

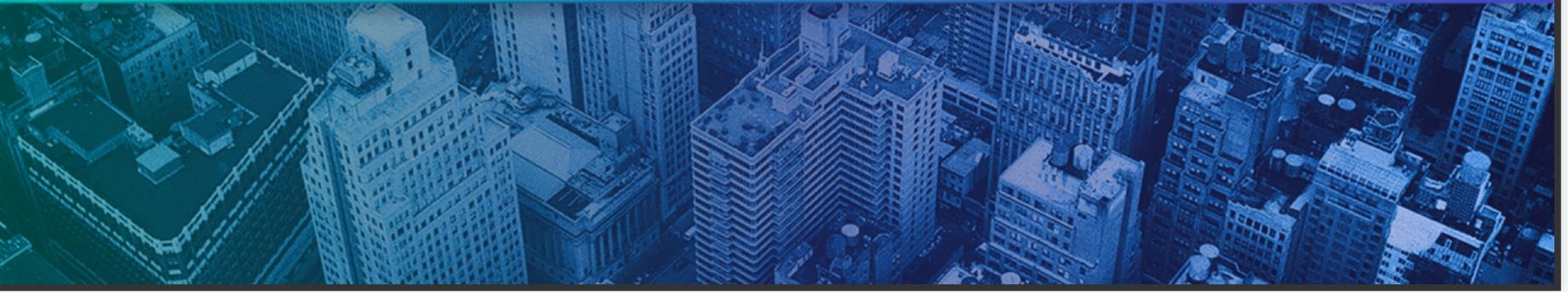


Онлайн-образование



Меня хорошо видно && слышно?

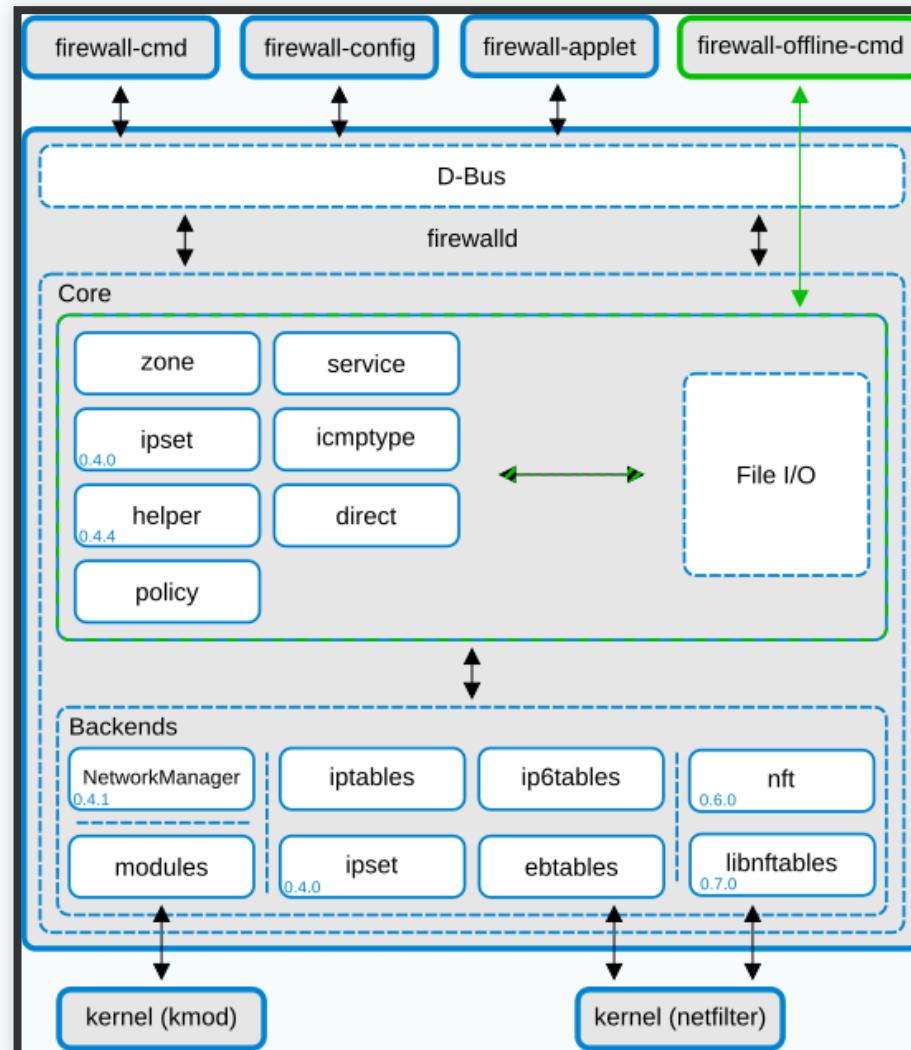
Ставьте  , если все хорошо
Напишите в чат, если есть проблемы



НЕ ЗАБЫТЬ ВКЛЮЧИТЬ
ЗАПИСЬ!!!

Фильтрация трафика. Firewalld.

Firewalld



Зоны

- трафик управляетя через зоны
- Зона может назначаться
 - на интерфейсы
 - на источники трафика (source)
 - на соединения, созданные в NetworkManager
- Один источник трафика либо интерфейс может принадлежать только одной зоне

Общие команды

```
firewall-cmd
  --list-all
  --list-all-zones
  --list-interfaces
  --list-[protocols/protocols/services/rich-rules/sources]
  --get-active-zones
  --get-default-zone
  --get-services/icmptypes/ipset-types/services
  --get-zone-of-interface=<iface_name>
  --get-zones
  --panic-on/off
  --query-panic
```

Общие команды

```
firewall-cmd --state
firewall-cmd --reload
firewall-cmd [--zone=<zone>]
  --add-interface=<interface>
  --add-source=<source/mask>
  --change-interface=<interface>
  --[ add/remove/query ]-service=<service> [ --timeout=<seconds> ]
  --[ add/remove/query ]-port=<port>[-<port>]/<protocol>
    [ --timeout=<seconds> ]
  --[ add/remove/query ]-masquerade
  --[ add/remove/query ]-icmp-block=<icmptype>
  --[ add/remove/query ]-forward-port=port=<port>[-<port>]:proto=<proto>
  {
    :toport=<port>[-<port>] | :toaddr=<address> |
    :toport=<port>[-<port>]:toaddr=<address>
  }
```

Зоны по умолчанию

- trusted – все сетевые соединения разрешены;
- work/home/internal
 - Устанавливается максимальное доверие к компьютерам в сети, разрешается устанавливать только конкретные входящие соединения (по умолчанию SSH и DHCPv6 client, в home и internal плюс MDNS и Samba client);
- dmz
 - Разрешаются только указанные входящие соединения (по умолчанию SSH);
- public
 - для использования в общественных местах, с максимальным недоверием к другим компьютерам, разрешены только конкретные входящие соединения (по умолчанию SSH и DHCPv6 client);

Зоны по умолчанию

- external
 - для роутеров, включег маскарадинг, с максимальным недоверием и четко установленными разрешенными входящими соединениями (по умолчанию SSH);
- block
 - входящие сетевые соединения отклоняются с icmp-host-prohibited сообщением, разрешены только соединения, инициированные в этой системе;
- drop -разрешаются только исходящие соединения, все входящие блокируются.

Работа с зонами

- Описания зон представлены в XML-файлах в
`/usr/lib/firewalld/zones`

```
firewall-cmd --list-all-zones
firewall-cmd --zone=public --list-all
firewall-cmd --get-zones
firewall-cmd --permanent --new-zone=otus
firewall-cmd --get-default-zone
firewall-cmd --get-active-zones
firewall-cmd --get-zone-of-interface=eth0
firewall-cmd --zone=otus --add-source=10.51.21.42/32
firewall-cmd --zone=home --add-interface=eth0 --permanent
firewall-cmd --zone=otus --add-port=8888/tcp
```

Компоненты зоны

- Сервисы
- Порты
- Блоки ICMP
- Маскарадинг
- Проброс портов
- Rich rules

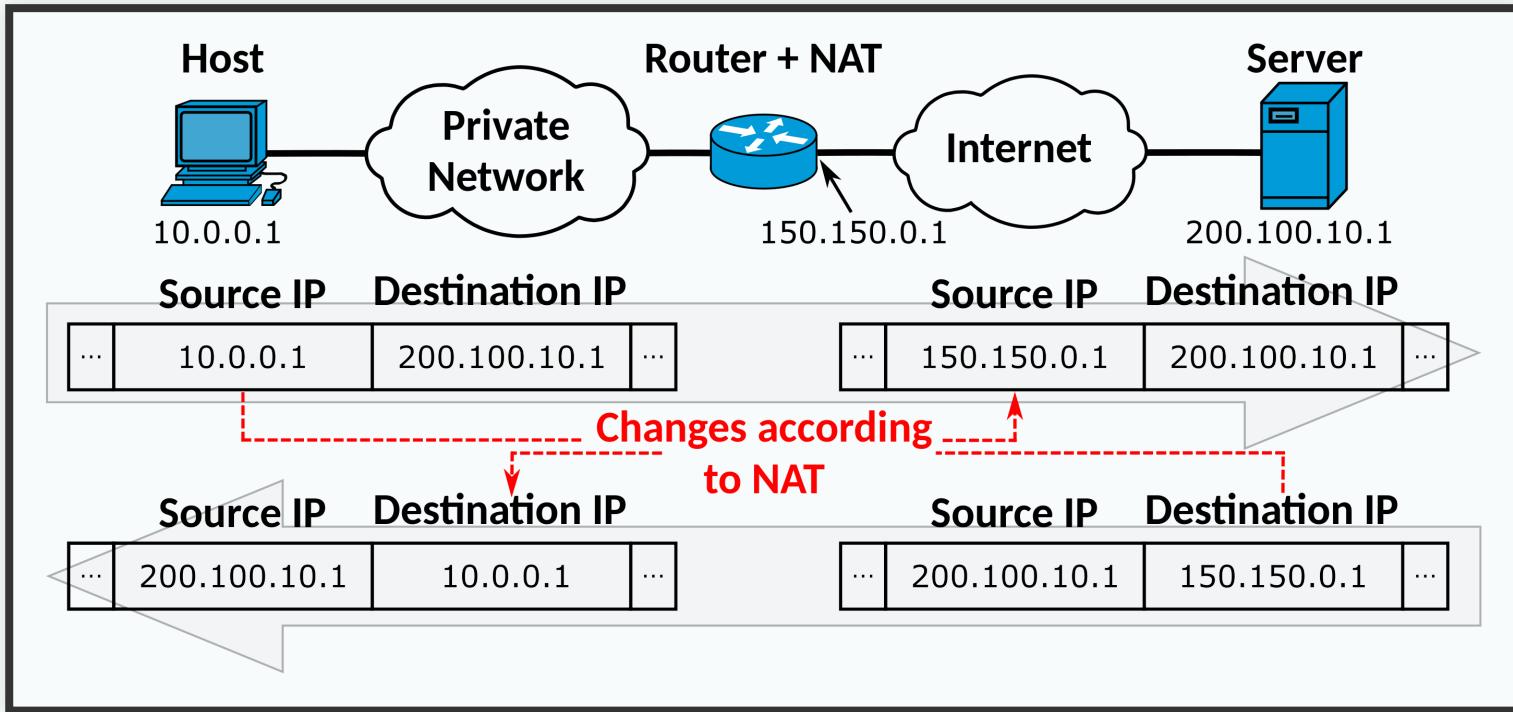
Сервисы и порты

```
firewall-cmd --get-services
firewall-cmd --query-service=nfs3
firewall-cmd --info-service=nfs3
cat /usr/lib/firewalld/services/high-availability.xml
ls /etc/firewalld/services
firewall-cmd --add-service=http
firewall-cmd --zone=otus --add-port=8888/tcp
```

Блоки істр

- `firewall-cmd --get-icmptypes`
- `firewall-cmd --info-icmptype=<icmptype>`
- добавить блокировку
 - `firewall-cmd --add-icmp-block=<icmptype>`
 - `firewall-cmd --query-icmp-block=<icmptype>`
 - `firewall-cmd --remove-icmp-block=<icmptype>`
- заблокировать все
 - `firewall-cmd --add-icmp-block-inversion`
- разрешить избранное
 - `firewall-cmd --add-icmp-block=<icmptype>`

Маскарадинг



Проброс портов

- добавим проброс

```
firewall-cmd --zone=otus \
--add-forward-port=port=2222:proto=tcp:toport=22:toaddr=10.51.2
firewall-cmd --zone=otus \
--query-forward-port=port=2222:proto=tcp:toport=22:toaddr=10.51.2
```

- проверим
- добавим маскарадинг в зону otus
 - `firewall-cmd --zone=otus --add-masquerade`
- проверим
- добавим маскарадинг в паблик зону
 - `firewall-cmd --add-masquerade`

Ipset

```
firewall-cmd --get-ipset-types
firewall-cmd --permanent --new-ipset=test --type=hash:net
firewall-cmd --permanent --info-ipset=test
firewall-cmd --permanent --ipset=test --add-entry=192.168.0.1
firewall-cmd --permanent --ipset=test --get-entries
firewall-cmd --permanent --ipset=test --add-entries-from-file=ipl
firewall-cmd --permanent --zone=drop --add-source=ipset:test
```

Rich rules

```
rule
  [source]
  [destination]
  service|port|protocol|icmp-block|icmp-type|
    masquerade|forward-port|source-port
  [log]
  [audit]
  [accept|reject|drop|mark]
```

Rich rules

- rule
 - rule [family="ipv4|ipv6"] [priority="priority"]
- source
 - source [not] address="address[/mask]" | mac="mac-address" | ipset="ipset"
- destination
 - destination [not] address="address[/mask]"
- service
 - service name="service name"
- port
 - port port="port value" protocol="tcp|udp"
- protocol
 - protocol value="protocol value"

Rich rules

- icmp-block
 - `icmp-block name="icmptype name"`
- forward-port
 - `forward-port port="port value" protocol="tcp|udp"`
`to-port="port value" to-addr="address"`
- source-port
 - `source-port port="port value" protocol="tcp|udp"`
- log
 - `log [prefix="prefix text"] [level="log level"]`
`[limit value="rate/duration"]`
- audit
 - `audit [limit value="rate/duration"]`

Rich rules: actions

- 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"]

Rich rules. Examples

- `firewall-cmd --add-rich-rule rule service name="http" log limit value="1/m" audit accept`
- `firewall-cmd --zone=otus --permanent --add-rich-rule 'rule family="ipv4" source address="10.51.21.42" service name="mysql" accept'`
- `firewall-cmd --add-rich-rule rule family="ipv4" source address="192.168.2.3" reject type="icmp-admin-prohibited"`

Direct

```
firewall-cmd --permanent ...
firewall-cmd --direct
--passthrough { ipv4/ipv6/eb } <args>
--add-chain { ipv4/ipv6/eb } <table> <chain>
--remove-chain { ipv4/ipv6/eb } <table> <chain>
--query-chain { ipv4/ipv6/eb } <table> <chain>
--get-chains { ipv4/ipv6/eb } <table>
--add-rule { ipv4/ipv6/eb } <table> <chain> <priority> <args>
--remove-rule { ipv4/ipv6/eb } <table> <chain> <args>
--query-rule { ipv4/ipv6/eb } <table> <chain> <args>
--get-rules { ipv4/ipv6/eb } <table> <chain>
```

Direct: examples

```
--add-rule ipv4 filter IN_public_allow \
    0 -m tcp -p tcp --dport 666 -j ACCEPT
--get-rules ipv4 filter IN_public_allow
--remove-rule ipv4 filter IN_public_allow \
    0 -m tcp -p tcp --dport 666 -j ACCEPT
```

Рефлексия



Отметьте 3 пункта, которые вам запомнились с вебинара



Что вы будете применять в работе из сегодняшнего вебинара?



Заполните, пожалуйста,
опрос о занятии по ссылке в чате