# Настройка взаимодействия с RADIUS-сервером для аутентификации при подключении пользователя через SSH

Настоящий документ содержит описание способа совместного использования Продуктов компании ООО «С-Терра СиЭсПи» и Продуктов третьих производителей.
ООО «С-Терра СиЭсПи» осуществляет сопровождение настоящего сценария в части настроек Продуктов Компании. Упоминание наименований, продуктов, торговых марок третьих организаций исключительно неформально и не является поддержкой, рекомендацией, либо рекламой. ООО «С-Терра СиЭсПи» не несет какой-либо ответственности в отношении работоспособности и использования этих Продуктов.
Документ имеет статус вспомогательного материала, который может быть использован технологическими партнерами, компаниями-интеграторами, при разработке собственных решений.
Решения, разработанные на базе данного сценария, могут применяться в действующих сетях/системах только после тестовой и/или опытной эксплуатации.

## Введение

Данный документ описывает настройку взаимодействия с RADIUS-сервером для аутентификации при подключении пользователя через SSH.

## Схема взаимодействия




*Рисунок 1. Схема взаимодействия*

# Общая логика работы

## Основной сценарий (с созданием пользователей на криптошлюзе)

Для работы аутентификации с использованием RADIUS-сервера в «С-Терра Шлюз» («криптошлюз» в дальнейшем) должны быть созданы все пользователи RADIUS-сервера, от которых будет вестись работа.

Пользователи `root` и `cscons` также должны быть указаны в настройках RADIUS-сервера, если с их правами планируется удаленное подключение. Если они отсутствуют на RADIUS-сервере, который в свою очередь в момент аутентификации доступен, удаленное подключение данными пользователями будет невозможно. Следует либо добавить соответствующие настройки на RADIUS-сервере, либо подключаться пользователями только локально.

При попытке подключения к криптошлюзу по протоколу SSH будет отправлен запрос на RADIUS-сервер и, в зависимости от ответа, аутентификация пользователя завершится успехом или неудачей. При недоступности RADIUS-сервера будет произведена попытка аутентификации с локальным паролем.

При локальном подключении к криптошлюзу, аутентификация с помощью RADIUS производиться не будет.

Для аутентификации используются модули PAM (pluggable authentication module). На криптошлюзе за локальную аутентификацию отвечает модуль `pam_unix`, а за аутентификацию через RADIUS-сервер отвечает модуль `pam_radius_auth`.

## Дополнительный сценарий (без создания пользователей на криптошлюзе)

При использовании ПО `libnss-ato` можно обойтись одним пользователем и не создавать на криптошлюзе множество пользователей, настроенных на RADIUS-сервере. После конфигурации `libnss-ato` любой пользователь, прошедший аутентификацию на RADIUS, будет сопоставлен с этим пользователем. В логах будет отображено имя пользователя RADIUS, но логин будет произведен с UID (и соответственно с правами) пользователя, указанного в настройках `libnss-ato` (см. Пример работы из Настройка стенда (дополнительный сценарий)). Конфигурация для такого случая представлена в отдельной главе (Настройка криптошлюза GW1).

Для аутентификации в таком сценарии используются модули PAM таким же образом, как и в основном сценарии.

# Настройка стенда (основной сценарий)

## Настройка криптошлюза GW1

1. Предполагается, что инициализация криптошлюза пройдена, задано имя хоста, заданы корректные сетевые настройки и RADIUS-сервер доступен по сети.
2. Настройте доступ к RADIUS-серверу. Для этого измените файл `/etc/pam_radius_auth.conf`. В данном файле необходимо указать адрес и порт RADIUS-сервера (в данном случае – `192.168.1.5:1812`), пароль для доступа к нему (в данном случае – `secret1`) и таймаут в секундах (`3`). **Остальные строки закомментируйте или удалите**.

   ```
   192.168.1.5:1812 secret1 3
   ```

3. Измените настройки аутентификации для SSH. Для этого в файле `/etc/pam.d/sshd` пропишите использование модуля `pam_radius_auth.so` в самой верхней строке сразу после первого комментария. **Остальные строки трогать не следует**.

   ```
   # PAM configuration for the Secure Shell service
   auth     [success=done     authinfo_unavail=ignore     ignore=ignore     default=bad]
   pam_radius_auth.so
   ...
   ```

   Действий, описанных выше, достаточно для успешной аутентификации с помощью RADIUS-сервера для пользователей, уже существующих на криптошлюзе (при условии наличия записей для них на RADIUS-сервере). Создать пользователя на криптошлюзе можно в cisco-like консоли используя следующие команды:

   ```
   GW1(config)#username testing secret 0 password
   GW1(config)#username testing privilege 15
   ```

   Где:

   - `username testing` – команда для добавления пользователя с именем `testing`;
   - `secret 0 password` – у создаваемого пользователя будет локальный пароль `password`, который будет храниться в зашифрованном виде;
   - `privilege 15` – у создаваемого пользователя будет сразу доступ к привилегированному режиму.

   Заданные настройки будут использоваться со следующей попытки подключения к криптошлюзу по SSH. Сервис `sshd` перезапускать нет необходимости.

# Проверка работоспособности

1. Проведите попытку подключения по SSH к криптошлюзу с пользователем `testing` консоли cisco-like (RADIUS пользователь `testing`) с устройства IPHost1:

```
root@IPHost1:~# ssh testing@192.168.1.1
```

```
testing@192.168.1.1's password:
S-Terra Gate 5.0.XXXXX (amd64)
GW1#
```

   При этом в системных логах будут следующие записи:

```
root@GW1:~# cat /var/log/auth.log
```

```
2025-11-19T13:44:08.406836+03:00 GW1 sshd[5690]: Accepted password for testing from
192.168.1.100 port 48664 ssh2
2025-11-19T13:44:08.412773+03:00 GW1 sshd[5690]: pam_unix(sshd:session): session
opened for user testing(uid=1002) by (uid=0)
2025-11-19T13:44:08.453978+03:00 GW1 sshd[5690]: pam_env(sshd:session): deprecated
reading of user environment enabled
```

```
root@GW1:~# cat /var/log/cspvpngate.log
```

```
2025-11-19T13:44:08.556522+03:00 GW1 -cs_console: 0072500b Command interpreter started
2025-11-19T13:44:08.613366+03:00 GW1 -cs_console: 00725001 Cisco-like console started
by user "testing"
```

2. Проведите попытку подключения по SSH к криптошлюзу с пользователем `root` консоли linux bash (RADIUS пользователь `root`) с устройства IPHost1:

```
root@IPHost1:~# ssh root@192.168.1.1
```

```
root@192.168.1.1's password:
S-Terra Gate 5.0.XXXXX (amd64)
root@GW1:~#
```

   При этом в системных логах будут следующие записи:

```
root@GW1:~# cat /var/log/auth.log
```

```
2025-11-19T13:45:45.956100+03:00 GW1 sshd[5742]: Accepted password for root from
192.168.1.100 port 57414 ssh2
2025-11-19T13:45:45.960153+03:00 GW1 sshd[5742]: pam_unix(sshd:session): session
opened for user root(uid=0) by (uid=0)
2025-11-19T13:45:46.002525+03:00 GW1 sshd[5742]: pam_env(sshd:session): deprecated
reading of user environment enabled
```

3. Искусственно нарушите доступность RADIUS-сервера (к примеру, при помощи записи firewall на GW1), затем проведите попытку подключения по SSH к криптошлюзу с пользователем `root` консоли linux bash с устройства IPHost1:

```
root@IPHost1:~# ssh root@192.168.1.1
```

```
root@192.168.1.1's password:
S-Terra Gate 5.0.XXXXX (amd64)
root@GW1:~#
```

   При этом в системных логах будут следующие записи:

```
root@GW1:~# cat /var/log/auth.log
```

```
2025-11-19T13:47:59.511891+03:00 GW1 sshd[5770]: pam_radius_auth: RADIUS server
192.168.1.5:1812 failed to respond
2025-11-19T13:47:59.512504+03:00 GW1 sshd[5770]: pam_radius_auth: All RADIUS servers
failed to respond.
2025-11-19T13:48:01.174533+03:00 GW1 sshd[5770]: Accepted password for root from
192.168.1.100 port 36486 ssh2
2025-11-19T13:48:01.181203+03:00 GW1 sshd[5770]: pam_unix(sshd:session): session
opened for user root(uid=0) by (uid=0)
```

```
2025-11-19T13:48:01.222016+03:00 GW1 sshd[5770]: pam_env(sshd:session): deprecated
reading of user environment enabled
```

# Настройка стенда (дополнительный сценарий)

## Настройка криптошлюза GW1

До настроек, указанных ниже должны быть проведены все настройки из основного сценария из главы Настройка криптошлюза GW1.

Приведенные ниже настройки наложат определенные ограничения на систему.
Создать нового пользователя (как в системе, так и в консоли cisco-like) можно будет только после временного отката настроек `nsswitch` к прежнему состоянию (не требует перезагрузки ни сервиса, ни системы, настройки применяются сразу). В частности, из-за этого могут быть проблемы при установке различных пакетов.
Приведенные ниже настройки не являются рекомендуемыми, а лишь предлагаются как решение, альтернативное основному (описанному выше) сценарию.

1. Создайте файл `/etc/libnss-ato.conf` и поместите туда строчку с нужным пользователем (в данного пользователя будут маппироваться все остальные) из `/etc/passwd`.

   Пример:

   Для настройки используется ранее созданный при помощи консоли cisco-like (как в пункте 3 главы Настройка криптошлюза GW1) пользователь `testing`.

   ```
   root@GW1:~# cat /etc/passwd | grep testing > /etc/libnss-ato.conf
   root@GW1:~# cat /etc/libnss-ato.conf
   testing:x:1001:4::/var/cspvpn/users//testing:/opt/VPNagent/bin/cs_console
   ```

2. В файле `/etc/nsswitch.conf` добавьте к строкам `passwd:` и `shadow:` модуль с названием `ato` (перед модификацией следует создать резервную копию файла на случай необходимости временного отката):

   ```
   passwd:         files ato
   group:          files
   shadow:         files ato
   ```

## Проверка работоспособности

Проведите попытку подключения по SSH к криптошлюзу с пользователем `newuser` с устройства IPHost1. Пользователь `newuser` настроен только на RADIUS-сервере:

```
root@IPHost1:~# ssh newuser@192.168.1.1
newuser@192.168.1.1's password:
S-Terra Gate 5.0.XXXXX (amd64)
GW1#
```

При этом в системных логах будут следующие записи:

```
root@GW1:~# cat /var/log/auth.log
2025-11-19T15:06:37.337988+03:00 GW1 sshd[5911]: Accepted password for newuser from 192.168.1.100 port 33770 ssh2
2025-11-19T15:06:37.340909+03:00 GW1 sshd[5911]: pam_unix(sshd:session): session opened for user newuser(uid=1002) by (uid=0)
2025-11-19T15:06:37.391026+03:00 GW1 sshd[5911]: pam_env(sshd:session): deprecated reading of user environment enabled
```

Следует обратить внимание на UID. Он совпадает с UID пользователя `testing`, использующегося в конфигурации `libnss-ato`.

# Приложение

## Пример конфигурации RADIUS-сервера для Debian 12

Для тестирования можно создать RADIUS-сервер (пример для Debian 12).

1. Скачайте информацию по пакетам, обновите систему и установите пакет `freeradius` (опция `-y` автоматически отвечает положительно на все вопросы `apt`):

```
root@Radius1:~# apt -y update && apt -y upgrade && apt -y install freeradius
```

2. Добавьте в начало файла `/etc/freeradius/3.0/mods-config/files/authorize` следующие строки (в строках указаны имена пользователей и их пароли):

```
testing Cleartext-Password := "password"
root Cleartext-Password := "password"
```

Где:

- `testing` – имя пользователя;
- `password` – пароль.

3. Добавьте в конец файла `/etc/freeradius/3.0/clients.conf` следующие строки (адрес RADIUS-клиента (GW1) и пароль доступа, выделенные в секцию `client` под названием `test`):

```
client test {
        ipaddr = 192.168.1.1
        secret = secret1
}
```

Где:

- `test` – имя настройки (можно задать любое);
- `ipaddr` – адрес клиента (в данном случае адрес GW1);
- `secret` – пароль доступа (должен совпадать с заданным в пункте 2 раздела «Настройка криптошлюза GW1»)

4. Перезапустите сервис `freeradius` и поставьте его на автозагрузку:

```
root@Radius1:~# systemctl restart freeradius.service
root@Radius1:~# systemctl enable freeradius.service
```

## Отладка RADIUS-сервера

1. Остановите сервис `freeradius`:

```
root@Radius1:~# systemctl stop freeradius.service
```

2. Выполните команду для получения отладочной информации:

```
root@Radius1:~# freeradius -X
```