CA 서버로 구성된 다른 Cisco IOS 라우터에 Cisco IOS 라우터 구성 및 등록

목차

소개

이 문서에서는 Cisco IOS® 라우터를 CA(Certificate Authority) 서버로 구성하는 방법에 대해 설명합니다.또한 CA 서버에서 IPsec 인증을 위한 루트 및 ID 인증서를 얻기 위해 다른 Cisco IOS 라우터를 등록하는 방법을 보여줍니다.

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 IOS Software 릴리스 12.3(4)T3을 실행하는 Cisco 2600 Series 라우터 2개

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.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

인증서 서버에 대한 RSA 키 쌍 생성 및 내보내기

첫 번째 단계는 Cisco IOS CA 서버가 사용하는 RSA 키 쌍을 생성하는 것입니다.라우터(R1)에서 다음 출력에 표시된 대로 RSA 키를 생성합니다.

```
R1(config)#crypto key generate rsa general-keys label cisco1 exportable
The name for the keys will be: cisco1
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]

R1(config)#
*Jan 22 09:51:46.116: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

참고: 인증서 서버에 사용할 키 쌍(*key-label*)에 대해 동일한 이름을 사용해야 합니다(나중에 지원되는 crypto pki server cs-label ***명령을 통해***).

생성된 키 쌍 내보내기

키를 비휘발성 RAM(NVRAM) 또는 TFTP(컨피그레이션에 따라)로 내보냅니다. 이 예에서는 NVRAM이 사용됩니다.구현에 따라 인증서 정보를 저장하기 위해 별도의 TFTP 서버를 사용할 수 있습니다.

```
R1(config)#crypto key export rsa cisco1 pem url nvram: 3des cisco123

% Key name: cisco1
   Usage: General Purpose Key
Exporting public key...
Destination filename [cisco1.pub]?
Writing file to nvram:cisco1.pub
```

```
Exporting private key...
Destination filename [cisco1.prv]?
Writing file to nvram:cisco1.prv
R1(config)#
```

TFTP 서버를 사용하는 경우 다음과 같이 생성된 키 쌍을 다시 가져올 수 있습니다.

```
crypto key import rsa key-label pem [usage-keys] {terminal | url url} [exportable] passphrase
```

참고: 인증서 서버에서 키를 내보내지 않으려면 내보낼 수 없는 키 쌍으로 내보낸 후 인증서 서버로 다시 가져옵니다.이렇게 하면 키를 다시 뗄 수 없습니다.

생성된 키 쌍 확인

생성된 키 쌍을 확인하려면 **show crypto key mypubkey rsa** 명령을 실행합니다.

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

```
R1#show crypto key mypubkey rsa
% Key pair was generated at: 09:51:45 UTC Jan 22 2004
Key name: cisco1
 Usage: General Purpose Key
 Key is exportable.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00CC2DC8 ED26163A
  B3642376 FAA91C2F 93A3825B 3ABE6A55 C9DD3E83 F7B2BD56 126E0F11 50552843
  7F7CA4DA 3EC3E2CE 0F42BD6F 4C585385 3C43FF1E 04330AE3 37020301 0001
% Key pair was generated at: 09:51:54 UTC Jan 22 2004
Key name: cisco1.server
 Usage: Encryption Key
 Key is exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00EC5578 025D3066
  72149A35 32224BC4 3E41DD68 38B08D39 93A1AA43 B353F112 1E56DA42 49741698
  EBD02905 FE4EC392 7174EEBF D82B4475 2A2D7DEC 83E277F8 AEC590BE 124E00E1
  C1607433 5C7BC549 D532D18C DD0B7AE3 AECDDE9C 07AD84DD 89020301 0001
```

라우터에서 HTTP 서버 활성화

Cisco IOS CA Server는 SCEP(Simple Certificate Enrollment Protocol)를 통해서만 등록을 지원합니다. 따라서 이를 가능하게 하려면 라우터가 내장 Cisco IOS HTTP 서버를 실행해야 합니다.**ip http server** 명령을 사용하여 활성화합니다.

```
R1(config)#ip http server
```

라우터에서 CA 서버 활성화 및 구성

다음 단계를 완료하십시오.

1. 인증서 서버는 방금 수동으로 생성한 키 쌍과 동일한 이름을 사용해야 한다는 점을 기억해야

합니다.레이블은 생성된 키 쌍 레이블과 일치합니다.

```
R1(config)#crypto pki server cisco1
```

인증서 서버를 활성화한 후에는 미리 구성된 기본값을 사용하거나 CLI를 통해 인증서 서버의 기능에 대한 값을 지정할 수 있습니다.

2. database **url** 명령은 CA 서버의 모든 데이터베이스 항목이 기록되는 위치를 지정합니다.이 명령을 지정하지 않으면 모든 데이터베이스 항목이 플래시에 기록됩니다.

```
R1(cs-server)#database url nvram:
```

참고: TFTP 서버를 사용하는 경우 URL은 tftp://**<ip_address>/directory**여야 합니다.

3. 데이터베이스 레벨을 구성합니다.

```
R1(cs-server)#database level minimum
```

이 명령은 인증서 등록 데이터베이스에 저장되는 데이터 유형을 제어합니다.**Minimum**(최소) - 충분한 정보가 저장되므로 충돌 없이 새 인증서를 계속 발급하기 위한 목적으로만 충분합니다.기본값.**Names**(이름) - 최소 레벨에서 지정된 정보 외에 각 인증서의 일련 번호와 주체 이름입니다.**Complete**(완료) - 최소 및 이름 레벨에서 지정된 정보 외에 발급된 각 인증서가 데이터베이스에 기록됩니다.**참고: complete** 키워드는 대량의 정보를 생성합니다.이 명령이 실행된 경우 **database url** 명령을 통해 데이터를 저장할 외부 TFTP 서버도 지정해야 합니다.

4. 지정된 DN 문자열로 CA 발급자 이름을 구성합니다.이 예에서는 cisco1.cisco.com의 CN(Common Name), RTP의 L(Locality) 및 미국의 C(Country)가 사용됩니다.

```
R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US
```

5. CA 인증서 또는 인증서의 수명(일)을 지정합니다.유효한 값의 범위는 *1일~1825일입니다*.기본 CA 인증서 수명은 3년이고 기본 인증서 수명은 1년입니다.최대 인증서 수명은 CA 인증서 수명보다 *1*개월 미만입니다.예를 들면 다음과 같습니다.

```
R1(cs-server)#lifetime ca-certificate 365
R1(cs-server)#lifetime certificate 200
```

6. 인증서 서버에서 사용하는 CRL의 수명을 시간 단위로 정의합니다.최대 수명 값은 **336시간**(2주)입니다. 기본값은 **168시간**(1주)입니다.

```
R1(cs-server)#lifetime crl 24
```

7. 인증서 서버에서 발급한 인증서에 사용할 CDP(Certificate-Revocation-List Distribution Point)를 정의합니다.URL은 HTTP URL이어야 합니다.예를 들어, 서버의 IP 주소는 172.18.108.26입니다.

```
R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
```

8. CA 서버를 활성화하려면 **no shutdown** 명령을 실행합니다.

```
R1(cs-server)#no shutdown
```

참고: 인증서 서버를 완전히 구성한 후에만 이 명령을 실행합니다.

인증서 서버에 두 번째 IOS 라우터(R2) 구성 및 등록

다음 절차를 수행합니다.

1. 호스트 이름, 도메인 이름을 구성하고 R2에서 RSA 키를 생성합니다.라우터의 호스트 이름을 R2로 구성하려면 hostname 명령을 사용합니다.

```
Router(config)#hostname R2
R2(config)#
```

hostname 명령을 입력한 후 라우터의 호스트 이름이 즉시 변경되었습니다.라우터에서 도메인 이름을 구성하려면 **ip domain-name** 명령을 사용합니다.

```
R2(config)#ip domain-name cisco.com
```

crypto **key generate rsa** 명령을 사용하여 R2 키 쌍을 생성합니다.

```
R2(config)#crypto key generate rsa
The name for the keys will be: R2.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
```

2. 라우터가 사용해야 하는 CA(이 예에서는 Cisco IOS CA)에 선언하고 신뢰 지점 CA의 특성을 지정하려면 글로벌 컨피그레이션 모드에서 다음 명령을 사용합니다.

```
crypto ca trustpoint cisco
 enrollment retry count 5
 enrollment retry period 3
 enrollment url http://14.38.99.99:80
 revocation-check none
```

참고: crypto **ca trustpoint** 명령**은** 기존 crypto ca identity 명령 및 crypto ca trusted-root 명령을 통합하므로 단일 명령에서 결합된 기능을 제공합니다.

3. crypto ca **authenticate cisco** 명령(cisco는 신뢰 지점 레이블)을 사용하여 CA 서버에서 루트 인증서를 검색합니다.

```
R2(config)#crypto ca authenticate cisco
```

4. 다음을 **등록하고 생성하려면 crypto ca enroll cisco** 명령(cisco는 trustpoint label)을 사용합니다.

```
R2(config)#crypto ca enroll cisco
```

Cisco IOS CA 서버에 성공적으로 등록한 후 show crypto ca certificates 명령을 사용하여 발급된 인증서를 **확인해야 합니다**.명령의 출력입니다.이 명령은 Cisco IOS CA 서버에 구성된 매개변수에 해당하는 자세한 인증서 정보를 표시합니다.

```
R2#show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 02
  Certificate Usage: General Purpose
  Issuer:
    cn=cisco1.cisco.com
    l=RTP
    c=US
  Subject:
    Name: R2.cisco.com
    hostname=R2.cisco.com
  CRL Distribution Point:
 http://172.18.108.26/cisco1cdp.cisco1.crl
Validity Date:
    start date: 15:41:11 UTC Jan 21 2004
    end   date: 15:41:11 UTC Aug 8 2004
    renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: cisco

CA Certificate
  Status: Available
  Certificate Serial Number: 01
```

```
Certificate Usage: Signature
Issuer:
  cn=cisco1.cisco.com
  l=RTP
  c=US
Subject:
  cn=cisco1.cisco.com
  l=RTP
  c=US
Validity Date:
  start date: 15:39:00 UTC Jan 21 2004
  end   date: 15:39:00 UTC Jan 20 2005
Associated Trustpoints: cisco
```

5. 영구 플래시 메모리에 키를 저장하려면 다음 명령을 입력합니다.

```
hostname(config)#write memory
```

6. 컨피그레이션을 저장하려면 다음 명령을 입력합니다.

```
hostname#copy run start
```

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.

- **show crypto ca certificates**—인증서를 표시합니다.
- **show crypto key mypubkey rsa** - 키 쌍을 표시합니다.

```
!% Key pair was generated at: 09:28:16 EST Jan 30 2004
  !Key name: ese-ios-ca
  ! Usage: General Purpose Key
  ! Key is exportable.
  ! Key Data:
  !  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00AF2198
  !  C56F1A8F 5AC501FF ADFB1489 1F503F91 CA3C3FA3 9FB2C150 FFCBF815 2AA73060
  !  E79AF510 E292C171 C6804B45 0CAAD4AF 5834AB85 B204208B 3960D20D 9B51AF7B
  !  ACF12D3D F5BC6EAE 77186AE9 1471F5A4 443CE5B5 1336EC33 5FEB3398 002C15EE
  !  9F8FD331 83490D8A 983FBBE1 9E72A130 121A3B97 A3ACD147 C37DA3D6 77020301 0001
  !% Key pair was generated at: 09:28:17 EST Jan 30 2004
  !Key name: ese-ios-ca.server
  ! Usage: Encryption Key
  ! Key is exportable.
  ! Key Data:
  !  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 0096456A 01AEC6A5
  !  0049CCA7 B41B675E 5317328D DF879CAE DB96A739 26F2A03E 09638A7A 99DFF8E9
  !  18F7635D 6FB6EE27 EF93B3DE 336C148A 6A7A91CB 6A5F7E1B E0084174 2C22B3E2
  !  3ABF260F 5C4498ED 20E76948 9BC2A360 1C799F8C 1B518DD8 D9020301 0001
```

- **crypto pki server ese-ios-ca info crl**—CRL(certificate revocation list)을 표시합니다.

```
! Certificate Revocation List:
  !    Issuer: cn=ese-ios-ca,ou=ESE,o=Cisco Systems Inc,l=Raleigh,st=NC
  !    This Update: 09:58:27 EST Jan 30 2004
  !    Next Update: 09:58:27 EST Jan 31 2004
  !    Number of CRL entries: 0
  !    CRL size: 300 bytes
```

- **crypto pki server ese-ios-ca info requests** - 보류 중인 등록 요청을 표시합니다.

```
! Enrollment Request Database:
  ! ReqID  State      Fingerprint                      SubjectName
```

```
! ------------------------------------------------------------
```

- **show crypto pki server** - 현재 PKI(공개 키 인프라) 서버 상태를 표시합니다.

```
! Certificate Server status: enabled, configured
!    Granting mode is: manual
!    Last certificate issued serial number: 0x1
!    CA certificate expiration timer: 10:58:20 EDT Jun 21 2005
!    CRL NextUpdate timer: 09:58:26 EST Jan 31 2004
!    Current storage dir: nvram:
!    Database Level: Names - subject name data written as .cnm
```

- **crypto pki server** *cs-label* **grant { all |** *transaction-id* **}**—모든 또는 특정 SCEP 요청을 허용합니다.
- **crypto pki server** *cs-label* **reject { all |** *transaction-id* **}**—모든 또는 특정 SCEP 요청을 거부합니다.
- **crypto pki server cs-label password generate [** *minutes* **]** —비밀번호가 유효한 SCEP 요청에 대한 OTP(일회성 비밀번호)를 생성합니다(분 - 시간(분)).유효한 범위는 1~1440분입니다.기본값은 60분입니다.**참고:** 한 번에 하나의 OTP만 유효합니다.두 번째 OTP가 생성된 경우 이전 OTP는 더 이상 유효하지 않습니다.
- **crypto pki server** *cs-label* **revoke** *certificate-serial-number*—**일련 번호**를 기준으로 인증서를 취소합니다.
- **crypto pki server** *cs-label* **request** *pkcs10* **{url** *url* **|** *terminal***} [pem]**—base64 또는 PEM PKCS10 인증서 등록 요청을 요청 데이터베이스에 수동으로 추가합니다.
- **crypto pki server** *cs-label* **info crl** - 현재 CRL의 상태에 대한 정보를 표시합니다.
- **crypto pki server** *cs-label* **info request** - 모든 미해결 인증서 등록 요청을 표시합니다.

자세한 확인 정보는 이 문서의 Verify the Generated Key Pair 섹션을 참조하십시오.

문제 해결

문제 해결 정보는 IP 보안 문제 해결 - 디버그 명령 이해 및 사용을 참조하십시오.

참고: 대부분의 경우 CA 서버를 삭제하고 재정의할 때 문제를 해결할 수 있습니다.

관련 정보

- **IPsec 협상/IKE 프로토콜**
- **기술 지원 및 문서 – Cisco Systems**