

Оглавление



- Работа с firewalld в CentoS 7
 - Общие команды управления
 - Запуск firewalld `systemctl start firewalld` Добавление в автозагрузку `systemctl enable firewalld` Управление правилами
 - Применение новых правил (загрузка постоянных правил, добавленных с permanent) `firewall-cmd --reload` Применение новых правил с принудительным разрывом сессий `firewall-cmd --complete-reload` Сделать правила, установленные в данный момент постоянными (иначе после перезапуска они пропадут) `firewall-cmd --runtime-to-permanent` Добавление сервиса
 - Добавление порта
 - Удаление сервиса/порта
 - Управление зонами
 - Похожие записи:

Работа с firewalld в CentoS 7

Требуется разрешить доступ только к определенным портам, а все остальное скрыть? Firewalld в этом поможет.

Ниже я покажу как происходит Работа с firewalld в CentoS 7 и некоторые команды управления им:

Общие команды управления

Проверим, запущен ли firewalld

```
systemctl status firewalld
```

Результат будет подобным:

```
● firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled;
 vendor preset: enabled)
  Active: active (running) since Чт 2018-01-11 11:11:40 MSK; 1h 44min
```

```
ago
Docs: man:firewalld(1)
Main PID: 32463 (firewalld)
CGroup: /system.slice/firewalld.service
└─32463 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid
```

Также можно выполнить команду

```
firewall-cmd --state
```

Запуск firewalld

```
systemctl start firewalld
```

Добавление в автозагрузку

```
systemctl enable firewalld
```

Управление правилами

Просмотр списка активных правил:

```
firewall-cmd --list-all
```

Вывод означает следующее:

```
public
target: default
icmp-block-inversion: no
interfaces:
sources:
services: dhcpv6-client ssh http https
ports:
protocols:
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
```

Установлены правила для зоны Public, а именно сделать доступными снаружи сервисы `dhcprv6-client` (DHCP), `ssh`, `http`, `https` для всех интерфейсов

Применение новых правил (загрузка постоянных правил, добавленных с `permanent`)

```
firewall-cmd --reload
```

Применение новых правил с принудительным разрывом сессий

```
firewall-cmd --complete-reload
```

Сделать правила, установленные в данный момент постоянными (иначе после перезапуска они пропадут)

```
firewall-cmd --runtime-to-permanent
```

Добавление сервиса

Получим список сервисов, которые можно использовать. Сервисы в данном случае — набор портов и протоколов, на которых данные сервисы доступны.

```
firewall-cmd --get-services
```

Разрешим доступ для `ntp` извне на постоянной основе

```
firewall-cmd --permanent --zone=public --add-service=ntp
```

Или например **разрешим доступ по HTTP и HTTPS** т.е. доступ к вебсерверу на сервере

```
firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
```

Зону указывать не обязательно, **по умолчанию используется зона public**, если не указано иначе.

Параметр **—permanent** означает, что данное правило будет применено на

постоянной основе, иначе правило будет действовать **до перезагрузки**

После добавления правил, не забудьте их применить.

Также **можно добавить свой сервис**, если его нет в общем списке:

```
firewall-cmd --permanent --new-service=myservice
```

где myservice — имя вашего сервиса

Будем считать, что сервису для работы нужны **1234/tcp** и **1235/udp** порты

```
firewall-cmd --permanent --service=myservice --add-port=1234/tcp  
firewall-cmd --permanent --service=myservice --add-port=1235/udp
```

Можно добавить краткое и полное описание сервиса

```
firewall-cmd --permanent --service=myservice --set-short="My  
Service"  
firewall-cmd --permanent --service=myservice --set-description="Long  
Description for My Service"
```

После этого созданный сервис можно использовать в правилах

```
firewall-cmd --permanent --add-service=myservice
```

Добавление порта

Добавление одного порта, в данном случае порт **80** и протокол **TCP**

```
firewall-cmd --permanent --add-port=80/tcp
```

Добавление диапазона портов

```
firewall-cmd --permanent --add-port=6666-6669/udp
```

Удаление сервиса/порта

Удаление портов и сервисов **происходит аналогично добавлению**, только

заменяется add на remove

Т.е. добавили порт

```
firewall-cmd --permanent --add-port=80/tcp
```

удалили его

```
firewall-cmd --permanent --remove-port=80/tcp
```

Управление зонами

Список всех зон

```
firewall-cmd --list-all-zones
```

Список активных (используемых) зон

```
firewall-cmd --get-active-zones
```

Информация о зоне public

```
firewall-cmd --list-all --zone=public
```

Действие по умолчанию для зоны

```
firewall-cmd --permanent --zone=public --set-target=DROP
```

DROP — сброс всех соединений

В данном случае для зоны public включается правило «**запрещено всё, что не разрешено**»

Похожие записи:

1. Установка VNC на CentOS 7
2. Как установить RabbitMQ в CentOS 7