Configuration du concentrateur Cisco VPN 3000 version 4.7.x pour obtenir un certificat numérique et un certificat SSL

Contenu

Introduction

Ce document comporte des instructions pas à pas sur la façon dont configurer les Concentrateurs de la gamme Cisco VPN 3000 authentifier avec l'utilisation de numérique ou des certificats d'identité et des Certificats SSL.

Remarque: Dans le concentrateur VPN, l'Équilibrage de charge doit être désactivé avant que vous génériez un autre certificat ssl puisque ceci empêche la génération de certificat.

Référez-vous à comment obtenir un certificat numérique de Microsoft Windows CA utilisant l'ASDM sur une ASA afin d'apprendre un scénario plus à peu près identique avec PIX/ASA 7.x.

Référez-vous à l'inscription de certificat de Cisco IOS utilisant l'exemple amélioré de configuration de commandes d'inscription afin d'apprendre un scénario plus à peu près identique avec des Plateformes de Cisco IOS®.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur le concentrateur de Cisco VPN 3000 qui exécute la version 4.7.

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.

Installez les Certificats numériques sur le concentrateur VPN

Procédez comme suit :

1. Choisissez l'**Administration > Certificate Management > s'inscrivent** afin de sélectionner la demande numérique ou de certificat d'identité.
2. Choisissez l'**Administration > Certificate Management > l'inscription > le certificat d'identité** et le clic **s'inscrivent par l'intermédiaire de PKCS10 Request(Manual)**.
3. Complétez les champs demandés, et cliquez sur alors **s'inscrivent**.Ces champs sont complétés cet exemple.**Nom commun** — altiga30**Unité organisationnelle** — IPSECCERT (l'OU devrait apparier le groupname configuré d'IPsec)**Organisation** — Cisco Systems**Localité** — RTP**État/province** — La Caroline du Nord**Pays** — Les USA**Nom de domaine complet** — (non utilisé ici)**Taille de clé** — 512**Remarque:** Si vous demandez un certificat ssl ou un certificat d'identité utilisant l'inscription de certificat simple Protocol (SCEP), ce sont les seules options RSA disponibles.Bits RSA 512Bits RSA 768Bits RSA 1024Bits RSA 2048Bits DSA 512Bits DSA 768Bits DSA 1024
4. Après que vous clic **vous inscriviez**, plusieurs fenêtres apparaissent. La première fenêtre confirme que vous avez demandé un certificat.Une nouvelle fenêtre du navigateur également ouvre et affiche votre fichier de demande PKCS.
5. Sur votre serveur de l'autorité de certification (CA), mettez en valeur la demande et collez-la dans votre serveur CA afin de soumettre votre demande. Cliquez sur **Next** (Suivant).
6. **La demande avancée** choisie et cliquent sur Next.
7. 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**, et puis cliquez sur Next.
8. Coupez-collez votre fichier PKCS dans le champ texte sous la section enregistrée de demande. Cliquez sur Submit alors.
9. Délivrez le certificat d'identité sur le serveur CA.
10. Téléchargez la racine et les certificats d'identité. Sur votre serveur CA, sélectionnez le **contrôle sur un certificat en attente**, et cliquez sur Next.
11. **La base** choisie **64 encodée**, et cliquent sur Download le **certificat de CA** sur le serveur CA.
12. Sauvegardez le certificat d'identité sur votre lecteur local.
13. Sur le serveur CA, choisi **récupérez le certificat de CA ou la liste des révocations de certificat** afin d'obtenir le certificat racine. Cliquez ensuite sur **Next**.
14. Sauvegardez le certificat racine sur votre lecteur local.
15. Installez la racine et les certificats d'identité sur le concentrateur VPN 3000. Afin de faire ceci, la **gestion** choisie > le **gestionnaire** > l'**installation de certificat > installent le certificat obtenu par l'intermédiaire de l'inscription**. Sous l'état d'inscription, le clic **installent**.

16. Cliquez sur Upload le **fichier du poste de travail**.
17. Cliquez sur **parcourent** et sélectionnent le fichier de certificat racine que vous avez enregistré à votre lecteur local.Choisi **installez** pour installer le certificat d'identité sur le concentrateur VPN. La gestion **|** La fenêtre de Gestion de certificat apparaît comme confirmation, et votre nouveau certificat d'identité apparaît dans la table de certificats d'identité.**Remarque:** Terminez-vous ces étapes pour générer un nouveau certificat si le certificat échoue.**Administration > Certificate Management** choisi.Cliquez sur Delete dans la case d'actions pour répertorier de certificat ssl.**Réinitialisation** choisie de **gestion >** de **système**.Sélectionnez la **sauvegarde la configuration active à la période de la réinitialisation**, choisissez **maintenant**, et cliquez sur Apply. Vous pouvez maintenant générer un nouveau certificat après que la recharge soit complète.

Installez les Certificats SSL sur le concentrateur VPN

Si vous utilisez une connexion sécurisée entre votre navigateur et le concentrateur VPN, le concentrateur VPN exige un certificat ssl. Vous avez besoin également d'un certificat ssl sur l'interface que vous utilisez pour gérer le concentrateur VPN et pour le webvpn, et pour chaque interface qui termine des tunnels de webvpn.

Les Certificats SSL d'interface, s'inexistants, sont automatiquement générés quand les réinitialisations de concentrateur VPN 3000 après que vous amélioriez le logiciel de concentrateur VPN 3000. Puisqu'un certificat auto-signé auto-est généré, ce certificat n'est pas vérifiable. Aucune autorité de certification n'a garanti son identité. Mais ce certificat te permet pour établir le contact initial avec le concentrateur VPN utilisant le navigateur. Si vous voulez le remplacer par un autre certificat ssl auto-signé, terminez-vous ces étapes :

1. Choisissez l'**Administration > Certificate Management**.
2. Cliquez sur **se produisent** afin d'afficher le nouveau certificat dans la table de certificat ssl et remplacer existant.Cette fenêtre te permet pour configurer des champs pour le SSL délivre un certificat le concentrateur VPN se produit automatiquement. Ces Certificats SSL sont pour des interfaces et pour l'Équilibrage de charge.Si vous voulez obtenir un certificat ssl vérifiable (c'est-à-dire, un émis par une autorité de certification), voyez les Certificats numériques d'installer sur la section de concentrateur VPN de ce document afin d'utiliser la même procédure que vous utilisez pour obtenir des certificats d'identité. Mais cette fois, sur l'**Administration > Certificate Management > s'inscrivent la** fenêtre, **certificat ssl de** clic (au lieu du certificat d'identité).**Remarque:** Référez-vous à la *gestion | Section Gestion de certificat de* volume de référence de concentrateur VPN 3000 II : Gestion et version 4.7 de surveillance pour des informations complètes sur des Certificats numériques et des Certificats SSL.

Renouvelez les Certificats SSL sur le concentrateur VPN

Cette section décrit comment renouveler les Certificats SSL :

Si c'est pour le certificat ssl généré par le concentrateur VPN, allez à l'**Administration > Certificate Management** sur la section SSL. Cliquez sur l'option de **renouveler**, et cela renouvelle le certificat ssl.

Si c'est pour un certificat accordé par un serveur externe CA, terminez-vous ces étapes :

1. Choisissez le **>Delete d'Administration > Certificate Management** sous des *Certificats SSL* afin de supprimer les Certificats expirés de l'interface publique.Clic **oui** afin de confirmer la suppression du certificat ssl.
2. Choisissez l'**Administration > Certificate Management > se produisent** afin de générer le nouveau certificat ssl.Le nouveau certificat ssl pour l'interface publique apparaît.

Informations connexes

- Page d'assistance des concentrateurs VPN Cisco 3000
- Négociation IPSec/Protocoles IKE
- Support et documentation techniques - Cisco Systems