**Звіт на тему**: Налаштувати VPN тунель WireGuard між сервером та клієнтом

**Виконав**: 05 09

Ось послідовні кроки, які вам потрібно буде виконати, щоб налаштувати VPN тунель WireGuard:

1. Встановіть будь-який дистрибутив Linux на вашу віртуальну машину. Залежно від вашого вибору, процедура може відрізнятися. Завантажте образ ISO з офіційного сайту дистрибутива, створіть нову віртуальну машину та встановіть систему.
2. Встановлення WireGuard: Після успішної установки Linux залежності WireGuard, відкрийте термінал і введіть наступну команду для встановлення WireGuard:

sudo apt install wireguard

1. WireGuard використовує пару приватного та публічного ключів для аутентифікації. Генеруйте ключі на сервері та клієнті. В терміналі виконайте наступні команди на сервері та клієнті:

wg genkey | sudo tee /etc/wireguard/privatekey | wg pubkey | sudo tee /etc/wireguard/publickey

1. **Налаштування сервера**: Створіть конфігураційний файл для сервера, використовуючи приватний ключ сервера та публічний ключ клієнта. Введіть наступну команду у терміналі сервера для створення файлу конфігурації:

sudo nano /etc/wireguard/wg0.conf

Вставте наступний зразок конфігурації сервера, замінивши <SERVER\_PRIVATE\_KEY> на приватний ключ сервера та <CLIENT\_PUBLIC\_KEY> на публічний ключ клієнта:

[Interface]

Address = 10.0.0.1/24

ListenPort = 51820

PrivateKey = <SERVER\_PRIVATE\_KEY>

[Peer]

PublicKey = <CLIENT\_PUBLIC\_KEY>

AllowedIPs = 10.0.0.2/32

Збережіть та закрийте файл конфігурації (наприклад, у Nano натисніть Ctrl + X, потім підтвердіть збереження змін).

1. Налаштування клієнта: Аналогічно створіть конфігураційний файл для клієнта. Введіть наступну команду у терміналі клієнта для створення файлу конфігурації:

sudo nano /etc/wireguard/wg0.conf

Вставте наступний зразок конфігурації клієнта, замінивши <CLIENT\_PRIVATE\_KEY> на приватний ключ клієнта та <SERVER\_PUBLIC\_IP> на публічну IP-адресу сервера:

[Interface]

Address = 10.0.0.2/24

PrivateKey = <CLIENT\_PRIVATE\_KEY>

[Peer]

PublicKey = <SERVER\_PUBLIC\_KEY>

Endpoint = <SERVER\_PUBLIC\_IP>:51820

AllowedIPs = 0.0.0.0/0

1. Запуск сервера та клієнта: Запустіть WireGuard на сервері та клієнті, використовуючи наступні команди:

sudo wg-quick up wg0 # Запуск сервера

sudo wg-quick up wg0 # Запуск клієнта

1. Перевірка з'єднання: Після запуску сервера та клієнта вони повинні встановити VPN-тунель. Ви можете перевірити з'єднання, виконавши на сервері або клієнті команду:

sudo wg

Якщо все пройшло успішно, ви повинні побачити вивід з інформацією про з'єднання.

Це базова інструкція з налаштування VPN тунелю WireGuard між сервером та клієнтом. Зверніть увагу, що вам може знадобитися налаштувати файрвол на сервері, щоб дозволити трафік через порт 51820. Також будьте обережні з налаштуванням безпеки, включаючи захист приватного ключа і обмеження доступу до VPN-сервера.