VPN 클라이언트(고정/동적 할당 IP 주소)를 VPN 3000 Concentrator 구성에 대한 IPSec 구성 예

목차

소개
사전 요구 사항
요구 사항
사용되는 구성 요소
네트워크 다이어그램
표기 규칙
VPN 3000 Concentrator 구성
사용자에게 고정 IP 주소 할당
VPN 클라이언트 구성
다음을 확인합니다.
문제 해결
문제가 될 수 있는 부분
VPN 클라이언트
VPN 집선 장치
VPN 3000 Concentrator - 샘플 디버그
관련 정보

소개

이 샘플 컨피그레이션에서는 Cisco VPN Client(4.x 이상)(Static/Dynamic 할당 IP 주소)를 실행하는 PC에서 Cisco VPN 3000 Concentrator로 IPsec 터널을 형성하여 사용자가 VPN Concentrator 내에서 네트워크에 안전하게 액세스할 수 있도록 하는 방법을 보여 줍니다.

Cisco ACS를 사용한 RADIUS 인증과 동일한 시나리오에 대한 자세한 내용은 Using Cisco Secure ACS for Windows with the VPN 3000 Concentrator - IPSec을 참조하십시오. MS-RADIUS 인증과 동일한 시나리오에 대한 자세한 내용은 Cisco VPN 3000 Concentrator with MS RADIUS를 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

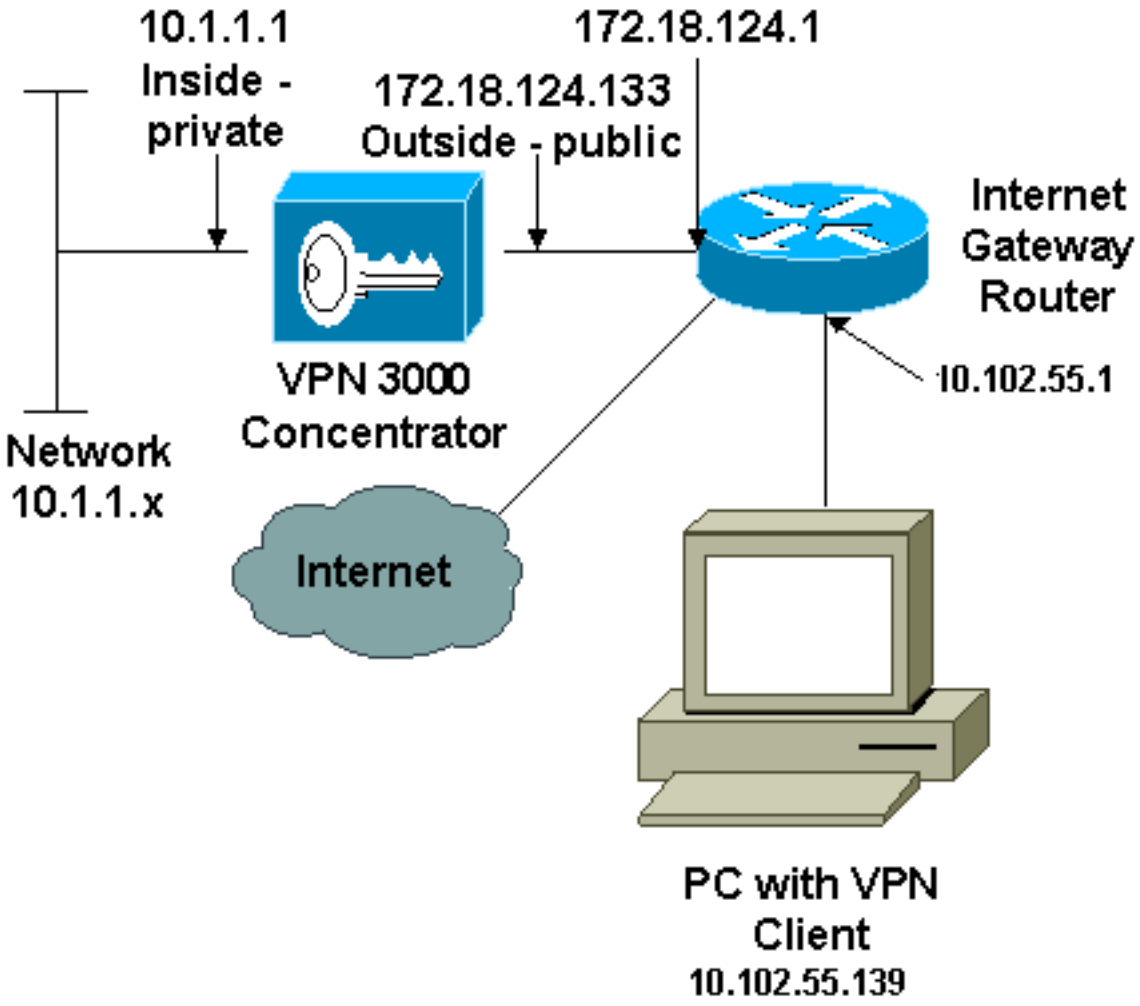
- Cisco VPN 3030 Concentrator 버전 4.1.7.A
- Cisco VPN Client 버전 4.x 이상

참고: 이 컨피그레이션은 최근 Cisco VPN Concentrator 버전 4.7.2.H를 사용하여 다시 테스트되었습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다. 실습 환경에서 사용된 RFC 1918 주소입니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

VPN 3000 Concentrator 구성

VPN 3000 Concentrator를 구성하려면 다음 단계를 완료하십시오.

참고: 공간 제한으로 인해 일부 화면 캡처는 부분 화면만 표시합니다.

1. VPN Concentrator 콘솔 포트에 연결하고 프라이빗(내부) 및 퍼블릭(외부) 인터페이스에 할당된 IP 주소가 있는지 확인합니다.또한 VPN Concentrator가 모르는 대상에 대한 패킷을 기본 게이트웨이(일반적으로 인터넷 게이트웨이 라우터)로 전달할 수 있도록 기본 게이트웨이가 할당되었는지 확인합니다

.

```
97 01/21/2005 12:18:50.300 SEV=3 PSH/23 RPT=1
PSH - Console user "admin" failed login
Login: admin
Password:



                Welcome to
               Cisco Systems
       VPN 3000 Concentrator Series
          Command Line Interface
Copyright (C) 1998-2004 Cisco Systems, Inc.



1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

Main -> _
```

```
               Cisco Systems
       VPN 3000 Concentrator Series
          Command Line Interface
Copyright (C) 1998-2004 Cisco Systems, Inc.



1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

Config -> 1
```

이 표는 현재 IP 주소를 보여줍니다

.

```
5) Tunneling and Security
6) Back

Config -> 1

This table shows current IP addresses.

  Intf         Status       IP Address/Subnet Mask          MAC Address
--------------------------------------------------------------------------------
Ether1-Pri|      UP      |       10.1.1.1/255.255.255.0  | 00.90.A4.00.06.94
Ether2-Pub|      UP      | 172.18.124.133/255.255.255.0  | 00.90.A4.00.06.95
Ether3-Ext|Not Configured|        0.0.0.0/0.0.0.0        |
--------------------------------------------------------------------------------
DNS Server(s): 10.1.0.121, 10.1.0.122
DNS Domain Name:
Default Gateway: 172.18.124.1

1) Configure Ethernet #1 (Private)
2) Configure Ethernet #2 (Public)
3) Configure Ethernet #3 (External)
4) Configure Power Supplies
5) Back

Interfaces ->
```

```
DNS Domain Name:
Default Gateway: 172.18.124.1

1) Configure Ethernet #1 (Private)
2) Configure Ethernet #2 (Public)
3) Configure Ethernet #3 (External)
4) Configure Power Supplies
5) Back

Interfaces -> 5

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

Config -> 2

1) Servers (Authentication, Authorization, Accounting, DNS, DHCP, etc.)
2) Address Management
3) IP Routing (static routes, OSPF, etc.)
4) Management Protocols (Telnet, TFTP, FTP, etc.)
5) Event Configuration
6) General Config (system name, time, etc.)
7) Client Update
8) Load Balancing Configuration
9) Back

System -> 3_
```

```
 8) Load Balancing Configuration
 9) Back

 System -> 3

 1) Static Routes
 2) Default Gateways
 3) OSPF
 4) OSPF Areas
 5) DHCP Parameters
 6) Redundancy
 7) Reverse Route Injection
 8) DHCP Relay
 9) Back

 Routing -> 1

 Static Routes
 ------------
 Destination     Mask            Metric Destination
 ------------------------------------------------------------
 0.0.0.0         0.0.0.0              1 172.18.124.1
 10.0.0.0        255.0.0.0           10 10.1.16.111
 192.168.0.0     255.255.0.0         10 10.1.16.111

 1) Add Static Route
 2) Modify Static Route
 3) Delete Static Route
 4) Back

 Routing ->
```

```
 8) Load Balancing Configuration
 9) Back

 System -> 3

 1) Static Routes
 2) Default Gateways
 3) OSPF
 4) OSPF Areas
 5) DHCP Parameters
 6) Redundancy
 7) Reverse Route Injection
 8) DHCP Relay
 9) Back

 Routing -> 1

 Static Routes
 ------------
 Destination     Mask            Metric Destination
 ------------------------------------------------------------
 0.0.0.0         0.0.0.0              1 172.18.124.1



 1) Add Static Route
 2) Modify Static Route
 3) Delete Static Route
 4) Back

 Routing ->
```

2. 공용 인터페이스에 대해 **Public** 필터 옵션을 선택해야 합니다

.

Configuration | Interfaces | Ethernet 2

You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.

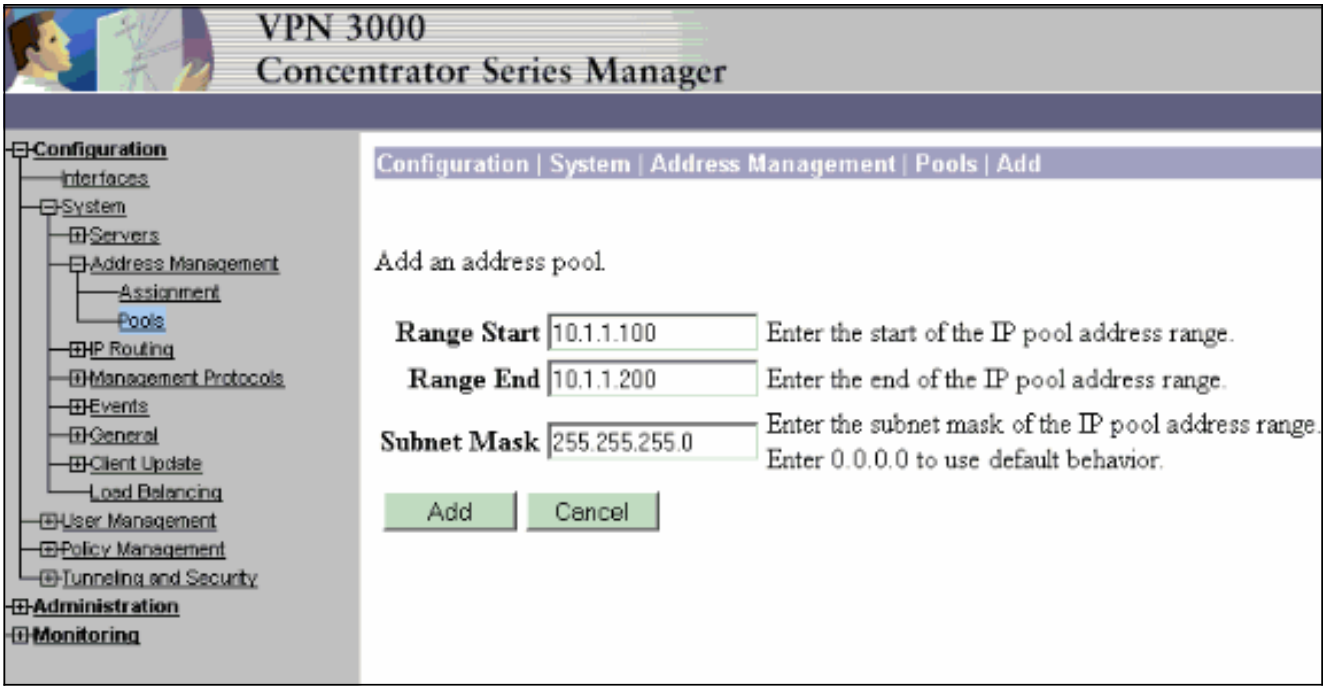
Configuring Ethernet Interface 2 (Public).

General | RIP | OSPF | Bandwidth | WebVPN

General Parameters			
Sel	**Attribute**	**Value**	**Description**
○	**Disabled**		Select to disable this interface.
○	**DHCP Client**		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.
◉	**Static IP Addressing**		Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface.
	IP Address	192.168.1.2	
	Subnet Mask	255.255.255.0	
	Public Interface	☑	Check to make this interface a "public" interface.
	MAC Address	00.03.A0.89.BF.D1	The MAC address for this interface.
	Filter	2. Public (Default)	Select the filter for this interface.
	Speed	10/100 auto	Select the speed for this interface.

3. 브라우저를 VPN Concentrator의 내부 인터페이스로 가리키고 **Configuration > System > Address Management > Address Pools** > Add를 선택하여 **사용 가능한 IP 주소 범위를 할당합니다.**내부 네트워크의 다른 디바이스와 충돌하지 않는 IP 주소 범위를 지정합니다.**참고:** 이러한 화면은 랩 설정에서만 이를 허용하도록 필터가 추가되었기 때문에 외부 공용 인터페이스 관리가 표시됩니다

.

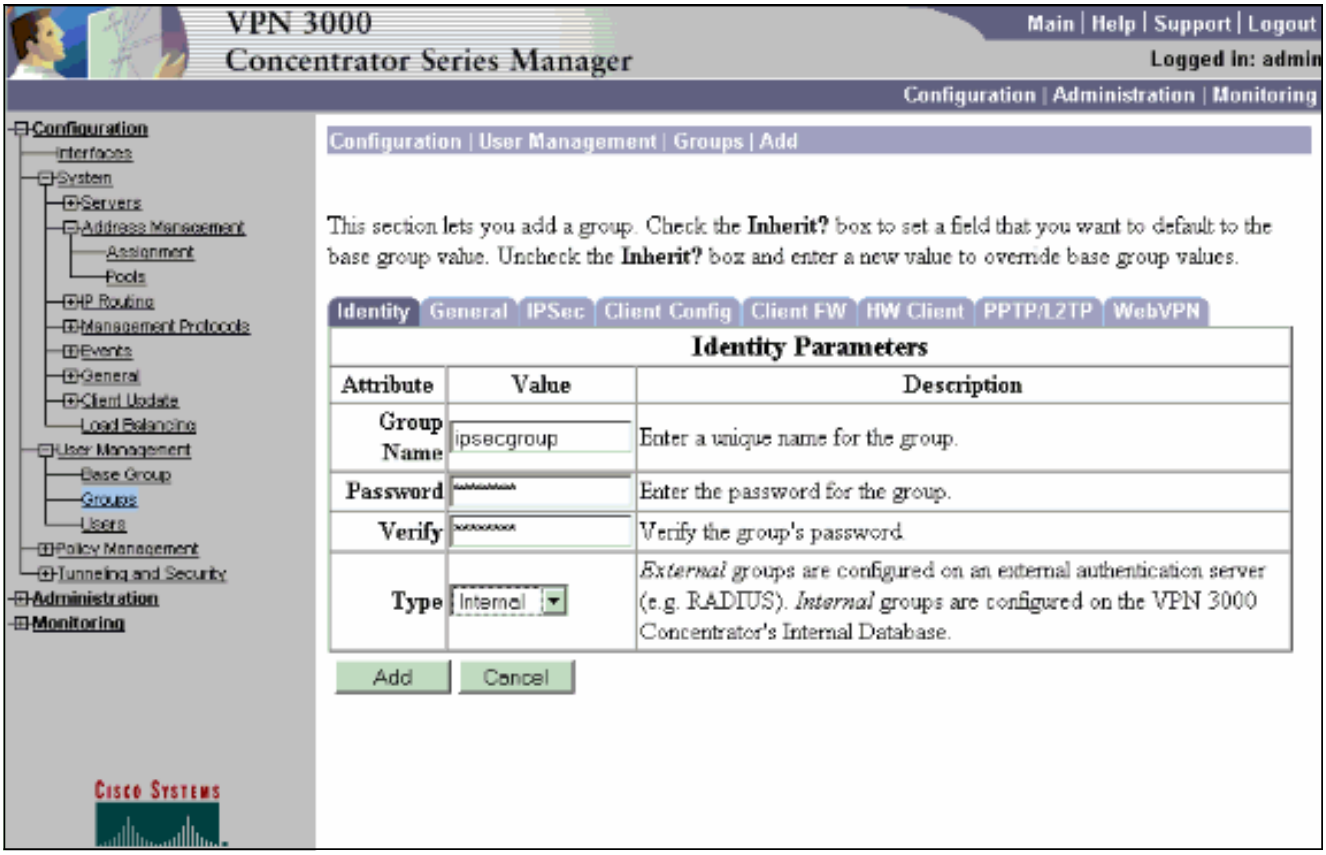


4. Configuration(구성) > System(시스템) > Address Management(주소 관리) > Assignment(할당)를 선택하고 Use Address Pools(주소 풀 사용) 확인란을 선택한 다음 Apply(적용)를 클릭하여 VPN Concentrator가 풀을 사용하도록 지시합니다

.

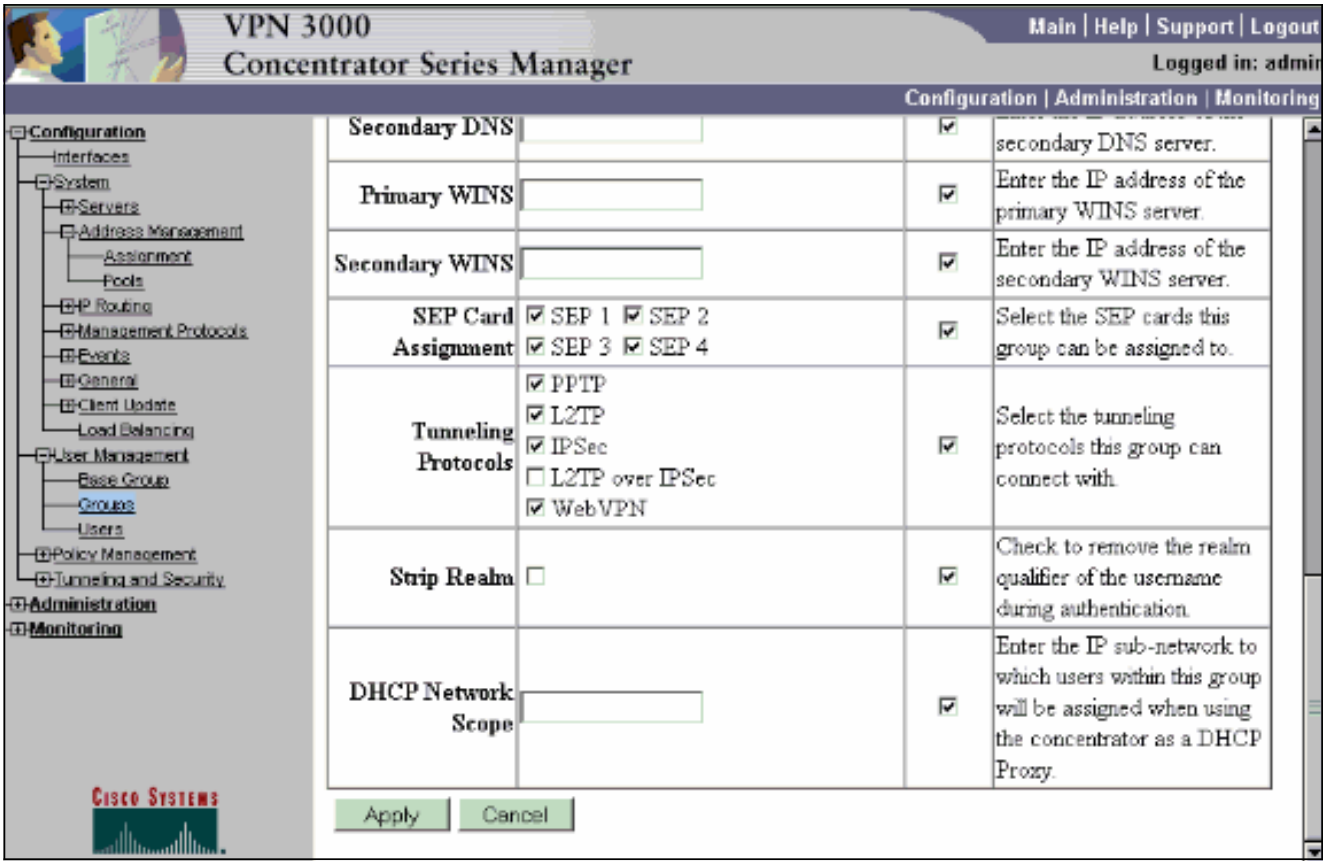
5. 사용자에 대한 IPsec 그룹을 구성하고 그룹 이름과 암호를 정의하려면 Configuration > User Management > Groups > Add Group을 선택합니다.다음 예에서는 password/verify="cisco123"과 함께 group="ipsecgroup"을 사용합니다

.



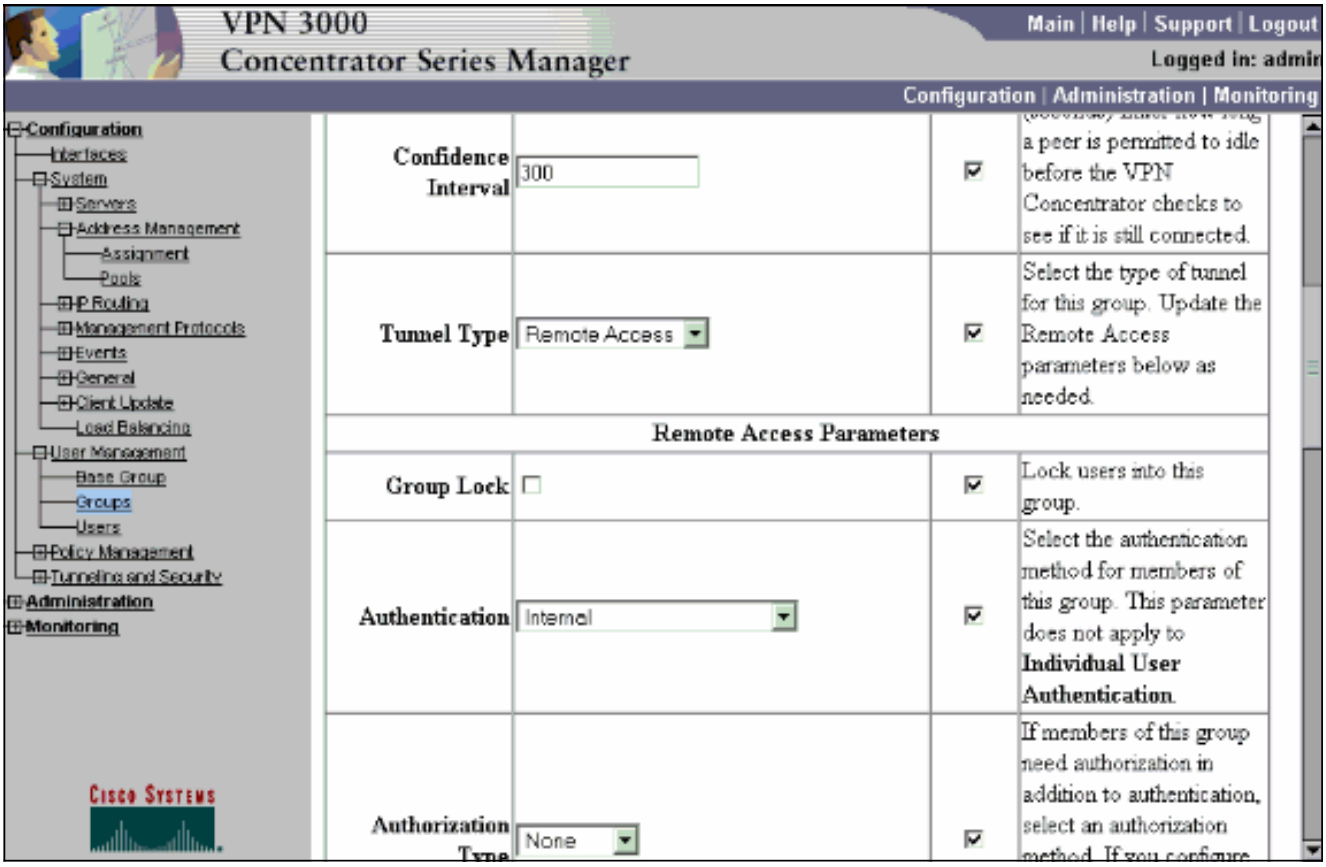
6. 그룹의 General(일반) 탭에서 **IPSec**이 선택되었는지 확인합니다

.



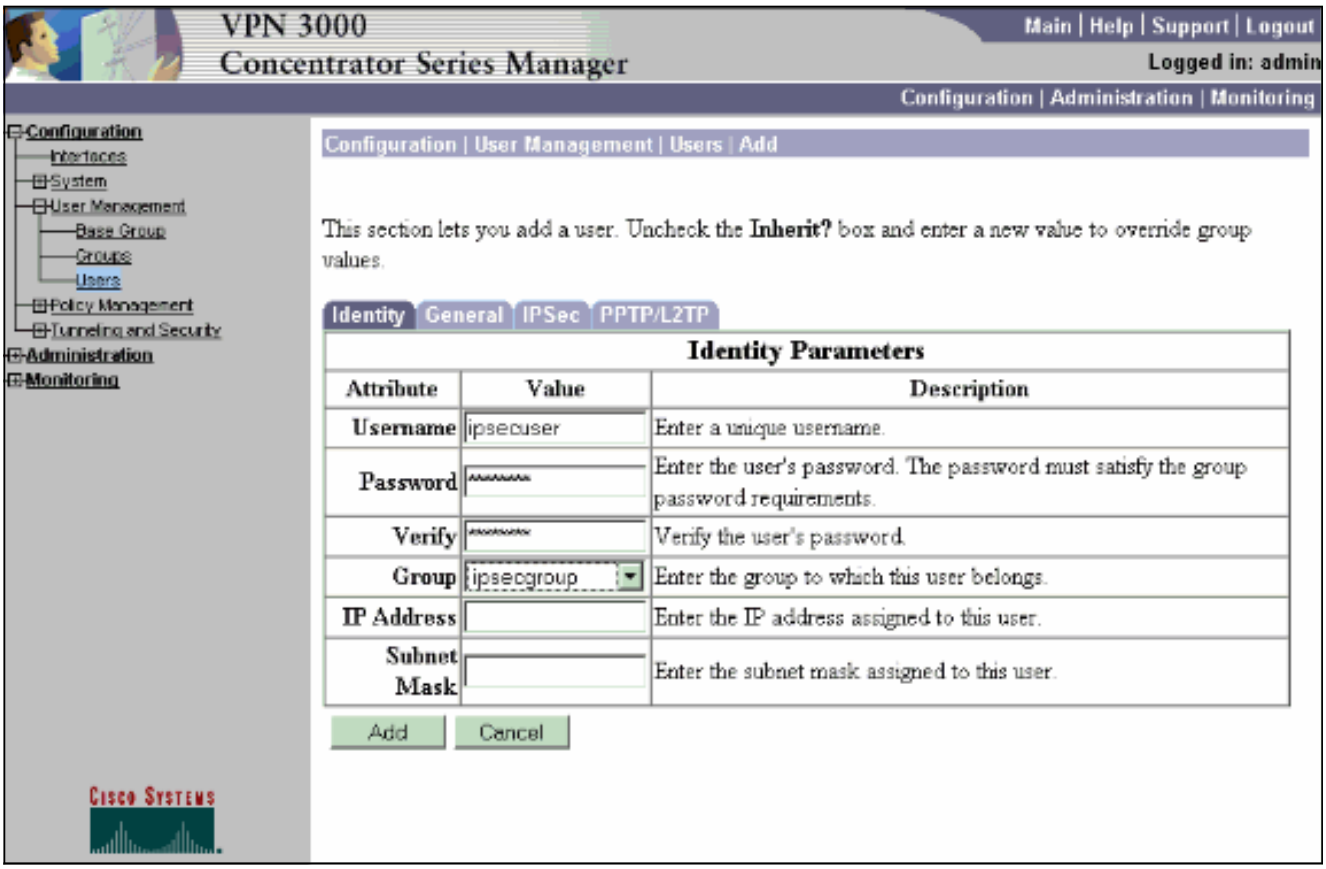
7. 그룹의 IPSec 탭에서 인증이 Internal(내부)로 설정되어 있는지 **확인합니다**. Configuration(**구성) > User Management(사용자 관리) > Groups(그룹) > Modify Group(그룹 수정)을** 선택하고 Current Groups(현재 그룹) 옵션에서 ipsecgroup을 선택합니다

.



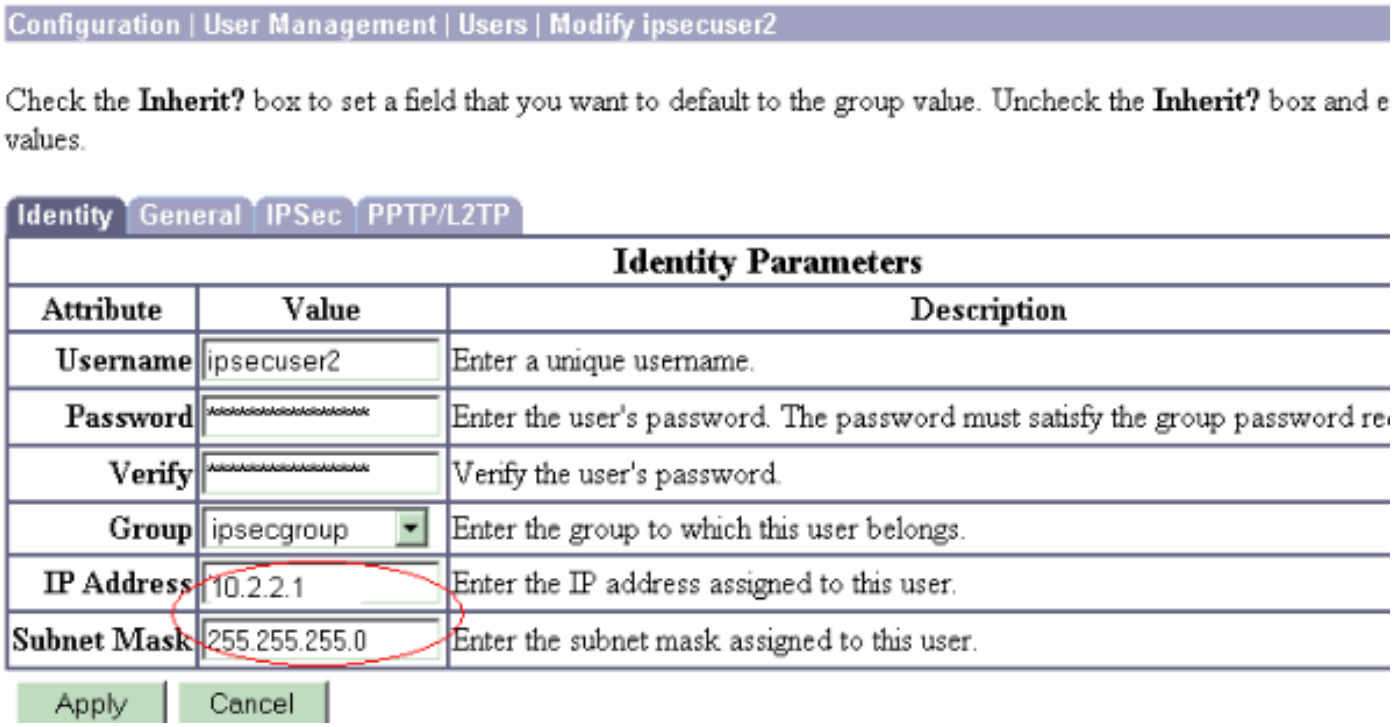
8. Configuration(**구성**) > **User Management(사용자 관리)** > Users(**사용자**) > Add(**추가**)**를** 선택하고 이전에 정의한 그룹에 사용자를 추가합니다.이 예에서 사용자는 "ipsecgroup" 그룹에서 "xyz12345" 암호를 가진 "ipsecuser"입니다

.

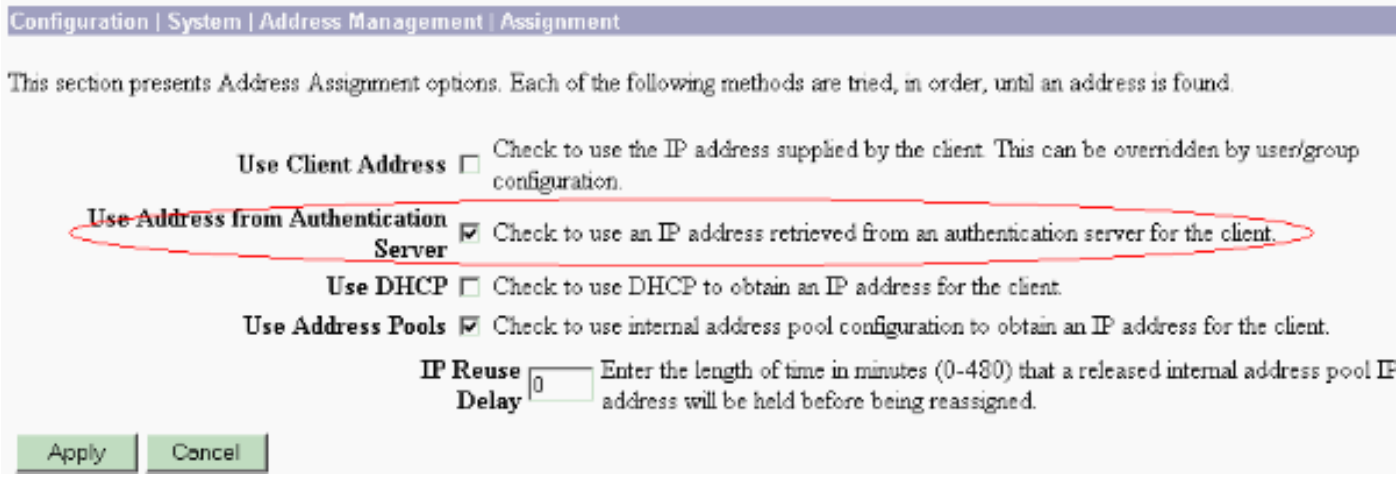


사용자에게 고정 IP 주소 할당

원격 VPN 사용자가 VPN 3000 Series Concentrator에 연결할 때마다 고정 IP 주소를 할당하려면 Configuration(구성) **> User Management(사용자 관리) > Users(사용자) > Modify ipsecuser2 > identity를** 선택합니다. 사용자(ipsecuser2)에 대한 이 컨피그레이션에서는 사용자가 연결할 때마다 고정 IP 주소 10.2.2.1/24이 할당됩니다.



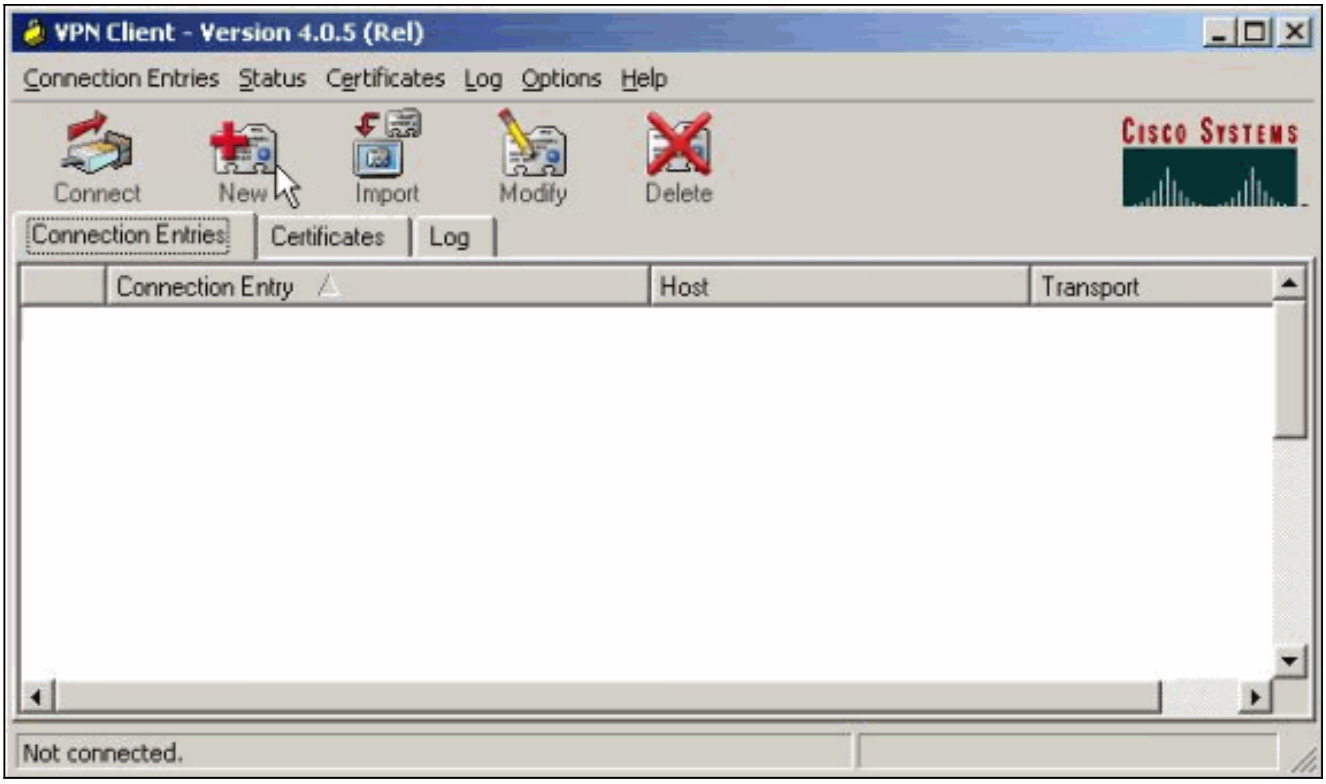
참고: VPN Concentrator가 할당된 IP 주소를 프로비저닝하려면 Configuration(컨피그레이션) **> System(시스템) > Address Management(주소 관리) > Assignment(할당)**로 이동해야 합니다. Use **Address from Authentication Server(인증 서버에서 주소 사용)**를 선택하여 인증 서버에서 검색된 IP 주소를 사용자별로 할당합니다. **User Management > Users > Add or Modify** 창의 Identity Parameters 탭에 입력된 IP 주소 및 서브넷 마스크는 내부 인증 서버에 있는 것으로 간주됩니다.



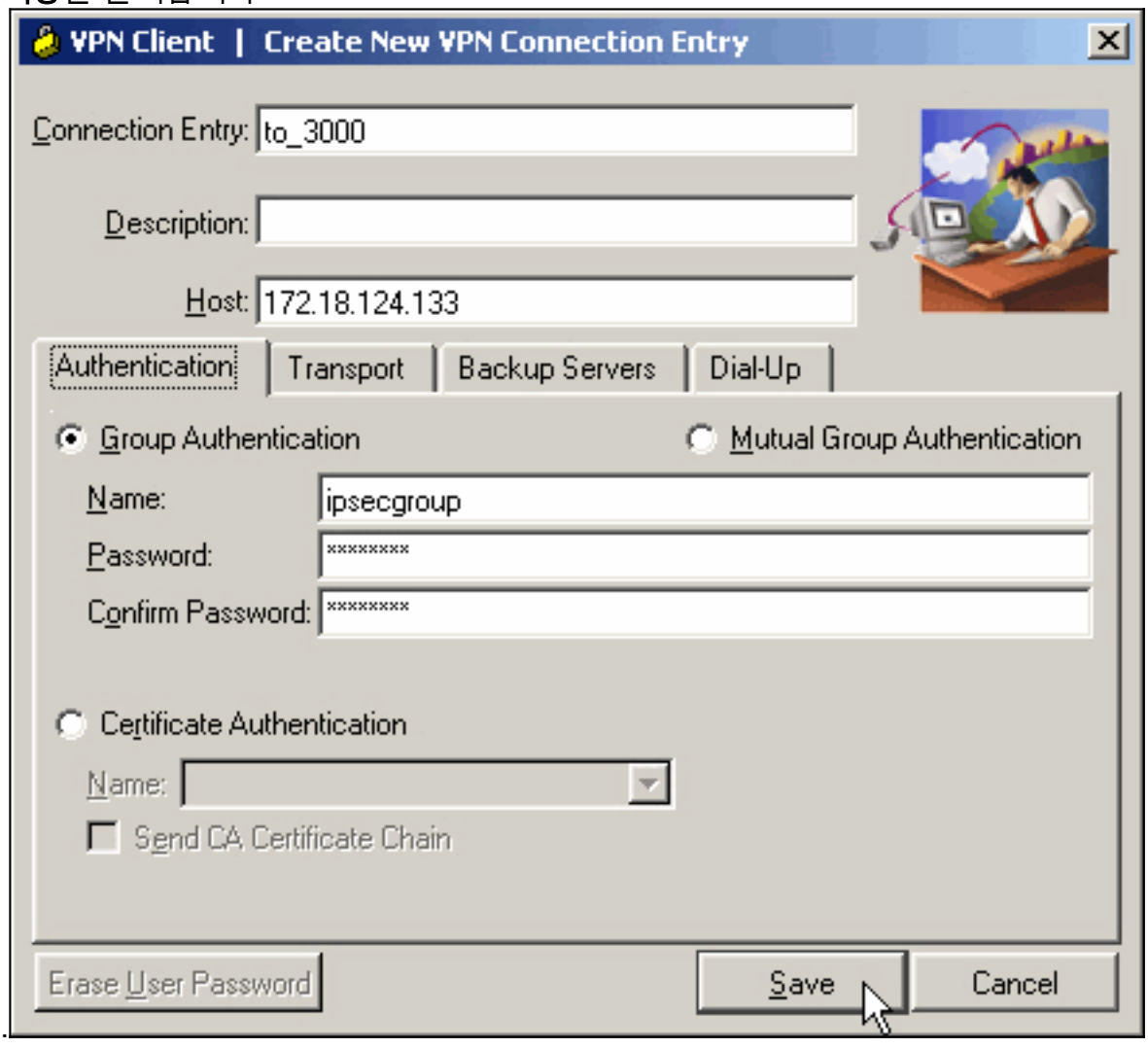
VPN 클라이언트 구성

VPN 클라이언트를 구성하려면 다음 단계를 완료합니다.

1. 새 연결 항목을 생성하려면 New를 클릭합니다
   .

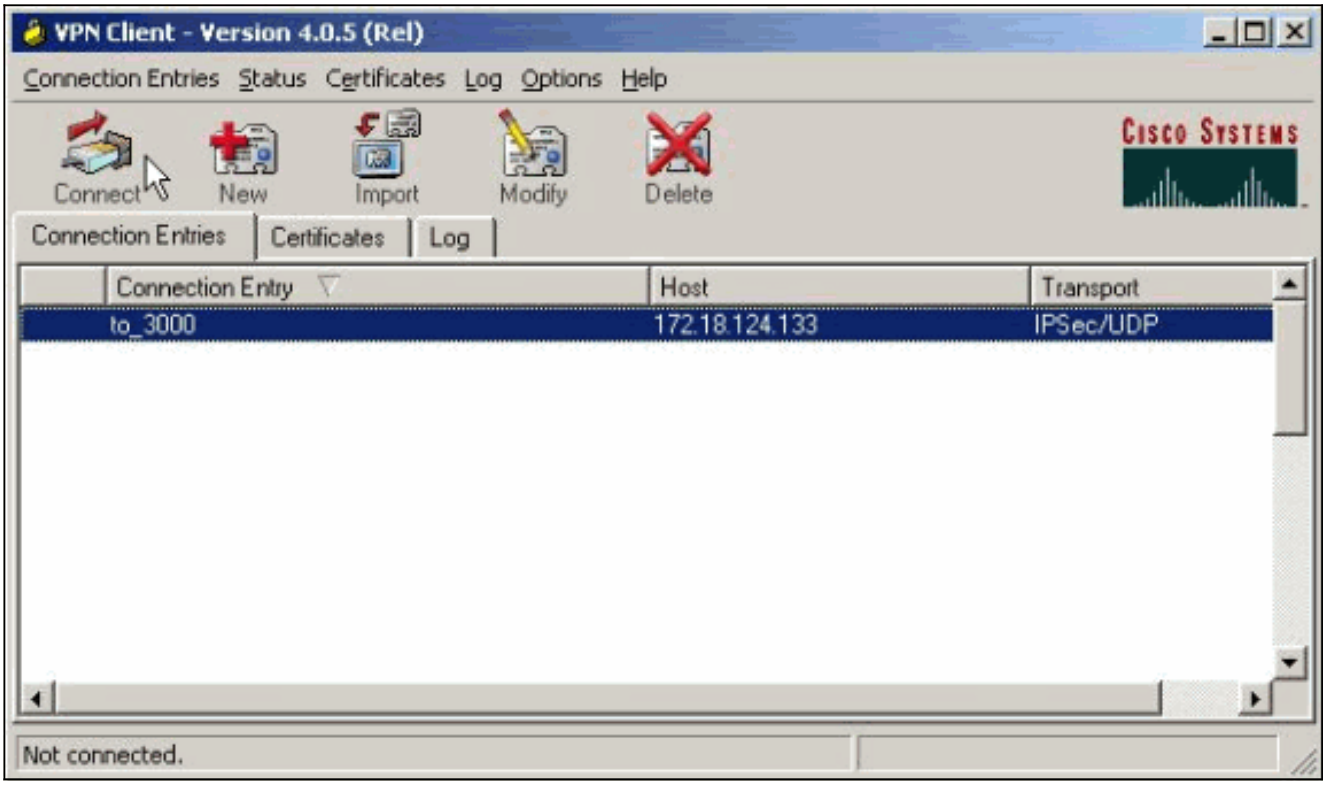


2. 연결의 이름을 지정하고 VPN Concentrator의 공용 인터페이스의 IP 주소를 입력하고 그룹 자격 증명을 제공합니다. 이 경우 이름은 ipsecgroup이고 **비밀번호**는 **cisco123**입니다. 완료되면 **저장**을 클릭합니다



3. 목록에서 연결 항목을 선택하고 **연결**을 클릭합니다. 사용자 이름/비밀번호를 입력하라는 프롬프트가 표시되면 사용자 이름/비밀번호를 입력합니다

.



다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

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

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: 디버그 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

문제가 될 수 있는 부분

이러한 오류는 발생할 수 있는 잠재적인 오류입니다. 이러한 오류에 대한 해결 방법은 VPN 클라이언트 및 VPN Concentrator 섹션을 참조하십시오.

- 사용자는 `Unable to negotiate IPSec or host did not response`(IPSec) .VPN 3000 디버그는 다음을 표시합니다.
  ```
  14 02/20/2001 08:59:29.100 SEV=4 IKE/22 RPT=5 10.102.55.139
  No Group found matching badgroup for Pre-shared key peer 10.102.55.139
  ```
  일반적인 원인: 사용자가 구성되지 않은 그룹 이름으로 연결을 시도합니다.
- 사용자가 연결할 수 없으며 VPN 3000 디버그가 표시됩니다.
  ```
  Filter missing on interface 2, IKE data from Peer x.x.x.x dropped
  ```
  일반적인 원인: 공용 인터페이스에 필터가 없습니다. 일반적으로 "공용" 필터이지만 전용 필터일 수 있습니다. "none"이 잘못되었습니다. Configuration(**구성**) > **Interfaces** > **Ethernet 2** > Filter(필터)를 선택하고 필터를 "public" 또는 다른 값(즉, "none"이 아님)으로 설정합니다. 필터

구성 방법에 대한 자세한 내용은 이 문서의 구성 섹션을 참조하십시오.

- 사용자가 연결할 수 없으며 `Unable to negotiate IPSec or host did not respected(IPSec )` .VPN 3000 디버그는 다음을 표시합니다.
  `Terminating connection attempt: IPSEC not permitted for group >group<`
  일반적인 원인: 그룹에서 IPsec을 선택하지 않았습니다. Configuration(**구성**) > **User Management(사용자 관리)** > **Groups(그룹)** > **<group>** > Modify(**수정**) > **General(일반)을 선택하고 Tunneling Protocols(터널링 프로토콜)에서 IPSec이 선택되었는지 확인합니다.**
- 사용자가 여러 번 시도한 후에는 연결할 수 없으며 가 .VPN 3000 디버그는 다음을 표시합니다.
  `Authentication rejected: Reason = User was not found handle = 14, server = Internal, user = <user>`
  일반적인 원인: 사용자가 사용자 데이터베이스에 없습니다. 사용자 인증 창이 표시될 때 올바른 사용자 이름을 입력해야 합니다.
- 사용자가 연결할 수 없으며 VPN 3000 디버그가 표시됩니다.
  `Filter missing on interface 0, IKE data from Peer x.x.x.x dropped`
  일반적인 원인: 기본 경로가 없습니다. 컨피그레이션에 기본 경로가 있는지 확인합니다. Configuration(**컨피그레이션**) > **System(시스템)** > **IP 라우팅** > **Default Gateway(기본 게이트웨이)를** 선택하고 기본 게이트웨이를 지정합니다.
- 사용자가 연결할 수 없으며 `IPSec` .VPN 3000 디버그는 다음을 표시합니다.
  `User [ <user> ]`
  `IKE rcv'd FAILED IP Addr status!`
  일반적인 원인: VPN 클라이언트에 IP 주소를 제공하기 위해 선택된 옵션이 없습니다. Configuration(**컨피그레이션**) > **System(시스템)** > Address Management(**주소 관리**) > Address Assignment(**주소 할당)를** 선택하고 옵션을 선택합니다.
- 사용자가 연결할 수 없으며 가 .VPN 3000 디버그는 다음을 표시합니다.
  `The calculated HASH doesn't match the received value`
  일반적인 원인: VPN 클라이언트의 그룹 암호가 VPN Concentrator에 구성된 암호와 다릅니다. VPN 클라이언트 및 Concentrator 모두에서 비밀번호를 확인합니다.
- VPN Concentrator 뒤의 리소스에 대한 VPN 풀을 설정했습니다. 리소스에 액세스할 수는 있지만 ping할 수는 없습니다.**일반적인 원인:** ICMP 패킷을 차단하는 VPN Concentrator 뒤에 PIX가 있습니다. 해당 PIX에 로그인하여 **액세스 목록을 적용하여 ICMP** 패킷을 활성화합니다.
- VPN Concentrator 디버그가 없으며 모든 사용자 또는 일부 사용자가 연결할 수 없습니다.기본 VPN Concentrator Public 필터에는 이 트래픽을 허용하는 규칙이 포함되어 있습니다.프로토콜 = UDP, 포트 = 500프로토콜 = UDP, 포트 = 10000프로토콜 = ESP프로토콜 = AHVPN Concentrator의 필터가 이 트래픽을 허용할 경우 VPN 클라이언트와 VPN Concentrator 간의 디바이스가 이러한 포트 중 일부(방화벽일 수 있음)를 차단할 수 있습니다. 확인하려면 VPN Concentrator 외부의 네트워크에서 VPN Concentrator에 연결해 보십시오. 이 경우 VPN 클라이언트 PC와 VPN Concentrator 간의 디바이스가 트래픽을 차단하고 있습니다.
- 사용자는 연결할 수 없으며 다음 로그를 볼 수 있습니다.
  `07/10/2006 11:48:59.280 SEV=4 IKE/0 RPT=141 10.86.190.92`
  `Group [NYMVPN]`
  `received an unencrypted packet when crypto active!! Dropping packet`
  일반적인 원인: 잘못 정의된 그룹 이름 또는 암호입니다. VPN 클라이언트에 대한 VPN 3000 Concentrator에서 새 그룹 이름 및 암호를 다시 생성합니다.
- 사용자는 VPN Concentrator 뒤의 호스트에 ping 또는 텔넷을 할 수 있지만 사용자는 Remote Desktop 9RDP(9RDP) 또는 유사한 애플리케이션을 사용할 수 없습니다.**일반적인 원인:** 퍼블릭 인터페이스에서 퍼블릭 필터가 활성화되지 않습니다. 이 문서의 Configure the VPN 3000 Concentrator 섹션에서 2단계를 참조하십시오.
- 사용자는 연결할 수 있지만 VPN 터널을 통해 전달되는 트래픽은 없습니다.**일반적인 원인:** NAT-투명성이 활성화되지 않았습니다. 대부분의 경우 VPN 클라이언트가 PAT 디바이스 뒤에

있습니다. PAT는 TCP 및 UDP 포트 번호를 사용하여 주소 공간을 절약합니다. 그러나 VPN 트래픽을 캡슐화하는 ESP는 TCP 또는 UDP와 별도의 프로토콜입니다. 이는 많은 PAT 디바이스가 ESP 트래픽을 처리할 수 없음을 의미합니다. NAT-T는 ESP 패킷을 UDP 패킷으로 캡슐화하여 PAT 디바이스를 쉽게 통과할 수 있도록 합니다. 따라서 ESP 트래픽이 PAT 디바이스를 통해 흐르도록 허용하려면 Concentrator에서 NAT-T를 활성화해야 합니다. 자세한 내용은 VPN 3000 Concentrator에서 IPSec에 대한 NAT 투명 모드 구성을 참조하십시오.

VPN 클라이언트

Start(**시작**) > **Programs(프로그램) > Cisco Systems VPN 3000 Client(Cisco Systems VPN 3000 클라이언트) > Log Viewer(로그 뷰어)를** 선택하여 로그 뷰어를 표시합니다.

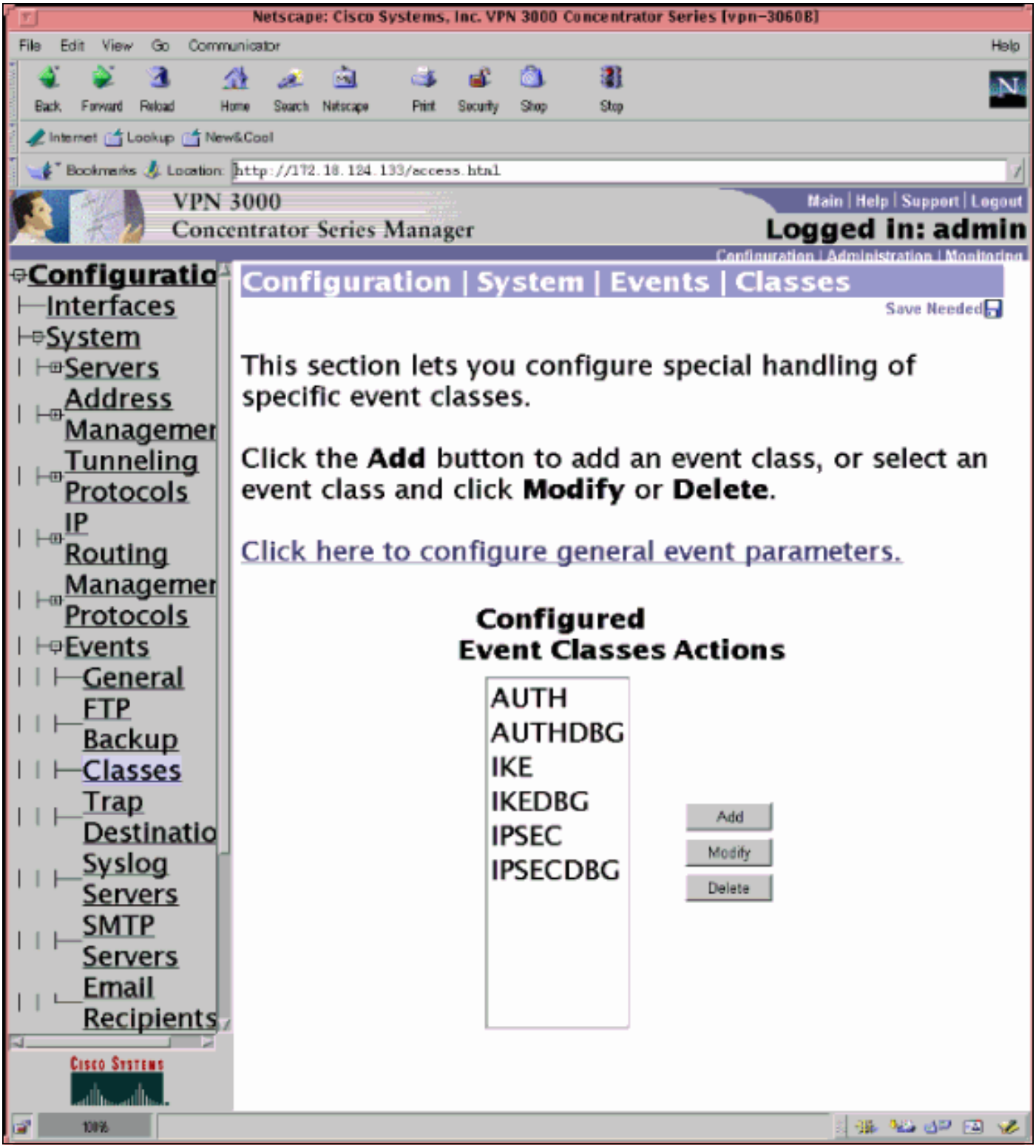
VPN 집선 장치

이벤트 **연결** 실패**가** 있는 경우 이 디버그를 켜려면 Configuration **> System > Events > Classes**를 선택합니다.

- AUTH - 1-13을 기록할 심각도
- AUTHDBG - 1-13을 기록할 심각도
- IKE - 로깅할 심각도 1-13
- IKEDBG - 1-13을 기록할 심각도
- IPSEC - 기록할 심각도 1-13
- IPSECDBG - 1-13을 기록할 심각도

참고: 필요한 경우 나중에 AUTHDECODE, IKEDECODE, IPSECDECODE를 추가할 수 있습니다.

추가 문제 해결 세부 정보는 VPN 3000 Concentrator의 연결 문제 해결을 참조하십시오.



로그를 보려면 **Monitoring > Filterable Event Log**를 선택합니다.

VPN 3000 Concentrator - 샘플 디버그

```
1 02/07/2002 08:00:13.320 SEV=8 IKEDBG/0 RPT=69 172.18.124.241
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + VENDOR (13) + VENDOR
 (13) + NONE (0) ... total length : 562

4 02/07/2002 08:00:13.320 SEV=9 IKEDBG/0 RPT=70 172.18.124.241
processing SA payload
```

```
5 02/07/2002 08:00:13.320 SEV=9 IKEDBG/0 RPT=71 172.18.124.241
processing ke payload

6 02/07/2002 08:00:13.320 SEV=9 IKEDBG/0 RPT=72 172.18.124.241
processing ISA_KE

7 02/07/2002 08:00:13.320 SEV=9 IKEDBG/1 RPT=7 172.18.124.241
processing nonce payload

8 02/07/2002 08:00:13.320 SEV=9 IKEDBG/1 RPT=8 172.18.124.241
Processing ID

9 02/07/2002 08:00:13.320 SEV=9 IKEDBG/47 RPT=4 172.18.124.241
processing VID payload

10 02/07/2002 08:00:13.320 SEV=9 IKEDBG/49 RPT=4 172.18.124.241
Received xauth V6 VID

11 02/07/2002 08:00:13.320 SEV=9 IKEDBG/47 RPT=5 172.18.124.241
processing VID payload

12 02/07/2002 08:00:13.320 SEV=9 IKEDBG/49 RPT=5 172.18.124.241
Received DPD VID

13 02/07/2002 08:00:13.320 SEV=9 IKEDBG/47 RPT=6 172.18.124.241
processing VID payload

14 02/07/2002 08:00:13.320 SEV=9 IKEDBG/49 RPT=6 172.18.124.241
Received Cisco Unity client VID

15 02/07/2002 08:00:13.320 SEV=9 IKEDBG/23 RPT=2 172.18.124.241
Starting group lookup for peer 172.18.124.241

16 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/1 RPT=2
AUTH_Open() returns 136

17 02/07/2002 08:00:13.320 SEV=7 AUTH/12 RPT=2
Authentication session opened: handle = 136

18 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/3 RPT=2
AUTH_PutAttrTable(136, 728a84)

19 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/6 RPT=2
AUTH_GroupAuthenticate(136, 9b143bc, 482fb0)

20 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/59 RPT=2
AUTH_BindServer(9a08630, 0, 0)

21 02/07/2002 08:00:13.320 SEV=9 AUTHDBG/69 RPT=2
Auth Server 16b3fa0 has been bound to ACB 9a08630, sessions = 1

22 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/65 RPT=2
AUTH_CreateTimer(9a08630, 0, 0)

23 02/07/2002 08:00:13.320 SEV=9 AUTHDBG/72 RPT=2
Reply timer created: handle = 3B2001B

24 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/61 RPT=2
AUTH_BuildMsg(9a08630, 0, 0)

25 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/64 RPT=2
AUTH_StartTimer(9a08630, 0, 0)

26 02/07/2002 08:00:13.320 SEV=9 AUTHDBG/73 RPT=2
```

```
Reply timer started: handle = 3B2001B, timestamp = 10085308, timeout = 30000

27 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/62 RPT=2
AUTH_SndRequest(9a08630, 0, 0)

28 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/50 RPT=3
IntDB_Decode(62b6d00, 115)

29 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/47 RPT=3
IntDB_Xmt(9a08630)

30 02/07/2002 08:00:13.320 SEV=9 AUTHDBG/71 RPT=2
xmit_cnt = 1

31 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/47 RPT=4
IntDB_Xmt(9a08630)

32 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/49 RPT=2
IntDB_Match(9a08630, 2ebe71c)

33 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/63 RPT=2
AUTH_RcvReply(9a08630, 0, 0)

34 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/50 RPT=4
IntDB_Decode(2ebe71c, 44)

35 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/48 RPT=2
IntDB_Rcv(9a08630)

36 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/66 RPT=2
AUTH_DeleteTimer(9a08630, 0, 0)

37 02/07/2002 08:00:13.420 SEV=9 AUTHDBG/74 RPT=2
Reply timer stopped: handle = 3B2001B, timestamp = 10085318

38 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/58 RPT=2
AUTH_Callback(9a08630, 0, 0)

39 02/07/2002 08:00:13.420 SEV=6 AUTH/41 RPT=2 172.18.124.241
Authentication successful: handle = 136, server = Internal, group = ipsecgroup

40 02/07/2002 08:00:13.420 SEV=7 IKEDBG/0 RPT=73 172.18.124.241
Group [ipsecgroup]
Found Phase 1 Group (ipsecgroup)

41 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/4 RPT=2
AUTH_GetAttrTable(136, 728c4c)

42 02/07/2002 08:00:13.420 SEV=7 IKEDBG/14 RPT=2 172.18.124.241
Group [ipsecgroup]
Authentication configured for Internal

43 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/2 RPT=2
AUTH_Close(136)

44 02/07/2002 08:00:13.420 SEV=9 IKEDBG/0 RPT=74 172.18.124.241
Group [ipsecgroup]
processing IKE SA

45 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=75 172.18.124.241
Group [ipsecgroup]
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
```

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

50 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=76 172.18.124.241
Group [ipsecgroup]
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

53 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=77 172.18.124.241
Group [ipsecgroup]
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

57 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=78 172.18.124.241
Group [ipsecgroup]
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

61 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=79 172.18.124.241
Group [ipsecgroup]
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 7

65 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=80 172.18.124.241
Group [ipsecgroup]
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

68 02/07/2002 08:00:13.420 SEV=7 IKEDBG/28 RPT=2 172.18.124.241
Group [ipsecgroup]
IKE SA Proposal # 1, Transform # 2 acceptable
Matches global IKE entry # 1

70 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/60 RPT=2
AUTH_UnbindServer(9a08630, 0, 0)

71 02/07/2002 08:00:13.420 SEV=9 AUTHDBG/70 RPT=2
Auth Server 16b3fa0 has been unbound from ACB 9a08630, sessions = 0

72 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/10 RPT=2
AUTH_Int_FreeAuthCB(9a08630)

73 02/07/2002 08:00:13.420 SEV=7 AUTH/13 RPT=2
Authentication session closed: handle = 136

74 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=81 172.18.124.241

Group [ipsecgroup]
constructing ISA_SA for isakmp

75 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=82 172.18.124.241
Group [ipsecgroup]
constructing ke payload
```

```
76 02/07/2002 08:00:13.450 SEV=9 IKEDBG/1 RPT=9 172.18.124.241
Group [ipsecgroup]
constructing nonce payload

77 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=83 172.18.124.241
Group [ipsecgroup]
Generating keys for Responder...

78 02/07/2002 08:00:13.450 SEV=9 IKEDBG/1 RPT=10 172.18.124.241
Group [ipsecgroup]
constructing ID

79 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=84
Group [ipsecgroup]
construct hash payload

80 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=85 172.18.124.241
Group [ipsecgroup]
computing hash

81 02/07/2002 08:00:13.450 SEV=9 IKEDBG/46 RPT=5 172.18.124.241
Group [ipsecgroup]
constructing Cisco Unity VID payload

82 02/07/2002 08:00:13.450 SEV=9 IKEDBG/46 RPT=6 172.18.124.241
Group [ipsecgroup]
constructing xauth V6 VID payload

83 02/07/2002 08:00:13.450 SEV=9 IKEDBG/46 RPT=7 172.18.124.241
Group [ipsecgroup]
constructing dpd vid payload

84 02/07/2002 08:00:13.450 SEV=9 IKEDBG/46 RPT=8 172.18.124.241
Group [ipsecgroup]
constructing VID payload

85 02/07/2002 08:00:13.450 SEV=9 IKEDBG/48 RPT=2 172.18.124.241
Group [ipsecgroup]
Send Altiga GW VID

86 02/07/2002 08:00:13.450 SEV=8 IKEDBG/0 RPT=86 172.18.124.241
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR (13) + VENDOR (1
3) + VENDOR (13) + VENDOR (13) + NONE (0) ... total length : 344

89 02/07/2002 08:00:13.480 SEV=8 IKEDBG/0 RPT=87 172.18.124.241
RECEIVED Message (msgid=0) with payloads :
HDR + HASH (8) + NOTIFY (11) + NONE (0) ... total length : 76

91 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=88 172.18.124.241
Group [ipsecgroup]
processing hash

92 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=89 172.18.124.241
Group [ipsecgroup]
computing hash

93 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=90 172.18.124.241
Group [ipsecgroup]
Processing Notify payload

94 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=91 172.18.124.241
Group [ipsecgroup]
```

```
constructing blank hash

95 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=92 172.18.124.241
Group [ipsecgroup]
constructing qm hash

96 02/07/2002 08:00:13.480 SEV=8 IKEDBG/0 RPT=93 172.18.124.241
SENDING Message (msgid=ec88ba81) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 100

98 02/07/2002 08:00:21.810 SEV=8 IKEDBG/0 RPT=94 172.18.124.241
RECEIVED Message (msgid=ec88ba81) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 85

100 02/07/2002 08:00:21.810 SEV=9 IKEDBG/1 RPT=11
process_attr(): Enter!

101 02/07/2002 08:00:21.810 SEV=9 IKEDBG/1 RPT=12
Processing MODE_CFG Reply attributes.

102 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/1 RPT=3
AUTH_Open() returns 137

103 02/07/2002 08:00:21.810 SEV=7 AUTH/12 RPT=3
Authentication session opened: handle = 137

104 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/3 RPT=3
AUTH_PutAttrTable(137, 728a84)

105 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/5 RPT=1
AUTH_Authenticate(137, 50093bc, 4b5708)

106 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/59 RPT=3
AUTH_BindServer(9b1544c, 0, 0)

107 02/07/2002 08:00:21.810 SEV=9 AUTHDBG/69 RPT=3
Auth Server 16b3fa0 has been bound to ACB 9b1544c, sessions = 1

108 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/65 RPT=3
AUTH_CreateTimer(9b1544c, 0, 0)

109 02/07/2002 08:00:21.810 SEV=9 AUTHDBG/72 RPT=3
Reply timer created: handle = 3B4001A

110 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/61 RPT=3
AUTH_BuildMsg(9b1544c, 0, 0)

111 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/64 RPT=3
AUTH_StartTimer(9b1544c, 0, 0)

112 02/07/2002 08:00:21.810 SEV=9 AUTHDBG/73 RPT=3
Reply timer started: handle = 3B4001A, timestamp = 10086157, timeout = 30000

113 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/62 RPT=3
AUTH_SndRequest(9b1544c, 0, 0)

114 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/50 RPT=5
IntDB_Decode(62b6d00, 102)

115 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/47 RPT=5
IntDB_Xmt(9b1544c)

116 02/07/2002 08:00:21.810 SEV=9 AUTHDBG/71 RPT=3
xmit_cnt = 1
```

```
117 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/47 RPT=6
IntDB_Xmt(9b1544c)

118 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/49 RPT=3
IntDB_Match(9b1544c, 2ebe71c)

119 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/63 RPT=3
AUTH_RcvReply(9b1544c, 0, 0)

120 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/50 RPT=6
IntDB_Decode(2ebe71c, 62)

121 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/48 RPT=3
IntDB_Rcv(9b1544c)

122 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/66 RPT=3
AUTH_DeleteTimer(9b1544c, 0, 0)

123 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/74 RPT=3
Reply timer stopped: handle = 3B4001A, timestamp = 10086167

124 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/58 RPT=3
AUTH_Callback(9b1544c, 0, 0)

125 02/07/2002 08:00:21.910 SEV=6 AUTH/4 RPT=1 172.18.124.241
Authentication successful: handle = 137, server = Internal, user = ipsecuser

126 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/3 RPT=4
AUTH_PutAttrTable(137, 1861c60)

127 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/60 RPT=3
AUTH_UnbindServer(9b1544c, 0, 0)

128 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/70 RPT=3
Auth Server 16b3fa0 has been unbound from ACB 9b1544c, sessions = 0

129 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/59 RPT=4
AUTH_BindServer(9b1544c, 0, 0)

130 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/69 RPT=4
Auth Server 16b3fa0 has been bound to ACB 9b1544c, sessions = 1

131 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/65 RPT=4
AUTH_CreateTimer(9b1544c, 0, 0)

132 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/72 RPT=4
Reply timer created: handle = 3B5001A

133 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/61 RPT=4
AUTH_BuildMsg(9b1544c, 0, 0)

134 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/64 RPT=4
AUTH_StartTimer(9b1544c, 0, 0)

135 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/73 RPT=4
Reply timer started: handle = 3B5001A, timestamp = 10086167, timeout = 30000

136 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/62 RPT=4
AUTH_SndRequest(9b1544c, 0, 0)

137 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/50 RPT=7
IntDB_Decode(2ec5350, 44)
```

```
138 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/47 RPT=7
IntDB_Xmt(9b1544c)

139 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/71 RPT=4
xmit_cnt = 1

140 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/47 RPT=8
IntDB_Xmt(9b1544c)

141 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/49 RPT=4
IntDB_Match(9b1544c, 2ec3f64)

142 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/63 RPT=4
AUTH_RcvReply(9b1544c, 0, 0)

143 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/50 RPT=8
IntDB_Decode(2ec3f64, 44)

144 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/48 RPT=4
IntDB_Rcv(9b1544c)

145 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/66 RPT=4
AUTH_DeleteTimer(9b1544c, 0, 0)

146 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/74 RPT=4
Reply timer stopped: handle = 3B5001A, timestamp = 10086177

147 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/58 RPT=4
AUTH_Callback(9b1544c, 0, 0)

148 02/07/2002 08:00:22.010 SEV=6 AUTH/41 RPT=3 172.18.124.241
Authentication successful: handle = 137, server = Internal, group = ipsecgroup

149 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/3 RPT=5
AUTH_PutAttrTable(137, 1861c60)

150 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/60 RPT=4
AUTH_UnbindServer(9b1544c, 0, 0)

151 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/70 RPT=4
Auth Server 16b3fa0 has been unbound from ACB 9b1544c, sessions = 0

152 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/59 RPT=5
AUTH_BindServer(9b1544c, 0, 0)

153 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/69 RPT=5
Auth Server 16b3fa0 has been bound to ACB 9b1544c, sessions = 1

154 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/65 RPT=5
AUTH_CreateTimer(9b1544c, 0, 0)

155 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/72 RPT=5
Reply timer created: handle = 3B6001A

156 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/61 RPT=5
AUTH_BuildMsg(9b1544c, 0, 0)

157 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/64 RPT=5
AUTH_StartTimer(9b1544c, 0, 0)

158 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/73 RPT=5
Reply timer started: handle = 3B6001A, timestamp = 10086177, timeout = 30000
```

```
159 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/62 RPT=5
AUTH_SndRequest(9b1544c, 0, 0)

160 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/50 RPT=9
IntDB_Decode(2ec39ec, 44)

161 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/47 RPT=9
IntDB_Xmt(9b1544c)

162 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/71 RPT=5
xmit_cnt = 1

163 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/47 RPT=10
IntDB_Xmt(9b1544c)

164 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/49 RPT=5
IntDB_Match(9b1544c, 2ec5350)

165 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/63 RPT=5
AUTH_RcvReply(9b1544c, 0, 0)

166 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/50 RPT=10
IntDB_Decode(2ec5350, 44)

167 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/48 RPT=5
IntDB_Rcv(9b1544c)

168 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/66 RPT=5
AUTH_DeleteTimer(9b1544c, 0, 0)

169 02/07/2002 08:00:22.110 SEV=9 AUTHDBG/74 RPT=5
Reply timer stopped: handle = 3B6001A, timestamp = 10086187

170 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/58 RPT=5
AUTH_Callback(9b1544c, 0, 0)

171 02/07/2002 08:00:22.110 SEV=6 AUTH/41 RPT=4 172.18.124.241
Authentication successful: handle = 137, server = Internal, group = ipsecgroup

172 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/4 RPT=3
AUTH_GetAttrTable(137, 729c04)

173 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/4 RPT=4
AUTH_GetAttrTable(137, 728c4c)

174 02/07/2002 08:00:22.110 SEV=7 IKEDBG/14 RPT=3 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Authentication configured for Internal

175 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/2 RPT=3
AUTH_Close(137)

176 02/07/2002 08:00:22.110 SEV=4 IKE/52 RPT=61 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
User (ipsecuser) authenticated.

177 02/07/2002 08:00:22.110 SEV=9 IKEDBG/0 RPT=95 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing blank hash

178 02/07/2002 08:00:22.110 SEV=9 IKEDBG/0 RPT=96 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing qm hash
```

```
179 02/07/2002 08:00:22.110 SEV=8 IKEDBG/0 RPT=97 172.18.124.241
SENDING Message (msgid=4cc78f4e) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 60

181 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/60 RPT=5
AUTH_UnbindServer(9b1544c, 0, 0)

182 02/07/2002 08:00:22.110 SEV=9 AUTHDBG/70 RPT=5
Auth Server 16b3fa0 has been unbound from ACB 9b1544c, sessions = 0

183 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/10 RPT=3
AUTH_Int_FreeAuthCB(9b1544c)

184 02/07/2002 08:00:22.110 SEV=7 AUTH/13 RPT=3
Authentication session closed: handle = 137

185 02/07/2002 08:00:22.110 SEV=8 IKEDBG/0 RPT=98 172.18.124.241
RECEIVED Message (msgid=4cc78f4e) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 56

187 02/07/2002 08:00:22.110 SEV=9 IKEDBG/1 RPT=13
process_attr(): Enter!

188 02/07/2002 08:00:22.110 SEV=9 IKEDBG/1 RPT=14
Processing cfg ACK attributes

189 02/07/2002 08:00:22.180 SEV=8 IKEDBG/0 RPT=99 172.18.124.241
RECEIVED Message (msgid=38a7c320) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 154

191 02/07/2002 08:00:22.180 SEV=9 IKEDBG/1 RPT=15
process_attr(): Enter!

192 02/07/2002 08:00:22.180 SEV=9 IKEDBG/1 RPT=16
Processing cfg Request attributes

193 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=1
MODE_CFG: Received request for IPV4 address!

194 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=2
MODE_CFG: Received request for IPV4 net mask!

195 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=3
MODE_CFG: Received request for DNS server address!

196 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=4
MODE_CFG: Received request for WINS server address!

197 02/07/2002 08:00:22.180 SEV=6 IKE/130 RPT=1 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Received unsupported transaction mode attribute: 5

199 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=5
MODE_CFG: Received request for Application Version!

200 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=6
MODE_CFG: Received request for Banner!

201 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=7
MODE_CFG: Received request for Save PW setting!

202 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=8
MODE_CFG: Received request for Default Domain Name!
```

```
203 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=9
MODE_CFG: Received request for Split Tunnel List!

204 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=10
MODE_CFG: Received request for PFS setting!

205 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=11
MODE_CFG: Received request for FWTYPE!

206 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=12
MODE_CFG: Received request for UDP Port!

207 02/07/2002 08:00:22.180 SEV=9 IKEDBG/31 RPT=1 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Obtained IP addr (10.1.1.100) prior to initiating Mode Cfg (XAuth enabled)

209 02/07/2002 08:00:22.180 SEV=9 IKEDBG/0 RPT=100 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing blank hash

210 02/07/2002 08:00:22.180 SEV=9 IKEDBG/0 RPT=101 172.18.124.241
0000: 00010004 0A010164 F0010000 F0070000     .......d........
0010: 00070062 43697363 6F205379 7374656D     ...bCisco System
0020: 732C2049 6E632E2F 56504E20 33303030     s, Inc./VPN 3000
0030: 20436F6E 63656E74 7261746F 72205665      Concentrator Ve
0040: 7273696F 6E20332E 352E5265 6C206275     rsion 3.5.Rel bu
0050: 696C7420 62792076 6D757270 6879206F     ilt by vmurphy o

216 02/07/2002 08:00:22.180 SEV=9 IKEDBG/0 RPT=102 172.18.124.241
0000: 6E204E6F 76203237 20323030 31203131     n Nov 27 2001 11
0010: 3A32323A 3331                           :22:31

218 02/07/2002 08:00:22.180 SEV=9 IKEDBG/0 RPT=103 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing qm hash

219 02/07/2002 08:00:22.180 SEV=8 IKEDBG/0 RPT=104 172.18.124.241
SENDING Message (msgid=38a7c320) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 174

221 02/07/2002 08:00:22.190 SEV=9 IKEDBG/21 RPT=1 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

223 02/07/2002 08:00:22.190 SEV=4 AUTH/22 RPT=86
User ipsecuser connected

224 02/07/2002 08:00:22.190 SEV=7 IKEDBG/22 RPT=1 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

226 02/07/2002 08:00:22.200 SEV=4 IKE/119 RPT=68 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
PHASE 1 COMPLETED

227 02/07/2002 08:00:22.200 SEV=6 IKE/121 RPT=1 172.18.124.241
Keep-alive type for this connection: DPD

228 02/07/2002 08:00:22.200 SEV=7 IKEDBG/0 RPT=105 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Starting phase 1 rekey timer: 82080000 (ms)

229 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=106 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
```

```
sending notify message

230 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=107 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing blank hash

231 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=108 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing qm hash

232 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=109 172.18.124.241
SENDING Message (msgid=be237358) with payloads :
HDR + HASH (8) + NOTIFY (11) + NONE (0) ... total length : 88

234 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=110 172.18.124.241
RECEIVED Message (msgid=472c326b) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total leng
th : 792

237 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=111 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing hash

238 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=112 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing SA payload

239 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=17 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing nonce payload

240 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=18 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Processing ID

241 02/07/2002 08:00:22.200 SEV=5 IKE/25 RPT=62 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Received remote Proxy Host data in ID Payload:
Address 10.1.1.100, Protocol 0, Port 0

244 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=19 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Processing ID

245 02/07/2002 08:00:22.200 SEV=5 IKE/24 RPT=61 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Received local Proxy Host data in ID Payload:
Address 172.18.124.133, Protocol 0, Port 0

248 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=113
QM IsRekeyed old sa not found by addr

249 02/07/2002 08:00:22.200 SEV=5 IKE/66 RPT=121 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
IKE Remote Peer configured for SA: ESP-3DES-MD5

251 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=114 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing IPSEC SA

252 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=115
Proposal # 2, Transform # 1, Type ESP, Id Triple-DES
Parsing received transform:
  Phase 2 failure:
```

```
  Mismatched attr types for class HMAC Algorithm:
    Rcv'd: SHA
    Cfg'd: MD5

256 02/07/2002 08:00:22.200 SEV=7 IKEDBG/27 RPT=1 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
IPSec SA Proposal # 3, Transform # 1 acceptable

258 02/07/2002 08:00:22.200 SEV=7 IKEDBG/0 RPT=116 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
IKE: requesting SPI!

259 02/07/2002 08:00:22.200 SEV=9 IPSECDBG/6 RPT=1
IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000, seq 129, err
 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKe
yLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 708648, lifetime2 0, ds
Id 300

263 02/07/2002 08:00:22.200 SEV=9 IPSECDBG/1 RPT=1
Processing KEY_GETSPI msg!

264 02/07/2002 08:00:22.200 SEV=7 IPSECDBG/13 RPT=1
Reserved SPI 1037485220

265 02/07/2002 08:00:22.200 SEV=8 IKEDBG/6 RPT=1
IKE got SPI from key engine: SPI = 0x3dd6c4a4

266 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=117 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
oakley constucting quick mode

267 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=118 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing blank hash

268 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=119 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing ISA_SA for ipsec

269 02/07/2002 08:00:22.200 SEV=5 IKE/75 RPT=121 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 seconds

271 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=20 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing ipsec nonce payload

272 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=21 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing proxy ID

273 02/07/2002 08:00:22.200 SEV=7 IKEDBG/0 RPT=120 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Transmitting Proxy Id:
  Remote host: 10.1.1.100  Protocol 0  Port 0
  Local host:  172.18.124.133  Protocol 0  Port 0

277 02/07/2002 08:00:22.200 SEV=7 IKEDBG/0 RPT=121 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Sending RESPONDER LIFETIME notification to Initiator

279 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=122 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing qm hash
```

```
280 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=123 172.18.124.241
SENDING Message (msgid=472c326b) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0)
... total length : 172

283 02/07/2002 08:00:22.210 SEV=8 IKEDBG/0 RPT=124 172.18.124.241
RECEIVED Message (msgid=64c59a32) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total leng
th : 796

286 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=125 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing hash

287 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=126 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing SA payload

288 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=22 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing nonce payload

289 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=23 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Processing ID

290 02/07/2002 08:00:22.210 SEV=5 IKE/25 RPT=63 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Received remote Proxy Host data in ID Payload:
Address 10.1.1.100, Protocol 0, Port 0

293 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=24 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Processing ID

294 02/07/2002 08:00:22.210 SEV=5 IKE/34 RPT=61 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Received local IP Proxy Subnet data in ID Payload:
 Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0

297 02/07/2002 08:00:22.210 SEV=8 IKEDBG/0 RPT=127
QM IsRekeyed old sa not found by addr

298 02/07/2002 08:00:22.210 SEV=5 IKE/66 RPT=122 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
IKE Remote Peer configured for SA: ESP-3DES-MD5

300 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=128 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing IPSEC SA

301 02/07/2002 08:00:22.210 SEV=8 IKEDBG/0 RPT=129
Proposal # 2, Transform # 1, Type ESP, Id Triple-DES
Parsing received transform:
  Phase 2 failure:
  Mismatched attr types for class HMAC Algorithm:
    Rcv'd: SHA
    Cfg'd: MD5

305 02/07/2002 08:00:22.210 SEV=7 IKEDBG/27 RPT=2 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
IPSec SA Proposal # 3, Transform # 1 acceptable
```

```
307 02/07/2002 08:00:22.210 SEV=7 IKEDBG/0 RPT=130 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
IKE: requesting SPI!

308 02/07/2002 08:00:22.210 SEV=9 IPSECDBG/6 RPT=2
IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000, seq 130, err
 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKe
yLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 708648, lifetime2 0, ds
Id 300

312 02/07/2002 08:00:22.210 SEV=9 IPSECDBG/1 RPT=2
Processing KEY_GETSPI msg!

313 02/07/2002 08:00:22.210 SEV=7 IPSECDBG/13 RPT=2
Reserved SPI 1517437317

314 02/07/2002 08:00:22.210 SEV=8 IKEDBG/6 RPT=2
IKE got SPI from key engine: SPI = 0x5a724185

315 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=131 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
oakley constucting quick mode

316 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=132 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing blank hash

317 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=133 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing ISA_SA for ipsec

318 02/07/2002 08:00:22.210 SEV=5 IKE/75 RPT=122 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 seconds

320 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=25 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing ipsec nonce payload

321 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=26 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing proxy ID

322 02/07/2002 08:00:22.210 SEV=7 IKEDBG/0 RPT=134 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Transmitting Proxy Id:
  Remote host: 10.1.1.100  Protocol 0  Port 0
  Local subnet:  0.0.0.0  mask 0.0.0.0 Protocol 0  Port 0

326 02/07/2002 08:00:22.210 SEV=7 IKEDBG/0 RPT=135 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Sending RESPONDER LIFETIME notification to Initiator

328 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=136 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing qm hash

329 02/07/2002 08:00:22.220 SEV=8 IKEDBG/0 RPT=137 172.18.124.241
SENDING Message (msgid=64c59a32) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0)
... total length : 176

332 02/07/2002 08:00:22.220 SEV=8 IKEDBG/0 RPT=138 172.18.124.241
RECEIVED Message (msgid=472c326b) with payloads :
```

```
HDR + HASH (8) + NONE (0) ... total length : 48

334 02/07/2002 08:00:22.220 SEV=9 IKEDBG/0 RPT=139 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing hash

335 02/07/2002 08:00:22.220 SEV=9 IKEDBG/0 RPT=140 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
loading all IPSEC SAs

336 02/07/2002 08:00:22.220 SEV=9 IKEDBG/1 RPT=27 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Generating Quick Mode Key!

337 02/07/2002 08:00:22.220 SEV=9 IKEDBG/1 RPT=28 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Generating Quick Mode Key!

338 02/07/2002 08:00:22.220 SEV=7 IKEDBG/0 RPT=141 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Loading host:
  Dst: 172.18.124.133
  Src: 10.1.1.100

340 02/07/2002 08:00:22.220 SEV=4 IKE/49 RPT=129 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Security negotiation complete for User (ipsecuser)
Responder, Inbound SPI = 0x3dd6c4a4, Outbound SPI = 0x8104887e

343 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/6 RPT=3
IPSEC key message parse - msgtype 1, len 624, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 64, label 0, pad 0, spi 8104887e, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, ds
Id 0

347 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=3
Processing KEY_ADD msg!

348 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=4
key_msghdr2secassoc(): Enter

349 02/07/2002 08:00:22.220 SEV=7 IPSECDBG/1 RPT=5
No USER filter configured

350 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=6
KeyProcessAdd: Enter

351 02/07/2002 08:00:22.220 SEV=8 IPSECDBG/1 RPT=7
KeyProcessAdd: Adding outbound SA

352 02/07/2002 08:00:22.220 SEV=8 IPSECDBG/1 RPT=8
KeyProcessAdd: src 172.18.124.133 mask 0.0.0.0, dst 10.1.1.100 mask 0.0.0.0

353 02/07/2002 08:00:22.220 SEV=8 IPSECDBG/1 RPT=9
KeyProcessAdd: FilterIpsecAddIkeSa success

354 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/6 RPT=4
IPSEC key message parse - msgtype 3, len 336, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 32, label 0, pad 0, spi 3dd6c4a4, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, ds
Id 0

358 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=10
Processing KEY_UPDATE msg!
```

```
359 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=11
Update inbound SA addresses

360 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=12
key_msghdr2secassoc(): Enter

361 02/07/2002 08:00:22.220 SEV=7 IPSECDBG/1 RPT=13
No USER filter configured

362 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=14
KeyProcessUpdate: Enter

363 02/07/2002 08:00:22.220 SEV=8 IPSECDBG/1 RPT=15
KeyProcessUpdate: success

364 02/07/2002 08:00:22.220 SEV=8 IKEDBG/7 RPT=1
IKE got a KEY_ADD msg for SA: SPI = 0x8104887e

365 02/07/2002 08:00:22.220 SEV=8 IKEDBG/0 RPT=142
pitcher: rcv KEY_UPDATE, spi 0x3dd6c4a4

366 02/07/2002 08:00:22.220 SEV=4 IKE/120 RPT=129 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
PHASE 2 COMPLETED (msgid=472c326b)

367 02/07/2002 08:00:22.280 SEV=8 IKEDBG/0 RPT=143 172.18.124.241
RECEIVED Message (msgid=64c59a32) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

369 02/07/2002 08:00:22.280 SEV=9 IKEDBG/0 RPT=144 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing hash

370 02/07/2002 08:00:22.280 SEV=9 IKEDBG/0 RPT=145 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
loading all IPSEC SAs

371 02/07/2002 08:00:22.280 SEV=9 IKEDBG/1 RPT=29 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Generating Quick Mode Key!

372 02/07/2002 08:00:22.280 SEV=9 IKEDBG/1 RPT=30 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Generating Quick Mode Key!

373 02/07/2002 08:00:22.280 SEV=7 IKEDBG/0 RPT=146 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Loading subnet:
  Dst: 0.0.0.0  mask: 0.0.0.0
  Src: 10.1.1.100

375 02/07/2002 08:00:22.280 SEV=4 IKE/49 RPT=130 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Security negotiation complete for User (ipsecuser)
Responder, Inbound SPI = 0x5a724185, Outbound SPI = 0x285e6ed0

378 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/6 RPT=5
IPSEC key message parse - msgtype 1, len 624, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 64, label 0, pad 0, spi 285e6ed0, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, ds
Id 0

382 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=16
```

```
Processing KEY_ADD msg!

383 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=17
key_msghdr2secassoc(): Enter

384 02/07/2002 08:00:22.280 SEV=7 IPSECDBG/1 RPT=18
No USER filter configured

385 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=19
KeyProcessAdd: Enter

386 02/07/2002 08:00:22.280 SEV=8 IPSECDBG/1 RPT=20
KeyProcessAdd: Adding outbound SA

387 02/07/2002 08:00:22.280 SEV=8 IPSECDBG/1 RPT=21
KeyProcessAdd: src 0.0.0.0 mask 255.255.255.255, dst 10.1.1.100 mask 0.0.0.0

388 02/07/2002 08:00:22.280 SEV=8 IPSECDBG/1 RPT=22
KeyProcessAdd: FilterIpsecAddIkeSa success

389 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/6 RPT=6
IPSEC key message parse - msgtype 3, len 336, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 32, label 0, pad 0, spi 5a724185, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, ds
Id 0

393 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=23
Processing KEY_UPDATE msg!

394 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=24
Update inbound SA addresses

395 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=25
key_msghdr2secassoc(): Enter

396 02/07/2002 08:00:22.280 SEV=7 IPSECDBG/1 RPT=26
No USER filter configured

397 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=27
KeyProcessUpdate: Enter

398 02/07/2002 08:00:22.280 SEV=8 IPSECDBG/1 RPT=28
KeyProcessUpdate: success

399 02/07/2002 08:00:22.280 SEV=8 IKEDBG/7 RPT=2
IKE got a KEY_ADD msg for SA: SPI = 0x285e6ed0

400 02/07/2002 08:00:22.280 SEV=8 IKEDBG/0 RPT=147
pitcher: rcv KEY_UPDATE, spi 0x5a724185

401 02/07/2002 08:00:22.280 SEV=4 IKE/120 RPT=130 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
PHASE 2 COMPLETED (msgid=64c59a32)
```

관련 정보

- Cisco VPN 3000 Series Concentrator 지원 페이지
- Cisco VPN 3000 Series 클라이언트 지원 페이지
- IPSec 협상/IKE 프로토콜
- 기술 지원 및 문서 – Cisco Systems