**Завдання**. Налаштувати OpenVPN server на операційній системі Windows Server, та з’єднати декілька пристроїв за допомогою налаштованого OpenVPN.

**Виконав**: 05 09

ЗМІСТ

[Встановлення служби OpenVPN сервера у Windows 2](#_Toc139528419)

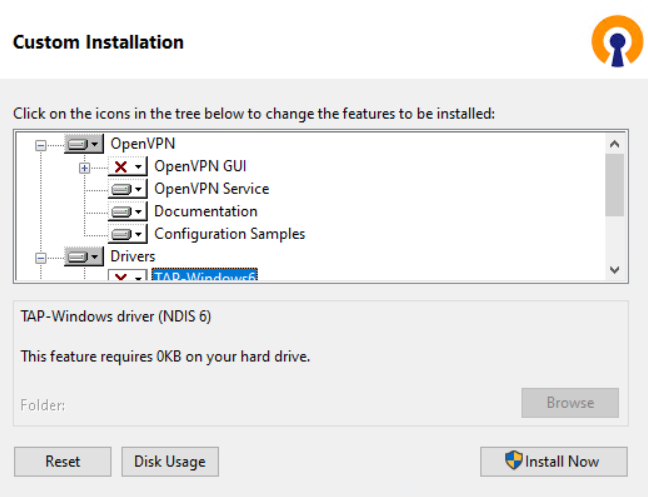
[Налаштування OpenVPN клієнта у Windows 9](#_Toc139528420)

# Встановлення служби OpenVPN сервера у Windows

Завантажте MSI інсталятор OpenVPN для вашої версії Windows з офіційного сайту (https://openvpn.net/community-downloads/). У нашому випадку це OpenVPN-2.5.5-I602-amd64.msi (https://swupdate.openvpn.org/community/releases/OpenVPN-2.5.5-I602-amd64.msi).

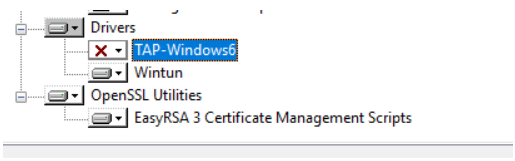
Запустіть інсталяцію.

Якщо ви плануєте, сервер OpenVPN працював в автоматичному режимі, можна не встановлювати OpenVPN GUI. Обов'язково встановіть OpenVPN Services.



Починаючи з версії OpenVPN 2.5, драйвер WinTun підтримується від розробників WireGuard. Вважається, що цей драйвер працює швидше, ніж класичний OpenVPN драйвер TAP. Встановіть драйвер Wintun, відмовтеся від установки TAP-Windows6.

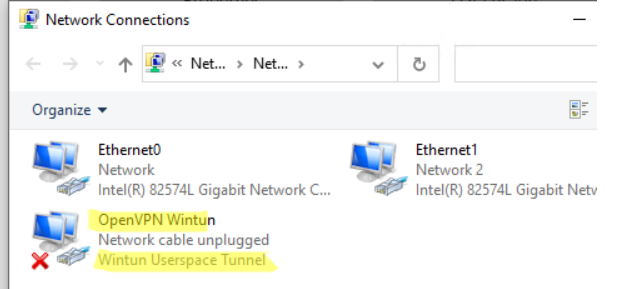
Встановіть OpenSSL утиліту EasyRSA Certificate Management Scripts.



Запустіть інсталяцію.

За промовчанням OpenVPN встановлюється до каталогу **C:\Program Files\OpenVPN**.

Після встановлення з'явиться новий адаптер типу Wintun Userspace Tunnel. Цей адаптер вимкнено, якщо служба OpenVPN не запущена.



Створюємо ключі шифрування та сертифікати для OpenVPN

OpenVPN базується на шифруванні OpenSSL. Це означає, що для обміну трафіком між клієнтом та серверами VPN потрібно згенерувати ключі та сертифікати з використанням RSA3.

Відкрийте командний рядок та перейдіть до каталогу easy-rsa:

cd C:\Program Files\OpenVPN\easy-rsa

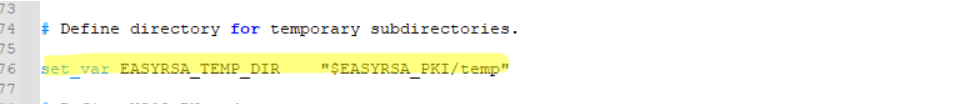
Створіть копію файлу:

copy vars.example vars

Відкрийте файл vars за допомогою будь-якого текстового редактора. Перевірте шляхи до робочих директорій.

Обов'язково виправте змінну EASYRSA\_TEMP\_DIR наступним чином:

set\_var EASYRSA\_TEMP\_DIR "$EASYRSA\_PKI/temp"



Можете заповнити поля для сертифікатів (опційно)

set\_var EASYRSA\_REQ\_COUNTRY "UA"

set\_var EASYRSA\_REQ\_PROVINCE "KYIV"

set\_var EASYRSA\_REQ\_CITY " KYIV "

set\_var EASYRSA\_REQ\_ORG "ISZZI"

set\_var EASYRSA\_REQ\_EMAIL " admin@server.vpn.ru "

set\_var EASYRSA\_REQ\_OU "IT department "

Термін дії сертифікатів задається за допомогою:

#set\_var EASYRSA\_CA\_EXPIRE 3650

#set\_var EASYRSA\_CERT\_EXPIRE 825

Збережіть файл та виконайте команду:

EasyRSA-Start.bat

Наступні команди виконуються серед EasyRSA Shell:

Ініціалізація PKI:

./easyrsa init-pki

Має з'явитися напис:

init-pki complete; you may now create a CA or requests.

Your newly created PKI dir is: C:/Program Files/OpenVPN/easy-rsa/pki

Тепер потрібно згенерувати кореневий CA:

./easyrsa build-ca

Введіть двічі пароль для CA:

“CA creation complete and you may now import і sign cert requests.”

Ця команда сформувала:

Кореневий сертифікат центру сертифікації: «C:Program FilesOpenVPNeasy-rsapkica.crt»

Ключ центру сертифікації «C:Program FilesOpenVPNeasy-rsapkiprivateca.key»

Тепер потрібно згенерувати запит сертифіката та ключ для вашого сервера OpenVPN:

./easyrsa gen-req server nopass

Утиліта згенерує два файли:

req: C:/Program Files/OpenVPN/easy-rsa/pki/reqs/server.req

key: C:/Program Files/OpenVPN/easy-rsa/pki/private/server.key

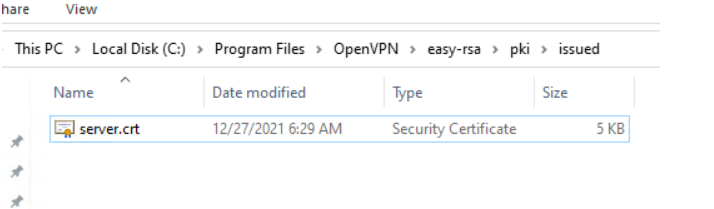
Підпишемо запит на випуск сертифіката сервера за допомогою нашого CA:

./easyrsa sign-req server server

Підтвердьте правильність даних, набравши yes.

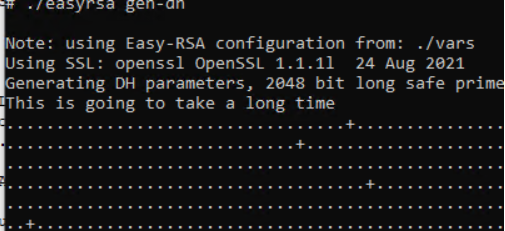
Потім введіть пароль CA від кореневого CA.

У каталозі issued з'явиться сертифікат сервера («C:\Program Files\OpenVPN\easy-rsa\pki\issued\server.crt")



Тепер можна створити ключі Діффі-Хеллмана (займе тривалий час):

./easyrsa gen-dh



Для додаткового захисту сервера VPN бажано включити tls-auth. Ця технологія дозволяє використовувати підписи HMAC до handshake-пакетів SSL/TLS, ініціюючи додаткову перевірку цілісності. Пакети без такого підпису відкидаються VPN сервером. Це захистить вас від сканування порту VPN сервера, атак DoS, переповнення буфера SSL/TLS.

Згенеруйте ключ tls-auth:

cd C:\Program Files\OpenVPN\bin

openvpn --genkey secret ta.key

Повинен з'явитися файл "C:\Program Files\OpenVPN\bin\ta.key". Перемістіть його до каталогу C:\Program Files\OpenVPN\easy-rsa\pki

Тепер можна створити ключі для клієнтів OpenVPN. Для кожного клієнта, який підключатиметься до вашого сервера, потрібно створити власні ключі.

Є кілька способів генерації ключів та передачі їх клієнтам. У наступному прикладі ми створимо на сервері ключ клієнта та захистимо його паролем:

./easyrsa gen-req slava

./easyrsa sign-req client slava



Даний ключ («C:Program FilesOpenVPNeasy-rsapkiprivateslava.key») потрібно передати клієнту і повідомити пароль. Клієнт може зняти захист паролем для ключа:

openssl rsa -in "C:\Program Files\OpenVPN\easy-rsa\pki\private\slava.key"-out "C:\Program Files\OpenVPN\easy-rsa\pki\private\slava\_use.key"

На сервері з OpenVPN можна створити необмежену кількість ключів і сертифікатів для користувачів. Аналогічно сформуйте ключі та сертфікати для інших клієнтів.

Ви можете відохвати скомпрометовані сертифікати клієнтів:

cd C:\Program Files\OpenVPN\easy-rsa

EasyRSA-Start.bat

./easyrsa revoke slava

Отже, ми згенерували набір ключів та сертифікатів для OpenVPN сервера. Тепер можна настроїти та запустити службу OpenVPN.

Конфігураційний файл OpenVPN сервера у Windows

Скопіюйте типовий конфігураційний файл OpenVPN сервера:

copy "C:Program Files\OpenVPN\sample-config\server.ovpn" "C:Program Files\OpenVPN\config-auto\server.ovpn"

Відкрийте файл server.ovpn у будь-якому текстовому редакторі та внесіть налаштування. Я використовую наступний конфіг для OpenVPN:

# Вказуємо порт, протокол та пристрій

port 1194

proto udp

dev tun

# Вказуємо шляхи до сертифікатів сервера

ca "C:\Program Files\OpenVPN\easy-rsa\pki\ca.crt"

cert "C:\Program Files\OpenVPN\easy-rsa\pki\issued\server.crt"

key "C:\Program Files\OpenVPN\easy-rsa\pki\private\server.key"

dh "C:\Program Files\OpenVPN\easy-rsa\pki\dh.pem"

# Вказуємо налаштування IP мережі, адреси з якої отримуватимуть VPN клієнти

server 10.24.1.0 255.255.255.0

#якщо потрібно дозволити клієнтам підключатися під одним ключем, потрібно включити опцію duplicate-cn (не рекомендується)

#duplicate-cn

# TLS захист

tls-auth "C:\Program Files\OpenVPN\easy-rsa\pki\ta.key" 0

cipher AES-256-GCM

# Інша параметри

keepalive 20 60

persist-key

persist-tun

status "C:\Program Files\OpenVPN\log\status.log"

log "C:\Program Files\OpenVPN\log\openvpn.log"

verb 3

mute 20

windows-driver wintun

Збережіть файл.

OpenVPN дозволяє використовувати як TCP, і UDP для підключення. У цьому прикладі я запустив OpenVPN на 1194 UDP. Рекомендується використовувати протокол UDP, оптимально як з точки зору продуктивності, так і безпеки.

Не забудьте відкрити на фаєрволі порти для вказаного вами порту OpenVPN на клієнті та сервері. Можна відкрити порти Windows Defender за допомогою PowerShell.

Правило для сервера:

New-NetFirewallRule -DisplayName "AllowOpenVPN-In" -Direction Inbound -Protocol UDP -LocalPort 1194 -Action Allow

Правило для клієнта:

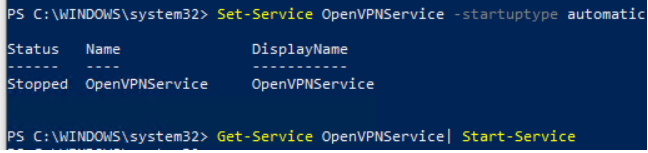
New-NetFirewallRule -DisplayName "AllowOpenVPN-Out" -Direction Outbound -Protocol UDP -LocalPort 1194 -Action Allow

Тепер потрібно запустити службу OpenVPN та змінити тип її запуску на автоматичний. Скористайтеся такими командами PowerShell, щоб увімкнути службу:

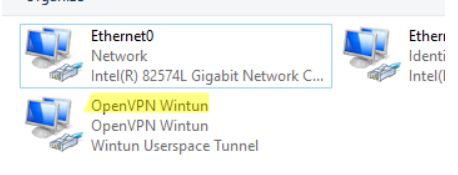
Set-Service OpenVPNService -startuptype automatic -passthru

Get-Service OpenVPNService| Start-Service

запуск служби OpenVPNService



Відкрийте панель керування і переконайтеся, що віртуальний мережний адаптер OpenVPN Wintun тепер активний. Якщо ні, дивіться лог «C:/Program Files/OpenVPN/log/server.log»



Цей конфіг дозволить видаленим клієнтам отримати доступ лише до сервера, але інші комп'ютери та сервіси в локальній мережі сервера для них недоступні. Щоб дозволити клієнтам OpenVPN отримати доступ до внутрішньої мережі, потрібно:

Включити опцію IPEnableRouter в реєстрі (включає IP маршрутизацію у Windows, у тому числі включає маршрутизацію меду мережами Hyper-V):

reg add HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters /v IPEnableRouter /t REG\_DWORD /d 1

Додайте до конфгураційного файлу сервера OpenVPN маршрути до внутрішньої IP мережі:

push "route 10.24.1.0 255.255.255.0"

push "route 192.168.100.0 255.255.255.0"

Якщо потрібно, призначте клієнту адреси серверів DNS:

push "dhcp-option DNS 192.168.100.11"

push "dhcp-option DNS 192.168.100.12"

Якщо потрібно загорнути всі запити клієнта (у тому числі Інтернет трафік) на ваш сервер OpenVPN, додайте опцію:

push "redirect-gateway def1"

# Налаштування OpenVPN клієнта у Windows

Створіть на сервері шаблонний конфігураційний файл для клієнта VPN (на базі iшаблону client.ovpn) з наступними параметрами (ім'я файлу kbuldovov.ovpn)

client

dev tun

proto udp

remote your\_vpn\_server\_address 1194

resolv-retry infinite

nobind

persist-key

persist-tun

ca ca.crt

cert kbuldogov.crt

key kbuldogov.key

remote-cert-tls server

tls-auth ta.key 1

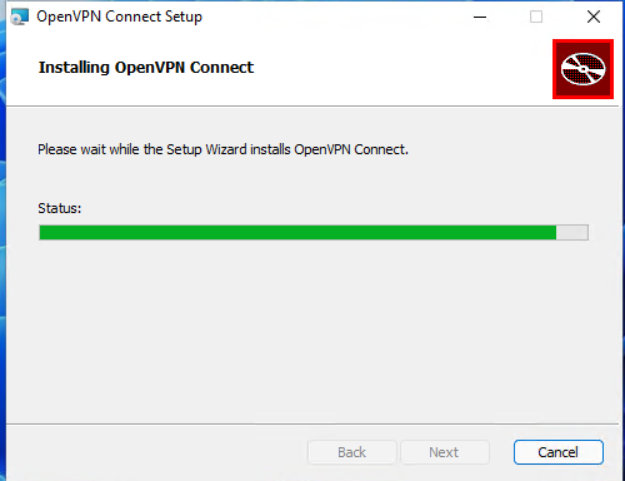
cipher AES-256-GCM

connect-retry-max 25

verb 3

У директиві remote вказується публічна IP-адреса або DNS ім'я вашого сервера OpenVPN.

Завантажте та встановіть клієнт OpenVPN Connect для Windows (<https://openvpn.net/downloads/openvpn-connect-v3-windows.msi>).



Тепер на комп'ютер із клієнтом OpenVPN потрібно з сервера скопіювати файли:

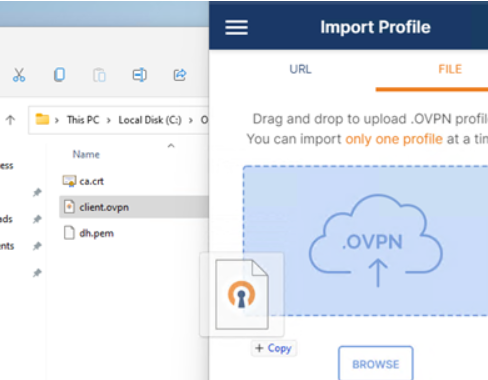
ca.crt

slava.crt

slava.key

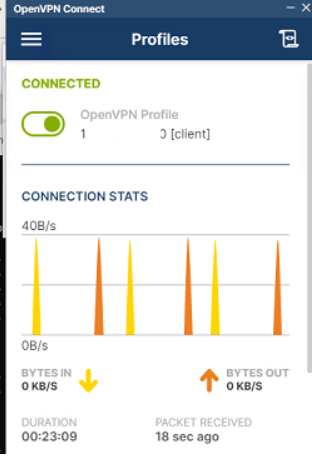
dh.pem

client.ovpn



Тепер імпортуйте файл із профілем \*.ovpn і спробуйте підключитися до вашого VPN сервера.

Якщо все налаштовано правильно, з'явиться таке зображення.



Перевірте тепер лог OpenVPN на клієнті "C:\Program Files\OpenVPN Connect\agent.log"

Mon Dec 27 08:09:30 2021 proxy\_auto\_config\_url

Mon Dec 27 08:09:31 2021 TUN SETUP

TAP ADAPTERS:

guid='{25EE4A55-BE90-45A0-88A1-8FA8FEF24C42}' index=22 name='Local Area Connection'

Open TAP device "Local Area Connection" PATH="\\.\Global\{25EE4A55-BE90-45A0-88A1-8FA8FEF24C42}.tap" SUCCEEDED

TAP-Windows Driver Version 9.24

ActionDeleteAllRoutesOnInterface iface\_index=22

netsh interface ip set interface 22 metric=1

Ok.

netsh interface ip set address 22 static 10.24.1.6 255.255.255.252 gateway=10.24.1.5 store=active

IPHelper: add route 10.24.1.1/32 22 10.24.1.5 metric=-1

Клієнт успішно підключиться до OpenVPN сервера та отримав IP адресу 10.24.1.6.

Перевірте тепер лог на сервері ("C:\Program Files\OpenVPN\log\openvpn.log"). Тут також видно, що клієнт із сертифікатом kbuldogov успішно підключиться до вашого сервера.

2021-12-27 08:09:35 192.168.13.202:55648 [kbuldogov] Peer Connection Initiated with [AF\_INET6]::ffff:192.168.13.202:55648

2021-12-27 08:09:35 kbuldogov/192.168.13.202:55648 MULTI\_sva: pool returned IPv4=10.24.1.6, IPv6=(Not enabled)

2021-12-27 08:09:35 kbuldogov/192.168.13.202:55648 MULTI: Learn: 10.24.1.6 -> kbuldogov/192.168.13.202:55648

2021-12-27 08:09:35 kbuldogov/192.168.13.202:55648 MULTI: primary virtual IP for kbuldogov/192.168.13.202:55648: 10.24.1.6