

Server OpenVPN, zdalny dostęp do sterownika PLC, Dynamiczny DNS

Informator Techniczny Teltonika nr 1 – Routery RUT

23.09.2019 r.

UWAGA!

Przed przystąpieniem do konfiguracji należy pamiętać:

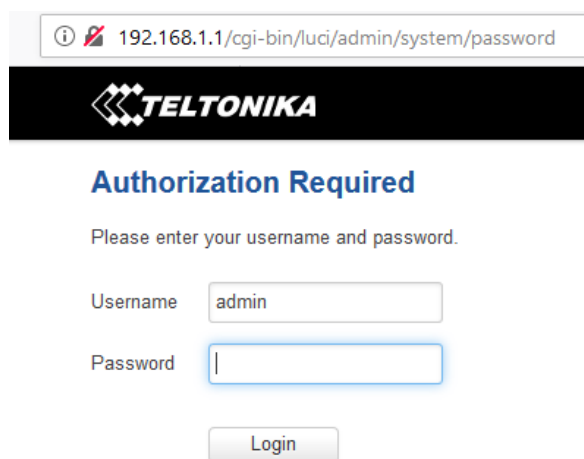
- 1) Karta SIM musi posiadać **publiczny** (statyczny lub dynamiczny) adres IP. Więcej o prywatnych i publicznych adresach na: https://wiki.teltonika.lt/view/Private_and_Public_IP_Addresses.
- 2) Przedstawiona poniżej instrukcja jest jedynie przykładem konfiguracji. Wszystkie parametry (adresy IP, maski podsieci, APN, itd.) należy przystosować do własnej konfiguracji sprzętowej.

Dodatkowe informacje:

- Zaleca się aktualizację Firmware do najnowszej dostępnej wersji dla danego urządzenia (dostępne na: https://wiki.teltonika.lt/view/Network_products lub przez WebUI routera w zakładce system -> Firmware)

PODSTAWOWA KONFIGURACJA ROUTERA

Kablem Ethernet podłącz komputer do Routera. Następnie w polu adresu przeglądarki wpisz adres IP routera (domyślnie 192.168.1.1).



Zaloguj się do WebUI (domyślnie Username: „admin”, hasło: „admin01”).

Przy pierwszym logowaniu konieczna będzie zmiana domyślnego hasła.

You haven't changed the default password for this router.

Change password

You must change password to leave this page! Password requirements: Minimum 8 characters, at least one uppercase letter, one lowercase letter and one number.

Administrator Password

New password

Confirm new password

Save

W pierwszym kroku kreatora konfiguracji wybierz odpowiednią strefę czasową (dodatkowo możesz zsynchronizować czas z przeglądarką internetową komputera lub lokalizatorem GPS).

Step 1 - General Step 2 - Mobile Step 3 - LAN Step 4 - WiFi Step 5 - RMS

Step - General

Please select your timezone.

Time Zone Settings

Current system time 2019-09-23 08:24:53 Sync with GPS Sync with browser

Time zone Europe/Warsaw

Skip Wizard Next

W drugim kroku skonfiguruj połączenie mobilne. Wpisz APN oraz metodę potwierdzenia autentyczności, które pozwolą na przypisanie **publicznego adresu IP (!)**, kod PIN karty oraz (opcjonalnie) numer telefonu.

Step 1 - General **Step 2 - Mobile** Step 3 - LAN Step 4 - WiFi Step 5 - RMS

Mobile Configuration

Next, let's configure your mobile settings so you can start using internet right away.

Mobile Configuration (SIM1)

APN pro.plusgsm.pl ☐ Auto

PIN number 9628

Dialing number *99#

MTU 1500

Authentication method None

Service mode Automatic

Show mobile info at login page ☐

Skip Wizard Next

W kolejnym kroku wpisz adres IP routera w sieci wewnętrznej (pamiętaj, aby router znajdował się w tej samej podsieci, co urządzenia, z którymi będzie się łączył) oraz maskę podsieci. DHCP pozostaw włączone oraz określ limit dynamicznie przydzielanych adresów IP.

Step 1 - General **Step 2 - Mobile** **Step 3 - LAN** **Step 4 - WiFi** **Step 5 - RMS**

Step - LAN

Here we will setup the basic settings of a typical LAN configuration. The wizard will cover 2 basic configurations: static IP address LAN and DHCP client.

General configuration

IP address

192.168.1.1

Netmask

255.255.255.0

Enable DHCP

☒

Start

100

Limit

150

Lease time

12

Hours

▼

Start IP address:

192.168.1.100

End IP address:

192.168.1.250

Skip Wizard

Next

Krok 4 (opcjonalny): konfiguracja WiFi. Skonfiguruj nazwę Punktu Dostępowego, tryb, kanał, szyfrowanie oraz klucz według potrzeb.

Step 1 - General **Step 2 - Mobile** **Step 3 - LAN** **Step 4 - WiFi** **Step 5 - RMS**

Step - Wireless

Now let's configure your wireless radio. (Note: if you are currently connecting via wireless and you change parameters, like SSID, encryption, etc. your connection will be dropped and you will have to reconnect with a new set of parameters.)

WiFi Configuration

Enable wireless

☒

SSID

RUT955_AMC

Mode

802.11g+n

▼

Channel

Auto

▼

Encryption

WPA2-PSK

▼

Cipher

Force TKIP and CCMP (AES)

▼

Key

••••••••

👁

Country Code

PL - Poland

▼

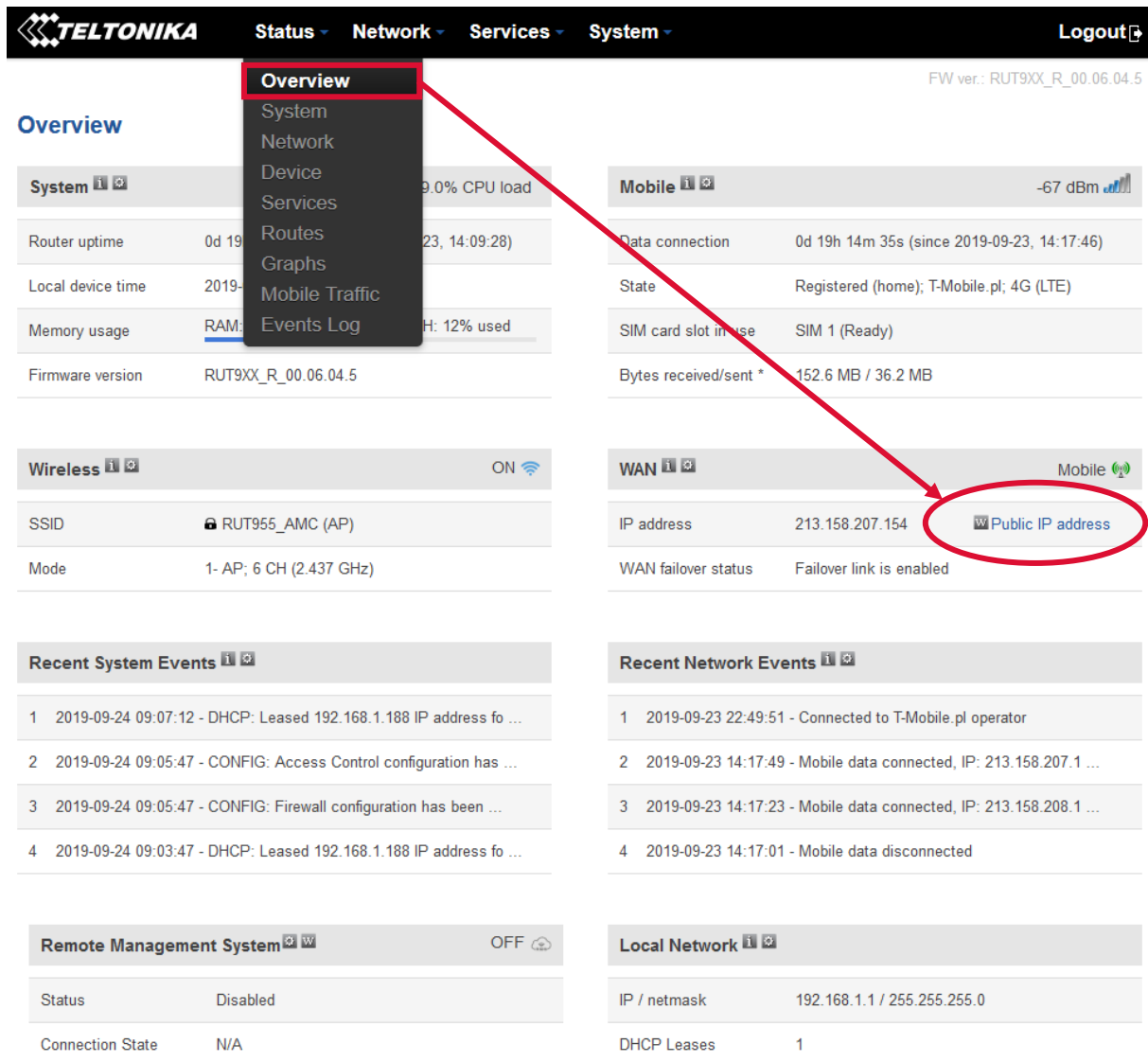
Skip Wizard

Next

Ostatnim krokiem jest aktywacja licencji **RMS**. Aby dowiedzieć się więcej o systemie zdalnego zarządzania odwiedź www.rms.teltonika.lt lub skontaktuj się z amc@astor.com.pl.

KONFIGURACJA SERVERA OPENVPN

Upewnij się, że router posiada publiczny adres IP w zakładce Status -> Overview



TELTONIKA Status Network Services System Logout

FW ver.: RUT9XX_R_00.06.04.5

Overview

System 9.0% CPU load

Router uptime	0d 19h 14m 35s (since 2019-09-23, 14:09:28)
Local device time	2019-09-24 09:05:47
Memory usage	RAM: 12% used
Firmware version	RUT9XX_R_00.06.04.5

Mobile -67 dBm

Data connection	0d 19h 14m 35s (since 2019-09-23, 14:17:46)
State	Registered (home); T-Mobile.pl; 4G (LTE)
SIM card slot in use	SIM 1 (Ready)
Bytes received/sent *	152.6 MB / 36.2 MB

Wireless ON

SSID	RUT955_AMC (AP)
Mode	1- AP; 6 CH (2.437 GHz)

WAN Mobile

IP address	213.158.207.154 Public IP address
WAN failover status	Failover link is enabled

Recent System Events

- 2019-09-24 09:07:12 - DHCP: Leased 192.168.1.188 IP address for ...
- 2019-09-24 09:05:47 - CONFIG: Access Control configuration has been ...
- 2019-09-24 09:05:47 - CONFIG: Firewall configuration has been ...
- 2019-09-24 09:03:47 - DHCP: Leased 192.168.1.188 IP address for ...

Recent Network Events

- 2019-09-23 22:49:51 - Connected to T-Mobile.pl operator
- 2019-09-23 14:17:49 - Mobile data connected, IP: 213.158.207.1 ...
- 2019-09-23 14:17:23 - Mobile data connected, IP: 213.158.208.1 ...
- 2019-09-23 14:17:01 - Mobile data disconnected

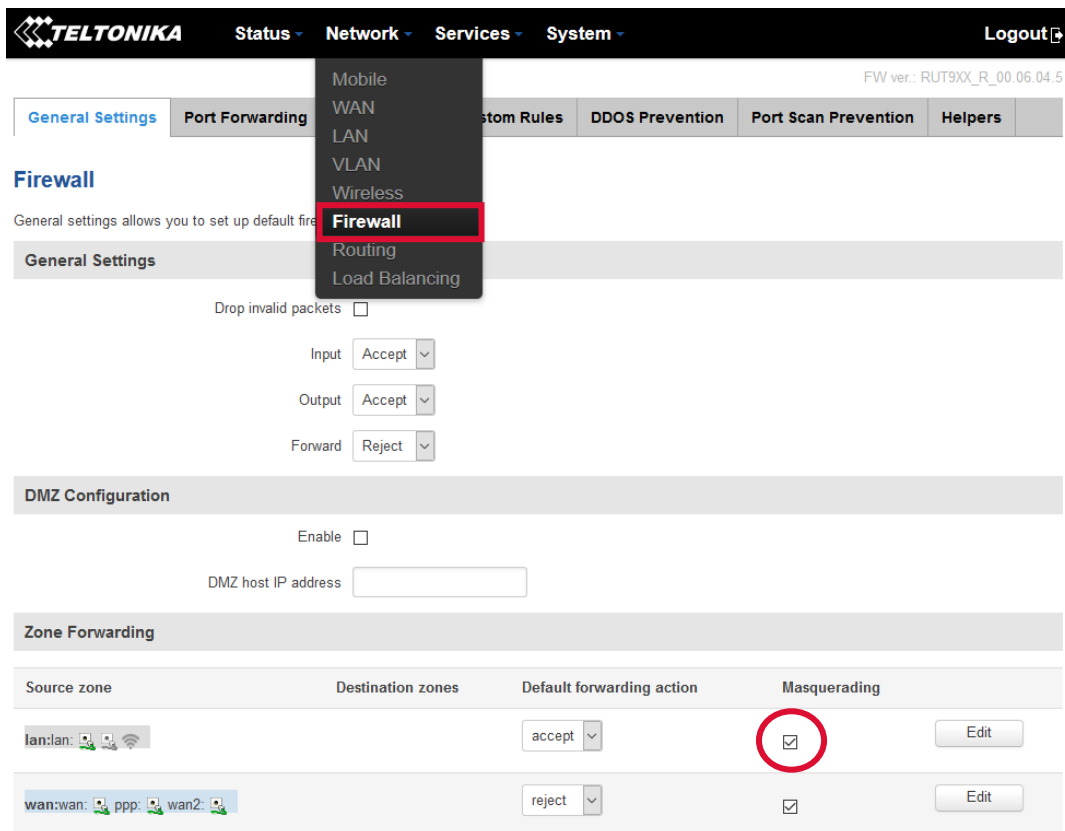
Remote Management System OFF

Status	Disabled
Connection State	N/A

Local Network

IP / netmask	192.168.1.1 / 255.255.255.0
DHCP Leases	1

Aby pozwolić na zdalne połączenie się do sieci routera należy włączyć Maskaradę sieci LAN w zakładce Network -> Firewall.



TELTONIKA Status Network Services System Logout

FW ver.: RUT9XX_R_00.06.04.5

General Settings Port Forwarding Custom Rules DDOS Prevention Port Scan Prevention Helpers

Firewall

General settings allows you to set up default firewall rules.

General Settings

Drop invalid packets ☐

Input: Accept

Output: Accept

Forward: Reject

DMZ Configuration

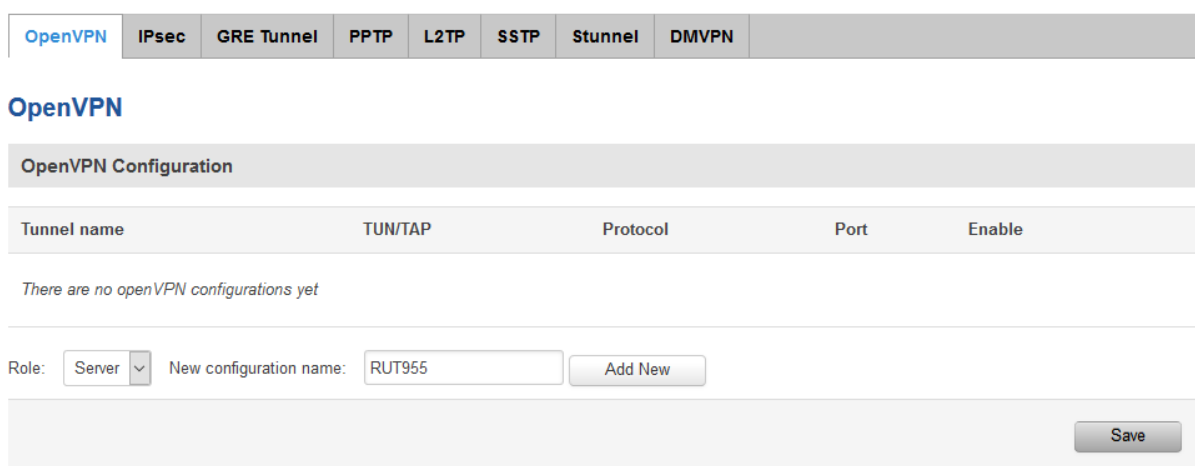
Enable ☐

DMZ host IP address:

Zone Forwarding

Source zone	Destination zones	Default forwarding action	Masquerading	
lan:lan		accept	☒	Edit
wan:wan	ppp, wan2	reject	☒	Edit

Przejdź do zakładki Services -> VPN. Wybierz rolę „Server” oraz nadaj nazwę Servera OpenVPN. Dodaj instancję przyciskiem „Add New”.



OpenVPN IPsec GRE Tunnel PPTP L2TP SSTP Stunnel DMVPN

OpenVPN

OpenVPN Configuration

Tunnel name	TUN/TAP	Protocol	Port	Enable
There are no openVPN configurations yet				

Role: Server New configuration name: RUT955 Add New

Save

Parametry Servera:

- 1) TUN/TAP
 - a. **TUN** – połączenie tunelowe
 - b. **TAP** – połączenie mostkowe
- 2) Protokół
 - a. **UDP** – większa prędkość transmisji, wymaga mniej zasobów, brak pewności przesłania każdego z pakietów
 - b. **TCP** – mniejsza prędkość transmisji, wymaga dużej ilości zasobów, pewność przesłania każdego pakietu
- 3) Port (**1194**) – port wykorzystywany do połączenia VPN.
- 4) LZO (**ON**) – algorytm bezstratnej kompresji danych. Z kompresją danych połączenie VPN spowoduje mniejsze obciążenie sieci.
- 5) Encryption (**BF-CBC 128**) – algorytm szyfrowania danych. Zależnie od wybranego algorytmu i długości klucza możesz manipulować stosunkiem poziomu bezpieczeństwa do prędkości transmisji.
- 6) Authentication (**TLS**) – metoda potwierdzenia autentyczności.
- 7) Keep alive (**10 120**) – parametr utrzymywania połączenia. Pierwsza wartość określa interwał wysyłania zapytania „Ping”. Druga wartość określa czas oczekiwania Klienta na odpowiedź. Po przekroczeniu określonego czasu Klient przystąpi do ponownego nawiązania połączenia. Wartości 10 120 są ustawieniem domyślnym i stosunkowo uniwersalnym. Parametr dostosuj do własnych potrzeb.
- 8) Virtual network IP address (**10.0.0.0**) – IP wirtualnej sieci VPN.
- 9) Virtual network netmask (**255.255.255.0**) – maska wirtualnej podsieci VPN.
- 10) Push option – opcje przekazywane każdemu połączonemu klientowi OpenVPN, np. „route 192.168.1.0 255.255.255.0” zezwoli na przekierowanie do sieci lokalnej 192.168.1.0 przez server OpenVPN (t.j. zdalny dostęp do sieci przez tunel VPN).

Main Settings

Enable ☒

TUN/TAP TUN (tunnel) ▼

Protocol UDP ▼

Port

LZO ☒

Encryption BF-CBC 128 (default) ▼

Authentication TLS ▼

TLS cipher All ▼

Client to client ☐

Keep alive

Virtual network IP address

Virtual network netmask

Push option 

GENEROWANIE CERTYFIKATÓW/KLUCZY TLS

Dokładny poradnik generowania kluczy krok po kroku znajduje się pod adresem [https://wiki.teltonika.lt/view/How_to_generate_TLS_certificates_\(Windows\)%3F](https://wiki.teltonika.lt/view/How_to_generate_TLS_certificates_(Windows)%3F).

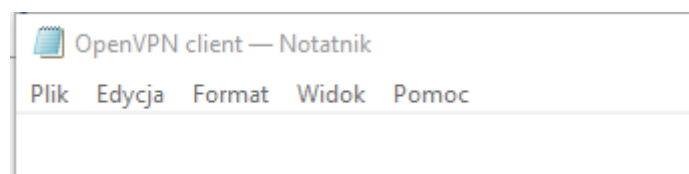
Po wygenerowaniu wszystkich plików dołącz je do konfiguracji serwera OpenVPN

Certificate authority	Przeglądaj...	ca.crt
Server certificate	Przeglądaj...	server.crt
Server key	Przeglądaj...	server.key
Diffie Hellman parameters	Przeglądaj...	dh2048.pem
CRL file (optional)	Przeglądaj...	Nie wybrano pliku.

Po wypełnieniu wszystkich pól konfiguracji i dołączeniu plików TLS zatwierdź ustawienia przyciskiem Save.

KONFIGURACJA KLIENTA OPENVPN

Stwórz dokument tekstowy w wybranej przez siebie lokalizacji oraz rozpocznij jego edycję.



Będzie to plik konfiguracyjny klienta OpenVPN. Wypełnij plik poniższym tekstem:

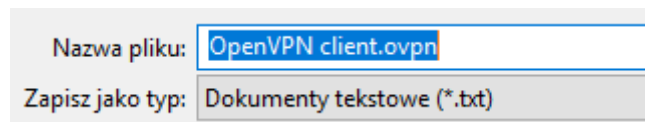
```
client
dev tun
proto udp4
remote 213.158.208.138 1194
ca "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\ca.crt"
cert "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\Client1.crt"
key "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\Client1.key"
keepalive 10 120
persist-key
persist-tun
cipher BF-CBC
comp-lzo
verb 7
```

Przedstawiona konfiguracja klienta jest poprawna jedynie przy ustawieniach Servera prezentowanych w punkcie „Konfiguracja Servera OpenVPN”. W tym momencie należy odpowiednio zmienić ustawienia klienta tak, aby odpowiadały one ustawieniom Servera.

Linia „remote IP port” odnosi się do adresu IP WAN Servera oraz portu. Adres sprawdź w zakładce Status -> Overview w polu „WAN”.

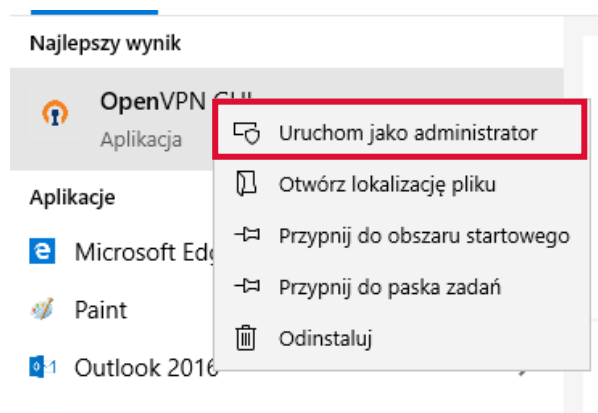
Linie: „ca”, „cert”, „key” odnoszą się do wcześniej wygenerowanych plików TLS. Wpisz odpowiednią lokalizację plików na swoim komputerze.

Gdy plik jest gotowy wybierz opcję Plik -> Zapisz jako... . Do nazwy pliku dołącz końcówkę „.ovpn”, aby plik został zapisany w odpowiednim formacie.

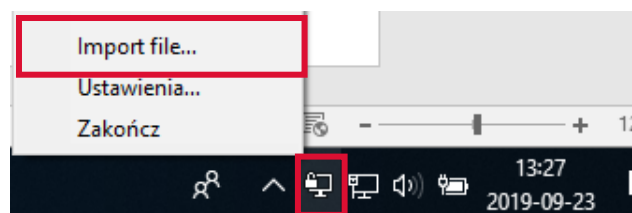


ŁĄCZENIE Z SERVEREM OPENVPN

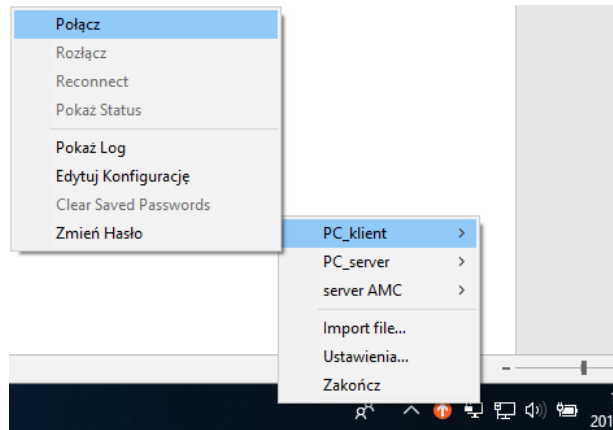
Uruchom OpenVPN GUI jako **administrator**.



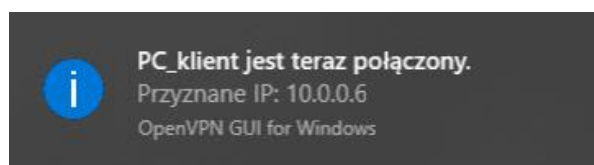
W prawym dolnym rogu paska zadań pojawi się ikona graficznego interfejsu użytkownika OpenVPN. Prawym przyciskiem myszy rozwiń opcje, wybierz „Import file” oraz odszukaj stworzony plik konfiguracyjny klienta OpenVPN.



Po zaimportowaniu pliku połącz się z Serverem.



Proces łączenia z Serverem zakończy się komunikatem o przyznaniu IP wirtualnej sieci.



Ostatnim krokiem jest przetestowanie połączenia komendami ping. Testy rozpocznij od Servera wirtualnej sieci (10.0.0.1), następnie lokalnego IP routera (192.168.1.1), a następnie urządzeń w sieci, do których chcesz mieć zdalny dostęp (np. 192.168.1.128).

```
C:\Users\lukasz>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time=79ms TTL=64
Reply from 10.0.0.1: bytes=32 time=81ms TTL=64
Reply from 10.0.0.1: bytes=32 time=102ms TTL=64
Reply from 10.0.0.1: bytes=32 time=92ms TTL=64

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 79ms, Maximum = 102ms, Average = 88ms

C:\Users\lukasz>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=69ms TTL=64
Reply from 192.168.1.1: bytes=32 time=77ms TTL=64
Reply from 192.168.1.1: bytes=32 time=73ms TTL=64
Reply from 192.168.1.1: bytes=32 time=88ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 69ms, Maximum = 88ms, Average = 76ms

C:\Users\lukasz>ping 192.168.1.128

Pinging 192.168.1.128 with 32 bytes of data:
Reply from 192.168.1.128: bytes=32 time=69ms TTL=63
Reply from 192.168.1.128: bytes=32 time=71ms TTL=63
Reply from 192.168.1.128: bytes=32 time=74ms TTL=63
Reply from 192.168.1.128: bytes=32 time=91ms TTL=63

Ping statistics for 192.168.1.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 69ms, Maximum = 91ms, Average = 76ms
```

DYNAMICZNY DNS – DLA KART SIM Z DYNAMICZNYM ADRESEM IP

1. DNS i DDNS

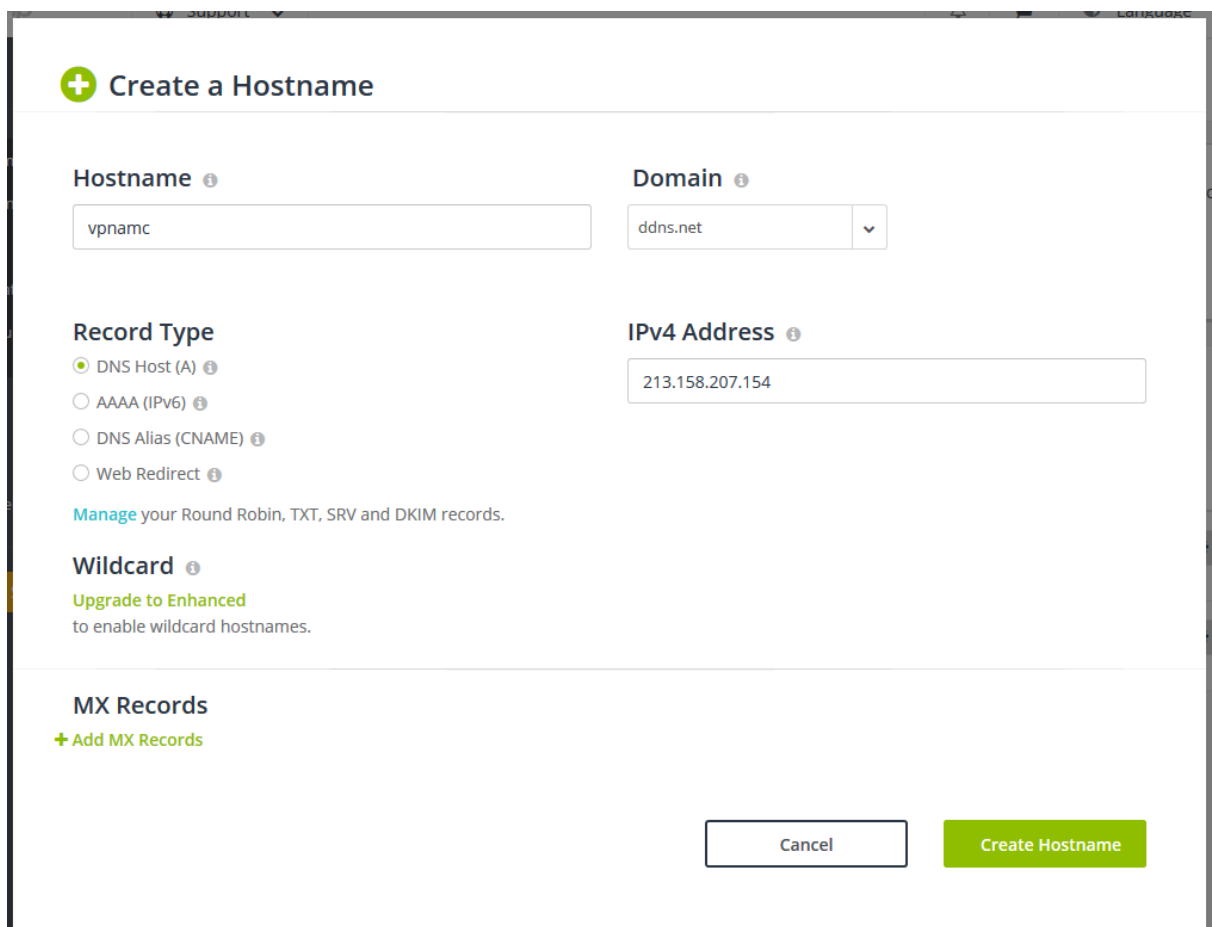
Usługa DNS (Domain Name System) umożliwia przetłumaczenie adresu IP z postaci numerycznej na domenową. Serwisy DDNS (Dynamic Domain Name System) są w stanie świadczyć taką usługę dla dynamicznie zmieniających się adresów IP (głównie stosowane w przypadku kart SIM z publicznym adresem IP).

Połączenie z Serverem OpenVPN zostanie przerwane, gdy jego adres IP (przydzielany dynamicznie przez operatora) zostanie zmieniony. W takiej sytuacji stosuje się DDNS, np. linię „remote 213.158.208.138 1194” w pliku konfiguracyjnym zmieniamy na „remote vpnamc.ddns.net”.

2. Konfiguracja DDNS

(więcej przykładów na https://wiki.teltonika.lt/view/DDNS_Configuration_Examples)

Załącz konto na jednym z serwisów DDNS wspieranym przez routery Teltonika (dyn.com, dyndns.org, noip.com oraz wiele innych). Na wybranym przez siebie serwisie stwórz swoją domenę, wpisując nazwę oraz WAN IP routera (zakładka Status -> Overview), np.



Create a Hostname

Hostname Domain

Record Type ☒ DNS Host (A) ☐ AAAA (IPv6) ☐ DNS Alias (CNAME) ☐ Web Redirect

IPv4 Address

Manage your Round Robin, TXT, SRV and DKIM records.

Wildcard
 Upgrade to Enhanced to enable wildcard hostnames.

MX Records
 + Add MX Records

Cancel Create Hostname

Przejdź do zakładki Services -> Dynamic DNS. Domyślnie stworzona jest jedna, nieaktywna instancja DDNS. Przejdź do jej edycji przyciskiem „Edit”.

DDNS

DDNS Configuration

DDNS name	Hostname	Status	Enable	
Myddns	yourhost.example.com	N/A	☐	EditDelete

New configuration name:

Add New

Save

Zaznacz okno „Enable”, wybierz serwis DDNS, którego używasz, wypełnij nazwę użytkownika oraz hasło. Z tabeli źródła IP wybierz opcję „Public” i zostaw domyślne URL wykrywające Twoje IP. Dobierz częstotliwość wykrywania oraz wymuszania nowego IP.

DDNS

Enable ☒

Use HTTP Secure ☐

Status N/A

Service

no-ip.com

Lookup host

Hostname

User name

Password

IP address source

Public

Public, Private, Custom or Script IP source setting, will disable DNS rebinding protection

URL to detect

IP renew interval

IP renew interval unit

Minutes

Force IP renew

Force IP renew unit

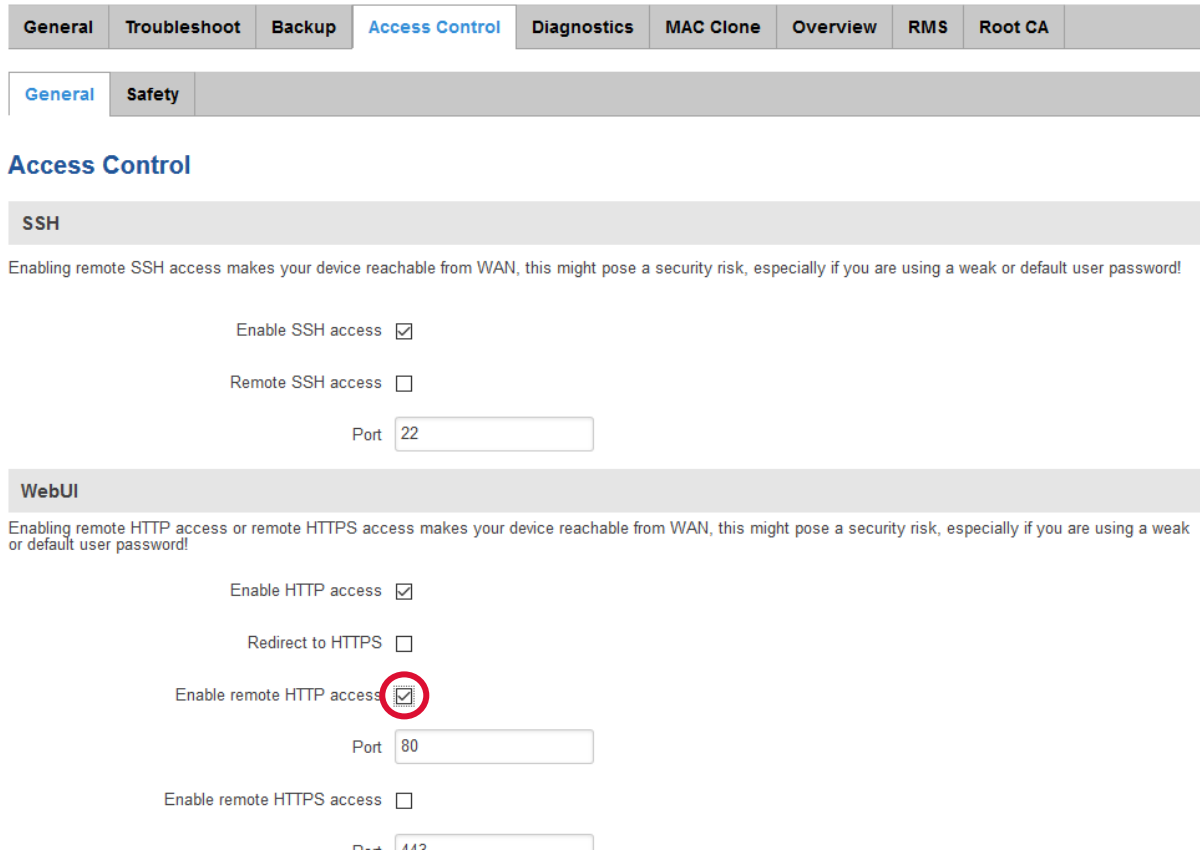
Minutes

Back to Overview

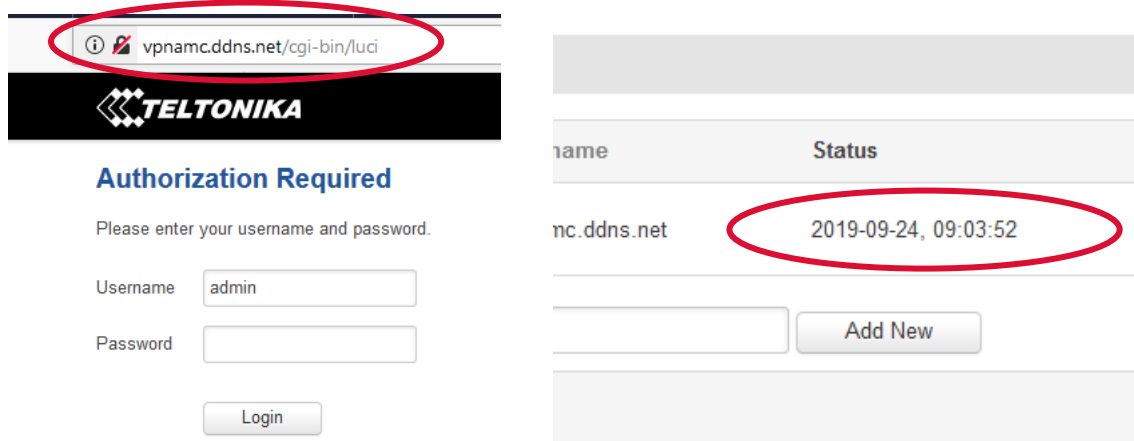
Save

Zapisz konfigurację przyciskiem „Save”.

Ostatnim krokiem jest zezwolenie na zdalny dostęp. Przejdź do zakładki System -> Administration. Następnie w zakładce Access Control zaznacz pole „Enable remote HTTP access”.



Jeśli konfiguracja przebiegła pomyślnie, w zakładce Dynamic DNS pojawi się data przydzielenia domeny, a zdalny dostęp będzie możliwy.



Po przetestowaniu domeny, w pliku konfiguracyjnym Klienta OpenVPN zmień adres IP i port z linii „remote ...” na domenę, np. „remote vpnamc.ddns.net”.