Configuration du chiffrement des clés pré-partagées dans un routeur

Table des matières

Introduction

Ce document décrit comment configurer le chiffrement des clés pré-partagées actuelles et nouvelles dans un routeur.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

L’information contenue dans le présent document est fondée sur cette version logicielle:

- Logiciel Cisco IOS XE® version 16.9

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Conventions

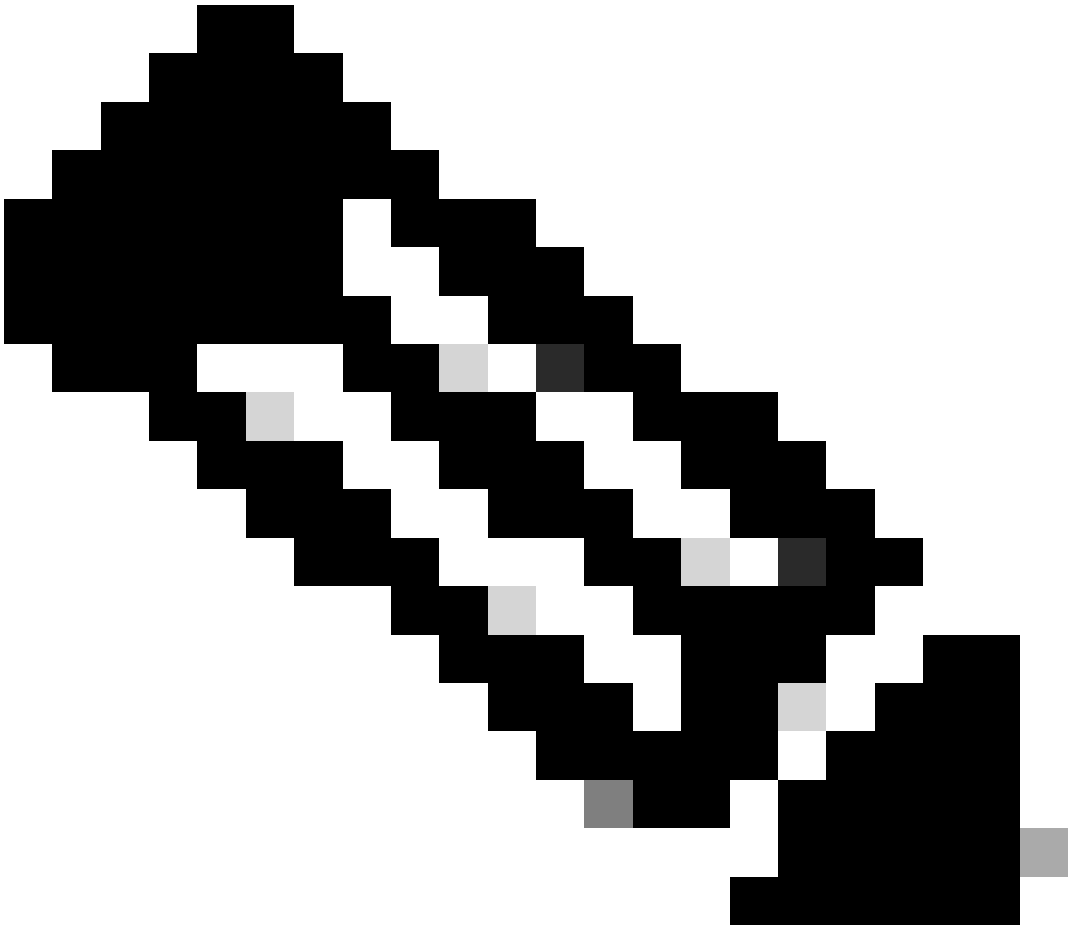
Pour plus d’informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Informations générales

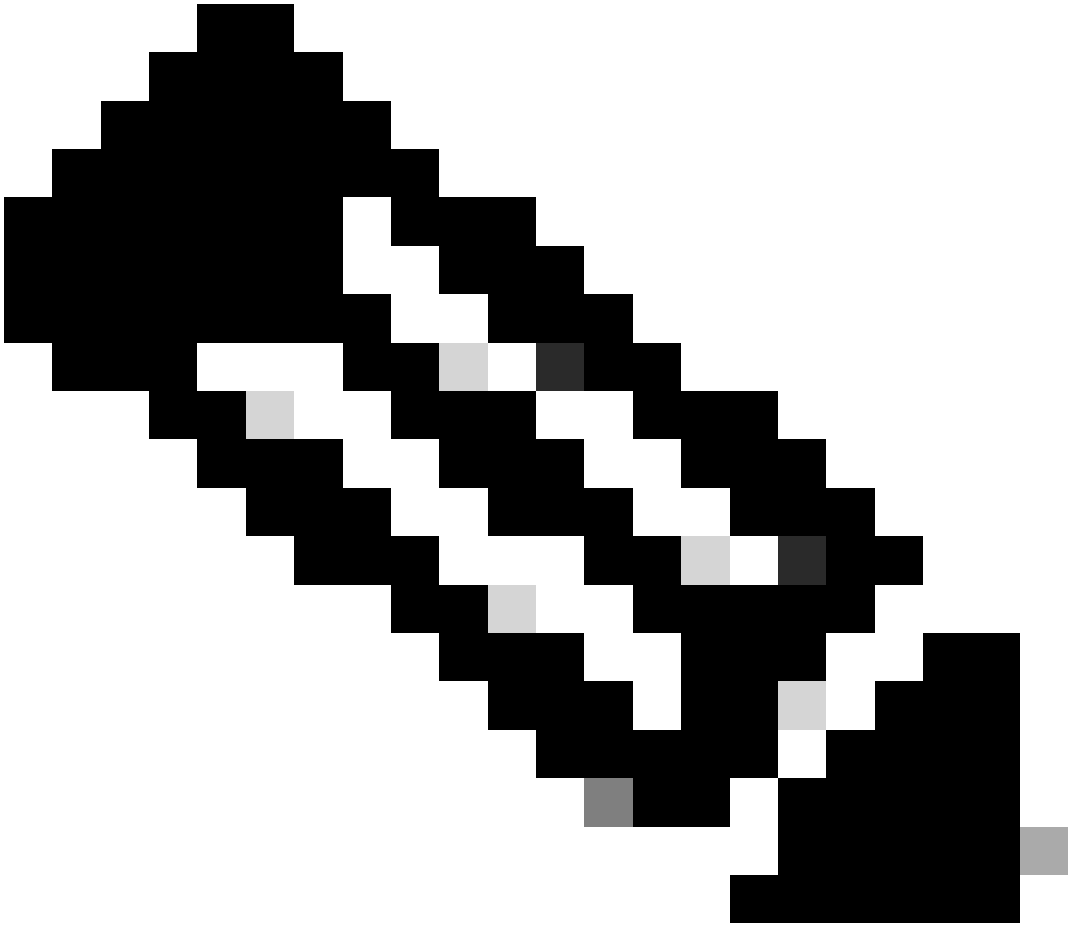
Le code de la version 12.3(2)T du logiciel Cisco IOS introduit la fonctionnalité qui permet au routeur de chiffrer la clé pré-partagée ISAKMP (Internet Security Association and Key Management Protocol) au format sécurisé de type 6 dans la mémoire vive non volatile (NVRAM). La clé pré-partagée à chiffrer peut être configurée soit en standard, sous un anneau de clés ISAKMP, en mode agressif, ou comme mot de passe de groupe sous un serveur Easy VPN (EzVPN) ou une configuration client.

Configurer

Cette section vous présente les informations que vous pouvez utiliser pour configurer les fonctionnalités décrites dans ce document.



Remarque : Utilisez l’outil de recherche de commandes pour obtenir plus d’information sur les commandes figurant dans la présente section.



Remarque : seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations et aux outils Cisco internes.

Ces deux commandes ont été introduites afin d'activer le chiffrement de clé pré-partagée :

- key config-key password-encryption [clé primaire]
- password encryption aes

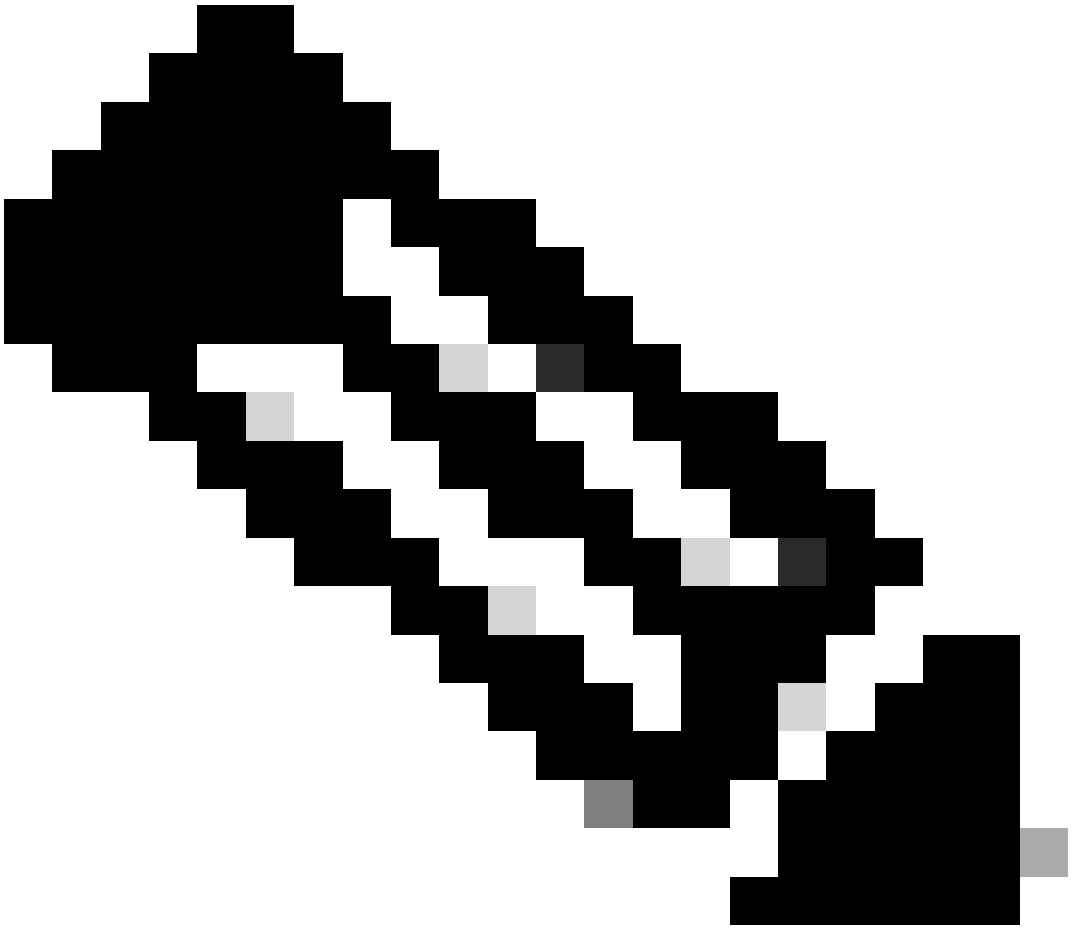
La [clé primaire] est le mot de passe/clé utilisé pour chiffrer toutes les autres clés dans la configuration du routeur à l'aide d'un chiffrement symétrique AES (Advanced Encryption Standard). La clé primaire n'est pas stockée dans la configuration du routeur et ne peut pas être vue ou obtenue de quelque manière que ce soit lorsqu'elle est connectée au routeur.

Une fois configurée, la clé primaire est utilisée pour chiffrer toutes les clés actuelles ou nouvelles dans la configuration du routeur. Si la [clé primaire] n'est pas spécifiée sur la ligne de commande, le routeur invite l'utilisateur à entrer la clé et à la saisir de nouveau pour vérification. Si une clé existe déjà, l'utilisateur est invité à saisir l'ancienne clé en premier. Les clés ne sont pas chiffrées

tant que vous n'exécutez pas la commande password encryption aes.

La clé primaire peut être modifiée (bien que cela ne soit pas nécessaire à moins que la clé ne soit compromise d'une certaine manière) avec la commande key config-key... à nouveau avec la nouvelle commande [primary-key]. Toutes les clés chiffrées actuelles de la configuration du routeur sont chiffrées à nouveau avec la nouvelle clé.

Vous pouvez supprimer la clé primaire lorsque vous émettez la commande no key config-key.... Cependant, cela rend inutilisables toutes les clés actuellement configurées dans la configuration du routeur (un message d'avertissement s'affiche pour détailler cette opération et confirmer la suppression de la clé primaire). Comme la clé primaire n'existe plus, les mots de passe de type 6 ne peuvent pas être déchiffrés et utilisés par le routeur.



Remarque : pour des raisons de sécurité, ni la suppression de la clé primaire ni la suppression de la aes commande password encryption ne déchiffre les mots de passe dans la configuration du routeur. Une fois les mots de passe chiffrés, ils ne sont pas déchiffrés. Les clés chiffrées actuelles de la configuration peuvent toujours être déchiffrées, à condition que la clé primaire ne soit pas supprimée.

De plus, afin de voir les messages de type debug des fonctions de cryptage de mot de passe, utilisez la commande **password logging** en mode de configuration.

Configurations

Ce document utilise ces configurations sur le routeur :

- Chiffrer la clé pré-partagée actuelle
- Ajouter une nouvelle clé primaire de manière interactive
- Modifier la clé primaire actuelle de manière interactive
- Supprimer la clé primaire

Chiffrer la clé pré-partagée actuelle

```
    <#root>

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
```

Ajouter une nouvelle clé primaire de manière interactive

```
    <#root>


Router(config)#
```

```
key config-key password-encrypt



New key:



<enter key>



Confirm key:



<confirm key>



Router(config)#
```

Modifier la clé primaire actuelle de manière interactive

```
    <#root>

Router(config)#



key config-key password-encrypt



 Old key:
```

```
<enter current 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 primary key
```

Supprimer la clé primaire

```
    <#root>

Router(config)#



no key config-key password-encrypt



WARNING: All type 6 encrypted keys will become unusable
```

```
Continue with primary key deletion ? [yes/no]:

yes

Router(config)#
```

Vérifier

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

Dépannage

Aucune information de dépannage spécifique n'est actuellement disponible pour cette configuration.

Informations connexes

- **Page d'assistance IPsec**
- **Assistance technique de Cisco et téléchargements**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.