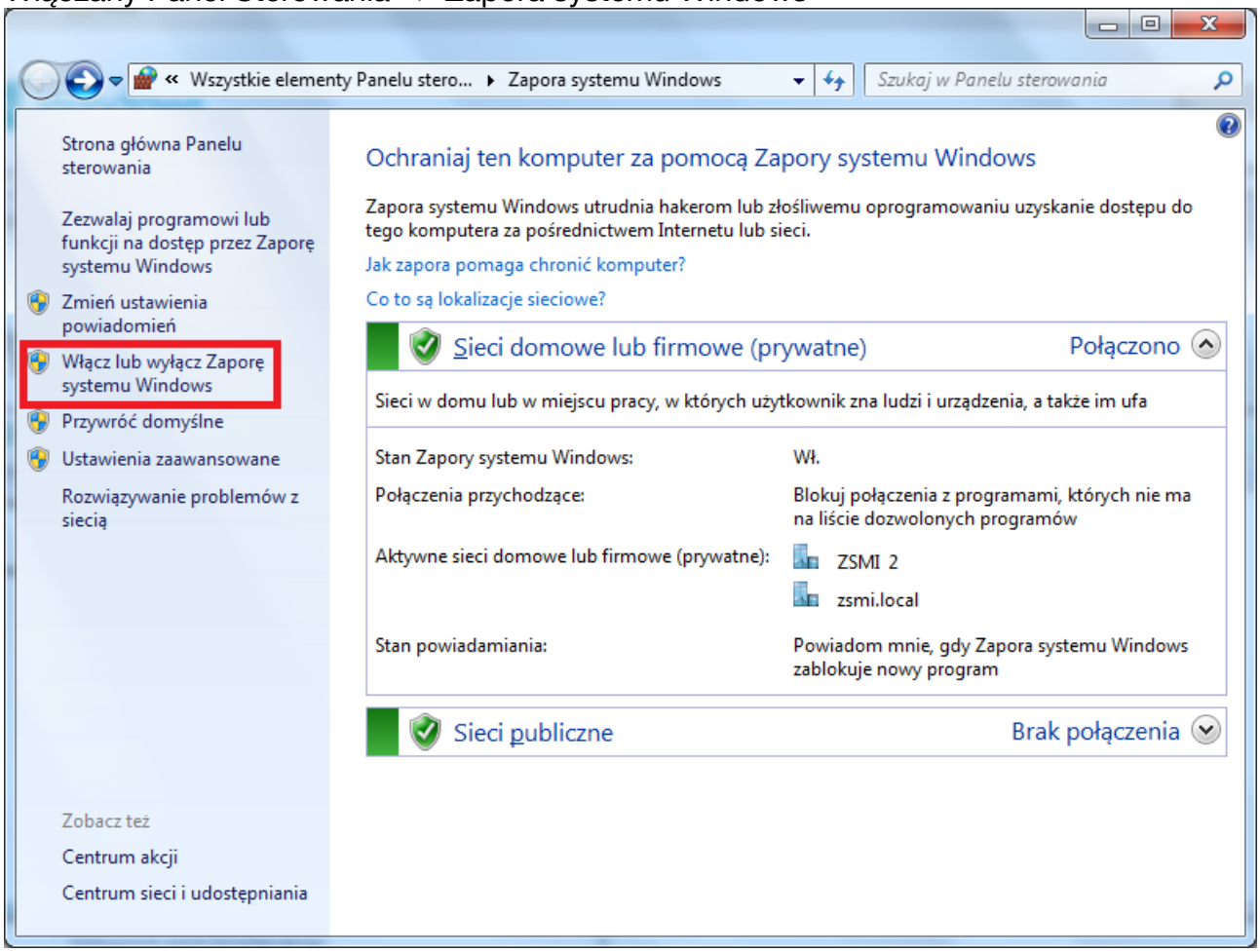
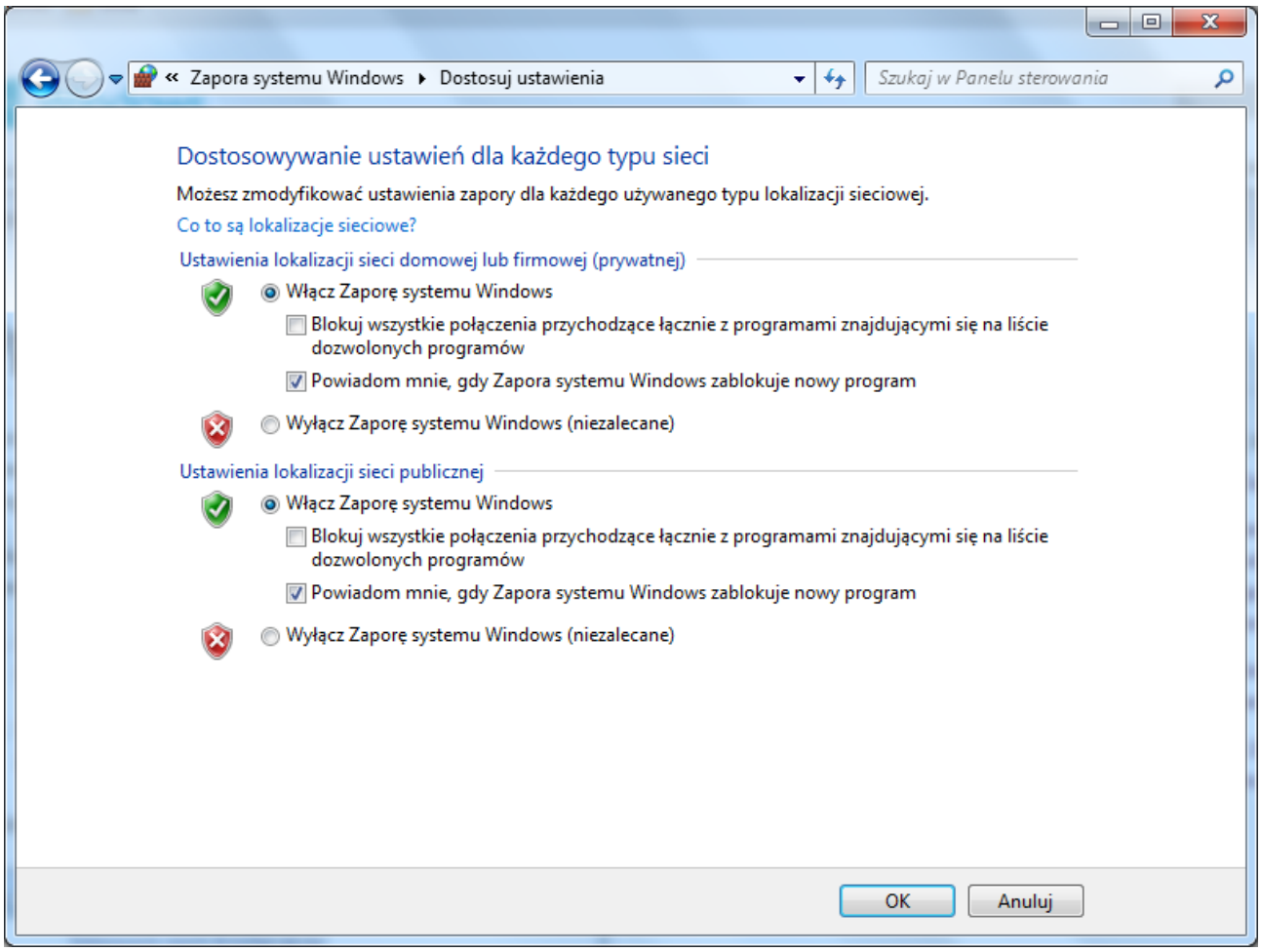
Zapora systemu Windows

Wykorzystując maszynę wirtualną z zainstalowanym systemem Windows 10 przeczytaj oraz wykonaj poniższe zadania.

Włączanie lub wyłączanie zapory systemu Windows

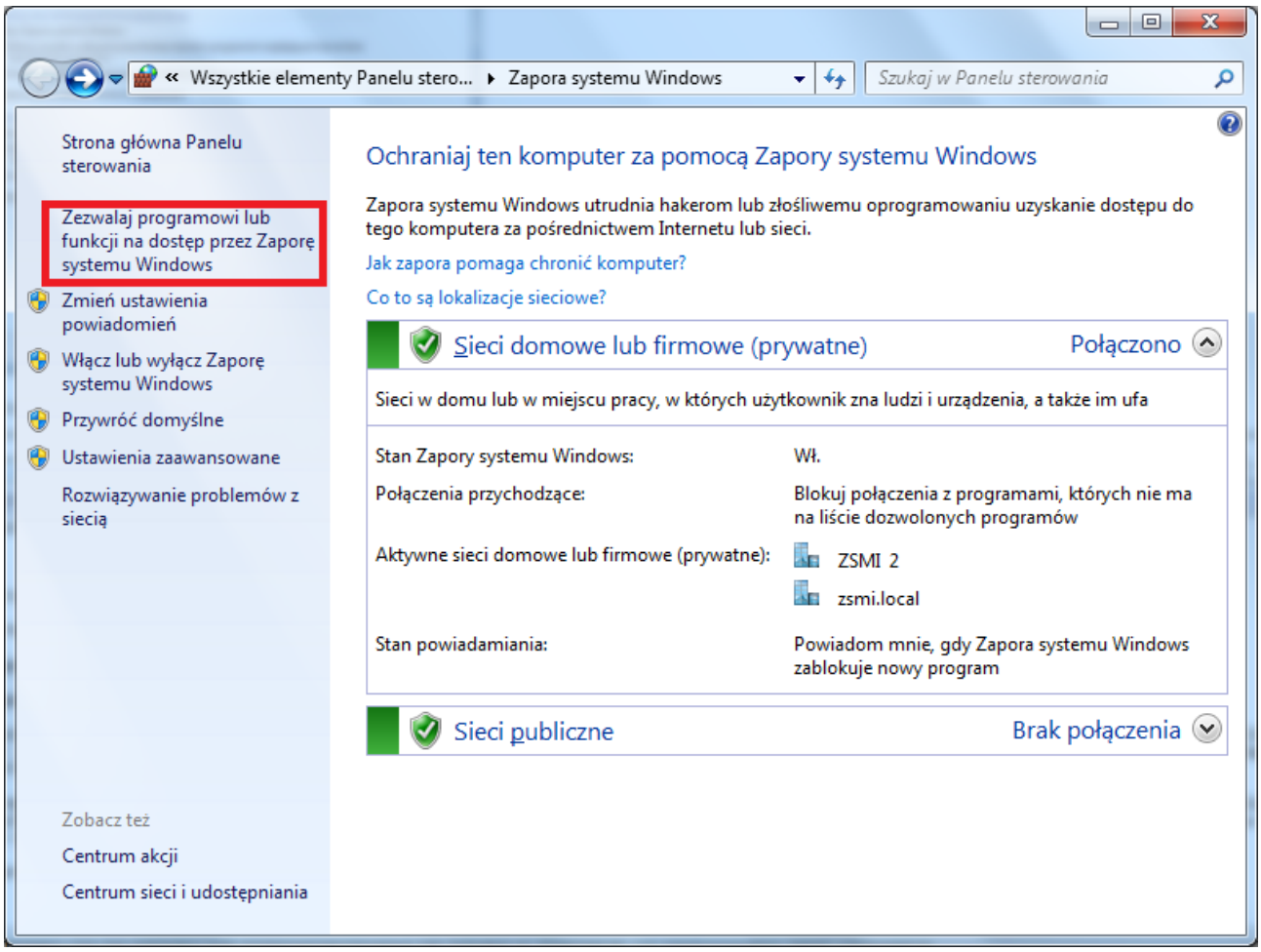
Włączany Panel Sterowania => Zapora systemu Windows

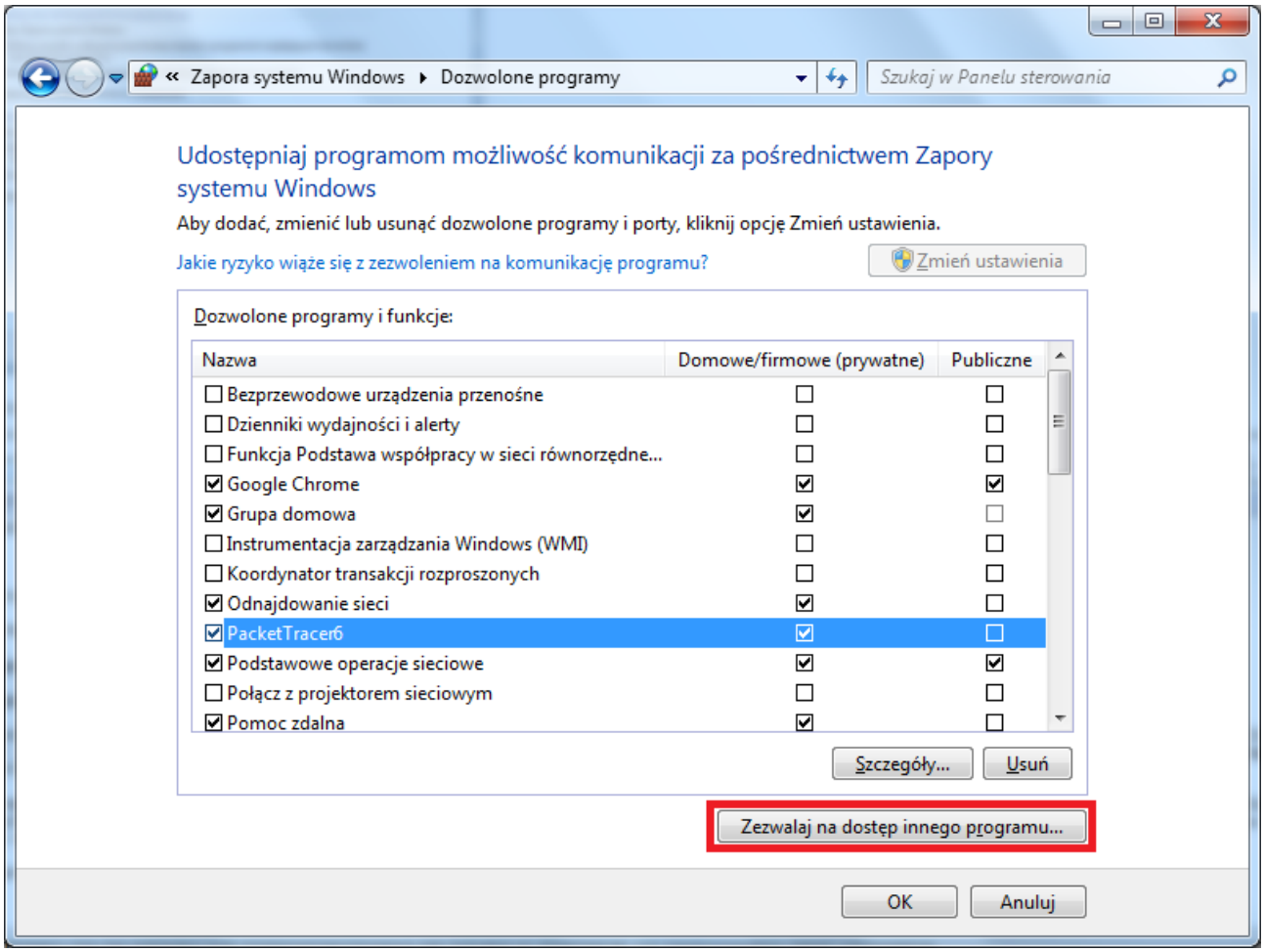




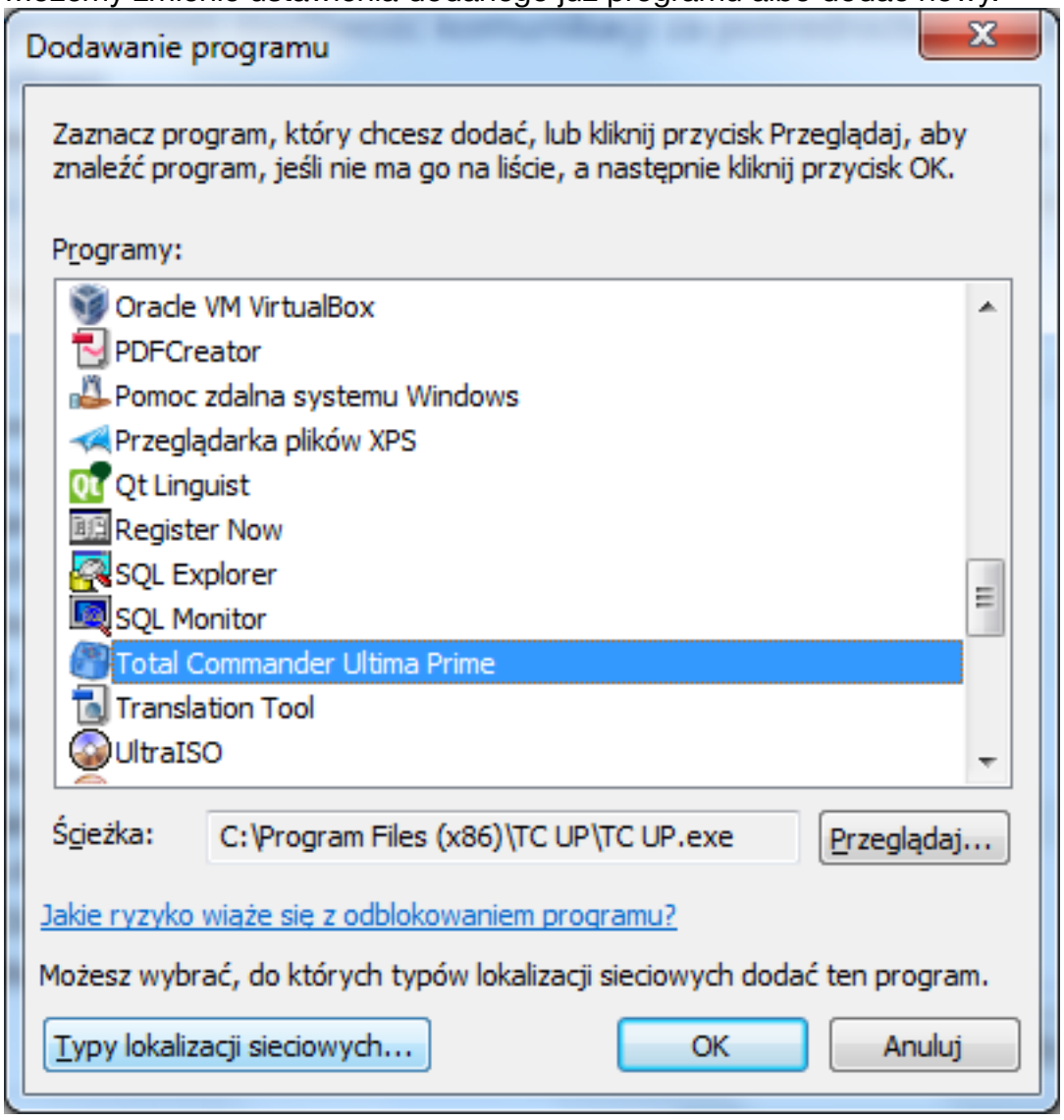
Zapora systemu Windows ma osobne ustawienia dla 3 profili: domenowego, prywatnego (sieć domowa lub firmowa), publicznego. Zapora domyślnie jest włączona. A jej wyłączenie nie jest zalecane. Domyślnie również zaznaczona jest opcja "powiadom mnie, gdy zapora systemu Windows zablokuje nowy program".
Istnieje możliwość zaznaczenia opcji "blokuj wszystkie połączenia przychodzące łącznie z programami znajdującymi się na liście dozwolonych programów". Używamy tego, gdy potrzebna jest maksymalna ochrona komputera, gdy łączymy się z siecią publiczną w niepewnym miejscu.

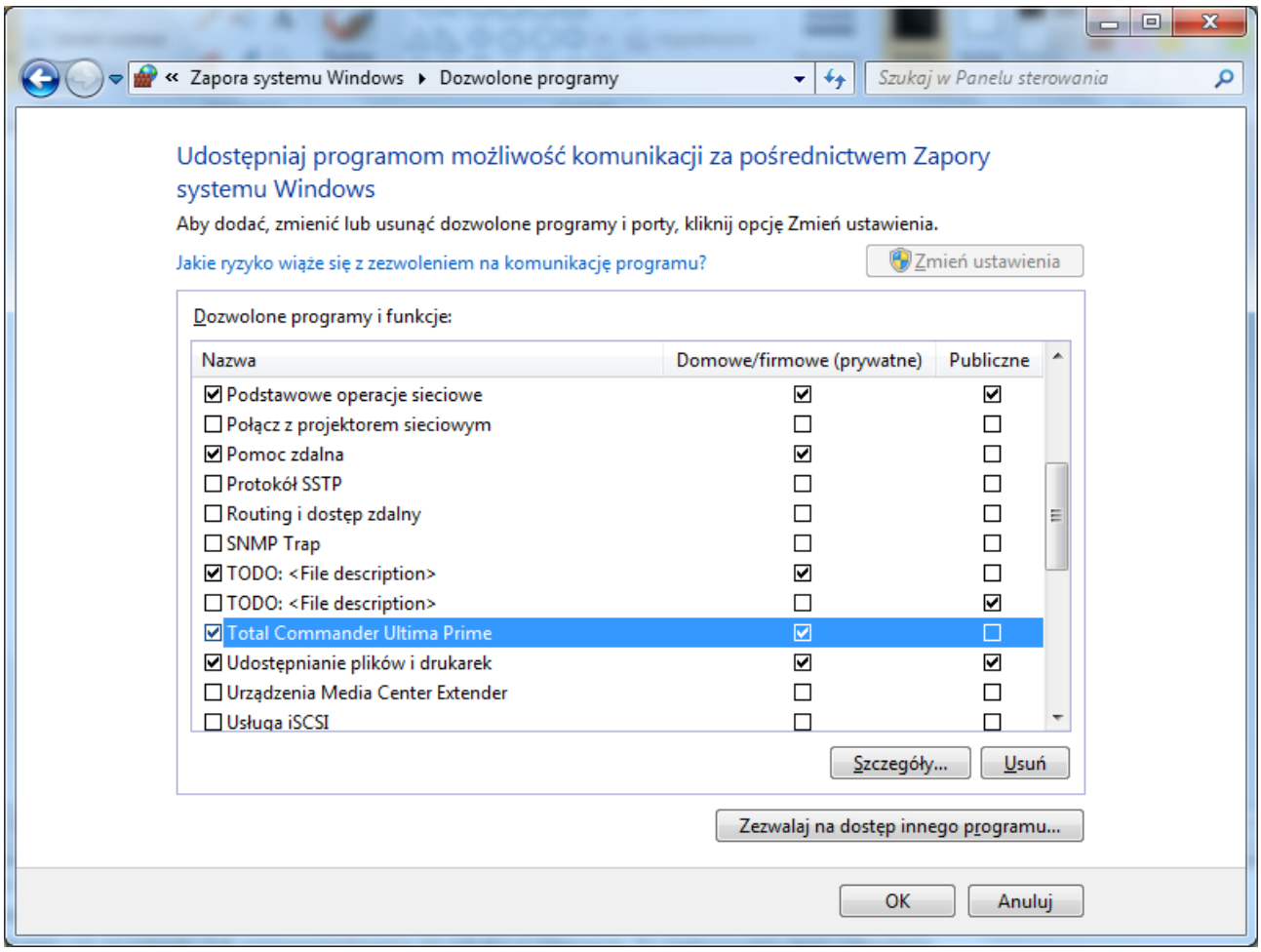
Zezwalanie programowi na komunikowanie się przez Zaporę systemu Windows


« Wszystkie elementy Panelu stero... ▸ Zapora systemu Windows
Szukaj w Panelu sterowania
Strona główna Panelu sterowania
Zezwalaj programowi lub funkcji na dostęp przez Zaporę systemu Windows
Zmień ustawienia powiadomień
Włącz lub wyłącz Zaporę systemu Windows
Przywróć domyślne
Ustawienia zaawansowane
Rozwiązywanie problemów z siecią
Zobacz też
Centrum akcji
Centrum sieci i udostępniania
Ochraniaj ten komputer za pomocą Zapory systemu Windows
Zapora systemu Windows utrudnia hakerom lub złośliwemu oprogramowaniu uzyskanie dostępu do tego komputera za pośrednictwem Internetu lub sieci.
Jak zapora pomaga chronić komputer?
Co to są lokalizacje sieciowe?
Sieci domowe lub firmowe (prywatne)
Połączono
Sieci w domu lub w miejscu pracy, w których użytkownik zna ludzi i urządzenia, a także im ufa
Stan Zapory systemu Windows:
Wł.
Połączenia przychodzące:
Blokuj połączenia z programami, których nie ma na liście dozwolonych programów
Aktywne sieci domowe lub firmowe (prywatne):
ZSMI 2
zsmi.local
Stan powiadamiania:
Powiadom mnie, gdy Zapora systemu Windows zablokuje nowy program
Sieci publiczne
Brak połączenia

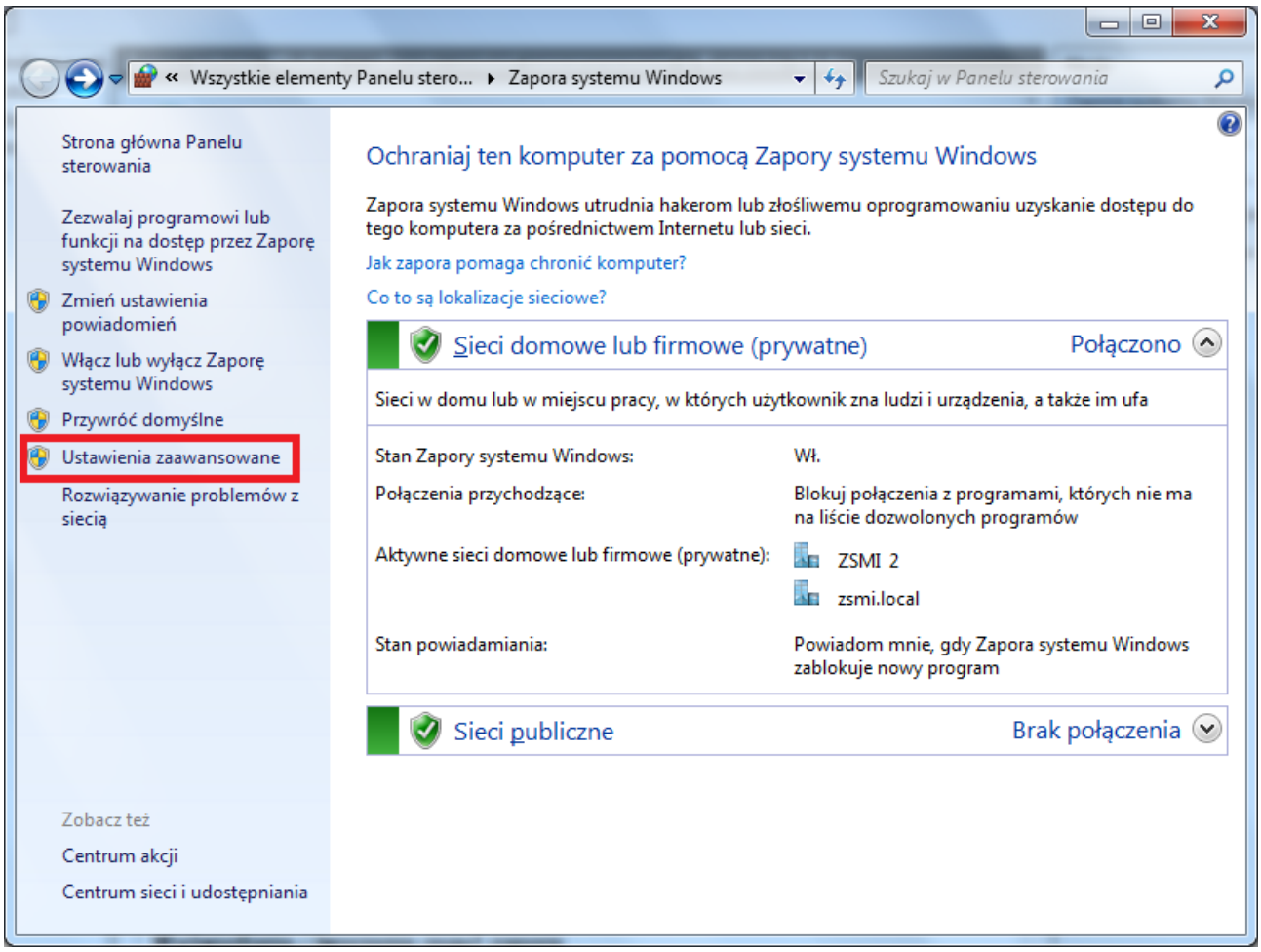

« Zapora systemu Windows ▸ Dozwolone programy
Szukaj w Panelu sterowania
Udostępniaj programom możliwość komunikacji za pośrednictwem Zapory systemu Windows
Aby dodać, zmienić lub usunąć dozwolone programy i porty, kliknij opcję Zmień ustawienia.
Jakie ryzyko wiąże się z zezwoleniem na komunikację programu?
Zmień ustawienia
Dozwolone programy i funkcje:
Nazwa
Domowe/firmowe (prywatne)
Publiczne
Bezprzewodowe urządzenia przenośne
Dzienniki wydajności i alerty
Funkcja Podstawa współpracy w sieci równorzędne...
Google Chrome
Grupa domowa
Instrumentacja zarządzania Windows (WMI)
Koordynator transakcji rozproszonych
Odnajdowanie sieci
PacketTracer6
Podstawowe operacje sieciowe
Połącz z projektorem sieciowym
Pomoc zdalna
Szczegóły...
Usuń
Zezwalaj na dostęp innego programu...
OK
Anuluj

Możemy zmienić ustawienia dodanego już programu albo dodać nowy.

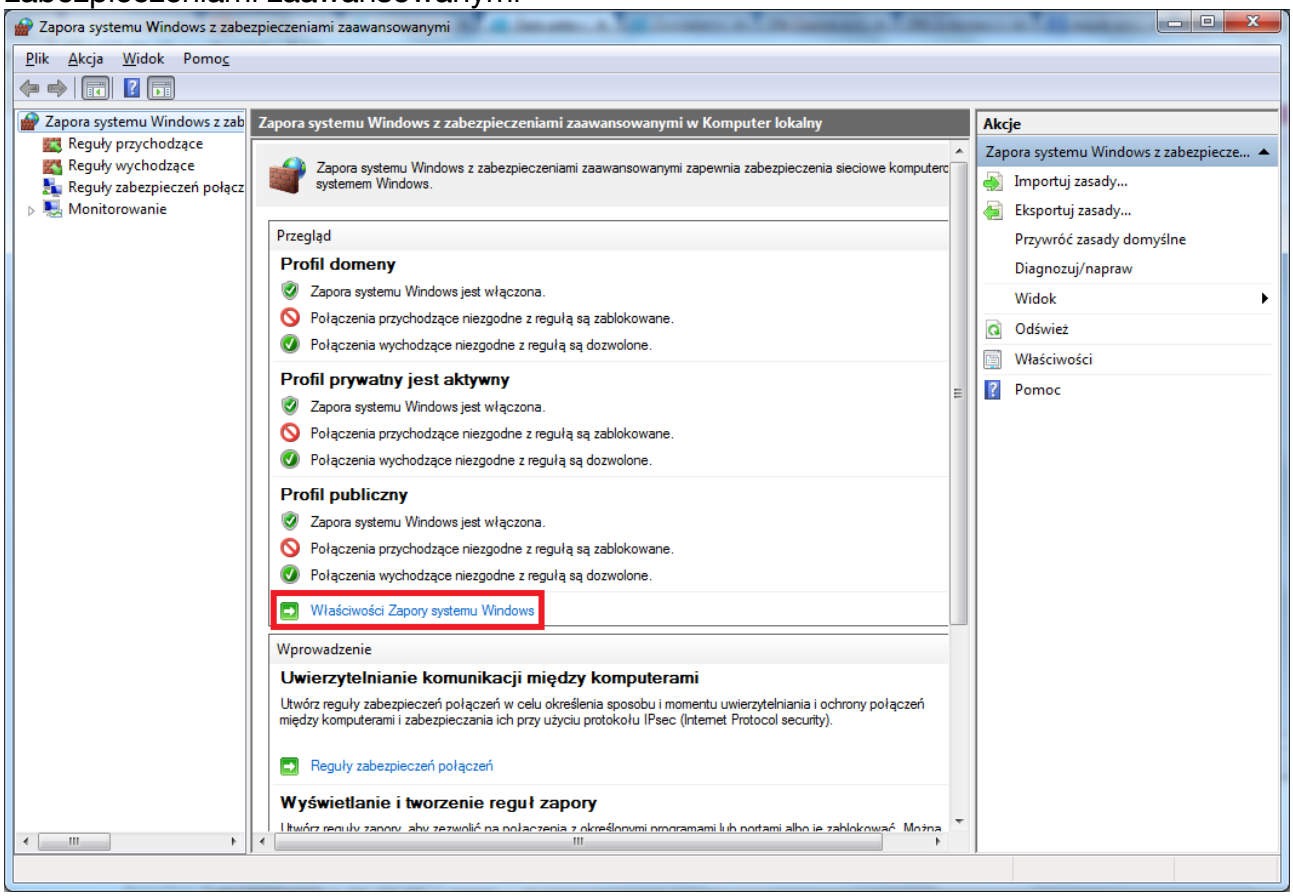




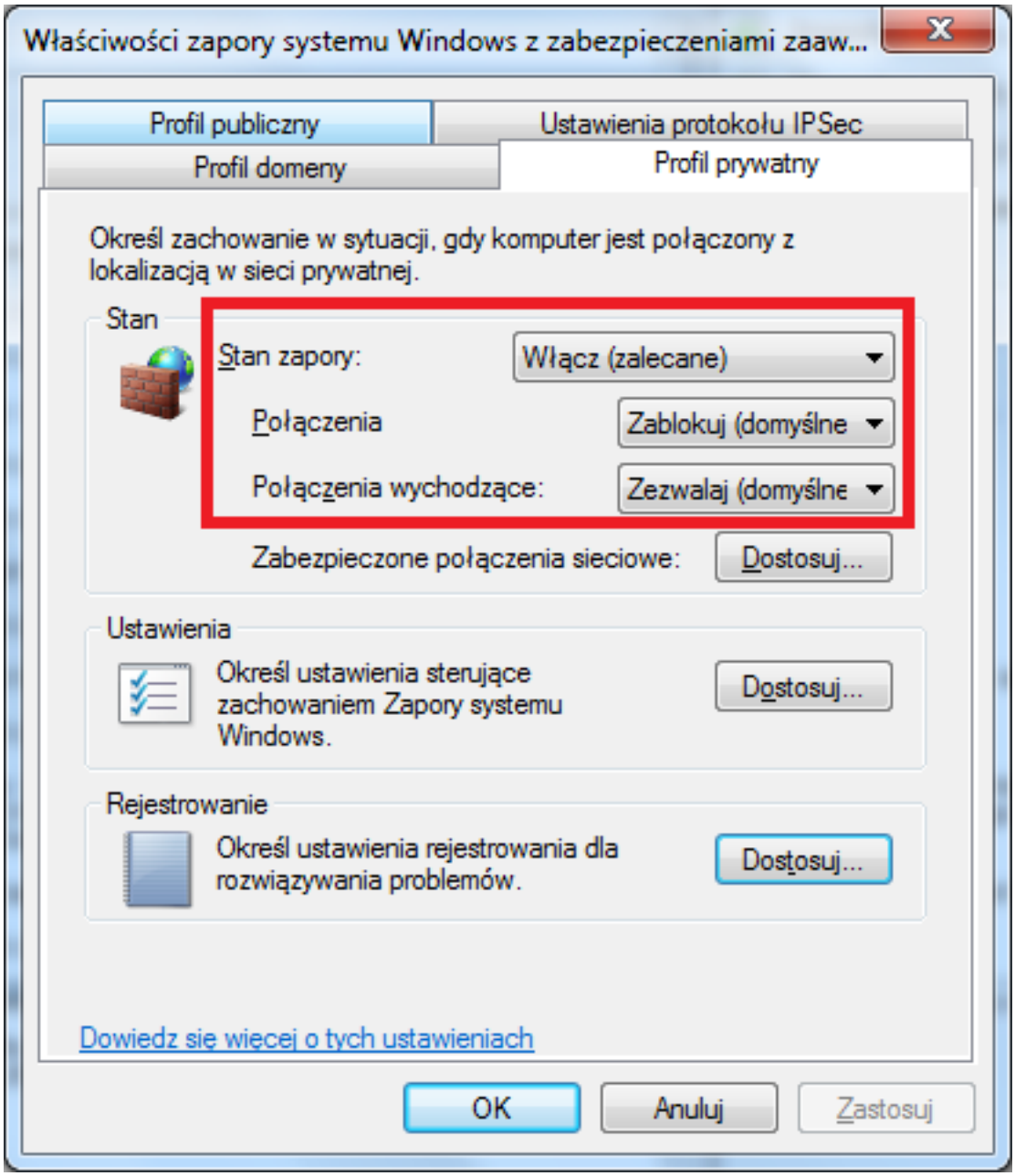
Zapora systemu Windows z zabezpieczeniami zaawansowanymi



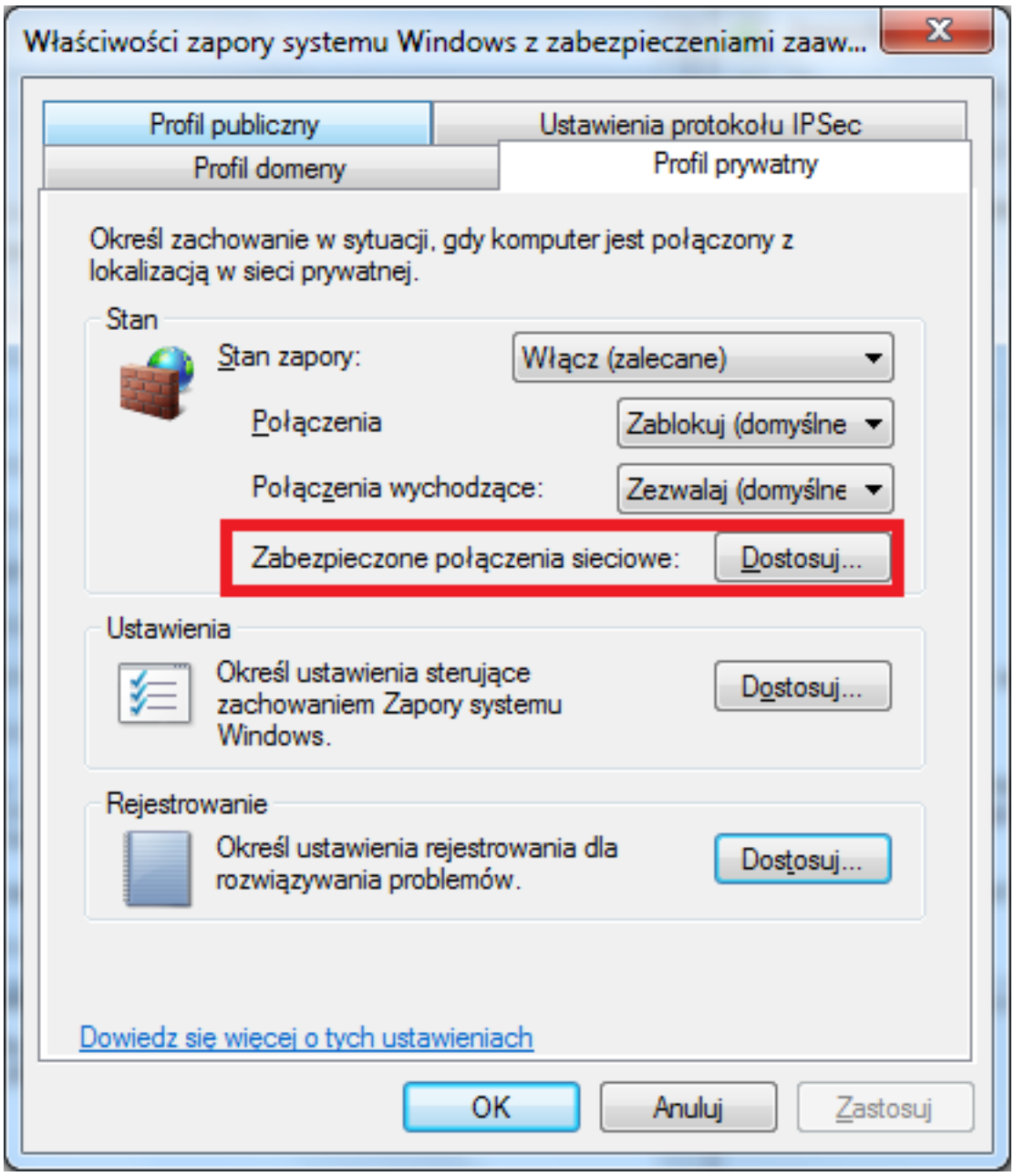
Wchodzimy w ustawienia zaawansowane, pojawia się Zapora systemu Windows z zabezpieczeniami zaawansowanymi

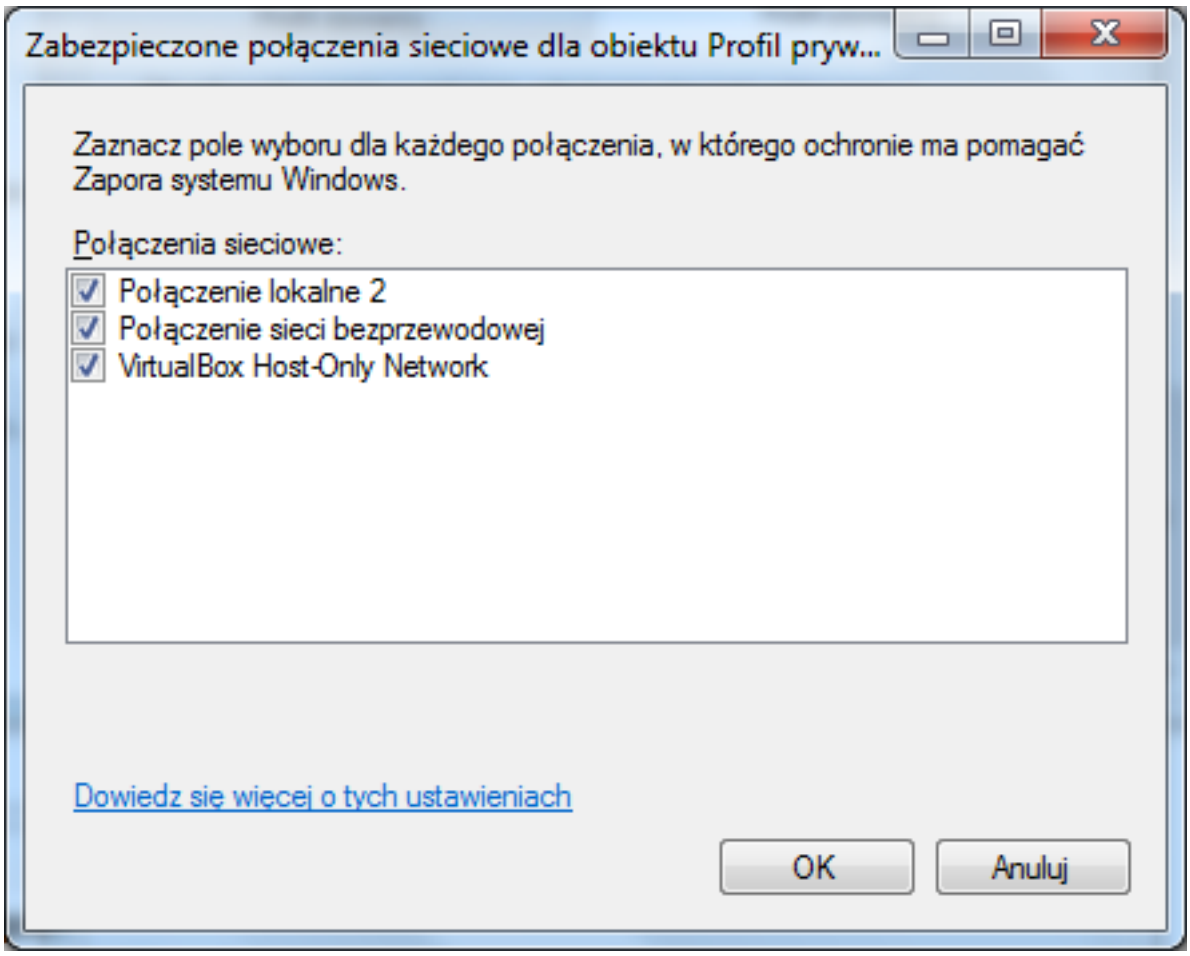


Zapora systemu Windows ma osobne ustawienia dla 3 profili: domenowego, prywatnego (sieć domowa lub firmowa), publicznego. Zapora domyślnie jest włączona. Połączenia przychodzące niezgodne z regułą są zablokowane. Połączenia wychodzące niezgodne z regułą są dozwolone. Te ustawienia można zmienić poprzez właściwości zapory systemu Windows.

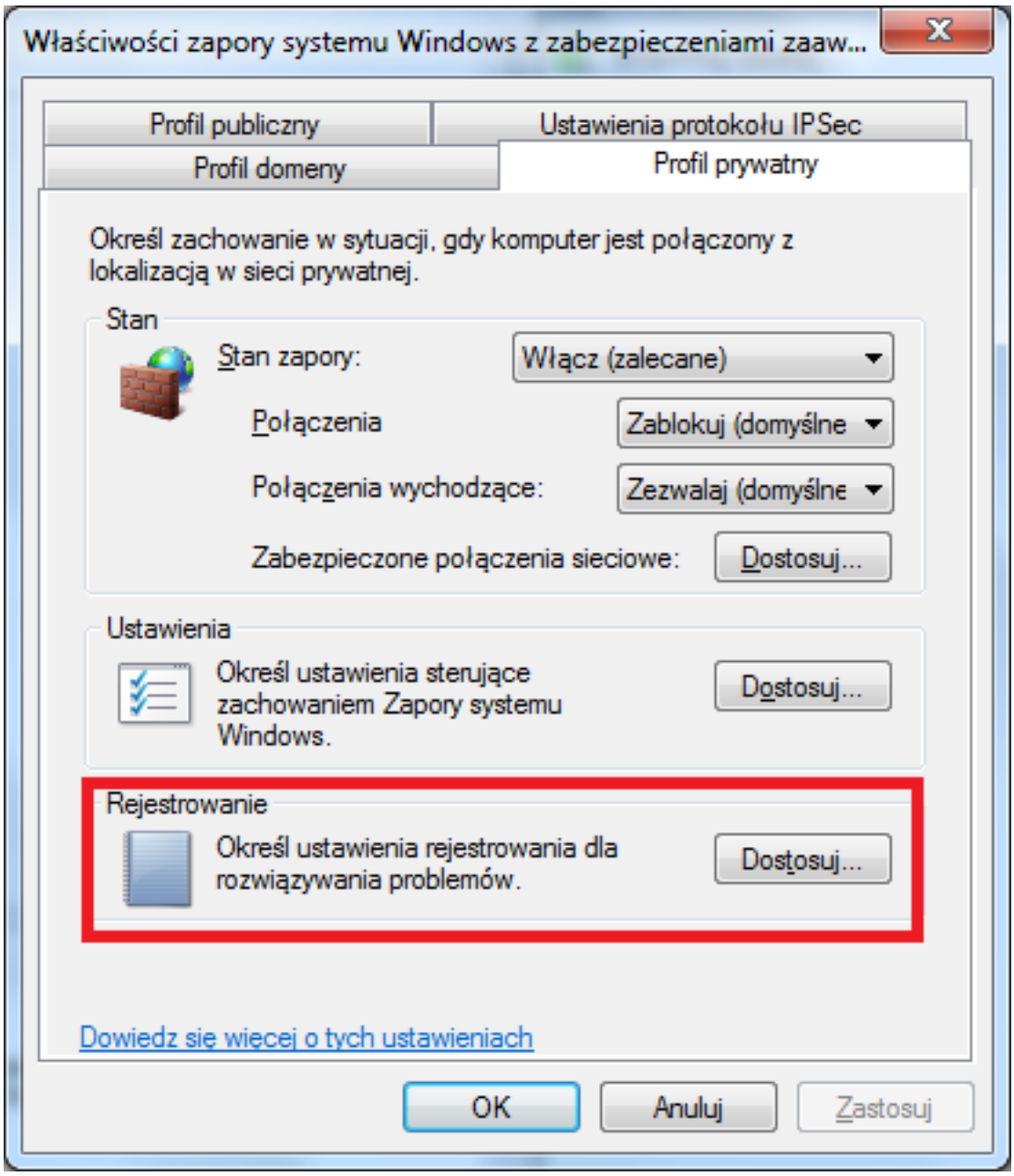


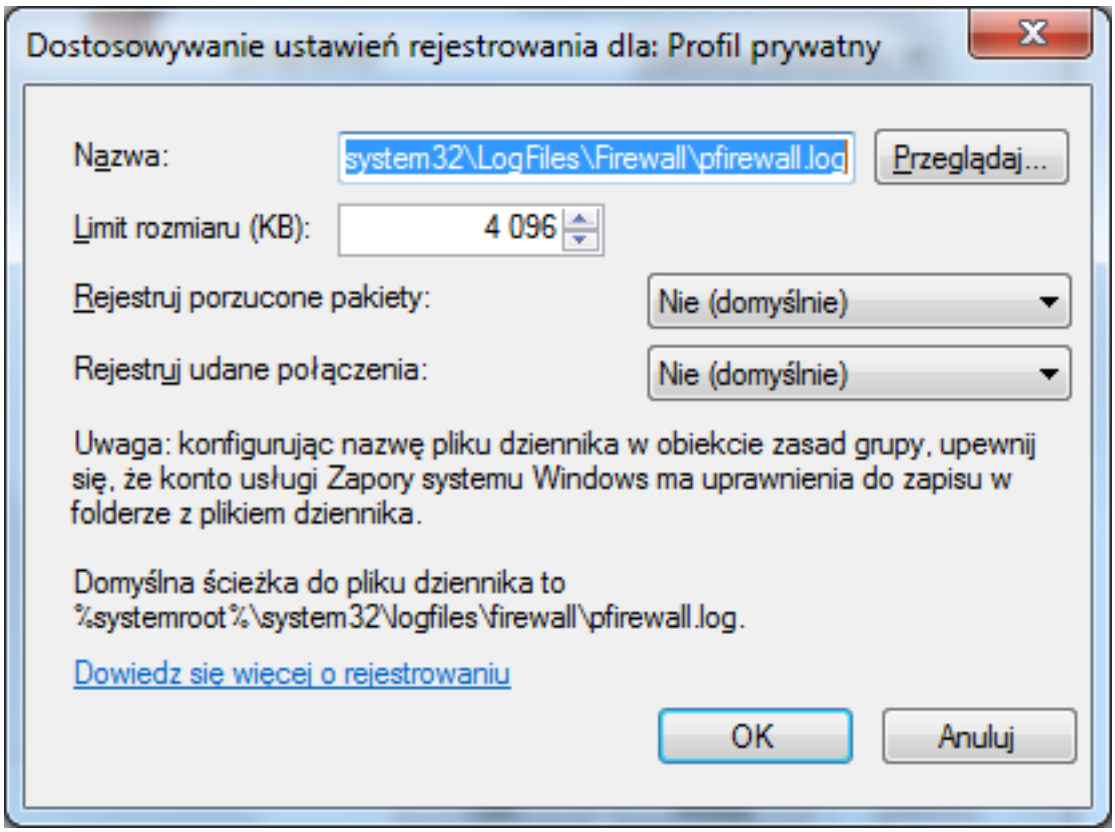
Możemy określić, połączenia jakich kart sieciowych będą chronione.


Właściwości zapory systemu Windows z zabezpieczeniami zaaw...
Profil publiczny
Ustawienia protokołu IPSec
Profil domeny
Profil prywatny
Określ zachowanie w sytuacji, gdy komputer jest połączony z lokalizacją w sieci prywatnej.
Stan
Stan zapory:
Włącz (zalecane)
Połączenia
Zablokuj (domyślne
Połączenia wychodzące:
Zezwalaj (domyślne
Zabezpieczone połączenia sieciowe:
Dostosuj...
Ustawienia
Określ ustawienia sterujące zachowaniem Zapory systemu Windows.
Dostosuj...
Rejestrowanie
Określ ustawienia rejestrowania dla rozwiązywania problemów.
Dostosuj...
Dowiedz się więcej o tych ustawieniach
OK
Anuluj
Zastosuj



Połączenia sieciowe można rejestrować. Dziennik tworzony jest w lokalizacji %systemroot%\system32\LogFiles\Firewall\pfirewall.log. Jak widać domyślnie połączenia nie są logowane.

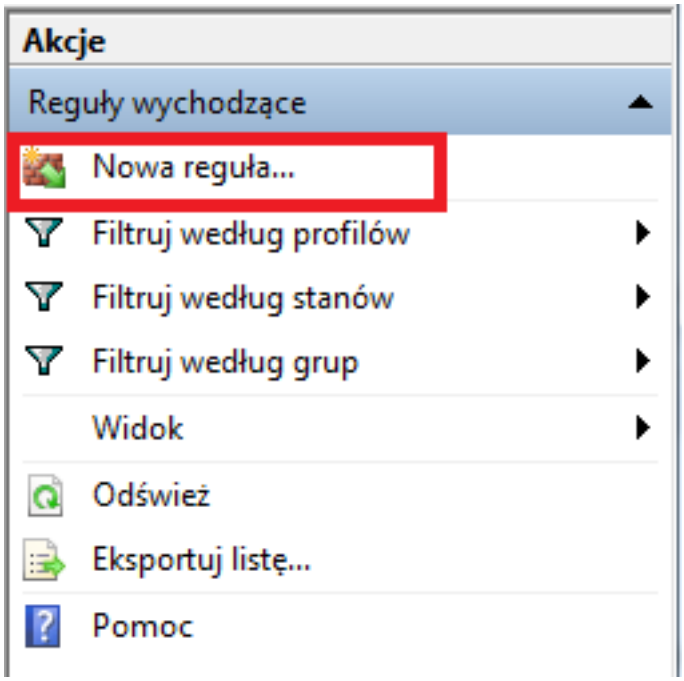

Właściwości zapory systemu Windows z zabezpieczeniami zaaw...
Profil publiczny
Ustawienia protokołu IPSec
Profil domeny
Profil prywatny
Określ zachowanie w sytuacji, gdy komputer jest połączony z lokalizacją w sieci prywatnej.
Stan
Stan zapory:
Włącz (zalecane)
Połączenia
Zablokuj (domyślne
Połączenia wychodzące:
Zezwalaj (domyślne
Zabezpieczone połączenia sieciowe:
Dostosuj...
Ustawienia
Określ ustawienia sterujące zachowaniem Zapory systemu Windows.
Dostosuj...
Rejestrowanie
Określ ustawienia rejestrowania dla rozwiązywania problemów.
Dostosuj...
Dowiedz się więcej o tych ustawieniach
OK
Anuluj
Zastosuj

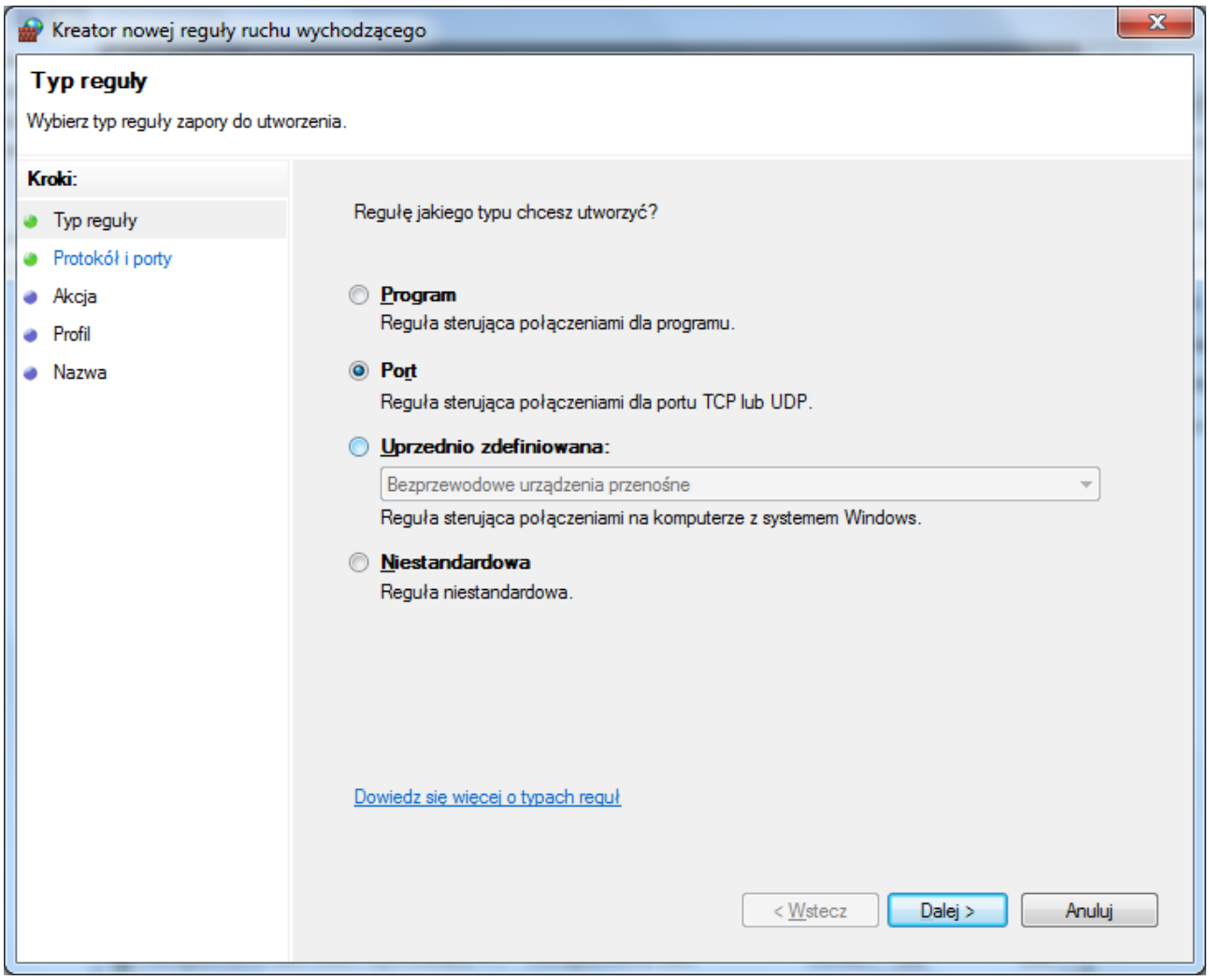


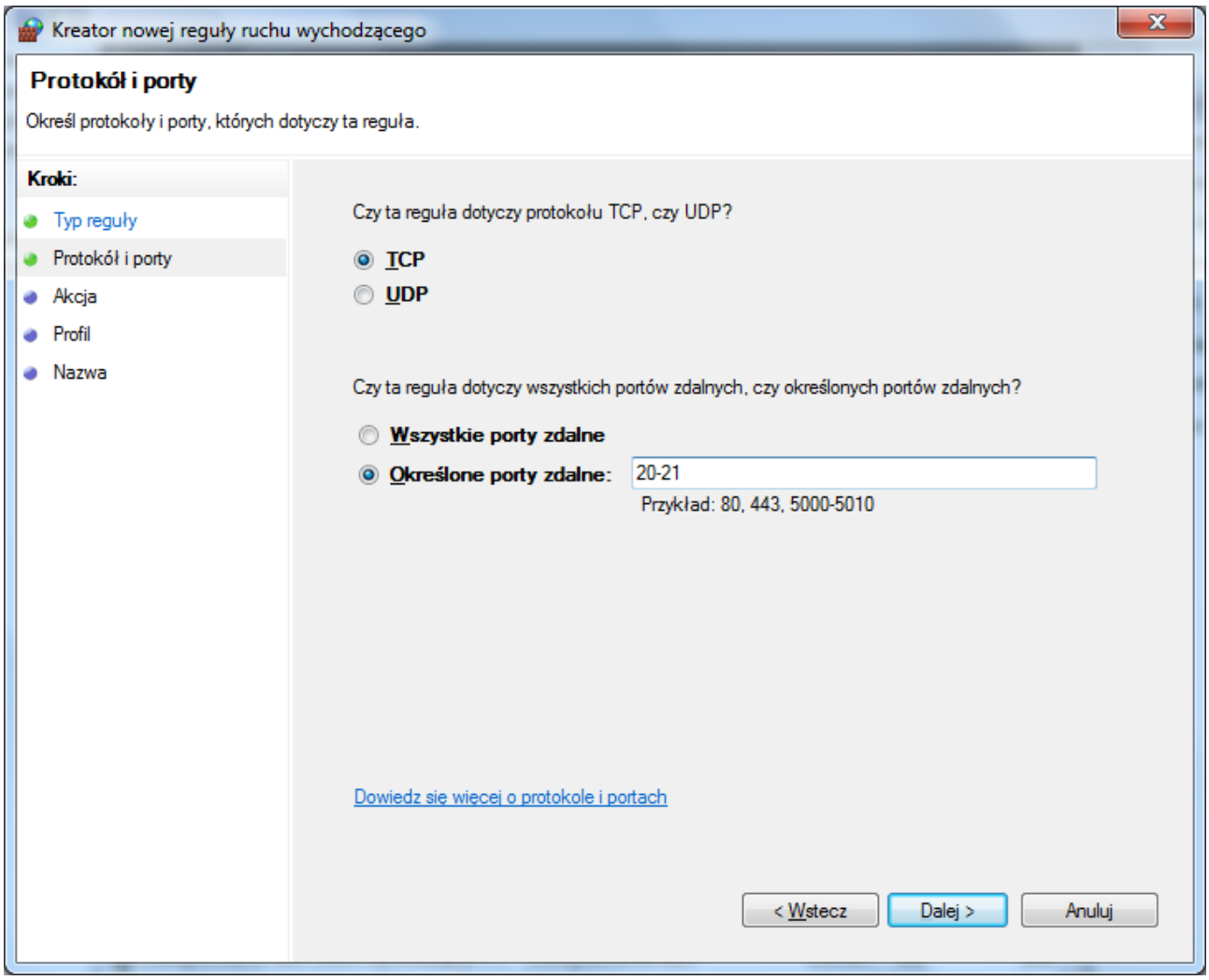
Dodanie reguły

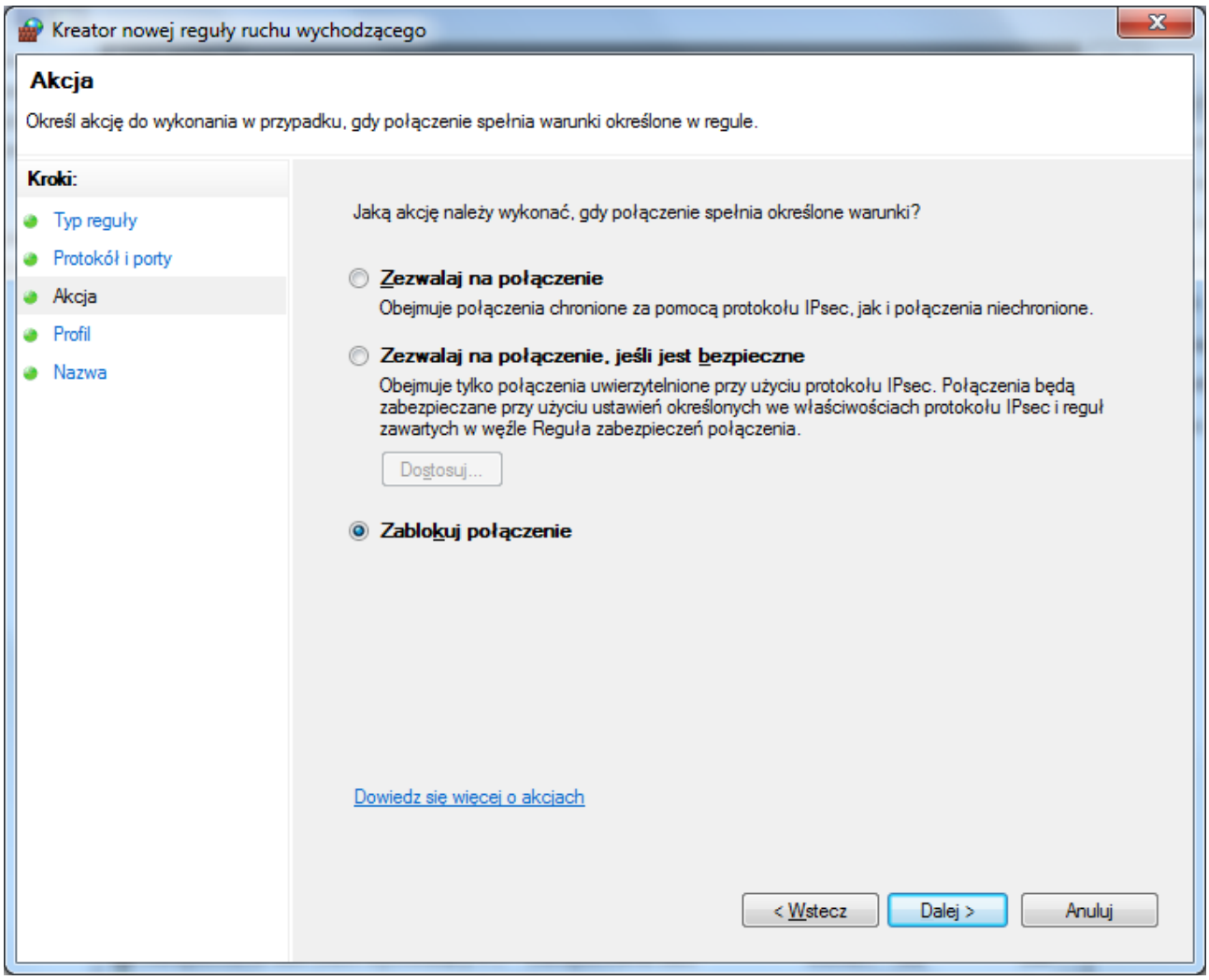
Wchodząc w Zaporę systemu Windows z zabezpieczeniami zaawansowanymi widzimy zdefiniowane reguły przychodzące i wychodzące. Możemy je edytować, usuwać, dodawać nowe.

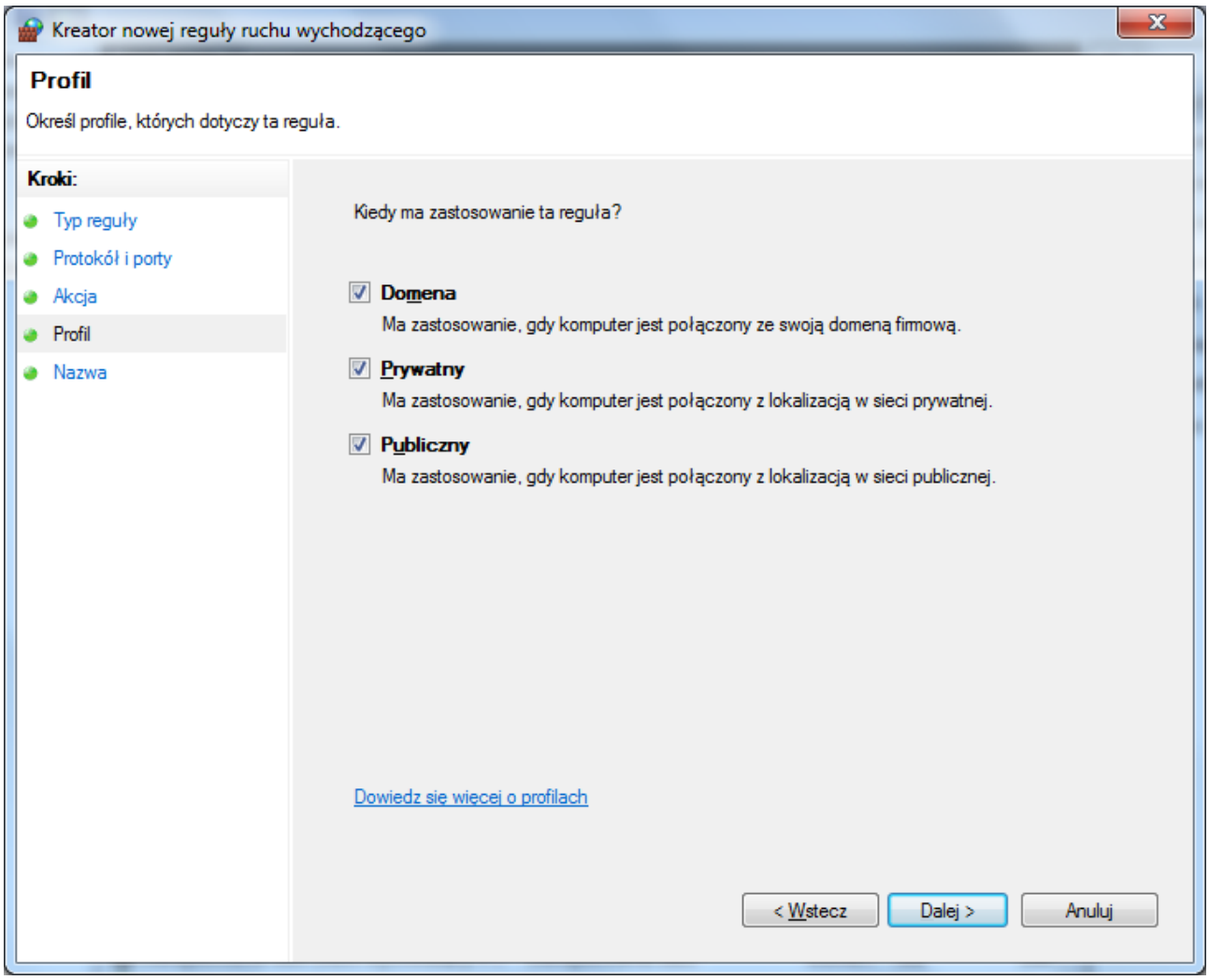
Poniżej pokazano dodanie nowej reguły wychodzącej do blokowania połączeń z serwerem FTP

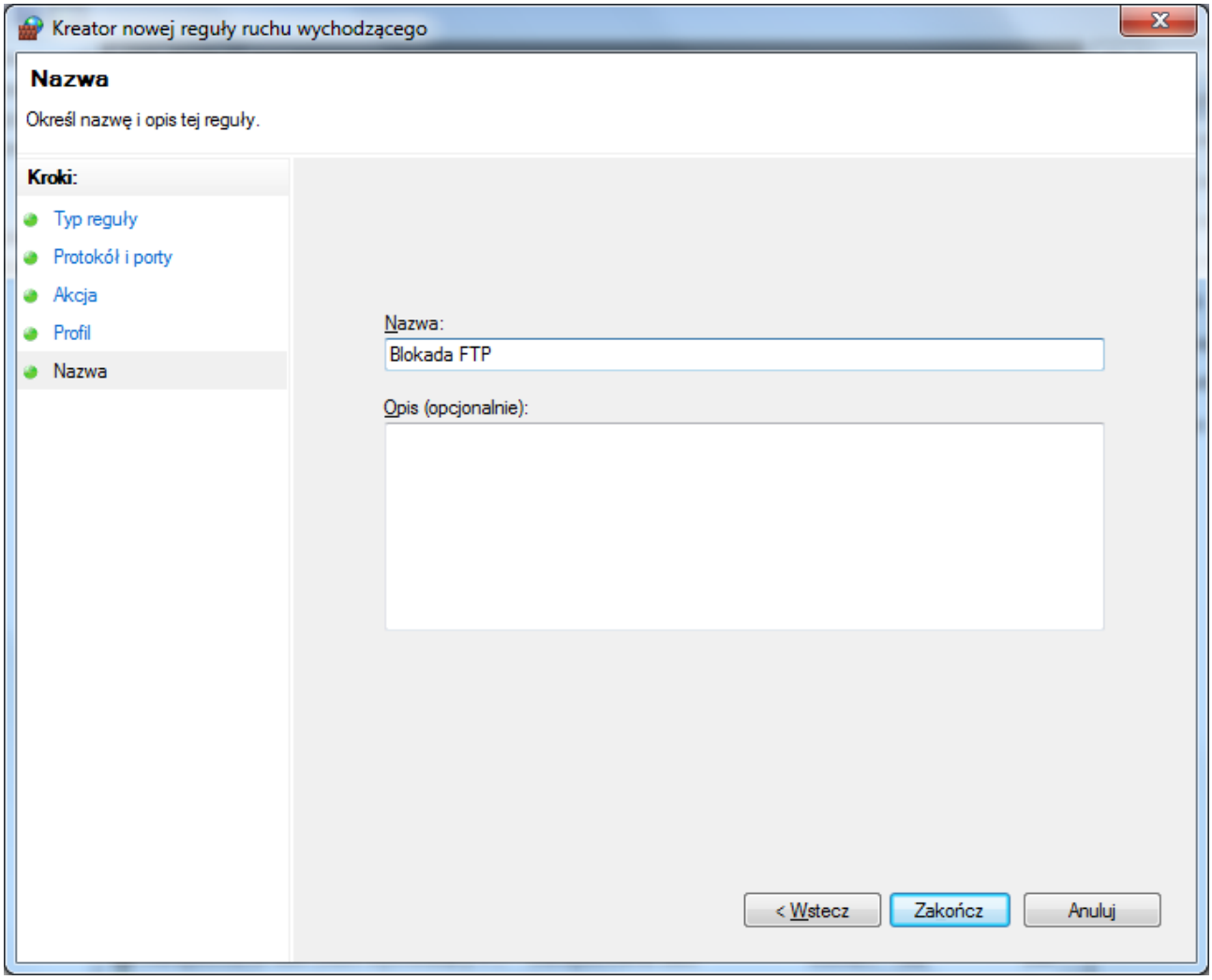



Kreator nowej reguły ruchu wychodzącego
Typ reguły
Wybierz typ reguły zapory do utworzenia.
Kroki:
Typ reguły
Protokół i porty
Akcja
Profil
Nazwa
Regułę jakiego typu chcesz utworzyć?
Program
Reguła sterująca połączeniami dla programu.
Port
Reguła sterująca połączeniami dla portu TCP lub UDP.
Uprzednio zdefiniowana:
Bezprzewodowe urządzenia przenośne
Reguła sterująca połączeniami na komputerze z systemem Windows.
Niestandardowa
Reguła niestandardowa.
Dowiedz się więcej o typach reguł
< Wstecz
Dalej >
Anuluj

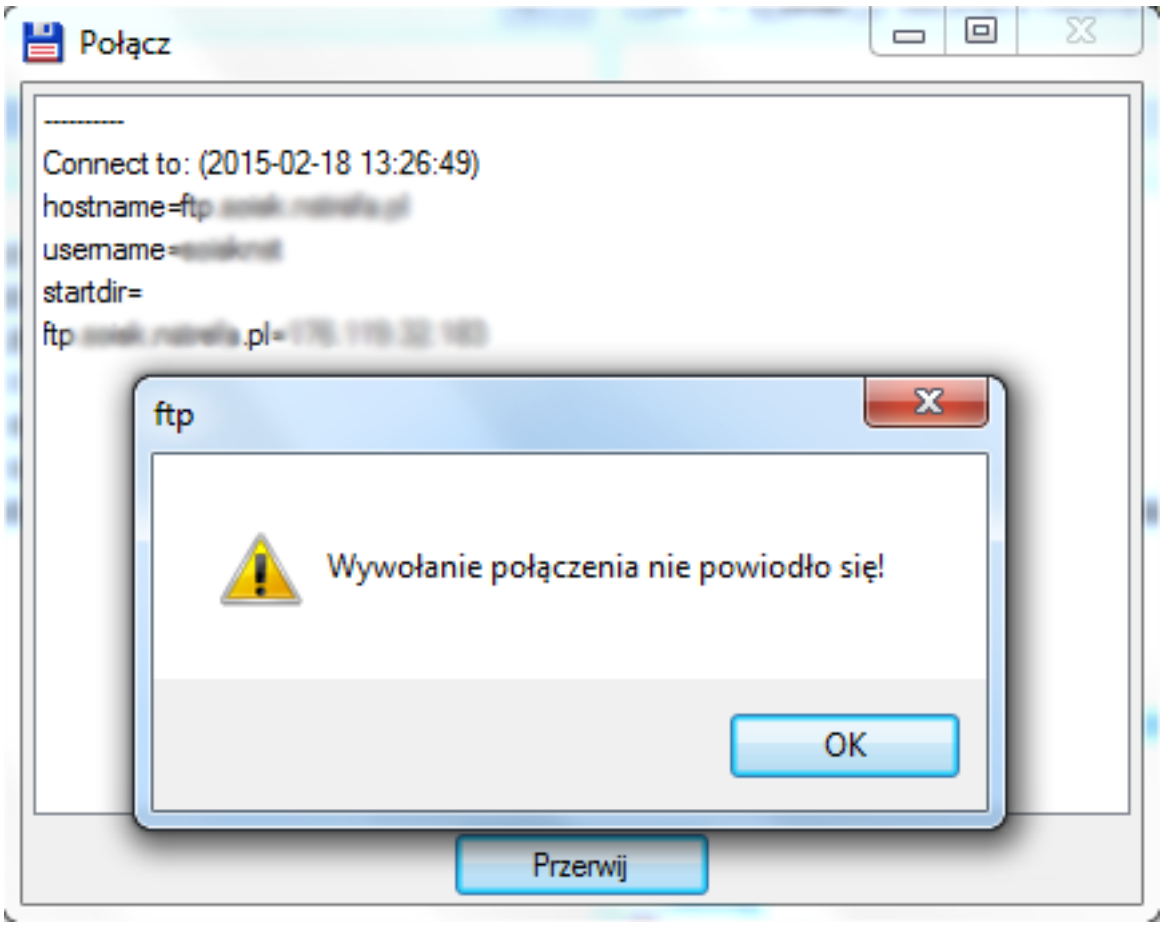

Kreator nowej reguły ruchu wychodzącego
Protokół i porty
Określ protokoły i porty, których dotyczy ta reguła.
Kroki:
Typ reguły
Protokół i porty
Akcja
Profil
Nazwa
Czy ta reguła dotyczy protokołu TCP, czy UDP?
TCP
UDP
Czy ta reguła dotyczy wszystkich portów zdalnych, czy określonych portów zdalnych?
Wszystkie porty zdalne
Określone porty zdalne:
20-21
Przykład: 80, 443, 5000-5010
Dowiedz się więcej o protokole i portach
< Wstecz
Dalej >
Anuluj


Kreator nowej reguły ruchu wychodzącego
Akcja
Określ akcję do wykonania w przypadku, gdy połączenie spełnia warunki określone w regule.
Kroki:
Typ reguły
Protokół i porty
Akcja
Profil
Nazwa
Jaką akcję należy wykonać, gdy połączenie spełnia określone warunki?
Zezwalaj na połączenie
Obejmuje połączenia chronione za pomocą protokołu IPsec, jak i połączenia niechronione.
Zezwalaj na połączenie, jeśli jest bezpieczne
Obejmuje tylko połączenia uwierzytelnione przy użyciu protokołu IPsec. Połączenia będą zabezpieczane przy użyciu ustawień określonych we właściwościach protokołu IPsec i reguł zawartych w węźle Reguła zabezpieczeń połączenia.
Dostosuj...
Zablokuj połączenie
Dowiedz się więcej o akcjach
< Wstecz
Dalej >
Anuluj


Kreator nowej reguły ruchu wychodzącego
Profil
Określ profile, których dotyczy ta reguła.
Kroki:
Typ reguły
Protokół i porty
Akcja
Profil
Nazwa
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.
Dowiedz się więcej o profilach
< Wstecz
Dalej >
Anuluj

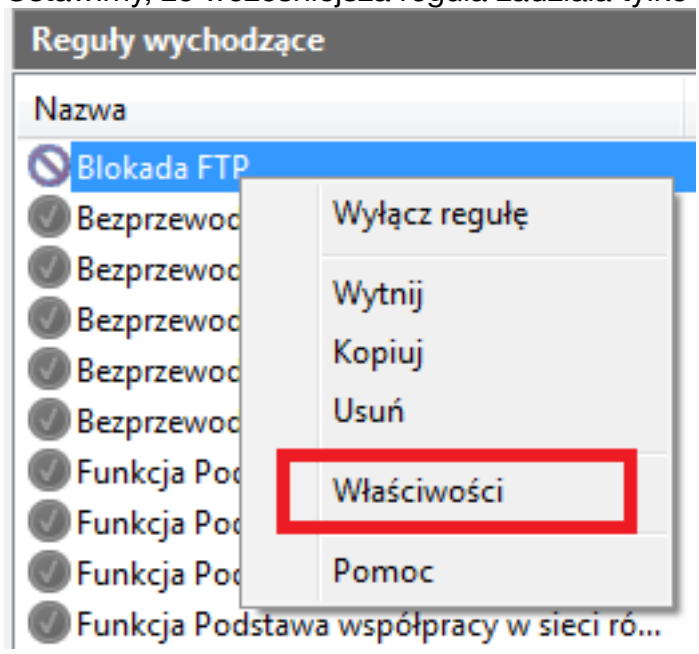


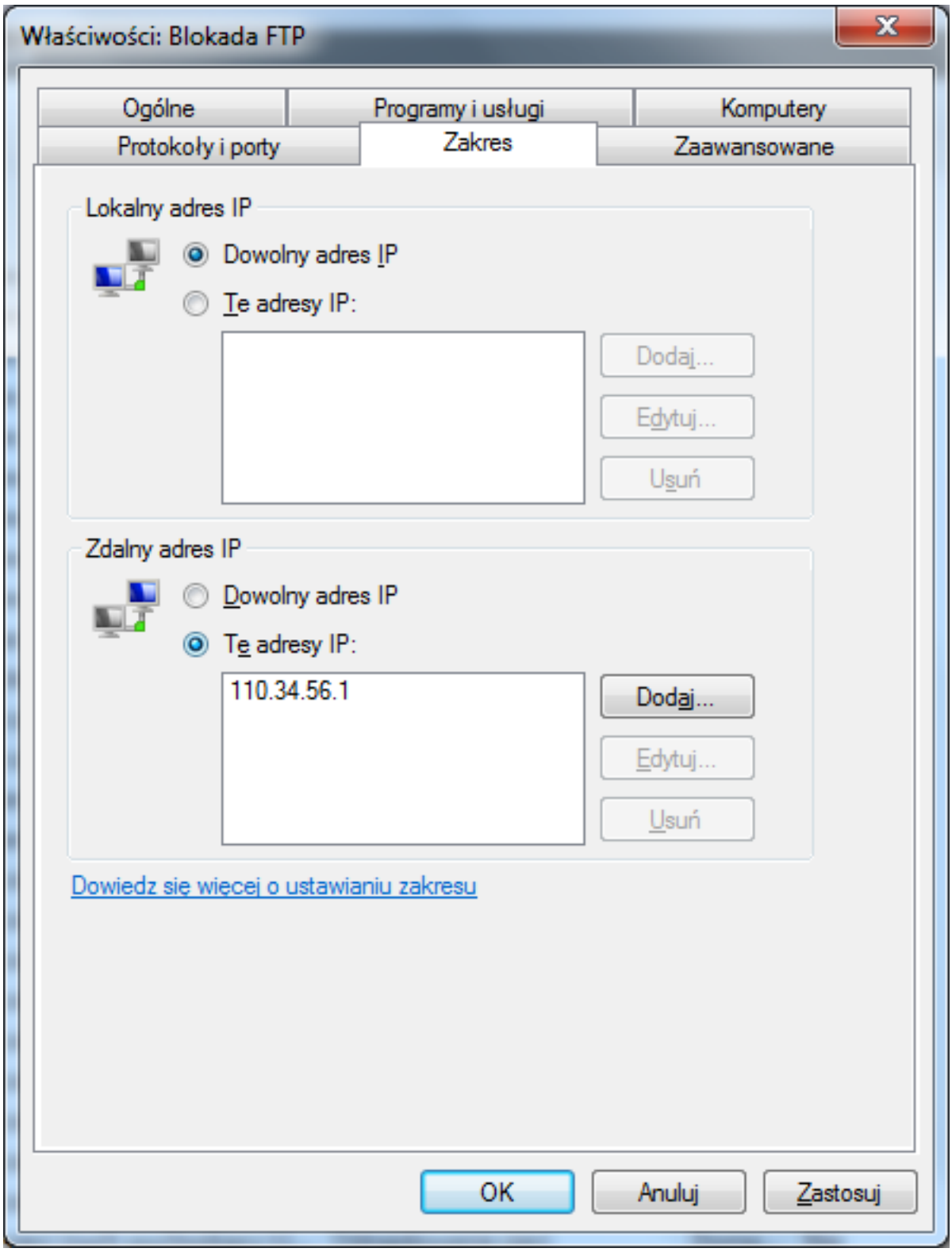
Jak widać wszystko działa poprawnie



Edycja reguły

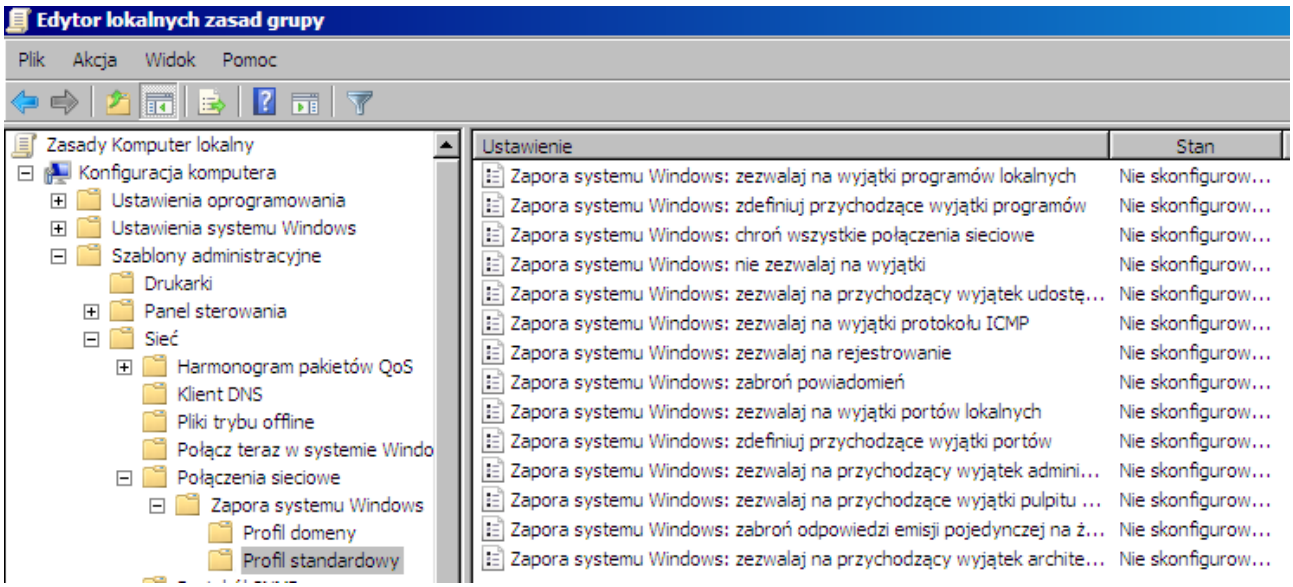
Ustawimy, że wcześniejsza reguła zadziała tylko na jeden adres IP.





Zapora w zasadach grupy

Ustawienia zapory dostępne są gpedit.msc => konfiguracja komputera => szablony administracyjne => sieć => połączenia sieciowe => zapora systemu Windows



Ćwiczenia

Zablokuj możliwość przeglądania stron internetowych

Zablokuj tylko soisk.info

Masz mieć możliwość przeglądania tylko strony soisk.info. Dostęp do innych stron ma być zablokowany.

Zablokuj możliwość testowania połączeń za pomocą polecenia ping.

Edytuj wcześniejszą regułę. Blokada ma działać tylko w zakresie całej sieci lokalnej.

Zablokuj możliwość korzystania z serwera DHCP.