Igor Zawartka  
Klasa 2ia  
Grupa 2.  
2020.11.23

Ćwiczenie 008  
**VPN**

# Wstęp

**Połączenie VPN** pozwala ukryć przed np. naszym dostawcą nasz ruch sieciowy. Będzie on jednak nadal widoczny dla serwera VPN i jego dostawcy. Inną zaletą jest możliwość pominięcia blokad regionalnych i banów na IP.

**Site-to-site VPN** jest to typ VPNu, w którym szyfrowanie i deszyfrowanie odbywa się przez router na obu końcach.

# Protokoły VPN

## Protocol Point to Point (PPTP)

**(PORT TCP 1723)**

Najprostszy z protokołów i zarazem najszybszy. Do jego zalet należy również łatwość konfiguracji i kompatybilność. Niestety jego szyfrowanie zostało już dawno złamane i jest uznawany za mało bezpieczny.

## Layer 2 Tunneling Protocol & IPsec (L2TP/IPsec)

**(PORT UDP 1701 / 500)**

Jest to połączenie dwóch protokołów, które zastosowane razem tworzą bezpieczne i szybkie połączenie VPN. Podobnie jak poprzedni, ten protokół również jest dosyć łatwy w konfiguracji i kompatybilny. Istnieją jednak podejrzenia, że IPsec został już złamany, przez co jego bezpieczeństwo bywa podważane.

## Internet Key Exchange V2 (IKEV2)

**(PORT UDP 500)**

Został opracowany przez Microsoft i jest podobny do L2TP/IPsec. Niestety również używa on protokołu IPsec przez co nie może być zaklasyfikowany jako całkowicie bezpieczny. Podobnie jak poprzednicy, jest on szybki i w miarę łatwy do skonfigurowania.

## Secure Socket Tunneling Protocol (SSTP)

**(PORT TCP 443)**

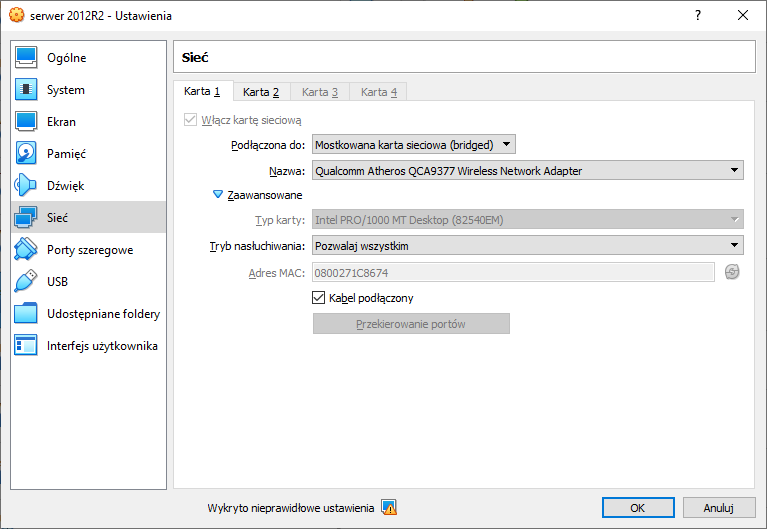
Domyślnie używa on portu 443, przez co przepuszczany jest przez większość Firewalli blokujących ruchy VPN. Póki co jego szyfrowanie nie zostało złamane, więc można go uznać za bezpieczny. Ponadto rozwijany jest on przez Microsoft, dzięki czemu dostajemy go w pakiecie z Windowsem jeszcze od czasów Visty SP1. Ma to jednak swoją wadę, gdyż nie ma on otwartych źródeł, a instalacja na systemach innych niż Windows jest dosyć trudna.

## OpenVPN

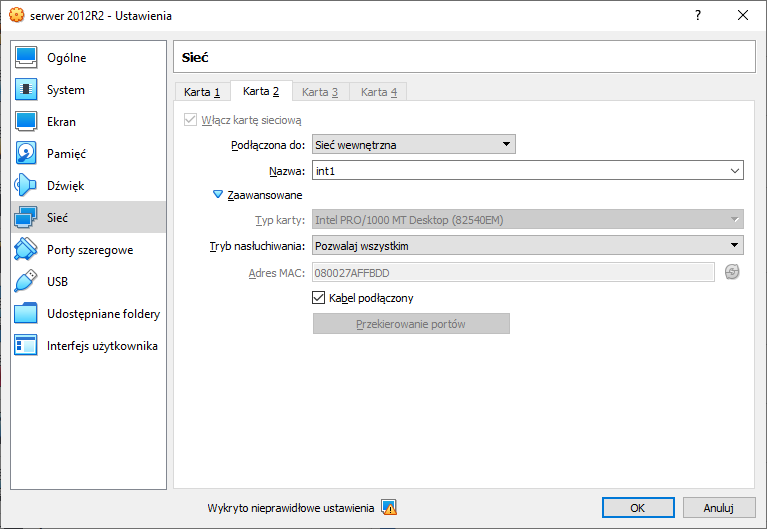
**(PORT TCP / UDP 1194)**

Jest to dosyć nowoczesny protokół, bezpieczny i z otwartym źródłem. Pozwala on na szyfrowanie jednym z kilku algorytmów do wyboru. Jego wadami jest konieczność zainstalowania zewnętrznego oprogramowania oraz trudność konfiguracji w porównaniu z konkurencyjnymi protokołami.

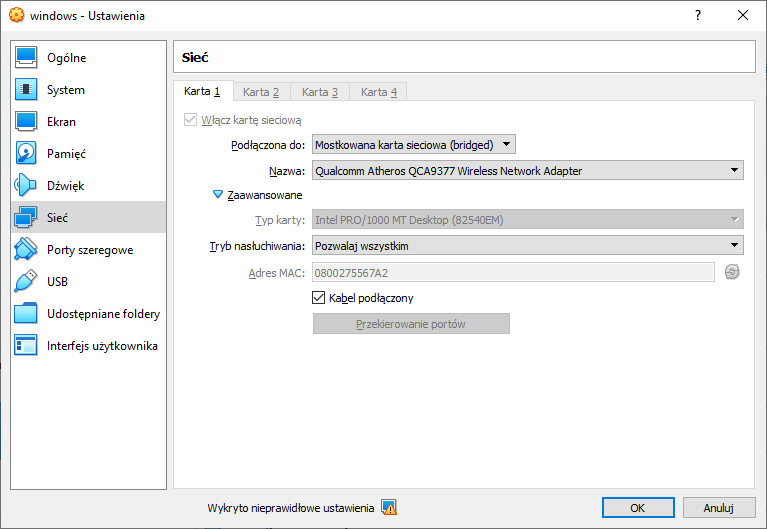
# Przygotowanie komputerów



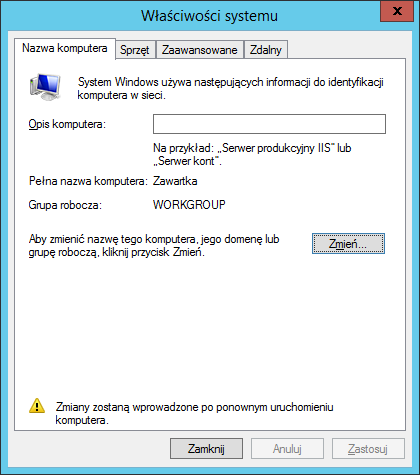
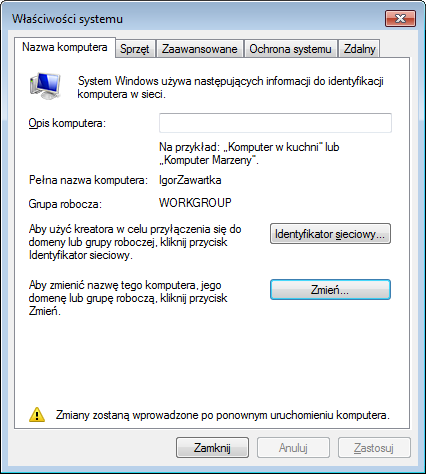
Obrazek : Konfiguracja pierwszej karty na serwerze



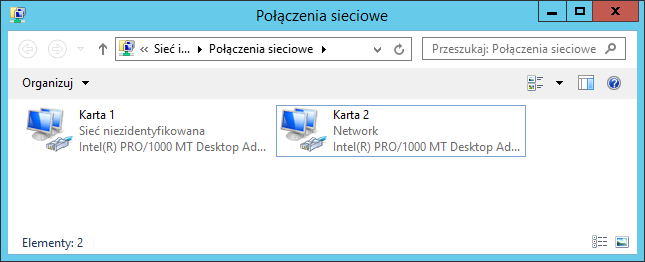
Obrazek : Konfiguracja drugiej karty na serwerze



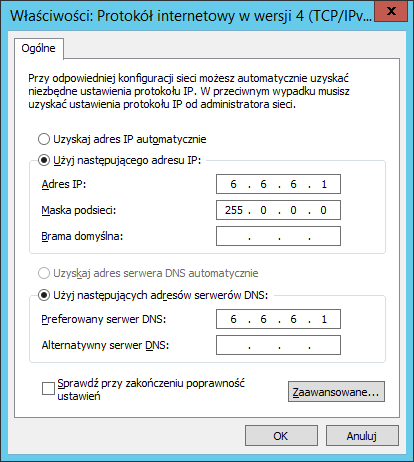
Obrazek : Konfiguracja karty klienta



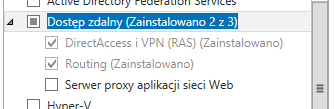
Obrazek : Zmiana nazw komputerów serwera i klienta



Obrazek : Karty sieciowe na serwerze



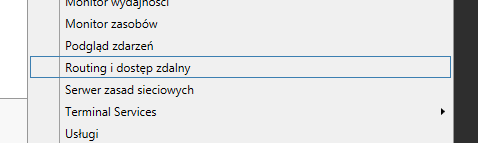
Obrazek : Konfiguracja IPv4 karty bez dostępu do internetu



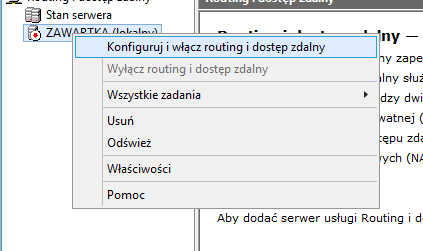
Obrazek : Zainstalowanie roli dostępu zdalnego

(u mnie już zainstalowany, następnie trzeba także wybrać funkcję VPN)

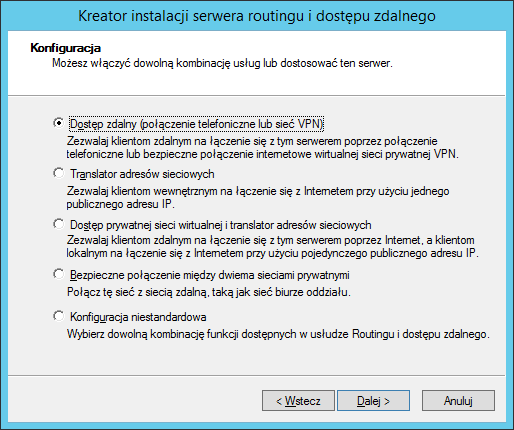
# Konfiguracja VPN



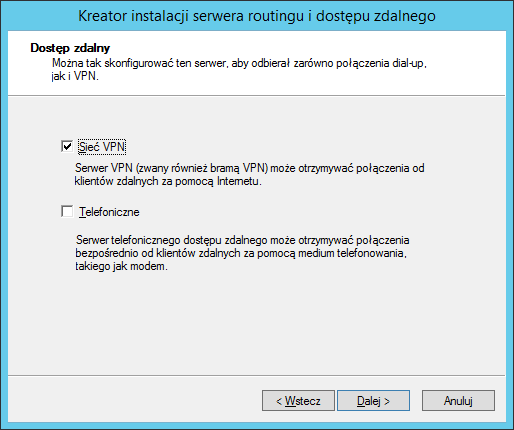
Obrazek : Uruchomienie narzędzia "Routing i dostęp zdalny"



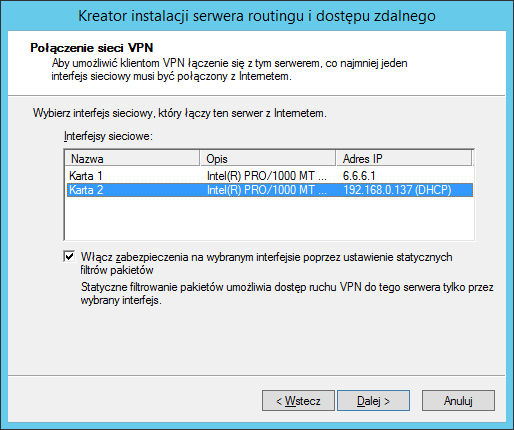
Obrazek : Wybranie opcji powyżej



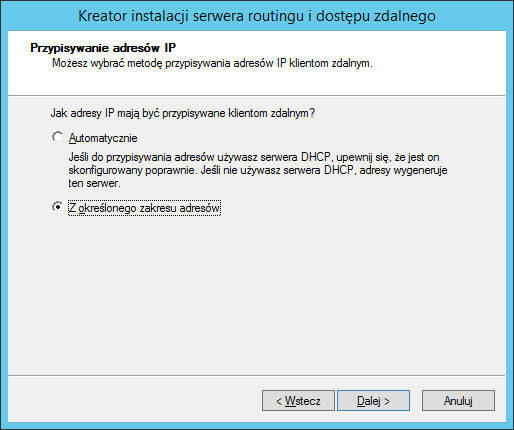
Obrazek : Wybranie opcji "Dostęp zdalny"



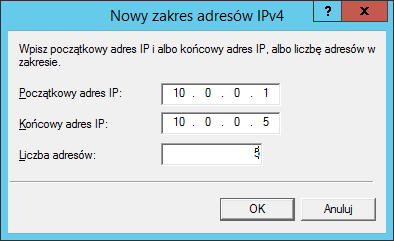
Obrazek : Wybranie "Sieć VPN"



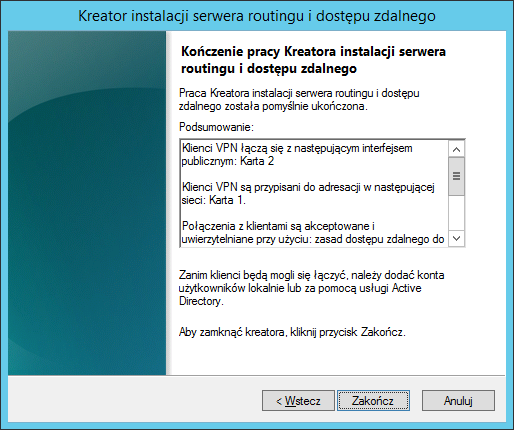
Obrazek : Wybranie karty sieciowej z dostępem do internetu



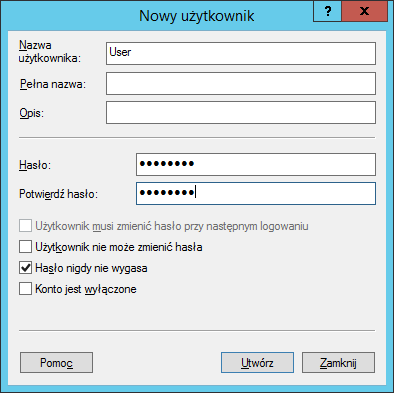
Obrazek : Wybranie drugiej opcji



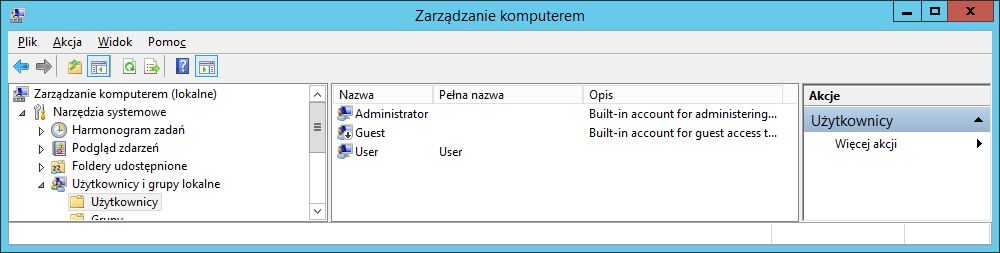
Obrazek : Stworzenie nowego zakresu adresów IP



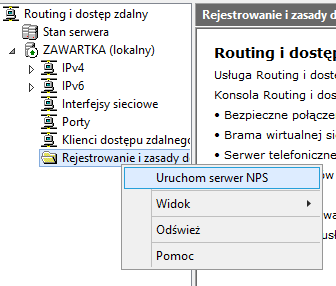
Obrazek : Zakończenie pracy kreatora



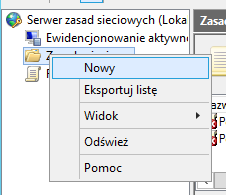
Obrazek : Stworzenie nowego użytkownika



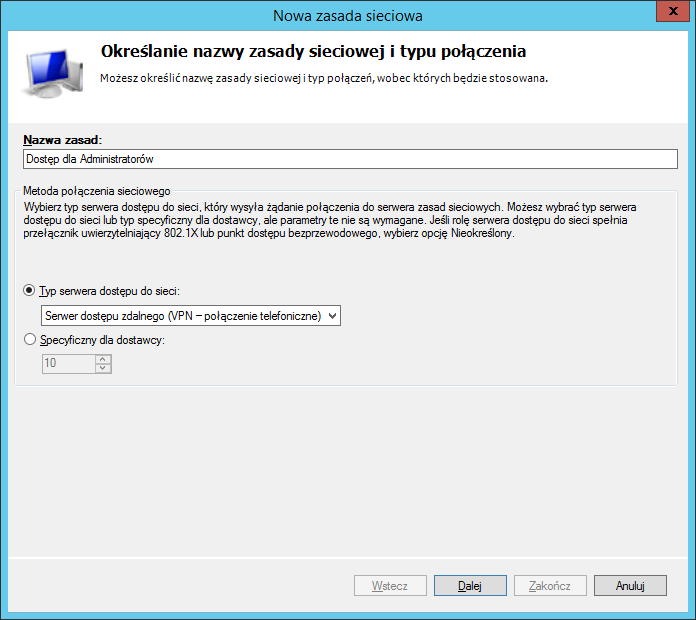
Obrazek : Użytkownicy



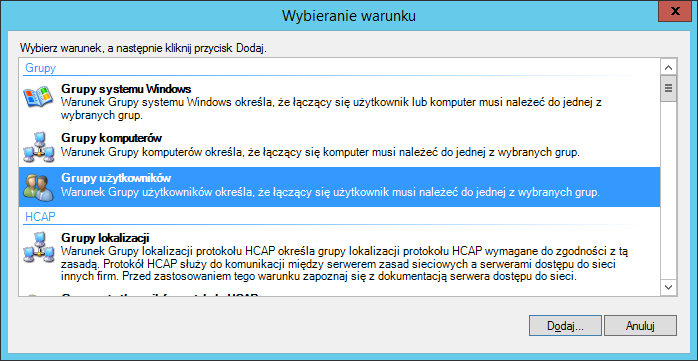
Obrazek : Uruchomienie serwera NPS



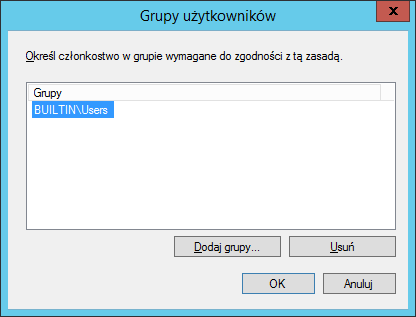
Obrazek : Dodanie nowej zasady sieciowej



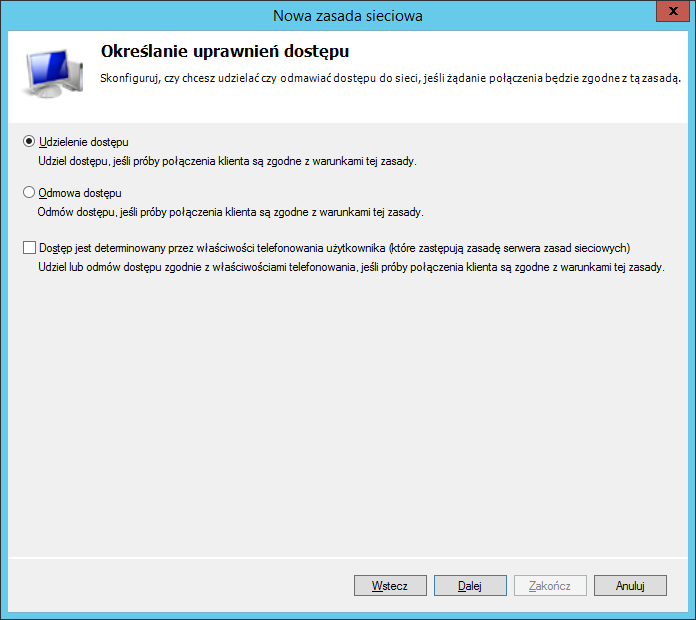
Obrazek : Ustawienie nazwy i typu zasady



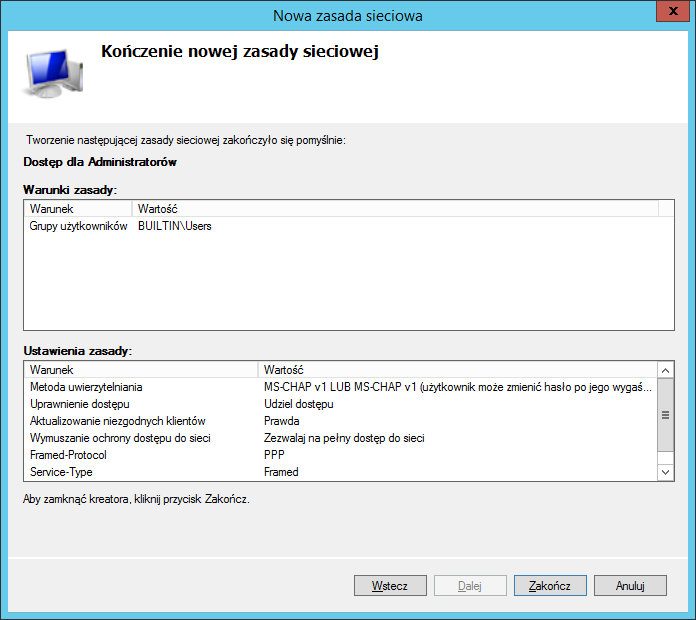
Obrazek : Dodanie warunku



Obrazek : Dodanie grupy Users

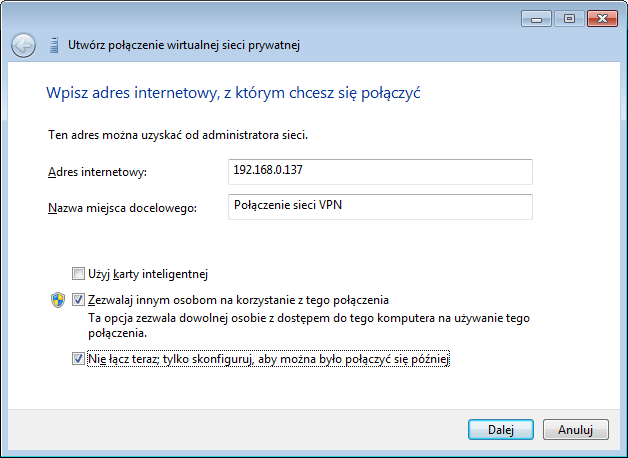


Obrazek : Wybranie opcji "Udzielenie dostępu"

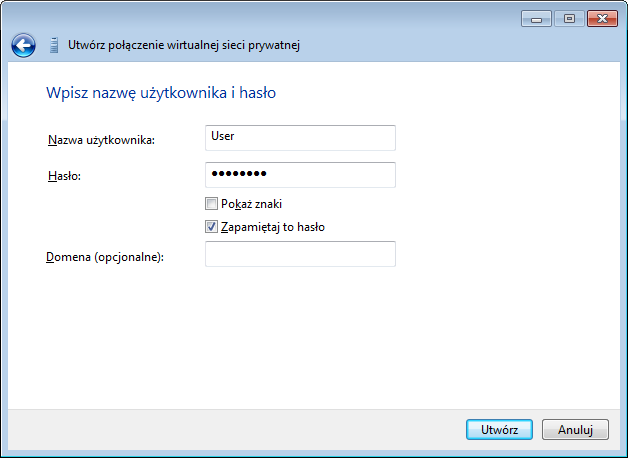


Obrazek : Potwierdzenie dodania zasady

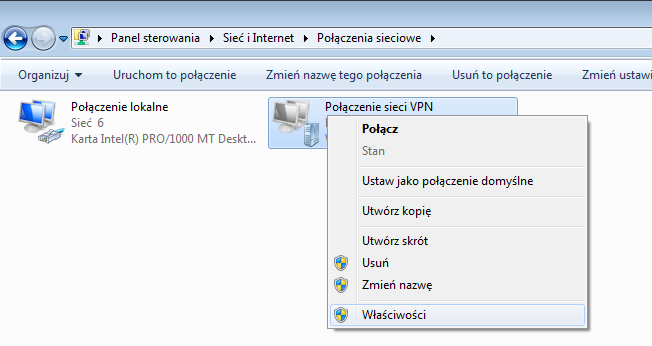
# Testowe połączenie



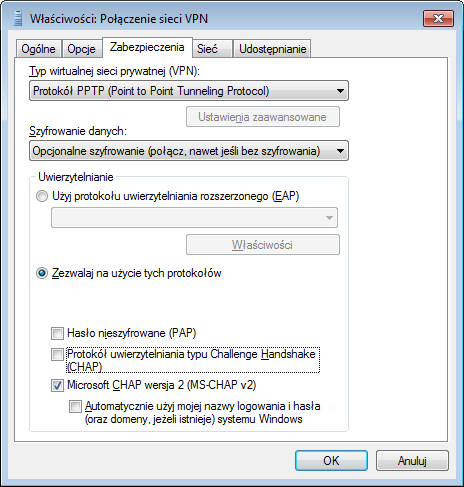
Obrazek : Utworzenie nowego połączenia VPN



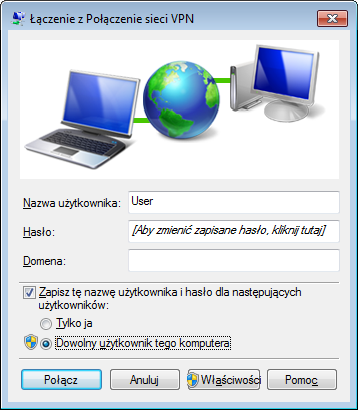
Obrazek : Zalogowanie się na użytkownika User



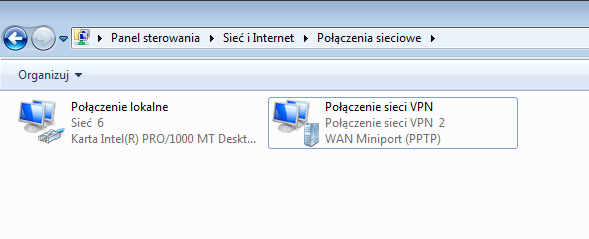
Obrazek : Przejście do ustawień VPN



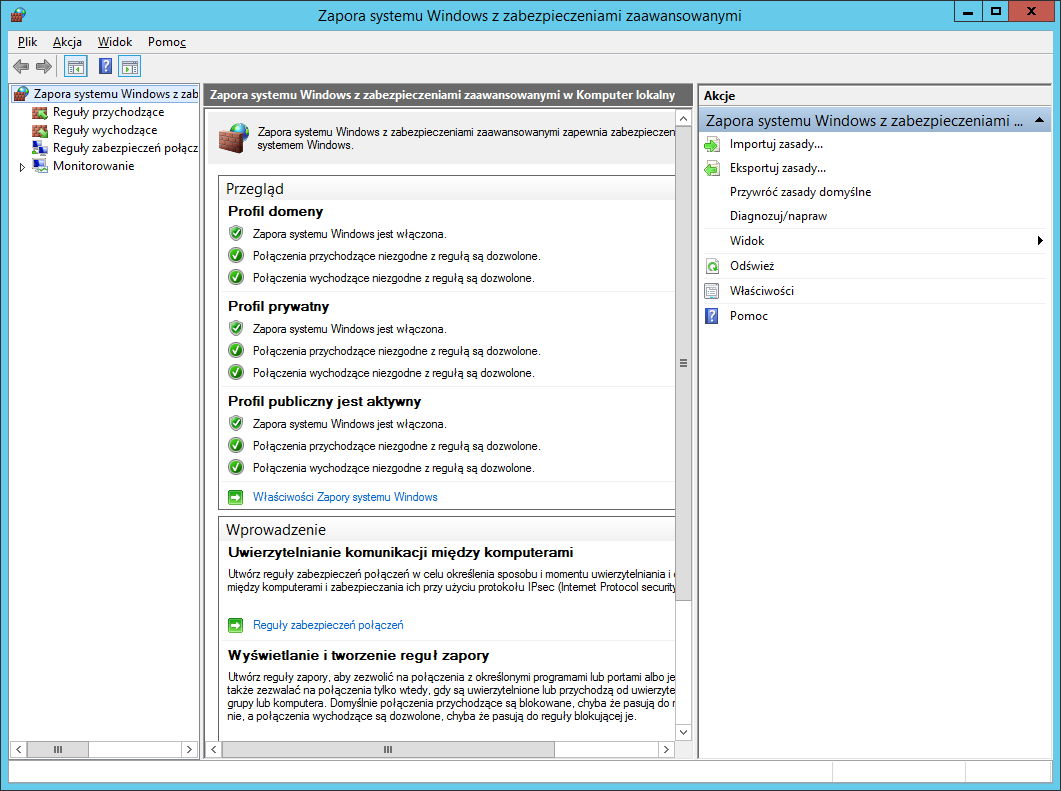
Obrazek : Skonfigurowanie protokołów i zabezpieczeń połączenia



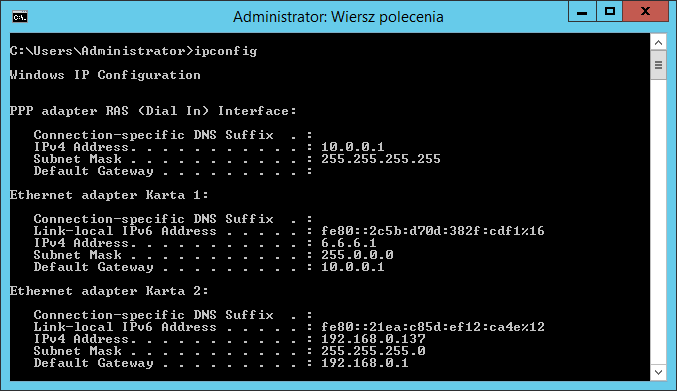
Obrazek : Połączenie się



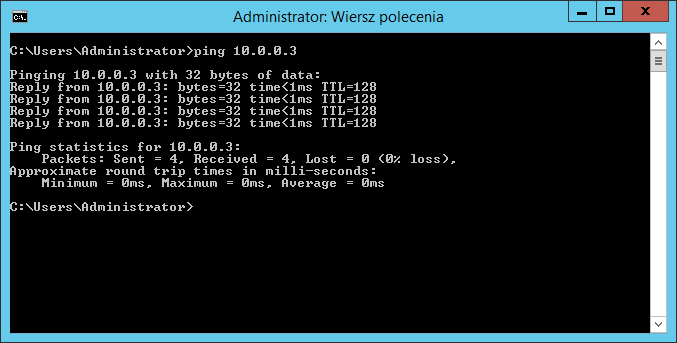
Obrazek : Udało się połączyć!



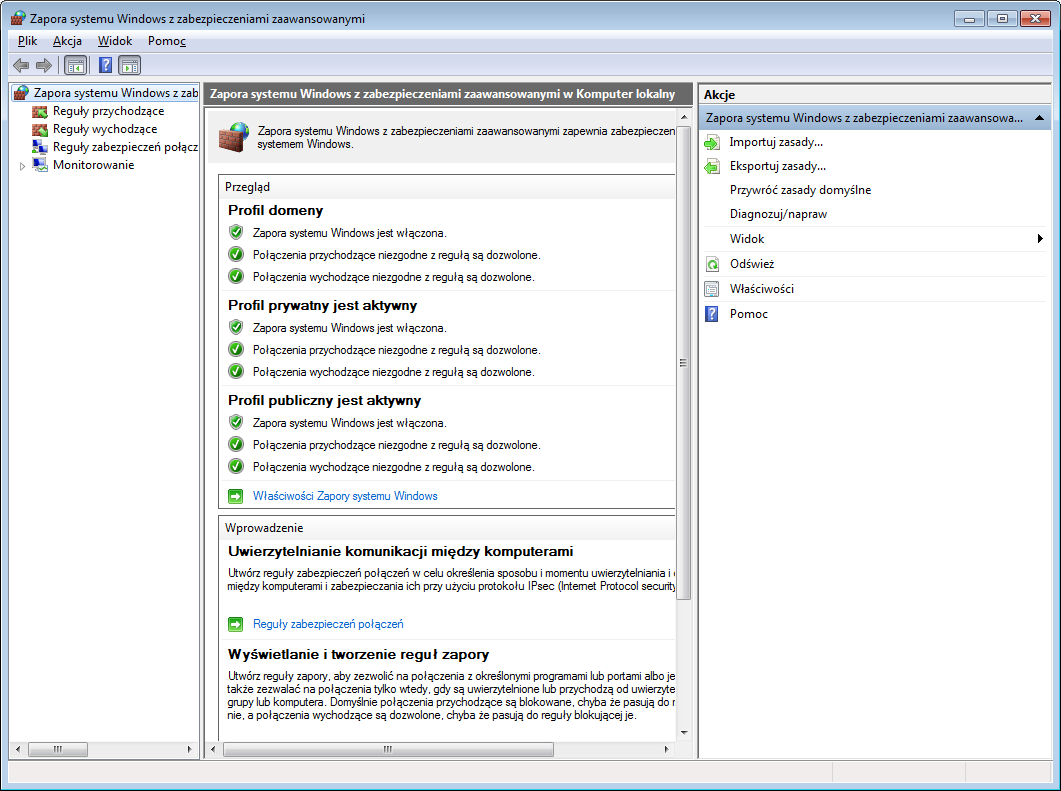
Obrazek : Zapora na serwerze



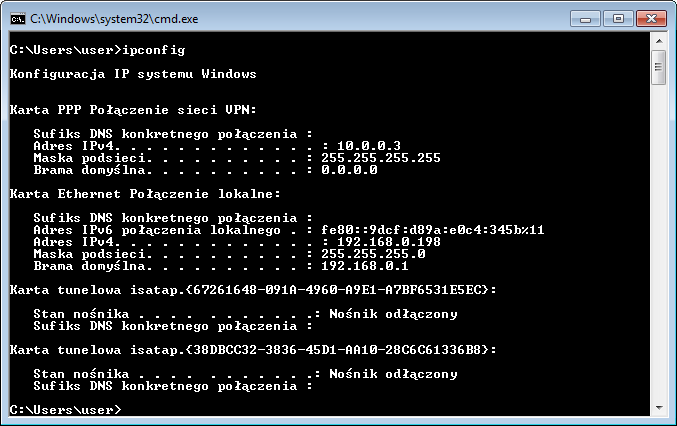
Obrazek : Polecenie ipconfig z serwera



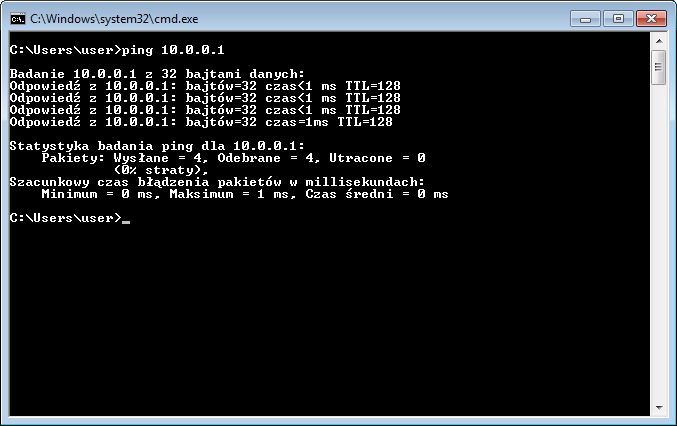
Obrazek : Ping z serwera do klienta



Obrazek : Zapora na kliencie



Obrazek 35: Polecenie ipconfig z klienta



Obrazek : Ping z klienta do serwera

Spis treści

[Wstęp 1](#_Toc57128829)

[Protokoły VPN 1](#_Toc57128830)

[Protocol Point to Point (PPTP) 1](#_Toc57128831)

[Layer 2 Tunneling Protocol & IPsec (L2TP/IPsec) 1](#_Toc57128832)

[Internet Key Exchange V2 (IKEV2) 1](#_Toc57128833)

[Secure Socket Tunneling Protocol (SSTP) 1](#_Toc57128834)

[OpenVPN 1](#_Toc57128835)

[Przygotowanie komputerów 2](#_Toc57128836)

[Konfiguracja VPN 5](#_Toc57128837)

[Testowe połączenie 12](#_Toc57128838)