Contenu

Introduction

Ce document fournit une configuration d'échantillon pour le RÉSEAU LOCAL dynamique au RÉSEAU LOCAL VPN entre les Routeurs de Cisco IOS® qui utilisent des Certificats numériques tout en utilisant la caractéristique d'Autorité de certification (CA) IOS. Ce document explique comment configurer le serveur IOS CA avec configurer un routeur Cisco IOS afin d'obtenir un certificat d'identité par l'intermédiaire de l'inscription automatique.

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 Cisco 2851 qui exécute le Logiciel Cisco IOS version 12.4(6)T
- Routeur de Cisco 871 qui exécute la version du logiciel Cisco IOS 12.3(14)YT1

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.

Conventions

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

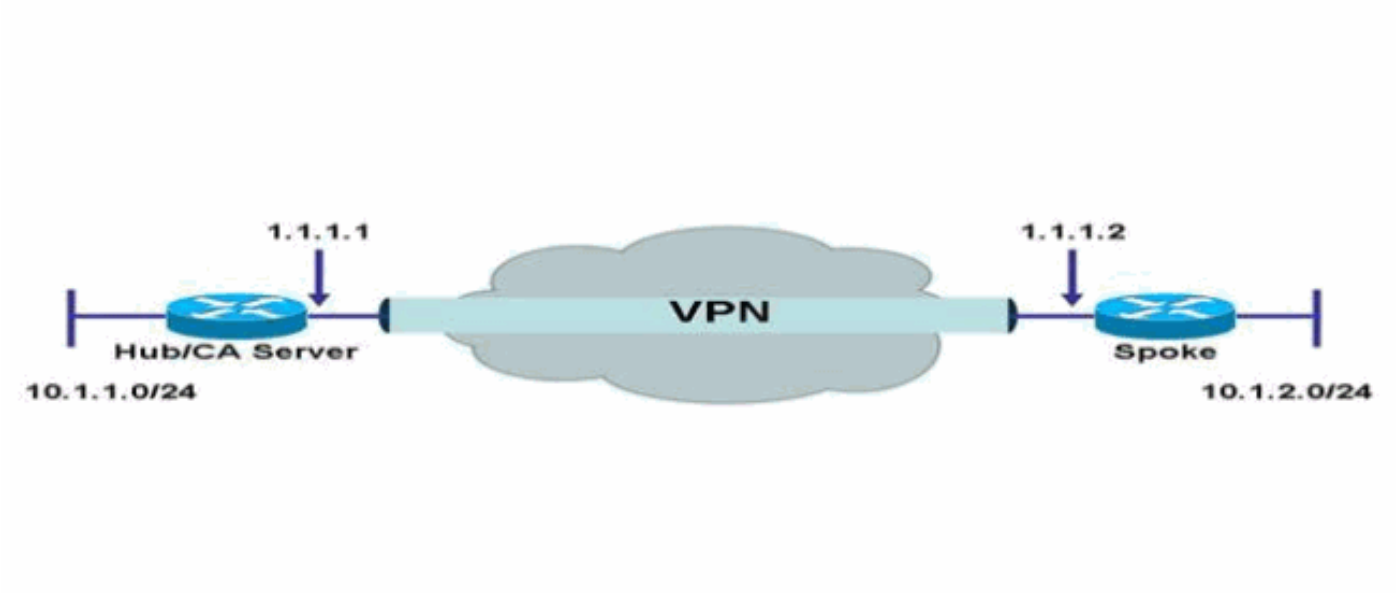
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes :

- Configurez le serveur IOS CA sur le routeur
- Authentifiez et inscrivez-vous à un serveur IOS CA
- Configuration du concentrateur
- Configuration du rayon

Configurez le serveur IOS CA sur le routeur

Terminez-vous ces étapes afin de configurer le serveur IOS CA sur le routeur :

1. Émettez la commande de **crypto pki server** afin d'entrer les paramètres pour la configuration du serveur IOS CA.Dans ce cas, l'étiquette qui est donnée à la configuration du serveur IOS CA est **Cisco**. L'étiquette peut être quelque chose que vous voudriez.`HubIOSCA(config)#`**`crypto pki server cisco`**
2. Émettez la commande secondaire d'**issuer-name** afin de définir les informations de certificat.Dans ce cas, le nom commun (NC), la localité (l), l'état (St), et le code de pays (c) sont définis en tant qu'affiché ici :`HubIOSCA(cs-server)#`**`issuer-name CN=iosca.cisco.com L=RTP ST=NC C=US`**
3. Émettez la commande de **concession**.Dans ce cas, le serveur IOS accorde automatiquement un certificat au client.`HubIOSCA(cs-server)#`**`grant auto`**
4. N'émettez l'**aucune** commande **fermée** afin d'activer le serveur IOS CA.`HubIOSCA(cs-server)#`**`no`**

shutAprès que vous sélectionniez cette commande, vous êtes incité à entrer dans un mot de passe pour protéger la clé privée.Quelques configurations de serveur ne peuvent pas être changées après génération de certificat de CA. Entrez dans un mot de passe pour protéger la clé privée ou pour écrire le **retour à la** sortie.`HubIOSCA(cs-server)#no shut`

Authentifiez et inscrivez-vous à un serveur IOS CA

Le serveur de certificat a également un point de confiance automatiquement généré du même nom. Le point de confiance enregistre le certificat du serveur de certificat. Après que le routeur le détecte qu'un point de confiance est utilisé pour enregistrer le certificat du serveur de certificat, le point de confiance verrouille de sorte qu'il ne puisse pas être modifié.

1. Avant que vous configuriez le serveur de certificat, vous pouvez émettre la commande de **crypto pki trustpoint** afin de manuellement créer et installer ce point de confiance.Ceci te permet pour spécifier une paire de clés RSA alternative (utilisant la commande de **rsakeypair**).**Remarque:** Le point de confiance automatiquement généré et le certificat de serveur de certificat ne sont pas disponibles pour l'identité de périphérique de serveur de certificat. Par conséquent, n'importe quelle interface de ligne de commande (CLI), comme la commande d'**ip http secure-trustpoint**, qui est utilisée pour spécifier le point de confiance CA pour obtenir des Certificats et pour authentifier le certificat se connectant du client doit indiquer un point de confiance supplémentaire configuré sur le périphérique de serveur de certificat.Si le serveur est un serveur de certificat racine, il emploie les paires de clés RSA et plusieurs autres attributs pour générer un certificat auto-signé. Le certificat de CA associé a ces extensions d'utilisation principale :Signature numériqueSigne de certificatSigne de Liste des révocations de certificat (CRL)Dans ce cas, le routeur de HubIOSCA est inscrit avec un certificat utilisant un point de confiance différent afin de pouvoir établir un tunnel VPN avec le routeur en étoile. Définissez un point de confiance, comme affiché ici (l'iosca est le nom donné à ce nouveau point de confiance) :`HubIOSCA(config)#crypto pki trustpoint iosca`
2. Écrivez l'URL d'inscription, comme affiché ici :`HubIOSCA(ca-trustpoint)#enrollment url http://1.1.1.1:80`Dans ce cas, un contrôle de révocation CRL n'est pas fait.`HubIOSCA(ca-trustpoint)#revocation-check none`
3. Émettez la commande d'**iosca de crypto ca authenticat** afin de recevoir le certificat racine.`HubIOSCA(config)#crypto ca authenticate iosca`Le certificat a ces attributs :`Fingerprint MD5: 441446A1 CA3C32B6 3B680204 452A00B2 Fingerprint SHA1: 6C09E064 E4B09087 DDFFADCD 2E9C6853 1669BF39Do you accept this certificate? [yes/no]: yesTrustpoint CA certificate accepted.`
4. Émettez la commande d'**iosca de crypto ca enroll** afin d'obtenir le certificat d'identité.`Start certificate enrollment... Create a challenge password. You need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons, your password is not saved in the configuration. Please make a note of it.Password:Re-enter password: The subject name in the certificate includes: HubIOSCA.cisco.com Include the router serial number in the subject name? [yes/no]: no Include an IP address in the subject name? [no]: no Request certificate from CA? [yes/no]: yes Certificate request sent to Certificate Authority The show crypto ca certificate iosca verbose command shows the fingerprint.`
5. Émettez la **crypto** commande de **CERT de PKI d'exposition** afin de vérifier que les Certificats ont été installés.`HubIOSCA#show crypto pki certCertificate Status: Available Certificate Serial Number: 02 Certificate Usage: General Purpose Issuer: cn=iosca.cisco.com L\=RTP ST\=NC C\=US Subject: Name: HubIOSCA.cisco.com hostname=HubIOSCA.cisco.com Validity Date: start date: 19:11:55 UTC Aug 11 2006 end date: 19:11:55 UTC Aug 11 2007 Associated Trustpoints: iosca CA Certificate Status: Available Certificate Serial Number: 01 Certificate Usage: Signature Issuer: cn=iosca.cisco.com L\=RTP ST\=NC C\=US Subject: cn=iosca.cisco.com L\=RTP ST\=NC C\=US Validity Date: start date: 19:01:54 UTC Aug 11 2006 end date: 19:01:54 UTC Aug 10 2009 Associated Trustpoints: iosca cisco`**Remarque:** Puisque le serveur CA est également un

pair d'IPSec, le routeur concentrateur doit authentifier et s'inscrire au serveur CA qui est sur le même routeur.

Configuration du concentrateur

Configuration du concentrateur
HubIOSCA#**show crypto pki cert**Certificate Status: Available Certificate Serial Number: 02 Certificate Usage: General Purpose Issuer: cn=iosca.cisco.com L\=RTP ST\=NC C\=US Subject: Name: HubIOSCA.cisco.com hostname=HubIOSCA.cisco.com Validity Date: start date: 19:11:55 UTC Aug 11 2006 end date: 19:11:55 UTC Aug 11 2007 Associated Trustpoints: iosca CA Certificate Status: Available Certificate Serial Number: 01 Certificate Usage: Signature Issuer: cn=iosca.cisco.com L\=RTP ST\=NC C\=US Subject: cn=iosca.cisco.com L\=RTP ST\=NC C\=US Validity Date: start date: 19:01:54 UTC Aug 11 2006 end date: 19:01:54 UTC Aug 10 2009 Associated Trustpoints: iosca cisco

Configuration du rayon

Configuration du rayon
HubIOSCA#**show crypto pki cert**Certificate Status: Available Certificate Serial Number: 02 Certificate Usage: General Purpose Issuer: cn=iosca.cisco.com L\=RTP ST\=NC C\=US Subject: Name: HubIOSCA.cisco.com hostname=HubIOSCA.cisco.com Validity Date: start date: 19:11:55 UTC Aug 11 2006 end date: 19:11:55 UTC Aug 11 2007 Associated Trustpoints: iosca CA Certificate Status: Available Certificate Serial Number: 01 Certificate Usage: Signature Issuer: cn=iosca.cisco.com L\=RTP ST\=NC C\=US Subject: cn=iosca.cisco.com L\=RTP ST\=NC C\=US Validity Date: start date: 19:01:54 UTC Aug 11 2006 end date: 19:01:54 UTC Aug 10 2009 Associated Trustpoints: iosca cisco

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

L'authentification de certificat échoue pour un tunnel L2L.

Parfois, la négociation IPSec peut échouer quand vous utilisez un certificat de CA valide pour l'authentification d'ISAKMP. La négociation de tunnel VPN fonctionne avec des clés pré-partagées parce que les clés pré-partagées sont les paquets vraiment petits. Si l'authentification de certificat doit envoyer le certificat entier à travers, ceci crée de grands paquets qui obtient fragmenté. La fragmentation empêche le certificat à authentifier correctement entre les périphériques.

Diminuez le MTU et commutez à bidirectionnel simultané afin de résoudre ce problème. Placez la valeur de MTU à une taille qui ne doit pas être fragmentée :

```
Router(config)#interface type [slot_#/]port_#Router(config-if)#ip mtu MTU_size_in_bytes
```

Informations connexes

- Support et documentation techniques - Cisco Systems