

IPsec

Установка

- CentOS

```
dnf install libreswan
```

- Debian

```
...
```

Файлы

- `/etc/ipsec.d` - директория для файлов конфигурации
 - `*.conf` - файл конфигурации для создания соединения
 - `*.secrets` - файл хранящий секретный ключ

Конфигурация

1. После установки необходимо создать файл `*.conf` в директории `/etc/ipsec.d` и указать в нем необходимые параметры соединения

```
1 conn GRE-over-IPsec
2     auto=start
3     type=tunnel
4     authby=secret
5     ike=3des-sha2;dh14
6     esp=aes-sha2
7     left=10.10.10.1
8     right=20.20.20.100
9     leftprotoport=gre
10    rightprotoport=gre
11    pfs=no
```

, где -

- **Раздел conn** содержит спецификацию соединения, определяющую сетевое соединение, которое должно быть сделано с использованием IPsec. Данное имя является произвольным и используется для идентификации соединения.
- `auto=start` означает, что даже после перезагрузки произойдет согласование соединения.
- `type=tunnel` — тип соединения туннель (Host-to-Host соединение).
- `authby=secret` означает, что аутентификация будет по секретному ключу.
- `ike=3des-sha1;dh14` — настройка фазы ike, вся информация дается в задании. Шифрование 3DES. Проверка целостности SHA-1. Группа Диффи — Хеллмана 14 (2048).
- `esp=aes-sha2` — настройка второй фазы.
- `left=20.20.20.100` — Local IP-адрес.

- o `right=10.10.10.1` — Remote IP-адрес.
 - o `leftprotoport=gre` и `rightprotoport=gre` — используем протокол GRE.
 - o `pfs=no` — прямая секретность ключа. Иногда возникает проблема из-за этой настройки. Выключаем
2. После чего, если используется аутентификация по секретному ключу, необходимо создать в той же директории файл `*.secrets`

```
1 10.10.10.1 20.20.20.100 : PSK "WSR-2019"
```

, где -

- o `10.10.10.1` - локальный адрес
 - o `20.20.20.100` - удаленный адрес
 - o `:` PSK
 - o `"WSR-2019"` - ключ
3. Затем необходимо повторить те же действия на противоположном хосте, поменяв местами адрес **источника** и **назначения**
 4. После завершения конфигурации, необходимо включить автозапуск и запустить сервис

```
1 systemctl enable ipsec
2 systemctl start ipsec
```

5. Для применения настроек необходимо перезапустить сервис командой `ipsec restart`

Проверка

`ipsec status` - пункт **"Total IPsec connections"** должен содержать **одно загруженное** и **одно активное** соединение

```
000
000 Total IPsec connections: loaded 1, active 1
000
000 State Information: DDoS cookies not required, Accepting new IKE connections
000 IKE SAs: total(1), half-open(0), open(0), authenticated(1), anonymous(0)
000 IPsec SAs: total(1), authenticated(1), anonymous(0)
000
000 #1: "IPsec_tunnel":500 STATE_PARENT_I3 (PARENT SA established): EVENT_SA_REKEY in 1026s; newest ISAKMP: idle;
000 #2: "IPsec_tunnel":500 STATE_U2_IPSEC_I (IPsec SA established): EVENT_SA_REKEY in 26467s; newest IPSEC: eroute owner: isakmp#1: idle;
000 #2: "IPsec_tunnel" esp.67346039@20.20.20.100 esp.59243bfa@10.10.10.1 tun.0@20.20.20.100 tun.0@10.10.10.1 ref=0 refhim=0 Traffic: ESPIn=16KB ESPout=17KB! ESP
max=0B
000
000 Bare Shunt list:
000
[root@L-FW ~]#
```