

Uniwersytet Morski w Gdyni

przedmiot:

## **Narzędzia Informatyczne**

### **Ćw. 8 Wprowadzenie do zapory Windows**

#### **1. Cel ćwiczenia**

Celem ćwiczenia jest przedstawienie sposobów prawidłowej konfiguracji zapory systemu Windows. W ćwiczeniu przedstawiono także metody testowania ustanowionych reguł.

#### **2. Wprowadzenie**

System operacyjny Windows posiada programowy firewall (Zapora sieciowa systemu Windows – nazwa zależna od wersji systemu operacyjnego). Zadaniem firewall'a jest blokowanie niepożądanego ruchu sieciowego. Z zagadnieniem ruchu sieciowego związane są następujące definicje:

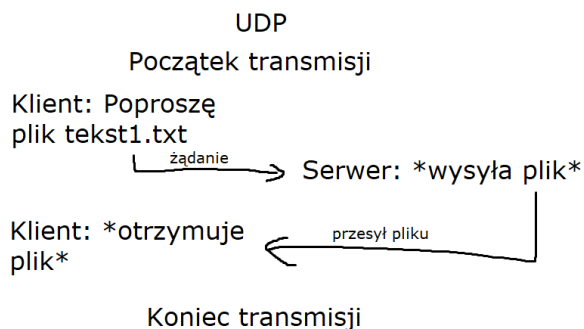
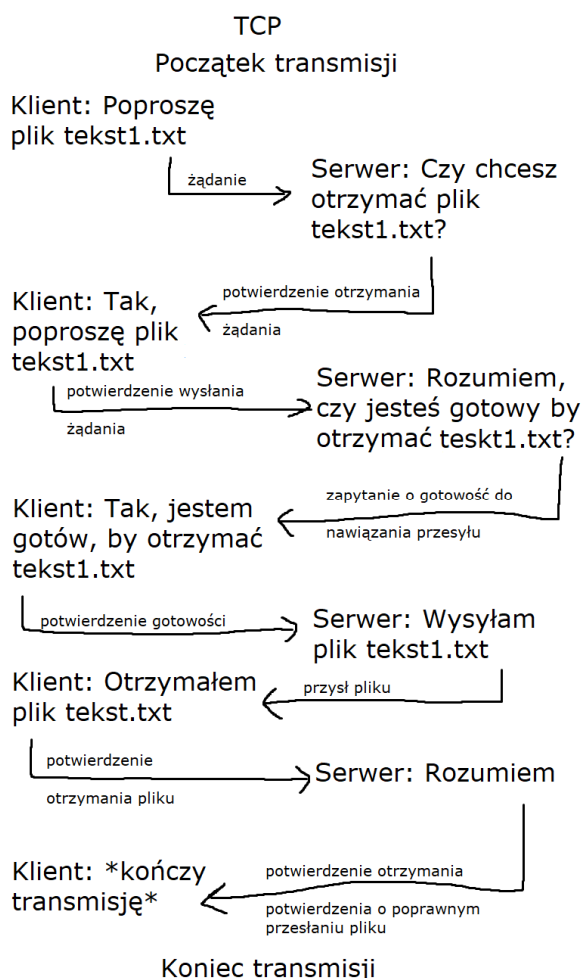
- Firewall – jest to program (lub funkcja systemu operacyjnego) filtrująca przychodzące pakiety, odrzucając te niepożądane. Może także identyfikować użytkowników stosując certyfikaty. Poprawnie skonfigurowany firewall powinien odrzucić wszystkie pakiety służące przeprowadzeniu znanych ataków.
- Adres IP – jest to logiczny adres komputera, serwera lub urządzenia sieciowego w sieci. Służy on do poprawnej komunikacji pomiędzy urządzeniami. Można to rozumieć jako osobisty adres każdego urządzenia na którym pracować będzie komunikacja sieciowa.
- Port sieciowy – jest to numer identyfikujący konkretne połączenie pomiędzy dwoma urządzeniami sieciowymi. Zakres dostępnych portów do wykorzystania to 0 – 65535. Porty można rozumieć jako „furtki” otwierane na rzecz wymiany danych pomiędzy dwoma komputerami (lub dowolnymi urządzeniami korzystającymi ze standardu TCP/IP). Porty służą do dokonywania połączeń w konkretnym, określonym celu, np. port 53 służy do komunikacji pomiędzy urządzeniami związanej z rozwiązywaniem nazw IP (DNS). Stawiając jakąkolwiek sieciową usługę na serwerze musimy określić na jakich portach będzie ona funkcjonować w sieci (najczęściej gotowe usługi mają z góry określone porty na jakich pracują), i to na tych portach komputery klienckie będą do tej usługi otrzymywać dostęp.

Różne usługi mogą korzystać z tych samych portów jeśli korzystają z innych protokołów (TCP lub UDP), jeśli będą korzystać z tego samego protokołu wywołają konflikt i uszkodzą wszelką komunikację na tym porcie.

- Gniazdo – jest to reprezentacja punktu końcowego połączenia. Gniazdo przyjmuje postać IP:Port (np. 192.168.0.20:8823). Podając gniazdo umożliwiamy połączenie się z komputerem (identyfikowanym przez adres IP z gniazda) i nawiązanie komunikacji na określonym porcie (również podanym w gnieździe).
- ICMP – jest to protokół sieciowy (warstwa 3) służący do diagnostyki sieci i trasowania (wyznaczania trasy dla pakietu). Głównymi programami korzystającymi z protokołu ICMP są ping i traceroute (programy systemu Windows lub ich odpowiedniki w innych OS).
- TCP – jest to protokół klient-serwer służący do przesyłania pakietów. Klient rozpoczyna transmisję poprzez wysłanie żądania do serwera, następnie serwer odpowiada przesyłając zażądane dane. Zaletą protokołu TCP,

jest to, że ustanowienie połączenia musi zostać potwierdzone przez obie strony, przesłanie i odebranie pakietu także – oznacza to, że nie ma możliwości, by jakiś pakiet zażądany został nieprzesłany (jeśli nie otrzymano potwierdzenia odebrania pakietu operacja zostaje powtórzona), żadne żądanie nie zostanie pominięte (jeśli serwer nie odeśle potwierdzenia otrzymania żądania, klient wyśle je ponownie). Każda operacja jest potwierdzana, dzięki czemu wszystkie pakiety zostają dostarczone w całości, z zachowaniem kolejności i bez duplikatów. Niestety każde potwierdzenie trwa określoną ilość czasu i dostarczenie pakietu do klienta jest, o czas spędzony na potwierdzenia, opóźnione. Protokół ten śledzi transmisję, więc nie ma żadnego narzutu (serwer przesyła tylko i wyłącznie pakiet, o który nie został poproszony itp.), transmisja zostaje rozpoczęta i zakończona w konkretnym czasie.

- UDP – jest to protokół bezpołączeniowy. Oznacza to, że nie śledzi transmisji, transmisja nie ma określonego początku i końca. W odróżnieniu od TCP, UDP nie sprawdza poprawności przesłania żądań i odpowiedzi. Nie ma też ściśle określonej zasady jedno żądanie to jedna odpowiedź. Klient wysyła serwerowi żądanie, jeśli to dotrze, serwer jako odpowiedź od razu wysyła żądane dane. Oznacza to, że do klienta dane docierają szybciej niż w przypadku TCP, ale jeśli żądanie nie dotrze do serwera lub dotrze uszkodzone, klient nie otrzyma danych. Logika działania UDP pozwala także na wysyłanie do wielu klientów na raz (multicast). UDP wykorzystuje się w przypadkach, gdzie dane do klienta muszą dotrzeć jak najszybciej (np. wideokonferencje, strumieniowanie muzyki, internetowe gry), a utrata kilku pakietów nie powoduje niezdadności danych do użytku (np. chwilowo stracimy obraz wideokonferencji, lub doświadczymy tzw. laga gry internetowej – nie powoduje to nieprzydatności całej transmisji). W przypadku UDP do korekcji błędów wykorzystywane są pozostałe warstwy modelu OSI.

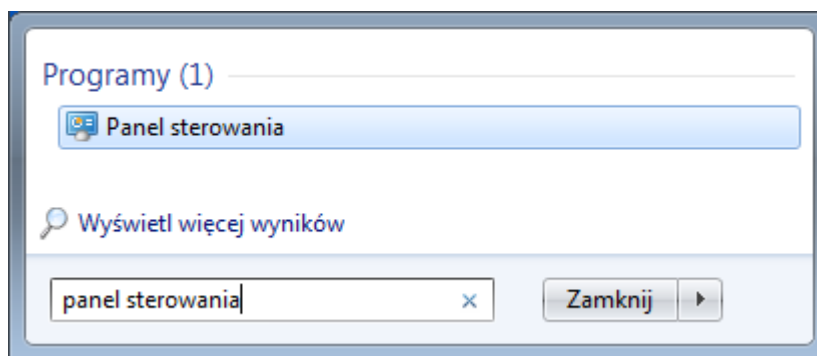


### 3. Przykłady

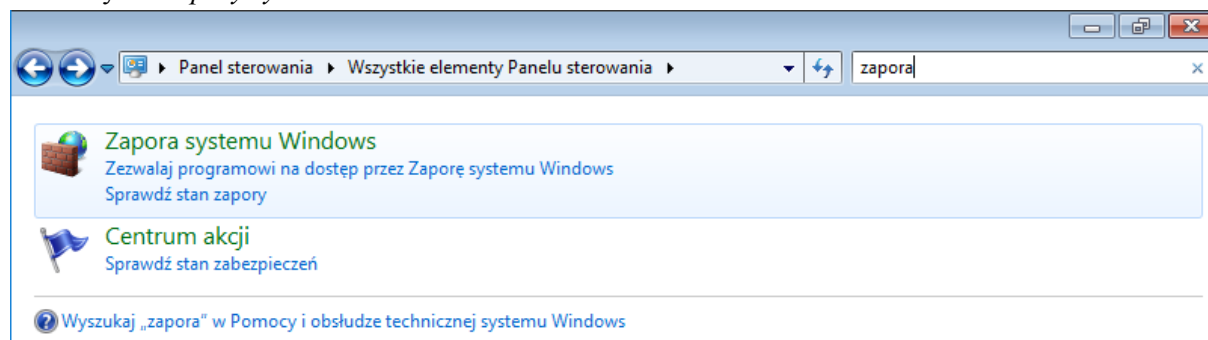
Poniższa instrukcja przedstawia przykładową konfigurację wirtualnych maszyn prezentującą konfigurację infrastruktury i zapory sieciowej.

#### 3.1. Przykład konfiguracji zapory sieciowej

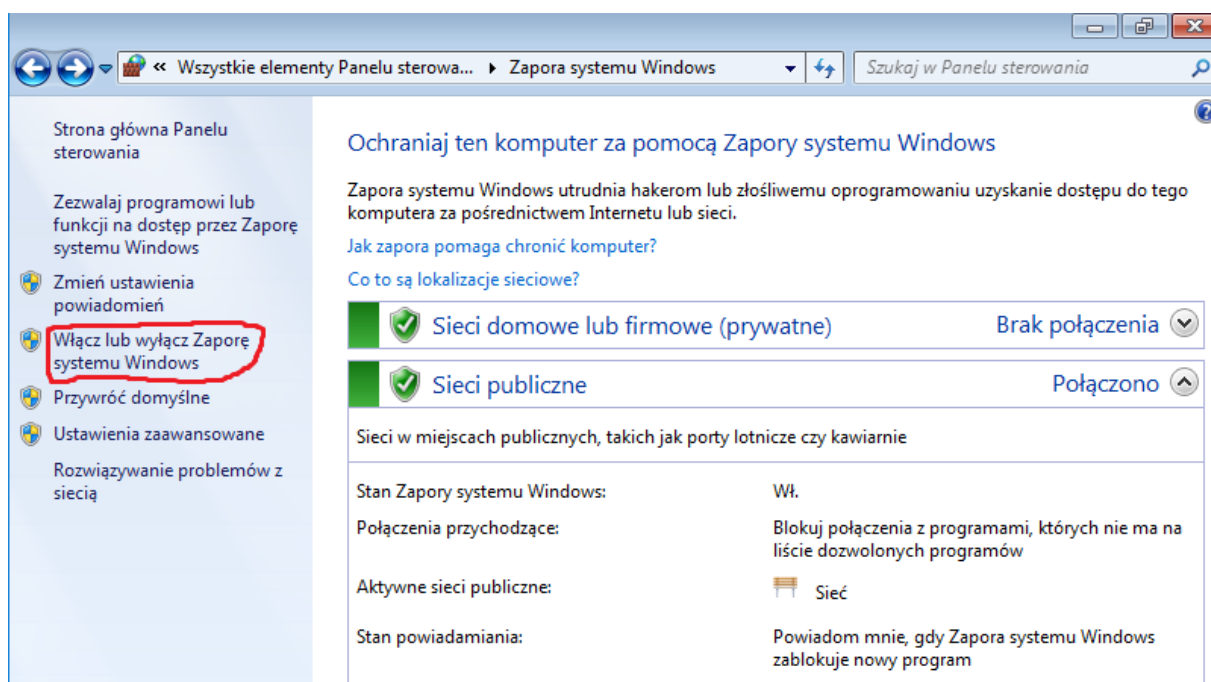
W pierwszej kolejności konfigurujemy kartę sieciową maszyny wirtualnej z systemem Windows, tak aby posiadała dostęp do Internetu (*NAT* lub *Mostkowana karta sieciowa*). Następnie uruchamiamy maszynę i przechodzimy do *Panelu sterowania*.



Przechodzimy do *Zapory systemu Windows*



Ukaże nam się krótkie podsumowanie, do jakich sieci jesteśmy podłączeni (w tym przypadku do sieci o nazwie *Sieć* w lokalizacji publicznej). Klikając *Włącz lub Wyłącz Zaporę systemu Windows* przejdziemy do ustawień rygorystyki zapory.



Uzyskujemy możliwość konfiguracji zapory oddzielnie dla różnych typów lokalizacji (prywatnych – domowa/firmowa i publicznych), mamy możliwość całkowitego zablokowania przychodzącego ruchu sieciowego dla wybranej lokalizacji zaznaczając „*Blokuj wszystkie połączenia przychodzące...*” oraz możemy włączyć i wyłączyć zaporę. Wyłączanie zapory sieciowej nie jest zalecane, lecz czasami opcja ta jest bardzo użyteczna. Przykładem może być tworzenie i konfigurowanie infrastruktury sieciowej oraz usług serwerowych – zdarza się, że postawimy usługę serwerową lecz komputery klienckie nie są w stanie z nią połączyć. Bardzo często problemem jest nieodpowiednio skonfigurowana zapora sieciowa, więc zanim zaczniemy przekonfigurowywać usługę i próbować poprawiać instalację warto wyłączyć chwilowo zaporę (oczywiście jeśli chwilowe wyłączenie zapory nie naraża urządzenia na niebezpieczeństwo – zazwyczaj jednak jeśli wprowadzamy i testujemy usługę robimy to w środowisku izolowanym, gdzie wyłączenie zapory nie wprowadza żadnego zagrożenia) i sprawdzić czy w takim przypadku usługa działa. Jeśli tak to oznacza, że wszystko zrobiliśmy poprawnie, pozostaje jedynie włączyć zaporę sieciową i wprowadzić odpowiednie reguły.



## Dostosowywanie ustawień dla każdego typu sieci

Możesz zmodyfikować ustawienia zapory dla każdego używanego typu lokalizacji sieciowej.

Co to są lokalizacje sieciowe?

Ustawienia lokalizacji sieci domowej lub firmowej (prywatnej)



☒ Włącz Zaporę systemu Windows

☐ Blokuj wszystkie połączenia przychodzące łącznie z programami znajdującymi się na liście dozwolonych programów

☒ Powiadom mnie, gdy Zapora systemu Windows zablokuje nowy program



☐ Wyłącz Zaporę systemu Windows (niezalecane)

Ustawienia lokalizacji sieci publicznej



☒ Włącz Zaporę systemu Windows

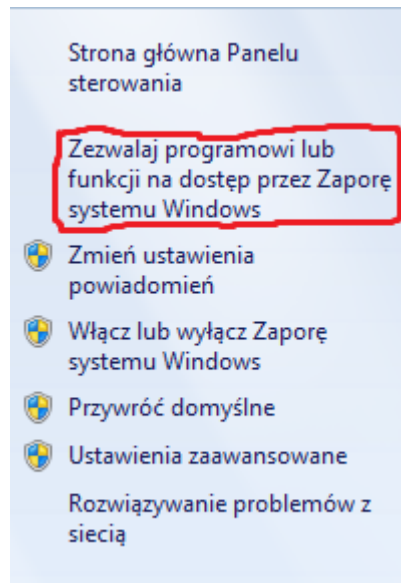
☐ Blokuj wszystkie połączenia przychodzące łącznie z programami znajdującymi się na liście dozwolonych programów

☒ Powiadom mnie, gdy Zapora systemu Windows zablokuje nowy program



☐ Wyłącz Zaporę systemu Windows (niezalecane)

Zapora systemu Windows pozwala na odblokowywanie dostępu do sieci programom poprzez narzędzie „Zezwalaj programowi...”, pozwala ono automatycznie zdefiniować regułę dla pliku wykonywalnego dla wybranej lokalizacji sieciowej.




Ukaże się nam lista programów – wyjątków, które posiadają własne reguły zapory.

## Udostępniaj programom możliwość komunikacji za pośrednictwem Zapory systemu Windows

Aby dodać, zmienić lub usunąć dozwolone programy i porty, kliknij opcję **Zmień ustawienia**.

Jakie ryzyko wiąże się z zezwoleniem na komunikację programu?

 **Zmień ustawienia**

**Dozwolone programy i funkcje:**

Nazwa	Domowe/firmowe (prywatne)	Publiczne
<input type="checkbox"/> Beprzewodowe urządzenia przenośne	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache — klient hostowanej pamięci podręc...	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache — odnajdowanie węzłów równorzędn...	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache — pobieranie zawartości (używa prot...	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache — serwer hostowanej pamięci podręc...	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Dzienniki wydajności i alerty	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Funkcja Podstawa współpracy w sieci równorzędn...	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Grupa domowa	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Instrumentacja zarządzania Windows (WMI)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Koordynator transakcji rozproszonych	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Odnajdowanie sieci	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Podstawowe operacje sieciowe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

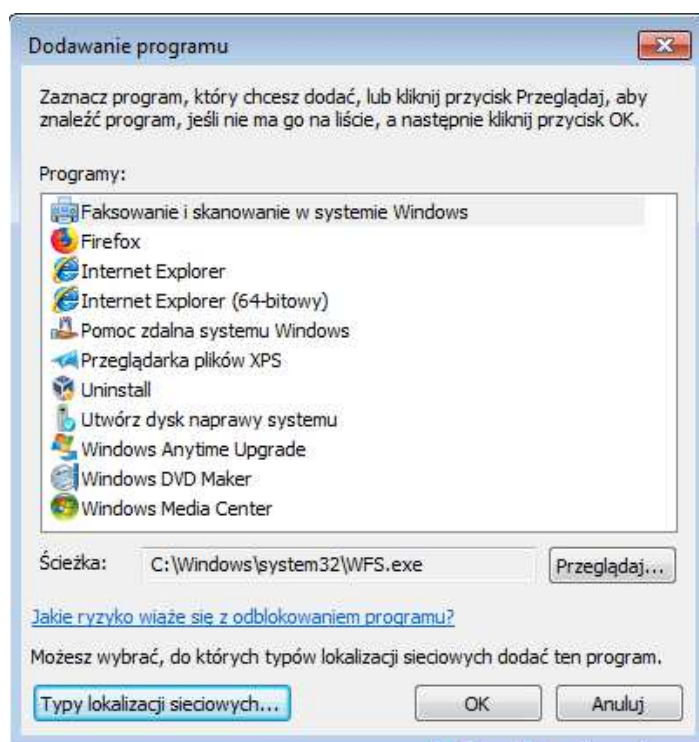
**Szczegóły...** **Usuń**

**Zezwalaj na dostęp innego programu...**

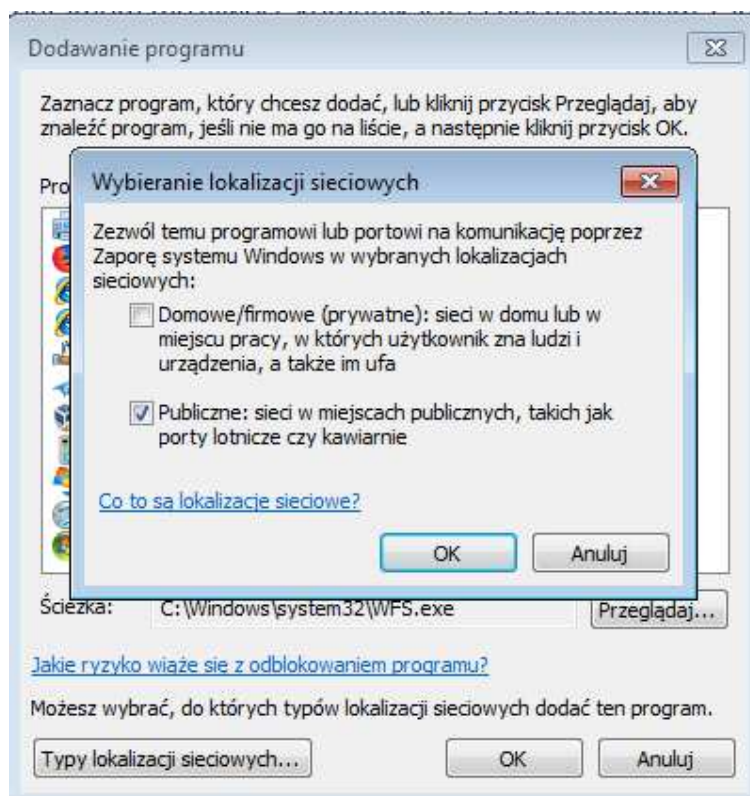
**OK** **Anuluj**

Jak widać, większość reguł nie jest aktywna (checkbox przy ich nazwie jest odznaczony). Możemy łatwo edytować reguły (m.in. zmieniać lokalizację w której są aktywne), poprzez naciśnięcie *Zmień ustawienia*, a następnie zaznaczanie checkbox'ów lokalizacji. Możemy również zdefiniować wyjątek dla programu spoza listy, aby tego dokonać klikamy *Zezwalaj na dostęp innego programu...*

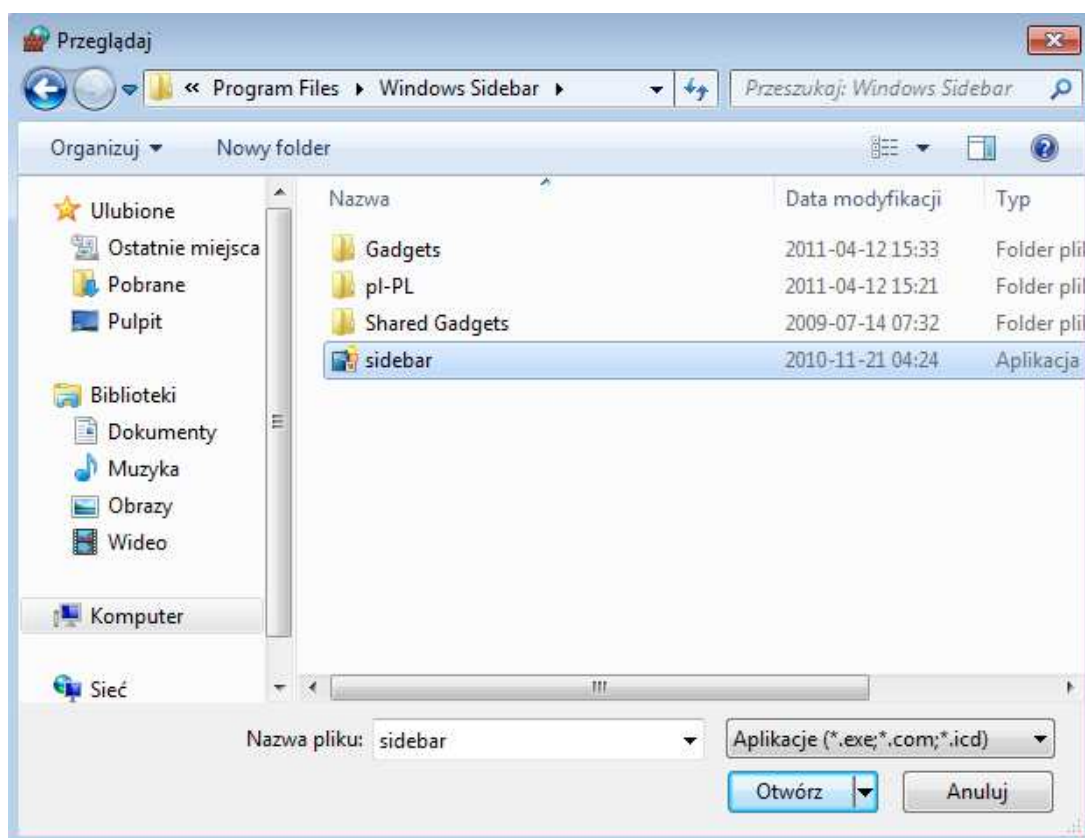




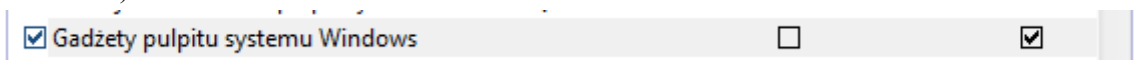
Został uruchomiony kreator *Dodawania programu*, klikając *Typy lokalizacji sieciowych* możemy zmienić jakich lokalizacji będzie dotyczyć nowy wyjątek.



Klikając *Przeglądaj* możemy wybrać plik wykonywalny, którego wyjątek będzie dotyczył. Wybierzmy więc dowolny plik wykonywalny.



Następnie zatwierdzamy wyjątek. Do listy zostanie dodany nowy program (w tym przypadku *Gadżety pulpitu systemu Windows*)



Wyjątek jest zbędny – stworzony został jedynie jako przykład, więc możemy go wyłączyć lub usunąć.

Aby wyłączyć wyjątek wystarczy odznaczyć checkbox. (wyłączenie wyjątku nie powoduje jego usunięcia, lecz zablokowanie dostępu programu do sieci)



Aby wyjątek usunąć należy go wybrać i kliknąć *Usun*.



Dozwolone programy i funkcje:

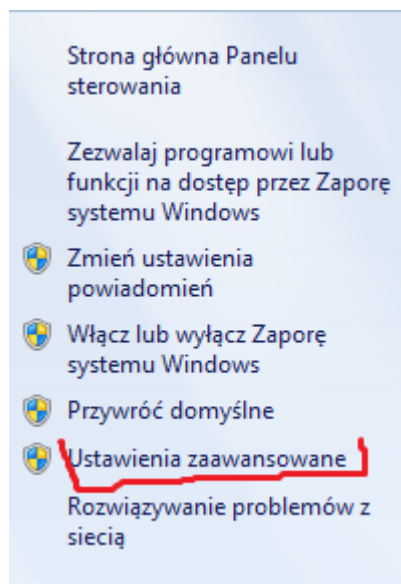
Nazwa	Domowe/firmowe (prywatne)	Publiczne
<input checked="" type="checkbox"/> Gadżety pulpitu systemu Windows	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Grupa domowa	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Instrumentacja zarządzania Windows (WMI)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Koordynator transakcji rozproszonych	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Odnajdowanie sieci	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Podstawowe operacje sieciowe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Połącz z projektorem sieciowym	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Pomoc zdalna	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Protokół SSTP	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Pulpit zdalny	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Pulpit zdalny — funkcja RemoteFX	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Routing i dostęp zdalny	<input type="checkbox"/>	<input type="checkbox"/>

Szczegóły... **Usuń**

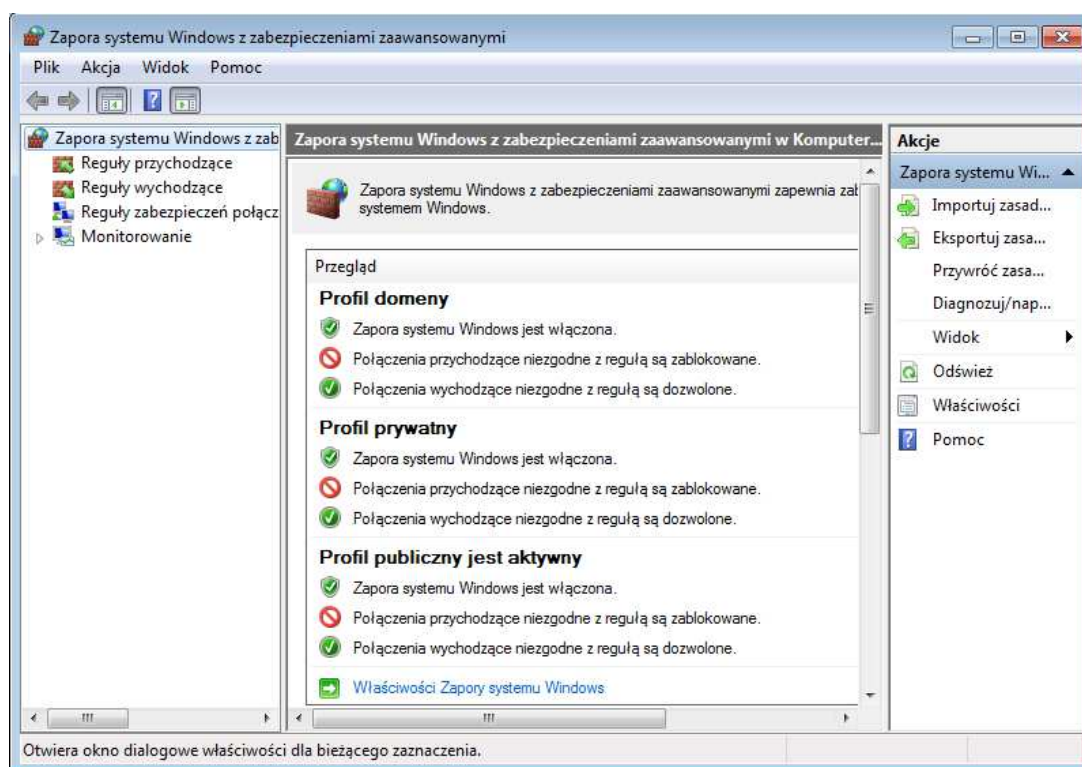
Wyjątek zostanie usunięty, a wraz z nim wszystkie automatycznie utworzone reguły zapory.

Wyjątki są świetnym narzędziem pozwalającym na odblokowywanie zapytań dla wybranych plików wykonywalnych. Nie pozwala jednak na tworzenie reguł złożonych i całkowicie blokuje komunikację, a nie np. tylko wybrane porty.

Prawdziwą siłą *Zapory systemu Windows* jest możliwość definiowania własnych Reguł *przychodzących* i *wychodzących*. Aby tego dokonać musimy przejść do *Ustawień zaawansowanych*.

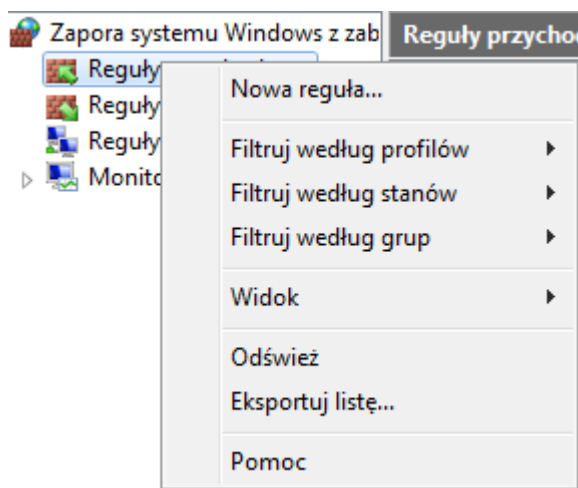


Uruchomiona zostanie *Zapora systemu Windows* z zabezpieczeniami zaawansowanymi.



Definiować możemy *Reguły przychodzące* i *Reguły wychodzące*.

Zdefiniujemy regułę przychodzącą blokującą porty 80, 8080, 443 (dostęp do stron WWW) programowi *Internet Explorer*. Należy nacisnąć na *Reguły przychodzące* prawym przyciskiem myszy i kliknąć *Nowa reguła*.

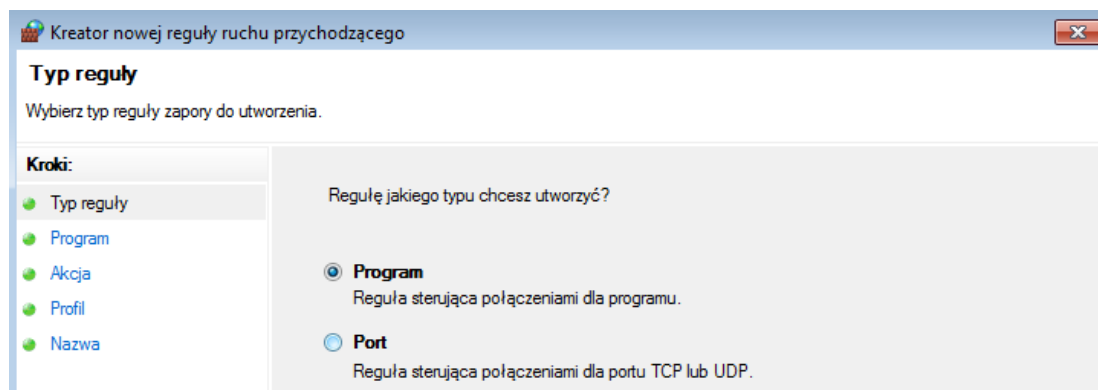


Otwarty zostanie *Kreator nowej reguły ruchu przychodzącego*. W kreatorze możemy stworzyć regułę dla *Programu*, *Portu*, doczepić nową regułę do już *uprzednio zdefiniowanej* lub stworzyć *Regułę niestandardową*. Poszczególne opcje pozwalają na tworzenie reguły o innych zasadach działania:

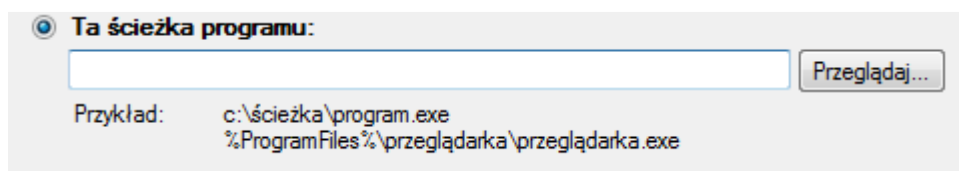
- Program – służy do odblokowywania lub blokowania komunikacji sieciowej programu (odblokowuje lub blokuje komunikację na wszystkich portach)
- Port – służy do odblokowywania lub blokowania komunikacji **WSZYSTKICH** programów na określonych portach (TCP lub UDP)

- Reguła niestandardowa – pozwala na stworzenie reguły powiązanej z konkretnym programem, lecz działającej na wybranych portach i na wybranych adresach IP (możemy zablokować/odblokować komunikację programu na wybranym porcie lub z konkretnym adresem IP)

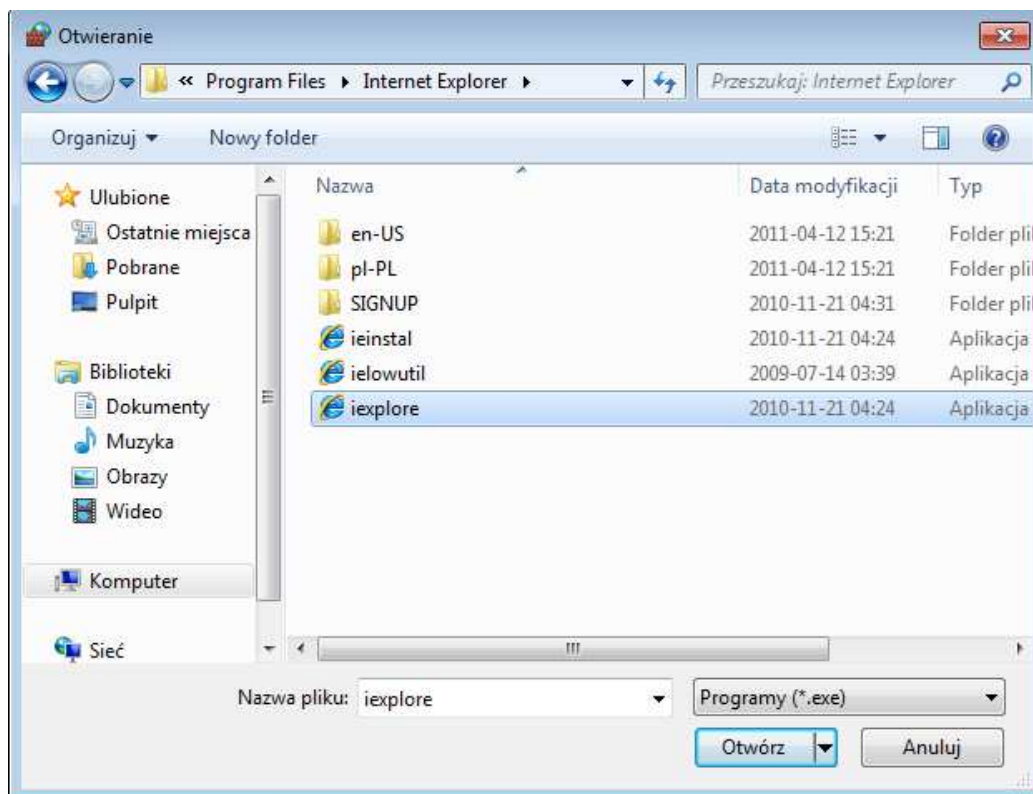
Stworzymy regułę blokującą całkowicie komunikację sieciową dla programu *Internet Explorer*. W tym celu odpowiednim typem reguły będzie *Program*.



Przechodzimy do kolejnego kroku (naciskamy *Dalej*), a następnie zaznaczamy opcję *Ta ścieżka programu:*.



Naciskamy przycisk *Przeglądaj* i wybieramy *C:\Program Files\Internet Explorer\iexplore.exe* i naciskamy *Otwórz*.



Naciskamy *Dalej*, aby przejść do następnego kroku, a następnie wybieramy opcję *Zablokuj połączenie* i klikamy *Dalej*.

☒ **Zablokuj połączenie**

W następnym kroku musimy zdefiniować, w jakiej lokalizacji reguła ma zastosowanie. W tym przypadku zaznaczamy wszystkie i klikamy *Dalej*.

Kiedy ma zastosowanie ta reguła?

☒ **Domena**

Ma zastosowanie, gdy komputer jest połączony ze swoją domeną firmową.

☒ **Prywatny**

Ma zastosowanie, gdy komputer jest połączony z lokalizacją w sieci prywatnej.

☒ **Publiczny**

Ma zastosowanie, gdy komputer jest połączony z lokalizacją w sieci publicznej.

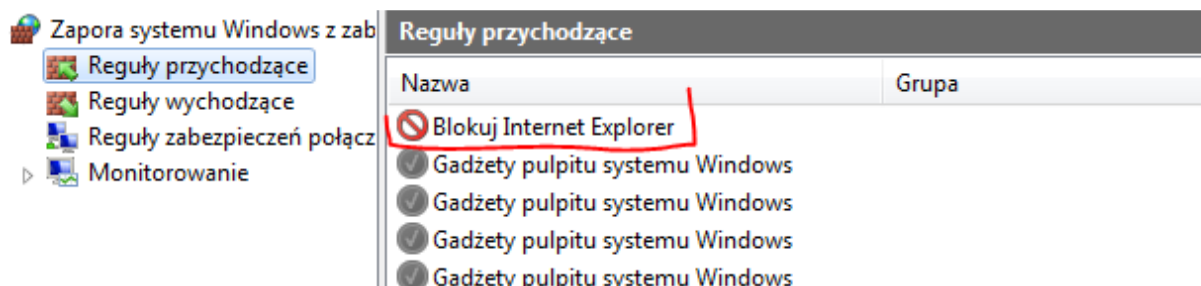
Następnie nadajemy regule nazwę (w tym przypadku *Blokuj Internet Explorer*) i klikamy *Zakończ*.

Nazwa:

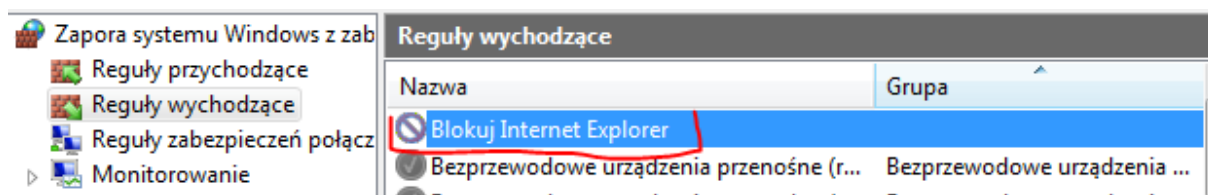
Blokuj Internet Explorer

Opis (opcjonalnie):

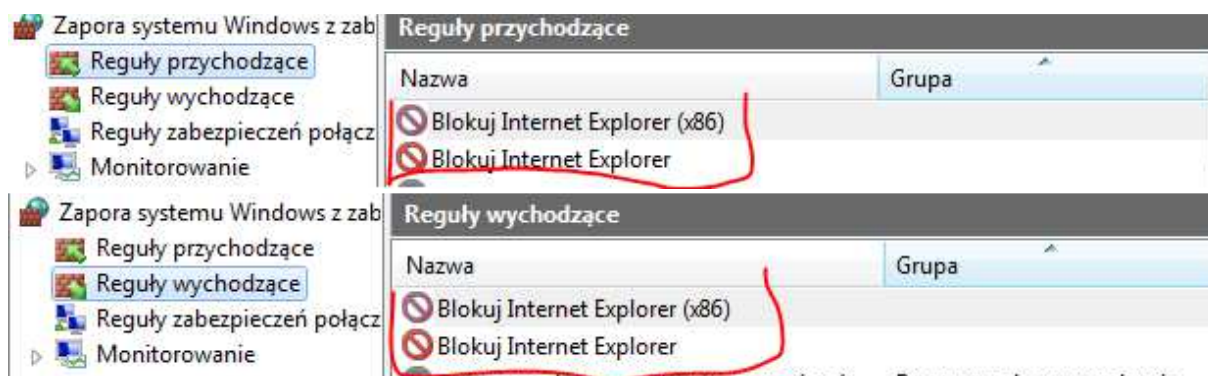
W wyniku operacji powstała nowa *reguła przychodząca*



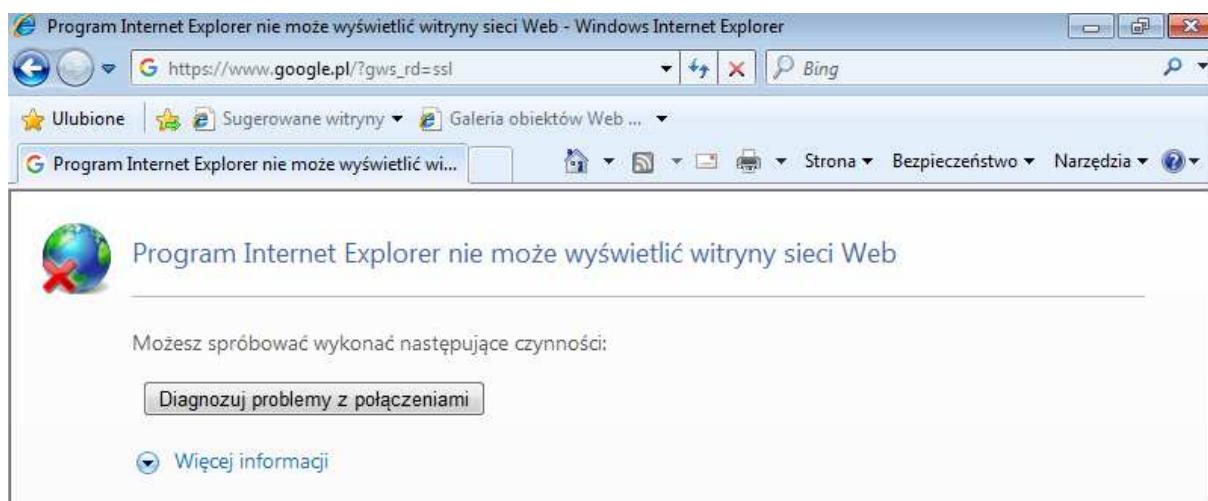
*Internet Explorer* nie będzie w stanie odbierać komunikacji, lecz chcemy ją także zablokować komunikację wychodzącą – w tym celu tworzymy analogiczną *Regułę wychodzącą*.



Reguły te jednak nie wystarczą aby zablokować *Internet Explorer*'a. *Internet Explorer* zainstalowany w systemie jest w dwóch wersjach 64-bitowej i 32-bitowej, my zablokowaliśmy jedynie 64-bitową. Domyślnie jednak uruchamiana jest jednak wersja 32-bitowa, więc dla niej musimy również stworzyć zarówno regułę przychodzącą jak i wychodzącą (ścieżka programu: *C:\Program Files (x86)\Internet Explorer\iexplore.exe*)



Dopiero teraz *Internet Explorer* zostaje odcięty od komunikacji sieciowej.



Użytkownik może jednak zainstalować inną przeglądarkę internetową (w tym przypadku *Firefox*) i wciąż połączyć się z Internetem.





Fundusze Europejskie  
Wiedza Edukacja Rozwój

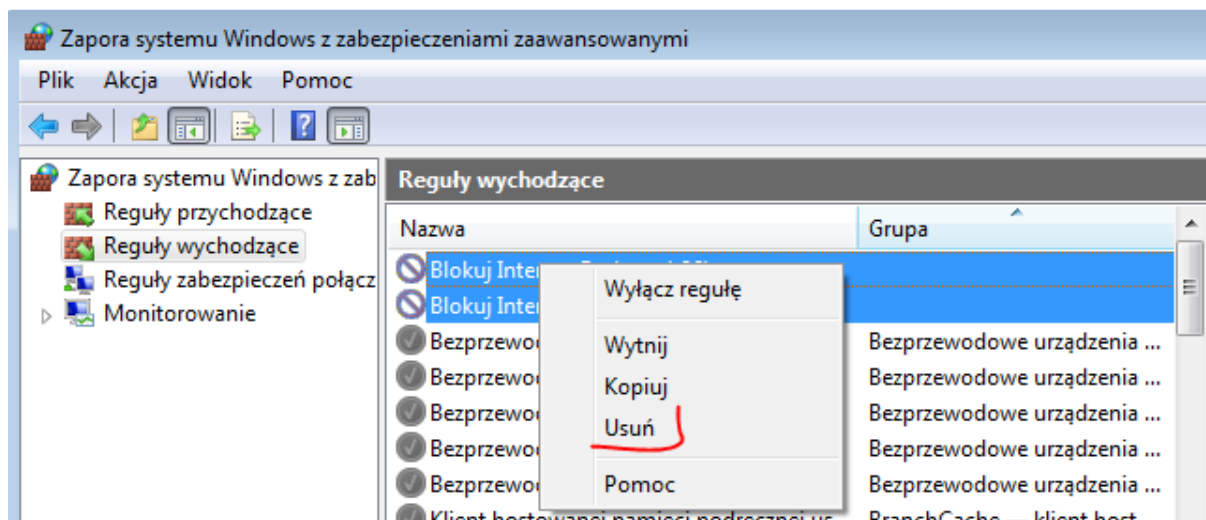


Rzeczpospolita  
Polska

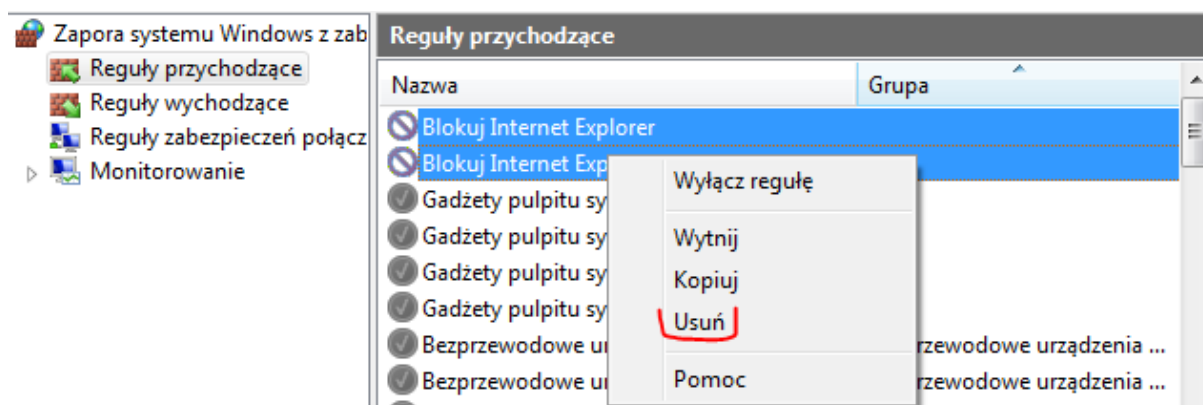
Unia Europejska  
Europejski Fundusz Społeczny



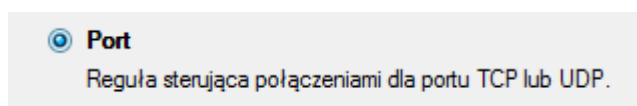
Aby całkowicie zablokować dostęp do stron WWW, dla wszystkich przeglądarek internetowych możemy zablokować porty przez nie wykorzystywane (80, 443, 8080). Wpierw jednak usuńmy reguły stworzone dla programu *Internet Explorer*.



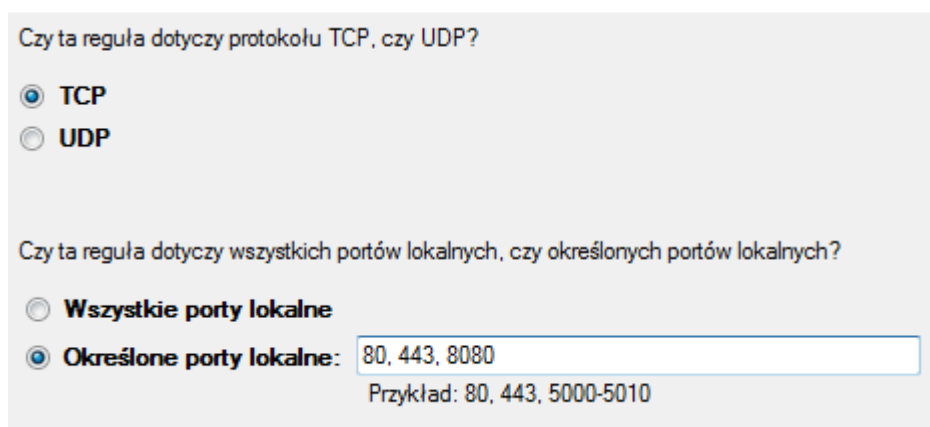




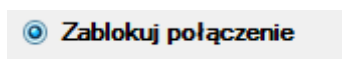
Następnie stwórzmy regułę przychodzącą dla Portu. Jako typ reguły wybieramy *Port*



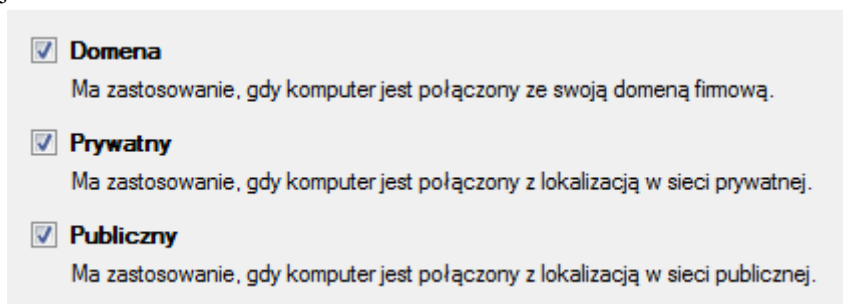
Wybieramy TCP oraz określamy porty 80,443,8080



Wybieramy *Zablokuj połączenia*



Wszystkie lokalizacje



oraz nadajemy Nazwę (w tym przypadku *Blokuj TCP 80,443,8080*).

*Projekt „SezAM wiedzy, kompetencji i umiejętności” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój*

Tworzymy taką samą regułę lecz dla portu UDP i nazywamy ją *Blokuj UDP 80,443,8080*

Czy ta reguła dotyczy protokołu TCP, czy UDP?

☐ TCP

☒ UDP

Czy ta reguła dotyczy wszystkich portów lokalnych, czy określonych portów lokalnych?

☐ Wszystkie porty lokalne

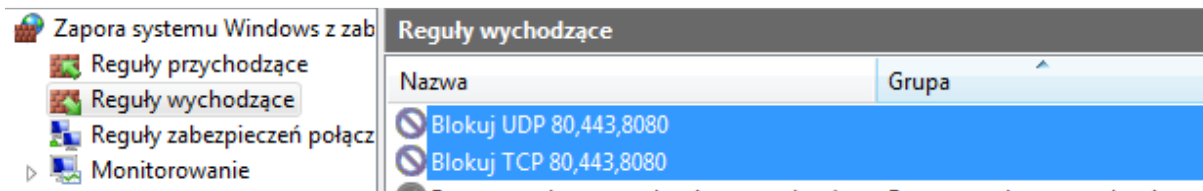
☒ Określone porty lokalne:

Przykład: 80, 443, 5000-5010

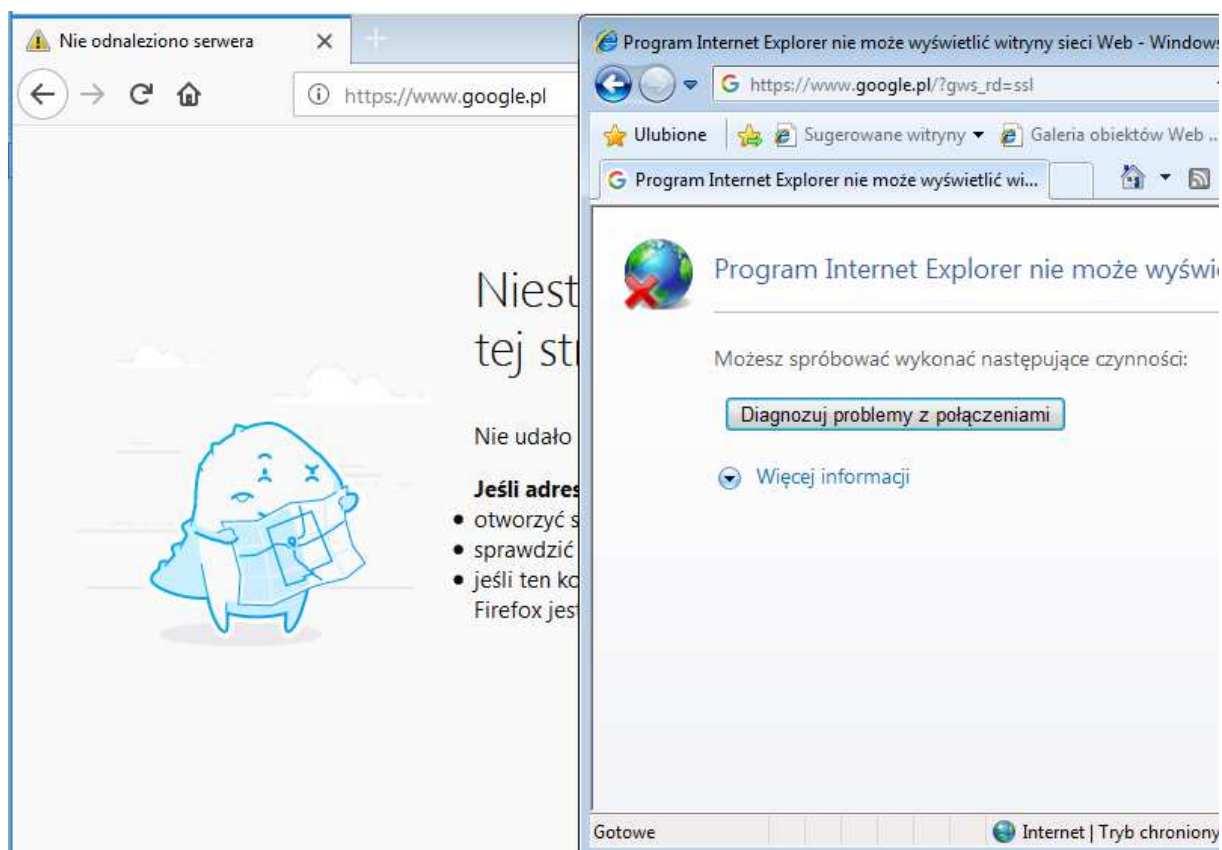
Otrzymamy dwie blokujące reguły przychodzące blokujące protokoły TCP i UDP na portach 80, 443, 8080



Operację powtarzamy tworząc Reguły wychodzące.



W wyniku żadna przeglądarka internetowa (nawet nowo zainstalowana) nie będzie wstanie wyświetlać stron WWW



Usuńmy utworzone reguły.

Niestety nie zawsze wiemy jakie programy komunikują się z siecią i na jakich portach. W przypadku posiadania na komputerze niepożądanego programu, który komunikuje się z siecią musimy wpierw ustalić na jakich portach i z jakimi adresami komunikują się programy z siecią.

System Windows posiada wbudowany program netstat, który pozwala wyświetlić całą aktywną komunikację sieciową. Wywołujemy go z konsoli (z uprawnieniami administracyjnymi). Aby wyświetlić wszystkie połączenia wywołujemy polecenie netstat -a



```
C:\Windows\system32>netstat -a
```

#### Aktywne połączenia

Protokół	Adres lokalny	Obcy adres	Stan
TCP	0.0.0.0:135	Win7VM1-Device:0	NASŁUCHIWANIE
TCP	0.0.0.0:445	Win7VM1-Device:0	NASŁUCHIWANIE
TCP	0.0.0.0:5357	Win7VM1-Device:0	NASŁUCHIWANIE
TCP	0.0.0.0:49152	Win7VM1-Device:0	NASŁUCHIWANIE
TCP	0.0.0.0:49153	Win7VM1-Device:0	NASŁUCHIWANIE
TCP	0.0.0.0:49154	Win7VM1-Device:0	NASŁUCHIWANIE
TCP	0.0.0.0:49155	Win7VM1-Device:0	NASŁUCHIWANIE
TCP	0.0.0.0:49156	Win7VM1-Device:0	NASŁUCHIWANIE
TCP	10.0.2.15:139	Win7VM1-Device:0	NASŁUCHIWANIE
TCP	10.0.2.15:49908	www:https	CZAS_OCZEKIWANIA
TCP	[::]:135	Win7VM1-Device:0	NASŁUCHIWANIE
TCP	[::]:445	Win7VM1-Device:0	NASŁUCHIWANIE
TCP	[::]:5357	Win7VM1-Device:0	NASŁUCHIWANIE
TCP	[::]:49152	Win7VM1-Device:0	NASŁUCHIWANIE
TCP	[::]:49153	Win7VM1-Device:0	NASŁUCHIWANIE
TCP	[::]:49154	Win7VM1-Device:0	NASŁUCHIWANIE
TCP	[::]:49155	Win7VM1-Device:0	NASŁUCHIWANIE
TCP	[::]:49156	Win7VM1-Device:0	NASŁUCHIWANIE
UDP	0.0.0.0:3702	:::	
UDP	0.0.0.0:3702	:::	
UDP	0.0.0.0:5355	:::	
UDP	0.0.0.0:62493	:::	
UDP	10.0.2.15:137	:::	
UDP	10.0.2.15:138	:::	
UDP	10.0.2.15:1900	:::	
UDP	127.0.0.1:1900	:::	
UDP	127.0.0.1:56379	:::	
UDP	[::]:3702	:::	
UDP	[::]:3702	:::	
UDP	[::]:5355	:::	
UDP	[::]:62494	:::	
UDP	[::]:1900	:::	
UDP	[::]:56378	:::	

Uzyskujemy cały aktywny aktualnie ruch sieciowy, jeśli chcemy możemy zablokować jakieś z tych portów lub adresów.

Warto wywołać polecenie netstat -b, aby otrzymać listę połączeń, które system operacyjny był w stanie powiązać do konkretnego programu (nie są to wszystkie połączenia, jedynie te które system operacyjny był w stanie rozróżnić)



```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>netstat -b

Aktywne połączenia

Protokół Adres lokalny Obcy adres Stan
TCP 10.0.2.15:49921 185.225.250.17:http USTANOWIONO
[firefox.exe]
TCP 10.0.2.15:49922 ec2-52-27-184-151:https USTANOWIONO
[firefox.exe]
TCP 10.0.2.15:49923 ec2-52-40-109-206:https USTANOWIONO
[firefox.exe]
TCP 10.0.2.15:49924 93.184.220.29:http USTANOWIONO
[firefox.exe]
TCP 10.0.2.15:49925 99.84.159.62:https USTANOWIONO
[firefox.exe]
TCP 10.0.2.15:49926 waw02s14-in-f3:https USTANOWIONO
[firefox.exe]
TCP 10.0.2.15:49927 muc03s08-in-f46:http USTANOWIONO
[firefox.exe]
TCP 10.0.2.15:49928 waw02s05-in-f42:https USTANOWIONO
[firefox.exe]
TCP 10.0.2.15:49929 muc03s08-in-f46:http USTANOWIONO
[firefox.exe]
TCP 10.0.2.15:49930 waw02s14-in-f3:https CZAS_OCZEKIWANIA
TCP 10.0.2.15:49931 waw02s07-in-f163:https USTANOWIONO
[firefox.exe]
TCP 10.0.2.15:49932 waw02s16-in-f14:https USTANOWIONO
[firefox.exe]
TCP 10.0.2.15:49933 ec2-52-33-113-226:https USTANOWIONO
[firefox.exe]
TCP 10.0.2.15:49934 waw02s07-in-f162:https USTANOWIONO
[firefox.exe]
TCP 127.0.0.1:49911 Win7UM1-Device:49912 USTANOWIONO
[firefox.exe]
TCP 127.0.0.1:49912 Win7UM1-Device:49911 USTANOWIONO
[firefox.exe]
TCP 127.0.0.1:49913 Win7UM1-Device:49914 USTANOWIONO
[firefox.exe]
```

Wykazane zostały połączenia, które nawiązuje program *Firefox*.

Warto również wywołać polecenie `netstat -n`, aby wyświetlić aktywne połączenia TCP.

```
C:\Windows\system32>netstat -n

Aktywne połączenia

Protokół Adres lokalny Obcy adres Stan
TCP 10.0.2.15:49941 172.217.16.35:443 USTANOWIONO
TCP 10.0.2.15:49942 216.58.215.78:443 USTANOWIONO
TCP 10.0.2.15:49943 172.217.20.163:443 USTANOWIONO
TCP 127.0.0.1:49911 127.0.0.1:49912 USTANOWIONO
TCP 127.0.0.1:49912 127.0.0.1:49911 USTANOWIONO
TCP 127.0.0.1:49913 127.0.0.1:49914 USTANOWIONO
TCP 127.0.0.1:49914 127.0.0.1:49913 USTANOWIONO
TCP 127.0.0.1:49915 127.0.0.1:49916 USTANOWIONO
TCP 127.0.0.1:49916 127.0.0.1:49915 USTANOWIONO
TCP 127.0.0.1:49917 127.0.0.1:49918 USTANOWIONO
TCP 127.0.0.1:49918 127.0.0.1:49917 USTANOWIONO
TCP 127.0.0.1:49919 127.0.0.1:49920 USTANOWIONO
TCP 127.0.0.1:49920 127.0.0.1:49919 USTANOWIONO
```

Sprawdźmy z jaką domeną skojarzony jest adres 172.217.20.163

```
C:\Windows\system32>ping -a 172.217.20.163

Badanie waw02s07-in-f163.1e100.net [172.217.20.163] z 32 bajtami danych:
```

Możemy teraz sprawdzić do kogo należy ta domena



Wszystko

Zakupy

Grafika

Filmy

Wiadomości

Więcej

Ustawienia

Narzędzia

Okolo 63 wyników (0,44 s)

### What is 1e100.net? - Google Help - Google Support

→ <https://support.google.com/faqs/answer/174717?hl=en> ▼ Tłumaczenie strony

1e100.net is a Google-owned domain name used to identify the servers in our network. Following standard industry practice, we make sure each IP address has ...

Przejdźmy do wyniku wyszukiwania

## What is 1e100.net?

1e100.net is a Google-owned domain name used to identify the servers in our network.

Wygląda na to, że jest to jedna z domen google. Spingujemy więc google.pl by sprawdzić czy uzyskamy oczekiwany rezultat.

```
C:\Windows\system32>ping google.pl  
Badanie google.pl [172.217.20.163] z 32 bajtami danych:  
Control=C
```

Pingując google.pl otrzymaliśmy ten sam adres, który badaliśmy.

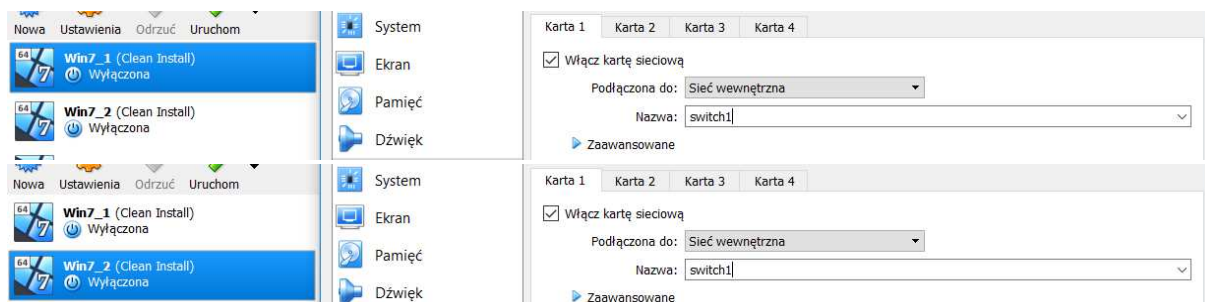
Przeprowadzone badania pozwalają określić, że przeglądarka Firefox łączy się aktualnie z domeną Google (adres google.pl to 172.217.20.163) oraz że ruch jest szyfrowany (używany jest port 443).

### 3.2. Przykład testowania zapory sieciowej

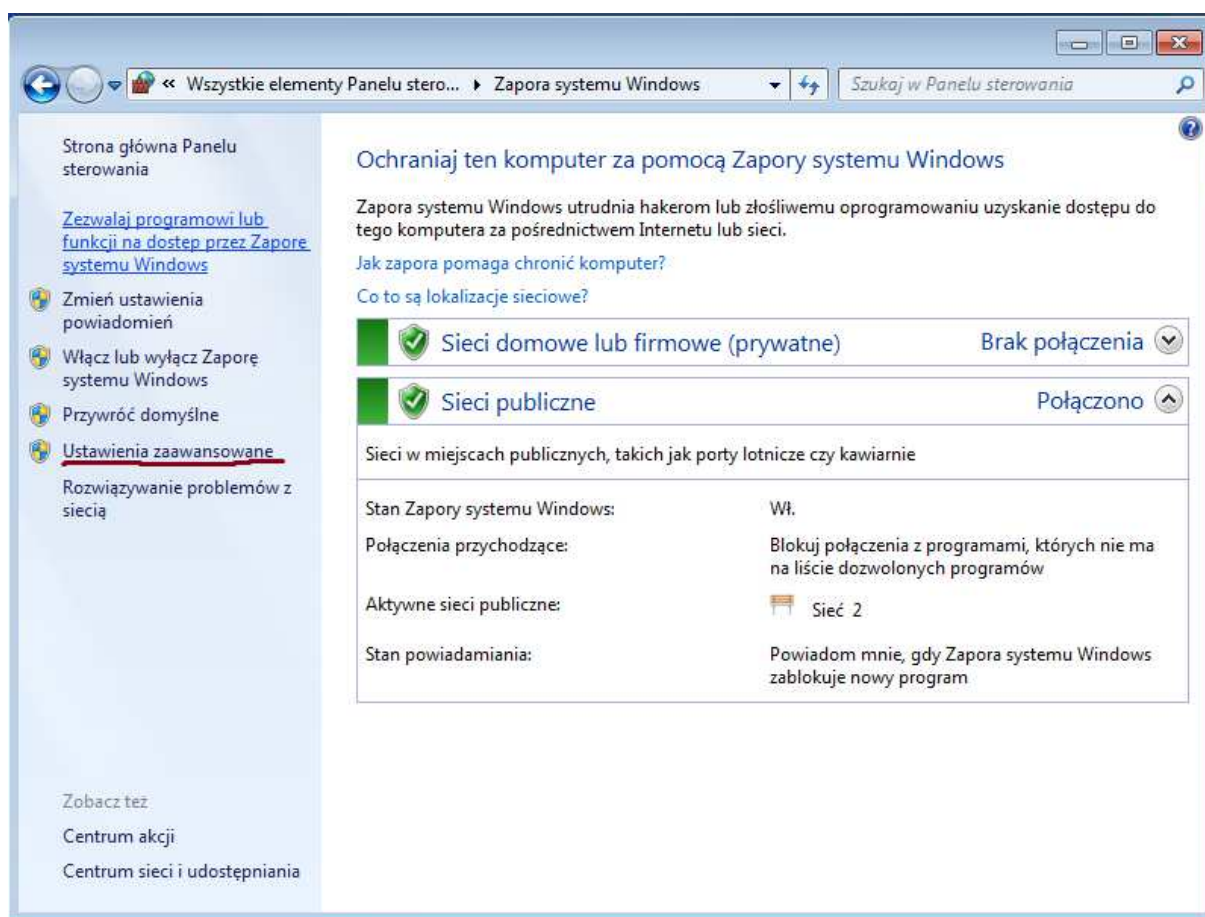
W pierwszej kolejności konfigurujemy karty sieciowe wirtualnych maszyn z Windowsem, tak aby działały w jednej sieci. Może to być *Sieć wewnętrzna* lub *Mostkowana karta sieciowa* – nie jest to istotne, ważne aby komputery znajdowały się w tej samej podsieci i były dla siebie widoczne (powinny mieć możliwość wzajemnie poprawnie się pingować). Można także dopilnować by komputery miały unikalne nazwy hosta i umieścić w tej samej grupie roboczej (jest to jednak opcjonalne – dopóki nie zamierzamy korzystać z usług sieciowych Windows tj. udostępnianie [SMB], ta sama nazwa hosta i przynależność komputerów do różnych grup roboczych nie stanowi problemu – grupa robocza oddziałuje jedynie na usługi natywne dla systemów Windows pełnione w sieci lokalnej i w wirtualnej sieci lokalnej [VPN]). Jako lokalizację sieci wybieramy *sieć publiczna* (zapora sieciowa w tej konfiguracji ma najbardziej restrykcyjne reguły).

W tym przypadku na obu maszynach interfejs sieciowy skonfigurowano jako *sieć wewnętrzna* i zastosowano statyczną adresację IP. Jako lokalizację sieci wybrano *sieć publiczną*. Nie umieszczono komputerów w tej samej grupie roboczej i nie zadbano o unikalność nazw hostów.

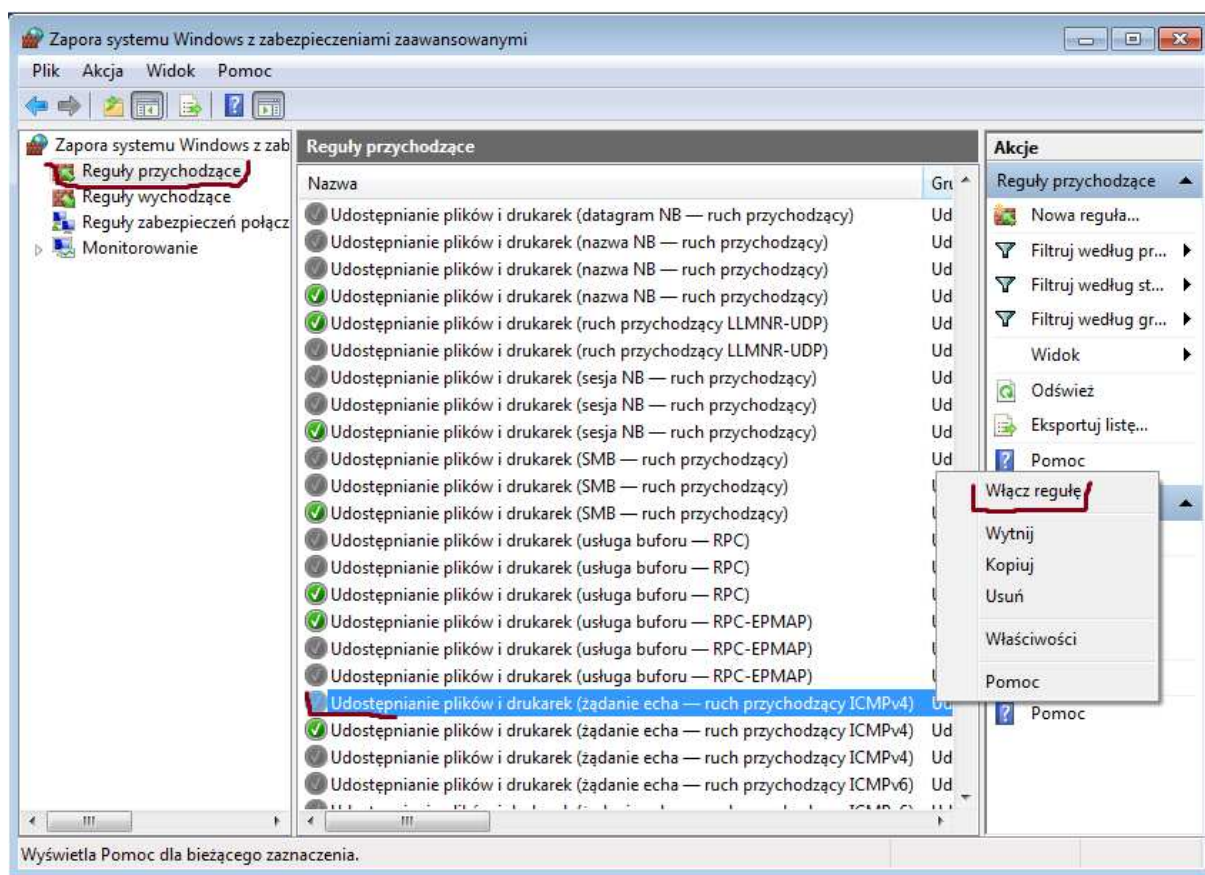




Posłużono się protokołem ICMP w celu sprawdzenia połączenia pomiędzy komputerami (polecenie ping). Jeśli wybrano lokalizację *Sieć publiczna*, to ping do drugiego komputera nie zadziała. W tym przypadku ruch sieciowy ICMP jest blokowany przez zaporę. Należy włączyć gotową regułę, która odblokuje działanie protokołu ICMP. Aby tego dokonać wystarczy przejść do *Zapory systemu Windows*, następnie do *ustawień zaawansowanych*.

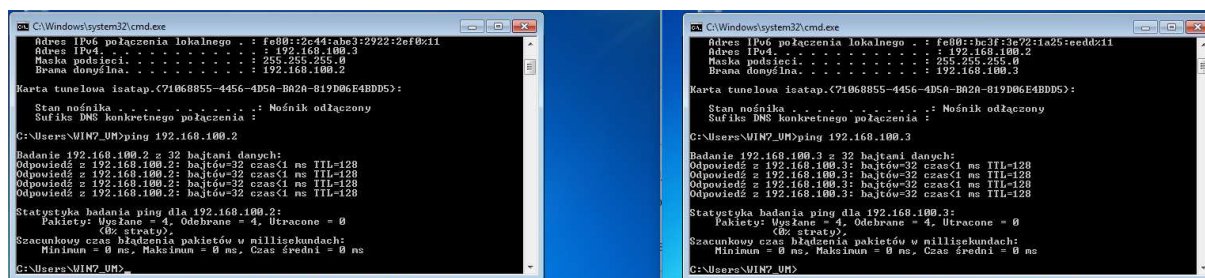


Kolejnym krokiem jest włączenie reguły przychodzącej ICMPv4 dla profilu *Publicznego*.



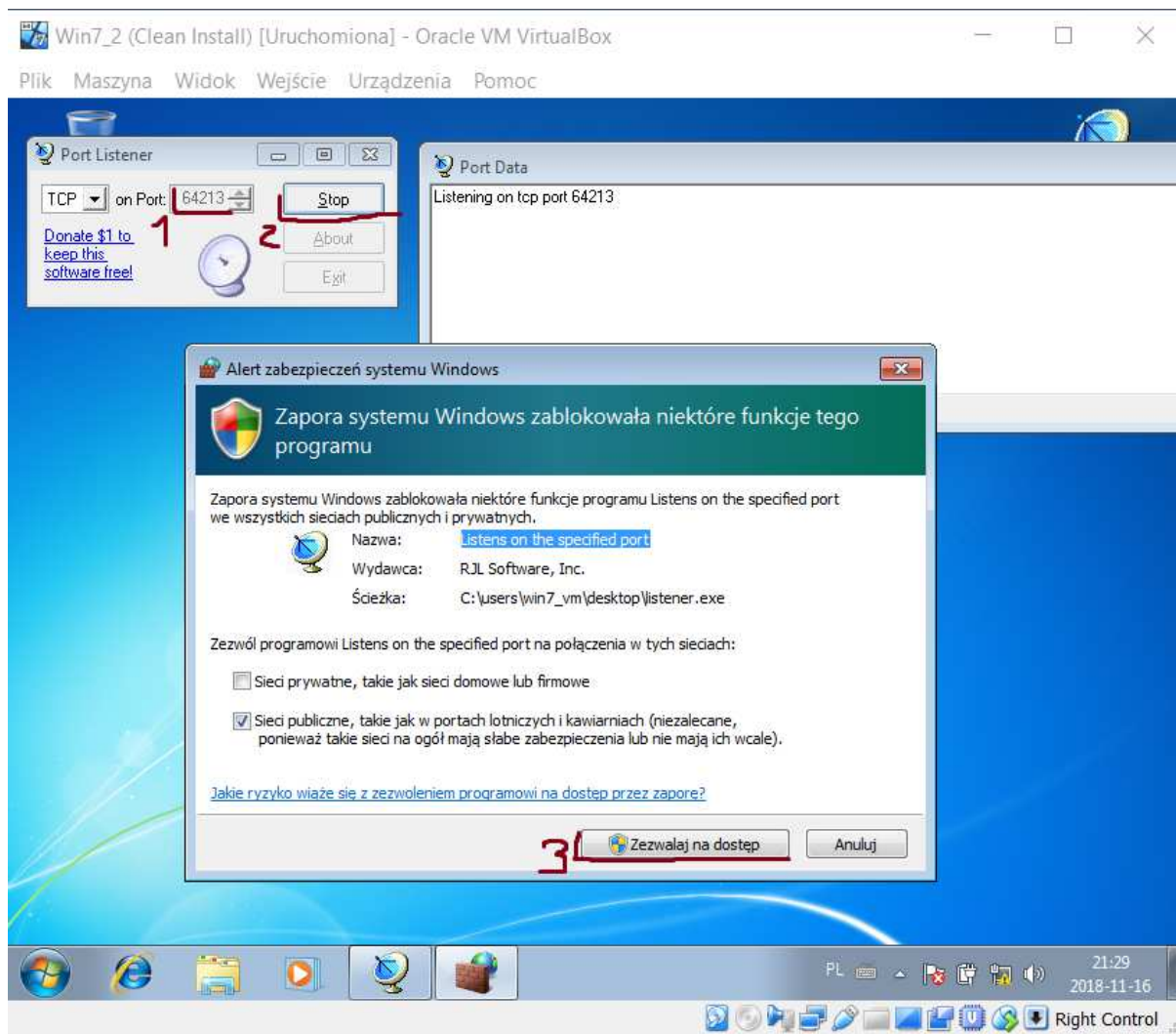
✓ Udostępnianie plików i drukarek (zadanie... Udostępnianie plików i druk... Publi...

Po odblokowaniu w zaporze protokołu ICMPv4 na obu maszynach wirtualnych pingi powinny odbywać się poprawnie.

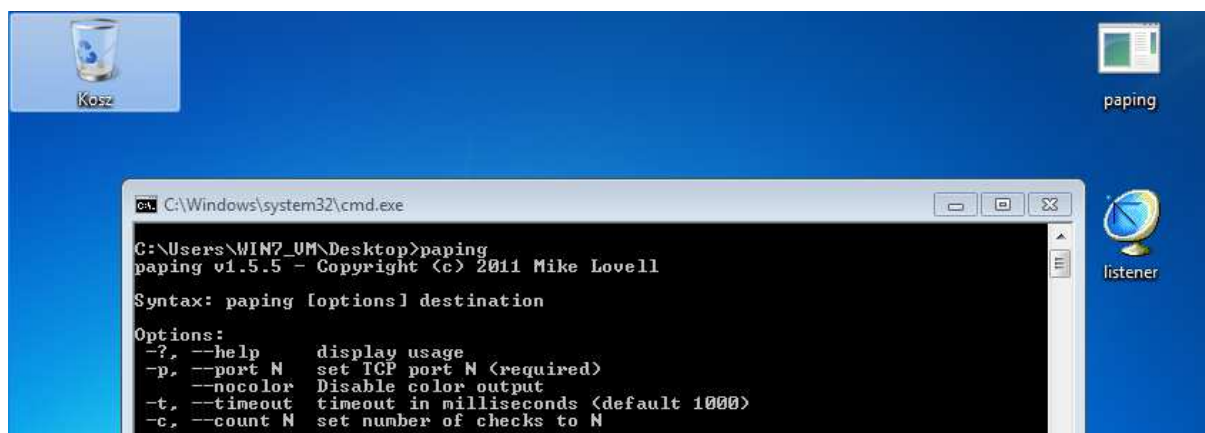


Mamy więc poprawne połączenie pomiędzy dwoma maszynami wirtualnymi. Odblokowanie ICMP nie pozwala jednak świadczyć usług sieciowych pomiędzy tymi maszynami – do tego należy posłużyć się protokołami TCP lub UDP. Program ping nie potrafi wysyłać zapytań TCP i UDP – ogranicza się jedynie do ICMP. Posłużymy się w tym celu dwoma programami: *PortListener* – do nasłuchiwania portów oraz *paping* – do wysyłania zapytań.

W pierwszej kolejności skonfigurujemy program *PortListener*. Obierzemy jakiś dowolny nieużywany port TCP (w tym przypadku 64213) i uruchomimy nasłuchiwanie na drugiej maszynie. Przy pierwszym uruchomieniu program poprosi o zgodę na automatyczne odblokowanie sobie zatory – stworzona zostanie reguła dla programu (wszystkie porty, które będą przez ten program wykorzystywane zostaną automatycznie odblokowane na czas działania programu). Tymczasowo dokonajmy automatycznego odblokowania zatory.



Z poziomu pierwszej maszyny wyślijmy zapytanie na ten port za pomocą programu *paping*, lecz najpierw odczytajmy jego składnię.



Wynika z tego, że aby dokonać wysłania żądania do maszyny drugiej należy posłużyć się poleceniem `paping 192.168.100.2 -p 64213`

*Projekt „SezAM wiedzy, kompetencji i umiejętności” jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój*





```
C:\Users\WIN7_UM\Desktop>paping 192.168.100.2 -p 64213
paping v1.5.5 - Copyright (c) 2011 Mike Lovell

Connecting to 192.168.100.2 on TCP 64213:

Connected to 192.168.100.2: time=0.00ms protocol=TCP port=64213
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=64213
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=64213
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=64213
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=64213
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=64213
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=64213
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=64213
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=64213
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=64213

Connection statistics:
  Attempted = 10, Connected = 10, Failed = 0 (0.00%)
Approximate connection times:
  Minimum = 0.00ms, Maximum = 0.00ms, Average = 0.00ms
```

Wygłąda na to, że możemy połączyć się z nasłuchiwanym portem na drugiej maszynie. Jako, iż stworzyliśmy regułę dla całego programu *PortListener*, możemy zmienić nasłuchiwany port bez zmiany konfiguracji zapory sieciowej.

Zmieńmy więc nasłuchiwany port na inny (w tym przypadku 62208) i spróbujmy wysłać na niego żądania.

The screenshot shows a Windows command prompt window titled "MASZYNA 1" and a Port Listener application window titled "MASZYNA 2".

**Command Prompt (MASZYNA 1):**

```
C:\Windows\system32\cmd.exe
Connection statistics:
  Attempted = 10, Connected = 10, Failed = 0 (0.00%)
Approximate connection times:
  Minimum = 0.00ms, Maximum = 0.00ms, Average = 0.00ms

C:\Users\WIN7_UM\Desktop>paping 192.168.100.2 -p 62208
paping v1.5.5 - Copyright (c) 2011 Mike Lovell

Connecting to 192.168.100.2 on TCP 62208:

Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208

Connection statistics:
  Attempted = 6, Connected = 6, Failed = 0 (0.00%)
Approximate connection times:
  Minimum = 0.00ms, Maximum = 0.00ms, Average = 0.00ms

C:\Users\WIN7_UM\Desktop>
```

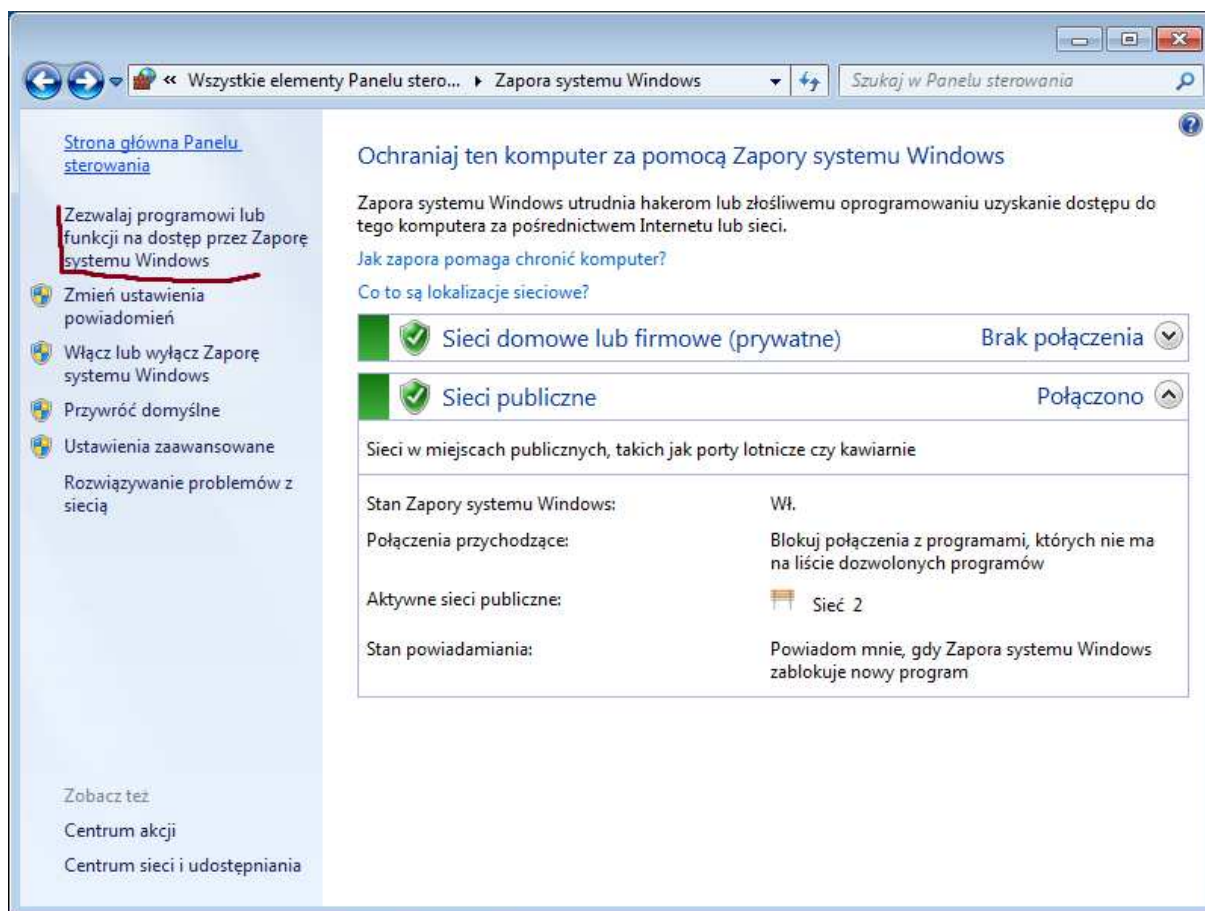
**Port Listener (MASZYNA 2):**

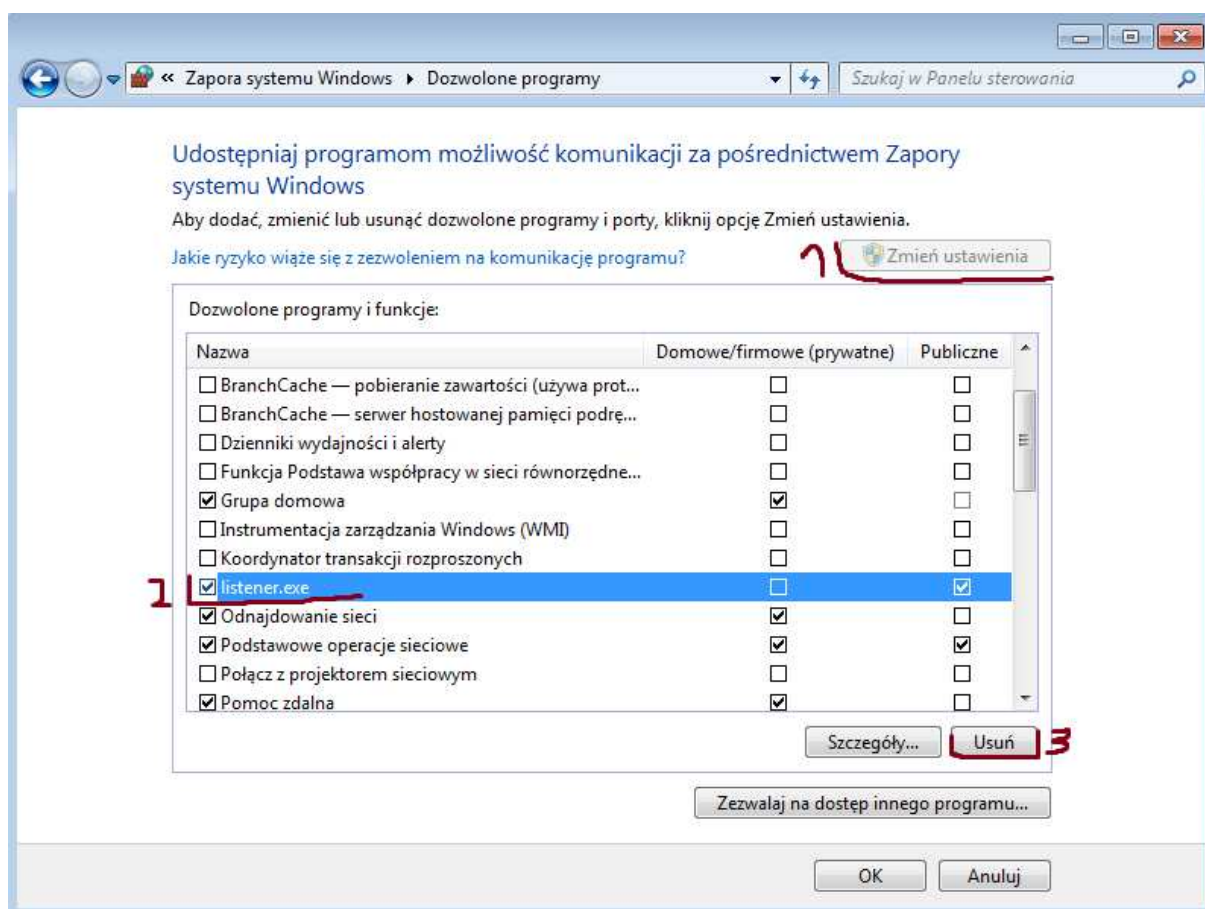
The Port Listener application is configured to listen on TCP port 62208. It shows a list of client connections:

- Client connected
- Client disconnected
- Client connected
- Client disconnected
- Client connected
- Client disconnected
- Client connected
- Client disconnected
- Client connected
- Client disconnected

The application also has a "Stop" button and a "Right-click for options" button.

Usuńmy regułę z zapory dla aplikacji *PortListener*, ponieważ nie czerpiemy żadnej korzyści z odblokowania zapory dla programu testowego (takie działanie zapory nie przenosi się na inne programy świadczące usługi – dotyczy jedynie *PortListener'a*).





Żądania na port nie będą teraz działać.

```
C:\Users\WIN7_UM\Desktop>paping 192.168.100.2 -p 62208
paping v1.5.5 - Copyright (c) 2011 Mike Lovell

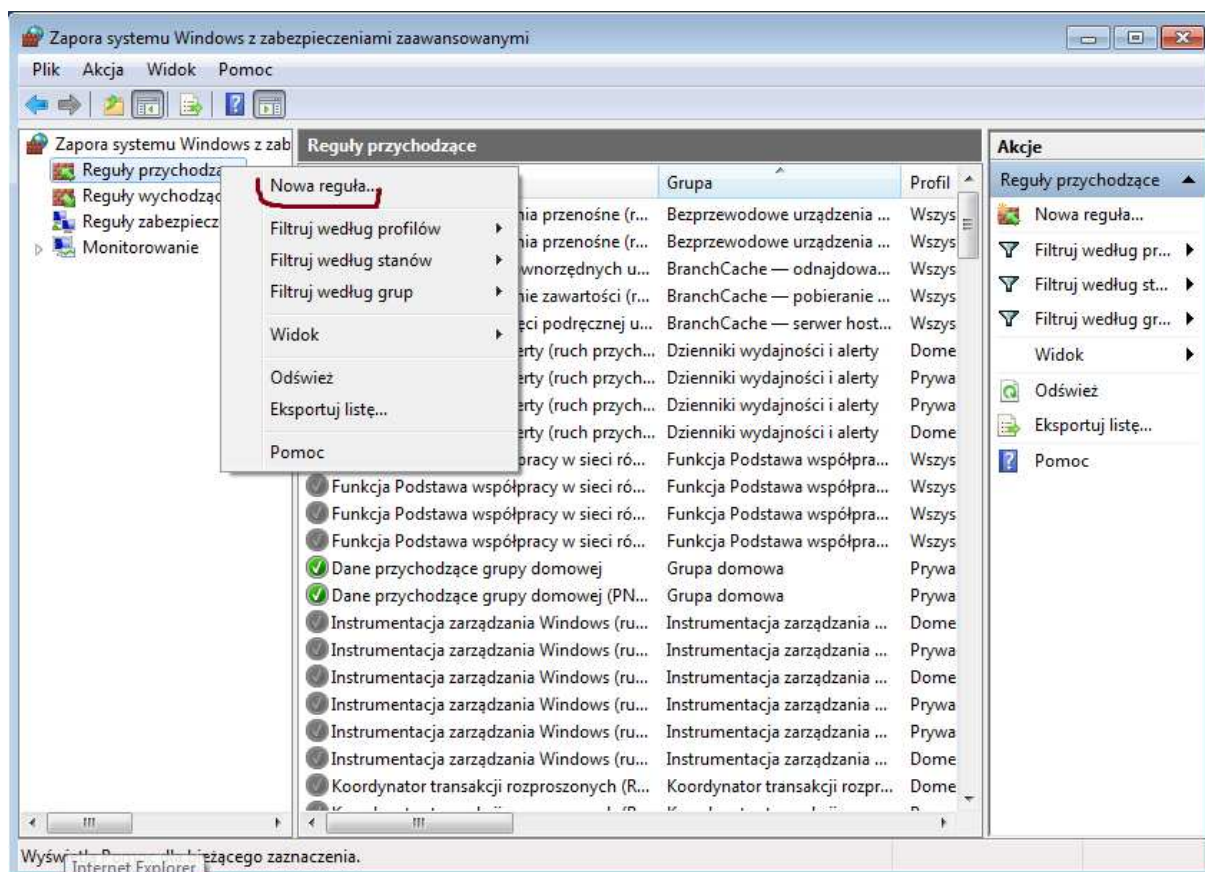
Connecting to 192.168.100.2 on TCP 62208:

Connection timed out
Connection timed out
Connection timed out
Connection timed out
Connection timed out
Connection timed out
Connection timed out

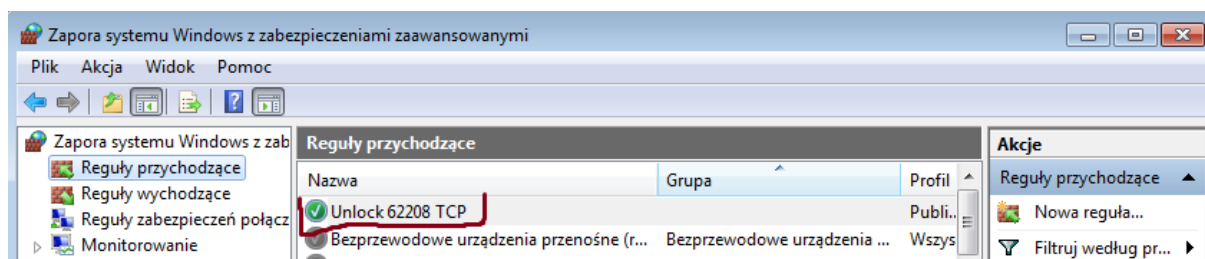
Connection statistics:
  Attempted = 7, Connected = 0, Failed = 7 (100.00%)
Approximate connection times:
  Minimum = 0.00ms, Maximum = 0.00ms, Average = 0.00ms
```

Żądania nie docierają ponieważ port TCP 62208 jest aktualnie zablokowany. Stwórzmy więc regułę w zaporze maszyny drugiej, która port ten odblokuje i dopuści na nim do komunikacji. Aby tego dokonać musimy stworzyć regułę przychodząca dla portu TCP 62208. Przechodzimy do *Zapora sieciowa Windows* → *Ustawienia zaawansowane* → *Reguły przychodzące*. Następnie klikając prawy przycisk myszy wywołujemy menu kontekstowe z którego wybieramy opcję *Nowa reguła*.





Wywołany zostanie kreator. Jako typ reguły wybieramy *Port*, klikamy *Dalej*, wybieramy *TCP* i w *Określone porty lokalne* wpisujemy 62208, a następnie klikamy *Dalej*. W kolejnym kroku wybieramy *Zezwalaj na połączenie*. Następnie będziemy mogli wybrać w jakich lokalizacjach reguła będzie miała zastosowanie. Aktualnie lokalizacją jest *Sieć publiczna*, więc pozostawiamy wybraną jedynie opcję *Publiczny*. Nadajemy dowolną nazwę (w tym przypadku *Unlock 62208 TCP*). Stworzona zostanie nowa reguła odblokowująca port 62208.



Sprawdźmy czy utworzyliśmy regułę poprawnie wykonując żądanie na ten port.



```
G:\Users\WIN7_UM\Desktop>ping 192.168.100.2 -p 62208
ping v1.5.5 - Copyright (c) 2011 Mike Lovell

Connecting to 192.168.100.2 on TCP 62208:

Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208
Connected to 192.168.100.2: time=0.00ms protocol=TCP port=62208

Connection statistics:
    Attempted = 14, Connected = 14, Failed = 0 (0.00%)
Approximate connection times:
    Minimum = 0.00ms, Maximum = 0.00ms, Average = 0.00ms
```

Wygląda na to, że wszystko jest w porządku. Możemy na maszynie drugiej świadczyć usługę sieciową wykorzystując port TCP 62208.

## 4. Zadania

*Na każdym etapie zadania twórz screenshot'y (w nazwach powinna znajdować się numeracja wskazująca wykonywaną kolejność kroków), a następnie spakuj do archiwum zip o nazwie WdZOW\_LAB\_NrAlbumu oraz wyślij na adres e-mail podany przez prowadzącego zajęcia laboratoryjne.*

### 4.1 Skonfiguruj działanie zapory sieciowej na maszynie z systemem Windows

- ...

### 4.2 Skonfiguruj i przetestuj działanie zapory sieciowej komputera z systemem operacyjnym MS Windows

- ....

## Literatura

1. A. Kisielewicz, Wprowadzenie do informatyki, Helion, Gliwice 2002
2. Scott H. A. Clark, W sercu PC – wg Petera Nortona, Helion, Gliwice 2002
3. J. Shim, J. Siegel, R. Chi, Technologia Informacyjna, Dom Wydawniczy ABC, Warszawa, 1999
4. A. Silberschatz, P.B. Galvin, G. Gagne, Podstawy systemów operacyjnych, WNT, Warszawa 2006
5. A. S. Twnenbaum, Systemy operacyjne, Helion, Gliwice 2010
6. P. Beynon-Davies, Systemy baz danych, WNT, Warszawa 2000
7. W. Stallings, Systemy operacyjne, Struktura i zasady budowy, PWN, Warszawa 2006
8. A. Jakubowski, Podstawy SQL. Ćwiczenia praktyczne, Helion, Gliwice 2004