Configuration de VPN Client 3.x pour obtenir un certificat numérique

Contenu

Introduction

Ce document explique comment configurer le Client VPN Cisco 3.x pour obtenir un certificat numérique.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur un PC qui exécute le Client VPN Cisco 3.x.

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.

Configurer le client VPN

Terminez-vous ces étapes pour configurer le client vpn.

1. **Le début** choisi > **programme** > **client vpn de Cisco Systems Inc.** > **gestionnaire de certificat** pour lancer le gestionnaire de certificat de client vpn.
2. Sélectionnez l'onglet personnel de Certificats et cliquez sur New.**Remarque:** Des Certificats d'ordinateur pour authentifier des utilisateurs pour des connexions VPN ne peuvent pas être faits avec IPsec.
3. Quand le client vpn vous incite pour un mot de passe, spécifiez un mot de passe pour protéger le certificat. N'importe quelle exécution qui exige l'accès à la clé privée du certificat exige du mot de passe spécifié de continuer.
4. Sélectionnez le **fichier** pour demander un certificat utilisant le format PKCS #10 à la page d'inscription. Cliquez ensuite sur **Next**.
5. Cliquez sur **parcourent**, et spécifient un nom du fichier pour le fichier de demande de certificat. Pour le type de fichier, le **PEM** choisi **a encodé le fichier de demande (*.req)** et la **sauvegarde de** clic.
6. Cliquez sur Next à la page d'inscription de client vpn.
7. Complétez les champs sur la forme d'inscription.Cet exemple affiche les champs :Nom commun = User1Service = IPSECCERT (ceci devrait apparier l'unité organisationnelle (OU) et le nom de groupe sur le concentrateur VPN 3000.)Société = Cisco SystemsÉtat = Caroline du NordPays = les USAEmail = User1@email.comAdresse IP = (facultatif ; utilisé pour spécifier l'adresse IP sur la demande de certificat)Domaine = cisco.comCliquez sur Next quand vous êtes fait.
8. Cliquez sur Finish pour procéder à l'inscription.
9. Sélectionnez l'onglet de demandes d'inscription pour vérifier la demande sur le gestionnaire de certificat de client vpn.
10. Amenez le serveur de l'autorité de certification (CA) et le client vpn relie simultanément pour soumettre la demande.
11. Sélectionnez la **demande un certificat** et cliquez sur Next sur le serveur CA.
12. **La demande avancée** choisie du type de demande et cliquent sur Next.
13. Choisi **soumettez une demande de certificat utilisant un fichier PKCS encodé par base64 #10 ou une demande de renouvellement utilisant un fichier PKCS encodé par base64 #7** sous des demandes avancées de certificat, et puis cliquez sur Next.
14. Mettez en valeur le fichier de demande de client vpn, et collez-le au serveur CA sous la demande enregistrée. Cliquez sur Submit alors.
15. Sur le serveur CA, délivrez le certificat d'identité pour la demande de client vpn.
16. Téléchargez la racine et les certificats d'identité au client vpn. Sur le serveur CA, sélectionnez le **contrôle sur un certificat en attente**, et puis cliquez sur Next.
17. **Base** choisie **64 encodée**. Cliquez sur Download alors le **certificat de CA** sur le serveur CA.
18. Sélectionnez un fichier pour télécharger le récupérer de la page de certificat de CA ou de liste des révocations de certificat pour obtenir le certificat racine sur le serveur CA. Cliquez ensuite sur **Next**.
19. **Le gestionnaire** choisi > le **certificat de CA** > l'**importation de certificat sur le client vpn**, et sélectionnent alors le fichier de la racine CA pour installer la racine et les certificats d'identité.
20. **Le gestionnaire** choisi de **certificat** > les **Certificats personnels** > l'**importation**, et choisissent le fichier de certificat d'identité.
21. Assurez-vous que le certificat d'identité apparaît sous l'onglet personnel de Certificats.
22. Assurez-vous que le certificat racine apparaît sous l'onglet de Certificats CA.

Vérifiez

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

Dépannez

Quand vous tentez de s'inscrire avec le serveur de Microsoft CA, il peut générer ce message d'erreur.

```
Initiating online request
Generating key pair
Generating self-signed Certificate
Initiating online request
Received a response from the CA
Your certificate request was denied
```

Si vous recevez ce message d'erreur, référez-vous aux logs de Microsoft CA pour des détails, ou référez-vous à ces pour en savoir plus de ressources.

- Windows ne peut pas trouver une autorité de certification qui traite la demande
- XCCC : « Votre demande de certificat a été refusée » le message d'erreur se produit quand vous demandez un certificat pour des conférences Secure

Informations connexes

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