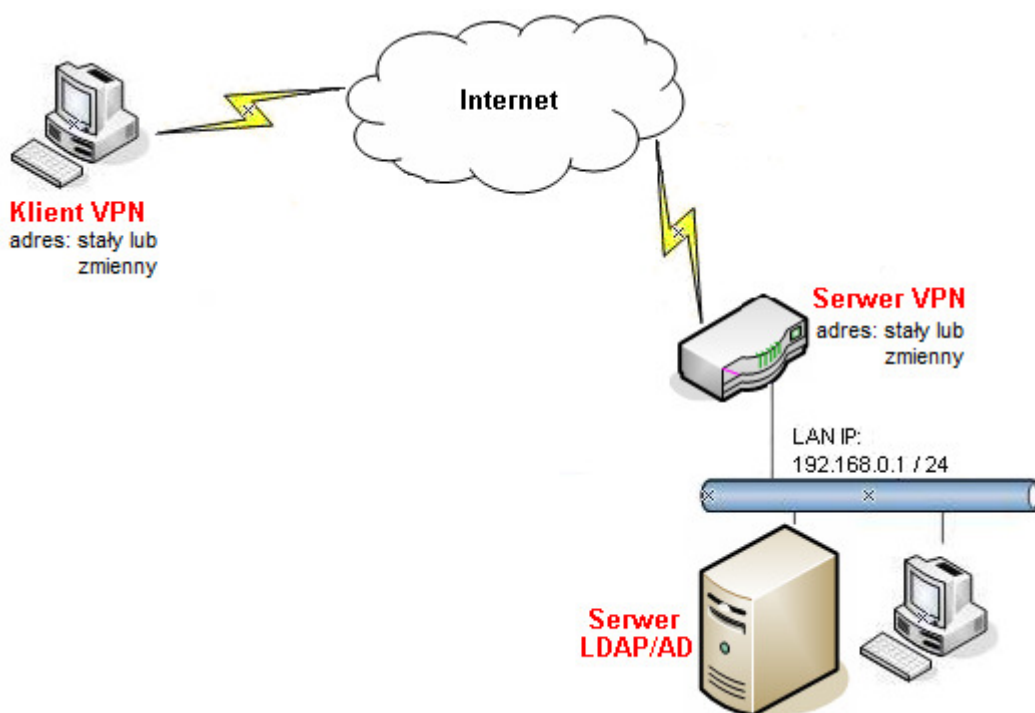


1. Konfiguracja serwera VPN
  - 1.1. LDAP/AD
  - 1.2. Ustawienia ogólne
  - 1.3. Konto PPTP
2. Konfiguracja klienta VPN
3. Status połączenia
  - 3.1. Klient VPN
  - 3.2. Serwer VPN

Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

- typ tunelu: Host-LAN
- protokół VPN: PPTP
- brak szyfrowania
- uwierzytelnianie PAP
- Adres Serwera VPN: stały (IP - 99.99.99.10) lub zmienny (domenowy - serwer.abc.xyz)
- Adres Klienta VPN: stały (IP - 99.99.99.11) lub zmienny
- Serwer LDAP/AD:
  - adres IP: 192.168.0.254
  - domena: abc.xyz
  - użytkownik test znajduje się w CN=Users, DC=abc, DC=xyz

### Uwagi

- Dla autentykacji LDAP/AD z użyciem PPTP Vigor wspiera tylko uwierzytelnianie PAP bez szyfrowania.
- 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. Konfiguracja serwera VPN

### 1.1. LDAP/AD

Przeglądarka serwera Active Directory:

Active Directory Explorer - Sysinternals: www.sysinternals.com [192.168.0.254 [abc2003.abc.xyz]]

File Edit Favorites Search Compare History Help

Path: CN=Users,DC=abc,DC=xyz,192.168.0.254 [abc2003.abc.xyz]

Attribute	Syntax	Count	Value(s)
cn	DirectoryString	1	Users
description	DirectoryString	1	Default container for upgraded user accounts
distinguishedName	DN	1	CN=Users,DC=abc,DC=xyz
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
name	DirectoryString	1	Users
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLC
objectCategory	DN	1	CN=Container,CN=Schema,CN=Configuration,DC=abc,DC=xyz
objectClass	OID	2	top;container
objectGUID	OctetString	1	{23A53274-FE85-4FD8-A1F2-28A682D2BC84}
showInAdvancedViewO...	Boolean	1	FALSE
systemFlags	Integer	1	-1946157056
uSNCreated	Integer8	1	0x10D0
whenCreated	GeneralizedTime	1	2010-09-22 12:34:26
whenChanged	GeneralizedTime	1	2010-09-22 12:34:26

Przejdź do zakładki **Aplikacje i usługi >> LDAP/Active Director**.

Typy powiązania:

- prosty: uwierzytelnianie bez akcji wyszukiwania
- anonimowy: najpierw akcja anonimowego wyszukiwania, następnie uwierzytelnianie
- regularny: podobny do trybu anonimowego. Różnica polega na tym, że serwer sprawdza prawa do wyszukiwania. Konieczność zdefiniowania użytkownika oraz hasła.

Poniżej konfiguracja zgodna z założeniami przykładu.

Aplikacje i Usługi >> Active Directory /LDAP

Active Directory /LDAP | [Ustawienia domyślne](#) |

**Ustawienia ogólne**
**Profile Active Directory / LDAP**

Włącz

Typ powiązania Tryb regularny ▾

Adres serwera 192.168.0.254

Port docelowy 389

Użyj SSL

Regularny - DN CN=Administrator, CN=Users, DC=abc, [

Regularny - Hasło ●●●●●●

Aplikacje i Usługi >> Active Directory /LDAP

Active Directory /LDAP | [Ustawienia domyślne](#) |

**Ustawienia ogólne**
**Profile Active Directory / LDAP**

Indeks	Nazwa	Nazwa wyróżniająca DN
1.	test	

Aplikacje i Usługi >> Active Directory /LDAP>>Profil serwera

Indeks Nr 1

Nazwa test

Identyfikator nazwy CN cn

Podstawowa nazwa wyróżniająca DN CN=Users, DC=abc, DC=xyz

Dodatkowy filtr

Grupowa nazwa wyróżniająca DN

### 1.2. Ustawienia ogólne

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**. Zaznacz stworzony profil AD/LDAP.

VPN i Dostęp Zdalny>> Ustawienia ogólne PPP

#### Ustawienia ogólne PPP

<p><b>Parametry PPP dla VPN</b></p> <p>Uwierzytelnianie ppp: PAP/CHAP/MS-CHAP/MS-CHAPv2</p> <p>Opcje szyfrowania PPP(MPPE): Opcjonalny MPPE</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>192.168.1.200</td></tr> <tr><td></td><td>LAN 2</td><td>192.168.2.200</td></tr> <tr><td></td><td>LAN 3</td><td>192.168.3.200</td></tr> <tr><td></td><td>LAN 4</td><td>192.168.4.200</td></tr> <tr><td></td><td>LAN 5</td><td>192.168.5.200</td></tr> </table>	Początkowy IP	LAN 1	192.168.1.200		LAN 2	192.168.2.200		LAN 3	192.168.3.200		LAN 4	192.168.4.200		LAN 5	192.168.5.200	<p><b>Metody uwierzytelniania PPP</b></p> <p><input checked="" type="checkbox"/> Użytkownik zdalny</p> <p><input checked="" type="checkbox"/> RADIUS</p> <p><input checked="" type="checkbox"/> AD/LDAP</p> <p><input checked="" type="checkbox"/> test</p> <p><b>Uwaga:</b> Wybierz 'Tylko PAP' w ustawieniach ogólnych PPP jeśli chcesz używać AD/LDAP do uwierzytelniania!!</p> <p><b>Uwaga:</b> Domyślny priorytet: użytkownik zdalny -&gt; RADIUS -&gt; AD/LDAP.</p> <p><b>Kiedy używane uwierzytelnianie Radius lub LDAP:</b> Przypisz IP z podsięci: LAN1</p>
Początkowy IP	LAN 1	192.168.1.200														
	LAN 2	192.168.2.200														
	LAN 3	192.168.3.200														
	LAN 4	192.168.4.200														
	LAN 5	192.168.5.200														

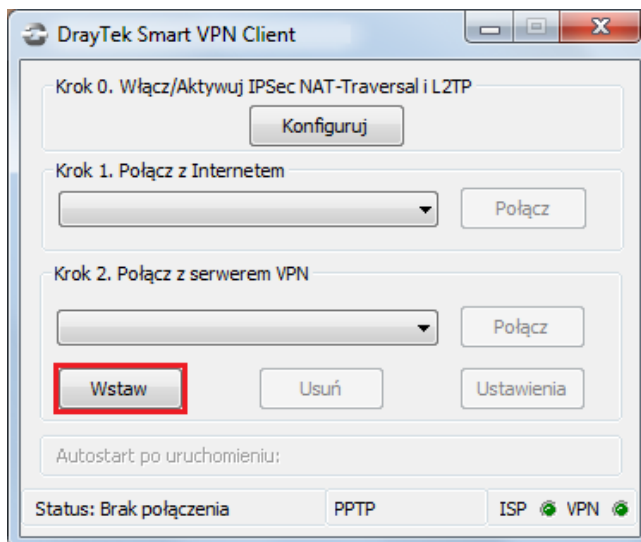
#### Uwaga

Kolejność sprawdzania konta użytkownika podczas uwierzytelniania:

1. Lokalna baza danych
2. RADIUS
3. AD/LDAP

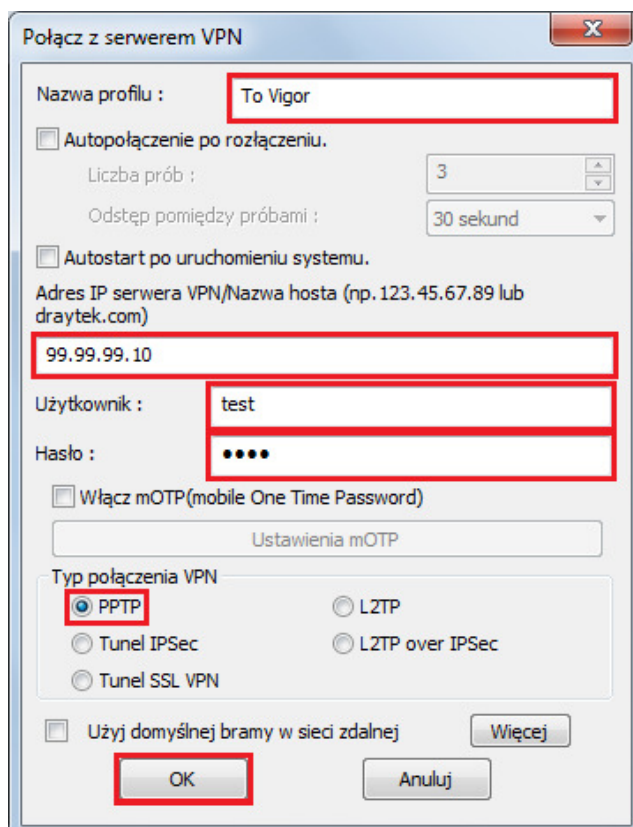
### 2. Konfiguracja klienta VPN

Kliknij przycisk **Wstaw**.



Wypełnij dane dotyczące adresu serwera i typu VPN:

- w polu Nazwa profilu wpisz dowolną nazwę dla połączenia 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 użytkownik wpisz odpowiednią nazwę zgodną ze stworzonym profilem. W przykładzie użyto 'test'
- w polu Hasło wpisz odpowiednie hasło zgodne z serwerem LADAP/AD. W przykładzie użyto 'test'
- w polu Typ połączenia VPN wybierz PPTP
- kliknij przycisk OK, aby kontynuować



Wypełnij dane dotyczące Ustawień PPTP:

- w polu Metoda uwierzytelniania wybierz PAP
- kliknij przycisk OK, aby zapisać zmiany

Ustawienia PPTP

Metoda uwierzytelniania: PAP

Szyfrowanie MPPE: Brak szyfrowania

Uzyskaj adres IP oraz serwera DNS automatycznie

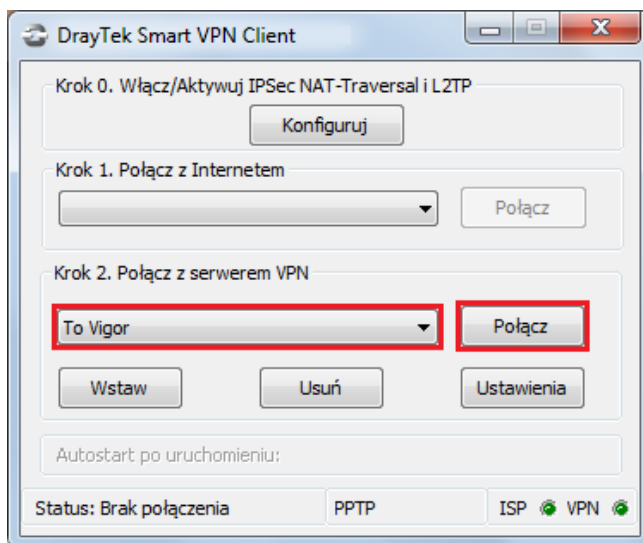
Użyj następującego adresu IP oraz serwera DNS:

Adres IP: 192 . 168 . 1 . 10

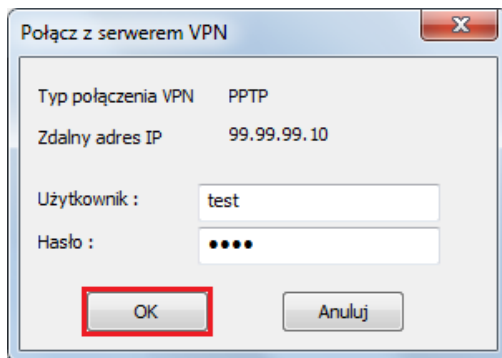
Adres DNS: 192 . 168 . 1 . 1

OK Anuluj

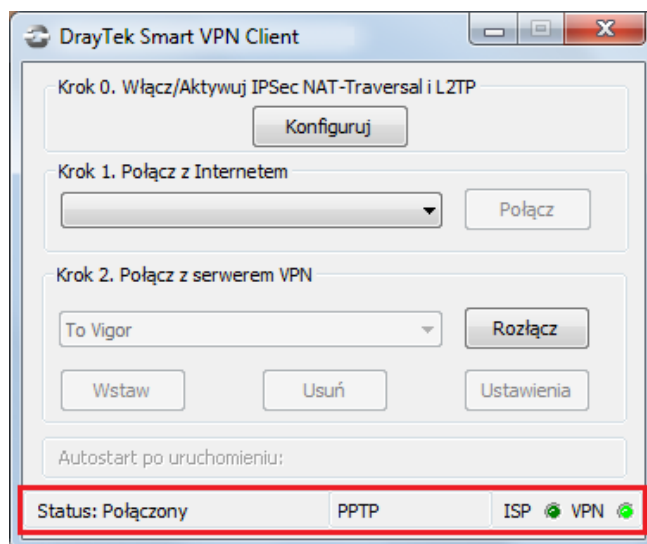
Wybierz odpowiedni profil a następnie kliknij Połącz.



Następnie kliknij OK.



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



### 3. Status Połączenia

#### 3.1. 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
```

#### 3.2. Serwer VPN

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

**VPN i Dostęp Zdalny>> Zarządzanie połączeniem**

---

**Wymuszanie inicjacji połączeń** Czas odświeżania : 10

Tryb Główny:

Tryb Backup:

**Stan połączenia VPN**

Bieżąca strona: 1 Nr strony  >>

VPN	Typ	Zdalny IP	Sieć wirtualna	Tx pakietów	Tx prędkość	Rx pakietów	Rx prędkość	Czas akt.
1 (test) LDAP/AD Authentication	PPTP	99.99.99.11	192.168.0.10/32	328	9668	308	1840	0:0:21

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

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