

## Konfiguracja OpenVPN w AS30GSM200P



## 1. Czym jest VPN ?

**VPN (Virtual Private Network)** – tłumacząc dosłownie Wirtualna Sieć Prywatna - tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. Można opcjonalnie kompresować lub szyfrować przesyłane dane w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa.

Rozwiązania oparte na VPN stosowane są np. w sieciach korporacyjnych firm, których zdalni użytkownicy pracują ze swoich domów na niezabezpieczonych łączach. Wirtualne Sieci Prywatne charakteryzują się dość dużą efektywnością, nawet na słabych łączach (dzięki kompresji danych) oraz wysokim poziomem bezpieczeństwa (ze względu na szyfrowanie). Rozwiązanie to sprawdza się w firmach, których pracownicy często podróżują lub korzystają z możliwości telepracy.

**OpenVPN** – pakiet oprogramowania, który implementuje techniki tworzenia bezpiecznych połączeń punkt-punkt (VPN) lub strona-strona w sieciach routowanych lub mostkowanych. Umożliwia on tworzenie zaszyfrowanych połączeń między hostami przez sieć publiczną Internet (tunel) – używa do tego celu biblioteki OpenSSL.

OpenVPN używa bibliotek OpenSSL do szyfrowania danych i kanałów kontrolnych. Może również korzystać z HMAC by stworzyć dodatkową warstwę zabezpieczenia połączenia. Pakiet jest w stanie również wykorzystać możliwości sprzętowe, by polepszyć stopień i jakość szyfrowania.

OpenVPN oferuje kilka metod uwierzytelnienia użytkowników: poprzez klucze, certyfikaty lub nazwę użytkownika i hasło.

Aby korzystać z powyższej funkcjonalności, należy zapoznać się z protokołami SSL oraz TLS oraz odpowiadającej im implementacji w postaci **OpenSSL**.

### UWAGA!

Urządzenie konfigurujemy z poziomu przeglądarki:

Adres : 192.168.1.234

Login: admin

Hasło:12345

Po zalogowaniu się na urządzenie, możemy dokonać modyfikacji tych wartości.

## 2. Generacja certyfikatów i kluczy prywatnych

Pierwszym krokiem podczas konfiguracji OpenVPN jest wygenerowanie certyfikatów i kluczy prywatnych dla Urzędu Certyfikacji, klienta i serwera. Urząd Certyfikacji jest instytucją, która przydziela certyfikaty serwerowi i klientom.

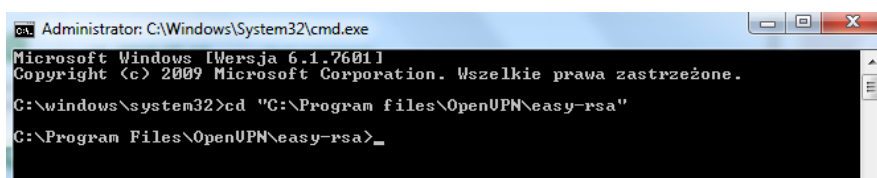
Kolejne kroki postępowania :

1. Pobieramy i instalujemy aplikację OpenVPN GUI ze strony :

<https://openvpn.net/index.php/download/community-downloads.html>

Po pobraniu instalujemy aplikację zaznaczając dodatkowe opcje **OpenSSL Utilities** i **OpenVPN RSA Certificate Management Scripts**.

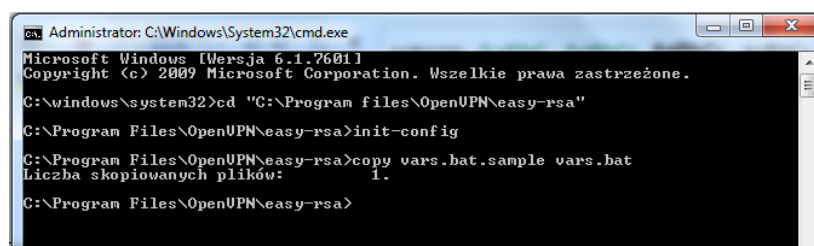
2. Uruchamiamy wiersz poleceń jako **administrator** i za pomocą komendy **cd** przechodzimy do folderu, **easy-rsa**.



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Wersja 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Wszelkie prawa zastrzeżone.
C:\windows\system32>cd "C:\Program files\OpenUPN\easy-rsa"
C:\Program Files\OpenUPN\easy-rsa>
```

Folder ten znajduję się w lokalizacji, którą wskazaliśmy podczas instalowania aplikacji. Domyślna lokalizacja to **C:\Program Files\OpenVPN\easy-rsa**.

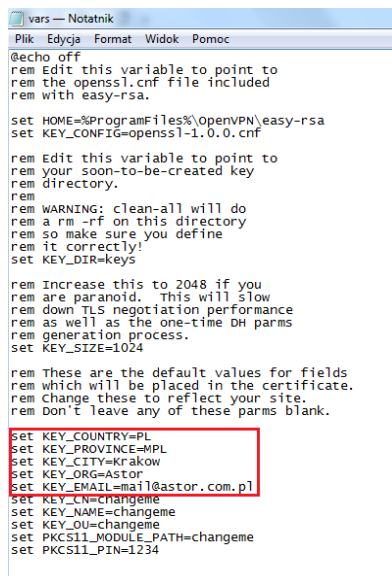
3. W konsoli wykonujemy instrukcję **init-config**.



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Wersja 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Wszelkie prawa zastrzeżone.
C:\windows\system32>cd "C:\Program files\OpenUPN\easy-rsa"
C:\Program Files\OpenUPN\easy-rsa>init-config
C:\Program Files\OpenUPN\easy-rsa>copy vars.bat.sample vars.bat
Liczba skopiowanych plików: 1.
C:\Program Files\OpenUPN\easy-rsa>
```

W folderze **easy-rsa** utworzony został plik **vars.bat**.

4. Otwieramy plik **vars.bat** w notatniku i zmieniamy wartości parametrów **KEY\_COUNTRY**, **KEY\_PROVINCE**, **KEY\_CITY**, **KEY\_ORG** i **KEY\_EMAIL**, by odpowiadały naszej organizacji.



```
vars - Notatnik
Plik  Edycja  Format  Widok  Pomoc

@echo off
rem Edit this variable to point to
rem the openssl.cnf file included
rem with easy-rsa.
set HOME=%ProgramFiles%\OpenVPN\easy-rsa
set KEY_CONFIG=openssl-1.0.0.cnf

rem Edit this variable to point to
rem your soon-to-be-created key
rem directory.
rem
rem WARNING: clean-all will do
rem a rm -rf on this directory
rem so make sure you define
rem it correctly!
set KEY_DIR=keys

rem Increase this to 2048 if you
rem are paranoid. This will slow
rem down TLS negotiation performance
rem as well as the one-time DH parms
rem generation process.
set KEY_SIZE=1024

rem These are the default values for fields
rem which will be placed in the certificate.
rem Change these to reflect your site.
rem Don't leave any of these parms blank.

set KEY_COUNTRY=PL
set KEY_PROVINCE=MPL
set KEY_CITY=Krakow
set KEY_ORG=ASTOR
set KEY_EMAIL=mail@astor.com.pl
set KEY_CN=changeme
set KEY_NAME=changeme
set KEY_OU=changeme
set PKCS11_MODULE_PATH=changeme
set PKCS11_PIN=1234
```

**KEY\_COUNTRY** – Kraj

**KEY\_PROVINCE** – Region (Województwo)

**KEY\_CITY** – Miasto

**KEY\_ORG** – Organizacja (Firma)

**KEY\_EMAIL** – Adres Email

5. Następnie za pomocą wiersza poleceń generujemy certyfikat urzędu certyfikacji

Wpisujemy kolejno trzy instrukcje

- **vars**
- **clean-all**
- **build-ca**

Ostatni skrypt powoduje wygenerowanie certyfikatu i klucza prywatnego Urzędu Certyfikacji. Zostaniemy poproszeni o podanie wartości takich jak kraj, nazwa miasta i nazwa firmy. Można pozostawić wartości domyślne. **Organisation Unit Name** można potraktować jako dział w firmie.

Zmienić musimy jedynie parametr **Common Name** na **Certyfikat**.

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Wersja 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\windows\system32>cd "C:\Program Files\OpenUPN\easy-rsa"

C:\Program Files\OpenUPN\easy-rsa>init-config
C:\Program Files\OpenUPN\easy-rsa>copy vars.bat.sample vars.bat
Liczba skopiowanych plików: 1.

C:\Program Files\OpenUPN\easy-rsa>vars
C:\Program Files\OpenUPN\easy-rsa>clean-all
Nie można odnaleźć określonego pliku.
Liczba skopiowanych plików: 1.
Liczba skopiowanych plików: 1.

C:\Program Files\OpenUPN\easy-rsa>build-ca
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
writing new private key to 'keys\ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.

Country Name (2 letter code) [PL]:PL
State or Province Name (full name) [MPL]:MPL
Locality Name (eg, city) [Krakow]:Krakow
Organization Name (eg, company) [Astor]:Astor
Organizational Unit Name (eg, section) [changel]:AstorDPT
Common Name (eg, your name or your server's hostname) [changel]:Certyfikat
Name [changel]:Certyfikat
Email Address [mail@astor.com.pl]:mail@astor.com.pl

C:\Program Files\OpenUPN\easy-rsa>
```

## 6. Następnie należy wygenerować certyfikaty i klucze serwera

W tym celu w wierszu poleceń wpisujemy instrukcję **build-key-server NazwaSerwera**. Ponownie będziemy poproszeni o zmianę wartości. Ponownie pozostawiamy domyślne. Wymagana jest tylko zmiana Common Name na NazwaSerwera. Pola **challenge password** oraz **optional company name** można pozostawić puste.

Następnie pojawią się dwa pytania. W obu przypadkach należy wybrać **y** i nacisnąć Enter.

```
Administrator: C:\Windows\System32\cmd.exe
C:\Program Files\OpenUPN\easy-rsa>build-key-server ServerASTOR
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
writing new private key to 'keys\ServerASTOR.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.

Country Name (2 letter code) [PL]:PL
State or Province Name (full name) [MPL]:MPL
Locality Name (eg, city) [Krakow]:Krakow
Organization Name (eg, company) [Astor]:Astor
Organizational Unit Name (eg, section) [changel]:AstorDPT
Common Name (eg, your name or your server's hostname) [changel]:ServerASTOR
Name [changel]:ServerASTOR
Email Address [mail@astor.com.pl]:mail@astor.com.pl

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'PL'
stateOrProvinceName     :PRINTABLE:'MPL'
localityName            :PRINTABLE:'Krakow'
organizationName        :PRINTABLE:'Astor'
organizationalUnitName  :PRINTABLE:'AstorDPT'
commonName              :PRINTABLE:'ServerASTOR'
name                   :PRINTABLE:'ServerASTOR'
emailAddress            :IA5STRING:'mail@astor.com.pl'
Certificate is to be certified until Jul 13 11:59:57 2026 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenUPN\easy-rsa>
```

## 7. Następnie wygenerujemy klucz klienta

W wierszu poleceń wpisujemy instrukcję **build-key NazwaKlienta** lub **build-key-pass NazwaKlienta**, jeśli chcemy by dostęp do klienta był chroniony hasłem. Będziemy wtedy poproszeni o dwukrotne wpisanie hasła. Podobnie jak wcześniej wartości pozostawiamy domyślnie. Common Name należy ustawić na NazwaKlienta.

Ponownie pojawią się dwa pytania, na które odpowiadamy wpisując **y** i klikając Enter.



```
Administrator: C:\Windows\System32\cmd.exe
C:\Program Files\OpenUPN\easy-rsa>build-key KlientASTOR
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....++++++
writing new private key to 'keys\KlientASTOR.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

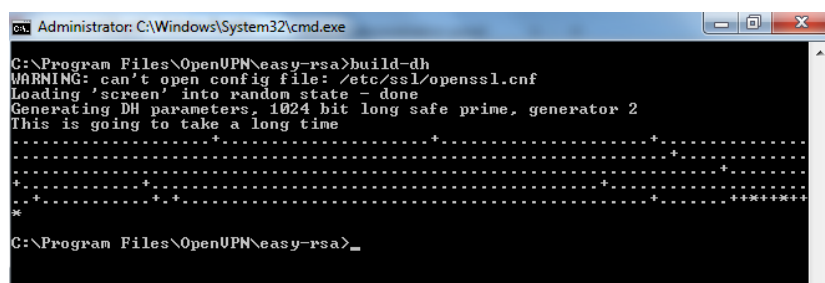
Country Name (2 letter code) [PL]:PL
State or Province Name (full name) [MPL]:MPL
Locality Name (eg, city) [Krakow]:Krakow
Organization Name (eg, company) [Astor]:Astor
Organizational Unit Name (eg, section) [changeme]:AstorDPT
Common Name (eg, your name or your server's hostname) [changeme]:KlientASTOR
Name [changeme]:KlientASTOR
Email Address [mail@astor.com.pl]:mail@astor.com.pl

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'PL'
stateOrProvinceName     :PRINTABLE:'MPL'
localityName            :PRINTABLE:'Krakow'
organizationName        :PRINTABLE:'Astor'
organizationalUnitName  :PRINTABLE:'AstorDPT'
commonName              :PRINTABLE:'KlientASTOR'
name                   :PRINTABLE:'KlientASTOR'
emailAddress            :IA5STRING:'mail@astor.com.pl'
Certificate is to be certified until Jul 13 12:05:41 2026 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenUPN\easy-rsa>
```

## 8. Na koniec generujemy plik z parametrami Diffiego-Hellmana, wywołując instrukcję **build-dh**.



```
Administrator: C:\Windows\System32\cmd.exe
C:\Program Files\OpenUPN\easy-rsa>build-dh
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.....++++++
*
C:\Program Files\OpenUPN\easy-rsa>
```

W folderze **easy-rsa** utworzony został folder **keys** zawierający wszystkie potrzebne pliki.

### 3. Konfiguracja OpenVPN – serwer - AS30GSM200P

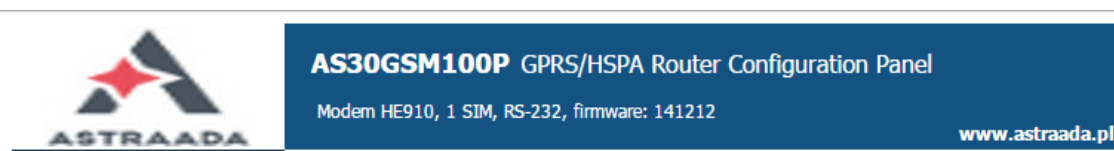
Po podaniu odpowiednich certyfikatów i kluczy w zakładce OpenVPN po stronie urządzenia AS30GSM200P, możemy przejść do finalizacji owej konfiguracji.

1. Wpisujemy w przeglądarce internetowej adres ip 192.168.1.234.  
Domyślny login: admin  
Domyślne hasło: 12345

Aby połączyć się z urządzeniem komputer musi znajdować się w tej samej rodzinie adresów.  
W naszym przypadku IP komputera będzie wyglądać następująco :

192.168.1.xx

2. Sprawdzamy wersję wgranego firmware'u na urządzenie !



Poprawną wersją jest firmware : **141212 lub 141224**

3. W zakładce *Time* sprawdzamy poprawność ustawionego czasu.

#### NTP

RTC time (UTC)	2015-03-12 10:33:31
NTP Peer 1 preferred server	<input type="checkbox"/> Enabled Set this option to enable peer 1 server querying <input type="text"/> Enter IP address NTP server
NTP Peer 2 server	<input type="checkbox"/> Enabled Set this option to enable peer 2 server querying <input type="text"/> Enter IP address NTP server
NTP Peer 3 server	<input type="checkbox"/> Enabled Set this option to enable peer 3 server querying <input type="text"/> Enter IP address NTP server
Date (Y/M/D)	2015   3   12
Time (h:m:s)	10   33   29
Set date/time	<input type="button" value="Set"/> Please enter date/time below and press Set button

4. W zakładce *GSM Network* uzupełniamy pole *APN* odpowiednią wartością, aby uzyskać stały, zewnętrzny adres IP.

Device status		GSM connection	
Basic			
Local network			
GSM network			
Connection control			
Ports configuration			
TCP/IP forwarding			
VLAN			
Static routes			
		SIM slot	
		PIN	<input type="checkbox"/> Enabled
			Enter PIN here
		APN	m2m.plusgsm.pl
			Enter APN here

5. Przechodzimy do zakładki *OpenVPN*. Uzupełniamy pola następującymi wartościami:

OpenVPN mode: **Server**

Connection mode: **Router (TUN) multi-client**

VPN device: **GSM**

Port: **1194** (dowolnie wybrany wolny port)

Protocol: **TCP**

Network: **10.1.0.0** (przykładowa adresacja)

Netmask: **255.255.255.0**

- Wybieramy 1 z tuneli OpenVPN, po czym ustawiamy *OpenVPN mode* w tryb serwer, zgodnie z naszymi oczekiwaniami.
- W zakładce Connection mode wybieramy jeden z dwóch wariantów:
  - tryb bridge(TAP)
  - tryb routera(TUN)
  - W tym przykładzie zostanie zaprezentowane połączenie w trybie **TUN – (multiclient)**.
- W zakładce VPN wybieramy **GSM**.
- Deklarujemy na którym porcie będzie obsługiwane połączenie. Standardowo, do tego typu operacji z wykorzystaniem protokołów TCP bądź UDP wykorzystuje się port 1194, lecz można wykorzystać inny, wolny port.
  - **Należy zapamiętać wybrany port !**
- Wybieramy protokół: TCP bądź UDP, w tym przykładzie skonfigurowane połączenie po **TCP**.
  - **Należy zapamiętać wybrany protokół !**
- Podajemy sieć i maskę VPNa, zalecane podane wartości:
  - Network:10.1.0.0
  - Netmask:255.255.255.0

**Należy zapamiętać podane informacje, ponieważ są one niezbędne do dalszej konfiguracji !**



OpenVPN tunnels	
<b>Device status</b>	
<b>Basic</b>	
Local network	
GSM network	
Connection control	
Ports configuration	
TCP/IP forwarding	
VLAN	
Static routes	
Dynamic DNS	
Access control	
<b>Advanced</b>	
<b>OpenVPN</b>	
IPsec static	
IPsec mobile	
IPsec authentication	
N2N	
CARP	
NTRIP	
SMS Actions	
<b>Administration</b>	
Time	
Syslog	
User files	
<b>Tunnel configuration</b>	openVPN tunnel 1 Please select VPN tunnel you would like to configure
<b>OpenVPN mode</b>	Server
<b>Connection mode</b>	Router (TUN) multi
<b>Remote Server IP or domain</b>	
<b>Remote Server as domain name</b>	<input type="checkbox"/> Enter Remote Server as domain name
<b>VPN device</b>	GSM
<b>NAT-T</b>	<input type="checkbox"/> Enable NAT Traversal (NAT-T) Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.
<b>Port</b>	1194
<b>Protocol</b>	TCP
<b>Network</b>	10.1.0.0
<b>Netmask</b>	255.255.255.0

## 6. Przechodzimy do konfiguracji certyfikatów oraz kluczy:

W następujących polach uzupełniamy je zawartością podanych plików z folderu **easy-rsa\keys**:

- CA cert: certyfikat urzędu certyfikującego (ca.crt)
- Server/client cert: certyfikat dla serwera (NazwaSerwera.crt)
- Server/client private key: klucz prywatny dla serwera (NazwaSerwera.key)
- DH PEM: plik z parametrami Diffiego-Hellmana (dh1024.pem)

Powyższe pliki można otworzyć za pomocą notatnika.

## 7. Jeżeli chcemy mieć możliwość korzystania z adresacji sieci LAN(192.168.1.0/24) po stronie urządzenia AS30GSM200P Uzupełniamy pole:

Additional configuration: **push "route 192.168.1.0 255.255.255.0"**

**Należy zwrócić uwagę aby cały ten skrypt był napisany w jednej linii bez użycia klawisza ENTER!!**

Wklejamy całą zawartość pliku, łącznie z nagłówkami !

CA cert	<pre>-----BEGIN CERTIFICATE----- MIIG0zCCBLugAwIBAgIJALTR4P/c+6t6MA0GCSqGSIb3DQE BCwUAMIGHMQswCQYD VQ0GEwJQTDELMAkGA1UECBMCV1AxEtAPBgNVBAcTCFN6Y3p </pre> <p>Generate</p>
CA key	<pre>-----BEGIN PRIVATE KEY----- MIIJQwIBADANBgkqhkiG9w0BAQEFAASCCS0wgGkpAgEAAoI CAQCcIm6K1sVrMM8m b0B5/nv1/dCtK5GFdaq7AwaTa2M4TdZLVZMVuSFs0ruUxDU </pre>
Server/client cert	<p>Certificate:</p> <p>Data:</p> <p>Version: 3 (0x2)</p> <p>Serial Number: 1 (0x1)</p> <p>Generate</p>
Server/client private key	<pre>-----BEGIN PRIVATE KEY----- MIIJQwIBADANBgkqhkiG9w0BAQEFAASCCS0wgGkoAgEAAoI CAQCaSGyjmDooKfm 6TVZHuu59RB0zXFa/pTGcPmv8t0jcG4kuan1C+5khtpgjII </pre>
DH PEM	<pre>-----BEGIN DH PARAMETERS----- MIIBCAKCAQEAjSkUvTAS6MkysQLPSBrKXjZmEWc1Nsk/1bH XEzVxUE6RztMIXekQ Ibo1/3YuekeG7xgl7f13F4S87KuAoSpmKzzIj918owFa76b </pre> <p>Generate</p>
TLS key	<div></div> <p>This field is optional</p>
LZO compression	<input checked="" type="checkbox"/> <b>Enabled</b> Set this option to enable LZO compression
Additional configuration	<pre>push "route 192.168.1.0 255.255.255.0"</pre>

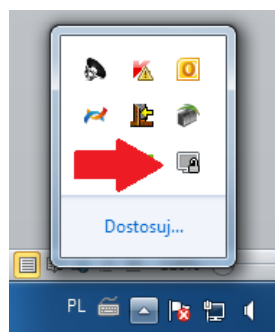
8. Jeżeli wszystko zostało wykonane poprawnie, **zatwierdzamy wszystkie zmiany** !

Backup and restore  
Discard changes  
Save settings

9. Po załadowaniu nowych informacji, należy sprawdzić czy zostały one poprawnie wgrane na urządzenie. Jest to szczególnie ważne gdy łączymy się poprzez publiczne IP.

## 4. Konfiguracja OpenVPN – klient – OpenVPN-GUI

- Po poprawnym skonfigurowaniu serwera, należy skonfigurować urządzenie, które będzie klientem w sieci OpenVPN. Zakładamy, że najczęstszym wyborem w tym wypadku będzie komputer.  
Uruchamiamy program OpenVPN GUI jako **administrator**.
- Po uruchomieniu, w prawym dolnym rogu powinna pojawić się ikonka:



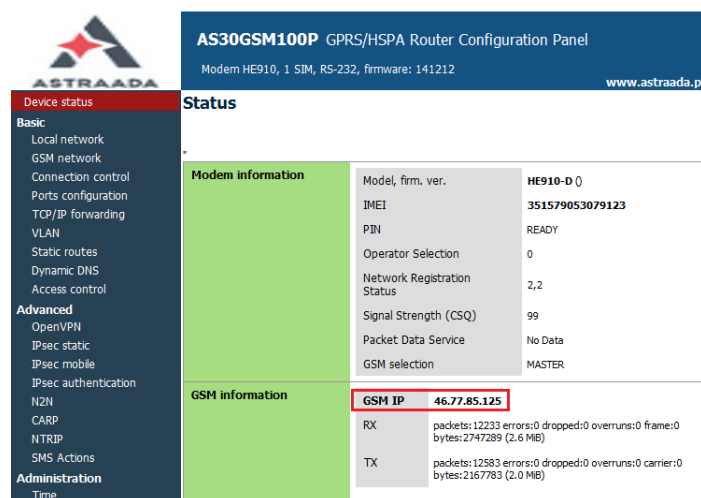
- Aby nawiązać połączenie, należy podać parametry połączenia. Dzięki nim program jest w stanie określić takie informacje jak: klient/serwer, TCP/UDP, który port jest używany, adresy IP. Służą do tego pliki z rozszerzeniem .ovpn.

W folderze **OpenVPN\config** tworzymy plik **client.ovpn** i wklejamy do niego poniższą konfigurację z odpowiednim adresem IP serwera.

```
client # ustawiamy computer jako klienta
dev tun # connection mode ustawiamy jako tun
proto tcp # wybieramy protokol
remote 87.251.253.19 1194 # podajemy adres IP karty sim użytej w modemie GSM i port
ca ca.crt # nazwa certyfikatu urzędu certyfikującego
cert NazwaKlienta.crt # nazwa certyfikatu klienta
key NazwaKlienta.key # nazwa klucza prywatnego klienta
comp-lzo # używanie kompresji lzo
verb 4 # poziom komunikatów podczas połączenia
```

Za **NazwaKlienta** wpisujemy nazwę pliku certyfikatu oraz klucza klienta znajdującego się w folderze **OpenVPN/easy-rsa**.

**Adres IP karty sim** używanej w modemie GSM, można znaleźć w panelu konfiguracji routera, dostępnego pod adresem **192.168.1.234** w przeglądarce w zakładce **Device status**.



**AS30GSM100P** GPRS/HS-PA Router Configuration Panel  
Modem HE910, 1 SIM, RS-232, firmware: 141212 [www.astraada.pl](http://www.astraada.pl)

**Status**

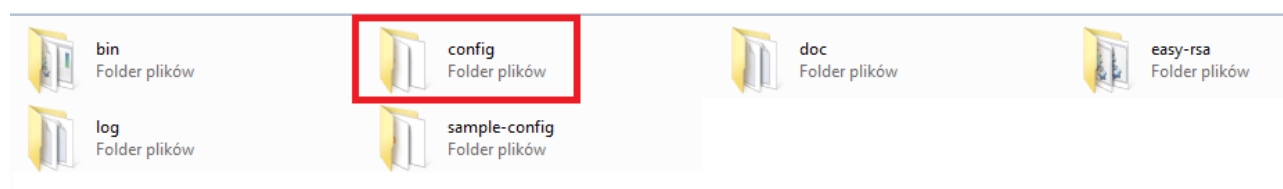
**Modem information**

Model, firm. ver.	HE910-D 0
IMEI	351579053079123
PIN	READY
Operator Selection	0
Network Registration Status	2,2
Signal Strength (CSQ)	99
Packet Data Service	No Data
GSM selection	MASTER

**GSM information**

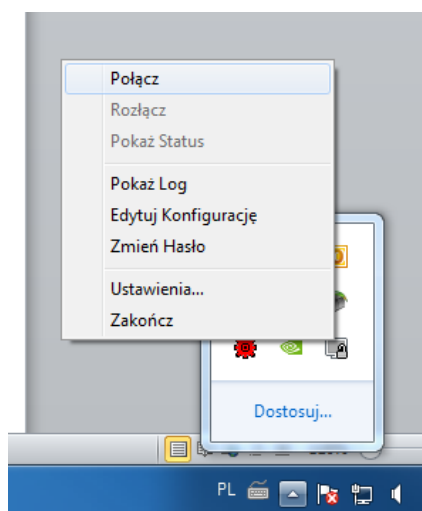
GSM IP	46.77.85.125
RX	packets:12233 errors:0 dropped:0 overruns:0 frame:0 bytes:2747289 (2.6 MB)
TX	packets:12583 errors:0 dropped:0 overruns:0 carrier:0 bytes:2167783 (2.0 MB)

W folderze umieszczamy również wszystkie **certyfikaty i klucze** z folderu **easy-rsa\keys**.

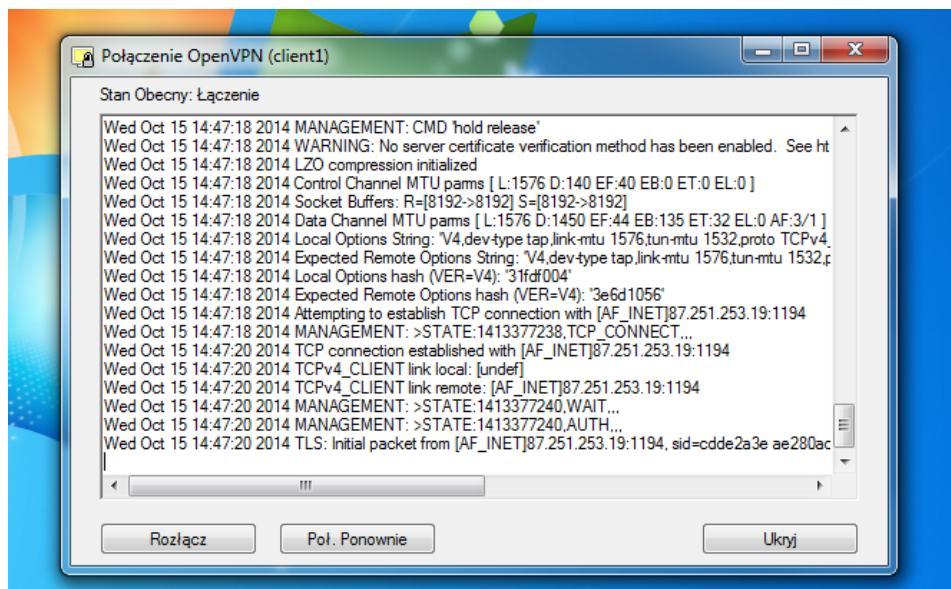


**Przeniesienie tych plików do folderu /config jest warunkiem wykrycia przez program konfiguracji, która umożliwia nam połączenie !**

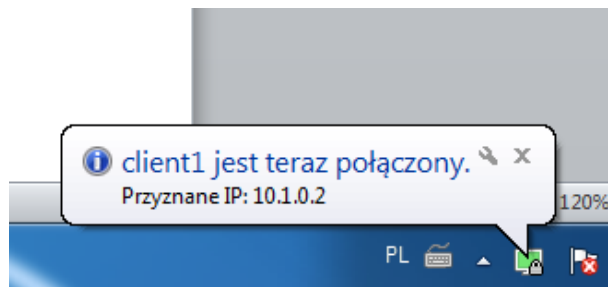
- Po poprawnym przeniesieniu tych plików, przechodzimy do ikonki OpenVPN w prawym dolnym rogu, klikamy na nią prawym przyciskiem, powinniśmy mieć możliwość połączenia się po OpenVPN:



- Klikamy **Połącz** i czekamy na odpowiedź. Na ekranie interfejsu graficznego będą pojawiać się komunikaty. Ich liczba i szczegółowość zależy od parametru **verb**, który jest umieszczony w pliku client.ovpn. Poniżej obraz opisanej sytuacji:



- Jeżeli wszystko przebiegło pomyślnie, powinniśmy dostrzec taki komunikat:



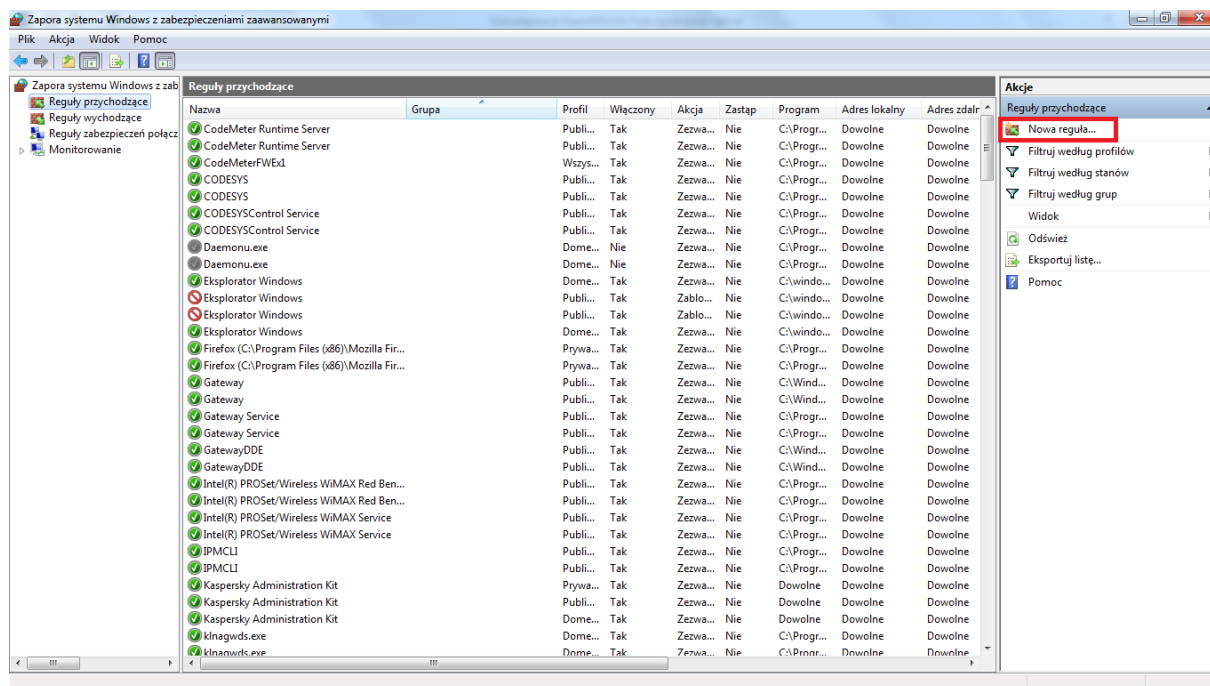
Oznacza to, iż zostało nawiązanie połączenie, automatyczne zostało nam przydzielony adres IP z puli dostępnych adresów.

Od tej pory jesteśmy połączeni pomiędzy komputerem a urządzeniem za pomocą OpenVPN.

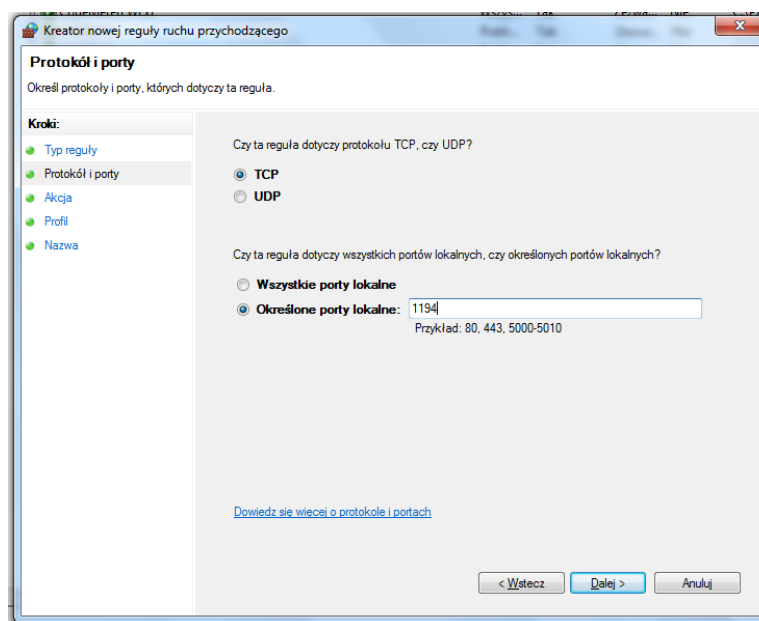
Jeśli klient nie jest w stanie się połączyć, to możliwe jest, że program jest blokowany przez firewall. Należy wtedy dodać odpowiedni wyjątek na port 1194.

## 5. Dodawanie wyjątku na port 1194

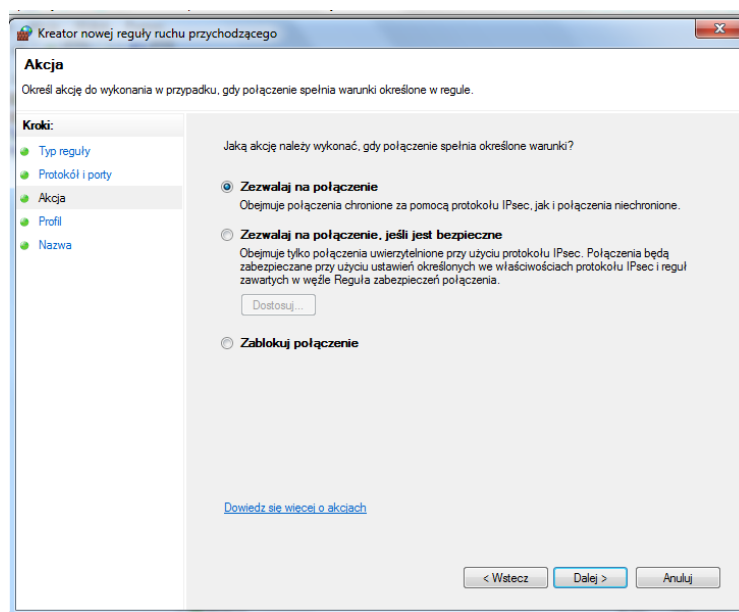
1. Przechodzimy do **Panelu Sterowania|System i Zabezpieczenia|Zapora Systemu Windows**, następnie **Ustawienia zaawansowane**.
2. W oknie dialogowym przechodzimy do **reguł przychodzących** i dodajemy nową regułę.



3. Wybieramy **Port**, protokół **TCP** i wpisujemy nr portu : **1194**



4. Następnie klikamy dalej i zaznaczamy opcję **Zezwalaj na połączenie**



5. Przechodzimy dalej i kończymy dodawanie wyjątku

6. Następnie przechodzimy do **reguł wychodzących** i powtarzamy wcześniejsze czynności