

Лабораторная 8.

Развертывание nDPI

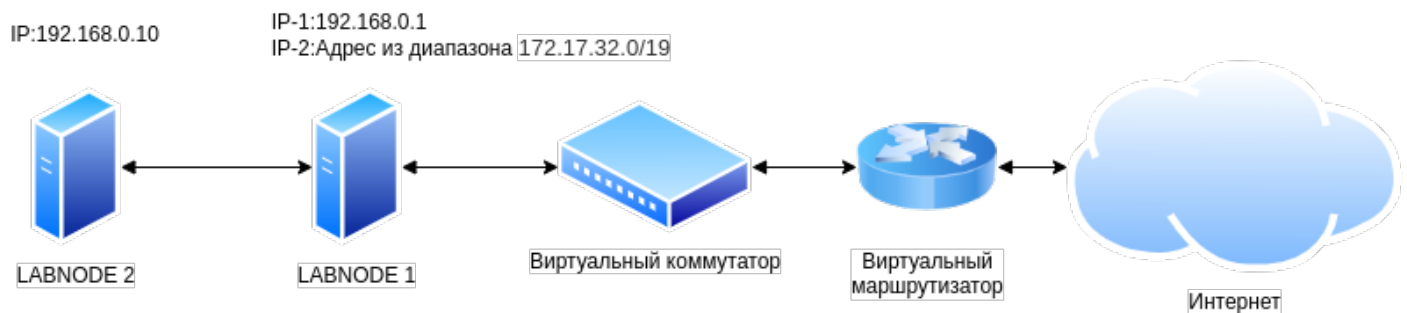
Цель:

Получение базовых навыков работы в настройке программной АТС Asterisk.

Задачи:

1. Подключится к облачной платформе СПбГУТ
2. Добавить репозитории ntop
3. Установить пакеты nDPI
4. Отловить трафик пользователей по приложению

Схема виртуального стенда:



Ход работы:

Переходим на **Labnode1**

1. Настройка репозитория

```
cp /var/lib/cloud/s3cfg .s3cfg
s3cmd get s3://dpi/ntop.deb
sudo apt install ./ntop.deb -y
```

2. Обновляем локальные индексы пакетов

```
sudo apt update
```

3. Устанавливаем пакеты nDPI

```
sudo apt install pfring-dkms nprobe ntopng n2disk centos -y
```

4. Запускаем ntopng и добавляем в автозапуск

```
sudo systemctl enable ntopng --now
```

5. Переходим в веб-интерфейс dpi

6. Перейти в браузер по адресу [ip адрес из сети 172.17.32.0/19]:3000

7. Авторизуйтесь

Логин	Пароль
admin	admin

0. После авторизации потребуется сменить пароль, приведите к виду

Логин	Пароль
admin	labpass1!

0. Авторизуйтесь в Linphone

1. Найдете в веб интерфейсе SIP трафик
2. Снимите трафик за 1 минуту

Вопросы:

1. Какие функциональные возможности есть у nDPI?
2. Что необходимо сделать, чтобы увидеть проходящий через nDPI сетевой трафик?
3. Как возможно изменять политику обслуживания пользователей?
4. Какие есть способы добавить свою сигнатуру в nDPI

Версия #19

Тарабанов Илья Федорович создал 1 сентября 2022 11:11:13

Тарабанов Илья Федорович обновил 14 ноября 2023 15:16:46