Configure the Encrypt Pre-shared Keys in a Router

Contents

Introduction

This document describes how to set up encryption of both current and new pre-shared keys in a router.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on this software version:

- Cisco IOS XE® Software Release 16.9

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Cisco IOS Software Release 12.3(2)T code introduces the functionality that allows the router to encrypt the Internet Security Association and Key Management Protocol (ISAKMP) pre-shared key in secure type 6 format in nonvolatile RAM, Non-Volatile RAM (NVRAM). The pre-shared key to be encrypted can be configured either as standard, under an ISAKMP key ring, in aggressive mode, or as the group password under an Easy VPN (EzVPN) server or client setup.

Configure

This section presents you with the information you can use to configure the features this document describes.

> **Note**: Use the Command Lookup Tool to obtain more information on the commands used in this section.

> **Note**: Only registered Cisco users can access internal Cisco tool and information.

These two commands were introduced in order to enable pre-shared key encryption:

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

The **[primary key]** is the password/key used to encrypt all other keys in the router configuration with the use of an Advance Encryption Standard (AES) symmetric cipher. The primary key is *not* stored in the router configuration and *cannot* be seen or obtained in any way while connected to the router.

Once configured, the primary key is used to encrypt any current or new keys in the router configuration. If the **[primary key]** is not specified on the command line, the router prompts the user to enter the key and to re-enter it for verification. If a key already exists, the user is prompted to enter the old key first. Keys are not encrypted until you issue the **password encryption aes** command.

The primary key can be changed (although this is not be necessary unless the key has become compromised in some way) with the **key config-key...** command again with the new **[primary-key]**. Any current encrypted keys in the router configuration are re-encrypted with the new key.

You can delete the primary key when you issue the **no key config-key...**. However, this renders all currently configured keys in the router configuration useless (a warning message displays that details this and confirms the primary key deletion). Since the primary key no longer exists, the type 6 passwords cannot be decrypted and used by the router.

> **Note**: For security reasons, neither the removal of the primary key, nor the removal of the password encryption aes command decrypts the passwords in the router configuration. Once passwords are encrypted, they are not decrypted. Current encrypted keys in the configuration can still be decrypted provided the primary key is not removed.

Additionally, in order to see debug-type messages of password encryption functions, use the **password logging** command in the configuration mode.

Configurations

This document uses these configurations on the router:

- Encrypt the Current Pre-shared Key
- Add a New Primary Key Interactively

- Modify the Current Primary Key Interactively
- Delete the Primary Key

Encrypt the Current Pre-shared Key

<#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
```

Add a New Primary Key Interactively

<#root>

```
Router(config)#

key config-key password-encrypt


New key:

<enter key>

Confirm key:

<confirm key>

Router(config)#
```

Modify the Current Primary Key Interactively

```
<#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
```

Delete the Primary Key

```
<#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)#
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshoot information available for this configuration.

Related Information

- **IPsec Support Page**
- **Cisco Technical Support & Downloads**