# Configuratie en inschrijving van een Cisco VPN 3000 Concentrator aan een Cisco IOS router als een CA Server

### Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Netwerkdiagram Conventies Het RSA-toetstitel voor de certificaatserver genereren en exporteren Het gegenereerde sleutelpaar exporteren Controleer het gegenereerde toetspatroon Schakel de HTTP-server in op de router De CA Server op de router inschakelen en configureren Configuratie en inschrijving van Cisco VPN 3000 Concentrator Verifiëren Problemen oplossen Gerelateerde informatie

## **Inleiding**

Dit document beschrijft hoe u een Cisco IOS® router kunt configureren als een CA-server (certificaatinstantie). Daarnaast wordt geïllustreerd hoe u een Cisco VPN 3000 Concentrator aan de Cisco IOS router kunt aanmelden om een wortel- en ID-certificaat voor IPSec-verificatie 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:

Cisco 2600 Series router die Cisco IOS-softwarerelease 12.3(4)T3 draait

Cisco VPN 3030 Concentrator versie 4.1.2

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 voor meer informatie over documentconventies de technische Tips van Cisco.

### 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. genereren u in de router (R1) de RSA toetsen zoals hieronder te zien is:

R1(config)#crypto key generate rsa general-keys label ciscol exportable
The name for the keys will be: ciscol
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

De toetsen moeten dan worden geëxporteerd naar Non-Volatile 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: ciscol
Usage: General Purpose Key
Exporting public key...
Destination filename [ciscol.pub]?
Writing file to nvram:ciscol.pub
Exporting private key...
Destination filename [ciscol.prv]?
Writing file to nvram:ciscol.prv
Rl(config)#
```

Als u een TFTP-server gebruikt, kunt u het gegenereerde sleutelpaar opnieuw importeren zoals hieronder wordt gezien:

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. Daarom kan de toets niet opnieuw worden uitgeschakeld.

#### Controleer het gegenereerde toetspatroon

U kunt het gegenereerde sleutelpaar controleren door een beroep te doen op de **opdracht** Encrypt**-toets mypubkey rsa**:

Bepaalde opdrachten met **show worden ondersteund door de tool** <u>Output Interpreter (alleen voor</u> <u>geregistreerde klanten)</u>. Hiermee kunt u een analyse van de output van opdrachten met **show genereren**.

```
R1#show crypto key mypubkey rsa
% Key pair was generated at: 09:51:45 UTC Jan 22 2004
Key name: ciscol
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: ciscol.server
Usage: Encryption Key
Key is exportable.
Kev 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**:

R1(config)#ip http server

### De CA Server op de router inschakelen en configureren

Volg deze procedure.

 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 de certificaatinschrijving 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, moet u ook een externe TFTP server 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 (Naam) 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 3 jaar en de standaardcertificaatlevensduur is 1 jaar. De maximale levensduur van het certificaat is 1 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** (2 weken). De standaardwaarde is **168 uur** (1 week). R1(cs-server)#lifetime crl 24

- 7. Defineer een Distributiepunt van de Revocatie-Lijst (CDP) dat in de certificaten moet worden gebruikt die door de certificaatserver worden afgegeven. De URL moet een HTTP URL zijn.Het IP-adres van onze server is bijvoorbeeld 172.18.108.26.
  R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
- 8. Schakel de CA-server in door de opdracht **no shutdown** uit te geven. R1(cs-server)#**no shutdown**

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

### Configuratie en inschrijving van Cisco VPN 3000 Concentrator

Volg deze procedure.

 Selecteer Beheer > certificaatbeheer en kies Klik hier om een CA-certificaat te installeren om het basiscertificaat van Cisco IOS CA Server op te halen.

Subject No Certificate Identity Certi Subject	Authorities ficates (curre	nt: 0, maximum: 20) Issuer	Expiration	Actions				
Subject No Certificate Identity Certi	Authorities	nt: 0, maximum: 20)						
Subject No Certificate	Authorities							
Subject	Issuer		No Certificate Authorities					
	Tannar	Expiration	SCEP Issuer	Actions				
• Click here • <u>Click here</u> • <u>Click here</u> Certificate Au	to install a CA <u>to enroll with a</u> <u>to install a cert</u> u <b>thorities</b> [ <u>9</u>	certificate a Certificate Authority <u>ificate</u> <u>iew All CRL Caches   Cle</u>	<u>ar Ail CRL Caches</u> ] (cu <del>rrent</del> : 0,	mæsimum: 20)				
This section lets y certificate is requ	700 view and m ired before ider	anage certificates on t utity and SSL certifica	he VPN 3000 Concentrator tes can be installed.	Installation of a CA				
				Refresh				

2. Selecteer **SCEP** als de installatiemethode.



3. Voer de URL van de Cisco IOS CA Server, een CA beschrijver in en klik op

**Ophalen.Opmerking:** De juiste URL in dit voorbeeld is http://14.38.99.99/cgi-bin/pkiclient.exe (u moet het volledige pad van /cgi-bin/pkiclient.exe

omvatten).

Administration	Certificate Management   Install   0	CA Certificate   SCEP				
Enter the information needed to retrieve the CA certificate via SCEP. Please wait for the operation to complete.						
URL	http://14.38.99.99/cgi-bin/pkiclient.ex					
CA Descriptor	CB.	Required for some PKI configurations.				
Retrieve	Dancel					

Selecteer **Administratie > certificaatbeheer** om te controleren of het basiscertificaat is geïnstalleerd. Dit getal illustreert de details van het basiscertificaat.

Administration   Ce	dministration   Certificate Management Sunday, 25 January 2004 08:52: Refresh					
This section lets you view and manage certificates on the VPN 3000 Concentrator.						
<u>Click here to</u> <u>Click here to</u> <u>Click here to</u>	enroll with a Certific install a certificate <b>horities</b> (View All C	cate Authority RLCaches   Clea	r Al CRL Caches 1	(current 1. maximum: 20)		
Subject	Issuer	Expiration	SCEP Issuer	Actions		
ciscol.cisco.com	cisco 1. cisco.com	01/20/2005	Yes	View   Configure   Delete   SCEP		
Identity Certificates (current: 0, maximum: 20)           Subject         Issuer         Expiration         Actions						
No Identity Certificates						

4. Selecteer Klik hier om zich bij een certificaatinstantie in te schrijven om het ID-certificaat van

section lets you v					
	riew and manage co	ertificates on th	æ VPN 3000 Co	oncentrator.	
<u>Click here to e</u> <u>Click here to u</u>	moll with a Certific astall a certificate	<u>ate Authority</u>	- A11CDI Contore 1	(current: 1. cuarticum: 20)	
Subject	Issuer	Expiration	SCEP Issuer	Actions	
o1.cisco.com (	cisco1.cisco.com	01/20/2005	Yes	View   Configure   Delete   SCEP	
ntity Certifics Subject	ates (current: 0, ms Issuer	vinun 20)	Expiration	Actions	
No Identity Certificates					

5. Selecteer Inschrijven via SCEP op cisco1.cisco.com (cisco1.cisco.com is de GN van de Cisco IOS CA

Server).

Administration   Certificate Management   Enroll   Identity Certificate
Select the enrollment method for the identity certificate. To install a certificate with SCEP, the issuing CA's certificate must also be installed with SCEP. <u>Click here to install a new CA using SCEP before enrolling</u> .
Enroll via PKCS10 Request (Manual)     Enroll via SCEP at cisco1.cisco.com
<< Go back to Certificate Management

6. Vul het inschrijvingsformulier in door alle informatie in te voeren die in het certificaatverzoek moet worden opgenomen.Klik na voltooiing van het formulier op **Inschrijven** om het registratieverzoek aan de CA server in te dienen.

inter the information to be included Common Name (CN)	in the certificate request. F	Enter the common name for the VPN 3000 Concentrator to be used in this PKI.
Organizational Unit (OU)	TAC	Enter the department.
Organization (0)	Cisco	Enter the Organization or company.
Locality (L)	RTP	Enter the city or town
State/Province (SP)	NC	Enter the State or Province.
Country (C)	US	Enter the two-letter country abbreviation (e.g. United States = $US$ ).
Subject AlternativeName (FQDN)		Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKL
Subject AlternativeName (E- Mail Address)		Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI.
Challenge Password		Enter and verify the challenge password for this
Verify Challenge Password	- 1	certificate request.
Key Size	PSA 512 bits 😁	Select the key size for the generated RSA key pair.

Nadat u op Inschrijven klikt, toont de VPN 3000 Concentrator "Een certificaatverzoek is gegenereerd".

Administration Certificate Management	Enrollment   Request Generated
A certificate request has been generated.	
SCEP Status: Installed	
<ul> <li><u>Go to Certificate Management</u></li> <li><u>Go to Certificate Enrollment</u></li> <li><u>Go to Certificate Installation</u></li> </ul>	

Opm

**erking:** De Cisco IOS CA Server kan worden geconfigureerd om de certificaten automatisch te verlenen met de Cisco IOS CA Server **subsidie automatisch**. Deze opdracht wordt voor dit voorbeeld gebruikt. Als u de gegevens van het ID-certificaat wilt zien, selecteert u **Beheer** > **certificaatbeheer**. Het weergegeven certificaat is vergelijkbaar.

Administration   Certificate Management Sunday, 25 January 2004 F							
This section lets you view and manage certificates on the VPN 3000 Concentrator. <ul> <li><u>Click here to enroll with a Certificate Authority</u></li> <li><u>Click here to install a certificate</u></li> </ul>							
Certificate Authorities [View All CRL Caches   Clear All CRL Caches ] (current: 1, maximum: 20)							
Subject	Issue	и	Expiration	a SCEP Issuer Actions		Actions	
ciscol.cisco.com ciscol.cisco.c		om	01/20/2005	Yes	View	Configure   Daleia   SCEP	
Identity Certificates (current: 1, maximum: 20)							
Subject	Issuer		Expiration		Actions		
rtp-vpn3000 at Cisco		ciscol.cisco.com		08/12/2004		View Renew Delete	

## Verifiëren

Zie <u>Controleer het</u> gedeelte <u>Generated Key</u> pair voor verificatieinformatie.

### Problemen oplossen

Raadpleeg voor informatie over probleemoplossing <u>verbindingsproblemen met VPN 3000</u> <u>Concentrator</u> of <u>IP security probleemoplossing - Oplossingen en gebruik van debug-opdrachten</u>.

## Gerelateerde informatie

- Ondersteuning van Cisco VPN 3000 Series Concentrator-pagina
- <u>Cisco VPN 3000 Series clientondersteuningspagina</u>
- IPsec-ondersteuningspagina
- <u>Technische ondersteuning Cisco-systemen</u>