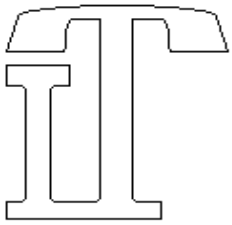


INSTYTUT TELEKOMUNIKACJI
POLITECHNIKA WARSZAWSKA

Sławomir Górniak Piotr Kijewski Krzysztof Szczypiorski
e-mail:{S.Gorniak,P.Kijewski,K.Szczypiorski@tele.pw.edu.pl}

Bezpieczna sieć LAN chroniona przy pomocy firewalla

PRACOWNIA PROBLEMOWA
OPIEKUN: DR RYSZARD KOSSOWSKI

Warszawa, luty-czerwiec 1996

Streszczenie

Praca prezentuje najpopularniejszy obecnie i najskuteczniejszy sposób zabezpieczenia sieci lokalnych podłączonych do Internetu - „ściany przeciwogniowe" - firewalle. W części pierwszej - teoretycznej - przedstawiono: koncepcję włamań do systemów unixowych, wprowadzenie do firewalli, opis mechanizmów tworzących firewalle, różne konfiguracje systemów, w części drugiej - opisano eksperymentalną bezpieczną podsieć zrealizowaną w Zakładzie Teleinformatyki i Telekomutacji IT PW chronioną przy pomocy omawianej techniki.

Podziękowania

Projekt ten nie powstałby bez pomocy osób życzliwych. Chcielibyśmy podziękować Panu dr. Ryszardowi Kossowskiemu za nadzór nad naszymi poczynaniami, a także Panu mgr. inż. Grzegorzowi Łubkowskiemu i Panu mgr. inż. Karolowi Górskiemu za użyczenie niezbędnego sprzętu. W projekcie aktywnie uczestniczył także Zbigniew Bazydło, któremu tą drogą również składamy serdeczne podziękowania.

S.Górniak, P.Kijewski, K.Szczypiorski

Spis treści

Spis ilustracji

Wprowadzenie

Strzeż skarbu tego, lecz i zapisz w duszy:
Igranie z ogniem najtrwalszą stal kruszy.
William Shakespeare, fragment sonetu 95

Jeśli mówimy o świecie bez granic, jeśli myślimy o swobodnych kontaktach pomiędzy ludźmi należącymi do różnych narodowości i kultur mamy na myśli jedno z dwóch pojęć: science-fiction albo Internet. Science-fiction nie będziemy się zajmować, odniesiemy się natomiast do Internetu - zwanego cyberprzestrzenią albo NetCity, będącego czymś więcej niż tylko telekomunikacyjną siecią.

Internet z dnia na dzień rozrasta się. Pojawiające się nowe węzły umożliwiają pracę coraz większej liczbie użytkowników. Szybka wymiana danych pomiędzy dwoma odległymi komputerami, dostęp do najświeższych informacji przechowywanych w odległej o tysiące kilometrów bazie danych to tylko niektóre atrybuty pracy w sieci otulającej cały glob.

Na pewno nikt nie życzy sobie aby jego dom odwiedzali ludzie nie proszeni. Rzadko tęskni się do kolejnej wizyty akwizytorów oferujących plastikowe obrusy albo nylonowe dresy. Nigdy nie pożąda się wizyty złodziei złaknionych kosztowności. Nikt też nie pragnie, aby jego sieć lokalną podłączoną do Internetu inwigilowali intruzi.

W tej pracy przedstawimy skuteczną metodę ochrony informacji przekazywanych przy pomocy sieci Internet - technikę „ścian przeciwogniowych” (firewalli). Najpierw przedstawimy teoretyczny aspekt zagadnienia, a następnie przystąpimy do opisu zrealizowanej w Zakładzie Teleinformatyki i Telekomutacji IT PW eksperymentalnej bezpiecznej podsieci.

1. Teoria

1.1 Koncepcja włamań

1.1.1 Wyzwanie

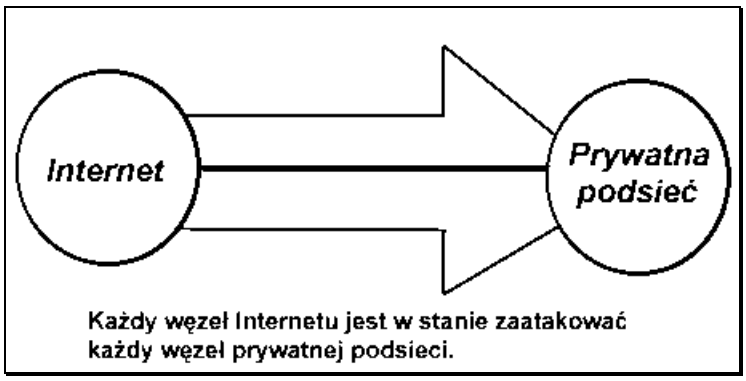
Każdy administrator komputera podłączonego do Internetu, szczególnie pracującego pod kontrolą systemu UNIX, musi sobie zdawać sprawę z tego, że jego komputer może stać się wyzwaniem dla włamywacza.

UNIX, mimo że jest najlepszą platformą dla aplikacji internetowych, posiada wiele słabych punktów pod względem bezpieczeństwa danych. Oczywiście firewalle, o których będziemy w tej pracy mówić, nie są ściśle związane z UNIXem, jednak do takiej konfiguracji będziemy się odnosić.

Zdarzają się przeróżni włamywacze - jedni traktują włamania tak jak sport, inni poszukują konkretnych informacji - jednak jedni i drudzy nie są przez nas mile widziani.

1.1.2 Idea włamań do systemu UNIX

Najczęściej włamywacz (zwany hackerem lub crackerem) - pragnie uzyskać zdalny dostęp do atakowanej maszyny i rozpocząć na niej sesję zwykłego użytkownika. Następnie, wykorzystując rozmaite błędy w systemie, próbuje zdobyć prawa administratora komputera - gdy już prawa te posiądzie, integralność danych zgromadzonych w tej maszynie leży całkowicie w jego rękach. Jako niekontrolowane „furtki” do systemu mogą posłużyć źle napisane lub skonfigurowane programy z atrybutem *Set User ID*[1] lub *Set Group ID*[2].



Rys. 1-A Możliwości ataku prywatnej podsieci

1.1.3 Rola administratora

Administrator (root) ma za zadanie tak skonfigurować system, aby zmniejszyć maksymalnie prawdopodobieństwo pomyślnego włamania. Wiadomo, że w pełni bezpieczne systemy nie istnieją, i że wszelkie niedociągnięcia ujawniają się podczas intensywnej pracy. Stąd też administrator musi instalować regularnie publikowane przez producenta używanego systemu „patche” (łaty) - poprawki usuwające błędy w firmowym oprogramowaniu. Powinien też dokładnie kontrolować

[1] program może być uruchamiany z prawami (przywilejami) właściciela - najczęściej administratora
[2] program może być uruchamiany z prawami grupy

przychodzące pakiety, na przykład przy pomocy programu TCP-wrappers, rozszerzającego możliwości logowania[3] komunikatów systemowych. Logi takie powinny być przechowywane w komputerze, do którego dostęp mają tylko zaufani użytkownicy.

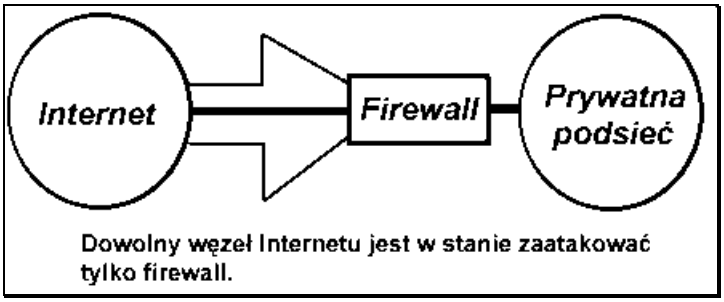
Administrator powinien przywiązywać dużą uwagę do konfiguracji komputerów w swojej podsieci. W podsieci, w której znajduje się kilkadziesiąt „zaufanych" (tj. „ufających sobie") komputerów, najgorzej zabezpieczona maszyna obniża bezpieczeństwo całej grupy - jest jej najsłabszym punktem. Powoduje to konieczność chronienia każdego z komputerów w danej podsieci, oczywiście bez gwarancji skuteczności takiej polityki.

Także zbędne usługi oraz programy dostępne w systemie mogą zmniejszać bezpieczeństwo sieci.

1.2 Wprowadzenie do firewalli

1.2.1 Pierwsze spotkanie

Najlepszym rozwiązaniem problemu bezpieczeństwa podsieci internetowej jest firewall. Firewall eliminuje konieczność zabezpieczania każdego komputera z osobna, jest ścianą przeciwoogniwą, odgradzającą prywatną „spokojną" podsieć od „agresywnego" Internetu.

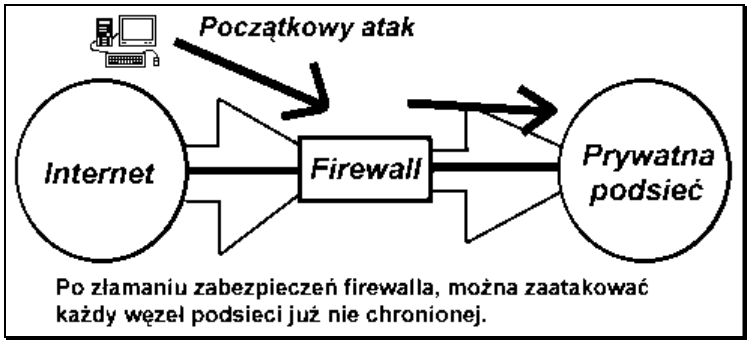


Rys. 1-B Możliwość ataku z Internetu tylko na firewall

Oczywiście sama konfiguracja firewalla, który jest odpowiednio skonfigurowaną maszyną lub grupą maszyn, musi być na tyle dobra, by nie dopuścić do ominięcia go przez włamywacza, co spowodowałoby praktycznie nieograniczony dostęp do wszystkich komputerów funkcjonujących w danej podsieci.

1.2.2 Polityka bezpieczeństwa

We wszystkich środowiskach sieciowych należy przyjąć określoną politykę bezpieczeństwa. System musi być chroniony według ściśle zdefiniowanych reguł. Przy korzystaniu z firewalla istnieją dwie odmienne reguły: *„To, co nie jest wyraźnie zabronione, jest dozwolone"* oraz *„To, co nie jest*



Rys. 1-C Dostęp do podsieci po złamaniu zabezpieczeń firewalla

[3] księgowania

wyraźnie dozwolone, jest zabronione". Przyjęcie pierwszego założenia jest dość wygodne - administrator blokuje jedynie porty IP[4] oraz usługi o których wiadomo, że mogą być niepewne (w domyśle niebezpieczne). Temu spojrzeniu można przeciwstawić drugie założenie - wszystkie porty zostają zablokowane, za wyjątkiem tych, o których wie się, że są pewne. Z punktu widzenia bezpieczeństwa, ostatnia reguła jest znakomita, niestety powoduje spore utrudnienia dla zwykłych użytkowników. **Bez przyjęcia określonej polityki bezpieczeństwa firewall nie może istnieć**.

1.2.3 Drugie spotkanie - wnętrze firewalla

Firewall jest złożony zazwyczaj z routera filtrującego przychodzące pakiety (*screening router*) oraz komputera zwanego *bastion host*. Zadanie firewalla jest proste:

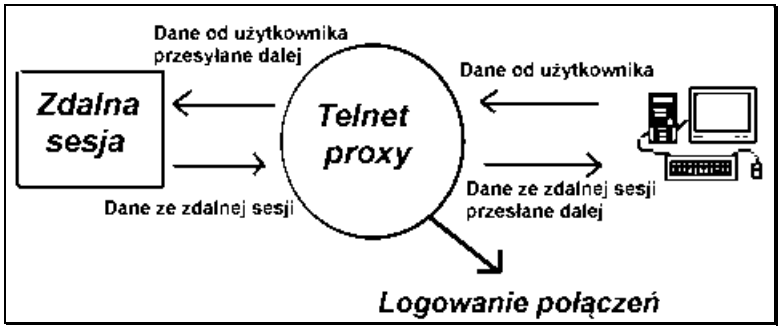
- sprawdzić, skąd został wysłany,
- dokładnie „prześwietlić" (przefiltrować) każdy przychodzący z zewnątrz pakiet,
- sprawdzić, do którego komputera zmierza,
- na który port IP jest skierowany.

Następnie podejmowana jest decyzja dotycząca przekierowania tego pakietu - do niektórych portów będzie on mógł dotrzeć bez żadnych przeszkód, do niektórych innych - poprzez bastion host (tak zwany *proxy server* lub *gateway*), do innych zaś z definicji dostać się nie będzie mógł - zostanie po prostu odrzucony. Ma to na celu dokładną eliminację wszelkich zagrożeń płynących z zewnatrz - żadna usługa nie jest do konca bezpieczna a „dziury" w rozmaitych programach wykrywane są w bardzo krótkich odstępach czasu.

Podsieć, która nie jest chroniona przez gateway jest nazywana w skrócie DMZ - *Strefa Zdemilitaryzowana* (*De-Militarized Zone*).

1.2.4 Ogólne zasady

Usługi typu proxy mają za zadanie odebrać cały ruch skojarzony z daną usługą na danym porcie IP, a następnie przekierować go na komputer udostępniający tę usługę. Zatem zewnętrzny świat nie komunikuje się z właściwym, docelowym serwerem, lecz z jego proxy. Ma to oczywiście niebagatelne znaczenie - przy



Rys. 1-D Przykład działania proxy

[4] sieci udostępniają użytkownikom usługi; usługi są umieszczone pod znanymi adresami - tzw. portami; proces użytkownika (np. klient) na jednej maszynie porozumiewa się z procesem (np. serwerem) na drugiej poprzez porty

przyjęciu drugiego założenia dotyczącego bezpieczeństwa każdy port, który nie jest konieczny do poprawnego działania podsieci jest zablokowany - proxy umożliwiający pobranie udostępnionych informacji jest więc jedynym sensownym rozwiązaniem. Można korzystać z proxy przy takich usługach jak telnet, FTP czy WWW. Na przykład nowe programy obsługujące te usługi, w tym Netscape, posiadają możliwość korzystania z proxy.

Wszelkie usługi udostępnione obcym osobom muszą być bezpieczne dla systemu, dlatego też powinno stosować się logiczną zmianę katalogu głównego dla poszczególnych usług (*chroot*), gdy instalujemy serwer WWW, FTP lub sendmail.

> Katalogiem głównym z punktu widzenia osoby łączącej się z naszym komputerem nie może być nasz właściwy katalog główny lecz jego ścisły wycinek - np. /usr/local/httpd - bez możliwości przedostania się w inne miejsce. Chroni to na przykład przed kradzieżą plików konfiguracyjnych systemu, w tym pliku z hasłami użytkowników.

Przy definiowaniu firewalla należy wspomnieć o pojęciach takich jak *application level* i *circuit level*. Pojęcia te opisują sposób w jaki rozmaite usługi są przechwytywane i obsługiwane przez firewall. O application level gateway mówi się, gdy dany pakiet przechwytuje usługa tego samego typu, co docelowa dla tego pakietu i ona przesyła go dalej swoim protokołem - dzieje się tak na przykład przy mail-exchangerze zapewniającym wymianę poczty elektronicznej. Circuit level gateway polega na przesłaniu pakietów przez usługi nie potrafiące zrozumieć informacji niesionej przez pakiet. W ekstremalnym przypadku ten gateway dla świata zewnętrznego wygląda jak proxy, zaś dla komputerów wewnątrz podsieci - jak filtr. Zaletą circuit level gateway jest możliwość zastosowania go dla różnych, ale nie dla wszystkich protokołów. Obarczony jest on różnymi wadami - na przykład nie jest w stanie stwierdzić, czy przesyłany przez niego pakiet jest bezpieczny dla systemu.

1.2.5 Trochę ekonomii

Instalowanie firewalla nie jest niestety bezpłatne, obojętne, czy kupujemy go u konkretnego dostawcy, czy też budujemy go sami na podstawie darmowych, ogólnie dostępnych programów. W cenę wliczony musi być zakup oraz utrzymanie sprzętu takiego jak dobry router, umożliwiający filtrowanie pakietów oraz silne komputery. Gdy decydujemy się na komercyjnego firewalla dochodzą niebagatelne koszty zakupu i upgrade'u oprogramowania - w przypadku używania oprogramowania darmowego pozostaje śledzenie kolejnych jego wersji. Warto tu wspomnieć o darmowym pakiecie Firewall Toolkit firmy TIS oraz o pakiecie SOCKS zawierającym narzędzia do budowania circuit level proxy-servers.

Trzeba też pomyśleć o wyszkoleniu personelu aby w każdej sytuacji można było sobie poradzić z ewentualną rekonfiguracją firewalla lub z jego naprawą. Do kosztów firewalla doliczyć trzeba też stratę pewnych usług świadczonych w Internecie, operujących na niepewnych portach bądź opartych na protokole UDP. Należy jednak zdać sobie sprawę także z kosztów ponoszonych przy zaniechaniu instalacji firewalla - trudy śledzenia działalności hackerów, konieczność

ustawicznego czuwania, przy ewentualnych włamaniach - koszty reinstalacji systemu, backupu danych, które mogły być przez włamywacza zmienione (nie mówiąc już o kosztach, które poniosłoby się w przypadku kradzieży ważnych danych). Administrator systemu może w takim przypadku bardzo łatwo stracić pracę. Zaniechanie budowy firewalla oznacza w praktyce gotowość na sponsorowanie działalności hackerów.

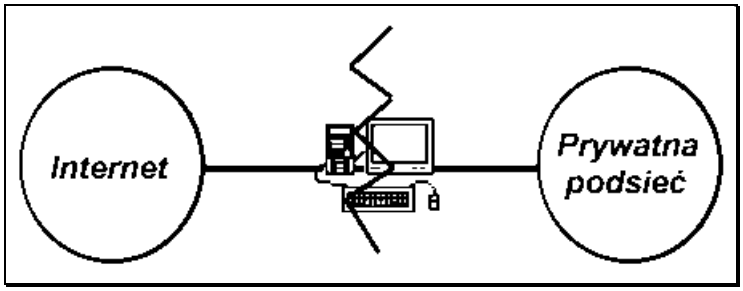
1.2.6 Typy firewalli

1.2.6.1 Screening Router

Najprostszym firewallem jest odpowiednio skonfigurowany router, umożliwiający filtrowanie pakietów - zwany *packet filter* lub screening router. Zadaniem takiego routera jest sprawdzenie na podstawie docelowego adresu czy powinien dany pakiet przesłać dalej, czy go odrzucić. Ustawiając pewne reguły routingu (*rulesets*), można eliminować niektóre aplikacje uchodzące za niebezpieczne - na przykład tftp, X11, RPC oraz „Berkeley ‘r’-utilities” (rsh, rlogin, rcp). Router taki nie musi być koniecznie sprzętowy, lecz może bazować na odpowiednim oprogramowaniu które oferuje dobre możliwości konfiguracji. Występują tu jednak pewne niedogodności - dane są sprawdzane na poziomie pakietów, nie sposób więc dokładnie sprawdzić ich zawartości. Nie można także uwierzytelnić konkretnych osób korzystających z danych usług w chronionej podsieci. Łatwo jest się pomylić przy konstruowaniu reguł. Filtrowanie pakietów pociąga za sobą też spowolnienie działania sieci - sprawdzenie każdego pakietu zajmuje pewien czas. Screening router jest jednak bardzo wygodny z punktu widzenia użytkowników - jego obecność jest prawie niewidoczna i nie wymaga instalowania proxy-servers dla żadnej z usług.

1.2.6.2 Dual Homed Gateways

W tym wariancie nie występuje screening router, lecz jedynie komputer posiadający przynajmniej dwa interfejsy sieciowe. Taki komputer mógłby być routerem, ale nie jest. Jego zadaniem jest niedopuszczenie do bezpośrednich połączeń między Internetem a siecią chronioną. W efekcie cały firewall składa się z bastion hosta, a sieć za nim staje się niewidzialna z zewnątrz. Komputery znajdujące się wewnątrz tej sieci mogą się komunikować z Internetem tylko poprzez bastiona.



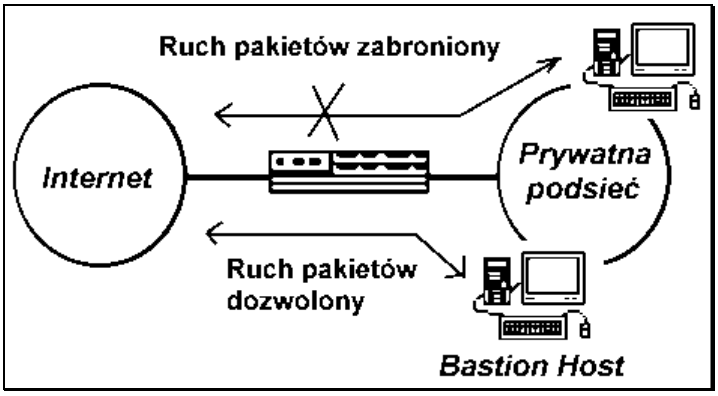
Rys. 1-E Schemat Dual Homed Gateway

Użytkownicy mogą albo posiadać konta na bastionie, albo korzystać z proxy-services. Lepsza jest druga sytuacja. Na bastionie bowiem nie powinno się zakładać żadnych kont ani instalować żadnych usług poza niezbędnymi, zapewniającymi jedynie dobre funkcjonowanie firewalla. Każdy program na dysku komputera może stanowić zagrożenie dla jego bezpieczeństwa. Bastion host jest

na tyle ważnym ogniwem firewalla (w przypadku Dual Homed Gateway - jedynym), że nie można sobie na to pozwolić. Przeniknięcie do bastion hosta oznacza w praktyce zniszczenie firewalla. Bastion pomiędzy swoimi obowiązkami powinien również sprawować pełną kontrolę nad systemowymi komunikatami i troszczyć się o ich logowanie. Każda próba przeniknięcia przez firewall musi być odnotowana. Jednakże instalowanie proxy-services, chociaż bezpiecznych, nie jest możliwe dla wszystkich usług - wiele z nich byłoby po prostu niedostępnych (szczególnie nowe usługi do których należy bądź samemu napisać odpowiedni program, bądź poczekać - czasem dość długo - aż taki program zostanie udostępniony). Chociaż Dual Homed Gateway w tym wariancie oferuje duże bezpieczeństwo (przy adekwatnej konfiguracji), jest mało elastyczne, przez co trudne do utrzymania.

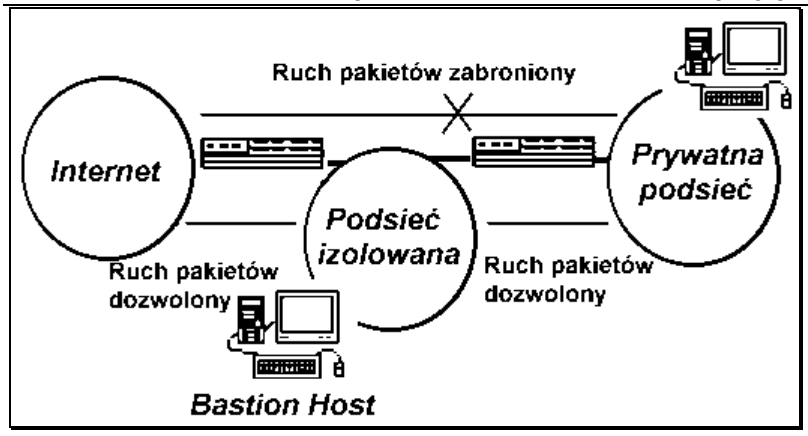
1.2.6.3 Screened Host Gateway

Tutaj występuje tak screening router jak i bastion host. Usługi są dostarczane poprzez proxy-services na bastionie znajdującym się wewnątrz naszej sieci, do którego pakiety kierowane są przez screening router. Filtrowanie pakietów powstrzymuje pozostałe komputery wewnątrz sieci przed bezpośrednią komunikacją z Internetem, uniemożliwiając obejście proxy-services. Jednak ta konfiguracja jest dużo bardziej elastyczna niż poprzednio omawiana - możliwości połączeń nie ograniczają się jedynie do korzystania z proxy-services, lecz router może niektóre aplikacje przesyłać bezpośrednio od danego komputera na zewnątrz. Elastyczność ta ma jednak swoją cenę - nie mamy już tylko jednego newralgicznego punktu, lecz dwa - router i bastion host. Jest też drugi problem skoro istnieje możliwość uruchomienia usług omijających bastiona, możemy ulec pokusie i naciskom użytkowników, i uruchomić usługi które mogą się okazać niebezpieczne.



Rys. 1-F Schemat Screened Host Gateway

1.2.6.4 Screened Subnet Gateway



Rys. 1-G Schemat Screened Subnet Gateway

Konfiguracja ta polega na utworzeniu izolowanej podsieci pomiędzy naszą chronioną siecią a Internetem. Izolowanie tej podsieci stwarza dodatkowe możliwości zabezpieczeń przed włamaniami. Teraz, uzyskanie przez obcą osobę dostępu do bastiona nie oznacza zniszczenia całego firewalla, gdyż istnieje jeszcze drugi router. Nie wchodzi tu też w rachubę podsłuchanie tego, co się dzieje wewnątrz naszej sieci. Nie są także rozgłaszane ścieżki routingu. Przykład ten przypomina trochę konfigurację Dual Homed Gateway, przy czym jeden komputer jest tu zastąpiony całą dodatkową podsiecią. Dużą zaletą Screened Subnet Gateway jest możliwość umieszczania dodatkowych hostów wewnątrz strefy zdemilitaryzowanej, na których chcielibyśmy udostępnić pewne usługi niemile widziane na bastionie. Podobnie jak w poprzednio omawianej konfiguracji niektóre aplikacje uruchomione w prywatnej podsieci mogą komunikować się bezpośrednio z Internetem z ominięciem proxy. Wariant Screened Subnet Gateway jest obecnie najczęściej stosowany, jako reprezentujący najwyższy poziom bezpieczeństwa.

1.2.6.5 Podsumowanie

Wszystkie podane uprzednio konfiguracje firewalli są najczęściej wymieniane i proponowane. Nie są jednak jedyne - można sobie wyobrazić najrozmaitsze inne konfiguracje i hybrydy firewalli składających się na przykład z kilku bastionów, z połączenia bastiona z zewnętrznym routerem w jedną całość itp.

1.2.7 Problemy związane z filtrowaniem pakietów

Problemy z filtrowaniem pakietów wiążą się z przyjętą polityką bezpieczeństwa. Konfiguracja packet filter powinna uwzględniać przyjęte założenia dotyczące udostępnianych usług. Wspomnieliśmy uprzednio o konieczności bezbłędnej konfiguracji firewalla. Pamiętać należy, aby wszelkie odwołania do poszczególnych komputerów dotyczyły ich adresów IP, a nie ich nazw i domen. Gdy zaniedbamy to, uzdolniony hacker mógłby oszukać serwer DNS podstawiając fałszywe informacje i podszywając się pod jeden z zaufanych komputerów, co otworzyłoby mu drogę do zniszczenia firewalla (*DNS Spoofing Attack*).

Pakiety można filtrować na dwa sposoby:

- poprzez sprawdzanie adresu źródłowego i docelowego
- poprzez sprawdzanie portu, którego dotyczy połączenie.

Pierwsza metoda umożliwia wykrycie pakietów wyglądających na wysłane z naszej podsieci, a w rzeczywistości spreparowanych przez intruza (zmiana adresu źródła).

Niestety, gdy nasz firewall ufa pewnej grupie obcych komputerów, hacker może spróbować zmienić adres źródła na adres jednego z zaufanych komputerów (*Source Address Spoofing*). Nie będzie to wykryte przez nasz system ochrony[5].

Możliwe jest również dla hackera przekierowanie całego ruchu wchodzącego do naszej podsieci przez całkowicie obcy komputer poprzez zmianę ścieżek routingu. Dzięki temu mógłby on przeglądać każdy pakiet, w szczególności pakiety zawierające hasła *(Man in the Middle Attack)*.

Rozmaite problemy dotyczą też filtrowania przez numer portu. Podczas filtrowania pakietów sprawdzana jest regularnie flaga ACK (potwierdzenie w nagłówku pakietu). Przy nawiązywaniu wirtualnego połączenia TCP, pierwszy pakiet nie ma ustawionej tej flagi. Gdy połączenie inicjowane jest z naszej podsieci, na przykład na zdalny port 23, jednocześnie losowo tworzony jest port na naszym komputerze - może to być port 34567. Załóżmy, że pozwalamy na ruch pakietów na porcie 23 - pakiet wychodzący nie natrafia na żadną przeszkodę. Gdy po wirtualnym połączeniu nadchodzi pakiet z zewnątrz, kieruje się on na port 34567, który nie jest bezpiecznym portem. Normalnie pakiet ten zostałby odrzucony i połączenie nie mogłoby zostać poprawnie nawiązane. Istnieje jednak wspomniana flaga ACK, która, gdy jest ustawiona, pozwala na przepuszczenie pakietu dalej. W przypadku, w którym na zdalnym porcie 23 funkcjonowałaby inna usługa niż się spodziewamy, połączenie inicjowane z obcego komputera zostałoby odrzucone - flaga ACK nie zostałaby ustawiona. Tutaj uwidacznia się problem z protokołem UDP - nagłówek UDP nie posiada takiego pola kontrolnego i nie może być w prosty sposób przesłany przez firewall. Stąd często wszelkie usługi UDP nie są możliwe do zrealizowania. Problem ten nie zachodzi tylko wtedy, gdy połączenie odbywa się jednocześnie na tym samym porcie na obydwu komputerach.

Na inne trudności natrafiamy, gdy pakiet wysłany do nas z zewnątrz był zbyt duży i uległ fragmentacji. Pakiety powstałe z podziału nie niosą w sobie informacji na który port zostały skierowane (poza pierwszym). Czy taki pakiet dojdzie w dobrym stanie do docelowego komputera, to zależy od przyjętej taktyki. W mniej restrykcyjnym przypadku, każdy pakiet nie niosący informacji na jaki port został skierowany będzie przepuszczany dalej. Wówczas, gdy pierwszy pakiet zostanie odrzucony jako niepewny, dalsze jego fragmenty przejdą przez firewall i zostaną odrzucone dopiero przez docelowy komputer. Tyle mówi teoria, praktyka jednak trochę od niej odbiega. Można bowiem stworzyć sztucznie taki podział, by otrzymać bardzo małe fragmenty, w których po prostu zabraknie miejsca na część pierwotnego nagłówka - będzie się on znajdował w kilku fragmentach. Jest wówczas praktycznie możliwe przesłanie danych przez taki filtr który nie ma określonej najmniejszej możliwej wielkości pakietu (*Tiny Fragment Attack*). Innym

[5] tę metodę ataku zastosował Kevin Mitnick

sposobem na ominięcie odfiltrowania jest stworzenie takiej serii fragmentów, z której pierwszy zawierał będzie dane bezpieczne z punktu widzenia filtru, lecz następne będą miały możliwość przykrycia niektórych pól pakietu w trakcie łączenia się. W tym przypadku, kolejne fragmenty zmodyfikują nagłówek właściwego pakietu, same jednak przejdą bez problemów przez filtr. Nie są one bowiem widziane jako fragmenty z zerowym przesunięciem, a tylko takie mogą być odfiltrowane (*Overlapping Fragment Attack*).

Z protokołami TCP i UDP związany jest protokół kontroli ICMP. Może on służyć do ataku polegającego na niedopuszczeniu do użycia żadnej usługi (przykład *Denial of Service Attack*). Wysyłanie pakietu ICMP zawierającego informację o rzekomym przerwaniu połączenia istotnie je przerywało na starych typach systemów unixowych. Jednakże całkowita blokada pakietów ICMP wiąże się ze stratą wielu użytecznych informacji przesyłanych tą drogą.

Trzeba zwrócić uwagę także na inne protokoły, takie jak IP-over-IP, wykorzystywany przez MBONE (Multicast Backbone). Należy rozważyć zasadność blokowania bądź przepuszczania pakietów tego typu przez firewall.

1.3 Inne aspekty bezpieczeństwa

Pomimo istnienia firewalla, trzeba pomyśleć o logowaniu się do naszego systemu z zewnątrz. Problemem jest na przykład co zrobić, gdy nasz użytkownik pragnie rozpocząć pracę na naszym systemie z zewnątrz Internetu. Zezwolenie na to wiąże się z określonymi zagrożeniami. Po pierwsze, jego hasło może być przechwycone w podsieci z której się loguje (poprzez tzw. *sniffing*), co daje intruzowi bezpośredni dostępem do naszej sieci. Problem ten można rozwiązać poprzez przesyłanie wyłącznie zaszyfrowanych haseł. Inną metodą jest używanie jednorazowych haseł - najbardziej znanym systemem automatycznej zmiany haseł jest system S/Key. Stosuje się także czasowe samoczynne zmiany haseł - jest to specyficzny typ haseł zmieniających się co pewien czas poprzez algorytm znany systemowi oraz tak zwaną kartę użytkownika z której można odczytać hasło (*Time Based Passwords*).

Kolejnym zagrożeniem w takiej sytuacji jest możliwość przejęcia przez osobę nieuprawnioną połączenia już uwierzytelnionego - właściwa osoba traci połączenie, a zyskuje je włamywacz. Jednym ze sposobów na przeciwstawienia się takiej sytuacji jest ufanie, że zdalny system posiada przynajmniej takie same zabezpieczenia jak nasz - połączenia z innych systemów są blokowane. Można też szyfrować wszystkie połączenia (*End-to-end encryption*).

2. Praktyka

2.1 Projekt wstępny

Budowę bezpiecznej podsieci rozpoczęliśmy od wnikliwej analizy - odpowiedzi na trzy pytania: co w podsieci **jest/może być** niebezpieczne, co **powinniśmy** zrobić oraz co **możemy** uczynić, by zapewnić sieci bezpieczeństwo.

Pierwsze pytanie jest próbą określenia zagrożeń występujących w sieci - odpowiedź na nie pobudza do wygenerowania pewnej liczby rozwiązań (pytanie drugie). Trzecia kwestia sprowadza się praktycznie do przyziemnego pytania: **jakie są nasze uwarunkowania finansowe czyli na co nas stać?**

Wynik analizy znalazł wyraz w przyjętej (zgodnie z założeniami na wyrost) **polityce bezpieczeństwa**. Jako metodę realizacji polityki przyjęliśmy firewalla oraz pewną grupę aplikacji tworzących razem **bezpieczne środowisko sieciowe**.

Poniżej przedstawimy w kolejności: politykę bezpieczeństwa, wybraną konfigurację firewalla, zastosowane mechanizmy uwierzytelnienia, bezpieczne aplikacje oraz sprzęt, na którym postanowiliśmy eksperymentować.

2.1.1 Polityka bezpieczeństwa

Politykę bezpieczeństwa w formie dokumentu wydanego przez zespół zarządzający siecią (Załogę „G") przedstawiono w Dodatku A.

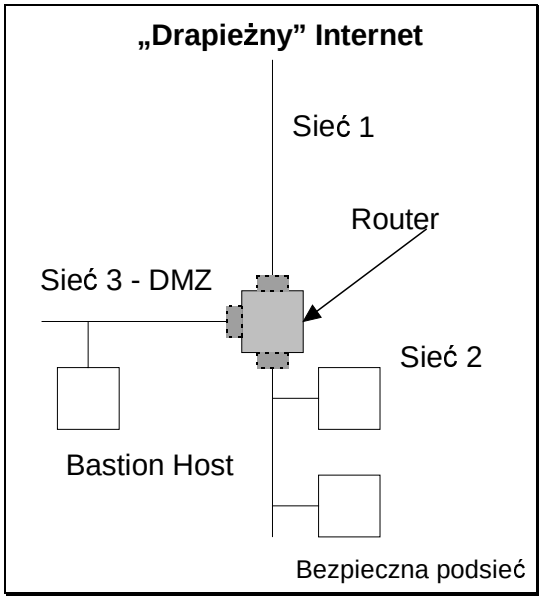
2.1.2 Konfiguracja firewalla

Wybrana została zmodyfikowana konfiguracja **screened subnet gateway**. Modyfikacja polega na zastąpieniu dwóch routerów jednym, posiadającym trzy interfejsy sieciowe.

Tak zbudowany system oferuje największe bezpieczeństwo, przy stosunkowo niewielkich nakładach sprzętowych.

Rysunek obok przedstawia proponowaną konfigurację:

- Sieć 1 - utożsamia „drapieżny" Internet,
- Sieć 2 - jest bezpieczną podsiecią,
- Sieć 3 - jest strefą zdemilitaryzowaną z bastion hostem oferującym serwisy proxy,
- Router - jest „prześwietlającym" (filtrującym) pakiety routerem.



Rys. 2-A Schemat sieci

Jeszcze raz przypomnijmy zalety takiego systemu:

- „wtargnięcie” do bastion hosta nie oznacza zniszczenia całego firewalla - nie jest możliwa obserwacja ruchu wewnątrz Sieci 2,
- oferowanie w DMZ różnych usług kłopotliwych do filtrowania,
- możliwość ukrycia informacji o nazwach maszyn (fake DNS) w Sieci 2,
- elastyczność konfiguracji systemu - wybrane usługi mogą omijać Sieć 3 i komunikować się bezpośrednio z Internetem.

2.1.3 Filtrowanie pakietów i Application Gateway[6]

Obowiązuje reguła *default deny* (domyślnie zabronione) jako realizacja wyrażonego w polityce bezpieczeństwa założenia: „co nie jest wyraźnie dozwolone - jest zakazane”. Poszczególne przewidziane w polityce bezpieczeństwa do udostępnienia usługi są odblokowywane i „przepuszczane” w następujący sposób:

Usługa	Sposób wejścia do podsieci	Sposób wyjścia z podsieci
TELNET	poprzez proxy	bezpośrednio lub poprzez proxy
FTP	poprzez proxy	bezpośrednio lub poprzez proxy
WWW (http)	brak możliwości	bezpośrednio lub poprzez proxy
SMTP (e-mail)	poprzez proxy	poprzez proxy
traceroute, ping, finger	brak możliwości	poprzez proxy
IRC	brak możliwości	bezpośrednio lub poprzez proxy
X11	brak możliwości	poprzez proxy

DNS jest realizowany na dwóch serwerach - jeden w Sieci 3 (DMZ), drugi w Sieci 2 - w taki sposób, że zapytania ze strony Sieci 1 (Internetu) są kierowane do DMZ i udzielane odpowiedzi nie zdradzają konfiguracji[7] bezpiecznej podsieci.

Podobna sytuacja dotyczy mail-exchangera (MX) - poczta przychodząca z Internetu jest odbierana w DMZ i przekazywana do wyróżnionego MX w bezpiecznej podsieci. Chroni to przed atakiem na systemy MX bezpiecznej podsieci[8].

2.1.4 Mechanizmy uwierzytelnienia

Użytkownicy łączący się z bezpieczną podsiecią ze strony Internetu (usługi TELNET i FTP) będą uwierzytelniani przy pomocy systemu haseł jednorazowych S/Key.

2.1.5 Fundamenty

System będzie budowany w oparciu o:

- TIS FWTK version 2.0α (Firewall Toolkit)

[6] application gateway jest maszyną, na której uruchomione są proxy
[7] nazw maszyn
[8] możliwym do przeprowadzenia jedynie po ewentualnym „wtargnięciu” do bastiona

- oprogramowanie umożliwiające filtrowanie pakietów - IPfilter version 3.04β,
- zmodyfikowany[9] pakiet S/Key,
- inne własne oprogramowanie.

2.1.6 Inne oprogramowanie

Planuje się wykorzystać dostępne w Internecie oprogramowanie public domain, gnu, freeware, shareware w tym:

- Netscape Atlas version 3.02β,
- Pretty Good Privacy version 2.6.3i,
- oraz standardowe aplikacje umieszczone w pakietach dystrybucyjnych FreeBSD i Solaris 2.4.

2.1.7 Sprzęt

Router:

PC 386 SX-16 - 8 MB RAM - dysk SCSI 340 MB - z trzema interfejsami sieciowymi zgodnymi ze standardem Ethernet - pracujący pod kontrolą systemu FreeBSD 2.1-0 Release,

Bastion host:

PC 486 DX-33 - 16 MB RAM - dysk SCSI 340 MB - z jednym interfejsem sieciowym zgodnym ze standardem Ethernet - pracujący pod kontrolą systemu FreeBSD 2.1-0 Release,

Host:

Sun IPC - 16 MB RAM - dysk SCSI 400 MB - z jednym interfejsem sieciowym zgodnym ze standardem Ethernet - pracujący pod kontrolą systemu Solaris 2.4 (Sun OS 5.4).

2.2 Rezultat

Bezpieczną podsieć zorganizowano w pracowni 331 (w budynku Wydziału Elektroniki i Technik Informacyjnych).

Po wielu perypetiach - sprzęt, protokół RIP i demon routed - system zaczął działać (!!!).

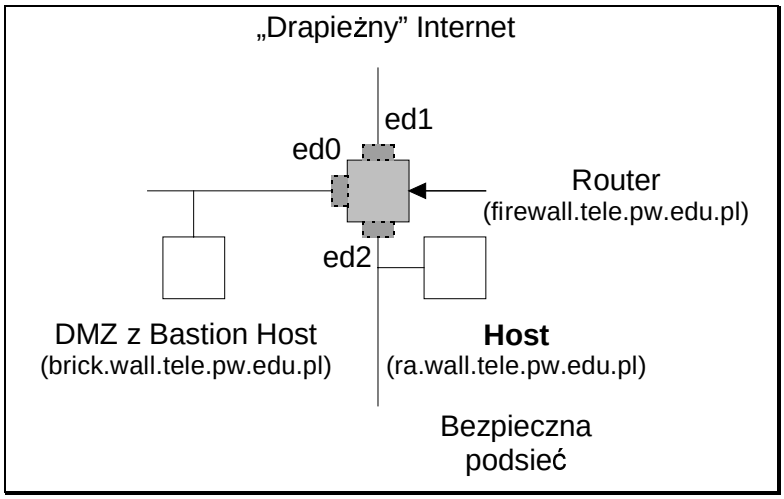
2.2.1 Jak to działa?

Poniżej przedstawiono sposób działania poszczególnych elementów zbudowanego systemu.

[9] użyto funkcji skrótu MD5, gdyż użyta w oryginalnej implementacji funkcja MD4 została złamana

2.2.1.1 Filtrowanie

W przyjętej przez nas konfiguracji (Screened Subnet Gateway), jak już wspomnieliśmy, teoretycznie powinny znaleźć się dwa routery - jeden na styku pomiędzy Internetem a DMZ, drugi na styku między DMZ a bezpieczną podsiecią. Z braku sprzętu zmodyfikowaliśmy „wzorcową" konfigurację - zbudowaliśmy „podwójny" router z trzema kartami sieciowymi (oznaczonymi wg. rysunku ed0, ed1, ed2) - zablokowaliśmy możliwość przepływu pakietów między ed1 a ed2.



Rys. 2-B Interfejsy sieciowe

Wygenerowaliśmy także szereg zasad pozwalających routerowi na „przesiewanie" przechodzących przez niego informacji na stykach ed1-ed0 oraz ed0-ed2. Zasady (rulesets) mają na celu właściwe określenie, które pakiety mogą zostać przepuszczone do bezpiecznej podsieci. wszystkie inne, a które - o wątpliwym przeznaczeniu - powinny zostać zatrzymane.

Istnieją oczywiście różnice pomiędzy zasadami określonymi dla tych dwóch styków. Do DMZ może dostać się dużo więcej pakietów niż do bezpiecznej podsieci.

2.2.1.1.1 Styk ed1 - ed0

Poniżej w formie tabeli przedstawiono reguły dla styku ed1-ed0.

Usługa	Kier.	Prot.	Akcja	Skąd	Port	Dokąd	Port	ACK
RIP	we	udp	puść	router	>1023	rt. ZTiT	520	-
RIP	wy	udp	puść	rt. ZTiT	520	router	>1023	-
RIP	wy	udp	puść	rt. ZTiT	>1023	router	520	-
RIP	we	udp	puść	rt. ZTiT	520	router	>1023	-
RIP	we	udp	puść	router	520	rt. ZTiT	520	-
RIP	wy	udp	puść	rt. ZTiT	520	sieć buf.	520	-
telnet	we	tcp	puść	podsieć	>1023	*	23	-
telnet	wy	tcp	puść	*	23	podsieć	>1023	+
FTP	wy	tcp	puść	podsieć	>1023	*	21	-
FTP	we	tcp	puść	*	21	podsieć	>1023	+
FTP	wy	tcp	puść	podsieć	>1023	*	>1023	-
FTP	we	tcp	puść	*	>1023	podsieć	>1023	+
FTP	wy	tcp	puść	bastion	>1023	*	21	-
FTP	we	tcp	puść	*	21	bastion	>1023	+
FTP	we	tcp	blokuj	*	20	bastion	6000-9	-
FTP	we	tcp	puść	*	20	bastion	>1023	-

FTP	wy	tcp	puść	bastion	>1023	*	20	+
FTP	we	tcp	puść	*	>1023	bastion	21	-
FTP	wy	tcp	puść	bastion	21	*	>1023	+
FTP	wy	tcp	puść	bastion	20	*	>1023	-
FTP	we	tcp	puść	*	>1023	bastion	20	+
FTP	we	tcp	puść	*	>1023	bastion	>1023	-
FTP	wy	tcp	puść	bastion	>1023	*	>1023	-
SMTP	wy	tcp	puść	bastion	>1023	*	25	-
SMTP	we	tcp	puść	*	25	bastion	>1023	+
SMTP	we	tcp	puść	*	>1023	bastion	25	-
SMTP	wy	tcp	puść	bastion	25	*	>1023	+
HTTP	wy	tcp	puść	bastion	>1023	*	*	-
HTTP	we	tcp	puść	*	*	bastion	>1023	+
HTTP	we	tcp	puść	*	>1023	bastion	80	-
HTTP	wy	tcp	puść	bastion	80	*	>1023	+
DNS	wy	udp	puść	bastion	53	*	53	-
DNS	we	udp	puść	*	53	bastion	53	-
DNS	we	udp	puść	*	*	bastion	53	-
DNS	wy	udp	puść	bastion	53	*	*	-
DNS	wy	tcp	puść	bastion	>1023	*	53	+
DNS	we	tcp	puść	*	53	bastion	>1023	+
DNS	we	tcp	puść	*	>1023	bastion	53	-
DNS	wy	tcp	puść	bastion	53	*	>1023	+
spoof	we	*	blokuj	podsieć	*	*	*	-

- wszystkie wyjściowe pakiety nieobjęte innymi zasadami są blokowane
- wszystkie wejściowe pakiety nieobjęte innymi zasadami są blokowane

```
block in on ed1 all
block out on ed1 all
```

- porty na których odbywa się wymiana informacji o ścieżkach routingu (RIP) są odblokowane dla ruchu pakietów UDP, ale tylko pomiędzy naszym routerem o adresie 148.81.65.65 a routerem novellowym podsieci ZTiT.

```
pass in on ed1 proto udp from 148.81.65.65 port gt 1023 to 148.81.65.79 port =
520
pass out on ed1 proto udp from 148.81.65.79 port = 520 to 148.81.65.65 port gt
1023
pass out on ed1 proto udp from 148.81.65.79 port gt 1023 to 148.81.65.65 port =
520

pass in on ed1 proto udp from 148.81.65.79 port = 520 to 148.81.65.65 port gt
1023
pass in on ed1 proto udp from 148.81.65.65 port = 520 to 148.81.65.79 port = 520
pass out on ed1 proto udp from 148.81.65.79 port = 520 to
148.81.65.64/255.255.255.192 port = 520
```

- bezpośredni TELNET jest usługą, na którą zezwalamy, ale inicjowany może być jedynie z chronionej podsieci na zewnątrz - przepuszczamy więc pakiety TCP z naszej podsieci z portów większych od 1023 idące do zdalnego portu 23, oraz pakiety z zewnętrznego portu 23 na porty >1023, ale z ustawioną flagą ACK.

```
pass out on ed1 proto tcp from 148.81.65.56/255.255.255.248 port gt 1023 to any
port = 23
pass in on ed1 proto tcp from any port = 23 to 148.81.65.56/255.255.255.248 port
gt 1023 flags A/A
```

- FTP: pozwalamy na komunikację serwerów z naszej podsieci z serwerami zewnętrznymi na zdalnym porcie 21, inicjowaną tylko z naszej podsieci (ustawiona flaga ACK). Pozwalamy także na "pasywny" przepływ danych na wszystkich portach powyżej 1023, wybór portu musi się dokonać w naszej podsieci - flaga ACK.

```
pass out on ed1 proto tcp from 148.81.65.56/255.255.255.248 port gt 1023 to any
port = 21
pass in on ed1 proto tcp from any port = 21 to 148.81.65.56/255.255.255.248 port
gt 1023 flags A/A
pass out on ed1 proto tcp from 148.81.65.56/255.255.255.248 port gt 1023 to any
port gt 1023
pass in on ed1 proto tcp from 148.81.65.56/255.255.255.248 port gt 1023 to any
port gt 1023 flags A/A
```

- dla potrzeb FTP proxy, pozwalamy także bastionowi na połączenia na porcie 21 z serwerami zewnętrznymi

```
pass out on ed1 proto tcp from 148.81.65.50 port gt 1023 to any port = 21
pass in on ed1 proto tcp from any port = 21 to 148.81.65.50 port gt 1023 flags
A/A
```

- pozwalamy także na połączenia zewnętrzne z bastionem, na portach powyżej 1023 z wyłączeniem 6000-6009, które nie są pewne ze względu na serwery X11.

```
block in on ed1 proto tcp from any port = 20 to 148.81.65.50 port 5999 >< 6010
pass in on ed1 proto tcp from any port = 20 to 148.81.65.50 port > 1023
pass out on ed1 proto tcp from 148.81.65.50 port > 1023 to any port = 20 flags
A/A
```

- zewnętrzne serwery mogą też inicjować połączenia tak w trybie pasywnym jak i normalnym z anonymous-ftpd na bastionie (148.81.65.50). Dla tych zasad nie ma odpowiedników na "wewnętrznym" styku, gdyż wewnątrz chronionej podsieci nie zezwala się na anonymous ftp podobnie jak i a serwer WWW).

```
pass in on ed1 proto tcp from any port > 1023 to 148.81.65.50 port = 21
pass out on ed1 proto tcp from 148.81.65.50 port = 21 to any port > 1023 flags
A/A
pass out on ed1 proto tcp from 148.81.65.50 port = 20 to any port > 1023
pass in on ed1 proto tcp from any port > 1023 to 148.81.65.50 port = 20 flags
A/A
pass in on ed1 proto tcp from any port > 1023 to 148.81.65.50 port > 1023
pass out on ed1 proto tcp from 148.81.65.50 port > 1023 to any port > 1023
```

- wszelkie usługi pocztowe, odbywające się na porcie 25, są dozwolone tylko pomiędzy światem zewnętrznym a bastion-hostem wewnątrz podsieci buforowej.

```
pass out on ed1 proto tcp from 148.81.65.50 port > 1023 to any port = 25
pass in on ed1 proto tcp from any port = 25 to 148.81.65.50 port > 1023 flags
A/A
pass in on ed1 proto tcp from any port > 1023 to 148.81.65.50 port = 25
```

```
pass out on ed1 proto tcp from 148.81.65.50 port = 25 to any port > 1023 flags
A/A
```

- dwie kolejne zasady pozwalają na połączenia http-proxy z bastiona na wszystkie zewnętrzne serwery WWW. Następne dwie pozwalają na ruch pakietów http z Internetu do serwera WWW zainstalowanego na bastionie. Nie zezwala się na połączenia bezpośrednie z podsieci na zewnątrz.

```
pass out on ed1 proto tcp from 148.81.65.50 port > 1023 to any
pass in on ed1 proto tcp from any to 148.81.65.50 port > 1023 flags A/A
pass in on ed1 proto tcp from any port > 1023 to 148.81.65.50 port = 80
pass out on ed1 proto tcp from 148.81.65.50 port = 80 to any port > 1023 flags
A/A
```

- poważnym problemem jest ruch między serwerami DNS. Generalnie zezwala się na połączenia typu UDP serwerów DNS oraz klientów z Internetu z bastionem, na którym działa DNS-serwer. Także połączenia TCP bastiona z Internetem są dozwolone.

```
pass out on ed1 proto udp from 148.81.65.50 port = 53 to any port = 53
pass in on ed1 proto udp from any port = 53 to 148.81.65.50 port = 53
pass in on ed1 proto udp from any to 148.81.65.50 port = 53
pass out on ed1 proto udp from 148.81.65.50 port = 53 to any
pass out on ed1 proto tcp from 148.81.65.50 port > 1023 to any port = 53
pass in on ed1 proto tcp from any port = 53 to 148.81.65.50 port > 1023 flags
A/A
pass in on ed1 proto tcp from any port > 1023 to 148.81.65.50 port = 53
pass out on ed1 proto tcp from 148.81.65.50 port = 53 to any port > 1023 flags
A/A
```

- blokujemy WSZELKIE połączenia mogące świadczyć o chęci ataku na naszą podsieć poprzez spoofing - podszycie się innego komputera za któryś z naszej podsieci - blokujemy więc połączenia od komputerów zgłaszających się numerami naszych komputerów

```
block in on ed1 from 148.81.65.48/255.255.255.240 to any
```

Tu kończą się reguły dla "zewnętrznej" części routera. W drugiej części zajmiemy się zasadami określonymi dla routingu pakietów pomiędzy DMZ a bezpieczną podsiecią.

2.2.1.1.2 Styk ed0 - ed2

Poniżej w formie tabeli przedstawiono reguły dla styku ed0-ed2.

Usługa	Kier.	Prot.	Akcja	Skąd	Port	Dokąd	Port	ACK
RIP	we	udp	puść	podsieć	>1023	router	520	-
RIP	wy	udp	puść	router	520	podsieć	>1023	-
RIP	wy	udp	puść	router	>1023	podsieć	520	-
RIP	we	udp	puść	router	520	podsieć	>1023	-
RIP	we	udp	puść	podsieć	520	router	520	-
RIP	wy	udp	puść	router	520	podsieć	520	-
telnet	we	tcp	puść	podsieć	>1023	*	23	-
telnet	wy	tcp	puść	*	23	podsieć	>1023	+

FTP	we	tcp	puść	podsieć	>1023	*	21	-
FTP	wy	tcp	puść	*	21	podsieć	>1023	+
FTP	we	tcp	puść	podsieć	>1023	*	>1023	-
FTP	wy	tcp	puść	*	>1023	podsieć	>1023	+
FTP	we	tcp	puść	podsieć	>1023	bastion	21	-
FTP	wy	tcp	puść	bastion	21	podsieć	>1023	+
FTP	wy	tcp	puść	bastion	>1023	podsieć	>1023	-
FTP	we	tcp	puść	podsieć	>1023	bastion	>1023	+
FTP	wy	tcp	blokuj	bastion	*	podsieć	6000-9	-
SMTP	wy	tcp	puść	podsieć	>1023	bastion	25	-
SMTP	we	tcp	puść	bastion	25	podsieć	>1023	+
SMTP	we	tcp	puść	bastion	>1023	podsieć	25	-
SMTP	wy	tcp	puść	podsieć	25	bastion	>1023	+
HTTP	we	tcp	puść	podsieć	>1023	bastion	80	-
HTTP	wy	tcp	puść	bastion	80	podsieć	>1023	-
DNS	we	udp	puść	podsieć	53	bastion	53	-
DNS	we	tcp	puść	podsieć	>1023	bastion	53	-
DNS	wy	udp	puść	bastion	53	podsieć	53	-
DNS	wy	tcp	puść	bastion	53	podsieć	>1023	+
DNS	wy	udp	puść	bastion	>1023	podsieć	53	-
DNS	wy	tcp	puść	bastion	>1023	podsieć	53	-
DNS	we	udp	puść	podsieć	53	bastion	>1023	-
DNS	we	tcp	puść	podsieć	53	bastion	>1023	+

- standardowo wszelki ruch pakietów jest zabroniony, poza następującymi:

```
block in on ed2 all
block out on ed2 all
```

- reguły dla protokołu routingu - RIP.

```
pass in on ed2 proto udp from 148.81.65.56/255.255.255.248 port gt 1023 to
148.81.65.57 port = 520
pass out on ed2 proto udp from 148.81.65.57 port = 520 to
148.81.65.56/255.255.255.248 port gt 1023
pass out on ed2 proto udp from 148.81.65.57 port gt 1023 to
148.81.65.56/255.255.255.248 port = 520

pass in on ed2 proto udp from 148.81.65.57 port = 520 to
148.81.65.56/255.255.255.248 port gt 1023
pass in on ed2 proto udp from 148.81.65.56/255.255.255.248 port = 520 to
148.81.65.63 port = 520
pass out on ed2 proto udp from 148.81.65.57 port = 520 to
148.81.65.56/255.255.255.248 port = 520
```

- pozwalamy na połączenia typu TELNET z naszej podsieci na zewnątrz, przy czym przyjmujemy z powrotem tylko pakiety posiadające ustawioną flagę ACK.

```
pass in on ed2 proto tcp from 148.81.65.56/255.255.255.248 port > 1023 to any
port = 23
pass out on ed2 proto tcp from any port = 23 to 148.81.65.56/255.255.255.248
port > 1023 flags A/A
```

- pozwalamy na bezpośrednie FTP inicjowane z naszej podsieci na zewnątrz.

```
pass in on ed2 proto tcp from 148.81.65.56/255.255.255.248 port > 1023 to any
port = 21
pass out on ed2 proto tcp from any port = 21 to 148.81.65.56/255.255.255.248
port > 1023 flags A/A
```

- pozwalamy także na zdalne przesyłanie plików lecz tylko w trybie pasywnym, czyli z wyborem portu przez nasz komputer.

```
pass in on ed2 proto tcp from 148.81.65.56/255.255.255.248 port > 1023 to any
port > 1023
pass out on ed2 proto tcp from any port > 1023 to 148.81.65.56/255.255.255.248
port > 1023 flags A/A
```

- jeśli zewnętrzny komputer nie posiada możliwości działania w trybie pasywnym, można skorzystać z proxy na bastionie, na co pozwalają kolejne reguły

```
pass in on ed2 proto tcp from 148.81.65.56/255.255.255.248 port > 1023 to
148.81.65.50 port = 21
pass out on ed2 proto tcp from 148.81.65.50 port = 21 to
148.81.65.56/255.255.255.248 port > 1023 flags A/A
pass out on ed2 proto tcp from 148.81.65.50 port > 1023 to
148.81.65.56/255.255.255.248 port > 1023
pass in on ed2 proto tcp from 148.81.65.56/255.255.255.248 port > 1023 to
148.81.65.50 port > 1023 flags A/A
```

- standardowo zablokowane jest połączenie na portach 6000-6009 z powodów wymienionych wyżej.

```
block out on ed2 proto tcp from 148.81.65.50 to 148.81.65.56/255.255.255.248
port 5999 >< 6010
```

- wewnątrz chronionej podsieci zezwala się na połączenia pocztowe tylko pomiędzy komputerami z naszej podsieci a bastion hostem, który jest jednocześnie mail-exchangerem dla niej.

```
pass out on ed2 proto tcp from 148.81.65.56/255.255.255.248 port > 1023 to
148.81.65.50 port = 25
pass in on ed2 proto tcp from 148.81.65.50 port = 25 to
148.81.65.56/255.255.255.248 port > 1023 flags A/A
pass in on ed2 proto tcp from 148.81.65.50 port > 1023 to 148.81.65.60 port = 25
pass out on ed2 proto tcp from 148.81.65.60 port = 25 to 148.81.65.50 port >
1023 flags A/A
```

- pozwalamy na ruch pakietów http tylko przez proxy zainstalowane na porcie 80 bastion hosta.

```
pass in on ed2 proto tcp from 148.81.65.56/29 port > 1023 to 148.81.65.50 port =
80
pass out on ed2 proto tcp from 148.81.65.50 port = 80 to 148.81.65.56/29 port >
1023
```

- DNS jest tak skonfigurowany, aby przepuszczać do wewnątrz podsieci wszystkie informacje o nazwach domen poza naszą podsiecią, blokując jednocześnie informacje o prawdziwych nazwach istniejących wewnątrz podsieci.

```
pass in on ed2 proto udp from 148.81.65.60 port = 53 to 148.81.65.50 port = 53
pass in on ed2 proto tcp from 148.81.65.60 port > 1023 to 148.81.65.50 port = 53
pass out on ed2 proto udp from 148.81.65.50 port = 53 to 148.81.65.60 port = 53
pass out on ed2 proto tcp from 148.81.65.50 port = 53 to 148.81.65.60 port >
1023 flags A/A
pass out on ed2 proto udp from 148.81.65.50 port > 1023 to 148.81.65.60 port =
53
pass out on ed2 proto tcp from 148.81.65.50 port > 1023 to 148.81.65.60 port =
53
pass in on ed2 proto udp from 148.81.65.60 port = 53 to 148.81.65.50 port > 1023
pass in on ed2 proto tcp from 148.81.65.60 port = 53 to 148.81.65.50 port > 1023
flags A/A
```

Pozwalamy na ruch pakietów na urządzeniu ed0, gdyż wszelkie reguły zostały już określone dla dwóch pozostałych urządzeń wyjściowych.

```
pass in on ed0 all
pass out on ed0 all
```

2.2.1.2 Proxy

Plikiem konfiguracyjnym usług proxy jest **/usr/local/etc/netperm-table**. Wszystkie usługi są chronione przy pomocy zgrabnego (tylko 200 linii) TCP-wrappera - o nazwie netacl (**net**work **a**ccess **c**contro**l**). Dzięki netacl jest możliwa logiczna zmiana katalogu (chroot).

2.2.1.2.1 FTP - ftp-gw

Ftp-gw kontroluje dostęp do zasobów poprzez analizę adresów docelowych IP i nazw maszyn. Umożliwia blokowanie poszczególnych komend ftp oraz pełne logowanie sesji. Dzięki ftp-gw użytkownicy z bezpiecznej podsieci mogą łączyć się z zewnętrznymi serwerami nie mającymi wsparcia dla passive mode. Ftp-gw współpracuje z opisanym w dalszej części systemem uwierzytelniającym - authd.

2.2.1.2.2 TELNET - tn-gw

Tn-gw jest funkcjonalnie podobne do ftp-gw. Przy telnecie następuje chroot. Tn-gw został napisany w sposób niezwykle ascetyczny - nie komunikuje się z żadnymi dodatkowymi procesami poza authd.

2.2.1.3 SMTP

Sendmail jest najpopularniejszym programem pocztowym dla systemu UNIX - realizującym protokół SMTP (Simple Mail Transfer Protocol). Z kilku powodów sendmail jest uznawany za twór niebezpieczny[10]:

- jest potwornie skomplikowany,
- realizuje wiele różnorodnych funkcji i wymaga zbioru praw niezbędnych do ich zrealizowania.

W zbudowanym przez nas firewallu na bastione zamiast sendmaila umieściliśmy smapa z pakietu TIS FWTK. Smap jest bardzo krótkim programem[11]

[10] inne dostępne systemy pocztowe takie jak - smail 3, MMDF, Z-Mail - wcale nie są bezpieczniejsze

przechwytującym zewnętrzne połączenia SMTP, jest uruchamiany z poziomu inetd bez uprawnień roota.

Poczta wychodząca z podsieci ma usuniętą ścieżkę informującą skąd dokładnie pochodzi - wygląda tak jakby została nadana z bastiona (z brick.wall.tele.pw.edu.pl).

2.2.1.4 DNS - serwery nazw domen

Zastosowany został dosyć sprytny rodzaj konfiguracji DNSa. Nie jest bowiem wskazane, aby każdy, kto tylko chce został z zewnątrz poinformowany o nazwach komputerów znajdujących się wewnątrz naszej podsieci. Funkcjonują więc obok siebie **dwa serwery nazw domen** - jeden na bastionie (tzw. fake server) - uznawany przez resztę świata za jedyny i prawidłowy, drugi zaś - wewnątrz chronionej podsieci (tzw. real server).

Serwer na bastionie odpowiada na zapytania z zewnątrz ukrywając prawdziwe nazwy komputerów (stąd nazwa fake) - sam zaś otrzymuje niezbędne informacje o nazwach komputerów w Internecie.

Właściwym serwerem (stąd nazwa real), znającym prawdziwe nazwy komputerów, jest serwer znajdujący się wewnątrz bezpiecznej podsieci. Jego klientami są zarówno komputery z bezpiecznej podsieci, jak i bastion (który powinien znać wszystkie te nazwy choćby do zestawiania połączenia). Bastion prowadzi swój DNS serwer, lecz on sam nie jest jego klientem. Potrzebny jest on jednakże nie tylko po to, by podawać światu fałszywe dane, lecz także by służyć prawdziwemu serwerowi danymi o hostach z zewnątrz.

Rozwiązanie takie funkcjonuje i sprawuje się doskonale. Wszystkie komputery z chronionej podsieci widziane są z zewnątrz jako ***unknown.wall.tele.pw.edu.pl***.

Pliki konfiguracyjne „przekłamującego" serwera i „prawdziwego" serwera przedstawiono w dodatku B.

2.2.1.5 S/Key jako metoda uwierzytelnienia

*„bezradność poranka / **jednorazowy** kubek/ zapach kawy"*

2.2.1.5.1 Jednorazowe hasło = Wieczne bezpieczeństwo

Metoda **prostego uwierzytelnienia** użytkownika względem hosta[12] przy pomocy haseł jednorazowych została zaproponowana przez Neila Hallera z Bellcore [Haller95] i nosi nazwę **The S/Key One-Time Password System**. Oparta na funkcji skrótu technika, mimo że jest prosta w implementacji i niekłopotliwa w użyciu, skutecznie **chroni przed atakiem powtórzenia**. Wykorzystaliśmy ją jako metodę uwierzytelnienia zewnętrznych zgłoszeń (poprzez demona authd z TIS FWTK).

[11] składa się z 700 linii, podzcas gdy sendmail z 30.000!!!
[12] podczas logowania się

2.2.1.5.2 Generacja jednorazowego hasła

Najpierw wyznacza się Skrót=f(ziarno||hasło), gdzie f jest mocną funkcją skrótu, natomiast *ziarno* jest jawną wartością ustalaną przez hosta, umożliwiająca użytkownikowi korzystanie z tego samego *hasła* na różnych maszynach[13].

Pierwsze hasło jednorazowe wylicza się poddając *Skrót* N-razy funkcji skrótu - $f^N(\text{Skrót})$[14], następne hasło jako $f^{N-1}(\text{Skrót})$ itd. N jest wartością jawną ustalaną przez użytkownika albo hosta.

2.2.1.5.3 Weryfikacja jednorazowego hasła

Intruz obserwujący sieć nie będzie w stanie wygenerować właściwego jednorazowego hasła, będzie mógł jedynie sprawdzić (podobnie jak host) prawdziwość posiadanego. Weryfikacja polega na sprawdzeniu czy skrót odebranego hasła odpowiada poprzedniemu hasłu.

2.2.1.5.4 Implementacja Bellcore S/Key

Oryginalna implementacja Bellcore[15] przeznaczona dla systemu UNIX opiera się na złamanej niedawno funkcji skrótu MD4. W bezpiecznej podsieci zaimplementowano funkcję MD5.

Jednorazowe hasła generowane przez Bellcore S/Key są 64-bitowe - 128-bitowy skrót MD4 (także MD5) jest dzielony na połowy i tak otrzymane części są poddawane działaniu XOR. Aby ułatwić użycie systemu - ukryć metodę przed przeciętnym użytkownikiem, dla którego 64-bitowa liczba nie wygląda atrakcyjnie - hasła są konwertowane do postaci czytelnej dla człowieka. Czytelne hasła składają się z sześciu krótkich (od 1 do 4 znaków) angielskich słów wybranych ze słownika zawierającego 2048 wyrazów (wzorcowy przedstawiono w [Haller95]). Dostępne są programy (tzw. kalkulatory) dla systemów UNIX, DOS, a także applety w języku Java[16], wyznaczające te hasła. Kalkulatory mogą posłużyć do wygenerowania listy jednorazowych haseł na czas podróży.

Przykład haseł jednorazowych:
LOOK AT ME NICE NUDE DES
HEAT SUN DRY FACE WET HAND
LOVE YOU KICK HER KILL HIM

2.2.2 Jak można z tego korzystać - czyli podręcznik użytkownika

W tej części przedstawimy sposoby korzystania z usług dostępnych w bezpiecznej podsieci.

[13] co oczywiście nie jest bezpieczne, ale niestety powszechne nawet wśród administratorów

[14] formalnie można zapisać to korzystając z rekurencji: $\forall_{M} \forall_{n \in N \wedge n>1} f^n(M) = f(f^{n-1}(M))$

[15] dostępna w sieci Internet pod adresem `ftp://ftp.bellcore.com` - ścieżka `/pub/nmh/skey`

[16] http://www.tele.pw.edu.pl/~kszczypi/jotp.html

2.2.2.1 Korzystanie z FTP

Połączenie się z wybranym serwerem FTP spoza bezpiecznej podsieci **poprzez proxy** jest niezwykle proste. Wydajemy komendę:

```
ftp brick.wall.tele.pw.edu.pl
```

Po połączeniu się z proxy jesteśmy proszeni o podanie nazwy użytkownika i hosta, do którego chcemy się dostać:

```
ftp brick.wall.tele.pw.edu.pl
220 brick FTP proxy (Version 2.0 alpha) ready.
Name (brick:citcom01): anonymous@ftp.lamesite.org.pl
331- (----GATEWAY CONNECTED TO ftp.lamesite.org.pl----)
331- (220 ftp.lamesite.org.pl FTP server (Some OS) ready.)
331 Guest login ok, send ident as password
Password: #######
230 Guest login ok, access restrictions apply.
ftp>dir
...
```

Połączenie się z serwerem FTP wewnątrz bezpiecznej podsieci **poprzez proxy** jest również niezwykle proste. Wydajemy komendę:

```
ftp brick.wall.tele.pw.edu.pl
```

Po połączeniu się z proxy jesteśmy proszeni o podanie nazwy użytkownika i hosta, do którego chcemy się dostać:

```
ftp brick.wall.tele.pw.edu.pl
Connected to brick.wall.tele.pw.edu.pl
220-Before using the proxy you must first authenticate
220 brick FTP proxy (Version 2.0 alpha) ready.
Name (brick:citcom01):
331- ID citcom01 s/key is 265 at997666:LOOK AT ME NICE NUDE DES
230 User authenticated to proxy
ftp>user citcom01@ra
331- (----GATEWAY CONNECTED TO ra----)
331 Password required for citcom01.
Password: ########
230 User citcom01 logged in.
ftp>
...
```

2.2.2.2 Korzystanie z TELNET

Korzystanie z TELNET **poprzez proxy** jest również nieuciążliwe. Wydajemy komendę:

```
telnet brick.wall.tele.pw.edu.pl
Trying 148.81.65.50
Connected to brick.wall.tele.pw.edu.pl
Escape character is '^}'.
tn-gw->c neutron.elka.pw.edu.pl
...
```

2.2.2.3 Zmiana haseł poprzez proxy

Zmiana hasła polega na:

```
Trying 148.81.65.50
Connected to brick.wall.tele.pw.edu.pl
Escape character is '^}'.
tn-gw->pass
Changing passwords
Enter Username: citcom01
331- ID citcom01 s/key is 264 at680213:HEAT SUN DRY FACE WET HAND
New Password: ########
Repeat New Password: ########
ID citcom01 s/key is 666 at960703
tn-gw->quit
...
```

2.2.2.4 Korzystanie z WWW

Polega wyłącznie na odpowiednim skonfigurowaniu programu Netscape (pole Proxy w Options).

2.2.2.5 Korzystanie z finger, traceroute, ping

Na porcie 69 został umieszczony serwer świadczący te usługi - wywołanie poprzez:

```
telnet brick.wall.tele.pw.edu.pl 69.
```

Literatura

[Chapma92] - D. Brent Chapman, Network (in)security through IP packet filtering, In Proceedings of the Third Usenix UNIX Security Symposium, p. 63-76, Baltimore, MD, 1992

[Chapma95] - D. Brent Chapman, Elizabeth D. Zwicky, Building Internet Firewalls, O'Reilly & Associates Inc., 1995

[Cheswi94] - William R. Cheswick, Steven M. Bellovin, Firewalls and Internet Security, Addison-Wesley Publishing Company, 1994

[FIPS112] - Federal Information Processing Standards Publication - Password Usage - FIPS 112, May 1985

[FIPS191] - Federal Information Processing Standards Publication - Guideline for The Analysis Local Area Network Security - FIPS 191, November 1994

[Haller95] - N. Haller - The S/KEY One-Time Password System, RFC 1760, February 1995

[Ranum93] - Marcus J. Ranum, Thinking About Firewalls, Trusted Information Systems, Inc.

[Rivest92a] - R.Rivest - The MD4 Message-Digest Algorithm, RFC 1320, April 1992

[Rivest92b] - R.Rivest - The MD5 Message-Digest Algorithm, RFC 1321, April 1992

[Schnei94] - B. Schneier - Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, New York, 1994

[TIS94] - Firewall Toolkit Documentation, Trusted Information Systems, Inc., 1994

[Wack95] - J. Wack, L. Carnahan - Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls - NIST Special Publication 800-10, NIST, 1995

[Ziemba95] - G. Ziemba, D. Reed, P. Traina - Security Considerations for IP Fragment Filtering, RFC 1858, October 1995

Kontakt z autorami

Sławomir Górniak - e-mail: S.Gorniak@tele.pw.edu.pl
WWW: http://www.tele.pw.edu.pl/~toja
PGP key: finger -l toja@rhea.tele.pw.edu.pl

Piotr Kijewski - e-mail: P.Kijewski@tele.pw.edu.pl
WWW: http://www.tele.pw.edu.pl/~alph
PGP key: finger -l alph@hyperion.tele.pw.edu.pl

Krzysztof Szczypiorski - e-mail: K.Szczypiorski@tele.pw.edu.pl
WWW: http://www.tele.pw.edu.pl/~kszczypi
PGP key: finger -l kszczypi@bach.tele.pw.edu.pl

Adres zbiorowy
e-mail: firewall@tele.pw.edu.pl

DODATEK A: Polityka bezpieczeństwa podsieci Wall

1. Wstęp

Niezwykły wzrost aktywności użytkowników sieci lokalnej oraz potrzeba wymiany informacji pomiędzy połączonymi sieciami tworzącymi Internet zmusza do sformułowania precyzyjnych zasad bezpieczeństwa.

Ten dokument prezentuje politykę bezpieczeństwa eksperymentalnej sieci lokalnej Wall będącej podsiecią i jednocześnie własnością* Zakładu Teleinformatyki i Telekomutacji (ZTiT) IT PW.

Grupę (określaną dalej jako Załoga „G") odpowiedzialną za podsieć tworzą:

* Piotr Kijewski - koordynator,
* Zbigniew Bazydło - administrator sieci,
* Sławomir Górniak - administrator sieci,
* Krzysztof Szczypiorski - administrator ds. bezpieczeństwa.

Procedury wyboru członków grupy oraz zarządzania nie będą w tym dokumencie omawiane.

2. Cel

Polityka bezpieczeństwa jest zbiorem wymagań dotyczących bezpieczeństwa sprzętu, oprogramowania i informacji (określanych dalej zasobami sieciowymi). Polityka nakreśla szkielet podsieci Wall - definiuje:

- procedury utrzymania i administracji,
- zasady kontroli dostępu,
- uwierzytelnienia

Określa także usługi dostępne w podsieci.

Przy formułowaniu polityki przyjęto zasadę: „co nie jest wyraźnie dozwolone - jest zakazane".

Politykę ukształtowały zaprezentowane poniżej zagrożenia i oczekiwania.

3. Zagrożenia

Każda podsieć internetowa może zostać zaatakowana od strony wewnętrznej i zewnętrznej. Atak może nastąpić:

- przez wykorzystanie nieznanych błędów w stosowanym protokole sieciowym, systemach operacyjnych lub w aplikacjach,
- w wyniku zaniedbania lub błędu konfiguracji ze strony administratorów,
- poprzez użycie przechwyconych lub źle dobranych haseł użytkowników.

4. Oczekiwania

Zakłada się na potrzeby eksperymentu, że zasoby podsieci Wall są cenne i istnieje racjonalna potrzeba chronienia ich przede wszystkim od strony zewnętrznej.

* niezupełnie: router jest własnością Zbigniewa Bazydło, a umieszczony w nim twardy dysk: Zakładu Podstaw Telekomunikacji IT PW

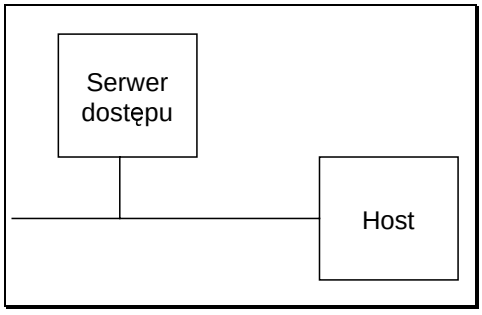
Poziom ochrony zasobów ustala się na więcej niż średni (wg. normy FIPS 112 - Password Usage).

Działalność użytkowników ogranicza się do korzystania z usług internetowych - nie planuje się utworzenia grup roboczych.

Kradzież informacji lub przejęcie sprzętu podsieci Wall przez niepowołane osoby nie wpływa bezpośrednio na bezpieczeństwo pozostałych zasobów ZTiT.

5. Środowisko

Z punktu widzenia użytkownika podsieć Wall składa się z serwera dostępu **brick.wall.tele.pw.edu.pl** i hosta **ra.wall.tele.pw.edu.pl** pracującego pod kontrolą systemu Solaris 2.4 (Sun OS 5.4). Konta użytkowników są umieszczone na **ra**.



Rys. 5-A Środowisko sieciowe

Z punktu widzenia administracji i utrzymania podsieć Wall zawiera oprócz ww. urządzeń router **firewall.tele.pw.edu.pl**.

brick.wall i **firewall** tworzą „ścianę przeciwogniową" (firewall) izolującą podsieć od drapieżnego Internetu.

6. Kontrola dostępu

6.1 Aspekt utrzymania i administracji

Za rozbudowę podsieci: instalację nowego sprzętu, oprogramowania odpowiada Załoga „G".

Przewiduje się:

1. Umieszczenie maszyn w zamkniętym pomieszczeniu kontrolowanym przez pracowników ZTiT.
2. Instalację wyłącznie bezpiecznych (tj. sprawdzonych) systemów operacyjnych.
3. Ustawiczne „patchowanie" (łatanie) systemu.
4. Sporządzanie logów (dzienników) systemowych.
5. Zrezygnowanie ze wszystkich niepotrzebnych usług.
6. Zabezpieczenie plików z hasłami użytkowników.
7. Zabezpieczenie prywatnych informacji o użytkownikach.

Nie przewiduje się:

1. Tworzenia kont grupowych.
2. Udostępniania kont osobom nie spełniającym wymagań określonych w pkt. 6.2.

6.2 Użytkownicy (tzw. u"rz"ytkownicy)

Zasady:

1. Konta są zakładane przez Załogę „G".
2. Prawo do otrzymania konta mają studenci ZTiT, doktoranci oraz pracownicy naukowi IT PW.
3. Załoga „G" ma prawo odmówić przydzielenia konta bez podania powodu.

4. Użytkownicy mają obowiązek zapoznać się z politykę bezpieczeństwa i pisemnie ją zaakceptować; dotyczy to także wszelkich późniejszych zmian.
5. **Użytkownicy powinni chwalić Załogę „G" za to, że umożliwia im bezpieczną pracę.**
6. Wszelkie próby ataku na komputery znajdujące się w podsieci Wall lub poza nią ze strony użytkowników podsieci Wall grożą utratą konta i poinformowaniem władz uczelni - dziekana Wydziału Elektroniki I Technik Informacyjnych PW.
7. Świadome ujawnienie hasła osobom trzecim może spowodować utratę konta bez uprzedzenia.

7. Uwierzytelnienie

7.1 Połączenia zewnętrzne i lokalne

Przy połączeniach zewnętrznych - podczas połączenia się z serwerem dostępu - użytkownik jest proszony o podanie nazwy konta i hasła jednorazowego. Hasło jednorazowe jest tworzone na podstawie tajnego hasła użytkownika i podanych przez system unikalnych parametrów, chroni przed przechwyceniem hasła - otrzymaniem nieuwierzytelnionego dostępu. Użytkownik po podaniu właściwego hasła otrzymuje możliwość połączenia się z hostem w bezpiecznej podsieci. Połączenie z hostem w bezpiecznej podsieci wymaga podania nazwy konta i hasła. **Hasło uwierzytelniające przed serwerem dostępu musi być inne niż hasło uwierzytelniające przed hostem.**

Przy połączeniach lokalnych (wewnętrznych) użytkownicy nie są uwierzytelniani przed serwerem dostępu. W praktyce połączeniem lokalnym jest jedynie logowanie się do systemu z konsoli hosta.

7.2 Polityka haseł

Przewiduje się wprowadzenie i przestrzeganie polityki haseł. Poniższe uwagi dotyczą haseł uwierzytelniających przed serwerem dostępu, jak i przed hostem:

- **długość**: 8 znaków,
  Dobrana ze względu na **Oczekiwania**. Kontrolowana przez system haseł.
- **zawartość**: 96 znaków drukowalnych,
  Umożliwia stworzenie 96^8 różnych haseł (ponad $7{,}21*10^{15}$).
- **okres ważności**:
  - dla zwykłych użytkowników : 3 miesiące
  - dla administratorów : 1 miesiąc
- **źródło**: użytkownicy (w przyszłości generator haseł),
  Poprawność będzie kontrolowana przez system haseł, poza tym hasła będą testowane aby uniknąć haseł łatwych do przewidzenia (popularnych lub skojarzonych z daną osobą wyrazów).
- **własność**: indywidualna,
- **dystrybucja**: inicjujące hasło użytkownik otrzymuje osobiście od administratora ds. bezpieczeństwa, kolejne hasło powinno zostać ustanowione przez użytkownika przy pierwszym pomyślnym zalogowaniu się.

- **przechowywanie**: odciski* haseł dostępne tylko dla systemu uwierzytelniania,
- **wprowadzanie:** poprzez terminale - bez drukowania na ekranie (nie dotyczy haseł jednorazowych),
- **transmisja:** tekst jawny (brak szyfrowania),

  Nie przewiduje się możliwości łączenia administratorów spoza bezpiecznej podsieci.
- **czas uwierzytelnienia**: podczas logowania, po 10 minutach braku aktywności wykonanie procedury ”auto-logout”.

7.3 Uwagi

Przewiduje się korzystanie jedynie z uwierzytelnionej poczty elektronicznej.

8. Usługi

Przewiduje się udostępnienie następujących usług:
- TELNET,
- FTP - w tym anonymous FTP,
- WWW (http) - w tym serwer WWW,
- IRC,
- SMTP (e-mail),
- finger, traceroute, ping,
- X11 (w ograniczonej formie).

Nie przewiduje się udostępnienie następujących usług:
- RPC,
- r-komendy (rlogin, rsh),
- PPP, SLIP.

Załącznik - formularze użytkownika

Wniosek o (przyznanie konta - zmodyfikowanie danych użytkownika)* w podsieci WALL

Proszę o (założenie konta - zmodyfikowanie informacji przechowywanych)* w podsieci Wall:

Nazwisko .....
Imię .....
Funkcja .....
Adres kontaktowy .....
..... Telefon .....
Maszyna .....
Username .....
UID .....
Koniec ważności .....
E-mail (aliase) .....
Limit miejsca na dysku .....
Korzystam z modemu T N

Akceptuję Politykę Bezpieczeństwa w podsieci Wall z dnia .....

Warszawa,----------

* wynik zastosowania silnej funkcji skrótu (kryptograficznej funkcji jednokierunkowej)
* niepotrzebne skreślić

```
       data, czytelny podpis użytkownika

Decyzja:   ..................................................................

Warszawa,-----------------------------------------------------
       data, podpis administratora
```

DODATEK B: Konfiguracja DNS

1. ”Fake server” - brick.wall.tele.pw.edu.pl

1.1 named.boot

```
;
;
directory /var/named
;
;
cache       .                         named.root
secondary   wall.tele.pw.edu.pl       wall.zone
secondary   65.81.148.in-addr.arpa    wall.revzone
secondary   0.0.127.in-addr.arpa      named.local
;
```

1.2 named.local

```
;
;  Configuration file named.local for DMZ fake NS
;
@  IN SOA   brick.wall.tele.pw.edu.pl. zbyniek.brick.wall.tele.pw.edu.pl.
   (
      912345  ;Serial
      10800   ;Refresh
      3600    ;Retry
      432000  ;Expire
      86400   ;Minimum
   )
   IN NS brick.wall.tele.pw.edu.pl.

localhost   IN A  127.0.0.1
1  IN PTR   localhost
```

1.3 named.root

```
;
;  Configuration file named.root for DMZ fake NS
;
wall.tele.pw.edu.pl.          99999999  IN NS brick.wall.tele.pw.edu.pl.
tele.pw.edu.pl.               99999999  IN NS liszt.tele.pw.edu.pl.
pw.edu.pl.                    99999999  IN NS europa.coi.pw.edu.pl.
edu.pl.                       99999999  IN NS cocos.fuw.edu.pl.
pl.                           99999999  IN NS bilbo.nask.org.pl.
.                             99999999  IN NS NIC.NORDU.NET.
                              99999999  IN NS HIMMELSBORG.DNA.LTH.SE.
                              99999999  IN NS C.NYSER.NET.
                              99999999  IN NS TERP.UMD.EDU.
                              99999999  IN NS A.ISI.EDU.
                              99999999  IN NS AOS.BRL.MIL.
                              99999999  IN NS NS.NASA.GOV.
                              99999999  IN NS NS.NIC.DDN.MIL.
;
brick.wall.tele.pw.edu.pl.    99999999  IN A  148.81.65.50
```

```
liszt.tele.pw.edu.pl.          99999999  IN A  148.81.65.108
europa.coi.pw.edu.pl.          99999999  IN A  148.81.28.2
cocos.fuw.edu.pl.              99999999  IN A  148.81.4.6
bilbo.nask.org.pl.             99999999  IN A  148.81.16.51
NIC.NORDU.NET.                 99999999  IN A  192.36.148.17
HIMMELSBORG.DNA.LTH.SE.        99999999  IN A  130.235.16.11
C.NYSER.NET.                   99999999  IN A  192.33.4.12
TERP.UMD.EDU.                  99999999  IN A  128.8.10.90
A.ISI.EDU.                     99999999  IN A  26.3.0.103
AOS.BRL.MIL.                   99999999  IN A  192.5.25.82
NS.NASA.GOV.                   99999999  IN A  128.102.16.10
NS.NIC.DDN.MIL.                99999999  IN A  192.67.67.53
```

1.4 named.revzone

```
;
;  Configuration file wall.revzone for DMZ fake NS
;
$ORIGIN 48.65.81.148.in-addr.arpa.
@  IN SOA   brick.wall.tele.pw.edu.pl. zbyniek.brick.wall.tele.pw.edu.pl.
   (
   960525  ;Serial
   10800   ;Refresh
   3600    ;Retry
   432000  ;Expire
   86400   ;Minimum
   )
@  IN NS brick.wall.tele.pw.edu.pl.
@     PTR   fwnet.wall.tele.pw.edu.pl.
@     A  255.255.255.64
;
;  Real DNS information
;
50.65.81.148.in-addr.arpa. PTR   brick.wall.tele.pw.edu.pl.
;
;  Fake DNS information
;
;*.65.81.148.in-addr.arpa.    PTR   unknown.wall.tele.pw.edu.pl.
49.65.81.148.in-addr.arpa.    PTR   unknown.wall.tele.pw.edu.pl.
51.65.81.148.in-addr.arpa.    PTR   unknown.wall.tele.pw.edu.pl.
52.65.81.148.in-addr.arpa.    PTR   unknown.wall.tele.pw.edu.pl.
53.65.81.148.in-addr.arpa.    PTR   unknown.wall.tele.pw.edu.pl.
54.65.81.148.in-addr.arpa.    PTR   unknown.wall.tele.pw.edu.pl.
55.65.81.148.in-addr.arpa.    PTR   unknown.wall.tele.pw.edu.pl.
56.65.81.148.in-addr.arpa.    PTR   unknown.wall.tele.pw.edu.pl.
57.65.81.148.in-addr.arpa.    PTR   unknown.wall.tele.pw.edu.pl.
58.65.81.148.in-addr.arpa.    PTR   unknown.wall.tele.pw.edu.pl.
59.65.81.148.in-addr.arpa.    PTR   unknown.wall.tele.pw.edu.pl.
60.65.81.148.in-addr.arpa.    PTR   unknown.wall.tele.pw.edu.pl.
61.65.81.148.in-addr.arpa.    PTR   unknown.wall.tele.pw.edu.pl.
62.65.81.148.in-addr.arpa.    PTR   unknown.wall.tele.pw.edu.pl.
63.65.81.148.in-addr.arpa.    PTR   unknown.wall.tele.pw.edu.pl.
```

1.5 wall.zone

```
;
;  Configuration file wall.zone for DMZ fake NS
;
@  IN SOA   brick.wall.tele.pw.edu.pl. zbyniek.brick.wall.tele.pw.edu.pl.
   (
   960525   ;Serial
```

```
   10800    ;Refresh
   3600     ;Retry
   432000   ;Expire
   86400    ;Minimum
   )
   IN NS brick.wall.tele.pw.edu.pl.
wall.tele.pw.edu.pl. IN MX 0  brick.wall.tele.pw.edu.pl.
;
;  Fake DNS informations
;
brick       IN A  148.81.65.50
unknown     IN A  148.81.65.48
unknown     IN A  148.81.65.49
unknown     IN A  148.81.65.51
unknown     IN A  148.81.65.52
unknown     IN A  148.81.65.53
unknown     IN A  148.81.65.54
unknown     IN A  148.81.65.55
unknown     IN A  148.81.65.56
unknown     IN A  148.81.65.57
unknown     IN A  148.81.65.58
unknown     IN A  148.81.65.59
unknown     IN A  148.81.65.60
unknown     IN A  148.81.65.61
unknown     IN A  148.81.65.62
unknown     IN A  148.81.65.63
```

2.”Real server” - ra.wall.tele.pw.edu.pl

2.1 named.boot

```
;
;
directory   /var/named
;
cache    .           named.root
primary     wall.tele.pw.edu.pl     wall.zone
primary     65.81.148.in-addr.arpa  wall.revzone
primary     0.0.127.in-addr.arpa    named.local
forwarders  148.81.65.50
slave
;
;
```

2.2 named.local

```
;
;  Configuration file named.local for Screen Subnet NS forwarder
;
@  IN SOA   ra.wall.tele.pw.edu.pl. zbyniek.ra.wall.tele.pw.edu.pl.
   (
      960525  ;Serial
      10800   ;Refresh
      3600    ;Retry
      432000  ;Expire
      86400   ;Minimum
   )
```

```
   IN NS ra.wall.tele.pw.edu.pl.
;
localhost   IN A  127.0.0.1
1  IN PTR   localhost
```

2.3 named.root

```
;
;  Configuration file named.root for Screen Subnet NS forwarder
;
wall.tele.pw.edu.pl.    99999999 IN NS ra.wall.tele.pw.edu.pl.
ra.wall.tele.pw.edu.pl. 99999999 IN A  148.81.65.60
;
```

2.4 wall.revzone

```
;
;  Configuration file wall.revzone for Screen Subnet NS forwarder
;
$ORIGIN 48.65.81.148.in-addr.arpa.
@  IN SOA   ra.wall.tele.pw.edu.pl. zbyniek.ra.wall.tele.pw.edu.pl.
   (
   960525  ;Serial
   10800   ;Refresh
   3600    ;Retry
   432000  ;Expire
   86400   ;Minimum
   )
@  IN NS ra.wall.tele.pw.edu.pl.
@     PTR   fwnet.wall.tele.pw.edu.pl.
@     A  255.255.255.64
;
;     FIREWALL NETWORK
;
48.65.81.148.in-addr.arpa. PTR   fwnet.wall.tele.pw.edu.pl.
;
;               DMZ SUBNET HOSTS
;
49.65.81.148.in-addr.arpa. PTR   dmz-gate.wall.tele.pw.edu.pl.
50.65.81.148.in-addr.arpa. PTR   brick.wall.tele.pw.edu.pl.
51.65.81.148.in-addr.arpa. PTR   dmz1.wall.tele.pw.edu.pl.
52.65.81.148.in-addr.arpa. PTR   dmz2.wall.tele.pw.edu.pl.
53.65.81.148.in-addr.arpa. PTR   dmz3.wall.tele.pw.edu.pl.
54.65.81.148.in-addr.arpa. PTR   dmz4.wall.tele.pw.edu.pl.
;
;               SCREEN SUBNET HOSTS
;
56.65.81.148.in-addr.arpa. PTR   screen.wall.tele.pw.edu.pl.
57.65.81.148.in-addr.arpa. PTR   screen-gate.wall.tele.pw.edu.pl.
58.65.81.148.in-addr.arpa. PTR   screen1.wall.tele.pw.edu.pl.
59.65.81.148.in-addr.arpa. PTR   screen2.wall.tele.pw.edu.pl.
60.65.81.148.in-addr.arpa. PTR   ra.wall.tele.pw.edu.pl.
61.65.81.148.in-addr.arpa. PTR   screen3.wall.tele.pw.edu.pl.
62.65.81.148.in-addr.arpa. PTR   screen4.wall.tele.pw.edu.pl.
```

2.5 wall.zone

```
;
;  Configuration file wall.zone for Screen Subnet NS forwarder
;
```

```
@  IN SOA   ra.wall.tele.pw.edu.pl. zbyniek.ra.wall.tele.pw.edu.pl.
   (
   960525   ;Serial
   10800    ;Refresh
   3600     ;Retry
   432000   ;Expire
   86400    ;Minimum
   )
;
   IN NS ra.wall.tele.pw.edu.pl.
wall.tele.pw.edu.pl. IN MX 0  brick.wall.tele.pw.edu.pl.
;
;     DMZ SUBNET HOSTS
;
dmz            IN A  148.81.65.48
dmz-gate       IN A  148.81.65.49
brick          IN A  148.81.65.50
dmz1           IN A  148.81.65.51
dmz2           IN A  148.81.65.52
dmz3           IN A  148.81.65.53
dmz4           IN A  148.81.65.54
;
;     SCREEN SUBNET HOSTS
;
screen         IN A  148.81.65.56
screen-gate    IN A  148.81.65.57
screen1        IN A  148.81.65.58
screen2        IN A  148.81.65.59
screen3        IN A  148.81.65.61
ra             IN A  148.81.65.60
screen4        IN A  148.81.65.62
```