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

Contenu

Introduction

Ce document décrit comment configurer un routeur de Cisco IOS® en tant que serveur d'Autorité de certification (CA). Supplémentaire, il illustre comment s'inscrire un concentrateur de Cisco VPN 3000 au routeur Cisco IOS pour obtenir une racine et un certificat d'ID pour l'authentification d'IPSec.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

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

- Version 4.1.2 de Concentrateur Cisco VPN 3030

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

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.

Générez et exportez la paire de clés RSA pour le serveur de certificat

La première étape est de générer la paire de clés RSA que le serveur du Cisco IOS CA utilise. Sur le routeur (R1), générez les clés RSA comme vu ici :

```
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
```

Note: Vous devez employer le même nom pour la paire de clés (clé-*étiquette*) cette vous plan pour utiliser pour le serveur de certificat (par l'intermédiaire de la commande de Cs-*étiquette de* ***crypto pki server*** couverte plus tard).

Exportez les paires de clé générée

Les clés doivent alors être exportées à la mémoire vive non volatile (NVRAM) ou au TFTP (basé sur votre configuration). Dans cet exemple, NVRAM est utilisé. Basé sur votre implémentation, vous pourriez potentiellement vouloir utiliser un serveur distinct TFTP 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 les paires de clé générée comme vu ici :

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

Note: Si vous ne voulez pas que la clé soit exportable de votre serveur de certificat, importez-la de nouveau au serveur de certificat après qu'elle ait été exportée comme paire de clés non-exportable. Par conséquent, la clé ne peut pas être enlevée de nouveau.

Vérifiez les paires de clé générée

Vous pouvez vérifier les paires de clé générée en appelant la commande de **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.

```
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
```

Activez le serveur HTTP sur le routeur

Le serveur du Cisco IOS CA prend en charge seulement des inscriptions faites par l'intermédiaire de l'inscription de certificat simple Protocol (SCEP). En conséquence, afin de faire ce possible, le routeur doit exécuter le serveur HTTP intégré de Cisco IOS. Pour l'activer, utilisez la commande d'**ip http server** :

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

Activez et configurez le serveur CA sur le routeur

Suivez cette procédure.

1. Il est très important de se souvenir que le serveur de certificat doit utiliser le même nom que la paire de clés vous juste a manuellement généré. L'étiquette apparie l'étiquette de paires de clé générée :
   ```
   R1(config)#crypto pki server cisco1
   ```

   Après que vous ayez activé un serveur de certificat, vous pouvez utiliser les valeurs par défaut préconfigurées ou spécifier des valeurs par l'intermédiaire du CLI pour la fonctionnalité du serveur de certificat.
2. La commande de **database url** spécifie l'emplacement où toutes les entrées de base de données pour le serveur CA sont écrites.Si cette commande n'est pas spécifiée, toutes les entrées de base de données sont écrites pour flasher.
   ```
   R1(cs-server)#database url nvram:
   ```

   Note: Si vous utilisez un serveur TFTP, l'URL doit être **tftp:// <ip_address>/directory**.
3. Configurez la database level :
   ```
   R1(cs-server)#database level minimum
   ```

   Cette commande contrôle quel type de données est enregistré dans la base de données d'inscription de certificat.**Minimum** — Assez d'informations sont stockées pour continuer seulement de délivrer de nouveaux Certificats sans conflit ; la valeur par défaut.**Noms** — En plus des informations fournies dans le niveau minimal, le numéro de série et le nom du sujet de chaque certificat.**Complet** — En plus des informations fournies aux niveaux minimaux et de noms, chaque certificat délivré est écrit à la base de données.**Note**: Le mot clé **complet** produit un grand nombre d'informations. S'il est émis, vous devez également spécifier un serveur externe TFTP en lequel pour enregistrer les données par l'intermédiaire du **database url** commandez.
4. Configurez le nom d'émetteur CA à la Dn-chaîne spécifiée. Dans cet exemple, la NC (nom commun) de cisco1.cisco.com, L (localité) de RTP, et C (pays) des USA sont utilisés :
   ```
   R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US
   ```

5. Spécifiez la vie, en quelques jours, d'un certificat de CA ou d'un certificat.Les valeurs valides s'étendent de *1 jour à 1825 jours*. La vie par défaut de certificat de CA est de **3 ans** et la vie par défaut de certificat est de **1 an**. La vie maximum de certificat est de *1 mois moins* que la vie du certificat de CA. Exemple :
   ```
   R1(cs-server)#lifetime ca-certificate 365
   R1(cs-server)#lifetime certificate 200
   ```
6. Définissez la vie, en quelques heures, du CRL qui est utilisé par le serveur de certificat. La valeur maximum de vie est de **336 heures** (2 semaines). La valeur par défaut est de **168 heures** (1 semaine).
   ```
   R1(cs-server)#lifetime crl 24
   ```

7. Définissez un point de distribution de liste des révocations de certificat (CDP) à utiliser dans les Certificats qui sont délivrés par le serveur de certificat. L'URL doit être un URL HTTP.Par exemple, l'adresse IP de notre serveur est 172.18.108.26.
   ```
   R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
   ```

8. Activez le serveur CA en n'émettant l'**aucune commande shutdown**.
   ```
   R1(cs-server)#no shutdown
   ```

   Note: Émettez cette commande seulement après que vous avez complètement configuré

votre serveur de certificat.

Configurez et inscrivez-vous le concentrateur de Cisco VPN 3000

Suivez cette procédure.

1. En sélectionnant l'**Administration > Certificate Management** et choisissez **a cliquez ici pour installer un certificat de CA** pour récupérer le certificat racine du serveur du Cisco IOS CA.
2. **SCEP** choisi comme méthode d'installation.
3. Écrivez l'URL du serveur du Cisco IOS CA, un descripteur CA, et le clic **récupèrent**.**Note**: L'URL correct 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 l'**Administration > Certificate Management** pour vérifier que le certificat racine a été installé. Cette figure montre les détails de certificat racine.
4. Choisi **a cliquez ici pour s'inscrire avec une autorité de certification** pour obtenir le certificat d'ID du serveur du Cisco IOS CA.
5. Choisi **inscrivez-vous par l'intermédiaire de SCEP chez cisco1.cisco.com** (cisco1.cisco.com est la NC du serveur du Cisco IOS CA).
6. Remplissez le formulaire d'inscription en écrivant toutes les informations à inclure dans la demande de certificat.Àla fin de la forme, le clic **s'inscrivent** pour commencer la demande d'inscription au serveur CA.Après que vous clic vous inscriviez, le concentrateur VPN 3000 affiche « une demande de certificat a été généré ».**Note**: Le serveur du Cisco IOS CA peut être configuré pour accorder automatiquement les Certificats avec la **concession de** commande secondaire de serveur du Cisco IOS CA **automatique**. Cette commande est utilisée pour cet exemple. Pour voir les détails de l'ID délivrent un certificat, **Administration > Certificate Management** choisi. Le certificat affiché est semblable à ceci.

Vérifiez

Voyez que le vérifier que les paires de clé générée sectionnent pour les informations de vérification.

Dépannez

Pour information l'information de dépannage, référez-vous aux problèmes de connexion de dépannage sur le dépannage de concentrateur VPN 3000 ou de sécurité IP - en comprenant et en utilisant 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