Содержание

Введение

В выпуске программного обеспечения Cisco IOS® Software Release 12.3(2)T реализована функциональность, которая позволяет маршрутизатору шифровать предварительный общий ключ ISAKMP в защищенном формате типа 6 в энергонезависимой памяти (NVRAM). Шифруемый предварительный общий ключ может быть настроен в качестве стандартного, в связке ключей ISAKMP, в агрессивном режиме или как пароль группы в настройках сервера или клиента EzVPN. Этот пример конфигурации подробно описывает настройку шифрования для существующих и новых предварительных общих ключей.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на этой версии программного обеспечения:

- ПО Cisco IOS версии 12.3(2)T

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

В данном разделе приводятся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Эти две новых команды представлены для включения шифрования предварительного общего ключа:

- **key config-key password-encryption** *[главный ключ]*
- **password encryption aes**

[Главный ключ] пароль/ключ, используемый для шифрования всех других ключей в конфигурации маршрутизатора с использованием симметричного шифра Стандарта шифрования усовершенствования (AES). Главный ключ не сохранен в конфигурации маршрутизатора и *не может* быть замечен или получен в любом случае, в то время как связано с маршрутизатором.

После того, как настроенный, главный ключ используется для шифрования любых существующих или новых ключей в конфигурации маршрутизатора. Если *[главный ключ]* не задан на командной строке, маршрутизатор побуждает пользователя вводить ключ и повторно вводить его для проверки. Если ключ уже существует, пользователю предлагают ввести старый ключ сначала. Ключи не зашифрованы, пока вы не выполняете **команду password encryption aes**.

Главный ключ может быть изменен (невзирая на то, что это не должно быть необходимо, пока ключ не стал поставившим под угрозу в некотором роде) путем запуска **команды key config-key...** снова с новым *[отмычка]*. Любые существующие зашифрованные ключи в конфигурации маршрутизатора повторно шифруются с новым ключом.

Когда вы не выполняете **key config-key,** можно удалить главный ключ**....** Однако это представляет все в настоящее время настраиваемые ключи в бесполезной конфигурации маршрутизатора (предупреждающее сообщение отображается, который детализирует это и подтверждает удаление главного ключа). Так как главный ключ больше не существует, пароли типа 6 не могут быть дешифрованы и использоваться маршрутизатором.

Примечание: Из соображений безопасности ни удаление главного ключа, ни удаление **команды password encryption aes** не дешифровали пароли в конфигурации маршрутизатора. Как только пароли зашифрованы, они *не* дешифрованы. Существующие зашифрованные ключи в конфигурации все еще в состоянии быть дешифрованными, если не удален главный ключ.

Кроме того, для наблюдения сообщений типа отладки функций шифрования пароля, используйте **команду password logging** в режиме конфигурации.

Конфигурации

Этот документ использует эти конфигурации на маршрутизаторе:

- Зашифруйте существующий предварительный общий ключ

- Добавьте новый главный ключ в интерактивном режиме
- Модифицируйте существующий главный ключ в интерактивном режиме
- Удалите главный ключ

Зашифруйте существующий предварительный общий ключ

```
Router#show running-config Building
configuration.....crypto isakmp policy 10 authentication
pre-sharecrypto isakmp key cisco123 address
10.1.1.1..endRouter#configure terminalEnter
configuration commands, one per line.  End with
CNTL/Z.Router(config)#key config-key password-encrypt
testkey123Router(config)#password encryption
aesRouter(config)#^ZRouter#Router#show running-config
Building configuration.....password encryption
aes..crypto isakmp policy 10 authentication pre-
sharecrypto isakmp key 6
FLgBaJHXdYY_AcHZZMgQ_RhTDJXHUBAAB address 10.1.1.1..end
```

Добавьте новый главный ключ в интерактивном режиме

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

Модифицируйте существующий главный ключ в интерактивном режиме

```
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
```

Удалите главный ключ

```
Router(config)#no key config-key password-encrypt
WARNING: All type 6 encrypted keys will become
unusableContinue with master key deletion ? [yes/no]:
yesRouter(config)#
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Зашифрованный общий ключ
- Страница поддержки IPSec
- Cisco Systems – техническая поддержка и документация