Configurer et inscrire un routeur Cisco IOS sur un autre routeur Cisco IOS configuré en tant que serveur d'autorité de certification

Contenu

Introduction

Ce document décrit comment configurer un routeur Cisco IOS® en tant que serveur d'autorité de certification (CA). En outre, il illustre comment inscrire un autre routeur Cisco IOS pour obtenir un certificat racine et ID pour l'authentification IPsec auprès du serveur AC.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Deux routeurs de la gamme Cisco 2600 qui exécutent le logiciel Cisco IOS Version 12.3(4)T3.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Générer et exporter la paire de clés RSA pour le serveur de certificats

La première étape consiste à générer la paire de clés RSA que le serveur AC Cisco IOS utilise. Sur le routeur (R1), générez les clés RSA comme le montre le résultat suivant :

```
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
```

Remarque : Vous devez utiliser le même nom pour la paire de clés (*key-label*) que vous prévoyez d'utiliser pour le serveur de certificats (via la commande **crypto pki server** ***cs-label traitée ultérieurement).***

Exporter la paire de clés générée

Exportez les clés vers la mémoire vive non volatile (NVRAM) ou TFTP (en fonction de votre configuration). Dans cet exemple, la mémoire NVRAM est utilisée. En fonction de votre implémentation, vous pouvez utiliser un serveur TFTP distinct pour stocker vos informations de

certificat.

```
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)#
```

Si vous utilisez un serveur TFTP, vous pouvez réimporter la paire de clés générée comme le montre cette commande :

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

Remarque : si vous ne voulez pas que la clé soit exportable à partir de votre serveur de certificats, réimportez-la sur le serveur de certificats après son exportation en tant que paire de clés non exportable. De cette façon, la clé ne peut plus être retirée.

Vérifier la paire de clés générées

Émettez la commande **show crypto key mypubkey rsa** afin de vérifier la paire de clés générée.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

```
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
```

Activer le serveur HTTP sur le routeur

Le serveur AC Cisco IOS prend uniquement en charge les inscriptions effectuées via le protocole SCEP (Simple Certificate Enrollment Protocol). Par conséquent, afin de rendre cela possible, le routeur doit exécuter le serveur HTTP Cisco IOS intégré. Utilisez la commande **ip http server** afin

de l'activer :

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

Activer et configurer le serveur AC sur le routeur

Procédez comme suit :

1. Il est très important de se rappeler que le serveur de certificats doit utiliser le même nom que la paire de clés que vous venez de générer manuellement.L'étiquette correspond à l'étiquette de paire de clés générée :
   ```
   R1(config)#crypto pki server cisco1
   ```

   Après avoir activé un serveur de certificats, vous pouvez utiliser les valeurs par défaut préconfigurées ou spécifier des valeurs via l'interface de ligne de commande pour la fonctionnalité du serveur de certificats.
2. La commande **database url** spécifie l'emplacement où toutes les entrées de base de données du serveur AC sont écrites. Si cette commande n'est pas spécifiée, toutes les entrées de base de données sont écrites dans Flash.
   ```
   R1(cs-server)#database url nvram:
   ```

   Remarque : si vous utilisez un serveur TFTP, l'URL doit être **tftp://<ip_address>/directory**.
3. Configurez le niveau de base de données :
   ```
   R1(cs-server)#database level minimum
   ```

   Cette commande contrôle le type de données stocké dans la base de données d'inscription de certificat :**Minimum** : suffisamment d'informations sont stockées uniquement pour continuer à émettre de nouveaux certificats sans conflit. Valeur par défaut.**Noms** : en plus des informations fournies au niveau minimal, le numéro de série et le nom de sujet de chaque certificat.**Complète** - En plus des informations fournies dans les niveaux minimal et de noms, chaque certificat émis est écrit dans la base de données.**Note :** Le mot clé **complet** produit une grande quantité d'informations. Si elle est émise, vous devez également spécifier un serveur TFTP externe dans lequel stocker les données via la commande **database url**.
4. Configurez le nom de l'émetteur CA sur la chaîne DN spécifiée. Dans cet exemple, le CN (Common Name) de cisco1.cisco.com, L (Locality) de RTP et C (Country) des États-Unis sont utilisés :
   ```
   R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US
   ```

5. Spécifiez la durée de vie, en jours, d'un certificat CA ou d'un certificat.Les valeurs valides vont de *1 jour à 1 825 jours*. La durée de vie du certificat de l'autorité de certification par défaut est de trois ans et la durée de vie du certificat par défaut est d'un an. La durée de vie maximale du certificat est *inférieure d'un mois* à la durée de vie du certificat de l'autorité de certification. Exemple :
   ```
   R1(cs-server)#lifetime ca-certificate 365
   R1(cs-server)#lifetime certificate 200
   ```
6. Définissez la durée de vie, en heures, de la liste de révocation de certificats utilisée par le serveur de certificats. La durée de vie maximale est de **36 heures** (deux semaines). La valeur par défaut est **168 heures** (une semaine).

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

7. Définissez un CDP (Certificate-Revocation-List Distribution Point) à utiliser dans les certificats émis par le serveur de certificats.L'URL doit être une URL HTTP. Par exemple, notre serveur avait l'adresse IP 172.18.108.26 :
   ```
   R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
   ```

8. Émettez la commande **no shutdown** afin d'activer le serveur AC :
   ```
   R1(cs-server)#no shutdown
   ```

   Remarque : Émettez cette commande uniquement après avoir complètement configuré votre serveur de certificats.

Configuration et inscription du deuxième routeur IOS (R2) au serveur de certificats

Suivez la procédure suivante .

1. Configurez un nom d'hôte, un nom de domaine et générez les clés RSA sur R2.Utilisez la commande **hostname** afin de configurer le nom d'hôte du routeur sur R2 :
   ```
   Router(config)#hostname R2
   R2(config)#
   ```
   Notez que le nom d'hôte du routeur a changé immédiatement après que vous ayez entré la commande **hostname**.Utilisez la commande **ip domain-name** afin de configurer le nom de domaine sur le routeur :
   ```
   R2(config)#ip domain-name cisco.com
   ```

   Utilisez la commande **crypto key generate rsa** afin de générer la paire de clés R2 :
   ```
   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. Utilisez ces commandes en mode de configuration globale afin de déclarer à l'autorité de certification que votre routeur doit utiliser (l'autorité de certification Cisco IOS dans cet exemple) et de spécifier les caractéristiques de l'autorité de certification de point de confiance :

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

   Remarque : La commande **crypto ca trustpoint** unifie la commande **crypto ca identity** et la commande **crypto ca trust-root**, fournissant ainsi des fonctionnalités combinées sous une seule commande.
3. Utilisez la commande **crypto ca authenticate cisco** (cisco est l'étiquette trustpoint) afin de récupérer le certificat racine du serveur AC :

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

4. Utilisez la commande **crypto ca enroll cisco** (cisco est l'étiquette trustpoint) afin d'inscrire et de générer :
```
R2(config)#crypto ca enroll cisco
```

   Une fois que vous êtes inscrit au serveur AC de Cisco IOS, vous devriez voir les certificats émis à l'aide de la commande **show crypto ca certificate**. Voici le résultat de la commande. La commande affiche les informations détaillées sur le certificat, qui correspondent aux paramètres configurés dans le serveur CA Cisco IOS :
```
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. Entrez cette commande afin d'enregistrer la clé dans la mémoire Flash persistante :
```
hostname(config)#write memory
```

6. Entrez cette commande afin d'enregistrer la configuration :
```
hostname#copy run start
```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

- **show crypto ca certificate** : affiche les certificats.
- **show crypto key mypubkey rsa** : affiche la paire de clés.

```
!% 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** : affiche la liste de révocation de certificats (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 pki server ese-ios-ca info request** - Affiche les demandes d'inscription en attente.

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

- **show crypto pki server** - Affiche l'état actuel du serveur PKI (Public Key Infrastructure).

```
! 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 | *tranaction-id*}** - Autorise toutes les demandes SCEP ou certaines.
- **crypto pki server *cs-label* rejeter { all | *tranaction-id*}** - Rejette toutes les demandes SCEP ou certaines.
- **crypto pki server cs-label password generate [*minutes*]**—Génère un mot de passe OTP (one-time password) pour une demande SCEP (minutes - durée (en minutes) pendant laquelle le mot de passe est valide. La plage valide est comprise entre 1 et 1 440 minutes. La valeur par défaut est 60 minutes.**Remarque :** un seul TP est valide à la fois. Si un second OTP est généré, le précédent OTP n'est plus valide.
- **crypto pki server *cs-label* révoke *certificate-serial-number*** —révoque un certificat en fonction de son numéro de série.
- **crypto pki server *cs-label* request *pkcs10* {url *url* | *terminal*} [pem]** : ajoute manuellement la demande d'inscription de certificat Base64 ou PEM PKCS10 à la base de données des demandes.

- **crypto pki server *cs-label* info crl** : affiche des informations sur l'état de la liste de révocation de certificats actuelle.
- **crypto pki server *cs-label* info request** : affiche toutes les demandes d'inscription de certificat en suspens.

Consultez la section Vérifier la paire de clés générée de ce document pour plus d'informations de vérification.

Dépannage

Référez-vous à Dépannage de la sécurité IP - Compréhension et utilisation des commandes de débogage pour obtenir des informations de dépannage.

Remarque : Dans de nombreuses situations, vous pouvez résoudre les problèmes lorsque vous supprimez et redéfinissez le serveur AC.

Informations connexes

- Négociation IPSec/Protocoles IKE
- Support et documentation techniques - Cisco Systems