

Konfigurowanie domyślnej zapory sieciowej Windows Server

Zapory sieciowe (firewall – ściana ognia) mają za zadanie blokować niechciany ruch sieciowy z i do naszego serwera czy komputera. Bez stosowania zapory sieciowej nasz komputer może bardzo szybko paść ofiarą złośliwego oprogramowania i przykładowo przesyłać ruch sieciowy w miejsce przez nas niepożądane. Przykładowo bez zapory osoba/zespół atakujący nasz serwer (bądź całą sieć/system informatyczny) może wykradać z niego poufne informacje, oddziaływać na naszą sieć, wysyłać za jej pomocą spam itp. W najgorszym wypadku taki atak może doprowadzić do paraliżu całej sieci, serwera bądź całkowitego przejęcia kontroli nad serwerem/zniszczeniem go (w sensie oprogramowania). Dlatego NIGDY nie powinno się pozostawiać żadnego systemu bez zapory sieciowej. Większość tego typu oprogramowania działa na zasadzie:

- filtracji pakietów – narzędzie sprawdza czy dany pakiet rzeczywiście pochodzi od spodziewanej aplikacji oraz czy „odpytuje” usługę docelową na właściwym porcie; gdy wszystko się zgadza akceptuje ruch
- NAT (Network Address Translation – sieciowe tłumaczenie adresów) – inaczej zwany maskaradą. Pozwala na „schowanie” komputerów podłączonych w sieci lokalnej za jednym adresem zewnętrznym serwera/trasownika. W ten sposób wszystkie komputery z sieci widoczne są dla innych komputerów sieci rozległej jako jeden komputer. Dzięki temu nawet w przypadku „złamania” komputera-serwera istnieje duża szansa ochrony komputerów klienckich – szybka reakcja administratora pozwala odciąć zagrożone komputery od komunikacji z siecią rozległą.
- proxy (pośrednik ruchu) – serwer tego typu wykonuje zapytania sieciowe w imieniu maszyny (użytkownika) zlecającej. Najlepszym przykładem tego typu zabezpieczenia jest przekierowywanie ruchu przeglądarki na tego typu serwer. Po pierwsze maskuje się w ten sposób tożsamość klienta (serwer strony widzi adres IP serwera proxy, nie komputera docelowego), po drugie tego typu serwer może efektywnie wpływać na szybkość transmisji danych - serwer proxy gromadzi przeważnie najczęściej pobierane dane, które były poprzez niego żądane; dzięki temu ponowne zapytanie o nie będzie przesyłane przez niego, a nie serwer docelowy zapytania. W przypadku gdy serwer znajduje się w sieci lokalnej powoduje to przesyłanie danych z prędkością sieci lokalnej (aktualnie po kablach LAN min. 10 Mbps). Dodatkowo serwer tego typu może być skonfigurowany tak by blokować pewne niechciane treści, przykładowo obraźliwe strony, niektóre dane (reklamy na stronach WWW) itp.

INFORMACJA: Na obecną chwilę większość z nas posiada w domu urządzenie sieciowe o nazwie router. Urządzenia te posiadają wbudowaną zaporę sieciową oddzielającą nas od świata zewnętrznego. Nie znaczy to, iż nie warto „zainwestować” w konfigurację dodatkowej zapory w swoim komputerze (systemy OS X/Linux posiadają ją w zasadzie od niepamiętnych czasów, np. ipfw czy iptables, które to najczęściej wybierane są także do sporej ilości urządzeń trasujących). Windows od XP z Service Pack 2 także posiada domyślną zaporę sieciową, która w połączeniu z zaporą zewnętrzną (router) na domowe potrzeby w pełni wystarcza. Można też pokusić się o rozwiązania komercyjne (dostawcy zewnętrzni; niektóre wersje darmowe do zastosowań domowych).

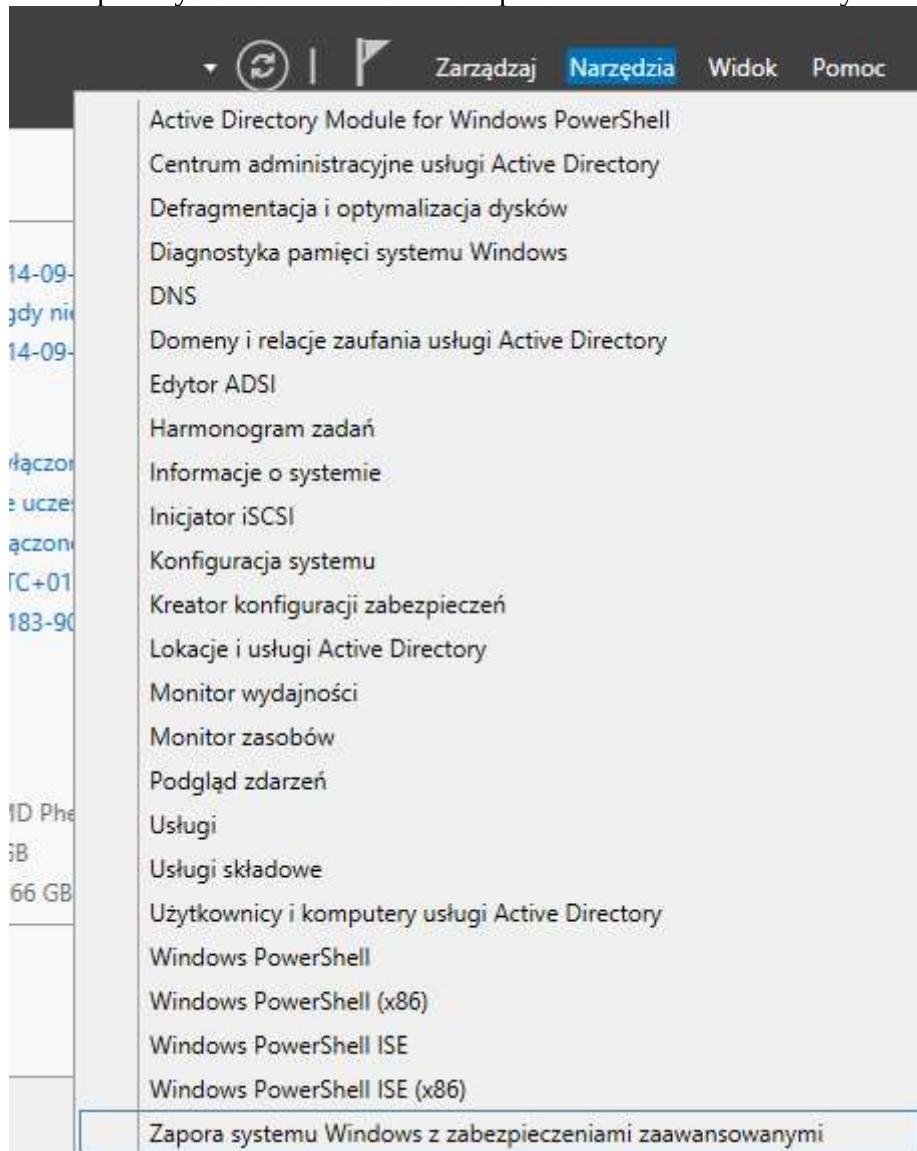
Firma Microsoft od wydania Windows 2003 Server dołącza do swoich produktów serwerowych wbudowaną w system ochronę ogniomową. Narzędzie stoi na przyzwoitym poziomie i zapewnia ochronę w czasie rzeczywistym. Ponadto w ofercie znajdują się takie narzędzia jak ISA Server (Microsoft Internet Security and Acceleration Server) oraz ForeFront. Niestety (albo stety) ISA Server został porzucony przez firmę w roku 2006 (jego „kariera” zakończyła się wraz z Windows 2003 Server; projektowany był dla Windows 2000 Server). Z kolei ceniony przez użytkowników ForeFront nie jest obecnie dostępny (i wedle rozkładu firmy nie będzie) dla Windows 2012 Server. W przypadku tego ostatniego narzędzia nie jest na szczęście tak źle – większość jego funkcji (jak ochrona połączeń VPN, serwer Proxy, monitorowanie działań użytkowników czy ochrona połączeń

zdalnych) zostały zaimplementowane jako role i narzędzia serwera Windows 2012 R2 (wydany w roku 2014).

Na zajęciach bliżej poznamy możliwości standardowej (domyślnej) zapory sieciowej systemu Windows. Prócz samej ochrony pozwala ona także na inne operacje (w połączeniu z usługą ActiveDirectory).

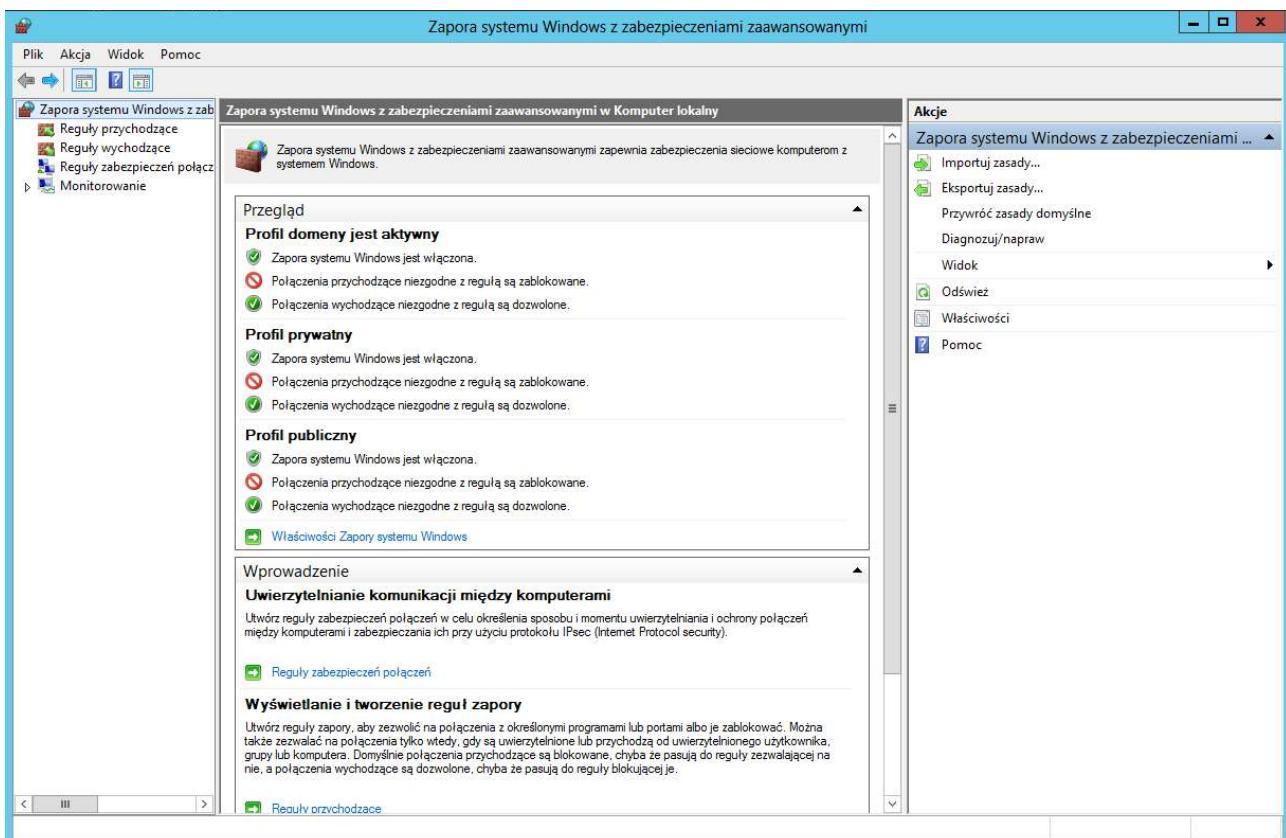
1. Konfiguracja i użytkowanie

Konfigurowanie zapory sieciowej w systemie Windows 2012 można rozpocząć od wybrania jej w menu Narzędzia->Zapora systemu Windows z zabezpieczeniami zaawansowanymi



Proszę pamiętać by nie wybierać opcji zapory sieciowej poprzez Panel sterowania – tam pierwotnie otworzy się identyczne okno do tego, jakie możemy zobaczyć np. w systemie Windows 8 (trzeba dodatkowo wybierać opcje zaawansowane).

Okno zaawansowanej zapory sieciowej to nic innego jak jedna z przystawek systemu Windows. Okno pozwala na pełną konfigurację zasad zabezpieczenia danego komputera.



Po prawej stronie mamy możliwe akcje:

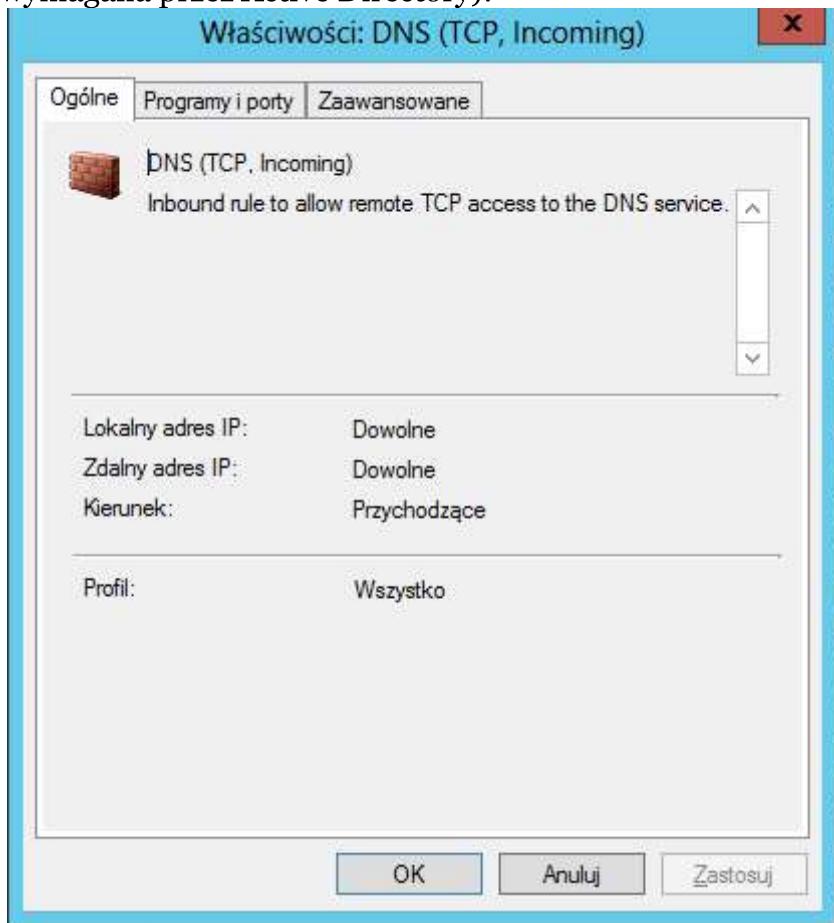
- Importuj zasady.../Eksportuj zasady... - funkcja pozwala na wyeksportowanie bieżących zasad zapory do pliku. Następnie tego typu plik można importować na tym samym komputerze (eksport jest formą kopii bezpieczeństwa ustawień zapory) jak też importować z niego zasady na inny komputer (bądź do zasad domeny)
- Przywróć zasady domyślne – przywraca zasady jakie domyślnie sugeruje Microsoft. Dotyczy to zarówno właściwości zapory jak i reguł przychodzących/wychodzących oraz zabezpieczeń połączeń sieciowych
- Diagnozuj/napraw – opcja ogólna dla wszystkich ustawień sieci w systemie Windows; kreator próbuje pomóc ustalić aktualny problem z dostępem do sieci/Internetu systemu Windows (który po części może być spowodowany ustawieniami zapory)
- Widok – pozwala dostosować widoczne elementy przystawki (mniej/więcej szczegółów)
- Odśwież – narzędzie najczęściej nie odświeża swoje widoku zaraz po zmianie pewnych ustawień (bądź nie odświeży zmian dokonanych na komputerze zdalnie/przez innego zalogowanego administratora). Opcja ta pozwala na ewentualne zobaczenie tychże zmian (następuje jego przeładowanie)
- Właściwości – pokazuje zaawansowane ustawienia poszczególnych profili zapory sieciowej. Zapora sieciowa w systemie Windows 2012 Server posiada 4 profile: Publiczny, Prywatny, Domenowy oraz Ustawienia protokołu IPSec.
- Pomoc – otwiera zawartość pliku pomocy dla zapory (zawartość na witrynie firmy Microsoft w języku angielskim).

Po lewej stronie mamy drzewo nawigacyjne poszczególnych opcji narzędzia:

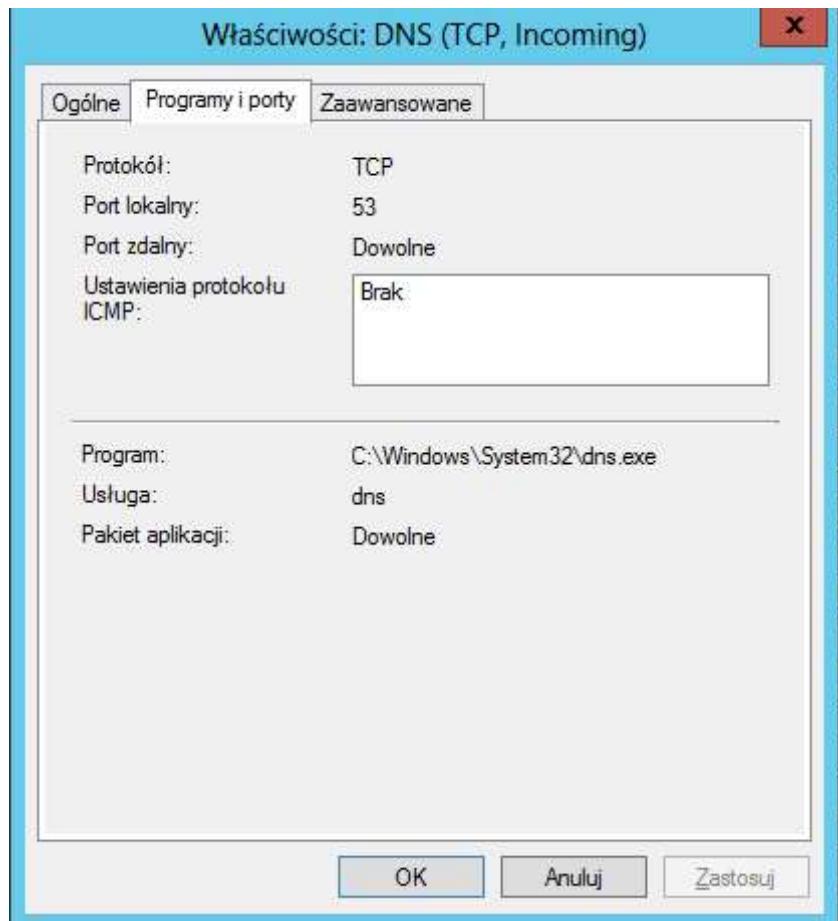
- Reguły przychodzące – tutaj przechowywane są wszystkie wyjątki dla poszczególnych aplikacji, portów oraz protokołów, które mają być przepuszczane/blokowane w przypadku, gdy połączenie jest inicjowane SPOZA naszego serwera; najlepszym przykładem może być próba pobrania i wyświetlenia przez klienta strony WWW z naszego serwera bądź podłączenia się poprzez protokół pulpitu zdalnego (RDP).
- Reguły wychodzące – ustawienia analogiczne do poprzednich – pozwalają na kontrolowanie ruchu inicjonowanego przez NASZ serwer. Reguły te najczęściej służą jako

blokada poszczególnych aplikacji (szczególnie nowo instalowanych – nigdy nie wiadomo jakie informacje zbierają i gdzie je przesyłają); tutaj jak przykład może być blokowanie połączeń do zdalnych serwerów FTP (mało bezpieczne) czy też wysyłanie zaproszeń pomocy zdalnej (użytkownik sam powinien decydować kiedy tego typu ruch będzie inicjowany).

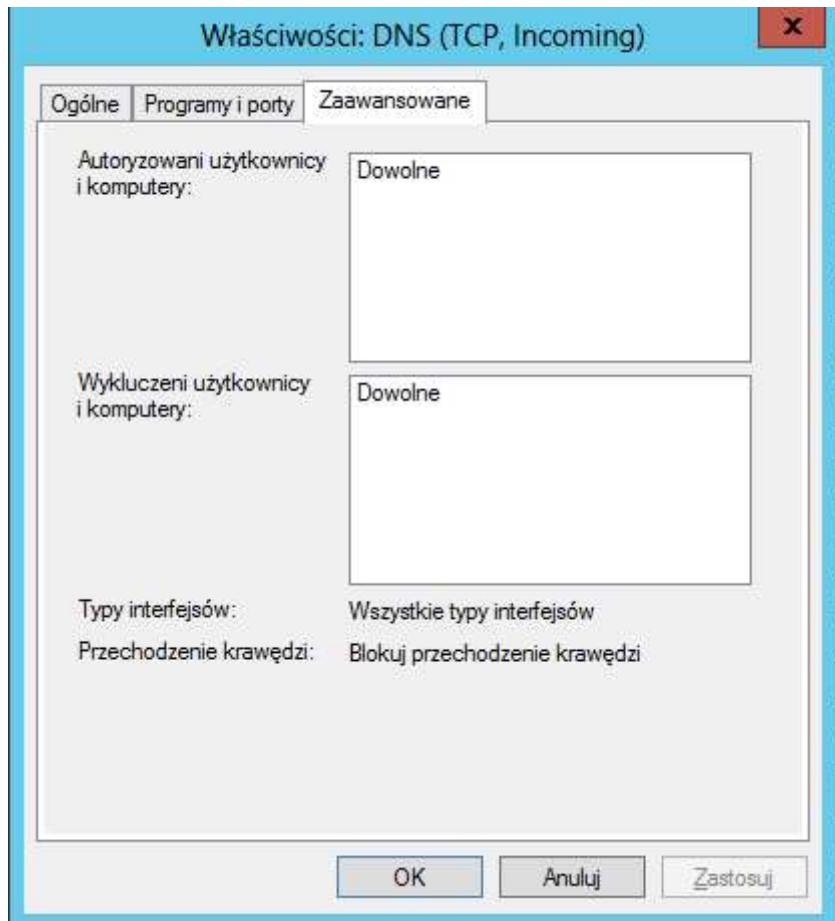
- Reguły zabezpieczeń połączeń – tutaj przechowywane są wszystkie reguły połączeń pomiędzy dwoma komputerami/sieciami komputerowymi. Tego typu reguły służą m. in. ustanowieniu połączeń VPN bądź tuneli IPSec.
- Monitorowanie – pozwala przejrzeć aktualne, aktywne ustawienia zapory sieciowej. Opcja zawiera trzy podkategorie:
 - 1) Zapora – pokazuje wszystkie aktywne reguły zapory sieciowej (przychodzące i wychodzące). W polu Akcje możemy wybrać:
 - a) Eksportuj listę... - wyeksportuje wszystkie aktualne reguły zapory do pliku tekstowego.
 - b) Właściwości – pozwala wyświetlić szczegółowe właściwości aktualnie wybranej reguły. Okno właściwości zawiera trzy zakładki. Przykładowo dla reguły DNS (w naszym wypadku usługa serwera wymagana przez Active Directory):



Zakładka Ogólne zawiera nazwę wybranej reguły, jej opis (aktualnie wybrana jest reguła domyślnie tworzona przez system; własne mogą nie zawierać opisu jeżeli sami go nie stworzymy), Lokalny adres IP komputera, który może korzystać z tej reguły (w powyższym przypadku każdy ustawiony adres na dowolnym interfejsie sieciowym może z niej korzystać), Zdalny adres IP komputera, który może połączyć się z usługą DNS (domyślnie dowolny adres IP z dowolnej puli adresowej – zarówno lokalnej jak i globalnej), Kierunek z którego ma być inicjowane połączenie (w tym wypadku przychodzące połączenie – z zewnątrz) oraz Profil, do którego odnosi się reguła (ta konkretna odnosi się do wszystkich profili jednocześnie).



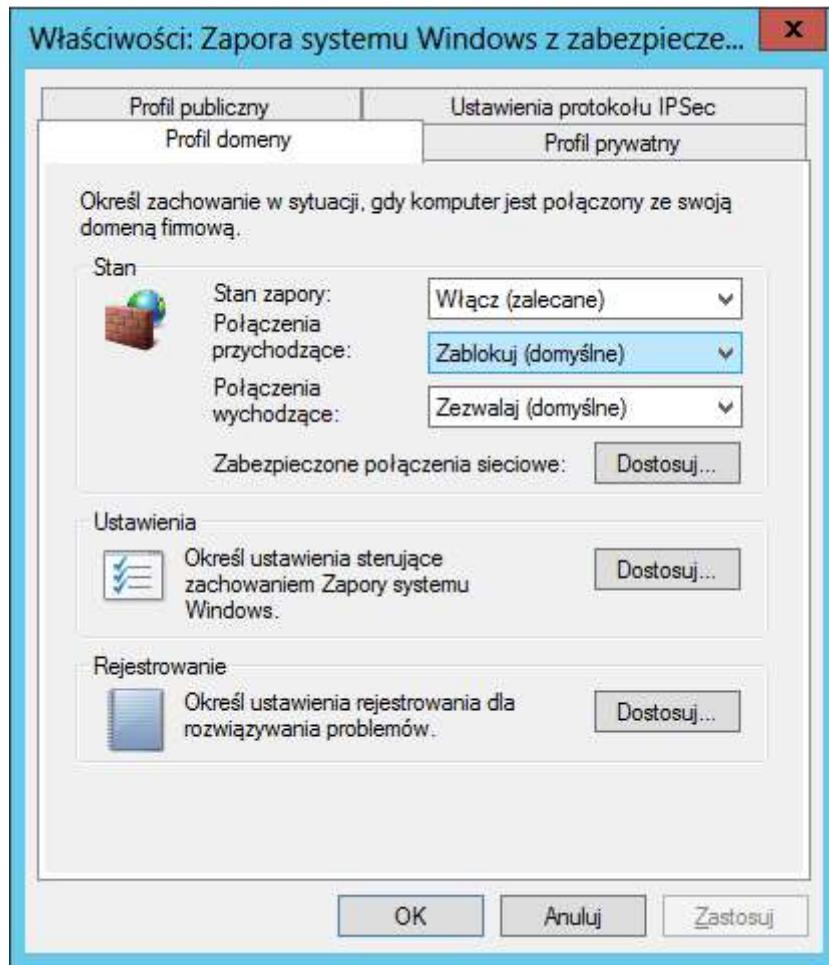
Zakładka Programy i porty wskazuje, który Protokół akceptowany jest przez regułę (w tym wypadku TCP), przez który Port lokalny ma być realizowany ruch (na którym nasłuchuje nasz program – port docelowy; w tym wypadku jest to standardowy port DNS – 53), który Port zdalny ma być akceptowany przez regułę (port źródłowy, na którym maszyna zdalna zainicjowała transmisję; w tym wypadku nie ma to większego znaczenia), Ustawienia protokołu ICMP (protokół „diagnostyczny”; dla tego połączenia nie odgrywa roli), Program, dla którego realizowana jest reguła (w tym wypadku program dns.exe), Usługa (w tym wypadku tożsama z nazwą programu lecz nie musi to być regułą!) oraz Pakiet aplikacji (jeżeli inne aplikacje mogą korzystać z tej reguły).



Zakładka Zaawansowane zawiera informacje o Autoryzowanych użytkownikach i komputerach (w powyższym przypadku nie ma znaczenia ani użytkownik, ani komputer, który będzie obsługiwany przez regułę – może to być każdy), Wykluczonych użytkownikach i komputerach (na powyższym zrzucie nie ma wykluczonych komputerów ani użytkowników, którzy nie mogliby korzystać z tej reguły), Typach interfejsu (nie ma nałożonych ograniczeń co do kart sieciowych, które mogą obsługiwać tę regułę) oraz Przechodzeniu krawędzi (przechodzenie krawędzi pozwala na akceptowanie nieuchcianych pakietów/niebezpiecznych, które przeszły przez urządzenia brzegowe (krawędziowe), do których wlicza się np. NAT router czy sprzętowy firewall – przykładem może być tutaj usługa Teredo tunelująca IPv6 w IPv4; więcej informacji o tej opcji można znaleźć na tej stronie <http://serverfault.com/questions/89824/windows-advanced-firewall-what-does-edge-traversal-mean>).

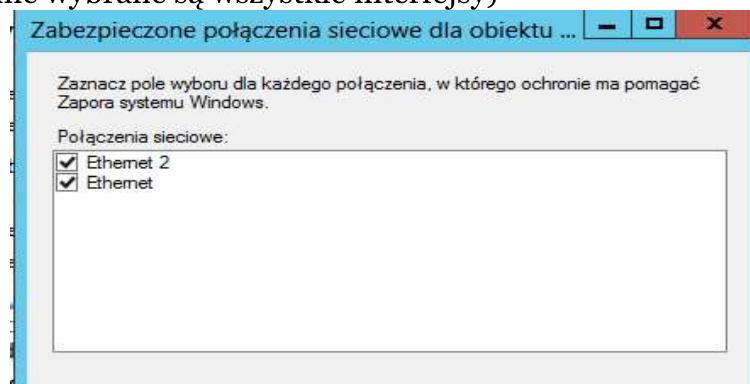
- 2) Reguły zabezpieczeń połączeń – tutaj wyświetlają się wszystkie aktywne reguły dla połączeń (domyślnie nie ma żadnych)
- 3) Skojarzenia zabezpieczeń – wyświetlane są reguły zabezpieczeń połączeń pomiędzy poszczególnymi komputerami (połączenia VPN/IPSec/Tuneli)

Kolejnym ważnym aspektem są właściwości Zapory systemu Windows. Ustawienia są bardzo podobne dla innych profili dlatego omówione zostaną właściwości jednego z nich. Zakładka każdego profilu wygląda tak samo jak na poniższym zrzucie:

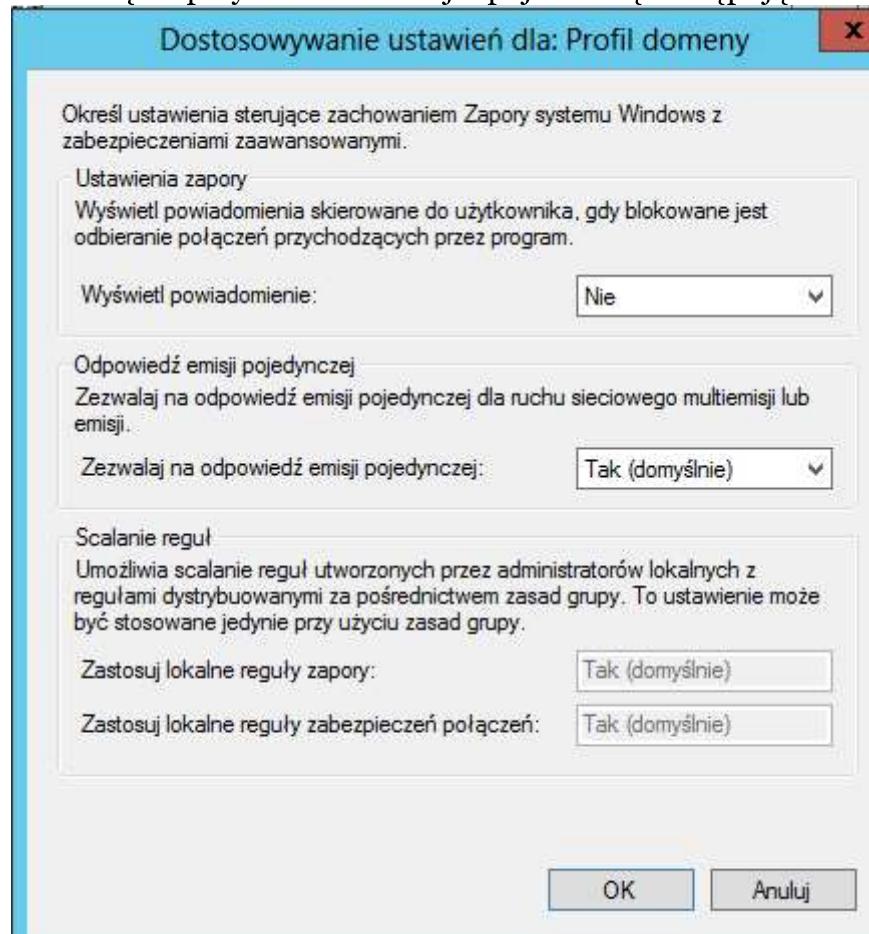


W grupie Stan można ustawić następujące właściwości:

- Stan zapory - może przyjąć wartość Włącz (wszystkie reguły zapory są stosowane dla tego profilu) lub Wyłącz (ruch NIE JEST filtrowany przez zaporę dla tego profilu)
- Połączenia przychodzące - może przyjąć trzy wartości:
 - 1) Zablokuj – jeżeli dany ruch inicjowany przez inny komputer nie będzie posiadał odpowiedniej reguły to zostanie zablokowany
 - 2) Zablokuj wszystkie połączenia – żadne połączenie z zewnątrz nie będzie mogło zostać zainicjowane (nawet to z reguł zapory)
 - 3) Zezwalaj – wszystkie połączenia z zewnątrz będą domyślnie inicjowane (nawet jeżeli nie istnieją odpowiednie reguły w zaporze)
- Połączenia wychodzące – może przyjąć wartość Zezwalaj (każdy ruch jest domyślnie przepuszczany do sieci) lub Zablokuj (jedynie odpowiednio utworzone reguły będą zezwalać na ruch do sieci)
- Zabezpieczone połączenia sieciowe – klikając przycisk dostosuj przenosimy się do nowego okna, które pozwala wybrać interfejsy sieciowe, dla których będzie stosowany stan zapory sieciowej (domyślnie wybrane są wszystkie interfejsy)



Grupa Ustawienia pozwala dostosować ustawienia zachowania się zapory w określonych sytuacjach. Po naciśnięciu przycisku Dostosuj... pojawia się następujące okno:

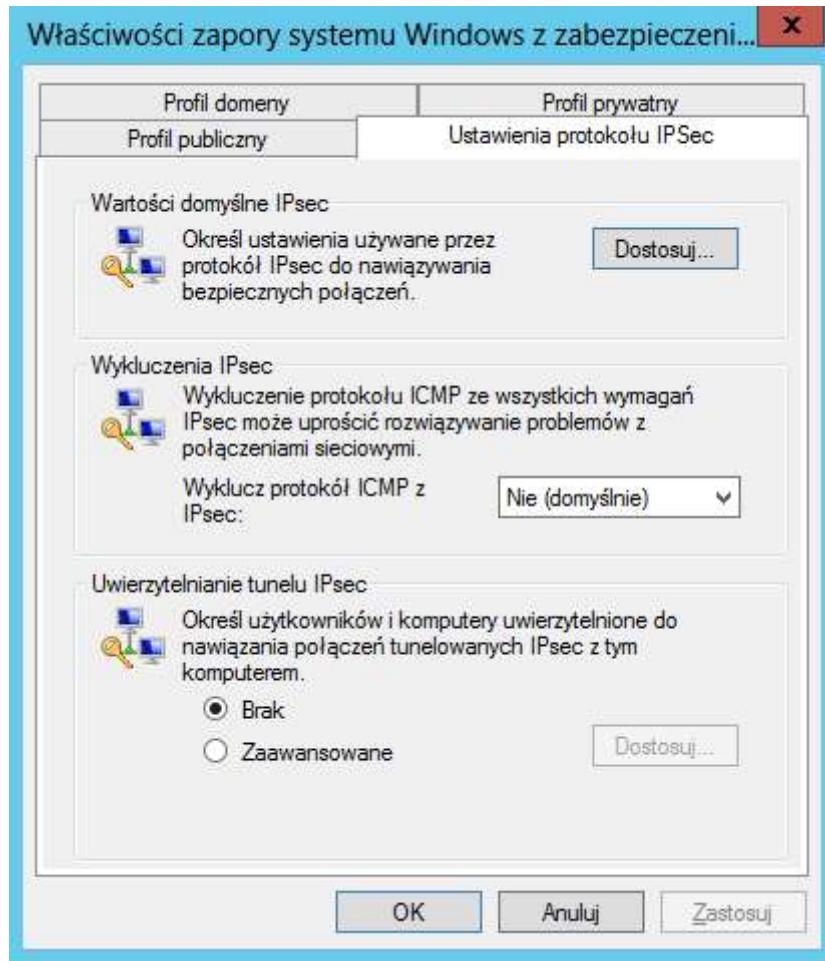


W Ustawieniach zapory można określić (wartości Tak/Nie) czy system ma informować użytkownika o operacji zablokowania pakietu przychodzącego z zewnątrz (domyślnie nie informuje).

Odpowiedź emisji pojedynczej (wartości Tak/Nie) pozwala na zablokowanie na odpowiedzi ping i inne komunikaty ICMP (komunikaty rozgłoszeniowe).

Scalanie reguł pozwala na zastosowanie powyższych reguł z zasadami grupy. Wtedy stosowane są one na wszystkich komputerach podłączonych do usługi Active Directory.

Właściwości zapory mają jeszcze jedną, inną zakładkę od pozostałych – Ustawienia protokołu IPSec. Protokół ten pozwala na bezpieczne i pewne przesyłanie danych (sprawdzanie integralności, podpis maszyny wysyłającej dane oraz opcjonalnie zaszyfrowanie przesyłanej informacji). Jednym z zastosowań tego protokołu jest tworzenie sieci VPN. Karta jego ustawień wygląda następująco:



Grupa Wartości domyślnie IPsec pozwala na określenie takich wartości jak sposób wymiany kluczy pomiędzy komputerami, sposób ochrony danych w trybie szybkim (ochrona/szyfrowanie poszczególnych pakietów) czy metody uwierzytelniania poszczególnych użytkowników (domyślnie protokół Kerberos).

Z protokołu IPsec można wykluczyć protokół ICMP (wartości Tak/Nie).

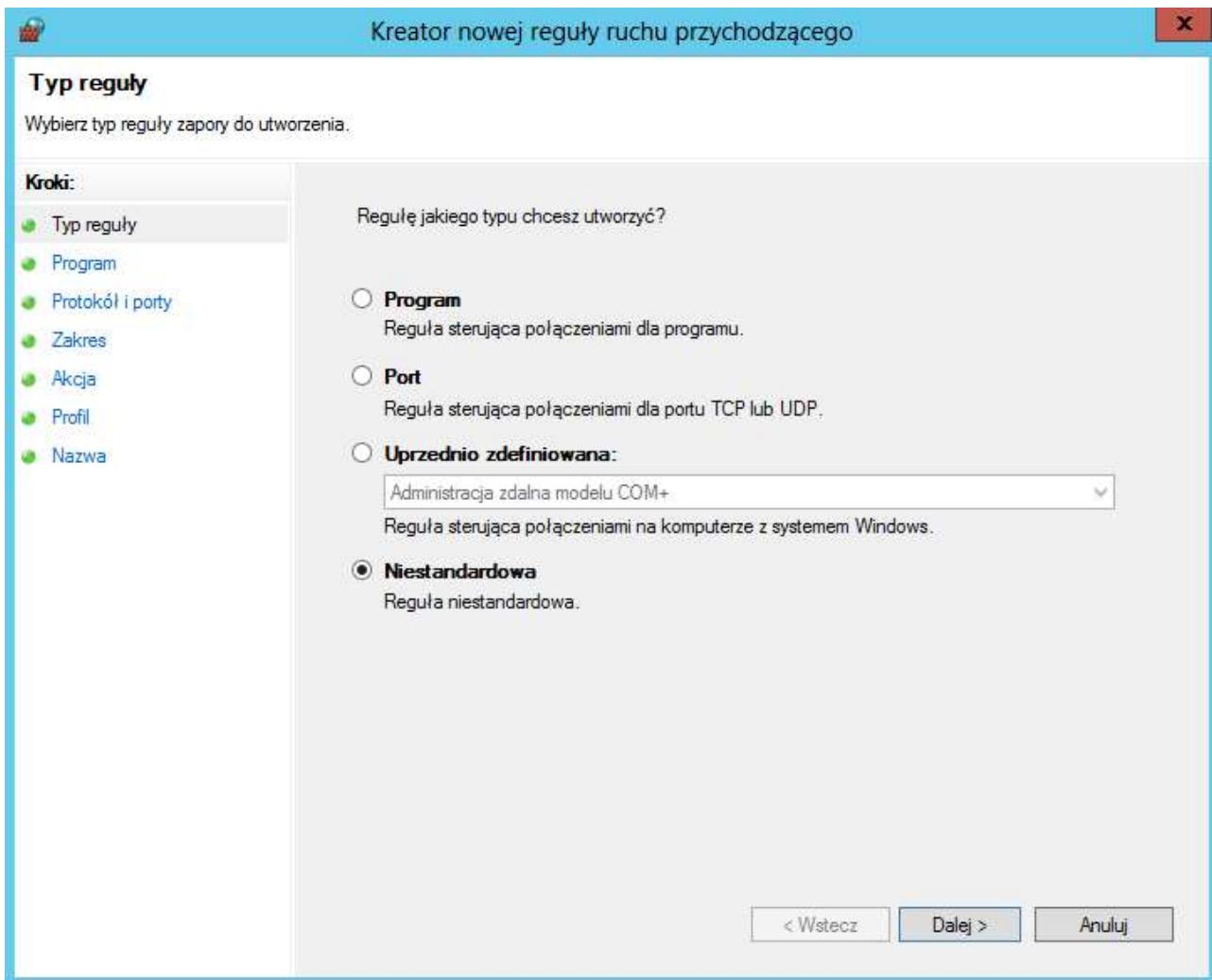
Uwierzytelnianie tunelu IPsec pozwala na wybranie autoryzowanych/odrzucających maszyn komputerowych i/lub konkretnych użytkowników.

INFORMACJA: Aktualnie protokół IPsec jest domyślnie zaimplementowany w IPv6. W IPv4 jego obsługę można jedynie uruchomić jednak stanowi on osobną usługę.

INFORMACJA: Na zajęciach nie będzie omawiane tworzenie połączeń pomiędzy IPsec pomiędzy dwiema sieciami – jest to niewykonalne (trzeba by posiadać drugie miejsce docelowe, gdzie łączylibyśmy się poprzez np. Internet). Z kolei temat tworzenia połączenia IPsec pomiędzy dwiema stacjami (w sieci LAN) wykracza poza standardową konfigurację zapory ogniodzielnej – dokładny opis w języku angielskim zestawienia tego typu połączenia można znaleźć pod tym adresem -

http://www.it.cornell.edu/services/managed_servers/howto/ipsec.cfm .

Tworzenie reguł przychodzących/wychodzących przebiega tak samo. Gdy klikamy Nowa reguła... pojawia się takie oto okno:



Jeżeli będziemy tworzyć regułę dla Programu to tylko wskazany przez nas program (lub pakiet programów) będzie mógł korzystać z utworzonej reguły. Decydując się na regułę dla Portu system będzie przepuszczał cały ruch bez względu na aplikację jaka go zainicjuje lecz tylko na wskazanym porcie/grupie portów. Opcja Uprzednio zdefiniowana pozwala na ponowne wykorzystanie wcześniej zdefiniowanej reguły (np. w regułach wychodzących). Decydując się na regułę Niestandardową można utworzyć regułę mieszaną – przykładowo działającą na określonym porcie, dla konkretnego programu, z określonymi protokołami itp. To właśnie ją utworzymy.

Kreator nowej reguły ruchu przychodzącego

Program

Okreś pełną ścieżkę i nazwę pliku wykonywalnego programu, którego dotyczy ta reguła.

Kroki:

- Typ reguły
- Program**
- Protokół i porty
- Zakres
- Akcja
- Profil
- Nazwa

Czy ta reguła dotyczy wszystkich programów, czy określonego programu?

Wszystkie programy
Reguła dotyczy wszystkich połączeń na komputerze, które pasują do właściwości innych reguł.

Ta ścieżka programu:
Przykład: c:\ścieżka\program.exe
%ProgramFiles%\przeglądarka\przeglądarka.exe

Uslugi
Okreś usługi, których dotyczy ta reguła.

Dostosuj...

Dostosowanie ustawień usług

Zastosuj tę regułę w następujący sposób:

Zastosuj do wszystkich programów i usług

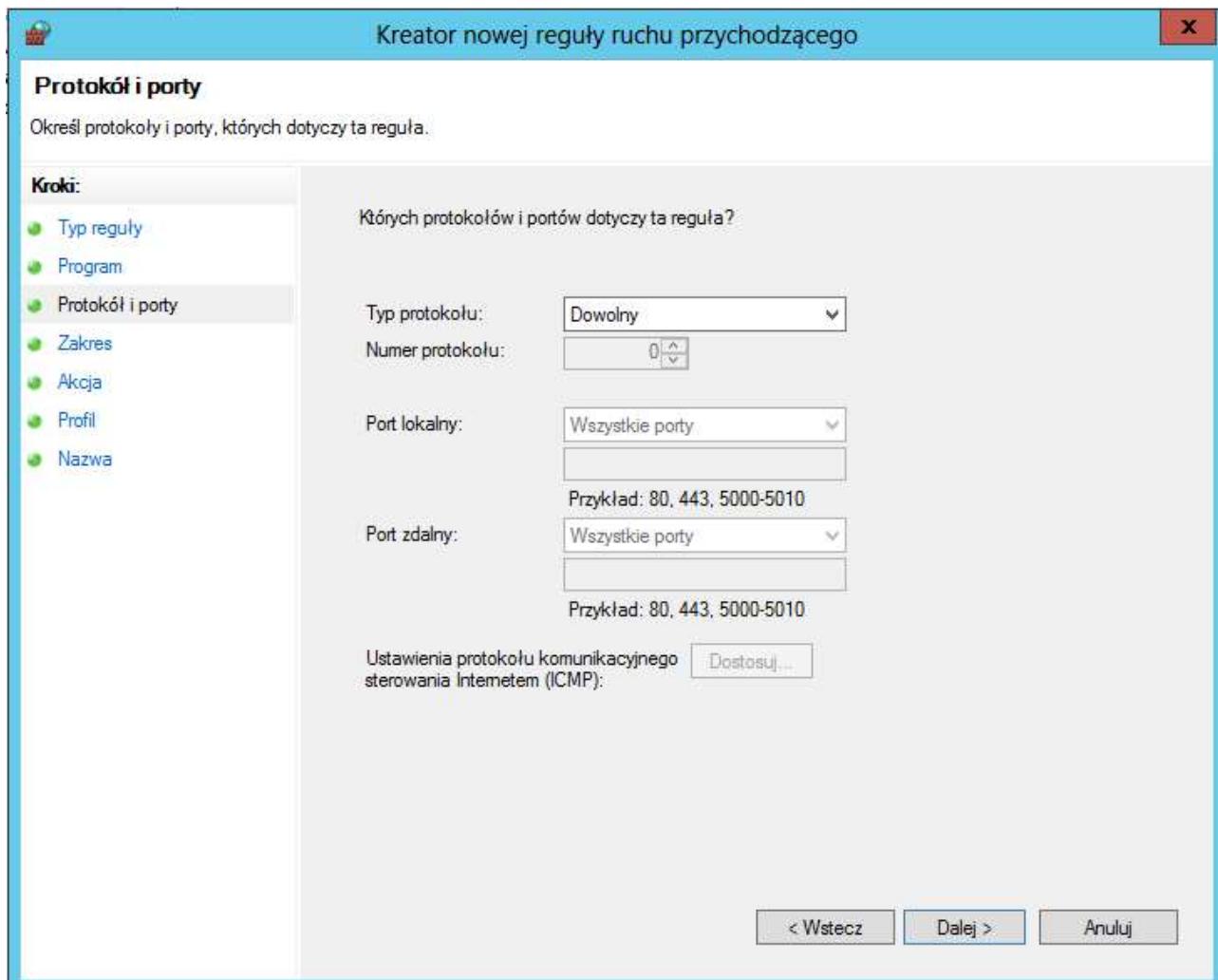
Nazwa	Nazwa krótka
Agent instalacji w systemie Windows dla wszystkich uż... AllUserInstallAgent	
Agent ochrony dostępu do sieci napagent	
Agent zasad IPsec PolicyAgent	
Aplikacja systemowa modelu COM+ COMSysApp	
Asystent łączności sieciowej NcaSvc	
Automatyczna konfiguracja sieci przewodowej dot3svc	
Bufor wydruku Spooler	
Centrum dystrybucji kluczy Kerberos Kdc	
DFS Namespace Dfs	

Zastosuj do usług o tej krótkiej nazwie (przykład: eventlog):

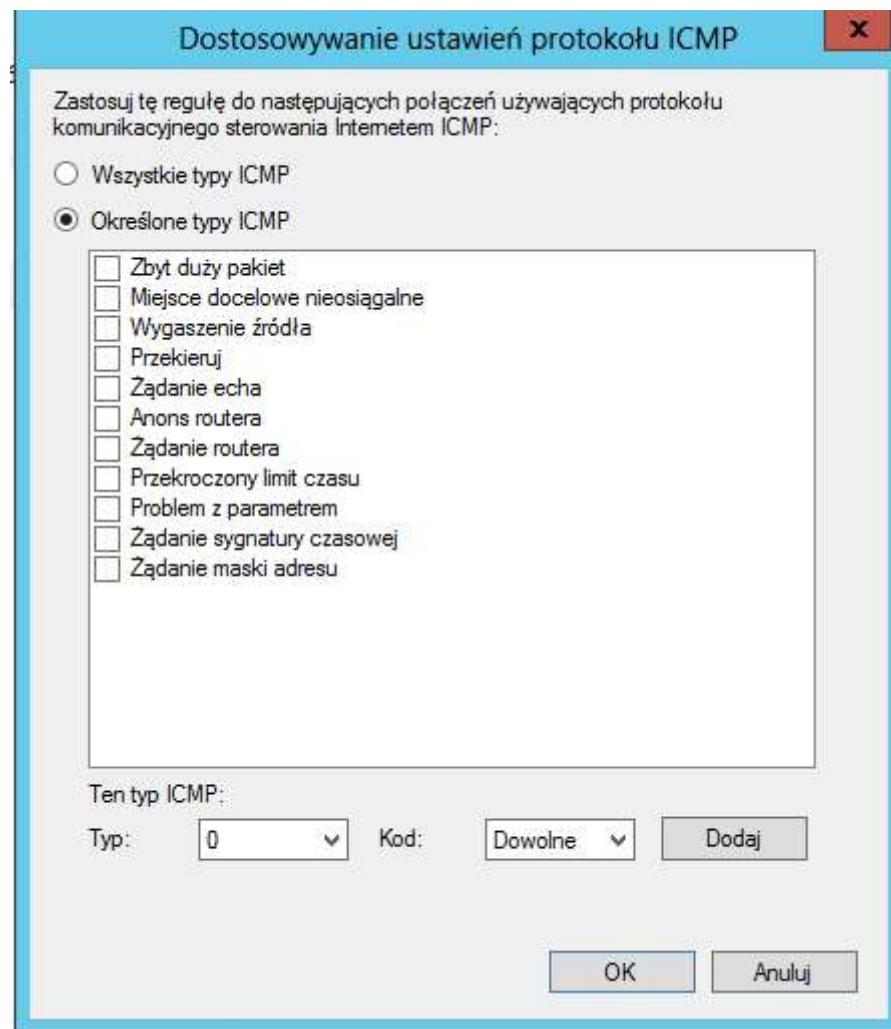
OK | Anuluj

< Wstecz | Dalej > | Anuluj

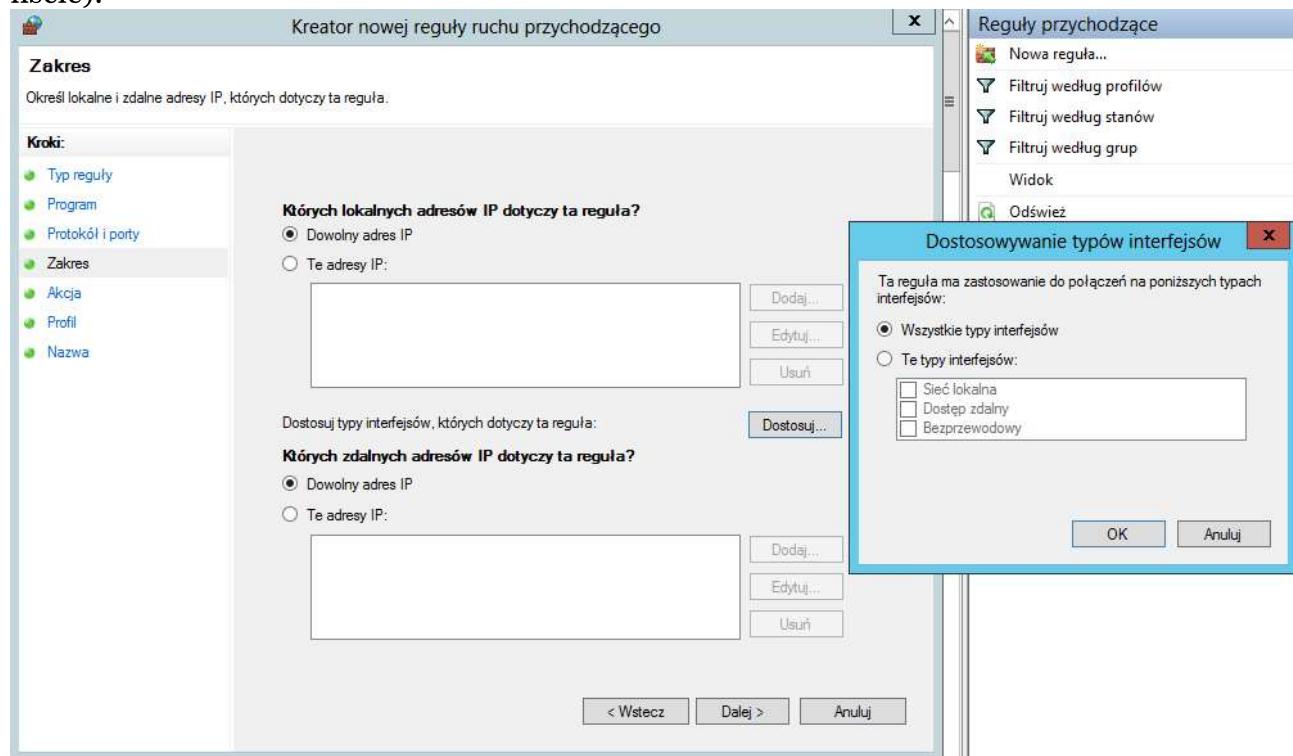
Na powyższym zrzucie możemy wybrać dla którego programu chcemy utworzyć regułę. Domyślnie wybrane są wszystkie dostępne w systemie programy. Można wskazać konkretny program (ściezka bezwzględna lub względna, jednak trzeba wskazać plik exe). Można ponadto wskazać konkretne usługi, które będą mogły korzystać z reguły (domyślnie mogą korzystać wszystkie usługi). Wprowadzanie usług może odbywać się poprzez wskazanie konkretnej z listy lub poprzez jej skróconą nazwę.



Następny zrzut pozwala wybrać protokół, dla którego będziemy ustanawiać połączenia. Protokół wybiera się z listy Typ protokołu. Następnie można wybrać numer protokołu (tylko w wypadku Niestandardowy – w innych jego numer sam się ustanawia), Port lokalny na którym będzie wyzwalana reguła (można wybrać wszystkie porty, tylko wskazane, przekierowanie krawędzi bądź odtwarzania), Port zdalny (jak wyżej lecz można wybierać tylko pomiędzy wszystkie porty/określone porty). Jeżeli wybieramy opcję określone porty to w następnym polu istnieje możliwość wpisania konkretnych portów dla których reguła ma obowiązywać – można podać tylko jeden, zakres, lub wymienić konkretne po przecinku. Ustawienia protokołu komunikacyjnego sterowania Internetem (ICMP) można dostosować jedynie w przypadku wybranych protokołów (np. ICMPv4, ICMPv6).

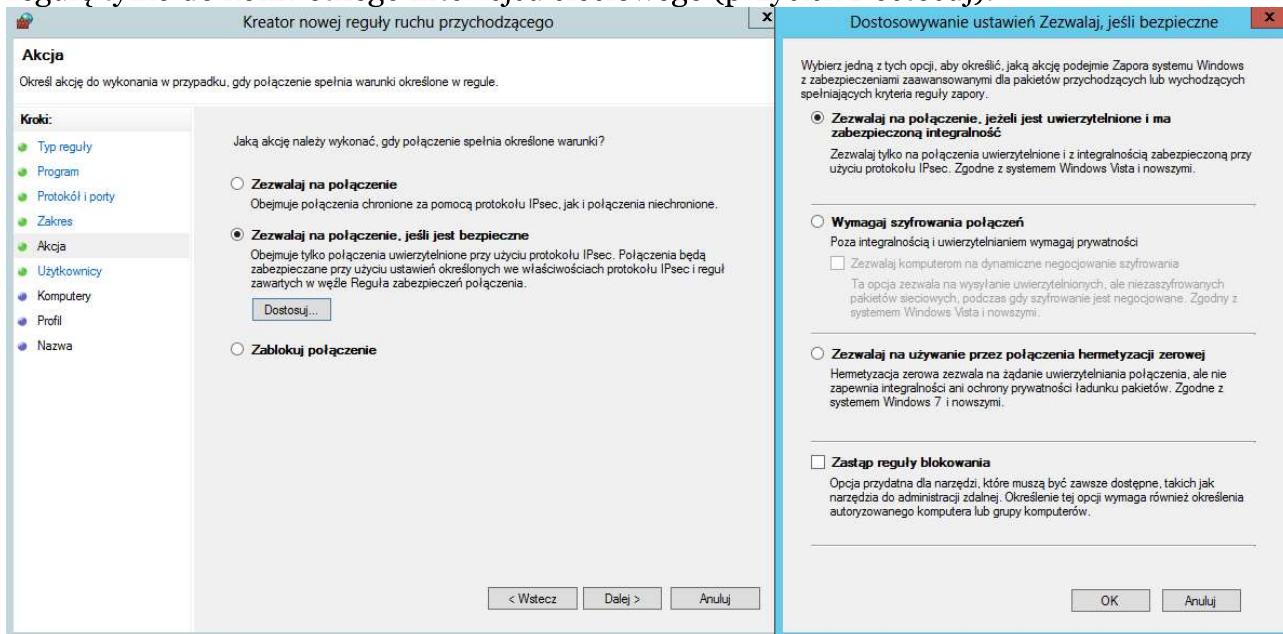


Okno dostosowania ustawień protokołu ICMP (można dodawać inne niż wymienione na liście).

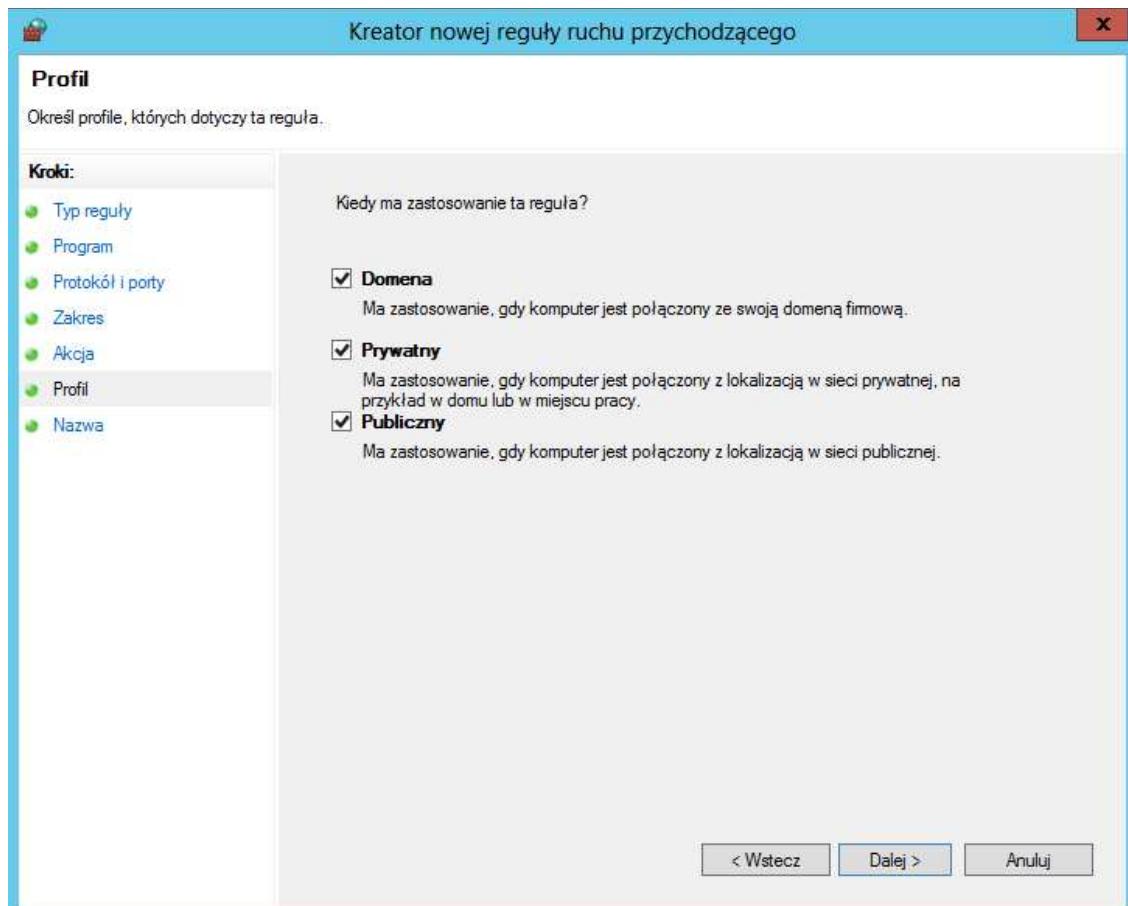


W zakresie podajemy adres/adresy komputerów lokalnych/zdalnych, które mogą korzystać

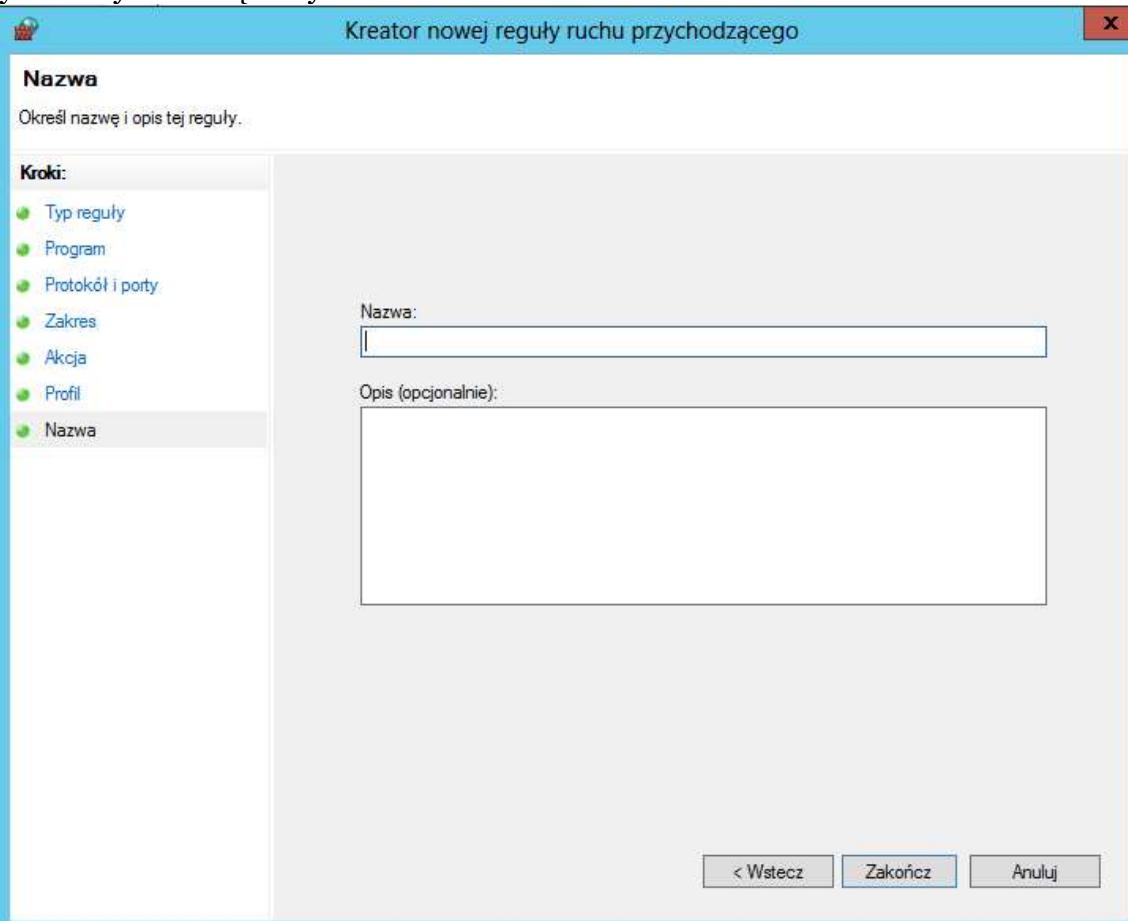
z reguły (domyślnie mogą korzystać wszystkie adresy). Dodatkowo można ograniczyć regułę tylko do konkretnego interfejsu sieciowego (przycisk Dostosuj).



W Akcji wybieramy co dana reguła ma powodować. Do wyboru jest Zezwolenie na połączenie (domyślnie) – ruch dla tej reguły będzie przekazywany. Druga opcja to Zablokuj połączenie – reguła ma blokować ruch, który będzie spełniał wcześniej postawione kryteria. Opcja Zezwala na połączenie, jeśli jest bezpieczne ma zastosowanie przy protokole IPSec. Wymusza ona korzystanie z połączenia szyfrowanego. Po kliknięciu Dostosuj... można wybrać stopień bezpieczeństwa pakietów. Domyślnie jest ustalone połączenie poprzez protokół IPSec. Opcja Wymagaj szyfrowania połączeń pozwala wymuszać, oprócz samej autoryzacji IPSec, także szyfrowanie danych. Zezwala na używanie przez połączenia hermetyzacji zerowej pozwala na używanie NIEZABEZPIECZONYCH danych wewnętrz ZABEZPIECZONEGO połączenia. Opcja silnie niezalecana (jedynie dla trybu zgodności ze starymi/niekompatybilnymi systemami). Zastąp reguły blokowania jest potrzebne jedynie w przypadku gdy zachodzi obawa, że reguła może zablokować podstawowe narzędzia administracji (np. pulpit zdalny lub administrację zdальną).



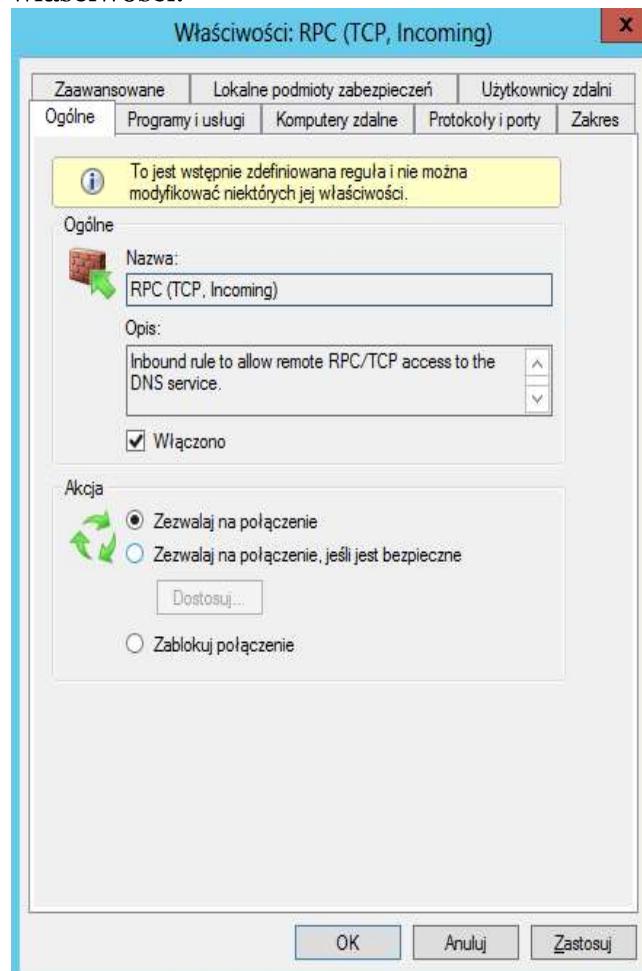
W kolejnym etapie wybiera się, dla którego profilu ma mieć zastosowanie tworzona reguła. Domyślnie wybrane są wszystkie.



Na koniec podajemy nazwę reguły (musi być unikatowa) oraz opis (opcjonalny; warto go

dodać by pamiętać do czego była tworzona reguła).

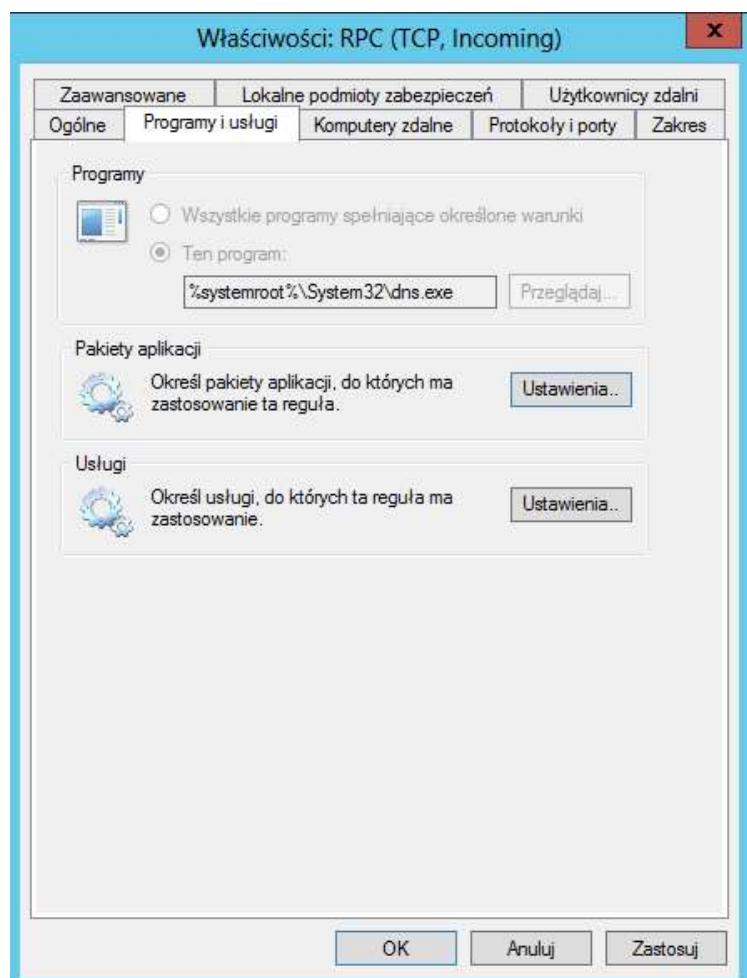
Każda z utworzonych reguł można przejrzeć i modyfikować w dowolnym czasie. Wystarczy zaznaczyć ją na liście w regułach przychodzących/wychodzących i wybrać jej właściwości.

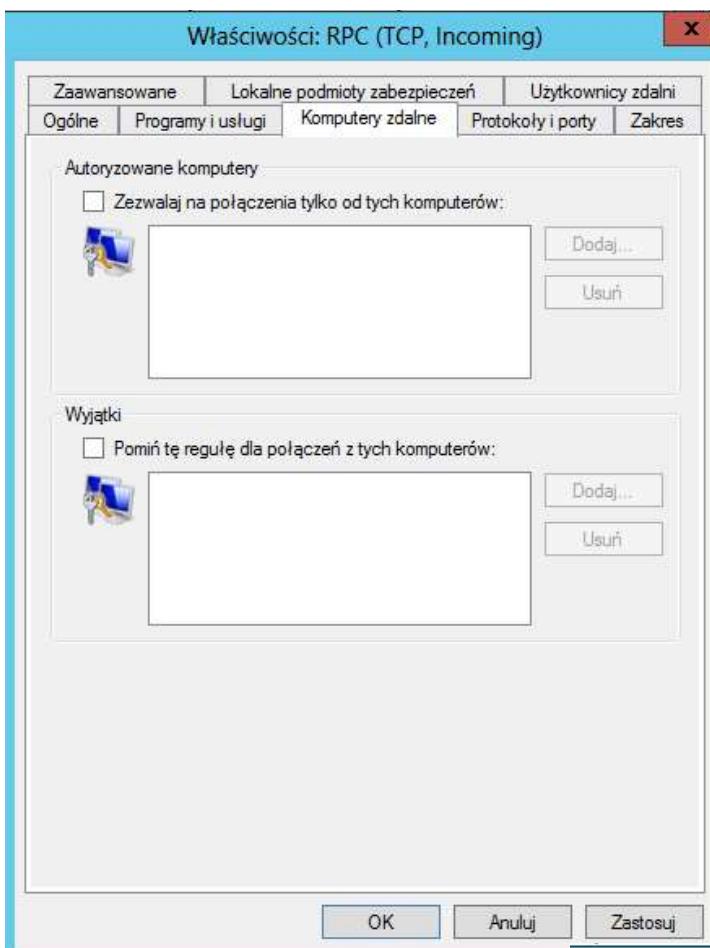


Zakładka Programy i usługi pozwala na określenie programów, dla których reguła jest stosowana. Można także ustalić Pakiety aplikacji oraz Usługi, dla których reguła działa.

Zakładka Ogólne zawiera nazwę reguły (najczęściej nie podlega zmianie), Opis (nie podlega zmianie w regułach wbudowanych), Włączono określa, czy reguła jest włączona, natomiast grupa Akcja pozwala na określenie co ma robić wskazana reguła (ustawienia identyczne jak w fazie projektu).

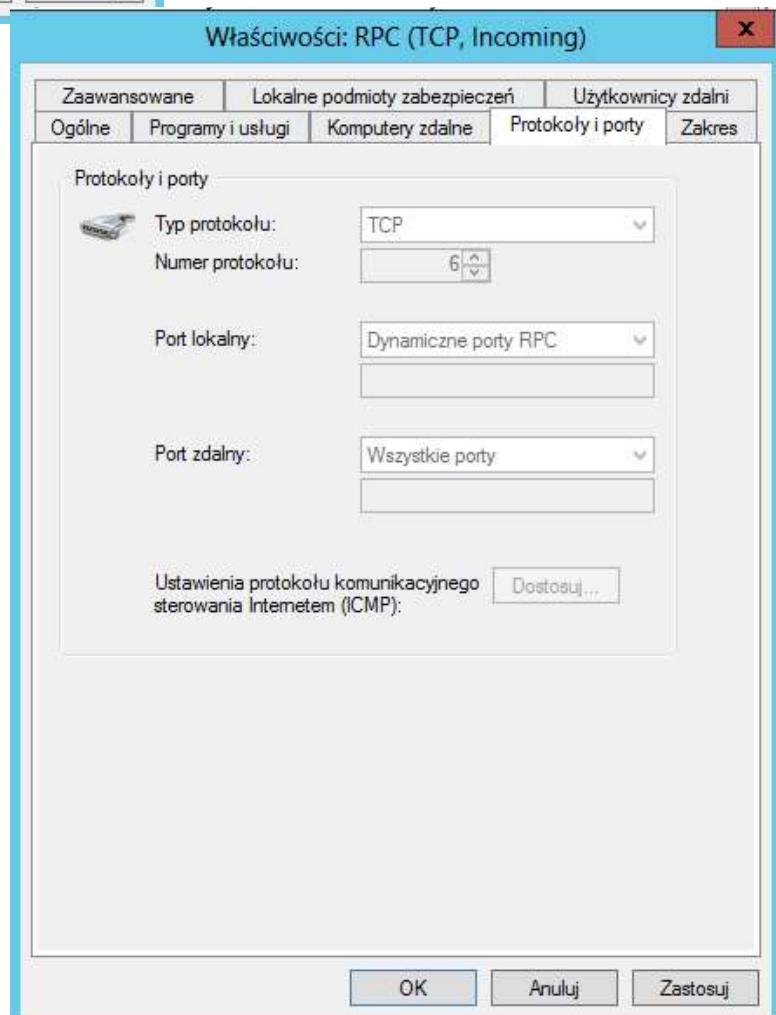
Proszę zauważać, że system daje informacje o tym, iż reguła jest wstępnie zdefiniowana przez dostawcę (Microsoft) i niektórych jej opcji nie można zmienić.

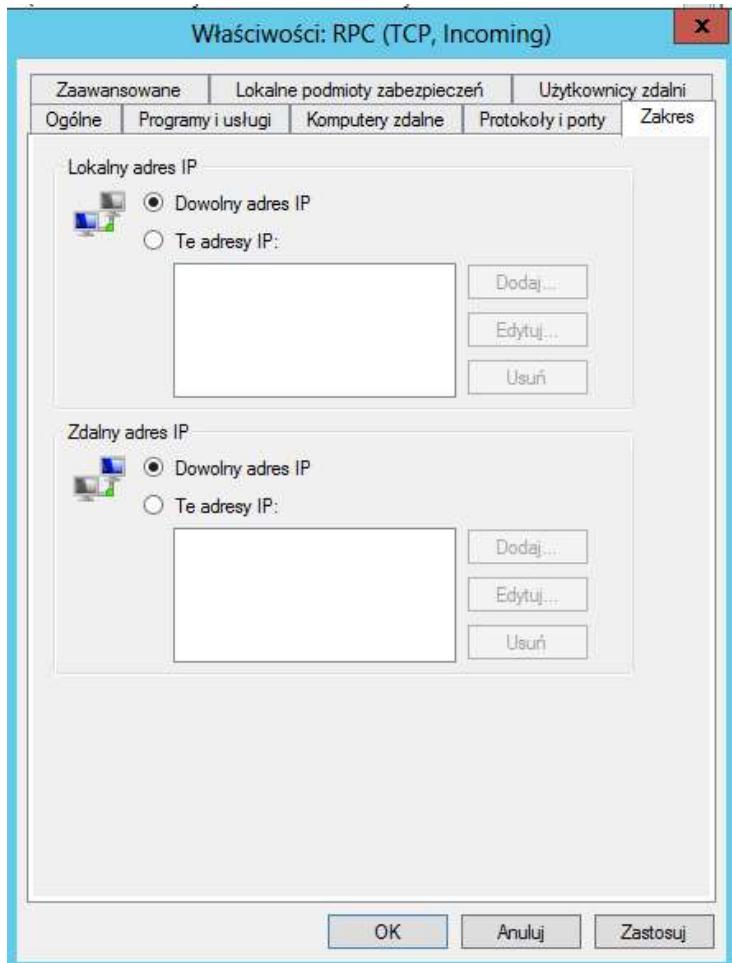




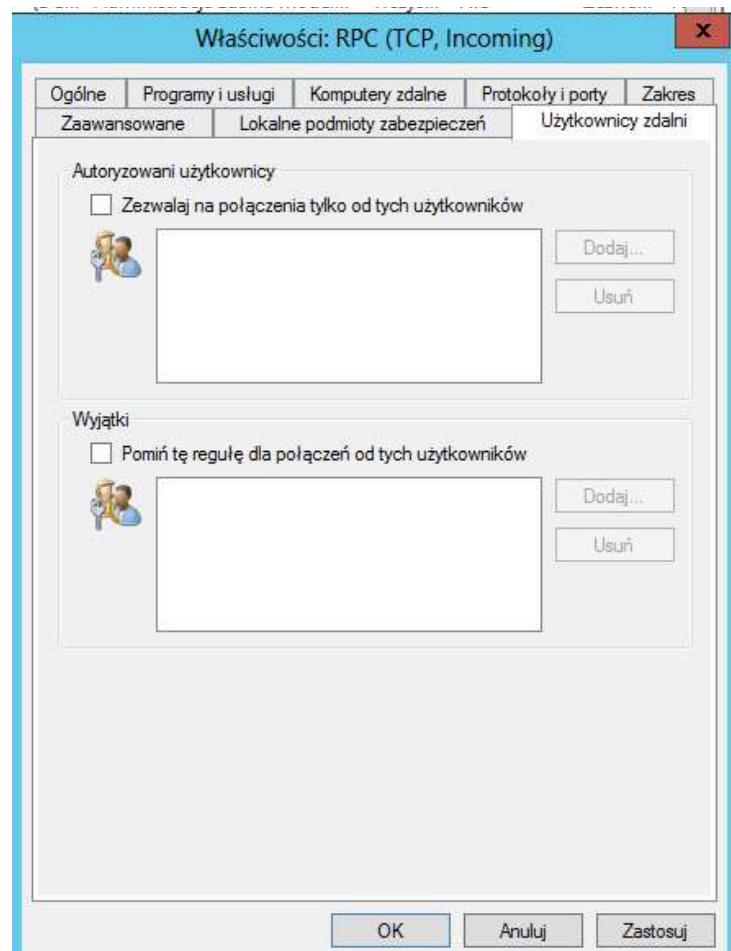
Na tej karcie można dodawać autoryzowane komputery (które mogą korzystać z reguły), a które nie mogą (Wyjątki).

Karta pozwala na zmianę typu obsługiwanej protokołu. W tym wypadku zmiana jest niemożliwa (reguła dodana przez system).



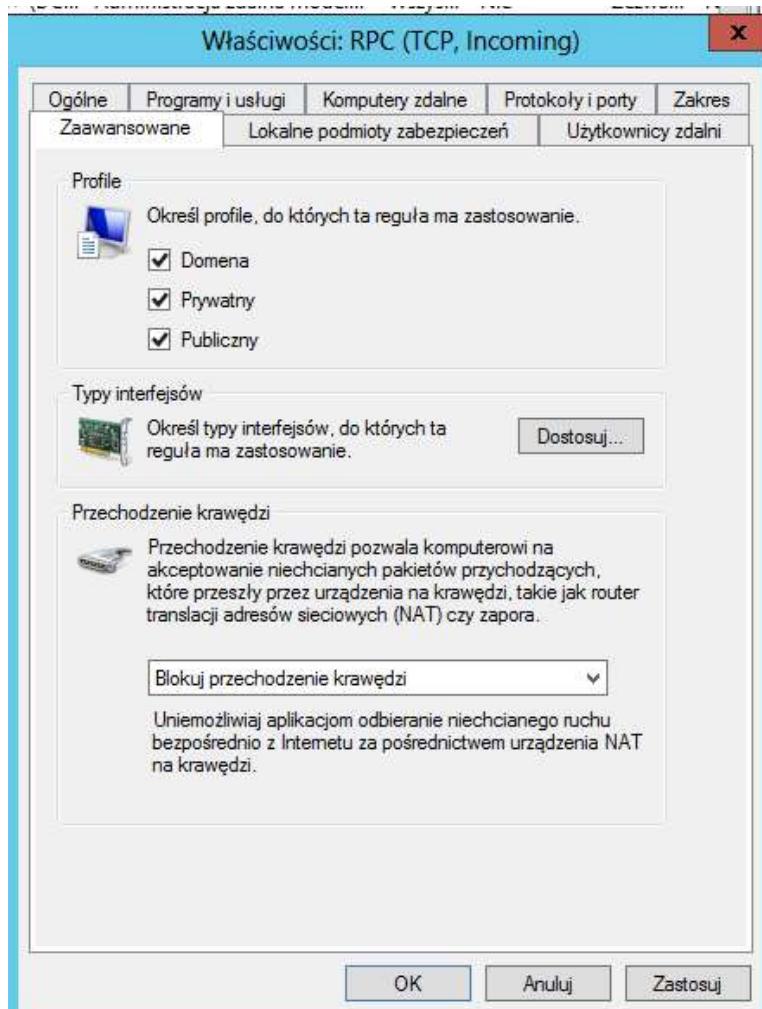


Możliwość zmiany zakresu adresów IP, które będą miały dostęp do reguły/które będą pozbawione dostępu do niej.



Pozwala na użytkowanie tej reguły przez określonych użytkowników/pominięcie wskazanych użytkowników.

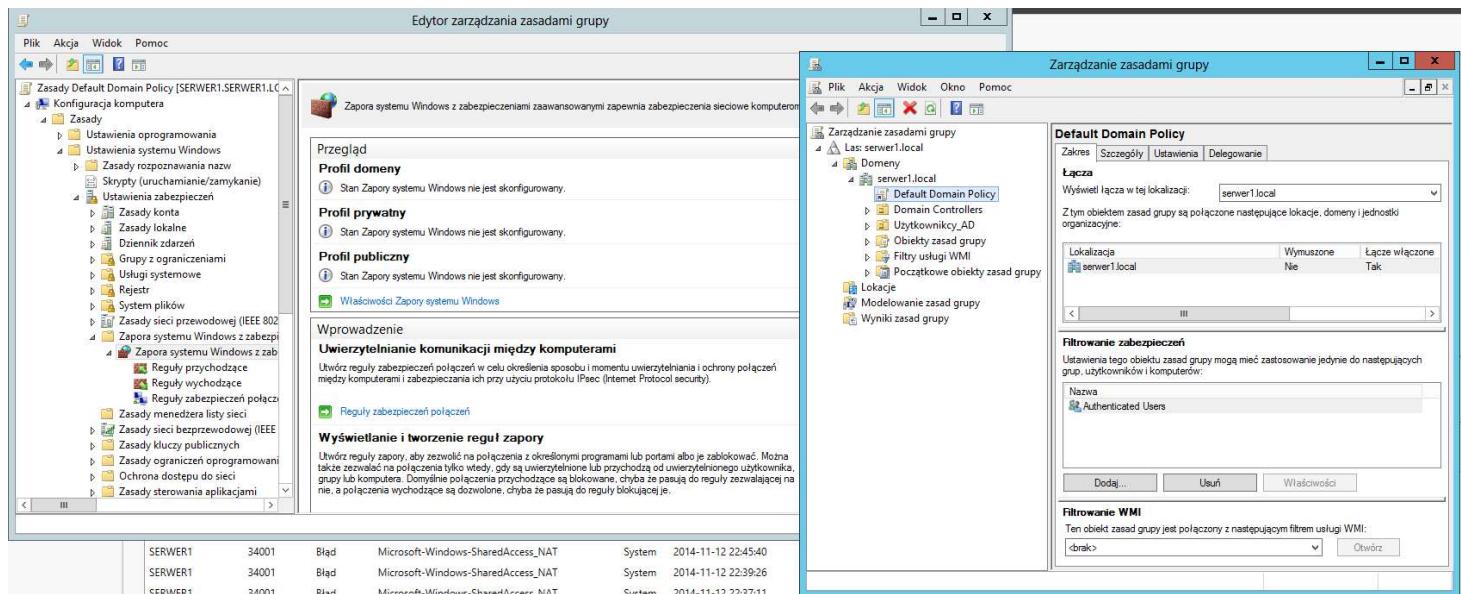
Identycznie wygląda zakładka Lokalne podmioty zabezpieczeń (tylko do połączeń lokalnych!!)



Ostatnia zakładka pozwala na określenie Profili, interfejsów oraz Przechodzenia krawędzi dla pakietów z tej reguły.

UWAGA!

Proszę pamiętać, że wszystkie dotychczas przedstawione ustawienia dotyczą tylko LOKALNEGO SERWERA/kont Administracyjnych na nim. Zasady te nie są dystrybuowane dla poszczególnych zasad zabezpieczeń w domenie! Aby zmieniać zasady zabezpieczeń w domenie (wedle zasad grup) trzeba przejść do Zarządzania Zasadami grupy, wybrać zasadę, dla której chcemy dodać nowe reguły, wybrać jej edycję, a następnie, w nowym oknie, należy wybrać Konfiguracja komputera->Zasady->Ustawienia systemu Windows->Zapora systemu Windows z zabezpieczeniami zaawansowanymi. Tutaj można zaimportować wszystkie zasady z komputera (serwera), można też tworzyć nowe, własne. Sposób ten jest o tyle wygodny, że zwalnia administratora systemu z konfiguracji każdego stanowiska z osobna.



ZADANIA:

1. Proszę utworzyć 10 reguł dla różnych programów (proszę poszukać programy działające w sieci lokalnej, które wymagają różnego typu reguł (np. serwer WWW, serwer poczty itd.). Proszę przetestować działanie programów bez reguł i z regułami (można także wykorzystać usługi/reguły/role systemowe).
2. Proszę spróbować wyłączać/włączać poszczególne reguły wbudowane w w zaporę. Należy przetestować jak ich wyeliminowanie wpływa na działanie systemu (serwerowego i klienckiego). Proszę przetestować minimum 10 reguł (w tym reguły Active Directory i pokrewne).
3. Proszę przetestować działanie Profili. Szczególnie włączanie/wyłączanie ruchu wchodzącego/wychodzącego.