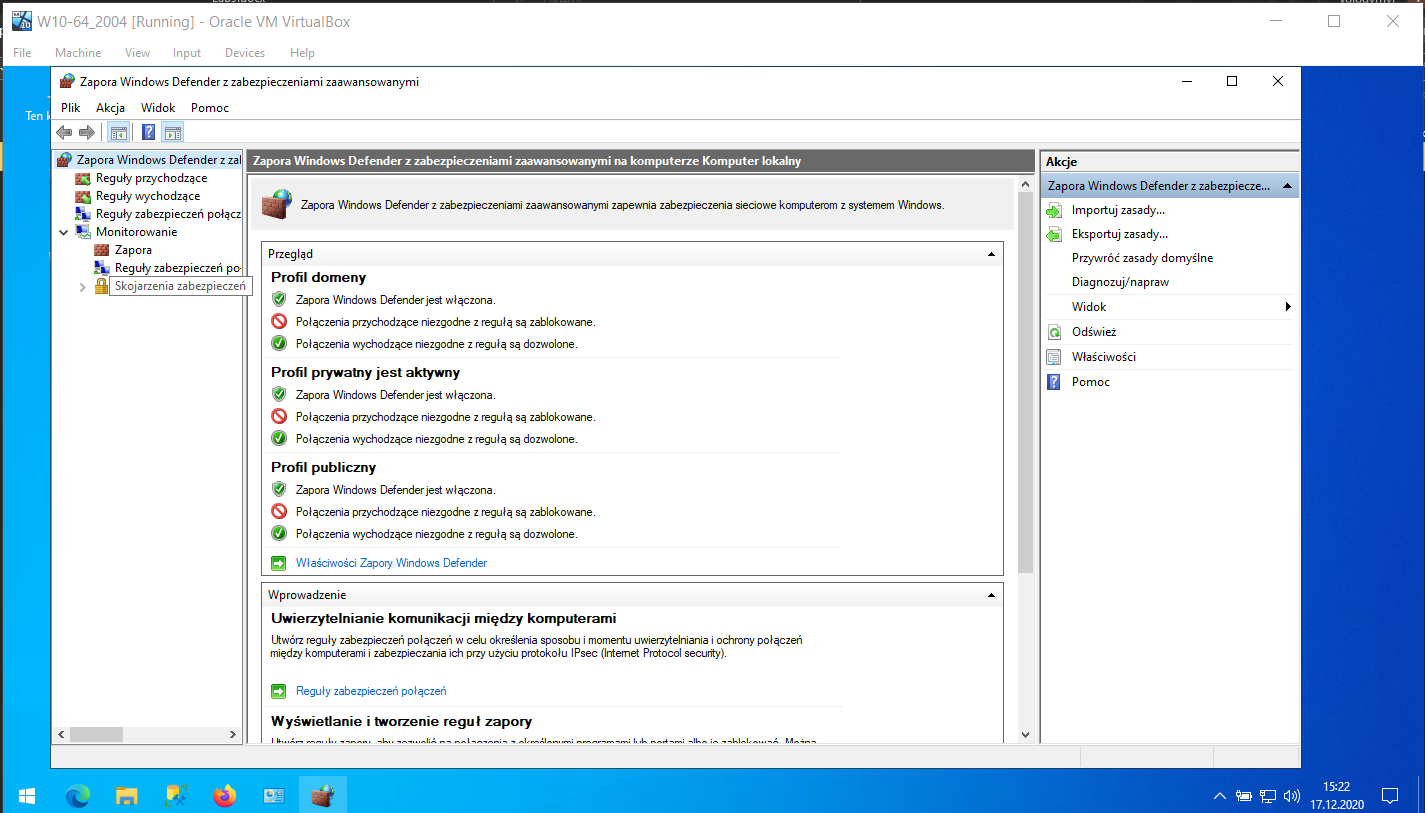
Windows Defender – program antywirusowy chroniący przed wszelkimi typami szkodliwego oprogramowania, w tym przed oprogramowaniem szpiegującym. Początkowo program służył jedynie do zwalczania programów szpiegowskich. Funkcjonował jako darmowy dodatek do systemu Windows XP, natomiast w przypadku systemów Windows Vista, Windows 7, Windows 8 i Windows 10 jest ich integralną częścią.

W najnowszym systemie Windows 10, program Windows Defender otrzymał nowy interfejs, który wraz z zawsze aktywną ikoną obszaru powiadomień, ma niejako przypominać użytkownikowi, że jest chroniony antywirusem (w domyśle: nie potrzebuje innego).

1. **Stan**



Standardowo wszystkie profile są włączone. Użytkownik jest chroniony przed wykorzystaniem Internetu.

1. **Reguły**

Mówiąc prościej, Zapora systemu Windows z zabezpieczeniami zaawansowanymi to snap-in zarządzania dla Zapory systemu Windows, z którego można w bardzo szczegółowy sposób kontrolować wszystkie reguły i wyjątki określające działanie Zapory systemu Windows.

**- Reguły przychodzące**

odnoszą się do ruchu przychodzącego z sieci lub Internetu do komputera lub urządzenia z systemem Windows. Na przykład, jeśli pobierasz plik przez BitTorrent, pobieranie tego pliku jest filtrowane przez regułę ruchu przychodzącego.

**- Reguły wychodzące**

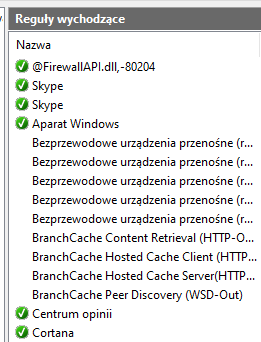
zasady te dotyczą ruchu pochodzącego z komputera i przechodzącego do sieci i Internetu. Na przykład prośba o załadowanie strony internetowej How-To Geek w przeglądarce internetowej to ruch wychodzący i jest filtrowana przez regułę ruchu wychodzącego. Kiedy witryna jest pobierana i ładowana przez przeglądarkę, jest to ruch przychodzący.

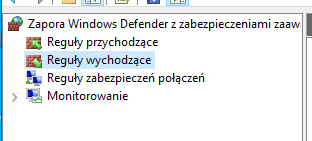
**- Reguły zabiezpieczeń połączeń**

brak wspólnych reguł, które są używane do zabezpieczenia ruchu między dwoma określonymi komputerami podczas przekraczania sieci. Ten typ reguły jest używany w bardzo kontrolowanych środowiskach ze specjalnymi wymaganiami bezpieczeństwa. W przeciwieństwie do reguł przychodzących i wychodzących, które są stosowane tylko do komputera lub urządzenia, reguły zabezpieczeń połączeń wymagają, aby oba komputery uczestniczące w komunikacji stosowały te same reguły.

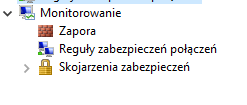
Wszystkie reguły można skonfigurować tak, aby były specyficzne dla określonych komputerów, kont użytkowników, programów, aplikacji, usług, portów, protokołów lub kart sieciowych.

Można wyświetlić reguły określonego typu, wybierając odpowiednią kategorię w kolumnie po lewej stronie.

Niektóre zasady będą miały zielony znacznik wyboru obok nazwy, podczas gdy inne będą miały szary kolor. Reguły z zielonym znacznikiem wyboru są włączone, co oznacza, że ​​są używane przez zaporę systemu Windows. Te z szarym znacznikiem wyboru są wyłączone i nie są używane przez Zaporę systemu Windows.



1. **Zakres monitorowania**

Poniżej wymienionych trzech typów reguł jest sekcja o nazwie "Monitorowanie". Po jej rozwinięciu można wyświetlić aktywne reguły zapory, aktywne reguły zabezpieczeń połączeń i wyświetlić aktywne powiązania zabezpieczeń.

Stowarzyszenie bezpieczeństwa to coś, czego większość z nas nigdy nie użyje. Jest to informacja o bezpiecznym szyfrowanym kanale na lokalnym komputerze lub urządzeniu, dzięki czemu informacje te mogą być wykorzystane do przyszłego ruchu sieciowego do określonego zdalnego komputera lub urządzenia. Tutaj można zobaczyć, którzy użytkownicy są obecnie podłączeni do komputera i który pakiet ochrony był używany przez system Windows do utworzenia powiązania zabezpieczeń.

**Ocena jakości Zapory Windows Defender**

Kilka lat temu program Windows Defender był naprawdę zły - nie był wystarczająco bezpieczny, aby chronić wszystkie komputery PC przed wirusami komputerowymi i złośliwym oprogramowaniem.

Ale ostatnio Windows zmienił Defendera w całkiem przyzwoity darmowy program antywirusowy. Na przykład firma Microsoft niedawno zaktualizowała Defendera, aby obejmowała piaskownicę i wykrywanie złośliwego oprogramowania w chmurze - zwiększając ogólną ochronę i przyspieszając wykrywanie zagrożeń.

Program Windows Defender nie mógł zablokować wielu wystąpień złośliwego oprogramowania podczas testów. Firma Microsoft nie wydaje wystarczającej liczby regularnych aktualizacji oprogramowania Defender. Powiedzmy, że zarazisz się wirusem, ale Microsoft nie pomoże Ci - po prostu powiedzą Ci, że powinieneś mieć zainstalowany inny program antywirusowy! Ogólnie rzecz biorąc, chociaż program Windows Defender jest dobrym podstawowym programem antywirusowym, obecnie nie ufałbym mu, jeśli chodzi o bezpieczeństwo mojego komputera, nawet z systemem Windows 10.

**Dlaczego warto korzystać z zapory windows?**

Zapora to funkcja bezpieczeństwa, która robi dwie rzeczy:

* Blokuje nieproszony ruch przychodzący przez Internet, który uważa za niebezpieczny. Na przykład może uniemożliwić przeglądarce internetowej lub jakiejkolwiek innej aplikacji łączącej się z Internetem, którą właśnie zainstalowałeś, dopóki nie udzielisz jej pozwolenia na łączenie się z Internetem. Zobacz kurs online dotyczący bezpieczeństwa cybernetycznego
* Blokuje nieautoryzowany dostęp do sieci lub udostępnionych plików. Jeśli ktoś próbuje połączyć się z Twoją udostępnioną siecią lub uzyskać dostęp do udostępnionych danych, ale nie ma na to pozwolenia, Twoja zapora sieciowa może temu zapobiec.

Zapora to ogólna funkcja zabezpieczeń, którą warto mieć. Może blokować dostęp robaków i innego złośliwego oprogramowania do komputera. Może też zapobiec przejęciu sieci przez hakerów.

Jest to szczególnie przydatne, jeśli:

* Korzystasz z połączenia szerokopasmowego, które jest domyślnie włączone przez cały czas. Może to uczynić cię łatwiejszym celem ataków złośliwego oprogramowania.
* Udostępniasz pliki rodzinie w sieci domowej. Twoja zapora sieciowa może odizolować Twoją sieć od reszty Internetu, aby nikt inny nie miał do niej dostępu.
* Używasz publicznych sieci Wi-Fi do łączenia się z Internetem. Sieci na lotniskach, dworcach kolejowych, parkach czy kawiarniach są mniej bezpieczne niż sieć w domu, ponieważ każdy może się z nimi połączyć. Zapora sieciowa nie szyfruje połączenia tak jak VPN, ale może ograniczyć potencjalne zagrożenia.

Jeśli wyłączysz zaporę Windows Defender, nie otrzymasz powiadomienia, gdy aplikacja na Twoim komputerze spróbuje połączyć się z Internetem. Może to spowodować lukę w zabezpieczeniach.

Należy jednak pamiętać, że zapora zapewnia tylko makro ochronę.

Nadal potrzebujesz oprogramowania chroniącego przed złośliwym oprogramowaniem do mikro-ochrony, tj. Do skanowania pobranych plików, aplikacji i innych plików oraz do pilnowania pamięci USB, odtwarzaczy multimedialnych i zewnętrznych dysków twardych.

A to prowadzi nas do podstawowych funkcji programu Windows Defender.

**Wniosek**

Zapowa Windows oczywiście jest niezbędna w Windowsie. Korzystamy z niej codziennie. Ale jak już wiemy nie wszystkie rodzaje wirusów są sprawdzane i filtrowane przez niej. Dlatego oprucz tego, że mamy zainstalowanej zapory Windows musimy mieć jeszcze większego i liepszego antywirusa. Moja ocena to 6 z 10.