Ściany Ogniowe

Autorzy: Mirosław Bartyna, Grzegorz Lisowski, Robert Bejster IVFDS

STRESZCZENIE

Globalny Internet wywołał prawdziwą rewolucję w sposobach prowadzenia biznesu, dostępu do informacji itp. Firmy korzystając z technologii internetowych zmieniły metody komunikacji z klientami, sprzedaży produktów i nawiązywania nowych kontaktów. Ze względu na to, że firmy wykorzystują Internet do kreowania nowych modeli biznesowych, sprawa bezpieczeństwa sieci stała się ważniejsza niż kiedykolwiek. Aby utrzymać dobrą współpracę i zaufanie partnerów i klientów, firmy muszą zapewnić im dostęp do swoich kluczowych aplikacji, danych oraz innych zasobów, zabezpieczając jednocześnie wszystkie elementy własnego systemu informatycznego: systemy komputerowe, aplikacje i użytkowników na poziomie Internetu, intranetu i extranetu.

SPIS TREŚCI

1. ZAGROŻENIA SYSTEMÓW INFORMATYCZNYCH[8,9,13,18]

Atak najczęściej jest przeprowadzany w celu:

- włamania – są to formy ataków których skutkiem ma być uzyskanie uprawnień do pracy w danym systemie nie pociągając za sobą żadnych destrukcyjnych dla systemu działań, Czyli włamywacz pragnie pracować tak jak zwykły użytkownik.
- blokada usług - celem tego ataku jest przeszkodzenie użytkownikom w używaniu własnych komputerów.
- kradzieży informacji – celem tego ataku jest kradzież istotnych dla pracy systemu informacji, chodzi głównie o kradzież informacji pozwalających włamywaczom na dostęp do komputerów sieci tj. nazwy użytkowników i haseł.

Sieci koncentrują się przeważnie na zagrożeniach ze strony Internetu, a przecież wewnętrzny użytkownik również może stanowić zagrożenie. Badania bowiem wykazują, że w sporej części przypadków włamania popełniane są przez użytkowników wewnętrznych. W dodatku, instytucje kontaktujące się z partnerami gospodarczymi poprzez sieci prywatne budują magistrale, przez które może nastąpić "atak". Pracownicy firm kooperujących mogą dzięki nim wykradać sobie wzajemnie wiele cennych informacji. Ataki z zewnątrz to najczęstsza forma zakłócenia stabilnej pracy sieci. Odbywają się z zewnątrz sieci lokalnej to znaczy np. z Internetu, dostęp poprzez lukę w systemie zabezpieczeń, błąd serwisu sieciowego lub po prostu słaby poziom zabezpieczeń firmy.

1.1. Rodzaje ataków:

- Atak na serwer http - konsekwencje to utrata danych witryny internetowej lub pojawienie się treści kompromitujących firmę.
- Atak na poszczególne komputery bądź serwer główny (DOS, Wirusy) - konsekwencje przerwa w pracy sieci, konkretnych końcówek, wszystkich końcówek, serwera a co za tym idzie całej sieci, może to spowodować wielogodzinną przerwę w pracy. Skutki mogą być niewinne i skończyć się na zawieszeniu poszczególnych maszyn bądź całej sieci ale może też prowadzić do fizycznego uszkodzenia komputerów, wymazania BIOS'u na płycie głównej lub uszkodzenia twardych dysków.

1.2. Metody dokonywania ataków:

1.2.1. DOS

DOS (Denial Of Service) to atak mający na celu zablokowanie konkretnego serwisu sieciowego np. strony WWW, lub też zawieszenie komputera. Możliwe jest przesterowanie ataków DOS w bardziej skomplikowany sposób, co może doprowadzić do awarii działania całej sieci. Niejednokrotnie atakujący za pomocą tzw. techniki spoofingu lub ukrywa swój prawdziwy adres internetowy, tak więc namierzenie go często staje się niemożliwe, lub jest prawdopodobne jedynie przy pomocy specjalisty a i ten niejednokrotnie spędza nad tym długie godziny.

1.2.2. Sniffing

Sniffing to wykorzystywanie interfejsu sieciowego do odbierania danych nie przeznaczonych dla komputera, w którym ten interfejs jest zainstalowany. Możliwość sniffingu mają na przykład mostki w sieciach token ring, posiadają one zazwyczaj dwa interfejsy sieciowe. Odbierają one wszystkie pakiety, podróżujące po sieci i retransmitują do innych interfejsów część z nich, choć nie wszystkie. Urządzeniami dokonującymi sniffingu są również tzw. analizatory sieci. Ich zadaniem jest pomoc administratorowi w diagnozowaniu wielu ukrytych problemów, które mogą być niewidoczne z danej maszyny. Urządzenia wykorzystujące snifflng są użyteczne i potrzebne. Jednak fakt ich istnienia, powoduje że mogą one zostać wykorzystane przez złośliwych użytkowników w celu przechwytywania wszelkich danych płynących przez sieć. Może on przechwytywać wszystkie dane przez krótki czas lub przez dłuższy okres czasu. Do momentu aż włamywaczowi skończy się przestrzeń do przechowywania przechwyconych danych. Wszystkie te dane mogą zostać następnie użyte w celu przygotowania ataku na system komputerowy.

1.2.3. Spoofing

Spoofing jest to podszywanie się podczas którego maszyna sieciowa udaje inną maszynę. Następuje przerwanie normalnego przepływu danych, może również obejmować wprowadzenie danych do łącza komunikacyjnego. Podszywanie się ma na celu wprowadzenie w błąd innych komputerów na temat pochodzenia danych oraz nakłonienie ich do przesłania żądanych informacji lub zmiany informacji.

Według standardu EEEE 802 dla sieci (w tym także Ethernet), każdy interfejs sieciowy ma przyznany 48 bitowy unikatowy numer sieciowy. Jest on używany do wychwytywania ramek skierowanych do tego interfejsu. Większość programów nie kontroluje adresu źródłowego pakietów opuszczających interfejs. Kiedy pakiet dociera do odbiorcy przyjmuje on za prawdziwe dane dotyczące nadawcy, jakie znajdują się w pakiecie. Choć każdy interfejs ma swój niepowtarzalny numer nadany przez producenta, to istnieją takie urządzenia, które pozwalają na zmianę tego adresu. W takim przypadku dany interfejs może imitować inne urządzenie bez konieczności ingerowania w warstwę aplikacji. Pozwala to na proste przeprowadzenie spoofingu nie tylko sprzętowego, ale i innych np. : DNS spoofing, IP spoofing. Dzieje się tak dlatego, iż warstwa aplikacji znajduje się powyżej warstwy sprzętowej, a wyżej leżące warstwy protokołu IP zależą od warstw niższych.

1.2.4. ARP Spoofing

ARP Spoofing (Address Resolution Protocol Spoofing) jest bardzo częstą metodą spoofingu. Jest to protokół odpowiedzialny za tłumaczenie adresu EP na adresy sprzętowe. Kiedy pakiet jest wysyłany przez sieć, najpierw określana jest podsieć, do której ma on dotrzeć, np. przez określenie adresu rutera, przez który będzie on przesyłany, a następnie adres EP jest tłumaczony na adres fizyczny, który jest rozgłaszany (w przypadku sieci Ethernet) do wszystkich dostępnych interfejsów. Interfejs, który ma odpowiedni adres odbierze pakiet i tylko on powinien odpowiedzieć na zapytanie. Jednak, jak już wcześniej pisałem, istnieją metody odebrania pakietów również przez maszyny, do których nie był on adresowany. Adresy EP maszyn oraz skojarzone z nimi adresy sprzętowe są przechowywane w buforze(cache) ARP każdego hosta. Kiedy datagram jest przesyłany przez sieć, sprawdzana jest zawartość bufora ARP i, jeżeli istnieje tam wpis odpowiadający adresowi docelowego miejsca, gdzie ma dotrzeć datagram, nie ma potrzeby wysyłania zapytania ARP. Zapisy w buforze ulegają

przeterminowaniu po kilku minutach od ich stworzenia. Kiedy wpis ARP o danym hoście wygaśnie, wysyłane jest zapytanie ARP. Jeżeli komputer będzie wyłączony, zapytanie zostanie bez odpowiedzi. Zanim jednak wpis zostanie przeterminowany, datagramy są wysyłane, lecz nie odbierane. Klasycznym przykładem spoo-fingu ARP jest zmiana adresu EP na adres maszyny wyłączonej. Włamywacz może zorientować się, jaka maszyna w sieci jest wyłączona, lub samemu ją wyłączyć. Wtedy zmieniając konfigurację swojej maszyny może on skonfigurować ją tak, aby wskazywała EP odłączonej maszyny. Kiedy ponownie zostanie wysłane zapytanie ARP, jego system odpowie na nie, przesyłając nowy adres sprzętowy, który zostanie skojarzony z adresem IP wyłączonej maszyny. Jeżeli jakieś usługi w sieci były udostępniane na podstawie zaufania według danych wskazywanych przez ARP, będą one dostępne dla osoby niepowołanej. Atak za pomocą spoofingu ARP jest również możliwy w przypadku, kiedy istnieją w sieci maszyny o dwóch takich samych adresach IP. Tak sytuacje powinna być niedopuszczalna, jednak często występuje takie zjawisko i nie zawsze jest one zamierzone. Dzieje się tak np. przez instalowanie jednej kopii oprogramowania na wielu maszynach z jedną konfiguracją. Kiedy jest wysyłane zapytanie ARP każdy z hostów o danym EP odpowie na nie. W zależności od systemu albo pierwsza albo ostatnia odpowiedź zostanie umieszczona w buforze. Niektóre systemy wykrywają taką sytuację i jest to oznaka możliwości wystąpienia spoofingu. Aby bronić się przed spoofingiem ARP, stosuje się wpisy permanentne w przypadku hostów o szczególnym znaczeniu. W takim przypadku zapisy w buforze nie ulegają przedawnieniu i nie może zaistnieć sytuacja, kiedy włamywacz będzie chciał wysłać nowy adres sprzętowy danej maszyny. Wadą tej metody jest konieczność zmiany wpisów ARP w przypadku np. Wymiany interfejsu sieciowego w maszynach znajdujących się w sieci.

1.2.5. DNS spoofing

Niektóre systemy udzielają zaufania na podstawie adresu EP, inne korzystają do tego celu z nazw DNS (Domain Name System - system nazw domen). Nazwy są łatwiejsze do zapamiętania i dlatego często są używane zamiast adresów EP. Kiedy odwołujemy się do hosta za pomocą nazwy DNS, odpowiedni mechanizm przetwarza go na adres EP. Zadanie to jest realizowane przez serwer DNS, który odpowiada także na zapytania odwrotne, kiedy mamy adres IP i chcemy otrzymać skojarzoną z nim nazwę. Host wysyłający zapytanie ufa, że serwer zwróci mu poprawną wartość. System DNS jest systemem złożonym i bazuje na rozproszonej bazie danych. Informacje nie są przechowywane w centralnym miejscu, ale odpowiednie systemy zawierają wpisy dotyczące określonych domen. System, na którym zainstalowany j es t serwer nazw, określany jest mianem „nameserver". Każdy z komputerów podłączonych do sieci ma zdefiniowane nazwy nameserwerów, które będą zajmować się tłumaczeniem adresów nazw na EP i odwrotnie. W przypadku gdy serwer nazw gdzieś w Internecie został przechwycony podczas ataku i jest pod kontrolą włamywacza. Serwer ten będzie udzielał autorytatywnych odpowiedzi na temat pewnych domen i wszystkie hosty w Internecie będą mu ufały. Odpowiedzi te mogą nakłaniać klientów do połączenia się z serwerami, które są pod kontrolą włamywacza zamiast z serwerami autoryzowanymi. Sfałszowane tłumaczenie odwrotne adresu może oszukać serwer, który próbuje stwierdzić, czy adres IP przyszłego klienta zgadza się z autoryzowaną nazwą.

1.2.6. Spoofing połączeń TCP

Protokół TCP pozwala zbudować zorientowany na połączenia, pewny ciąg bajtów na wierzchu warstwy IP, warstwa ta przesyła bezpołączeniowe, niepewne datagramy. Możliwy do przeprowadzenia jest spoofing za pomocą datagramów IP, które mają adres IP należący do innej maszyny. Spoofing ten stanowi mechanizm ataku na zabezpieczenia innej maszyny korzystającej z

protokołu EP do odbierania rozkazów. Maszyna włamywacza może wysłać datagramy IP ze sfałszowanym adresem źródłowym do dowolnej innej maszyny, podczas gdy maszyna, do której dany adres należy legalnie, jest aktywna. Można tego dokonać bez zamiaru odebrania odpowiedzi na te datagramy. Inne maszyny będą odbierały je jako pochodzące od autoryzowane - go posiadacza adresu EP, jaki mają. Wymuszą one wykonanie poleceń, które nie są żądane przez prawdziwego użytkownika. Aby skutecznie sfałszować datagram TCP/IP który będzie uznany za część istniejącego połączenia włamywacz musi jedynie ocenić liczbę porządkowy, która zostanie przypisana do następnego bajtu danych wysłanych przez prawdziwego nadawcę.

1.2.7. Hijacking przechwytywanie połączenia

Może ono się odbywać w dwóch warstwach protokołów sieciowych. W warstwie transportowej TCP, jak również w warstwie sesji SMB lub NFS. Włamywacz aby przechwycić współużytkowane połączenie sieciowe, musi dotrzeć do obydwu warstw, wynika to z faktu iż SMB korzysta z portów TCP do utworzenia połączenia. W celu przechwycenia istniejącego połączenia TCP, musi ona przewidzieć numer sekwencyjny, używany przez komputery komunikujące się ze sobą. Jest on wykorzystywany do porządkowania pakietów, jak również pozwala on stwierdzić, czy wszystkie pakiety dotarły do miejsca przeznaczenia. Następnym krokiem jaki wykonuje włamywacz jest przekierowanie połączenia TCP/IP do swojego komputera. Następnie uruchamia atak odmowy usługi przeciwko komputerowi klienckiemu, nie może on wtedy przekazać informacji o tym, że coś się źle dzieje. W celu przechwycenia sesji SMB (np. mapowanie dysków) włamywacz musi określić prawidłowe identyfikatory ramki NetBIOS-u, drzewa jak również użytkownika na poziomie serwera w istniejącym połączeniu NetBIOS-u. Włamania takie teoretycznie nie powinny mieć miejsca wynika to z faktu iż narzędzia do przechwytywania połączeń SMB nie są tak dostępne jak na przykład do przechwytywanie połączeń TCP jak również z faktu iż prawidłowo zabezpieczony host internetowy nie udostępnia NetBIOS-u do Internetu.

1.2.8. Atak Ping of Death

Jest to atak warstwy sieciowej. Specjalnie zbudowany pakiet ICMP, który łamie zasady konstrukcji tego pakietu. Wyniku czego może nastąpić awaria komputera odbierającego z oprogramowaniem sieciowym sprawdzającym prawidłowość pakietów ICMP.

1.2.9. Atak na serwer główny

Konsekwencje to utrata kontroli praktycznie nad całą siecią, możliwość utraty wszystkich danych, zakłócenie pracy dowolnych usług sieciowych w całej firmie. Po przejęciu kontroli nad głównym serwerem możliwe jest przechwytywanie danych wędrujących wewnątrz sieci a co za tym idzie poznanie struktury wewnętrznej firmy. Możliwe jest fałszowanie danych przesyłanych siecią, wiadomości między szefem a współpracownikami. Najpowszechniej praktykowaną metodą uzyskiwania dostępu do odległego systemu jest wykonywanie zdalnego logowania *(Telnet),* przeprowadzanego najczęściej na bazie łączności modemowej "dial-up". Warunkiem wykonania pomyślnego logowania na odległym komputerze jest znajomość identyfikatora i hasła użytkownika, który jest do tego upoważniony. Uzyskanie identyfikatora z reguły sprowadza się do zdobycia adresu e-mail dowolnego użytkownika tego systemu. Hasła użytkowników mogą być pozyskane drogą zgadywania, przechwytywania lub rozszyfrowania pliku zawierającego hasła użytkowników systemu. Co ciekawe, sama aplikacja nie stanowi zagrożenia - to przyjęty system kontroli tożsamości jest słaby. Statystyki podają, iż duża większość użytkowników jako hasła dostępu do konta przyjmuje łatwe do zapamiętania słowa

(np. imiona, nazwy miejscowości, ...), które w równie łatwy sposób mogą być odgadnięte przez cierpliwego włamywacza.

1.3. Działanie tzw. „złośliwych programów”:

- **wirus** (ang. *virus)* - program dopisujący się do innego programu, który atakuje system w trakcie uruchomienia swojego "żywiciela";
- **bakteria** (ang. *bacteria),* **królik** (ang. *rabbit)* - program wielokrotnie kopiujący i uruchamiający swój własny kod źródłowy celem pełnego zagarnięcia zasobów komputera (procesora, pamięci operacyjnej, przestrzeni dyskowej) i doprowadzenia do upadku systemu;
- **koń trojański** (ang. *trojan horse)* - program, który udaje pracę innego legalnego programu w międzyczasie wykonuje szereg niepożądanych czynności;
- **bomba czasowa** (ang. *time bomb),* **bomba logiczna** (ang. *logie bomb)* - fragment progra-złożonych usług na pojedynczym adresie IP. Połączenia do portów SMTP i POP mogą być statycznie tłumaczone na połączenia z serwerem pocztowym, zaś port HTTP może oznaczać połączenie z serwerem WWW. Dzięki temu, że podczas tłumaczenia można określić dowolny adres IP, usługi możemy przydzielić różnym maszynom, które znajdują się wewnątrz chronionej sieci.

2. POLITYKA BEZPIECZEŃSTWA[1,8,9,12]

2.1. Budowa polityki bezpieczeństwa sieci prywatnej

Instalacja oprogramowania "firewall" powinna być poprzedzona staranną analizą potrzeb organizacji zakresie wykorzystania sieci Internet. Należy dokładnie sprecyzować z jakich usług będą korzysta pracownicy organizacji (użytkownicy lokalni), a jakie usługi będą świadczone na rzecz użytkowników zewnętrznych - w ostatnich latach coraz więcej organizacji decyduję się na prowadzenie komercyjnej działalności za pośrednictwem sieci Internet (np. reklama w serwisie WWW). W procesie planowania polityki bezpieczeństwa należy uwzględnić konieczność ochrony wszystkich newralgicznych punktach systemu informatycznego (np. serwery baz danych, serwery aplikacji, ...). Budowa polityki bezpieczeństwa realizowana jest w następujących etapach:

1. Określenie wymagań użytkowników lokalnych w zakresie korzystania z usług sieci Internet.
2. Weryfikacja wymagań użytkowników lokalnych.
3. Określenie zakresu usług sieci prywatnej dostępnych dla użytkowników sieci Internet.
4. Weryfikacja udostępnianych usług sieci prywatnej.
5. Planowanie polityki bezpieczeństwa.
6. Zatwierdzenie przyjętej koncepcji ochrony.
7. Wdrożenie polityki bezpieczeństwa.
8. Testowanie systemu pod względem szczelności i efektywności.
9. Szkolenia użytkowników (jeżeli jest to konieczne).

Należy pamiętać, iż dopiero w momencie zatwierdzenia projektu systemu ochrony przez kierownictwo organizacji można przystąpić do wyboru oprogramowania, które sprosta zadaniu wdrożenia przyjętej polityki bezpieczeństwa. Z uwagi na dużą ilość dostępnych rozwiązań, wybór najbardziej odpowiedniego produktu nie jest łatwy. Jako decydujące kryterium możemy przyjąć: stopień złożoności technologicznej, zakres realizowanych zadań, przejrzystość interfejsu użytkownika i oczywiście cenę. [1]

2.2. Wdrożenie polityki bezpieczeństwa

Dysponując zatwierdzonym projektem systemu ochrony można przystąpić do fazy wdrożenia polityki bezpieczeństwa, która sprowadza się do zainstalowania i konfiguracji oprogramowania "firewall", odpowiedzialnego za egzekwowanie przyjętych ograniczeń. Proces wdrożenia polityki bezpieczeństwa obejmuje następujące fazy:

1. Definicja obiektów sieciowych.
2. Definicja użytkowników systemu.
3. Specyfikacja dodatkowych usług sieciowych. (opcjonalnie)
4. Ustalenie zasad bezpieczeństwa.
5. Weryfikacja i instalacja.

3. WYBÓR ZAPORY OGNIOWEJ[1,8]

Większość z zapór ogniowych może spełniać swe funkcje w wielu różnych konfiguracjach.
Niektóre z zadań jakie powinna spełniać zapora ogniowa:

- łączenie przez tunele szyfrowane takich sieci prywatnych, które czerpią dane z Internetu. W efekcie powstaje sieć rozległa, złożona z sieci lokalnych połączonych tunelami szyfrowanymi.
- zagwarantowanie kontrolowanego dostępu użytkownikom przebywającym poza przedsiębiorstwem macierzystym. Między zaporą przedsiębiorstwa i komputerem użytkownika można w razie potrzeby utworzyć tunel szyfrowany.
- ochronę usług izolowanych, na przykład serwera przedsiębiorstwa łączącego się z serwerem WWW usytuowanym w sieci operatora świadczącego usługi dostępu.
- zarządzanie blokadami między wieloma sieciami intranetowymi, zapewniające odizolowanie poufnych informacji w obrębie jednego przedsiębiorstwa albo spółki.
- ograniczenie dostępu do sieci prywatnej (intranet) przy jednoczesnym pełnym otarciu wewnętrznych serwerów WWW czy FTP *(File Transfer Protocol)* na usługi publiczne. Dla takich serwerów tworzy się wtedy osobną podsieć, nazywaną strefą zdemilitaryzowaną albo bastionem. Zapora ogniowa musi tu dysponować trzema interfejsami LAN.

Między bezpośrednim połączeniem z Internetem a pełną izolacją istnieje spora przestrzeń aplikacyjna. Producenci starają się tworzyć produkty, mające zapełnić tą lukę. Zapora ogniowa musi trafiać w potrzeby użytkownika oraz być adekwatną do zaawansowania technicznego samych zainteresowanych. Dostosowanie produktu do środowiska sieciowego może być kłopotliwe dla niedoświadczonego administratora. Bardzo często nie obejdzie się bez porady specjalisty. Zdarza się nawet, że niektóre firmy korzystają z fachowych porad specjalistów zajmujących się bezpieczeństwem Internetowym. Przy wyborze zapory nie trzeba się kierować wyborem renomowanych marek, czy delikatnością administrowania. Najważniejszą rzeczą jest aby zapora ogniowa potrafiła sprostać naszym potrzebom i oczekiwaniom.

3.1. Domyślne przepuszczanie kontra domyślne powstrzymywanie

Podstawowym zadaniem zapory sieciowej jest ograniczenie przepływu danych między dwoma sieciami. Aby postawić zaporę, trzeba najpierw określić, jakie rodzaje danych mają być przez

nią przepuszczane, a jakie nie. Nazywa się to definiowaniem polityki zapory. Po tej operacji należy utworzyć mechanizmy, które będą zdefiniowaną politykę wprowadzać w życie .
Są dwie podstawowe strategie definiowania polityki zapory:

- domyślne przepuszczanie

Ta strategia polega na określeniu zbioru warunków, których skutkiem będzie blokowanie danych. Każdy host lub protokół, który nie zostanie objęty polityką, będzie domyślnie przepuszczany.

- domyślne powstrzymywanie

Ta strategia polega na określeniu protokołów, które będą mogły przechodzić przez zaporę, a także hostów, które będą mogły przesyłać przez nią dane i z którymi komputery wewnątrz zapory będą mogły się kontaktować. Wszystko, co nie będzie objęte definicjami, zostanie powstrzymane od przejścia przez zaporę.

Oba tryby mają wady i zalety. Główną zaletą domyślnego przepuszczania jest łatwość konfiguracji. Blokuje się protokoły "niebezpieczne" i polega na swoich możliwościach wykrywania nowych niebezpieczeństw i odpowiedniego reagowania w przypadku ich opracowania (wykrycia). Tryb domyślnego powstrzymywania polega na przepuszczaniu tylko tych protokołów, o które proszą użytkownicy i zarząd. Każdy protokół, który nie jest używany przez firmę, zostanie zablokowany.
Ani jeden, ani drugi tryb pracy nie stanowi panaceum na problemy bezpieczeństwa. W obu przypadkach można utworzyć konfigurację, która nie będzie prawidłowo zabezpieczała sieci przez niewłaściwe przepuszczenie (bądź nie zablokowanie) jakiegoś "niebezpiecznego" protokołu.

4. TYPY ZAPÓR OGNIOWYCH[3,6,19]

4.1. Bramy na poziomie sieci

Zaporę ogniową na poziomie sieci przeważnie jest realizowana za pomocą routera lub innego specjalnego komputera filtrującego pakiety. Każdy pakiet IP zawiera takie dane jak adres urządzenia emitującego pakiety i adres docelowy, na podstawie których zapora decyduje czy dany pakiet przepuścić czy *zatrzymać*. Protokoły takie jak TCP czy UDP dodają do nagłówków pakietów standardowe numery portów źródła i punktu przeznaczenia, identyfikujące aplikacje związane z tymi urządzeniami. Na podstawie analizy portu przeznaczenia można rozpoznać określoną usługę i w efekcie zastosować bardziej rygorystyczne reguły selekcji dla uaktywnienia lub zablokowania połączenia.
Działanie zapory ogniowej na poziomie sieci oparte jest o tzw. listy dostępowe lub czarne listy, zawierające adresy które są blokowane przez zaporę. Router lub specjalny komputer może być skonfigurowany tak aby blokować wszystkie wiadomości przychodzące z określonej firmy, oraz do niej wysyłane. Blokowanie pakietów zazwyczaj odbywa się za pomocą pliku zawierającego adresy IP określonych firm czy ośrodków. Zapora będzie wtedy blokowała wszystkie pakiety przychodzące z tych firm, lub zmierzające do nich. W momencie gdy odnajduje on pa-

kiet zawierający zastrzeżony adres, zatrzymuje go uniemożliwiając mu przedostanie się do sieci lokalnej. Zapora taka odpowiada także na żądania użytkowników dotyczące takich usług jak FTP, HTTP czy Telnet. Może ona być zaprogramowana na przykład w taki sposób aby użytkownicy sieci lokalnej mieli dostęp do serwerów WWW, ale nie mogli korzystać z usługi FTP. Zazwyczaj można określić, które z informacji dołączonych do pakietu mają być kontrolowane przez router. Informacje w oparciu o które może odbywać się selekcja to: adres źródłowy, adres docelowy, protokół sesji (np. TCP, UDP), źródłowy i docelowy port aplikacji dla żądanej usługi oraz informacja czy pakiet jest początkiem żądania połączenia.

4.2. Bramy na poziomie aplikacji

Bramy poziomu aplikacji są złożonymi zaporami ogniowymi, które zapobiegają przepływowi danych określonego typu między sieciami. Aplikacja typu proxy działa jako pośrednik pomiędzy serwerem internetowym a klientem. Zamiast komunikować się między sobą bezpośrednio, każdy z nich porozumiewa się z serwerem proxy. Serwer proxy utrzymuje stan połączenia TCP między klientem a serwerem internetowym i dzięki temu każda ze stron "wierzy", że jest połączona ze sobą bezpośrednio. Serwer proxy nie tylko przekazuje żądania od klientów, ale również je analizuje. Dzięki temu ma możliwość kontrolowania tego, jakie operacje realizują twoi użytkownicy. W zależności od szczegółów twojej polityki bezpieczeństwa, żądania te mogą zostać zatwierdzone i przekazane dalej, bądź może nastąpić ich odrzucenie.

Korzyści ze stosowania serwera proxy:

- blokuje dostęp do usług Internetu, z których nie chcesz, by korzystali pracownicy twojej firmy,
- chroni istotne zasoby Intranetu,
- ukrywa prawdziwy adres IP użytkownika przed resztą Internetu,
- gromadzi informacje o użytkownikach oraz dane statystyczne dotyczące wykorzystywania sieci,
- jest stosunkowo łatwy w konfigurowaniu i utrzymywaniu.

Wady, niedogodności używania serwera proxy:

- wymaga oprogramowania klienta, które potrafi "rozmawiać" z serwerem proxy,
- nie daje ochrony przed atakami pochodzącymi od wewnątrz,
- utrudnia administrowanie siecią i wymaga dodatkowego szkolenia zarówno administratorów, jak i użytkowników,
- może obniżyć szybkość pracy aplikacji,
- nie daje możliwości filtrowania pakietów.

4.3. Filtrowanie pakietów

Filtry pakietów pozwalają lub blokują przepływ pakietów danych podczas ich przesyłania z jednej sieci lub jej segmentu do innej sieci lub jej segmentu.
W dużych sieciach zapory ogniowe najczęściej stosują filtrowanie pakietów. Polega to na sprawdzeniu czy kolejne kawałki danych przepływające przez sieć spełniają określone kryteria. Pakiety po sprawdzeniu zgodności z regułami są przepuszczane lub blokowane. Zwykle wymogi dotyczą dopuszczalnych adresów IP przychodzących i wychodzących pakietów, stosowanych protokołów sieciowych czy numerów portów serwera. Zapory oparte na filtrowaniu pakietów często rezydują nie na serwerze, lecz na odpowiednim ruterze (screening

router), urządzeniu, które stanowi styk Intranetu z sieciami zewnętrznymi. Transmitowane są przez nie wszystkie dane wchodzące i wychodzące. (tutaj wspomnieć o spoofingu).

Kryteria filtrowania

Pakiety mogą być filtrowane wg następujących kryteriów:

- adres źródłowy pakietów,
- adres docelowy pakietów,
- numer portu źródłowego,
- numer portu docelowego,
- czy pakiet próbuje zainicjować połączenie.

Reguły filtrowania pakietów korzystają z informacji datagramu IP, aby ustalić, jakie pakiety mogą przejść przez zaporę ogniową.

Cechy filtrowania pakietów

- reguły filtrujące pakiety są szybkie, a poza tym niewidoczne dla użytkowników,
- trudne jest tworzenie listy takich zasad, które nigdy nie przepuszczą intruzów i nigdy (lub prawie nigdy) nie przeszkodzą w normalnych operacjach pracowników firmy,
- implementacja jest tym trudniejsza, im bardziej rośnie liczba blokowanych lub przepuszczanych usług, sieci, hostów,
- kiedy rośnie liczba reguł, rośnie również czas sprawdzania, czy dany datagram powinien zostać przesłany, rośnie również prawdopodobieństwo, że datagram, który powinien przejść zostanie zablokowany i odwrotnie,
- filtrowanie pakietów blokuje dostęp do sieci mniej doświadczonym intruzom i utrudnia uzyskanie dostępu intruzom bardziej zawansowanym,
- kiedy pozwolisz na dostęp do wewnętrznego hosta, nie masz kontroli nad tym co się dzieje, wtedy zdalny użytkownik może podjąć próbę znalezienia słabych punktów tego komputera, wykorzystując prawdopodobnie dostęp do innych hostów sieci,
- filtry pakietów korzystają z informacji przechowywanych w nagłówkach datagramów IP. Oznacza to, że intruzi mogą fałszować IP, preparując źródłowy adres IP datagramu, w wyniku czego zapora będzie sądziła, że dane pochodzą z autoryzowanego hosta.
  filtry pakietów nie udostępniają mechanizmu uwierzytelniania użytkowników, polegają one na systemie bezpieczeństwa zdalnych systemów, z których możliwy jest dostęp. Jeżeli intruz włamie się do systemu zdalnego, który ma dostęp przez zaporę ogniową, może się przedostać przez zaporę, bez możliwości wykrycia.

4.4. Kombinowane zapory ogniowe

W profesjonalnych zastosowaniach filtrowanie pakietów jest często łączone z tzw. usługami proxy. Są to funkcje zapór ogniowych, które powodują, że w trakcie trwania sesji sprawdzane są wszystkie prośby dotyczące transmisji danych i zezwolenie na transmisję jest wydawane bądź nie. Usługi proxy mogą być oferowane na poziomie pakietów danych i na poziomie aplikacji. Zapory ogniowe stosujące filtrowanie pakietów są zazwyczaj szybsze od bram aplikacji.

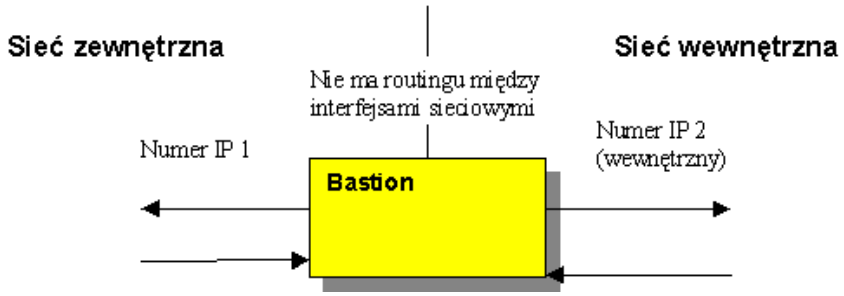
5. ARCHITEKTURY ZAPÓR OGNIOWYCH[1,3,6,19]

5.1. Router filtrujący transmitowane pakiety *(Screening Router)*

Wśród architektur typu firewall router filtrujący występuje najczęściej, niekiedy będąc jedynym elementem zabezpieczającym sieć. W zależności od rozwiązania jest to specjalizowane urządzenie sieciowe (router) lub jego odpowiednik oparty o komputer i oprogramowanie umożliwiające filtrowanie pakietów. Zasadniczo ten typ zabezpieczenia umożliwia separację ruchu pomiędzy sieciami, lub konkretnymi urządzeniami, na poziomie protokołu IP (lub IPX). Można zapewnić kontrolę przepływu pakietów w zależności od adresu IP, IPX i MAC nadawcy lub odbiorcy, rodzaju usługi sieciowej (telnet, ftp,smtp, ...), itp. Ten typ zabezpieczenia stosuje się jako rozszerzenie możliwości funkcjonującej już struktury połączenia sieci prywatnej i publicznej. Najczęściej konieczna jest jedynie zmiana konfiguracji routera i/lub dodanie funkcji odpowiedzialnych za ochronę danych.

5.2. Komputer-twierdza *(Bastion Host)*

W terminologii militarnej twierdza to dobrze strzeżona, ufortyfikowana i zorientowana na długotrwałą obronę przed agresorem budowla. Jest to możliwe dzięki zastosowaniu wielu wymyślnych zabezpieczeń, wzmocnieniu ścian, przygotowaniu niespodzianek w postaci potoków gorącej smoły itp. Przenosząc definicje twierdzy na grunt sieci komputerowych możemy opisać urządzenie, które z punktu widzenia sieci może być narażone na częste i bezpośrednie ataki potencjalnych włamywaczy komputerowych i dlatego pozostaje pod szczególnym nadzorem administratora systemu. Prowadzi on wzmożony monitoring pracy takiego urządzenia oraz dokonuje modyfikacji konfiguracji i oprogramowania celem podniesienia poziomu zabezpieczeń systemowych. Rozwiązanie stosuje się na serwerach sieci prywatnej, aby wyeliminować nieautoryzowany dostęp i we właściwy sposób reagować na próby ingerencji w system ze strony osób trzecich.



5.3. Komputer z dwoma interfejsami sieciowymi *(Dual Homed Gateway)*

Kolejnym z rozwiązań jest takie skonfigurowanie struktury wewnętrznej chronionej sieci komputerowej, aby dostęp do sieci publicznej miał tylko jeden komputer w sieci lokalnej. Komputer taki, posiadający dwa interfejsy sieciowe, widziany jest z obu podłączonych sieci, jednak bezpośrednia komunikacja pomiędzy nimi nie jest możliwa ze względu na blokadę transmisji pakietów wprost pomiędzy interfejsami. Jest to niewątpliwie jedna z realizacji zabezpieczenia Firewall - Bastion Host opisanego powyżej. Komunikacja pomiędzy sieciami

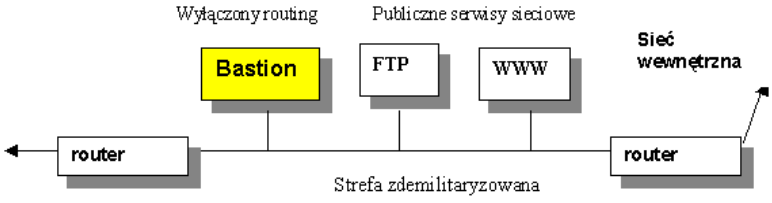
publiczną i lokalną jest możliwa dwuetapowo, przez wstępne zalogowanie się na komputerze pośredniczącym, i dostęp na poziomie którejś z dozwolonych usług (np. telnet lub ftp) do komponentów drugiej sieci. Rygorystyczne przestrzeganie poprawności zabezpieczenia systemu oraz ciągły nadzór nad jego pracą został ograniczony w tym rozwiązaniu do jednego komputera pełniącego rolę gateway'a pomiędzy separowanymi sieciami.

5.4. Konstrukcja filtrująca przepływające pakiety *(Screened Host Gateway)*

Rozwiązanie które zostanie tu opisane jest często stosowaną konstrukcją skladającą się ze współpracujących ze sobą: routera filtrującego pakiety oraz komputera o funkcjonalności twierdzy sieciowej. Zazwyczaj komputer pracuje w wewnętrznej, chronionej sieci, a router zapewnia takie mechanizmy dostępu, aby komputer ten był jedynym urządzeniem widzianym i dostępnym w sieci prywatnej od strony sieci publicznej. Jest to możliwe dzięki filtrowaniu pakietów docierających do routera i przesyłaniu do wnętrza chronionego obszaru tylko tych, które spełniają przyjęte kryteria bezpiecznego dostępu. Zazwyczaj ogranicza się dostęp tylko dla niektórych usług sieciowych. Korzystając z przedstawionego rozwiązania administrator ma do dyspozycji dodatkowe narzędzia i metody umożliwiające konstruowanie zaawansowanych systemów zabezpieczających zasoby sieci prywatnej.

5.5. Wydzielona podsieć realizująca filtrację pakietów *(Screened Subnet)*

Jest to rozwiązanie zbliżone do przedstawionego poprzednio, lecz wykorzystanego dwukrotnie (patrz rysunek). Dla zapewnienia bezpieczeństwa dostępu wydzielono podsieć, która zazwyczaj widoczna jest i dostępna bez większych ograniczeń tak z sieci prywatnej jak i z publicznej. Nie jest natomiast możliwe bezpośrednie komunikowanie się tych dwu sieci. Za taką konfigurację odpowiadają routery filtrując pakiety pod kątem adresata i nadawcy informacji. Dostęp do sieci publicznej z wewnętrznej sieci chronionej możliwy jest dwuetapowo poprzez komputer pracujący w dodatkowej podsieci. Czasami dla zapewnienia bezpiecznej, lecz bezpośredniej pracy pomiędzy sieciami instalowane są w podsieci pośredniczącej komputery-twierdze umożliwiające komunikację na poziomie niektórych usług sieciowych dzięki odpowiedniemu oprogramowaniu lub konfiguracji (Application Level Gateway). Wykorzystywanie dodatkowej podsieci, wydzielonej ze struktury fizycznej sieci prywatnej, ma na celu taką konfigurację sieci, aby możliwe było bezpieczne udostępnianie pewnych zasobów dla sieci publicznej przy jednoczesnej blokadzie dostępu do sieci prywatnej z zewnątrz. Aby zrealizować ten postulat należy umieścić komputery i urządzenia, które chcemy udostępniać ogółowi użytkowników sieci komputerowych, w wydzielonej podsieci utworzonej struktury. Zadaniem administratora jest w takim wypadku właściwa konfiguracja tych urządzeń, aby nie stały się "bocznymi drzwiami" do chronionego systemu, oraz czuwanie nad poprawnością pracy serwera pośredniczącego.



5.6. Gateway realizowany na poziomie aplikacji (Application Level Gateway)

Wiele usług wykorzystywanych w sieciach komputerowych pracuje na zasadzie transmisji danych poprzez kolejne urządzenia, które wysyłają informację dalej, dopiero po przyjęciu jej w całości, oraz przeanalizowaniu zawartości pól sterujących (store-and-forward). Takie rozwiązanie umożliwia realizację kolejnego rodzaju zabezpieczenia, polegającego na pośredniczeniu w przesyłaniu danych określonego typu. Jeśli oprogramowanie realizujące tą funkcję zostanie uruchomione na komputerze dostępnym z obydwu sieci (prywatnej i publicznej) to możliwa jest wymiana informacji pomiędzy tymi, wzajemnie nieosiągalnymi sieciami. Rozwiązanie takie jest stosowane powszechnie podczas przesyłania poczty elektronicznej, której dedykuje się dla usługi publicznej jeden z komputerów o funkcjach twierdzy, a następnie dzięki właściwej konfiguracji zapewnia się transmisję poczty adresowanej do wnętrza sieci prywatnej i na odwrót, bez konieczności komunikacji bezpośredniej pomiędzy nadawcą a odbiorcą wiadomości. Na podobnej zasadzie funkcjonują tzw. proxy-services, czyli rozwiązania bazujące na buforowaniu danych i komunikowaniu korespondentów lub usług niejako w imieniu każdej ze stron. Np. http-proxy (oprogramowanie umożliwiające dostęp poprzez firewall do popularnego ostatnio systemu multimedialnego World Wide Web) wystepując w imieniu użytkownika z sieci wewnętrznej realizuje dostęp do zdalnych serwerów, a następnie uzyskaną odpowiedź przekazuje do wnętrza chronionej sieci komputerowej.

5.7. Routery hybrydowe *(Hybrid Gateways)*

W tej grupie rozwiązań umieszczono inne niż wymienione już architektury firewall. Przykładowo, reprezentantem tej grupy jest rozwiązanie oparte o strukturę: komputer połączony poprzez, wchodzący w skład sieci prywatnej, serwer komunikacyjny. W takim rozwiązaniu komputer ma bezpośredni dostęp do sieci zewnętrznej na zasadach połączenia wyłącznie w tym kierunku, nierzadko poprzez dedykowany strumień danych (tzw. tunel). Rozwiązanie to umożliwia szczegółową specyfikację dostępu do zasobów sieci komputerowej poprzez wskazanie kiedy, jak i na jakich zasadach komputer zestawiający połączenie do serwera komunikacyjnego może korzystać z sieci.

6. PRAKTYCZNE ASPEKTY STOSOWANIA ZAPÓR OGNIOWYCH[16,17]

6.1. Wydajne zapory dla przedsiębiorstw

Pojęcia "zapora ogniowa" i "wysoka wydajność" raczej rzadko występują obok siebie w jednym zdaniu. Biorąc jednak pod uwagę fakt, że łącza sprzęgające sieć LAN z Internetem muszą oferować coraz większe przepustowości, dla wielu administratorów to właśnie wydajność jest jedną z najważniejszych cech zapory. Amerykańskie firmy Opus One i Spirent Communications (partnerzy IDG) opracowały testy porównawcze, które zmierzyły wydajność dostępnych na rynku zapór. Testy mierzyły wydajność każdej zapory, symulując różne sytuacje i rodzaje ruchu pakietów. Testowaniu poddano zapory produkowane przez szesnaście czołowych firm: Cisco (PIX 525), Check Point (Firewall-1), Computer Associates (eTrust),

CyberGuard (KnightStar), Enternet (Enternet Firewall), Lucent Technologies (Brick), NetScreen (NetScreen-100), Network-1 (CyberwallPlus), Network Associates (WebShield), Novell (BorderManager), Nokia (IP650), Secure Computing (SideWinder), SonicWall (SonicWall Pro VX), Symantec (Raptor), TopLayer (AppSwitch 3500) i WatchGuard (Firebox II). Blisko połowa wymienionych zapór sprzedawana jest w postaci zestawu zawierającego oprogramowanie i sprzęt (rozwiązanie oparte na dedykowanej warstwie sprzętowej). Pozostałe zapory to oprogramowanie, które można zainstalować na standardowym komputerze pracującym pod jednym z popularnych systemów operacyjnych. Nie przetestowano zapory Internet Security & Acceleration Server 2000 Microsoftu, która trafiła na rynek już w czasie testowania.

Dla administratorów poszukujących wysoko wydajnych zapór (np. eksploatujących kilka sieci Ethernet 100 Mb/s, które trzeba od siebie odseparować) przeznaczone są produkty oferowane przez NetScreen (NetScreen-100), Cisco (PIX 525) i CyberGuard (KnightStar) pracują bardzo wydajnie. Po podsumowaniu wszystkich testów wydajności na szczególne uznanie zasługuje zapora produkowana przez NetScreen, która uplasowała się na czołowych miejscach we wszystkich kategoriach oceny. Aby sprawdzić, jak zapory sprawują się w różnych (ale typowych) warunkach, opracowano trzy testy: przepływność pierwotna, obsługa połączeń masowych i maksymalne obciążenie użytkownikami.

6.1.1. Przepływność pierwotna

Test ten symuluje dość wiernie ruch pakietów, z jakim zapora może mieć do czynienia wtedy, gdy jest usytuowana w centralnym punkcie dużej sieci komputerowej (separacja poszczególnych segmentów sieci LAN) lub gdy obsługuje aplikacje internetowe (a więc pracuje w środowisku, w którym współużytkowane przez wielu użytkowników pliki muszą zawsze przechodzić przez zaporę).

Testy używały pakietów o skrajnie różnych długościach: bardzo długich (1400 bajtów) i bardzo krótkich (64 bajty). Dla każdej sieci większym obciążeniem są zawsze długie pakiety. Trzeba jednak pamiętać, że dla niejednego urządzenia sieciowego to właśnie krótkie pakiety stanowią prawdziwe wyzwanie. Dlaczego? Ponieważ przy większej liczbie krótkich pakietów zapora musi dysponować wystarczająco dużym zapasem mocy obliczeniowej, aby poradzić sobie z taką nawałnicą. Każdy pakiet musi być przecież odpowiednio przetworzony i obsłużony. Niektóre aplikacje sieciowe pracują wydajniej, gdy mają za partnera zaporę radzącą sobie lepiej z długimi pakietami, a inne wymagają obecności zapory, która lepiej obsługuje większą liczbę krótkich pakietów.

Dziewięć zapór radzi sobie bez problemu z długimi pakietami, nie zakłócając w znaczącym stopniu pracy całej sieci. Trzy produkty - oferowane przez TopLayer (AppSwitch 3500), Nokia (IP650) i NetScreen (NetScreen-100) – są w stanie podołać obciążeniu przekraczającemu 50 proc. obciążenia nominalnego (chodzi o sieć 100 Mb/s), gdy uruchomiono test przesyłający krótkie pakiety. Wyniki dowodzą, że wybór zapory spełniającej wymagania określonego środowiska nie stanowi większego problemu. Jeśli jednak aplikacje uruchamiane w przedsiębiorstwie generują zupełnie różne typy ruchu pakietów, sprawa może być trudniejsza.

Są takie zapory (rozwiązania firm Enternet, Secure Computing i WatchGuard), które obsługują długie pakiety z szybkością 200 Mb/s, ale ich przepływność bardzo wyraźnie spada, gdy zaczynają obsługiwać krótkie pakiety. Najpierw więc należy w miarę dokładnie określić długość pakietów krążących po naszej sieci, a następnie przystąpić do wyboru zapory, biorąc pod uwagę wyniki podane przez nasz test.

6.1.2. Obsługa połączeń masowych

Drugi test sprawdza, jak zapora radzi sobie z bardzo dużą liczbą połączeń TCP. Test bada, czy zapora nie gubi wtedy pakietów albo nie retransmituje ich. Możliwość obsługi dużej liczby połączeń TCP to szczególnie pożądana cecha zapór chroniących wiele serwerów webowych. Protokół TCP został bowiem tak zaprojektowany, że utraty pakietów (albo duże opóźnienia występujące podczas ustanawiania połączenia) są szczególnie dotkliwe dla klientów korzystających z usług serwera webowego. Widać to wyraźnie w przypadku aplikacji webowych, kiedy jedna strona może się składać z kilkunastu, a niekiedy nawet z kilkudziesięciu elementów, a każdy z nich wymaga oddzielnego połączenia z serwerem.
Testy symulowały różną liczbę połączeń TCP (od 25 000 do 120 000) i różne szybkości (od 100 do 15 000 połączeń na sekundę). Serwer webowy akceptujący np. 100 połączeń TCP na sekundę obsłuży po ośmiu godzinach pracy prawie 3 mln połączeń.
Trzy czwarte testowanych zapór uzyskało zadowalające wyniki, obsługując co najmniej 500 połączeń na sekundę. Pomiary prowadzono dla ruchu dwukierunkowego, dotyczą więc połączeń przychodzących i wychodzących. Na początku uruchomiono test generujący 100 i 1000 połączeń na sekundę (ruch jednokierunkowy; tylko połączenia wychodzące), po to, aby skonfigurować w odpowiedni sposób zaporę i upewnić się, że wszystko pracuje poprawnie. Tylko połowa urządzeń radzi sobie z ruchem dwukierunkowym generowanym z szybkością 10 000 połączeń na sekundę. Serwer webowy może przy takim ruchu obsłużyć w ciągu jednego miesiąca 25 mld żądań. Tylko niewiele przedsiębiorstw ma takie wymagania. Dla większości wystarczy wydajność ok. 1 mld żądań na miesiąc, co odpowiada 500 połączeniom na sekundę. Większość testowanych produktów spełnia takie wymaganie.
W świecie zapór połączenie to wyjątkowo cenna rzecz. Jeśli zapora pracuje jako filtr pakietów, ustanawianie połączeń nie jest trudne - wszystkie pakiety wyglądają tu podobnie. Jeśli jednak zapora pracuje jako pełny serwer proxy (a taką możliwość daje produkt firmy CyberGuard), musi wykonać olbrzymią pracę. Urządzenia takie muszą najczęściej współpracować z systemem operacyjnym, aby mogły zawiadywać efektywnie wszystkimi połączeniami TCP i zarządzać tabelami zawierającymi informacje o stanie tych połączeń.
Test połączeń masowych sprawdzał, czy zapora jest w stanie sprostać wielu (ok. 100) regułom obowiązującym w takim środowisku pracy (ustanawianie i obsługa wielu połączeń TCP). Reguły często po ustanowieniu połączenia TCP tworzyły dynamicznie zasady, kreujące "szybką ścieżkę dostępu", zwiększając tym samym szybkość przetwarzania pakietów.
Testy wykazały, że bariera 100 połączeń na sekundę była do pokonania dla większości produktów. Tylko kilka zapór, w tym Raptor (Symantec) i SideWinder (Secure Computing), nie mogło sobie poradzić z taką szybkością, uzyskując wynik odpowiadający zaledwie kilku procentom możliwych do ustanowienia połączeń. Niektóre produkty były skrępowane innymi ograniczeniami. Zapora firmy Network Associates (WebShield) może obsłużyć tylko do 4096 połączeń (jest to ograniczenie sprzętowe). Dlatego może ona chronić sieć składającą się co najwyżej z ok. 500 stanowisk pracy, chociaż teoretycznie jest w stanie obsłużyć wszystkie 4096 połączeń z szybkością 10 tys. połączeń na sekundę.
Inaczej jest w przypadku zapory KnightStar (CyberGuard), oferującej dwa tryby operacji: pełny serwer proxy lub filtr pakietów. Kiedy zapora pracuje jako filtr pakietów, obsługa 10 tys. połączeń nie jest dla niej problemem. Kiedy jednak pracuje w trybie serwera proxy, radzi sobie tylko ze 100 połączeniami na sekundę.
Obsługa 10 tys. połączeń na sekundę wymaga od zapory doskonałej wydajności. Mało jest aplikacji i systemów informatycznych, które mają aż tak duże wymagania. Wśród testowanych urządzeń znajdują się jednak i takie, które radzą sobie nawet z tak dużą liczbą połączeń. Są to zapory produkowane przez firmy Cisco, CyberGuard, Enternet i NetScreen.

6.1.3. Rzeczywiści użytkownicy

Trzeci test sprawdza, jak zapora zachowuje się, gdy obsługuje bardzo dużą liczbę stanowisk pracy. Test ten pozwala ocenić zaporę pod kątem jej przydatności w takim środowisku, w którym musi chronić budynek pełen komputerów PC, których użytkownicy cały czas nawigują po Webie. Używając superszybkich przełączników firmy Extreme Networks, po obu stronach zapory umieszczono 20 stanowisk pracy. Ponieważ po każdej z dwóch stron zapory do jednego portu podłączono wiele stanowisk pracy, w sieci symulowano bardzo duży ruch, nawet coś w rodzaju pewnego chaosu pakietów. Każda zapora musiała sobie sama radzić z tak dużym ruchem (buforując dane i zawiadując w odpowiedni sposób pakietami), tak aby uzyskać jak największą wydajność. Testy tworzyły wiele równoległych połączeń (najcięższy test tworzył nawet 800 połączeń) i następnie uruchamiały procedury przesyłającą dane jednocześnie przez te wszystkie połączenia.
Wyniki podzielono na trzy kategorie: obciążenie niskie (od 100 do 300 jednoczesnych transferów danych); obciążenie średnie (od 400 do 600); obciążenie wysokie (od 700 do 800). Ponieważ połączenia były ustanawiane wcześniej i testy koncentrowały się na operacji jednoczesnego transmitowania danych, test symulujący obciążenie wysokie generował tyle pakietów, że połączenie Fast Ethernet (pełny dupleks) obsługujące zaporę było w 100 proc. nasycone pakietami
Testy używały tych samych 100 reguł, o których wspomniano wcześniej (były to typowe mechanizmy zwiększające bezpieczeństwo pracy chronionego systemu informatycznego). Wynik końcowy uwzględniał wszystkie typy obciążeń: niskie, średnie i wysokie. Jeśli dane musiały być retransmitowane, wynik w odpowiedni sposób obniżano.
Te zapory, którym jest wszystko jedno, jaką liczbę połączeń muszą obsłużyć, pracują z taką samą wydajnością po uruchomieniu testów symulujących różne obciążenia. Do tej kategorii zaliczają się zapory oferowane przez firmy Cisco, CyberGuard, NetScreen, Enternet i Network-1, chociaż przepływność ogólna tej ostatniej zapory jest bardzo mała. Biorą pod uwagę przepływność ogólną, najlepsze wyniki uzyskały produkty firm Nokia, NetScreen, Check Point i Cisco.
Inne zapory nie pracują już tak elastycznie - przy obciążeniu niskim uzyskują niezłą wydajność, ale nie potrafią pracować równie wydajnie po uruchomieniu testu symulującego obciążenie wysokie. Przy obciążeniu niskim najlepszym wynikiem może się pochwalić produkt firmy Secure Computing (SideWinder). Po zwiększeniu obciążenia wydajność tej zapory wyraźnie jednak spada. Podobnie zachowuje się zapora firmy Novell.

6.1.4. Najlepsza zapora

Przy wyborze zapory nie należy się kierować wyłącznie przepływnością pierwotną urządzenia. Liczą się też takie cechy jak łatwość zarządzania, elastyczność pracy i dokumentacja.
Jednak wydajność zapory jest bardzo ważna i - co ciekawe - zależy niejednokrotnie od tego, jakie środowisko będzie musiała obsługiwać. Przeglądając wyniki testów i konfrontując je ze środowiskiem, w którym zapora ma być zainstalowana, można zadecydować, które urządzenie będzie się w nim sprawować najlepiej. Jeśli zamierzamy chronić sieć budynku pełnego komputerów PC, zapora firmy Check Point (Firewall-1) powinna się znaleźć na czołowym miejscu, a zaporę firmy TopLayer (AppSwitch 3500) należałoby raczej wykluczyć (słabe wyniki przy obsłudze dużej liczby użytkowników). Jeśli jednak chcemy chronić większą liczbę serwerów webowych, zapory te można zamienić miejscami (zapora TopLayer obsługuje bardzo dużą liczbę połączeń TCP i oferuje doskonałą przepływność pierwotną). Dużym zainteresowaniem administratorów będą się zapewne cieszyć produkty trzech firm: Cisco, CyberGuard i NetScreen. [4]

6.1.5. Zapory - fakty i mity

Mit: Rozwiązania, które są oparte na dedykowanej warstwie sprzętowej, pracują najwydajniej.
Chociaż pierwsze miejsca we wszystkich testach zajęły zapory oparte na dedykowanych rozwiązaniach sprzętowych, wiele rozwiązań, wykorzystujących standardowe komputery pracujące pod ogólnie używanymi systemami operacyjnymi, uzyskało całkiem zadowalające wyniki. Na przykład zapory firm CyberGuard (KnightStar) i Secure Computing (SideWinder) uzyskały po uruchomieniu testu mierzącego przepływność pierwotną lepsze wyniki niż takie sprzętowe produkty jak Firebox II (WatchGuard) i SonicWall Pro VX (SonicWall).

Fakt:System operacyjny Windows NT nie jest zbyt dobrą platformą do instalowania zapory (pracuje za wolno).
Wiele zapór (w tym eTrust, CyberwallPlus i Raptor) instalowano na wydajnym komputerze, dysponującym dwoma procesorami Pentium III 650 MHz, pracującym pod systemem operacyjnym Windows NT. Jednak rozwiązanie firmy SonicWall (dedykowany sprzęt, oparty na układzie scalonym StrongARM, pracującym z trzy razy mniejszą szybkością niż wspomniane procesory Intela) zajęło we wszystkich niemal testach wyższe miejsca niż zapory uruchamiane na komputerze Windows NT. Dlatego decydując się na rozwiązanie oparte na oprogramowaniu instalowanym na komputerze pracującym pod systemem operacyjnym Windows, proszę pamiętać, że wydajność programów obsługujących protokół TCP/IP, towarzyszących temu systemowi, pozostawia wiele do życzenia.

Mit: Filtrowanie pakietów pracuje najszybciej.
Chociaż producenci zapór przyznają, że pełne serwery proxy pracują zbyt wolno, aby mogły obsługiwać z powodzeniem duże systemy informatyczne, to urządzenia dokonujące dogłębnej inspekcji pakietów (albo rozwiązania pośrednie, czyli w połowie serwer proxy, w połowie filtr pakietów) mogą z powodzeniem konkurować z czystym filtrowaniem pakietów.
Testy wykazały, że produkty oferowane przez Cisco, NetScreen i TopLayer (rozwiązania filtrujące i analizujące dogłębnie transmitowane pakiety) rywalizowały z powodzeniem z zaporą firmy CyberGuard, po skonfigurowaniu jej jako filtr pakietów.

Fakt: Zapora potrafi wykonywać jedne operacje lepiej, a inne gorzej.
Wiele zapór (na przykład Firewall-1 i WebShield) spisuje się bardzo dobrze, gdy chronią sieć przedsiębiorstwa przed światem zewnętrznym (pracują na styku Internet/sieć LAN), a uzyskują dużo gorsze wyniki po zainstalowaniu ich w innych środowiskach (gdy użyjemy ich np. do odseparowania od siebie dwóch sieci LAN). Administrator powinien więc dokładnie poznać swoje środowisko sieciowe, a dopiero potem przystąpić do wyboru odpowiedniej zapory.

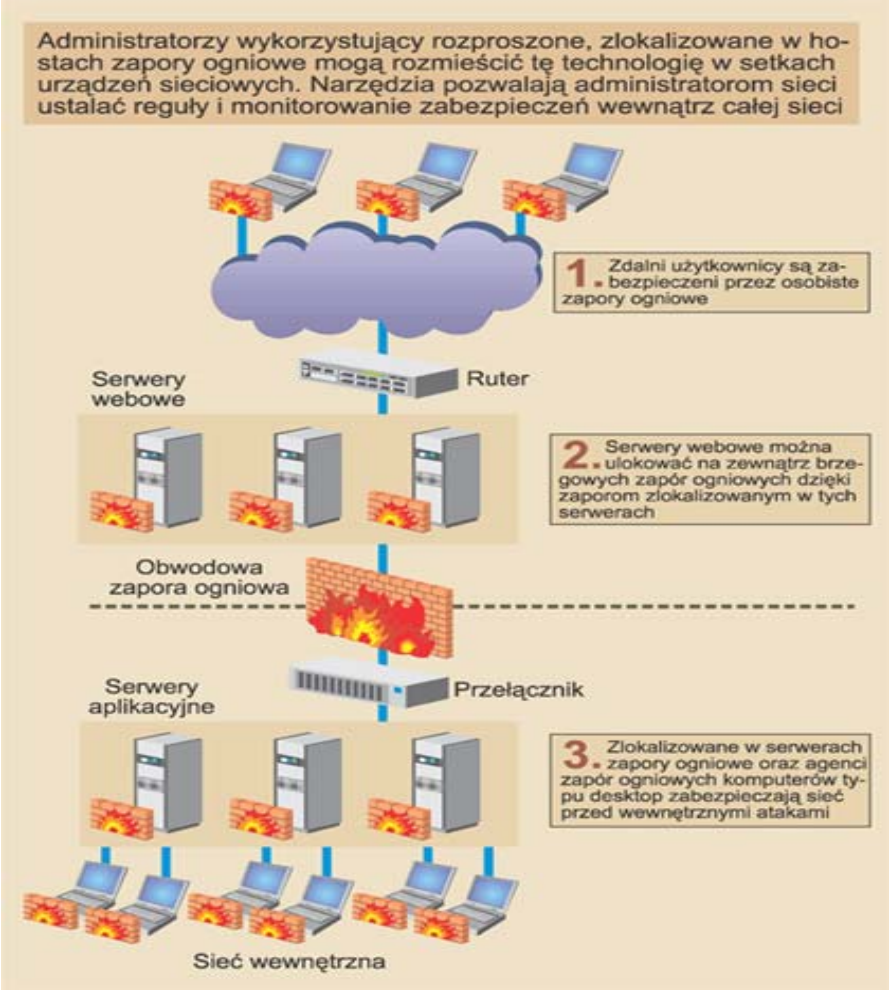
6.2. Karty sieciowe zaporami ogniowymi

Zapory ogniowe wbudowane w karty sieciowe 3Com odciążają główne procesory komputerów i umożliwiają centralne zarządzanie bezpieczeństwem.

Firma 3Com poinformowała o wprowadzeniu na rynek nowej, przeznaczonej do notebooków, karty sieciowej Firewall PC Card oraz nowych wersji kart Firewall Desktop PCI i Firewall Server PCI. Wymienione karty, pracujące w technologii Fast Ethernet 10/100, mają zintegrowaną zaporę ogniową wykorzystującą firmware stworzony przez Secure Computing Corporation. Wraz z oprogramowaniem 3Com Embedded Firewall Policy Server tworzą one system ochrony, w którym karty z wbudowanymi zaporami są konfigurowane i zarządzane przez centralną konsolę. Jeden Firewall Policy Server obsługuje w ten sposób do 1000 kart. Rozszerzenie rozwiązania zintegrowanego systemu zapór (wprowadzonego na rynek w lutym br.), o karty 3Com Firewall PC Cards ma umożliwiać administratorom sieci ochronę zdalnych pracowników, podłączających się do sieci korporacyjnej przez szerokopasmowe łącza VPN. Firewall Policy Server potrafi wykryć, czy użytkownik podłącza się z wewnątrz czy z zewnątrz korporacyjnej sieci LAN. W zależności od miejsca podłączenia użytkownika jest wykorzystywana właściwa dla tej lokalizacji polityka bezpieczeństwa. Dodatkowo 3Com Embedded Firewall Policy Server automatycznie wykrywa obecność nowych produktów, co pozwala na łatwe uaktualnienie lub zmianę konfiguracji zdefiniowanych polityk bezpieczeństwa. W takim systemie jest utrudnione nieuzgodnione z personelem technicznym przenoszenie komputerów w ramach sieci korporacyjnej. Po konfiguracji zapory na karcie komputer może komunikować się tylko z wyznaczonym do tego urządzeniem. Zarządzanie zdalnym PC może odbywać się poprzez tunel VPN z centralnej konsoli zarządzającej. Dodatkowo, w przypadku próby włamania, administratorzy mogą wyłączyć atakowany komputer, jeżeli jest on podłączony do sieci przez kartę 3Com Firewall PC Card.
Zintegrowane rozwiązanie 3Com Embedded Firewall ma umożliwiać menedżerom IT tworzenie ogólno firmowego, rozproszonego systemu bezpieczeństwa, istotnego szczególnie w administracji publicznej, w sektorze bankowo-finansowym, medycznym oraz w instytucjach edukacyjnych.

6.3. Rozproszone zapory ogniowe

Dostęp sieciowy z i do przedsiębiorstwa wymaga solidnych zabezpieczeń. Rozwiązaniem mogą być zapory ogniowe zlokalizowane w hostach (host-resident firewall).
Zapory ogniowe tego typu obejmują osobiste zapory zdalnych użytkowników, agentów zapór ogniowych dla stacji roboczych i rozproszone zapory zlokalizowane w serwerach aplikacyjnych.



Rys. Rozproszone zapory ogniowe [16]

Większość zapór ogniowych zlokalizowanych w hostach, jeśli są konfigurowane i zarządzane w sposób scentralizowany, przyjęto nazywać zlokalizowanymi w hostach rozproszonymi zaporami ogniowymi.
Podobnie jak konwencjonalne zapory ogniowe ochrona zlokalizowana w hostach działa na zasadzie ograniczania ruchu przez implementację reguł kontroli dostępu. W niektórych przypadkach takie zapory dodatkowo wykrywają intruzów i zapobiegają skutkom ich działań. Reguł kontroli dostępu używa się do określenia rodzaju ruchu, miejsca i czasu jego przekazania.
W przypadku osobistych zapór ogniowych implementowanie tych zasad może być tak proste jak deklarowanie wysokiego, średniego i niskiego poziomu bezpieczeństwa.
W przypadku zapór zlokalizowanych w serwerze i agentów zapór ogniowych w stacjach roboczych można stosować politykę zabezpieczeń specyficznych dla danego przedsiębiorstwa, zazwyczaj definiowaną na poziomie protokołów.
Konwencjonalne zapory ogniowe zależą od topologii sieci, w której pracują. Ograniczając ruch w określonych punktach, zapewniają kontrolę i badanie wszystkiego, co przychodzi i wychodzi. W aktywnym środowisku e-biznesowym mogą powodować zatory. Natomiast zapory zlokalizowane w serwerach rozpraszają funkcje zabezpieczające w wielu procesorach, zapewniając nieograniczoną wirtualną skalowalność. Równocześnie eliminują pojedyncze punkty błędu wprowadzane przez konwencjonalne parametryczne zapory ogniowe.
Rozproszone zapory ogniowe zapewniają możliwość określenia scentralizowanej polityki i monitorowanie bezpieczeństwa. Scentralizowana polityka powinna zapewnić możliwość przeniesienia reguł bezpieczeństwa do setek, a nawet tysięcy hostów użytkowników końcowych, serwerów aplikacyjnych tudzież agentów zapór ogniowych. Monitorowanie

bezpieczeństwa zazwyczaj obejmuje gromadzenie i analizę danych dziennika, statystyki zapór ogniowych i - w razie potrzeby - szczegółowe monitorowanie pojedynczych hostów. Zlokalizowane w serwerach zapory są podzbiorem centralnie zarządzanych, rozproszonych zapór ogniowych. Pozwalają dostawcom aplikacji (ASP) i usług internetowych (ISP) oraz przedsiębiorstwom z dużymi farmami serwerowymi zabezpieczać szczególnie ważne serwery. Chociaż zlokalizowane w hostach zapory ogniowe zwiększają obciążenie CPU, to jednak obciążenie to jest rozdzielane pomiędzy komputery farmy serwerowej, minimalizując wpływ na wydajność.
Zapory ogniowe zlokalizowane w hostach zabezpieczają przed szkodliwymi działaniami użytkowników dysponujących prawami wewnętrznego dostępu. Ponadto pozwalają na konfigurowanie zabezpieczeń uwzględniających specyficzne funkcje hosta.
Takie zapory wzmacniają infrastrukturę zabezpieczeń serwerów przed atakami, rekompensując wrodzone słabości zabezpieczeń sieciowych systemów operacyjnych.
Serwery informacyjne i aplikacyjne można ukryć przed niepożądanym dostępem użytkowników przez odrzucanie prób połączeń. Serwery webowe, pocztowe i baz danych też mogą funkcjonować w tym trybie. Jeśli serwera nie można zobaczyć, to nie można go zaatakować.
Większość zapór ogniowych zlokalizowanych w hostach służy do zabezpieczania serwerów internetowych. Tak zabezpieczone serwery mogą być rozmieszczone przed lub za brzegową zaporą ogniową (perimeter firewall).
Przedsiębiorstwa mające do czynienia z przepływem informacji o szczególnym znaczeniu, np. numery kart kredytowych, historie chorób itp., powinny się zdecydować na dwa poziomy zabezpieczeń na swoich serwerach webowych (za zaporami brzegowymi).
Jednak w środowisku, gdzie wydajność jest najważniejsza, należy rozważyć rozmieszczenie serwerów webowych jako hostów - "bastionów" stawiających bezpośrednio czoło Internetowi. W ten sposób można zabezpieczyć serwery protokołów SMTP, HTTP i FTP. W środowisku ASP/ISP farmy wewnętrznych serwerów można zabezpieczyć bez obwodowej zapory ogniowej.
Konwencjonalne zapory ogniowe dotyczą tylko ruchu na obwodzie sieci. Główną zaletą zlokalizowanych w hostach zapór jest to, że mogą filtrować ruch międzysieciowy bez względu na jego pochodzenie.

6.4. Osobiste zapory ogniowe

Użytkownicy, sieci dysponujący bezpośrednim połączeniem z Internetem (modem kablowy, DSL, ISDN, SDI) i rezydujący poza obszarem działania korporacyjnych zapór ogniowych, są narażeni na różnego rodzaju ataki. Ale nawet ci, którzy są pod ochroną korporacyjnych zapór ogniowych, mogą spodziewać się niepożądanych działań, pochodzących z sieci wewnętrznej.
Chociaż zakres ochrony przez większość korporacyjnych zapór ogniowych można uznać za dostateczny, to jednak nie chronią one całkowicie przed włamaniami. Do uszczelniania korporacyjnych zapór ogniowych mogą posłużyć zapory osobiste, zapewniające ochronę dodatkową, chroniące indywidualnych użytkowników przed hakerami, którzy przedostali się przez korporacyjne zapory ogniowe.
Jednak podstawowe zastosowanie osobistych zapór ogniowych to ochrona:
- pracowników mobilnych, często podłączających się do różnorodnych sieci w czasie podróży;
- małych, zamiejscowych oddziałów firmy, nie posiadających korporacyjnej zapory ogniowej;
- pracowników z dostępem przez modem kablowy lub DSL, pracujących w domu.
Wysoka cena korporacyjnych zapór ogniowych, dochodząca niekiedy do kilkudziesięciu tysięcy dolarów, zniechęca mniejsze firmy lub oddziały zamiejscowe do ich powszechnego

stosowania. Ponadto firmy często korzystają z modemów kablowych jako niedrogiego środka połączenia z Internetem.
Osobiste zapory ogniowe są relatywnie tanimi programami lub urządzeniami instalowanymi bezpośrednio na PC. Przejmują one kontrolę nad sprzętem sieciowym i wykonują podstawowe funkcje zapór ogniowych: wykrywanie włamań, kontrola dostępu, egzekwowanie reguł polityki udostępniania zasobów i rejestrowanie zdarzeń. Filtrując cały ruch sieciowy, dopuszczają jedynie komunikację autoryzowaną. W przeglądzie omówiono dwie kategorie rozwiązań osobistych zapór ogniowych: rozwiązania czysto programowe i oddzielne urządzenia.
Produkty czysto programowe można podzielić na dwa rodzaje: rozwiązania korporacyjne, przystosowane do centralnego zarządzania, i rozwiązania autonomiczne, lepiej dostosowane do biur domowych lub właścicieli małego biznesu.
Jeżeli osobista zapora ogniowa ma być używana przez więcej niż kilku użytkowników, to powinna istnieć jakaś możliwość jej centralnej dystrybucji i zarządzania. Takimi cechami charakteryzują się opisane dalej Sygate Personal Firewall firmy Sygate Technologies (dawniej Sybergen) i BlackICE Defender firmy Network ICE. Rozwiązania bardziej autonomiczne to Norton Personal Firewall 2000 firmy Symantec i Personal Firewall firmy McAfee.com. [5]

6.4.1. Bezpieczny desktop

Sygate Personal Firewall skutecznie zakrywa wszystkie porty - potencjalny haker może odnosić wrażenie, że maszyna jest odłączona od sieci lub wyłączona. Program uniemożliwia uzyskanie jakichkolwiek informacji, dostępnych zazwyczaj na komputerach podpiętych bezpośrednio do Internetu, takich jak nazwa komputera i jego użytkownika lub grupy użytkowników. Używany z Sygate Management Server może efektywnie i dostatecznie zabezpieczać również środowisko korporacyjne.
Panel sterujący programu jest bardzo prosty. Można z niego blokować każdy port, a program pozwala specyfikować ruch TCP, UDP lub oba naraz. Personal Firewall zawiera także zaawansowane wsparcie protokołu ICMP (Internet Control Message Protocol), ze sterowaniem opartym na typie ICMP, a także wsparcie pcAnywhere Symanteca.
Panel sterowania pozwala na ustawienie pięciu stopni ochrony: "bardzo wysoki", "wysoki", "średni", "niski" i "wyłączony". Stopnie "bardzo wysoki" i "wyłączony" to pozycje skrajne - praktycznie uniemożliwiają one korzystanie z komputera w sieci (pierwszy ze względu na całkowitą blokadę, drugi z uwagi na pełne otwarcie). Stopień "wysoki" umożliwia dostęp do Internetu przez Internet Explorer i Outlook, zachowując jednocześnie wysoki poziom bezpieczeństwa. Inne aplikacje, aby mogły być używane, muszą być wprowadzone na listę aplikacji dopuszczonych do użytkowania w sieci. Aplikacje, które mają gwarantowany dostęp do sieci, zachowują ten dostęp niezależnie od ustawionego poziomu ochrony. Sygate Personal Firewall pozwala administratorom ustawiać poziom ochrony przypisany do określonych przedziałów czasowych w ciągu dnia. Umożliwia to zwiększenie zakresu dostępu w ciągu dnia pracy i uszczelnianie go w godzinach popołudniowych i nocnych. W pakiecie można znaleźć wiele praktycznych funkcji, takich jak powiadamianie o incydentach za pośrednictwem poczty elektronicznej i zabezpieczanie hasłem.
Okno konfiguracyjne pakietu oferuje szereg możliwości. Zaawansowane ustawienia portu mogą być adjustowane ręcznie lub według typowych szablonów, takich jak: "allow to browse Network Neighborhood" czy "share via Network Neighborhood". Inne opcje to wybierane jednym kliknięciem DHCP (Dynamic Host Configuration Protocol), kilka dobrze znanych VPN, pcAnywhere itp. W przypadku ręcznego sterowania dostępem do portu można otwierać specyficzne porty lokalne dla portów zewnętrznych, jak również dopuścić wewnętrzny dostęp aplikacyjny przez specyficzne porty. Obie opcje mogą być ustawiane zarówno dla ruchu TCP, jak i UDP (lub obu naraz).

Instalacja pakietu jest rutynowa, aczkolwiek Sygate Personal Firewall wymaga restartu systemu po instalacji. Dokumentacja programu jest wystarczająco szczegółowa i nie odbiega od poziomu dokumentacji innych produktów.
Pakiet antywłamaniowy **BlackICE Defender** firmy Network ICE wywodzi swoją nazwę od pojęcia Intrusion Countermeasure Electronics, odnoszącego się do oprogramowania podejmującego próby zneutralizowania lub usunięcia intruza w odpowiedzi na wtargnięcia do sieci. Chociaż BlackICE nie do końca jest tego typu oprogramowaniem, to jednak zawiera mechanizm o nazwie Backtrace, pozwalający na uzyskanie szczegółowych informacji o napastniku. Mechanizm sprawdza cały ruch wchodzący i wychodzący oraz aktywność podejrzanych programów. Mechanizm pracuje w czasie rzeczywistym, nie blokując dostępu do sieci. Napastnik identyfikowany jest po adresie IP, węzłach, DNS, adresach MAC i NetBIOS. Niestety, BlackICE blokuje tylko porty, natomiast nie kontroluje aplikacji. Tak więc jeżeli "koń trojański" znajdzie furtkę do systemu, to może użyć dowolnego otwartego portu do komunikowania się ze swoim autorem.
BlackICE ma cztery poziomy ochrony: 'ufny", "ostrożny", "nerwowy" i "paranoiczny"(!). Chociaż każdy z tych poziomów dopuszcza pełną komunikację wychodzącą, to jednocześnie na każdym z nich są zapewniane coraz bardziej restrykcyjne filtry dla ruchu wejściowego. Przy ręcznym wprowadzaniu adresów IP - i do grupy zaufanych, i blokowanych - BlackICE dopuszcza zarówno pełny dostęp, jak i całkowitą blokadę pakietów od nich przychodzących. Network ICE przestrzega przed dodawaniem adresów IP do bloku zaufanych, jeżeli nie jest się całkowicie pewnym, że są bezpieczne.
Ponieważ adresy IP mogą być z łatwością fałszowane, dobrym zwyczajem jest konfigurowanie routerów sieciowych w sposób nie dopuszczający pakietów powiązanych z adresami własnej podsieci IP, jeżeli pochodzą spoza tej podsieci.
Poza czterema poziomami ochrony BlackICE ma cztery poziomy alarmów: "krytyczny", "poważny", "ostrzegający" i "informacyjny". Program jest trochę rozwlekły w przypadku raportowania zdarzeń - rejestruje prawie wszystko. Na szczęście okno historii zdarzeń pozwala na oglądanie czasowo zależnej reprezentacji ruchu sieciowego odnoszącej się do potencjalnych ataków. Pakiet jest niezwykle łatwy w instalacji - instaluje się jako usługa Windows NT, bez potrzeby przeładowywania systemu. Jest to cecha przypisywana oprogramowaniu korporacyjnemu, które powinno być instalowane w sposób nie zakłócający pracy systemów. Dokumentacja towarzysząca pakietowi jest gruntowna, zawiera opisy wszystkich mechanizmów zawartych w programie. Zawiera także bardzo dobry wstęp do zagadnienia wykrywania intruzów i sposobów zapobiegania atakom.
Norton Personal Firewall 2000 firmy Symantec używa tego samego interfejsu co okno zarządzające programu Norton AntiVirus 2000. Firma połączyła te dwa programy, tak więc można zarządzać Norton Personal Firewall 2000 i Norton AntiVirus 2000 z tego samego panelu sterującego.
Menu "Security" pozwala na blokowanie zewnętrznego dostępu, a menu "Privacy" pozwala na ograniczenie innym osobom możliwości transmisji prywatnych informacji z komputera bez używania połączeń szyfrowanych. Norton Personal Firewall jest jedynym produktem wśród prezentowanych, który w konfiguracji domyślnej umożliwia przetransmitowanie nazwy użytkownika, nazwy komputera, domeny i adresu MAC karty sieciowej. Wszystkie te dane są łakomym kąskiem dla hakera. Problem ten związany jest ze starszymi modelami modemów kablowych, wymagającymi nazwy komputera przy uwierzytelnieniu przed przydzieleniem adresu TCP/IP przez DHCP. Firma, chcąc uniknąć problemów z tymi modemami, przyjęła zasadę, która uaktywnia NetBIOS Name i NetBIOS Datagram domyślnie. Jest rozważana zmiana domyślnych ustawień konfiguracyjnych w przyszłych wydaniach pakietu. Aby wyłączyć te funkcje ręcznie, należy po prostu wybrać opcje "Internet security" i "Advanced options", a następnie wybrać zakładkę Firewall i wyłączyć NetBIOS Name i NetBIOS Datagram. Blokowanie adresu MAC jest bardzo ważne. Jest to przecież globalnie unikatowy identyfikator i połączony z innymi informacjami może pozwolić hakerowi na penetrowanie

poszczególnych maszyn, nawet w sytuacji, gdy adresy IP są przydzielane przez DHCP. Chociaż pakiet jest niewątpliwie wysokiej klasy zaporą ogniową, ta cecha, związana z początkowymi ustawieniami konfiguracyjnymi, może obniżać jego wartość w oczach mniej doświadczonych użytkowników.
Program jest niezwykle łatwy do zainstalowania, chociaż wymaga przeładowania systemu. Dokumentacja jest wystarczająca i zawiera sporo informacji dla mniej doświadczonych użytkowników. Jest już dostępna wersja 2001, kompatybilna z Windows ME, monitorująca i blokująca kontrolki ActiveX, aplety Javy i cookies.
PC Firewall w powłoce McAfee
Personal Firewall firmy McAfee.com jest desktopową wersją PC Firewall firmy ConSeal - McAfee nabyła prawa do używania motoru tej firmy w swoim produkcie. Chociaż nowa powłoka została pod każdym względem ulepszona w stosunku do pierwowzoru, to jednak ogranicza użytkownika w wykonywaniu zmian, zwłaszcza modyfikowaniu zestawu reguł. Produkt nie jest jednak przeznaczony dla administratorów systemu, tak jak jego protoplasta. Produkt firmy McAfee.com pracuje w trybie adaptacyjnym, ale używa też wbudowanych zestawów reguł, podobnych do stosowanych w PC Firewall. Wszystkie dostosowania wykonywane przez użytkownika modyfikują po prostu zestaw reguł. Konfiguracja domyślna blokuje wszystkie drukarki sieciowe i współdzielenie plików, dopóki nie zmieni się tego ustawienia w oknie konfiguracyjnym "NetBIOS over TCP/IP". Program pozwala także na blokowanie aplikacji specyfikowanych przez użytkownika.
Chociaż produkt jest łatwy do zarządzania, to jednak brak mu elastyczności i skalowalności. Produkt tego typu powinien wykazywać się cechami, takimi jak możliwość użytkowania w różnych systemach i przez użytkowników z różnym stopniem doświadczenia. Do zainstalowania wymaga on sterowników sieciowych, co nie jest cechą pożądaną przez zbyt wielu użytkowników. Większość użytkowników korporacyjnych używających Windows NT nie ma dostępu do nich i musi do tego celu zatrudniać personel IT.
Przy instalowaniu programu wraz z Norton AntiVirus 2000 może wystąpić problem wstrzymywania pracy programu instalującego. Aby tego uniknąć, należy wykluczyć z przeszukiwań antywirusowych podkatalog SIGNAL9*.*. Po tych zmianach instalacja przebiega bezproblemowo, chociaż program żąda zainstalowania swoich sterowników jako usług sieciowych, co jest krokiem dodatkowym, nie spotykanym w innym przypadku. Sama instalacja jest też czasochłonna i zaleca się, aby wykonywały ją osoby z pewnym doświadczeniem.

6.4.2. Sprzętowe rozwiązania osobistych zapór ogniowych

Każda sieć potrzebuje pewnej formy zabezpieczeń, problem jednak tkwi w dokładnym wypośrodkowaniu pomiędzy ceną mechanizmów zabezpieczających a łatwością ich użycia. Wraz ze wzrostem liczby połączeń typu "always on" (takich jak DSL) potrzeba stosowania prostych zapór ogniowych staje się w przypadku telepracowników coraz pilniejsza. Na rynku można znaleźć wiele rozwiązań: od produktów czysto programowych, pracujących na powszechnie stosowanych pecetach, do jednostek, kosztujących dziesiątki tysięcy dolarów, przeznaczonych do ochrony sieci przedsiębiorstw.
Przyjrzyjmy się trzem urządzeniom średniej skali, w cenach od 400 do kilku tysięcy USD. Są to SOHO firmy Sonic-Wall, SOHO firmy WatchGuard Technologies i Interceptor firmy Technologic/eSoft. Urządzenia te są przygotowane dla oddziałów firm, biur domowych i użytkowników bez większego doświadczenia.
SOHO SonicWall i SOHO WatchGuard są urządzeniami specjalnego przeznaczenia, z czteroportowym hubem, i pracują pod kontrolą zagnieżdżonego systemu operacyjnego. Interceptor jest zbudowany w oparciu o elementy PC i odmianę systemu operacyjnego Unix, oferuje również możliwość podłączenia klawiatury i monitora.

Najciekawszą propozycją wydaje się SOHO firmy SonicWall - charakteryzuje się on najkorzystniejszym stosunkiem ceny do możliwości.
SOHO firmy WatchGuard jest urządzeniem podstawowym, bez nadmiaru mechanizmów, ale dzięki temu niezwykle prostym. Z kolei Interceptor firmy eSoft jest bardzo elastyczny i zawiera rozbudowane opcje menu.
Ustawianie i konfigurowanie
Na ocenę urządzenia w znacznym stopniu wpływa wrażenie przy pierwszym zetknięciu się z produktem. Urządzeniem zabierającym najmniej czasu w procesie ustawienia i konfigurowania jest WatchGuard SOHO - proces ten można zamknąć w kilkunastu minutach. Niewiele więcej zajmuje instalowanie SonicWall SOHO. Interceptor natomiast wymaga dużo więcej pracy i szczegółowego studiowania dokumentacji.
Wyjątkowym mechanizmem SonicWall SOHO jest sposób, w jaki po raz pierwszy należy zmienić hasło domyślne. Jest to czynność często ignorowana przez wielu nawet doświadczonych użytkowników, chociaż może to narażać bezpieczeństwo sieci. Jest to też jedyne urządzenie, które nie odpowiada na ping z sieci zewnętrznej. Jednym z ograniczeń SonicWall SOHO jest konieczność stosowania przeglądarki Netscape przy ustawianiu - program konfiguracyjny, napisany w Javie, nie współpracuje poprawnie z przeglądarką Internet Explorer. Pomijając to ograniczenie proces instalacji wymaga wprowadzenia minimalnej ilości informacji i można go zamknąć w kwadransie. Na stronie webowej firmy można obejrzeć ekrany zarządzania urządzeniem
SonicWall SOHO i WatchGuard SOHO mają ekrany konfiguracyjne zorganizowane w proste okienka zaznaczania pozycji, pozwalające na wyłączenie rozgłaszania protokołowego sieci Microsoft Server Message Block na zaporach ogniowych, stwarzającego spore ryzyko niebezpieczeństwa dla użytkowników z małych biur, chcących współdzielić pliki - niekoniecznie przez Internet. W pozostałych produktach wymaga to znacznie więcej zabiegów. Wspólną wadą wszystkich urządzeń jest brak narzędzi diagnostycznych, pozwalających np. wykrywać błędnie ustawione adresy IP. Główną tego przyczyną jest brak możliwości dołączania do większości urządzeń klawiatury czy monitora. Interceptor jest jedynym urządzeniem, które pozwala na użycie tego dodatkowego wyposażenia.
Mechanizmy zarządzania
Jedną z ważniejszych funkcji zarządzania w przypadku implementacji sprzętowej jest możliwość uaktualniania firmware, pozwalająca na wprowadzanie nowych mechanizmów do urządzeń i usuwanie ewentualnych błędów. Najłatwiejszym uaktualnianiem charakteryzuje się WatchGuard SOHO - jego firmware jest stale dostępne na witrynie webowej, zawierającej dokładną instrukcję uaktualniania. Interceptor dysponuje prostym menu do wykonywania uaktualnienia (wcześniej trzeba zarejestrować się u dostawcy, aby otrzymać identyfikator i hasło). Proces uaktualniania SonicWall SOHO wymaga odszukania nowego firmware na witrynie dostawcy, sprowadzenia go na PC i następnie załadowania do urządzenia. Ustawienie publicznego serwera webowego w sieci chronionej (co oznacza, iż jest on dostępny w Internecie) jest proste w przypadku WatchGuard SOHO i SonicWall SOHO. Interceptor wymaga znacznie większych zabiegów i najprostszym wyjściem wydaje się użycie trzeciej karty interfejsu sieciowego podłączonego do wydzielonej sieci.
Każda z zapór ogniowych dysponuje różnymi rodzajami raportów. Najlepsze raporty to takie, które wskazują potencjalne problemy bezpieczeństwa. WatchGuard SOHO i SonicWall SOHO pokazują strefy chronione i nie chronione. Oba także ostrzegają, jeżeli ustawienia konfiguracyjne mogą narażać bezpieczeństwo sieci. WatchGuard SOHO może wysyłać swoje logi do odległego hosta, ale jest to funkcja bardzo uproszczona. SonicWall SOHO można ustawić na przesyłanie plików logu pocztą elektroniczną pod dowolny adres internetowy. Interceptor zawiera różnego rodzaju raporty, ale większość z nich wymaga, przy interpretacji, kwalifikacji doświadczonego administratora Unixa. Urządzenie może być skonfigurowane do wysyłania alarmów na pagery lub pocztą elektroniczną - w razie zaistnienia określonych zdarzeń, takich jak wykrycie skanowania portu czy serii nielegalnych logowań.

Ostatnią sprawą z zakresu administrowania jest zarządzanie hasłami. Interceptor wymaga wprowadzenia wielu różnych haseł do poruszania się po różnych pozycjach menu. Pozostałe dwa urządzenia wymagają jedynie wprowadzenia identyfikatora administratora i pojedynczego hasła.

Ochrona i mechanizmy sieciowe

Najlepszymi mechanizmami ochrony dysponuje SonicWall SOHO oraz Interceptor, który oferuje wiele opcji przystosowania zapory ogniowej. Słabiej w mechanizmy ochronne jest wyposażony WatchGuard SOHO. Chociaż blokuje on zewnętrzny ruch do sieci, przez ustawienia specyficznych portów sieciowych jako dostępnych lub utworzenie specyficznych reguł filtracji na zaporze ogniowej, to jednak nie ma on takich możliwości przystosowywania jak pozostałe.

Najnowsza wersja SonicWall SOHO zawiera możliwość skanowania antywirusowego na zaporze ogniowej, bez konieczności instalowania indywidualnego oprogramowania antywirusowego na każdym komputerze.

Z kolei różnorodne konfigurowanie interfejsu sieciowego dopuszcza jedynie Interceptor (Token Ring, Frame Relay, ISDN).

Większość użytkowników potrzebuje serwera DHCP, pracującego na zaporze ogniowej i ułatwiającego rozdział adresów IP do reszty sieci. Zarówno WatchGuard SOHO, jak i SonicWall SOHO zawierają serwery DHCP łatwe do ustawiania. Ustawienie Interceptora jest bardziej skomplikowane. W pierwszej kolejności należy ustalić adres IP i dopiero wówczas uruchomić serwer DHCP z interfejsem webowym.

Wszystkie zapory zawierają mechanizm NAT (Network Address Translation), pozwalający na skuteczną ochronę sieci lokalnej przed atakiem z zewnątrz. NAT pozwala na ustawienie prywatnych adresów IP poza zaporą ogniową i odwzorowanie ich w pojedynczy, wirtualny adres IP. Uniemożliwia to hakerowi namierzenie maszyny, z której pochodzi ruch pakietów. Poza tym można w ten sposób oszczędzić rzeczywiste adresy IP dostępne w organizacji.

Domyślne ustawienia w każdym urządzeniu blokują dostęp zewnętrzny i dopuszczają ruch wewnętrzny poza sieć. W każdej zaporze można poprzez interfejs webowy ustawiać dodatkowe reguły. Mechanizmy VPN, a także blokowanie poszczególnych URL dostępne są we wszystkich urządzeniach.

7. PROGRAMOWE FILTRY PAKIETÓW DOSTĘPNYCH W SYSTEMIE LINUX

Jednym z niezwykle popularnych systemów operacyjnych stosowanych do zarządzania siecią komputerową jest Linux. Niezaprzeczalną jego zaletą jest jego bezpłatność. Całe oprogramowanie dostępne jest formie Open Source. Użytkownik otrzymuje kod źródłowy programu kompiluje go na swojej maszynie uzyskując ten sposób wykonywalny program. Jest to bardzo wygodne z punktu widzenia bezpieczeństwa systemu gdyż umożliwia swobodny wgląd kod programu. Możliwa jest jego analiza ewentualne wychwytywanie dostępnych dziur zabezpieczeniach itp.

Z tego też względu Linux doskonale nadaje się do zastosowania jako narzędzie zabezpieczające naszą sieć przed atakami globalnego Internetu. Posiada on bardzo rozbudowane opcje konfiguracji jako firewall, możliwości te są wciąż rozwijane przez jego użytkowników.

Spośród wielu pakietów Linux oferuje kilka narzędzi które umożliwiają użycie go jako firewalla. Istnieje możliwość łączenia ich ze sobą już na poziomie jądra.

Spośród dostępnych filtrów pakietów wyróżniamy:

- Ipfw
- Ipchains (ver. 2.2.)
- Iptables (ver. 2.2.4)

Narzędzia wymienione powyżej wymienione są kolejności ich powstawania. Im nowszy tym bardziej ma rozwinięte możliwości konfiguracji jest wygodniejszy użyciu.

Przed przedstawieniem jakiegoś konkretnego przykładu zastosowania tych narzędzi należy trochę zgłębić podstawy ich działania.

Cały ruch przesyłany przez sieć jest przesyłany w formie pakietów. Początek każdego pakietu mówi skąd przybył i dokąd zmierza, ponadto zawiera inne elementy takie jak protokół, port źródłowy przeznaczenia. Ta część pakietu nazywana jest nagłówkiem.
Filtry pakietów to oprogramowanie, które sprawdza nagłówki pakietów decydując następnie o ich dalszym losie. Możliwych jest kilka sposobów postępowania pakietem tj. można go odrzucić, anulować lub zaakceptować. Należy jeszcze wspomnieć czym różni się anulowanie pakietu od jego odrzucenia. W przypadku anulowania filtr pakietów zachowuje się tak jakby pakiet nigdy do niego nie trafił tj. otrzymuje go zaraz nim zapomina, natomiast w drugim przypadku do źródła informacji przesyłana jest informacja o odrzuceniu pakietu.
Generalnie jądro systemu dzieli ruch firewall'a na trzy typy i do każdego nich stosuje inny filtr. Przychodzący ruch zanim zostanie zaakceptowany, jest testowany według reguł wchodzącej ściany ogniowej (input). Wychodzący ruch przed wysłaniem jest testowany zgodnie regułami ściany wychodzącej (output), natomiast ruch przekazywany poprzez system jest testowany zgodnie regułami ściany ogniowej przekazującej (forward). Oprócz tych trzech kategorii użytkownik może definiować własne kategorie. Jądro dla każdej kategorii utrzymuje listę reguł nazywanych łańcuchami. Każdy pakiet wchodzący, przesyłany przez warstwy rutujące Linuxa lub wychodzący jest przechodzi kolejno przez wszystkie reguły w danym łańcuchu.

7.1. IPCHAINS[15]

Polecenie **ipchains** posiada następujące opcje (wymienię tylko te najistotniejsze dla nas):

A – dodaje regułę na koniec łańcucha
C – sprawdza pakiet zgodnie regułami łańcuchu
D – usuwa wybraną regułę z łańcucha
F – usuwa wszystkie reguły z łańcucha
I – wstawia regułę do łańcucha
L – wypisuje listę wszystkich reguł w łańcuchu
P – ustawia domyślną politykę
X – usuwa określony łańcuch

Reguły ściany ogniowej składają się z filtra, do którego dopasowywane są pakiety. Gdy pakiet zostanie dopasowany, podejmowane jest działanie które może być albo standardową zasadą albo może wskazywać na zdefiniowany przez łańcuch reguł, w celu dalszego przetworzenia.
Standardowe zasady postępowania to:
accept – zezwala na przejście pakietu
reject – odrzuca pakiet zwracając do nadawcy komunikat o błędzie
deny – odrzuca pakiet, a do nadawcy nie jest wysyłany żaden komunikat
masq – maskuje pakiety w ten sposób aby wyglądały tak jakby pochodziły z lokalnego hosta

redirect – przekierowanie pakietu

Do konstruowania filtrów możemy użyć także parametrów polecenia ipchains :
- p *protokół* – definiuje protokół
- s *adres* - definiuje źródło pakietu
- d *adres* - definiuje cel pakietu
- j *cel* – określa standardowe zasady postępowania lub zdefiniowany przez użytkownika łańcuch do którego powinna być przekazana kontrola
- i *nazwa* – określa nazwę interfejsu
- b – wskazuje regułę pasującą do danego pakietu w obu kierunkach

Poniżej zamieszczono przykładowy plik konfiguracyjny firewall'a dla sieci.
Sieć lokalna którą firewall ma chronić jest przyłączona do interfejsu eth0, adres tej sieci to: 192.168.0.0. Internet jest przyłączony do interfejsu eth1.

Rc.firewall

```
echo Początek skryptu obsługi firewall'a
export PATH=/sbin

#
#ustawianie domyślnej polityki na DENY przed wyczyszczeniem wszystkich
#reguł z łańcucha, zabezpieczy nas to przed niepożądanymi skutkami awarii
#firewall'a w przypadku gdyby coś poszło źle w poniższym skrypcie
#

# Ustawienie polityki DENY dla łańcucha wejściowego oraz wyczyszczenie tego
#     łańcucha

ipchains -P input DENY
ipchains -F input

# Ustawienie polityki DENY dla łańcucha przekazującego oraz wyczyszczenie  #
      tego łańcucha

ipchains -P forward DENY
ipchains -F forward

# zakładamy że użytkownicy w sieci wewnętrznej są godni zaufania i mogą    #
      uzyskać dostęp do naszego firewall'a

ipchains -P output ACCEPT
ipchains -F output

#  Uruchomienie weryfikacji adresów źródłowych, operacja ta pozwala na
#zabezpieczenie się przed atakami typu spoofing


for f in /proc/sys/net/ipv4/conf/*/rp_filter; do echo 1 > $f; done

# od strony sieci lokalnej mają być akceptowane wszystkie pakiety
ipchains -A input -i eth0 -j ACCEPT

#akceptowanie pakietów pochodzących z interfejsu lokalnego

ipchains -A input -i lo -s 127.0.0.0/8 -d 127.0.0.0/8 -j ACCEPT

# Internet konfiguracja
# akceptacja DHCP
```

```
ipchains -A input -i eth1 -p udp -s 0/0 67 -d 0/0 68 -j ACCEPT
# akceptacja DNS
ipchains -A input -i eth1 -p udp -s 0/0 53 -d 0/0 1024:65535 -j ACCEPT

# blokada każdej próby dostępu do uprzywilejowanych portów
ipchains -A input -i eth1 -p tcp -d 0/0 0:1024 -j DENY --log
ipchains -A input -i eth1 -p udp -d 0/0 0:1024 -j DENY --log

# allow all TCP except incoming connections (priv. ports blocked above)
ipchains -A input -i eth1 -p tcp ! --syn -j ACCEPT

#przykładowo odrzucamy wszystkie połączenia z adresem podejrzanej sieci
ipchains -A input -i eth1 -s 224.0.0.0/3 -j DENY
ipchains -A input -i eth1 -d 224.0.0.0/3 -j DENY
ipchains -A input -i eth1 -s 224.0.1.40/3 -j DENY
ipchains -A input -i eth1 -d 224.0.1.40/3 -j DENY

# blokada zdalnego połączenia z x-serwerem
ipchains -A input -i eth1 -p udp --dport 6000:6010 -j DENY --log
ipchains -A input -i eth1 -p tcp --dport 6000:6010 -j DENY --log

# zezwalamy na caly ruch bazujący na protokole UDP powyżej portu 1023
ipchains -A input -i eth1 -p udp --dport 1024: -j ACCEPT

# ICMP
# Dopuszczamy cały ruch tego typu
ipchains -A input -p icmp -j ACCEPT

# przechwytujemy cały pozostały ruch kierowany na wejścia interfejsów,     #
odrzucamy go i logujemy
ipchains -A input -j DENY --log

#- output ----------------------------------------

# Internet
#  wszystkie pakiety adresowane do sieci wewnętrznej na interfejsie
# eth1(strona Internetu) są odrzucane

ipchains -A output -i eth1 -d 192.168.0.0/24 -j REJECT


#- forward ---------------------------------------
#załadowanie modułów potrzebnych przy wykorzystywanych usługach np.irc ftp:
modprobe ip_masq_irc
modprobe ip_masq_ftp
modprobe ip_masq_autofw

#uruchomienie funkcji przekazywania pakietów
echo 1 > /proc/sys/net/ipv4/ip_forward

# uruchomienie masquarady dla ruchu od naszej sieci do Internetu
ipchains -A forward -i eth1 -s 192.168.0.0/24 -j MASQ

# przechwytujemy cały pozostały ruch i go odrzucamy
ipchains -A forward -j REJECT --log

echo Firewall uruchomiony

#rc.firewall koniec
```

7.2. IPTABLES [14]

Konfiguracja **iptables** odbiega nieco od ipchains, głównie dlatego że nowy filtr jest w dużej mierze modularny. Opcje, które kiedyś były stałymi parametrami programu ipchains są tutaj realizowane przez poszczególne moduły. Do poprawnego działania potrzebne są odpowiednie moduły, wkompilowane w jądro 2.4 oraz program iptables, służący do konfiguracji filtra.
Filozofia nowego filtra jest podobna do poprzedniej wersji - mamy tutaj także trzy domyślne zestawy reguł INPUT, FORWARD i OUTPUT oraz szereg celów które określają co należy zrobić z pakietem pasującym do danej regułki. Najczęściej używane to ACCEPT, DROP oraz REJECT. Znaczącą różnicą jest natomiast to że pakiety przesyłane z innych interfejsów przechodzą wyłącznie przez zestaw FORWARD. Dwa pozostałe zestawy INPUT i OUTPUT obsługują wyłącznie pakiety kończące drogę na lokalnym systemie lub na nim generowane.
Funkcja śledzenia połączeń jest w iptables realizowana przez moduł *state*.

Poniżej zamieszczono przykładowy plik konfiguracyjny firewall'a dla sieci z wykorzystaniem iptables.
Sieć lokalna którą firewall ma chronić jest przyłączona do interfejsu eth0, dostęp do Internetu realizowany jest przez interfejs ppp0.

```
#!/bin/sh

#  .
#  Ten skrypt zawiera funkcje zmniejszające szansę odcięcia
#  sobie dostępu do danego hosta podczas zdalnej konfiguracji.
#

#  Opcje skryptu:
#  flush - czyści wszystkie regulki i ustawia otwarta politykę
#  temp - konfiguruje tymczasowe regulki (patrz poniżej)
#  bez opcji - konfiguruje iptables

#  Kolejność operacji:
# 1. zerowanie wszystkich tablic
# 2. ustawienie restrykcyjnej polityki DROP
#   3. ustawienie specjalnego dostępu dla interfejsu lo
#   4. ustawienie specjalnego dostępu dla sieci LAN
#   5. ustawienie odrzucania połączeń dla IDENT i SOCKS
#   6. zezwolenie dla pakietów ICMP Echo (ping)
#   7. konfiguracja stateful-inspection (moduł state)
#   8. ustawienie dostępu dla konkresnych usług
#  9.  konfiguracja NAT i PAT
#  10. konfiguracja logowania zablokowanych pakietów

export PATH=""

iptablesflush(){
/sbin/iptables -P INPUT ACCEPT
/sbin/iptables -P OUTPUT ACCEPT
/sbin/iptables -P FORWARD ACCEPT
/sbin/iptables -F
}
if [ "$1" = "flush" ] ; then
iptablesflush
exit O
```

```
fi

#  Bezpieczne wywołanie iptables, gwarantujące ze
#  nasze regulki zostaną załadowane albo w całości
#  albo w ogolę. Zapobiega to sytuacji, kiedy tracimy
#  dostęp do danego hosta z powodu jednej , złe skonstruowanej
#  regulki   która   miała   nas   do   niego   wpuszczać
   iptables (){
echo -n .
/sbin/iptables $@
if [ "$?" != "O" ] ; then
iptablesflush
exit l
fi
}


#  Możemy włączyć nasze nowe regulki tylko na chwile.
#  Pozwala to sprawdzić, czy po ich uzupełnieniu nadal
#  mamy dostęp do hosta, jeśli nie to automatycznie
#  odzyskamy go po 30 sekundach. Skrypt należy tylko
#  wywołać     z     opcja     "temp".
   if [ "$1" = "temp" ] ; then
(sleep 30; /sbin/iptables -P INPUT ACCEPT ;\
 /sbin/iptables -P OUTPUT ACCEPT ;\
 /sbin/iptables -P FORWARD ACCEPT ;\
 /sbin/iptables -F) & fi

echo -n "Instalacja reguł"

# Lądujemy moduł stateful-inspection dla FTP


/sbin/modprobe ip_conntrack_ftp


#     Czyścimy wszystkie tablice
iptables -F
iptables -F -t nat

#  Domyślnie nie przepuszczamy nic
   iptables -P INPUT DROP
   iptables -P FORWARD DROP
   iptables -P OUTPUT DROP

#  Interfejs lokalny ma specjalne prawa
   iptables -A INPUT -i lo -j ACCEPT
   iptables -A OUTPUT -o lo -j ACCEPT
   iptables -A FORWARD -o lo -j ACCEPT

#  Wpuszczamy wszystko z sieci lokalnej i wypuszczamy
#  wszystko na nią. Nie należy dodawać tutaj analogicznej
#  regulki dla FORWARD, to załatwi za nas moduł state
   iptables -A INPUT -i ethO -j ACCEPT
iptables -A OUTPUT -o ethO -j ACCEPT

#  Odrzucamy z komunikatem ICMP Port Unreachable połączenia
#  na IDENT oraz SOCKS (często sprawdzane przez serwery IRC)
   iptables -A INPUT -p tcp —dport 113 \
-j REJECT —reject-with icmp-port-unreachable
iptables -A INPUT -p tcp —dport 1080 \
-j REJECT —reject-with icmp-port-unreachable
```

```
#  Akceptujemy pakiety ICMP Echo (ping) wchodzące i wychodzące
#  Akceptacja odpowiedzi jest realizowana przez moduł state RELATED
   iptables -A INPUT -p icmp —icmp-type echo-request -j ACCEPT
   iptables -A FORWARD -p icmp —icmp-type echo-request -j ACCEPT

#  Zezwalamy na wszystko co odbywa się w ramach już dozwolonych
#  połączeń
iptables -A INPUT -p tcp -j ACCEPT -m state —state ESTABLISHED
iptables -A INPUT -p udp -j ACCEPT -m state —state ESTABLISHED
iptables -A INPUT -p icmp -j ACCEPT -m state —state ESTABLISHED
iptables -A INPUT -p icmp -j ACCEPT -m state —state RELATED
iptables -A FORWARD -p tcp -j ACCEPT -m state —state ESTABLISHED
iptables -A FORWARD -p tcp -j ACCEPT -m state —state RELATED iptables
-A FORWARD -p udp -j ACCEPT -m state —state ESTABLISHED iptables -A
FORWARD -p icmp -j ACCEPT -m state —state ESTABLISHED iptables -A
FORWARD -p icmp -j ACCEPT -m state —state RELATED iptables -A OUTPUT
-p tcp -j ACCEPT -m state —state ESTABLISHED iptables -A OUTPUT -p
tcp -j ACCEPT -m state —state RELATED  iptables -A OUTPUT -p udp -j
ACCEPT -m state —state ESTABLISHED iptables -A OUTPUT -p icmp -j
ACCEPT -m state —state ESTABLISHED iptables -A OUTPUT -p icmp -j
ACCEPT -m state —state RELATED

# Usługi TCP, które wypuszczamy z naszej sieci:
# 80,8080 (WWW), 22 (SSH), 21 (FTP), 25 (SMTP), 119 (news), 53 (DNS)
# 8888 (Napster), 2064 (distributed.net), 706 (SILC)
  TCP OUT ALLOW=80,8080,22,995,21,25,53,23,119,8888,2064,6667,706
# Usługi UDP: 123 (NTP), 53 (DNS)
  UDP_OUT_ALLOW=123,53

iptables -A OUTPUT -o pppO -p tcp -j ACCEPT -m state —state NEW \
-m multiport —destination-port $TCP_OUT_ALLOW
iptables -A OUTPUT -o pppO -p udp -j ACCEPT -m state —state NEW \
-m multiport —destination-port $UDP_OUT_ALLOW
iptables -A FORWARD -o pppO -p tcp -j ACCEPT -m state —state NEW \
-m multiport —destination-port $TCP OUT ALLOW
iptables -A FORWARD -o pppO -p udp -j ACCEPT -m state —state NEW \
-m multiport —destination-port $UDP_OUT_ALLOW

#  Przerzucamy port 6699 (Napster) z zewnętrznego interfejsu
#  na host w sieci lokalnej (10.1.1.3). Znane jako port
#  forwarding lub Port Address Translation
iptables -t nat -A PREROUTING -p tcp -d 251.61.252.110/32 —dport 6699 \ -j
DNAT —to-destination 10.1.1.3

# Maskarada (NAT) dla wszystkich hostow z sieci lokalnej
  iptables -t nat -A POSTROUTING -p all -s 10.1.1.0/24 -j MASO.UERADE

# Logujemy pakiety które nie zostały zaakceptowane przez
# żadna z powyższych regulek. Zostaną one wyblokowane dzięki
# polityce DROP we wszystkich tablicach
  iptables -A INPUT -j LOG -m limit —limit 10/hour
  iptables -A OUTPUT -j LOG -m limit —limit 10/hour
  iptables -A FORWARD -j LOG -m limit —limit 10/hour

echo .
```

Jak widać na podanych powyżej przykładach narzędzia udostępniane przez Linuxa służące filtrowaniu pakietów są niezwykle bogate w funkcje. Zatem stosowanie zapór ogniowych opartych na Linuksie jest bardzo dobrym rozwiązaniem zwłaszcza wtedy gdy zależy nam na zminimalizowaniu kosztów.

LITERATURA

[1] Mirosław Hajder, Heorhii Loutskii, Wiesław Stręciwilk „Informatyka – wirtualna podróż w świat systemów i sieci komputerowych" Wydawnictwo Wyższej Szkoły Informatyki i Zarządzania z siedzibą w Rzeszowie; Rzeszów 2002r.

[2] Mark Sportacka „Sieci komputerowe. Księga eksperta." Wydawnictwo Helion Gliwice 1999r.

[3] Vademecum teleinformatyka I, Wydawnictwo IDG 1999r.

[4] NetWorld listopad 2001 str. 52-58

[5] NetWorld marzec 2001 str. 50-55

[6] E.Schetina, K. Green, J. Carlson "Bezpieczeństwo w sieci" 10/2002

[7] M.Camou, J.Goerzen, A.van Couwenberghe „Debian Linux. Księga experta" 10/2001

[8] J.Chirilo „Hack wars. Na tropie hakerów. Administrator kontratakuje" tom.I 05/2002

[9] J.Chirilo „Hack wars. Administrator kontratakuje" tom.II 05/2002

[10] T.Rak „Suse Linux 7.2. Czarna księga administratora" 02/2002

[11] R.K. Burk, D.Horwath „UNIX – Internet. Księga experta" 06/1999

[12] S. Garfinkel, G.Spaffort „WWW - Bezpieczeństwo i handel" 09/1999

[13] A.Dudek „Nie tylko virusy. Haking, cracking, bezpieczeństwo internetu" 06/1998

[14] P.Krawczyk kravietz@aba.krakow.pl „Filtrowanie statefull – inspection w Linuksie i BSD

[15] P.Russel ipchains@rustcorp.com „Linux IPCHAINS howto"

[16] http://www.networld.pl/news

[17] http://www.networld.pl/artykuly

[18] C. Hunt „TCP/IP Administracja sieci"

[19] E.D.Zwicky,S. Cooper, D.B. Chapman "Internet Firewall, tworzenie zapór ogniowych" 2001