Отчет по лабораторной работе №13

Отчет о выполнении лабораторной работы по управлению брандмауэром с помощью firewall-cmd

Лупупа Чилеше

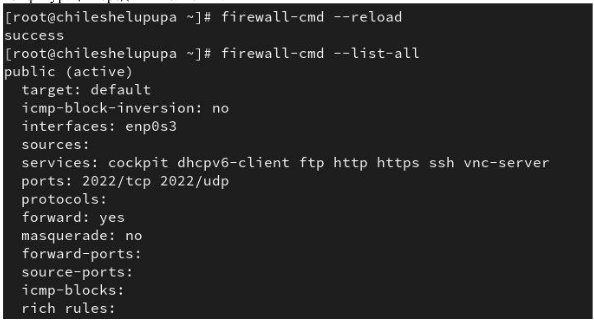
Содержание

# 1 Цель работы

Получить навыки настройки пакетного фильтра в Linux. Целью этой лабораторной работы было понять и попрактиковаться в управлении брандмауэром Linux с помощью утилиты firewall-cmd. Это включало проверку конфигураций, изменение правил и понимание различий между динамическими и постоянными конфигурациями.

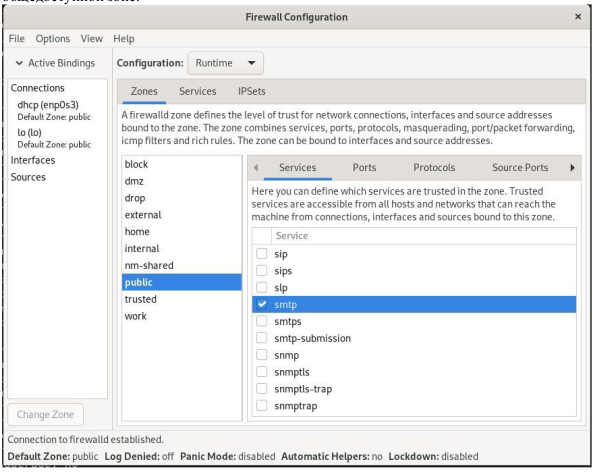
# 2 Управление брандмауэром с помощью firewall-cmd

**Получение административных привилегий:** - Command: su – - Успешно переключился на пользователя root. Этот шаг обеспечил нам наличие необходимых разрешений для управления брандмауэром. **Определение зоны по умолчанию:** Команда: firewall-cmd –get-default-zone - Вывод: была отображена зона по умолчанию (например, «публичная»). - На этом этапе проверялась зона, которую система использует для неуправляемых подключений.



**Список доступных зон:**

* Команда: firewall-cmd –get-zones
* Вывод: был отображен список зон (например, «блокировать dmz, удалить внешний дом, внутреннюю общедоступную доверенную работу»)
* Подтверждены зоны, доступные для настройки сетевых интерфейсов

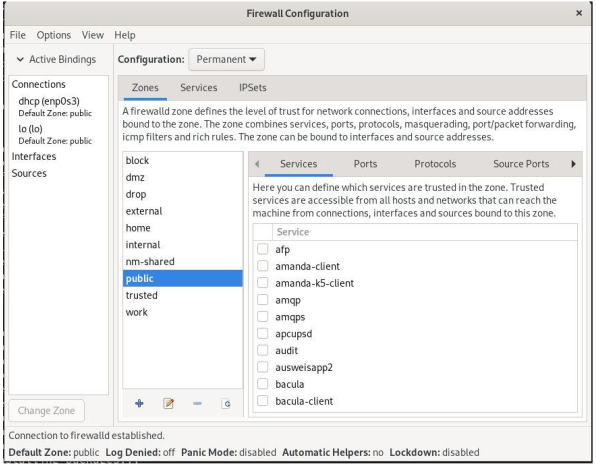


**Просмотр доступных услуг:**

* Команда: firewall-cmd –get-services
* Вывод: отобразился список предопределенных служб, которыми можно управлять с помощью брандмауэра.
* Это было важно для понимания спектра сервисов, поддерживаемых firewalld.

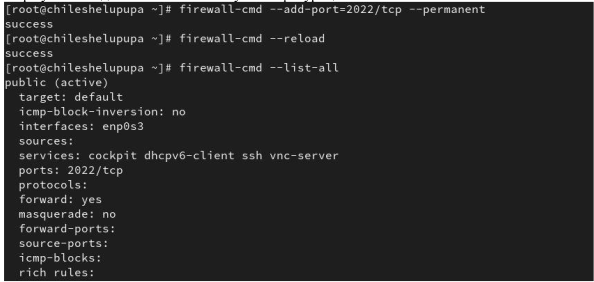
**Листинговые услуги в текущей зоне:**

* Команда: firewall-cmd –list-services
* Вывод: список активных служб в текущей зоне по умолчанию.
* Проверено, какие службы уже разрешены через брандмауэр.



**Сравнение результатов команд –list-all:**

* Команды: firewall-cmd –list-all и firewall-cmd –list-all –zone=public
* Вывод: обе команды отображали аналогичную информацию, показывая активные службы, порты и интерфейсы для «общедоступной» зоны.
* Это продемонстрировало, как просмотреть подробные сведения о конфигурациях брандмауэра для конкретных зон.



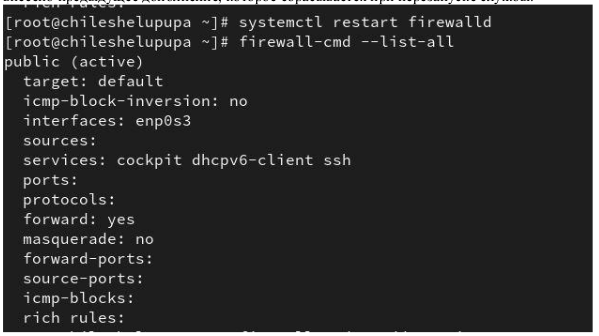


**Добавление службы VNC-сервера:**

* Команда: firewall-cmd –add-service=vnc-server
* Команда выполнена успешно. Служба vnc-сервера была добавлена в конфигурацию среды выполнения.

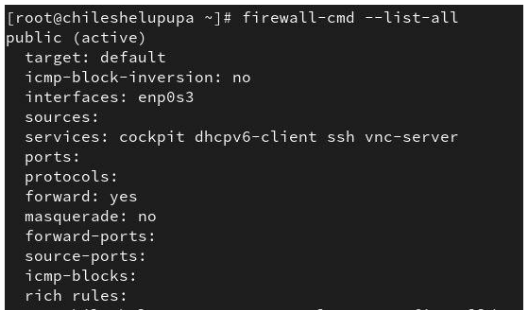
fig:

**Проверка добавления VNC-сервера:** - Команда: firewall-cmd –list-all - Вывод: подтверждено, что служба vnc-сервера указана в списке активных служб.



**Перезапускаем firewalld:**

* Команда: systemctl перезапустить firewalld
* Служба firewalld успешно перезапущена.
* Команда: firewall-cmd –list-all
* Вывод: служба vnc-сервера больше не отображается.
* Объяснение: Это произошло потому, что в конфигурацию среды выполнения было внесено предыдущее дополнение, которое сбрасывается при перезапуске службы.



**Перезагрузка конфигурации firewalld:** - Команды: firewall-cmd –reload и firewall-cmd –list-all - Вывод: После перезагрузки в рантайм-конфигурации появился сервис vnc-сервера. - Этот шаг подчеркнул необходимость перезагрузки firewalld, чтобы постоянные изменения вступили в силу.

**Добавление TCP-порта 2022 в постоянную конфигурацию:**

* Команда: firewall-cmd –add-port=2022/tcp –permanent
* Порт успешно добавлен в постоянную конфигурацию.

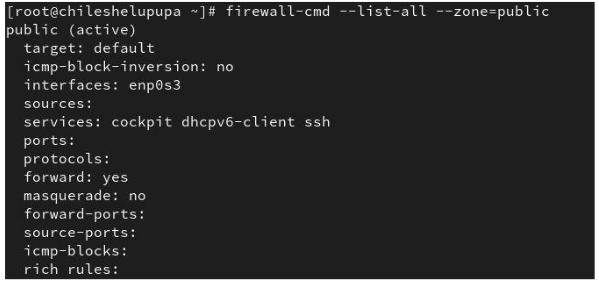
 - Это подтвердило, что порт был правильно добавлен и активен как во время выполнения, так и в постоянной конфигурации.

# 3 Управление брандмауэром с помощью firewall-config

**Запускаем конфигурацию брандмауэра**

**Команда:** firewall-config

**Объяснение:** Команда firewall-config запускает графический интерфейс пользователя (GUI) для управления брандмауэром. Этот интерфейс упрощает процесс настройки. Если инструмент firewall-config не установлен, система предложит пользователю установить его. Для управления брандмауэром необходимы права администратора, поэтому пользователь должен указать пароль root.



**Переключиться на постоянную конфигурацию**

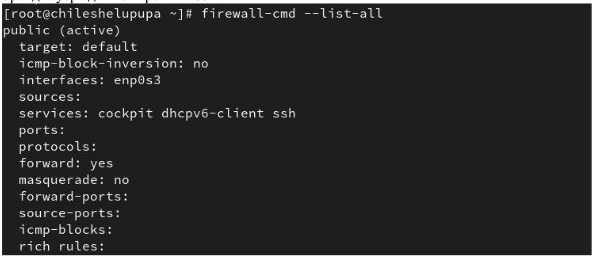
**Действие:** выберите «Постоянно» в раскрывающемся меню «Конфигурация».

**Объяснение:** Параметр конфигурации определяет, будут ли изменения применяться временно (во время выполнения) или постоянно. Если выбрать «Постоянно», любые внесенные изменения сохранятся даже после перезагрузки системы. Это гарантирует, что правила брандмауэра остаются согласованными и их не нужно повторно применять вручную.

**Включите службы HTTP, HTTPS и FTP**

**Действие:** В “общедоступной” зоне включите службы http, https и ftp.

**Пояснение:** Зоны в брандмауэре определяют уровень доверия для сетевых подключений. “Общедоступная” зона обычно используется для ненадежных сетей, таких как Интернет. Включив эти службы, брандмауэр разрешает входящие подключения для веб-трафика (HTTP/HTTPS) и передачи файлов (FTP) в общедоступной зоне.



**Проверьте текущую конфигурацию брандмауэра**

**Команда:** firewall-cmd –list-all

**Пояснение:** Эта команда отображает текущую конфигурацию брандмауэра, включая активные зоны, разрешенные службы, порты и протоколы. Поскольку изменения были внесены в постоянную конфигурацию, они еще не отражены в конфигурации среды выполнения.

fig:

## 3.1 Вывод

Заключение Лабораторная работа позволила получить практический опыт работы с firewall-cmd и лучше понять правила управления брандмауэром в системе Linux. Различие между конфигурациями во время выполнения и постоянными конфигурациями и их соответствующими вариантами использования является фундаментальной концепцией, обеспечивающей эффективное управление брандмауэром. В этой лабораторной работе было продемонстрировано, как настроить брандмауэр с помощью графического интерфейса firewall-config. Благодаря включению определенных служб, добавлению портов и внесению изменений сетевая безопасность системы была адаптирована к конкретным требованиям. Различие между конфигурациями во время выполнения и постоянными конфигурациями обеспечивает гибкость и контроль над настройками брандмауэра.