McAfee®

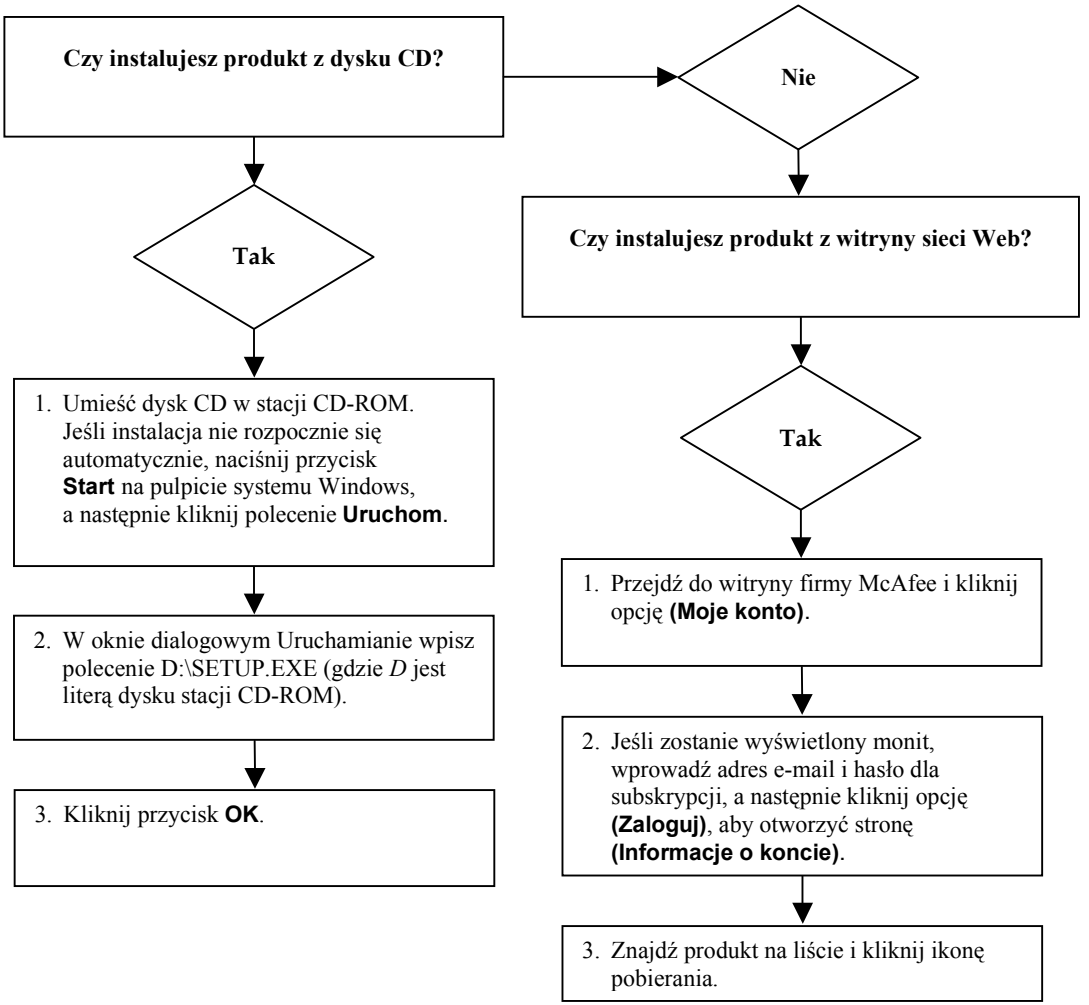
personalfirewallplus

Podręcznik użytkownika

McAfee®

Karta Szybki start

Wydrukowanie tej wygodnej w użyciu strony pomocy może przydać się podczas instalacji produktu z dysku CD lub witryny sieci Web.



Więcej informacji

Do przeglądania podręczników użytkownika zamieszczonych na dysku CD produktu wymagane jest zainstalowanie programu Acrobat Reader. Jeśli program ten nie został zainstalowany, należy zainstalować go teraz z dysku CD produktu firmy McAfee.

1. Włóż dysk CD produktu do stacji dysków CD-ROM.
2. Otwórz Eksploratora Windows: Na pulpicie systemu Windows kliknij przycisk **Start**, a następnie kliknij polecenie **Wyszukaj**.
3. Znajdź folder Manuals i kliknij dwukrotnie plik PDF podręcznika użytkownika, który chcesz otworzyć.

Korzyści z rejestracji

Firma McAfee zaleca wykonanie prostej procedury (dostępnej w produkcie) w celu wysyłania rejestracji bezpośrednio do naszej firmy. Rejestracja zapewnia otrzymanie na czas odpowiedniej pomocy technicznej oraz następujące korzyści:

- BEZPŁATNA elektroniczna pomoc techniczna
- Aktualizacje pliku definicji wirusów (DAT) przez jeden rok po zainstalowaniu zakupionego oprogramowania VirusScan

  Cennik oferty dodatkowego roku pobierania sygnatur wirusów znajduje się w witrynie http://www.mcafee.com/.
- 60-dniowa gwarancja wymiany dysku CD z oprogramowaniem w przypadku wystąpienia uszkodzeń lub błędów
- Aktualizacje filtru SpamKiller przez jeden rok po zainstalowaniu zakupionego oprogramowania SpamKiller

  Cennik oferty dodatkowego roku aktualizacji filtru znajduje się w witrynie http://www.mcafee.com/.
- Aktualizacje zakupionego oprogramowania McAfee Internet Security Suite przez jeden rok po jego zainstalowaniu

  Cennik oferty dodatkowego roku aktualizacji treści znajduje się w witrynie http://www.mcafee.com/.

Pomoc techniczna

Aby uzyskać pomoc techniczną, należy odwiedzić witrynę

http://www.mcafeehelp.com/.

W tej witrynie przez całą dobę dostępny jest łatwy w użyciu kreator odpowiedzi umożliwiający rozwiązanie najczęściej spotykanych problemów.

Doświadczeni użytkownicy mogą także korzystać z opcji zaawansowanych, takich jak drzewo pomocy lub wyszukiwanie według słów kluczowych. Jeśli rozwiązanie nie zostanie znalezione, użytkownik może skorzystać z BEZPŁATNYCH funkcji Chat Now! i E-mail Express! firmy McAfee. Korzystając z tych narzędzi, można szybko i bezpłatnie skontaktować się przez Internet z wykwalifikowanymi pracownikami pomocy technicznej. W przeciwnym wypadku informacje na temat telefonicznej pomocy technicznej można uzyskać w witrynie

http://www.mcafeehelp.com/.

Spis treści

Karta Szybki start iii

1 Wprowadzenie 7

Nowe funkcje 7
Wymagania systemowe 9
Odinstalowywanie zapór innych firm 9
Ustawianie domyślnej zapory 10
Ustawianie poziomu zabezpieczeń 10
Testowanie programu McAfee Personal Firewall Plus 12
Korzystanie z programu McAfee SecurityCenter 13

2 Korzystanie z programu McAfee Personal Firewall Plus 15

Informacje o stronie Podsumowanie 15
Informacje o stronie Aplikacje internetowe 21
Zmiana reguł aplikacji 22
Przyznawanie dostępu i blokowanie aplikacji internetowych 22
Informacje o stronie Zdarzenia przychodzące 23
Omówienie zdarzeń 24
Wyświetlanie zdarzeń w dzienniku zdarzeń przychodzących 26
Reagowanie na zdarzenia przychodzące 28
Zarządzanie dziennikiem zdarzeń przychodzących 32
Informacje o alertach 34
Alerty czerwone 34
Alerty zielone 40
Alerty niebieskie 42

Skorowidz 43

Wprowadzenie 1

McAfee Personal Firewall Plus - zapraszamy!

Oprogramowanie McAfee Personal Firewall Plus zapewnia zaawansowaną ochronę komputera oraz osobistych informacji użytkownika. Program Personal Firewall tworzy barierę między komputerem a Internetem, dyskretnie monitorując ruch internetowy w poszukiwaniu podejrzanych działań.

Funkcje programu:

- Broni przed potencjalnymi sondowaniami i atakami hakerów.
- Uzupełnia ochronę antywirusową.
- Monitoruje aktywność internetową i sieciową.
- Wyświetla alerty o potencjalnie wrogich zdarzeniach.
- Dostarcza szczegółowych informacji na temat podejrzanego ruchu internetowego.
- Integruje funkcje witryny Hackerwatch.org łącznie z raportowaniem zdarzeń, narzędziami do samotestowania oraz możliwością przesyłania pocztą e-mail zgłoszonych zdarzeń do innych ekspertów online.
- Zawiera funkcje szczegółowego śledzenia oraz badania zdarzeń.

Nowe funkcje

- **Udoskonalona obsługa gier**
  Program McAfee Personal Firewall Plus chroni komputer przed próbami włamań i podejrzanymi działaniami podczas pełnoekranowej sesji gry, ale może ukrywać alerty w razie ich wykrycia. Alerty czerwone pojawią się po wyjściu z gry.
- **Udoskonalone zarządzanie dostępem**
  Program McAfee Personal Firewall Plus umożliwia użytkownikom dynamiczne przyznawanie aplikacjom tymczasowego dostępu do Internetu. Dostęp jest ograniczony do czasu między uruchomieniem aplikacji a jej zamknięciem. Gdy produkt Personal Firewall wykryje nieznany program próbujący komunikować się z Internetem, czerwony alert umożliwia przyznanie tej aplikacji tymczasowego dostępu do sieci.

- **Ulepszone sterowanie zabezpieczeniami**
  Funkcja blokowania dostępna w programie McAfee Personal Firewall Plus umożliwia natychmiastowe zablokowanie całego przychodzącego i wychodzącego ruchu sieciowego między komputerem a Internetem. Użytkownicy mogą włączać i wyłączać funkcję blokowania z trzech miejsc w programie.

- **Udoskonalona obsługa sytuacji awaryjnych**
  Za pomocą polecenia Resetuj ustawienia można automatycznie przywrócić ustawienia domyślne. Jeśli program Personal Firewall będzie działać w sposób niepożądany, którego użytkownik nie będzie mógł poprawić, może on przywrócić domyślne ustawienia produktu.

- **Ochrona połączeń z Internetem**
  Aby zapobiec przypadkowemu zablokowaniu połączeń z Internetem przez użytkownika, opcja zabraniania dostępu z adresu internetowego jest wyłączona z alertu niebieskiego, jeśli program Personal Firewall wykryje, że źródłem przychodzącego ruchu sieciowego może być serwer DHCP lub DNS. Jeśli ruch przychodzący nie pochodzi z serwera DHCP lub DNS, opcja pojawi się na alercie.

- **Ulepszona integracja z witryną HackerWatch.org**
  Raportowanie o potencjalnych hakerach jest prostsze niż kiedykolwiek. Program McAfee Personal Firewall Plus poszerza funkcjonalność witryny HackerWatch.org, umożliwiając między innymi wysyłanie do bazy danych informacji o podejrzanych zdarzeniach.

- **Rozszerzona inteligentna obsługa aplikacji**
  Gdy aplikacja próbuje uzyskać dostęp do Internetu, program Personal Firewall sprawdza najpierw, czy aplikacja ta jest uważana za zaufaną czy szkodliwą. Jeśli zostanie rozpoznana jako zaufana, program Personal Firewall automatycznie zezwoli jej na dostęp do Internetu bez konieczności podejmowania działań przez użytkownika.

- **Zaawansowane wykrywanie koni trojańskich**
  Program McAfee Personal Firewall Plus łączy zarządzanie połączeniami aplikacji z ulepszoną bazą danych. Umożliwia to wykrycie i zablokowanie dostępu do Internetu większej liczby potencjalnie szkodliwych aplikacji, takich jak konie trojańskie, mogących przekazywać dane osobiste.

- **Udoskonalone śledzenie wizualne**
  Zawiera ono przejrzyste mapy graficzne pokazujące źródło ataków i przepływ danych na całym świecie, w tym szczegółowe informacje kontaktowe/informacje o właścicielu pochodzące z jego adresu IP.

- **Większa prostota używania**
  Program McAfee Personal Firewall Plus udostępnia Asystenta konfiguracji i Samouczek użytkownika prowadzące przez proces konfiguracji i korzystania z zapory. Pomimo, że produkt został zaprojektowany do działania bez jakiejkolwiek interwencji, firma McAfee dostarcza użytkownikom bogate zasoby pozwalające zrozumieć i docenić zalety działania zapory.

- **Ulepszony system wykrywania włamań**
  System wykrywania włamań (IDS, Intrusion Detection System) programu Personal Firewall wykrywa typowe wzorce ataków oraz inne podejrzane działania. Monitoruje on każdy przychodzący pakiet danych w poszukiwaniu podejrzanych transferów danych lub metod przesyłania oraz rejestruje je w dzienniku zdarzeń.

- **Ulepszona analiza ruchu**
  Program McAfee Personal Firewall Plus umożliwia użytkownikom wgląd zarówno w dane przychodzące, jak i wychodzące z ich komputerów. Pokazuje też połączenia aplikacji oraz programy, które aktywnie „nasłuchują" w oczekiwaniu na otwarcie połączeń. Umożliwia to użytkownikom zauważenie i podjęcie działań w stosunku do aplikacji, które mogą być narażone na włamania.

Wymagania systemowe

- Microsoft® Windows 98, Windows Me, Windows 2000 lub Windows XP
- Komputer z procesorem zgodnym z Pentium
  Windows 98, 2000: 133 MHz lub szybszy
  Windows Me: 150 MHz lub szybszy
  Windows XP (Home/Professional): 300 MHz lub szybszy
- Pamięć RAM
  Windows 98, Me, 2000: 64 MB
  Windows XP (Home/Professional): 128 MB
- 40 MB wolnego miejsca na dysku twardym
- Przeglądarka Microsoft® Internet Explorer w wersji 5.5 lub nowszej

UWAGA
Najnowszą wersję przeglądarki Internet Explorer można pobrać z witryny firmy Microsoft http://www.microsoft.com/worldwide.

Odinstalowywanie zapór innych firm

Przed rozpoczęciem instalacji oprogramowania McAfee Personal Firewall Plus na komputerze, należy odinstalować inne zapory. W tym celu należy postępować zgodnie z instrukcją odinstalowania tych programów.

UWAGA
W przypadku korzystania z systemu Windows XP nie jest konieczne wyłączenie wbudowanej zapory przed zainstalowaniem oprogramowania McAfee Personal Firewall Plus. Jednakże jest to zalecane. Pozostawienie włączonej wbudowanej zapory uniemożliwi rejestrowanie zdarzeń przychodzących w dzienniku zdarzeń przychodzących programu McAfee Personal Firewall Plus.

Ustawianie domyślnej zapory

Program McAfee Personal Firewall może zarządzać uprawnieniami i ruchem aplikacji internetowych na komputerze, nawet jeśli wykryje uruchomioną zaporę systemu Windows.

Po zainstalowaniu program McAfee Personal Firewall automatycznie wyłącza Zaporę systemu Windows i ustawia się jako zapora domyślna. Od tej chwili użytkownik korzysta tylko z funkcji i komunikatów programu McAfee Personal Firewall. Jeśli następnie użytkownik włączy Zaporę systemu Windows za pomocą Centrum zabezpieczeń systemu Windows lub Panelu sterowania, pozwalając na działanie na komputerze obu zapór, może to doprowadzić do częściowej utraty rejestrowanych danych przez program McAfee Personal Firewall, a także do powielania się komunikatów o stanie i alertów.

UWAGA

Jeśli włączone są obie zapory, program McAfee Personal Firewall nie pokazuje na karcie Zdarzenia przychodzące wszystkich zablokowanych adresów IP. Zapora systemu Windows przechwytuje i blokuje większość z tych zdarzeń, uniemożliwiając ich wykrycie i rejestrowanie przez program McAfee Personal Firewall. Program McAfee Personal Firewall może jednakże blokować dodatkowy ruch w oparciu o inne czynniki bezpieczeństwa i taki ruch będzie rejestrowany.

Rejestrowanie jest domyślnie wyłączone w Zaporze systemu Windows, ale jeśli użytkownik wybierze włączenie obu zapór, może również włączyć rejestrowanie w Zaporze systemu Windows. Domyślnym plikiem dziennika Zapory systemu Windows jest plik C:\Windows\pfirewall.log.

Aby być pewnym, że komputer jest chroniony przez co najmniej jedną zaporę, Zapora systemu Windows jest automatycznie włączana ponownie po odinstalowaniu programu McAfee Personal Firewall.

Jeśli użytkownik wyłączy program McAfee Personal Firewall lub ustawi ustawienie zabezpieczeń na poziomie **Otwarty** bez ręcznego włączenia Zapory systemu Windows, komputer zostanie pozbawiony całej ochrony z wyjątkiem wcześniej zablokowanych aplikacji.

Ustawianie poziomu zabezpieczeń

Istnieje możliwość skonfigurowania opcji zabezpieczeń określających sposób reagowania programu Personal Firewall w momencie wykrycia niepożądanego ruchu. Domyślnie włączony jest **Standardowy** poziom zabezpieczeń. W przypadku **Standardowego** poziomu zabezpieczeń zezwolenie aplikacji na dostęp do Internetu przydziela jej pełny dostęp. Pełny dostęp umożliwia aplikacji zarówno wysyłanie danych, jak również pozwala na odbieranie niepożądanych danych poprzez porty niesystemowe.

Aby skonfigurować ustawienia zabezpieczeń:

1 Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Opcje**.

2 Kliknij ikonę **Ustawienia zabezpieczeń**.

3 Ustaw poziom zabezpieczeń przesuwając suwak na żądany poziom.

Możliwe jest ustawienie w zakresie od poziomu Blokowanie do poziomu Otwarty.

- **Blokowanie -** Wszystkie połączenia komputera z Internetem są zamknięte. Ustawienie to można wykorzystać do zablokowania portów skonfigurowanych jako otwarte na stronie Usługi systemowe.
- **Wyższy poziom zabezpieczeń -** Gdy aplikacja żąda określonego typu dostępu do Internetu (na przykład dostępu tylko dla połączeń wychodzących), użytkownik może zezwolić lub zabronić aplikacji na takie połączenie. Później, jeśli aplikacja zażąda pełnego dostępu można go jej przyznać lub ograniczyć tylko dla połączeń wychodzących.
- **Zabezpieczenia standardowe (zalecane) -** Gdy aplikacja zażąda i uzyska dostęp do Internetu, to uzyska dostęp pełny umożliwiający obsługę ruchu przychodzącego i wychodzącego.
- **Zabezpieczenia zaufania -** Przy pierwszej próbie uzyskania dostępu do Internetu wszystkie aplikacje są automatycznie traktowane jako zaufane. Można jednakże skonfigurować program Personal Firewall do korzystania z alertów w celu powiadamiania użytkownika o nowych aplikacjach w komputerze. Ustawienie to można wykorzystać w przypadku, gdy nie działają niektóre gry lub multimedia strumieniowe.
- **Otwarty -** Zapora jest wyłączona. Ustawienie to zezwala na przechodzenie całego ruchu internetowego przez program Personal Firewall bez filtrowania.

UWAGA
Zablokowane wcześniej aplikacje są dalej blokowane, kiedy zapora jest ustawiona w trybie zabezpieczeń **Otwarty** lub **Blokowanie**. Aby temu zapobiec, można zmienić uprawnienia aplikacji na **Zezwalaj na pełny dostęp** lub usunąć regułę **Zablokowane** z listy **Aplikacje internetowe**.

4 Wybierz dodatkowe ustawienia zabezpieczeń:

UWAGA
Jeśli na komputerze zainstalowany jest system operacyjny Windows XP i dodano kilku użytkowników systemu XP, opcje te będą dostępne wyłącznie po zalogowaniu jako administrator.

- **Rejestruj zdarzenia wykrywania włamań (IDS) w dzienniku zdarzeń przychodzących -** Po wybraniu tej opcji zdarzenia wykryte przez system IDS będą się pojawiały w dzienniku zdarzeń przychodzących. System wykrywania włamań wykrywa typowe rodzaje ataków oraz inne podejrzane działania. Funkcja wykrywania włamań monitoruje każdy przychodzący i wychodzący pakiet danych w poszukiwaniu podejrzanych transferów danych lub metod przesyłania. Są one porównywane z bazą „sygnatur" i pakiety pochodzące od atakującego komputera zostają automatycznie odrzucone.

  System IDS poszukuje określonych wzorców ruchu sieciowego wykorzystywanego przez włamywaczy. System IDS sprawdza każdy pakiet przychodzący do komputera w celu wykrycia ruchu charakterystycznego dla podejrzanych lub znanych ataków. Na przykład, jeżeli program Personal Firewall napotka pakiety ICMP, analizuje je w poszukiwaniu podejrzanych wzorców ruchu sieciowego przez porównanie ruchu ICMP z wzorcami znanych ataków.

- **Akceptuj żądania ICMP ping** - Ruch ICMP jest wykorzystywany głównie do śledzenia i wysyłania poleceń ping. Polecenie ping jest często używane do przeprowadzania szybkich testów przed próbą zainicjowania połączeń. Polecenie ping może być bardzo często wysyłane do komputera, na którym zainstalowano program typu P2P do udostępniania plików. Po wybraniu tej opcji program Personal Firewall będzie zezwalał na wszystkie żądania poleceń ping bez ich rejestrowania w dzienniku zdarzeń przychodzących. Jeśli opcja ta nie zostanie wybrana program Personal Firewall będzie blokował wszystkie żądania poleceń ping i będzie je rejestrował w dzienniku zdarzeń przychodzących.

- **Zezwalaj użytkownikom z ograniczeniami na zmianę ustawień programu Personal Firewall** - Jeżeli na komputerze zainstalowany jest system Windows XP lub Windows 2000 z wieloma użytkownikami, wybranie tej opcji pozwoli użytkownikom z ograniczeniami na modyfikowanie ustawień programu Personal Firewall.

5 Po zakończeniu wprowadzania zmian kliknij przycisk **OK**.

Testowanie programu McAfee Personal Firewall Plus

Istnieje możliwość przetestowania instalacji programu Personal Firewall pod kątem istnienia możliwych luk w zabezpieczeniach umożliwiających włamanie oraz podejrzane działanie.

Aby przetestować instalację programu Personal Firewall za pomocą ikony McAfee na pasku zadań:

- Kliknij prawym przyciskiem myszy ikonę programu McAfee  znajdującą się na pasku zadań systemu Windows, a następnie wybierz polecenie **Testuj zaporę**.

Program Personal Firewall otworzy przeglądarkę Internet Explorer i przejdzie do obsługiwanej przez firmę McAfee witryny http://www.HackerWatch.org/. Aby przetestować program Personal Firewall należy postępować zgodnie z poleceniami wyświetlanymi na stronie Probe (Sondowanie) witryny Hackerwatch.org.

Korzystanie z programu McAfee SecurityCenter

Program McAfee SecurityCenter pełni rolę centrum zabezpieczeń i jest dostępny za pomocą ikony znajdującej się na pasku zadań lub z pulpitu systemu Windows. Dzięki niemu możliwe jest wykonywanie następujących zadań:

- Uzyskanie darmowej analizy zabezpieczeń komputera.
- Uruchamianie, zarządzanie i konfiguracja za pomocą jednej ikony wszystkich subskrypcji produktów firmy McAfee.
- Przeglądanie stale aktualizowanych alertów o wirusach oraz najnowszych informacji o produkcie.
- Szybki dostęp do łączy do często zadawanych pytań oraz szczegółowych informacji o koncie w witrynie internetowej firmy McAfee.

> **UWAGA**
> Aby uzyskać więcej informacji na temat funkcji tego programu, należy kliknąć przycisk **Pomoc** w oknie dialogowym **SecurityCenter**.

Jeśli włączono wszystkie zainstalowane aplikacje firmy McAfee, po uruchomieniu programu SecurityCenter na pasku zadań systemu Windows (w obszarze powiadomień systemu Windows XP) zostanie wyświetlona czerwona ikona z literą M  . Jest to obszar zawierający zegar i znajdujący się zazwyczaj w prawym dolnym rogu pulpitu systemu Windows.

Jeśli chociaż jedna z zainstalowanych na komputerze aplikacji firmy McAfee zostanie wyłączona, ikona programu McAfee zmieni kolor na czarny  .

Aby uruchomić program McAfee SecurityCenter:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee  , a następnie wybierz polecenie **Otwórz program SecurityCenter**.

Aby uruchomić program Personal Firewall z poziomu aplikacji McAfee SecurityCenter:

1. W programie SecurityCenter kliknij kartę **Personal Firewall Plus**.
2. Z menu Działanie wybierz właściwe zadanie.

Aby uruchomić program Personal Firewall z poziomu systemu Windows:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee  znajdującą się na pasku zadań systemu Windows, a następnie wskaż pozycję **Personal Firewall**.
2. Wybierz zadanie.

Korzystanie z programu McAfee Personal Firewall Plus 2

Aby otworzyć program Personal Firewall:

- Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz zadanie.

Informacje o stronie Podsumowanie

Podsumowanie w programie Personal Firewall zawiera cztery strony podsumowania:

- Podsumowanie główne
- Podsumowanie aplikacji
- Podsumowanie zdarzeń
- Podsumowanie witryny HackerWatch

Na tych stronach podsumowania znajdują się różnorodne raporty na temat ostatnich zdarzeń przychodzących, stanu aplikacji oraz raporty witryny HackerWatch.org na temat ogólnoświatowej aktywności włamań. Znajdują się tu również łącza do typowych zadań wykonywanych w programie Personal Firewall.

Aby otworzyć stronę Podsumowanie główne w programie Personal Firewall:

- Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Wyświetl podsumowanie** (Rysunek 2-1).

Rysunek 2-1. Strona Podsumowanie główne

Aby przejść do innych stron podsumowania, należy kliknąć opisane poniżej elementy.

Element	Opis
Zmień widok	Aby otworzyć listę ze stronami podsumowania, należy kliknąć łącze **Zmień widok**. Następnie należy wybrać z listy stronę podsumowania, która ma zostać wyświetlona.
Strzałka w prawo	Aby wyświetlić następną stronę podsumowania, należy kliknąć ikonę strzałki w prawo,
Strzałka w lewo	Aby wyświetlić poprzednią stronę podsumowania, należy kliknąć ikonę strzałki w lewo.
Początek	Aby powrócić do strony **Podsumowanie główne**, należy kliknąć ikonę strony głównej (z rysunkiem domu).

Na stronie Podsumowanie główne można znaleźć następujące informacje.

Element	Opis
Ustawienie zabezpieczeń	Stan ustawienia zabezpieczeń określa ustawiony poziom zabezpieczeń zapory. Po kliknięciu łącza można zmienić poziom zabezpieczeń.
Zablokowane zdarzenia	Stan zablokowanych zdarzeń wyświetla liczbę zdarzeń zablokowanych w bieżącym dniu. Po kliknięciu łącza wyświetlane są szczegóły zdarzenia ze strony Zdarzenia przychodzące.
Zmiany reguł aplikacji	Stan reguł aplikacji wyświetla liczbę zmienionych ostatnio reguł aplikacji. Kliknięcie łącza wyświetla listę aplikacji z przyznanym i zablokowanym dostępem oraz umożliwia modyfikację uprawnień aplikacji.
Nowości	W sekcji **Nowości** jest wyświetlana aplikacja, której ostatnio przyznano pełny dostęp do Internetu.
Ostatnie zdarzenie	W sekcji **Ostatnie zdarzenie** są wyświetlane ostatnie zdarzenia przychodzące. Po kliknięciu łącza można przeprowadzić śledzenie zdarzenia lub umieścić adres IP na liście zaufanych adresów. Umieszczenie adresu IP na liście zaufanych adresów umożliwi przepuszczenie całego ruchu z tego adresu IP do lokalnego komputera.
Raport dzienny	W sekcji **Raport dzienny** jest wyświetla liczba zablokowanych przez program Personal Firewall zdarzeń przychodzących w bieżącym dniu, tygodniu oraz miesiącu. Po kliknięciu łącza wyświetlane są szczegóły zdarzenia ze strony Zdarzenia przychodzące.
Aktywne aplikacje	W sekcji **Aktywne aplikacje** są wyświetlane aplikacje, które w danej chwili są uruchomione na komputerze i korzystają z połączenia z Internetem. Po kliknięciu nazwy aplikacji są wyświetlane adresy IP, z którymi połączona jest dana aplikacja.
Typowe zadania	Kliknięcie łącza znajdującego się w sekcji **Typowe zadania** umożliwia przejście do stron programu Personal Firewall, na których można przeglądać działanie zapory i wykonywać zadania.

Aby wyświetlić stronę Podsumowanie aplikacji:

1 Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Wyświetl podsumowanie**.

2 Kliknij łącze **Zmień widok**, a następnie wybierz opcję **Podsumowanie aplikacji**.

Na stronie Podsumowanie aplikacji można znaleźć następujące informacje.

Element	Opis
Monitor ruchu	W sekcji **Monitor ruchu** są wyświetlane przychodzące i wychodzące połączenia z Internetem nawiązane w ciągu ostatnich piętnastu minut. Aby wyświetlić szczegóły monitorowania przepływu danych, należy kliknąć wykres.
Aktywne aplikacje	W sekcji **Aktywne aplikacje** są wyświetlane informacje o wykorzystaniu przepustowości pasma przez najbardziej aktywne aplikacje na komputerze w ciągu ostatnich dwudziestu czterech godzin. **Aplikacja** - Aplikacja uzyskująca dostęp do Internetu. **%** - Procentowa wartość wykorzystania przepustowości pasma przez aplikację. **Uprawnienie** - Typ dostępu do Internetu dozwolony dla aplikacji. **Utworzona reguła** - Data utworzenia reguły dla aplikacji.
Nowości	W sekcji **Nowości** jest wyświetlana aplikacja, której ostatnio przyznano pełny dostęp do Internetu.
Aktywne aplikacje	W sekcji **Aktywne aplikacje** są wyświetlane aplikacje, które w danej chwili są uruchomione na komputerze i korzystają z połączenia z Internetem. Po kliknięciu nazwy aplikacji są wyświetlane adresy IP, z którymi połączona jest dana aplikacja.
Typowe zadania	Kliknięcie łącza znajdującego się w sekcji **Typowe zadania** umożliwia przejście do stron programu Personal Firewall, na których można przeglądać stan aplikacji i wykonywać związane z aplikacjami zadania.

Aby wyświetlić stronę Podsumowanie zdarzeń:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Wyświetl podsumowanie**.
2. Kliknij łącze **Zmień widok**, a następnie wybierz opcję **Podsumowanie zdarzeń**.

Na stronie Podsumowanie zdarzeń można znaleźć następujące informacje.

Element	Opis
Porównanie portów	W sekcji **Porównanie portów** jest wyświetlany wykres kołowy najczęściej wykorzystywanych portów w komputerze w ciągu ostatnich 30 dni. Kliknięcie nazwy portu spowoduje wyświetlenie szczegółów ze strony Zdarzenia przychodzące. Umieszczenie wskaźnika myszy nad numerem portu spowoduje wyświetlenie opisu tego portu.
Najczęstsze ataki	W sekcji **Najczęstsze ataki** są wyświetlane najczęściej blokowane adresy IP, czas wystąpienia ostatniego zdarzenia przychodzącego dla każdego adresu oraz ogólna liczba zdarzeń przychodzących z ostatnich trzydziestu dni dla każdego adresu. Kliknięcie zdarzenia wyświetla jego szczegóły ze strony Zdarzenia przychodzące.
Raport dzienny	W sekcji **Raport dzienny** jest wyświetla liczba zablokowanych przez program Personal Firewall zdarzeń przychodzących w bieżącym dniu, tygodniu oraz miesiącu. Kliknięcie liczby wyświetla szczegóły zdarzenia z dziennika zdarzeń przychodzących.
Ostatnie zdarzenie	W sekcji **Ostatnie zdarzenie** są wyświetlane ostatnie zdarzenia przychodzące. Po kliknięciu łącza można przeprowadzić śledzenie zdarzenia lub umieścić adres IP na liście zaufanych adresów. Umieszczenie adresu IP na liście zaufanych adresów umożliwi przepuszczenie całego ruchu z tego adresu IP do lokalnego komputera.
Typowe zadania	Kliknięcie łącza znajdującego się w sekcji **Typowe zadania** umożliwia przejście do stron programu Personal Firewall, na których można przeglądać szczegóły zdarzeń i wykonywać związane ze zdarzeniami zadania.

Aby wyświetlić stronę Podsumowanie witryny HackerWatch:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Wyświetl podsumowanie**.
2. Kliknij łącze **Zmień widok**, a następnie wybierz opcję **HackerWatch**.

Na stronie Podsumowanie witryny HackerWatch można znaleźć następujące informacje**.**

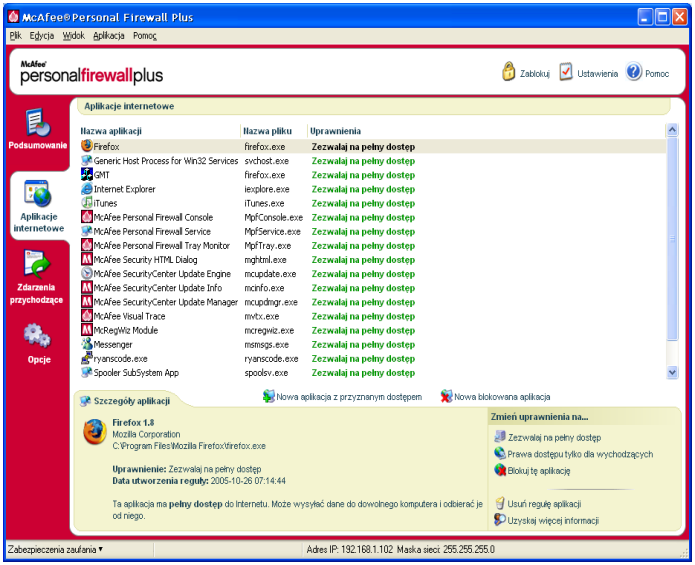
Element	Opis
Globalna aktywność	W sekcji **Globalna aktywność** wyświetlana jest mapa świata z zaznaczoną ostatnio zablokowaną działalnością monitorowaną przez witrynę HackerWatch.org. Aby otworzyć mapę Global Threat Analysis (analizy globalnego zagrożenia) w witrynie HackerWatch.org, należy kliknąć mapę.
Śledzenie zdarzeń	W sekcji **Śledzenie zdarzeń** jest wyświetla liczba zdarzeń przychodzących przesłanych do witryny HackerWatch.org.
Globalna aktywność portów	W sekcji **Globalna aktywność portów** są wyświetlane najczęściej atakowane porty w ciągu ostatnich pięciu dni (potencjalne zagrożenia). Kliknięcie portu wyświetla jego numer i opis.
Typowe zadania	Kliknięcie łącza znajdującego się w sekcji **Typowe zadania** umożliwia przejście do stron witryny HackerWatch.org, gdzie można uzyskać informacje na temat aktywności hakerów na całym świecie.

Informacje o stronie Aplikacje internetowe

Strona Aplikacje internetowe umożliwia wyświetlanie listy aplikacji z przyznanym oraz zablokowanym dostępem.

Aby otworzyć stronę Aplikacje internetowe:

- Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Aplikacje** (Rysunek 2-2).



Rysunek 2-2. Strona Aplikacje internetowe

Strona Aplikacje internetowe dostarcza następujących informacji:

- Nazwy aplikacji
- Nazwy plików
- Bieżące poziomy uprawnień
- Szczegóły aplikacji: nazwa i wersja aplikacji, nazwa firmy, ścieżka dostępu do aplikacji, poziom uprawnień aplikacji, znaczniki czasowe oraz objaśnienia poszczególnych typów uprawnień.

Zmiana reguł aplikacji

Program Personal Firewall umożliwia zmienianie reguł dostępu aplikacji.

Aby zmienić regułę aplikacji:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż opcję **Personal Firewall**, a następnie wybierz polecenie **Aplikacje internetowe**.
2. Na liście **Aplikacje internetowe** prawym przyciskiem myszy kliknij regułę aplikacji i wybierz inny poziom:
   - **Zezwalaj na pełny dostęp -** Pozwala aplikacji na ustanawianie wychodzących i przychodzących połączeń z Internetem.
   - **Prawa dostępu tylko dla wychodzących -** Pozwala aplikacji na ustanawianie wyłącznie wychodzących połączeń z Internetem.
   - **Blokuj tę aplikację -** Blokuje aplikacji dostęp do Internetu.

     UWAGA
     Wcześniej blokowane aplikacje są nadal blokowane, kiedy zapora jest ustawiona w trybie **Otwarty** lub **Blokowanie**. Aby temu zapobiec, można zmienić regułę dostępu tej aplikacji na **Zezwalaj na pełny dostęp** lub usunąć regułę **Blokuj tę aplikację** z listy **Aplikacje internetowe**.

Aby usunąć regułę aplikacji:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee  znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Aplikacje internetowe**.
2. Na liście **Aplikacje internetowe** prawym przyciskiem myszy kliknij regułę aplikacji i wybierz polecenie **Usuń regułę aplikacji**.

Następnym razem, gdy aplikacja zażąda dostępu do Internetu, będzie można ponownie ustawić jej poziom uprawnień w celu dodania jej do listy.

Przyznawanie dostępu i blokowanie aplikacji internetowych

Aby zmienić listę aplikacji internetowych z przyznanym dostępem i zablokowanych:

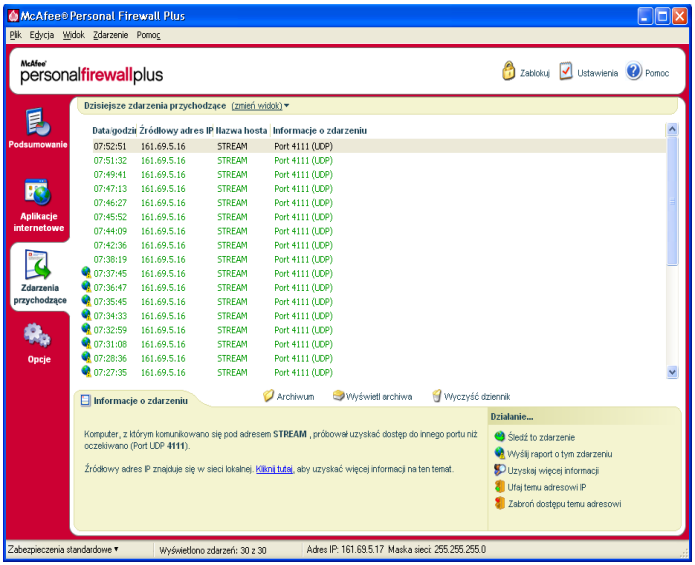
1. Kliknij prawym przyciskiem myszy ikonę programu McAfee  znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Aplikacje internetowe**.
2. Na stronie Aplikacje internetowe kliknij jedną z następujących opcji:
   - **Nowa aplikacja z przyznanym dostępem** - Zezwala aplikacji na pełny dostęp do Internetu.
   - **Nowa blokowana aplikacja** - Blokuje aplikacji dostęp do Internetu.
   - **Usuń regułę aplikacji** - Usuwa regułę aplikacji.

Informacje o stronie Zdarzenia przychodzące

Strona Zdarzenia przychodzące służy do wyświetlania dziennika zdarzeń przychodzących generowanego w momencie blokowania przez program Personal Firewall niepożądanych połączeń internetowych.

Aby otworzyć stronę Zdarzenia przychodzące:

- Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące** (Rysunek 2-3).



Rysunek 2-3. Strona Zdarzenia przychodzące

Na stronie Zdarzenia przychodzące znajdują się następujące informacje:

- Znaczniki czasu
- Źródłowe adresy IP
- Nazwy hostów
- Nazwy usług lub aplikacji
- Szczegóły zdarzenia: typy połączenia, porty połączenia, nazwa lub adres IP hosta oraz wyjaśnienia zdarzeń występujących na tych portach.

Omówienie zdarzeń

Informacje o adresach IP

Adresy IP składa się z czterech liczb, każdej z zakresu od 0 do 255. Liczby te identyfikują określone miejsce w Internecie, do którego można skierować ruch sieciowy.

Typy adresów IP

Pewna liczba adresów IP traktowana jest inaczej z różnych przyczyn:

Nierutowalne adresy IP - Znane również jako „prywatna przestrzeń IP”. Adresy te nie mogą być używane w Internecie. Prywatne bloki IP to 10.x.x.x, 172.16.x.x- 172.31.x.x oraz 192.168.x.x.

Pętlowe adresy IP - Wykorzystywane są w celach testowych. Ruch sieciowy wysłany do takiego bloku adresów IP wraca do urządzenia, które taki pakiet wygenerowało. Nigdy nie opuszcza tego urządzenia i jest przeważnie wykorzystywany do testowania sprzętu i oprogramowania. Pętlowy blok IP to 127.x.x.x.

Pusty adres IP - Jest to adres nieprawidłowy. Jego wykrycie przez program Personal Firewall oznacza, że ruch sieciowy użył pustego adresu IP. Często oznacza to, że nadawca celowo ukrywa źródło ruchu. Nadawca nie będzie w stanie odebrać żadnych odpowiedzi na generowany ruch sieciowy, chyba że pakiet zostanie odebrany przez aplikację, która zrozumie zawartość tego pakietu zawierającą instrukcje specyficzne dla tej aplikacji. Wszystkie adresy rozpoczynające się liczbą 0 (0.x.x.x) są adresami pustymi. Na przykład 0.0.0.0 jest pustym adresem IP.

Zdarzenia z adresu 0.0.0.0

Występowanie zdarzeń pochodzących z adresu IP 0.0.0.0 ma zazwyczaj dwie przyczyny. Pierwszą, a zarazem najczęstszą, jest otrzymanie przez komputer nieprawidłowo skonstruowanego pakietu. Internet nie jest zawsze w 100% niezawodny i możliwe jest występowanie błędnych pakietów. Program Personal Firewall przechwytuje pakiety zanim protokół TCP/IP może je sprawdzić, więc pakiety takie mogą być raportowane jako zdarzenie.

Inna sytuacja ma miejsce, gdy źródłowy adres IP jest fałszywy lub ktoś się pod niego podszywa. Występowanie pakietów podszywających się może być znakiem, że ktoś przeprowadza skanowanie komputera w poszukiwaniu koni trojańskich. Program Personal Firewall blokuje tego typu działania, więc komputer pozostaje bezpieczny.

Zdarzenia z adresu 127.0.0.1

Czasami zdarzenia mają źródłowy adres IP 127.0.0.1. Jest on nazywany adresem pętlowym (ang. loopback) lub hostem lokalnym (ang. localhost).

Wiele programów wykorzystuje adres pętlowy do komunikowania się ze swoimi składnikami. Na przykład, wiele osobistych serwerów poczty e-mail lub WWW można skonfigurować poprzez interfejs sieci Web. Aby uzyskać do nich dostęp, należy wpisać „http://localhost/” w przeglądarce sieci Web.

Jednakże program Personal Firewall pozwala na ruch z tych programów, jeśli więc pojawiają się zdarzenia spod adresu 127.0.0.1, najprawdopodobniej taki źródłowy adres IP jest fałszywy lub ktoś się pod niego podszywa. Występowanie pakietów podszywających się oznacza zazwyczaj, że inny komputer przeprowadza skanowanie w poszukiwaniu koni trojańskich. Program Personal Firewall blokuje próby włamań tego typu, więc komputer pozostaje bezpieczny.

Niektóre programy, a zwłaszcza Netscape w wersji 6.2 i nowszej, wymagają dodania adresu 127.0.0.1 do listy zaufanych adresów IP. Składniki tego programu komunikują się ze sobą w taki sposób, że Personal Firewall nie może określić, czy ma do czynienia z ruchem lokalnym czy nie.

Biorąc dalej jako przykład program Netscape 6.2, jeśli adres 127.0.0.1 nie zostanie dodany do listy zaufanych adresów, nie będzie możliwe korzystanie z listy znajomych. Reasumując, jeśli zostanie zauważony ruch z adresu 127.0.0.1, a wszystkie aplikacje w komputerze działają normalnie, to ruch ten można bezpiecznie zablokować. Jednakże jeśli jakiś program (np. Netscape) działa niestabilnie, należy dodać adres 127.0.0.1 do listy zaufanych adresów IP programu Personal Firewall.

Jeśli dodanie adresu 127.0.0.1 do listy zaufanych adresów IP usunęło problem, należy rozważyć związane z tym kwestie. Jeśli użytkownik doda adres 127.0.0.1 do listy zaufanych, jego program będzie działał, ale zwiększy się niebezpieczeństwo wystąpienia podszywających się ataków. Jeśli użytkownik nie doda adresu do listy zaufanych, jego program nie będzie działał, ale komputer pozostanie chroniony przed takim złośliwym ruchem sieciowym.

Zdarzenia pochodzące z komputerów w sieci LAN

Zdarzenia mogą być generowane przez komputery w sieci lokalnej (LAN) użytkownika. Aby pokazać, że zdarzenia te są generowane przez sieć, program Personal Firewall wyświetla je w kolorze zielonym.

W przypadku ustawień większości firmowych sieci LAN powinno zostać wybrane ustawienie **Ufaj wszystkim komputerom w sieci LAN** w opcjach Zaufane adresy IP.

W niektórych sytuacjach sieć lokalna może być tak samo niebezpieczna jak Internet. Szczególnie w przypadku, gdy komputer pracuje w szerokopasmowej sieci wykorzystującej modem DSL lub kablowy. W takim przypadku nie należy wybierać opcji **Ufaj wszystkim komputerom w sieci LAN**. Zamiast tego należy dodać adresy IP komputerów lokalnych do listy zaufanych adresów IP.

Zdarzenia pochodzące z prywatnych adresów IP

Adresy IP w formacie 192.168.xxx.xxx, 10.xxx.xxx.xxx oraz 172.16.0.0- 172.31.255.255 są tak zwanymi nierutowalnymi lub prywatnymi adresami IP. Adresy te nie powinny nigdy opuścić lokalnej sieci i w większości przypadków można im zaufać.

Blok 192.168.xxx.xxx jest wykorzystywany przez usługę udostępniania połączenia internetowego (ICS) firmy Microsoft. Jeśli w przypadku korzystania z usługi ICS w dzienniku znajdują się zdarzenia z tego bloku IP, to adres IP 192.168.255.255 można dodać do listy zaufanych adresów IP. Spowoduje to przyznanie zaufania do całego bloku 192.168.xxx.xxx.

Jeśli użytkownik nie korzysta z sieci prywatnej, a zdarzenia z tych zakresów adresów IP pojawiają się w dzienniku, wówczas źródłowy adres IP może być fałszywy lub ktoś się pod niego podszywa. Występowanie pakietów podszywających się jest zazwyczaj znakiem, że ktoś przeprowadza skanowanie w poszukiwaniu koni trojańskich. Ważne jest, aby pamiętać, że program Personal Firewall zblokował tę próbę, więc komputer pozostaje bezpieczny.

W związku z tym, że prywatne adresy IP odnoszą się do różnych komputerów w zależności od sieci, w której pracuje komputer użytkownika, zgłaszanie tego typu zdarzeń nie przyniesie żadnych rezultatów, tak więc nie jest to konieczne.

Wyświetlanie zdarzeń w dzienniku zdarzeń przychodzących

Dziennik zdarzeń przychodzących wyświetla zdarzenia na różne sposoby. Domyślny widok wyświetla zdarzenia tylko z bieżącego dnia. Można również wyświetlić zdarzenia z ostatniego tygodnia lub wyświetlić cały dziennik.

Program Personal Firewall pozwala również na wyświetlenie zdarzeń przychodzących z określonych dni, określonych adresów internetowych (adresów IP) lub zdarzeń zawierających identyczne informacje.

Aby uzyskać informacje o zdarzeniu, należy kliknąć to zdarzenie, a informacje pojawią się w okienku **Informacje o zdarzeniu**.

Wyświetlanie zdarzeń z bieżącego dnia

Ta opcja służy do przeglądania zdarzeń z bieżącego dnia.

Aby wyświetlić zdarzenia z bieżącego dnia:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. W dzienniku zdarzeń przychodzących kliknij wpis prawym przyciskiem myszy, a następnie kliknij polecenie **Pokaż dzisiejsze zdarzenia**.

Wyświetlanie zdarzeń z bieżącego tygodnia

Ta opcja służy do przeglądania zdarzeń tygodniowych.

Aby wyświetlić zdarzenia z bieżącego tygodnia:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. W dzienniku zdarzeń przychodzących kliknij wpis prawym przyciskiem myszy, a następnie kliknij polecenie **Pokaż zdarzenia z tego tygodnia**.

Wyświetlanie całego dziennika zdarzeń przychodzących

Ta opcja służy do przeglądania wszystkich zdarzeń.

Aby wyświetlić wszystkie zdarzenia z dziennika zdarzeń przychodzących:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż opcję **Personal Firewall**, a następnie kliknij polecenie **Zdarzenia przychodzące**.
2. W dzienniku zdarzeń przychodzących kliknij wpis prawym przyciskiem myszy, a następnie kliknij polecenie **Pokaż cały dziennik**.

   Wyświetlone zostaną wszystkie zdarzenia z dziennika zdarzeń przychodzących.

Wyświetlanie zdarzeń z określonego dnia

Ta opcja służy do przeglądania zdarzeń z określonego dnia.

Aby pokazać zdarzenia z określonego dnia:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. W dzienniku zdarzeń przychodzących kliknij wpis prawym przyciskiem myszy, a następnie kliknij polecenie **Pokaż tylko zdarzenia z tego dnia**.

Wyświetlanie zdarzeń z określonego adresu internetowego

Opcja ta służy do przeglądania innych zdarzeń pochodzących z określonego adresu internetowego.

Aby pokazać zdarzenia dla adresu internetowego:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie kliknij polecenie **Zdarzenia przychodzące**.
2. W dzienniku zdarzeń przychodzących kliknij wpis prawym przyciskiem myszy, a następnie kliknij polecenie **Pokaż tylko zdarzenia dla wybranego adresu internetowego**.

Wyświetlanie zdarzeń zawierających identyczne informacje o zdarzeniu

Opcja ta służy do przeglądania innych zdarzeń w dzienniku zdarzeń przychodzących, które w kolumnie Informacje o zdarzeniu zawierają takie same informacje jak wybrane zdarzenie. W ten sposób można uzyskać informacje o liczbie wystąpień tego zdarzenia oraz czy pochodzi ono z tego samego źródła. W kolumnie Informacje o zdarzeniu znajduje się opis zdarzenia oraz, jeśli jest znany, typowy program lub usługa korzystająca z tego portu.

Aby pokazać zdarzenia zawierające identyczne informacje o zdarzeniu:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie kliknij polecenie **Zdarzenia przychodzące**.
2. W dzienniku zdarzeń przychodzących kliknij wpis prawym przyciskiem myszy, a następnie kliknij polecenie **Pokaż tylko zdarzenia z tymi samymi informacjami o zdarzeniu**.

Reagowanie na zdarzenia przychodzące

Poza przeglądaniem szczegółowych informacji o zdarzeniach w dzienniku zdarzeń przychodzących użytkownik może przeprowadzić wizualne śledzenie adresów IP zdarzenia z dziennika zdarzeń przychodzących lub uzyskać szczegółowe informacje na temat tego zdarzenia w witrynie ochrony przed włamaniami społeczności online HackerWatch.org.

Śledzenie wybranego zdarzenia

Dla zdarzenia znajdującego się w dzienniku zdarzeń przychodzących można spróbować przeprowadzić wizualne śledzenie za pomocą aplikacji Visual Trace.

Aby prześledzić wybrane zdarzenie:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. W dzienniku zdarzeń przychodzących kliknij prawym przyciskiem myszy zdarzenie, które ma być śledzone, a następnie polecenie **Śledź wybrane zdarzenie**. Można również dwukrotnie kliknąć zdarzenie, aby rozpocząć śledzenie.

Program Personal Firewall domyślnie rozpoczyna wizualne śledzenie wykorzystując do tego zintegrowany program Personal Firewall Visual Trace.

Uzyskiwanie porad z witryny HackerWatch.org

Aby uzyskać poradę z witryny HackerWatch.org:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż opcję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Na stronie Zdarzenia przychodzące wybierz wpis zdarzenia, a następnie w panelu **Działanie** kliknij łącze **Uzyskaj więcej informacji**.

Zostanie uruchomiona domyślna przeglądarka sieci Web i otworzy się witryna HackerWatch.org, z której można pobrać informacje na temat danego typu zdarzenia oraz uzyskać poradę dotyczącą jego raportowania.

Raportowanie zdarzenia

Aby wysłać raport na temat zdarzenia, które mogło być atakiem na komputer:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Kliknij zdarzenie, o którym raport ma zostać wysłany, a następnie w panelu **Działanie** kliknij łącze **Wyślij raport o tym zdarzeniu**.

Program Personal Firewall wyśle raport o zdarzeniu do witryny HackerWatch.org wykorzystując unikatowy identyfikator użytkownika.

Rejestrowanie się w witrynie HackerWatch.org

Przy pierwszym otwarciu strony Podsumowanie program Personal Firewall skontaktuje się z witryną HackerWatch.org, aby wygenerować unikatowy identyfikator użytkownika. Jeśli użytkownik jest już zarejestrowany, jego dane rejestracyjne są sprawdzane automatycznie. W przypadku nowego użytkownika w celu korzystania z funkcji filtrowania/przesyłania pocztą e-mail zdarzeń do witryny HackerWatch.org należy podać przydomek oraz adres e-mail, a następnie kliknąć na sprawdzające łącze znajdujące się w potwierdzającej wiadomości e-mail przesłanej z tej witryny.

Zdarzenia można raportować do witryny HackerWatch.org bez sprawdzenia identyfikatora użytkownika. Jednakże, aby mieć możliwość filtrowania i przesyłania zdarzeń pocztą e-mail do przyjaciela, wymagana jest rejestracja.

Zarejestrowanie w celu korzystania z tej usługi pozwala na śledzenie zgłoszeń oraz na powiadamianie użytkownika w przypadku, gdy witryna HackerWatch.org będzie potrzebowała więcej informacji lub dalszych działań ze strony użytkownika. Aby jakakolwiek uzyskana informacja była informacją użyteczną, musi istnieć możliwość jej potwierdzenia, co zapewnia wymagana rejestracja użytkownika.

Wszystkie adresy e-mail przekazane do witryny HackerWatch.org są przechowywane jako dane poufne. Jeśli dostawca usług internetowych żąda dodatkowych informacji, żądanie takie jest kierowane do witryny HackerWatch.org; adres e-mail użytkownika nigdy nie jest ujawniany.

Ufanie adresowi

Aby dodać adres IP do listy zaufanych adresów IP i umożliwić trwałe połączenie, można skorzystać ze strony Zdarzenia przychodzące.

Jeśli na stronie Zdarzenia przychodzące znajduje się zdarzenie zawierające adres IP, z którego dostęp ma być dozwolony, program Personal Firewall można skonfigurować tak, aby zawsze zezwalał na połączenia z tego adresu.

Aby dodać adres IP do listy zaufanych adresów IP:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Kliknij prawym przyciskiem myszy zdarzenie, którego adres IP ma zostać dodany do adresów zaufanych, a następnie kliknij polecenie **Ufaj źródłowemu adresowi IP**.

Sprawdź, czy adres IP wyświetlany w oknie dialogowym Ufaj temu adresowi IP jest prawidłowy, a następnie kliknij przycisk **OK**. Adres IP zostanie dodany do listy Zaufane adresy IP.

Aby sprawdzić, czy adres IP został dodany:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Opcje**.
2. Kliknij ikonę **Zaufane i zabronione adresy IP**, a następnie kliknij kartę **Zaufane adresy IP**.

Adres IP pojawi się jako zaznaczony na liście Zaufane adresy IP.

Zabranianie dostępu adresowi

Jeśli w dzienniku zdarzeń przychodzących pojawia się adres IP oznacza to, że ruch z tego adresu został zablokowany. Zabranianie dostępu do adresu nie daje zatem dodatkowej ochrony, chyba że w komputerze celowo pozostawiono otwarte porty wykorzystując funkcję usług systemowych lub na komputerze uruchomiona jest aplikacja mająca uprawnienie do odbierania ruchu.

Dodanie adresu IP do listy zabronionych adresów ma sens tylko, jeśli co najmniej jeden port pozostaje celowo otwarty oraz jeśli istnieją podstawy, aby uważać, że dostęp do otwartych portów z tego adresu musi być zablokowany.

Jeśli na stronie Zdarzenia przychodzące znajduje się zdarzenie zawierające adres IP, który ma być zabroniony, program Personal Firewall można skonfigurować tak, aby nigdy nie zezwalał na połączenia z tego adresu.

Aby zabronić dostępu do adresu IP, co do którego istnieje przypuszczenie, że jest źródłem podejrzanej lub niepożądanej aktywności internetowej, można skorzystać ze strony Zdarzenia przychodzące zawierającej listę adresów IP całego przychodzącego ruchu internetowego.

Aby dodać adres IP do listy zabronionych adresów IP:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Na stronie Zdarzenia przychodzące znajduje się lista adresów IP całego przychodzącego ruchu internetowego. Wybierz adres IP, a następnie wykonaj jedną z poniższych czynności:
   - Kliknij prawym przyciskiem myszy adres IP, a następnie wybierz polecenie **Zabroń dostępu źródłowemu adresowi IP**.
   - Z menu **Działanie** kliknij polecenie **Zabroń dostępu temu adresowi**.
3. W oknie dialogowym Dodaj regułę zabronionego adresu IP zastosuj co najmniej jedno z następujących ustawień, aby skonfigurować regułę zabronionego adresu IP:
   - **Pojedynczy adres IP**: Adres IP, do którego dostęp ma zostać zabroniony. Domyślnie jest to adres IP wybrany ze strony Zdarzenia przychodzące.
   - **Zakres adresów IP**: Adresy IP zawarte między adresem określonym w polu Od adresu IP, a adresem IP określonym w polu Do adresu IP.
   - **Niech ta reguła wygasa**: Data i godzina, o której wygaśnie reguła zabronionego adresu IP. Wybierz datę i godzinę z odpowiedniego menu rozwijanego.
   - **Opis**: Opcjonalnie opisuje nową regułę.
   - Kliknij przycisk **OK**.
4. W oknie dialogowym kliknij przycisk **Tak**, aby potwierdzić ustawienie. Kliknij przycisk **Nie**, aby powrócić do okna dialogowego Dodaj regułę zabronionego adresu IP.

Jeśli program Personal Firewall wykryje zdarzenie z zabronionego połączenia internetowego, zostanie wyświetlony alert zgodnie z metodą określoną na stronie Ustawienia alertu.

Aby sprawdzić, czy adres IP został dodany:

1. Kliknij kartę **Opcje**.
2. Kliknij ikonę **Zaufane i zabronione adresy IP**, a następnie kartę **Zabronione adresy IP**.

Adres IP pojawi się jako zaznaczony na liście Zabronione adresy IP.

Zarządzanie dziennikiem zdarzeń przychodzących

Strona Zdarzenia przychodzące umożliwia zarządzanie zdarzeniami w dzienniku zdarzeń przychodzących generowanymi w momencie blokowania przez program Personal Firewall niepożądanego ruchu internetowego.

Archiwizowanie dziennika zdarzeń przychodzących

Dziennik zdarzeń przychodzących można zarchiwizować, aby zapisać wszystkie rejestrowane zdarzenia, łącznie z ich datą i godziną, źródłowymi adresami IP, nazwami hostów, portów i informacjami o zdarzeniu. Aby zapobiec nadmiernemu powiększaniu się dziennika zdarzeń przychodzących, zaleca się jego okresowe archiwizowanie.

Aby zarchiwizować dziennik zdarzeń przychodzących:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Na stronie Zdarzenia przychodzące kliknij łącze **Archiwizuj**.
3. W oknie dialogowym Archiwizuj dziennik kliknij przycisk **Tak**, aby kontynuować operację.
4. Kliknij przycisk **Zapisz**, aby zapisać archiwum w domyślnej lokalizacji lub wybierz lokalizację do zapisania archiwum.

Uwaga: Domyślnie program Personal Firewall automatycznie tworzy archiwum dziennika zdarzeń przychodzących. Zaznacz lub usuń zaznaczenie pola wyboru **Automatycznie archiwizuj rejestrowane zdarzenia** znajdujące się na stronie Ustawienia dziennika zdarzeń, aby włączyć lub wyłączyć tę opcję.

Przeglądanie zarchiwizowanego dziennika zdarzeń przychodzących

Można wyświetlać wszystkie wcześniej zarchiwizowane dzienniki zdarzeń przychodzących. Zapisane archiwum zawiera datę i godzinę, źródłowe adresy IP, nazwy hostów, porty i informacje o zdarzeniu.

Aby wyświetlić zarchiwizowany dziennik zdarzeń przychodzących:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Na stronie Zdarzenia przychodzące kliknij łącze **Wyświetl archiwa**.
3. Wybierz lub znajdź nazwę pliku archiwum i kliknij przycisk **Otwórz**.

Czyszczenie dziennika zdarzeń przychodzących

Można wyczyścić wszystkie informacje znajdujące się w dzienniku zdarzeń przychodzących.

OSTRZEŻENIE: Po wyczyszczeniu dziennika zdarzeń przychodzących nie ma możliwości jego odtworzenia. Jeśli dziennik zdarzeń ma być wykorzystywany w przyszłości, powinien zostać zarchiwizowany.

Aby wyczyścić dziennik zdarzeń przychodzących:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż opcję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Na stronie Zdarzenia przychodzące kliknij łącze **Wyczyść dziennik**.
3. Kliknij przycisk **Tak** w oknie dialogowym, aby wyczyścić dziennik.

Kopiowanie zdarzenia do schowka

Zdarzenie można skopiować do schowka w celu wklejenia go do pliku tekstowego za pomocą Notatnika.

Aby skopiować zdarzenia do schowka:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee, wskaż opcję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Prawym przyciskiem myszy kliknij zdarzenie z dziennika zdarzeń przychodzących.
3. Kliknij polecenie **Kopiuj wybrane zdarzenie do schowka**.
4. Uruchom program Notatnik.
   - Wpisz `notepad` w wierszu polecenia lub kliknij przycisk **Start** systemu Windows, wskaż **Programy**, a następnie **Akcesoria**. Wybierz polecenie **Notatnik**.
5. Kliknij menu **Edycja**, a następnie polecenie Wklej. Tekst zdarzenia pojawi się w Notatniku. Powtarzaj tę czynność, aż do skopiowania wszystkich koniecznych zdarzeń.
6. Zapisz plik Notatnika w bezpiecznym miejscu.

Usuwanie wybranego zdarzenia

Istnieje możliwość usuwania zdarzeń z dziennika zdarzeń przychodzących.

Aby usunąć zdarzenia z dziennika zdarzeń przychodzących:

1. Kliknij prawym przyciskiem myszy ikonę programu McAfee znajdującą się na pasku zadań systemu Windows, wskaż pozycję **Personal Firewall**, a następnie wybierz polecenie **Zdarzenia przychodzące**.
2. Na stronie Zdarzenia przychodzące kliknij wpis zdarzenia, które chcesz usunąć.
3. W menu Edycja kliknij polecenie **Usuń wybrane zdarzenie**. Zdarzenie zostanie usunięte z dziennika zdarzeń przychodzących.

Informacje o alertach

Stanowczo zaleca się zaznajomienie z rodzajami alertów występującymi w trakcie korzystania z programu Personal Firewall. Przejrzenie poniższych rodzajów alertów oraz dostępnego wyboru reakcji na nie pozwoli użytkownikowi na świadome reagowanie na wyświetlony alert.

UWAGA
Zalecenia zawarte w alertach pomagają w podjęciu decyzji dotyczącej sposobu obsługi zdarzenia wywołującego alert. W celu wyświetlania zaleceń w alertach kliknij kartę **Opcje**, kliknij ikonę **Ustawienia alertów**, a następnie z listy **Inteligentne zalecenia** wybierz opcję **Użyj inteligentnych zaleceń** (domyślnie) lub **Wyświetlaj tylko inteligentne zalecenia**.

Alerty czerwone

Alerty czerwone zawierają ważne informacje wymagające natychmiastowej uwagi:

- **Zablokowano aplikację internetową** - Ten alert jest wyświetlany, gdy program Personal Firewall zablokuje aplikacji dostęp do Internetu. Na przykład, jeśli wyświetlony zostanie alert o programie będącym koniem trojańskim, zapora McAfee automatycznie odmówi temu programowi dostępu do Internetu i zaleci przeskanowanie komputera w poszukiwaniu wirusów.
- **Aplikacja żąda dostępu do Internetu -** Alert ten jest wyświetlany, gdy program Personal Firewall wykryje ruch internetowy lub sieciowy wywołany przez nową aplikację.
- **Zmodyfikowano aplikację -** Ten alert zostaje wyświetlony w przypadku, gdy program Personal Firewall wykryje, że aplikacja, której wcześniej zezwolono na dostęp do Internetu, zmieniła się. Jeśli dana aplikacja nie była ostatnio uaktualniana, należy zachować ostrożność w przyznawaniu takiej zmodyfikowanej aplikacji uprawnień dostępu do Internetu.

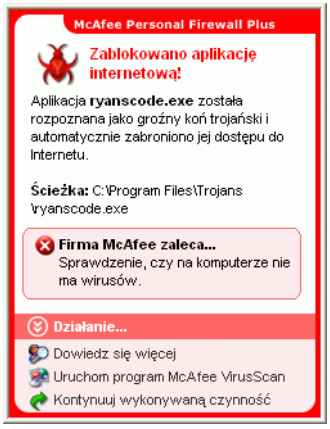
- **Aplikacja żąda dostępu w roli serwera-** Ten alert zostaje wyświetlony, gdy program Personal Firewall wykryje, że aplikacja, której wcześniej zezwolono na dostęp do Internetu, zażądała dostępu do Internetu w roli serwera.

  UWAGA
  W systemie operacyjnym Windows XP SP2 domyślne ustawienie aktualizacji automatycznych powoduje pobieranie i instalowanie aktualizacji systemu operacyjnego Windows oraz innych uruchomionych na komputerze programów firmy Microsoft bez powiadamiania użytkownika. Jeśli aplikacja została zmodyfikowana w wyniku jednej z takich cichych aktualizacji systemu Windows, to program McAfee Personal Firewall wyświetli alert przy następnym uruchomieniu takiej aplikacji firmy Microsoft.

  WAŻNE
  Aplikacjom wymagającym dostępu do Internetu w celu aktualizacji produktu w trybie online (na przykład usługom firmy McAfee) należy przyznać odpowiednie uprawnienia dostępu.

Alert Zablokowano aplikację internetową

Jeśli wyświetlony zostanie alert o programie będącym koniem trojańskim (Rysunek 2-4), program Personal Firewall automatycznie odmówi temu programowi dostępu do Internetu i zaleci przeskanowanie komputera w poszukiwaniu wirusów. Jeśli program McAfee VirusScan nie został zainstalowany, można uruchomić program McAfee SecurityCenter.



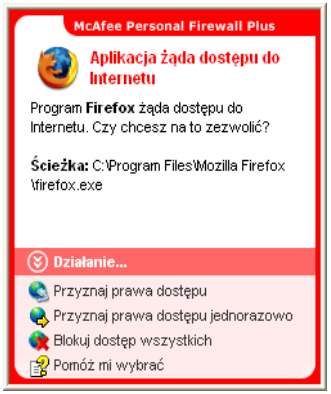
Rysunek 2-4. Alert Zablokowano aplikację internetową

Należy zapoznać się z krótkim opisem tego zdarzenia, a następnie wybrać jedną z następujących opcji:

- Kliknij polecenie **Dowiedz się więcej** w celu uzyskania szczegółowych informacji o zdarzeniu za pośrednictwem dziennika zdarzeń przychodzących (aby uzyskać więcej informacji, patrz *Informacje o stronie Zdarzenia przychodzące* na stronie 23).
- Kliknij przycisk **Uruchom program McAfee VirusScan**, aby przeskanować komputer w poszukiwaniu wirusów.
- Kliknij przycisk **Kontynuuj wykonywaną czynność**, jeśli nie chcesz podejmować dalszych działań poza tymi, które zostały już podjęte przez program Personal Firewall.
- Kliknij przycisk **Przyznaj prawa dostępu dla wychodzących**, aby zezwolić na połączenie wychodzące (**Wyższy** poziom zabezpieczeń).

Alert Aplikacja żąda dostępu do Internetu

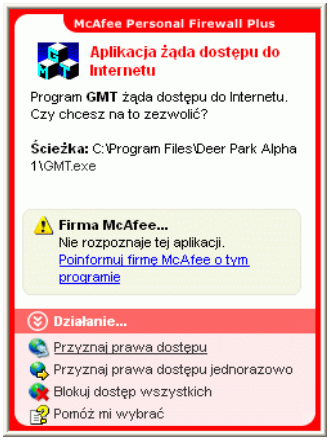
Jeśli w opcjach Ustawienia zabezpieczeń wybrano poziom zabezpieczeń **Standardowy** lub **Wysoki**, program Personal Firewall wyświetli alert (Rysunek 2-5) w momencie wykrycia połączeń internetowych lub sieciowych dla nowych lub zmodyfikowanych aplikacji.



Rysunek 2-5. Alert Aplikacja żąda dostępu do Internetu

Po wyświetleniu alertu zalecającego zachowanie ostrożności przed przyznaniem aplikacji dostępu do Internetu użytkownik może uzyskać dodatkowe informacje o tej aplikacji, klikając łącze **Kliknij tutaj, aby dowiedzieć się więcej**. Opcja ta pojawi się w alercie tylko wówczas, gdy program Personal Firewall zostanie skonfigurowany do korzystania z funkcji Inteligentne zalecenia.

Zapora McAfee może nie rozpoznać aplikacji próbującej uzyskać dostęp do Internetu (Rysunek 2-6).



Rysunek 2-6. Alert Nierozpoznana aplikacja

Z tego powodu zapora McAfee nie może podać zalecanego sposobu postępowania z daną aplikacją. Można wysłać raport na temat tej aplikacji do firmy McAfee, klikając łącze **Poinformuj firmę McAfee o tym programie**. Spowoduje to wyświetlenie strony sieci Web umożliwiającej podanie informacji związanych z aplikacją. Należy wprowadzić jak najwięcej znanych informacji.

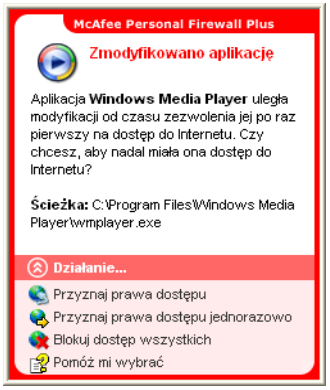
Przesyłane informacje w połączeniu z innymi narzędziami badawczymi są używane przez operatorów HackerWatch do określenia, czy aplikacja powinna zostać umieszczona w bazie danych znanych aplikacji, a jeśli tak, to w jaki sposób ma być traktowana przez program Personal Firewall.

Należy zapoznać się z krótkim opisem tego zdarzenia, a następnie wybrać jedną z następujących opcji:

- Kliknij przycisk **Przyznaj prawa dostępu**, aby zezwolić aplikacji na wychodzące i przychodzące połączenia internetowe.
- Kliknij przycisk **Przyznaj prawa dostępu jednorazowo**, aby zezwolić aplikacji na tymczasowe połączenie internetowe. Dostęp jest ograniczony do czasu między uruchomieniem aplikacji a jej zamknięciem.
- Kliknij przycisk **Blokuj dostęp wszystkich**, aby zabronić połączenia z Internetem.
- Kliknij przycisk **Przyznaj prawa dostępu dla wychodzących**, aby zezwolić na połączenie wychodzące (**Wyższy** poziom zabezpieczeń).
- Kliknij przycisk **Pomóż mi wybrać**, aby wyświetlić Pomoc online dotyczącą uprawnień dostępu aplikacji.

Alert Zmodyfikowano aplikację

Jeśli opcjach Ustawienia zabezpieczeń wybrano poziom zabezpieczeń **Zaufany**, **Standardowy** lub **Wysoki**, program Personal Firewall wyświetla alert (Rysunek 2-7) w momencie wykrycia zmiany w aplikacji, która wcześniej uzyskała zezwolenie na dostęp do Internetu. Jeśli dana aplikacja nie była ostatnio uaktualniana, należy zachować ostrożność w przyznawaniu takiej zmodyfikowanej aplikacji uprawnień dostępu do Internetu.



Rysunek 2-7. Alert Zmodyfikowano aplikację

Należy zapoznać się z krótkim opisem tego zdarzenia, a następnie wybrać jedną z następujących opcji:

- Kliknij przycisk **Przyznaj prawa dostępu**, aby zezwolić aplikacji na wychodzące i przychodzące połączenia internetowe.
- Kliknij przycisk **Przyznaj prawa dostępu jednorazowo**, aby zezwolić aplikacji na tymczasowe połączenie internetowe. Dostęp jest ograniczony do czasu między uruchomieniem aplikacji a jej zamknięciem.
- Kliknij przycisk **Blokuj dostęp wszystkich**, aby zabronić połączenia z Internetem.
- Kliknij przycisk **Przyznaj prawa dostępu dla wychodzących**, aby zezwolić na połączenie wychodzące (**Wyższy** poziom zabezpieczeń).
- Kliknij przycisk **Pomóż mi wybrać**, aby wyświetlić Pomoc online dotyczącą uprawnień dostępu aplikacji.

Alert Aplikacja żąda dostępu w roli serwera

Jeśli w opcjach ustawień zabezpieczeń wybrano poziom zabezpieczeń **Wysoki**, program Personal Firewall wyświetla alert (Rysunek 2-8), gdy aplikacja, której wcześniej zezwolono na dostęp do Internetu, zażąda dostępu do Internetu w roli serwera.

Rysunek 2-8. Alert Aplikacja żąda dostępu w roli serwera

Na przykład, alert zostanie wyświetlony, gdy program MSN Messenger zażąda dostępu w roli serwera, aby podczas rozmowy wysłać plik.

Należy zapoznać się z krótkim opisem tego zdarzenia, a następnie wybrać jedną z następujących opcji:

- Kliknij przycisk **Przyznaj prawa dostępu jednorazowo**, aby zezwolić aplikacji na tymczasowy dostęp do Internetu. Dostęp jest ograniczony do czasu między uruchomieniem aplikacji a jej zamknięciem.

- Kliknij przycisk **Przyznaj prawa dostępu w roli serwera**, aby zezwolić aplikacji na wychodzące i przychodzące połączenie z Internetem.
- Kliknij przycisk **Ogranicz do praw dostępu dla wychodzących**, aby zabronić przychodzącego połączenia internetowego.
- Kliknij przycisk **Blokuj dostęp wszystkich**, aby zabronić połączenia z Internetem.
- Kliknij przycisk **Pomóż mi wybrać**, aby wyświetlić Pomoc online dotyczącą uprawnień dostępu aplikacji.

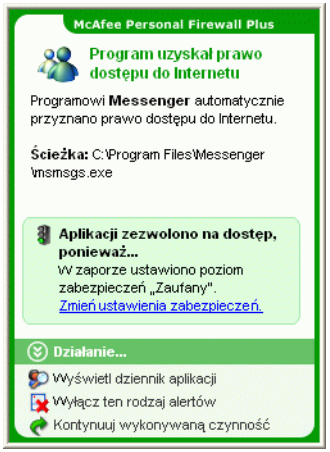
Alerty zielone

Alerty zielone informują użytkownika o zdarzeniach występujących w programie Personal Firewall takich jak aplikacje, którym automatycznie przyznano dostęp do Internetu.

Program uzyskał prawo dostępu do Internetu - Ten alert zostaje wyświetlony, gdy program Personal Firewall automatycznie umożliwia dostęp do Internetu wszystkim nowym aplikacjom, a następnie powiadamia o tym użytkownika (**Zaufany** poziom zabezpieczeń). Przykładem zmodyfikowanej aplikacji jest aplikacja posiadająca zmodyfikowane reguły automatycznie zezwalające jej na dostęp do Internetu.

Alert Aplikacja uzyskała dostępu do Internetu

Po wybraniu poziomu zabezpieczeń **Zaufany** w opcjach Ustawienia zabezpieczeń program Personal Firewall automatycznie przyznaje dostęp do Internetu wszystkim nowym aplikacjom, a następnie powiadamia o tym zdarzeniu użytkownika w alercie (Rysunek 2-9).



Rysunek 2-9. Program uzyskał prawo dostępu do Internetu

Należy zapoznać się z krótkim opisem tego zdarzenia, a następnie wybrać jedną z następujących opcji:

- Kliknij polecenie **Wyświetl dziennik aplikacji** w celu uzyskania szczegółowych informacji o zdarzeniu za pośrednictwem dziennika aplikacji internetowych (aby uzyskać więcej informacji, patrz *Informacje o stronie Aplikacje internetowe* na stronie 21).
- Kliknij polecenie **Wyłącz ten rodzaj alertów**, aby zapobiec wyświetlaniu alertów tego typu.
- Kliknij przycisk **Kontynuuj wykonywaną czynność**, jeśli nie chcesz podejmować dalszych działań poza tymi, które zostały już podjęte przez program Personal Firewall.
- Kliknij przycisk **Blokuj dostęp wszystkich**, aby zabronić połączenia z Internetem.

Alert Zmodyfikowano aplikację

Po wybraniu poziomu zabezpieczeń **Zaufany** w opcjach Ustawienia zabezpieczeń program Personal Firewall automatycznie przyznaje dostęp do Internetu wszystkim zmodyfikowanym aplikacjom. Należy zapoznać się z krótkim opisem tego zdarzenia, a następnie wybrać jedną z następujących opcji:

- Kliknij polecenie **Wyświetl dziennik aplikacji** w celu uzyskania szczegółowych informacji o zdarzeniu za pośrednictwem dziennika aplikacji internetowych (aby uzyskać więcej informacji, patrz *Informacje o stronie Aplikacje internetowe* na stronie 21).
- Kliknij polecenie **Wyłącz ten rodzaj alertów**, aby zapobiec wyświetlaniu alertów tego typu.
- Kliknij przycisk **Kontynuuj wykonywaną czynność**, jeśli nie chcesz podejmować dalszych działań poza tymi, które zostały już podjęte przez program Personal Firewall.
- Kliknij przycisk **Blokuj dostęp wszystkich**, aby zabronić połączenia z Internetem.

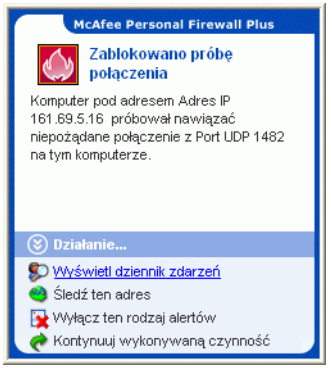
Alerty niebieskie

Alerty niebieskie mają charakter informacyjny i nie wymagają reakcji użytkownika.

- **Zablokowano próbę połączenia -** Ten alert jest wyświetlany, gdy program Personal Firewall zablokuje niepożądany ruch internetowy lub sieciowy. (Zaufany, Standardowy lub Wyższy poziom zabezpieczeń).

Alert Zablokowano próbę połączenia

Jeśli wybrano poziom zabezpieczeń **Zaufany**, **Standardowy** lub **Wyższy**, program Personal Firewall wyświetla alert (Rysunek 2-10) w momencie zablokowania niepożądanego ruchu internetowego lub sieciowego.



Rysunek 2-10. Alert Zablokowano próbę połączenia

Należy zapoznać się z krótkim opisem tego zdarzenia, a następnie wybrać jedną z następujących opcji:

- Kliknij polecenie **Wyświetl dziennik zdarzeń** w celu uzyskania szczegółowych informacji o zdarzeniu za pośrednictwem dziennika zdarzeń przychodzących programu Personal Firewall (aby uzyskać więcej informacji, patrz *Informacje o stronie Zdarzenia przychodzące* na stronie 23).
- Kliknij przycisk **Śledź ten adres**, aby przeprowadzić wizualne śledzenie adresów IP dla tego zdarzenia za pomocą aplikacji Visual Trace.
- Kliknij przycisk **Zabroń dostępu temu adresowi**, aby zablokować dostęp do komputera z danego adresu. Adres zostanie dodany do listy zabronionych adresów IP.
- Kliknij przycisk **Ufaj temu adresowi**, aby zezwolić na dostęp do komputera z danego adresu IP.
- Kliknij polecenie **Kontynuuj wykonywaną czynność**, jeśli nie chcesz podejmować dalszych działań poza tymi, które zostały już podjęte przez program Personal Firewall.

Skorowidz

A

adresy IP
- informacje, 24
- ufanie, 30
- zabranianie, 30

alerty
- Aplikacja żąda dostępu do Internetu, 34
- Aplikacja żąda dostępu w roli serwera, 35
- Nowa aplikacja z przyznanym dostępem, 40
- Zablokowano aplikację internetową, 34
- Zablokowano próbę połączenia, 42
- Zmodyfikowano aplikację, 34

Aplikacje internetowe
- informacje, 21
- przyznawanie dostępu i blokowanie, 22
- zmiana reguł aplikacji, 22

Automatyczne aktualizacje systemu Windows, 35

D

domyślna zapora, ustawianie, 10

Dziennik zdarzeń
- informacje, 23
- przeglądanie, 32
- zarządzanie, 32

H

HackerWatch.org
- porada, 29
- raportowanie zdarzenia do, 29
- rejestrowanie, 29

K

Karta Szybki start, iii

M

McAfee SecurityCenter, 13

N

nowe funkcje, 7

O

odinstalowywanie
- zapory innych firm, 9

śledzenie zdarzenia, 28

P

Personal Firewall
- korzystanie, 15
- testowanie, 12

Podsumowanie, strona, 15

R

raportowanie zdarzenia, 29

T

testowanie programu Personal Firewall, 12

W

wprowadzenie, 7

wymagania systemowe, 9

wyświetlanie zdarzeń w dzienniku zdarzeń, 26

Z

Zapora systemu Windows, 10

zdarzenia
- archiwizowanie dziennika zdarzeń, 32
- czyszczenie dziennika zdarzeń, 33
- eksportowanie, 33
- informacje, 23
- kopiowanie, 33
- odpowiadanie na, 28
- śledzenie
  - omówienie, 23
  - przeglądanie zarchiwizowanych dzienników zdarzeń, 32

pętlowe, 24
pochodzące z komputerów w sieci LAN, 25
pochodzące z prywatnych adresów IP, 26
porada HackerWatch.org, 29
raportowanie, 29
usuwanie, 34
więcej informacji, 29
wyświetlanie
    wszystkie, 27
    z bieżącego dnia, 26
    z bieżącego tygodnia, 27
    z jednego adresu, 27
    z jednego dnia, 27
    z tymi samymi informacjami o zdarzeniu, 28
z adresu 0.0.0.0, 24
z adresu 127.0.0.1, 24