# Практическая работа «Удаленный доступ: SSH»

**Цель:** Настройка протокола SSH для обеспечения защищенного удаленного доступа с использованием парольного доступа и доступа по ключу.

**Описание:** В приведенных примерах будет использоваться топология, представленная на рис. SSH\_01

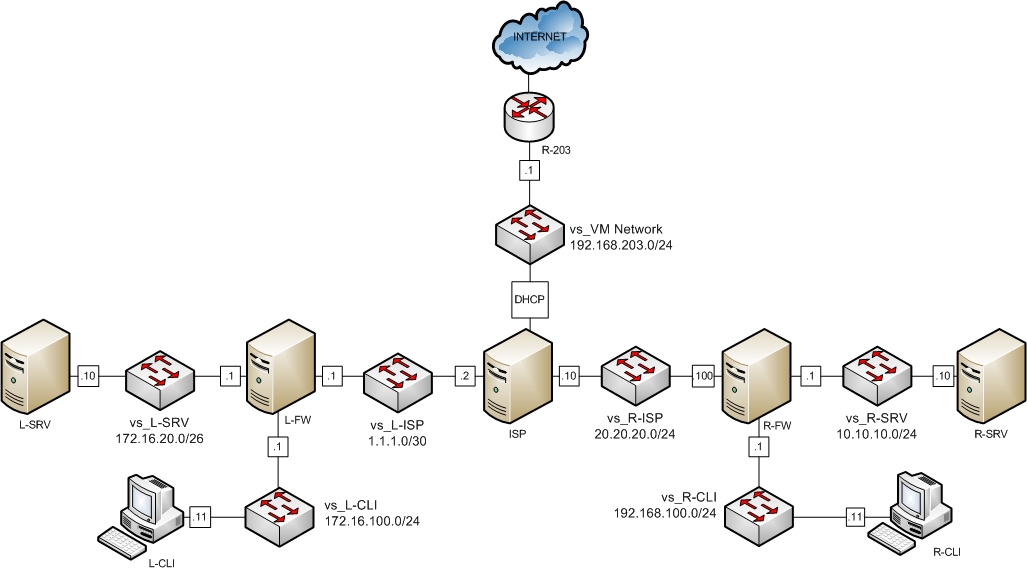


Рисунок SSH\_01 Топология сети

**Краткие теоретические сведения:**

(информация, приведенная ниже на этой странице, взята с источника <https://losst.ru/avtorizatsiya-po-klyuchu-ssh>)

SSH или Secure Shell - это зашифрованный протокол, который часто используется для взаимодействия и удаленного управления серверами. Если необходимо что-либо сделать на удаленном сервере, скорее всего, придется воспользоваться SSH и работать через терминал. SSH существует несколько способов авторизации. Можно каждый раз вводить пароль пользователя или использовать более безопасный и надежный способ - ключи SSH. Что самое интересное, он более удобен для применения, поскольку даже не нужно будет вводить пароль.

Пароли передаются по безопасному каналу, но они недостаточно сложны для противостояния попыткам перебора. Вычислительная мощность современных систем в сочетании со специальными скриптами делают перебор очень простым. Конечно, существуют другие способы дополнительной безопасности, например, fail2ban, но аутентификация по ключу SSH более надежна.

Каждая пара ключей состоит из открытого и закрытого ключа. Секретный ключ сохраняется на стороне клиента и не должен быть доступен кому-либо еще. Утечка ключа позволит злоумышленнику войти на сервер, если не была настроена дополнительная аутентификация по паролю.

Открытый ключ используется для шифрования сообщений, которые можно расшифровать только закрытым ключом. Это свойство и используется для аутентификации с помощью пары ключей. Открытый ключ загружается на удаленный сервер, к которому необходимо получить доступ. Его нужно добавить в специальный файл **~/.ssh/authorized\_keys**.

Когда клиент попытается выполнить проверку подлинности через этот ключ, сервер отправит сообщение, зашифрованное с помощью открытого ключа, если клиент сможет его расшифровать и вернуть правильный ответ - аутентификация пройдена (Рис. SSH\_02).

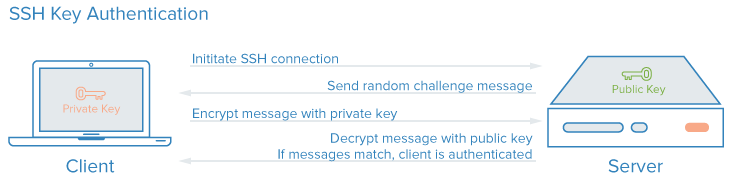


Рисунок SSH\_02 Аутентификация SSH

Пример SSH\_01:

В приведенной топологии (рис. SSH\_01) настроить на компьютерах **L-SRV** и **ISP** удаленный доступ по протоколу SSH по следующим критериям (Таблица SSH\_01):

**Таблица SSH\_01** Параметры подключения SSH

|  |  |  |  |
| --- | --- | --- | --- |
| **Устройство** | **Пользователи** | **Порт** | **Доступ** |
| L-SRV | ssh\_c  ssh\_p | 1022 | Пароль  Ключ |
| ISP | ssh\_isp | 22 | Ключ |

В качестве пароля использовать **ssh\_pass**

Проверку подключения осуществлять с компьютера **L-FW**

Настройка:

1. Настроить имена устройств и IP адресацию в соответствии с топологией.
2. Заполнить файл /etc/hosts, [доменными имен](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BC%D0%B5%D0%BD%D0%BD%D0%BE%D0%B5_%D0%B8%D0%BC%D1%8F)ами устройств и соответствующими им IP адресами

|  |  |
| --- | --- |
| **L-SRV (Debian):** | **ISP (Centos):** |
| nano /etc/hosts  172.16.20.10 L-SRV  172.16.20.1 L-FW  1.1.1.2 ISP | vi /etc/hosts  172.16.20.10 L-SRV  172.16.20.1 L-FW  1.1.1.2 ISP |

1. Создать на всех устройствах пользователей, указанных в таблице SSH\_01.

|  |  |
| --- | --- |
| **L-SRV (Debian):** | **ISP (Centos):** |
| useradd –m –s /bin/bash ssh\_c  passwd ssh\_c  ssh\_pass  ssh\_pass | useradd ssh\_isp  passwd ssh\_isp  ssh\_pass  ssh\_pass |

На устройстве L-FW создаем пользователей, для которых будет обеспечиваться доступ ***по ключам*** (**ssh\_c** и **ssh\_isp**).

1. На устройствах **L-SRV, ISP** включить доступ по SSH и установить необходимый порт:

|  |  |
| --- | --- |
| **L-SRV (Debian):** | **ISP (Centos):** |
| nano /etc/ssh/sshd\_config | vi /etc/ssh/sshd\_config |
| Port 1022 | Port 22 |

1. Перезапустить ssh на обоих устройствах:

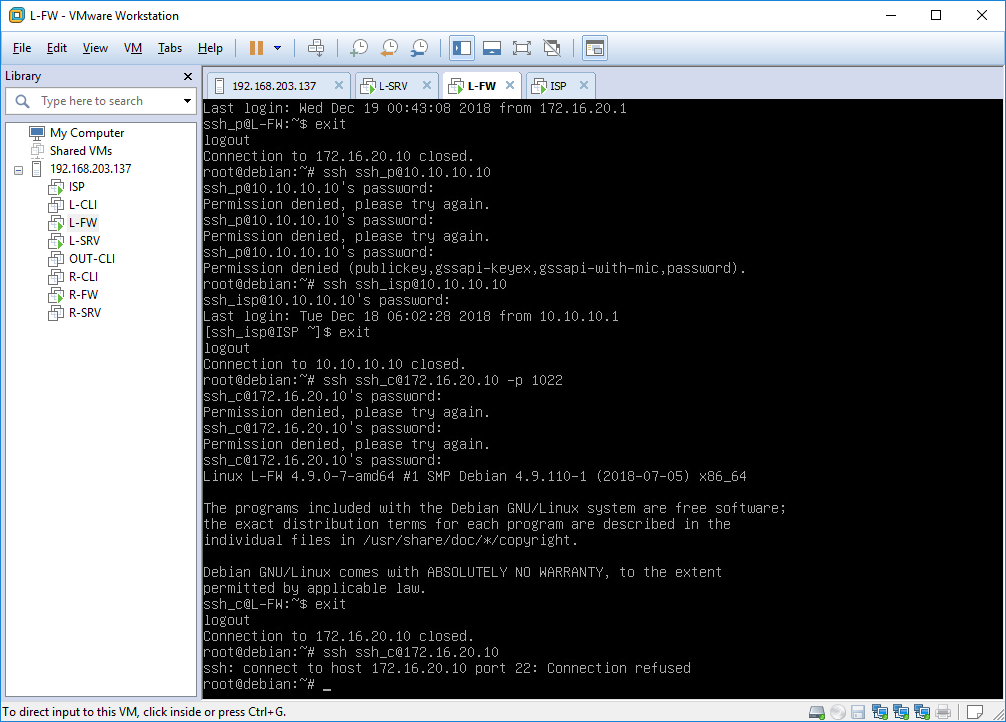
systemctl restart sshd

1. Проверить доступ по паролям к устройствам L-SRV, ISP с хоста L-FW:

**L-FW -> L-SRV**

ssh ssh\_c@172.16.20.10

Выводится ошибка:

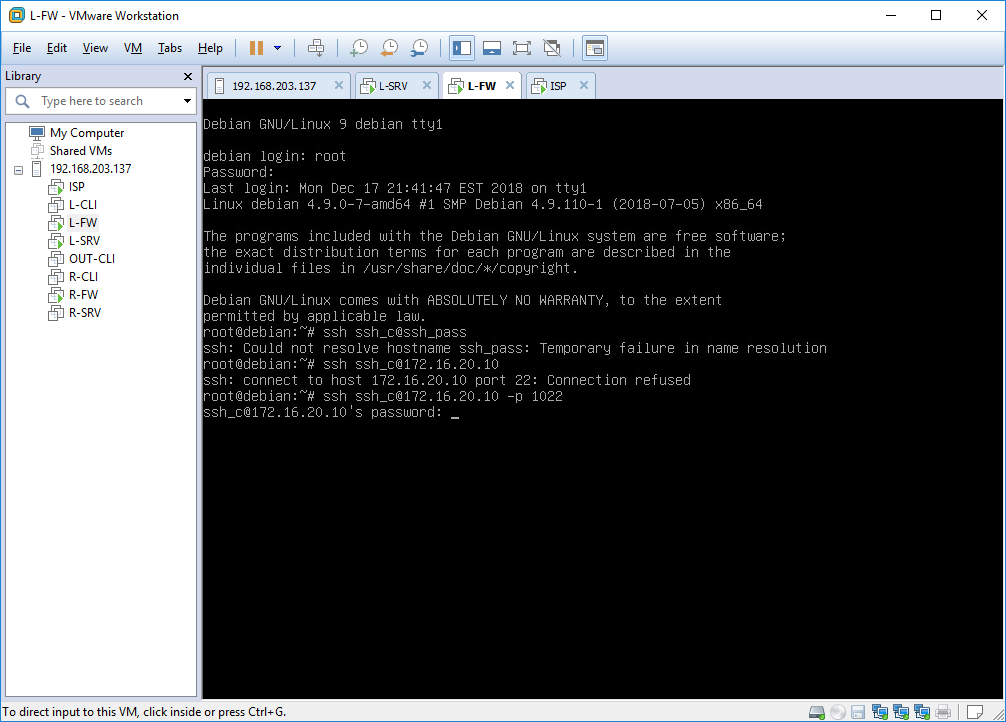


Связано это с тем, что по-умолчанию подключение осуществляется на порт 22. А в конфигурационном файле на L-SRV был установлен порт 1022.

Выполнить подключение **на порт 1022** и ввести пароль **ssh\_pass**

При первом подключении необходимо ввести **yes** на запрос демона sshd

ssh ssh\_c@172.16.20.10 –p 1022



В случае удачного подключения в терминале будет выведено имя пользователя и имя хоста:

ssh\_c@L-FW:~$

1. Для выхода ввести **exit**
2. Аналогично проверить возможность удаленного подключения под оставшимися пользователями к соответствующим устройствам.

### Настройка подключения по ключу

Генерацию ключей будет проводиться на устройстве, с которого будет осуществляться подключение к удаленным компьютерам, т.е. L-FW, а затем открытые пароли будут переданы на сервера.

1. Зайти на L-FW под именем пользователя **ssh\_p**
2. Сгенерировать ключ

ssh-keygen -t rsa -b 1024

1. Создается два файла **id\_rsa** и **id\_rsa.pub**. PUB ключ - это публичный, а **id\_rsa** секретный. Необходимо файл **id\_rsa.pub** перенести на сервер, куда будет осуществляться подключение. В данном случае – на **L-SRV** в директорию **/home/ssh\_p/.ssh/** (в каталог того пользователя под которым будет соединение по ssh).
2. Перенести ключ на удаленный сервер. Для этого можно воспользоваться командой:

ssh-copy-id ssh\_p@172.16.20.10 или ssh-copy-id ssh\_p@L-SRV

Ввести пароль

При этом на удаленном сервере (L-SRV) в каталоге **~/.ssh** создается файл **autorized\_keys,** в который прописывается **открытый** ключ.

1. Проверить подключение к **L-SRV** с использованием *ключа*:

Перейти на **L-FW** и ввести команду:

ssh ssh\_p@L-SRV –p 1022

Если все сделано правильно, то должно произойти подключение без запроса пароля:

ssh\_p@L-SRV:~$

1. Для создания подключения по ключу на удаленный сервер ISP необходимо выполнить шаги 8)-12) для пользователя **ssh\_isp**.
2. После создания и проверки подключений можно (и нужно) удалить файлы открытых ключей **id\_rsa.pub** из каталога **~/.ssh** каждого пользователя на компьютере **L-FW**.

Таким образом, настроены подключения к удаленным серверам по протоколу ssh,причем для пользователей **ssh\_p** и **ssh\_isp** аутентификация происходит по ключам, а пользователь **ssh\_c** должен вводить пароль.

Пример SSH\_02:

В настроенную в предыдущем примере (ssh\_01) схему подключения по протоколу ssh внести изменения, обеспечив подключение по нужным портам (таблица SSH\_01) без необходимости их указания каждый раз в процессе аутентификации

Настройка:

1. Для выполнения данной настройки необходимо внести изменения в конфигурационный файл **/etc/ssh/ssh\_config**, в котором содержатся настройки пользовательские настройки ssh на хосте с которого будет осуществляться подключение (L-FW). Порты для подключения предварительно должны быть настроены на удаленных серверах (см. п.3) пример SSH\_01)

nano /etc/ssh/ssh\_config

1. Добавить в конец файла следующие команды:

Host L-SRV

Port 1022

Host ISP

Port 22

1. Перезагрузить sshd

systemctl restart sshd

1. Проверить подключение к **L-SRV** без указания номера порта:

ssh ssh\_p@L-SRV

1. Проверить подключение к **ISP** без указания номера порта:

ssh ssh\_isp@ISP

**Примечание:** Порт **22** для ssh является стандартным портом подключения, поэтому для него настройки можно не делать.

Пример SSH\_03:

Выполнить настройку L-FW, которая будет обеспечивать подлючение по протоколу ssh к компьютеру L-SRV **по-умолчанию** под именем пользователя **ssh\_p**, а к ISP - под **ssh\_isp**.

Настройка:

L-FW:

1. Отредактировать файл **ssh\_config**:

nano /etc/ssh/ssh\_config

Host L-SRV

Port 1022

*User ssh\_p*

Host ISP

Port 22

*User ssh\_isp*

1. Перезагрузить sshd

systemctl restart sshd

1. Проверить подключение к **L-SRV** без указания имени пользователя:

ssh L-SRV

1. Проверить подключение к **ISP** без указания имени пользователя:

ssh ISP

Пример SSH\_04:

Вывести для пользователей, подключающихся к **L-SRV** по протоколу **ssh** баннер следующего содержания: **Are you sure? Be careful**. Не выводить данный баннер для пользователя **ssh\_c**

Настройка:

1. Зайти на устройство L-SRV по логином root
2. Создать нового пользователя **empl** с паролем **cisco**
3. Создать файл следующего содержания

nano /etc/ssh/ssh\_banner

Are you sure? Be careful

1. Отредактировать конфигурационный файл sshd\_config

nano /etc/ssh/ssh\_config

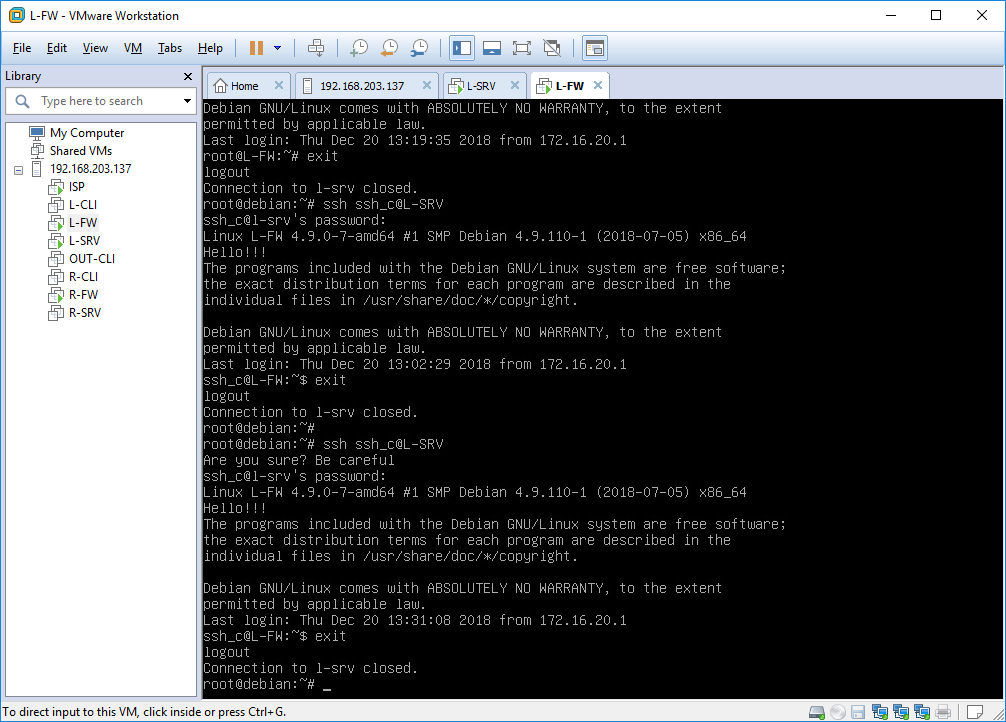
Banner /etc/ssh/ssh\_banner

1. Перезагрузить sshd

systemctl restart sshd

1. Подключиться к L-SRV с устройства L-FW под именем ssh\_c

ssh ssh\_c@L-SRV



Нажать CTRL+Z для отмены подключения

1. Подключиться под именем **empl**

Баннер выводится для обоих пользователей

Отключения баннера для ssh\_c

Для выполнения данной настройки необходимо воспользоваться диреrтивой **Match** в файле **sshd\_config**.

Директива **Match** представляет собой начало условного блока. Если выполнены все критерии, указанные в строке Match, директивы в последующих строках блока выполняются, позволяя обойти значения глобальных директив файла **sshd\_config** для случая, являющегося критерием директивы Match. Блоком считаются все строки, идущие после строки с критерием (Match - строки) до следующей match-строки или до конца файла. Аргумент директивы Match - одна или несколько пар записей критериев.

1. Зайти на устройство L-SRV по логином root
2. Открыть для редактирования конфигурационный файл sshd\_config

nano /etc/ssh/ssh\_config

1. В конце файла ввести строки

Match User ssh\_c

Banner no

1. Перезагрузить **sshd**

systemctl restart sshd

1. Подключиться к **L-SRV** с устройства **L-FW** сначала под именем **ssh\_c** а затем под именем **empl**

Баннер выводится для пользователя **empl**

Задание для самостоятельного выполнения:

Отключить на **L-SRV** парольную аутентификацию ssh, оставив только вход по ключу. По паролю на **L-SRV** может заходить только пользователь **empl**

Для решения данной задачи и задач, возникающих в дальнейшем можно (и нужно!!!) использовать источники информации:

1. **man**
2. Источники в интернете:

<http://www.opennet.ru/base/sec/ssh_tips.txt.html>

<https://www.help.ubuntu.ru/wiki/ssh>

и многие другие…