

## Server OpenVPN, zdalny dostęp do sterownika PLC, Dynamiczny DNS

Informator Techniczny Teltonika nr 1 – Modemy TRB i Routery RUTX

17.07.2020 r.

### UWAGA!

Przed przystąpieniem do konfiguracji należy pamiętać:

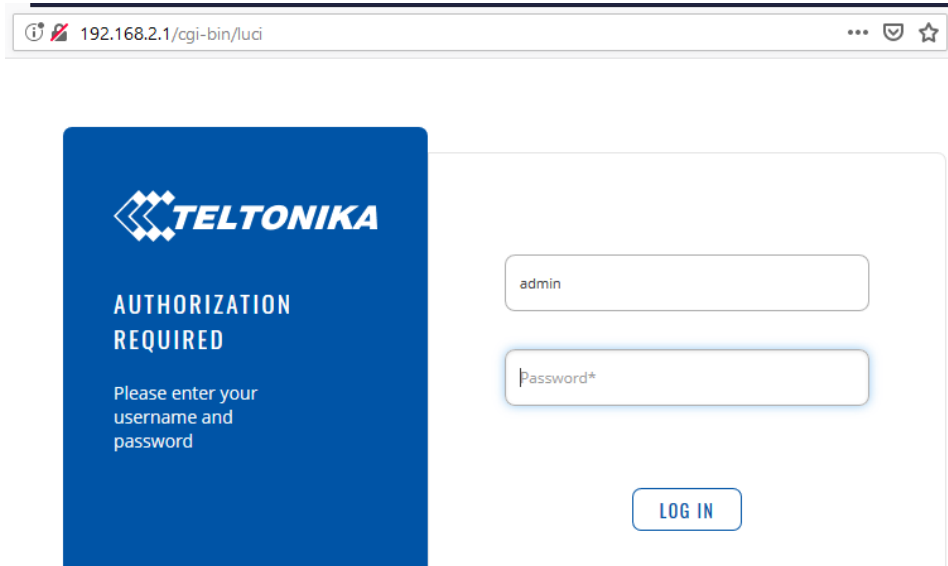
- 1) Karta SIM musi posiadać **publiczny** (statyczny lub dynamiczny) adres IP. Więcej o prywatnych i publicznych adresach na: [https://wiki.teltonika.lt/view/Private\\_and\\_Public\\_IP\\_Addresses](https://wiki.teltonika.lt/view/Private_and_Public_IP_Addresses).
- 2) Przedstawiona poniżej instrukcja jest jedynie przykładem konfiguracji. Wszystkie parametry (adresy IP, maski podsieci, APN, itd.) należy przystosować do własnej konfiguracji sprzętowej.
- 3) Informacje w tym dokumencie są zaktualizowane zgodnie z wersją Firmware **02.04.1**

Dodatkowe informacje:

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

## PODSTAWOWA KONFIGURACJA MODEMU

Kablem USB (lub Ethernet w przypadku TRB140, TRB245, TRB255) podłącz komputer do modemu. Następnie w polu adresu przeglądarki wpisz adres IP modemu (domyślnie 192.168.2.1).



192.168.2.1/cgi-bin/luci

**TELTONIKA**

**AUTHORIZATION REQUIRED**

Please enter your username and password

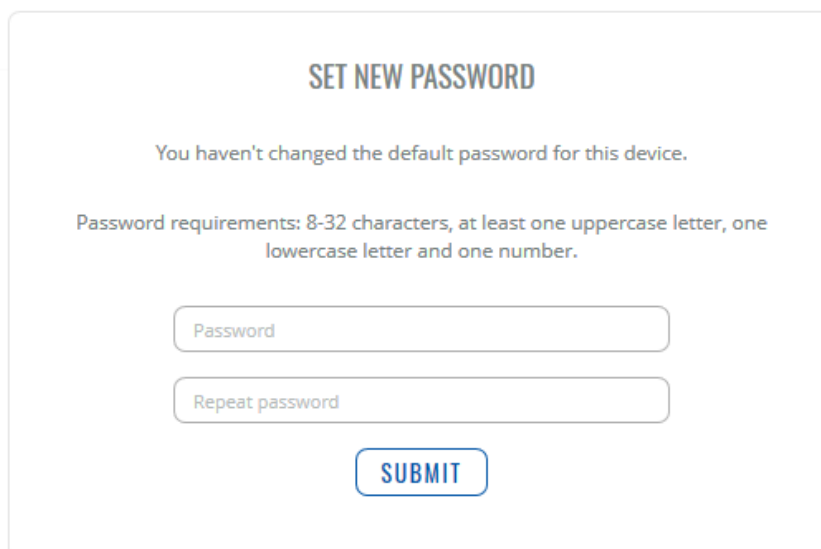
admin

Password\*

LOG IN

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

Przy pierwszym logowaniu konieczna będzie zmiana domyślnego hasła.



**SET NEW PASSWORD**

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

Password requirements: 8-32 characters, at least one uppercase letter, one lowercase letter and one number.

Password

Repeat password

SUBMIT

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

The screenshot shows the 'SYSTEM' sidebar on the left with 'SETUP WIZARD' selected. The main panel is titled 'TIME ZONE SETTINGS'. It displays the current system time as 'Thu Jul 16 11:19:43 2020' with a 'SYNC WITH BROWSER' button. Below, the 'Time zone' is set to 'Europe/Warsaw' in a dropdown menu. At the bottom, there are 'SKIP WIZARD' and 'NEXT' buttons.

W drugim kroku, w zakładce Network -> LAN, wpisz adres IP modemu w sieci wewnętrznej (pamiętaj, aby modem 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.

The screenshot shows the 'SYSTEM' sidebar on the left with 'LAN CONFIGURATION' selected. The main panel is titled 'LAN CONFIGURATION'. It shows 'IP address' set to '192.168.2.1' and 'Netmask' set to '255.255.255.0'. Below, the 'DHCP CONFIGURATION' section has 'Enable DHCP' checked (radio button 'on' selected). The 'Start' address is '100', 'Limit' is '150', 'Lease time' is '12', and 'Units' is set to 'Hours'. At the bottom, there are '< BACK', 'SKIP WIZARD', and 'NEXT' buttons.

W kolejnym kroku skonfiguruj połączenie mobilne w zakładce Network -> Mobile. Wpisz APN oraz metodę potwierdzenia autentyczności, które pozwolą na przypisanie **publicznego adresu IP (!)** oraz kod PIN karty.

The screenshot shows the 'MOBILE CONFIGURATION | MOB1S1A1' page. On the left is a navigation sidebar with 'SYSTEM' selected. The main content area contains the following fields:

- Auto APN:  off  on
- APN:
- Custom APN:
- Authentication Type:
- PIN:

At the bottom, there are three buttons: '< BACK', 'SKIP WIZARD', and 'NEXT'.

Krok 4 (opcjonalny): konfiguracja **RMS**. Aby dowiedzieć się więcej o systemie zdalnego zarządzania odwiedź [www.rms.teltonika.lt](http://www.rms.teltonika.lt) lub skontaktuj się z [amc@astor.com.pl](mailto:amc@astor.com.pl).

The screenshot shows the 'RMS SETTINGS' page. On the left is a navigation sidebar with 'SYSTEM' selected. The main content area contains the following fields:

- Connection type:  ?
- Hostname:
- Port:

Below these fields is a 'STATUS' section with the following information:

Management status	Enabled
Connection state	Failure (Error: Device is not registered in RMS. Please login to rms.teltonika.lt and add this device to your account device list.)
Serial number	1101804319
IMEI	865546040098580
Next Connection After	00:00:41

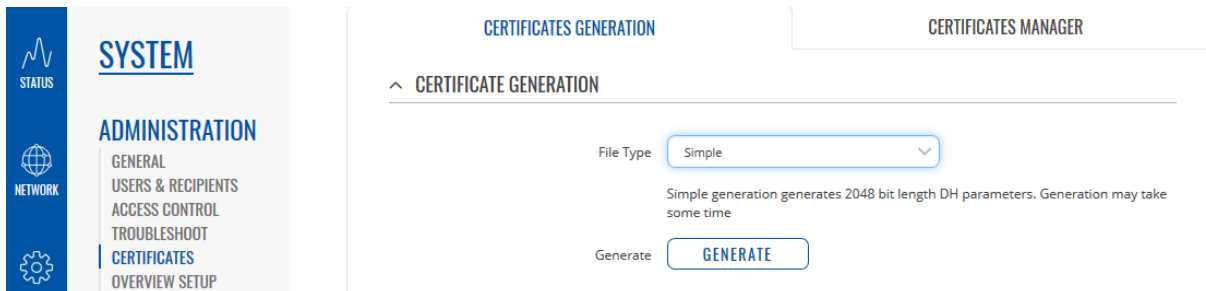
At the bottom, there are four buttons: '< BACK', 'SKIP WIZARD', 'REFRESH', and 'CONNECT'. At the very bottom right, there is a 'SAVE & APPLY' button.

## GENEROWANIE CERTYFIKATÓW/KLUCZY TLS

Przejdź do zakładki System -> Administration -> Certificates. W rozwijanej liście File Type pozostaw domyślną opcję „Simple”. Wygeneruj klucze i certyfikaty za pomocą przycisku „Generate”.

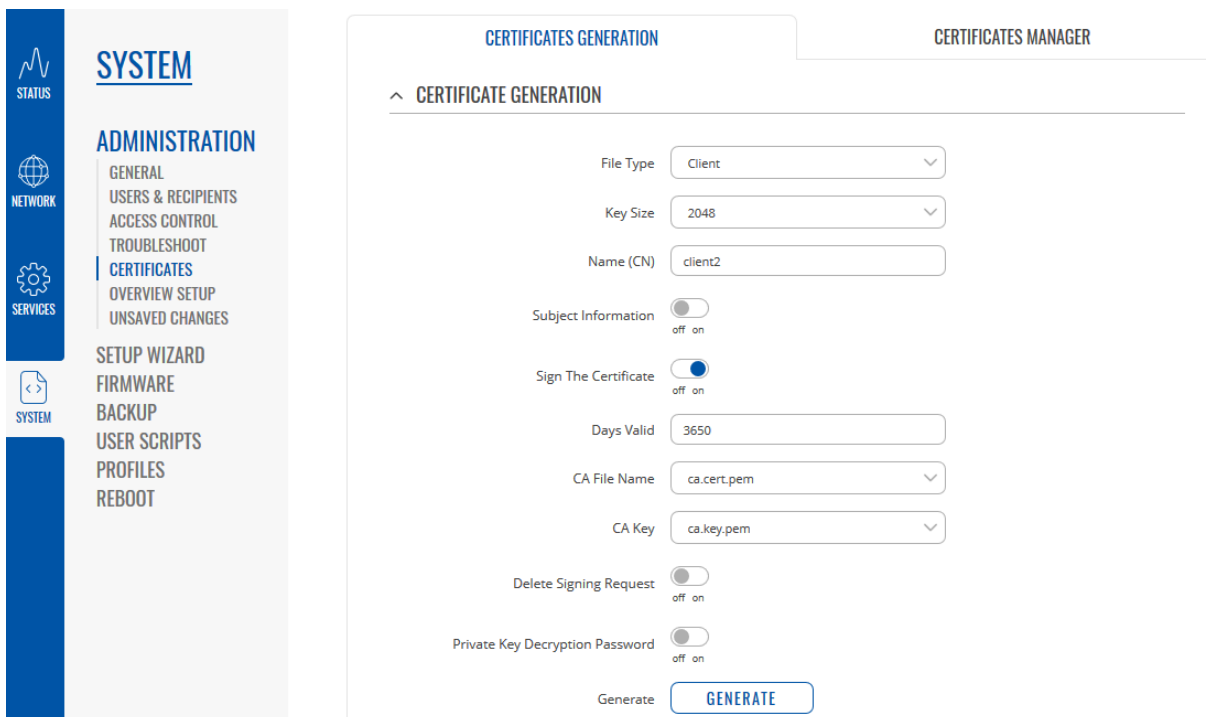
Wygenerowanie wszystkich kluczy i parametrów Diffie-Hellman może potrwać do kilku minut.

Generowanie będzie odbywać się w tle. W międzyczasie możesz przejść do dalszej konfiguracji.



The screenshot shows the 'CERTIFICATES GENERATION' tab in the system administration interface. The 'CERTIFICATE GENERATION' section is expanded, showing a 'File Type' dropdown menu set to 'Simple'. Below it, a note states: 'Simple generation generates 2048 bit length DH parameters. Generation may take some time'. A 'Generate' button with the text 'GENERATE' is visible.

Opcja „Simple” wygeneruje certyfikat dla jednego klienta. Aby wygenerować certyfikaty dla kolejnych klientów wybierz z listy rozwijanej File Type opcję „Client”. Nadaj nazwę CN, według której certyfikat będzie rozpoznawany. Zaznacz opcję „Sign The Certificate”. Wpisz okres ważności certyfikatu. (Jeśli wygenerowałeś więcej niż jeden zestaw certyfikatów, to wybierz odpowiedni z listy „CA File Name oraz CA Key”).

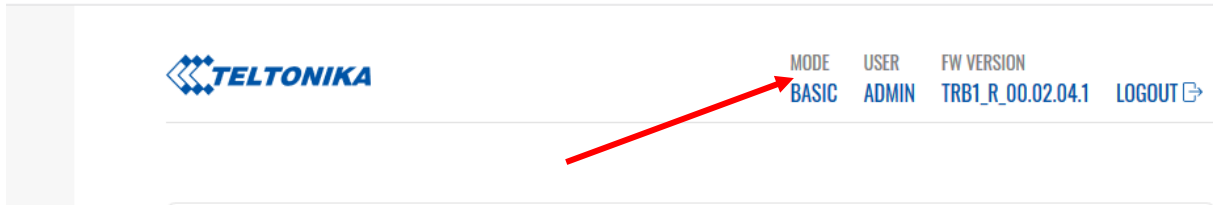


The screenshot shows the 'CERTIFICATES GENERATION' tab with the 'CERTIFICATE GENERATION' section expanded. The 'File Type' dropdown is set to 'Client'. Other fields include 'Key Size' (2048), 'Name (CN)' (client2), 'Days Valid' (3650), 'CA File Name' (ca.cert.pem), and 'CA Key' (ca.key.pem). There are three toggle switches: 'Subject Information' (off), 'Sign The Certificate' (checked/on), and 'Delete Signing Request' (off). A 'Private Key Decryption Password' toggle is also present (off). A 'Generate' button with the text 'GENERATE' is at the bottom.

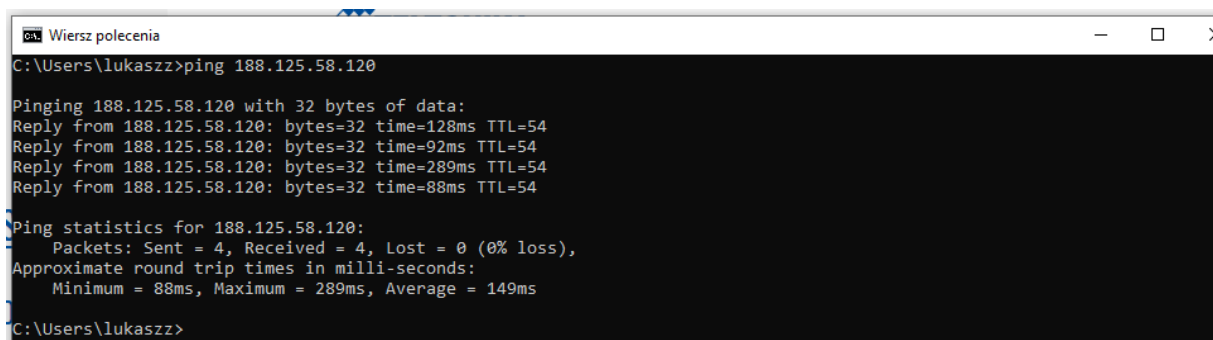
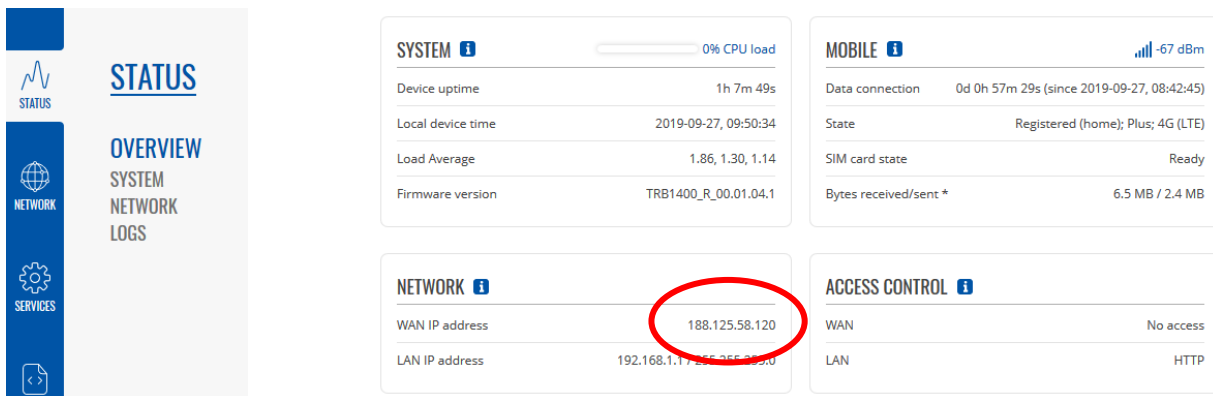
Przejdź do zakładki Certificates Manager. Pobierz certyfikat CA, certyfikat każdego z klientów oraz klucz każdego z klientów. Wykorzystaj przycisk w kolumnie „Export”.

## KONFIGURACJA SERVERA OPENVPN

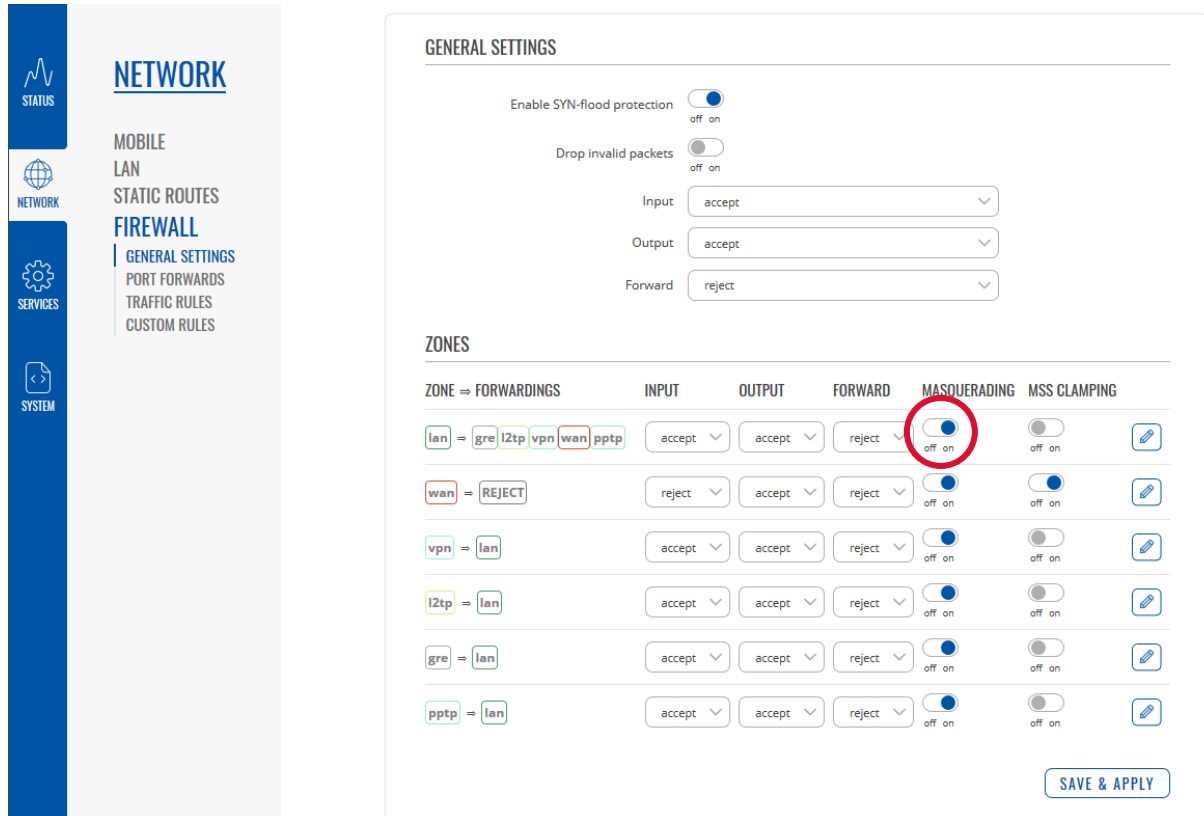
Przejdź w zaawansowany tryb konfiguracji modemu klikając w pole MODE



Upewnij się, że modem posiada publiczny adres IP. Sprawdź adres w zakładce Status -> Overview, następnie użyj komendy „ping” korzystając z innego źródła Internetu.



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



**GENERAL SETTINGS**

Enable SYN-flood protection  off on

Drop invalid packets  off on

Input: accept

Output: accept

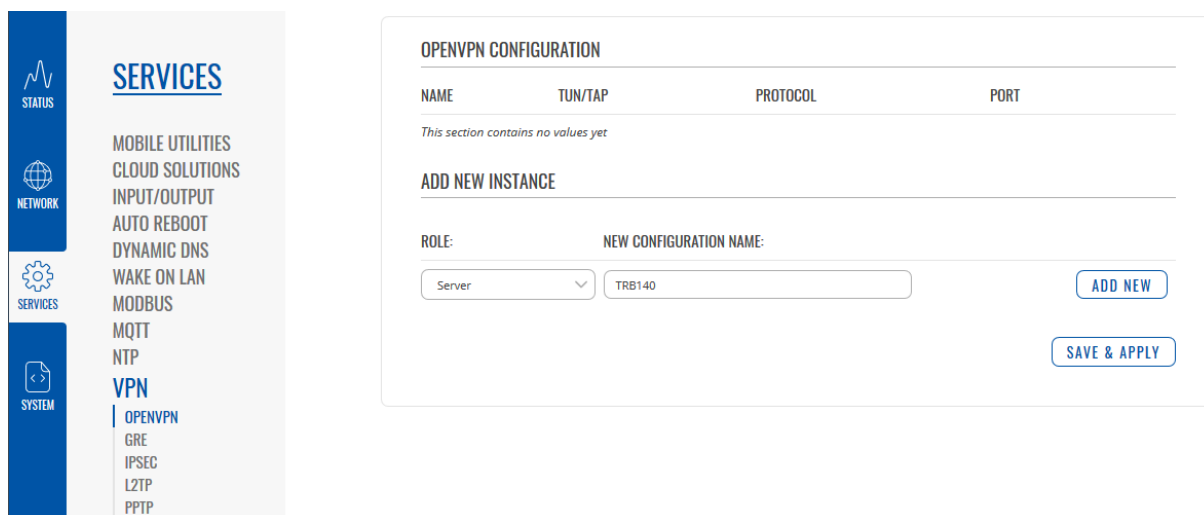
Forward: reject

**ZONES**

ZONE => FORWARDINGS	INPUT	OUTPUT	FORWARD	MASQUERADING	MSS CLAMPING
lan = gre l2tp vpn wan pptp	accept	accept	reject	<input checked="" type="checkbox"/> off on	<input type="checkbox"/> off on
wan = REJECT	reject	accept	reject	<input checked="" type="checkbox"/> off on	<input checked="" type="checkbox"/> off on
vpn = lan	accept	accept	reject	<input checked="" type="checkbox"/> off on	<input type="checkbox"/> off on
l2tp = lan	accept	accept	reject	<input checked="" type="checkbox"/> off on	<input type="checkbox"/> off on
gre = lan	accept	accept	reject	<input checked="" type="checkbox"/> off on	<input type="checkbox"/> off on
pptp = lan	accept	accept	reject	<input checked="" type="checkbox"/> off on	<input type="checkbox"/> off on

SAVE & APPLY

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



**OPENVPN CONFIGURATION**

NAME	TUN/TAP	PROTOCOL	PORT
This section contains no values yet			

**ADD NEW INSTANCE**

ROLE: Server

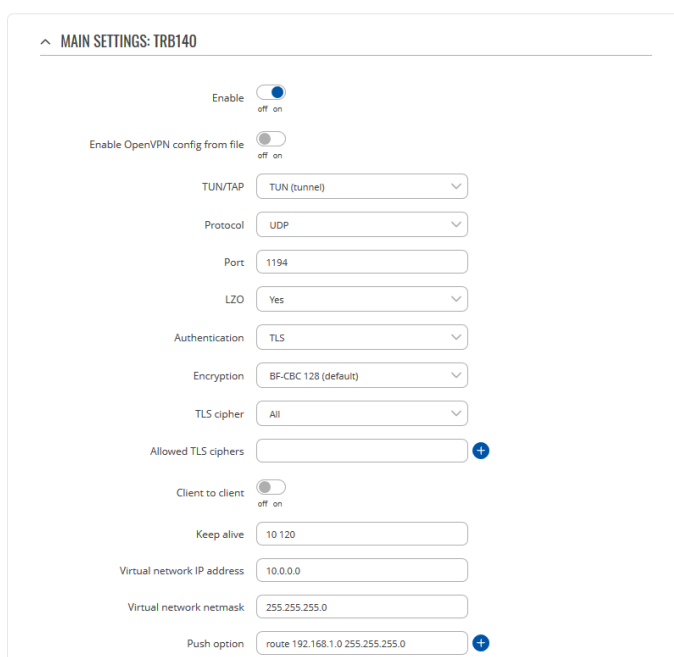
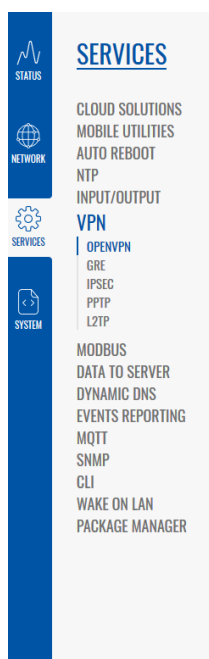
NEW CONFIGURATION NAME: TRB140

ADD NEW

SAVE & APPLY

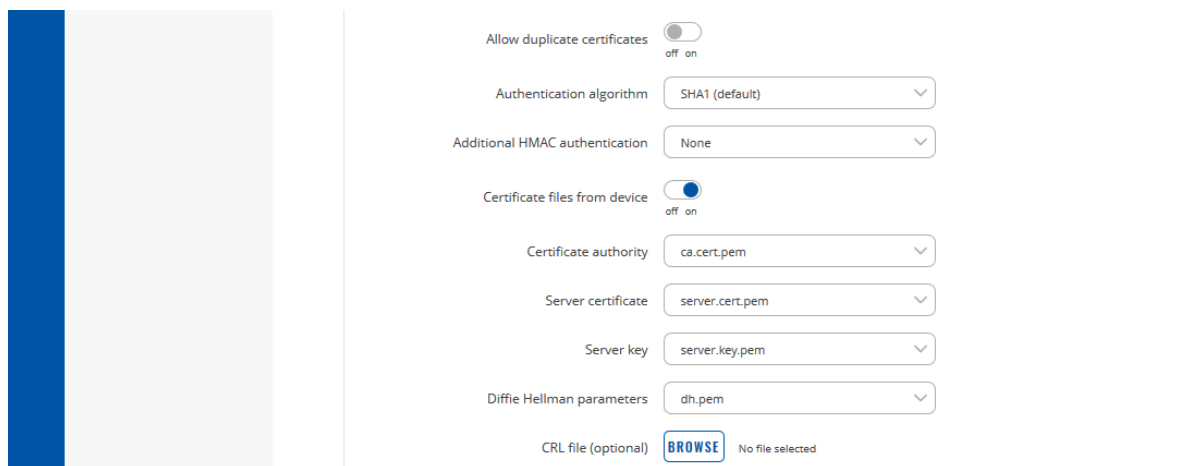
## Parametry Servera:

- 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 (**YES**) – 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).



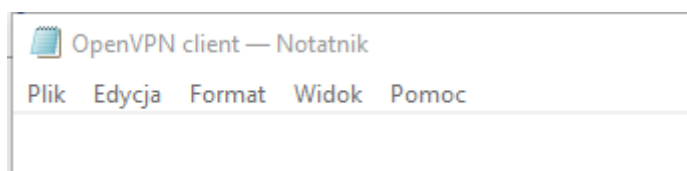


- 11) Allow duplicate certificates (**OFF**) – zezwolenie duplikowania certyfikatów. Włączenie tej opcji umożliwi połączenie wielu klientów za pomocą tego samego certyfikatu.
- 12) Certificate files from device (**ON**) – korzystanie z certyfikatów wygenerowanych na urządzeniu. Wyłączenie tej opcji umożliwi importowanie certyfikatów i kluczy z komputera. Jeśli pliki zostały wygenerowane na urządzeniu, to wybierz z listy rozwijanej odpowiednie pliki



## 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:

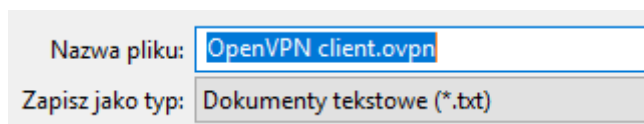
```
client
dev tun
proto udp4
remote 188.125.58.120 1194
ca "C:\\Users\\lukasz\\Downloads\\ca.cert.pem"
cert "C:\\Users\\lukasz\\Downloads\\client.cert.pem"
key "C:\\Users\\lukasz\\Downloads\\client.key.pem"
keepalive 10 120
persist-key
persist-tun
cipher BF-CBC
comp-lzo
verb 7
```

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 -> Overwiew w polu „WAN”.

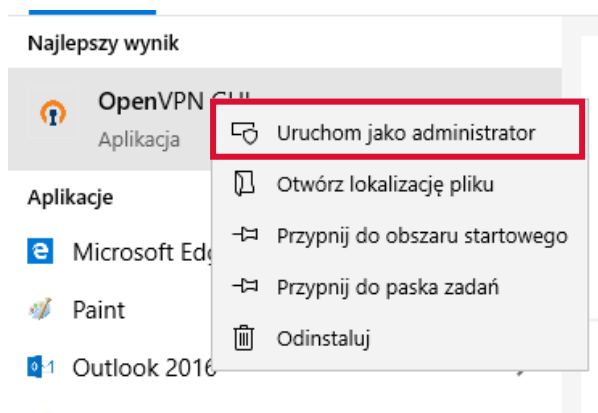
Linie: „ca”, „cert”, „key” odnoszą się do wcześniej wygenerowanych plików TLS. Wpisz odpowiednią lokalizację plików na swoim komputerze.

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

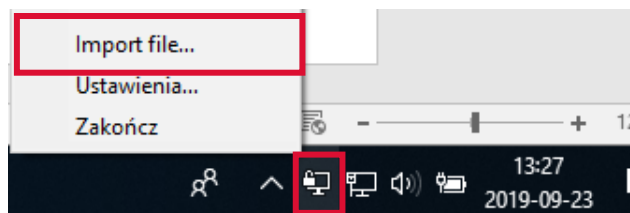


## ŁĄCZENIE Z SERVEREM OPENVPN

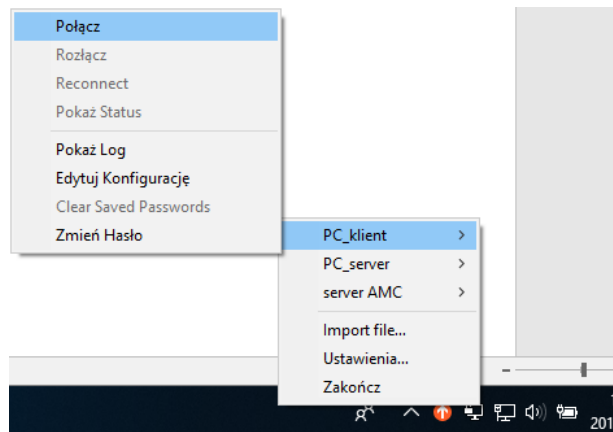
Uruchom OpenVPN GUI jako **administrator**.



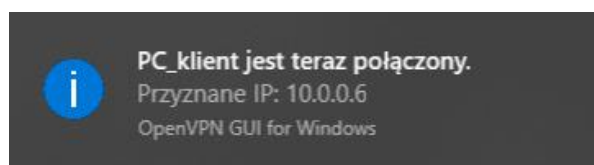
W prawym dolnym rogu paska zadań pojawi się ikona graficznego interfejsu użytkownika OpenVPN. Prawym przyciskiem myszy rozwiń opcje, wybierz „Import file” oraz odszukaj stworzony plik konfiguracyjny klienta OpenVPN.



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 modemu (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

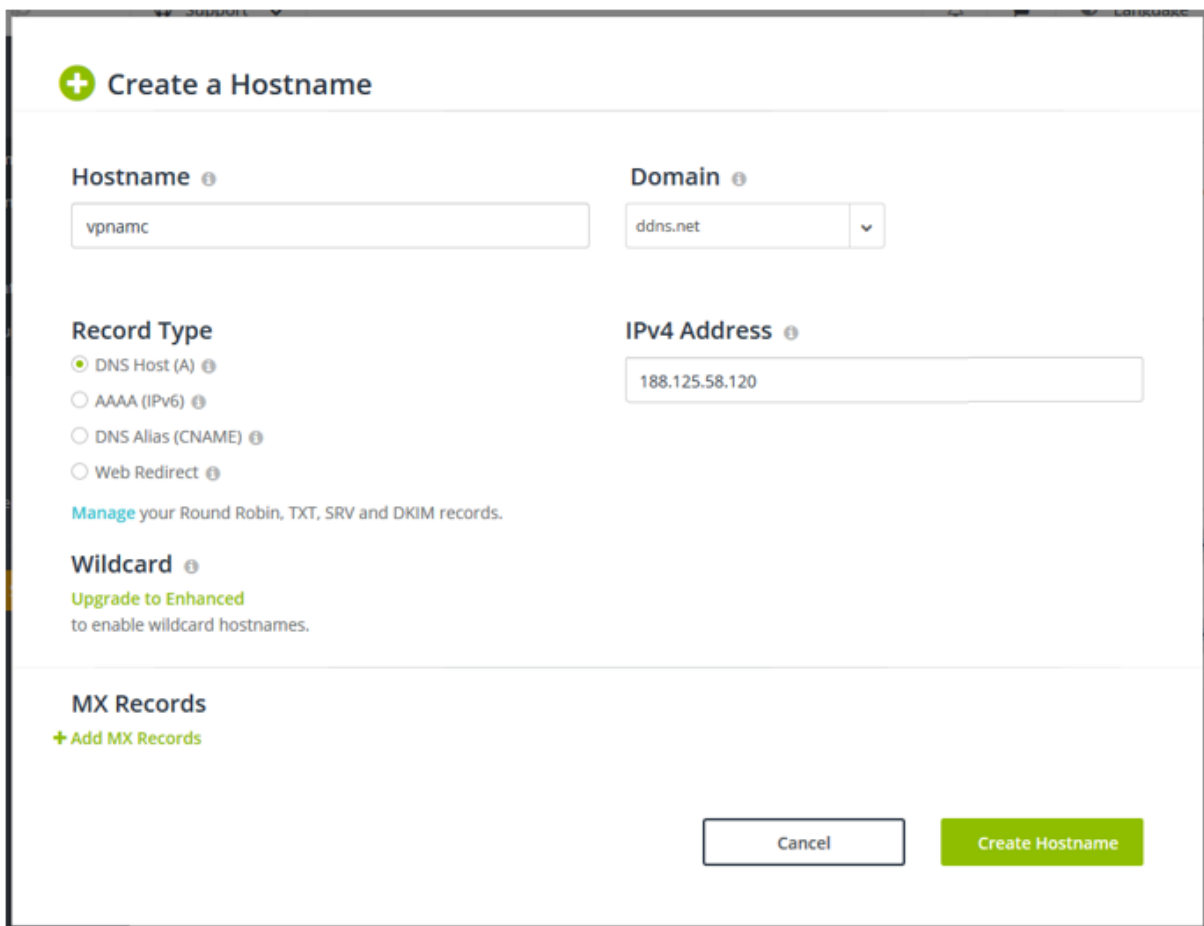
Usługa DNS (Domain Name System) umożliwia przetłumaczenie adresu IP z postaci numerycznej na domenową. Serwisy DDNS (Dynamic Domain Name System) są w stanie świadczyć taką usługę dla dynamicznie zmieniających się adresów IP (głównie stosowane w przypadku kart SIM z publicznym adresem IP).

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](https://wiki.teltonika.lt/view/DDNS_Configuration_Examples))

Załącz konto na jednym z serwisów DDNS wspieranym przez modemy Teltonika (dyn.com, dyndns.org, noip.com oraz wiele innych). Na wybranym przez siebie serwisie stwórz swoją domenę, wpisując nazwę oraz WAN IP modemu (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](#)

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

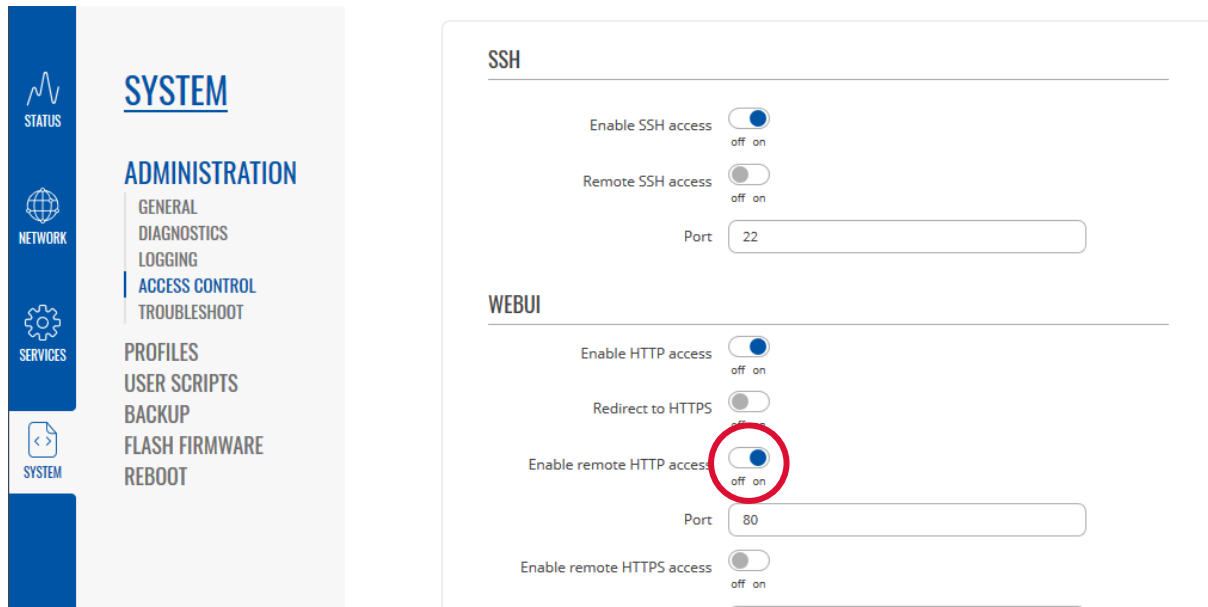
The screenshot shows the 'SERVICES' menu on the left with 'DYNAMIC DNS' highlighted. The main panel is titled 'DYNAMIC DNS OVERVIEW' and displays a table with one entry: 'MYDDNS'. The status is 'Stopped', the hostname is 'yourhost.example.com', and the IP is '-'. The last update is 'Never' and the next update is '-'. The check interval is '10 minutes' and the force interval is '72 hours'. There are edit and delete icons for this entry. Below the table is a section 'ADD DYNAMIC DNS CONFIGURATION' with a 'NAME' input field and 'ADD' and 'SAVE & APPLY' buttons.

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.

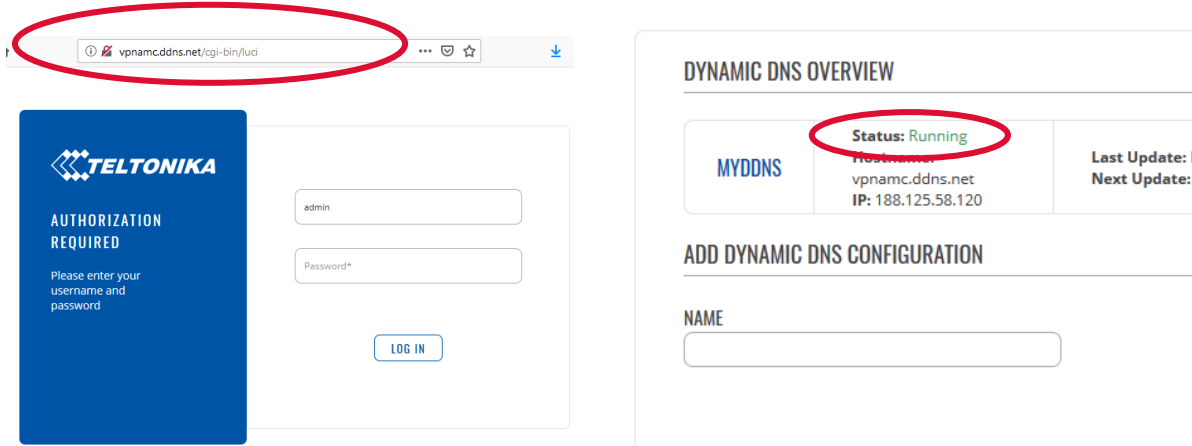
The screenshot shows the 'DYNAMIC DNS DETAILS FOR: MYDDNS' configuration page. It includes an 'Enabled' toggle switch (currently off), a 'Lookup Hostname' field with 'vpnamc.ddns.net', a 'DDNS Service provider' dropdown menu (set to 'no-ip.com'), a 'Domain' field with 'vpnamc.ddns.net', a 'Username' field with 'lzastor', a 'Password' field with masked characters, an 'IP address source' dropdown menu (set to 'Public'), a 'URL to detect' field with 'http://checkip.dyndns.com', a 'Check Interval' field with '10' and a 'minutes' dropdown, and a 'Force Interval' field with '72' and a 'hours' dropdown. There are '< BACK' and 'SAVE & APPLY' buttons at the bottom.

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 status pozytywnego 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 vpnmc.ddns.net”.