Configurar as chaves criptografadas pré-compartilhadas em um roteador

Contents

[Introdução](#)

[Pré-requisitos](#)

- [Requisitos](#)
- [Componentes Utilizados](#)
- [Conventions](#)

[Informações de Apoio](#)

[Configurar](#)

- [Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar a criptografia de chaves pré-compartilhadas novas e atuais em um roteador.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações aqui são baseadas nesta versão de software:

- Software Cisco IOS XE® versão 16.9

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

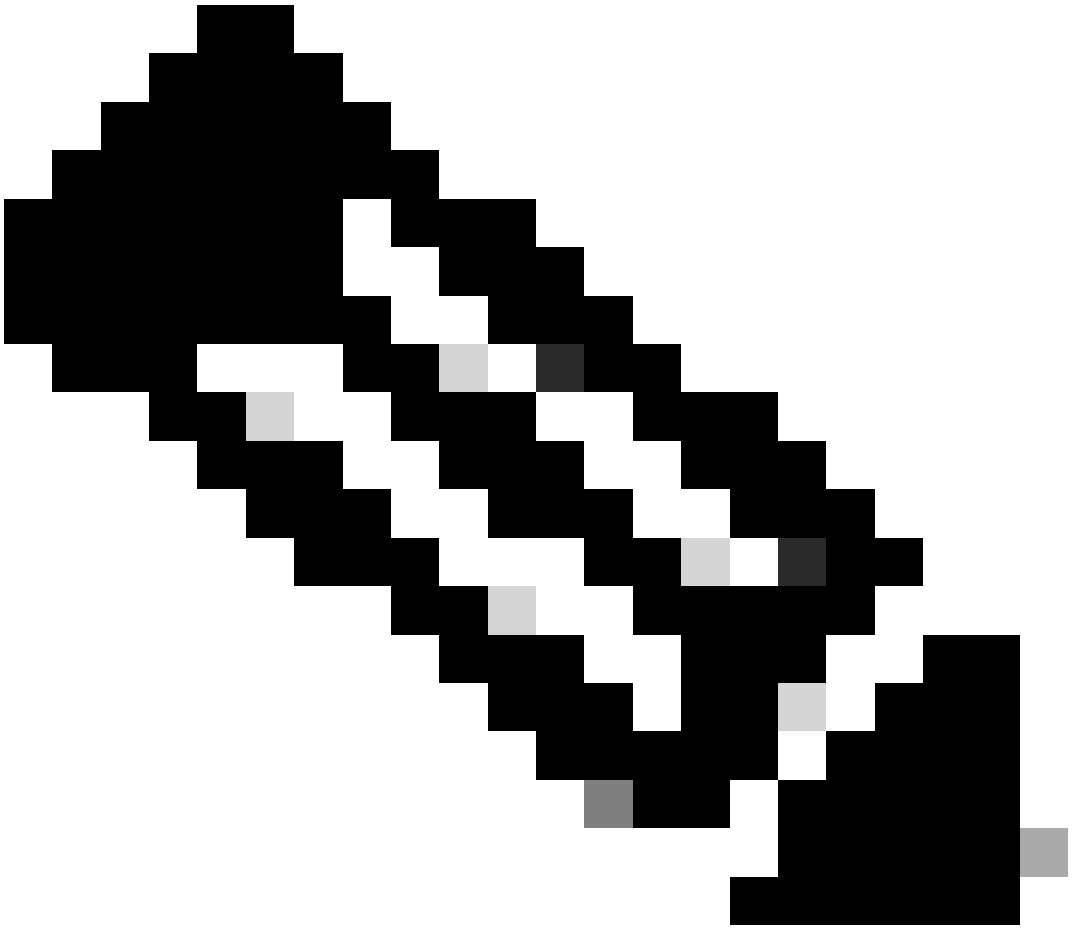
Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

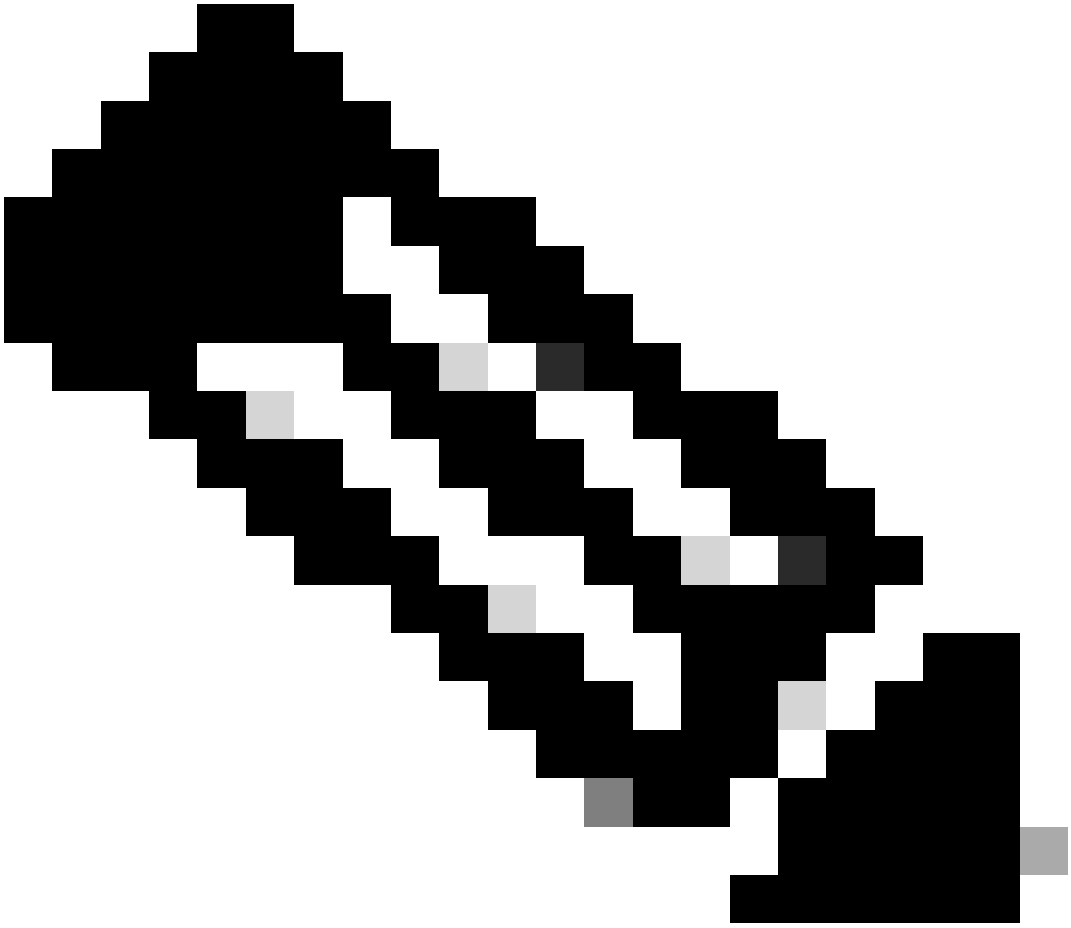
O código do Cisco IOS Software Release 12.3(2)T introduz a funcionalidade que permite que o roteador criptografe a chave pré-compartilhada do Internet Security Association and Key Management Protocol (ISAKMP) em formato seguro tipo 6 em RAM não volátil, RAM não volátil (NVRAM). A chave pré-compartilhada a ser criptografada pode ser configurada como padrão, em um anel de chave ISAKMP, no modo agressivo ou como a senha de grupo em um servidor Easy VPN (EzVPN) ou configuração de cliente.

Configurar

Esta seção apresenta as informações que você pode usar para configurar os recursos descritos neste documento.



Observação: use a ferramenta de pesquisa de comando para obter mais informações sobre os comandos usados nesta seção.



Observação: somente usuários registrados da Cisco podem acessar ferramentas e informações internas da Cisco.

Estes dois comandos foram introduzidos para habilitar a criptografia de chave pré-compartilhada:

- key config-key password-encryption [chave primária]
- aes de criptografia de senha

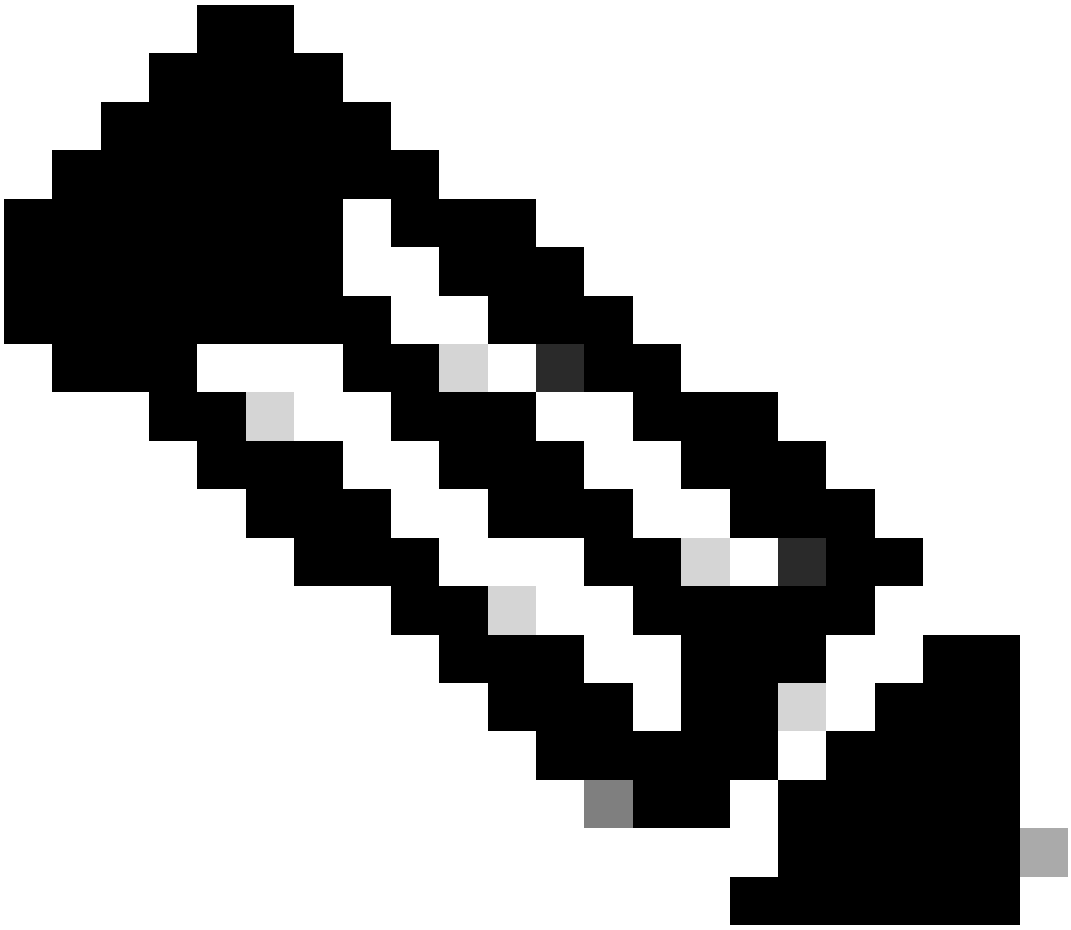
A [primary key] é a senha/chave usada para criptografar todas as outras chaves na configuração do roteador com o uso de uma cifra simétrica AES (Advance Encryption Standard). A chave primária não é armazenada na configuração do roteador e não pode ser vista ou obtida de nenhuma forma enquanto estiver conectada ao roteador.

Uma vez configurada, a chave primária é usada para criptografar qualquer chave nova ou atual na configuração do roteador. Se [primary key] não for especificado na linha de comando, o roteador solicita que o usuário insira a chave novamente para verificação. Se já existir uma chave, o usuário é solicitado a digitar primeiro a chave antiga. As chaves não são criptografadas até que

você emita o comando password encryption aes.

A chave primária pode ser alterada (embora isso não seja necessário, a menos que a chave tenha sido comprometida de alguma forma) com o comando key config-key... novamente com o novo [primary-key]. Todas as chaves criptografadas atuais na configuração do roteador são criptografadas novamente com a nova chave.

Você pode excluir a chave primária ao emitir o comando no key config-key.... No entanto, isso inutiliza todas as chaves configuradas atualmente na configuração do roteador (uma mensagem de aviso é exibida detalhando isso e confirmando a exclusão da chave primária). Como a chave primária não existe mais, as senhas tipo 6 não podem ser descriptografadas e usadas pelo roteador.



Observação: por motivos de segurança, nem a remoção da chave primária, nem a remoção do aes comando password encryption descriptografam as senhas na configuração do roteador. Quando as senhas são criptografadas, elas não são descriptografadas. As chaves criptografadas atuais na configuração ainda podem ser descriptografadas, desde que a chave primária não seja removida.

Além disso, para ver as mensagens do tipo de depuração das funções de criptografia de senha, use o comando **password logging** no modo de configuração.

Configurações

Este documento usa estas configurações no roteador:

- Criptografar a chave pré-compartilhada atual
- Adicionar uma nova chave primária interativamente
- Modificar a Chave Primária Atual Interativamente
- Excluir a chave primária

Criptografar a chave pré-compartilhada atual

```
    <#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
```

Adicionar uma nova chave primária interativamente

```
    <#root>


Router(config)#
```

```
key config-key password-encrypt



New key:


<enter key>


Confirm key:


<confirm key>


Router(config)#
```

Modificar a Chave Primária Atual Interativamente

```
    <#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
```

Excluir a chave primária

```
    <#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)#
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

No momento, não há informações específicas de solução de problemas disponíveis para essa configuração.

Informações Relacionadas

- **Página de suporte do IPSec**
- **Suporte técnico e downloads da Cisco**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.