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 autre routeur Cisco IOS pour obtenir une racine et un certificat d'ID pour l'authentification d'IPsec du serveur CA.

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 :

- Deux Routeurs de gamme Cisco 2600 qui exécutent la version du logiciel Cisco IOS 12.3(4)T3.

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 à 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 cette sortie affiche :

```
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 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

Exportez les clés 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 vouloir utiliser un serveur distinct TFTP afin de 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 cette commande montre :

```
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 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. De cette façon, la clé ne peut pas être enlevée de nouveau.

Vérifiez les paires de clé générée

Émettez la commande de **show crypto key mypubkey rsa** afin de vérifier les paires de clé 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
```

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. Employez la commande d'**ip http server** afin de l'activer :

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

Activez et configurez le serveur CA sur le routeur

Procédez comme suit :

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:`**Remarque:** 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.**Remarque:** Le mot clé **complet** produit un grand nombre d'informations. S'il est émis, vous devriez 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. Sur 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 trois ans et la vie par défaut de certificat est d'un an. La vie maximum de certificat est d'*un 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** (deux semaines). La valeur par défaut est de **168 heures** (une semaine).`R1(cs-server)#lifetime crl 24`
7. Définissez un point de distribution de liste des révocations de certificat (CDP) pour l'utiliser dans les Certificats qui sont délivrés par le serveur de certificat.L'URL doit être un URL HTTP. Par exemple, notre serveur a eu une adresse IP de 172.18.108.26 :`R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl`

8. N'émettez l'**aucune commande shutdown** afin d'activer le serveur CA :`R1(cs-server)#no shutdown`**Remarque:** Émettez cette commande seulement après que vous avez complètement configuré votre serveur de certificat.

Configurez et inscrivez-vous le deuxième routeur IOS (R2) au serveur de certificat

Suivez cette procédure.

1. Configurez une adresse Internet, un domain-name, et générez les clés RSA sur R2.Employez la commande d'**adresse Internet** afin de configurer l'adresse Internet du routeur pour être R2 :`Router(config)#hostname R2R2(config)#`Notez que l'adresse Internet du routeur a changé juste après que vous avez sélectionné la commande d'**adresse Internet**.Employez la commande d'**ip domain-name** afin de configurer le nom de domaine sur le routeur :`R2(config)#ip domain-name cisco.com`Employez la commande de **crypto key generate rsa** afin de générer la paire de clés R2 :`R2(config)#crypto key generate rsaThe name for the keys will be: R2.cisco.comChoose the size of the key modulus in the range of 360 to 2048 for yourGeneral Purpose Keys. Choosing a key modulus greater than 512 may takea few minutes.How many bits in the modulus [512]:% Generating 512 bit RSA keys ...[OK]`
2. Employez ces commandes en mode de configuration globale afin de déclarer au CA que votre routeur devrait utiliser (Cisco IOS CA dans cet exemple) et spécifier des caractéristiques pour le point de confiance CA :`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 de **crypto ca trustpoint** unifie la commande existante de **crypto ca identity** et la commande de **crypto ca trusted-root**, fournissant de ce fait la fonctionnalité combinée sous une commande simple.
3. Employez la commande de **Cisco de crypto ca authenticat** (Cisco est l'étiquette de point de confiance) afin de récupérer le certificat racine du serveur CA :`R2(config)#crypto ca authenticate cisco`
4. Employez la commande de **Cisco de crypto ca enroll** (Cisco est l'étiquette de point de confiance) afin de s'inscrire et se produire :`R2(config)#crypto ca enroll ciscoAprès` s'être avec succès inscrit au Cisco IOS CA le serveur, vous devriez voir les Certificats délivrés à l'aide du **show crypto ca certificat de** commande. C'est la sortie de la commande. La commande affiche les informations détaillées de certificat, qui correspondent aux paramètres configurés dans le serveur du Cisco IOS CA :`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. Sélectionnez cette commande afin de sauvegarder la clé à la mémoire flash persistante :`hostname(config)#write memory`
6. Sélectionnez cette commande afin de sauvegarder la configuration :`hostname#copy run start`

Vérifiez

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 certificat** ? Certificats d'affichages.
- **show crypto key mypubkey rsa** ? Affiche la paire de clés.`hostname#`**`copy run start`**
- **crl de l'information du crypto pki server ese-IOS-Ca** ? Affiche le Liste des révocations de certificat (CRL).`hostname#`**`copy run start`**
- **demandes de l'information du crypto pki server ese-IOS-Ca** ? Demandes en attendant d'inscription d'affichages.`hostname#`**`copy run start`**
- **show crypto pki server** ? Affiche l'état en cours de serveur d'Infrastructure à clés publiques (PKI).`hostname#`**`copy run start`**
- **concession de Cs-***étiquette de* **crypto pki server {toute |** *transaction - id***}** ? Accorde tous ou des demandes de la particularité SCEP.
- **anomalie de Cs-***étiquette de* **crypto pki server {toute |** *transaction - id***}** ? Rejette tous ou des demandes de la particularité SCEP.
- **le mot de passe de Cs-étiquette de crypto pki server se produisent [des** *minutes***]** ? Génère un mot de passe une fois (OTP) pour une demande SCEP (minutes - durée (en quelques minutes) qui le mot de passe est valide. La plage valide est de 1 à 1440 minutes. Le par défaut est de 60 minutes.**Remarque:** Seulement un OTP est valide à la fois. Si un deuxième OTP est généré, l'OTP précédent n'est plus valide.
- *la Cs-étiquette de* **crypto pki server retirent le certificat-séquentiel-***nombre* ? Retire un certificat basé sur son numéro de série.
- **demande** *pkcs10* **{***URL de Cs-étiquette de* **crypto pki server URL |** *terminal***} [PEM]** ? Ajoute manuellement la demande base64 ou d'inscription de certificat PEM PKCS10 à la base de données de demande.
- **crl de l'information de Cs-***étiquette de* **crypto pki server** ? Affiche des informations concernant le statut du courant CRL.
- **demande de l'information de Cs-***étiquette de* **crypto pki server** ? Affiche toutes les demandes exceptionnelles d'inscription de certificat.

Voyez le vérifier la section de paires de clé générée de ce document pour les informations supplémentaires de vérification.

Dépannez

Référez-vous au dépannage de sécurité IP - Comprenant et utilisant des commandes de débogage pour information l'information de dépannage.

Remarque: Dans beaucoup de situations, vous pouvez résoudre les problèmes quand vous supprimez et redéfinissez le serveur CA.

Informations connexes

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