DOI: https://doi.org/10.26642/ten-2025-1(95)-317-324
УДК 637.5.02

І.Г. Фальковський, ст. викладач
В.В. Воротніков, д.т.н., доц.
В.В. Миколайчук, ст. викладач
Державний університет «Житомирська політехніка»

SoftEther VPN на OpenWRT у віртуальному середовищі VirtualBox

У статті подано детальний посібник з інсталяції та налаштування VPN-сервера SoftEther на платформі OpenWRT, розгорнутій у віртуальному середовищі Oracle VirtualBox. Розглянуто покроковий процес створення віртуального середовища, встановлення необхідних пакетів і налаштування мережевих параметрів для забезпечення стабільного та захищеного VPN-з'єднання. Посібник починається з огляду можливостей OpenWRT і переваг використання SoftEther VPN, особливо для малого бізнесу та індивідуальних користувачів, які прагнуть створити приватну зашифровану мережу.

У статті докладно описано підготовку середовища OpenWRT у VirtualBox, зокрема конфігурацію мережевих інтерфейсів, налаштування фаєрволу та встановлення компонентів SoftEther VPN. Також висвітлено налаштування самого VPN-сервера, зокрема управління користувачами, параметри шифрування та правила фаєрволу для захисту від несанкціонованого доступу. Наголошено на важливості використання VPN для безпечного віддаленого доступу до мережевих ресурсів в умовах зростання популярності дистанційної та розподіленої роботи.

Процес налаштування викладено у зрозумілому покроковому форматі, що робить його доступним навіть для користувачів з обмеженим досвідом у сфері мережевого адміністрування. Наведено практичні поради щодо усунення типових проблем, які можуть виникати під час інсталяції, зокрема з підключенням або у випадку конфліктів із наявними мережевими конфігураціями. Крім того, подано рекомендації з підтримки та моніторингу VPN-сервера після його впровадження, що сприяє підвищенню рівня безпеки та продуктивності.

Скориставшись цим посібником, читачі отримають знання й інструменти, необхідні для розгортання повнофункціонального й захищеного VPN-сервера SoftEther на базі OpenWRT, що дозволить створити надійне приватне мережеве рішення. Такий підхід особливо корисний для організацій, які прагнуть забезпечити безпечний віддалений доступ для працівників, а також для індивідуальних користувачів, які бажають захистити свою онлайн-активність і персональні дані. У завершенні розглянуто можливості масштабування такої інфраструктури та подано поради щодо її подальшого налаштування відповідно до специфічних потреб користувача.

Ключові слова: *OpenWRT; віртуальна машина; Oracle VirtualBox; операційна система; VPN; SoftEther VPN.*

Постановка проблеми. Використання SoftEther VPN server на OpenWRT має значні переваги, зокрема, забезпечення високого рівня безпеки, гнучкості налаштувань та сумісності з різними VPN-протоколами, такими як L2TP/IPsec, OpenVPN, та SSTP. Це робить його привабливим рішенням для створення надійного та масштабованого VPN-з'єднання, що підходить як для невеликих організацій, так і для індивідуальних користувачів. Проте, попри всі переваги SoftEther VPN, його інтеграція з OpenWRT залишається недостатньо висвітленою у офіційній документації на сайті OpenWRT [1]. Існуючі інструкції не охоплюють усіх аспектів налаштування, залишаючи користувачів без детальних інструкцій щодо установки та конфігурації цього VPN-сервера на платформі OpenWRT. Це може створити труднощі для тих, хто прагне використати всі можливості SoftEther VPN у поєднанні з OpenWRT.

Для вивчення цього питання та демонстрації практичного застосування SoftEther VPN server на OpenWRT, у цій статті було обрано віртуальну машину Oracle VirtualBox. Такий підхід є найпростішим способом створення лабораторного стенду, що дозволяє безпечно експериментувати з налаштуваннями та протестувати різні сценарії роботи VPN-сервера без ризику для основної мережі. Віртуальне середовище також забезпечує гнучкість у налаштуваннях та можливість швидкого відновлення системи у випадку виникнення помилок, що робить його ідеальним інструментом для вивчення та експериментування з OpenWRT та SoftEther VPN.

Аналіз останніх досліджень. На жаль, надання детального аналізу останніх досліджень виключно на тему SoftEther VPN на OpenWRT є дещо складним завданням з кількох причин:

- **розрізненість досліджень.** Більшість досліджень, пов'язаних з VPN, зосереджуються на загальних аспектах безпеки, продуктивності та нових протоколах (WireGuard, ChaCha20), а не на конкретних реалізаціях, таких як SoftEther на OpenWRT;

- **часта зміна технологій.** Сфера VPN постійно розвивається. Нові версії SoftEther, OpenWRT та зміни в протоколах можуть швидко застаріти дослідження;
- **відсутність централізованої бази даних.** Не існує єдиного репозиторію, де б збиралися всі дослідження саме з цієї теми.

Дуже актуальною є тема використання та оптимізація SoftEther для малопотужних пристроїв. Це комплексна задача, яка вимагає індивідуального підходу в кожному конкретному випадку, де рішення на основі OpenWRT пристроїв дозволяє стандартизувати підходи у реалізації. У роботі [2], присвяченій впровадженню WireGuard VPN у середовище домашнього офісу приділена значна увага перспективам заміни VPN-сервера на SoftEther для пристроїв, що не можуть функціонувати з профільним сервером. У роботі [3] надано ряд рекомендацій для зменшення ризиків безпеки при налаштуванні SoftEther VPN на різних пристроях, в тому числі і малопотужних.

Огляд апаратних вимог для встановлення ВПН-сервера на ВМ OpenWRT. Загальні вимоги до апаратного забезпечення розглянуто в публікаціях [5] та [4]. Важливим аспектом при розгортанні VPN-сервера є мережеві інтерфейси. Вибір кількості інтерфейсів для OpenWRT, що виконує функцію VPN-сервера, визначається потребами та сценаріями використання мережі. Однак, можна виділити основні рекомендації.

Необхідні інтерфейси:

- **WAN (Wide Area Network).** Цей зовнішній інтерфейс відповідає за підключення до Інтернету або зовнішньої мережі. Він необхідний для отримання трафіку з Інтернету та встановлення VPN-з'єднань;
- **LAN (Local Area Network).** Внутрішній інтерфейс, що забезпечує підключення до локальної мережі, дозволяє маршрутизувати трафік і надавати доступ до VPN-сервера для внутрішніх пристроїв.

Додаткові інтерфейси залежно від потреб:

- **VPN-інтерфейс.** У разі налаштування VPN-сервера для підключення клієнтів через VPN-тунель може знадобитися окремий VPN-інтерфейс;
- **DMZ (демілітаризована зона)**. Корисний для ізоляції певних служб або пристроїв, що потребують обмеженого доступу;
- **Інтерфейс гостьової мережі.** Використовується для надання гостям доступу до Інтернету з обмеженим доступом до внутрішньої мережі.

Використання VLAN (Virtual LAN):

Використання VLAN (віртуальних локальних мереж) дозволяє ефективно налаштовувати доступ та ізоляцію різних мережевих сегментів за допомогою одного фізичного інтерфейсу. Як правило, необхідно мати щонайменше два основних інтерфейси: один для зовнішнього підключення (WAN) і один для внутрішньої мережі (LAN). Додаткові інтерфейси можуть бути додані залежно від конкретних вимог та обмежень. Основним завданням є правильна сегментація та налаштування маршрутизації і файерволу для забезпечення безпеки та оптимальної роботи VPN-сервера на OpenWRT. Далі буде розглянуто конкретний приклад розгортання VPN-сервера з мінімальним набором мережевих інтерфейсів.

Реалізація VPN-сервера SoftEther на OpenWRT

Підключаємо у створеній по методиці [4] віртуальній машині додатковий інтерфейс Adapter 2, що буде відповідати за внутрішню мережу (рис. 1).

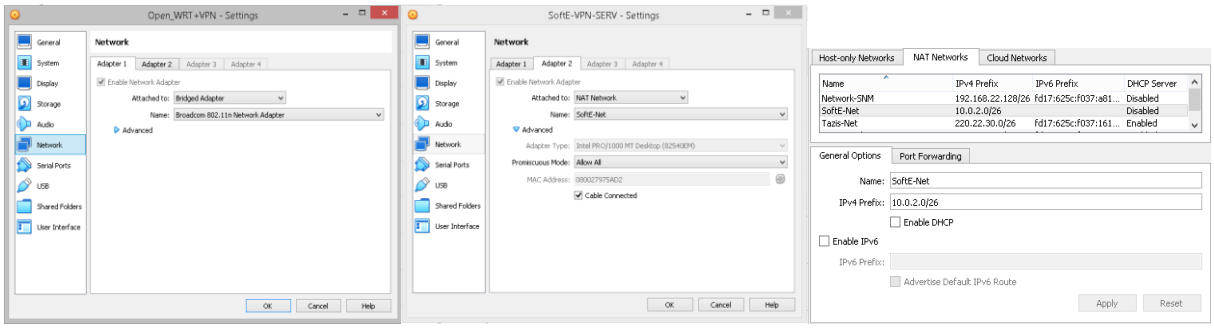

Рис. 1. Мережеві інтерфейси віртуальної машини

Редагуємо файл конфігурації мережеві за допомогою вбудованого текстового редактору vi.

vi /etc/config/network

Для підключень до мережі вимикаємо налаштування DHCP на мережевих адаптерах, та налаштовуємо статичні адреси, приводячи конфігурацію до наступного вигляду:

```
config interface loopback
        option ifname lo
        option proto static
        option ipaddr 127.0.0.1
        option netmask 255.0.0.0
config interface wan
        option ifname eth0
        option proto static
```

Вводимо у дію зміни:
/etc/init.d/network restart

option ipaddr 192.168.1.121
option netmask 255.255.255.0
option gateway 192.168.1.1
list dns 193.24.25.1
list dns 193.24.25.250
config interface lan
option ifname eth1
option proto static
option ipaddr 10.0.2.3
option netmask 255.255.255.192
option gateway 10.0.2.1
list dns 10.0.2.1

Можливі помилки оновлення через неактуальність конфігураційного файлу репозиторіїв /etc/opkg/distfeeds.conf [4]. У цьому випадку необхідно додати наступні рядки до файлу:
src/gz openwrt_corehttps://downloads.openwrt.org/releases/$(VERSION)/targets/$(BOARD)/$(SUBTARGET)/packages
src/gz openwrt_base https://downloads.openwrt.org/releases/$(VERSION)/packages/$(ARCH)/base
src/gz openwrt_luci https://downloads.openwrt.org/releases/$(VERSION)/packages/$(ARCH)/luci
src/gz openwrt_packages https://downloads.openwrt.org/releases/$(VERSION)/packages/$(ARCH)/packages
src/gz openwrt_routing https://downloads.openwrt.org/releases/$(VERSION)/packages/$(ARCH)/routing
src/gz openwrt_telephony https://downloads.openwrt.org/releases/$(VERSION)/packages/$(ARCH)/telephony

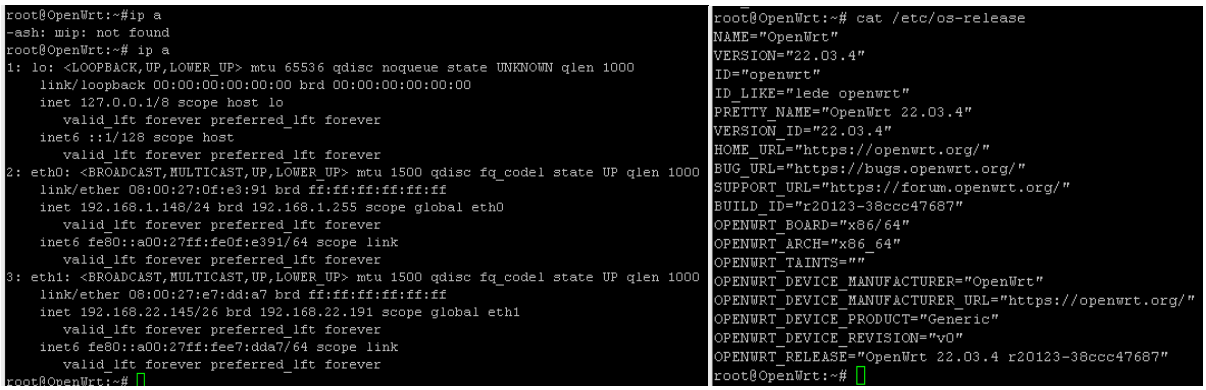

Рис. 2. Мережеві інтерфейси віртуальної машини OpenWRT та вивід os-release

Визначаємо значення змінних $(VERSION), $(BOARD)/$(SUBTARGET), $(ARCH). Відповідно до виводу команди cat /etc/os-release (рис. 2) змінні приймають наступні значення:

$(VERSION) - 22.03.4, $(BOARD)/$(SUBTARGET) - x86/64, $(ARCH) - x86_64

Тоді рядки конфігураційного файлу репозиторіїв /etc/opkg/distfeeds.conf приймають вигляд:
src/gz openwrt_core https://downloads.openwrt.org/releases/$(VERSION)/targets/$(BOARD)/$(SUBTARGET)/packages
src/gz openwrt_core https://downloads.openwrt.org/releases/22.03.4/targets/x86/64/packages
src/gz openwrt_base https://downloads.openwrt.org/releases/22.03.4/packages/x86_64/base
src/gz openwrt_luci https://downloads.openwrt.org/releases/22.03.4/packages/x86_64/luci
src/gz openwrt_packages https://downloads.openwrt.org/releases/22.03.4/packages/x86_64/packages
src/gz openwrt_routing https://downloads.openwrt.org/releases/22.03.4/packages/x86_64/routing
src/gz openwrt_telephony https://downloads.openwrt.org/releases/22.03.4/packages/x86_64/telephony

Встановлюємо необхідні пакети, виконавши оновлення:

opkg update

Спроба встановити сервер SoftEtherVPN показує проблема – великий об’єм дистрибутиву, що викладено на сайті https://github.com/SoftEtherVPN/SoftEtherVPN_Stable. Об’єм актуального, на момент написання цього матеріалу, файлу SoftEtherVPN_Stable-master.zip складає більше 28 Mb, а у розархівованому вигляді 75 Мб. Такого об’єму вільного місця на системах OpenWRT, як правило, немає. Є кілька можливих варіантів вирішення цієї проблеми:

- спільний ресурс для зберігання та встановлення. Завантажити та розпакувати SoftEtherVPN на мережевий ресурс, до якого має доступ OpenWRT. Після цього можна спробувати встановити його безпосередньо з мережевого ресурсу. Потрібно буде змонтувати цей ресурс на OpenWRT через NFS, CIFS або інший протокол, який підтримується OpenWRT. Потім виконати компіляцію або встановлення безпосередньо з цього змонтованого ресурсу;

- у [5] запропоновано ще один підхід, що дозволяє підготувати всі необхідні пакети для встановлення безпосередньо на пристрій, де ресурси обмежені. Підготовка дистрибутивів виконується на окремому Linux-комп'ютері із встановленими інструментами для компіляції, куди завантажено OpenWRT SDK, додано до нього репозиторій SoftEtherVPN, та виконано компіляцію пакету під архітектуру маршрутизатора. Після цього, компільовані пакети копіюються на OpenWRT і встановлюються, щоб запустити SoftEtherVPN безпосередньо на пристрої;
- зовнішнє сховище для OpenWRT. Додати зовнішній USB-накопичувач або інший тип сховища, якщо пристрій OpenWRT підтримує його. Це розширить доступне місце для файлів і встановлення великих пакетів. В силу апаратних обмежень, таке рішення не універсальне:
  - обмеження USB-порту. Далеко не всі пристрої з OpenWRT мають USB-порти. Якщо він є, зазвичай це USB 2.0, що обмежує швидкість передачі даних (до ~480 Мбіт/с). Для простих задач цього вистачає, але для інтенсивних операцій швидкість може стати вузьким місцем;
  - процесор та оперативна пам'ять. Більшість пристроїв OpenWRT розраховані на економію ресурсів, маючи слабкі процесори та обмежену ОЗП. Доступ до зовнішнього диску може створювати додаткове навантаження на процесор, особливо при одночасному виконанні VPN, маршрутизації чи інших задач;
  - файлова система. OpenWRT підтримує різні файлові системи (наприклад, ext4, FAT, NTFS), але для стабільної роботи та сумісності рекомендується використовувати ext4 або інші Linux-сумісні файлові системи. NTFS підтримується обмежено і вимагає додаткових драйверів, що може бути нестабільно або потребувати багато ресурсів;
  - енергоспоживання. Деякі USB-накопичувачі, особливо HDD, споживають більше енергії, ніж може забезпечити USB-порт маршрутизатора. У таких випадках потрібен накопичувач із зовнішнім живленням або USB-концентратор з живленням;
  - швидкість роботи. У багатьох випадках швидкість доступу до даних на USB-накопичувачі буде меншою, ніж до внутрішньої флеш-пам'яті. Це впливає на продуктивність системи при запуску програм чи обробці великих обсягів даних.

Переходимо до генерації private, public та pre-shared ключів. Створення private та public комплекту серверних ключів:

wg genkey | tee wg.key | wg pubkey > wg.pub

Створення pre-shared ключа, його збереження у файл та зміна прав доступу до цього файлу:

wg genpsk
echo "2CWsxXL0T62J+4jyeWJ5ywuzFP2tDAsUNqgwj/0bvAY=" > wg.psk
chmod 600 wg.psk

Для кожного клієнтського хосту теж необхідно згенерувати пару ключів private та public.

Pre-shared Key (PSK) не є обов'язковим, але додає додатковий рівень симетричної криптографії, що підвищує безпеку WireGuard VPN з'єднання. Він використовується в поєднанні з основними ключами для забезпечення більш захищеного каналу зв'язку. Генерація та використання PSK досить проста і вимагає лише невеликих змін у конфігураційних файлах як на сервері, так і на клієнті (рис. 3).

```
root@OpenWrt:~# wg genkey | tee wg.key | wg pubkey > wg.pub
root@OpenWrt:~# wg genpsk > wg.psk
Warning: writing to world accessible file.
Consider setting the umask to 077 and trying again.
root@OpenWrt:~# wg genpsk
Ak7fhTtSI3idViEg/3yRvwy+ASaYXOL5UfWvhIQzYWQ=
root@OpenWrt:~# wg genkey | tee wg.key | wg pubkey > wg.pub
root@OpenWrt:~# wg genpsk
RxlnhpM5m8VrMieJyAppze5Ak7onL+2VOrZFJ7/Mteo=
root@OpenWrt:~# echo "RxlnhpM5m8VrMieJyAppze5Ak7onL+2VOrZFJ7/Mteo=" > wg.psk
root@OpenWrt:~# chmod 600 wg.psk
root@OpenWrt:~# ls
wg.key  wg.psk  wg.pub
root@OpenWrt:~#
```

Рис. 3. Генерація ключів на сервері

Додамо у файл ***/etc/config/network*** секцію, що відповідає за налаштування VPN-інтерфейсу на сервері.

config interface 'vpnwg'	
option proto 'wireguard'	інтерфейс використовує протокол WireGuard
option private_key 'SERVER_PRIVATE_KEY'	вміст файлу приватного ключа сервера.
option listen_port '51820'	порт, на якому буде слухати сервер.
list addresses '10.8.0.1/24'	IP-адреса сервера у VPN-мережі.

Серверу виділена IP-адреса 10.8.0.1 з підмережею 10.8.0.0/24. Це означає, що сервер буде мати IP-адресу 10.8.0.1, а вся підмережа 10.8.0.0/24 доступна для використання клієнтами.

Наступна секція налаштовує параметри для конкретного клієнта на сервері:

config wireguard_vpnwg

option public_key 'CLIENT1_PUBLIC_KEY'	вміст файлу публічного ключа клієнта1
option preshared_key 'PRESHARED_KEY'	вміст файлу pre-shared ключа для додаткового захисту
list allowed_ips '10.8.0.2/32'	виділена клієнту1 IP-адреса
option route_allowed_ips '1'	дозволяє маршрутизацію трафіку через цей інтерфейс
option persistent_keepalive '25'	вказує на інтервал (у секундах), з яким клієнт буде відправляти keepalive-пакети для підтримки з'єднання активним.

Мережа 10.8.0.1/24 виділена для VPN-з'єднання. Сервер використовує IP-адресу 10.8.0.1, а решта адрес з підмережі 10.8.0.0/24 можуть використовуватись клієнтами (наприклад, 10.8.0.2, 10.8.0.3 і так далі). Адреса 10.8.0.2/32 виділена конкретному клієнту. Це означає, що даний клієнт буде мати IP-адресу 10.8.0.2 у VPN-мережі.

Таким чином, сервер має IP-адресу 10.8.0.1 у VPN-мережі 10.8.0.0/24, а клієнти отримують IP-адреси з цієї ж мережі (наприклад, 10.8.0.2, 10.8.0.3 і так далі). Цей підхід забезпечує можливість організувати VPN-мережу, в якій кожен клієнт має свою унікальну IP-адресу, що дозволяє серверу ефективно маршрутизувати трафік між клієнтами та внутрішньою мережею (рис. 4).

Скористаємося практикою налаштування маршруту через файл /etc/config/network. Така конфігурація створює маршрут з VPN-мережі до внутрішньої мережі. Ось секція конфігурації, яку потрібно додати до файлу /etc/config/network:

config route	Ця секція забезпечує маршрутизацію при якій всі пакети, що надходять до внутрішньої мережі 192.168.22.128/26, будуть перенаправлятися через інтерфейс vpnwg до шлюзу 10.8.0.1, який є адресою WireGuard сервера у VPN-мережі.
option interface 'vpnwg'	
option target '192.168.22.128'	
option netmask '255.255.255.192'	
option gateway '10.8.0.1'	
Вводимо у дію зміни:	***/etc/init.d/network restart***
Вмикаємо інтерфейс:	***ifup vpnwg***
Перевіряємо його стан по логам	***logread | grep wg***
	logread | grep vpnwg

Налаштовуємо файрвол, щоб дозволити трафік на порт WireGuard та забезпечити маршрутизацію між VPN-інтерфейсом і внутрішньою мережею. У файл /etc/config/firewall додаємо наступні налаштування:

config zone ***option name vpn*** ***option network 'vpnwg'*** ***option input ACCEPT*** ***option output ACCEPT*** ***option forward ACCEPT***	Конфігураційна зона **vpn**
config forwarding ***option src vpn*** ***option dest lan***	Дозволяє пересилання трафіку з зони **vpn** (інтерфейс WireGuard) до зони **lan** (внутрішня мережа).
config forwarding ***option src lan*** ***option dest vpn***	Дозволяє пересилання трафіку з зони **lan** (внутрішня мережа) до зони **vpn** (інтерфейс WireGuard).
config rule ***option name Allow-WireGuard-Inbound*** ***option src wan*** ***option dest_port 51820*** ***option proto udp*** ***option target ACCEPT***	Секція дозволяє вхідний трафік на порт 51820 (порт за замовчуванням для WireGuard) з інтерфейсу **wan** (зовнішня мережа).
config rule ***option name Allow-SSH-From-VPN*** ***option src vpn*** ***option dest lan*** ***option dest_port 22*** ***option proto tcp*** ***option target ACCEPT***	Дозволяє вхідний SSH-трафік (порт 22) з зони **vpn** до зони **lan** (внутрішня мережа).

Внесені зміни вводяться у дію командою — ***/etc/init.d/firewall restart***
Перевіряємо стан ВПН-інтерфейсу — ***wg show***
ip link show vpnwg

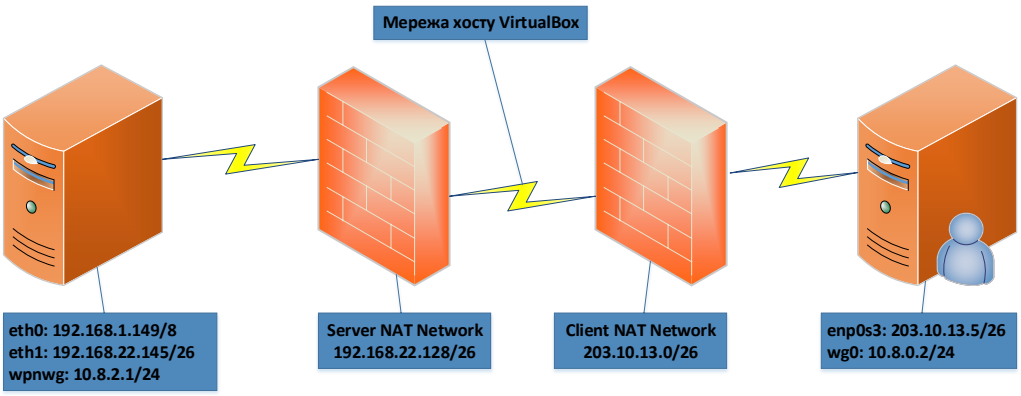

Рис. 4. Загальна схема мережі, використана при написанні статті

Клієнти WireGuard VPN

Підтримка WireGuard VPN реалізована на багатьох операційних системах: Linux, Windows, macOS, Android, iOS, FreeBSD, OpenBSD. Для підключення до WireGuard VPN використовуються нативні клієнти WireGuard, оскільки WireGuard використовує власний протокол, який не сумісний зі стандартними VPN-клієнтами. Встановлення WireGuard VPN клієнта виконується звичним для кожної операційної системи методом.

У Linux, FreeBSD та OpenBSD встановлення виконується через пакетний менеджер дистрибуції (наприклад, apt для Ubuntu чи pkg для FreeBSD). У Windows, клієнт доступний на офіційному сайті WireGuard for Windows. Для macOS, клієнт завантажується з App Store, для Android – доступний у Google Play Store, а для iOS доступний у App Store.

WireGuard використовує асиметричне шифрування, що означає, що кожен клієнт і сервер мають пари приватних і публічних ключів. Приватні ключі зберігаються локально і ніколи не передаються. Публічні ключі використовуються для автентифікації підключення між клієнтом і сервером.

Спробуємо встановити WireGuard клієнт на Linux сервер (рис. 5).

```
student@serv-22-1-2:~$ wg genkey | tee client_private.key | wg pubkey > client_public.key
student@serv-22-1-2:~$ dir
client_private.key  client_public.key
student@serv-22-1-2:~$
```

Рис. 5. Генерація ключів на Linux-клієнті

sudo apt update — Оновлюємо систему, щоб переконатися, що всі пакети актуальні.
sudo apt upgrade –y
sudo apt install resolvconf — Встановлюємо resolvconf
sudo apt install wireguard -y — Встановлюємо WireGuard за допомогою менеджера apt
wg --version — Перевіряємо, чи встановлений WireGuard
wg genkey | tee client_private.key | wg pubkey > client_public.key
Генеруємо приватний та публічний ключі клієнта

Створюємо конфігураційний файл для WireGuard. Зазвичай це файл /etc/wireguard/wg0.conf. Вміст файлу наступний:

```
[Interface]
PrivateKey = <CLIENT_PRIVATE_KEY>          # Згенерований приватний ключ клієнта
Address = 10.8.0.2/24                      # IP-адреса клієнта у VPN мережі
DNS = 193.24.25.1, 193.24.25.250           # DNS-сервери, що використовуються
[Peer]
PublicKey = <SERVER_PUBLIC_KEY>            # Публічний ключ сервера
PresharedKey = <PRESHARED_KEY>             # Згенерований pre-shared ключ (якщо використовується)
Endpoint = <SERVER_IP>:51820               # IP-адреса і порт сервера
AllowedIPs = 0.0.0.0/0                     # Адреси дозволені до маршрутизації через цей тунель
```

PersistentKeepalive = 25 ***# Підтримка з'єднання активним***

sudo wg-quick up wg0 Запускаємо клієнт WireGuard
sudo wg show Перевіряємо статус інтерфейсу
sudo systemctl enable wg-quick@wg0 Автоматичний запуск інтерфейсу при завантаженні

Перевіряємо працездатність ВПН на сервері та клієнті (рис. 6):

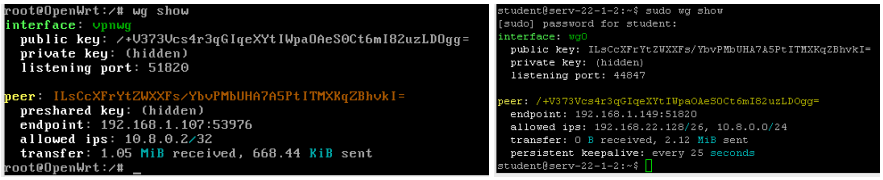

Рис. 6. Перевірка ВПН на сервері wg show та на Linux-клієнті sudo wg show

Список використаної літератури:

1. SoftEther VPN / OpenWrt wiki. – 2024 [Electronic resource]. – Access mode : https://openwrt.org/docs/guide-user/services/vpn/softethervpn/start.
2. *Saukkonen S.* Building a Secure VPN Infrastructure Using SoftEther VPN / *S.Saukkonen.* – 2020 [Electronic resource]. – Access mode : https://www.theseus.fi/bitstream/handle/10024/347871/Saukkonen_Samu.pdf?sequence=2.
3. SoftEther VPN Implementation Guide. – 2023 [Electronic resource]. – Access mode : http://surl.li/kdcply.
4. *Фальковський І.Г.* OpenWRT у віртуальному середовищі VirtualBox / *І.Г. Фальковський, О.С. Головня* // Вісник Хмельницького національного університету. Технічні науки. – 2023. – № 4. – С. 358–364.
5. VPN (Virtual Private Network) / OpenWrt wiki. – 2024 [Electronic resource]. – Access mode : https://openwrt.org/docs/guide-user/services/vpn/start.

References:

1. «SoftEther VPN» (2024), *OpenWrt wiki*, [Online], available at: https://openwrt.org/docs/guide-user/services/vpn/softethervpn/start
2. Saukkonen, S. (2020), «Building a Secure VPN Infrastructure Using SoftEther VPN», [Online], available at: https://www.theseus.fi/bitstream/handle/10024/347871/Saukkonen_Samu.pdf?sequence=2
3. *SoftEther VPN Implementation Guide* (2023), [Online], available at: http://surl.li/kdcply
4. Falkovskyi, I.H. and Holovnia, O.S. (2023), «OpenWRT in a VirtualBox Virtual Environment», *Bulletin of Khmelnytskyi National University. Technical Sciences*, No. 4, pp. 358–364.
5. «VPN (Virtual Private Network)» (2024), *OpenWrt wiki*, [Online], available at: https://openwrt.org/docs/guide-user/services/vpn/start

Фальковський Ігор Геннадійович – старший викладач кафедри комп'ютерної інженерії та кібербезпеки Державного університету «Житомирська політехніка».
https://orcid.org/0009-0002-0022-1068.
Наукові інтереси:
– комп'ютерні мережі та мережні технології;
– системний та мережний моніторинг;
– технології та засоби віртуалізації;
– кібербезпека та захист інформації.
E-mail: falkovsky@ukr.net.

Воротніков Володимир Володимирович – доктор технічних наук, доцент, професор кафедри комп'ютерної інженерії та кібербезпеки Державного університету «Житомирська політехніка».
https://orcid.org/0000-0001-8584-3901.
Наукові інтереси:
– комп'ютерні мережі та мережні технології;
– мережна безпека;
– кібербезпека та захист інформації;
– керування складними інформаційними системами.
E-mail: kkik_vvv@ztu.edu.ua.

Миколайчук Вадим Володимирович – старший викладач кафедри комп'ютерної інженерії та кібербезпеки Державного університету «Житомирська політехніка».
https://orcid.org/0009-0005-2007-4570.

Наукові інтереси:
- комп'ютерні мережі та мережні технології;
- хмарні технології;
- кібербезпека та захист інформації;
- DevOps/DevSecOps.

E-mail: kkik_mvv@ztu.edu.ua.

Falkovskyi I.H., Vorotnikov V.V., Mykolaichuk V.V.

SoftEther VPN on OpenWRT in a virtual environment using VirtualBox

This article provides a comprehensive guide on installing and configuring a SoftEther VPN server on an OpenWRT platform, deployed within an Oracle VirtualBox virtual machine. It outlines the step-by-step process of setting up the virtual environment, installing the necessary packages, and configuring network settings to ensure a secure and stable VPN connection. The guide begins with an overview of OpenWRT's capabilities and the benefits of using SoftEther VPN, particularly for small businesses and individual users seeking to establish a private, encrypted network.

The article delves into the specifics of preparing the OpenWRT environment on VirtualBox, including network interface configurations, firewall adjustments, and the installation of SoftEther VPN components. It also covers the configuration of the VPN server, including user management, encryption settings, and firewall rules to secure the connection against unauthorized access. The importance of using a VPN for secure remote access to network resources is highlighted, especially in today's increasingly remote and distributed work environments.

The configuration process is presented in a clear, step-by-step manner, making it accessible even to users with limited experience in network administration. Practical tips are provided to troubleshoot common issues that may arise during the setup process, such as connectivity problems or conflicts with existing network configurations. Additionally, the article discusses best practices for maintaining and monitoring the VPN server once it is operational, ensuring ongoing security and performance.

By following this guide, readers will be equipped with the knowledge and tools needed to deploy a functional and secure SoftEther VPN server on an OpenWRT platform, enabling them to create a robust and private network solution. This can be particularly valuable for organizations looking to provide secure remote access to employees, or for individuals seeking to protect their online activities and personal data. The article concludes with a discussion on the potential scalability of this setup and suggestions for further customization based on specific user needs.

Keywords: OpenWRT; virtual machine; Oracle VirtualBox; operating system; SoftEther VPN; VPN.

Стаття надійшла до редакції 23.04.2025.