Contenido

Introducción

El código Cisco IOS® Software Release 12.3(2)T introduce funciones que permiten que el router cifre la clave ISAKMP previamente compartida en el formato seguro de tipo 6 en la memoria RAM no volátil (NVRAM). La clave previamente compartida que se cifrará se puede configurar como estándar, bajo un anillo fundamental ISAKMP, en el modo agresivo o como un contraseña de grupo bajo una configuración de cliente o servidor EzVPN. Esta configuración de ejemplo muestra cómo configurar el cifrado de las claves previamente compartidas existentes y nuevas.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en esta versión del software:

- Cisco IOS Software Release 12.3(2)T

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

Esta sección le presenta con la información que usted puede utilizar para configurar las características este documento describe.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Presentan a estos dos comandos new para habilitar el cifrado de la clave previamente compartida:

- *[master key]* **dominante de la encripción de contraseña de la config-clave**
- **aes de la encripción de contraseña**

El [master key] es la contraseña/la clave usada para cifrar el resto de las claves en la configuración del router con el uso de una cifra simétrica anticipada de la norma de encripción (AES). La clave principal no se salva en la configuración del router y *no se puede* considerar u obtener de ninguna manera mientras que está conectada con el router.

Una vez que está configurada, la clave principal se utiliza para cifrar cualquier clave existente o nueva en la configuración del router. Si el *[master key]* no se especifica en la línea de comando, los prompts de router el usuario para ingresar la clave y para entrarla de nuevo para la verificación. Si existe una clave ya, se indica al usuario que ingrese la vieja clave primero. Las claves no se cifran hasta que usted publique el **comando password encryption aes**.

La clave principal se puede cambiar (aunque esto no debe ser necesaria a menos que la clave se haya comprometido de cierta manera) publicando el **comando key config-key…** otra vez con el nuevo *[master-key]*. Cualquier clave cifrada existente en la configuración del router se encripta nuevamente con la nueva clave.

Usted puede borrar la clave principal cuando usted no publica la **ninguna config-clave dominante….** Sin embargo, esto hace todas las claves actualmente configuradas en la configuración del router inútiles (las visualizaciones de un mensaje de advertencia que detalla esto y confirma la cancelacíon de la clave principal). Puesto que existe la clave principal no más, las contraseñas del tipo 6 no pueden ser unencrypted y utilizadas por el router.

Nota: Por razones de seguridad, ni el retiro de la clave principal, ni el retiro de los unencrypts del **comando password encryption aes las** contraseñas en la configuración del router. Una vez que se cifran las contraseñas, no son unencrypted. Las claves cifradas existentes en la configuración pueden todavía ser unencrypted proporcionaron a la clave principal no se quitan.

Además, para ver los mensajes del debug-tipo de las funciones de encripción de contraseña, utilice el **comando password logging** en el modo de configuración.

Configuraciones

Este documento utiliza estas configuraciones en el router:

- Cifre la clave previamente compartida existente
- Agregue una nueva clave principal recíprocamente
- Modifique la clave principal existente recíprocamente
- Borre la clave principal

Cifre la clave previamente compartida existente

```
Router#show running-config Building
configuration.....crypto isakmp policy 10 authentication
pre-sharecrypto isakmp key cisco123 address
10.1.1.1..endRouter#configure terminalEnter
configuration commands, one per line.  End with
CNTL/Z.Router(config)#key config-key password-encrypt
testkey123Router(config)#password encryption
aesRouter(config)#^ZRouter#Router#show running-config
Building configuration.....password encryption
aes..crypto isakmp policy 10 authentication pre-
sharecrypto isakmp key 6
FLgBaJHXdYY_AcHZZMgQ_RhTDJXHUBAAB address 10.1.1.1..end
```

Agregue una nueva clave principal recíprocamente

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

Modifique la clave principal existente recíprocamente

```
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
```

Borre la clave principal

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

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Clave Precompartida Cifrada
- Página de soporte de IPSec
- Soporte Técnico y Documentación - Cisco Systems