Настройка основных средств аутентификации, авторизации и учета на сервере доступа

Содержание

Введение
Перед началом работы
Условные обозначения
Предварительные условия
Используемые компоненты
Схема сети
Общая настройка AAA
Включение AAA
Выбор внешнего сервера AAA
Настройка сервера AAA
Настройка аутентификации
Аутентификация при входе в систему
Аутентификация по протоколу PPP
Настройка авторизации
Авторизация выполнения
Авторизация сети
Настройка учета
Примеры настройки учета
Дополнительные сведения

Введение

В данном документе объясняется, как настроить аутентификацию, авторизацию и учет (Authentication, Authorization and Accounting — AAA) на маршрутизаторе Cisco с использованием протоколов Radius или TACACS+. Целью данного документа является не перечисление всех функций аутентификации, авторизации и учета, а объяснение основных команд с примерами и рекомендациями.

Примечание: Считайте раздел по Общей конфигурации AAA перед продолжением конфигурации Cisco IOS®. В противном случае возможны ошибки в настройке и последующая блокировка.

Перед началом работы

Условные обозначения

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

Предварительные условия

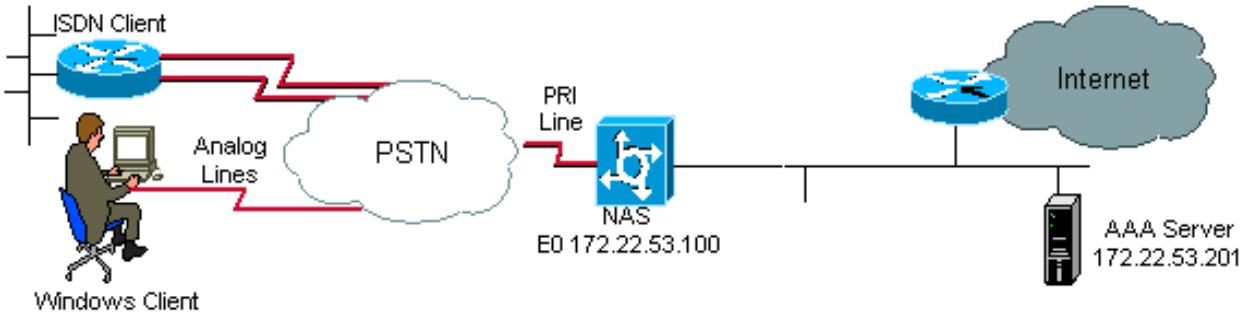
Обзор и подробные сведения о командах и параметрах аутентификации, авторизации и учета содержатся в документе Руководство по настройке безопасности IOS 12.2: аутентификация, авторизация и учет.

Используемые компоненты

Информация в данном документе основана на программном обеспечении основной линии Cisco IOS версии 12.1.

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Схема сети



Общая настройка AAA

Включение AAA

Чтобы включить AAA, настройте в глобальной конфигурации команду aaa new-model.

Примечание: Пока эта команда не включена, все другие команды AAA скрыты.

% Warning: Команда aaa new-model сразу применяет локальную проверку подлинности ко всем линиям и интерфейсам (кроме строки консоли **line con 0**). Если сеанс Telnet установлен с маршрутизатором после активации этой команды (или если время ожидания соединения истекло и требуется повторное соединение), пользователь должен пройти аутентификацию с использованием локальной базы данных маршрутизатора. Чтобы избежать блокировки маршрутизатором, перед началом настройки AAA рекомендуется определить на сервере доступа имя пользователя и пароль. Сделайте это следующим образом:

```
Router(config)# username xxx password yyy
```

Совет: Сохраните свою конфигурацию до настройки ваших команд AAA. Только после того,

как вы полностью завершите настройку AAA (и удостоверитесь в правильности работы), можно сохранить конфигурацию снова. Это позволяет проводить восстановление после непредвиденных блокировок (до сохранения конфигурации) путем перезагрузки маршрутизатора.

Выбор внешнего сервера AAA

В глобальной конфигурации определите протокол безопасности, используемый с функциями AAA (Radius, TACACS+). Если эти два протокола не подходят, можно использовать локальную базу данных на маршрутизаторе.

Если вы используете протокол TACACS+, введите команду tacacs-server host <IP-адрес_сервера_AAA> <ключ>.

Если вы используете протокол Radius, введите команду radius-server host <IP-адрес_сервера_AAA> <ключ>.

Настройка сервера AAA

На сервере AAA настройте следующие параметры:

- Имя сервера доступа.
- IP-адрес, который сервер доступа использует для связи с сервером AAA.**Примечание:** Если оба устройства расположены в одной и той же сети Ethernet, то по умолчанию при отправке пакета AAA сервер доступа использует IP-адрес, определенный в интерфейсе Ethernet. Эта проблема становится важной, когда маршрутизатор имеет несколько интерфейсов (и соответственно несколько адресов).
- *Тот же ключ <ключ>, что и заданный на сервере доступа.***Примечание:** Ключ учитывает регистр.
- Протокол, используемый сервером доступа (TACACS+ или RADIUS).

Точная процедура, используемая для настройки указанных выше параметров, описана в документации сервера AAA. Если сервер AAA настроен неверно, запросы AAA от сетевого устройства хранения данных будут игнорироваться сервером AAA и подключение может быть прервано.

Сервер AAA должен быть доступен по IP-протоколу с сервера доступа (выполните эхо-запрос для проверки подключения).

Настройка аутентификации

Аутентификация служит для проверки личности пользователей, прежде чем им будет предоставлен доступ к сети и к сетевым сервисам (для проверки которых используется авторизация).

Настройка аутентификации AAA:

1. Сначала определите именованный список способов аутентификации (в режиме глобальной конфигурации).
2. Примените данный список к одному или нескольким интерфейсам (в режиме

конфигурации интерфейса).

Единственным исключением является список методов по умолчанию (который называется «default»). Список методов по умолчанию автоматически применяется ко всем интерфейсам, кроме тех, у которых есть явно определенный именованный список методов. Определенный список методов переопределяет список методов по умолчанию.

Ниже приведены примеры аутентификации по протоколу Radius, при входе в систему и по протоколу PPP (наиболее часто используемый способ, чтобы объяснить методы и именованные списки. Во всех примерах протокол TACACS+ может быть заменен Radius или локальной аутентификацией.

Программное обеспечение Cisco IOS использует для аутентификации пользователей первый метод. Если этот метод не отвечает (о чем сообщает слово ERROR), программное обеспечение Cisco IOS выбирает следующий метод аутентификации из списка методов. Этот процесс продолжается до тех пор, пока посредством указанного в списке метода не будет установлено соединение или пока не будет осуществлена попытка подключения всеми указанными способами.

Важно отметить, что программное обеспечение Cisco IOS пытается выполнить аутентификацию с помощью следующего метода из списка, только если предыдущий метод не дал результатов. Если произошел сбой аутентификации на любом этапе цикла, то есть, сервер AAA или локальная база данных имен пользователей отказывается предоставить доступ пользователю (на что указывает слово FAIL), процесс аутентификации останавливается и другие методы не применяются.

Для выполнения аутентификации пользователей необходимо настроить имя пользователя и пароль в сервере AAA.

Аутентификация при входе в систему

При помощи команды aaa authentication login можно выполнить аутентификацию пользователей, которым требуется доступ к серверу доступа с правами выполнения (TTY, VTY, консоль и AUX).

Пример 1: Доступ с правами выполнения с использованием протокола Radius, затем локального метода

```
Router(config)# aaa authentication login default group radius local
```

В приведенной выше команде:

- именованный список — это список по умолчанию (default).
- существуют два метода аутентификации (групповой RADIUS и локальный).

Все пользователи проходят аутентификацию на сервере Radius (первый метод). Если сервер Radius не отвечает, то используется локальная база данных маршрутизатора (второй метод). Для локальной аутентификации определите имя пользователя и пароль:

```
Router(config)# username xxx password yyy
```

Так как используется список по умолчанию в команде aaa authentication login, аутентификация при входе в систему будет автоматически выполнена для всех соединений при входе в систему (таких как TTY, VTY, консоль и AUX).

Примечание: Сервер (Radius или TACACS+) не отвечает на запрос аутентификации AAA, отправленный сервером доступа, если отсутствует IP-соединение, если сервер доступа неправильно определен на сервере AAA либо если сервер AAA неправильно определен на сервере доступа.

Примечание: Если использовать пример, приведенный выше, не включая ключевое слово local, то получится:

```
Router(config)# aaa authentication login default group radius
```

Примечание: Если сервер AAA не отвечает на запрос проверки подлинности, аутентификация закончится неудачей (поскольку маршрутизатор не имеет никакого другого способа).

Примечание: Ключевое слово группы позволяет группировать имеющиеся хосты сервера. Данная возможность позволяет выбирать подмножество настроенных серверных хостов и использовать их для той или иной службы. Дополнительные сведения по этой функции см. в документе Группа серверов AAA.

Пример 2: Доступ к консоли с использованием пароля линии

Расширим конфигурацию, использовавшуюся в примере 1, так чтобы при входе на консоль выполнялась только аутентификация по паролю, заданному для линии консоли 0.

Список CONSOLE определен и применяется к линии консоли 0.

Вводим следующее:

```
Router(config)# aaa authentication login CONSOLE line
```

В приведенной выше команде:

- именованный список – это CONSOLE.
- существует только один способ аутентификации (линейный).

После того, как создан именованный список (в данном случае CONSOLE), чтобы он вступил в силу, его необходимо применить к линии или интерфейсу. *Для этого используется команда login authentication имя_списка:*

```
Router(config)# line con 0
Router(config-line)# exec-timeout 0 0
Router(config-line)# password cisco
Router(config-line)# login authentication CONSOLE
```

Список CONSOLE переопределяет список методов по умолчанию для линии консоли 0. Чтобы получить доступ к консоли, введите пароль «cisco» (настроен для линии консоли 0). Список по умолчанию по-прежнему используется для соединений TTY, VTY и AUX.

Примечание: Для аутентифицирования консольного доступа локальным именем пользователя и паролем используйте:

```
Router(config)# aaa authentication login CONSOLE local
```

Примечание: В этом случае в локальной базе данных маршрутизатора должны быть настроены имя пользователя и пароль. Список необходимо также применить к линии или

интерфейсу.

Примечание: Чтобы не иметь никакой аутентификации, использовать

```
Router(config)# aaa authentication login CONSOLE none
```

Примечание: В данном случае аутентификация при доступе к консоли отсутствует. Список необходимо также применить к линии или интерфейсу.

Пример 3: Переход в привилегированный режим (enable) с использованием внешнего сервера AAA

Чтобы перейти в режим enable, введите команды аутентификации (привилегии уровня 15).

Вводим следующее:

```
Router(config)# aaa authentication enable default group radius enable
```

Будет запрашиваться только пароль, имя пользователя — $enab15$. Следовательно, имя пользователя $enab15$ должно быть определено на сервере AAA.

Если сервер Radius не отвечает, нужно ввести разрешающий пароль, локально настроенный на маршрутизаторе.

Аутентификация по протоколу PPP

Для аутентификации соединения PPP используется команда aaa authentication ppp. Обычно проводится аутентификация удаленных пользователей, подключенных через сеть ISDN или аналоговую сеть, которым нужен доступ к Интернету или к сети центрального офиса через сервер доступа.

Пример 1: Единый метод аутентификации по протоколу PPP для всех пользователей

Сервер доступа имеет интерфейс ISDN, настроенный на прием вызовов от внешних клиентов PPP. **Используется команда dialer rotary-group 0, но настройку можно выполнить на главном интерфейсе или интерфейсе профиля номеронабирателя.**

Вводим следующее

```
Router(config)# aaa authentication ppp default group radius local
```

Эта команда обеспечивает аутентификацию всех пользователей PPP, использующих Radius. Если сервер Radius не отвечает, используется локальная база данных.

Пример 2: Аутентификация по протоколу PPP с помощью определенного списка

Чтобы использовать именованный список вместо списка по умолчанию, введите следующие команды:

```
Router(config)# aaa authentication ppp ISDN_USER group radius Router(config)# int dialer 0
Router(config-if)# pp authentication chap ISDN_USER
```

В этом примере списком является ISDN_USER, а методом — Radius.

Пример 3: Запуск протокола PPP в сеансе в символьном режиме

Сервер доступа имеет внутреннюю плату модема (Mica, Microcom или Next Port). **Предположим, что обе команды — aaa authentication login и aaa authentication ppp — настроены.**

Если пользователь модема сначала получает доступ к маршрутизатору через сеанс выполнения в символьном режиме (например, с помощью окна терминала после набора), аутентификация пользователя выполняется на линии TTY. **Чтобы инициировать сеанс в пакетном режиме, пользователям следует ввести команду ppp default или ppp. Поскольку аутентификация по протоколу PPP настроена явно (с использованием команды aaa authentication ppp), аутентификация пользователя снова выполняется на уровне PPP.**

Чтобы избежать этой повторной аутентификации, можно использовать ключевое слово if-needed.

```
Router(config)# aaa authentication login default group radius local Router(config)# aaa
authentication ppp default group radius local if-needed
```

Примечание: Если клиент начинает сеанс PPP напрямую, аутентификация PPP осуществляется сразу, так как для входа на сервер доступа не требуется регистрации.

Дополнительные сведения об аутентификации AAA см. в документах Руководство по настройке безопасности IOS 12.2: Настройка аутентификации и Примеры практического применения Cisco AAA.

Настройка авторизации

Авторизация — это процесс, который позволяет контролировать, что пользователь может и не может делать.

Правила авторизации AAA идентичны правилам аутентификации:

1. Сначала определите именованный список способов авторизации.
2. Далее примените данный список к одному или нескольким интерфейсам (за исключением списка методов по умолчанию).
3. Используется первый метод в списке; в случае сбоя используется второй метод и т. д.

Списки методов зависят от запрошенного типа авторизации. В данном документе рассматриваются авторизация выполнения и авторизация сети.

Дополнительные сведения о других типах авторизации см. в документе Руководство по настройке безопасности Cisco IOS, выпуск 12.2.

Авторизация выполнения

Команда aaa authorization exec определяет, обладает ли пользователь правами на запуск оболочки EXEC. Это средство должно вернуть информацию о профиле пользователя, такую как данные автокоманд, время ожидания простоя, таймаут сеанса, список доступа, привилегии и другие факторы, индивидуальные для каждого пользователя.

Авторизация выполнения выполняется только по линиям VTY и TTY.

В следующем примере используется Radius.

Пример 1: Одинаковые методы аутентификации выполнения для всех пользователей

Сначала используется команда аутентификации:

```
Router(config)# aaa authentication login default group radius local
```

Все пользователи, которые хотят войти на сервер доступа, должны авторизоваться, используя Radius (первый метод) или локальную базу данных (второй метод).

Вводим следующее:

```
Router(config)# aaa authorization exec default group radius local
```

Примечание: На AAA-сервере, Service-Type=1 (вход в систему) должен быть выбран.

Примечание: С данным примером, если **ключевое слово local** не включено и не отвечает AAA-сервер, то авторизация никогда не будет возможна, и связь прервется.

Примечание: В Примерах 2 и 3 ниже, мы не должны добавлять команду на маршрутизаторе, но только настраивать профиль на сервере доступа.

Пример 2: Назначение уровней привилегий выполнения с сервера AAA

Руководствуясь примером 1, если пользователю, выполняющему вход на сервер доступа, разрешено непосредственно входить в привилегированный режим enable, настройте следующую AV-пару Cisco на сервере AAA:

```
shell:priv-lvl=15
```

Это означает, что пользователь перейдет непосредственно в режим enable.

Примечание: Если для первого метода ответ не получен, то используется локальная база данных. **Однако пользователь не войдет непосредственно в режим enable, ему придется ввести команду enable и указать разрешающий пароль (enable).**

Пример 3: Назначение времени ожидания простоя от сервера AAA

Для настройки времени ожидания простоя (так, чтобы в случае отсутствия трафика по истечении этого времени сеанс прекращался) используйте атрибут RADIUS IETF 28: Idle-Timeout для профиля пользователя.

Авторизация сети

Команда aaa authorization network выполняет авторизацию для всех запросов сетевых сервисов, например PPP, SLIP и ARAP. В этом разделе рассматривается протокол PPP, который наиболее часто используется.

Сервер AAA проверяет, разрешен ли сеанс PPP для клиента. Более того, клиент может

запросить параметры PPP: обратный вызов, сжатие, IP-адрес и т.п. Данные параметры необходимо настраивать в профиле пользователя на сервере AAA. Для определенного клиента профиль AAA может содержать время ожидания простоя, список доступа и другие атрибуты пользователя, которые будут загружены программным обеспечением Cisco IOS и применены к данному клиенту.

Следующий пример демонстрирует авторизацию с использованием Radius:

Пример 1: Одинаковые методы авторизации сети для всех пользователей

Сервер доступа используется для приема удаленных соединений PPP.

Во-первых, пользователи проходят аутентификацию (как было настроено ранее) с помощью команды:

```
Router(config)# aaa authentication ppp default group radius local
```

затем они должны быть авторизованы с помощью команды:

```
Router(config)# aaa authorization network default group radius local
```

Примечание: На сервере AAA выполните следующую настройку:

- Service-Type=7 (framed)
- Framed-Protocol = PPP

Пример 2: Применение пользовательских атрибутов

Можно использовать сервер AAA для назначения атрибутов каждого пользователя, таких как IP-адрес, номер обратного вызова, значение времени ожидания простоя номеронабирателя или список доступа и т. д.. В этом случае сетевое устройство хранения данных будет загружать соответствующие атрибуты из профиля пользователя с сервера AAA.

Пример 3: Авторизация по протоколу PPP с использованием определенного списка

Подобно аутентификации, можно настроить имя списка, а не использовать список по умолчанию:

```
Router(config)# aaa authorization network ISDN_USER group radius local
```

Затем к интерфейсу применяется этот список:

```
Router(config)# int dialer 0
Router(config-if)# ppp authorization ISDN_USER
```

Дополнительные сведения об аутентификации AAA см. в документах Руководство по настройке безопасности IOS 12.2: Настройка аутентификации и Примеры практического применения Cisco AAA.

Настройка учета

Функция учета AAA позволяет отслеживать сервисы, к которым пользователи получают доступ, а также потребляемый объем сетевых ресурсов.

Правила учета AAA идентичны правилам аутентификации и авторизации:

1. Сначала следует определить именованный список методов учета.
2. Далее примените данный список к одному или нескольким интерфейсам (за исключением стандартного списка методов).
3. Используется первый метод в списке; в случае сбоя используется второй метод и т. д.

Используется первый метод в списке; в случае сбоя используется второй метод и т. д.

- Учет ресурсов сети служит для предоставления данных всем сеансам PPP, SLIP и ARAP (AppleTalk Remote Access Protocol): количество пакетов, количество октетов, время сеанса, время начала и окончания.
- Учет выполнения предоставляет данные о пользовательских сеансах терминала выполнения (например, о сеансе Telnet) для сервера доступа к сети: время сеанса, время начала и окончания.

Дополнительные сведения о других типах авторизации см. в документе Руководство по настройке безопасности Cisco IOS, выпуск 12.2.

Нижеприведенные примеры показывают, как можно отправлять данные на сервер AAA.

Примеры настройки учета

Пример 1: Создание записей учета начала и окончания сеанса

Для каждого удаленного сеанса PPP учетные данные передаются на сервер AAA после аутентификации клиента и после отключения с использованием ключевого слова start-stop.

```
Router(config)# aaa accounting network default start-stop group radius local
```

Пример 2: Создание только записей учета окончания сеанса

Если учетные данные нужно послать только после отключения клиента, используйте ключевое слово stop и введите следующую строку:

```
Router(config)# aaa accounting network default stop group radius local
```

Пример 3: Создание записей учета ресурсов для ошибок согласования и аутентификации

До этого момента учет AAA поддерживал записи начала и окончания сеанса для вызовов, прошедших пользовательскую аутентификацию.

В случае ошибок аутентификации или согласования PPP запись аутентификации отсутствует.

В качестве решения можно использовать учет окончания сеанса для ошибок ресурса AAA:

```
Router(config)# aaa accounting send stop-record authentication failure
```

На сервер AAA посылается запись об окончании сеанса.

Пример 4: Включение полного учета ресурсов

Для включения функции полного учета ресурсов, которая формирует запись начала сеанса при установлении вызова и запись окончания сеанса при завершении вызова, настройте следующие параметры:

```
Router(config)# aaa accounting resource start-stop
```

Эта команда была введена в программное обеспечение Cisco IOS версии 12.1(3)T.

С помощью этой команды запись учета начала и окончания сеанса при установлении и завершении вызова позволяет отслеживать подключение ресурсов к устройству. Отдельная запись учета начала и окончания сеанса при аутентификации пользователя отслеживает процесс управления пользователями. Эти два набора записей учета связаны посредством уникального идентификатора сеанса для вызова.

Дополнительные сведения об аутентификации AAA см. в документах Руководство по настройке безопасности IOS 12.2: Настройка аутентификации и Примеры практического применения Cisco AAA.

Дополнительные сведения

- Техническая поддержка - Cisco Systems