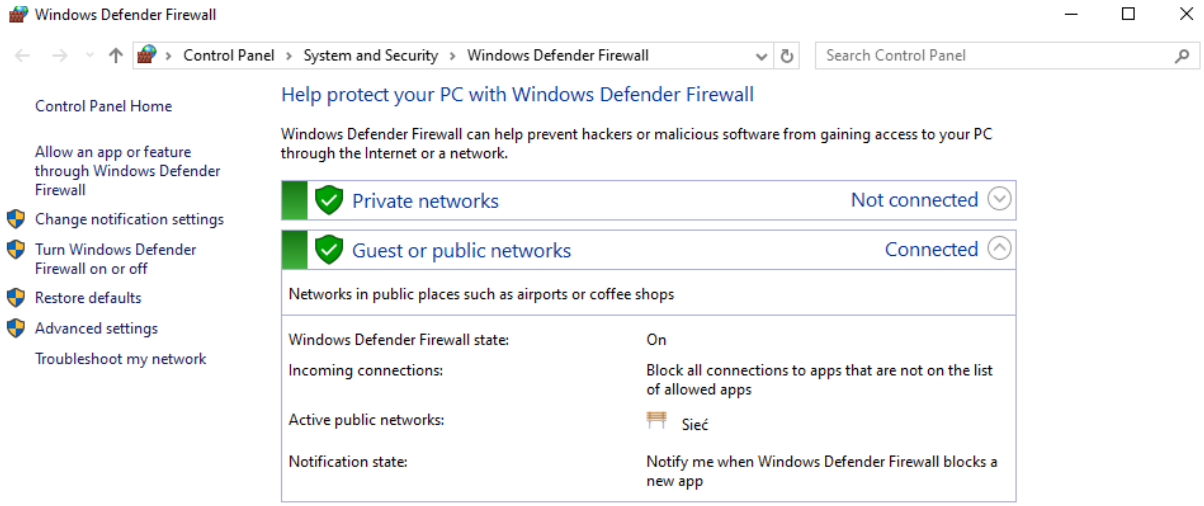
Krótki poradnik o Windows Firewall.

Jako że podstawowa konfiguracja Windows Firewall nie jest zbyt skomplikowana poświęce naszą uwagę tworzeniu reguły w konkretnym scenariuszu.

Windows Firewall to wbudowany system zapory ogniowej w systemie operacyjnym Windows, który chroni komputer przed nieautoryzowanym dostępem z sieci.

Konfiguracja Windows Firewall

1. Otwórz Panel sterowania i kliknij na "Windows Firewall".
2. W sekcji "Settings" wybierz "Włącz Windows Firewall" dla sieci domowej i publicznej.
3. W sekcji "Rules" możesz dodać nowe reguły, aby zezwolić lub zabronić dostępu do określonych aplikacji lub portów.



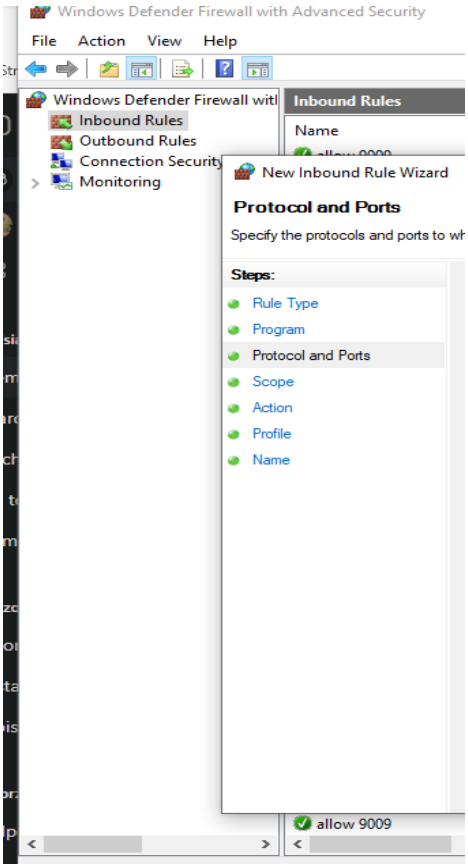
Czym jest Windows Firewall?

Windows Firewall to wbudowana zapora sieciowa w systemach operacyjnych Windows, która odgrywa kluczową rolę w cyberbezpieczeństwie, monitorując i kontrolując ruch sieciowy w celu ochrony przed nieautoryzowanym dostępem oraz innymi zagrożeniami. Umożliwia precyzyjne definiowanie reguł w oparciu o protokoły, porty, programy i użytkowników, co pozwala na dostosowanie zabezpieczeń do specyficznych potrzeb i środowiska. Dobrze skonfigurowany firewall nie tylko blokuje próby skanów i nieautoryzowanego dostępu, jak ping, UDP czy TCP, ale także umożliwia logowanie podejrzanych działań oraz segmentację sieci dla lepszej ochrony. Dzięki regularnym aktualizacjom i ścisłej kontroli dostępu, firewall skutecznie chroni systemy przed nowymi zagrożeniami, stanowiąc solidną barierę bezpieczeństwa w sieci.

Scenariusz

Załóżmy scenariusz że mamy atakującego który próbował ataku ssh na nasz serwer lub zeskanować nasze porty i podczas tego nie używał proxychainów ani nie maskował swojego adresu IP podszywając się pod inny. Chcemy go zablokować poprzez dodanie reguły do firewall, jak to robimy?

Krótki opis każdego elementu który będzie niezbędny w stworzeniu **„reguły”**



Scope (Zasięg): Określa, które adresy IP mogą korzystać z reguły zapory; definiuje, czy reguła dotyczy lokalnych, zdalnych lub obu typów adresów.

Actions (Akcje): Decyduje o tym, co ma się stać z ruchem, który pasuje do reguły; może to być zezwolenie na ruch, blokowanie go lub rejestrowanie.

Profiles (Profile): Umożliwia przypisanie reguły do jednego lub więcej profili zapory (domena, prywatny, publiczny), co pozwala na różne ustawienia w różnych środowiskach.

Protocols and Ports (Protokoły i porty): Określa, które protokoły (np. TCP, UDP) oraz porty (np. 80 dla HTTP) są objęte regułą, co pozwala na szczegółowe dostosowanie reguły.

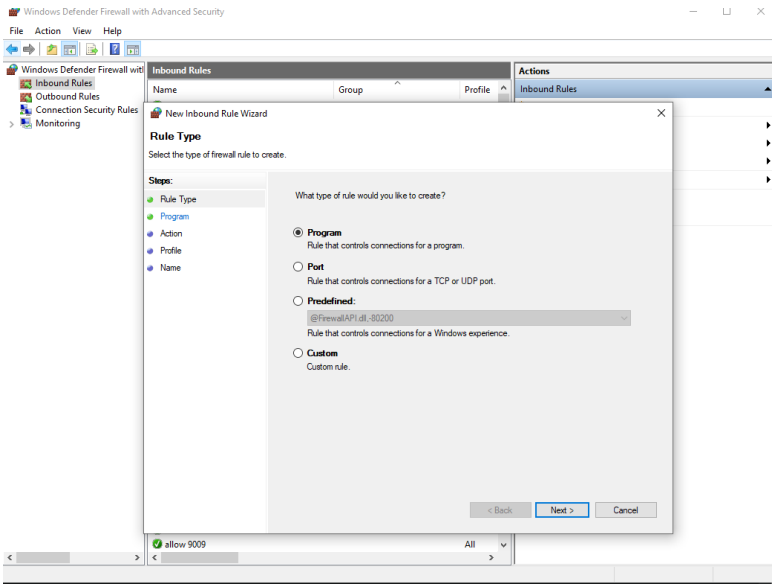
Programs (Programy): Umożliwia określenie, które aplikacje są objęte regułą; można zezwolić lub zablokować ruch tylko dla określonych programów.

Users (Użytkownicy): Definiuje, dla których użytkowników lub grup reguła ma zastosowanie; można ograniczyć dostęp na podstawie konta użytkownika.

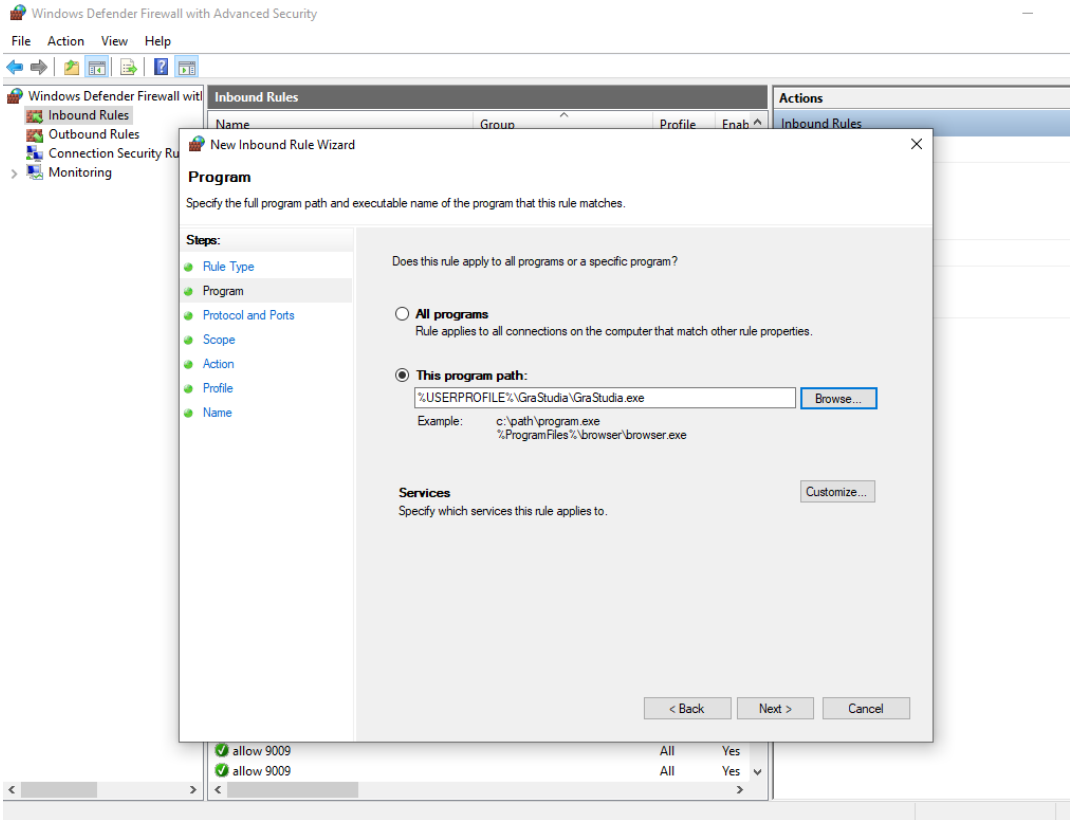
Logging (Rejestrowanie): Umożliwia włączenie lub wyłączenie rejestrowania zdarzeń związanych z regułą, co jest przydatne do monitorowania i diagnostyki.

Proces tworzenia „**reguły**”

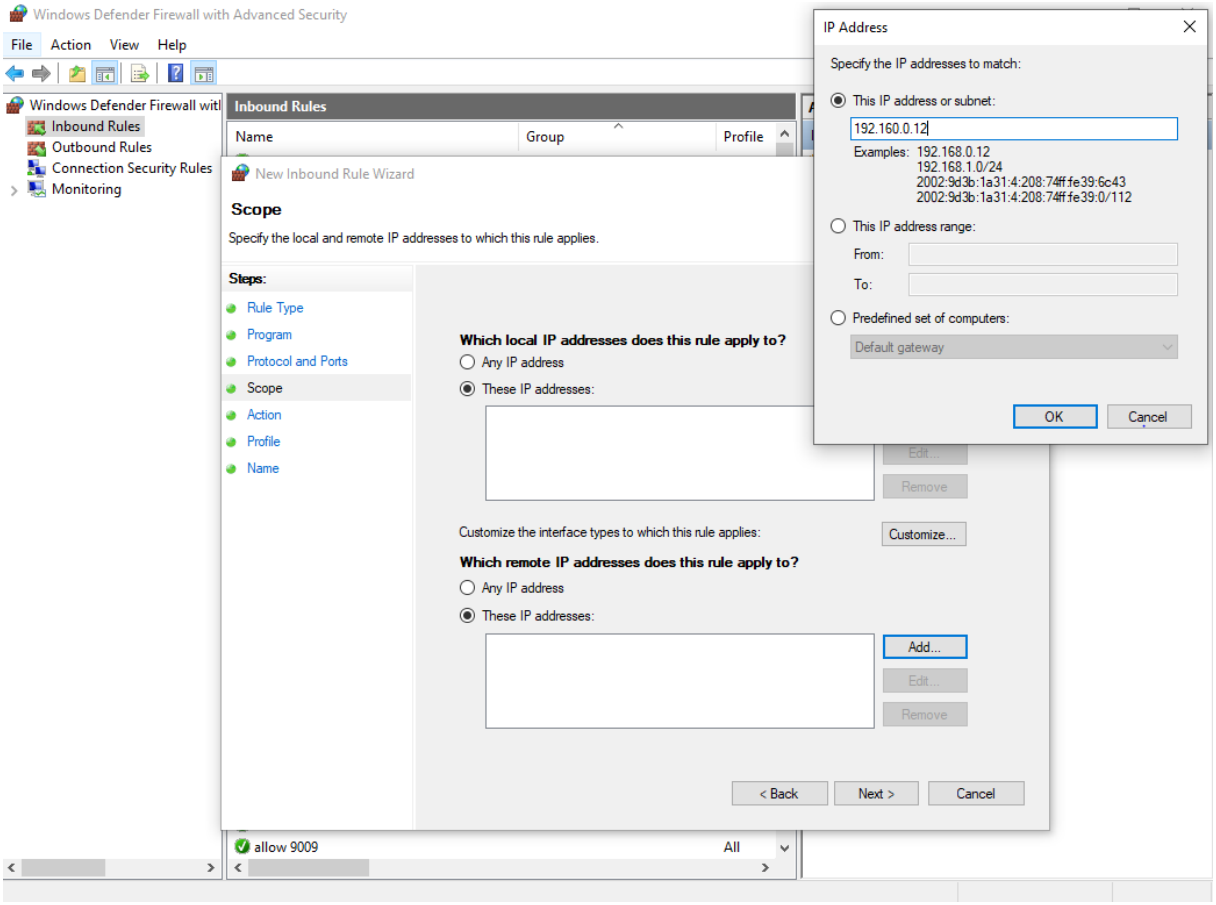
1. Uruchom **“Windows Defender Firewall with Advanced Security”**
2. W sekcji "**Actions**" kliknij na **"New Rule".**
3. Wybierz **"Inbound Rules"** i kliknij "Dalej".



4. Następnie zdefiniuj typ reguły czy jest to program czy port czy konkretny adress

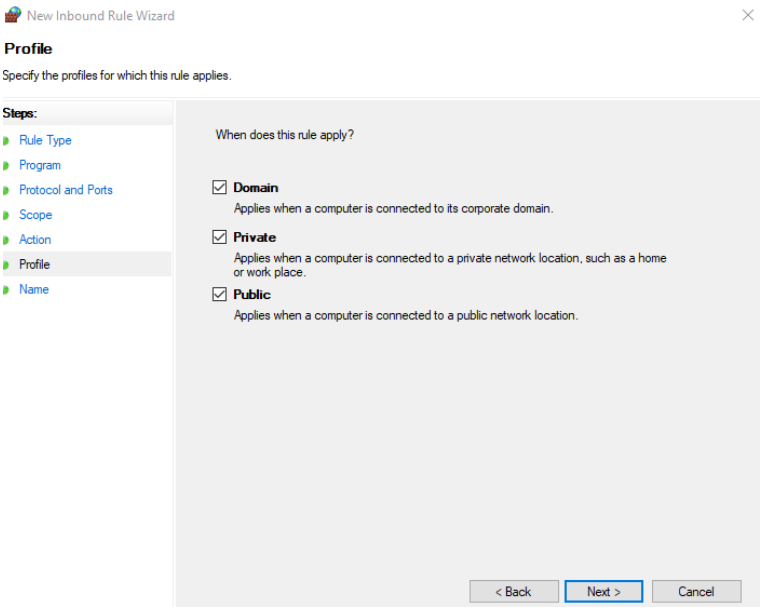


5. W **„Steps”** wejdź w **„Scope”** a następnie dodaj adres



6. Następnie wejdz w **„Action”** wybierz **„Block the connection”**

7. Skonfiguruj co **„Reguła”** ma blokować



8. Nazwij regułę, opisz i kliknij "Zakończ".

W ten sposób dodaliśmy reguły która blokuje jakikolwiech ruch przychodzący ze złośliwego adresu IP.

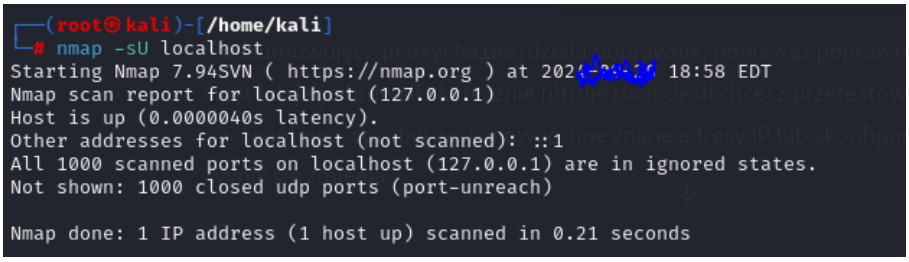
Jak dobrze skonfigurowany Firewall reaguje na rózne rodzaje skanów wykonanych przez skanery podatności typu nmap?

1. TCP Scan

Firewall może blokować nieautoryzowane połączenia na zamkniętych portach, odpowiadając pakietem **RST (Reset)**, co sygnalizuje, że port jest zamknięty, lub ignorować próbę, co może sprawić, że skanujący uzna port za „ukryty" lub zamknięty. Przy poprawnej konfiguracji, firewall zezwala tylko na połączenia na portach, które są wyraźnie dozwolone, blokując pozostałe.

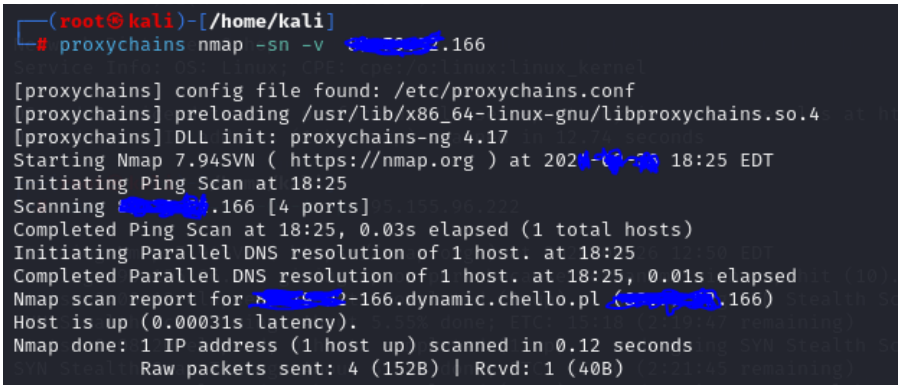
2. UDP Scan

Reakcja: Ponieważ UDP jest protokołem bezpołączeniowym, firewall nie zawsze musi wysyłać odpowiedź na nieautoryzowane zapytania. W przypadku zamkniętych portów dobrze skonfigurowany firewall zazwyczaj po prostu ignoruje próbę, co może dać skanującemu fałszywe wrażenie, że port jest otwarty lub zamknięty (tzw. **"silent drop"**). W niektórych przypadkach może odpowiedzieć komunikatem **ICMP Destination Unreachable**.



3. ICMP Scan (Ping)

Reakcja: Firewall może być skonfigurowany tak, aby blokował zapytania ICMP (np. **Echo Request**), co uniemożliwia skanującym ustalenie, czy host jest dostępny. W zależności od polityki bezpieczeństwa, firewall może całkowicie ignorować ping, co sprawia, że host wydaje się niedostępny, lub odpowiadać jedynie na zapytania zaufanych źródeł.



Monitorowanie Logów

Dlaczego Monitorowanie jest Ważne?

Monitorowanie to kluczowy element zarządzania bezpieczeństwem, który pozwala na:

Wykrywanie nieautoryzowanych prób dostępu – Śledzenie prób połączeń umożliwia szybkie reagowanie na potencjalne zagrożenia.

Analizę ruchu sieciowego – Dzięki monitorowaniu można zrozumieć, jakie rodzaje ruchu są normalne, a co może wskazywać na problem.

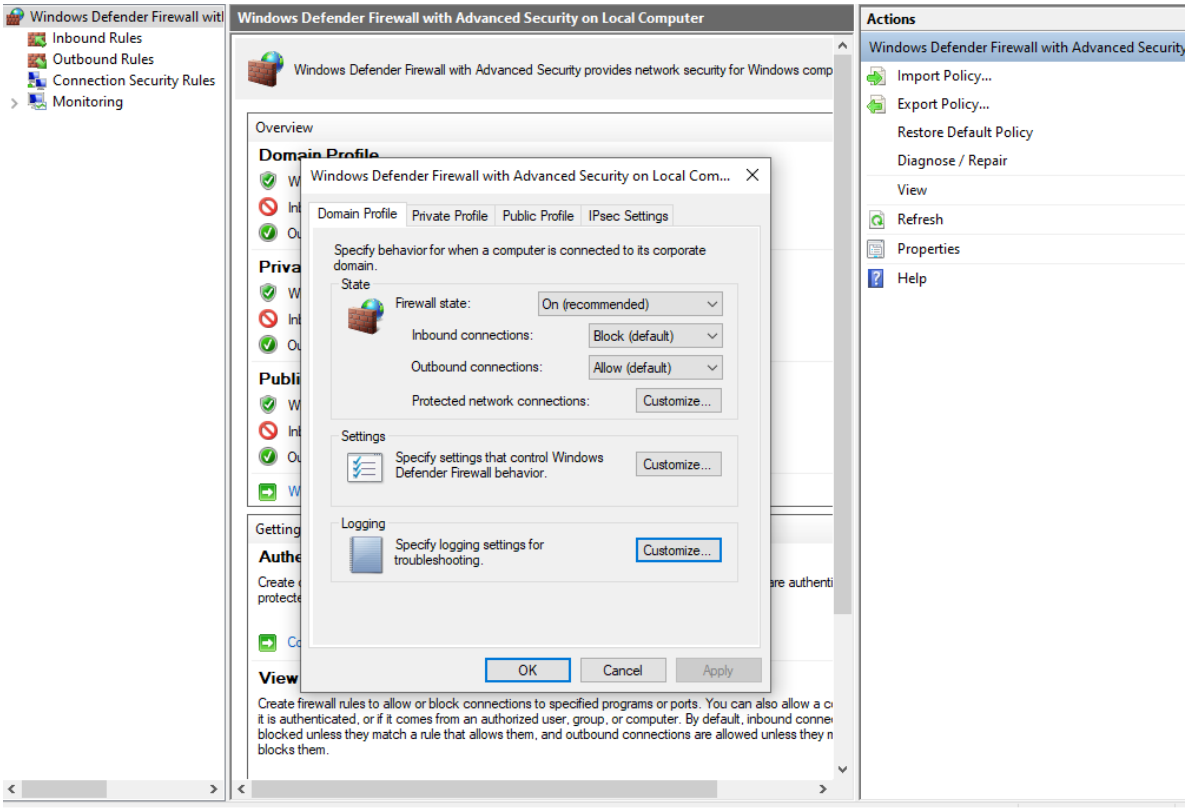
Audyt i zgodność – Posiadanie odpowiednich logów jest często wymagane do celów audytowych i zgodności z przepisami.

Włączanie Logowania w Windows Firewall

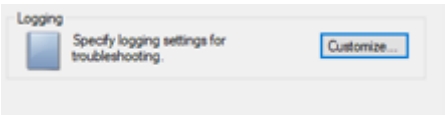
Otwórz Windows Defender Firewall z Zaawansowanymi Zabezpieczeniami

Możesz to zrobić naciskając skrót klawiszowy Winodws + R i wpisując wf.msc

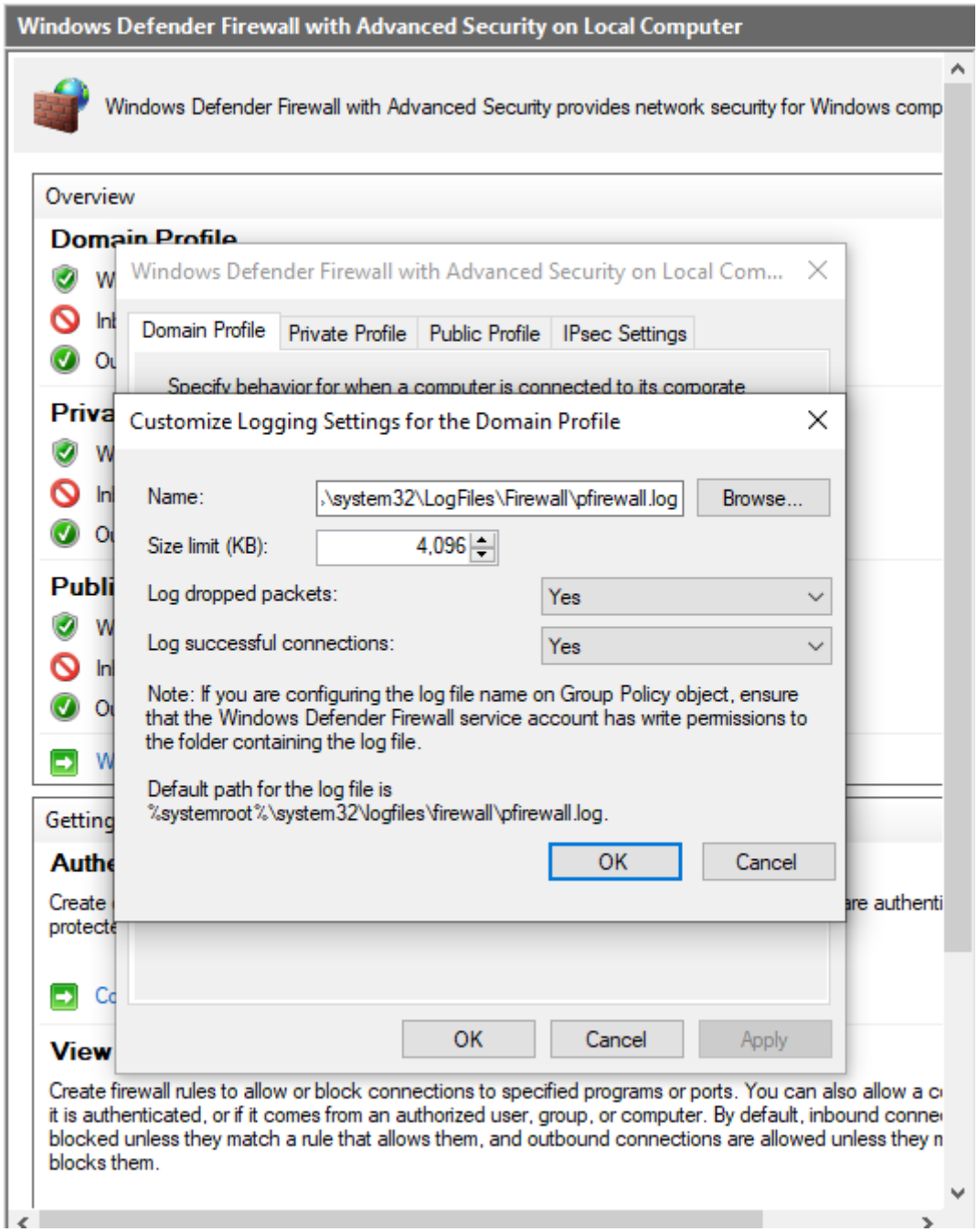
Następnie pklikasz prawym przyciskiem myszy na Windows Defender Firewall with Advanced Security i wybierasz „properties”.



Wchodzisz w zakładkę „Logging”



A następnie klikasz **Customize** w sekcji **Log dropped packets** oraz **Log successful connections** i wybierasz odpowiednie opcje, aby rejestrować zarówno zablokowane pakiety, jak i udane połączenia.



Po włączeniu logowania, można analizować logi, aby identyfikować nieautoryzowane działania:

Lokalizacja logów: Logi znajdują się w lokalizacji domyślnej, zazwyczaj w C:\Windows\System32\LogFiles\Firewall.

Narzędzia do analizy: Możesz użyć prostych narzędzi do przeglądania plików tekstowych, takich jak Notepad, lub bardziej zaawansowanych narzędzi analitycznych jak np. ELK lub Splunk.