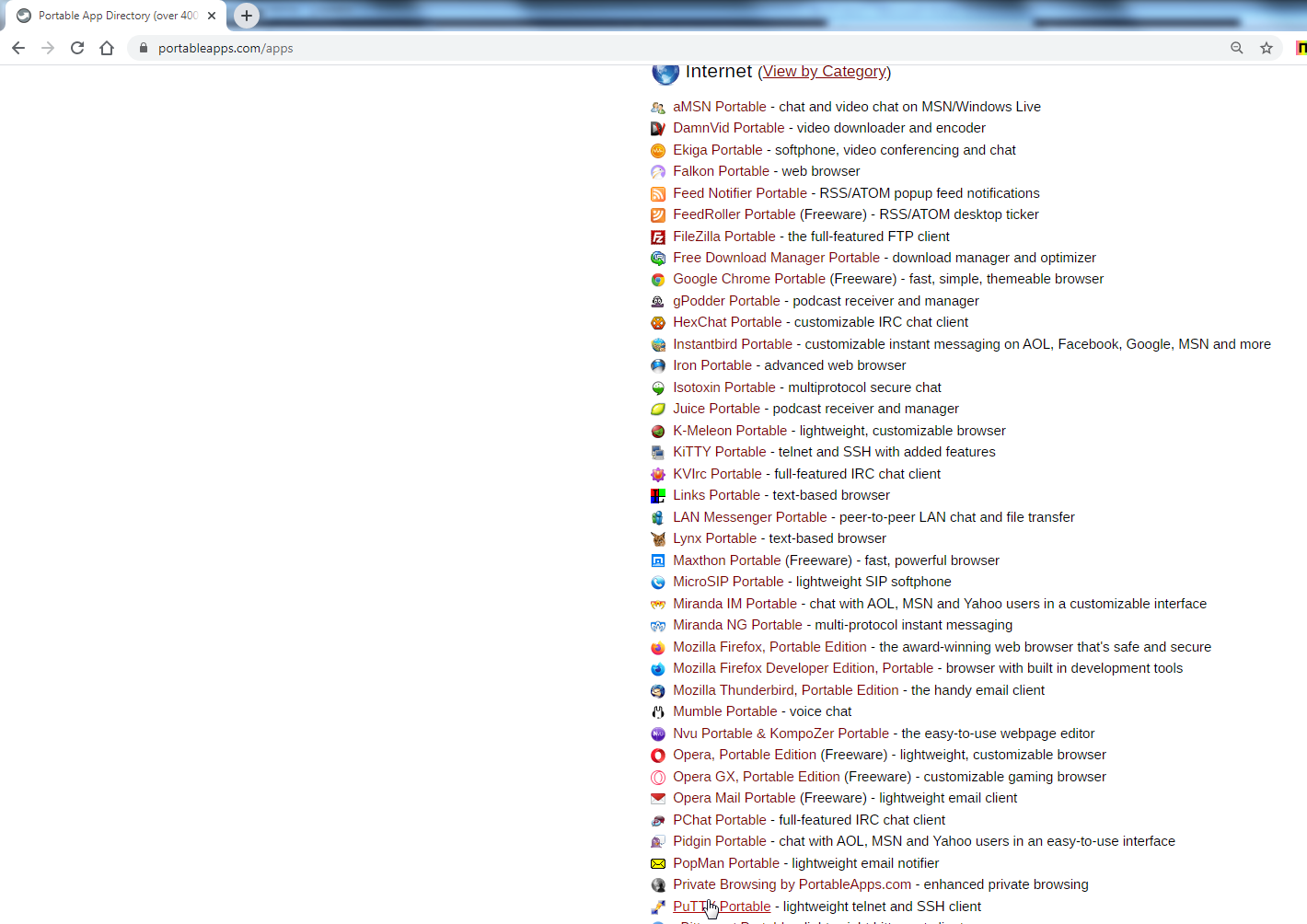
# Занятие 6-7. Лабораторная работа 3. Организация межсетевого экрана firewalld в Linux.

Сетевым экраном по умолчанию для ОС CentOS 7 является сетевой экран **firewalld**. Задача данной лабораторной работы — выполнить настройку сетевого экрана **firewalld**.

Приведенный ниже материал более подробно изложен в файле [**"Настройка сетевого экрана firewalld в CentOS 7.docx"**](Настройка%20сетевого%20экрана%20firewalld%20в%20CentOS%207.docx). Начните работу с его изучения. Выполните все примеры, приведенные в этом документе.

Для выполнения упражнений и задания лабораторной работы предполагается использование программы **PuTTY**. Эта программа является клиентом для различных протоколов удалённого доступа: SSH, Telnet, rlogin. Переносимую версию PuTTY для ОС Windows (файл **PuTTYPortable\_0.74\_English.paf.exe**) можно скачать по адресу <https://portableapps.com/apps>:



Запустите указанный файл и укажите место для установки программы. Установка программы не требует полномочий администратора и может быть выполнена в любое удобное место, в том числе на съемном носителе.

## Основные понятия.

Служба **firewalld** основывается на понятии ***зоны***.

**Зона** определяет уровень доверия к подключению. Каждая зона содержит определённый набор правил, в соответствии с которыми и работает подключение. Зоны присваиваются сетевым интерфейсам и управляют поведением брандмауэра. Компьютеры, которые часто подключаются к разным сетям (например, ноутбуки) могут использовать зоны, чтобы изменять наборы правил в зависимости от среды. Например, при подключении к общественной сети Wi-Fi брандмауэр может применять более строгие правила, а в домашней сети — менее строгие.

Администратор имеет возможность создавать собственные зоны с нужными правилами фильтрации, имеет возможность модифицировать уже существующие зоны. При необходимости, все сделанные изменения можно отменить, выполнив откат до состояния по умолчанию.

Использование зон особенно важно на серверах с несколькими сетевыми интерфейсами, поскольку для разных сетевых адаптеров можно назначить разные по строгости правила.

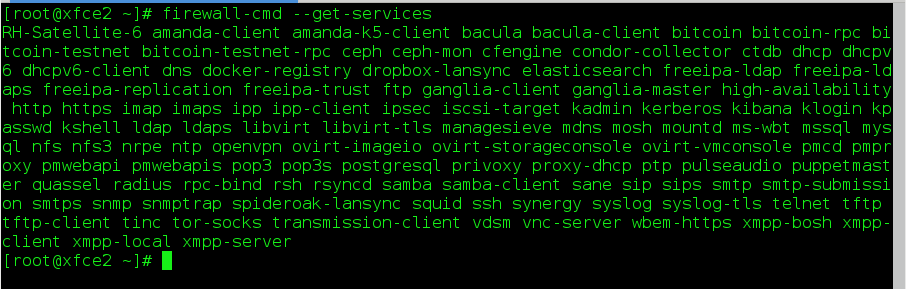
На серверах, имеющих только один сетевой интерфейс, можно ограничиться одной зоной, которая является зоной по умолчанию. Для каждого пакета, поступающего в систему, определяется его адрес отправителя и на основе этого исходного адреса **firewalld** определяет, принадлежит ли пакет определенной зоне. Если это не так, используется зона для входящего сетевого интерфейса. Если какая-либо конкретная зона недоступна, пакет обрабатывается настройками в зоне по умолчанию.

Второе важное понятие в **firewalld** — это **служба (сервис)**. В **firewalld** определены некоторые службы по умолчанию, что позволяет администраторам легко разрешать или запрещать доступ к определенным портам на сервере.

С каждым сервисом связан файл конфигурации, в котором объясняется, какие порты UDP или TCP задействованы, и если требуется, какие модули ядра должны быть загружены. Файлы конфигурации сервисов хранятся в каталоге **/usr/lib/firewalld/services** или **/etc/firewalld/services**.

Чтобы получить список всех доступных на компьютере сервисов **firewalld**, следует выполнить команду

firewall-cmd --get-services



По сути, работа с **firewalld** сводится к тому, чтобы нужные сервисы добавить в нужные зоны. В особых случаях конфигурация может быть улучшена более конкретными настройками.

## Средства управления конфигурацией сетевого экрана

Управление брандмауэром **firewalld** осуществляется с помощью инструмента командной строки **firewall-cmd** или графического инструмента конфигурации **firewall-config** (требуется установка с помощью **yum**).

При работе с любым из этих инструментов важно помнить, где именно сделаны изменения. Оба инструмента могут работать с конфигурацией, хранящейся в оперативной памяти и с конфигурацией, хранящейся на диске (постоянная конфигурация). При внесении изменений в конфигурацию с помощью любого из этих инструментов не забудьте зафиксировать изменения на диске. Сначала выполняется команда, создающая временные изменения в текущей конфигурации сетевого экрана **firewalld**. Затем проводится тестирование работы брандмауэра после сделанных изменений. Если сетевой экран работает, как предполагалось, команда выполняется повторно с дополнительным флагом **--permanent**. Команды **firewall-cmd** применяют флаг **--permanent** для сохранения сделанных изменений.

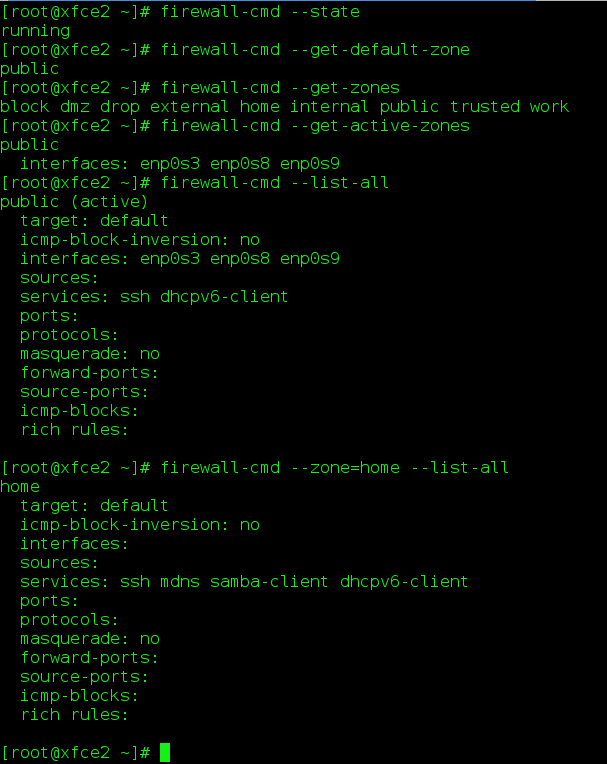
**Внимание**. Для настройки сетевого экрана **firewalld** нельзя использовать команду **iptables**, т.к. использование **iptables** может сильно испортить существующую конфигурацию брандмауэра, особенно если служба **iptables** запускается в системе, в которой уже запущена служба **firewalld**. Чтобы убедиться, что этого никогда не произойдет, используйте команду

systemctl mask iptables

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

### Команда firewall-cmd

|  |  |  |
| --- | --- | --- |
| **Команда** | **Описание** | |
| **Работа с зонами** | | |
| firewall-cmd --state | Проверить состояние **firewalld**. | |
| firewall-cmd --get-default-zone | Проверяем зону по умолчанию. | |
| firewall-cmd --set-default-zone=home | Устанавливаем зону **home** зоной по умолчанию. | |
| firewall-cmd --get-zones | Получаем список зон. | |
| firewall-cmd --get-active-zones | Получаем список задействованных зон. | |
| firewall-cmd --list-all | Вывести правила для текущей зоны. | |
| firewall-cmd --zone=home --list-all | Вывести правила для определённой зоны (**home**). | |
| firewall-cmd --zone=home --change-interface=enp0s8 | Временный (до конца сеанса работы) перевод интерфейса **enp0s8** в зону **home** | |
| **Работа с портами** | | |
| firewall-cmd --list-ports | | Вывести список всех добавленных портов. |
| firewall-cmd --permanent --zone=public --add-port=2222/tcp | | Открываем порт. |
| firewall-cmd --permanent --zone=public --remove-port=2222/tcp | | Закрываем порт. |
| firewall-cmd --permanent --zone=public --add-port=2222-3333/tcp | | Открываем диапазон портов. |
| **Работа с сервисами** | | |
| firewall-cmd --get-services | Вывести все доступные сервисы | |
| firewall-cmd --zone=public --add-service=http | Временно (до конца сеанса) включить поддержку сервиса **http** в зоне **public** | |
| firewall-cmd --add-service=http | Временно (до конца сеанса) включить поддержку сервиса **http** в зоне по умолчанию | |
| firewall-cmd --zone=public --permanent --add-service=http | Включить поддержку сервиса **http** в зоне **public** на постоянной основе | |
| firewall-cmd --zone=public --permanent --list-services | Вывести список правил, действующих на постоянной основе в зоне **public**. | |



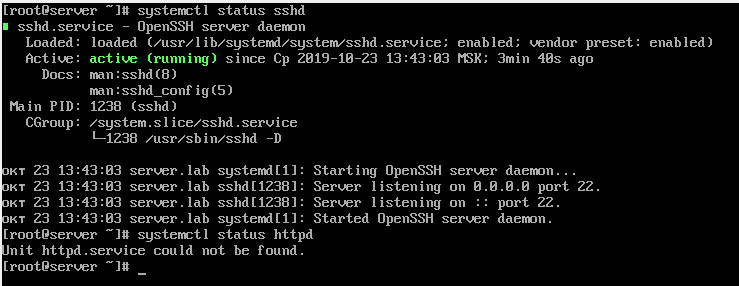
## Задание. Настройка межсетевого экрана firewalld

1. Проверить, какой брандмауэр работает в системе — **firewalld** или **iptables** (команда **systemctl**).

Если используется брандмауэр **iptables**:

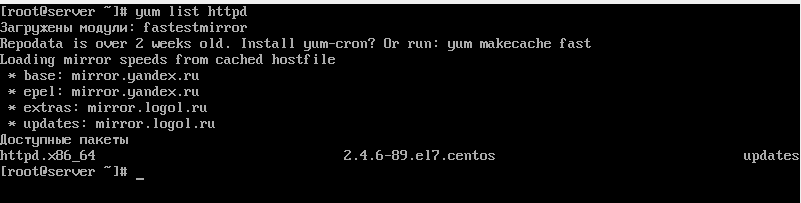
* останавливаем его (команда **systemctl**),
* предохраняемся от случайного запуска (systemctl mask iptables)
* запускаем брандмауэр **firewalld** (команда **systemctl**)
* и проверяем, что он работает (команда **systemctl**, команда **firewall-cmd**)

1. Вывести список доступных зон.
2. Вывести список активных зон.
3. Вывести имя зоны, используемой по умолчанию.
4. Вывести правила для зоны по умолчанию.
5. Вывести правила для всех остальных зон. Сравнить их.
6. Вывести список всех доступных сервисов.
7. Проверить, запущены ли демоны **sshd** (сервер SSH) и **httpd** (web-сервер):



В данном примере сервер SSH (**sshd**) выполняется, а web-сервер (**httpd**) даже не установлен.

Найти в доступных репозиториях пакет **httpd**:



Установить пакет **httpd**:

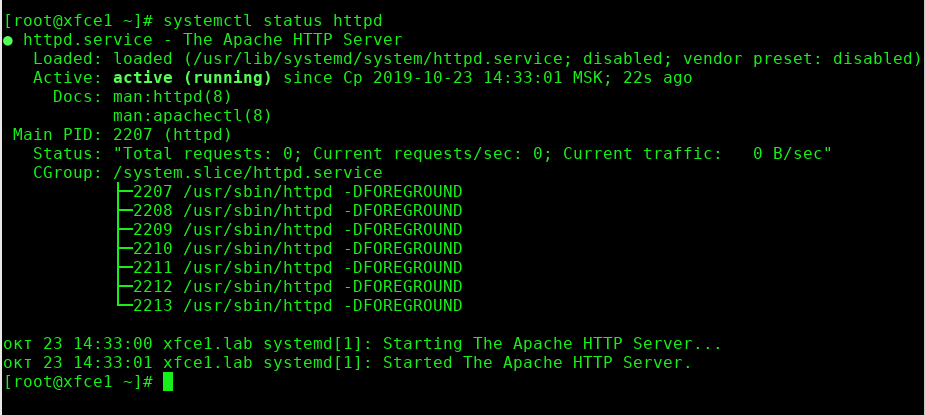
yum –y install httpd

Запустить web-сервер:

systemctl start httpd

Проверить состояние службы httpd:

systemctl status httpd



1. Временно (до конца сеанса) включить поддержку сервиса **http** в зоне по умолчанию.
2. Убедиться, что сервисы **ssh** и **http** открыты для входящих соединений. Для этого в ОС Windows
   * запустить браузер и установить в нем соединение с web-сервером, работающим в CentOS. Для подключения в строке адреса указать определенный ранее IP-адрес сетевого интерфейса CentOS, работающего в режиме **Виртуальный адаптер хоста**;
   * запустить приложение **PuTTY** и подключиться к указанному IP-адресу по протоколу SSH.
3. **Составить отчет о проделанной работе. Указать, какие пункты задания выполнены, и какие команды при этом использовались. Отчет может быть проиллюстрирован скриншотами.**