Projekt z przedmiotu:

Urządzenia Teleinformatyki

Instrukcja:

Mikrotik VPN – Wireguard

Kraków, 15 maja 2023

Sprawozdanie wykonali:

Aleksander Dodov

Adam Rzepka

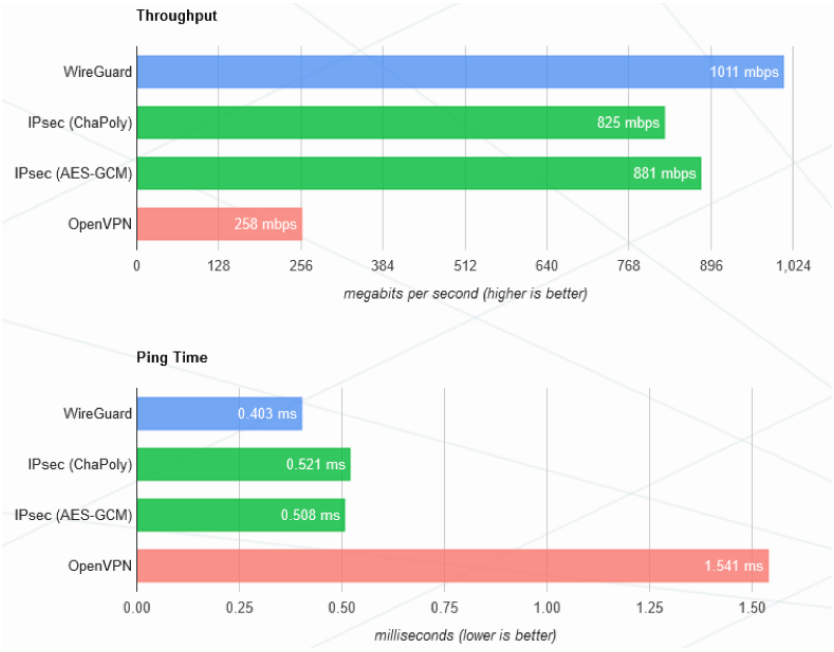
Prowadzący: dr inż. **Jacek Stępień**

1. Wprowadzenie

WireGuard to nowoczesny, otwarto źródłowy, protokół VPN. WireGuard jest zaprojektowany w celu zapewnienia prostoty, wydajności i bezpieczeństwa. Dzięki swojej minimalistycznej architekturze, WireGuard jest łatwy do konfiguracji i obsługi, a jednocześnie oferuje znakomitą wydajność, co czyni go atrakcyjnym rozwiązaniem dla zarówno indywidualnych użytkowników, jak i przedsiębiorstw. WireGuard został zaprojektowany z myślą o zastąpieniu starszych protokołów VPN, takich jak PPTP, SSTP, OpenVPN czy te oparte o IPSec.

Zalety Wireguard:

- Dzięki wykorzystaniu mechanizmu par kluczy prywatny/publiczny oraz algorytmowi szyfrowania ChaCha20-Poly1305, Wireguard pod względem bezpieczeństwa nie ustępuje rozwiązaniom opartym o certyfikaty i AES, czy IKE i IPSec..
- Bardzo dużą zaletą Wireguard jest wydajność, Wspomniane wyżej algorytmy szyfrowania sprawnie działają również bez sprzętowej akceleracji, a architektura oprogramowania zapewnia znacznie mniejsze opóźnienia i narzut oraz bezproblemowe funkcjonowanie również w niestabilnych sieciach (np. komórkowych).
- Minimalistyczny kod źródłowy. Wireguard, napisany w C, został zaimplementowany jako moduł jądra linuxa w marcu 2020 (kernel 5.6). Ma zaledwie ~4 000 linijek kodu w porównaniu do OpenVPN-a który ma ~70 000 linijek.



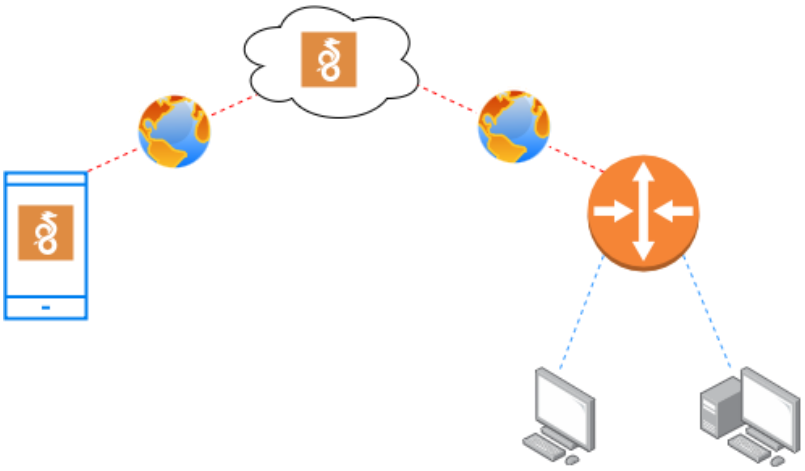
Wady Wireguard:

- Minimalna liczba funkcji, brak dynamicznego przydzielania adresów IP, dynamicznego split-routingu.
- Obsługa tylko UDP.
- W systemach takich jak Windows/Android/MacOS/IOS wymagana aplikacja

2. Konfiguracja Wireguard VPN na routerach MikroTik

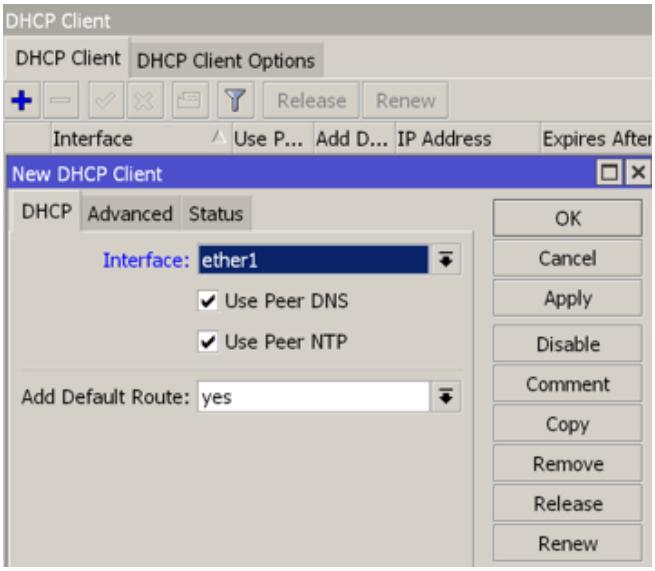
Celem ćwiczenia jest Wireguard VPN w mieszanym scenariusz (RoadWarrior/Remote access to Lan). Konfiguracja opierać będzie się o serwer Wireguard umieszczony w chmurze. Pozwoli ona na elastyczną konfiguracje, niezależną od dostępności publicznych adresów IP.
Dzięki temu możliwe będzie uzyskanie dostępu do urządzeń wewnątrz sieci lokalnej zarówno z telefonu jak i innej sieci lokalnej.

Topologia ćwiczenia:



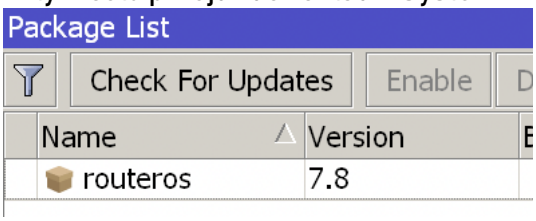
a) DHCP client na WAN

Podłącz router do Internetu na interfejsie ether1
Ustaw router, aby pobierał adres z serwera DHCP na tym interfejsie
IP -> DHCP Client -> +



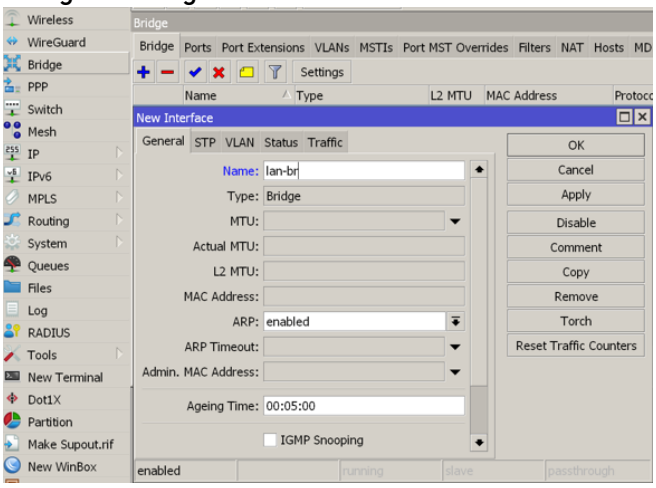
W ramach laboratorium w celu dostępu do sieci WAN wykorzystamy DHCP-Client.
Ważną opcją jest zaznaczenie Add Default Route – yes

b) Upewnij się, że twoje urządzenie ma aktualną wersję systemu RouterOS.
W tym celu przejdź do zakładki System -> Packages i zweryfikuj wersję oprogramowania:

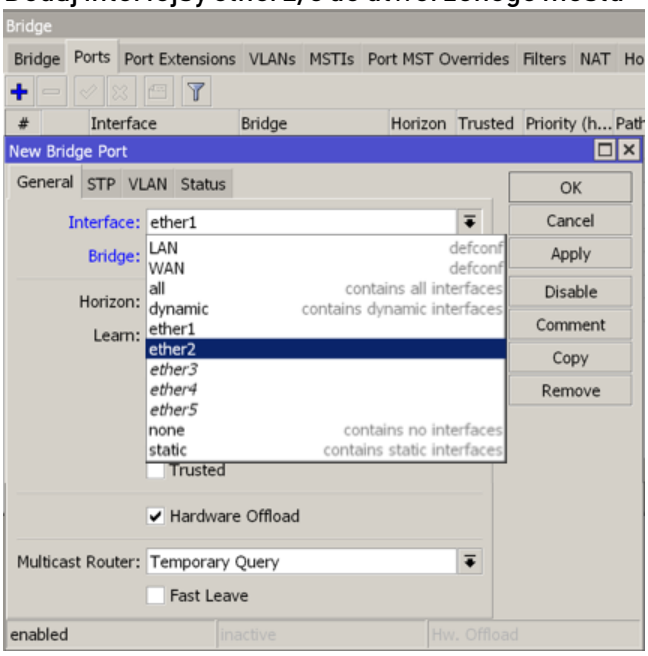


Jeżeli twoje urządzenie nie jest aktualnie, to wybierzcie opcję
„Check four updates" branch -> stable i Download&Install

c) Lan-br
Utwórz most lan-br
Bridge -> Bridge -> +



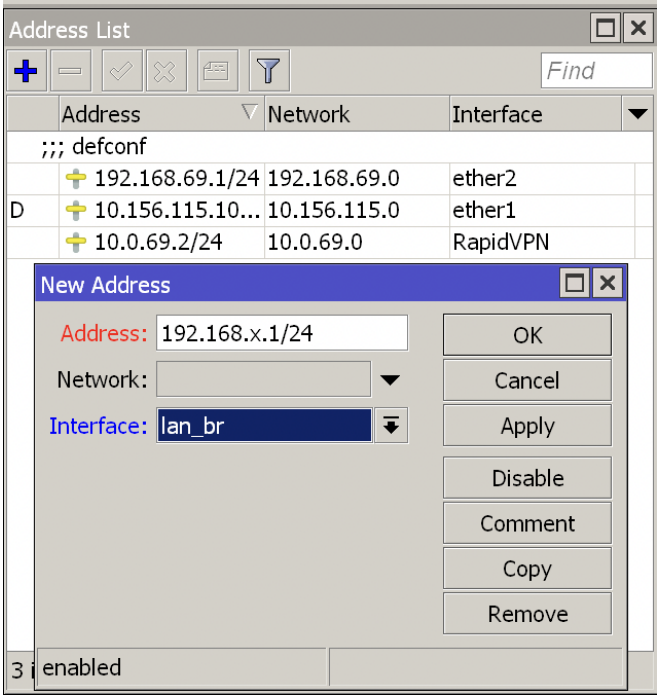
Dodaj interfejsy ether2/3 do utworzonego mostu



d) Dodaj Address listę

IP -> Address List -> +

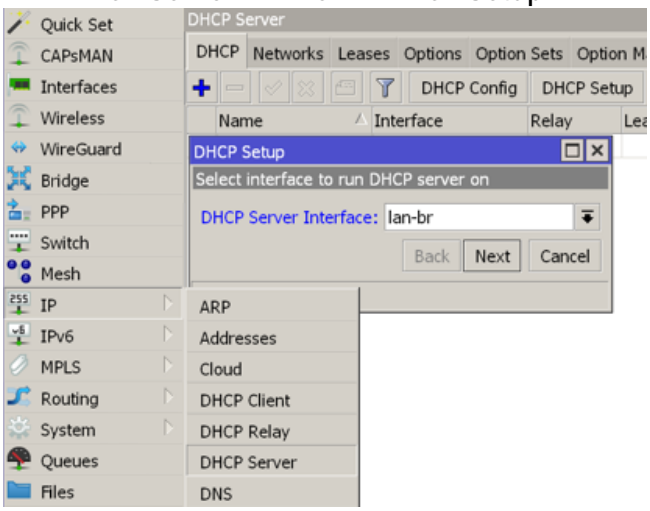
Dodaj adres 192.168.x.1/24 gdzie x to numer twojej grupy na utworzonym interfejsie **bridge**



e) serwer DHCP

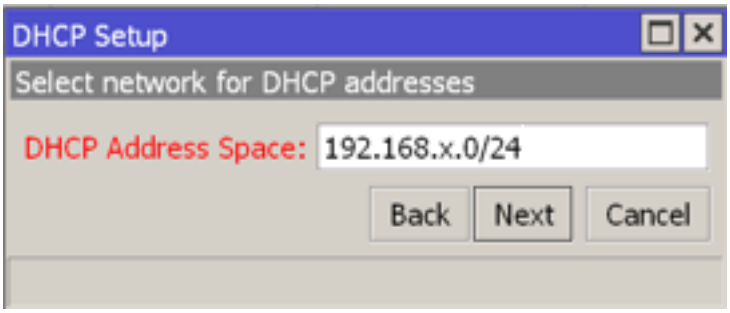
Skonfiguruj DHCP na lan-br

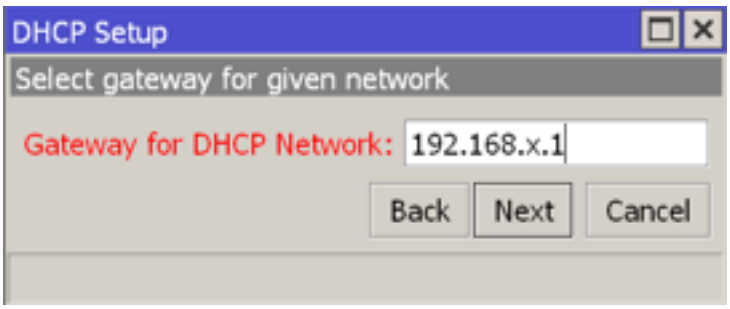
IP -> DHCP Server -> DHCP -> DHCP Setup

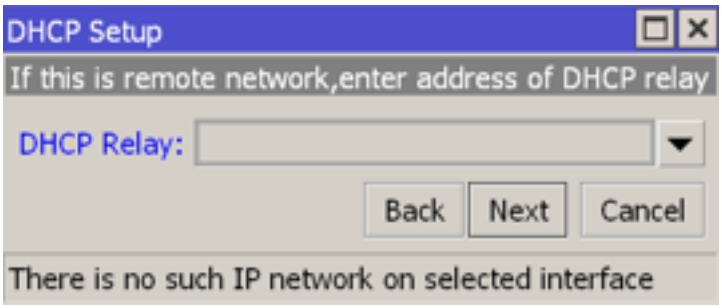


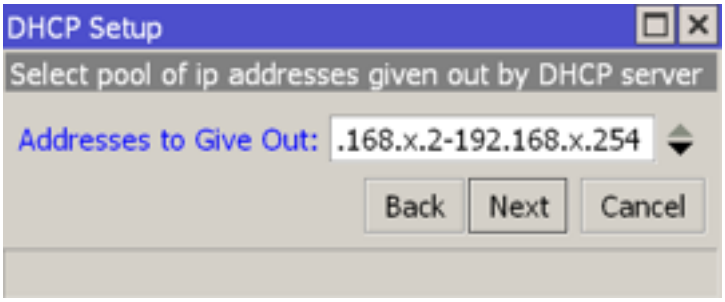
Przejdź po kolei przez konfigurator

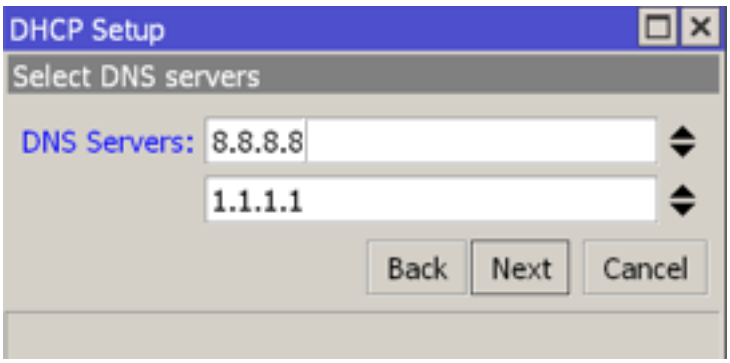
Zastąp „x” numerem swojej grupy

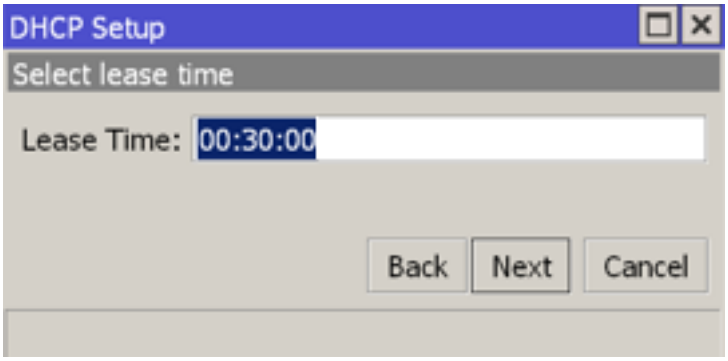

DHCP Setup
Select network for DHCP addresses
DHCP Address Space: 192.168.x.0/24
Back
Next
Cancel


DHCP Setup
Select gateway for given network
Gateway for DHCP Network: 192.168.x.1
Back
Next
Cancel


DHCP Setup
If this is remote network,enter address of DHCP relay
DHCP Relay:
Back
Next
Cancel
There is no such IP network on selected interface


DHCP Setup
Select pool of ip addresses given out by DHCP server
Addresses to Give Out: .168.x.2-192.168.x.254
Back
Next
Cancel

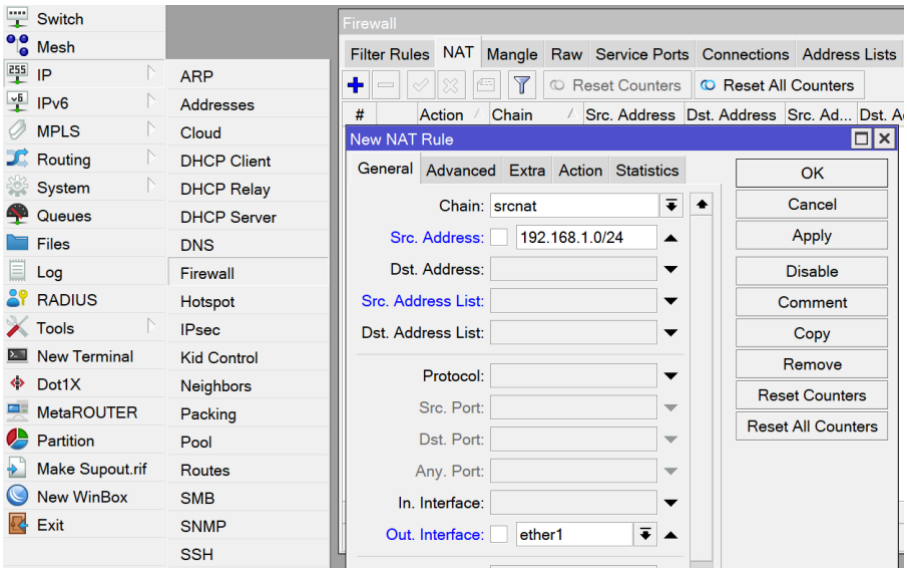

DHCP Setup
Select DNS servers
DNS Servers: 8.8.8.8
1.1.1.1
Back
Next
Cancel

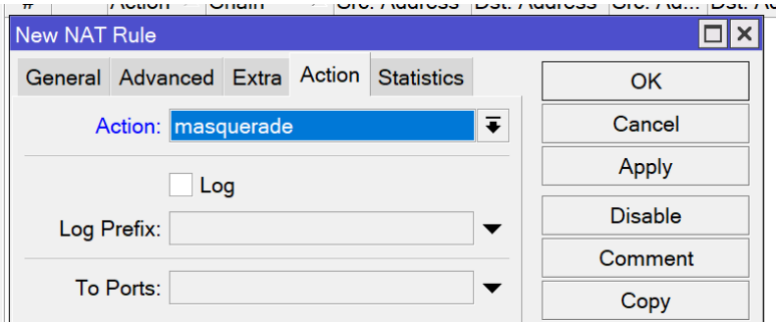


f) NAT

Następnym elementem jaki powinniśmy skonfigurować jest translacja adresów. Adres źródłowy to nasza sieć LAN. Interfejs wychodzący to nasz interfejs WAN (w naszym przypadku eth1). W zakładce Action wybieramy opcje masquerade.

IP -> Firewall -> NAT -> +





3. Konfiguracja Wireguard:
   Pobierz pliki konfiguracyjne dla serwera oraz klienta wireguard:

Pliki konfiguracyjne:

Grupa 1

Grupa 2

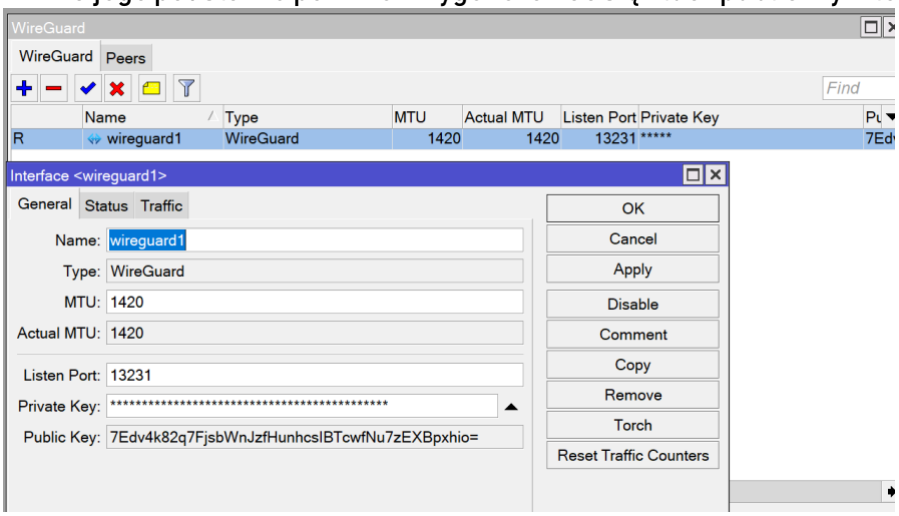
Grupa 3

Grupa 4

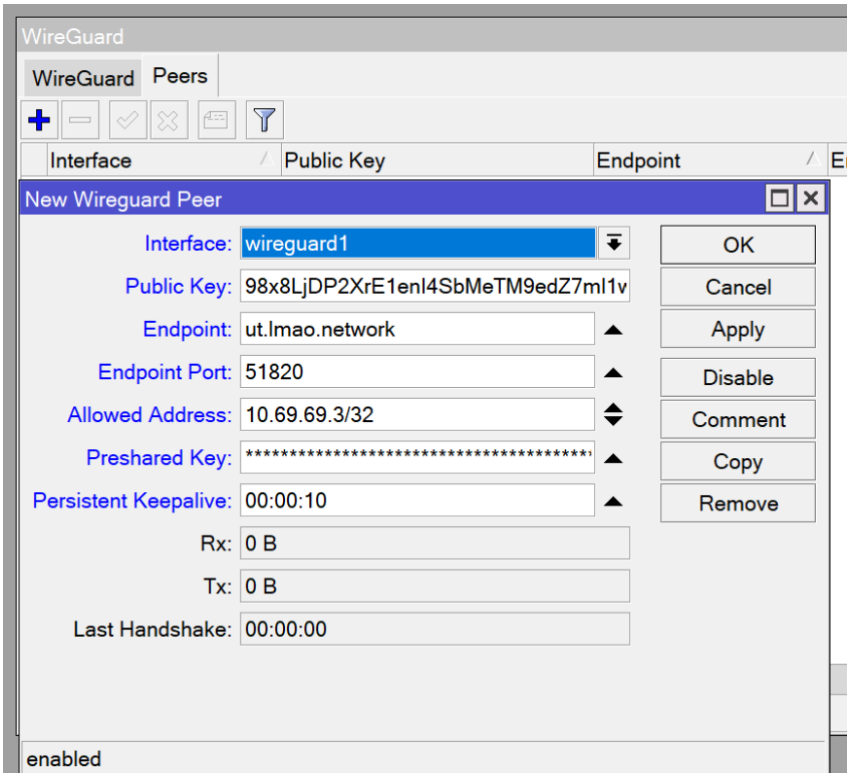
Grupa 5

a) Wypakuj pobrany przez Ciebie wcześniej plik Grupa_x.zip
Otworz plik Grupa_x_router.conf za pomocą wybranego edytora tekstu (np. Notepad++)

b) Dodaj nowy interfejs Wireguard
   Wireguard -> wireguard -> +
   Przekopiuj z pliku konfiguracjnego private key
   Na jego podstawie powinien wygenerować się klucz publiczny interfejsu



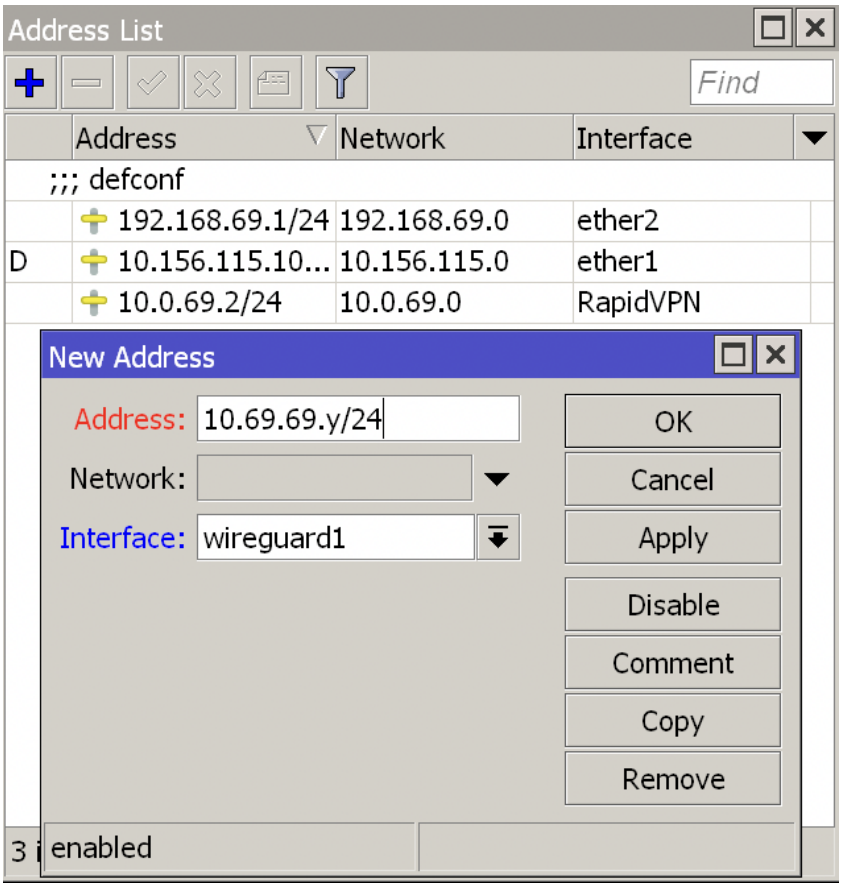
c) Dodaj nowego peer-a
   Wireguard -> Peers -> +
   Wybierz utworzony interfejs wireguard1 w „Name:”
   Przekopiuj z pliku konfiguracjnego wartości:
   a. Public Key
   b. Endpoint
   c. Endpoint Port
   d. Allowed Address
   e. Preshared Key
   f. Persistent Keepalive



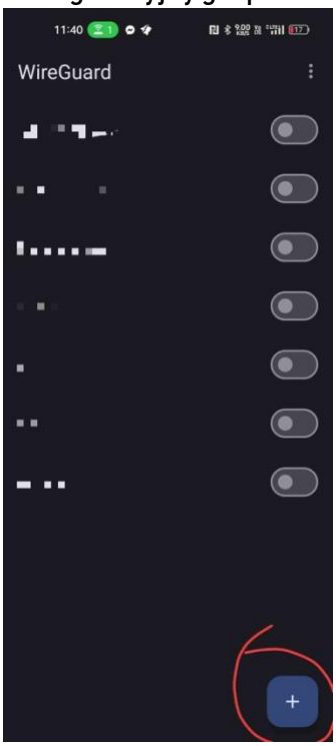
d) Dodaj Address listę

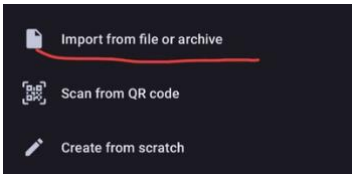
IP -> Address List -> +

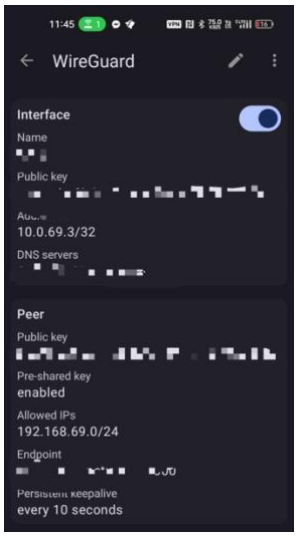
10.69.69.y/24 gdzie y to ostatni oktet adresu konfiguracji dla twojego routera:



4. Sprawdź poprawność i przetestuj sprawność tunelu VPN
    a. Pobierz aplikację na telefon/laptop
    https://www.wireguard.com/install/
    b. Pobierz aplikację „termux" lub „PingTools" w celu diagnostyki dostępu do sieci
    c. W aplikacji Wireguard dodaj pobrany przez Ciebie w punkcie 3 a) plik konfiguracyjny grupa-x-clinet.conf







e) Ping
    a. Przejdź do aplikacji, która pozwoli Ci na użycie komendy ping.
    b. Spróbuj odpytać adresy IP routera oraz urządzenia wewnątrz sieci 192.168.x.0/24
    c. Jeżeli komenda ping się nie wykona poprawnie zawołaj prowadzącego