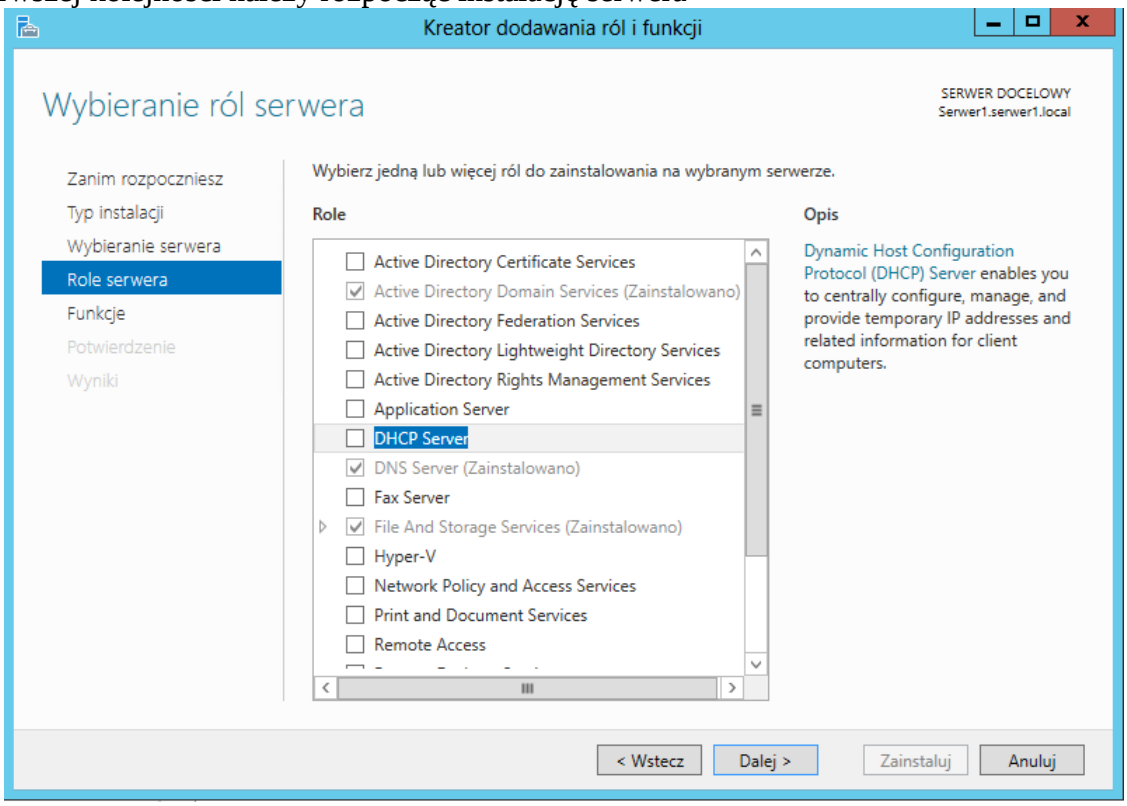
Konfiguracja serwera DHCP

W małych sieciach, w których zachodzi potrzeba posiadania serwera (wymiana plików, autoryzacja domenowa itp.) można zrezygnować z zakupu dodatkowego urządzenia rozdzielającego adresy sieciowe. Innym powodem nadania takiej roli systemowi serwerowemu może być chęć większej kontroli nad dzierżawą adresów IP, możliwością zarezerwowania dowolnych z nich na własne cele czy też zbudowanie złożonej sieci, w której będą występować zróżnicowane klasy IP, podsieci różniej długości/różnego przeznaczenia (sprzęt potrafiący w ten sposób zarządzać dynamicznym przydziałem adresów kosztuje znacznie więcej niż jego popularny, chiński odpowiednik).

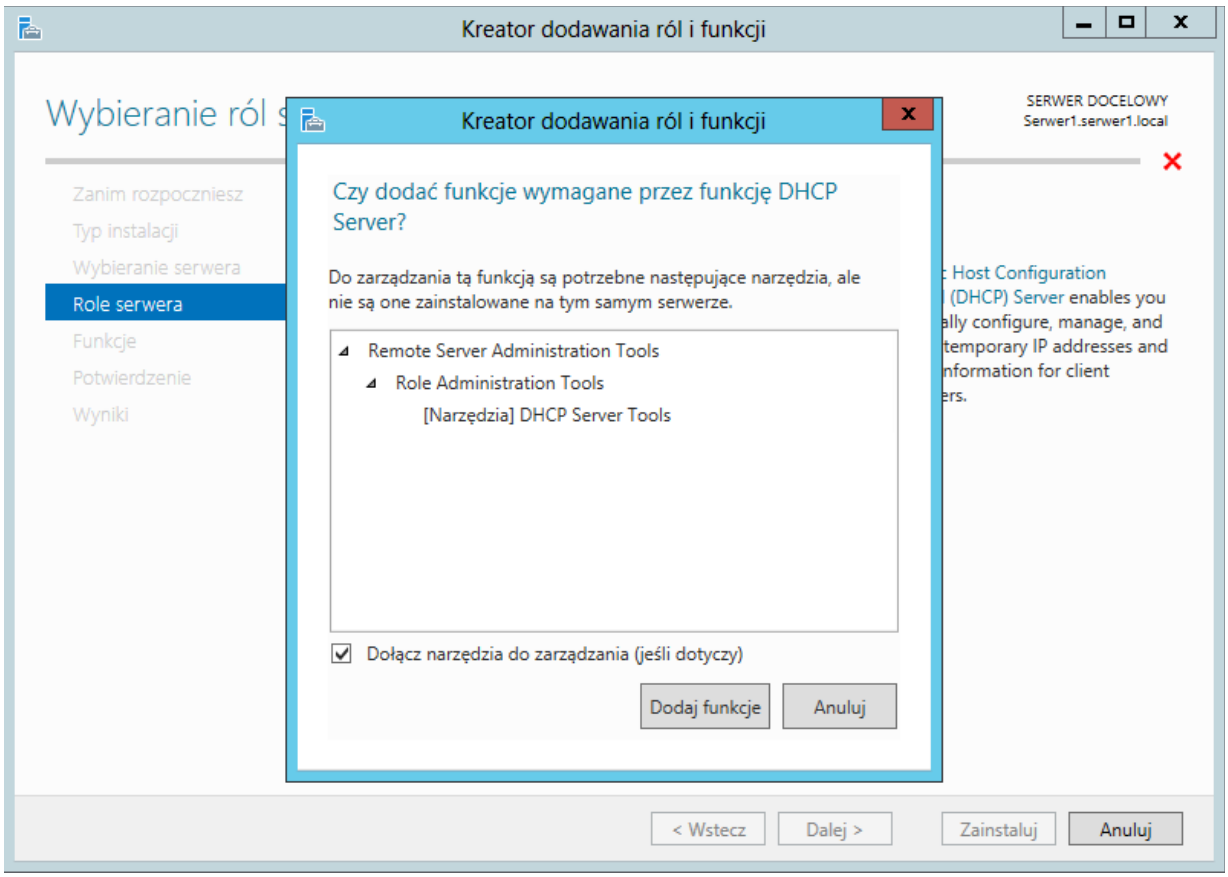
Windows 2012, tak jak zresztą jak i poprzednie wersje edycji serwerowych, również pozwala na utworzenie roli serwera DHCP. Wraz z instalacją tejże funkcji otrzymujemy odpowiednie narzędzie o nazwie DHCP, pozwalające na tworzenie oraz zarządzanie adresami IPv4 oraz IPv6 (w przypadku tworzenia prywatnych podsieci dla tego drugiego). Wydawać by się mogło, że uruchamianie serwera DHCP dla IPv6 jest zajęciem na siłę (protokół potrafi się sam konfigurować, a nadany w ten sposób adres jest stale przypisany do danego urządzenia), lecz może ono być przydane w specjalistycznych zadaniach gdyż pozwala nadać np. drugi adres, prywatny, do działań w intranecie).

Sama instalacja i konfiguracja serwera nie jest specjalnie trudna i nie wykracza poziomem ponad np. konfigurowanie AD. Dodatkowo nadamy później naszemu serwerowi rolę tłumaczenia adresów sieciowych (NAT) dzięki czemu komputery podłączane do naszej sieci będą mogły korzystać z sieci szerokopasmowej.

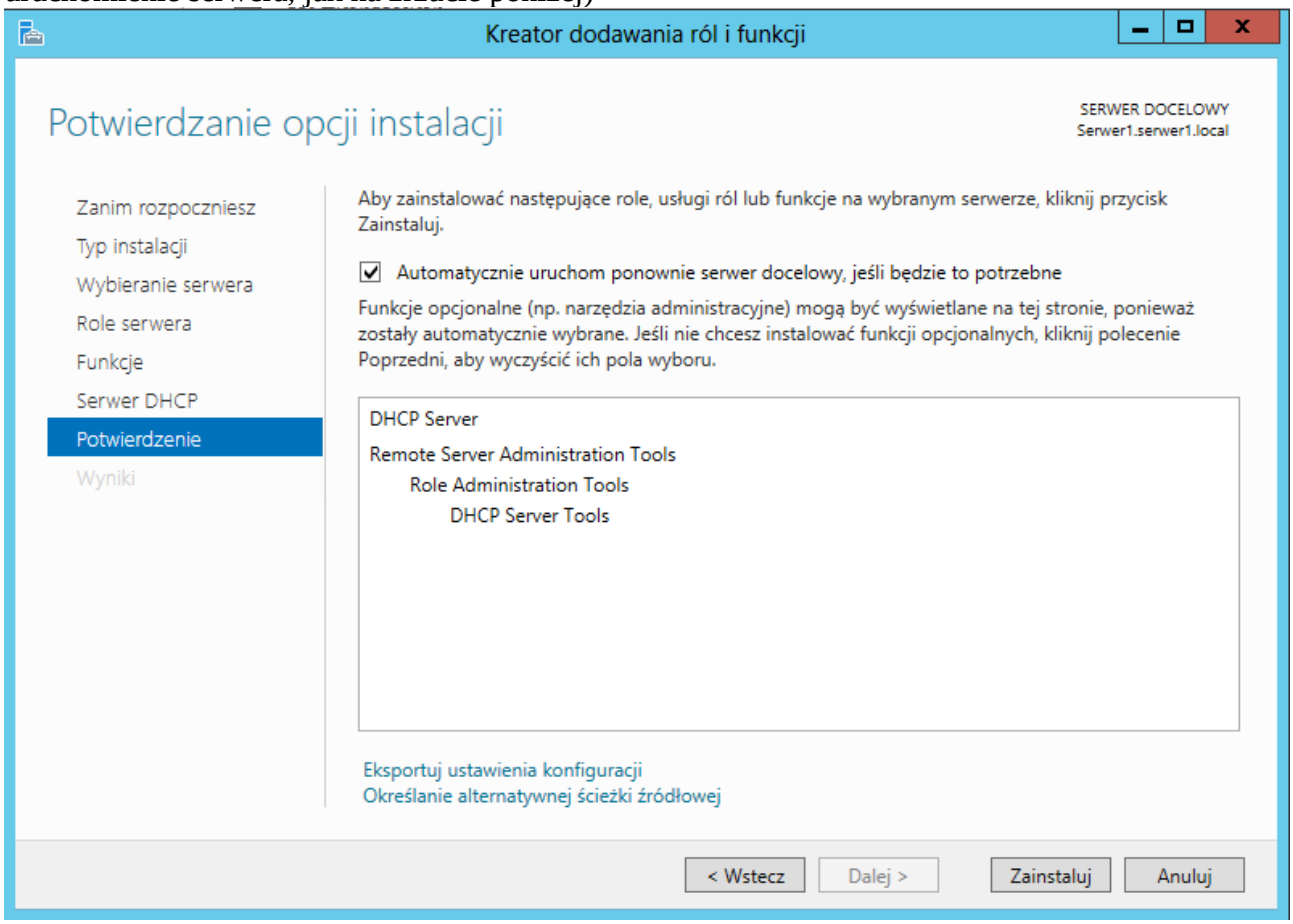
W pierwszej kolejności należy rozpocząć instalację serwera



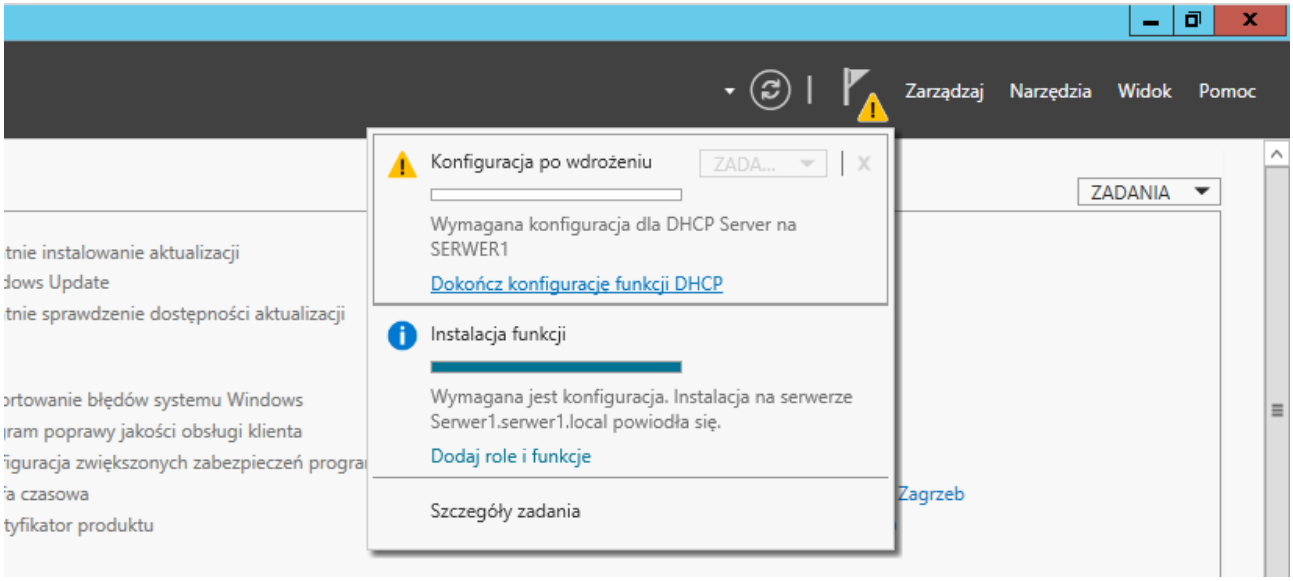
Wraz z nim będą chciały dodać się następujące usługi (narzędzia)



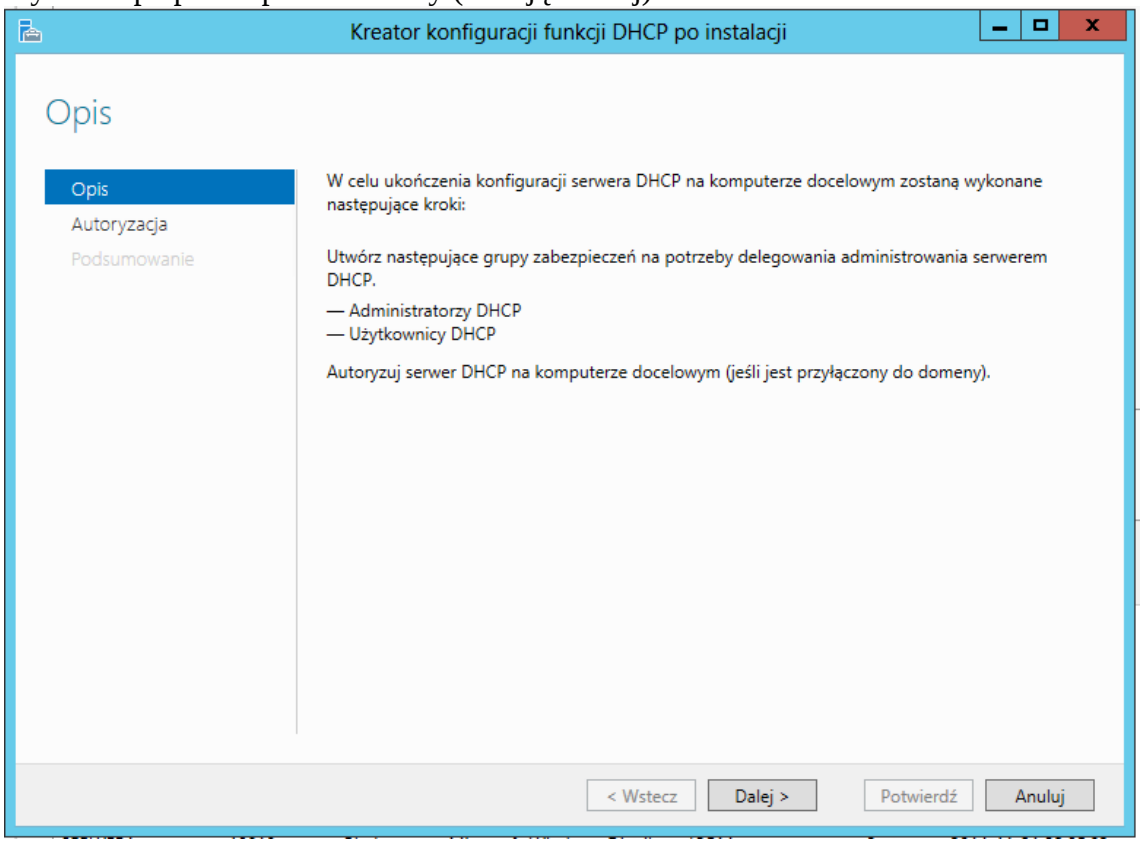
Przechodzimy do finalizacji instalacji (kilka kliknięć na Dalej, później najlepiej zaznaczyć ponowne uruchomienie serwera, jak na zrzucie poniżej)



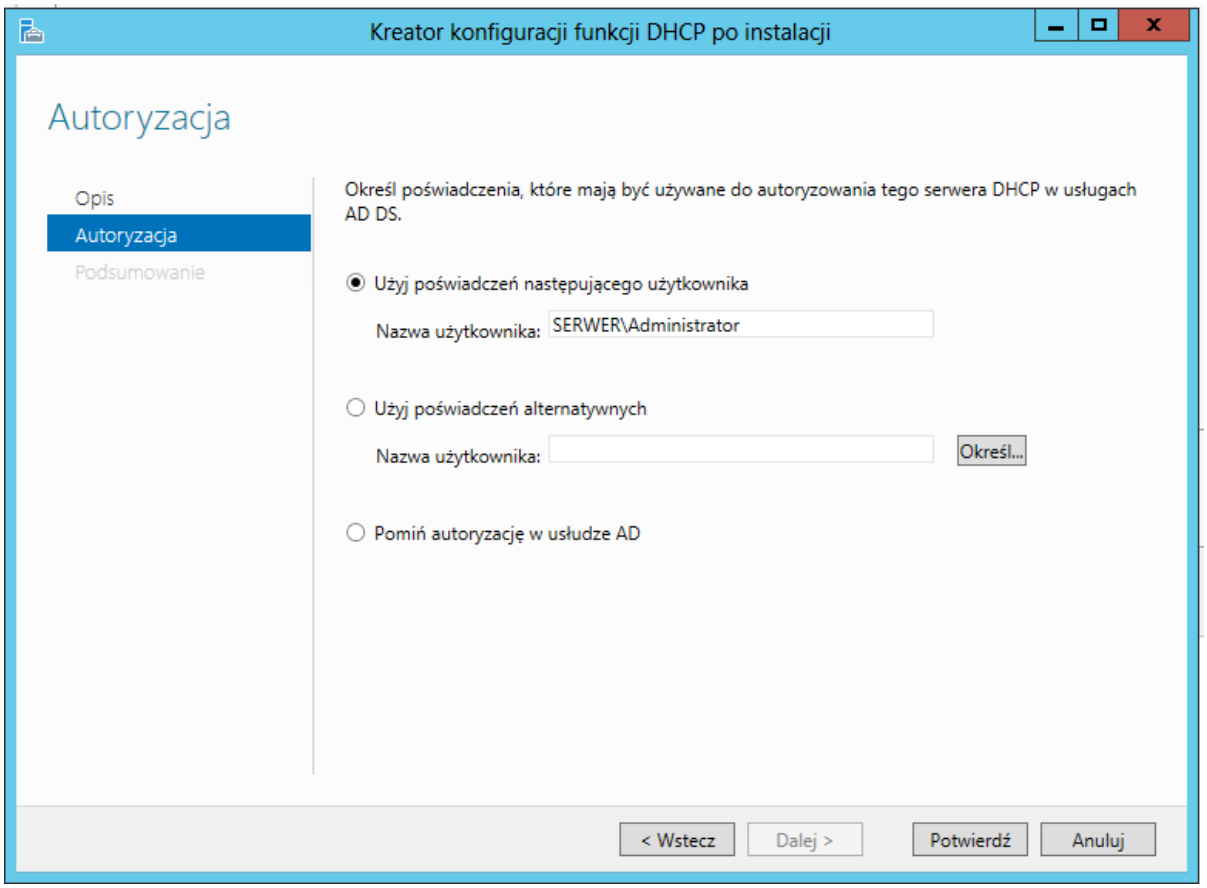
Dokańczamy konfigurację DHCP



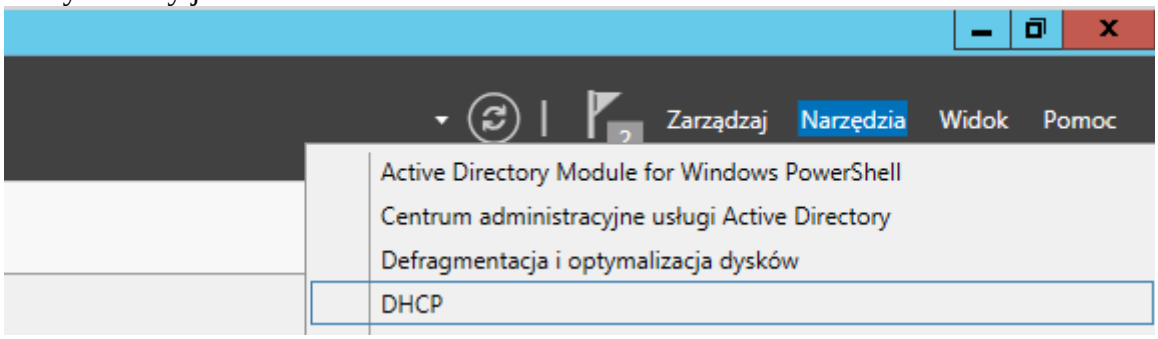
Pierwszy ekran po prostu potwierdzamy (klikając Dalej)



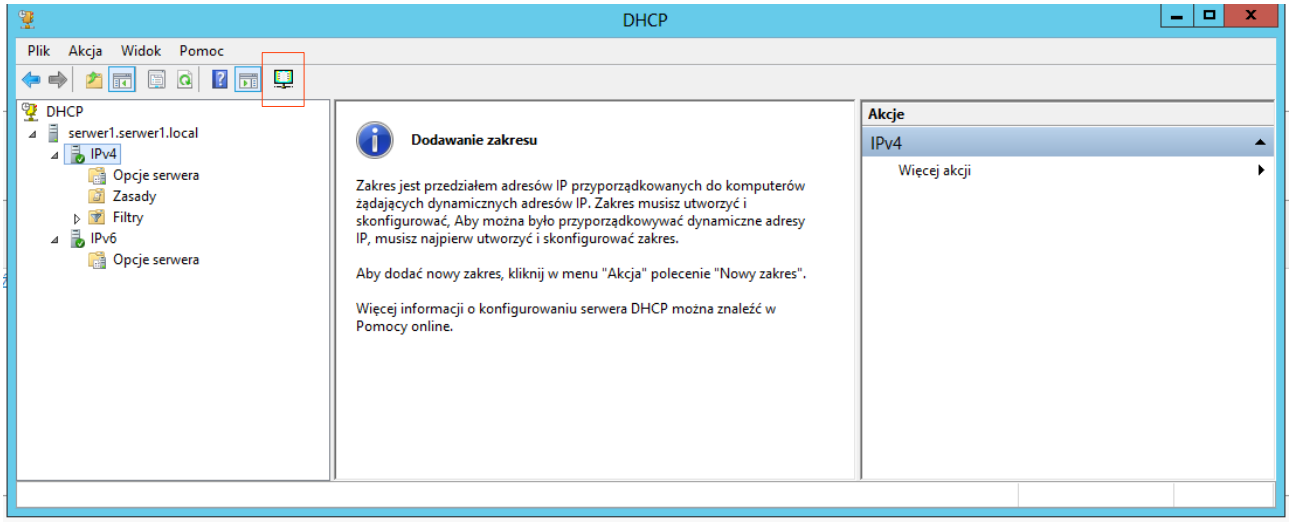
Ponieważ mamy ustawioną rolę AD, serwer DHCP będzie musiał w niej zostać autoryzowany. W tym kroku wybieramy poświadczenia użytkownika, które zostaną do tego wykorzystane (można rzecz jasna wybrać brak poświadczenia).



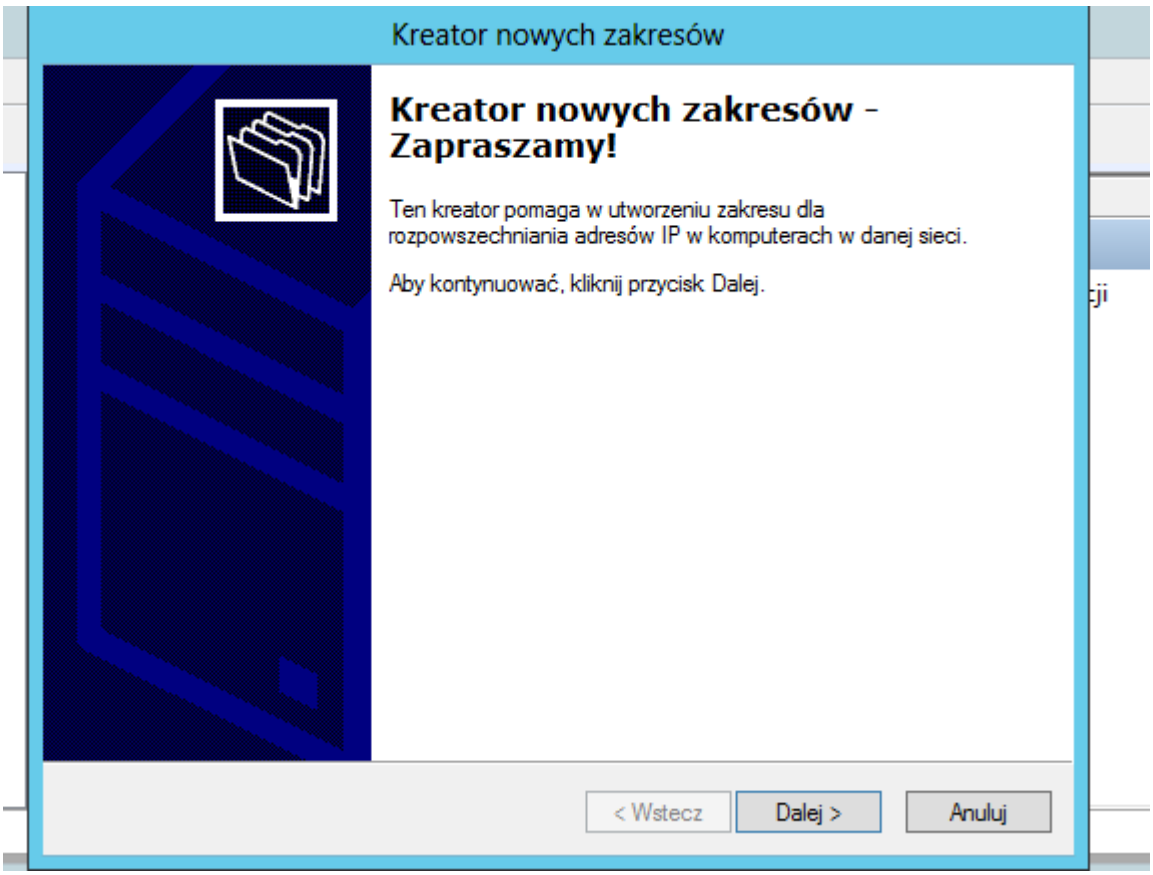
Po wszystkim klikamy zakończ. Od tego momentu mamy dostępne nowe narzędzie o nazwie DHCP. Wybieramy je.



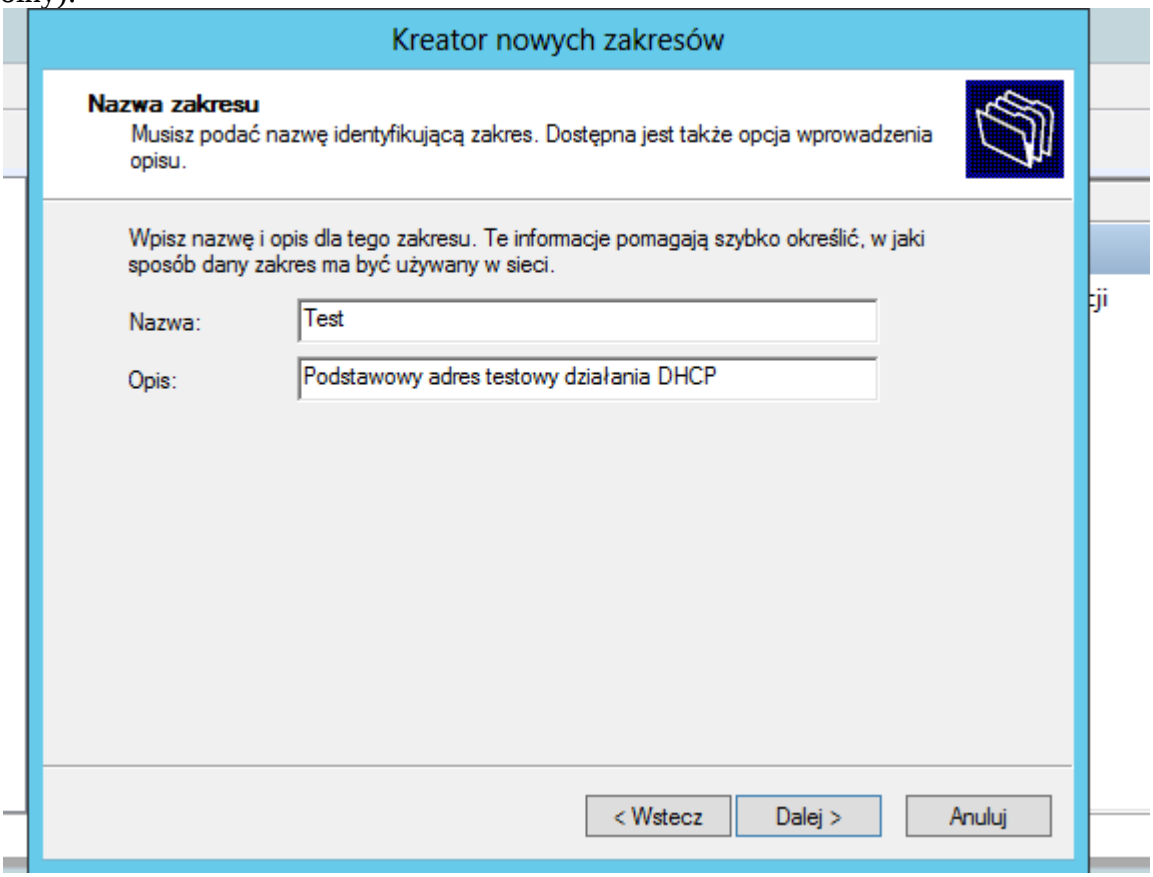
Okno narzędzia niczym nie różni się od większości innych narzędzi – opiera się na dobrze znanej konsoli MMC.



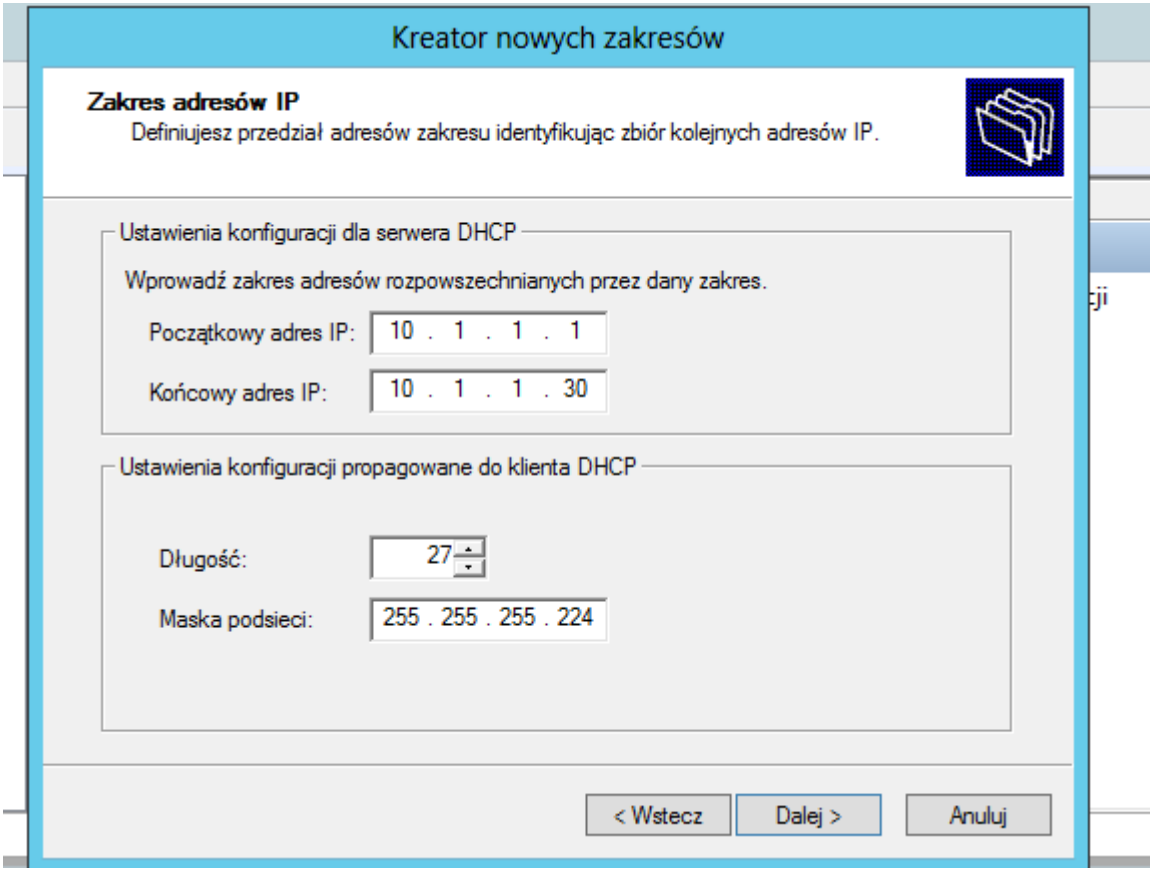
W celu utworzenia nowego zakresu adresów IP należy wybrać IPv4 i kliknąć przycisk Nowy zakres



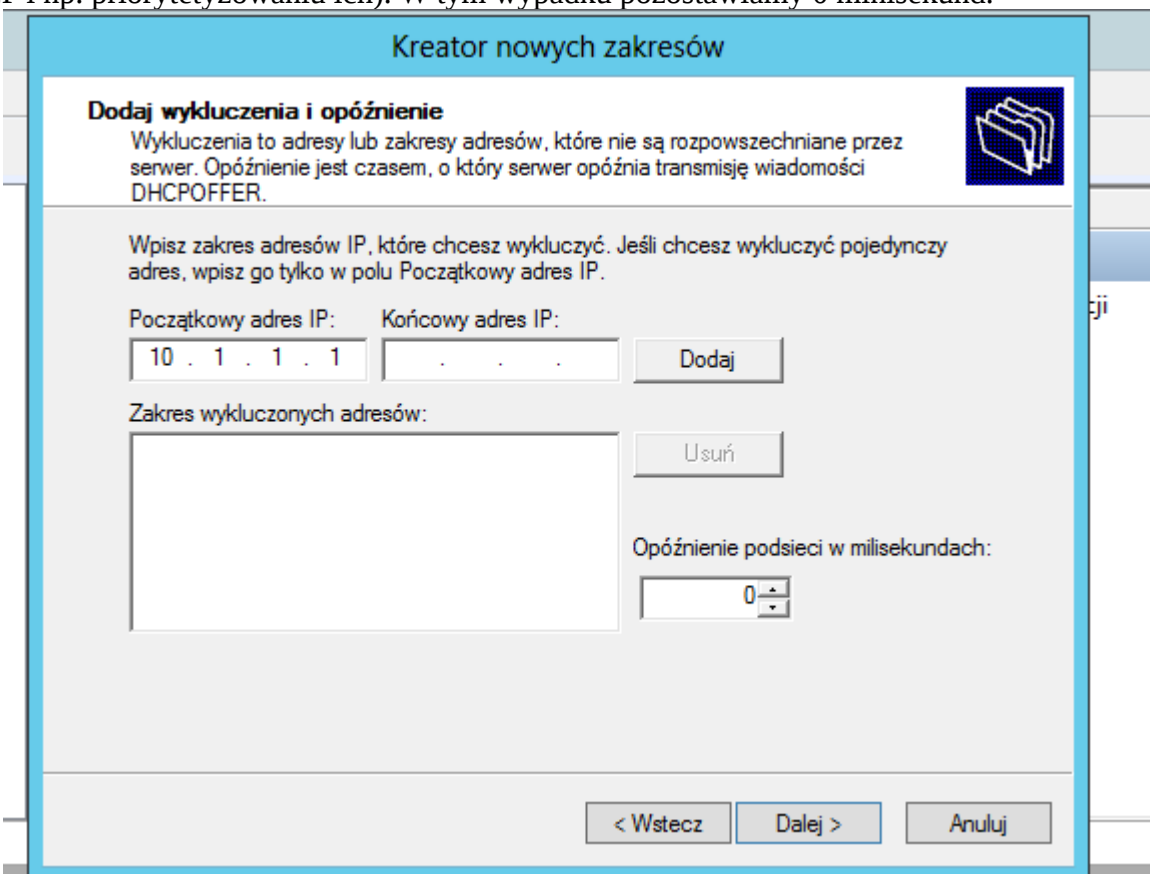
W następnym kroku trzeba dodać nazwę nowego zakresu (dowolna) oraz jego krótki opis (dowolny):



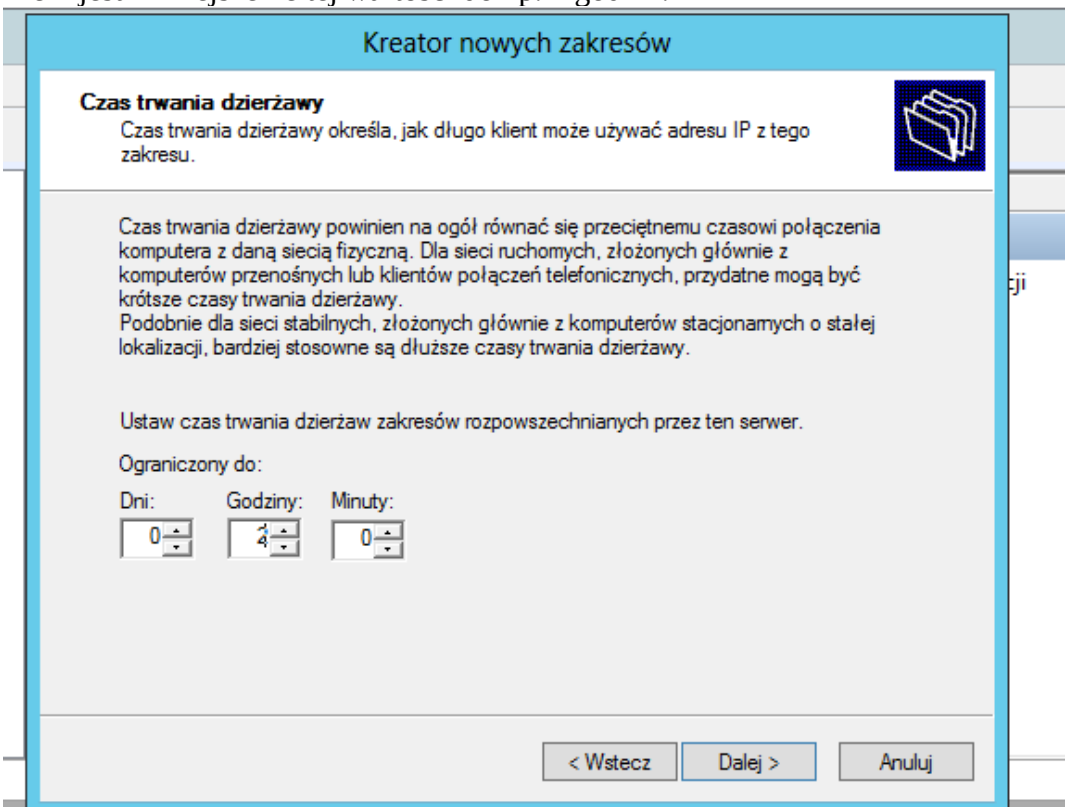
W kolejnym korku ustawiany jest zakres adresów IP. Do celów testowych utworzymy pulę 30 adresów IP (łącznie 32 adresy) 10.1.1.0/27.



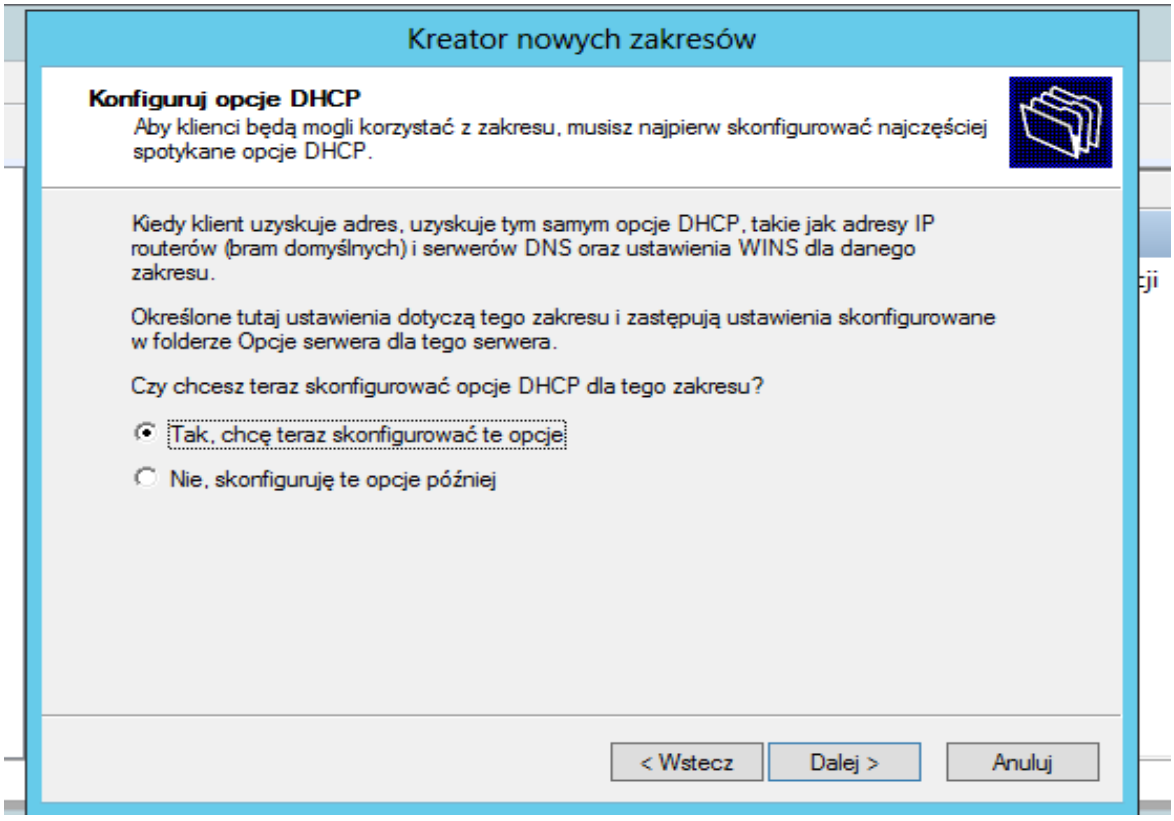
Kolejny etap to wykluczenie pojedynczego/grupy adresów IP, które mają nie być dystrybuowane przez serwer DHCP. Możemy dodać tutaj np. adres 10.1.1.1 – będzie on zarezerwowany dla naszego serwera. Ponadto można w tym kroku ustawić opóźnienie w milisekundach, o ile serwer ma opóźniać wysyłanie sygnału rozgłoszeniowego (opcja przydatka w przypadku kilku serwerów DHCP i np. priorytetyzowaniu ich). W tym wypadku pozostawiamy 0 minisekund.



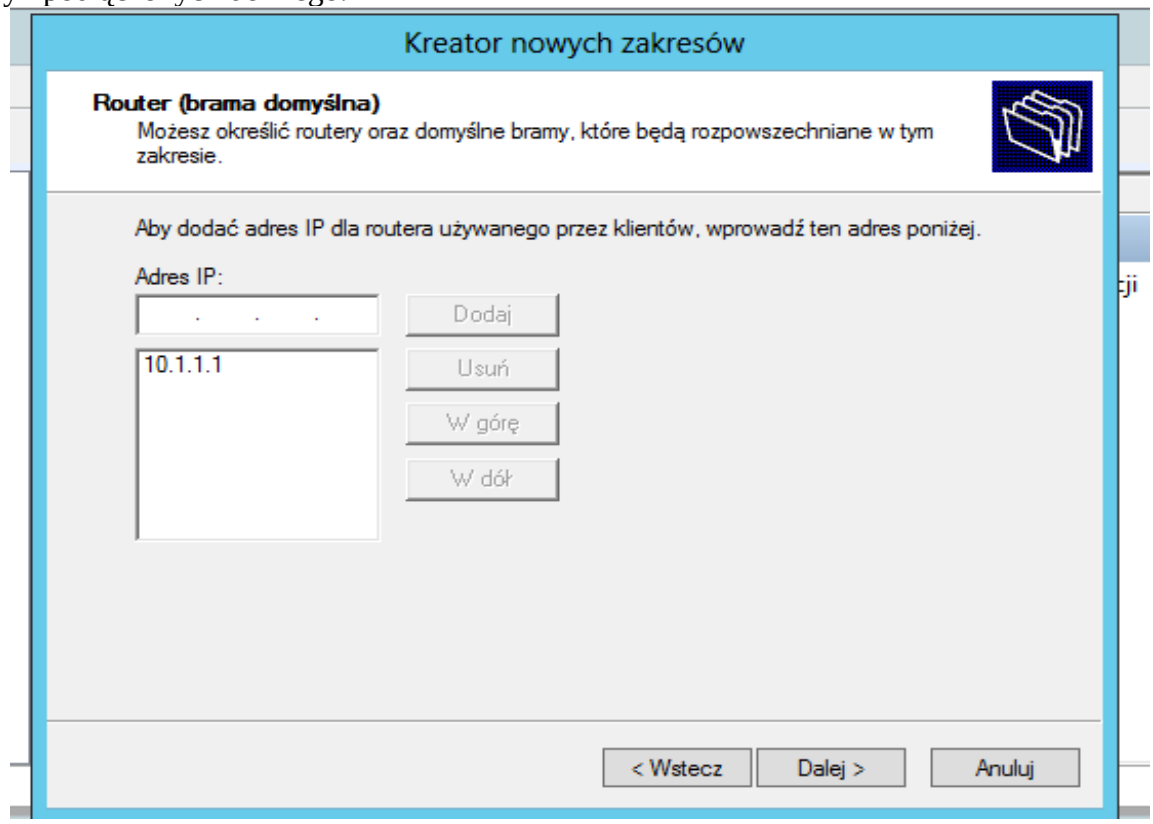
W następnym oknie podajemy domyślny czas dzierżawy adresów. Serwer proponuje 8 dni co w normalnych warunkach nie jest najlepszym rozwiązaniem – tego typu praktyki mogą prowadzić do różnego rodzaju ataków na nasz serwer (chociażby przepełnienia zakresu). O wiele lepszym rozwiązaniem jest zmniejszenie tej wartości do np. 2 godzin.



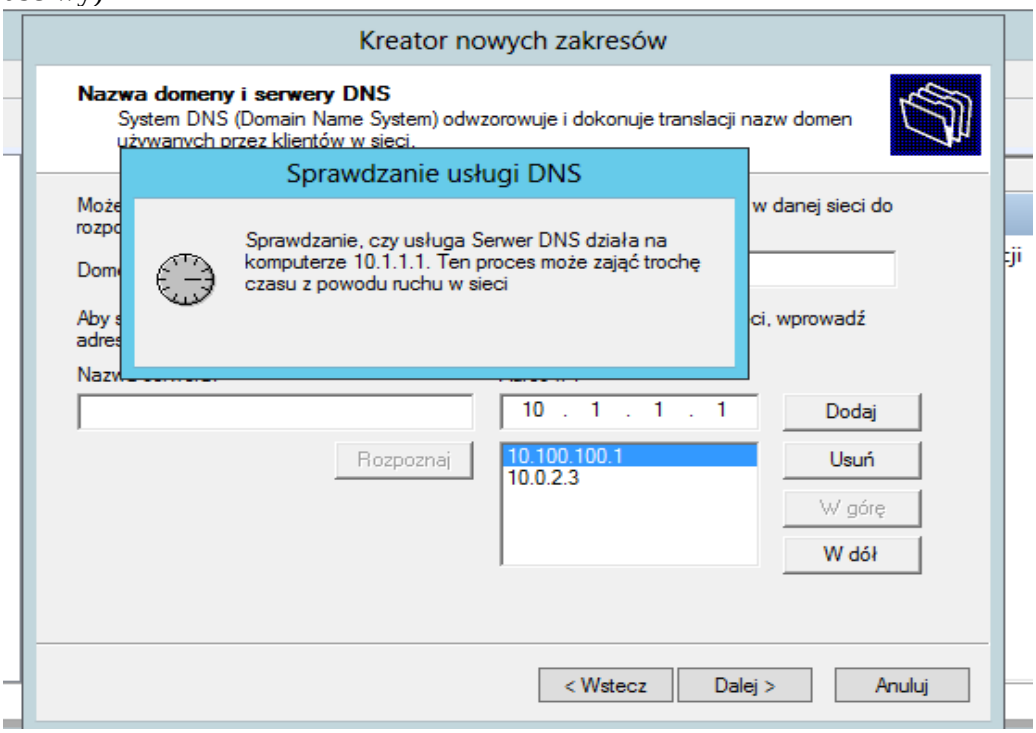
Następnie zostaniemy zapytani, czy chcemy dodatkowo konfigurować pewne opcje serwera DHCP, jak dystrybuowane adresy DNS, bramy domyślne itp. Bez nich nasz zakres może nie dawać możliwości klientom na korzystanie z dostępu do sieci Internet.



W routerach dodajemy adres naszego serwera. To on będzie bramą internetową dla wszystkich maszyn podłączonych do niego.



Kolejnym ustawieniem będą serwery DNS. Proszę zauważyć, że zostały aktualnie przyjęte adresy na interfejsach sieciowych (10.0.2.3 został wzięty z karty Ethernet, 10.100.100.1 z karty Ethernet2). Oczywiście ten drugi adres będzie zamieniany więc można wpisać nowy adres serwer 10.1.1.1. System przeprowadzi wstępną analizę serwera DNS; okaże się, że adres może nie działać prawidłowo. Wiemy co robimy więc akceptujemy (dodajemy) adres, a 10.100.100.1 kasujemy (UWAGA – adres może być dla poszczególnych osób inny; nie ma się czym przejmować tylko usunąć właściwy)

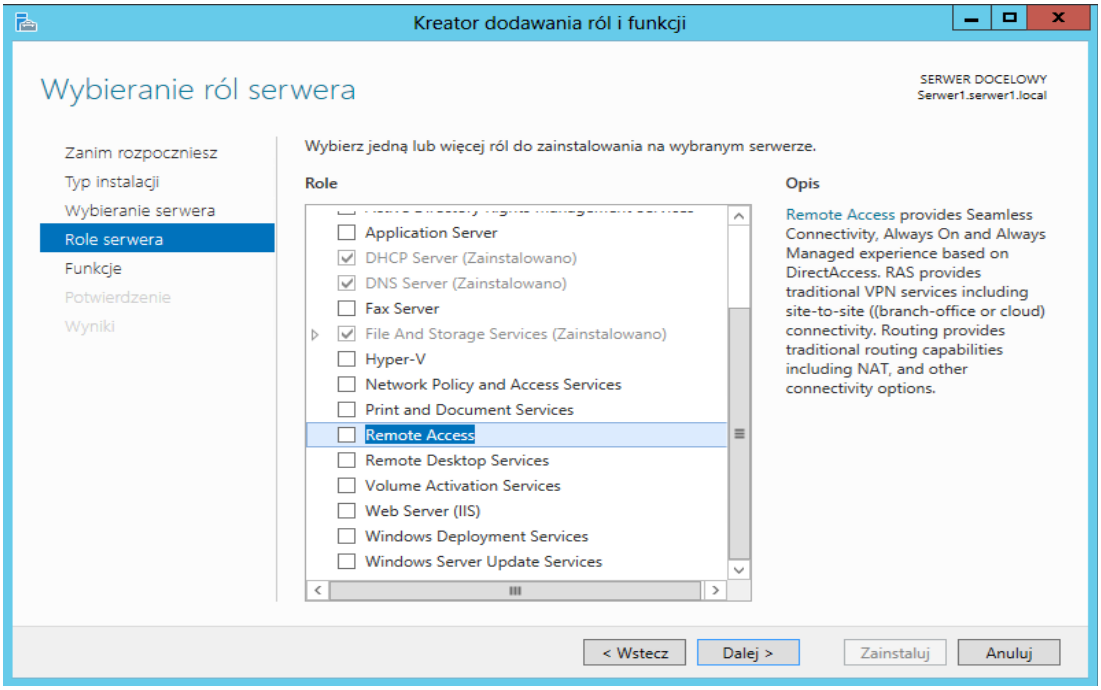


Następnie będziemy zapytani o serwery WINS. Nie są nam potrzebne, pomijamy je.

Później zostaniemy zapytani, czy uaktywnić tworzony zakres. Odpowiadamy twierdząco. Kończymy pracę kreatora.

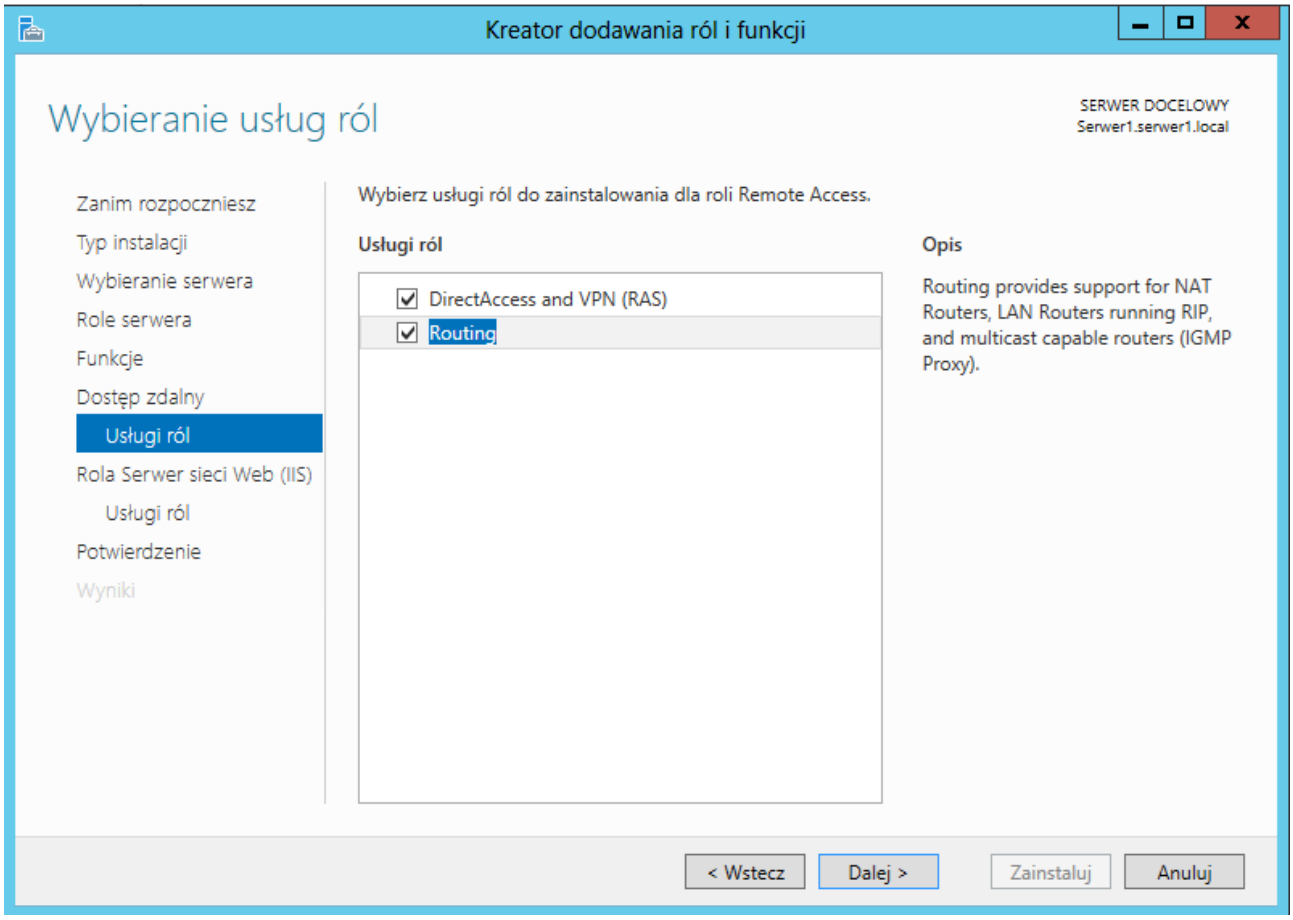
Od tego momentu komputery, które będą podłączały się do sieci, w której działa nasz serwer, mogą otrzymywać adres właśnie od niego.

Czas na utworzenie serwera NAT z prawdziwego zdarzenia. Po pierwsze trzeba wyłączyć udostępnianie połączenia internetowego jakie było utworzone w materiale 5. Następnie trzeba dodać nową rolę serwera – Remote Access.

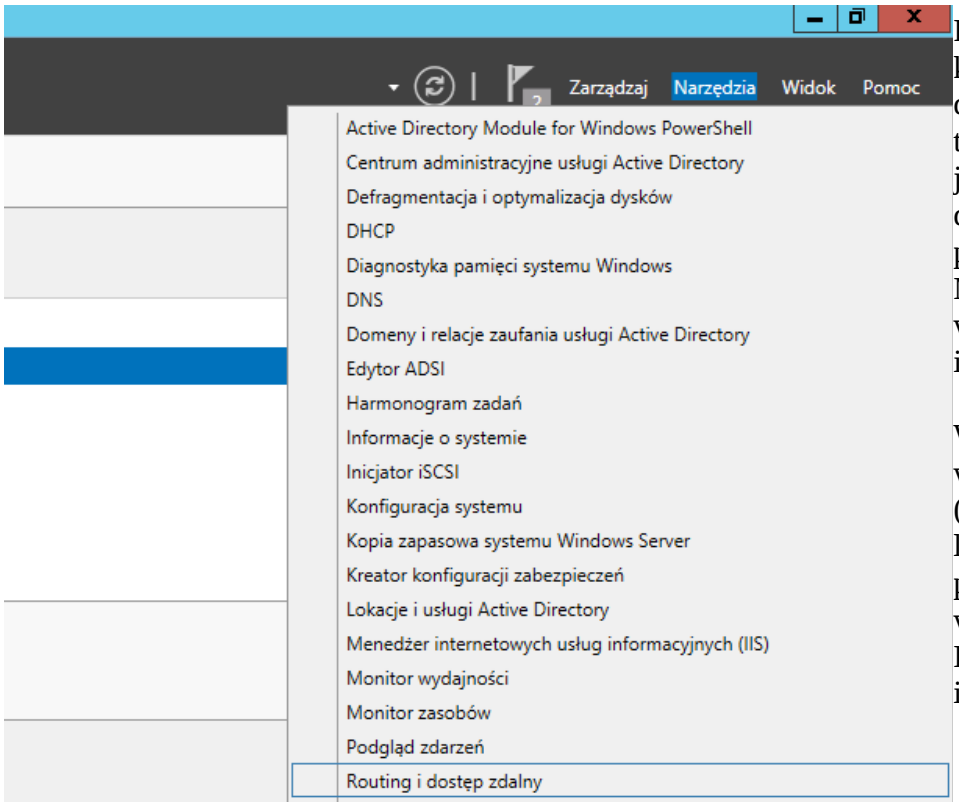


Oczywiście akceptujemy wszystkie powiązanie, jakie nakazuje nam instalator (bez tego funkcja będzie niepełna/nie będzie działać w ogóle).

W oknie Wybieranie usług ról konieczne jest zaznaczyć pole Routing (natomiast można odznaczyć DirectAccess and VPN – chociaż niekoniecznie).

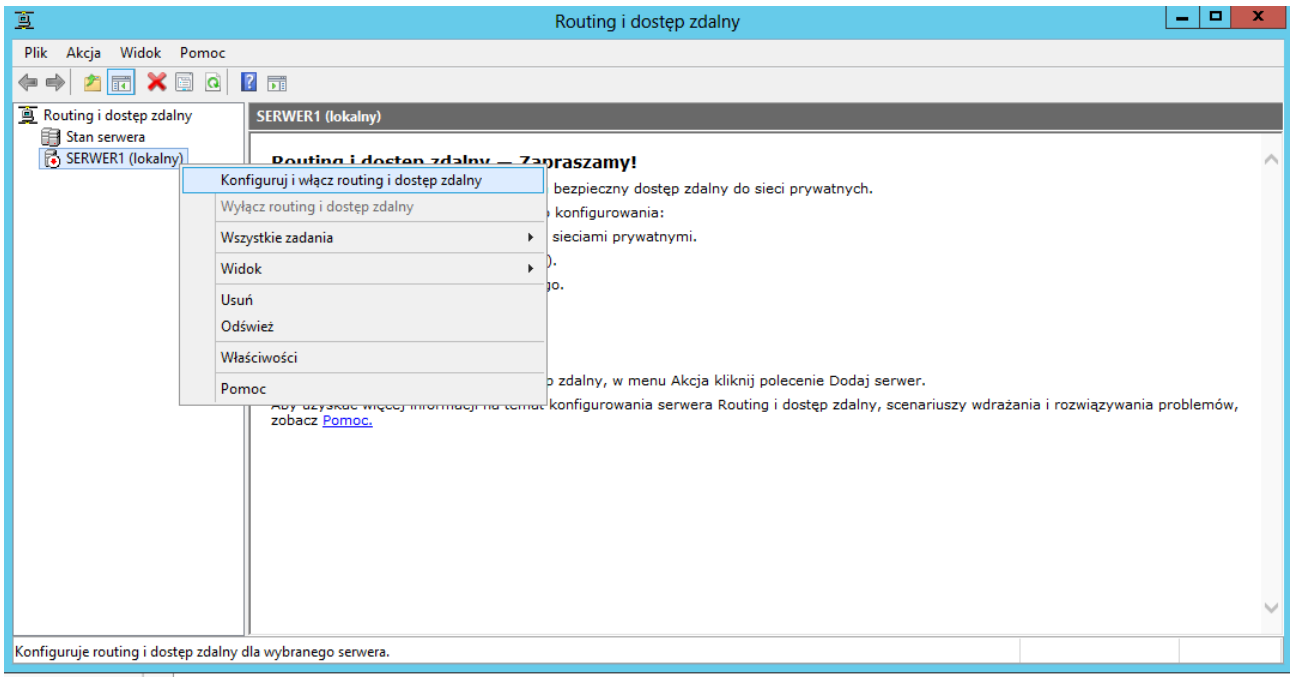


Kolejnym etapem będzie skonfigurowanie ról serwera IIS (Internet Information Services) – czyli inaczej mówiąc serwera WWW. Tutaj możemy zostawić domyślne ustawienia – potencjalnie zawsze można dodawać nowe role w miarę potrzeb.
Na koniec potwierdzamy naszą konfigurację i klikamy przycisk Zainstaluj.

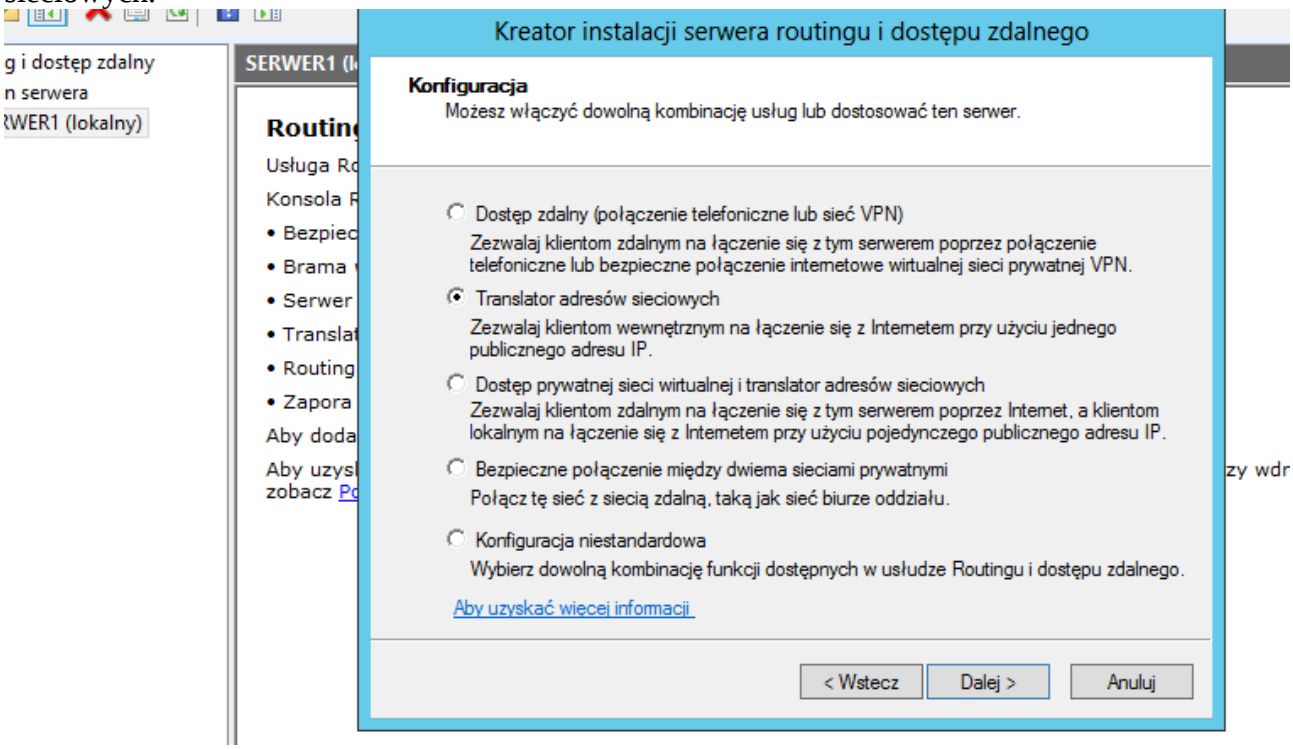


Po instalacji nie musimy konfigurować usługi dostępu zdalnego – można to ewentualnie zrobić jeżeli chcemy łączyć się do naszego serwera poprzez sieć WAN. Możemy natomiast wybrać narzędzie Routing i dostęp zdalny.

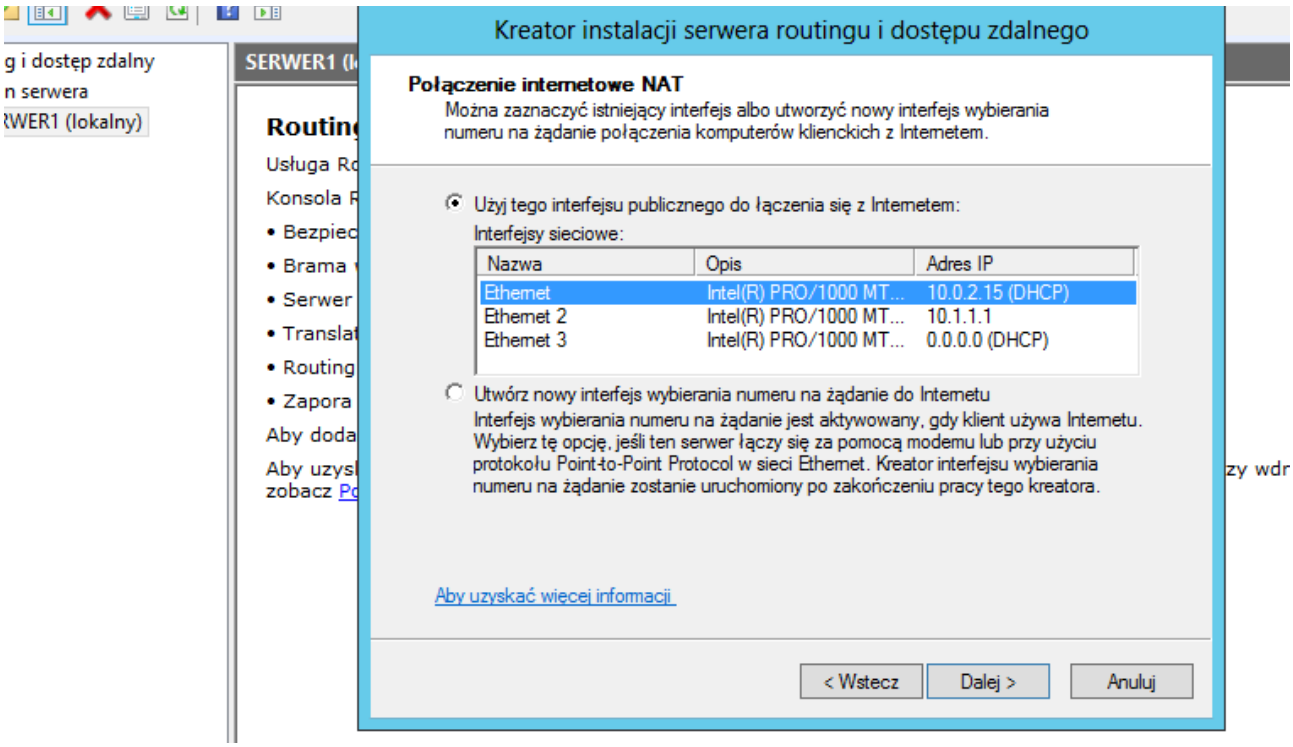
W oknie, które się pojawi, wybieramy nasz serwer (w nawiasie napis lokalny) prawym przyciskiem myszy i wybieramy opcję Konfiguruj i włącz routing i dostęp zdalny.



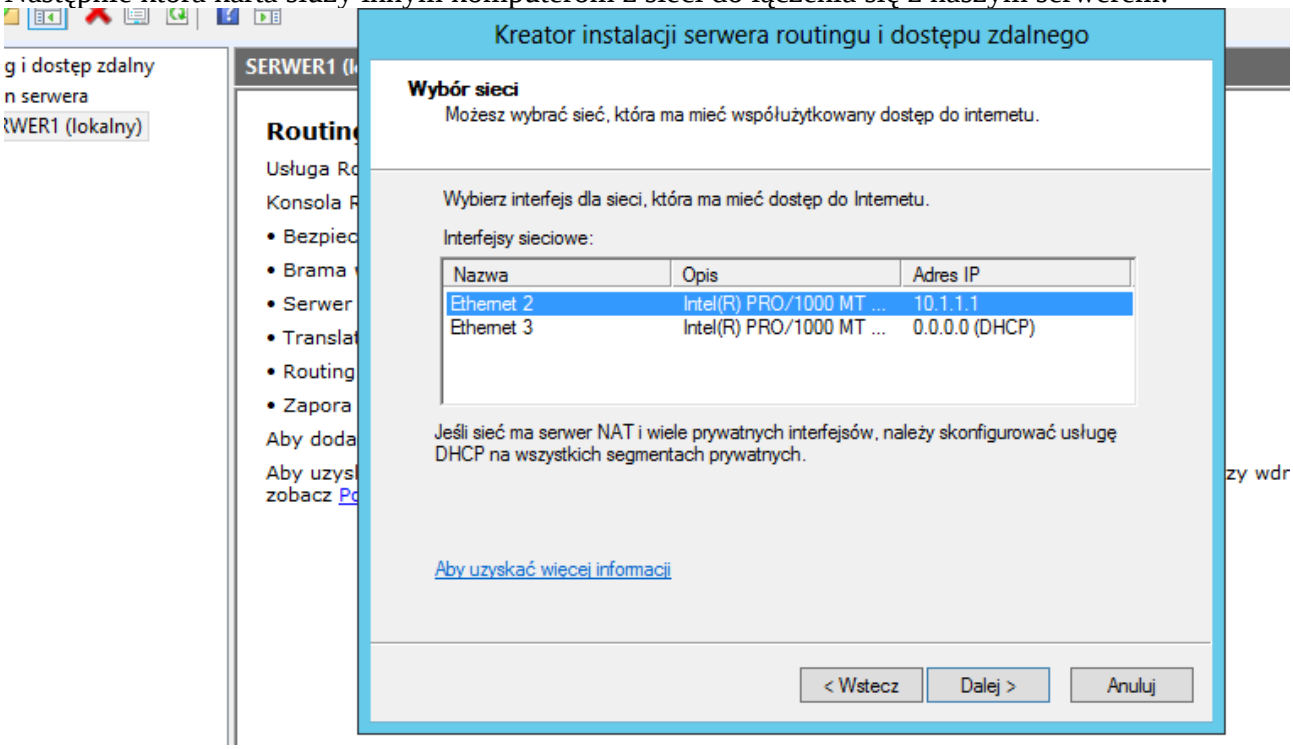
Po ekranie powitalnym zostaniemy poproszeni przez konfigurator o wybranie odpowiedniej roli naszej usługi. Możemy włączyć kilka z nich, jednak nam zależy tylko na Translacji adresów sieciowych.



W kolejnym kroku zaznaczamy kartę, która dostarcza nam dostęp do sieci szerokopasmowej:

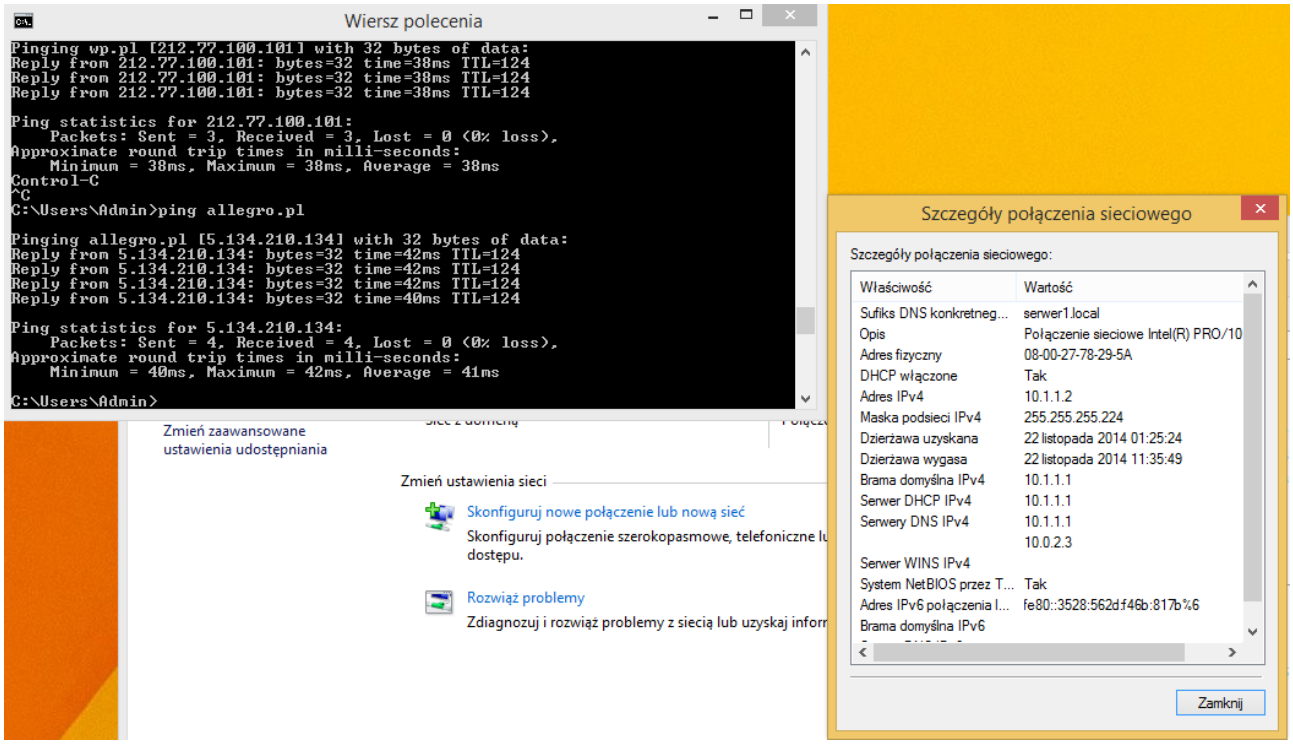


Następnie która karta służy innym komputerom z sieci do łączenia się z naszym serwerem:



Kończymy konfigurację i czekamy aż serwer wszystko poustawia.

Jeżeli wszystko się udało i serwer nie zwrócił błędu to powinniśmy mieć od tej chwili pełny dostęp do internetu z każdego komputera znajdującego się w naszej sieci lokalnej, która ma dostęp do naszego serwera.

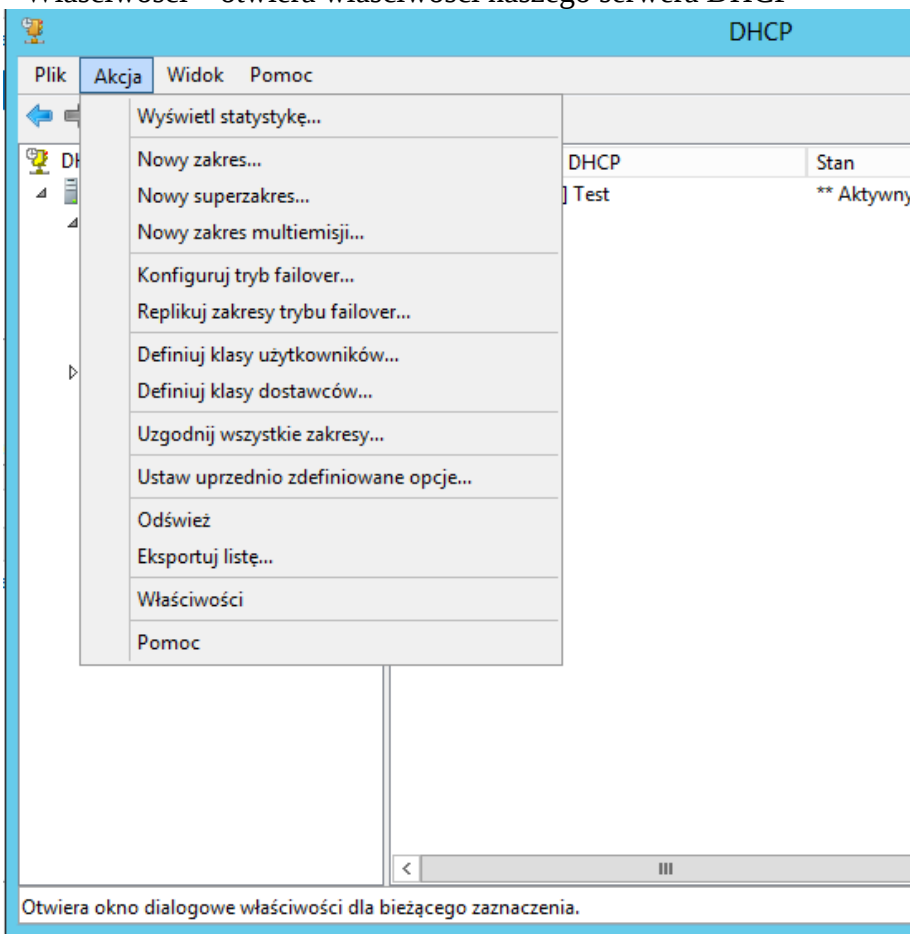


Więcej informacji o Routingu i dostępie zdalnym można znaleźć na stronie:
http://technet.microsoft.com/en-us/network/dd420463.aspx

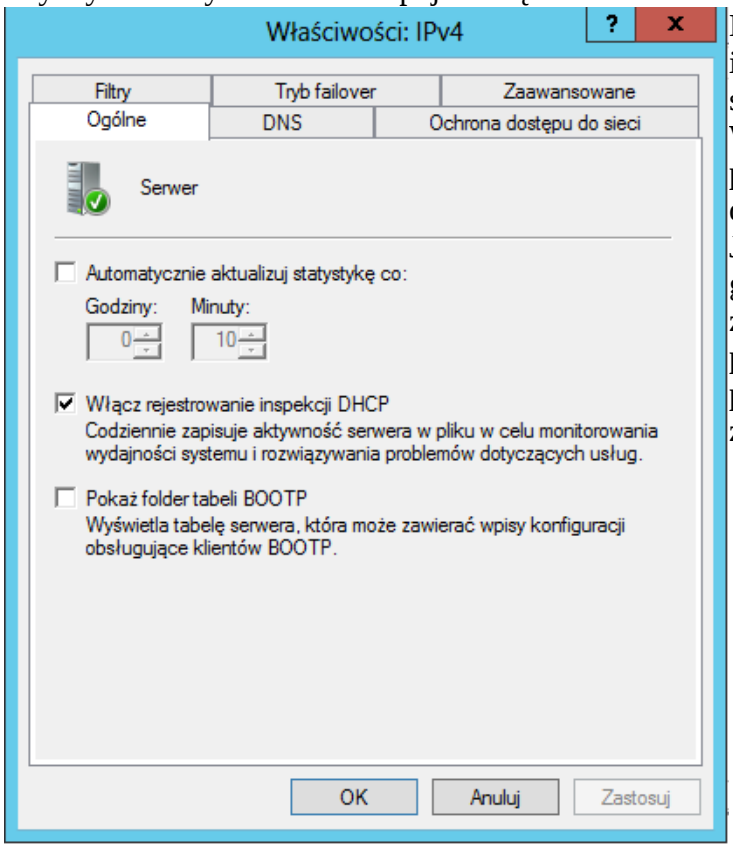
Bliższe spojrzenie na usługę DHCP

Menu Akcja narzędzia DHCP zawiera wszystkie możliwe operacje, jakich możemy dokonać na naszym serwerze. Patrząc od góry:
- Wyświetl statystykę – wyświetla szczegółową statystykę naszego serwera. Możemy się z niej dowiedzieć ile czasu jest on w trybie nasłuchu, kiedy rozpoczął pracę, ile adresów IP jest dostępnych, ile aktualnie wykorzystanych itd. Tego typu zestawienie pozwala na sprecyzowanie czy potrzebna będzie ingerencja w nasz serwer DHCP (zwiększenie/zmniejszenie puli), podgląd czy ktoś zbyt często nie wysyła żądań o nadanie IP (podejrzenie ataku) itp.
- Nowy zakres... - powoduje uruchomienie kreatora nowego zakresu puli DHCP.
- Nowy superzakres... - jeżeli mamy dodanych kilka zakresów adresów IP możemy połączyć je w jeden zakres, w celu wygodniejszej administracji nimi
- Nowy zakres multiemisjii... - uruchamia kreatora nowego zakresu puli DHCP dla adresów multicast (niefortunne tłumaczenie). Historycznie domyślnym zakresem multicast są adresy D – 224.0.0.0-239.255.255.255 (oczywiście teraz niemal nikt o to nie dba)
- Konfiguruj tryb failover... - pozwala na skonfigurowanie serwera, który przejmie rolę aktualnie używanego w przypadku wystąpienia błędów/uszkodzeń/niedyspozycji naszego głównego serwera (obecny). TRZEBA POSIADAĆ DRUGI SERWER (nie da się skonfigurować serwera zapasowego na aktualnie używanym)
- Definiuj klasy użytkowników – pozwala na definiowanie klas użytkowników DHCP. Opcja przydatna dla serwera wielozakresowego; w przeciwnym wypadku wystarczą jedynie trzy już zdefiniowane klasy
- Definiuj klasy dostawców – podobnie jak poprzednio z tym, że pozwala definiować dostawców zakresów IP (poszczególne systemy, które będą „nabywać” adresy z naszego zakresu)
- Uzgodnij wszystkie zakresy... - pozwala na weryfikację i potencjalne wychwycenie niezgodności pomiędzy zakresami dostępnymi w bazie danych (systemu) a rejestrem (aktualnie używanymi)
- Ustaw uprzednio zdefiniowane opcje... - pozwala zmieniać poszczególne opcje serwera DHCP/opcje dostawców, a także pozwala usuwać/dodawać nowe. Należy pamiętać, że dana opcja musi być obsługiwana przez klienta; w przeciwnym wypadku zmiana/dodanie/usunięcie opcji nic

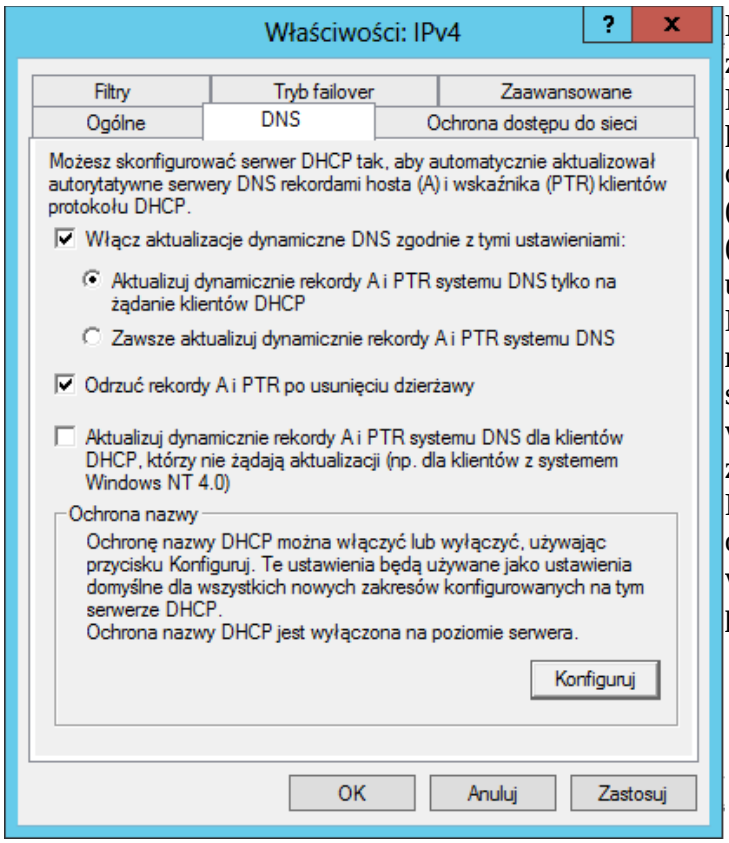
nie zmieni; jeżeli opcji nie będzie reakcja na taki stan będzie zależeć od klienta serwera DHCP.
- Odśwież – odświeża widok serwera (jeżeli ulegnie zmianie w trakcie przeglądania to nie zobaczymy tego przez odświeżeniem)
- Eksportuj listę... - eksportuje listę zakresów do pliku tekstowego
- Właściwości – otwiera właściwości naszego serwera DHCP



Gdy wybierzemy Właściwości pojawi się takie oto okno:

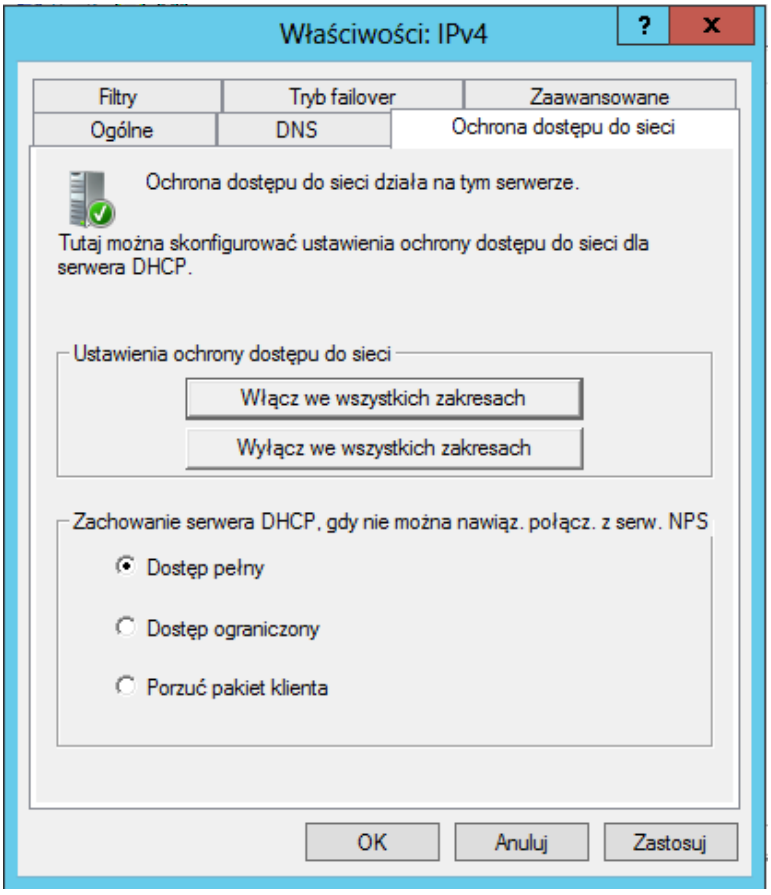


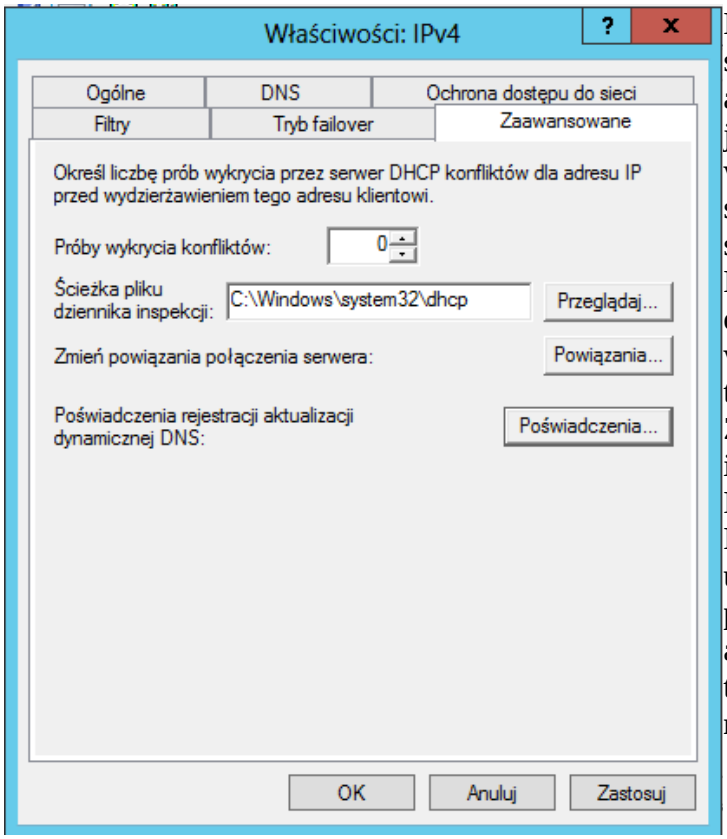
Na karcie ogólne możemy ustawić intensywność aktualizacji stanu naszego serwera DHCP co określony czas. Włączenie rejestrowania inspekcji DHCP pozwala na zapisywanie raportu z działania naszego serwera.
Jeżeli zaznaczymy ostatnią opcję to w gałęzi IPv4 pojawi się nowy folder zawierający zdefiniowane konfiguracje protokołu BOOTP. Na chwilę obecną protokół ten jest niemal nieużywany – zastąpił go DHCP z usługami TFTP/PXE.



Karta DNS pozwala na skonfigurowanie zachowań serwera DNS dla klientów DHCP. Można wymusić aktualizacje dla klientów, wysyłać je tylko na ich żądanie, odrzucać odniesienia do rekordów A (adres IP dla żądanej domeny) oraz PTR (odwrotna translacja) w przypadku usunięcia dzierżawy (adres wygasł). Dodatkowo można wymusić aktualizację rekordów A/PTR na klientach starszych systemów operacyjnych (jeżeli nie ma ich w sieci to lepiej nie ustawiać tej opcji – zmniejsza bezpieczeństwo)
Pod przyciskiem konfiguruj kryje się opcja włączenia ochrony nazwy – opcja ta wpływa na bezpieczeństwo serwera DNS przed tzw. zatruciem.

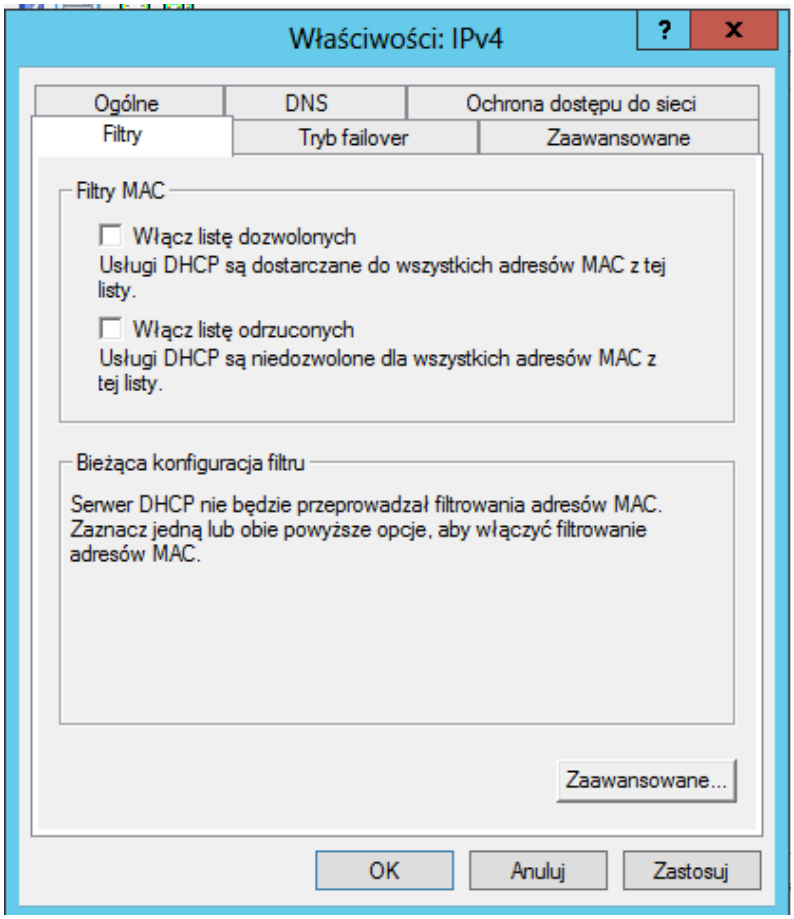
Ochrona dostępu do sieci pozwala na konfigurowanie zachowania serwera DHCP w przypadku gdy system posiada ustawione opcje NAP (Network Access Policy). Można ustawić odpowiednie zachowania serwera w przypadku, gdy dany klient nie spełnia zasad ustalonych dla inspekcji systemowej.





Karta zaawansowane pozwana wymusić na serwerze DHCP sprawdzenie, czy dany adres IP już nie jest przydzielony do jakiegoś komputera w sieci (błąd wygaśnięcia dzierżawy/ustawienie statyczne). Domyślnie nie jest to sprawdzane.
Można także zmieniać ścieżkę pliku dziennika zdarzeń (jeżeli mamy inne woluminy dobrym pomysłem jest trzymać tego typu dane z dala od woluminu C)
Zmiana powiązań pozwala na zmienienie interfejsów sieciowych, na których serwer DHCP nasłuchuje żądań dzierżawy.
Możemy także wprowadzić nazwę użytkownika oraz jego domeny w przypadku, gdy serwer DNS nie jest częścią aktualnego serwera Windows. Przydatne tylko w przypadku, gdy serwer DHCP ma rejestrować aktualizacje na serwerze DNS.

Zakładka filtry pozwala na dodatkową filtrację przydziału/odmowy dzierżawy adresów dla poszczególnych sprzętów sieciowych. Operacja ta będzie działała na podstawie dostarczonych w listach (katalog Filtry) adresach MAC (sprzętowe). Dodatkowo pod przyciskiem Zaawansowane można znaleźć listę sprzętów (początki adresów MAC), które są wyłączone z filtracji (produkty z tej listy mają krytyczne znaczenie dla pracy sieci).



Zakładka Tryb failover jest dla nas niedostępna (brak serwera zapasowego) więc została pominięta.

PODSUMOWANIE

Powyższe konfiguracje zostały przeprowadzone w ramach jednej maszyny fizycznej korzystającej z kart sieciowych ustawionych z opcją Attached to: internal network (VirtualBox, karty sieciowe). Jedynie karta sieciowa serwera Windows 2012 dostarczająca połączenie pozostała w trybie NAT. Zmiana na sieć wewnętrzną była o tyle konieczna, że w przypadku posiadania innego serwer DHCP system kliencki (Windows 8) mógłby dostać adres IP z zewnętrznego serwera DHCP, czego z kolei w ćwiczeniu należy unikać. Ponadto tego typu ustawienia nie są do końca bezpieczne – należy pamiętać, że im serwer Windows posiada więcej ról i narzędzi, tym łatwiejszym celem się staje. Pomimo tego, że firma Microsoft od pewnego czasu zamyka domyślnie większość ustawień (trzeba je samemu odblokować) to i tak sporo z nich może stanowić furtki dla włamywaczy (o których my za to możemy nie wiedzieć/nie pamiętać). Dlatego sama firma Microsoft zaleca ustanawiać tzw. serwery dedykowane (dedykowany serwer DHCP/DNS, dedykowany AD, dedykowany NAP itp.), a łączyć je przez jeden serwer tzw. Proxy (substytut tamtych, przekierowujący zapytania do odpowiednich serwerów).

ZADANIA:

1. Do utworzonego już zakresu DHCP Ipv4 należy dodać następny zakres, kontynuując numerację 30 hostową w sieci (maska 27).
2. Kolejnym etapem będzie złączenie tych zakresów w jeden superzakres. Jaki jest wynik operacji? Jak rozdawane są adresy IP dla Windows 8.
3. VirtualBox posiada możliwość zmiany adresu MAC karty (można też zmienić MAC poprzez opcje systemowe). Należy sprawdzić jak będzie zachowywał się serwer DHCP gdy co kilka sekund będziemy zmieniać adres MAC naszego wirtualnego systemu,a następnie będziemy wysyłali żądanie przydzielenia dzierżawy.
4. Czym jest zatrucie DNS?
5. Czym jest DirectAccess? Czy można go konfigurować na adres IPv4?
6. Proszę podać przykład konfiguracji zasady DHCP
7. W jaki sposób przekierowywać usługi do urządzeń znajdujących się za NAT w usłudze routing i dostęp zdalny? Do czego służy przekierowanie usług/portów?