SSH-туннель

Устройства Инфинет допускают создание до 16 независимых туннелей L2 через соединения SSH. Интерфейс tap может иметь IP-адрес и использоваться как самостоятельный сетевой интерфейс, например, для машрутизации, а также в составе группы коммутации. Кроме того, интерфейс tap может быть использован в качестве родительского для интерфейсов vlan, lag и prf, в том числе для использования в составе сети MINT.

SSH-туннель между двумя устройствами Инфинет

На первом устройстве, выполняющем функцию сервера, создадим интерфейс "*tap0*" и назначим ему IP-адрес "*192.168.1.1/24*". Устанавливаем логин "*ssh_tun*" и пароль "*$ecRet*" для созданного интерфейса. Настроим размер внутреннего окна приема сервера SSH, для достижения максимальной производительности, параметр "*-window*" на обоих сторонах туннеля следует устанавливать в значения не менее 128000. Период продолжительности проверки активности сеанса установим равным 30 секундам. Активируем SSH демон.

Устройство 1 (сервер)

```
ifc tap0 192.168.1.1/24 up
sshd tunnel add ssh_tun $ecRet tap0
sshd -window=128000 -keepalive=30
sshd start
```

На втором устройстве так же создадим интерфейс "*tap0*" и назначим ему IP-адрес "*192.168.1.2/24*". Настроим параметры внутреннего окна, продолжительности проверки и значение интерфейса на сервере, если на сервере настроен интерфейс "*tap0*", нужно указывать "*-remote-if=0*". Логин и пароль должны совпадать с указанными на удалённой стороне. Опционально указываем алгоритм шифрования, алгоритм обмена ключами и другие параметры туннеля. Получить список поддерживаемых алгоритмов можно командой: "*sshtun tap0 -algo-list*", где "*kex*" - алгоритмов SSH для обмена ключами, "*hostkey*" - аутентификации, "*cipher*" - кодирования данных, "*hash*" - проверки данных и "*compress*" - сжатия данных. Активируем SSH-демон. Для того чтобы запустить SSH туннель, необходимо обязательно ввести команду "*sshtun start*".

Устройство 2 (клиент)

```
ifc tap0  192.168.1.2/24 up
sshtun tap0 -window=128000 -keepalive=30 -remote-if=0
sshtun tap0 ssh_tun:$ecRet@192.168.1.1 start
sshtun tap0 -cipher-algos=aes256-cbc -kex-algos=diffie-hellman-group1-sha1 -hostkey-algos=ssh-rsa  -hash-
algos=hmac-sha1 -comp-algos=none
sshd start
sshtun start
```

- На разных концах туннеля можно настроить на tap-интерфейсах IP-адреса из разных подсетей (например 192.168.1.1/24 и 192.168.100.1/24). Однако при такой конфигурации с обеих сторон будут необходимы статические маршруты, настраиваемые командой:

```
route add <net>/<mask> <local_interface_ip_address> -iface
```

При добавлении маршрута с указанием адреса локального интерфейса в качестве шлюза и опцией "*-iface*" пакеты будут отправляться через данный интерфейс (в нашем случае tap0).

- При настройке SSH-туннеля с использованием порта, отличного от "*22*".

На сервере:

Добавить команду "*sshd -port*" с указанием порта в диапазоне 1...32767.

```
sshd -port 32000
```

На клиенте:

В команду, указывающую адрес сервера, логин и пароль, следует добавить номер порта.

```
sshtun tap0 ssh_tun:$ecRet@10.10.10.1:32000
```

- Между двумя устройствами можно настроить более одного SSH-туннеля. Для этого создаются дополнительные tap-интерфейсы.

Устройство 1 (сервер)

```
ifc tap0 192.168.1.1/24 up
sshd tunnel add ssh_tun $ecRet tap0
sshd -window=128000 -keepalive=30
sshd start
ifc tap1 192.168.100.1/24 up
sshd tunnel add ssh_tun $ecRet tap1
sshd -window=128000 -keepalive=30
sshd start
```

Устройство 2 (клиент)

```
ifc tap0  192.168.1.2/24 up
sshtun tap0 -window=128000 -keepalive=30 -remote-if=0
sshtun tap0 ssh_tun:$ecRet@192.168.1.1 start
sshd start
sshtun start
ifc tap1  192.168.100.2/24 up
sshtun tap1 -window=128000 -keepalive=30 -remote-if=1
sshtun tap1 ssh_tun:$ecRet@192.168.100.1 start
sshtun start
```

SSH-туннель между устройством Инфинет и клиентом с запущенным openssh

На устройстве Инфинет конфигурация производится описанным выше способом.

```
ifc tap0 10.10.20.1/24 up
sshd tunnel add TEST QQTEST tap0
sshd start
```

В данном примере клиентское устройство - это сервер с ОС Debian. На клиентском устройстве необходимо предварительно установить пакет uml-utilities.

```
tunctl
ifconfig tap0 up
ifconfig tap0 10.10.20.2/24
ssh -N –o Tunnel=Ethernet –w 0:0 TEST@10.10.20.1
```

Далее система запросит пароль и, при успешном его вводе, поднимется туннель, по которому могут быть переданы данные. Чтобы туннель работал в фоновом режиме следует использовать команду:

```
ssh -fN –o Tunnel=Ethernet –w 0:0 TEST@10.10.20.1
```

Title

ВНИМАНИЕ

Без опции -N (не выполнять команды) туннель, при наличии установленного на устройстве Инфинет пароля, не поднимется.