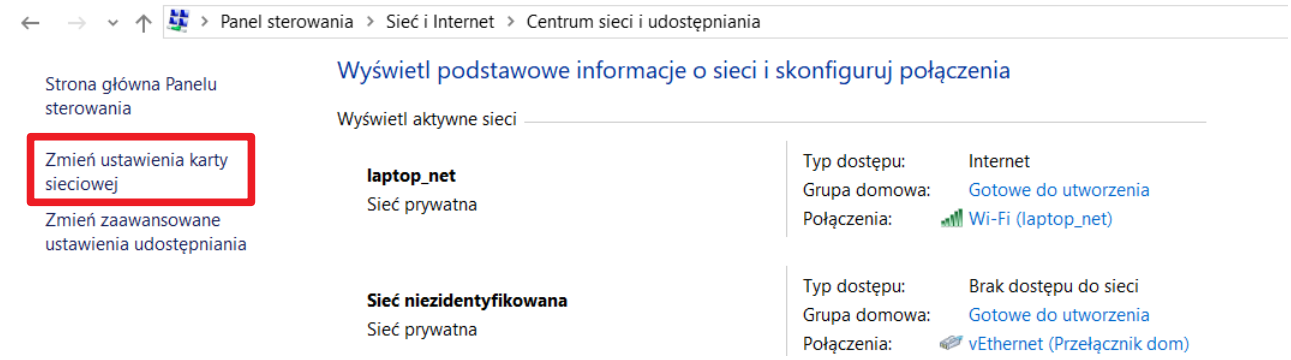
Zadanie z lokalnych sieci komputerowych.

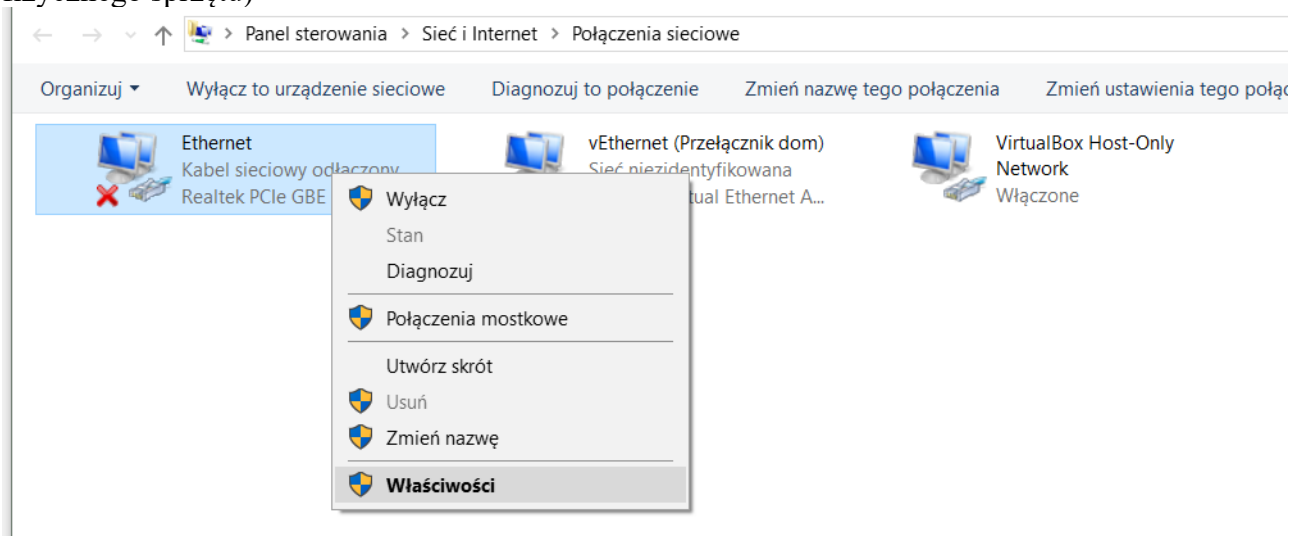
1. Cel zajęć

Kilku znajomych chce zagrać w grę sieciową. Obecnie większość gier oferuje możliwość gry przez internet. Jednak znajomi chcą zagrać ze sobą bez dostępu do sieci internet. W związku z tym należy odpowiednio skonfigurować ustawienia poszczególnych komputerów oraz urządzeń sieciowych.

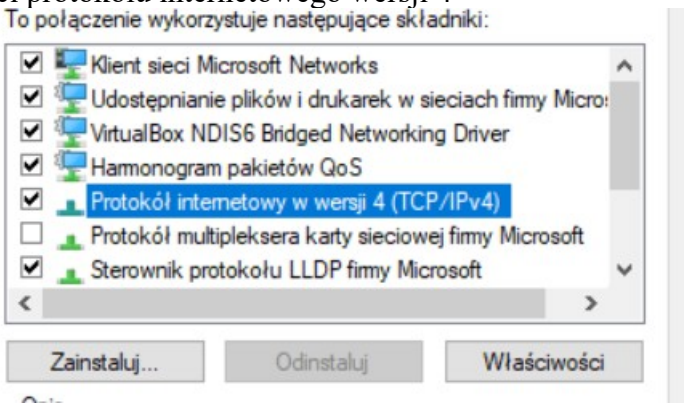
2. Konfiguracja.
a) wariant prosty
- pobieramy dowolną grę sieciową, np. Quake 3 Arena Demo (https://www.dobreprogramy.pl/Quake-III-Arena,Program,Windows,68282.html). Wybór gry może mieć wpływ na przebieg ćwiczenia (konfiguracja zapory)
- przechodzimy do centrum sieci i udostępniania



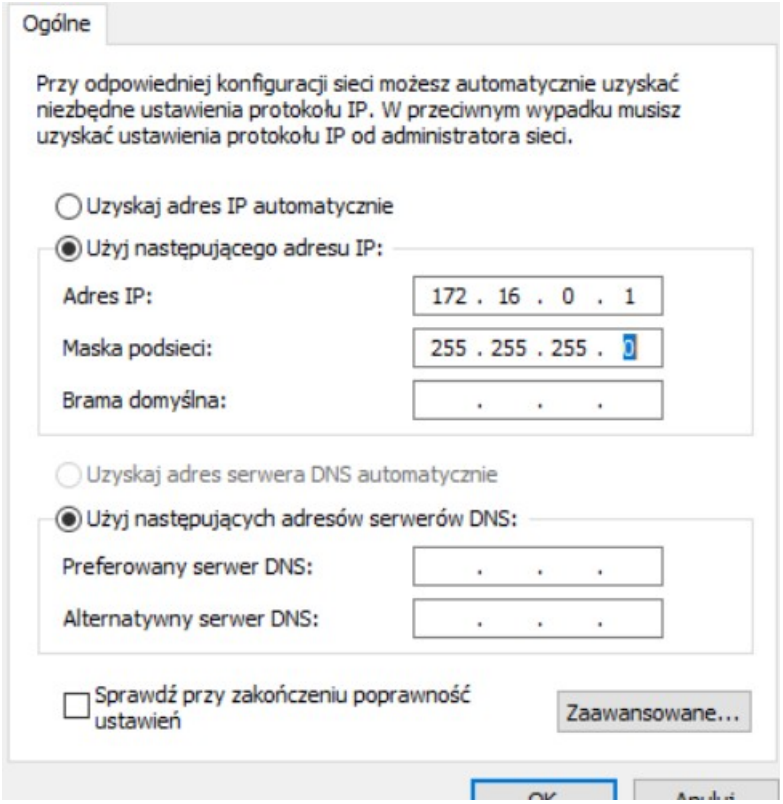
- wybieramy opcję zaznaczoną w ramkę
- wybieramy kartę, dla której chcemy dokonać zmian ustawień sieci (poniżej przykładowa karta – rodzaj i ilość kart zależna jest od systemu operacyjnego, zainstalowanego oprogramowania oraz fizycznego sprzętu)



- zmieniamy właściwości protokołu internetowego wersji 4



- ustawiamy adres IP z tzw. puli nietrasowalnej/prywatnej; propozycją na zajęcia jest pula 172.16.0.0/24, z czego komputery powinny posiadać RÓŻNE adresy w obrębie danej sieci (np. 172.16.0.1, 172.16.0.2 – jednak żaden z komputerów NIE MOŻE ZAWIERAĆ TEGO SAMEGO ADRESU!)



UWAGA! Wpisany powyżej adres jest tylko PRZYKŁADEM! W ramach zajęć należy podać INNY adres, najpierw upewniając się, że NIKT INNY tego adresu nie zajął.

Ponieważ chcemy jedynie posiadać połączenia lokalne toteż nie musimy wypełniać bramy domyślnej ani serwerów DNS.

ZADANIE DODATKOWE: Proszę opisać rolę bramy domyślnej, serwera DNS oraz WINS.

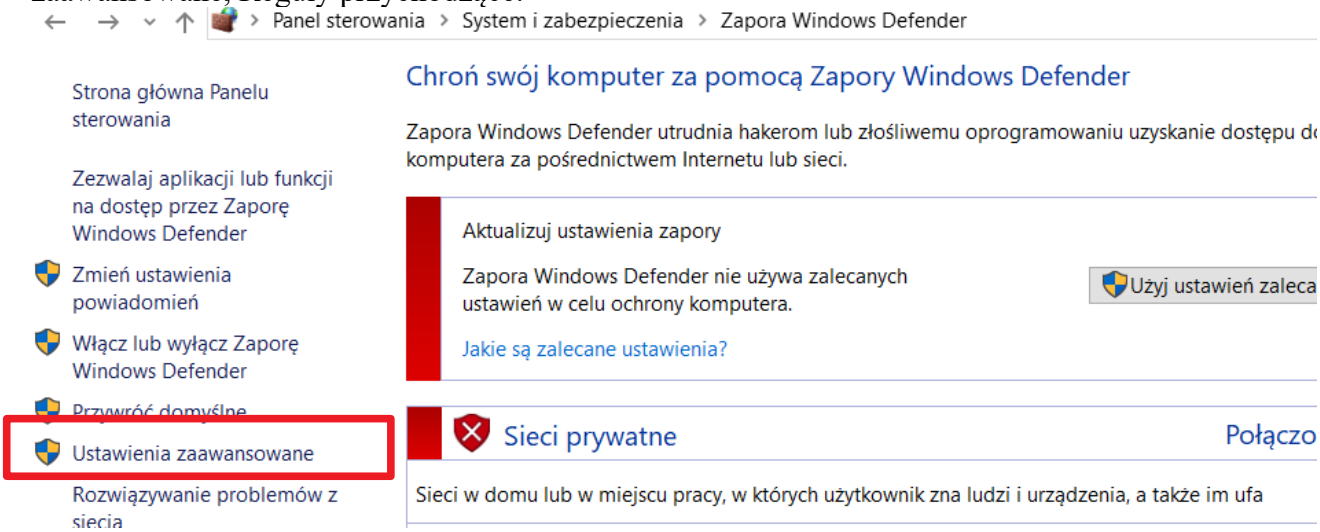
Działanie sieci należy sprawdzić poprzez polecenie ping. Przykładowe działanie polecenia ping:

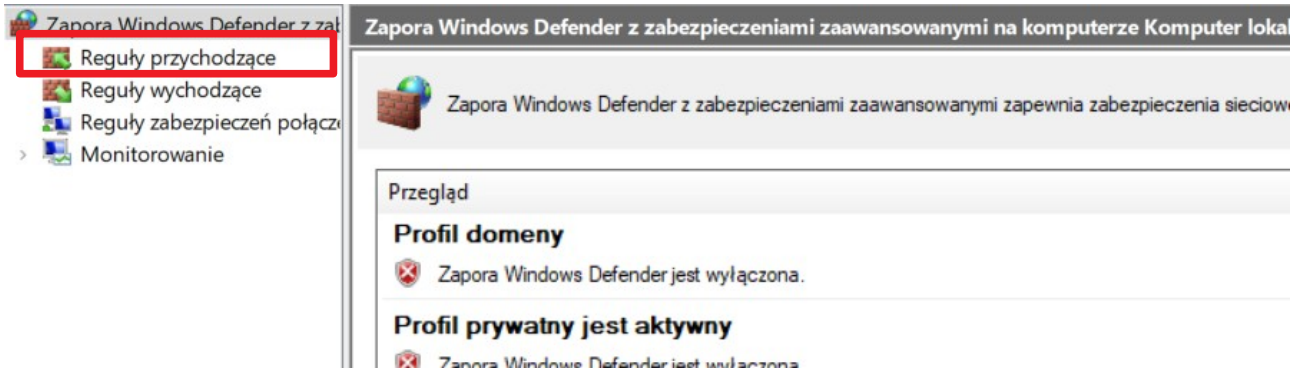
```
C:\Users\adminteb>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time=1ms TTL=64
Reply from 192.168.10.1: bytes=32 time=1ms TTL=64
Reply from 192.168.10.1: bytes=32 time=1ms TTL=64
Reply from 192.168.10.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Jeżeli wpisując adres z sieci (dowolnego INNEGO komputera niż nasz!) otrzymamy podobne komunikaty to będzie to oznaczać, że komputery są ze sobą połączone. Gdyby jednak odpowiedzi się nie pojawiły – możliwe iż będzie to problem konfiguracji zapory sieciowej.

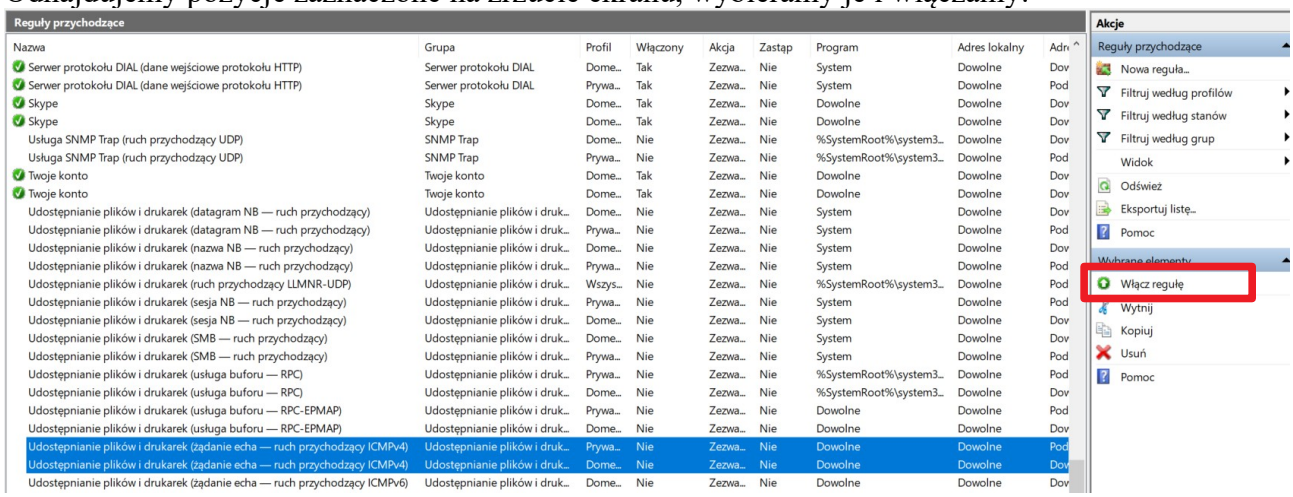
- przechodzimy do ustawień Zapory sieciowej/Firewall/Zapory Windows Defender (widok Centrum sieci i udostępniania)

- jeżeli w poprzednim kroku odpowiedzi na ping nie działały osobom, które zapytanie wysyłały w kierunku naszego komputera, należy włączyć możliwość odpowiedzi na nie klikając Ustawienia zaawansowane, Reguły przychodzące:





Odnajdujemy pozycje zaznaczone na zrzucie ekranu, wybieramy je i włączamy:



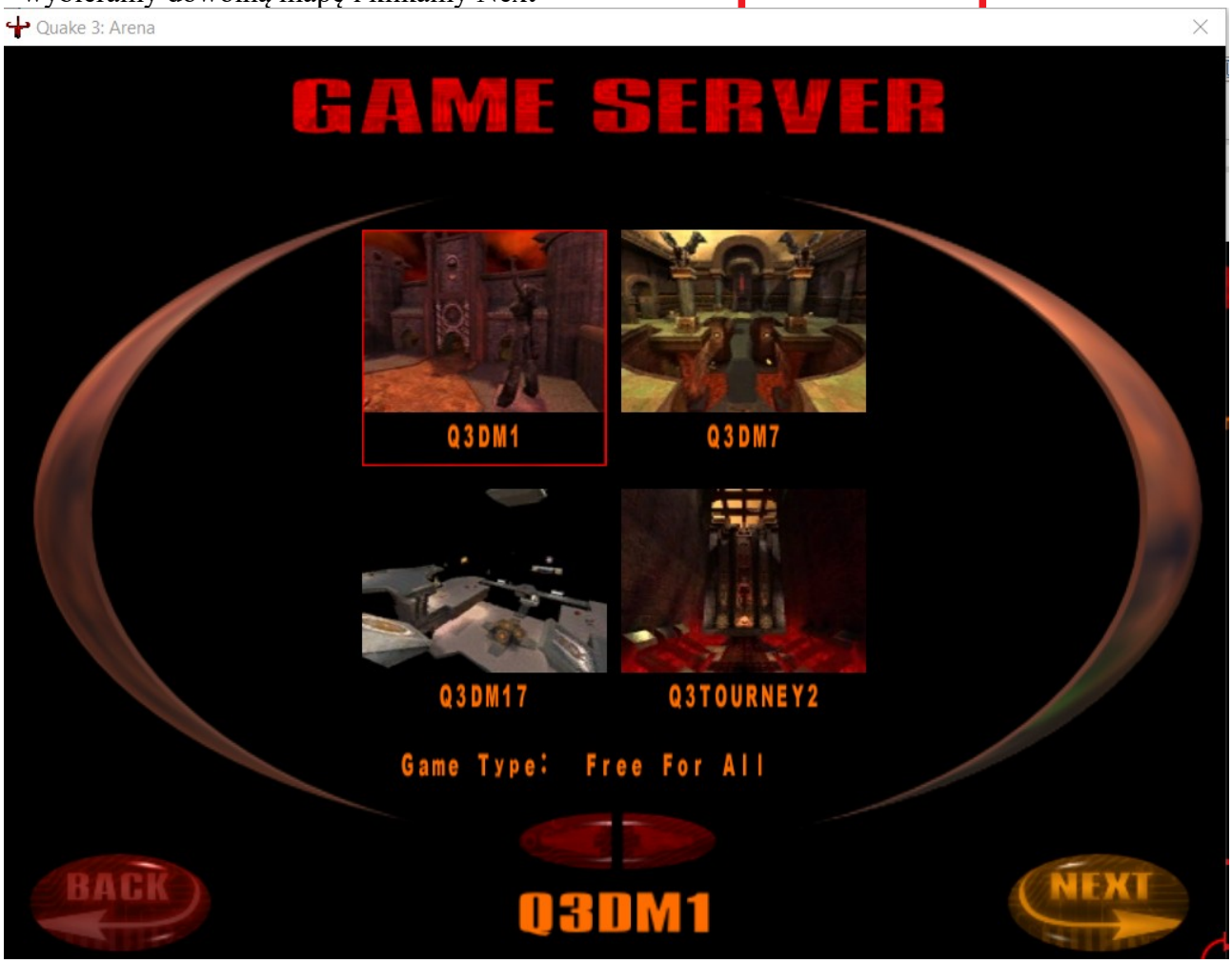
Teraz ping powinien działać bez zarzutu pomiędzy każdym komputerem.

ZADANIE DODATKOWE: Proszę znaleźć informacje o protokole ICMP i scharakteryzować jego rolę w diagnostyce sieci.

- uruchamiany grę, wybieramy tryb multiplayer:

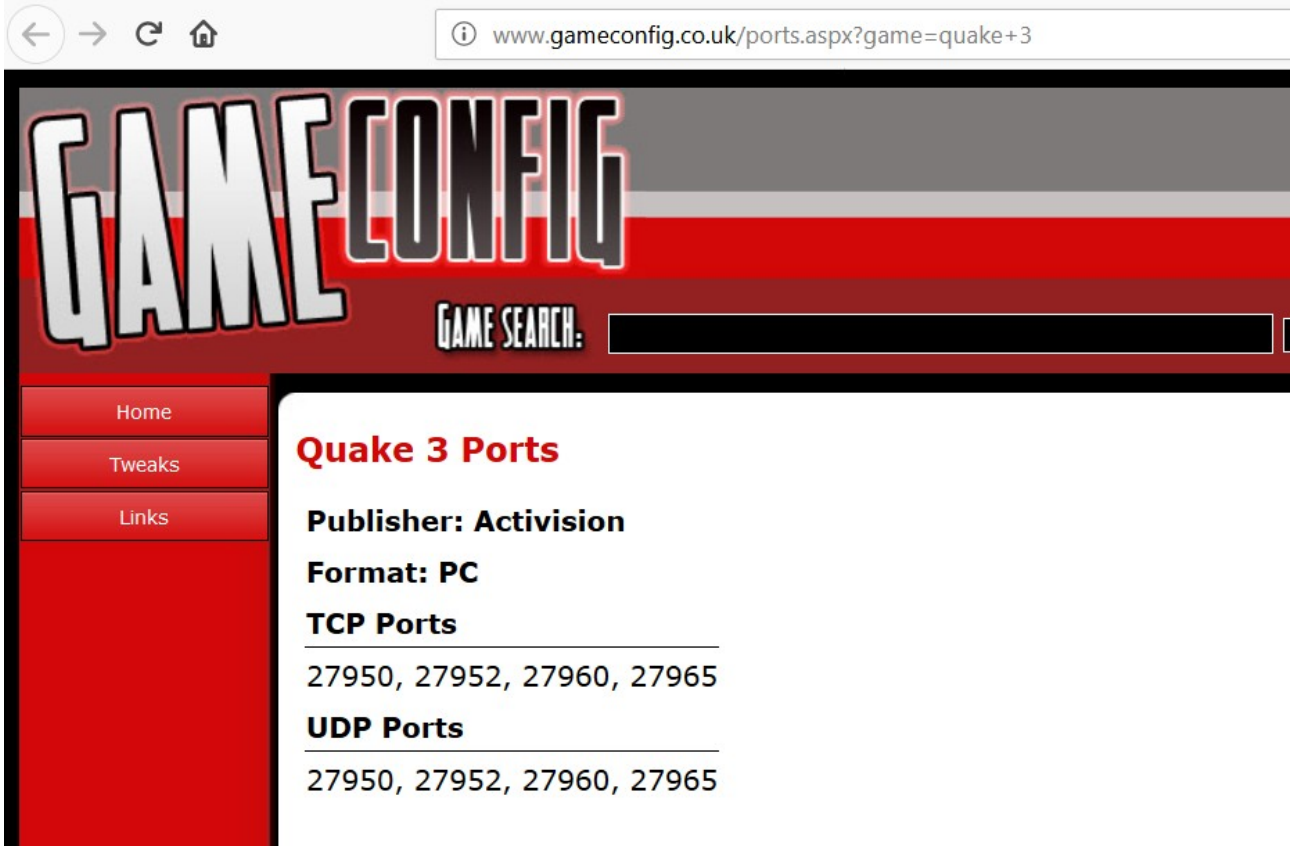
- wybieramy opcje Create:

- wybieramy dowolną mapę i klikamy Next

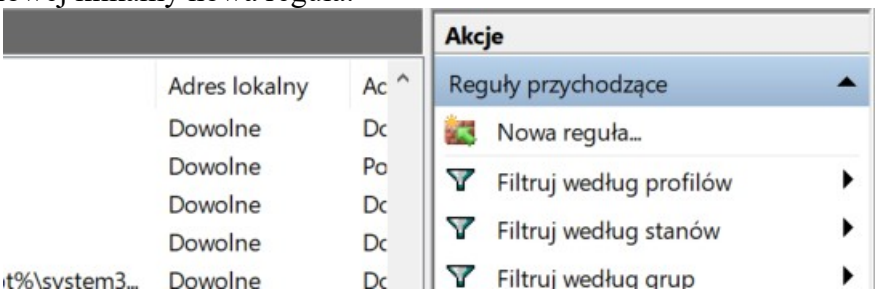


- od tego momentu gra oczekuje na podłączenie się innych graczy

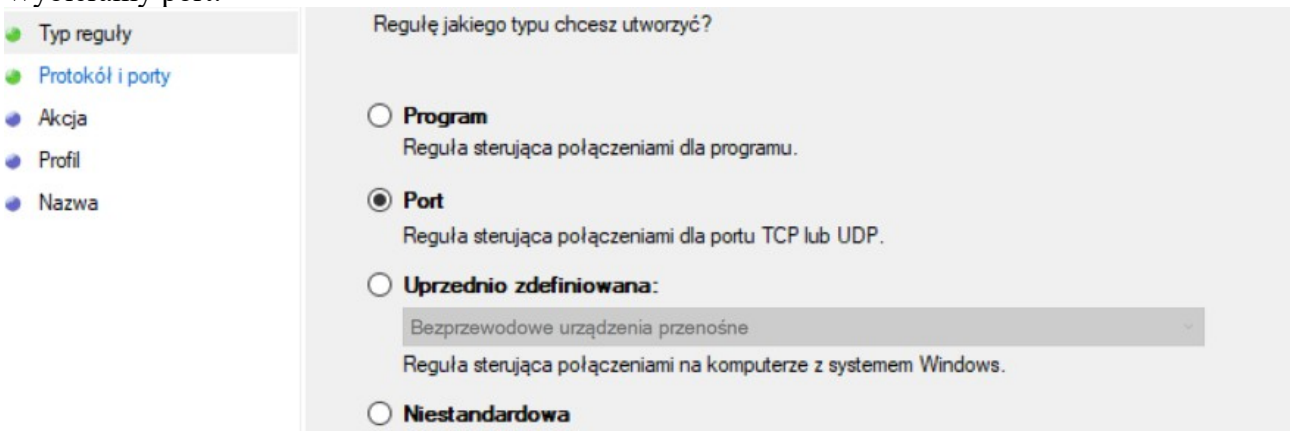
- inni gracze mogą sprawdzić czy nasz serwer się pojawił. Tak gdzie my kliknęliśmy opcję Create, inni powinni widzieć nasz serwer. Jeżeli tak się nie dzieje możliwe jest, że musimy otworzyć dodatkowo port. Porty mogą być dostępne w dokumentacji bądź na stronach WWW, np.:



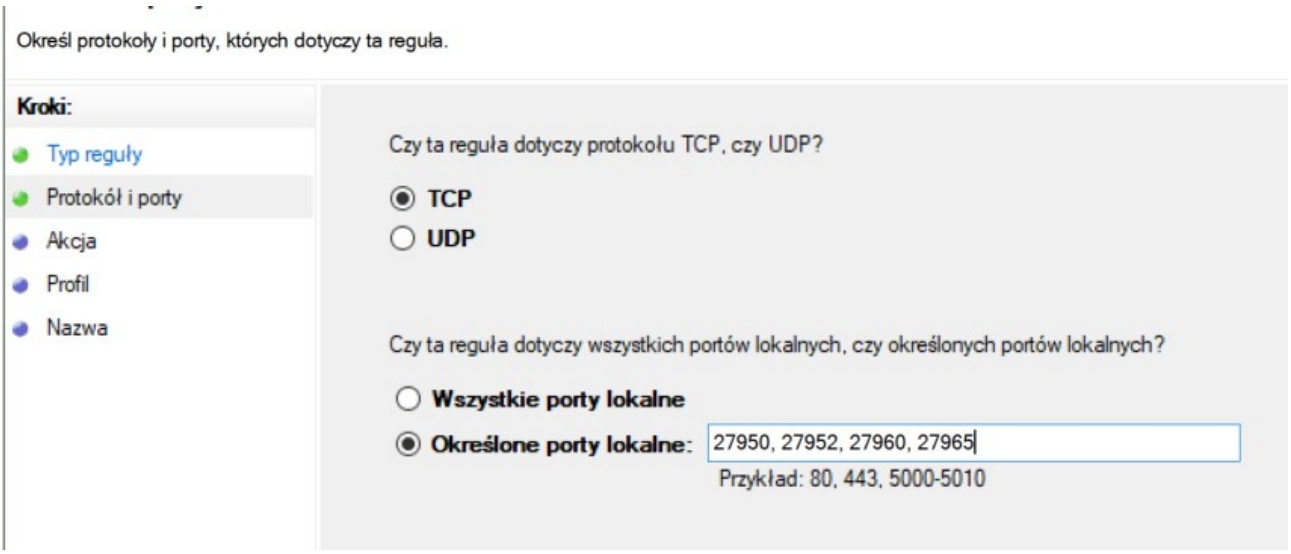
W Zaporze sieciowej klikamy nowa reguła:



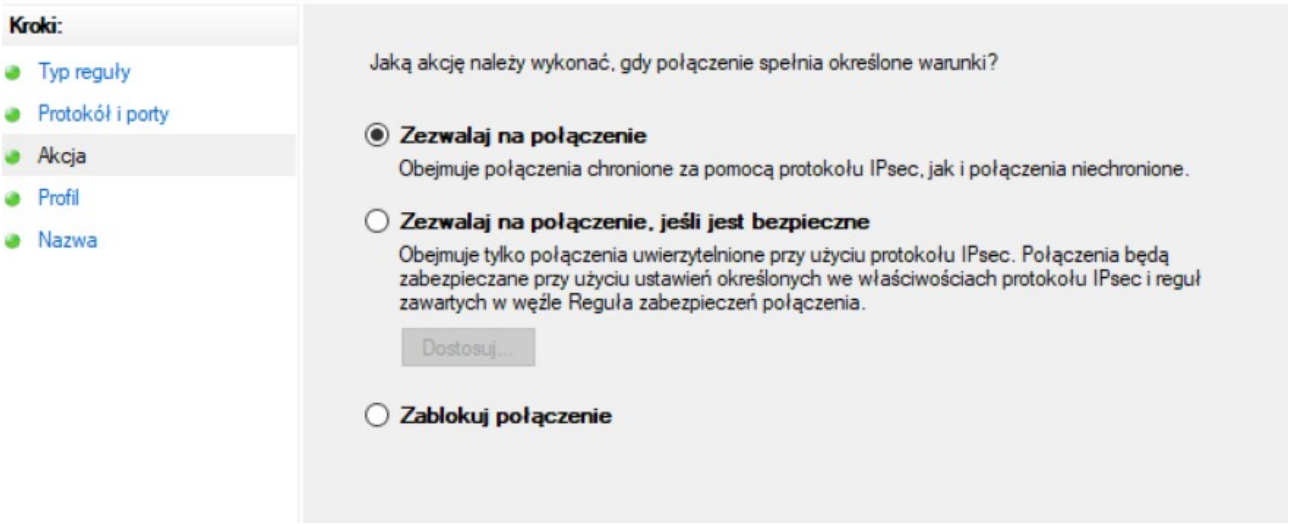
Wybieramy port:



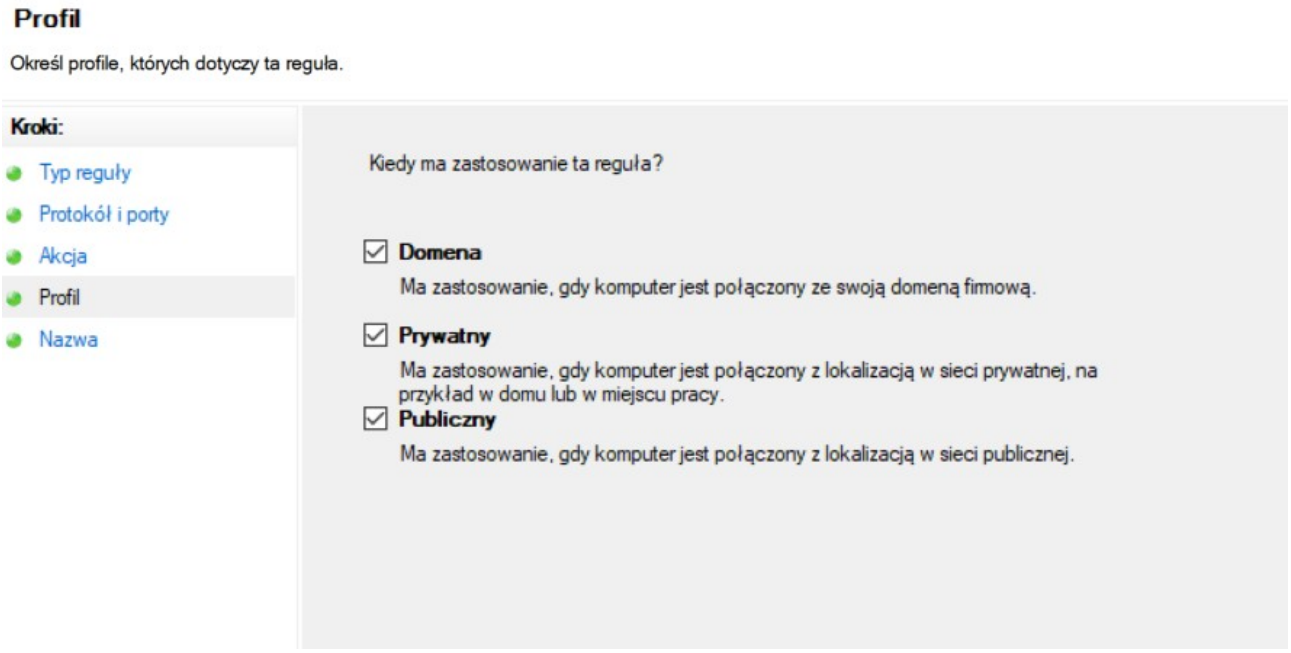
- wybieramy protokół oraz wpisujemy odpowiednie porty:



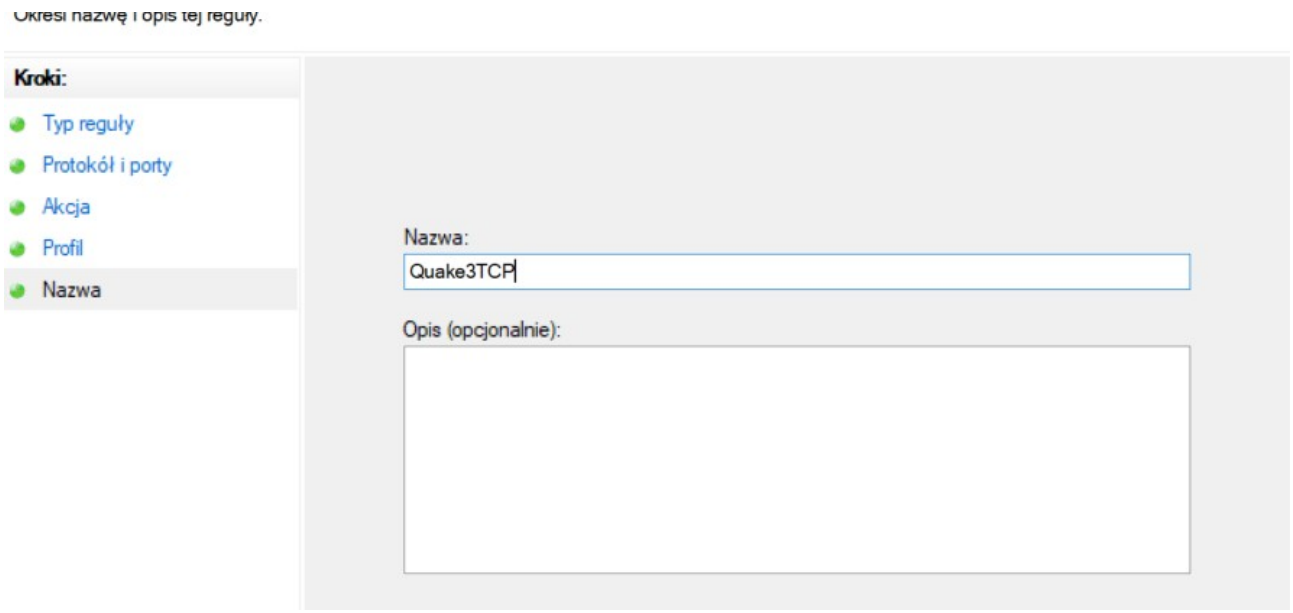
- akcje pozostawiamy bez zmian:



- przekierowujemy porty w każdym profilu:

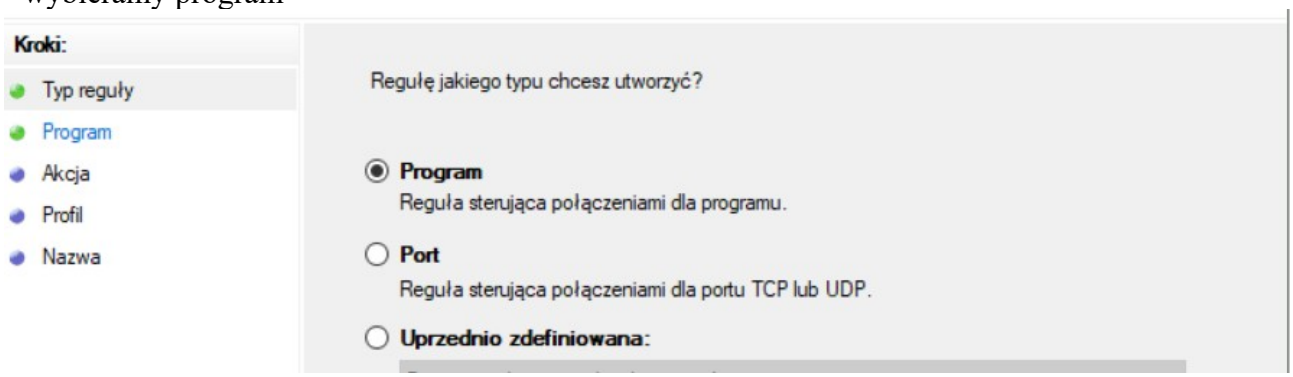


- zapisujemy regułę pod określoną nazwą (dowolną). Jeżeli chcemy możemy dodać dodatkowy komentarz:

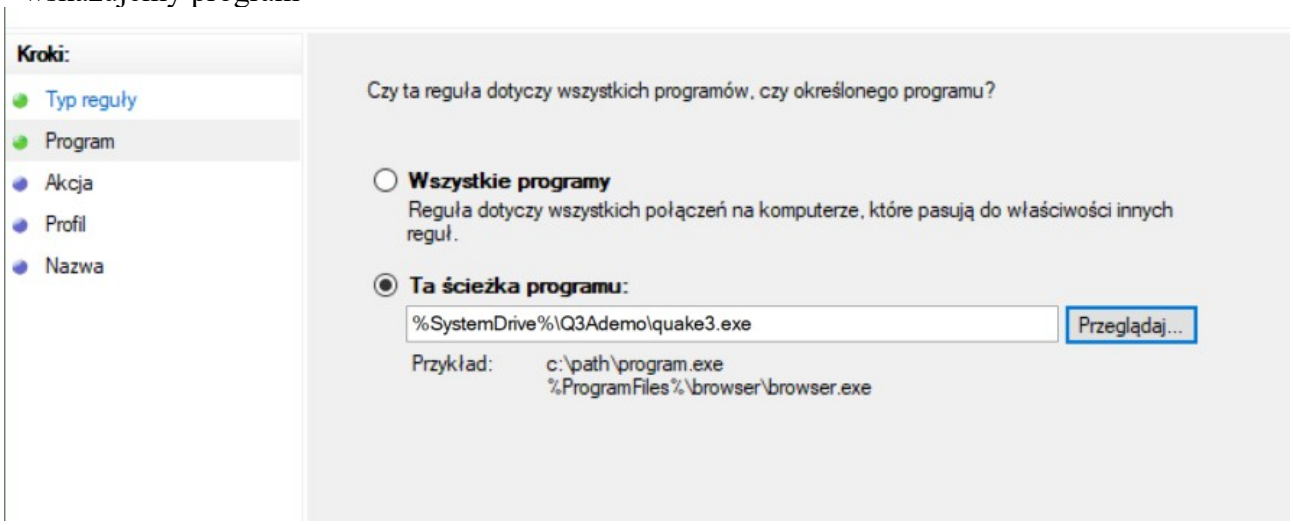


- ponawiamy operację dla portów UDP

ALTERNATYWNIE możemy wybrać program, dla którego zapora ma przekierowywać wszystkie wymagane porty. W tym celu:
- klikamy Nowa reguła…
- wybieramy program



- wskazujemy program



Od tego momentu powinniśmy mieć możliwość prowadzenia rozgrywek sieciowych bez internetu.

b) wariant z DHCP

Ten wariant wymaga niemal tych samych kroków co poprzedni. Tutaj jednak ustawiamy adresy IP na pozyskiwanie automatyczne. Dzięki temu nie musimy tracić połączenia z internetem Jeżeli w poprzednim kroku ustawialiśmy przekierowania portów w zaporze – możemy od razu przystąpić do rozgrywki.

c) wykorzystanie przełącznika zarządzanego celem ograniczenia zasięgu rozgrywki LAN

Niekiedy nasza sieć LAN może być na tyle duża, że będziemy potrzebować ją podzielić. W tym wypadku można dokonać tego poprzez odpowiedni podział adresacji IP lub wykorzystać dodatkowe właściwości urządzeń sieciowych podziału na mniejsze podsieci.

Wybierając urządzenia będziemy mieć do czynienia z urządzeniami typu przełącznik zarządzany (warstwy 2 lub 3 modelu ISO-OSI). Obecnie najtańsze egzemplarze kosztują nieznacznie drożej od wersji niezarządzanych, dają jednak większe możliwości konfiguracji i zarządzania siecią.

Każdy z przełączników ma własne, niezależnie oprogramowanie. Cechą wspólną jest funkcjonalność. W naszym wypadku wymagane są dwie funkcjonalności:
- VLAN – technologia, która pozwala na wirtualny podział fizycznej sieci komputerowej (VLAN – Virtual LAN). Podział następuje poprzez utworzenie sieci, której „identyfikatorem" nie jest połączenie ze sobą kabli sieciowych, a identyfikator liczbowy. Ponieważ VLAN modyfikuje przesyłaną ramkę danych tylko urządzenia zgodne ze standardem IEEE802.3q pozwalają na łączenie w tego typu sieć.

ZADANIE DODATKOWE: Krótko opisać czym różnią się od siebie pakiet, segment oraz ramka danych.

W przypadku przełączników najszybszym i najbezpieczniejszym utworzeniem VLAN będzie użycie tzw. nieetykietowanego (untagged). Dzięki temu poszczególne urządzenia DOCELOWE nie będą wiedzieć iż mają do czynienia z VLAN – przełącznik sam zadba o odpowiednie rozprowadzenie pakietów pomiędzy portami.

ZADANIE: Dodać minimum 3 porty do VLAN id 5, pozostałe pozostawiając bez przydziału/bez zmian. Zaobserwować działanie sieci pomiędzy portami w VLAN jak i poza nim.

- izolacja portów (port isolation/safe ports) – zabezpieczenie to działa jedynie w obrębie danego przełącznika. Pozwala na (niemal) fizyczne oddzielenie od siebie portów. Konfiguracja sprawdza się do wskazania, z którymi portami może komunikować jest wskazany port. Przykład: jako administratorzy możemy wskazać, by port numer 1 mógł komunikować się z portami 3 i 5, jednak portom 3 i 5 wskażemy, że mogą się jedynie komunikować z portem 1. Spowoduje to, że port 3 i 5 będzie mógł przesyłać (w obie strony) dane do urządzenia podpiętego na porcie 1, jednak urządzenia na portach 3 i 5 nie będą mieć jakiejkolwiek formy komunikacji pomiędzy sobą.

ZADANIE: Dokonać izolacji wszystkich portów w taki sposób, żeby zachowana została komunikacja jedynie pomiędzy nimi a portem 1. Sprawdzić efekt.

ZADANIE OGÓLE: wypróbować poznane możliwości konfiguracji urządzenia w połączeniu z tworzeniem rozgrywek sieciowych. Zwrócić uwagę w jaki sposób na rozgrywkę wpływa konfiguracja izolacji portów na tworzenie serwera gry.