"Пример установки паролей на Telnet, консоль и вспомогательный порт на маршрутизаторе Cisco"

Содержание

Введение

В этом документе приведены примеры конфигураций для настройки защиты паролем при входящих соединениях EXEC с маршрутизатором.

Предварительные условия

Требования

Чтобы выполнить задачи, описанные в данном документе, необходимо иметь привилегированный доступ EXEC к интерфейсу командной строки маршрутизатора.

Сведения об использовании командной строки и командных режимов см. в документе об использовании Cisco IOS.

Инструкции по подключению консоли к маршрутизатору см. в документации, поставляемой вместе с маршрутизатором, или обратитесь к интерактивной документации для нужного оборудования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Маршрутизатор Cisco 2509
- Версия 12.2 (19) программного обеспечения Cisco IOS

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

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Общие сведения

Использование функции защиты по паролю для контроля или ограничения доступа к интерфейсу командной строки (CLI) вашего маршрутизатора является одним из основных элементов общего плана безопасности.

Защита маршрутизатора от неавторизованного удалённого доступа, обычно Telnet – самое обычное средство защиты, нуждающееся в конфигурации, однако защиту маршрутизатора от неавторизованного локального доступа нельзя упускать из виду.

Примечание: Защита с помощью пароля – лишь один из множества способов, которые следует использовать для эффективного и безопасного режима работы сети. Межсетевые экраны, access-lists и контроль физического доступа к оборудованию являются другими элементами, которые нужно рассмотреть при реализации плана обеспечения безопасности.

Доступ к командной строке или строке EXEC маршрутизатора может быть получен разными способами, но во всех случаях входящее соединение с маршрутизатором осуществляется по каналу TTY. **Как видно их примера выходных данных по команде show line, существует четыре основных типа каналов TTY:**

```
2509#show line Tty Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int* 0 CTY - - - - - 0 0
0/0 - 1 TTY 9600/9600 - - - - - 0 0 0/0 - 2 TTY 9600/9600 - - - - - 0 0 0/0 - 3 TTY 9600/9600 -
- - - - 0 0 0/0 - 4 TTY 9600/9600 - - - - - 0 0 0/0 - 5 TTY 9600/9600 - - - - - 0 0 0/0 - 6 TTY
9600/9600 - - - - - 0 0 0/0 - 7 TTY 9600/9600 - - - - - 0 0 0/0 - 8 TTY 9600/9600 - - - - - 0 0
0/0 - 9 AUX 9600/9600 - - - - - 0 0 0/0 - 10 VTY - - - - - 0 0 0/0 - 11 VTY - - - - - 0 0 0/0 -
12 VTY - - - - - 0 0 0/0 - 13 VTY - - - - - 0 0 0/0 - 14 VTY - - - - - 0 0 0/0 -2509#
```

Тип строки CTY - это консольный порт. В конфигурации любого маршрутизатора она

появляется в виде line con 0, а в выходных данных команды show line – в виде cty. Консольный порт в основном используется для доступа к локальным системам с помощью консольного терминала.

Линии TTY – это асинхронные линии, которые используются для входящих или исходящих модемных соединений и подключений терминала. Они обозначаются в конфигурации маршрутизатора или сервера доступа как "линии x". Особые номера линий - это функция оборудования, встроенного или установленного на маршрутизатор или сервер доступа.

Линия AUX – это вспомогательный порт, отображаемый в конфигурации как line aux 0.

Линии VTY – это линии связи виртуального терминала маршрутизатора, используемые исключительно для управления входящими соединениями Telnet. Они являются действительными, в том смысле, что они - функция программного обеспечения - нет никаких аппаратных средств, привязанных к ним. **Они отображены в конфигурации в виде строки vty 0 4.**

Можно настроить каждый из этих типов каналов связи защитой по паролю. Линии могут быть настроены для использования одинакового пароля для всех пользователей или паролей для отдельных пользователей. Пароли пользователей могут быть настроены локально на маршрутизаторе, либо можно использовать сервер аутентификации для предоставления аутентификации.

Никаких запретов на установление разных типов защиты паролем на разных линиях не существует. Хотя широко распространена практика применения на маршрутизаторе одного пароля для консоли и отдельных для каждого пользователя паролей для других входящих соединений.

Ниже приведен пример выходных данных маршрутизатора для команды show running-config:

```
2509#show running-configBuilding configuration...Current configuration : 655 bytes!version
12.2.. . !--- Configuration edited for brevityline con 0line 1 8line aux 0line vty 0 4!end
```

Настройте пароли на линии

Для задания пароля в строке используется команда password в режиме настройки с командной строкой. Чтобы включить проверку пароля при подключении, воспользуйтесь командой login в режиме конфигурации линии.

Примечание: Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" (Поиск команд) (только для зарегистрированных клиентов).

Процедура конфигурации

В этом примере пароль настраивается для всех пользователей, которым нужно использовать консоль.

1. Из привилегированного приглашения EXEC (или "enable") войдите в режим конфигурации и перейдите в режим линейной конфигурации с помощью следующих команд. Обратите внимание, что приглашение изменяется в зависимости от текущего режима.router#**configure terminal**Enter configuration commands, one per line. End with

CNTL/Z.router(config)#**line con 0**router(config-line)#

2. Настройте пароль и включите проверку пароля при входе.router(config-line)#**password letmein**router(config-line)#**login**
3. Выйдите из режима конфигурирования.router(config-line)#**end**router#%SYS-5-CONFIG_I: Configured from console by console **Примечание:** Не делайте save configuration changes к **line con 0**, пока не была проверена ваша способность войти.

Примечание: Под конфигурацией line console **вход в систему** является командой требуемой конфигурации к проверке enable password при входе в систему. Консольная аутентификация требует, чтобы работали и **пароль** и команды **входа в систему**.

Проверка конфигурации

Проверьте конфигурацию маршрутизатора, чтобы удостовериться в том, что команды вводились корректно:

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

- **show running-config - вывод текущей конфигурации маршрутизатора.**router#**show running-config**Building configuration.....*!--- Lines omitted for brevity*!line con 0**password letmeinlogin**line 1 8line aux 0line vty 0 4!end Для тестирования конфигурации выполните разрегистрацию с консоли и повторно зарегистрируйтесь, используя настроенный пароль для доступа к маршрутизатору:router#**exit**router con0 is now availablePress RETURN to get started.User Access VerificationPassword: *!--- Password entered here is not displayed by the router*router> **Примечание:** Перед выполнением данного теста убедитесь, что имеется альтернативное подключение к маршрутизатору, такое как Telnet или удаленное, на случай возникновения проблемы повторного входа на маршрутизатор.

Устранение сбоев входа в систему

Если не удается выполнить повторный вход в маршрутизатор, а конфигурация не сохранена, то перезагрузка маршрутизатора приведет к отмене всех внесенных изменений.

Если же изменения в конфигурации были сохранены, а повторный вход на маршрутизатор выполнить не удается, пароль придется восстанавливать. Для получения инструкций по определенной платформе см. раздел "Процедуры восстановления пароля".

Настройка локальных паролей для отдельных пользователей

Для установки системы аутентификации на основе имени пользователя используйте команду username в режиме глобальной конфигурации. Чтобы включить проверку пароля при входе, используйте команду login local в режиме линейной конфигурации.

Процедура конфигурации

В этом примере пароли настроены для пользователей, которые осуществляют попытки подключиться к маршрутизатору на линиях VTY по протоколу Telnet.

1. Из привилегированного приглашения EXEC (или "enable") необходимо войти в режим

настройки и ввести комбинации имен пользователей и паролей по одной для каждого пользователя, которому планируется разрешить доступ к маршрутизатору:`router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. router(config)#username russ password montecito router(config)#username cindy password belgium router(config)#username mike password rottweiler`

2. Переключитесь в режим настройки с помощью следующих команд. Обратите внимание, что приглашение изменяется в зависимости от текущего режима.`router(config)#line vty 0 4router(config-line)#`
3. Настройка проверки пароля при входе.`router(config-line)#login local`
4. Выйдите из режима конфигурирования.`router(config-line)#endrouter#%SYS-5-CONFIG_I: Configured from console by console` **Примечание:** Для отключения автоматической Telnet, когда вы вводите имя на CLI, настраиваете **никакую регистрацию, предпочтенную** на линии, которая используется. В то время как **transport preferred none** предоставляет те же выходные данные, он также отключает автоматическую Telnet для определенного хоста, которые настроены с **командой ip host**. Это непохоже **на команду no logging preferred**, которая останавливает его для неопределенных хостов и позволяет ему работать для определенных.

Проверка конфигурации

Проверьте конфигурацию маршрутизатора, чтобы удостовериться в том, что команды вводились корректно:

- **show running-config - вывод текущей конфигурации маршрутизатора.**`router#show running-configBuilding configuration...!!--- Lines omitted for brevity !username russ password 0 montecitousername cindy password 0 belgiumusername mike password 0 rottweiler!!--- Lines omitted for brevity !line con 0line 1 8line aux 0line vty 0 4 login local!end` Для того чтобы протестировать эту конфигурацию, к маршрутизатору должны быть выполнено подключения Telnet. **Это можно сделать путем подключения от другого узла сети. Либо выполните проверку от самого маршрутизатора, организовав доступ по протоколу Telnet к IP-адресу любого интерфейса на маршрутизаторе в состоянии up/up, как показывают выходные данные команды show interfaces.Ниже приведен образец выхода, если бы адрес интерфейса ethernet 0 был 10.1.1.1:**`router#telnet 10.1.1.1Trying 10.1.1.1 ... OpenUser Access VerificationUsername: mikePassword:!--- Password entered here is not displayed by the router router`

Устранение неполадок, связанных с паролем пользователя

Имена пользователей и пароли интерпретируются с учетом регистра символов. Вход пользователей с использованием неверного имени пользователя или пароля запрещается.

Если пользователи не могут войти в систему маршрутизатора со своими паролями, измените имена пользователей и пароли на маршрутизаторе.

Настройте пароль линии AUX

Для определения пароля на линии AUX выполните команду **пароля** в режиме конфигурации с командной строки. Чтобы к проверке enable password при входе в систему, выполните команду **входа в систему** в режиме конфигурации с командной строки.

Процедура конфигурации

В данном примере пароль настроен для всех пользователей, пытающихся использовать Порт AUX.

1. Выполните **команду show line** для проверки линии, используемой Портом AUX.`R1#show line Tty Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int* 0 CTY - - - - - 0 0 0/0 - 65 AUX 9600/9600 - - - - - 0 1 0/0 - 66 VTY - - - - - 0 0 0/0 - 67 VTY - - - - - 0 0 0/0 -`
2. В данном примере Порт AUX находится на линии 65. Выполните эти команды для настройки линии AUX маршрутизатора:`R1# conf tR1(config)# line 65R1(config-line)#modem inoutR1(config-line)#speed 115200R1(config-line)#transport input allR1(config-line)#flowcontrol hardwareR1(config-line)#loginR1(config-line)#password ciscoR1(config-line)#endR1#`

Проверка конфигурации

Исследуйте конфигурацию маршрутизатора, чтобы проверить, что были должным образом введены команды:

- **Команда show running-config** отображает текущую конфигурацию маршрутизатора:`R1#show running-configBuilding configuration...!--- Lines omitted for brevity.line aux 0 password cisco login modem InOut transport input all speed 115200 flowcontrol hardware!--- Lines omitted for brevity.!end`

Настройте проверку подлинности AAA для начала сеанса

Чтобы включить AAA для регистрации, используйте команду login authentication в режиме линейной конфигурации. Также необходимо настроить службы AAA.

Процедура конфигурации

Данный пример отображает настройку маршрутизатора на получение паролей пользователей от сервера TACACS+, когда пользователи пытаются подключиться к маршрутизатору.

Примечание: Настройка маршрутизатора для использования серверов AAA других типов (например, RADIUS) проводится аналогично. Дополнительные сведения см. в разделе "Настройка аутентификации".

Примечание: Этот документ не обращается к конфигурации самого AAA-сервера. Сведения о настройке AAA-сервера см. в разделе "Протоколы сервера защиты ".

1. В командной строке, работающей в привилегированном режиме EXEC (или "включенный"), войдите в режим настройки и введите команды для настройки маршрутизатора таким образом, чтобы он мог использовать службы AAA для аутентификации:`router#configure terminalEnter configuration commands, one per line. End with CNTL/Z.router(config)#aaa new-modelrouter(config)#aaa authentication login my-auth-list tacacs+router(config)#tacacs-server host 192.168.1.101router(config)#tacacs-server key letmein`
2. Переключитесь в режим настройки с помощью следующих команд. Обратите

внимание, что приглашение изменяется в зависимости от текущего режима.`router(config)#`**`line 1 8`**`router(config-line)#`

3. Настройка проверки пароля при входе.`router(config-line)#login authentication my-auth-list`
4. Выйдите из режима конфигурирования.`router(config-line)#`**`end`**`router#%SYS-5-CONFIG_I: Configured from console by console`

Проверка конфигурации

Проверьте конфигурацию маршрутизатора, чтобы удостовериться в том, что команды вводились корректно:

- **show running-config - вывод текущей конфигурации маршрутизатора.**`router#`**`write terminal`**`Building configuration...Current configuration:!version 12.0service timestamps debug uptimeservice timestamps log uptimeno service password-encryption!hostname router!`**`aaa new-modelaaa authentication login my-auth-list tacacs+`**`!`*`!--- Lines omitted for brevity`*`...!`**`tacacs-server host 192.168.1.101tacacs-server key letmein`**`!line con 0line 1 8 `**`login authentication my-auth-list`**`line aux 0line vty 0 4!end`

Для того, чтобы протестировать данную конфигурацию, для линии должны быть настроены входящее и исходящее подключения. Конкретные сведения по настройке асинхронных линий для модемных подключений см. в Руководстве по подключению модем-маршрутизатор.

В качестве альтернативного решения можно настроить одну или более VTY линий для осуществления AAA аутентификации и на ее основе – тестирования.

Устранение неполадок при сбое AAA

Прежде чем применять команды отладки, ознакомьтесь с разделом "Важные сведения о командах отладки".

Для отладки неудачной попытки регистрации выполните команду отладки, соответствующую вашей конфигурации:

- debug aaa authentication
- debug radius
- debug kerberos

Дополнительные сведения

- Настройка аутентификации
- Ссылка команды отладки Cisco IOS
- Техническая поддержка - Cisco Systems