Дипломное задание по курсу «Системный администратор»

- вам предстоит установить две виртуальные машины
- сконфигурировать на них сеть
- запустить сервисы и настроить firewall
- имплементировать скрипт локального резервного копирования
- автоматизировать его запуск

Примечание:

Формулировки задания предполагают, что вы используете дистрибутив на основе Red Hat, например, CentOS Stream или Rocky Linux. Но вы можете использовать любой другой дистрибутив. В этом случае часть пунктов придётся адаптировать.

Задание

Если вы работаете с виртуальными машинами в облаке, можно пропустить пункты по конфигурации сетевых интерфейсов и использовать адреса, которые выдал провайдер!

1. Создайте две виртуальные машины: **frontend1** и **backend1**.
2. Настройте в VirtualBox Host only адаптер на обеих виртуальных машинах (аналогично заданию по firewall).
3. Добавьте интерфейс bridge на **обе машины**.
4. Установите на обе виртуальные машины Linux. Задайте им соответствующие хостнеймы: **frontend1** и **backend1**.
5. Установите на **обе машины** nginx и отключите firewalld, libvirtd и SELinux.

```
sudo systemctl disable --now firewalld libvirtd; sudo setenforce 0
sudo tee /etc/selinux/config <<< 'SELINUX=disabled'
```

6. Удалите интерфейс bridge с **backend1**.
7. Сконфигурируйте статические адреса на Host only интерфейсах (на bridge получите автоматически). Пропишите эти настройки в конфигурационных файлах вашего дистрибутива так, чтобы после перезагрузки настройки интерфейсов применялись. (Используйте специфичный для дистрибутива механизм, например NetworkManager.)
    - **frontend1** - **172.16.0.11/24**
    - **backend1** - **172.16.0.22/24**
8. Сконфигурируйте на **backend1** `nginx`, заменив содержимое `/etc/nginx/nginx.conf` следующим ниже, запустите сервис.

```
user nginx;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;

events { worker_connections 768; }

http {
    server {
        listen 8080;
        server_name _;
        default_type text/html;

        location / {
            return 200
            "<html>\nCurrent time: $time_iso8601<br/>\n
            Connection from: $remote_addr\n</html>";
        }
    }
}
```

9. Сгенерируйте на **frontend1** ssl ключ `/etc/nginx/key.pem` и самоподписной ssl-сертификат `/etc/nginx/cert.pem`, при чём в поле commonName укажите хостнейм вашего фронтенда (аналогично сертификату из задания по http/https).
10. Настройте на **frontend1** `nginx`, включив `proxy_pass` на `172.16.0.22:8080`, при чём так, чтобы `nginx` на **frontend1** слушал порт 443 и использовал ssl-шифрование. Используйте сертификат и ключ, сгенерированные на прошлом шаге. (Содержимое секции `server {}` нужно написать самостоятельно.) Проверить конфигурацию, не запуская сервер, можно с помощью команды `nginx -t`. Она сообщит не только о наличии ошибок, но и укажет строки, которые не смогла интерпретировать. Запустите сервис.

```
user nginx;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;

events { worker_connections 768; }

http {
    server {
        ...
    }
}
```

11. Настройте с помощью `iptables` firewall на **frontend1** так, чтобы он пропускал tcp соединения только на 443 и 22 порт, а также позволял устанавливать исходящие соединения. На **backend1** firewall настраивать не нужно: считаем внутреннюю сеть безопасной. Сохраните конфигурацию так, чтобы после перезагрузки виртуальной машины она снова была применена.
12. Откройте с хостовой машины https://*frontend1*/ (используйте IP адрес bridge интерфейса) и убедитесь, что проксирование работает, а в строке `Frontend:` отображается адрес виртуальной машины **frontend1**.

    Браузер может предупреждение о невалидном сертификате — это нормально, поскольку мы используем созданный нами самоподписной сертификат. Предупреждение нужно пропустить и согласиться на риски, после этого страница откроется.

13. Напишите скрипт `/usr/local/sbin/www_backup` для резервного копирования содержимого директории `/var/www` на сервере **backend1** в архив `/srv/backup/YYYY-MM-DD_www.tar.gz`, где YYYY-MM-DD - дата запуска скрипта. Напишите строку в crontab пользователя `root`, чтобы запускать этот скрипт раз в сутки, в 2 часа ночи. Убедитесь, что скрипт работает – запустите его. (Оставлять виртуальную машину работать до утра не обязательно, достаточно одного ручного запуска. :)

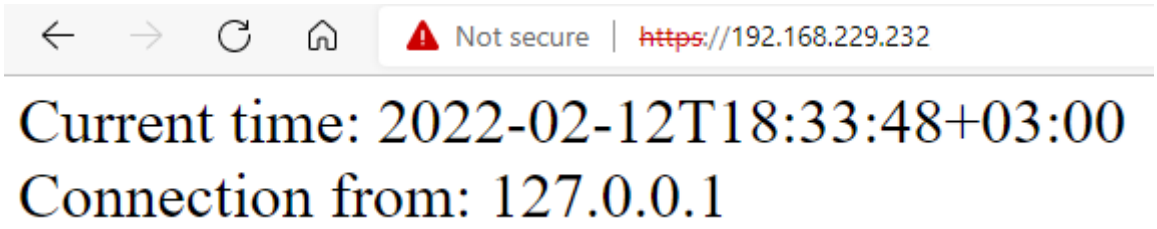
Как сдавать

После установки и настройки виртуальных машин обе необходимо перезагрузить, и только после этого делать скриншоты для задания. Если что-то не работает, нужно исправить конфигурацию и перезагрузить машину, то есть убедиться, что после перезагрузки всё продолжит работать.

В качестве решения пришлите скриншоты терминала с выводом следующих команд:

- на обеих виртуальных машинах:
  - `ip -br -4 addr`
- на **frontend1**:
  - `cat /etc/nginx/nginx.conf`
  - `openssl x509 -noout -issuer -subject -dates -in /etc/nginx/cert.pem`
  - `iptables-save`
- на **backend1**:
  - `cat /usr/local/sbin/www_backup`
  - `sudo crontab -l`
  - `ls -l /srv/backup`

А также скриншот веб-браузера на вашей хостовой машине с открытой страницей **https://<ip адрес frontend1>**, достаточно текста страницы и куска адресной строки с протоколом и значком, предупреждающем о небезопасном https соединении, например:



Connection from должен показывать адрес frontend1.

Убедительная просьба прилагать к работе скриншоты отдельными файлами и не использовать слишком мелкие шрифты. Допускается открытие сайта с одной из виртуальных машин с помощью текстового браузера или `curl`, если нет возможности использовать bridge интерфейс и / или браузер в хостовой машине.