Konfigurieren und Registrieren eines Cisco VPN 300-Concentrators für einen Cisco IOS-Router als CA-Server

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Netzwerkdiagramm Konventionen Generieren und Exportieren des RSA-Schlüsselpaars für den Zertifikatsserver Exportieren des generierten Schlüsselpaars Überprüfen Sie das generierte Schlüsselpaar. Aktivieren des HTTP-Servers auf dem Router Aktivieren und Konfigurieren des CA-Servers auf dem Router Konfigurieren und Registrieren des Cisco VPN 300 Concentrator Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie Sie einen Cisco IOS®-Router als CA-Server (Certificate Authority) konfigurieren. Außerdem wird veranschaulicht, wie ein Cisco VPN 300 Concentrator beim Cisco IOS-Router angemeldet wird, um ein Root- und ID-Zertifikat für die IPSec-Authentifizierung zu erhalten.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

Cisco Router der Serie 2600 mit Cisco IOS Software, Version 12.3(4)T3

Cisco VPN 3030 Concentrator Version 4.1.2

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions</u>.

Generieren und Exportieren des RSA-Schlüsselpaars für den Zertifikatsserver

Der erste Schritt besteht in der Generierung des RSA-Schlüsselpaars, das vom Cisco IOS CA-Server verwendet wird. Generieren Sie auf dem Router (R1) die RSA-Schlüssel wie folgt:

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
Hinweis: Sie müssen den gleichen Namen für das Schlüsselpaar (Schlüsselb)

Hinweis: Sie müssen den gleichen Namen für das Schlüsselpaar (*Schlüsselbezeichnung*) verwenden, den Sie für den Zertifikatsserver verwenden möchten (über den später beschriebenen Befehl crypto pki server *cs-label*).

Exportieren des generierten Schlüsselpaars

Die Schlüssel müssen dann je nach Konfiguration in einen Non-Volatile RAM (NVRAM) oder

TFTP exportiert werden. In diesem Beispiel wird NVRAM verwendet. Abhängig von Ihrer Implementierung können Sie möglicherweise einen separaten TFTP-Server verwenden, um Ihre Zertifikatsinformationen zu speichern.

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)#
```

Wenn Sie einen TFTP-Server verwenden, können Sie das generierte Schlüsselpaar wie folgt erneut importieren:

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

Hinweis: Wenn der Schlüssel nicht vom Zertifikatsserver exportiert werden soll, importieren Sie ihn zurück zum Zertifikatsserver, nachdem er als nicht exportierbares Schlüsselpaar exportiert wurde. Daher kann der Schlüssel nicht wieder abgenommen werden.

Überprüfen Sie das generierte Schlüsselpaar.

Sie können das generierte Schlüsselpaar überprüfen, indem Sie den Befehl **show crypto key mypubkey rsa** aufrufen:

Bestimmte **show**-Befehle werden vom <u>Output Interpreter Tool</u> unterstützt (nur <u>registrierte</u> Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

```
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.
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
```

```
Aktivieren des HTTP-Servers auf dem Router
```

Der Cisco IOS CA-Server unterstützt nur Registrierungen, die über das Simple Certificate Enrollment Protocol (SCEP) erfolgen. Daher muss der Router den integrierten Cisco IOS HTTP-Server ausführen, um dies zu ermöglichen. Um sie zu aktivieren, verwenden Sie den Befehl **ip http server**:

R1(config)#ip http server

Aktivieren und Konfigurieren des CA-Servers auf dem Router

Befolgen Sie dieses Verfahren.

1. Beachten Sie, dass der Zertifikatsserver den gleichen Namen wie das Schlüsselpaar verwenden muss, das Sie gerade manuell erstellt haben. Die Bezeichnung entspricht dem generierten Schlüsselpaarlabel:

R1(config)#crypto pki server ciscol

Nachdem Sie einen Zertifikatsserver aktiviert haben, können Sie die vorkonfigurierten Standardwerte verwenden oder Werte über CLI für die Funktionalität des Zertifikatsservers angeben.

 Der Datenbank-URL-Befehl gibt den Speicherort an, an dem alle Datenbankeinträge für den CA-Server geschrieben werden.Wenn dieser Befehl nicht angegeben ist, werden alle Datenbankeinträge in Flash geschrieben.
 R1(cs-server)#database url nvram:

Hinweis: Wenn Sie einen TFTP-Server verwenden, muss die URL **tftp://<ip_address>/directory** lauten.

3. Konfigurieren Sie die Datenbankebene: R1(cs-server)#database level minimum

Dieser Befehl steuert, welche Datentypen in der Datenbank für die Zertifikatsregistrierung gespeichert werden. **Minimum**: Es werden genügend Informationen gespeichert, um weiterhin neue Zertifikate ohne Konflikte auszustellen. den Standardwert. **Namen**: Zusätzlich zu den Informationen, die in der Mindeststufe angegeben sind, müssen die Seriennummer und der Betreffname jedes Zertifikats angegeben werden. **Complete (Abgeschlossen)**: Zusätzlich zu den Informationen, die in der Minimal- und der Namensebene angegeben sind, wird jedes ausgestellte Zertifikat in die Datenbank geschrieben. **Hinweis:** Das **vollständige** Schlüsselwort erzeugt eine große Menge an Informationen. Wenn die Daten ausgegeben werden, müssen Sie auch einen externen TFTP-Server angeben, in dem die Daten über den **Datenbank-URL-**Befehl gespeichert werden sollen.

4. Konfigurieren Sie den Namen des CA-Emittenten in die angegebene DN-Zeichenfolge. In diesem Beispiel werden die CN (Common Name) von cisco1.cisco.com, L (Locality) von RTP und C (Country) von US verwendet:
B1 (as server) #issuer percentage and LEPER GEUR

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

5. Geben Sie die Lebensdauer (in Tagen) eines Zertifizierungsstellenzertifikats oder Zertifikats an.Gültige Werte liegen zwischen 1 Tag und 1825 Tagen. Die standardmäßige Lebensdauer des Zertifizierungsstellenzertifikats beträgt 3 Jahre, und die standardmäßige Lebensdauer des Zertifikats beträgt 1 Jahr. Die maximale Lebensdauer eines Zertifikats beträgt 1 Monat

weniger als die Lebensdauer des Zertifizierungsstellenzertifikats. Beispiel: R1(cs-server)#lifetime ca-certificate 365 R1(cs-server)#lifetime certificate 200

6. Definieren Sie die Lebensdauer des vom Zertifikatsserver verwendeten CRL in Stunden. Der maximale Lebenszeitwert beträgt 336 Stunden (2 Wochen). Der Standardwert ist 168 Stunden (1 Woche).

R1(cs-server)#lifetime crl 24

7. Definieren Sie einen CDP (Certificate Revocation List Distribution Point), der in den Zertifikaten verwendet wird, die vom Zertifikatsserver ausgegeben werden. Beim URL muss es sich um eine HTTP-URL handeln.Die IP-Adresse unseres Servers ist beispielsweise 172.18.108.26.

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

8. Aktivieren Sie den CA-Server, indem Sie den Befehl no shutdown eingeben. R1(cs-server) #no shutdown

Hinweis: Geben Sie diesen Befehl nur dann aus, wenn Sie den Zertifikatsserver vollständig konfiguriert haben.

Konfigurieren und Registrieren des Cisco VPN 300 Concentrator

Befolgen Sie dieses Verfahren.

1. Wählen Sie Administration > Certificate Management aus, und klicken Sie hier, um ein CA-Zertifikat zu installieren, um das Stammzertifikat vom Cisco IOS CA-Server abzurufen.

uninisiration [Certificate Ma	nagement	Sunday, 25	January 2004 08:42:4
				Refresh
is section lets y rtificate is requ	70u view and m ired before ider	anage certificates on the ubity and SSL certificates	: VPN 3000 Concentrator s can be installed.	r. Installation of a CA
Click here <u>Click here</u> <u>Click here</u> <u>Click here</u>	to install a CA to enroll with a to install a cert	certificate <u>Certificate Authority</u> <u>ificate</u>		
ertificate Au	uthorities [🕅	iew All CRL Caches Clear .	A <u>fi CRL Caches</u>] (current: O	. maximum 20)
ertificate Au Subject	u thoritie s [<u>17</u> Issuer	iew All CRL Caches Clear. Expiration	A <u>tl CRL Caches</u>] (current: 0 SCEP Issuer	. maximum: 20) Actions
ertificate Au Subject Io Certificate	u thorities [½] Issuer Authorities	iew All CRL Caches Clear. Expiration	A <u>il CRL Caches</u>] (curr ent : 0 SCEP Issuer	Actions
Certificate Au Subject No Certificate dentity Certi	uthorities [½ Issuer Authorities ificates (curre	nt: 0, maximum: 20)	<u>Atl CRL Caches</u>] (current: 0 SCEP Issuer	Actions
Certificate Au Subject No Certificate dentity Certi Subject	uthorities [½ Issuer Authorities ificates (curre	iew All CRL Caches Clear . Expiration ent: 0, maximum: 20) Issuer	A <u>ti CRL Caches</u>] (current: 0 SCEP Issuer Expiration	Actions Actions
Certificate Au Subject No Certificate dentity Certi Subject No Identity Ce	nthorities [½ Issuer Authorities ificates (curre I rtificates	iew All CRL Caches Clear . Expiration ent: 0, maximum: 20) Issuer	A <u>ti CRL Caches</u>] (current: 0 SCEP Issuer Expiration	Actions

2. Wählen Sie als Installationsmethode SCEP



aus.

 Geben Sie die URL des Cisco IOS CA-Servers, einen CA-Deskriptor, ein, und klicken Sie auf Retrieve. Hinweis: Die richtige URL in diesem Beispiel ist http://14.38.99.99/cgibin/pkiclient.exe (Sie müssen den vollständigen Pfad von /cgi-bin/pkiclient.exe angeben).

Administration Certificate Management Install CA Certificate SCEP							
Enter the informa complete.	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	COL	Required for some PKI configurations.					
Retrieve	Dancel						

Wählen Sie Administration > Certificate Management aus, um zu überprüfen, ob das Stammzertifikat installiert wurde. In dieser Abbildung werden die Details des Stammzertifikats

veranschaulicht.

This section lets you view and manage certificates on the VPN 3000 Concentrator. • Click here to enrol with a Certificate Authority • Click here to install a certificate Certificate Authorities [View All CRL Caches Clear All CRL Caches] (current 1, maximum: 20) Subject Issuer Expiration SCEP Issuer Actions ciscol.cisco.com 01/20/2005 Yts View Configure Delete SCEP Identity Certificates (current: 0, maximum: 20) Subject Issuer Expiration Actions No Identity Certificates Issuer	Administration Certificate Management Sunday, 25 January 2004 08:52:23 Refresh@							
Click here to enrol with a Certificate Authority Click here to install a certificate Certificate Authorities [View AllCRL Caches]Clear AllCRL Caches] (current 1, maximum: 20) Subject Issuer Expiration SCEP Issuer Actions ciscol.cisco.com ciscol.cisco.com 01/20/2005 Yes View]Configure Delete SCEP Identity Certificates (current: 0, maximum: 20) Subject Issuer Expiration Actions No Identity Certificates	This section lets you view and manage certificates on the VPN 3000 Concentrator.							
Subject Issuer Expiration SCEP Issuer Actions ciscol.cisco.com ciscol.cisco.com 01/20/2005 Yes View/Configure Delete SCEP Identity Certificates (current: 0, maximum: 20) Subject Issuer Expiration Actions No Identity Certificates	 <u>Click here to enroll with a Certificate Authority</u> <u>Click here to install a certificate</u> <u>Certificate Authorities Litient AUCEL Caches Current 1 maximum: 20</u>) 							
ciscol.cisco.com ciscol.cisco.com 01/20/2005 Yes View/Configure Delete SCEP Identity Certificates (current: 0, maximum: 20) Subject Issuer Expiration Actions No Identity Certificates Issuer Expiration Actions	Subject	Issuer	Expiration	SCEP Issuer	Actions			
Identity Certificates (current: 0, maximum: 20) Subject Issuer Expiration Actions No Identity Certificates Image: Certificates Image: Certificates Image: Certificates	cisco1.cisco.com	cisco 1. cisco.com	01/20/2005	Yes	View Configure Delete SCEP			

4. Klicken Sie **hier, um sich bei einer Zertifizierungsstelle anzumelden**, um das ID-Zertifikat vom Cisco IOS CA-Server zu

					Reffestio
us section lets you	i view and manage c	ertificates on th	æ VPN 3000 Co	oncentrator.	
 <u>Click here to</u> <u>Click here to</u> 	enroll with a Certific install a certificate	ate Authority]		
ertificate Aut	h olities [<u>View All C</u>	RL Caches Clea	r All CRL Caches]	(current: 1, maxim	um: 20)
Subject	Tansa	Ехрианов	SCEP Issuer	Action	s
scol.cisco.com	ciscol.cisco.com	01/20/2005	Yes	<u>View Configure De</u>	lete SCEP
lentity Certifi Subject	cates (current: 0, m. Issuer	aximum 20)	Expiration	Act	ions
-	C				

5. Wählen Sie Anmeldung über SCEP unter cisco1.cisco.com aus (cisco1.cisco.com ist der CN des Cisco IOS CA-

Servers).

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. Füllen Sie das Anmeldeformular aus, indem Sie alle Informationen eingeben, die in der Zertifikatsanforderung enthalten sein müssen.Klicken Sie nach Ausfüllen des Formulars auf Anmelden, um die Registrierungsanfrage für den CA-Server zu starten.

Common Name (CN)	rto-spon3000	Enter the common name for the VPN 3000 Concentrator
	in the state of th	to be used in this PKL
Organizational Unit (OU)	TAC	Enter the department.
Organization (O)	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		certificate request.
Key Size	RSA512 bits 💌	Select the key size for the generated RSA key pair.

Wenn Sie auf Anmelden klicken, wird im VPN 3000-Konzentrator die Meldung "Eine Zertifikatsanforderung wurde erstellt" angezeigt.

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

eis: Der Cisco IOS CA Server kann so konfiguriert werden, dass die Zertifikate automatisch mit dem Unterbefehl für den Cisco IOS CA-Server zugewiesen werden. Dieser Befehl wird für dieses Beispiel verwendet. Um die Details des ID-Zertifikats anzuzeigen, wählen Sie Administration > Certificate Management (Verwaltung > Zertifikatsverwaltung). Das angezeigte Zertifikat ähnelt diesem.

Administration Certificate Management Sunday, 25 January 2004 R								
This section lets you view and manage certificates on the VPN 3000 Concentrator.								
 <u>Click here to enry</u> <u>Click here to inst</u> 	<u>oll with a Certific all a certificate</u>	cate Autho	<u>nty</u>					
Certificate Author	ities [View AllC	RLCaches	Clear All CRL Cach	es](current: 1, mas	amum	: 20)		
Subject	Issue	u .	Expiration	SCEP Is suer		Actions		
cisco 1. cisco. com	cisco1.cisco.c	om	01/20/2005	Yes	View	Configure Delete SCEP		
Identity Certificates (current 1, maximum: 20)								
Subject Issuer Expiration Actions								
rtp-upn3000 at Cisco	ciscol.cis	DO. DOM	08/12/2004		View Renew Delete			

<u>Überprüfen</u>

Informationen zur Überprüfung finden Sie im Abschnitt <u>Überprüfen des generierten</u> <u>Schlüsselpaars</u>.

Fehlerbehebung

Weitere Informationen zur Fehlerbehebung finden Sie unter <u>Beheben von Verbindungsproblemen</u> <u>beim VPN 300-Konzentrator</u> oder <u>IP Security Troubleshooting - Understanding and Using debug</u> <u>Commands</u>.

Zugehörige Informationen

- <u>Support-Seite für Cisco VPN Concentrator der Serie 3000</u>
- <u>Cisco VPN Client Support-Seite der Serie 3000</u>
- IPSec-Support-Seite
- <u>Technischer Support Cisco Systems</u>