# Настройка сетевого экрана firewalld в CentOS 7

Если сервер подключен к Интернету, он должен быть защищен от несанкционированного доступа. **Сетевой экран** (***брандмауэр, firewall***) является частью этой защиты. Ядро Linux реализует межсетевой экран через свою компоненту — инфраструктуру **netfilter**. Чтобы настроить, какие пакеты разрешены, а какие нет, в **Red Hat Enterprise Linux** (RHEL) **7** / **CentOS 7** по умолчанию используется системная служба **firewalld**.

## О сетевом экране Linux

Сетевой экран можно использовать для ограничения трафика, поступающего на сервер или выходящего с сервера. Межсетевой экран реализован в ядре Linux с помощью подсистемы **netfilter**. **Netfilter** позволяет модулям ядра проверять каждый входящий, исходящий или пересылаемый пакет и воздействовать на такой пакет, разрешая или блокируя его.

### Предыдущие решения

Для взаимодействия с компонентой ядра **netfilter** могут использоваться разные инструменты. В более ранних версиях **RHEL / CentOS** для настройки фильтрации пакетов **netfilter** использовалась утилита **iptables**, запускаемая из командной строки. Она обеспечивала подробный способ определения правил брандмауэра, но его было трудно использовать из-за сложного синтаксиса команд **iptables** и потому, что правила упорядочения могли быть относительно сложными. Служба **iptables** по-прежнему предлагается в **RHEL 7 / CentOS 7**. Однако она не рекомендуется в качестве службы по умолчанию и не может использоваться на сервере, где также используется **firewalld**.

### Сетевой экран firewalld

В RHEL 7 был представлен новый метод: **firewalld** — это системная служба, которая может настраивать правила брандмауэра с использованием различных интерфейсов пользователя.

**Firewalld** был разработан как совершенно новое решение для управления брандмауэрами Linux. Он использует службу **firewalld** для управления конфигурацией брандмауэра **netfilter**. Служба **firewalld** несовместима со службой **iptables**. Никогда не следует использовать **firewalld** и **iptables** в одной системе; они взаимоисключающие.

Основные понятия, используемые демоном **firewalld** — **зоны** и **службы**.

### Зоны демона firewalld

**Зона** — это набор правил, которые применяются к входящим пакетам, соответствующим конкретному адресу источника или сетевому интерфейсу. **Firewalld** применяется по умолчанию только к входящим пакетам, а на исходящих пакетах фильтрация не выполняется.

Использование зон особенно важно на серверах с несколькими сетевыми интерфейсами.

На таких серверах зоны позволяют администраторам легко назначать определенный набор правил. Например, интерфейсы Wi-Fi и LAN могут иметь разные правила фильтрации пакетов.

На серверах, имеющих только один сетевой интерфейс, вполне можно использовать только одну зону, которая является зоной по умолчанию. Каждый пакет, поступающий в систему, анализируется на предмет адреса источника, и на основе этого адреса источника **firewalld** определяет, принадлежит ли пакет к определенной зоне. Если это не так, используется зона для входящего сетевого интерфейса. Если конкретная зона недоступна, пакет обрабатывается настройками в зоне по умолчанию.

**Firewalld** работает с некоторыми зонами по умолчанию. Ниже приведен список этих зон, отсортированных в соответствии с уровнем доверия по умолчанию от ненадежных до доверенных:

* **drop**

Любые входящие сетевые пакеты отбрасываются без каких-либо уведомлений. Возможны только исходящие сетевые подключения.

* **block**

Любые входящие сетевые подключения отклоняются с отправлением сообщения **icmp-host-prohibited** для IPv4 и **icmp6-adm-prohibited** для IPv6. Возможны только сетевые подключения, инициированные внутри этой системы.

* **public**

Для использования в общественных местах. Вы не доверяете другим компьютерам в сети, чтобы не нанести вред вашему компьютеру. Принимаются только выбранные входящие соединения.

* **external**

Для использования во внешних сетях с включенным механизмом **преобразования сетевых адресов** (**NAT**), особенно для маршрутизаторов. Вы не доверяете другим компьютерам в сети, чтобы не нанести вред вашему компьютеру. Принимаются только выбранные входящие соединения.

* **dmz**

Для компьютеров в вашей демилитаризованной зоне, которые являются доступными публично для внешней сети и имеют ограниченный доступ к вашей внутренней сети. Принимаются только выбранные входящие соединения.

* **work**

Для использования в рабочих зонах. Вы в основном доверяете другим компьютерам в сети, чтобы не навредить вашему компьютеру. Принимаются только выбранные входящие соединения.

* **home**

Для использования в домашних условиях. Вы в основном доверяете другим компьютерам в сети, чтобы не навредить вашему компьютеру. Принимаются только выбранные входящие соединения.

* **internal**

Для использования во внутренних сетях. Вы в основном доверяете другим компьютерам в сети, чтобы не навредить вашему компьютеру. Принимаются только выбранные входящие соединения.

* **trusted**

Все сетевые подключения принимаются.

### Какую зону следует использовать?

Например, общедоступное подключение к сети WIFI должно быть в основном ненадежным, а подключение к проводной домашней сети должно быть достаточно надежным. Выберите зону, которая наилучшим образом соответствует используемой вами сети.

### Как настроить или добавить зоны?

Для настройки или добавления зон можно использовать один из инструментов **firewalld** для обработки и изменения конфигурации. Это графический инструмент конфигурации **firewall-config** (по умолчанию не установлен) или инструмент командной строки **firewall-cmd**.

### Как установить или изменить зону для соединения

Для каждого сетевого интерфейса в каталоге **/etc/sysconfig/network-scripts/** есть файл конфигурации **ifcfg‑*имя\_интерфейса***, например, **ifcfg-enp0s3**. Файл конфигурации содержит все параметры сетевого интерфейса:

TYPE="Ethernet"

PROXY\_METHOD="none"

BROWSER\_ONLY="no"

BOOTPROTO="dhcp"

DEFROUTE="yes"

IPV4\_FAILURE\_FATAL="no"

IPV6INIT="yes"

IPV6\_AUTOCONF="yes"

IPV6\_DEFROUTE="yes"

IPV6\_FAILURE\_FATAL="no"

IPV6\_ADDR\_GEN\_MODE="stable-privacy"

NAME="enp0s3"

UUID="52c94ff0-ea9c-413e-becb-188b896734b7"

DEVICE="enp0s3"

ONBOOT="yes"

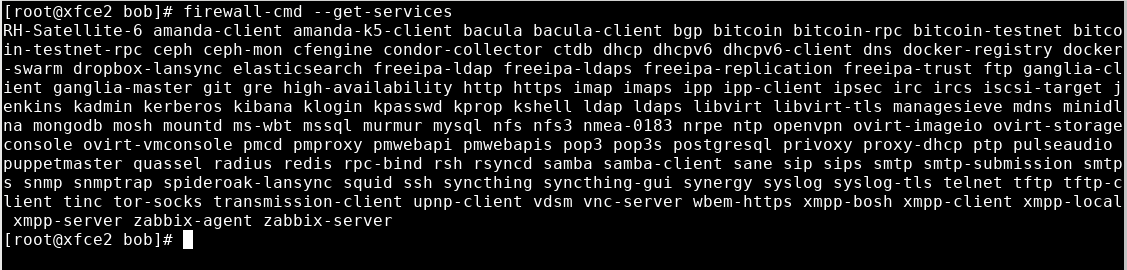
Зона сохраняется в файле конфигурации сетевого интерфейса при помощи параметра **ZONE =**. Если параметр **ZONE** отсутствует или имеет пустое значение, используется зона по умолчанию, заданная в **firewalld**.

### Сервисы (службы) Firewalld

Вторым ключевым элементом при работе с **firewalld** является сервис (служба). Сервис в **firewalld** отличается от службы в **systemd**. Сервис в **firewalld** представляет собой комбинацию записей, состоящих из порта и/или протокола. В **firewalld** определены сервисы по умолчанию, которые позволяют администраторам легко разрешать или запрещать доступ к определенным портам на сервере.

С каждым сервисом связан файл конфигурации, который объясняет, какие порты UDP или TCP задействованы, и, если требуется, какие модули ядра должны быть загружены. Чтобы получить список всех сервисов, доступных на вашем компьютере, вы можете использовать команду

**firewall‑cmd --get‑services**.



По сути, при работе с **firewalld** все сводится к тому, что в нужные зоны необходимо добавлять нужные сервисы. В особых случаях конфигурация может быть расширена за счет более конкретных настроек.

Файлы сервисов (служб) хранятся в каталоге **/usr/lib/firewalld/services** или **/etc/firewalld/services**. В следующем листинге показано, как выглядит содержимое файла сервиса **http**.

<?xml version="1.0" encoding="utf-8"?>

<service>

<short>WWW (HTTP)</short>

<description>HTTP is the protocol used to serve Web pages. If you plan to make your Web server publicly available, enable this option. This option is not required for viewing pages locally or developing Web pages.</description>

<port protocol="tcp" port="80"/>

</service>

### Работа с firewalld

Для настройки сетевого экрана **firewalld** доступны два инструмента: инструмент командной строки **firewall-cmd**; и инструмент с графическим интерфейсом **firewall-config**. Всё, что можно сделать с помощью инструмента командной строки, можно сделать и с помощью графического инструмента.

При работе с любым из этих инструментов следует знать, **где именно вносятся изменения**. Оба инструмента работают с состоянием конфигурации, хранящимся в памяти, в дополнение к состоянию конфигурации, хранящемуся на диске (постоянному состоянию). При использовании любого из этих инструментов обязательно передайте изменения на диск, прежде чем продолжить.

**ВНИМАНИЕ!** Ранее для управления сетевым экраном ядра **netfilter** вместо демона **firewalld** использовалось другое программное решение — утилита командной строки **iptables**. Название **iptables** использовалось также для обозначения собственно сетевого экрана. В некоторых дистрибутивах Linux программа **iptables** используется и сейчас. Программы **iptables** и **firewalld** несовместимы друг с другом. При работе с **firewalld** убедитесь, что исключена возможность случайного использования **iptables** для настройки брандмауэра. Использование **iptables** может серьезно испортить конфигурацию вашего брандмауэра, особенно если служба **iptables** загружена в системе, где уже загружена служба **firewalld**. Чтобы убедиться, что это никогда не может случиться, используйте команду

systemctl mask iptables

Эта команда гарантирует, что служба **iptables** не может быть запущена случайно.

#### Упражнение. Управление брандмауэром с помощью firewall-cmd.

1. Откройте shell с полномочиями суперпользователя root. Введите команду

firewall-cmd --get-default-zone

Она показывает текущую зону по умолчанию. Вы увидите текущую зону по умолчанию, которой по умолчанию является зона **public**.

1. Чтобы увидеть, какие зоны доступны, введите команду

firewall-cmd --get-zones

1. Теперь покажите сервисы, доступные на вашем сервере, используя команду

firewall-cmd --get-services

Обратите внимание, что параметры **firewall-cmd --get** показывают, что доступно на вашем сервере.

1. Чтобы увидеть, какие службы доступны в текущей зоне, введите

firewall-cmd --list-services

Вы увидите короткий список, содержащий клиент протокола DHCP, а также Secure Shell (SSH).

[root@xfce2 firewalld]# firewall-cmd --get-default-zone # вывести зону по умолчанию

public

[root@xfce2 firewalld]# firewall-cmd --get-zones # какие зоны доступны

block dmz drop external home internal public trusted work

[root@xfce2 firewalld]# firewall-cmd --get-services # сервисы доступные на сервере

RH-Satellite-6 amanda-client amanda-k5-client bacula bacula-client bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc ceph ceph-mon cfengine condor-collector ctdb dhcp dhcpv6 dhcpv6-client dns docker-registry docker-swarm dropbox-lansync elasticsearch freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp ganglia-client ganglia-master git gre high-availability http https imap imaps ipp ipp-client ipsec irc ircs iscsi-target jenkins kadmin kerberos kibana klogin kpasswd kprop kshell ldap ldaps libvirt libvirt-tls managesieve mdns minidlna mongodb mosh mountd ms-wbt mssql murmur mysql nfs nfs3 nmea-0183 nrpe ntp openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy proxy-dhcp ptp pulseaudio puppetmaster quassel radius redis rpc-bind rsh rsyncd samba samba-client sane sip sips smtp smtp-submission smtps snmp snmptrap spideroak-lansync squid ssh syncthing syncthing-gui synergy syslog syslog-tls telnet tftp tftp-client tinc tor-socks transmission-client upnp-client vdsm vnc-server wbem-https xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server

[root@xfce2 firewalld]# firewall-cmd --get # опции --get:

usage: see firewall-cmd man page

firewall-cmd: error: ambiguous option: --get could match --get-log-denied, --get-all-passthroughs, --get-icmptypes, --get-ipset-types, --get-all-rules, --get-ipsets, --get-rules, --get-zone-of-interface, --get-services, --get-entries, --get-zone-of-source, --get-protocols, --get-destinations, --get-modules, --get-automatic-helpers, --get-chains, --get-zones, --get-ports, --get-target, --get-active-zones, --get-description, --get-module, --get-helpers, --get-passthroughs, --get-source-ports, --get-family, --get-default-zone, --get-short, --get-all-chains, --get-destination

[root@xfce2 firewalld]# firewall-cmd --list-services # службы доступные в текущей зоне

ssh dhcpv6-client

[root@xfce2 firewalld]#

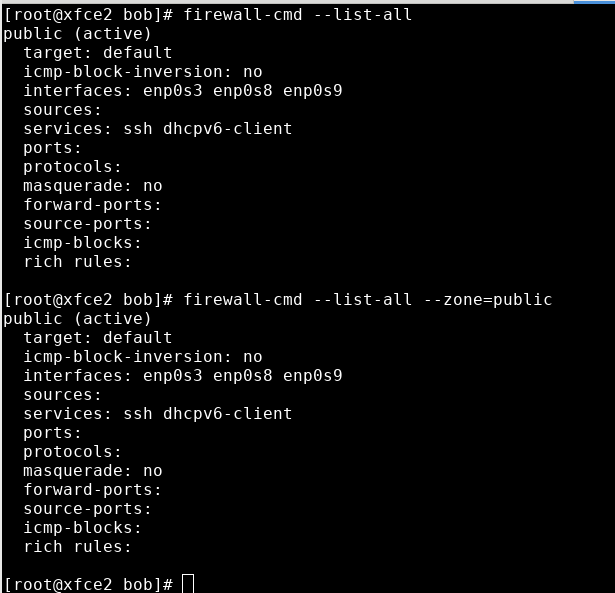
1. Теперь введите

firewall-cmd --list-all

Посмотрите на вывод и сравните вывод с результатом

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

Обе команды показывают полный обзор текущей конфигурации брандмауэра, как показано в листинге.



Обратите внимание, что вы видите гораздо больше, чем просто зону и службы, которые настроены в этой зоне; вы также видите информацию об интерфейсах и более продвинутых предметах.

## Примеры использования утилиты firewall-cmd.

* Получить статус **firewalld**:

firewall-cmd --state

* Перезагрузить брандмауэр, не теряя информацию о состоянии:

firewall-cmd --reload

* Получить список всех поддерживаемых зон:

firewall-cmd --get-zones

* Получить список всех поддерживаемых служб:

firewall-cmd --get-service

* Получить список всех зон с включенными функциями:

firewall-cmd --list-all-zones

* Распечатать зону <zone> с включенными функциями. Если зона опущена, будет использоваться зона по умолчанию

firewall-cmd [--zone=<zone>] --list-all

* Получить зону по умолчанию, установленную для сетевых подключений:

firewall-cmd --get-default-zone

* Установить зону по умолчанию:

firewall-cmd --set-default-zone=<zone>

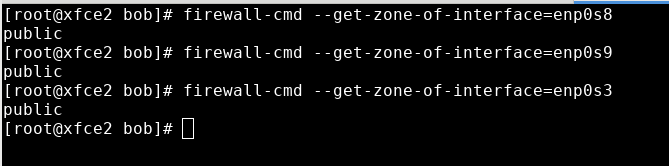
Все интерфейсы, расположенные в зоне по умолчанию, будут помещены в новую зону по умолчанию, что определяет ограничения для новых попыток подключения, инициированного извне. Активные соединения не затрагиваются.

* Получить активные зоны:

firewall-cmd --get-active-zones

* Получить зону, связанную с интерфейсом:

firewall-cmd --get-zone-of-interface=<interface>



* Добавить интерфейс в зону:

firewall-cmd [--zone=<zone>] --add-interface=<interface>

* Изменить зону, к которой принадлежит интерфейс:

firewall-cmd [--zone=<zone>] --change-interface=<interface>

* Удалить интерфейс из зоны:

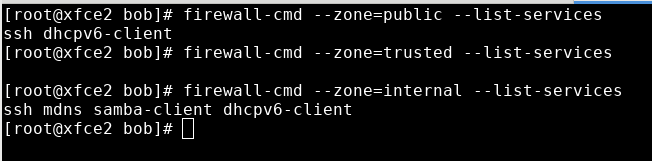
firewall-cmd [--zone=<zone>] --remove-interface=<interface>

* Запросить, находится ли интерфейс в зоне:

firewall-cmd [--zone=<zone>] --query-interface=<interface>

* Список включенных служб в зоне:

firewall-cmd [ --zone=<zone> ] --list-services



* Включить службу в зоне:

firewall-cmd [--zone=<zone>] --add-service=<service> [--timeout=<seconds>]

* Включить службу http в зоне по умолчанию:

firewall-cmd --add-service=http

* Отключить службу в зоне:

firewall-cmd [--zone=<zone>] --remove-service=<service>

* Отключить службу http-в зоне **home**:

firewall-cmd --zone=home --remove-service=http

* Запросить, включена ли служба в зоне:

firewall-cmd [--zone=<zone>] --query-service=<service>

Возвращает 1, если служба включена в зоне, в противном случае 0.

* Включить комбинацию порта и протокола в зоне:

firewall-cmd [--zone=<zone>] --add-port=<port>[-<port>]/<protocol> [--timeout=<seconds>]

Позволяет использовать комбинацию порта и протокола. Порт может быть одним портом <port> или диапазоном портов <port> - <port>. Протокол может быть либо **tcp**, либо **udp**.

* Отключить комбинацию порта и протокола в зоне:

firewall-cmd [--zone=<zone>] --remove-port=<port>[-<port>]/<protocol>

* Запросить, включена ли комбинация порта и протокола в зоне:

firewall-cmd [--zone=<zone>] --query-port=<port>[-<port>]/<protocol>

* Включить блокировку ICMP в зоне:

firewall-cmd [--zone=<zone>] --add-icmp-block=<icmptype>

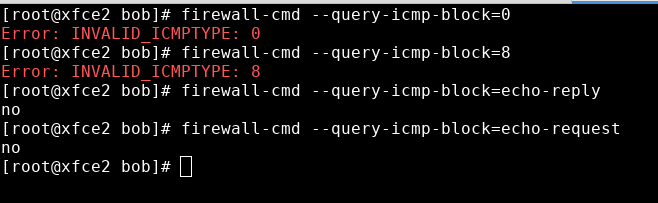
Позволяет заблокировать выбранное сообщение ICMP. Сообщения ICMP являются либо информационными запросами, либо создаются как ответ на информационные запросы или в условиях ошибки.

* Отключить блокировку ICMP в зоне:

firewall-cmd [--zone=<zone>] --remove-icmp-block=<icmptype>

* Запрос о состоянии ICMP-блокировки в зоне

firewall-cmd [--zone=<zone>] --query-icmp-block=<icmptype>



* Включить переадресацию или отображение портов в зоне:

firewall-cmd [--zone=<zone>] --add-forward-port=port=<port>[-<port>]:proto=<protocol> { :toport=<port>[-<port>] | :toaddr=<address> | :toport=<port>[-<port>]:toaddr=<address> }

Порт port отображается либо на тот же порт на другом хосте, либо на другой порт на том же хосте, либо на другой порт на другом хосте. Порт может быть отдельным портом <port> или диапазоном портов <port>-<port>. Протокол protocol — это либо **tcp**, либо **udp**. toport — это порт <port> или диапазон портов <port> - <port>. toaddr — это адрес IPv4. Переадресация портов — IPv4 только из-за ограничений ядра.

* Отключить переадресацию или отображение портов в зоне:

firewall-cmd [--zone=<zone>] --remove-forward-port=port=<port>[-<port>]:proto=<protocol> { :toport=<port>[-<port>] | :toaddr=<address> | :toport=<port>[-<port>]:toaddr=<address> }

* Запрос состояния переадресации или сопоставления портов в зоне:

firewall-cmd [--zone=<zone>] --query-forward-port=port=<port>[-<port>]:proto=<protocol> { :toport=<port>[-<port>] | :toaddr=<address> | :toport=<port>[-<port>]:toaddr=<address> }

* Переслать соединение **ssh** на хост 127.0.0.2 в зоне **home**:

firewall-cmd --zone=home --add-forward-port=port=22:proto=tcp:toaddr=127.0.0.2

## Расширенные правила (rich rules)

**Rich rules** (расширенные правила) предоставляют администраторам простой в использовании выразительный язык для определения пользовательских правил, которые не могут быть созданы с использованием синтаксиса **firewalld** по умолчанию.

### Синтаксис Rich Rule

С помощью расширенного языка (rich language) более сложные правила брандмауэра могут быть созданы простым для понимания способом. Язык использует **ключевые слова** со значениями.

Расширенный язык расширяет элементы текущей зоны (служба, порт, icmp-блок, icmp-тип, маскарад, forward-port и source-port) дополнительными адресами источника и назначения, ведением журнала, действиями и ограничениями для журналов и действий.

Информацию о расширенном языковом представлении, используемом в файлах конфигурации зоны, можно найти в **firewalld.zone (5)**.

**Rich rules** используются для создания правил разрешения/запрета, но с расширенными опциями, такими как:

* Конфигурация журнала (логгирования) (Logging configuration)
* Переадресация портов (Port forwarding)
* Маскировка (Masquerading)
* Ограничение скорости (Rate limiting)
* Разрешение / запрет подключения для одной конкретной зоны (Allow/deny connections for one specific zone)

Общая структура правила

rule

[source]

[destination]

service|port|protocol|icmp-block|icmp-type|masquerade|forward-port|source-port

[log]

[audit]

[accept|reject|drop|mark]

Полное правило предоставляется в виде **одной** строки.

Структура правила для описания источника в черном или белом списке:

rule

source

[log]

[audit]

accept|reject|drop|mark

Используется для предоставления или ограничения доступа из источника source к этой машине или машинам, которые доступны этой машине.

**Важная информация о параметрах элемента**: параметры для элемента в правиле должны быть добавлены точно после элемента. Если параметр размещен где-то еще, он может использоваться для другого элемента, если он соответствует параметрам другого элемента, или приведет к ошибке правила.

Ниже дается описание элементов расширенного правила: rule, source, destination, service, port, protocol, icmp-block, masquerade, icmp-type, forward-port, source-port, log, audit, action, limit.

**Rule**

rule [family="ipv4|ipv6"]

Если указан элемент правила family, он может быть "ipv4" или "ipv6", что ограничивает правило использованием версий протокола IPv4 или IPv6. Если элемент family не указан, правило будет добавлено для IPv4 и IPv6. Если в правиле используются адреса источника или получателя, необходимо указать элемент family. Это также относится и к переадресации портов / пакетов.

**Source**

source [not] address="address[/mask]"|mac="mac-address"|ipset="ipset"

Если присутствует элемент source address, источник попытки подключения может быть ограничен значением этого элемента. Адрес address — это либо отдельный IP-адрес, либо сетевой IP-адрес, MAC-адрес или IPSet. Адрес должен соответствовать семейству правила family (IPv4 / IPv6). Маска подсети выражается либо в точечно-десятичной (/x.x.x.x), либо в префиксной (/ x) нотации для IPv4, а также в префиксной нотации (/ x) для сетевых адресов IPv6. Можно инвертировать смысл адреса, добавив слово not перед адресом address. Все, кроме указанного адреса, будут совпадать.

**Destination**

destination [not] address="address[/mask]"

Если присутствует элемент destination, цель может быть ограничена значением этого элемента. Адрес назначения destination использует тот же синтаксис, что и адрес источника source.

Использование адресов источника и назначения не является обязательным, а использование адресов назначения возможно не для всех элементов. Это зависит от использования адресов назначения, например, в записях служб.

**Service**

service name="*service name*"

Служба *service name* будет добавлена к правилу. Служба *service name* является одной из служб, предоставляемых демоном **firewalld**. Для получения списка поддерживаемых служб можно использовать команду firewall-cmd --get-services.

Если служба предоставляет адрес назначения, он будет конфликтовать с адресом назначения в правиле и приведет к ошибке. Службы, использующие адреса назначения внутри [сети], в основном являются службами, использующими многоадресную передачу.

**Port**

port port="*port value*" protocol="tcp|udp"

Порт *port value* может быть либо номером порта *portid*, либо диапазоном портов *portid-portid*. Протокол *protocol* может быть TCP или UDP.

**Protocol**

protocol value="*protocol value*"

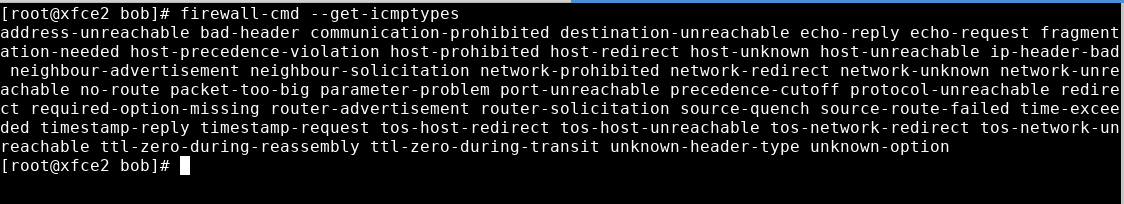
Значением элемента protocol value может быть либо идентификационный номер протокола, либо имя протокола. Допустимые записи протоколов содержатся в файле **/etc/protocols**.

**ICMP-Block**

icmp-block name="icmptype name"

icmptype — это один из поддерживаемых демоном **firewalld** типов сообщений **ICMP**. Для получения списка поддерживаемых типов **ICMP** используйте команду:

firewall-cmd --get-icmptypes



С этим элементом не разрешено указывать действие. **icmp-block** использует действие **reject** для внутреннего использования.

**Masquerade**

masquerade

Включить маскировку в правиле. Источник и адрес назначения могут быть предоставлены для ограничения маскировки в этой области.

Здесь не разрешено указывать действие.

**ICMP-Type**

icmp-type name="icmptype name"

icmptype — это один из поддерживаемых демоном **firewalld** типов сообщений **ICMP**. Для получения списка поддерживаемых типов **ICMP** используйте команду:

firewall-cmd --get-icmptypes

**Forward-Port**

forward-port port="*port value*" protocol="tcp|udp" to-port="port value" to-addr="address"

Переадресация порта / пакетов с локального порта *port value* по протоколу "**tcp**" или "**udp**" либо на другой порт локально, либо на другой компьютер, либо на другой порт на другом компьютере.

Значением порта port может быть либо один номер порта, либо диапазон портов portid‑portid. Параметр to-addr — это IP-адрес.

Здесь не разрешено указывать действие. forward-port использует действие **accept** внутренне.

**Source-Port**

source-port port="port value" protocol="tcp|udp"

Значением элемента source-port может быть либо номер порта *portid*, либо диапазон портов *portid-portid*. Протокол protocol может быть TCP или UDP.

**Log**

**Audit**

**Action**

Действие **action** может быть одним из: **accept**, **reject**, **drop** или **mark** — принять, отклонить, отбросить или пометить.

Правило может содержать элемент или только источник. Если правило содержит элемент, то новое соединение, соответствующее элементу, будет обработано действием. Если правило не содержит элемента, всё, поступающее с адреса источника, будет обработано действием **action**.

accept [limit value="rate/duration"]

reject [type="reject type"] [limit value="rate/duration"]

drop [limit value="rate/duration"]

mark set="mark[/mask]" [limit value="rate/duration"]

Действие **accept** — все новые попытки подключения будут предоставлены.

Действие **reject** — все попытки подключения не будут приняты, и их источник получит сообщение ICMP об отклонении. Тип отклонения может быть установлен для указания соответствующего сообщения об ошибке ICMP (v6). Для получения информации о допустимых типах отклонения см. **--reject-with type** на справочной странице **iptables-extensions (8)**. Поскольку типы отклонения различаются для IPv4 и IPv6, при использовании типа отклонения необходимо указать семейство протоколов **family**.

Действие **drop** — все пакеты будут отброшены немедленно, информация не отправляется источнику.

Действие **mark** — все пакеты будут помечены в цепочке PREROUTING в таблице **mangle** комбинацией метки и маски. См. раздел "**Limit**" с описанием тега **limit**.

**Limit**

limit value="rate/duration"

Можно ограничить **Log, Audit** и **Action**. Правило, использующее этот тег, будет соблюдаться, пока этот предел не будет достигнут. Показатель представляет собой натуральное положительное число [1, ..] Продолжительность составляет s, m, h, d. **s** означает секунды, **m** минуты, **h** часы и **d** дни. Максимальное предельное значение равное "2 / d", что означает максимум два совпадения в день.

Примеры расширенных правил (rich rules). Этот формат (то есть одна строка, которая задает целое правило) использует, например, команда firewall-cmd --add-rich-rule.

Опция

[**--permanent**] [**--zone**=*zone*] **--add-rich-rule**='*rule*' [**--timeout**=*timeval*]

добавляет расширенное правило (rich rule) '*rule*' для зоны *zone*. Эта опция может быть указана несколько раз. Если зона не указана, будет использоваться зона по умолчанию. Если указан тайм-аут, правило будет активным в течение указанного периода времени и впоследствии будет автоматически удалено. *timeval* — это число (в секундах) или число, за которым следует один из символов s (секунды), m (минуты), h (часы), например 20m или 1h.

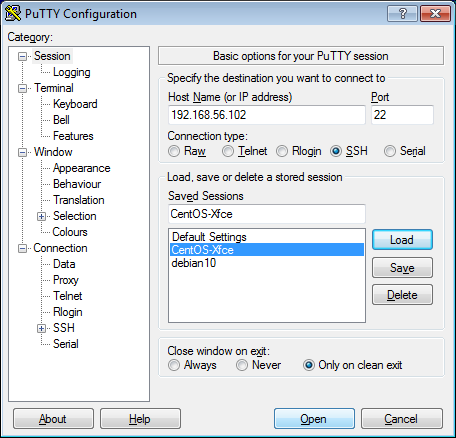
#### Пример. Добавление расширенного правила в зону по умолчанию.

Команда

firewall-cmd --add-rich-rule='rule family=ipv4 source address=192.168.56.101 port port=22 protocol=tcp reject'

должна добавлять в зону по умолчанию расширенное правило "отбрасывать все подключения к порту 22 со стороны узла 192.168.56.101".

* Проверяем до добавления **rich rule** в зону **firewalld**. Устанавливаем сеанс SSH между узлом 192.167.66.101 (Windows 7, PuTTY) и сервером SSH 192.168.56.102 (CentOS 7.6.1810): OK,

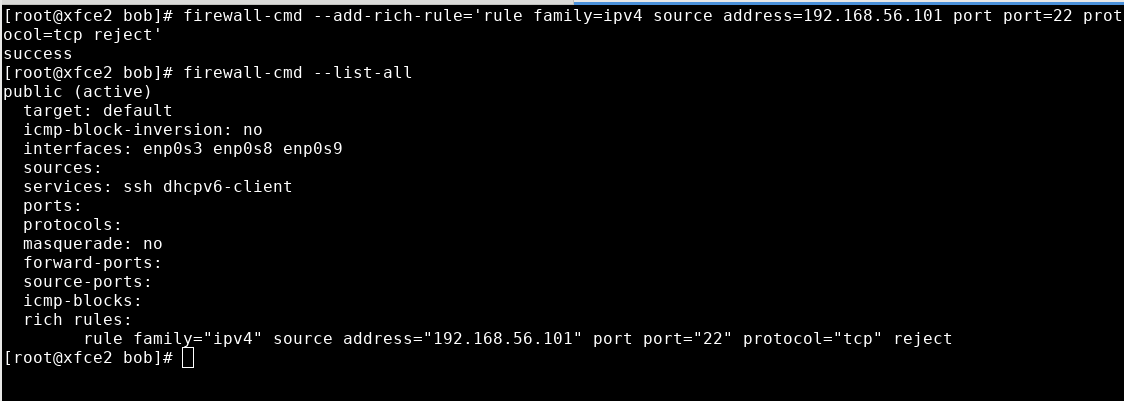


* На хосте CentOS добавляем расширенное правило в зону по умолчанию:

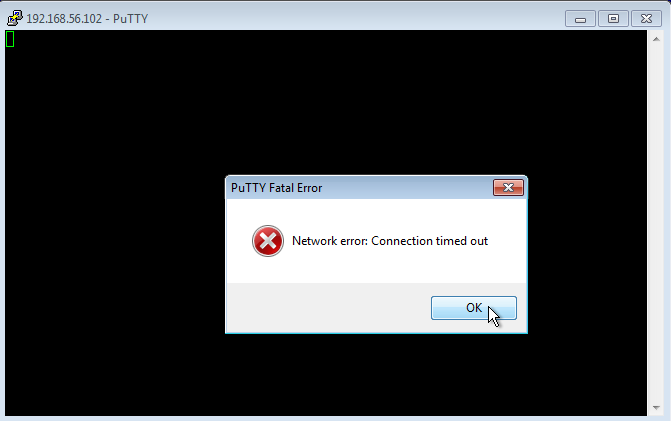
firewall-cmd --add-rich-rule='rule family=ipv4 source address=192.168.56.101 port port=22 protocol=tcp reject'

и проверяем все функции зоны по умолчанию:

firewall-cmd --list-all



* Снова устанавливаем сеанс SSH между узлом 192.167.66.101 (Windows 7, PuTTY) и сервером SSH 192.168.56.102 (CentOS 7.6.1810): ошибка соединения



На хосте CentOS выполняем удаленное перенаправление порта

ssh -R 2222:localhost:22 [user@192.168.56.101](mailto:user@192.168.56.101)

Отказ! Правильно, там же нет сервера SSH.

Воспроизвести рассмотренный пример применения расширенного правила, используя основную машину Windows и виртуальную машину CentOS. IP-адреса у вас, естественно, могут отличаться от приведенных в примере.