Configuración del cifrado de claves previamente compartidas en un router

Contenido

Introducción

Este documento describe cómo configurar el cifrado de las claves previamente compartidas actuales y nuevas en un router.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Versión 16.9 del software Cisco IOS XE®

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

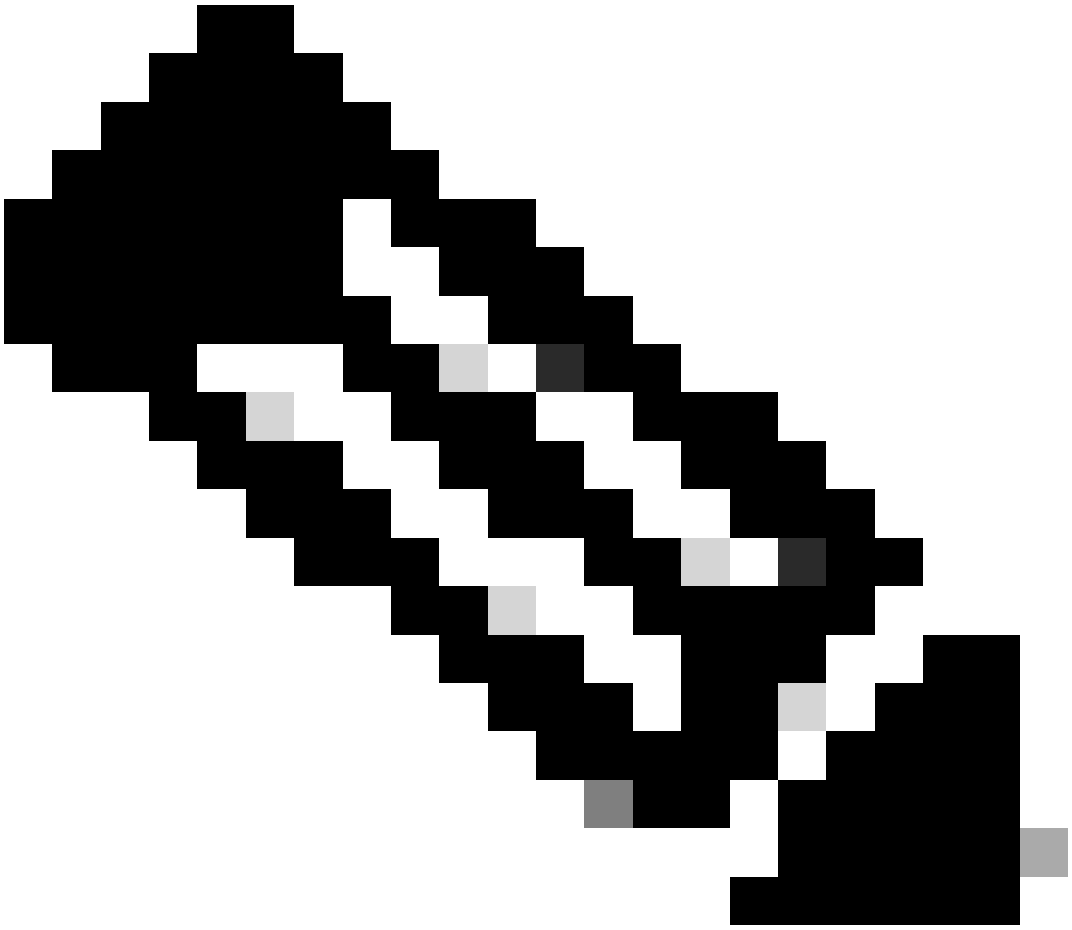
Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

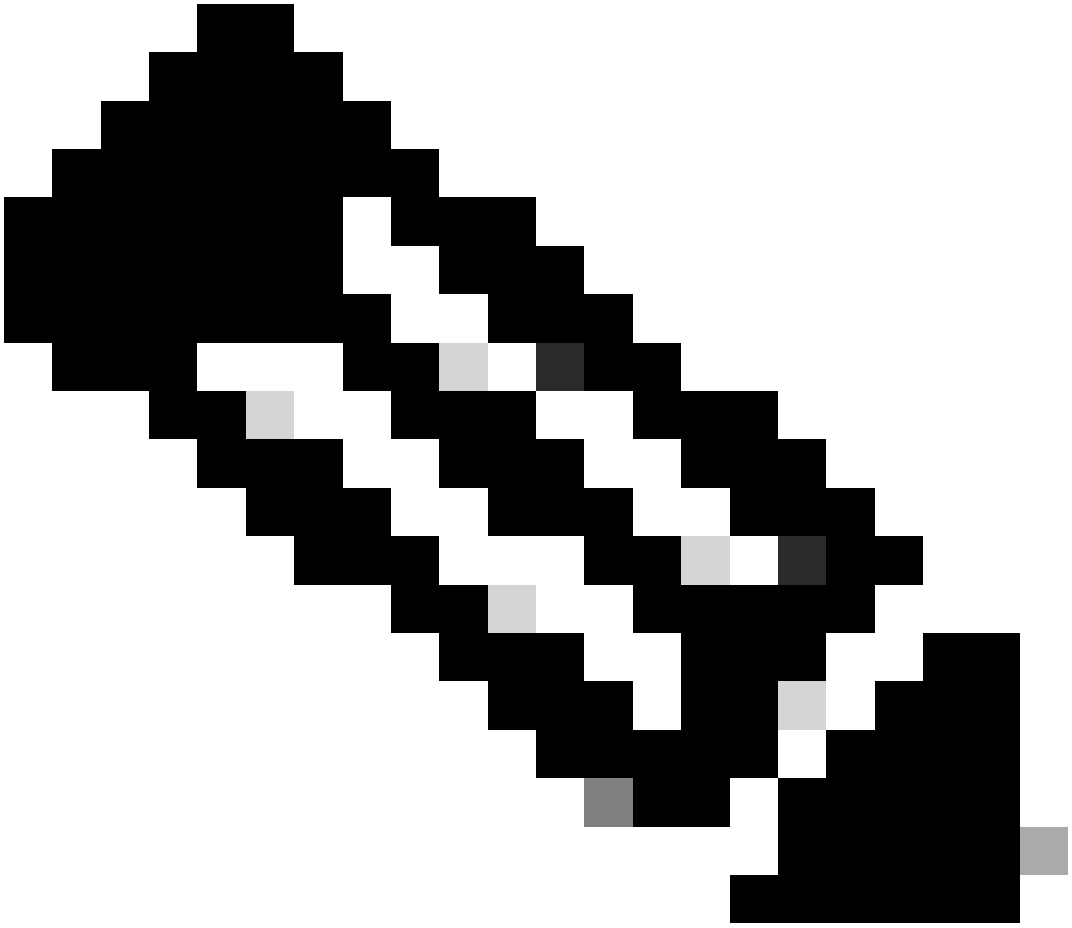
El código de la versión 12.3(2)T del software del IOS de Cisco introduce la funcionalidad que permite que el router cifre la clave precompartida del protocolo ISAKMP (Internet Security Association and Key Management Protocol) en formato de tipo 6 seguro en RAM no volátil, RAM no volátil (NVRAM). La clave previamente compartida que se va a cifrar se puede configurar como estándar, con un anillo de claves ISAKMP, en modo agresivo o como contraseña de grupo en una configuración de cliente o servidor Easy VPN (EzVPN).

Configurar

En esta sección se presenta la información que puede utilizar para configurar las funciones que describe este documento.



Nota: Utilice la herramienta Command Lookup para obtener más información sobre los comandos utilizados en esta sección.



Nota: solo los usuarios registrados de Cisco pueden acceder a la información y a las herramientas internas de Cisco.

Estos dos comandos se introdujeron para habilitar el cifrado de clave previamente compartida:

- key config-key password-encryption [primary key]
- password encryption aes

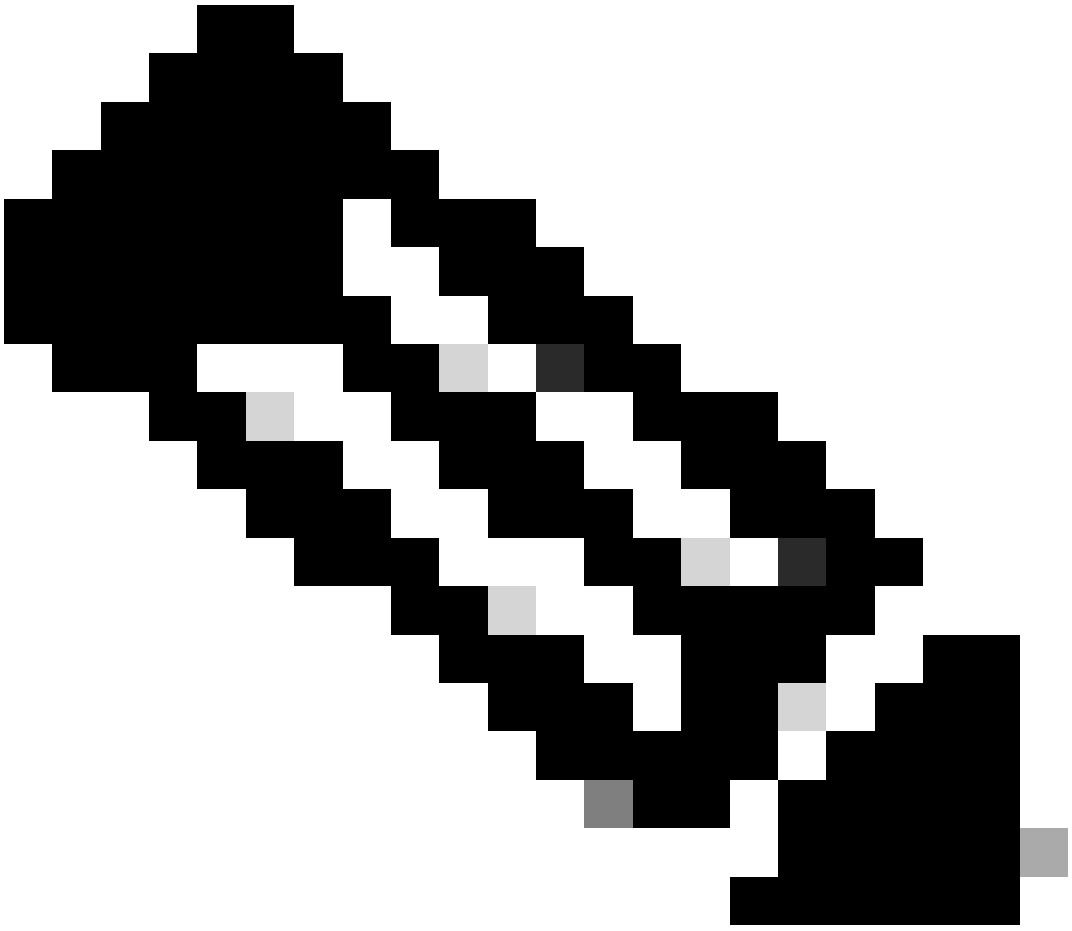
La [clave principal] es la contraseña/clave utilizada para cifrar todas las demás claves de la configuración del router con el uso de un cifrado simétrico del estándar de cifrado avanzado (AES). La clave principal no se almacena en la configuración del router y no se puede ver ni obtener de ninguna manera mientras esté conectado al router.

Una vez configurada, la clave principal se utiliza para cifrar cualquier clave nueva o actual en la configuración del router. Si [clave principal] no se especifica en la línea de comandos, el router le pide al usuario que ingrese la clave y que la vuelva a ingresar para verificarla. Si ya existe una clave, se solicita al usuario que introduzca primero la clave antigua. Las claves no se cifran hasta

que ejecute el comando password encryption aes.

La clave primaria se puede cambiar (aunque esto no es necesario a menos que la clave se haya visto comprometida de alguna manera) con el comando key config-key... nuevamente con la nueva [primary-key]. Las claves cifradas actuales de la configuración del router se vuelven a cifrar con la nueva clave.

Puede eliminar la clave principal cuando ejecute no key config-key... Sin embargo, esto hace que todas las claves configuradas actualmente en la configuración del router sean inútiles (se muestra un mensaje de advertencia que detalla esto y confirma la eliminación de la clave principal). Dado que la clave principal ya no existe, el router no puede descifrar y utilizar las contraseñas de tipo 6.



Nota: Por motivos de seguridad, ni la eliminación de la clave principal ni el aes comando password encryption descifran las contraseñas en la configuración del router. Una vez cifradas las contraseñas, no se descifran. Las claves cifradas actuales de la configuración se pueden descifrar siempre que no se quite la clave principal.

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

Configuraciones

Este documento utiliza estas configuraciones en el router:

- Cifrar la clave precompartida actual
- Agregar una nueva clave principal de forma interactiva
- Modificar la clave principal actual de forma interactiva
- Eliminar la clave principal

Cifrar la clave precompartida actual

```
    <#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
```

Agregar una nueva clave principal de forma interactiva

```
    <#root>

Router(config)#



key config-key password-encrypt
```

```
New key:


<enter key>


Confirm key:


<confirm key>


Router(config)#
```

Modificar la clave principal actual de forma interactiva

```
    <#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
```

Eliminar la clave principal

```
    <#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)#
```

Verificación

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

Troubleshoot

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

Información Relacionada

- **Página de soporte de IPSec**
- **Soporte técnico y descargas de Cisco**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).