

Troubleshooting de Rejeição do Analisador de Formato Hexadecimal da Chave Manual PPPK do PQC

Contents

Problema

Ao [configurar o IPsec](#) (Segurança IP) no Cisco IOS XE com PQC (Criptografia pós-quântica) e PPK manual (Chaves pré-compartilhadas pós-quânticas) no formato hexadecimal, o dispositivo pode rejeitar o formato hexadecimal PPK com qualquer um destes erros:

```
Device(config-ikev2-keyring-peer)#ppk manual id peer1 key hex 3a4b5
```

```
% Invalid input detected at '^' marker.
```

```
Device(config-ikev2-keyring-peer)#
```

```
Device(config-ikev2-keyring-peer)#ppk manual id peer1 key hex 3a4b5c88
```

```
% Invalid hex key.All characters in hex string must be ASCII.
```

```
Device(config-ikev2-keyring-peer)#
```

Ambiente

- Roteadores Cisco executando o software Cisco IOS XE
- IPsec usando implementação de criptografia pós-quântica com chaves PPK manuais

Resolução

O roteador valida valores de byte decodificados com strings hexadecimais para a configuração manual da chave PPK. O valor decodificado deve atender a estes dois requisitos:

- O PPK codificado hexadecimal deve representar uma cadeia de caracteres ASCII válida. Como cada caractere ASCII é codificado usando 8 bits, e cada caractere hexadecimal representa 4 bits de informação, a string hexadecimal de entrada deve consistir em um número par de caracteres. Por exemplo, a string hexadecimal 3a4b5 é uma entrada inválida, pois tem um número ímpar (5) de caracteres hexadecimais.
- O analisador aceita valores hex somente se os bytes decodificados permanecerem dentro do intervalo de bytes ASCII padrão (0x00-0x7F). A chave problemática 3a4b5c88 foi rejeitada porque:

```
0x3a = 58 (ascii ":") valid
0x4b = 75 (ascii "K") valid
0x5C = 92 (ascii "\") valid
0x88 = 136 invalid - outside of standard ASCII range
```

Para resolver esse erro, use valores hexadecimais onde cada byte permanece dentro do intervalo ASCII padrão (0x00-0x7F), por exemplo:

```
Device(config-ikev2-keyring-peer)#ppk manual id peer1 key hex 3a4b5c88
% Invalid hex key.All characters in hex string must be ASCII.
Device(config-ikev2-keyring-peer)#ppk manual id peer1 key hex 3a4b5c78
Device(config-ikev2-keyring-peer)#
```

Causa

Entrada de chave PPK inválida em formato hexadecimal porque está fora do intervalo de [caracteres ASCII padrão](#) (0x00-0x7F).

Conteúdo relacionado

- [Configurando A Criptografia Quantum-Safe Usando Chaves Pós-Compartilhadas Quantum](#)
- 'Bug da Cisco ID [CSCwn32983](#)'(Bug interno da Cisco para tornar o erro do analisador mais

claro)

- [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.