Cisco VPN 3000 Concentrator에서 HTTP를 통한 CRL 확인

목차

소개

이 문서에서는 HTTP 모드를 사용하여 Cisco VPN 3000 Concentrator에 설치된 CA(Certification Authority) 인증서를 확인하는 CRL(Certificate Revocation List)을 활성화하는 방법에 대해 설명합니다.

인증서는 일반적으로 전체 유효 기간 동안 유효해야 합니다. 그러나 이름 변경, 제목과 CA 간의 연결 변경, 보안 손상 등의 이유로 인증서가 무효화되면 CA는 인증서를 폐기합니다. X.509에서 CA는 정기적으로 서명된 CRL을 발행하여 인증서를 폐기합니다. 여기서 폐기된 각 인증서는 일련 번호로 식별됩니다. CRL 확인을 활성화하면 VPN Concentrator가 인증을 위해 인증서를 사용할 때마다 CRL을 확인하여 검증되는 인증서가 폐기되지 않았는지 확인합니다.

CA는 LDAP(Lightweight Directory Access Protocol)/HTTP 데이터베이스를 사용하여 CRL을 저장하고 배포합니다. 다른 방법도 사용할 수 있지만 VPN Concentrator는 LDAP/HTTP 액세스를 사용합니다.

HTTP CRL 검사는 VPN Concentrator 버전 3.6 이상에서 도입되었습니다. 그러나 LDAP 기반 CRL 검사는 이전 3.x 릴리스에서 도입되었습니다. 이 문서에서는 HTTP를 사용하는 CRL 확인에만 대해 설명합니다.

참고: VPN 3000 Series Concentrator의 CRL 캐시 크기는 플랫폼에 따라 달라지며 관리자의 요청에 따라 구성할 수 없습니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- IKE(Internet Key Exchange) 인증을 위한 인증서를 사용하여 VPN 3.x 하드웨어 클라이언트에서 IPsec 터널을 성공적으로 설정했습니다(CRL 검사가 활성화되지 않음).
- VPN Concentrator는 CA 서버에 항상 연결되어 있습니다.
- CA 서버가 공용 인터페이스에 연결된 경우 공용(기본) 필터에서 필요한 규칙을 열었습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- VPN 3000 Concentrator 버전 4.0.1 C
- VPN 3.x 하드웨어 클라이언트
- Windows 2000 서버에서 실행되는 인증서 생성 및 CRL 확인을 위한 Microsoft CA 서버

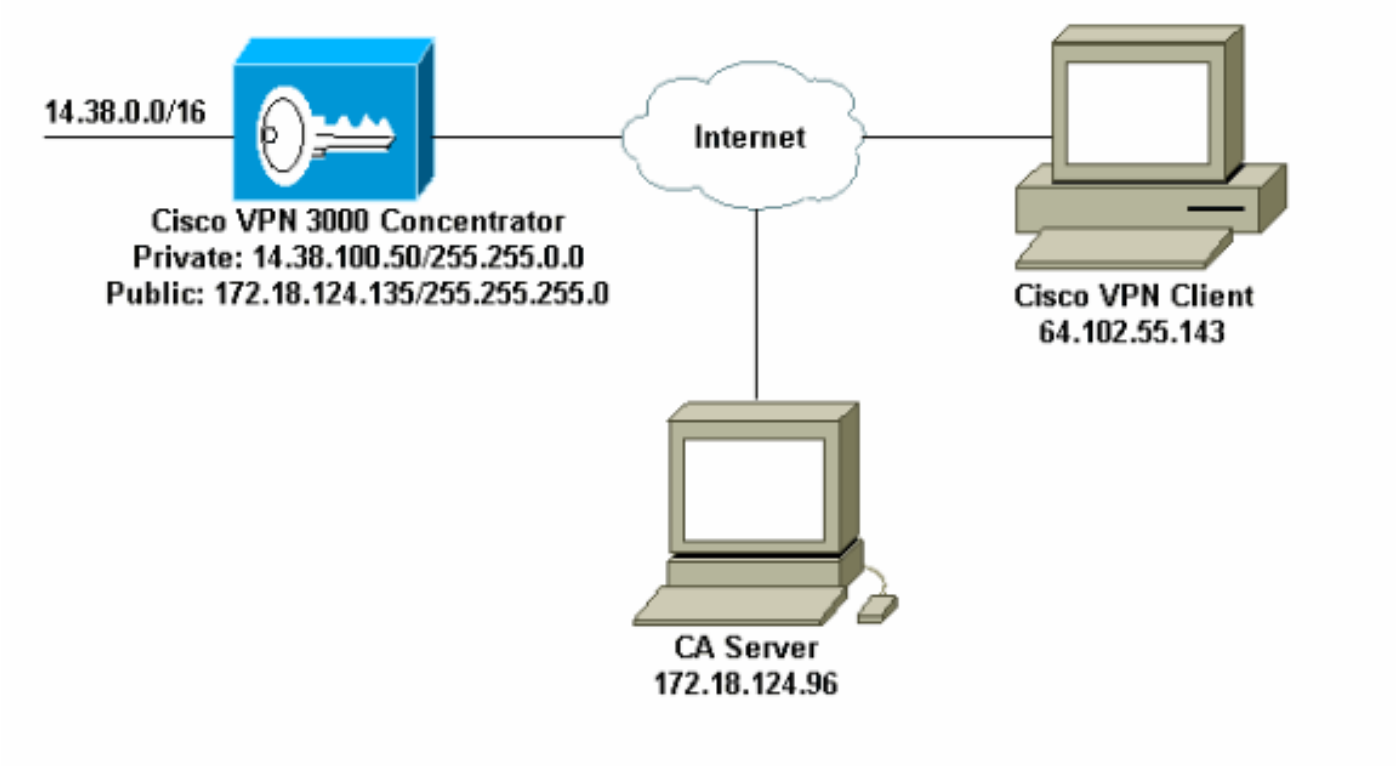
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



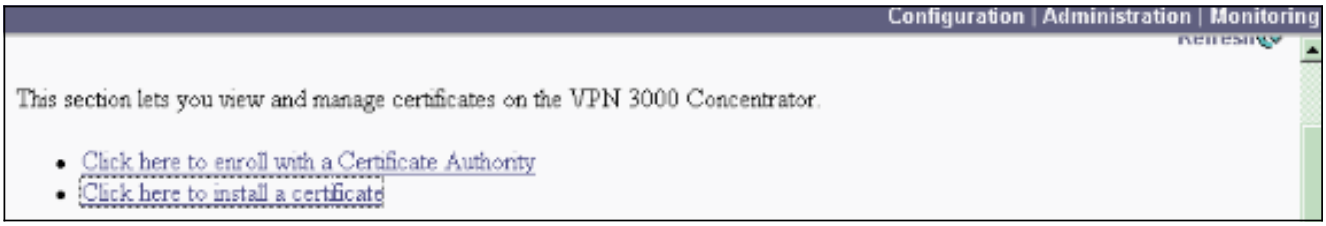
VPN 3000 Concentrator 구성

단계별 지침

VPN 3000 Concentrator를 구성하려면 다음 단계를 완료하십시오.

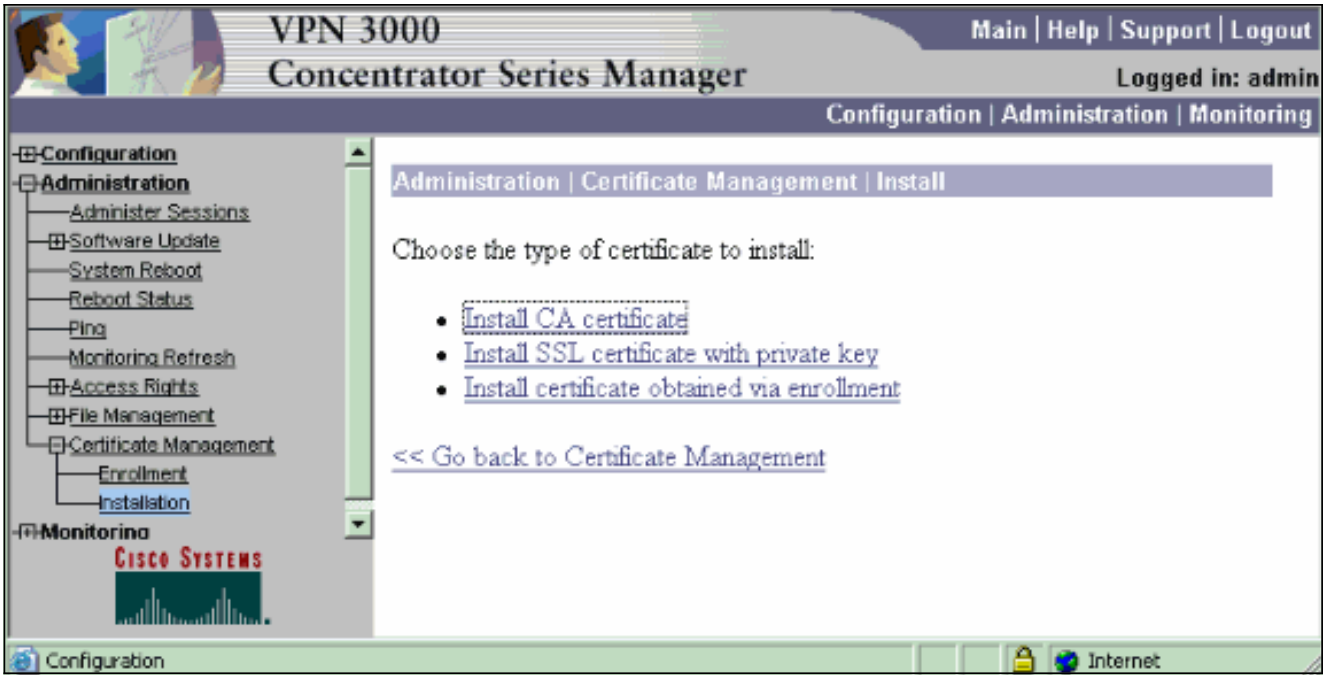
1. 인증서가 **없는** 경우 인증서를 요청하려면 Administration > **Certificate Management**를 선택합니다.Click **here to install a certificate to install the root certificate to install the** to install the VPN Concentrator(VPN Concentrator에 루트 인증서를 설치하려면 여기를 클릭)를 선택합니다

   .



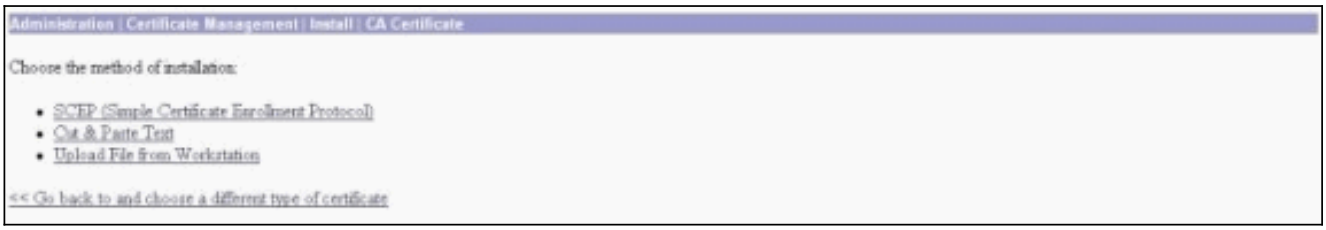
2. Install **CA certificate(CA 인증서 설치)를 선택합니다**

   .



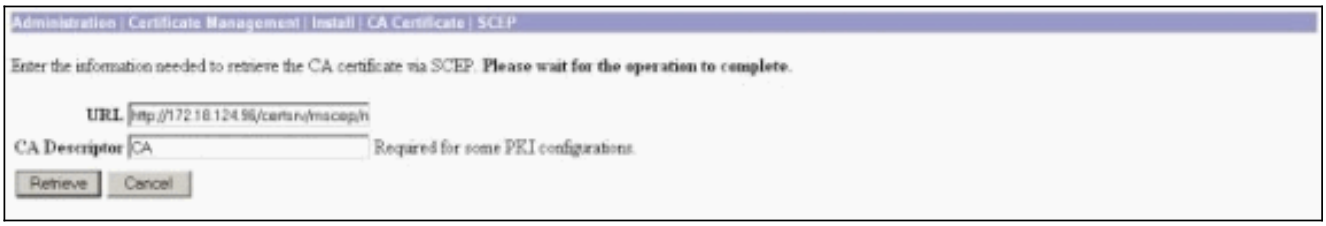
3. SCEP**(Simple Certificate Enrollment Protocol)를 선택하여** CA 인증서를 검색합니다

.



4. SCEP 창의 URL 대화 상자에 CA 서버의 전체 URL을 입력합니다.이 예에서 CA 서버의 IP 주소는 172.18.124.96입니다. 이 예에서는 Microsoft의 CA 서버를 사용하므로 전체 URL은 http://172.18.124.96/certsrv/mscep/mscep.dll입니다. 그런 다음 CA Descriptor 대화 상자에 한 단어 설명자를 입력합니다. 이 예에서는 CA를 사용합니다

.

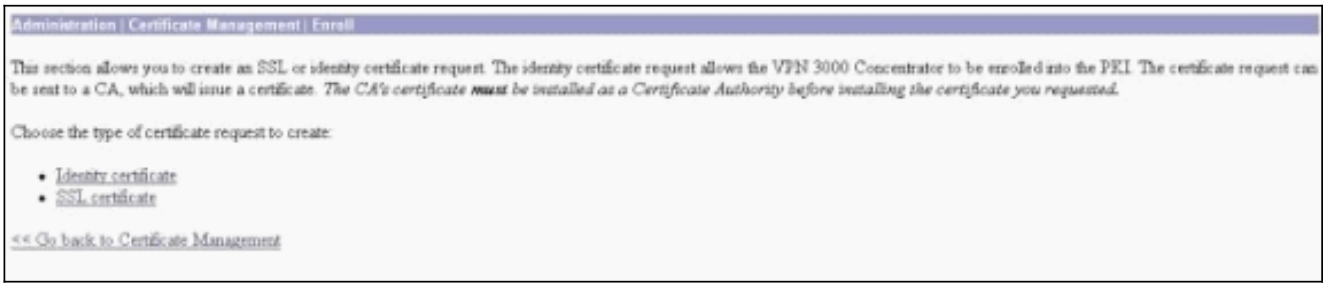


5. Retrieve를 **클릭합니다**.CA 인증서가 Administration(관리) > Certificate Management(인증서 관리) 창 아래에 나타나야 합니다. 인증서가 표시되지 않으면 1단계로 돌아가 절차를 다시 수행하십시오

.

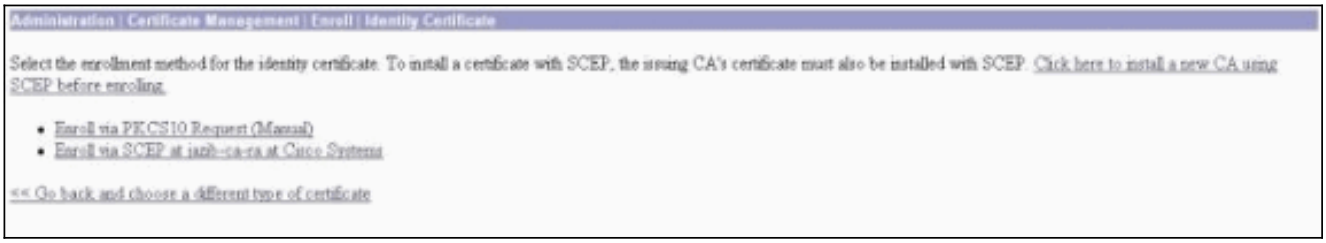
6. CA 인증서가 있으면 **Administration > Certificate Management > Enroll**을 선택하고 **Identity certificate를 클릭합니다**

.



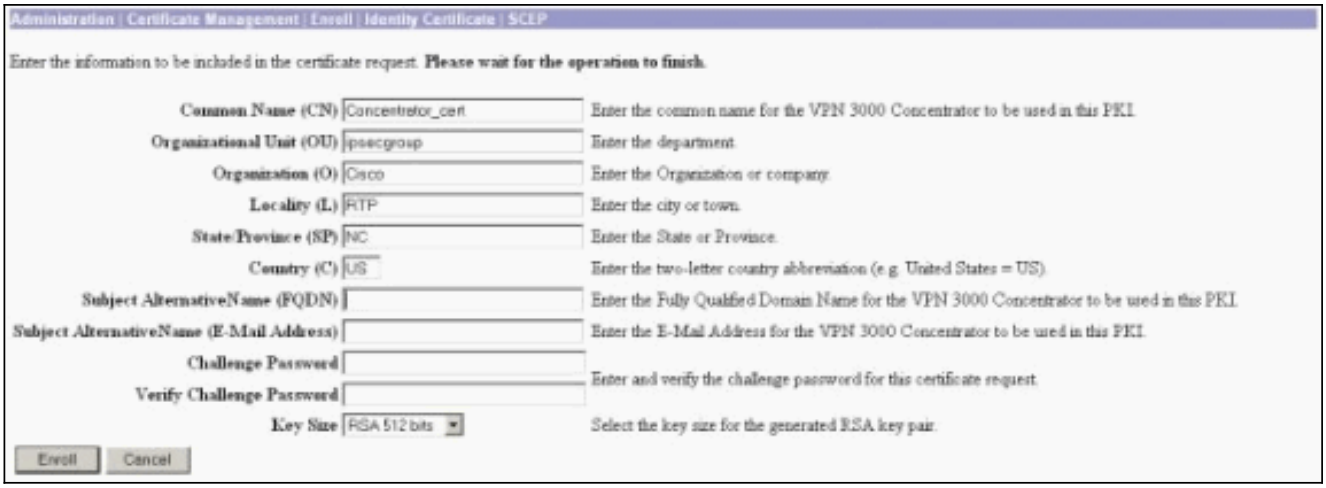
7. ID **인증서를** 신청하려면 **Enroll via SCEP via ...**(SCEP를 통해 등록)를 클릭합니다

.



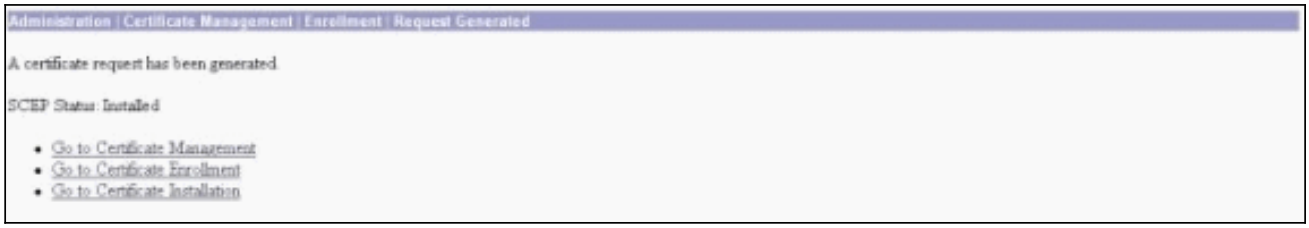
8. 등록 양식을 작성하려면 다음 단계를 완료하십시오.PKI(Public-Key Infrastructure)에서 사용할 VPN Concentrator의 일반 이름을 CN(Common Name) 필드에 입력합니다.OU(조직 구성 단위) 필드에 부서를 입력합니다. OU는 구성된 IPsec 그룹 이름과 일치해야 합니다.조직(O) 필드에 조직 또는 회사를 입력합니다.Locality (L) 필드에 구/군/시를 입력합니다.시/도(SP) 필드에 시/도를 입력합니다.국가(C) 필드에 국가를 입력합니다.PKI에서 FQDN(Fully Qualified Domain Name) 필드에 사용할 VPN Concentrator의 FQDN(Fully Qualified Domain Name)을 입력합니다.PKI에서 사용할 VPN Concentrator의 이메일 주소를 Subject Alternative Name (email Address) 필드에 입력합니다.Challenge Password 필드에 인증서 요청에 대한 챌린지 비밀번호를 입력합니다.Verify Challenge Password 필드에 챌린지 비밀번호를 다시 입력합니다.Key Size(키 크기) 드롭다운 목록에서 생성된 RSA 키 쌍의 키 크기를 선택합니다

.



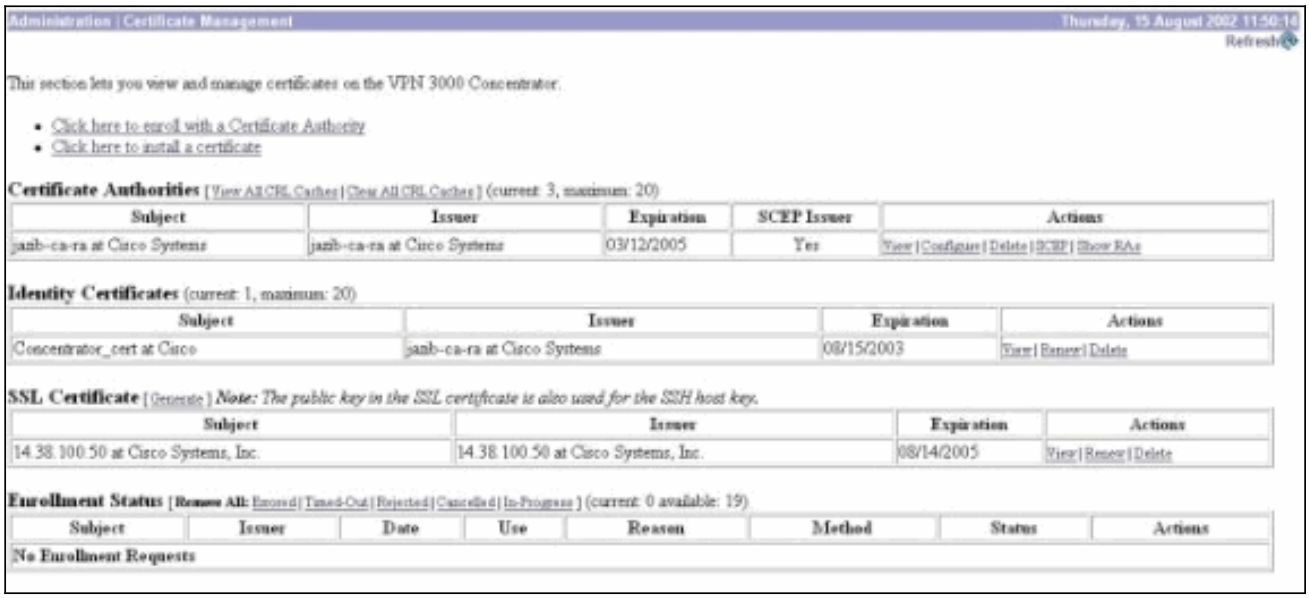
9. Enroll(**등록**)을 선택하고 폴링 상태에서 SCEP 상태를 봅니다.
10. CA 서버로 이동하여 ID 인증서를 승인합니다. CA 서버에서 승인되면 SCEP 상태가 Installed(설치됨)로 표시됩니다

.



11. Certificate Management(인증서 관리)에서 ID 인증서를 확인해야 합니다.그렇지 않은 경우 CA 서버의 로그에서 자세한 트러블슈팅을 확인하십시오

.

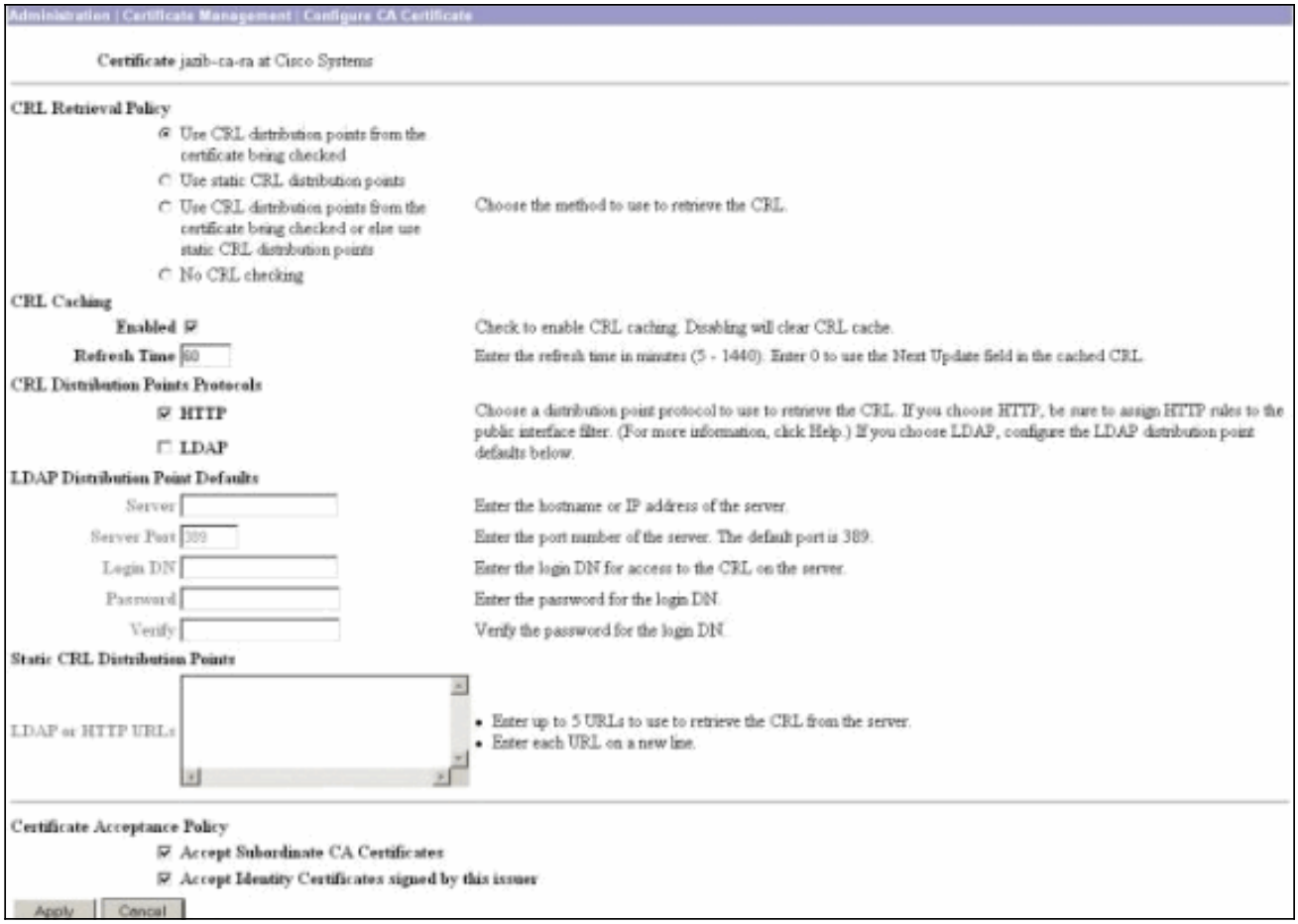


12. 인증서에 CDP(CRL Distribution Point)가 있는지 확인하려면 받은 인증서에 대한 보기를 선택합니다.CDP는 이 인증서의 발급자의 모든 CRL 배포 지점을 나열합니다. 인증서에 CDP가 있고 DNS 이름을 사용하여 CA 서버로 쿼리를 보내는 경우 VPN Concentrator에 정의된 DNS 서버가 IP 주소로 호스트 이름을 확인하도록 해야 합니다. 이 경우 CA 서버의 호스트 이름 예제는 DNS 서버의 IP 주소 172.18.124.96을 확인하는 jazib-pc입니다

.

13. CA 인증서**에서** Configure(구성)를 클릭하여 수신된 인증서에 대한 CRL 확인을 활성화합니다.받은 인증서에 CDP가 있고 이를 사용하려면 **Use CRL distribution points from the certificate를 선택합니다**.시스템이 네트워크 배포 지점에서 CRL을 검색하고 검사해야 하므로 CRL 검사를 활성화하면 시스템 응답 시간이 느려질 수 있습니다. 또한 네트워크가 느리거나 혼잡한 경우 CRL 검사가 실패할 수 있습니다. CRL 캐싱을 활성화하여 이러한 잠재적 문제를 완화합니다. 이렇게 하면 검색된 CRL이 로컬 휘발성 메모리에 저장되므로 VPN Concentrator가 인증서의 폐기 상태를 더 신속하게 확인할 수 있습니다.CRL 캐싱이 활성화된 경우 VPN Concentrator는 먼저 필요한 CRL이 캐시에 있는지 확인하고 인증서의 폐기 상태를 확인해야 할 때 CRL의 일련 번호 목록과 비교하여 인증서의 일련 번호를 확인합니다. 일련 번호가 발견되면 인증서가 폐기된 것으로 간주됩니다. VPN Concentrator는 캐시에서 필요한 CRL을 찾지 못한 경우, 캐시된 CRL의 유효 기간이 만료된 경우 또는 구성된 새로 고침 시간이 경과한 경우 외부 서버에서 CRL을 검색합니다. VPN Concentrator는 외부 서버로부터 새 CRL을 수신하면 새 CRL로 캐시를 업데이트합니다. 캐시는 최대 64개의 CRL을 포함할 수 있습니다.**참고:** CRL 캐시가 메모리에 있습니다. 따라서 VPN Concentrator를 재부팅하면 CRL 캐시가 지워집니다. VPN Concentrator는 새로운 피어 인증 요청을 처리할 때 업데이트된 CRL로 CRL 캐시를 다시 채웁니다.Use static **CRL distribution points(고정 CRL 배포 지점 사용**)를 선택한 경우 이 창에 지정된 대로 최대 5개의 고정 CRL 배포 지점을 사용할 수 있습니다. 이 옵션을 선택하는 경우 하나 이상의 URL을 입력해야 합니다.Use CRL distribution points **from the certificate에서 Use CRL distribution points(CRL 배포 지점 사용)를 선택하거나 Use static CRL distribution points(고정 CRL 배포 지점 사용)를** 선택할 수도 있습니다. VPN Concentrator가 인증서에서 5개의 CRL 배포 지점을 찾을 수 없는 경우 고정 CRL 배포 지점을 최대 5개까지 추가합니다. 이 옵션을 선택하는 경우 하나 이상의 CRL 배포 지점 프로토콜을 활성화합니다. 또한 하나 이상의 고정 CRL 배포 지점을 입력해야 합니다(5개 이하).CRL **확인**을 비활성화하려면 No CRL Checking을 선택합니다.CRL Caching(CRL 캐싱)에서 **Enabled(활성화됨**) 상자를 선택하여 VPN Concentrator가 검색된 CRL을 캐시하도록 허용합니다. 기본값은 CRL 캐싱을 활성화하지 않는 것입니다. CRL 캐싱을 비활성화하면(상자의 선택을 취소) CRL 캐시가 지워집니다.확인 중인 인증서의 CRL 배포 지점을 사용하는 CRL 검색 정책을 구성한 경우 CRL을 검색하는 데 사용할 배포 지점 프로토콜을 선택합니다. 이 경우 **HTTP**를 선택하여 CRL을 검색합니다. CA 서버가 공용 인터페이스를 향하는 경우 공용 인터페이스 필터에 HTTP 규칙을 할당합니다

.



모니터링

Administration(**관리**) > **Certificate Management(인증서 관리)**를 선택하고 View All CRL cache(모든 CRL 캐시 **보기)를** 클릭하여 VPN Concentrator가 CA 서버의 CRL을 캐시했는지 확인합니다.

다음을 확인합니다.

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

Concentrator의 로그

CRL 검사가 작동하는지 확인하기 위해 VPN Concentrator에서 이러한 이벤트를 활성화합니다.

1. 로깅 **수준을** 설정하려면 Configuration > **System** > **Events** > **Classes**를 선택합니다.
2. Class Name(클래스 이름)에서 **IKE**, **IKEDBG**, **IPSEC**, **IPSECDBG** 또는 CERT를 **선택합니다.**
3. Add(추가) 또는 **Modify(수정)**를 클릭하고 **Severity to Log(기록할 심각도) 옵션 1-13을 선택합니다**.
4. 수정하려면 **적용**을 클릭하고, 새 항목을 추가하려면 추가를 클릭합니다.

성공한 Concentrator 로그

CRL 검사에 성공하면 이러한 메시지는 Filterable Event Logs에 표시됩니다.

```
1315 08/15/2002 13:11:23.520 SEV=7 CERT/117 RPT=1
```

```
The requested CRL was found in cache.
The CRL Distribution point is: http://jazib-pc/CertEnroll/jazib-ca-ra.crl

1317 08/15/2002 13:11:23.520 SEV=8 CERT/46 RPT=1
CERT_CheckCrl(62f56e8, 0, 0)

1318 08/15/2002 13:11:23.520 SEV=7 CERT/2 RPT=1
Certificate has not been revoked: session = 2

1319 08/15/2002 13:11:23.530 SEV=8 CERT/50 RPT=1
CERT_Callback(62f56e8, 0, 0)

1320 08/15/2002 13:11:23.530 SEV=5 IKE/79 RPT=2 64.102.60.53
Group [ipsecgroup]
Validation of certificate successful
(CN=client_cert, SN=61521511000000000086)
```

Successful Concentrator 로그의 전체 출력은 Successful Concentrator Logs를 참조하십시오.

실패한 로그

CRL의 체크인이 실패하면 이러한 메시지는 Filterable Event Logs에 표시됩니다.

```
1332 08/15/2002 18:00:36.730 SEV=7 CERT/6 RPT=2
Failed to retrieve revocation list: session = 5

1333 08/15/2002 18:00:36.730 SEV=7 CERT/114 RPT=2
CRL retrieval over HTTP has failed. Please make sure that proper filter rules
have been configured.

1335 08/15/2002 18:00:36.730 SEV=7 CERT/8 RPT=2
Error processing revocation list: session = 5, reason = Failed to retrieve CRL
from the server.
```

실패한 Concentrator 로그의 전체 출력은 폐기된 Concentrator 로그를 참조하십시오.

성공한 클라이언트 로그의 전체 출력은 성공한 클라이언트 로그를 참조하십시오.

실패한 클라이언트 로그의 전체 출력은 폐기된 클라이언트 로그를 참조하십시오.

문제 해결

자세한 문제 해결 정보는 VPN 3000 Concentrator의 연결 문제 해결을 참조하십시오.

관련 정보

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