

Презентация лабораторной работы №13

Фильтр пакетов

Кхари Жекка Кализая Арсе

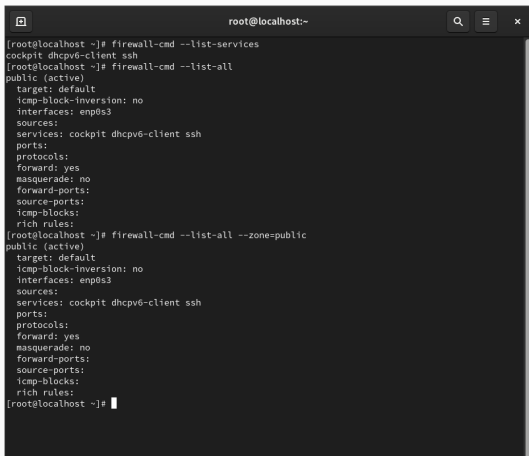
Лабораторная работа

Последовательность выполнения работы

Управление брандмауэром с помощью firewall-cmd

Управление брандмауэром с помощью firewall-cmd

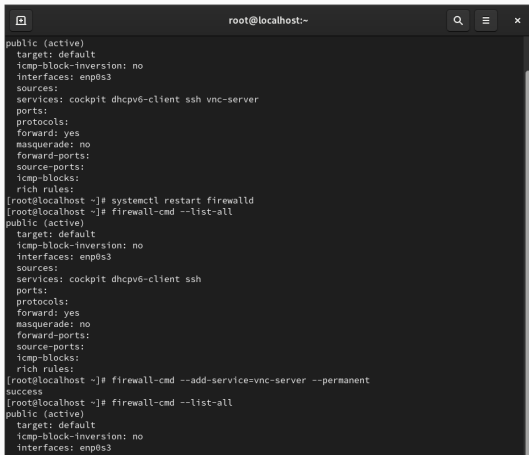
- команды для информации: `firewall-cmd --get-default-zone` `firewall-cmd --get-zones` `firewall-cmd --get-services` `firewall-cmd --list-services` `firewall-cmd --list-all` `firewall-cmd --list-all --zone=public`



```
root@localhost:~  
[root@localhost ~]# firewall-cmd --list-services  
cockpit dhcpv6-client ssh  
[root@localhost ~]# firewall-cmd --list-all  
public (active)  
  target: default  
  icmp-block-inversion: no  
  interfaces: enp0s3  
  sources:  
  services: cockpit dhcpv6-client ssh  
  ports:  
  protocols:  
  forward: yes  
  masquerade: no  
  forward-ports:  
  source-ports:  
  icmp-blocks:  
  rich rules:  
[root@localhost ~]# firewall-cmd --list-all --zone=public  
public (active)  
  target: default  
  icmp-block-inversion: no  
  interfaces: enp0s3  
  sources:  
  services: cockpit dhcpv6-client ssh  
  ports:  
  protocols:  
  forward: yes  
  masquerade: no  
  forward-ports:  
  source-ports:  
  icmp-blocks:  
  rich rules:  
[root@localhost ~]#
```

Управление брандмауэром с помощью firewall-cmd

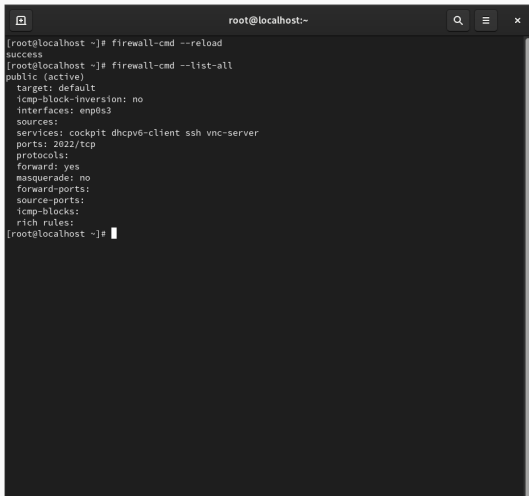
- команды: `firewall-cmd --add-service=vnc-server` `firewall-cmd --list-all`
`systemctl restart firewalld` `firewall-cmd --list-all` `firewall-cmd --add-service=vnc-server --permanent` `firewall-cmd --list-all`



```
root@localhost:~  
public (active)  
target: default  
icmp-block-inversion: no  
interfaces: enp0s3  
sources:  
services: cockpit dhcpv6-client ssh vnc-server  
ports:  
protocols:  
forward: yes  
masquerade: no  
forward-ports:  
source-ports:  
icmp-blocks:  
rich rules:  
[root@localhost ~]# systemctl restart firewalld  
[root@localhost ~]# firewall-cmd --list-all  
public (active)  
target: default  
icmp-block-inversion: no  
interfaces: enp0s3  
sources:  
services: cockpit dhcpv6-client ssh  
ports:  
protocols:  
forward: yes  
masquerade: no  
forward-ports:  
source-ports:  
icmp-blocks:  
rich rules:  
[root@localhost ~]# firewall-cmd --add-service=vnc-server --permanent  
success  
[root@localhost ~]# firewall-cmd --list-all  
public (active)  
target: default  
icmp-block-inversion: no  
interfaces: enp0s3
```

Управление брандмауэром с помощью firewall-cmd

- команды: `firewall-cmd --reload` `firewall-cmd --list-all`
`--add-port=2022/tcp --permanent` `firewall-cmd --reload` `firewall-cmd --list-all`

A terminal window titled 'root@localhost:~' with search, menu, and close icons. It shows the execution of 'firewall-cmd --reload' which returns 'success', followed by 'firewall-cmd --list-all' which displays the current firewall configuration. The configuration includes: target: default, icmp-block-inversion: no, interfaces: enp0s3, sources: (empty), services: cockpit dhcpv6-client ssh vnc-server, ports: 2022/tcp, protocols: (empty), forward: yes, masquerade: no, forward-ports: (empty), source-ports: (empty), icmp-blocks: (empty), and rich rules: (empty).

```
root@localhost:~  
[root@localhost ~]# firewall-cmd --reload  
success  
[root@localhost ~]# firewall-cmd --list-all  
public (active)  
target: default  
icmp-block-inversion: no  
interfaces: enp0s3  
sources:  
services: cockpit dhcpv6-client ssh vnc-server  
ports: 2022/tcp  
protocols:  
forward: yes  
masquerade: no  
forward-ports:  
source-ports:  
icmp-blocks:  
rich rules:  
[root@localhost ~]#
```

Управление брандмауэром с помощью firewall-config

Управление брандмауэром с помощью firewall-config

- КОМАНДЫ:

firewall-config firewall-cmd --list-all firewall-cmd --reload firewall-cmd --list-all

The screenshot displays a Linux desktop environment. In the foreground, the 'Firewall Configuration' window is open, showing the 'Services' tab. The 'public' service is selected in the 'Sources' list. Below the 'Services' list, there is a section for 'Service' with checkboxes for various services like 'afp', 'amanda-client', 'amanda-k5-client', 'amqp', 'amqps', 'apcupsd', 'audit', 'ausweisapp2', 'bacula', and 'bacula-client'. The 'public' service is highlighted. In the background, a terminal window shows the command 'firewall-config' being executed, and a web browser window displays a page titled 'Управление брандмауэром с помощью firewall-config'.

Управление брандмауэром с помощью firewall-config

В терминале и под учетной записью своего пользователя запустите интерфейс firewall-config:

```
firewall-config
```

Если система предлагает вам её установить. Также при запуске будет предложено ввести пароль пользователя с полномочиями управления этой службой.

Появится меню рядом с параметром (Configuration). Откройте раскрывающийся список и выберите (Personal). Это позволит сделать постоянными все настройки, которые вы вносите при конфигурировании.

В появившемся окне (Public) и на этой вкладке нажмите (Add). Введите порт 2022 и протокол (tcp), чтобы добавить их в список.

После этого нажмите (Apply) и на этой вкладке нажмите (Add). Введите порт 2022 и протокол (tcp), чтобы добавить их в список.

В терминале введите:

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

Обратите внимание, что изменения, которые вы только что внесли, ещё не вступили в силу. Это связано с тем, что вы настроили их как постоянные изменения, а не как временные.

Введите конфигурацию firewall-cmd:

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

или доступными сервисами:

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

После этого изменения будут применены.

Итоговая работа

Введите конфигурацию межсетевого экрана, которая позволяет получить доступ к службам:

```
firewall-cmd --set-active
```

и в командной строке (для службы telnet), так и в графическом интерфейсе (для служб ftp, port, smtp).

3. Убедитесь, что конфигурация является постоянной и будет активирована после перезагрузки компьютера.

13.6. Содержание отчёта