Тема: Настройка WireGuard на Astra Linux

Цель работы: получить навык настройки vpn-туннеля по протоколу WireGuard с помощью терминала в Astra Linux на основе официальной документации.

Теоретические сведения

1. Что такое WireGuard?

WireGuard — это современный и высокопроизводительный протокол для создания защищённых VPN-соединений. Его можно представить как более быстрый и простой аналог OpenVPN или IPsec.

Ключевые особенности:

- **Работает на уровне ядра** операционной системы, что обеспечивает высокую скорость и низкую задержку.
- **Простота настройки:** Вместо сложной системы сертификатов (как в OpenVPN) используется простая криптография на основе **пар ключей** (публичный и приватный), как в SSH.
- **Устойчивость к смене IP:** Автоматически поддерживает соединение, даже если у клиента или сервера меняется физический IP-адрес (например, при переходе между сетями Wi-Fi и мобильным интернетом).

2. Базовая архитектура и термины

В WireGuard все узлы равноправны (peer-to-peer), но для простоты в вашей работе будет использоваться классическая модель **«звезда»**:

- **Сервер (wgserver):** Центральный узел с фиксированным физическим IP-адресом. К нему подключаются все клиенты.
- **Клиент (wgclient):** Узел, который устанавливает соединение с сервером.
- **Виртуальный интерфейс (wg0):** Создаваемое WireGuard виртуальное сетевое устройство. Оно настраивается так же, как и физическая сетевая карта, но работает только внутри VPN-сети.
- **Виртуальный адрес:** IP-адрес, который получает устройство *внутри* VPN-сети (например, 10.0.0.1/24). Он не должен совпадать с физическим адресом устройства в локальной сети.
- **Контрагент (Peer):** Любая сторона соединения. Для сервера контрагентами являются клиенты, для клиента — сервер.

3. Криптография и ключи

Главное отличие WireGuard — использование криптографии на основе ключей для аутентификации, а не сертификатов.

- **Ключевая пара:** Для каждого узла (сервера и каждого клиента) создается своя уникальная пара:
    - **Закрытый (приватный) ключ:** Должен храниться в секрете на том узле, где он создан. Никому не передается.
    - **Открытый (публичный) ключ:** Может передаваться по незащищенным каналам. Открытый ключ сервера нужно указать в настройках всех клиентов, а открытый ключ *каждого* клиента — в настройках сервера.
- **Разделяемый (preshared) ключ:** Необязательный, но рекомендуемый элемент для усиления защиты. Это один и тот же секретный ключ, который добавляется в настройки и сервера, и клиента. Передаваться должен только по защищенным каналам.

4. Практические аспекты настройки в Astra Linux

В вашей работе настройка будет выполняться в **терминале** с использованием команд wg и wg-quick.

Алгоритм настройки для сервера и клиента:

1. **Установка:**

sudo apt update

sudo apt install wireguard wireguard-tools

(На клиенте, если планируется использовать параметр DNS, дополнительно установите sudo apt install resolvconf).

2. **Генерация ключей:** На *каждом* узле (сервере и каждом клиенте) выполните команды для создания своих собственных ключей:

Создать закрытый ключ

wg genkey | sudo tee /etc/wireguard/privkey > /dev/null

sudo chmod 600 /etc/wireguard/privkey

Создать соответствующий открытый ключ

sudo cat /etc/wireguard/privkey | wg pubkey | sudo tee /etc/wireguard/pubkey

Важно: Обменяйтесь открытыми ключами (содержимым файлов pubkey) между сервером и клиентами.

3. **Создание конфигурации сервера (**/etc/wireguard/wg0.conf**):**
    - В секции [Interface] укажите свой закрытый ключ, виртуальный адрес сервера (например, Address = 10.0.0.1/24) и порт для прослушивания (ListenPort = 51820).
    - В секции [Peer] для *каждого* клиента укажите его открытый ключ (PublicKey) и его виртуальный IP-адрес (AllowedIPs = 10.0.0.2/32 для первого клиента, 10.0.0.3/32 для второго и т.д.).
    - Добавьте правила для маршрутизации трафика (PostUp и PostDown), чтобы клиенты могли выходить в интернет через сервер.
4. **Создание конфигурации клиента (**/etc/wireguard/wg0.conf**):**
    - В секции [Interface] укажите свой закрытый ключ, виртуальный адрес клиента (например, Address = 10.0.0.2/24) и опционально DNS-сервер (DNS = 77.88.8.1).
    - В секции [Peer] укажите открытый ключ сервера (PublicKey), его физический адрес и порт (Endpoint = <физический_IP_сервера>:51820), а также AllowedIPs = 0.0.0.0/0 (чтобы направлять весь интернет-трафик через сервер) или AllowedIPs = 10.0.0.1/32 (только для доступа к VPN-сети).
5. **Включение и управление:**
    - Включить интерфейс: sudo wg-quick up wg0
    - Выключить интерфейс: sudo wg-quick down wg0
    - Проверить статус соединения: sudo wg show
    - Добавить службу в автозагрузку: sudo systemctl enable wg-quick@wg0
6. **Важное замечание:** На сервере необходимо разрешить пересылку пакетов (IP-forwarding):

bash

echo "net.ipv4.ip_forward=1" | sudo tee -a /etc/sysctl.conf

sudo sysctl -p

5. Краткий вывод для работы

1. WireGuard не использует сертификаты. Вся аутентификация строится на обмене **открытыми ключами**.
2. На сервере в секциях [Peer] перечисляются все клиенты с их открытыми ключами и виртуальными IP-адресами.
3. Клиент в своей конфигурации указывает открытый ключ и физический адрес сервера.
4. Для управления туннелем используются команды wg-quick up/down, а для просмотра статуса — wg show.

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 (аналогично предыдущей работе)

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 – server, client
- Настройте нужные репозитории в /etc/apt/sources.list, проверьте работу интернета.

2. Настройка WireGuard

В соответствии с официальной документацией настройте WireGuard через терминал.

https://wiki.astralinux.ru/pages/viewpage.action?pageId=348174305

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

Зафиксируйте скриншотами результаты работы.

3. Проверка работы OpenVPN

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

4. Ответьте на контрольные вопросы

Блок 1. Общие концепции VPN

1. **Определение:** Дайте определение VPN (Virtual Private Network) и поясните его основное назначение.
2. **Сравнение:** В чем ключевое отличие между OpenVPN и WireGuard с точки зрения архитектуры (клиент-серверная vs. одноранговая) и принципов аутентификации (сертификаты vs. ключи)?

Блок 2. OpenVPN (по практической работе)

3. **Назначение:** Для чего в OpenVPN используется связка из сертификатов и ключей? Опишите роль Удостоверяющего Центра (ЦС).
4. **Процесс:** Опишите базовый алгоритм настройки сервера OpenVPN с помощью графической утилиты fly-admin-openvpn-server.
5. **ГОСТ:** Какую особенность имеет реализация OpenVPN в Astra Linux в плане криптографии? Назовите основной алгоритм.
6. **Клиент:** Какие файлы (сертификаты и ключи) необходимо передать клиенту для подключения к серверу OpenVPN? Почему их передача должна быть защищена?

Блок 3. WireGuard (по практической работе)

7. **Криптография:** Объясните, как происходит аутентификация в WireGuard. Какие типы ключей используются и какие из них являются критически важными для безопасности?
8. **Конфигурация:** Назовите обязательные параметры для секции [Interface] и [Peer] в конфигурационном файле WireGuard. В чем их смысл?
9. **Маршрутизация:** Как параметр AllowedIPs = 0.0.0.0/0 в конфигурации клиента влияет на маршрутизацию его трафика?
10. **Управление:** Какими командами в терминале можно включить/выключить виртуальный интерфейс WireGuard (wg0) и проверить статус текущего соединения?

Блок 4. Сравнение и анализ

11. **Сравнение:** Перечислите по 2-3 ключевых преимущества OpenVPN и WireGuard. Когда, на ваш взгляд, выбор того или иного протокола будет более оправдан?
12. **Диагностика:** В чем заключается общий подход к диагностике проблем для обоих протоколов (просмотр логов)? Приведите пример команды для просмотра системных логов в Astra Linux.
13. **Безопасность:** Какой из двух протоколов по умолчанию использует сертификаты (PKI), а какой — пары открытых/закрытых ключей? Как это влияет на сложность администрирования в крупной сети?