

在Cisco IOS路由器中的加密预共享密钥的配置示例

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[Configure](#)

[配置](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

[Introduction](#)

Cisco IOS® 软件版本 12.3(2)T 代码引入了一种功能，允许路由器在非易失性 RAM (NVRAM) 中以安全类型 6 格式对 ISAKMP 预共享密钥进行加密。要加密的预共享密钥可以在主动模式中的 ISAKMP 密钥环下配置为标准密码，也可以在 EzVPN 服务器或客户端设置下配置为组密码。此配置示例详细介绍了如何为现有和新建的预共享密钥设置加密。

[Prerequisites](#)

[Requirements](#)

There are no specific requirements for this document.

[Components Used](#)

本文的信息根据此软件版本：

- Cisco IOS 软件版本 12.3(2)T

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

[Conventions](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

Configure

此部分提交您与您能使用配置功能本文描述的信息。

Note: 使用[命令查找工具](#) ([仅限注册用户](#)) 可获取有关本部分所使用命令的详细信息。

引入了下面两个新命令，以实现预共享密钥加密：

- **key config-key password-encryption [master key]**
- **密码加密aes**

[master 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。master key 并非 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它。

配置之后，master key 可用于为路由器配置中所有现有或新建的密钥加密。如果没有在命令行中指定 **[master 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。

要更改 master key (除非密钥受到某种方式的危害，否则无需更改)，请使用新的 **[master-key]** 重新发出 **key config-key...** 命令。路由器配置中所有现有的已加密密钥都会与新密钥一起重新加密。

发出 **no key config-key....** 命令时可以删除 master key。但是，此操作会使路由器配置中所有当前已配置的密钥失效 (系统将显示一条警告消息，详细说明此情况，并确认对 master key 的删除)。由于 master key 不再存在，因此路由器不能再对类型 6 密码进行解密和使用。

Note: 由于安全原因，删除 master key 和删除 **password encryption aes** 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，就不能 解密。如果没有删除 master key，仍然可以对配置中现有的已加密密钥进行解密。

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：

- [为现有的预共享密钥加密](#)
- [以交互方式添加新的 Master Key](#)
- [以交互方式修改现有的 Master Key](#)
- [删除 Master Key](#)

为现有的预共享密钥加密

```
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
```

以交互方式添加新的 Master Key

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

以交互方式修改现有的 Master Key

```
.  
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
```

删除 Master Key

```
.  
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)#
```

Verify

当前没有可用于此配置的验证过程。

Troubleshoot

目前没有针对此配置的故障排除信息。

Related Information

- [已加密的预共享密钥](#)

- [IPsec支持页面](#)
- [Technical Support & Documentation - Cisco Systems](#)