McAfee®

Total Protection 2007

Podręcznik użytkownika

Spis treści

McAfee Total Protection 7

McAfee SecurityCenter 9

Funkcje 10
Korzystanie z programu SecurityCenter 11
Nagłówek 11
Lewa kolumna 11
Okienko główne 12
Jak działają ikony programu SecurityCenter 13
Jak działa stan ochrony 15
Naprawianie problemów dotyczących ochrony 21
Wyświetlanie informacji dotyczących programu SecurityCenter 22
Korzystanie z Menu zaawansowanego 23
Konfigurowanie opcji programu SecurityCenter 25
Konfigurowanie stanu ochrony 26
Konfigurowanie opcji użytkowników 27
Konfigurowanie opcji aktualizacji 31
Konfigurowanie opcji alertów 36
Wykonywanie typowych zadań 39
Wykonywanie typowych zadań 39
Przeglądanie ostatnich zdarzeń 40
Automatyczne przeprowadzanie konserwacji komputera 41
Ręczne przeprowadzanie konserwacji komputera 42
Zarządzanie siecią 43
Uzyskiwanie dodatkowych informacji na temat wirusów 44

McAfee QuickClean 45

Omówienie funkcji programu QuickClean 46
Funkcje 46
Oczyszczanie komputera 47
Korzystanie z programu QuickClean 49

McAfee Shredder 51

Omówienie funkcji programu Shredder 52
Funkcje 52
Wymazywanie niepożądanych plików za pomocą programu Shredder 53
Korzystanie z programu Shredder 54

McAfee Network Manager 55

Funkcje....56
Jak działają ikony programu Network Manager....57
Konfigurowanie zarządzanej sieci....59
Praca z mapą sieci....60
Dołączanie do sieci zarządzanej....63
Zdalne zarządzanie siecią....67
Monitorowanie stanu i uprawnień....68
Naprawa luk w zabezpieczeniach....71

McAfee VirusScan 73

Funkcje....74
Zarządzanie ochroną przed wirusami....77
Korzystanie z ochrony przed wirusami....78
Korzystanie z ochrony przed oprogramowaniem szpiegującym....82
Korzystanie z programów SystemGuard....83
Korzystanie ze skanowania skryptów....93
Korzystanie z ochrony poczty e-mail....94
Korzystanie z ochrony wiadomości błyskawicznych....96
Ręczne skanowanie komputera....97
Skanowanie ręczne....98
Administrowanie programem VirusScan....103
Zarządzanie listami elementów zaufanych....104
Zarządzanie poddanymi kwarantannie programami, plikami cookie i innymi plikami....105
Przeglądanie ostatnich zdarzeń i dzienników....107
Automatyczne przesyłanie anonimowych informacji....108
Jak działa system generowania alertów zabezpieczeń....109
Dodatkowa pomoc....111
Często zadawane pytania....112
Rozwiązywanie problemów....114

McAfee Personal Firewall 117

Funkcje....118
Uruchamianie zapory....121
Uruchamianie zapory....121
Zatrzymywanie zapory....122
Praca z alertami....123
Informacje o alertach....124
Zarządzanie alertami informacyjnymi....127
Wyświetlanie alertów podczas korzystania z gier....127
Ukrywanie alertów informacyjnych....127
Konfigurowanie ochrony przy użyciu zapory....129
Zarządzanie poziomami zabezpieczeń zapory....130
Konfigurowanie inteligentnych zaleceń dla alertów....134
Optymalizacja zabezpieczeń programu Firewall....136
Blokowanie i odblokowywanie zapory....139
Zarządzanie programami i uprawnieniami....141
Przyznawanie programom dostępu do Internetu....142
Przyznawanie programom praw dostępu tylko dla połączeń wychodzących....145

Blokowanie dostępu programów do Internetu 147
Usuwanie praw dostępu programów 149
Informacje o programach 150
Zarządzanie usługami systemowymi 153
Konfigurowanie portów usług systemowych 154
Zarządzanie połączeniami z komputerem 157
Udzielanie zaufania połączeniom z komputerami 158
Blokowanie połączeń z komputerami 163
Rejestrowanie, monitorowanie i analiza 169
Rejestrowanie zdarzeń 170
Praca ze statystykami 174
Śledzenie ruchu internetowego 175
Monitorowanie ruchu internetowego 179
Informacje o bezpieczeństwie internetowym 183
Uruchamianie samouczka witryny HackerWatch 184

McAfee SpamKiller 185

Funkcje 186
Obsługa kont pocztowych w sieci Web 189
Dodawanie kont poczty internetowej 190
Modyfikowanie ustawień kont poczty internetowej 192
Usuwanie kont poczty internetowej 194
Zarządzanie filtrowaniem poczty internetowej 195
Zarządzanie listą znajomych 197
Omówienie zarządzania listą znajomych 198
Automatyczna aktualizacja znajomych 200
Modyfikowanie opcji filtrowania 203
Modyfikowanie ustawień filtrowania wiadomości e-mail 204
Zmiana sposobu przetwarzania wiadomości zidentyfikowanych jako spam 206
Filtrowanie wiadomości zawierających określone zestawy znaków 207
Zgłaszanie wiadomości uznanych za spam 208
Zarządzanie filtrami osobistymi 209
Omówienie zarządzania filtrami osobistymi 210
Korzystanie z wyrażeń regularnych 213
Obsługa programu SpamKiller 219
Zarządzanie ochroną przed spamem 220
Korzystanie z pasków narzędzi 221
Konfigurowanie ochrony przed atakami typu „phishing” 223
Wyłączanie lub włączanie ochrony przed atakami typu „phishing” 224
Modyfikowanie ustawień filtrowania ataków typu „phishing” 225
Dodatkowa pomoc 227
Często zadawane pytania 228

McAfee Privacy Service 231

Funkcje 232
Konfigurowanie ochrony rodzicielskiej 233
Konfigurowanie grupy klasyfikacji zawartości użytkownika 234
Ustawianie poziomu blokowania plików cookie użytkownika 236
Ustawianie internetowych limitów czasu użytkownika 244
Blokowanie witryn sieci Web 245
Dozwolone witryny sieci Web 249
Zezwalanie witrynom sieci Web na zapisywanie plików cookie 251

Blokowanie potencjalnie niepożądanych obrazów w sieci Web 253
Ochrona informacji w Internecie 255
Blokowanie reklam, wyskakujących okien i pluskiew internetowych 256
Blokowanie informacji osobistych 258
Ochrona haseł 259
Konfigurowanie Magazynu haseł 260

McAfee Data Backup 265

Funkcje 266
Archiwizowanie plików 267
Konfigurowanie opcji archiwizowania 268
Przeprowadzanie pełnych i szybkich archiwizacji 273
Praca ze zarchiwizowanymi plikami 277
Używanie eksploratora archiwum lokalnego 278
Przywracanie zarchiwizowanych plików 280
Zarządzanie archiwami 282

McAfee Wireless Network Security 283

Funkcje 284
Uruchamianie programu Wireless Network Security 286
Uruchamianie programu Wireless Network Security 286
Zatrzymywanie programu Wireless Network Security 287
Ochrona sieci bezprzewodowych 289
Konfigurowanie zabezpieczonych sieci bezprzewodowych 290
Dodawanie komputerów do chronionej sieci bezprzewodowej 302
Administrowanie sieciami bezprzewodowymi 307
Zarządzanie sieciami bezprzewodowymi 308
Zarządzanie zabezpieczeniami sieci bezprzewodowych 319
Konfigurowanie ustawień zabezpieczeń 320
Administrowanie kluczami sieciowymi 325
Monitorowanie sieci bezprzewodowych 335
Monitorowanie połączeń w sieci bezprzewodowej 336
Monitorowanie chronionych sieci bezprzewodowych 341
Rozwiązywanie problemów 347

McAfee EasyNetwork 363

Funkcje 364
Konfigurowanie programu EasyNetwork 365
Uruchamianie programu EasyNetwork 366
Dołączanie do sieci zarządzanej 367
Opuszczanie zarządzanej sieci 371
Udostępnianie i wysyłanie plików 373
Udostępnianie plików 374
Wysyłanie plików do innych komputerów 377
Udostępnianie drukarek 379
Praca z udostępnianymi drukarkami 380

Referencja **383**

Słownik **384**

Informacje o firmie McAfee **401**

Copyright 402

Indeks **403**

ROZDZIAŁ 1

McAfee Total Protection

Pakiet McAfee Total Protection Suite zapewnia kompleksową ochronę tożsamości, komputera i sieci bezprzewodowej oraz zautomatyzowane tworzenie kopii zapasowych ważnych plików. Możesz bezstresowo korzystać z Internetu — przeglądać sieć Web, robić zakupy, realizować transakcje bankowe, wysyłać i odbierać pocztę e-mail oraz wiadomości błyskawiczne — wiedząc, że oprogramowanie McAfee jest zawsze aktywne, zawsze aktualne i zawsze zapewnia ochronę. Niezawodna ochrona oprogramowania McAfee eliminuje zagrożenia i automatycznie powstrzymuje hakerów, dzięki czemu komputer jest zawsze bezpieczny i w doskonałym stanie. Program McAfee Network Manager umożliwia monitorowanie i eliminowanie problemów z zabezpieczeniami na wszystkich komputerach domowych. McAfee EasyNetwork to narzędzie pozwalające na łatwe udostępnianie plików i drukarek w sieci. W zmodernizowanym programie McAfee SecurityCenter można w prosty sposób sprawdzać stan zabezpieczeń, przeprowadzać skanowanie w poszukiwaniu wirusów i oprogramowania szpiegującego oraz aktualizować zabezpieczenia. Subskrypcja zapewni automatyczne otrzymywanie najnowszego oprogramowania i aktualizacji.

Pakiet Total Protection zawiera następujące programy:

- SecurityCenter
- Privacy Service
- Shredder
- VirusScan
- Personal Firewall
- SpamKiller
- Data Backup
- Wireless Security
- Network Manager
- EasyNetwork
- SiteAdvisor

ROZDZIAŁ 2

McAfee SecurityCenter

Program McAfee SecurityCenter to łatwe w obsłudze środowisko, w którym użytkownicy programów firmy McAfee mogą uruchamiać, zarządzać i konfigurować swoje subskrypcje zabezpieczeń.

Program SecurityCenter jest także źródłem informacji o alertach wirusowych, produktach, pomocy technicznej i subskrypcjach, a także umożliwia szybki dostęp do narzędzi i wiadomości dostępnych w witrynie sieci Web firmy McAfee.

W tym rozdziale

Funkcje 10
Korzystanie z programu SecurityCenter 11
Konfigurowanie opcji programu SecurityCenter 25
Wykonywanie typowych zadań 39

Funkcje

Program McAfee SecurityCenter oferuje następujące nowe funkcje i korzyści:

Nowy sposób przedstawiania informacji o stanie ochrony

Łatwe przeglądanie informacji o stanie zabezpieczeń komputera, sprawdzanie aktualizacji i usuwanie potencjalnych źródeł zagrożeń.

Ciągłe aktualizacje i uaktualnienia

Automatyczne instalowanie codziennych aktualizacji. Gdy tylko dostępna staje się nowa wersja produktu McAfee, użytkownik w okresie subskrypcji otrzymuje ją bezpłatnie, co zapewnia skuteczną ochronę przed najnowszymi zagrożeniami.

Wyświetlanie na bieżąco alertów

Alerty zabezpieczeń powiadamiają o epidemiach wirusowych i zagrożeniach bezpieczeństwa oraz udostępniają opcje reagowania w celu usunięcia, zneutralizowania lub uzyskania dodatkowych informacji na temat zagrożenia.

Wygodne odnawianie subskrypcji

Firma McAfee oferuje różne opcje odnawiania subskrypcji, a tym samym zapewnienia ciągłości ochrony.

Narzędzia optymalizujące wydajność

Dla utrzymania komputera w stanie najwyższej sprawności należy usuwać nieużywane pliki, defragmentować pliki używane i przywracać system do poprzedniego stanu.

Prawdziwa pomoc online

Pomoc ekspertów firmy McAfee w dziedzinie bezpieczeństwa komputerów można uzyskać przez czat internetowy, pocztę e-mail i telefon.

Bezpieczne przeglądanie Internetu

Zainstalowany dodatek plug-in McAfee SiteAdvisor do przeglądarki pomaga chronić przed oprogramowaniem szpiegującym, spamem, wirusami oraz próbami oszustw za pośrednictwem Internetu dzięki ocenie witryn sieci Web odwiedzanych przez użytkownika, wyświetlanej również w wynikach wyszukiwania. Można obejrzeć szczegółowe oceny, które uzyskała dana witryna, dotyczące wysyłania poczty e-mail, plików do pobrania, powiązań z innymi witrynami sieciowymi, jak również takich uciążliwych elementów jak wyskakujące okna czy śledzące pliki cookie innych firm.

ROZDZIAŁ 3

Korzystanie z programu SecurityCenter

Program SecurityCenter można uruchomić za pomocą ikony programu McAfee SecurityCenter znajdującej się w obszarze powiadomień systemu Windows na prawym końcu paska zadań lub z pulpitu systemu Windows.

Po otwarciu programu SecurityCenter okienko Początek wyświetla stan zabezpieczeń komputera oraz umożliwia szybki dostęp do funkcji aktualizacji, skanowania (jeśli zainstalowany jest program McAfee VirusScan) oraz innych typowych zadań:

Nagłówek

Pomoc

Umożliwia przeglądanie pliku pomocy.

Lewa kolumna

Aktualizuj

Umożliwia aktualizację produktu. Dzięki temu komputer jest chroniony przed najnowszymi zagrożeniami.

Funkcja skanowania

Jeśli zainstalowany jest program McAfee VirusScan, można wykonywać ręczne skanowanie komputera.

Typowe zadania

Umożliwia wykonywanie typowych zadań, takich jak przejście do okienka Początek, wyświetlanie ostatnich zdarzeń, zarządzanie siecią komputerową (jeśli komputer obsługuje funkcje zarządzania używane w tej sieci) oraz konserwacja komputera. Jeśli został zainstalowany program McAfee Data Backup, można również tworzyć kopie zapasowe danych.

Zainstalowane składniki

Umożliwia wyświetlenie usług zabezpieczeń, które chronią bezpieczeństwo komputera.

Okienko główne

Stan ochrony

W obszarze **Czy jestem chroniony?** wyświetlany jest ogólny stan ochrony komputera. Poniżej można wyświetlić szczegółowe informacje o stanie według kategorii lub typu.

SecurityCenter — informacje

Umożliwia sprawdzenie, kiedy ostatni raz był aktualizowany komputer, kiedy przeprowadzono ostatnie skanowanie (jeśli program McAfee VirusScan jest zainstalowany) oraz kiedy wygaśnie subskrypcja.

W tym rozdziale

Jak działają ikony programu SecurityCenter 13
Jak działa stan ochrony 15
Naprawianie problemów dotyczących ochrony 21
Wyświetlanie informacji dotyczących programu SecurityCenter 22
Korzystanie z Menu zaawansowanego 23

Jak działają ikony programu SecurityCenter

Ikony programu SecurityCenter są wyświetlane w obszarze powiadomień systemu Windows na prawym końcu paska zadań. Służą do informowania, czy komputer jest w pełni chroniony, wyświetlania stanu uruchomionego zadania skanowania (jeśli program McAfee VirusScan jest zainstalowany), sprawdzania dostępności aktualizacji, przeglądania ostatnich zdarzeń, wykonywania czynności w ramach konserwacji komputera oraz uzyskiwania dostępu do pomocy w witrynie sieci Web firmy McAfee.

Otwieranie programu SecurityCenter i korzystanie z dodatkowych funkcji

Po uruchomieniu programu SecurityCenter w obszarze powiadomień systemu Windows na prawym końcu paska zadań zostaje wyświetlona ikona (M) programu SecurityCenter.

Aby otworzyć program SecurityCenter lub skorzystać z dodatkowych funkcji:

- Kliknij prawym przyciskiem myszy główną ikonę programu SecurityCenter, a następnie kliknij jedno z następujących poleceń:
  - Otwórz program SecurityCenter
  - Aktualizacje
  - Szybkie łącza

    Podmenu zawiera łącza do okienek Początek, Przeglądaj ostatnie zdarzenia, Zarządzaj siecią, Konserwacja komputera oraz Data Backup (jeśli jest zainstalowany).
  - Weryfikuj subskrypcję

    (Ten element jest wyświetlany, kiedy wygaśnie co najmniej jedna subskrypcja produktu).
  - Centrum uaktualnień
  - Biuro obsługi klienta

Sprawdzanie stanu ochrony komputera

Jeśli komputer nie jest w pełni chroniony, w obszarze powiadomień systemu Windows na prawym końcu paska zadań jest wyświetlana ikona stanu ochrony. W zależności od stanu ochrony może być ona czerwona lub żółta.

Aby sprawdzić stan ochrony komputera:

- Kliknij ikonę stanu ochrony, aby otworzyć program SecurityCenter i naprawić problemy, które się pojawiły.

Sprawdzanie stanu aktualizacji

Podczas sprawdzania aktualizacji w obszarze powiadomień systemu Windows na prawym końcu paska zadań zostaje wyświetlona ikona aktualizacji  .

Aby sprawdzić stan aktualizacji:

- Wskaż ikonę aktualizacji, aby wyświetlić stan aktualizacji w etykiecie narzędzia.

Jak działa stan ochrony

Ogólny stan ochrony komputera jest widoczny w sekcji **Czy jestem chroniony?** programu SecurityCenter.

Stan ochrony jest wyświetlany w celu powiadamiania użytkownika, że komputer jest w pełni chroniony przed najnowszymi zagrożeniami bezpieczeństwa, lub sygnalizowania problemów wymagających uwagi i wskazania sposobów ich rozwiązania. Jeśli problem dotyczy więcej niż jednej kategorii, po jego naprawieniu stan pełnej ochrony może być przywrócony dla kilku kategorii.

Na stan ochrony wpływają między innymi następujące czynniki: zewnętrzne zagrożenia bezpieczeństwa, programy zabezpieczające zainstalowane na komputerze, programy łączące się z Internetem oraz sposób konfiguracji tych programów zabezpieczających i internetowych.

Domyślnie jeśli funkcje Ochrona przed spamem lub Blokowanie zawartości nie są zainstalowane, problemy niekrytyczne, są automatycznie ignorowane i nie są śledzone w ramach badania ogólnego stanu ochrony. Jeśli jednak przy danym problemie występuje łącze **Ignoruj**, użytkownik może wybrać zignorowanie tego problemu, jeśli na pewno nie chce go naprawiać.

Czy jestem chroniony?

Sprawdź ogólny poziom ochrony komputera w obszarze **Czy jestem chroniony?** programu SecurityCenter:

- **Tak** — oznacza, że komputer jest w pełni chroniony (kolor zielony).
- **Nie** — oznacza, że komputer jest częściowo chroniony (kolor żółty) lub niechroniony (kolor czerwony).

Aby automatycznie naprawić większość problemów dotyczących ochrony, kliknij przycisk **Napraw** wyświetlany obok stanu ochrony. Jeśli jednak jeden lub kilka problemów się powtarza i konieczna jest reakcja użytkownika, kliknij łącze dotyczące danego problemu w celu wykonania proponowanego działania.

Jak działają kategorie i typy ochrony

W obszarze **Czy jestem chroniony?** w programie SecurityCenter można wyświetlać szczegółowe informacje o stanie według następujących kategorii i typów ochrony:

- Komputer i pliki
- Internet i sieć
- Poczta i wiadomości błyskawiczne
- Funkcje ochrony rodzicielskiej

Typy ochrony wyświetlane w programie SecurityCenter zależą od zainstalowanych produktów. Na przykład typ ochrony PC Health (stan komputera) jest wyświetlany, jeśli zainstalowano oprogramowanie McAfee Data Backup.

Jeśli nie występują żadne problemy dotyczące danej kategorii, jej stan jest oznaczony kolorem zielonym. Po kliknięciu kategorii oznaczonej kolorem zielonym po prawej stronie zostanie wyświetlona lista włączonych typów ochrony oraz lista już zignorowanych problemów. Jeśli nie występują żadne problemy, zamiast problemów wyświetlane są zalecenia dotyczące wirusów. Można również kliknąć przycisk **Konfiguruj**, aby zmienić opcje dotyczące danej kategorii.

Jeśli stan wszystkich typów ochrony w obrębie danej kategorii jest oznaczony kolorem zielonym, wtedy stan tej kategorii jest także oznaczony kolorem zielonym. Podobnie, jeśli stan wszystkich kategorii ochrony jest oznaczony kolorem zielonym, ogólny stan ochrony będzie również oznaczony kolorem zielonym.

Jeśli stan niektórych kategorii ochrony jest sygnalizowany kolorem żółtym lub czerwonym, można rozwiązać odpowiadające im problemy dotyczące ochrony poprzez naprawienie tych problemów lub ich zignorowanie. To działanie zmieni stan kategorii na oznaczony kolorem zielonym.

Jak działa ochrona komputera i plików

Kategoria ochrony komputera i plików obejmuje następujące typy ochrony:

- **Ochrona przed wirusami** — Ochrona przez skanowanie w czasie rzeczywistym zabezpiecza komputer przed wirusami, robakami, końmi trojańskimi, podejrzanymi skryptami, atakami hybrydowymi i innymi zagrożeniami. Funkcje tej ochrony skanują automatycznie pliki i próbują je wyczyścić (włącznie ze skompresowanymi plikami .exe, sektorem rozruchowym, pamięcią i krytycznymi plikami), podczas gdy z plików tych korzysta komputer lub użytkownik.
- **Ochrona przed oprogramowaniem szpiegującym** — Funkcje tej ochrony szybko wykrywają, blokują i usuwają oprogramowanie szpiegujące, reklamowe i inne potencjalnie niepożądane programy, które zbierają i wysyłają prywatne dane użytkowników bez ich zgody.
- **Aplikacje SystemGuards** — Programy SystemGuard wykrywają zmiany w komputerze i powiadamiają użytkownika w chwili wystąpienia zmian. Następnie użytkownik może przejrzeć te zmiany i podjąć decyzję, czy na nie pozwolić.
- **Ochrona systemu Windows** — Ochrona systemu Windows udostępnia informacje o stanie usługi Windows Update na komputerze użytkownika. Jeśli program VirusScan jest zainstalowany, dostępna jest również ochrona przed przepełnieniem buforu.

Jednym z czynników wpływających na zabezpieczenie komputera i plików są zewnętrzne zagrożenia wirusowe. Na przykład: czy zainstalowane oprogramowanie antywirusowe zapewnia skuteczną ochronę w przypadku pojawienia się epidemii wirusowej? Innymi czynnikami zapewniającymi ochronę komputera przed najnowszymi zagrożeniami są: konfiguracja oprogramowania antywirusowego oraz działanie opcji jego bieżącej aktualizacji za pomocą aktualnych plików sygnatur wykrywania.

Otwieranie okienka konfiguracji Komputer i pliki

Jeśli nie występują żadne problemy w kategorii **Komputer i pliki**, okienko konfiguracji można otworzyć, korzystając z okienka informacyjnego.

Aby otworzyć okienko konfiguracji Komputer i pliki:

1. W okienku Początek kliknij kategorię **Komputer i pliki**.
2. W prawym okienku kliknij przycisk **Konfiguruj**.

Jak działają zabezpieczenia Internetu i sieci

Kategoria ochrony Internet i sieć obejmuje następujące typy ochrony:

- **Ochrona przy użyciu zapory** — Zapora chroni komputer przed włamaniami i niepożądanym ruchem sieciowym. Pomaga w zarządzaniu przychodzącymi i wychodzącymi połączeniami z Internetem.
- **Ochrona sieci bezprzewodowej** — Zapewnia ochronę domowej sieci bezprzewodowej przed włamaniami i przechwyceniem danych. Jeśli jednak użytkownik jest aktualnie podłączony do zewnętrznej sieci bezprzewodowej, poziom ochrony może być różny w zależności od poziomu zabezpieczeń tej sieci.
- **Ochrona przeglądania sieci Web** — Ochrona przeglądania sieci Web umożliwia ukrywanie reklam, wyskakujących okienek i pluskiew internetowych na komputerze podczas przeglądania sieci Web.
- **Ochrona przed atakami typu „phishing”** — Funkcja ochrony przed atakami typu „phishing” pomaga blokować fałszywe witryny sieci Web gromadzące informacje osobiste za pośrednictwem m.in. hiperłączy przesyłanych w wiadomościach e-mail i wiadomościach błyskawicznych czy wyskakujących okien.
- **Ochrona informacji osobistych** — Ochrona informacji osobistych umożliwia blokowanie rozpowszechniania poufnych i tajnych informacji przez Internet.

Otwieranie okienka konfiguracji Internet i sieć

Jeśli nie występują żadne problemy w kategorii **Internet i sieć**, okienko konfiguracji można otworzyć z okienka informacyjnego.

Aby otworzyć okienko konfiguracji Internet i sieć:

1. W okienku Początek kliknij kategorię **Internet i sieć**.
2. W prawym okienku kliknij przycisk **Konfiguruj**.

Jak działa ochrona poczty e-mail i wiadomości błyskawicznych

Kategoria ochrony poczty e-mail i wiadomości błyskawicznych obejmuje następujące typy ochrony:

- **Ochrona poczty e-mail** — Ochrona poczty e-mail automatycznie skanuje i próbuje wyczyścić wirusy, oprogramowanie szpiegujące oraz potencjalne zagrożenia w przychodzących i wychodzących wiadomościach e-mail i ich załącznikach.
- **Ochrona przed spamem** — Funkcja ochrony przed spamem pomaga zatrzymać niepożądane wiadomości e-mail przed wtargnięciem do skrzynki odbiorczej.
- **Ochrona wiadomości błyskawicznych** — Ochrona wiadomości błyskawicznych automatycznie skanuje i próbuje wyczyścić wirusy, oprogramowanie szpiegujące oraz potencjalne zagrożenia w załącznikach przychodzących wiadomości błyskawicznych. Blokuje ona także klienty wiadomości błyskawicznych przed wymianą niepożądanej zawartości lub informacji osobistych przez Internet.
- **Bezpieczne przeglądanie Internetu** — Jeśli zainstalowano dodatek plug-in McAfee SiteAdvisor do przeglądarki, pomaga on chronić przed oprogramowaniem szpiegującym, spamem, wirusami oraz próbami oszustw za pośrednictwem Internetu. Jest to możliwe dzięki ocenie witryn sieci Web — tych odwiedzanych przez użytkownika i tych zwracanych w wynikach wyszukiwania. Można wyświetlić szczegółowe oceny, które uzyskała dana witryna, dotyczące wysyłania poczty e-mail, pobierania, koalicji z innymi witrynami sieciowymi, jak również takich problematycznych elementów jak wyskakujące okna czy śledzące pliki cookie innych firm.

Otwieranie okienka konfiguracji poczty e-mail i wiadomości błyskawicznych

Jeśli nie występują żadne problemy w kategorii **Poczta e-mail i wiadomości błyskawiczne**, okienko konfiguracji można otworzyć z okienka informacyjnego.

Aby otworzyć okienko konfiguracji poczty e-mail i wiadomości błyskawicznych:

1. W okienku Początek kliknij kategorię **Poczta e-mail i wiadomości błyskawiczne**.
2. W prawym okienku kliknij przycisk **Konfiguruj**.

Jak działają Funkcje ochrony rodzicielskiej

Kategoria ochrony Funkcje ochrony rodzicielskiej obejmuje następujący typ ochrony:

- **Funkcje ochrony rodzicielskiej** — Blokowanie zawartości zapobiega przeglądaniu przez użytkowników niepożądanej zawartości internetowej dzięki blokowaniu potencjalnie szkodliwych witryn sieci Web. Można również monitorować i ograniczać aktywność użytkowników w Internecie oraz sposób korzystania z niego.

Otwieranie okienka konfiguracji funkcji ochrony rodzicielskiej

Jeśli nie występują żadne problemy w kategorii **Funkcje ochrony rodzicielskiej**, okienko konfiguracji można otworzyć z okienka informacyjnego.

Aby otworzyć okienko konfiguracji funkcji ochrony rodzicielskiej:

1. W okienku Początek kliknij kategorię **Funkcje ochrony rodzicielskiej**.
2. W prawym okienku kliknij przycisk **Konfiguruj**.

Naprawianie problemów dotyczących ochrony

Większość problemów dotyczących ochrony może być naprawiona automatycznie. Jeśli jednak jeden lub kilka problemów powtarza się, musi je rozwiązać użytkownik.

Automatyczne naprawianie problemów dotyczących ochrony

Większość problemów dotyczących ochrony może być naprawiona automatycznie.

Aby automatycznie naprawić problemy dotyczące ochrony:

- Kliknij przycisk **Napraw** wyświetlany obok stanu ochrony.

Ręczne naprawianie problemów dotyczących ochrony

Jeśli jeden lub więcej problemów nie zostało rozwiązanych automatycznie, kliknij łącze dotyczące danego problemu w celu wykonania proponowanego działania.

Aby ręcznie naprawić problemy dotyczące ochrony:

- Wykonaj dowolną z następujących czynności:
  - Jeśli nie wykonano pełnego skanowania komputera w ciągu ostatnich 30 dni, kliknij przycisk **Skanuj** znajdujący się po lewej stronie głównej sekcji wyświetlającej stan ochrony, aby wykonać skanowanie ręczne. (Ten element jest dostępny, jeśli zainstalowano program McAfee VirusScan).
  - Jeśli pliki sygnatur wykrywania (DAT) są nieaktualne, kliknij przycisk **Aktualizuj** znajdujący się po lewej stronie głównej sekcji wyświetlającej stan ochrony w celu aktualizacji ochrony komputera.
  - Jeśli program nie jest zainstalowany, kliknij łącze **Zadbaj o pełną ochronę**, aby go zainstalować.
  - Jeśli w programie brakuje niektórych składników, zainstaluj go ponownie.
  - Jeśli zapewnienie pełnej ochrony wymaga zarejestrowania programu, kliknij łącze **Zarejestruj teraz**, aby go zarejestrować. (Ten element jest wyświetlany, kiedy upłynie ważność co najmniej jednego programu).
  - Jeśli upłynęła ważność programu, kliknij łącze **Sprawdź moją subskrypcję teraz**, aby sprawdzić stan konta. (Ten element jest wyświetlany, kiedy upłynie ważność co najmniej jednego programu).

Wyświetlanie informacji dotyczących programu SecurityCenter

Znajdująca się u dołu okienka stanu ochrony sekcja SecurityCenter — informacje umożliwia dostęp do opcji programu SecurityCenter oraz wyświetla informacje dotyczące ostatniej aktualizacji, ostatniego skanowania (jeśli zainstalowano program McAfee VirusScan) oraz daty wygaśnięcia subskrypcji produktów firmy McAfee.

Otwieranie okienka konfiguracji programu SecurityCenter

Dla wygody użytkownika do otwarcia okienka konfiguracji programu SecurityCenter w celu zmiany opcji można skorzystać z okienka Początek.

Aby otworzyć okienko konfiguracji programu SecurityCenter:

- W okienku Początek w obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.

Wyświetlanie informacji o zainstalowanych produktach

Można wyświetlić listę zainstalowanych produktów informującą o numerach ich wersji oraz datach ostatnich aktualizacji.

Aby wyświetlić informacje o zainstalowanych produktach firmy McAfee:

- W okienku Początek w obszarze **SecurityCenter — informacje** kliknij polecenie **Wyświetl szczegóły**, aby otworzyć okno z informacjami o produktach.

Korzystanie z Menu zaawansowanego

Po pierwszym otwarciu programu SecurityCenter w jego lewej kolumnie zostanie wyświetlone Menu podstawowe. Zaawansowani użytkownicy mogą kliknąć polecenie **Menu zaawansowane**, aby na jego miejscu otworzyć bardziej szczegółowe menu poleceń. Dla wygody użytkownika przy każdym kolejnym otwarciu program SecurityCenter jest wyświetlany z ostatnio używanym menu.

Menu zaawansowane składa się z następujących elementów:

- Strona główna
- Raporty i dzienniki (udostępnia listę ostatnich zdarzeń oraz dzienniki według typu przechowujące informacje z ostatnich 30, 60 i 90 dni).
- Konfiguruj
- Przywróć
- Narzędzia

ROZDZIAŁ 4

Konfigurowanie opcji programu SecurityCenter

Program SecurityCenter wyświetla ogólny stan ochrony komputera, umożliwia tworzenie kont użytkowników oprogramowania firmy McAfee, automatycznie instaluje najnowsze aktualizacje produktu oraz automatycznie powiadamia użytkownika za pomocą alertów i dźwięków o wystąpieniu powszechnych epidemii wirusowych, zagrożeniach bezpieczeństwa i aktualizacjach produktu.

W okienku konfiguracji programu SecurityCenter można zmienić opcje programu SecurityCenter dotyczące następujących funkcji:

- Stan ochrony
- Użytkownicy
- Automatyczne aktualizacje
- Alerty

W tym rozdziale

Konfigurowanie stanu ochrony 26
Konfigurowanie opcji użytkowników 27
Konfigurowanie opcji aktualizacji 31
Konfigurowanie opcji alertów 36

Konfigurowanie stanu ochrony

Ogólny stan ochrony komputera jest widoczny w sekcji **Czy jestem chroniony?** programu SecurityCenter.

Stan ochrony jest wyświetlany w celu powiadamiania użytkownika, że komputer jest w pełni chroniony przed najnowszymi zagrożeniami bezpieczeństwa, a także w celu sygnalizowania problemów wymagających uwagi i wskazania sposobów ich rozwiązania.

Domyślnie, jeśli funkcje Ochrona przed spamem lub Blokowanie zawartości nie są zainstalowane, problemy niekrytyczne są automatycznie ignorowane i nie są śledzone w ramach badania ogólnego stanu ochrony. Jeśli jednak przy danym problemie występuje łącze **Ignoruj**, użytkownik może wybrać zignorowanie tego problemu, jeśli na pewno nie chce go naprawiać. Jeśli w późniejszym czasie zdecyduje się naprawić wcześniej zignorowany problem, może uwzględnić go w śledzeniu w ramach badania stanu ochrony.

Konfigurowanie ignorowanych problemów

Użytkownik może uwzględniać problemy w śledzeniu lub je z niego wyłączać w ramach badania ogólnego stanu ochrony komputera. Jeśli przy danym problemie występuje łącze **Ignoruj**, użytkownik może wybrać zignorowanie tego problemu, jeśli na pewno nie chce go naprawiać. Jeśli w późniejszym czasie zdecyduje się naprawić wcześniej zignorowany problem, może uwzględnić go w śledzeniu w ramach badania stanu ochrony.

Aby skonfigurować ignorowane problemy:

1. W obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
2. Kliknij strzałkę obok kategorii **Stan ochrony**, aby ją rozwinąć, a następnie kliknij przycisk **Zaawansowane**.
3. W okienku Zignorowane problemy wykonaj jedną z następujących czynności:
   - Aby sprawdzać wcześniej zignorowane problemy w ramach badania stanu ochrony, usuń zaznaczenie ich pól wyboru.
   - Aby pomijać określone problemy w ramach badania stanu ochrony, zaznacz ich pola wyboru.
4. Kliknij przycisk **OK**.

Konfigurowanie opcji użytkowników

Jeżeli używane są programy firmy McAfee, które wymagają uprawnień użytkowników, uprawnienia te domyślnie odnoszą się do kont użytkowników systemu Windows na tym komputerze. Aby uprościć zarządzanie użytkownikami tych programów, można w każdej chwili przełączyć się na używanie kont użytkowników oprogramowania firmy McAfee.

W przypadku przełączenia się na używanie kont użytkowników oprogramowania firmy McAfee wszystkie istniejące nazwy użytkowników oraz uprawnienia z programu Funkcje ochrony rodzicielskiej zostaną automatycznie zaimportowane. Jednak przy pierwszym przełączeniu się należy utworzyć konto administratora. Następnie można rozpocząć tworzenie i konfigurowanie innych kont użytkowników oprogramowania firmy McAfee.

Przełączanie się na używanie kont użytkowników oprogramowania firmy McAfee

Domyślnie użytkownik korzysta z kont użytkownika systemu Windows. Jednak przełączenie się na używanie kont użytkowników oprogramowania firmy McAfee pozwala uniknąć konieczności tworzenia dodatkowych kont użytkowników systemu Windows.

Aby przełączyć się na używanie kont użytkowników oprogramowania firmy McAfee:

1. W obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
2. Kliknij strzałkę obok kategorii **Użytkownicy**, aby ją rozwinąć, a następnie kliknij przycisk **Zaawansowane**.
3. Aby korzystać z kont użytkowników oprogramowania firmy McAfee, kliknij przycisk **Przełącz**.

W przypadku przełączenia się po raz pierwszy na używanie kont użytkowników oprogramowania firmy McAfee należy utworzyć konto administratora (strona 28).

Tworzenie konta administratora

Przy pierwszym przełączeniu się na używanie kont użytkowników oprogramowania firmy McAfee zostaje wyświetlony monit o utworzenie konta administratora.

Aby utworzyć konto administratora:

1. W polu **Hasło** wprowadź hasło, a następnie wprowadź je ponownie w polu **Potwierdź hasło**.
2. Wybierz z listy tajne pytanie umożliwiające odzyskanie hasła i w polu **Odpowiedź** wprowadź odpowiedź na nie.
3. Kliknij przycisk **Zastosuj**.

   Po zakończeniu ten typ konta użytkownika zostanie zaktualizowany w wyświetlanym okienku poprzez zaimportowanie wszystkich istniejących nazw użytkowników oraz uprawnień z programu Funkcje ochrony rodzicielskiej. Jeśli konta użytkowników są konfigurowane po raz pierwszy, zostanie wyświetlone okienko zarządzania użytkownikami.

Konfigurowanie opcji użytkowników

W przypadku przełączenia się na używanie kont użytkowników firmy McAfee wszystkie istniejące nazwy użytkowników oraz uprawnienia z programu Funkcje ochrony rodzicielskiej zostaną automatycznie zaimportowane. Jednak przy pierwszym przełączeniu się należy utworzyć konto administratora. Następnie można rozpocząć tworzenie i konfigurowanie innych kont użytkowników firmy McAfee.

Aby skonfigurować opcje użytkowników:

1. W obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
2. Kliknij strzałkę obok kategorii **Użytkownicy**, aby ją rozwinąć, a następnie kliknij przycisk **Zaawansowane**.
3. W obszarze **Konta użytkowników** kliknij przycisk **Dodaj**.
4. W polu **Nazwa użytkownika** wprowadź nazwę użytkownika.
5. W polu **Hasło** wprowadź hasło, a następnie wprowadź je ponownie w polu **Potwierdź hasło**.
6. Zaznacz pole wyboru **Użytkownik startowy**, jeśli ten nowy użytkownik ma być logowany automatycznie podczas uruchamiania programu SecurityCenter.
7. W obszarze **Typ konta użytkownika** wybierz typ konta dla tego użytkownika, a następnie kliknij przycisk **Utwórz**.

   Uwaga: Po utworzeniu konta użytkownika należy w obszarze Funkcje ochrony rodzicielskiej skonfigurować ustawienia dla użytkownika z ograniczonymi uprawnieniami.
8. Aby edytować hasło, automatyczne logowanie lub typ konta użytkownika, wybierz jego nazwę na liście i kliknij przycisk **Edytuj**.
9. Po zakończeniu kliknij przycisk **Zastosuj**.

Pobieranie hasła administratora

W przypadku zapomnienia hasła administratora, można je odzyskać.

Aby pobrać hasło administratora:

1. Kliknij prawym przyciskiem myszy ikonę (M) programu SecurityCenter, a następnie kliknij polecenie **Przełącz użytkownika**.
2. Na liście **Nazwa użytkownika** wybierz pozycję **Administrator**, a następnie kliknij przycisk **Nie pamiętam hasła**.
3. Wpisz odpowiedź na wyświetlone tajne pytanie wybrane podczas tworzenia konta administratora.
4. Kliknij przycisk **Prześlij**.

   Zostanie wyświetlone zapomniane hasło administratora.

Zmienianie hasła administratora

W przypadku problemów z zapamiętaniem hasła administratora lub podejrzeń, że zostało ono ujawnione nieuprawnionej osobie, można je zmienić.

Aby zmienić hasło administratora:

1. Kliknij prawym przyciskiem myszy ikonę (M) programu SecurityCenter, a następnie kliknij polecenie **Przełącz użytkownika**.
2. Na liście **Nazwa użytkownika** wybierz pozycję **Administrator**, a następnie kliknij przycisk **Zmień hasło**.
3. Wprowadź istniejące hasło w polu **Stare hasło**.
4. Wprowadź nowe hasło w polu **Hasło**, a następnie wprowadź je ponownie w polu **Potwierdź hasło**.
5. Kliknij przycisk **OK**.

Konfigurowanie opcji aktualizacji

Jeśli komputer jest połączony z Internetem, program SecurityCenter co cztery godziny automatycznie sprawdza aktualizacje wszystkich usług McAfee, a następnie automatycznie instaluje najnowsze aktualizacje produktu. Można jednak w dowolnej chwili ręcznie sprawdzić aktualizacje, korzystając z ikony programu SecurityCenter wyświetlanej w obszarze powiadomień systemu Windows na prawym końcu paska zadań.

Automatyczne sprawdzanie dostępności aktualizacji

Gdy komputer jest podłączony do Internetu, program SecurityCenter co cztery godziny automatycznie sprawdza, czy są dostępne aktualizacje. Program SecurityCenter można jednak skonfigurować w taki sposób, aby przed pobraniem lub zainstalowaniem aktualizacji było wyświetlane powiadomienie.

Aby automatycznie sprawdzać dostępność aktualizacji:

1. W obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
2. Kliknij strzałkę obok stanu **Opcja automatycznych aktualizacji jest włączona**, aby rozwinąć jego okienko, a następnie kliknij przycisk **Zaawansowane**.
3. W okienku Opcje aktualizacji zaznacz jedną z następujących opcji:
   - Instaluj aktualizacje automatycznie i powiadamiaj mnie, gdy produkt zostanie zaktualizowany (zalecane) (strona 32)
   - Pobieraj aktualizacje automatycznie i powiadamiaj mnie, gdy są gotowe do zainstalowania (strona 33)
   - Powiadamiaj przed pobieraniem jakichkolwiek aktualizacji (strona 33)
4. Kliknij przycisk **OK**.

Uwaga: W celu zapewnienia maksymalnej ochrony firma McAfee zaleca umożliwienie programowi SecurityCenter automatyczne sprawdzanie aktualizacji i ich instalowanie. W celu umożliwienia tylko ręcznej aktualizacji usług zabezpieczeń można wyłączyć automatyczne aktualizacje (strona 34).

Automatyczne pobieranie i instalowanie aktualizacji

W przypadku wybrania opcji **Instaluj aktualizacje automatycznie i powiadamiaj mnie, gdy usługi zostaną zaktualizowane (zalecane)** w sekcji Opcje aktualizacji programu SecurityCenter aktualizacje będą pobierane i instalowane automatycznie.

Automatyczne pobieranie aktualizacji

W przypadku zaznaczenia opcji **Pobieraj aktualizacje automatycznie i powiadamiaj mnie, gdy są gotowe do zainstalowania** w sekcji Opcje aktualizacji program SecurityCenter automatycznie pobiera aktualizacje, a następnie powiadamia użytkownika, gdy są gotowe do zainstalowania. Użytkownik może wybrać, czy aktualizacja ma zostać zainstalowana, czy odłożona na później (strona 34).

Aby zainstalować automatycznie pobraną aktualizację:

1. Kliknij opcję **Aktualizuj moje produkty teraz** w wyświetlanym alercie, a następnie kliknij przycisk **OK**.

   Przed rozpoczęciem pobierania aktualizacji po wyświetleniu monitu, należy zalogować się w witrynie sieci Web firmy McAfee, aby zweryfikować subskrypcję.

2. Po pomyślnej weryfikacji subskrypcji należy kliknąć przycisk **Aktualizuj** w okienku Aktualizacje w celu pobrania i zainstalowania aktualizacji. Jeśli subskrypcja wygasła, należy kliknąć przycisk **Odnów moją subskrypcję** w oknie alertu i postępować zgodnie z wyświetlanymi instrukcjami.

Uwaga: W niektórych przypadkach może zostać wyświetlony monit o ponowne uruchomienie komputera w celu dokończenia aktualizacji. Zapisz pracę i zamknij wszystkie programy przed ponownym uruchomieniem komputera.

Powiadamianie przed pobieraniem aktualizacji

W przypadku zaznaczenia opcji **Powiadamiaj przed pobieraniem aktualizacji** w okienku Opcje aktualizacji program SecurityCenter wyświetla powiadomienie przed pobraniem aktualizacji. Użytkownik może zdecydować się na pobranie aktualizacji usług zabezpieczeń i zainstalowanie ich w celu usunięcia zagrożenia atakiem.

Aby pobrać i zainstalować aktualizację:

1. Zaznacz opcję **Aktualizuj moje produkty teraz** w wyświetlanym alercie, a następnie kliknij przycisk **OK**.
2. W razie wyświetlenia monitu zaloguj się w witrynie sieci Web.

   Aktualizacja zostanie pobrana automatycznie.
3. Kliknij przycisk **OK**, gdy instalacja aktualizacji dobiegnie końca.

Uwaga: W niektórych przypadkach może zostać wyświetlony monit o ponowne uruchomienie komputera w celu dokończenia aktualizacji. Zapisz pracę i zamknij wszystkie programy przed ponownym uruchomieniem komputera.

Wyłączanie automatycznych aktualizacji

W celu zapewnienia maksymalnej ochrony firma McAfee zaleca, aby umożliwić programowi SecurityCenter automatyczne sprawdzanie oraz instalowanie aktualizacji. Jeśli jednak aktualizacje mają być wykonywane tylko ręcznie, można wyłączyć aktualizacje automatyczne.

Uwaga: Należy pamiętać o ręcznym sprawdzaniu aktualizacji (strona 35) co najmniej raz w tygodniu. W przypadku braku regularnego sprawdzania aktualizacji komputer nie będzie chroniony za pomocą najnowszych aktualizacji zabezpieczeń.

Aby wyłączyć automatyczne aktualizacje:

1. W obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
2. Kliknij strzałkę obok stanu **Opcja automatycznych aktualizacji jest włączona**, aby rozwinąć jego okienko.
3. Kliknij opcję **Wył.**
4. Kliknij przycisk **Tak**, aby potwierdzić zmianę.

   W nagłówku programu zostaną zaktualizowane informacje o stanie.

W przypadku nieprzeprowadzenia w ciągu siedmiu dni ręcznego sprawdzenia aktualizacji zostanie wyświetlony alert przypominający o konieczności sprawdzenia aktualizacji.

Odkładanie aktualizacji na później

W przypadku braku czasu na przeprowadzenie aktualizacji usług zabezpieczeń, gdy pojawia się alert, można zignorować alert lub poprosić o wyświetlenie go później:

Aby odłożyć aktualizację na później:

- Wykonaj jedną z poniższych czynności:
  - Zaznacz opcję **Przypomnij mi później** w wyświetlanym alercie, a następnie kliknij przycisk **OK**.
  - Zaznacz opcję **Zamknij ten alert**, a następnie kliknij przycisk **OK**, aby zamknąć okno alertu bez podejmowania żadnego działania.

Ręczne sprawdzanie dostępności aktualizacji

Program SecurityCenter co cztery godziny automatycznie sprawdza aktualizacje, gdy komputer jest połączony z Internetem, a następnie instaluje najnowsze aktualizacje produktu. Można jednak w dowolnej chwili ręcznie sprawdzić aktualizacje, korzystając z ikony programu SecurityCenter wyświetlanej w obszarze powiadomień systemu Windows na prawym końcu paska zadań.

Uwaga: W celu zapewnienia maksymalnej ochrony firma McAfee zaleca umożliwienie programowi SecurityCenter automatyczne sprawdzanie aktualizacji i ich instalowanie. W celu umożliwienia tylko ręcznej aktualizacji usług zabezpieczeń można wyłączyć automatyczne aktualizacje (strona 34).

Aby ręcznie sprawdzić dostępność ewentualnych aktualizacji:

1. Upewnij się, że komputer jest połączony z Internetem.
2. Kliknij prawym przyciskiem myszy ikonę M programu SecurityCenter wyświetlaną w obszarze powiadomień systemu Windows na prawym końcu paska zadań, a następnie kliknij polecenie **Aktualizacje**.

   Podczas gdy program SecurityCenter sprawdza aktualizacje, można kontynuować wykonywanie za jego pomocą innych zadań.

   Dla wygody użytkownika w obszarze powiadomień systemu Windows, z prawej strony paska zadań, pojawi się animowana ikona. Gdy program SecurityCenter zakończy działanie, ikona automatycznie zniknie.
3. W razie wyświetlenia monitu zaloguj się w witrynie sieci Web, aby zweryfikować stan subskrypcji.

Uwaga: W niektórych przypadkach może zostać wyświetlony monit o ponowne uruchomienie komputera w celu dokończenia aktualizacji. Zapisz pracę i zamknij wszystkie programy przed ponownym uruchomieniem komputera.

Konfigurowanie opcji alertów

Program SecurityCenter automatycznie powiadamia użytkownika za pomocą alertów i dźwięków o wystąpieniu powszechnych epidemii wirusowych, zagrożeniach bezpieczeństwa i aktualizacjach produktu. Program SecurityCenter można jednak skonfigurować w taki sposób, aby wyświetlał tylko alerty wymagające natychmiastowej uwagi.

Konfigurowanie opcji alertów

Program SecurityCenter automatycznie powiadamia użytkownika za pomocą alertów i dźwięków o wystąpieniu powszechnych epidemii wirusowych, zagrożeniach bezpieczeństwa i aktualizacjach produktu. Program SecurityCenter można jednak skonfigurować w taki sposób, aby wyświetlał tylko alerty wymagające natychmiastowej uwagi.

Aby skonfigurować opcje alertów:

1. W obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
2. Kliknij strzałkę obok kategorii **Alerty**, aby ją rozwinąć, a następnie kliknij przycisk **Zaawansowane**.
3. W okienku Opcje alertów zaznacz jedną z następujących opcji:
   - **Powiadom, gdy pojawi się powszechna epidemia wirusowa lub zagrożenie bezpieczeństwa**
   - **Pokaż alerty informacyjne, gdy zostanie wykryty tryb gier**
   - **Odtwórz dźwięk przy wystąpieniu alertu**
   - **Pokaż ekran powitalny firmy McAfee podczas uruchamiania systemu Windows**
4. Kliknij przycisk **OK**.

Uwaga: Aby wyłączyć przyszłe alerty informacyjne pochodzące od samego alertu, zaznacz pole wyboru **Nie pokazuj tego alertu ponownie**. Alerty można ponownie włączyć później w okienku Alerty informacyjne.

Konfigurowanie alertów informacyjnych

Alerty informacyjne powiadamiają użytkownika o wystąpieniu zdarzeń, które nie wymagają natychmiastowej reakcji użytkownika. W przypadku wyłączenia przyszłych alertów informacyjnych pochodzących od samego alertu można je ponownie włączyć później w okienku Alerty informacyjne.

Aby skonfigurować alerty informacyjne:

1. W obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
2. Kliknij strzałkę obok kategorii **Alerty**, aby ją rozwinąć, a następnie kliknij przycisk **Zaawansowane**.
3. W okienku **Konfiguracja programu SecurityCenter** kliknij kategorię **Alerty informacyjne**.
4. Usuń zaznaczenie pola wyboru **Ukryj alerty informacyjne**, a następnie na liście alertów usuń zaznaczenie pól wyboru przy alertach, które mają być wyświetlane.
5. Kliknij przycisk **OK**.

ROZDZIAŁ 5

Wykonywanie typowych zadań

Program umożliwia wykonywanie typowych zadań, takich jak przejście do okienka Początek, wyświetlanie ostatnich zdarzeń, zarządzanie siecią komputerową (jeśli komputer obsługuje funkcje zarządzania używane w tej sieci) oraz konserwacja komputera. Jeśli został zainstalowany program McAfee Data Backup, można również tworzyć kopie zapasowe danych.

W tym rozdziale

Wykonywanie typowych zadań 39
Przeglądanie ostatnich zdarzeń 40
Automatyczne przeprowadzanie konserwacji komputera ..41
Ręczne przeprowadzanie konserwacji komputera 42
Zarządzanie siecią 43
Uzyskiwanie dodatkowych informacji na temat wirusów .44

Wykonywanie typowych zadań

Program umożliwia wykonywanie typowych zadań, takich jak przejście do okienka Początek, wyświetlanie ostatnich zdarzeń, konserwacja komputera, zarządzanie siecią komputerową (jeśli komputer obsługuje funkcje zarządzania używane w tej sieci) oraz tworzenie kopii zapasowych danych (jeśli został zainstalowany program McAfee Data Backup).

Aby wykonać typowe zadania:

- W obszarze **Typowe zadania** w Menu podstawowym wykonaj jedną z następujących czynności:
  - Aby powrócić do okienka Początek, kliknij polecenie **Początek**.
  - Aby obejrzeć ostatnie zdarzenia wykryte przez oprogramowanie zabezpieczające, kliknij polecenie **Ostatnie zdarzenia**.
  - Aby usunąć nieużywane pliki, zdefragmentować dane lub przywrócić komputer do poprzedniego stanu, kliknij polecenie **Konserwacja komputera**.
  - Aby wykonać czynności dotyczące zarządzania siecią komputerową, na komputerze obsługującym funkcje zarządzania w tej sieci kliknij polecenie **Zarządzaj siecią**.

    Program Network Manager monitoruje komputery w sieci pod kątem wyszukiwania luk w zabezpieczeniach. Dzięki temu można łatwo identyfikować problemy dotyczące bezpieczeństwa.

- Aby utworzyć kopię zapasową plików, kliknij polecenie **Data Backup**, jeśli został zainstalowany program McAfee Data Backup.

  Funkcja zautomatyzowanego tworzenia kopii zapasowych zapisuje zaszyfrowane kopie najważniejszych plików w miejscu wskazanym przez użytkownika, na nośniku CD/DVD, w pamięci USB lub na dysku zewnętrznym bądź sieciowym.

Wskazówka: Jako dodatkowe udogodnienie typowe zadania można wykonywać z dwóch różnych lokalizacji (w sekcji **Początek** w Menu zaawansowanym oraz w menu **QuickLinks** dostępnym po kliknięciu ikony M programu SecurityCenter znajdującej się na prawym końcu paska zadań). Można wyświetlić ostatnie zdarzenia oraz kompleksowe dzienniki według typu w obszarze **Raporty i dzienniki** w Menu zaawansowanym.

Przeglądanie ostatnich zdarzeń

Ostatnie zdarzenia są rejestrowane w momencie wystąpienia zmian w komputerze. Dzieje się to na przykład w momencie włączenia lub wyłączenia określonego typu ochrony, usunięcia zagrożenia lub zablokowania próby połączenia z Internetem. Można wyświetlić 20 ostatnich zdarzeń wraz z dotyczącymi ich szczegółami.

Szczegółowe informacje na temat zdarzeń związanych z określonym produktem można znaleźć w jego pliku pomocy.

Aby przeglądać ostatnie zdarzenia:

1. Kliknij prawym przyciskiem myszy główną ikonę SecurityCenter, wskaż polecenie **QuickLinks**, a następnie kliknij polecenie **Przeglądaj ostatnie zdarzenia**.

   Na liście zostaną wyświetlone ostatnie zdarzenia wraz z datą i krótkim opisem.

2. W obszarze **Ostatnie zdarzenia** wybierz zdarzenie, aby wyświetlić dotyczące go szczegóły w okienku szczegółów.

   W obszarze **Działanie** zostaną wyświetlone dostępne czynności.

3. Aby wyświetlić pełniejszą listę zdarzeń, kliknij przycisk **Wyświetl dziennik**.

Automatyczne przeprowadzanie konserwacji komputera

W celu systematycznego zwalniania cennego miejsca na dysku twardym oraz optymalizacji wydajności komputera można skonfigurować wykonywanie zadań programów QuickClean lub Defragmentator dysku według regularnego harmonogramu. Zadania te obejmują usuwanie, niszczenie oraz defragmentowanie plików i folderów.

Aby automatycznie przeprowadzać konserwację komputera:

1. Kliknij prawym przyciskiem myszy główną ikonę programu SecurityCenter, wskaż polecenie **QuickLinks**, a następnie kliknij polecenie **Konserwacja komputera**.
2. W obszarze **Harmonogram zadań** kliknij przycisk **Start**.
3. Na liście operacji wybierz pozycję **QuickClean** lub **Defragmentator dysku**.
4. Wykonaj jedną z poniższych czynności:
   - Aby zmodyfikować istniejące zadanie, zaznacz je, a następnie kliknij przycisk **Modyfikuj**. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
   - Aby utworzyć nowe zadanie, w polu **Nazwa zadania** wprowadź jego nazwę, a następnie kliknij przycisk **Utwórz**. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
   - Aby usunąć zadanie, zaznacz je i kliknij przycisk **Usuń**.
5. W obszarze **Podsumowanie zadania** można sprawdzić, kiedy zadanie zostało ostatni raz wykonane, kiedy będzie wykonane następny raz oraz jaki jest jego stan.

Ręczne przeprowadzanie konserwacji komputera

Można wykonywać ręcznie zadania konserwacji komputera: aby usunąć nieużywane pliki, zdefragmentować dane lub przywrócić komputer do poprzedniego stanu.

Aby ręcznie przeprowadzać konserwację komputera:

- Wykonaj jedną z poniższych czynności:
  - Aby skorzystać z programu QuickClean, kliknij prawym przyciskiem myszy główną ikonę SecurityCenter, wskaż polecenie **QuickLinks**, kliknij polecenie **Konserwacja komputera**, a następnie kliknij przycisk **Start**.
  - Aby skorzystać z programu Defragmentator dysku, kliknij prawym przyciskiem myszy główną ikonę SecurityCenter, wskaż polecenie **QuickLinks**, kliknij polecenie **Konserwacja komputera**, a następnie kliknij przycisk **Analizuj**.
  - Aby skorzystać z programu Przywracanie systemu, w Menu zaawansowanym kliknij kategorię **Narzędzia**, kliknij opcję **Przywracanie systemu**, a następnie kliknij przycisk **Start**.

Usuwanie nieużywanych plików i folderów

Program QuickClean służy do zwalniania cennego miejsca na dysku twardym oraz optymalizacji wydajności komputera.

Aby usunąć nieużywane pliki i foldery:

1. Kliknij prawym przyciskiem myszy główną ikonę programu SecurityCenter, wskaż polecenie **QuickLinks**, a następnie kliknij polecenie **Konserwacja komputera**.
2. W obszarze **QuickClean** kliknij przycisk **Start**.
3. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Defragmentowanie plików i folderów

W miarę usuwania plików i folderów oraz dodawania nowych plików dochodzi do ich fragmentacji. Wskutek tej fragmentacji wydłuża się czas dostępu do dysku i pogarsza się ogólna wydajność komputera, chociaż zazwyczaj nie powoduje ona poważnej niesprawności.

Defragmentacja umożliwia ponowne zapisanie części danego pliku w przylegających do siebie sektorach dysku twardego w celu zwiększenia szybkości dostępu i odczytu.

Aby defragmentować pliki i foldery:

1. Kliknij prawym przyciskiem myszy główną ikonę programu SecurityCenter, wskaż polecenie **QuickLinks**, a następnie kliknij polecenie **Konserwacja komputera**.
2. W obszarze **Defragmentator dysku** kliknij przycisk **Analizuj**.
3. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Przywracanie komputera do poprzedniego stanu

Punkty przywracania są obrazami stanu komputera, które system Windows zapisuje okresowo oraz w momencie wystąpienia ważnych zdarzeń (na przykład w przypadku instalowania programu lub sterownika). Można jednak w dowolnej chwili utworzyć i nazwać własny punkt przywracania.

Punkty przywracania służą do cofania szkodliwych zmian wprowadzonych na komputerze oraz przywracania go do poprzedniego stanu.

Aby przywrócić komputer do poprzedniego stanu:

1. W Menu zaawansowanym kliknij kategorię **Narzędzia**, a następnie kliknij opcję **Przywracanie systemu**.
2. W obszarze **Przywracanie systemu** kliknij przycisk **Start**.
3. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Zarządzanie siecią

W przypadku komputera, który ma funkcje zarządzania siecią, moduł Network Manager umożliwia monitorowanie komputerów w sieci pod kątem wyszukiwania luk w zabezpieczeniach. Dzięki temu można łatwo identyfikować problemy dotyczące bezpieczeństwa.

Jeśli stan ochrony komputera w danej sieci nie jest monitorowany, oznacza to, że komputer nie należy do sieci lub należy do niej, ale nie można nim zarządzać. Szczegółowe informacje można znaleźć w pliku pomocy dotyczącym modułu Network Manager.

Aby zarządzać siecią:

1. Kliknij prawym przyciskiem myszy główną ikonę SecurityCenter, wskaż polecenie **QuickLinks**, a następnie kliknij polecenie **Zarządzaj siecią**.
2. Kliknij ikonę odpowiadającą danemu komputerowi na mapie sieci.
3. W obszarze **Działanie** kliknij opcję **Monitoruj ten komputer**.

Uzyskiwanie dodatkowych informacji na temat wirusów

Skorzystaj z Biblioteki informacji o wirusach oraz funkcji Virus Map (Mapa ataków wirusowych), aby:

- Dowiedzieć się więcej o najnowszych wirusach, wirusowych oszustwach w poczcie e-mail i innych zagrożeniach.
- Otrzymać darmowe narzędzia do usuwania wirusów, które pomogą naprawić komputer.
- Zobaczyć, gdzie na świecie mają miejsce poważne ataki wirusów komputerowych.

Aby uzyskać dodatkowe informacje na temat wirusów:

1. W Menu zaawansowanym kliknij kategorię **Narzędzia**, a następnie kliknij opcję **Informacje o wirusie**.
2. Wykonaj jedną z poniższych czynności:
   - Uzyskaj informacje o wirusach, korzystając z bezpłatnej biblioteki informacji o wirusach firmy McAfee.
   - Uzyskaj informacje o wirusach, korzystając z mapy ataków wirusowych na świecie dostępnej w witrynie sieci Web firmy McAfee.

ROZDZIAŁ 6

McAfee QuickClean

Podczas przeglądania witryn internetowych na komputerze szybko gromadzą się różne śmieci. Chroń swoją prywatność i przy pomocy programu QuickClean usuwaj śmieci internetowe i niepotrzebne wiadomości e-mail. Program QuickClean identyfikuje i usuwa pliki, które gromadzą się podczas przeglądania witryn internetowych, na przykład pliki cookie, wiadomości e-mail, pobrane pliki, historię — wszelkie dane zawierające informacje o użytkowniku. Zapewnia on ochronę prywatności, oferując bezpieczne usuwanie poufnych informacji.

Program QuickClean usuwa również niepotrzebne aplikacje. Wystarczy określić pliki, które mają zostać usunięte i wymieść śmieci bez usuwania ważnych informacji.

W tym rozdziale

Omówienie funkcji programu QuickClean 46
Oczyszczanie komputera..... 47

Omówienie funkcji programu QuickClean

W tej sekcji zostały opisane funkcje programu QuickClean.

Funkcje

Program QuickClean udostępnia zestaw wydajnych i łatwych w użyciu narzędzi, które bezpiecznie usuwają cyfrowe odpady. Można zwolnić cenne miejsce na dysku i zoptymalizować wydajność pracy komputera.

ROZDZIAŁ 7

Oczyszczanie komputera

Program QuickClean pozwala na bezpieczne usuwanie plików i folderów.

Podczas przeglądania stron internetowych przeglądarka kopiuje każdą stronę internetową, łącznie z jej grafikami, do folderu pamięci podręcznej na dysku. W ten sposób przeglądarka może szybko załadować stronę podczas jej kolejnego wyświetlenia. Buforowanie plików jest przydatne, jeśli użytkownik wielokrotnie odwiedza te same strony internetowe, a ich zawartość nie zmienia się zbyt często. Najczęściej jednak buforowane pliki nie są przydatne i mogą zostać usunięte.

Przy użyciu opisanych poniżej funkcji oczyszczania można usuwać wiele różnych elementów.

- Oczyszczanie Kosza: Opróżnia zawartość Kosza systemu Windows.
- Oczyszczanie plików tymczasowych: Usuwa pliki zapisane w folderach tymczasowych.
- Oczyszczanie skrótów: Usuwa uszkodzone skróty i skróty bez skojarzonych z nimi programów.
- Oczyszczanie zagubionych fragmentów plików: Usuwa z komputera zagubione fragmenty plików.
- Oczyszczanie rejestru: Usuwa informacje rejestru systemu Windows dotyczące nieistniejących już na komputerze programów.
- Oczyszczanie pamięci podręcznej: Usuwa buforowane pliki, które zbierają się podczas przeglądania Internetu. Tego typu pliki zapisywane są najczęściej jako tymczasowe pliki internetowe.
- Oczyszczanie plików cookie: Usuwa pliki cookie. Tego typu pliki zapisywane są najczęściej jako tymczasowe pliki internetowe. Cookie są małymi plikami, które przeglądarka przechowuje na komputerze na żądanie serwera sieci Web. Za każdym razem, gdy dana strona jest wyświetlana przez serwer sieci Web, przeglądarka wysyła z powrotem do serwera dany plik cookie. Pliki cookie działają jak etykietki, które pozwalają serwerowi sieci Web śledzić przeglądane na komputerze strony i sprawdzać, jak często są odwiedzane.
- Oczyszczanie historii przeglądarki: Usuwa historię przeglądanych stron.
- Oczyszczanie wiadomości e-mail programów Outlook Express i Outlook (elementy usunięte i wysłane): Usuwa wiadomości e-mail z folderów Elementy wysłane i Elementy usunięte programu Outlook.
- Oczyszczanie ostatnio używanych elementów: Usuwa przechowywaną na komputerze listę ostatnio używanych elementów, takich jak dokumenty pakietu Microsoft Office.
- Oczyszczanie formantów ActiveX i dodatków plug-in: Usuwa formanty ActiveX i dodatki plug-in.

ActiveX to technologia używana do implementowania formantów w programach. Formant ActiveX może dodać przycisk do interfejsu programu. Większość z tych formantów jest nieszkodliwa, jednak potencjalnie można użyć technologii ActiveX do przechwytywania informacji z komputera.
Dodatki plug-in to małe programy dołączane do większych aplikacji w celu zapewnienia dodatkowych funkcji. Dodatki plug-in umożliwiają przeglądarce sieci Web na dostęp i wykonywanie osadzonych w dokumentach HTML plików, których format normalnie byłby nierozpoznawany przez przeglądarkę (np. animacja, pliki wideo i audio).

- Oczyszczanie punktu przywracania systemu: Usuwa z komputera stare punkty przywracania systemu.

W tym rozdziale

Korzystanie z programu QuickClean 49

Korzystanie z programu QuickClean

W sekcji tej opisano, jak używać programu QuickClean.

Oczyszczanie komputera

Niepotrzebne pliki i foldery można usuwać, zwalniając miejsce na dysku i zwiększając wydajność pracy komputera.

Aby oczyścić komputer:

1. W Menu zaawansowanym kliknij opcję **Narzędzia**.
2. Kliknij przycisk **Konserwacja komputera**, a następnie kliknij przycisk **Start** w obszarze **McAfee QuickClean**.
3. Wykonaj jedną z poniższych czynności:
   - Kliknij przycisk **Dalej**, aby zaakceptować domyślne operacje oczyszczania na liście.
   - Zaznacz lub usuń zaznaczenie odpowiednich operacji oczyszczania, a następnie kliknij przycisk **Dalej.** W wypadku operacji Oczyszczanie ostatnio używanych elementów kliknij przycisk **Właściwości**, aby usunąć zaznaczenie programów, których list nie chcesz usuwać.
   - Kliknij przycisk **Przywróć ustawienia domyślne**, aby przywrócić domyślne operacje oczyszczania, a następnie kliknij przycisk **Dalej.**
4. Po wykonaniu analizy kliknij przycisk **Dalej**, aby potwierdzić zamiar usunięcia pliku. Można rozwinąć listę, aby przejrzeć pliki przeznaczone do usunięcia i ich położenie.
5. Kliknij przycisk **Dalej**.
6. Wykonaj jedną z poniższych czynności:
   - Kliknij przycisk **Dalej**, aby zaakceptować domyślnie **Nie, chcę usunąć pliki, korzystając ze standardowego sposobu usuwania plików w systemie Windows**.
   - Kliknij przycisk **Tak, chcę bezpiecznie wymazać moje pliki za pomocą programu Shredder** i podaj liczbę przebiegów niszczenia. Pliki usunięte za pomocą programu Shredder nie mogą zostać przywrócone.
7. Kliknij przycisk **Zakończ**.
8. W obszarze **Program QuickClean — podsumowanie** można sprawdzić liczbę usuniętych plików rejestru oraz ilość miejsca odzyskanego na dysku po oczyszczeniu dysku i usunięciu plików internetowych.

ROZDZIAŁ 8

McAfee Shredder

Usunięte z komputera pliki można odzyskać nawet po opróżnieniu Kosza. Gdy plik jest usuwany, system Windows oznacza tylko miejsce zajmowane przez ten plik na dysku jako nieużywane, ale plik nadal tam się znajduje. Za pomocą komputerowych narzędzi diagnostycznych możliwe jest odtworzenie informacji finansowych, podań o pracę lub innych usuniętych dokumentów. Program Shredder zapewnia ochronę prywatności poprzez bezpieczne i trwałe usuwanie niepożądanych plików.

Aby trwale usunąć plik, należy go wielokrotnie zastąpić nowymi danymi. System Microsoft® Windows nie usuwa plików w sposób bezpieczny, ponieważ każda operacja na plikach byłaby wtedy bardzo powolna. Zniszczenie dokumentu nie zawsze uniemożliwia jego odzyskanie, ponieważ niektóre programy tworzą tymczasowe, ukryte kopie otwartych plików. Jeśli niszczone są tylko dokumenty widoczne w programie Windows® Explorer, ich tymczasowe kopie mogą pozostać na komputerze.

Uwaga: W wypadku niszczonych plików nie są tworzone kopie zapasowe. Nie można przywrócić plików, które usunął program Shredder.

W tym rozdziale

Omówienie funkcji programu Shredder 52
Wymazywanie niepożądanych plików za pomocą programu Shredder 53

Omówienie funkcji programu Shredder

W tej sekcji zostały opisane funkcje programu Shredder.

Funkcje

Program Shredder pozwala wymazać zawartość Kosza, tymczasowe pliki internetowe, historię odwiedzanych witryn internetowych, pliki, foldery oraz zawartość dysków.

ROZDZIAŁ 9

Wymazywanie niepożądanych plików za pomocą programu Shredder

Program Shredder zapewnia ochronę prywatności poprzez bezpieczne i trwałe usuwanie niepożądanych plików, takich jak zawartość Kosza i tymczasowe pliki internetowe, oraz historię odwiedzanych witryn sieci Web. Można wybrać pliki i foldery przeznaczone do zniszczenia lub wskazać je, przeglądając dysk.

W tym rozdziale

Korzystanie z programu Shredder.....54

Korzystanie z programu Shredder

W sekcji tej opisano, jak używać programu Shredder.

Niszczenie plików, folderów i zawartości dysków.

Pliki mogą pozostawać na komputerze nawet po opróżnieniu Kosza. Kiedy jednak pliki zostaną zniszczone za pomocą programu Shredder, dane zostaną usunięte w sposób trwały i hakerzy nie będą mieli już do nich dostępu.

Aby zniszczyć pliki, foldery i zawartość dysków:

1. W Menu zaawansowanym kliknij opcję **Narzędzia**, a następnie kliknij przycisk **Shredder**.
2. Wykonaj jedną z poniższych czynności:
   - Kliknij przycisk **Wymaż pliki i foldery**, aby zniszczyć pliki i foldery.
   - Kliknij przycisk **Wymaż cały dysk**, aby usunąć zawartość dysków**.**
3. Wybierz jeden z następujących poziomów niszczenia:
   - **Szybki**: Wybrane elementy są niszczone w jednym przebiegu.
   - **Dokładny**: Wybrane elementy są niszczone w 7 przebiegach.
   - **Niestandardowy**: Wybrane elementy są niszczone przez wykonanie do 10 przebiegów. Większa liczba przebiegów niszczenia zwiększa poziom bezpieczeństwa usuwania plików.
4. Kliknij przycisk **Dalej**.
5. Wykonaj jedną z poniższych czynności:
   - Jeśli usuwasz pliki, na liście **Wybierz pliki do zniszczenia** kliknij pozycję **Zawartość Kosza**, **Tymczasowe pliki internetowe** lub **Historia przeglądarki**. Jeśli usuwasz całą zawartość dysku, kliknij odpowiedni dysk.
   - Kliknij przycisk **Przeglądaj**, przejdź do plików, które chcesz zniszczyć, i zaznacz je.
   - Podaj ścieżkę do plików przeznaczonych do zniszczenia na liście **Wybierz pliki do zniszczenia**.
6. Kliknij przycisk **Dalej**.
7. Kliknij przycisk **Zakończ**, aby zakończyć operację.
8. Kliknij przycisk **Gotowe**.

ROZDZIAŁ 10

McAfee Network Manager

Program McAfee® Network Manager przedstawia w formie graficznej komputery i składniki, które tworzą sieć domową. Program Network Manager umożliwia zdalne monitorowanie stanu ochrony każdego zarządzanego komputera i zdalne rozwiązywanie problemów związanych ze znanymi zagrożeniami ich bezpieczeństwa.

Przed przystąpieniem do użytkowania programu Network Manager można zapoznać się z jego niektórymi najczęściej używanymi funkcjami. Szczegółowe informacje na temat konfigurowania tych funkcji i korzystania z nich zamieszczono w pomocy programu Network Manager.

W tym rozdziale

Funkcje....56
Jak działają ikony programu Network Manager....57
Konfigurowanie zarządzanej sieci....59
Zdalne zarządzanie siecią....67

Funkcje

Program Network Manager udostępnia następujące funkcje:

Graficzna mapa sieci

Mapa sieci programu Network Manager dostarcza graficznego przeglądu stanu zabezpieczeń komputerów i pozostałych składników, tworzących sieć domową. Po wprowadzenia w sieci zmian (na przykład po dodaniu komputera) mapa sieci uwzględnia je. Aby dostosować jej widok do potrzeb, można ją odświeżać, zmieniać nazwę sieci i wyświetlać lub ukrywać jej elementy. Można również wyświetlać szczegóły dotyczące dowolnego elementu przedstawionego na mapie sieci.

Zarządzanie zdalne

Mapę sieci programu Network Manager można wykorzystywać do zarządzania stanem zabezpieczeń komputerów tworzących sieć domową. Można zaprosić komputer do dołączenia do sieci zarządzanej, monitorować stan ochrony zarządzanego komputera i rozwiązywać problemy związane ze znanymi zagrożeniami bezpieczeństwa sieci pochodzącymi ze zdalnego komputera, który znajduje się w sieci.

Jak działają ikony programu Network Manager

Poniższa tabela opisuje ikony często używane na mapach sieci w programie Network Manager.

Ikona	Opis
	Reprezentuje połączony komputer zarządzany
	Reprezentuje niepołączony komputer zarządzany
	Reprezentuje komputer niezarządzany z zainstalowanym oprogramowaniem zabezpieczającym McAfee 2007
	Przedstawia niepołączony komputer niezarządzany
	Reprezentuje połączony komputer bez zainstalowanego oprogramowania zabezpieczającego McAfee 2007 lub nieznane urządzenie sieciowe
	Reprezentuje niepołączony komputer bez zainstalowanego oprogramowania zabezpieczającego McAfee 2007 lub nieznane niepołączone urządzenie sieciowe
	Wskazuje, że dany element jest chroniony i połączony
	Wskazuje, że dany element wymaga uwagi użytkownika
	Wskazuje, że dany element wymaga uwagi użytkownika i jest rozłączony
	Reprezentuje router bezprzewodowy w sieci domowej
	Reprezentuje standardowy router w sieci domowej
	Reprezentuje Internet, jeśli jest połączony
	Reprezentuje Internet, jeśli nie jest połączony

ROZDZIAŁ 11

Konfigurowanie zarządzanej sieci

Konfigurowanie zarządzanej sieci odbywa się za pomocą elementów naniesionych na mapę sieci oraz poprzez dodawanie do sieci składników (komputerów).

W tym rozdziale

Praca z mapą sieci 60
Dołączanie do sieci zarządzanej 63

Praca z mapą sieci

Zawsze, gdy dowolny komputer połączy się z, program Network Manager analizuje stan sieci w celu określenia listy należących do niej urządzeń (zarządzanych i niezarządzanych), atrybutów routera i stany połączenia internetowego. Jeśli żadne urządzenia nie zostaną znalezione, program Network Manager zakłada, że połączony komputer jest pierwszym należącym do sieci i automatycznie określa, że jest on zarządzany oraz ma uprawnienia administracyjne. Nazwa sieci domyślnie zawiera nazwę grupy roboczej lub domeny komputera z zainstalowanym oprogramowaniem zabezpieczającym McAfee 2007, który jako pierwszy połączył się z siecią; nazwę sieci można jednak zmienić w dowolnym momencie.

Po wprowadzenia w sieci zmian (na przykład po dodaniu komputera) można dostosować mapę sieci. Aby dostosować widok mapy do własnych potrzeb, można na przykład ją odświeżyć, zmienić nazwę sieci i wyświetlić lub ukryć jej składniki. Można również wyświetlać szczegóły dotyczące dowolnego składnika przedstawionego na mapie sieci.

Uzyskiwanie dostępu do mapy sieci

Aby uzyskać dostęp do mapy sieci, należy uruchomić program Network Manager z listy typowych zadań programu SecurityCenter. Mapa sieci to graficzna reprezentacja komputerów i pozostałych składników, tworzących sieć domową.

Aby uzyskać dostęp do mapy sieci:

- W menu podstawowym lub zaawansowanym kliknij polecenie **Zarządzaj siecią**.
  Mapa sieci pojawi się w prawym okienku.

Uwaga: Przy pierwszym użyciu mapy sieci wyświetlany jest monit o potwierdzenie, że inne komputery w sieci są zaufane.

Odświeżanie mapy sieci

Mapę sieci można odświeżyć w dowolnym momencie, np. po dodaniu do zarządzanej sieci kolejnego komputera.

Aby odświeżyć mapę sieci:

1. W menu podstawowym lub zaawansowanym kliknij opcję **Zarządzaj siecią**.
   Mapa sieci zostanie wyświetlona w prawym okienku.
2. W menu **Działanie** kliknij opcję **Odśwież mapę sieci**.

Uwaga: Łącze **Odśwież mapę sieci** jest dostępne tylko, gdy na mapie sieci nie jest zaznaczony żaden element. Aby usunąć zaznaczenie elementu, kliknij wybrany element lub kliknij obszar białego tła na mapie sieci.

Zmiana nazwy sieci

Domyślnie nazwa sieci zawiera nazwę grupy roboczej lub domeny pierwszego komputera, który połączy się z siecią i ma zainstalowane oprogramowanie zabezpieczające McAfee 2007. Jeśli ta nazwa jest nieodpowiednia, można ją zmienić.

Aby zmienić nazwę sieci:

1. W menu podstawowym lub zaawansowanym kliknij opcję **Zarządzaj siecią**.
   Mapa sieci zostanie wyświetlona w prawym okienku.
2. W menu **Działanie** kliknij opcję **Zmień nazwę sieci**.
3. Wpisz nazwę sieci w polu **Zmień nazwę sieci**.
4. Kliknij przycisk **OK**.

Uwaga: Łącze **Zmień nazwę sieci** jest dostępne tylko, gdy na mapie sieci nie jest zaznaczony żaden element. Aby usunąć zaznaczenie elementu, kliknij wybrany element lub kliknij obszar białego tła na mapie sieci.

Pokazywanie i ukrywanie elementów na mapie sieci

Domyślnie na mapie sieci są widoczne wszystkie komputery i pozostałe składniki obecne w sieci domowej. Jeśli jednak istnieją elementy ukryte, można je ponownie pokazać w dowolnym momencie. Ukrywać można tylko elementy niezarządzane; ukrycie komputerów zarządzanych jest niemożliwe.

Aby...	W menu podstawowym lub zaawansowanym kliknij polecenie **Zarządzaj siecią**, a następnie...
Ukrycie elementu na mapie sieci	Kliknij element na mapie sieci, a następnie kliknij opcję **Ukryj ten element** w obszarze **Działanie**. W oknie dialogowym potwierdzenia kliknij przycisk **Tak**.
Wyświetlenie ukrytych elementów na mapie sieci	W obszarze **Działanie** kliknij opcję **Pokaż ukryte elementy**.

Wyświetlenie szczegółów elementu

Aby wyświetlić szczegółowe informacje na temat dowolnego składnika w sieci, należy zaznaczyć go na mapie sieci. Wyświetlane informacje obejmują: nazwę składnika, stan jego ochrony oraz inne informacje wymagane do zarządzania składnikiem.

Aby wyświetlić szczegóły elementu:

1. Kliknij ikonę elementu na mapie sieci.
2. W obszarze **Szczegóły** zapoznaj się z informacjami o danym elemencie.

Dołączanie do sieci zarządzanej

Aby komputer mógł być zarządzany zdalnie lub uzyskać uprawnienie do zdalnego zarządzania innymi komputerami w sieci, musi zostać zaufanym członkiem sieci. Członkostwo w sieci jest przyznawane nowym komputerom przez komputery obecne już w sieci, posiadające uprawnienia administracyjne. Aby mieć pewność, że do sieci dołączają tylko zaufane komputery, użytkownik przyznający dostęp i użytkownik dołączający muszą się wzajemnie uwierzytelnić.

Komputer dołączający do sieci jest monitowany o ujawnienie pozostałym komputerom w sieci swojego stanu ochrony przez produkty firmy McAfee. Jeśli komputer zgodzi się na ujawnienie stanu ochrony, staje się *zarządzanym* członkiem sieci. Jeśli komputer odmówi ujawnienia stanu ochrony, staje się *niezarządzanym* członkiem sieci. Komputery niezarządzane w sieci to zwykle komputery-goście, które chcą uzyskać dostęp do innych funkcji sieci (na przykład udostępniania plików i drukarek).

Uwaga: Jeśli na komputerze, który dołączył do sieci, są zainstalowane inne programy sieciowe firmy McAfee (na przykład McAfee Wireless Network Security lub EasyNetwork), również w tych programach komputer jest rozpoznawany jako zarządzany. Poziom uprawnień przypisany do komputera w programie Network Manager dotyczy wszystkich programów sieciowych firmy McAfee. Aby uzyskać więcej informacji o znaczeniu uprawnień gościa, pełnych i administracyjnych w innych programach sieciowych McAfee, należy zapoznać się z dokumentacją danego programu.

Dołączanie do sieci zarządzanej

Otrzymane zaproszenie do dołączenia do sieci zarządzanej użytkownik może zaakceptować lub odrzucić. Można także określić, czy dany komputer i pozostałe komputery w sieci mają mieć możliwość wzajemnego monitorowania ustawień zabezpieczeń (na przykład sprawdzania, czy usługi ochrony antywirusowej komputera są aktualne).

Aby dołączyć do sieci zarządzanej:

1. W oknie dialogowym zaproszenia zaznacz pole wyboru **Pozwól temu komputerowi i pozostałym komputerom w tej sieci monitorować wzajemnie ustawienia bezpieczeństwa**, aby pozostałe komputery w sieci zarządzanej mogły monitorować ustawienia zabezpieczeń komputera.
2. Kliknij przycisk **Dołącz**.
   Po zaakceptowaniu zaproszenia zostaną wyświetlone dwie karty do gry.
3. Potwierdź, że karty do gry są takie same jak wyświetlane na komputerze, który wysłał zaproszenie do dołączenia do sieci zarządzanej.
4. Kliknij przycisk **Potwierdź**.

Uwaga: Jeśli na komputerze, który wysłał zaproszenie do dołączenia do sieci zarządzanej, nie są wyświetlane te same karty, które są widoczne w oknie dialogowym potwierdzania zabezpieczeń, oznacza to, że w sieci zarządzanej doszło do naruszenia zabezpieczeń. Dołączenie do sieci mogłoby stanowić zagrożenie dla komputera, dlatego w takiej sytuacji w oknie dialogowym potwierdzania zabezpieczeń należy kliknąć opcję **Odrzuć**.

Zapraszanie komputera do dołączenia do sieci zarządzanej

Jeśli do sieci zarządzanej zostanie dodany komputer lub w sieci tej istnieje inny komputer niezarządzany, można zaprosić go do dołączenia do sieci. Do dołączenia do sieci zapraszać mogą tylko komputery z uprawnieniami administracyjnymi. Wysyłając zaproszenie, należy określić także poziom uprawnienia, który ma zostać przyznany komputerowi dołączającemu do sieci.

Aby zaprosić komputer do dołączenia do sieci zarządzanej:

1. Kliknij ikonę komputera niezarządzanego na mapie sieci.
2. Kliknij opcję **Monitoruj ten komputer** w obszarze **Działanie**.
3. W oknie dialogowym Zaproś komputer do dołączenia do zarządzanej sieci kliknij jedną z opcji:
   - **Przyznaj dostęp typu Gość**
     Dostęp typu Gość pozwala komputerowi na uzyskiwanie dostępu do sieci.
   - **Przyznaj dostęp Pełny do wszystkich zarządzanych aplikacji sieciowych**
     Pełny dostęp (podobnie jak dostęp typu Gość) pozwala komputerowi na uzyskiwanie dostępu do sieci.
   - **Przyznaj dostęp Administrator do wszystkich zarządzanych aplikacji sieciowych**
     Dostęp typu Administrator pozwala komputerowi na uzyskiwanie dostępu z uprawnieniami administracyjnymi do sieci. Pozwala także przyznawać dostęp innym komputerom, które chcą dołączyć do sieci zarządzanej.
4. Kliknij przycisk **Zaproś**.
   Do innego komputera zostanie wysłane zaproszenie do dołączenia do sieci. Kiedy zapraszany komputer je zaakceptuje, zostaną wyświetlone dwie karty do gry.
5. Potwierdź, że karty do gry są takie same jak wyświetlane na komputerze, który zapraszasz do dołączenia do sieci zarządzanej.
6. Kliknij opcję **Przyznaj prawa dostępu**.

Uwaga: Jeśli na komputerze, który zapraszasz do dołączenia do sieci zarządzanej, nie są wyświetlane te same karty, które są widoczne w oknie dialogowym potwierdzania zabezpieczeń, oznacza to, że w sieci zarządzanej doszło do naruszenia zabezpieczeń. Zezwolenie temu komputerowi na dołączenie do sieci mogłoby stanowić zagrożenie innych komputerów, dlatego w takiej sytuacji w oknie dialogowym potwierdzania zabezpieczeń kliknij przycisk **Odmów dostępu**.

Rezygnowanie z ufania komputerom w sieci

Jeśli zgoda na ufanie innym komputerom w sieci została wyrażona przez pomyłkę, można przestać im ufać.

Aby przestać ufać komputerom w sieci:

- Kliknij opcję **Przestań ufać komputerom w tej sieci** w obszarze **Działanie**.

Uwaga: Łącze **Przestań ufać komputerom w tej sieci** jest dostępne tylko w sytuacji, gdy do sieci nie dołączyły żadne inne komputery zarządzane.

ROZDZIAŁ 12

Zdalne zarządzanie siecią

Po skonfigurowaniu zarządzanej sieci można użyć programu Network Manager do zdalnego zarządzania komputerami i składnikami sieci. Można monitorować stan i poziomy uprawnień komputerów i składników oraz zdalnie naprawiać luki w zabezpieczeniach.

W tym rozdziale

Monitorowanie stanu i uprawnień.....68
Naprawa luk w zabezpieczeniach 71

Monitorowanie stanu i uprawnień

Sieć zarządzana ma dwa typy użytkowników: użytkownikami zarządzanymi i użytkownikami niezarządzanymi. Użytkownicy zarządzani zezwalają na monitorowanie swojego stanu ochrony w programie firmy McAfee przez inne komputery w sieci; użytkownicy niezarządzani — nie zezwalają na to. Komputery niezarządzane to zwykle komputery-goście, które chcą uzyskać dostęp do innych funkcji sieci (na przykład udostępniania plików i drukarek). Komputer niezarządzany można w dowolnej chwili zaprosić do sieci (aby stał się komputerem zarządzanym) z innego komputera zarządzanego w sieci. Analogicznie, komputer zarządzany może w dowolnym momencie stać się niezarządzanym.

Komputery zarządzane mają uprawnienia dostępu administracyjnego, pełnego lub typu Gość. Uprawnienia dostępu administracyjnego pozwalają komputerowi zarządzanemu zarządzać stanem ochrony pozostałych komputerów zarządzanych w sieci oraz przyznawać pozostałym komputerom członkostwo w sieci. Uprawnienia dostępu pełnego i typu Gość pozwalają komputerowi tylko na uzyskiwanie dostępu do sieci. Poziom uprawnień komputera można zmodyfikować w dowolnym momencie.

Ponieważ sieć zarządzana obejmuje także urządzenia (na przykład routery), za pomocą programu Network Manager można także zarządzać takimi urządzeniami. Można także konfigurować i modyfikować ustawienia wyświetlania urządzenia na mapie sieci.

Monitorowanie stanu ochrony komputera

Jeśli stan ochrony komputera nie jest monitorowany w sieci (ponieważ komputer nie jest członkiem sieci lub jest jej elementem niezarządzanym), można zażądać jego monitorowania.

Aby monitorować stan ochrony komputera:

1. Kliknij ikonę komputera niezarządzanego na mapie sieci.
2. Kliknij opcję **Monitoruj ten komputer** w obszarze **Działanie**.

Kończenie monitorowania stanu ochrony komputera

Monitorowanie stanu ochrony komputera zarządzanego w sieci prywatnej można zakończyć. W efekcie komputer staje się komputerem niezarządzanym.

Aby zakończyć monitorowanie stanu ochrony komputera:

1. Kliknij ikonę komputera zarządzanego na mapie sieci.
2. Kliknij opcję **Zakończ monitorowanie tego komputera** w obszarze **Działanie**.
3. W oknie dialogowym potwierdzenia kliknij przycisk **Tak**.

Modyfikowanie uprawnień komputera zarządzanego

Uprawnienia komputera zarządzanego można zmodyfikować w dowolnym momencie. Umożliwia to określanie, które komputery mogą monitorować stan ochrony (ustawienia zabezpieczeń) innych komputerów w sieci.

Aby zmodyfikować uprawnienia komputera zarządzanego:

1. Kliknij ikonę komputera zarządzanego na mapie sieci.
2. Kliknij opcję **Modyfikuj uprawnienia dla tego komputera** w obszarze **Działanie**.
3. W oknie dialogowym modyfikowania uprawnień zaznacz lub wyczyść pole wyboru w celu określenia, czy dany komputer i pozostałe komputery w sieci zarządzanej mają mieć możliwość wzajemnego monitorowania stanu ochrony.
4. Kliknij przycisk **OK**.

Zarządzanie urządzeniem

Zarządzanie urządzeniem umożliwia jego administracyjna strona sieci Web, dostępna z programu Network Manager.

Aby zarządzać urządzeniem:

1 Kliknij ikonę urządzenia na mapie sieci.

2 Kliknij opcję **Zarządzaj tym urządzeniem** w obszarze **Działanie**.
W otwartym oknie przeglądarki sieci Web zostanie wyświetlona administracyjna strona sieci Web urządzenia.

3 W oknie przeglądarki sieci Web podaj informacje logowania i skonfiguruj ustawienia zabezpieczeń urządzenia.

Uwaga: Jeśli urządzenie to router bezprzewodowy lub punkt dostępu chroniony przez program Wireless Network Security, do konfigurowania jego ustawień zabezpieczeń należy używać programu Wireless Network Security.

Modyfikowanie ustawień wyświetlania urządzenia

Modyfikując ustawienia wyświetlania urządzenia, można zmienić nazwę urządzenia wyświetlaną na mapie sieci oraz określić, czy urządzenie jest routerem bezprzewodowym.

Aby zmodyfikować ustawienia wyświetlania urządzenia:

1 Kliknij ikonę urządzenia na mapie sieci.

2 Kliknij opcję **Modyfikuj właściwości urządzenia** w obszarze **Działanie**.

3 Aby określić wyświetlaną nazwę urządzenia, wpisz ją w polu **Nazwa**.

4 Aby określić typ urządzenia, kliknij jedną z następujących opcji:

- **Router**
  Opcja reprezentuje standardowy router w sieci domowej.
- **Router bezprzewodowy**
  Opcja reprezentuje router bezprzewodowy w sieci domowej.

5 Kliknij przycisk **OK**.

Naprawa luk w zabezpieczeniach

Zarządzane komputery z uprawnieniami administratora mogą monitorować stan ochrony McAfee innych zarządzanych komputerów w sieci i zdalnie naprawiać wszelkie zgłoszone luki w zabezpieczeniach. Na przykład jeśli stan ochrony McAfee zarządzanego komputera wskazuje, że program VirusScan jest wyłączony, inny zarządzany komputer z uprawnieniami administratora może *naprawić* tę lukę w zabezpieczeniach zdalnie włączając program VirusScan.

Podczas zdalnego naprawiania luk w zabezpieczeniach program Network Manager automatycznie naprawia najczęściej zgłaszane problemy. Jednak niektóre luki w zabezpieczeniach mogą wymagać ręcznej interwencji na lokalnym komputerze. W takim przypadku program Network Manager naprawia te problemy, które można naprawić zdalnie, a następnie monituje o naprawienie pozostałych poprzez zalogowanie do programu SecurityCenter na zagrożonym komputerze i postępowanie zgodnie z podanymi zaleceniami. W niektórych przypadkach sugerowanym sposobem naprawy jest instalacja oprogramowania zabezpieczającego McAfee 2007 na zdalnym komputerze lub komputerach w sieci.

Naprawianie luk w zabezpieczeniach

Za pomocą programu Network Manager można automatycznie naprawić większość luk w zabezpieczeniach zdalnych komputerów zarządzanych. Jeśli na przykład na komputerze zdalnym program VirusScan jest wyłączony, za pomocą programu Network Manager można go automatycznie włączyć.

Aby naprawić luki w zabezpieczeniach:

1. Kliknij ikonę elementu na mapie sieci.
2. Sprawdź stan zabezpieczenia elementu wyświetlany w obszarze **Szczegóły**.
3. Kliknij opcję **Napraw luki w zabezpieczeniach** w obszarze **Działanie**.
4. Po rozwiązaniu problemów z zabezpieczeniami, kliknij przycisk **OK**.

Uwaga: Mimo że program Network Manager automatycznie naprawia większość luk w zabezpieczeniach, część napraw może wymagać uruchomienia programu SecurityCenter na komputerze podatnym na ataki i postępowania zgodnie z podawanymi zaleceniami.

Instalowanie oprogramowania zabezpieczającego McAfee na zdalnych komputerach

Jeśli jeden lub więcej komputerów w sieci nie posiada oprogramowania zabezpieczającego McAfee 2007, jego stan zabezpieczeń nie może być zdalnie monitorowany. Aby zdalnie monitorować te komputery, należy na każdym z nich zainstalować oprogramowanie zabezpieczające McAfee 2007.

Aby zainstalować oprogramowanie zabezpieczające McAfee na zdalnym komputerze:

1. W przeglądarce zainstalowanej na zdalnym komputerze otwórz stronę http://download.mcafee.com/us/.
2. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby zainstalować na komputerze oprogramowanie zabezpieczające McAfee 2007.

ROZDZIAŁ 13

McAfee VirusScan

Program VirusScan oferuje wszechstronną, niezawodną i zawsze aktualną ochronę przed wirusami i oprogramowaniem szpiegującym. Dzięki wykorzystaniu wielokrotnie nagradzanej technologii skanowania opracowanej przez firmę McAfee program VirusScan zabezpiecza system przed wirusami, robakami, końmi trojańskimi, podejrzanymi skryptami, programami typu rootkit, przepełnieniami buforu, atakami hybrydowymi, oprogramowaniem szpiegującym, potencjalnie niepożądanymi programami i innymi zagrożeniami.

W tym rozdziale

Funkcje 74
Zarządzanie ochroną przed wirusami 77
Ręczne skanowanie komputera 97
Administrowanie programem VirusScan 103
Dodatkowa pomoc 111

Funkcje

W tej wersji programu VirusScan dostępne są następujące funkcje:

Ochrona przed wirusami

Skanowanie w czasie rzeczywistym umożliwia skanowanie plików w momencie, gdy użytkownik lub system próbuje uzyskać do nich dostęp.

Funkcja skanowania

Wyszukiwanie wirusów i innych zagrożeń na dyskach twardych, dyskietkach oraz w pojedynczych plikach i folderach. Można również zeskanować element, klikając go prawym przyciskiem myszy.

Wykrywanie oprogramowania szpiegującego i reklamowego

Program VirusScan rozpoznaje i usuwa oprogramowanie szpiegujące i reklamowe, a także wszelkie inne programy, które mogą narazić prywatność użytkownika i spowolnić pracę komputera.

Automatyczne aktualizacje

Automatyczne aktualizacje zapewniają ochronę przed najnowszymi znanymi i niezidentyfikowanymi zagrożeniami bezpieczeństwa.

Szybkie skanowanie w tle

Szybkie i nieprzeszkadzające w pracy skanowanie identyfikuje i usuwa wirusy, konie trojańskie, robaki, oprogramowanie szpiegujące i reklamowe oraz dialery i inne zagrożenia.

Ostrzeganie o zagrożeniach bezpieczeństwa w czasie rzeczywistym

Alerty zabezpieczeń powiadamiają o epidemiach wirusowych i zagrożeniach bezpieczeństwa oraz udostępniają opcje reagowania w celu usunięcia, zneutralizowania lub uzyskania dodatkowych informacji na temat zagrożenia.

Wykrywanie i czyszczenie w wielu punktach ataku

Program VirusScan monitoruje i czyści w kluczowych punktach ataku w komputerze: wiadomości e-mail, załączniki do wiadomości błyskawicznych, a także pliki pobierane z Internetu.

Monitorowanie poczty e-mail w poszukiwaniu działalności robaków

Program WormStopper™ zapobiega wysyłaniu robaków do innych komputerów przez konie trojańskie i informuje użytkownika zanim nieznane programy wyślą wiadomości e-mail.

Monitorowanie skryptów w poszukiwaniu działalności robaków

Program ScriptStopper™ blokuje uruchamianie w komputerze znanych, szkodliwych skryptów.

Program McAfee X-ray for Windows

Program McAfee X-ray wykrywa i niszczy programy typu rootkit oraz inne programy, które ukrywają się przed systemem Windows.

Ochrona przed przepełnieniem buforu

Ochrona przed przepełnieniem buforu chroni przed przepełnieniami buforu. Przepełnienie bufora występuje wtedy, gdy podejrzane programy lub procesy próbują zapisać więcej danych w buforze (miejscu zapisu tymczasowych danych), niż może on pomieścić, niszcząc lub nadpisując ważne dane w sąsiednich buforach.

Programy McAfee SystemGuard

Programy SystemGuard badają komputer pod kątem pewnych rodzajów aktywności mogących być przejawem działania wirusa, oprogramowania szpiegującego lub hakera.

ROZDZIAŁ 14

Zarządzanie ochroną przed wirusami

Można w czasie rzeczywistym zarządzać ochroną przed wirusami i oprogramowaniem szpiegującym, zarządzać programami SystemGuard i ochroną przed skryptami. Możliwe jest na przykład wyłączenie skanowania lub określenie zakresu skanowania.

Tylko użytkownicy z uprawnieniami administracyjnymi mogą modyfikować zaawansowane opcje.

W tym rozdziale

Korzystanie z ochrony przed wirusami 78
Korzystanie z ochrony przed oprogramowaniem szpiegującym 82
Korzystanie z programów SystemGuard..... 83
Korzystanie ze skanowania skryptów 93
Korzystanie z ochrony poczty e-mail..... 94
Korzystanie z ochrony wiadomości błyskawicznych..... 96

Korzystanie z ochrony przed wirusami

Od momentu włączenia ochrony przed wirusami (skanowania w czasie rzeczywistym) komputer jest nieustannie monitorowany pod kątem aktywności wirusów. Funkcja skanowania w czasie rzeczywistym powoduje skanowanie plików za każdym razem, gdy użytkownik lub system próbuje uzyskać do nich dostęp. Kiedy funkcje ochrony przed wirusami wykryją zainfekowany plik, następuje próba oczyszczenia lub usunięcia infekcji. Jeśli pliku nie można oczyścić lub usunąć, jest wyświetlany alert z monitem o podjęcie dalszych działań.

Tematy pokrewne

- Jak działa system generowania alertów zabezpieczeń (strona 109)

Wyłączanie ochrony przed wirusami.

Jeśli ochrona przed wirusami zostanie wyłączona, komputer przestanie być chroniony w sposób ciągły przed aktywnością wirusów. Jeśli wymagane jest zatrzymanie ochrony przed wirusami, należy się upewnić, że komputer nie jest połączony z Internetem.

Uwaga: Wyłączenie ochrony przed wirusami spowoduje wyłączenie również ochrony w czasie rzeczywistym przed oprogramowaniem szpiegującym, ochrony wiadomości e-mail oraz wiadomości błyskawicznych.

Aby wyłączyć ochronę przed wirusami:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Komputer i pliki**.
3. W polu **Ochrona przed wirusami** kliknij opcję **Wyłączona**.
4. W oknie dialogowym potwierdzenia wykonaj jedną z poniższych czynności:
   - Aby ponownie uruchomić ochronę przed wirusami po określonym czasie, zaznacz pole wyboru **Ponownie włącz skanowanie w czasie rzeczywistym po** i wybierz czas z menu.
   - Aby zapobiec uruchomieniu ochrony przed wirusami po określonym czasie, usuń zaznaczenie pola wyboru **Ponownie włącz przed wirusami po**.

5 Kliknij przycisk **OK**.

Jeśli ochrona w czasie rzeczywistym jest skonfigurowana tak, aby samoczynnie rozpoczynała działanie po uruchomieniu systemu Windows, komputer będzie chroniony po ponownym uruchomieniu.

Tematy pokrewne

- Konfiguracja ochrony w czasie rzeczywistym (strona 80)

Włączanie ochrony przed wirusami

Funkcja ochrony przed wirusami nieustannie monitoruje komputer pod kątem aktywności wirusów.

Aby włączyć ochronę przed wirusami:

1 W Menu zaawansowanym kliknij opcję **Konfiguruj**.

2 W okienku konfiguracji kliknij opcję **Komputer i pliki**.

3 W polu **Ochrona przed wirusami** kliknij opcję **Włączona**.

Konfigurowanie ochrony w czasie rzeczywistym

Ochronę przed wirusami w czasie rzeczywistym można modyfikować. Można na przykład skanować same pliki programów i dokumenty albo wyłączyć skanowanie w czasie rzeczywistym podczas uruchamiania systemu Windows (nie zalecane).

Konfiguracja ochrony w czasie rzeczywistym

Ochronę przed wirusami w czasie rzeczywistym można modyfikować. Można na przykład skanować same pliki programów i dokumenty albo wyłączyć skanowanie w czasie rzeczywistym podczas uruchamiania systemu Windows (nie zalecane).

Aby skonfigurować ochronę w czasie rzeczywistym:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Komputer i pliki**.
3. W obszarze **Ochrona przed wirusami** kliknij przycisk **Zaawansowane**.
4. Zaznacz lub usuń zaznaczenie następujących pól:
   - **Skanuj w poszukiwaniu nieznanych wirusów przy użyciu heurystyk**: Pliki są dopasowywane do sygnatur znanych wirusów w celu wykrycia obecności niezidentyfikowanych wirusów. Opcja skanowania w poszukiwaniu nowych, nieznanych wirusów zapewnia największą dokładność skanowania, ale wiąże się z wydłużeniem czasu pracy skanera.
   - **Skanuj stację dyskietek przy zamykaniu**: Stacja dyskietek jest skanowana podczas wyłączania komputera.
   - **Skanuj w poszukiwaniu programów szpiegujących i potencjalnie niepożądanych**: Oprogramowanie szpiegujące i reklamowe oraz inne programy, które potencjalnie gromadzą i wysyłają dane użytkowników bez ich zgody, są wykrywane i usuwane.
   - **Skanuj i usuwaj śledzące pliki cookie**: Pliki cookie, które potencjalnie gromadzą i wysyłają dane bez zgody użytkownika, są wykrywane i usuwane. Plik cookie identyfikuje użytkowników odwiedzających witrynę internetową.
   - **Skanuj dyski sieciowe**: Skanowane są dyski podłączone do sieci.
   - **Włącz ochronę przed przepełnieniem buforu**: Gdy wykryte zostanie działanie dążące do przepełnienia buforu, jest ono blokowane, a użytkownik zostaje o tym powiadomiony.
   - **Uruchom skanowanie w czasie rzeczywistym podczas uruchamiania systemu Windows (zalecane)**: Ochrona w czasie rzeczywistym jest włączana przy każdym uruchomieniu komputera, nawet jeśli zostanie on wyłączony na czas danej sesji.

5 Kliknij jeden z poniższych przycisków:

- **Wszystkie pliki (zalecane)**: Skanowane są pliki wszystkich typów używanych w systemie. Opcji tej należy użyć, aby zapewnić najdokładniejsze skanowanie komputera.
- **Tylko pliki programów i dokumenty**: Skanowane są tylko pliki programów i dokumenty.

6 Kliknij przycisk **OK**.

Korzystanie z ochrony przed oprogramowaniem szpiegującym

Ochrona przed oprogramowaniem szpiegującym usuwa oprogramowanie szpiegujące, reklamowe oraz inne potencjalnie niepożądane programy, które gromadzą i wysyłają dane użytkowników bez ich zgody.

Wyłączanie ochrony przed oprogramowaniem szpiegującym

Jeśli ochrona przed oprogramowaniem szpiegującym zostanie wyłączona, potencjalnie niepożądane programy, które zbierają i przesyłają dane bez zgody użytkownika, nie będą wykrywane.

Aby wyłączyć ochronę przed oprogramowaniem szpiegującym:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Komputer i pliki**.
3. W polu **Ochrona przed oprogramowaniem szpiegującym** kliknij opcję **Wyłączona**.

Włączanie ochrony przed oprogramowaniem szpiegującym

Ochrona przed oprogramowaniem szpiegującym usuwa oprogramowanie szpiegujące, reklamowe oraz inne potencjalnie niepożądane programy, które gromadzą i wysyłają dane użytkowników bez ich zgody.

Aby włączyć ochronę przed oprogramowaniem szpiegującym:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Komputer i pliki**.
3. W polu **Ochrona przed oprogramowaniem szpiegującym** kliknij opcję **Włączona**.

Korzystanie z programów SystemGuard

Programy SystemGuard wykrywają potencjalnie nieautoryzowane zmiany w komputerze i powiadamiają użytkownika w chwili wystąpienia zmian. Następnie użytkownik może przejrzeć te zmiany i podjąć decyzję, czy na nie pozwolić.

Programy SystemGuard dzielą się na opisane poniżej kategorie.

Program

Programy SystemGuard z kategorii Program wykrywają zmiany w plikach uruchomieniowych, rozszerzeniach i plikach konfiguracyjnych.

Przeglądarka

Programy SystemGuard z kategorii Przeglądarka wykrywają zmiany ustawień w przeglądarce Internet Explorer, łącznie z atrybutami przeglądarki i ustawieniami zabezpieczeń.

Windows

Programy SystemGuard z kategorii Windows wykrywają zmiany w usługach, certyfikatach i plikach konfiguracyjnych systemu Windows®.

Wyłączanie programów SystemGuard

Jeśli programy SystemGuard zostaną wyłączone, potencjalne nieautoryzowane zmiany w systemie nie będą wykrywane.

Aby wyłączyć wszystkie programy SystemGuard:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Komputer i pliki**.
3. W polu **Ochrona przez program SystemGuard** kliknij opcję **Wyłączona**.

Włączanie programów SystemGuard

Programy SystemGuard wykrywają potencjalnie nieautoryzowane zmiany w komputerze i powiadamiają użytkownika w chwili wystąpienia zmian.

Aby włączyć programy SystemGuard:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Komputer i pliki**.
3. W polu **Ochrona przez program SystemGuard** kliknij opcję **Włączona**.

Konfigurowanie programów SystemGuard

Ustawienia programów SystemGuard można modyfikować. W wypadku każdej wykrytej zmiany można zdecydować, czy ma zostać wyświetlone ostrzeżenie wraz z zanotowaniem wystąpienia zdarzenia w dzienniku, czy ma tylko zostać dokonany zapis w dzienniku lub czy wyłączyć program SystemGuard.

Konfiguracja programów SystemGuard

Ustawienia programów SystemGuard można modyfikować. W wypadku każdej wykrytej zmiany można zdecydować, czy ma zostać wyświetlone ostrzeżenie wraz z zanotowaniem wystąpienia zdarzenia w dzienniku, czy ma tylko zostać dokonany zapis w dzienniku lub czy wyłączyć program SystemGuard.

Aby skonfigurować programy SystemGuard:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Komputer i pliki**.
3. W obszarze **Ochrona przez programy SystemGuard** kliknij przycisk **Zaawansowane**.
4. Na liście programów SystemGuard kliknij kategorię, aby wyświetlić listę skojarzonych programów SystemGuard i ich stan.
5. Kliknij nazwę programu SystemGuard.
6. W obszarze **Szczegóły** sprawdź informacje o programie SystemGuard.
7. W obszarze **Działanie** wykonaj jedną z następujących czynności:
   - Kliknij opcję **Pokaż alerty**, aby było wyświetlane ostrzeżenie, gdy wystąpi zmiana i zdarzenie zostanie zapisane w dzienniku.
   - Kliknij opcję **Rejestruj tylko zmiany**, aby po wykryciu zmiany nie była wykonywana żadna akcja. Zmiana jest tylko zapisywana w dzienniku.
   - Kliknij opcję **Wyłącz ten program SystemGuard**, aby wyłączyć program SystemGuard. W przypadku wystąpienia zmiany nie zostanie wyświetlone ostrzeżenie i nie zostanie dokonany wpis w dzienniku.
8. Kliknij przycisk **OK**.

Omówienie programów SystemGuard

Programy SystemGuard wykrywają potencjalnie nieautoryzowane zmiany w komputerze i powiadamiają użytkownika w chwili wystąpienia zmian. Następnie użytkownik może przejrzeć te zmiany i podjąć decyzję, czy na nie pozwolić.

Programy SystemGuard dzielą się na opisane poniżej kategorie.

Program

Programy SystemGuard z kategorii Program wykrywają zmiany w plikach uruchomieniowych, rozszerzeniach i plikach konfiguracyjnych.

Przeglądarka

Programy SystemGuard z kategorii Przeglądarka wykrywają zmiany ustawień w przeglądarce Internet Explorer, łącznie z atrybutami przeglądarki i ustawieniami zabezpieczeń.

Windows

Programy SystemGuard z kategorii Windows wykrywają zmiany w usługach, certyfikatach i plikach konfiguracyjnych systemu Windows®.

Informacje o aplikacjach SystemGuard z kategorii Program

Aplikacje SystemGuard z kategorii Program wykrywają wymienione poniżej elementy.

Instalacje formantów ActiveX

Wykrywanie formantów ActiveX pobieranych poprzez przeglądarkę Internet Explorer. Formanty ActiveX są pobierane z witryn internetowych i przechowywane na komputerze w folderze C:\Windows\Downloaded Program Files lub C:\Windows\Temp\Temporary Internet Files. W rejestrze istnieją również odwołania do tych formantów poprzez ich identyfikatory CLSID (długi ciąg liczb w nawiasach klamrowych).

Internet Explorer używa wielu zatwierdzonych formantów ActiveX. Jeśli funkcja jakiegoś formantu ActiveX nie jest znana, może on zostać usunięty bez szkody dla komputera. Jeśli zajdzie taka potrzeba, przeglądarka Internet Explorer pobierze ten formant podczas następnej wizyty w witrynie sieci Web, która będzie go wymagała.

Elementy uaktywniane podczas uruchamiania systemu

Monitorowane są zmiany startowych folderów i kluczy rejestru. Klucze startowe w rejestrze systemu Windows i foldery startowe w menu Start przechowują ścieżki dostępu do programów w komputerze. Programy wymienione w tych lokalizacjach są ładowane podczas uruchamiania systemu Windows. Oprogramowanie szpiegujące oraz potencjalnie niepożądane programy często próbują ładować się podczas uruchamiania systemu Windows.

Uchwyty uruchamiania powłoki systemu Windows

Monitorowane są zmiany listy programów ładowanych do programu explorer.exe. Uchwyt uruchamiania powłoki jest programem ładowanym do powłoki explorer.exe systemu Windows. Program będący uchwytem uruchamiania powłoki otrzymuje wszystkie polecenia wykonania uruchamiane na komputerze. Każdy program załadowany do powłoki programu explorer.exe może wykonywać dowolne dodatkowe zadania przed faktycznym uruchomieniem innego programu. Oprogramowanie szpiegujące lub inne potencjalnie niepożądane programy mogą korzystać z uchwytów uruchamiania powłoki, aby zapobiegać uruchamianiu programów zapewniających bezpieczeństwo.

Shell Service Object Delay Load (Opóźnione ładowanie obiektów usług powłoki)

Monitorowanie zmian w plikach wymienionych w Shell Service Object Delay Load (Opóźnione ładowanie obiektów usług powłoki). Pliki te ładowane są przez program explorer.exe podczas uruchamiania komputera. Ponieważ program explorer.exe stanowi powłokę komputera, jest zawsze uruchamiany i ładuje pliki wymienione w tym kluczu. Pliki te są ładowane we wczesnej fazie procesu uruchamiania, zanim nastąpi interwencja użytkownika.

Informacje o aplikacjach SystemGuard z kategorii Windows

Aplikacje SystemGuard z kategorii Windows wykrywają wymienione poniżej elementy.

Programy obsługi menu kontekstowego

Zapobieganie nieautoryzowanym zmianom w menu kontekstowym systemu Windows. To menu pozwala na wykonanie specyficznych operacji na plikach poprzez ich kliknięcie prawym przyciskiem myszy.

Biblioteki DLL AppInit

Zapobieganie nieautoryzowanym zmianom lub dodatkom do bibliotek AppInit.DLL systemu Windows. Wartość rejestru AppInit_DLL zawiera listę plików ładowanych wraz z biblioteką user32.dll. Pliki z listy wartości AppInit_DLL są ładowane w początkowej fazie procedury startowej systemu Windows, umożliwiając ukrycie się potencjalnie niebezpiecznych bibliotek .DLL zanim będzie możliwa interwencja użytkownika.

Plik Hosts systemu Windows

Monitorowanie zmian w pliku Hosts. Plik Hosts używany jest w celu przekierowania niektórych nazw domen do określonych adresów IP. Na przykład kiedy ma zostać wyświetlona witryna www.example.com, przeglądarka sprawdza plik Hosts, odnajduje wpis example.com i wskazuje adres IP tej domeny. Niektóre programy szpiegujące próbują zmienić plik Hosts, aby wymusić przekierowanie przeglądarki do innej witryny i uniemożliwić prawidłowe aktualizowanie oprogramowania.

Powłoka Winlogon

Monitorowanie powłoki Winlogon. Powłoka ta jest ładowana, gdy użytkownik loguje się do systemu Windows. Powłoka jest głównym interfejsem użytkownika (UI) używanym do zarządzania systemem Windows. Zazwyczaj jest nią program Eksplorator Windows (explorer.exe). Jednakże powłokę systemu Windows można łatwo zmienić, tak aby wskazywała inny program. Jeśli to nastąpi, przy każdym logowaniu użytkownika uruchamiany będzie program inny niż powłoka systemu Windows.

Winlogon User Init

Monitorowanie zmian ustawień logowania Windows użytkownika. Klucz HKLM\Software\Microsoft WindowsNT\CurrentVersion\Winlogon\Userinit określa, jaki program jest uruchamiany po zalogowaniu się użytkownika do systemu Windows. Domyślny program przywraca profil, czcionki, kolory i inne ustawienia przypisane do danej nazwy użytkownika. Oprogramowanie szpiegujące i inne potencjalnie niepożądane programy mogą próbować uruchomić się poprzez dodanie swoich wpisów do tego klucza.

Protokoły systemu Windows

Monitorowanie zmian protokołów sieciowych. Niektóre typy oprogramowania szpiegującego lub inne potencjalnie niepożądane programy przejmują kontrolę nad różnymi sposobami wysyłania i odbierania informacji przez komputer. Realizują to poprzez filtry i programy obsługi protokołów systemu Windows.

Dostawcy usługi warstwowej (Winsock)

Monitorowanie dostawców usługi warstwowej (LSP), którzy mogą przejąć dane poprzez sieć i zmienić je lub przekierować. Do zatwierdzonych dostawców usługi warstwowej należy oprogramowanie do kontroli rodzicielskiej, zapory i inne programy związane z bezpieczeństwem. Oprogramowanie szpiegujące może wykorzystać dostawców usługi warstwowej do monitorowania aktywności sieciowej użytkownika i modyfikacji danych. Aby uniknąć konieczności ponownej instalacji systemu Windows, należy używać programów firmy McAfee, które automatycznie usuną oprogramowanie szpiegujące i usługi warstwowe, które padły ofiarą ataku.

Polecenia Otwórz powłoki systemu Windows

Zapobiegają zmianom poleceń Otwórz powłoki systemu Windows (explorer.exe). Polecenia Otwórz powłoki umożliwiają uruchamianie określonych programów podczas otwierania pewnych typów plików. Na przykład robak może próbować uruchomić się przy każdym uruchomieniu aplikacji z rozszerzeniem .exe.

Udostępniony harmonogram zadań

Monitorowanie klucza rejestru SharedTaskScheduler, który zawiera listę programów uruchamianych podczas startu systemu Windows. Niektóre typy oprogramowania szpiegującego oraz potencjalnie niepożądane programy modyfikują ten klucz i dodają się do listy bez pozwolenia użytkownika.

Usługa Posłaniec systemu Windows

Monitorowanie usługi Posłaniec systemu Windows, która jest nieudokumentowaną funkcją programu Windows Messenger umożliwiającą użytkownikom wysyłanie wyskakujących komunikatów. Niektóre typy oprogramowania szpiegującego oraz potencjalnie niepożądane programy próbują włączyć tę usługę i za jej pośrednictwem wysyłać niepożądane reklamy. Ponieważ usługa ta jest podatna na znane zagrożenia, może również zostać niewłaściwie wykorzystana w celu zdalnego uruchomienia kodu.

Plik win.ini systemu Windows

Plik win.ini jest to tekstowy plik zawierający listę programów uruchamianych podczas startu systemu Windows. Składnia ładowania programów istnieje w tym pliku w celu umożliwienia obsługi starszych wersji systemu Windows. Większość programów nie korzysta z pliku win.ini do ładowania programów, jednakże niektóre typy oprogramowania szpiegującego lub inne potencjalnie niepożądane programy są projektowane tak, aby wykorzystywać tę składnię do ładowania się podczas uruchamiania systemu Windows.

Informacje o programach SystemGuard z kategorii Przeglądarka

Programy SystemGuard z kategorii Przeglądarka wykrywają wymienione poniżej elementy.

Obiekty pomocnicze przeglądarki

Monitorowanie dodatków do obiektów pomocniczych przeglądarki (BHO, Browser Helper Objects). Obiekty BHO są programami pełniącymi rolę dodatków plug-in przeglądarki Internet Explorer. Programy szpiegujące oraz przejmujące kontrolę nad przeglądarką często korzystają z obiektów BHO, aby wyświetlać reklamy lub śledzić zachowanie użytkowników podczas przeglądania sieci Web. Obiekty BHO są również używane przez wiele normalnych programów, takich jak popularne paski wyszukiwania.

Paski przeglądarki Internet Explorer

Monitorowanie zmian na liście programów znajdujących się na pasku przeglądarki Internet Explorer. Pasek eksploratora jest panelem, takim jak panele Szukaj, Ulubione lub Historia, które są widoczne w przeglądarce Internet Explorer (IE) lub w Eksploratorze Windows.

Dodatki plug-in przeglądarki Internet Explorer

Zapobieganie instalowaniu przez oprogramowanie szpiegujące dodatków plug-in przeglądarki Internet Explorer. Dodatki plug-in przeglądarki Internet Explorer to dodatkowe oprogramowanie ładowane wraz ze startem przeglądarki Internet Explorer. Programy szpiegujące często korzystają z dodatków plug-in przeglądarki Internet Explorer, aby wyświetlać reklamy lub śledzić zachowanie użytkowników podczas przeglądania sieci Web. Normalne dodatki plug-in poszerzają zakres funkcji przeglądarki Internet Explorer.

Obiekt ShellBrowser przeglądarki Internet Explorer

Monitorowanie zmian instancji obiektu ShellBrowser przeglądarki Internet Explorer. Obiekt ShellBrowser przeglądarki Internet Explorer zawiera informacje i ustawienia danej instancji przeglądarki Internet Explorer. Jeśli ustawienia te ulegną zmianie lub dodany zostanie nowy obiekt ShellBrowser, może on przejąć pełną kontrolę nad przeglądarką Internet Explorer, dodając funkcje, takie jak paski narzędzi, menu i przyciski.

Obiekt WebBrowser przeglądarki Internet Explorer

Monitorowanie zmian instancji obiektu WebBrowser przeglądarki Internet Explorer. Obiekt WebBrowser przeglądarki Internet Explorer zawiera informacje i ustawienia danej instancji przeglądarki Internet Explorer. Jeśli ustawienia te ulegną zmianie lub dodany zostanie nowy obiekt WebBrowser, może on przejąć pełną kontrolę nad przeglądarką Internet Explorer, dodając funkcje, takie jak paski narzędzi, menu i przyciski.

Uchwyty wyszukiwania adresów URL przeglądarki Internet Explorer

Monitorowanie zmian uchwytów wyszukiwania adresów URL przeglądarki Internet Explorer. Uchwyt wyszukiwania adresów URL używany jest wówczas, gdy użytkownik wpisze adres w polu adresu przeglądarki z pominięciem nazwy protokołu, jak na przykład http:// lub ftp://. Po wprowadzeniu takiego adresu przeglądarka może skorzystać z uchwytu wyszukiwania adresów URL w celu wyszukania w Internecie podanej lokalizacji.

Adresy URL przeglądarki Internet Explorer

Monitorowanie zmian wstępnie zdefiniowanych adresów URL przeglądarki Internet Explorer. Uniemożliwia to oprogramowaniu szpiegującemu oraz innym potencjalnie niepożądanym programom zmienianie ustawień przeglądarki bez pozwolenia użytkownika.

Ograniczenia przeglądarki Internet Explorer

Monitorowanie ograniczeń przeglądarki Internet Explorer, które pozwalają administratorowi komputera na uniemożliwienie użytkownikowi dokonywania zmian strony głównej oraz innych opcji przeglądarki Internet Explorer. Opcje te są widoczne tylko w przypadku, gdy zostały celowo ustawione przez administratora.

Strefy zabezpieczeń przeglądarki Internet Explorer

Monitorowanie stref zabezpieczeń przeglądarki Internet Explorer. Przeglądarka Internet Explorer ma cztery wstępnie zdefiniowane strefy zabezpieczeń: Internet, Lokalny intranet, Zaufane witryny oraz Witryny z ograniczeniami. Każda strefa zabezpieczeń posiada własne, wstępnie zdefiniowane lub dostosowane przez użytkownika ustawienie zabezpieczeń. Strefy zabezpieczeń stanowią cel dla niektórych typów oprogramowania szpiegującego lub innych potencjalnie niepożądanych programów, ponieważ obniżenie poziomu zabezpieczeń pozwala im ominąć alerty bezpieczeństwa i działać niezauważenie.

Zaufane witryny przeglądarki Internet Explorer

Monitorowanie zaufanych witryn przeglądarki Internet Explorer Lista zaufanych witryn jest katalogiem witryn sieci Web uznanych przez użytkownika za zaufane. Lista ta jest celem niektórych typów oprogramowania szpiegującego lub innych potencjalnie niepożądanych programów, ponieważ stanowi sposób uznania za zaufane podejrzanych witryn bez pozwolenia użytkownika.

Zasady przeglądarki Internet Explorer

Monitorowanie zasad przeglądarki Internet Explorer. Te ustawienia przeglądarki są zazwyczaj zmieniane przez administratora systemu, ale mogą być wykorzystane przez oprogramowanie szpiegujące. Zmiany mogą uniemożliwić ustawienie innej strony głównej lub ukryć karty okna dialogowego Opcje internetowe dostępnego z poziomu menu Narzędzia.

Korzystanie ze skanowania skryptów

Skrypt może tworzyć, kopiować lub usuwać pliki. Może również otworzyć rejestr systemu Windows.

Skanowanie skryptów automatycznie blokuje uruchamianie na komputerze znanych szkodliwych skryptów.

Wyłączanie skanowania skryptów

Jeśli skanowanie skryptów zostanie wyłączone, podejrzane wykonania skryptów nie będą wykrywane.

Aby wyłączyć skanowanie skryptów:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Komputer i pliki**.
3. W polu **Ochrona przez skanowanie skryptów** kliknij opcję **Wyłączona**.

Włączanie skanowania skryptów

Skanowanie skryptów ostrzega użytkownika, jeśli wykonanie skryptu prowadzi do utworzenia, skopiowania lub usunięcia pliku albo otwarcia rejestru systemu Windows.

Aby włączyć skanowanie skryptów:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Komputer i pliki**.
3. W polu **Ochrona przez skanowanie skryptów** kliknij opcję **Włączona**.

Korzystanie z ochrony poczty e-mail

Ochrona poczty e-mail wykrywa i blokuje zagrożenia w poczcie przychodzącej (POP3) i wychodzącej (SMTP) oraz w załącznikach zawierających wirusy, konie trojańskie, robaki, oprogramowanie szpiegujące, reklamowe i inne zagrożenia.

Wyłączanie ochrony poczty e-mail

Jeśli ochrona poczty e-mail zostanie wyłączona, potencjalne zagrożenia w poczcie przychodzącej (POP3), wychodzącej (SMTP) i załącznikach nie będą wykrywane.

Aby wyłączyć ochronę poczty e-mail:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W polu **Ochrona poczty e-mail** kliknij opcję **Wyłączona**.

Włączanie ochrony poczty e-mail

Ochrona poczty e-mail wykrywa zagrożenia w poczcie przychodzącej (POP3), wychodzącej (SMTP) oraz w załącznikach.

Aby włączyć ochronę poczty e-mail:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W polu **Ochrona poczty e-mail** kliknij opcję **Włączona**.

Konfigurowanie ochrony poczty e-mail

Opcje ochrony wiadomości e-mail pozwalają na skanowanie otrzymywanych i wysyłanych wiadomości oraz kontrolę aktywności robaków. Robaki replikują się i zużywają zasoby systemu, spowalniając lub zatrzymując zadania. Robaki mogą wysyłać swoje własne kopie poprzez wiadomości e-mail. Mogą na przykład próbować rozesłać wiadomości e-mail do osób znajdujących się w książce adresowej.

Konfiguracja ochrony poczty e-mail

Opcje ochrony wiadomości e-mail pozwalają na skanowanie otrzymywanych i wysyłanych wiadomości oraz kontrolę aktywności robaków.

Aby skonfigurować ochronę poczty e-mail:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona poczty e-mail** kliknij opcję **Zaawansowane**.
4. Zaznacz lub usuń zaznaczenie następujących pól:
   - **Skanuj przychodzące wiadomości e-mail**: Wiadomości przychodzące (POP3) będą skanowane pod kątem wystąpienia potencjalnych zagrożeń.
   - **Skanuj wychodzące wiadomości e-mail**: Wiadomości wychodzące (SMTP) będą skanowane pod kątem wystąpienia potencjalnych zagrożeń.
   - **Włącz program WormStopper**: Program WormStopper blokuje robaki w wiadomościach e-mail.
5. Kliknij przycisk **OK**.

Korzystanie z ochrony wiadomości błyskawicznych

Ochrona wiadomości błyskawicznych wykrywa zagrożenia w przychodzących załącznikach wiadomości błyskawicznych.

Wyłączanie ochrony wiadomości błyskawicznych

Jeśli ochrona wiadomości błyskawicznych zostanie wyłączona, zagrożenia w przychodzących załącznikach wiadomości błyskawicznych nie będą wykrywane.

Aby wyłączyć ochronę wiadomości błyskawicznych:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. Pod polu **Ochrona wiadomości błyskawicznych** kliknij opcję **Wyłączona**.

Włączanie ochrony wiadomości błyskawicznych

Ochrona wiadomości błyskawicznych wykrywa zagrożenia w przychodzących załącznikach wiadomości błyskawicznych.

Aby włączyć ochronę wiadomości błyskawicznych:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. Pod polu **Ochrona wiadomości błyskawicznych** kliknij opcję **Włączona**.

ROZDZIAŁ 15

Ręczne skanowanie komputera

Wirusy i inne zagrożenia można wyszukiwać na dyskach twardych, dyskietkach oraz w pojedynczych plikach i folderach. Jeżeli program VirusScan wykryje podejrzany plik, spróbuje go wyczyścić, o ile ten plik nie jest potencjalnie niepożądanym programem. Jeśli program VirusScan nie jest w stanie wyczyścić pliku, można go poddać kwarantannie lub usunąć.

W tym rozdziale

Skanowanie ręczne.....98

Skanowanie ręczne

Skanowanie ręczne można przeprowadzić w dowolnym momencie. Na przykład, jeśli program VirusScan został właśnie zainstalowany, można przeprowadzić skanowanie, aby upewnić się, że w komputerze nie ma żadnych wirusów ani innych zagrożeń. Innym przykładem jest sytuacja, kiedy zostało wyłączone skanowanie w czasie rzeczywistym. Można wtedy przeprowadzić skanowanie, aby upewnić się, że komputer wciąż jest bezpieczny.

Skanowanie z użyciem ustawień ręcznego skanowania

Ten typ skanowania używa określonych przez użytkownika ustawień ręcznego skanowania. Program VirusScan skanuje zawartość skompresowanego pliku (z rozszerzeniami .zip, .cab itp.), ale zlicza go jako jeden plik. Ponadto wyświetlana liczba przeskanowanych plików może być inna niż w rzeczywistości, jeśli w okresie, jaki upłynął od ostatniego skanowania, usunięto tymczasowe pliki internetowe.

Aby wykonać skanowanie z użyciem ustawień ręcznego skanowania:

1. W Menu podstawowym kliknij opcję **Skanuj**. Po zakończeniu skanowania jest wyświetlane podsumowanie pokazujące liczbę przeskanowanych i wykrytych elementów, liczbę elementów wyczyszczonych oraz datę ostatniego skanowania.
2. Kliknij przycisk **Zakończ**.

Tematy pokrewne

- Konfigurowanie ręcznego skanowania (strona 100)

Skanowanie bez użycia ustawień ręcznego skanowania

Ten typ skanowania nie używa określonych przez użytkownika ustawień ręcznego skanowania. Program VirusScan skanuje zawartość skompresowanego pliku (z rozszerzeniami .zip, .cab itp.), ale zlicza go jako jeden plik. Ponadto wyświetlana liczba przeskanowanych plików może być inna niż w rzeczywistości, jeśli w okresie, jaki upłynął od ostatniego skanowania, usunięto tymczasowe pliki internetowe.

Aby wykonać skanowanie bez użycia ustawień ręcznego skanowania:

1. W Menu zaawansowanym kliknij opcję **Początek**.
2. W okienku Początek kliknij przycisk **Skanuj**.
3. W obszarze **Lokalizacje do skanowania** zaznacz pola wyboru obok plików, folderów i dysków, które mają zostać zeskanowane.
4. W obszarze **Opcje** zaznacz pola wyboru obok typów plików, które mają zostać zeskanowane.
5. Kliknij przycisk **Skanuj teraz**. Po zakończeniu skanowania jest wyświetlane podsumowanie pokazujące liczbę przeskanowanych i wykrytych elementów, liczbę elementów wyczyszczonych oraz datę ostatniego skanowania.
6. Kliknij przycisk **Zakończ**.

Uwaga: Te opcje nie są zapisywane.

Skanowanie z poziomu Eksploratora Windows

Możliwe jest wykonanie skanowania w poszukiwaniu wirusów i innych zagrożeń w wybranych plikach, folderach lub na dyskach bezpośrednio z Eksploratora Windows.

Aby zeskanować pliki z poziomu Eksploratora Windows:

1. Otwórz Eksploratora Windows.
2. Kliknij prawym przyciskiem myszy dysk, folder lub plik, który ma zostać przeskanowany, a następnie kliknij przycisk **Skanuj**. Wybierane są wszystkie ustawienia domyślne, aby zapewnić najbardziej dokładne skanowanie.

Konfigurowanie ręcznego skanowania

Przeprowadzając skanowanie ręczne lub zaplanowane, można określić typy plików do skanowania, lokalizacje przeznaczone do skanowania oraz termin rozpoczęcia skanowania.

Konfigurowanie typów plików, które będą skanowane

Można skonfigurować typy plików, które mają być skanowane.

Aby skonfigurować typy plików do skanowania:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Komputer i pliki**.
3. W obszarze **Ochrona przed wirusami** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed wirusami kliknij przycisk **Skanowanie ręczne**.
5. Zaznacz lub usuń zaznaczenie następujących pól:
   - **Skanuj w poszukiwaniu nieznanych wirusów przy użyciu heurystyk**: Pliki są dopasowywane do sygnatur znanych wirusów w celu wykrycia obecności niezidentyfikowanych wirusów. Opcja skanowania w poszukiwaniu nowych, nieznanych wirusów zapewnia największą dokładność skanowania, ale wiąże się z wydłużeniem czasu pracy skanera.
   - **Skanuj pliki .zip i inne pliki archiwów**: Są wykrywane i usuwane wirusy w plikach .zip i innych plikach archiwów. Zdarza się, że wirusy są umieszczane w plikach ZIP, które z kolei są dodawane do innych zbiorów ZIP w celu oszukania skanerów antywirusowych.
   - **Skanuj w poszukiwaniu programów szpiegujących i potencjalnie niepożądanych**: Oprogramowanie szpiegujące i reklamowe oraz inne programy, które potencjalnie gromadzą i wysyłają dane użytkowników bez ich zgody, są wykrywane i usuwane.
   - **Skanuj i usuwaj śledzące pliki cookie**: Pliki cookie, które potencjalnie gromadzą i wysyłają dane bez zgody użytkownika, są wykrywane i usuwane. Plik cookie identyfikuje użytkowników odwiedzających witrynę internetową.
   - **Skanuj w poszukiwaniu programów typu rootkit i stealth**: Są wykrywane i usuwane programy typu rootkit oraz inne programy, które ukrywają się przed systemem Windows.
6. Kliknij jeden z poniższych przycisków:
   - **Wszystkie pliki (zalecane)**: Skanowane są pliki wszystkich typów używanych w systemie. Opcji tej należy użyć, aby zapewnić najdokładniejsze skanowanie komputera.

- **Tylko pliki programów i dokumenty**: Skanowane są tylko pliki programów i dokumenty.

7 Kliknij przycisk **OK**.

Konfiguracja lokalizacji przeznaczonych do skanowania

Można skonfigurować lokalizacje, które mają być skanowane podczas skanowania ręcznego lub zaplanowanego.

Aby określić miejsce skanowania:

1 W Menu zaawansowanym kliknij opcję **Konfiguruj**.

2 W okienku konfiguracji kliknij opcję **Komputer i pliki**.

3 W obszarze **Ochrona przed wirusami** kliknij przycisk **Zaawansowane**.

4 W okienku Ochrona przed wirusami kliknij przycisk **Skanowanie ręczne**.

5 W obszarze **Domyślna lokalizacja do skanowania** zaznacz pola wyboru obok plików, folderów i dysków, które mają zostać zeskanowane.

W celu zapewnienia możliwie najdokładniejszego skanowania należy się upewnić, że zaznaczono pole **Krytyczne pliki**.

6 Kliknij przycisk **OK**.

Planowanie skanowań

Możliwe jest zaplanowanie skanowań w celu kompleksowego sprawdzenia komputera pod kątem obecności wirusów i innych zagrożeń w określonych odstępach czasu.

Aby zaplanować skanowanie:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Komputer i pliki**.
3. W obszarze **Ochrona przed wirusami** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed wirusami kliknij przycisk **Zaplanowane skanowanie**.
5. Upewnij się, że zostało zaznaczone pole **Włącz skanowanie według harmonogramu**.
6. Zaznacz pole wyboru obok dnia tygodnia, w którym ma być wykonywane skanowanie.
7. Aby określić godzinę rozpoczęcia, kliknij odpowiednie wartości na listach czasu rozpoczęcia.
8. Kliknij przycisk **OK**.

Wskazówka: Aby użyć domyślnego harmonogramu, kliknij przycisk **Resetuj.**

ROZDZIAŁ 16

Administrowanie programem VirusScan

Można usuwać pozycje z listy zaufanych programów, zarządzać plikami poddanymi kwarantannie, plikami cookie oraz innymi plikami, przeglądać zdarzenia i dzienniki oraz wysyłać raporty o podejrzanych działaniach do firmy McAfee.

W tym rozdziale

Zarządzanie listami elementów zaufanych 104
Zarządzanie poddanymi kwarantannie programami, plikami cookie i innymi plikami 105
Przeglądanie ostatnich zdarzeń i dzienników..... 107
Automatyczne przesyłanie anonimowych informacji 108
Jak działa system generowania alertów zabezpieczeń 109

Zarządzanie listami elementów zaufanych

Gdy użytkownik ufa programowi SystemGuard, programowi, przepełnieniu buforu lub klientowi poczty e-mail, taki element może zostać dodany do listy elementów zaufanych, dzięki czemu nie będzie już wykrywany jako zagrożenie.

Jeśli okaże się, że programowi zaufano przez pomyłkę lub jeśli ma on być wykrywany, należy usunąć go z tej listy.

Zarządzanie listami elementów zaufanych

Gdy użytkownik ufa programowi SystemGuard, programowi, przepełnieniu buforu lub klientowi poczty e-mail, taki element może zostać dodany do listy elementów zaufanych, dzięki czemu nie będzie już wykrywany jako zagrożenie.

Jeśli okaże się, że programowi zaufano przez pomyłkę lub jeśli ma on być wykrywany, należy usunąć go z tej listy.

Aby usunąć elementy z listy zaufanych:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Komputer i pliki**.
3. W obszarze **Ochrona przed wirusami** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed wirusami kliknij przycisk **Listy zaufanych adresów**.
5. Na liście zaznacz zaufaną aplikację SystemGuard, program, przepełnienie buforu lub klienta poczty e-mail, aby wyświetlić jego elementy i ich stan zaufania.
6. W obszarze **Szczegóły** sprawdź informacje o danym elemencie.
7. W obszarze **Działanie** kliknij odpowiednią akcję.
8. Kliknij przycisk **OK**.

Zarządzanie poddanymi kwarantannie programami, plikami cookie i innymi plikami

Programy poddane kwarantannie, pliki cookie i inne pliki można przywrócić, usunąć lub wysłać do analizy do firmy McAfee.

Przywracanie programów poddanych kwarantannie, plików cookie i innych plików

Jeśli jest to konieczne, można przywrócić poddane kwarantannie programy, pliki cookie i inne pliki.

Aby przywrócić programy poddane kwarantannie, pliki cookie i inne pliki:

1. W Menu zaawansowanym kliknij opcję **Przywróć**.
2. W okienku przywracania kliknij opcję **Programy i pliki cookie** lub **Pliki**, zależnie od wymaganego działania.
3. Wybierz poddane kwarantannie programy, pliki cookie lub inne pliki, które mają zostać przywrócone.
4. Aby uzyskać więcej informacji na temat wirusa poddanego kwarantannie, kliknij jego nazwę wykrywania w polu **Szczegóły**. Zostanie wyświetlona biblioteka informacji o wirusach z opisem wirusa.
5. W obszarze **Działanie** kliknij przycisk **Przywróć**.

Usuwanie poddanych kwarantannie programów, plików cookie i innych plików

Można usunąć poddane kwarantannie programy, pliki cookie i inne pliki.

Aby usunąć poddane kwarantannie programy, pliki cookie i inne pliki:

1. W Menu zaawansowanym kliknij opcję **Przywróć**.
2. W okienku przywracania kliknij opcję **Programy i pliki cookie** lub **Pliki**, zależnie od wymaganego działania.
3. Wybierz poddane kwarantannie programy, pliki cookie lub inne pliki, które mają zostać przywrócone.
4. Aby uzyskać więcej informacji na temat wirusa poddanego kwarantannie, kliknij jego nazwę wykrywania w polu **Szczegóły**. Zostanie wyświetlona biblioteka informacji o wirusach z opisem wirusa.
5. W obszarze **Działanie** kliknij przycisk **Usuń**.

Wysyłanie programów poddanych kwarantannie, plików cookie i innych plików do firmy McAfee

Można wysyłać poddane kwarantannie programy, pliki cookie i inne pliki do firmy McAfee w celu ich analizy.

Uwaga: Jeśli wysyłany plik przekroczy maksymalny dopuszczalny rozmiar, może zostać odrzucony. W większości przypadków tak się nie dzieje.

Aby wysłać poddane kwarantannie programy lub inne pliki do firmy McAfee:

1. W Menu zaawansowanym kliknij opcję **Przywróć**.
2. W okienku przywracania kliknij opcję **Programy i pliki cookie** lub **Pliki**, zależnie od wymaganego działania.
3. Wybierz poddane kwarantannie programy, pliki cookie lub inne pliki, które mają zostać wysłane do firmy McAfee.
4. Aby uzyskać więcej informacji na temat wirusa poddanego kwarantannie, kliknij jego nazwę wykrywania w polu **Szczegóły**. Zostanie wyświetlona biblioteka informacji o wirusach z opisem wirusa.
5. W obszarze **Działanie** kliknij opcję **Wyślij do firmy McAfee**.

Przeglądanie ostatnich zdarzeń i dzienników

Lista ostatnich zdarzeń i dzienniki zawierają zdarzenia pochodzące ze wszystkich zainstalowanych produktów firmy McAfee.

Na liście Ostatnie zdarzenia można sprawdzić ostatnie 30 istotnych zdarzeń, które nastąpiły na komputerze. Można tu przywrócić zablokowane programy, włączyć ponownie skanowanie w czasie rzeczywistym oraz określić zaufane przepełnienia buforu.

Można również wyświetlić dzienniki, w których zostały zapisane wszystkie zdarzenia, które nastąpiły w ciągu ostatnich 30 dni.

Przeglądanie zdarzeń

Na liście Ostatnie zdarzenia można sprawdzić ostatnie 30 istotnych zdarzeń, które nastąpiły na komputerze. Można tu przywrócić zablokowane programy, włączyć ponownie skanowanie w czasie rzeczywistym oraz określić zaufane przepełnienia buforu.

Aby wyświetlić zdarzenia:

1. W Menu zaawansowanym kliknij opcję **Raporty i dzienniki**.
2. W okienku Raporty i dzienniki kliknij opcję **Ostatnie zdarzenia**.
3. Wybierz zdarzenie, które ma zostać wyświetlone.
4. W obszarze **Szczegóły** sprawdź informacje o danym zdarzeniu.
5. W obszarze **Działanie** kliknij odpowiednią akcję.

Wyświetlanie dziennika

W dziennikach zapisane jest każde zdarzenie, które miało miejsce w ciągu ostatnich 30 dni.

Aby wyświetlić dzienniki:

1. W Menu zaawansowanym kliknij opcję **Raporty i dzienniki**.
2. W okienku Raporty i dzienniki kliknij opcję **Ostatnie zdarzenia**.
3. W okienku Ostatnie zdarzenia kliknij opcję **Wyświetl dziennik**.
4. Wybierz typ dziennika, który ma zostać wyświetlony, a następnie wybierz dziennik.
5. W obszarze **Szczegóły** sprawdź informacje z danego dziennika.

Automatyczne przesyłanie anonimowych informacji

Możliwe jest anonimowe przesyłanie do firmy McAfee wirusa, potencjalnie niepożądanego programu lub informacji pozwalających śledzić hakerów. Ta opcja jest dostępna tylko podczas instalacji.

Nie są zbierane żadne informacje mogące posłużyć do identyfikacji osoby.

Wysyłanie raportów do firmy McAfee

Możliwe jest przesyłanie do firmy McAfee wirusa, potencjalnie niepożądanego programu lub informacji pozwalających śledzić hakerów. Ta opcja jest dostępna tylko podczas instalacji.

Aby automatycznie przesyłać anonimowe informacje:

1. Podczas instalacji programu VirusScan zaakceptuj domyślne ustawienie opcji **Prześlij anonimowe informacje**.
2. Kliknij przycisk **Dalej**.

Jak działa system generowania alertów zabezpieczeń

Jeśli skanowanie w czasie rzeczywistym wykryje zagrożenie, wyświetlany jest alert. W przypadku większości wirusów, koni trojańskich, skryptów i robaków, skanowanie w czasie rzeczywistym automatycznie próbuje wyczyścić plik i wyświetla alert. W przypadku potencjalnie niepożądanych programów i zdarzeń objętych ochroną SystemGuard skanowanie w czasie rzeczywistym wykrywa plik lub zmianę i wyświetla alert. W przypadku przepełnienia buforu, śledzenia plików cookie oraz aktywności skryptów skanowanie w czasie rzeczywistym automatycznie blokuje działanie i wyświetla alert.

Alerty te można podzielić na trzy podstawowe typy.

- Czerwony alert
- Żółty alert
- Zielony alert

Użytkownik może zdefiniować działania podejmowane przez program po wykryciu plików, wiadomości e-mail, podejrzanych skryptów, a także potencjalnych robaków i potencjalnie niepożądanych programów, zdarzeń objętych ochroną SystemGuard lub przepełnień buforu.

Zarządzanie alertami

Programy firmy McAfee korzystają z szeregu alertów pomagających użytkownikowi w zarządzaniu bezpieczeństwem. Alerty te można podzielić na trzy podstawowe typy.

- Czerwony alert
- Żółty alert
- Zielony alert

Czerwony alert

Czerwony alert wymaga odpowiedzi ze strony użytkownika. W niektórych przypadkach program firmy McAfee nie potrafi określić, jak automatycznie odpowiedzieć na konkretne działanie. W takiej sytuacji czerwony alert opisuje dane działanie i daje użytkownikowi do wyboru jedną lub więcej opcji.

Żółty alert

Żółty alert to niekrytyczne powiadomienie, które zazwyczaj wymaga odpowiedzi ze strony użytkownika. Żółty alert opisuje dane działanie i daje użytkownikowi do wyboru jedną lub więcej opcji.

Zielony alert

W większości przypadków zielony alert zawiera podstawowe informacje o zdarzeniu i nie wymaga reakcji.

Konfigurowanie opcji alertów

Jeśli użytkownik zdecyduje się nie wyświetlać więcej danego alertu, a później zmieni zdanie, może wrócić i skonfigurować alert w ten sposób, aby się znowu pojawiał. Więcej informacji na temat konfigurowania opcji alertów można znaleźć w dokumentacji programu SecurityCenter.

ROZDZIAŁ 17

Dodatkowa pomoc

W tym rozdziale omówiono często zadawane pytania oraz scenariusze rozwiązywania problemów.

W tym rozdziale

Często zadawane pytania 112
Rozwiązywanie problemów 114

Często zadawane pytania

Ten rozdział zawiera odpowiedzi na najczęściej zadawane pytania.

Zostało wykryte zagrożenie — co robić?

Programy firmy McAfee korzystają z alertów pomagających użytkownikowi w zarządzaniu bezpieczeństwem. Alerty te można podzielić na trzy podstawowe typy.

- Czerwony alert
- Żółty alert
- Zielony alert

Użytkownik może zdefiniować działania podejmowane przez program po wykryciu plików, wiadomości e-mail, podejrzanych skryptów, a także potencjalnych robaków i potencjalnie niepożądanych programów, programów SystemGuard lub przepełnień buforu.

Więcej informacji na temat zarządzania poszczególnymi zagrożeniami można znaleźć w bibliotece informacji o wirusach, pod adresem: http://us.mcafee.com/virusInfo/default.asp?affid=.

Tematy pokrewne

- Jak działa system generowania alertów zabezpieczeń (strona 109)

Czy mogę używać programu VirusScan z przeglądarkami Netscape, Firefox i Opera?

Można używać przeglądarki Netscape, Firefox lub Opera jako przeglądarki domyślnej, ale konieczne jest zainstalowanie na komputerze przeglądarki Microsoft Internet Explorer w wersji 6.0 lub nowszej.

Czy podczas skanowania komputer powinien być połączony z Internetem?

Aby wykonać skanowanie komputer nie musi być połączony z Internetem, ale należy się z nim łączyć co najmniej raz w tygodniu w celu pobrania aktualizacji z firmy McAfee.

Czy program VirusScan skanuje załączniki poczty e-mail?

Jeśli włączone jest skanowanie w czasie rzeczywistym i ochrona poczty e-mail, skanowany jest każdy załącznik, gdy tylko odbierana jest wiadomość e-mail.

Czy program VirusScan skanuje pliki wewnątrz archiwów ZIP?

Program VirusScan skanuje zarówno pliki .zip, jak i inne pliki archiwów.

Dlaczego podczas skanowania wychodzących wiadomości e-mail występują błędy?

W trakcie skanowania wiadomości wychodzących mogą wystąpić następujące rodzaje błędów:

- Błąd protokołu. Serwer poczty e-mail odrzucił wiadomość.
  W przypadku wystąpienia błędu protokołu lub błędu systemowego pozostałe wiadomości e-mail dla danej sesji będą przetwarzane i wysyłane do serwera.
- Błąd połączenia. Połączenie z serwerem poczty e-mail zostało przerwane.
  Jeśli wystąpi błąd połączenia, upewnij się, że komputer jest połączony z Internetem, po czym spróbuj ponownie wysłać wiadomość z listy **Elementy wysłane** w programie pocztowym.
- Błąd systemu. Wystąpił błąd obsługi plików lub inny błąd systemowy.
- Błąd szyfrowanego połączenia SMTP. Wykryto szyfrowane połączenie SMTP zainicjowane przez używany program pocztowy. W przypadku wystąpienia błędu szyfrowanego połączenia SMTP wymagane jest wyłączenie szyfrowanego połączenia SMTP w programie pocztowym, aby umożliwić skanowanie wiadomości e-mail.

Jeśli przy wysyłaniu wiadomości e-mail zostanie przekroczony limit czasu, należy wyłączyć opcję skanowania poczty wychodzącej albo wyłączyć szyfrowane połączenia SMTP w programie pocztowym.

Tematy pokrewne

- Konfiguracja ochrony poczty e-mail (strona 95)

Rozwiązywanie problemów

Ten rozdział zawiera pomoc dotyczącą ogólnych problemów, jakie może napotkać użytkownik.

Wirusa nie można wyczyścić ani usunąć

W przypadku niektórych wirusów konieczne jest ręczne wyczyszczenie komputera. Spróbuj ponownie uruchomić komputer, a następnie jeszcze raz przeprowadzić skanowanie.

Jeśli komputer nie jest w stanie wyczyścić ani usunąć wirusa, należy poszukać dodatkowych informacji w Bibliotece informacji o wirusach, pod adresem http://us.mcafee.com/virusInfo/default.asp?affid=.

Dodatkową pomoc można uzyskać w witrynie sieci Web firmy McAfee poświęconej obsłudze klienta.

Uwaga: Nie można usunąć wirusów z dysków CD-ROM, DVD ani dyskietek zabezpieczonych przed zapisem.

Po ponownym uruchomieniu komputera nadal nie można usunąć elementu

W niektórych sytuacjach po zeskanowaniu i usunięciu elementów konieczne jest ponowne uruchomienie komputera.

Jeśli element nie zostanie usunięty po ponownym uruchomieniu komputera, należy wysłać plik do firmy McAfee.

Uwaga: Nie można usunąć wirusów z dysków CD-ROM, DVD ani dyskietek zabezpieczonych przed zapisem.

Tematy pokrewne

- Zarządzanie poddanymi kwarantannie programami, plikami cookie i innymi plikami (strona 105)

Brakuje niektórych składników lub są one uszkodzone

W pewnych sytuacjach program VirusScan może nie zostać poprawnie zainstalowany:

- Gdy na dysku komputera jest za mało wolnego miejsca lub w komputerze jest się za mało pamięci. Należy sprawdzić, czy komputer spełnia wymagania niezbędne do poprawnej pracy programu.
- Gdy przeglądarka internetowa jest nieprawidłowo skonfigurowana.
- Gdy połączenie z Internetem nie działa prawidłowo. Sprawdź, czy połączenie działa poprawnie. Jeśli tak nie jest, spróbuj połączyć się jeszcze raz w późniejszym czasie.
- Brakuje plików lub instalacja się nie powiodła.

Najlepszym wyjściem jest rozwiązanie tych potencjalnych problemów, a następnie ponowne zainstalowanie programu VirusScan.

ROZDZIAŁ 18

McAfee Personal Firewall

Program Personal Firewall zapewnia zaawansowaną ochronę komputera i danych osobistych. Program Personal Firewall tworzy barierę między komputerem a Internetem, dyskretnie monitorując ruch internetowy w poszukiwaniu podejrzanych działań.

W tym rozdziale

Funkcje 118
Uruchamianie zapory 121
Praca z alertami 123
Zarządzanie alertami informacyjnymi 127
Konfigurowanie ochrony przy użyciu zapory 129
Zarządzanie programami i uprawnieniami 141
Zarządzanie usługami systemowymi 153
Zarządzanie połączeniami z komputerem 157
Rejestrowanie, monitorowanie i analiza 169
Informacje o bezpieczeństwie internetowym 183

Funkcje

Program Personal Firewall zapewnia kompleksową ochronę połączeń przychodzących i wychodzących przy użyciu zapory oraz automatycznie dopuszcza zaufane aplikacje i wspomaga blokowanie oprogramowania szpiegującego, koni trojańskich i programów rejestrujących znaki wpisywane z klawiatury. Broni on przed skanowaniem i atakami hakerów, monitoruje ruch internetowy i sieciowy, wyświetla alerty o potencjalnie wrogich lub podejrzanych zdarzeniach, podaje szczegółowe informacje o ruchu internetowym oraz stanowi uzupełnienie ochrony antywirusowej.

Standardowy poziomy ochrony i poziomy niestandardowe

Ochrona przed włamaniami i podejrzanymi działaniami z użyciem domyślnych ustawień programu Firewall lub ustawień niestandardowych, dostosowanych do wymagań użytkownika w zakresie bezpieczeństwa.

Wyświetlane na bieżąco zalecenia

Otrzymywanie na bieżąco zaleceń pomaga w określeniu, czy programom należy przyznać dostęp do Internetu oraz, czy dany ruch sieciowy jest godny zaufania.

„Inteligentne" zarządzanie dostępem programów

Zarządzanie dostępem programów do Internetu za pośrednictwem alertów i dzienników zdarzeń lub konfigurowanie w programie Firewall uprawnień dostępu dla określonych aplikacji w okienku Uprawnienia programów.

Niezakłócanie korzystania z gier

Zapobieganie wyświetlaniu alertów dotyczących prób włamania i podejrzanych działań w trakcie korzystania z gier na pełnym ekranie oraz konfigurowanie programu Firewall tak, by alerty były wyświetlane po zakończeniu gry.

Ochrona komputera podczas uruchamiania

Przed uruchomieniem systemu Windows program Firewall chroni komputer użytkownika przed próbami włamania, niepożądanymi programami i niepożądanym ruchem sieciowym.

Nadzorowanie portów usług systemowych

Porty usług systemowych mogą być furtką otwierającą dostęp do komputera. Program Firewall pozwala na tworzenie otwartych i zamkniętych portów usług systemowych wymaganych przez niektóre aplikacje oraz na zarządzanie nimi.

Zarządzanie połączeniami z komputerem

Określanie zaufanych zdalnych połączeń i adresów IP, z których można łączyć się z komputerem użytkownika, oraz blokowanie ich.

Kompleksowe informacje w witrynie HackerWatch

Witryna HackerWatch jest miejscem gromadzenia informacji na temat bezpieczeństwa, w którym śledzi się pochodzące z całego świata wzorce ataków i włamań. Dostarcza ona również najświeższych wiadomości o programach działających na komputerze użytkownika. Można w niej przeglądać kompleksowe statystyki zdarzeń dotyczących bezpieczeństwa i portów internetowych.

Blokowanie programu Firewall

Natychmiastowe zablokowanie całego przychodzącego i wychodzącego ruchu sieciowego między komputerem użytkownika a Internetem.

Przywracanie ustawień programu Firewall

Natychmiastowe przywracanie pierwotnych ustawień ochrony programu Firewall. Jeśli program Personal Firewall zaczyna działać w niepożądany sposób i nie udaje się tego skorygować, można przywrócić jego ustawienia domyślne.

Zaawansowane wykrywanie koni trojańskich

Łączy zarządzanie połączeniami programów z ulepszoną bazą danych w celu wykrywania i blokowania dostępu do Internetu potencjalnie złośliwych aplikacji, takich jak konie trojańskie, oraz zapobiegania przekazywaniu danych osobistych użytkownika.

Rejestrowanie zdarzeń

Rejestrowanie zdarzeń można włączyć i wyłączyć. Jeśli jest ono włączone, można określić, które typy zdarzeń mają być rejestrowane. Rejestrowanie zdarzeń pozwala na wyświetlanie ostatnich zdarzeń przychodzących i wychodzących. Można także wyświetlać zdarzenia wykrywania włamań.

Monitorowanie ruchu internetowego

Możliwość przeglądania czytelnych map geograficznych, które przedstawiają źródła wrogich ataków i ruchu na całym świecie. Ponadto można uzyskać szczegółowe informacje na temat właściciela oraz dane geograficzne źródłowych adresów IP. Można również analizować ruch przychodzący i wychodzący oraz monitorować wykorzystanie przepustowości przez programy i ich działanie.

Ochrona przed włamaniami

Ochrona prywatności użytkownika za pośrednictwem systemu zabezpieczeń przed włamaniami i potencjalnymi zagrożeniami pochodzącymi z Internetu. Za pomocą funkcji zbliżonych do heurystycznych firma McAfee zapewnia trójwarstwową ochronę przez blokowanie elementów wykazujących symptomy ataków lub cechy charakterystyczne dla prób włamań.

Zaawansowana analiza ruchu

Sprawdzanie przychodzącego i wychodzącego ruchu internetowego oraz połączeń programów, m.in. takich, które aktywnie „nasłuchują” w oczekiwaniu na otwarcie połączeń. Umożliwia to zauważenie programów, które mogą być narażone na włamania, i podjęcie w stosunku do nich odpowiednich działań.

Uruchamianie zapory

Po zainstalowaniu zapory komputer będzie chroniony przed włamaniami i niepożądanym ruchem sieciowym. Ponadto można obsługiwać alerty i zarządzać dostępem dla przychodzących i wychodzących połączeń z Internetem znanych i nieznanych programów. Automatycznie zostaną włączone inteligentne zalecenia i standardowy poziom zabezpieczeń.

Jeśli zapora zostanie wyłączona w okienku Konfiguracja sieci i Internetu, komputer przestanie być chroniony przed włamaniami i niepożądanym ruchem sieciowym oraz nie będzie możliwe skuteczne zarządzanie przychodzącymi i wychodzącymi połączeniami internetowymi. Jeśli trzeba wyłączyć ochronę przy użyciu zapory, należy to robić tymczasowo i tylko w razie potrzeby. Zaporę można również wyłączyć w panelu Konfiguracja sieci i Internetu.

Zapora automatycznie wyłącza zaporę systemu Windows® i staje się zaporą domyślną.

Uwaga: Aby skonfigurować program Firewall, należy otworzyć okienko Konfiguracja Internetu i sieci.

Uruchamianie zapory

Włączenie ochrony przy użyciu zapory chroni komputer przed włamaniami i niepożądanym ruchem sieciowym oraz pomaga w zarządzaniu wychodzącymi i przychodzącymi połączeniami z Internetem.

Aby włączyć ochronę przy użyciu zapory:

1. W okienku programu McAfee SecurityCenter wykonaj jedną z następujących czynności:
   - Kliknij opcję **Internet i sieć**, a następnie opcję **Konfiguruj**.
   - Kliknij opcję **Menu zaawansowane**, następnie opcję **Konfiguruj** w okienku **Początek**, a potem wybierz opcję **Internet i sieć**.
2. W okienku **Konfiguracja Internetu i sieci**, w obszarze **Ochrona przy użyciu zapory** kliknij opcję **Włącz**.

Zatrzymywanie zapory

Wyłączenie ochrony przy użyciu zapory powoduje narażenie komputera na włamania i niepożądany ruch sieciowy. Przy wyłączonej ochronie przy użyciu zapory nie można zarządzać przychodzącymi i wychodzącymi połączeniami internetowymi.

Aby wyłączyć ochronę przy użyciu zapory:

1. W okienku programu McAfee SecurityCenter wykonaj jedną z następujących czynności:
   - Kliknij opcję **Internet i sieć**, a następnie opcję **Konfiguruj**.
   - Kliknij opcję **Menu zaawansowane**, następnie opcję **Konfiguruj** w okienku **Początek**, a potem wybierz opcję **Internet i sieć**.
2. W okienku **Konfiguracja Internetu i sieci**, w obszarze **Ochrona przy użyciu zapory** kliknij opcję **Wyłącz**.

Praca z alertami

Zapora wykorzystuje szereg alertów pomagających zarządzać bezpieczeństwem użytkownika. Alert te można podzielić na cztery podstawowe typy.

- Alert Koń trojański został zablokowany
- Czerwony alert
- Żółty alert
- Zielony alert

Alerty mogą także zawierać informacje pomocne w podjęciu reakcji na nie lub uzyskaniu informacji o programach działających na komputerze.

Informacje o alertach

Zapora wykorzystuje cztery podstawowe typy alertów. Ponadto w niektórych alertach są zawarte informacje pomagające uzyskać informacje o programach działających na komputerze użytkownika.

Alert Koń trojański został zablokowany

Koń trojański sprawia wrażenie normalnego programu, lecz może zakłócić pracę komputera użytkownika, uszkodzić go lub umożliwić nieautoryzowany dostęp do niego. Alert o koniu trojańskim zostaje wyświetlony, gdy przy użyciu zapory wykryto a następnie zablokowano konia trojańskiego na komputerze użytkownika i zawiera zalecenie wykonania skanowania w celu wykrycia dodatkowych zagrożeń. Ten alert występuje na każdym poziomie zabezpieczeń z wyjątkiem poziomu Otwarty, lub gdy wyłączono inteligentne zalecenia.

Czerwony alert

Najczęściej występujący typ alertu to alert czerwony, który na ogół wymaga reakcji użytkownika. W pewnych sytuacjach automatyczne określenie przy użyciu zapory dokładnego przebiegu działań w stosunku do programu lub zdarzenia sieciowego jest niemożliwe. Dlatego alert zawiera opis działań w stosunku do programu lub zdarzenia sieciowego poprzedzający jedną lub więcej opcji, na które użytkownik musi odpowiedzieć. Jeśli inteligentne zalecenia są włączone, programy są dodawane do listy w okienku Uprawnienia programów.

Poniżej opisano najczęściej występujące opisy alertów:

- **Program żąda dostępu do Internetu**: Zapora wykryła program próbujący uzyskać dostęp do Internetu.
- **Program został zmodyfikowany**: Zapora wykryła program, który został w pewien sposób zmieniony, być może wskutek aktualizacji w trybie online.
- **Program zablokowany**: Zapora zablokowała program, ponieważ znajduje się on na liście w okienku Uprawnienia programów.

W zależności od ustawień użytkownika oraz działań programu lub charakteru zdarzenia sieciowego, najczęściej proponowane są następujące opcje:

- **Przyznaj prawa dostępu**: Zezwala programowi na komputerze użytkownika na dostęp do Internetu. Odpowiednia zasada zostaje dodana do listy na stronie Uprawnienia programów.
- **Przyznaj prawa dostępu jednorazowo**: Zezwala programowi na komputerze użytkownika na tymczasowy dostęp do Internetu. Na przykład instalacja nowego programu może wymagać tylko jednorazowego dostępu.

- **Blokuj dostęp**: Zapobiega uzyskaniu przez program dostępu do Internetu.
- **Przyznaj prawa dostępu tylko dla połączeń wychodzących**: Zezwala tylko na połączenie wychodzące z Internetem. Ten alert wyświetlany jest zwykle, gdy ustawiony jest poziom zabezpieczeń Wysoki lub Ukryty.
- **Ufaj tej sieci**: Zezwala na ruch przychodzący z danej sieci i wychodzący do niej. Sieć jest dodawana do listy w sekcji Zaufane adresy IP.
- **Nie ufaj tej sieci tym razem**: Zablokowanie ruchu przychodzącego z danej sieci i wychodzącego do niej.

Żółty alert

Żółty alert to niekrytyczne powiadomienie, które informuje użytkownika o zdarzeniu sieciowym wykrytym przez zaporę. Na przykład alert **Wykryto nową sieć** jest wyświetlany, gdy zapora jest uruchamiana jest po raz pierwszy, lub gdy komputer z zainstalowaną zaporą został podłączony do nowej sieci. Można wybrać czy ufać lub nie ufać tej sieci. Jeśli sieć zostanie określona jako zaufana, zapora zezwala na ruch z dowolnego komputera w tej sieci, a jej adres jest dodawany do listy Zaufane adresy IP.

Zielony alert

W większości przypadków zielony alert zawiera podstawowe informacje o zdarzeniu i nie wymaga reakcji. Zielone alerty są wyświetlane zwykle, gdy ustawiony jest poziom zabezpieczeń Standardowy, Wysoki, Ukryty lub Blokada. Opisy zielonych alertów są następujące:

- **Program został zmodyfikowany**: Informuje o tym, że program, któremu wcześniej zezwolono na dostęp do Internetu, został zmodyfikowany. Można podjąć decyzję o zablokowaniu programu, ale jeśli użytkownik nie zareaguje, alert przestanie być wyświetlany i program nadal będzie miał dostęp do Internetu.
- **Program uzyskał dostęp do Internetu**: Powiadamia o tym, że program uzyskał dostęp do Internetu. Można podjąć decyzję o zablokowaniu programu, ale jeśli użytkownik nie zareaguje, alert przestanie być wyświetlany i program nadal będzie miał dostęp do Internetu.

Pomoc dla użytkownika

W wielu alertach zapory zawarte są dodatkowe informacje pomagające zarządzać bezpieczeństwem komputera użytkownika, w tym:

- **Więcej informacji na temat tego programu**: Przejście do witryny firmy McAfee poświęconej globalnemu bezpieczeństwu, gdzie można uzyskać informacje o programie wykrytym przez zaporę na komputerze użytkownika.

- **Poinformuj firmę McAfee o tym programie**: Przesłanie informacji do firmy McAfee o nieznanym pliku wykrytym przez zaporę na komputerze użytkownika.
- **Firma McAfee zaleca**: Porada na temat postępowania z alertami. Na przykład alert może zawierać zalecenie przyznania programowi dostępu do Internetu.

Zarządzanie alertami informacyjnymi

Podczas korzystania z zapory można wyświetlać lub ukrywać alerty informacyjne o wystąpieniu określonych zdarzeń.

Wyświetlanie alertów podczas korzystania z gier

Domyślnie alerty informacyjne zapory nie są wyświetlane podczas korzystania z gier w trybie pełnoekranowym. Można jednak tak skonfigurować zaporę, aby alerty informacyjne były wyświetlane podczas rozgrywki, gdy wykryta zostanie próba włamania lub podejrzane działanie.

Aby włączyć wyświetlanie alertów podczas korzystania z gier:

1. W okienku Typowe zadania kliknij opcję **Menu zaawansowane**.
2. Kliknij przycisk **Konfiguruj**.
3. W okienku SecurityCenter Configuration (SecurityCenter — konfiguracja) kliknij opcję **Alerty**.
4. Kliknij opcję **Zaawansowane**.
5. W okienku **Opcje alertów** wybierz opcję **Pokazuj alerty informacyjne, gdy zostanie wykryty tryb gier**.

Ukrywanie alertów informacyjnych

Alerty informacyjne powiadamiają użytkownika o zdarzeniach, które nie wymagają jego natychmiastowej uwagi.

Aby ukryć alerty informacyjne:

1. W okienku Typowe zadania kliknij opcję **Menu zaawansowane**.
2. Kliknij przycisk **Konfiguruj**.
3. W okienku SecurityCenter Configuration (SecurityCenter — konfiguracja) kliknij opcję **Alerty**.
4. Kliknij opcję **Zaawansowane**.
5. W okienku **SecurityCenter Configuration** (SecurityCenter — konfiguracja) kliknij opcję **Alerty informacyjne**.
6. W okienku **Alerty informacyjne** wykonaj jedną z następujących czynności:
   - Wybierz typ alertu, który ma być ukrywany.

- Wybierz opcję **Ukryj alerty informacyjne**, aby ukryć wszystkie alerty informacyjne.

7 Kliknij przycisk **OK**.

ROZDZIAŁ 19

Konfigurowanie ochrony przy użyciu zapory

Zapora oferuje wiele metod zarządzania bezpieczeństwem i dostosowania sposobu reakcji na zdarzenia i alerty dotyczące bezpieczeństwa.

Po zainstalowaniu zapory po raz pierwszy poziom zabezpieczeń jest ustawiony jako Standardowy. W większości przypadków to ustawienie spełnia wszystkie wymagania dotyczące bezpieczeństwa. Jednak zapora udostępnia również inne poziomy, od bardzo restrykcyjnego do bardzo tolerancyjnego.

Zapora umożliwia również odbieranie zaleceń dotyczących alertów i dostępu programów do Internetu.

W tym rozdziale

Zarządzanie poziomami zabezpieczeń zapory 130
Konfigurowanie inteligentnych zaleceń dla alertów 134
Optymalizacja zabezpieczeń programu Firewall 136
Blokowanie i odblokowywanie zapory 139

Zarządzanie poziomami zabezpieczeń zapory

Poziomy zabezpieczeń można skonfigurować w celu określenia zakresu zarządzania i reagowania na alerty w przypadku wykrycia przez zaporę niepożądanego ruchu sieciowego oraz przychodzących i wychodzących połączeń internetowych. Domyślnie włączony jest poziom zabezpieczeń Standardowy.

W przypadku ustawienia standardowego poziomu zabezpieczeń i włączenia inteligentnych zaleceń czerwone alerty są wyposażone w opcję zezwalania na dostęp lub jego blokowania nieznanym lub zmodyfikowanym programom. W przypadku wykrycia znanych programów są wyświetlane zielone alerty informacyjne i następuje automatyczne przyznanie dostępu. Przyznanie dostępu umożliwia programowi tworzenie połączeń wychodzących i nasłuchiwanie w oczekiwaniu na połączenia przychodzące.

Ogólnie rzecz biorąc, im bardziej restrykcyjny poziom zabezpieczeń (poziom Ukryty i Wysoki), tym więcej jest wyświetlanych opcji i alertów, na które musi zareagować użytkownik.

Zapora ma sześć poziomów zabezpieczeń. W kolejności od najbardziej do najmniej restrykcyjnego, poziomy są następujące:

- **Blokada**: Blokuje wszystkie połączenia internetowe.
- **Ukryty**: Blokuje wszystkie przychodzące połączenia internetowe.
- **Wysoki**: Alerty wymagają reakcji użytkownika na każde żądanie przychodzącego i wychodzącego połączenia internetowego.
- **Standardowy**: Alerty powiadamiają użytkownika, gdy nieznane lub nowe programy żądają dostępu do Internetu.
- **Zaufany**: Zezwala na wszystkie przychodzące i wychodzące połączenia internetowe oraz automatycznie dodaje je do listy w okienku Uprawnienia programów.
- **Otwarty**: Zezwala na wszystkie przychodzące i wychodzące połączenia internetowe.

Zapora umożliwia również natychmiastowe przywrócenie standardowego poziomu zabezpieczeń w okienku Przywróć ustawienia domyślne ochrony przy użyciu zapory.

Ustawianie poziomu zabezpieczeń na poziom Blokada

Ustawienie poziomu zabezpieczeń zapory na poziom Blokada powoduje zablokowanie wszystkich przychodzących i wychodzących połączeń sieciowych, w tym dostępu do witryn sieci Web, poczty e-mail oraz aktualizacji zabezpieczeń. Zastosowanie tego poziomu zabezpieczeń powoduje takie same skutki, jak wyłączenie połączenia z Internetem. Ustawienie to można wykorzystać do zablokowania portów ustawionych jako otwarte w okienku Usługi systemowe. W trybie blokady nadal mogą być wyświetlane alerty monitujące o zablokowanie programów.

Aby ustawić poziom zabezpieczeń zapory na poziom Blokada:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Poziom zabezpieczeń przesuń suwak tak, aby bieżącym poziomem był poziom **Blokada**.
3. Kliknij przycisk **OK**.

Ustawienie poziomu zabezpieczeń na Ukryty

Ustawienie poziomu zabezpieczeń zapory na Ukryty powoduje zablokowanie wszystkich przychodzących połączeń sieciowych z wyjątkiem otwartych portów. To ustawienie powoduje całkowite ukrycie obecności komputera w Internecie. W przypadku ustawienia poziomu zabezpieczeń na Ukryty zapora wyświetla alerty, gdy nowe programy próbują nawiązać połączenia wychodzące lub otrzymują żądania połączeń przychodzących. Zablokowane i dodane programy są wyświetlane w okienku Uprawnienia programów.

Aby ustawić poziom zabezpieczeń zapory na Ukryty:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Poziom zabezpieczeń przesuń suwak tak, aby bieżącym poziomem był poziom **Ukryty**.
3. Kliknij przycisk **OK**.

Ustawianie poziomu zabezpieczeń na Wysoki

W przypadku ustawienia poziomu zabezpieczeń na Wysoki zapora informuje użytkownika, gdy nowe programy próbują nawiązać połączenia wychodzące lub otrzymują żądania połączeń przychodzących. Zablokowane i dodane programy są wyświetlane w okienku Uprawnienia programów. W przypadku ustawienia poziomu zabezpieczeń na Wysoki program żąda tylko tego typu dostępu, który jest mu aktualnie potrzebny, na przykład dostępu tylko do połączeń wychodzących, który użytkownik może przyznać lub zablokować. Później, jeśli program wymaga zarówno połączeń przychodzących, jak i wychodzących, można przyznać mu pełen dostęp w okienku Uprawnienia programów.

Aby ustawić poziom zabezpieczeń zapory na Wysoki:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Poziom zabezpieczeń przesuń suwak tak, aby bieżącym poziomem był poziom **Wysoki**.
3. Kliknij przycisk **OK**.

Ustawienie poziomu zabezpieczeń na Standardowy

Poziom Standardowy jest domyślnym i zalecanym poziomem zabezpieczeń.

W przypadku ustawienia poziomu zabezpieczeń na Standardowy zapora monitoruje połączenia przychodzące i wychodzące oraz wyświetla alerty, gdy nowe programy próbują uzyskać dostęp do Internetu. Zablokowane i dodane programy są wyświetlane w okienku Uprawnienia programów.

Aby ustawić poziom zabezpieczeń zapory na Standardowy:

1. W okienku Konfiguracja Internetu i sieci kliknij opcję **Zaawansowane**.
2. W okienku Poziom zabezpieczeń przesuń suwak tak, aby bieżącym poziomem był poziom **Standardowy**.
3. Kliknij przycisk **OK**.

Ustawianie poziomu zabezpieczeń na poziom Zaufanie

Ustawienie poziomu zabezpieczeń zapory na poziom Zaufanie powoduje zezwolenie na wszystkie połączenia przychodzące i wychodzące. W przypadku poziomu Zaufanie zapora automatycznie przyznaje dostęp wszystkim programom i dodaje je do listy dozwolonych programów w okienku Uprawnienia programów.

Aby ustawić poziom zabezpieczeń zapory na poziom Zaufanie:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Poziom zabezpieczeń przesuń suwak tak, aby bieżącym poziomem był poziom **Zaufanie**.
3. Kliknij przycisk **OK**.

Konfigurowanie inteligentnych zaleceń dla alertów

Zaporę można skonfigurować tak, aby uwzględniała, wykluczała lub wyświetlała w alertach zalecenia dotyczące programów próbujących uzyskać dostęp do Internetu.

Włączenie inteligentnych zaleceń pomaga w podejmowaniu decyzji dotyczących reakcji na alerty. W przypadku włączenia inteligentnych zaleceń, przy standardowym poziomie zabezpieczeń, zapora automatycznie przepuszcza lub blokuje znane programy oraz wyświetla alerty i zalecane działania w przypadku wykrycia nieznanych i potencjalnie niebezpiecznych programów.

Jeśli inteligentne zalecenia są wyłączone, zapora nie przepuszcza automatycznie programów i nie blokuje dostępu do Internetu oraz nie sugeruje żadnych działań.

W przypadku skonfigurowania zapory tak, aby inteligentne zalecenia były jedynie wyświetlane, alert monituje o przyznanie lub zablokowanie dostępu i sugeruje działania, które należy podjąć.

Włączanie inteligentnych zaleceń

Włączenie inteligentnych zaleceń pomaga w podejmowaniu decyzji dotyczących reakcji na alerty. W przypadku włączenia inteligentnych zaleceń zapora automatycznie przepuszcza lub blokuje programy i informuje użytkownika o nierozpoznanych i potencjalnie niebezpiecznych programach.

Aby włączyć inteligentne zalecenia:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Poziom zabezpieczeń, w obszarze **Inteligentne zalecenia** wybierz opcję **Włącz inteligentne zalecenia**.
3. Kliknij przycisk **OK**.

Wyłączanie inteligentnych zaleceń

W przypadku wyłączenia inteligentnych zaleceń alerty nie zawierają wskazówek, jak reagować na alert i jak zarządzać dostępem programów do Internetu. W przypadku wyłączenia inteligentnych zaleceń zapora automatycznie przepuszcza lub blokuje programy i informuje użytkownika o nierozpoznanych i potencjalnie niebezpiecznych programach. Jeśli wykryje nowy program, który jest podejrzany lub stanowi ewentualne zagrożenie, automatycznie zablokuje dostęp programu do Internetu.

Aby wyłączyć inteligentne zalecenia:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Poziom zabezpieczeń, w obszarze **Inteligentne zalecenia** wybierz opcję **Wyłącz inteligentne zalecenia**.
3. Kliknij przycisk **OK**.

Wyświetlanie tylko inteligentnych zaleceń

Wyświetlanie inteligentnych zaleceń pomaga podjąć decyzję co do reakcji na alerty dotyczące nierozpoznanych i potencjalnie niebezpiecznych programów. W przypadku ustawienia opcji inteligentnych zaleceń **Tylko wyświetl** są wyświetlane informacje o obsłudze alertów, ale w odróżnieniu od opcji **Włącz inteligentne zalecenia** wyświetlane zalecenia nie są automatycznie stosowane i zapora nie zezwala automatycznie programom na dostęp do Internetu, ani go nie blokuje. Zamiast tego alerty zawierają zalecenia pomagające podjąć decyzję o przepuszczeniu lub zablokowaniu programu.

Aby jedynie wyświetlać inteligentne zalecenia:

1. W okienku Konfiguracja Internetu i sieci kliknij opcję **Zaawansowane**.
2. W okienku Poziom zabezpieczeń, w obszarze **Inteligentne zalecenia** wybierz opcję **Tylko wyświetl**.
3. Kliknij przycisk **OK**.

Optymalizacja zabezpieczeń programu Firewall

Istnieje wiele zagrożeń bezpieczeństwa komputera. Na przykład niektóre programy mogą próbować połączyć się z Internetem przed uruchomieniem systemu Windows®. Ponadto zaawansowani użytkownicy mogą sprawdzić, czy komputer użytkownika jest połączony z siecią, używając polecenia ping. Zapora zapewnia obronę przed obydwoma typami włamań, umożliwiając włączenie ochrony podczas rozruchu i zablokowanie żądań ICMP (ping). Pierwsze ustawienie blokuje dostęp programów do Internetu podczas uruchamiania systemu Windows, a drugie blokuje żądania ping umożliwiające innym użytkownikom wykrycie obecności danego komputera w sieci.

Do standardowych ustawień instalacji należy automatyczne wykrywanie najbardziej typowych prób włamań, np. ataków typu DoS (odmowa usługi) czy prób z użyciem programów wykorzystujących luki w zabezpieczeniach. Korzystanie ze standardowych ustawień instalacji gwarantuje ochronę przed tymi atakami i próbami skanowania komputera, jednak ochronę tę można wyłączyć w okienku Wykrywanie włamań.

Ochrona komputera podczas uruchamiania

Zapora może chronić komputer podczas uruchamiania systemu Windows. Ochrona podczas rozruchu blokuje wszystkie nowe programy, które nie miały wcześniej dostępu do Internetu, a wymagają go. Po uruchomieniu zapory wyświetla ona alerty dla programów, które zażądały dostępu do Internetu podczas uruchamiania, przy czym dostęp ten można przyznać lub zablokować. Aby użyć tej opcji, poziom zabezpieczeń musi być ustawiony na Otwarty lub Blokada.

Aby chronić komputer podczas uruchamiania:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Poziom zabezpieczeń, w obszarze Ustawienia zabezpieczeń wybierz opcję **Włącz ochronę podczas rozruchu**.
3. Kliknij przycisk **OK**.

Uwaga: Zablokowane połączenia i włamania nie są rejestrowane, gdy włączona jest ochrona podczas rozruchu.

Konfigurowanie ustawień żądania ping

Użytkownicy komputerów mogą używać narzędzia ping, które wysyła i odbiera komunikaty żądania echa ICMP, w celu określenia, czy dany komputer jest połączony z siecią. Zaporę można skonfigurować tak, aby blokowała lub umożliwiała użytkownikom innych komputerów użycie polecenia ping dla danego komputera.

Aby skonfigurować ustawienia żądań ICMP ping:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Poziom zabezpieczeń, w obszarze **Ustawienia zabezpieczeń** wykonaj jedną z następujących czynności:
   - Wybierz opcję **Zezwalaj na żądania ICMP ping**, aby umożliwić wykrywanie danego komputera z sieci za pomocą żądań ping.
   - Usuń zaznaczenie opcji **Zezwalaj na żądania ICMP ping**, aby uniemożliwić wykrycie komputera w sieci za pomocą żądań ping.
3. Kliknij przycisk **OK**.

Konfiguracja wykrywania włamań

Funkcja wykrywania włamań (IDS) monitoruje pakiety danych w poszukiwaniu podejrzanych danych lub metod przesyłania. Funkcja IDS analizuje ruch i pakiety danych w poszukiwaniu określonych wzorców ruchu sieciowego używanych przez intruzów. Na przykład, jeżeli zapora wykrywa pakiety ICMP, analizuje je w poszukiwaniu podejrzanych wzorców ruchu sieciowego, porównując ruch ICMP do wzorców znanych ataków. Zapora porównuje pakiety z bazą danych sygnatur. Jeżeli są one podejrzane lub szkodliwe, odrzuca pakiety z atakującego komputera, a potem, opcjonalnie, rejestruje zdarzenie.

Do standardowych ustawień instalacji należy automatyczne wykrywanie najbardziej typowych prób włamań, np. ataków typu DoS (odmowa usługi) czy prób z użyciem programów wykorzystujących luki w zabezpieczeniach. Korzystanie ze standardowych ustawień instalacji gwarantuje ochronę przed tymi atakami i próbami skanowania komputera, jednak ochronę tę można wyłączyć w okienku Wykrywanie włamań.

Aby skonfigurować wykrywanie włamań:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Wykrywanie włamań**.
3. W obszarze **Wykryj próby włamań** wykonaj jedną z następujących czynności:
   - Wybierz nazwę, aby automatycznie wykryć atak lub skanowanie.

- Usuń nazwę, aby wyłączyć automatyczne wykrywanie ataku lub skanowania.

4 Kliknij przycisk **OK**.

Konfiguracja ustawień stanu ochrony związanych z zaporą

Program SecurityCenter śledzi problemy, które składają się na ogólny stan ochrony komputera użytkownika. Można jednak tak skonfigurować zaporę, aby określone problemy na komputerze użytkownika, które mogą wpływać na stan ochrony, były ignorowane. Można tak skonfigurować program SecurityCenter, aby ignorowane były sytuacje, gdy: poziom zabezpieczeń zapory jest ustawiony na Otwarty, usługa zapory nie jest uruchomiona oraz zapora tylko dla ruchu wychodzącego nie jest zainstalowana na komputerze.

Aby skonfigurować ustawienia stanu ochrony związane z zaporą:

1 W okienku Typowe zadania kliknij opcję **Menu zaawansowane**.

2 Kliknij przycisk **Konfiguruj**.

3 W okienku SecurityCenter Configuration (SecurityCenter — konfiguracja) kliknij opcję **Alerty**.

4 Kliknij opcję **Zaawansowane**.

5 W okienku Typowe zadania kliknij opcję **Menu zaawansowane**.

6 Kliknij przycisk **Konfiguruj**.

7 W okienku SecurityCenter Configuration (SecurityCenter — konfiguracja) kliknij opcję **Stan ochrony**.

8 Kliknij opcję Zaawansowane.

9 W okienku Zignorowane problemy wybierz jedną lub więcej z następujących opcji:

- **W zaporze ustawiono poziom zabezpieczeń Otwarty.**
- **Usługa zapory nie została uruchomiona.**
- **Ochrona ruchu wychodzącego za pomocą zapory nie jest zainstalowana na komputerze.**

10 Kliknij przycisk **OK**.

Blokowanie i odblokowywanie zapory

Blokowanie jest przydatne w sytuacjach awaryjnych, w przypadku konieczności odizolowania komputera w celu rozwiązania problemu lub w razie wątpliwości dotyczących zarządzania dostępem programu do Internetu.

Natychmiastowe zablokowanie zapory

Zablokowanie zapory natychmiast blokuje cały przychodzący i wychodzący ruch sieciowy między komputerem użytkownika a Internetem. Uniemożliwia wszystkim połączeniom zdalnym dostęp do komputera i blokuje wszystkim programom na komputerze dostęp do Internetu.

Aby natychmiast zablokować zaporę i zatrzymać cały ruch sieciowy:

1. W okienku Główne lub Typowe zadania przy włączonym **Menu podstawowym** lub **zaawansowanym** kliknij opcję **Blokada zapory**.
2. W okienku Blokada zapory kliknij opcję **Blokada**.
3. W oknie dialogowym kliknij przycisk **Tak**, aby potwierdzić natychmiastowe zablokowanie całego ruchu przychodzącego i wychodzącego.

Natychmiastowe odblokowanie zapory

Zablokowanie zapory natychmiast blokuje cały przychodzący i wychodzący ruch sieciowy między komputerem użytkownika a Internetem. Uniemożliwia wszystkim połączeniom zdalnym dostęp do komputera i blokuje wszystkim programom na komputerze dostęp do Internetu. Po zablokowaniu zapory można ją odblokować, aby zezwolić na ruch sieciowy.

Aby natychmiast odblokować zaporę i zezwolić na ruch sieciowy:

1. W okienku Główne lub Typowe zadania przy włączonym **Menu podstawowym** lub **zaawansowanym** kliknij opcję **Blokada zapory**.
2. W okienku Blokada włączona kliknij opcję **Odblokuj**.
3. W okienku dialogowym kliknij przycisk **Tak**, aby potwierdzić odblokowanie zapory i zezwolenie na ruch sieciowy.

Przywracanie ustawień zapory

Można szybko przywrócić pierwotne ustawienia ochrony przy pomocy zapory. Spowoduje to ustawienie poziomu zabezpieczeń na standardowy, włączenie inteligentnych zaleceń, wyczyszczenie listy zaufanych i zabronionych adresów IP oraz usunięcie wszystkich programów z okienka Uprawnienia programów.

Aby przywrócić pierwotne ustawienia ochrony przy pomocy zapory:

1. W okienku Główne lub Typowe zadania przy włączonym **Menu podstawowym** lub **zaawansowanym** kliknij opcję **Przywróć ustawienia domyślne zapory**.
2. W okienku Przywróć ustawienia domyślne ochrony przy użyciu zapory kliknij opcję **Przywróć ustawienia domyślne**.
3. W oknie dialogowym Przywróć ustawienia domyślne ochrony przy użyciu zapory kliknij przycisk **Tak**, aby potwierdzić przywrócenie domyślnych ustawień konfiguracji zapory.

Ustawienie poziomu zabezpieczeń na poziom Otwarty

Ustawienie poziomu zabezpieczeń zapory na Otwarty umożliwia zaporze przyznanie dostępu wszystkim przychodzącym i wychodzącym połączeniom sieciowym. Aby przyznać dostęp wcześniej zablokowanym programom, należy użyć okienka Uprawnienia programów.

Aby ustawić poziom zabezpieczeń zapory na poziom Otwarty:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Poziom zabezpieczeń przesuń suwak tak, aby bieżącym poziomem był poziom **Otwarty**.
3. Kliknij przycisk **OK**.

Uwaga: Po ustawieniu poziomu zabezpieczeń zapory na **Otwarty** wcześniej zablokowane programy nadal będą blokowane. Aby temu zapobiec, można zmienić regułę programu na **Pełny dostęp**.

ROZDZIAŁ 20

Zarządzanie programami i uprawnieniami

Zapora umożliwia zarządzanie i tworzenie uprawnień dostępu dla istniejących i nowych programów wymagających dostępu do Internetu dla ruchu przychodzącego i wychodzącego. Zapora umożliwia przyznanie programom pełnego dostępu lub dostępu tylko dla połączeń wychodzących. Można również zablokować dostęp programów do Internetu.

W tym rozdziale

Przyznawanie programom dostępu do Internetu 142
Przyznawanie programom praw dostępu tylko dla połączeń wychodzących 145
Blokowanie dostępu programów do Internetu 147
Usuwanie praw dostępu programów 149
Informacje o programach 150

Przyznawanie programom dostępu do Internetu

Niektóre programy, na przykład przeglądarki internetowe, do prawidłowego funkcjonowania wymagają dostępu do Internetu.

Zapora umożliwia użycie strony Uprawnienia programów w celu:

- Przyznania programom dostępu
- Przyznania programom dostępu tylko dla połączeń wychodzących
- Zablokowania programom dostępu

Pełny dostęp i dostęp tylko dla połączeń wychodzących można przyznać z poziomu dziennika Zdarzenia wychodzące i dziennika Ostatnie zdarzenia.

Przyznawanie programowi pełnego dostępu

Wiele programów na komputerze wymaga dostępu do Internetu dla połączeń przychodzących i wychodzących. Program Personal Firewall zawiera listę programów, którym są automatycznie przyznawane prawa pełnego dostępu, ale uprawnienia te można zmienić.

Aby przyznać programowi dostęp do Internetu tylko dla połączeń wychodzących:

1. W okienku Konfiguracja Internetu i sieci kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Uprawnienia programów**.
3. W obszarze **Uprawnienia programów** wybierz program z opcją **Zablokowane** lub **Prawa dostępu tylko dla wychodzących**.
4. W obszarze **Akcja** kliknij przycisk **Przyznaj prawa pełnego dostępu**.
5. Kliknij przycisk **OK**.

Przyznawanie nowemu programowi pełnego dostępu

Wiele programów na komputerze wymaga dostępu do Internetu dla połączeń przychodzących i wychodzących. Zapora zawiera listę programów, którym są automatycznie przyznawane prawa pełnego dostępu, ale uprawnienia te można zmienić.

Aby przyznać nowemu programowi pełny dostęp do Internetu:

1. W okienku Konfiguracja Internetu i sieci kliknij opcję **Zaawansowane**.
2. W okienku **Zapora** kliknij opcję **Uprawnienia programów**.
3. W obszarze **Uprawnienia programów** kliknij opcję **Dodaj dozwolony program**.
4. W oknie dialogowym **Dodawanie programu** znajdź i wybierz program, który chcesz dodać.
5. Kliknij przycisk **Otwórz**.
6. Kliknij przycisk **OK**.

   Nowo dodany program zostanie wyświetlony w obszarze **Uprawnienia programów**.

Uwaga: Uprawnienia nowo dodanego programu można zmienić tak, jak w przypadku istniejącego programu, wybierając program, a następnie w obszarze **Akcja** klikając opcję **Przyznaj prawa dostępu tylko dla wychodzących** lub **Blokuj dostęp**.

Przyznawanie pełnego dostępu z poziomu dziennika Ostatnie zdarzenia

Wiele programów na komputerze wymaga dostępu do Internetu dla połączeń przychodzących i wychodzących. Można wybrać program z dziennika Ostatnie zdarzenia i przyznać mu pełny dostęp do Internetu.

Aby przyznać programowi pełny dostęp z poziomu dziennika Ostatnie zdarzenia:

1. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W okienku Ostatnie zdarzenia wybierz opis zdarzenia, a następnie kliknij opcję **Przyznaj prawa pełnego dostępu**.
3. W oknie dialogowym Uprawnienia programów kliknij przycisk **Tak**, aby potwierdzić przyznanie programowi pełnego dostępu.

Tematy pokrewne

- Wyświetlanie zdarzeń wychodzących (strona 172)

Przyznawanie pełnego dostępu z poziomu dziennika Zdarzenia wychodzące

Wiele programów na komputerze wymaga dostępu do Internetu dla połączeń przychodzących i wychodzących. Można wybrać program z dziennika Zdarzenia wychodzące i przyznać mu pełny dostęp do Internetu.

Aby przyznać programowi pełny dostęp do Internetu z poziomu dziennika Zdarzenia wychodzące:

1. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
3. Wybierz opcję **Internet i sieć**, a następnie opcję **Zdarzenia wychodzące**.
4. W okienku Zdarzenia wychodzące wybierz źródłowy adres IP, a następnie kliknij opcję **Przyznaj prawa dostępu**.
5. W oknie dialogowym Uprawnienia programów kliknij przycisk **Tak**, aby potwierdzić chęć przyznania pełnego dostępu do Internetu.

Tematy pokrewne

- Wyświetlanie zdarzeń wychodzących (strona 172)

Przyznawanie programom praw dostępu tylko dla połączeń wychodzących

Niektóre programy na komputerze wymagają dostępu do Internetu tylko dla połączeń wychodzących. Korzystając z zapory, można przyznawać programom dostęp do Internetu tylko dla połączeń wychodzących.

Przyznawanie programowi dostępu tylko dla połączeń wychodzących

Wiele programów na komputerze wymaga dostępu do Internetu dla połączeń przychodzących i wychodzących. Program Personal Firewall zawiera listę programów, którym są automatycznie przyznawane prawa pełnego dostępu, ale uprawnienia te można zmienić.

Aby przyznać programowi dostęp tylko dla połączeń wychodzących:

1. W okienku Konfiguracja Internetu i sieci kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Uprawnienia programów**.
3. W obszarze **Uprawnienia programów** wybierz program z opcją **Zablokowane** lub **Pełny dostęp**.
4. W obszarze **Akcja** kliknij przycisk **Przyznaj prawa dostępu tylko dla wychodzących**.
5. Kliknij przycisk **OK**.

Przyznawanie dostępu tylko dla połączeń wychodzących z dziennika Ostatnie zdarzenia

Wiele programów na komputerze wymaga dostępu do Internetu dla połączeń przychodzących i wychodzących. Można wybrać program z dziennika Ostatnie zdarzenia i przyznać mu dostęp do Internetu tylko dla połączeń wychodzących.

Aby przyznać programowi dostęp tylko dla połączeń wychodzących z poziomu dziennika Ostatnie zdarzenia:

1. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W okienku Ostatnie zdarzenia wybierz opis zdarzenia, a następnie kliknij opcję **Przyznaj prawa dostępu tylko dla wychodzących**.
3. W oknie dialogowym Uprawnienia programów kliknij przycisk **Tak**, aby potwierdzić przyznanie programowi dostępu tylko dla połączeń wychodzących.

Tematy pokrewne

- Wyświetlanie zdarzeń wychodzących (strona 172)

Przyznawanie dostępu tylko dla połączeń wychodzących z poziomu dziennika Zdarzenia wychodzące

Wiele programów na komputerze wymaga dostępu do Internetu dla połączeń przychodzących i wychodzących. Można wybrać program z dziennika Zdarzenia wychodzące i przyznać mu dostęp do Internetu tylko dla połączeń wychodzących.

Aby z poziomu dziennika Zdarzenia wychodzące przyznać programowi dostęp tylko dla połączeń wychodzących:

1. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
3. Wybierz opcję **Internet i sieć**, a następnie opcję **Zdarzenia wychodzące**.
4. W okienku Zdarzenia wychodzące wybierz źródłowy adres IP, a następnie kliknij opcję **Przyznaj prawa dostępu tylko dla połączeń wychodzących**.
5. W oknie dialogowym Uprawnienia programów kliknij przycisk **Tak**, aby potwierdzić przyznanie programowi dostępu tylko dla połączeń wychodzących.

Tematy pokrewne

- Wyświetlanie zdarzeń wychodzących (strona 172)

Blokowanie dostępu programów do Internetu

Zapora umożliwia blokowanie dostępu programów do Internetu. Należy się upewnić, że zablokowanie programu nie przerwie połączenia z siecią lub działania innego programu, który do prawidłowego funkcjonowania wymaga dostępu do Internetu.

Blokowanie dostępu programu

Wiele programów na komputerze wymaga dostępu do Internetu dla połączeń przychodzących i wychodzących. Program Personal Firewall zawiera listę programów, którym są automatycznie przyznawane prawa pełnego dostępu, ale uprawnienia te można zablokować.

Aby zablokować dostęp programu do Internetu:

1. W okienku Konfiguracja Internetu i sieci kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Uprawnienia programów**.
3. W obszarze **Uprawnienia programów** wybierz program z opcją **Prawa pełnego dostępu** lub **Prawa dostępu tylko dla wychodzących**.
4. W obszarze **Akcja** kliknij opcję **Zablokuj dostęp**.
5. Kliknij przycisk **OK**.

Blokowanie dostępu nowego programu

Wiele programów na komputerze wymaga dostępu do Internetu dla połączeń przychodzących i wychodzących. Program Personal Firewall zawiera listę programów, którym są automatycznie przyznawane prawa pełnego dostępu. Można też dodać nowy program, a następnie zablokować jego dostęp do Internetu.

Aby zablokować dostęp nowego programu do Internetu:

1. W okienku Konfiguracja Internetu i sieci kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Uprawnienia programów**.
3. Na karcie **Uprawnienia programów** kliknij opcję **Dodaj zablokowany program**.
4. W oknie dialogowym **Dodawanie programu** znajdź i wybierz program, który chcesz dodać.
5. Kliknij przycisk **Otwórz**.
6. Kliknij przycisk **OK**.

   Nowo dodany program zostanie wyświetlony w obszarze **Uprawnienia programów**.

Uwaga: Uprawnienia nowo dodanego programu można zmienić tak, jak uprawnienia istniejącego programu, wybierając program, a następnie klikając opcję **Przyznaj prawa dostępu tylko dla wychodzących** lub **Przyznaj prawa pełnego dostępu** w obszarze **Akcja**.

Blokowanie dostępu z poziomu dziennika Ostatnie zdarzenia

Wiele programów na komputerze wymaga dostępu do Internetu dla połączeń przychodzących i wychodzących. Można jednak zablokować dostęp programów do Internetu z poziomu dziennika Ostatnie zdarzenia.

Aby zablokować dostęp programu z poziomu dziennika Ostatnie zdarzenia:

1. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W okienku Ostatnie zdarzenia wybierz opis zdarzenia, a następnie kliknij opcję **Blokuj dostęp**.
3. W oknie dialogowym Uprawnienia programów kliknij przycisk **Tak**, aby potwierdzić zablokowanie dostępu programu.

Tematy pokrewne

- Wyświetlanie zdarzeń wychodzących (strona 172)

Usuwanie praw dostępu programów

Przed usunięciem uprawnienia programu należy się upewnić, że jego brak nie wpłynie negatywnie na pracę komputera lub na połączenie sieciowe.

Usuwanie uprawnienia programu

Wiele programów na komputerze wymaga dostępu do Internetu dla połączeń przychodzących i wychodzących. Program Personal Firewall zawiera listę programów, którym są automatycznie przyznawane prawa pełnego dostępu, ale można usunąć z niej programy, które zostały dodane automatycznie lub ręcznie.

Aby usunąć uprawnienie nowego programu:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Uprawnienia programów**.
3. W obszarze **Uprawnienia programów** wybierz program.
4. W obszarze **Akcja** kliknij opcję **Usuń uprawnienie programu**.
5. Kliknij przycisk **OK**.

   Program zostanie usunięty z listy w okienku Uprawnienia programów.

Uwaga: Zapora zapobiega modyfikowaniu ustawień niektórych programów poprzez ograniczenie lub wyłączenie dostępnych działań.

Informacje o programach

Jeśli nie ma pewności, jakie uprawnienie powinien mieć program, informacje ułatwiające decyzję można znaleźć w witrynie internetowej HackerWatch firmy McAfee.

Informacje o programie

Wiele programów na komputerze wymaga dostępu do Internetu dla połączeń przychodzących i wychodzących. Program Personal Firewall zawiera listę programów, którym są automatycznie przyznawane prawa pełnego dostępu, ale uprawnienia te można zmienić.

Zapora ułatwia decyzję o przyznaniu lub zablokowaniu dostępu programu do Internetu. Należy upewnić się, że połączenie z Internetem zostało nawiązane i za pomocą przeglądarki można otworzyć witrynę HackerWatch firmy McAfee. Zawiera ona bieżące informacje o programach, ich wymaganiach dotyczących dostępu do Internetu i zagrożeniach bezpieczeństwa.

Aby uzyskać informacje o programie:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Uprawnienia programów**.
3. W obszarze **Uprawnienia programów** wybierz program.
4. W obszarze **Akcja** kliknij opcję **Więcej informacji**.

Informacje o programie znajdujące się w dzienniku Zdarzenia wychodzące

Program Personal Firewall pozwala uzyskać informacje o programach, które są wyświetlane w dzienniku Zdarzenia wychodzące.

Przed uzyskiwaniem informacji o programie należy upewnić się, że komputer jest połączony z Internetem i ma zainstalowaną przeglądarkę internetową.

Aby uzyskać informacje o programie z poziomu dziennika Zdarzenia wychodzące:

1. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
3. Wybierz opcję **Internet i sieć**, a następnie opcję **Zdarzenia wychodzące**.
4. W okienku Zdarzenia wychodzące wybierz źródłowy adres IP, a następnie kliknij opcję **Dowiedz się więcej**.

   Informacje o programie można obejrzeć w witrynie HackerWatch. W witrynie HackerWatch można znaleźć aktualne informacje o

programach, wymaganiach dotyczących dostępu do Internetu i zagrożeniach bezpieczeństwa.

Tematy pokrewne

- Wyświetlanie zdarzeń wychodzących (strona 172)

ROZDZIAŁ 21

Zarządzanie usługami systemowymi

Niektóre programy (w tym serwery sieci Web i programy serwerów do udostępniania plików) do swojego prawidłowego działania wymagają odbierania połączeń z innych komputerów za pośrednictwem określonych portów usług systemowych. Zazwyczaj zapora zamyka te porty usług systemowych, ponieważ to głównie one są źródłem zagrożeń w systemie użytkownika. Aby akceptować połączenia ze zdalnych komputerów, porty usług systemowych muszą być jednak otwarte.

Na liście poniżej wymieniono standardowe porty typowych usług.

- Protokół FTP — porty 20-21
- Serwer poczty (IMAP) — port 143
- Serwer poczty (POP3) — port 110
- Serwer poczty (SMTP) — port 25
- Serwer Microsoft Directory Server (MSFT DS) — port 445
- Serwer Microsoft SQL Server (MSFT SQL) — port 1433
- Serwer pomocy zdalnej/terminali (RDP) — port 3389
- Zdalne wywołania procedur (RPC) — port 135
- Bezpieczny serwer sieci Web (HTTPS) — port 443
- Usługa Universal Plug and Play (UPNP) — port 5000
- Serwer sieci Web (HTTP) — port 80
- Udostępnianie plików systemu Windows (NETBIOS) — porty 137–139

W tym rozdziale

Konfigurowanie portów usług systemowych..... 154

Konfigurowanie portów usług systemowych

Aby zezwolić na zdalny dostęp komputerów do usługi, należy wskazać określoną usługę i powiązany z nią port, który ma być otwarty. Usługę lub port powinno się zaznaczyć tylko wtedy, gdy ma się pewność, że muszą być otwarte. Otwarcie portu jest konieczne rzadko.

Zezwolenie na dostęp do istniejącego portu usług systemowych

W okienku Usługi systemowe można otworzyć lub zamknąć istniejący port, zezwalając na zdalny dostęp komputera do usługi sieciowej lub blokując go. Otwarcie portu usług systemowych może spowodować, że komputer będzie podatny na zagrożenia z Internetu. Dlatego port należy otwierać tylko wtedy, gdy jest to konieczne.

Aby zezwolić na dostęp do portu usług systemowych:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Usługi systemowe**.
3. W obszarze **Otwórz port usług systemowych** wybierz usługę systemową, której port chcesz otworzyć.
4. Kliknij przycisk **OK**.

Blokowanie dostępu do istniejącego portu usługi systemowej

W okienku Usługi systemowe można otworzyć lub zamknąć istniejący port, zezwalając na zdalny dostęp komputera do usługi sieciowej lub blokując go. Otwarcie portu usług systemowych może spowodować, że komputer będzie podatny na zagrożenia z Internetu. Dlatego port należy otwierać tylko wtedy, gdy jest to konieczne.

Aby zablokować dostęp do portu usługi systemowej:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Usługi systemowe**.
3. Na liście **Otwarty port usługi systemowej** usuń zaznaczenie przy wybranej usłudze systemowej, aby zamknąć jej port.
4. Kliknij przycisk **OK**.

Konfiguracja nowego portu usług systemowych

W okienka Usługi systemowe można dodać nowy port usług systemowych, a następnie otworzyć lub zamknąć, zezwalając na zdalny dostęp komputera do usługi sieciowej lub blokując go. Otwarcie portu usług systemowych może spowodować, że komputer będzie podatny na zagrożenia z Internetu. Dlatego port należy otwierać tylko wtedy, gdy jest to konieczne.

Aby utworzyć i skonfigurować nowy port usług systemowych:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Usługi systemowe**.
3. Kliknij przycisk **Dodaj**.
4. W obszarze **Dodaj konfigurację portu** wprowadź następujące dane:
   - nazwa programu,
   - porty TCP/IP połączeń przychodzących,
   - porty TCP/IP połączeń wychodzących,
   - porty UDP połączeń przychodzących,
   - porty UDP połączeń wychodzących.
5. Można też wprowadzić opis nowej konfiguracji.
6. Kliknij przycisk **OK**.

   Skonfigurowany port usług systemowych zostanie wyświetlony w obszarze **Otwórz port usług systemowych**.

Modyfikacja portu usług systemowych

Otwarcie lub zamknięcie portu umożliwia lub blokuje dostęp do usługi sieciowej na komputerze. W okienku Usługi systemowe można modyfikować informacje dotyczące połączeń przychodzących i wychodzących dla istniejącego portu. Jeśli informacje dotyczące portu są wprowadzone niepoprawnie, usługa systemowa nie działa.

Aby zmodyfikować port usług systemowych:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Usługi systemowe**.
3. Wybierz usługę systemową i kliknij przycisk **Edytuj**.
4. W obszarze **Dodaj konfigurację portu** wprowadź następujące dane:
   - nazwa programu,
   - porty TCP/IP połączeń przychodzących,
   - porty TCP/IP połączeń wychodzących,

- porty UDP połączeń przychodzących,
- porty UDP połączeń wychodzących.

5 Można też wprowadzić opis zmienionej konfiguracji.

6 Kliknij przycisk **OK**.

Zmodyfikowany skonfigurowany port usług systemowych zostanie wyświetlony w obszarze **Otwórz port usług systemowych**.

Usuwanie portu usług systemowych

Otwarcie lub zamknięcie portu umożliwia lub blokuje dostęp do usługi sieciowej na komputerze. W okienku Usługi systemowe można usunąć istniejący port i przypisaną do niego usługę systemową. Po usunięciu portu i usługi systemowej z okienka Usługi systemowe, zdalne komputery nie mają już dostępu do usługi sieciowej na komputerze użytkownika.

Aby usunąć port usług systemowych:

1 W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.

2 W okienku Zapora kliknij opcję **Usługi systemowe**.

3 Wybierz usługę systemową, a następnie kliknij przycisk **Usuń**.

4 W oknie dialogowym **Usługi systemowe** kliknij przycisk **Tak**, aby potwierdzić usunięcie usługi systemowej.

Usunięty port usług systemowych nie będzie już wyświetlany w okienku Usługi systemowe.

ROZDZIAŁ 22

Zarządzanie połączeniami z komputerem

Zaporę można skonfigurować tak, aby można było zarządzać określonymi zdalnymi połączeniami z komputerem użytkownika. W takim przypadku należy stworzyć reguły oparte na adresach protokołu internetowego (IP) przypisanych do zdalnych komputerów. Komputerom przypisanym do zaufanych adresów IP można ufać i mogą one łączyć się z komputerem użytkownika. Komputerom o nieznanych, podejrzanych lub wzbudzających nieufność adresach można blokować możliwość łączenia się z komputerem użytkownika.

Przy zezwalaniu na połączenie należy się upewnić, że zaufany komputer jest bezpieczny. Jeśli zaufany komputer jest zainfekowany robakiem lub innym mechanizmem, komputer użytkownika może również być zagrożony. Ponadto firma McAfee zaleca, aby zaufane komputery były również chronione za pomocą zapory i aktualnego programu antywirusowego. Zapora nie rejestruje ruchu ani nie generuje alertów o zdarzeniach z adresów IP znajdujących się na liście zaufanych adresów IP.

Komputerom, którym są przypisane nieznane, podejrzane lub wzbudzające nieufność adresy IP, można zabronić łączenia się z komputerem użytkownika.

Ponieważ program Firewall blokuje cały niepożądany ruch, zwykle nie jest konieczne blokowanie adresu IP. Blokowanie adresu IP ma sens tylko w przypadku, gdy użytkownik jest pewien, że połączenie internetowe stanowi określone zagrożenie. Należy upewnić się, że nie są blokowane ważne adresy IP, takie jak adresy serwerów DNS czy DHCP lub innych serwerów usługodawcy internetowego. Zależnie od ustawień zabezpieczeń program Firewall może generować alert o wykryciu zdarzenia wywołanego przez zablokowany komputer.

W tym rozdziale

Udzielanie zaufania połączeniom z komputerami 158
Blokowanie połączeń z komputerami 163

Udzielanie zaufania połączeniom z komputerami

Zaufane adresy IP można dodawać, edytować i usuwać w okienku Zaufane i zabronione adresy IP w obszarze **Zaufane adresy IP**.

Lista **Zaufane adresy IP** w okienku Zaufane i zabronione adresy IP pozwala na odbieranie całego ruchu z określonego komputera przez komputer użytkownika. Program Firewall nie rejestruje ruchu ani nie generuje alertów o zdarzeniach z adresów IP znajdujących się na liście **Zaufane adresy IP**.

Zapora udziela zaufania wszystkim sprawdzonym adresom IP na liście i zawsze zezwala na ruch sieciowy z zaufanego adresu IP na każdym porcie. Zapora nie rejestruje żadnych zdarzeń z zaufanych adresów IP. Działania, w których uczestniczy komputer przypisany do zaufanego adresu IP i komputer użytkownika nie są filtrowane ani analizowane przez zaporę.

Przy zezwalaniu na połączenie należy się upewnić, że zaufany komputer jest bezpieczny. Jeśli zaufany komputer jest zainfekowany robakiem lub innym mechanizmem, komputer użytkownika może również być zagrożony. Ponadto firma McAfee zaleca, aby zaufane komputery były również chronione za pomocą zapory i aktualnego programu antywirusowego.

Dodawanie połączenia z zaufanym komputerem

W zaporze można dodać połączenie z zaufanym komputerem i przypisany do niego adres IP.

Lista **Zaufane adresy IP** w okienku Zaufane i zabronione adresy IP pozwala na odbieranie całego ruchu z określonego komputera przez komputer użytkownika. Program Firewall nie rejestruje ruchu ani nie generuje alertów o zdarzeniach z adresów IP znajdujących się na liście **Zaufane adresy IP**.

Komputery z przypisanym zaufanym adresem IP mogą się zawsze łączyć z tym komputerem. Przed dodaniem, edycją lub usunięciem zaufanego adresu IP należy upewnić się, że usuwanie go i komunikacja z komputerem o tym adresie są bezpieczne.

Aby dodać połączenie z zaufanym komputerem:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Zaufane i zabronione adresy IP**.
3. W okienku Zaufane i zabronione adresy IP wybierz opcję **Zaufane adresy IP**.
4. Kliknij przycisk **Dodaj**.
5. W obszarze **Dodaj regułę zaufanego adresu IP** wykonaj jedną z następujących czynności:
   - Wybierz opcję **Pojedynczy adres IP**, a następnie wprowadź adres IP.
   - Wybierz opcję **Zakres adresów IP**, a następnie wprowadź początkowe i końcowe adresy IP w polach **From IP Address** (Z adresu IP) i **To IP Address** (Na adres IP).
6. Można też wybrać opcję **Reguła wygasa za** i wprowadzić liczbę dni, w czasie których reguła będzie obowiązywać.
7. Dodatkowo można wprowadzić opis reguły.
8. Kliknij przycisk **OK**.
9. W oknie dialogowym Dodaj regułę zaufanego adresu IP kliknij przycisk **Tak**, aby potwierdzić dodanie połączenia z zaufanym komputerem.

   Nowo dodany adres IP zostanie wyświetlony na liście **Zaufane adresy IP**.

Dodawanie zaufanego komputera z poziomu dziennika Zdarzenia przychodzące

Połączenie z zaufanym komputerem i związany z nim adres IP można dodać z poziomu dziennika Zdarzenia przychodzące.

Komputery z przypisanym zaufanym adresem IP mogą się zawsze łączyć z tym komputerem. Przed dodaniem, edycją lub usunięciem zaufanego adresu IP należy upewnić się, że usuwanie go i komunikacja z komputerem o tym adresie są bezpieczne.

Aby dodać połączenie z zaufanym komputerem z poziomu dziennika Zdarzenia przychodzące:

1. Upewnij się, że włączone jest Menu zaawansowane. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
3. Kliknij opcję **Internet i sieć**, a następnie opcję **Zdarzenia przychodzące**.
4. W okienku Zdarzenia przychodzące wybierz źródłowy adres IP i kliknij opcję **Zaufaj temu adresowi**.
5. W oknie dialogowym Dodaj regułę zaufanego adresu IP kliknij przycisk **Tak**, aby potwierdzić zaufanie do tego adresu IP.

   Nowo dodany adres IP zostanie wyświetlony na liście **Zaufane adresy IP**.

Tematy pokrewne

- Rejestrowanie zdarzeń (strona 170)

Edycja połączenia z zaufanym komputerem

W zaporze można edytować połączenie z zaufanym komputerem i przypisany do niego adres IP.

Komputery z przypisanym zaufanym adresem IP mogą się zawsze łączyć z tym komputerem. Przed dodaniem, edycją lub usunięciem zaufanego adresu IP należy upewnić się, że usuwanie go i komunikacja z komputerem o tym adresie są bezpieczne.

Aby edytować połączenie z zaufanym komputerem:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Zaufane i zabronione adresy IP**.
3. W okienku Zaufane i zabronione adresy IP wybierz opcję **Zaufane adresy IP**.
4. Wybierz adres IP, a następnie kliknij przycisk **Edytuj**.
5. W obszarze **Dodaj regułę zaufanego adresu IP** wykonaj jedną z następujących czynności:
   - Wybierz opcję **Pojedynczy adres IP**, a następnie wprowadź adres IP.
   - Wybierz opcję **Zakres adresów IP**, a następnie wprowadź początkowe i końcowe adresy IP w polach **From IP Address** (Z adresu IP) i **To IP Address** (Na adres IP).
6. Można też zaznaczyć opcję **Reguła wygasa za** i wpisać liczbę dni, w czasie których reguła będzie obowiązywać.
7. Dodatkowo można wprowadzić opis reguły.
8. Kliknij przycisk **OK**.

   Zmodyfikowany adres IP zostanie wyświetlony w obszarze **Zaufane adresy IP**.

Usuwanie połączenia z zaufanym komputerem

W zaporze można usunąć połączenie z zaufanym komputerem i przypisany do niego adres IP.

Komputery z przypisanym zaufanym adresem IP mogą się zawsze łączyć z tym komputerem. Przed dodaniem, edycją lub usunięciem zaufanego adresu IP należy upewnić się, że usuwanie go i komunikacja z komputerem o tym adresie są bezpieczne.

Aby usunąć połączenie z zaufanym komputerem:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Zaufane i zabronione adresy IP**.
3. W okienku Zaufane i zabronione adresy IP wybierz opcję **Zaufane adresy IP**.
4. Zaznacz adres IP, a następnie kliknij przycisk **Usuń**.
5. W oknie dialogowym **Zaufane i zabronione adresy IP** kliknij przycisk **Tak**, aby potwierdzić usunięcie zaufanego adresu IP w obszarze **Zaufane adresy IP**.

Blokowanie połączeń z komputerami

Zaufane adresy IP można dodawać, edytować i usuwać w okienku Zaufane i zabronione adresy IP w obszarze **Zabronione adresy IP**.

Komputerom, którym są przypisane nieznane, podejrzane lub wzbudzające nieufność adresy IP, można zabronić łączenia się z komputerem użytkownika.

Ponieważ program Firewall blokuje cały niepożądany ruch, zwykle nie jest konieczne blokowanie adresu IP. Blokowanie adresu IP ma sens tylko w przypadku, gdy użytkownik jest pewien, że połączenie internetowe stanowi określone zagrożenie. Należy upewnić się, że nie są blokowane ważne adresy IP, takie jak adresy serwerów DNS czy DHCP lub innych serwerów usługodawcy internetowego. Zależnie od ustawień zabezpieczeń program Firewall może generować alert o wykryciu zdarzenia wywołanego przez zablokowany komputer.

Dodawanie połączenia z zabronionym komputerem

W zaporze można dodać połączenie z zabronionym komputerem i przypisany do niego adres IP.

Komputerom, którym są przypisane nieznane, podejrzane lub wzbudzające nieufność adresy IP, można zabronić łączenia się z komputerem użytkownika.

Ponieważ program Firewall blokuje cały niepożądany ruch, zwykle nie jest konieczne blokowanie adresu IP. Blokowanie adresu IP ma sens tylko w przypadku, gdy użytkownik jest pewien, że połączenie internetowe stanowi określone zagrożenie. Należy upewnić się, że nie są blokowane ważne adresy IP, takie jak adresy serwerów DNS czy DHCP lub innych serwerów usługodawcy internetowego. Zależnie od ustawień zabezpieczeń program Firewall może generować alert o wykryciu zdarzenia wywołanego przez zablokowany komputer.

Aby dodać połączenie z zabronionym komputerem:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Zaufane i zabronione adresy IP**.
3. W okienku Zaufane i zabronione adresy IP wybierz opcję **Zabronione adresy IP**.
4. Kliknij przycisk **Dodaj**.
5. W obszarze Dodaj regułę zabronionego adresu IP wykonaj jedną z następujących czynności:
   - Wybierz opcję **Pojedynczy adres IP**, a następnie wprowadź adres IP.
   - Wybierz opcję **Zakres adresów IP**, a następnie wprowadź początkowe i końcowe adresy IP w polach **From IP Address** (Z adresu IP) i **To IP Address** (Na adres IP).
6. Można też zaznaczyć opcję **Reguła wygasa za** i wpisać liczbę dni, w czasie których reguła będzie obowiązywać.
7. Dodatkowo można wprowadzić opis reguły.
8. Kliknij przycisk **OK**.
9. W oknie dialogowym **Dodaj regułę zabronionego adresu IP** kliknij przycisk **Tak**, aby potwierdzić dodanie połączenia z zabronionym komputerem.

   Nowo dodany adres IP zostanie wyświetlony na liście **Zabronione adresy IP**.

Edycja połączenia z zabronionym komputerem

W zaporze można edytować połączenie z zabronionym komputerem i przypisany do niego adres IP.

Komputerom, którym są przypisane nieznane, podejrzane lub wzbudzające nieufność adresy IP, można zabronić łączenia się z komputerem użytkownika.

Ponieważ program Firewall blokuje cały niepożądany ruch, zwykle nie jest konieczne blokowanie adresu IP. Blokowanie adresu IP ma sens tylko w przypadku, gdy użytkownik jest pewien, że połączenie internetowe stanowi określone zagrożenie. Należy upewnić się, że nie są blokowane ważne adresy IP, takie jak adresy serwerów DNS czy DHCP lub innych serwerów usługodawcy internetowego. Zależnie od ustawień zabezpieczeń program Firewall może generować alert o wykryciu zdarzenia wywołanego przez zablokowany komputer.

Aby edytować połączenie z zabronionym komputerem:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Zaufane i zabronione adresy IP**.
3. W okienku Zaufane i zabronione adresy IP wybierz opcję **Zabronione adresy IP**.
4. Wybierz adres IP, a następnie kliknij przycisk **Edytuj**.
5. W obszarze **Dodaj regułę zaufanego adresu IP** wykonaj jedną z następujących czynności:
   - Wybierz opcję **Pojedynczy adres IP**, a następnie wprowadź adres IP.
   - Zaznacz opcję **Zakres adresów IP**, a następnie w polach **From IP Address** (Z adresu IP) i **To IP Address** (Na adres IP) wprowadź początkowe i końcowe adresy IP.
6. Można też zaznaczyć opcję **Reguła wygasa za** i wprowadzić liczbę dni, w czasie których reguła będzie obowiązywać.
7. Dodatkowo można wprowadzić opis reguły.

   Kliknij przycisk **OK**. Zmodyfikowany adres IP zostanie wyświetlony w obszarze **Zabronione adresy IP**.

Usuwanie połączenia z zabronionym komputerem

W zaporze można usunąć połączenie z zabronionym komputerem i przypisany do niego adres IP.

Komputerom, którym są przypisane nieznane, podejrzane lub wzbudzające nieufność adresy IP, można zabronić łączenia się z komputerem użytkownika.

Ponieważ program Firewall blokuje cały niepożądany ruch, zwykle nie jest konieczne blokowanie adresu IP. Blokowanie adresu IP ma sens tylko w przypadku, gdy użytkownik jest pewien, że połączenie internetowe stanowi określone zagrożenie. Należy upewnić się, że nie są blokowane ważne adresy IP, takie jak adresy serwerów DNS czy DHCP lub innych serwerów usługodawcy internetowego. Zależnie od ustawień zabezpieczeń program Firewall może generować alert o wykryciu zdarzenia wywołanego przez zablokowany komputer.

Aby usunąć połączenie z zabronionym komputerem:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Zaufane i zabronione adresy IP**.
3. W okienku Zaufane i zabronione adresy IP wybierz opcję **Zabronione adresy IP**.
4. Wybierz adres IP i kliknij przycisk **Usuń**.
5. W oknie dialogowym **Zaufane i zabronione adresy IP** kliknij przycisk **Tak**, aby potwierdzić usunięcie adresu IP z listy **Zabronione adresy IP**.

Blokowanie dostępu komputerowi z poziomu dziennika Zdarzenia przychodzące

Połączenia z komputerem i związanym z nim adresem IP można zabronić z poziomu dziennika Zdarzenia przychodzące.

Adresy IP, które są wyświetlane w dzienniku Zdarzenia przychodzące, są zablokowane. Zabranianie dostępu adresowi nie zapewnia zatem żadnej dodatkowej ochrony, chyba że komputer użytkownika używa portów, które są celowo otwarte lub znajduje się na nim program, któremu przyznano prawa dostępu do Internetu.

Dodanie adresu IP do listy **Zabronione adresy IP** jest uzasadnione tylko wówczas, gdy co najmniej jeden port pozostaje celowo otwarty, oraz jeśli istnieją powody, aby uważać, że dostęp do otwartych portów z tego adresu musi być zablokowany.

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 zabronić dostępu połączeniu z zaufanym komputerem z poziomu dziennika Zdarzenia przychodzące:

1. Upewnij się, że włączone jest Menu zaawansowane. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
3. Kliknij opcję **Internet i sieć**, a następnie opcję **Zdarzenia przychodzące**.
4. W okienku Zdarzenia przychodzące wybierz źródłowy adres IP, a następnie kliknij opcję **Zabroń dostępu temu adresowi**.
5. W oknie dialogowym **Dodaj regułę zabronionego adresu IP** kliknij przycisk **Tak**, aby potwierdzić chęć zabronienia dostępu adresowi IP.

   Nowo dodany adres IP zostanie wyświetlony na liście **Zabronione adresy IP**.

Tematy pokrewne

- Rejestrowanie zdarzeń (strona 170)

Blokowanie dostępu komputerowi z poziomu dziennika Zdarzenia wykrywania włamań

Połączenia z komputerem i związanym z nim adresem IP można zabronić z poziomu dziennika Zdarzenia wykrywania włamań.

Komputerom, którym są przypisane nieznane, podejrzane lub wzbudzające nieufność adresy IP, można zabronić łączenia się z komputerem użytkownika.

Ponieważ program Firewall blokuje cały niepożądany ruch, zwykle nie jest konieczne blokowanie adresu IP. Blokowanie adresu IP ma sens tylko w przypadku, gdy użytkownik jest pewien, że połączenie internetowe stanowi określone zagrożenie. Należy upewnić się, że nie są blokowane ważne adresy IP, takie jak adresy serwerów DNS czy DHCP lub innych serwerów usługodawcy internetowego. Zależnie od ustawień zabezpieczeń program Firewall może generować alert o wykryciu zdarzenia wywołanego przez zablokowany komputer.

Aby zabronić połączenia z komputerem z poziomu dziennika Zdarzenia wykrywania włamań:

1. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
3. Kliknij opcję **Internet i sieć**, a następnie kliknij opcję **Zdarzenia wykrywania włamań**.
4. W okienku Zdarzenia wykrywania włamań wybierz źródłowy adres IP, a następnie kliknij opcję **Zabroń dostępu temu adresowi**.
5. W oknie dialogowym **Dodaj regułę zabronionego adresu IP** kliknij przycisk **Tak**, aby potwierdzić chęć zabronienia dostępu adresowi IP.

   Nowo dodany adres IP zostanie wyświetlony na liście **Zabronione adresy IP**.

Tematy pokrewne

- Rejestrowanie zdarzeń (strona 170)

ROZDZIAŁ 23

Rejestrowanie, monitorowanie i analiza

Korzystając z zapory, można obszernie i w sposób czytelny rejestrować, a także monitorować i analizować zdarzenia i ruch internetowy. Zrozumienie ruchu i zdarzeń internetowych pomaga zarządzać połączeniami z Internetem.

W tym rozdziale

Rejestrowanie zdarzeń 170
Praca ze statystykami 174
Śledzenie ruchu internetowego 175
Monitorowanie ruchu internetowego 179

Rejestrowanie zdarzeń

Korzystając z zapory można określić, czy rejestrowanie ma być włączone czy wyłączone. Jeśli jest ono włączone, można określić, które typy zdarzeń mają być rejestrowane. Rejestrowanie zdarzeń pozwala na przeglądanie ostatnich zdarzeń przychodzących i wychodzących. Można także wyświetlać zdarzenia wykrywania włamań.

Konfiguracja ustawień dziennika zdarzeń

Aby śledzić działanie zapory i związane z nim zdarzenia, można określić i skonfigurować rodzaje zdarzeń, które mają być wyświetlane.

Aby skonfigurować rejestrowanie zdarzeń:

1. W okienku Konfiguracja sieci i Internetu kliknij opcję **Zaawansowane**.
2. W okienku Zapora kliknij opcję **Ustawienia dziennika zdarzeń**.
3. W okienku Ustawienia dziennika zdarzeń wykonaj jedną z następujących czynności:
   - Wybierz opcję **Rejestruj zdarzenie**, aby włączyć rejestrację zdarzeń.
   - Wybierz opcję **Nie rejestruj zdarzenia**, aby wyłączyć rejestrację zdarzeń.
4. W obszarze **Ustawienia dziennika zdarzeń** określ rodzaje zdarzeń, które mają być rejestrowane. Rodzaje zdarzeń obejmują:
   - żądania ICMP ping,
   - ruch z zabronionych adresów IP,
   - zdarzenia na portach usług systemowych,
   - zdarzenia na nieznanych portach,
   - przypadki wykrywania włamań (IDS).
5. Aby zapobiec rejestrowaniu na określonych portach, wybierz polecenie **Nie rejestruj zdarzeń na następujących portach**, a następnie wpisz numery poszczególnych portów oddzielone przecinkami lub zakresy portów oddzielone myślnikami. Na przykład: `137-139, 445, 400-5000`.
6. Kliknij przycisk **OK**.

Wyświetlanie ostatnich zdarzeń

Jeśli włączono rejestrowanie, można wyświetlić ostatnie zdarzenia. W okienku Ostatnie zdarzenia jest wyświetlana data i opis zdarzenia. W okienku Ostatnie zdarzenia są wyświetlane tylko działania programów, których dostęp do Internetu został wyraźnie zablokowany.

Aby wyświetlić ostatnie zdarzenia zapory:

- W **Menu zaawansowanym**, w okienku Typowe zadania kliknij opcję **Raporty i dzienniki** lub opcję **Przeglądaj ostatnie zdarzenia**. W tym celu można też kliknąć opcję **Przeglądaj ostatnie zdarzenia** w okienku Typowe zadania menu podstawowego.

Wyświetlanie zdarzeń przychodzących

Jeśli jest włączone rejestrowanie, można wyświetlić i posortować zdarzenia przychodzące.

Dziennik zdarzeń przychodzących obejmuje następujące kategorie rejestrowania:

- Data i godzina
- Źródłowy adres IP
- Nazwa hosta
- Typ informacji i zdarzenia

Aby wyświetlić zdarzenia przychodzące zapory:

1. Upewnij się, że włączone jest Menu zaawansowane. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
3. Kliknij opcję **Internet i sieć**, a następnie opcję **Zdarzenia przychodzące**.

Uwaga: Adres IP z dziennika zdarzeń przychodzących można uznać za zaufany, zablokować go lub śledzić.

Tematy pokrewne

- Dodawanie zaufanego komputera z poziomu dziennika Zdarzenia przychodzące (strona 160)
- Blokowanie dostępu komputerowi z poziomu dziennika Zdarzenia przychodzące (strona 167)
- Śledzenie komputera z poziomu dziennika Zdarzenia przychodzące (strona 176)

Wyświetlanie zdarzeń wychodzących

Jeśli jest włączone rejestrowanie, można wyświetlić zdarzenia wychodzące. Dane zdarzeń wychodzących obejmują nazwę programu próbującego uzyskać dostęp na zewnątrz, datę i godzinę zdarzenia oraz lokalizację programu na komputerze.

Aby wyświetlić zdarzenia wychodzące zapory:

1. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
3. Wybierz opcję **Internet i sieć**, a następnie opcję **Zdarzenia wychodzące**.

Uwaga: Programowi z dziennika Zdarzenia wychodzące można przyznać pełny dostęp lub dostęp tylko dla połączeń wychodzących. W dzienniku można również znaleźć dodatkowe informacje o programie.

Tematy pokrewne

- Przyznawanie pełnego dostępu z poziomu dziennika Zdarzenia wychodzące (strona 144)
- Przyznawanie dostępu tylko dla połączeń wychodzących z poziomu dziennika Zdarzenia wychodzące (strona 146)
- Informacje o programie znajdujące się w dzienniku Zdarzenia wychodzące (strona 150)

Wyświetlanie zdarzeń wykrywania włamań

Jeśli włączone jest rejestrowanie, można wyświetlić zdarzenia przychodzące. Dane zdarzenia wykrywania włamań zawierają datę i godzinę zdarzenia, źródłowy adres IP i nazwę hosta. Dziennik zawiera również opis typu zdarzenia.

Aby wyświetlić zdarzenia wykrywania włamań:

1. W okienku Typowe zadania kliknij opcję **Raporty i Dzienniki**.
2. W obszarze Ostatnie zdarzenia kliknij opcję **Wyświetl dziennik**.
3. Kliknij opcję **Internet i sieć**, a następnie kliknij opcję **Zdarzenia wykrywania włamań**.

Uwaga: Adres IP z dziennika Zdarzenia wykrywania włamań można zablokować i śledzić.

Tematy pokrewne

- Blokowanie dostępu komputerowi z poziomu dziennika Zdarzenia wykrywania włamań (strona 168)
- Śledzenie komputera z poziomu dziennika Zdarzenia wykrywania włamań (strona 177)

Praca ze statystykami

Wykorzystanie poświęconej bezpieczeństwu witryny sieci Web firmy McAfee HackerWatch pozwala zaporze dostarczać użytkownikowi statystyk o globalnych zdarzeniach związanych z bezpieczeństwem Internetu i aktywnością portów.

Wyświetlanie światowych statystyk dotyczących zagrożeń bezpieczeństwa

Program HackerWatch monitoruje zagrożenia internetowe z całego świata. Dotyczące ich informacje można przeglądać w programie SecurityCenter. Informacje dotyczą przypadków przekazanych do programu HackerWatch w ciągu ostatnich 24 godzin, 7 dni i 30 dni.

Aby wyświetlić światowe statystyki dotyczące zagrożeń bezpieczeństwa:

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **HackerWatch**.
3. Wyświetl światowe statystyki dotyczące zagrożeń bezpieczeństwa w obszarze **Monitorowanie zdarzeń**.

Wyświetlanie aktywności dotyczącej portów internetowych na świecie

Program HackerWatch monitoruje zagrożenia internetowe z całego świata. Dotyczące ich informacje można przeglądać w programie SecurityCenter. Wyświetlone informacje opisują porty związane z najistotniejszymi zdarzeniami przekazanymi do programu HackerWatch w ciągu ostatnich siedmiu dni. Zazwyczaj wyświetlane są informacje o portach HTTP, TCP i UDP.

Aby wyświetlić aktywność portów na całym świecie:

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **HackerWatch**.
3. W obszarze **Niedawna aktywność portów** wyświetl najistotniejsze zdarzenia dotyczące portów.

Śledzenie ruchu internetowego

Zapora udostępnia kilka opcji śledzenia ruchu internetowego. Umożliwiają one lokalizację komputera sieciowego, uzyskanie informacji o domenie i sieci oraz odszukanie komputerów z dzienników zdarzeń przychodzących i zdarzeń wykrywania włamań.

Lokalizowanie komputera w sieci

Programu Visual Tracer można użyć do zlokalizowania komputera, który łączy się lub próbuje połączyć się z komputerem użytkownika, przy wykorzystaniu jego nazwy i adresu IP. Przy pomocy programu Visual Tracer można również uzyskać dostęp do informacji o sieci i rejestracji. Program Visual Tracer umożliwia wyświetlenie mapy świata pokazującej najbardziej prawdopodobną drogę, którą pokonały dane z komputera źródłowego do komputera użytkownika.

Aby zlokalizować komputer:

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **Wątek śledzenia wizualnego**.
3. Wprowadź adres IP komputera i kliknij opcję **Zlokalizuj**.
4. W obszarze **Wątek śledzenia wizualnego** wybierz polecenie **Widok mapy**.

Uwaga: Nie można śledzić zdarzeń związanych z pętlowymi, prywatnymi lub nieprawidłowymi adresami IP.

Uzyskiwanie informacji o rejestracji komputera

Informacje o rejestracji komputera można uzyskać, korzystając z modułu Visual Trace w programie SecurityCenter. Informacje zawierają nazwę domeny, nazwę i adres rejestrującego oraz kontakt administracyjny.

Aby uzyskać informacje o domenie komputera:

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **Wątek śledzenia wizualnego**.
3. Wprowadź adres IP komputera, a następnie kliknij opcję **Zlokalizuj**.
4. W obszarze **Wątek śledzenia wizualnego** wybierz polecenie **Widok rejestracji**.

Informacje o sieci komputera

Informacje o sieci komputera można uzyskać, korzystając z modułu Visual Trace w programie SecurityCenter. Informacje o sieci zawierają szczegóły dotyczące sieci, w której znajduje się domena.

Aby uzyskać informacje o sieci komputera:

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **Wątek śledzenia wizualnego**.
3. Wprowadź adres IP komputera, a następnie kliknij opcję **Zlokalizuj**.
4. W obszarze **Wątek śledzenia wizualnego** wybierz polecenie **Widok sieci**.

Śledzenie komputera z poziomu dziennika Zdarzenia przychodzące

Z okienka Zdarzenia przychodzące można śledzić adres IP, który jest wyświetlony w dzienniku Zdarzenia przychodzące.

Aby śledzić adres IP komputera z poziomu dziennika Zdarzenia przychodzące:

1. Upewnij się, że włączone jest Menu zaawansowane. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
3. Kliknij opcję **Internet i sieć**, a następnie opcję **Zdarzenia przychodzące**.
4. W okienku Zdarzenia przychodzące wybierz źródłowy adres IP, a następnie kliknij opcję **Śledź ten adres**.
5. W okienku Wątek śledzenia wizualnego kliknij jedną z następujących opcji:
   - **Widok mapy**: Geograficzna lokalizacja komputera przy użyciu wybranego adresu IP.
   - **Widok rejestracji**: Wyszukiwanie informacji o domenie przy użyciu wybranego adresu IP.
   - **Widok sieci**: Wyszukiwanie informacji o sieci przy użyciu wybranego adresu IP.
6. Kliknij przycisk **Gotowe**.

Tematy pokrewne

- Śledzenie ruchu internetowego (strona 175)
- Wyświetlanie zdarzeń przychodzących (strona 171)

Śledzenie komputera z poziomu dziennika Zdarzenia wykrywania włamań

Z poziomu okienka Zdarzenia wykrywania włamań można śledzić adres IP, który jest wyświetlony w dzienniku Zdarzenia wykrywania włamań.

Aby śledzić adres IP komputera z poziomu dziennika Zdarzenia wykrywania włamań:

1. W okienku Typowe zadania kliknij opcję **Raporty i dzienniki**.
2. W obszarze **Ostatnie zdarzenia** kliknij opcję **Wyświetl dziennik**.
3. Kliknij opcję **Internet i sieć**, a następnie kliknij opcję **Zdarzenia wykrywania włamań**.W okienku Zdarzenia wykrywania włamań wybierz źródłowy adres IP, a następnie kliknij opcję **Śledź ten adres**.
4. W okienku Wątek śledzenia wizualnego kliknij jedną z następujących opcji:
   - **Widok mapy**: Geograficzna lokalizacja komputera przy użyciu wybranego adresu IP.
   - **Widok rejestracji**: Wyszukiwanie informacji o domenie przy użyciu wybranego adresu IP.
   - **Widok sieci**: Wyszukiwanie informacji o sieci przy użyciu wybranego adresu IP.
5. Kliknij przycisk **Gotowe**.

Tematy pokrewne

- Śledzenie ruchu internetowego (strona 175)
- Rejestrowanie, monitorowanie i analiza (strona 169)

Śledzenie monitorowanego adresu IP

Monitorowany adres IP można śledzić w celu utworzenia widoku geograficznego pokazującego najbardziej prawdopodobną trasę danych otrzymanych z komputera źródłowego przez komputer użytkownika. Ponadto można uzyskać informacje rejestracyjne i sieciowe dotyczące danego adresu IP.

Aby monitorować wykorzystanie przepustowości przez programy:

1. Upewnij się, że jest włączone menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **Monitor ruchu**.
3. W obszarze **Monitor ruchu** kliknij opcję **Aktywne programy**.
4. Wybierz program, a następnie adres IP wyświetlany pod nazwą programu.
5. W obszarze **Działania programu** kliknij opcję **Śledź ten adres IP**.
6. W obszarze **Wątek śledzenia wizualnego** można wyświetlić mapę pokazującą najbardziej prawdopodobną trasę, jaką dane są przesyłane z komputera źródłowego do tego komputera. Ponadto można uzyskać informacje rejestracyjne i sieciowe dotyczące danego adresu IP.

Uwaga: Aby wyświetlić najnowsze dane statystyczne, kliknij przycisk **Odśwież** w obszarze **Wątek śledzenia wizualnego**.

Tematy pokrewne

- Monitorowanie ruchu internetowego (strona 179)

Monitorowanie ruchu internetowego

Zapora umożliwia kilka sposobów monitorowania ruchu internetowego, między innymi:

- **Wykres Analiza ruchu**: Pokazuje ostatni przychodzący i wychodzący ruch internetowy.
- **Wykres Wykorzystanie ruchu**: Pokazuje wartość procentową wykorzystania przepustowości przez najbardziej aktywne programy w ciągu ostatnich 24 godzin.
- **Aktywne programy**: Pokazuje programy, które obecnie wykorzystują najwięcej połączeń sieciowych komputera oraz adresy IP, z którymi te programy się łączą.

Informacje o wykresie Analiza ruchu

Wykres Analiza ruchu jest liczbową i graficzną reprezentacją przychodzącego i wychodzącego ruchu internetowego. Ponadto Monitor ruchu wyświetla programy, które wykorzystują największą liczbę połączeń sieciowych komputera oraz adresy IP, z którymi te programy się łączą.

W okienku Analiza ruchu można obejrzeć najnowsze dane na temat przychodzącego i wychodzącego ruchu internetowego, bieżącą, średnią i maksymalną szybkość przesyłania danych. Można także sprawdzić dane dotyczące ilości przesyłanych danych, w tym ilość danych przesłanych od uruchomienia zapory i całkowitą ilość danych przesłanych w bieżącym miesiącu i w miesiącach poprzednich.

W okienku Analiza ruchu są wyświetlane na bieżąco dane o aktywności internetowej na komputerze użytkownika, w tym ilość danych przychodzącego i wychodzącego ruchu internetowego w ostatnim czasie, szybkość połączenia i całkowita ilość danych przesłanych przez Internet.

Ciągła zielona linia oznacza bieżącą szybkość transferu dla ruchu przychodzącego. Przerywana zielona linia oznacza średnią szybkość transferu dla ruchu przychodzącego. Jeśli bieżąca szybkość transferu i średnia szybkość transferu są takie same, linia przerywana na wykresie nie jest wyświetlana. Linia ciągła reprezentuje wtedy zarówno średnią, jak i bieżącą szybkość transferu.

Ciągła czerwona linia reprezentuje bieżącą szybkość transferu dla ruchu wychodzącego. Przerywana czerwona linia reprezentuje średnią szybkość transferu dla ruchu wychodzącego. Jeśli bieżąca szybkość transferu i średnia szybkość transferu są takie same, linia przerywana na wykresie nie jest wyświetlana. Linia ciągła reprezentuje wtedy zarówno średnią, jak i bieżącą szybkość transferu.

Tematy pokrewne

- Analiza ruchu przychodzącego i wychodzącego (strona 180)

Analiza ruchu przychodzącego i wychodzącego

Wykres Analiza ruchu jest liczbową i graficzną reprezentacją przychodzącego i wychodzącego ruchu internetowego. Ponadto Monitor ruchu wyświetla programy, które wykorzystują największą liczbę połączeń sieciowych komputera oraz adresy IP, z którymi te programy się łączą.

Aby przeanalizować ruch przychodzący i wychodzący:

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **Monitor ruchu**.
3. W obszarze **Monitor ruchu** kliknij opcję **Analiza ruchu**.

Wskazówka: Aby wyświetlić najnowsze dane statystyczne, kliknij przycisk **Odśwież** w obszarze **Analiza ruchu**.

Tematy pokrewne

- Informacje o wykresie Analiza ruchu (strona 179)

Monitorowanie przepustowości wykorzystywanej przez programy

Można wyświetlić wykres kołowy, który zawiera przybliżone wartości procentowe przepustowości wykorzystywanej przez najaktywniejsze programy na komputerze w okresie ostatnich dwudziestu czterech godzin. Wykres kołowy stanowi wizualną reprezentację względnych wartości wykorzystania przepustowości pasma przez programy.

Aby monitorować wykorzystanie przepustowości przez programy:

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **Monitor ruchu**.
3. W obszarze **Monitor ruchu** kliknij opcję **Analiza ruchu**.

Wskazówka: Aby wyświetlić najnowsze dane statystyczne, kliknij opcję **Odśwież** w obszarze **Wykorzystanie ruchu**.

Monitorowanie aktywności programów

Można wyświetlić dane dotyczące aktywności programu (ruch przychodzący i wychodzący) obejmujące połączenia ze zdalnych komputerów i porty.

Aby monitorować wykorzystanie przepustowości przez programy:

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **Monitor ruchu**.
3. W obszarze **Monitor ruchu** kliknij opcję **Aktywne programy**.
4. Można wyświetlić następujące informacje:
   - Wykres Aktywność programu: Wybierz program, dla którego ma zostać wyświetlony wykres aktywności.
   - Połączenie nasłuchujące: Wybierz opcję Nasłuchiwanie znajdującą się pod nazwą programu.
   - Połączenie komputera: Wybierz adres IP pod nazwą programu, procesem systemowym lub usługą.

Uwaga: Aby wyświetlić najnowsze dane statystyczne, kliknij opcję **Odśwież** w obszarze **Aktywne programy**.

ROZDZIAŁ 24

Informacje o bezpieczeństwie internetowym

Wykorzystanie poświęconej bezpieczeństwu witryny sieci Web firmy McAfee HackerWatch pozwala zaporze dostarczać aktualnych informacji o programach i aktywności w Internecie. W witrynie HackerWatch dostępny jest także podręcznik zapory w formacie HTML.

W tym rozdziale

Uruchamianie samouczka witryny HackerWatch 184

Uruchamianie samouczka witryny HackerWatch

Więcej informacji na temat zapory znajduje się w samouczku witryny HackerWatch w programie SecurityCenter.

Aby uruchomić samouczek witryny HackerWatch:

1. Upewnij się, że włączone jest Menu zaawansowane, a następnie kliknij opcję **Narzędzia**.
2. W okienku Narzędzia kliknij opcję **HackerWatch**.
3. W obszarze **Zasoby witryny HackerWatch** kliknij przycisk **Wyświetl samouczek**.

ROZDZIAŁ 25

McAfee SpamKiller

Program SpamKiller odfiltrowuje spam i wiadomości e-mail typu „phishing”, oferując opisane poniżej możliwości.

Opcje użytkownika

- filtrowanie wielu kont poczty e-mail,
- importowanie kontaktów do listy znajomych,
- tworzenie niestandardowych filtrów i raportowanie spamu do firmy McAfee w celu dalszych analiz,
- opcje oznaczania wiadomości jako spam i jako nie-spam,
- obsługa wielu użytkowników (Windows® XP i Vista™).

Filtrowanie

- automatyczna aktualizacja filtrów,
- tworzenie niestandardowych filtrów wiadomości e-mail,
- wielowarstwowy aparat filtrujący,
- filtry wiadomości typu „phishing”.

W tym rozdziale

Funkcje 186
Obsługa kont pocztowych w sieci Web 189
Zarządzanie listą znajomych 197
Modyfikowanie opcji filtrowania 203
Zarządzanie filtrami osobistymi 209
Obsługa programu SpamKiller 219
Konfigurowanie ochrony przed atakami typu „phishing” . 223
Dodatkowa pomoc 227

Funkcje

W tej wersji programu SpamKiller dostępne są opisane poniżej funkcje.

Filtrowanie

Zaawansowana technologia filtrowania zwiększa zakres czynności dostępnych dla użytkownika.

Phishing

Funkcja Phishing z łatwością rozpoznaje i blokuje strony sieci Web, które mogą potencjalnie dokonywać ataków typu "phishing".

Instalacja

Wyjątkowo prosta instalacja i konfiguracja.

Interfejs

Intuicyjny interfejs użytkownika pomagający zabezpieczyć komputer przed spamem.

Pomoc techniczna

Bezpłatna pomoc techniczna za pośrednictwem poczty e-mail i wiadomości błyskawicznych zapewnia szybką i przystępną obsługę klienta.

Przetwarzanie wiadomości typu spam

Opcjonalne ustawienia dotyczące postępowania z wiadomościami poczty e-mail uznanymi za spam. Funkcja umożliwia wyświetlanie wiadomości, które mogły zostać nieprawidłowo odfiltrowane.

Obsługiwane programy pocztowe

- dowolne programy poczty e-mail zgodne z protokołem POP3,
- obsługa interfejsu MAPI w programie Outlook® 2000 lub nowszym,
- obsługa filtrowania poczty internetowej korzystającej z protokołu POP3 lub płatnych serwisów MSN®/Hotmail®.

Obsługiwane paski narzędzi poczty e-mail

- Program Outlook Express w wersji 6.0 lub nowszej
- Outlook 2000, XP, 2003 lub 2007
- Eudora® w wersji 6.0 lub nowszej,
- Thunderbird™ w wersji 1.5 lub nowszej

Obsługiwana ochrona przed atakami typu "phishing"

Dowolna przeglądarka sieci Web zgodna z protokołem HTTP, włącznie z programami:

- Internet Explorer
- Firefox®
- Netscape®

ROZDZIAŁ 26

Obsługa kont pocztowych w sieci Web

Można dodawać konta poczty internetowej w celu filtrowania spamu, edytować informacje o kontach poczty internetowej lub usuwać konta, gdy nie mają już być dłużej filtrowane.

Można również zarządzać filtrowaniem poczty internetowej. Przykładowo, można wyłączać lub włączać filtrowanie wiadomości e-mail w kontach poczty internetowej, zarządzać odfiltrowanymi już wiadomościami oraz przeglądać dzienniki.

W tym rozdziale

Dodawanie kont poczty internetowej 190
Modyfikowanie ustawień kont poczty internetowej 192
Usuwanie kont poczty internetowej 194
Zarządzanie filtrowaniem poczty internetowej 195

Dodawanie kont poczty internetowej

Można dodawać następujące rodzaje kont poczty internetowej w celu filtrowania ich pod kątem spamu:

- poczta internetowa POP3 (na przykład Yahoo□)
- MSN/Hotmail (w pełni obsługiwana jest tylko wersja płatna)

Dodawanie kont poczty internetowej POP3 lub MSN/Hotmail

Dodawanie kont poczty e-mail w celu filtrowania pod kątem spamu.

Aby dodać konto poczty internetowej POP3 lub MSN/Hotmail:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Konta pocztowe w sieci Web**.
5. W okienku Konta pocztowe w sieci Web kliknij przycisk **Dodaj**.
6. Podaj informacje o koncie poczty internetowej w następujących polach:
   - **Opis**: Opisuje konto. W tym polu można wpisać dowolne informacje.
   - **Adres e-mail**: Przypisuje adres poczty e-mail do tego konta.
   - **Typ konta**: Określa typ konta poczty e-mail.
   - **Serwer**: Określa nazwę serwera przypisanego do danego konta.
   - **Nazwa użytkownika**: Określa nazwę użytkownika przypisaną do danego konta.
   - **Hasło**: Określa hasło używane w celu uzyskania dostępu do danego konta.
   - **Potwierdź hasło**: Potwierdza podane hasło.
7. Kliknij przycisk **Dalej**.
8. W obszarze **Opcje sprawdzania** wykonaj jedną z następujących czynności, aby określić częstotliwość sprawdzania konta przez program SpamKiller:
   - W polu **Sprawdź co** wpisz odpowiednią wartość.

     Program SpamKiller będzie sprawdzać konto w podanych tu odstępach czasu (w minutach). W przypadku wprowadzenia zera, program SpamKiller będzie sprawdzać konto tylko po nawiązaniu połączenia z Internetem.

- Zaznacz pole wyboru **Sprawdź podczas uruchamiania**.

  Program SpamKiller będzie sprawdzać konto podczas każdego kolejnego uruchamiania komputera. Zaznacz tę opcję, jeśli masz stałe łącze internetowe.

9 Jeśli korzystasz z połączenia telefonicznego, wykonaj jedną z następujących czynności w obszarze **Opcje połączenia**, aby określić, w jaki sposób program SpamKiller ma łączyć się z Internetem:

- Kliknij opcję **Nigdy nie wybieraj numeru połączenia.**

  Umożliwia wyłączenie opcji samodzielnego wybierania numeru połączenia przez program SpamKiller. W takim przypadku użytkownik musi najpierw ręcznie nawiązać połączenie telefoniczne.

- Kliknij opcję **Wybierz numer w przypadku braku połączenia**.

  Gdy połączenie z Internetem jest niedostępne, program SpamKiller automatycznie podejmuje próbę nawiązania go przy użyciu domyślnego telefonicznego połączenia z Internetem.

- Kliknij opcję **Zawsze wybieraj określony numer**.

  Program SpamKiller będzie zawsze próbował uzyskać połączenie przy użyciu podanego numeru telefonicznego.

- Kliknij pozycję na liście **Wybierz numer połączenia**.

  Ten wpis definiuje połączenie telefoniczne, z którego będzie korzystał program SpamKiller przy próbie nawiązania połączenia.

- Kliknij opcję **Utrzymaj połączenie po zakończeniu filtrowania**.

  Komputer będzie utrzymywał połączenie z Internetem po zakończeniu procesu filtrowania.

10 Kliknij przycisk **Zakończ**.

Modyfikowanie ustawień kont poczty internetowej

Można włączać lub wyłączać konta poczty internetowej lub edytować ich właściwości. Można na przykład zmienić adres poczty e-mail, opis i rodzaj konta, hasło, częstotliwość sprawdzania przez program SpamKiller obecności spamu na koncie oraz sposób łączenia się komputera z Internetem.

Edycja internetowych kont POP3 lub MSN/Hotmail

Można włączać lub wyłączać konta poczty internetowej lub edytować ich właściwości. Można na przykład zmienić adres poczty e-mail, opis konta, informacje o serwerze, częstotliwość sprawdzania konta przez program SpamKiller pod kątem spamu oraz sposób łączenia się komputera z Internetem.

Aby dokonać edycji konta internetowej poczty POP3 lub MSN/Hotmail:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Konta pocztowe w sieci Web**.
5. Wybierz konto, które ma być zmienione, a następnie kliknij przycisk **Edytuj**.
6. Informacje o koncie zmień w następujących polach:
   - **Opis**: Opisuje konto. W tym polu można wpisać dowolne informacje.
   - **Adres e-mail**: Przypisuje adres poczty e-mail do tego konta.
   - **Typ konta**: Określa typ konta poczty e-mail.
   - **Serwer**: Określa nazwę serwera przypisanego do danego konta.
   - **Nazwa użytkownika**: Określa nazwę użytkownika przypisaną do danego konta.
   - **Hasło**: Określa hasło używane w celu uzyskania dostępu do danego konta.
   - **Potwierdź hasło**: Potwierdza podane hasło.
7. Kliknij przycisk **Dalej**.
8. W obszarze **Opcje sprawdzania** wykonaj jedną z następujących czynności, aby określić częstotliwość sprawdzania konta przez program SpamKiller:
   - W polu **Sprawdź co** wpisz odpowiednią wartość.

Program SpamKiller będzie sprawdzać konto w podanych tu odstępach czasu (w minutach). W przypadku wprowadzenia zera, program SpamKiller będzie sprawdzać konto tylko po nawiązaniu połączenia z Internetem.

- Zaznacz pole wyboru **Sprawdź podczas uruchamiania**.

  Program SpamKiller będzie sprawdzać konto podczas każdego kolejnego uruchamiania komputera. Zaznacz tę opcję, jeśli masz stałe łącze internetowe.

9 Jeśli korzystasz z połączenia telefonicznego, wykonaj jedną z następujących czynności w obszarze **Opcje połączenia**, aby określić, w jaki sposób program SpamKiller ma łączyć się z Internetem:

- Kliknij opcję **Nigdy nie wybieraj numeru połączenia.**

  Umożliwia wyłączenie opcji samodzielnego wybierania numeru połączenia przez program SpamKiller. W takim przypadku użytkownik musi najpierw ręcznie nawiązać połączenie telefoniczne.

- Kliknij opcję **Wybierz numer w przypadku braku połączenia**.

  Gdy połączenie z Internetem jest niedostępne, program SpamKiller automatycznie podejmuje próbę nawiązania go przy użyciu domyślnego telefonicznego połączenia z Internetem.

- Kliknij opcję **Zawsze wybieraj określony numer**.

  Program SpamKiller będzie zawsze próbował uzyskać połączenie przy użyciu podanego numeru telefonicznego.

- Kliknij pozycję na liście **Wybierz numer połączenia**.

  Ten wpis definiuje połączenie telefoniczne, z którego będzie korzystał program SpamKiller przy próbie nawiązania połączenia.

- Kliknij opcję **Utrzymaj połączenie po zakończeniu filtrowania**.

  Komputer będzie utrzymywał połączenie z Internetem po zakończeniu procesu filtrowania.

10 Kliknij przycisk **Zakończ**.

Usuwanie kont poczty internetowej

Można usuwać konta poczty internetowej, jeśli ich filtrowanie nie jest już wymagane.

Usuwanie konta poczty internetowej

Konto e-mail, którego nie trzeba już filtrować, należy usunąć.

Aby usunąć konto poczty internetowej:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Konta pocztowe w sieci Web**.
5. Wybierz konto, które ma zostać usunięte, a następnie kliknij przycisk **Usuń**.

Zarządzanie filtrowaniem poczty internetowej

Można wyłączać lub włączać filtrowanie wiadomości e-mail w kontach poczty internetowej, zarządzać odfiltrowanymi już wiadomościami oraz przeglądać dzienniki.

Wyłączanie filtrowania poczty internetowej

Można wyłączyć filtrowanie poczty internetowej, co zapobiega filtrowaniu wiadomości e-mail.

Aby wyłączyć filtrowanie poczty internetowej:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Konta pocztowe w sieci Web**.
5. Usuń zaznaczenie pola wyboru obok konta, które ma zostać wyłączone.
6. Kliknij przycisk **OK**.

Włączanie filtrowania poczty internetowej

Jeśli filtrowanie któregokolwiek konta poczty internetowej zostało wyłączone, można je włączyć ponownie.

Aby włączyć filtrowanie poczty internetowej:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Konta pocztowe w sieci Web**.
5. Zaznacz pole wyboru obok konta, które chcesz włączyć.
6. Kliknij przycisk **OK**.

Zarządzanie odfiltrowanymi wiadomościami w kontach poczty internetowej

Można przeglądać, kopiować lub usuwać wiadomości z konta poczty internetowej, które zostały odfiltrowane.

Aby przeglądać, kopiować lub usuwać wiadomości z konta poczty internetowej, które zostały odfiltrowane:

1. W Menu zaawansowanym kliknij opcję **Raporty i dzienniki**.
2. W okienku Raporty i dzienniki kliknij opcję **Filtrowana poczta z sieci Web**.
3. W okienku Filtrowana poczta z sieci Web wybierz wiadomość, którą chcesz wyświetlić, skopiować lub usunąć.
4. W obszarze **Działanie** wykonaj jedną z następujących czynności:
   - Kliknij przycisk **Kopiuj**, aby skopiować wiadomość do schowka.
   - Kliknij przycisk **Usuń**, aby usunąć wiadomość.

Przeglądanie dzienników odfiltrowanej poczty internetowej

Dzienniki odfiltrowanej poczty internetowej można przeglądać. Na przykład można sprawdzić, kiedy wiadomość e-mail została odfiltrowana oraz z którego konta pochodzi.

Aby wyświetlić dzienniki odfiltrowanych wiadomości poczty internetowej:

1. W Menu zaawansowanym kliknij opcję **Raporty i dzienniki**.
2. W okienku Raporty i dzienniki kliknij opcję **Ostatnie zdarzenia**.
3. W okienku Ostatnie zdarzenia kliknij opcję **Wyświetl dziennik**.
4. W lewym okienku rozwiń listę **Poczta e-mail i wiadomości błyskawiczne**, a następnie kliknij pozycję **Zdarzenia filtrowania poczty z sieci Web**.
5. Wybierz dziennik, który ma zostać wyświetlony.
6. W obszarze **Szczegóły** sprawdź informacje z danego dziennika.

ROZDZIAŁ 27

Zarządzanie listą znajomych

Aby zapewnić odbieranie wszystkich wiadomości od swoich znajomych, należy dodać ich adresy do listy znajomych. Można również dodawać adresy domen, edytować lub usuwać znajomych oraz skonfigurować automatyczną aktualizację listy znajomych.

W tym rozdziale

Omówienie zarządzania listą znajomych 198
Automatyczna aktualizacja znajomych 200

Omówienie zarządzania listą znajomych

W sekcji tej opisano, jak zarządzać listą znajomych.

Ręczne dodawanie znajomych z poziomu paska zadań programu SpamKiller

Aby zapewnić odbieranie wszystkich wiadomości od swoich znajomych, należy dodać ich adresy do listy znajomych.

W wypadku korzystania do obsługi poczty e-mail z programów Outlook, Outlook Express, Windows Mail, Eudora lub Thunderbird, można dodawać znajomych z poziomu paska zadań programu SpamKiller.

Aby dodać znajomego z poziomu programu Outlook:

- W programie poczty e-mail wybierz wiadomość, a następnie kliknij przycisk **Dodaj znajomego**.

Aby dodać znajomego z poziomu programu Outlook Express, Windows Mail, Eudora lub Thunderbird:

- Wybierz wiadomość w programie poczty e-mail. Następnie w menu **SpamKiller** kliknij opcję **Dodaj znajomego**.

Ręczne dodawanie znajomych

Aby zapewnić odbieranie wszystkich wiadomości od swoich znajomych, należy dodać ich adresy do listy znajomych. Można również dodawać domeny.

Aby ręcznie dodać znajomych:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze Ochrona przed spamem kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Znajomi**.
5. W okienku Znajomi kliknij przycisk **Dodaj**.
6. Wpisz informacje o znajomym w następujących polach:
   - **Nazwa**: Określa imię i nazwisko znajomego.
   - **Typ**: Określa, czy podany zostanie pojedynczy adres e-mail, czy też cała domena.
   - **Adres e-mail**: Określa adres e-mail znajomego lub domenę, skąd wiadomości nie mają być odfiltrowywane.
7. Kliknij przycisk **OK**.

Edycja listy znajomych

Jeśli informacje dotyczące znajomych zmienią się, można uaktualnić listę, aby zapewnić odbiór wszystkich ich wiadomości.

Aby dokonać edycji listy znajomych:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze Ochrona przed spamem kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Znajomi**.
5. Wybierz znajomego, którego dane mają zostać poddane edycji, a następnie kliknij przycisk **Edytuj**.
6. Zmień informacje o znajomym w następujących polach:
   - **Nazwa**: Określa imię i nazwisko znajomego.
   - **Typ**: Określa, czy podany zostanie pojedynczy adres e-mail, czy też cała domena.
   - **Adres e-mail**: Określa adres e-mail znajomego lub domenę, skąd wiadomości nie mają być odfiltrowywane.
7. Kliknij przycisk **OK**.

Usuwanie znajomych

Usunięcie znajomych z tej listy powoduje włączenie filtrowania pochodzących od nich wiadomości.

Aby usunąć znajomych:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Znajomi**.
5. Wybierz znajomego, który ma zostać usunięty, a następnie kliknij przycisk **Usuń.**

Automatyczna aktualizacja znajomych

Aby zapewnić odbieranie wszystkich wiadomości od swoich znajomych, można ręcznie zaimportować ich adresy z książki adresowej lub skonfigurować automatyczną aktualizację.

Ręczne importowanie książek adresowych

Program SpamKiller umożliwia importowanie książek adresowych i aktualizowanie listy znajomych.

Aby ręcznie zaimportować książki adresowe:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Książki adresowe**.
5. Wybierz książkę adresową przeznaczoną do importu, a następnie kliknij przycisk **Uruchom teraz**.
6. Kliknij przycisk **OK**.

Dodawanie książek adresowych

Aby zapewnić odbieranie wszystkich wiadomości od swoich znajomych, zaleca się zaimportować wszystkie książki adresowe.

Aby dodać książki adresowe:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Książki adresowe**.
5. W okienku Książki adresowe kliknij przycisk **Dodaj**.
6. Na liście **Typ** kliknij typ książki adresowej, który chcesz zaimportować.
7. W razie potrzeby wybierz źródło książki adresowej z listy **Źródło**.
8. Na liście **Harmonogram** kliknij opcję **Codziennie**, **Co tydzień** lub **Co miesiąc**, aby określić, jak często program SpamKiller ma sprawdzać książkę adresową w poszukiwaniu nowych adresów.
9. Kliknij przycisk **OK**.

Edycja książek adresowych

Program SpamKiller umożliwia zgodne z harmonogramem importowanie książek adresowych i aktualizowanie listy znajomych. Można również edytować książki adresowe i zmieniać harmonogram ich importowania.

Aby dokonać edycji książek adresowych:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Książki adresowe**.
5. Wybierz książkę adresową, której ustawienia chcesz zmienić, a następnie kliknij przycisk **Edytuj**.
6. Wykonaj dowolną z poniższych czynności:
   - Na liście **Typ** kliknij typ książki adresowej, który chcesz zaimportować.
   - W razie potrzeby wybierz źródło książki adresowej z listy **Źródło**.
   - Na liście **Harmonogram** kliknij opcję **Codziennie**, **Co tydzień** lub **Co miesiąc**, aby określić, jak często program SpamKiller ma sprawdzać książkę adresową w poszukiwaniu nowych adresów.
7. Kliknij przycisk **OK**.

Usuwanie książek adresowych

Książkę adresową można usunąć z listy, jeśli program SpamKiller nie ma dłużej automatycznie importować z niej adresów.

Aby usunąć książkę adresową z listy automatycznego importowania:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Książki adresowe**.
5. Wybierz książkę adresową, która ma zostać usunięta, a następnie kliknij przycisk **Usuń**.

ROZDZIAŁ 28

Modyfikowanie opcji filtrowania

Opcje filtrowania obejmują zmianę poziomu filtrowania, modyfikację filtrów specjalnych, dostosowanie sposobu obsługi wiadomości, określanie zestawów znaków przeznaczonych do filtrowania oraz raportowanie spamu do firmy McAfee.

W tym rozdziale

Modyfikowanie ustawień filtrowania wiadomości e-mail . 204
Zmiana sposobu przetwarzania wiadomości zidentyfikowanych jako spam 206
Filtrowanie wiadomości zawierających określone zestawy znaków 207
Zgłaszanie wiadomości uznanych za spam 208

Modyfikowanie ustawień filtrowania wiadomości e-mail

Można zmienić stopień agresywności filtrowania wiadomości. Jeśli poprawne wiadomości są przechwytywane przez filtr, można obniżyć poziom filtrowania.

Można również włączać lub wyłączać filtry specjalne. Na przykład domyślnie są odfiltrowywane wiadomości zawierające głównie obrazy. Aby otrzymywać takie wiadomości, można wyłączyć ten filtr.

Zmiana poziomu filtrowania wiadomości e-mail

Można zmienić stopień agresywności filtrowania wiadomości. Na przykład, jeśli poprawne wiadomości są przechwytywane przez filtr, można obniżyć poziom filtrowania.

Aby zmienić poziom filtrowania wiadomości e-mail:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Opcje filtrowania**.
5. W obszarze **Opcje filtrowania** przesuń suwak do jednego z następujących ustawień poziomu filtrowania:
   - **Niski**: Większość wiadomości poczty e-mail jest akceptowana.
   - **Średnio-niski**: Tylko wiadomości z oczywistym spamem będą odfiltrowywane.
   - **Średni**: Większa ilość wiadomości będzie akceptowana.
   - **Średnio-wysoki**: Wszelkie wiadomości przypominające spam będą odfiltrowywane.
   - **Wysoki**: Akceptowane są tylko wiadomości od nadawców znajdujących się na liście znajomych.
6. Kliknij przycisk **OK**.

Modyfikacja filtrów specjalnych

Filtry specjalne można włączać lub wyłączać. Na przykład domyślnie są odfiltrowywane wiadomości zawierające głównie obrazy. Aby otrzymywać takie wiadomości, można wyłączyć ten filtr.

Aby dokonać modyfikacji filtrów specjalnych:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. Wybierz opcję **Opcje filtrowania**.
5. W obszarze **Filtry specjalne** zaznacz lub usuń zaznaczenie dowolnego z następujących pól wyboru:
   - **Odfiltruj wiadomości zawierające ukryty tekst**: Ukryty tekst jest używany w celu uniknięcia wykrycia spamu.
   - **Odfiltruj wiadomości zawierające przede wszystkim obrazy**: Wiadomości zawierające dużą ilość obrazów w większości wypadków są spamem.
   - **Odfiltruj wiadomości zawierające celowe błędy w znacznikach formatowania HTML**: Błędne formatowanie jest stosowane, aby uniemożliwić prawidłowe odfiltrowanie spamu.
   - **Nie odfiltrowuj wiadomości większych niż**: Wiadomości o rozmiarze większym od podanego nie będą filtrowane. Można tu zwiększać lub zmniejszać rozmiar wiadomości (prawidłowy zakres 0–250 KB).
6. Kliknij przycisk **OK**.

Zmiana sposobu przetwarzania wiadomości zidentyfikowanych jako spam

Można zmienić sposób oznaczania i przetwarzania spamu. Na przykład można zmienić nazwę znacznika spamu lub ataku typu „phishing” oraz określić, czy wiadomość ma pozostać w Skrzynce odbiorczej, czy w folderze programu SpamKiller.

Modyfikacja sposobu przetwarzania wiadomości

Można zmienić sposób oznaczania i przetwarzania spamu. Na przykład można zmienić nazwę znacznika spamu lub ataku typu „phishing” oraz określić, czy wiadomość ma pozostać w Skrzynce odbiorczej, czy w folderze programu SpamKiller.

Aby zmodyfikować sposób przetwarzania wiadomości zidentyfikowanych jako spam przez program SpamKiller:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Przetwarzanie**.
5. Wykonaj jedną z poniższych czynności:
   - Kliknij opcję **Oznacz jako spam i przenieś do folderu programu SpamKiller**.

     Jest to ustawienie domyślne. Wiadomości zawierające spam będą przenoszone do folderu programu SpamKiller.
   - Kliknij opcję **Oznacz jako spam i pozostaw w skrzynce odbiorczej**.

     Wiadomości zidentyfikowane jako spam pozostaną w skrzynce odbiorczej.
   - Wpisz niestandardowy znacznik w polu **Dodaj ten dostosowywany znacznik do tematu wiadomości rozpoznanych jako spam**.

     Podany znacznik będzie dodawany do tematu każdej wiadomości e-mail zidentyfikowanej jako spam.
   - Wpisz niestandardowy znacznik w polu **Dodaj ten dostosowywany znacznik do tematu wiadomości wysyłanych w ramach ataku typu „phishing”**.

     Podany znacznik będzie dodawany do tematu każdej wiadomości e-mail zidentyfikowanej jako atak typu „phishing”.
6. Kliknij przycisk **OK**.

Filtrowanie wiadomości zawierających określone zestawy znaków

Zestawy znaków używane są do reprezentacji języka, włączając w to alfabet, liczby i inne symbole. Można odfiltrować wiadomości zawierające określone zestawy znaków. Nie należy jednak odfiltrowywać zestawów znaków dla języków, w których otrzymywane są poprawne wiadomości e-mail.

Na przykład, jeśli chcemy filtrować wiadomości w języku włoskim, ale otrzymujemy ważne wiadomości e-mail w języku angielskim, nie należy wybierać zestawu znaków dla Europy Zachodniej. Wybranie zestawu znaków dla Europy Zachodniej odfiltruje wiadomości w języku włoskim, ale również wiadomości w języku angielskim i we wszystkich językach używających zestawu znaków zachodnioeuropejskich.

Filtrowanie wiadomości zawierających określone zestawy znaków

Można odfiltrować wiadomości zawierające określone zestawy znaków. Nie należy jednak odfiltrowywać zestawów znaków dla języków, w których otrzymywane są poprawne wiadomości e-mail.

Aby odfiltrować wiadomości zawierające określone zestawy znaków:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Zestawy znaków**.
5. Zaznacz pola wyboru obok zestawów znaków przewidzianych do odfiltrowania.
6. Kliknij przycisk **OK**.

Zgłaszanie wiadomości uznanych za spam

Spam można zgłosić firmie McAfee, która przeprowadzi odpowiednie analizy i przygotuje aktualizacje filtrów.

Zgłaszanie wiadomości uznanych za spam

Spam można zgłosić firmie McAfee, która przeprowadzi odpowiednie analizy i przygotuje aktualizacje filtrów.

Aby wysyłać raporty o spamie do firmy McAfee:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Wysyłanie raportów do firmy McAfee**.
5. Zaznacz dowolne z następujących pól wyboru:
   - **Włącz raportowanie po kliknięciu opcji Oznacz jako spam**: Wiadomość będzie zgłaszana firmie McAfee za każdym razem, gdy zostanie oznaczona jako spam.
   - **Włącz raportowanie po kliknięciu opcji Oznacz jako nie-spam**: Wiadomość będzie zgłaszana firmie McAfee za każdym razem, gdy zostanie oznaczona jako nie-spam.
   - **Wyślij całą wiadomość (nie tylko nagłówek)**: Podczas zgłaszania spamu firmie McAfee wysyłana będzie cała wiadomość, a nie tylko jej nagłówek.
6. Kliknij przycisk **OK**.

ROZDZIAŁ 29

Zarządzanie filtrami osobistymi

Filtr definiuje, jakich elementów ma wyszukiwać program SpamKiller w wiadomości e-mail.

Program SpamKiller stosuje wiele filtrów, jednak możliwe jest również tworzenie nowych filtrów lub edycja istniejących, aby bardzo dokładnie zdefiniować, które wiadomości mają być uznawane za spam. Na przykład, jeśli warunek filtrowania zawiera słowo „kredyt”, program SpamKiller wyszukuje wiadomości ze słowem „kredyt”.

Dodając filtry, należy dokładnie sprawdzać wyrażenia, jakie mamy zamiar odfiltrowywać. Jeśli może ono często występować w zwykłych wiadomościach, nie należy go używać do filtrowania.

W tym rozdziale

Omówienie zarządzania filtrami osobistymi 210
Korzystanie z wyrażeń regularnych 213

Omówienie zarządzania filtrami osobistymi

W sekcji tej wyjaśniono, jak zarządzać filtrami osobistymi.

Dodawanie filtrów osobistych

Tworzenie filtrów jest opcjonalne. Dotyczą one wiadomości przychodzących. Nie należy tworzyć filtrów uwzględniających często używane słowa, występujące w wiadomościach, które nie są spamem.

Aby dodać filtr:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Filtry osobiste**.
5. Kliknij przycisk **Dodaj**.
6. Na liście **Element** kliknij pozycję określającą, czy filtr ma szukać słów lub wyrażeń w tematach wiadomości, w treści, w nagłówkach, czy też w nazwach nadawców.
7. Na liście **Warunki** kliknij pozycję określającą, czy filtr ma szukać wiadomości zawierającej, czy nie zawierającej podane słowa lub wyrażenia.
8. W polu **Słowa lub wyrażenia** wpisz, czego należy szukać w wiadomości. Na przykład wpisanie słowa „kredyt” spowoduje odfiltrowanie wszystkich wiadomości zawierających to słowo.
9. Zaznacz pole wyboru **Filtr korzysta z wyrażeń regularnych**, aby zdefiniować wzorce znaków używanych w warunkach filtrowania. Aby sprawdzić dany wzór znaków, kliknij opcję **Testuj**.
10. Kliknij przycisk **OK**.

Edycja filtrów osobistych

Filtr definiuje, jakich elementów ma wyszukiwać program SpamKiller w wiadomości e-mail. Program SpamKiller stosuje wiele filtrów, jednak możliwe jest również tworzenie nowych filtrów lub edycja istniejących, aby bardzo dokładnie zdefiniować, które wiadomości mają być uznawane za spam.

Aby dokonać edycji filtru:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Filtry osobiste**.
5. Wybierz filtr, który ma zostać zmieniony, a następnie kliknij przycisk **Edytuj**.
6. Na liście **Element** kliknij pozycję określającą, czy filtr ma szukać słów lub wyrażeń w tematach wiadomości, w treści, w nagłówkach, czy też w nazwach nadawców.
7. Na liście **Warunki** kliknij pozycję określającą, czy filtr ma szukać wiadomości zawierającej, czy nie zawierającej podane słowa lub wyrażenia.
8. W polu **Słowa lub wyrażenia** wpisz, czego należy szukać w wiadomości. Na przykład wpisanie słowa „kredyt” spowoduje odfiltrowanie wszystkich wiadomości zawierających to słowo.
9. Zaznacz pole wyboru **Filtr korzysta z wyrażeń regularnych**, aby zdefiniować wzorce znaków używanych w warunkach filtrowania. Aby sprawdzić dany wzór znaków, kliknij opcję **Testuj**.
10. Kliknij przycisk **OK**.

Usuwanie filtrów osobistych

Można usuwać filtry, których nie chcemy już dłużej używać. Takie filtry są usuwane na stałe.

Aby usunąć filtr:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Filtry osobiste**.
5. Wybierz filtr, który ma zostać usunięty, a następnie kliknij przycisk **Usuń**.
6. Kliknij przycisk **OK**.

Korzystanie z wyrażeń regularnych

Wyrażenia regularne to znaki specjalne i sekwencje, które mogą być używane do definiowania wyrażeń. Na przykład:

- Wyrażenie regularne **[0-9]*\.[0-9]+**

  Powoduje wyszukanie liczb zmiennoprzecinkowych w zapisie bez wykładnika. Powyższe wyrażenie regularne znajdzie następujące elementy: „12,12”, „.1212” i „12,0”, ale nie „12” i „12”.

- Wyrażenie regularne **\D*[0-9]+\D***

  Powoduje wyszukanie wszystkich słów zawierających cyfry: „SpamKi11er” i „V1AGRA”, ale nie „SpamKiller” i „VIAGRA”.

Korzystanie z wyrażeń regularnych

Wyrażenia regularne to znaki specjalne i sekwencje, które mogą być używane do definiowania wyrażeń.

****

Oznacza następny znak jako znak specjalny lub literał. Na przykład "n" powoduje wyszukanie znaku "n". "\n" powoduje wyszukanie znaku nowego wiersza. Sekwencja "\\" powoduje wyszukanie znaku "\", natomiast "\(" — znaku "(".

^

Oznacza początek ciągu.

$

Oznacza koniec ciągu.

*

Wyszukuje znak poprzedzający powtarzający się zero lub więcej razy. Na przykład "zo*" powoduje wyszukanie "z" lub "zoo".

+

Wyszukuje znak poprzedzający powtarzający się jeden lub więcej razy. Na przykład "zo+" powoduje wyszukanie "zoo", ale nie "z".

?

Wyszukuje znak poprzedzający występujący, powtarzający się zero lub jeden raz. Na przykład "z?gd?" powoduje wyszukanie "gd" w wyrazie "nigdy".

.

Oznacza dowolny jeden znak z wyjątkiem znaku nowego wiersza.

(wzór)

Wyszukuje wzór i zapamiętuje znalezione wystąpienie. Wyszukany podłańcuch można uzyskać z wynikowej kolekcji wyszukanych wystąpień za pomocą numeru [0]...[n]. Aby wyszukać znaki nawiasów ( ), należy użyć wyrażenia "\(" lub "\)".

x|y

Wyszukuje wartość x lub y. Na przykład "s|tama" powoduje wyszukanie "s" lub "tama". "(s|t)ama" powoduje wyszukanie "sama" lub "tama".

{n}

n jest liczbą całkowitą nieujemną. Wyszukuje sekwencję dokładnie n powtórzeń. Na przykład "o{2}" nie powoduje wyszukania "o" w wyrazie "Robert", ale powoduje wyszukanie pierwszych dwóch o w wyrazie "goooool".

{n,}

n jest liczbą całkowitą nieujemną. Wyszukuje sekwencję co najmniej n powtórzeń. Na przykład "o{2,}" nie powoduje wyszukania "o" w wyrazie "Robert", ale powoduje wyszukanie wszystkich o w wyrazie "goooool". Wyrażenie "o{1,}" jest równoważne wyrażeniu "o+". "o{0,}" jest równoważne wyrażeniu "o*".

{n,m}

m oraz n są liczbami całkowitymi nieujemnymi. Wyszukuje sekwencję co najmniej n i maksymalnie m powtórzeń. Na przykład "o{1,3}" powoduje wyszukanie pierwszych trzech o w wyrazie "goooool". Wyrażenie "o{0,1}" jest równoważne wyrażeniu "o?".

[xyz]

Zestaw znaków. Wyszukuje dowolny ze znaków w nawiasie kwadratowym. Na przykład "[abc]" powoduje wyszukanie "a" w wyrazie "jasny".

[^xyz]

Wykluczenie zestawu znaków. Wyszukuje dowolny ze znaków, który nie jest wymieniony w nawiasie. Na przykład "[^abc]" powoduje wyszukanie "p" w wyrazie "paczka".

[a-z]

Zakres znaków. Wyszukuje dowolny ze znaków w określonym zakresie. Na przykład "[a-z]" powoduje wyszukanie dowolnej małej lub dużej litery alfabetu z zakresu od "a" do "z" oraz od "A" do "Z".

[A-Z]

Zakres znaków. Wyszukuje dowolny ze znaków w określonym zakresie. Na przykład "[A-Z]" powoduje wyszukanie dowolnej dużej lub małej litery alfabetu z zakresu od "A" do "Z" oraz od "a" do "z".

[^m-z]

Wykluczenie przedziału znaków. Wyszukuje dowolny ze znaków, który nie znajduje się w określonym przedziale. Na przykład "[^m-z]" powoduje wyszukanie dowolnego znaku, który nie znajduje się w przedziale od "m" do "z".

\b

Wyszukuje granicę słowa, czyli miejsce pomiędzy słowem a spacją. Na przykład "er\b" powoduje wyszukanie "er" w słowie "rower", ale nie powoduje wyszukania "er" w słowie "roweru".

\B

Wyszukuje granicę, która nie jest granicą słowa. "we*r\B" powoduje wyszukanie "wer" w wyrażeniu "nowa wersja".

\d

Wyszukuje cyfrę. Równoważne wyrażeniu [0-9].

\D

Wyszukuje znak inny niż cyfra. Równoważne wyrażeniu [^0-9].

\f

Wyszukuje znak końca strony.

\n

Wyszukuje znak nowego wiersza.

\r

Wyszukuje znak powrotu karetki.

\s

Wyszukuje dowolny odstęp, w tym znak spacji, znak tabulacji, znak końca strony itd. Równoważne wyrażeniu "[\f\n\r\t\v]".

\S

Wyszukuje dowolny znak, który nie jest odstępem. Równoważne "[^ \f\n\r\t\v]".

\t

Wyszukuje znak tabulacji.

\v

Wyszukuje znak tabulatora w pionie.

\w

Wyszukuje dowolny znak alfanumeryczny lub podkreślenie. Równoważne wyrażeniu "[A-Za-z0-9_]".

\W

Wyszukuje dowolny znak, który nie występuje w słowie. Równoważne wyrażeniu "[^A-Za-z0-9_]".

\num

Wyszukuje wartość określoną przez num, gdzie num jest dodatnią liczbą całkowitą. Odwołuje się do zapamiętanych wyników wyszukiwania. Na przykład "(.)\1" powoduje wyszukanie dwóch kolejnych identycznych znaków. \n Wyszukuje znak określony przez wartość n, gdzie n jest liczbą ósemkową. Liczby ósemkowe muszą zawierać 1, 2 lub 3 cyfry. Na przykład zarówno "\11", jak i "\011" oznaczają znak tabulatora. "\0011" jest równoważne wyrażeniu "\001" & "1". Wartości ósemkowe nie mogą być większe niż 256. W przeciwnym razie wyrażenie tworzą tylko dwie pierwsze cyfry. Umożliwia używanie kodów ASCII w wyrażeniach regularnych.

\xn

Wyszukuje znak określony przez wartość n, gdzie n jest liczbą szesnastkową. Liczby szesnastkowe muszą zawierać dokładnie dwie cyfry. Na przykład "\x41" oznacza znak "A". "\x041" jest równoważne wyrażeniu "\x04" & "1". Umożliwia używanie kodów ASCII w wyrażeniach regularnych.

ROZDZIAŁ 30

Obsługa programu SpamKiller

Obsługa programu SpamKiller obejmuje obsługę ochrony przed spamem oraz ustawienia pasków narzędzi.

Obsługując ochronę przed spamem, można włączać lub wyłączać filtrowanie.

Używając pasków narzędzi, można wyłączać lub włączać paski narzędzi poczty e-mail udostępniane przez program SpamKiller oraz oznaczać wiadomości jako spam lub jako nie-spam, korzystając z tych pasków narzędzi.

W tym rozdziale

Zarządzanie ochroną przed spamem 220
Korzystanie z pasków narzędzi 221

Zarządzanie ochroną przed spamem

Filtrowanie wiadomości e-mail można wyłączać i włączać.

Ochronę przed spamem można wyłączyć, aby zapobiec filtrowaniu wiadomości e-mail. Ponowne włączenie ochrony przed spamem zapewnia filtrowanie wiadomości e-mail.

Wyłączanie ochrony przed spamem

Istnieje możliwość wyłączenia ochrony przed spamem, co zapobiega filtrowaniu wiadomości e-mail.

Aby wyłączyć filtrowanie:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W polu **Ochrona przed spamem** kliknij opcję **Wyłączona**.

Włączanie ochrony przed spamem

Można włączyć ochronę przed spamem w celu ponownego filtrowania wiadomości e-mail.

Aby włączyć filtrowanie:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W polu **Ochrona przed spamem** kliknij opcję **Włączona**.

Korzystanie z pasków narzędzi

Można wyłączać lub włączać paski narzędzi do zarządzania wiadomościami e-mail w obsługiwanych aplikacjach klienckich poczty e-mail.

W wypadku korzystania do obsługi poczty e-mail z programów Outlook, Outlook Express, Windows Mail, Eudora lub Thunderbird, można również oznaczać wiadomości jako spam lub nie-spam z poziomu paska zadań programu SpamKiller.

Wyłączanie paska narzędzi

Można wyłączać lub włączać paski narzędzi w obsługiwanych aplikacjach klienckich poczty e-mail.

Aby wyłączyć pasek narzędzi:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Paski narzędzi poczty e-mail** i usuń zaznaczenie pola wyboru obok paska narzędzi, który chcesz wyłączyć.
5. Kliknij przycisk **OK**.

Włączanie paska narzędzi

Każdy wyłączony pasek narzędzi można ponownie włączyć.

Aby włączyć pasek narzędzi:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.
3. W obszarze **Ochrona przed spamem** kliknij przycisk **Zaawansowane**.
4. W okienku Ochrona przed spamem kliknij opcję **Paski narzędzi poczty e-mail** i zaznacz pole wyboru obok paska narzędzi, który chcesz włączyć.
5. Kliknij przycisk **OK**.

Oznaczanie wiadomości jako spam lub nie-spam z poziomu paska narzędzi programu SpamKiller

W wypadku korzystania do obsługi poczty e-mail z programów Outlook, Outlook Express, Windows Mail, Eudora lub Thunderbird, można oznaczać wiadomości jako spam lub nie-spam z poziomu paska zadań programu SpamKiller.

Jeśli oznaczymy wiadomość jako spam, wiadomość otrzyma etykietkę [SPAM] lub inną zdefiniowaną przez użytkownika i pozostanie w Skrzynce odbiorczej, folderze programu SpamKiller (Outlook, Outlook Express, Windows Mail, Thunderbird) lub w folderze Śmieci (Eudora).

Jeśli oznaczymy wiadomość jako nie-spam, etykietka wiadomości zostaje usunięta i wiadomość zostanie przeniesiona do skrzynki odbiorczej.

Aby oznaczać wiadomości jako spam lub nie-spam w programie Outlook:

1. Wybierz wiadomość w programie poczty e-mail.
2. Na pasku narzędzi **SpamKiller** kliknij opcję **Oznacz jako spam** lub **Oznacz jako nie-spam**.

Aby oznaczyć wiadomości jako spam lub nie-spam w programach Outlook Express, Windows Mail, Eudora lub Thunderbird:

1. Wybierz wiadomość w programie poczty e-mail.
2. W menu **SpamKiller** kliknij opcję **Oznacz jako spam** lub **Oznacz jako nie-spam.**

ROZDZIAŁ 31

Konfigurowanie ochrony przed atakami typu „phishing”

Niechciana poczta e-mail jest klasyfikowana jako spam (wiadomości e-mail nakłaniające do zakupów) lub phishing (wiadomości e-mail nakłaniające do podania informacji osobistych fałszywej lub potencjalnie fałszywej witrynie sieci Web).

Filtr Phishing pomaga zapewnić ochronę przed stronami sieci Web, które są potencjalnie fałszywe. W przypadku wykrycia próby przejścia na fałszywą lub potencjalnie fałszywą witrynę sieci Web następuje przekierowanie na stronę filtru Phishing.

Można wyłączyć lub włączyć ochronę przed atakami typu „phishing” lub zmienić opcje filtrowania.

W tym rozdziale

Wyłączanie lub włączanie ochrony przed atakami typu „phishing” 224
Modyfikowanie ustawień filtrowania ataków typu „phishing” 225

Wyłączanie lub włączanie ochrony przed atakami typu „phishing”

Można wyłączyć lub włączyć ochronę przed atakami typu „phishing”. Na przykład można wyłączyć ochronę przed atakami typu „phishing”, aby uzyskać dostęp do zaufanej strony sieci Web, która została zablokowana.

Wyłączanie ochrony przed atakami typu „phishing”

Można wyłączyć ochronę przed atakami typu „phishing”, aby uzyskać dostęp do zaufanej strony sieci Web, która została zablokowana.

Aby wyłączyć ochronę przed atakami typu „phishing”:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Internet i sieć**.
3. W polu **Phishing** kliknij opcję **Wyłączona**.

Włączanie ochrony przed atakami typu „phishing”

Ochronę przed atakami typu „phishing” można ponownie włączyć celem zapewnienia ochrony przed fałszywymi witrynami sieci Web.

Aby włączyć ochronę przed atakami typu „phishing”:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Internet i sieć**.
3. W polu **Phishing** kliknij opcję **Włączona**.

Modyfikowanie ustawień filtrowania ataków typu „phishing”

Program McAfee stosuje dwie metody określania, czy strona sieci Web jest fałszywa czy też nie: poprzez porównywanie wyświetlanej właśnie strony sieci Web z listą stron znanych jako fałszywe lub poprzez próbę sprawdzenia, czy oglądana strona jest fałszywa.

Modyfikowanie ustawień filtrowania ataków typu „phishing”

Program McAfee stosuje dwie metody określania, czy strona sieci Web jest fałszywa czy też nie. W celu zapewnienia pełnej ochrony należy pozostawić włączone obie opcje.

Aby zmienić opcje ochrony przed atakami typu „phishing”:

1. W Menu zaawansowanym kliknij opcję **Konfiguruj**.
2. W okienku konfiguracji kliknij opcję **Internet i sieć**.
3. W polu **Phishing** kliknij przycisk **Zaawansowane**.
4. Zaznacz lub usuń zaznaczenie dowolnego z następujących pól wyboru:
   - **Włącz przeszukiwanie czarnej i białej listy, aby wykrywać fałszywe witryny sieci Web**: Porównuje wyświetlaną stronę sieci Web z listą stron znanych jako fałszywe.
   - **Włącz analizę heurystyczną, aby wykrywać fałszywe witryny sieci Web**: Próbuje rozpoznać, czy oglądana strona sieci Web jest fałszywa.
5. Kliknij przycisk **OK**.

ROZDZIAŁ 32

Dodatkowa pomoc

W tym rozdziale omówiono często zadawane pytania.

W tym rozdziale

Często zadawane pytania 228

Często zadawane pytania

Ten rozdział zawiera odpowiedzi na najczęściej zadawane pytania.

Co to są konta POP3, MSN/Hotmail oraz MAPI?

Program SpamKiller został zaprojektowany do pracy z następującymi rodzajami kont poczty e-mail: POP3, internetowa poczta POP3, MSN/Hotmail oraz MAPI. Występują pomiędzy nimi pewne różnice, które wpływają na sposób filtrowania w programie SpamKiller.

POP3

Jest to najbardziej popularny typ konta i jest to standard internetowej poczty e-mail. W wypadku konta POP3 program SpamKiller łączy się bezpośrednio z serwerem i filtruje wiadomości, zanim zostaną one pobrane przez program do obsługi poczty e-mail.

POP3 Web Mail

Konta internetowej poczty POP3 są kontami w sieci Web. Filtrowanie kont internetowej poczty POP3 jest podobne do filtrowania kont POP3.

MSN/Hotmail

Konta MSN/Hotmail są kontami w sieci Web. Filtrowanie kont MSN/Hotmail jest podobne do filtrowania kont POP3.

MAPI

MAPI jest systemem zaprojektowanym przez firmę Microsoft, który obsługuje wiele typów komunikacji obejmujących internetową pocztę e-mail, faksowanie oraz przesyłanie wiadomości z użyciem serwera Exchange. Z tego powodu interfejs MAPI jest często używany w środowiskach korporacyjnych, w których działa serwer Microsoft Exchange. Jednak wiele osób korzysta z programu Microsoft Outlook do obsługi prywatnej poczty e-mail. Program SpamKiller ma dostęp do kont MAPI, ale z następującymi ograniczeniami:

- Filtrowanie nie jest zwykle przeprowadzane przed pobraniem wiadomości przez program obsługi poczty e-mail.
- Program SpamKiller filtruje tylko domyślną skrzynkę odbiorczą i wiadomości internetowej poczty e-mail.

Co to jest filtr ataków typu „phishing”?

Niechciana poczta e-mail jest klasyfikowana jako spam (wiadomości e-mail nakłaniające do zakupów) lub phishing (wiadomości e-mail nakłaniające do podania informacji osobistych fałszywej lub potencjalnie fałszywej witrynie sieci Web).

Filtr Phishing zabezpiecza użytkownika przed witrynami sieci Web znajdującymi się na czarnej liście (witrynami sieci Web, które są źródłami ataków typu „phishing”, lub podobnymi fałszywymi witrynami) lub na szarej liście (witryn zawierających niebezpieczną treść lub łącza do witryn sieci Web na czarnej liście).

W przypadku wykrycia próby przejścia na fałszywą lub potencjalnie fałszywą witrynę sieci Web następuje przekierowanie na stronę filtru Phishing.

Dlaczego firma McAfee używa plików cookie?

Firma McAfee korzysta ze specjalnych znaczników programowych, nazywanych „plikami cookie”, które umożliwiają rozpoznawanie klientów podczas ich kolejnych odwiedzin w witrynie firmy. Pliki cookie to bloki tekstu umieszczone w plikach przechowywanych na dysku twardym komputera użytkownika. Służą one do identyfikowania użytkowników, gdy po raz kolejny łączą się z witryną.

Firma McAfee używa plików cookie do:

- zarządzania uprawnieniami subskrypcji użytkownika;
- identyfikowania użytkownika jako powtórnie odwiedzającego witrynę, aby uniknąć ponawiania rejestracji przy każdej wizycie;
- lepszego zrozumienia preferencji nabywczych użytkownika i dostosowania usług do jego potrzeb;
- prezentowania informacji, produktów i ofert specjalnych, które mogą zainteresować użytkownika.

Firma McAfee prosi również użytkownika o podanie imienia, co pozwala na nawiązanie bardziej indywidualnej relacji podczas przeglądania witryny.

Firma McAfee nie realizuje usług subskrypcji dla użytkowników korzystających z przeglądarek skonfigurowanych do odrzucania plików cookie. Informacje zgromadzone przez firmę McAfee nie są sprzedawane, wypożyczane ani udostępniane żadnym podmiotom zewnętrznym.

Firma McAfee zezwala reklamodawcom na umieszczanie plików cookie w przeglądarkach osób odwiedzających jej witrynę. Firma McAfee nie ma dostępu do informacji zawartych w plikach cookie reklamodawców.

ROZDZIAŁ 33

McAfee Privacy Service

Program Privacy Service zapewnia zaawansowaną ochronę użytkownika, całej rodziny, informacji osobistych i komputera. Zapewnia ochronę przed kradzieżą tożsamości, blokuje przesyłanie informacji osobistych umożliwiających identyfikację użytkownika i filtruje potencjalnie obraźliwą zawartość online (w tym obrazy, reklamy, wyskakujące okna i pluskwy internetowe). Oferuje także zaawansowane funkcje ochrony rodzicielskiej, które pozwalają monitorować, kontrolować i rejestrować zachowania dzieci podczas przeglądania sieci Web, a także jest bezpiecznym miejscem przechowywania haseł.

Przed rozpoczęciem korzystania z programu Privacy Service można zapoznać się z jego niektórymi najczęściej używanymi funkcjami. Szczegółowe informacje na temat konfigurowania tych funkcji i korzystania z nich zamieszczono w pomocy programu Privacy Service.

W tym rozdziale

Funkcje....232
Konfigurowanie ochrony rodzicielskiej....233
Ochrona informacji w Internecie....255
Ochrona haseł....259

Funkcje

Program Privacy Service udostępnia następujące funkcje:

- ochronę przeglądania sieci Web,
- ochronę informacji osobistych,
- kontrolę rodzicielską,
- przechowywanie haseł.

Ochrona przeglądania sieci Web

Ochrona przeglądania sieci Web umożliwia blokowanie na komputerze reklam, wyskakujących okien i pluskiew internetowych. Funkcja blokowania reklam i wyskakujących okien zapobiega wyświetlaniu w przeglądarce internetowej większości reklam i wyskakujących okien. Funkcja blokowania pluskiew internetowych uniemożliwia śledzenie przez witryny sieci Web czynności wykonywanych online i przesyłanie informacji do nieupoważnionych źródeł. Kompleksowe blokowanie reklam, wyskakujących okien i pluskiew internetowych poprawia bezpieczeństwo i zapobiega zakłócaniu przeglądania sieci Web przez niechciane zawartości.

Ochrona informacji osobistych

Ochrona informacji osobistych umożliwia blokowanie wysyłania poufnych lub tajnych informacji (na przykład numerów kart kredytowych, numerów rachunków bankowych, adresów itp.) przez Internet.

Kontrola rodzicielska

Kontrola rodzicielska umożliwia skonfigurowanie ocen zawartości, które ograniczają możliwość dostępu do witryn sieci Web i zawartości, która może być wyświetlana przez użytkownika, a także umożliwia ustawienie limitów czasu Internetu, określających okres i czas w ciągu którego użytkownik ma dostęp do Internetu. Kontrola rodzicielska umożliwia ograniczenie dostępu do określonych witryn sieci Web oraz umożliwia lub blokuje dostęp w oparciu o grupy wiekowe i słowa kluczowe.

Przechowywanie haseł

Magazyn haseł jest bezpiecznym miejscem przechowywania haseł osobistych. Umożliwia on przechowywanie haseł ze świadomością, że nikt inny (nawet administrator firmy McAfee lub administrator systemu) nie ma do nich dostępu.

ROZDZIAŁ 34

Konfigurowanie ochrony rodzicielskiej

Po dodaniu użytkownika można skonfigurować dla niego funkcję ochrony rodzicielskiej. Funkcja ochrony rodzicielskiej to ustawienia definiujące grupę klasyfikacji zawartości użytkownika, poziom blokowania plików cookie i ograniczenia czasu dostępu do Internetu. Grupa klasyfikacji zawartości określa, jakiego rodzaju zawartość internetowa i witryny sieci Web będą dostępne dla użytkownika (w zależności od grupy wiekowej, do jakiej należy). Poziom blokowania plików cookie określa, czy witryny sieci Web mogą odczytywać pliki cookie ustawione przez nie na komputerze w czasie, gdy zalogowany jest dany użytkownik. Ograniczenia czasu dostępu do Internetu określają, w jakich dniach i godzinach użytkownik może korzystać z Internetu.

Można także skonfigurować globalną ochronę rodzicielską, która będzie miała zastosowanie do wszystkich użytkowników innych niż dorośli. Można na przykład zablokować lub zezwolić na dostęp do określonych witryn sieci Web bądź zablokować wyświetlanie potencjalnie niepożądanych obrazów w czasie, gdy Internet przeglądają użytkownicy inni niż dorośli. Możliwe jest również skonfigurowanie globalnych ustawień blokowania plików cookie dla wszystkich użytkowników. Jeśli jednak poziom blokowania plików cookie określonego użytkownika różni się od globalnych ustawień blokowania plików cookie, pierwszeństwo mają ustawienia globalne.

Uwaga: Do skonfigurowania funkcji ochrony rodzicielskiej wymagane są uprawnienia Administratora.

W tym rozdziale

Konfigurowanie grupy klasyfikacji zawartości użytkownika 234
Ustawianie poziomu blokowania plików cookie użytkownika 236
Ustawianie internetowych limitów czasu użytkownika 244
Blokowanie witryn sieci Web 245
Dozwolone witryny sieci Web 249
Zezwalanie witrynom sieci Web na zapisywanie plików cookie 251
Blokowanie potencjalnie niepożądanych obrazów w sieci Web 253

Konfigurowanie grupy klasyfikacji zawartości użytkownika

Użytkownik może należeć do jednej z następujących grup klasyfikacji zawartości:

- Małe dziecko
- Dziecko
- Młodszy nastolatek
- Starszy nastolatek
- Dorosły

Zawartość jest klasyfikowana (to znaczy udostępniana lub blokowana) w zależności od grupy, do której należy dany użytkownik. Na przykład określone witryny sieci Web mogą być blokowane dla użytkowników należących do grupy małych dzieci, ale dostępne dla użytkowników z grupy starszych nastolatków. Użytkownicy z grupy dorosłych mają dostęp do każdej zawartości. Nowi użytkownicy są domyślnie dodawani do grupy małych dzieci i podlegają wszystkim ograniczeniom dostępności zawartości.

Jako Administrator użytkownik może ustawić grupę klasyfikacji zawartości użytkownika, a następnie zablokować lub zezwolić na dostęp do witryn sieci Web na podstawie tych grup. Aby w przypadku określonego użytkownika sklasyfikować zawartość bardziej restrykcyjnie, można zapobiec przeglądaniu przez niego dowolnych witryn sieci Web, które nie znajdują się na globalnej liście **Dozwolone witryny sieci Web**. Aby uzyskać więcej informacji, zobacz: Blokowanie witryn sieci Web w oparciu o słowa kluczowe (strona 248) i Dozwolone witryny sieci Web (strona 249).

Ustawianie grupy klasyfikacji zawartości użytkownika

Grupa klasyfikacji zawartości użytkownika to grupy wiekowa, która określa, jakiego rodzaju zawartość internetowa i witryny sieci Web będą dostępne dla użytkownika.

Aby ustawić grupę klasyfikacji zawartości użytkownika:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W okienku konfiguracji programu SecurityCenter kliknij opcję **Zaawansowane** w obszarze **Użytkownicy**.
4. W okienku Użytkownicy kliknij opcję **Funkcje ochrony rodzicielskiej**.
5. Zaznacz nazwę użytkownika na liście.
6. W obszarze **Klasyfikacja zawartości** kliknij grupę wiekową, którą chcesz przypisać do użytkownika.
   Następnie możesz sklasyfikować w zależności od grupy wiekowej, co umożliwia blokowanie wyświetlania zawartości, która jest nieodpowiednia dla określonego wielu lub poziomu dojrzałości.
7. Aby zapobiec przeglądaniu przez użytkownika witryn sieci Web, które nie znajdują się na globalnej liście **Dozwolone witryny sieci Web**, zaznacz pole wyboru **Ogranicz dostęp tego użytkownika do witryn z listy „Dozwolone witryny sieci Web”**.
8. Kliknij przycisk **OK**.

Ustawianie poziomu blokowania plików cookie użytkownika

Niektóre witryny sieci Web monitorują indywidualne preferencje i zachowania osób je odwiedzających za pomocą małych plików, tzw. plików *cookie*, zapisywanych na komputerze użytkownika. Administrator może przypisać użytkownikowi jeden z następujących poziomów blokowania plików cookie:

- Akceptuj wszystkie pliki cookie
- Odrzucaj wszystkie pliki cookie
- Monituj użytkownika o zaakceptowanie plików cookie

Ustawienie akceptowania wszystkich plików cookie umożliwia witrynom sieci Web odczytywanie plików cookie zapisanych w komputerze, gdy dany użytkownik jest zalogowany. Ustawienie odrzucania wszystkich plików cookie uniemożliwia witrynom sieci Web odczytywanie plików cookie. Ustawienia monitowania użytkownika o zaakceptowanie plików cookie monituje użytkownika za każdym razem, gdy witryna sieci Web stara się zapisać plik cookie w komputerze. Użytkownik może w każdym takim przypadku zdecydować, czy zezwolić na zapisanie pliku cookie. Po podjęciu decyzji zaakceptowania lub odrzucenia pliku cookie określonej witryny sieci Web, użytkownik nie jest ponownie monitowany podczas przeglądania tej witryny.

Uwaga: Niektóre witryny sieci Web do prawidłowego działania wymagają włączenia obsługi plików cookie.

Ustawianie poziomu blokowania plików cookie użytkownika

Niektóre witryny sieci Web monitorują indywidualne preferencje i zachowania osób je odwiedzających za pomocą małych plików, tzw. plików *cookie*, zapisywanych na komputerze użytkownika. Dla każdego użytkownika komputera można określić sposób obsługi plików cookie.

Aby ustawić poziom blokowania plików cookie użytkownika:

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W okienku Konfiguracja programu SecurityCenter kliknij opcję **Zaawansowane** w obszarze **Użytkownicy**.
4. W okienku Użytkownicy kliknij kategorię **Funkcje ochrony rodzicielskiej**.
5. Wybierz z listy nazwę użytkownika.
6. W obszarze **Blokowanie plików cookie** kliknij jedną z następujących opcji:
   - **Akceptuj wszystkie pliki cookie:** Wszystkie witryny sieci Web mogą odczytywać pliki cookie zapisane w tym komputerze.
   - **Odrzucaj wszystkie pliki cookie:** Żadna witryna sieci Web nie może odczytywać plików cookie zapisanych w tym komputerze.
   - **Monituj użytkownika o zaakceptowanie plików cookie:** Gdy użytkownik próbuje wyświetlić stronę sieci Web, zostaje wyświetlony komunikat monitujący o zaakceptowanie lub odrzucenie pliku cookie.
7. Kliknij przycisk **OK**.

Dodawanie witryny sieci Web do listy akceptowanych plików cookie użytkownika

Jeśli poziom blokowania plików cookie ustawiony dla użytkownika określa, że jest on monitowany o zezwolenie witrynom sieci Web na ustawienie plików cookie, ale pliki cookie z pewnych witryn sieci Web mają być akceptowane bez monitowania, należy dodać te witryny do listy akceptowanych plików cookie użytkownika.

Aby dodać witrynę sieci Web do listy akceptowanych plików cookie użytkownika:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W okienku konfiguracji programu SecurityCenter kliknij opcję **Zaawansowane** w obszarze **Użytkownicy**.
4. W okienku Użytkownicy kliknij opcję **Funkcje ochrony rodzicielskiej**.
5. Zaznacz nazwę użytkownika na liście.
6. W obszarze **Blokowanie plików cookie** kliknij przycisk **Wyświetl listę**.
7. W obszarze **Witryny sieci Web z akceptacją plików cookie**, w polu **http://** wpisz adres witryny sieci Web, a następnie kliknij przycisk **Dodaj**.
8. Kliknij przycisk **Gotowe**.

Modyfikowanie witryny sieci Web na liście akceptowanych plików cookie użytkownika

Jeśli adres witryny sieci Web uległ zmianie lub został wprowadzony nieprawidłowo w czasie dodawania do listy akceptowanych plików cookie użytkownika, można go zmodyfikować.

Aby zmodyfikować witrynę sieci Web na liście akceptowanych plików cookie użytkownika:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W okienku konfiguracji programu SecurityCenter kliknij opcję **Zaawansowane** w obszarze **Użytkownicy**.
4. W okienku Użytkownicy kliknij opcję **Funkcje ochrony rodzicielskiej**.
5. Zaznacz nazwę użytkownika na liście.
6. W obszarze **Blokowanie plików cookie** kliknij przycisk **Wyświetl listę**.
7. W obszarze **Witryny sieci Web z akceptacją plików cookie** kliknij pozycję na liście **Witryny sieci Web**, zmodyfikuj adres witryny sieci Web w polu **http://**, a następnie kliknij przycisk **Aktualizuj**.
8. Kliknij przycisk **Gotowe**.

Usuwanie witryny sieci Web z listy akceptowanych plików cookie użytkownika

Jeśli witryna sieci Web została dodana do listy akceptowanych plików cookie użytkownika przez pomyłkę, można ją usunąć.

Aby usunąć witrynę sieci Web z listy akceptowanych plików cookie użytkownika:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W okienku konfiguracji programu SecurityCenter kliknij opcję **Zaawansowane** w obszarze **Użytkownicy**.
4. W okienku Użytkownicy kliknij opcję **Funkcje ochrony rodzicielskiej**.
5. Zaznacz nazwę użytkownika na liście.
6. W obszarze **Blokowanie plików cookie** kliknij przycisk **Wyświetl listę**.
7. W obszarze **Witryny sieci Web z akceptacją plików cookie** kliknij pozycję na liście **Witryny sieci Web**, a następnie kliknij przycisk **Usuń**.
8. W oknie dialogowym Potwierdzenie usunięcia kliknij przycisk **Tak**.
9. Kliknij przycisk **Gotowe**.

Dodawanie witryny sieci Web do listy odrzucanych plików cookie użytkownika

Jeśli poziom blokowania plików cookie ustawiony dla użytkownika określa, że jest on monitowany o zezwolenie witrynom sieci Web na ustawienie plików cookie, ale pliki cookie z pewnych witryn sieci Web mają być odrzucane mieć bez monitowania, należy dodać te witryny do listy odrzucanych plików cookie użytkownika.

Aby dodać witrynę sieci Web do listy odrzucanych plików cookie użytkownika:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W okienku konfiguracji programu SecurityCenter kliknij opcję **Zaawansowane** w obszarze **Użytkownicy**.
4. W okienku Użytkownicy kliknij opcję **Funkcje ochrony rodzicielskiej**.
5. Zaznacz nazwę użytkownika na liście.
6. W obszarze **Blokowanie plików cookie** kliknij przycisk **Wyświetl listę**.
7. Kliknij opcję **Witryny sieci Web z odrzucaniem plików cookie**.
8. W obszarze **Witryny sieci Web z odrzucaniem plików cookie**, w polu **http://** wpisz adres witryny sieci Web, a następnie kliknij przycisk **Dodaj**.
9. Kliknij przycisk **Gotowe**.

Modyfikowanie witryny sieci Web na liście odrzucanych plików cookie użytkownika

Jeśli adres witryny sieci Web uległ zmianie lub został wprowadzony nieprawidłowo w czasie dodawania do listy odrzucanych plików cookie użytkownika, można go zmodyfikować.

Aby zmodyfikować witrynę sieci Web na liście odrzucanych plików cookie użytkownika:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W okienku konfiguracji programu SecurityCenter kliknij opcję **Zaawansowane** w obszarze **Użytkownicy**.
4. W okienku Użytkownicy kliknij opcję **Funkcje ochrony rodzicielskiej**.
5. Zaznacz nazwę użytkownika na liście.
6. W obszarze **Blokowanie plików cookie** kliknij przycisk **Wyświetl listę**.
7. Kliknij opcję **Witryny sieci Web z odrzucaniem plików cookie**.
8. W obszarze **Witryny sieci Web z odrzucaniem plików cookie** kliknij pozycję na liście **Witryny sieci Web**, zmodyfikuj adres witryny sieci Web w polu **http://**, a następnie kliknij przycisk **Aktualizuj**.
9. Kliknij przycisk **Gotowe**.

Usuwanie witryny sieci Web z listy odrzucanych plików cookie użytkownika

Jeśli witryna sieci Web została dodana do listy odrzucanych plików cookie użytkownika przez pomyłkę, można ją usunąć.

Aby usunąć witrynę sieci Web z listy odrzucanych plików cookie użytkownika:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W okienku konfiguracji programu SecurityCenter kliknij opcję **Zaawansowane** w obszarze **Użytkownicy**.
4. W okienku Użytkownicy kliknij opcję **Funkcje ochrony rodzicielskiej**.
5. Zaznacz nazwę użytkownika na liście.
6. W obszarze **Blokowanie plików cookie** kliknij przycisk **Wyświetl listę**.
7. Kliknij opcję **Witryny sieci Web z odrzucaniem plików cookie**.
8. W obszarze **Witryny sieci Web z odrzucaniem plików cookie** kliknij pozycję na liście **Witryny sieci Web**, a następnie kliknij przycisk **Usuń**.
9. W oknie dialogowym Potwierdzenie usunięcia kliknij przycisk **Tak**.
10. Kliknij przycisk **Gotowe**.

Ustawianie internetowych limitów czasu użytkownika

Administrator może skorzystać z siatki internetowych limitów czasu do określenia, czy i kiedy użytkownik może uzyskać dostęp do Internetu. Można przyznać użytkownikowi nieograniczony lub ograniczony dostęp do Internetu, a także całkowicie go zablokować.

Siatka internetowych limitów czasu umożliwia określanie limitów czasu w odstępach trzydziestominutowych. Zielone części siatki oznaczają dni i godziny, w których użytkownik ma dostęp do Internetu. Czerwone części siatki oznaczają dni i godziny, w których dostęp jest zabroniony. Jeśli użytkownik podejmie próbę uzyskania dostępu do Internetu w zabronionym okresie, oprogramowanie McAfee wyświetli powiadomienie o ograniczeniu.

Jeśli dostęp do Internetu jest całkowicie zabroniony, użytkownik może się zalogować i korzystać z komputera, ale nie może korzystać z Internetu.

Ustawianie limitów czasowych użytkownika

Za pomocą siatki ograniczeń czasu dostępu do Internetu można określić, w jakich godzinach wybrany użytkownik ma dostęp do Internetu. Zielone fragmenty siatki oznaczają dni i godziny, w których użytkownik może korzystać z Internetu. Czerwone fragmenty oznaczają dni i godziny, w których użytkownik nie ma dostępu do Internetu.

Aby ustawić ograniczenia czasu dostępu do Internetu:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W okienku konfiguracji programu SecurityCenter kliknij opcję **Zaawansowane** w obszarze **Użytkownicy**.
4. W okienku Użytkownicy kliknij opcję **Funkcje ochrony rodzicielskiej**.
5. Zaznacz nazwę użytkownika na liście.
6. W obszarze **Ograniczenia czasu dostępu do Internetu** kliknij i przeciągnij myszą, aby określić dni i godziny, kiedy ten użytkownik może korzystać z Internetu.
7. Kliknij przycisk **OK**.

Blokowanie witryn sieci Web

Jeśli administrator chce uniemożliwić wszystkim niepełnoletnim użytkownikom dostęp do konkretnej witryny sieci Web, może ją zablokować. Gdy użytkownik próbuje uzyskać dostęp do zablokowanej witryny sieci Web, wyświetlony zostaje komunikat informujący o braku możliwości uzyskania dostępu do witryny z powodu zablokowania jej przez program McAfee.

Użytkownicy (w tym administratorzy) należący do grupy dorosłych użytkowników mają dostęp do wszystkich witryn sieci Web, nawet jeśli znajdują się one na liście **Blokowane witryny sieci Web**. Aby przetestować blokowanie witryn sieci Web, należy zalogować się jako inny użytkownik niż osoba dorosła.

Administrator może również blokować witryny sieci Web na podstawie słów kluczowych, które te witryny zawierają. Program McAfee przechowuje domyślną listę słów kluczowych i odpowiadających im reguł, które określają, czy użytkownik z danej grupy wiekowej może oglądać witrynę sieci Web, w której występuje określone słowo kluczowe, czy też nie. Jeśli włączono skanowanie według słów kluczowych, do oceny zawartości witryny używana jest domyślna lista słów kluczowych. Jednak można dodać własne dozwolone słowa kluczowe do domyślnej listy i przypisać je do konkretnych grup wiekowych. Dodawane reguły dotyczące słów kluczowych zastępują reguły, które mogą być przypisane do odpowiednich słów kluczowych znajdujących się na domyślnej liście. Użytkownik może sprawdzać istniejące słowa kluczowe lub określać nowe słowa, które zostaną powiązane z określonymi grupami wiekowymi.

Blokowanie witryny sieci Web

Blokowanie witryny sieci Web ma na celu uniemożliwienie wszystkim użytkownikom innym niż dorośli uzyskanie dostępu do niej. Próba uzyskania dostępu do witryny powoduje wyświetlenie komunikatu informującego o zablokowaniu witryny przez produkt firmy McAfee.

Aby zablokować witrynę sieci Web:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Funkcje ochrony rodzicielskiej**.
3. W sekcji informacji o funkcjach ochrony rodzicielskiej kliknij polecenie **Konfiguruj**.
4. W okienku konfiguracji funkcji ochrony rodzicielskiej należy upewnić się, że funkcje ochrony rodzicielskiej są włączone, a następnie kliknąć przycisk **Zaawansowane**.
5. W okienku Blokowane witryny sieci Web, w polu **http://** wpisz adres witryny sieci Web, a następnie kliknij przycisk **Dodaj**.
6. Kliknij przycisk **OK**.

Modyfikowanie blokowanej witryny sieci Web

Jeśli adres witryny sieci Web uległ zmianie lub został wprowadzony nieprawidłowo w czasie dodawania do listy Blokowane witryny sieci Web, można go zmodyfikować.

Aby zmodyfikować blokowaną witrynę sieci Web:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Funkcje ochrony rodzicielskiej**.
3. W sekcji informacji o funkcjach ochrony rodzicielskiej kliknij polecenie **Konfiguruj**.
4. W okienku konfiguracji funkcji ochrony rodzicielskiej kliknij opcję **Zaawansowane**.
5. W obszarze Blokowane witryny sieci Web kliknij pozycję na liście **Blokowane witryny sieci Web**, zmodyfikuj adres witryny sieci Web w polu **http://**, a następnie kliknij przycisk **Aktualizuj**.
6. Kliknij przycisk **OK**.

Usuwanie blokowanej witryny sieci Web

Jeśli witryna sieci Web nie ma być już blokowana, należy usunąć ją z listy **Blokowane witryny sieci Web**.

Aby usunąć blokowaną witrynę sieci Web:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Funkcje ochrony rodzicielskiej**.
3. W sekcji informacji o funkcjach ochrony rodzicielskiej kliknij polecenie **Konfiguruj**.
4. W okienku konfiguracji funkcji ochrony rodzicielskiej kliknij opcję **Zaawansowane**.
5. W obszarze Blokowane witryny sieci Web kliknij pozycję na liście **Blokowane witryny sieci Web**, a następnie kliknij przycisk **Usuń**.
6. W oknie dialogowym Potwierdzenie usunięcia kliknij przycisk **Tak**.
7. Kliknij przycisk **OK**.

Wyłączanie skanowania według słów kluczowych

Domyślnie skanowanie według słów kluczowych jest włączone, co oznacza, że do oceny zawartości wyświetlanej witryny używana jest domyślna lista słów kluczowych programu McAfee. Choć firma McAfee nie zaleca takiego postępowania, skanowanie według słów kluczowych można wyłączyć w dowolnej chwili.

Aby wyłączyć skanowanie według słów kluczowych:

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij kategorię **Funkcje ochrony rodzicielskiej**.
3. W sekcji informacji kategorii Funkcje ochrony rodzicielskiej kliknij pozycję **Konfiguruj**.
4. W okienku Konfiguracja kategorii Funkcje ochrony rodzicielskiej kliknij opcję **Zaawansowane**.
5. W okienku Globalna kontrola rodzicielska kliknij opcję **Skanowanie według słów kluczowych**.
6. W okienku Skanowanie według słów kluczowych kliknij opcję **Wyłącz**.
7. Kliknij przycisk **OK**.

Blokowanie witryn sieci Web w oparciu o słowa kluczowe

Aby blokować na podstawie zawartości witryny sieci Web, których konkretne adresy nie są znane, można zastosować blokowanie na podstawie ich słów kluczowych. Wystarczy wpisać słowo kluczowe, a następnie określić, które grupy wiekowe użytkowników nie powinny mieć możliwości wyświetlania witryn zawierających te słowo kluczowe.

Aby blokować witryny sieci Web w oparciu o słowa kluczowe:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Funkcje ochrony rodzicielskiej**.
3. W sekcji informacji o funkcjach ochrony rodzicielskiej kliknij polecenie **Konfiguruj**.
4. W okienku konfiguracji funkcji ochrony rodzicielskiej kliknij opcję **Zaawansowane**.
5. W okienku globalnej ochrony rodzicielskiej kliknij opcję **Skanowanie według słów kluczowych** i upewnij się, że jest włączona.
6. W okienku globalnej ochrony rodzicielskiej kliknij opcję **Słowa kluczowe**.
7. Wpisz słowo kluczowe w polu **Szukaj**.
   Witryny zawierające to słowo kluczowe będą blokowane.
8. Przesuń suwak **Minimalny wiek**, aby określić najniższą grupę wiekową.
   Użytkownicy z tej grupy wiekowej i grup wyższych będą mogli wyświetlać witryny zawierające dane słowo kluczowe.
9. Kliknij przycisk **OK**.

Dozwolone witryny sieci Web

Administrator może pozwolić wszystkim użytkownikom na dostęp do konkretnej witryny sieci Web, zastępując domyślne ustawienia i blokowane witryny sieci Web.

Informacje o blokowanych witrynach sieci Web zawiera sekcja Blokowanie witryn sieci Web (strona 245).

Zezwalanie na korzystanie z danej witryny sieci Web

Aby dana witryna sieci Web nie była blokowana dla żadnego użytkownika, należy dodać jej adres do listy **Dozwolone witryny sieci Web**. Podczas dodawania witryny sieci Web do listy **Dozwolone witryny sieci Web** zastępowane są wszystkie domyślne ustawienia i witryny sieci Web dodane do listy **Blokowane witryny sieci Web**.

Aby zezwolić na korzystanie z witryny sieci Web:

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij kategorię **Funkcje ochrony rodzicielskiej**.
3. W sekcji informacji kategorii Funkcje ochrony rodzicielskiej kliknij pozycję **Konfiguruj**.
4. W okienku Konfiguracja kategorii Funkcje ochrony rodzicielskiej kliknij opcję **Zaawansowane**.
5. W okienku Globalna kontrola rodzicielska kliknij opcję **Dozwolone witryny sieci Web**.
6. W okienku Dozwolone witryny sieci Web wpisz adres witryny sieci Web w polu **http://**, a następnie kliknij przycisk **Dodaj**.
7. Kliknij przycisk **OK**.

Wskazówka: Można uniemożliwić użytkownikowi przeglądanie wszystkich witryn sieci Web, których nie ma na liście **Dozwolone witryny sieci Web**. Więcej informacji zawiera sekcja Ustawianie grupy klasyfikacji zawartości użytkownika (strona 234).

Modyfikowanie dozwolonej witryny sieci Web

Jeśli adres witryny sieci Web uległ zmianie lub został wprowadzony nieprawidłowo w czasie dodawania do listy **Dozwolone witryny sieci Web**, można go zmodyfikować.

Aby zmodyfikować dozwoloną witrynę sieci Web:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Funkcje ochrony rodzicielskiej**.
3. W sekcji informacji o funkcjach ochrony rodzicielskiej kliknij polecenie **Konfiguruj**.
4. W okienku konfiguracji funkcji ochrony rodzicielskiej kliknij opcję **Zaawansowane**.
5. W okienku globalnej ochrony rodzicielskiej kliknij opcję **Dozwolone witryny sieci Web**.
6. W obszarze Dozwolone witryny sieci Web kliknij pozycję na liście **Dozwolone witryny sieci Web**, zmodyfikuj adres w polu **http://**, a następnie kliknij przycisk **Aktualizuj**.
7. Kliknij przycisk **OK**.

Usuwanie dozwolonej witryny sieci Web

Dozwoloną witrynę sieci Web można usunąć w dowolnym momencie. W zależności od ustawień, usunięcie witryny sieci Wen z listy **Dozwolone witryny sieci Web** może sprawić, że użytkownicy produktu firmy McAfee nie będą mieli do niej dostępu .

Aby usunąć dozwoloną witrynę sieci Web:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Funkcje ochrony rodzicielskiej**.
3. W sekcji informacji o funkcjach ochrony rodzicielskiej kliknij polecenie **Konfiguruj**.
4. W okienku konfiguracji funkcji ochrony rodzicielskiej kliknij opcję **Zaawansowane**.
5. W okienku globalnej ochrony rodzicielskiej kliknij opcję **Dozwolone witryny sieci Web**.
6. W obszarze Dozwolone witryny sieci Web kliknij pozycję na liście **Dozwolone witryny sieci Web**, a następnie kliknij przycisk **Usuń**.
7. W oknie dialogowym Potwierdzenie usunięcia kliknij przycisk **Tak**.
8. Kliknij przycisk **OK**.

Zezwalanie witrynom sieci Web na zapisywanie plików cookie

Po zablokowaniu dla wszystkich witryn sieci Web odczytu plików cookie zapisanych na danym komputerze lub skonfigurowaniu ustawień niektórych użytkowników tak, aby przed zaakceptowaniem pliku cookie wyświetlany był komunikat, a następnie stwierdzeniu, że określone witryny sieci Web nie działają prawidłowo, można zezwolić, aby te witryny odczytywały pliki cookie.

Więcej informacji o plikach cookie i poziomach ich blokowania zawiera sekcja Ustawianie poziomu blokowania plików cookie użytkownika (strona 236).

Zezwalanie witrynie sieci Web na ustawianie plików cookie

Jeśli po włączeniu blokowania odczytywania przez wszystkie witryny sieci Web plików cookie ustawionych przez nie na komputerze lub monitowania określonych użytkowników o zaakceptowanie plików cookie okazało się, że pewne witryny sieci Web nie działają poprawnie, można zezwolić im na odczytywanie swoich plików cookie.

Aby zezwolić witrynie sieci Web na ustawianie plików cookie:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Funkcje ochrony rodzicielskiej**.
3. W sekcji informacji o funkcjach ochrony rodzicielskiej kliknij polecenie **Konfiguruj**.
4. W okienku konfiguracji funkcji ochrony rodzicielskiej kliknij opcję **Zaawansowane**.
5. W okienku globalnej ochrony rodzicielskiej kliknij opcję **Pliki cookie**.
6. W okienku Pliki cookie, w polu **http://** wpisz adres witryny sieci Web, a następnie kliknij przycisk **Dodaj**.
7. Kliknij przycisk **OK**.

Modyfikowanie listy akceptowanych plików cookie

Jeśli adres witryny sieci Web uległ zmianie lub został wprowadzony nieprawidłowo w czasie dodawania do listy **Akceptuj pliki cookie**, można go zmodyfikować.

Aby zmodyfikować listę plików cookie:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Funkcje ochrony rodzicielskiej**.
3. W sekcji informacji o funkcjach ochrony rodzicielskiej kliknij polecenie **Konfiguruj**.
4. W okienku konfiguracji funkcji ochrony rodzicielskiej kliknij opcję **Zaawansowane**.
5. W okienku globalnej ochrony rodzicielskiej kliknij opcję **Pliki cookie**.
6. W obszarze Pliki cookie kliknij pozycję na liście **Akceptuj pliki cookie**, zmodyfikuj adres w polu **http://**, a następnie kliknij przycisk **Aktualizuj**.
7. Kliknij przycisk **OK**.

Zapobieganie ustawianiu plików cookie przez witrynę sieci Web

Aby zapobiec odczytywaniu przez określoną witrynę sieci Web plików cookie zapisanych przez nią na komputerze, należy usunąć ją z listy **Akceptuj pliki cookie**.

Aby zapobiec ustawianiu plików cookie przez witrynę sieci Web:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Funkcje ochrony rodzicielskiej**.
3. W sekcji informacji o funkcjach ochrony rodzicielskiej kliknij polecenie **Konfiguruj**.
4. W okienku konfiguracji funkcji ochrony rodzicielskiej kliknij opcję **Zaawansowane**.
5. W okienku globalnej ochrony rodzicielskiej kliknij opcję **Pliki cookie**.
6. W okienku Pliki cookie kliknij pozycję na liście **Akceptuj pliki cookie**, a następnie kliknij przycisk **Usuń**.
7. W oknie dialogowym Potwierdzenie usunięcia kliknij przycisk **Tak**.
8. Kliknij przycisk **OK**.

Blokowanie potencjalnie niepożądanych obrazów w sieci Web

Można chronić członków rodziny przez blokowanie wyświetlania potencjalnie niepożądanych obrazów podczas przeglądania stron w Internecie. Obrazy można zablokować dla wszystkich użytkowników lub dla wszystkich użytkowników z wyjątkiem członków grupy wiekowej dorosłych. Więcej informacji o grupach wiekowych zawiera sekcja Ustawianie grupy klasyfikacji zawartości użytkownika (strona 234).

Domyślnie analiza obrazów jest włączona dla wszystkich użytkowników z wyjątkiem członków grupy wiekowej dorosłych; jednak administrator może ją wyłączyć w dowolnej chwili.

Blokowanie potencjalnie niepożądanych obrazów

Domyślnie produkty firmy McAfee mają włączoną funkcję analizy obrazów, która pozwala chronić innych domowników przed kontaktem z nieodpowiednimi obrazami w czasie przeglądania Internetu. Jeśli produkt firmy McAfee wykryje potencjalnie nieodpowiedni obraz, zastąpi go własnym, zawierającym informację o zablokowaniu oryginalnego obrazu. Do wyłączenia funkcji analizy obrazów wymagane są uprawnienia Administratora.

Aby blokować potencjalnie nieodpowiednie obrazy:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Funkcje ochrony rodzicielskiej**.
3. W sekcji informacji o funkcjach ochrony rodzicielskiej kliknij polecenie **Konfiguruj**.
4. W okienku konfiguracji funkcji ochrony rodzicielskiej kliknij opcję **Zaawansowane**.
5. W okienku globalnej ochrony rodzicielskiej kliknij opcję **Analiza obrazów**.
6. W okienku Analiza obrazów wykonaj jedną z następujących czynności:
   - Kliknij opcję **Wszyscy użytkownicy**, aby zablokować potencjalnie niepożądane obrazy dla wszystkich użytkowników.
   - Kliknij opcję **Nastolatki i dzieci**, aby zablokować potencjalnie niepożądane obrazy dla wszystkich użytkowników poza członkami grupy dorosłych.
7. Kliknij przycisk **OK**.

ROZDZIAŁ 35

Ochrona informacji w Internecie

Program Privacy Service umożliwia ochronę członków rodziny i informacji osobistych podczas przeglądania stron w Internecie. Administrator może na przykład tak skonfigurować program McAfee, aby blokował reklamy, wyskakujące okienka i pluskwy internetowe podczas przeglądania stron internetowych przez użytkowników. Można również uniemożliwić przesyłanie przez Internet informacji osobistych (takich jak: nazwisko, adres, numery kart kredytowych i numery kont bankowych), dodając je do obszaru zablokowanych informacji.

W tym rozdziale

Blokowanie reklam, wyskakujących okien i pluskiew internetowych 256
Blokowanie informacji osobistych 258

Blokowanie reklam, wyskakujących okien i pluskiew internetowych

Jeśli użytkownik jest administratorem, może skonfigurować w produkcie firmy McAfee blokowanie reklam, wyskakujących okien i pluskiew internetowych w czasie, gdy użytkownicy korzystają z Internetu. Funkcja blokowania reklam i wyskakujących okien uniemożliwia wyświetlanie w przeglądarce internetowej większości reklam i wyskakujących okien. Może to pomóc zwiększyć szybkość i sprawność przeglądania Internetu. Funkcja blokowania pluskiew internetowych uniemożliwia śledzenie przez witryny sieci Web czynności wykonywanych online i przesyłanie informacji do nieupoważnionych źródeł. Pluskwy internetowe (nazywane także sygnalizatorami sieci Web, tagami pikselowymi, czystymi lub niewidocznymi plikami GIF) to małe pliki graficzne osadzające się na stronach HTML i umożliwiające nieautoryzowanym źródłom ustawianie plików cookie na komputerze użytkownika. Te pliki cookie mogą następnie przesyłać informacje do nieautoryzowanego źródła.

Blokowanie reklam, wyskakujących okien i pluskiew internetowych jest domyślnie włączone. Jako Administrator użytkownik może wyłączyć blokowanie reklam, wyskakujących okien i pluskiew internetowych w dowolnym momencie.

Blokowanie reklam

Użytkownik może blokować reklamy pojawiające się w czasie korzystania z Internetu przez wszystkich użytkowników.

Aby zablokować reklamy:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Internet i sieć**.
3. W sekcji informacji o Internecie i sieci kliknij polecenie **Konfiguruj**.
4. W okienku Konfiguracja Internetu i sieci kliknij przycisk **Zaawansowane** w obszarze **Ochrona przeglądania sieci Web**.
5. W okienku Blokowanie reklam, wyskakujących okien i pluskiew internetowych zaznacz pole wyboru **Blokuje reklamy pojawiające się na stronach sieci Web podczas przeglądania Internetu**.
6. Kliknij przycisk **OK**.

Blokowanie wyskakujących okien

Użytkownik może blokować wyskakujące okna pojawiające się w czasie korzystania z Internetu przez wszystkich użytkowników..

Aby blokować wyskakujące okna:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Internet i sieć**.
3. W sekcji informacji o Internecie i sieci kliknij polecenie **Konfiguruj**.
4. W okienku Konfiguracja Internetu i sieci kliknij przycisk **Zaawansowane** w obszarze **Ochrona przeglądania sieci Web**.
5. W okienku Blokowanie reklam, wyskakujących okien i pluskiew internetowych zaznacz pole wyboru **Uniemożliwia wyświetlanie wyskakujących okien podczas korzystania z Internetu**.
6. Kliknij przycisk **OK**.

Blokowanie pluskiew internetowych

Pluskwy internetowe (nazywane także sygnalizatorami sieci Web, tagami pikselowymi, czystymi lub niewidocznymi plikami GIF) to małe pliki graficzne osadzające się na stronach HTML i umożliwiające nieautoryzowanym źródłom ustawianie plików cookie na komputerze użytkownika. Te pliki cookie mogą następnie przesyłać informacje do nieautoryzowanego źródła. Użytkownik może zapobiec ładowaniu pluskiew internetowych na komputer, blokując je.

Aby blokować pluskwy internetowe:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Internet i sieć**.
3. W sekcji informacji o Internecie i sieci kliknij polecenie **Konfiguruj**.
4. W okienku Konfiguracja Internetu i sieci kliknij przycisk **Zaawansowane** w obszarze **Ochrona przeglądania sieci Web**.
5. W okienku Blokowanie reklam, wyskakujących okien i pluskiew internetowych zaznacz pole wyboru **Blokuj pluskwy internetowe na tym komputerze**.
6. Kliknij przycisk **OK**.

Blokowanie informacji osobistych

Chroń informacje osobiste (takie jak nazwisko, adres, numery kart kredytowych i numery kont bankowych) przed przesyłaniem ich przez Internet, dodając je do obszaru zablokowanych informacji. W przypadku wykrycia przez program McAfee, że wysyłane dane zawierają informacje umożliwiające identyfikację użytkownika, wykonywane są następujące czynności:

- Jeśli użytkownik jest administratorem, zostanie wyświetlony monit o potwierdzenie wysłania informacji.
- Jeśli użytkownik nie jest administratorem, blokowane informacje zostaną zastąpione gwiazdkami (*). Na przykład jeśli w treści wiadomości e-mail znajdzie się informacja *Lance Armstrong wygrał turniej*, a słowo *Armstrong* będzie ustawione jako blokowana informacja osobista, wysłana wiadomość będzie miała postać: *Lance* ********* *wygrał turniej*.

Można zablokować następujące rodzaje informacji osobistych: nazwisko, adres, kod pocztowy, informacje o ubezpieczeniu społecznym, numer telefonu, numery kart kredytowych, numery kont bankowych, rachunki maklerskie i karty telefoniczne. Aby zablokować informacje osobiste innego typu, można ustawić typ jako **inne**.

Blokowanie informacji osobistych

Można zablokować następujące informacje osobiste: nazwisko, adres, kod pocztowy, informacje o ubezpieczeniu społecznym, numer telefonu, numery kart kredytowych, numery kont bankowych, rachunki maklerskie i karty telefoniczne. Aby zablokować informacje osobiste innego typu, można ustawić typ jako **inne**.

Aby zablokować informacje osobiste:

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij kategorię **Internet i sieć**.
3. W sekcji informacji kategorii Internet i sieć kliknij opcję **Konfiguruj**.
4. Upewnij się, że w okienku Konfiguracja kategorii Internet i sieć włączona jest ochrona informacji osobistych, a następnie kliknij przycisk **Zaawansowane**.
5. W okienku Zablokowane informacje kliknij opcję **Dodaj**.
6. Wybierz na liście typ informacji, który chcesz zablokować.
7. Wprowadź informacje osobiste, a następnie kliknij przycisk **OK**.
8. W oknie dialogowym Ochrona informacji osobistych kliknij przycisk **OK**.

ROZDZIAŁ 36

Ochrona haseł

Magazyn haseł jest bezpiecznym obszarem przechowywania osobistych haseł. Umożliwia on przechowywanie haseł, dając użytkownikowi pewność, że nikt inny (nawet administrator programu McAfee ani administrator systemu) nie ma do nich dostępu.

W tym rozdziale

Konfigurowanie Magazynu haseł 260

Konfigurowanie Magazynu haseł

Przed rozpoczęciem korzystania z Magazynu haseł należy ustawić hasło do Magazynu haseł. Tylko użytkownicy znający to hasło będą mogli mieć dostęp do Magazynu haseł. Jeśli użytkownik zapomni to hasło, można je zresetować; jednak wszystkie hasła zapisane wcześniej w Magazynie haseł zostaną usunięte.

Po skonfigurowaniu hasła do Magazynu haseł można dodawać, edytować lub usuwać hasła z magazynu.

Dodawanie hasła do magazynu haseł

Jeśli zapamiętanie wszystkich swoich haseł sprawia trudności, można dodać je do magazynu haseł. Magazyn haseł jest bezpiecznym miejscem, do którego dostęp mają tylko użytkownicy znający odpowiednie hasło.

Aby dodać hasło do magazynu haseł:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Internet i sieć**.
3. W sekcji informacji o Internecie i sieci kliknij polecenie **Konfiguruj**.
4. W okienku Konfiguracja Internetu i sieci kliknij przycisk **Zaawansowane** w obszarze **Ochrona informacji osobistych**.
5. W okienku Ochrona informacji osobistych kliknij opcję **Magazyn haseł**.
6. Wpisz hasło do magazynu haseł w polu **Hasło**, a następnie wpisz je ponownie w polu **Potwierdź hasło**.
7. Kliknij przycisk **Otwórz**.
8. W okienku Magazyn haseł kliknij przycisk **Dodaj**.
9. Wpisz opis hasła (na przykład napisz, czego dotyczy) w polu **Opis**, a następnie wpisz hasło w polu **Hasło**.
10. Kliknij przycisk **Dodaj**, a następnie przycisk **OK**.

Modyfikowanie hasła w magazynie haseł

Aby wpisy w magazynie haseł były zawsze aktualne i prawidłowe, należy je aktualizować zawsze, gdy hasła ulegną zmianie.

Aby zmodyfikować hasło w magazynie haseł:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Internet i sieć**.
3. W sekcji informacji o Internecie i sieci kliknij polecenie **Konfiguruj**.
4. W okienku Konfiguracja Internetu i sieci kliknij przycisk **Zaawansowane** w obszarze **Ochrony informacji osobistych**.
5. W okienku Ochrona informacji osobistych kliknij opcję **Magazyn haseł**.
6. Wpisz hasło magazynu haseł w polu **Hasło**.
7. Kliknij przycisk **Otwórz**.
8. W okienku Magazyn haseł kliknij wpis, a następnie kliknij przycisku **Edytuj**.
9. Zmodyfikuj opis hasła (na przykład napisz, czego dotyczy) w polu **Opis** lub zmodyfikuj hasło w polu **Hasło**.
10. Kliknij przycisk **Dodaj**, a następnie przycisk **OK**.

Usuwanie hasła z magazynu haseł

Hasło można usunąć z magazynu haseł w dowolnym momencie. Hasła usuniętego z magazynu nie można odzyskać.

Aby usunąć hasło z magazynu haseł:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Internet i sieć**.
3. W sekcji informacji o Internecie i sieci kliknij polecenie **Konfiguruj**.
4. W okienku Konfiguracja Internetu i sieci kliknij przycisk **Zaawansowane** w obszarze **Ochrony informacji osobistych**.
5. W okienku Ochrona informacji osobistych kliknij opcję **Magazyn haseł**.
6. Wpisz hasło magazynu haseł w polu **Hasło**.
7. Kliknij przycisk **Otwórz**.
8. W okienku Magazyn haseł kliknij wpis, a następnie kliknij przycisku **Usuń**.
9. W oknie dialogowym Potwierdzenie usunięcia kliknij przycisk **Tak**.
10. Kliknij przycisk **OK**.

Resetowanie hasła magazynu haseł

W przypadku zapomnienia hasła do magazynu można je zresetować; powoduje to jednak usunięcie wszystkich wcześniej wprowadzonych haseł.

Aby zresetować hasło magazynu haseł:

1. W obszarze **Typowe zadania** kliknij opcję **Początek**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Internet i sieć**.
3. W okienku informacji o Internecie i sieci kliknij polecenie **Konfiguruj**.
4. W okienku Konfiguracja Internetu i sieci kliknij przycisk **Zaawansowane** w obszarze **Ochrony informacji osobistych**.
5. W okienku Ochrona informacji osobistych kliknij opcję **Magazyn haseł**.
6. W obszarze **Resetowanie hasła do magazynu** wpisz nowe hasło w polu **Hasło**, a następnie wpisz je ponownie w polu **Potwierdź hasło**.
7. Kliknij przycisk **Resetuj**.
8. W oknie dialogowym Potwierdzenie resetowania hasła kliknij przycisk **Tak**.

ROZDZIAŁ 37

McAfee Data Backup

Programu Data Backup należy używać, aby zapobiec przypadkowej utracie danych, archiwizując pliki i foldery na dysku CD, DVD, USB, zewnętrznym dysku twardym lub dysku sieciowym. Archiwizacja lokalna pozwala na zarchiwizowanie (utworzenie kopii zapasowych) osobistych danych na dysku CD, DVD, USB, zewnętrznym dysku twardym lub dysku sieciowym. Dostarcza to użytkownikowi lokalne kopie jego danych, dokumentów i innych materiałów osobistych na wypadek ich przypadkowej utraty.

Przed przystąpieniem do użytkowania programu Data Backup można zapoznać się z jego niektórymi najczęściej używanymi funkcjami. Szczegółowe informacje na temat konfigurowania tych funkcji i korzystania z nich zamieszczono w pomocy programu Data Backup. Po przejrzeniu funkcji programu, należy upewnić się, że dostępne są odpowiednie nośniki do przeprowadzania lokalnych archiwizacji.

W tym rozdziale

Funkcje....266
Archiwizowanie plików....267
Praca ze zarchiwizowanymi plikami....277

Funkcje

Program Data Backup pozwala na zapisywanie i przywracanie plików z fotografiami, muzyką i innymi ważnymi informacjami.

Planowana lokalna archiwizacja danych

Zabezpiecz dane, archiwizując pliki i foldery na dysku CD, DVD, USB, zewnętrznym dysku twardym lub dysku sieciowym. Po zainicjowaniu pierwszej archiwizacji archiwizacja przyrostowa będzie później wykonywana automatycznie.

Przywracanie za pomocą jednego kliknięcia

W razie omyłkowego skasowania lub uszkodzenia plików lub folderów na komputerze, można przywrócić ich ostatnie wersje z używanych nośników archiwum.

Kompresja i szyfrowanie

Domyślnie archiwizowane pliki są kompresowane, dzięki czemu oszczędza się miejsce na nośniku. Dodatkowe zabezpieczenie archiwum zapewnia jego szyfrowanie (opcja domyślna).

ROZDZIAŁ 38

Archiwizowanie plików

Programu McAfee Data Backup można użyć w celu archiwizowania kopii plików z komputera na dysku CD, DVD, USB, zewnętrznym dysku twardym lub dysku sieciowym. Archiwizowanie plików w ten sposób pozwala na łatwe odzyskanie informacji na wypadek przypadkowej utraty danych lub ich uszkodzenia.

Przed rozpoczęciem archiwizowania plików należy wybrać domyślną lokalizację archiwum (dysk CD, DVD, USB, zewnętrzny dysk twardy lub dysk sieciowy). Firma McAfee skonfigurowała wcześniej część innych ustawień, na przykład foldery i typy plików, które mają być archiwizowane — można jednak zmienić te ustawienia.

Po skonfigurowaniu opcji archiwum lokalnego można zmienić domyślne ustawienia mówiące o tym, jak często program Data Backup ma przeprowadzać pełną lub szybką archiwizację. Archiwizowanie ręczne można uruchomić w dowolnym momencie.

W tym rozdziale

Konfigurowanie opcji archiwizowania 268
Przeprowadzanie pełnych i szybkich archiwizacji.....273

Konfigurowanie opcji archiwizowania

Przed rozpoczęciem archiwizowania danych należy skonfigurować pewne opcje archiwum lokalnego. Na przykład trzeba skonfigurować monitorowane lokalizacje i typy plików. Monitorowane lokalizacje to foldery w komputerze, które program Data Backup monitoruje pod kątem pojawienia się nowych plików lub zmian w plikach. Monitorowane typy plików to typy plików (na przykład .doc, .xls itd.) znajdujące się w lokalizacjach monitorowanych, które program Data Backup archiwizuje. Domyślnie program Data Backup monitoruje wszystkie typy plików przechowywanych w monitorowanych lokalizacjach.

Można skonfigurować dwa typy monitorowanych lokalizacji: lokalizacje monitorowane dokładnie i lokalizacje monitorowane częściowo. Po skonfigurowaniu lokalizacji monitorowanej dokładnie program Data Backup archiwizuje wszystkie pliki monitorowanych typów znajdujące się w tym folderze i jego podfolderach. Po skonfigurowaniu lokalizacji monitorowanej częściowo program Data Backup archiwizuje wszystkie pliki monitorowanych typów znajdujące się tylko w tym folderze (nie w jego podfolderach). Można również określić lokalizacje, które mają być wyłączone z lokalnego archiwum. Domyślnie pulpit systemu Windows oraz folder Moje dokumenty skonfigurowane są jako lokalizacje monitorowane dokładnie.

Po skonfigurowaniu typów monitorowanych plików i lokalizacji, należy skonfigurować lokalizację archiwum (czyli dysk CD, DVD, USB, zewnętrzny dysk twardy lub dysk sieciowy, na których będą magazynowane dane poddane archiwizacji). Lokalizację archiwum można zmienić w dowolnym momencie.

Z powodów związanych z bezpieczeństwem lub rozmiarami archiwum, dla archiwizowanych plików domyślnie włączone są opcje szyfrowania i kompresji. Zawartość szyfrowanych plików jest zamieniana z tekstu na kod, mający na celu uniemożliwienie odczytania informacji przez osoby nieznające metody jego odszyfrowania. Kompresowane pliki są kompresowane do postaci, która minimalizuje przestrzeń wymaganą do ich przechowywania lub przesyłania. Pomimo, że firma McAfee tego nie zaleca, można w dowolnym momencie wyłączyć szyfrowanie lub kompresję.

Zawieranie lokalizacji w archiwum

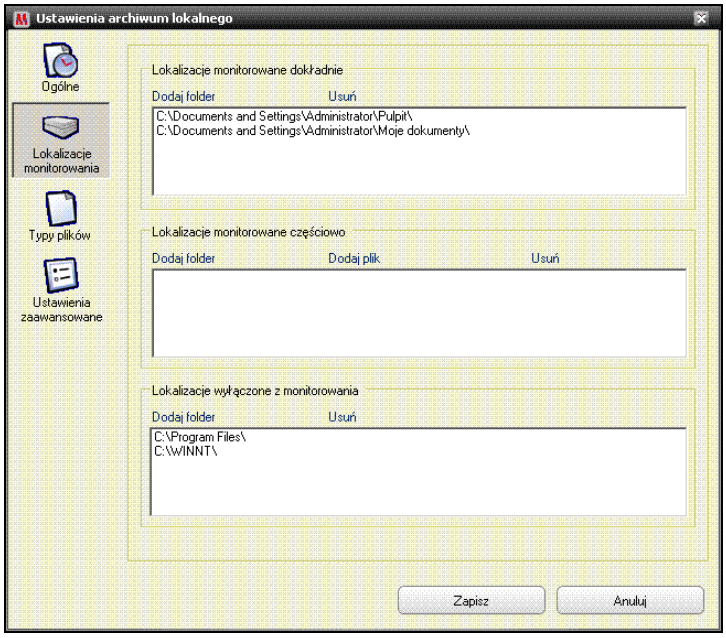
Można skonfigurować dwa typy monitorowanych lokalizacji, które będą poddane archiwizacji: dokładny i częściowy. Po skonfigurowaniu lokalizacji monitorowanej dokładnie program Data Backup monitoruje zawartość folderu oraz jego podfolderów pod kątem zmian. Po skonfigurowaniu lokalizacji monitorowanej częściowo program Data Backup monitoruje tylko zawartość folderu (nie jego podfolderów).

Aby zawrzeć lokalizację w archiwum:

1 Kliknij kartę **Archiwum lokalne**.

2 W okienku po lewej stronie kliknij przycisk **Ustawienia**.

3 W oknie dialogowym Ustawienia archiwum lokalnego kliknij przycisk **Lokalizacje monitorowania**.



4 Wykonaj jedną z poniższych czynności:

- Aby archiwizować zawartość folderu razem z zawartością jego podfolderów kliknij przycisk **Dodaj folder** w polu **Lokalizacje monitorowane dokładnie**.
- Aby archiwizować zawartość folderu, ale nie jego podfolderów, kliknij przycisk **Dodaj folder** w polu **Lokalizacje monitorowane częściowo**.

5 W oknie dialogowym Przeglądanie w poszukiwaniu folderu przejdź do folderu, który chcesz monitorować, a następnie kliknij przycisk **OK**.

6 Kliknij przycisk **Zapisz**.

Wskazówka: Jeśli program Data Backup ma monitorować folder, który nie został jeszcze utworzony, można kliknąć przycisk **Utwórz nowy folder** w oknie dialogowym Przeglądanie w poszukiwaniu folderu, aby dodać folder i jednocześnie skonfigurować go jako monitorowaną lokalizację.

Konfiguracja typów archiwizowanych plików

Można określić, jakie typy plików mają być archiwizowane w lokalizacjach monitorowanych dokładnie lub częściowo. Można wybrać z istniejącej listy typów plików lub dodać do niej nowy typ.

Aby skonfigurować archiwizowane typy plików:

1 Kliknij kartę **Archiwum lokalne**.

2 W okienku po lewej stronie kliknij przycisk **Ustawienia**.

3 W oknie dialogowym Ustawienia archiwum lokalnego kliknij przycisk **Typy plików**.

4 Rozwiń listę typów plików i zaznacz pola wyboru przy typach plików, które mają być archiwizowane.

5 Kliknij przycisk **Zapisz**.

Wskazówka: Aby dodać nowy typ plików do listy **Selected File Types** (Wybrane typy plików) wpisz rozszerzenie pliku w polu **Dodaj niestandardowy typ pliku do grupy „Inne”**, a następnie kliknij przycisk **Dodaj**. Nowy typ plików automatycznie staje się typem monitorowanym.

Wykluczenie lokalizacji z archiwum

Lokalizację wyklucza się z archiwum, jeśli nie chcemy tej lokalizacji (folderu) i jej zawartości archiwizować.

Aby wykluczyć lokalizację z archiwum:

1. Kliknij kartę **Archiwum lokalne**.
2. W okienku po lewej stronie kliknij przycisk **Ustawienia**.
3. W oknie dialogowym Ustawienia archiwum lokalnego kliknij przycisk **Watch Folders** (Monitorowane foldery).
4. Kliknij przycisk **Dodaj folder** w kategorii **Lokalizacje wyłączone z monitorowania**.
5. W oknie dialogowym Przeglądanie w poszukiwaniu folderu przejdź do folderu, który chcesz wyłączyć z monitorowania, wybierz go, a następnie kliknij przycisk **OK**.
6. Kliknij przycisk **Zapisz**.

Wskazówka: Jeśli program Data Backup ma wyłączyć z monitorowania folder, który nie został jeszcze utworzony, można kliknąć przycisk **Utwórz nowy folder** w oknie dialogowym Przeglądanie w poszukiwaniu folderu, aby dodać folder i jednocześnie wyłączyć go z monitorowania.

Zmiana lokalizacji archiwum

Gdy lokalizacja archiwum zostanie zmieniona, pliki archiwizowane wcześniej w innej lokalizacji będą oznaczone jako *Nigdy nie archiwizowano*.

Aby zmienić lokalizację archiwum:

1. Kliknij kartę **Archiwum lokalne**.
2. W okienku po lewej stronie kliknij przycisk **Ustawienia**.
3. Kliknij przycisk **Zmień lokalizację archiwum**.
4. W oknie dialogowym Lokalizacja archiwum wykonaj jedną z poniższych czynności:
   - Kliknij przycisk **Wybierz nagrywarkę CD/DVD**, na liście **Nagrywarka** kliknij znajdujący się w komputerze napęd CD lub DVD, a następnie kliknij przycisk **Zapisz**.
   - Kliknij przycisk **Wybierz lokalizację dysku**, przejdź do dysku USB, dysku lokalnego lub zewnętrznego dysku twardego, wybierz go, a następnie kliknij przycisk **OK**.
   - Kliknij przycisk **Wybierz lokalizację sieciową**, przejdź do folderu sieciowego, zaznacz go, a następnie kliknij przycisk **OK**.

5 Potwierdź nową lokalizację archiwum w polu **Wybrana lokalizacja archiwum**, a następnie kliknij przycisk **OK**.

6 W oknie dialogowym potwierdzenia kliknij przycisk **OK**.

7 Kliknij przycisk **Zapisz**.

Wyłączanie szyfrowania i kompresowania archiwum

Szyfrowanie archiwizowanych plików chroni poufność danych użytkownika, zmieniając zawartość plików tak, że stają się one nie do odczytania. Kompresowanie archiwizowanych plików pomaga zminimalizować ich rozmiar. Domyślnie zarówno szyfrowanie, jak i kompresowanie, są włączone; jednakże w dowolnej chwili można te opcje wyłączyć.

Aby wyłączyć szyfrowanie i kompresowanie archiwum:

1 Kliknij kartę **Archiwum lokalne**.

2 W okienku po lewej stronie kliknij przycisk **Ustawienia**.

3 W oknie dialogowym Ustawienia archiwum lokalnego kliknij przycisk **Ustawienia zaawansowane**.

4 Usuń zaznaczenie pola wyboru **Włącz szyfrowanie w celu zwiększenia bezpieczeństwa**.

5 Usuń zaznaczenie pola wyboru **Włącz kompresję w celu zmniejszenia ilości zajmowanego miejsca**.

6 Kliknij przycisk **Zapisz**.

Uwaga: Firma McAfee zaleca niewyłączanie szyfrowania i kompresowania podczas archiwizowania plików.

Przeprowadzanie pełnych i szybkich archiwizacji

Można przeprowadzić dwa typy archiwizacji: pełną lub szybką. Podczas przeprowadzania archiwizacji pełnej, archiwizowany jest pełen zestaw danych w zależności od skonfigurowanych monitorowanych typów plików i lokalizacji. Podczas przeprowadzania archiwizacji szybkiej, archiwizowane są tylko te monitorowane pliki, które uległy zmianie od ostatniej pełnej lub szybkiej archiwizacji.

Domyślnie program Data Backup ma zaplanowane przeprowadzanie pełnej archiwizacji monitorowanych typów plików w monitorowanych lokalizacjach w każdy poniedziałek o godzinie 9:00, a archiwizacji szybkiej co 48 godzin od ostatniej szybkiej lub pełnej archiwizacji. Ten harmonogram zapewnia utrzymywanie przez cały czas aktualnego archiwum. Jednakże, jeśli archiwizacja nie ma być przeprowadzana co 48 godzin, można ten harmonogram zmienić i dopasować do własnych potrzeb.

W każdej chwili można przeprowadzić archiwizację monitorowanych lokalizacji na żądanie użytkownika. Na przykład jeśli zmieniony został plik, który ma być archiwizowany, ale program Data Backup nie ma zaplanowanego przeprowadzania pełnej lub szybkiej archiwizacji przez najbliższe kilka godzin, można ręcznie archiwizować pliki. Gdy pliki zostaną archiwizowane ręcznie, interwał ustawiony dla automatycznych archiwizacji zostaje wyzerowany.

Można również przerwać archiwizację automatyczną lub ręczną, jeśli będzie miała ona miejsce w nieodpowiednim momencie. Na przykład jeśli użytkownik wykonuje zadanie zużywające dużo zasobów systemowych i rozpocznie się automatyczna archiwizacja, można ją zatrzymać. Gdy archiwizacja automatyczna zostanie zatrzymana, interwał ustawiony dla automatycznych archiwizacji zostaje wyzerowany.

Planowanie automatycznych archiwizacji

Można ustawić częstotliwość dokonywania pełnych i szybkich archiwizacji, aby zapewnić stałą ochronę danych.

Aby zaplanować automatyczne archiwizacje:

1. Kliknij kartę **Archiwum lokalne**.
2. W okienku po lewej stronie kliknij przycisk **Ustawienia**.
3. W oknie dialogowym Ustawienia archiwum lokalnego kliknij przycisk **Ogólne**.
4. Aby przeprowadzić pełną archiwizację co dzień, tydzień lub miesiąc, kliknij jedną z poniższych opcji w polu **Archiwizacja pełna co**:
   - **Dzień**
   - **Tydzień**

- **Miesiąc**

5 Zaznacz pole wyboru znajdujące się obok dnia, w którym ma być przeprowadzana pełna archiwizacja.

6 Kliknij wartość na liście **O**, aby określić godzinę, o której ma być przeprowadzona pełna archiwizacja.

7 Aby przeprowadzać archiwizację szybką codziennie lub co godzinę, kliknij jedną z poniższych opcji w polu **Archiwizacja szybka**:

- **Godziny**
- **Dni**

8 Wprowadź liczbę oznaczającą częstotliwość w polu **Archiwizacja szybka co**.

9 Kliknij przycisk **Zapisz**.

Przerywanie automatycznej archiwizacji

Program Data Backup automatycznie archiwizuje pliki w monitorowanych lokalizacjach zgodnie ze zdefiniowanym przez użytkownika harmonogramem. Jednakże, jeśli użytkownik chce przerwać trwającą archiwizację, może to zrobić w dowolnym momencie.

Aby przerwać automatyczną archiwizację:

1 W okienku po lewej stronie kliknij łącze **Zatrzymaj archiwizowanie**.

2 W oknie dialogowym potwierdzenia kliknij przycisk **Tak**.

Uwaga: Łącze **Zatrzymaj archiwizowanie** pojawia się tylko wtedy, gdy trwa archiwizacja.

Ręczne przeprowadzanie archiwizacji

Pomimo, że archiwizacje automatyczne przeprowadzane są zgodnie ze zdefiniowanym wcześniej harmonogramem, można przeprowadzić szybką lub pełną archiwizację ręcznie w dowolnym momencie. Podczas przeprowadzania archiwizacji szybkiej, archiwizowane są tylko te pliki, które uległy zmianie od ostatniej pełnej lub szybkiej archiwizacji. Podczas przeprowadzania archiwizacji pełnej archiwizowane są monitorowane typy plików we wszystkich monitorowanych lokalizacjach.

Aby ręcznie przeprowadzić szybką lub pełną archiwizację:

1. Kliknij kartę **Archiwum lokalne**.
2. Aby przeprowadzić archiwizację szybką, kliknij przycisk **Archiwizacja szybka** w okienku po lewej stronie.
3. Aby przeprowadzić archiwizację pełną, kliknij przycisk **Archiwizacja pełna** w okienku po lewej stronie.
4. W oknie dialogowym Program gotowy do rozpoczęcia archiwizowania potwierdź ilość dostępnego miejsca oraz ustawienia, a następnie kliknij przycisk **Kontynuuj**.

ROZDZIAŁ 39

Praca ze zarchiwizowanymi plikami

Po zarchiwizowaniu plików do pracy z nimi można użyć programu Data Backup. Zarchiwizowane pliki prezentowane są w tradycyjnym widoku eksploratora, co pozwala je łatwo zlokalizować. Wraz z rozrastaniem się archiwum użytkownik może chcieć sortować lub wyszukiwać pliki. Można również otwierać pliki bezpośrednio w widoku eksploratora, aby obejrzeć ich zawartość bez potrzeby pobierania plików.

Pliki są pobierane z archiwum, jeśli lokalna kopia danego pliku jest nieaktualna, brakująca lub zostanie uszkodzona. Program Data Backup dostarcza również informacje potrzebne do zarządzania lokalnymi archiwami i nośnikami danych.

W tym rozdziale

Używanie eksploratora archiwum lokalnego 278
Przywracanie zarchiwizowanych plików 280
Zarządzanie archiwami 282

Używanie eksploratora archiwum lokalnego

Eksplorator archiwum lokalnego pozwala wyświetlać i manipulować plikami zarchiwizowanymi lokalnie. Dla każdego pliku można wyświetlić jego nazwę, typ, lokalizację, rozmiar, stan (zarchiwizowany, niezarchiwizowany lub archiwizacja w toku) i datę zarchiwizowania pliku. Można również sortować pliki według dowolnego z tych kryteriów.

W przypadku posiadania dużego archiwum można szybko znaleźć plik przez jego wyszukiwanie. Można wyszukiwać plik podając całą lub część jego nazwy lub ścieżki dostępu do niego, następnie można zawęzić wyszukiwanie poprzez podanie przybliżonego rozmiaru pliku i daty jego ostatniej archiwizacji.

Po zlokalizowaniu pliku można go otworzyć bezpośrednio w eksploratorze archiwum lokalnego. Program Data Backup otwiera plik w jego macierzystym programie, pozwalając na wprowadzenie zmian bez opuszczania eksploratora archiwum lokalnego. Plik zostaje zapisany w oryginalnej monitorowanej lokalizacji na komputerze użytkownika i podlega automatycznej archiwizacji zgodnie ze zdefiniowanym przez użytkownika harmonogramem.

Sortowanie zarchiwizowanych plików

Zarchiwizowane pliki i foldery można sortować według poniższych kryteriów: nazwa, typ pliku, rozmiar, stan (czyli zarchiwizowany, niezarchiwizowany lub archiwizacja w toku), data archiwizacji pliku lub lokalizacja plików w komputerze (ścieżka).

Aby posortować zarchiwizowane pliki:

1. Kliknij kartę **Archiwum lokalne**.
2. W okienku po prawej stronie kliknij nazwę kolumny.

Wyszukiwanie zarchiwizowanego pliku

W przypadku posiadania dużego repozytorium zarchiwizowanych plików, można szybko znaleźć plik przez jego wyszukiwanie. Można szukać pliku, podając całą lub część jego nazwy lub ścieżki dostępu do niego, następnie można zawęzić wyszukiwanie poprzez podanie przybliżonego rozmiaru pliku i daty jego ostatniej archiwizacji.

Aby wyszukać zarchiwizowany plik:

1. Wprowadź całą lub część nazwy pliku w polu **Wyszukaj** na górze ekranu, a następnie naciśnij klawisz Enter.
2. Wprowadź pełną lub częściową ścieżkę w polu **Pełna lub częściowa ścieżka**.
3. Określ przybliżony rozmiar wyszukiwanego pliku, wykonując jedną z poniższych czynności:
   - Kliknij opcję **<100 kB**, **<1 MB** lub **>1 MB**.
   - Kliknij przycisk **Rozmiar w kB**, a następnie podaj przybliżony rozmiar w odpowiednich polach.
4. Określ przybliżoną datę ostatniej archiwizacji online wyszukiwanego pliku, wykonując jedną z poniższych czynności:
   - Kliknij przycisk **W tym tygodniu**, **W tym miesiącu** lub **W tym roku**.
   - Kliknij przycisk **Określ daty**, na liście kliknij pole **Zarchiwizowane**, a następnie kliknij odpowiednie wartości daty z listy.
5. Kliknij przycisk **Wyszukaj**.

Uwaga: W przypadku, gdy przybliżony rozmiar pliku lub data jego ostatniej archiwizacji nie są znane, kliknij przycisk **Nieznane**.

Otwieranie zarchiwizowanego pliku

Można zbadać zawartość zarchiwizowanego pliku poprzez otwarcie go bezpośrednio w eksploratorze archiwum lokalnego.

Aby otworzyć zarchiwizowane pliki:

1. Kliknij kartę **Archiwum lokalne**.
2. W okienku po prawej stronie kliknij nazwę pliku, a następnie kliknij przycisk **Otwórz**.

Wskazówka: Zarchiwizowany plik można również otworzyć, klikając dwukrotnie jego nazwę.

Przywracanie zarchiwizowanych plików

Jeśli monitorowany plik zostanie uszkodzony, będzie brakujący lub zostanie omyłkowo usunięty można przywrócić jego kopię z archiwum lokalnego. Z tego powodu ważne jest regularne archiwizowanie plików. Z archiwum lokalnego można również przywrócić starsze wersje plików. Na przykład jeśli dany plik jest regularnie archiwizowany, ale zajdzie potrzeba powrotu do jego poprzedniej wersji, można tego dokonać przez zlokalizowanie pliku w lokalizacji archiwum. Jeśli lokalizacją archiwum jest dysk lokalny lub sieciowy, można je przeglądać w poszukiwaniu pliku. Jeśli lokalizacją archiwum jest zewnętrzny dysk twardy lub dysk USB, należy najpierw podłączyć dysk do komputera i dopiero później przeglądać go w poszukiwaniu pliku. Jeśli lokalizacją archiwum jest dysk CD lub DVD, należy najpierw włożyć dysk CD lub DVD do komputera, a następnie przejrzeć go w poszukiwaniu pliku.

Można również przywracać pliki zarchiwizowane na jednym komputerze z innego komputera. Na przykład jeśli zestaw plików został zarchiwizowany na zewnętrznym dysku twardym w komputerze A, można przywrócić te pliki na komputerze B. Aby to uczynić, należy zainstalować program Data Backup na komputerze B i podłączyć zewnętrzny dysk twardy. Następnie w programie Data Backup należy wykonać przeglądanie w poszukiwaniu plików i zostaną one dodane do listy **Brakujące pliki**, skąd można je przywrócić.

Więcej informacji na temat archiwizowania plików można znaleźć w sekcji Archiwizowanie plików. Jeśli monitorowany plik zostanie celowo usunięty z archiwum, można również usunąć jego wpis z listy **Brakujące pliki**.

Przywracanie brakujących plików z archiwum lokalnego

Archiwum lokalne programu Data Backup pozwala na odzyskanie brakujących danych z monitorowanego folderu na komputerze lokalnym. Na przykład jeśli plik przeniesiono lub usunięto z monitorowanego folderu, a został on już zarchiwizowany, można go przywrócić z archiwum lokalnego.

Aby przywrócić brakujący plik z archiwum lokalnego:

1. Kliknij kartę **Archiwum lokalne**.
2. Na karcie **Brakujące pliki** na dole ekranu, zaznacz pole wyboru znajdujące się przy nazwie pliku, który chcesz przywrócić.
3. Kliknij przycisk **Przywróć**.

Wskazówka: Można przywrócić wszystkie pliki z listy **Brakujące pliki**, klikając przycisk **Przywróć wszystko**.

Przywracanie starszej wersji pliku z archiwum lokalnego

Jeśli użytkownik chce przywrócić starszą wersję zarchiwizowanego pliku, może go zlokalizować i dodać do listy **Brakujące pliki**. Następnie można ten plik przywrócić, tak samo jak każdy inny plik z listy **Brakujące pliki**.

Aby przywrócić starszą wersję pliku z archiwum lokalnego:

1. Kliknij kartę **Archiwum lokalne**.
2. Na karcie **Brakujące pliki** na dole ekranu kliknij przycisk **Przeglądaj** i przejdź do lokalizacji, w której przechowywane jest archiwum.

   Nazwy folderów archiwów mają następujący format: `cre ddmmrr_gg-mm-ss_***`, gdzie `ddmmrr` jest datą archiwizacji plików, `gg-mm-ss` określa czas ich archiwizacji, a `***` zastępuje ciąg znaków `Pełna` lub `Inc`, w zależności od tego, czy przeprowadzono archiwizację pełną czy szybką.
3. Wybierz lokalizację, a następnie kliknij przycisk **OK**.

   Pliki zawarte w wybranej lokalizacji pojawią się na liście **Brakujące pliki**, skąd można je przywrócić. Więcej informacji na ten temat można znaleźć w sekcji Przywracanie brakujących plików z archiwum lokalnego.

Usuwanie plików z listy brakujących plików

Gdy zarchiwizowany plik zostanie przeniesiony lub usunięty z monitorowanego folderu, automatycznie pojawi się on na liście **Brakujące pliki**. Zwraca to uwagę użytkownika na fakt, że wystąpiła niezgodność pomiędzy plikami zarchiwizowanymi a plikami znajdującymi się w monitorowanych folderach. Jeśli plik został celowo przeniesiony lub usunięty z monitorowanego folderu, można go również usunąć z listy **Brakujące pliki**.

Aby usunąć plik z listy Brakujące pliki:

1. Kliknij kartę **Archiwum lokalne**.
2. Na karcie **Brakujące pliki** na dole ekranu, zaznacz pole wyboru znajdujące się przy nazwie pliku, który chcesz usunąć.
3. Kliknij przycisk **Usuń**.

Wskazówka: Można usunąć wszystkie pliki z listy **Brakujące pliki**, klikając przycisk **Usuń wszystko**.

Zarządzanie archiwami

W każdej chwili można wyświetlić podsumowanie pełnych i szybkich archiwizacji. Na przykład można wyświetlić informacje o ilości danych, które są w danej chwili monitorowane, ilości danych, które zostały zarchiwizowane oraz ilości danych, które są obecnie monitorowane, ale nie zostały jeszcze zarchiwizowane. Można również wyświetlić informacje dotyczące harmonogramu archiwizacji, takie jak data ostatniej i następnej archiwizacji.

Wyświetlanie podsumowania aktywności użytkownika związanej z archiwizacją

Informacje o aktywności użytkownika związanej z archiwizacją można wyświetlić w dowolnym momencie. Na przykład można zobaczyć procent zarchiwizowanych plików, rozmiar monitorowanych danych, rozmiar zarchiwizowanych danych oraz rozmiar danych, które są monitorowane, ale nie zostały jeszcze zarchiwizowane. Można również wyświetlić daty ostatniej i następnej archiwizacji.

Aby obejrzeć podsumowanie aktywności użytkownika dotyczącej kopii zapasowych:

1. Kliknij kartę **Archiwum lokalne**.
2. Na górze ekranu kliknij przycisk **Podsumowanie konta**.

ROZDZIAŁ 40

McAfee Wireless Network Security

Program Wireless Network Security zawiera zgodne ze standardami branżowymi zabezpieczenia przed kradzieżą danych, nieautoryzowanym dostępem do sieci i wykorzystaniem jej do bezprawnego pobierania plików. Program Wireless Network Security szyfruje osobiste i prywatne dane wysyłane przez sieć Wi-Fi oraz blokuje hakerom dostęp do sieci bezprzewodowej.

Program Wireless Network Security uniemożliwia hakerom skuteczne atakowanie sieci bezprzewodowej:

- uniemożliwiając nieautoryzowanym użytkownikom uzyskanie dostępu do sieci Wi-Fi,
- zapobiegając przechwytywaniu danych przesyłanych przez sieć Wi-Fi,
- wykrywając próby połączenia z siecią Wi-Fi.

Program Wireless Network Security łączy w sobie funkcje ułatwiające obsługę, na przykład natychmiastową blokadę połączenia z Internetem, oraz możliwość szybkiego dodawania do sieci wiarygodnych użytkowników ze skutecznymi funkcjami zabezpieczeń, na przykład automatycznym, szyfrowanym generowaniem kluczy oraz planowaniem cyklicznych zmian klucza.

W tym rozdziale

Funkcje....284
Uruchamianie programu Wireless Network Security 286
Ochrona sieci bezprzewodowych....289
Administrowanie sieciami bezprzewodowymi 307
Zarządzanie zabezpieczeniami sieci bezprzewodowych....319
Monitorowanie sieci bezprzewodowych....335

Funkcje

Program Wireless Network Security oferuje następujące funkcje:

Zawsze włączona ochrona

Program Wireless Network Security automatycznie wykrywa i chroni każdą zagrożoną sieć bezprzewodową, z którą łączy się użytkownik.

Intuicyjny interfejs

Chroni sieć bez potrzeby podejmowania trudnych decyzji i znajomości skomplikowanych terminów technicznych.

Silne szyfrowanie automatyczne

Zezwala na dostęp do sieci jedynie przyjaciołom i członkom rodziny oraz chroni dane wysyłane i odbierane przez użytkownika.

Rozwiązanie oparte wyłącznie na oprogramowaniu

Program Wireless Network Security współpracuje ze standardowym routerem bezprzewodowym lub punktem dostępu i oprogramowaniem zabezpieczającym. Nie jest konieczny zakup dodatkowych urządzeń.

Automatyczna cykliczna zmiana klucza

Nawet najbardziej uparci hakerzy nie są w stanie przechwycić informacji, ponieważ klucz jest cyklicznie zmieniany

Dodawanie użytkowników sieci

Przyznawanie uprawnień dostępu do sieci przyjaciołom i członkom rodziny jest bardzo łatwe. Użytkowników można dodawać za pośrednictwem sieci bezprzewodowej lub przenosząc oprogramowanie na dysku USB.

Intuicyjne narzędzie do monitorowania połączeń

Narzędzie do monitorowania sieci bezprzewodowych jest intuicyjne i dostarcza wielu istotnych informacji, w tym również danych o mocy sygnału i stanie bezpieczeństwa.

Rejestrowanie zdarzeń i alerty

Więcej informacji o sieci bezprzewodowej dostarczają zaawansowanym użytkownikom łatwe do zrozumienia raporty i alerty.

Tryb wstrzymania

Chwilowo wstrzymuje cykliczną zmianę klucza, dzięki czemu poszczególne aplikacje mogą działać bez przerw.

Zgodność z popularnymi urządzeniami

Program Wireless Network Security automatycznie dokonuje aktualizacji, uzupełniając swoje zasoby o najnowsze moduły routerów bezprzewodowych i punktów dostępu najpopularniejszych marek, w tym: Linksys®, NETGEAR®, D-Link®, Belkin®, TRENDnet® i innych.

Uruchamianie programu Wireless Network Security

Program Wireless Network Security jest automatycznie włączany po zainstalowaniu i nie trzeba go włączać ręcznie. Opcjonalnie można jednak włączyć lub wyłączyć ochronę bezprzewodową ręcznie.

Po zainstalowaniu programu Wireless Network Security komputer próbuje nawiązać połączenie z routerem bezprzewodowym. Po nawiązaniu połączenia komputer programuje klucz szyfrowana na routerze bezprzewodowym. Jeśli domyślne hasło zostało zmienione, program Wireless Network Security monituje o hasło, aby skonfigurować na routerze bezprzewodowym współdzielony klucz szyfrowania w trybie silnych zabezpieczeń. Także na komputerze jest konfigurowany ten sam współdzielony klucz i tryb szyfrowania, co pozwala nawiązać bezpieczne połączenie bezprzewodowe.

Uruchamianie programu Wireless Network Security

Program Wireless Network Security jest domyślnie włączony; ochronę bezprzewodową można jednak włączyć lub wyłączyć ręcznie.

Włączenie ochrony bezprzewodowej zabezpiecza sieć bezprzewodową przed włamaniem i przechwyceniem danych. Jeśli jednak komputer jest połączony z zewnętrzną siecią bezprzewodową, skuteczność ochrony zależy od poziomu zabezpieczeń tej sieci.

Aby ręcznie włączyć ochronę bezprzewodową:

1. W okienku programu McAfee SecurityCenter wykonaj jedną z następujących czynności:
   - Kliknij opcję **Internet i sieć**, a następnie opcję **Konfiguruj**.
   - Kliknij opcję **Menu zaawansowane**, następnie opcję **Konfiguruj** w okienku **Strona główna**, a potem wybierz opcję **Internet i sieć**.
2. W okienku **Konfiguracja Internetu i sieci**, w obszarze **Ochrona bezprzewodowa** kliknij opcję **Włącz**.

Uwaga: Program Wireless Network Security jest automatycznie włączany, jeśli w komputerze zainstalowano zgodną kartę sieci bezprzewodowej.

Zatrzymywanie programu Wireless Network Security

Program Wireless Network Security jest domyślnie włączony; ochronę bezprzewodową można jednak włączyć lub wyłączyć ręcznie.

Wyłączenie ochrony bezprzewodowej naraża komputer na włamania i przechwycenie danych.

Aby wyłączyć ochronę bezprzewodową:

1 W okienku programu McAfee SecurityCenter wykonaj jedną z następujących czynności:

- Kliknij opcję **Internet i sieć**, a następnie opcję **Konfiguruj**.
- Kliknij opcję **Menu zaawansowane**, następnie opcję **Konfiguruj** w okienku **Strona główna**, a potem wybierz opcję **Internet i sieć**.

2 W okienku **Konfiguracja Internetu i sieci**, w obszarze **Ochrona bezprzewodowa** kliknij opcję **Wyłącz**.

ROZDZIAŁ 41

Ochrona sieci bezprzewodowych

Program Wireless Network Security chroni sieć, stosując szyfrowanie komunikacji bezprzewodowej (WEP, WPA lub WPA2, w zależności od urządzenia). Automatycznie programuje on na klientach i routerach bezprzewodowych poprawne poświadczenia (klucze szyfrujące), dzięki którym router bezprzewodowy upoważnia komputery do nawiązania połączenia. Sieci bezprzewodowe chronione szyfrowaniem blokują nieautoryzowanym użytkownikom możliwość uzyskania dostępu do sieci i chronią dane przesyłane przez nią. Aby to osiągnąć, program Wireless Network Security:

- tworzy i rozpowszechnia długi, silny, losowy i współdzielony klucz szyfrowania;
- cyklicznie zmienia klucze szyfrowania zgodnie z ustalonym planem;
- konfiguruje każde urządzenie bezprzewodowe za pomocą kluczy szyfrowania.

W tym rozdziale

Konfigurowanie zabezpieczonych sieci bezprzewodowych 290
Dodawanie komputerów do chronionej sieci bezprzewodowej 302

Konfigurowanie zabezpieczonych sieci bezprzewodowych

Po zainstalowaniu program Wireless Network Security automatycznie monituje o włączenie ochrony niezabezpieczonej sieci bezprzewodowej, z którą użytkownik jest połączony, lub dołączenie do już chronionej sieci bezprzewodowej.

Jeśli użytkownik nie jest połączony z siecią bezprzewodową, program Wireless Network Security skanuje w poszukiwaniu sieci chronionej przez produkty firmy McAfee i mającej silny sygnał, a następnie monituje o dołączenie do niej. Jeśli żadne chronione sieci nie są dostępne, program Wireless Network Security skanuje w poszukiwaniu niezabezpieczonych sieci mających silny sygnał i, jeśli znajdzie taką sieć, monituje o włączenie jej ochrony.

Jeśli sieć bezprzewodowa nie jest chroniona przez program McAfee Wireless Network Security, firma McAfee uznaje ją za „niechronioną” — nawet jeśli używa mechanizmów zabezpieczających, na przykład WEP lub WPA.

Jeśli sieć bezprzewodowa nie jest chroniona przez program Wireless Network Security, firma McAfee uznaje ją za niechronioną, nawet jeśli stosuje mechanizmy zabezpieczające komunikację bezprzewodową, jak WEP i WPA.

Typy dostępu — informacje

Każdy komputer bezprzewodowy z zainstalowanym programem Wireless Network Security może tworzyć chronioną sieć bezprzewodową. Pierwszemu komputerowi w sieci, chroniącemu router i tworzącemu chronioną sieć bezprzewodową, automatycznie przyznawany jest dostęp administracyjny do danej sieci. Istniejący użytkownik z dostępem administracyjnym może przyznawać komputerom dołączającym do sieci później dostęp administracyjny, pełny lub typu Gość.

Komputery z dostępem administracyjnym i pełnym mogą wykonywać następujące zadania:

- chronić i usuwać router lub punkt dostępu,
- zmieniać klucze bezpieczeństwa,
- zmieniać ustawienia zabezpieczeń sieci,
- naprawiać sieci,
- przyznawać komputerom dostęp do sieci,
- odwoływać dostęp do chronionej sieci bezprzewodowej,
- zmieniać poziom administracyjny komputera.

Komputery z dostępem typu Gość mogą wykonywać w sieci następujące zadania:

- łączyć się z siecią,
- dołączać do sieci,
- modyfikować ustawienia specyficzne dla komputera-gościa.

Uwaga: Komputer może mieć dostęp administracyjny do jednej sieci, ale tylko dostęp typu Gość lub pełny do innej. Komputer z dostępem typu Gość lub pełnym może utworzyć nową sieć.

Tematy pokrewne

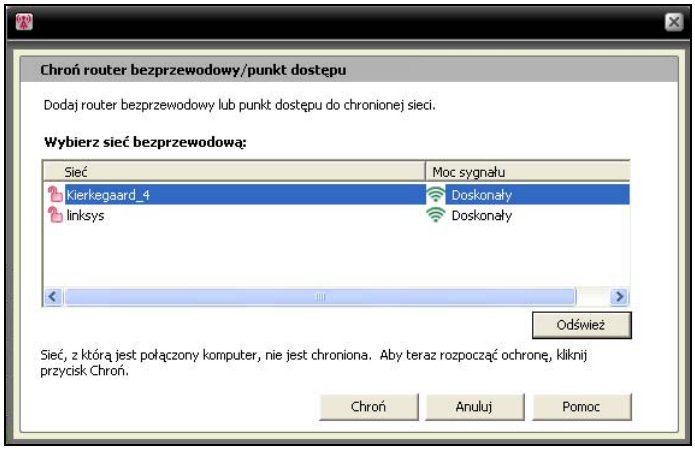
- Dołączanie do chronionej sieci bezprzewodowej (strona 294)
- Przyznawanie komputerom dostępu administracyjnego (strona 298)
- Odwoływanie dostępu do sieci (strona 317)

Tworzenie chronionych sieci bezprzewodowych

Aby utworzyć chronioną sieć bezprzewodową, należy najpierw dodać jej router bezprzewodowy lub punkt dostępu.

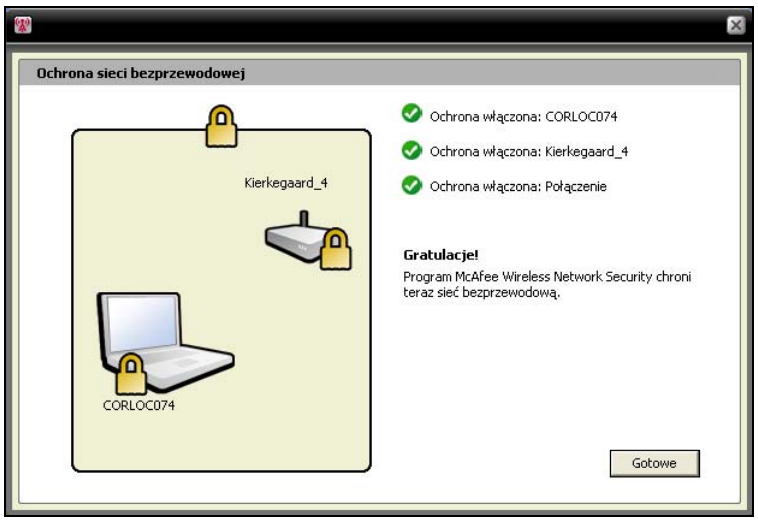
Aby dodać router bezprzewodowy lub punkt dostępu:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl narzędzia**.
3. W okienku Narzędzia ochrony, w obszarze **Chroń router bezprzewodowy/punkt dostępu** kliknij polecenie **Chroń**.
4. W okienku Chroń router bezprzewodowy/punkt dostępu zaznacz sieć bezprzewodową, która ma być chroniona, a następnie kliknij polecenie **Chroń**.



W czasie, gdy program Wireless Network Security próbuje włączyć ochronę komputera, routera i połączenia sieciowego, pojawia się okienko Ochrona sieci bezprzewodowej.

Pomyślne włączenie ochrony tych składników gwarantuje pełną ochronę sieci bezprzewodowej.



5 Kliknij przycisk **Gotowe**.

Uwaga: Po włączeniu ochrony sieci okno dialogowe Kolejne kroki przypomina, że program Wireless Network Security należy zainstalować na każdym komputerze bezprzewodowym, aby umożliwić im dołączenie do sieci.

Jeśli istnieje skonfigurowany wcześniej ręcznie klucz wstępny dla routera lub punktu dostępu, a użytkownik nie był połączony w czasie próby włączenia ochrony routera lub punktu dostępu, należy także wprowadzić klucz w polu Klucz WEP, a następnie kliknąć przycisk Połącz. Jeśli nazwa administratora routera bezprzewodowego i jego hasło zostały zmienione, przed włączeniem ochrony routera lub punktu dostępu program monituje o wprowadzenie tych informacji.

Tematy pokrewne

- Chronienie innych urządzeń bezprzewodowych (strona 300)
- Dodawanie komputerów do chronionej sieci bezprzewodowej (strona 302)

Dołączanie do chronionych sieci bezprzewodowych

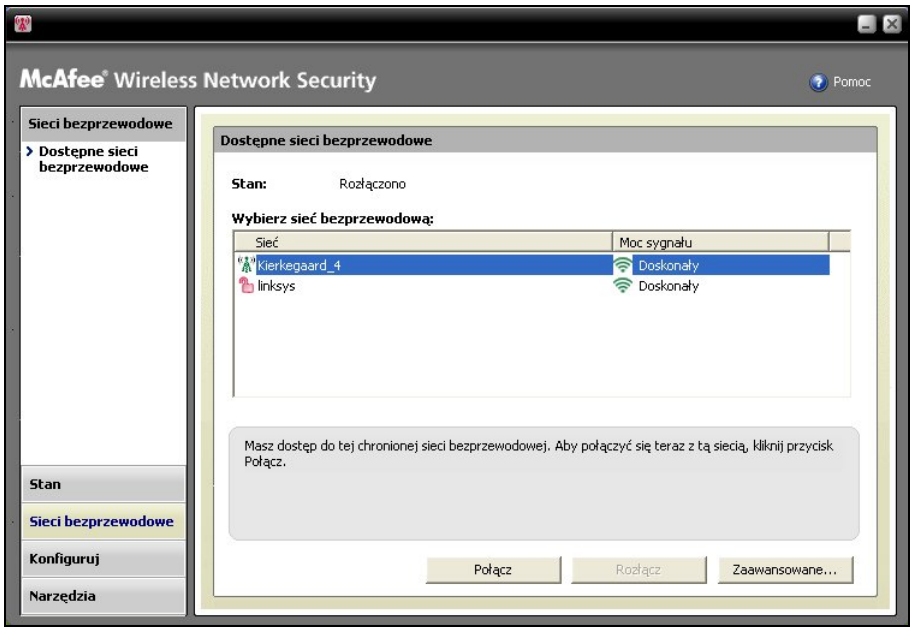
Chroniona sieć bezprzewodowa uniemożliwia hakerom przechwytywanie danych przesyłanych przez nią i podłączanie się do niej. Aby nieupoważniony komputer mógł uzyskać dostęp do chronionej sieci bezprzewodowej, musi najpierw do niej dołączyć.

Gdy komputer żąda dołączenia do zarządzanej sieci, do komputerów w sieci mających uprawnienia administracyjne jest wysyłany komunikat. Jego administrator jest odpowiedzialny za decyzję, który typ dostępu przyznać komputerowi: gość, pełny czy administrator.

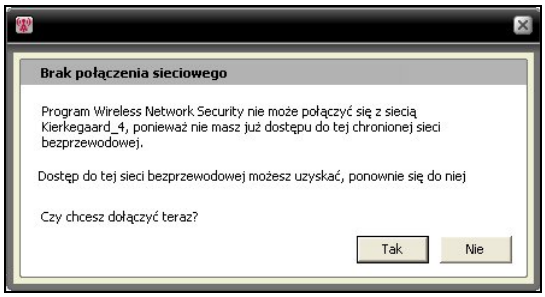
Przed dołączeniem do chronionej sieci należy zainstalować Wireless Network Security, a następnie połączyć się z chronioną siecią bezprzewodową. Do dołączenia się do sieci wymagane jest zezwolenie od użytkownika z dostępem administracyjnym do chronionej sieci bezprzewodowej. Po dołączeniu do sieci ponowne łączenie się z nią nie wymaga powtórnego dołączania do niej. Zarówno użytkownik przyznający dostęp, jak i dołączający muszą mieć aktywne połączenie bezprzewodowe. Komputer przyznający dostęp musi mieć dostęp administracyjny i być połączony z siecią.

Aby dołączyć do chronionej sieci bezprzewodowej:

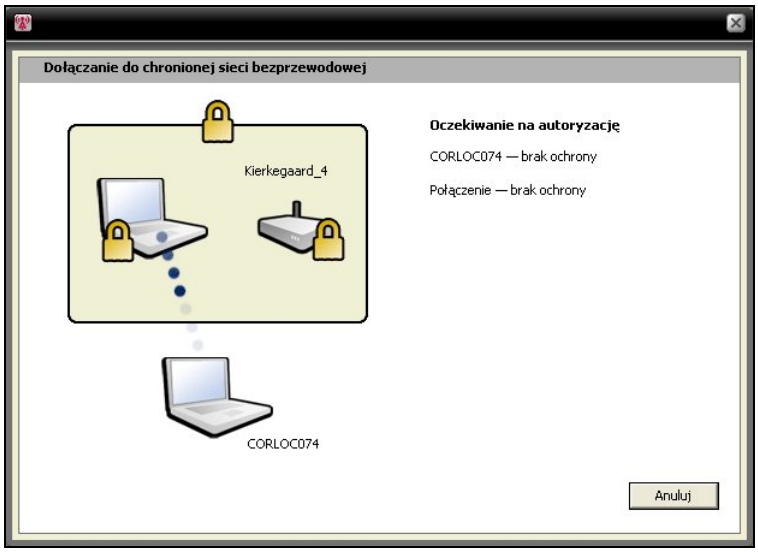
1. Na niechronionym komputerze kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl sieci bezprzewodowe**.
3. W okienku Dostępne sieci bezprzewodowe zaznacz sieć, a następnie kliknij polecenie **Połącz**.



4 W oknie dialogowym Dołącz do chronionej sieci bezprzewodowej kliknij przycisk **Tak**, aby dołączyć do sieci.



Program Wireless Network Security żąda uprawnienia do dołączenia do sieci, a na komputerze próbującym dołączyć do sieci pojawia się okno dialogowe Dołączanie do chronionej sieci bezprzewodowej.



5 Na komputerze administratora pojawia się okienko dołączania do sieci, w którym może on przyznać dostęp typu Gość, pełny lub administracyjny.

W oknie dialogowym Dołącz do sieci należy wybrać jedną z następujących opcji:

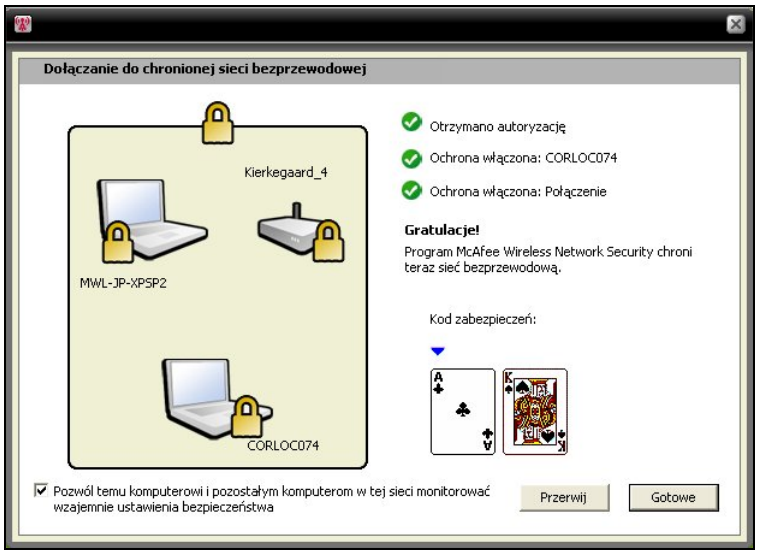
Przyznaj dostęp typu Gość	Pozwala komputerowi na wysyłanie plików do innych komputerów w sieci bezprzewodowej, ale nie na udostępnianie ich za pomocą programu McAfee EasyNetwork.
Przyznaj dostęp Pełny do wszystkich zarządzanych aplikacji sieciowych	Pozwala komputerowi na wysyłanie plików i udostępnianie ich za pomocą programu McAfee EasyNetwork.
Przyznaj dostęp Administrator do wszystkich zarządzanych aplikacji sieciowych	Pozwala komputerowi na wysyłanie plików i udostępnianie ich za pomocą programu McAfee EasyNetwork, przyznawanie dostępu pozostałym komputerom oraz zmianę poziomów uprawnień w sieci bezprzewodowej innych komputerów.

6 Kliknij opcję **Przyznaj prawa dostępu**.

7 Sprawdź, czy karty do gry wyświetlane w okienku Przyznawanie praw dostępu do sieci są identyczne z wyświetlanymi na komputerze dołączającym do sieci bezprzewodowej. Jeżeli są to takie same karty, kliknij przycisk **Przyznaj prawa dostępu**.

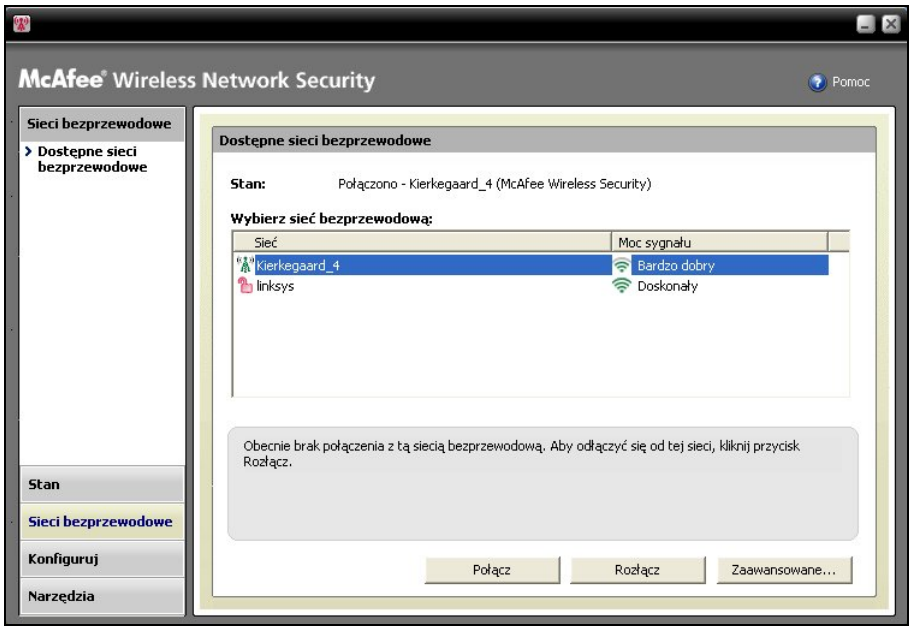
Jeśli na komputerach nie są wyświetlane identyczne karty, mogło nastąpić naruszenie zabezpieczeń. Przyznanie temu komputerowi dostępu do sieci może stanowić zagrożenie dla komputera. Aby uniemożliwić temu komputerowi uzyskanie dostępu do sieci bezprzewodowej, kliknij przycisk **Odmów dostępu**.

8 W okienku Przyznawanie praw dostępu do sieci pojawi się potwierdzenie, że nowy komputer jest chroniony przez program Wireless Network Security. Aby umożliwić monitorowanie ustawień zabezpieczeń innych komputerów i monitorowanie zabezpieczeń swojego komputera przez inne komputery, kliknij opcję **Pozwól temu komputerowi i pozostałym komputerom w tej sieci monitorować wzajemnie ustawienia bezpieczeństwa**.



9 Kliknij przycisk **Gotowe**.

10 Zawartość okienka Dostępne sieci bezprzewodowe potwierdza, że komputer jest połączony z chronioną siecią bezprzewodową.



Tematy pokrewne

- Dodawanie komputerów do chronionej sieci bezprzewodowej (strona 302)

Łączenie z chronionymi sieciami bezprzewodowymi

Jeżeli użytkownik dołączył już do chronionej sieci bezprzewodowej, ale później rozłączył się, a jego dostęp nie został odwołany, może połączyć się z siecią ponownie, bez konieczności powtórnego dołączania.

Aby połączyć się z chronioną siecią bezprzewodową:

1 Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.

2 Wybierz polecenie **Wyświetl sieci bezprzewodowe**.

3 W okienku Dostępne sieci bezprzewodowe zaznacz sieć, a następnie kliknij polecenie **Połącz**.

Przyznawanie komputerom dostępu administracyjnego

Komputery z uprawnieniami administratora mogą chronić routery bezprzewodowe, zmieniać tryby zabezpieczeń i przyznawać prawa dostępu do chronionej sieci bezprzewodowej innym komputerom.

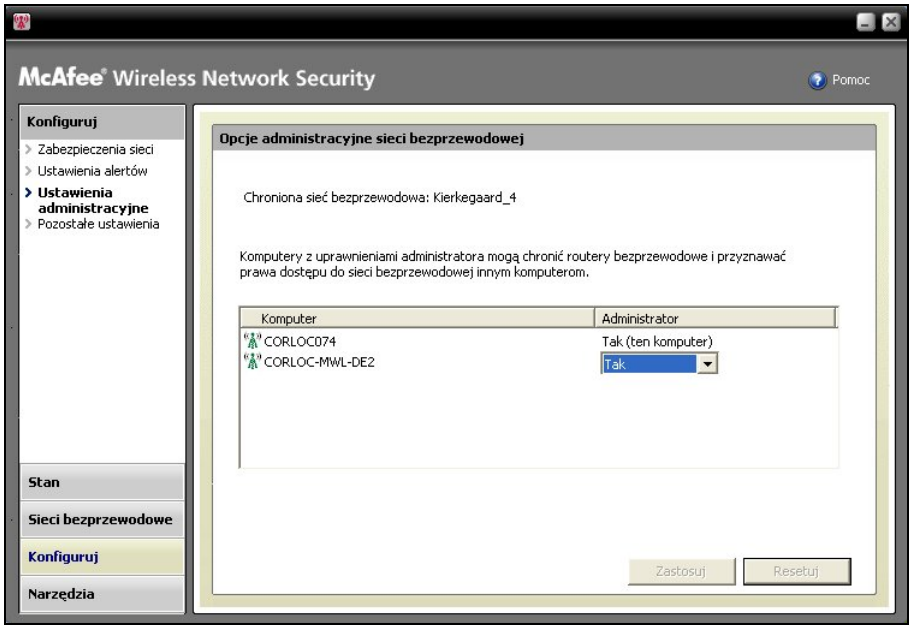
Aby skonfigurować dostęp administracyjny:

1 Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.

2 Wybierz polecenie **Wyświetl konfigurację**.

3 W okienku konfiguracji kliknij opcję **Ustawienia administracyjne**.

4 W okienku Opcje administracyjne sieci bezprzewodowej wybierz opcję **Tak** lub **Nie**, aby zezwolić lub nie zezwolić na dostęp administracyjny.



5 Kliknij przycisk **Zastosuj**.

Tematy pokrewne

- Typy dostępu — informacje (strona 291)
- Odwoływanie dostępu do sieci (strona 317)

Chronienie innych urządzeń bezprzewodowych

Program Wireless Network Security pozwala dodawać do sieci jedną lub większą liczbę bezprzewodowych drukarek, serwerów druku i konsol do gier.

Aby dodać bezprzewodową drukarkę, serwer druku lub konsolę do gier:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl narzędzia**.
3. W okienku Narzędzia ochrony, w obszarze **Chroń urządzenie nie będące punktem dostępu** kliknij polecenie **Chroń**.
4. W okienku Chroń urządzenie bezprzewodowe zaznacz urządzenie bezprzewodowe, a następnie kliknij polecenie **Chroń**.
5. Alert Włączono ochronę urządzenia nie będącego punktem dostępu potwierdza, że urządzenie zostało dodane do sieci.

Łączenie z sieciami z wyłączonym rozgłaszaniem SSID

Połączenie z sieciami bezprzewodowymi, które mają wyłączone rozgłaszanie SSID, jest niemożliwe. Routery, które mają wyłączone rozgłaszanie SSID, nie pojawiają się w okienku Dostępne sieci bezprzewodowe.

Firma McAfee zaleca nie chronić routerów bezprzewodowych, które mają wyłączone rozgłaszanie SSID, za pomocą programu Wireless Network Security.

Aby połączyć się z siecią bezprzewodową, która ma wyłączone rozgłaszanie SSID:

1 Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.

2 Wybierz polecenie **Wyświetl sieci bezprzewodowe**.

3 W okienku Dostępne sieci bezprzewodowe kliknij opcję **Zaawansowane**.

4 W okienku Sieci bezprzewodowe kliknij opcję **Dodaj**.

5 W okienku Dodaj sieć bezprzewodową określ następujące ustawienia, a następnie kliknij przycisk **OK**:

Ustawienie	Opis
Sieć	Nazwa sieci. Jeśli sieć jest modyfikowana, tej nazwy nie można zmienić.
Ustawienia zabezpieczeń	Zabezpieczenia niechronionej sieci. Należy zwrócić uwagę, że jeśli karta sieci bezprzewodowej nie obsługuje wybranego trybu, nawiązanie połączenia jest niemożliwe. Dostępne tryby zabezpieczeń to: Wyłączone, Otwarte WEP, Współdzielone WEP, Automatyczne WEP, WPA-PSK i WPA2-PSK.
Tryb szyfrowania	Szyfrowanie powiązane z wybranym trybem zabezpieczeń. Dostępne tryby szyfrowania to: WEP, TKIP, AES i TKIP+AES.

Uwaga: Firma McAfee zaleca nie chronić routerów bezprzewodowych, które mają wyłączone rozgłaszanie SSID, za pomocą programu Wireless Network Security. Jeżeli użycie tej funkcji jest wymagane, należy ją stosować tylko w sytuacji, gdy rozgłaszanie SSID jest wyłączone.

Dodawanie komputerów do chronionej sieci bezprzewodowej

Komputery można dodawać do chronionej sieci bezprzewodowej za pomocą urządzenia wymiennego, na przykład dysku flash USB lub płyty CD do wielokrotnego zapisu, bądź za pomocą technologii Windows Connect Now.

Dodawanie komputerów za pomocą urządzenia wymiennego

Program Wireless Network Security pozwala dodawać do chronionej sieci bezprzewodowej komputery, na których nie ma programu Wireless Network Security, za pomocą dysku flash USB lub płyty CD do wielokrotnego zapisu.

Aby dodać komputer:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl narzędzia**.
3. W okienku Narzędzia ochrony, w obszarze **Chroń komputer** kliknij polecenie **Chroń**.
4. W okienku Ochrona innego komputera wybierz polecenie **Skopiuj program na wymienne urządzenie, takie jak klucz USB**.

5 Wybierz lokalizację napędu CD lub dysku flash USB, na który zostanie skopiowany program Wireless Network Security.

6 Kliknij przycisk **Kopiuj**.

7 Po skopiowaniu wszystkich plików na płytę CD lub dysk flash USB włóż urządzenie wymienne do komputera, który ma być chroniony. Jeśli program nie uruchomi się automatycznie, w programie Windows Explorer odszukaj na nośniku wymiennym plik **Install.exe** i kliknij go.

8 Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Uwaga: Komputer można dodać do chronionej sieci bezprzewodowej także za pomocą technologii Windows Connect Now.

Tematy pokrewne

- Dodawanie komputerów za pomocą technologii Windows Connect Now (strona 304)

Dodawanie komputerów za pomocą technologii Windows Connect Now

Program Wireless Network Security pozwala dodawać do chronionej sieci bezprzewodowej komputery, na których nie ma programu Wireless Network Security, za pomocą technologii Windows Connect Now.

Aby dodać komputer za pomocą technologii Windows Connect Now:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl narzędzia**.
3. W okienku Narzędzia ochrony, w obszarze **Chroń komputer** kliknij polecenie **Chroń**.
4. W okienku Ochrona innego komputera wybierz polecenie **Utwórz dysk Windows Connect Now**.
5. Wybierz lokalizację, do której zostaną skopiowane informacje Windows Connect Now.
6. Kliknij przycisk **Kopiuj**.
7. Włóż dysk Windows Connect Now do komputera, który ma być chroniony.
8. Jeśli dysk nie uruchomi się automatycznie, wykonaj jedną z następujących czynności:
   - Zainstaluj technologię Windows Connect Now: Na pasku zadań systemu Windows kliknij przycisk **Start**, a następnie kliknij polecenie Panel sterowania. W przypadku używania widoku kategorii Panelu sterowania kliknij pozycję **Połączenia sieciowe i internetowe**, a następnie pozycję **Kreator sieci bezprzewodowej**. W przypadku używania widoku klasycznego Panelu sterowania kliknij pozycję **Kreator sieci bezprzewodowej**. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
   - Otwórz plik `setupSNK.exe` na dysku Windows Connect Now, a następnie skopiuj i wklej klucz w interfejsie klienta wyboru sieci bezprzewodowej.

Uwaga: W przypadku łączenia z siecią za pomocą technologii Windows Connect Now należy wstrzymać cykliczną zmianę klucza. W przeciwnym razie nawiązanie połączenia sieciowego będzie niemożliwe. Próba połączenia zakończy się niepowodzeniem, ponieważ w wyniku cyklicznej zmiany klucza tworzony jest nowy klucz, inny niż użyty przez technologię Windows Connect Now.

Komputery można dodawać do chronionej sieci bezprzewodowej za pomocą urządzenia wymiennego, na przykład dysku flash USB lub płyty CD do wielokrotnego zapisu.

Tematy pokrewne

- Dodawanie komputerów za pomocą urządzenia wymiennego (strona 302)

ROZDZIAŁ 42

Administrowanie sieciami bezprzewodowymi

Program Wireless Network Security zapewnia pełny zestaw narzędzi administracyjnych, które pomagają w zarządzaniu siecią bezprzewodową i utrzymywaniu jej.

W tym rozdziale

Zarządzanie sieciami bezprzewodowymi.....308

Zarządzanie sieciami bezprzewodowymi

Informacje wysyłane i odbierane w czasie połączenia z chronioną siecią bezprzewodową są szyfrowane. Hakerzy nie mogą odszyfrować danych przesyłanych przez chronioną sieć i nie mogą połączyć się z nią. Program Wireless Network Security zapewnia szereg narzędzi, które pomagają w zarządzaniu siecią i zapobieganiu włamaniom sieciowym.

Ikony programu Wireless Network Security — informacje

Ikony programu Wireless Network Security reprezentują różne typy połączeń sieciowych i poziomy mocy sygnału.

Ikony połączenia sieciowego

Poniższa tabela opisuje ikony często używane przez program Wireless Network Security w okienkach Stan sieci bezprzewodowej, Narzędzia ochrony i Dostępne sieci bezprzewodowe. Ikony reprezentują różne stany połączenia sieciowego i zabezpieczeń.

Ikona	Okienka stanu	Okienka zabezpieczeń
	Komputer jest połączony z wybraną chronioną siecią bezprzewodową.	Urządzenie jest chronione przez program Wireless Network Security.
	Komputer ma dostęp do chronionej sieci bezprzewodowej, ale nie jest aktualnie połączony.	Urządzenie ma zabezpieczenia WEP lub WPA.
	Komputer był członkiem chronionej sieci bezprzewodowej, ale dostęp został odwołany po rozłączeniu komputera z siecią.	Urządzenie ma wyłączony program Wireless Network Security.

Ikony mocy sygnału

Poniższa tabela opisuje ikony często używane przez program Wireless Network Security do reprezentowania różnych poziomów mocy sygnału.

Ikona	Opis
	Doskonała moc sygnału
	Bardzo dobra moc sygnału
	Dobra moc sygnału
	Niska moc sygnału

Tematy pokrewne

- Wyświetlanie mocy sygnału sieci (strona 339)
- Wyświetlanie aktualnie chronionych komputerów (strona 346)
- Wyświetlanie trybu zabezpieczeń sieci (strona 338)

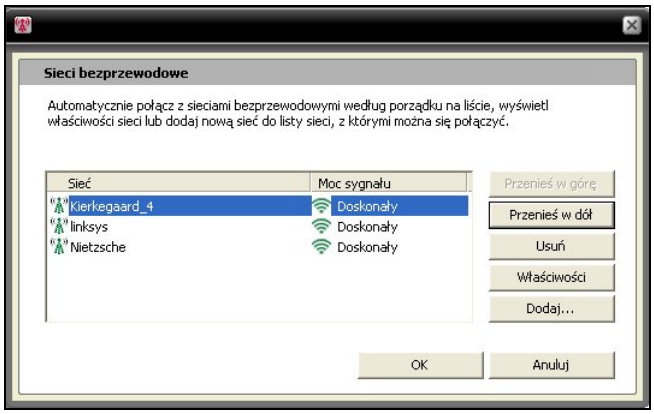
Wyświetlanie listy preferowanych sieci

Program Wireless Network Security pozwala określać preferowane sieci bezprzewodowe. Umożliwia to określanie porządku sieci, z którymi komputer automatycznie się łączy. Program Wireless Network Security próbuje połączyć się z pierwszą siecią na liście.

Tak funkcja jest przydatna na przykład w sytuacji, gdy użytkownik chce połączyć się z siecią bezprzewodową należącą do innej osoby, z dala od swojego miejsca zamieszkania. Sieć tę można przenieść na początek listy.

Aby wyświetlić listę preferowanych sieci:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl sieci bezprzewodowe**.
3. W okienku Dostępne sieci bezprzewodowe kliknij opcję **Zaawansowane**.
4. Zaznacz sieć, której pozycję chcesz zmienić, i kliknij przycisk **Przenieś w górę** lub **Przenieś w dół**.



5. Kliknij przycisk **OK**.

Tematy pokrewne

- Usuwanie preferowanych sieci bezprzewodowych (strona 311)

Usuwanie preferowanych sieci bezprzewodowych

Programu Wireless Network Security można używać do usuwania preferowanych sieci.

Jest to przydatne na przykład w przypadku usuwania nieaktualnych sieci z listy.

Aby usunąć preferowane sieci:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl sieci bezprzewodowe**.
3. W okienku Dostępne sieci bezprzewodowe kliknij opcję **Zaawansowane**.
4. W okienku Sieci bezprzewodowe zaznacz sieć, a następnie kliknij polecenie **Usuń**.
5. Kliknij przycisk **OK**.

Tematy pokrewne

- Wyświetlanie listy preferowanych sieci (strona 310)

Zmienianie nazw chronionych sieci bezprzewodowych

Za pomocą programu Wireless Network Security można zmieniać nazwy istniejących chronionych sieci bezprzewodowych.

Zmiana nazwy sieci jest pomocna, jeśli jest ona podobna lub taka sama jak używana w sąsiedztwie albo gdy użytkownik chce utworzyć nazwę unikatową i łatwiejszą do rozpoznania.

Komputery połączone z chronioną siecią bezprzewodową mogą wymagać powtórnego ręcznego nawiązania połączenia i są informowane o zmianie nazwy.

Po zmianie nazwy sieci jej nowa nazwa pojawia się w okienku Chroniony router bezprzewodowy/punkt dostępu.

Aby zmodyfikować nazwę chronionej sieci bezprzewodowej:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl konfigurację**.
3. Wpisz nową nazwę w polu **Nazwa chronionej sieci bezprzewodowej** okienka Zabezpieczenia sieci.
4. Kliknij przycisk **Zastosuj**.

   W czasie, gdy program Wireless Network Security zmienia nazwę chronionej sieci bezprzewodowej, jest wyświetlane okno dialogowe Aktualizacja ustawień zabezpieczeń sieci. Zmiana nazwy sieci trwa mniej niż minutę, ale zależy od ustawień komputera i mocy sygnału.

Uwaga: Firma McAfee jako działanie zabezpieczające zaleca zmianę domyślnego identyfikatora SSID routera lub punktu dostępu. Mimo że program Wireless Network Security obsługuje domyślne identyfikatory SSID, na przykład „linksys", „belkin54g" lub „NETGEAR", zmiana identyfikatora SSID chroni przed zagrożeniami ze strony nieautoryzowanych punktów dostępu.

Konfigurowanie ustawień alertów

Program Wireless Network Security pozwala konfigurować ustawienia alertów tak, aby były wyświetlane w przypadku wystąpienia określonych zdarzeń, na przykład połączenia nowego komputera z siecią.

Aby skonfigurować zachowanie alertów:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl konfigurację**.
3. Kliknij ikonę **Ustawienia alertu**.
4. Zaznacz lub wyczyść pola jednego lub większej liczby poniższych zdarzeń, a następnie kliknij przycisk **Zastosuj**.

Ustawienie alertu	Opis
Dokonano cyklicznej zmiany klucza szyfrującego chronionej sieci bezprzewodowej.	Wyświetla alert Wykonano cykliczną zmianę klucza bezpieczeństwa po dokonaniu ręcznej lub automatycznej cyklicznej zmiany klucza bezpieczeństwa. Cykliczne zmiany klucza zapobiegają przechwytywaniu danych użytkownika lub podłączaniu się do jego sieci przez hakerów.
Z siecią połączył się lub odłączył się od niej kolejny chroniony komputer.	Wyświetla alert Połączono komputer lub Odłączono komputer po połączeniu lub rozłączeniu komputera z chronioną siecią bezprzewodową. Dane na połączonych komputerach są od teraz chronione przed włamaniami i przechwyceniem.
Przyznano prawa dostępu do chronionej sieci bezprzewodowej kolejnemu komputerowi.	Wyświetla alert Komputerowi przyznano dostęp do sieci po udzieleniu przez komputer administratora innemu komputerowi zezwolenia na dołączenie do chronionej sieci bezprzewodowej. Przyznanie komputerowi dostępu do chronionej sieci chroni go przed przechwytywaniem danych użytkownika przez hakerów.
Wstrzymano lub wznowiono cykliczną zmianę klucza chronionej sieci bezprzewodowej.	Wyświetla alert Wstrzymano cykliczną zmianę klucza lub Wznowiono cykliczną zmianę klucza po ręcznym wstrzymaniu lub wznowieniu cyklicznej zmiany klucza. Cykliczne zmiany klucza zapobiegają przechwytywaniu danych użytkownika lub podłączaniu się do jego sieci przez hakerów.
Odwołano prawa dostępu wszystkich odłączonych komputerów.	Wyświetla alert Unieważniono dostęp po odwołaniu praw dostępu komputerów niepołączonych z siecią. Rozłączone komputery muszą powtórnie przyłączyć się do sieci.
Do chronionej sieci bezprzewodowej dodano lub usunięto z niej router.	Wyświetla alert Do sieci dodano router/punkt dostępu lub Niechroniony router/punkt dostępu po dodaniu do chronionej sieci bezprzewodowej lub usunięciu z niej bezprzewodowego routera lub punktu dostępu.
Zmieniono informacje logowania do chronionego routera bezprzewodowego.	Wyświetla alert Zmieniono informacje logowania routera/punktu dostępu po dokonaniu przez administratora programu Wireless Network Security zmiany nazwy użytkownika lub hasła routera lub punktu dostępu.

Zmieniono nazwę lub ustawienie zabezpieczeń chronionej sieci bezprzewodowej.	Wyświetla alert Zmieniono ustawienia sieci lub Zmieniono nazwę sieci po dokonaniu przez użytkownika zmiany nazwy chronionej sieci bezprzewodowej lub jej ustawień zabezpieczeń.
Naprawiono ustawienia chronionej sieci bezprzewodowej.	Wyświetla alert Sieć została naprawiona po naprawieniu ustawień zabezpieczeń bezprzewodowego routera lub punktu dostępu w sieci.

Uwaga: Aby zaznaczyć lub wyczyścić wszystkie ustawienia, można kliknąć opcję **Zaznacz wszystko** lub **Wyczyść wszystko**. Aby zresetować ustawienia zabezpieczeń programu Wireless Network Security, należy kliknąć opcję **Przywróć ustawienia domyślne**.

Tematy pokrewne

- Automatyczna cykliczna zmiana klucza (strona 326)
- Dołączanie do chronionej sieci bezprzewodowej (strona 294)
- Łączenie z chronionymi sieciami bezprzewodowymi (strona 298)
- Rozłączanie z chronionymi sieciami bezprzewodowymi (strona 316)
- Wstrzymywanie automatycznej cyklicznej zmiany klucza (strona 329)
- Odwoływanie dostępu do sieci (strona 317)
- Usuwanie routerów bezprzewodowych lub punktów dostępu (strona 315)
- Zmienianie poświadczeń dla urządzeń bezprzewodowych (strona 323)
- Zmienianie nazw chronionych sieci bezprzewodowych (strona 311)
- Naprawianie ustawień zabezpieczeń sieci (strona 324)

Wyświetlanie powiadomień o połączeniach

Program Wireless Network Security można skonfigurować tak, aby powiadamiał o połączeniu komputera z siecią bezprzewodową.

Aby wyświetlić powiadomienie o połączeniu z siecią bezprzewodową:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl konfigurację**.
3. Kliknij ikonę **Inne ustawienia**.
4. Zaznacz opcję **Po połączeniu z siecią bezprzewodową wyświetl komunikat z powiadomieniem**.
5. Kliknij przycisk **Zastosuj**.

Tematy pokrewne

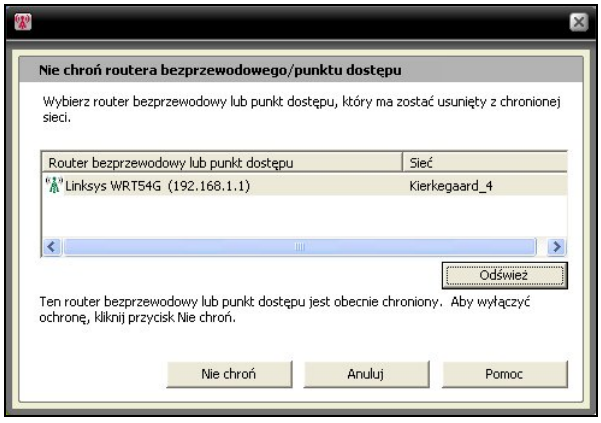
- Łączenie z chronionymi sieciami bezprzewodowymi (strona 298)

Usuwanie routerów bezprzewodowych lub punktów dostępu

Program Wireless Network Security pozwala usuwać dowolną liczbę routerów lub punktów dostępu z chronionej sieci.

Aby usunąć router bezprzewodowy lub punkt dostępu:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl narzędzia**.
3. W okienku Narzędzia ochrony, w obszarze **Nie chroń urządzenia** kliknij polecenie **Nie chroń**.
4. W okienku Nie chroń routera bezprzewodowego/punktu dostępu zaznacz router bezprzewodowy lub punkt dostępu, który ma zostać usunięty z chronionej sieci, a następnie kliknij polecenie **Nie chroń**.



5 Kliknij przycisk **OK** w oknie dialogowym Niechroniony router bezprzewodowy/punkt dostępu, aby potwierdzić usunięcie routera bezprzewodowego/punktu dostępu z sieci.

Tematy pokrewne

- Tworzenie chronionych sieci bezprzewodowych (strona 292)

Rozłączanie z chronionymi sieciami bezprzewodowymi

Program Wireless Network Security pozwala komputerowi rozłączać się z siecią.

Jest to przydatne na przykład w sytuacji, gdy komputer połączył się z siecią, używając nazwy identycznej jak nazwa sieci. Użytkownik może rozłączyć się z tą siecią i połączyć z własną.

Funkcja jest przydatna także w sytuacji przypadkowego połączenia się z nieprawidłową siecią, z powodu mocy sygnału jej punktu dostępu lub z powodu interferencji radiowych.

Aby rozłączyć się z chronioną siecią bezprzewodową:

1 Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.

2 Wybierz polecenie **Wyświetl sieci bezprzewodowe**.

3 W okienku Dostępne sieci bezprzewodowe zaznacz sieć, a następnie kliknij polecenie **Rozłącz**.

Tematy pokrewne

- Odwoływanie dostępu do sieci (strona 317)
- Opuszczanie chronionych sieci bezprzewodowych (strona 318)

Odwoływanie dostępu do sieci

Program Wireless Network Security pozwala odwołać prawa dostępu do sieci komputerów, które nie są z nią połączone. Tworzony jest w tym celu nowy plan cyklicznych zmian klucza bezpieczeństwa: komputery niepołączone z chronioną siecią bezprzewodową stracą do niej dostęp, ale mogą go odzyskać, powtórnie dołączając do sieci. Dostęp komputerów połączonych jest zachowywany.

Można na przykład odwołać prawa dostępu komputera gościa po jego rozłączeniu. Ponadto, osoba dorosła może odwołać prawa dostępu komputera używanego przez dziecko, kontrolując w ten sposób jego dostęp do Internetu. Odwołać można także prawa dostępu komputera, któremu przyznano je omyłkowo.

Aby odwołać prawa dostępu wszystkich komputerów rozłączonych z siecią chronioną:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl narzędzia**.
3. W okienku Narzędzia kliknij opcję Narzędzia konserwacji.
4. W okienku Narzędzia konserwacji, w obszarze **Odwołaj prawa dostępu** kliknij polecenie **Odwołaj**.
5. W okienku Odwołaj prawa dostępu kliknij przycisk **Odwołaj**.
6. Kliknij przycisk **OK** w oknie programu Wireless Network Security.

Tematy pokrewne

- Rozłączanie z chronionymi sieciami bezprzewodowymi (strona 316)
- Opuszczanie chronionych sieci bezprzewodowych (strona 318)

Opuszczanie chronionych sieci bezprzewodowych

Za pomocą programu Wireless Network Security można anulować swoje prawa dostępu do chronionej sieci.

Aby opuścić sieć:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl konfigurację**.
3. W okienku konfiguracji kliknij opcję **Inne ustawienia**.
4. W okienku Inne ustawienia, w obszarze Dostęp do chronionej sieci zaznacz sieć, którą chcesz opuścić, a następnie kliknij polecenie **Opuść sieć**.
5. W okienku Odłącz od sieci kliknij przycisk **Tak**, aby opuścić sieć.

Uwaga: Aby po opuszczeniu chronionej sieci powtórnie do niej dołączyć, należy uzyskać prawa dostępu od innego użytkownika.

Tematy pokrewne

- Rozłączanie z chronionymi sieciami bezprzewodowymi (strona 316)
- Odwoływanie dostępu do sieci (strona 317)

ROZDZIAŁ 43

Zarządzanie zabezpieczeniami sieci bezprzewodowych

Program Wireless Network Security zapewnia pełny zestaw narzędzi, które pomagają w zarządzaniu funkcjami zabezpieczeń sieci bezprzewodowej.

W tym rozdziale

Konfigurowanie ustawień zabezpieczeń 320
Administrowanie kluczami sieciowymi 325

Konfigurowanie ustawień zabezpieczeń

Po połączeniu z chronioną siecią bezprzewodową program Wireless Network Security automatycznie chroni sieć. Użytkownik może jednak w dowolnym momencie konfigurować dodatkowe ustawienia zabezpieczeń.

Konfigurowanie trybów zabezpieczeń

Użytkownik może określić tryb zabezpieczeń chronionej sieci bezprzewodowej. Tryby zabezpieczeń definiują szyfrowanie komunikacji między komputerem a routerem lub punktem dostępu.

Przy włączaniu ochrony sieci automatycznie ustawiany jest tryb WEP. Firma McAfee zaleca jednak zmianę trybu zabezpieczeń na WPA2 lub WPA-PSK AES. Program Wireless Network Security za pierwszym razem używa trybu WEP, ponieważ jest on obsługiwany przez wszystkie routery i karty sieci bezprzewodowej. Większość nowych routerów i kart sieci bezprzewodowej pracuje w trybie WPA, który jest bardziej bezpieczny.

Aby zmienić tryb zabezpieczeń chronionej sieci bezprzewodowej:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl konfigurację**.
3. W polu **Tryb zabezpieczeń** okienka Zabezpieczenia sieci zaznacz typ zabezpieczeń, który chcesz wdrożyć, i kliknij przycisk **Zastosuj**.

Poniższa tabela opisuje dostępne tryby zabezpieczeń:

Zabezpie-czenie	Tryb	Opis
Słabe	WEP	Tryb WEP (Wired Equivalent Privacy) należy do standardu komunikacji bezprzewodowej IEEE 802.11 i jest używany do zabezpieczania sieci bezprzewodowych IEEE 802.11. Tryb WEP zabezpiecza sieć przed sondowaniem przez niedoświadczonych hakerów, ale nie jest tak bezpieczny jak szyfrowanie WPA-PSK. Program Wireless Network Security używa silnych (trudnych do odgadnięcia i długich) kluczy, firma McAfee zaleca stosowanie trybu zabezpieczeń WPA.
Średnie	WPA-PSK TKIP	Tryb WPA (Wi-Fi Protected Access) to wczesna wersja standardu zabezpieczeń 802.11i. Szyfrowanie TKIP używane w trybie WPA ma wzmocnić zabezpieczenia znane z trybu WEP. Szyfrowanie TKIP zapewnia integralności komunikatów, mechanizm ponownego nadawania kluczy i mieszanie kluczy w pakietach.
Silne	WPA-PSK AES	Ten tryb zabezpieczeń stanowi połączenie trybów WPA i AES. AES (Advanced Encryption Standard) to oparty na szyfrze blokowym standard szyfrowania stosowany przez rząd USA.
Silniejsze	WPA2-PSK AES	Ten tryb zabezpieczeń stanowi połączenie trybów WPA2 i AES. WPA2 to kolejny krok na drodze do przyjęcia standardu zabezpieczeń 802.11i. W trybie WPA2 stosowana jest metoda CCMP (Counter Mode CBC MAC Protocol), która jest bardziej bezpieczna i skalowalna od szyfrowania TKIP. Jest to najsilniejszy tryb zabezpieczeń dostępny w zastosowaniach prywatnych.
Najsilniejsze	WPA2-PSK TKIP+AES	Ten tryb zabezpieczeń stanowi połączenie trybów WPA2 i AES oraz WPA-PSK TKIP. Oferuje większą elastyczność, umożliwiając korzystanie zarówno ze starych, jak i nowszych kart sieci bezprzewodowej.

Uwaga: Po zmianie trybu zabezpieczeń konieczne może być ponowne, ręczne nawiązanie połączenia.

Tematy pokrewne

- Naprawianie ustawień zabezpieczeń sieci (strona 324)
- Wyświetlanie trybu zabezpieczeń sieci (strona 338)

Konfigurowanie ustawień zabezpieczeń sieci

Użytkownik może modyfikować właściwości sieci chronionych przez program Wireless Network Security. Jest to przydatne na przykład w przypadku zmiany trybu zabezpieczeń z WEP na WPA.

Firma McAfee zaleca zmodyfikowanie ustawień zabezpieczeń sieci zawsze, gdy sugeruje to wyświetlony alert.

Aby skonfigurować właściwości niechronionej sieci:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl sieci bezprzewodowe**.
3. W okienku Dostępne sieci bezprzewodowe kliknij opcję **Zaawansowane**.
4. W okienku Sieci bezprzewodowe kliknij opcję **Właściwości**.
5. W okienku Właściwości sieci bezprzewodowej zmodyfikuj następujące ustawienia, a następnie kliknij przycisk **OK**:

Ustawienie	Opis
Sieć	Nazwa sieci. Jeśli sieć jest modyfikowana, tej nazwy nie można zmienić.
Ustawienia zabezpieczeń	Zabezpieczenia niechronionej sieci. Należy zwrócić uwagę, że jeśli karta sieci bezprzewodowej nie obsługuje wybranego trybu, nawiązanie połączenia jest niemożliwe. Dostępne tryby zabezpieczeń to: Wyłączone, Otwarte WEP, Współdzielone WEP, Automatyczne WEP, WPA-PSK i WPA2-PSK.
Tryb szyfrowania	Szyfrowanie powiązane z wybranym trybem zabezpieczeń. Dostępne tryby szyfrowania to: WEP, TKIP, AES i TKIP+AES.

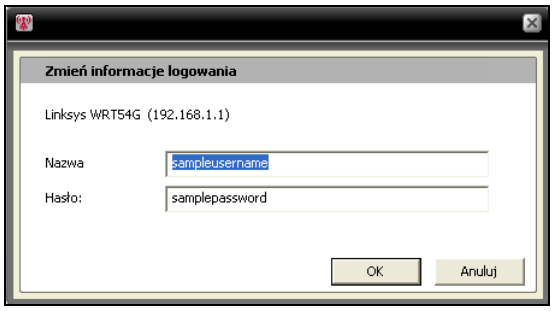
Zmienianie poświadczeń dla urządzeń bezprzewodowych

Użytkownik może zmienić nazwę użytkownika i hasło dla urządzenia, przechowywane na chronionym routerze bezprzewodowym lub punkcie dostępu. Lista urządzeń pojawia się w obszarze **Chronione urządzenia sieci bezprzewodowej**.

Firma McAfee zaleca zmieniać poświadczenia, ponieważ większość urządzeń bezprzewodowych pochodzących od określonego producenta ma takie same poświadczenia logowania. Zmiana poświadczeń logowania pomaga zapobiegać uzyskaniu dostępu do bezprzewodowego routera lub punktu dostępu przez inne osoby, które mogą zmienić ich ustawienia.

Aby zmienić nazwę użytkownika i hasło dla chronionego urządzenia bezprzewodowego:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl konfigurację**.
3. W okienku Zabezpieczenia sieci, w obszarze **Chronione urządzenia sieci bezprzewodowej** zaznacz router bezprzewodowy lub punkt dostępu, a następnie kliknij polecenie **Zmień nazwę użytkownika lub hasło**.



4. Po wprowadzeniu informacji logowania kliknij przycisk **OK** w oknie dialogowym programu Wireless Network Security.

   Nowa nazwa użytkownika i hasło pojawią się w obszarze **Chronione urządzenia sieci bezprzewodowej**.

Uwaga: Część routerów nie obsługuje nazw użytkownika. W ich przypadku nazwa użytkownika nie pojawi się w obszarze **Chronione urządzenia sieci bezprzewodowej**.

Naprawianie ustawień zabezpieczeń sieci

Jeśli występują problemy z ustawieniami lub konfiguracją zabezpieczeń, można naprawić ustawienia routera lub punktu dostępu za pomocą programu Wireless Network Security.

Aby naprawić ustawienia zabezpieczeń:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl narzędzia**.
3. W okienku Narzędzia kliknij opcję **Narzędzia konserwacji**.
4. W obszarze **Napraw ustawienia zabezpieczeń sieci** kliknij polecenie **Napraw**.
5. W okienku Napraw ustawienia zabezpieczeń sieci kliknij polecenie **Napraw**.

   Alert programu Wireless Network Security informuje, czy sieć została naprawiona czy nie.

Uwaga: Jeżeli próba naprawienia sieci nie powiedzie się, należy połączyć się z siecią za pomocą połączenia kablowego, a następnie spróbować ponownie. Jeśli hasło routera lub punktu dostępu zmieniło się, aby się połączyć, należy ponownie je wprowadzić.

Administrowanie kluczami sieciowymi

Program Wireless Network Security generuje długie, silne, losowe klucze szyfrowania, za pomocą generatora losowego kluczy. W trybie WEP klucze są tłumaczone na 26-cyfrowe wartości szesnastkowe (co daje 104 bity entropii, czyli siły, a więc maksymalną wartość obsługiwaną przez 128-bitowe zabezpieczenia WEP). Klucze w trybie WPA to 63-znakowe łańcuchy znaków ASCII. Każdy znak ma 64 możliwe wartości (6 bitów), co daje 384 bity entropii, a więc więcej niż 256 bitów obsługiwanych przez zabezpieczenia WPA.

Zarządzanie kluczami sieciowymi obejmuje wyświetlanie ich w postaci tekstu lub znaków gwiazdki dla chronionych punktów dostępu, usuwanie zapisanych kluczy dla niechronionych punktów dostępu, włączanie, wyłączanie, modyfikowanie częstotliwości i wstrzymywanie cyklicznych zmian klucza oraz ręczne dokonywanie cyklicznej zmiany klucza.

Automatyczna cykliczna zmiana klucza sprawia, że narzędzia hakerów nie są w stanie przechwycić informacji, ponieważ klucz jest stale zmieniany.

W przypadku podłączania do sieci urządzeń bezprzewodowych, które nie są obsługiwane przez program Wireless Network Security (na przykład bezprzewodowego komputera kieszonkowego), należy jednak zapisać klucz, zatrzymać jego cykliczną zmianę, a następnie wpisać go w interfejsie urządzenia.

Wyświetlanie bieżących kluczy

Program Wireless Network Security daje szybki dostęp do informacji o zabezpieczeniach komunikacji bezprzewodowej w chronionej sieci bezprzewodowej.

Aby wyświetlić bieżący klucz:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl stan**.
3. W okienku Stan sieci bezprzewodowej, w obszarze Chroniona sieć bezprzewodowa kliknij polecenie **Bieżący klucz**.

   Klucz skonfigurowany dla sieci pojawi się w oknie dialogowym Konfiguracja klucza.

Tematy pokrewne

- Wyświetlanie liczby cyklicznych zmian klucza (strona 342)

Automatyczna cykliczna zmiana klucza

Automatyczna cykliczna zmiana klucza jest domyślnie włączona, ale jeśli zostanie wstrzymana, można ją ponownie włączyć z komputera z dostępem administracyjnym.

Program Wireless Network Security można skonfigurować tak, aby stosował automatyczną cykliczną zmianę klucza bezpieczeństwa chronionej sieci bezprzewodowej.

Program Wireless Network Security automatycznie generuje nieskończony szereg silnych kluczy, które są synchronizowane w całej sieci. Połączenie bezprzewodowe może być chwilowo zakłócane w momencie ponownego uruchamiania routera bezprzewodowego z nową konfiguracją klucza bezpieczeństwa, ale zwykle nie jest to odczuwane przez użytkowników sieci.

Jeśli z siecią nie są połączone żadne komputery, cykliczna zmiana klucza ma miejsce, gdy z siecią połączy się pierwszy komputer.

Aby włączyć automatyczną cykliczną zmianę klucza:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl konfigurację**.
3. W okienku Zabezpieczenia sieci zaznacz opcję **Włącz automatyczną cykliczną zmianę klucza**.

   Cykliczną zmianę klucza można także wznowić w okienku Stan sieci bezprzewodowej.
4. Kliknij przycisk **Zastosuj**.

Uwaga: Domyślnie cykliczna zmiana klucza następuje automatycznie co trzy godziny, ale jej częstotliwość można zmienić tak, by spełniała wymagania dotyczące zabezpieczeń sieci.

Tematy pokrewne

- Zmienianie częstotliwości cyklicznej zmiany klucza (strona 327)
- Wznawianie cyklicznej zmiany klucza (strona 327)
- Wyświetlanie liczby cyklicznych zmian klucza (strona 342)

Wznawianie cyklicznej zmiany klucza

Automatyczna cykliczna zmiana klucza jest domyślnie włączona, ale jeśli zostanie wstrzymana, można ją wznowić z komputera z dostępem administracyjnym.

Aby wznowić cykliczną zmianę klucza:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl stan**.
3. W okienku Stan sieci bezprzewodowej kliknij polecenie **Wznów cykliczną zmianę klucza**.

   Alerty Uruchomiono cykliczną zmianę klucza i Wykonano cykliczną zmianę klucza bezpieczeństwa potwierdzają, że cykliczna zmiana klucza rozpoczęła się i zakończyła pomyślnie.

Tematy pokrewne

- Automatyczna cykliczna zmiana klucza (strona 326)
- Wstrzymywanie automatycznej cyklicznej zmiany klucza (strona 329)
- Wyświetlanie liczby cyklicznych zmian klucza (strona 342)

Zmienianie częstotliwości cyklicznej zmiany klucza

Jeśli program Wireless Network Security skonfigurowano tak, aby stosował automatyczną cykliczną zmianę klucza bezpieczeństwa chronionej sieci bezprzewodowej, można zmienić długość okresu między dwiema zmianami — od piętnastu minut do piętnastu dni.

Firma McAfee zaleca zmienianie klucza bezpieczeństwa codziennie.

Aby zmienić częstotliwość automatycznej cyklicznej zmiany klucza:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl konfigurację**.
3. W okienku Zabezpieczenia sieci upewnij się, że automatyczna cykliczna zmiana klucza jest włączona, a następnie przesuń suwak **Częstotliwość** na jedno z następujących ustawień:
   - **co 15 min.**
   - **co 30 min.**
   - **co 1 godz.**
   - **co 3 godz.**
   - **co 12 godz.**

- **co 1 dzień**
- **co 7 dni**
- **co 15 dni**

4 Kliknij przycisk **Zastosuj**.

Uwaga: Przed ustawieniem częstotliwości automatycznej cyklicznej zmiany klucza należy się upewnić, że funkcja ta jest włączona.

Tematy pokrewne

- Włącz automatyczną cykliczną zmianę klucza (strona 326)
- Wyświetlanie liczby cyklicznych zmian klucza (strona 342)

Wstrzymywanie automatycznej cyklicznej zmiany klucza

Cykliczną zmianę klucza można wstrzymać z dowolnego komputera połączonego z siecią bezprzewodową. Może to być pożądane w następujących sytuacjach:

- Aby zezwolić na uzyskanie dostępu do sieci gościowi, który nie ma zainstalowanego programu Wireless Network Security.
- Aby zezwolić na uzyskanie dostępu do sieci komputerowi z systemem innym niż Windows, na przykład Macintosh lub Linux, bądź urządzeniu TiVo. Po zatrzymaniu cyklicznej zmiany klucza należy zanotować klucz i wpisać go w interfejsie urządzenia.
- Aby zachować połączenie bezprzewodowe wolne od zakłóceń spowodowanych przez cykliczną zmianę klucza, niezbędne dla niektórych aplikacji, na przykład gier online.
- Automatyczną cykliczną zmianę klucza należy wznowić jak najszybciej, aby zapewnić pełną ochronę sieci przed hakerami.

Aby wyświetlić bieżący klucz:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl stan**.
3. W okienku Stan sieci bezprzewodowej, w obszarze Chroniona sieć bezprzewodowa kliknij polecenie **Bieżący klucz**. Klucz pojawi się w oknie dialogowym Konfiguracja klucza. Inne komputery, na których nie zainstalowano programu Wireless Network Security, mogą użyć tego klucza do nawiązania połączenia z chronioną siecią bezprzewodową.
4. W oknie dialogowym Konfiguracja klucza kliknij polecenie **Wstrzymaj cykliczną zmianę klucza**.
5. W oknie dialogowym Wstrzymano cykliczną zmianę klucza kliknij przycisk **OK**, aby kontynuować pracę.

Ostrzeżenie: Jeśli cykliczna zmiana klucza nie została wstrzymana, nieobsługiwane urządzenia bezprzewodowe, które nawiązały połączenie z siecią ręcznie, zostaną rozłączone w momencie zmiany klucza.

W takiej sytuacji można utworzyć dysk Windows Connect Now, a następnie za pomocą pliku tekstowego skopiować i wkleić klucz w interfejsie innego komputera lub urządzenia.

Tematy pokrewne

- Włącz automatyczną cykliczną zmianę klucza (strona 326)
- Dodawanie komputerów za pomocą technologii Windows Connect Now (strona 304)
- Wznawianie cyklicznej zmiany klucza (strona 327)

- Automatyczna cykliczna zmiana klucza (strona 326)
- Wyświetlanie liczby cyklicznych zmian klucza (strona 342)

Ręczne dokonywanie cyklicznej zmiany klucza

Program Wireless Network Security pozwala ręcznie dokonać cyklicznej zmiany klucza, nawet w sytuacji, gdy automatyczna cykliczna zmiana klucza jest włączona.

Aby ręcznie dokonać cyklicznej zmiany klucza sieciowego:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl narzędzia**.
3. W okienku Narzędzia kliknij opcję **Narzędzia konserwacji**.
4. W okienku Narzędzia konserwacji, w obszarze **Zmieniaj klucz szyfrujący ręcznie** kliknij polecenie **Zmień**.

   Wyświetlony alert Uruchomiono cykliczną zmianę klucza potwierdza, że cykliczna zmiana klucza została rozpoczęta. Po dokonaniu zmiany klucza bezpieczeństwa pojawia się alert Wykonano cykliczną zmianę klucza bezpieczeństwa, potwierdzając że cykliczna zmiana klucza zakończyła się pomyślnie.

Uwaga: Aby ułatwić zarządzanie kluczami bezpieczeństwa, w okienku Zabezpieczenia sieci można włączyć automatyczną cykliczną zmianę klucza.

Jeśli z siecią bezprzewodową nie są połączone żadne komputery, cykliczna zmiana klucza ma automatycznie miejsce, gdy z siecią połączy się pierwszy komputer.

Tematy pokrewne

- Włącz automatyczną cykliczną zmianę klucza (strona 326)
- Zmienianie częstotliwości cyklicznej zmiany klucza (strona 327)
- Wyświetlanie liczby cyklicznych zmian klucza (strona 342)

Wyświetlanie kluczy w postaci znaków gwiazdki

Klucze są domyślnie wyświetlane w postaci znaków gwiazdki, ale można skonfigurować program Wireless Network Security tak, aby wyświetlał klucze w sieciach niechronionych przez program Wireless Network Security w postaci tekstu.

W sieciach chronionych przez program Wireless Network Security klucze są wyświetlane w postaci tekstu.

Aby wyświetlać klucze w postaci znaków gwiazdki:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl konfigurację**.
3. Kliknij ikonę **Inne ustawienia**.
4. Wyczyść pole wyboru **Wyświetlaj klucze w postaci tekstu**.
5. Kliknij przycisk **Zastosuj**.

Tematy pokrewne

- Wyświetlaj klucze w postaci tekstu (strona 332)

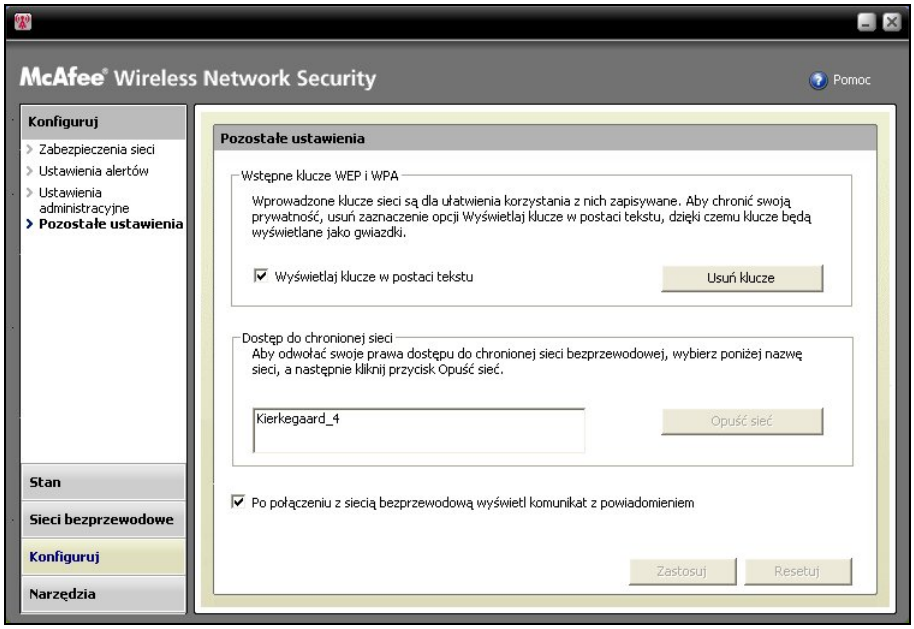
Wyświetlaj klucze w postaci tekstu

Klucze są domyślnie wyświetlane w postaci znaków gwiazdki, ale można skonfigurować program Wireless Network Security tak, aby wyświetlał klucze w sieciach niechronionych przez program Wireless Network Security w postaci tekstu.

W sieciach chronionych przez program Wireless Network Security klucze są wyświetlane w postaci tekstu.

Aby wyświetlać klucze w postaci tekstu:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl konfigurację**.
3. Kliknij ikonę **Inne ustawienia**.



4. Zaznacz pole wyboru **Wyświetlaj klucze w postaci tekstu**.
5. Kliknij przycisk **Zastosuj**.

Tematy pokrewne

- Wyświetlanie kluczy w postaci znaków gwiazdki (strona 331)

Usuwanie kluczy sieciowych

Program Wireless Network Security automatycznie zapisuje klucze WEP i wstępne klucze WPA, które można usunąć w dowolnym momencie.

Aby usunąć wszystkie klucze sieciowe:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl konfigurację**.
3. W okienku **Konfiguruj** kliknij opcję **Inne ustawienia**.
4. W okienku **Inne ustawienia**, w obszarze **Wstępne klucze WEP i WPA** kliknij polecenie **Usuń klucze**.
5. W oknie dialogowym Wyczyść klucze kliknij przycisk **Tak**, jeśli na pewno chcesz usunąć wszystkie przechowywane klucze WEP i wstępne klucze WPA.

Ostrzeżenie: Klucze są trwale usuwane z komputera. Po usunięciu kluczy sieciowych, aby połączyć się z siecią z zabezpieczeniami WEP lub WPA, trzeba wprowadzić prawidłowy klucz.

ROZDZIAŁ 44

Monitorowanie sieci bezprzewodowych

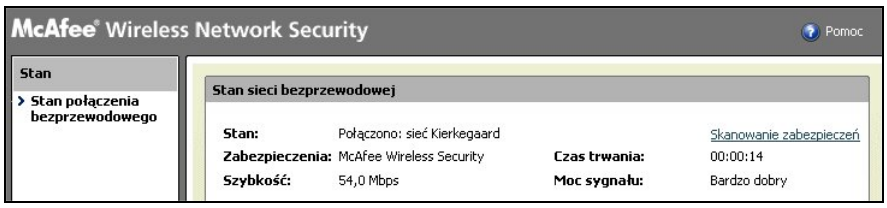
Program Wireless Network Security pozwala monitorować stan sieci bezprzewodowej i chronionych komputerów.

W tym rozdziale

Monitorowanie połączeń w sieci bezprzewodowej.....336
Monitorowanie chronionych sieci bezprzewodowych.....341
Rozwiązywanie problemów.....347

Monitorowanie połączeń w sieci bezprzewodowej

Stan, tryb zabezpieczeń, szybkość, czas trwania i moc sygnału połączenia sieciowego oraz raport zabezpieczeń można wyświetlić w okienku Stan sieci bezprzewodowej.



Poniższa tabela opisuje wskaźniki stanu bezprzewodowego połączenia sieciowego.

Stan	Opis	Informacje
Stan	Określa, czy komputer jest połączony z siecią, i wskazuje sieć, z którą jest połączony.	Wyświetlanie stanu połączenia (strona 337)
Zabezpieczenia	Określa tryb zabezpieczeń sieci, z którą komputer jest połączony. Jeśli komputer jest chroniony przez program Wireless Network Security, wyświetlana jest nazwa „Wireless Network Security”.	Wyświetlanie trybu zabezpieczeń sieci (strona 338)
Szybkość	Określa szybkość połączenia komputera z siecią.	Wyświetlanie szybkości połączenia sieciowego (strona 338)
Czas trwania	Określa czas trwania połączenia komputera z siecią.	Wyświetlanie czasu trwania połączenia sieciowego (strona 339)
Moc sygnału	Określa względną moc sygnału sieci.	Wyświetlanie mocy sygnału sieci (strona 340)

Skanowanie zabezpieczeń	Kliknięcie polecenia **Skanowanie zabezpieczeń** powoduje wyświetlenie informacji o zabezpieczeniach, na przykład podatność sieci bezprzewodowej na zagrożenia, problemy dotyczące wydajności i stan sieci bezprzewodowej.	Wyświetlanie raportu zabezpieczeń w trybie online (strona 340)

Tematy pokrewne

- Ikony programu Wireless Network Security — informacje (strona 308)

Wyświetlanie stanu połączenia

Przeglądając stan połączenia sieciowego w okienku Stan sieci bezprzewodowej, można sprawdzić, czy komputer jest połączony z siecią czy rozłączony.

Aby wyświetlić stan połączenia bezprzewodowego:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl stan**.

   Komputery połączone z chronioną siecią bezprzewodową oraz data i godzina nawiązania połączenia przez każdy z nich są wyświetlane w obszarze **Komputery** okienka Stan sieci bezprzewodowej.

Tematy pokrewne

- Monitorowanie połączeń w sieci bezprzewodowej (strona 336)
- Wyświetlanie trybu zabezpieczeń sieci (strona 338)
- Wyświetlanie szybkości połączenia sieciowego (strona 338)
- Wyświetlanie czasu trwania połączenia sieciowego (strona 339)
- Wyświetlanie mocy sygnału sieci (strona 340)
- Wyświetlanie raportu zabezpieczeń w trybie online (strona 340)

Wyświetlanie trybu zabezpieczeń sieci

W okienku Stan sieci bezprzewodowej można przeglądać tryb zabezpieczeń połączenia sieciowego.

Aby wyświetlić tryb zabezpieczeń sieci:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl stan**.

   Tryb zabezpieczeń jest wyświetlany w polu **Zabezpieczenia** okienka Stan sieci bezprzewodowej.

   Jeśli sieć bezprzewodowa jest chroniona przez program Wireless Network Security, wyświetlana jest nazwa „Wireless Network Security”.

Tematy pokrewne

- Monitorowanie połączeń w sieci bezprzewodowej (strona 336)
- Wyświetlanie stanu połączenia (strona 337)
- Wyświetlanie szybkości połączenia sieciowego (strona 338)
- Wyświetlanie czasu trwania połączenia sieciowego (strona 339)
- Wyświetlanie mocy sygnału sieci (strona 340)
- Wyświetlanie raportu zabezpieczeń w trybie online (strona 340)

Wyświetlanie szybkości połączenia sieciowego

W okienku Stan sieci bezprzewodowej można przeglądać szybkość połączenia komputera z siecią.

Aby wyświetlić szybkość połączenia sieciowego:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl stan**.

   Szybkość połączenia jest wyświetlana w polu **Szybkość** okienka Stan sieci bezprzewodowej.

Tematy pokrewne

- Monitorowanie połączeń w sieci bezprzewodowej (strona 336)
- Wyświetlanie stanu połączenia (strona 337)
- Wyświetlanie trybu zabezpieczeń sieci (strona 338)
- Wyświetlanie czasu trwania połączenia sieciowego (strona 339)
- Wyświetlanie mocy sygnału sieci (strona 340)
- Wyświetlanie raportu zabezpieczeń w trybie online (strona 340)

Wyświetlanie czasu trwania połączenia sieciowego

W okienku Stan sieci bezprzewodowej można przeglądać czas trwania połączenia komputera z siecią.

Aby wyświetlić czas trwania połączenia z siecią:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl stan**.

   Czas trwania połączenia komputera z siecią bezprzewodową jest wyświetlany w polu **Czas trwania**.

Tematy pokrewne

- Monitorowanie połączeń w sieci bezprzewodowej (strona 336)
- Wyświetlanie stanu połączenia (strona 337)
- Wyświetlanie trybu zabezpieczeń sieci (strona 338)
- Wyświetlanie szybkości połączenia sieciowego (strona 338)
- Wyświetlanie mocy sygnału sieci (strona 340)
- Wyświetlanie raportu zabezpieczeń w trybie online (strona 340)

Wyświetlanie mocy sygnału sieci

W okienku Stan sieci bezprzewodowej można przeglądać moc sygnału sieci.

Aby wyświetlić moc sygnału sieci:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl stan**.

   Jakość sygnału jest wyświetlana w polu **Moc sygnału**.

Tematy pokrewne

- Monitorowanie połączeń w sieci bezprzewodowej (strona 336)
- Wyświetlanie stanu połączenia (strona 337)
- Wyświetlanie trybu zabezpieczeń sieci (strona 338)
- Wyświetlanie szybkości połączenia sieciowego (strona 338)
- Wyświetlanie czasu trwania połączenia sieciowego (strona 339)
- Wyświetlanie raportu zabezpieczeń w trybie online (strona 340)

Wyświetlanie raportu zabezpieczeń w trybie online

W okienku Stan sieci bezprzewodowej można przeglądać raport dotyczący połączenia bezprzewodowego i jego zabezpieczeń lub ich braku.

Strona sieci Web programu McAfee Wi-FiScan zawiera informacje opisujące luki w zabezpieczeniach sieci bezprzewodowej, problemy dotyczące wydajności, stan sieci bezprzewodowej i zalecane rozwiązanie zabezpieczeń, oraz określa, czy połączenie jest bezpieczne.

Przed wyświetleniem raportu zabezpieczeń należy upewnić się, że komputer ma połączenie z Internetem.

Aby wyświetlić raport zabezpieczeń sieci w trybie online:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl stan**.
3. W okienku Stan sieci bezprzewodowej kliknij polecenie **Skanowanie zabezpieczeń**.

   Po otwarciu przeglądarki należy pobrać i zainstalować składnik ActiveX. W zależności od swojej konfiguracji przeglądarka może zablokować formant. Aby rozpocząć skanowanie, należy zezwolić przeglądarce na pobranie i uruchomienie składnika. Czas trwania skanowania zależy od szybkości połączenia internetowego.

Uwaga: Informacje na temat pobierania składników ActiveX zawiera dokumentacja przeglądarki.

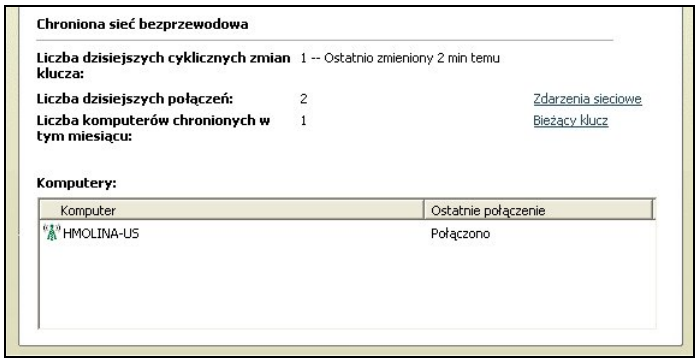
Program McAfee Wi-FiScan obsługuje program Explorer w wersji 5.5 i nowszych.

Tematy pokrewne

- Monitorowanie połączeń w sieci bezprzewodowej (strona 336)
- Wyświetlanie stanu połączenia (strona 337)
- Wyświetlanie trybu zabezpieczeń sieci (strona 338)
- Wyświetlanie szybkości połączenia sieciowego (strona 338)
- Wyświetlanie czasu trwania połączenia sieciowego (strona 339)
- Wyświetlanie mocy sygnału sieci (strona 340)

Monitorowanie chronionych sieci bezprzewodowych

Program Wireless Network Security pozwala wyświetlać liczbę połączeń, cyklicznych zmian klucza oraz chronionych komputerów w okienku Stan sieci bezprzewodowej. Wyświetlać można także zdarzenia sieciowe, bieżący klucz i listę aktualnie chronionych komputerów.



Poniższa tabela opisuje wskaźniki stanu chronionego bezprzewodowego połączenia sieciowego.

Stan	Opis	Informacje
Liczba dzisiejszych cyklicznych zmian klucza	Określa dzienną liczbę cyklicznych zmian klucza w chronionej sieci bezprzewodowej.	Wyświetlanie liczby cyklicznych zmian klucza (strona 343)
Liczba dzisiejszych połączeń	Określa dzienną liczbę połączeń z chronioną siecią bezprzewodową.	Wyświetlanie dziennej liczby połączeń (strona 344)
Liczba komputerów chronionych w tym miesiącu	Określa liczbę komputerów chronionych w bieżącym miesiącu.	Wyświetlanie miesięcznej liczby chronionych komputerów (strona 344)
Zdarzenia sieciowe	Kliknięcie opcji **Zdarzenia sieciowe** powoduje wyświetlenie zdarzeń dotyczących sieci, połączenia i cyklicznej zmiany klucza.	Wyświetlanie zdarzeń chronionej sieci bezprzewodowej (strona 344)

Komputery	Określa liczbę komputerów połączonych z chronioną siecią bezprzewodową oraz datę i godzinę nawiązania połączenia przez każdy z nich.	Wyświetlanie aktualnie chronionych komputerów (strona 346)

Wyświetlanie liczby cyklicznych zmian klucza

Program Wireless Network Security pozwala wyświetlać dzienną liczbę cyklicznych zmian klucza w chronionej sieci oraz datę i godzinę ostatniej takiej zmiany.

Aby wyświetlić dzienną liczbę cyklicznych zmian klucza:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl stan**.

   Łączna liczba połączeń oraz szczegóły ostatniej cyklicznej zmiany klucza są wyświetlane w polu **Liczba dzisiejszych cyklicznych zmian klucza**, w obszarze **Chroniona sieć bezprzewodowa** okienka Stan sieci bezprzewodowej.

Tematy pokrewne

- Monitorowanie chronionych sieci bezprzewodowych (strona 341)
- Wyświetlanie dziennej liczby połączeń (strona 344)
- Wyświetlanie miesięcznej liczby chronionych komputerów (strona 344)
- Wyświetlanie zdarzeń chronionej sieci bezprzewodowej (strona 344)
- Wyświetlanie aktualnie chronionych komputerów (strona 346)
- Administrowanie kluczami sieciowymi (strona 325)
- Automatyczna cykliczna zmiana klucza (strona 326)
- Ręczne dokonywanie cyklicznej zmiany klucza (strona 330)

Wyświetlanie dziennej liczby połączeń

Program Wireless Network Security pozwala wyświetlać dzienną liczbę połączeń z chronioną siecią.

Aby wyświetlić połączenia z chronioną siecią bezprzewodową:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl stan**.

   Łączna liczba połączeń jest wyświetlana w polu **Liczba dzisiejszych połączeń**, w obszarze **Chroniona sieć bezprzewodowa** okienka Stan sieci bezprzewodowej.

Tematy pokrewne

- Monitorowanie chronionych sieci bezprzewodowych (strona 341)
- Wyświetlanie miesięcznej liczby chronionych komputerów (strona 344)
- Wyświetlanie zdarzeń chronionej sieci bezprzewodowej (strona 344)
- Wyświetlanie aktualnie chronionych komputerów (strona 346)

Wyświetlanie miesięcznej liczby chronionych komputerów

Program Wireless Network Security pozwala wyświetlać liczbę komputerów chronionych w bieżącym miesiącu.

Aby wyświetlić liczbę komputerów chronionych w bieżącym miesiącu:

1. Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl stan**.
3. Liczba komputerów chronionych w bieżącym miesiącu jest wyświetlana w polu **Liczba komputerów chronionych w tym miesiącu**, w obszarze **Chroniona sieć bezprzewodowa** okienka Stan sieci bezprzewodowej.

Tematy pokrewne

- Monitorowanie chronionych sieci bezprzewodowych (strona 341)
- Wyświetlanie liczby cyklicznych zmian klucza (strona 343)
- Wyświetlanie dziennej liczby połączeń (strona 344)
- Wyświetlanie zdarzeń chronionej sieci bezprzewodowej (strona 344)
- Wyświetlanie aktualnie chronionych komputerów (strona 346)

Wyświetlanie zdarzeń chronionej sieci bezprzewodowej

Program Wireless Network Security rejestruje zdarzenia w sieci bezprzewodowej, na przykład cykliczne zmiany kluczy bezpieczeństwa, nawiązanie przez inne komputery połączenia z siecią chronioną przez produkty firmy McAfee lub dołączenie innych komputerów do sieci chronionej przez produkty firmy McAfee.

Program Wireless Network Security pozwala wyświetlać raport opisujący zdarzenia, które miały miejsce w sieci. Użytkownik może określić typy zdarzeń wyświetlanych w raporcie oraz sortować informacje na ich temat według dat, zdarzeń lub komputerów.

Aby wyświetlić zdarzenia sieciowe:

1 Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.

2 Wykonaj jedną z poniższych czynności:

Aby...	Wykonaj następujące kroki...
Wyświetlić zdarzenia sieciowe z okienka Stan sieci bezprzewodowej	1. Wybierz polecenie **Wyświetl stan**. 2. W okienku Stan sieci bezprzewodowej, w obszarze **Chroniona sieć bezprzewodowa** kliknij polecenie **Zdarzenia sieciowe**.
Wyświetlić zdarzenia sieciowe z okienka Stan sieci bezprzewodowej	1. Kliknij polecenie **Wyświetl narzędzia**. 2. W okienku Narzędzia kliknij opcję **Narzędzia konserwacji**. 3. W okienku Narzędzia konserwacji, w obszarze **Wyświetl dziennik zdarzeń** kliknij polecenie **Wyświetl**.

3 Zaznacz co najmniej jeden z następujących typów zdarzeń do wyświetlenia:

- **Zdarzenia sieciowe**: Powoduje wyświetlenie informacji na temat aktywności w sieci, na przykład ochrony routera bezprzewodowego lub punktu dostępu.
- **Zdarzenia połączeń**: Powoduje wyświetlenie informacji na temat połączeń sieciowych, na przykład daty i godziny nawiązania przez komputer połączenia z siecią.
- **Zdarzenia cyklicznej zmiany klucza**: Powoduje wyświetlenie informacji na temat dat i godzin cyklicznych zmian klucza bezpieczeństwa.

4 Kliknij przycisk **Zamknij**.

Tematy pokrewne

- Monitorowanie chronionych sieci bezprzewodowych (strona 341)
- Wyświetlanie liczby cyklicznych zmian klucza (strona 343)
- Wyświetlanie dziennej liczby połączeń (strona 343)
- Wyświetlanie dziennej liczby połączeń (strona 344)
- Wyświetlanie aktualnie chronionych komputerów (strona 346)

Wyświetlanie aktualnie chronionych komputerów

Pozwala wyświetlić liczbę komputerów połączonych z chronioną siecią bezprzewodową oraz datę i godzinę ostatniego nawiązania połączenia przez każdy z nich.

Aby wyświetlić listę komputerów połączonych z chronioną siecią:

1 Kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.

2 Wybierz polecenie **Wyświetl stan**.

3 Komputery połączone z chronioną siecią bezprzewodową oraz data i godzina ostatniego nawiązania połączenia przez każdy z nich są wyświetlane w obszarze **Komputery** okienka Stan sieci bezprzewodowej.

Tematy pokrewne

- Monitorowanie chronionych sieci bezprzewodowych (strona 341)
- Wyświetlanie liczby cyklicznych zmian klucza (strona 343)
- Wyświetlanie dziennej liczby połączeń (strona 343)
- Wyświetlanie miesięcznej liczby chronionych komputerów (strona 344)
- Wyświetlanie zdarzeń chronionej sieci bezprzewodowej (strona 344)

ROZDZIAŁ 45

Rozwiązywanie problemów

Użytkownik może rozwiązywać problemy wynikające z używania programu Wireless Security z urządzeniami innych producentów, w tym między innymi:

- trudności z instalacją,
- brak możliwości włączenia ochrony lub skonfigurowania sieci,
- brak możliwości połączenia komputerów z siecią,
- brak możliwości połączenia z siecią lub Internetem,
- inne problemy.

W tym rozdziale

Instalowanie programu Wireless Network Security.....348
Włączanie ochrony i konfigurowanie sieci 350
Łączenie komputerów z siecią 353
Łączenie z Internetem i siecią 355
Inne problemy 360

Instalowanie programu Wireless Network Security

Użytkownik może rozwiązywać następujące problemy z instalacją:

- Wybór komputerów, na których program ma zostać zainstalowany
- Nie wykryto karty sieci bezprzewodowej
- Kilka kart sieciowych
- Nie można pobrać programu na komputery bezprzewodowe, ponieważ sieć jest już zabezpieczona

Wybór komputerów, na których program ma zostać zainstalowany

Program Wireless Network Security należy zainstalować na każdym komputerze w sieci bezprzewodowej (w przeciwieństwie do innych programów firmy McAfee, można go zainstalować na wielu komputerach). Należy przestrzegać postanowień umowy licencyjnej zakupionego oprogramowania. W niektórych przypadkach konieczne może być zakupienie dodatkowych licencji.

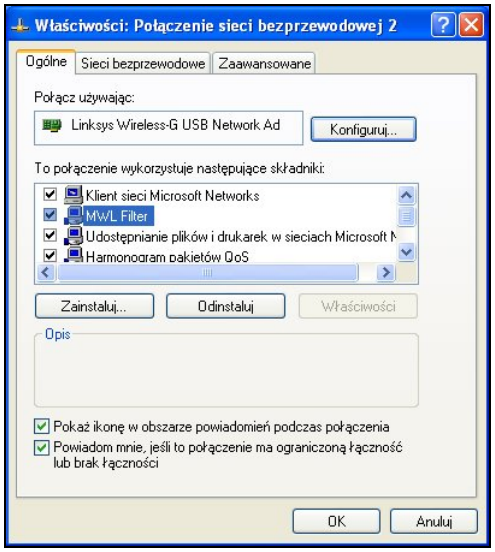
Program można (ale nie jest to wymagane) zainstalować na komputerach, które nie mają kart sieci bezprzewodowej. Nie będzie on jednak aktywny na tych komputerach, ponieważ nie potrzebują one ochrony w sieci bezprzewodowej.

Program Wireless Network Security jest obecnie obsługiwany przez systemy Windows XP i Windows 2000.

Nie wykryto zgodnej karty sieci bezprzewodowej

Jeśli karta sieci bezprzewodowej nie zostanie wykryta po zainstalowaniu i włączeniu, należy uruchomić ponownie komputer. Jeśli karta mimo to nie jest wykrywana, należy wykonać następujące kroki:

1. Otwórz okno dialogowe Właściwości połączenia sieci bezprzewodowej.
2. W klasycznym menu Start systemu Windows kliknij przycisk **Start**, wskaż polecenie **Ustawienia** i wybierz polecenie **Połączenia sieciowe**.
3. Kliknij ikonę **Połączenie sieci bezprzewodowej**.
4. W oknie dialogowym Stan połączenia sieci bezprzewodowej kliknij przycisk **Właściwości**.
5. W okienku Właściwości połączenia sieci bezprzewodowej wyczyść pole wyboru **Filtr MWL**, a następnie ponownie je zaznacz.



6. Kliknij przycisk **OK**.

   Jeśli to nie rozwiąże problemu, spróbuj użyć programu Wi-FiScan. Jeśli program Wi-FiScan działa, karta sieciowa jest obsługiwana. W przeciwnym razie musisz zaktualizować sterownik karty (w witrynie sieci Web Windows Update lub producenta karty) lub zakupić nowe urządzenie.

Tematy pokrewne

- Wyświetlanie raportu zabezpieczeń w trybie online (strona 340)

Kilka kart sieciowych

Jeśli komunikat o błędzie stwierdza, że zainstalowano wiele kart sieci bezprzewodowej, należy wyłączyć lub odłączyć wszystkie karty poza jedną. Program Wireless Home Network Security działa tylko z jedną kartą sieci bezprzewodowej.

Pobieranie w chronionej sieci kończy się niepowodzeniem

Jeżeli użytkownik ma instalacyjny dysk CD, może zainstalować program Wireless Network Security z dysku CD na wszystkich komputerach bezprzewodowych.

Jeśli użytkownik zainstalował program na jednym komputerze i włączył ochronę sieci przed zainstalowaniem go na pozostałych komputerach bezprzewodowych, ma do wyboru następujące opcje:

- Wyłącz ochronę sieci. Pobierz program i zainstaluj go na wszystkich komputerach bezprzewodowych. Ponownie włącz ochronę sieci.
- Wyświetl klucz sieciowy. Następnie wprowadź go na komputerach bezprzewodowych, które chcesz połączyć z siecią. Pobierz program i zainstaluj program, a następnie dołącz wszystkie komputery do sieci.
- Pobierz plik wykonywalny na komputer już połączony z siecią i zapisz go na dysku flash USB lub dysku CD, aby następnie zainstalować go na innych komputerach.
- Utwórz dysk Windows Connect Now i użyj go.

Tematy pokrewne

- Usuwanie routerów bezprzewodowych lub punktów dostępu (strona 315)
- Wyświetlanie bieżących kluczy (strona 325)
- Dodawanie komputerów za pomocą urządzenia wymiennego (strona 302)
- Dodawanie komputerów za pomocą technologii Windows Connect Now (strona 304)

Włączanie ochrony i konfigurowanie sieci

Użytkownik może rozwiązywać następujące problemy z włączaniem ochrony i konfigurowaniem sieci:

- Nieobsługiwany router lub punkt dostępu
- Aktualizacja oprogramowania układowego routera lub punktu dostępu
- Błąd zdublowanych administratorów
- Sieć wydaje się być niezabezpieczona
- Nie można naprawić

Nieobsługiwany router lub punkt dostępu

Jeśli komunikat o błędzie stwierdza, że router bezprzewodowy lub punkt dostępu może nie być obsługiwany, program Wireless Network Security nie mógł skonfigurować urządzenia, ponieważ go nie rozpoznał lub nie znalazł.

Należy sprawdzić, czy posiadana wersja programu Wireless Network Security jest najnowszą, żądając dokonania aktualizacji (firma McAfee stale dodaje obsługę nowych routerów i punktów dostępu). Jeśli posiadany router lub punkt dostępu znajduje się na liście obsługiwanych punktów dostępu, a mimo to wyświetlany jest komunikat o błędzie, wystąpiły problemy z komunikacją między komputerem a routerem lub punktem dostępu.

Tematy pokrewne

- Obsługiwane routery bezprzewodowe
  http://www.mcafee.com/router

Aktualizacja oprogramowania układowego routera lub punktu dostępu

Jeśli komunikat o błędzie stwierdza, że wersja oprogramowania układowego routera bezprzewodowego lub punktu dostępu nie jest obsługiwana, nie oznacza to, że samo urządzenie nie jest obsługiwane. Należy sprawdzić, czy posiadana wersja programu Wireless Network Security jest najnowszą, żądając dokonania aktualizacji (firma McAfee stale dodaje obsługę nowych wersji oprogramowania układowego).

Jeśli posiadana wersja programu Wireless Network Security jest najnowszą, należy odwiedzić witrynę sieci Web producenta lub organizacji zapewniającej pomoc techniczną dla routera lub punktu dostępu i zainstalować wersję oprogramowania układowego wymienioną na liście obsługiwanych routerów.

Tematy pokrewne

- Obsługiwane routery bezprzewodowe
  http://www.mcafee.com/router

Błąd zdublowanych administratorów

Po skonfigurowaniu routera lub punktu dostępu należy wylogować się z interfejsu administratora. W niektórych przypadkach, jeśli użytkownik się nie wylogował, router lub punkt dostępu zachowuje się tak, jakby był nadal konfigurowany z innego komputera, co powoduje wyświetlenie komunikatu o błędzie.

Jeśli nie można się wylogować, należy odłączyć zasilanie routera lub punktu dostępu, a następnie podłączyć je ponownie.

Cykliczna zmiana klucza nie powiodła się

Cykliczna zmiana klucza nie powiodła się, ponieważ:

- Informacje logowania dla routera lub punktu dostępu zostały zmienione.
- Wersja oprogramowania układowego routera lub punktu dostępu została zmieniona na taką, która nie jest obsługiwana.
- Router lub punkt dostępu nie jest dostępny. Należy upewnić się, że router lub punkt dostępu jest włączony i połączony z siecią.
- Błąd zdublowanych administratorów.
- W przypadku niektórych routerów bezprzewodowych jeśli inny komputer jest ręcznie zalogowany do interfejsu sieci Web, klient McAfee może nie uzyskać dostępu do interfejsu zarządzania w celu dokonania cyklicznej zmiany klucza szyfrowania.

Tematy pokrewne

- Zmienianie poświadczeń dla urządzeń bezprzewodowych (strona 323)
- Automatyczna cykliczna zmiana klucza (strona 326)

Nie można naprawić routera lub punktu dostępu

Jeśli naprawa nie powiedzie się, należy spróbować poniższych metod. Każdą z procedur można wykonać niezależnie od innych.

- Połącz się z siecią za pomocą połączenia kablowego, a następnie ponownie spróbuj ją naprawić.
- Odłącz zasilanie routera lub punktu dostępu, podłącz je ponownie, a następnie ponownie spróbuj się połączyć.
- Zresetuj router bezprzewodowy lub punkt dostępu do ustawień domyślnych i napraw go. Spowoduje to przywrócenie oryginalnych ustawień komunikacji bezprzewodowej. Następnie zresetuj ustawienia połączenia internetowego.
- Korzystając z opcji zaawansowanych, opuść sieć na wszystkich komputerach i zresetuj router bezprzewodowy lub punkt dostępu do ustawień domyślnych, a następnie włącz jego ochronę. Spowoduje to przywrócenie oryginalnych ustawień komunikacji bezprzewodowej. Następnie zresetuj ustawienia połączenia internetowego.

Tematy pokrewne

- Naprawianie ustawień zabezpieczeń sieci (strona 324)

Sieć wydaje się być niechroniona

Jeśli sieć jest wyświetlana jako niezabezpieczona, nie jest chroniona. Aby sieć była bezpieczna, należy włączyć jej ochronę. Należy pamiętać, że program Wireless Network Security działa tylko ze zgodnymi routerami i punktami dostępu.

Tematy pokrewne

- Tworzenie chronionych sieci bezprzewodowych (strona 292)
- Obsługiwane routery bezprzewodowe
  http://www.mcafee.com/router

Łączenie komputerów z siecią

Użytkownik może rozwiązywać następujące problemy z łączeniem komputerów z siecią:

- Oczekiwanie na autoryzację
- Przyznanie dostępu nieznanemu komputerowi

Oczekiwanie na autoryzację

Jeśli w wyniku próby dołączenia do chronionej sieci komputer pozostaje w stanie oczekiwania na autoryzację, należy sprawdzić, czy:

- Komputer bezprzewodowy, który ma już dostęp do sieci jest włączony i połączony z siecią.
- Jest obecna osoba, która może przyznać dostęp na tym komputerze, gdy się pojawi.
- Odległość między komputerami pozwala na komunikację bezprzewodową.

Jeśli opcja **Przyznaj prawa dostępu** nie jest dostępna na komputerze już połączonym z siecią, należy spróbować przyznać dostęp z innego komputera.

Jeśli inne komputery nie są dostępne, należy wyłączyć ochronę sieci z komputera, który ma już do niej dostęp, i włączyć ponownie ochronę z komputera, który nie miał dostępu. Następnie należy dołączyć do sieci z komputera, który ją wcześniej chronił.

Można także użyć funkcji Ochrona innego komputera.

Tematy pokrewne

- Dołączanie do chronionej sieci bezprzewodowej (strona 294)
- Opuszczanie chronionych sieci bezprzewodowych (strona 318)
- Usuwanie routerów bezprzewodowych lub punktów dostępu (strona 315)
- Dodawanie komputerów do chronionej sieci bezprzewodowej (strona 302)

Przyznanie dostępu nieznanemu komputerowi

Po otrzymaniu żądania przyznania dostępu nieznanemu komputerowi można odmówić przyznania mu dostępu do czasu sprawdzenia jego wiarygodności. Może to bowiem być próba uzyskania nieuprawnionego dostępu do sieci.

Łączenie z Internetem i siecią

Użytkownik może rozwiązywać następujące problemy z łączeniem z Internetem i siecią:

- Złe połączenie z Internetem
- Chwilowe przerwy w połączeniu
- Urządzenia (nie komputer użytkownika) tracą połączenie
- Monit o wprowadzenie klucza WEP, WPA lub WPA2
- Nie można połączyć się
- Aktualizacja karty sieci bezprzewodowej
- Niski poziom sygnału
- System Windows nie może skonfigurować połączenia bezprzewodowego
- System Windows nie wykazuje połączenia

Nie można połączyć się z Internetem

Jeśli nie można się połączyć, należy spróbować uzyskać dostęp do sieci za pomocą połączenia kablowego, a następnie połączyć się z Internetem. Jeśli mimo to nie można się połączyć, należy sprawdzić, czy:

- modem jest włączony,
- ustawienia PPPoE są poprawne,
- linia DSL lub kablowa jest aktywna.

Problemy z łącznością, takie jak mała szybkość i słaby sygnał, mogą być także powodowane przez zakłócenia komunikacji bezprzewodowej. Aby rozwiązać problem, należy spróbować następujących metod:

- Zmień kanał używany przez telefon bezprzewodowy.
- Usuń potencjalne źródła zakłóceń.
- Przenieś router bezprzewodowy, punkt dostępu lub komputer w inne miejsce.
- Zmień kanał używany przez router lub punkt dostępu. Użytkownikom w Ameryce Północnej i Południowej zaleca się korzystanie z kanałów 1, 4, 7 i 11. Pozostałym użytkownikom zaleca się korzystanie z kanałów 1, 4, 7 i 13. Wiele routerów domyślnie używa kanału 6.
- Upewnij się, że router i karta sieci bezprzewodowej (zwłaszcza karta USB) nie są skierowane w stronę ściany.
- Upewnij się, że karta USB sieci bezprzewodowej nie znajduje się za routerem bezprzewodowym/punktem dostępu.
- Umieść router z dala od ścian i metalowych obiektów.

Przerywane połączenie

Jeśli jest chwilowo zakłócane (na przykład w czasie gry w trybie online), przyczyną może być cykliczna zmiana klucza. Aby temu zapobiec, można wstrzymać cykliczną zmianę klucza.

Firma McAfee zaleca wznowić cykliczną zmianę klucza jak najszybciej, aby zapewnić pełną ochronę sieci przez hakerami.

Tematy pokrewne

- Automatyczna cykliczna zmiana klucza (strona 326)
- Wznawianie cyklicznej zmiany klucza (strona 327)
- Wstrzymywanie automatycznej cyklicznej zmiany klucza (strona 329)
- Ręczne dokonywanie cyklicznej zmiany klucza (strona 330)

Urządzenia tracą łączność

Jeśli część urządzeń traci połączenie, gdy używany jest program Wireless Network Security, należy spróbować rozwiązać problem, używając następujących metod:

- Wstrzymaj cykliczną zmianę klucza
- Zaktualizuj sterownik karty sieci bezprzewodowej
- Wyłącz menedżera klienta karty sieciowej

Tematy pokrewne

- Wstrzymywanie automatycznej cyklicznej zmiany klucza (strona 329)

Monit o wprowadzenie klucza WEP, WPA lub WPA2

Jeśli aby połączyć się z chronioną siecią bezprzewodową, trzeba wprowadzić klucz WEP, WPA lub WPA-2, prawdopodobnie na komputerze nie zainstalowano oprogramowania.

Aby działać prawidłowo, program Wireless Network Security musi zostać zainstalowany na każdym komputerze bezprzewodowym w sieci.

Tematy pokrewne

- Uruchamianie programu Wireless Network Security (strona 286)
- Dodawanie komputerów do chronionej sieci bezprzewodowej (strona 302)

Nie można połączyć się z siecią bezprzewodową

Jeśli nie można się połączyć, należy spróbować poniższych metod. Każdą z procedur można wykonać niezależnie od innych.

- Jeśli nie jesteś połączony z chroniona siecią, sprawdź, czy masz prawidłowy klucz, i wprowadź go ponownie.
- Odłącz kartę sieci bezprzewodowej i ponownie ją podłącz, lub wyłącz ją i ponownie włącz.
- Wyłącz router lub punkt dostępu, a następnie ponownie spróbuj się połączyć.
- Sprawdź, czy router bezprzewodowy lub punkt dostępu jest połączony, i napraw ustawienia zabezpieczeń.
- Uruchom ponownie komputer.
- Zaktualizuj kartę sieci bezprzewodowej lub kup nową. Sieć może na przykład korzystać z zabezpieczeń WPA-PSK TKIP, a karta sieci bezprzewodowej może nie obsługiwać tego trybu (sieci wykazują, że działają w trybie WEP, mimo że faktycznie są ustawione na tryb WPA).
- Jeśli po uaktualnieniu routera bezprzewodowego lub punktu dostępu nadal nie możesz się połączyć, nowa wersja routera może nie być obsługiwana. Sprawdź, czy router lub punkt dostępu jest obsługiwany. Jeśli nie jest, przywróć wersję obsługiwaną lub poczekaj na odpowiednie uaktualnienie programu Wireless Security.

Tematy pokrewne

- Naprawianie ustawień zabezpieczeń sieci (strona 324)
- Aktualizowanie karty sieci bezprzewodowej (strona 358)

Aktualizacja karty sieci bezprzewodowej

Korzystanie z programu Wireless Network Security może wymagać zaktualizowania karty sieci bezprzewodowej.

Aby zaktualizować kartę sieciową:

1. Na pulpicie kliknij przycisk **Start**, wskaż polecenie **Ustawienia**, a następnie kliknij polecenie **Panel sterowania**.
2. Kliknij dwukrotnie ikonę **System**. Zostanie wyświetlone okno dialogowe **Właściwości systemu**.
3. Wybierz kartę **Sprzęt**, a następnie kliknij przycisk **Menedżer urządzeń**.
4. Na liście Menedżera urządzeń kliknij dwukrotnie kartę sieciową.
5. Wybierz kartę **Sterownik** i zanotuj nazwę posiadanego sterownika.
6. Przejdź do witryny sieci Web producenta karty sieciowej i znajdź aktualizację. Sterowniki znajdują się zwykle w sekcji pomocy technicznej lub plików do pobrania. Jeżeli korzystasz z karty miniPCI, przejdź do witryny producenta komputera, a nie karty.
7. Jeśli aktualizacja sterownika jest dostępna, postępuj zgodnie z instrukcjami w witrynie sieci Web, aby ją pobrać.
8. Wróć na kartę **Sterownik** i kliknij przycisk **Aktualizuj sterownik**. Pojawi się kreator systemu Windows.
9. Aby zainstalować sterownik, postępuj zgodnie z instrukcjami w witrynie sieci Web.

Niski poziom sygnału

Jeśli połączenie jest przerywane lub wolne, poziom sygnału może być zbyt niski. Aby poprawić sygnał, należy spróbować poniższych metod:

- Upewnij się, że urządzenia bezprzewodowe nie są blokowane przez metalowe obiekty, na przykład piece, przewody wentylacyjne lub duże urządzenia. Sygnał sieci bezprzewodowej jest tłumiony przez takie obiekty.
- Jeśli sygnał przenika przez ścianę, upewnij się, że nie robi tego pod ostrym kątem. Im dłuższa droga w ścianie, tym bardziej sygnał słabnie.
- Jeśli router bezprzewodowy lub punkt dostępu ma więcej niż jedną antenę, ustaw je poprzecznie w stosunku do siebie (jedną poziomo, a drugą pionowo — pod kątem 90 stopni).
- Niektórzy producenci oferują anteny wzmacniające sygnał. Anteny kierunkowe zapewniają większy zasięg, natomiast dookólne — największą wszechstronność zastosowań. Instalując antenę, należy postępować zgodnie z instrukcjami producenta.

Jeśli powyższe kroki nie przyniosą poprawy, należy dodać do sieci punkt dostępu, który będzie znajdował się bliżej komputera, z którym użytkownik chce się połączyć. Jeśli drugi punkt dostępu zostanie skonfigurowany z zastosowaniem tej samej nazwy sieciowej (SSID) i innego kanału, karta sieciowa automatycznie znajdzie najsilniejszy sygnał i nawiąże połączenie poprzez właściwy punkt dostępu.

Tematy pokrewne

- Ikony mocy sygnału (strona 309)
- Wyświetlanie mocy sygnału sieci (strona 339)

System Windows nie obsługuje połączenia bezprzewodowego

Jeśli komunikat systemu Windows o błędzie wskazuje, że system nie może skonfigurować połączenia bezprzewodowego, można go zignorować. Łączenie z siecią i konfigurowanie sieci bezprzewodowych umożliwia program Wireless Network Security.

Należy upewnić się, że pole wyboru **Użyj systemu Windows do konfiguracji ustawień sieci bezprzewodowej** na karcie Sieci bezprzewodowe okna dialogowego Właściwości połączenia sieci bezprzewodowej systemu Windows jest wyczyszczone.

Program Wireless Network Security pozwala:

- Kartom zainstalowanym na komputerach z systemem Windows 2000 na łączenie się z sieciami WPA, nawet jeśli menedżer klienta karty sieciowej nie jest obsługiwany.
- Kartom zainstalowanym na komputerach z systemem Windows XP na łączenie się z sieciami WPA2, bez konieczności instalowania pakietu poprawek SP2.
- Kartom zainstalowanym na komputerach z systemem Windows XP SP1 na łączenie się z sieciami WPA i WPA2, bez konieczności instalowania pakietu poprawek, który nie jest obsługiwany przez system Windows XP SP1.

System Windows nie wykazuje połączenia

Jeśli użytkownik jest połączony, ale ikona połączenia sieciowego w systemie Windows wykazuje brak połączenia (znak X), można to zignorować. Połączenie działa prawidłowo.

Inne problemy

Użytkownik może rozwiązywać następujące problemy:

- Nazwa sieci jest inna niż używana przez pozostałe programy
- Problem z konfigurowaniem routerów bezprzewodowych lub punktów dostępu
- Zamiana komputerów
- Wybór innego trybu zabezpieczeń
- Oprogramowanie nie działa po uaktualnieniu systemów operacyjnych

Nazwa sieci różni się od używanej przez inne programy

Jeśli nazwa sieci jest inna niż prezentowana przez inne programy (na przykład zawiera frazę „_SafeAaf”), jest to normalne.

Program Wireless Network Security oznacza chronione przez siebie sieci odpowiednim kodem.

Konfigurowanie routerów bezprzewodowych lub punktów dostępu

Jeśli podczas konfigurowania routera lub punktu dostępu bądź dodawania do sieci wielu routerów lub punktów dostępu wyświetlany jest komunikat o błędzie, należy sprawdzić, czy wszystkie routery i punkty dostępu mają odrębne adresy IP.

Jeśli nazwa routera bezprzewodowego lub punktu dostępu jest widoczna w oknie dialogowym Chroń router bezprzewodowy/punkt dostępu, ale próba jego skonfigurowania powoduje wystąpienie błędu: Sprawdź, czy router lub punkt dostępu jest obsługiwany.

Jeśli router lub punkt dostępu jest skonfigurowany, ale zdaje się nie być połączony z właściwą siecią (na przykład nie widać innych komputerów w sieci LAN), należy sprawdzić, czy skonfigurowany został właściwy router lub punkt dostępu (własny, a nie, na przykład, należący do sąsiada). W tym celu należy odłączyć zasilanie routera lub punktu dostępu i upewnić się, że połączenie zostanie przerwane. Jeśli skonfigurowany został niewłaściwy router lub punkt dostępu, należy wyłączyć jego ochronę i włączyć ochronę właściwego routera lub punktu dostępu.

Jeśli nie można skonfigurować ani dodać routera lub punktu dostępu, który jest obsługiwany, niektóre z dokonanych zmian mogą uniemożliwiać jego prawidłowe skonfigurowanie.

- Postępuj zgodnie z instrukcjami producenta routera lub punktu dostępu, aby skonfigurować jego ustawienia DHCP lub adres IP. Niektórzy producenci zapewniają odpowiednie narzędzia konfiguracyjne.
- Zresetuj router bezprzewodowy lub punkt dostępu do domyślnych ustawień fabrycznych i ponownie spróbuj naprawić sieć. Być może zmieniony został port administracji routera lub punktu dostępu bądź wyłączona została administracja przez połączenie bezprzewodowe. Upewnij się, że używasz konfiguracji domyślnej, a konfiguracja sieci bezprzewodowej jest włączona. Inną możliwą przyczyną jest wyłączenie administracji za pośrednictwem protokołu http. W takim przypadku należy sprawdzić, czy administracja za pośrednictwem protokołu http jest włączona. Do administrowania urządzeniem należy używać portu 80.
- Jeśli router bezprzewodowy lub punkt dostępu nie znajduje się na liście routerów bezprzewodowych i punktów dostępu, które są chronione i z którymi komputer się łączy, należy włączyć rozgłaszanie identyfikatora SSID i sprawdzić, czy router lub punkt dostępu jest widoczny na liście dostępnych sieci bezprzewodowych w programie Wireless Network Security.
- Przyczyną rozłączenia lub problemów z nawiązaniem połączenia może być włączone filtrowanie adresów MAC. Wyłącz filtrowanie adresów MAC.
- Jeśli nie można wykonywać działań w sieci (na przykład udostępniać plików i drukować na udostępnianych drukarkach) między dwoma komputerami połączonymi bezprzewodowo z siecią, należy

sprawdzić, czy nie została włączona izolacja punktu dostępu. Izolacja punktu dostępu zapobiega łączeniu się dwóch komputerów w sieci ze sobą.

- Jeśli używana jest zapora programowa inna niż McAfee Personal Firewall, należy upewnić się, że podsieć jest wiarygodna.

Tematy pokrewne

- Obsługiwane routery bezprzewodowe http://www.mcafee.com/router

Zamiana komputerów

Jeśli komputer, który chronił sieć został zastąpiony innym, i żaden z pozostałych komputerów nie ma dostępu do sieci (uzyskanie dostępu do sieci jest zupełnie niemożliwe), należy zresetować router bezprzewodowy lub punkt dostępu do domyślnych ustawień fabrycznych i ponownie włączyć ochronę sieci.

Wybór innego trybu zabezpieczeń

Jeśli komunikat o błędzie stwierdza, że wybrany tryb zabezpieczeń nie jest obsługiwany przez kartę sieci bezprzewodowej, należy wybrać inny tryb zabezpieczeń.

- Wszystkie karty sieciowe obsługują zabezpieczenia WEP.
- Większość kart obsługujących zabezpieczenia WPA korzysta zarówno z trybu WPA-PSK TKIP, jak i WPA-PSK AES.
- Karty obsługujące zabezpieczenia WPA2 korzystają z trybów zabezpieczeń WPA, a także trybów WPA2-PSK TKIP, WPA2-PSK AES i WPA2-PSK TKIP/AES.

Tematy pokrewne

- Konfigurowanie ustawień zabezpieczeń (strona 320)
- Wyświetlanie trybu zabezpieczeń sieci (strona 338)

Oprogramowanie ulega awarii po uaktualnieniu systemów operacyjnych

Jeśli program Wireless Network Security uległ awarii po uaktualnieniu systemów operacyjnych, należy go usunąć i zainstalować ponownie.

ROZDZIAŁ 46

McAfee EasyNetwork

Program McAfee® EasyNetwork umożliwia bezpieczne udostępnianie plików, upraszcza ich przesyłanie oraz automatyzuje proces udostępniania drukarek innym komputerom w obrębie sieci domowej.

Przed przystąpieniem do użytkowania programu EasyNetwork można zapoznać się z jego niektórymi najczęściej używanymi funkcjami. Szczegółowe informacje na temat konfigurowania tych funkcji i korzystania z nich zamieszczono w pomocy programu EasyNetwork.

W tym rozdziale

Funkcje....364
Konfigurowanie programu EasyNetwork....365
Udostępnianie i wysyłanie plików....373
Udostępnianie drukarek....379

Funkcje

Program EasyNetwork jest wyposażony w następujące funkcje:

Udostępnianie plików

Program EasyNetwork ułatwia udostępnianie plików na komputera innym komputerom w sieci. Udostępniając pliki innym komputerom w sieci, przyznaje się im tylko uprawnienia do odczytu. Jedynie komputery należące do zarządzanej sieci (czyli komputery z uprawnieniami pełnego dostępu lub uprawnieniami administratora) mogą udostępniać pliki i mieć dostęp do plików udostępnianych przez innych użytkowników.

Przesyłanie plików

Można wysyłać pliki do innych komputerów należących do zarządzanej sieci. Po odebraniu pliku pojawia się on w skrzynce odbiorczej programu EasyNetwork. Skrzynka odbiorcza jest tymczasowym miejscem przechowywania dla wszystkich plików przysyłanych przez inne komputery w sieci.

Automatyczne udostępnianie drukarek

Po przyłączeniu komputera do zarządzanej sieci program EasyNetwork automatycznie udostępnia wszystkie lokalne drukarki podłączone do komputera, traktując aktualne nazwy drukarek jako nazwy drukarek udostępnionych. Wykrywa również drukarki udostępniane przez inne komputery w sieci i pozwala na ich konfigurowanie i używanie.

ROZDZIAŁ 47

Konfigurowanie programu EasyNetwork

Aby można było korzystać z funkcji programu EasyNetwork, należy uruchomić go i dołączyć do zarządzanej sieci. Po dołączeniu do sieci można ją opuścić w każdej chwili.

W tym rozdziale

Uruchamianie programu EasyNetwork 366
Dołączanie do sieci zarządzanej 367
Opuszczanie zarządzanej sieci 371

Uruchamianie programu EasyNetwork

Domyślnie natychmiast po instalacji jest wyświetlany monit o uruchomienie programu EasyNetwork, jednak program EasyNetwork można także uruchomić później.

Uruchom program EasyNetwork

Domyślnie natychmiast po instalacji jest wyświetlany monit o uruchomienie programu EasyNetwork, jednak program EasyNetwork można także uruchomić później.

Aby uruchomić program EasyNetwork:

- W menu **Start** wybierz polecenie **Programy**, następnie polecenie **McAfee**, a potem kliknij polecenie **McAfee EasyNetwork**.

Wskazówka: Jeśli podczas instalacji została wyrażona zgoda na utworzenie ikon na pulpicie oraz ikon szybkiego uruchamiania, program EasyNetwork można też uruchomić, klikając dwukrotnie ikonę McAfee EasyNetwork na pulpicie lub klikając ikonę McAfee EasyNetwork w obszarze powiadomień znajdującym się w prawej części paska zadań.

Dołączanie do sieci zarządzanej

Po zainstalowaniu programu SecurityCenter na komputerze jest uruchamiany działający w tle agent sieciowy. W programie EasyNetwork agent sieciowy jest odpowiedzialny za wykrywanie prawidłowego połączenia sieciowego, wykrywanie lokalnych drukarek do udostępnienia oraz monitorowanie stanu sieci.

Jeśli na żadnym innym komputerze w sieci, z którą jest połączony komputer nie zostanie znaleziony działający agent sieciowy, komputer automatycznie staje się członkiem sieci i wyświetlany jest monit z prośbą o określenie, czy sieć jest zaufana. Ponieważ jest to pierwszy komputer dołączany do sieci, nazwa komputera staje się częścią nazwy sieci. Nazwę sieci można jednak w każdej chwili zmienić.

Gdy komputer nawiązuje połączenie z siecią, do wszystkich pozostałych komputerów podłączonych w danej chwili do sieci jest wysyłane żądanie dołączenia do niej. Żądanie to może zostać zaakceptowane przez dowolny komputer z uprawnieniami administracyjnymi w danej sieci. Z takiego komputera można również określić poziom uprawnień dla komputerów dołączonych w danej chwili do sieci, na przykład poziom Gościa (tylko możliwość przesyłania plików) lub poziom pełny/administracyjny (możliwość przesyłania i udostępniania plików). W sieci zarządzanej przez program EasyNetwork z komputerów z dostępem administracyjnym można przyznawać prawo dostępu innym komputerom oraz zarządzać uprawnieniami (to znaczy podwyższać lub obniżać poziom uprawnień komputerów). Zadań administracyjnych nie można przeprowadzać z komputerów z dostępem pełnym. Przed uzyskaniem przez komputer zgody na dołączenie do sieci zostają sprawdzone jego zabezpieczenia.

Uwaga: Po dołączeniu do sieci, jeśli na komputerze są zainstalowane inne programy sieciowe McAfee (na przykład McAfee Wireless Network Security lub Network Manager), w programach tych dany komputer jest również rozpoznawany jako komputer zarządzany. Poziom uprawnień przypisany do komputera dotyczy wszystkich programów sieciowych McAfee. Aby uzyskać więcej informacji o znaczeniu uprawnień gościa, pełnych i administracyjnych w innych programach sieciowych McAfee, należy zapoznać się z dokumentacją danego programu.

Dołączanie do sieci

Gdy komputer po zainstalowaniu programu EasyNetwork po raz pierwszy nawiązuje połączenie z siecią zaufaną, wyświetlane jest pytanie, czy ma zostać dołączony do sieci zarządzanej. Gdy zostanie wyrażona zgoda na dołączenie komputera, do wszystkich pozostałych komputerów w sieci z uprawnieniami administracyjnymi jest wysyłane żądanie. Aby komputer mógł udostępniać drukarki lub pliki i wysyłać lub kopiować pliki w sieci, żądanie musi zostać zaakceptowane. Jeśli dany komputer jest pierwszym komputerem w sieci, automatycznie otrzymuje w niej uprawnienia administracyjne.

Aby dołączyć komputer do sieci:

1. W oknie Udostępniane pliki kliknij opcję **Tak, dołącz teraz komputer do sieci**.
   Gdy komputer administracyjny w sieci zaakceptuje to żądanie, zostanie wyświetlony komunikat z pytaniem, czy zezwolić temu komputerowi i pozostałym komputerom w sieci na wzajemne zarządzanie ustawieniami zabezpieczeń.
2. Aby zezwolić temu komputerowi i pozostałym komputerom w sieci na wzajemne zarządzanie ustawieniami zabezpieczeń, kliknij przycisk **Tak**. Aby nie zezwolić na to, kliknij przycisk **Nie**.
3. Potwierdź, czy na komputerze akceptującym żądanie są wyświetlane karty do gry, które w danej chwili są wyświetlane w oknie dialogowym potwierdzania zabezpieczeń, a następnie kliknij opcję **Potwierdź**.

Uwaga: Jeśli na komputerze akceptującym żądanie nie są wyświetlane te same karty, które są widoczne w oknie dialogowym potwierdzania zabezpieczeń, oznacza to, że w sieci zarządzanej doszło do naruszenia zabezpieczeń. Dołączenie do sieci mogłoby stanowić zagrożenie dla komputera, dlatego w takiej sytuacji w oknie dialogowym potwierdzania zabezpieczeń należy kliknąć opcję **Odrzuć**.

Przyznawanie dostępu do sieci zarządzanej

Gdy komputer żąda dołączenia do sieci zarządzanej, do komputerów w sieci mających uprawnienia administracyjne jest wysyłany komunikat. Pierwszy komputer, który odpowie na komunikat, uzyskuje status przyznającego prawa. Jego użytkownik jest odpowiedzialny za decyzję, który typ dostępu przyznać komputerowi: gość, pełny czy administrator.

Aby przyznać dostęp do sieci:

1. W oknie alertu zaznacz jedno z następujących pól wyboru:
   - **Przyznaj dostęp typu Gość**: Pozwala użytkownikowi na wysyłanie plików do pozostałych komputerów, lecz nie zezwala na udostępnianie plików.

- **Przyznaj dostęp Pełny do wszystkich zarządzanych aplikacji sieciowych**: Pozwala użytkownikowi na wysyłanie i udostępnianie plików.
- **Przyznaj dostęp Administrator do wszystkich zarządzanych aplikacji sieciowych**: Pozwala użytkownikowi na wysyłanie i udostępnianie plików, przyznawanie dostępu pozostałym komputerom oraz zmianę poziomów uprawnień innych komputerów.

2 Kliknij opcję **Przyznaj prawa dostępu**.

3 Potwierdź, że na komputerze są wyświetlane karty do gry, które w danej chwili są wyświetlane w oknie dialogowym potwierdzania zabezpieczeń, a następnie kliknij opcję **Potwierdź**.

Uwaga: Jeśli na komputerze nie są wyświetlane te same karty, które są widoczne w oknie dialogowym potwierdzania zabezpieczeń, oznacza to, że w sieci zarządzanej doszło do naruszenia zabezpieczeń. Przyznanie temu komputerowi dostępu do sieci mogłoby stanowić zagrożenie własnego komputera, dlatego w takiej sytuacji w oknie dialogowym potwierdzania zabezpieczeń kliknij przycisk **Odrzuć**.

Zmiana nazwy sieci

Domyślnie nazwa sieci zawiera nazwę pierwszego komputera, który do niej dołączył. Nazwę sieci można jednak w każdej chwili zmienić. Gdy zmieniona zostaje nazwa sieci, zmienia się opis sieci wyświetlany w programie EasyNetwork.

Aby zmienić nazwę sieci:

1. W menu **Opcje** kliknij polecenie **Konfiguruj**.
2. W oknie dialogowym Konfigurowanie wpisz nazwę sieci w polu **Nazwa sieci**.
3. Kliknij przycisk **OK**.

Opuszczanie zarządzanej sieci

Jeśli użytkownik dołączy do zarządzanej sieci, a następnie zrezygnuje z przynależności do niej, może tę sieć opuścić. Po zrzeczeniu się przynależności do sieci użytkownik może do niej w każdej chwili na nowo dołączyć, przy czym musi mu zostać ponownie przyznane prawo dołączenia do sieci i ponownie muszą zostać sprawdzone zabezpieczenia komputera. Więcej informacji można znaleźć w sekcji Dołączanie do zarządzanej sieci (strona 367).

Opuszczanie zarządzanej sieci

Użytkownik może opuścić zarządzaną sieć, do której wcześniej dołączył.

Aby opuścić zarządzaną sieć:

1. W menu **Narzędzia** kliknij polecenie **Opuść sieć**.
2. W oknie dialogowym Opuść sieć wybierz nazwę sieci, którą chcesz opuścić.
3. Kliknij opcję **Opuść sieć**.

ROZDZIAŁ 48

Udostępnianie i wysyłanie plików

Program EasyNetwork ułatwia udostępnianie plików znajdujących się na danym komputerze i wysyłanie ich do innych komputerów w sieci. Udostępniając pliki innym komputerom w sieci, przyznaje się im tylko uprawnienia do odczytu. Jedynie komputery należące do zarządzanej sieci (czyli komputery z uprawnieniami pełnego dostępu lub uprawnieniami administratora) mogą udostępniać pliki i mieć dostęp do plików udostępnianych przez innych użytkowników.

W tym rozdziale

Udostępnianie plików.....374
Wysyłanie plików do innych komputerów.....377

Udostępnianie plików

Program EasyNetwork ułatwia udostępnianie plików komputera innym komputerom w sieci. Udostępniając pliki innym komputerom w sieci, przyznaje się im tylko uprawnienia do odczytu. Jedynie komputery należące do zarządzanej sieci (czyli komputery z uprawnieniami pełnego dostępu lub uprawnieniami administratora) mogą udostępniać pliki i mieć dostęp do plików udostępnianych przez innych użytkowników. Jeśli udostępniany jest folder, udostępniane są wszystkie pliki zawarte w tym folderze i w jego podfolderach. Kolejne pliki dodawane do tego folderu nie są automatycznie udostępniane. Jeśli udostępniany plik lub folder zostaje usunięty, automatycznie zostaje usunięty z okna Udostępniane pliki. Udostępnianie pliku można zakończyć w każdej chwili.

Dostęp do udostępnianego pliku odbywa się na dwa sposoby: przez otwarcie pliku bezpośrednio w programie EasyNetwork lub przez skopiowanie pliku do dowolnego miejsca na komputerze, a następnie otwarcie go. Jeśli lista udostępnianych plików staje się długa, udostępniane pliki, które są potrzebne, można wyszukać.

Uwaga: Dostęp do plików udostępnianych przy użyciu programu EasyNetwork nie jest możliwy z innych komputerów przy użyciu Eksploratora Windows. Udostępnianie plików w programie EasyNetwork odbywa się poprzez połączenia bezpieczne.

Udostępnianie pliku

Gdy plik zostaje udostępniony, automatycznie staje się dostępny dla wszystkich innych członków z pełnym lub administracyjnym dostępem do sieci zarządzanej.

Aby udostępnić plik:

1. W Eksploratorze Windows znajdź plik, który ma być udostępniany.
2. Przeciągnij plik z miejsca, w którym się znajduje w Eksploratorze Windows, do okna Udostępniane pliki w programie EasyNetwork.

Wskazówka: Plik można również udostępnić inaczej, klikając polecenie **Udostępnij pliki** w menu **Narzędzia**. W oknie dialogowym Udostępnij przejdź do folderu zawierającego plik, który ma być udostępniony, zaznacz ten plik, a następnie kliknij opcję **Udostępnij**.

Kończenie udostępniania pliku

Jeśli plik jest udostępniany w sieci zarządzanej, udostępnianie można w każdej chwili zakończyć. Gdy udostępnianie pliku zostanie zakończone, inne komputery należącej do danej sieci zarządzanej nie będą już miały do niego dostępu.

Aby zakończyć udostępnianie pliku:

1. W menu **Narzędzia** kliknij polecenie **Zakończ udostępnianie plików**.
2. W oknie dialogowym Zakończ udostępnianie plików zaznacz plik, który ma już nie być udostępniany.
3. Kliknij opcję **Nie udostępniaj**.

Kopiowanie udostępnianego pliku

Udostępniane pliki można skopiować na własny komputer z dowolnego komputera w zarządzanej sieci. Dzięki temu, nawet jeśli dany komputer zakończy udostępnianie pliku, użytkownik ma jego kopię.

Aby skopiować plik:

- Przeciągnij plik z okna Udostępniane pliki w programie EasyNetwork w dowolne miejsce w Eksploratorze Windows lub na pulpit systemu Windows.

Wskazówka: Udostępniany plik można również skopiować, zaznaczając plik w programie EasyNetwork, a następnie klikając polecenie **Kopiuj do** w menu **Narzędzia**. W oknie dialogowym Kopiuj do przejdź do folderu, do którego plik ma zostać skopiowany, zaznacz go, a następnie kliknij opcję **Zapisz**.

Wyszukiwanie udostępnianego pliku

Możliwe jest wyszukiwanie pliku, który został udostępniony na komputerze użytkownika lub innym komputerze należącym do danej sieci. W miarę wpisywania kryteriów wyszukiwania program EasyNetwork automatycznie wyświetla odpowiadające im wyniki w oknie Udostępniane pliki.

Aby wyszukać udostępniany plik:

1. W oknie Udostępniane pliki kliknij opcję **Wyszukaj**.
2. Kliknij jedną z następujących opcji na liście **Zawiera**:
   - **Zawiera wszystkie słowa**: Powoduje wyszukanie nazw plików lub ścieżek zawierających wszystkie słowa określone na liście **Nazwa pliku lub ścieżka do pliku**, w dowolnej kolejności.

- **Zawiera którekolwiek ze słów**: Powoduje wyszukanie nazw plików lub ścieżek zawierających którekolwiek ze słów określonych na liście **Nazwa pliku lub ścieżka do pliku**.
- **Zawiera cały łańcuch znaków**: Powoduje wyszukanie nazw plików lub ścieżek zawierających całą frazę określoną na liście **Nazwa pliku lub ścieżka do pliku**.

3 Wpisz część, całą nazwę pliku lub ścieżki na liście **Nazwa pliku lub ścieżka do pliku**.

4 Kliknij jeden z następujących typów pliku na liście **Typ**:

- **Any** (Dowolny): Powoduje wyszukanie wszystkich typów udostępnianych plików.
- **Dokument**: Powoduje wyszukanie wszystkich udostępnianych dokumentów.
- **Obraz**: Powoduje wyszukanie wszystkich udostępnianych plików obrazów.
- **Wideo**: Powoduje wyszukanie wszystkich udostępnianych plików wideo.
- **Audio**: Powoduje wyszukanie wszystkich udostępnianych plików audio.

5 Na listach **Od** i **Do** kliknij daty odpowiadające zakresowi dat utworzenia pliku.

Wysyłanie plików do innych komputerów

Możliwe jest wysyłanie plików do innych komputerów należących do danej sieci zarządzanej. Przed wysłaniem pliku program EasyNetwork sprawdza, czy na komputerze odbierającym plik jest dostatecznie dużo dostępnego miejsca na dysku.

Gdy plik zostaje odebrany, pojawia się w skrzynce odbiorczej programu EasyNetwork. Skrzynka odbiorcza to miejsce tymczasowego przechowywania wszystkich plików przysyłanych z innych komputerów w sieci. Jeśli program EasyNetwork jest otwarty podczas odbierania pliku, plik ten natychmiast pojawia się w skrzynce odbiorczej; w przeciwnym razie wyświetlany jest komunikat w obszarze powiadomień w prawej części paska zadań systemu Windows. Jeśli użytkownik nie chce, aby były wyświetlane komunikaty z powiadomieniami, można je wyłączyć. Jeśli w skrzynce odbiorczej już istnieje plik o tej samej nazwie, nazwa nowego pliku zostaje zmieniona za pomocą przyrostka liczbowego. Pliki pozostają w skrzynce odbiorczej do czasu, aż zostaną zaakceptowane (czyli skopiowane do wybranego miejsca na komputerze).

Wysyłanie pliku do innego komputera

Możliwe jest wysłanie pliku do innego komputera w zarządzanej sieci bez jego udostępniania. Aby użytkownik na komputerze odbiorczym mógł przejrzeć plik, musi go na nim zapisać. Więcej informacji można znaleźć w sekcji Przyjmowanie pliku z innego komputera (strona 378).

Aby wysłać plik do innego komputera:

1. W Eksploratorze Windows znajdź plik, który ma zostać wysłany.
2. Przeciągnij plik z miejsca, w którym się znajduje w Eksploratorze Windows na ikonę aktywnego komputera w programie EasyNetwork.

Wskazówka: Można wysłać wiele plików jednocześnie do danego komputera, naciskając podczas zaznaczania plików klawisz CTRL. Pliki można również wysyłać, klikając polecenie **Wyślij** w menu **Narzędzia**, zaznaczając pliki, a następnie klikając opcję **Wyślij**.

Przyjmowanie pliku z innego komputera

Jeśli inny komputer w sieci zarządzanej przysyła plik, musi on zostać przyjęty (przez zapisanie go w folderze na lokalnym komputerze). Jeśli program EasyNetwork nie jest otwarty lub nie jest na pierwszym planie na pulpicie, gdy plik jest przysyłany do lokalnego komputera, wyświetlany jest komunikat w obszarze powiadomień w prawej części paska zadań systemu Windows. Kliknij komunikat z powiadomieniem, aby otworzyć program EasyNetwork i uzyskać dostęp do tego pliku.

Aby odebrać plik z innego komputera:

- Kliknij opcję **Odebrane**, a następnie przeciągnij plik ze skrzynki odbiorczej programu EasyNetwork do folderu w Eksploratorze Windows.

Wskazówka: Plik z innego komputera można również odebrać, zaznaczając go w skrzynce odbiorczej programu EasyNetwork, a następnie klikając polecenie **Akceptuj** w menu **Narzędzia**. W oknie dialogowym Przyjmij do folderu przejdź do folderu, w którym mają zostać zapisane odbierane pliki, zaznacz go, a następnie kliknij opcję **Zapisz**.

Odbieranie powiadomienia o wysłaniu pliku

Użytkownik może otrzymać powiadomienie o wysłaniu do niego pliku z innego komputera w zarządzanej sieci. Jeśli program EasyNetwork nie jest w danej chwili otwarty lub nie jest na pierwszym planie na pulpicie, wyświetlany jest komunikat w obszarze powiadomień w prawej części paska zadań systemu Windows.

Aby otrzymywać powiadomienia, gdy zostaje wysłany plik:

1. W menu **Opcje** kliknij polecenie **Konfiguruj**.
2. W oknie dialogowym Konfiguruj zaznacz pole wyboru **Powiadom mnie, kiedy inny komputer wysyła do mnie pliki**.
3. Kliknij przycisk **OK**.

ROZDZIAŁ 49

Udostępnianie drukarek

Gdy komputer zostaje dołączony do zarządzanej sieci, program EasyNetwork automatycznie udostępnia wszystkie lokalne drukarki podłączone do danego komputera. Ponadto wykrywa drukarki udostępniane przez inne komputery w sieci oraz umożliwia ich konfigurowanie i używanie.

W tym rozdziale

Praca z udostępnianymi drukarkami 380

Praca z udostępnianymi drukarkami

Po przyłączeniu komputera do zarządzanej sieci program EasyNetwork automatycznie udostępnia wszystkie lokalne drukarki podłączone do komputera, traktując aktualne nazwy drukarek jako nazwy drukarek udostępnionych. Wykrywa również drukarki udostępniane przez inne komputery w sieci i pozwala na ich konfigurowanie i używanie. Jeśli sterownik drukarki został skonfigurowany do druku za pośrednictwem sieciowego serwera druku (na przykład bezprzewodowego serwera druku USB), program EasyNetwork traktuje taką drukarkę jako lokalną i automatycznie udostępnia ją w sieci. Udostępnianie drukarki można zakończyć w każdej chwili.

Ponadto program EasyNetwork wykrywa drukarki udostępniane przez wszystkie pozostałe komputery w sieci. Jeśli program wykryje zdalną drukarkę, która nie jest jeszcze podłączona do lokalnego komputera, przy pierwszym otwarciu programu EasyNetwork w oknie Udostępniane pliki pojawi się łącze **Dostępne drukarki sieciowe**. Umożliwia to zainstalowanie dostępnych drukarek lub odinstalowanie drukarek już podłączonych do danego komputera. Można również odświeżyć listę drukarek wykrytych w sieci.

Jeśli komputer nie został jeszcze dołączony do zarządzanej sieci, lecz już jest z nią połączony, dostęp do udostępnianych drukarek jest możliwy za pomocą standardowego panelu sterowania systemu Windows.

Kończenie udostępniania drukarki

Udostępnianie drukarki można w każdej chwili zakończyć. Należące do sieci komputery, na których zainstalowano daną drukarkę, nie będą już mogły na niej drukować.

Aby zakończyć udostępnianie drukarki:

1. W menu **Narzędzia** kliknij polecenie **Drukarki**.
2. W oknie dialogowym Zarządzaj drukarkami sieciowymi kliknij nazwę drukarki, której udostępnianie ma być zakończone.
3. Kliknij opcję **Nie udostępniaj**.

Instalowanie dostępnej drukarki sieciowej

Komputer należący do sieci zarządzanej może korzystać z drukarek udostępnianych w tej sieci. W tym celu należy zainstalować sterownik obsługujący daną drukarkę. Jeśli właściciel drukarki, która wcześniej została zainstalowana na danym komputerze, zakończy jej udostępnianie, drukowanie na niej z tego komputera nie będzie już możliwe.

Aby zainstalować dostępną drukarkę sieciową:

1. W menu **Narzędzia** kliknij polecenie **Drukarki**.
2. W oknie dialogowym Dostępne drukarki sieciowe kliknij nazwę drukarki.
3. Kliknij opcję **Zainstaluj**.

ROZDZIAŁ 50

Referencja

W Słowniku terminów znajdują się najczęściej stosowane w produktach firmy McAfee terminy związane z bezpieczeństwem i ich definicje.

Dokument Informacje o firmie McAfee zawiera informacje prawne dotyczące firmy McAfee Corporation.

Słownik

8

802.11

Zestaw standardów IEEE technologii bezprzewodowej sieci LAN. Standard 802.11 definiuje interfejs radiowy pomiędzy klientem bezprzewodowym a stacją bazową lub dwoma klientami bezprzewodowymi. Specyfikacje standardu 802.11 obejmują 802.11a, standard sieci o przepustowości do 54 Mb/s w paśmie 5 GHz, 802.11b, standard sieci o przepustowości do 11 Mb/s w paśmie 2,4 GHz, 802.11g, standard sieci o przepustowości do 54 Mb/s w paśmie 2,4 GHz, oraz 802.11i, pakiet standardów zabezpieczeń bezprzewodowej sieci Ethernet.

802.11a

Rozszerzenie standardu 802.11 stosowane w bezprzewodowych sieciach LAN, umożliwiające przesyłanie danych z prędkością do 54 Mb/s w paśmie 5 GHz. Prędkość transmisji jest większa niż w przypadku standardu 802.11b, jednak zasięg jest znacznie mniejszy.

802.11b

Rozszerzenie standardu 802.11 stosowane w bezprzewodowych sieciach LAN, umożliwiające transmisję z prędkością 11 Mb/s w paśmie 2,4 GHz. 802.11b jest obecnie uważany za standard sieci bezprzewodowej.

802.11g

Rozszerzenie standardu 802.11 stosowane w bezprzewodowych sieciach LAN, umożliwiające transmisję z prędkością do 54 Mb/s w paśmie 2,4 GHz.

802.1x

Ten standard nie jest obsługiwany przez oprogramowanie Wireless Home Network Security. Jest to standard IEEE definiujący uwierzytelnianie w sieciach przewodowych i bezprzewodowych, najczęściej stosowany w połączeniu ze standardem sieci bezprzewodowej 802.11. Zapewnia on silne, wzajemne uwierzytelnianie pomiędzy klientem a serwerem uwierzytelniania. Ponadto standard 802.1x może zapewniać dynamiczne klucze WEP przydzielane podczas każdej sesji poszczególnym użytkownikom, likwidując obciążenia administracyjne i zagrożenia bezpieczeństwa związane ze statycznymi kluczami WEP.

A

adres IP

Adres protokołu internetowego lub inaczej adres IP to unikalna liczba składająca się z czterech części oddzielonych kropkami (np. 63.227.89.66). Każdy komputer w Internecie od największego serwera do komputera przenośnego komunikującego się przez telefon komórkowy ma unikatowy numer IP. Nie każdy komputer ma swoją nazwę domeny, ale każdy posiada adres IP.

Na poniższej liście znajdują się szczególne typy adresów IP:

- Nierutowalne adresy IP: znane również jako „prywatna przestrzeń adresowa IP". Są to adresy IP, które nie mogą być używane w Internecie. Prywatne bloki adresów IP to 10.x.x.x, 172.16.x.x–172.31.x.x oraz 192.168.x.x.
- Pętlowe adresy IP**:** Adresy pętlowe są używane w celach testowych. Ruch sieciowy wysłany do takiego bloku adresów IP wraca do urządzenia, które wygenerowało pakiet. Nigdy nie opuszcza tego urządzenia i przeważnie służy do testowania sprzętu i oprogramowania. Pętlowy blok adresów IP to 127.x.x.x.

Pusty adres IP: Jest to adres nieprawidłowy. Jego pojawienie się oznacza, że ruch sieciowy miał pusty adres IP. Jest to sytuacja nienormalna i często spowodowana celowym ukrywaniem przez nadawcę źródła 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.

adres MAC (Media Access Control Address, adres kontroli dostępu do nośnika)

Niskopoziomowy adres przypisany do urządzenia fizycznego z dostępem do sieci.

analiza obrazu

Uniemożliwia wyświetlenie potencjalnie niepożądanych obrazów. Obrazy są blokowane dla wszystkich użytkowników poza członkami grupy dorosłych.

archiwizacja

Proces tworzenia kopii monitorowanych plików lokalnie na dysku CD lub DVD, pamięci USB, zewnętrznym dysku twardym lub dysku sieciowym.

archiwizacja pełna

Proces archiwizowania pełnego zestawu danych w zależności od skonfigurowanych monitorowanych typów plików i lokalizacji.

archiwizacja szybka

Proces archiwizacji tylko tych monitorowanych plików, które uległy zmianie od ostatniej archiwizacji pełnej lub szybkiej.

atak słownikowy

Ataki słownikowe stanowią próbę określenia hasła użytkownika poprzez stosowanie kolejnych słów z listy. Atakujący nie wprowadzają ręcznie wszystkich kombinacji, lecz stosują narzędzia próbujące automatycznie zidentyfikować hasło użytkownika.

atak typu „brute force”

Nazywany również łamaniem zabezpieczeń metodą „brute force”, metoda prób i błędów wykorzystywana przez aplikacje do odkodowywania zaszyfrowanych danych (np. haseł) poprzez zaangażowanie licznych środków (przy użyciu „siły”) zamiast inteligentnych strategii. Tak jak przestępca może próbować włamać się do sejfu, próbując różne możliwe kombinacje szyfru, podobnie łamanie zabezpieczeń metodą „brute force” obejmuje wypróbowanie wszystkich możliwych kombinacji dopuszczalnych znaków w sekwencji. Atak typu „brute force” stanowi podejście niezawodne, ale czasochłonne.

atak typu „man-in-the-middle”

Atakujący przechwytuje wiadomości podczas wymiany kluczy publicznych, a następnie przesyła je dalej, podstawiając własny klucz publiczny zamiast żądanego. Dzięki temu z punktu widzenia obu pierwotnie komunikujących się urządzeń ich komunikacja jest wciąż bezpośrednia. Atakujący stosuje program, który zachowuje się jak serwer w stosunku do klienta oraz jak klient w stosunku do serwera. Taki atak może być wykorzystany do uzyskania dostępu do wiadomości lub umożliwienia atakującemu ich zmiany przed przesłaniem dalej. Nazwa pochodzi od gry w piłkę, w której kilka osób rzuca ją między sobą, a jedna osoba w środku stara się ją przechwycić.

atak typu „phishing”

Jest to oszustwo mające na celu kradzież cennych informacji, takich jak numery kart kredytowych, numery ubezpieczenia, identyfikatory użytkownika i hasła. Wiadomość e-mail, która wygląda jak oficjalny list od usługodawcy internetowego, banku lub sklepu, jest wysyłana do potencjalnych ofiar. Takie wiadomości e-mail mogą być wysłane do wybranych lub dowolnych osób z założeniem, że pewien odsetek odbiorców naprawdę posiada konto w organizacji, pod którą podszywa się nadawca.

atak typu DoS (odmowa usługi)

W Internecie atak typu DoS (Denial of Service, odmowa usługi) to zdarzenie, podczas którego użytkownik lub organizacja jest pozbawiana dostępu do usług lub zasobów, z których normalnie korzysta. Zazwyczaj utrata dostępu do usługi to brak możliwości skorzystania z określonej usługi sieciowej (np. poczta e-mail) lub utrata łączności sieciowej i wszystkich usług. W najgorszych przypadkach witryna sieci Web odwiedzana przez miliony osób może zostać zmuszona do czasowego zawieszenia działalności. Atak DoS może również zniszczyć oprogramowanie i pliki w systemie komputerowym. Jest on zazwyczaj celowy i złośliwy, jednak czasami może nastąpić przypadkowo. Atak typu DoS stanowi naruszenie zabezpieczeń systemu komputerowego, które na ogół nie skutkuje kradzieżą informacji czy utratą bezpieczeństwa. Jednak te ataki mogą kosztować osobę lub firmę, przeciwko której są skierowane, wiele czasu i pieniędzy.

B

biała lista

Lista witryn sieci Web, do których dostęp jest dozwolony, ponieważ nie są one uznawane za szkodliwe.

biblioteka

Obszar pamięci masowej w trybie online przeznaczony na pliki opublikowane przez użytkowników programu Data Backup. Biblioteka to witryna sieci Web w Internecie, dostępna dla wszystkich użytkowników Internetu.

brama zintegrowana

Urządzenie łączące funkcje punktu dostępu, routera i zapory. Niektóre urządzenia mogą posiadać rozszerzenia zabezpieczeń i funkcje mostkowania.

C

czarna lista

Lista witryn sieci Web uważanych za szkodliwe. Witryna sieci Web może zostać umieszczona na czarnej liście, ponieważ służy oszustwom lub wykorzystuje luki w zabezpieczeniach przeglądarki w celu wysyłania do użytkownika potencjalnie niepożądanych programów.

D

DNS

Akronim nazwy Domain Name System (system nazw domen). System hierarchiczny, w którym hosty podłączone do Internetu mają przypisany adres w postaci nazwy domeny (np. bluestem.prairienet.org) oraz adresu IP (np. 192.17.3.4). Adres w postaci nazwy domeny jest używany przez ludzi i jest automatycznie tłumaczony na numeryczny adres IP, używany przez oprogramowanie do routingu pakietów. Nazwy DNS składają się z domeny najwyższego poziomu (np. .com, .org lub .net), domeny drugiego poziomu (nazwa witryny przedsiębiorstwa, organizacji lub osoby) oraz opcjonalnie jednej lub więcej poddomen (serwery w domenie drugiego poziomu). Patrz także serwer DNS i adres IP.

domena

Adres połączenia sieciowego identyfikujący właściciela tego adresu w formacie hierarchicznym: serwer.organizacja.typ. Na przykład www.whitehouse.gov identyfikuje serwer sieci Web znajdujący się w Białym Domu, który stanowi organ rządu Stanów Zjednoczonych.

dysk sieciowy

Dysk twardy lub napęd taśmowy podłączony do serwera sieciowego, który jest udostępniany wielu użytkownikom. Dyski sieciowe są czasem nazywane dyskami zdalnymi.

E

ESS (Extended Service Set, rozszerzony zestaw usług)

Zestaw dwóch lub więcej sieci tworzących pojedynczą podsieć.

F

funkcje ochrony rodzicielskiej

Ustawienia umożliwiające skonfigurowanie klasyfikacji zawartości ograniczającej dostęp do witryn sieci Web i zawartości, którą może przeglądać dany użytkownik, a także internetowych limitów czasu określających czas i okres, w ciągu którego użytkownik ma dostęp do Internetu. Kontrola rodzicielska umożliwia ograniczenie dostępu do określonych witryn sieci Web oraz umożliwia lub blokuje dostęp w oparciu o grupy wiekowe i słowa kluczowe.

G

grupy klasyfikacji zawartości

Grupy wiekowe, do których należą użytkownicy. Zawartość jest klasyfikowana (to znaczy udostępniana lub blokowana) w zależności od grupy klasyfikacji zawartości, do której należy dany użytkownik. Grupy klasyfikacji zawartości to: małe dziecko, dziecko, młodszy nastolatek, starszy nastolatek i dorosły.

H

hasło

Kod (zazwyczaj alfanumeryczny) używany do uzyskania dostępu do komputera, programu lub witryny sieci Web.

I

Internet

Internet to ogromna liczba połączonych ze sobą sieci, które korzystają z protokołów TCP/IP do odnajdywania i przesyłania danych. Internet rozwinął się z połączonych komputerów uniwersyteckich i szkolnych (na przełomie lat 60-tych i 70-tych ubiegłego wieku). Przedsięwzięcie to zostało sfinansowane przez Departament Obrony Stanów Zjednoczonych i było znane pod nazwą ARPANET. Dziś Internet jest ogólnoświatową siecią, na którą składa się prawie 100 000 niezależnych sieci.

intranet

Sieć prywatna stanowiąca zazwyczaj wewnętrzną sieć organizacji, która funkcjonuje w sposób bardzo podobny do Internetu. Często stosowaną praktyką jest udostępnianie sieci intranet autonomicznym komputerom używanym przez studentów lub pracowników poza miasteczkiem uniwersyteckim lub poza miejscem pracy. Sieci te są zabezpieczane przez zapory, procedury logowania i hasła.

K

karta PCI sieci bezprzewodowej

Łączy komputer osobisty z siecią. Karta jest podłączana do gniazda PCI wewnątrz komputera.

karta sieci bezprzewodowej

Zawiera układy umożliwiające komputerowi lub innemu urządzeniu komunikację z routerem bezprzewodowym (połączenie się z siecią bezprzewodową). Karty sieci bezprzewodowej mogą być wbudowane w główne układy urządzenia lub być odrębnymi urządzeniami dodatkowymi podłączanymi do odpowiedniego portu urządzenia głównego.

karta sieciowa

Karta podłączana do laptopa lub innego urządzenia, łącząca je z siecią LAN.

karta USB sieci bezprzewodowej

Zapewnia rozszerzalny interfejs szeregowy Plug and Play. Ten interfejs oferuje standardowe, ekonomiczne połączenie bezprzewodowe dla urządzeń peryferyjnych takich jak klawiatura, mysz, joystick, drukarka, skaner, urządzenie pamięci masowej i kamera wideokonferencyjna.

klient

Aplikacja działająca na komputerze osobistym lub stacji roboczej i zależna od serwera podczas wykonywania pewnych operacji. Na przykład klient poczty e-mail to aplikacja umożliwiająca wysyłanie i odbieranie wiadomości e-mail.

klient poczty e-mail

Program obsługujący konto poczty e-mail. Na przykład Microsoft Outlook lub Eudora.

klucz

Seria liter i/lub cyfr używana przez dwa urządzenia do uwierzytelniania ich komunikacji. Oba urządzenia muszą posiadać klucz. Patrz także WEP, WPA, WPA2, WPA-PSK i WPA2- PSK.

kompresja

Proces, w wyniku którego dane (pliki) są kompresowane do postaci, w której zajmują mniej miejsca podczas przechowywania lub przesyłania.

konto MAPI

Akronim nazwy Messaging Application Programming Interface (interfejs programowy aplikacji komunikacyjnych). Specyfikacja interfejsu firmy Microsoft umożliwiająca różnym aplikacjom komunikacyjnym i aplikacjom dla grup roboczych (między innymi do obsługi poczty e-mail, poczty głosowej i faksów) współpracę z pojedynczym klientem, takim jak klient Exchange. Z tego powodu interfejs MAPI jest często używany w środowiskach korporacyjnych, w których działa serwer Microsoft Exchange. Jednak wiele osób korzysta z programu Microsoft Outlook do obsługi prywatnej poczty e-mail.

konto MSN

Akronim nazwy Microsoft Network. Usługa online i portal internetowy. Jest to konto w sieci Web.

konto POP3

Akronim nazwy Post Office Protocol 3. Większość użytkowników indywidualnych posiada konto tego typu. Jest to aktualna wersja standardu protokołu Post Office Protocol powszechnie używanego w sieciach TCP/IP. Nazywane również standardowym kontem e-mail.

koń trojański

Konie trojańskie to programy udające niegroźne aplikacje. Nie jest on wirusem, ponieważ nie potrafi tworzyć własnych kopii, ale stanowi równie poważne zagrożenie.

kwarantanna

Gdy zostaną wykryte podejrzane pliki, są one poddawane kwarantannie. Później można podjąć wobec nich odpowiednie działanie.

L

LAN (Local Area Network, sieć lokalna)

Sieć komputerowa obejmująca stosunkowo niewielki obszar. Większość sieci LAN jest ograniczonych do pojedynczego budynku lub ich grupy. Sieć LAN można jednak połączyć z innymi sieciami LAN znajdującymi się w dowolnej odległości za pomocą linii telefonicznych lub fal radiowych. System połączonych w ten sposób sieci LAN jest nazywany siecią rozległą (WAN). Większość sieci LAN łączy stacje robocze i komputery osobiste, najczęściej za pomocą prostych koncentratorów lub przełączników. Każdy węzeł (odrębny komputer) w sieci LAN posiada własny procesor używany do wykonywania programów, ale może także uzyskać dostęp do danych i urządzeń (np. drukarek) znajdujących się w dowolnym miejscu sieci LAN. Oznacza to, że wielu użytkowników może współużytkować dane i drogie urządzenia, takie jak drukarki laserowe. Użytkownicy mogą również korzystać z sieci LAN do komunikowania się ze sobą, na przykład za pomocą wiadomości e-mail lub programów do rozmów.

lokalizacja monitorowana częściowo

Folder w komputerze, który jest monitorowany przez program Data Backup w celu wykrycia zmian. Po skonfigurowaniu lokalizacji monitorowanej częściowo program Data Backup tworzy kopie zapasowe wszystkich plików monitorowanych typów znajdujących się w tym folderze, ale pomija te w podfolderach.

lokalizacja monitorowana dokładnie

Folder (i wszystkie podfoldery) w komputerze, który jest monitorowany przez program Data Backup w celu wykrycia zmian. Po skonfigurowaniu lokalizacji monitorowanej dokładnie program Data Backup tworzy kopie zapasowe wszystkich plików monitorowanych typów znajdujących się w tym folderze i jego podfolderach.

lokalizacje monitorowane

Foldery w komputerze monitorowane przez program Data Backup.

M

MAC (Media Access Control lub Message Authenticator Code)

W przypadku pierwszego terminu patrz adres MAC. Drugi termin (kod uwierzytelniania wiadomości) oznacza kod używany do identyfikacji danej wiadomości (np. wiadomości RADIUS). Kod jest najczęściej kryptograficznie silnym kodowaniem treści wiadomości, które zawiera unikatową wartość zapewniającą ochronę przed odtworzeniem.

magazyn haseł

Bezpieczny obszar pamięci masowej przeznaczony na osobiste hasła. Umożliwia przechowywanie haseł, gwarantując, że żaden inny użytkownik (nawet administrator firmy McAfee ani administrator systemu) nie ma do nich dostępu.

mapa sieci

W usłudze Network Manager — graficzne przedstawienie komputerów i elementów składowych, które tworzą sieć domową.

N

nagłówek

Nagłówek stanowi informację dodawaną do wiadomości na czas jej istnienia. Zawiera on informacje dla oprogramowania internetowego o sposobie dostarczenia wiadomości, lokalizacji, do której należy przesyłać odpowiedzi, unikalnym identyfikatorze wiadomości e-mail oraz innych danych administracyjnych. Przykłady pól nagłówka to: Do, Od, DW, Data, Temat, ID wiadomości i Odebrano.

niekontrolowany punkt dostępu

Punkt dostępu, który nie został autoryzowany przez firmę do działania. Problem polega na tym, że niekontrolowane punkty dostępu często nie spełniają zasad bezpieczeństwa sieci LAN (WLAN). Niekontrolowany punkt dostępu stanowi otwarte, niezabezpieczone łącze do sieci korporacyjnej z zewnątrz fizycznie chronionej placówki.

W prawidłowo zabezpieczonej sieci WLAN niekontrolowane punkty dostępu mogą wyrządzić więcej szkód niż wrodzy użytkownicy. Nieautoryzowani użytkownicy próbujący uzyskać dostęp do sieci WLAN najczęściej nie będą w stanie dotrzeć do cennych zasobów korporacyjnych, jeśli w sieci zastosowano skuteczne mechanizmy uwierzytelniania. Jednak w momencie, gdy pracownik lub haker podłączy się do niekontrolowanego punktu dostępu, mogą pojawić się poważne problemy. Taki punkt umożliwia każdemu, kto posiada urządzenie obsługujące protokół 802.11, uzyskanie dostępu do sieci korporacyjnej. W ten sposób nieupoważnione osoby mogą uzyskać dostęp do kluczowych zasobów firmy.

P

plik cookie

W sieci WWW to blok danych przechowywany przez serwer sieci Web w systemie klienta. Gdy użytkownik ponownie otwiera tę samą witrynę sieci Web, przeglądarka wysyła kopię pliku cookie do serwera. Pliki cookie służą do identyfikacji użytkowników, informowania serwera, aby wysłał dostosowaną wersję żądanej strony sieci Web, wysyłania informacji dotyczących konta użytkownika i do innych celów administracyjnych.

Pliki cookie umożliwiają witrynie sieci Web rozpoznawanie użytkowników oraz śledzenie liczby osób odwiedzających witrynę, czasu wizyty i przeglądanych stron. Pliki cookie są też używane przez firmy w celu dostosowania witryn sieci Web do wymagań użytkowników. Wiele witryn sieci Web wymaga podania nazwy użytkownika i hasła w celu uzyskania dostępu do określonych stron, po czym wysyła do komputera plik cookie, aby użytkownik nie musiał rejestrować się przy każdej wizycie. Jednak pliki cookie można także wykorzystać w celach destrukcyjnych. Firmy reklamowe często korzystają z plików cookie w celu określenia, jakie witryny użytkownik najczęściej odwiedza, aby następnie wyświetlać reklamy na jego ulubionych stronach. Przed zezwoleniem na pliki cookie z witryny sieci Web należy upewnić się, że dana witryna jest zaufana.

Pliki cookie są źródłem informacji dla legalnych firm, ale mogą także dostarczać informacji hakerom. Wiele witryn sieci Web należących do sklepów internetowych umieszcza informacje o kartach kredytowych i inne informacje osobiste w plikach cookie, aby ułatwić klientom dokonywanie zakupów. Niestety, błędy w zabezpieczeniach mogą umożliwić hakerom dostęp do informacji przechowywanych w plikach cookie na komputerach klientów.

pluskwy internetowe

Małe pliki graficzne osadzające się na stronach HTML i umożliwiające nieautoryzowanym źródłom umieszczanie plików cookie na komputerze użytkownika. Te pliki cookie mogą następnie przesyłać informacje do nieautoryzowanego źródła. Pluskwy internetowe są także nazywane sygnalizatorami sieci Web, tagami pikselowymi, czystymi lub niewidocznymi plikami GIF.

poczta e-mail

Poczta elektroniczna, wiadomości wysyłane przez Internet albo w obrębie sieci lokalnej LAN lub rozległej WAN należącej do firmy. Załączniki do wiadomości e-mail w formie plików EXE (pliki wykonywalne) lub VBS (skrypt języka Visual Basic) stają się coraz bardziej popularne jako środki przenoszenia wirusów i koni trojańskich.

podszywanie się pod adres IP

Fałszowanie adresu IP znajdującego się w pakiecie IP. To działanie stosowane jest w wielu typach ataków, między innymi w przechwytywaniu sesji. Często fałszowane są nagłówki wiadomości e-mail stanowiących spam, dzięki czemu nie można wyśledzić nadawcy.

port

Miejsce, przez które informacje dostają się do komputera i go opuszczają; na przykład konwencjonalny modem analogowy jest podłączony do portu szeregowego. Numery portów w połączeniach TCP/IP są wirtualnymi wartościami używanymi do dzielenia ruchu na strumienie odpowiadające danej aplikacji. Porty są przypisane do standardowych protokołów, takich jak SMTP czy HTTP, aby ułatwić programom ich użycie w celu nawiązywania połączeń. Docelowy port dla pakietów TCP wskazuje poszukiwaną aplikację lub serwer.

potencjalnie niepożądany program

Potencjalnie niepożądane programy, takie jak oprogramowanie szpiegujące, reklamowe oraz inne programy, które gromadzą i wysyłają dane użytkownika bez jego zgody.

PPPoE

Akronim nazwy Point-to-Point Protocol Over Ethernet. Używany przez wielu dostawców łączy DSL, protokół PPPoE obsługuje warstwy protokołu i uwierzytelnianie często używane w protokole PPP oraz umożliwia nawiązywanie połączeń punkt-punkt w zwykle wielopunktowej architekturze sieci Ethernet.

protokół

Uzgodniony format transmisji danych pomiędzy dwoma urządzeniami. Z punktu widzenia użytkownika jedynym istotnym aspektem jest to, że w celu nawiązania komunikacji z innymi komputerami jego komputer lub urządzenie musi obsługiwać właściwe protokoły. Implementacja protokołu może mieć postać sprzętową albo programową.

proxy

Komputer (lub oprogramowanie na nim uruchomione), który funkcjonuje jako bariera pomiędzy siecią a Internetem, prezentując witrynom zewnętrznym tylko pojedynczy adres sieciowy. Działając jako pośrednik reprezentujący wszystkie wewnętrzne komputery, serwer proxy chroni tożsamość komputerów w sieci i jednocześnie umożliwia dostęp do Internetu. Zobacz też: serwer proxy.

przeglądarka

Program klienta używający protokołu HTTP (Hypertext Transfer Protocol) do wysyłania żądań do serwerów sieci Web w Internecie. Przeglądarka sieci Web umożliwia graficzne przedstawienie zawartości przeglądanej przez użytkownika.

przepełnienie bufora

Przepełnienie bufora występuje wtedy, gdy podejrzane programy lub procesy próbują zapisać więcej danych w buforze (miejscu zapisu tymczasowych danych), niż może on pomieścić, niszcząc lub nadpisując ważne dane w sąsiednich buforach.

przepustowość

Ilość danych, którą można przesłać w określonym czasie. W przypadku urządzeń cyfrowych przepustowość jest zazwyczaj wyrażana w bitach na sekundę (b/s) lub bajtach na sekundę. W przypadku urządzeń analogowych przepustowość jest wyrażana w cyklach na sekundę lub hercach (Hz).

przywracanie

Proces przywracania kopii pliku z repozytorium kopii zapasowych online lub z archiwum.

publiczny punkt dostępu

Określona lokalizacja geograficzna, w której punkt dostępu zapewnia ruchomym użytkownikom korzystającym z sieci bezprzewodowej dostęp do publicznych usług sieci szerokopasmowej. Publiczne punkty dostępu często znajdują się w miejscach, w których przebywają duże grupy ludzi, takich jak porty lotnicze, dworce kolejowe, biblioteki, przystanie, centra konferencyjne i hotele. Na ogół mają one niewielki zasięg.

publikowanie

Proces publicznego udostępniania w Internecie pliku, który ma kopię zapasową.

punkt dostępu

Urządzenie sieciowe umożliwiające klientom w standardzie 802.11 łączenie się z siecią lokalną (LAN). Punkty dostępu zwiększają fizyczny zasięg sieci bezprzewodowej. Jest on czasem określany jako router bezprzewodowy.

R

RADIUS (Remote Access Dial-In User Service)

Protokół zapewniający uwierzytelnianie użytkowników, zwykle podczas zdalnego dostępu. Pierwotnie zdefiniowany do użytku z serwerami telefonicznego dostępu zdalnego, protokół ten jest obecnie używany w wielu środowiskach uwierzytelniania, między innymi w uwierzytelnianiu 802.1x ze współdzielonym hasłem użytkownika sieci WLAN.

repozytorium kopii zapasowych online

Lokalizacja na serwerze w trybie online, w której przechowywane są kopie zapasowe monitorowanych plików.

roaming

Możliwość przemieszczania się z obszaru zasięgu jednego punktu dostępu do drugiego, bez zakłócania dostępu do usług lub utraty połączenia.

robak

Robak to samopowielający się wirus, który ładuje się do aktywnej pamięci komputera i może rozsyłać swoje kopie za pomocą wiadomości e-mail. Robaki powielają się i zużywają zasoby systemowe, spowalniając pracę komputera lub wstrzymując wykonywane zadania.

router

Urządzenie sieciowe przekazujące pakiety z jednej sieci do drugiej. W oparciu o wewnętrzne tablice routingu, routery analizują każdy przychodzący pakiet i przekazują go w odpowiedni sposób. Interfejs routera, do którego wysyłane są wychodzące pakiety, może być określony na podstawie dowolnej kombinacji źródłowych i docelowych adresów, a także bieżących warunków ruchu w sieci, takich jak obciążenie, koszty połączenia i uszkodzenia łączy. Czasami określany jako punkt dostępu.

S

serwer

Komputer lub oprogramowanie zapewniające określone usługi programom działającym na innych komputerach. „Serwer poczty” działający u usługodawcy internetowego to oprogramowanie obsługujące całą przychodzącą i wychodzącą pocztę wszystkich użytkowników. Serwer w sieci lokalnej LAN to urządzenie stanowiące podstawowy węzeł sieci. Na serwerze może również działać oprogramowanie udostępniające określone usługi, dane lub inne możliwości wszystkim komputerom klienckim, które są z nim połączone.

serwer DNS

Skrócona nazwa serwera systemu nazw domen. Komputer, który może odpowiadać na zapytania DNS. Serwer DNS przechowuje bazę danych hostów i przypisanych im adresów IP. Po otrzymaniu na przykład nazwy apex.com serwer DNS zwróciłby adres IP serwera hipotetycznej firmy Apex. Nazywany również serwerem nazw. Patrz także DNS i adres IP.

serwer proxy

Składnik zapory zarządzający ruchem internetowym do i z sieci lokalnej (LAN). Serwer proxy może poprawić wydajność, dostarczając często żądane dane, takie jak popularne strony sieci Web. Może on również filtrować i odrzucać żądania uważane za niewłaściwe, takie jak żądania nieautoryzowanego dostępu do plików zastrzeżonych.

serwer SMTP

Akronim nazwy Simple Mail Transfer Protocol (prosty protokół przesyłania poczty). Protokół TCP/IP służący do przesyłania wiadomości z jednego komputera w sieci do drugiego. Ten protokół jest używany w Internecie do przesyłania wiadomości e-mail.

sieć

Sieć powstaje z połączenia co najmniej dwóch komputerów.

sieć zarządzana

Sieć domowa z dwoma typami użytkowników: użytkownikami zarządzanymi i użytkownikami niezarządzanymi. Użytkownicy zarządzani zezwalają na monitorowanie swojego stanu ochrony w programie firmy McAfee przez inne komputery w sieci; użytkownicy niezarządzani — nie zezwalają na to.

skanowanie w czasie rzeczywistym

Wirusy i oznaki innych działań są wyszukiwane w plikach, gdy użytkownik lub system próbuje uzyskać do nich dostęp.

skrypt

Skrypty mogą tworzyć, kopiować lub usuwać pliki. Mogą również otwierać rejestr systemu Windows.

słowo kluczowe

Słowo, które można przypisać do pliku posiadającego kopię zapasową w celu ustanowienia zależności lub połączenia z innymi plikami, do których przypisano to samo słowo kluczowe. Przypisywanie słów kluczowych do plików ułatwia wyszukiwanie plików opublikowanych w Internecie.

SSID (Service Set Identifier)

Nazwa sieciowa urządzeń w podsystemie bezprzewodowej sieci LAN. To 32-znakowy łańcuch tekstu zwykłego dodawany do nagłówka każdego pakietu w sieci WLAN. Identyfikator SSID odróżnia jedną sieć WLAN od drugiej, przez co wszyscy użytkownicy sieci muszą podać ten sam identyfikator SSID, aby uzyskać dostęp do danego punktu dostępu. Identyfikator SSID uniemożliwia dostęp urządzeniu klienckiemu, które go nie posiada. Jednak domyślnie punkt dostępu rozgłasza swój identyfikator SSID w swoim sygnale. Nawet jeśli rozgłaszanie identyfikatora SSID jest wyłączone, haker może go wykryć, przechwytując pakiety.

SSL (Secure Sockets Layer)

Protokół zaprojektowany przez firmę Netscape w celu przesyłania prywatnych dokumentów przez Internet. Protokół SSL działa, korzystając z publicznego klucza do szyfrowania danych, które są następnie przesyłane połączeniem SSL. Przeglądarki Netscape Navigator i Internet Explorer obsługują i używają protokołu SSL, a wiele witryn sieci Web korzysta z tego protokołu do przekazywania od użytkowników poufnych informacji, takich jak numery kart kredytowych. Zgodnie z konwencją adresy URL wymagające połączenia SSL rozpoczynają się przedrostkiem https: zamiast http:.

standardowe konto e-mail

Większość użytkowników indywidualnych posiada konto tego typu. Patrz także konto POP3.

synchronizacja

Proces usuwania rozbieżności pomiędzy plikami przechowywanymi na lokalnym komputerze a ich kopiami zapasowymi. Synchronizacja jest wykonywana, gdy wersja pliku w repozytorium kopii zapasowych online jest nowsza niż ta znajdująca się w innych komputerach. Synchronizacja aktualizuje kopię pliku na innych komputerach do wersji z repozytorium kopii zapasowych online.

SystemGuard

Programy SystemGuard wykrywają nieautoryzowane zmiany w komputerze i powiadamiają użytkownika w chwili ich wystąpienia.

szyfrowanie

Proces transformacji danych z tekstu na kod, mający na celu uniemożliwienie odczytania informacji przez osoby nie znające metody jego odszyfrowania.

T

tekst zaszyfrowany

Dane, które zostały zaszyfrowane. Tekstu zaszyfrowanego nie można odczytać, dopóki nie zostanie on przekonwertowany na zwykły tekst (odszyfrowany) za pomocą klucza.

TKIP (Temporal Key Integrity Protocol)

Prowizoryczna metoda usuwania naturalnej luki w zabezpieczeniach WEP, w szczególności podczas ponownego używania kluczy szyfrowania. Protokół TKIP zmienia klucze tymczasowe co 10 000 pakietów, zapewniając metodę dynamicznej dystrybucji, która znacząco zwiększa bezpieczeństwo sieci. Proces zabezpieczeń TKIP rozpoczyna się 128-bitowym kluczem tymczasowym współdzielonym przez klientów i punkty dostępu. Protokół TKIP łączy klucz tymczasowy z adresem MAC komputera klienckiego, a następnie dodaje stosunkowo duży 16-oktetowy wektor inicjowania w celu utworzenia klucza szyfrującego dane. Ta procedura gwarantuje, że każda stacja do szyfrowania danych używa strumieni o innym kluczu. Protokół TKIP do szyfrowania używa algorytmu RC4. Protokół WEP również używa algorytmu RC4.

tworzenie kopii zapasowej

Proces tworzenia kopii monitorowanych plików na bezpiecznym serwerze w trybie online.

typy monitorowanych plików

Typy plików (na przykład .doc, .xls itd.) znajdujących się w lokalizacjach monitorowanych, dla których program Data Backup tworzy kopie zapasowe lub które archiwizuje.

U

udostępnianie

Operacja umożliwiająca odbiorcom wiadomości e-mail uzyskanie przez ograniczony okres czasu dostępu do wybranych plików posiadających kopie zapasowe. Podczas udostępniania pliku kopia zapasowa pliku jest wysyłana do określonych odbiorców wiadomości e-mail. Odbiorcy otrzymują wiadomość e-mail od programu Data Backup informującą, że udostępniono im pliki. Wiadomość e-mail zawiera również łącze do udostępnionych plików.

URL

Akronim nazwy Uniform Resource Locator. Standardowy format adresów internetowych.

uwierzytelnianie

Proces identyfikacji osoby, na ogół oparty na weryfikacji nazwy użytkownika i hasła. Celem uwierzytelniania jest sprawdzenie, czy dana osoba jest tą, za którą się podaje, natomiast nie definiuje ono jej praw dostępu.

V

VPN (Virtual Private Network, wirtualna sieć prywatna)

Sieć utworzona z wykorzystaniem publicznych łączy w celu połączenia węzłów. Na przykład może istnieć pewna liczba systemów umożliwiających utworzenie sieci, korzystających z Internetu jako nośnika do przesyłania danych. Te systemy stosują szyfrowanie i inne mechanizmy zabezpieczeń, aby zagwarantować, że tylko autoryzowani użytkownicy mają dostęp do sieci, a dane nie mogą zostać przechwycone.

W

wardriver

Intruz wyposażony w laptop, specjalne oprogramowanie i prowizoryczny sprzęt, jeżdżący po miastach, przedmieściach i parkach biznesowych w celu przechwytywania ruchu w bezprzewodowych sieciach LAN.

WEP (Wired Equivalent Privacy)

Protokół szyfrowania i uwierzytelniania zdefiniowany jako część standardu 802.11. Wczesne wersje są oparte na algorytmach szyfrowania RC4 i mają istotne wady. Protokół WEP stara się zapewnić bezpieczeństwo poprzez szyfrowanie danych przesyłanych drogą radiową, dzięki czemu są one chronione podczas przesyłania z jednego punktu do drugiego. Jednak praktyka pokazała, że protokół WEP nie jest tak bezpieczny, jak kiedyś sądzono.

węzeł

Pojedynczy komputer podłączony do sieci.

Wi-Fi (Wireless Fidelity)

Termin stosowany w odniesieniu do dowolnego typu sieci 802.11, w tym protokołu 802.11b, 802.11a, dwuzakresowego itd. Jest on używany przez stowarzyszenie Wi-Fi Alliance.

Wi-Fi Alliance

Stowarzyszenie zrzeszające wiodących dostawców sprzętu bezprzewodowego i oprogramowania, którego celem jest (1) certyfikacja zgodności wszystkich produktów opartych na protokole 802.11 oraz (2) promocja na wszystkich rynkach nazwy Wi-Fi jako globalnej marki wszelkich produktów bezprzewodowej sieci LAN opartych na protokole 802.11. Działa ono jako konsorcjum, laboratorium testowe i izba rozrachunkowa dla dostawców, którzy chcą promować zgodność produktów i wspierać rozwój branży.

Mimo że wszystkie produkty 802.11a/b/g są nazywane Wi-Fi, to tylko produkty, które pomyślnie przeszły testy stowarzyszenia Wi-Fi Alliance mogą nosić oznaczenie certyfikacyjne Wi-Fi Certified (zastrzeżony znak towarowy). Produkty, które przeszły testy, muszą posiadać na opakowaniu oznaczenie informujące o certyfikacie Wi-Fi Certified i wykorzystywanym paśmie częstotliwości radiowej. Stowarzyszenie nosiło wcześniej nazwę Wireless Ethernet Compatibility Alliance (WECA, Stowarzyszenie kompatybilności bezprzewodowej sieci Ethernet), ale w październiku 2002 roku zmieniono nazwę, aby lepiej odzwierciedlała promowaną markę Wi-Fi.

Wi-Fi Certified

Wszelkie produkty przetestowane i zaaprobowane przez stowarzyszenie Wi-Fi Alliance są oznaczone certyfikatem Wi-Fi Certified (zastrzeżony znak towarowy) jako zgodne ze sobą, nawet jeśli pochodzą od różnych producentów. Użytkownik może korzystać z punktu dostępu dowolnego producenta w połączeniu ze sprzętem klienckim innego dowolnego producenta, jeśli oba produkty noszą oznaczenie Wi-Fi Certified. Zazwyczaj jednak każdy produkt Wi-Fi używający tej samej częstotliwości radiowej (na przykład 2,4 GHz dla 802.11b lub 11g, 5 GHz dla 802.11a) współpracuje z innymi, nawet jeśli nie mają one certyfikatu Wi-Fi Certified.

WLAN (Wireless Local Area Network, bezprzewodowa sieć lokalna)

Patrz także LAN. Sieć lokalna korzystająca z nośnika bezprzewodowego do nawiązywania połączeń. W sieci WLAN do komunikacji pomiędzy węzłami zamiast przewodów stosuje się fale radiowe o wysokiej częstotliwości.

WPA (Wi-Fi Protected Access)

Standard znacznie zwiększający poziom ochrony danych i kontroli dostępu w istniejących i przyszłych systemach bezprzewodowej sieci LAN. Zaprojektowany do pracy na istniejącym sprzęcie jako aktualizacja oprogramowania, standard WPA pochodzi od standardu IEEE 802.11i i jest z nim kompatybilny. Po prawidłowej instalacji gwarantuje użytkownikom bezprzewodowej sieci LAN, że ich dane są chronione, a do sieci mają dostęp tylko autoryzowani użytkownicy.

WPA-PSK

Specjalny tryb WPA zaprojektowany dla użytkowników indywidualnych, którzy nie wymagają silnych zabezpieczeń klasy korporacyjnej i nie posiadają dostępu do serwerów uwierzytelniania. W tym trybie użytkownik indywidualny wprowadza hasło początkowe służące do aktywacji standardu Wi-Fi Protected Access w trybie wstępnie współdzielonego klucza. Hasło należy zmieniać w wypadku każdego komputera bezprzewodowego i punktu dostępu. Patrz także WPA2-PSK i TKIP.

WPA2

Patrz także WPA. WPA2 jest aktualizacją standardu zabezpieczeń WPA i jest oparty na standardzie 802.11i IEEE.

WPA2-PSK

Patrz także WPA-PSK i WPA2. WPA2-PSK jest standardem podobnym do WPA-PSK i jest oparty na standardzie WPA2. Znaną funkcją standardu WPA2-PSK jest to, że urządzenia często obsługują wiele trybów szyfrowania jednocześnie (np. AES, TKIP), podczas gdy starsze urządzenia na ogół obsługują tylko jeden tryb szyfrowania (np. wszystkie komputery klienckie muszą korzystać z tego samego trybu szyfrowania).

współdzielone hasło

Patrz także RADIUS. Chroni poufne części wiadomości RADIUS. Współdzielone hasło to hasło w bezpieczny sposób współdzielone przez stronę uwierzytelniającą i serwer uwierzytelniania.

wyskakujące okna

Niewielkie okna pojawiające się na tle innych okien na ekranie komputera. Wyskakujące okna są często używane w przeglądarkach sieci Web do wyświetlania reklam. Oprogramowanie firmy McAfee blokuje wyskakujące okna, które są automatycznie wyświetlane podczas ładowania strony sieci Web przez przeglądarkę. Oprogramowanie firmy McAfee nie blokuje wyskakujących okien ładowanych po kliknięciu łącza.

Z

zapora

System zaprojektowany w celu zapobiegania nieautoryzowanemu dostępowi do lub z sieci prywatnej. Implementacja zapory może mieć postać zarówno sprzętową jak i programową, a także stanowić ich połączenie. Zapory są często stosowane w celu uniemożliwienia nieautoryzowanym użytkownikom Internetu uzyskania dostępu do sieci prywatnych podłączonych do Internetu, w szczególności sieci intranet. Wszystkie wiadomości wchodzące lub wychodzące z sieci intranet przechodzą przez zaporę. Zapora analizuje każdą wiadomość i blokuje te, które nie spełniają określonych kryteriów zabezpieczeń. Zapora jest uważana za pierwszą linię obrony podczas ochrony prywatnych informacji. W celu zwiększenia bezpieczeństwa dane można szyfrować.

zdarzenie

Zdarzenia z adresu 0.0.0.0

Istnieją dwie prawdopodobne przyczyny występowania zdarzeń z adresu IP 0.0.0.0. Pierwsza i najczęstsza to odebranie z jakiegoś powodu nieprawidłowo skonstruowanego pakietu przez komputer. Internet nie jest środowiskiem w 100% niezawodnym i nieprawidłowe pakiety mogą się zdarzyć. Program Firewall przechwytuje pakiety przed ich sprawdzeniem przez protokół TCP/IP, więc pakiety takie mogą być raportowane jako zdarzenie.

Druga sytuacja zachodzi, kiedy źródłowy adres IP jest adresem podszywającym się lub sfałszowanym. Występowanie pakietów podszywających się może oznaczać, że ktoś przeprowadza skanowanie w poszukiwaniu koni trojańskich i właśnie trafił na ten komputer. Należy pamiętać, że program Firewall blokuje takie próby.

Zdarzenia z adresu 127.0.0.1

Czasami zdarzenia mają źródłowy adres IP 127.0.0.1. Należy pamiętać, że ten adres IP jest adresem specjalnym, nazywanym również adresem pętlowym.

Bez względu na rodzaj używanego komputera, adres 127.0.0.1 zawsze oznacza ten lokalny komputer. Ten adres jest także znany pod nazwą localhost, ponieważ nazwa komputera localhost zawsze zwraca adres IP 127.0.0.1. Czy to oznacza, że komputer próbuje włamać się sam do siebie? Czy jakiś koń trojański lub oprogramowanie szpiegujące przejmuje kontrolę nad komputerem? Mało prawdopodobne. Wiele normalnych programów wykorzystuje adres pętlowy do komunikowania się ze swoimi składnikami. Na przykład wiele serwerów pocztowych lub serwerów sieci Web pozwala na ich konfigurację za pomocą interfejsu internetowego, który jest zazwyczaj dostępny pod adresem http://localhost/.

Jednak program Firewall zezwala na ruch z tych programów, więc jeśli w raportach pojawiają się zdarzenia z adresu 127.0.0.1, najprawdopodobniej taki źródłowy adres IP jest fałszywy lub ktoś się pod niego podszywa. Występowanie pakietów podszywających się zwykle świadczy o tym, że ktoś przeprowadza skanowanie w poszukiwaniu koni trojańskich. Należy pamiętać, że program Firewall blokuje takie próby. Oczywiście zgłaszanie zdarzeń z adresu 127.0.0.1 nie jest pomocne, zatem nie trzeba tego robić.

Niektóre programy, w tym przeglądarka Netscape w wersji 6.2 i nowszej, wymagają dodania adresu 127.0.0.1 do listy **zaufanych adresów IP**. Składniki tych programów komunikują się ze sobą w taki sposób, że program Firewall nie jest w stanie określić, czy ma do czynienia z ruchem lokalnym.

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. Dlatego jeśli w dzienniku pojawi się ruch z adresu 127.0.0.1, a wszystkie aplikacje w komputerze działają normalnie, to ruch ten można bezpiecznie zablokować. Jeżeli jednak jakiś program (np. Netscape) działa niestabilnie, należy dodać adres 127.0.0.1 do listy **zaufanych adresów IP** programu Firewall i sprawdzić, czy problem został rozwiązany.

Jeśli dodanie adresu 127.0.0.1 do listy **Zaufane adresy IP** usunęło problem, należy zastanowić się nad dostępnymi możliwościami: jeśli użytkownik doda adres 127.0.0.1 do listy zaufanych, program będzie działał, ale zwiększy się niebezpieczeństwo wystąpienia ataków z wykorzystaniem podszywania się. W przeciwnym razie używany program nie będzie działał, ale komputer będzie chroniony przed tego rodzaju złośliwym ruchem sieciowym.

Zdarzenia pochodzące z komputerów w sieci LAN

W większości środowisk korporacyjnych sieci LAN wszystkie komputery znajdujące się w sieci LAN można traktować jako zaufane.

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 jest używany przez usługę udostępniania połączenia internetowego (ICS, Internet Connection Sharing) firmy Microsoft. Jeśli używana jest usługa ICS, a w dzienniku znajdują się zdarzenia z tego bloku adresów IP, to adres 192.168.255.255 można dodać do listy **Zaufane adresy IP**. Spowoduje to określenie całego bloku 192.168.xxx.xxx jako zaufanego.

Jeśli użytkownik nie korzysta z sieci prywatnej, a w dzienniku pojawiają się zdarzenia z tych zakresów adresów IP, wówczas źródłowy adres IP może być fałszywy lub ktoś się pod niego podszywa. Występowanie pakietów podszywających się zwykle świadczy o tym, że ktoś przeprowadza skanowanie w poszukiwaniu koni trojańskich. Należy pamiętać, że program Firewall blokuje takie próby.

Prywatne adresy IP stanowią grupę oddzielną od internetowych adresów IP, więc przesyłanie raportów o takich zdarzeniach jest bezcelowe.

zewnętrzny dysk twardy

Dysk twardy znajdujący się na zewnątrz obudowy komputera.

zwykły tekst

Dowolna wiadomość, która nie jest zaszyfrowana.

Informacje o firmie McAfee

Firma McAfee, Inc. z siedzibą w Santa Clara w Kalifornii, będąca światowym liderem w dziedzinie ochrony przed włamaniami i zarządzania ryzykiem wystąpienia zagrożeń, dostarcza proaktywne i sprawdzone rozwiązania i usługi służące zabezpieczaniu systemów i sieci na całym świecie. Dzięki bogatemu doświadczeniu w dziedzinie bezpieczeństwa oraz zaangażowaniu w dostarczanie innowacyjnych technologii firma McAfee daje użytkownikom indywidualnym, firmom i usługodawcom możliwość blokowania ataków, zapobiegania zakłóceniom oraz ciągłego śledzenia i ulepszania stanu swoich zabezpieczeń.

Copyright

Indeks

8

802.11 384
802.11a 384
802.11b 384
802.11g 384
802.1x 384

A

Administrowanie kluczami sieciowymi 325, 342
Administrowanie programem VirusScan 103
Administrowanie sieciami bezprzewodowymi 307
adres IP 385
adres MAC (Media Access Control Address, adres kontroli dostępu do nośnika) 385
Aktualizacja karty sieci bezprzewodowej .. 357, 358
Aktualizacja oprogramowania układowego routera lub punktu dostępu 351
analiza obrazu 385
Analiza ruchu przychodzącego i wychodzącego 179, 180
archiwizacja 385
archiwizacja pełna 385
archiwizacja szybka 385
Archiwizowanie plików 267
atak słownikowy 385
atak typu 386
atak typu DoS (odmowa usługi) 386
Automatyczna aktualizacja znajomych 200
Automatyczna cykliczna zmiana klucza 314, 326, 327, 328, 329, 330, 342, 352, 356
Automatyczne naprawianie problemów dotyczących ochrony 21
Automatyczne pobieranie aktualizacji 32, 33
Automatyczne pobieranie i instalowanie aktualizacji 32
Automatyczne przeprowadzanie konserwacji komputera 41
Automatyczne przesyłanie anonimowych informacji 108
Automatyczne sprawdzanie dostępności aktualizacji 32

B

biała lista 386
biblioteka 386
Blokowanie dostępu do istniejącego portu usługi systemowej 154
Blokowanie dostępu komputerowi z poziomu dziennika Zdarzenia przychodzące . 167, 171
Blokowanie dostępu komputerowi z poziomu dziennika Zdarzenia wykrywania włamań 168, 173
Blokowanie dostępu nowego programu 148
Blokowanie dostępu programów do Internetu 147
Blokowanie dostępu programu 147
Blokowanie dostępu z poziomu dziennika Ostatnie zdarzenia 148
Blokowanie i odblokowywanie zapory 139
Blokowanie informacji osobistych 258
Blokowanie pluskiew internetowych 257
Blokowanie połączeń z komputerami 163
Blokowanie potencjalnie niepożądanych obrazów 253
Blokowanie potencjalnie niepożądanych obrazów w sieci Web 253
Blokowanie reklam 256
Blokowanie reklam, wyskakujących okien i pluskiew internetowych 256
Blokowanie witryn sieci Web 245, 249
Blokowanie witryn sieci Web w oparciu o słowa kluczowe 234, 248
Blokowanie witryny sieci Web 246
Blokowanie wyskakujących okien 257
Błąd zdublowanych administratorów 351
Brakuje niektórych składników lub są one uszkodzone 115
brama zintegrowana 386

C

Chronienie innych urządzeń bezprzewodowych 293, 300
Co to jest filtr ataków typu 229
Co to są konta POP3, MSN/Hotmail oraz MAPI? 228
Copyright 402
Cykliczna zmiana klucza nie powiodła się . 352

czarna lista....387
Często zadawane pytania....112, 228
Czy jestem chroniony?....15
Czy mogę używać programu VirusScan z przeglądarkami Netscape, Firefox i Opera? 112
Czy podczas skanowania komputer powinien być połączony z Internetem? 112
Czy program VirusScan skanuje pliki wewnątrz archiwów ZIP? 113
Czy program VirusScan skanuje załączniki poczty e-mail?....113

D

Defragmentowanie plików i folderów....42
Dlaczego firma McAfee używa plików cookie? 229
Dlaczego podczas skanowania wychodzących wiadomości e-mail występują błędy? 113
DNS....387
Dodatkowa pomoc....111, 227
Dodawanie filtrów osobistych....210
Dodawanie hasła do magazynu haseł....260
Dodawanie komputerów do chronionej sieci bezprzewodowej 293, 298, 302, 354, 356
Dodawanie komputerów za pomocą technologii Windows Connect Now303, 304, 329, 350
Dodawanie komputerów za pomocą urządzenia wymiennego 302, 305, 350
Dodawanie kont poczty internetowej 190
Dodawanie kont poczty internetowej POP3 lub MSN/Hotmail 190
Dodawanie książek adresowych....200
Dodawanie połączenia z zabronionym komputerem 164
Dodawanie połączenia z zaufanym komputerem 159
Dodawanie witryny sieci Web do listy akceptowanych plików cookie użytkownika 238
Dodawanie witryny sieci Web do listy odrzucanych plików cookie użytkownika241
Dodawanie zaufanego komputera z poziomu dziennika Zdarzenia przychodzące ..160, 171
Dołączanie do chronionych sieci bezprzewodowych 291, 294, 314, 354
Dołączanie do sieci....368
Dołączanie do sieci zarządzanej 63, 64, 367, 371
domena 387
Dozwolone witryny sieci Web 234, 249
dysk sieciowy 387

E

Edycja filtrów osobistych 211
Edycja internetowych kont POP3 lub MSN/Hotmail.... 192
Edycja książek adresowych 201
Edycja listy znajomych.... 199
Edycja połączenia z zabronionym komputerem 165
Edycja połączenia z zaufanym komputerem 161
ESS (Extended Service Set, rozszerzony zestaw usług).... 387

F

Filtrowanie wiadomości zawierających określone zestawy znaków.... 207
Funkcje .10, 46, 52, 56, 74, 118, 186, 232, 266, 284, 364
funkcje ochrony rodzicielskiej.... 387

G

grupy klasyfikacji zawartości 387

H

hasło.... 388

I

Ikony programu Wireless Network Security — informacje 308, 337
Informacje o alertach 124
Informacje o aplikacjach SystemGuard z kategorii Program.... 85
Informacje o aplikacjach SystemGuard z kategorii Windows 87
Informacje o bezpieczeństwie internetowym 183
Informacje o firmie McAfee.... 401
Informacje o programach.... 150
Informacje o programach SystemGuard z kategorii Przeglądarka.... 90
Informacje o programie 150
Informacje o programie znajdujące się w dzienniku Zdarzenia wychodzące ... 150, 172
Informacje o sieci komputera 176
Informacje o wykresie Analiza ruchu. 179, 180
Inne problemy.... 360
Instalowanie dostępnej drukarki sieciowej. 381
Instalowanie oprogramowania zabezpieczającego McAfee na zdalnych komputerach.... 72
Instalowanie programu Wireless Network Security 348
Internet.... 388

intranet....388

J

Jak działa ochrona komputera i plików....17
Jak działa ochrona poczty e-mail i wiadomości błyskawicznych....19
Jak działa stan ochrony....15
Jak działa system generowania alertów zabezpieczeń....78, 109, 112
Jak działają Funkcje ochrony rodzicielskiej..20
Jak działają ikony programu Network Manager 57
Jak działają ikony programu SecurityCenter.13
Jak działają kategorie i typy ochrony....16
Jak działają zabezpieczenia Internetu i sieci .18

K

karta PCI sieci bezprzewodowej 388
karta sieci bezprzewodowej....388
karta sieciowa....388
karta USB sieci bezprzewodowej....388
Kilka kart sieciowych....350
klient....388
klient poczty e-mail....388
klucz....389
kompresja....389
Konfiguracja lokalizacji przeznaczonych do skanowania 101
Konfiguracja nowego portu usług systemowych....155
Konfiguracja ochrony poczty e-mail....95, 113
Konfiguracja ochrony w czasie rzeczywistym 79, 80
Konfiguracja programów SystemGuard....84
Konfiguracja typów archiwizowanych plików 270
Konfiguracja ustawień dziennika zdarzeń...170
Konfiguracja ustawień stanu ochrony związanych z zaporą....138
Konfiguracja wykrywania włamań 137
Konfigurowanie alertów informacyjnych....37
Konfigurowanie grupy klasyfikacji zawartości użytkownika....234, 249, 253
Konfigurowanie ignorowanych problemów..26
Konfigurowanie inteligentnych zaleceń dla alertów 134
Konfigurowanie Magazynu haseł....260
Konfigurowanie ochrony poczty e-mail....95
Konfigurowanie ochrony przed atakami typu 223
Konfigurowanie ochrony przy użyciu zapory 129
Konfigurowanie ochrony rodzicielskiej 233
Konfigurowanie ochrony w czasie rzeczywistym 80
Konfigurowanie opcji aktualizacji.... 31
Konfigurowanie opcji alertów 36
Konfigurowanie opcji archiwizowania.... 268
Konfigurowanie opcji programu SecurityCenter.... 25
Konfigurowanie opcji użytkowników 27, 29
Konfigurowanie portów usług systemowych 154
Konfigurowanie programów SystemGuard.. 84
Konfigurowanie programu EasyNetwork... 365
Konfigurowanie ręcznego skanowania. 98, 100
Konfigurowanie routerów bezprzewodowych lub punktów dostępu 361
Konfigurowanie stanu ochrony.... 26
Konfigurowanie trybów zabezpieczeń 320
Konfigurowanie typów plików, które będą skanowane.... 100
Konfigurowanie ustawień alertów.... 312
Konfigurowanie ustawień zabezpieczeń.... 320, 362
Konfigurowanie ustawień zabezpieczeń sieci 322
Konfigurowanie ustawień żądania ping..... 137
Konfigurowanie zabezpieczonych sieci bezprzewodowych.... 290
Konfigurowanie zarządzanej sieci.... 59
konto MAPI.... 389
konto MSN 389
konto POP3.... 389
koń trojański 389
Kończenie monitorowania stanu ochrony komputera 69
Kończenie udostępniania drukarki 380
Kończenie udostępniania pliku.... 375
Kopiowanie udostępnianego pliku 375
Korzystanie z Menu zaawansowanego.... 23
Korzystanie z ochrony poczty e-mail 94
Korzystanie z ochrony przed oprogramowaniem szpiegującym.... 82
Korzystanie z ochrony przed wirusami 78
Korzystanie z ochrony wiadomości błyskawicznych.... 96
Korzystanie z pasków narzędzi 221
Korzystanie z programów SystemGuard..... 83
Korzystanie z programu QuickClean..... 49
Korzystanie z programu SecurityCenter..... 11
Korzystanie z programu Shredder 54
Korzystanie z wyrażeń regularnych.... 213, 214
Korzystanie ze skanowania skryptów..... 93
kwarantanna.... 389

L

LAN (Local Area Network, sieć lokalna) ...389
lokalizacja monitorowana częściowo 390
lokalizacja monitorowana dokładnie.....390
lokalizacje monitorowane.....390
Lokalizowanie komputera w sieci 175

Ł

Łączenie komputerów z siecią 353
Łączenie z chronionymi sieciami bezprzewodowymi 298, 314, 315
Łączenie z Internetem i siecią 355
Łączenie z sieciami z wyłączonym rozgłaszaniem SSID.....300

M

MAC (Media Access Control lub Message Authenticator Code).....390
magazyn haseł 390
mapa sieci 390
McAfee Data Backup 265
McAfee EasyNetwork 363
McAfee Network Manager.....55
McAfee Personal Firewall.....117
McAfee Privacy Service.....231
McAfee QuickClean.....45
McAfee SecurityCenter.....9
McAfee Shredder 51
McAfee SpamKiller 185
McAfee Total Protection 7
McAfee VirusScan 73
McAfee Wireless Network Security.....283
Modyfikacja filtrów specjalnych.....205
Modyfikacja portu usług systemowych.....155
Modyfikacja sposobu przetwarzania wiadomości 206
Modyfikowanie blokowanej witryny sieci Web 246
Modyfikowanie dozwolonej witryny sieci Web 250
Modyfikowanie hasła w magazynie haseł...261
Modyfikowanie listy akceptowanych plików cookie.....252
Modyfikowanie opcji filtrowania.....203
Modyfikowanie uprawnień komputera zarządzanego.....69
Modyfikowanie ustawień filtrowania ataków typu 225
Modyfikowanie ustawień filtrowania wiadomości e-mail.....204
Modyfikowanie ustawień kont poczty internetowej 192
Modyfikowanie ustawień wyświetlania urządzenia 70
Modyfikowanie witryny sieci Web na liście akceptowanych plików cookie użytkownika 239
Modyfikowanie witryny sieci Web na liście odrzucanych plików cookie użytkownika242
Monit o wprowadzenie klucza WEP, WPA lub WPA2..... 356
Monitorowanie aktywności programów 181
Monitorowanie chronionych sieci bezprzewodowych....341, 342, 343, 344, 346
Monitorowanie połączeń w sieci bezprzewodowej.....336, 337, 338, 339, 340
Monitorowanie przepustowości wykorzystywanej przez programy 180
Monitorowanie ruchu internetowego.. 178, 179
Monitorowanie sieci bezprzewodowych 335
Monitorowanie stanu i uprawnień 68
Monitorowanie stanu ochrony komputera 68

N

nagłówek..... 390
Naprawa luk w zabezpieczeniach..... 71
Naprawianie luk w zabezpieczeniach..... 71
Naprawianie problemów dotyczących ochrony 21
Naprawianie ustawień zabezpieczeń sieci . 314, 322, 324, 352, 357
Natychmiastowe odblokowanie zapory..... 139
Natychmiastowe zablokowanie zapory 139
Nazwa sieci różni się od używanej przez inne programy 360
Nie można naprawić routera lub punktu dostępu 352
Nie można połączyć się z Internetem 355
Nie można połączyć się z siecią bezprzewodową..... 357
Nie wykryto zgodnej karty sieci bezprzewodowej..... 349
niekontrolowany punkt dostępu..... 391
Nieobsługiwany router lub punkt dostępu.. 351
Niski poziom sygnału 359
Niszczenie plików, folderów i zawartości dysków. 54

O

Obsługa kont pocztowych w sieci Web..... 189
Obsługa programu SpamKiller..... 219
Ochrona haseł 259
Ochrona informacji w Internecie 255
Ochrona komputera podczas uruchamiania 136
Ochrona sieci bezprzewodowych 289
Oczekiwanie na autoryzację 354

Oczyszczanie komputera 47, 49
Odbieranie powiadomienia o wysłaniu pliku 378
Odkładanie aktualizacji na później.....33, 34
Odświeżanie mapy sieci 61
Odwoływanie dostępu do sieci...291, 299, 314, 316, 317, 318
Omówienie funkcji programu QuickClean ...46
Omówienie funkcji programu Shredder 52
Omówienie programów SystemGuard 85
Omówienie zarządzania filtrami osobistymi 210
Omówienie zarządzania listą znajomych 198
Oprogramowanie ulega awarii po uaktualnieniu systemów operacyjnych 362
Optymalizacja zabezpieczeń programu Firewall 136
Opuszczanie chronionych sieci bezprzewodowych 316, 317, 318, 354
Opuszczanie zarządzanej sieci 371
Otwieranie okienka konfiguracji funkcji ochrony rodzicielskiej.....20
Otwieranie okienka konfiguracji Internet i sieć 18
Otwieranie okienka konfiguracji Komputer i pliki 17
Otwieranie okienka konfiguracji poczty e-mail i wiadomości błyskawicznych 19
Otwieranie okienka konfiguracji programu SecurityCenter 22
Otwieranie programu SecurityCenter i korzystanie z dodatkowych funkcji 13
Otwieranie zarchiwizowanego pliku 279
Oznaczanie wiadomości jako spam lub nie-spam z poziomu paska narzędzi programu SpamKiller 222

P

Planowanie automatycznych archiwizacji...273
Planowanie skanowań 102
plik cookie 391
pluskwy internetowe.....391
Po ponownym uruchomieniu komputera nadal nie można usunąć elementu 114
Pobieranie hasła administratora.....30
Pobieranie w chronionej sieci kończy się niepowodzeniem 350
poczta e-mail 391
podszywanie się pod adres IP.....392
Pokazywanie i ukrywanie elementów na mapie sieci 62
port 392
potencjalnie niepożądany program.....392
Powiadamianie przed pobieraniem aktualizacji 32, 33
PPPoE 392
Praca z alertami 123
Praca z mapą sieci..... 60
Praca z udostępnianymi drukarkami..... 380
Praca ze statystykami..... 174
Praca ze zarchiwizowanymi plikami 277
protokół..... 392
proxy 392
Przeglądanie dzienników odfiltrowanej poczty internetowej..... 196
Przeglądanie ostatnich zdarzeń..... 40
Przeglądanie ostatnich zdarzeń i dzienników 107
Przeglądanie zdarzeń 107
przeglądarka..... 392
Przełączanie się na używanie kont użytkowników oprogramowania firmy McAfee 27
przepełnienie bufora 392
Przeprowadzanie pełnych i szybkich archiwizacji 273
przepustowość 393
Przerywane połączenie 356
Przerywanie automatycznej archiwizacji.... 274
Przyjmowanie pliku z innego komputera .. 377, 378
przywracanie..... 393
Przywracanie brakujących plików z archiwum lokalnego..... 280
Przywracanie komputera do poprzedniego stanu 43
Przywracanie programów poddanych kwarantannie, plików cookie i innych plików 105
Przywracanie starszej wersji pliku z archiwum lokalnego..... 281
Przywracanie ustawień zapory 140
Przywracanie zarchiwizowanych plików ... 280
Przyznanie dostępu nieznanemu komputerowi 354
Przyznawanie dostępu do sieci zarządzanej 368
Przyznawanie dostępu tylko dla połączeń wychodzących z dziennika Ostatnie zdarzenia 145
Przyznawanie dostępu tylko dla połączeń wychodzących z poziomu dziennika Zdarzenia wychodzące..... 146, 172
Przyznawanie komputerom dostępu administracyjnego 291, 298
Przyznawanie nowemu programowi pełnego dostępu 143

Przyznawanie pełnego dostępu z poziomu dziennika Ostatnie zdarzenia 143
Przyznawanie pełnego dostępu z poziomu dziennika Zdarzenia wychodzące 144, 172
Przyznawanie programom dostępu do Internetu.....142
Przyznawanie programom praw dostępu tylko dla połączeń wychodzących.....145
Przyznawanie programowi dostępu tylko dla połączeń wychodzących 145
Przyznawanie programowi pełnego dostępu 142
publiczny punkt dostępu.....393
publikowanie 393
punkt dostępu 393

R

RADIUS (Remote Access Dial-In User Service).....393
Referencja.....383
Rejestrowanie zdarzeń.....160, 167, 168, 170
Rejestrowanie, monitorowanie i analiza.....169, 177
repozytorium kopii zapasowych online.....393
Resetowanie hasła magazynu haseł.....263
Rezygnowanie z ufania komputerom w sieci 66
Ręczne dodawanie znajomych 198
Ręczne dodawanie znajomych z poziomu paska zadań programu SpamKiller.....198
Ręczne dokonywanie cyklicznej zmiany klucza.....330, 342, 356
Ręczne importowanie książek adresowych .200
Ręczne naprawianie problemów dotyczących ochrony 21
Ręczne przeprowadzanie archiwizacji 275
Ręczne przeprowadzanie konserwacji komputera 42
Ręczne skanowanie komputera 97
Ręczne sprawdzanie dostępności aktualizacji 34, 35
roaming.....393
robak.....393
router 394
Rozłączanie z chronionymi sieciami bezprzewodowymi.....314, 316, 317, 318
Rozwiązywanie problemów 114, 347

S

serwer 394
serwer DNS 394
serwer proxy.....394
serwer SMTP.....394
sieć.....394
Sieć wydaje się być niechroniona 353
sieć zarządzana 394
Skanowanie bez użycia ustawień ręcznego skanowania..... 99
Skanowanie ręczne 98
skanowanie w czasie rzeczywistym..... 394
Skanowanie z poziomu Eksploratora Windows 99
Skanowanie z użyciem ustawień ręcznego skanowania..... 98
skrypt 394
słowo kluczowe 395
Sortowanie zarchiwizowanych plików..... 278
Sprawdzanie stanu aktualizacji..... 14
Sprawdzanie stanu ochrony komputera..... 13
SSID (Service Set Identifier)..... 395
SSL (Secure Sockets Layer)..... 395
standardowe konto e-mail..... 395
synchronizacja 395
System Windows nie obsługuje połączenia bezprzewodowego..... 360
System Windows nie wykazuje połączenia 360
SystemGuard 395
szyfrowanie..... 395

Ś

Śledzenie komputera z poziomu dziennika Zdarzenia przychodzące..... 171, 176
Śledzenie komputera z poziomu dziennika Zdarzenia wykrywania włamań 173, 177
Śledzenie monitorowanego adresu IP..... 178
Śledzenie ruchu internetowego... 175, 176, 177

T

tekst zaszyfrowany 395
TKIP (Temporal Key Integrity Protocol) ... 396
Tworzenie chronionych sieci bezprzewodowych..... 292, 316, 353
Tworzenie konta administratora 27, 28
tworzenie kopii zapasowej..... 396
Typy dostępu — informacje 291, 299
typy monitorowanych plików..... 396

U

udostępnianie..... 396
Udostępnianie drukarek..... 379
Udostępnianie i wysyłanie plików..... 373
Udostępnianie plików..... 374
Udostępnianie pliku..... 374
Udzielanie zaufania połączeniom z komputerami 158
Ukrywanie alertów informacyjnych 127
URL 396
Uruchamianie programu EasyNetwork 366

Uruchamianie programu Wireless Network Security 286, 356
Uruchamianie samouczka witryny HackerWatch 184
Uruchamianie zapory 121
Uruchom program EasyNetwork....366
Urządzenia tracą łączność 356
Ustawianie grupy klasyfikacji zawartości użytkownika....235
Ustawianie internetowych limitów czasu użytkownika....244
Ustawianie limitów czasowych użytkownika 244
Ustawianie poziomu blokowania plików cookie użytkownika 237
Ustawianie poziomu blokowania plików cookie użytkownika 236
Ustawianie poziomu blokowania plików cookie użytkownika 251
Ustawianie poziomu zabezpieczeń na poziom Blokada 131
Ustawianie poziomu zabezpieczeń na poziom Zaufanie 133
Ustawianie poziomu zabezpieczeń na Wysoki 132
Ustawienie poziomu zabezpieczeń na poziom Otwarty 140
Ustawienie poziomu zabezpieczeń na Standardowy 132
Ustawienie poziomu zabezpieczeń na Ukryty 131
Usuwanie blokowanej witryny sieci Web ...247
Usuwanie dozwolonej witryny sieci Web ...250
Usuwanie filtrów osobistych 212
Usuwanie hasła z magazynu haseł 262
Usuwanie kluczy sieciowych 333
Usuwanie kont poczty internetowej 194
Usuwanie konta poczty internetowej 194
Usuwanie książek adresowych 201
Usuwanie nieużywanych plików i folderów .42
Usuwanie plików z listy brakujących plików 281
Usuwanie poddanych kwarantannie programów, plików cookie i innych plików 105
Usuwanie połączenia z zabronionym komputerem 166
Usuwanie połączenia z zaufanym komputerem 162
Usuwanie portu usług systemowych 156
Usuwanie praw dostępu programów 149
Usuwanie preferowanych sieci bezprzewodowych 310, 311
Usuwanie routerów bezprzewodowych lub punktów dostępu 314, 315, 350, 354
Usuwanie uprawnienia programu 149
Usuwanie witryny sieci Web z listy akceptowanych plików cookie użytkownika 240
Usuwanie witryny sieci Web z listy odrzucanych plików cookie użytkownika243
Usuwanie znajomych.... 199
uwierzytelnianie.... 396
Uzyskiwanie dodatkowych informacji na temat wirusów.... 44
Uzyskiwanie dostępu do mapy sieci.... 60
Uzyskiwanie informacji o rejestracji komputera 175
Używanie eksploratora archiwum lokalnego 278

V

VPN (Virtual Private Network, wirtualna sieć prywatna) 396

W

wardriver.... 396
WEP (Wired Equivalent Privacy).... 397
węzeł.... 397
Wi-Fi (Wireless Fidelity).... 397
Wi-Fi Alliance 397
Wi-Fi Certified 397
Wirusa nie można wyczyścić ani usunąć.... 114
WLAN (Wireless Local Area Network, bezprzewodowa sieć lokalna) 397
Włączanie filtrowania poczty internetowej 195
Włączanie inteligentnych zaleceń.... 134
Włączanie ochrony i konfigurowanie sieci. 350
Włączanie ochrony poczty e-mail 94
Włączanie ochrony przed atakami typu..... 224
Włączanie ochrony przed oprogramowaniem szpiegującym.... 82
Włączanie ochrony przed spamem 220
Włączanie ochrony przed wirusami.... 79
Włączanie ochrony wiadomości błyskawicznych.... 96
Włączanie paska narzędzi.... 221
Włączanie programów SystemGuard 83
Włączanie skanowania skryptów.... 93
WPA (Wi-Fi Protected Access).... 397
WPA2 398
WPA2-PSK.... 398
WPA-PSK.... 398
współdzielone hasło.... 398
Wstrzymywanie automatycznej cyklicznej zmiany klucza 314, 327, 329, 356
Wybór innego trybu zabezpieczeń.... 362

Wybór komputerów, na których program ma zostać zainstalowany 348
Wykluczenie lokalizacji z archiwum 271
Wykonywanie typowych zadań.....39
Wyłączanie automatycznych aktualizacji32, 34, 35
Wyłączanie filtrowania poczty internetowej 195
Wyłączanie inteligentnych zaleceń 135
Wyłączanie lub włączanie ochrony przed atakami typu.....224
Wyłączanie ochrony poczty e-mail 94
Wyłączanie ochrony przed atakami typu 224
Wyłączanie ochrony przed oprogramowaniem szpiegującym 82
Wyłączanie ochrony przed spamem.....220
Wyłączanie ochrony przed wirusami. 78
Wyłączanie ochrony wiadomości błyskawicznych.....96
Wyłączanie paska narzędzi 221
Wyłączanie programów SystemGuard.....83
Wyłączanie skanowania skryptów 93
Wyłączanie skanowania według słów kluczowych.....247
Wyłączanie szyfrowania i kompresowania archiwum 272
Wymazywanie niepożądanych plików za pomocą programu Shredder.....53
wyskakujące okna 398
Wysyłanie plików do innych komputerów..377
Wysyłanie pliku do innego komputera.....377
Wysyłanie programów poddanych kwarantannie, plików cookie i innych plików do firmy McAfee 106
Wysyłanie raportów do firmy McAfee.....108
Wyszukiwanie udostępnianego pliku.....375
Wyszukiwanie zarchiwizowanego pliku 279
Wyświetlaj klucze w postaci tekstu.....331, 332
Wyświetlanie aktualnie chronionych komputerów 309, 342, 343, 344, 346
Wyświetlanie aktywności dotyczącej portów internetowych na świecie.....174
Wyświetlanie alertów podczas korzystania z gier 127
Wyświetlanie bieżących kluczy 325, 350
Wyświetlanie czasu trwania połączenia sieciowego 336, 337, 338, 339, 340
Wyświetlanie dziennej liczby połączeń.....341, 343, 344, 346
Wyświetlanie dziennika 107
Wyświetlanie informacji dotyczących programu SecurityCenter.....22
Wyświetlanie informacji o zainstalowanych produktach 22
Wyświetlanie kluczy w postaci znaków gwiazdki..... 331, 332
Wyświetlanie liczby cyklicznych zmian klucza 325, 326, 327, 328, 330, 342
Wyświetlanie listy preferowanych sieci 310, 311
Wyświetlanie miesięcznej liczby chronionych komputerów 341, 342, 343, 344, 346
Wyświetlanie mocy sygnału sieci309, 339, 359
Wyświetlanie ostatnich zdarzeń 171
Wyświetlanie podsumowania aktywności użytkownika związanej z archiwizacją ... 282
Wyświetlanie powiadomień o połączeniach315
Wyświetlanie raportu zabezpieczeń w trybie online.....336, 337, 338, 339, 340, 349
Wyświetlanie stanu połączenia.. 336, 337, 338, 339, 340
Wyświetlanie szybkości połączenia sieciowego 336, 337, 338, 339, 340
Wyświetlanie światowych statystyk dotyczących zagrożeń bezpieczeństwa ... 174
Wyświetlanie trybu zabezpieczeń sieci 309, 322, 338, 362
Wyświetlanie tylko inteligentnych zaleceń 135
Wyświetlanie zdarzeń chronionej sieci bezprzewodowej.....341, 342, 343, 344, 346
Wyświetlanie zdarzeń przychodzących..... 171, 176
Wyświetlanie zdarzeń wychodzących 143, 144, 145, 146, 148, 151, 172
Wyświetlanie zdarzeń wykrywania włamań173
Wyświetlenie szczegółów elementu 62
Wznawianie cyklicznej zmiany klucza326, 327, 329, 356

Z

Zamiana komputerów 362
Zapobieganie ustawianiu plików cookie przez witrynę sieci Web..... 252
zapora..... 398
Zapraszanie komputera do dołączenia do sieci zarządzanej..... 65
Zarządzanie alertami..... 110
Zarządzanie alertami informacyjnymi..... 127
Zarządzanie archiwami..... 282
Zarządzanie filtrami osobistymi 209
Zarządzanie filtrowaniem poczty internetowej 195
Zarządzanie listami elementów zaufanych. 104
Zarządzanie listą znajomych..... 197
Zarządzanie ochroną przed spamem..... 220
Zarządzanie ochroną przed wirusami 77
Zarządzanie odfiltrowanymi wiadomościami w kontach poczty internetowej 196

Zarządzanie poddanymi kwarantannie programami, plikami cookie i innymi plikami 105, 114
Zarządzanie połączeniami z komputerem ...157
Zarządzanie poziomami zabezpieczeń zapory 130
Zarządzanie programami i uprawnieniami ..141
Zarządzanie sieciami bezprzewodowymi....308
Zarządzanie siecią 43
Zarządzanie urządzeniem 70
Zarządzanie usługami systemowymi....153
Zarządzanie zabezpieczeniami sieci bezprzewodowych 319
Zatrzymywanie programu Wireless Network Security 287
Zatrzymywanie zapory 122
Zawieranie lokalizacji w archiwum 269
Zdalne zarządzanie siecią....67
zdarzenie....399
zewnętrzny dysk twardy....400
Zezwalanie na korzystanie z danej witryny sieci Web 249
Zezwalanie witrynie sieci Web na ustawianie plików cookie....251
Zezwalanie witrynom sieci Web na zapisywanie plików cookie....251
Zezwolenie na dostęp do istniejącego portu usług systemowych....154
Zgłaszanie wiadomości uznanych za spam .208
Zmiana lokalizacji archiwum 271
Zmiana nazwy sieci....61, 370
Zmiana poziomu filtrowania wiadomości e-mail 204
Zmiana sposobu przetwarzania wiadomości zidentyfikowanych jako spam 206
Zmienianie częstotliwości cyklicznej zmiany klucza....326, 327, 330
Zmienianie hasła administratora 30
Zmienianie nazw chronionych sieci bezprzewodowych 311, 314
Zmienianie poświadczeń dla urządzeń bezprzewodowych 314, 323, 352
Zostało wykryte zagrożenie — co robić?....112
zwykły tekst....400