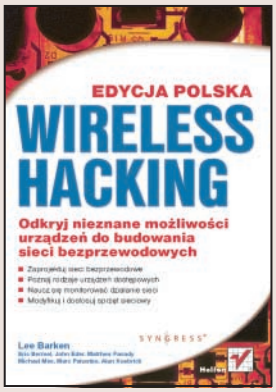
Wireless Hacking. Edycja polska



Autorzy: Lee Barken i inni
Tłumaczenie: Adam Jarczyk
ISBN: 83-7361-794-9
Tytuł oryginału: Wireless Hacking
Format: B5, stron: 328

Odkryj nieznane możliwości urządzeń do budowania sieci bezprzewodowych

- Zaprojektuj sieci bezprzewodowe
- Poznaj rodzaje urządzeń dostępowych
- Naucz się monitorować działanie sieci
- Modyfikuj i dostosuj sprzęt sieciowy

Sieci bezprzewodowe stają się coraz popularniejsze. Producenci sprzętu prześcigają się we wprowadzaniu na rynek coraz nowszych i prostszych w obsłudze urządzeń. Wszystkie te urządzenia posiadają jednak podstawową wadę — są projektowane pod kątem możliwie najszerszego rynku, co niestety wyklucza zastosowanie ich w sposób odbiegający od tego, czego — zdaniem ich producentów — może oczekiwać użytkownik. Na szczęście jednak istnieją ludzie, którzy nie obawiają się rozkręcania takich urządzeń i modyfikowania ich tak, aby spełniały nieco wyższe oczekiwania, stawiane przez użytkowników sieci bezprzewodowych.

Jeśli chcesz zostać kimś takim i jesteś ciekawy, jak można wycisnąć maksimum możliwości z urządzeń sieci bezprzewodowej, przeczytaj książkę „Wireless hacking. Edycja polska". Dowiesz się z niej, jak projektować i instalować sieci bezprzewodowe, jak modyfikować urządzenia dostępowe, wyposażając je w pozornie niedostępne dla nich funkcje, i jak budować urządzenia sieciowe zasilane energią słoneczną. Nauczysz się konfigurować systemy operacyjne urządzeń bezprzewodowych, instalować anteny i poprawiać osiągi urządzeń sieciowych.

- Projektowanie sieci bezprzewodowych
- Bezpieczeństwo transmisji w sieciach bezprzewodowych
- Punkty dostępowe
- Systemy operacyjne dla urządzeń sieciowych
- Monitorowanie działania sieci
- Instalowanie anten
- Zasilanie słoneczne dla punktów dostępowych

Wykorzystaj wiadomości z tej książki do stworzenia idealnej sieci bezprzewodowej

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Rozdział 3.

Bezpieczeństwo sieci bezprzewodowej

W tym rozdziale:

- Portal przechwytujący
- Budowanie VPN z PPTP
- Edukacja użytkowników sieci bezprzewodowej
- Inne metody

Wprowadzenie

W SoCalFreeNet projektujemy sieci bezprzewodowe jako miejsca, w których ludzie z sąsiedztwa mogą odpocząć i przespacerować się po WWW. Bezpieczne przeglądanie stron WWW w sieci bezprzewodowej tworzy atmosferę wspólnoty, podobnie jak park miejski. Nasza grupa często używa analogii do parku, aby wyrazić cele działań przy budowaniu i utrzymywaniu sieci.

Stworzyliśmy sąsiedzką sieć bezprzewodową, aby pozwolić zwykłym ludziom na łączenie się z Internetem za pomocą podstawowych urządzeń bezprzewodowych. Nacisk na to, by trzymać się podstaw, umożliwia korzystanie z sieci najróżnorodniejszym użytkownikiem, od elity technicznej aż po babcie i dziadków mających po raz pierwszy w życiu kontakt z Siecią. Nowi użytkownicy sieci bezprzewodowej mogą wchłonąć tylko ograniczoną ilość wiadomości, zanim przytłoczy ich technologia, więc staramy się, by dla takich użytkowników złożoność zabezpieczeń miała określone granice.

Bezpieczeństwo sieci bezprzewodowych oczywiście sprawia pewne problemy. Biorą się one przede wszystkim z fizycznej natury sygnałów bezprzewodowych. Sygnały komputerowe przesyłane tradycyjnymi sieciami kablowymi rozchodzą się w sposób o wiele bardziej kontrolowany, sterowany przez przełączniki, routery i zapory, które grają w sieci rolę „odźwiernych". W przeciwieństwie do nich nasze sieci bezprzewodowe „rzucają pakietami" we wszystkie strony; pakiet zatrzymuje się dopiero wtedy, gdy

poziom sygnału spadnie w końcu na tyle, by inne urządzenia nie mogły *słyszeć* naszego sygnału. Czułe odbiorniki pozwalają nieraz odbierać sygnały z sieci bezprzewodowych z odległości kilku kilometrów (jeden z naszych użytkowników zbudował z urządzeń Linksys na pustyni łącze o długości ponad 20 kilometrów bez dodatkowego wzmacniania sygnałów). Oznacza to jednocześnie, że ktoś może próbować podsłuchiwać naszą sieć z dużej odległości.

Tacy podsłuchiwacze przypominają nam o starej prawdzie, że jedni ludzie korzystają z techniki (bezprzewodowej) do osiągania pozytywnych celów, a inni będą używać naszej sieci do negatywnych działań. Tacy niegodziwi użytkownicy często mogą stwarzać problemy innym ludziom i architektom naszej bezprzewodowej społeczności. I podobnie jak w parku, musimy podjąć odpowiednie działania, by wspólne dobro pozostało czyste — więc musimy pozbierać śmieci.

Użytkownicy o złych zamiarach mogą stwarzać problemy, ogólnie mówiąc, na trzy sposoby:

- atakując innych użytkowników w lokalnej sieci,
- atakując użytkowników lub komputery w Internecie,
- popełniając przestępstwa w naszej sieci sąsiedzkiej.

Przestępstwa zachodzą, gdy użytkownik próbuje włamać się do komputera lub atakuje innych użytkowników w Internecie. Może też wykorzystać połączenie z Internetem do pobierania pornografii dziecięcej lub przeprowadzania nielegalnych transakcji.

Wszystkie te działania mogą potencjalnie narobić poważnych szkód w społeczności sieci, a nawet spowodować pociągnięcie do odpowiedzialności architektów sieci bezprzewodowej. Dlatego też nasi architekci zabrali się do szukania rozwiązań takich problemów. Wprawdzie za bezpieczeństwo zawsze odpowiada użytkownik, lecz są pewne kroki, które możemy podjąć, aby zwiększyć bezpieczeństwo sieci. W niniejszym rozdziale zostaną omówione następujące metody zwiększania bezpieczeństwa:

- Instalacja portalu przechwytującego.
- Pisanie własnych umów o zasadach korzystania z usług.
- Grafika dla portalu przechwytującego.
- Budowanie VPN z PPTP.
- Włączanie obsługi VPN.
- Konfiguracja użytkowników w sieci sąsiedzkiej.
- Edukacja użytkowników sieci bezprzewodowej.
- Początek i koniec.

Niniejszy rozdział poświęcony jest przede wszystkim sposobom ochrony społeczności użytkowników. Zawarty w nim materiał koncentruje się na nowatorskich podejściach do zagadnień bezpieczeństwa naszego bezprzewodowego „parku miejskiego”.

Portal przechwytujący

Groźba spraw sądowych jest jedną z największych barier w tworzeniu bezpiecznych sieci ogólnodostępnych. Poza kwestiami prawnymi sieci stawiają wiele wyzwań związanych z bezpieczeństwem. Wprawdzie opisane tu zabezpieczenia rozwiązują wiele problemów i skracają listę zagrożeń, lecz środki te są skuteczne tylko wtedy, gdy społeczność użytkowników z nich korzysta. Wielu użytkowników chce się po prostu jak najszybciej połączyć z Internetem i całkowicie ignoruje bezpieczeństwo. Ta ignorancja jest inspiracją dla starego amerykańskiego powiedzenia: „Można zaprowadzić konia do wody, lecz nie można zmusić go do picia".

Idea portalu przechwytującego bierze się z kwestii prawnych związanych z użytkowaniem sieci bezprzewodowych. Poza zwiększeniem bezpieczeństwa portal jest wygodnym narzędziem do dostarczania informacji i wskazówek społeczności użytkowników. Narzędzie to „siedzi" po prostu w połączeniu z Internetem i przechwytuje pierwsze połączenie z WWW. Gdy nadchodzi pierwsze żądanie połączenia od użytkownika, portal przechwytujący kieruje użytkownika do strony zawierającej oświadczenie o odpowiedzialności prawnej i wytyczne dla użytkowników. Ta strona, często nazywana w literaturze Terms of Service (ToS — zasady świadczenia usługi), jest podstawą umowy prawnej społeczności sieci z użytkownikiem. Tutaj użytkownik może przeczytać o zagadnieniach bezpieczeństwa w sieci. SoCalFreeNet wykorzystuje tę stronę do zachęcania użytkowników, by podejmowali działania zapobiegawcze i używali pewnych bardziej zaawansowanych funkcji zabezpieczeń, które udostępniamy.

Warto wiedzieć… odpowiedzialność prawna

Udostępnianie swobodnego dostępu do sieci bezprzewodowej ma pewne implikacje prawne. Ochrona społeczności przed wytoczeniem sprawy sądowej jest ważnym zastosowaniem technologii portalu przechwytującego. Portal ten służy też jako ważne narzędzie edukacyjne uświadamiające użytkowników o bezpieczeństwie i własnej odpowiedzialności w tej kwestii.

Przygotowania

Wiele funkcji opisanych w tym rozdziale wykorzystuje zaporę sieciową open source o nazwie m0n0wall (zapora ta będzie dokładniej omówiona w rozdziale 6.). Zespół m0n0wall tworzą programiści, którzy zebrali się, aby zbudować system w nowym stylu z wygodnym, opartym na WWW mechanizmem konfiguracji. Interfejs graficzny ułatwia konfigurację portalu przechwytującego m0n0wall i wirtualnych sieci prywatnych (VPN — Virtual Private Network) opartych na protokole PPTP (Point-to-Point Tunneling Protocol). PPTP-VPN służy jako zaszyfrowany tunel, którego użytkownicy mogą używać, by chronić się przed podsłuchiwaniem za strony innych użytkowników sieci. Pokażemy, jak wykorzystać obie funkcje do zwiększenia bezpieczeństwa naszej sąsiedzkiej sieci bezprzewodowej.

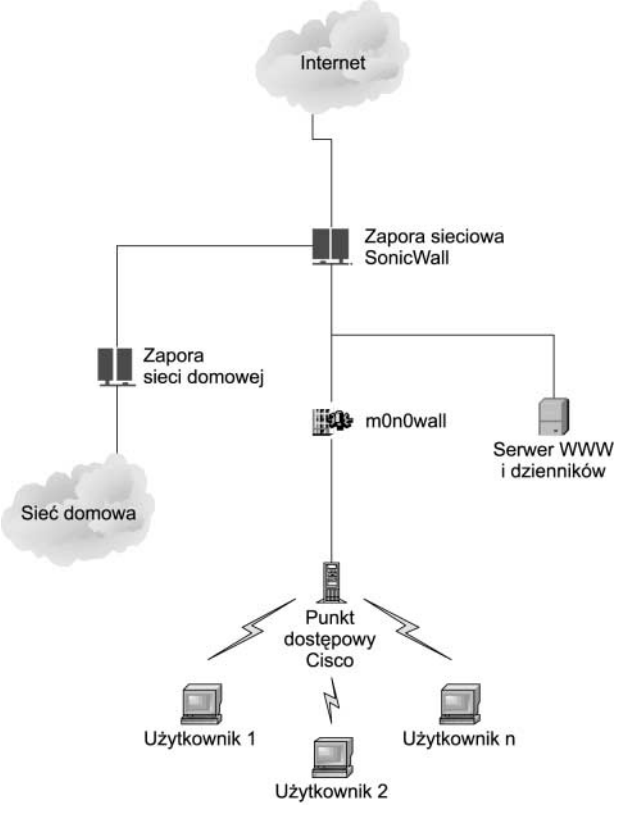
Przygotowania sieci do zainstalowania portalu przechwytującego wymagają trzech kroków:

1. Zaprojektowania i zbudowania sieci z myślą o bezpieczeństwie.
2. Wyboru oprogramowania i sprzętu dla portalu przechwytującego.
3. Instalacji i konfiguracji m0n0wall.

Struktura sieci nastawiona na bezpieczeństwo

Budowanie bezpiecznej sieci bezprzewodowej zaczyna się od bezpiecznej architektury naszej tradycyjnej sieci kablowej. Będziemy kierować się zasadą ograniczania dostępu tylko do niezbędnych usług. Ta zasada w świecie zabezpieczeń jest lepiej znana pod nazwami „default deny" (odmawianie domyślnie) i „least priviledge" (minimalny niezbędny poziom przywilejów). Osiągnięcie tego celu zaczyna się od dobrego projektu ogólnego. Rysunek 3.1 przedstawia układ sieci sąsiedzkiej *node0* zbudowanej przez SoCalFreeNet — przykład jednego z możliwych sposobów, jak skonfigurować prosty, jednowęzłowy hotspot w obszarze mieszkalnym.

Rysunek 3.1.
Przykład bezpiecznej architektury sieci



Taka struktura sieci chroni członków społeczności lokalnej, którzy udostępniają sieć sąsiedzką. Serwer m0n0wall służy jako portal przechwytujący i koncentrator VPN PPTP dla klientów bezprzewodowych. Punkt dostępowy Cisco służy jako proste radio dostępowe dla klientów. Po kupieniu tego konkretnego urządzenia Cisco 1120 zdaliśmy sobie sprawę, że nie pozwala ono podłączyć anteny zewnętrznej. Dobudowaliśmy więc zaraz

do punktu dostępowego zewnętrzne złącze SMC. Zmodyfikowane urządzenie Cisco jest podłączone do dookólnej anteny 15,3 dBi umieszczonej na dachu domu jednego z członków grupy. Dom i antena zostały pominięte na rysunku, lecz widać na nim logiczną infrastrukturę obsługującą ten węzeł SoCalFreeNet. Niektóre węzły SoCalFreeNet są pojedynczymi, niezależnymi punktami dostępowymi w domach użytkowników, podczas gdy inne należą do większego systemu przekazywania o topologii gwiaździstej (o którym wspomnieliśmy w rozdziale 2.). Punkty dostępowe można też instalować w ramach systemu Sputnik (patrz rozdział 8.).

Ostrzeżenie: Zagrożenie dla sprzętu

Wszystkie zewnętrzne połączenia muszą być zabezpieczone przed wpływami atmosferycznymi. Woda może przedostawać się do złączy i powodować z upływem czasu straty sygnału. Istnieje wiele różnych opinii co do poprawnych technik zabezpieczania sprzętu przed wpływami atmosferycznymi. Pod poniższym adresem została opisana jedna z możliwych: *www.qsl.net/n9zia/wireless/sealing_andrews_connectors.html*.

Schemat sieci z rysunku 3.1 przedstawia połączenia tylko na podstawowym poziomie. Istnieje skomplikowany zestaw reguł gwarantujący, że użytkownicy mogą tylko wyjść do Internetu, a zarazem pozwalający administratorom na zarządzanie infrastrukturą. Ochrona środowiska wymaga poprawnej konfiguracji na wszystkich poziomach.

Warto wiedzieć… Utrata gwarancji

Modyfikacja sprzętu przez dodanie złącza zewnętrznej anteny powoduje utratę gwarancji Cisco. Ten konkretnie model punktu dostępowego spełniał nasze wymogi co do mocy wyjściowej, lecz nie pozwalał podłączyć anteny zewnętrznej… tak szczerze mówiąc, chcieliśmy po prostu sprawdzić, czy możemy to zrobić.

Wybór sprzętu i oprogramowania dla portalu przechwytującego

Kolejnym krokiem przygotowań będzie wybór urządzenia i oprogramowania do roli portalu przechwytującego. Podstawowe zadanie portalu polega na dostarczaniu informacji o warunkach świadczenia usług, gdy użytkownik próbuje się połączyć po raz pierwszy. Dostarczenie tej informacji może się odbyć technicznie na kilka sposobów.

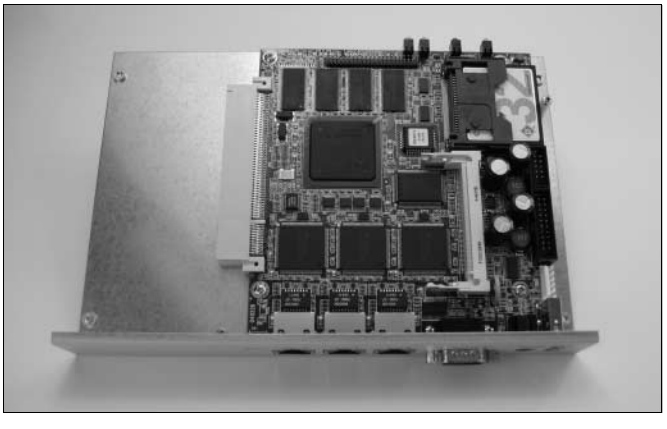
Ponieważ wiele z naszych projektów sieci bezprzewodowych ma ograniczenia mocy zasilania, nasze możliwości wyboru są ograniczone do portali przechwytujących, które mogą pracować w urządzeniach wbudowanych. Są to miniaturowe komputery z zainstalowanymi różnorodnymi „odchudzonymi" wersjami Uniksa. Wiele z tych wersji systemów współpracuje z urządzeniami Soekris (*www.soekris.com*). Oto kilka przykładów konfiguracji tych małych, wygodnych urządzeń:

- **net4501-30**: procesor 133 MHz, 64 MB SDRAM, 3 porty Ethernet, 2 szeregowe, gniazdo CF, 1 gniazdo Mini-PCI, złącze PCI 3,3V.
- **net4521-30**: procesor 133 MHz, 64 MB SDRAM, 3 porty Ethernet, 1 szeregowy, gniazdo CF, 1 gniazdo Mini-PCI, dwa gniazda PC-Card, PoE.
- **net4801-50**: procesor 266 MHz, 128 MB SDRAM, 3 porty Ethernet, 2 szeregowe, złącze USB, gniazdo CF, 44-stykowe złącze IDE, 1 gniazdo Mini-PCI, złącze PCI 3,3V.

Jak widać, urządzenia te mają wiele funkcji małego komputera upakowanych do małego pudełka. Pozwalają nam korzystać z zaawansowanych rozwiązań, wymagając zarazem minimum miejsca i energii. Dla tej konkretnie implementacji wybraliśmy net4801. Większa „moc przerobowa" tego urządzenia pozwala nam poradzić sobie z dodatkowym obciążeniem powodowanym przez usługę PPTP-VPN omówioną w dalszej części rozdziału. Rysunki 3.2 i 3.3 przedstawiają widok urządzenia z zewnątrz i od środka. Więcej informacji o sprzęcie Soekris zawiera rozdział 4.

Rysunek 3.2.
Widoki z zewnątrz

Rysunek 3.3.
Widok wnętrza



Po dokonaniu wyboru sprzętu wybór oprogramowania był już łatwy. Ponieważ zdecydowaliśmy się na komputer jednopłytowy, skupiliśmy się na Pebble (omówionym dokładniej w rozdziale 6.) i m0n0wall. Obie dystrybucje obsługują portale przechwytujące. Pebble zawiera NoCat, podczas gdy autorzy m0n0wall napisali własny portal. Pebble to sympatyczna dystrybucja Debiana zawierająca sterowniki HostAP, serwer DHCP (Dynamic Host Configuration Protocol), serwer DNS, serwer WWW i oczywiście SSH. Autorzy m0n0wall poszli drogą zapory sieciowej i zdecydowali się na obsługę routingu, NAT, DHCP, IPSec/PPTP, buforowania DNS, DynDNS, SNMP, sterowników urządzeń bezprzewodowych i kształtowania ruchu.

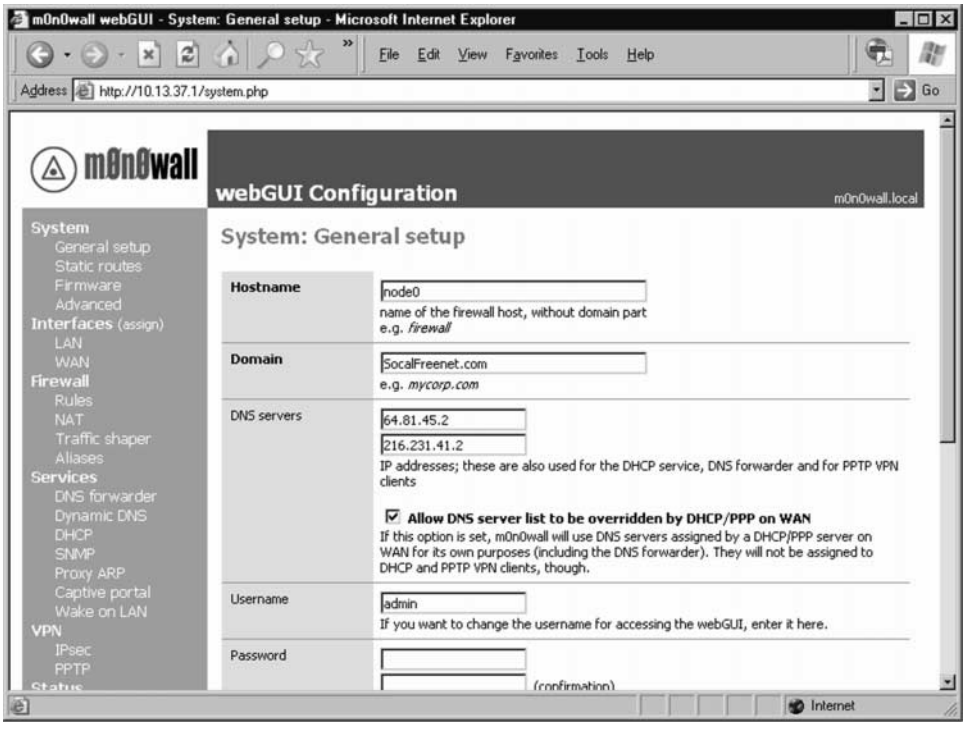
- **NAT** (Network Addres Translation — translacja adresów sieciowych): mechanizm pozwalający zredukować zapotrzebowanie na globalnie unikatowe adresy IP. NAT pozwala organizacjom używającym nieunikatowych globalnie adresów IP łączyć się z Internetem, przekładając te adresy na przestrzeń adresów publicznych. Inaczej Network Address Translator.
- **DHCP** (Dynamic Host Configuration Protocol — protokół dynamicznej konfiguracji hostów): mechanizm dynamicznego przydzielania adresów IP, dzięki czemu adres można wykorzystać ponownie, gdy host go już nie potrzebuje.
- **Buforowanie DNS**: mechanizm przechowujący w pamięci informacje DNS i przyspieszający odpowiedź na powtarzające się zapytania DNS.
- **DynDNS**: pozwala urządzeniu używać zewnętrznego adresu DHCP, a jednocześnie oferować usługi wymagające statycznego adresu IP (serwer WWW, serwer pocztowy itp.). Zwykle stosuje się w połączeniu z dostawcą dynamicznego DNS, aby zapewnić usługę dla użytkowników DHCP.
- **SNMP** (Simple Network Management Protocol — prosty protokół zarządzania sieciami): protokół do zarządzania sieciami, używany niemal wyłącznie w sieciach TCP/IP. SNMP pozwala monitorować i sterować urządzeniami sieciowymi oraz zarządzać konfiguracjami, wydajnością i bezpieczeństwem. SNMP nadaje się też doskonale do gromadzenia statystyk (patrz rozdział 7.).

Kolejną opcją systemu sieciowego dla komputerów jednopłytowych jest Linux Embedded Appliance Firewall (LEAF); patrz *http://leaf.sourceforge.net*. Ta dystrybucja udostępnia usługi warstwy sieciowej i może obsługiwać portal przechwytujący NoCat. Portal trzeba jednakże zainstalować osobno. Obrazy systemu Pebble zawierają NoCat dołączony do systemu i wstępnie zainstalowany.

Wprawdzie Pebble oferuje dużą elastyczność i doskonale nadaje się do scenariuszy wielowęzłowych (zwłaszcza dzięki obsłudze chipsetu Atheros), lecz w mniejszych scenariuszach często wybieramy m0n0wall z uwagi na prostotę i doskonały interfejs użytkownika. m0n0wall mieści duże możliwości na 8-megabajtowej karcie Compact Flash (CF) i zawiera wygodny interfejs zarządzania pokazany na rysunku 3.4.

Po wybraniu sprzętu i oprogramowania pod m0n0wall możemy po prostu zainstalować zaporę sieciową. Witryna m0n0wall (*www.m0n0.ch/wall/installation.php*) zawiera doskonałe instrukcje, jak przeprowadzić ten stosunkowo prosty proces. Ogólnie mówiąc, wystarczy zapisać obraz Soekris na karcie CF, włożyć kartę CF do gniazda i włączyć zasilanie. Interfejs Soekris oparty na WWW ma domyślnie ustawiony adres 192.168.1.1/24 z włączonym DHCP. Aby zacząć zarządzać urządzeniem, należy podłączyć się do portu eth0 i otrzymać adres IP. Jak widać, interfejs jest bardzo intuicyjny. Rozdział 6. zawiera bardziej szczegółowe, krok po kroku, instrukcje instalacji Pebble i m0n0wall.

Po wejściu do konfiguracji musimy podać adresy IP dla portów sieci lokalnej (LAN) i rozległej (WAN). Mając te porty zdefiniowane, będziemy mogli zmieniać wszelkie opcje związane z zaporą sieciową, zgodnie z wymogami środowiska. Po pełnym skonfigurowaniu i przetestowaniu środowiska pora przejść do portalu przechwytującego.



Rysunek 3.4. *Interfejs zarządzania m0n0wall*

Uwaga… Różnorodne środowiska

Przykład przedstawiony w tym rozdziale używa odrębnego punktu dostępowego, lecz wielu użytkowników woli wbudować bezprzewodową kartę sieciową bezpośrednio do systemu m0n0wall. Sieć można skonfigurować na wiele sposobów. Ważne tylko, by wszystko było uruchomione i przetestowane przed przejściem do następnego etapu. W tym rozdziale opisujemy konfigurację m0n0wall z zewnętrznym punktem dostępowym (Cisco 1120). W rozdziale 6. opiszemy konfigurację m0n0wall z bezprzewodową kartą sieciową w Soekris.

Instalacja portalu przechwytującego

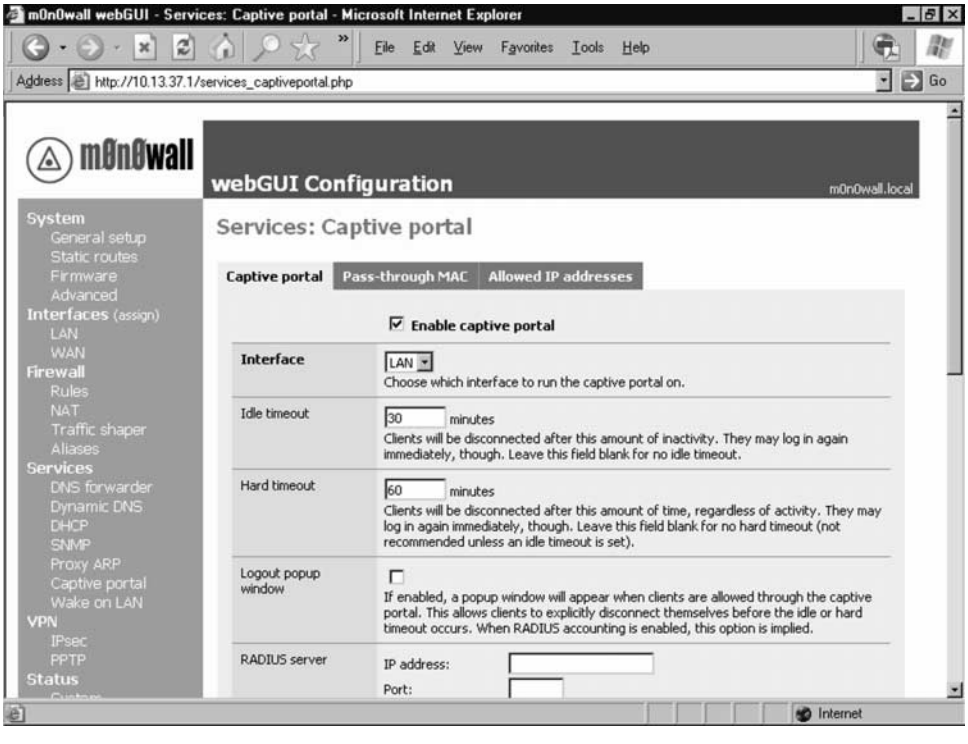
Po zainstalowaniu i uruchomieniu m0n0wall możemy zacząć przechwytywać użytkowników do portalu. Dzięki interfejsowi graficznemu m0n0wall jest to proces szybki i łatwy. Kliknij po prostu opcję *Captive Portal* pod *Services*/*Captive Portal*, a następnie:

1. Zaznacz opcję *Enable captive portal*.
2. Kliknij przycisk *Browse…* pod *Portal page contents* i załaduj HTML przeznaczony dla portalu. Formułowanie umowy o warunkach świadczenia usług opiszemy w następnym podpunkcie.

Uwaga... Serwery Radius

m0n0wall obsługuje również uwierzytelnianie Radius. Wystarczy dodać nasz serwer w sekcji *Radius Server*.

Rysunek 3.5 przedstawia zakładkę Captive Portal. Zakładki Pass-through MAC i Allowed IP Addresses omówimy w dalszej części rozdziału.



Rysunek 3.5. *Zakładka Captive Portal*

Pisanie własnych warunków świadczenia usług

Portal przechwytujący jest już na chodzie, więc następnym krokiem będzie napisanie umowy o warunkach świadczenia usług. Umowa ta instruuje użytkownika o zakresie jego odpowiedzialności przy korzystaniu z sieci i chroni operatorów przed odpowiedzialnością prawną. W tym lubującym się w sprawach sądowych świecie nawet dawanie za darmo bezprzewodowego dostępu niesie ze sobą pewne ryzyko. Umowa na stronie portalu przechwytującego uświadamia użytkowników i pozwala operatorom sieci skupiać się bardziej na budowaniu lepszych sieci bezprzewodowych.

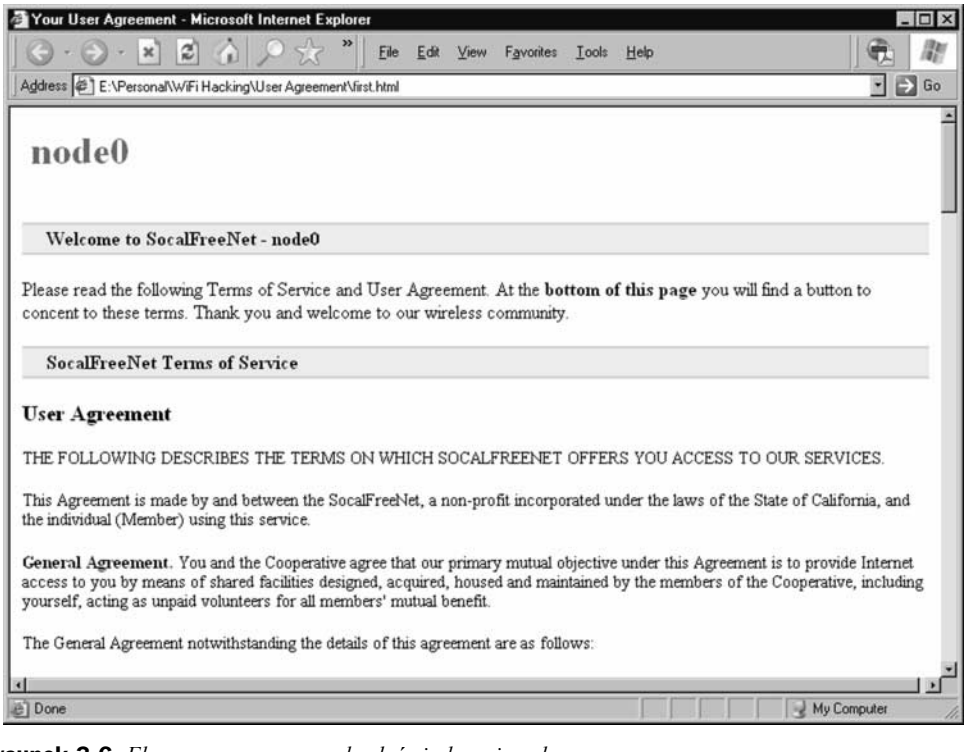
W SoCalFreeNet używamy umowy, która mówi mniej więcej:

„Masz tu darmowy dostęp bezprzewodowy. Nie nadużywaj go, bo ci go zabierzemy. Przestrzegaj prawa i bądź miły dla innych użytkowników”.

Dalej umowa zawiera kilka mocnych stwierdzeń zwalniających SoCalFreeNet i właściciela sprzętu od odpowiedzialności, jeśli użytkownik zrobi coś głupiego, np. poliże punkt dostępowy podłączony do zasilania. Wprawdzie zdajemy sobie sprawę, że niektóre przepisy prawne mogą być dziwne, lecz nikt nie chce pójść siedzieć za zachowanie głupiego użytkownika. Niektórzy użytkownicy po prostu podejmują nieprzemyślane decyzje, a nie chcemy, by społeczność sieciowa i operatorzy ucierpieli na tym. Zapobieganie błędom jest dobrym podejściem, więc SoCalFreeNet szczyci się tym, że zabezpiecza społeczność sieci bezprzewodowych tak, jak to tylko możliwe. Budowanie bezpiecznych systemów zwiększa przyjemność wszystkich użytkowników ze spacerów po „bezprzewodowym parku".

Sformułowanie naszej umowy z użytkownikami kosztowało mnóstwo wysiłku. Poprawne skonstruowanie takiego dokumentu wymaga pomocy ekspertów (prawników). Niestety, autorzy nie szczycą się znajomością prawa na poziomie eksperckim. Przy pisaniu umowy o warunkach świadczenia usług radzimy skontaktować się z dobrym prawnikiem zajmującym się technologią. Jeśli wynajęcie prawnika wykracza poza budżet projektu, radzimy skontaktować się z lokalną grupą użytkowników sieci bezprzewodowych lub z nami (*www.socalfreenet.org*) i poprosić o pomoc. Łącząc zasoby, możemy osiągnąć masę krytyczną i wykonać potrzebne zadania.

Rysunek 3.6 przedstawia ekran umowy, którzy użytkownicy dostają przy pierwszej próbie otwarcia internetowej strony WWW. Po wyrażeniu zgody na warunki świadczenia użytkownik zostaje automatycznie połączony ponownie ze stroną WWW, której zażądał.



Rysunek 3.6. *Ekran umowy o warunkach świadczenia usług*

Warto wiedzieć… Jak napisać poprawną umowę?

Autorzy nie uważają się za ekspertów w dziedzinie prawa. Napisanie poprawnej umowy o współpracy z użytkownikiem wymaga ekspertyzy w dziedzinie prawa związanego z technologią. Wydawca i autorzy zalecają skorzystanie z odpowiedniej pomocy prawnej przy tworzeniu dokumentów prawnych związanych z siecią.

Grafika w portalu przechwytującym

Mając w pełni funkcjonujący portal, możemy wyświetlić u użytkownika stronę WWW z naszą umową o warunkach świadczenia usług. Zazwyczaj tworzymy stronę z umową offline, a następnie ładujemy ją do urządzenia m0n0wall. Jednakże ładowanie strony zawierającej tylko kod HTML do m0n0wall ogranicza nasze możliwości wykorzystania grafiki. Grafika we wspomnianym wcześniej przykładzie wykorzystuje jedynie proste różnice w kolorach. Wyjście poza to ograniczenie wymaga drobnej zmiany w konfiguracji i w naszej stronie portalu.

Wprawdzie strona portalu nadaje się do wyświetlania tekstu, lecz m0n0wall nie pozwala ładować lokalnych obrazów (za mało miejsca na karcie CF). Strony WWW nabierają życia dzięki grafice. Logo grupy SoCalFreeNet jest miłym dodatkiem do naszej strony z umową. Dodanie obrazów wymaga kilku prostych kroków:

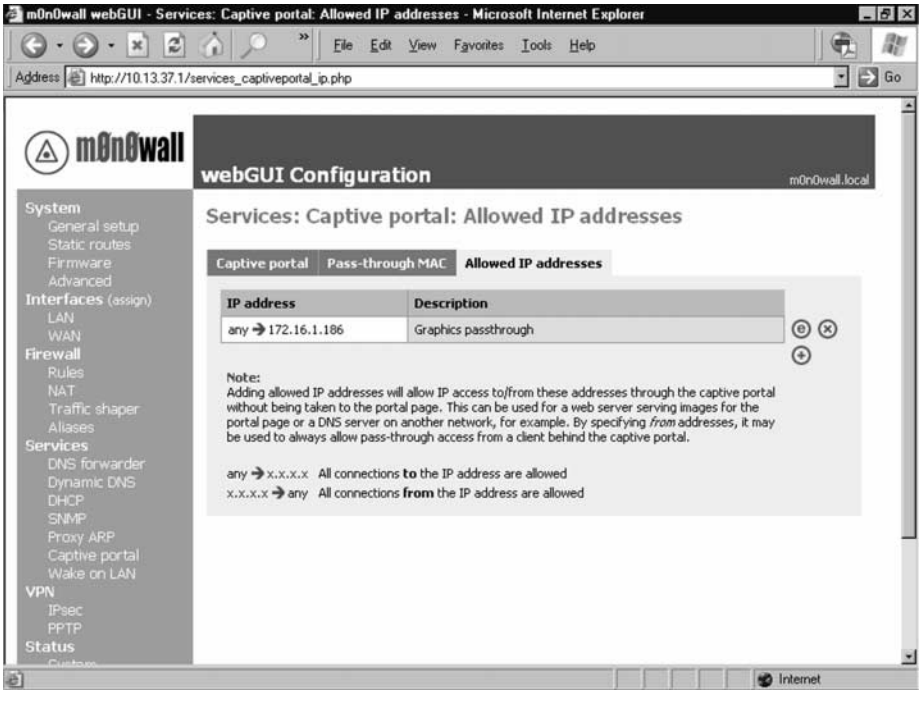
1. Wybierz serwer WWW, który będzie mieścił grafikę. U nas jest to serwer WWW i dzienników zdarzeń mieszczący się po zewnętrznej stronie m0n0wall (WAN).
2. Gdy obrazy są już dostępne w sieci, dodaj do strony portalu znacznik <IMG> z pełnym adresem obrazu. Zamiast `<IMG SRC="/images/logo.gif">` używamy `<IMG SRC="http:/172.16.1.186/images/logo.gif">`. Mówi to przeglądarce użytkownika, by pobrać obraz dla strony portalu z innego serwera. W naszym przypadku jest to serwer WWW w naszej sieci.

Uwaga… Problem z DNS-em

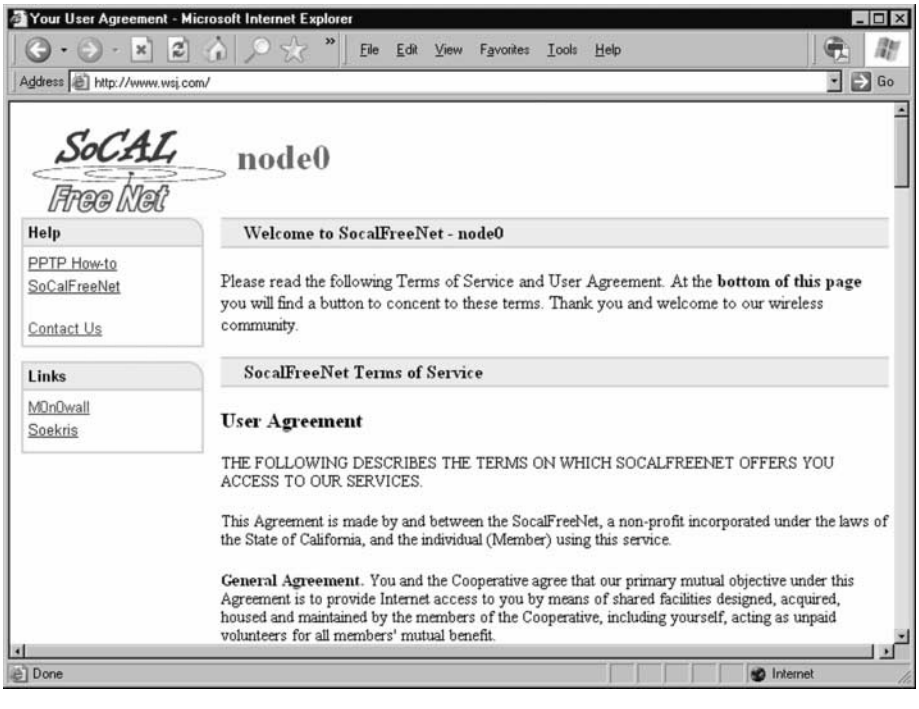
Odkryliśmy, że portal przechwytujący nie przepuszcza DNS, zanim użytkownik nie zaakceptuje umowy. Aby sobie z tym poradzić, podajemy bezpośrednio adres IP zamiast nazwy hosta. Jeśli nie znasz adresu IP serwera, którego chcesz użyć, sprawdź go poleceniem `ping`.

3. Skonfiguruj portal przechwytujący m0n0wal tak, by dawał użytkownikom dostęp do adresu IP serwera mieszczącego obrazy. W tym celu kliknij *Services*/*Captive Portal* w lewym menu m0n0wall, następnie wybierz zakładkę *Allowed IP addresses* nad pozycjami do konfiguracji. Na koniec kliknij ikonę plusa po prawej stronie okna (patrz rysunek 3.7); adresem IP serwera jest 172.16.1.186. Wskazując adresy innych serwerów, upewnij się, czy administrator WWW zezwala na odwołania do swojej witryny. Jest to uznawane za dobrą etykietę w Sieci.

Rysunek 3.8 przedstawia stronę umowy wzbogaconą o logo SoCalFreeNet. Możemy pójść jeszcze dalej, używając np. ramek. Otwarcie umysłu na innowacje często daje ciekawe wyniki. Członkowie SoCalFreeNet wciąż starają się twórczo zwiększać przyjemność i bezpieczeństwo korzystania z sieci przez lokalne społeczności.



Rysunek 3.7. *Ekran Allowed IP addresses*



Rysunek 3.8. *Strona umowy z logo SoCalFreeNet*

Warto wiedzieć... Zgoda administratora

Przed umieszczeniem w portalu przechwytującym odwołania bezpośrednio do grafiki mieszczącej się w serwerze WWW należy uzyskać na to zgodę administratora WWW tego serwera.

Budowanie VPN z PPTP

Realia i wyzwania otwartych sieci bezprzewodowych prowadzą do powstawania wielu interesujących rozwiązań. Pojawienie się szyfrowania WEP (Wired Equivalent Privacy) dało wczesną formę ochrony. Solidność tego rozwiązania kruszyła się w miarę, jak analitycy zabezpieczeń znajdowali punkty podatne na atak, a krakerzy zaczęli łamać szyfry. Słabości tego mechanizmu szyfrowania doprowadziły do powstania WPA (Wi-Fi Protected Access), a później 802.1x. Obecnie mechanizm WPA też trafił pod lupę, ponieważ analitycy zaczęli znajdować w nim problemy. Niektórzy przypuszczają, że problemy te doprowadzą do upadku WPA. Ponieważ WPA stoi na niepewnym gruncie, postanowiliśmy szukać innych rozwiązań. Wprawdzie technologie 802.1x są obiecujące, lecz wymagają zainstalowania znaczącej infrastruktury. Co więcej, instalowanie tej technologii w starszych systemach operacyjnych bywa problematyczne.

Opracowanie zabezpieczeń wymaga cierpliwości i pomysłowości. Wielu kreatywnych użytkowników przechodzi na technologię wirtualnych sieci prywatnych (VPN), dającą wyższy poziom ochrony. Ewolucja w stronę technologii VPN pomaga użytkownikom cieszyć się łącznością bezprzewodową. Dla naszej bezprzewodowej VPN wybraliśmy PPTP. Wprawdzie z protokołem PPTP są pewne problemy, lecz wiele luk w bezpieczeństwie już zostało naprawionych.

Jeśli chodzi o problem ataków ze zgadywaniem haseł, używamy długich i skomplikowanych, aby znacznie zmniejszyć ryzyko. Chociaż PPTP nadal prezentuje pewne zagrożenia, uważamy, że zaoferowane rozwiązanie jest znacznym postępem w stosunku do przesyłania informacji w sieci sąsiedzkiej otwartym tekstem. To oczywiste, że w każdym projekcie bezprzewodowym muszą być stosowane narzędzia do szyfrowania wygodne dla użytkowników. W wielu naszych węzłach szyfrowanie nie jest w ogóle stosowane, ponieważ użytkownicy wolą podejście „otwarte". Takie rozwiązanie jest wprawdzie mniej bezpieczne, lecz łatwiej je wdrożyć i obsługiwać. Podobnie jak we wszystkich decyzjach związanych z bezpieczeństwem, musimy sami ocenić sytuację i znaleźć kompromis pomiędzy bezpieczeństwem a użytecznością.

Uwaga... Wczesne problemy z PPTP

W roku 1998 słynni analitycy zabezpieczeń, Schneier i Mudge, opublikowali przełomowy dokument (*www.schneier.com/pptp.html*) o słabościach implementacji PPTP Microsoftu. Microsoft naprawił wiele z opisanych problemów w następnych wersjach (poprawki wymagają aktualizacji DUN 1.3), jednakże zagrożenie odgadnięcia hasła nadal jest aktualne. Stosowanie złożonych haseł, dłuższych niż 14 znaków, pozwala poważnie zmniejszyć zagrożenie.

Przygotowania

Gdy nabierzemy więcej pewności, że takiego rozwiązania VPN chcemy, możemy przejść do implementacji. Wymogi wstępne są takie same jak w przypadku opisanego wcześniej portalu przechwytującego. Musimy zainstalować oprogramowanie m0n0wall, skonfigurować porty i przetestować łączność. Pomoże to zapewnić, że będziemy koncentrować się na konfiguracji VPN zamiast na innych problemach z konfiguracją.

Ostrzeżenie: Zagrożenie dla sprzętu

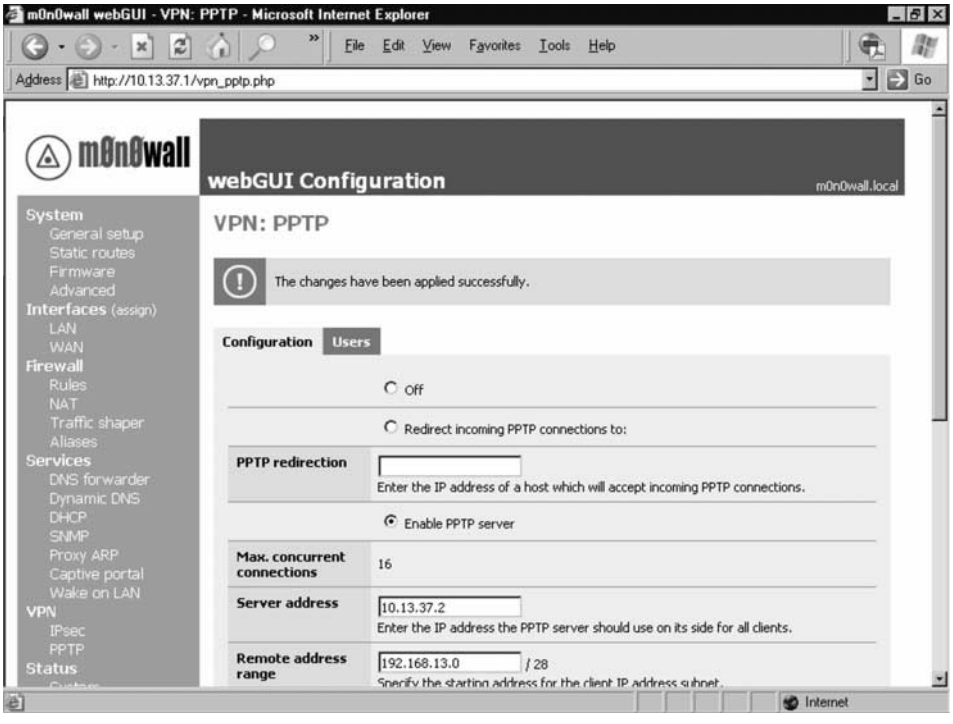
Wprawdzie tunel PPTP daje ochronę użytkownikom na tyle mądrym, by z niego korzystać, lecz nasza sieć nadal pozwala łączyć się otwartym tekstem. Ponieważ wielu użytkowników sieci bezprzewodowej nie ma wystarczającej wiedzy o bezpieczeństwie, by rozumieć zagrożenia biorące się z komunikacji otwartym tekstem, musimy aktywnie szkolić użytkowników i egzekwować używanie zabezpieczeń.

Instalacja VPN

Konfiguracja VPN składa się z dwóch głównych etapów. Pierwszy koncentruje się na konfiguracji urządzenia m0n0wall, natomiast drugi na konfiguracji klientów. Na szczęście klient PPTP jest wbudowany w wiele wersji Windows, w tym Windows 95, NT, 2000, XP i nowsze.

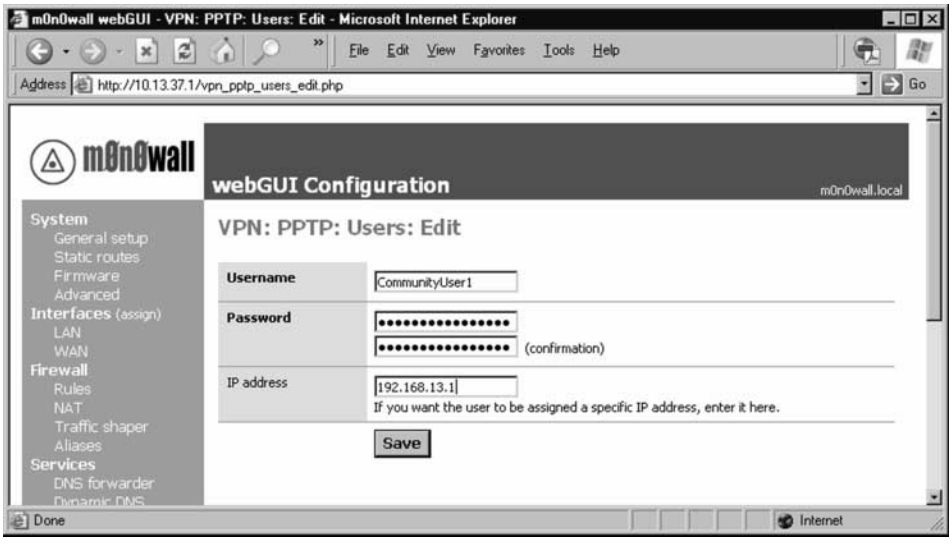
Po stronie serwera m0n0wall w wersji 1.1 obsługuje tunele IPSec i PPTP. Skonfigurowanie PPTP z użyciem interfejsu WWW m0n0wall jest proste:

1. Wybierz opcję *VPN*/*PPTP* z paska menu po lewej stronie. Zwróć uwagę na zakładki Configuration i Users na górze strony. Podczas konfiguracji będziemy używać obu.
2. Na zakładce Configuration zaznacz pole wyboru *Enable PPTP server*.
3. W polu *Server address* wpisz adres serwera PPTP. Jest to adres systemu m0n0wall, którego klienty będą używać po podłączeniu swoich tuneli VPN. W naszym przykładzie serwer ma adres 10.13.37.2. Jest to po prostu IP bezpośrednio ponad adresem bramy domyślnej po stronie LAN. Pamiętaj, by podać adres spoza zakresu DHCP zdefiniowanego w menu *DHCP*/*Services*.
4. Wpisz adres sieci w polu *Remote address range*. Jeśli nie masz doświadczenia z podsieciami i nie wiesz, jak wybrać odpowiedni adres sieci /28, sugeruję wpisać zero w ostatnim oktecie. W naszym przykładzie został wybrany zakres 192.168.13.0.
5. Możesz opcjonalnie włączyć wymuszanie szyfrowania 128-bitowego. Zalecamy to, o ile nie zdarzy się jakiś konflikt z użytkownikiem.
6. Kliknij *Save* na dole strony. Na górze strony pojawi się komunikat „The changes have been applied successfully” (patrz rysunek 3.9.). Mamy teraz działający serwer PPTP w systemie m0n0wall; wystarczy jeszcze dodać konta użytkowników.



Rysunek 3.9. *Konfiguracja VPN: PPTP*

7. Pozostając w menu *VPN*/*PPTP*, kliknij zakładkę *Users* w górnej części ekranu.
8. Kliknij ikonę w kształcie plusa po prawej stronie ekranu. Pojawi się ekran dodawania nowego użytkownika (patrz rysunek 3.10).



Rysunek 3.10. *Ekran edycji użytkownika*

9. W polu *Username* wpisz pożądaną nazwę logowania. W naszym przykładzie użyliśmy nazwy `CommunityUser1`.

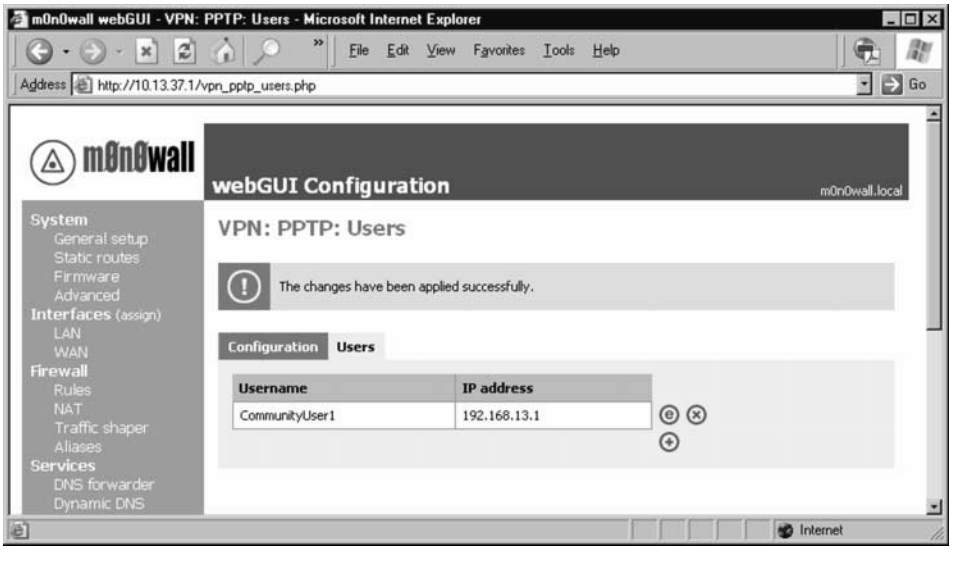
10. W polu *Password* wpisz dwukrotnie długie i skomplikowane hasło. Pod pojęciem „skomplikowane" rozumiemy wykorzystanie cyfr, liter wielkich i małych i znaków specjalnych (np. `&`). Jedna z wygodnych metod mnemotechnicznych polega na użyciu pierwszych liter kolejnych słów piosenki. Na przykład, (nie używaj tego przykładu w swoim środowisku!) „**M**ary **h**ad **a** **l**ittle **l**amb, **A** **l**ittle **l**amb, **A**nd **i**ts **f**leece **w**as **w**hite **a**s **s**now" da hasło `2MhallAllAifwwas2`. Dodaliśmy cyfrę 2 na początek i na koniec hasła, by zwiększyć złożoność.

Warto wiedzieć… hasła w systemie m0n0wall

W chwili publikacji tej książki m0n0wall nie pozwalał na używanie znaków specjalnych (`~ ! @ # $ % ^ & *`…). Jeśli nowsza wersja m0n0wall pozwala na to, zdecydowanie zalecamy korzystanie ze znaków specjalnych. Zwiększa to wykładniczo trudność złamania hasła.

11. W polu *IP address* wpisz IP, który ten użytkownik zawsze otrzyma. Zdecydowanie zalecamy skorzystać z tej opcji, ponieważ pozwala bezpośrednio skojarzyć wpisy w dziennikach PPTP z konkretnymi użytkownikami. Adres IP musi należeć do zakresu, który zdefiniowaliśmy w *Remote address range* na pierwszej zakładce (192.168.13.0/28). W naszym przykładzie wpisaliśmy pierwszy IP z zakresu (192.168.13.1).

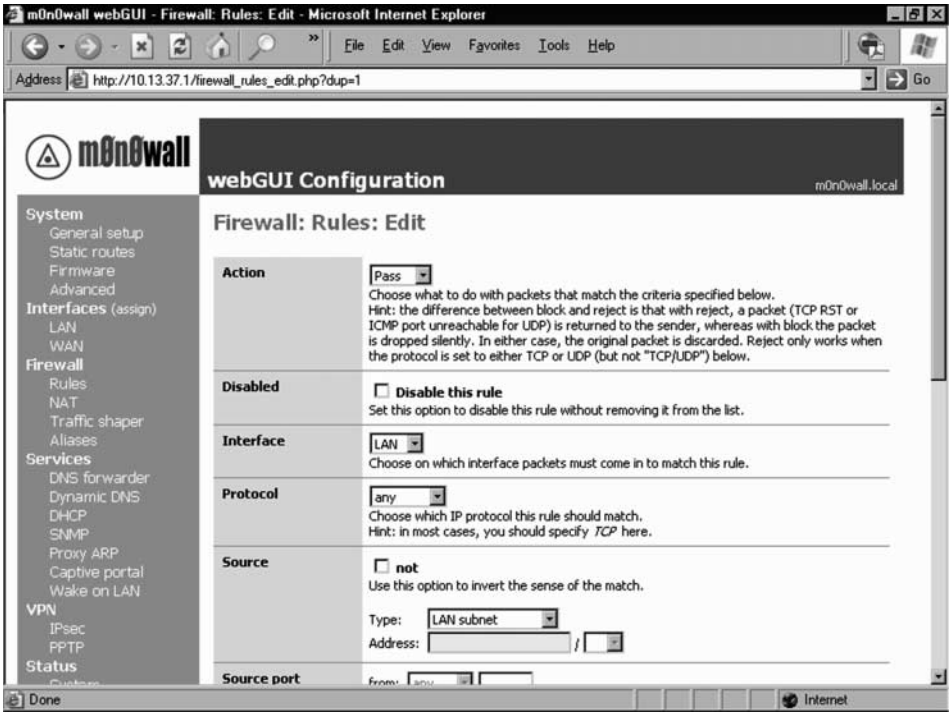
12. Aby zmiany zaczęły obowiązywać, kliknij *Apply changes* na górze okna. Uwaga: ta czynność zerwie połączenia wszystkich użytkowników połączonych obecnie przez VPN PPTP. Ponieważ konfigurujemy VPN po raz pierwszy, nie powinno to sprawić problemu. Ponownie na górze ekranu pojawi się komunikat, że zmiany zostały wprowadzone. Rysunek 13.11 przedstawia ostateczny efekt.



Rysunek 3.11. *Ostateczny rezultat*

13. Ostatnim krokiem wymaganym w konfiguracji m0n0wall jest utworzenie reguły zapory sieciowej pozwalającej na przesyłanie ruchu PPTP. Kliknij *Firewall*/*Rules* po lewej stronie. Pojawi się menu konfiguracyjne z jedną regułą zdefiniowaną już dla interfejsu LAN.

14. Ponownie kliknij ikonę plusa po prawej stronie ekranu konfiguracji. Jest tu jeszcze kilka innych ikon, w tym e dla edycji, x do usuwania oraz strzałki do przenoszenia reguł w górę i w dół. m0n0wall przetwarza reguły zapory sieciowej z góry na dół. Rysunek 3.12 przedstawia ekran nowej reguły.



Rysunek 3.12. *Ekran edycji nowej reguły zapory sieciowej*

15. Pojawi się ekran nowej reguły zapory sieciowej. Na tym ekranie zostaw w polu *Action* czynność *Pass* (przepuść).

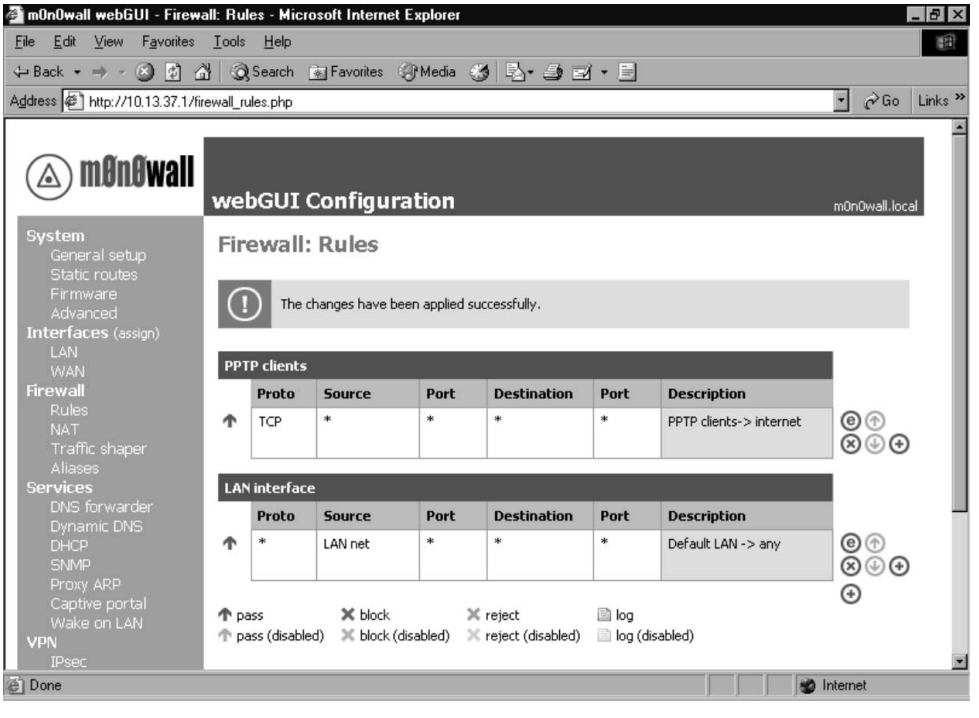
16. Zaznacz opcję *PPTP* w polu listy rozwijanej *Interface*.

17. W polu *Protocol* wybierz opcję *TCP/UDP*.

18. Dla reszty pól możesz zostawić ustawienia domyślne lub zmodyfikować dla konkretnego środowiska. W polu *Description* wpisz opis reguły. My używamy opisu „PPTP clients -> internet", aby przypominać, jaką rolę pełni ta reguła.

19. Kliknij przycisk *Save* na dole ekranu. Spowoduje to powrót do menu *Firewall*/*Rules*, w którym pojawi się nowa reguła w sekcji PPTP clients.

20. Ponownie trzeba będzie kliknąć przycisk *Apply Changes*, aby nowa reguła zaczęła obowiązywać. Pojawi się komunikat potwierdzający, że zmiany zostały wprowadzone. Rysunek 3.13 przedstawia ostateczny rezultat.



Rysunek 3.13. *Reguły zapory sieciowej — ostateczny wynik*

Mamy już w pełni skonfigurowany serwer, możemy przejść do konfigurowania klienta PPTP w systemie użytkownika.

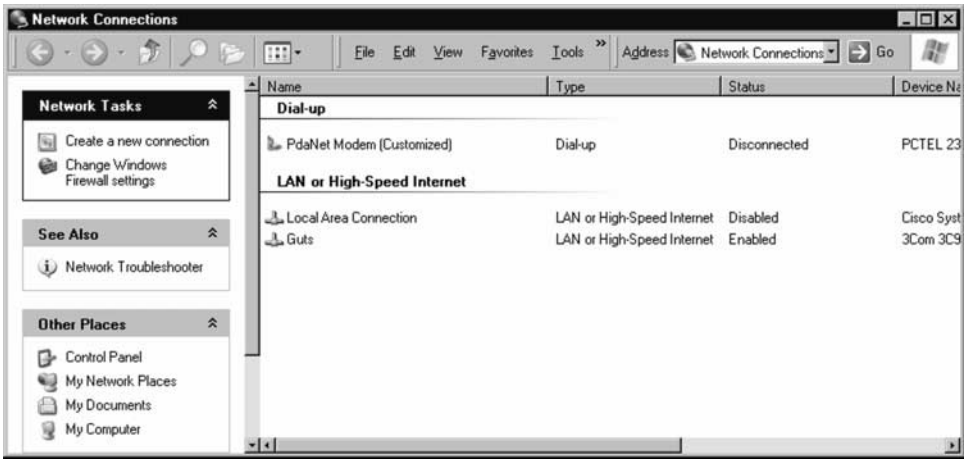
Uwaga... Bezpieczeństwo haseł

Stosowanie słabych haseł może spowodować narażenie bezpieczeństwa naszej VPN. Użytkownicy przeważnie nie lubią złożonych haseł. Warto pomyśleć nad wyborem haseł, które użytkownik może zapamiętać, a które jednocześnie będą miały sens z punktu widzenia bezpieczeństwa.

Konfiguracja użytkowników sieci

Po stronie użytkownika wykorzystamy klienta PPTP już wbudowanego w system Windows. Zademonstrujemy konfigurację na przykładzie Windows XP. Metoda konfiguracji jest podobna we wszystkich wersjach, zaczynając od Windows 95 aż do najnowszej.

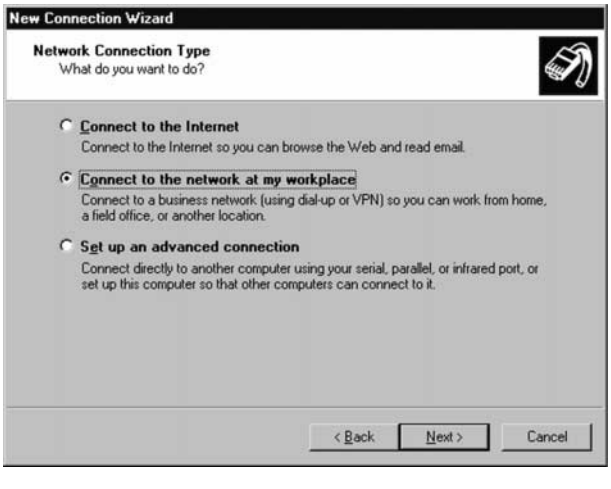
1. Kliknij *Start*/*Network Connections*. Jak widać na rysunku 3.14, pojawi się okno Network Connections z wyświetlonymi aktualnymi połączeniami sieciowymi.
2. Kliknij łącze *Create a new connection* w lewym górnym rogu okna. Jak widać na rysunku 3.15, pojawi się kreator *New Connection Wizard*.
3. Kliknij przycisk *Next*. Pojawi się okno dialogowe *New Connection Type*. Wybierz opcję *Connect to network at my workplace*, jak na rysunku 3.16.



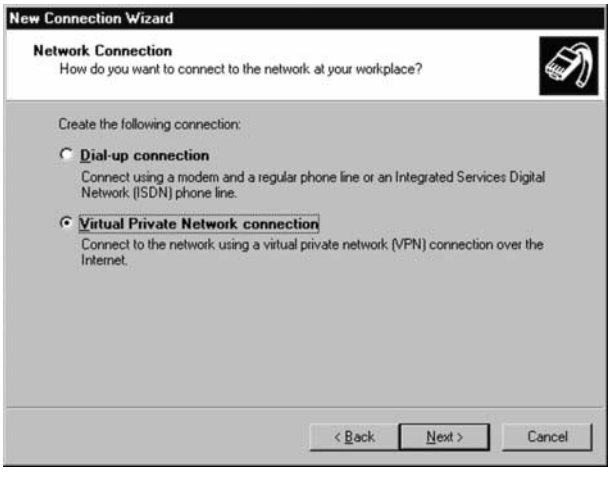
Rysunek 3.14. *Ekran Network Connections*

Rysunek 3.15. *Ekran powitalny kreatora New Connection Wizard*

Rysunek 3.16. *Wybór opcji Connect to network at my workplace*

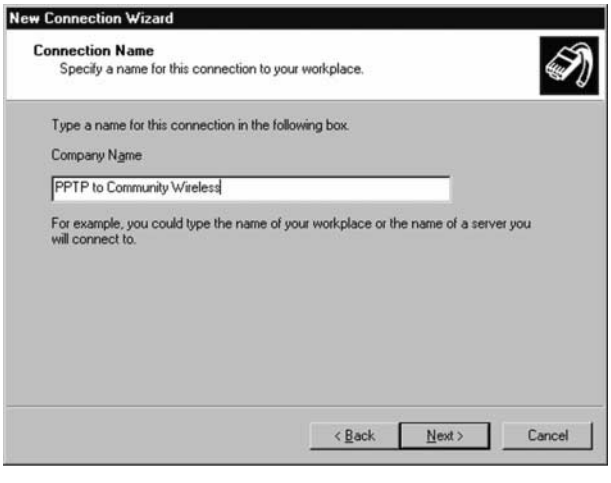


4. Kliknięcie przycisku *Next* spowoduje przejście do ekranu *Network Connection*. Wybierz opcję *Virtual Private Network*, jak na rysunku 3.17.



Rysunek 3.17. *Wybór opcji Virtual Private Network*

5. Kliknięcie przycisku *Next* spowoduje wyświetlenie zapytania *Company Name*. Tu wpisz opis swojego połączenia PPTP. Jak widać na rysunku 3.18, wpisaliśmy PPTP to Community Wireless.

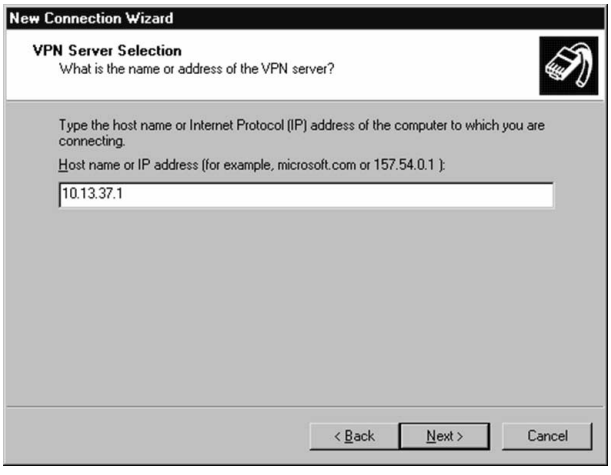


Rysunek 3.18. *Opis połączenia PPTP*

6. Kliknięcie przycisku *Next* **może** otworzyć okno dialogowe Automatic Dial. Jeśli to nastąpi, wybierz opcję *Do not dial the initial connection*.

7. Kliknięcie przycisku *Next* spowoduje przejście do okna dialogowego *Server Name or Address*. Jak widać na rysunku 3.19, wpisaliśmy adres IP naszego systemu m0n0wall. Jest to adres interfejsu internetowego w m0n0wall, w naszym przykładzie 10.13.37.1. Adres ten można znaleźć w systemie m0n0wall, klikając pozycję menu *Interfaces/LAN* w oknie WWW konfiguracji m0n0wall.

Rysunek 3.19.
Adres IP systemu m0n0wall



8. Kliknięcie przycisku *Next* spowoduje przejście do okna dialogowego *Create this connection.for*:. Jeśli chcesz, aby wszyscy użytkownicy używali tego połączenia, zaznacz *Anyone's use*; w przeciwnym razie wybierz opcję *My use only*. Pozostaje to najczęściej w gestii członka społeczności sieciowej używającego połączenia PPTP.
9. Kliknięcie przycisku *Next* otworzy okno *Completing the New Connection Wizard*. Tu można opcjonalnie dodać skrót na pulpicie.
10. Kliknij *Finish*, aby otworzyć okno *PPTP authentication* (patrz rysunek 3.20). Aby przetestować ustawienia, wpisz nazwę użytkownika, którą wcześniej zdefiniowaliśmy w konfiguracji m0n0wall.

Rysunek 3.20.
Okno PPTP Authentication

11. Kliknięcie przycisku *Connect* powoduje otwarcie okienka *Connecting*, jak na rysunku 3.21.
12. Jeśli wszystko zostało skonfigurowane poprawnie, pojawi się okno komunikatu o rejestrowaniu w sieci (patrz rysunek 3.22). Moje gratulacje, VPN PPTP działa!

Rysunek 3.21.
Okno Connecting

Rysunek 3.22.
Rejestrowanie komputera w sieci

Edukacja użytkowników sieci bezprzewodowej

Dobre bezpieczeństwo zaczyna się od użytkowników. Użytkownicy lokalni muszą podjąć dodatkowe kroki, na przykład stosować mocne hasła, aby którykolwiek z naszych opcjonalnych mechanizmów zabezpieczeń mógł działać. Wszystkie mechanizmy, które omawialiśmy do tej pory, koncentrują się na technologii. W świecie komputerów w grę wchodzi dodatkowa umiejętność zwana *inżynierią społeczną*. Definiujemy inżynierię społeczną jako sztukę wpływania niekonwencjonalnymi środkami na działania innych ludzi. Wprawdzie inżynieria społeczna często jest kojarzona ze złymi hakerami (tzw. *black hats* — czarne kapelusze), nie wszystkie działania w tej dziedzinie powodują szkody. Wiele z tych samych umiejętności, które stosują „czarne kapelusze", może posłużyć do osiągnięcia pozytywnych wyników. Idea całej niniejszej książki odzwierciedla tę zasadę.

Media nagłaśniające przypadki złych działań hakerów spowodowały, że pojęcie „hacking" nabrało pejoratywnego znaczenia. Określenie „haker" początkowo oznaczało kogoś, kto robi niekonwencjonalne rzeczy, aby tworzyć nowe rozwiązania (stąd tytuł naszej książki, *Wireless Hacking*). My też szukamy metod wykraczania poza dotychczasowe możliwości technologii i nowych sposobów tworzenia bezpiecznych środowisk społecznych sieci bezprzewodowych.

Słowo „społeczność" implikuje kontakty społeczne. Kontakty te są dla nas jedną z podstawowych metod dzielenia się pomysłami i, ogólnie, cieszenia się życiem społecznym. Jest to kolejna droga, którą możemy propagować bezpieczeństwo i edukować użytkowników w kwestii tego, jak mogą bezpiecznie cieszyć się tworzonym przez nas „bezprzewodowym parkiem miejskim".

Przygotowania

Dobra dokumentacja pomaga użytkownikom szybko uczyć się konfiguracji i zarządzania swoim sprzętem. Ponieważ grupa wolontariuszy jest ograniczona, sieć sąsiedzka opiera się na przyjaznych użytkownikach, którzy poświęcają swój czas na pomaganie innym.

Wiele z tej pomocy ma postać drukowaną. Podobnie jak niniejsza książka, dokumentacja projektu może pomóc w tworzeniu silnej społeczności użytkowników i zapewnianiu bezpieczeństwa.

Początek i koniec

Solidne bezpieczeństwo bierze się z wiedzy użytkowników. Budowanie bazy tej wiedzy wymaga cierpliwości i przyjaznego podejścia. Gdy użytkownik zwraca się do nas z pytaniem, staramy się przemyśleć problem z jego perspektywy i wykorzystać informacje zwracane przez użytkownika w projekcie sieci. Na przykład wybraliśmy PPTP z uwagi na łatwość implementacji po stronie użytkowników.

W miarę jak użytkownicy zaczną rozumieć technologię bezprzewodową i dowiadywać się o różnych nowych elementach jej bezpieczeństwa, ich ciekawość zacznie rosnąć. Dzięki dobrze opracowanej dokumentacji użytkownik będzie miał gdzie uczyć się i zdobywać nowe wiadomości. SoCalFreeNet wykorzystuje strony portalu przechwytującego jako punkt startowy dla użytkowników, którzy chcą dowiedzieć się czegoś więcej o bezpieczeństwie i swojej roli.

Przy łączeniu się z siecią lokalnej społeczności użytkownik powinien podjąć kilka prostych środków ostrożności:

- Zawsze używaj osobistej zapory sieciowej. Zapory te często znajdują się w komputerach użytkowników. W system Windows XP jest wbudowana niedawno udoskonalona zapora sieciowa.
- Używaj mocnych haseł, aby utrudnić ataki na nie.
- Nawet dobre hasła czasem zawodzą. Wiele opartych na WWW programów pocztowych przesyła hasła przez sieć otwartym tekstem. W naszej sieci bezprzewodowej oznacza to, że inni użytkownicy mogą widzieć hasło do poczty innej osoby. Użytkownik powinien się upewnić, czy przy korzystaniu z witryn wymagających poufnych informacji w prawym dolnym rogu okna przeglądarki znajduje się rysunek kłódki. Jego obecność oznacza, że witryna używa SSL.
- Wierz lub nie, nawet ta kłódeczka nie gwarantuje pełnej ochrony. Niektóre ataki wykorzystują urządzenie pośredniczące (man-in-the-middle) i pozwalają podglądać zaszyfrowany ruch. Z tego powodu zachęcamy użytkowników, by używali tunelu PPTP i jednocześnie sprawdzali obecność kłódki na ekranie.
- Do bardzo poufnych czynności warto rozważyć skorzystanie z bardziej konwencjonalnych metod.
- Systemy powinny być regularnie łatane. Użytkownicy mogą domagać się pomocy w wyjaśnieniu, jak sprawdzać i instalować poprawki.
- Należy uczyć dzieci, jak korzystać z Internetu i zachować w nim bezpieczeństwo.
- Jeśli masz podejrzenia lub dziwne uczucie przy przeglądaniu witryny WWW, zatrzymaj się i pomyśl o bezpieczeństwie. Posłuchaj swojego instynktu. Internet

odzwierciedla życie na wiele sposobów, a świat wirtualny ma swoje getta i rejony, które należy omijać. Unikaj sklepów o złej reputacji lub witrynach o marnej jakości. Często traktują one bezpieczeństwo jako mało ważne.

Wprawdzie architekci SoCalFreeNet nieustannie szukają i oferują alternatywne metody zabezpieczeń, prawdziwe bezpieczeństwo spoczywa w rękach użytkowników. Jeśli użytkownicy zdecydują się zignorować oferowane przez nas opcje zabezpieczeń, nasze wysiłki pójdą na marne.

Propagowanie przez nas kwestii bezpieczeństwa na poziomie społeczności jest najbardziej podstawowym elementem bezpieczeństwa. Najlepsze wyniki daje położenie nacisku na bezpieczeństwo i ułatwianie użytkownikom korzystania z zabezpieczeń. Jeśli użyjemy technik inżynierii społecznej, aby pomóc naszym użytkownikom uczyć się bezpieczeństwa, będziemy mieli większą szansę zabezpieczyć sieć sąsiedzką.

Warto wiedzieć... Świadomość bezpieczeństwa

Powyższa lista obejmuje tylko najważniejsze zagadnienia bezpieczeństwa, o których SoCalFreeNet informuje użytkowników. Zdajemy sobie sprawę, że istnieje mnóstwo źródeł informacji pomagających użytkownikom, a nasza lista mogłaby mieć objętość wielokrotnie większą. Jest ona zamieszczona tutaj tylko jako przykład.

Inne metody

W każdej sąsiedzkiej sieci bezprzewodowej mogą pojawić się inne interesujące problemy. Oto kilka dodatkowych pomysłów, które możemy wziąć pod uwagę przy tworzeniu bezpiecznego środowiska sieci:

- **Squid Proxy** — narzędzie open source o nazwie Squid Proxy może posłużyć do uniemożliwiania użytkownikom korzystania z nieodpowiednich serwisów WWW, na przykład pornograficznych lub szerzących nienawiść. Narzędzie to jest wysoko cenione i na dodatek może pomóc w ograniczeniu ruchu w łączu szerokopasmowym poprzez buforowanie treści WWW. Adres: *www.squid-cache.org*.
- **Snort** — narzędzie open source służące do wykrywania włamań. Monitorując ruch przechodzący przez naszą sieć, Snort może ostrzec nas przed atakami pochodzącymi z sieci bezprzewodowej. Ostatnio zespół autorów narzędzia dodał do niego wyspecjalizowane funkcje do wykrywania ataków bezprzewodowych. Adres: *www.snort.org*.
- **OpenSSH** — OpenSSH oferuje funkcję zwaną przekazywaniem portów. Używając tego rozwiązania możemy utworzyć bardzo dobrą VPN o bezpieczeństwie wyższym niż w naszym rozwiązaniu PPTP. Jeśli sieć ma odpowiednią infrastrukturę, najwyższy poziom ochrony zapewnia rozwiązanie hierarchiczne z obustronnym uwierzytelnianiem, takie jak EAP-PEAP.