9D F3 34 FE 89 BF AA B2 B7 AD 34 D2 74 4D 05 DA
Length : 28

224 10/10/2000 17:12:44.990 SEV=8 IKEDBG/0 RPT=37

QM IsRekeyed old sa not found by addr

225 10/10/2000 17:12:44.990 SEV=5 IKE/66 RPT=13 161.44.17.135

User [37297304]

IKE Remote Peer configured for SA: ESP-3DES-MD5

226 10/10/2000 17:12:44.990 SEV=9 IKEDBG/0 RPT=38 161.44.17.135

User [37297304]

processing IPSEC SA

227 10/10/2000 17:12:44.990 SEV=8 IKEDBG/0 RPT=39

Proposal # 1, Transform # 1, Type ESP, Id DES-CBC

Parsing received transform:

Phase 2 failure:

Mismatched transform IDs for protocol ESP:

Rcv'd: DES-CBC

Cfg'd: Triple-DES

232 10/10/2000 17:12:45.000 SEV=7 IKEDBG/27 RPT=1 161.44.17.135

User [37297304]

IPSec SA Proposal # 2, Transform # 1 acceptable

233 10/10/2000 17:12:45.000 SEV=7 IKEDBG/0 RPT=40 161.44.17.135

User [37297304]

IKE: requesting SPI!

234 10/10/2000 17:12:45.000 SEV=6 IKE/0 RPT=2

AM received unexpected event EV_ACTIVATE_NEW_SA in state AM_ACTIVE

235 10/10/2000 17:12:45.000 SEV=9 IPSECDBG/6 RPT=1

IPSEC key message parse - msgtype 6, len 164, vers 1, pid 00000000, seq 13,
err 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0,
hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 300,
lifetime2 2000000000, dsId 2

239 10/10/2000 17:12:45.000 SEV=9 IPSECDBG/1 RPT=1

Processing KEY_GETSPI msg!

240 10/10/2000 17:12:45.000 SEV=7 IPSECDBG/13 RPT=1

Reserved SPI 1773955517

241 10/10/2000 17:12:45.000 SEV=8 IKEDBG/6 RPT=1

IKE got SPI from key engine: SPI = 0x69bc69bd

242 10/10/2000 17:12:45.000 SEV=9 IKEDBG/0 RPT=41 161.44.17.135

User [37297304]

oakley constructing quick mode

243 10/10/2000 17:12:45.000 SEV=9 IKEDBG/0 RPT=42 161.44.17.135

User [37297304]

constructing blank hash

244 10/10/2000 17:12:45.000 SEV=9 IKEDBG/0 RPT=43 161.44.17.135

User [37297304]
constructing ISA_SA for ipsec

245 10/10/2000 17:12:45.000 SEV=9 IKEDBG/1 RPT=17 161.44.17.135
User [37297304]
constructing ipsec nonce payload

246 10/10/2000 17:12:45.000 SEV=9 IKEDBG/1 RPT=18 161.44.17.135
User [37297304]
constructing proxy ID

247 10/10/2000 17:12:45.000 SEV=7 IKEDBG/0 RPT=44 161.44.17.135
User [37297304]
Transmitting Proxy Id:
Remote host: 192.168.1.1 Protocol 0 Port 0
Local host: 172.18.124.134 Protocol 0 Port 0

251 10/10/2000 17:12:45.000 SEV=9 IKEDBG/0 RPT=45 161.44.17.135
User [37297304]
constructing QM hash

252 10/10/2000 17:12:45.000 SEV=8 IKEDBG/0 RPT=46 161.44.17.135
SENDING Message (msgid=48687ca1) with payloads :
HDR + HASH (8) ... total length : 136

254 10/10/2000 17:12:45.010 SEV=8 IKEDECODE/0 RPT=36 161.44.17.135
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): 9D F3 34 FE 89 BF AA B2
Responder Cookie(8): B7 AD 34 D2 74 4D 05 DA
Next Payload : HASH (8)
Exchange Type : Oakley Quick Mode
Flags : 1 (ENCRYPT)
Message ID : 48687ca1
Length : 52

261 10/10/2000 17:12:45.010 SEV=8 IKEDBG/0 RPT=47 161.44.17.135
RECEIVED Message (msgid=48687ca1) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

263 10/10/2000 17:12:45.010 SEV=9 IKEDBG/0 RPT=48 161.44.17.135
User [37297304]
processing hash

264 10/10/2000 17:12:45.010 SEV=9 IKEDBG/0 RPT=49 161.44.17.135
User [37297304]
loading all IPSEC SAs

265 10/10/2000 17:12:45.010 SEV=9 IKEDBG/1 RPT=19 161.44.17.135
User [37297304]
Generating Quick Mode Key!

266 10/10/2000 17:12:45.010 SEV=9 IKEDBG/1 RPT=20 161.44.17.135
User [37297304]
Generating Quick Mode Key!

267 10/10/2000 17:12:45.020 SEV=7 IKEDBG/0 RPT=50 161.44.17.135
User [37297304]
Loading host:
Dst: 172.18.124.134
Src: 192.168.1.1

268 10/10/2000 17:12:45.020 SEV=4 IKE/49 RPT=13 161.44.17.135
User [37297304]
Security negotiation complete for User (37297304)

Responder, Inbound SPI = 0x69bc69bd, Outbound SPI = 0x991518b4

271 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/6 RPT=2
IPSEC key message parse - msgtype 1, Len 536, vers 1, pid 00000000, seq 0,
err 0, type 2, mode 1, state 64, label 0, pad 0, spi 991518b4, encrKeyLen 24,
hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 0,
lifetime2 0, dsId 2

274 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=2
Processing KEY_ADD MSG!

275 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=3
key_msghdr2secassoc(): Enter

276 10/10/2000 17:12:45.020 SEV=7 IPSECDBG/1 RPT=4
No USER filter configured

277 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=5
KeyProcessAdd: Enter

278 10/10/2000 17:12:45.020 SEV=8 IPSECDBG/1 RPT=6
KeyProcessAdd: Adding outbound SA

279 10/10/2000 17:12:45.020 SEV=8 IPSECDBG/1 RPT=7
KeyProcessAdd: src 172.18.124.134 mask 0.0.0.0, dst 192.168.1.1 mask 0.0.0.0

280 10/10/2000 17:12:45.020 SEV=8 IPSECDBG/1 RPT=8
KeyProcessAdd: FilterIpsecAddIkeSa success

281 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/6 RPT=3
IPSEC key message parse - msgtype 3, Len 292, vers 1, pid 00000000, seq 0,
err 0, type 2, mode 1, state 32, label 0, pad 0, spi 69bc69bd, encrKeyLen 24,
hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 0,
lifetime2 0, dsId 2

284 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=9
Processing KEY_UPDATE MSG!

285 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=10
Update inbound SA addresses

286 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=11
key_msghdr2secassoc(): Enter

287 10/10/2000 17:12:45.020 SEV=7 IPSECDBG/1 RPT=12
No USER filter configured

288 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=13
KeyProcessUpdate: Enter

289 10/10/2000 17:12:45.020 SEV=8 IPSECDBG/1 RPT=14
KeyProcessUpdate: success

290 10/10/2000 17:12:45.020 SEV=8 IKEDBG/7 RPT=1
IKE got a KEY_ADD MSG for SA: SPI = 0x991518b4

291 10/10/2000 17:12:45.020 SEV=8 IKEDBG/0 RPT=51
pitcher: rcv KEY_UPDATE, spi 0x69bc69bd

[成功的使用本地认证的 IPsec 调试](#)

1 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=1 161.44.17.135
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): 9D F3 34 FE 89 BF AA B2
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 : 307

7 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=1 161.44.17.135
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + NONE (0)
... total length : 307

10 10/10/2000 17:12:32.560 SEV=9 IKEDBG/0 RPT=2 161.44.17.135
processing SA payload

11 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=2 161.44.17.135
SA Payload Decode :
DOI : IPSEC (1)
Situation : Identity Only (1)
Length : 120

14 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=3 161.44.17.135
Proposal Decode:
Proposal # : 1
Protocol ID : ISAKMP (1)
#of Transforms: 4
Spi : 00 00 00 00
Length : 108

18 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=4 161.44.17.135
Transform # 1 Decode for Proposal # 1:
Transform # : 1
Transform ID : IKE (1)
Length : 24

20 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=5 161.44.17.135
Phase 1 SA Attribute Decode for Transform # 1:
Encryption Alg: DES-CBC (1)
Hash Alg : MD5 (1)
DH Group : Oakley Group 1 (1)
Auth Method : Preshared Key (1)

24 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=6 161.44.17.135
Transform # 2 Decode for Proposal # 1:
Transform # : 2
Transform ID : IKE (1)
Length : 24

26 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=7 161.44.17.135
Phase 1 SA Attribute Decode for Transform # 2:
Encryption Alg: Triple-DES (5)
Hash Alg : MD5 (1)
DH Group : Oakley Group 1 (1)
Auth Method : Preshared Key (1)

30 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=8 161.44.17.135
Transform # 3 Decode for Proposal # 1:
Transform # : 3
Transform ID : IKE (1)
Length : 24

32 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=9 161.44.17.135
Phase 1 SA Attribute Decode for Transform # 3:
Encryption Alg: Triple-DES (5)
Hash Alg : SHA (2)

DH Group : Oakley Group 1 (1)
Auth Method : Preshared Key (1)

36 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=10 161.44.17.135

Transform # 4 Decode for Proposal # 1:

Transform # : 4
Transform ID : IKE (1)
Length : 24

38 10/10/2000 17:12:32.560 SEV=8 IKEDECODE/0 RPT=11 161.44.17.135

Phase 1 SA Attribute Decode for Transform # 4:

Encryption Alg: DES-CBC (1)
Hash Alg : SHA (2)
DH Group : Oakley Group 1 (1)
Auth Method : Preshared Key (1)

42 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=3 161.44.17.135

Proposal # 1, Transform # 1, Type ISAKMP, Id IKE

Parsing received transform:

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

47 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=4 161.44.17.135

Phase 1 failure against global IKE proposal # 2:

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

50 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=5 161.44.17.135

Proposal # 1, Transform # 2, Type ISAKMP, Id IKE

Parsing received transform:

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

55 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=6 161.44.17.135

Proposal # 1, Transform # 3, Type ISAKMP, Id IKE

Parsing received transform:

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

60 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=7 161.44.17.135

Phase 1 failure against global IKE proposal # 2:

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

62 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=8 161.44.17.135

Phase 1 failure against global IKE proposal # 3:

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

65 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=9 161.44.17.135

Proposal # 1, Transform # 4, Type ISAKMP, Id IKE

Parsing received transform:

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

Cfg'd: Oakley Group 2

70 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=10 161.44.17.135
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

73 10/10/2000 17:12:32.560 SEV=8 IKEDBG/0 RPT=11 161.44.17.135
Phase 1 failure against global IKE proposal # 3:
Mismatched attr types for class Hash Alg:
Rcv'd: SHA
Cfg'd: MD5

75 10/10/2000 17:12:32.560 SEV=7 IKEDBG/0 RPT=12 161.44.17.135
Oakley proposal is acceptable

76 10/10/2000 17:12:32.560 SEV=9 IKEDBG/0 RPT=13 161.44.17.135
processing ke payload

77 10/10/2000 17:12:32.560 SEV=9 IKEDBG/0 RPT=14 161.44.17.135
processing ISA_KE

78 10/10/2000 17:12:32.560 SEV=9 IKEDBG/1 RPT=1 161.44.17.135
processing nonce payload

79 10/10/2000 17:12:32.560 SEV=9 IKEDBG/1 RPT=2 161.44.17.135
Processing ID

80 10/10/2000 17:12:32.560 SEV=9 IKEDBG/1 RPT=3 161.44.17.135
processing vid payload

81 10/10/2000 17:12:32.580 SEV=9 IKEDBG/23 RPT=1 161.44.17.135
Starting group lookup for peer 161.44.17.135

82 10/10/2000 17:12:32.680 SEV=7 IKEDBG/0 RPT=15 161.44.17.135
Found Phase 1 Group (vpn3000)

83 10/10/2000 17:12:32.680 SEV=7 IKEDBG/14 RPT=1 161.44.17.135
Authentication configured for Internal

84 10/10/2000 17:12:32.680 SEV=9 IKEDBG/0 RPT=16 161.44.17.135
constructing ISA_SA for isakmp

85 10/10/2000 17:12:32.680 SEV=9 IKEDBG/0 RPT=17 161.44.17.135
constructing ke payload

86 10/10/2000 17:12:32.680 SEV=9 IKEDBG/1 RPT=4 161.44.17.135
constructing nonce payload

87 10/10/2000 17:12:32.680 SEV=9 IKE/0 RPT=1 161.44.17.135
Generating keys for Responder...

88 10/10/2000 17:12:32.680 SEV=9 IKEDBG/1 RPT=5 161.44.17.135
constructing ID

89 10/10/2000 17:12:32.680 SEV=9 IKEDBG/0 RPT=18
construct hash payload

90 10/10/2000 17:12:32.680 SEV=9 IKEDBG/0 RPT=19 161.44.17.135
computing hash

91 10/10/2000 17:12:32.680 SEV=9 IKEDBG/1 RPT=6 161.44.17.135
constructing vid payload

92 10/10/2000 17:12:32.680 SEV=8 IKEDBG/0 RPT=20 161.44.17.135
SENDING Message (msgid=0) with payloads :
HDR + SA (1) ... total length : 248

93 10/10/2000 17:12:32.730 SEV=8 IKEDECODE/0 RPT=12 161.44.17.135
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): 9D F3 34 FE 89 BF AA B2
Responder Cookie(8): B7 AD 34 D2 74 4D 05 DA
Next Payload : HASH (8)
Exchange Type : Oakley Aggressive Mode
Flags : 1 (ENCRYPT)
Message ID : 0
Length : 52

99 10/10/2000 17:12:32.730 SEV=8 IKEDBG/0 RPT=21 161.44.17.135
RECEIVED Message (msgid=0) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

101 10/10/2000 17:12:32.730 SEV=9 IKEDBG/0 RPT=22 161.44.17.135
processing hash

102 10/10/2000 17:12:32.730 SEV=9 IKEDBG/0 RPT=23 161.44.17.135
computing hash

103 10/10/2000 17:12:33.410 SEV=8 IKEDECODE/0 RPT=13 161.44.17.135
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): 9D F3 34 FE 89 BF AA B2
Responder Cookie(8): B7 AD 34 D2 74 4D 05 DA
Next Payload : HASH (8)
Exchange Type : Oakley Quick Mode
Flags : 1 (ENCRYPT)
Message ID : 48687ca1
Length : 308

110 10/10/2000 17:12:33.410 SEV=9 IKEDBG/21 RPT=1 161.44.17.135
Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

111 10/10/2000 17:12:33.410 SEV=9 IKEDBG/0 RPT=24 161.44.17.135
constructing blank hash

112 10/10/2000 17:12:33.410 SEV=9 IKEDBG/0 RPT=25 161.44.17.135
constructing qm hash

113 10/10/2000 17:12:33.410 SEV=8 IKEDBG/0 RPT=26 161.44.17.135
SENDING Message (msgid=fc2ce5eb) with payloads :
HDR + HASH (8) ... total length : 68

115 10/10/2000 17:12:44.680 SEV=8 IKEDECODE/0 RPT=14 161.44.17.135
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): 9D F3 34 FE 89 BF AA B2
Responder Cookie(8): B7 AD 34 D2 74 4D 05 DA
Next Payload : HASH (8)
Exchange Type : Oakley Transactional
Flags : 1 (ENCRYPT)
Message ID : fc2ce5eb
Length : 92

122 10/10/2000 17:12:44.680 SEV=8 IKEDBG/0 RPT=27 161.44.17.135
RECEIVED Message (msgid=fc2ce5eb) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 85

124 10/10/2000 17:12:44.680 SEV=9 IKEDBG/1 RPT=7
process_attr(): Enter!

125 10/10/2000 17:12:44.680 SEV=9 IKEDBG/1 RPT=8
Processing cfg reply attributes.

126 10/10/2000 17:12:44.980 SEV=7 IKEDBG/14 RPT=2 161.44.17.135
User [37297304]
Authentication configured for Internal

127 10/10/2000 17:12:44.980 SEV=4 IKE/52 RPT=7 161.44.17.135
User [37297304]
User (37297304) authenticated.

128 10/10/2000 17:12:44.980 SEV=9 IKEDBG/31 RPT=1 161.44.17.135
User [37297304]
Obtained IP addr (192.168.1.1) prior to initiating Mode Cfg (XAuth enabled)

130 10/10/2000 17:12:44.980 SEV=9 IKEDBG/0 RPT=28 161.44.17.135
User [37297304]
constructing blank hash

131 10/10/2000 17:12:44.980 SEV=9 IKEDBG/0 RPT=29 161.44.17.135
0000: 00010004 C0A80101 F0010000

132 10/10/2000 17:12:44.980 SEV=9 IKEDBG/0 RPT=30 161.44.17.135
User [37297304]
constructing QM hash

133 10/10/2000 17:12:44.980 SEV=8 IKEDBG/0 RPT=31 161.44.17.135
SENDING Message (msgid=fc2ce5eb) with payloads :
HDR + HASH (8) ... total length : 80

135 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=15 161.44.17.135
ISAKMP HEADER : (Version 1.0)
Initiator Cookie(8): 9D F3 34 FE 89 BF AA B2
Responder Cookie(8): B7 AD 34 D2 74 4D 05 DA
Next Payload : HASH (8)
Exchange Type : Oakley Transactional
Flags : 1 (ENCRYPT)
Message ID : fc2ce5eb
Length : 68

142 10/10/2000 17:12:44.990 SEV=8 IKEDBG/0 RPT=32 161.44.17.135
RECEIVED Message (msgid=fc2ce5eb) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 64

144 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=9
process_attr(): Enter!

145 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=10
Processing cfg ACK attributes

146 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=11
Received IPV4 address ack!

147 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=12
Received Save PW ack!

148 10/10/2000 17:12:44.990 SEV=4 AUTH/21 RPT=18
User 37297304 connected

149 10/10/2000 17:12:44.990 SEV=7 IKEDBG/22 RPT=1 161.44.17.135
User [37297304]
Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

151 10/10/2000 17:12:44.990 SEV=8 IKEDBG/0 RPT=33 161.44.17.135
RECEIVED Message (msgid=48687ca1) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0)
... total length : 304

154 10/10/2000 17:12:44.990 SEV=9 IKEDBG/0 RPT=34 161.44.17.135
User [37297304]
processing hash

155 10/10/2000 17:12:44.990 SEV=9 IKEDBG/0 RPT=35 161.44.17.135
User [37297304]
processing SA payload

156 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=16 161.44.17.135
SA Payload Decode :
DOI : IPSEC (1)
Situation : Identity Only (1)
Length : 180

159 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=17 161.44.17.135
Proposal Decode:
Proposal # : 1
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 99 15 18 B4
Length : 28

163 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=18 161.44.17.135
Transform # 1 Decode for Proposal # 1:
Transform # : 1
Transform ID : DES-CBC (2)
Length : 16

165 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=19 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
HMAC Algorithm: MD5 (1)
Encapsulation : Tunnel (1)

167 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=20 161.44.17.135
Proposal Decode:
Proposal # : 2
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 99 15 18 B4
Length : 28

171 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=21 161.44.17.135
Transform # 1 Decode for Proposal # 2:
Transform # : 1
Transform ID : Triple-DES (3)
Length : 16

173 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=22 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
HMAC Algorithm: MD5 (1)
Encapsulation : Tunnel (1)

175 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=23 161.44.17.135
Proposal Decode:
Proposal # : 3
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 99 15 18 B4
Length : 28

179 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=24 161.44.17.135

Transform # 1 Decode for Proposal # 3:

Transform # : 1
Transform ID : DES-CBC (2)
Length : 16

181 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=25 161.44.17.135

Phase 2 SA Attribute Decode for Transform # 1:

HMAC Algorithm: SHA (2)
Encapsulation : Tunnel (1)

183 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=26 161.44.17.135

Proposal Decode:

Proposal # : 4
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 99 15 18 B4
Length : 28

187 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=27 161.44.17.135

Transform # 1 Decode for Proposal # 4:

Transform # : 1
Transform ID : Triple-DES (3)
Length : 16

189 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=28 161.44.17.135

Phase 2 SA Attribute Decode for Transform # 1:

HMAC Algorithm: SHA (2)
Encapsulation : Tunnel (1)

191 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=29 161.44.17.135

Proposal Decode:

Proposal # : 5
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 99 15 18 B4
Length : 28

195 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=30 161.44.17.135

Transform # 1 Decode for Proposal # 5:

Transform # : 1
Transform ID : NULL (11)
Length : 16

197 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=31 161.44.17.135

Phase 2 SA Attribute Decode for Transform # 1:

HMAC Algorithm: MD5 (1)
Encapsulation : Tunnel (1)

199 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=32 161.44.17.135

Proposal Decode:

Proposal # : 6
Protocol ID : ESP (3)
#of Transforms: 1
Spi : 99 15 18 B4
Length : 28

203 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=33 161.44.17.135

Transform # 1 Decode for Proposal # 6:

Transform # : 1
Transform ID : NULL (11)
Length : 16

205 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=34 161.44.17.135
Phase 2 SA Attribute Decode for Transform # 1:
HMAC Algorithm: SHA (2)
Encapsulation : Tunnel (1)

207 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=13 161.44.17.135
User [37297304]
processing nonce payload

208 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=14 161.44.17.135
User [37297304]
Processing ID

209 10/10/2000 17:12:44.990 SEV=5 IKE/25 RPT=13 161.44.17.135
User [37297304]
Received remote Proxy Host data in ID Payload:
Address 161.44.17.135, Protocol 0, Port 0

212 10/10/2000 17:12:44.990 SEV=7 IKEDBG/1 RPT=15 161.44.17.135
User [37297304]
Modifying client proxy src address!

213 10/10/2000 17:12:44.990 SEV=9 IKEDBG/1 RPT=16 161.44.17.135
User [37297304]
Processing ID

214 10/10/2000 17:12:44.990 SEV=5 IKE/24 RPT=7 161.44.17.135
User [37297304]
Received local Proxy Host data in ID Payload:
Address 172.18.124.134, Protocol 0, Port 0

217 10/10/2000 17:12:44.990 SEV=9 IKEDBG/0 RPT=36 161.44.17.135
User [37297304]
Processing Notify payload

218 10/10/2000 17:12:44.990 SEV=8 IKEDECODE/0 RPT=35 161.44.17.135
Notify Payload Decode :
DOI : IPSEC (1)
Protocol : ISAKMP (1)
Message : Initial contact (24578)
Spi : 9D F3 34 FE 89 BF AA B2 B7 AD 34 D2 74 4D 05 DA
Length : 28

224 10/10/2000 17:12:44.990 SEV=8 IKEDBG/0 RPT=37
QM IsRekeyed old sa not found by addr

225 10/10/2000 17:12:44.990 SEV=5 IKE/66 RPT=13 161.44.17.135
User [37297304]
IKE Remote Peer configured for SA: ESP-3DES-MD5

226 10/10/2000 17:12:44.990 SEV=9 IKEDBG/0 RPT=38 161.44.17.135
User [37297304]
processing IPSEC SA

227 10/10/2000 17:12:44.990 SEV=8 IKEDBG/0 RPT=39
Proposal # 1, Transform # 1, Type ESP, Id DES-CBC
Parsing received transform:
Phase 2 failure:
Mismatched transform IDs for protocol ESP:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

232 10/10/2000 17:12:45.000 SEV=7 IKEDBG/27 RPT=1 161.44.17.135
User [37297304]

IPSec SA Proposal # 2, Transform # 1 acceptable

233 10/10/2000 17:12:45.000 SEV=7 IKEDBG/0 RPT=40 161.44.17.135

User [37297304]

IKE: requesting SPI!

234 10/10/2000 17:12:45.000 SEV=6 IKE/0 RPT=2

AM received unexpected event EV_ACTIVATE_NEW_SA in state AM_ACTIVE

235 10/10/2000 17:12:45.000 SEV=9 IPSECDBG/6 RPT=1

IPSEC key message parse - msgtype 6, len 164, vers 1, pid 00000000, seq 13, err 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 300, lifetime2 2000000000, dsId 2

239 10/10/2000 17:12:45.000 SEV=9 IPSECDBG/1 RPT=1

Processing KEY_GETSPI msg!

240 10/10/2000 17:12:45.000 SEV=7 IPSECDBG/13 RPT=1

Reserved SPI 1773955517

241 10/10/2000 17:12:45.000 SEV=8 IKEDBG/6 RPT=1

IKE got SPI from key engine: SPI = 0x69bc69bd

242 10/10/2000 17:12:45.000 SEV=9 IKEDBG/0 RPT=41 161.44.17.135

User [37297304]

oakley constructing quick mode

243 10/10/2000 17:12:45.000 SEV=9 IKEDBG/0 RPT=42 161.44.17.135

User [37297304]

constructing blank hash

244 10/10/2000 17:12:45.000 SEV=9 IKEDBG/0 RPT=43 161.44.17.135

User [37297304]

constructing ISA_SA for ipsec

245 10/10/2000 17:12:45.000 SEV=9 IKEDBG/1 RPT=17 161.44.17.135

User [37297304]

constructing ipsec nonce payload

246 10/10/2000 17:12:45.000 SEV=9 IKEDBG/1 RPT=18 161.44.17.135

User [37297304]

constructing proxy ID

247 10/10/2000 17:12:45.000 SEV=7 IKEDBG/0 RPT=44 161.44.17.135

User [37297304]

Transmitting Proxy Id:

Remote host: 192.168.1.1 Protocol 0 Port 0

Local host: 172.18.124.134 Protocol 0 Port 0

251 10/10/2000 17:12:45.000 SEV=9 IKEDBG/0 RPT=45 161.44.17.135

User [37297304]

constructing QM hash

252 10/10/2000 17:12:45.000 SEV=8 IKEDBG/0 RPT=46 161.44.17.135

SENDING Message (msgid=48687ca1) with payloads :

HDR + HASH (8) ... total length : 136

254 10/10/2000 17:12:45.010 SEV=8 IKEDECODE/0 RPT=36 161.44.17.135

ISAKMP HEADER : (Version 1.0)

Initiator Cookie(8): 9D F3 34 FE 89 BF AA B2

Responder Cookie(8): B7 AD 34 D2 74 4D 05 DA

Next Payload : HASH (8)

Exchange Type : Oakley Quick Mode

Flags : 1 (ENCRYPT)
Message ID : 48687ca1
Length : 52

261 10/10/2000 17:12:45.010 SEV=8 IKEDBG/0 RPT=47 161.44.17.135
RECEIVED Message (msgid=48687ca1) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

263 10/10/2000 17:12:45.010 SEV=9 IKEDBG/0 RPT=48 161.44.17.135
User [37297304]
processing hash

264 10/10/2000 17:12:45.010 SEV=9 IKEDBG/0 RPT=49 161.44.17.135
User [37297304]
loading all IPSEC SAs

265 10/10/2000 17:12:45.010 SEV=9 IKEDBG/1 RPT=19 161.44.17.135
User [37297304]
Generating Quick Mode Key!

266 10/10/2000 17:12:45.010 SEV=9 IKEDBG/1 RPT=20 161.44.17.135
User [37297304]
Generating Quick Mode Key!

267 10/10/2000 17:12:45.020 SEV=7 IKEDBG/0 RPT=50 161.44.17.135
User [37297304]
Loading host:
Dst: 172.18.124.134
Src: 192.168.1.1

268 10/10/2000 17:12:45.020 SEV=4 IKE/49 RPT=13 161.44.17.135
User [37297304]
Security negotiation complete for User (37297304)
Responder, Inbound SPI = 0x69bc69bd, Outbound SPI = 0x991518b4

271 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/6 RPT=2
IPSEC key message parse - msgtype 1, Len 536, vers 1, pid 00000000, seq 0,
err 0, type 2, mode 1, state 64, label 0, pad 0, spi 991518b4, encrKeyLen 24,
hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 0,
lifetime2 0, dsId 2

274 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=2
Processing KEY_ADD MSG!

275 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=3
key_msghdr2secassoc(): Enter

276 10/10/2000 17:12:45.020 SEV=7 IPSECDBG/1 RPT=4
No USER filter configured

277 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=5
KeyProcessAdd: Enter

278 10/10/2000 17:12:45.020 SEV=8 IPSECDBG/1 RPT=6
KeyProcessAdd: Adding outbound SA

279 10/10/2000 17:12:45.020 SEV=8 IPSECDBG/1 RPT=7
KeyProcessAdd: src 172.18.124.134 mask 0.0.0.0, dst 192.168.1.1 mask 0.0.0.0

280 10/10/2000 17:12:45.020 SEV=8 IPSECDBG/1 RPT=8
KeyProcessAdd: FilterIpsecAddIkeSa success

281 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/6 RPT=3
IPSEC key message parse - msgtype 3, Len 292, vers 1, pid 00000000, seq 0,

err 0, type 2, mode 1, state 32, label 0, pad 0, spi 69bc69bd, encrKeyLen 24,
hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 0,
lifetime2 0, dsId 2

284 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=9
Processing KEY_UPDATE MSG!

285 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=10
Update inbound SA addresses

286 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=11
key_msghdr2secassoc(): Enter

287 10/10/2000 17:12:45.020 SEV=7 IPSECDBG/1 RPT=12
No USER filter configured

288 10/10/2000 17:12:45.020 SEV=9 IPSECDBG/1 RPT=13
KeyProcessUpdate: Enter

289 10/10/2000 17:12:45.020 SEV=8 IPSECDBG/1 RPT=14
KeyProcessUpdate: success

290 10/10/2000 17:12:45.020 SEV=8 IKEDBG/7 RPT=1
IKE got a KEY_ADD MSG for SA: SPI = 0x991518b4

291 10/10/2000 17:12:45.020 SEV=8 IKEDBG/0 RPT=51
pitcher: rcv KEY_UPDATE, spi 0x69bc69bd

成功的使用 SDI 时的调试

SDI调试

如果成功(在SDI的第一验证)

```
10/06/2000 11:57:04/U 37297304/vpn3000 000037297304/37297304
372
10/06/2000 11:57:04/L Node Secret Sent to Client zekie.cisco.com
10/06/2000 15:57:05/U 37297304/vpn3000 000037297304/37297304
372
10/06/2000 11:57:05/U PASSCODE Accepted zekie.cisco.com
```

如果成功(在SDI的第一验证以后)

```
10/06/2000 16:06:09U 37297304/vpn3000 000037297304/37297304
372
10/06/2000 12:06:09L PASSCODE Accepted zekie.cisco.com
```

VPN 3000集中器调试(在测验)

调试“类名称”对于验证：

- AUTH
- AUTHDBG
- AUTHDECODE

4 10/06/2000 14:09:25.000 SEV=8 AUTHDBG/1 RPT=1
AUTH_Open() returns 14

5 10/06/2000 14:09:25.000 SEV=7 AUTH/12 RPT=1
Authentication session opened: handle = 14

6 10/06/2000 14:09:25.000 SEV=8 AUTHDBG/3 RPT=1

AUTH_PutAttrTable(14, 5a2aa0)

7 10/06/2000 14:09:25.000 SEV=8 AUTHDBG/5 RPT=1
AUTH_Authenticate(14, e5187e0, 306bdc)

8 10/06/2000 14:09:25.000 SEV=8 AUTHDBG/59 RPT=1
AUTH_BindServer(71e097c, 0, 0)

9 10/06/2000 14:09:25.000 SEV=9 AUTHDBG/69 RPT=1
Auth Server 649ab4 has been bound to ACB 71e097c, sessions = 1

10 10/06/2000 14:09:25.000 SEV=8 AUTHDBG/65 RPT=1
AUTH_CreateTimer(71e097c, 0, 0)

11 10/06/2000 14:09:25.000 SEV=9 AUTHDBG/72 RPT=1
Reply timer created: handle = 490011

12 10/06/2000 14:09:25.000 SEV=8 AUTHDBG/61 RPT=1
AUTH_BuildMsg(71e097c, 0, 0)

13 10/06/2000 14:09:25.000 SEV=8 AUTHDBG/51 RPT=1
Sdi_Build(71e097c)

14 10/06/2000 14:09:25.010 SEV=8 AUTHDBG/64 RPT=1
AUTH_StartTimer(71e097c, 0, 0)

15 10/06/2000 14:09:25.010 SEV=9 AUTHDBG/73 RPT=1
Reply timer started: handle = 490011, timestamp = 8553930, timeout = 4000

16 10/06/2000 14:09:25.010 SEV=8 AUTHDBG/62 RPT=1
AUTH_SndRequest(71e097c, 0, 0)

17 10/06/2000 14:09:25.010 SEV=8 AUTHDBG/52 RPT=1

Sdi_Xmt(71e097c)

18 10/06/2000 14:09:25.010 SEV=9 AUTHDBG/71 RPT=1
xmit_cnt = 1

19 10/06/2000 14:09:26.080 SEV=8 AUTHDBG/63 RPT=1
AUTH_RcvReply(71e097c, 0, 0)

20 10/06/2000 14:09:26.080 SEV=8 AUTHDBG/53 RPT=1
Sdi_Rcv(71e097c)

21 10/06/2000 14:09:26.080 SEV=8 AUTHDBG/66 RPT=1
AUTH_DeleteTimer(71e097c, 0, 0)

22 10/06/2000 14:09:26.080 SEV=9 AUTHDBG/74 RPT=1
Reply timer stopped: handle = 490011, timestamp = 8554037

23 10/06/2000 14:09:26.080 SEV=8 AUTHDBG/58 RPT=1
AUTH_Callback(71e097c, 0, 0)

24 10/06/2000 14:09:26.080 SEV=6 AUTH/4 RPT=1
Authentication successful: handle = 14, server = 172.18.124.99, user = 37297304

25 10/06/2000 14:09:26.080 SEV=8 AUTHDBG/2 RPT=1
AUTH_Close(14)

26 10/06/2000 14:09:26.080 SEV=8 AUTHDBG/60 RPT=1
AUTH_UnbindServer(71e097c, 0, 0)

27 10/06/2000 14:09:26.080 SEV=9 AUTHDBG/70 RPT=1

Auth Server 649ab4 has been unbound from ACB 71e097c, sessions = 0

28 10/06/2000 14:09:26.080 SEV=8 AUTHDBG/10 RPT=1
AUTH_Int_FreeAuthCB(71e097c)

29 10/06/2000 14:09:26.080 SEV=9 AUTHDBG/19 RPT=1
instance = 15, clone_instance = 0

30 10/06/2000 14:09:26.080 SEV=7 AUTH/13 RPT=1
Authentication session closed: handle = 14

错误调试

在客户端或用户没激活的用户名不正确

SDI调试

10/06/2000 16:30:21U junk/vpn3000
10/06/2000 12:30:21L User Not on Client zekie.cisco.com

VPN 3000 Debug

21 10/06/2000 14:20:06.310 SEV=3 AUTH/5 RPT=5
Authentication rejected: Reason = Unspecified
handle = 15, server = 172.18.124.99, user = junk

好用户名，坏密码

SDI调试

10/06/2000 16:33:07U 37297304/vpn3000 000037297304/37297304 372
10/06/2000 12:33:07L ACCESS DENIED, PASSCODE Incorrect zekie.cisco.com

VPN 3000 Debug

249 10/06/2000 14:22:52.160 SEV=3 AUTH/5 RPT=6
Authentication rejected: Reason = Unspecified
handle = 16, server = 172.18.124.99, user = 37297304

SDI下来服务器不可达的或守护程序

SDI调试

不显示(没有收到请求)

VPN 3000 Debug

77 10/06/2000 14:28:55.600 SEV=4 AUTH/9 RPT=7
Authentication failed: Reason = Network error
handle = 17, server = 172.18.124.99, user = 37297304

作为SDI方框的客户端没配置的VPN3000

SDI调试

10/06/2000 17:37:42U --/172.18.124.134 -->/
10/06/2000 13:36:42L Client Not Found zekie.cisco.com

VPN 3000 Debug

```
113 10/06/2000 15:26:27.440 SEV=3 AUTH/5 RPT=8
Authentication rejected: Reason = Unspecified
handle = 21, server = 172.18.124.99, user = 37297304
```

[已经删除VPN 3000集中器作为从SDI服务器的客户端，然后被重新加写它](#)

SDI服务器设法发送SECURID文件，以替换旧的SECURID文件，但VPN 3000已经具有此文件。

在SDI的消息

```
10/06/2000 13:42:18L Node Verification Failed zekie.cisco.com
VPN 3000 Debug
```

```
21 10/06/2000 15:32:03.030 SEV=3 AUTH/5 RPT=9
Authentication rejected: Reason = Unspecified
handle = 22, server = 172.18.124.99, user = 37297304
```

要解决此问题，删除VPN 3000集中器上的SECURID文件，操作方法是选择Administration>File management>Files> SECURID>Delete。在重新测试，VPN 3000集中器接受从SDI服务器的新的文件。如果SDI上的Edit Client > Sent Node Secret复选框变成灰色，那么SDI服务器不能完成交换。一旦VPN 3000集中器有SECURID文件，**Sent Node Secret复选框**被检查/没有变灰。

相关信息

- [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](#)
- [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](#)