# Cisco VPN Client to VPN 3000 Concentrator with IPSec SDI Authentication(서버 버전 3.3)

## 목차



# 소개

Cisco VPN 3000 Concentrator는 SDI(Security Dynamics International) 서버를 통해 Cisco VPN 클라이언트를 인증하도록 구성할 수 있습니다. VPN 3000 Concentrator는 SDI 클라이언트 역할을 하며 UDP(User Datagram Protocol) 포트 5500에서 SDI 서버와 통신합니다. 다음 문서는 SDI 서버, VPN 3000 Concentrator 및 Cisco VPN Client가 제대로 작동하는지 확인한 다음 구성 요소를 결합하는 방법을 보여줍니다. VPN 3000 Concentrator가 아직 구성되지 않은 경우 초기 설치 및 컨피그레이션을 위해 CLI(Command Line Interface)를 사용하여 SDI 없이 VPN 3000 Concentrator 설치 및 구성의 단계를 사용합니다. VPN 3000 Concentrator가 이전에 구성된 경우 Modify Existing Configuration (Without SDI)(기존 컨피그레이션 수정(SDI 없음) 단계를 수행합니다.

# 사전 요구 사항

## 요구 사항

이 문서에 대한 특정 요건이 없습니다.

## 사용되는 구성 요소

이 구성은 아래의 소프트웨어 및 하드웨어 버전을 사용하여 개발 및 테스트되었습니다.

- SDI 서버 3.3(UNIX 및 NT)
- VPN 3000 Concentrator(2.5.2)
- VPN 클라이언트 2.5.2.A

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 라이브 네트워크에서 작업하는 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

## 표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

# 배경 정보

이 문서는 Cisco VPN 3000 클라이언트(2.5.x) 또는 Cisco VPN 클라이언트(3.x)에 모두 적용됩니다. 이제 3.0 이상의 릴리스를 통해 개별 그룹에 대해 개별 SDI 서버를 구성할 수 있습니다. 이는 전체적으로 정의되고 모든 그룹에서 사용되는 하나의 SDI 서버와 다릅니다. 개별 SDI 서버가 구성되지 않은 그룹은 전체적으로 정의된 SDI 서버를 사용합니다.

SDI에는 3가지 유형의 새 PIN(개인 식별 번호) 모드가 있습니다. VPN 3000 Concentrator는 아래에 표시된 것처럼 처음 두 옵션을 지원합니다.

- 사용자가 새 PIN을 선택합니다.
- 서버가 새 PIN을 선택하고 사용자에게 알립니다.
- 서버가 새 PIN을 선택하고 사용자에게 알립니다. 사용자는 PIN을 변경할 수 있습니다.

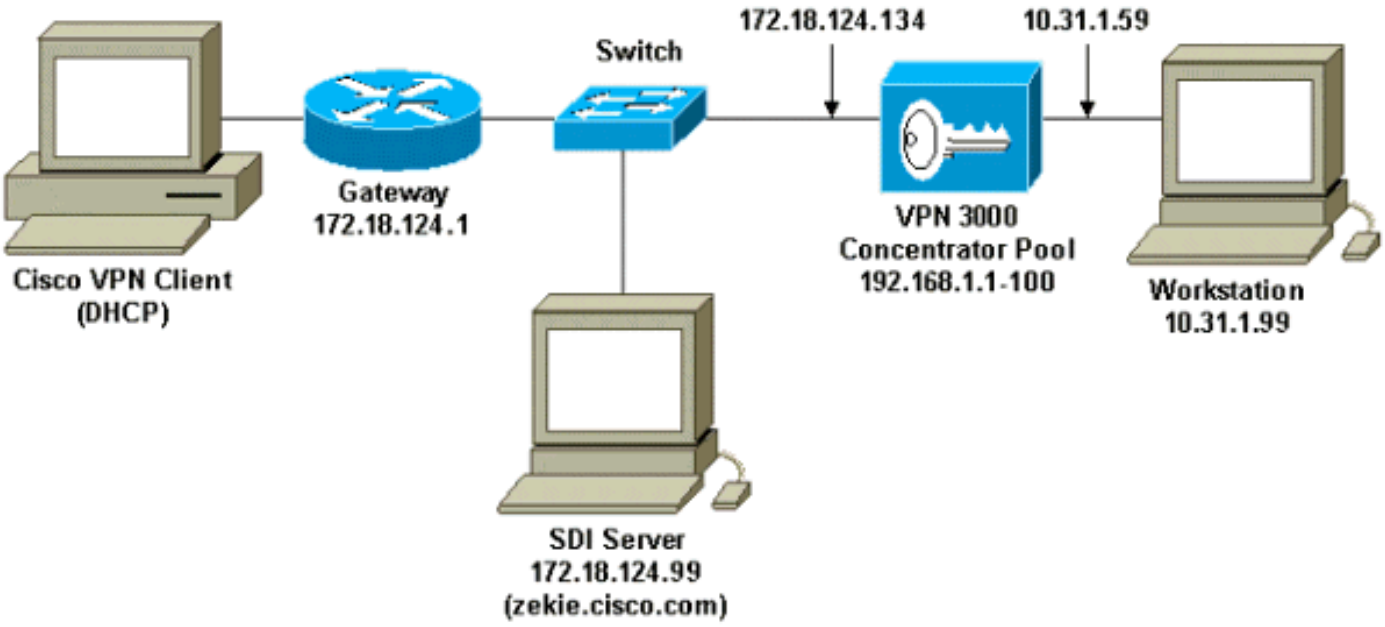
# 구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

**참고:** 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 명령 조회 도구(등록된 고객만 해당)를 사용합니다.

## 네트워크 다이어그램

이 문서에서는 아래 다이어그램에 표시된 네트워크 설정을 사용합니다.




## 구성

### SDI 없이 VPN 3000 Concentrator 설치 및 구성

그룹의 사용자를 로컬로 인증하도록 VPN 3000 Concentrator를 구성했습니다. SDI를 추가하기 전에 이 작업을 수행하면 Cisco VPN Client와 VPN 3000 Concentrator 간의 IPSec이 작동하는지 확인할 수 있습니다. Administration(관리) > System Reboot(시스템 재부팅) > Schedule reboot(재부팅 예약) **> Reboot with Factory/Default Configuration(공장/기본 컨피그레이션으로 재부팅)으로** 이동하여 콘솔 포트에서 VPN 300 **Concentrator 컨피그레이션을 지웠습니다**.

재부팅 후 다음 초기 컨피그레이션이 완료되었습니다.

**VPN 3000 Concentrator Concentrator 구성**

```
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
```

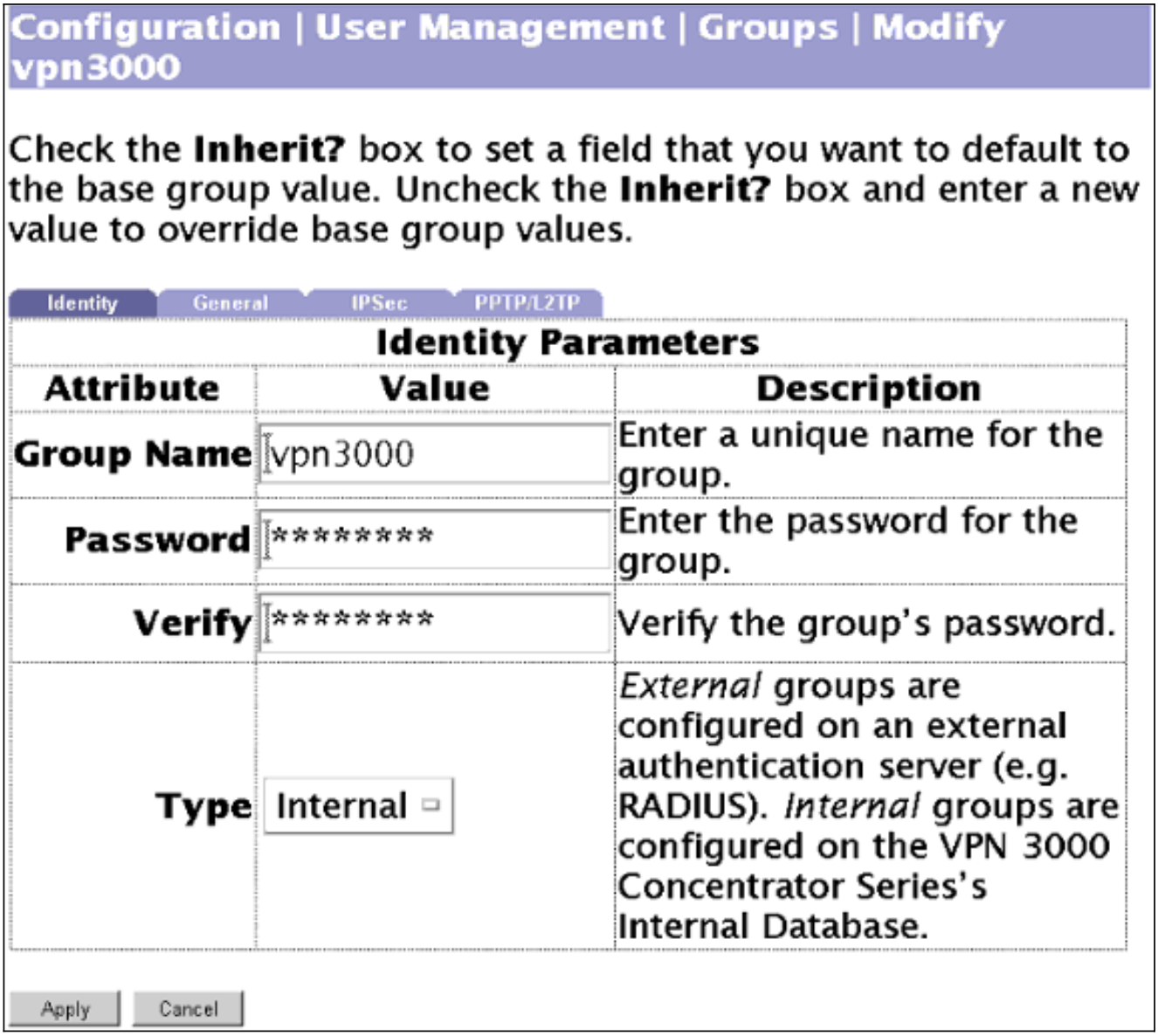
```
2) Disable Client Specified Address Assignment

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
```

## 기존 구성 수정(SDI 없음)

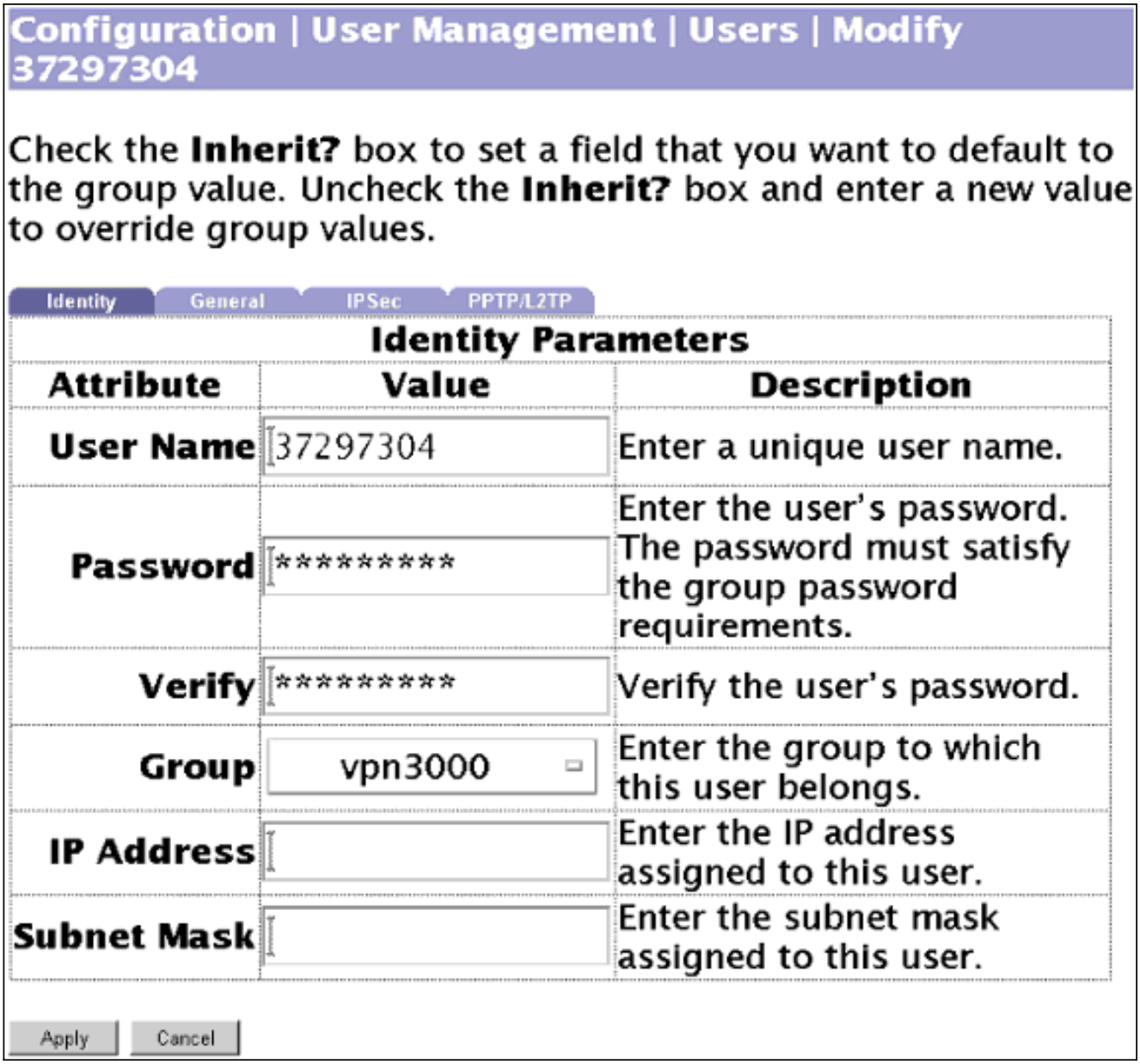
VPN 3000 Concentrator가 이전에 구성된 경우 다음 화면을 사용하여 그룹, 사용자 및 IPSec/IKE 설정을 확인합니다.

1. 로컬 인증이 있는 그룹을 추가하려면 이 화면을 사용합니다
   .

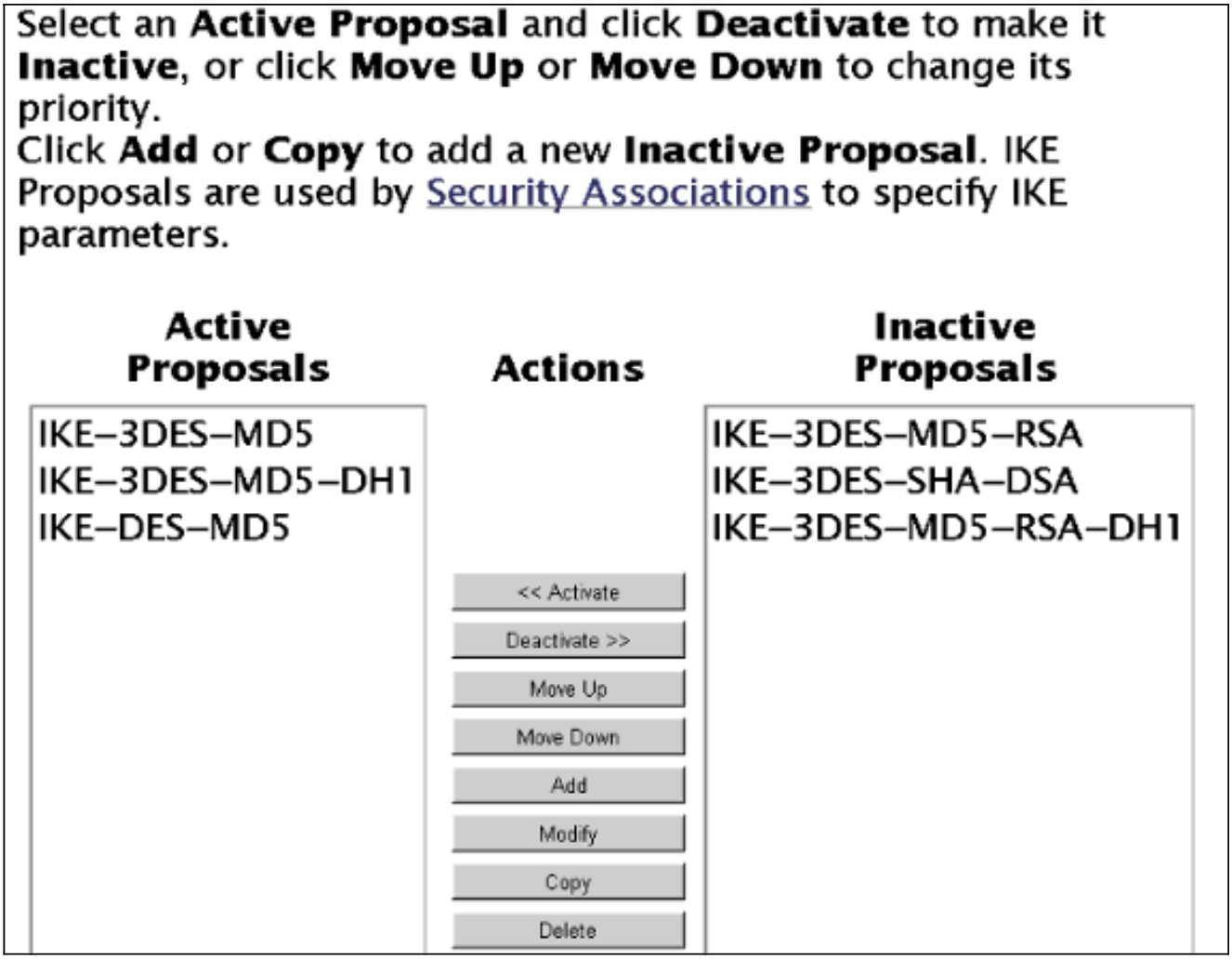



2. 로컬 인증을 사용하여 그룹에 사용자를 추가하려면 이 화면을 사용합니다

.




3. IPSec > IKE 제안서 화면을 사용하여 IKE 설정을 추가합니다(표시된 설정은 시스템 기본값 ).




## SDI 없이 Cisco VPN 클라이언트 및 VPN 3000 Concentrator 테스트

VPN 3000 Concentrator의 기존 컨피그레이션을 수정한 후 Cisco VPN Client를 설치하고 172.18.124.134(concentrator의 공용 인터페이스)에서 종료하도록 새 연결을 구성했습니다. 그룹 액세스 정보는 "vpn3000"(그룹 이름)이고 그룹 암호는 그룹의 암호입니다. **Connect**를 클릭했을 때 사용자 이름은 "37297304"(사용자 이름)이고 사용자 암호는 VPN 3000 Concentrator에 로컬로 저장된 사용자의 암호입니다. 아직 SDI가 관련되어 있지 않음). IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE 디버그에 대한 로컬 인증과 함께 올바른 IPSec 디버그를 참조하십시오.

## VPN 3000 Concentrator 없이 SDI 서버 작업 테스트

### UNIX(Solaris)

1. SDI 서버에서 Solaris 관리 도구를 사용하여 sdittest 계정을 만듭니다./etc/passwd 항목은 다음과 같아야 합니다.
   ```
   sditest:x:76:10::/local/0/sditest:/local/0/opt/ace/prog/sdshell
   ```
   **참고:** 사용자 홈 디렉토리 및 "sdshell"에 대한 값과 경로는 시스템에 따라 다릅니다.
2. sditest에 토큰을 할당합니다.
3. UNIX 호스트로 텔네팅을 sditest로 시도합니다. 호스트는 UNIX 비밀번호 및 PASSCODE를 입력하라는 메시지를 표시합니다. 인증 후 해당 호스트에서 sditt로 로그인할 수 있습니다.

### Microsoft Windows NT

1. SecurSight Agent를 설치합니다.

2. Programs > **SecurSight > Test Authentication을 선택합니다**.

## VPN 3000 Concentrator와 통신하도록 SDI/사용자 구성

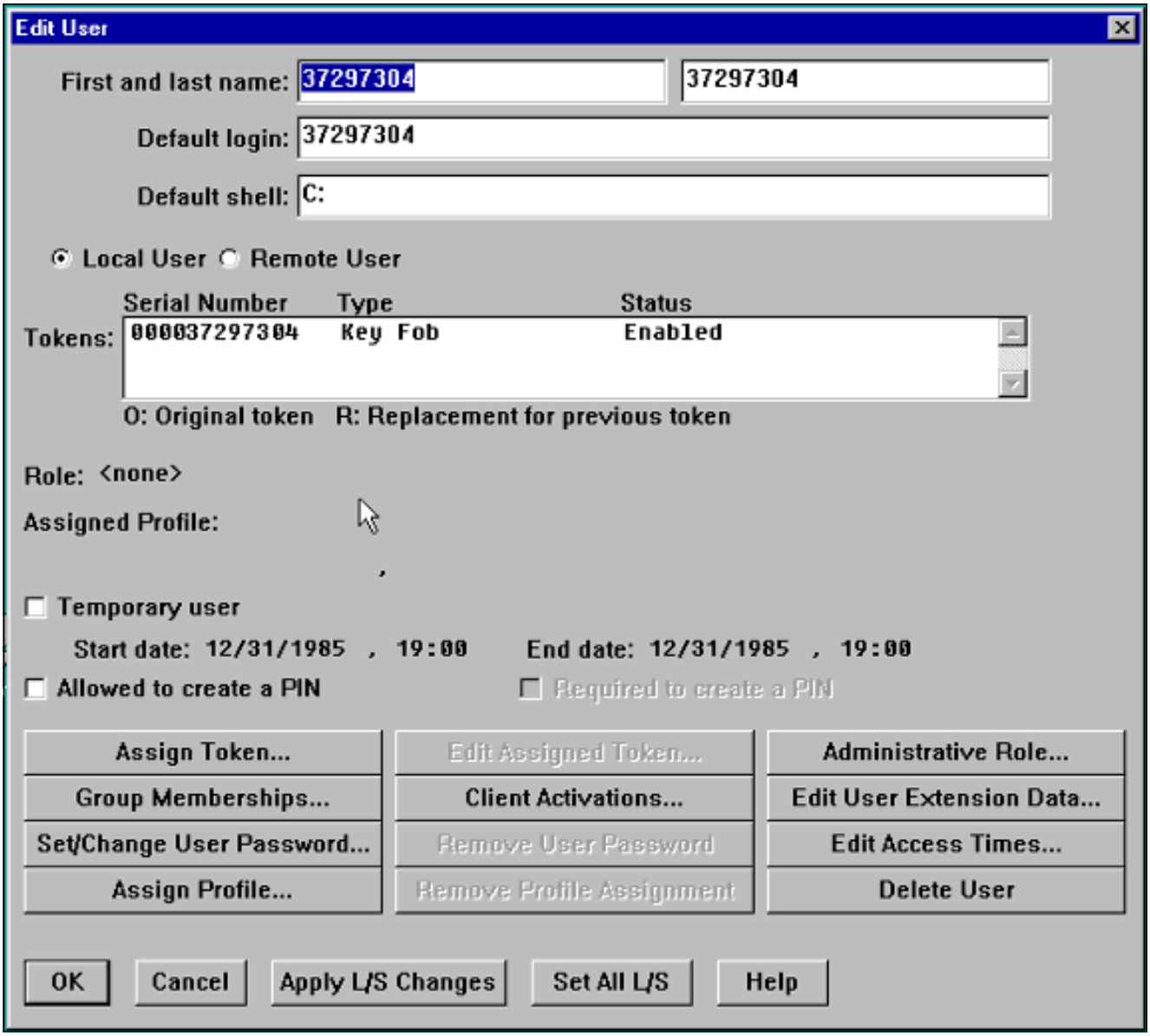
VPN 3000 Concentrator와 통신하도록 SDI/사용자를 구성하려면 다음 단계를 사용합니다.

1. SDI Server Edit Token(SDI 서버 토큰 편집) 화면에서 토큰이 새 PIN 모드가 아닌 "Enabled(활성화됨)"인지 확인합니다.
2. Resynchronize **Token(토큰 재동기화)**을 클릭하고 **Set PIN to Next Token Code(PIN을 다음 토큰코드로 설정)를 클릭합니다**

.


3. Edit User(사용자 수정) 화면에서 사용자에게 토큰을 할당하고 "Allowed to create a PIN(PIN 생성 허용)"이 선택되지 않았는지 확인합니다.
4. Client Activations(클라이언트 활성화)를 클릭하고 VPN 3000 Concentrator가 포함되어 있는지 확인합니다

.



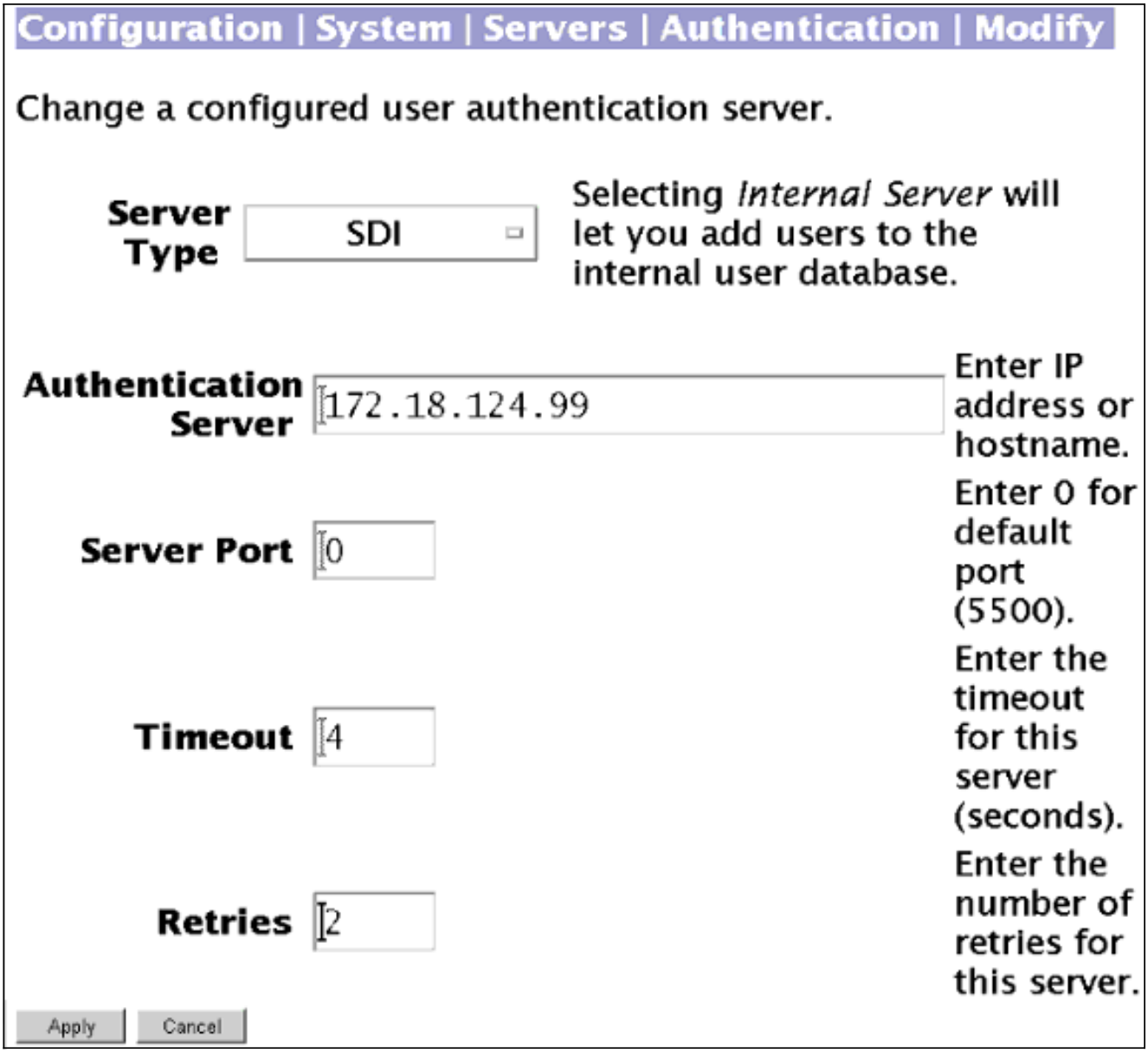

**참고:** VPN 3000 Concentrator는 SDI 서버의 클라이언트로 간주됩니다. 아래 화면은 SDI 서버 클라이언트 추가/편집 화면입니다. 이 클라이언트는 새 클라이언트이므로 "Sent Node Secret" 상자가 회색으로 표시됩니다. SDI 서버에서는 Concentrator에 "노드 암호" 파일을 보낼 수 없습니다. 이 파일은 Administration(관리) > File **Management(파일 관리) > Files(파일)** 섹션의 Concentrator에 "SECURID"로 표시됩니다. VPN 3000에서 성공적으로 인증하면 "노드 비밀" 파일이 VPN 3000 Concentrator에 표시되고 "Sent Node Secret" 상자가 선택됩니다.

5. User **Activations(사용자 활성화)**를 클릭하고 사용자가 포함되어 있는지 확인합니다.

## SDI에 VPN 3000 Concentrator 구성 및 테스트

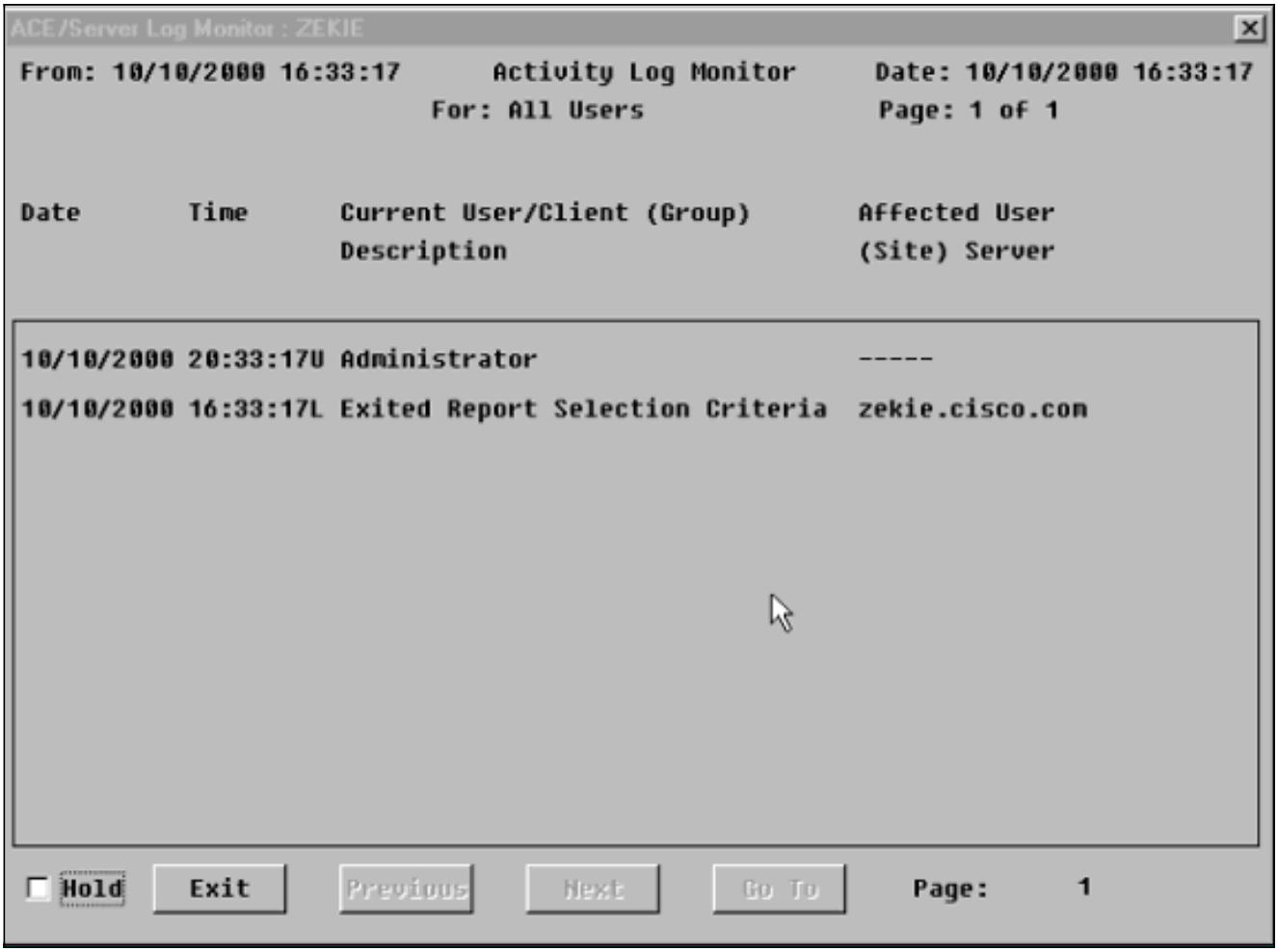
다음 단계를 사용하여 SDI에 VPN 3000 Concentrator를 구성하고 테스트합니다.

1. 다음 화면을 사용하여 SDI에 인증하도록 VPN 3000 Concentrator를 구성합니다
.

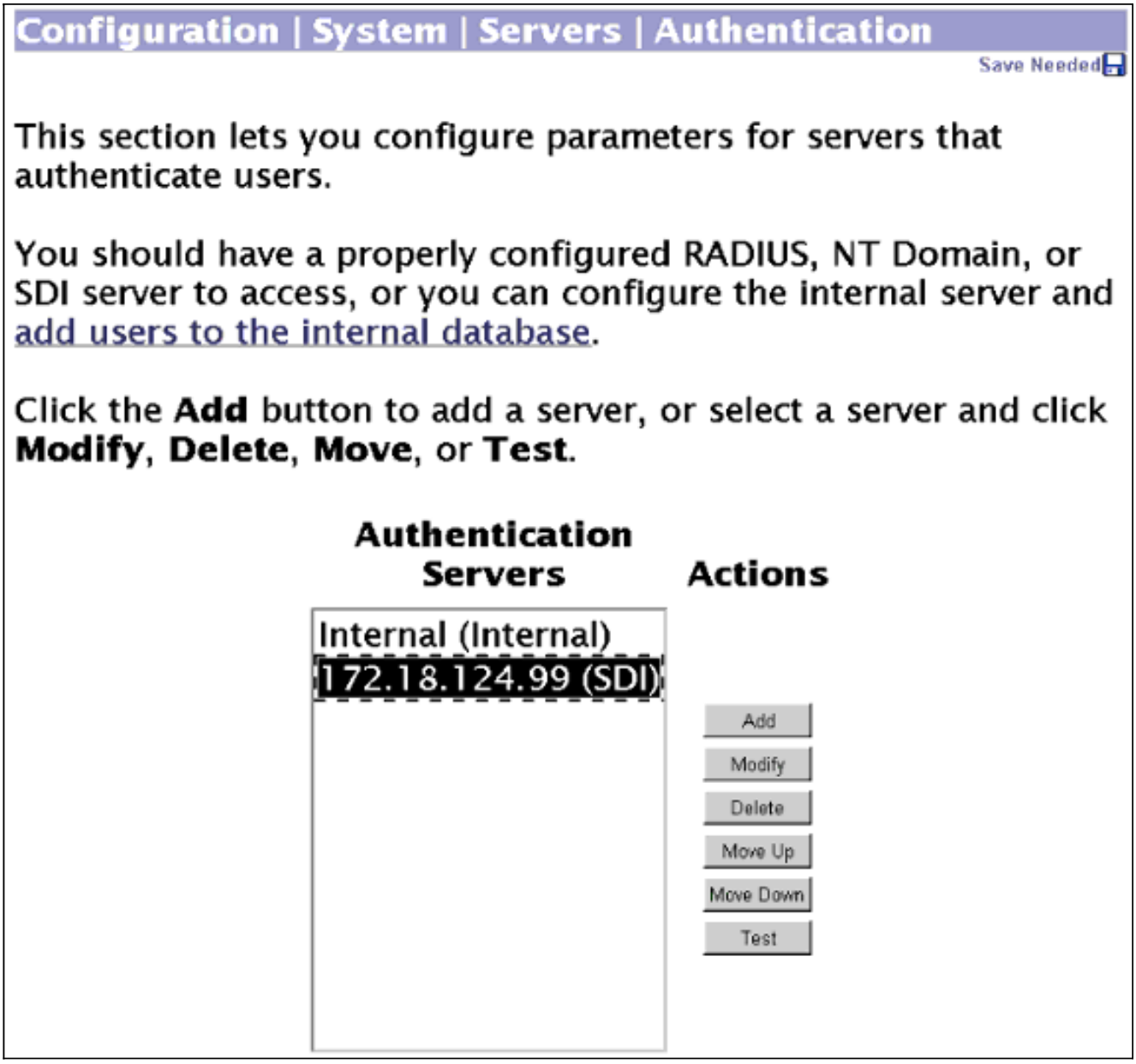



2. SDI에서 Report(보고서) > Log Monitor(로그 모니터) > Activity Monitor(작업 모니터)로 이동하고 OK(확인)를 클릭하여 수신 요청을 확인합니다

.




3. VPN 3000 Concentrator에서 **Test(테스트)**를 클릭하여 연결을 테스트합니다
.




4. 인증이 정상이면 VPN 3000 Concentrator에 다음이 표시됩니다.**인증 성공**

위의 예에서는 하나의 전역 SDI 서버를 정의했습니다. 또한 Configuration(컨피그레이션) > User Management(사용자 **관리) > Groups(그룹)**로 이동하여 각 그룹을 강조 표시하고 Modify Auth Server(인증 서버 수정)를 선택하여 각 그룹에 대해 개별 SDI 서버를 정의하도록 선택할 수 **있습니다**.

디버그 정보는 이 문서의 다음 섹션을 참조하십시오.

- VPN 3000 Concentrator에서 디버깅 켜기
- SDI를 사용한 올바른 디버그
- 잘못된 디버그

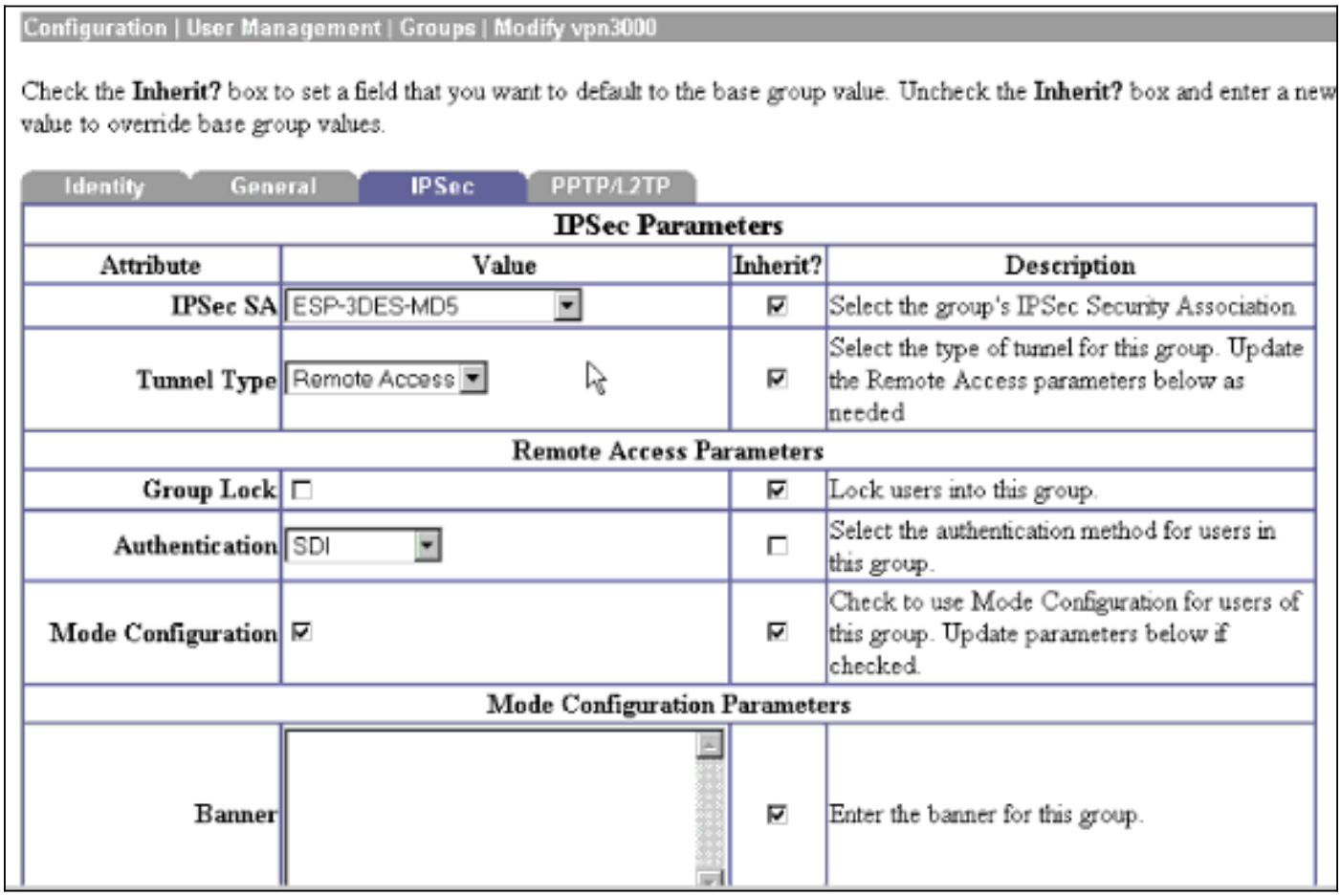
## 다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

### SDI를 사용하여 Cisco VPN Client to VPN 3000 Concentrator 테스트

모든 것이 이 시점까지 작동하는 경우 Cisco VPN Client, VPN 3000 Concentrator 및 SDI 서버를 결

합해야 합니다. "vpn3000"이라는 작업 그룹을 수정하여 SDI 서버에 요청을 전송하려면 VPN 3000 Concentrator에서 한 번 변경해야 합니다.


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 | ☑ | Select the group's IPSec Security Association |
| Tunnel Type | Remote Access | ☑ | Select the type of tunnel for this group. Update the Remote Access parameters below as needed |
| **Remote Access Parameters** | | | |
| Group Lock | ☐ | ☑ | Lock users into this group. |
| Authentication | SDI | ☐ | Select the authentication method for users in this group. |
| Mode Configuration | ☑ | ☑ | Check to use Mode Configuration for users of this group. Update parameters below if checked. |
| **Mode Configuration Parameters** | | | |
| Banner | | ☑ | Enter the banner for this group. |

# 문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

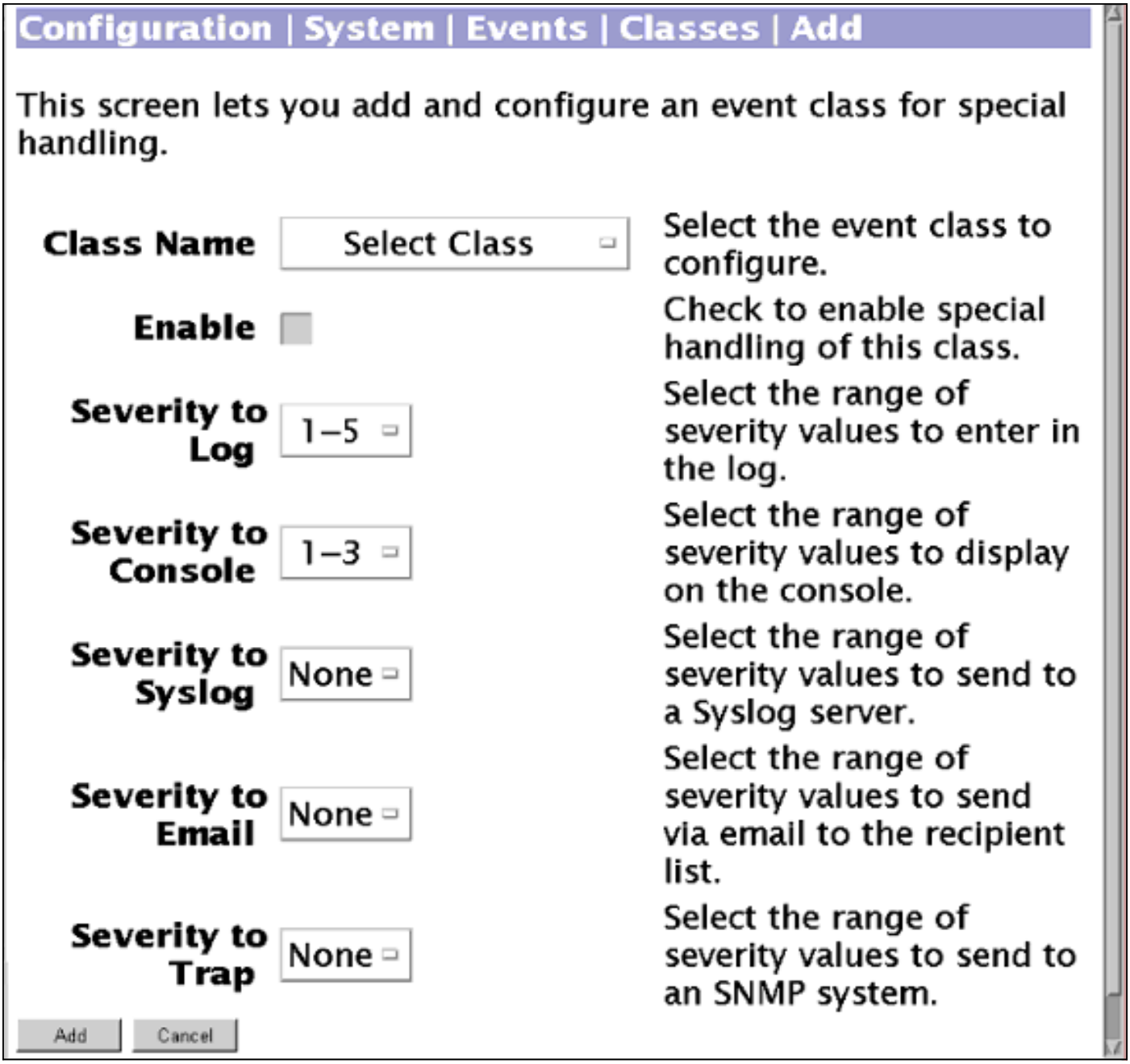
## VPN 3000 Concentrator에서 디버깅 켜기

**인증을 위한 클래스 이름:**

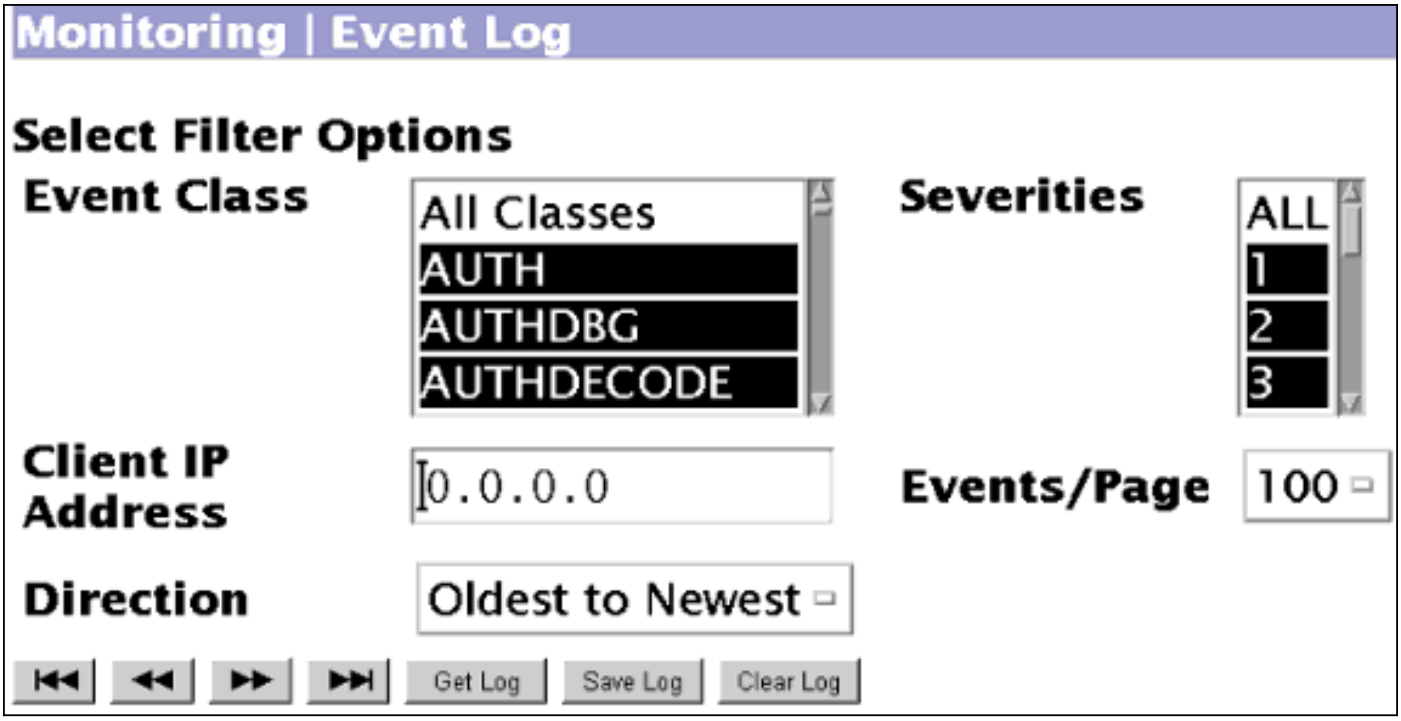
- 인증
- AUTHDBG
- AUTHDECODE

**IPSec의 클래스 이름:**

- IKE, IKEDBG, IKEDECODE
- IPSEC, IPSECDBG, IPSECDECODE
- 기록할 심각도 = 1-9
- 콘솔에 대한 심각도 = 1-3




Get **Log(로그** 가져오기)를 클릭하여 디버그 작업의 결과를 봅니다.




## 로컬 인증을 사용하는 올바른 IPSec 디버그

```
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
```

## 로컬 인증을 사용하는 올바른 IPSec 디버그

```
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
```

## SDI를 사용한 올바른 디버그

### SDI 디버그

*성공한 경우(SDI의 첫 번째 인증)*

```
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
```

*성공한 경우(SDI의 첫 번째 인증 이후)*

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

### VPN 3000 Concentrator 디버그(테스트)

인증을 위한 "클래스 이름" 디버그:

- 인증
- 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
```

## 잘못된 디버그

### 잘못된 사용자 이름 또는 사용자가 클라이언트에서 활성화되지 않았습니다.

*SDI 디버그*

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

*VPN 3000 디버그*

```
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
```

### 사용자 이름, 잘못된 암호

*SDI 디버그*

```
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 디버그*

```
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 서버에 연결할 수 없거나 데몬 다운

*SDI 디버그*

아무것도 표시 안 함(요청을 받지 않음)

*VPN 3000 디버그*

```
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
```

### VPN 3000이 SDI 상자에 클라이언트로 구성되지 않음

*SDI 디버그*

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

*VPN 3000 디버그*

```
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 서버에서 클라이언트로 VPN 3000 Concentrator를 제거한 후 다시 추가했습니다.

SDI 서버가 이전 파일을 대체하기 위해 SECURID 파일을 전송하려고 했지만 VPN 3000에 이 파일이 이미 있습니다.

*SDI에 대한 메시지*

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

*VPN 3000 디버그*

```
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
```

이 문제를 해결하려면 VPN 3000 Concentrator에서 Administration(관리) > File **management(파일 관리) > Files(파일) > SECURID > Delete(삭제)**로 이동하여 SECURID 파일을 삭제합니다. 재테스트 시 VPN 3000 Concentrator는 SDI 서버의 새 파일을 수락합니다. SDI**에서 Edit Client > Sent Node Secret** 확인란이 회색으로 표시되면 SDI 서버가 Exchange를 완료할 수 없습니다. VPN 3000 Concentrator에 SECURID 파일이 있으면 **Sent Node Secret** 확인란이 선택/회색으로 표시되지 않습니다.

## 관련 정보

- IPSec SDI Authentication 5.0 이상을 사용하여 VPN 3000 Concentrator에 Cisco VPN 클라이언트 구성
- Cisco VPN 3000 Series Concentrator 지원 페이지
- Cisco VPN 3000 Series 클라이언트 지원 페이지
- IPSec 지원 페이지
- Technical Support - Cisco Systems