

사용자 인증 및 어카운팅 컨피그레이션에 RADIUS를 사용하는 Windows용 VPN 3000 Concentrator와 VPN 클라이언트 4.x 간 IPsec 예

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[VPN 3000 Concentrator에서 그룹 사용](#)

[VPN 3000 Concentrator에서 그룹 및 사용자 특성을 사용하는 방법](#)

[VPN 3000 Series Concentrator 구성](#)

[RADIUS 서버 구성](#)

[VPN 클라이언트 사용자에게 고정 IP 주소 할당](#)

[VPN 클라이언트 구성](#)

[계정 추가](#)

[다음을 확인합니다.](#)

[VPN Concentrator 확인](#)

[VPN 클라이언트 확인](#)

[문제 해결](#)

[Windows용 VPN 클라이언트 4.8 문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 사용자 인증 및 어카운팅에 RADIUS를 사용하는 Cisco VPN 3000 Concentrator와 Microsoft Windows용 Cisco VPN Client 4.x 간에 IPsec 터널을 설정하는 방법에 대해 설명합니다. 이 문서에서는 Windows용 Cisco ACS(Secure Access Control Server)를 사용하여 VPN 3000 Concentrator에 연결하는 사용자를 인증하는 것이 좋습니다. VPN 3000 Concentrator의 그룹은 단일 엔티티로 처리되는 사용자 모음입니다. 개별 사용자와 달리 그룹을 구성하면 시스템 관리를 간소화하고 구성 작업을 간소화할 수 있습니다.

Microsoft Windows [2003 인증을](#) 사용하는 Cisco VPN Client(4.x for Windows)와 PIX 500 Series Security Appliance 7.x 간의 원격 액세스 VPN 연결을 설정하려면 Microsoft Windows 2003 IAS RADIUS 인증 구성 예를 참조하십시오. 서비스(IAS) RADIUS 서버.

사용자 인증에 RADIUS를 사용하는 Cisco VPN Client 4.x와 라우터 간의 연결을 구성하려면 [Cisco IOS 라우터와 사용자 인증](#)에 RADIUS를 사용하는 Windows용 Cisco VPN Client 4.x 간 IPsec 구성

을 참조하십시오.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Windows RADIUS용 Cisco Secure ACS가 설치되어 있고 다른 디바이스와 제대로 작동합니다.
- Cisco VPN 3000 Concentrator는 HTML 인터페이스를 통해 구성되고 관리할 수 있습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure ACS for Windows 버전 4.0
- 이미지 파일 4.7.2.B가 포함된 Cisco VPN 3000 Series Concentrator
- Cisco VPN Client 4.x

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.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

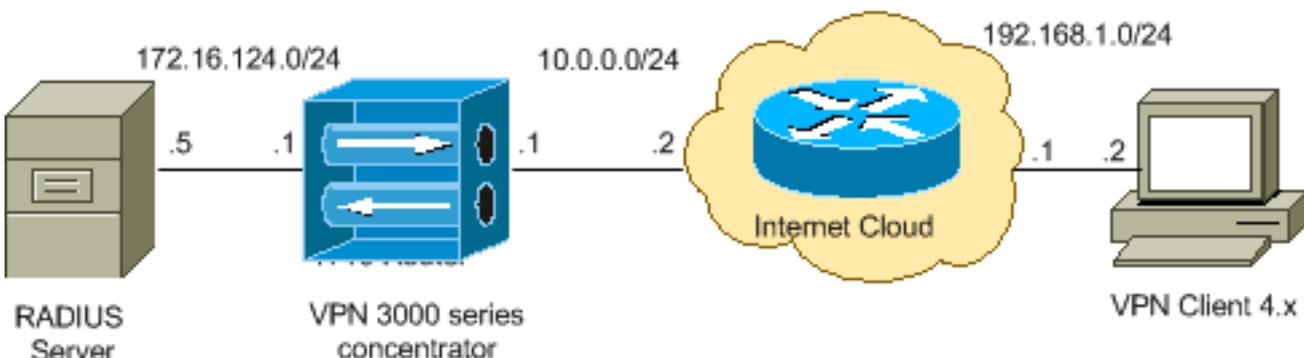
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: [명령 조회 도구](#)([등록된](#) 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다. 이는 [실](#)

습 환경에서 사용된 RFC [1918](#) 주소입니다.

VPN 3000 Concentrator에서 그룹 사용

Windows용 Cisco Secure ACS와 VPN 3000 Concentrator 모두에 대해 그룹을 정의할 수 있지만, 그룹을 다소 다르게 사용합니다. 작업을 간소화하기 위해 다음 작업을 수행합니다.

- 초기 터널을 설정할 때에 대한 **VPN 3000 Concentrator**에서 **단일 그룹**을 구성합니다. 이 그룹은 종종 터널 그룹이라고 하며 사전 공유 키(그룹 비밀번호)를 사용하여 VPN 3000 Concentrator에 대한 암호화된 IKE(Internet Key Exchange) 세션을 설정하는 데 사용됩니다. VPN Concentrator에 연결하려는 모든 Cisco VPN 클라이언트에서 구성해야 하는 동일한 그룹 이름 및 비밀번호입니다.
- 정책 관리를 위해 표준 RADIUS 특성 및 VSA(Vendor Specific Attributes)를 사용하는 **Windows용 Cisco Secure ACS** 서버에서 그룹을 구성합니다. VPN 3000 Concentrator와 함께 사용해야 하는 VSA는 RADIUS(VPN 3000) 특성입니다.
- **Windows RADIUS용 Cisco Secure ACS** 서버에서 **사용자를 구성하고 동일한 서버에 구성된 그룹 중 하나에 할당**합니다. 사용자는 그룹에 대해 정의된 특성을 상속하며 Cisco Secure ACS for Windows는 사용자가 인증될 때 이러한 특성을 VPN Concentrator로 전송합니다.

VPN 3000 Concentrator에서 그룹 및 사용자 특성을 사용하는 방법

VPN 3000 Concentrator는 VPN Concentrator를 사용하여 터널 그룹을 인증하고 RADIUS를 사용하는 사용자를 인증한 후 수신한 특성을 구성해야 합니다. VPN Concentrator는 인증이 VPN Concentrator에서 수행되었는지 또는 RADIUS에서 수행되었는지에 관계없이 다음과 같은 기본 설정 순서로 특성을 사용합니다.

1. **사용자 특성** - 이러한 특성은 항상 다른 속성보다 우선합니다.
2. **Tunnel Group attributes(터널 그룹 특성)** - 사용자를 인증할 때 반환되지 않는 모든 특성은 터널 그룹 특성에 의해 채워집니다.
3. **Base Group attributes(기본 그룹 특성)** - 사용자 또는 터널 그룹 특성에서 누락된 모든 특성은 VPN Concentrator Base Group(VPN Concentrator 기본 그룹) 특성으로 채워집니다.

VPN 3000 Series Concentrator 구성

IPsec 연결에 필요한 매개 변수에 대해 Cisco VPN 3000 Concentrator를 구성하고 VPN 사용자가 RADIUS 서버로 인증하도록 AAA 클라이언트를 구성하려면 이 섹션의 절차를 완료합니다.

이 Lab 설정에서 VPN Concentrator는 먼저 콘솔 포트를 통해 액세스되며 다음과 같은 출력에 따라 최소 컨피그레이션이 추가됩니다.

```
Login: admin
!-- The password must be "admin". Password:***** Welcome to Cisco Systems VPN 3000 Concentrator
Series Command Line Interface Copyright (C) 1998-2005 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 This table shows current IP addresses. Intf Status IP
Address/Subnet Mask MAC Address -----
----- Ether1-Pri| DOWN | 10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not
Configured| 0.0.0.0/0.0.0.0 | Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
----- DNS Server(s): DNS Server Not
```

```

Configured DNS Domain Name: Default Gateway: Default Gateway Not Configured 1) Configure
Ethernet #1 (Private) 2) Configure Ethernet #2 (Public) 3) Configure Ethernet #3 (External) 4)
Configure Power Supplies 5) Back Interfaces -> 1 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPsec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 1 1)
Disable 2) Enable using DHCP Client 3) Enable using Static IP Addressing Ethernet Interface 1 ->
[ ] 3 This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address ----
----- Ether1-Pri| DOWN |
10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 | Ether3-
Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
----- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default Gateway:
Default Gateway Not Configured > Enter IP Address Ethernet Interface 1 -> [ 10.1.1.1 ]
172.16.124.1 20 02/14/2007 09:50:18.830 SEV=3 IP/2 RPT=3 IP Interface 1 status changed to Link
Down. 21 02/14/2007 09:50:18.830 SEV=3 IP/1 RPT=3 IP Interface 1 status changed to Link Up. 22
02/14/2007 09:50:18.950 SEV=3 IP/1 RPT=4 IP Interface 1 status changed to Link Up. > Enter
Subnet Mask 23 02/14/2007 09:50:19.460 SEV=3 IP/2 RPT=4 IP Interface 1 status changed to Link
Down. Ethernet Interface 1 -> [ 255.255.255.0 ] 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPsec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 11
This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address -----
----- Ether1-Pri| Up |
172.16.124.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 |
Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
----- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default
Gateway: Default Gateway Not Configured 1) Configure Ethernet #1 (Private) 2) Configure Ethernet
#2 (Public) 3) Configure Ethernet #3 (External) 4) Configure Power Supplies 5) Back Interfaces -
>

```

VPN Concentrator가 Quick Configuration(빠른 컨피그레이션)에 나타나고 이러한 항목이 구성됩니다.

- 시간/날짜
- Interfaces/Masks in Configuration > Interfaces(public=10.0.0.1/24, private=172.16.124.1/24)
- Configuration(컨피그레이션) > System(시스템) > IP routing(IP 라우팅) > Default_Gateway(10.0.0.2)의 기본 게이트웨이

이때 VPN Concentrator는 내부 네트워크에서 HTML을 통해 액세스할 수 있습니다.

참고: VPN Concentrator가 외부에서 관리되는 경우 다음 단계를 수행합니다.

1. Configuration > 1-Interfaces > 2-Public > 4-Select IP Filter > 1. Private (Default)을 선택합니다.
2. 외부 관리자의 IP 주소를 추가하려면 Administration(관리) > 7-Access Rights(7-액세스 권한) > 2-Access Control List(2-액세스 제어 목록) > 1-Add Manager Workstation(관리자 워크스테이션 추가)을 선택합니다.

이러한 단계는 외부에서 VPN Concentrator를 관리하는 경우에만 필요합니다.

이 두 단계를 완료하면 나머지 컨피그레이션은 웹 브라우저를 사용하여 방금 구성한 인터페이스의 IP에 연결하여 GUI를 통해 수행할 수 있습니다. 이 예와 이 시점에서 VPN Concentrator는 내부 네트워크에서 HTML을 통해 액세스할 수 있습니다.

1. GUI를 시작한 후 인터페이스를 다시 확인하려면 Configuration > Interfaces를 선택합니다

Configuration | Interfaces Friday, 27 October 2006
Save Needed  Re

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	172.16.124.1	255.255.255.0	00.03.A0.89.BF.D0	
Ethernet 2 (Public)	UP	10.0.0.1	255.255.255.0	00.03.A0.89.BF.D1	10.0.0.2
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

- Windows RADIUS용 Cisco Secure ACS 서버를 VPN 3000 Concentrator 구성에 추가하려면 다음 단계를 완료하십시오. Configuration > System > Servers > Authentication을 선택하고 왼쪽 메뉴에서 Add를 클릭합니다

Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type: Selecting *Internal Server* will let you add users to database. If you are using RADIUS authenticator additional authorization check, do not configure at

Authentication Server: Enter IP address or hostname.

Used For: Select the operation(s) for which this RADIUS se

Server Port: Enter 0 for default port (1645).

Timeout: Enter the timeout for this server (seconds).

Retries: Enter the number of retries for this server.

Server Secret: Enter the RADIUS server secret.

Verify: Re-enter the secret.

서버 유형 **RADIUS**를 선택하고 Windows RADIUS용 Cisco Secure ACS 서버에 대해 이러한 매개변수를 추가합니다. 다른 모든 매개변수는 기본 상태로 둡니다. **Authentication Server(인증 서버)** - Windows RADIUS용 Cisco Secure ACS 서버의 IP 주소를 입력합니다. **Server Secret(서버 암호)** - RADIUS 서버 암호를 입력합니다. Cisco Secure ACS for Windows 컨피그레이션에서 VPN 3000 Concentrator를 구성할 때 사용하는 암호와 동일해야 합니다. **Verify(확인)** - 확인을 위한 비밀번호를 다시 입력합니다. 이렇게 하면 VPN 3000 Concentrator의 전역 컨피그레이션에 인증 서버가 추가됩니다. 이 서버는 인증 서버가 특별히 정의된 경우를 제외하고 모든 그룹에서 사용됩니다. 인증 서버가 그룹에 대해 구성되지 않은 경우 글로벌 인증 서버로 돌아갑니다.

- VPN 3000 Concentrator에서 터널 그룹을 구성하려면 다음 단계를 완료하십시오. 왼쪽 메뉴에서 Configuration > User Management > Groups를 선택하고 Add를 클릭합니다. 구성 탭에서 이러한 매개변수를 변경하거나 추가합니다. 다음 매개변수를 모두 변경할 때까지 Apply(적용

)를 클릭하지 마십시오.참고: 이러한 매개변수는 원격 액세스 VPN 연결에 필요한 최소값입니다. 또한 이러한 매개변수는 VPN 3000 Concentrator의 기본 그룹의 기본 설정이 변경되지 않았다고 가정합니다

.ID

Configuration | User Management | Groups | Add

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

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

Group Name(그룹 이름) - 그룹 이름을 입력합니다. 예를 들어, IPsecUsers입니다

.Password(비밀번호) - 그룹의 비밀번호를 입력합니다. IKE 세션의 사전 공유 키입니다

.Verify(확인) - 확인을 위한 비밀번호를 다시 입력합니다.유형 - 기본값으로 둡니다. 내부

.IPsec

Configuration | User Management | Groups | Modify ipsecgroup

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

IPSec Parameters			
Attribute	Value	Inherit?	Description
IPSec SA	<input type="text" value="ESP-3DES-MD5"/>	<input checked="" type="checkbox"/>	Select the group's IPSec Security Association.
IKE Peer Identity Validation	<input type="text" value="If supported by certificate"/>	<input checked="" type="checkbox"/>	Select whether or not to validate the identity of the peer.
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives.
Confidence Interval	<input type="text" value="300"/>	<input checked="" type="checkbox"/>	(seconds) Enter how long a peer is permitted to remain idle before the concentrator checks to see if it is still connected.
Tunnel Type	<input type="text" value="Remote Access"/>	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Upstream IPsec is required for Remote Access.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	<input type="text" value="RADIUS"/>	<input type="checkbox"/>	Select the authentication method for members of this group. This method only applies to Individual User Authentication .
Authorization Type	<input type="text" value="None"/>	<input checked="" type="checkbox"/>	If members of this group need authorization, select the authorization method. If you configure this method, you must also configure an Authorization Server.

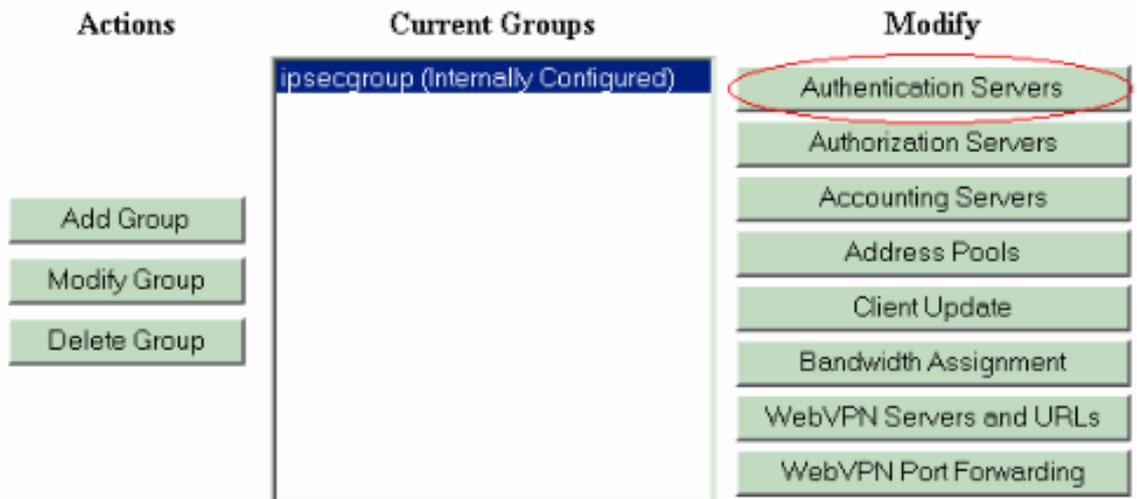
Tunnel Type(터널 유형) - Remote-Access(원격 액세스)를 선택합니다.Authentication(인증) - RADIUS. 이렇게 하면 VPN Concentrator에서 사용자를 인증하는 데 사용할 방법을 알 수 있습니다.Mode Config(모드 컨피그레이션) - 모드 컨피그레이션을 확인합니다.Apply를 클릭합니다.

- VPN 3000 Concentrator에서 여러 인증 서버를 구성하려면 다음 단계를 완료하십시오.그룹이 정의되면 해당 그룹을 강조 표시하고 Modify(수정) 열 아래에서 **Authentication Servers(인증**

서버)를 클릭합니다. 개별 인증 서버는 글로벌 서버에 없는 경우에도 각 그룹에 대해 정의할 수 있습니다

This section lets you configure groups. A group is a collection of users treated as a single entity.

Click the **Add Group** button to add a group, or select a group and click **Delete Group** or **Modify Group**. To group parameters, select a group and click the appropriate button.



서버 유형 **RADIUS**를 선택하고 Windows RADIUS용 Cisco Secure ACS 서버에 대해 이러한 매개변수를 추가합니다. 다른 모든 매개변수는 기본 상태로 둡니다. **Authentication Server(인증 서버)** - Windows RADIUS용 Cisco Secure ACS 서버의 IP 주소를 입력합니다. **Server Secret(서버 암호)** - RADIUS 서버 암호를 입력합니다. Cisco Secure ACS for Windows 컨피그레이션에서 VPN 3000 Concentrator를 구성할 때 사용하는 암호와 동일해야 합니다. **Verify(확인)** - 확인을 위한 비밀번호를 다시 입력합니다.

5. Configuration > System > Address Management > Assignment를 선택하고 Use Address from Authentication Server를 선택하여 클라이언트가 인증되면 RADIUS 서버에 생성된 IP 풀에서 VPN 클라이언트에 IP 주소를 할당합니다

This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.

Use Client Address Check to use the IP address supplied by the client. This can be overridden by user/group configuration.

Use Address from Authentication Server Check to use an IP address retrieved from an authentication server for the client.

Use DHCP Check to use DHCP to obtain an IP address for the client.

Use Address Pools Check to use internal address pool configuration to obtain an IP address for the client.

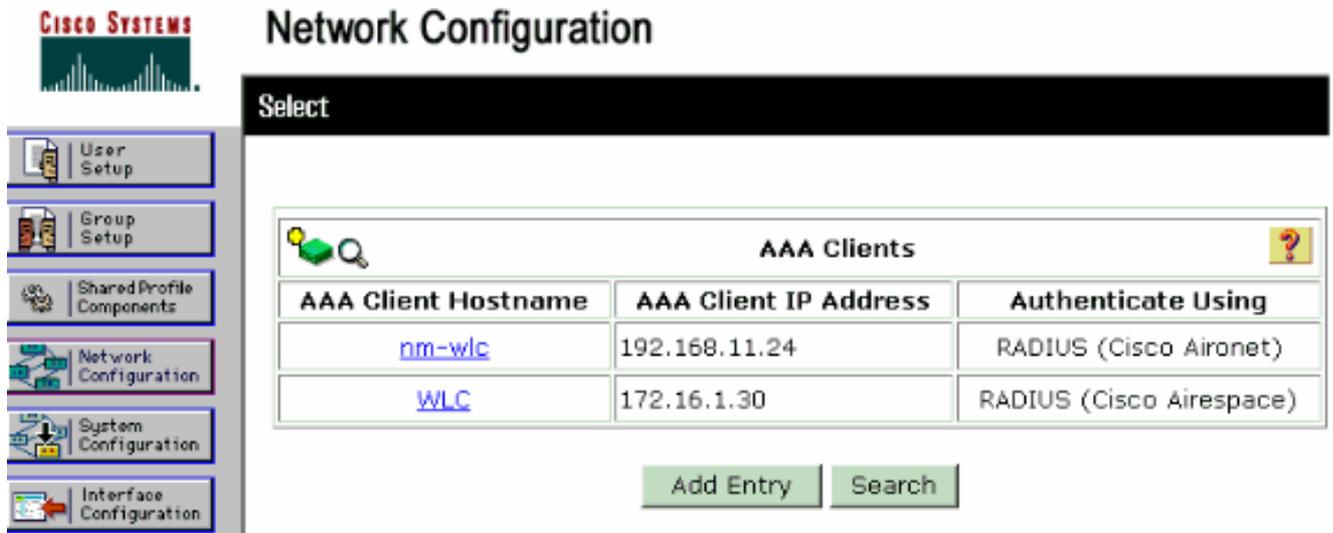
IP Reuse Delay Enter the length of time in minutes (0-480) that a released internal address pool IP address will be held before being reassigned.

RADIUS 서버 구성

이 섹션에서는 Cisco VPN 3000 Series Concentrator - AAA 클라이언트에서 전달되는 VPN 클라이언트 사용자 인증을 위해 Cisco Secure ACS를 RADIUS 서버로 구성하는 데 필요한 절차에 대해 설명합니다.

Windows RADIUS용 Cisco Secure ACS 서버를 실행하는 PC에서 관리 세션을 시작하려면 **ACS Admin** 아이콘을 두 번 클릭합니다. 필요한 경우 적절한 사용자 이름과 비밀번호를 사용하여 로그인합니다.

1. Windows용 Cisco Secure ACS 서버 컨피그레이션에 VPN 3000 Concentrator를 추가하려면 다음 단계를 완료하십시오. RADIUS 서버에 AAA 클라이언트를 추가하려면 Network Configuration을 선택하고 **Add Entry**를 클릭합니다



The screenshot shows the Cisco Systems Network Configuration interface. On the left is a navigation menu with options: User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, and Interface Configuration. The main area is titled 'Network Configuration' and contains a 'Select' dropdown menu. Below it is a table titled 'AAA Clients' with a search icon and a help icon. The table has three columns: AAA Client Hostname, AAA Client IP Address, and Authenticate Using. It lists two entries: 'nm-wlc' with IP 192.168.11.24 and 'WLC' with IP 172.16.1.30, both using RADIUS authentication. At the bottom are 'Add Entry' and 'Search' buttons.

AAA Client Hostname	AAA Client IP Address	Authenticate Using
nm-wlc	192.168.11.24	RADIUS (Cisco Aironet)
WLC	172.16.1.30	RADIUS (Cisco Airespace)

VPN 3000 Concentrator에 대해 다음 매개변수를 추가합니다

Network Configuration

Edit

Add AAA Client

AAA Client Hostname	<input type="text" value="VPN3000"/>
AAA Client IP Address	<input type="text" value="172.16.124.1"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

Submit

Submit + Apply

Cancel

AAA Client Hostname(AAA 클라이언트 호스트 이름) - VPN 3000 Concentrator(DNS 확인용)의 호스트 이름을 입력합니다.**AAA Client IP Address**(AAA 클라이언트 IP 주소) - VPN 3000 Concentrator의 IP 주소를 입력합니다.**Key**(키) - RADIUS 서버 암호를 입력합니다. VPN Concentrator에서 인증 서버를 추가할 때 구성한 암호와 동일해야 합니다.**Authenticate Using**(다음을 사용하여 인증) - **RADIUS(Cisco VPN 3000/ASA/PIX 7.x+)**를 선택합니다. 이렇게 하면 VPN 3000 VSA가 Group configuration(그룹 컨피그레이션) 창에 표시됩니다.
.Submit(제출)을 클릭합니다.Interface Configuration(인터페이스 컨피그레이션)을 선택하고 **RADIUS(Cisco VPN 3000/ASA/PIX 7.x+)**를 클릭한 다음 **Group [26] Vendor-Specific(26) 벤더별 그룹**를 선택합니다

Interface Configuration

Edit

RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)

User Group

- [026/3076/001] Access-Hours
- [026/3076/002] Simultaneous-Logins
- [026/3076/005] Primary-DNS
- [026/3076/006] Secondary-DNS
- [026/3076/007] Primary-WINS
- [026/3076/008] Secondary-WINS
- [026/3076/009] SEP-Card-Assignment
- [026/3076/011] Tunneling-Protocols
- [026/3076/012] IPSec-Sec-Association
- [026/3076/013] IPSec-Authentication
- [026/3076/015] IPSec-Banner1
- [026/3076/016] IPSec-Allow-Passwd-Store

Submit

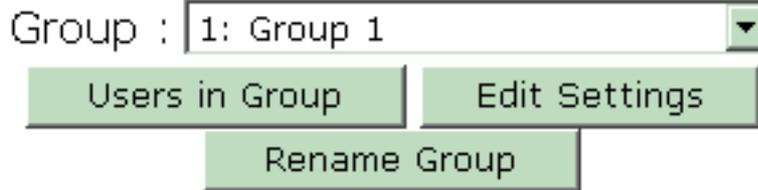
Cancel

참고: 'RADIUS 특성 26'은 모든 벤더별 특성을 나타냅니다. 예를 들어, **Interface Configuration(인터페이스 컨피그레이션) > RADIUS(Cisco VPN 3000)**를 선택하고 사용 가능한 모든 특성이 026으로 시작되는지 확인합니다. 이 경우 이러한 모든 벤더별 특성이 IETF RADIUS 26 표준에 속함을 나타냅니다. 이러한 특성은 기본적으로 사용자 또는 그룹 설정에 표시되지 않습니다. 그룹 설정에 표시하려면 네트워크 컨피그레이션에서 RADIUS로 인증하는 AAA 클라이언트(이 경우 VPN 3000 Concentrator)를 생성합니다. 그런 다음 User Setup, Group Setup 또는 Interface 컨피그레이션에서 둘 다에 나타나야 하는 특성을 선택합니다. 사용 가능한 특성 및 사용 방법에 대한 자세한 내용은 RADIUS 특성을 참조하십시오. Submit(제출)을 클릭합니다.

2. Windows용 Cisco Secure ACS 구성에 그룹을 추가하려면 다음 단계를 완료하십시오. **그룹 설정**을 선택한 다음 템플릿 그룹(예: 그룹 1)을 선택하고 **그룹 이름 바꾸기**를 클릭합니다

Group Setup

Select



Group : 1: Group 1

Users in Group Edit Settings

Rename Group

이름을 조직에 적합한 이름으로 변경합니다(예: ipsecgroup). 사용자가 이러한 그룹에 추가되므로 그룹 이름이 해당 그룹의 실제 용도를 반영하도록 합니다. 모든 사용자가 동일한 그룹에 속해 있는 경우 이를 VPN Users Group이라고 할 수 있습니다.**Edit Settings(설정 수정)**를 클릭하여 새로 이름이 변경된 그룹의 매개변수를 편집합니다

Group Setup

Jump To

Group Settings : ipsecgroup

Access Restrictions

Group Disabled 

Members of this group will be denied access to the network.

Callback 

No callback allowed

Dialup client specifies callback number

Use Windows Database callback settings (where possible)

Cisco

VPN 3000 RADIUS를 클릭하고 이러한 권장 특성을 구성합니다. 이렇게 하면 이 그룹에 할당된 사용자가 Cisco VPN 3000 RADIUS 특성을 상속할 수 있습니다. 그러면 Windows용 Cisco Secure ACS의 모든 사용자에게 대한 정책을 중앙 집중화할 수 있습니다

Group Setup

Jump To

Cisco VPN 3000/ASA/PIX v7.x+ RADIUS Attributes

[3076\001] Access-Hours

[3076\002] Simultaneous-Logins

[3076\005] Primary-DNS

[3076\006] Secondary-DNS

[3076\007] Primary-WINS

[3076\008] Secondary-WINS

[3076\009] SEP-Card-Assignment

참고: VPN

3000 Series Concentrator 컨피그레이션의 3단계에서 터널 그룹이 설정되고 VPN Concentrator의 Base Group이 원래 기본 설정에서 변경되지 않는 한 기술적으로 VPN 3000 RADIUS 특성을 구성할 필요가 없습니다. 권장 VPN 3000 특성: **Primary-DNS** - 기본 DNS 서버의 IP 주소를 입력합니다. **Secondary-DNS** - 보조 DNS 서버의 IP 주소를 입력합니다. **Primary-WINS** - 기본 WINS 서버의 IP 주소를 입력합니다. **Secondary-WINS** - 보조 WINS 서버의 IP 주소를 입력합니다. **Tunneling-Protocols(터널링 프로토콜)** - IPsec을 선택합니다. 이렇게 하면 IPsec 클라이언트 연결만 허용됩니다. PPTP 또는 L2TP는 허용되지 않습니다. **IPsec-Sec-Association—ESP-3DES-MD5**를 입력합니다. 그러면 모든 IPsec 클라이언트가 사용 가능한 최고 수준의 암호화를 사용하여 연결됩니다. **IPsec-Allow-Password-Store(IPsec-Allow-Password-Store)** - **Disallow(허용 안 함)**를 선택하여 사용자가 VPN 클라이언트에 암호를 저장할 수 없도록 합니다. **IPsec-Banner** - 연결 시 사용자에게 표시할 시작 메시지 배너를 입력합니다. 예: "Welcome to MyCompany employee VPN access!" **IPsec-Default Domain(IPsec-기본도메인)** - 회사의 도메인 이름을 입력합니다. 예: "mycompany.com"이 속성 세트는 필요하지 않습니다. 그러나 VPN 3000 Concentrator의 Base Group 특성이 변경되었는지 확실하지 않으면 다음 특성을 구성하는 것이 좋습니다. **Simultaneous-Logins(동시 로그인)** - 사용자가 동일한

사용자 이름으로 동시에 로그인할 수 있도록 허용하는 횟수를 입력합니다. 권장 사항은 1 또는 2입니다.**SEP-Card-Assignment(SEP-Card-Assignment) - Any-SEP를 선택합니다.IPsec-Mode-Config - ON을 선택합니다.IPsec over UDP**—이 그룹의 사용자가 UDP 프로토콜을 통해 IPsec을 사용하여 연결하도록 하지 않는 한 OFF를 선택합니다. ON을 선택할 경우 VPN 클라이언트는 UDP를 통한 IPsec을 로컬로 비활성화하고 정상적으로 연결할 수 있습니다.**IPsec over UDP Port - 4001~49151 범위의 UDP 포트 번호를 선택합니다. IPsec over UDP가 ON인 경우에만 사용됩니다.다음 특성 집합을 사용하려면 먼저 VPN Concentrator에 어떤 특성을 설정해야 사용할 수 있습니다. 고급 사용자에게만 권장됩니다.Access-Hours(액세스 시간) - Configuration(컨피그레이션) > Policy Management(정책 관리)에서 VPN 3000 Concentrator에 다양한 액세스 시간을 설정해야 합니다. 대신 Cisco Secure ACS for Windows에서 사용 가능한 액세스 시간을 사용하여 이 특성을 관리합니다.IPsec-Split-Tunnel-List - Configuration(컨피그레이션) > Policy Management(정책 관리) > Traffic Management(트래픽 관리)에서 VPN Concentrator에 네트워크 목록을 설정해야 합니다. 클라이언트에 전송되어 목록에 있는 네트워크에만 데이터를 암호화하라는 네트워크 목록입니다.VPN 클라이언트 사용자가 인증된 후 IP 주소를 VPN 클라이언트 사용자에게 할당하려면 Group setup(그룹 설정)에서 IP 할당을 선택하고 AAA 서버 풀에서 Assigned from AAA Server Pool(할당됨)을 선택합니다**

Group Setup

The screenshot shows a configuration window titled "IP Assignment". At the top, there is a "Jump To" dropdown menu currently set to "IP Address Assignment". Below the title bar, there are four radio button options for IP assignment methods:

- No IP address assignment
- Assigned by dialup client
- Assigned from AAA Client pool
- Assigned from AAA server pool

Below the selected option, there are two list boxes:

- Available Pools:** An empty list box.
- Selected Pools:** A list box containing "pool1".

Between the two list boxes are two arrow buttons: a right-pointing arrow (to move an item from Available to Selected) and a left-pointing arrow (to move an item from Selected to Available). Below the Selected Pools list box are "Up" and "Down" buttons for navigating the list.

VPN 클라이언트 사용자를 위한 IP 풀을 생성하려면 System configuration(시스템 컨피그레이션) > IP pools(IP 풀)를 선택하고 Submit(제출)을 클릭합니다

System Configuration

Edit

New Pool 	
Name	<input type="text" value="pool1"/>
Start Address	<input type="text" value="10.1.1.1"/>
End Address	<input type="text" value="10.1.1.10"/>

Submit

Cancel

System Configuration

Select

AAA Server IP Pools 			
Pool Name	Start Address	End Address	In Use
pool1	10.1.1.1	10.1.1.10	0%

구성을 저장하고 새 그룹을 활성화하려면 Submit > Restart를 선택합니다. 그룹을 더 추가하려면 이 단계를 반복합니다.

3. Windows용 Cisco Secure ACS에서 사용자를 구성합니다. User Setup(사용자 설정)을 선택하고 사용자 이름을 입력한 다음 Add/Edit(추가/수정)를 클릭합니다

User Setup

Select

User:

Find

Add/Edit

List users beginning with letter/number:

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#)
[N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)
[0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

List all users

Remove Dynamic Users

사용자 설정 섹션에

서 다음 매개변수를 구성합니다

User Setup

User: ipsecuser1 (New User)

Account Disabled

Supplementary User Info ?

Real Name	<input type="text" value="user1"/>
Description	<input type="text" value="user1"/>

User Setup ?

Password Authentication:

ACS Internal Database ▾

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password	<input type="password" value="*****"/>
Confirm Password	<input type="password" value="*****"/>

Separate (CHAP/MS-CHAP/ARAP)

Password	<input type="text"/>
Confirm Password	<input type="text"/>

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

▾

Password Authentication(비밀번호 인증) - ACS Internal Database(ACS 내부 데이터베이스)를 선택합니다. Cisco Secure PAP - Password(Cisco 보안 PAP - 비밀번호) - 사용자의 비밀번호를 입력합니다. Cisco Secure PAP - Confirm Password(Cisco 보안 PAP - 비밀번호 확인) - 새 사용자의 비밀번호를 다시 입력합니다. 사용자가 할당된 그룹 - 이전 단계에서 생성한 그룹의 이름을 선택합니다. 사용자 설정을 저장하고 활성화하려면 Submit(제출)을 클릭합니다. 사용자를 추가하려면 이 단계를 반복합니다.

VPN 클라이언트 사용자에게 고정 IP 주소 할당

다음 단계를 완료하십시오.

1. 새 VPN 그룹 IPSECGRP를 생성합니다.
2. 고정 IP를 수신할 사용자를 생성하고 IPSECGRP를 선택합니다. Assign **static IP address address** with the static IP address that is assignment(클라이언트 IP 주소 할당 아래에 할당된 고정 IP 주소를 사용하여 고정 IP 주소 할당)를 선택합니다

User Setup

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm
Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

IPSECGRP

Callback

- Use group setting
- No callback allowed
- Callback using this number
- Dialup client specifies callback number
- Use Windows Database callback settings

Client IP Address Assignment

- Use group settings
- No IP address assignment
- Assigned by dialup client
- Assign static IP address
- Assigned by AAA client pool

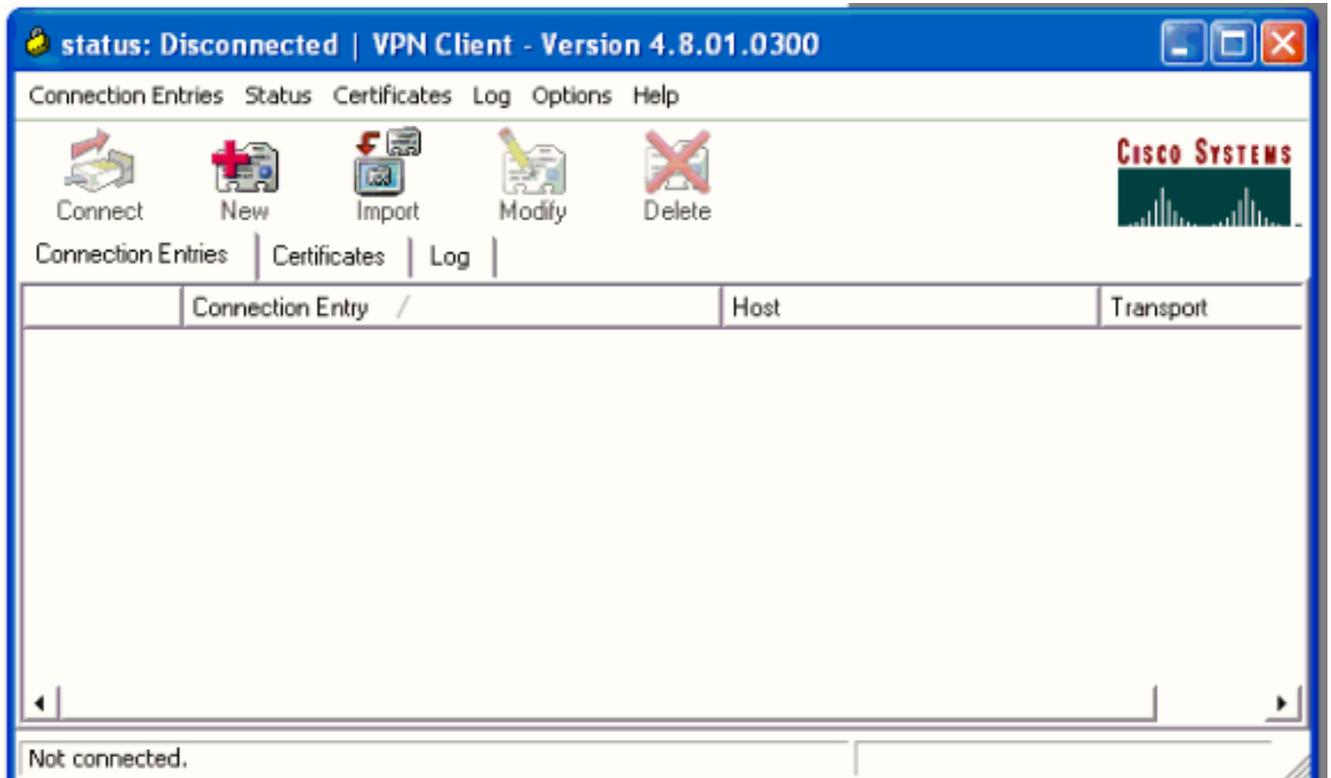
Submit

Delete

Cancel

이 섹션에서는 VPN 클라이언트측 컨피그레이션에 대해 설명합니다.

1. Start(시작) > Programs(프로그램) > Cisco Systems VPN Client(Cisco Systems VPN 클라이언트) > VPN Client(VPN 클라이언트)를 선택합니다.
2. Create New VPN Connection Entry(새 VPN 연결 항목 생성) 창을 시작하려면 New(새로 만들기)를 클릭합니다



3. 프롬프트가 표시되면 항목에 이름을 할당합니다. 원하는 경우 설명을 입력할 수도 있습니다. Host(호스트) 열에서 VPN 3000 Concentrator 공용 인터페이스 IP 주소를 지정하고 Group Authentication(그룹 인증)을 선택합니다. 그런 다음 그룹 이름과 암호를 입력합니다. 새 VPN 연결 항목을 완료하려면 Save(저장)를 클릭합니다

VPN Client | Create New VPN Connection Entry

Connection Entry: vpnuser

Description: Headoffice

Host: 10.0.0.1

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication Mutual Group Authentication

Name: ipsecgroup

Password: *****

Confirm Password: *****

Certificate Authentication

Name: [Dropdown]

Send CA Certificate Chain

Erase User Password | Save | Cancel

참고: VPN

Client가 Cisco VPN 3000 Series Concentrator에 구성된 것과 동일한 그룹 이름과 암호를 사용하도록 구성되어 있는지 확인하십시오.

계정 추가

인증이 수행된 후 어카운팅을 추가할 수 있습니다.

1. VPN 3000에서 Configuration(구성) > System(시스템) > Servers(서버) > Accounting Servers(계정 관리 서버)를 선택하고 Windows 서버용 Cisco Secure ACS를 추가합니다.
2. Configuration(컨피그레이션) > User Management(사용자 관리) > Groups(그룹)를 선택하고 그룹을 강조 표시하고 Modify Acct(계정 수정)를 클릭할 때 각 그룹에 개별 어카운팅 서버를 추가할 수 있습니다. 서버. 그런 다음 서버 암호를 사용하여 어카운팅 서버의 IP 주소를 입력합니다

Configure and add a RADIUS user accounting server.

Accounting Server	<input type="text" value="172.16.124.5"/>	Enter IP address or hostname.
Server Port	<input type="text" value="1646"/>	Enter the server UDP port number.
Timeout	<input type="text" value="1"/>	Enter the timeout for this server (se
Retries	<input type="text" value="3"/>	Enter the number of retries for this
Server Secret	<input type="text" value="*****"/>	Enter the RADIUS server secret.
Verify	<input type="text" value="*****"/>	Re-enter the server secret.
<input type="button" value="Add"/> <input type="button" value="Cancel"/>		

Cisco Secure ACS for Windows에서 회계 레코드는 다음과 같이 출력에 표시됩니다

Select

RADIUS Accounting active.csv

Regular Expression Start Date & Time End Date & Time Rows per Page

Filtering is not applied.

Date	Time	User-Name	Group-Name	Calling-Station-Id	Acct-Status-Type	Acct-Session-Id	Acct-Session-Time	Service-Type	Framed-Protocol	Acct-Input-Octets	Acct-Output-Octets	Acct-Input-Packets	Acct-Output-Packets
10/27/2006	18:38:20	ipsecuser1	ipsecgroup	192.168.1.2	Start	E8700001	..	Framed	PPP
10/27/2006	18:38:20	VPN 3000 Concentrator	Default Group	..	Accounting On
10/27/2006	13:17:10	VPN 3000 Concentrator	Default Group	..	Accounting Off

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

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

VPN Concentrator 확인

VPN 3000 Concentrator 측에서 원격 VPN 터널 설정을 확인하려면 **Administration(관리) > Administer Sessions(세션 관리)**를 선택합니다.

Remote Access Sessions

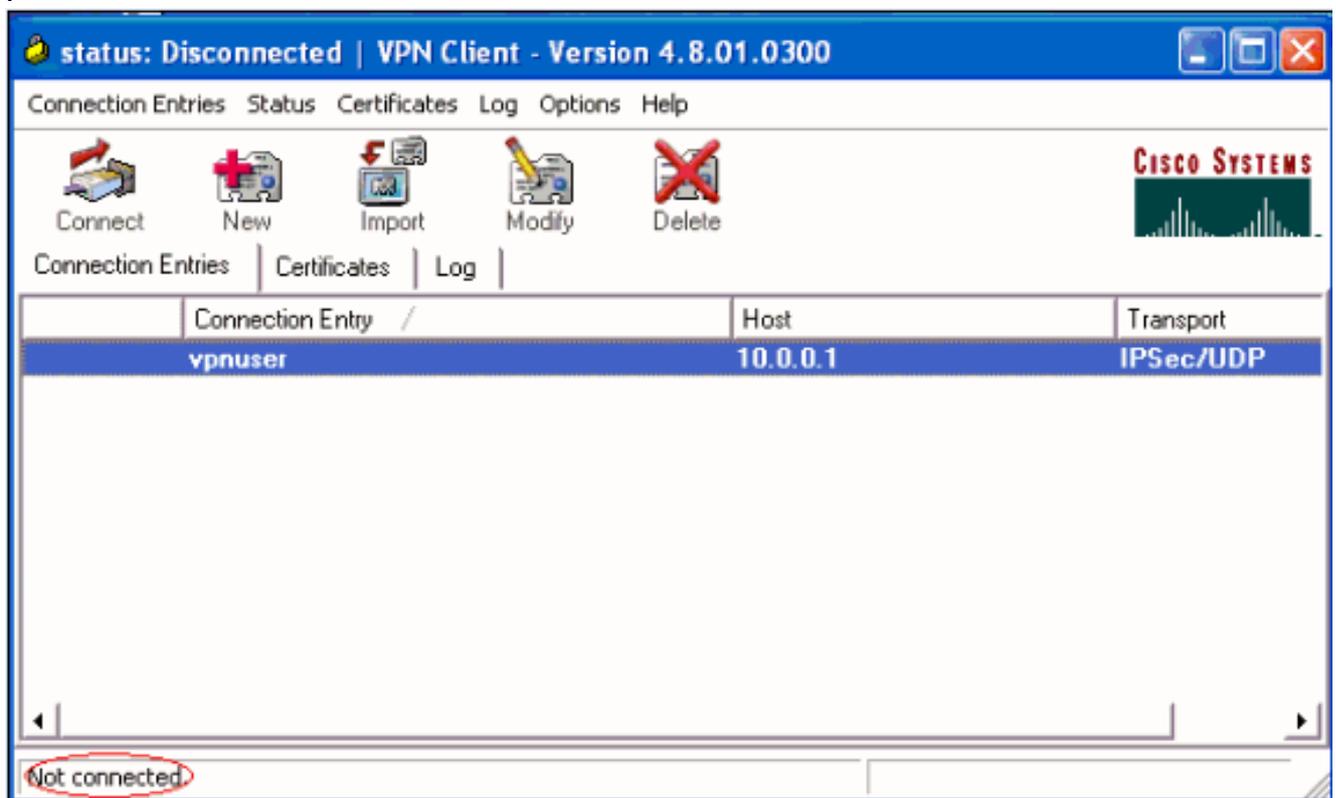
[[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token	Actions
ipsecuser1	10.1.1.9 192.168.1.2	ipsecgroup	IPSec 3DES-168	Oct 27 17:22:14 0:05:11	WinNT 4.8.01.0300	0 8056	N/A	[Logout Ping]

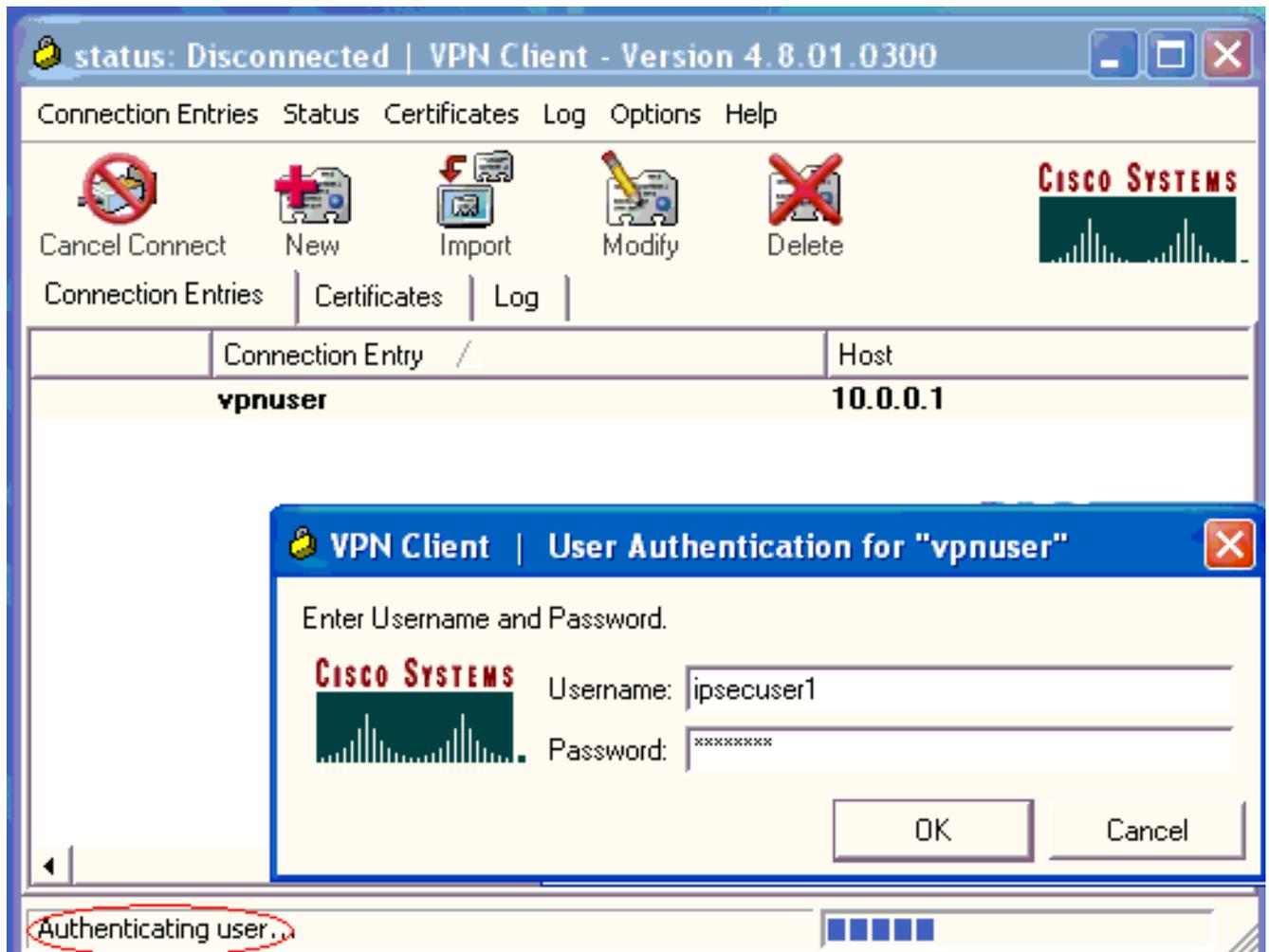
VPN 클라이언트 확인

VPN 클라이언트를 확인하려면 다음 단계를 완료하십시오.

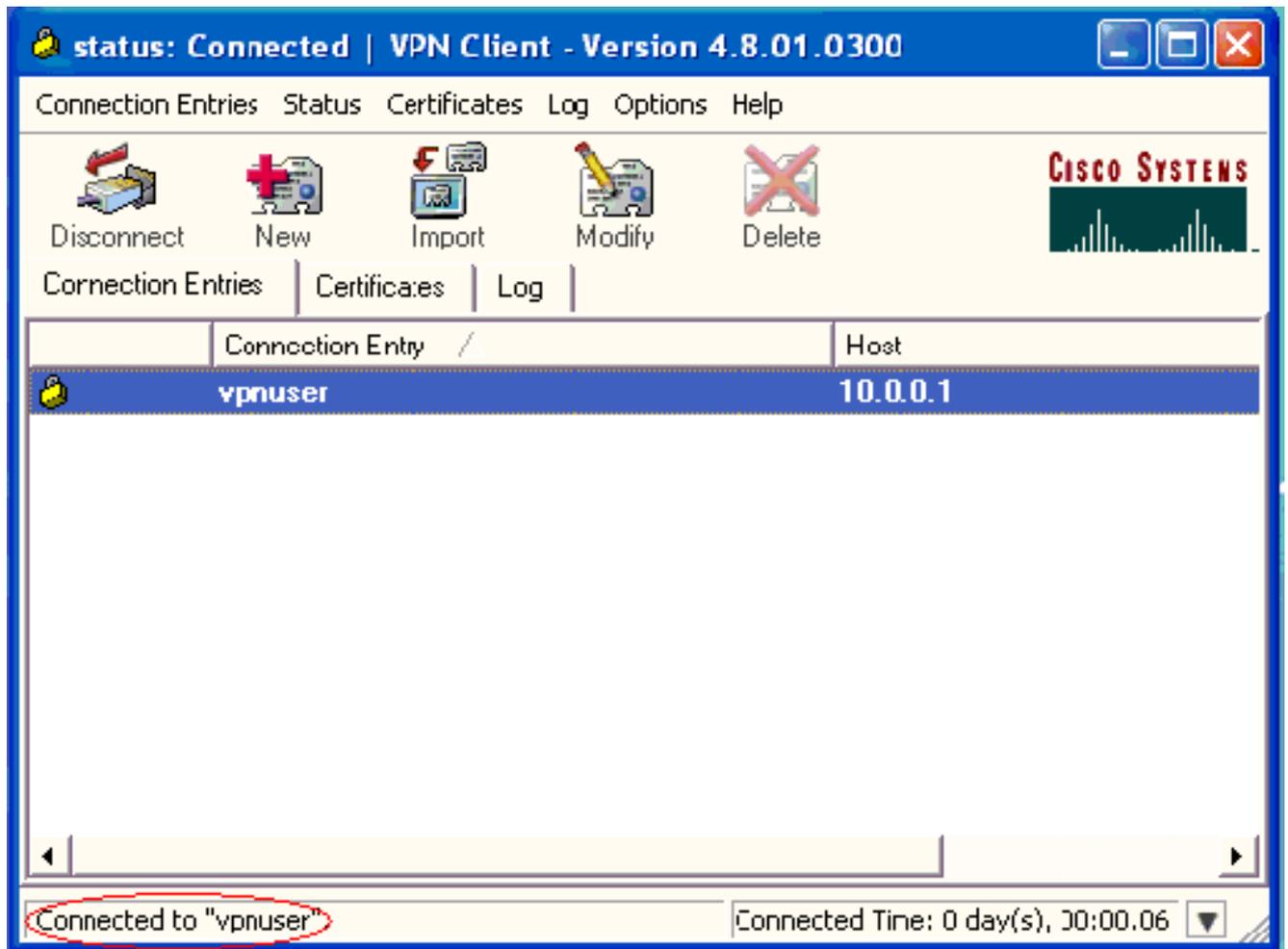
1. VPN 연결을 시작하려면 Connect를 클릭합니다



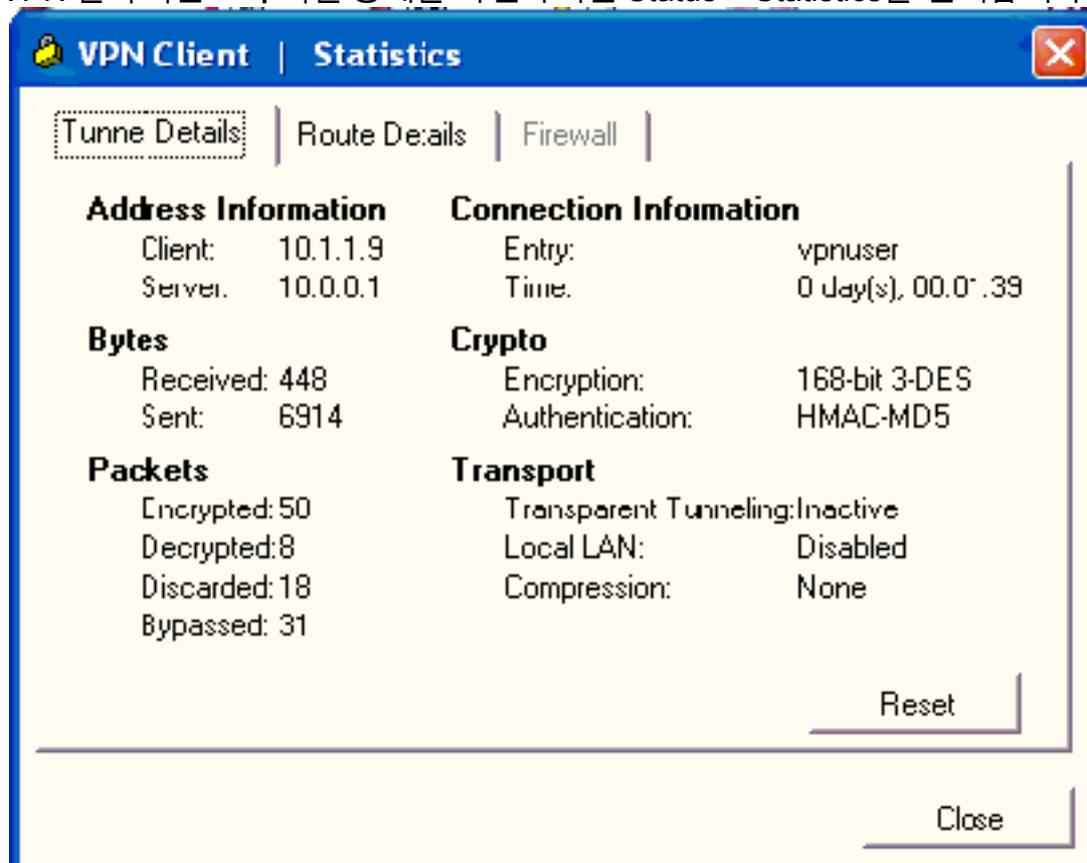
2. 이 창은 사용자 인증을 위해 나타납니다. VPN 연결을 설정하려면 유효한 사용자 이름 및 비밀번호를 입력합니다



3. VPN 클라이언트는 중앙 사이트의 VPN 3000 Concentrator에 연결됩니다



4. VPN 클라이언트의 터널 통계를 확인하려면 Status > Statistics를 선택합니다



문제 해결

컨피그레이션 문제를 해결하려면 다음 단계를 완료하십시오.

1. RADIUS 서버와 VPN 3000 Concentrator 간의 연결을 테스트하려면 Configuration(컨피그레이션) > System(시스템) > Servers(서버) > Authentication(인증)을 선택하고 다음 단계를 완료합니다. 서버를 선택한 다음 테스트를 클릭합니다

Configuration | System | Servers | Authentication

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

You should have a properly configured RADIUS, NT Domain, SDI or Kerberos/Active Direct configure the internal server and [add users to the internal database](#).

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

Authentication Servers	Actions
172.16.124.5 (Radius/User Authentication) Internal (Internal)	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Test"/>

RADIUS 사용자 이름 및 비밀번호를 입력하고 OK(확인)를 클릭합니다

Configuration | System | Servers | Authentication | Test

Enter a username and password with which to test. **Please wait for the operation**

Username

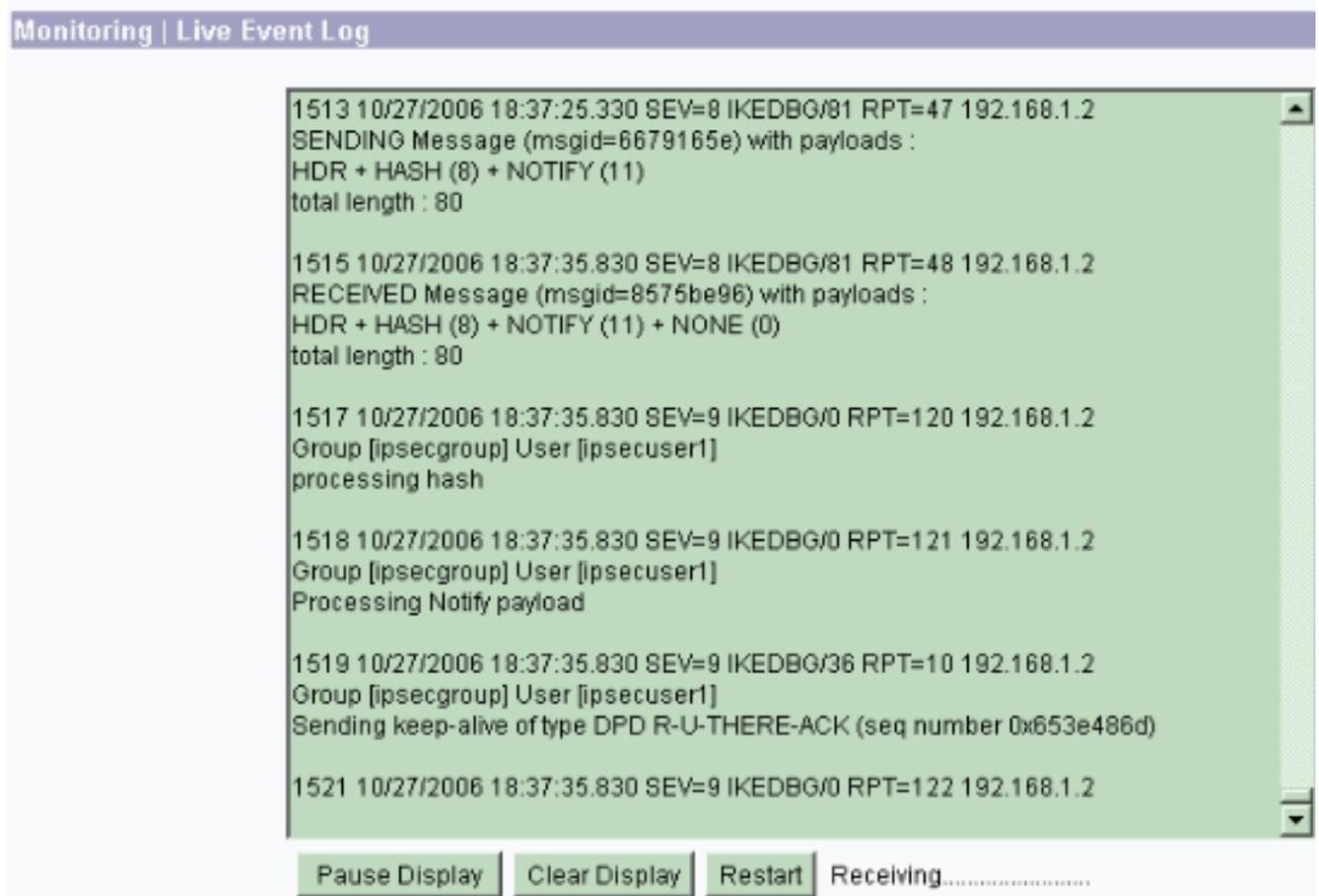
Password

Success

 Authentication Successful

성공적인 인증이 나타납니다.

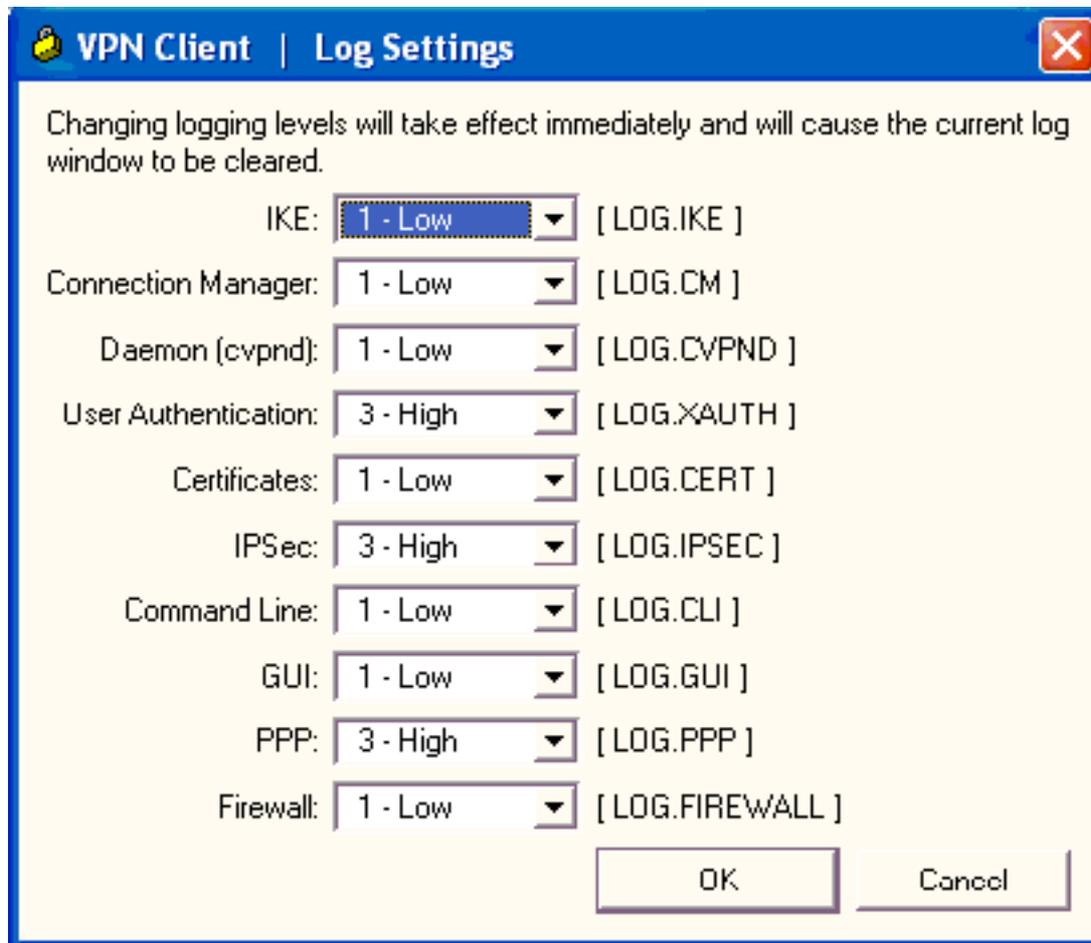
- 장애가 발생하면 구성 문제 또는 IP 연결 문제가 발생합니다. ACS 서버의 Failed Attempts Log에서 실패와 관련된 메시지를 확인합니다. 이 로그에 메시지가 표시되지 않으면 IP 연결 문제가 발생할 수 있습니다. RADIUS 요청이 RADIUS 서버에 도달하지 않습니다. 적절한 VPN 3000 Concentrator 인터페이스에 적용된 필터가 RADIUS(1645) 패킷 수신 및 발신을 허용하는지 확인합니다. 테스트 인증이 성공했지만 VPN 3000 Concentrator에 대한 로그인이 계속 실패하면 콘솔 포트를 통해 Filterable Event Log(필터링 가능한 이벤트 로그)를 확인합니다. 연결이 작동하지 않을 경우 Configuration(구성) > System(시스템) > Events(이벤트) > Classes(클래스) > Modify(Severity to Log(로그에 심각도=1-9, 콘솔에 심각도=1-3))를 선택하면 VPN Concentrator에 AUTH, IKE 및 IPsec 이벤트 클래스를 추가할 수 있습니다. AUTHDBG, AUTHDECODE, IKEDBG, KEDECODE, IPSECDBG 및 IPSECDECODE도 사용할 수 있지만 너무 많은 정보를 제공할 수 있습니다. RADIUS 서버에서 전달되는 특성에 대한 자세한 정보가 필요한 경우 AUTHDECODE, KEDECODE 및 IPSECDECODE는 Severity to Log=1-13 수준에서 이를 제공합니다.
- Monitoring(모니터링) > Event Log(이벤트 로그)에서 이벤트 로그를 검색합니다



[Windows용 VPN 클라이언트 4.8 문제 해결](#)

Windows용 VPN 클라이언트 4.8의 문제를 해결하려면 다음 단계를 완료하십시오.

- VPN 클라이언트에서 로그 레벨을 활성화하려면 Log(로그) > Log(로그) 설정을 선택합니다



2. VPN 클라이언트의 로그 항목을 보려면 Log(로그) > Log Window(로그 창)를 선택합니다

Cisco Systems VPN Client Version 4.8.01.0300
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
Config file directory: C:\Program Files\Cisco Systems\VPN Client

1 13:26:29.234 10/31/06 Sev=Warning/2 IKE/0xA3000067
Received an IPC message during invalid state (IKE_MAIN:507)

2 13:26:36.109 10/31/06 Sev=Warning/2 CVPND/0xE3400013
AddRoute failed to add a route: code 87
Destination 192.168.1.255
Netmask 255.255.255.255
Gateway 10.1.1.9
Interface 10.1.1.9

3 13:26:36.109 10/31/06 Sev=Warning/2 CM/0xA3100024
Unable to add route. Network: c0a801ff, Netmask: ffffffff, Interface: a010109, Gateway: a010109

Cisco Systems VPN Client Version 4.8.01.0300
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
Config file directory: C:\Program Files\Cisco Systems\VPN Client

1 13:27:31.640 10/31/06 Sev=Info/4IPSEC/0x63700019
Activate outbound key with SPI=0x2c9afd45 for inbound key with SPI=0xc9c1b7d5

2 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x63700013
Delete internal key with SPI=0xc9c1b7d5

3 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x6370000C
Key deleted by SPI 0xc9c1b7d5

4 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x63700013
Delete internal key with SPI=0x2c9afd45

5 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x6370000C
Key deleted by SPI 0x2c9afd45

[관련 정보](#)

- [Cisco VPN 3000 Series Concentrator 지원 페이지](#)
- [Cisco VPN 클라이언트 지원 페이지](#)
- [IPSec 협상/IKE 프로토콜](#)
- [Cisco Secure ACS for Windows 지원 페이지](#)
- [RADIUS 서버에서 동적 필터 구성](#)
- [기술 지원 및 문서 - Cisco Systems](#)