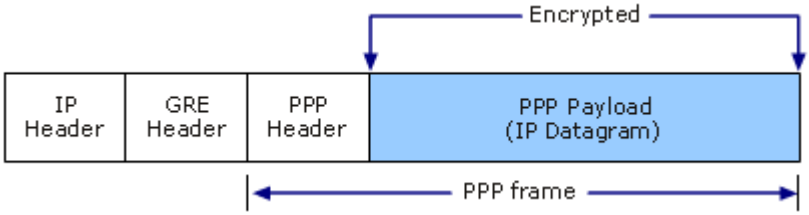
Tworzenie połączeń VPN.

Lokalne sieci komputerowe są jedną z najistotniejszych funkcji sieci komputerowych. O ile dostęp do sieci rozległej (Internet) jest niemal wymagany do codziennego funkcjonowania firmy (dostęp do bankowości elektronicznej, dostęp do wiadomości elektronicznych, portali aukcyjnych czy elektronicznej obsługi urzędowej), o tyle w przedsiębiorstwie posiadającym kilka stanowisk komputerowych połączenie lokalne i zapewnienie dostępu do usług lokalnych, jak serwer plików, wymiana bezpośrednia danych, dostęp do urządzeń drukujących/skanujących czy lokalnego serwera WWW jest znacznie ważniejsze. Sieć lokalna jest bowiem na 99,9% przypadków izolowana od połączeń rozległych (WAN), posiada własną adresację IP (zarówno w IPv4 jak i w IPv6) i tylko członkowie tejże sieci mogą korzystać z wyżej wymienionych usług.

INFORMACJA: W większych firmach/korporacjach sieć lokalna może przybrać formę Intranetu. Pierwszy człon (Intra) informuje, że mamy do czynienia z czymś wewnętrznym, drugi iż jest to sieć (w przypadku Internetu mamy do czynienia z czymś łączącym, jest pomiędzy sieciami). Jak łatwo się domyślić Intranet może spełniać te same funkcje co Internet (zapewniać dostęp do poczty, do stron WWW, programów i aplikacji HTML5) jednak tylko w obrębie wskazanej puli adresowej/sieci lokalnej. Rozwiązanie to jest o tyle popularne, że szczelnie izoluje (a przynajmniej powinno szczelnie izolować) powyżej wymienione usługi od sieci globalne. Dzięki temu nikt nie powinien zagrozić ich działaniu.

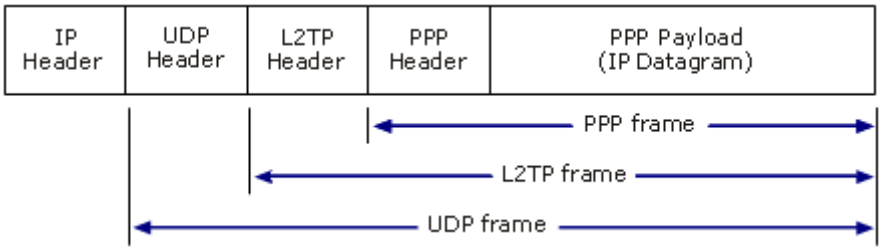
Niekiedy zachodzi potrzeba, by dany pracownik (np. przebywający w delegacji) miał dostęp do zasobów sieci lokalnej/intranetu. Normalnie takie połączenie nie byłoby możliwe. Jednak dzięki VPN (Virtual Private Network – Wirtualna Sieć Prywatna) możliwe jest korzystanie z sieci lokalnej będąc poza nią. Usługa ta tworzy bowiem tunel pomiędzy danym urządzeniem a serwerem dostępnym globalnie w sieci Internet. Jeżeli urządzenie (komputer) zostanie poprawnie zweryfikowany (login/hasło, plik klucza itd.) następuje włączenie go w strukturę sieci lokalnej. Od tej pory komputer widziany jest tak jakby znajdował się w budynku firmy, chociaż może być równie dobrze tysiące kilometrów dalej. Ponieważ transmisja jest najczęściej szyfrowana, dane przesyłane pomiędzy urządzeniami się bezpieczne (nawet w przypadku przechwycenia pakietów metodą np. człowiek pomiędzy bądź w trybie mieszanym).

System Windows Server pozwala na tworzenie następujących typów połączeń VPN:
- PPTP (Point-to-Point Tunneling Protocol) – połączenie ustanawiane pomiędzy klientem a serwerem. Dane transportowane są szyfrowane. Połączenia można ustanawiać zarówno w obrębie sieci lokalnej/intranetu jak i poprzez sieć globalną (Internet). Protokołem transportowym jest TCP. Ramka tego typu połączenia wygląda następująco:

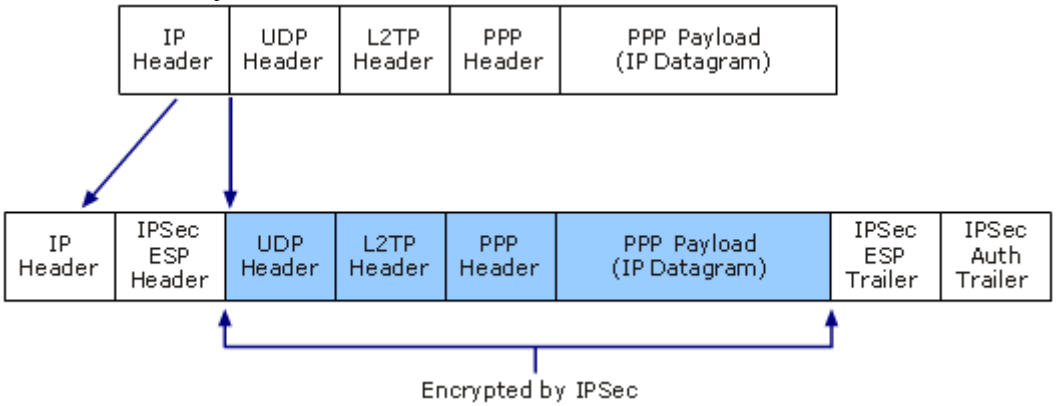


gdzie IP Header to nagłówek IP, GRE Header to nagłówek protokołu GRE (Generic Routing Encapsulation – Enkapsulacja Ogólnego Trasowania), PPP Header to nagłówek protokołu Punkt-Punkt oraz PPP Payload, który zawiera właściwą, zaszyfrowaną część ramki (dane).
- L2TP (Level Two Tunneling Protocol) – główną zaletą tego typu tuneli jest jego lekkość (bazuje na protokole UDP). Nazwa tunelu pochodzi od zawartego w nim protokołu L2F (Layer Two Forwarding) rozwijanego przez Cisco Systems; pozwala on na transportowanie niemal dowolnego protokołu w obrębie połączenia VPN (dzięki wykorzystywaniu UDP jako bazy). Poprzedni tunel także pozwala na transportowanie innych protokołów, jednak należy pamiętać, że opóźnienia generowane przez TCP mogą dla niektórych z nich generować błędy/powodować błędne działanie. Microsoft wykorzystuje do szyfrowania danych protokół IPSec. Stąd nazwa używana w systemie

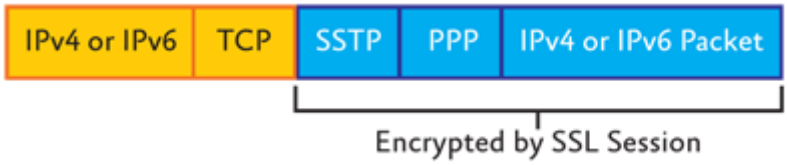
Windows – L2TP/IPSec. Trzeba pamiętać, że zarówno klient jak i serwer muszą obsługiwać protokół IPSec. Na chwilę obecną jest to jedno z lepszych i bardziej bezpiecznych połączeń oferowanych przez Microsoft dla protokołu IPv4.
Ramka L2TP:



Ramka L2TP/IPSec Encapsulation:



- SSTP (Secure Socket Tunneling Protocol) – ta wersja tunelowania wykorzystuje protokół HTTPS, czyli TCP na porcie 443. Bezpieczeństwo danych zapewnia protokół SSL. Polecany jest szczególnie przy połączeniach do lokalizacji, gdzie inne połączenia są niewykonalne – operator blokuje wszystkie usługi poza WWW (gdzie wykorzystywany jest właśnie port 80 i 443).
Ramka SSTP:



Proszę zauważyć, że jest to pierwszy rodzaj tunelowania VPN w pełni przystosowany do nowego protokołu IPv6.

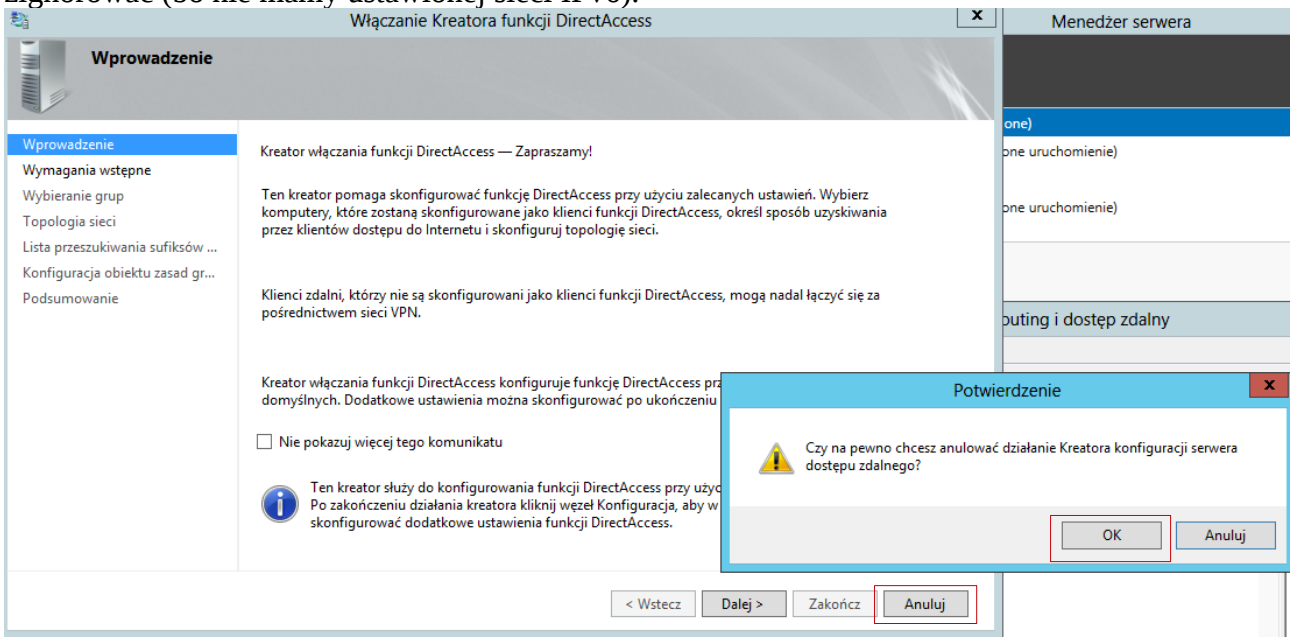
INFORMACJA: Firma Microsoft dla połączeń w IPv6 wprowadza zupełnie nowy rodzaj połączeń – DirectAccess (Połączenie bezpośrednie). W przypadku posiadania odpowiednich adresów prywatnych IPv6 (w stosie prywatnym) komputery będą tworzyć w swoim obrębie sieć LAN, która nie wymaga dodatkowych połączeń czy konfiguracji (IPv6 domyślnie szyfruje pakiety IPSec). W chwili obecnej usługa ta jest w fazie testowej, aczkolwiek jej stabilność pozwala na wdrażanie jej. Warunkiem jest posiadanie połączenia IPv6 (natywnego) z odpowiednią konfiguracją adresową.

Źródło: http://technet.microsoft.com/en-us/library/cc771298(v=ws.10).aspx
http://technet.microsoft.com/en-us/network/dd420463.aspx

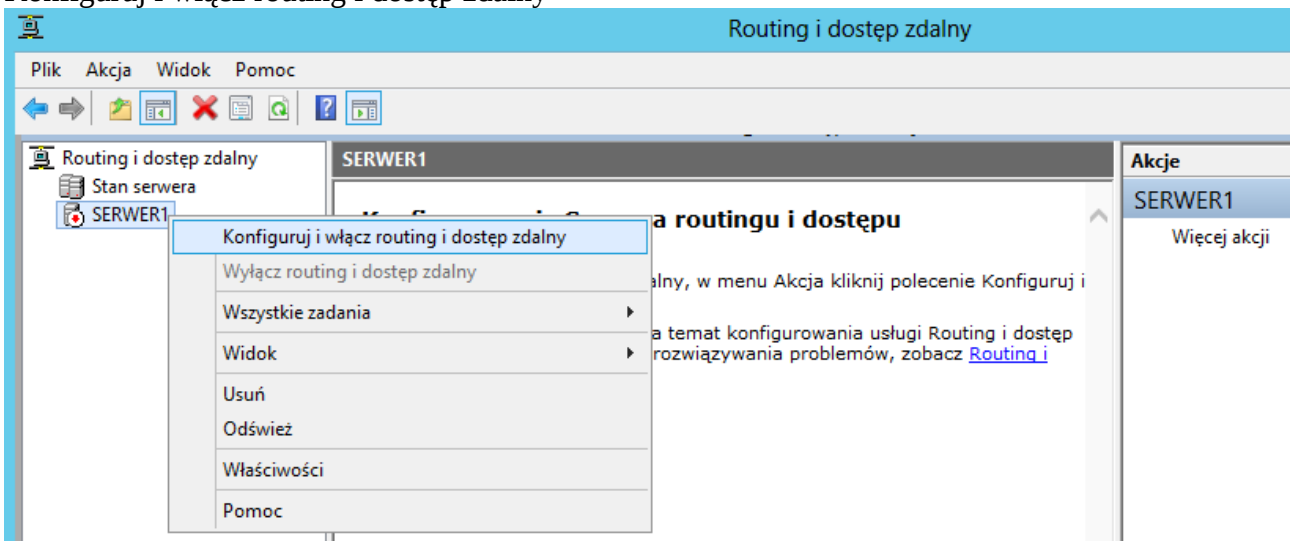
Konfiguracja i użytkowanie VPN w Windows Server 2012

1. Wybieramy przystawkę Routing i dostęp zdalny (Menedżer Serwera – zakładka Narzędzia->Routing i dostęp zdlany; konsola MMC i wybranie przystawki itp.).

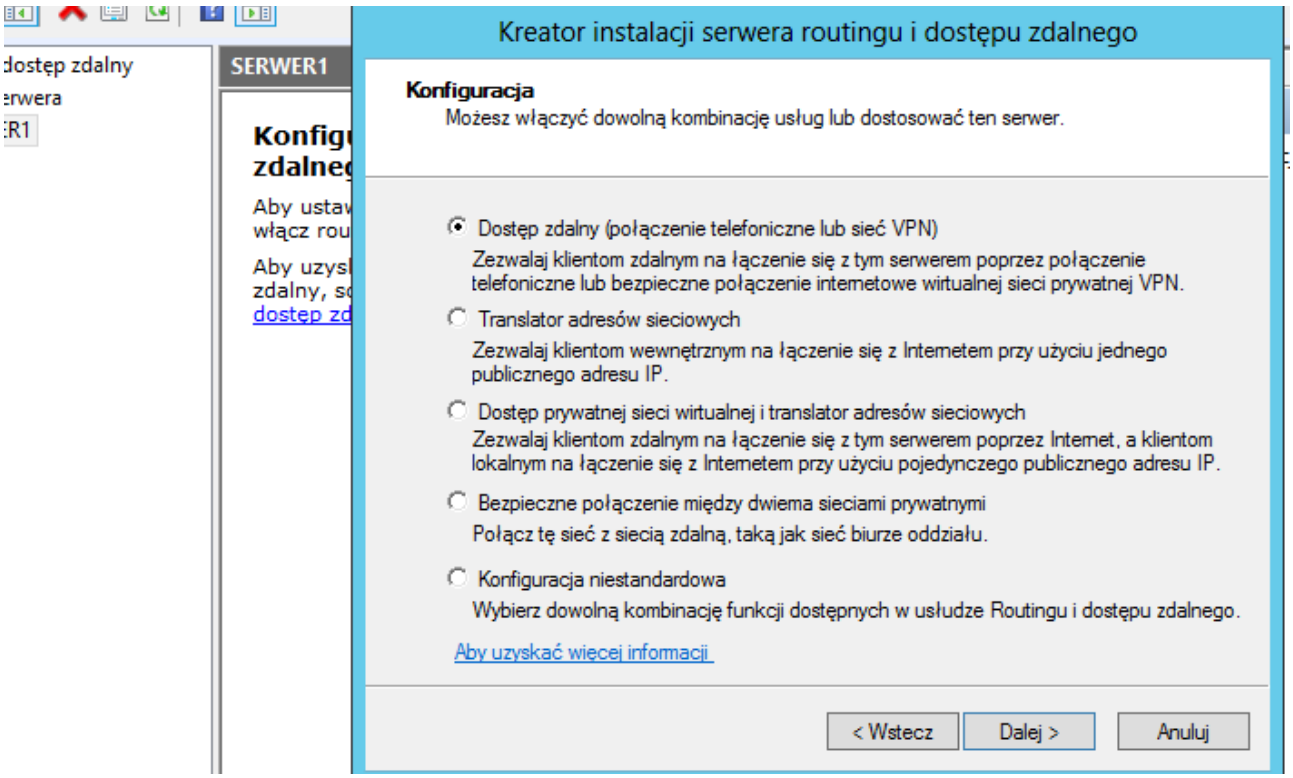
2. Prawdopodobnie narzędzie będzie proponowało nam włączenie usługi DirectAccess. Należy je zignorować (bo nie mamy ustawionej sieci IPv6).



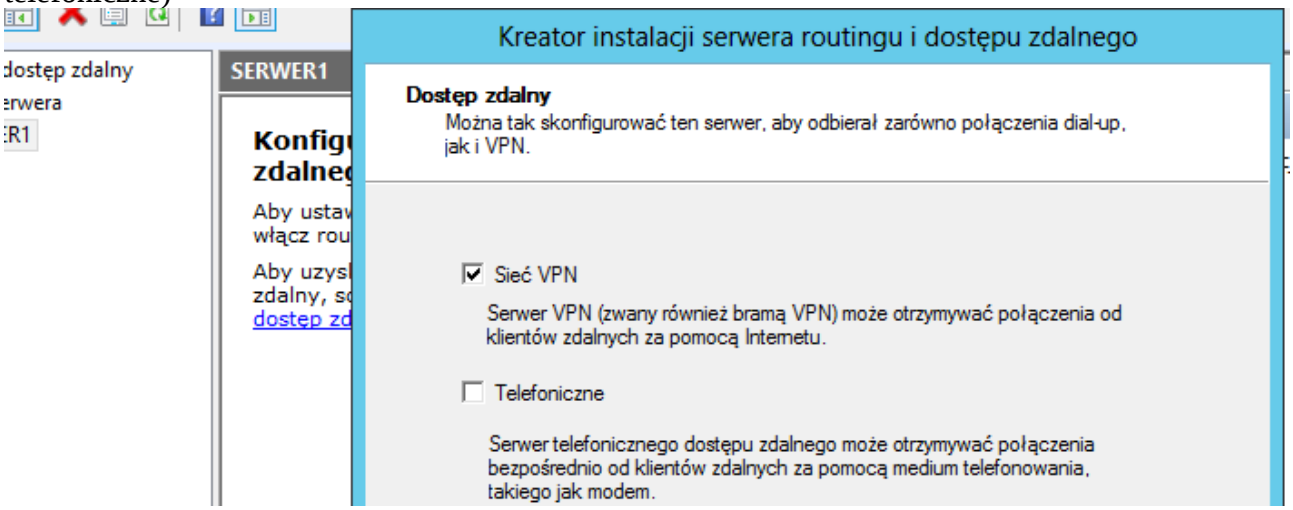
3. Następnie klikamy na nazwie naszego serwera prawym przyciskiem myszy i wybieramy Konfiguruj i włącz routing i dostęp zdalny



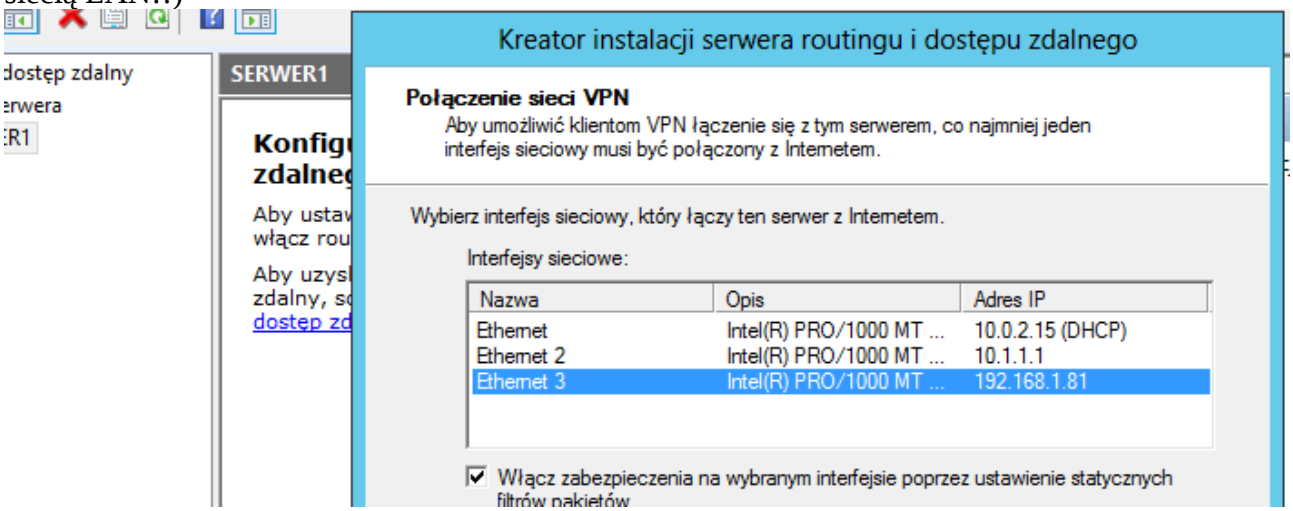
4. W oknie wyboru konfiguracji roli serwera wybieramy opcję Dostęp zdalny (połączenie telefoniczne lub sieć VPN)



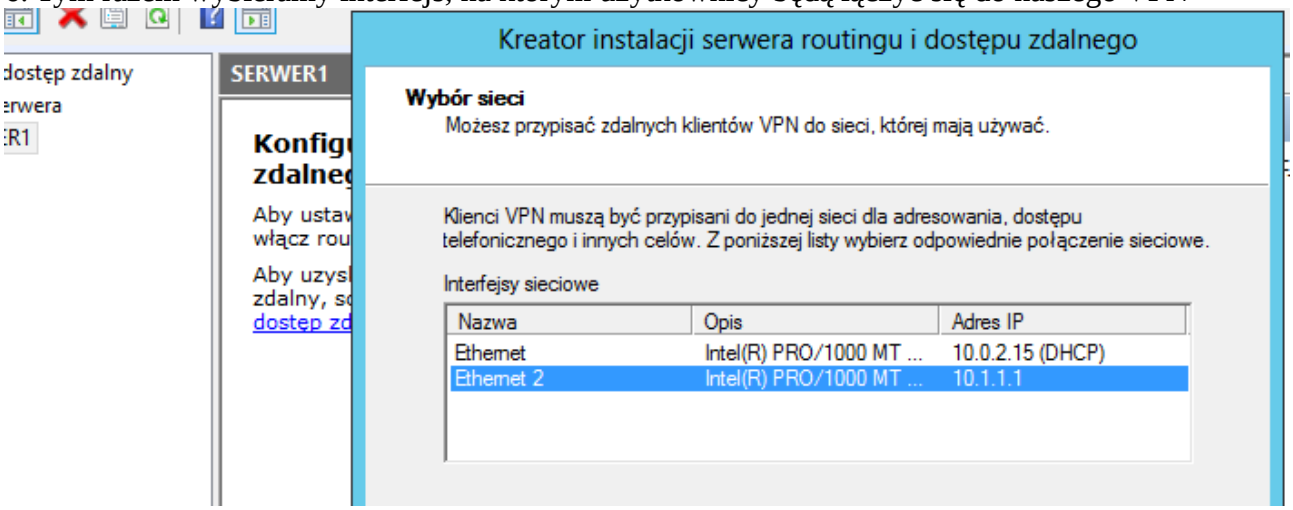
4. W następnej odsłonie okna wybieramy Sieć VPN (bo ją chcemy skonfigurować – nie połączenie telefoniczne)



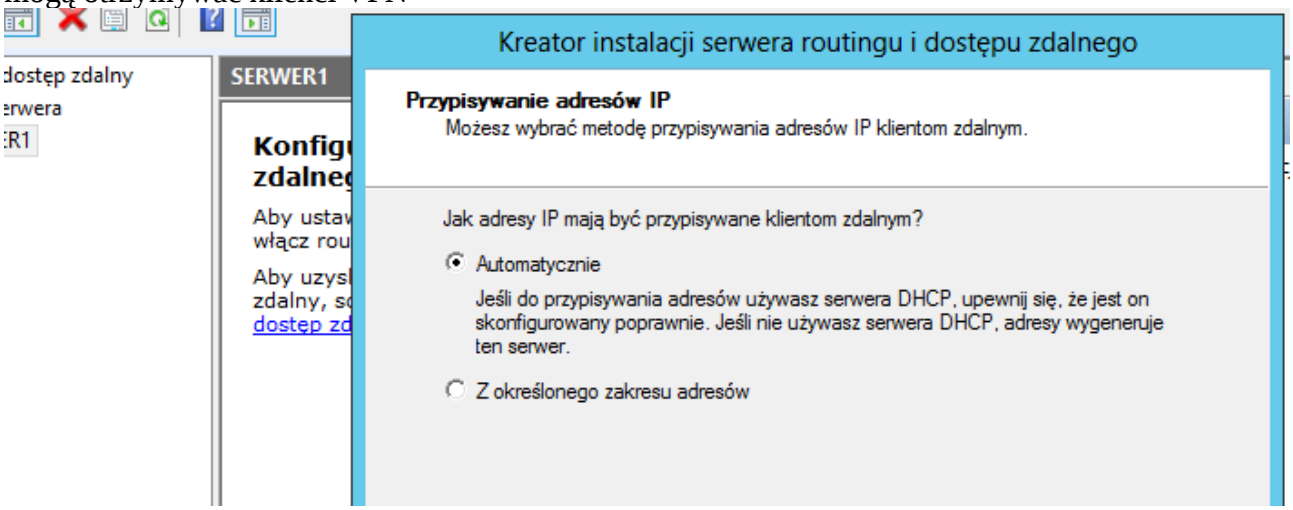
5. W następnym etapie wybieramy kartę sieciową, która łączy nasz serwer z INTERNETEM (nie siecią LAN!!)



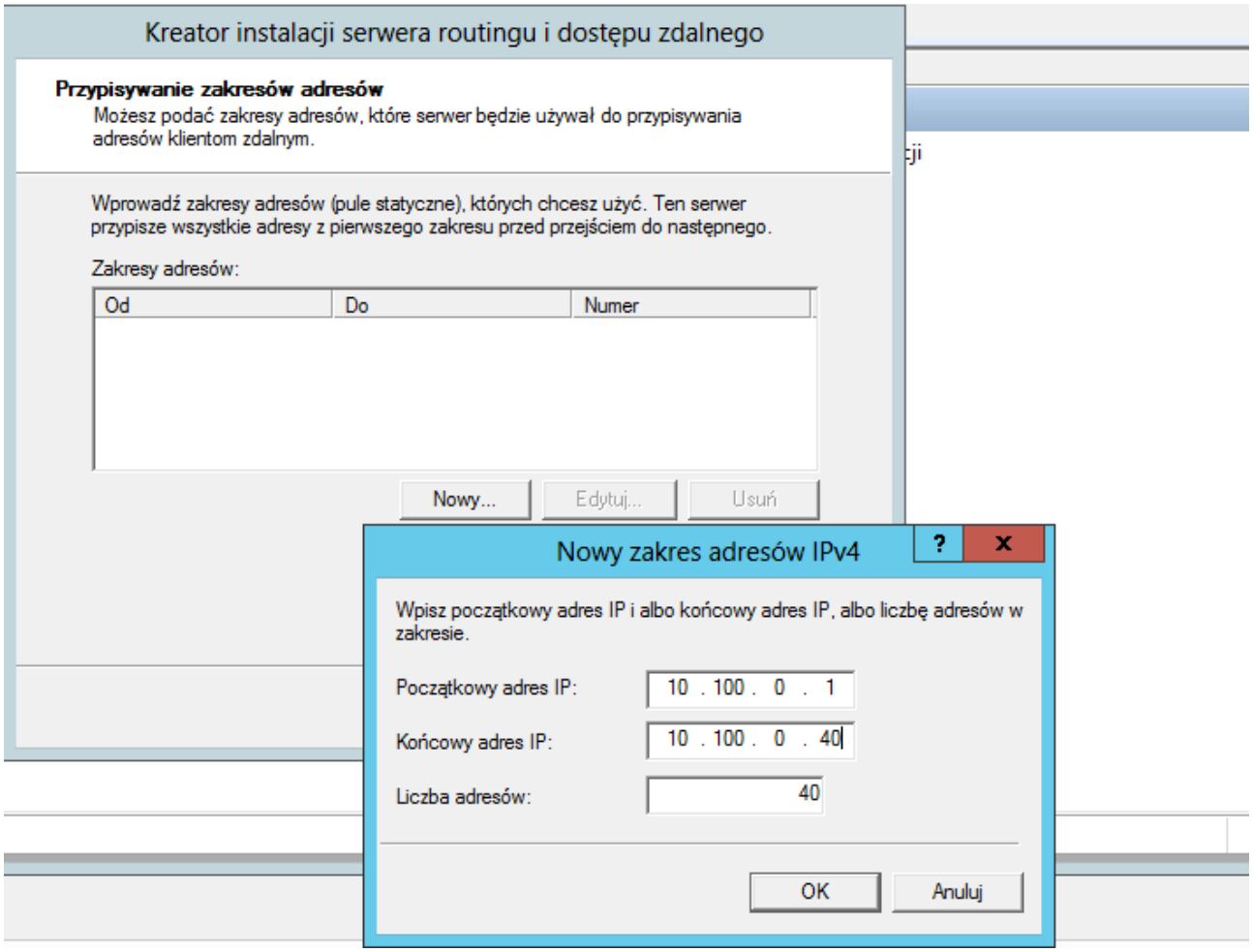
6. Tym razem wybieramy interfejs, na którym użytkownicy będą łączyć się do naszego VPN



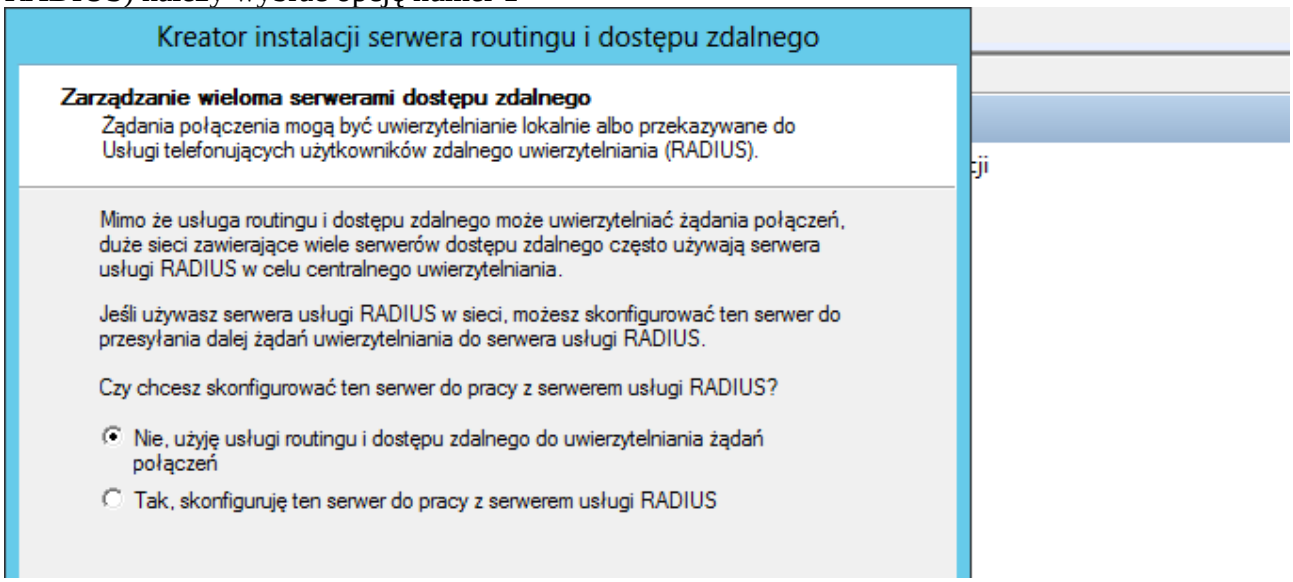
7. Teraz trzeba wybrać opcję, w jaki sposób mają być przydzielane adresy IP podłączanym klientom VPN. Jeżeli mamy skonfigurowany serwer DHCP (np. przy poprzednich ćwiczeniach) to można wybrać pierwszą opcję. W przeciwnym wypadku należy ustawić określony zakres adresów, jakie mogą otrzymywać klienci VPN



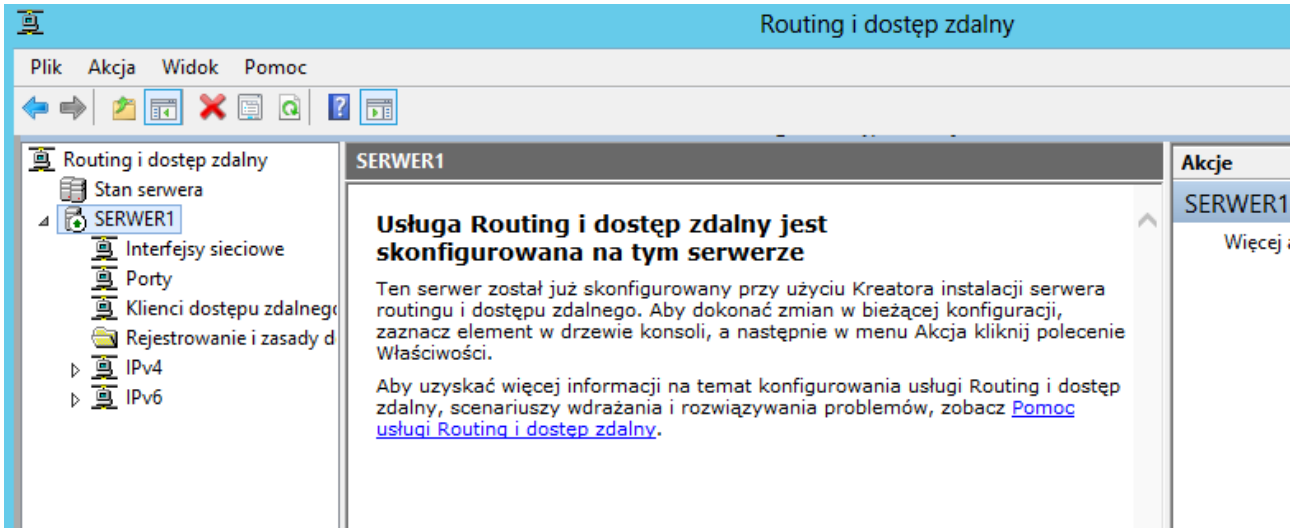
8. Jeżeli nie użyjemy DHCP, to musimy adresy IP wpisywać ręcznie (określać poszczególne pule)



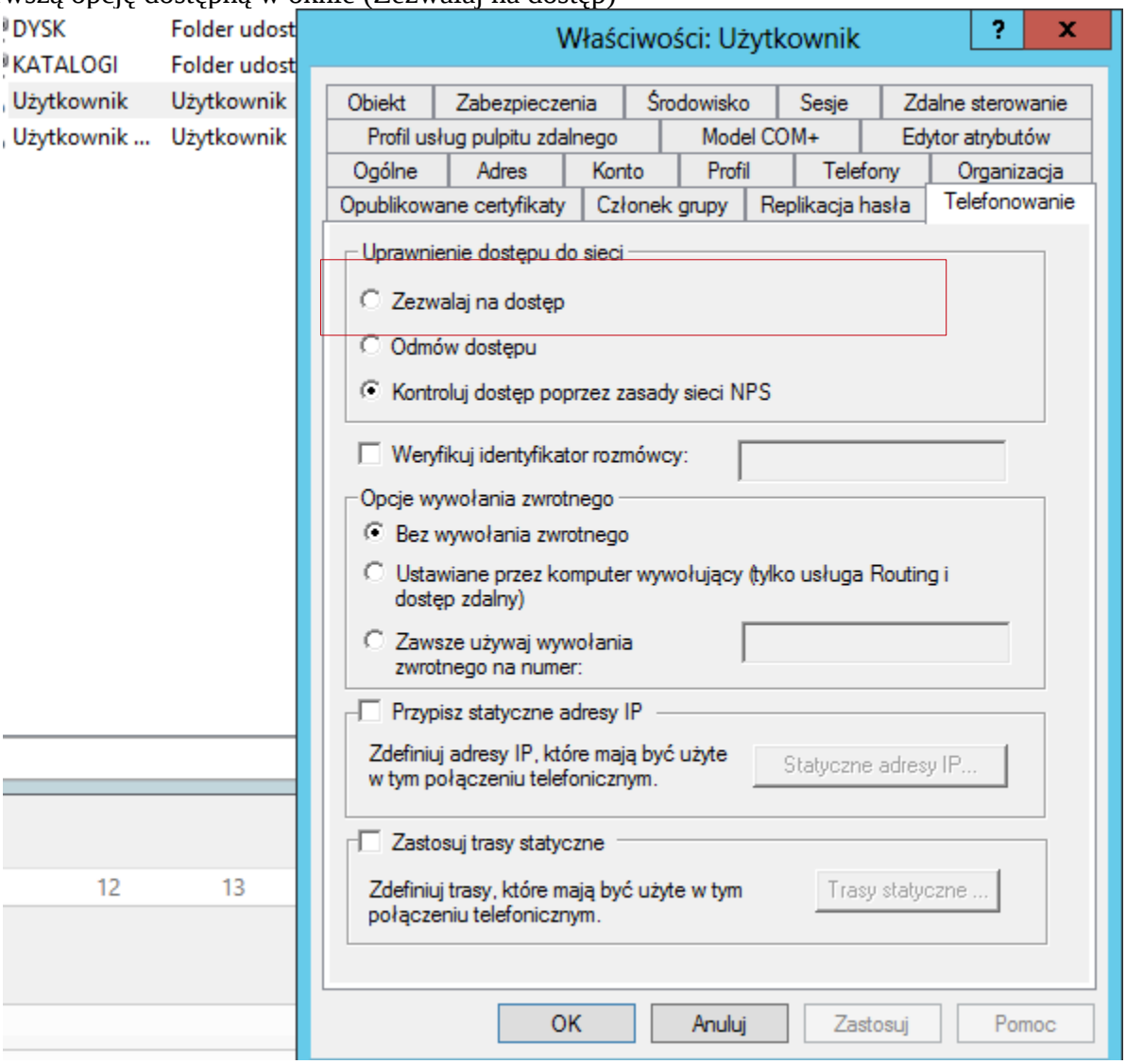
9. Jednym z końcowych ustawień jest określenie w jaki sposób klienci mają być autoryzowani do naszej sieci. Ponieważ nie konfigurowaliśmy serwera RADIUS (wymaga osobnego serwera z rolą RADIUS) należy wybrać opcję numer 1



10. Kończymy konfigurację poprzez potwierdzenie. Serwer jest już wstępnie przygotowany do nawiązywania połączeń.



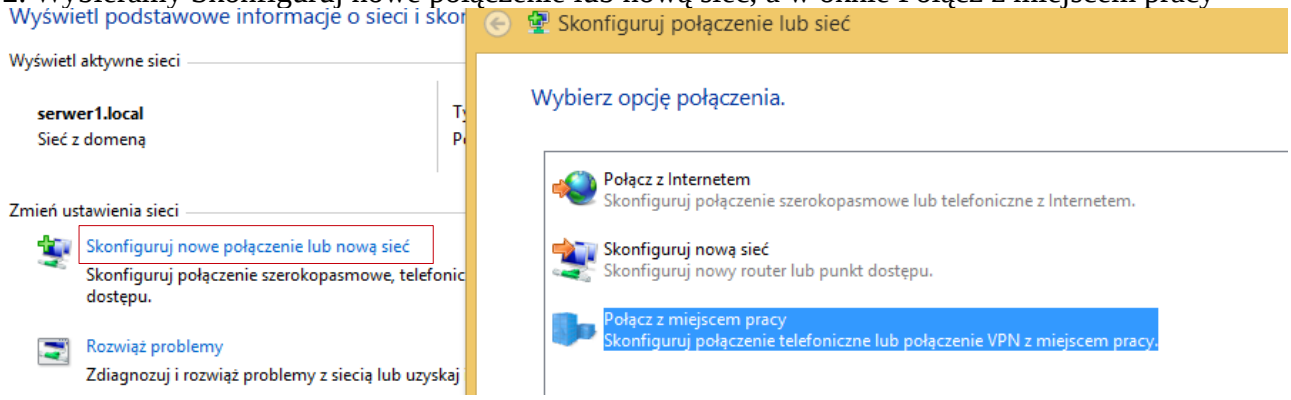
11. Teraz czas dodać użytkownikom uprawnienia do logowania się przez sieć VPN. Otwieramy narzędzie Użytkownicy i komputery usługi Active Directory.
12. Wybieramy użytkownika, któremu chcemy zezwolić na łączenie się do sieci VPN. Przechodzimy na zakładkę Telefonowanie (Remote access w wersji angielskiej). Zaznaczany pierwszą opcję dostępną w oknie (Zezwalaj na dostęp)



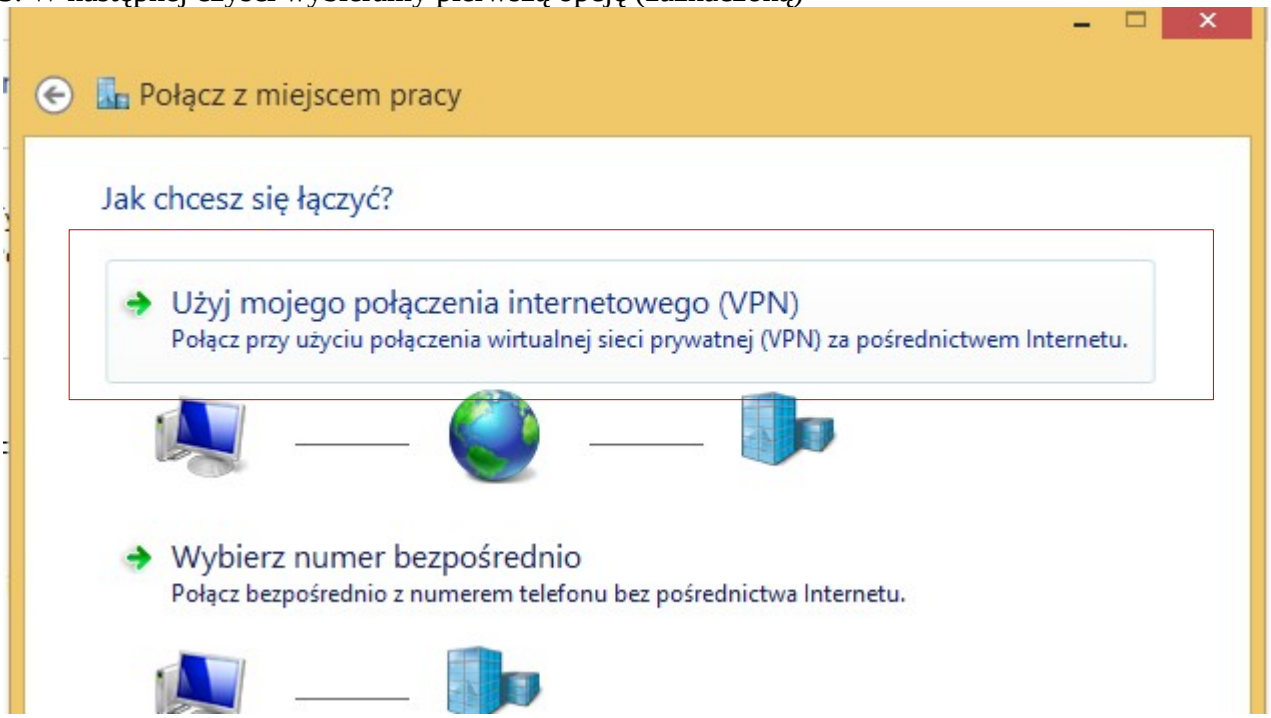
UWAGA! Gdybyśmy mieli zainstalowaną rolę Network Policy and Access Services to moglibyśmy korzystać z aktualnie wybranej opcji (NPS). Dzięki niej możemy znacznie lepiej kontrolować kogo chcemy dopuścić do sieci, kogo skierować do sieci tymczasowej (ograniczonej) itd.

KONFIGURACJA KLIENTA

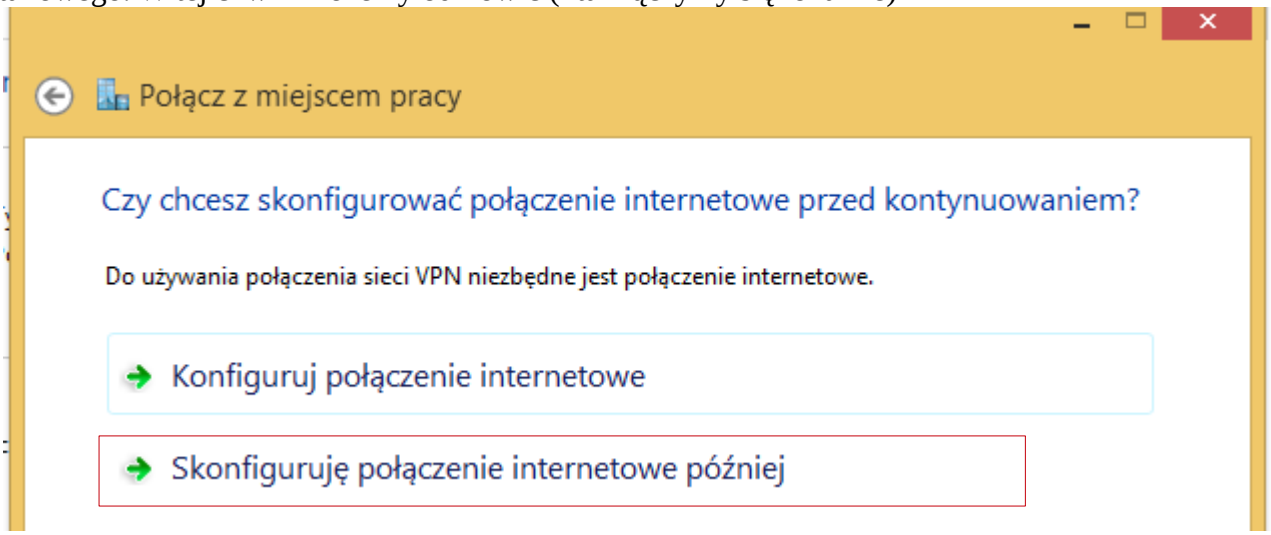
1. Otwieramy Centrum sieci i udostępniania (Windows Vista/7/8.x/10)
2. Wybieramy Skonfiguruj nowe połączenie lub nową sieć, a w oknie Połącz z miejscem pracy



3. W następnej czyści wybieramy pierwszą opcję (zaznaczoną)

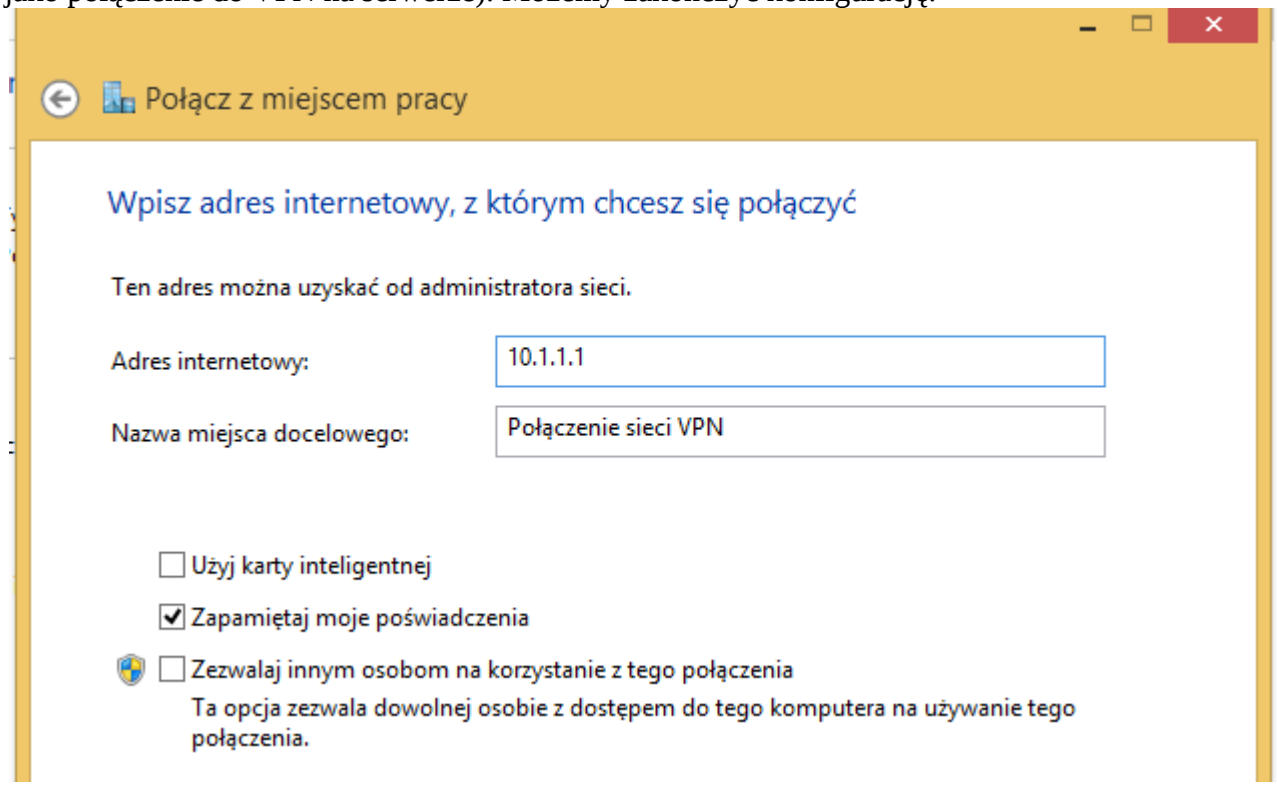


4. Jeżeli nasz system nie jest połączony z internetem to zostaniemy poproszeni o konfigurację takowego. W tej chwili możemy odmówić (i tak łączymy się lokalnie)

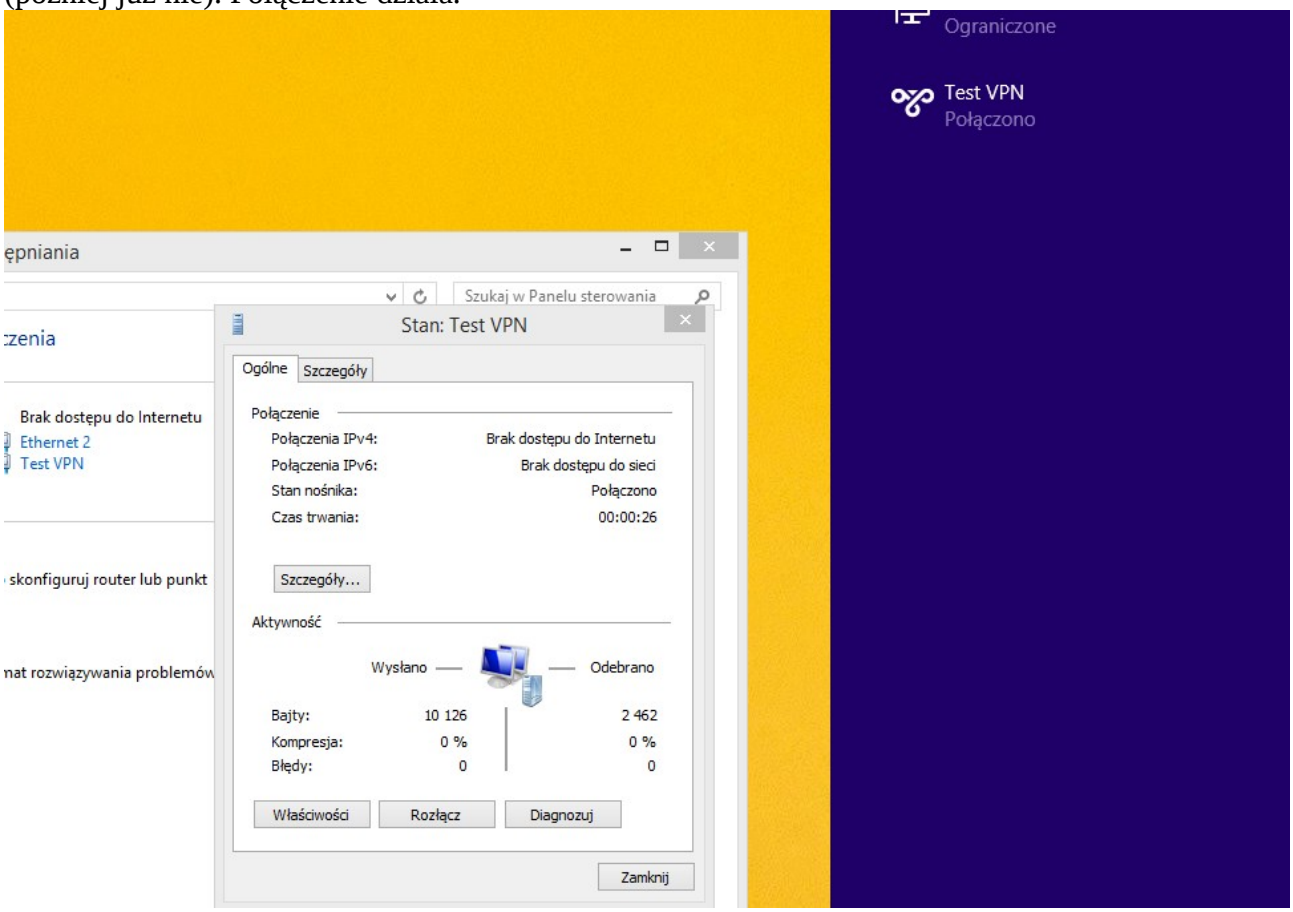


5. Na ostatnim ekranie wpisujmy adres IP serwera (adres przypisany do karty, którą wskazaliśmy

jako połączenie do VPN na serwerze). Możemy zakończyć konfigurację.

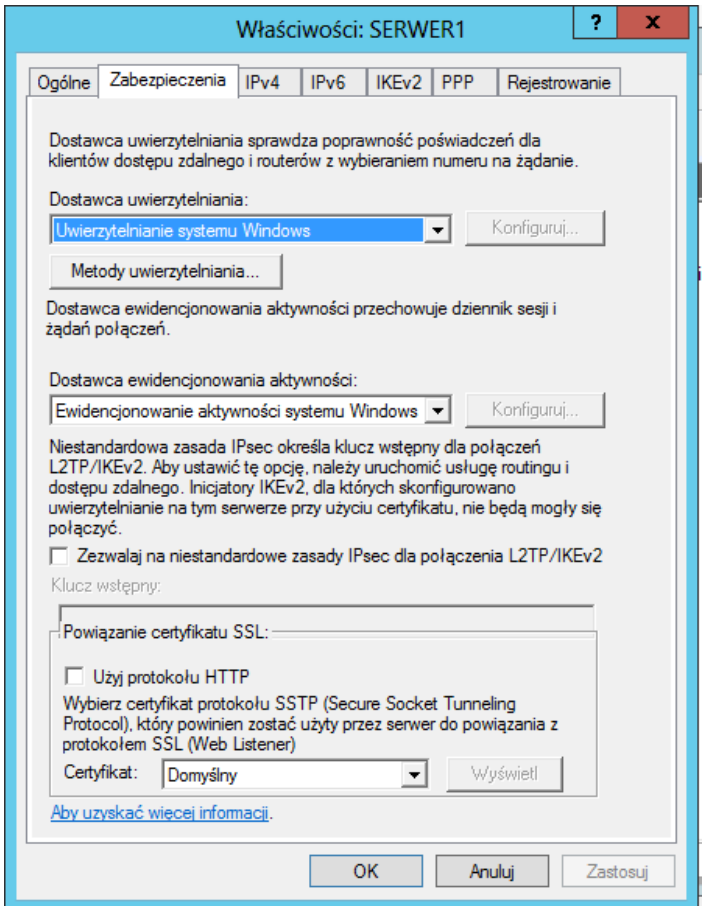


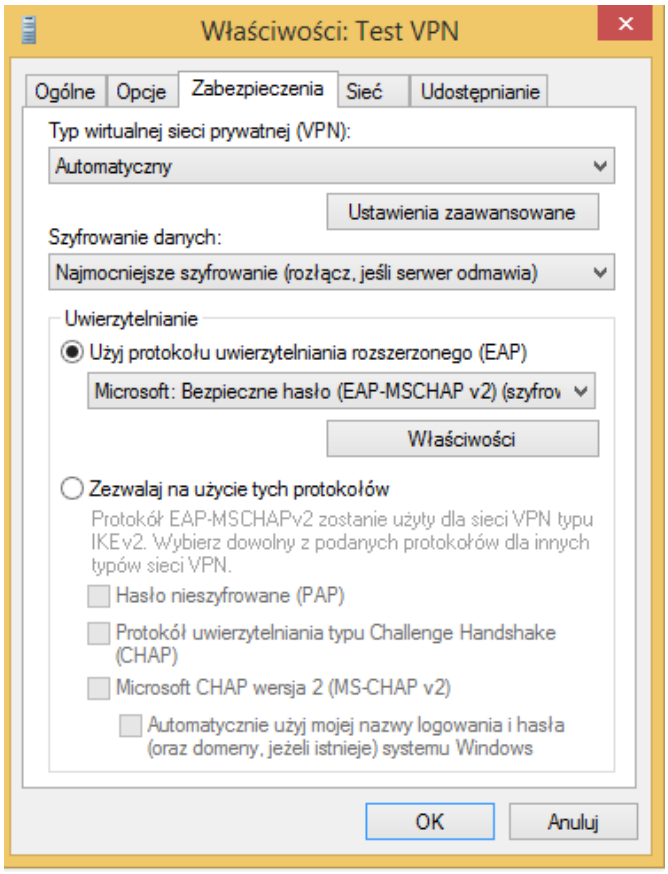
6. Teraz wystarczy się połączyć. Przy pierwszym łączeniu zostaniemy poproszeni o login/hasło (później już nie). Połączenie działa.



ZADANIA:

1. Proszę sprawdzić jak współdziałają ze sobą zmiany w zabezpieczeniach serwera/klienta, na kartach Zabezpieczenia





Podpowiedź: na Windows Server należy wybrać Właściwości serwera w Routing i dostęp zdalny, w Windows 8.x, w Centrum sieci i udostępniania, należy wybrać Zmień ustawienia karty sieciowej, a następnie Właściwości utworzonego połączenia VPN.

2. Proszę sprawdzić czy inny użytkownik domeny/komputera lokalnego może logować się do VPN poprzez konto innego użytkownika (podając w autoryzacji jego login i hasło).

3. Proszę sprawdzić czy istnieje możliwość udostępniania połączenia internetowego w ramach połączenia VPN (Windows Server ma dostęp do internetu, Windows 8.x nie).