McAfee®

Wireless Protection 2007

Podręcznik użytkownika

Spis treści

ROZDZIAŁ 1

McAfee Wireless Protection

Pakiet McAfee Wireless Protection Suite eliminuje problemy i zagrożenia związane z korzystaniem z sieci bezprzewodowych. Niezawodne i proste w obsłudze zabezpieczenia uniemożliwiają hakerom skuteczne atakowanie sieci bezprzewodowej Wi-Fi®, chronią informacje osobiste i dane transakcji oraz zapobiegają wykorzystywaniu sieci bezprzewodowej przez osoby nieupoważnione, chcące w ten sposób uzyskać dostęp do Internetu. W programie McAfee Wireless Network Security używane są silne, cyklicznie zmieniane klucze szyfrowania, które pokrzyżują plany nawet najbardziej upartym intruzom. W skład pakietu Wireless Protection wchodzi też program McAfee EasyNetwork — narzędzie pozwalające na łatwe udostępnianie plików i drukarek w sieci. Program McAfee Network Manager, również zawarty w pakiecie, monitoruje komputery w sieci pod kątem wyszukiwania luk w zabezpieczeniach i ułatwia eliminowanie ewentualnych problemów dotyczących bezpieczeństwa.

Pakiet Wireless Protection zawiera następujące programy:

- SecurityCenter
- Wireless Network Security
- Network Manager
- EasyNetwork

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

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

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

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 26).

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 30)
   - Pobieraj aktualizacje automatycznie i powiadamiaj mnie, gdy są gotowe do zainstalowania (strona 31)
   - Powiadamiaj przed pobieraniem jakichkolwiek aktualizacji (strona 31)
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 32).

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 32).

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 33) 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 32).

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

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

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

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

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

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

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

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

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 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

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 14

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

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

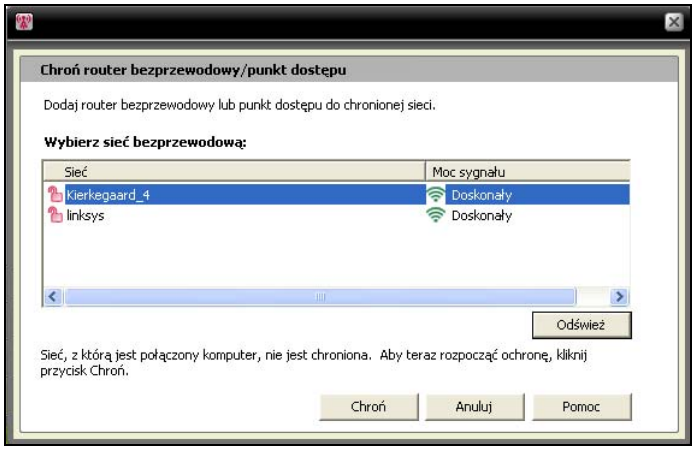
- Dołączanie do chronionej sieci bezprzewodowej (strona 82)
- Przyznawanie komputerom dostępu administracyjnego (strona 86)
- Odwoływanie dostępu do sieci (strona 105)

Tworzenie chronionych sieci bezprzewodowych

Aby utworzyć chronioną sieć bezprzewodową, należy najpierw dodać jej router bezprzewodowy lub punkt dostępu.

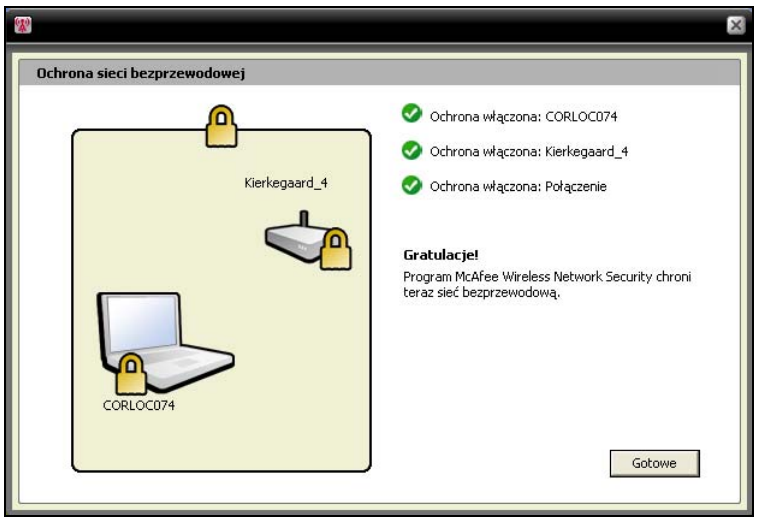
Aby dodać router bezprzewodowy lub punkt dostępu:

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 88)
- Dodawanie komputerów do chronionej sieci bezprzewodowej (strona 90)

Dołączanie do chronionych sieci bezprzewodowych

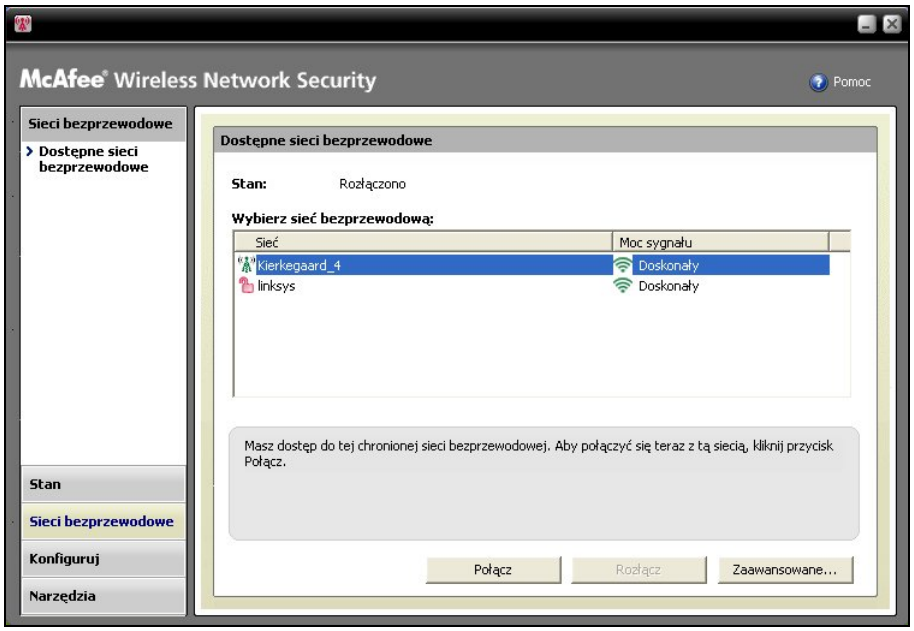
Chroniona sieć bezprzewodowa uniemożliwia hakerom przechwytywanie danych przesyłanych przez nią i podłączanie się do niej. Aby nieupoważniony komputer mógł uzyskać dostęp do chronionej sieci bezprzewodowej, musi najpierw do niej dołączyć.

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.

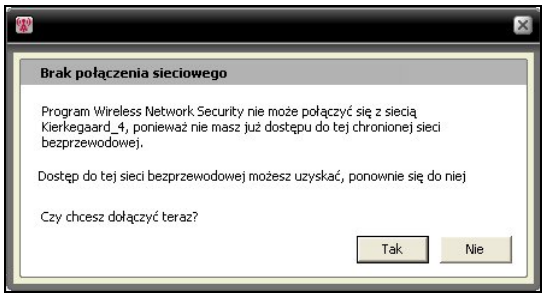
Przed dołączeniem do chronionej sieci należy zainstalować Wireless Network Security, a następnie połączyć się z chronioną siecią bezprzewodową. Do dołączenia się do sieci wymagane jest zezwolenie od użytkownika z dostępem administracyjnym do chronionej sieci bezprzewodowej. Po dołączeniu do sieci ponowne 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:

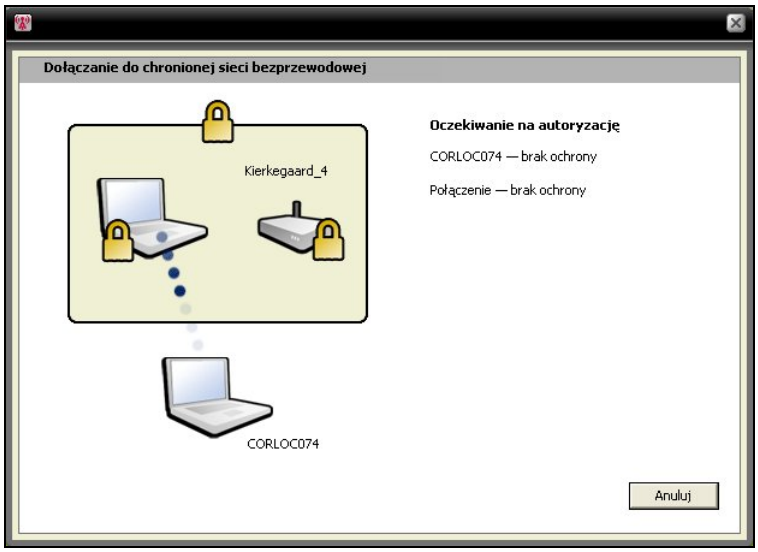
1. Na niechronionym komputerze kliknij prawym przyciskiem myszy ikonę programu Wireless Network Security w obszarze powiadomień systemu Windows.
2. Wybierz polecenie **Wyświetl sieci bezprzewodowe**.
3. W okienku Dostępne sieci bezprzewodowe zaznacz sieć, a następnie kliknij polecenie **Połącz**.



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:

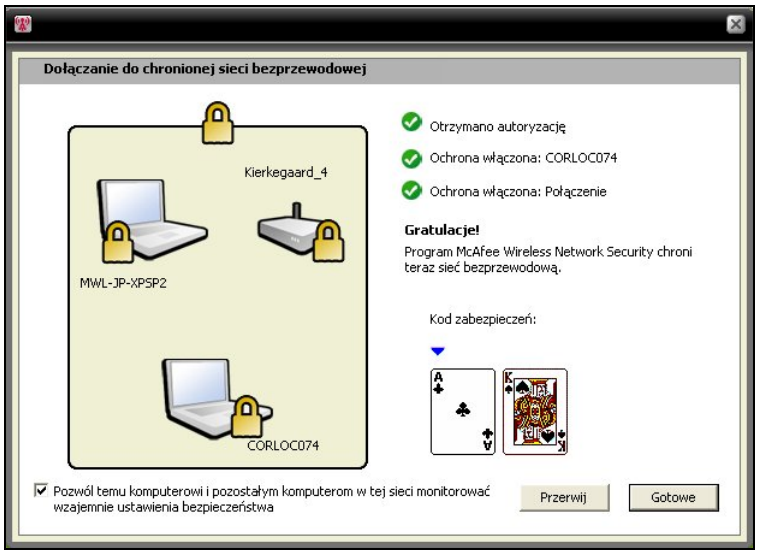
Przyznaj dostęp typu Gość	Pozwala komputerowi na wysyłanie plików do innych komputerów w sieci bezprzewodowej, ale nie na udostępnianie ich za pomocą programu McAfee EasyNetwork.
Przyznaj dostęp Pełny do wszystkich zarządzanych aplikacji sieciowych	Pozwala komputerowi na wysyłanie plików i udostępnianie 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**.

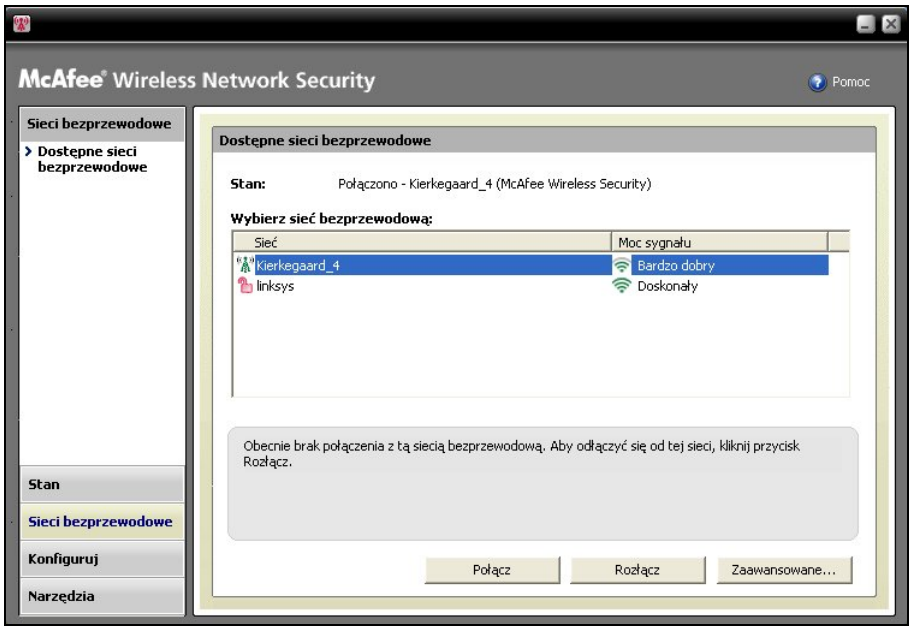
Jeśli na komputerach nie są wyświetlane identyczne karty, mogło nastąpić naruszenie zabezpieczeń. Przyznanie temu komputerowi dostępu do sieci może stanowić zagrożenie dla komputera. Aby uniemożliwić temu komputerowi uzyskanie dostępu do sieci bezprzewodowej, kliknij przycisk **Odmów dostępu**.

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 90)

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.

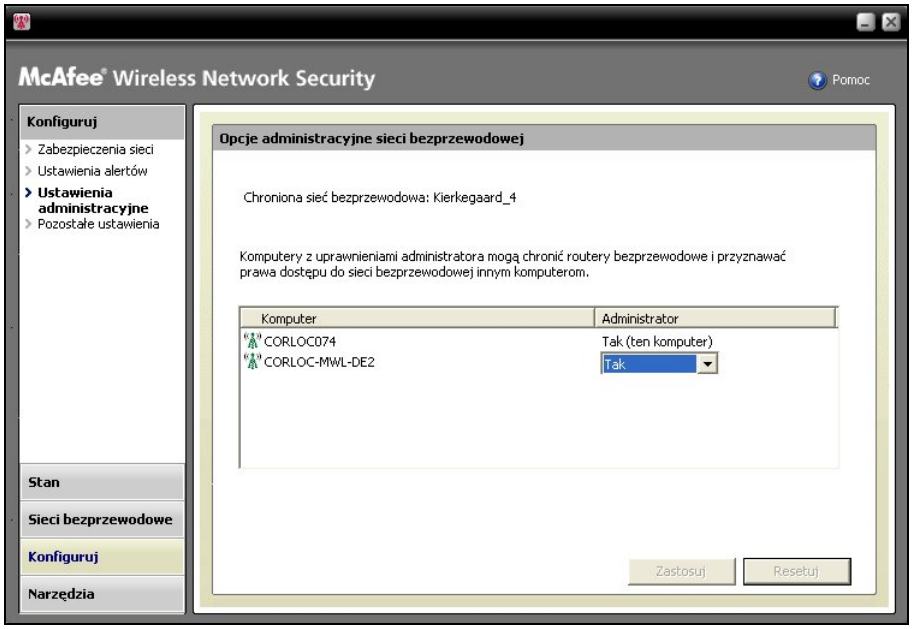
Aby skonfigurować dostęp administracyjny:

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 79)
- Odwoływanie dostępu do sieci (strona 105)

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 92)

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 90)

ROZDZIAŁ 15

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

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 127)
- Wyświetlanie aktualnie chronionych komputerów (strona 134)
- Wyświetlanie trybu zabezpieczeń sieci (strona 126)

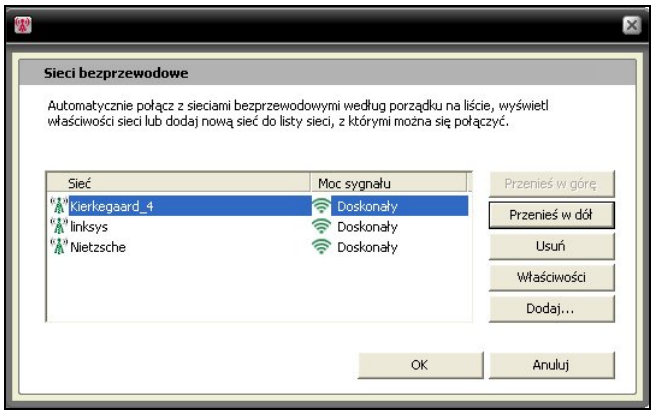
Wyświetlanie listy preferowanych sieci

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 99)

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 98)

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 114)
- Dołączanie do chronionej sieci bezprzewodowej (strona 82)
- Łączenie z chronionymi sieciami bezprzewodowymi (strona 86)
- Rozłączanie z chronionymi sieciami bezprzewodowymi (strona 104)
- Wstrzymywanie automatycznej cyklicznej zmiany klucza (strona 117)
- Odwoływanie dostępu do sieci (strona 105)
- Usuwanie routerów bezprzewodowych lub punktów dostępu (strona 103)
- Zmienianie poświadczeń dla urządzeń bezprzewodowych (strona 111)
- Zmienianie nazw chronionych sieci bezprzewodowych (strona 99)
- Naprawianie ustawień zabezpieczeń sieci (strona 112)

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

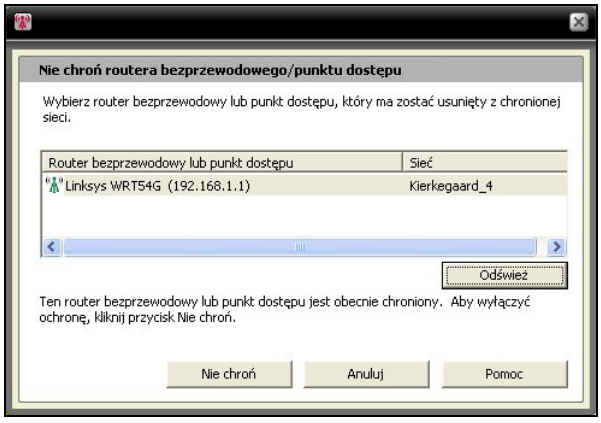
- Łączenie z chronionymi sieciami bezprzewodowymi (strona 86)

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 80)

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 105)
- Opuszczanie chronionych sieci bezprzewodowych (strona 106)

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 104)
- Opuszczanie chronionych sieci bezprzewodowych (strona 106)

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 104)
- Odwoływanie dostępu do sieci (strona 105)

ROZDZIAŁ 16

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

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 112)
- Wyświetlanie trybu zabezpieczeń sieci (strona 126)

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.

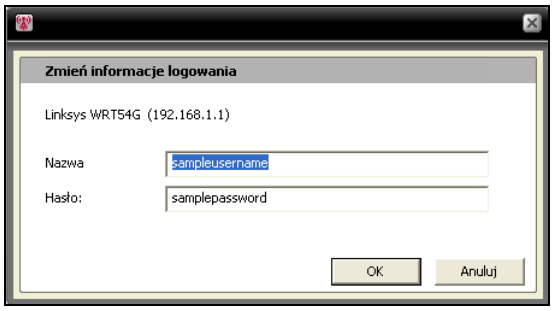
Zmienianie poświadczeń dla urządzeń bezprzewodowych

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 130)

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 115)
- Wznawianie cyklicznej zmiany klucza (strona 115)
- Wyświetlanie liczby cyklicznych zmian klucza (strona 130)

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 114)
- Wstrzymywanie automatycznej cyklicznej zmiany klucza (strona 117)
- Wyświetlanie liczby cyklicznych zmian klucza (strona 130)

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 114)
- Wyświetlanie liczby cyklicznych zmian klucza (strona 130)

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 114)
- Dodawanie komputerów za pomocą technologii Windows Connect Now (strona 92)
- Wznawianie cyklicznej zmiany klucza (strona 115)

- Automatyczna cykliczna zmiana klucza (strona 114)
- Wyświetlanie liczby cyklicznych zmian klucza (strona 130)

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 114)
- Zmienianie częstotliwości cyklicznej zmiany klucza (strona 115)
- Wyświetlanie liczby cyklicznych zmian klucza (strona 130)

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 120)

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.

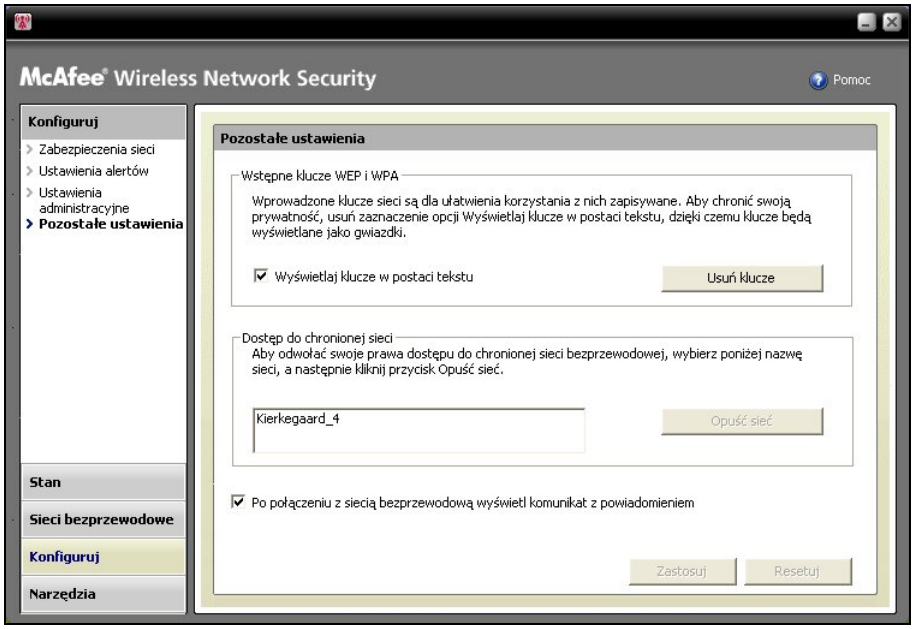
W sieciach chronionych przez program Wireless Network Security klucze są wyświetlane w postaci tekstu.

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 119)

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 17

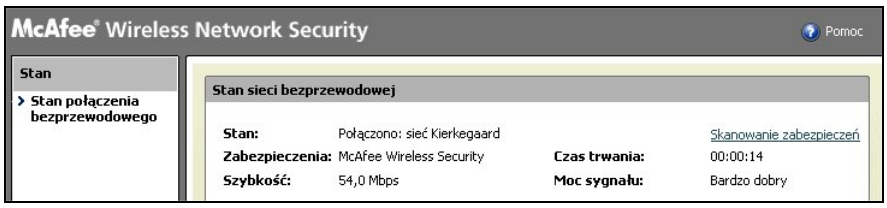
Monitorowanie sieci bezprzewodowych

Program Wireless Network Security pozwala monitorować stan sieci bezprzewodowej i chronionych komputerów.

W tym rozdziale

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 125)
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 126)
Szybkość	Określa szybkość połączenia komputera z siecią.	Wyświetlanie szybkości połączenia sieciowego (strona 126)
Czas trwania	Określa czas trwania połączenia komputera z siecią.	Wyświetlanie czasu trwania połączenia sieciowego (strona 127)
Moc sygnału	Określa względną moc sygnału sieci.	Wyświetlanie mocy sygnału sieci (strona 128)

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 128)

Tematy pokrewne

- Ikony programu Wireless Network Security — informacje (strona 96)

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 124)
- Wyświetlanie trybu zabezpieczeń sieci (strona 126)
- Wyświetlanie szybkości połączenia sieciowego (strona 126)
- Wyświetlanie czasu trwania połączenia sieciowego (strona 127)
- Wyświetlanie mocy sygnału sieci (strona 128)
- Wyświetlanie raportu zabezpieczeń w trybie online (strona 128)

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 124)
- Wyświetlanie stanu połączenia (strona 125)
- Wyświetlanie szybkości połączenia sieciowego (strona 126)
- Wyświetlanie czasu trwania połączenia sieciowego (strona 127)
- Wyświetlanie mocy sygnału sieci (strona 128)
- Wyświetlanie raportu zabezpieczeń w trybie online (strona 128)

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 124)
- Wyświetlanie stanu połączenia (strona 125)
- Wyświetlanie trybu zabezpieczeń sieci (strona 126)
- Wyświetlanie czasu trwania połączenia sieciowego (strona 127)
- Wyświetlanie mocy sygnału sieci (strona 128)
- Wyświetlanie raportu zabezpieczeń w trybie online (strona 128)

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 124)
- Wyświetlanie stanu połączenia (strona 125)
- Wyświetlanie trybu zabezpieczeń sieci (strona 126)
- Wyświetlanie szybkości połączenia sieciowego (strona 126)
- Wyświetlanie mocy sygnału sieci (strona 128)
- Wyświetlanie raportu zabezpieczeń w trybie online (strona 128)

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 124)
- Wyświetlanie stanu połączenia (strona 125)
- Wyświetlanie trybu zabezpieczeń sieci (strona 126)
- Wyświetlanie szybkości połączenia sieciowego (strona 126)
- Wyświetlanie czasu trwania połączenia sieciowego (strona 127)
- Wyświetlanie raportu zabezpieczeń w trybie online (strona 128)

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.

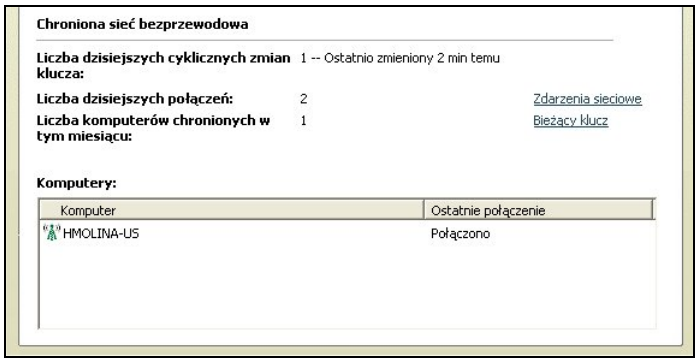
Program McAfee Wi-FiScan obsługuje program Explorer w wersji 5.5 i nowszych.

Tematy pokrewne

- Monitorowanie połączeń w sieci bezprzewodowej (strona 124)
- Wyświetlanie stanu połączenia (strona 125)
- Wyświetlanie trybu zabezpieczeń sieci (strona 126)
- Wyświetlanie szybkości połączenia sieciowego (strona 126)
- Wyświetlanie czasu trwania połączenia sieciowego (strona 127)
- Wyświetlanie mocy sygnału sieci (strona 128)

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 131)
Liczba dzisiejszych połączeń	Określa dzienną liczbę połączeń z chronioną siecią bezprzewodową.	Wyświetlanie dziennej liczby połączeń (strona 132)
Liczba komputerów chronionych w tym miesiącu	Określa liczbę komputerów chronionych w bieżącym miesiącu.	Wyświetlanie miesięcznej liczby chronionych komputerów (strona 132)
Zdarzenia sieciowe	Kliknięcie opcji **Zdarzenia sieciowe** powoduje wyświetlenie zdarzeń dotyczących sieci, połączenia i cyklicznej zmiany klucza.	Wyświetlanie zdarzeń chronionej sieci bezprzewodowej (strona 132)

Komputery	Określa liczbę komputerów połączonych z chronioną siecią bezprzewodową oraz datę i godzinę nawiązania połączenia przez każdy z nich.	Wyświetlanie aktualnie chronionych komputerów (strona 134)

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 129)
- Wyświetlanie dziennej liczby połączeń (strona 132)
- Wyświetlanie miesięcznej liczby chronionych komputerów (strona 132)
- Wyświetlanie zdarzeń chronionej sieci bezprzewodowej (strona 132)
- Wyświetlanie aktualnie chronionych komputerów (strona 134)
- Administrowanie kluczami sieciowymi (strona 113)
- Automatyczna cykliczna zmiana klucza (strona 114)
- Ręczne dokonywanie cyklicznej zmiany klucza (strona 118)

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 129)
- Wyświetlanie miesięcznej liczby chronionych komputerów (strona 132)
- Wyświetlanie zdarzeń chronionej sieci bezprzewodowej (strona 132)
- Wyświetlanie aktualnie chronionych komputerów (strona 134)

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 129)
- Wyświetlanie liczby cyklicznych zmian klucza (strona 131)
- Wyświetlanie dziennej liczby połączeń (strona 132)
- Wyświetlanie zdarzeń chronionej sieci bezprzewodowej (strona 132)
- Wyświetlanie aktualnie chronionych komputerów (strona 134)

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 129)
- Wyświetlanie liczby cyklicznych zmian klucza (strona 131)
- Wyświetlanie dziennej liczby połączeń (strona 131)
- Wyświetlanie dziennej liczby połączeń (strona 132)
- Wyświetlanie aktualnie chronionych komputerów (strona 134)

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 129)
- Wyświetlanie liczby cyklicznych zmian klucza (strona 131)
- Wyświetlanie dziennej liczby połączeń (strona 131)
- Wyświetlanie miesięcznej liczby chronionych komputerów (strona 132)
- Wyświetlanie zdarzeń chronionej sieci bezprzewodowej (strona 132)

ROZDZIAŁ 18

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

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.

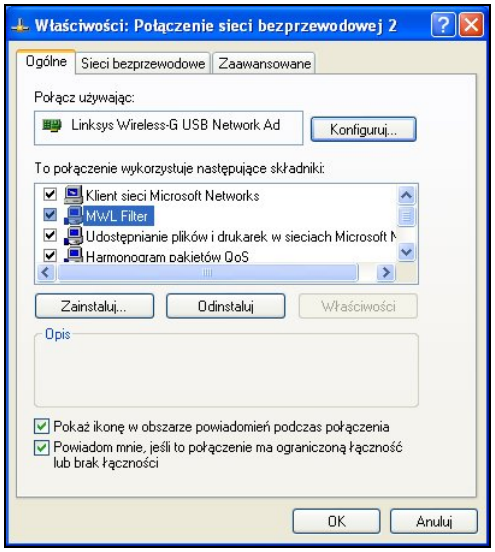
Program można (ale nie jest to wymagane) zainstalować na komputerach, które nie mają kart sieci bezprzewodowej. Nie będzie on jednak aktywny na tych komputerach, ponieważ nie potrzebują one ochrony w sieci bezprzewodowej.

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 128)

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 103)
- Wyświetlanie bieżących kluczy (strona 113)
- Dodawanie komputerów za pomocą urządzenia wymiennego (strona 90)
- Dodawanie komputerów za pomocą technologii Windows Connect Now (strona 92)

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 111)
- Automatyczna cykliczna zmiana klucza (strona 114)

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 112)

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 80)
- 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 82)
- Opuszczanie chronionych sieci bezprzewodowych (strona 106)
- Usuwanie routerów bezprzewodowych lub punktów dostępu (strona 103)
- Dodawanie komputerów do chronionej sieci bezprzewodowej (strona 90)

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 114)
- Wznawianie cyklicznej zmiany klucza (strona 115)
- Wstrzymywanie automatycznej cyklicznej zmiany klucza (strona 117)
- Ręczne dokonywanie cyklicznej zmiany klucza (strona 118)

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 117)

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 74)
- Dodawanie komputerów do chronionej sieci bezprzewodowej (strona 90)

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 112)
- Aktualizowanie karty sieci bezprzewodowej (strona 146)

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 97)
- Wyświetlanie mocy sygnału sieci (strona 127)

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 108)
- Wyświetlanie trybu zabezpieczeń sieci (strona 126)

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 19

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

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 20

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

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 155).

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 21

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

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 166).

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 22

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

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 23

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

J

K

L

Ł

M

N

O

P

R

S

T

U

V

W

Z