Configureer en registreer een Cisco IOS-router aan een andere Cisco IOS-router die als een CA-server is configureren

Inhoud

Inleiding

Dit document beschrijft hoe u een Cisco IOS® router kunt configureren als een CA-server (certificaatinstantie). Bovendien illustreert het hoe te om een andere Cisco IOS router in te schrijven om een wortel en IDD certificaat voor IPsec authenticatie van de CA server te verkrijgen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Twee Cisco 2600 Series routers die Cisco IOS-softwarerelease 12.3(4)T3 uitvoeren.

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Het RSA-toetstitel voor de certificaatserver genereren en exporteren

De eerste stap is het genereren van het RSA sleutelpaar dat de Cisco IOS CA server gebruikt. Op de router (R1), genereer de RSA toetsen zoals deze uitvoer toont:

```
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
```

Opmerking: U moet dezelfde naam gebruiken voor het sleutelpaar (*toetsenbord-label*) dat u van plan bent te gebruiken voor de licentieserver (via de **crypto-***pakketserver cs-label* opdracht dat later is bedekt).

Het gegenereerde sleutelpaar exporteren

Exporteren de toetsen naar niet-vluchtige RAM (NVRAM) of TFTP (gebaseerd op uw configuratie). In dit voorbeeld wordt NVRAM gebruikt. Gebaseerd op uw implementatie, zou u een afzonderlijke server van TFTP kunnen willen gebruiken om uw certificaatinformatie op te slaan.

```
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)#
```

Als u een TFTP-server gebruikt, kunt u het gegenereerde sleutelpaar opnieuw importeren zoals in deze opdracht wordt weergegeven:

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

Opmerking: Als u niet wilt dat de sleutel van uw certificaatserver kan worden geëxporteerd, importeert u deze terug naar de certificaatserver nadat de sleutel is geëxporteerd als een niet-exporteerbaar sleutelpaar. Op deze manier kan de toets niet meer worden uitgeschakeld.

Controleer het gegenereerde toetspatroon

Geef de **show crypto key mypubkey rsa** opdracht uit om het gegenereerde sleutelpaar te controleren.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

```
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
```

Schakel de HTTP-server in op de router

De Cisco IOS CA Server ondersteunt alleen inschrijvingen die gedaan worden via Eenvoudig certificaatinschrijving Protocol (SCEP). Om dit mogelijk te maken, moet de router de ingebouwde Cisco IOS HTTP-server uitvoeren. Gebruik de opdracht **ip http server** om het mogelijk te maken:

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

De CA Server op de router inschakelen en configureren

Voer de volgende stappen uit:

1. Het is zeer belangrijk om te onthouden dat de certificaatserver dezelfde naam moet gebruiken als het sleutelpaar dat u handmatig hebt gegenereerd.Het label komt overeen met het label van het gegenereerde sleutelpaar:
   ```
   R1(config)#crypto pki server cisco1
   ```

   Nadat u een certificaatserver hebt ingeschakeld, kunt u de vooraf ingestelde standaardwaarden gebruiken of waarden via CLI specificeren voor de functionaliteit van de certificaatserver.
2. De **database url** opdracht specificeert de locatie waar alle database items voor de CA server worden uitgeschreven. Als deze opdracht niet is opgegeven, worden alle databases naar Flash geschreven.
   ```
   R1(cs-server)#database url nvram:
   ```

   Opmerking: Als u een TFTP-server gebruikt, moet de URL worden **tftp://<ip_adres>/folder**.
3. Configuratie van het gegevensbestand:
   ```
   R1(cs-server)#database level minimum
   ```

   Deze opdracht bepaalt welk type gegevens in de database van certificaten worden opgeslagen:**Minimaal**—er wordt alleen voldoende informatie opgeslagen om door te gaan met het uitgeven van nieuwe certificaten zonder conflicten. De standaardwaarde.**Namen**—Naast de informatie op het minimale niveau, tevens het serienummer en de onderwerpnaam van elk certificaat.**Volledig** - Naast de informatie in de minimum- en naamniveaus, wordt elk afgegeven certificaat aan de gegevensbank geschreven.**Opmerking:** het **complete** sleutelwoord produceert een grote hoeveelheid informatie. Als het wordt uitgegeven, zou u ook een externe TFTP server moeten specificeren waarin om de gegevens via de **database url** opdracht op te slaan.
4. Configureer de CA emittent naam aan de gespecificeerde DN-string. In dit voorbeeld worden de CN (Common Name) van cisco1.cisco.com, L (Locality) van RTP en C (Land) van de Verenigde Staten gebruikt:
   ```
   R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US
   ```

5. Specificeer de levensduur, in dagen, van een CA-certificaat of een certificaat.Geldige waarden variëren van *1 dag tot 1825 dagen*. De standaard CA-certificaatlevensduur is drie jaar en de standaardcertificaatlevensduur is één jaar. De maximale levensduur van het certificaat is *één maand minder* dan de levensduur van het CA-certificaat. Bijvoorbeeld:
   ```
   R1(cs-server)#lifetime ca-certificate 365
   R1(cs-server)#lifetime certificate 200
   ```
6. Defineer de levensduur, in uren, van het CRL dat door de certificaatserver wordt gebruikt. De maximale levensduur bedraagt **336 uur** (twee weken). De standaardwaarde is **168 uur** (één week).
   ```
   R1(cs-server)#lifetime crl 24
   ```

7. Defineer een Distributiepunt van de Revocatie-Lijst (CDP) om in de certificaten te gebruiken die door de certificaatserver worden verleend.De URL moet een HTTP URL zijn. Onze server had bijvoorbeeld een IP-adres van 172.18.108.26:
```
R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
```

8. Geef de opdracht **no shutdown uit** om de CA server in te schakelen:
```
R1(cs-server)#no shutdown
```

   Opmerking: geef deze opdracht alleen uit nadat u de certificeringsserver volledig hebt ingesteld.

Het configureren en invoeren van de tweede IOS-router (R2) naar de certificaatserver

Volg deze procedure.

1. Configureer een hostname, een domeinnaam en genereer de RSA-toetsen op R2.Gebruik het bevel van de **hostname** om de hostname van de router te vormen om R2 te zijn:
```
Router(config)#hostname R2
R2(config)#
```
   Merk op dat de hostname van de router onmiddellijk veranderde nadat u de opdracht **hostname** had ingevoerd.Gebruik de opdracht **ip-**domeinnaam om de domeinnaam op de router te configureren:
```
R2(config)#ip domain-name cisco.com
```

   Gebruik de **crypto-toets om rsa-**opdracht **te genereren** om het R2-sleutelpaar te genereren:
```
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. Gebruik deze opdrachten in de wereldwijde configuratiemodus om aan CA te verklaren dat uw router (Cisco IOS CA in dit voorbeeld) zou moeten gebruiken en specificeer kenmerken voor de vertrouwde point CA:

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

   Opmerking: De **opdracht crypto ca trustpoint** verenigt de bestaande opdracht **crypto ca** en **crypto kunnen** een **betrouwbare** wortelopdracht krijgen, waardoor een gecombineerde functie onder één opdracht wordt verleend.
3. Gebruik **crypto kan cisco** opdracht **echt verklaren** (cisco is het etiket van het trustpunt) om het wortelcertificaat van de CA server terug te krijgen:
```
R2(config)#crypto ca authenticate cisco
```

4. Gebruik de opdracht **cisco-inrol** (cisco is het **type** trustpunt) van **crypto om** zich in te schrijven

en te genereren:

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

Nadat u zich met succes hebt aangemeld aan de Cisco IOS CA server, dient u de afgegeven certificaten te zien door de opdracht **shows crypto ca certificaten** te gebruiken. Dit is de uitvoer van de opdracht. De opdracht geeft de gedetailleerde certificaatinformatie weer, die overeenkomt met de parameters die in de Cisco IOS CA-server zijn ingesteld:

```
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. Typ deze opdracht om de toets op te slaan in het persistente Flash-geheugen:

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

6. Typ deze opdracht om de configuratie op te slaan:

```
hostname#copy run start
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **toont crypto ca certificaten**—displays certificaten.
- **toon crypto toets mypubkey rsa**-Geeft het sleutelpaar weer.

```
!% 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-server server ese-ios-ca info crl**-Hiermee wordt de lijst met ingetrokken certificaten weergegeven (CRL).

```
! 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 server server ese-ios-ca info verzoeken**-displays hangende inschrijvingsverzoeken.

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

- **Toon crypto pki server**-Toont de huidige openbare zeer belangrijke infrastructuur (PKI) serverstaat.

```
! 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
```

- **gift** ***op het*** **label** ***van*** **een cryptoserver |** alle of specifieke SCEP-verzoeken worden door *de* ***operatie*** ondersteund.
- *cs-label* ***server van crypto-pki wordt niet alle gebruikt | transactie-id*** —wijst alle of specifieke SCEP-verzoeken af.
- **het wachtwoord voor crypto-plosetservers cs-label genereren [** ***minuten***]genereert een eenmalig wachtwoord (OTP) voor een SCEP-verzoek (minuten - lengte van de tijd (in minuten) dat het wachtwoord geldig is. Het geldige bereik loopt van 1 tot 1440 minuten. De standaardinstelling is 60 minuten.**Opmerking:** slechts één OTP is tegelijkertijd geldig. Als een tweede OTP wordt gegenereerd, is de vorige OTP niet langer geldig.
- **cryptografische server** ***cs-label*** **intrekken** ***certificaat-serienummer-*** herroepen op basis van het serienummer van het certificaat.
- **verzoek om** ***pkcs10*** **van een server van crypto pki {url** ***url*** **|** ***terminal*****} [pem]**—voegt handmatig de base64 of PEM PKCS10 certificaatinschrijvingsaanvraag toe aan de aanvraaggegevensbank.

- **Informatie over informatie over de *huidige CRL op een* server** met **crypto-label** informatie over de status van de huidige CRL.
- **crypto server *cs-label* info request** —Hiermee geeft u alle uitstaande aanvragen voor registratie van certificaten weer.

Zie het gedeelte Generated Key pair van dit document controleren voor extra verificatieinformatie.

Problemen oplossen

Raadpleeg IP-beveiligingsproblemen oplossen - Opdrachten voor probleemoplossing begrijpen en gebruiken.

Opmerking: In veel situaties kunt u de problemen oplossen wanneer u de CA server verwijdert en opnieuw definieert.

Gerelateerde informatie

- IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems