디지털 인증서를 사용하는 Windows 2000과 VPN 3000 Concentrator 사이의 L2TP Over IPsec 컨피그레이션 예

목차

소개

이 문서에서는 L2TP/IPSec 내장 클라이언트를 사용하여 Windows 2000 클라이언트에서 VPN 3000 Concentrator에 연결하는 데 사용되는 단계별 절차를 보여줍니다. VPN Concentrator에 대한 연결을 인증하는 데 CEP(Certificate Enrollment Protocol) 없이 디지털 인증서(독립형 루트 CA)를 사용하는 것으로 가정합니다. 이 문서에서는 설명을 위해 Microsoft 인증서 서비스를 사용합니다. Microsoft 웹 사이트에서 구성 방법에 대한 설명서를 참조하십시오.

참고: Windows 2000 화면의 모양이 변경될 수 있기 때문에 이는 예입니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco VPN 3000 Concentrator 시리즈에 대한 것입니다.

목표

이 절차에서 다음 단계를 완료합니다.

1. 루트 인증서를 가져옵니다.
2. 클라이언트에 대한 ID 인증서를 가져옵니다.
3. 네트워크 연결 마법사의 도움으로 VPN 3000에 대한 연결을 생성합니다.
4. VPN 3000 Concentrator를 구성합니다.

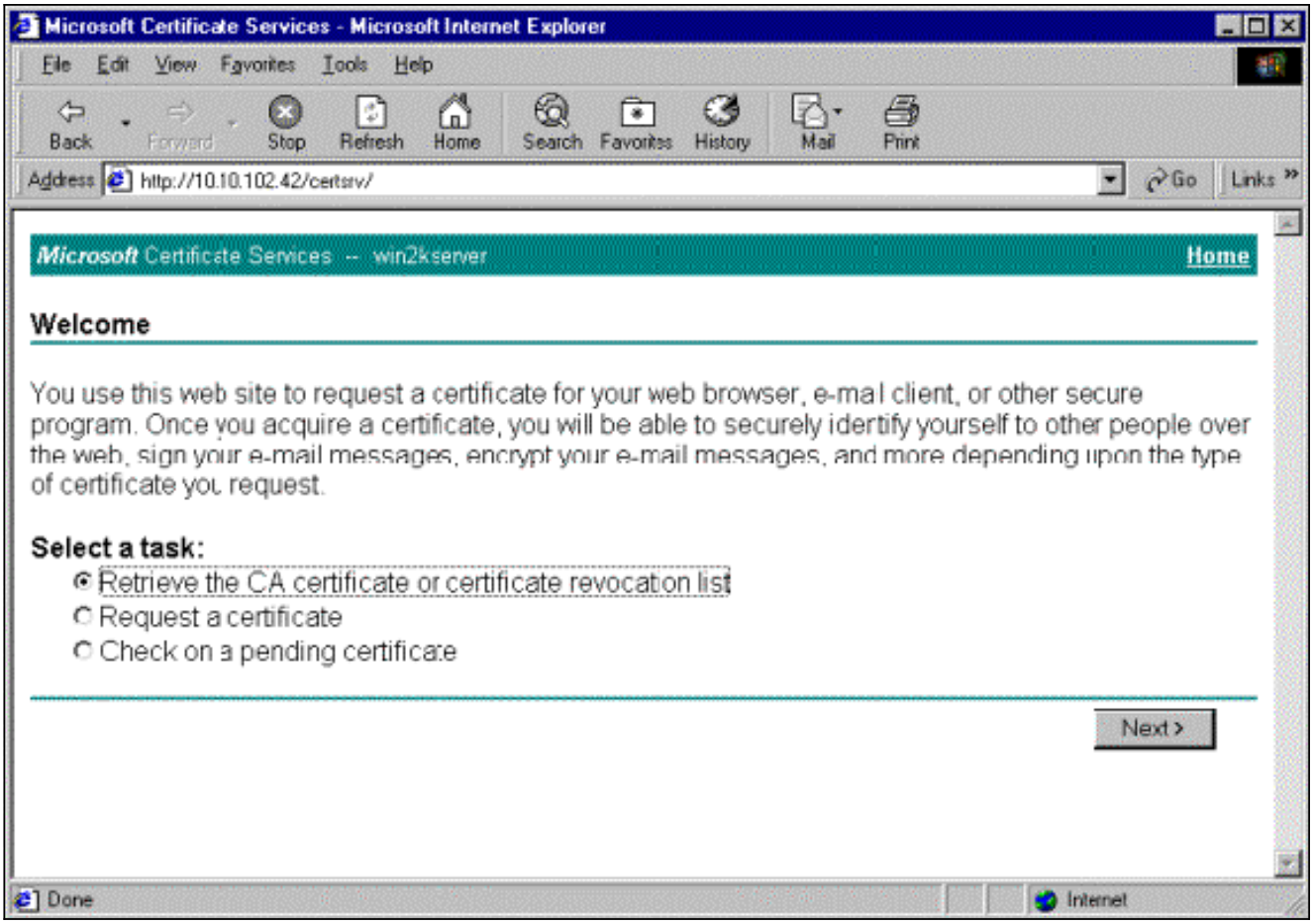
표기 규칙

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

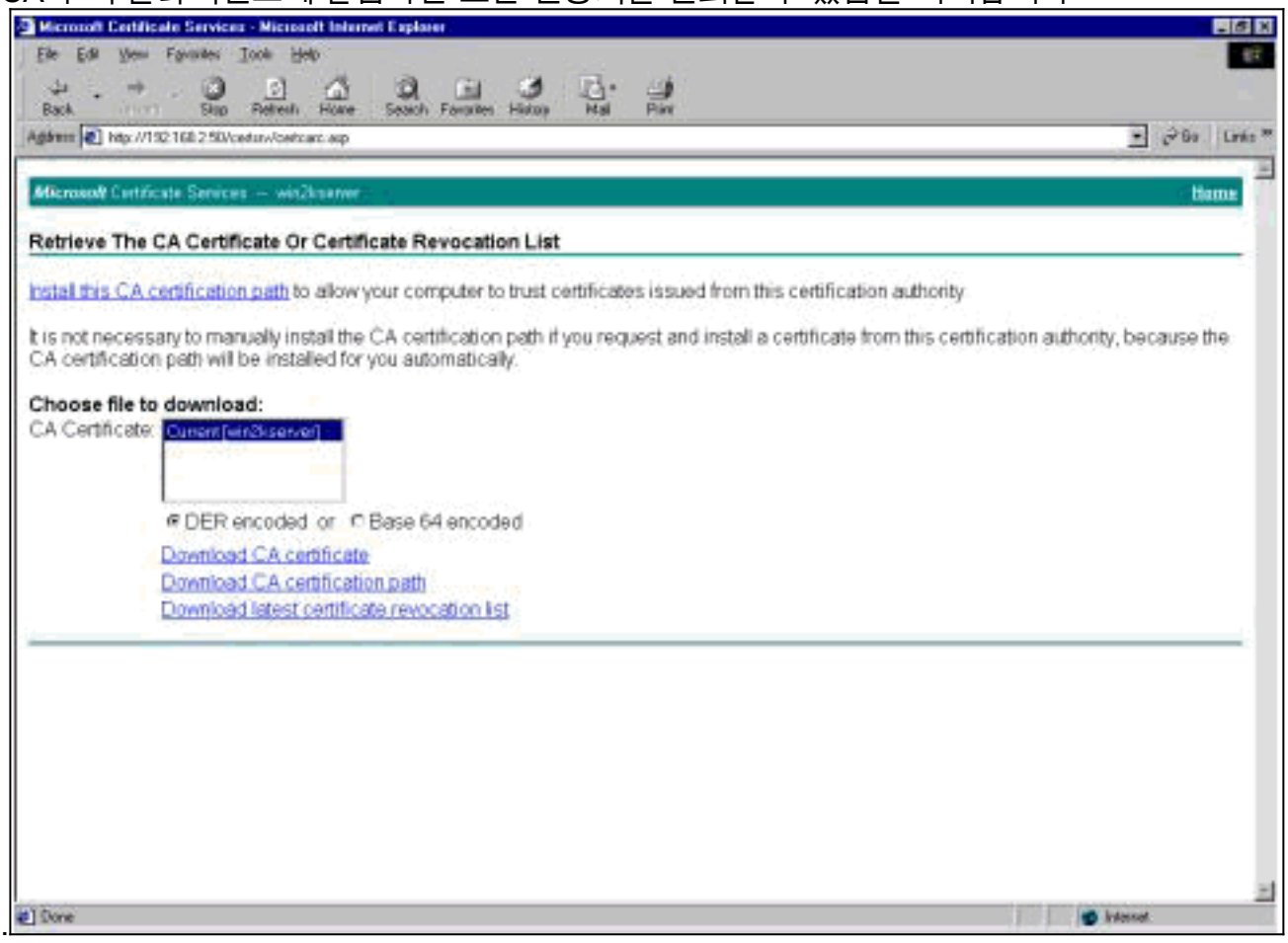
루트 인증서 얻기

루트 인증서를 가져오려면 다음 지침을 완료합니다.

1. 브라우저 창을 열고 Microsoft Certificate Authority의 URL(일반적으로 http://servername 또는 CA/certsrv의 IP 주소)을 입력합니다.인증서 검색 및 요청을 위한 시작 창이 표시됩니다.
2. Welcome(시작) 창의 Select a task(작업 선택)에서 Retrieve the **CA certificate or certificate revocation list(CA 인증서 또는 인증서 해지 목록 검색)를** 선택하고 **Next(다음)**를 클릭합니다 .



3. Retrieve the CA certificate or certificate revocation list(CA 인증서 또는 인증서 해지 목록 검색) 창에서 왼쪽 **모서리**에 있는 **Install this CA certification path(이 CA 인증 경로 설치)**를 클릭합니다.이렇게 하면 CA 인증서가 신뢰할 수 있는 루트 인증 기관 저장소에 추가됩니다. 이는 이 CA가 이 클라이언트에 발급하는 모든 인증서를 신뢰할 수 있음을 의미합니다

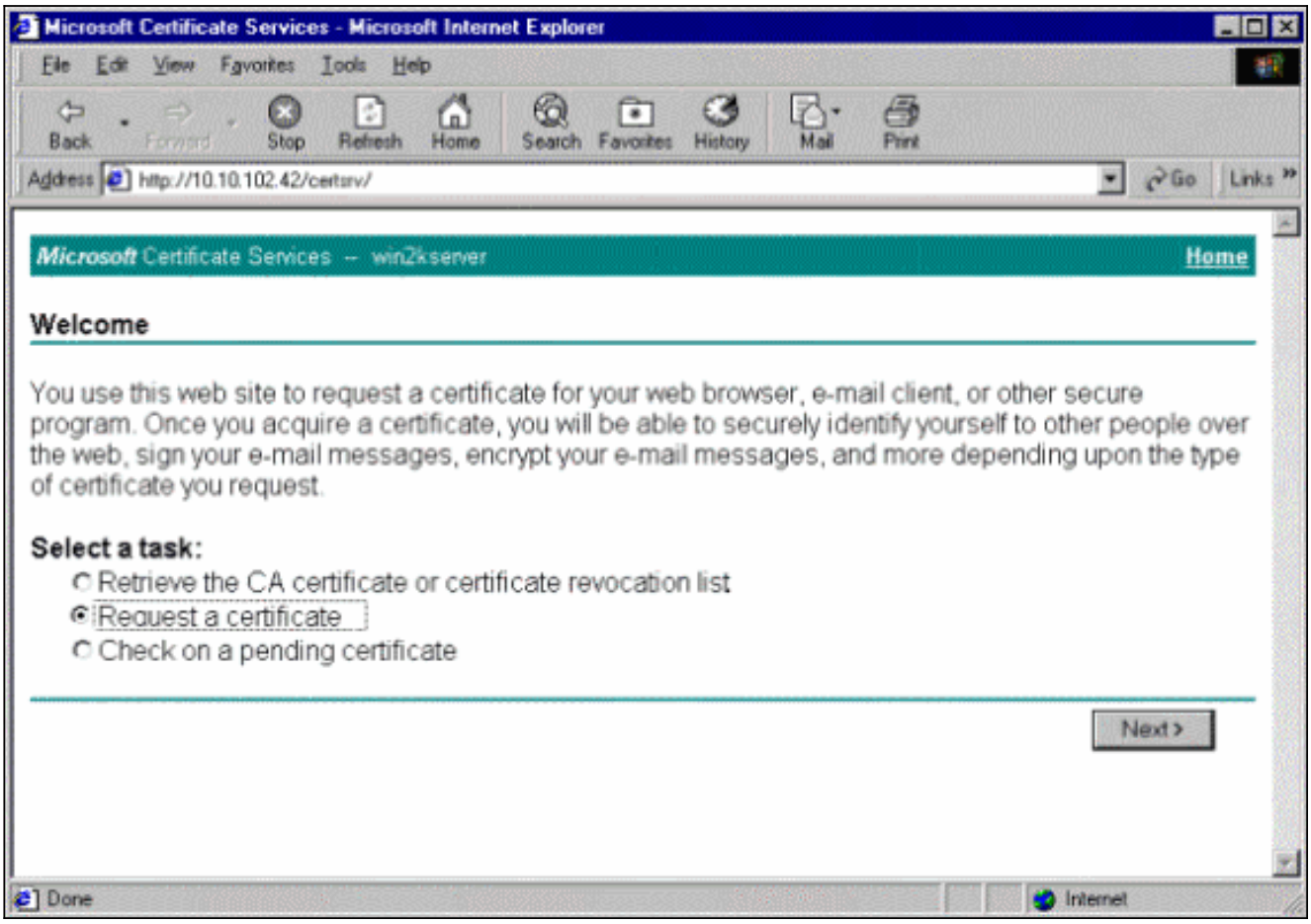


클라이언트에 대한 ID 인증서 얻기

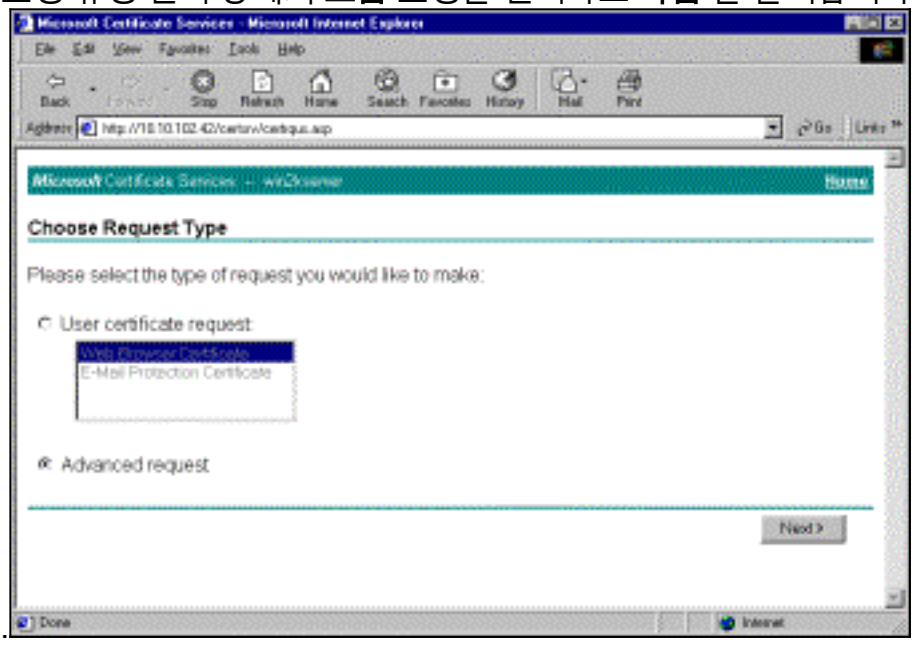
클라이언트에 대한 ID 인증서를 가져오려면 다음 단계를 완료합니다.

1. 브라우저 창을 열고 Microsoft Certificate Authority의 URL(일반적으로 http://servername 또는 CA/certsrv의 IP 주소)을 입력합니다.인증서 검색 및 요청을 위한 시작 창이 표시됩니다.
2. 시작 창의 작업 선택에서 **인증서** 요청을 선택하고 **다음** 을 클릭합니다

.

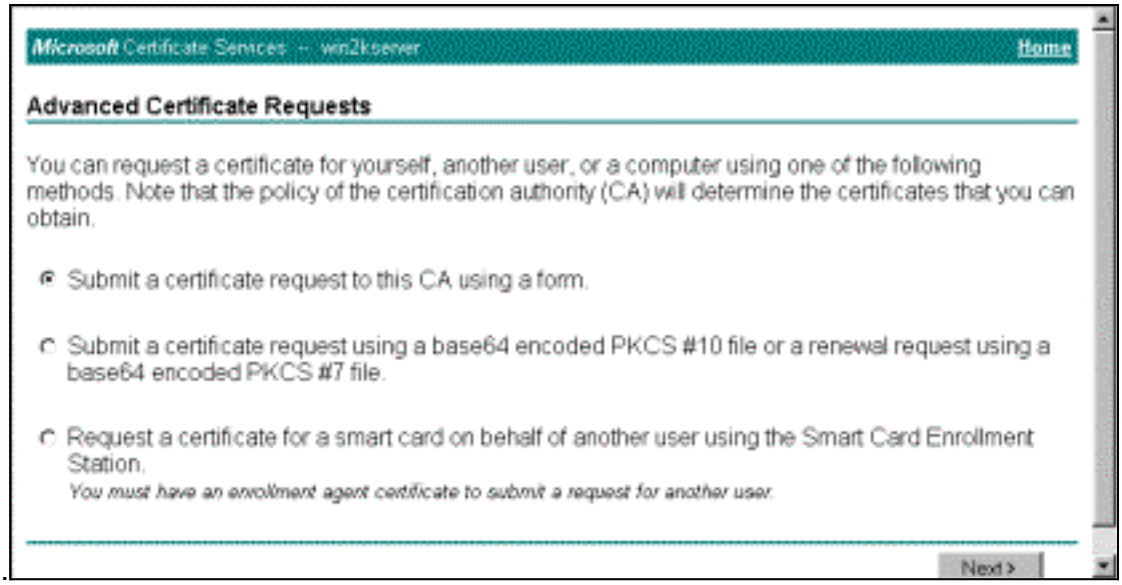


3. 요청 유형 선택 창에서 **고급** 요청을 선택하고 **다음** 을 클릭합니다

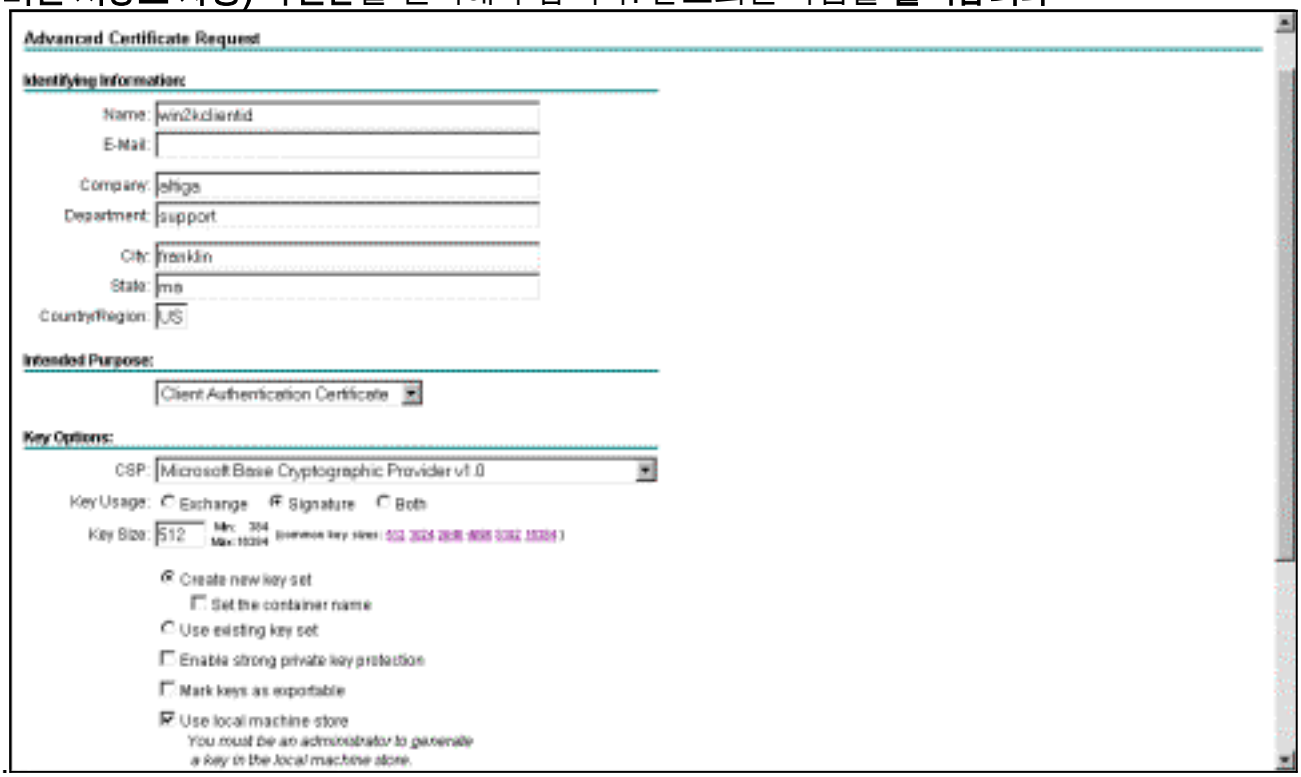


.

4. Advanced Certificate Requests(고급 인증서 요청) 창에서 **Submit a certificate request to this CA using a form(양식을 사용하여 이 CA에 인증서 요청 제출)을** 선택합니다

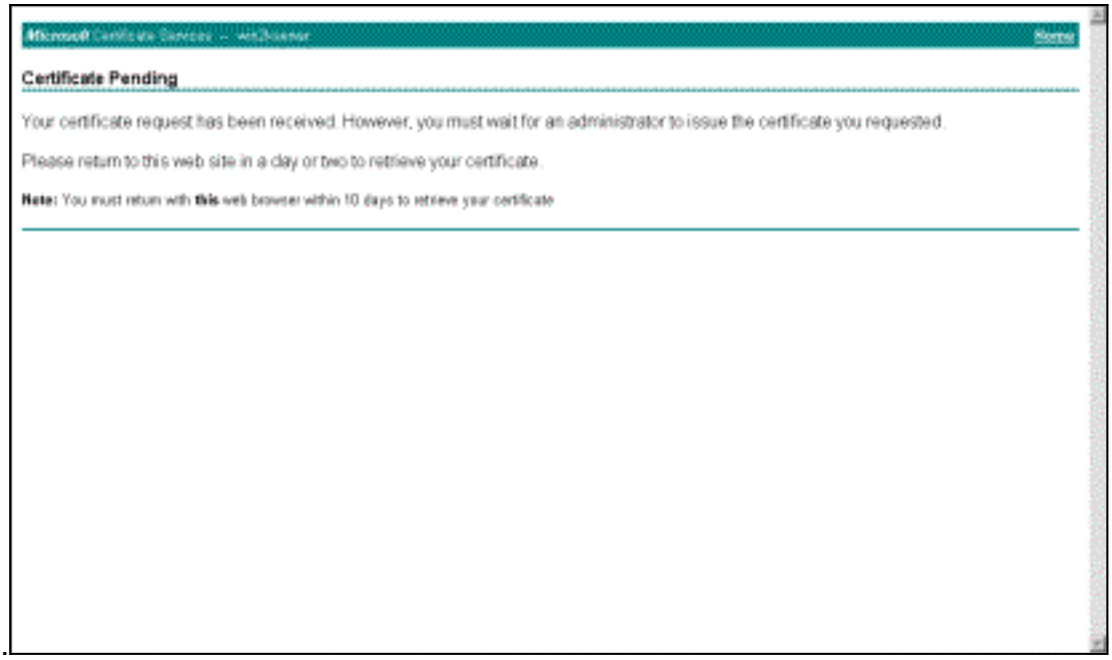


5. 이 예제와 같이 필드를 채웁니다.부서(조직 단위)의 값은 VPN Concentrator에 구성된 그룹과 일치해야 합니다. 1024보다 큰 키 크기를 지정하지 마십시오. **Use local machine store(로컬 머신 저장소 사용) 확인란**을 선택해야 합니다. 완료되면 다음을 **클릭합니다**

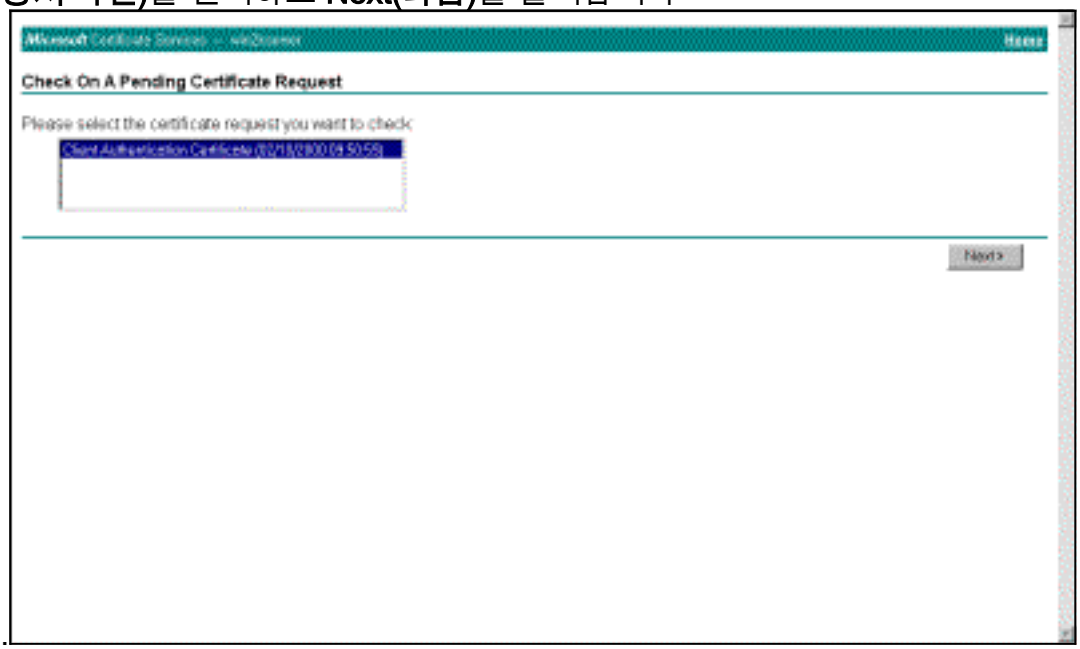


CA 서버가 구성된 방식에 따라 이 창이 가끔 나타납니다. 그럴 경우 CA 관리자에게 문의하십

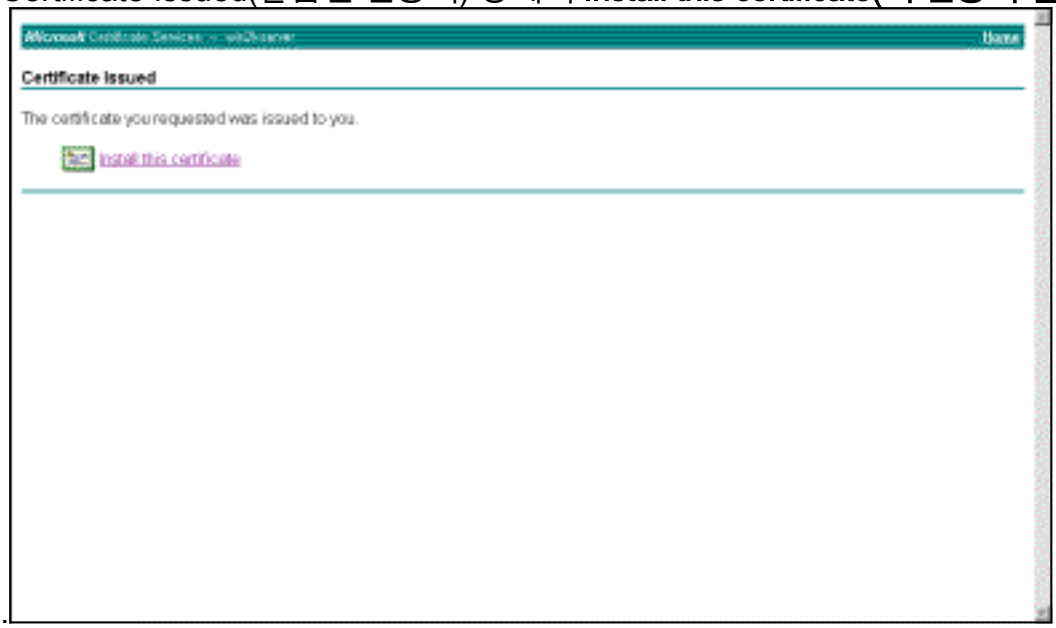
시오.



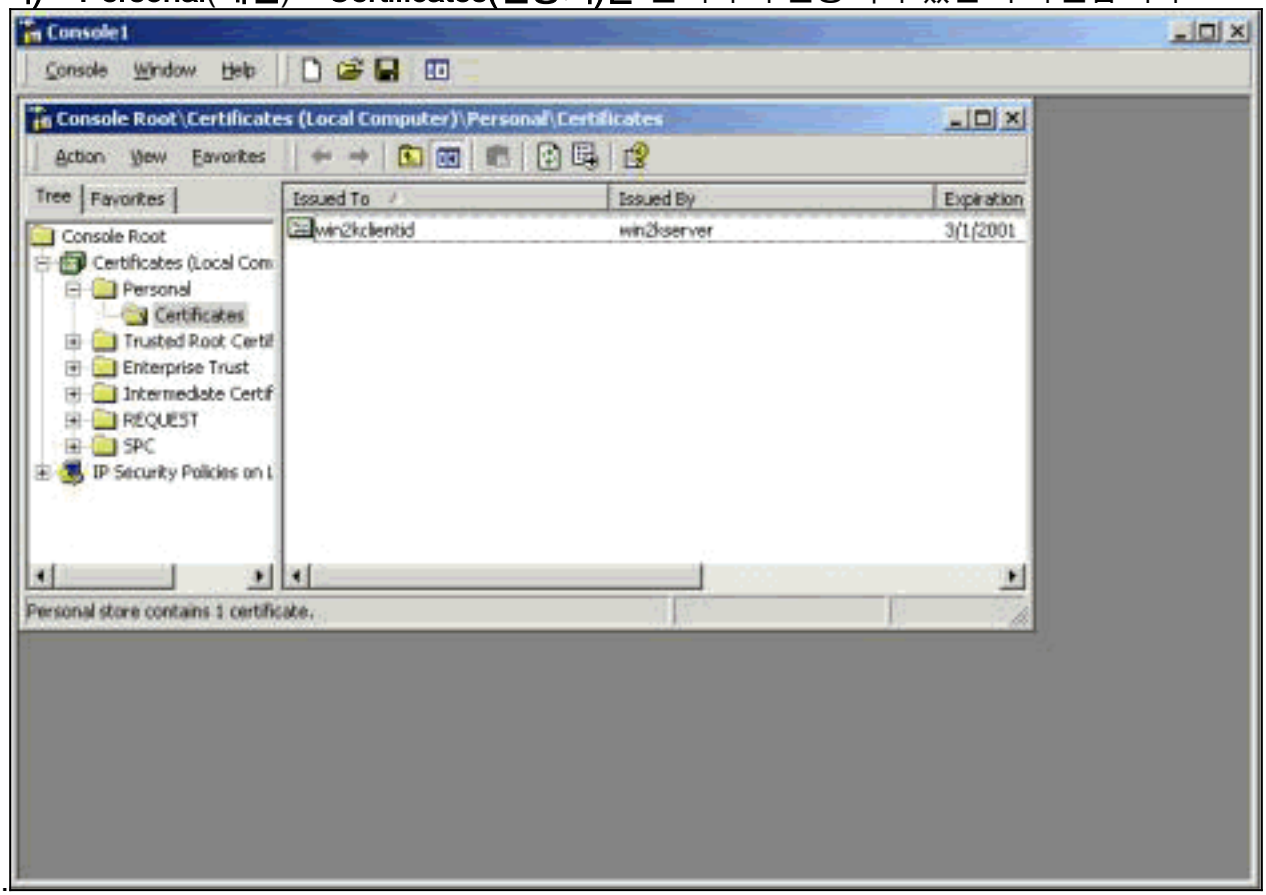
6. Home(**홈**)을 클릭하여 기본 화면으로 돌아간 다음 **Check on pending certificate(보류 중인 인증서 확인)**를 선택하고 **Next(다음)**를 클릭합니다



7. Certificate Issued(발급된 인증서) 창에서 **Install this certificate(이 인증서 설치)**를 클릭합니다



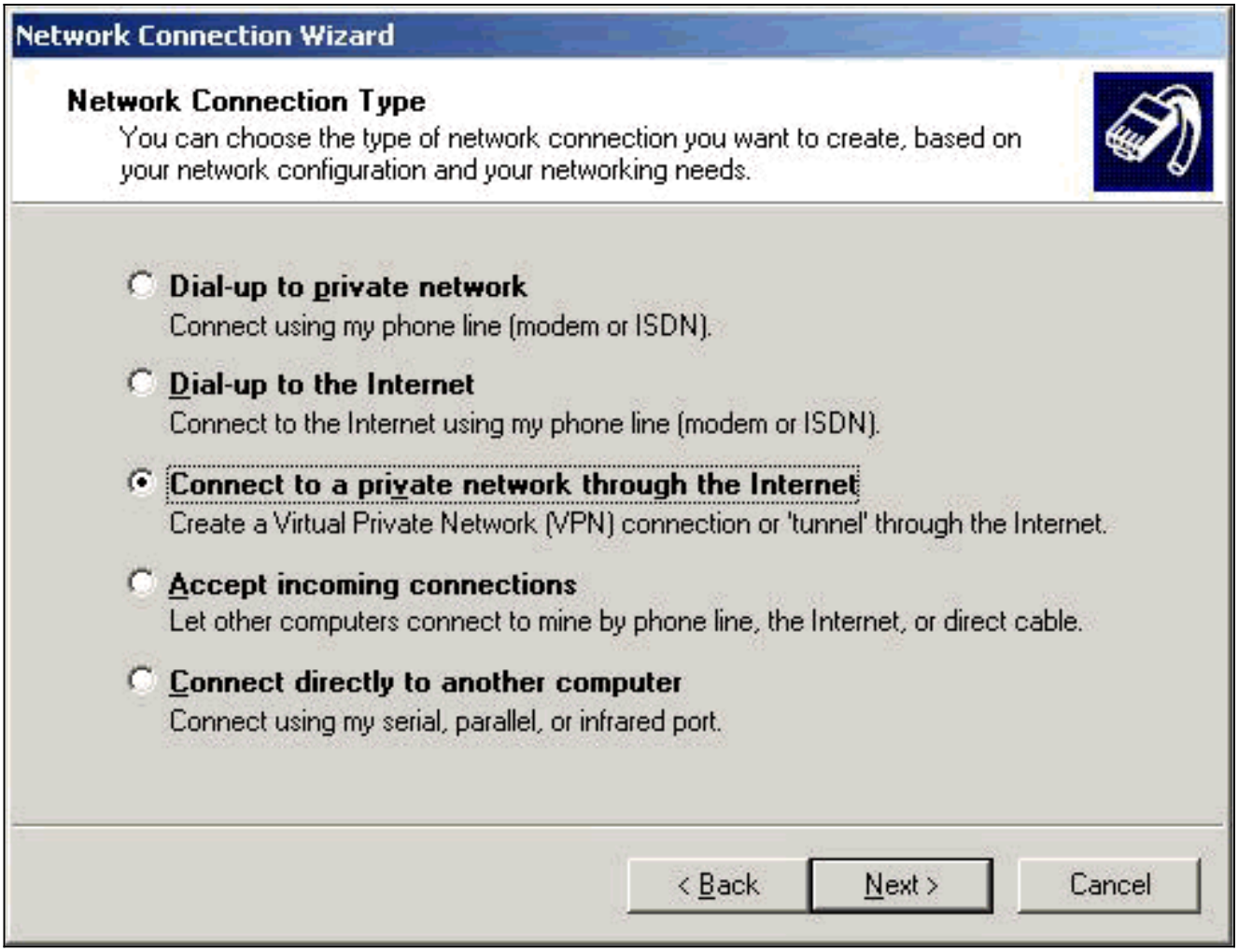
8. 클라이언트 인증서를 보려면 **시작 > 실행**을 선택하고 MMC(Microsoft Management Console)를 수행합니다.
9. Console(**콘솔**)을 클릭하고 **Add/Remove Snap-in(스냅인 추가/제거)을** 선택합니다.
10. Add(**추가**)를 클릭하고 **목록**에서 Certificate(인증서)를 선택합니다.
11. 인증서의 범위를 묻는 창이 나타나면 컴퓨터 계정을 **선택합니다**.
12. CA 서버의 인증서가 신뢰할 수 있는 루트 인증 기관 아래에 있는지 확인합니다. 또한 이 이미지에 표시된 대로 **Console Root(콘솔 루트)** > Certificate **(Local Computer)(인증서(로컬 컴퓨터) > Personal(개인) > Certificates(인증서)를** 선택하여 인증서가 있는지 확인합니다



네트워크 연결 마법사를 사용하여 VPN 3000에 대한 연결 만들기

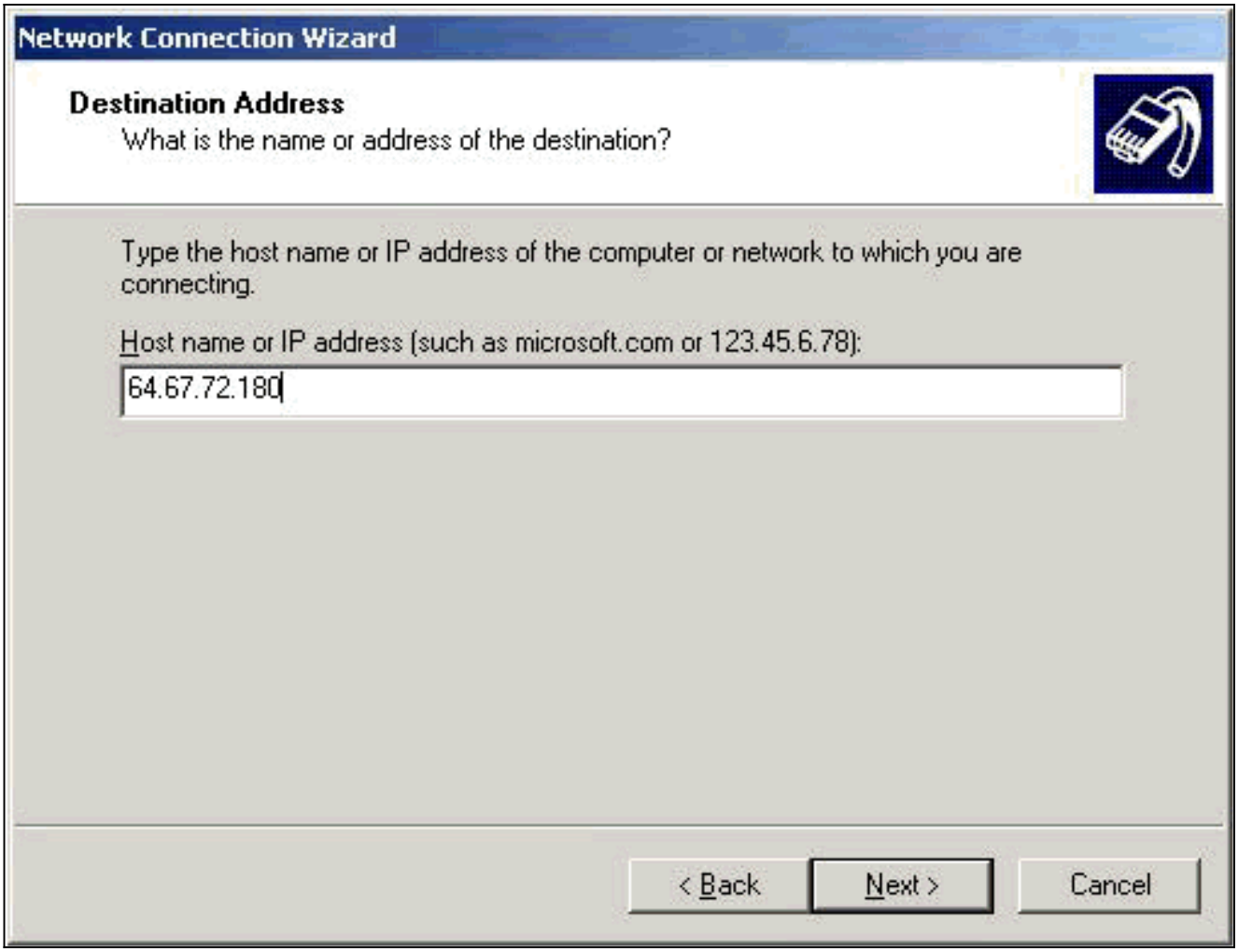
네트워크 연결 마법사의 도움으로 VPN 3000에 대한 연결을 생성하려면 다음 절차를 수행합니다.

1. **내 네트워크 환경**을 마우스 오른쪽 **버튼**으로 클릭하고 속성을 선택한 **다음 새 연결 만들기**를 클릭합니다.
2. Network Connection Type(네트워크 연결 유형) 창에서 **Connect to a private network through the Internet(인터넷을 통해 사설 네트워크에 연결)을** 선택한 다음 **Next(다음)**를 클릭합니다
.



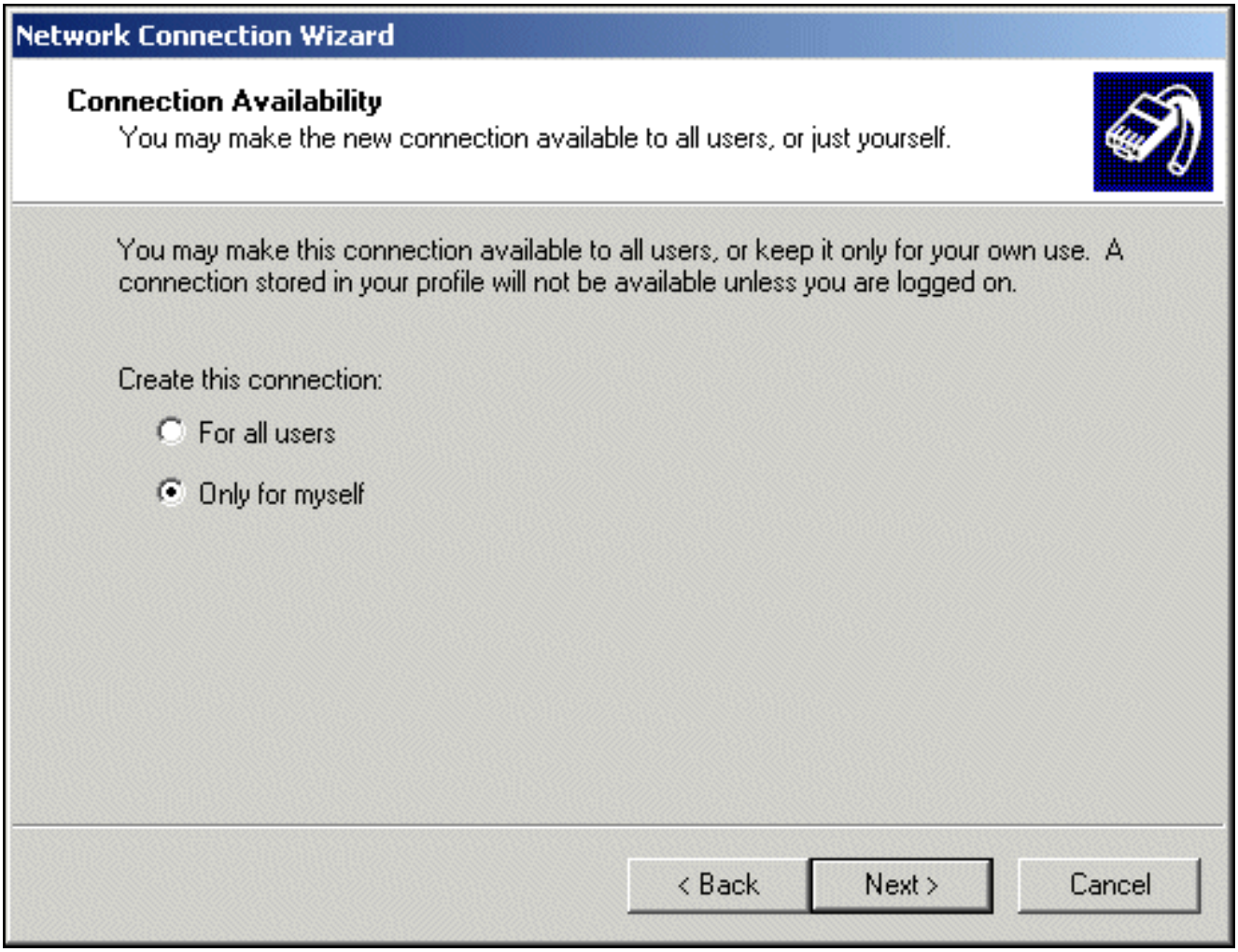
3. VPN Concentrator의 공용 인터페이스의 호스트 이름 또는 IP 주소를 입력하고 Next(**다음**)를 클릭합니다

.



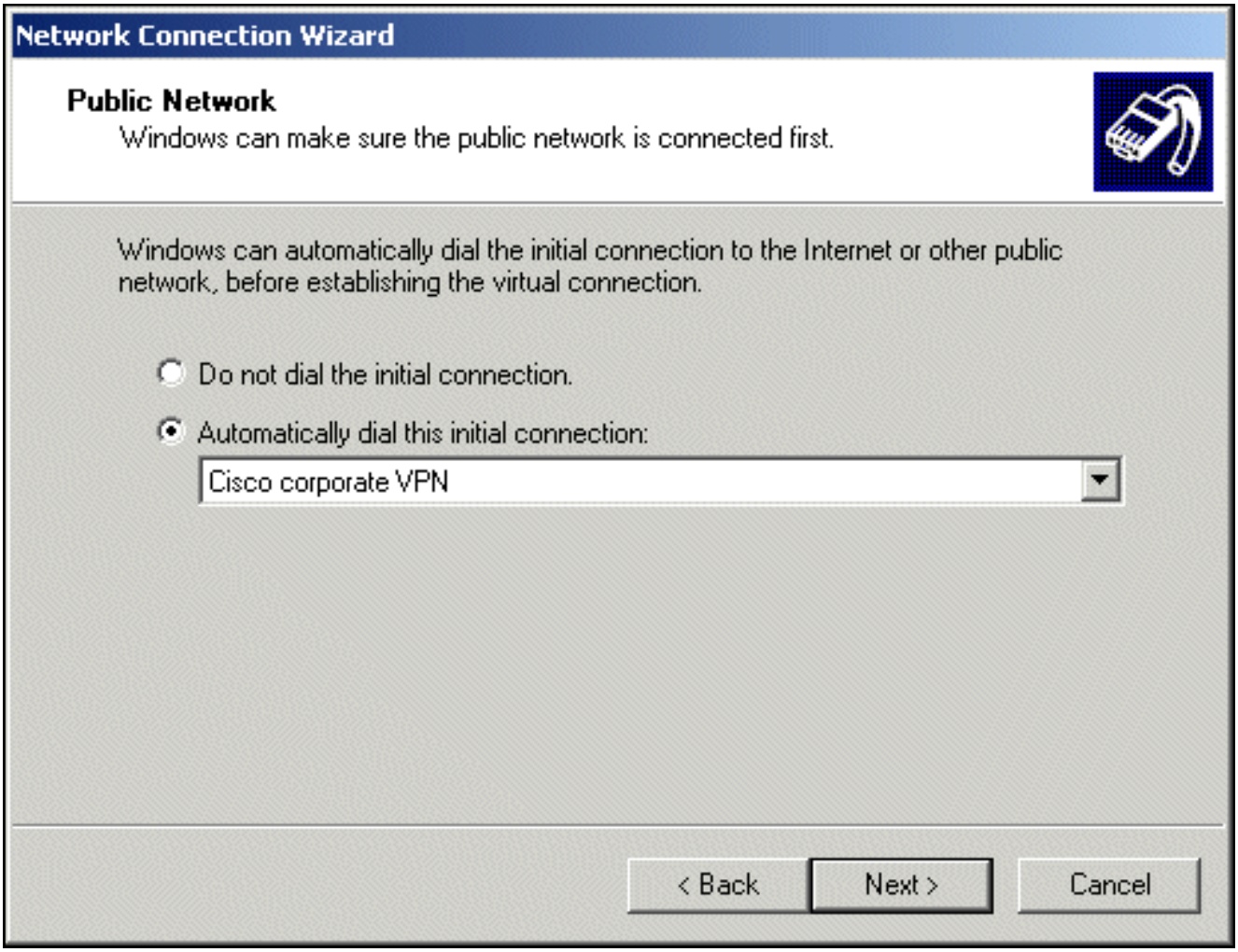
4. Connection Availability(연결 가용성) 창에서 **Only for myself(자신만)**를 선택하고 **Next(다음)**를 클릭합니다

.



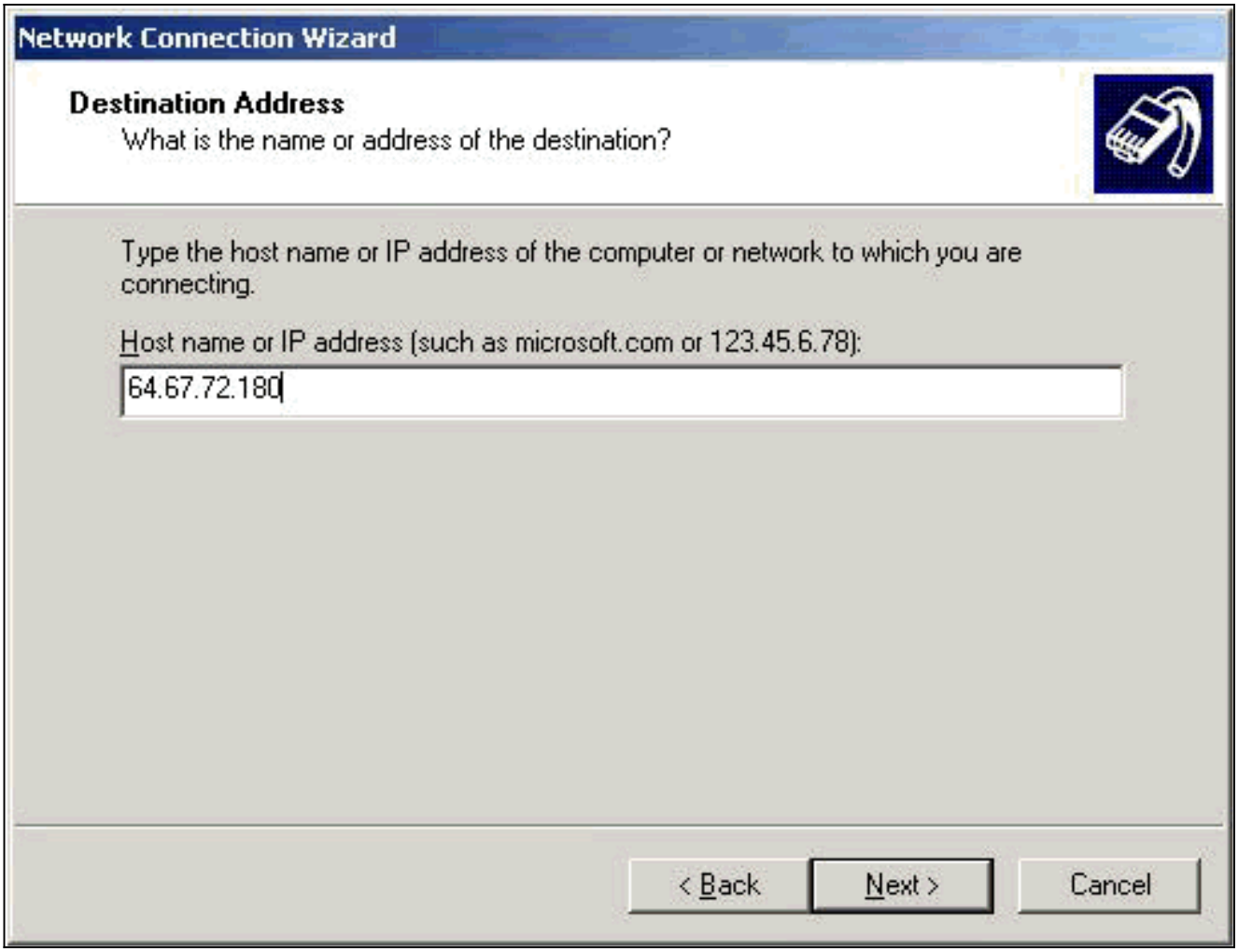
5. Public Network(공용 네트워크) 창에서 초기 연결(ISP 계정)을 자동으로 다이얼할지 여부를 선택합니다

.



6. Destination Address(대상 주소) 화면에서 VPN 3000 Concentrator의 호스트 이름 또는 IP 주소를 입력하고 Next(**다음**)를 클릭합니다

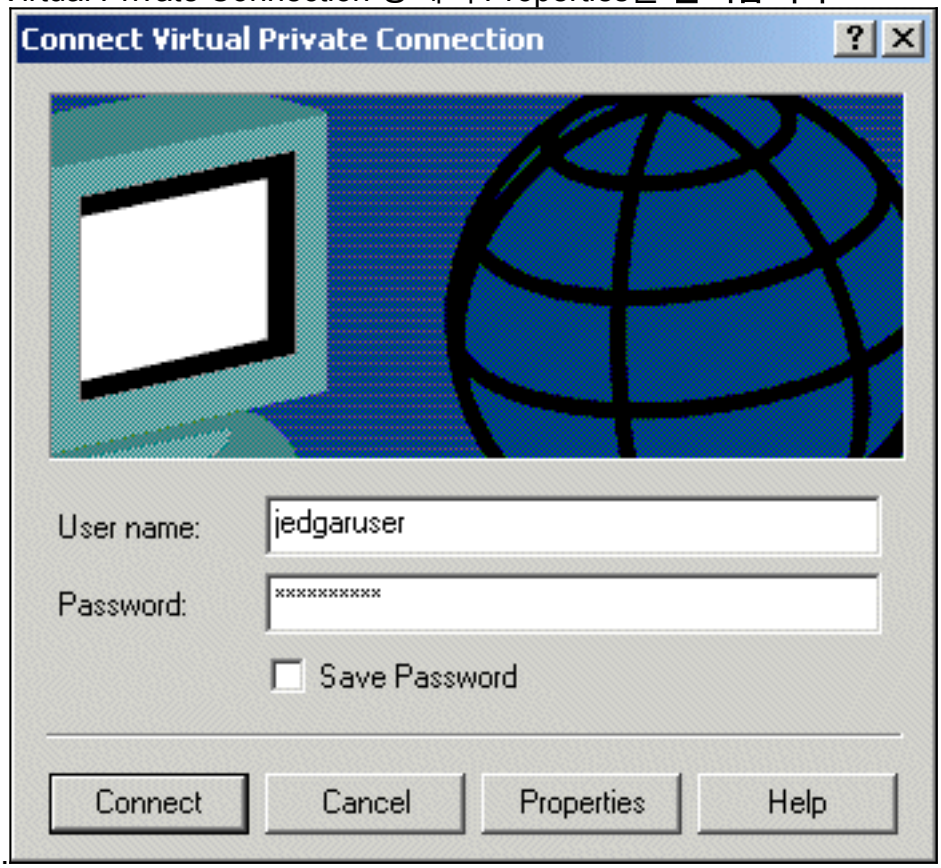
.



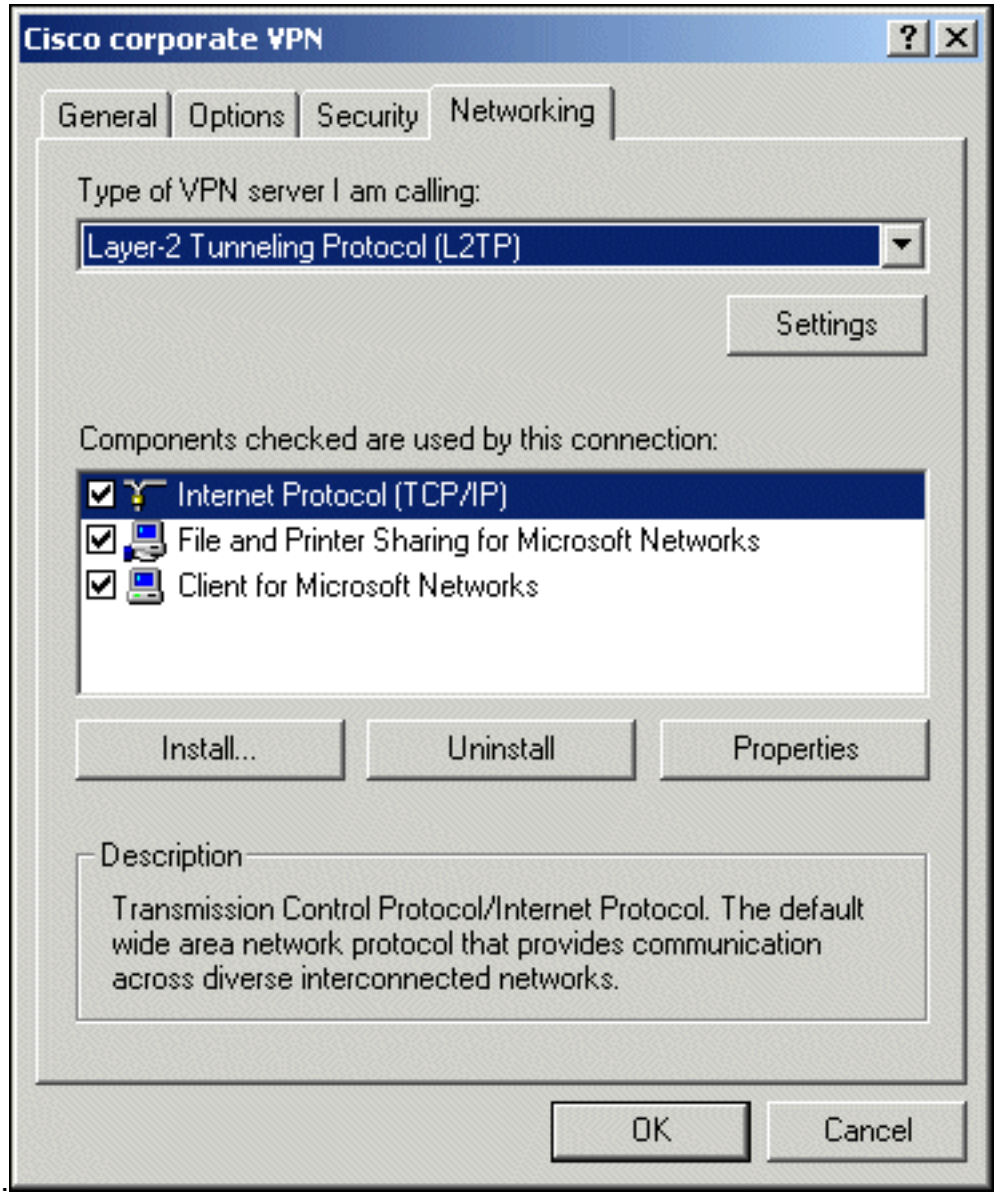
7. 네트워크 연결 마법사 창에서 연결 이름을 입력하고 마침을 **클릭합니다**.이 예에서 연결 이름은 "Cisco 기업 VPN"입니다

.

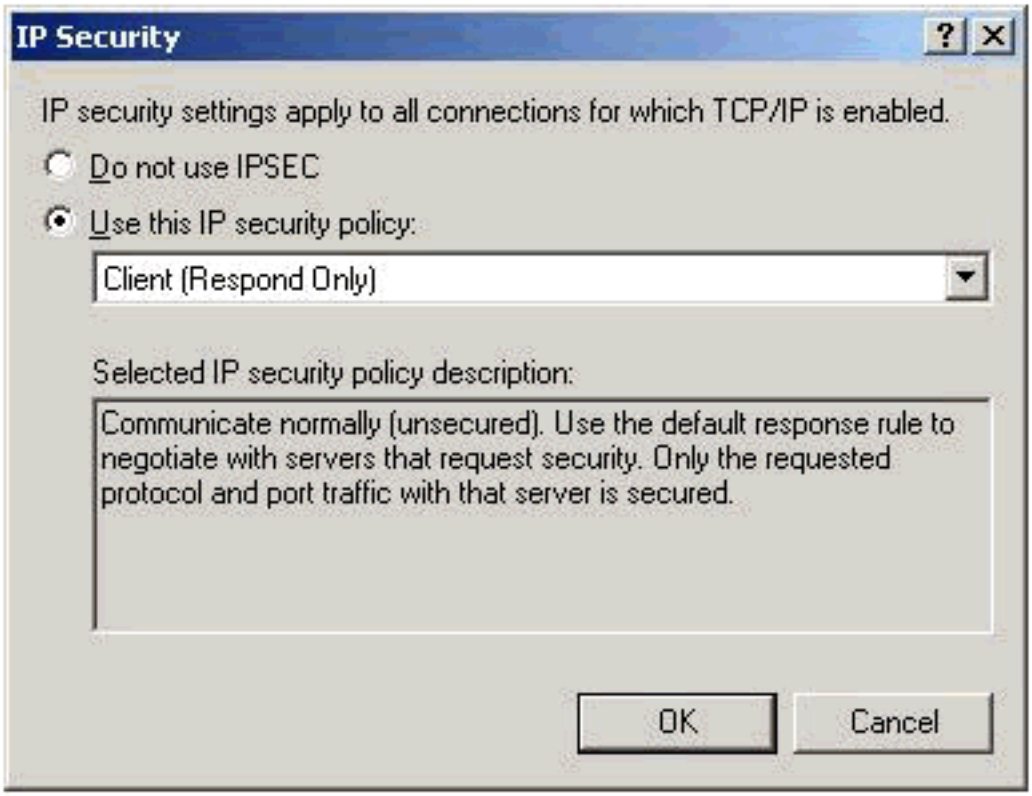
8. Virtual Private Connection 창에서 Properties를 **클릭합니다**



9. Properties(속성) 창에서 Networking(네트워킹) 탭을 선택합니다.
10. Type of VPN server I am calling(호출하는 VPN 서버 유형)의 풀다운 메뉴에서 **L2TP**를 선택하고 **Internet Protocol TCP/IP**를 강조 표시한 다음 Properties(**속성)를** 클릭합니다



11. **[고급] > [옵션] > [속성]을 선택합니다**.
12. IP Security(IP 보안) 창에서 **Use this IP security policy(이 IP 보안 정책 사용)를** 선택합니다



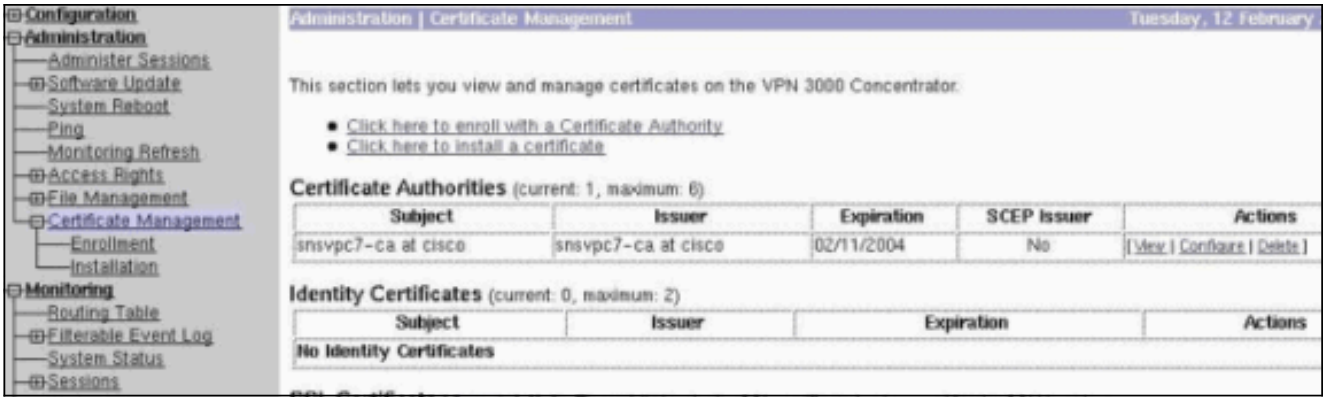
13. 풀다운 메뉴에서 **클라이언트(응답만) 정책**을 선택하고 연결 화면으로 돌아갈 때까지 **확인**을 여러 번 클릭합니다.
14. 연결을 시작하려면 사용자 이름과 암호를 입력하고 연결을 **클릭합니다**.

VPN 3000 Concentrator 구성

루트 인증서 얻기

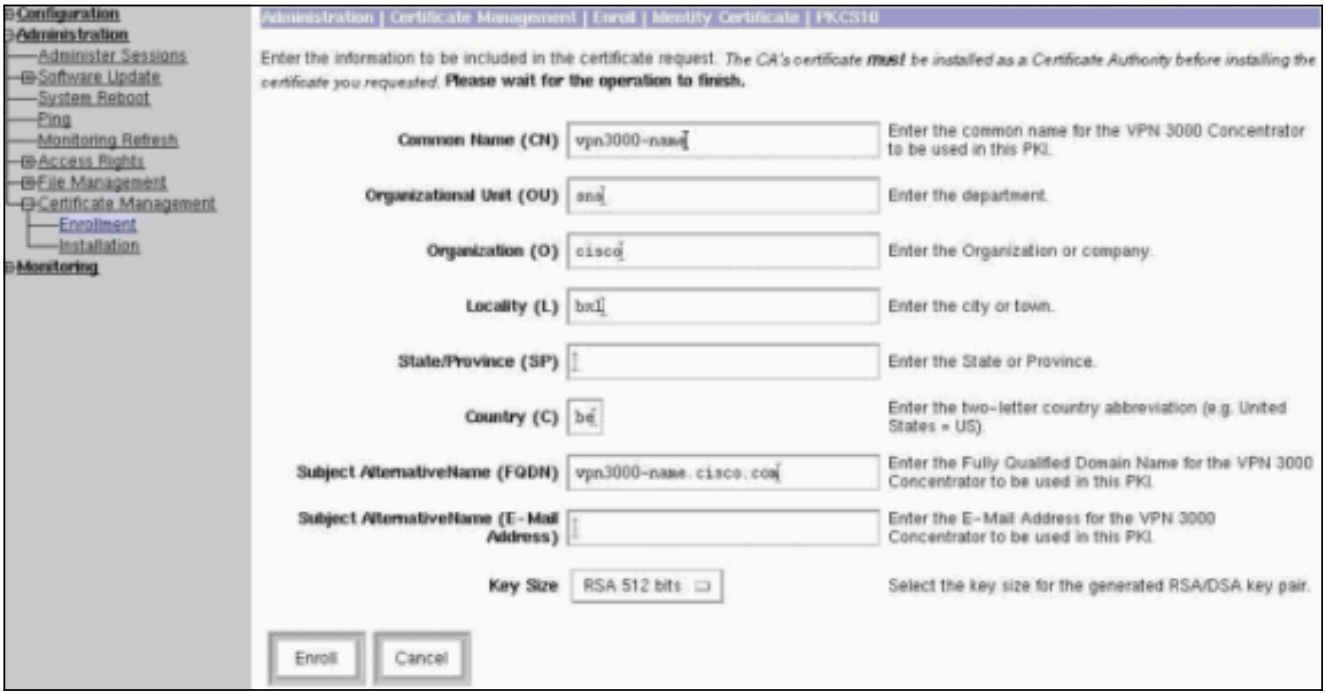
VPN 3000 Concentrator에 대한 루트 인증서를 가져오려면 다음 단계를 완료하십시오.

1. 브라우저에서 CA(대개 http://ip_add_of_ca/certsrv/)를 가리키고 **CA 인증서 또는 인증서 해지 목록을 검색한 후 Next(다음)**를 클릭합니다.
2. **Download CA certificate(CA 인증서 다운로드)**를 클릭하고 로컬 디스크의 어딘가에 파일을 저장합니다.
3. VPN 3000 Concentrator에서 **Administration(관리) > Certificate Management(인증서 관리)**를 선택하고 **Click here(여기를 클릭하여 인증서를 설치하고 CA Certificate를 설치합니다**.
4. 워크스테이션**에서 파일 업로드를 클릭합니다**.
5. Browse(**찾아보기**)를 클릭하고 방금 다운로드한 CA 인증서 파일을 선택합니다.
6. 파일 이름을 강조 표시하고 Install(설치)**을 클릭합니다**
.



VPN 3000 Concentrator의 ID 인증서 얻기

VPN 3000 Concentrator에 대한 ID 인증서를 가져오려면 다음 단계를 완료하십시오.

1. ConfAdministration **> Certificate Management > Enroll > Identity Certificate를 선택한** 다음 Enroll **via PKCS10 Request (Manual)를** 클릭합니다. 여기에 표시된 양식을 작성하고 Enroll(등록)을 **클릭합니다**
.


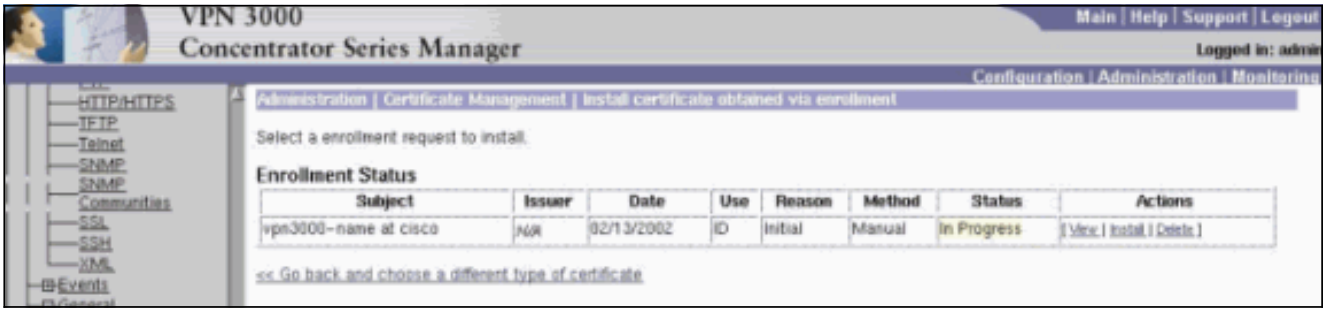
인증서 요청과 함께 브라우저 창이 나타납니다. 이 출력과 유사한 텍스트가 포함되어야 합니다.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBPDCB5wIBADBQMRUwEwYDVQQDEwx2cG4zMDAwLW5hbWUxDDAKBgNVBAsTA3Nu
czEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAcTA2J4bDELMAkGA1UEBhMCYmUwWjAN
BgkqhkiG9w0BAQEFAANJADBGAkEAx7K+pvE004qILNNw3kPVWXrdlqZV4yeOIPdh
C8/V5Yuqq5tMWY3L1W6DC0p256bvGqzd5fhqSkOhBVnNJ1Y/KQIBA6A0MDIGCSqG
SIb3DQEJDjElMCMwIQYDVR0RBBowGIIWdnBuMzAwMC1uYW1lLmNpc2NvLmNvbTAN
BgkqhkiG9w0BAQQFAANBABzcG3IKaWnDLFtrNf1QDi+D7w8dxPu74b/BRHn9fsKI
X6+X0ed0EuEgm1/2nfj8Ux0nV5F/c5wukUfysMmJ/ak=
-----END NEW CERTIFICATE REQUEST-----
```

2. 브라우저를 CA 서버로 이동하고 **Request a certificate(인증서 요청)를** 선택한 후 Next(**다음**)를 클릭합니다.
3. Advanced **Request(고급 요청)**를 선택하고 **Next(다음)**를 클릭한 다음 **Submit a certificate request using a base64 encoded PKCS #10 file(base64 encoded PKCS #7 파일을 사용하여 인증서 요청 제출)을 선택합니다**.

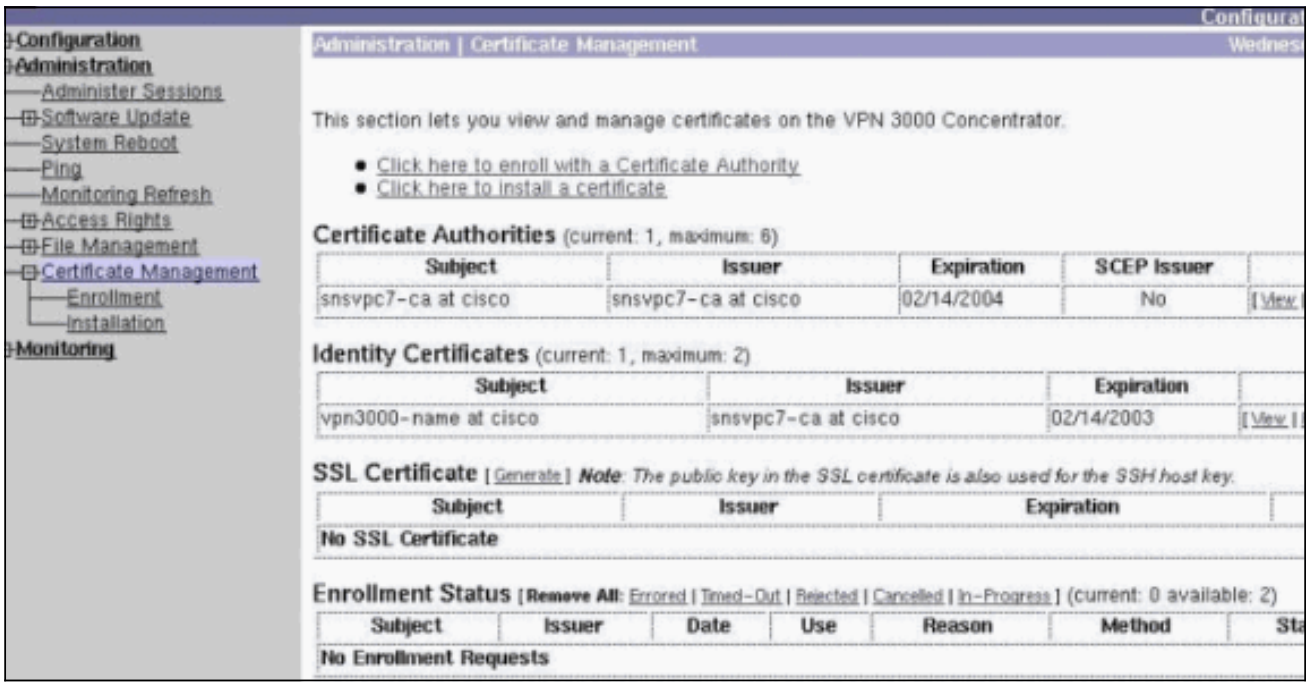
4. **Next(다음)**를 클릭합니다. 이전에 텍스트 영역에 표시된 인증서 요청의 텍스트를 잘라내어 붙여넣습니다. Submit(제출)**을 클릭합니다**.
5. CA 서버가 구성된 방법에 따라 Download **CA certificate(CA 인증서 다운로드)**를 클릭할 수 있습니다. 또는 CA에서 인증서를 발급한 후 CA 서버로 돌아가 **보류 중인 인증서 확인을** 선택합니다.
6. **Next(다음)**를 클릭하고 요청을 선택한 후 다시 **Next(다음)**를 클릭합니다.
7. Download **CA certificate(CA 인증서 다운로드)**를 클릭하고 파일을 로컬 디스크에 저장합니다.
8. VPN 3000 Concentrator에서 **Administration(관리) > Certificate Management(인증서 관리) > Install(설치)을** 선택하고 Install certificate **acquired received via enrollment(등록을 통해 가져온 인증서 설치)를** 클릭합니다.그런 다음 이 그림과 같이 "In Progress(진행 중)" 상태로 보류 중인 요청을 볼 수 있습니다

.



9. Install(**설치**)을 클릭한 다음 Upload **File from Workstation(워크스테이션에서 파일 업로드)을 클릭합니다**.
10. Browse(**찾아보기**)를 클릭하고 CA에서 발급한 인증서가 포함된 파일을 선택합니다.
11. 파일 이름을 강조 표시하고 Install(설치)**을 클릭합니다**.
12. 관리 **> 인증서 관리를 선택 합니다**. 이 이미지와 유사한 화면이 나타납니다

.



클라이언트에 대한 풀 구성

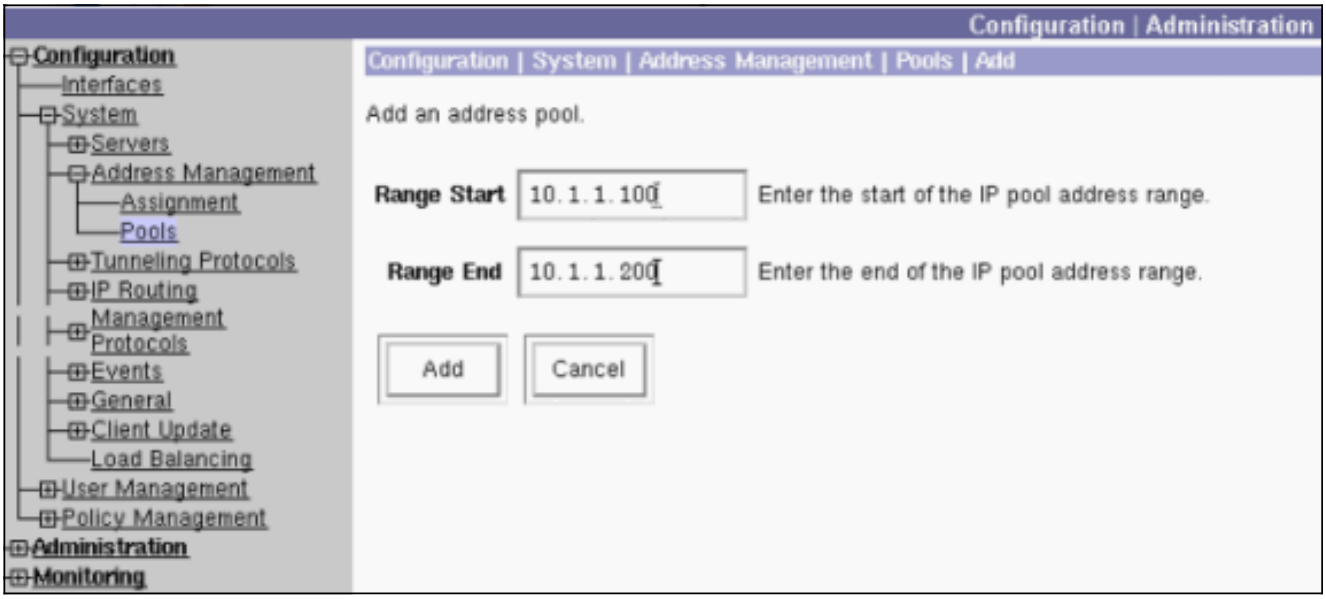
클라이언트에 대한 풀을 구성하려면 다음 절차를 완료합니다.

1. 사용 가능한 IP 주소 범위를 할당하려면 브라우저를 VPN 3000 Concentrator의 내부 인터페이스로 이동하고 Configuration(구성) > **System(시스템) > Address Management(주소 관리) >**

Pools(풀) > Add(추가)를 선택합니다.

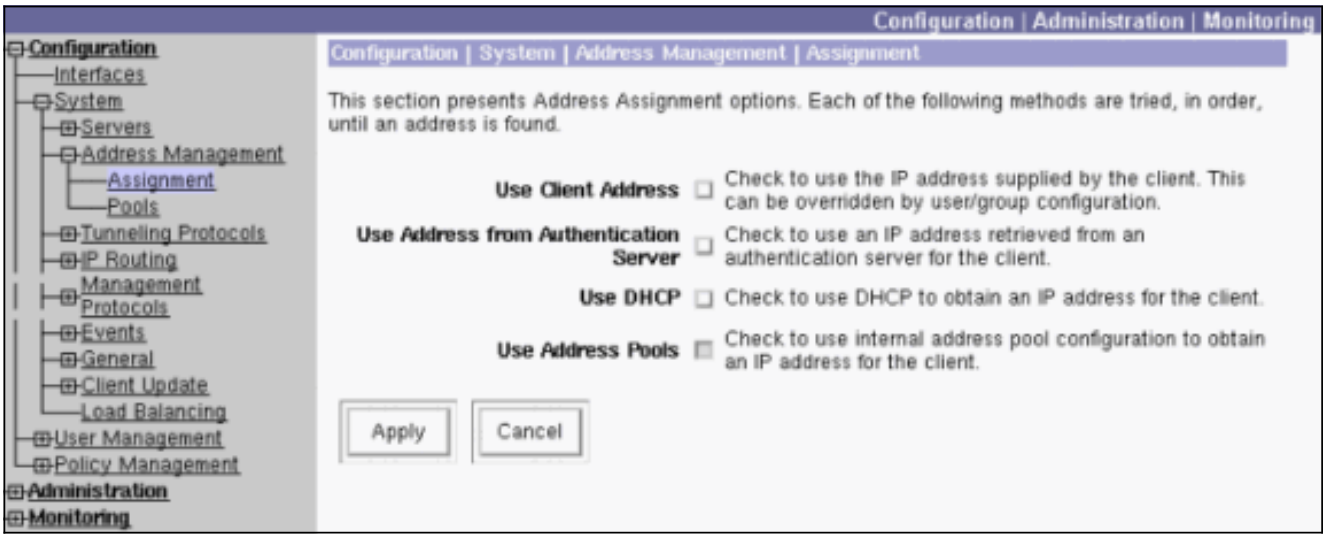
2. 내부 네트워크의 다른 디바이스와 충돌하지 않는 IP 주소 범위를 지정하고 Add(추가)를 **클릭합니다**

.



3. VPN 3000 Concentrator에 풀을 사용하도록 지정하려면 이 이미지와 같이 **Configuration > System > Address Management > Assignment**를 선택하고 **Use Address Pools(주소 풀 사용)** 상자를 선택한 후 **Apply(적용)**를 클릭합니다

.

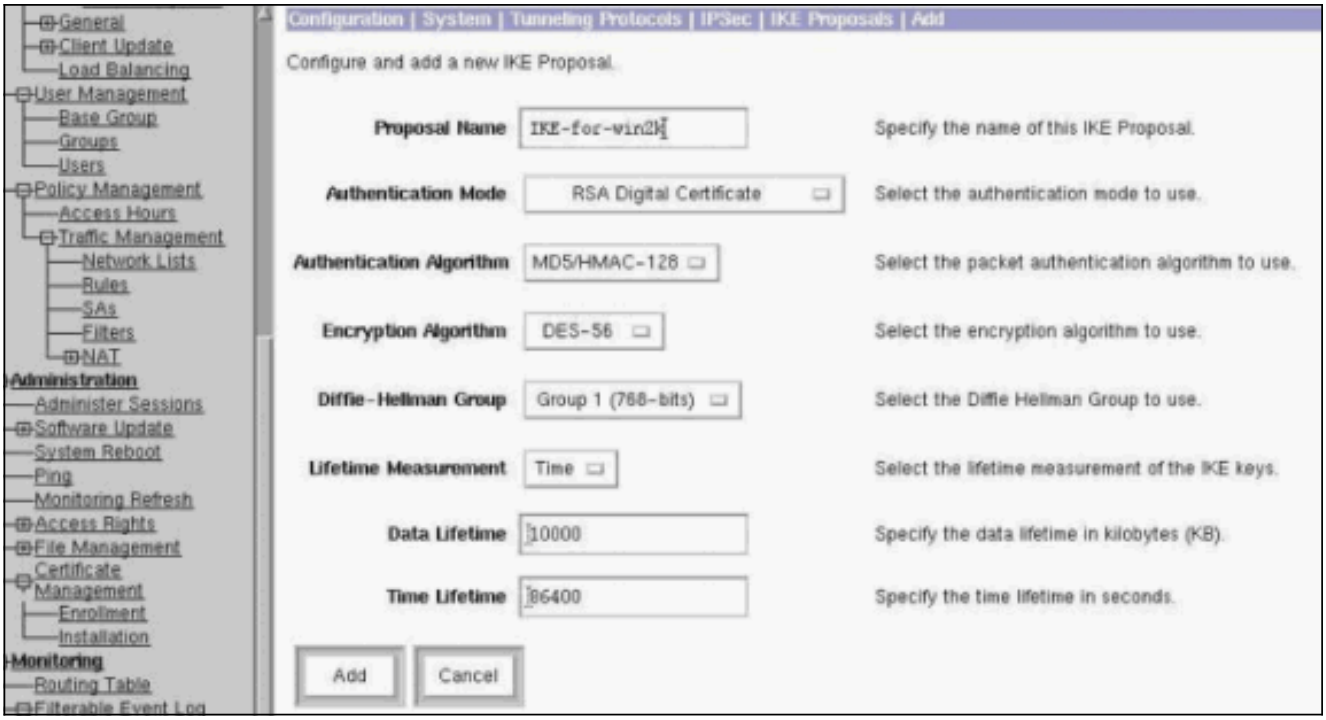


IKE 제안 구성

IKE 제안을 구성하려면 다음 단계를 완료하십시오.

1. 이 이미지에 표시된 대로 **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals**를 선택하고 **Add**를 클릭한 후 매개변수를 선택합니다

.



2. Add(**추가**)를 클릭하고 오른쪽 열에서 새 제안을 강조 표시한 다음 Activate(**활성화**)를 클릭합니다.

SA 구성

SA(Security Association)를 구성하려면 다음 절차를 수행합니다.

1. Configuration(**컨피그레이션**) > **Policy Management(정책 관리)** > **Traffic Management(트래픽 관리)** > **SA**를 선택하고 **ESP-L2TP-TRANSPORT**를 클릭합니다.이 SA를 사용할 수 없거나 다른 용도로 사용하는 경우 이 SA와 유사한 새 SA를 생성합니다. SA에 대해 다른 설정을 사용할 수 있습니다. 보안 정책에 따라 이 매개변수를 변경합니다.
2. Digital Certificate(디지털 인증서) 풀다운 메뉴에서 이전에 구성한 **디지털** 인증서를 선택합니다. IKE-**for-win2k** IKE(Internet Key Exchange) 제안을 선택합니다.**참고:** 이는 필수 사항이 아닙니다. L2TP/IPSec 클라이언트가 VPN Concentrator에 연결되면 Configuration(**구성**) > **System(시스템)** > **Tunneling Protocols(터널링 프로토콜)** > **IPSec** > **IKE Proposals(IKE 제안) 페이지**의 active(활성) 열 아래에 구성된 모든 IKE 제안이 순서대로 시도됩니다.이 그림에서는 SA에 필요한 컨피그레이션을 보여줍니다
.

그룹 및 사용자 구성

그룹 및 사용자를 구성하려면 다음 절차를 완료합니다.

1. Configuration **> User Management > Base Group을 선택합니다**.
2. General(일반) 탭에서 **L2TP over IPSec이** 선택되었는지 확인합니다.
3. IPSec 탭에서 **ESP-L2TP-TRANSPORT** SA**를** 선택합니다.
4. PPTP/L2TP 탭에서 모든 **L2TP 암호화** 옵션의 **선택을** 취소합니다.
5. Configuration(**컨피그레이션) > User Management(사용자 관리) > Users(사용자)**를 선택하고 Add(추가)**를 클릭합니다**.
6. Windows 2000 클라이언트에서 연결하는 데 사용하는 이름과 암호를 입력합니다. [그룹 선택] 아래에서 **[기본 그룹]**을 선택해야 합니다.
7. General(일반) 탭에서 **L2TP over IPSec** 터널링 **프로토콜을** 선택합니다.
8. IPSec 탭에서 **ESP-L2TP-TRANSPORT** SA**를** 선택합니다.
9. PPTP/L2TP 탭에서 모든 **L2TP 암호화 옵션**의 선택을 취소하고 Add(추가)를 **클릭합니다**.이제 L2TP/IPSec Windows 2000 Client를 사용하여 연결할 수 있습니다.**참고:** 원격 L2TP/IPSec 연결을 허용하도록 기본 그룹을 구성하도록 선택했습니다. 수신 연결을 수락하도록 SA의 OU(Organization Unit) 필드와 일치하는 그룹을 구성할 수도 있습니다. 구성이 동일합니다.

디버그 정보

```
269 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3868 10.48.66.76
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 7

271 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3869 10.48.66.76
```

```
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

274 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3870 10.48.66.76
Proposal # 1, Transform # 2, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

279 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3871 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

282 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3872 10.48.66.76
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

285 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3873 10.48.66.76
  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

288 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3874 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

291 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3875 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

294 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3876 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

297 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3877 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

300 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3878 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

303 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3879 10.48.66.76
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class DH Group:
```

```
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

306 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3880 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

309 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3881 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

312 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3882 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

315 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3883 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

318 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3884 10.48.66.76
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 7

321 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3885 10.48.66.76
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

324 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3886 10.48.66.76
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

329 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3887 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

332 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3888 10.48.66.76
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

335 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3889 10.48.66.76
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES
```

```
338 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3890 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

341 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3891 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

344 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3892 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

347 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3893 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

350 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3894 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

353 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3895 10.48.66.76
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

356 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3896 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

358 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3897 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

361 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3898 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

364 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3899 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

367 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3900 10.48.66.76
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
```

```
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

370 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3901 10.48.66.76
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

372 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3902 10.48.66.76
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

377 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3903 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

380 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3904 10.48.66.76
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

383 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3905 10.48.66.76
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

386 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3906 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

389 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3907 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

392 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3908 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

395 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3909 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

398 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3910 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2
```

```
401 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3911 10.48.66.76
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

404 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3912 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class Auth Method:
    Rcv'd: RSA signature with Certificates
    Cfg'd: Preshared Key

407 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3913 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

410 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3914 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

413 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3915 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

416 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3916 10.48.66.76
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

419 02/15/2002 12:47:24.430 SEV=7 IKEDBG/28 RPT=20 10.48.66.76
IKE SA Proposal # 1, Transform # 4 acceptable
Matches global IKE entry # 16

420 02/15/2002 12:47:24.440 SEV=9 IKEDBG/0 RPT=3917 10.48.66.76
constructing ISA_SA for isakmp

421 02/15/2002 12:47:24.490 SEV=8 IKEDBG/0 RPT=3918 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 80

423 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3919 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

425 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3920 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

427 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3921 10.48.66.76
processing ke payload

428 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3922 10.48.66.76
processing ISA_KE

429 02/15/2002 12:47:24.540 SEV=9 IKEDBG/1 RPT=104 10.48.66.76
processing nonce payload
```

```
430 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3923 10.48.66.76
constructing ke payload

431 02/15/2002 12:47:24.600 SEV=9 IKEDBG/1 RPT=105 10.48.66.76
constructing nonce payload

432 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3924 10.48.66.76
constructing certreq payload

433 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3925 10.48.66.76
Using initiator's certreq payload data

434 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=61 10.48.66.76
constructing Cisco Unity VID payload

435 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=62 10.48.66.76
constructing xauth V6 VID payload

436 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=39 10.48.66.76
Send IOS VID

437 02/15/2002 12:47:24.600 SEV=9 IKEDBG/38 RPT=20 10.48.66.76
Constructing VPN 3000 spoofing IOS Vendor ID payload
(version: 1.0.0, capabilities: 20000001)

439 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=63 10.48.66.76
constructing VID payload

440 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=40 10.48.66.76
Send Altiga GW VID

441 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3926 10.48.66.76
Generating keys for Responder...

442 02/15/2002 12:47:24.610 SEV=8 IKEDBG/0 RPT=3927 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + VENDOR (13) + NONE (0) ... total length : 229

445 02/15/2002 12:47:24.640 SEV=8 IKEDBG/0 RPT=3928 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + CERT (6) + SIG (9) + CERT_REQ (7) + NONE (0)
... total length : 1186

448 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=106 10.48.66.76
Processing ID

449 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3929 10.48.66.76
processing cert payload

450 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=107 10.48.66.76
processing RSA signature

451 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3930 10.48.66.76
computing hash

452 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3931 10.48.66.76
processing cert request payload

453 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3932 10.48.66.76
Storing cert request payload for use in MM msg 4

454 02/15/2002 12:47:24.650 SEV=9 IKEDBG/23 RPT=20 10.48.66.76
```

```
Starting group lookup for peer 10.48.66.76

455 02/15/2002 12:47:24.650 SEV=9 IKE/21 RPT=12 10.48.66.76
No Group found by matching IP Address of Cert peer 10.48.66.76

456 02/15/2002 12:47:24.650 SEV=9 IKE/20 RPT=12 10.48.66.76
No Group found by matching OU(s) from ID payload:
 ou=sns,

457 02/15/2002 12:47:24.650 SEV=9 IKE/0 RPT=12 10.48.66.76
Group [VPNC_Base_Group]
No Group name for IKE Cert session, defaulting to BASE GROUP

459 02/15/2002 12:47:24.750 SEV=7 IKEDBG/0 RPT=3933 10.48.66.76
Group [VPNC_Base_Group]
Found Phase 1 Group (VPNC_Base_Group)

460 02/15/2002 12:47:24.750 SEV=7 IKEDBG/14 RPT=20 10.48.66.76
Group [VPNC_Base_Group]
Authentication configured for Internal

461 02/15/2002 12:47:24.750 SEV=9 IKEDBG/19 RPT=20 10.48.66.76
Group [VPNC_Base_Group]
IKEGetUserAttributes: default domain = fenetwork.com

462 02/15/2002 12:47:24.770 SEV=5 IKE/79 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Validation of certificate successful
(CN=my_name, SN=6102861F000000000005)

464 02/15/2002 12:47:24.770 SEV=7 IKEDBG/0 RPT=3934 10.48.66.76
Group [VPNC_Base_Group]
peer ID type 9 received (DER_ASN1_DN)

465 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=108 10.48.66.76
Group [VPNC_Base_Group]
constructing ID

466 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3935 10.48.66.76
Group [VPNC_Base_Group]
constructing cert payload

467 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=109 10.48.66.76
Group [VPNC_Base_Group]
constructing RSA signature

468 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3936 10.48.66.76
Group [VPNC_Base_Group]
computing hash

469 02/15/2002 12:47:24.800 SEV=9 IKEDBG/46 RPT=64 10.48.66.76
Group [VPNC_Base_Group]
constructing dpd vid payload

470 02/15/2002 12:47:24.800 SEV=8 IKEDBG/0 RPT=3937 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + ID (5) + CERT (6) + SIG (9) + VENDOR (13) + NONE (0)
... total length : 1112

473 02/15/2002 12:47:24.800 SEV=4 IKE/119 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
PHASE 1 COMPLETED

474 02/15/2002 12:47:24.800 SEV=6 IKE/121 RPT=4 10.48.66.76
```

```
Keep-alive type for this connection: None

475 02/15/2002 12:47:24.800 SEV=6 IKE/122 RPT=4 10.48.66.76
Keep-alives configured on but peer does not support keep-alives (type = None)

476 02/15/2002 12:47:24.800 SEV=7 IKEDBG/0 RPT=3938 10.48.66.76
Group [VPNC_Base_Group]
Starting phase 1 rekey timer: 21600000 (ms)

477 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3939 10.48.66.76
RECEIVED Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 1108

480 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3940 10.48.66.76
Group [VPNC_Base_Group]
processing hash

481 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3941 10.48.66.76
Group [VPNC_Base_Group]
processing SA payload

482 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=110 10.48.66.76
Group [VPNC_Base_Group]
processing nonce payload

483 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=111 10.48.66.76
Group [VPNC_Base_Group]
Processing ID

484 02/15/2002 12:47:24.810 SEV=5 IKE/25 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Received remote Proxy Host data in ID Payload:
Address 10.48.66.76, Protocol 17, Port 1701

487 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=112 10.48.66.76
Group [VPNC_Base_Group]
Processing ID

488 02/15/2002 12:47:24.810 SEV=5 IKE/24 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Received local Proxy Host data in ID Payload:
Address 10.48.66.109, Protocol 17, Port 0

491 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3942
QM IsRekeyed old sa not found by addr

492 02/15/2002 12:47:24.810 SEV=5 IKE/66 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
IKE Remote Peer configured for SA: ESP-L2TP-TRANSPORT

493 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3943 10.48.66.76
Group [VPNC_Base_Group]
processing IPSEC SA

494 02/15/2002 12:47:24.810 SEV=7 IKEDBG/27 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
IPSec SA Proposal # 1, Transform # 1 acceptable

495 02/15/2002 12:47:24.810 SEV=7 IKEDBG/0 RPT=3944 10.48.66.76
Group [VPNC_Base_Group]
IKE: requesting SPI!

496 02/15/2002 12:47:24.810 SEV=8 IKEDBG/6 RPT=4
```

```
IKE got SPI from key engine: SPI = 0x10d19e33

497 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3945 10.48.66.76
Group [VPNC_Base_Group]
oakley constucting quick mode

498 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3946 10.48.66.76
Group [VPNC_Base_Group]
constructing blank hash

499 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3947 10.48.66.76
Group [VPNC_Base_Group]
constructing ISA_SA for ipsec

500 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=113 10.48.66.76
Group [VPNC_Base_Group]
constructing ipsec nonce payload

501 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=114 10.48.66.76
Group [VPNC_Base_Group]
constructing proxy ID

502 02/15/2002 12:47:24.820 SEV=7 IKEDBG/0 RPT=3948 10.48.66.76
Group [VPNC_Base_Group]
Transmitting Proxy Id:
  Remote host: 10.48.66.76  Protocol 17  Port 1701
  Local host:  10.48.66.109  Protocol 17  Port 0

506 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3949 10.48.66.76
Group [VPNC_Base_Group]
constructing qm hash

507 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3950 10.48.66.76
SENDING Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 156

510 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3951 10.48.66.76
RECEIVED Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

512 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3952 10.48.66.76
Group [VPNC_Base_Group]
processing hash

513 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3953 10.48.66.76
Group [VPNC_Base_Group]
loading all IPSEC SAs

514 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=115 10.48.66.76
Group [VPNC_Base_Group]
Generating Quick Mode Key!

515 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=116 10.48.66.76
Group [VPNC_Base_Group]
Generating Quick Mode Key!

516 02/15/2002 12:47:24.830 SEV=7 IKEDBG/0 RPT=3954 10.48.66.76
Group [VPNC_Base_Group]
Loading host:
  Dst: 10.48.66.109
  Src: 10.48.66.76

517 02/15/2002 12:47:24.830 SEV=4 IKE/49 RPT=4 10.48.66.76
```

```
Group [VPNC_Base_Group]
Security negotiation complete for User ()
Responder, Inbound SPI = 0x10d19e33, Outbound SPI = 0x15895ab9

520 02/15/2002 12:47:24.830 SEV=8 IKEDBG/7 RPT=4
IKE got a KEY_ADD msg for SA: SPI = 0x15895ab9

521 02/15/2002 12:47:24.830 SEV=8 IKEDBG/0 RPT=3955
pitcher: rcv KEY_UPDATE, spi 0x10d19e33

522 02/15/2002 12:47:24.830 SEV=4 IKE/120 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
PHASE 2 COMPLETED (msgid=781ceadc)

523 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3956
pitcher: recv KEY_SA_ACTIVE spi 0x10d19e33

524 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3957
KEY_SA_ACTIVE no old rekey centry found with new spi 0x10d19e33, mess_id 0x0
```

문제 해결 정보

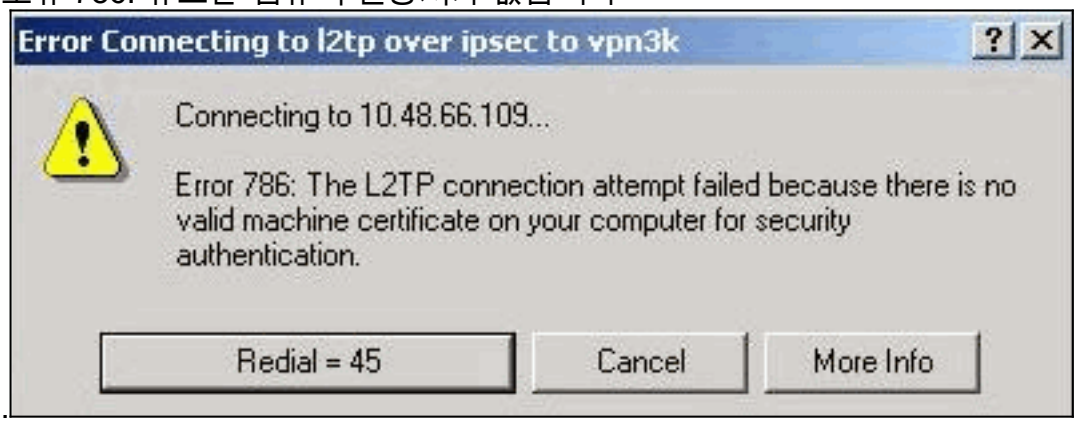
이 섹션에서는 몇 가지 일반적인 문제 및 각각에 대한 트러블슈팅 방법을 설명합니다.

- 서버를 시작할 수 없습니다

.

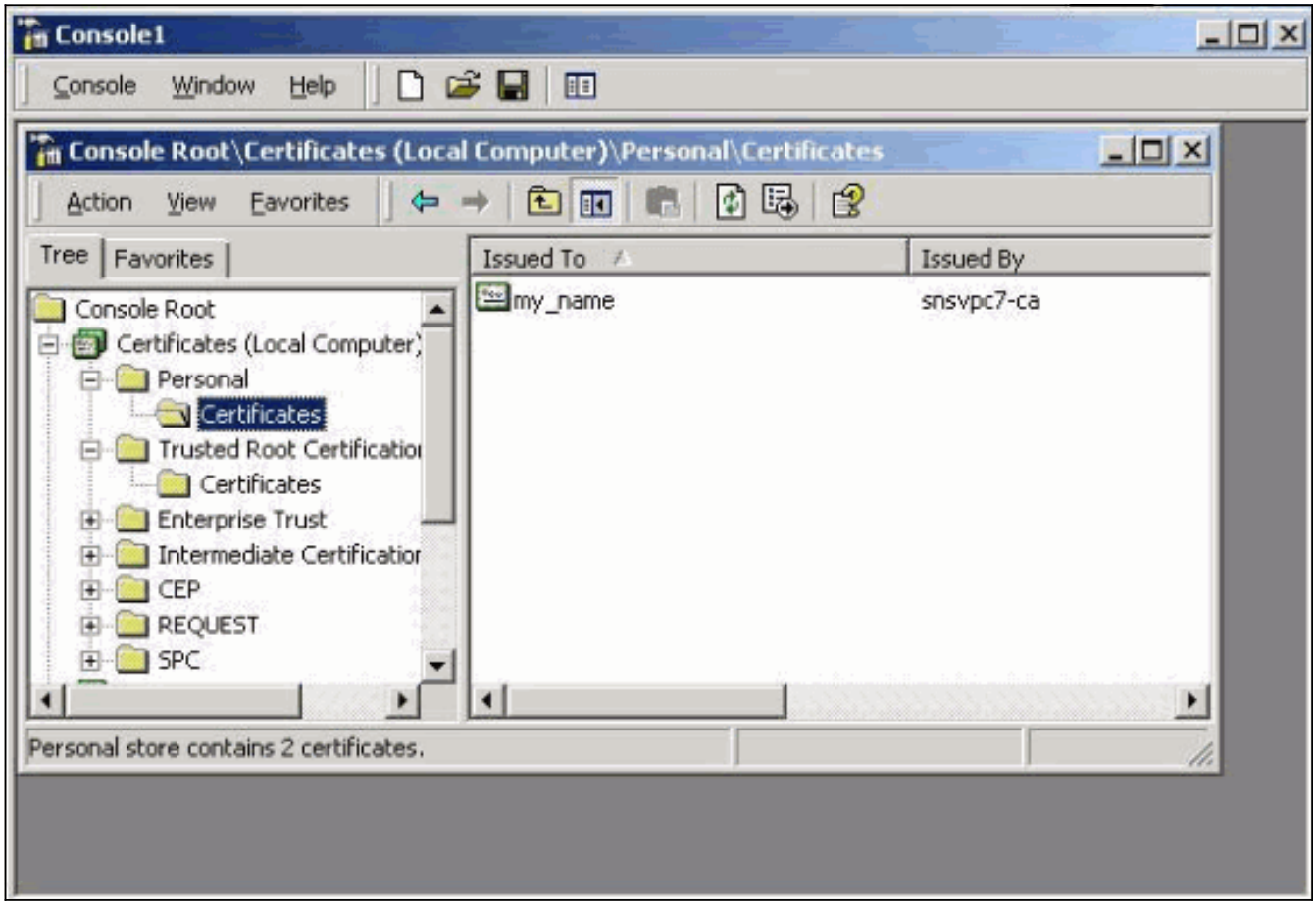
IPSec 서비스가 시작되지 않은 경우가 가장 많습니다. Start(**시작) > Programs(프로그램) > Administrative tools(관리 툴) > Service(서비스**)를 선택하고 IPSec **서비스가** 활성화되어 있는지 확인합니다.

- 오류 786: 유효한 컴퓨터 인증서가 없습니다



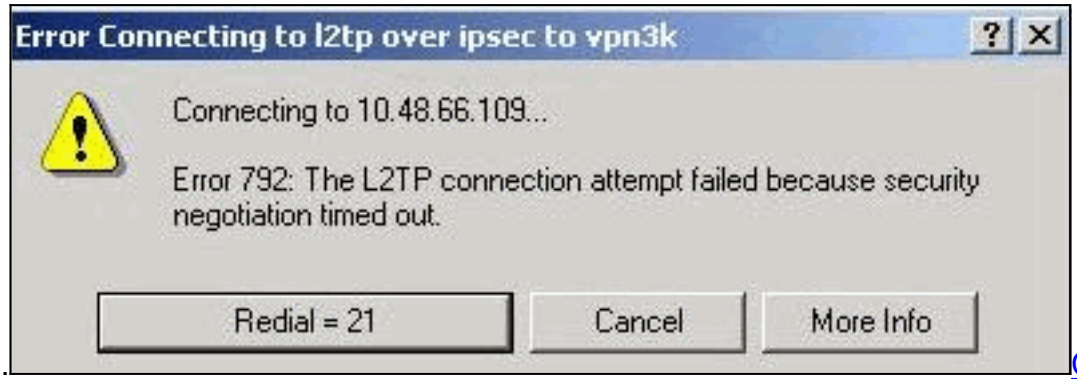
.이 오류는 로컬 컴퓨터의 인증서에 문제가 있음을 나타냅니다. 인증서를 쉽게 보려면 **시작 > 실행**을 선택하고 MMC를 실행하십시오. Console(**콘솔**)을 클릭하고 **Add/Remove Snap-in(스냅인 추가/제거)을** 선택합니다. Add(**추가**)를 클릭하고 **목록**에서 Certificate(인증서)를 선택합니다. 인증서의 범위를 묻는 창이 나타나면 컴퓨터 계정을 **선택합니다**.이제 CA 서버의 인증서가 Trusted **Root Certification** Authorities 아래에 있는지 확인할 수 **있습니다**. 이 이미지에 표시된 대로 Console Root(**콘솔 루트) > Certificate (Local Computer)(인증서(로컬 컴퓨터)) > Personal(개인) > Certificates(인증서)**를 선택하여 인증서가 있는지 확인할 수도 있습니다

.



인증서를 **클릭합니다**. 모든 것이 정확한지 확인합니다. 이 예에서는 인증서와 연결된 개인 키가 있습니다. 그러나 이 인증서는 만료되었습니다. 이것이 문제의 원인입니다

- 오류 792: 보안 협상 시간 초과.이 메시지는 오랜 시간이 지난 후에 나타납니다



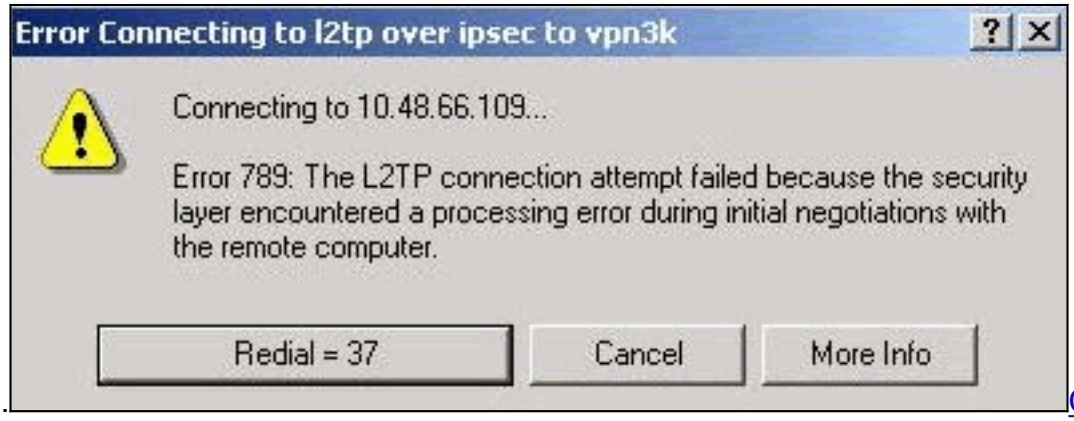
Cisco VPN 3000 Concentrator FAQ에 설명된 대로 관련 디버그를 켭니다. 자세히 읽어보십시오. 이 출력과 유사한 항목을 확인해야 합니다.

```
9337 02/15/2002 15:06:13.500 SEV=8 IKEDBG/0 RPT=7002 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

9340 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7003 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
```

```
  Mismatched attr types for class Auth Method:
    Rcv'd: RSA signature with Certificates
    Cfg'd: Preshared Key

9343 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7004 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

9346 02/15/2002 15:06:13.510 SEV=7 IKEDBG/0 RPT=7005 10.48.66.76
All SA proposals found unacceptable

9347 02/15/2002 15:06:13.510 SEV=4 IKE/48 RPT=37 10.48.66.76
Error processing payload: Payload ID: 1

9348 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7006 10.48.66.76
IKE SA MM:261e40dd terminating:
flags 0x01000002, refcnt 0, tuncnt 0

9349 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7007
sending delete message
```

이는 IKE 제안이 제대로 구성되지 않았음을 나타냅니다. 이 문서의 IKE 제안 구성 섹션에서 정보를 확인합니다.

- 오류 789: 보안 레이어에 처리 오류가 발생했습니다



Cisco VPN 3000 Concentrator FAQ에 설명된 대로 관련 디버그를 켭니다. 자세히 읽어보십시오. 이 출력과 유사한 항목을 확인해야 합니다.

```
11315 02/15/2002 15:36:32.030 SEV=8 IKEDBG/0 RPT=7686
Proposal # 1, Transform # 2, Type ESP, Id DES-CBC
Parsing received transform:
  Phase 2 failure:
  Mismatched attr types for class Encapsulation:
    Rcv'd: Transport
    Cfg'd: Tunnel

11320 02/15/2002 15:36:32.030 SEV=5 IKEDBG/0 RPT=7687
AH proposal not supported

11321 02/15/2002 15:36:32.030 SEV=4 IKE/0 RPT=27 10.48.66.76
Group [VPNC_Base_Group]
All IPSec SA proposals found unacceptable!
```

- 사용된 버전이 출력을 보려면 **Monitoring(모니터링) > System Status(시스템 상태)**를 선택합니다.

```
VPN Concentrator Type: 3005
Bootcode Rev: Altiga Networks/VPN Concentrator Version 2.2.int_9 Jan 19 2000 05:36:41
Software Rev: Cisco Systems, Inc./VPN 3000 Concentrator Version 3.5.Rel Nov 27 2001 13:35:16
Up For: 44:39:48
Up Since: 02/13/2002 15:49:59
```

```
RAM Size: 32 MB
```

관련 정보

- IPSec 협상/IKE 프로토콜 제품 지원
- Technical Support - Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.