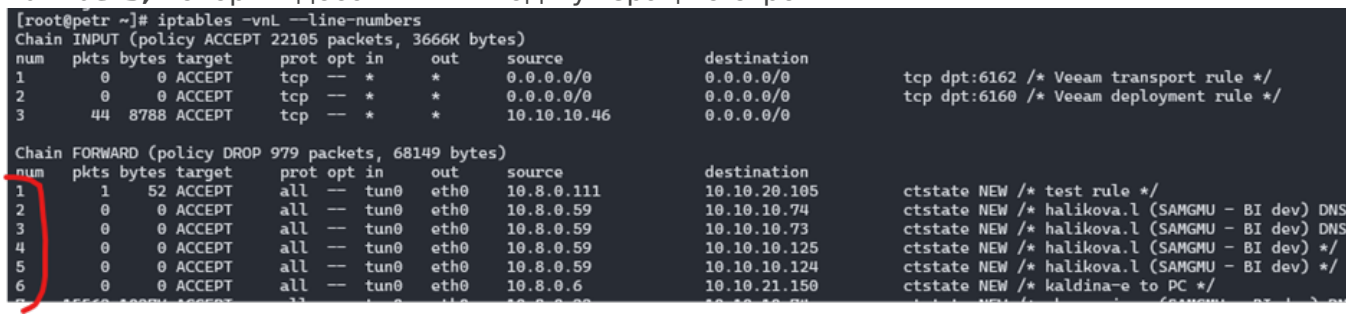
Удаление правил и отзыв сертификата

1. Если случайно добавили не, то правило в iptables или старое просто нужно удалить, то в выводе команды iptables необходимо добавить еще один ключик **--line-numbers,** который добавит в вывод нумерацию строк.



```
[root@petr ~]# iptables -vnL --line-numbers
Chain INPUT (policy ACCEPT 22105 packets, 3666K bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:6162 /* Veeam transport rule */
2        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:6160 /* Veeam deployment rule */
3       44  8788 ACCEPT     tcp  --  *      *       10.10.10.46          0.0.0.0/0

Chain FORWARD (policy DROP 979 packets, 68149 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        1    52 ACCEPT     all  --  tun0   eth0    10.8.0.111           10.10.20.105        ctstate NEW /* test rule */
2        0     0 ACCEPT     all  --  tun0   eth0    10.8.0.59            10.10.10.74         ctstate NEW /* halikova.l (SAMGMU - BI dev) DNS
3        0     0 ACCEPT     all  --  tun0   eth0    10.8.0.59            10.10.10.73         ctstate NEW /* halikova.l (SAMGMU - BI dev) DNS
4        0     0 ACCEPT     all  --  tun0   eth0    10.8.0.59            10.10.10.125        ctstate NEW /* halikova.l (SAMGMU - BI dev) */
5        0     0 ACCEPT     all  --  tun0   eth0    10.8.0.59            10.10.10.124        ctstate NEW /* halikova.l (SAMGMU - BI dev) */
6        0     0 ACCEPT     all  --  tun0   eth0    10.8.0.6             10.10.21.150        ctstate NEW /* kaldina-e to PC */
```

```
iptables -vnL --line-numbers
```

Для удаления нужного правила, просто вводим

iptables -D FORWARD номер

номер – собственно номер правила.

```
iptables -D FORWARD 1 – удалит наше правило.
```

Отзыв сертификата

Для отзыва сертификата, мы используем ту же самую утилиту easyrsa

```
./easyrsa revoke fursov.m
```

В процессе отзыва будет задан вопрос «уверены-ли вы», на который отвечаем **yes**

А так же будет запрошен пароль CA для отзыва сертификата

```
[root@petr easy-rsa]# ./easyrsa revoke fursov-m

Note: using Easy-RSA configuration from: ./vars


Please confirm you wish to revoke the certificate with the following subject:

subject=
    commonName                = fursov-m


Type the word 'yes' to continue, or any other input to abort.
  Continue with revocation: yes
Using configuration from ./openssl-1.0.cnf
Enter pass phrase for /etc/openvpn/easy-rsa/pki/private/ca.key:
Revoking Certificate 9292F95D156949D432654C6B84E43B3D.
Data Base Updated

IMPORTANT!!!

Revocation was successful. You must run gen-crl and upload a CRL to your
infrastructure in order to prevent the revoked cert from being accepted.

[root@petr easy-rsa]#
```

После отзыва сертификата, утилита в консоли напомнит, что необходимо будет обновить файлик crl – файл, в котором содержится список всех отозванных сертификатов.

Делается это в пару команд:

1. Генерация нового файла CRL:

```
/etc/openvpn/easy-rsa/easyrsa gen-crl
```

(запросит пароль CA)

2. Копирование его в нужную директорию:

```
cp /etc/openvpn/easy-rsa/pki/crl/pem /etc/openvpn/keys/crl.pem
```

Система спросит, перезаписать-ли файл, вводим – **y**

```
[root@petr easy-rsa]# cp /etc/openvpn/easy-rsa/pki/crl.pem /etc/openvpn/keys/crl.pem
cp: overwrite ‘/etc/openvpn/keys/crl.pem’? y
[root@petr easy-rsa]#
```

3. Перезапускаем сервер openvpn, чтобы настройки применились.

```
systemctl restart openvpn@server
```

Revision #2
Created 25 March 2025 11:43:58 by admin_vy
Updated 25 March 2025 11:50:11 by admin_vy