Cisco IOS ルータの暗号化事前共有キーの設定例

目次

はじめに

Cisco IOS® ソフトウェア リリース 12.3(2)T コードには、ルータで、不揮発性 RAM (NVRAM) 内の ISAKMP 事前共有キーをセキュア タイプ 6 形式で暗号化す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、ISAKMP キー リングにはアグレッシブ モードでの標準として、あるいは、EzVPN サーバやクライアントの設定にはグループ パスワードとして設定可能なものです。 この設定例では、既存の事前共有キーと新しい事前共有キーの両方の暗号化の設定方法を説明します。

前提条件

要件

このドキュメントに関しては個別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 ソフトウェア リリース 12.3(2)T

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『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。

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。

事前共有キーの暗号化を使用可能にするために、次の 2 つの新しいコマンドが追加されています。

- **key config-key password-encryption [マスター キー]**
- **password encryption aes**

[マスター キー] は、ルータ設定での他のすべてのキーの暗号化に使用するパスワードまたはキーです。この暗号化では、Advance Encryption Standard（AES）の対称暗号を使用します。 マスター キーはルータ設定には保存されず、ルータに接続中の場合に、このキーを表示または取得する方法はありません。

これが設定されていると、ルータ設定での既存のキーと新しいキーのすべての暗号化に、このマスター キーが使用されます。 コマンドラインで [マスター キー] が指定されなかった場合は、ルータから、キーの入力と確認用の再入力のプロンプトが表示されます。 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。

マスター キーを変更するには（何らかの方法によってキーの機密性が損なわれない限り必要ありませんが）、key config-key... コマンドを新しい [マスター キー] で再発行します。 ルータ設定での既存の暗号化キーは、すべてこの新しいキーで再暗号化されます。

マスター キーを削除する場合は、no key config-key... を発行します。 ただし、現在、ルータ設定に設定されているキーはすべて使用できなくなります（この説明が表示され、マスター キーの削除を確認する警告メッセージが表示されます）。 マスター キーが存在しなくなると、タイプ 6 のパスワードは、ルータでの暗号化解除と使用ができなくなります。

注: セキュリティ上の理由から、マスター キーや password encryption aes コマンドを削除しても、ルータ設定での各パスワードは暗号化解除されません。 パスワードは一度暗号化されると、暗号化解除されることはありません。 マスター キーが削除されていなければ、設定内の既存の暗号化キーは暗号化解除が可能です。

また、パスワードの暗号化機能のデバッグ タイプの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。

設定

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。

- 既存の事前共有キーの暗号化
- 対話形式による新しいマスター キーの追加
- 対話形式による既存のマスター キーの修正
- マスター キーの削除

既存の事前共有キーの暗号化

```
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
```

対話形式による新しいマスター キーの追加

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

対話形式による既存のマスター キーの修正

```
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
```

マスター キーの削除

```
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)#
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

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

- 暗号化事前共有キー
- IPsec に関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems