ルータでの事前共有鍵の暗号化の設定

内容

はじめに

このドキュメントでは、ルータの現在および新しい事前共有キーの暗号化を設定する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- Cisco IOS XE®ソフトウェアリリース16.9

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

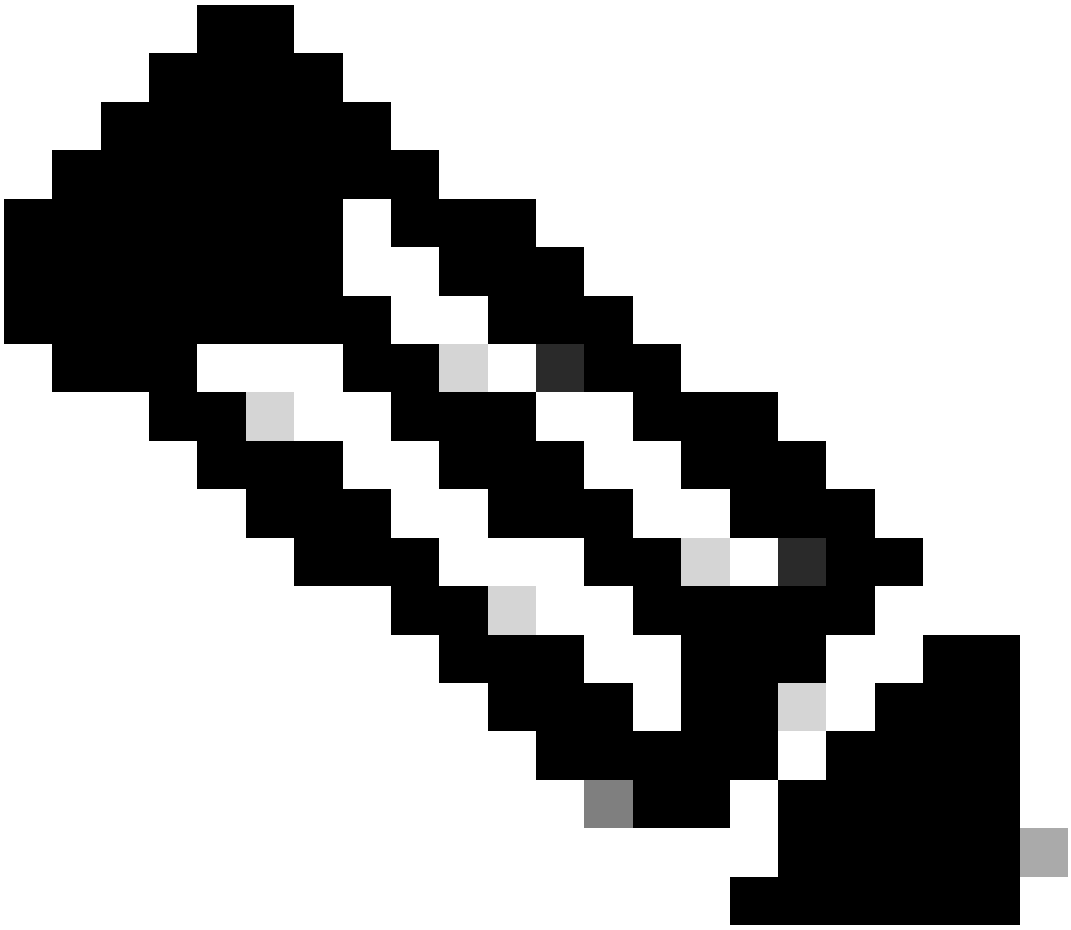
ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

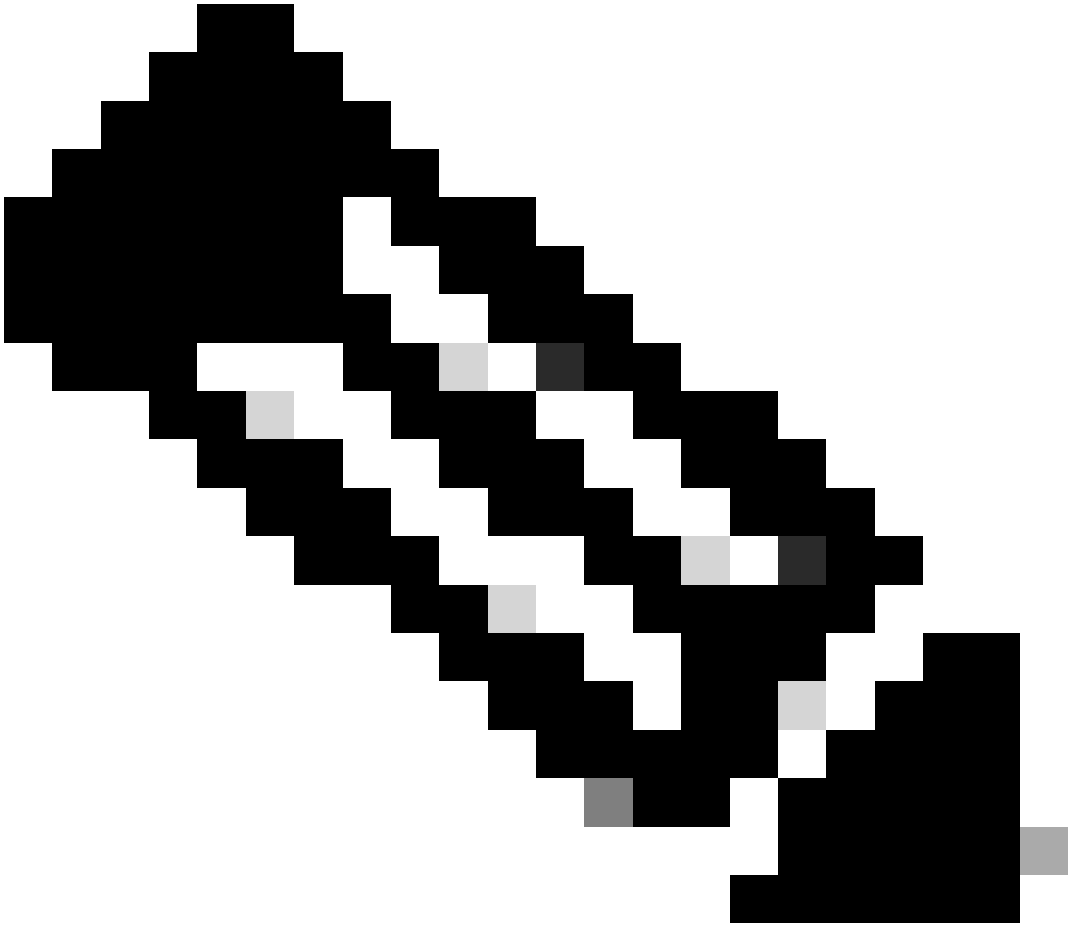
Cisco IOSソフトウェアリリース12.3(2)Tコードでは、ルータがInternet Security Association and Key Management Protocol(ISAKMP)事前共有キーを不揮発性RAM(NVRAM)の不揮発性RAM(NVRAM)のセキュアなタイプ6形式で暗号化できる機能が導入されています。暗号化対象の事前共有キーは、アグレッシブモードのISAKMPキーリングで標準として設定するか、Easy VPN(EzVPN)サーバまたはクライアントのセットアップでグループパスワードとして設定できます。

設定

このセクションでは、このドキュメントで説明している機能の設定に使用するための情報を説明します。



注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。



注：シスコの内部ツールおよび情報にアクセスできるのは、登録ユーザのみです。

事前共有キー(PSK)暗号化を有効にするために、次の2つのコマンドが導入されました。

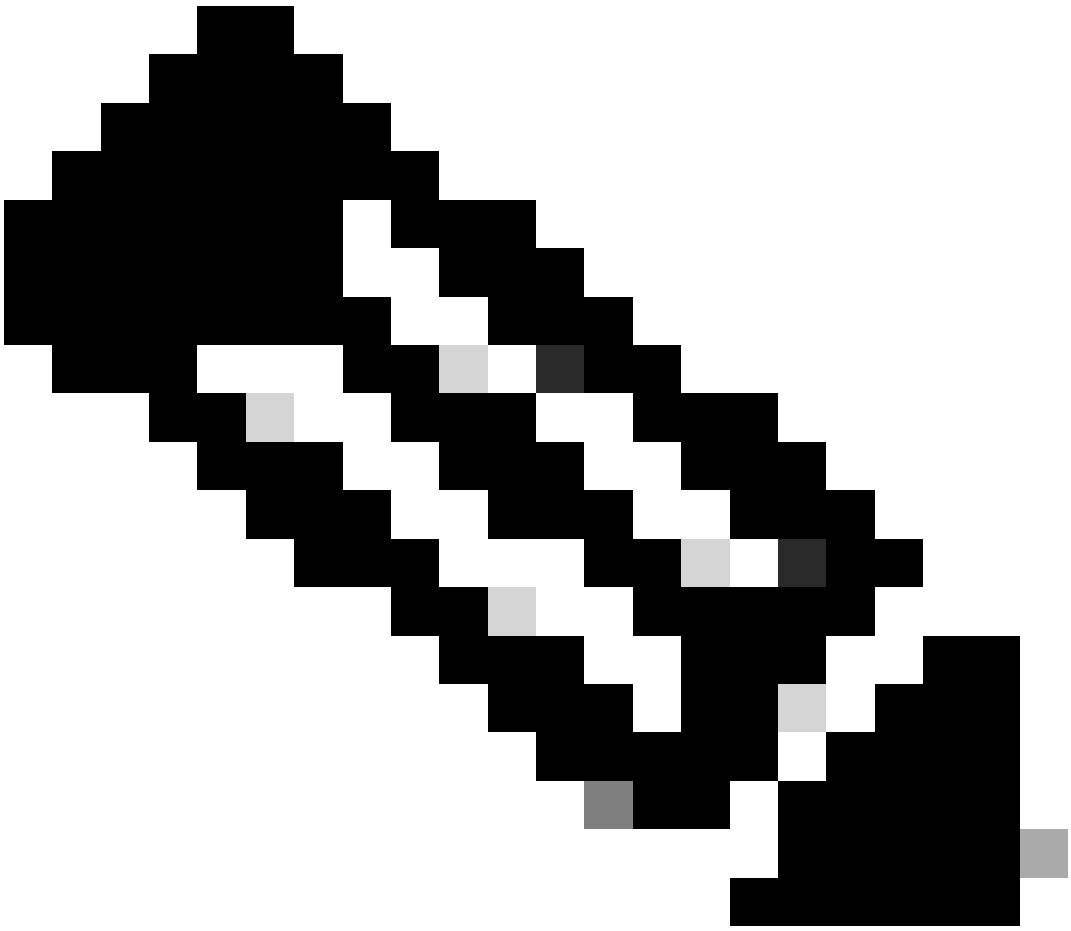
- key config-key password-encryption [プライマリキー]
- password encryption aes

[primary key]は、ルータ設定のその他すべてのキーを、Advance Encryption Standard（AES；高度暗号化規格）の対称暗号を使用して暗号化するために使用するパスワード/キーです。プライマリキーはルータ設定には保存されず、ルータに接続している間は、プライマリキーを表示したりプライマリキーを取得したりすることはできません。

設定後は、ルータ設定の現在のキーまたは新しいキーの暗号化にプライマリキーが使用されます。[primary key]がコマンドラインで指定されていない場合、ルータはユーザに対してキーの入力を求め、確認のためにもう一度入力するよう求めます。キーがすでに存在している場合は、まず古いキーを入力するようにプロンプトが表示されます。キーの暗号化は、password encryption aes コマンドを発行するまでは実行されません。

プライマリキーは、key config-key... コマンドを新しい[primary-key]でもう一度使用して変更できます（ただし、これはキーが何らかの形で侵害されない限り、必要ではありません）。 ルータ設定内の現在の暗号化キーはすべて、新しいキーで再暗号化されます。

no key config-key...を発行すると、プライマリキーを削除できます。 ただし、これによって、ルータ設定で現在設定されているすべてのキーが役に立たなくなります（これに関する詳細とプライマリキーの削除を確認する警告メッセージが表示されます）。プライマリキーが存在しなくなるため、タイプ6パスワードは復号化できず、ルータで使用できません。



注：セキュリティ上の理由から、プライマリキーやpassword encryption aes コマンドを削除しても、ルータ設定のパスワードは復号化されません。パスワードは暗号化されると、復号化されません。設定内の現在の暗号化キーは、プライマリキーが削除されていなくても復号化できます。

また、パスワード暗号化機能のデバッグタイプメッセージを表示するには、コンフィギュレーションモードで**password logging**コマンドを使用します。

コンフィギュレーション

このドキュメントでは、ルータでの次の設定を使用しています。

- 現在の事前共有キーの暗号化
- 新しい主キーを対話形式で追加する
- 現在の主キーを対話的に変更する
- 主キーの削除

現在の事前共有キーの暗号化
<#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
```

新しい主キーを対話形式で追加する

```
    <#root>

Router(config)#


key config-key password-encrypt


New key:
```

```
<enter key>


Confirm key:


<confirm key>


Router(config)#
```

現在の主キーを対話的に変更する

```
    <#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
```

主キーの削除

```
    <#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)#
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- **IPSec サポート ページ**
- **シスコのテクニカルサポートとダウンロード**

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。