在路由器中配置加密預共用金鑰

目錄

簡介

本文檔介紹如何在路由器中設定當前和新的預共用金鑰的加密。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據以下軟體版本而定：

- Cisco IOS XE®軟體版本16.9

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

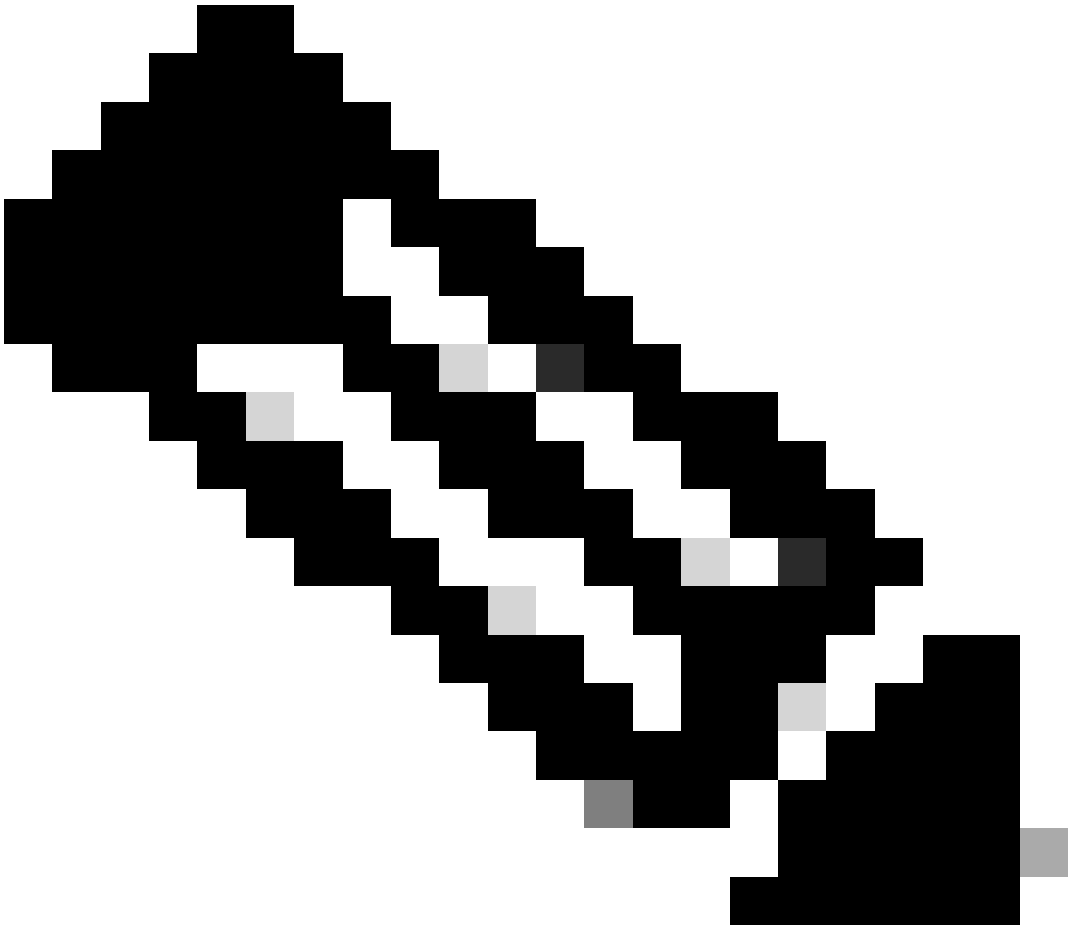
背景資訊

Cisco IOS軟體版本12.3(2)T程式碼引入了功能，允許路由器以安全型別6格式，在非易失性RAM、非易失性RAM (NVRAM)中加密網際網路安全關聯和金鑰管理通訊協定(ISAKMP)預先共用金鑰。要

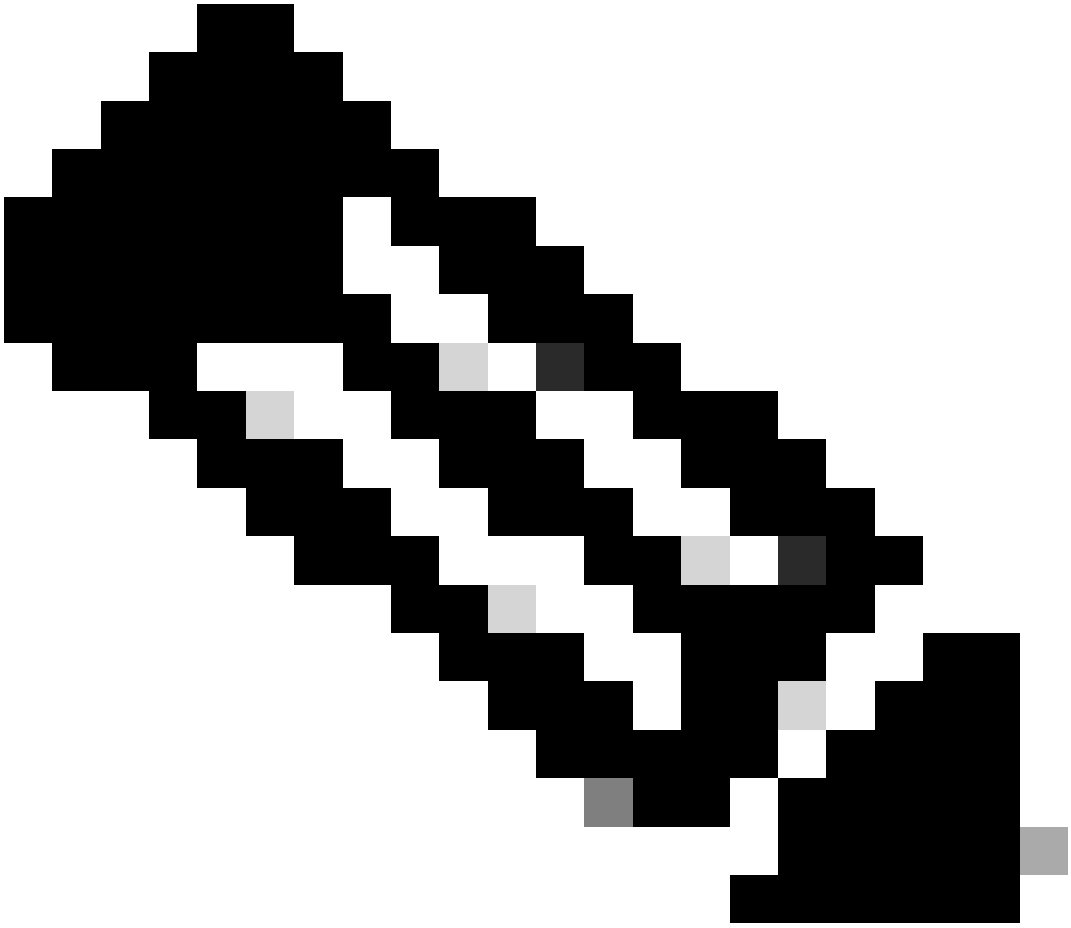
加密的預共用金鑰可以配置為標準、在ISAKMP金鑰環下、在主動模式下或作為Easy VPN (EzVPN)伺服器或客戶端設定下的組密碼。

設定

本節提供可用於設定本檔案所述功能的資訊。



注意：使用「命令查詢工具」可獲取有關本節中所用命令的詳細資訊。



注意：只有已註冊的思科使用者才能訪問內部思科工具和資訊。

引入了以下兩個命令以啟用預共用金鑰加密：

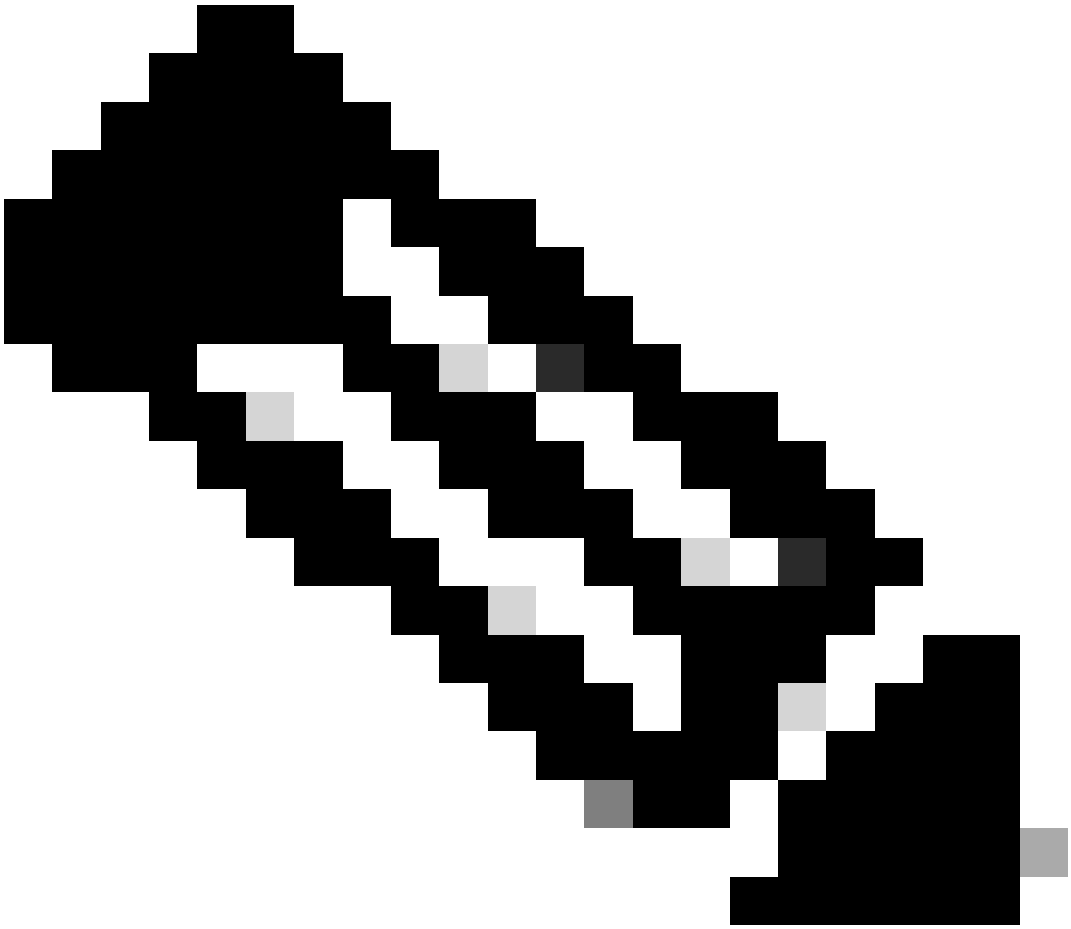
- key config-key password-encryption [primary key]
- 密碼加密aes

[primary key]是用於為路由器配置中的所有其他金鑰加密的密碼/金鑰，與高級加密標準(AES)對稱密碼配合使用。主金鑰不儲存在路由器配置中，並且無法在連線到路由器的情況下以任何方式檢視或獲取它。

配置後，主金鑰用於加密路由器配置中任何當前金鑰或新金鑰。如果沒有在命令列中指定[primary key]，路由器將提示使用者輸入金鑰並再次輸入以進行驗證。如果金鑰已存在，則會提示使用者先輸入舊金鑰。在您發出password encryption aes命令之前，金鑰不會加密。

可以使用新的[primary-key]再次用key config-key...命令更改主鍵（除非該鍵已受到某種方式的危害，否則無需更改）。 路由器配置中的所有當前加密金鑰都使用新金鑰重新加密。

您可以發出no key config-key...命令刪除主鍵。 但是，這會使路由器配置中所有當前配置的金鑰失效（顯示一條警告消息，詳細說明了此消息並確認主金鑰刪除）。由於主金鑰不再存在，路由器無法解密和使用6類口令。



注意：出於安全原因，刪除主金鑰和刪除password encryptionaes 命令都無法解密路由器配置中的口令。一旦密碼加密，就不會解密。如果主金鑰未被刪除，則仍可對配置中的當前加密金鑰進行解密。

此外，為了檢視密碼加密功能的調試型別消息，請在配置模式下使用**password logging**命令。

組態

本文檔在路由器上使用以下配置：

- 加密目前的預先共用金鑰
- 以互動方式新增主索引鍵
- 以互動方式修改目前的主鍵
- 刪除主鍵

加密目前的預先共用金鑰

```
    <#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
```

以互動方式新增主索引鍵

```
    <#root>

Router(config)#


key config-key password-encrypt



New key:


<enter key>


Confirm key:
```

```
<confirm key>

Router(config)#
```

以互動方式修改目前的主鍵

```
    <#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
```

刪除主鍵

```
    <#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)#
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- **IPsec支援頁面**
- **思科技術支援與下載**

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。