Configurer et inscrire un concentrateur Cisco VPN 3000 sur un routeur Cisco IOS en tant que serveur d'autorité de certification

Table des matières

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 concentrateur Cisco VPN 3000 sur le routeur Cisco IOS pour obtenir un certificat racine et un certificat d'ID pour l'authentification IPSec.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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

- Routeur de la gamme Cisco 2600 qui exécute le logiciel Cisco IOS Version 12.3(4)T3

- Concentrateur Cisco VPN 3030 version 4.1.2

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 aux 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 utilisée par le serveur Cisco IOS CA. Sur le routeur (R1), générez les clés RSA comme indiqué ici :

```
<#root>

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

Les clés doivent ensuite être exportées 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 éventuellement utiliser un serveur TFTP distinct pour

stocker vos informations de certificat.

<#root>

```
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 indiqué ici :

<#root>

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

Remarque : si vous ne souhaitez pas que la clé soit exportable à partir de votre serveur de certificats, réimportez-la sur le serveur de certificats après l'avoir exportée en tant que paire de clés non exportable. Par conséquent, la clé ne peut pas être retirée à nouveau.

Vérification de la paire de clés générée

Vous pouvez vérifier la paire de clés générée en appelant la commande show crypto key mypubkey rsa :

Certaines commandes show sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

<#root>

```
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 Cisco IOS CA prend uniquement en charge les inscriptions effectuées via le protocole SCEP (Simple Certificate Enrollment Protocol). Par conséquent, pour que cela soit possible, le routeur doit exécuter le serveur HTTP Cisco IOS intégré. Pour l'activer, utilisez la commande ip http server :

```
<#root>

R1(config)#
ip http server
```

Activer et configurer le serveur AC sur le routeur

Suivez la procédure suivante .

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 :

   <#root>

   ```
   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 pour le serveur AC sont écrites.

   Si cette commande n'est pas spécifiée, toutes les entrées de la base de données sont écrites dans Flash.

   <#root>

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

   Remarque : si vous utilisez un serveur TFTP, l'URL doit être tftp://<adresse_ip>/directory.

3. Configurez le niveau de base de données :

   <#root>

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

   Cette commande contrôle le type de données stocké dans la base de données d'inscription de certificats.

   - Minimum - Suffisamment d'informations sont stockées uniquement pour continuer à émettre de nouveaux certificats sans conflit ; la valeur par défaut.

- Noms : outre les informations fournies dans le niveau minimal, le numéro de série et le nom du sujet de chaque certificat.
- Complet : en plus des informations fournies dans les niveaux minimal et de noms, chaque certificat émis est écrit dans la base de données.

Remarque : le mot clé complete 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 de l'autorité de certification sur la chaîne DN spécifiée. Dans cet exemple, le CN (Common Name) de cisco1.cisco.com, L (Locality) de RTP et C (Country) de US sont utilisés :

```
<#root>

R1(cs-server)#

issuer-name CN=cisco1.cisco.com L=RTP C=US
```

5. Spécifiez la durée de vie, en jours, d'un certificat d'autorité de certification ou d'un certificat.

   Les valeurs valides vont de 1 jour à 1 825 jours. La durée de vie du certificat d'autorité de certification par défaut est de 3 ans et la durée de vie du certificat par défaut est de 1 an. La durée de vie maximale du certificat est inférieure d'un mois à la durée de vie du certificat d'autorité de certification. Exemple :

```
<#root>

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 (2 semaines). La valeur par défaut est 168 heures (1 semaine).

```
<#root>

R1(cs-server)#

lifetime crl 24
```

7. Définissez un point de distribution de liste de révocation de certificats (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, l'adresse IP de notre serveur est 172.18.108.26.

   ```
   <#root>

   R1(cs-server)#

   cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
   ```

8. Activez le serveur AC en émettant la commande no shutdown.

   ```
   <#root>

   R1(cs-server)#

   no shutdown
   ```

   Remarque : n'émettez cette commande qu'après avoir entièrement configuré votre serveur de certificats.

Configuration et inscription du concentrateur Cisco VPN 3000

Suivez la procédure suivante .

1. Sélectionnez Administration > Certificate Management et choisissez Click here to install a CA certificate pour récupérer le certificat racine du serveur de l'autorité de certification Cisco IOS.
2. Sélectionnez SCEP comme méthode d'installation.
3. Entrez l'URL du serveur CA Cisco IOS, un descripteur CA, et cliquez sur Récupérer.

   Remarque : l'URL correcte dans cet exemple est http://14.38.99.99/cgi-bin/pkiclient.exe (vous devez inclure le chemin d'accès complet de /cgi-bin/pkiclient.exe).

   Sélectionnez Administration > Certificate Management pour vérifier que le certificat racine a été installé. Cette figure illustre les détails du certificat racine.
4. Sélectionnez Cliquez ici pour vous inscrire auprès d'une autorité de certification afin d'obtenir le certificat d'ID auprès du serveur CA Cisco IOS.
5. Sélectionnez Enroll via SCEP sur cisco1.cisco.com (cisco1.cisco.com est le CN du serveur

CA Cisco IOS).

6. Remplissez le formulaire d'inscription en saisissant toutes les informations à inclure dans la demande de certificat.

   Une fois le formulaire rempli, cliquez sur Enroll pour commencer la demande d'inscription au serveur AC.

   Après avoir cliqué sur Enroll, le concentrateur VPN 3000 affiche « Une demande de certificat a été générée ».

   Remarque : le serveur Cisco IOS CA peut être configuré pour accorder automatiquement les certificats à l'aide de la sous-commande Cisco IOS CA Server grant automatic. Cette commande est utilisée pour cet exemple. Pour afficher les détails du certificat d'ID, sélectionnez Administration > Certificate Management. Le certificat affiché est similaire à celui-ci.

Vérifier

Consultez la section Vérifier la paire de clés générée pour obtenir des informations de vérification.

Dépannage

Pour des informations de dépannage, référez-vous à Dépannage des problèmes de connexion sur le concentrateur VPN 3000 ou à Dépannage de sécurité IP - Compréhension et utilisation des commandes de débogage.

Informations connexes

- Page d'assistance des concentrateurs VPN Cisco 3000
- Page d'assistance du Client VPN 3000 Series Cisco
- Page d'assistance IPsec
- Support technique - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.