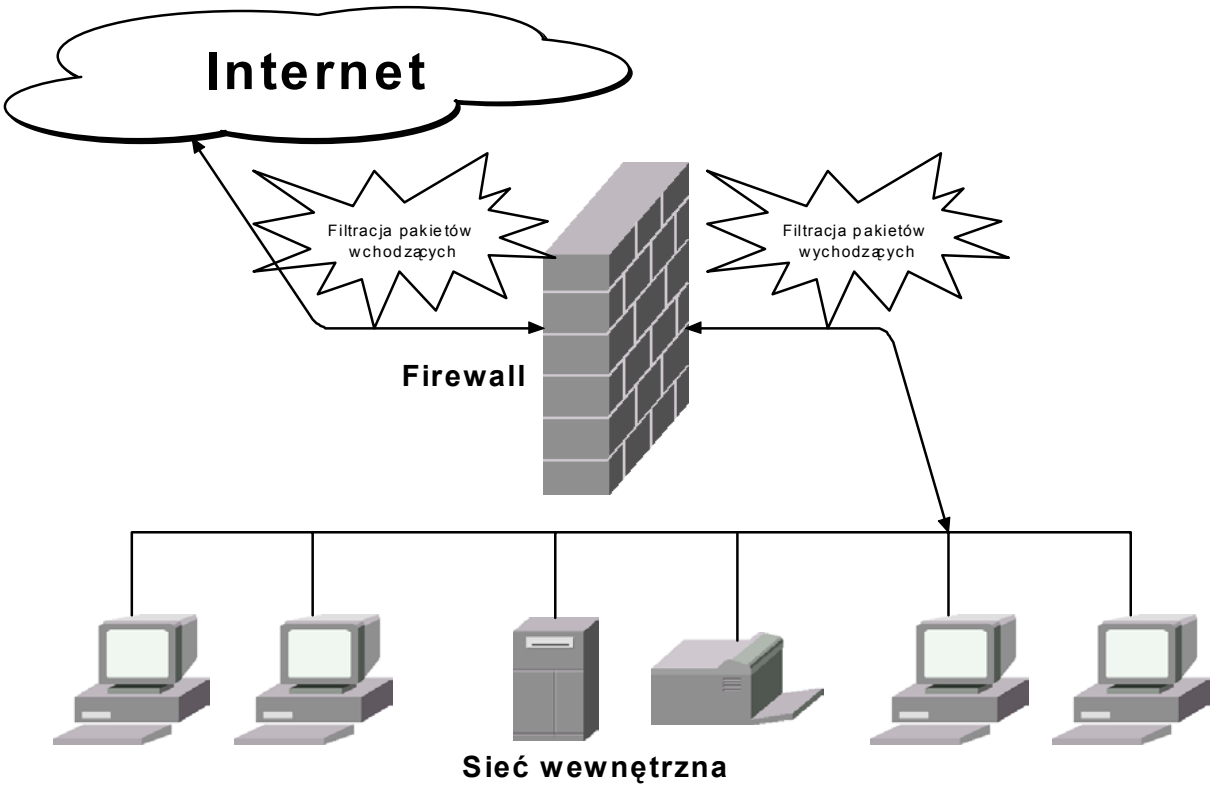
Firewall cz. I

Internet to dziś codzienność. Nazwa ta pojawia się niemal wszędzie, w reklamach, rozrywce, handlu, nauce. Dawno już przebrzmiały echa pierwszych zachwytów nad możliwościami tego superszybkiego i przy tym najtańszego medium przekazu informacji. Obecnie coraz częściej w różnych publikacjach pojawia się problem bezpieczeństwa. Ludzie i firmy zauważyły, że oprócz oczywistych korzyści Internet niesie szereg zagrożeń.
W poniższym tekście spróbuję przybliżyć sposoby zabezpieczania się przed nieautoryzowanym dostępem do naszych danych przez osoby trzecie.
Można by powiedzieć, że najprostszym i jednocześnie najskuteczniejszym zabezpieczeniem jest po porostu nie podłączać naszej sieci do Internetu. Owszem, jest to wyjście, ale nie satysfakcjonuje ono już dziś nikogo. Potrzeba uzyskania najbardziej aktualnych informacji sprawia, że coraz częściej ryzykujemy. Postaram się przedstawić sposób na zrównoważenie korzyści i niebezpieczeństwa - uczestniczenie w Internecie i jednoczesne zabezpieczenie się.
Pod groźnie brzmiącą angielską nazwą „firewall" kryje się właśnie urządzenie zabezpieczające.
Określenie to zostało zapożyczone z budownictwa, gdzie oznacza ścianę ogniotrwałą, zabezpieczającą przed przemieszczeniem się pożaru z jednej części budynku do drugiej. W informatyce funkcję pożaru przejęły różnego rodzaju zagrożenia, a firewall internetowy ma za zadanie zapobieganie ich przenikania z Internetu do sieci lokalnej.

Chociaż większość ludzi postrzega firewall jako zamknięta w jednym pudełku całość, tak naprawdę jest to zespół urządzeń sieciowych (hostów, routerów itp.) umiejscowionych w punkcie połączenia naszej sieci lokalnej z Internetem. Poniżej pokazany jest schematyczna zasada działania firewalla :



Co i przed czym próbujemy chronić ?

Uogólniając, firewall ma dwa podstawowe zadania : chronić i kontrolować. Za jego pomocą można zabezpieczać zgromadzone dane przed ciekawskimi, swoje zasoby sprzętowe przed wykorzystaniem ich przez nieautoryzowanych użytkowników, oraz swoją tożsamość sieciową (i nie tylko) przed zszarganiem jej przez podszywających się pod nas napastników, wykorzystujących nasze zasoby do dalszych „podbojów".

Istnieją różne rodzaje ataków, ze względu na to w jakim celu są przeprowadzane.
Pierwszy z nich to włamania, najczęstszy i jednocześnie najmniej szkodliwy rodzaj ataku. Większość napastników po prostu chce używać komputerów jakby byli ich użytkownikami. Ataki te często mają podłoże ambicjonalne czy też są przeprowadzane przez „kolekcjonerów" starających się włamać do jak największej liczby systemów.

Drugim, znacznie groźniejszym rodzajem ataku, jest blokada usług (*Denial of Service -DoS*). Polega on za zablokowaniu dostępu do danego hosta w sieci poprzez zasypanie go różnego rodzaju zgłoszeniami usług typu finger, echo, daytime czy też np. wysłaniem bardzo dużej ilości poczty elektronicznej. Metodę DoS wykorzystują m. inn. wszystkie „robaki internetowe" w takie jak I Love You, Romeo i Julia czy ostatnio Kurnikova, rozsyłające się w postaci poczty elektronicznej i zapychających w ten sposób sieć.

Trzecim, „komercyjnym" rodzajem ataku, jest kradzież informacji. Ataki tego typu najczęściej wykorzystują źle skonfigurowane usługi internetowe, zaprojektowane do podawania informacji, zmuszając je do wysłania większej ilości informacji niż zamierzono, lub udostępnienia ich niewłaściwym ludziom. Wiele z tych usług zostało zaprojektowanych do używania w sieciach lokalnych (jaskrawym przykładem takiej usługi jest współdzielenie plików w systemach Windows9x). Bardzo często w tego typu atakach wykorzystuje się oprogramowanie zwane *snifferami.* Pozwala ono na zainstalowanie elektronicznego podsłuchu i uzyskanie w ten sposób informacji o hasłach itp.

Teraz, gdy już wiemy co nam grozi, pora określić w jaki sposób zastosowanie firewalla zmniejszy to zagrożenie (piszę „zmniejszy" gdyż nie da się z pełną odpowiedzialnością powiedzieć że zagrożenia atakami można całkowicie wyeliminować).

W przypadku włamań i kradzieży informacji firewalle pomagają zapobiec nieautoryzowanemu dostępowi do systemu z zewnątrz. Pozwalają ściśle określić konta, do których jest możliwy dostęp spoza sieci lokalnej. Udostępniają też wiele mechanizmów rejestrowania (audytu), pozwalających szybko wykryć nieautoryzowane próby dostępu do systemu. Jednym z tego typu mechanizmów wykorzystywanych w firewallach jest pakiet darmowego oprogramowania z projektu Abacus firmy Psionic Software dostępny pod adresem
http://www.psionic.com/abacus

Dobrze skonfigurowany firewall potrafi nas również chociaż częściowo ochronić przed atakami typu DoS. Problem polega na tym, że aby zapewnić pełną ochronę przed tymi atakami należałoby wyłączyć usługi przeciwko którym są skierowane, a to z kolei stanowi przecież cel tych ataków.
Rola firewalla sprowadza się tu do dynamicznego blokowania routingu do atakujących hostów na podstawie zgłoszeń aplikacji monitorujących system. W najgorszym scenariuszu pozwoli to na zablokowanie tylko kilku zaatakowanych usług, bez blokowania całego hosta. Najczęściej jednak tego typu ataki są przeprowadzane z maszyn, na które się włamano. Prowadzi to niestety bardzo często do sytuacji : „orzeł, ja wygrywam, reszka, ty przegrywasz".
Stosując firewall możemy dodatkowo zablokować na nim przekazywanie pakietów zaadresowanych do „wrażliwych" portów komputerów z naszej sieci lokalnej (dotyczy to zwłaszcza tzw. "nukowania" komputerów z systemem Windows) ,co pozwoli na uniknięcie części zagrożeń.

Określamy strategię zabezpieczeń
Ostatnie dwadzieścia lat to silna ewolucja zarówno narzędzi zabezpieczających jak i technik włamań- mniej więcej tyle samo czasu poświęcono na próby włamań do systemów komputerowych co i na konstrukcję mechanizmów ochronnych.
Można pokusić się o stwierdzenie, że każda współczesna firma, niezależnie od jej wielkości, wykorzystuje Internet do celów marketingowo - komunikacyjnych. Związane jest to ściśle z problem polityki bezpieczeństwa.

Nawet najlepsze oprogramowanie czy sprzęt nie zabezpieczą naszych zasobów jeśli nie będzie przestrzeganych kilka podstawowych zasad przy ich wykorzystaniu.
Polityka bezpieczeństwa jest problemem bardzo ważnym ale jednocześnie bardzo subiektywnym. Każda firma ma inne wymagania i potrzeby w odniesieniu do pojęcia bezpieczeństwa. Związane jest to z wieloma kombinacjami sprzęt – oprogramowanie oraz z różnymi celami i skalą zabezpieczania się Właśnie dlatego polityka bezpieczeństwa będzie indywidualna dla każdej firmy i dlatego nie ma uniwersalnego "schematu zabezpieczeń" Profesjonalne zabezpieczenia są bardzo drogie, jednak straty mogą być znacznie większe. Często zastosowanie podstawowych zasad bezpieczeństwa wystarcza dla spełnienia założeń polityki bezpieczeństwa. Jeżeli mamy do czynienia z małą firmą, która wykorzystuje Internet do publikacji na swoim serwerze ogólnodostępnych materiałów marketingowych, oraz wysyła i odbiera pocztę elektroniczną o małym stopniu poufności to, dbając o wykonywanie kopii bezpieczeństwa oprogramowania serwera, oraz odcinając od sieci komputery zawierających "poufne" informacje uzyskamy wystarczający poziom zabezpieczeń.
W przypadku dużej firmy, przesyłającej za pomocą sieci publicznej duże ilości poufnych danych, prowadzącej handel przez internet oraz transferującej środki pieniężne, wymagane jest dobre przemyślenie kwestii bezpieczeństwa oraz zainwestowanie w sprzęt, oprogramowanie i, przede wszystkim, w ludzi, którzy będą potrafili sprawnie skomponować z tego system zabezpieczeń.
Najlepsza analogią będzie porównanie zabezpieczenia firmowej sieci komputerowej do zabezpieczeń pomieszczeń firmy. Biura są na ogół dobrze zabezpieczone przed włamaniami. Coraz bardziej wymyślne zamki, coraz częściej elektroniczne, reagujące na głos czy linie papilarne, sejfy które mogą wytrzymać bardzo wysokie temperatury, pancernych drzwi, systemy alarmowe monitorowane przez firmy ochroniarskie i policję oraz wielu innych mechanizmów przeszkadza intruzowi w naruszeniu naszego mienia. Jako nowoczesna firma, dostrzegająca korzyści płynące z prowadzenia działalności w Internecie, podłączamy się do sieci za pomocą stałego łącza. Nowe możliwości, nowe perspektywy. Firma kończy dzień - zamykamy wszystko na „cztery spusty”, aktywujemy alarm, strażnicy na dole siedzą przy monitorach i ..... I wszystko wygląda na porządnie zabezpieczone.. wszystko oprócz naszych komputerów.

Teraz skoncentrujemy się nad wykorzystaniem firewalla w polityce bezpieczeństwa firmy.
Cały ruch przechodzący z Internetu lub wychodzący z sieci wewnętrznej jest (a przynajmniej powinien być) przetwarzany przez firewall, możemy zatem zdecydować , co przepuszczamy a co zatrzymujemy (odfiltrowujemy).
Firewall jest logicznym separatorem, ogranicznikiem i analizatorem. Jak już wspomniałem, firewall to nie jedno, a zestaw urządzeń, kombinacja ruterów, hostów i sieci oraz odpowiedniego oprogramowania. Można go skonfigurować na wiele sposobów, zależnie od wybranej polityki bezpieczeństwa oraz dostępnych środków.

Oprócz oczywistych zalet firewall posiada niestety również dość znaczące wady.

Firewall można porównać do fosy otaczającej średniowieczny zamek - sieć wewnętrzną. Jedynym miejscem umożliwiającym dostęp jest most zwodzony, pozwalający ściśle kontrolować ruch w obie strony.
Kontrola ta wymaga jednak, aby każdy przychodzący lub wychodzący był dokładnie sprawdzany przez straże. Często więc będzie powodowała tworzenie się zatorów, zwłaszcza jeśli w danym momencie dużo ludzi będzie chciało wejść czy wyjść. Straż przy moście nie jest jednak nieomylna i czasami da się oszukać. Poza tym może kontrolować tylko wchodzących, nie mając wpływu na poczynania mieszkańców.

Podobnie będzie się rzecz miała z firewallem; kontrolować możemy tylko ruch przepuszczany przez niego (tak więc jeśli mamy w systemie jakąś boczną furtkę np. w postaci modemu, to cały nasz firewall jest psu na bude), nie mamy wpływu na poczynania naszych użytkowników wewnątrz systemu (a ich działalność bywa znacznie bardziej destrukcyjna niż skutki jakiegokolwiek włamania). Zawsze może się też zdarzyć, że jakaś nowa mocno zaawansowana technika ataku ominie nasze zabezpieczenia. Firewall nie jest w stanie nas ochronić przed wszystkimi możliwymi zagrożeniami, włączając w to także wirusy. Związane jest to z ograniczeniami przeglądania na firewallu zawartość pakietów. Z drugiej zaś strony konieczność kontrolowania każdej porcji danych spowoduje wolniejsze ich przetwarzanie i zmniejszenie wydajności łącza.

Jeśli po przeczytaniu powyższego akapitu uznałeś Czytelniku, że mimo wszystko jesteś w stanie znosić opisane niewygody uzyskując względne bezpieczeństwo jakie osiągamy stosując firewalla, zapraszam do praktycznej części tekstu dotyczącej budowy firewalla.

Przed rozpoczęciem instalacji pora odpowiedzieć sobie na podstawowe pytanie : kupujemy czy budujemy ? Dawniej każdy był zmuszony do samodzielnego skonstruowania firewalla. Obecnie na rynku są dostępne gotowe rozwiązania. Można je podzielić na tanie, programowe, jednostanowiskowe oraz systemy stanowiące połączenie sprzętu i oprogramowania, których ceny sięgają setek tysięcy dolarów.

Najczęściej chcielibyśmy, aby nasz firewall zabezpieczał całą sieć (zgodnie z rysunkiem pokazanym na początku). W zależności od stopnia złożoności i wielkości sieci możliwe są rożne kombinacje : od pojedynczego hosta zoptymalizowanego pod kątem filtracji pakietów, który w zupełności obsłuży większość sieci osiedlowych czy małe sieci firmowe do układu hostów i ruterów dynamicznie zarządzających przepływem pakietów. Wyznacznikiem rodzaju wybranego przez nas firewalla powinny być dwa czynniki : rzeczywiste potrzeby ochrony informacji wynikające z polityki bezpieczeństwa oraz zasobność kieszeni.

Nie bez znaczenia jest wybór systemu operacyjnego naszego firewalla (dotyczy hostów). Do niedawna UNIX był jedyną platformą, która zapewniała odpowiednią jakość i bezpieczeństwo usług filtrujących. Obecnie można stosować do tego celu Windows NT. Toczy się wiele sporów dotyczących wyższości jednego systemu nad drugim.
Prawda jak zwykle leży pomiędzy. Unixowcy (Linuxowcy) narzekają na Windows NT z uprzedzenia, poza tym „wychowani wśród pingwinów" mają skłonność do złego konfigurowania maszyn „okienkowych".
Z drugiej strony system Windows NT jest wbrew pozorom znacznie trudniejszy do poprawnej konfiguracji jako firewall z dwóch powodów.
Pierwszy to sposób implementacji standardów TCP/IP w obu rodzajach systemów. Unixowa implementacja została przez długie lata prób i błędów „doszlifowana" i pozbawiona większości usterek. Nie może się z nią pod tym względem równać wersja Microsoft'u, który TCP/IP w Windows NT implementował „od zera", popełniając błędy, o których w środowiskach uniksowych już dawno zapomniano.
Jest to podstawowy argument na korzyść rozwiązań na bazie Unixa (Linuxa)
Druga trudność z zabezpieczaniem Windows NT polega na całkowitej nieprzezroczystości systemu zaprojektowanego jako „czarna skrzynka". Upraszcza to instalację systemu, ale tylko w tych standardowych przypadkach. System Windows NT zawiera szereg „niepotrzebnych" protokołów i usług implementowanych „na sztywno" w standardowej instalacji, do których dostęp jest z reguły na poziomie rejestrów. Czyni to zabezpieczanie systemu zajęciem bardzo skomplikowanym. W zabezpieczeniach im coś mniej skomplikowane i bardziej konfigurowalne tym lepiej.

Dodatkowym argumentem za wybraniem na system operacyjny firewalla Linuxa jest cena. Licencja serwera Windows NT kosztuje spore pieniądze, podczas gdy dystrybucja Linuxa to najczęściej koszt wypalenia płyty CD-R czy kupna gazety komputerowej, która akurat umieściła wybraną dystrybucję na swoim krążku.

Budujemy ścianę ognia

Projektując nasz firewall nie zapominajmy o zasadzie dogłębnej obrony (*defense in deepth*) . Nie wolno nam ograniczyć się do jednego mechanizmu zabezpieczającego, jaki by nie był skuteczny. Należy raczej wykorzystywać kilka mechanizmów wzajemnie się wspomagających, a czasami nawet dublujących. Przykładem może tu być wielowarstwowe zabezpieczenie usługi *Secure Shell (ssh)* polegające na ograniczeniu dostępu do hosta za jej pomocą zarówno na poziomie filtrowania pakietów za pomocą *ipfwadm* czy *ipchains* oraz na stworzeniu listy adresów w pliku konfiguracyjnym *sshd_conf* z których możliwy jest dostęp.
Inny przykład : jeśli nie chcemy, aby użytkownicy wysyłali pocztę, nie tylko należy odfiltrować pakiety ale także usunąć programy pocztowe.
Taka redundancja zabezpieczeń pozwala, w przypadku uszkodzenia jednego z mechanizmów, na dalsze sprawne i bezpieczne funkcjonowanie systemu. Jeśli koszta takich „nadmiarowych" zabezpieczeń nie są zbyt wysokie, należy starać się je stosować.

Pamiętać należy także, iż cały łańcuch zabezpieczeń jest tak silny jak najsłabsze jego ogniwo. Oczywistym jest, że napastnicy zamiast próbować atakować od frontu nasz mur, będą starali się obejść go w poszukiwaniu tylniej furtki. Bardzo często zdarza się, że takie tylne wejście (*backdoor*) pozostawia sobie sam administrator, żeby np. mieć dostęp do systemu z modemu w wolne soboty.
Zawsze będzie istnieć najsłabszy punkt naszego systemu. Naszym zadaniem jest sprawić, aby był on na tyle silny, żeby wytrzymać większość ataków.

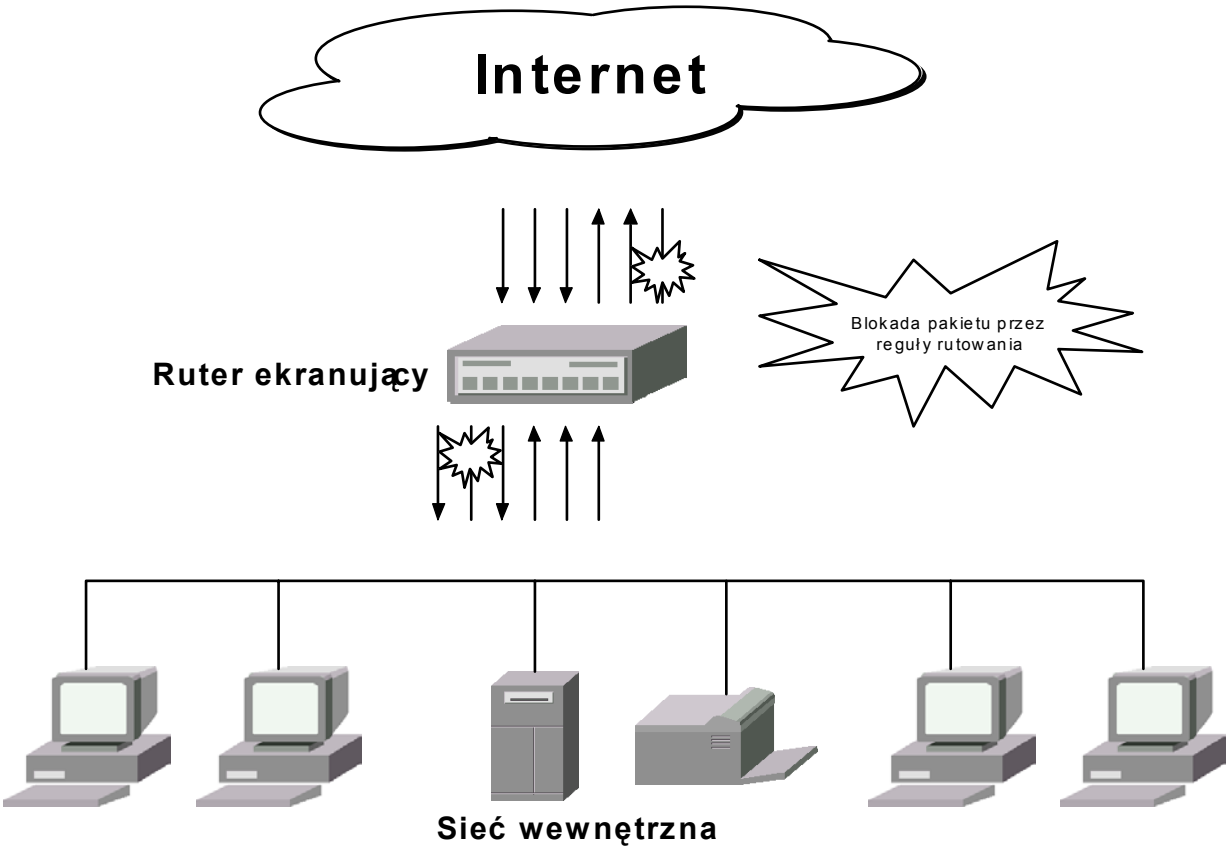
Bardzo ważna jest też zasada zabezpieczenia przez utajnienie. Jest to jedna z podstawowych zasad gwarantujących całkiem niezłe bezpieczeństwo, oczywiście dopóki nie zrobimy czegoś nierozsądnego w stylu np. ogłoszenia się na pl.comp.security jako właściciel systemu do którego nie można się włamać (przypadek skrajny, niemniej spotykany w przyrodzie).
Oczywiście zasada ta nie powinna funkcjonować jako jedyna filozofia zabezpieczeń w naszym systemie. Jej łączenie z innymi mechanizmami zabezpieczeń pozwoli na znaczne podniesienie poziomu bezpieczeństwa systemu.
W praktyce można stosować różne sztuczki maskujące istnienie naszego systemu w Internecie czy też uruchomionych na nim usług , np.:

- podłączanie się do Internetu okresowo, tylko na czas niezbędny do wykonania pracy
- uruchamianie serwerów usług (FTP, WWW, SSH) na innych niż standardowe portach
- prowadzenie „podwójnej administracji" polegającej na udostępnianie zgłoszeniom z zewnątrz innych danych o systemie niż tym z sieci wewnętrznej (doskonale się do tego nadają mechanizmy przerzucające routing zawarte w firewalu).

Szczególnym przypadkiem, często stosowanym przez zaawansowanych administratorów dużych sieci, jest postawienie hosta-pułapki, nafaszerowanego różnymi systemami logującymi. Jeśli system wykrywa próbę ataku to przekierowuje pakiety atakującego na host-pułapkę. Często minie dłuższy okres czasu, zanim włamywacz zorientuje się, że został wpuszczony w maliny. Oczywiście zabezpieczenie takie to wydatek na dodatkową maszynę (choć można też postawić taka pułapkę np. na hoście z dwiema kartami sieciowymi i dwoma interfejsami, co jest jednak jeszcze bardziej skomplikowane)

To na tyle jeśli chodzi o rozważania teoretyczne. Przejdźmy teraz do tego, co tygrysy lubią najbardziej, czyli do praktycznych realizacji złożonych systemów obronnych.

Pierwszy z nich będzie się opierał na wykorzystaniu routera filtrującego pakiety. Ruter taki nazywamy ruterem ekranującym (*screening router*). Ma on dostęp zarówno do danych z nagłówka IP (zawierającego adresy IP nadawcy i odbiorcy, rodzaj protokołu (TCP czy UDP lub ICMP), numery portów źródłowego i docelowego, typ komunikatu ICMP oraz wielkość pakietu), jak i do tych danych znajdujących się poza nagłówkiem. Pozwala to filtrowanie pakietów na podstawie bardziej szczegółowych informacji (np. nazwy strony www) oraz na weryfikację poprawności budowy pakietu (ważne przy atakach wykorzystujących fragmentację pakietów), oraz sprawdzenie poprawności portu docelowego. Ponadto router jest w stanie określić takie informacje jak adresy interfejsów sieciowych , zarówno tego z którego pakiet przybył jak i tego do którego podąża. Dodatkowo jest w stanie określić „historię" przepływu pakietów i podać takie informacje jak ilość pakietów wysłanych od i z danego hosta oraz ich powtarzalności i podobieństwa. Różnica miedzy zwykłym ruterem a ruterem ekranującym polega na tym, że zwykły router po porostu przekazuje pakiet wybierając dla niego najlepszą z dostępnych dróg natomiast router ekranujący sprawdza na podstawie zdefiniowanych reguł (w przypadku ruterów CISCO są to listy dostępu (*access-lists*)), czy dany pakiet może być przepuszczony.



System z ruterem ekranującym za zarówno zalety jak i wady.
Do jego zalet należy zaliczyć następujące fakty :

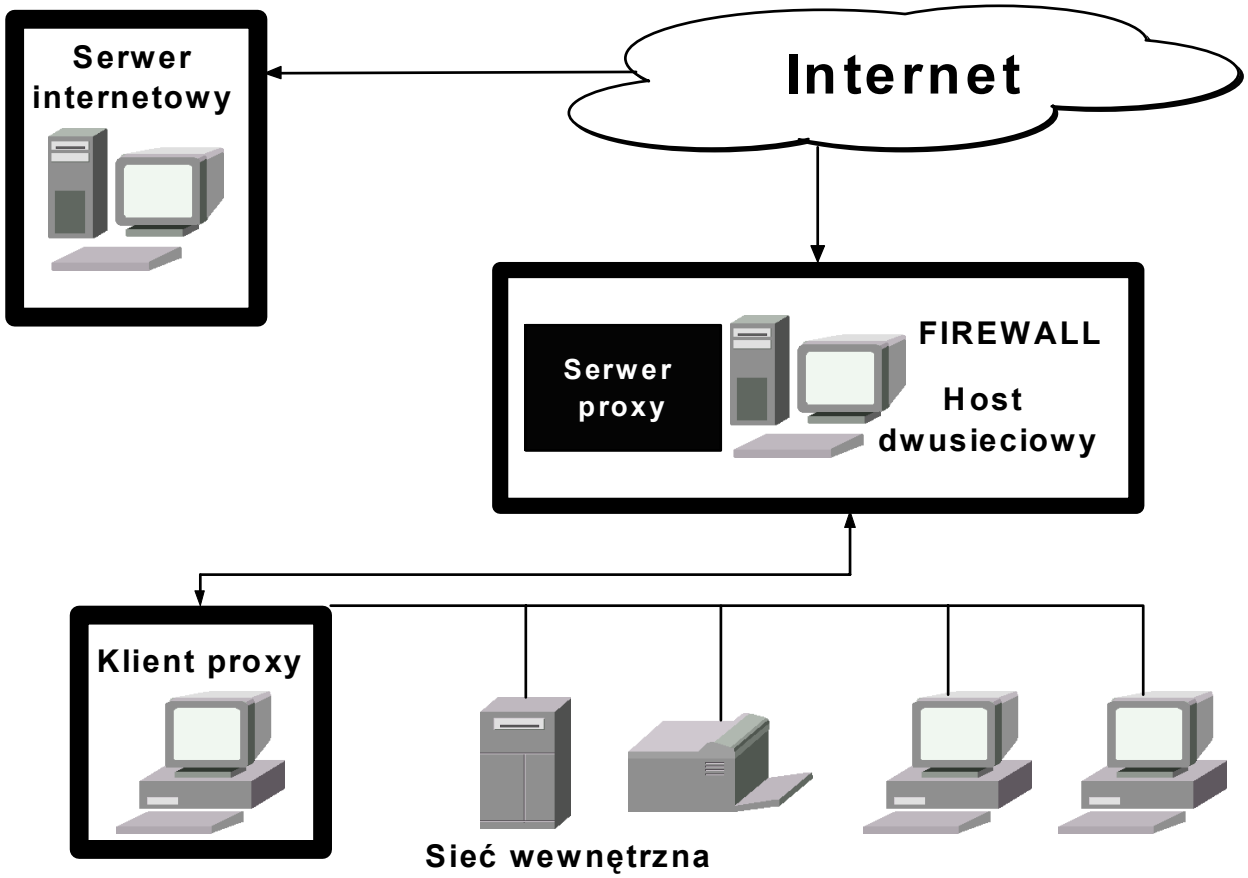
- jeden ruter może chronić całą sieć
- proste filtrowanie jest stosunkowo wydajne i w niewielkim stopniu obciąża ruter
- możemy w dość prosty sposób ustalić główne zasady filtrowania dla naszej sieci

Główne wady takiego rozwiązania to :

- dokładne reguły filtrowania są trudne do skonfigurowania, wymagając dużej wiedzy informatycznej oraz ... wysoce abstrakcyjnego myślenia
- reguły filtrowania są trudne do testowania
- nie da się dokładnie odfiltrować wszystkiego
- raz zdefiniowane reguły filtrowania są trudne w edycji (w przypadku CISCO najczęściej łatwiej jest usunąć całą listę dostępu, niż edytować istniejącą, zwłaszcza jeśli zawiera wiele pozycji, a my chcemy robić poprawki gdzieś w środku)
- im bardziej skomplikowane reguły filtrowania tym większe obciążenie routera i zmniejszenie wydajności sieci
- raz zapisane reguły filtrowania po kilku tygodniach są kompletnie nieczytelne nawet dla ich autora

Często stosuje się kombinacje routera ekranującego z innymi zabezpieczeniami, np. tzw. *proxy* czyli hostami pośredniczącymi.

Pośrednicy (*proxy*) to specjalne aplikacje lub serwery, stanowiące bufor pomiędzy użytkownikiem a serwerem internetowym. Jest to pojęcie dość szerokie W odniesieniu do firewalli będziemy tak nazywać host z dwoma interfejsami, jednym zewnętrznym a drugim wewnętrznym; lub też tzw. hosty bastionowe, będące dostępne zarówno z Internetu jak i z sieci lokalnej.
Główna idea takich usług została przedstawiona na poniższym rysunku.



Klient proxy to aplikacja: klient FTP, Telnetu czy przeglądarka www, która ma możliwość współpracy z serwerem proxy i de facto to z nim się komunikuje, zamiast bezpośrednio z docelowym hostem w Internecie. Serwer proxy ocenia żądania klientów i decyduje, które zaakceptować a które odrzucić. Jeśli żądanie zostaje zaakceptowane, serwer proxy łączy się z serwerem internetowym i przekazuje mu żądanie klienta. Następnie przekazuje odpowiedź serwera do klienta. W efekcie żadne dane nie płyną bezpośrednio z sieci Internet do sieci lokalnej bez wcześniejszego sprawdzenia.
Używając serwera proxy możemy również ustalić prawa poszczególnych użytkowników oraz zasady przepływu informacji z wybranych systemów.
Najpopularniejszy obecnie zestaw narzędzi do tworzenia systemów pośredniczących to SOCKS, który jako standard jest zawarty w większości aplikacji zarówno klientów jak i serwerów.

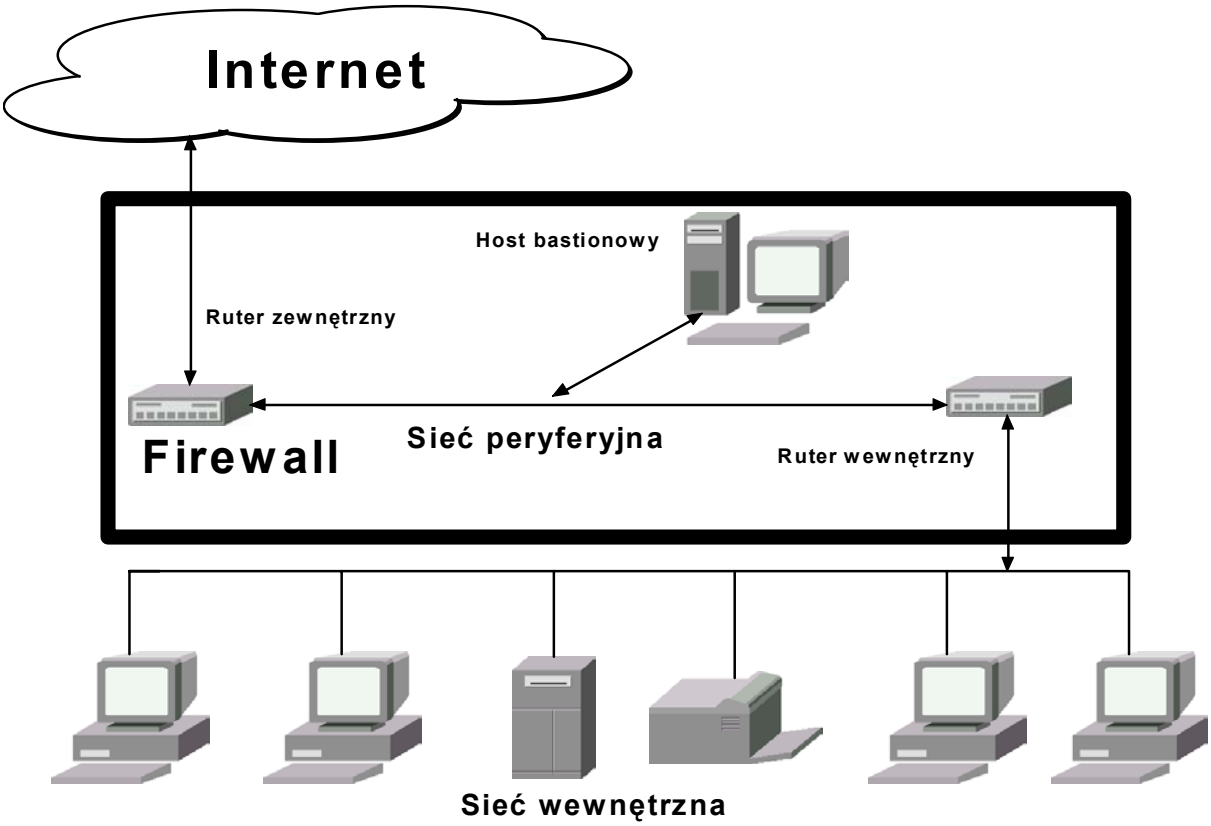
Zalety używania systemu pośredniczącego to :

- możliwość rejestracji zdarzeń (audyt)
- przyspieszenie obsługi poprzez buforowanie danych
- możliwość filtracji
- uwierzytelnianie na poziomie użytkownika
- konwersja IP pozwalająca zabezpieczyć się przed błędami w implementacji tego protokołu

Wadami natomiast są:

- nie przy wszystkich usługach istnieje możliwość pośredniczenia
- brak pełnej standaryzacji protokołów wymuszający instalację kilku serwerów dla jednej usługi
- konieczność przeszkolenia użytkowników w korzystaniu z systemu i ograniczenia przez to narzucane

Trzecie proponowane rozwiązanie stanowi swojego rodzaju połączenie powyższych dwóch, wykorzystujące zalety każdego z nich jednocześnie eliminując wady. Rozwiązanie to nosi nazwę architektury ekranowanej podsieci.
Schemat takiej konfiguracji firewalla jest przedstawiony na poniższym rysunku :



Przedstawiona powyżej konfiguracja jest najprostszą z możliwych w architekturze ekranowanej podsieci. Składa się z dwóch ruterów ekranujących podłączonych do sieci peryferyjnej. Jeden z nich jest umiejscowiony pomiędzy siecią peryferyjną i Internetem. Drugi jest umieszczony pomiędzy siecią peryferyjną i siecią lokalną. Aby przełamać tego typu obronę, napastnik musi przejść przez dwa rutery. Nawet jeśli uda mu się złamać zabezpieczenia hosta bastionowego (o jego roli potem), to nadal pozostaje mu do przebycia ruter wewnętrzny. Jest to w zasadzie konfiguracja nie posiadająca słabego miejsca, oczywiście jeśli dobrze skonfigurujemy filtrowanie na obu ruterach.

Zacznijmy od rutera zewnętrznego (*exterior router*), zwanego także ruterem dostępowym. Jego zadaniem jest ochrona sieci peryferyjnej, a pośrednio także sieci wewnętrznej. W praktyce jednak rutery zewnętrzne pozwalają wszystkim danym wydostać się na zewnątrz. W zasadzie nie musimy ustalać na nim żadnych reguł (byłyby to reguły zdublowane z rutera wewnętrznego)
Jeśli mamy dostęp do tego rutera (co nie zawsze jest możliwe, jeśli np.. jako ruter zewnętrzny traktujemy ruter dostępowy naszego providera), to jedynymi regułami do umieszczenia na nim są te chroniące maszyny w sieci peryferyjnej, hosty bastionowe i ruter wewnętrzny. Hosty w sieci peryferyjnej są chronione głównie przez własne zabezpieczenia, jednak, jak już wcześniej wspominałem, nadmiar zabezpieczeń nie zaszkodzi.
Należy zadbać o to, żeby na ruterze zewnętrznym znalazły się reguły blokujące pakiety wchodzące z Internetu ze sfałszowanym adresem źródłowym. Jest to jedyna funkcja, do której nie możemy wykorzystać rutera wewnętrznego, gdyż nie może on sprawdzić, czy pakiety podające jako swoje źródło sieć peryferyjną, nie są fałszywe.

Ruter zewnętrzny może także blokować pakiety wychodzące z sieci peryferyjnej z nieprawidłowym adresem źródłowym. Wszystkie pakiety wychodzące z naszej sieci powinny posiadać poprawny adres nadawcy. Jeśli tak nie jest, może to oznaczać próby włamania, albo poważne błędy w konfiguracji.
Wycinanie tego typu pakietów ma ta dobrą stronę, że uniemożliwia napastnikowi atakowanie innych systemów za pośrednictwem naszego.

Przejdźmy teraz do sieci peryferyjnej (*perimeter network*), zwanej też czasami strefą zdemilitaryzowaną (*DMZ*). Jest to idealne miejsce do umieszczenia w nim hostów z danymi, które mają być dostępne zarówno z sieci wewnętrznej jak i z Internetu. Hosty te powinny być zabezpieczone w technice ekranowanego hosta, przez własne systemy zabezpieczeń. Będziemy je nazywać hostami bastionowymi. Jednak nawet włamanie się na taki host nie pozwoli napastnikowi na podsłuchiwanie ruchu w sieci wewnętrznej, a jedynie danych wymienianych w sieci peryferyjnej, czyli o niskim stopniu poufności.
Głównym zadaniem sieci peryferyjnej jest oddzielenie ruchu pomiędzy hostami w sieci wewnętrznej od ruchu przeznaczonego do Internetu.

Pora zająć się wcześniej wspomnianym hostem bastionowym. Będzie to nasz pośrednik w kontaktach między połączeniami z zewnątrz a siecią lokalną. W sieci peryferyjnej może istniej jeden lub kilka takich hostów, zależnie od potrzeb. Możemy użyć hostów bastionowych do obsługi takich usług jak zewnętrzna poczta elektroniczna, publiczny ftp i www, DNS itp. Zgłoszenia wychodzące od klientów z sieci lokalnej możemy w tym momencie obsługiwać w dwojaki sposób :

- ustawić filtry pakietów na ruterach tak, aby pozwalały komputerom z sieci lokalnej na bezpośredni dostęp do serwerów internetowych (sposób wydajniejszy ale mniej bezpieczny)
- uruchomić na jednym lub kilku hostach bastionowych usługi pośredniczenia (*proxy servers*) i przepuszczanie przez nie zgłoszeń z sieci wewnętrznej. Jednocześnie należy zabronić bezpośredniego kontaktu pomiędzy siecią lokalną a Internetem poprzez odpowiednie reguły filtrowania na ruterach. Sposób ten jest znacznie bardziej bezpieczny, ale też konieczność pośredniczenia zmniejsza wydajność. Pamiętać też należy, że nie przy wszystkich usługach można pośredniczyć, co z kolei, aby zapewnić bezpieczeństwo, wymaga rezygnacji z tych usług. To zaś z kolei może obniżyć atrakcyjność sieci.

Dochodzimy do najbardziej newralgicznego punktu naszego firewalla jakim jest ruter wewnętrzny (interior router), zwany też ruterem dławiącym (*choke router*).
Jego rolą jest zabezpieczenie sieci wewnętrznej zarówno od strony Internetu jak i sieci peryferyjnej.
Ruter wewnętrzny filtruje większość pakietów. Pozwala to na wydzielenie na nim obsługiwanych zgłoszeń usług wychodzących z sieci wewnętrznej do Internetu. Są to usługi, które sieć wewnętrzna może bezpiecznie obsługiwać, bazując na filtrowaniu pakietów a nie na usługach pośredniczących. Lista usług na które pozwalamy bezpośrednio zależy od polityki bezpieczeństwa firmy. Można bezpiecznie obsługiwać w ten sposób wychodzący HTTP, FTP i inne. Im jednak więcej usług obsługujemy bezpośrednio, tym większe prawdopodobieństwo powstania gdzieś dziury w systemie.
Należy szczególnie pamiętać o obostrzeniach, jakie należy nałożyć za pośrednictwem rutera wewnętrznego na wymianę danych z hostem bastionowym. Powinno się do minimum zredukować ilość usług dozwolonych pomiędzy hostem bastionowym a siecią lokalną. Powód jest prosty : jeśli uda się włamanie na host bastionowy a my traktowaliśmy go jako host zaufany, napastnik ma wolną drogę, omijającą w efekcie filtry rutera wewnętrznego, do naszej sieci wewnętrznej.

Powyższe rozwiązanie jest skuteczne w większości przypadków. Rozwijać je można poprzez tworzenie dodatkowych, połączonych kaskadowo, sieci peryferyjnych o różnym stopniu zaufania, dotyczy to jednak naprawdę dużych sieci.
Rozwiązanie to najdroższe z prezentowanych. Jednak w przypadku firmy naprawdę warto zainwestować w dodatkowy sprzęt, uzyskując zabezpieczenie z prawdziwego zdarzenia.

Do zaprezentowanego rozwiązania sprzętowego należy dodać oprogramowanie do wykrywania i blokowania włamań. Doskonale się do tego nadaje wspominany już wcześniej projekt Abacus.

Podsumowując
Tak oto stosunkowo niewielkim kosztem udało nam się stworzyć profesjonalny system obrony. Oczywiście sama budowa firewalla to nie wszystko. Nawet najlepiej skonfigurowany firewall wymaga troskliwej i odpowiedzialnej opieki, konserwacji i unowocześniania. Jako że lepsze jest wrogiem dobrego, należy starać się utrzymywać wszystkie komponenty systemu w najnowszych stabilnych wersjach. Trzeba również na bieżąco śledzić wydarzenia w Internecie, bo być może pojawi się akurat nowe narzędzie które będziemy mogli dołożyć do naszego firewalla, lub wstawić w miejsce przestarzałego. Administrator firewalla nie może więc narzekać na

nudę. Poniżej przedstawiam listę pozycji książkowych z których korzystałem podczas pisania tego tekstu. Zawierają one wiele interesujących szczegółów, które na pewno okażą się pomocne podczas zarządzania zbudowanym przez nas firewallem.

Literatura

1. E.Zwicky, S. Cooper, D. Chapman „Internet Firewalls" Wydawnictwo ReadMe Warszawa 2001
2. Craig Hunt „TCP/IP – Administracja sieci - Wydanie drugie" Wydawnictwo ReadMe Warszawa 1998
3. Scott M. Ballew „Zarządzanie sieciami IP za pomocą routerów CISCO" Wydawnictwo ReadMe Warszawa 1998
4. A.Leinwand, B. Pinsky, M. Culpeper „Konfiguracja routerów CISCO cz. I i II" Wydawnictwo ReadMe Warszawa 2000
5. Douglas E. Comer „Sieci komputerowe i intersieci" Wydawnictwo Naukowo Techniczne Warszawa 1999
6. Adam Wolisz „Podstawy lokalnych sieci komputerowych tom II" Wydawnictwo Naukowo Techniczne Warszawa 1992
7. „CISCO User's Manual" CISCO Systems Inc.

Michał Zimnicki
PUH KOMKAS s.c.
www.komkas.com.pl