在路由器中安全存储预共享密钥

目录

简介

先决条件

- 要求
- 使用的组件
- 规则

背景信息

配置

- 配置

验证

相关信息

简介

本文档介绍如何在路由器中设置对当前和新的预共享密钥的加密。

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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

Cisco IOS软件版本12.3(2)T引入了允许路由器在非易失性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)预共享密钥的功能。 要加密的预共享密钥可以配置为标准、在ISAKMP密钥环下、在主动模式下或作为组密码，在简易虚拟专用网络(EzVPN)服务器或客户端设置下。

配置

此部分存在您与您能使用配置功能本文描述的信息。

引入了以下两个命令以启用预共享密钥加密：

- key config-key password-encryption [primary key]
- password encryption aes

[primary key] 是使用高级加密标准(AES)对称密码对路由器配置中的所有其他密钥进行加密的密码/密钥。主密钥不存储在路由器配置中，并且在连接到路由器时，不能以任何方式查看或获取主密钥。

配置后，主密钥用于加密路由器配置中的任何当前密钥或新密钥。如果在命令行中未指定[primary key] ，路由器将提示用户输入密钥并重新输入密钥进行验证。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。

可以使用key config-key password-encryption命令和新的[primary-key]再次更改主密钥（尽管除非密钥以某种方式受到危害，否则无需更改主密钥）。 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。

您可以在发出no key config-key password-encryption时删除主密钥。但是，这会使路由器配置中所有当前配置的密钥失效（显示一条警告消息，详细介绍该消息并确认主密钥删除）。 由于主密钥不再存在，路由器无法解密和使用第6类密码。



注意：出于安全原因，删除主密钥或删除password encryption aes命令都不会解密路由器配置中的密码。一旦密码加密，它们就不会被解密。如果主密钥未被删除，配置中的当前加密密钥仍可解密。

此外，为了查看密码加密功能的调试类型消息，请在配置模式下使用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
!
<output omitted>
!
end

Router#

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
!
<output omitted>
!
end
```

以交互方式添加新主键

```
<#root>

Router(config)#

key config-key password-encrypt


New 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:
```

```
New key:



Confirm key:



Router(config)#
*Jan  7 01:42:12.299: TYPE6_PASS: Master key change heralded, re-encrypting the keys with the new prima
```

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。

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）。