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。 暗号化する事前共有キーは、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、または EZVPN サーバあるいはクライアントの設定でグループ パスワードとして設定することができます。 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を設定する方法について詳しく説明します。

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。

これら二つの新しいコマンドは事前共有キー 暗号化を有効に するためにもたらされます:

- **キー config-key パスワード暗号化*[マスタ鍵]***
- **password encryption aes**

[マスタ鍵] Advance Encryption Standard（AES）対称暗号の使用のルータコンフィギュレーションの他のキーをすべて暗号化するのに使用されるパスワード/キーはです。 マスタ鍵はルータコンフィギュレーションでルータに接続されている間保存されないし、どうにか見られるか、または得る*ことができません*。

設定されて、マスタ鍵がルータコンフィギュレーションの既存か新しいキーを暗号化するのに使用されています。 *[マスタ鍵]*コマンド･ ラインで、ルータプロンプト ユーザ キーを入力し、確認のためにそれを再入力するために規定 されなければ。 既に存在 する古いキーを最初に入力するためにキーがユーザ プロンプト表示されれば。 キーは **password encryption aes コマンドを**発行するまで暗号化されません。

マスタ鍵は新しいのの**キー config-key**…コマンドを再度発行することによってキーが何らかのかたちで妥協されるようにならなかったら（これが必要ではないはずであるが）変更することができます*[マスタ鍵]*。 ルータコンフィギュレーションのどの存在暗号化されたキーでも New 鍵によって再び暗号化されます。

No 鍵 config-key を….発行するときマスタ鍵を削除できます ただし、これはこれを詳述し、マスタ鍵 削除を確認する）ルータコンフィギュレーションのすべての現在設定されたキーを無意味なものにします（警告メッセージ ディスプレイ。 もはや存在 する マスタ鍵以来型 6 パスワードはルータによって非暗号化および使用されて。

注: セキュリティの理由から、マスタ鍵の取り外し、**password encryption aes コマンド** unencrypts の取り外しルータコンフィギュレーションのパスワード。 パスワードが暗号化されれば、非暗号化ではないです。 設定の既存の暗号化キーは非暗号化ですまだ提供しましたマスタ鍵を取除かれません。

さらに、パスワード暗号化機能のデバッグ型メッセージを見るために、コンフィギュレーションモードで **password logging コマンドを**使用して下さい。

設定

この資料はルータのこれらのコンフィギュレーションを使用します:

- 既存の事前共有キーを暗号化して下さい
- 新しいマスタ鍵を対話型で追加して下さい
- 既存のマスタ鍵を対話型で修正して下さい
- マスタ鍵を削除して下さい

既存の事前共有キーを暗号化して下さい

```
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
```

新しいマスタ鍵を対話型で追加して下さい

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

既存のマスタ鍵を対話型で修正して下さい

```
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
```

マスタ鍵を削除して下さい

```
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

- 暗号化事前共有鍵
- 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