


Oprogramowanie zabezpieczające SO w tym skanery antywirusowe i profilaktyka antywirusowa.

Przed przystąpieniem do ćwiczenia sprawdź czy ustawienia maszyny wirtualnej z Windows



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>

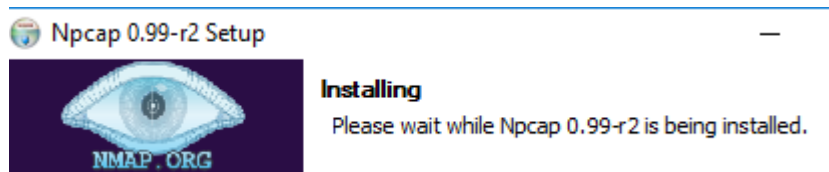
1.4 Włączenie ochrony rezydentnej (trybu monitora).

1.5 Włączenie automatycznych aktualizacji programu antywirusowego.

Zadanie 2

Wykonaj kolejne czynności dla konfiguracji zapory.

Zainstaluj program nmap z 



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

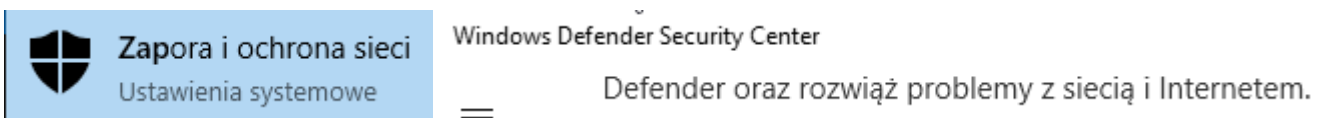
2.1b Opisz jakie porty są otwarte i jakie w tych portach pracują usługi.

```

Zenmap
Skan Narzędzia Profil Pomoc
Cek: 127.0.0.1 Profil: Intense scan Skan Anu
Komenda: nmap -T4 -A -v 127.0.0.1
Hosty Usługi
Wynik działania Nmapa Porty / Hosty Topologia Szczegóły hosta Skany
nmap -T4 -A -v 127.0.0.1
Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-17 21:39 ?rodkowoeuropejski czas letni
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:39
Completed NSE at 21:39, 0.00s elapsed
Initiating NSE at 21:39
Completed NSE at 21:39, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 21:39
Completed Parallel DNS resolution of 1 host. at 21:39, 0.01s elapsed
Initiating SYN Stealth Scan at 21:39
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 135/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 49154/tcp on 127.0.0.1
Discovered open port 49152/tcp on 127.0.0.1
Discovered open port 49153/tcp on 127.0.0.1
Discovered open port 49156/tcp on 127.0.0.1
Discovered open port 49155/tcp on 127.0.0.1
Discovered open port 5357/tcp on 127.0.0.1
Completed SYN Stealth Scan at 21:39, 0.64s elapsed (1000 total ports)
Initiating Service scan at 21:39

```

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



Zezwalaj aplikacji na dostęp przez zaporę

Aby dodać, zmienić lub usunąć dozwolone aplikacje i porty, kliknij pozycję Zmień ustawienia.

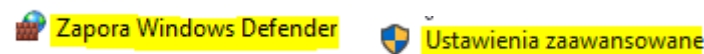
- Pulpit zdalny
- Udostępnianie plików i drukarek
- Zdalne zamykanie systemu

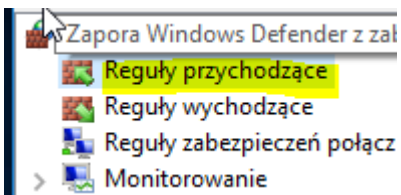
netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request"
protocol=icmpv4:8,any dir=in action=allow

```

c:\Windows\system32>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 drukarek
Udostępnianie plików i drukarek (żądanie echa — ruch przychodzący ICMPv4)	Udostępnianie plików i drukarek
Udostępnianie plików i drukarek (żądanie echa — ruch przychodzący ICMPv6)	Udostępnianie plików i drukarek

Profil	Włączony	Akcja	Zastęp	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
Dowolne	Dowolne	Dowolne

Właściwości: Udostępnianie plików i drukarek (żądanie echa — ruch przy... X

Zaawansowane Lokalne podmioty zabezpieczeń Użytkownicy zdalni

Ogólne Programy i usługi Komputery zdalne Protokoły i porty Zakres

i To jest wstępnie zdefiniowana reguła i nie można modyfikować niektórych jej właściwości.

Ogólne

Nazwa:

Opis:

Włączono

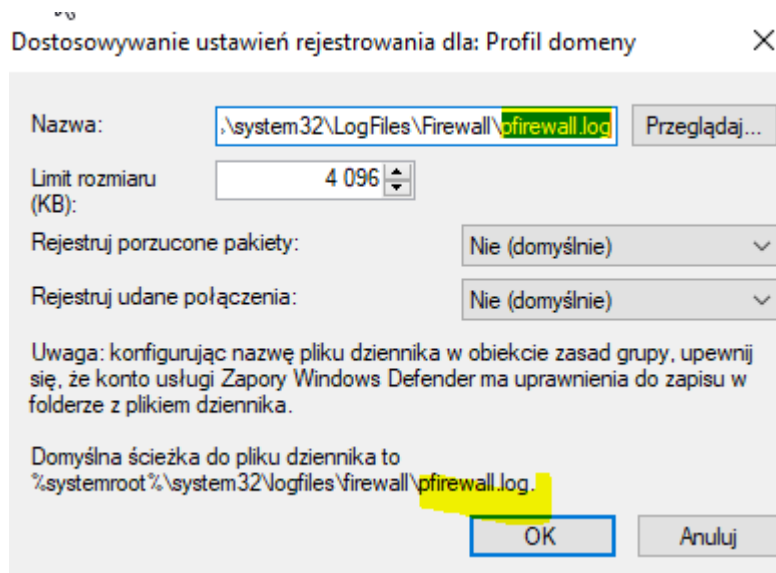
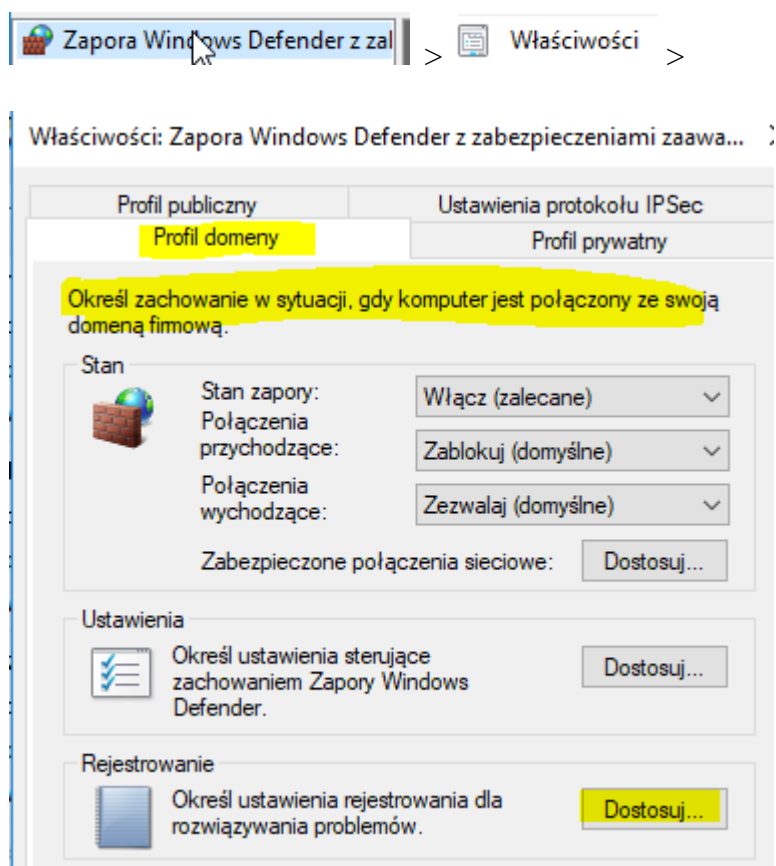
Akcja

Zezwalaj na połączenie

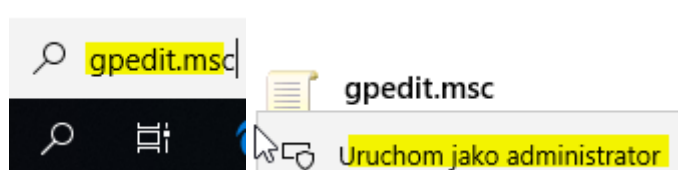
Zezwalaj na połączenie, jeśli jest bezpieczne

Zablokuj połączenie

2.3 Zapisz lokalizację 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**.

Zapora Windows Defender: chroń wszystkie połączenia sieciowe

Ustawienie	Stan
Zapora Windows Defender: zezwalaj na wyjątki programów I...	Nie skonfiguro...
Zapora Windows Defender: zdefiniuj wyjątki programów prz...	Nie skonfiguro...
Zapora Windows Defender: chroń wszystkie połączenia sieci	Włączone
Zapora Windows Defender: nie zezwalaj na wyjątki	Nie skonfiguro...
Zapora Windows Defender: zezwalaj na przychodzący wyjąte...	Nie skonfiguro...
Zapora Windows Defender: zezwalaj na wyjątki protokołu IC	Nie skonfiguro...
Zapora Windows Defender: zezwalaj na rejestrowanie	Nie skonfiguro...
Zapora Windows Defender: zabroń powiadomień	Nie skonfiguro...
Zapora Windows Defender: zezwalaj na wyjątki portów lokal...	Nie skonfiguro...
Zapora Windows Defender: zdefiniuj przychodzące wyjątki p...	Nie skonfiguro...
Zapora Windows Defender: zezwalaj na przychodzący wyjąte...	Nie skonfiguro...
Zapora Windows Defender: zezwalaj na przychodzące wyjątk...	Nie skonfiguro...
Zapora Windows Defender: zabroń odpowiedzi emisji pojed...	Nie skonfiguro...
Zapora Windows Defender: zezwalaj na przychodzące wyjątk...	Nie skonfiguro...

Zapora Windows Defender: chroń wszystkie połączenia sieciowe

Nie skonfigurowano Komentarz:

Włączone

Wyłączone

Obsługiwane w: System Windows XP Pr

Wkonaj gpupdate /force w celu odświeżenia zasad

Uruchom

Wiersz poleceń

Uruchom jako administrator

```
Administrator: Wiersz polecenia
Microsoft Windows [Version 10.0.17134.1]
(c) 2018 Microsoft Corporation. Wszelkie prawa zastrzeżone.

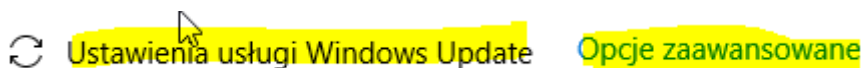
C:\Windows\system32>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

Zadanie 3

Zapisz w zeszycie kolejne czynności, które należy wykonać w celu

1. Ustawienia systemu operacyjnego w tryb automatycznych aktualizacji.



Opcje aktualizacji

Znajdź aktualizacje innych produktów firmy Microsoft, gdy aktualizuję system Windows.

Wyłączone

Automatycznie pobieraj aktualizacje, nawet za pośrednictwem taryfowych połączeń danych (mogą być naliczane opłaty)

Wyłączone

Wyświetlimy przypomnienie, gdy będziemy chcieli wykonać ponowne uruchomienie. Jeśli chcesz otrzymywać więcej powiadomień dotyczących ponownego uruchomienia, włącz to ustawienie.

Wyłączone

Wstrzymaj aktualizacje

Tymczasowo wstrzymaj instalowanie aktualizacji na tym urządzeniu na maksymalnie 35 dni. Gdy aktualizacje zostaną wznowione, konieczne będzie pobranie najnowszych aktualizacji na to urządzenie, aby można było ponownie wstrzymać aktualizacje.

Wyłączone

Wstrzymanie teraz spowoduje wstrzymanie aktualizacji do 23.04.2019

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 przyspieszyć 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

Opcje zaawansowane

Domyślnie dynamicznie optymalizujemy przepustowość, której urządzenie używa w celu pobierania i przekazywania aktualizacji systemu Windows i aplikacji oraz innych produktów firmy Microsoft. Jeśli martwisz się zużyciem danych, możesz ustawić określony limit.

Ustawienia pobierania

Ogranicz poziom przepustowości wykorzystywany do pobierania aktualizacji w tle

45%

Ogranicz poziom przepustowości wykorzystywany do pobierania aktualizacji na pierwszym planie

90%

Ustawienia wysyłania

Ogranicz poziom przepustowości wykorzystywany do przesyłania aktualizacji do innych komputerów przez Internet

50%

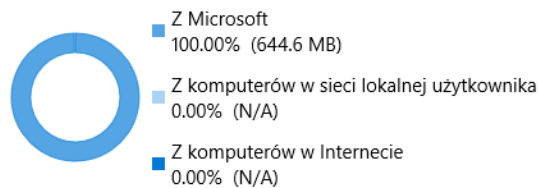
Miesięczny limit wysyłania danych

500 GB

Monitorowanie aktywności

Statystyka pobierania

Od 01.03.2019

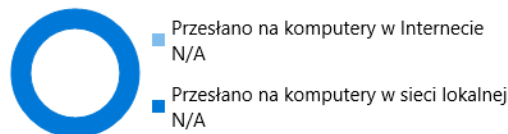


Średnia szybkość pobierania (zainicjowane przez użytkownika): N/A

Średnia szybkość pobierania (w tle): 10.7 Mbps

Statystyka wysyłania

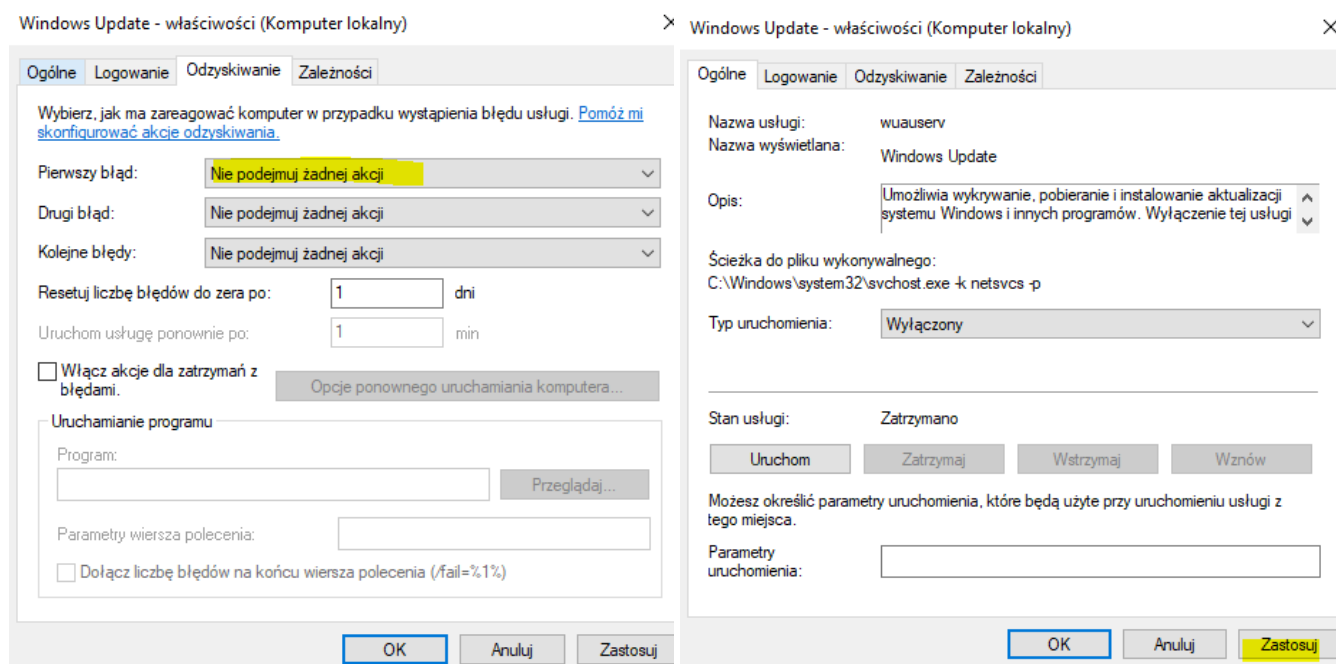
Od 01.03.2019



3. W celach sprawnego wykonywania ćwiczeń pozostaw ustawienie

The screenshot shows the Windows Update service properties window. The 'Zatrzymaj usługę' dialog box is open, displaying a progress bar and the message: 'Windows próbuje zatrzymać następującą usługę na Komputer lokalny...'. The 'Zatrzymaj' button is highlighted. The background window shows the service name 'wuauserv' and the display name 'Windows Update'. The 'Zatrzymaj' button is highlighted in the dialog box.

Efekt



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