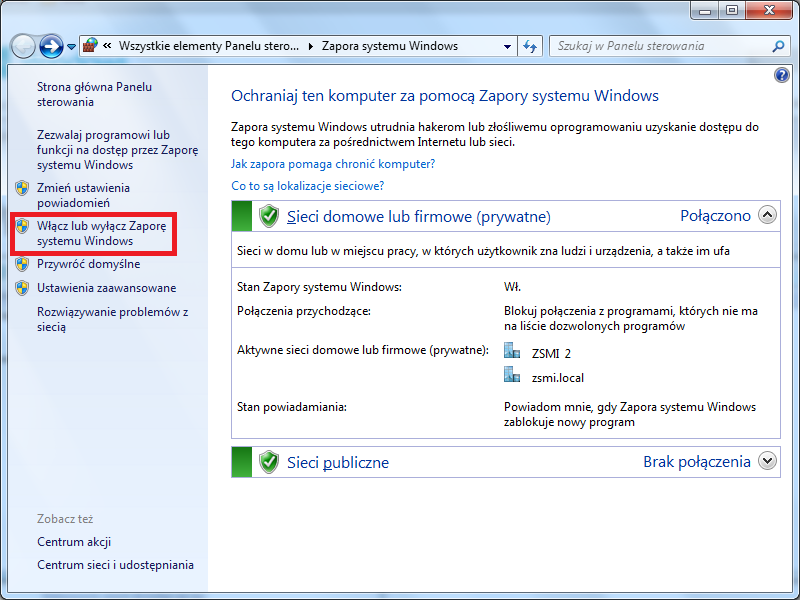
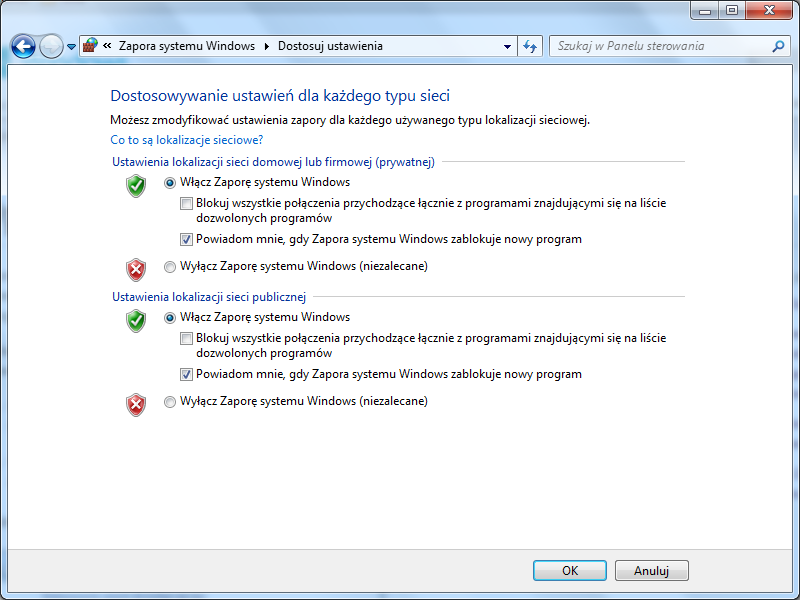
Włączanie lub wyłączanie zapory systemu Windows

Włączany Panel Sterowania => Zapora systemu Windows

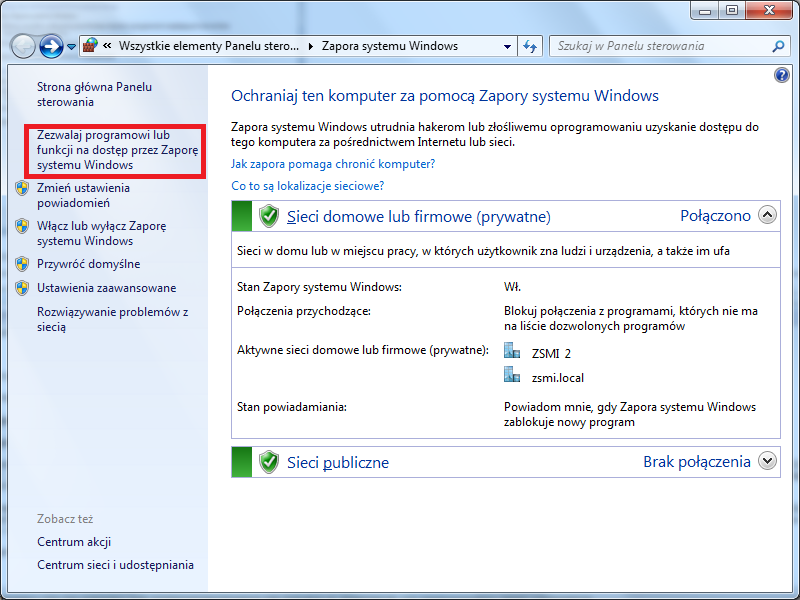
[](https://soisk.info/index.php/Plik:Zapora1.png)

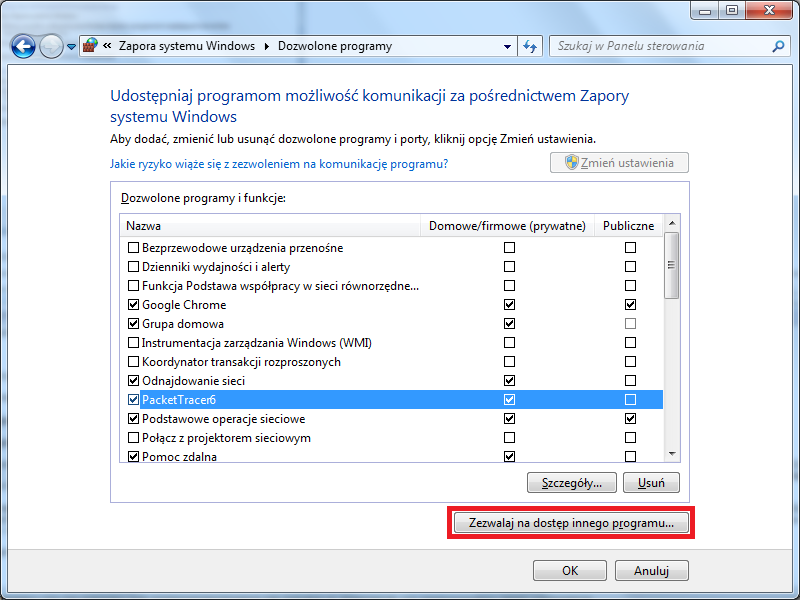
[](https://soisk.info/index.php/Plik:Zapora2.png)

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".

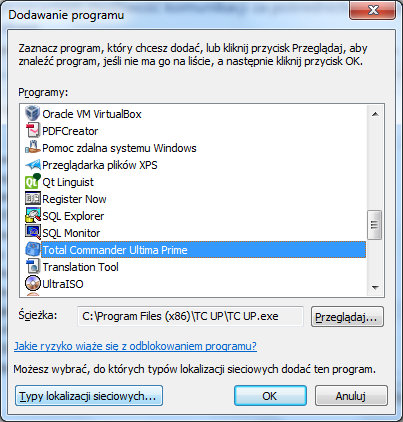
Istnieje możliwość zaznaczenia opcji "blokuj wszystkie połączenia przychodzące łącznie z programami znajdującymi się na liście dozwolonych programów". Używamy tego, gdy potrzebna jest maksymalna ochrona komputera, gdy łączymy się z siecią publiczną w niepewnym miejscu.

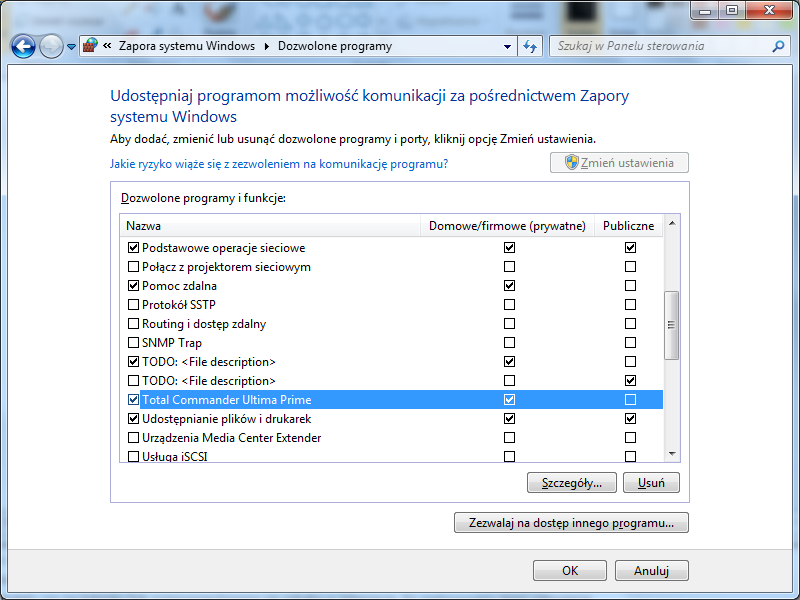
Zezwalanie programowi na komunikowanie się przez Zaporę systemu Windows

[](https://soisk.info/index.php/Plik:Zapora3.png)

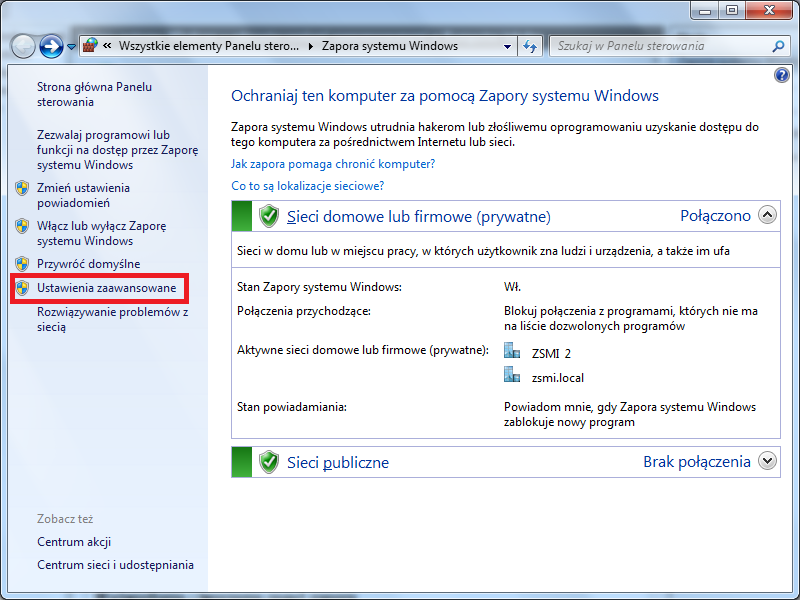
[](https://soisk.info/index.php/Plik:Zapora4.png)

Możemy zmienić ustawienia dodanego już programu albo dodać nowy.

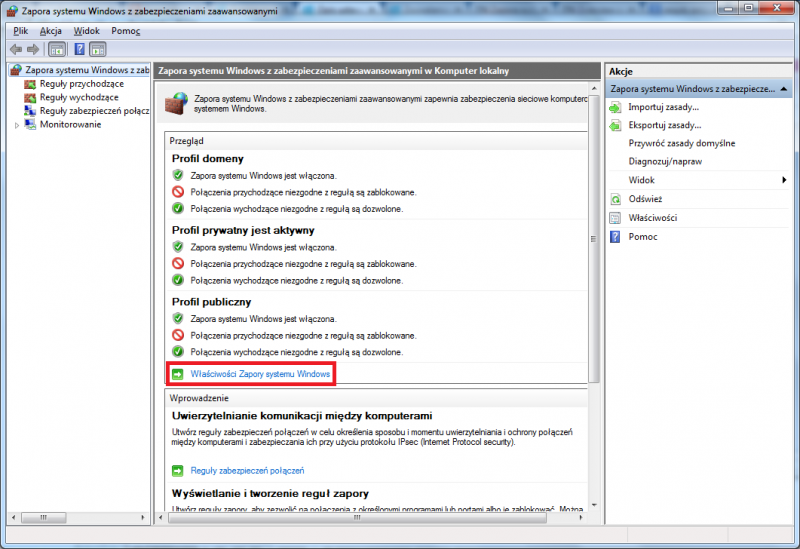
[](https://soisk.info/index.php/Plik:Zapora5.png)

[](https://soisk.info/index.php/Plik:Zapora6.png)

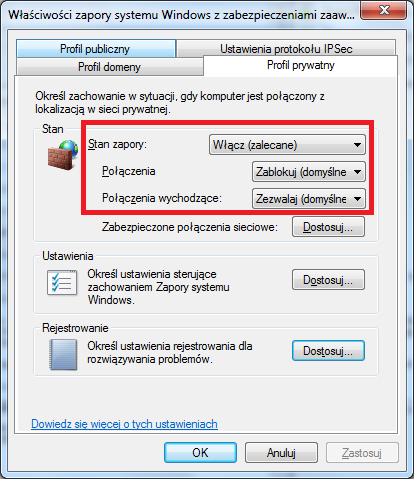
Zapora systemu Windows z zabezpieczeniami zaawansowanymi

[](https://soisk.info/index.php/Plik:Zapora7.png)

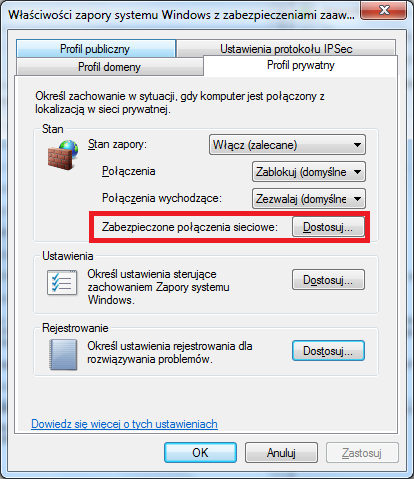
Wchodzimy w ustawienia zaawansowane, pojawia się Zapora systemu Windows z zabezpieczeniami zaawansowanymi

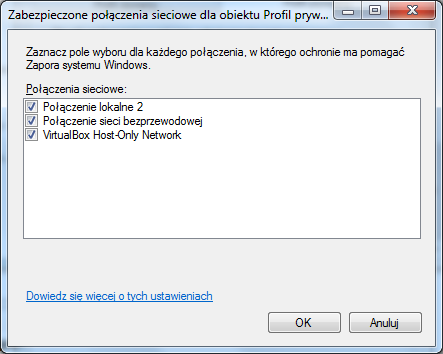
[](https://soisk.info/index.php/Plik:Zapora8.png)

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.

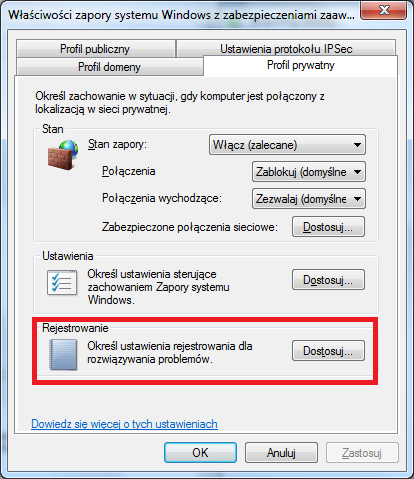
[](https://soisk.info/index.php/Plik:Zapora9.png)

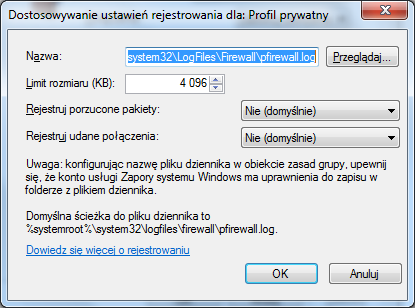
Możemy określić, połączenia jakich kart sieciowych będą chronione.

[](https://soisk.info/index.php/Plik:Zapora10.png)

[](https://soisk.info/index.php/Plik:Zapora11.png)

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

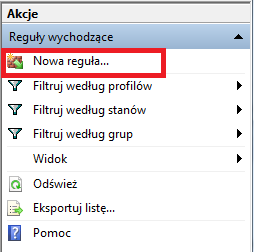
[](https://soisk.info/index.php/Plik:Zapora12.png)

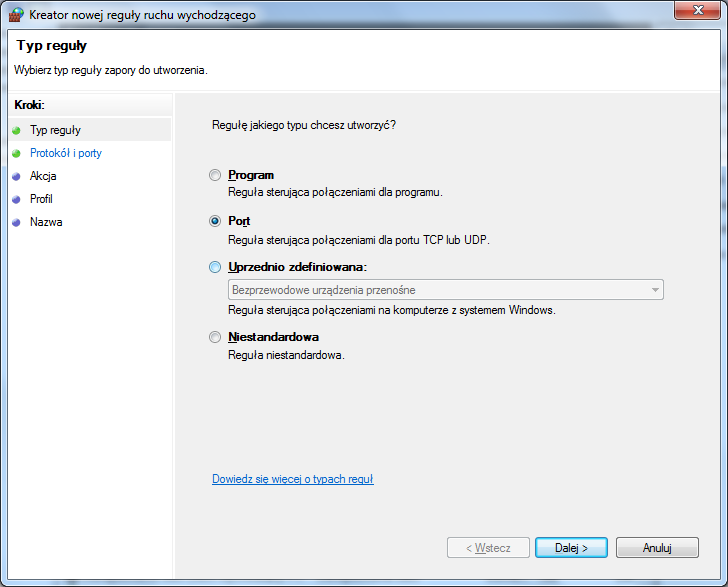
[](https://soisk.info/index.php/Plik:Zapora13.png)

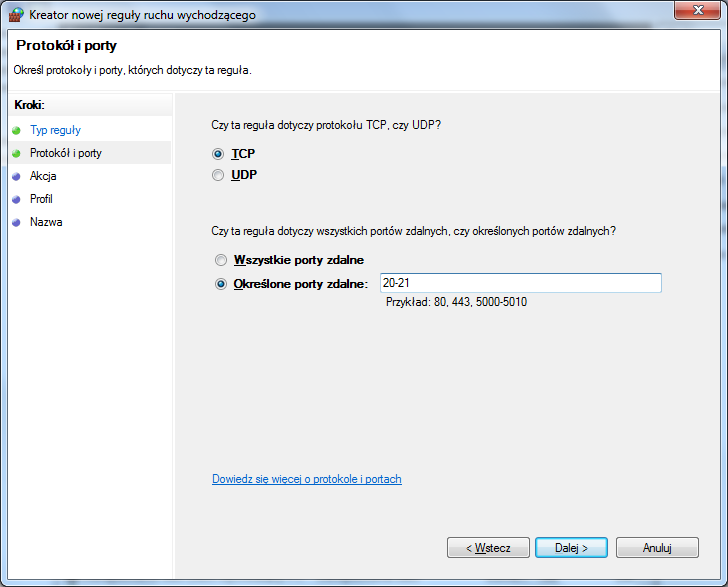
**Dodanie reguły**

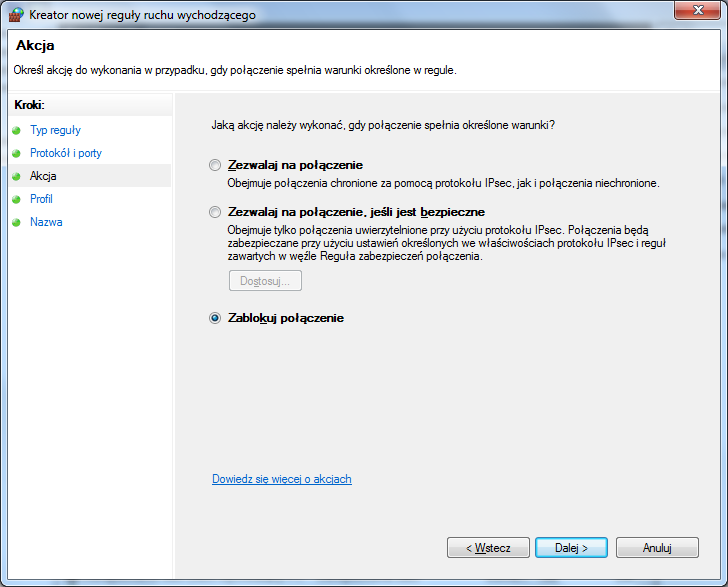
Wchodząc w Zaporę systemu Windows z zabezpieczeniami zaawansowanymi widzimy zdefiniowane reguły przychodzące i wychodzące. Możemy je edytować, usuwać, dodawać nowe.

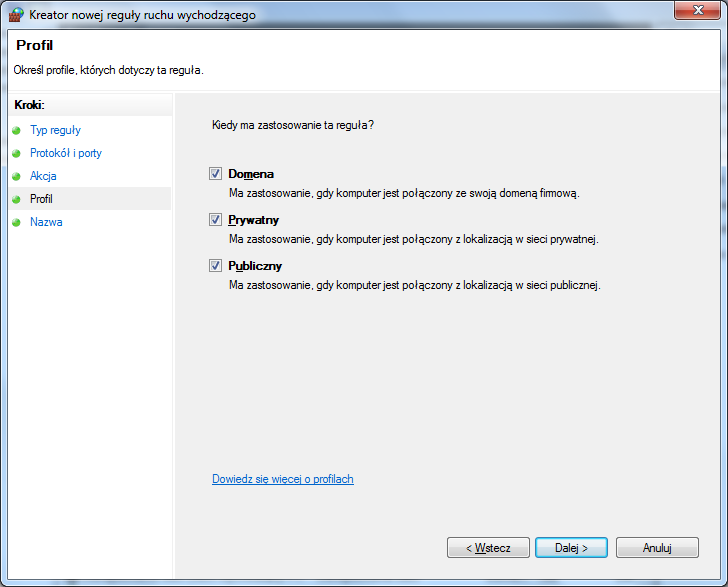
Poniżej pokazano dodanie nowej reguły wychodzącej do blokowania połączeń z serwerem FTP

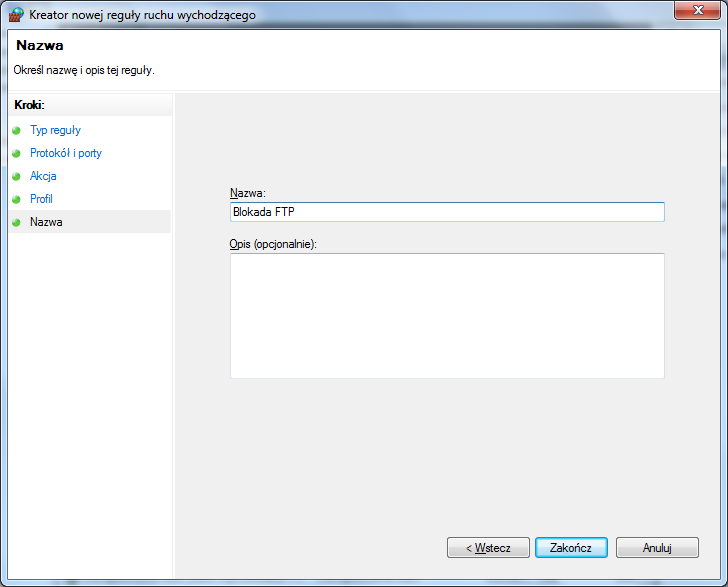
[](https://soisk.info/index.php/Plik:Zapora14.png)

[](https://soisk.info/index.php/Plik:Zapora15.png)

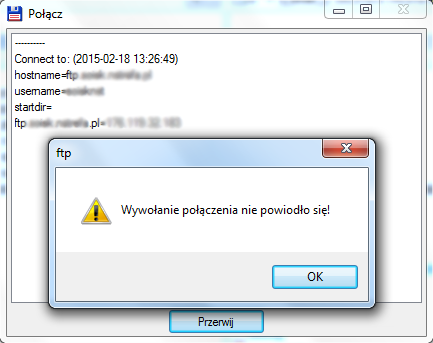
[](https://soisk.info/index.php/Plik:Zapora16.png)

[](https://soisk.info/index.php/Plik:Zapora17.png)

[](https://soisk.info/index.php/Plik:Zapora18.png)

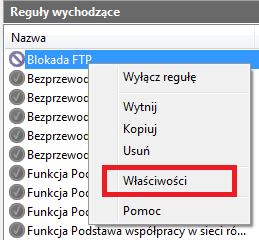
[](https://soisk.info/index.php/Plik:Zapora19.png)

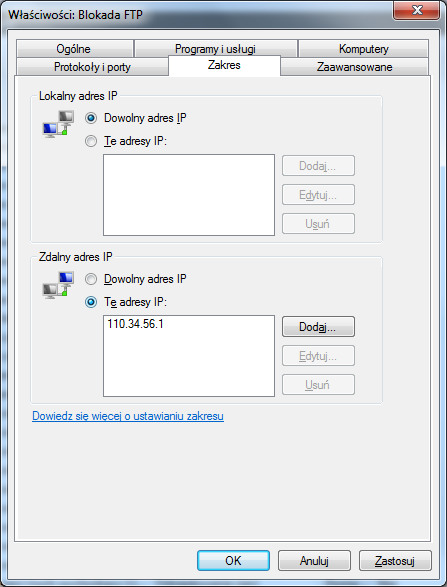
Jak widać wszystko działa poprawnie

[](https://soisk.info/index.php/Plik:Zapora20.png)

**Edycja reguły**

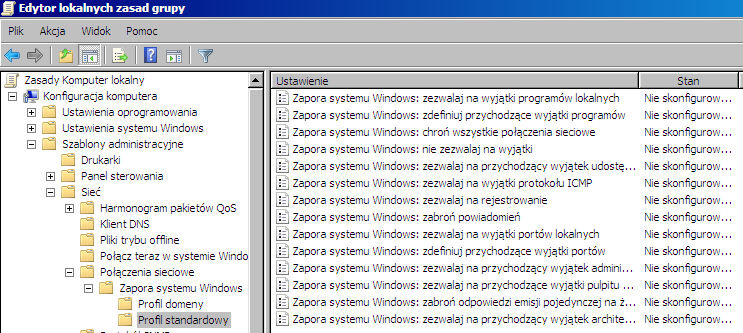
Ustawimy, że wcześniejsza reguła zadziała tylko na jeden adres IP.

[](https://soisk.info/index.php/Plik:Zapora21.png)

[](https://soisk.info/index.php/Plik:Zapora24.png)

Zapora w zasadach grupy

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

[](https://soisk.info/index.php/Plik:Zapora23.png)

Ustaw regułę przepuszczającą ping na zaporze.

Ćwiczenia

1. Zablokuj możliwość przeglądania stron internetowych
2. Zablokuj tylko soisk.info
3. Masz mieć możliwość przeglądania tylko strony soisk.info. Dostęp do innych stron ma być zablokowany.
4. Zablokuj możliwość testowania połączeń za pomocą polecenia ping.
5. Edytuj wcześniejszą regułę. Blokada ma działać tylko w zakresie całej sieci lokalnej.
6. Zablokuj możliwość korzystania z serwera DHCP.