# Projektowanie bezpiecznej konfiguracji sieci

Projekt z przedmiotu BSS

Tomasz Jordan Kruk
T.Kruk@ia.pw.edu.pl

1 listopada 2004

## Spis treści



## 1 Strategie zabezpieczeń

Przed opisaniem poszczególnych architektur zabezpieczeń sieci przedstawione zostaną podstawowe strategie używane do wymuszania bezpieczeństwa w sieci.

Jedną z najbardziej podstawowych zasad bezpieczeństwa jest *zasada minimalnych przywilejów* (ang. *least privilege*). Polega ona na tym, że każdy obiekt (użytkownik, administrator, program, system itp.) powinien mieć tylko takie uprawnienia, które są mu niezbędne do wykonania przydzielonego zadania - i żadnych więcej. Pomaga to ograniczyć ryzyko ataku i zniszczeń, które spowoduje. Nie każdy użytkownik musi mieć dostęp do wszystkich usług internetowych. Nie każdy musi mieć możliwość czytania wszystkich plików w systemie. Nie każdy system musi mieć dostęp do wszystkich plików innego systemu.

Klasycznym przykładem jest rejestrowanie się administratora systemu uniksowego do systemu. Doświadczeni administratorzy nigdy nie rejestrują się do systemu jako użytkownik *root*. Każdy ma własne konto z prawami zwykłego





użytkownika, natomiast przełącza się komendą *su* (ang. *switch user*) na użytkownika *root* tylko w przypadku konieczności dokonania właściwych czynności administracyjnych.

Inną zasadą bezpieczeństwa jest tzw. *dogłębna obrona* (ang. *defence in depth*). Nie powinno się polegać na tylko jednym mechanizmie zabezpieczającym, jakkolwiek wydaje się skuteczny. Powinno się instalować wiele mechanizmów wspierających bądź też uzupełniających swoją funkcjonalność. Nie jest realistycznym założenie, iż nasze pojedyncze zabezpieczenie jest nie do złamania. Dlatego też powinno się stosować ochronę wielowarstwową. Należy zapamiętać, iż celem stosowania nadmiarowych zabezpieczeń nie jest głównie obrona przed atakami, lecz ochrona przed awariami innych poziomów zabezpieczeń.

Kolejną zasadą bezpieczeństwa jest wykorzystywanie tzw. *wąskiego przejścia* (ang. *choke point*). Wąskie przejście zmusza napastników do używania kanału, który można kontrolować i monitorować. W sieciach takim wąskim gardłem jest ściana ogniowa między siecią wewnętrzną a siecią zewnętrzną. Każdy, kto chce zaatakować sieć wewnętrzną z sieci zewnętrznej, musi użyć tego kanału, który z kolei powinien być dostatecznie zabezpieczony przed próbami ataków. Koncepcja wąskiego przejścia staje się bezużyteczna, gdy istnieje inna efektywna droga do systemu. Takim potencjalnym obejściem może być na przykład niezabezpieczony serwer terminali dla połączeń telefonicznych czy też dodatkowe bezpośrednie połączenie z siecią innej firmy, która nie podjęła w trosce o własną sieć wystarczających środków bezpieczeństwa.

Podstawową zasadą bezpieczeństwa jest *zasada najsłabszego ogniwa*. Każdy łańcuch zabezpieczeń jest tak silny jak jego najsłabszy punkt. Napastnicy będą szukali właśnie takiego najsłabszego punktu i bezlitośnie wykorzystają jego słabości. Należy być świadomym słabych punktów swojej obrony i je albo wyeliminować, albo jeżeli eliminacja nie jest możliwa, na ich kontroli skupić szczególna uwagę. Najsłabsze ogniwo będzie istniało zawsze, trzeba jedynie sprawić by było wystarczająco silne, proporcjonalnie do ryzyka. Przykładowo przeważnie bardziej uzasadniona jest obawa przed atakami z sieci niż przed faktem fizycznego włamania się do zasobów instytucji. Często więc, m.in. ze względu na koszty, świadomie decyduje się, by ochrona fizyczna była właśnie takim ogniwem. Jednak nie wolno całkiem zaniedbać ochrony fizycznej, ponieważ istnieje ryzyko takich ataków.

Jedną z podstawowych zasad bezpieczeństwa jest *bezpieczna reakcja w przypadku uszkodzenia*. Jeżeli elementy systemu zabezpieczeń ulegają awarii, powinny uniemożliwić atakującemu dostęp, zamiast mu go w pełni otworzyć. Awaria zazwyczaj odetnie wtedy dostęp również uprawnionym użytkownikom (do momentu jej usunięcia), jest to jednak akceptowalna i uzasadniona niedogodność na zasadzie mniejszego zła. Jeżeli router filtrujący pakiety zostanie wyłączony przestanie routować pakiety. Jeżeli usługa pośredniczenia przestanie być aktywna, nie będzie udostępniała swoich usług.

Aby działać efektywnie, większość systemów zabezpieczeń wymaga od personelu *współpracy*, a przynajmniej niewykonywania czynności mogących storpedować system zabezpieczeń. Nawet najlepsza ściana ogniowa stanie się bezużyteczna, gdy któryś z pracowników uzna ją za niewygodną przeszkodę i zainstaluje przy swoim komputerze w sieci wewnętrznej modem wraz z protokołem PPP na komputerze biurowym. Jest to oczywista tylna furtka, która równie łatwo jak niesubordynowany pracownik może wykorzystać potencjalny intruz.

Współpracę personelu osiąga się metodami edukacyjnymi i restrykcyjnymi. Niezbędne są szkolenia informujące użytkowników o potencjalnych zagrożeniach wynikających z różnych działań konfiguracyjnych podejmowanych bez konsultacji z administratorami bezpieczeństwa - to jest metoda edukacyjna. Użytkownik świadomy zagrożeń dwa razy zastanowi się, zanim w imię własnej wygody zaryzykuje zmniejszenie odporności sieci teleinformatycznej instytucji na potencjalne włamania. Metoda restrykcyjna, komplementarna w stosunku do edukacyjnej, polega na wdrożeniu regulaminów korzystania z sieci komputerowej i wymuszeniu na pracownikach korzystania z zasobów informatycznych zgodnie z założeniami odpowiednich fragmentów polityki bezpieczeństwa teleinformatycznego danej instytucji. Użytkownik świadomy podpisanych zobowiązań dwa razy zastanowi się, zanim przyjmie ryzyko konsekwencji dyscyplinarnych, a być może i prawnych, złamania uprzednio zaakaceptowanych regulacji dotyczących wykorzystywania zasobów informatycznych.

Strategia określana mianem *zróżnicowanej obrony* jest ściśle powiązana z dogłębną obroną, ma jednak inne znaczenie. Wedle tej strategii nie można się nie tylko ograniczać do pojedynczej warstwy zabezpieczeń, ale i środki zabezpieczeń powinny być zróżnicowane. Systemy zabezpieczeń tego samego rodzaju (na przykład filtry pakietów) mają te same słabości techniczne. Również systemy konfigurowane przez tę samą osobę mogą zawierać ten sam błąd merytoryczny. Jest wysoce prawdopodobnym, że systemy operacyjne tego samego producenta będą miały tę samą lukę, np. w stosie protokołów TCP/IP. Z drugiej strony, tendencja do unifikacji używanych typów zabezpieczeń ma także swoje uzasadnienie. Łatwiej jest zarządzać dziesięcioma urządzeniami pracującymi pod kontrolą tego samego systemu operacyjnego, niż pod kontrolą dziesięciu różnych systemów operacyjnych.

Wśród strategii zabezpieczeń należy również wymienić prostotę. Po pierwsze, rozwiązania proste są łatwiej weryfikowalne pod względem ich poprawności. Po drugie, złożoność oznacza wiele źródeł potencjalnych dodatkowych problemów. Łatwiej jest zabezpieczyć jeden komputer z kilkoma usługami niż sieć komputerów z rozdystrybuowanymi usługami. Zawsze należy jednak pamiętać, że efektywne zabezpieczenie jest z natury skomplikowane. Zabezpieczenia powinno się konstruować tak prosto jak to jest możliwe - ale nie prościej. Mimo





wszystko, to bezpieczeństwo sieci a nie prostota projektu jest głównym celem wdrożenia systemu zabezpieczeń.

Jako ostatnią należy również wymienić kontrowersyjną w niektórych środowiskach strategię *zabezpieczania przez utajnianie* (ang. *security through obscurity*). Zabezpieczenia tego typu są niewłaściwe, gdy są jedyną formą zabezpieczenia (przykład: szyfr z niejawnym, czyli niezweryfikowanym pod względem mocy i poprawności, algorytmem szyfrującym) lub gdy uniemożliwiają określenie prawdziwego poziomu zabezpieczenia produktu. Warto jednak uczynić z tej strategii środek dodatkowy w zabezpieczaniu zasobów sieci. Pewnej grupy informacji nie powinno się udostępniać na zewnątrz. Przykładowo, nie powinno się udostępniać osobom postronnym:

- dokładnego rodzaju sprzętu jakiego używa się do realizacji ściany ogniowej,
- szczegółów polityki bezpieczeństwa kontroli i filtrowania ruchu zaimplementowanej w architekturze zabezpieczeń,
- nazw hostów i użytkowników,
- informacji o wdrożonych systemach wykrywania włamań.

Nie da się i nie zawsze jest sens utajniania wszystkich informacji dotyczących architektury zabezpieczeń, ale im mniej z nich wydostanie się na zewnątrz, tym trudniejsze zadanie będzie miał potencjalny napastnik.

Podsumowując, przy projektowaniu zabezpieczeń sieci instytucji, należy uwzględnić i odpowiednio powiązać następujące strategie zabezpieczeń:

- przydział minimalnych wystarczających przywilejów,
- wykorzystanie dogłębnej obrony,
- zapewnienie wąskiego przejścia,
- zasadę najsłabszego ogniwa,
- bezpieczną reakcję w przypadku uszkodzenia,
- wykorzystanie zróżnicowanych środków obrony,
- maksymalną prostotę wystarczająco bezpiecznego rozwiązania,
- wykorzystanie w pewnym zakresie zabezpieczania poprzez utajnianie.

# 2 Architektury styku z siecią Internet

W poniższym podrozdziale przedstawiono metody zabezpieczania sieci instytucji poprzez różne architektury zabezpieczeń. Architektury te różnią się takimi własnościami jak: poziom zabezpieczenia, łatwość instalacji i późniejszego zarządzania oraz cena rozwiązania.

## 2.1 Wszystko w jednym

Najprostszą architekturą jest pojedynczy obiekt (ang. *single-box architecture*) pełniący funkcję ściany ogniowej. Wadą takie rozwiązania jest fakt, iż całe bezpieczeństwo zależy od tego jednego miejsca. Nie ma wielowarstwowych zabezpieczeń. Inna wada to ograniczenie zakresu przyłożonych zabezpieczeń ze względu na ograniczenia wydajnościowe pojedynczej maszyny. W praktyce, zaletą pojedynczej architektury jest nie tyle zadowalający poziom bezpieczeństwa, co względy praktyczne. W porównaniu z bardziej rozbudowanymi architekturami jest tańsza i łatwiej zarządzalna. Ponieważ wszystkie funkcje mieszczą się w jednym pudełku, zabezpieczenia takie są oferowane przez producentów zabezpieczeń jako łatwo instalowalny i konfigurowalny, wymagający minimalnego doglądania w trakcie pracy, produkt. Ponieważ rozwiązania oferowane są jako seryjne produkty, ich cena może być odpowiednio niższa. Ponadto, zarządzanie takim zabezpieczeniem wymaga mniej wiedzy w zakresie sieci komputerowych i zabezpieczeń, niż w przypadku innych rozwiązań. Jest to rozwiązanie dedykowane przede wszystkim dla firm o nierozbudowanej infrastrukturze sieciowej oraz ograniczonym zakresie wykorzystania sieci.

Najprostszym typem pojedynczego zabezpieczenia jest zastosowanie *routera osłaniającego* określanego również mianem *routera ekranującego* w charakterze ściany ogniowej. Jest to rozwiązanie tanie, gdyż i tak zazwyczaj do kontaktu z siecią Internet potrzebny jest router. Wystarczy go jedynie skonfigurować tak, by filtrował pakiety. Ponieważ nowe routery poza klasycznym filtrowaniem pakietów oferują również bardziej zaawansowane mechanizmy, jak badanie stanu wybranych protokołów czy zwrotne listy dostępu, osiągnięty poziom bezpieczeństwa jest dużo wyższy od minimalnego.

Router ekranujący nadaje się do zastosowania jako ściana ogniowa w następujących przypadkach:

- chroniona sieć ma dobrze zabezpieczone hosty,
- liczba używanych protokołów jest ograniczona d o kilku prostych,
- potrzebna jest maksymalna wydajność i nadmiarowość.





Innym typem pojedynczego zabezpieczenia jest *host dwusieciowy* (ang. *dual-homed host*). Jest to architektura oparta o host, który ma co najmniej dwa interfejsy sieciowe. Host taki może służyć jako router pomiędzy sieciami, do których ma interfejsy (np. siecią wewnętrzną i zewnętrzną). Jednak aby używać takiego komputera jako ściany ogniowej, należy wyłączyć funkcję trasowania. Pakiety z jednej sieci nie są bezpośrednio przesyłane do drugiej podsieci. Systemy chronione ścianą ogniową mogą się z nią komunikować. Tak samo mogą się z nim komunikować systemy zewnętrzne. Powyższe grupy nie mogą się komunikować bezpośrednio. Ruch IP między nimi jest całkowicie zablokowany.

Host dwusieciowy może zapewnić bardzo wysoki poziom kontroli. Jeżeli nie dopuszcza się żadnym pakietom na przechodzenie między sieciami, można mieć np. pewność, ze każdy pakiet w wewnętrznej sieci, który ma zewnętrzny adres źródłowy, oznacza niebezpieczeństwo. Z drugiej strony, rozwiązanie takie nie jest zbyt wydajne. Hosty muszą więcej pracować nad każdym połączeniem niż filtr pakietów i potrzebują więcej zasobów. Host bastionowy sam w sobie musi być bardzo bezpiecznie skonfigurowany. Intruz, który potrafiłby opanować taki host, dostaje pełen dostęp do sieci prywatnej a także może skutecznie uniemożliwić korzystanie z sieci zewnętrznej.

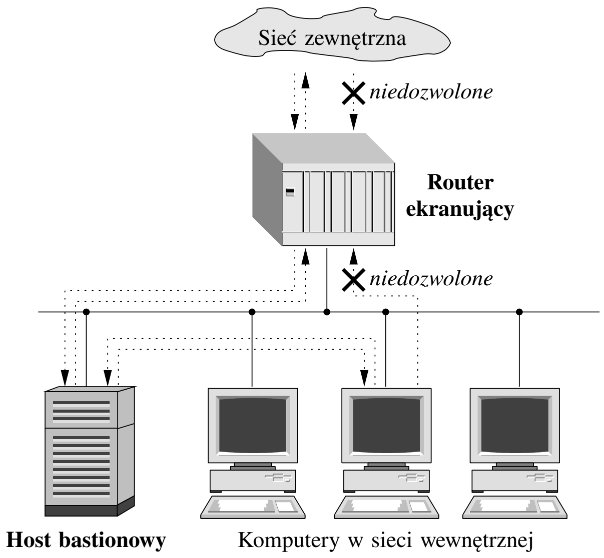
Host dwusieciowy może świadczyć usługi tylko poprzez pośredniczenie bądź bezpośrednią interakcję z użytkownikami. Problem polega na tym, że wymaga to zazwyczaj bazy kont użytkowników na hoście zabezpieczającym, a to stanowi samo w sobie dodatkowy problem. Ponadto, wielu użytkowników uważa za uciążliwość konieczność logowania się na takim hoście.

Pośredniczenie znacznie lepiej współpracuje z usługami wychodzącymi niż z przychodzącymi. W konfiguracji z hostem dwusieciowym większość usług internetowych musi być uruchamiana na tym hoście. Z drugiej strony, ma on przecież zasadnicze znaczenie dla bezpieczeństwa, więc nie powinno się na nim uruchamiać ryzykownych usług, jak np. serwer WWW. Reasumując, host z dwoma interfejsami nadaje się do zastosowania jako ściana ogniowa w następujących sytuacjach:

- ruch do sieci Internet jest niewielki,
- łączność z siecią Internet nie decyduje o prowadzeniu interesów firmy,
- sieć firmowa nie udostępnia na zewnątrz żadnych usług,
- sieć chroniona nie zawiera wyjątkowo wartościowych danych.

## 2.2 Architektura ekranowanego hosta

Podczas gdy architektura z hostem wielosieciowym udostępnia usługi z hosta, który jest przyłączony do wielu sieci (ale ma wyłączony routing), to *architek-*




Rysunek 1: Architektura z ekranowanym hostem.

*tura z ekranowanym hostem* (ang. *screened host*) udostępnia je z hosta, który jest przyłączony do sieci wewnętrznej z użyciem oddzielnego routera. W takim rozwiązaniu głównym zabezpieczeniem jest filtrowanie pakietów. Na rysunku 1 przedstawiono prostą wersję architektury z ekranowanym hostem. Host bastionowy jest umieszczony w sieci wewnętrznej. Filtrowanie pakietów w routerze skonfigurowano tak, by host bastionowy był jedynym hostem w sieci wewnętrznej, z którym mogą się łączyć hosty z sieci Internet (na przykład dostarczające pocztę elektroniczną). Dozwolone są tylko pewne typy połączeń, każdy system zewnętrzny próbujący uzyskać dostęp do wewnętrznych systemów lub usług musi się połączyć z tym hostem. Host bastionowy musi być szczególnie dobrze zabezpieczony.

Dzięki filtrowaniu pakietów host bastionowy może nawiązywać ze światem zewnętrznym dozwolone połączenia. Router ekranujący może być skonfigurowany tak, by wykonywał jedno z poniższych zadań:

- pozwalał hostom wewnętrznym na nawiązywanie połączeń z hostami w sieci Internet na potrzeby pewnych usług,





- zabraniał nawiązywania połączeń z wewnętrznych hostów - zmuszając je do korzystania z usług pośredniczenia w hoście bastionowym.

Oczywiście w zależności od potrzeb bądź dodatkowych ograniczeń możliwe są rozwiązania pośrednie. Niektóre usługi mogą być dostępne bezpośrednio przez filtr pakietów, inne tylko poprzez system pośredniczący. Jest to zależne od zaimplementowanej polityki bezpieczeństwa.

Pozornie architektura ekranowanego hosta wydaje się być bardziej ryzykowna od architektury z hostem wielosieciowym, gdyż pozwala na przepływ pakietów z sieci Internet do sieci wewnętrznej. W praktyce jednak i ta druga architektura jest podatna na awarie, które pozwalają pakietom przechodzić z sieci zewnętrznej do wewnętrznej. Ponadto, łatwiej jest bronić router niż host. W większości zastosowań, architektura ekranowanego hosta zapewnia i lepsze zabezpieczenie i większą użyteczność niż architektura z hostem wielosieciowym.

Ponieważ host bastionowy jest możliwym punktem awarii bądź ataku, nie należy na nim uruchamiać bardzo ryzykownych usług, na przykład serwera WWW. Host bastionowy powinien mieć zapewniony równie wysoki poziom ochrony, jakiego wymagałby host z wieloma interfejsami zastosowany jako pojedynczy element realizujący funkcje ściany ogniowej.

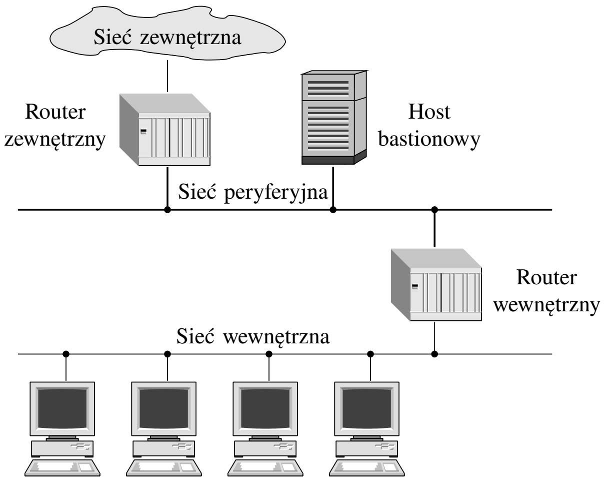
## 2.3 Architektura ekranowanej podsieci

*Architektura ekranowanej podsieci* (ang. *screened subnet architecture*) dodaje warstwę zabezpieczeń do architektury z ekranowanym hostem poprzez dodanie *sieci peryferyjnej* (ang. *perimeter network*), która dodatkowo izoluje sieć wewnętrzną od sieci Internet.

Najbardziej narażonymi na potencjalne ataki są hosty bastionowe. Pomimo ich odpowiedniego zabezpieczenia, należy przewidzieć sytuację, w której host bastionowy zostanie skutecznie zaatakowany. W architekturze z ekranowanym hostem nie ma żadnej linii obrony między hostami bastionowymi a pozostałymi maszynami należącymi do sieci wewnętrznej. Izolując host bastionowy od sieci wewnętrznej poprzez wprowadzenie sieci peryferyjnej można zmniejszyć skutki ewentualnego włamania do hosta bastionowego.

W najprostszym przypadku architektura z ekranowaną podsiecią tworzona jest poprzez wykorzystanie dwóch routerów, z których każdy podłączony jest do tej podsieci. Jeden jest umiejscowiony między siecią zewnętrzna a siecią ekranowaną, drugi między siecią wewnętrzną a siecią ekranowaną. Na rysunku 2 przedstawiono przykładową konfigurację ściany ogniowej, która opiera się na ekranowanej podsieci.

*Sieć peryferyjna* pełni funkcję dodatkowej bariery między napastnikiem a systemami wewnętrznymi. Jeżeli ktoś włamie się do hosta bastionowego będzie




Rysunek 2: Architektura ekranowanej podsieci z wykorzystaniem dwóch routerów.





mógł podejrzeć tylko ruch w tej sieci. Ponieważ żaden całkowicie wewnętrzny ruch nie przechodzi przez siec peryferyjną, ruch ten będzie zabezpieczony przed przechwyceniem nawet w przypadku włamania na host bastionowy. Oczywiście ruch do i z hosta do sieci zewnętrznych nadal będzie widoczny. Etapem projektowania ściany architektury zabezpieczeń jest m.in. upewnienie się, że ruch ten nie będzie zawierał niezabezpieczonych informacji na tyle poufnych, by ich ujawnienie naraziło cały ośrodek.

W opisywanej architekturze host bastionowy (lub kilka hostów bastionowych) włącza się do sieci peryferyjnej. Host ten jest głównym miejscem kontaktu połączeń przychodzących z zewnątrz z siecią instytucji. Usługi wychodzące są obsługiwane w jeden z następujących sposobów:

- ustawienie filtrów pakietów w zewnętrznym i wewnętrznym routerze tak, by pozwolić wewnętrznym klientom na bezpośredni dostęp do zewnętrznych serwerów,

- ustawienie serwerów proxy w hoście bastionowym (o ile wykorzystywane jest pośredniczenie) tak, by pozwolić wewnętrznym klientom na pośredni dostęp do zewnętrznych serwerów. Powinno się również ustawić filtrowanie pakietów, aby pozwolić wewnętrznym klientom na komunikację z serwerem proxy w hoście bastionowym i odwrotnie, ale jednocześnie zabronić bezpośredniej komunikacji między wewnętrznymi klientami a światem zewnętrznym.

W każdym z przypadków filtrowanie pakietów pozwala hostowi bastionowemu na połączenie się z siecią zewnętrzną oraz akceptowanie ustalonych typów połączeń z sieci zewnętrznej. Większość czynności hosta bastionowego polega na działaniu jako serwer proxy dla różnych usług.

*Router wewnętrzny*, określany również mianem *routera dławiącego* (ang. *choke router*), zabezpiecza sieć wewnętrzną przed atakami zarówno z sieci zewnętrznej jak i sieci peryferyjnej. Powinno się ograniczyć usługi dozwolone między hostem bastionowym a siecią wewnętrzną tylko do tych, które są rzeczywiście niezbędne, jak np. SMTP (by host bastionowy mógł przekierowywać przychodzącą pocztę), DNS (by host bastionowy mógł odpowiadać na zapytania komputerów zewnętrznych lub zadawać pytania, w zależności od konfiguracji) i tak dalej. Można również ograniczyć usługi w jeszcze większym zakresie umożliwiając komunikację w wybranych protokołach z hostem bastionowym tylko z wybranych komputerów sieci wewnętrznej. Przykładowo, SMTP może być ograniczone tylko do komunikacji między hostem bastionowym a wewnętrznym serwerem poczty.

Teoretycznie zadaniem *routera wewnętrznego* (ang. *exterior router*), zwanego czasem również *routerem dostępowym* (ang. *access router*), jest ochrona zarówno sieci peryferyjnej jak i sieci wewnętrznej. W praktyce, routery zewnętrzne zazwyczaj pozwalają wszystkim danym wychodzącym wydostać się na zewnątrz i prawie nie filtrują pakietów. Jedynymi specjalnymi regułami filtrowania w zewnętrznym routerze są te, które chronią maszyny w sieci peryferyjnej (czyli host bastionowy i router wewnętrzny). Zazwyczaj jednak specjalna ochrona nie jest konieczna, ponieważ hosty w sieci peryferyjnej chronione są przez własne zabezpieczenia. Aby wspierać usługi pośredniczące, dopuszczonych przez router wewnętrzny z hostów wewnętrznych do hosta bastionowego, router zewnętrzny może przepuszczać te protokoły tylko wtedy, gdy pochodzą z hosta bastionowego. Innym użytecznym zadaniem, które powinien wykonywać router zewnętrzny jest blokowanie wchodzących z sieci zewnętrznej pakietów z fałszywym adresem źródłowym, czyli pakietów usiłujących udawać pakiety z sieci wewnętrznej. Router zewnętrzny może również zabraniać wyjścia z sieci pakietom z nieprawidłowym adresem źródłowym.

Architektura z ekranowaną podsiecią jest odpowiednia do większości zastosowań. Oczywiście, podane rozwiązanie jest pewnym schematem posiadającym wiele różnych wariacji. Kładą one zazwyczaj jeszcze większy nacisk na bezpieczeństwo, na zwiększenie przepustowości bądź zapewnienie większego poziomu ciągłości działania w wypadku wystąpienia awarii.

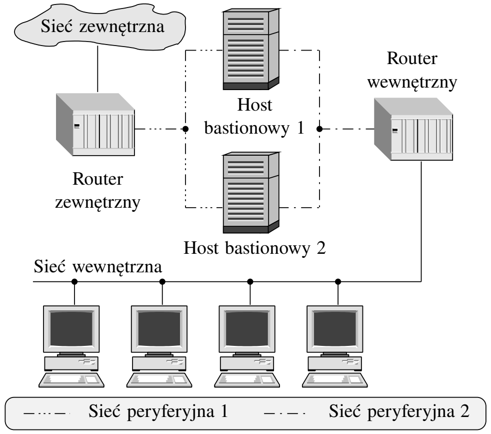
W *wieloczęściowej sieci ekranowej* (ang. *split-screened subnet*) nadal występują routery wewnętrzny i zewnętrzny, ale pomiędzy nimi jest kilka (zazwyczaj dwie) sieci. Osłonięte podsieci są przeważnie połączone ze sobą za pomocą jednego bądź wielu hostów wielosieciowych zamiast następnych routerów (rys. 3). Architektura ta stosowana jest w celu zapewnienia sobie wielowarstwowego zabezpieczenia i ochrony hostów z usługa pośredniczenia za pomocą routerów. Routery zapewniają ochronę przed fałszerstwem i takimi awariami hosta wielosieciowego, w wyniku których zaczyna on tarasować ruch. Host wielosieciowy, w porównaniu do filtrów pakietów, umożliwia bardziej dokładną kontrolę połączeń.

Architektura wieloczęściowej sieci ekranowej wykorzystywana jest czasem również w celu umożliwienia administracji usługami na hostach bastionowych z wykorzystaniem protokołów uznanych ogólnie za niewystarczająco bezpieczne, by mogły się znaleźć w sieci chronionej jedynie przez router zewnętrzny. Przykładami takich protokołów mogą być własne protokoły systemu NT używane podczas zdalnego uruchamiania menedżera użytkowników i monitora wydajności albo też usługi w systemach Unix wykorzystujące do konfiguracji protokół bez szyfrowania ruchu (np. telnet).

W pewnych przypadkach zasadnym jest zastosowanie *niezależnych podsieci ekranowanych*(ang. *independent screened subnet*) z oddzielnymi parami routerów zewnętrznych i wewnętrznych. Jednym z powodów może być konieczność zapewnienia nadmiarowości. Awaria czy skuteczny atak na jedną z sieci pe-








Rysunek 3: Architektura dwuczęściowej ekranowanej sieci bez przechodzącego ruchu.

ryferyjnych nie powoduje całkowitego braku łączności z siecią Internet. Rozwiązanie takie wydaje się być zasadnym na przykład w przypadku dostawców usług internetowych. W dużych instytucjach można też pokusić się o oddzielenie usług przychodzących (np. do oficjalnego serwera WWW naszej instytucji) od usług wychodzących (ruch generowany przez użytkowników z sieci wewnętrznej). Znacznie prościej jest zapewnić ścisłe bezpieczeństwo jeżeli ruch przychodzący i wychodzący zostaną rozdzielone.

Opisane powyżej architektury obrazują pewną strukturę logiczną systemu zabezpieczeń, jednak fizycznie pewna funkcjonalność może być na przykład scalona w jednym urządzeniu. Ze względu na cenę często *scala się router wewnętrzny z zewnętrznym* . W takiej sytuacji jedna grupa portów pełni funkcję routera zewnętrznego a druga grupa portów routera wewnętrznego. Podobnie jak w klasycznym rozwiązaniu występuje sieć peryferyjna, odgradzająca sieć zewnętrzną od sieci wewnętrznej. W normalnych warunkach poziom bezpieczeństwa jest dokładni taki sam jak przy rozłącznych routerach. Router taki stanowi jednak pojedynczy punkt awarii. W przypadku opanowania go przez intruza (co jest przy dobrym zabezpieczeniu mało prawdopodobne jednak nie niemożliwe) sieć wewnętrzna jest bezbronna.

W pewnych przypadkach można używać pojedynczej maszyny z wieloma interfejsami zarówno jako hosta bastionowego jak i routera zewnętrznego. Przypuśćmy, że do sieci zewnętrznej łączymy się jedynie przez łącze komutowane z wykorzystaniem protokołu PPP. W takim przypadku można używać PPP w hoście bastionowym i pozwolić mu działać i jako host bastionowy i jako router zewnętrzny. Używanie hosta wielosieciowego do routowania nie zapewni wydajności i elastyczności dedykowanego routera, ale nie jest to potrzebne w przypadku wolnego pojedynczego połączenia. W przeciwieństwie do łączenia routera zewnętrznego i wewnętrznego, połączenie hosta bastionowego z routerem zewnętrznym nie otwiera nowych poważnych luk. Po prostu host bastionowy jest chroniony przez filtry na swoich własnych interfejsach, które jak i w standardowej konfiguracji muszą być szczególnie uważnie zabezpieczone.

Nie wszystkie scalania są jednak bezpiecznie. Należy pamiętać o następujących zasadach:

- nie powinno się łączyć hosta bastionowego z routerem wewnętrznym,
- nie powinno używać się wielu routerów wewnętrznych dla jednej sieci peryferyjnej i jednego routera zewnętrznego,
- niebezpiecznie jest używać jednocześnie i ekranowanych podsieci i ekranowanych hostów.

W pierwszym przypadku system staje się systemem z ekranowanym hostem zamiast podsiecią. Jeżeli ktoś włamie się do hosta bastionowego, ma także natychmiast dostęp do sieci prywatnej.

W drugim przypadku problemem jest to, iż oprogramowanie routujące może uznać, iż najszybsza droga między dwoma komputerami wewnętrznymi będzie powadzić przez sieć peryferyjną. W przypadku konieczności wydzielenia w sieci wewnętrznej osobnych podsieci, lepiej wydzielić je na jednym routerze wewnętrznym albo też, w przypadku dużej liczby koniecznych podziałów, zdecydować się na stworzenie za routerem wewnętrznym prywatnej sieci szkieletowej łączącej wewnętrzne routery.

Nie stanowi natomiast, z punktu widzenia bezpieczeństwa, dodatkowego problemu użycie wielu routerów zewnętrznych podłączonych do tej samej sieci peryferyjnej.

# 3 Zalecenia odnośnie bezpiecznej konfiguracji

Architektura zabezpieczeń sieci jest pojęciem obejmującym swoim zakresem zarówno pojedyncze routery brzegowe z filtrowaniem pakietów jak i zaawansowane rozwiązania angażujące wiele ścian ogniowych, systemów pośredniczenia i systemów wykrywania włamań. Jest jednak kilka zaleceń ogólnych, odnoszących się do każdego systemu zabezpieczeń.

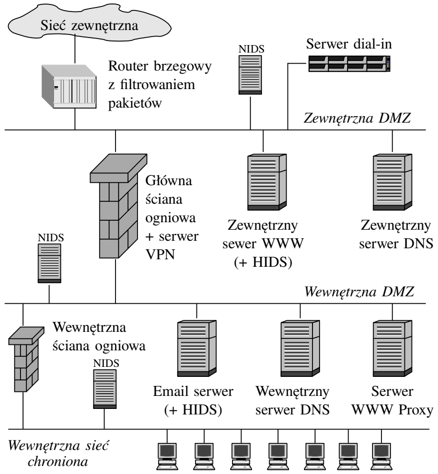




- *prostota rozwiązania* (ang. *KISS, Keep It Simple*), rozwiązanie nie może być zbyt skomplikowane, gdyż wtedy trudno w pełni je rozumieć, zweryfikować oraz nim zarządzać. Złożoność w projektowaniu i funkcjonalności często prowadzi do błędów konfiguracyjnych. Jest to najważniejsze z poniższych zaleceń.
- *wykorzystywanie urządzeń zgodnie z ich pierwotnym przeznaczeniem*, przede wszystkim zaleca się nie zatrudnianie do funkcji ściany ogniowej komputerów do tego pierwotnie nie dedykowanych. Analogicznie, podstawowym przeznaczeniem routerów jest routing a nie filtrowanie pakietów. Nie oznacza to, że nie należy wykorzystywać ich możliwości filtrowania pakietów, jednak nie powinno się polegać jedynie na routerach.
- *ochrona wielowarstwowa*, powinno się stosować architekturę wielowarstwową, przygotowywać kilka linii obrony. Tam, gdzie można wykorzystać kilka ścian ogniowych, należy je wykorzystać. Tam, gdzie można wdrożyć filtrowania pakietów w kilku punktach sieci, powinno się je wdrożyć. Jeżeli systemy operacyjne serwerów usług mają możliwość własnych metod zabezpieczenia, należy je również skonfigurować i uaktywnić.
- *niebagatelizowanie zagrożeń wewnętrznych* koncentrując się na zabezpieczeniach przed zagrożeniami zewnętrznymi nie wolno zapominać o potencjalnych zagrożeniach wewnętrznych. Rozpatrywać należy nie tylko sytuację, w której pracownik próbuje naruszyć bezpieczeństwo sieci własnej instytucji, ale i fakt, iż z powodu niedbałości bądź błędów użytkowników, intruz może uzyskać formalnie poprawny dostęp do zasobów wewnętrznych (zdobycie hasła pracownika, kradzież laptopa z konfiguracją VPN w przypadku użytkowników mobilnych), po czym może próbować atakować zasoby sieciowe mając już przyczółek w sieci wewnętrznej.

Decydując się na konkretną architekturę, która ma zabezpieczać sieć, należy rozpatrywać ściany ogniowe, które oferują następujące własności:

- filtrowanie pakietów i protokołów (filtrowanie na bazie typu protokołu, adresów i numerów portów źródła i celu, interfejsu wejściowego/wyjściowego pakietu),
- filtrowanie z badaniem stanu dla usług połączeniowych (co najmniej dla protokołów SMTP, FTP oraz HTTP),
- świadczenie usługi pośredniczenia (ang. *proxy*) dla planowanych do wykorzystywania protokołów,




Rysunek 4: Rozbudowana architektura ściany ogniowej.

- możliwość rejestracji zarówno ruchu przepuszczanego jak i odrzucanego,
- mechanizmy uwierzytelniania użytkowników o niestatycznym charakterze, tak by nawet ewentualne podsłuchanie protokołu uwierzytelniania nie umożliwiło intruzowi podanie się za uprawnionego użytkownika.

Decydując się na podłączenie do sieci Internet powinno się stworzyć co najmniej jedną ekranowaną sieć peryferyjną (najlepiej dwie, zewnętrzną i wewnętrzną), określaną również mianem strefy zdemilitaryzowanej (ang. *DMZ*). Usługi dostępne publicznie powinny być oddzielone od sieci wewnętrznej i umieszczone w sieci peryferyjnej. Użytkownicy wewnętrzni powinni być dodatkowo ochraniani przez wewnętrzną ścianę ogniową (co najmniej przez router dławiący).

Na rysunku 4 pokazano przykład dobrze zabezpieczonej sieci z dużą liczbą elementów zabezpieczających. Użytkownicy zdalni powinni raczej korzystać z sieci VPN. O ile serwer połączeń telefonicznych dial-in mógłby być umieszczony za ścianą ogniową, o tyle bezpieczniej jest powiązać go z serwerem usługi VPN, by połączenia zdalne mogły umożliwiać uwierzytelnienie i szyfrowanie. Jako dodatkowy element systemu zabezpieczeń, poza dotychczas omawianymi, pojawiają się systemy wykrywania intruzów (ang. *IDS*). Na rysunku umieszczono





sieciowe systemy wykrywania intruzów (ang. *network-based intrusion detection systems, NIDS*). Systemy typu host-based (ang. *HIDS*) mogą być dodatkowym zabezpieczeniem w przypadku instalacji na serwerach niekrytycznych pod względem wymagań na przepustowość, na przykład na serwerach poczty elektronicznej.

W przypadku sieci wewnętrznych zaleca się stosowanie mechanizmu translacji adresów (ang. *NAT*) oraz konfigurację osobnych, rozmieszczonych w osobnych podsieciach, serwerów DNS do wykorzystywania przez użytkowników zewnętrznych i użytkowników wewnętrznych. Informacja w serwerach DNS może być zróżnicowana - tak, by ukryć szczegóły konfiguracyjne sieci wewnętrznej przed potencjalnymi intruzami. Użytkownicy zdalni powinni być zobligowani wdrożoną polityką bezpieczeństwa teleinformatycznego instytucji, do instalacji na komputerach przenośnych, z których łączą się do sieci instytucji, systemów typu *osobista ściana ogniowa* (ang. *personal firewall*), zabezpieczających sam komputer przenośny przed atakami z sieci Internet.

Przed podjęciem decyzji o architekturze zabezpieczeń powinno się przeprowadzić analizę ryzyka krytyczności poszczególnych elementów i informacji przesyłanej w systemie teleinformatycznym. Rezultatem analizy powinny być decyzje dotyczące metody zabezpieczania i kosztów przeznaczonych na to zabezpieczenie.

Przed konfiguracją urzadzeń sieciowych pod względem zabezpieczania powinna być przygotowana polityka zabezpieczeń, zawierająca między innymi informacje jako informacje należy przepuszczać a jakie blokować. Domyślną polityką dotyczącą ruchu przychodzącego powinno być blokowanie wszystkich pakietów i połączeń, które jawnie nie zostały uznane za dozwolone. Alternatywa - blokowanie tego, co jest jawnie zabronione, jest rozwiązaniem mniej bezpiecznym.

Powinno się przyjąć jako generalną zasadę, iż każdy protokół i ruch, który nie jest niezbędnie konieczny powinien być zablokowany juz na pierwszym zabezpieczeniu, czyli na routerze dostępowym. Dzięki temu zredukuje się możliwość ataków i zmniejszy nasilenie ruchu w sieciach peryferyjnych, przez co zwiększy możliwość kontroli ruchu.

Zarówno do wychodzącego ruchu HTTP, jak i do wychodzącego i przychodzącego ruchu SMTP, powinno się wykorzystywać systemy pośredniczące (ang. *proxy*). Stosowane rozwiązania pośredniczące co najmniej powinny:

- umożliwiać blokowanie apletów i aplikacji w języku Java,
- posiadać możliwość filtrowania ActiveX i JavaScript,
- blokować zadane konfiguracją typy załączników MIME poczty elektronicznej,

- wykonywać skanowania antywirusowe.

To na ile aktywna zawartość stron WWW jest blokowana czy filtrowana zależy od przyjętej w instytucji polityki bezpieczeństwa. Należy znaleźć sensowny kompromis między możliwością przeglądania jak największego spektrum stron sieci WWW a bezpieczeństwem. Jedynym elementem, który bezwarunkowo powinien być blokowany są listy z wirusami i koniami trojańskimi. Z punktu widzenia bezpieczeństwa oczywiście idealną sytuacją byłoby blokowanie całej aktywnej zawartości wszystkich zewnętrznych stron WWW.

Załączniki poczty posiadające następujące rozszerzenia zawierają instrukcje, które mogą być wykonane półautomatycznie bądź automatycznie na komputerze odbiorczym: *.ade*, *.adp*, *.bas*, *.bat*, *.chm*, *.cmd*, *.com*, *.cpl*, *.crt*, *.dll*, *.eml*, *.exe*, *.hlp*, *.hta*, *.inf*, *.ins*, *.isp*, *.js*, *.jse*, *.lnk*, *.mdb*, *.mde*, *.msc*, *.msi*, *.msp*, *.mst*, *.pcd*, *.pif*, *.pl*, *.pot*, *.reg*, *.scr*, *.sct*, *.scx*, *.shs*, *.url*, *.vb*, *.vbe*, *.vbs*, *.wsc*, *.wsc*, *.wsf*, *.wsh*.

Rozszerzenia te w znakomitej większości są charakterystyczne dla systemów MS Windows. Nie oznacza to jednak, iż inne systemy operacyjne są wolne od zagrożeń związanych z możliwością uruchomienia robaków poprzez otwarcie załącznika poczty. Kod wykonywalny może być umieszczony również poprzez odwołania do adresów URL, a także w bezpiecznych wydawać by się mogło plikach jak np. pliki w postaci Postscript. To, że destrukcyjne czy intruzyjne załączniki preparowane są najczęściej dla systemu Windows wiąże się jedynie z mniejszą popularnością innych systemów, a nie ich lepszymi założeniami pod względem bezpieczeństwa. W najbliższym czasie można na przykład spodziewać się coraz większej liczby robaków przygotowywanych pod odbiorcę w systemie Linux - ze względu na rosnącą popularność tego systemu.

Domyślną polityką ściany ogniowej powinno być blokowanie całego przychodzącego ruchu o ile ten nie został jawnie dopuszczony dla wybranych protokołów czy adresów. Poniżej przedstawiono zestawienie serwisów i aplikacji, które powinny przedmiotem konfiguracji na ścianie ogniowej wraz z opisem działania, które należy przedsięwziąć. Zestawienie stworzono na bazie zaleceń organizacji CERT/CC (www.cert.org/tech_tips/packet_filtering.html) oraz SANS Institute (www.sans.org/top20.htm).

Jeżeli chodzi o filtrowanie protokołu ICMP, zaleca się blokowanie przychodzących żądań echa (ping i traceroute) oraz blokowanie wychodzących odpowiedzi echo, przekroczenia czasu, i nieosiągalności celu - z wyjątkiem pakietów typu „wiadomość zbyt duża” (typ 3, kod 4). Jest to podejście restrykcyjne, która utrudnia pracę również w przypadku prawidłowych prób użycia pakietów ICMP. Na podejście mniej restrykcyjne, pozwalające na ograniczoną listę dopuszczanych typów pakietów ICMP z określonych źródeł (np. od własnego dostawcy sieci Internet) można sobie pozwolić, o ile posiada się router, który potrafi do-





| **Aplikacja** | **Numer portu** | **Akcja** |
|---|---|---|
| Usługi logowania | telnet - 23/tcp | ograniczenie z silnym uwierzytelnianiem |
| | SSH - 22/tcp | ograniczenie do ustalonych systemów |
| | FTP - 21/tcp | ograniczenie z silnym uwierzytelnianiem |
| | *r-usługi* - 512-514/tcp | zawsze zablokowane |
| RPC i NFS | portmap/rpcbind - 111/tcp/udp | zawsze zablokowane |
| | NFS - 2049/tcp/udp | zawsze zablokowane |
| | lockd - 4045/tcp/udp | zawsze zablokowane |
| NetBIOS w Windows NT | 135/tcp/udp | zawsze zablokowane |
| | 137/udp | zawsze zablokowane |
| | 138/udp | zawsze zablokowane |
| | 139/tcp | zawsze zablokowane |
| | 445/tcp/udp (W2K) | zawsze zablokowane |
| X Window | 6000/tcp - 6255/tcp | zawsze zablokowane |
| Usługi nazewnicze | DNS - 53/udp | ograniczone do zewnętrznych serwerów DNS |
| | DNS, transfer strefy - 53/udp | zablokowane, o ile nie ma zewnętrznych *slave* |
| | LDAP - 389/tcp/udp | zawsze zablokowane |
| poczta | SMTP - 25/tcp | zablokowane z wyjątkiem serwerów poczty |
| | POP - 109/tcp i 110/tcp | zawsze zablokowane |
| | IMAP - 143/tcp | zawsze zablokowane |
| WWW | HTTP - 80/tcp i SSL - 443/tcp | zablokowane z wyjątkiem publicznych serwerów WWW |
| | być może również inne porty: 8000/tcp, 8080/tcp, 8888/tcp | |
| „małe porty” | porty poniżej 20/tcp/udp | zawsze zablokowane |
| | time - 37/tcp/udp | zawsze zablokowane |
| różne | TFTP - 69/udp | zawsze zablokowane |
| | finger - 79/tcp | zawsze zablokowane |
| | NNTP - 119/tcp | zawsze zablokowane |
| | NTP - 123/tcp | zawsze zablokowane |
| | LPD - 515/tcp | zawsze zablokowane |
| | syslog - 514/tcp | zawsze zablokowane |
| | SNMP - 161-162/tcp/udp | zawsze zablokowane |
| | BGP - 179/tcp | zawsze zablokowane |
| | SOCKS - 1080/tcp | zawsze zablokowane |

Rysunek 5: Zalecana konfiguracja filtrowania pakietów.

kładnie analizować i filtrować pakiety ICMP.

Następujące typy ruchu sieciowego powinny być zawsze zablokowane:

- ruch wejściowy z nieautoryzowanych źródeł podający jako adres źródła adres ściany ogniowej,
- ruch wejściowy z adresem źródłowym stwierdzającym, iż pakiet jakoby pochodzi z sieci wewnętrznej,
- ruch wejściowy ze źródła z zakresu zdefiniowanego w RFC 1918 jako zarezerwowanego dla sieci prywatnej,
- ruch wejściowy z nieautoryzowanego źródła zawierający protokół SNMP (Simple Network Management Protocol),
- ruch wejściowy zawierający informacje o routingu źródłowym IP,
- ruch wejściowy i wyjściowy zawierający jako źródło bądź przeznaczenie adres lokalny 127.0.0.1,
- ruch wejściowy i wyjściowy zawierający jako adres źródła bądź przeznaczenia 0.0.0.0,
- ruch wejściowy i wyjściowy zawierający adresy ukierunkowanego rozgłaszania (ang. *directed broadcast*).

Jeżeli ściana ogniowa została zainstalowana na standardowym systemie operacyjnym (np. Unix, Windows NT), system operacyjny musi oferować zminimalizowany (być może żaden) zestaw usług sieciowych. Najlepszą sytuacją jest ta, w której system taki nie oferuje żadnych usług sieciowych (żadne usługi nie słuchają na portach IP) oprócz niezbędnych do realizacji funkcji ściany ogniowej. System operacyjny musi być też regularnie uaktualniany poprzez nakładanie łatek na system przygotowanych przez producenta.

Kopia zapasowa systemu ściany ogniowej nie powinna być przeprowadzana przez sieć. Do tworzenia kopii powinno się wykorzystywać jedynie wewnętrzne mechanizmy, np. dołączony streamer. Wykonywanie kopii zapasowych przez sieć byłoby źródłem potencjalnych luk w systemie zabezpieczeń.

Ściana ogniowa powinna rejestrować ustalony przez administratora ruch. Zarejestrowane dzienniki systemowe powinny być analizowane przez administratora systemu codziennie. O ile system ściany ogniowej posiada zdalny interfejs graficzny do konfiguracji i przeglądania zapisanych informacji, warto zastanowić się czy nie należy stworzyć dedykowanej sieci wewnętrznej połączonej do ściany dedykowanym interfejsem jedynie do łączenia się ze ścianą ogniową przez administratora poprzez klienta interfejsu graficznego.





Mimo silnych zabezpieczeń każda instytucja powinna być przygotowana na wystąpienie incydentów naruszenia bezpieczeństwa zasobów sieciowych o różnym poziomie konsekwencji. Procedury obsługi incydentów powinny być przygotowane zanim takowe incydenty wystąpią.

# Literatura

[Amo99] Edward Amoroso. *Sieci: Wykrywanie intruzów*. Wydawnictwo RM (AT&T), 1999.

[GS97] Simson Garfinkel and Gene Spafford. *Bezpieczeństwo w Unixie i Internecie*. Wydawnictwo RM (O'Reilly and Associates, Inc.), 1997.

[Kae01] Merike Kaeo. *Tworzenie bezpiecznych sieci*. Wydawnictwo MIKOM (Cisco Press), 2001.

[Mou01] Gerhard Mourani. *Securing & Optimizing Linux: The Ultimate Solution*. OpenNA Inc., 2001.

[SP01] Matthew Strebe and Charles Perkins. *Firewalls, Ściany ogniowe*. Wydawnictwo MIKOM (Sybex Inc.), 2001.

[Sta99] Mariusz Stawowski. *Badanie zabezpieczeń sieci komputerowych*. Wydawnictwo ArsKom, 1999.

[WCP02] John Wack, Ken Cutler, and Jamie Pole. Guidelines on Firewalls and Firewall Policy. NIST Special Publication 800-41, National Institute of Standards and Technology, Jan 2002.

[ZCC01] Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman. *Internet Firewalls - tworzenie zapór ogniowych*. Wydawnictwo RM (O'Reilly and Associates, Inc.), 2001.