在路由器中配置加密预共享密钥

目录

简介

本文档介绍如何在路由器中设置当前和新预共享密钥的加密。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件版本：

- 思科IOS XE®软件版本16.9

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

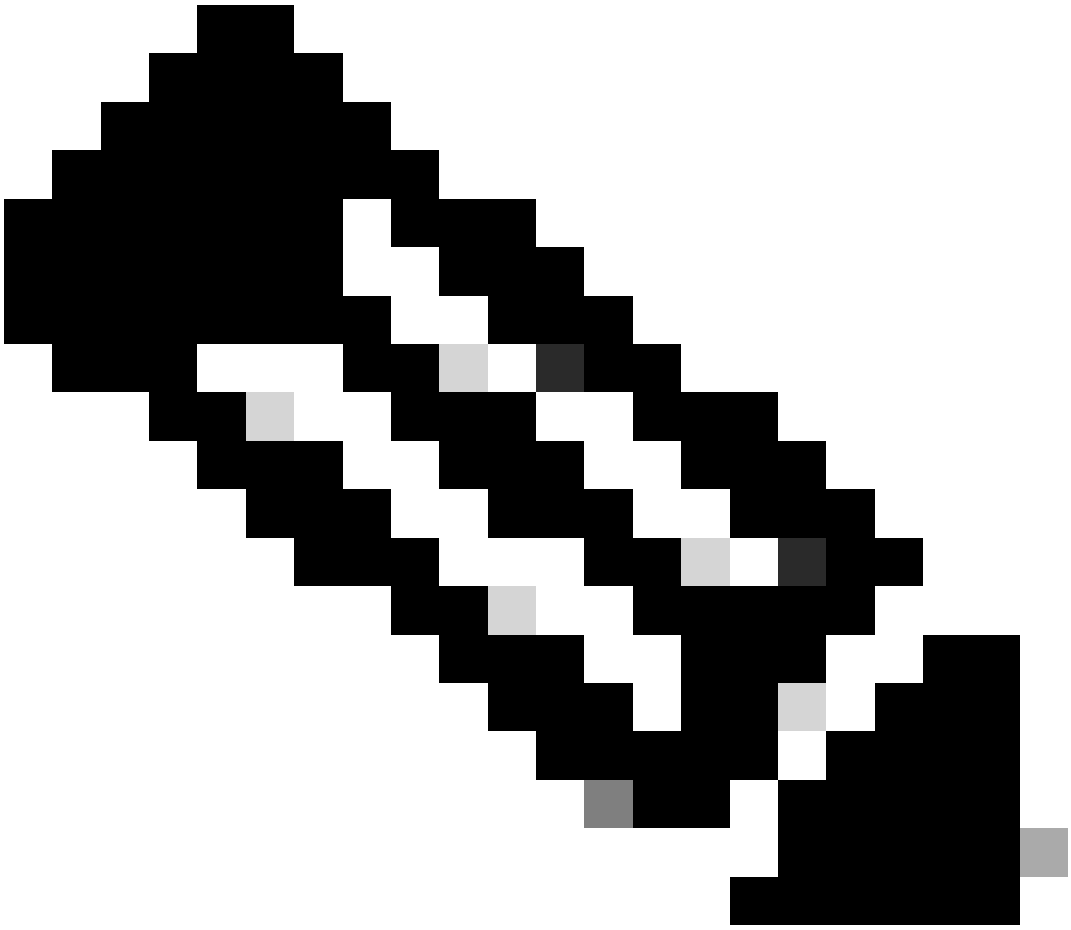
背景信息

Cisco IOS软件版本12.3(2)T代码引入了一项功能，允许路由器在非易失性RAM、非易失性RAM (NVRAM)中以安全类型6格式加密互联网安全关联和密钥管理协议(ISAKMP)预共享密钥。要加密的

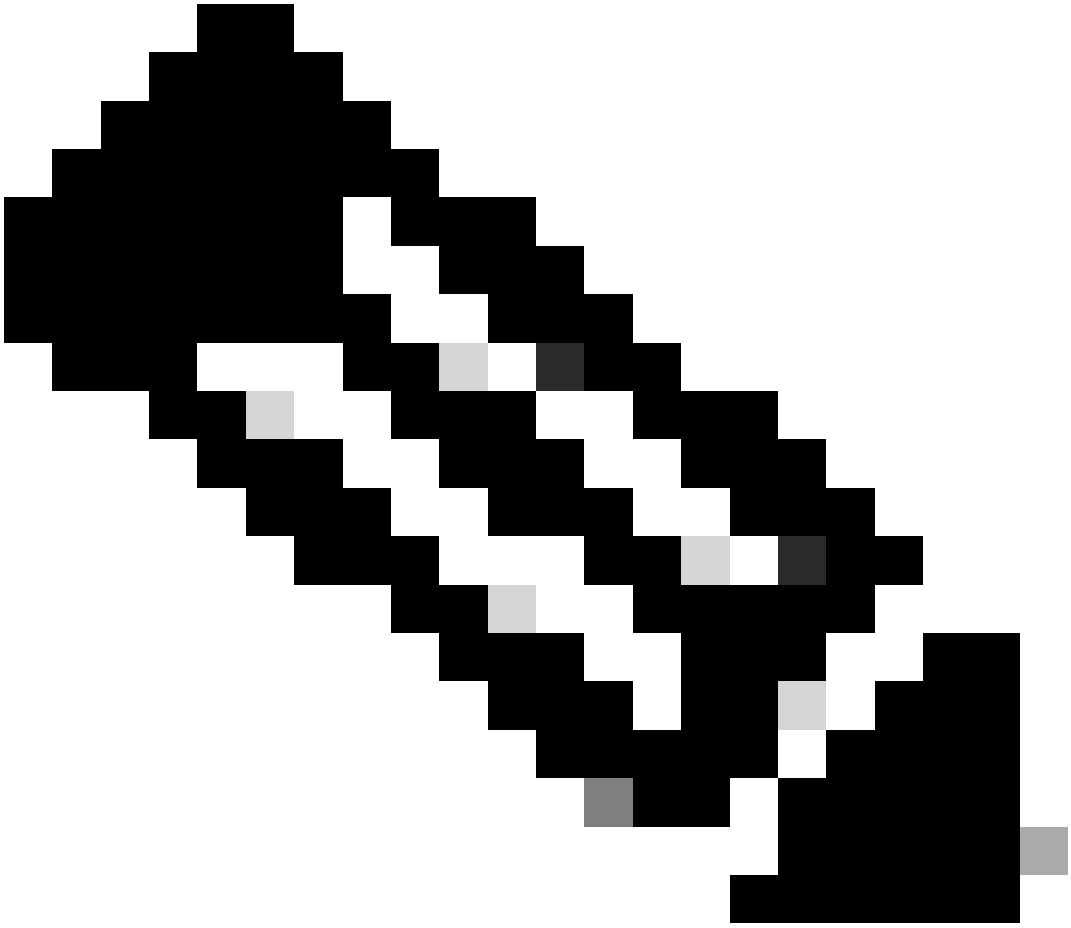
预共享密钥可以在ISAKMP密钥环下以主动模式配置为标准，也可以在Easy VPN (EzVPN)服务器或客户端设置下配置为组密码。

配置

此部分存在您与您能使用配置功能本文描述的信息。



注意：使用命令查找工具可获取关于此部分中所用命令的更多信息。



注意：只有思科注册用户才能访问内部思科工具和信息。

引入了以下两个命令以启用预共享密钥加密：

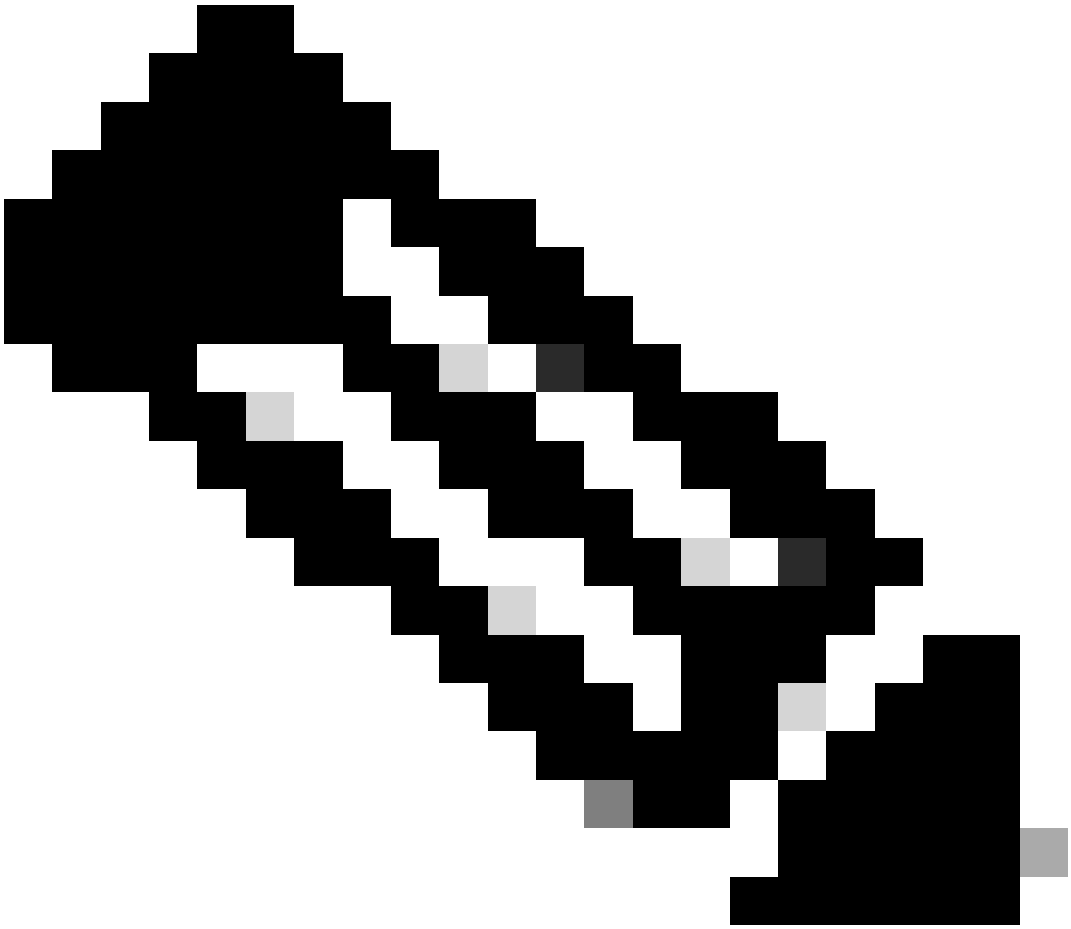
- key config-key password-encryption [主密钥]
- password encryption aes

[primary key]是用于为路由器配置中的所有其他密钥加密的密码/密钥，与高级加密标准(AES)对称密码配合使用。主密钥不存储在路由器配置中，而且在连接到路由器的情况下无法以任何方式查看或获取主密钥。

配置好之后，主密钥用于加密路由器配置中任何当前密钥或新密钥。如果没有在命令行中指定[primary key]，路由器会提示用户输入密钥并再次输入以进行验证。如果密钥已经存在，则会首先提示用户输入旧密钥。在您发出 password encryption aes 命令之前，密钥不会加密。

可使用key config-key... 命令和新的[primary-key]再次更改主密钥（尽管除非密钥已受到某种方式的危害，否则无需更改）。 路由器配置中的所有当前加密密钥都使用新密钥重新加密。

发出no key config-key...命令时可以删除主键。 但是，这会使路由器配置中当前配置的所有密钥失效（显示一条警告消息，详细介绍此情况并确认主密钥删除）。由于主密钥不再存在，路由器无法解密和使用第6类口令。



注意：出于安全原因，删除主密钥和删除password encryptionaes 命令都不会对路由器配置中的密码进行解密。一旦密码加密，就不会解密。如果未删除主密钥，则仍可解密配置中的当前加密密钥。

此外，为了查看密码加密功能的调试类型消息，应在配置模式下使用**password logging**命令。

配置

本文档在路由器上使用以下配置：

- 加密当前预共享密钥
- 以交互方式添加新主键
- 以交互方式修改当前主键
- 删除主键

加密当前预共享密钥

```
    <#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
```

以交互方式添加新主键

```
    <#root>

Router(config)#


key config-key password-encrypt



New key:


<enter key>



Confirm key:
```

```
<confirm key>

Router(config)#
```

以交互方式修改当前主键

```
    <#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
```

删除主键

```
    <#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)#
```

验证

当前没有可用于此配置的验证过程。

故障排除

当前没有可用于此配置的特定故障排除信息。

相关信息

- **IPSec 支持**页面
- **思科技**术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。