Cifre chaves pré-compartilhada no exemplo da configuração de roteador do Cisco IOS

Índice

Introdução

O código do Cisco IOS® Software Release 12.3(2)T introduz a funcionalidade que permite que o roteador criptografe a chave pré-compartilhada ISAKMP no formato protegido tipo 6 na 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 uma senha de grupo em um servidor EzVPN ou configuração de cliente. Esta configuração de exemplo detalha como configurar a criptografia das chaves pré-compartilhadas existentes e novas.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações aqui são baseadas nesta versão de software:

- Cisco IOS Software Release 12.3(2)T

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Configurar

Esta seção apresenta-o com a informação que você pode se usar para configurar as características este documento descreve.

Note: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Estes dois comandos new são introduzidos a fim permitir a criptografia da chave pré-compartilhada:

- *[master key]* ***chave da criptografia de senha da configuração-chave***
- **aes da criptografia de senha**

O [master key] é a senha/chave usada para cifrar todas chaves restantes na configuração de roteador com o uso de uma cifra simétrica avançada do padrão de codificação (AES). O chave mestre não é armazenado na configuração de roteador e *não pode* ser considerado ou obtido em nenhuma maneira quando conectado ao roteador.

Uma vez que configurado, o chave mestre é usado para cifrar todas as chaves existentes ou novas na configuração de roteador. Se o *[master key]* não é especificado na linha de comando, as alertas de roteador o usuário para incorporar a chave e para a reenter para a verificação. Se uma chave já existe, o usuário está alertado incorporar primeiramente a chave velha. As chaves não são cifradas até que você emita o **comando password encryption aes**.

O chave mestre pode ser mudado (embora este não deve ser necessário a menos que a chave se tornar comprometida de uma certa maneira) emitindo o **comando key config-key…** outra vez com o *[master-key]* novo. Todas as chaves cifradas existentes na configuração de roteador re-são cifradas com a chave nova.

Você pode suprimir do chave mestre quando você não emite **nenhuma configuração-chave chave….** Contudo, isto torna todas as chaves atualmente configuradas na configuração de roteador inúteis (indicadores de mensagem de advertência que detalha esta e confirma o supressão do chave mestre). Desde que o chave mestre já não existe, o tipo senhas 6 não pode ser unencrypted e usado pelo roteador.

Note: Por razões de segurança, nem a remoção do chave mestre, nem a remoção dos unencrypts do **comando password encryption aes as** senhas na configuração de roteador. Uma vez que as senhas são cifradas, não são unencrypted. As chaves cifradas existentes na configuração podem ainda ser unencrypted forneceram o chave mestre não são removidas.

Adicionalmente, a fim ver o debugar-tipo mensagens de funções de criptografia de senha, use o **comando password logging no** modo de configuração.

Configurações

Este documento usa estas configurações no roteador:

- Cifre a chave pré-compartilhada existente

- Adicionar um chave mestre novo interativamente
- Altere o chave mestre existente interativamente
- Suprima do chave mestre

Cifre a chave pré-compartilhada existente

```
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 um chave mestre novo interativamente

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

Altere o chave mestre existente interativamente

```
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
```

Suprima do chave mestre

```
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)#
```

Verificar

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

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Chave Preshared cifrada
- Página de suporte IPSec
- Suporte Técnico e Documentação - Cisco Systems