Exemple de configuration de chiffrement de clés prépartagées d'un routeur Cisco IOS

Contenu

Introduction

La version logicielle 12.3(2)T de Cisco IOSMD introduit une fonctionnalité qui permet au routeur de chiffrer la clé pré-partagée ISAKMP dans un format sécurisé de type 6 dans la mémoire RAM non-volatile (NVRAM). La clé pré-partagée à chiffrer peut être configurée en tant que norme, sous un porte-clés ISAKMP, en mode agressif ou comme mot de passe de groupe dans une installation de serveur ou client EzVPN. Cet exemple de configuration montre comment configurer le cryptage des clés pré-partagées existantes et nouvelles.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur cette version de logiciel :

- Logiciel Cisco IOS version 12.3(2)T

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

Cette section vous présente avec les informations que vous pouvez employer pour configurer les caractéristiques ce document décrit.

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

Ces deux nouvelles commandes sont introduites afin d'activer le chiffrement à clé pré-partagé :

- **key config-key password-encryption** ***[clé principale]***
- **password encryption aes**

[Clé principale] est le mot de passe/clé utilisée pour chiffrer toutes autres clés en configuration de routeur avec l'utilisation d'un chiffrement symétrique anticipé de la norme de chiffrement (AES). La clé principale n'est pas enregistrée en configuration de routeur et *ne peut pas* être vue ou obtenue de quelque façon tandis que connectée au routeur.

Une fois que configurée, la clé principale est utilisée pour chiffrer toutes les clés existantes ou nouvelles en configuration de routeur. Si *[clé principale]* n'est pas spécifié sur la ligne de commande, le routeur incite l'utilisateur à introduire la clé et à la ressaisir pour la vérification. Si une clé existe déjà, l'utilisateur est incité à introduire la vieille clé d'abord. Des clés ne sont pas chiffrées jusqu'à ce que vous émettiez la commande de **password encryption aes**.

La clé principale peut être changée (bien que ceci ne devrait pas être nécessaire à moins que la clé soit devenue compromise d'une certaine façon) en émettant la commande de **key config-key…** de nouveau avec le nouveau *[clé principale]*. Toutes les clés chiffrées existantes en configuration de routeur re-sont chiffrées avec la nouvelle clé.

Vous pouvez supprimer la clé principale quand vous n'émettez l'**aucun key config-key….** Cependant, ceci rend toutes les clés actuellement configurées en configuration de routeur inutiles (des affichages de message d'avertissement qui détaille ceci et confirme la suppression de clé principale). Puisque la clé principale n'existe plus, les mots de passe du type 6 ne peuvent pas être décryptés et utilisés par le routeur.

Remarque: Pour des raisons de sécurité, ni la suppression de la clé principale, ni la suppression du **password encryption aes** ne commandent des unencrypts les mots de passe en configuration de routeur. Une fois que des mots de passe sont chiffrés, ils ne sont pas décryptés. Les clés chiffrées existantes dans la configuration peuvent encore être décryptées ont fourni la clé principale n'est pas retirées.

Supplémentaire, afin de voir des messages de debug-type des fonctions de cryptage de mot de passe, utilisez la commande de **password logging** dans le mode de configuration.

Configurations

Ce document utilise ces configurations sur le routeur :

- Chiffrez la clé pré-partagée existante

- Ajoutez une nouvelle clé principale en mode interactif
- Modifiez la clé principale existante en mode interactif
- Supprimez la clé principale

Chiffrez la clé pré-partagée existante

```
Router#show running-config
Building configuration...
.
.crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisco123 address 10.1.1.1
.
.
endRouter#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#key config-key password-encrypt
testkey123
Router(config)#password encryption aes
Router(config)#^Z
Router#
Router#show running-config
Building configuration...
.
.
password encryption aes
.
.
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key 6 FLgBaJHXdYY_AcHZZMgQ_RhTDJXHUBAAB
address 10.1.1.1
.
.
end
```

Ajoutez une nouvelle clé principale en mode interactif

```
Router(config)#key config-key password-encrypt
New key: <enter key>
Confirm key: <confirm key>
Router(config)#
```

Modifiez la clé principale existante en mode interactif

```
Router(config)#key config-key password-encrypt
 Old key: <enter existing key>
New key: <enter new key>
Confirm key: <confirm new key>
Router(config)#
*Jan  7 01:42:12.299: TYPE6_PASS: Master key change
heralded,
re-encrypting the keys with the new master key
```

Supprimez la clé principale

```
Router(config)#no key config-key password-encrypt
WARNING: All type 6 encrypted keys will become unusable
Continue with master key deletion ? [yes/no]: yes
Router(config)#
```

Vérifier

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

Dépanner

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Clé pré-partagée chiffrée
- Page d'assistance IPsec
- Support et documentation techniques - Cisco Systems