Oprogramowanie zabezpieczające SO w tym skanery antywirusowe i profilaktyka antywirusowa.

Przed przystąpieniem do ćwiczenia sprawdź czy ustawienia maszyny wirtualnej z Windows

- pozostaw.

Polecane oprogramowania do ćwiczeń AVG_Protection_Free. Wybierz z Internetu lub urządzenia Napędy optyczne, wybierz obraz dysku oprogramowanie.iso.

Zadanie 1

Wykonaj kolejne czynności dla programu antywirusowego i antyspyware.

1.1 Instalacje programu do usuwania złośliwego oprogramowanie (szkodliwego kodu).

1.2 Aktualizacje (z folderu) baz programu do usuwania złośliwego oprogramowanie.

https://support.avg.com/SupportArticleView?l=pl&urlname=How-to-update-AVG

1.3 Skanowanie komputera i usuwanie złośliwego oprogramowanie.
Wirus testowy eicar pobierz z http://2016.eicar.org/85-0-Download.html

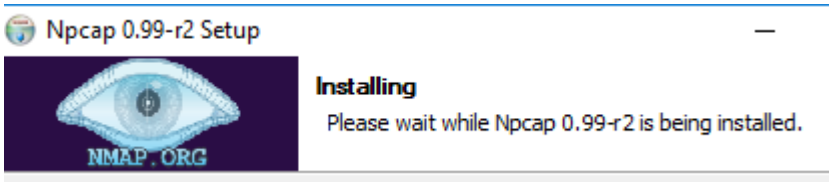
1.4 Włączenie ochrony rezydentnej (trybu monitora).

1.5 Włączenie automatycznych aktualizacji programu antywirusowego.

Zadanie 2

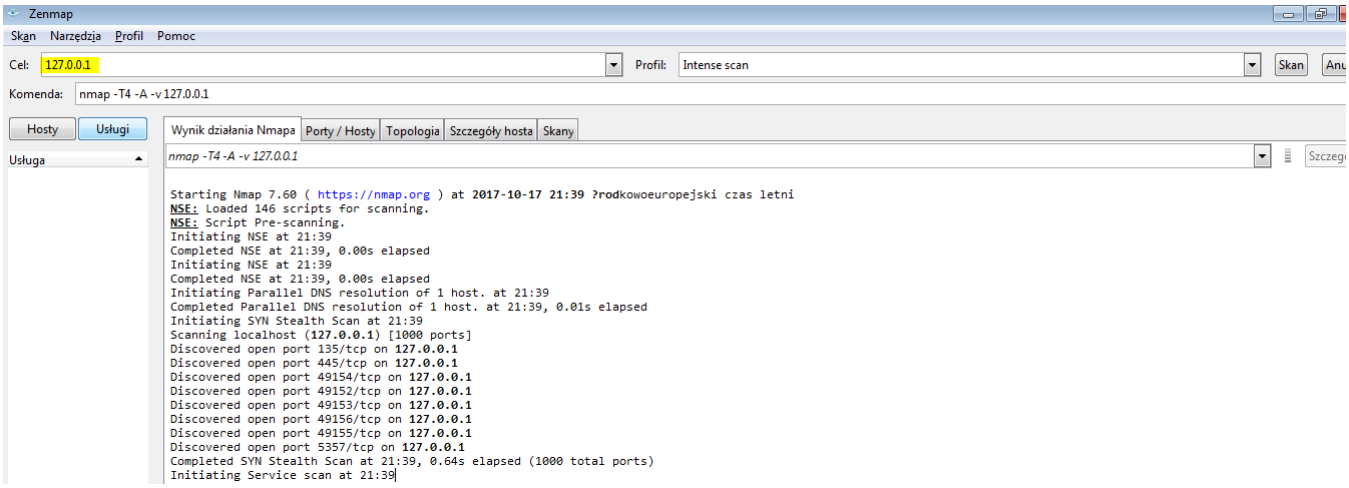
Wykonaj kolejne czynności dla konfiguracji zapory.

Zainstaluj program nmap z npcap-0.99-r2

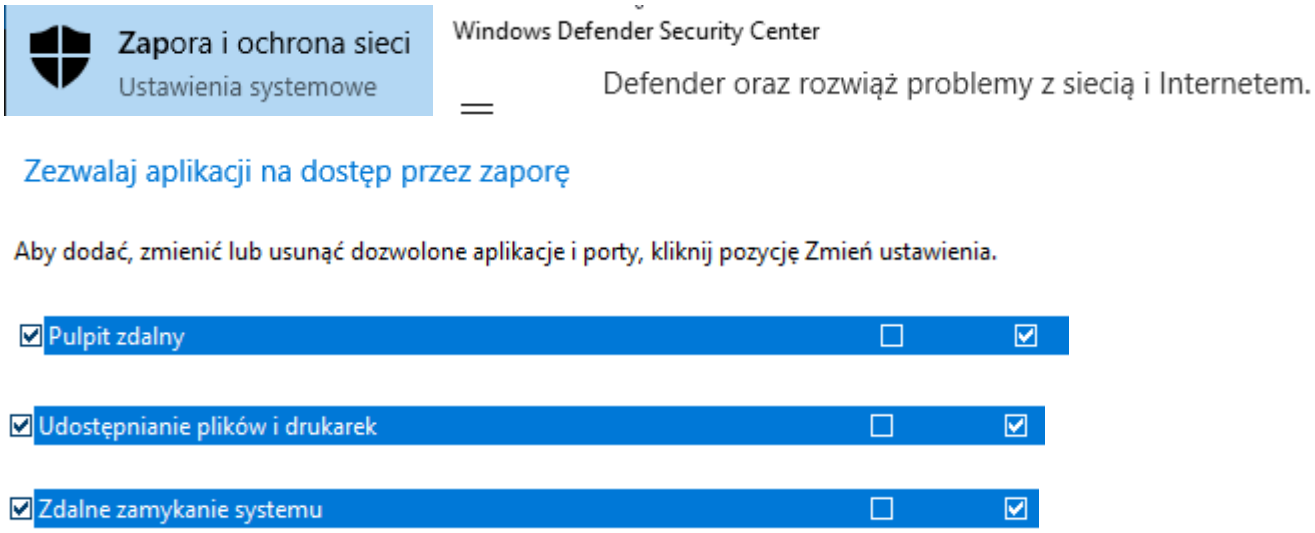


2.1a Sprawdź za pomocą programu nmap otwarte porty na komputerze. Cel: 127.0.0.1

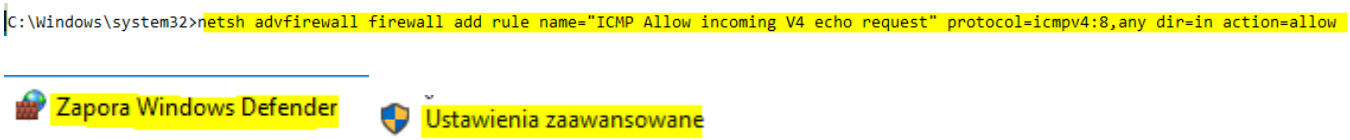
2.1b Opisz jakie porty są otwarte i jakie w tych portach pracują usługi.

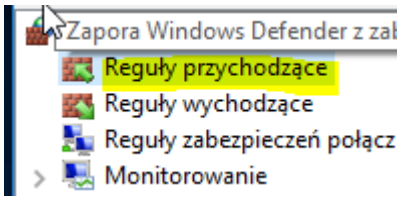


2.2 Włącz zaporę systemową. Ustaw zaporę, aby przepuszczała komunikacje programów Gadu-gadu, udostępnianie plików i drukarek, pulpit zdalny oraz ping.



netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=in action=allow



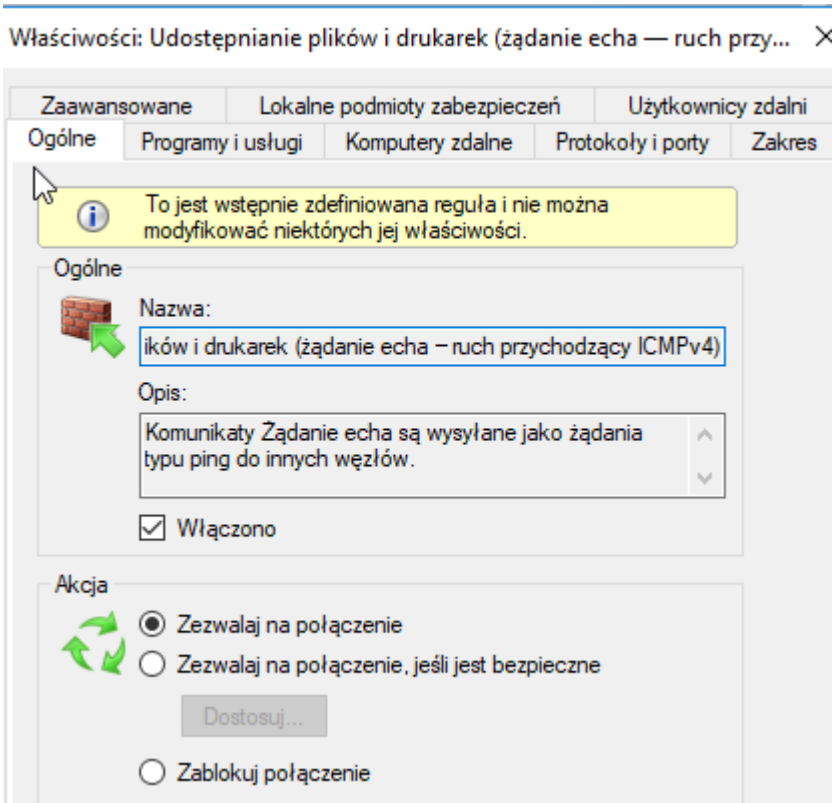


Nazwa	Grupa
Udostępnianie plików i drukarek (żądanie echa — ruch przychodzący ICMPv4)	Udostępnianie plików i
Udostępnianie plików i drukarek (żądanie echa — ruch przychodzący ICMPv4)	Udostępnianie plików i
Udostępnianie plików i drukarek (żądanie echa — ruch przychodzący ICMPv6)	Udostępnianie plików i

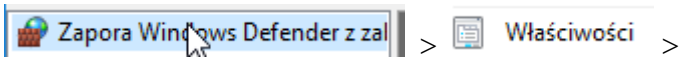
Profil	Włączony	Akcja	Zastąp	Program	Adres lokalny	Adres zdalny
Prywatny	Nie	Zezwa	Nie	Dowolne	Dowolne	Podsieć lokal
Publiczny	Tak	Zezwa	Nie	Dowolne	Dowolne	Podsieć lokal
Domena	Nie	Zezwa	Nie	Dowolne	Dowolne	Dowolne

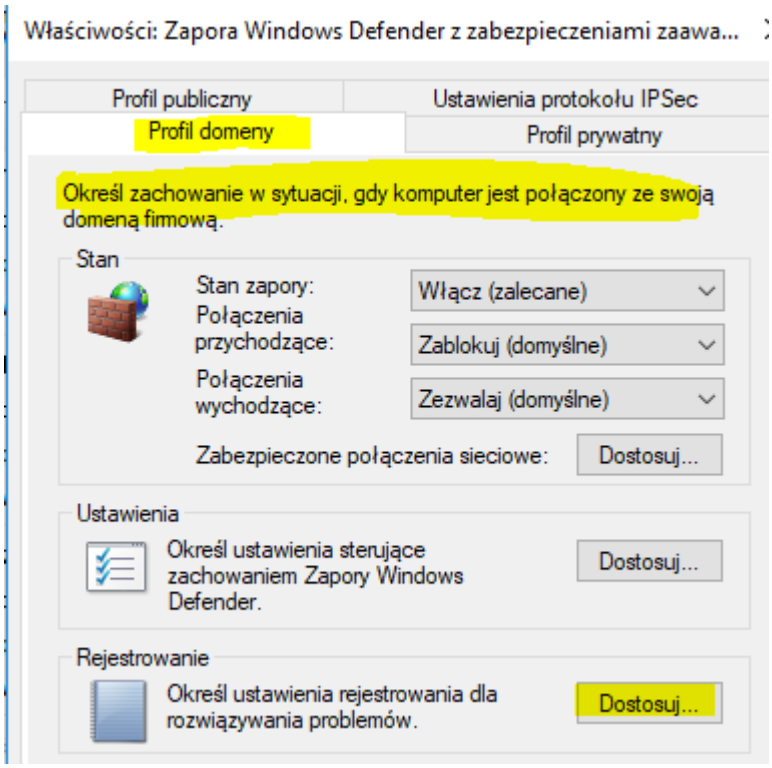
Port lokalny	Port zdalny	Autoryzowani użytkownicy	Autoryzowane komputery	Autoryzowane lok
Dowolne	Dowolne	Dowolne	Dowolne	Dowolne
Dowolne	Dowolne	Dowolne	Dowolne	Dowolne
Dowolne	Dowolne	Dowolne	Dowolne	Dowolne

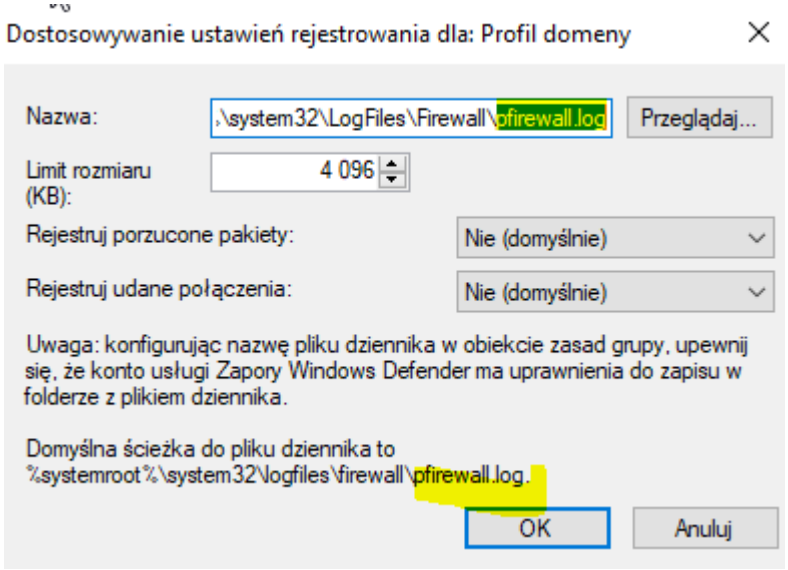
Autoryzowane lokalne podmioty zabezpieczeń	Właściciel użytkownika lokalnego	Pakiet aplikacji
Dowolne	Dowolne	Dowolne
Dowolne	Dowolne	Dowolne
Dowolne	Dowolne	Dowolne



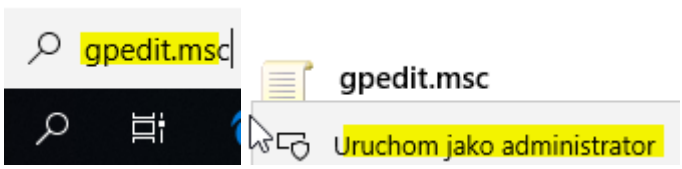
2.3 Zapisz lokalizacje domyślną. Ustaw logowanie porzuconych pakietów zapory do pliku c:\zapora.log





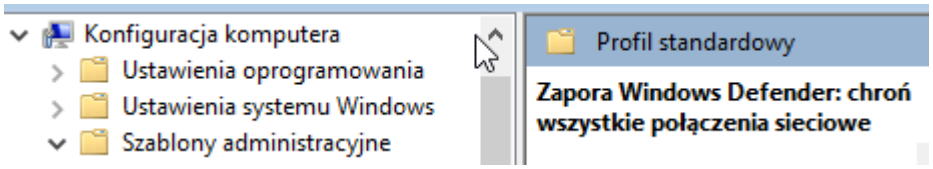


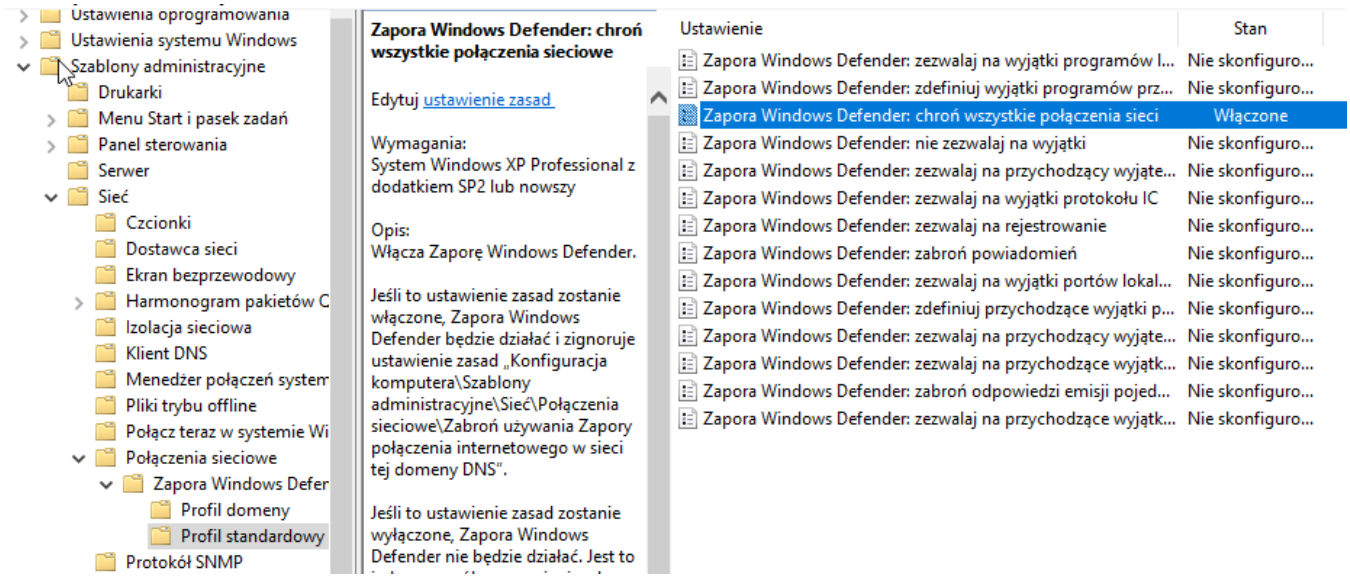
2.4 Ustaw włączenie zapory w zasadach grup (gpedit.msc)

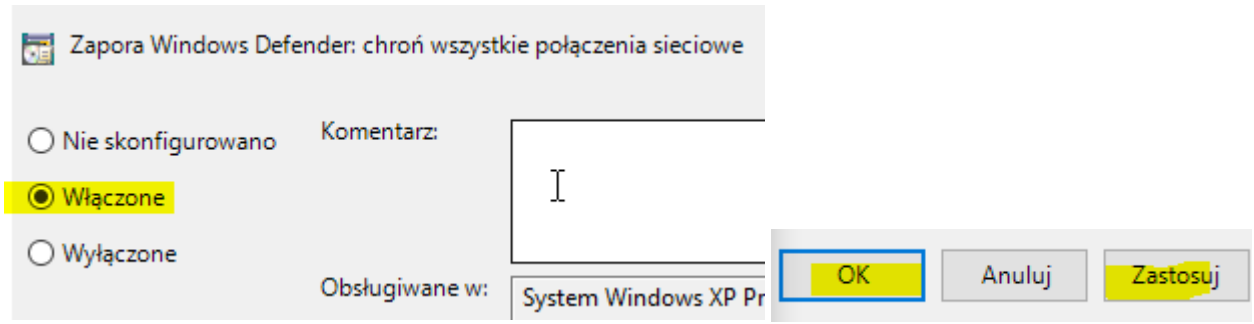


Konfiguracja Komputera → Szablony administracyjne → Sieć → Połączenia sieciowe → Zapora Windows Defender → Profil standardowy: chroń wszystkie połączenia sieciowe.

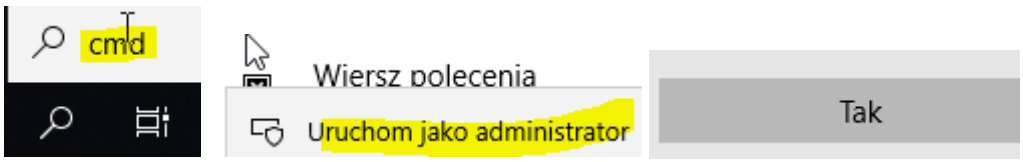
Edytuj ustawienie i zmień jego status na **włączony**. Zapisz zmiany poprzez użycie przycisku **Zastosuj**.

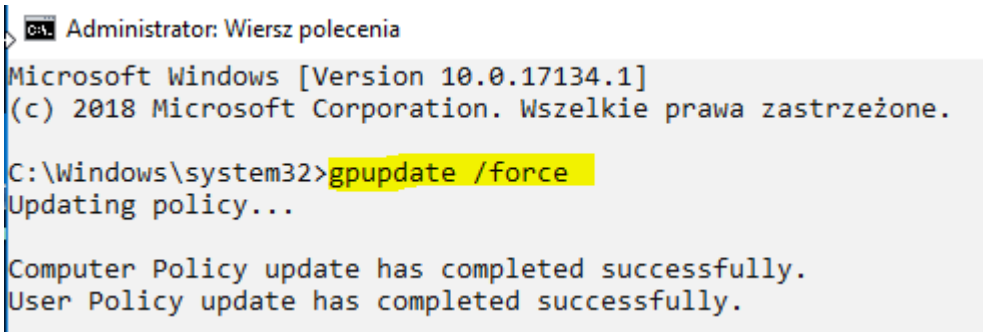






Wkonaj gpupdate /force w celu odświeżenia zasad

Uruchom 



Zadanie 3

Zapisz w zeszycie kolejne czynności, które należy wykonać w celu

1. Ustawienia systemu operacyjnego w tryb automatycznych aktualizacji.

2. Wyjaśnij czym różnią się poszczególne opcje.

Określ, kiedy mają być instalowane aplikacje

Wybierz poziom gotowości gałęzi, aby ustalić, kiedy są instalowane aktualizacje funkcji. "Półroczny kanał (kierowany)" informuje o dostępności aktualizacji dla większości osób, a "półroczny kanał" oznacza, że aktualizacja jest gotowa do powszechnego użycia w organizacjach.

Półroczny kanał (kierowany)

Aktualizacja funkcji zawiera nowe możliwości i ulepszenia. Można ją odroczyć na następującą liczbę dni:

0

Aktualizacja dotycząca jakości zawiera ulepszenia w zakresie zabezpieczeń. Można ją odroczyć na następującą liczbę dni:

0

Optymalizacja dostarczania

Ustawienia prywatności

Uwaga: usługa Windows Update może się aktualizować automatycznie, zanim będzie wyszukiwać inne aktualizacje.

Skonfiguruj automatyczną konfigurację urządzenia po aktualizacji w sekcji Prywatność Opcje logowania

---

Optymalizacja dostarczania

Optymalizacja dostarczania Windows Update umożliwia szybką i niezawodną aktualizację systemu Windows i aplikacji ze sklepu Store oraz innych produktów firmy Microsoft.

Zezwalaj na pobieranie plików z innych komputerów

W przypadku niestabilnego łącza internetowego lub aktualizowania kilku urządzeń, zaznaczenie opcji pobierania z innych komputerów pozwoli przyśpieszyć proces.

Włączenie tej funkcji może spowodować wysyłanie z komputera części pobranych aktualizacji i aplikacji systemu Windows do, w zależności od opcji zaznaczonych poniżej, komputerów w sieci lokalnej lub Internecie. Jeśli korzystasz z połączenia taryfowego, komputer nie będzie wysyłał treści do innych komputerów przez Internet.
Dowiedz się więcej

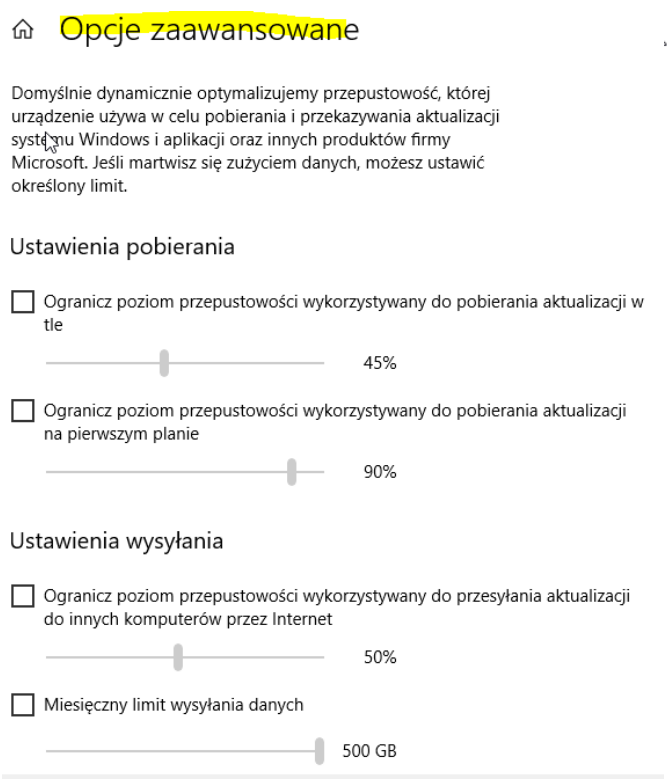
Zezwalaj na pobieranie plików z innych komputerów

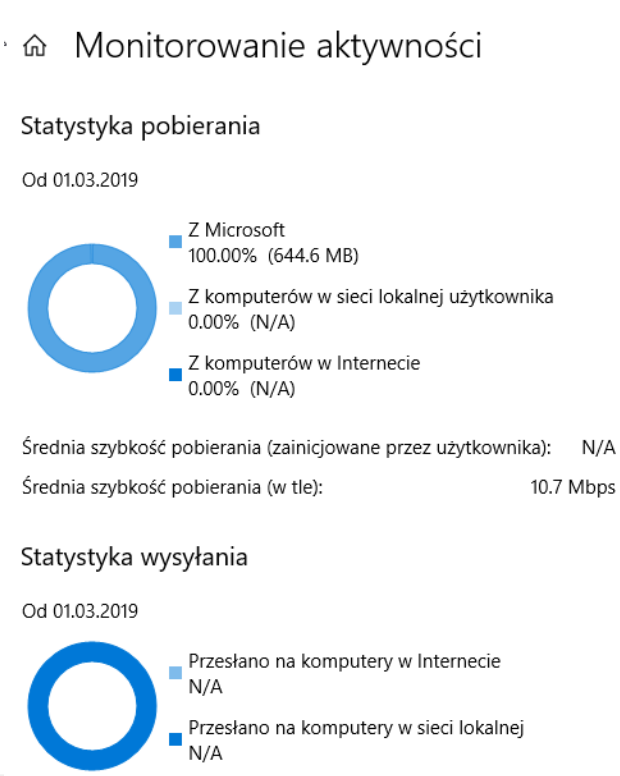
Włączone

- (•) Komputery w mojej sieci lokalnej
- ( ) Komputery w mojej sieci lokalnej i w Internecie

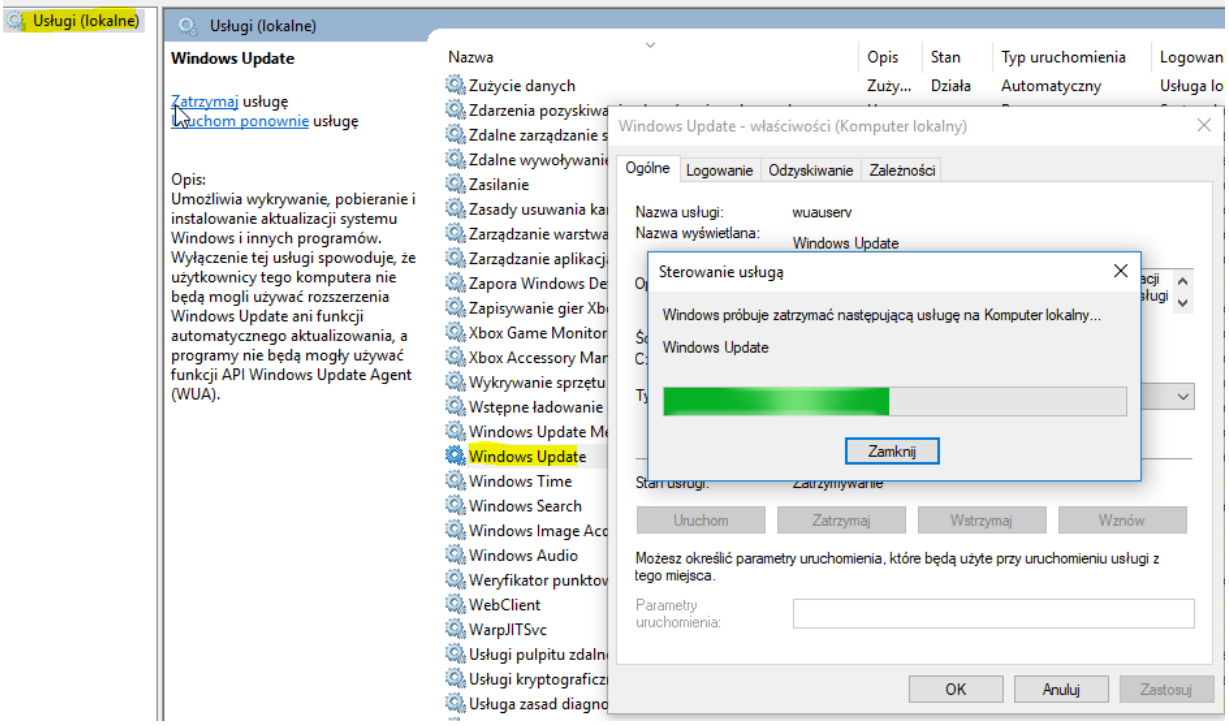
Opcje zaawansowane

Monitorowanie aktywności

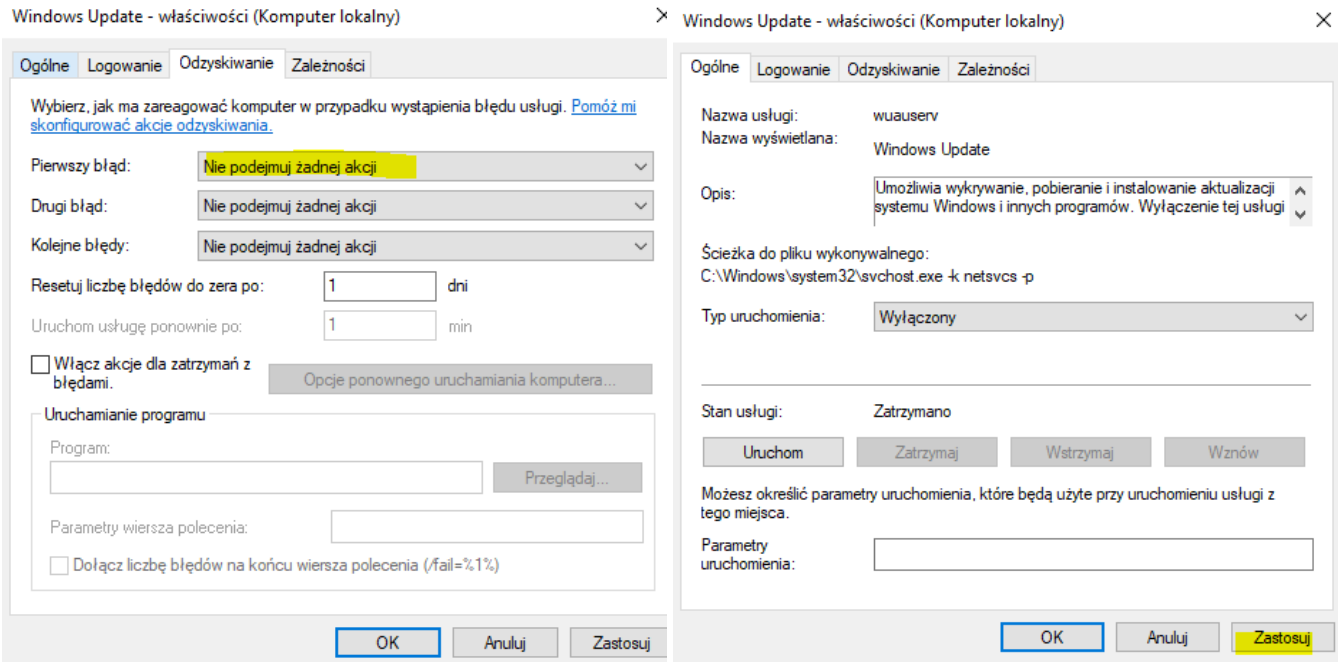




3. W celach sprawnego wykonywana ćwiczeń pozostaw ustawienie



Efekt



4. Ustawienia właściwej konfigurację przeglądarki programów pracujących w sieciach np. Internecie (wybierz dowolną).