Тема: Настройка OpenVPN на Astra Linux

Цель работы: получить навык настройки vpn-туннеля с помощью графического режима утилиты Open VPN с использованием официальной документации.

Теоретические сведения:

1. Что такое OpenVPN?

OpenVPN — это свободное и широко распространённое программное обеспечение для создания защищённых VPN-соединений (виртуальных частных сетей). Оно позволяет организовать зашифрованный канал между двумя устройствами или целыми сетями через интернет или другую публичную сеть.

Ключевые особенности:

- Работает на основе протоколов **SSL/TLS**, что обеспечивает высокий уровень безопасности.
- Поддерживает различные методы аутентификации, но основной и самый надёжный — это использование **цифровых сертификатов** и ключей.
- В Astra Linux OpenVPN может использовать российские криптографические алгоритмы ГОСТ, что важно для систем, требующих соответствия стандартам защиты информации.

2. Роли в сети OpenVPN

В любой VPN, построенной на OpenVPN, есть два основных участника:

- **Сервер OpenVPN:** Центральный узел, к которому подключаются все клиенты. Он управляет всей VPN-сетью, выдаёт IP-адреса, аутентифицирует клиентов и шифрует передаваемые данные. В вашей практической работе сервер будет настроен на одном из компьютеров.
- **Клиент OpenVPN:** Рабочая станция, ноутбук или другое устройство, которое устанавливает защищённое соединение с сервером. Чтобы подключиться, клиенту нужны специальные файлы: конфигурация, сертификат и закрытый ключ, полученные от администратора сервера.

3. Криптография в OpenVPN Astra Linux

Главная особенность реализации OpenVPN в Astra Linux — это поддержка **российских криптографических стандартов (ГОСТ)**.

- **Алгоритм «Кузнечик» (grasshopper-cbc):** Это блочный шифр, установленный ГОСТ Р 34.12-2015. В Astra Linux он **выбирается по умолчанию** для шифрования канала, если на сервере установлен пакет libgost-astra.
- **Алгоритм AES:** Если пакет ГОСТ не установлен, или для совместимости с системами общего назначения, может использоваться AES-256-GCM (или AES-256-CBC для старых систем).
- **Важно:** Если сервер использует «Кузнечик», то и на всех клиентах также должен быть установлен пакет libgost-astra. Иначе клиент не сможет расшифровать трафик.

4. Практические аспекты настройки в Astra Linux

В вашей работе для настройки сервера будет использоваться **графическая утилита** fly-admin-openvpn-server. Она автоматизирует большинство сложных действий.

Алгоритм настройки сервера:

1. **Установка пакетов:** Необходимо убедиться, что установлены пакеты openvpn и fly-admin-openvpn-server (а также libgost-astra для ГОСТ).
2. **Запуск утилиты:** Откройте меню «Пуск» → «Панель управления» → «Сеть» → «Настройка OpenVPN сервера».
3. **Первый запуск и генерация сертификатов:** При первом запуске утилита автоматически:

- Создаст конфигурационный файл сервера.
- Создаст свой собственный **Удостоверяющий центр (ЦС)** и выпустит сертификат для самого сервера. Этот процесс может занять некоторое время.

4. **Настройка параметров сети:** В открывшемся окне вы сможете задать:
   - **IP-адрес и маску** для создаваемой VPN-сети (по умолчанию 10.8.0.0/24).
   - **Сетевой порт** (по умолчанию 1194).
   - **Метод защитного преобразования** (по умолчанию grasshopper-cbc — «Кузнечик»).
5. **Управление клиентами:** На вкладке «Клиентские сертификаты» вы сможете **генерировать сертификаты и ключи для каждого клиента**. Это ключевой этап: нажав кнопку «Создать сертификат», вы создадите уникальный набор файлов для конкретного пользователя (например, имя_клиента.crt и имя_клиента.key).
6. **Запуск сервера:** После всех настроек нажмите кнопку **«Запустить»**. Служба будет запущена и настроена на автоматический старт при загрузке системы.

Настройка клиента:
На клиентской машине для подключения к серверу используется встроенный графический менеджер сетевых соединений (Network Manager). Главное условие — наличие на клиенте тех самых файлов (сертификат, ключ и сертификат ЦС), которые были созданы на сервере для этого конкретного клиента.

5. Диагностика

Для проверки работы VPN и выявления ошибок используется **системный журнал (логи)**.

- На сервере или клиенте можно открыть терминал и выполнить команду для просмотра событий:

sudo journalctl -f

или

sudo tail -f /var/log/syslog | grep ovpn-server

- В логах вы сможете увидеть, подключается ли клиент, какой метод шифрования используется (grasshopper-cbc или AES-256-GCM) и есть ли ошибки.

6. Краткий вывод для работы

1. **Сервер** настраивается через fly-admin-openvpn-server, где создаются сертификаты.
2. **Клиент** подключается через стандартный менеджер сетей Astra Linux, используя файлы, полученные с сервера.
3. **Кузнечик** — это российский стандарт шифрования, включённый по умолчанию.
4. Все действия логируются в системный журнал, куда стоит заглядывать при возникновении проблем.

Эта теоретическая база поможет вам осознанно выполнить практическую настройку, понимая назначение каждого шага. Обращайтесь к официальной документации по ссылке, если потребуются уточнения по деталям интерфейса.

Практическая часть:

Во время выполнения работы делайте снимки экрана основных настроек и полученных результатов. Добавляйте скриншоты с краткими комментариями в отчёт. Отчёт должен быть сделан в текстовом документе (предварительно в макете выберите узкие поля).

1. Настройка виртуальных машин

Настройке 2 виртуальные машины на Astra linux:

- Сеть. IPv4 - 192.168.88.10, 192.168.88.20. Шлюз: 192.168.88.2. DNS – 77.88.8.8, 77.88.8.1. IPv6 – откл.
- Имя PC – ФАМИЛИЯ-server, ФАМИЛИЯ-client (фамилию напишите на латинице), например ivanov-server
- Настройте нужные репозитории в /etc/apt/sources.list, проверьте работу интернета.

2. Настройка OpenVPN

В соответствии с официальной документацией настройте OpenVPN через графический режим.

https://wiki.astralinux.ru/display/doc/OpenVPN

При настройке используйте Кузнечик, учтите это в настройках подключения клиента к серверу.

Зафиксируйте скриншотами результаты работы.

Если в процессе работы не успеете всё сделать или сдать работу – сделай снимок состояния, назовите его своей фамилией.

3. Проверка работы OpenVPN

Установите утилиту tcpdump и проверить, что vpn-туннель действительно работает, воспользуйтесь поисковой системой или нейросетью.

Например.

1. **Запустите два терминала** на клиенте.
2. В первом: sudo tcpdump -i tun0 -n (показывает «внутренности» туннеля).
3. Во втором: sudo tcpdump -i eth0 -n (показывает «снаружи»).
4. Выполните curl http://example.com.
5. **Одновременно** посмотрите выводы обоих терминалов. Объясните в чём разница.
6. **Отключите VPN** и повторите curl http://example.com с tcpdump -i eth0 -n. Что изменилось?

4. Ответьте на вопрос

1. Для чего в реальной жизни может пригодиться умение настройки vpn-туннеля?
2. Какое программное обеспечение используется для организации защищённого канала связи на практике?