

# IPSec SDI 認証での VPN 3000 コンセントレータへの Cisco VPN クライアントの設定

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[SDI を使用する VPN 3000 コンセントレータへの Cisco VPN クライアントの接続をテストする  
トラブルシューティング](#)

[VPN 3000 コンセントレータでのデバッグの有効化](#)

[ローカル認証を用いるIPSec の正常なデバッグ](#)

[ローカル認証を用いるIPSec の正常なデバッグ](#)

[SDI での正常なデバッグ](#)

[不正なデバッグ](#)

[関連情報](#)

## 概要

Cisco VPN 3000 コンセントレータは、Security Dynamics International ( SDI ) サーバを使用して、Cisco VPN クライアントを認証するよう設定できます。VPN 3000 コンセントレータは、SDI サーバのユーザ データグラム プロトコル ( UDP ) ポート 5500 を使用して通信し、SDI クライアントとして機能します。このドキュメントでは、SDI サーバ、VPN 3000 コンセントレータ、および Cisco VPN クライアントの適切な動作を確実にし、それぞれを組み合わせる方法について説明します。VPN 3000 コンセントレータがまだ設定されない場合、[インストール](#)からのステップを使用し、[SDI なしで初期インストールおよび設定のための Command Line Interface \( CLI \)](#)を使用して [VPN 3000 コンセントレータを設定して下さい](#)。[VPN 3000 コンセントレータをあらかじめ設定している場合は、「既存の設定の修正 \( SDI を使用しない \)」](#)の手順を実行します。

## 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

## 使用するコンポーネント

この設定の作成とテストは、次のソフトウェアとハードウェアのバージョンで行われています。

- SDI サーバ 3.3 ( UNIX および NT )
- VPN 3000 コンセントレータ ( 2.5.2 )
- VPN クライアント 2.5.2.A

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

## 表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

## 背景説明

この文書は、Cisco VPN 3000 Client ( 2.5.x ) または Cisco VPN クライアント ( 3.x ) の両方に適用されます。今までは 1 つの SDI サーバでグローバルに定義し、すべてのグループが使用していたのに対し、リリース 3.0 以降では、グループごとに SDI サーバを設定できます。個別 SDI サーバの設定を持たないグループは、グローバルに定義された SDI サーバを使用します。

SDI には、3 タイプの新しい個人識別番号 ( PIN ) があります。VPN 3000 コンセントレータは、下記のオプションの最初の 2 つをサポートしています。

- ユーザが新しい PIN の選択をする。
- サーバが新しい PIN の選択およびユーザへの通知をする。
- サーバは新しい PIN を選び、ユーザを知らせます; ユーザは PIN を変更できる。

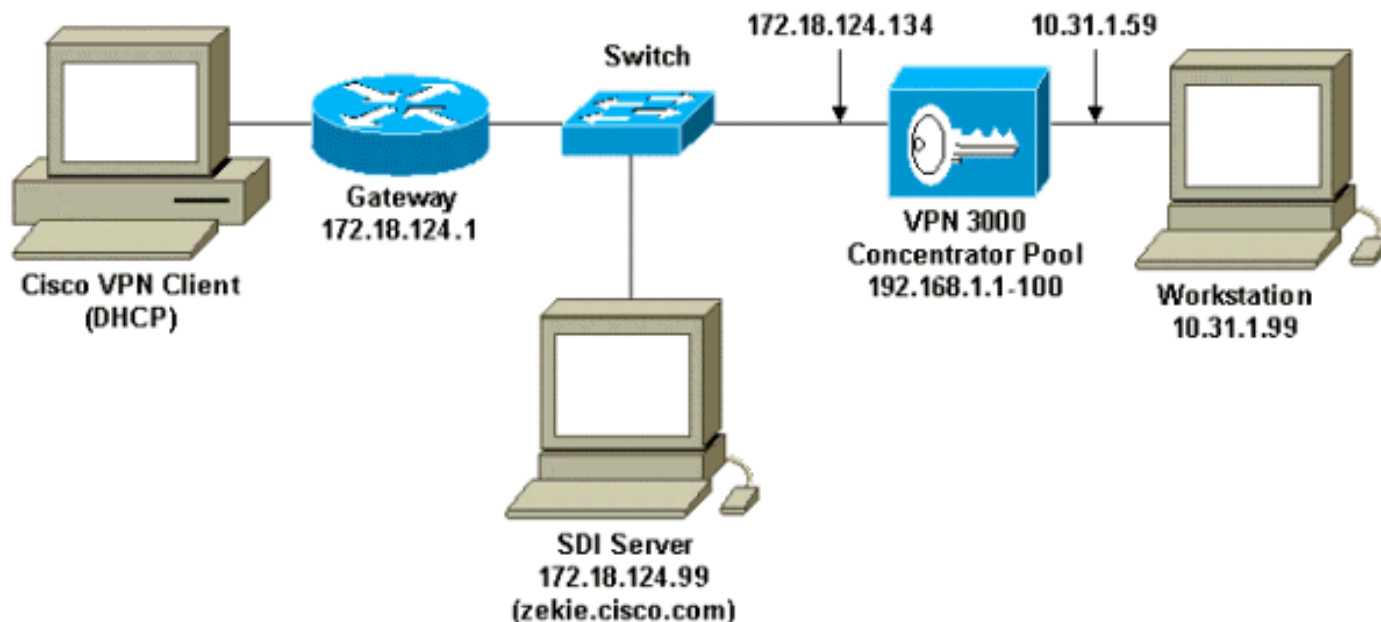
## 設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ( [登録ユーザ専用](#) ) を使用してください。

## ネットワーク図

このドキュメントでは次の図に示すネットワーク



## 設定

### SDI を使用しない VPN 3000 コンセントレータのインストールおよび設定

ローカルでグループのユーザを認証するために VPN 3000 コンセントレータを設定しました; 行うことにより SDI を追加する前に、Cisco VPN Client と VPN 3000 コンセントレータ間の IPsec がはたらいっていることを判別する可能性があります。[Administration]、[System Reboot]、[Schedule reboot]、[Reboot with Factory/Default Configuration] の順に選択して、コンソールポートでの VPN 3000 コンセントレータの設定をクリアにしました。

リブート後に、次の初期設定を行っています。

#### VPN 3000 コンセントレータの設定

```

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

```

既存の設定の修正 (SDI を使用しない)

VPN 3000 コンセントレータをあらかじめ設定している場合は、次の画面で、グループ、ユーザ、および IPsec/IKE 設定の確認を行います。

1. この画面で、ローカル認証を使用するグループを追加します。

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

Apply Cancel

2. この画面で、ローカル認証を使用するユーザをグループに追加します。

**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
<b>User Name</b>	37297304	Enter a unique user name.
<b>Password</b>	*****	Enter the user's password. The password must satisfy the group password requirements.
<b>Verify</b>	*****	Verify the user's password.
<b>Group</b>	vpn3000	Enter the group to which this user belongs.
<b>IP Address</b>		Enter the IP address assigned to this user.
<b>Subnet Mask</b>		Enter the subnet mask assigned to this user.

Apply    Cancel

3. IPsec > IKE プロポーザル画面で、IKE 設定を追加します (表示の設定はシステムのデフォルトです)。

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.

Active Proposals	Actions	Inactive Proposals
IKE-3DES-MD5 IKE-3DES-MD5-DH1 IKE-DES-MD5	<< Activate Deactivate >> Move Up Move Down Add Modify Copy Delete	IKE-3DES-MD5-RSA IKE-3DES-SHA-DSA IKE-3DES-MD5-RSA-DH1

### [SDI を使用しない Cisco VPN クライアントおよび VPN 3000 コンセントレータのテスト](#)

VPN 3000 コンセントレータの既存の設定の修正後に、Cisco VPN クライアントをインストールし、172.18.124.134 ( コンセントレータのパブリック インターフェイス ) を終端とする新しい接続を設定します。グループ アクセス情報は、"vpn3000" ( グループ名 ) で、グループ パスワードには、グループ用のパスワードを使用します。『Connect』をクリックしたときに、ユーザ名は"37297304" ( ユーザの名前 ) であり、ユーザパスワードはユーザ向けのパスワードでした ( VPN 3000 コンセントレータでローカルで保存される; SDI はまだ含みません )。IKE については[ローカル認証を用いた適切なIPSecデバッグ](#)を、IKEDBG、IKEDECODE、IPSEC、IPSECDBG、IPSECDECODE デバッグ参照して下さい。

### [VPN 3000 コンセントレータを使用しない SDI サーバ オペレーションのテスト](#)

#### UNIX ( Solaris )

- SDI サーバで、Solaris 管理者ツールを使用して、sditest アカウントを作成する。  
/etc/passwd エントリは、次のようになります。  
`sditest:x:76:10:::/local/0/sditest:/local/0/opt/ace/prog/sdshell` 注: ユーザのホーム ディレクトリ、"sdshell" の値およびパスは、システムによって異なります。
- トークンを sditest に割り当てる。
- sditest として UNIX ホストへの Telnet を試行する。ホストにより、UNIX パスワードおよび PASSCODE のプロンプトが表示される。認証後、sditest としてそのホストへ接続可能になります。



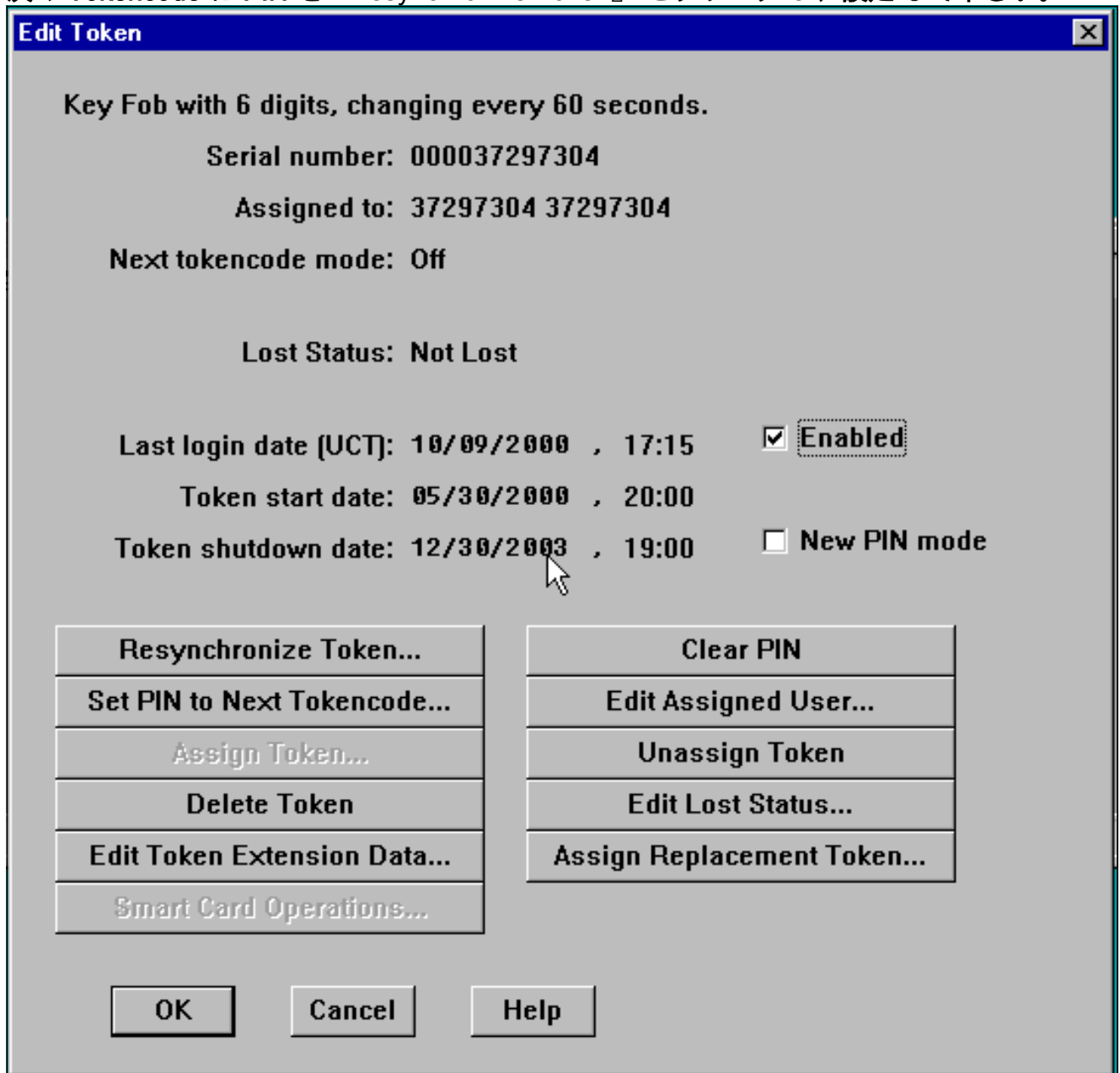
## Microsoft Windows NT

1. SecurSight Agent をインストールする。
2. [プログラム]、[SecurSight]、[Test Authentication] の順に選択する。

### VPN 3000 コンセントレータと通信するための SDI/User の設定

SDI/User を VPN 3000 コンセントレータに話すために設定するのに次のステップを使用して下さい:

1. SDI Server Edit Token 画面で、トークンが "Enabled" で、New PIN モードではないことを確認する。
2. 次の Tokencode に PIN を『Resynchronize Token』をクリックし、設定して下さい。



3. [Edit User] 画面で、ユーザにトークンを割り当て、[Allowed to create a PIN] チェックボックスがクリアになっていることを確認する。
4. アクティベーションを『Client』をクリックし、VPN 3000 コンセントレータが含まれていることを確認して下さい。



**Edit User** [X]

First and last name:

Default login:

Default shell:

Local User  Remote User

Serial Number	Type	Status
000037297304	Key Fob	Enabled

Tokens: [List Box]

O: Original token R: Replacement for previous token

Role: <none>

Assigned Profile: [List Box]

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: VPN 3000 コンセントレータは SDI サーバのクライアントとみなされます; 画面は下記の SDI サーバ Add/Edit Client 画面です。これは新しいクライアントであるため、[Sent Node Secret] ボックスは灰色表示になっています。SDI サーバには、コンセントレータに "node secret" ファイルを送信する機会はありません (このファイルは、[Administration]、[File Management]、[Files] の順に選択して開く [SECURID] のセクションのコンセントレータに表示されます。VPN 3000 からの認証が正常に終了すると、"node secret" ファイルが VPN 3000 コンセントレータに表示され、[Sent Node Secret] ボックスがチェックされます。

5. [User Activations] をクリックしてユーザが含まれていることを確認する。

## [SDI についての VPN 3000 コンセントレータのテスト](#)

SDI に VPN 3000 コンセントレータを設定し、テストするのに次のステップを使用して下さい。

1. 次の画面を使用して、SDI の認証を行うよう VPN 3000 コンセントレータを設定する。

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).

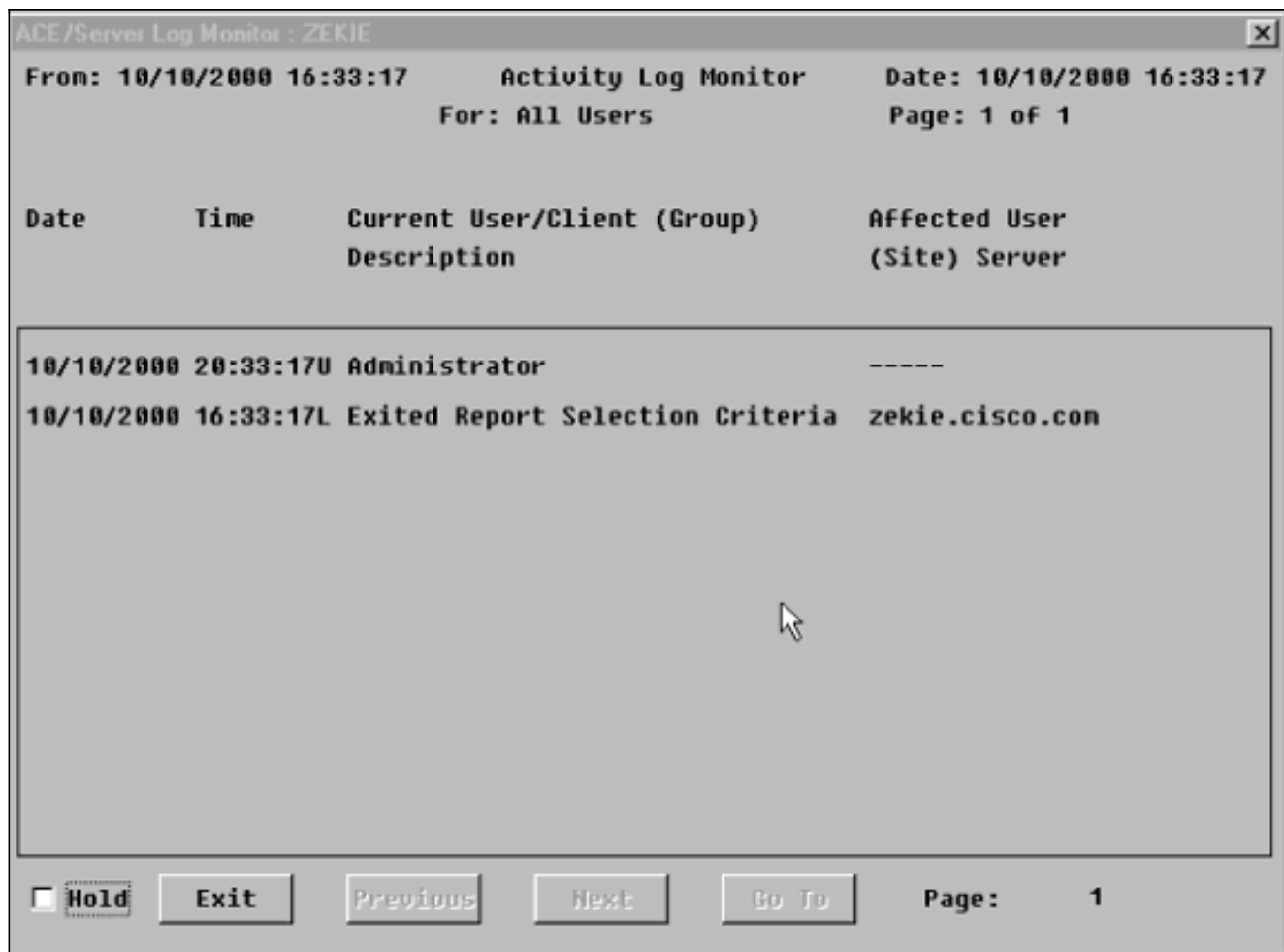
**Retries**

Enter the number of retries for this server.

Apply

Cancel

2. SDI から、[Report]、[Log Monitor]、[Activity Monitor] の順に選択して、[OK] をクリックして入ってくる要求を監視する。



3. VPN 3000 コンセントレータで、[Test] をクリックして接続をテストする。

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. 認証が正常な場合は、VPN 3000 コンセントレータに次が表示される。Authentication successful

上記の例では、1つのグローバルサーバが定義されています。また、[Configuration]、[User Management]、[Groups]の順に選択して、それぞれのグループを強調表示し、[Modify Auth Server]を選択すると、各グループにSDIサーバをそれぞれ定義するよう選択することもできます。

デバッグ情報については、次のセクションを参照してください。

- [VPN 3000 コンセントレータでのデバッグの有効化](#)
- [SDIでの正常なデバッグ](#)
- [不正なデバッグ](#)

## 確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

[SDIを使用するVPN 3000 コンセントレータへのCisco VPNクライアントの接続](#)

## [をテストする](#)

この時点ですべてが正しく動作している場合は、Cisco VPN コンセントレータ、VPN 3000 コンセントレータ、および SDI サーバを結合します。VPN 3000 コンセントレータで必要な唯一の変更は、SDI サーバに要求を送信するよう "vpn3000" と呼ばれる作業グループを修正することです。

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 checked="" type="checkbox"/>	Enter the banner for this group.

## [トラブルシューティング](#)

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

### [VPN 3000 コンセントレータでのデバッグの有効化](#)

認証のクラスネーム:

- AUTH
- AUTHDBG
- AUTHDECODE

認証のための Class Name : AUTHAUTHDBGAUTHDECODE

- IKE、IKEDBG、IKEDECODE
- IPSEC、IPSECDBG、IPSECDECODE
- Severity to Log = 1-9
- コンソールに対する重大度 = 1 ~ 3

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

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

Add

Cancel

デバッグ オペレーションの結果を表示するために『Get Log』 をクリックして下さい。

## Monitoring | Event Log

### Select Filter Options

Event Class

  
 AUTH  
 AUTHDBG  
 AUTHDECODE

Severities

  
 1  
 2  
 3

Client IP  
Address

Events/Page

Direction

### [ローカル認証を用いるIPSecの正常なデバッグ](#)

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: FilterIpssecAddIkeSa 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

## [ローカル認証を用いるIPSecの正常なデバッグ](#)

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: FilterIpssecAddIkeSa 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

## SDI での正常なデバッグ

### SDI デバッグ

#### 正常に終了した場合 ( SDI での最初の認証 )

```
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
```

#### 正常に終了した場合 ( SDI での最初の認証後 )

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

### VPN 3000 コンセントレータ デバッグ (テスト)

"認証のための ""Class Name"" のデバッグ : "

- 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

## 不正なデバッグ

### ユーザ名無効またはクライアントで有効になっていないユーザ

#### SDI デバッグ

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

#### VPN 3000 デバッグ

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

### ユーザ名有効、パスコード無効

#### SDI デバッグ

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 デバッグ

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 サーバに到達不能またはデーモン ダウン

#### SDI デバッグ

何も表示しない ( 要求を受信しない )

#### VPN 3000 デバッグ

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

### SDI ボックスでVPN 3000がクライアントとして設定されていない

#### SDI デバッグ

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

## VPN 3000 デバッグ

```
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
```

### [SDI サーバからクライアントとしての VPN 3000 コンセントレータを削除、再び追加](#)

SDI サーバは SECURID ファイルを送信して、古いファイルとの置換を試行しますが、VPN 3000 にはすでにこのファイルがあります。

### SDI でのメッセージ

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

```
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
```

この問題を解決するには、[Administration]、[File management]、[Files]、[SECURID]、[Delete] の順に選択して、VPN 3000 コンセントレータの SECURID ファイルを削除します。再テストで、VPN 3000 コンセントレータは、SDI サーバから新しいファイルを受け入れます。SDI で [Edit Client] の [Sent Node Secret] チェックボックスが灰色表示されている場合は、SDI サーバの交換は完了していません。VPN 3000 コンセントレータに SECURID ファイルがあると、[Sent Node Secret] チェックボックスが灰色表示にならずにチェックされます。

## [関連情報](#)

- [IPSec SDI 認証 5.0 およびそれ以降を使用する VPN 3000 コンセントレータへの Cisco VPN クライアントの設定](#)
- [Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ](#)
- [Cisco VPN 3000 シリーズ クライアントに関するサポート ページ](#)
- [IPSec に関するサポート ページ](#)
- [テクニカルサポート - Cisco Systems](#)