Contenu

Introduction

Tous les Certificats numériques ont construits à temps le temps d'expiration dans le certificat qui est assigné par le serveur émettant d'Autorité de certification (CA) pendant l'inscription. Quand un certificat numérique est utilisé pour l'authentification VPN IPSec de l'ISAKMP, il y a un contrôle automatique du temps d'expiration du certificat du périphérique de communication et de l'heure système sur le périphérique (point final VPN). Ceci s'assure qu'un certificat utilisé est valide et n'a pas expiré. Il est également pourquoi vous *devez* régler l'horloge interne sur chaque point final VPN (routeur). Si le Protocole NTP (Network Time Protocol) (ou le protocole de diffusion du temps en réseau (SNTP) [SNTP]) n'est pas possible sur les cryptos Routeurs VPN, alors utilisez la commande **réglée d'horloge de** manuel.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur tous les Routeurs qui exécutent l'image pour cette plate-forme respective.

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 de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Quand est-ce qu'un certificat numérique considéré n'a pas expiré

ou est expiré ?

- Un certificat est expiré (non valide) si l'heure système a lieu après le temps d'expiration de certificat ou avant la période émise du certificat.
- Un certificat n'est pas expiré (valide) si l'heure système est ou entre au certificat délivré temps et le temps expiré du certificat.

Le but de la caractéristique d'auto-enroll est de fournir à l'administrateur CA un mécanisme pour permettre à un routeur actuellement inscrit re-pour s'inscrire automatiquement avec son serveur CA sur un pour cent configuré de la vie du certificat de routeur. C'est une importante caractéristique pour la gestionnabilité/prise en charge des Certificats comme mécanisme de contrôle. Si vous utilisiez un CA particulier pour fournir des Certificats potentiellement aux milliers de routeurs VPN de branchement avec une vie d'un an (sans auto-enroll), alors pendant exactement une année du temps émis, tous les Certificats expirent et tous les branchements perdent la Connectivité par IPSec. Alternativement, si la caractéristique d'auto-enroll est placée au « auto-enroll 70", le comme indiqué dans cet exemple, puis dans 70% de la vie du certificat délivré (1 an), chaque routeur fournit automatiquement une nouvelle demande d'inscription au serveur du Cisco IOS® CA répertorié dans le point de confiance.

Remarque: Une exception à la caractéristique d'auto-enroll est que si elle est placée *inférieur ou égal à 10*, alors elle a lieu en quelques minutes. S'il est *plus grand que 10*, alors c'est un pourcentage de la vie du certificat.

Il y a quelques mises en garde que l'administrateur du Cisco IOS CA doit se rendre compte de avec l'auto-enroll. L'administrateur doit exécuter ces actions pour que la re-inscription soit réussi :

1. Manuellement accordez ou rejetez chaque demande de re-inscription sur le serveur du Cisco IOS CA (à moins que le « grant auto » est utilisé sur le serveur du Cisco IOS CA).Le serveur du Cisco IOS CA doit toujours accorder ou rejeter chacune de ces derniers des demandes (avec la supposition que le Cisco IOS CA n'a pas le « grant auto » activé). Cependant, aucune mesure administrative sur le routeur de inscription n'est exigée pour commencer le procédé de re-inscription.
2. Sauvegardez le nouveau certificat re-inscrit dans le routeur VPN de re-inscription, si approprié.S'il n'y a aucun changement de configuration unsaved en suspens du routeur, alors le nouveau certificat est automatiquement enregistré à la mémoire vive non volatile (NVRAM). Le nouveau certificat est écrit dans le NVRAM et le certificat précédent est retiré.S'il y a les modifications de configuration unsaved en suspens, alors vous devez émettre la commande de **début de passage de copie** sur le routeur de inscription afin de sauvegarder les modifications de configuration et le nouveau certificat re-inscrit dans le NVRAM. Une fois que la commande de **début de passage de copie** est terminée, puis le nouveau certificat est écrit dans le NVRAM et le certificat précédent est retiré.**Remarque:** Quand une nouvelle re-inscription est réussie, cela ne retire pas le certificat précédent pour cela périphérique inscrit sur le serveur CA. Quand les périphériques VPN communiquent, ils s'envoient le numéro de série de certificat (un numéro unique).**Remarque:** Par exemple, si vous êtes à 70% de la vie du certificat et un branchement VPN était re-de s'inscrire avec le CA, ce CA a deux Certificats pour cette adresse Internet. Cependant, le routeur de inscription a seulement un (le plus nouvel). Si vous choisissez à, vous pouvez administrativement retirer le vieux certificat, ou permettez-lui pour expirer normalement.**Remarque:** Les versions plus nouvelles de code de la caractéristique d'auto-enroll ont une option « de régénérer » les paires de clés utilisées pour

l'inscription.Cette option est « non par défaut » pour régénérer des paires de clés.Si cette option était choisie, rendez-vous compte de l'ID de bogue Cisco CSCea90136. Ce correctif de bogue tient compte pour que la nouvelle paire de clés soit mise dans des fichiers temporaires tandis que la nouvelle inscription de certificat a lieu au-dessus d'un tunnel existant d'IPSec (qu'utilise la vieille paire de clés).L'auto-enroll a l'option de générer de nouvelles clés au temps de renouvellement de certification. Actuellement ceci entraîne une perte de service pendant le temps où elle prend pour obtenir un nouveau certificat. C'est parce qu'il y a une nouvelle clé mais aucun certificat qui l'apparie.Ce featurette retient la vieux clé et certificat jusqu'à ce que le nouveau certificat soit disponible.La génération de clés automatique est également mise en application pour l'Inscription manuelle. Des clés sont générées (comme nécessaire) pour automatique ou l'Inscription manuelle.Version trouvée - 12.3PIH03Version à être dedans réparé - 12.3TVersion appliquée à - 12.3PI03Intégré dedans - AucunPour information les informations complémentaires, support technique de Cisco de contact.

Informations connexes

- Page d'assistance IPsec
- Support technique - Cisco Systems