agnitum

OUTPOSTPRO
FIREWALL

Instrukcja obsługi

www.agnitum.com
Instrukcja użytkownika

Szczegółowa dokumentacja dotycząca działania programu Outpost Firewall Pro.
Aby uzyskać pomoc w programie, naciśnij klawisz F1.
Aby uzyskać dodatkowe informacje, skorzystaj ze strony www.outpost.pl.

Spis treści

1. Witamy w programie Outpost Firewall Pro!

W dzisiejszych czasach, kiedy liczba zagrożeń związana z korzystaniem z Internetu rośnie w bardzo szybkim tempie, konieczne jest zupełnie nowatorskie podejście do tematu zabezpieczeń. Oznacza to, że producenci do oprogramowania stoją przed dużym wyzwaniem jakim jest dostarczanie narzędzi ochrony proaktywnej, co pozwala zabezpieczyć się nie tylko przed znanymi wirusami ale również przed nowymi niezdefiniowanymi jeszcze zagrożeniami.

Firma Agnitum wychodząc naprzeciw oczekiwaniom użytkowników prezentuje Outpost Firewall Pro. Program łączy w sobie najlepsze metody ochrony w jednym zintegrowanym produkcie, który zapewnia pełne bezpieczeństwo oraz niezawodność. Program Outpost Firewall Pro, chroni Twoje dane 24 godziny na dobę, siedem dni w tygodniu bez względu na to, jakie czynności wykonujesz.

Korzyści

- Program kontroluje połączenia Twojego komputera z innymi komputerami - blokuje dostęp hakerom oraz zapobiega nieupoważnionemu dostępowi do sieci. Poprzez ochronę dostępu do sieci aplikacji, program powstrzymuje złośliwe aplikacje przed komunikacją "z" i "do" Twojego komputera.
- Ochrona proaktywna monitoruje zachowanie wszystkich aplikacji, aby proaktywnie chronić przeciwko trojanom, spyware'om i wszystkim rodzajom technik hakerskich używanych do wykradania danych.
- Outpost Firewall Pro używa wyspecjalizowanych technik, które nie zezwalają na wyłączenie ochrony przez specjalnie stworzone do tego typu działań zagrożenia.
- Efektywny skaner zagrożeń wykrywa i przenosi do kwarantanny lub usuwa automatycznie spyware'y lub inne złośliwe oprogramowanie.
- Rezydentny monitor na żądanie stale chroni przed zagrożeniom i posiada niewielki wpływ na wydajność systemu.
- Moduł kontroli stron WWW chroni przed zagrożeniami w Internecie. Blokuje dostęp do zainfekowanych stron WWW oraz zapobiega ujawnieniu prywatnych danych.
- Skuteczna i łatwe w obsłudze zabezpieczenie oferuje rozległe wsparcie dla początkujących użytkowników, a zaawansowanym użytkownikom stwarza możliwość stworzenia własnych profili.
- Pomoc on-line zawiera informacje o interfejsie programu Outpost Firewall Pro, ustawieniach i funkcjonalności.

1.1. Wymagania systemowe

Outpost Firewall Pro może być zainstalowany na systemach operacyjnych Windows 2000 SP4, Windows XP, Windows Server 2003,Windows Vista i Windows 7. Minimalne wymagania systemowe dla Outpost Firewall Pro:

- Procesor: 450 MHz Intel Pentium lub kompatybilny;
- Pamięć: 256 MB;
- Miejsce na dysku twardym: 100 MB.

Uwaga:

- Outpost Firewall Pro wspiera platformy 32-bitowe oraz 64-bitowe. Pobierz odpowiednią wersję programu ze strony: www.outpost.pl.
- Do poprawnego działania programu nie są wymagane specjalne ustawienia konfiguracji programu lub urządzeń.

- Program Outpost Firewall nie powinien być uruchamiany z innymi programami służącymi do ochrony komputera przed złośliwymi programami. Może to spowodować niestabilność systemu lub jego utratę.

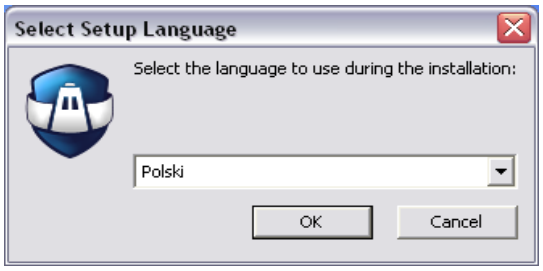
1.2. Instalacja Outpost Firewall Pro

Proces instalacji programu Outpost Firewall Pro jest zbliżony do instalacji wielu innych programów w systemie Windows. Instalacja programu Outpost Firewall Pro, krok po kroku:

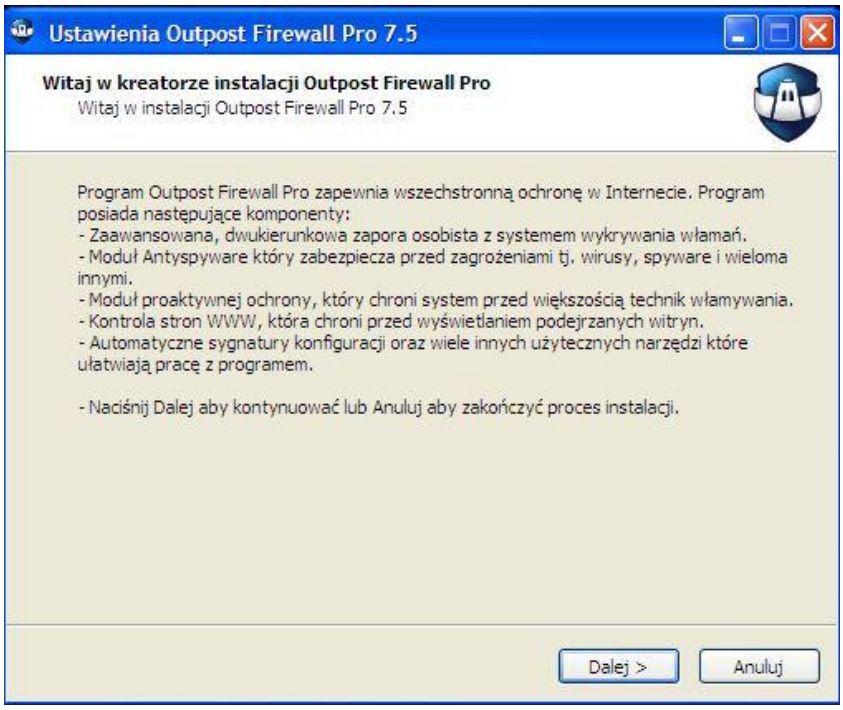
Uwaga:
Przed instalacją programu Outpost Firewall Pro, odinstaluj inne oprogramowanie tego typu, a następnie uruchom ponownie komputer.

1. Zamknij wszystkie aktywne aplikacje.
   a) jeśli instalujesz program pobrany ze strony uruchom OutpostFirewallProInstall.exe;
   b) jeśli instalujesz program z płyty CD, kreator instalacji zostanie uruchomiony automatycznie. Jeśli instalacja nie uruchamia się automatycznie, naciśnij przycisk **Start** na pasku zadań systemu Windows i wybierz **Uruchom**. W polu **Otwórz**, wprowadź pełną ścieżkę do pliku instalacyjnego (OutpostFirewallProInstall.exe). **Przykład:** Jeśli instalator znajduje się na dysku D: w folderze Downloads i podfolderze Outpost, prawidłowa ścieżka powinna wyglądać następująco: **D:\downloads\outpost\OutpostFirewallProInstall.exe**
2. Naciśnij przycisk **OK**.

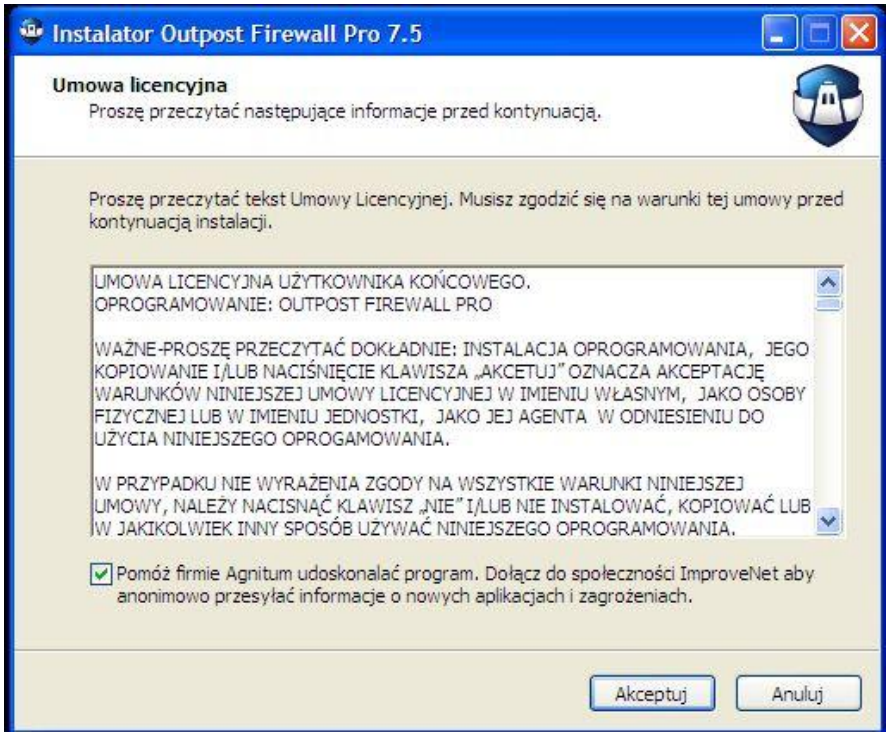
Kreator instalacji składa się z kilku kroków. Po każdym z nich przycisk **Dalej** przeniesie Cię do kolejnego kroku, a przycisk **Wstecz** cofnie Cię do poprzedniego kroku. Przycisk **Anuluj** przerywa proces instalacji. Instalacja rozpoczyna się wyborem języka programu.



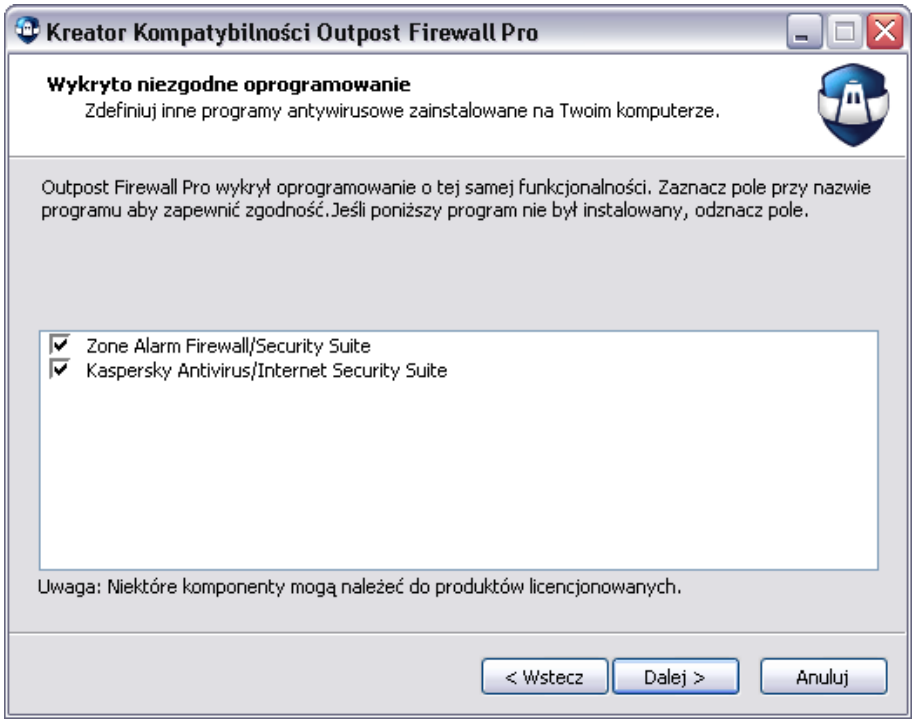
Wybierz pożądany język, a następnie naciśnij **OK**. Instalator wyświetli okno powitalne programu:



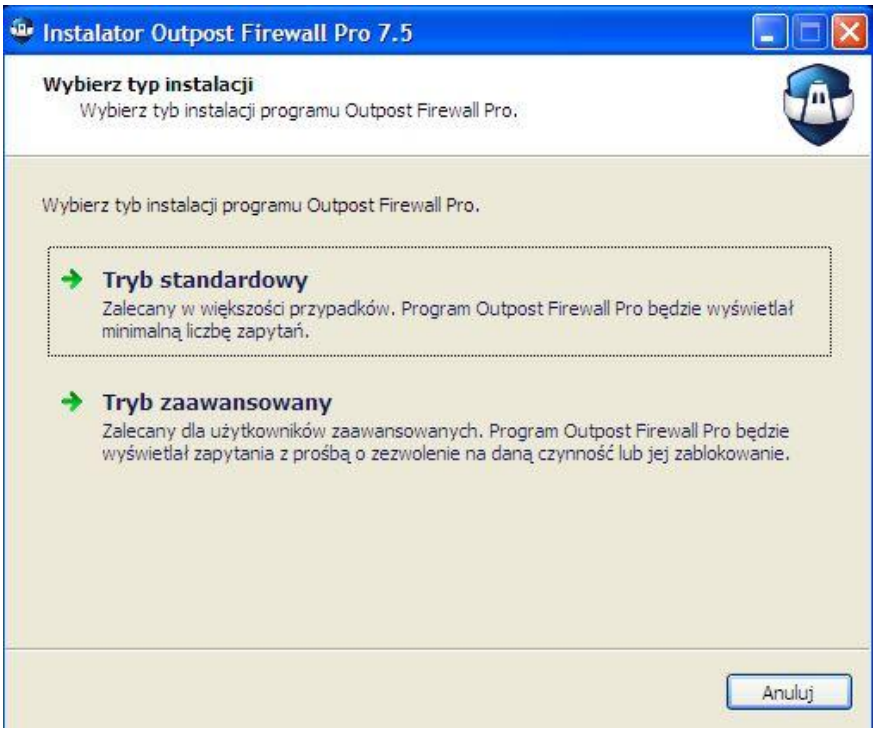
Po naciśnięciu przycisku **Dalej** zostaniesz poproszony o zaakceptowanie Umowy Licencyjnej. Prosimy o uważne jej przeczytanie. Przycisk **Dalej** stanie się aktywny po zaznaczeniu pola **Akceptuję Warunki umowy**:



Jeżeli z systemu nie został usunięty program do ochrony komputera, instalator wyświetli informację o wykryciu niekompatybilnego oprogramowania:

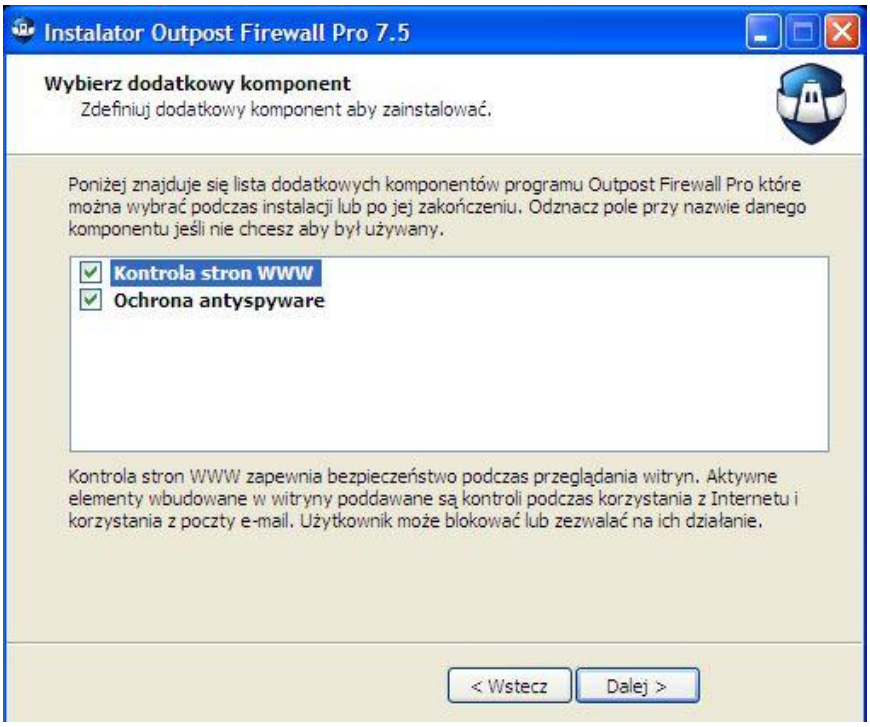


Po wykryciu niekompatybilnego oprogramowania, instalator nie będzie w stanie dokończyć procesu instalacji. Po wykryciu częściowo kompatybilnego oprogramowania, kreator zaproponuje możliwe rozwiązania, w celu zachowania poprawnego działania. Po zaakceptowaniu Umowy Licencyjnej, przycisk **Dalej** przeniesie Cię do kolejnego kroku, jakim jest **Wybór trybu instalacji**.

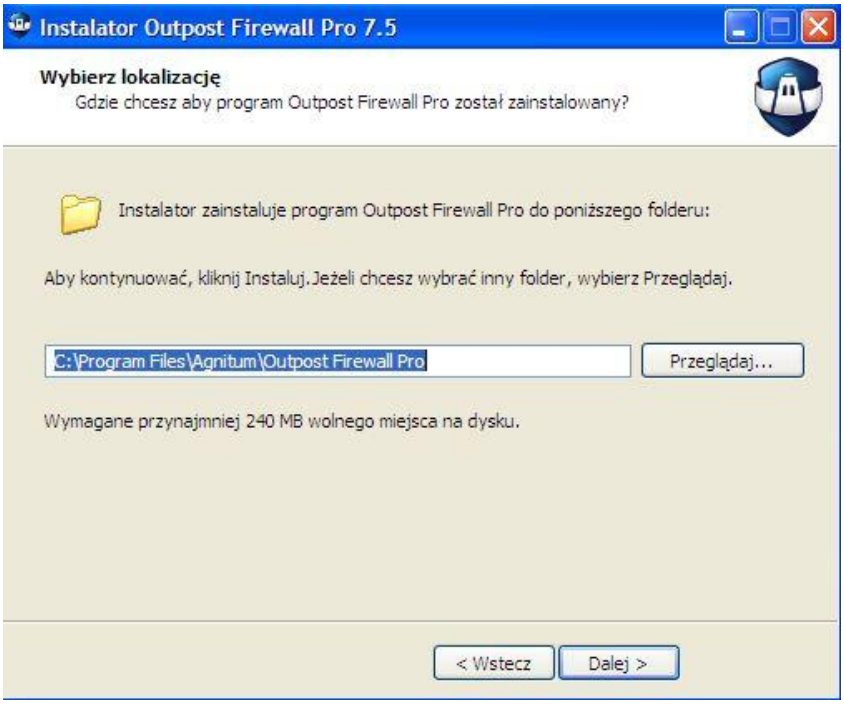


Wybór trybu standardowego spowoduje bezpośrednie uruchomienie instalacji aplikacji bez wyświetlania dodatkowych pytań pozwalających na konfigurację aplikacji.

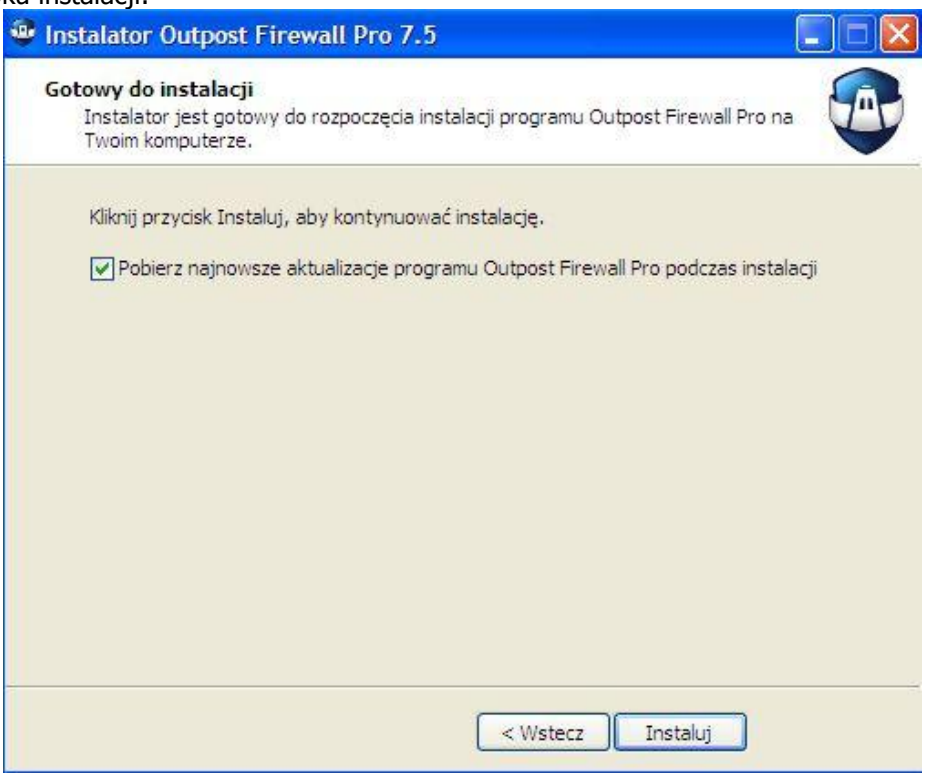
Tryb zaawansowany zalecany jest dla zaawansowanych użytkowników wyświetlając dodatkowe pytania konfiguracyjne.



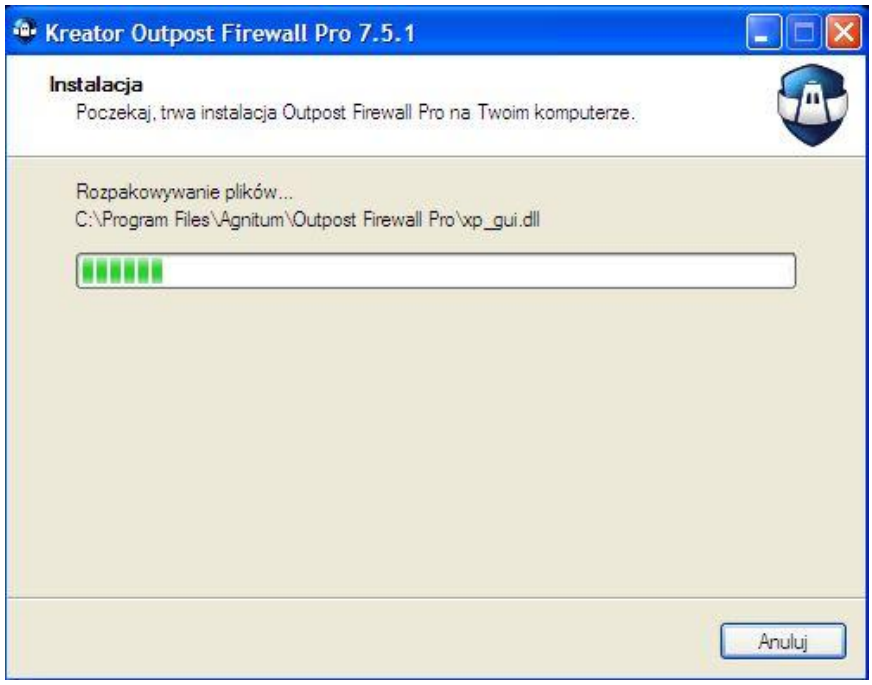
Wybór trybu zaawansowanego pozwoli na zdefiniowanie dodatkowych czynności konfiguracyjnych. W pierwszym kroku aplikacja umożliwi wybór komponentów aplikacji do zainstalowania.



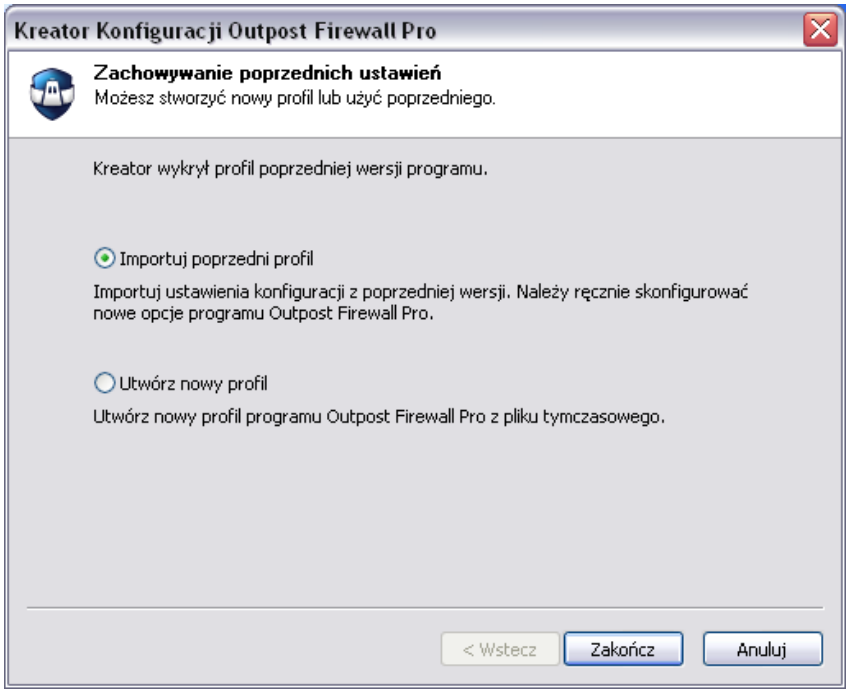
Wybierz folder docelowy, w którym program Outpost Firewall Pro zostanie zainstalowany - możesz wybrać folder domyślny lub wybrać inną lokalizację. Jeśli chcesz zmienić folder domyślny, naciśnij **Przeglądaj**. Wybierz folder lub stwórz nowy, a następnie naciśnij **OK**. Klikając **Dalej** przejdziesz do ostatniego kroku instalacji:



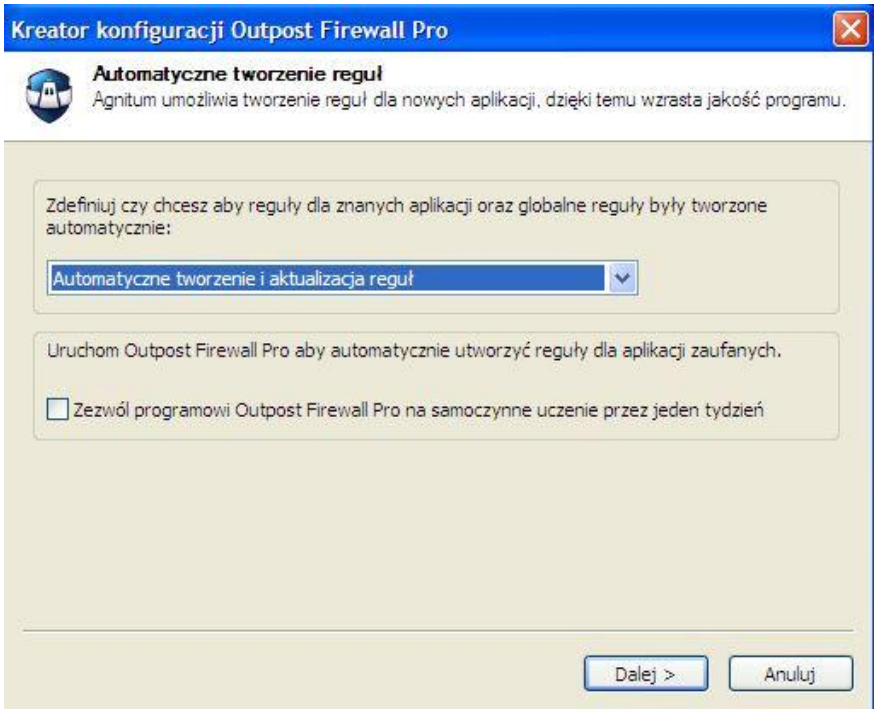
Zaznacz opcję **Pobierz najnowsze aktualizacje programu Outpost Firewall Pro podczas instalacji,** w celu pobrania ustawień reguł programu**.** Jeśli chcesz zmienić poprzednie ustawienia, naciśnij przycisk **Wstecz**. Wciśnięcie przycisku **Instaluj** rozpocznie proces instalacji. W trakcie instalacji możesz śledzić jej postęp:



Po zakończeniu instalacji, **Kreator** konfiguracji pomoże Ci stworzyć nowy profil lub zaimportować poprzedni (jeśli instalujesz nowszą wersję programu):



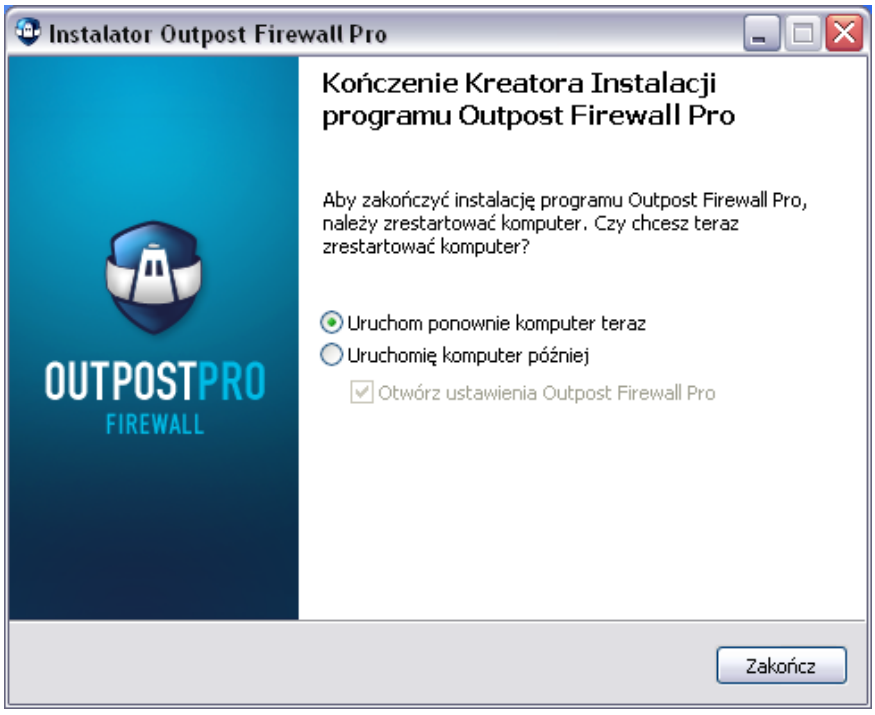
Podczas importowania poprzedniego profilu, system automatycznie skopiuje Twoje ustawienia z poprzedniej wersji aplikacji. W celu zakończenia instalacji programu Outpost Firewall Pro system zostanie uruchomiony ponownie.



W kolejnym kroku użytkownik ma możliwość wyboru automatycznego tworzenia reguł. Włączenie tej opcji sprawi, że globalne reguły i reguły dla znanych aplikacji będą tworzone automatycznie podczas pierwszego żądania wykonania czynności (na przykład, dostęp do sieci lub modyfikacja pamięci). Jeśli nie chcesz włączać autotworzenia reguł, wybierz **Wyłącz automatyczne tworzenie reguł**.

Opcja **Zezwól programowi Outpost Firewall Pro na samoczynne uczenie przez jeden tydzień** pozwoli na automatyczne stworzenie niezbędnych reguł**.**

Naciśnij **Zakończ,** aby zatwierdzić zmiany. System zostanie uruchomiony ponownie:



Ważne:
Przed uruchomieniem programu Outpost Firewall Pro musisz uruchomić ponownie komputer.

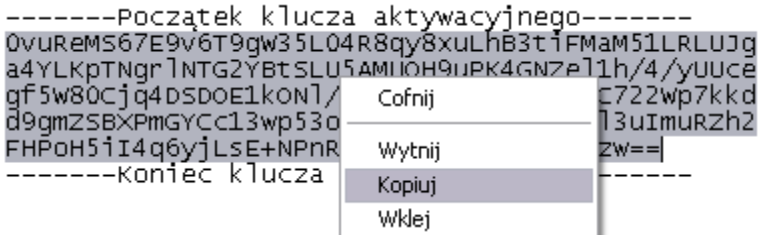
1.3. Rejestracja Outpost Firewall Pro

Program Outpost Firewall Pro jest dostępny w wersji próbnej. Masz prawo korzystać z wersji próbnej przez 30 dni od daty zainstalowania programu.

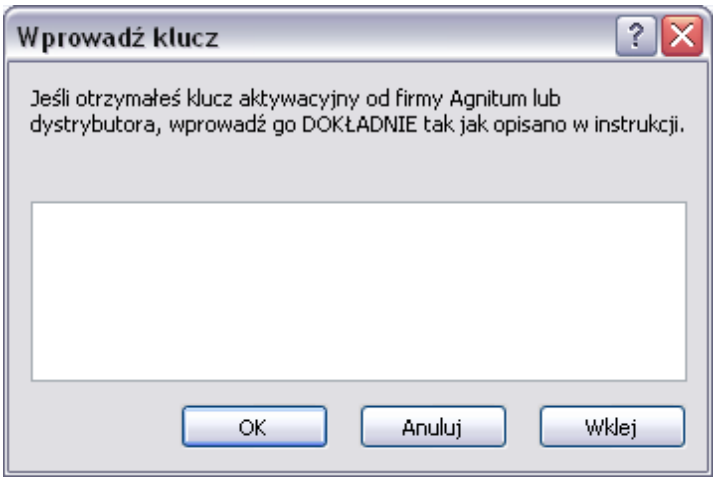
Informacje, gdzie można kupić program Outpost Firewall Pro dostępne są na stronie http://www.outpost.pl/gdzie-kupia/

Jak wprowadzić klucz aktywacyjny

1. Po otrzymaniu klucza aktywacyjnego, otwórz wiadomość zawierającą klucz, następnie zaznacz za pomocą myszy **początek klucza** i **koniec klucza.** Cały ciąg powinien być zaznaczony, tak jak to pokazane poniżej:



2. Kliknij prawym klawiszem myszy w podświetlony tekst i wybierz **Kopiuj** z menu kontekstowego aby skopiować klucz do schowka.
3. Wybierz **Start** > **Programy** > **Agnitum** > **Outpost Firewall Pro** i naciśnij **Wprowadź klucz aktywacyjny**. Naciśnij przycisk **Wprowadź klucz,** a następnie wybierz **Wklej.** Klucz aktywacyjny zostanie wprowadzony w puste pole.



4. Naciśnij **OK, aby** zatwierdzić klucz i zamknąć okno.

Program sprzedawany jest z licencją bezterminową oraz serwisem na rok lub dwa lata. Po wygaśnięciu serwisu możesz zakupić wznowienie, aby zawsze korzystać z najbardziej aktualnej ochrony. Informacje, gdzie można kupić program Outpost Firewall Pro dostępne są na stronie http://www.outpost.pl/gdzie-kupia/

Uwaga:
Program Outpost Firewall Pro i Outpost Security Suite są niezależnymi produktami a ich klucze aktywacyjne nie mogą być stosowane zamiennie. Oznacza to, że klucz do programu Outpost Firewall Pro nie będzie pasował do programu Outpost Security Suite i na odwrót. Upewnij się, że wprowadzasz prawidłowy klucz.

2. Interfejs użytkownika i podstawowe opcje

Gdy uruchamiasz program Outpost Firewall Pro po raz pierwszy wyświetla się okno główne programu, które jest równocześnie centralnym panelem programu. Z poziomu okna głównego możesz monitorować połączenia sieciowe oraz modyfikować istniejące ustawienia programu.

Aby wyświetlić główne okno programy, gdy jest ono zminimalizowane do ikony w zasobniku systemowym, należy:

1. Nacisnąć prawym przyciskiem myszy na ikonę programu.
2. Z menu kontekstowego wybrać **Pokaż/Ukryj**.

Aby zamknąć główne okno programu Outpost Firewall Pro, należy nacisnąć znak X w prawym górnym rogu programu. Program nie zostanie zamknięty; główne okno zostanie zminimalizowane do ikony w zasobniku systemowym.

Główne okno składa się z:

- **Paska narzędzi**
- **Lewego panelu**
- **Panelu informacyjnego**
- **Paska statusu**

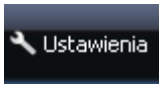
Pasek statusu znajduje się na dole głównego okna. Wyświetla on aktualny status programu.

2.1. Pasek narzędzi

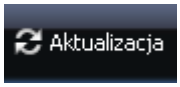
Pasek narzędzi znajduje się w górnej części głównego okna programu. Przyciski, których opis wyświetla się jeśli przez chwilę przytrzymasz nad nimi kursor myszy, powstały z myślą o użytkownikach. Umożliwiają one bezpośrednie przejście do wybranych funkcji programu (użytkownik nie musi przechodzić przez kilka okien).
Wygląd paska narzędzi:

Przyciski paska narzędzi:

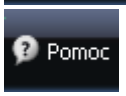
Uruchamia skanowanie systemu



Otwiera ustawienia programu Outpost Firewall Pro



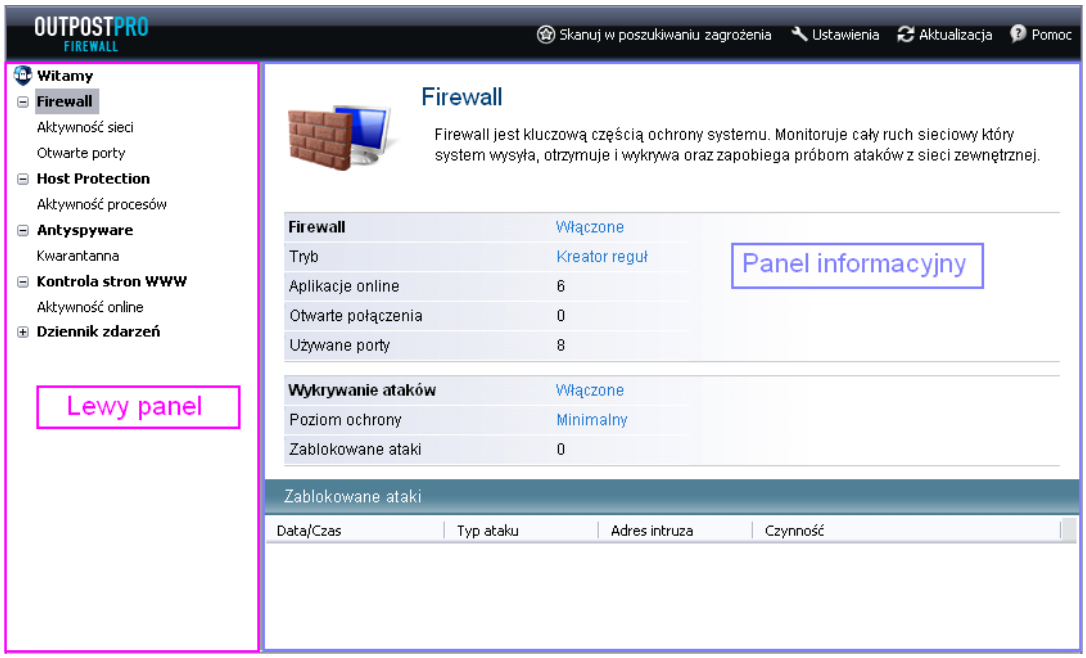
Pobiera najnowsze aktualizacje programu



Otwiera okno pomocy

2.2. Panele lewy i informacyjny

Główne okno programu składa się z dwóch paneli. Lewy panel zawiera listę wszystkich kategorii programu: połączenia, porty, moduły. Panel informacyjny wyświetla szczegółowe informacje dotyczące komponentu zaznaczonego w lewym panelu.



Jeżeli opcja rozpoczyna się od znaku (+) to oznacza, że posiada podkategorię. Jeżeli opcja rozpoczyna się od znaku (-) oznacza, że wszystkie podkategorie zostały już wyświetlone. Aby ukryć wyświetlone podkategorie należy kliknąć na przycisk minus.

W panelach znajdują się następujace grupy obiektów:

- **Firewall**
  Wybierając ten obiekt w lewym panelu, zostają wyświetlone informacje ogólne o firewallu, tj. status, tryb pracy, wykryte ataki i ogólne informacje o połączeniach. Po rozwinięciu listy dostępne są:
  - Aktywność sieci - wyświetla wszystkie aplikacje i procesy posiadające aktywne połączenia oraz szczegóły dotyczące tych połączeń.
  - Otwarte porty - Wyświetla wszystkie aplikacje i procesy, które używają w danym momencie określonych portów. Aby uzyskać więcej szczegółów, przejrzyj rozdział Zarzadzanie połączeniami sieciowymi.
- **Ochrona Proaktywna**
  Wyświetla ogólne informacje o ochronie proaktywnej tj.: kontrola systemu, kontrolę Anti-Leak i status kontroli komponentów, status autoochrony oraz inne ogólne informacje.
  - Aktywność procesów - wyświetla wszystkie lokalne zdarzenia w systemie monitorowane przez Host Protection. Aby uzyskać więcej szczegółów, przejrzyj rozdział Ochrona przed zagrożeniami w pamięci.
- **Antyspyware**
  Wyświetla ogólne informacje o module Antyspyware, statusie bazy danych sygnatur spyware oraz ogólne informacje o wykrytych obiektach.
  - Kwarantanna - wyświetla wszystkie obiekty umieszczone w kwarantannie. Aby uzyskać więcej szczegółów, przejrzyj rozdział Ochrona przed zagrożeniami.
- **Kontrola stron WWW**
  Wyświetla ogólne informacje o komponentach kontroli stron WWW, tj.: aktualny status, poziom ochrony i inne ogólne informacje o filtrowanej zawartości.
  - Aktywność online - wyświetla całą zawartość elementów przetwarzanych przez filtr. Aby uzyskać więcej szczegółów, przejrzyj rozdział Kontrola aktywności sieci.
- **Dziennik zdarzeń**
  Wyświetla szczegółowe informacje la wszystkich minionych aktywności systemu oraz programu, podzielone na kategorie.

2.3. Ikona zasobnika systemowego

Domyślnie, program Outpost Firewall Pro uruchamia się automatycznie podczas startu systemu Windows. Po załadowaniu, zostaje wyświetlona ikona (domyślna ikona programu Outpost Firewall Pro), w zasobniku systemowym. Pojawienie się ikony oznacza, że, program został uruchomiony i chroni Twój system.
Ikona udostępnia opcje, ustawienia oraz zdarzenia programu. Gdy naciśniesz prawym klawiszem myszy ikonę programu, zostanie wyświetlone menu kontekstowe.

Dostępne są następujące opcje:

- **Pokaż/Ukryj -** wyświetla lub ukrywa główne okno programu.
- **Wyszukaj zagrożenia -** uruchamia skaner Antyspyware.
- **Ustawienia -** wyświetla okno **Ustawień**.
- **Zarejestruj –** (Obecne tylko w wersji próbnej.) Umożliwia wprowadzenie klucza aktywacyjnego w celu uzyskania darmowych aktualizacji i wsparcia programu Outpost Firewall Pro.
- **Tryb pracy firewalla -** otwiera podmenu, które umożliwia zmianę trybu pracy firewalla na jeden z następujących: **Blokuj wszystko**, **Blokuj większość**, **Kreator reguł**, **Zezwól na większość** i **Zezwól na wszystko**.
- **Zawieś ochronę (lub Wznów ochronę) -** wyłącza (włącza) ochronę programu Outpost Firewall Pro.
- **Włącz tryb samoczynnego uczenia (lub Wyłącz tryb samoczynnego uczenia) -** gdy program jest w trybie samoczynnego uczenia, zezwala na aktywność wszystkim aplikacjom przez zdefiniowany okres czasu w celu stworzenia odpowiednich reguł.
- **Wyłącz autoochronę (lub Włącz autoochronę) -** wyłącza (włącza) autoochronę programu Outpost Firewall Pro.
- **Wyjście -** zamyka program. System nie jest chroniony.

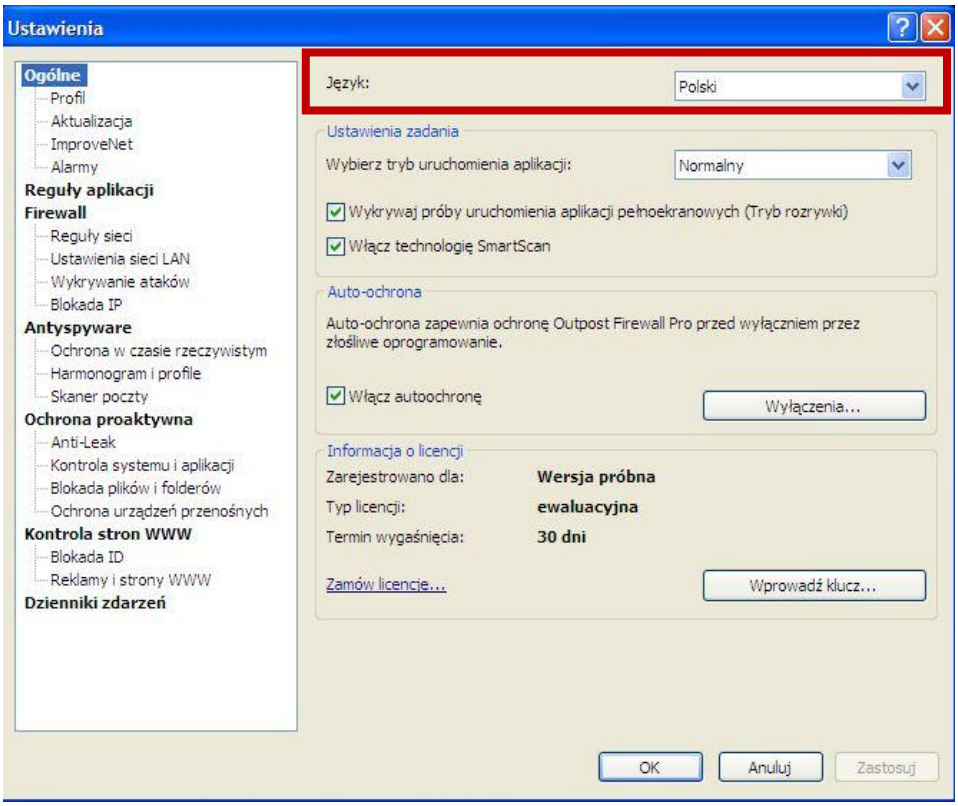
Uwaga:
Ikona zasobnika systemowego jest niewidoczna, gdy program jest uruchomiony w tle.

2.4. Język interfejsu

Język interfejsu jest wybierany podczas instalacji programu Outpost Firewall Pro, ale możesz go zmienić w dowolnym momencie pracy programu. Aby to zrobić:

1. Otwórz główne okno programu klikając dwa razy ikonę programu w zasobniku systemowym.
2. Naciśnij **Ustawienia** na pasku narzędzi.
3. Wybierz pożądany język programu **Outpost Firewall Pro** z listy.
4. Naciśnij **OK, aby** zachować zmiany:

Aby zmiany zostały zastosowane, należy ponownie uruchomić program. Pojawi się okno z komunikatem o wyłączaniu programu, który należy zaakceptować wciskając przycisk **OK**.



3. Podstawowa konfiguracja

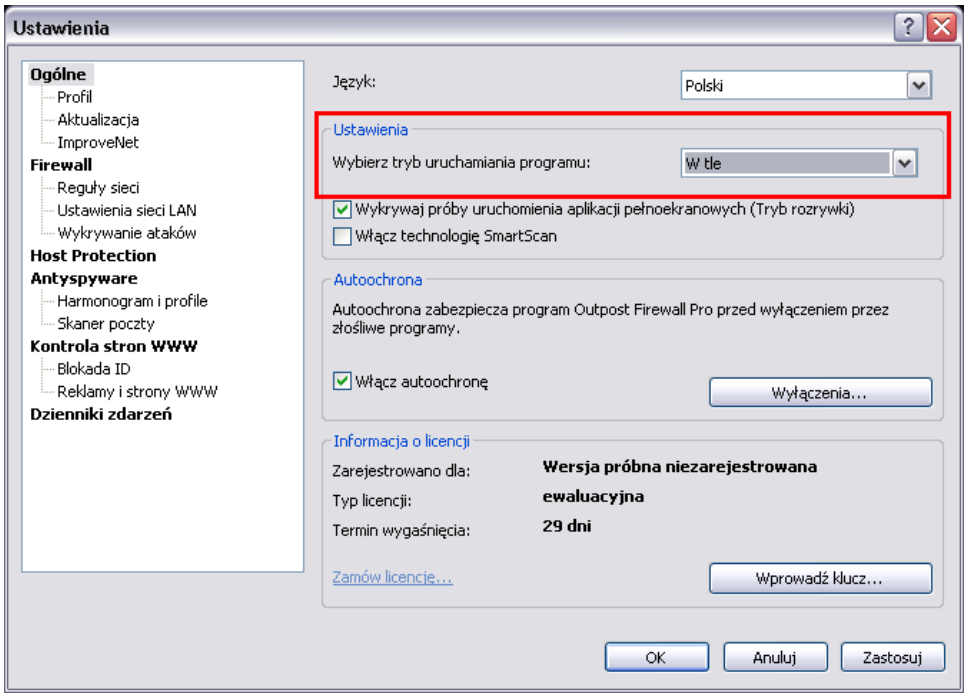
Program Outpost Firewall Pro zapewnia ochronę zaraz po instalacji. Ustawienia domyślne są zoptymalizowane dla ogólnego przeznaczenia i są zalecane do momentu dopóki nie zapoznasz się całkowicie z programem, w tym momencie możesz dostosować ustawienia do własnych potrzeb. Ten rozdział przedstawia krótki przegląd podstawowych czynności, z którymi początkujący użytkownik powinien się zapoznać, czyli: w jaki sposób stworzyć nowy profil, w jaki sposób zabezpieczać ustawienia oraz w jaki sposób Tryb rozrywki chroni Twój system gdy korzystasz z gier online.

3.1. Uruchamianie i zatrzymywanie pracy programu

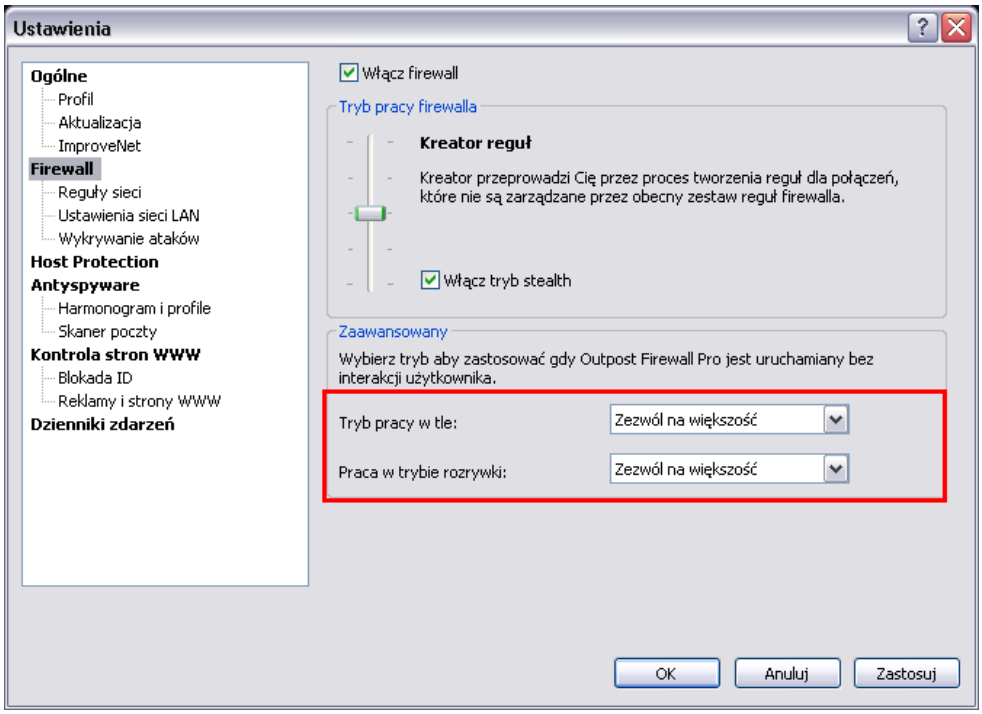
Domyślnie, program Outpost Firewall Pro uruchamia się automatycznie podczas startu systemu Windows. Po załadowaniu, zostaje wyświetlona ikona w zasobniku systemowym. Pojawienie się ikony oznacza, że program został uruchomiony i chroni Twój system. Podwójne kliknięcie myszy na ikonie programu Outpost Firewall Pro otwiera okno. Aby zamknąć główne okno programu, należy nacisnąć znak X w prawym górnym rogu programu. Program nie zostanie zamknięty; główne okno zostanie zminimalizowane do ikony w zasobniku systemowym.

Praca programu w tle

Gdy program pracuje w tle, ikona w zasobniku systemowym jest niewidoczna. Pozwala rodzicom oraz administratorom blokować niechciany ruch oraz zawartość stron WWW w sposób niewidoczny dla użytkownika. Jeśli chcesz, aby program Outpost Firewall Pro działał w tle, naciśnij **Ustawienia** na pasku narzędzi i zaznacz **Tryb pracy w tle**:

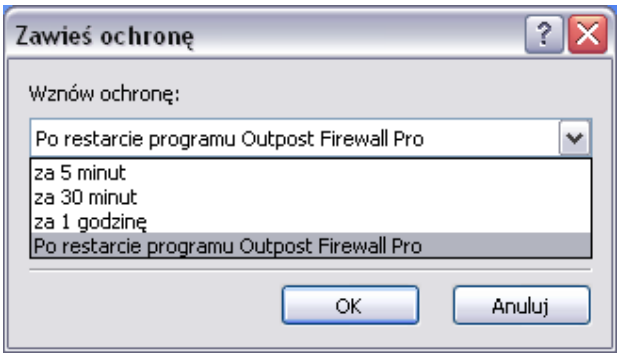


Tryb pracy w tle nie jest wspierany w Kreatorze reguł. Gdy program działa w tle (tryb w tle nie wymaga interakcji z użytkownikiem), musisz zdefiniować, który tryb pracy firewalla ma być zastosowany. Aby zdefiniować tryb pracy firewalla, który ma być zastosowany w trybie pracy w tle, naciśnij **Ustawienia** na pasku narzędzi, wybierz **Firewall**, a następnie zaznacz pożądany tryb pracy z listy **Tryb pracy w tle**:



Zawieszanie ochrony

Program Outpost Firewall Pro pozwala na tymczasowe zawieszanie ochrony na określony czas. Gdy zawiesisz ochronę, program nie będzie kontrolował aktywności; po przywróceniu ochrony, zastosuje konfigurację używaną przed zawieszeniem ochrony. Aby zawiesić ochronę, naciśnij prawym klawiszem myszy na ikonę w zasobniku systemowym i wybierz **Zawieś ochronę**. Program zapyta przez jaki okres czasu ochrona ma być zawieszona. Wybierz okres czasu i naciśnij **OK**:



Możesz wznowić ochronę w dowolnym momencie, naciskając prawym klawiszem myszy ikonę w zasobniku systemowym i wybierając **Wznów ochronę**.

Wyłączanie komponentów programu

Możesz także osobno wyłączyć komponenty programu zamiast zawieszać całą ochronę:

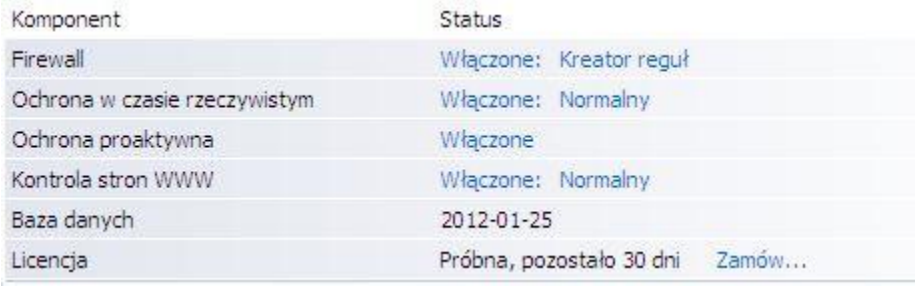
- Aby wyłączyć **firewall** naciśnij **Ustawienia** na pasku narzędzi, wybierz **Firewall** i odznacz pole **Włącz firewall**. Wyłączenie firewalla wyłącza także opcję wykrywania ataków. Szczegóły w rozdziale Zarządzanie połączeniami sieciowymi.
- Aby wyłączyć jedynie komponent **Wykrywanie ataków** naciśnij **Ustawienia** na pasku narzędzi, wybierz **Firewall** > **Wykrywanie ataków** i odznacz pole **Włącz wykrywanie ataków**. Szczegóły w rozdziale Ochrona przed atakami sieciowymi.
- Aby wyłączyć **Ochrona Proaktywna** naciśnij **Ustawienia** na pasku narzędzi, wybierz **Ochrona Proaktywna** i odznacz pole **Włącz Ochronę Proaktywną**.
- Aby wyłączyć **ochronę w czasie rzeczywistym** naciśnij **Ustawienia** na pasku narzędzi, wybierz **Antyspyware -> Ochrona w czasie rzeczywistym** i odznacz pole **Włącz ochronę w czasie rzeczywistym**. Szczegóły w rozdziale Ochrona w czasie rzeczywistym .
- Aby wyłączyć **Kontrolę stron WWW** naciśnij **Ustawienia** na pasku narzędzi, wybierz **Kontrola stron WWW** i odznacz pole **Włącz kontrolę stron WWW**. Szczegóły w rozdziale Kontrolowanie aktywności sieci.
- Aby wyłączyć **autoochronę** programu Outpost Firewall Pro naciśnij **Ustawienia** na pasku narzędzi i odznacz pole **Włącz autoochronę**. Szczegóły w rozdziale Ochrona wewnętrznych komponentów.

Uwaga:

Wyłączenie autoochrony może wpłynąć na zabezpieczenie systemu. Mimo że wyłączenie autoochrony jest wymagane przy instalacji modułów i innych zaawansowanych funkcji, powinno zostać włączone po zastosowanych zmianach.

3.2 Zarządzanie statusem ochrony

W głównym oknie programu zawarte są najważniejsze informacje na temat statusu ochrony zapewnianej przez program. Strona **Witamy** (pierwsza strona wyświetlana po kliknięciu ikony programu w zasobniku systemowym) przedstawia listę najważniejszych modułów oraz ich aktualnych trybów.
Pokaż okno statusu ochrony:



Komponent	Status	
Firewall	Włączone: Kreator reguł	
Ochrona w czasie rzeczywistym	Włączone: Normalny	
Ochrona proaktywna	Włączone	
Kontrola stron WWW	Włączone: Normalny	
Baza danych	2012-01-25	
Licencja	Próbna, pozostało 30 dni	Zamów...

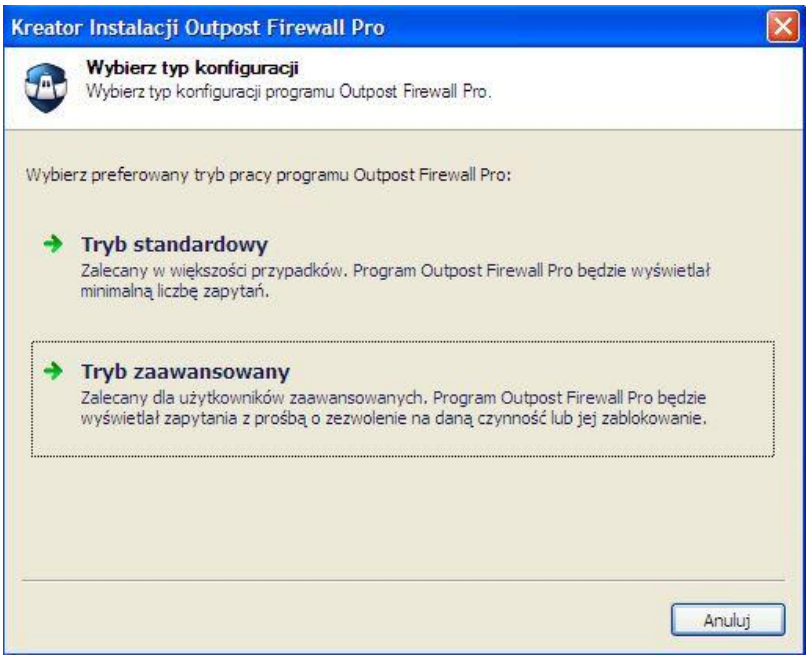
Wyświetlone są informacje o komponentach programu :

- **Firewall.** Naciśnięcie linku w kolumnie **Status** spowoduje przeniesienie do sekcji **Firewall**. Aby uzyskać więcej szczegółów, przejrzyj rozdział Zmiana trybu pracy programu.
- **Ochrona Proaktywna**. Naciśnięcie linku w kolumnie **Status** spowoduje przeniesienie do sekcji **Ochrona Proaktywna**. Aby uzyskać więcej szczegółów, przejrzyj rozdział **Ustawianie poziomu ochrony lokalnej**.
- **Ochrona w czasie rzeczywistym** Naciśnięcie linku w kolumnie **Status** spowoduje przeniesienie do sekcji **Antyspyware**. Aby uzyskać więcej szczegółów, przejrzyj rozdział **Ochrona w czasie rzeczywistym**.
- **Baza danych**. Naciśnięcie linku **Aktualizuj** który pojawi się w przypadku nieaktualnej bazy danych sygnatur, spowoduje uruchomienie procesu aktualizacji.
- Aby uzyskać więcej szczegółów, przejrzyj rozdział **Aktualizacja**.
- **Licencja**. Wyświetla typ licencji. Jeśli użytkownik nie jest zarejestrowany może w łatwy sposób tego dokonać, poprzez naciśnięcie linku
- **Zarejestruj**. Aby uzyskać więcej szczegółów, przejrzyj rozdział **Rejestracja programu**.

Jeśli dany moduł działa w trybie innym niż Normalny (zalecany), zostanie podświetlony kolorem żółtym, świadczącym o tym że moduł nie zapewnia wymaganego poziomu ochrony. Jeśli dany moduł jest wyłączony, zostanie podświetlony kolorem czerwonym, świadczącym o tym że moduł nie chroni Twojego systemu.

3.3. Tworzenie nowego profilu

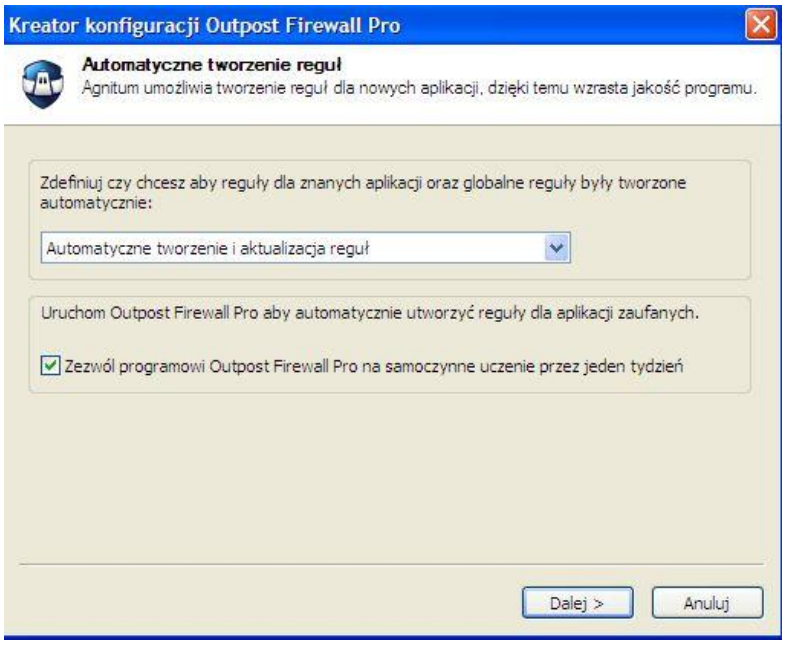
Na stan programu Outpost Firewall Pro wpływają następujące ustawienia: tryb pracy, poziom ochrony komponentów, reguły programów i globalne reguły, ustawienia sieci LAN, lista wyłączeń, itp. Całość stanowi konfigurację programu zwaną profilem. Pierwszy profil jest tworzony podczas instalacji programu, a następnie można zmieniać ustawienia lub tworzyć profile dla różnych działań. Pozwala to na tworzenie oddzielnych profili dla każdego użytkownika komputera, chroniąc dzieci przed dostępem do nieautoryzowanych stron WWW, uczestniczenia w grach online lub innych niedozwolonych czynności oraz na przenoszenie ustawień z jednego komputera na drugi oraz na tworzenie kopii zapasowej profilu.
Aby utworzyć nowy profil, naciśnij **Ustawienia** > **Profil** > **Nowy**. Profil programu jest przeprowadzany automatycznie przy pomocy **Kreatora instalacji:**



W pierwszym kroku należy wybrać poziom ochrony Dostępne są następujące poziomy (aby uzyskać więcej szczegółów, przejrzyj rozdział Ochrona przed zagrożeniami w pamięci):

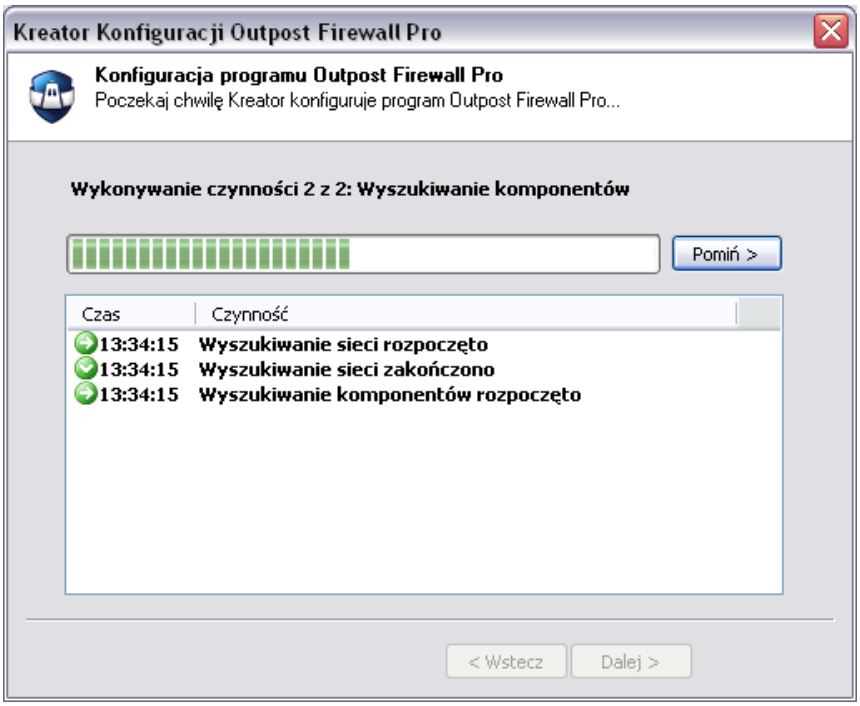
- **Tryb zaawansowany** - pozwala na największy poziom zabezpieczeń chroniąc przed technikami które są często wykorzystywane przez złośliwe programy, aby oszukać systemy bezpieczeństwa; zalecany dla użytkowników zaawansowanych.
- **Tryb standardowy -** chroni przed większością niebezpiecznych technik (na tym poziomie bezpieczeństwa niektóre testy bezpieczeństwa (leaktesty) zostaną zakończone niepowodzeniem).

Jeśli chcesz, aby program Outpost Firewall Pro zapobiegał wszelkim próbom dostępu do plików zainfekowanych przez znane zagrożenia, wybierz **Sprawdzaj pliki przy każdej próbie dostępu**. Ten tryb może zmniejszyć wydajność systemu.



Naciśnij **Dalej** aby przejść do kroku **Automatycznego tworzenia reguł**, który pozwala na włączenie automatycznego tworzenia reguł, tak więc reguły globalne i reguły znanych aplikacji są tworzone automatycznie gdy po raz pierwszy wysyłają żądanie (na przykład, dostęp do sieci lub modyfikacja pamięci procesu).
Opcja **Zezwól programowi Outpost Firewall Pro na samoczynne uczenie przez jeden tydzień** pozwala na automatyczne stworzenie niezbędnych reguł.

Naciskając **Dalej**, program Outpost Firewall Pro automatycznie przeskanuje system i dostosuje resztę ustawień bez nadzoru użytkownika. Pobierze najnowsze aktualizacje, skonfiguruje ustawienia sieci, utworzy bazę wiedzy kontroli komponentów.

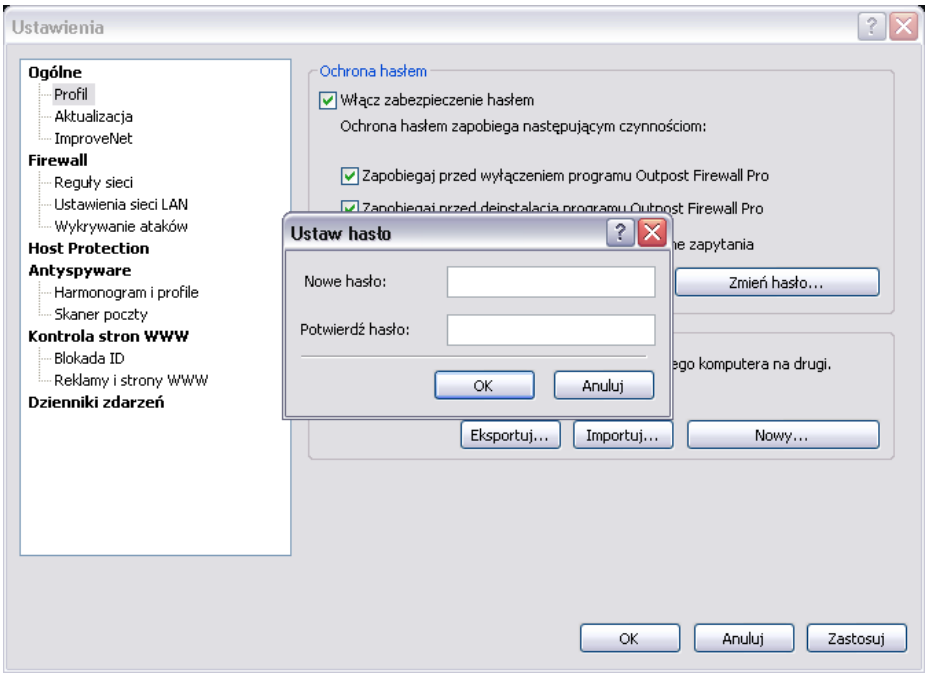


Naciśnij **Zakończ, aby** zatwierdzić zmiany i zapisać profil. Domyślnie utworzony profil jest nazwany jako **configuration.cfg** i zapisywany w folderze instalacyjnym programu Outpost Firewall Pro. Możesz tworzyć wiele profili zmieniając określone ustawienia, nadając nazwy każdemu z profili oraz zapisując profil we wskazanym miejscu na dysku, używając polecenia **Eksportuj**. Aby przełączyć profil, naciśnij **Importuj** i wyświetl plik profilu. Profil może być chroniony przed modyfikacją lub zamianą poprzez zdefiniowanie hasła. Aby uzyskać więcej szczegółów, przejrzyj rozdział Ochrona ustawień programu.

3.4. Zabezpieczenie ustawień hasłem

Program Outpost Firewall Pro pozwala chronić zdefiniowane ustawienia. Ustawienia zabezpieczone hasłem nie mogą zostać zmienione przez osoby trzecie. Możesz, na przykład, blokować dostęp niepożądanych stron WWW, wiedząc, że ustawienia te nie zostaną zmienione.

Ustawianie hasła
Aby ustawić hasło, naciśnij **Ustawienia** na pasku narzędzi, wybierz **Profil,** a następnie zaznacz pole **Włącz zabezpieczenie hasłem**:



Zdefiniuj hasło w polu dialogowym, wpisz je ponownie w polu Potwierdź hasło i naciśnij **OK** aby je zapisać. Naciśnij **OK** a program Outpost Firewall Pro będzie chronił Twoje ustawienia przed niepożądanymi zmianami.

Zmiana hasła
Aby zmienić hasło, naciśnij **Ustawienia** na pasku narzędzi, wybierz **Profil** a następnie naciśnij przycisk **Zmień hasło** w oknie **Ochrona hasłem**. Zdefiniuj i potwierdź nowe hasło a następnie naciśnij **OK.**

Wyłączanie hasła
Aby wyłączyć hasło, naciśnij **Ustawienia** na pasku narzędzi, wybierz **Profil** i odznacz pole **Włącz zabezpieczenie hasłem.** Gdy naciśniesz **OK,** wszystkie ustawienia firewalla będą dostępne dla każdego użytkownika.

Hasło może dodatkowo chronić program Outpost Firewall Pro przed wyłączeniem lub deinstalacją, zaznaczając odpowiednie pola. Zaznacz pole **Pytaj o hasło przed udzieleniem odpowiedzi**, jeśli chcesz aby program pytał o hasło gdy użytkownik ma udzielić odpowiedzi na zapytanie Kreatora reguł lub ochrony proaktywnej.

Uwaga:
Proszę zapamiętać hasło. Jeśli hasło zostanie zapomniane, użytkownik będzie musiał przeinstalować program Outpost Firewall Pro lub system operacyjny.

4. Aktualizacja Outpost Firewall Pro

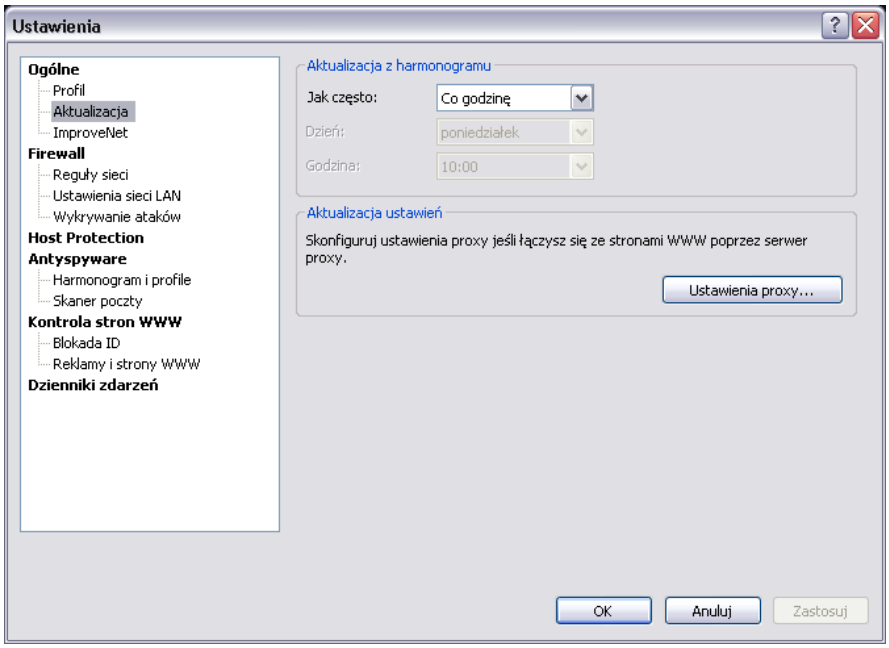
Aktualizacja programu jest kluczową czynnością, która powinna być przeprowadzana regularnie na komputerze, ponieważ tylko aktualne komponenty programu gwarantują utrzymanie maksymalnego poziomu bezpieczeństwa Twojego komputera.

Aktualizacja programu Outpost Firewall Pro, jest w 100% automatyczna, łącznie z pobieraniem aktualizacji komponentów, instalowaniem plików i modyfikacją rejestru. Domyślnie, program sprawdza co godzinę czy są dostępne nowe komponenty programu lub nowa baza sygnatur.

Jeśli ręcznie uruchomić aktualizację oprogramowania, naciśnij **Aktualizacja** na pasku narzędzi. Kreator aktualizacji programu Outpost Firewall Pro, zrealizuje wszystkie niezbędne zadania, pobierając najnowsze dostępne komponenty, ustawienia oraz bazy sygnatur wirusów. Po zakończeniu aktualizacji, naciśnij **Zakończ**. Proces aktualizacji można również uruchomić naciskając **Start** > **Wszystkie programy**> **Agnitum** > **Outpost Firewall Pro** > **Aktualizacja**.
Firma Agnitum pozwala konfigurować ustawienia aktualizacji z harmonogramu oraz pobierać aktualizacje reguł dzięki uczestnictwu w darmowym programie Agnitum ImproveNet.

4.1. Ustawienia aktualizacji

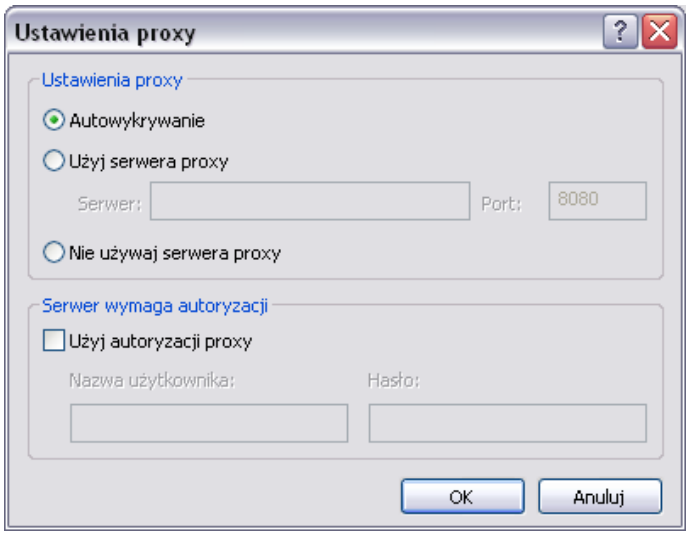
Aby skonfigurować aktualizacje programu, naciśnij **Ustawienia** na pasku narzędzi i wybierz **Aktualizacja**:



Harmonogram
Domyślnie, Outpost Security Suite aktualizuje się codziennie, jednakże możesz sam wybrać porę kiedy program Outpost Firewall Pro ma pobierać aktualizacje. Aby to zrobić, naciśnij przycisk **Ustawienia** na pasku narzędzi i wybierz **Aktualizacja**.
W oknie **Aktualizacja z harmonogramu** możesz zdefiniować, jak często mają być wykonywane aktualizacje, wybierając pożądany czas z listy **Jak często:**. Jeśli wybierzesz aktualizacje co tydzień, możesz także zdefiniować dzień i czas kiedy program ma pobierać aktualizacje. W ramach dziennych aktualizacji, możesz zdefiniować godzinę, o której aktualizacje mają być pobierane. Jeśli wybierzesz opcję **Ręcznie**, aktualizacje nie będą wykonywane aż do momentu, kiedy naciśniesz przycisk **Aktualizacja** na pasku narzędzi.

Ustawienia proxy
Jeśli użytkownik łączy się z Internetem poprzez serwer proxy, może zdefiniować połączenie w zakładce **Ustawienia Proxy** w oknie on **Aktualizacja,** w ustawieniach programu**.** Opcja autowykrywania jest

domyślna, ale możesz zdefiniować serwer i numer portu. Aby to zrobić, należy wybrać opcję **Użyj serwera proxy** w oknie **Ustawienia proxy** i wpisać nazwę serwera i numer portu**.**

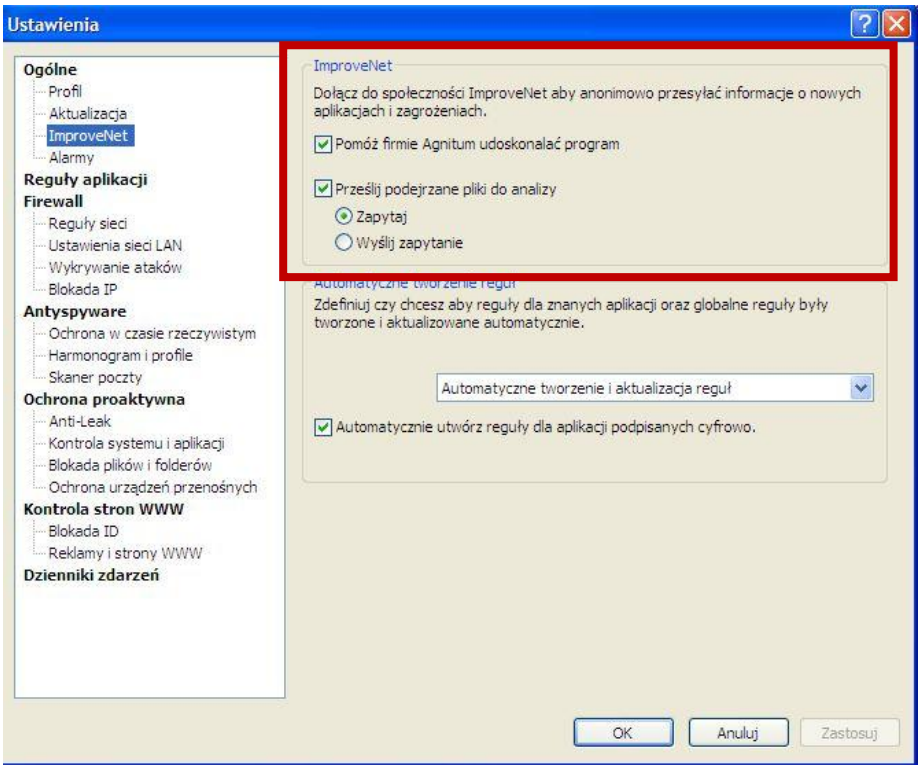


Podczas ustawiania serwera proxy, można zdefiniować czy ma wymagać autoryzację, zaznaczając pole **Użyj autoryzacji proxy** w oknie **Serwer wymaga autoryzacji** określić dostęp do dokumentów uwierzytelniających (nazwa użytkownika i hasło).
Jeśli przy połączeniu z Internetem komputer używa serwera proxy, chcesz pobierać aktualizacje bezpośrednio z serwera, należy zaznaczyć pole **Nie używaj serwera proxy**. Jeśli nie używasz serwera proxy, zaznacz pole **Nie używaj serwera proxy** lub **Autowykrywanie.**

4.2. Agnitum ImproveNet

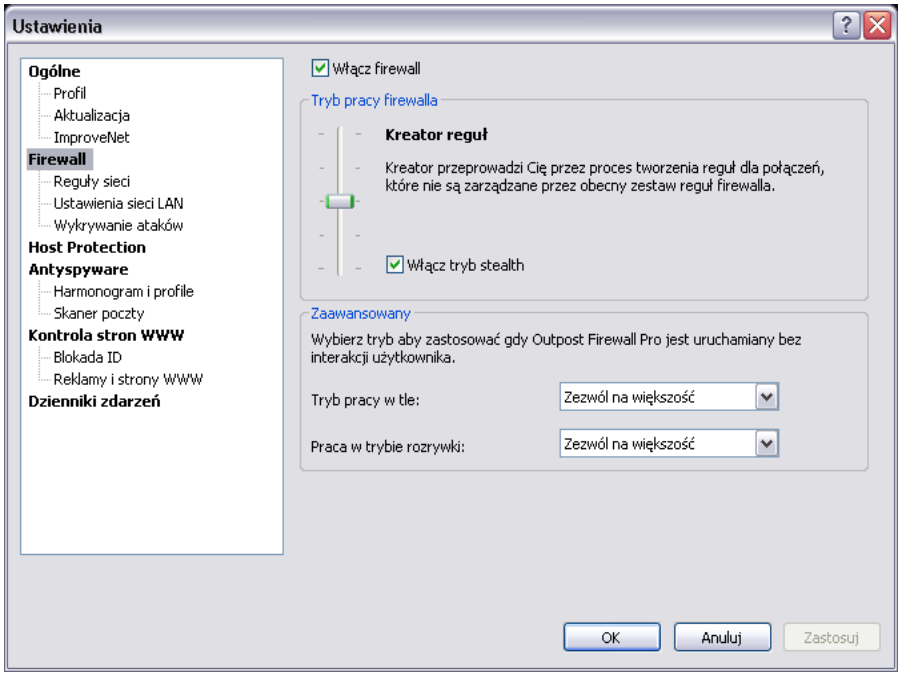
Zapraszamy do udziału w programie Agnitum ImproveNet , którego zadaniem jest poprawienie jakości oraz zwiększenie oferowanego poziomu bezpieczeństwa produktów firmy Agnitum. Za Twoją zgodą, program Outpost Firewall Pro będzie zbierał informacje tylko o aplikacjach zainstalowanych na komputerze. Dane są zbierane całkowicie anonimowo, co oznacza że nie zawierają nazwiska, adresu, informacji o sieci, czy innych prywatnych danych. Program zbiera dane o aplikacjach z dostępem do sieci, dla których nie istnieją zdefiniowane reguły. Informacje są kompresowane i wysyłane raz w tygodniu do firmy Agnitum w sposób niezauważalny dla użytkownika. Po stworzeniu nowej reguły i jej zatwierdzeniu przez firmę Agnitum, jest ona automatycznie udostępniana pozostałym użytkownikom poprzez aktualizację programu.

Aby przyczynić się do poprawy programu i dołączyć do społeczności ImproveNet firmy Agnitum. Naciśnij **Ustawienia** > **ImproveNet** a następnie zaznacz pole **Pomóż firmie Agnitum udoskonalać program**. Możesz wyłączyć tą opcję w każdym czasie, odznaczając pole.:



5. Zarządzanie połączeniami sieciowymi

Ponieważ liczba użytkowników Internetu ciągle wzrasta, wzrastają także potrzeby związane z ochroną prywatnych danych. Program Outpost Security Suite zapewnia szeroki wybór poziomów ochrony od całkowitego zablokowania wszystkich połączeń z Internetem, do zezwolenia na pełny dostęp każdej aplikacji.



5.1. Zmiana trybu pracy programu

Jedną z ważnych cech programu jest tryb pracy, który określa sposób postępowania programu Outpost Firewall Pro w momencie kiedy dana aplikacja próbuje nawiązać połączenie. Tryb **Blokuj większość** ustawia program w trybie bardzo restrykcyjnym i nie pozwala na nawiązywanie jakichkolwiek niezdefiniowanych połączeń, natomiast tryb **Zezwól na większość** pozwala na swobodne nawiązywanie połączeń za wyjątkiem tych, które zostały zabronione przez użytkownika.

Tryby pracy programu

- **Blokuj wszystko** - wszystkie połączenia sieciowe są blokowane, a komputer jest odcięty od sieci.
- **Blokuj większość** - wszystkie połączenia są blokowane, oprócz tych określonych jako dozwolone w regułach globalnych lub regułach aplikacji.
- **Kreator reguł** - dzięki niemu program pyta użytkownika o zezwolenie lub zablokowanie każdego nowego połączenia. Pozwala sprawdzić jakie połączenia sieciowe próbują być nawiązane.
- **Zezwól na większość** - wszystkie połączenia są akceptowane, za wyjątkiem określonych wcześniej jako zabronione w regułach globalnych lub regułach aplikacji.

Ikona znajdująca się w zasobniku systemowym odzwierciedla tryb pracy programu Outpost Firewall Pro. Wystarczy spojrzeć na ikonę programu, aby zorientować się w jakim trybie pracuje program. Jeśli Outpost Firewall Pro pracuje w trybie Zezwól na wszystko, w zasobniku systemowym pojawi się ikona w kolorze czerwonym – żadne połączenie z sieci nie będzie blokowane.

Uwaga:
Jeśli program Outpost Firewall pracuje w tle ikona nie będzie wyświetlana w zasobniku systemowym.

Zmiana trybu pracy
Aby zmienić tryb pracy należy:
1. Nacisnąć **Ustawienia** na pasku narzędzi.
2. Wybrać **Firewall**.
3. Przesunąć suwak w dół lub w górę, aby wybrać żądany tryb pracy i nacisnąć **OK:**

Aby wyłączyć firewalla, należy odznaczyć pole **Włącz firewall**.

Wskazówka:
Istnieje również możliwość zmiany trybu pracy programu za pomocą ikony w zasobniku systemowym. Naciśnij prawym klawiszem myszy na ikonę programu, wybierz **Tryb pracy firewalla,** a następnie wybierz wybrany tryb pracy.

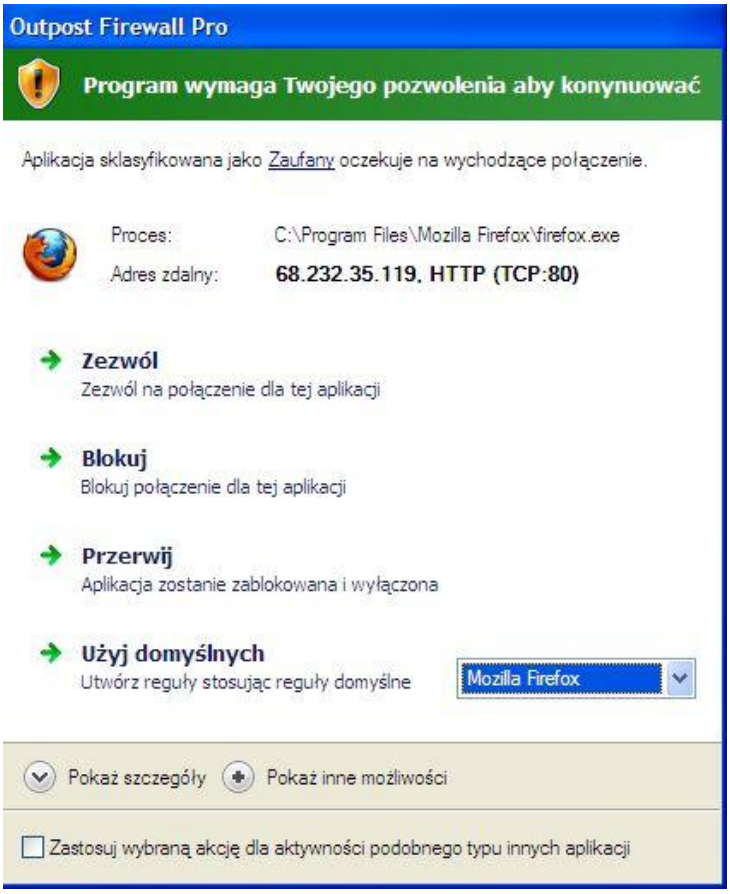
Uwaga:
Jeśli firewall jest wyłączony, opcja Wykrywanie ataków jest także wyłączone.

Niezależnie od wybranego trybu pracy, program Outpost Firewall Pro zawsze pracuje w ukryciu (w trybie stealth), co oznacza że Twój komputer jest niewidoczny dla innych użytkowników Internetu.

5.1.1. Praca w trybie kreatora reguł

Po instalacji, program Outpost Firewall Pro działa w trybie **Kreatora reguł**. Przy każdej próbie nawiązania połączenia przez jakikolwiek zainstalowany na komputerze program, użytkownik zostanie zapytany czy zezwolić na połączenie, czy też je zablokować. Program pozwala definiować parametry sieci dla każdego typu aplikacji. Zamiast tworzenia nowej (i często złożonej) reguły za każdym razem gdy nowa aplikacja

zostaje uruchomiona, program zezwala na wybieranie ustawień bazujących na podobnych znanych aplikacjach.



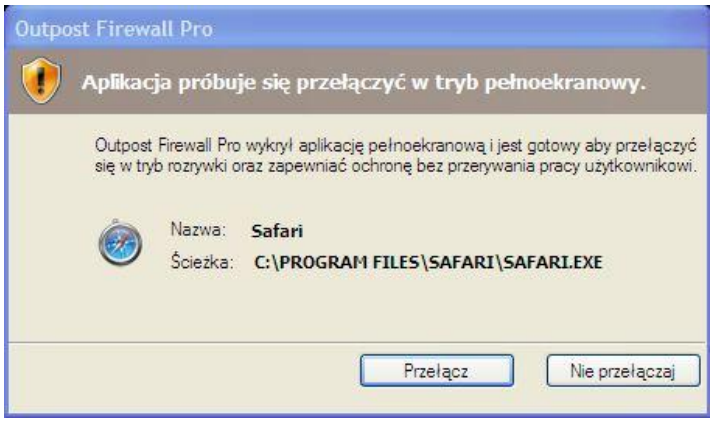
Poniżej znajdują się wszystkie opcje jakie może zaproponować **Kreator reguł** przy próbie nawiązania połączenia przez daną aplikację:

- **Zezwól -** dla całkowicie zaufanych programów. Wszystkie żądania sieciowe programu będą zezwolone i program będzie w grupie **Zaufanych**.
- **Blokuj -** dla programów, które nie powinny żądać połączenia sieciowego. Wszystkie żądania sieciowe programu będą zabronione i program będzie w grupie **Zablokowanych.**
- **Przerwij -** dla programów, które nie mogą połączyć się z siecią – dostęp do sieci blokowany na stałe.
- **Użyj domyślnych** – dla programów zostaną zastosowane reguły, zdefiniowane przez producenta.

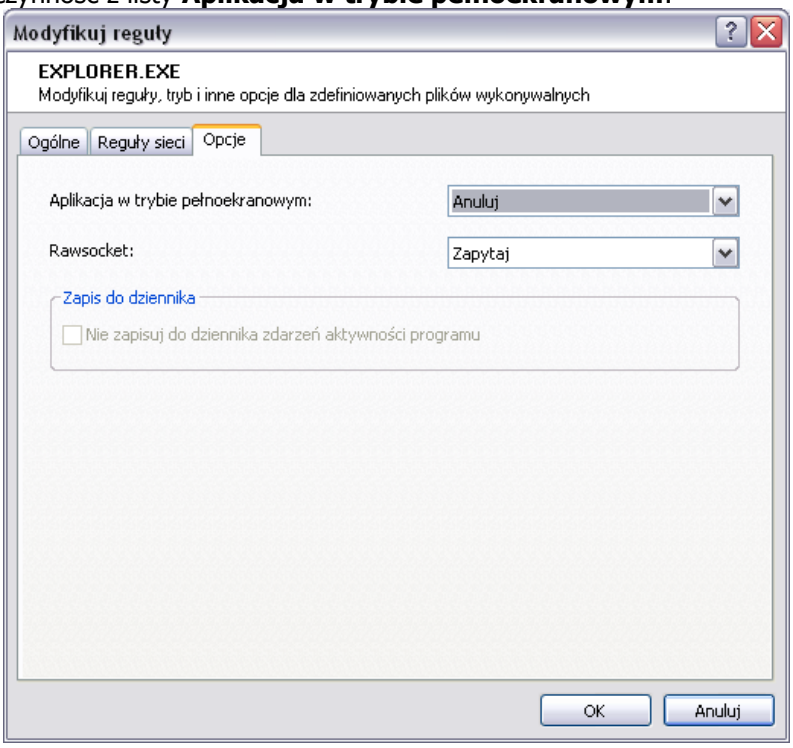
5.1.2. Praca w trybie rozrywki

Programy w czasie pracy często wyświetlają powiadomienia, ostrzeżenia itp. Może to być irytujące szczególnie w czasie gry lub oglądania filmu on - line. Program Outpost Firewall Pro umożliwia pracę w **trybie rozrywki.** Podczas pracy w trybie rozrywki, program Outpost Firewall Pro nadal zabezpiecza komputer użytkownika przed zagrożeniami z Internetu, nie wyświetlając przeszkadzających komunikatów, sugerując przełączenie się w tryb rozrywki za każdym razem kiedy użytkownik uruchamia inny program (np. grę lub program do odtwarzania filmów) w trybie pełnego ekranu.
Aby program Outpost Firewall Pro wykrywał aplikacje pełnoekranowe, naciśnij **Ustawienia** na pasku narzędzi i zaznacz pole **Wykrywaj próby uruchomienia aplikacji pełnoekranowych (Tryb**

rozrywki). Aby ustawić tryb pracy dla trybu rozrywki, naciśnij zakładkę **Firewall** i wybierz tryb z listy. Tryb firewalla będzie zastosowany za każdym razem, gdy program Outpost Firewall Pro zostanie przełączony w tryb rozrywki a następnie powróci do poprzedniego trybu, gdy tryb rozrywki nie będzie już używany.



Możesz także włączyć lub wyłączyć tryb rozrywki dla określonej aplikacji naciskając **Ustawienia** na pasku narzędzi, wybierając zakładkę **Reguły sieci** i podwójnie klikając na żądaną aplikację. W zakładce **Opcje**, wybierz niezbędną czynność z listy **Aplikacja w trybie pełnoekranowym**:



Uwaga:
Jeżeli aplikacja nie ma zdefiniowanych reguł dostępu do sieci, w momencie przechodzenia do trybu rozrywki, dodawana jest do grupy **Zaufanych**.

5.1.3. Doradca

Podczas pracy program Outpost Firewall Pro może wymagać interakcji z użytkownikiem wyświetlając okna z zapytaniami. Takie zapytanie może się pojawić gdy, na przykład, zachowanie programu jest inne niż w

regułach. Aby pomóc użytkownikowi w podjęciu decyzji, program Outpost Firewall Pro przedstawia dodatkowe informacje oraz sugestie, które są dostępne, gdy użytkownik naciśnie na link **Doradca**. Okno Doradcy:

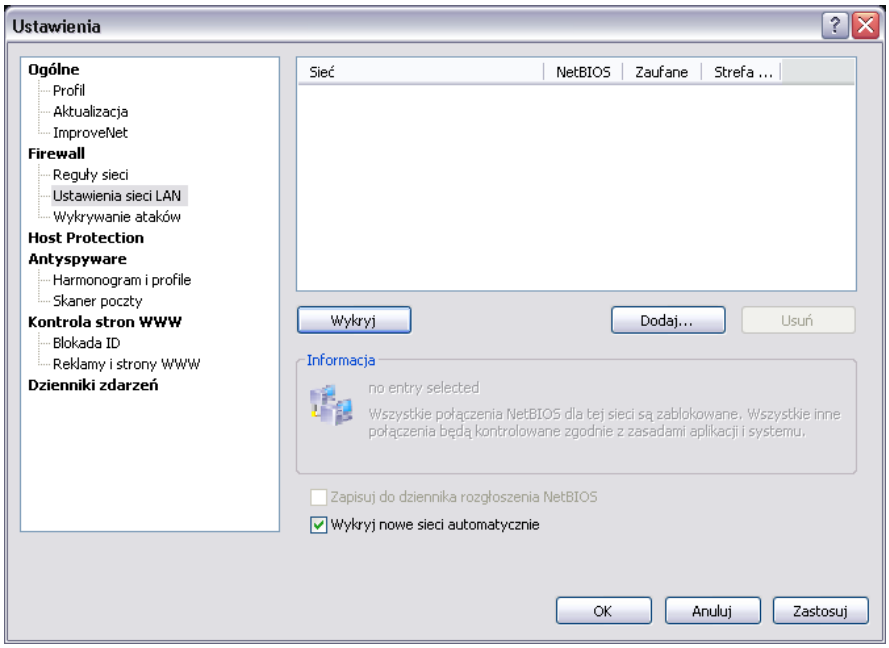
Po naciśnięciu na link **Doradca**, pojawi się okno zawierające szczegóły aktywności programu Outpost Firewall Pro, tj. właściwości programu wykonywalnego, który żąda połączenia oraz opis programów, dla których taka aktywność jest typowa.

5.2. Konfiguracja ustawień sieciowych

Fundamentalną różnicą pomiędzy siecią lokalną i Internetem jest poziom zaufania, który można przydzielić do każdego elementu. Sieć lokalna jest używana w domu lub biurze i złożona z "zaufanych" komputerów, należących do członków rodziny lub pracowników. Program pozwala na wykrywanie ustawień sieci LAN, do której należy komputer i ustawienie poziomu dostępu do każdej sieci.

5.2.1. Wykrywanie ustawień sieciowych

Podczas instalacji programu Outpost Firewall Pro program wykrywa i konfiguruje ustawienia sieci lokalnej. Jeżeli jednak zostało pominięte automatyczne wykrywanie ustawień sieciowych, wtedy należy ręcznie wykryć ustawienia, aby móc korzystać z dostępu do sieci LAN. Aby przeglądać listę sieci, do których należy komputer naciśnij **Ustawienia** na pasku narzędzi i wybierz **Ustawienia sieci LAN**:

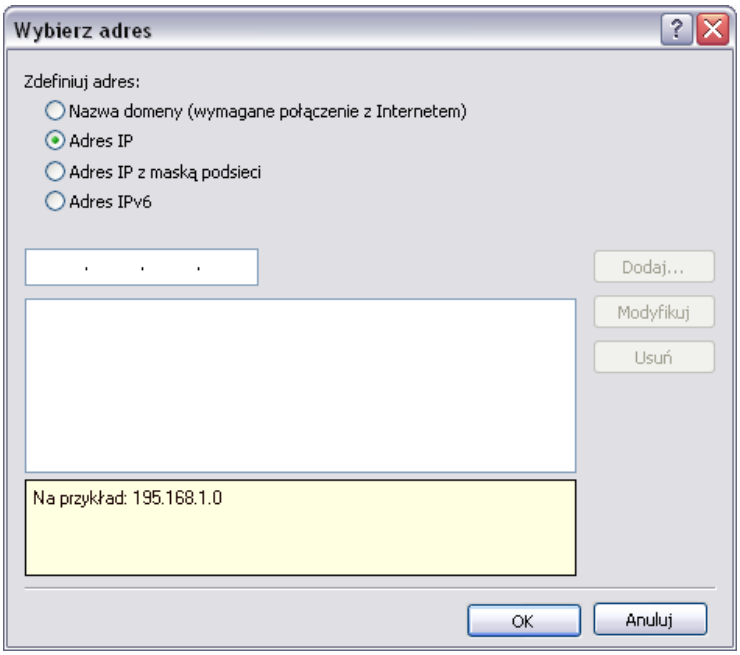


Automatyczne wykrywanie sieci LAN

W zakładce **Ustawienia sieci LAN** naciśnij **Wykryj** a program Outpost Firewall Pro automatycznie wykryje sieci do których należy Twój komputer oraz stworzy listę adresów IP, definiując domyślny poziom dostępu do każdej z wykrytych sieci. W dowolnym momencie możesz dostosować poziom dostępu dla określonych sieci. Zaznacz pole **Wykryj nowe sieci automatycznie** i naciśnij **OK** aby zapisać zmiany.

Ręczne dodawanie adresu sieciowego

Aby dodać ręcznie adres sieciowy do ustawień sieci LAN, ponieważ nie został on automatycznie wykryty i skonfigurowany przez program Outpost Firewall Pro, należy przejść do zakładki **Ustawienia sieci LAN**, nacisnąć **Dodaj,** następnie w oknie **Wybierz adres** zdefiniować połączenie sieciowe. Dostępne są następujące opcje:



- **Nazwa domeny**. Na przykład, www.outpost.pl. Wymagane jest aktywne połączenie internetowe, ponieważ nazwa domeny zostanie przekształcona na adres IP pobrany z Internetu.
- **Adres IP** . Na przykład, 216.12.219.12.
- **Adres IP z maską**. Na przykład, 216.12.219.1 - 216.12.219.255.
- **Adres IPv6**. Na przykład, 2002::a00:1.

Następnie należy wprowadzić wybrany adres komputera we wcześniej wybranym formacie (można używać wyrażeń regularnych) i nacisnąć przycisk **Dodaj**. Po dodaniu wszystkich wymaganych adresów należy nacisnąć przycisk **OK**, aby dodać je do listy **Ustawień sieci LAN.**

Usuwanie adresu sieciowego
Aby usunąć z listy ustawień sieci LAN wybrany adres IP lub całą sieć należy w ustawieniach sieci LAN zaznaczyć wybrany adres IP lub sieć i nacisnąć przycisk **Usuń**. Usunięcie z listy adresu IP jest równoznaczne z ograniczeniem poziomu zaufania dla tego adresu (odznaczenie pól **NetBIOS** i **Zaufane**). Aby uzyskać więcej szczegółów dotyczących konfigurowania poziomu dostępu do sieci LAN, przejrzyj rozdział, Poziom dostępu do sieci LAN.

5.2.2. Poziom dostępu do sieci LAN

Wszystkie komputery w sieci LAN mogą być przypisane do jednego z poniższych poziomów dostępu:

- **NetBIOS** - będą zezwolone tylko udostępnione pliki i drukarki. Aby ustawić ten poziom należy zaznaczyć pole **NetBIOS**.
- **Zaufane** - będą zezwolone wszystkie połączenia z i do sieci lokalnej. Aby ustawić ten poziom należy zaznaczyć pole **Zaufane**.
- **Strefa NAT -** będzie zezwolone udostępnianie połączenia internetowego z Twojego komputera.

Należy pamiętać, że adres IP z poziomem **Zaufane** posiada najwyższy priorytet. Wszystkie zablokowane programy mogą komunikować się z komputerem o tym adresie IP. Zalecane jest nadawanie poziomu **Zaufane** tylko najbardziej zaufanym komputerom.

Aby dzienniki zdarzeń były bardziej przejrzyste akietach można wyłączyć zapisywanie informacji o pakietach rozgłoszeniowych dla każdego wykrytego komputera lub podsieci. W tym celu należy w ustawieniach sieci LAN wyłączyć zaznaczenie pola **Zapisuj do dziennika rozgłoszenia NetBIOS**. Dzienniki zdarzeń będą bardziej przejrzyste.
Pakiety rozgłoszeniowe NetBIOS są przychodzacymi i wychodzacymi pakietami UDP z adresem nadawcy należącego do wybranej podsieci i wysyłanymi na adres 255.255.255.255 na portach 137 lub 138. Takie pakiety są używane na przykład przez stacje robocze do ogłoszenia swojej obecności w sieci.

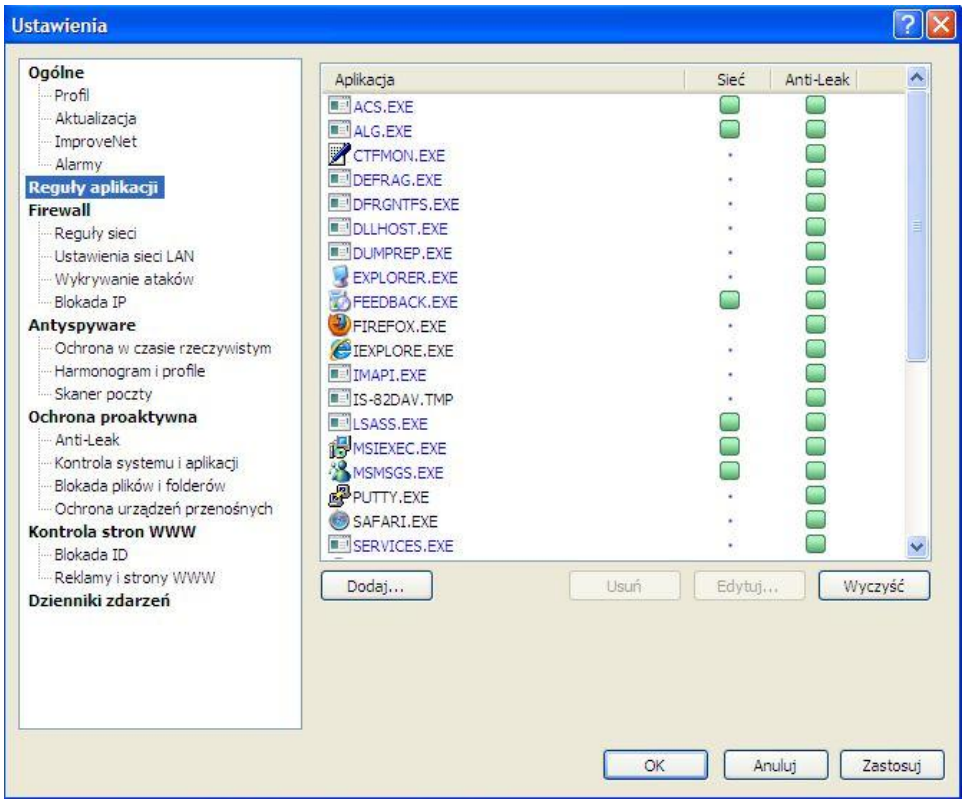
Uwaga:
Moduły programu Outpost Firewall Pro pracują niezależnie od poziomu dostępu do sieci LAN. Na przykład, po nadaniu adresowi www.outpost.pl poziomu **Zaufane,** moduły nadal będą blokować banery, aktywną zawartość, itd. z tej strony oraz wykonywać inne czynności bez względu na poziom dostępu do sieci.

5.3. Zarządzanie dostępem programów do sieci

Jedną z głównych opcji programu jest przyznawanie dostępu do sieci procesom i programom zgodnie ze zdefiniowanymi regułami. Pozwala to na elastyczne ustawienie dostępu do sieci i zapewnia, że żaden niepożądany proces nie uzyskał dostępu do sieci. Program Outpost Firewall Pro automatycznie tworzy listę zainstalowanych programów i ustawia zestaw reguł dając jednocześnie możliwość ręcznej zmiany listy programów i reguł dla programów. Aby uzyskać więcej szczegółów, przejrzyj odpowiednie rozdziały.

5.3.1. Zarządzanie listą programów

Podczas konfiguracji programu, wykrywane są wszystkie zainstalowane programy i tworzone są reguły zgodnie z wbudowanymi szablonami. Aby przeglądać listę wykrytych programów należy nacisnąć przycisk **Ustawienia** na pasku narzędzi i wybrać **Reguły aplikacji.**



Dla każdej aplikacji, przydzielone są dwie grupy ikon które wskazują tryb reguł stosowany do aplikacji poprzez firewall oraz komponenty ochrony Anti-Leak. Zielona ikona wskazuje że tylko reguły zezwalające są stosowane dla aplikacji; czerwona ikona wskazuje reguły blokujące które są stosowane dla aplikacji; żółta ikona oznacza że aplikacja jest traktowana zgodnie z regułami dla ruchu przychodzącego i wychodzącego; Brak ikony oznacza brak stosowania reguł dla aplikacji przez obydwa komponenty.
Możesz zmienić status aplikacji lub procesu przenosząc do innej grupy lub klikając prawym przyciskiem myszy i wybierając **Zawsze ufaj tej aplikacji/Zawsze blokuj tą aplikację**. Można również zmienić status programu zaznaczając program, a następnie przytrzymując lewy klawisz myszy, przeciągnąć do wybranej grupy programów.
Aby dodać program do listy, naciśnij przycisk **Dodaj**. Będziesz poproszony o dodanie pliku wykonywalnego. Po dodaniu pliku, wyświetli się okno **Edytuj.** Dzięki temu, będziesz mógł zdefiniować reguły dla nowego programu. Po zdefiniowaniu reguł i zatwierdzeniu ich przyciskiem **OK**, program pojawi się w wybranej grupie. Aby uzyskać więcej szczegółów dotyczących tworzenia i edytowania reguł programów, przejrzyj rozdział Zarządzanie regułami aplikacji. Aby usunąć zaznacz go i naciśnij przycisk **Usuń**.

Ustawianie dodatkowych opcji
Opcja **Modyfikuj reguły** pozwala wyświetlać szczegóły plików wykonywalnych aplikacji (zakładka **Ogólne**) i ustawiać dodatkowe opcje. Wybierz zakładkę **Opcje**, aby zdefiniować zachowanie programu Outpost Firewall Pro, gdy aplikacja zostaje przełączona w tryb pełnoekranowy. Jeśli chcesz, aby program zawsze lub nigdy nie przechodził w tryb rozrywki bez wyświetlania zapytania, wybierz pożądaną czynność z listy **Aplikacja w trybie pełnoekranowym.**

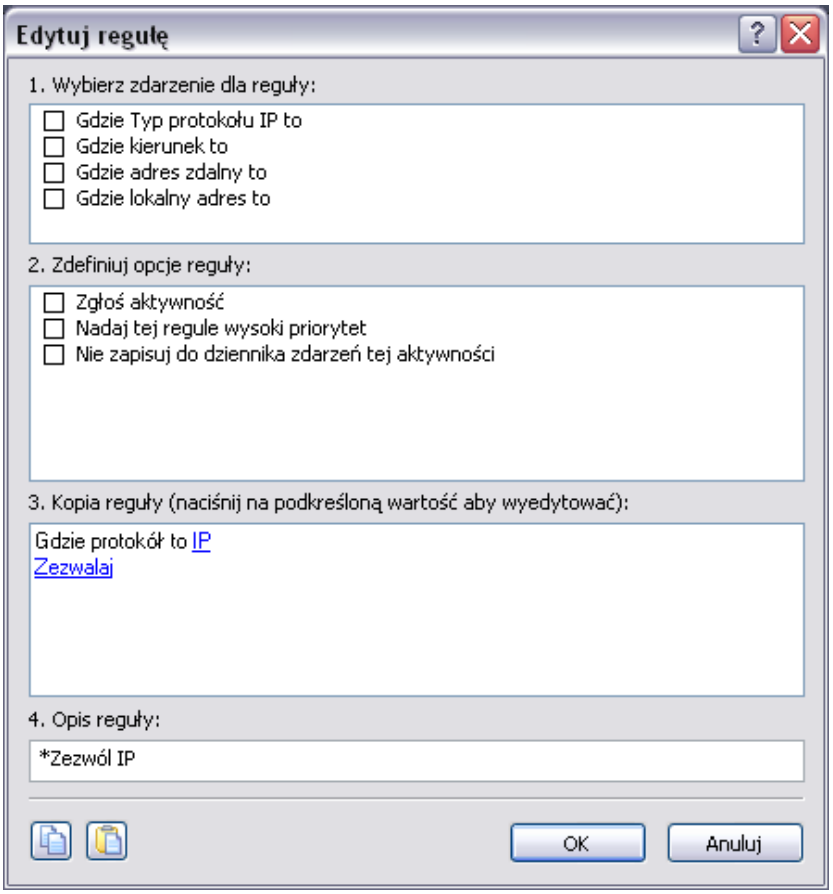
Niektóre aplikacje uzyskują dostęp do sieci bezpośrednio przez zapytania niskiego poziomu, znane również jako rawsockets. Zapytania nie mogą być zarządzane przez standardowe reguły protokołów lub aplikacji. Mogą funkcjonować jako backdoory dla szkodliwych aplikacji lub dawać możliwość dostępu do sieci bez ograniczeń. Aby zapewnić ochronę systemu, program Outpost Firewall Pro zezwala na kontrolę dostępu rawsocket. Możesz definiować, które aplikacje mogą tworzyć zapytania rawsocket, a które nie, wybierając odpowiednią opcję z listy **Rawsocket:**. Jeśli chcesz, aby program Outpost Firewall Pro pytał przy każdej próbie dostępu aplikacji do rawsockets, wybierz **Zapytaj**.

Uwaga:
Jeśli program pracuje w trybie **Kreatora reguł**, nie jest wymagane ręczne dodawanie aplikacji do listy. Program Outpost Firewall Pro zasugeruje reguły dla każdej aplikacji, przy pierwszej próbie dostępu aplikacji do sieci.

5.3.2. Zarządzanie regułami aplikacji

Aby wyświetlić aktualne reguły dla programu, naciśnij **Ustawienia > Firewall** na pasku narzędzi i wybierz **Reguły sieci**. Kliknij dwukrotnie lewym klawiszem myszy i wybierz zakładkę **Reguły sieci**.

Dodawanie nowej reguły
Aby stworzyć nową regułę, naciśnij **Nowa.** W oknie Edytuj regułę, zdefiniuj następujące parametry dla reguły:



Wybierz zdarzenie dla reguły Dostępne są następujące kryteria:

- **Gdzie kierunek to –** definiuje kierunek ruchu przychodzącego lub wychodzącego.
- **Gdzie adres zdalny to –** definuje wybrany adres IP lub nazwę DNS.
- **Gdzie port zdalny to** – definuje wybrany port używany przez zdalny komputer.
- **Gdzie lokalny port to** – definiuje wybrany port używany przez ten komputer.
- **Gdzie port lokalny jest równy portowi zdalnemu** – obydwa komputery używają tego samego numeru portu.

Zaznacz kryteria dla zdarzeń i zdefiniuj ustawienia w polu **Opis reguły.** Należy zdefiniować wszystkie podświetlone opcje. Aby uzyskać więcej szczegółów dotyczących używania makro adresów, przejrzyj rozdział Korzystanie z makro adresów.

Zdefiniuj opcje reguły. Dostępne są następujące czynności:

- **Zgłoś aktywność** – wyświetla ostrzeżenie o zastosowaniu reguły.
- **Uruchom badanie stanu połączenia** – uruchamia "badanie stanu połączenia" dla wybranego programu (przy połączeniu programu ze zdalnym serwerem, wszystkie dane przychodzące z serwera na otwarty port są filtrowane w zależności od zdefiniowanych ustawień).
- **Nie zapisuj do dziennika zdarzeń tej aktywności –** wyłącza zapisywanie do dziennika działań wykonywanych przez tą regułę. Po zaznaczeniu opcji, dane dotyczące reguły nie zostaną zapisane w dzienniku zdarzeń.

Opis reguły
Gdy wybierzesz jedną z powyższych czynności, w oknie **Opis reguły** zostaną wyświetlone wybrane czynności. Należy zaznaczyć odpowiednie opcje i zdefiniować program lub komendę poprzez naciśnięcie podświetlonego linku (**Zezwalaj** jest domyślne). Należy upewnić się, że wszystkie parametry w polu **Opis reguły** zostały zdefiniowane. Program Outpost Firewall Pro automatycznie utworzy **Nazwę reguły** zgodnie ze zdefiniowanymi parametrami. Naciśnij **OK,** aby zachować regułę. Utworzona reguła zostanie dodana do listy reguł.

Modyfikowanie istniejącej reguły
Aby zmodyfikować istniejącą regułę, należy zaznaczyć ją a następnie nacisnąć przycisk **Modyfikuj**. Należy wprowadzić zmiany w oknie Edytuj regułę a następnie nacisnąć **OK,** aby zachować zmiany. Wybrane reguły są aktywne (włączone) i stosowane przez firewall. Odznacz pole obok nazwy reguły, aby program Outpost Firewall Pro nie stosował się do wybranej reguły Możesz włączyć regułę w dowolnym momencie zaznaczając pole. Kolejność reguł wyświetlanych nie jest przypadkowa. Ich rozmieszczenie w oknie odpowiada priorytetowi reguły. Im reguła wyżej, tym większy priorytet. Aby zmienić priorytet reguły, należy ją zaznaczyć na liście i użyć przycisków **Przenieś w górę/Przenieś w dół.** Możesz także kopiować reguły lub usuwać używając przycisków **Kopiuj** lub **Usuń**. Aby skopiować regułę z jednej aplikacji do kolejnej, należy użyć przycisków kopiowania i wklejania w oknie **Modyfikuj reguły**.

Wskazówki:
- Aby szybciej zmienić parametry reguły można użyć pola znajdującego się w oknie dialogowym zestawu reguł programu.
- Reguły automatycznie tworzone przez program Outpost Firewall Pro są oznaczane kolorem niebieskim na liście. Reguły tworzone przez użytkownika są oznaczane kolorem **czarnym**.
- Zalecane jest zapisywanie aktualnego profilu przed zmianami.

5.4. Zarządzanie ruchem sieciowym w systemie

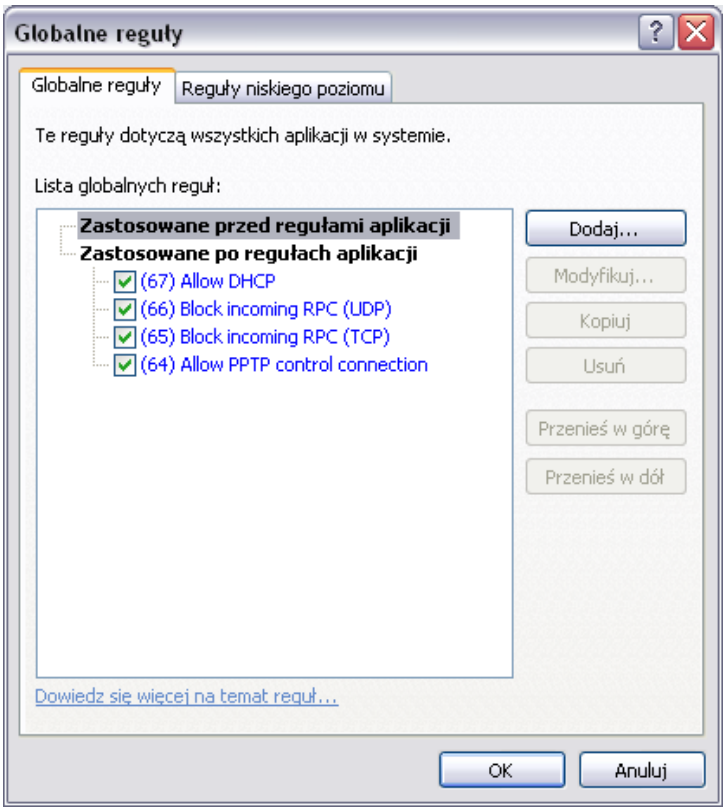
Poza kontrolą dostępu do sieci na poziomie programów, firewall programu Outpost Firewall Pro pozwala zaawansowanym użytkownikom na kontrolę całego ruchu na wszystkich poziomach.
Program Outpost Firewall Pro umożliwia:
- Definiowanie reguł wszystkich uruchomionych procesów za pomocą (globalnych reguł).
- Definiowanie ruchu nie powiązanego z aplikacjami (reguł niskiego poziomu).
- Kontrolowanie ruchu ICMP.

Aby uzyskać więcej szczegółów, przejrzyj odpowiednie rozdziały.

Uwaga:
Te ustawienia są przeznaczone dla użytkowników zaawansowanych. Jeśli ustawienie jest niepoprawnie skonfigurowane może spowodować, że firewall nie będzie chronił systemu zgodnie z Twoimi oczekiwaniami. W większości przypadków, nie jest wymagane modyfikowanie reguł lub dodawanie własnych.

5.4.1. Zarządzanie globalnymi regułami

Globalne reguły programu stosowane są do wszystkich procesów i programów próbujących uzyskać dostęp do sieci. Można, na przykład, zablokować cały ruch do wybranego protokołu lub z wybranego zdalnego komputera tworząc odpowiednie reguły. W celu zoptymalizowania funkcjonowania systemu program Outpost Firewall Pro posiada kilka zdefiniowanych globalnych reguł. Aby przeglądać listę globalnych reguł, naciśnij **Ustawienia** >**Firewall** > **Reguły systemowe:**



Możesz dodawać, modyfikować oraz usuwać globalne reguły w taki sam sposób jak reguły aplikacji. Wybrane reguły są aktywne (włączone) oraz wykonywane przez firewall. Odznacz pole obok nazwy reguły, aby program nie stosował się do wybranej reguły. Możesz włączyć regułę w dowolnym momencie zaznaczając pole. Kolejność reguł wyświetlanych nie jest przypadkowa. Ich rozmieszczenie w oknie odpowiada priorytetowi reguły. Im reguła wyżej, tym większy priorytet. Aby zmienić priorytet reguły, należy ją zaznaczyć na liście i użyć przycisków **Przenieś w górę/Przenieś w dół**
Możesz ustawiać, aby globalne reguły były zastosowane przed lub po regułach aplikacji. Możesz także kopiować reguły lub usuwać używając przycisków **Kopiuj** lub **Usuń**. Nie jest zalecane, aby usuwać wbudowane globalne reguły.

Wskazówki:

- Reguły automatycznie tworzone przez program Outpost Firewall Pro są oznaczane kolorem niebieskim na liście. Reguły tworzone przez użytkownika są oznaczane kolorem **czarnym**.
- Zalecane jest zapisywanie aktualnego profilu przed zmianami.

5.4.2. Zarządzanie regułami niskiego poziomu

Program Outpost Firewall Pro zezwala na kontrolowanie ruchu systemu przez sterowniki protokołów, które używają protokołów IP innych niż TCP lub UDP, pakietów wędrujących i innego ruch nie powiązany z aplikacjami, który nie może być kontrolowany na poziomie aplikacji. Aby wyświetlić listę reguł niskiego poziomu, naciśnij **Ustawienia** > **Firewall** > **Reguły sieci** > **Reguły globalne** i wybierz zakładkę **Reguły niskiego poziomu**.

Możesz dodawać, modyfikować lub usuwać reguły niskiego poziomu tak samo jak reguły aplikacji. Jedyne różnice to:

- Kryteria reguł zawierające typ protokołu IP, kierunek, adresy zdalny i lokalny.
- **Ustaw wysoki priorytet dla reguły,** ustawia regułę wyżej niż reguły aplikacji i globalne.

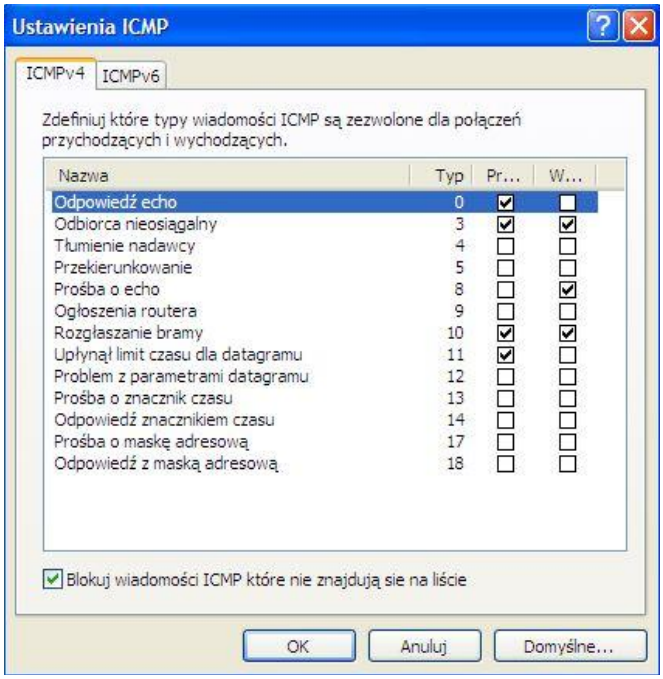
Wybrane reguły są aktywne (włączone) oraz wykonywane przez firewall. Odznacz pole obok nazwy reguły, aby program Outpost Firewall Pro nie stosował wybranej reguły. Możesz włączyć regułę w dowolnym momencie zaznaczając pole. Kolejność reguł wyświetlanych nie jest przypadkowa. Ich rozmieszczenie w oknie odpowiada priorytetowi reguły. Im reguła wyżej, tym większy priorytet. Aby zmienić priorytet reguły, należy ją zaznaczyć na liście i użyć przycisków **Przenieś w górę/Przenieś w dół**. Możesz także kopiować reguły lub usuwać używając przycisków **Kopiuj** lub **Usuń**. Nie jest zalecane usuwanie wbudowanych reguł niskiego poziomu.

Wskazówka:

- Reguły automatycznie tworzone przez program Outpost Firewall Pro są oznaczane kolorem niebieskim na liście. Reguły tworzone przez użytkownika są oznaczane kolorem **czarnym**.
- Zalecane jest zapisywanie aktualnego profilu przed zmianami.

5.4.3. Kontrola aktywności protokołu ICMP

Internet Control Message Protocol (ICMP) jest używany do wysyłania błędów i komunikatów kontrolnych pomiędzy komputerami w sieci. Program Outpost Firewall Pro pozwala zdefiniować typy i kierunki przesyłania komunikatów kontrolnych ICMP. Aby zdefiniować ustawienia filtrowania komunikatów ICMP naciśnij **Ustawienia** > **Firewall** > **Reguły sieci** poniżej opcji i naciśnij **Ustawienia ICMP**. W oknie **Ustawienia ICMP**, wyświetlone są główne typy komunikatów ICMP. Możesz zezwolić na przychodzące lub wychodzące komunikaty zaznaczając odpowiednie pole. Jeśli pole jest puste, połączenie jest zablokowane.



Użyj przycisku **Domyślne,** aby przywrócić wszystkie domyślne ustawienia ICMP.

Wskazówka:
Zalecane jest, aby nie zmieniać ustawień ICMP jeśli nie jesteś pewien wprowadzanych zmian.

5.4.4 Blokowanie podejrzanych adresów IP

Istnieje wiele sposobów blokowania podejrzanych adresów IP na przykład poprzez tworzenie specjalnych globalnych reguł firewalla czy reguł dla wybranych aplikacji. Program umożliwia blokowanie dostępu w maksymalnie prosty sposób. Służy do tego wbudowany moduł: **Blokada IP**, który umożliwia filtrowanie wszystkich przychodzących/wychodzących połączeń na podstawie określonych adresów IP.

Blokada IP umożliwia blokowanie działalności hakerskiej, blokowanie dostępu do stron WWW, reklam powiązanych z podejrzanymi adresami IP oraz blokowanie innych podejrzanych sieci komputerowych. Program umożliwia tworzenie własnych list zawierających podejrzane adresy IP lub korzystanie z gotowych list, które można zaimportować do programu.

Blokada IP posiada najwyższy priorytet. Priorytet ten jest wyższy od zdefiniowanych zaufanych aplikacji oraz sieci LAN uznanych za **Zaufane**. Żadna aplikacja, włączając w to system operacyjny,
nie ma możliwości nawiązania komunikacji z adresem, który znajduje sie w puli zablokowanych adresów IP.

Aby włączyć moduł **Blokada IP**, otwórz ustawienia programu , wybierz z listy po lewej **Blokada IP** a następnie zaznacz pole **Włącz blokadę IP**.
Program nie posiada gotowych list adresów IP ale można je pobrać za pośrednictwem Internetu lub stworzyć je ręcznie.

Aby zaimportować pobraną listę, naciśnij **Importuj** w sekcji **Blokada IP**, wybierz plik listy i naciśnij **Otwórz**. Lista jest zapisywana w konfiguracji programu i może być importowana lub eksportowana wraz z całym zestawem ustawień. Aby zapisać aktualną listę jako osobny plik, naciśnij **Eksportuj**, wybierz folder w którym lista ma być zapisana a następnie naciśnij **Zapisz**.

Uwaga:
Cała komunikacja z wybranym adresem IP dodanym do listy adresów podejrzanych będzie blokowana. Upewnij się, że chcesz dodać dany adres do listy.

Aby dodać wpis ręcznie, naciśnij **Edytuj listę hostów**, wprowadź adres w jednym z możliwych formatów, zdefiniuj komentarz (aby wiedzieć dlaczego adres IP został dodany do listy) a następnie naciśnij **Dodaj**. Wpis zostanie dodany do listy. Aby usunąć adres IP z listy, zaznacz dany adres a następnie naciśnij Usuń. Aby usunąć wszystkie adresy z listy, naciśnij przycisk **Usuń wszystko**.

Adresy można edytować w czterech formatach:

- **Nazwa domeny**. Na przykład, http://www.outpost.pl - wymagany jest dostęp do Internetu. Adres IP jest zapisywany razem z nazwą domeny i jest on używany do blokowania ruchu przez program
- **Adres IP**. Na przykład, 216.12.219.12.
- **Adres IP z maską podsieci**. Na przykład, 216.12.219.1/216.12.219.255.
- **Zakres IP**. Na przykład, 203.1.254.0-203.1.254.255.

Ręczne tworzenie listy:
Jeśli zamierzasz stworzyć listę ręcznie, przy użyciu edytora tekstu, zauważ że: nie można wstawiać spacji pomiędzy symbolami, należy definiować numer linii i oddzielać ją od danych przy użyciu przecinka. Jeśli definiujesz maskę podsieci, umieść ją od razu po adresie IP z przełącznikiem (slash) pomiędzy adresem a maską. Jeśli definiujesz zakres IP, używaj znaku minus.

Przykładowa lista powinna wyglądać następująco:

1,IP/MASK#komentarz (wpis z zamaskowanym adresem IP)
2,IP1-IP2#komentarz (wpis z zakresem od IP1 do IP2)
3,host,IP#komentarz (wpis z nazwą DNS)

Na przykład:
1,209.133.244.0/209.133.255.255#MEDIASENTRY-MEDIAFORCE
2,203.1.254.0-203.1.254.255#ASIO
3,hop.clickbank.net,209.81.0.46

Możesz ustawić program tak, aby zapisywał zablokowane pakiety w dzienniku lub wyświetlał alarm gdy pakiet jest zablokowany zaznaczając odpowiednie pola w oknie Czynności w sekcji **Blokada IP**.

6. Monitorowanie aktywności sieci

Wszystkie zdarzenia oraz aktywności są wyświetlane w głównym oknie programu oraz zapisywane w dziennikach zdarzeń. Aby wyświetlić informacje na temat aktywności sieci należy zaznaczyć **Aktywność sieci** w głównym oknie programu. Dzięki modułowi firewalla, możesz zapoznać się z **aktywnością sieci** w systemie oraz **aktualnie używanymi portami** przez działające aplikacje.

Uwaga:
Dzienniki są dostępne wyłącznie w **Widoku zaawansowanym**.

6.1 Aktywność sieci

Aby wyświetlić aktualną aktywność sieci w systemie, należy otworzyć główne okno programu i następnie wybrać **Aktywność sieci** w lewym panelu. Panel informacyjny wyświetli listę procesów które mają w tym momencie aktywne połączenie. Domyślnie, połączenia pojedynczej aplikacji są pogrupowane pod nazwą danej aplikacji. Aby wyświetlić listę połączeń aplikacji, naciśnij znak plus przy jej nazwie.
Aby wyświetlić wszystkie połączenia aplikacji, naciśnij prawym klawiszem myszy w polu panelu informacyjnego i wybierz polecenie **Sortuj**. W tym przypadku połączenia będą wylistowane bez grupowania. W tym trybie możesz sortować dane po wartości w każdej z kolumn klikając odpowiednią nazwę kolumny. Aby powrócić do domyślnego widoku, naciśnij prawym klawiszem myszy w polu panelu informacyjnego i wybierz polecenie **Sortuj**.

Oprócz widoku panelu, można także zmienić zawartość oraz liczbę wyświetlanych kolumn. Niektóre kolumny są wyświetlane tylko wtedy gdy rozwinięte są dane połączeń aplikacji. Aby zmienić wyświetlanie kolumn, należy nacisnąć prawym klawiszem myszy w polu panelu informacyjnego i wybrać polecenie **Kolumny**. W zakładce **Kolumny** należy wybrać kolumny, które mają być wyświetlane; można wybrać pojedyncze lub wszystkie kolumny. Można także zmienić kolejność wyświetlania kolumn poprzez wybranie nazwy kolumny i użycie polecenia **Przesuń w górę**/ **Przesuń w dół**.

Aby zmienić sposób w jaki wyświetlane są porty i adresy należy wybrać zakładkę **Rzędy** w oknie **Kolumny** i zdefiniować sposób wyświetlania. Naciśnij **OK**. aby zastosować zmiany.

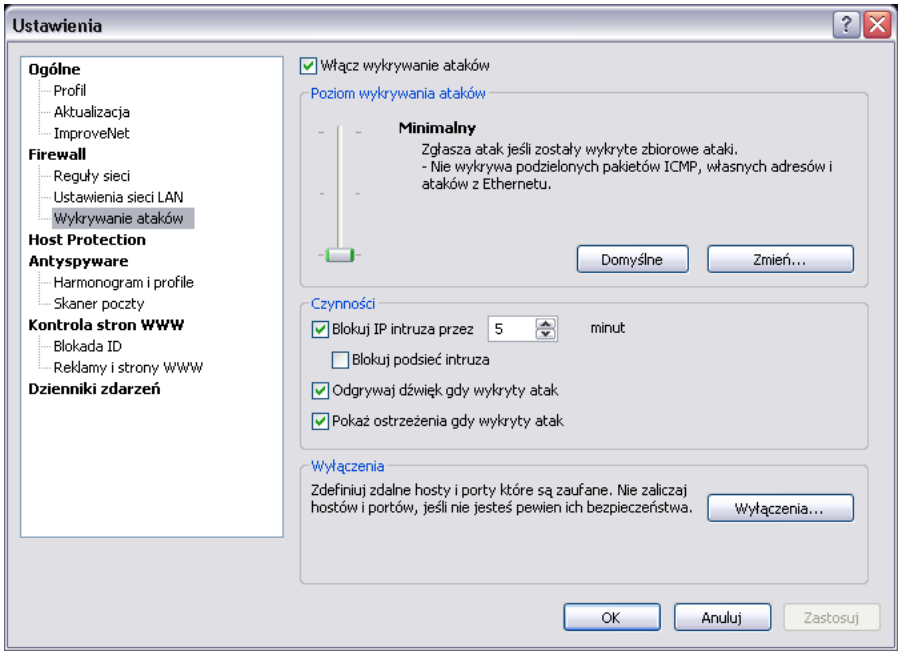
6.2 Otwarte porty

Wybierając opcję **Otwarte porty** w lewym panelu głównego okna można wyświetlać listę portów aktualnie używanych przez system i aplikacje. Struktura listy jest identyczna jak lista **Aktywność sieci**.

7. Ochrona przed atakami sieciowymi

Jednym z głównych obszarów ochrony firewallowej jest filtrowanie ruchu przychodzącego, które jest używane do kontroli całej aktywności ruchu przychodzącego oraz blokowania hakerów i złośliwych programów podczas próby ataku na komputer. Moduł Wykrywanie ataków wykrywa, ostrzega i zgłasza możliwe ataki z Internetu lub sieci lokalnej, do której podłączony jest komputer. Sprawdza przychodzące dane i ocenia ich legalność poprzez porównywanie ich z sygnaturami znanych ataków lub poprzez analizę zachowań. Pozwala na wykrywanie nie tylko znanych typów ataków takich jak skanowanie portów, ataków Denial of Service (DoS), ataków 'krótkie fragmenty' i klasy 'mój adres' i wiele innych, ale również przyszłe, jeszcze nie zdefiniowane ataki.

Aby włączyć moduł wykrywania ataków, naciśnij **Ustawienia** > **Firewall > Wykrywanie ataków** a następnie zaznacz pole **Włącz wykrywanie ataków**:



7.1. Definiowanie poziomu wykrywania ataków

Możesz definiować czułość programu Outpost Firewall Pro przy wykrywaniu ataków, wybierając określony poziom. Aby ustawić poziom wykrywania ataków, naciśnij **Ustawienia** > **Wykrywanie ataków** a następnie przesuń suwak na jedną z określonych wartości:

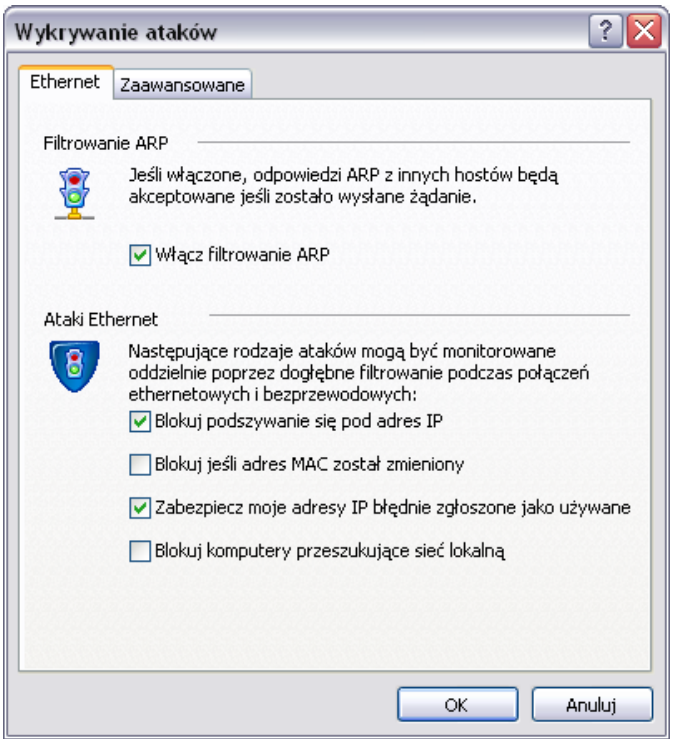
- **Maksymalny** - zgłasza każde pojedyncze skanowanie portu. Wykrywa ataki zewnętrzne oraz z Ethernetu.
- **Normalny** - zgłasza kiedy wiele portów jest skanowanych. Nie wykrywa podzielonych pakietów ICMP oraz własnych adresów. Wykrywa IP flood i duplikację adresów IP.
- **Minimalny -** zgłasza atak jeśli zostały wykryte zbiorowe ataki. Nie wykrywa podzielonych pakietów ICMP, własnych adresów i ataków z Ethernetu.

Poziom wykrywania ataków powinien być dostosowany do ryzyka zagrożenia na Twoim komputerze. Możesz także zmienić poziom ochrony naciskając przycisk **Zmień**.
Zakładka **Ethernet** pozwala zdefiniować ustawienia dla ataków Ethernet, zakładka **Zaawansowane** pozwala zdefiniować listę ataków wykrytych przez firewall oraz szczególnie chronione zagrożone porty. Gdy program Outpost Firewall Pro wykryje atak, może zmienić swoje zachowanie aby automatycznie chronić Cię przed przyszłymi atakami z tego samego adresu. Aby to zrobić, zaznacz pole **Blokuj IP intruza przez... minut.** Cały ruch z komputera atakującego będzie blokowany przez określony czas. Domyślną wartością jest 5 minut. Możesz także zablokować całą podsieć atakującego, do której należą adresy IP, zaznaczając pole **Blokuj podsieć intruza**.

Aby program wyświetlał powiadomienia o wykrytych atakach, zaznacz pole **Pokaż ostrzeżenia gdy wykryty atak** i/lub pole **Odgrywaj dźwięk gdy wykryty atak** w oknie **Czynności**.

7.2. Ochrona przed atakami z Ethernetu

Gdy dane są wysyłane z jednego komputera na drugi w danej sieci lokalnej, maszyna wysyłająca dane, wysyła także żądanie rozgłoszenia ARP, aby wyznaczyć MAC adres bazujący na adresie IP docelowego komputera. Następnie maszyna czeka na odesłanie MAC adresu. Podczas oczekiwania na pakiety rozgłoszeniowe oraz MAC adres, dane mogą zostać przejęte i przekierowane na inny komputer.
Moduł wykrywania ataków chroni także system przed zagrożeniami w sieci lokalnej. Wykrywa i blokuje ataki Ethernet, tj. IP spoofing, skanowanie ARP, ARP flood i inne. Aby zdefiniować ustawienia ataków Ethernet, naciśnij **Ustawienia** >**Wykrywanie ataków**> **Zmień:**



Dostępne są następujące opcje:

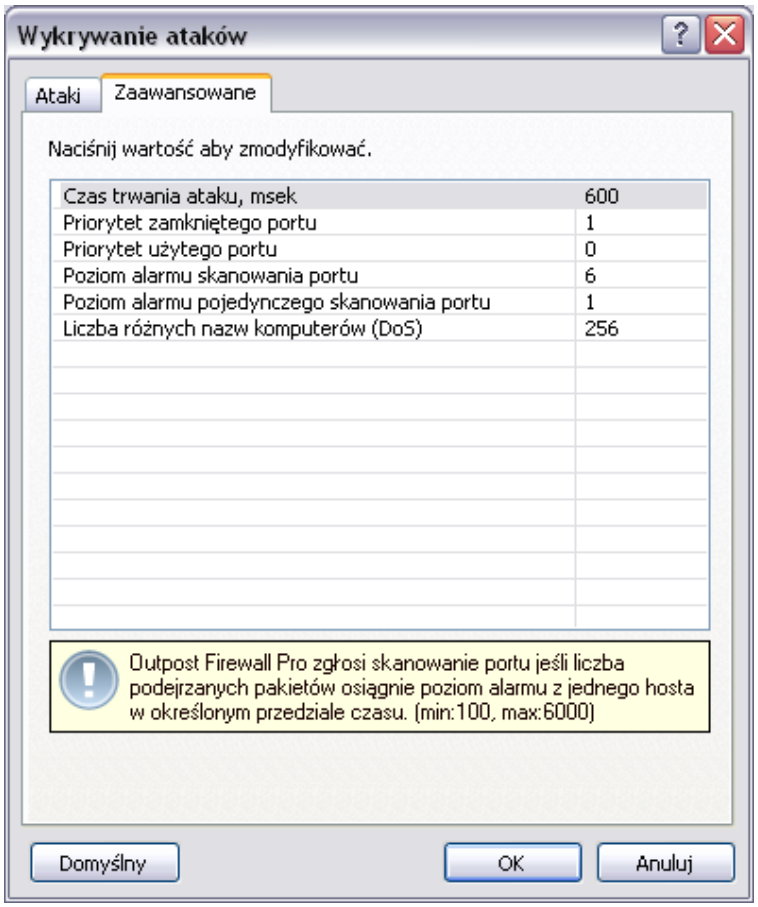
- **Włącz filtrowanie ARP -** zapobiega ARP spoofing gdy węzeł zaczyna wysyłanie ogromnej liczby odpowiedzi ARP z różnymi adresami MAC, próbując przeciążyć urządzenia w sieci. Jeśli opcja jest włączona, program zezwala jedynie na odpowiedzi przychodzące z jednych hostów, dla których było poprzednie wychodzące żądanie. Tylko pierwsza odpowiedź ARP jest akceptowana dla każdego żądania. Filtrowanie ARP chroni także przed ARP cache poisoning, które występuje gdy

ktoś z powodzeniem przechwytuje ruch Ethernetowy, używając odpowiedzi ARP oraz próbując zmienić adres karty sieciowej na taki, który może monitorować. Dodatkowo, zapobiega ARP flood, gdzie ogromna liczba fałszywych odpowiedzi ARP jest wysyłana do docelowych maszyn, zawieszając system.

- **Blokuj podszywanie się pod adres IP -** zabezpiecza przed atakami IP spoofing kiedy atakujący próbuje podszyć się pod adres IP.
- **Blokuj jeśli adres MAC został zmieniony -** program Outpost Firewall Pro wykrywa zmiany w adresach MAC i zgłasza atak. Hakerzy mogą zastępować poprawne adresy MAC własnymi adresami oraz przekierowywać pożądany ruch na maszynę hakera. Program Outpost Firewall Pro zgłosi taką aktywność i zablokuje.
- **Zabezpiecz moje adresy IP błędnie zgłoszone jako używane -** program Outpost Firewall Pro wykrywa sytuacje gdy dwa lub więcej hostów dzieli jeden adres IP. Może być to spowodowane próbą pozyskania dostępu do sieci lub zablokowanie komputera przed dostępem do sieci. Jeśli opcja jest włączona, program Outpost Firewall Pro blokuje odpowiedzi ARP z tego samego adresu IP, ale z innego adresu MAC.
- **Blokuj komputery przeszukujące sieć lokalną -** ogranicza liczbę odpowiedzi ARP. Blokuje skanowanie sieci.

7.3. Skanowanie portu

Moduł wykrywania ataków programu Outpost Firewall Pro wykonuje dwie niezależne funkcje, blokuje ataki i wykrywa skanowanie portu. W rozumieniu kontekstu, atak to wysyłanie szkodliwych danych, które może spowodować błędy w systemie (BSOD, zawieszenie systemu, itd.), lub próba uzyskania dostępu do danych na komputerze. Skanowanie portu to próba znalezienia otwartych portów w systemie w celu przeprowadzenia ataku. Po otrzymaniu żądania połączenia, moduł wykrywania ataków tworzy dziennik zdarzeń dotyczący żądania połączenia. Jeżeli otrzymano kilka żądań połączenia z tego samego zdalnego hosta, moduł wyświetli ostrzeżenie o skanowaniu portu. Czułość programu Outpost Firewall Pro w wykrywaniu skanowania portu jest definiowana poprzez **Poziom alarmu skanowania portu** (**Ustawienia** > **Wykrywanie ataków** > **Zmień** > **Zaawansowane** > **Zmień** > **Zaawansowane**):



Domyślnie, liczba żądań portu z tego samego hosta, który wywołuje alarm dla każdego poziomu wykrywania ataków wynosi: 2 dla **Maksymalnego**, 6 dla **Normalnego** i 12 dla **Minimalnego**.

Zwracanie szczególnej uwagi na zagrożone porty

Porty TCP i UDP są podzielone na kilka grup zgodnie z prawdopodobieństwem użycia przez atakującego portu w celu włamania się do systemu. Zazwyczaj, porty przypisane do zagrożonych usług tj. DCOM lub RPC powinny być monitorowane z większą uwagą, ponieważ są częstszym celem ataków hakerów. Możesz posiadać różne usługi przypisane do różnych portów, co również może przyciągać hakerów. Moduł wykrywania ataków pozwala stworzyć ustawienia dla różnych portów oraz listę portów na które program Outpost Firewall Pro będzie zwracał szczególną uwagę. Po otrzymaniu żądania połączenia na port, który może być używany przez zagrożone usługi,(na przykład, 80, 21, 23, 445, itd.), moduł nie uzna tego jako pojedynczego żądania, ale jako liczbę (X) żądań, gdzie X to waga (ważność) portu. Waga portu to ułamek dziesiętny, który określa podatność portu na zagrożenia. Im większa liczba, tym większa podatność na zagrożenia. Waga wszystkich portów, do których zostały wysłane żądania w określonym przedziale są zliczane i jeśli liczba przekroczy aktualny poziom alarmu skanowania, zostanie wyświetlone ostrzeżenie o skanowaniu portu. Nie ma sposobu, aby z całą pewnością określić czy nastąpiło skanowanie portów. Definiując ustawienie czułości modułu wykrywania ataków, określasz maksymalną liczbę prób połączenia z Twoim komputerem zanim pojawi się alarm o skanowaniu portu.

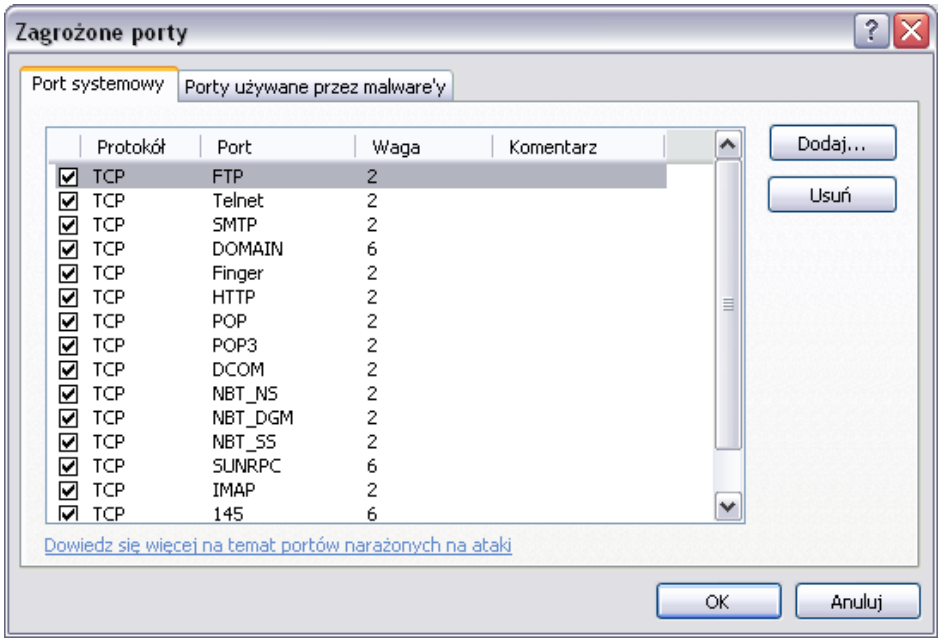
Przykład

Poziom wykrywania ataków jest ustawiony na **Normalny**; Waga zagrożonego portu 80 wynosi 7; Waga zagożonego portu 21 wynosi 3. Alarm o skanowaniu portu zostanie wyświetlony jeśli zdalny host:

- Próbuje połączyć się z portem 80 raz.

- Próbuje połączyć się z portem 21 raz a z pozostałymi portami trzy razy.
- Próbuje połączyć się do innych portów maksymalnie sześć razy.

Aby zdefiniować port, który uważasz że jest zagrożony, naciśnij **Ustawienia** > **Wykrywanie ataków**> **Zmień** > **Zaawansowane** i naciśnij **Wybierz** w oknie **Zagrożone porty**.



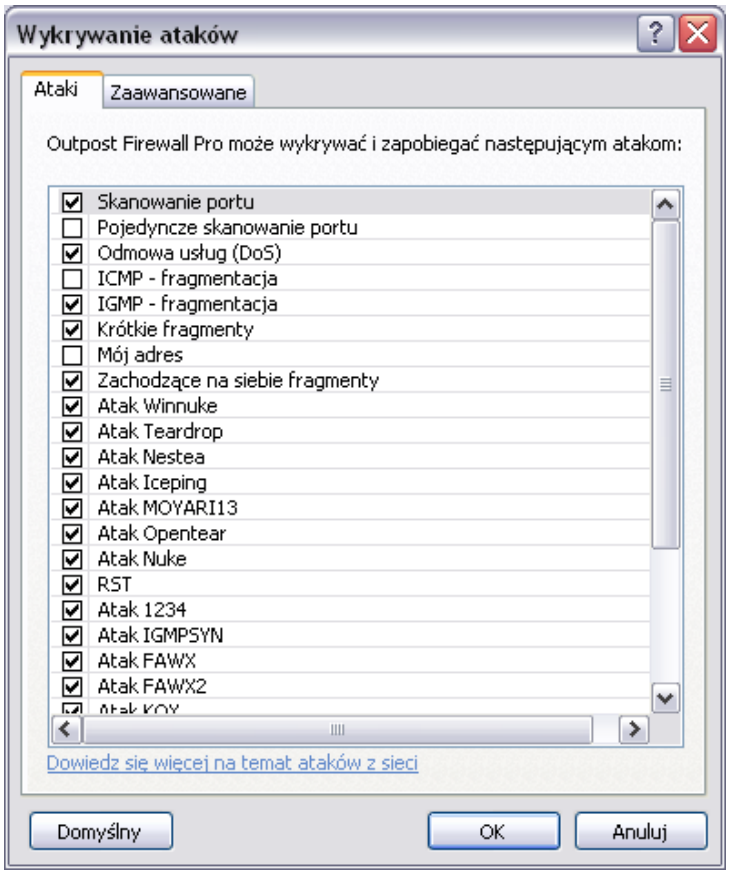
Zagrożone porty są podzielone na dwie grupy: **porty systemowe** i **porty używane przez zagrożenia**. Dodaj porty używane przez zagrożone usługi systemowe do listy portów systemowych. Dodaj porty eksploatowane przez zagrożenia do listy portów przez nie używanych. Aby dodać port, naciśnij **Dodaj** i zdefiniuj określone parametry: protokół, nazwę i wagę portu. Waga ułamek dziesiętny, który określa podatność portu na zagrożenia. Im większa liczba, tym większa podatność na zagrożenia. Możesz także dodać komentarz w odpowiednim polu. Naciśnij **OK, aby** dodać port do listy.

Uwaga:
Aby zdefiniować przedział czasu dla skanowania, edytuj ustawienia w oknie **Wykrywanie ataków (Ustawienia**> **Wykrywanie ataków** > **Zmień**> **Zaawansowane**> **Zmień**> **Zaawansowane**).

7.4. Lista ataków

Możesz wyznaczać rodzaje ataków, które program Outpost Firewall Pro będzie wykrywał i blokował. Domyślnie, wspieranych jest ponad 25 różnych typów ataków, ale możesz ustawić aby program nie wykrywał niektórych typów niższego zużycia zasobów systemu lub zatrzymać zbyt częste lub błędne wiadomości o ostrzeżeniach, które mogą się pojawiać, na przykład, gdy zaufana usługa w Twojej sieci jest błędnie rozpoznawana jako źródło ataku.

Aby zmienić listę wykrywania ataków, naciśnij **Zmień** w zakładce **Zaawansowane**, wchodząc wcześniej w **Ustawienia** >**Wykrywanie ataków** > **Zmień:**



Wszystkie wybrane typy ataków są wykrywane przez firewall. Aby wyłączyć dany typ, odznacz jego pole. Aby przywrócić ustawienia domyślne, naciśnij **Domyślny**.

7.5. Definiowanie zaufanych hostów i portów

W Twojej sieci mogą być komputery, które uważasz za zaufane, które nie są źródłem niebezpieczeństwa dla Twojego systemu, jak również porty w Twoim systemie, które nie służą jako backdoor'y dla intruzów. Innymi słowy, uważasz że moniotorowanie takich komputerów i portów jest zbędne. Moduł Wykrywanie ataków, zawiera listę wyłączeń, do której możesz dodać zaufane hosty i porty. Aby doda host, podsieć lub port do listy zaufanych, naciśnij **Ustawienia** > **Wykrywanie ataków** > **Wyłączenia**.

Definiowanie zaufanych hostów

W zakładce **Hosta i podsieci**, naciśnij **Dodaj** w oknie **Edytuj listę zaufanych hostów** zdefiniuj format adresu. Dostępne są następujące opcje:

- **Nazwa domeny**. Na przykład, www.outpost.pl. Wymagane jest aktywne połączenie internetowe, ponieważ nazwa domeny zostanie przekształcona na adres IP pobrany z Internetu.
- **Adres IP**. Na przykład, 216.12.219.12.
- **Adres IP z maską podsieci**. Na przykład, 216.12.219.1 - 216.12.219.255.
- **Adres IPv6**. Na przykład, 2002::a00:1.
- **Makra z listy**. Na przykład, LOCAL_NETWORK. Aby uzyskać więcej szczegółów dotyczących makro adresów, przejrzyj rozdział Korzystanie z makro adresów.

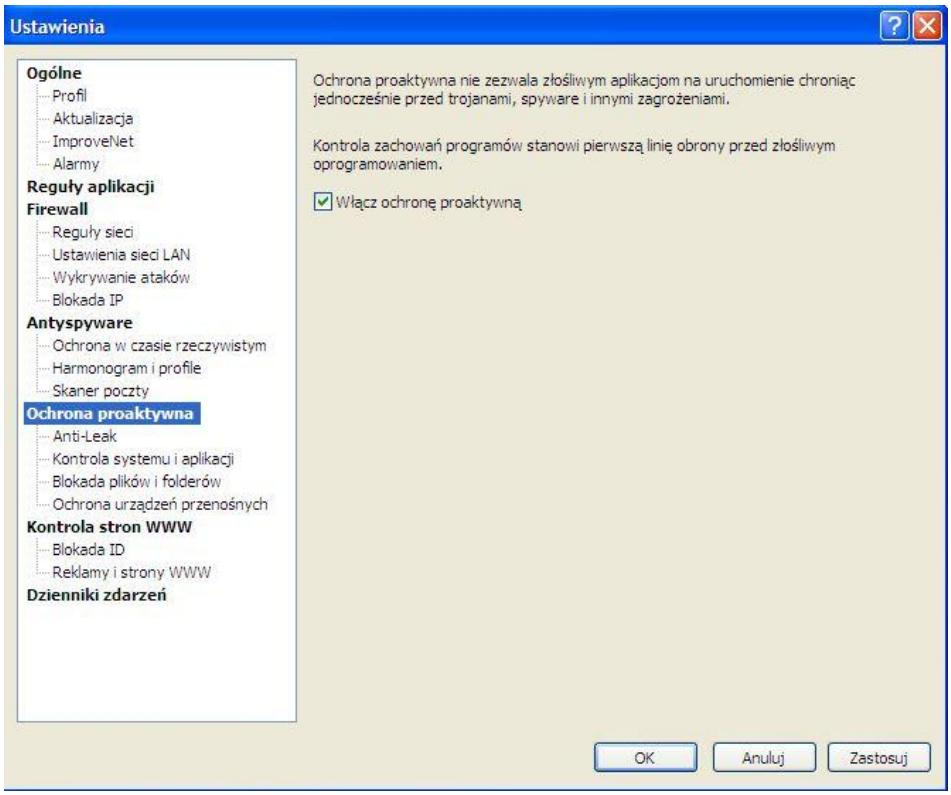
Następnie należy wprowadzić wybrany adres we wcześniej wybranym formacie (można używać wyrażeń regularnych) i nacisnąć przycisk **Dodaj.** Po dodaniu wszystkich wymaganych adresów należy nacisnąć przycisk **OK**, aby dodać je do listy. Aby usunąć z listy ustawień sieci LAN wybrany adres IP, naciśnij

przycisk **Usuń**. Aby wyłączyć wykrywanie ataków, odznacz pole **Wyszukuj ruch z bram hostów.** Zdefiniuj wszystkie hosta i podsieci, które uważasz za zaufane i naciśnij **OK,** aby zachować zmiany.

Definiowanie zaufanych portów
Wybierz zakładkę **Porty TCP** lub **Porty UDP.** Możesz wprowadzić numer portu lub zasięg przedzielone przecinkami, w polu tekstowym poniżej lub wybrać żądany port z listy, klikając dwukrotnie na niego. Aby usunąć port z listy, wymaż go z pola tekstowego. Po zdefiniowaniu wszystkich portów, naciśnij **OK** aby zachować zmiany.

8. Ochrona przed zagrożeniami w pamięci

Niektóre złośliwe programy mogą być uruchomione jako część zaufanych programów. Na przykład, niektóre konie trojańskie mogą dostać się do komputera jako moduł zaufanego programu (na przykład, Twojej przeglądarki), dzięki czemu osoba, która stworzyła Trojana, uzyskuje prawa dostępu do komputera. Inne Trojany mogą uruchamiać ukryte procesy i podszywać się pod aplikacje, które użytkownik uważa za zaufane. Ochrona proaktywna programu Outpost Firewall Pro nie zezwala na aktywność takim programom, dlatego też chroni w pełni system przed trojanami, spyware'ami i innymi zagrożeniami. Użycie technologii Kontrola Komponentów, Kontrola Anti-Leak i Kontrola krytycznych obiektów systemu zapewniają pierwszą linię obrony przed szkodliwym oprogramowaniem poprzez proaktywną kontrolę zachowań i interakcji w systemie.
Aby włączyć Ochronę Proaktywną, naciśnij **Ustawienia** na pasku narzędzi, wybierz **Ochrona Proaktywna** a następnie zaznacz **Włącz ochronę proaktywną**:



8.1. Ustawianie poziomu lokalnej ochrony

Aktualny poziom zabezpieczeń jest określany przez przez ustawienia poziomu lokalnej ochrony, który jest reprezentowany przez kombinację ustawień Kontroli Anti-Leak, Kontroli komponentów i Kontroli krytycznych obiektów systemu. Początkowy poziom ochrony jest definiowany podczas instalacji i konfiguracji i może być zmodyfikowany w dowolnym momencie zgodnie z potrzebami.
Aby zmienić poziom ochrony, naciśnij **Ustawienia** na pasku narzędzi i wybierz **Ochrona proaktywna**. Dostępne są następujące poziomy ochrony:

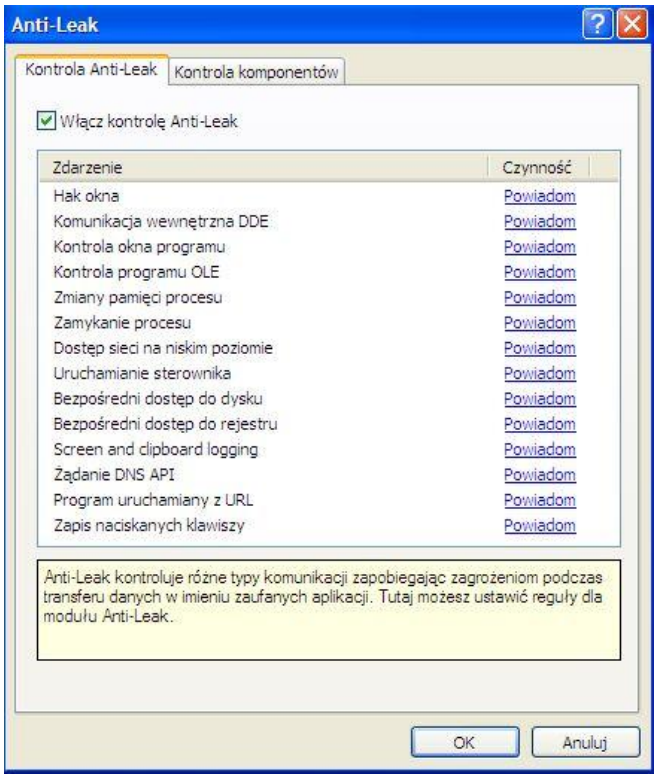
- **Maksymalny -** pozwala na największy poziom zabezpieczeń chroniąc przed technikami, które są często wykorzystywane przez złośliwe programy, aby omijać oprogramowania firewallowe. Żądanie dostępu do sieci przez nowe i zmienione komponenty jest monitorowane. Uruchamianie nowych i zmienionych plików wykonywalnych jest monitorowane. Zmiany krytycznych obiektów są monitorowane. Ten poziom zabezpieczeń może tworzyć dużą ilość zapytań wymagających ingerencji użytkownika. Zalecany jest dla użytkowników zaawansowanych.
- **Zaawansowany -** żądanie dostępu do sieci przez zmienione komponenty jest monitorowane. Cała aktywność systemu jest monitorowana. Zmiany krytycznych obiektów są monitorowane.
- **Normalny -** chroni przed większością niebezpiecznych technik. Żądanie dostępu do sieci przez zmienione wykonywalne jest monitorowane. Większość niebezpiecznych aktywności jest monitorowana. Niektóre testy bezpieczeństwa (leaktests) zostaną zakończone niepowodzeniem.
- **Minimalny -** po wybraniu tej opcji, kontrola Anti-Leak i krytyczne obiekty systemu są wyłączone. Tylko zmienione pliki wykonywalne są monitorowane. Zapewnia minimalną ilość zapytań.

Aby ustawić poziom ochrony do swoich potrzeb, naciśnij **Zmień**. W oknie możesz ustawiać parametry dla Kontroli Anti-Leak, Kontroli Komponentów i Kontroli krytycznych obiektów systemu, zgodnie z własnymi potrzebami. Aby przywrócić domyślny poziom ochrony, naciśnij **Domyślne**.

8.2. Kontrola legalności procesów

Istnieje wiele zaawansowanych niebezpiecznych technik wykorzystywanych przez złośliwe oprogramowanie do omijania oprogramowania firewallowego. Program Outpost Firewall Pro dostarcza proaktywną ochronę o nazwie **Kontrola Anti-Leak**, która blokuje znane niebezpieczne techniki, które są często wykorzystywane przez złośliwe programy, aby omijać oprogramowanie firewallowe (aby uzyskać więcej szczegółów, przejrzyj rozdział Opcje kontroli legalności procesów). Pozwala również na przechwycenie próby wycieku ważnych danych, większą kontrolę nad czynnościami wykonywanymi na stacji roboczej oraz blokowanie zagrożeń spyware, które te techniki wykorzystują. Jednakże niektóre techniki są również wykorzystywane przez zaufane programy do swoich normalnych czynności, a więc należy dostosować ustawienia do wymagań systemu ponieważ zablokowanie wybranej czynności może spowodować niestabilność systemu lub zakłócenia w pracy użytkownika.

Aby włączyć kontrolę Anti-Leak, naciśnij **Ustawienia** na pasku narzędzi, wybierz opcję **Ochrona proaktywna**, naciśnij przycisk **Zmień** i zaznacz pole **Włącz kontrolę Anit-Leak**. Dostępne ustawienia pozwalają zdefiniować czynności dla wszystkich aplikacji, które mają zezwolenie na ich wykonywanie. Wszystkie czynności podzielone są na niebezpieczne i mogą powodować niestabilność systemu lub przeciek danych oraz na podejrzane, które mogą być używane przez zaufane programy do wykonywania swoich czynności.



Wybierz czynność z listy, aby z prawej strony wyświetlić opis i ustawienia elementu. Domyślne ustawienie czynności zależy od poziomu ochrony jaki został wybrany podczas instalacji. Aby zezwolić lub zablokować czynność, należy zaznaczyć jedną z poniższych opcji:

- **Zapytaj**. Program Outpost Firewall Pro zapyta czy zezwolić na wybraną czynność czy nie.
- **Zezwól**. Wybrana czynność nie będzie blokowana dla żadnego programu.
- **Blokuj**. Wybrana czynność będzie blokowana dla wszystkich programów.

Istnieje również możliwość wyświetlania ostrzeżeń programu Outpost Firewall Pro w przypadku zezwolenia lub zablokowania aplikacji. W tym celu należy zaznaczyć pole **Zgłoś**.
Aby ustawić indywidualne reguły dla podejrzanych czynności danej aplikacji (na przykład, zezwolić danej aplikacji na modyfikowanie pamięci innych procesów), naciśnij przycisk **Wyłączenia** w oknie **Wyłączenia kontroli Anti-Leak** w ustawieniach **Ochrony proaktywnej**. Naciśnij **Dodaj,** aby wyświetlić pliki wykonywalne aplikacji. Po naciśnięciu **Otwórz**, na liście zostanie wyświetlona aplikacja, dla której można zdefiniować indywidualne ustawienia kontroli Anti-Leak. Aby zmienić ustawienia dla wybranej czynności, naciśnij link w kolumnie **Czynność.** Dostępne są takie same czynności jak w przypadku ustawień dla wszystkich programów. Możesz także ustawić globalne ustawienia systemu, definiując ustawienia **Użyj globalnych**. Naciśnij **OK, aby** zachować zmiany.

Uwaga:
Można wykonywać dowolną czynność dotyczącą innych instancji tego samego procesu, np. Internet Explorer może kontrolować inne okna Internet Explorer.

8.3. Monitorowanie aktywności systemu

Aby wyświetlić listę aktualnie używanych procesów, należy wybrać **Aktywność procesów** w głównym oknie. Domyślnie, podrzędne procesy pogrupowane są pod nazwą nadrzędnego procesu.

Użyj polecenia **Sortuj** w tytule danej kolumny aby wyświetlić dane według wartości. Aby powrócić do domyślnego widoku, kliknij prawym klawiszem myszy w pole panelu informacyjnego i naciśnij **Włącz sortowanie**.

Oprócz widoku panelu, można także zmienić zawartość oraz liczbę wyświetlanych kolumn poprzez kliknięcie prawym klawiszem myszy w dowolnym polu panelu informacyjnego i wybraniu polecenia **Kolumny**. W zakładce **Kolumny** można zaznaczyć kolumny które mają być wyświetlane. Można także zmienić kolejność wyświetlania kolumn zaznaczając nazwę kolumny a następnie używając poleceń **Przesuń w górę**/**Przesuń w dół**.

Kolumna **Status** wyświetla czy proces jest podpisany cyfrowo lub jest znany za pośrednictwem systemu ImproveNet (**Sprawdzony**)lub nie jest znany programowi (**Nieznany**).

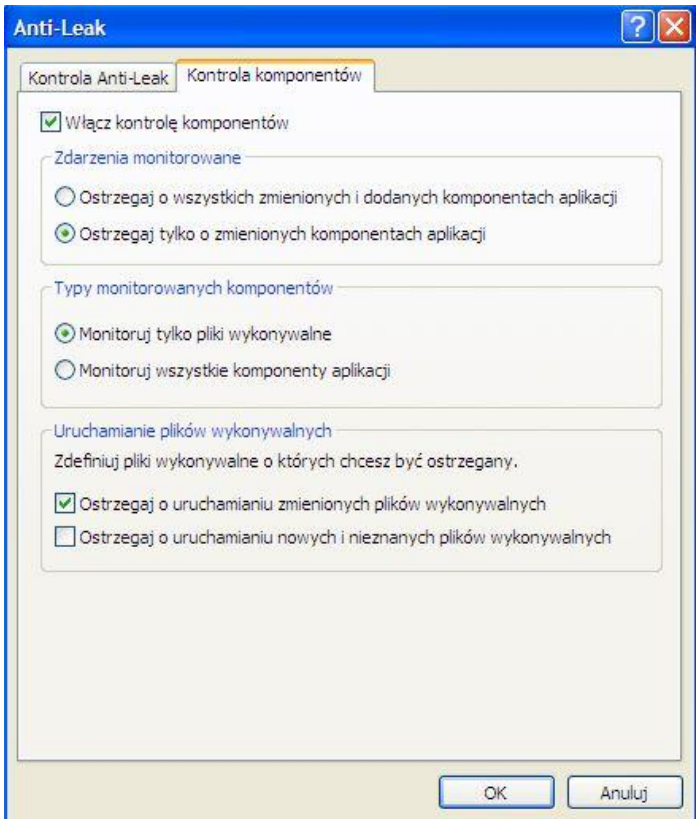
Uwaga:

Dziennik aktywności procesów jest dostępny wyłącznie w **Widoku zaawansowanym**.

8.4. Kontrola komponentów programu

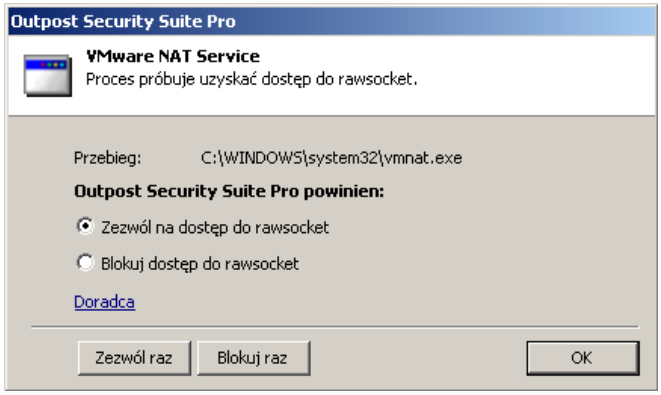
Program składa się z wielu współpracujących modułów. Każdy moduł w łatwy sposób może zostać podmieniony przez twórcę złośliwych programów na wirusa, trojana, itp. Program Outpost Security Suite nie tylko monitoruje każdy program, ale również sprawdza każdy komponent programu. Jeżeli komponent programu został zmieniony i program próbuje nawiązać połączenie sieciowe, program Outpost Firewall Pro wyświetli komunikat informujący o zmienionym komponencie i zapyta czy zezwolić na połączenie. Technologia, zwana **Kontrolą komponentów** jest odpowiedzialna za blokowanie dostępu do sieci złośliwym programom.

Aby zmienić poziom kontroli komponentów, naciśnij **Ustawienia** > **Ochrona Proaktywna** > **Zmień** i wybierz zakładkę **Kontrola komponentów**. Aby włączyć/wyłączyć Kontrolę komponentów, zaznacz/odznacz pole **Włącz kontrolę komponentów**:



Aby zdefiniować czy program Outpost Firewall Pro powinien monitorować wszystkie komponenty podczas rejestracji jako część zaufanego programu lub czy tylko zmienione komponenty, zaznacz odpowiednie opcje w oknie **Monitorowane zdarzenia**. Aby zdecydować, czy program ma ostrzegać o każdej zmianie lub dodaniu nowego komponentu aplikacji lub tylko o plikach wykonywalnych, zaznacz odpowiednie opcje w oknie **Monitorowane typy komponentów**.

W oknie **Uruchamianie plików wykonywalnych**, możesz ustawić, aby program Outpost Firewall Pro kontrolował uruchamianie zmienionych i/lub nowych plików wykonywalnych. Za każdym razem, gdy wystąpi zdarzenie, program Outpost Firewall Pro wyświetli okno z zapytaniem o czynność, czy zezwolić na aktywność aplikacji czy blokować plik.

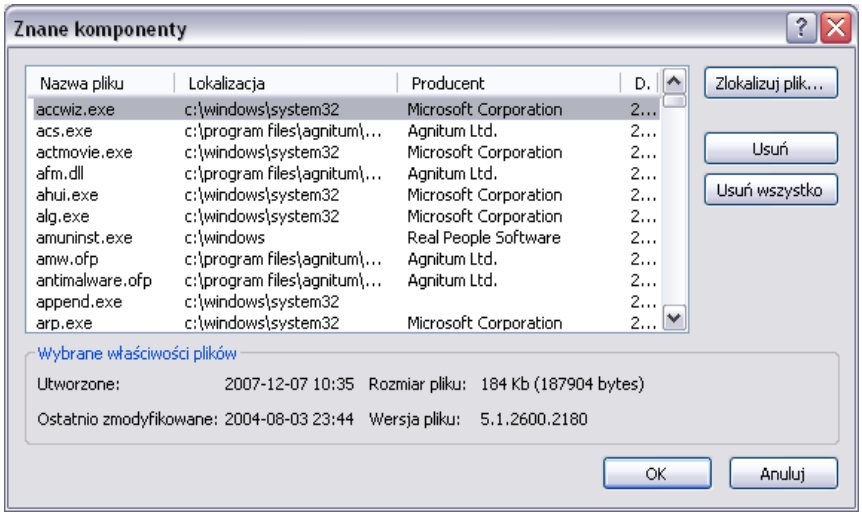


Jeśli chcesz się dowiedzieć czegoś więcej na temat pliku wykonywalnego, możesz nacisnąć przycisk **Szczegóły.**

Wskazówka:
Znane komponenty są oznaczane kolorem czerwonym, komponenty zdefiniowanej aplikacji są oznaczane kolorem zielonym.

Zarządzanie znanymi komponentami

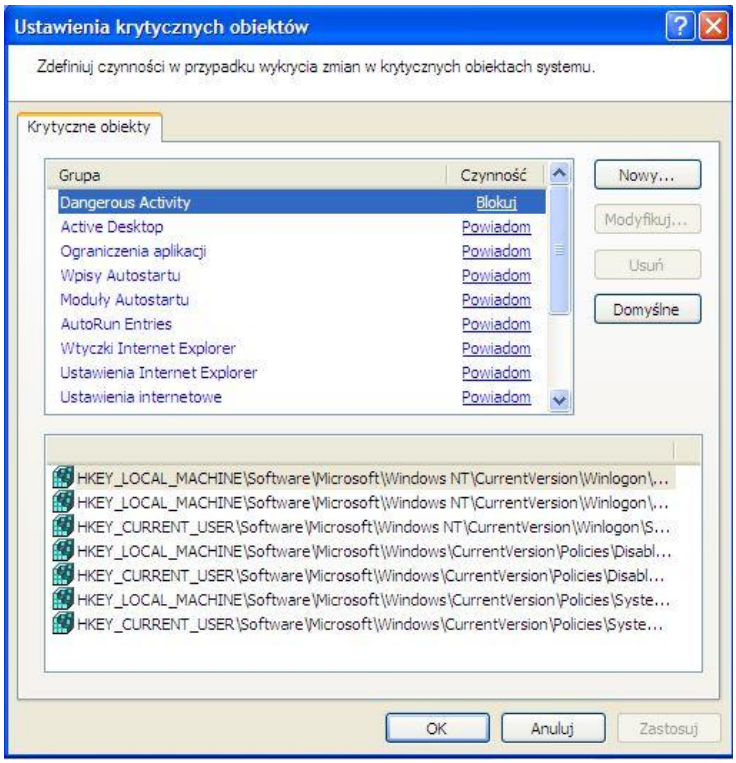
Możesz zarządzać komponentami, które mogą być używane przez aplikacje zainstalowane na komputerze. Program Outpost Firewall Pro nie będzie powiadamiał gdy aplikacja próbując uzyskać dostęp do sieci używa jednego z zarejestrowanych komponentów. Domyślnie, wszystkie komponenty systemu Windows są dodane do listy ponieważ są używane przez większość aplikacji Windows. Możesz modyfikować listę aby dostosować ją do własnych potrzeb.
Aby zmodyfikować listę komponentów, naciśnij **Wyświetl listę** w oknie **Znane komponenty** w ustawieniach **Ochrona Proaktywna**.



Komponenty są dodane automatycznie do listy, jeżeli użytkownik odpowie na aktualizację informacji o zmienionym komponencie w oknie zapytania kontroli komponentów.
Jeśli chcesz, aby informacje o komponencie były aktualizowane następnym razem gdy inne aplikacje próbują go użyć, usuń komponent z listy używając odpowiedniego przycisku. Aby otworzyć folder, w którym przechowywany jest komponent, naciśnij przycisk **Zlokalizuj plik**.

8.5. Kontrola krytycznych obiektów systemu

Jeśli instalujesz nowe oprogramowanie, system rejestruje komponenty w krytycznych miejscach rejestru systemu. Zagrożenia zazwyczaj rejestrują się w krytycznych obiektach systemu, dzięki czemu mogą przeprowadzać dane czynności nie wzbudzając podejrzeń programu. Jednakże, przed rozpoczęciem złośliwej działalności, zagrożenie próbuje modyfikować krytyczne wpisy. Aby temu zapobiec, program Outpost Firewall Pro chroni najważniejsze krytyczne obiekty systemu. Ostrzega oraz wyświetla okno z zapytaniem, jeśli plik wykonywalny próbuje modyfikować je. Lista krytycznych obiektów systemu, które są chronione przed złośliwymi i przypadkowymi zmianami jest dostępna po naciśnięciu **Ustawienia** > **Ochrona proaktywna** > **Kontrola systemu i aplikacji** > **Ustawienia**



Aby dowiedzieć się więcej na temat obiektu, zaznacz go aby zobaczyć opis poniżej. Aby włączyć kontrolę krytycznych obiektów systemu, zaznacz pole **Uruchom ochronę systemu**. Jeśli nie chcesz, aby któryś z obiektów był monitorowany przez program Outpost Firewall Pro, odznacz to pole. W dowolnym momencie możesz przywrócić domyślne ustawienia.

9. Ochrona przed zagrożeniami

Złośliwe programy stanowią powiększający się problem który dotyka wielu użytkowników komputerów. Coraz większa liczba użytkowników zmuszona jest stanąć wobec problemu jakim jest złośliwe oprogramowanie które infekuje ich systemy, gromadzi informacje na temat przeglądanych stron, zainstalowanych aplikacji i innych prywatnych danych, które wysyłane są do osób trzecich, oraz programów typu spyware które śledzą ruchy użytkowników bez ich zgody. Złośliwe programy mogą zmieniać teksty wiadomości, modyfikować pliki na dyskach twardych, wyświetlać irytujące reklamy, zmieniać strony startowe przeglądarek. Programy tego typu zajmują zasoby systemu, co powoduje znaczne zwolnienie pracy komputera. Moduł Antyspyware jest stworzony, aby chronić użytkownika przed niechcianymi i nielegalnymi czynnościami wykonywanymi przez zagrożenia. Możliwości programu dają pewność, że Twój komputer jest pozbawiony złośliwych programów, które mogą zainfekować system podczas przeglądania stron internetowych.

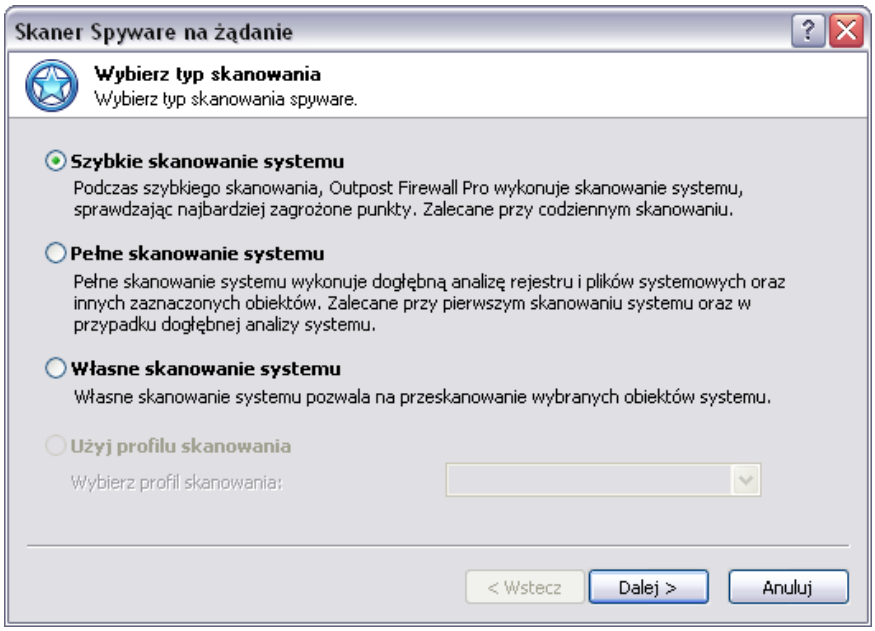
9.1. Przeprowadzanie skanowania systemu

Globalne skanowanie systemu na żądanie pozwala skanować i usuwać zagrożenia z dysków twardych, folderów sieciowych i zewnętrznych dysków. Dzięki wykluczeniu programów i plików ze skanowania (będąc pewnym, że nie są one narażone na infekcje), możesz definiować obszar skanowania zgodnie z postawionymi wymaganiami. Zalecane jest przeprowadzenie pełnego skanowania po instalacji programu Outpost Firewall Pro w celu wyszukania zagrożeń. Aby to zrobić, uruchom **Skaner na żądanie** naciskając przycisk **Skanuj w poszukiwaniu Spyware** na pasku narzędzi. Możesz także rozpocząć skanowanie

naciskając prawym klawiszem myszy na ikonę programu w zasobniku systemowym i wybierając **Uruchom skaner Antyspyware**. Kreator pomoże zdefiniować ustawienia skanowania i przeprowadzi Cię przez proces skanowania.

9.1.1. Wybór typu skanowania

W pierwszym kroku wybierz typ skanowania systemu. Dostępne są następujące opcje:



- **Szybkie skanowanie systemu** - ta opcja przeprowadza szybkie skanowanie systemu sprawdzając tylko najbardziej podatne na infekcje punkty (takie jak procesy, klucze rejestru, pliki i foldery). Ta opcja jest zalecana do użytku codziennego.
- **Pełne skanowanie systemu** - pełne skanowanie systemu opiera się na głębokiej analizie rejestru i plików systemu (procesy, skanowanie ciasteczek, skanowanie wpisów startowych). Ten rodzaj skanowania powinien być uruchamiany, gdy system skanowany jest po raz pierwszy. Operacja może zająć znaczną ilość czasu w zależności od szybkości procesora, ilości aplikacji oraz danych na dysku.
- **Własne skanowanie systemu** - ta operacja pozwala wybrać lokalizacje skanowania. Możesz dodawać określone lokalizacje, które chcesz, aby program przeskanował.
- **Użyj profilu skanowania** - ta opcja pozwala wybierać profil, który ma być przeskanowany. Ta opcja jest dostępna tylko wtedy, gdy istnieje więcej niż jeden profil.

Tworzenie profilu skanowania

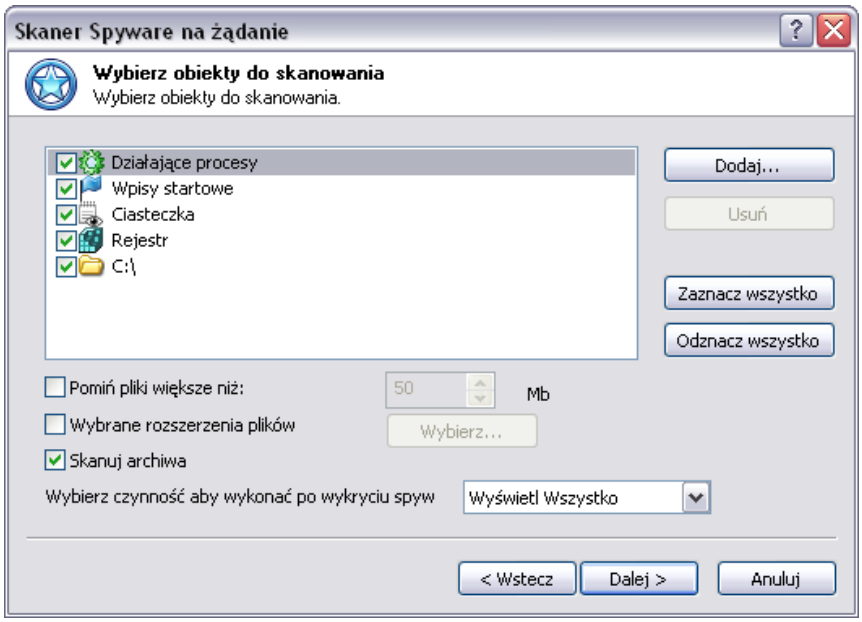
Profil skanowania składa się z predefiniowanych ustawień skanowania. Wystarczy, że wybierzesz nazwę profilu skanowania z listy. Aby stworzyć profil skanowania, naciśnij **Ustawienia** > **Harmonogram i profile**, w oknie **Profile skanowania** naciśnij **Nowy**. W oknie dialogowym podaj nazwę dla nowego profilu a następnie naciśnij **OK, aby** kontynuować.

W oknie **Edytuj profil skanowania**, możesz definiować obiekty, które mają być przeskanowane oraz inne ustawienia skanowania. Po zdefiniowaniu ustawień, naciśnij **OK, aby** zapisać profil. Nowy profil zostanie wyświetlony na liście **Profile skanowania**. Każdy profil można edytować i usuwać (oprócz domyślnych **Pełnego skanowania** i **Szybkiego skanowania**) w dowolnym momencie używając odpowiednich przycisków.

Po wybraniu typu skanowania, naciśnij **Dalej, aby** kontynuować.

9.1.2. Wybór obiektów do skanowania

Jeśli została wybrana opcja **Własne skanowanie systemu**, w oknie **Wybierz obiekty do skanowania** można definiować obiekty, dyski, foldery i pliki. Aby dodać folder do listy, naciśnij **Dodaj**, następnie w oknie **Wybierz foldery**, zaznacz konkretne lokalizacje.



Naciśnij **OK,** aby dodać foldery. Aby usunąć wybrane obiekty, naciśnij **Usuń**. Jeśli nie chcesz skanować plików o określonym rozmiarze, zaznacz pole **Pomiń pliki większe niż** i zdefiniuj pożądany rozmiar pliku. Możesz także ograniczyć skanowanie do określonych typów plików zaznaczając pole **Wybrane rozszerzenia plików**. Aby edytować listę rozszerzeń plików, naciśnij przycisk **Wybierz**. Najczęstsze typy plików, które mogą zawierać złośliwy kod są dodane do listy dla wygody użytkownika, ale można je również dodawać, edytować lub usuwać w zależności od potrzeb. Aby przywrócić domyślną listę, naciśnij przycisk **Domyślne**.

Aby skonfigurować zachowanie skanera, zdefiniuj czynność, jaka ma być wykonana po wykryciu zagrożenia. Dostępne są następujące czynności po wykryciu zagrożenia:

- **Wyświetl wszystko -** wszystkie wykryte obiekty będą wyświetlone na liście po zakończeniu skanowania. Każdy z wykrytych obiektów można przetworzyć osobno. Aby uzyskać więcej szczegółów, przejrzyj rozdział Usuwanie wykrytych zagrożeń.
- **Wylecz** - po wykryciu podejrzanego obiektu, program Outpost Firewall Pro spróbuje go wyleczyć. Jeśli obiekt będzie nieuleczalny, zostanie automatycznie umieszczony w kwarantannie.
- **Kwarantanna** - program Outpost Firewall Pro będzie umieszczał podejrzane obiekty w kwarantannie.

Jeśli uważasz, że archiwa mogą zawierać złośliwe programy, zaznacz pole **Skanuj archiwa**. Po zdefiniowaniu obiektów i lokalizacji do przeskanowania, naciśnij **Dalej, aby** rozpocząć proces skanowania.

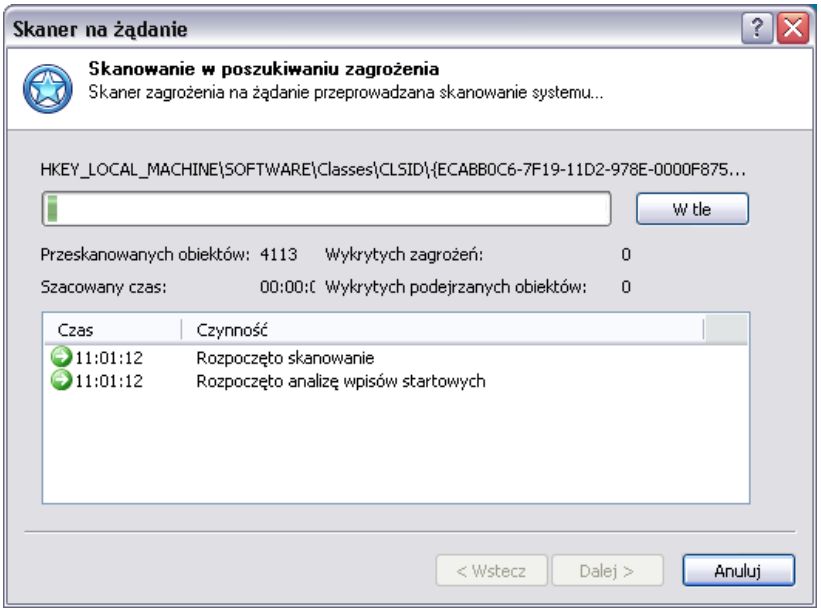
Uwaga:

- Spyware nie może być poddany leczeniu. Zostaje automatycznie i przenoszony do kwarantanny.
- Zdefiniowane czynności nie mają wpływu na krytyczne obiekty oraz ciasteczka. Jeśli podczas skanowania został wykryty krytyczny obiekt lub ciasteczko, żadna czynność nie zostanie podjęta. Po zakończeniu skanowania, dostępna będzie opcja **Wybierz czynność po wykryciu spyware**, jeśli wcześniej wybrano opcję **Wyświetl wszystko**.

- Program Outpost Firewall Pro skanuje pliki spakowane w formacie ZIP, RAR oraz CAB.

9.1.3. Skanowanie określonych lokalizacji

Po naciśnięciu przycisku **Dalej**, program Outpost Firewall Pro zacznie skanować wybrane obiekty i lokalizacje. Poziom postępu wyświetla bieżące skanowanie i statystyki: ogólną ilość skanowanych i wykrytych potencjalnie niebezpiecznych obiektów.



Proces skanowania może odbywać się w tle. Jeśli chcesz pracować z programem Outpost Firewall Pro, podczas gdy skanowanie jest w toku, naciśnij przycisk **W tle** a kreator zostanie zminimalizowany do paska postępu w panelu informacyjnym. Aby ponownie zobaczyć okno skanowania, wybierz **Antyspyware** w lewym panelu głównego okna i naciśnij **Pokaż szczegóły** w panelu informacyjnym. Aby przerwać skanowanie i zobaczyć rezultaty, naciśnij **Anuluj**.

Kiedy skanowanie jest ukończone, automatycznie wyświetlana jest lista wykrytych obiektów (jeśli takowe zostały znalezione). Jeśli Twój system jest czysty (brak podejrzanych obiektów), wyświetlają się tylko statystyki skanowania.

9.1.4. Usuwanie wykrytych zagrożeń

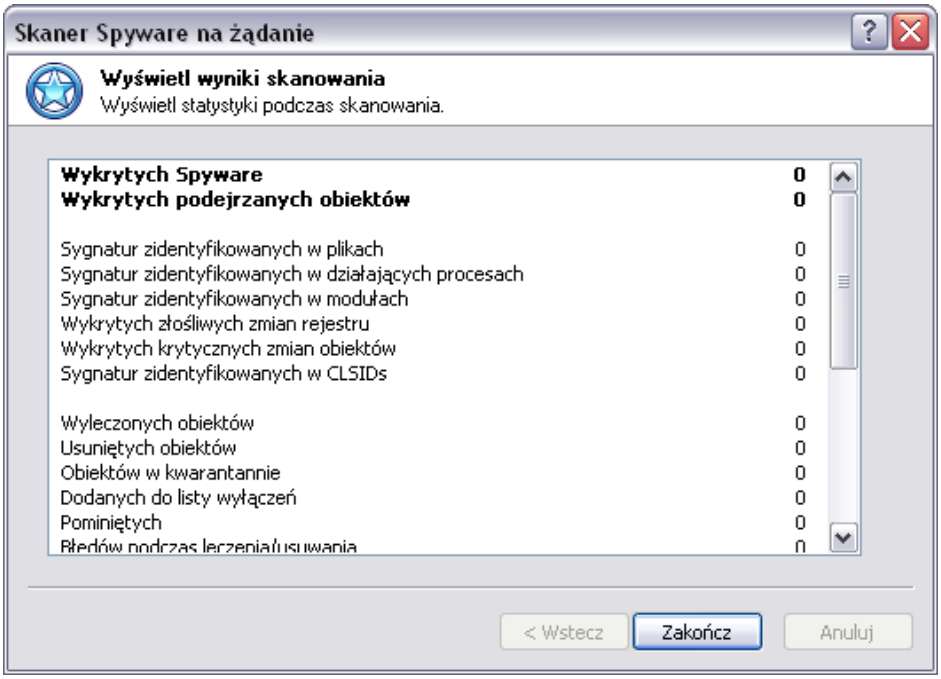
Opcja **Zdefiniuj czynności dla wykrytych obiektów** pozwala wyświetlać wykryte zagrożenia w celu ich usunięcia. Obok każdego wykrytego zagrożenia, wyświetlane są informacje o stopniu ryzyka, kategorii, do której należy i czynności, jaka została wykonana po wykryciu zagrożenia. Podwójne kliknięcie na obiekcie wyświetla lokalizację, w której się znajduje. Aby zmienić czynność, należy nacisnąć prawym klawiszem myszy na obiekt i wybrać czynność z menu.
Zaznacz obiekty i naciśnij **Dalej**. Program Outpost Firewall Pro wykona określone czynności – wyleczy obiekt, usunie go z pamięci lub przeniesie do kwarantanny. Znajdujące się w kwarantannie zagrożenie nie zagraża systemowi. Aby uzyskać więcej szczegółów, przejrzyj rozdział Kwarantanna.
Oprogramowanie, które nie zostało wybrane zostanie nienaruszone i będzie kontynuowało swoją aktywność w systemie.

Wskazówka:
W przypadku, gdy wiesz że dany program nie stanowi zagrożenia, możesz go dodać do listy wyłączeń. Program Outpost Firewall Pro będzie pomijał programy na liście wyłączeń i nie będzie wyświetlał ostrzeżeń, gdy wykryje ich aktywność. Aby dodać program do listy wyłączeń, należy nacisnąć prawym klawiszem myszy na nazwę programu i wybrać **Dodaj do wyłączeń.** Możesz także definiować foldery, które nie chcesz, aby program Outpost Firewall Pro skanował. W dowolnym momencie możesz usunąć programy i foldery z listy wyłączeń używając przycisku **Wyłączenia** w oknie **Antyspyware** w **Ustawieniach** programu.

Uwaga:
Ciasteczka nie są spyware'ami, ale mogą być użyte do wykradania prywatnych informacji z komputera. Programy spyware zainstalowane na komputerze mogą zapisywać informacje do ciasteczek i podczas wizyty na odpowiedniej stronie internetowej, informacje mogą zostać przesłane do osób trzecich.

9.1.5. Wyświetlanie rezultatów skanowania

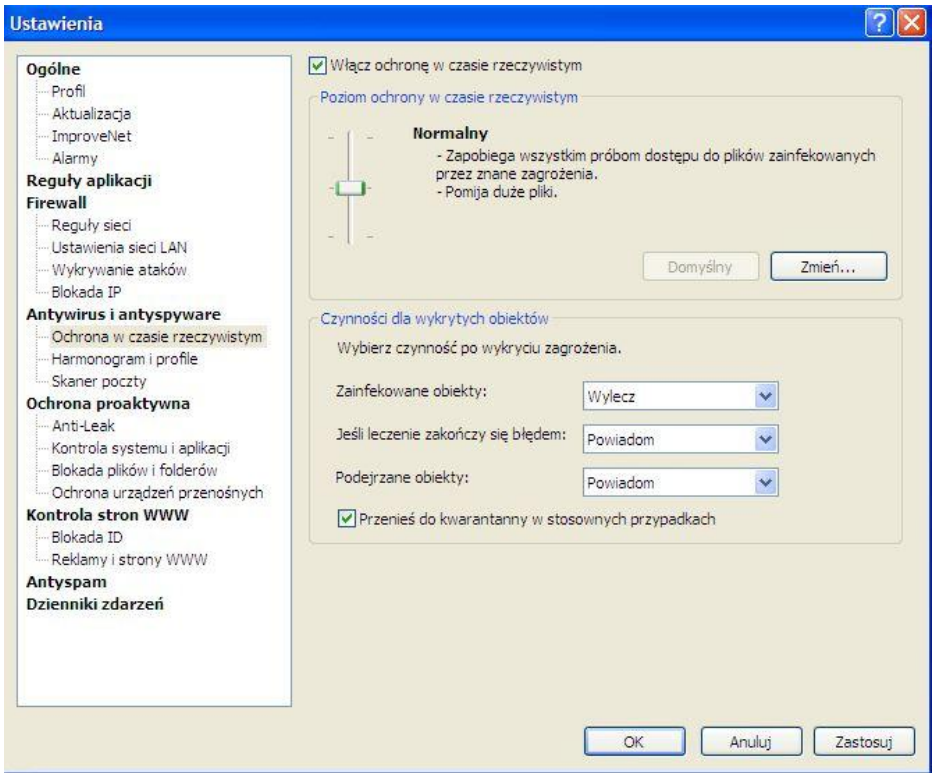
W ostatnim kroku kreator wyświetla raport skanowania z liczbą wykrytych, wyleczonych, usuniętych i przeniesionych do kwarantanny złośliwych programów (spyware) oraz inne szczegóły skanowania. Po obejrzeniu rezultatów należy nacisnąć **Zakończ**, aby zamknąć kreatora.



Uwaga:
Aby zobaczyć obiekty, które moduł Antyspyware wykrył i usunął, należy otworzyć **Dziennik zdarzeń** w lewym panelu programu Outpost Firewall Pro i wybrać zdarzenia dla **Antyspyware**.

9.2. Ochrona w czasie rzeczywistym

Moduł Antyspyware zapewnia ochronę w czasie rzeczywistym przed spyware'ami. Gdy ochrona w czasie rzeczywistym jest włączona, wszystkie narażone na infekcje obiekty są stale monitorowane. Aby włączyć ochronę w czasie rzeczywistym, należy nacisnąć **Ustawienia** > **Antyspyware** i zaznaczyć pole **Włącz ochronę w czasie rzeczywistym**:

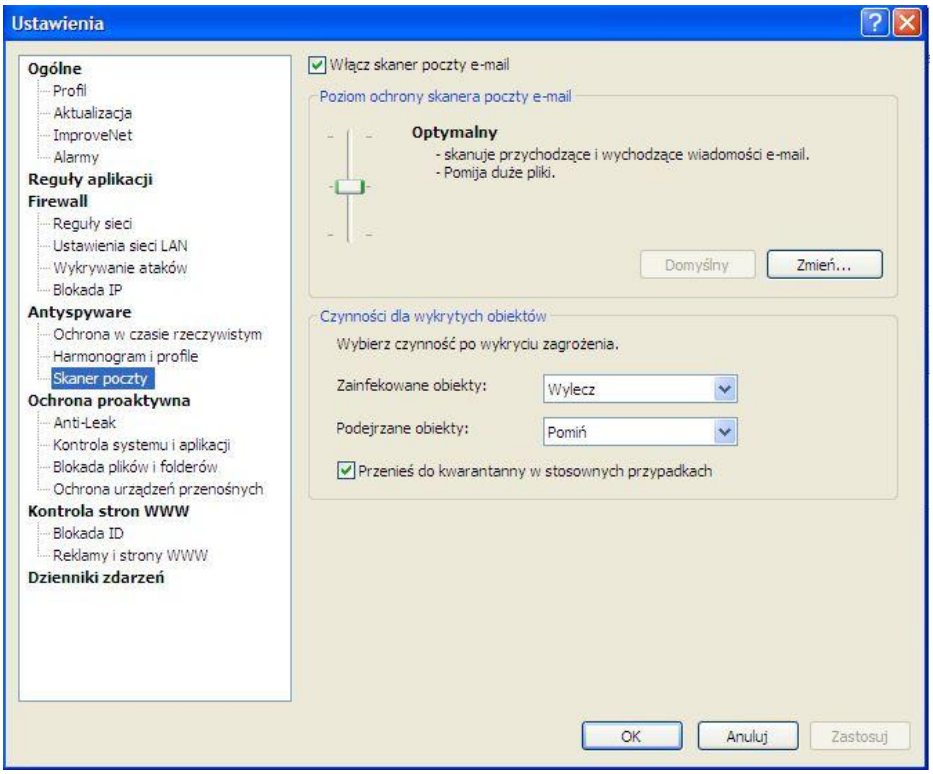


Podczas wykrycia podejrzanej aplikacji, program Outpost Firewall Pro będzie blokował aktywność tej aplikacji i wyświetlał ostrzeżenie, które zezwoli na natychmiastowe przeskanowanie obiektu. Możesz także ustawić wyświetlanie ostrzeżeń oraz odgrywanie dźwięków, gdy wykryte jest zagrożenie naciskając przycisk **Ostrzeżenia** i zaznaczając odpowiednie pole. Program Outpost Firewall Pro będzie wyświetlał ostrzeżenie oraz odgrywał zdefiniowany dźwięk za każdym razem gdy zostanie wykryte zagrożenie, przeniesione do kwarantanny lub wyleczone. Jeśli chcesz wyłączyć ze skanowania określone foldery, naciśnij przycisk **Wyłączenia** w ustawieniach **Antyspyware**, wybierz zakładkę **Ścieżki** i naciśnij **Dodaj**. Wybierz odpowiedni folder i naciśnij **OK**, aby dodać go do listy wyłączeń.

Uwaga:
Aby zobaczyć obiekty które moduł Antyspyware wykrył i usunął, wybierz **Dziennik zdarzeń** w głównym oknie programu i naciśnij dziennik **Antyspyware**.

9.3. Skanowanie załączników

Jednym z najprostszych sposobów dostania się złośliwego oprogramowania do zasobów komputera są załączniki dołączane do poczty. Po uruchomieniu załącznika, w którym jest wirus, następuje infekcja systemu, która może doprowadzić do awarii komputera. Program Outpost Firewall Pro chroni przed załącznikami zawierającymi wirusy, robaki i trojany oraz obejmuje kwarantanną te, które rozpoznał jako potencjalnie niebezpieczne.



Filtr załączników

Jeśli uważasz, że niektóre typy załączników są potencjalnie niebezpieczne mimo, że zostały przeskanowane na obecność wirusów (na przykład, skaner mógł nie wykryć nowej odmiany wirusa) lub skanowanie poczty zostało wyłączone, nadal masz możliwość zapobiegnięcia możliwemu uszkodzeniu systemu. Filtr załączników przenosi do kwarantanny lub usuwa określone typy plików zgodnie z ustawieniami w oknie **Filtr załączników** w ustawieniach **Skanera poczty**.

Występują trzy poziomy ochrony poczty :

• **Maksymalny –** wiadomości przychodzące i wychodzące są sprawdzane. Stosowane są metody heurystyczne celem wykrywania nowych infekcji Malware. Załączniki powyżej 5Mb nie będą skanowane. Sprawdzane będą obiekty OLE.

• **Optymalny -** wiadomości przychodzące i wychodzące są sprawdzane. Załączniki powyżej 5Mb nie będą skanowane.

• **Normalny –** tylko wiadomości przychodzące będą sprawdzane. Pliki powyżej 5Mb nie będą sprawdzane.

Użytkownik może wykonać modyfikację ustawień korzystając z przycisku **Zmień.** W zakładce **Filtr załączników,** możliwe jest zdefiniowanie ustawień dla typów załączników.

Zaznacz pole **Zmień nazwy załącznikom o określonych typach** jeśli chcesz zmienić rozszerzenie pliku lub **Przenieś do kwarantanny załączniki o określonych typach** aby przenieść je do kwarantanny. Aby dokonać edycji listy rozszerzeń, naciśnij przycisk **Rozszerzenia**. Najczęstsze typy plików, które mogą zawierać złośliwy kod zostały od razu dodane do listy. Użytkownik może dodawać, edytować lub usuwać rozszerzenia plików w zależności od potrzeb. Aby przywrócić oryginalną listę, naciśnij przycisk **Domyślne**.

Jeśli nie chcesz, aby filtr zmieniał nazwy załącznikom lub przenosił je do kwarantanny, zaznacz pole **Wyłącz filtr załączników**. Aby dostawać powiadomienia o czynnościach filtra, naciśnij przycisk **Ostrzeżenia** w oknie **Ostrzeżenia**.

Uwaga:

Wspierane są protokoły IMAP, POP3 i SMTP. Program Outpost Firewall Pro nie wspiera kont pocztowych na serwerze Microsoft Exchange.

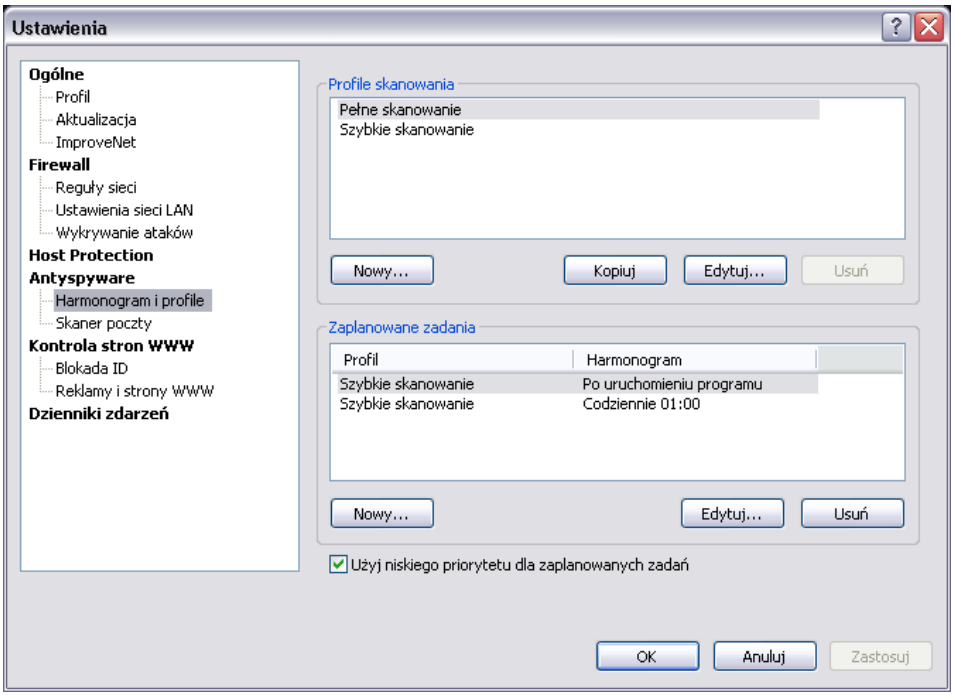
9.4. Kwarantanna

Domyślna procedura programu Outpost Firewall Pro dla usuniętych złośliwych programów nie oznacza ich permanentnego usunięcia lecz umieszczenia w specjalnie izolowanym miejscu zwanym **Kwarantanną**. Obiekty w kwarantannie nie stanowią zagrożenia dla komputera.
Obiekty, które zostały objęte **Kwarantanną** wyświetlone są w głównym oknie programu Outpost Firewall Pro. Dla każdego obiektu w kwarantannie, wyświetlane są data i czas wykrycia, opis oraz szczegółowe informacje dotyczące lokalizacji wszystkich połączonych ze sobą obiektów. Informacje te znajdują się w panelu **Szczegółowe informacje** znajdującym się poniżej.
Każdy obiekt w kwarantannie tj. spyware, może zostać przywrócony z kwarantanny. Aby przywrócić obiekt, naciśnij link **Przywróć**. (Wpisy rejestru oraz pliki INI zostaną przywrócone automatycznie). Możesz także przywrócić obiekt i dodać go do listy wyłączeń wybierając **Przywróć i dodaj do listy wyłączeń** z menu kontekstowego. Obiekty umieszczone w kwarantannie przez filtr załączników można zachowywać na dysku twardym używając polecenie **Zapisz jako**. To pozwoli na przeglądanie zawartości pliku bez szkody dla systemu. Możesz także na stałe usunąć każdy obiekt naciskając link **Usuń**. Aby usunąć wszystkie obiekty w kwarantannie, użyj polecenia **Wyczyść kwarantannę** z menu kontekstowego.

Uwaga:
Niektóre spyware'y nie mogą być umieszczane w kwarantannie i są automatycznie usuwane.

9.5. Sporządzanie harmonogramu skanowania systemu

Sporządzanie harmonogramu skanowania systemu jest bardzo użyteczną opcją jeśli chcesz zaoszczędzić czas lub chcesz wykonać regularne skanowanie. Program Outpost Firewall Pro pozwala przeprowadzać skanowanie w trybie bez nadzoru, gdy nie jesteś w pobliżu komputera. Aby ustawić skanowanie z harmonogramu, naciśnij **Ustawienia** > **Harmonogram i profile:**

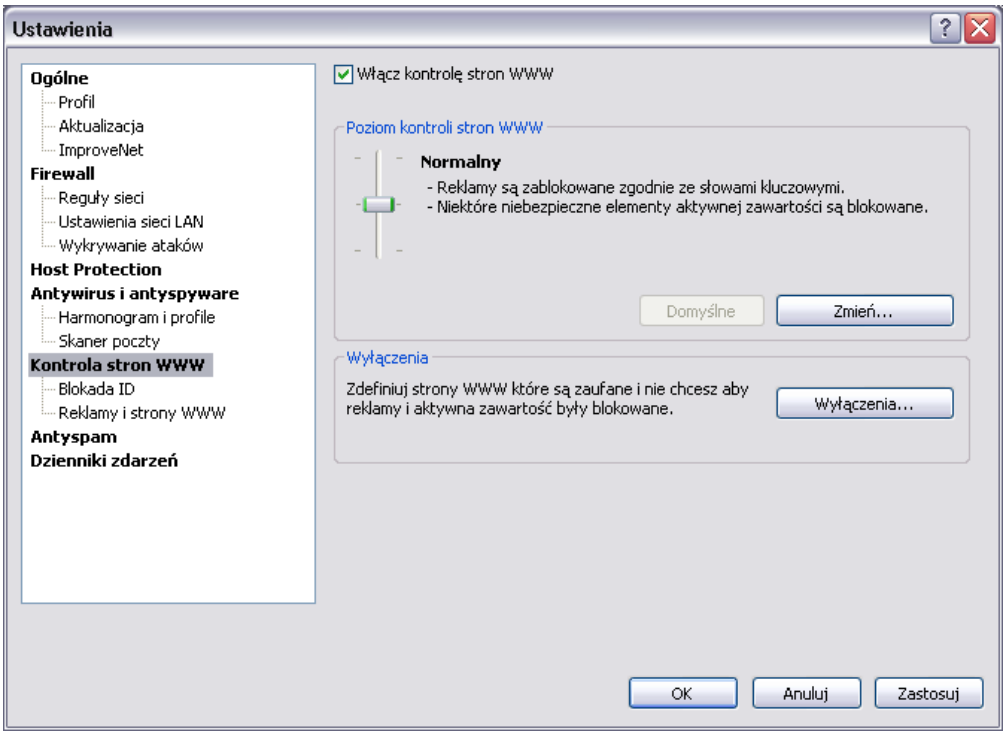


Domyślnie, skanowanie z harmonogramu jest przeprowadzane po aktualizacji bazy danych zagrożeń, codziennie o godzinie 1:00 nad ranem. Aby stworzyć zadanie z harmonogramu, naciśnij **Nowy**. Wprowadź nazwę dla zadania, wybierz profil skanowania z menu rozwijanego oraz zdefiniuj harmonogram skanowania. Aby stworzyć regularne skanowanie, użyj listy **Jak często:**. Jeśli wybierzesz skanowanie

Tygodniowo, będziesz mógł także zdefiniować dzień oraz godzinę, o której program Outpost Firewall Pro ma rozpocząć skanowanie. Jeśli wybierzesz skanowanie **Codziennie**, będziesz mógł zdefiniować czas rozpoczęcia skanowania. Aby tymczasowo wyłączyć zadanie z harmonogramu, bez usuwania, należy je zaznaczyć na liście i nacisnąć **Edytuj** i odznaczyć pole **To zadanie jest włączone**. Profil nie zostanie usunięty i w dowolnym momencie może być włączony. Aby usunąć profil, należy go zaznaczyć i nacisnąć przycisk **Usuń**.
Aby zachować zasoby systemowe, gdy system wykonuje krytyczne operacje, należy zaznaczyć pole **Użyj niski priorytet dla zadań z harmonogramu**. Naciśnij **OK,** aby zachować zmiany. Program Outpost Firewall Pro uruchomi skanowanie systemu zgodnie z zadaniem zdefiniowanym w harmonogramie.

10. Kontrola aktywności sieci

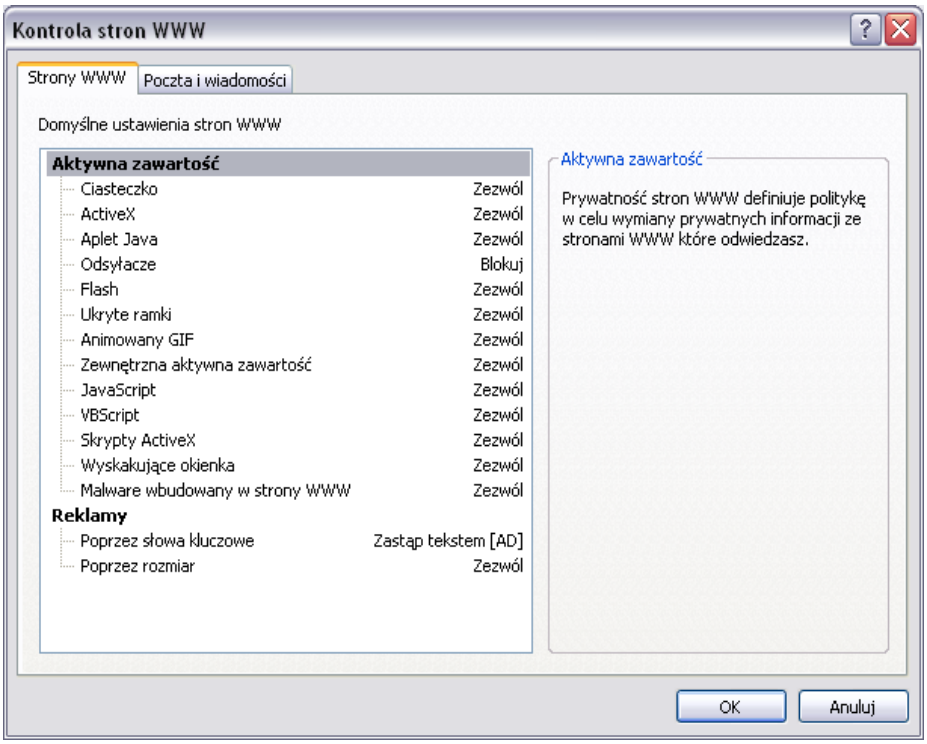
Współcześni projektanci stron WWW wbudowują aktywne elementy w strony, aby rozbudować ich funkcjonalność oraz udoskonalić użytkowanie strony WWW.
Te elementy zawierają ActiveX, Flash, JavaScript, VBScript oraz inne. Te technologie zostały dostarczone, aby polepszyć doznania użytkownika przeglądającego strony WWW. Niestety obecnie hakerzy z powodzeniem wykorzystują te same elementy aby przejść kontrolę nad Twoim komputerem. Aktywne elementy mogą stanowić zagrożenie dla Twojego systemu. Wiele stron używa ich także, aby wyświetlać natarczywe reklamy, które w znaczący sposób zmniejszają prędkość przeglądania stron. Poza tym, wiele stron WWW posiada banery reklamowe, które często są bardzo irytujące, zaśmiecają strony niepożądanymi obrazkami, spowalniając dodatkowo wyświetlanie stron.
Komponent kontroli stron WWW zapewnia ochronę podczas surfowania po Internecie. Kontroluje operacje aktywnych elementów, wbudowanych w strony WWW, które przeglądasz, lub w wiadomości e-mail, które otrzymujesz. Możesz zezwalać lub blokować te elementy niezależnie. Następujące elementy są kontrolowane przez moduł: ActiveX, Java aplety, programy bazujące na skryptach Java i Visual Basic, ciasteczka, wyskakujące okienka, skrypty ActiveX, wewnętrzna aktywna zawartość, odsyłacze, ukryte ramki, animowane obrazy GIF, animacje flash. Kontrola stron WWW blokuje wyświetlanie banerów reklamowych, co zwiększa prędkość przeglądania stron. Reklamy mogą być blokowane przy użyciu dwóch kryteriów: poprzez słowa kluczowe znalezione w kontekście strony lub poprzez rozmiar wyświetlanego obrazka. Aby włączyć ochronę przed niepożądanymi reklamami oraz aktywna zawartością, naciśnij **Ustawienia** > **Kontrola stron WWW** i zaznacz pole **Włącz kontrolę stron**:



10.1. Ustawianie poziomu kontroli stron WWW

Możesz zdefiniować jak gruntownie program Outpost Firewall Pro powinien przetwarzać zawartość stron WWW. Aby zmienić poziom kontroli stron WWW, naciśnij **Ustawienia** na pasku narzędzi a następnie wybierz **Kontrola stron WWW**. Dostępne są następujące poziomy:

- **Maksymalny** - reklamy są blokowane zgodnie ze słowami kluczowymi i rozmiarami. Cała niebezpieczna aktywna zawartość jest zablokowana.
- **Normalny** - reklamy są zablokowane zgodnie ze słowami kluczowymi. Niektóre niebezpieczne elementy aktywnej zawartości są blokowane.
- **Minimalny -** reklamy są zablokowane zgodnie ze słowami kluczowymi. Cała aktywna zawartość jest zezwolona.



Jeśli chcesz zdefiniować dodatkowe ustawienia, zmień poziom ochrony. Naciśnij przycisk **Zmień** a w wyświetlonym oknie będziesz mógł skonfigurować jaka czynność ma zostać podjęta w przypadku wykrycia aktywnej zawartości. Przejdź do zakładki **Strony WWW** lub **Poczta i wiadomości,** aby wybrać typ elementu, którym chcesz zmienić. Po prawej stronie okna wyświetlony jest opis elementu oraz ustawienia. Aby zezwolić lub zablokować dany element, wybierz jedną z dostępnych opcji:

- **Zezwól** - wszystkie elementy tego typu będą zezwolone.
- **Zapytaj** - program Outpost Firewall Pro będzie wyświetlał zapytanie przed zezwoleniem na element tego typu.
- **Blokuj** - elementy tego typu są zawsze blokowane.

Dla reklam, program Outpost Firewall Pro daje możliwość zastąpienia banerów reklamowych tekstem "[AD]" lub przeźroczystym obrazkiem w rozmiarze banera. Naciśnij **OK, aby** zapisać zmiany.
Przycisk **Domyślny** przywraca domyślne ustawienia poziomu ochrony.

Uwaga:

- Opcja **Zapytaj** nie jest dostępna dla ukrytych ramek oraz zewnętrznej aktywnej zawartości.
- Niektóre strony wymagają aby wybrane elementy aktywnej zawartości były aktywne, aby móc wyświetlić stronę prawidłowo. Jeśli ustawienia dla wszystkich stron będą bardzo restrykcyjne, mogą wystąpić następujące problemy: nie zostaną wyświetlone niezbędne obrazki, strona WWW nie zostanie załadowana w całości, strona WWW zostanie załadowana nieprawidłowo lub niektóre usługi zawarte w apletach nie będą działały. Jeśli taki problem występuje tylko na niektórych stronach, zmień ustawienia tych stron, dodając je do listy wyłączeń.

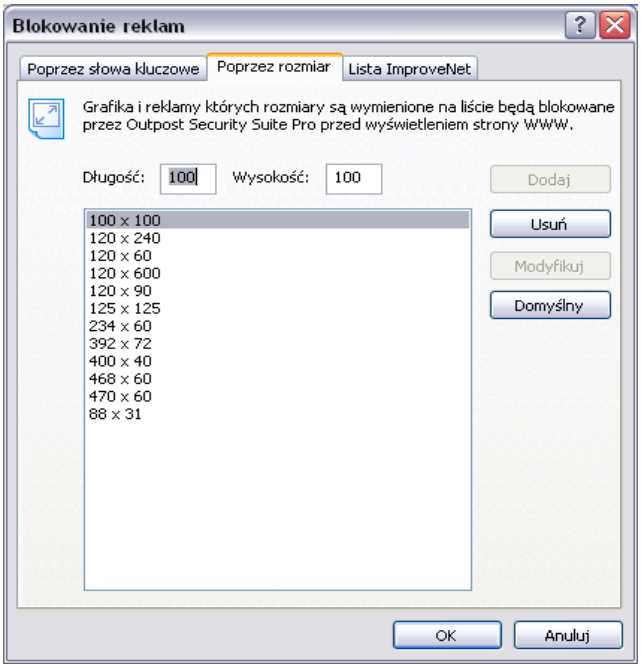
10.2. Blokowanie reklam

Reklamy mogą być blokowane na trzy sposoby: poprzez słowa kluczowe znalezione w kontekście strony WWW, poprzez rozmiar obrazków reklamowych oraz użycie danych zebranych poprzez program ImproveNet

Blokada poprzez słowa kluczowe

Program Outpost Firewall Pro blokuje reklamy bazując na słowach kluczowych znalezionych w reklamach internetowych, zlokalizowanych w "IMG SRC=" i "A HREF=" znaczników HTML. Jeśli baner zawiera jedno ze zdefiniowanych słów kluczowych, jest zastępowany tekstem [AD] lub przeźroczystym obrazem GIF, w rozmiarze reklamy. Aby otworzyć listę komponentów słów kluczowych, naciśnij **Ustawienia** > **Reklamy i strony WWW** > **Ustawienia**. Aby dodać słowo do listy zablokowanych, wprowadź je w pole tekstowe i naciśnij **Dodaj**. Słowo pojawi się na liście poniżej. Każda reklama zawierająca dodane słowo, nie będzie wyświetlana w przeglądarce internetowej. Słowa kluczowe można edytować oraz usuwać z listy. Możesz także importować oraz eksportować listę słów kluczowych używając odpowiednich przycisków.

Blokada poprzez rozmiar obrazka



Program Outpost Firewall Pro blokuje obrazki reklam bazując na ich rozmiarze zdefiniowanym w znaczniku HTML "A". Jeśli rozmiar banera pasuje do rozmiaru na liście, będzie zastępowany tekstem

"[AD]" lub przeźroczystym obrazem GIF, w rozmiarze reklamy. Domyślnie, standardowe rozmiary obrazków reklamowych znajdują się na liście. Aby zablokować baner o innym rozmiarze, naciśnij **Ustawienia** > **Reklamy i strony WWW**> **Ustawienia**, wybierz zakładkę **Poprzez rozmiar** i zdefiniuj długość i szerokość banera w odpowiednich polach a następnie naciśnij **Dodaj**. Zdefiniowany rozmiar pojawi się na liście poniżej. Każda reklama posiadająca rozmiar zdefiniowany na liście, nie będzie wyświetlana w przeglądarce internetowej. Rozmiary można edytować oraz usuwać z listy. Aby przywrócić domyślną zawartość listy, naciśnij przycisk **Domyślny**.

Blokada poprzez ImproveNet
Ta funkcja opiera się na tych samych zasadach co blokowanie reklam poprzez słowa kluczowe, z tą różnicą, że słowa kluczowe są współdzielone przez użytkowników programu Outpost Firewall Pro. Lista słów kluczowych jest automatycznie dostarczana wraz z aktualizacją programu. Możesz także wspomóc program ImproveNet, zgłaszając niepożądane słowo. Aby to zrobić, naciśnij link **Zgłoś niepożądane słowo**. Blokada poprzez ImproveNet jest funkcją opcjonalną, dlatego jeśli nie chcesz z niej korzystać możesz ją wyłączyć poprzez odznaczenie pola **Użyj listy słów kluczowych ImproveNet** w zakładce **Poprzez ImproveNet**.

Uwaga:
Banery reklamowe są blokowane zgodnie ze zdefiniowanymi ustawieniami. Dlatego, niektóre pożądane obrazki mogą być blokowane jeśli ustawienia są zbyt restrykcyjne, na przykład dodawanie słowa "obraz" do listy słów kluczowych. Z kolei, niektóre reklamy mogą nie być blokowane jeśli używane są ustawienia domyślne.

10.3. Wyłączenia

Jeśli masz problem z wyświetlaniem niektórych stron WWW ponieważ większość obrazków na stronie jest zablokowana, możesz dodać takie strony do listy wyłączeń, ustawiając poziom elementów aktywnej zawartości oraz reklam osobno dla każdej strony. Naciśnij **Ustawienia** > **Kontrola stron WWW** > **Wyłączenia** a następnie **Dodaj**, aby zdefiniować adres strony. Zaznacz pole **Zezwól na zawartość oraz reklamy na tej stronie,** aby strona była całkowicie zaufana. Możesz także zdefiniować indywidualne ustawienia zaznaczając pole **Zmień ustawienia dla tej strony**. W drugim przypadku, po naciśnięciu przycisku **Dodaj,** pojawi się okno **Edytuj właściwości**, które pozwoli na zmianę ustawień aktywnej zawartości oraz reklam. Strona WWW, która została dodana, posiada domyślne ustawienia aktywnej zawartości i reklam. Ustawienia są takie same jak globalne ustawienia dla wszystkich sieci. Jedyną różnicą jest możliwość zaznaczenia **Użyj globalnych ustawień** (dla aktywnych elementów — zamiast czynności **Zapytaj**). Ustawienia, globalnych wartości są wyświetlane w kolorze szarym; ustawienia z unikalnymi wartościami są wyświetlane w kolorze niebieskim. Dokonaj wyboru (naciśnij przycisk **Przywróć domyślne** jeśli chcesz używać globalnych ustawień), i naciśnij **OK** aby zapisać zmiany. W dowolnym momencie możesz edytować ustawienia aktywnej zawartości stron i reklam wybierając stronę z listy i naciskając **Właściwości**.

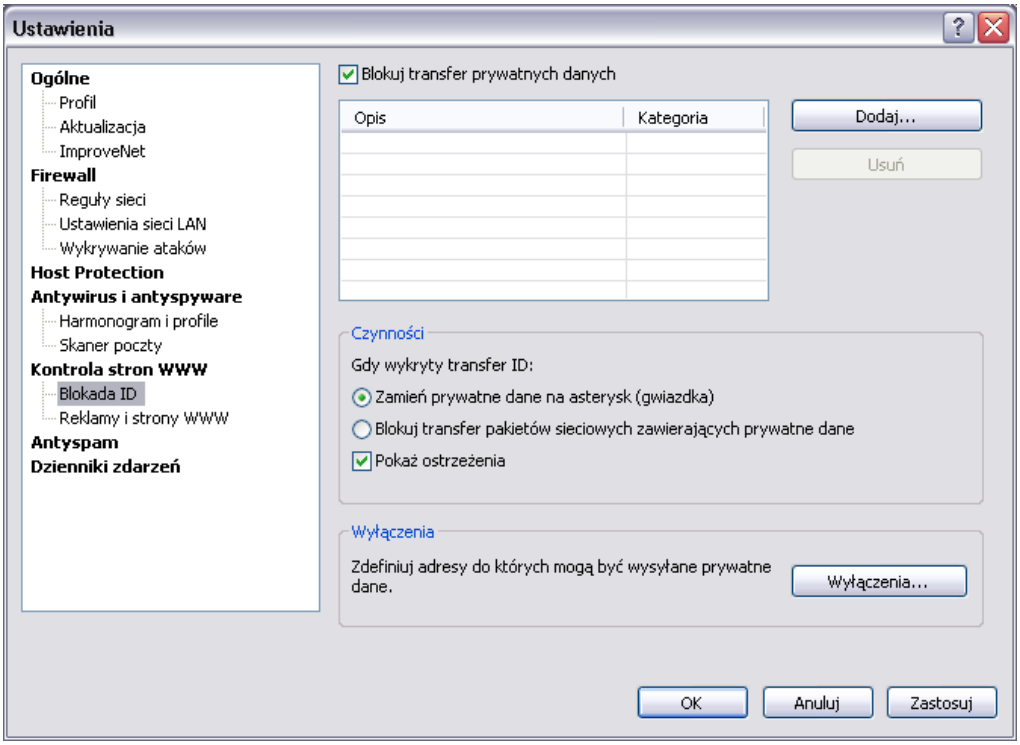
10.4. Czarna lista

Wiele stron WWW zawiera zagrożenie typu spyware. Baza danych programu Outpost Firewall Pro zawiera listę takich stron, których odwiedzanie nie jest zalecane. Próba połączenia z taką stroną lub wysyłanie danych jest automatycznie blokowane.
Pełna lista takich stron jest niewidzialna dla użytkownika. W przypadku wykrycia próby połączenia z jedną z takich stron, program dodaje je do listy widzialnej, która jest dostępna po wejściu w **Ustawienia**> **Reklamy i strony WWW**, a następnie naciśnięciu przycisku **Ustawienia** w oknie **Czarna lista stron WWW**. Jeśli na liście znajduje się strona, która uważasz za zaufaną, możesz zezwolić na dostęp do niej poprzez odznaczenie odpowiedniego pola.

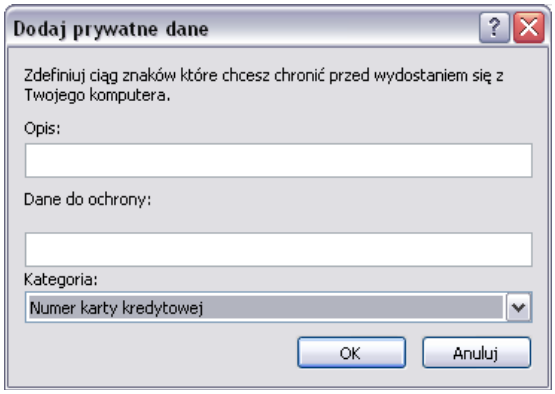
Jeśli chcesz, aby program wyświetlał ostrzeżenie o zablokowaniu strony, zaznacz pole **Pokaż ostrzeżenia**.

10.5. Blokowanie przesyłania prywatnych danych

Umożliwia zdefiniowanie prywatnych danych, które nigdy nie zostaną wysłane z komputera za pomocą przeglądarki internetowej, klienta pocztowego i innych programów. Pozwala to na ochronę przed zagrożeniami, które wykradają informacje takie jak numery kart kredytowych, hasła i inne prywatne dane. Aby chronić prywatne dane należy, należy wybrać **Blokada ID** w oknie **Ustawienia** i zaznaczyć pole **Blokuj transfer prywatnych danych**:



Naciśnij **Dodaj**, w oknie **Dodaj prywatne dane** zdefiniuj następujące parametry:



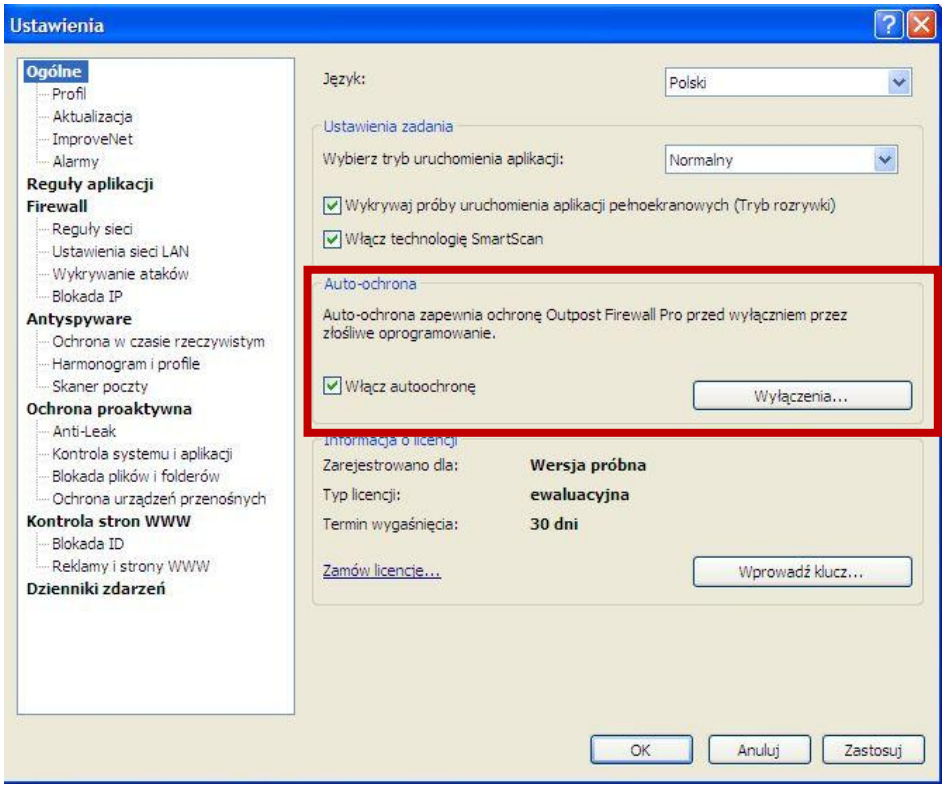
- **Opis** - opis, który będziesz mógł rozpoznać później, aby zidentyfikować ciąg.
- **Dane do ochrony** - kombinacja symboli, liter lub cyfr, które nie chcesz, aby przedostały się do sieci.
- **Kategoria** - kategoria, do której Twoje dane należą.

Po naciśnięciu **OK** i zatwierdzeniu zmian, transfer z komputera zdefiniowanego ciągu będzie blokowany. Po wykryciu przesyłania prywatnych danych, program Outpost Firewall Pro może **Zamieniać prywatne dane na asterysk (gwiazdkę)** lub **Blokować transfer pakietów sieciowych zawierających prywatne dane**. W pierwszym przypadku, każde żądające źródło otrzyma jedynie asteryski w miejscu danych, w drugim przypadku, każda próba źródła żądającego dane będzie całkowicie blokowana. W celu wyświetlania ostrzeżeń przy każdej próbie transferu zdefiniowanych danych z komputera, zaznacz pole **Pokaż ostrzeżenia**.
Jeśli jesteś pewien, że niektóre hosty są zaufane, możesz dodać je do listy wyłączeń naciskając przycisk **Wyłączenia**. Zdefiniuj potrzebne pola, a następnie naciśnij **Dodaj** i **OK, aby** zachować zmiany.

11. Ochrona wewnętrznych komponentów

Wewnętrzne komponenty programu coraz częściej stają się celem ataków hakerów, którzy próbują je wyłączyć przy użyciu rootkitów oraz innych zaawansowanych narzędzi. Aby przeciwstawić się temu zagrożeniu, program Outpost Firewall Pro jest wyposażony w autoochronę. Gdy autoochrona jest włączona, program Outpost Firewall Pro chroni sam siebie przed wirusami, trojanami lub spyware. Także próby symulacji naciskania klawiszy klawiatury, które mogłyby doprowadzić do wyłączenia firewalla są blokowane. Program Outpost Firewall Pro stale monitoruje swoje wewnętrzne komponenty na dysku twardym, we wpisach rejestru, w pamięci, procesach itd. nie zezwalając na jakiekolwiek zmiany.

Domyślnie, autoochrona jest włączona a dostęp do komponentów jest zabroniony dla wszystkich aplikacji. Jeśli uważasz, że niektóre aplikacje mogą uzyskać dostęp do komponentów programu Outpost Firewall Pro oraz kluczy rejestru, możesz dodać takie aplikacje do listy wyłączeń naciskając **Ustawienia** > **Wyłączenia**. Aby wyłączyć autoochronę, naciśnij **Ustawienia** i odznacz pole **Włącz autoochronę,** lub naciśnij prawym przyciskiem myszy na ikonę programu w zasobniku systemowym a następnie wybierz **Wyłącz autoochronę:**

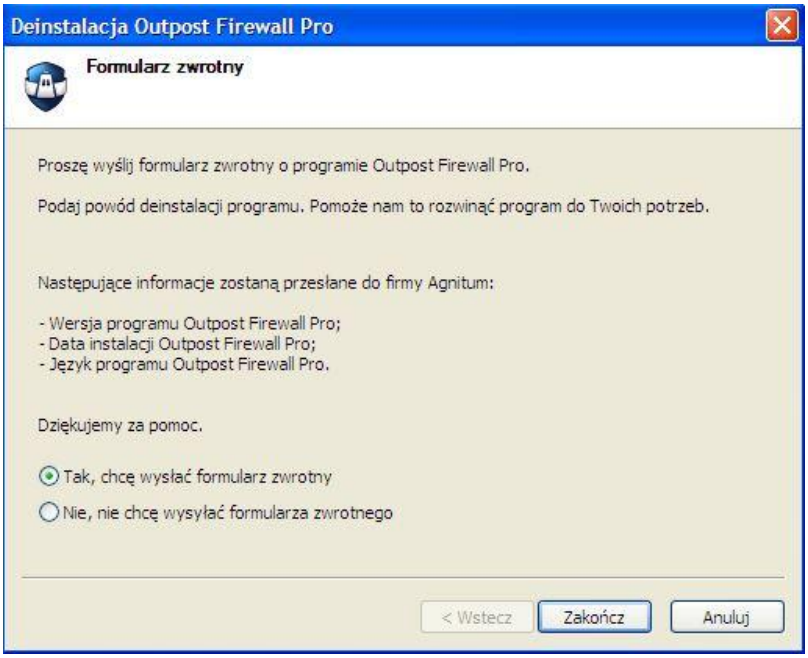


Uwaga:
Wyłączenie autoochrony może wpłynąć na poziom ochrony Twojego systemu. Pomimo że wyłączenie jej jest wymagane przy instalacji komponentów i innych zaawansowanych funkcji, po wprowadzonych zmianach autoochrona powinna zostać włączona.

12. Deinstalacja programu

Aby odinstalować program Outpost Firewall Pro należy:

1. Nacisnąć prawym klawiszem myszy na ikonę programu Outpost Firewall Pro w zasobniku systemowym i wybrać **Wyjście**.
2. Nacisnąć **Start** na pasku narzędzi Windows i wybrać **Panel sterowania** > **Dodaj lub usuń programy**.
3. Wybrać Agnitum **Outpost Firewall Pro** i nacisnąć **Usuń**.
4. Nacisnąć **Tak** w celu potwierdzenia usunięcia programu.
   Program zapyta o wysłanie formularza zwrotnego, abyś mógł sprecyzować powód jego usunięcia. To pomoże programistom dostosować do Twoich potrzeb następne wersje programu.



Uwaga:
Aby uniknąć problemów, uruchom ponownie komputer po zakończeniu procesu deinstalacji.

13. Dodatek

Ten dodatek zawiera kilka technicznych zagadnień, które mogą być pomocne dla użytkowników zaawansowanych w celu lepszego zrozumienia działania programu Outpost Firewall Pro.

13.1. Rozwiązywanie problemów

Jeśli potrzebujesz wsparcia podczas pracy z programem Outpost Firewall Pro, skontaktuj się z dystrybutorem oprogramowania mailowo (pomoc@dagma.pl) lub odwiedź stronę producenta

http://www.agnitum.com/support/index.php. Na stronie znajduje się baza wiedzy, dokumentacje, forum wsparcia oraz bezpośredni kontakt z pomocą techniczną.

13.2. Opcje kontroli legalności procesów

Dodawanie komponentów
System operacyjny Windows domyślnie włącza instalowanie haków, dzięki którym różne kody mogą zostać dodane do innych procesów. Zazwyczaj haki wykorzystywane są do wykonywania zwykłych, zaufanych czynności, np. przełączania układu klawiatury lub uruchamiania pliku PDF w przeglądarce internetowej. Jednakże mogą być również wykorzystywane przez złośliwe programy. Technikę nielegalnego wykorzystywania haków można sprawdzić, korzystając z testu wycieku (leak test) PC Audit (http://www.pcinternetpatrol.com/). Haki są często wykorzystywane przez złośliwe procesy (trojany, spyware'y, wirusy, robaki, itd.), które dołączają swój kod do legalnych procesów (np. Internet Explorer,Firefox). Program Outpost Firewall Pro kontroluje instalację haków (hook interceptor) w przestrzeni adresowej procesu, zabezpieczając w ten sposób przed złośliwymi programami.

Kontrola nad innym programem
Technologia DDE jest używana do kontrolowania programów. Większość przeglądarek to serwery DDE, które mogą być wykorzystywane przez złośliwe programy do przesyłania prywatnych informacji. Technikę wykorzystywania serwerów DDE, to nielegalnych działań można sprawdzić korzystając z testu wycieku (leak test) Surfer (http://www.firewallleak tester.com/leak test15.htm) oraz ZABypass. Program Outpost Firewall Pro monitoruje każdą próbę użycia komunikacji wewnętrznej DDE, bez względu na to czy proces jest uruchomiony czy nie. Monitorowanie komunikacji wewnętrznej DDE pozwala programowi na kontrolę metod używanych przez programy do przejęcia kontroli nad zaufanym procesem. Zapobiega przechwyceniu zaufanego programu przez złośliwy program i sprawdza czy komunikacja wewnętrzna DDE jest zezwolona podczas dostępu programu do sieci. W przypadku wykrycia próby następuje sprawdzenie legalności.

Kontrola okna programu
System Windows pozwala programom na wymianę informacji pomiędzy oknami programów. Złośliwe procesy mogą przejąć kontrolę nad programami korzystającymi z dostępu do sieci wysyłając informacje imitujące działania użytkownika. Technikę można sprawdzić korzystając z testu wycieku Breakout (http://www.firewallleak tester.com/leak test16.htm). Technika jest czasami używana przez zaufane procesy jak również przez złośliwe kody. Program Outpost Firewall Pro kontroluje takie próby.

Żądanie DNS
Usługa DNS Client zawiera potencjalną lukę zwaną tunelowanie DNS. Technikę można sprawdzić korzystając z testu wycieku DNSTester (http://www.klake.org/~jt/dnshell/). Program wykonuje podwójne sprawdzenie dostępu do usługi DNS Client. Kontroluje dostęp do DNS API nawet jeżeli usługa DNS Client jest uruchomiona pozwalając nadawać uprawnienia wybranym procesom korzystanie z usługi DNS Client.

Program uruchamiany z URL
Złośliwe procesy mogą uruchamiać w ukrytym oknie domyślną przeglądarkę z ustawionym adresem WWW, powodując, że firewall uważa, że wykonywana jest zaufana czynność. Firewalle mogą ufać programowi bez potrzeby sprawdzania co rzeczywiście uruchomił program po raz pierwszy i jakie zostały użyte dodatkowe parametry połączenia powodujące niemożność zablokowania techniki, co w konsekwencji może spowodować przesłanie poufnych danych. Przykładem użycia tej techniki są leaktesty Tooleaky, Ghost i Wallbreaker (http://www.firewallleak tester.com/leak test2.htm, http://www.firewallleak tester.com/leak test13.htm, http://www.firewallleak tester.com/leak test11.htm). Program Outpost Firewall Pro sprawdza każdy uruchomiony program i kontroluje uprawnienia do uruchomienia programu z URL oraz wyświetla ostrzeżenie czy zezwolić na taką czynność czy nie dla wybranego programu.

Kontrola programu OLE
Relatywnie nowa technika kontrolowania aktywności programów poprzez mechanizm OLE (skrót od komendy Object Linking and Embedding) - mechanizm systemu Windows pozwalający jednemu programowi na zarządzanie zachowaniem drugiego programu. Mechanizm systemu Windows używa techniki OLE do komunikacji i wymiany danych pomiędzy programami, np. zarządzanie działaniem programu Internet Explorer tak aby wysyłał dane użytkownika do zdalnego komputera. Przykładem użycia tej techniki są leaktesty PCFlank (http://www.pcflank.com/PCFlankleak test.exe). Program Outpost Firewall Pro wykrywa komunikację OLE i wyświetla ostrzeżenie czy jest to zwykłe działanie programu przejmującego kontrolę nad czynnością innego programu.

Zmiany pamięci procesu
Wiele koni trojańskich i wirusów wykorzystuje zaawansowane techniki do podszywania się pod zaufane programy pracujące w pamięci, aby ominąć zabezpieczenia i wykonać złośliwe czynności. Technikę można sprawdzić korzystając z testu wycieku Thermite i Copycat (http://www.firewallleak tester.com/leak test8.htm,http://www.firewallleak tester.com/leak test9.htm). Program Outpost Firewall Pro pozwala na kontrolę funkcji, które mogą być używane do wpisania złośliwego kodu do przestrzeni pamięci zaufanego programu. Cała przestrzeń pamięci używana przez aktywny program jest analizowana przez program Outpost Firewall Pro (nie tylko przez program korzystający z dostępu do sieci. Jeżeli złośliwy program będzie próbował zmienić pamięć zaufanego programu, Outpost Firewall Pro wykryje takie działanie i wyświetli ostrzeżenie. System pracuje proaktywnie: pozwala na zezwolenie lub zablokowanie zmiany pamięci innych procesów na poziomie programu. Na przykład, program Visual Studio 2005 może zmieniać pamięć, podczas gdy leaktest "copycat.exe" nie. Funkcja chroni również przez "nieznanymi" zagrożeniami niewykrywalnymi przez programy antywirusowe i antyspyware'owe.

Niskopoziomowy dostęp do sieci
Niektóre sterowniki sieciowe pozwalają na bezpośredni dostęp do karty sieciowej omijając standardowy stos TCP. Sterowniki mogą być wykorzystywane przez złośliwe programy do uzyskania niskopoziomowego dostępu do sieci i powodować dodatkowe zagrożenie dla systemu, ponieważ ruch sieciowy nie będzie monitorowany przez firewalla. Przykładem użycia tej techniki jest leaktest MBtest (http://www.firewallleaktester.com/leak test10.htm). Program Outpost Firewall Pro pozwala kontrolować programy żądające dostępu do sieci, omijające starndardowe metody. Funkcja zwiększa poziom bezpieczeństwa chroniąc przed wyciekiem danych. Użytkownik ma możliwość kontrolować próby programu uzyskania dostępu do otwartych sterowników sieciowych, tzn. bez zgody użytkownika, program nie może wysyłać nawet danych ARP lub IPX.

Ładowanie sterowników
Programy pracujące w profilu administratora mogą instalować sterowniki w trybie kernel-mode, aby uzyskać całkowity i nieograniczony dostęp do systemu. Przykładem użycia tej techniki są rootkity. Program Outpost Firewall Pro kontroluje próby instalacji sterowników oraz sprawdza każdy z plików sterownika na obecność zagrożeń przed załadowaniem do pamięci.

13.3. Korzystanie z makro adresów

Program Outpost Firewall Pro pozwala zdefiniować makro adresy w opisie reguły, aby ułatwić tworzenie reguł. Podczas tworzenia reguł dla połączeń intranetowych lub innych usług systemu Windows (np. DNS) zamiast ręcznego wprowadzania adresów IP można skorzystać z proponowanych definicji makro adresów, które są używane, np. do przydzielania wszystkich lokalnych adresów sieciowych jako LOCAL_NETWORK lub wszystkich adresów DNS jako DNS_SERVERS. Program Outpost Firewall Pro automatycznie rozpoznaje bieżącą wartość makro bez potrzeby zmiany w przypadku zmian ustawień karty sieciowej. Na przykład, mobilni użytkownicy zawsze będą chronieni bez względu do jakiej sieci są podłączeni. Po zdefiniowaniu lokalnego lub zdalnego adresu, istnieje możliwość wybrania jednego z następujących makro adresów:

- **DNS_SERVERS -** definiuje adresy wszystkich serwerów DNS w sieci lokalnej.

- **LOCAL_NETWORK -** definiuje adresy wszystkich lokalnych sieci i adresy rozgłoszeniowe dostępne dla komputera.
- **WINS_SERVERS -** definiuje adresy wszystkich serwerów WINS w sieci lokalnej.
- **GATEWAYS -** definiuje adresy wszystkich bramek w sieci lokalnej.
- **MY_COMPUTER -** definiuje wszystkie adresy IP komputera znajdującego się w różnych sieciach lokalnych oraz adresy loopback.
- **ALL_COMPUTER_ADDRESSES -** definiuje wszystkie adresy IP komputera znajdującego się w różnych sieciach lokalnych oraz adresy rozgłoszeniowy i multicastowy.
- **BROADCAST_ADDRESSES -** definuje adresy rozgłoszeniowe dostępne dla komputera. Adres rozgłoszeniowy jest adresem IP, który pozwala wysyłać informacje do wszystkich komputerów dostępnych w podsieci, a nie do wybranego komputera.
- **MULTICAST_ADDRESSES -** definiuje adresy multicastowe. Adres multicastowy jest pojedynczym adresem, który odwołuje do wielu kart sieciowych. Adres multicastowy jest synonimem grupy adresów.