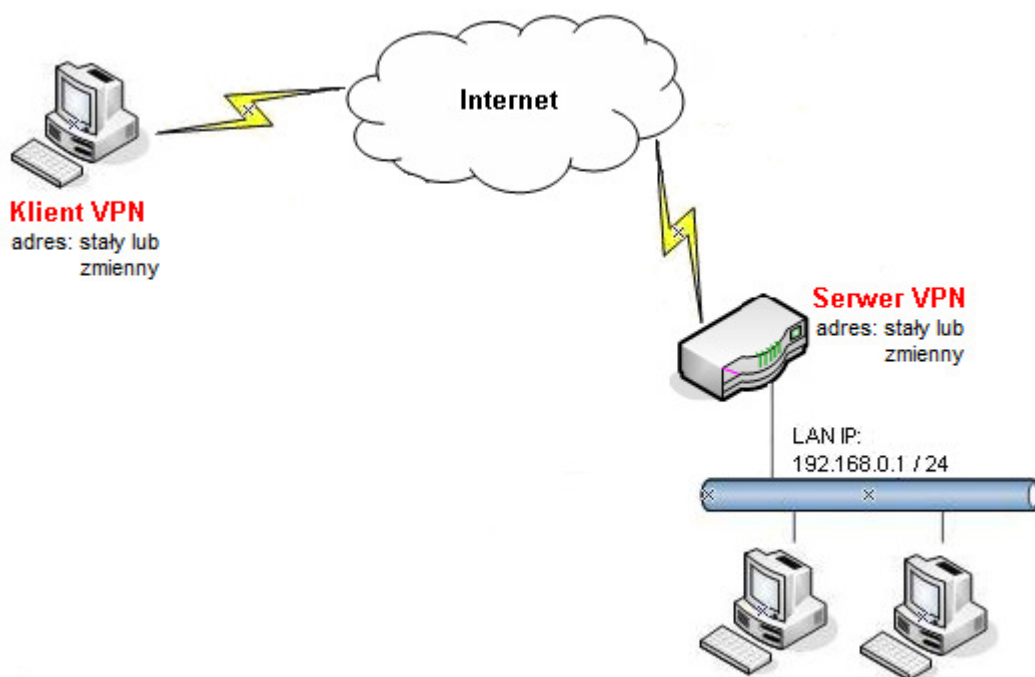


1. Aplikacje mOTP
  - 1.1. DroidOTP
  - 1.2. Mobile-OTP
2. Konfiguracja serwera VPN
3. Konfiguracja klienta VPN
4. Status połączenia
  - 4.1. Klient VPN
  - 4.2. Serwer VPN

Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

- typ tunelu: Host-LAN
- protokół VPN: PPTP
- wymagane szyfrowanie
- uwierzytelnianie mOTP (PIN 1234, Secret wygenerowany przez aplikację mOTP)
- Adres Serwera VPN: stały (IP - 99.99.99.10) lub zmienny (domenowy - serwer.abc.xyz)
- Adres Klienta VPN: stały lub zmienny

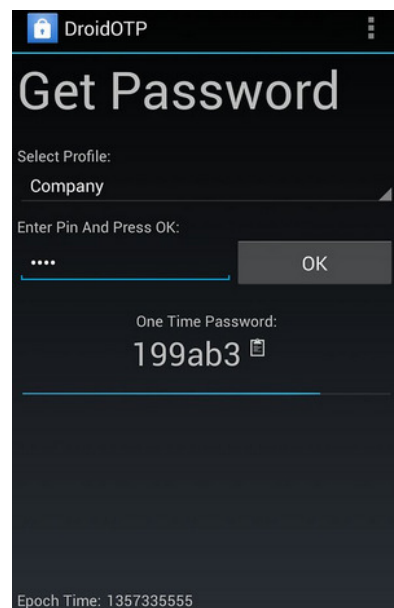
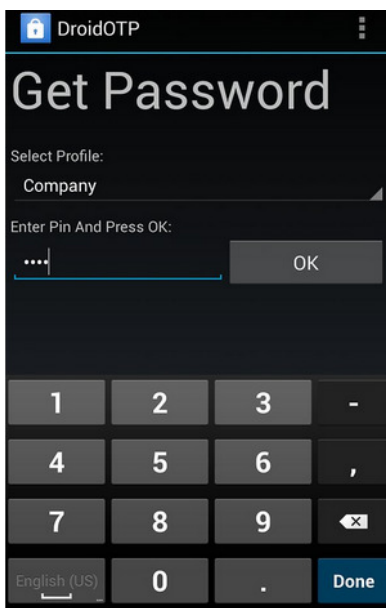
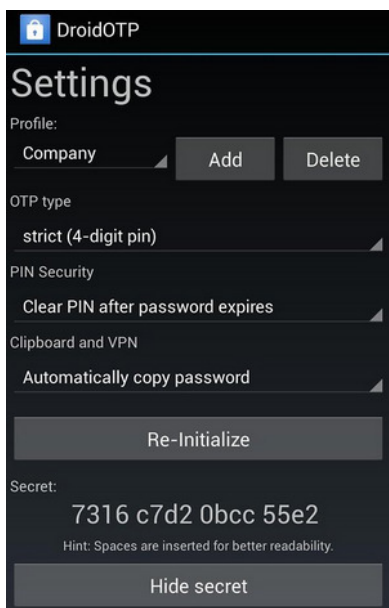
### Uwagi

- Hasło mOTP jest generowane na podstawie bieżącego czasu, kodu PIN oraz klucza Secret.
- Więcej na temat mOTP <http://motp.sourceforge.net>
- Połączenie PPTP z szyfrowaniem MPPE wymaga uwierzytelniania MS-CHAP lub MS-CHAP v2.
- Jeśli serwer VPN nie posiada stałego adresu IP to można wykorzystać opcję dynamicznego DNS (np. [www.noip.com](http://www.noip.com)) w celu reprezentowania zmiennego adresu IP poprzez adres domenowy.

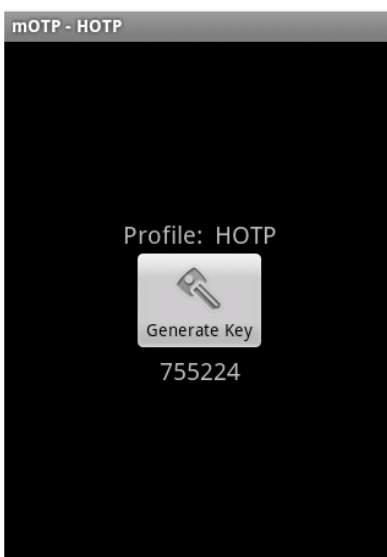
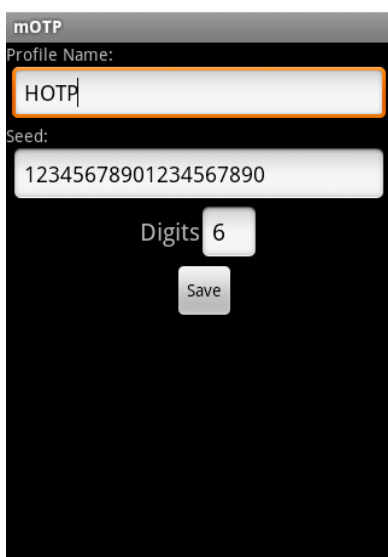
### 1. Aplikacje mOTP

1. Zainstalowanie aplikacji pobranej z Google Play
2. Stworzenie profilu m.in. wygenerowanie Secret
3. Wygenerowanie hasła po podaniu PIN

#### 1.1. DroidOTP marinits.net



#### 1.2. Mobile-OTP Miceli Bros



### 2. Konfiguracja serwera VPN

Przejdź do zakładki **System>>Ustawienia czasu**. Ustaw aktualny czas na Vigorze, gdyż będzie on niezbędny do poprawnej pracy mOTP.

System >> Ustawienia czasu

---

**Informacje o czasie**

Aktualny stan zegara: 2014 Aug 26 Tue 14:11:42 Pobierz teraz

---

**Ustawienia czasu**

Użyj czasu przeglądarki  
 Użyj czasu z Internetu

Serwer czasu:

Priorytet:

Strefa czasowa:

Uwzględniaj 1h przesunięcie czasu (zimowy/letni):

Okres uaktualniania:

Przejdź do zakładki **VPN i Dostęp Zdalny>>Protokoły VPN** i sprawdź (lub zaznacz) czy jest włączona obsługa protokołu PPTP.

VPN i Dostęp Zdalny>> Protokoły VPN

---

**Protokoły VPN**

<input checked="" type="checkbox"/>	Włącz obsługę PPTP
<input checked="" type="checkbox"/>	Włącz obsługę IPsec
<input checked="" type="checkbox"/>	Włącz obsługę L2TP
<input checked="" type="checkbox"/>	Włącz obsługę SSL VPN

Następnie przejdź do zakładki **VPN i Dostęp Zdalny>>Ustawienia Ogólne PPP**. Zmień Opcje szyfrowanie PPP(MPPE). W przykładzie użyto Wymagaj MPPE(40/128 bit).

VPN i Dostęp Zdalny>> Ustawienia ogólne PPP

---

**Ustawienia ogólne PPP**

<p><b>Parametry PPP dla VPN</b></p> <p>Uwierzytelnianie PPP: <input type="text" value="PAP/CHAP/MS-CHAP/MS-CHAPv2"/></p> <p>Opcje szyfrowania PPP(MPPE): <input type="text" value="Wymagaj MPPE(40/128 bit)"/></p> <p>Uwierzytelnianie zwrotne (PAP): <input type="radio"/> Tak <input checked="" type="radio"/> Nie</p> <p>Użytkownik: <input type="text"/></p> <p>Hasło: <input type="text"/></p> <p><b>Adresy przydzielane klientom zdalnym (Używane, gdy wyłączony serwer DHCP)</b></p> <table border="1"> <tr><td>Początkowy IP</td><td>LAN 1</td><td><input type="text" value="192.168.0.200"/></td></tr> <tr><td></td><td>LAN 2</td><td><input type="text" value="192.168.2.200"/></td></tr> <tr><td></td><td>LAN 3</td><td><input type="text" value="192.168.3.200"/></td></tr> <tr><td></td><td>LAN 4</td><td><input type="text" value="192.168.4.200"/></td></tr> <tr><td></td><td>LAN 5</td><td><input type="text" value="192.168.5.200"/></td></tr> </table>	Początkowy IP	LAN 1	<input type="text" value="192.168.0.200"/>		LAN 2	<input type="text" value="192.168.2.200"/>		LAN 3	<input type="text" value="192.168.3.200"/>		LAN 4	<input type="text" value="192.168.4.200"/>		LAN 5	<input type="text" value="192.168.5.200"/>	<p><b>Profile LDAP dla uwierzytelniania PPP</b></p> <p><u>Profil LDAP</u></p> <p>Uwaga: Wybierz 'Tylko PAP' w ustawieniach ogólnych PPP jeśli chcesz używać AD/LDAP do uwierzytelniania!!</p>
Początkowy IP	LAN 1	<input type="text" value="192.168.0.200"/>														
	LAN 2	<input type="text" value="192.168.2.200"/>														
	LAN 3	<input type="text" value="192.168.3.200"/>														
	LAN 4	<input type="text" value="192.168.4.200"/>														
	LAN 5	<input type="text" value="192.168.5.200"/>														

W kolejnym kroku przejdź do zakładki **VPN i Dostęp Zdalny >> Połączenia Host-LAN**. Stwórz odpowiednie konto do obsługi tunelu.

Kliknij np. indeks 1 i wpisz odpowiednie dane. Konfiguracja zgodna z założeniami przykładu:

- zaznacz **Włącz konto**
- ustaw **Czas nieaktywności**. Domyślnie jest tam wartość 300 oznaczająca rozłączenie tunelu po 5 minutach, gdy Vigor nie odnotuje ruchu VPN. Wpisz **0** w polu czas nieaktywności jeśli Vigor ma pozostawić połączenie pomimo braku ruchu. PPTP posiada wbudowane mechanizmy detekcji połączenia.
- jako akceptowany protokół zaznacz **PPTP**
- wpisz Użytkownika. W przykładzie użyto użytkownika 'test'
- włącz mOTP. W przykładzie użyto PINu 1234 oraz klucza Secret wygenerowanego przez aplikację mOTP

VPN i Dostęp Zdalny >> Użytkownik zdalny

Indeks Nr. 1

<p><b>Konto użytkownika</b></p> <p><input checked="" type="checkbox"/> Włącz konto</p> <p>Czas nieaktywności <input type="text" value="0"/> sek</p>	<p><b>Użytkownik</b> test</p> <p>Hasło(Maks. 19 znaków) <input type="text"/></p> <p><input checked="" type="checkbox"/> Włącz mOTP(Mobile One-Time Passwords)</p> <p>Kod PIN <input type="text" value="1234"/></p> <p>Klucz <input type="text" value="7316c7d20bcc55e2"/></p> <p>Secret <input type="text"/></p>
<p><b>Akceptowane protokoły</b></p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input type="checkbox"/> Tunel IPsec</p> <p><input type="checkbox"/> L2TP z polisą IPsec <input type="text" value="Brak"/></p> <p><input type="checkbox"/> Tunel SSL</p> <p><input type="checkbox"/> Określ węzeł zdalny</p> <p>IP klienta zdalnego <input type="text"/></p>	<p><b>Metoda uwierzytelniania IKE</b></p> <p><input checked="" type="checkbox"/> Klucz PSK</p> <p><input type="text" value="IKE PSK"/></p> <p><input type="checkbox"/> Podpis cyfrowy(X.509)</p> <p><input type="text" value="Brak"/></p>

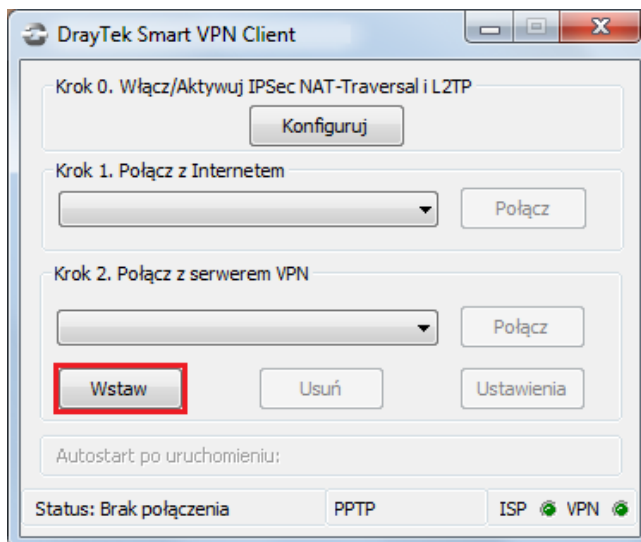
- jeśli chcesz dodatkowo weryfikować adres IP inicjującego połączenie zaznacz opcję **Określ węzeł zdalny**, a w polu **Adres IP klienta zdalnego** wpisz odpowiedni adres IP klienta VPN.

Określ węzeł zdalny

Adres IP klienta zdalnego

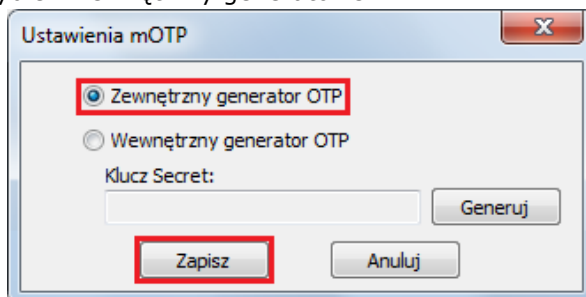
### 3. Konfiguracja klienta VPN

Kliknij przycisk **Wstaw**.



Wypełnij dane dotyczące adresu serwera i typu VPN:

- w polu Nazwa profilu wpisz dowolną nazwę dla połączeni np. To Vigor
- w polu Adres IP Serwera/Nazwa Hosta wpisz adres IP routera (w przykładzie 99.99.99.10), do którego zestawiasz tunel VPN, albo jego nazwę (w przykładzie serwer.abc.xyz).
- w polu Nazwa użytkownika wpisz odpowiednią nazwę zgodną ze stworzonym profilem. W przykładzie użyto 'test'
- włącz mOTP
- W ustawieniach mOTP wybierz zewnętrzny generator OTP

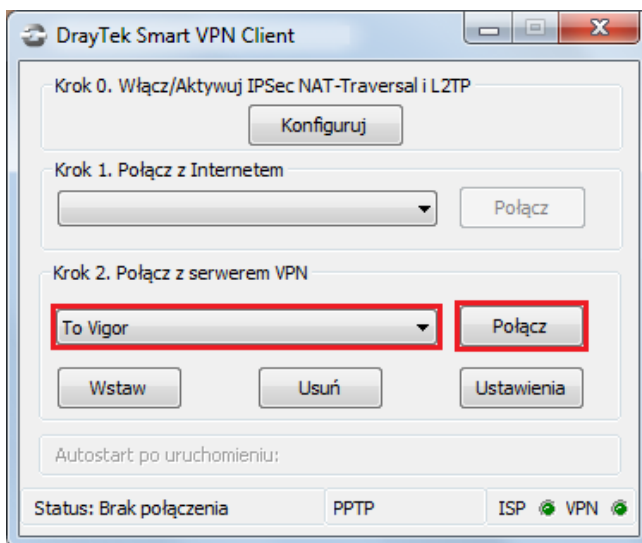


- w polu Typ połączenia VPN wybierz PPTP
- kliknij przycisk OK, aby kontynuować

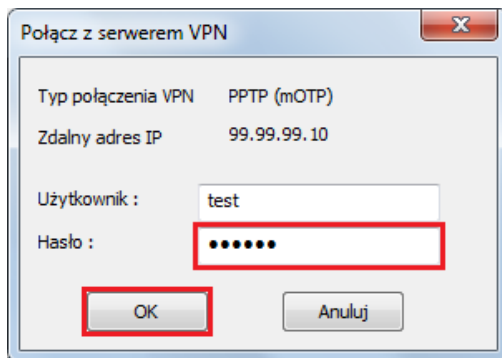
Wypełnij dane dotyczące Ustawień PPTP:

- w polu Metoda uwierzytelniania wybierz MS-CHAP v2
- w polu Szyfrowanie MPPE wybierz odpowiednią opcję zgodną z ustawieniami na Vigorze. W przykładzie użyto opcji Wymagane szyfrowanie
- kliknij przycisk OK, aby zapisać zmiany

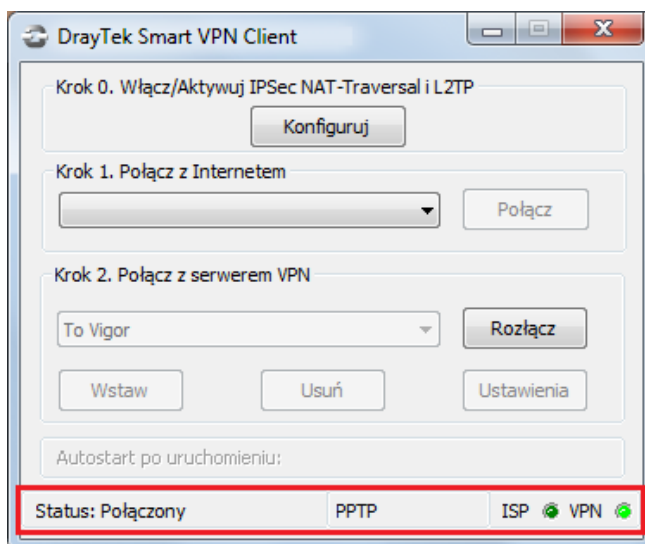
Wybierz odpowiedni profil a następnie kliknij Połącz.



Wygeneruj i wpisz hasło mOTP.



Przy poprawnym połączeniu zmieni się status na Połączony oraz zapali się zielone światło przy polu VPN.



### 4. Status Połączenia

#### 4.1. Klient VPN

Wybierz Menu Start a następnie Uruchom i wpisz cmd. Następnie wykonaj polecenie: ipconfig. Po wcześniejszym zainicjowaniu tunelu otrzymasz adres IP z sieci zdalnej. W omawianym przykładzie 192.168.0.10.

```
C:\>ipconfig

Konfiguracja IP systemu Windows

Karta PPP To Vigor:

Sufiks DNS konkretnego połączenia :
Adres IP. . . . . : 192.168.0.10
Maska podsieci. . . . . : 255.255.255.255
Brama domyślna. . . . . :
```

Dodatkowo wystarczy np. zwykły ping. Wykonaj polecenie ping adres\_LAN\_serwera (w przykładzie serwer VPN posiada adres LAN 192.168.0.1). Poprawna odpowiedź na ping świadczy o poprawnej komunikacji w tunelu VPN.

```
C:\>ping 192.168.0.1

Badanie 192.168.0.1 z użyciem 32 bajtów danych:

Odpowiedź z 192.168.0.1: bajtów=32 czas=1ms TTL=255
Odpowiedź z 192.168.0.1: bajtów=32 czas=1ms TTL=255
Odpowiedź z 192.168.0.1: bajtów=32 czas=1ms TTL=255
Odpowiedź z 192.168.0.1: bajtów=32 czas=1ms TTL=255

Statystyka badania ping dla 192.168.0.1:
Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
Minimum = 1 ms, Maksimum = 1 ms, Czas średni = 1 ms
```

#### 4.2. Serwer VPN

O tym, czy tunel został zainicjowany, możesz przekonać się wybierając **VPN i Dostęp Zdalny>>Kontrola połączeń** (rysunek poniżej).

VPN i Dostęp Zdalny>> Kontrola połączeń

Wymuszanie inicjacji połączeń Czas odświeżania : 10

Tryb główny:

Tryb backup:

Tryb rozkładu obciążenia:

---

Stan połączenia VPN

Bieżąca strona: 1 Nr strony

VPN	Typ	Zdalny IP	Sieć wirtualna	Tx pakietów	Tx prędk.(Bps)	Rx pakietów	Rx prędk.(Bps)	Czas akt.	
1 ( test ) Local User Database	PPTP/MPPE	99.99.99.11 via WAN1	192.168.0.10/32	4	27	342	276	0:1:38	<input type="button" value="Rozłącz"/>

xxxxxxx : Dane są szyfrowane.  
xxxxxxx : Dane nie są szyfrowane.

Krzysztof Skowina  
Specjalista ds. rozwiązań sieciowych  
[k.skowina@brinet.pl](mailto:k.skowina@brinet.pl)