Маршрутизатор с ПО Cisco IOS: Локальный, TACACS + и Проверка подлинности RADIUS Примера конфигурации соединения HTTP

Содержание

Введение

В данном документе описана настройка локальной, TACACS+ и RADIUS аутентификации HTTP-соединения. Также приведены некоторые соответствующие команды отладки.

Перед началом работы

Условные обозначения

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

Предварительные условия

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Сведения в этом документе основаны на версиях оборудования и программного

обеспечения, указанных ниже.

- ПО Cisco IOS® версии 11.2 или более поздняя
- Оборудование, поддерживающее данные редакции ПО

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.

Теоретические сведения

В ПО Cisco IOS® версии 11.2 добавлена функция управления маршрутизатором через HTTP-подключение. Раздел "Команды веб-браузера Cisco IOS" в Основы настройки Cisco IOS: Справочник команд содержит следующую информацию об этой функции.

"Команда ip http authentication позволяет указывать конкретный метод аутентификации для пользователей HTTP-сервера. HTTP-сервер использует метод enable password для аутентификации пользователя на уровне разрешений 15. Теперь команда ip http authentication позволяет указывать enable, local, TACACS или аутентификацию, авторизацию и учет (AAA) для аутентификации пользователей HTTP-сервера."."

Настройка

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

В данном документе используются следующие конфигурации.

- Настройка локальной аутентификации для пользователей HTTP-сервера
- Настройка аутентификации TACACS+ для пользователей HTTP-сервера
- Настройка аутентификации RADIUS для пользователей HTTP-сервера

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

Настройка локальной аутентификации для пользователей HTTP-сервера

- Конфигурации маршрутизатора
- Результаты для пользователей

Конфигурации маршрутизатора

Локальная аутентификация с ПО Cisco IOS версии 11.2
`!--- This is the part of the configuration related to local authentication. ! aaa new-model aaa authentication login default local aaa authorization exec local username one privilege 15 password one username three password three username four privilege 7 password four ip http server ip http authentication aaa ! !--- Example`

```
of command moved from level 15 (enable) to level 7 !
privilege exec level 7 clear line
```

Локальная аутентификация с ПО Cisco IOS версии 11.3.3.T или более поздней

```
!--- This is the part of the configuration !--- related
to local authentication. ! aaa new-model aaa
authentication login default local aaa authorization
exec default local username one privilege 15 password
one username three password three username four
privilege 7 password four ip http server ip http
authentication local ! !--- Example of command moved
from level 15 (enable) to level 7 ! privilege exec level
7 clear line
```

Результаты для пользователей

Эти результаты для пользователей в предыдущих конфигурациях маршрутизатора.

- **Пользователь 1**Пользователь пройдет веб-авторизацию, если URL введен как http://#.#.#.#://#.#.#.#.После подключения по протоколу Telnet к маршрутизатору пользователь может выполнять все команды после аутентификации имени пользователя.**После выполнения входа пользователь окажется в режиме enable (результатом команды show privilege будет 15).**Если на маршрутизаторе добавлена авторизация команд, пользователь сможет выполнять все команды.
- **Пользователь 3**Пользователь не пройдет веб-авторизацию из-за отсутствия уровня разрешений.После подключения по протоколу Telnet к маршрутизатору пользователь может выполнять все команды после аутентификации имени пользователя.**После выполнения входа пользователь окажется в режиме non-enable (результатом команды show privilege будет 1).**Если на маршрутизаторе добавлена авторизация команд, пользователь сможет выполнять все команды.
- **Пользователь 4**Пользователь пройдет веб-авторизацию, если URL введен как http://#.#.#.#/level/7/exec.**Появятся команды уровня 1, а также команда уровня 7 clear line.**После подключения по протоколу Telnet к маршрутизатору пользователь может выполнять все команды после аутентификации имени пользователя.**После выполнения входа пользователь получит уровень разрешений 7 (результатом команды show privilege будет 7)**Если на маршрутизаторе добавлена авторизация команд, пользователь сможет выполнять все команды.

Настройка аутентификации TACACS+ для пользователей HTTP-сервера

Конфигурации маршрутизатора

Аутентификация с ПО Cisco IOS версии 11.2

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Аутентификация с ПО Cisco IOS версий 11.3.3.T-12.0.5.T

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec default tacacs
ip http server
ip http authentication aaa|tacacs
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Аутентификация с ПО Cisco IOS версии 12.0.5.T и более поздними

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Результаты для пользователей

Эти результаты для пользователей в конфигурациях сервера ниже.

- **Пользователь 1**Пользователь пройдет веб-авторизацию, если URL введен как http://#.#.#.#://#.#.#.#.После подключения по протоколу Telnet к маршрутизатору пользователь может выполнять все команды после аутентификации имени пользователя.**После выполнения входа пользователь окажется в режиме enable (результатом команды show privilege будет 15).**Если на маршрутизаторе добавлена авторизация команд, пользователь сможет выполнять все команды.
- **Пользователь 2**Пользователь пройдет веб-авторизацию, если URL введен как http://#.#.#.#://#.#.#.#.После подключения по протоколу Telnet к маршрутизатору пользователь может выполнять все команды после аутентификации имени пользователя.**После выполнения входа пользователь окажется в режиме enable (результатом команды show privilege будет 15).**Если на маршрутизаторе добавлена авторизация команд, пользователь не сможет выполнить ни одной команды, поскольку конфигурация сервера не авторизует их.
- **Пользователь 3**Пользователь не пройдет веб-авторизацию из-за отсутствия уровня разрешений.После подключения по протоколу Telnet к маршрутизатору пользователь может выполнять все команды после аутентификации имени пользователя.**После выполнения входа пользователь окажется в режиме non-enable (результатом команды show privilege будет 1).**Если на маршрутизаторе добавлена авторизация команд,

пользователь сможет выполнять все команды.

- **Пользователь 4**Пользователь пройдет веб-авторизацию, если URL введен как http://#.#.#.#/level/7/exec.**Появятся команды уровня 1, а также команда уровня 7 clear line.**После подключения по протоколу Telnet к маршрутизатору пользователь может выполнять все команды после аутентификации имени пользователя.**После выполнения входа пользователь получит уровень разрешений 7 (результатом команды show privilege будет 7)**Если на маршрутизаторе добавлена авторизация команд, пользователь сможет выполнять все команды.

Настройка сервера Freeware Daemon Server

```
user = one {
default service = permit
login = cleartext "one"
service = exec {
priv-lvl = 15
}
}

user = two {
login = cleartext "two"
service = exec {
priv-lvl = 15
}
}

user = three {
default service = permit
login = cleartext "three"
}

user = four {
default service = permit
login = cleartext "four"
service = exec {
priv-lvl = 7
}
}
```

Cisco Secure ACS для настройки сервера UNIX

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 27
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=15
}
}
# ./ViewProfile -p 9900 -u two
User Profile Information
user = two{
profile_id = 28
profile_cycle = 1
password = clear "********"
service=shell {
set priv-lvl=15
```

```
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 29
profile_cycle = 1
password = clear "********"
default service=permit
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 30
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=7
}
}
```

[Cisco Secure ACS для настройки сервера Windows]

Пользователь 1 в группе 1

- Параметры группы**Установите флажок shell (exec).Установите флажок privilege level=15.Установите флажок Default (Undefined) Services (Стандартные (неопределенные) службы).Примечание: Если этого параметра нет в окне, откройте страницу Interface Configuration (Конфигурация интерфейса), выберите TACACS+ и затем Advanced Configuration Options (Дополнительные параметры конфигурации). Установите флажок Display enable default (undefined) service (Показывать стандартные (неопределенные) сервисы enable).**
- Параметры пользователяПароль из любой базы данных; введите пароль и подтвердите его в верхней области.

Пользователь 2 в группе 2

- Параметры группы**Установите флажок shell (exec).Установите флажок privilege level=15.Не устанавливайте флажок Default (Undefined) Services (Стандартные (неопределенные) службы).**
- Параметры пользователяПароль из любой базы данных; введите пароль и подтвердите его в верхней области.

Пользователь 3 в группе 3

- Параметры группы**Установите флажок shell (exec).Оставьте уровень разрешений privilege level незаполненным.Установите флажок Default (Undefined) Services (Стандартные (неопределенные) службы).Примечание: Если этого параметра нет в окне, откройте страницу Interface Configuration (Конфигурация интерфейса), выберите TACACS+ и затем Advanced Configuration Options (Дополнительные параметры конфигурации). Установите флажок Display enable default (undefined) service (Показывать стандартные (неопределенные) сервисы enable).**
- Параметры пользователяПароль из любой базы данных; введите пароль и подтвердите его в верхней области.

Пользователь 4 в группе 4

- Параметры группыУстановите флажок shell (exec).Установите флажок privilege level=7.Установите флажок Default (Undefined) Services (Стандартные (неопределенные) службы).Примечание: Если этого параметра нет в окне, откройте страницу Interface Configuration (Конфигурация интерфейса), выберите TACACS+ и затем Advanced Configuration Options (Дополнительные параметры конфигурации). Установите флажок Display enable default (undefined) service (Показывать стандартные (неопределенные) сервисы enable).
- Параметры пользователяПароль из любой базы данных; введите пароль и подтвердите его в верхней области.

Настройка аутентификации RADIUS для пользователей HTTP-сервера

Конфигурации маршрутизатора

Аутентификация с ПО Cisco IOS версии 11.2

```
aaa new-model
aaa authentication login default radius
aaa authorization exec radius
ip http server
ip http authentication aaa
!
!--- Example of command moved from level 15 (enable) to
level 7 ! privilege exec level 7 clear line radius-
server host 171.68.118.101 radius-server key cisco
```

Аутентификация с ПО Cisco IOS версий 11.3.3.T-12.0.5.T

```
aaa new-model
aaa authentication login default radius
aaa authorization exec default radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

Аутентификация с ПО Cisco IOS версии 12.0.5.T и более поздними

```
aaa new-model
aaa authentication login default group radius
aaa authorization exec default group radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

Результаты для пользователей

Эти результаты для пользователей в конфигурациях сервера ниже.

- **Пользователь 1**Пользователь пройдет веб-авторизацию, если URL введен как http://#.#.#.#://#.#.#.#.После подключения по протоколу Telnet к маршрутизатору пользователь может выполнять все команды после аутентификации имени пользователя.**После выполнения входа пользователь окажется в режиме enable (результатом команды show privilege будет 15).**
- **Пользователь 3**Пользователь не пройдет веб-авторизацию из-за отсутствия уровня разрешений.После подключения по протоколу Telnet к маршрутизатору пользователь может выполнять все команды после аутентификации имени пользователя.**После выполнения входа пользователь окажется в режиме non-enable (результатом команды show privilege будет 1).**
- **Пользователь 4**Пользователь пройдет веб-авторизацию, если URL введен как http://#.#.#.#/level/7/exec.**Появятся команды уровня 1, а также команда уровня 7 clear line.**После подключения по протоколу Telnet к маршрутизатору пользователь может выполнять все команды после аутентификации имени пользователя.**После выполнения входа пользователь получит уровень разрешений 7 (результатом команды show privilege будет 7)**

Конфигурация RADIUS на сервере, поддерживающем Cisco AV-Pairs

```
one Password= "one"
Service-Type = Shell-User
cisco-avpair = "shell:priv-lvl=15"

three Password = "three"
Service-Type = Login-User

four Password= "four"
Service-Type = Login-User
cisco-avpair = "shell:priv-lvl=7"
```

Cisco Secure ACS для настройки сервера UNIX

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 31
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="one"
}
reply_attributes= {
6=6
}
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 32
set server current-failed-logins = 0
```

```
profile_cycle = 3
radius=Cisco {
check_items= {
2="three"
}
reply_attributes= {
6=1
}
}
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 33
profile_cycle = 1
radius=Cisco {
check_items= {
2="four"
}
reply_attributes= {
6=1
9,1="shell:priv-lvl=7"
}
}
}
```

Cisco Secure ACS для настройки сервера Windows

- User = one, service type (атрибут 6) = administrative
- User = three, service type (атрибут 6) = login
- User = four, service type (атрибут 6) = login, проверьте поле Cisco AV-pairs и введите shell:priv-lvl=7

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Ниже указаны команды, используемые для отладки HTTP-аутентификации. Они выполняются на маршрутизаторе.

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

- **terminal monitor — отображаются результаты выполнения команды debug и системные сообщения об ошибках для текущего терминала и сеанса.**
- **debug aaa authentication — отображаются сведения при аутентификации AAA/TACACS+.**
- **debug aaa authorization — отображаются данные авторизации AAA/TACACS+.**
- **debug radius — отображаются подробные отладочные данные, связанные с RADIUS.**

- **debug tacacs — отображаются сведения, связанные с TACACS+.**
- **debug ip http authentication — используется для устранения неполадок с HTTP-аутентификацией.** Отображается метод аутентификации, применяемый маршрутизатором, и сообщения о состоянии, связанные с аутентификацией.

Дополнительные сведения

- Страница поддержки ПО доступа Cisco TACACS+
- Страница поддержки RADIUS
- Страница поддержки Cisco Secure ACS для Windows
- Страница поддержки Cisco Secure ACS для UNIX
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация