ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1998
Seria: INFORMATYKA z. 34 Nr kol. 1381

Piotr KLUCZWAJD, Jarosław ULCZOK, Robert WÓJCICKI
Politechnika Śląska, Instytut Informatyki

MECHANIZMY OCHRONY SIECI KOMPUTEROWYCH NA PRZYKŁADZIE OPROGRAMOWANIA SOLSTICE FIREWALL-1

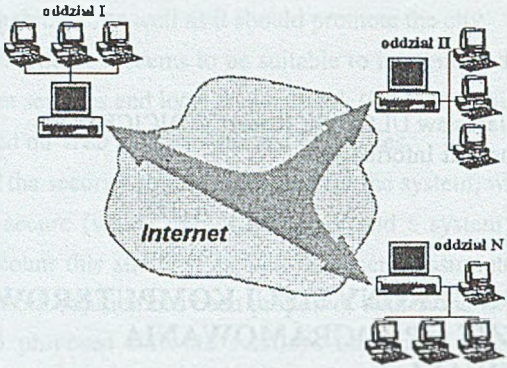
Streszczenie. Artukuł prezentuje elementy bezpieczeństwa rozległych, heterogenicznych sieci komputerowych. Stanowi próbę prezentacji metod i narzędzi ich ochrony na przykładzie oprogramowania firmy SunSoft - Solstice Firewall-1.

THE MECHANISMS OF NETWORK SECURITY BASED ON SOLSTICE FIREWALL-1

Summary. This article describes elements of security in heterogeneous, wide area networks. It presents methods and tools of protecting private networks based on Solstice Firewall-1 software.

1. Wstęp

Utrzymanie wysokiego poziomu bezpieczeństwa rozległych, heterogenicznych sieci komputerowych staje się bardzo skomplikowanym zadaniem z uwagi na złożoność technologiczną i dynamiczny rozwój tego środowiska. Duża część współczesnych sieci korporacyjnych funkcjonuje na zasadzie lokalnych sieci prywatnych (Intranet), połączonych ze sobą za pośrednictwem sieci publicznej (rys. 1). W przeświadczeniu wielu osób największym zagrożeniem dla sieci prywatnej jest sieć publiczna (np. Internet). W praktyce okazuje się, iż dużo większe zagrożenie stanowią użytkownicy lokalni, posiadający legalny dostęp do wyznaczonych zasobów systemu, którzy z pewnych względów dokonują przejęcia lub modyfikacji strategicznych informacji.



Rys. 1. Struktura sieci korporacyjnej funkcjonującej na zasadzie grupy lokalnych sieci prywatnych, połączonych ze sobą za pośrednictwem sieci publicznej
Fig. 1. Structure of corporate network functioning as a group of private, local networks connected using WAN

W systemie ochrony sieci lokalnej możemy wyróżnić cztery zasadnicze, ściśle powiązane ze sobą elementy:

- warstwa ochrony sieci komputerowych („firewall" - kontrola dostępu do sieci);
- warstwa ochrony danych przesyłanych w sieci publicznej - szyfrowanie przesyłanych informacji;
- warstwa ochrony serwerów sieciowych (kontrola dostępu do serwera);
- warstwa ochrony danych i aplikacji (kontrola dostępu do poszczególnych danych i aplikacji oraz szyfrowanie przesyłanych i przechowywanych informacji).

Jak do tej pory nie ma i prawdopodobnie jeszcze długo nie będzie jednego, uniwersalnego produktu, który sprostałby zadaniu pełnej ochrony rozległej sieci korporacyjnej. Najczęściej konieczne staje się łączenie oprogramowania wielu różnych producentów, co w dużym stopniu komplikuje proces administrowania i nadzorowania pracy systemu.

2. Elementy bezpieczeństwa sieciowego

Powszechny rozwój wszelkiego rodzaju sieci, w tym i sieci Internet, spowodował powstanie mody na zabezpieczanie systemów, moda ta jest bardziej nakazem chwili niż pozbawionym podstaw wymysłem.

Najbardziej oczywistym sposobem ochrony naszych zasobów jest po prostu ochrona fizyczna wrażliwych elementów naszego systemu komputerowego, takich jak np. pomieszczenie, w którym pracuje serwer, czy stacja robocza administratora sieci. Ponieważ

sieć i dostęp do danych sterowany jest właśnie z takich miejsc, ich zabezpieczenie jest kluczowe dla bezpieczeństwa. Nawet ogromne pieniądze wydane na zabezpieczenia nie przyniosą żadnych rezultatów, jeżeli nieuprawniony personel będzie miał swobodny (lub w miarę swobodny) dostęp do urządzeń typu konsola operatora.

Następny poziom zabezpieczeń to bezpieczeństwo systemu operacyjnego. Ustalono w tym zakresie pewne standardy, wypracowane przez Departament Ochrony USA (oraz inne organizacje). Powstały pojęcia poziomów bezpieczeństwa systemów operacyjnych oraz sposoby certyfikacji tych systemów (przetestowane i zatwierdzone), poczynając od całkowitego braku wiarygodności systemu (poziom D1), aż po najwyższy poziom bezpieczeństwa, gdzie cała konfiguracja sprzętowo-programowa wymaga matematycznej weryfikacji, a zarówno sprzęt, jak i oprogramowanie musi podlegać specjalnej ochronie w trakcie transportu zapewniającej jego nienaruszalność (aby nikt niczego nie podmienił) – *poziom A1*.

W tym miejscu należy zwrócić uwagę na problem wzrostu obciążenia systemu operacyjnego związanego z uaktywnieniem opcji bezpieczeństwa. W szczególności może się okazać, że mało wydajne serwery nie będą w stanie obsłużyć wszystkich użytkowników po uruchomieniu wszystkich programów zabezpieczających, ze względu na duże zużycie zasobów CPU i powierzchni dyskowej.

Najpopularniejszym sposobem identyfikacji i potwierdzania użytkownika w systemie komputerowym jest system haseł. Ogólnie metoda ta pozwala stwierdzić, że użytkownik wydaje się być tym, za kogo się podaje. O ile w przypadku systemów wielodostępnych, bazujących na klasycznych terminalach znakowych (łącza szeregowe), systemy haseł są stosunkowo bezpieczne, o tyle w środowisku sieciowym są one bardzo proste do złamania. Do najczęstszych metod należy podsłuchiwanie połączenia sieciowego w celu uzyskania kombinacji identyfikator-hasło (przykładem jest połączenie telnetem, gdzie hasło transmitowane jest otwartym tekstem). Inną metodą pozyskania hasła jest umieszczanie w systemie konia trojańskiego „udającego" np. program *login*. Jednak najczęstszym sposobem złamania hasła jest tzw. Dictionary Attack – polega on na próbkowaniu programu autoryzującego całym słownikiem danych.

Istnieją oczywiście techniki pozwalające pracować z hasłami w sposób bardziej bezpieczny. Do najpopularniejszych z nich należą:

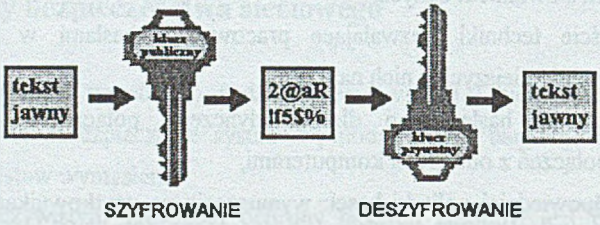
- stosowanie ważności hasła tylko dla pojedynczego połączenia - w przypadku sporadycznych połączeń z odległymi komputerami,
- zastosowanie odpowiedniej polityki haseł: wymuszenie na użytkownikach ich okresowej zmiany, stosowania znaków specjalnych, itp.,

- system jednokrotnych haseł – uwalnia użytkownika od pamiętania haseł chroniących do przeróżnych zasobów, z których musi korzystać.

Szyfrowanie zapewnia poufność i prywatność zarówno w odniesieniu do plików utrzymywanych na serwerze jak też danych przesyłanych poprzez sieć. Aktualnie mamy do czynienia z dwoma podstawowymi grupami systemów (algorytmów) szyfrujących.

Pierwsza z nich i jednocześnie najbardziej popularna to algorytmy poufnego klucza, często określana także jako algorytmy symetryczne lub algorytmy klucza prywatnego. W tej metodzie ten sam klucz używany jest zarówno do szyfrowania danych, jak i do ich rozkodowania. Ponieważ do obu czynności używany jest ten sam klucz, musi on być utrzymywany w „wielkim" sekrecie. Zaletą tej metody jest stosunkowo niski nakład obliczeń ponoszonych na szyfrowanie i rozkodowanie nawet dużych plików. Wadą jest konieczność dostarczenia klucza wszystkim zainteresowanym, co może doprowadzić do jego przechwycenia w przypadku przesyłania poprzez sieć publiczną. Najbardziej znanymi algorytmami klucza poufnego są: RC4, DES, IDEA, Skipjack.

Druga grupa algorytmów szyfrujących oparta jest na tzw. metodzie klucza publicznego, znanej także jako algorytmy klucza publiczno-prywatnego lub klucza asymetrycznego. W przeciwieństwie do metody klucza poufnego komunikujące się ze sobą strony używają dwu różnych kluczy - jednego do zaszyfrowania przesyłki, drugiego do jej rozkodowania. Nazwa „klucz publiczny" wzięła się stąd, że algorytmy te bazują na generowaniu klucza przez każdą ze stron i ich wymianie za pośrednictwem sieci publicznej bez utraty prywatności, bowiem klucz publiczny staje się użyteczny jedynie w przypadku posiadania sekretnego, znanego tylko lokalnie, klucza prywatnego (rys. 2). Algorytmy tego typu gwarantują nam prywatność, ale nie gwarantują autentyczności, co może doprowadzić do różnego typu ataków znanych jako „Man in the Middle" (człowiek w środku). Z tych to powodów algorytmy klucza publicznego są bardzo często stosowane wspólnie z tzw. podpisami cyfrowymi, pozwalającymi upewnić się co do wiarygodności źródła pochodzenia. Najbardziej znanymi algorytmami klucza publicznego są: RSA, El Gamal.



Rys. 2. Koncepcja szyfrowania danych w systemie klucza publicznego
Fig. 2. Concept of encryption using a public key

Obliczenie wartości klucza prywatnego (o odpowiedniej długości) przy znajomości klucza publicznego należy do bardzo skomplikowanych zadań matematycznych typu znajdowanie rozkładu dużych liczb naturalnych na czynniki pierwsze, które przy obecnym stanie wiedzy i technologii jest uznawane za praktycznie niewykonalne.

Jedną z metod próby globalnego zabezpieczenia transmisji w sieciach bazujących na protokole TCP/IP jest tzw. IP Security lub IP Sec, która de facto jest zbiorem protokołów opracowanych przez IETF (Internet Enginnering Task Force), a udokumentowanym w RFC 1825-1829. Standard ten gwarantuje autentyczność, prywatność i integralność danych działając na poziomie jądra IP. Niewątpliwą zaletą takiego rozwiązania jest zatem jego skuteczność w odniesieniu do każdej aplikacji sieciowej, niezależnie od tego, czy jest to poczta elektroniczna czy telnet. IP Sec zdefiniowano dla IPv4 (aktualnie stosowanego systemu adresowania IP), ale włączono go jako standardową własność do IPv6. Wdrożenie IP Sec polega na używaniu dwu opcjonalnych nagłówków IP:

- AH - Authentication Header, dedykowany do stwierdzania autentyczności i integralności danych,
- ESP - Encapsulating Security Payload zapewniający prywatność (szyfrowanie).

Specyfikacja IP Sec umożliwia komunikującym się stronom uzgodnienie odnośnych parametrów (mechanizm identyfikacji, algorytm szyfrowania, klucz, czas ważności połączenia, etc.), na bazie odpowiedniego pola w nagłówkach IP, tzw. SPI (Security Parameter Index). Dzięki temu istnieje możliwość ominięcia wszelkich restrykcji eksportowych USA, bowiem zamiast standardowego szyfrowania DES można uzgodnić np. 40-bitowy RC4. Jedynym nie ustalonym parametrem IP Sec jest sposób dystrybucji kluczy. Aktualna propozycja wskazuje na tzw. ISA Key Management Protocol (ISAKMP, Oalkey), ale na obecnym etapie używane są „ręczne" sposoby wymieniania kluczy. Jak dotąd jedynym komercyjnym pakietem posiadającym wdrożenie IP Sec i IPv6 jest OnNet32 for Windows z FTP Software.

Stwierdzanie autentyczności (ang. authentication) polega na upewnieniu się, że obiekt jest właśnie tym, za kogo (za co) się podaje. W dużych sieciach proces ten ma niebagatelne znaczenie. Przykładem mogą tu być fałszywe listy. Otrzymujemy przesyłkę, której nadawcą może być zupełnie inna osoba, niż wskazuje na to adres „From:"

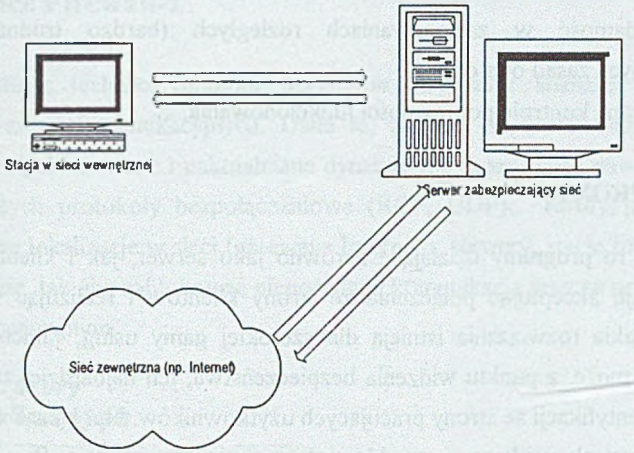
Podpisy cyfrowe - będące blokiem danych umieszczonych na końcu przesyłki - tworzone są na ogół na bazie techniki szyfrowania w systemie klucza publicznego, a wiarygodność klucza publicznego utwierdzana jest w procesie certyfikacji. Wydawaniem certyfikatów mogą się zajmować niezależne organizacje, takie jak Versign, dedykowane serwery (Certificate Authority) lub grupy takich serwerów połączone w strukturę hierarchiczną (Security Key Infrastructure). Podpis cyfrowy może powstać w wyniku zaszyfrowania zawartości przesyłki

kluczem prywatnym nadawcy, dzięki czemu odbiorca rozszyfrowując podpis cyfrowy kluczem publicznym nadawcy i porównując go z zawartością przesyłki, może określić autentyczność i integralność otrzymanych informacji.

Autoryzacja (ang. authorization) polega na sprawdzaniu, czy obiekt (użytkownik, aplikacja), który żąda dostępu do określonego zasobu systemu, jest do tego upoważniony. Realizowane jest to przez system operacyjny lub dedykowane oprogramowanie. Jednym z dobrze znanych systemów autoryzacji jest Kerberos. Używa on specjalnej metody kontroli uprawnień (użytkownik otrzymuje bilety na poszczególne usługi systemu od specjalnego serwera) i korzysta z algorytmu szyfrującego DES w trakcie transmitowania poprzez sieć wrażliwych informacji takich jak hasła. Podejrzenie sesji telnet obsługiwanej przez Kerberos nie umożliwia zatem przechwycenia hasła wprost. Dodatkowo, Kerberos definiuje przedział czasowy aktywności połączenia, po upłynięciu którego użytkownik musi ponownie poddać się procesowi autoryzacji, co stanowi zabezpieczenie przed intruzami próbującymi zareplikować przechwyconą sesję.

3. Techniki zabezpieczeń

Systemy „ścian ognia" (ang. „firewall") to swego rodzaju zapory, mające stanowić przeszkodę przed wtargnięciem z sieci rozległych nieuprawnionych osób do zasobów naszej sieci lokalnej. Historycznie systemy „firewall" powstały w celu bronienia się przed atakami z Internetu, ale coraz częściej stosowane są do obrony przed atakami z wewnątrz sieci. Dobrym przykładem jest bronienie działu księgowości przed nieautoryzowanymi pracownikami. Ze względu na swoją kluczową rolę „ściany ognia" instalowane są na ogół na pomostach pomiędzy sieciami LAN i WAN, bądź w systemach współpracujących z routerami stanowiącymi te pomosty. „Firewall" może być programem, sprzętem wyposażonym w „zaszyte" w układach elektronicznych oprogramowanie, jak również rozwiązaniem sprzętowo-programowym. Mimo ciągłych działań skierowanych przeciwko systemom „firewall" należą one do najbardziej skutecznych rozwiązań problemu bezpieczeństwa sieci. Należy jednak zaznaczyć, że „ściany ognia" wymagają bardzo solidnej i przemyślanej konfiguracji, która jest w zgodzie z założoną polityką bezpieczeństwa.



Rys. 3. Ogólna zasada funkcjonowania systemów zabezpieczeń sieci komputerowej
Fig. 3. Securing Network

Wszystkie dane kierowane do i z sieci wewnętrznej, przechodząc przez urządzenie chroniące sieć (komputer z oprogramowaniem lub np. router z zaimplementowanymi metodami ochrony), zostają poddane kontroli pod kątem zgodności ze zdefiniowanymi dla potrzeb przedsiębiorstwa założeniami *polityki bezpieczeństwa.* W zależności od warstwy, w której funkcjonują takie systemy, możemy wyróżnić:

- filtry pakietów,
- serwery proxy,
- rozwiązania integrujące zalety obu powyższych rozwiązań.

3.1. Filtry pakietów

Działają w warstwie sieciowej, egzaminując każdy wchodzący do i wychodzący z systemu pakiet, porównują informację zawartą w nagłówku pakietu z aktualnymi zasadami i albo akceptują i przekazują go dalej, albo odrzucają. Zasady funkcjonowania oparte są na początkowym i docelowym adresie IP, ewentualnie numerach portów (inteligentne routery IP). Takie rozwiązania pomimo niewątpliwych zalet:

- łatwości w implementacji,
- stosunkowo prostej konfiguracji dla niewielkich zastosowań,
- dużej elastyczności

nie są kwalifikowane jako system typu „firewall" i rzadko wykorzystywane jako zabezpieczenia skomplikowanych sieci korporacyjnych ze względu na:

- niedostateczny stopień zabezpieczeń (kontrola zbyt małej ilości elementów),
- małą przydatność w zastosowaniach rozległych (bardzo trudna weryfikacja zdefiniowanych zasad ochrony),
- skomplikowaną kontrolę poprawności funkcjonowania.

3.2. Serwery PROXY

Serwery Proxy to programy działające zarówno jako serwer, jak i klient. Funkcjonują w warstwie aplikacji, akceptując połączenia ze strony klientów i realizując w ich imieniu żądane zlecenie. Takie rozwiązania istnieją dla szerokiej gamy usług, takich jak X, FTP, TELNET, itp. Być może, z punktu widzenia bezpieczeństwa, ich najbardziej znaczącą zaletą jest wymaganie autentyfikacji ze strony pracujących użytkowników. Np. łącząc się z chronioną siecią z Internetu, użytkownik musi zwykle połączyć się z serwerem *Proxy*, poddać się weryfikacji, a następnie dopiero sfinalizować połączenie z docelowych hostem w chronionej sieci. Do wad serwerów *Proxy* można zaliczyć:

- ograniczoną liczba obsługiwanych aplikacji,
- bariery technologiczne w przypadku konieczności ewolucji,
- obniżenie wydajności systemu,
- duże obciążenia systemu operacyjnego i aplikacji,
- brak elastyczności.

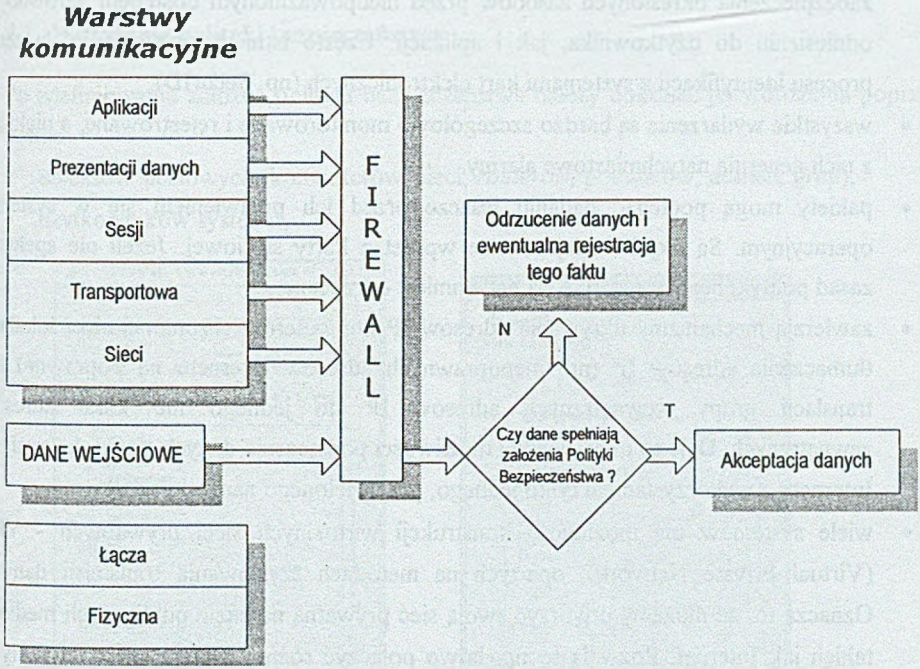
3.3. Technika SMLI (Statefull Multi-Layer Packet Filtering)

Aby efektywnie uzyskać rzeczywisty poziom bezpieczeństwa, nie jest wystarczające jedynie filtrowanie pakietów. *Firewall* musi śledzić i kontrolować przepływ komunikacji przez niego w jak najszerszym zakresie. Aby podjąć decyzję dotyczącą przekazania, odrzucenia, zaszyfrowania czy też zarejestrowania zdarzenia związanego z usługą TCP/IP, *Firewall* musi uzyskać, składować i poddawać obróbce informacje z wszystkich warstw komunikacyjnych, w tym również dotyczących pracy zewnętrznych aplikacji.

Przykładem aplikacji, która wykorzystuje opisaną powyżej technikę, a nazywaną *SMLI*, jest oprogramowanie *Firewall-1* firmy CheckPoint, która jest niewątpliwym liderem tego rynku (46% udziału, kolejny konkurent – to tylko 7% udział w rynku).

4. Solstice Firewall-1

Wykorzystując technikę *Statefull Inspection Firewall-1* analizuje dane uzyskane ze wszystkich warstw komunikacyjnych. Dane te, zależne od stanu bieżącego połączenia i „kontekstu", są składowane i uaktualniane dynamicznie, pozwalając nawet na śledzenie sesji wykorzystujących protokoły bezpołączeniowe (RCP, UDP). Każdy pakiet przechodzący przez kluczowe lokalizacje w sieci (gatewaye Internetu, serwery, stacje robocze, routery, itp.) podlega analizie, tak aby zablokować niepożądaną komunikację jeszcze przed pojawianiem się w systemie operacyjnym.



Rys. 4. Zasada funkcjonowania systemu Firewall-1
Fig. 4. Firewall-1 system

Jeśli dane wejściowe nie spełniają założeń, wówczas fakt ten podlega rejestracji, aby w połączeniu z narzędziami służącymi do ich analizy wspomagać pracę administratora.

Istotną zaletą takiego mechanizmu ochrony jest całkowita „przezroczystość" dla użytkownika i aplikacji.

Kolejną zaletą tej techniki jest to, ze wprowadzenie tak rozwiniętych mechanizmów ochrony nie pociąga za sobą zbyt dużego, dodatkowego obciążenia serwera (ok 3%), co pozwala na wykorzystanie takich rozwiązań nawet w sieciach o przepustowości do 100Mbps. Dla porównania, serwery typu *Proxy* zapewniają zadowalającą wydajność dla sieci 10Mbps.

Systemy firewall chronią naszą sieć na kilku poziomach, a także umożliwiają wdrożenie zupełnie nowych własności:

- użytkownicy wewnętrzni mogą mieć dostęp do wszystkich (lub wybranych) usług Internet, natomiast użytkownicy zewnętrzni nie będą mieli dostępu do jakiegokolwiek zasobu naszej sieci lokalnej.
- usługi takie jak e-mail, ftp, WWW mogą być dozwolone dla ruchu zewnętrznego tylko w odniesieniu do specyficznego komputera. Daje to nam otwartość na świat, jednocześnie chroniąc i ukrywając inne zasoby sieciowe.
- zaawansowane systemy identyfikacji i kontroli tożsamości są skuteczną metodą zabezpieczenia określonych zasobów przed nieupoważnionym dostępem zarówno w odniesieniu do użytkownika, jak i aplikacji. Często istnieje możliwość połączenia procesu identyfikacji z systemami kart elektronicznych (np. SecurID).
- wszystkie wydarzenia są bardzo szczegółowo monitorowane i rejestrowane, a niektóre z nich generują natychmiastowe alarmy.
- pakiety mogą podlegać badaniu jeszcze przed ich pojawieniem się w systemie operacyjnym. Są niejako zdejmowane wprost z karty sieciowej. Jeżeli nie spełniają zasad polityki bezpieczeństwa, są natychmiast odrzucane.
- zawierają mechanizmy ukrywania adresów IP komputerów chronionej sieci lokalnej, tłumaczenia adresów IP (np. niepoprawnych adresów Internetu na poprawne) lub translacji grupy wewnętrznych adresów IP do jednego lub kilku adresów zewnętrznych. Daje to m.in. wielkie możliwości podłączenia dużych sieci lokalnych do Internetu z wykorzystaniem tylko jednego, przydzielonego nam adresu IP.
- wiele systemów ma możliwość konstrukcji wirtualnych sieci prywatnych - VPN (Virtual Private Network), opartych na metodach szyfrowania transmisji danych. Oznacza to, że możemy utworzyć swoją sieć prywatną na bazie publicznych mediów, takich jak Internet. Pozwala to np. łatwo połączyć różne, odległe oddziały firmy w jedną bezpieczną sieć. Niekiedy istnieje możliwość kodowania tylko niektórych typów usług (jak np. telnet), pozostawiając inne w normalnej postaci, co pozwala utrzymać efektywność całego systemu.

4.1. Składniki systemu Solstice Firewall-1

W systemie Sostice Firewall wyróżnione zostały 4 funkcjonalnie różne komponenty:

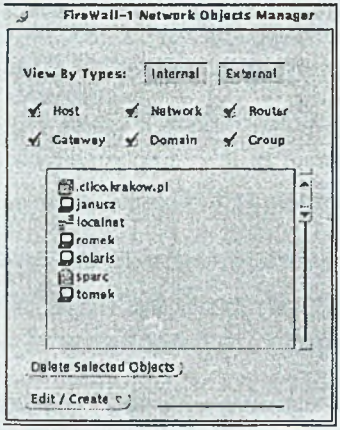
- Management Component - poprzez graficzny interfejs administrator zarządza repozytorium zasad bezpieczeństwa, obiektami sieciowymi, usługami sieciowymi, użytkownikami, itp.

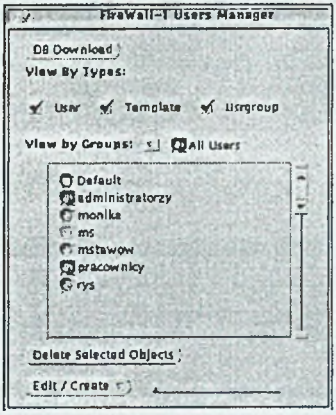
- Inspection Module
  - nadzoruje przestrzeganie polityki bezpieczeństwa,
  - obejmuje procesy snmpd, fwd,
  - jest wbudowany w jądro systemu operacyjnego,
  - jest usytuowany pomiędzy OSI Data Link i Network Layers.
- Router Module - poprzez graficzny interfejs administrator zarządza wbudowaną w router listą kontrolną oraz określa całokształt polityki bezpieczeństwa routera.
- Encryption Component - pozwala na prowadzenie w pełni poufnej komunikacji na bazie sieci publicznej (np. Internet).

4.2. Wdrażanie polityki bezpieczeństwa

Po zdefiniowaniu założeń polityki bezpieczeństwa należy dokonać jej wdrożenia poprzez określenie:

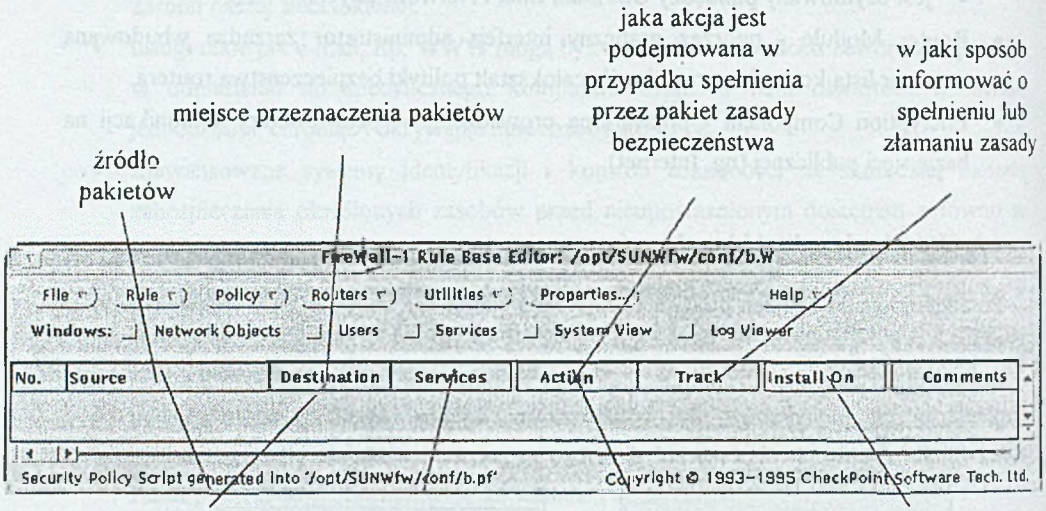
- obiektów sieciowych (komputerów, sieci, *routerów,* pomostów, domen, grup),
- użytkowników systemu,





- dodatkowych usług sieciowych (standardowo obsługiwanych jest ponad 150 usług sieciowych) - architektura ***Firewall-1*** umożliwia łatwe wdrażanie dowolnych rozszerzeń w kierunku nowej aplikacji, usługi lub protokołu,

- definicji zasad bezpieczeństwa - Solstice Firewall-1 stosuje bardzo prosty, ale skuteczny warunek początkowy: wszystko, co nie jest jednoznacznie dozwolone, jest zabronione! Oznacza to, że po zainstalowaniu Firewall-1 otrzymujemy ścianę ognia nie do sforsowania zarówno w odniesieniu do ruchu wewnętrznego, jak i zewnętrznego.



- weryfikacji i instalacji zasad bezpieczeństwa.

4.3. Translacja IP-adresów (ang. NAT)

W produktach tej klasy spotykać można dodatkowe zabezpieczenia sieci komputerowej w postaci szyfrowania połączeń między serwerem i klientem oraz translację adresów, tak aby ukryć strukturę wewnętrzną chronionej sieci. Wykorzystując tę ostatnią technikę, można doprowadzić do sytuacji (ale jedynie dla połączeń inicjowanych z wnętrza sieci), kiedy „ukrywamy" całą sieć, tak że z zewnątrz „widoczny" i dostępny jest jedynie jeden komputer – *Firewall*, z jednym IP-adresem. FW-1 pozwala zdefiniować do 20 różnych zasad translacji adresów IP odnoszących się do wybranych adresów i interfejsów sieciowych według czterech dostępnych trybów:

- ukrywanie lokalnych adresów (mapowanie wielu do jednego),
- tłumaczenie błędnych adresów na legalne adresy Internetu,

- rozszerzenie za "małych" klas adresowych,
- statyczna (jeden-na-jeden) translacja bloków adresowych o dowolnej wielkości dla wychodzących i wchodzących połączeń.

4.4. User Level Security

Przeźroczysta kontrola tożsamości użytkowników dla telnet, ftp, itp. Możliwe jest wykorzystanie:

- karty mikroprocesorowej SecurID,
- haseł jednokrotnego użytku S/Key,
- haseł UNIX,
- wewnętrznych haseł Firewall-1,
- RADIUS, AssureNet Pathways.

4.5. Client Level Security

Ochrona dostępu do aplikacji z wykorzystaniem analogicznych do *User Level Security* metod zabezpieczeń. Przykład: użytkownik uruchamia telnet do portu autoryzacyjnego (259). Po zalogowaniu Firewall-1 gwarantuje dostęp do zdefiniowanych przez administratora serwisów na określony okres czasu i z limitowaną liczbą połączeń.

4.6. Autoryzacja HTTP (Authenticated HTTP Proxy)

Wykorzystanie konfigurowalnych poziomów bezpieczeństwa i długości czasu autoryzacji umożliwia restrykcyjny dostęp do wybranych adresów URL, a przede wszystkim ochronę dowolnej liczby wewnętrznych serwerów WWW.

4.7. Skanowanie danych

Wprowadzenie mechanizmu skanowania danych pozwala na nadzorowanie (skanowanie) przesyłów odbywających się z użyciem protokołów FTP, WWW, SMTP, obsługę diagnostyki antywirusowej plików przesyłanych poprzez FTP, a co najważniejsze kontrolę apletów JAVA, ActiveX, na działanie których przeciętny użytkownik nie ma znaczącego wpływu, podnosząc poziom bezpieczeństwa danych przechowywanych lokalnie i zdalnie.

4.8. Serwer SMTP

Zabezpieczenie systemu komputerowego od strony usługi SMTP obejmuje:

- ukrywanie rzeczywistych adresów e-mail użytkowników wysyłających pocztę na zewnątrz sieci prywatnej,
- zmianę adresata (chronienie kluczowych kont),
- selekcję nadchodzących listów,
- blokowanie załączników,
- odrzucanie listów przekraczających wyznaczony rozmiar,
- sprawdzanie nadawcy (np.odrzucanie *reklam*).

4.9. Wirtualne sieci prywatne VPN (*Virtual Private Network*)

Oddzielnym zagadnieniem od dotychczas zaprezentowanych jest zapewnienie poufności informacji przesyłanej w sieciach publiczych, jak np. Internet. Zastosowanie mechanizmów szyfrowania/deszyfrowania pakietów IP (danych), elastyczna wymiana kluczy, bezpieczne algorytmy i metody szyfrowania (RSA, schemat *Diffie-Hellman*-a, SKIP, FWZ1, DES), selektywny wybór szyfrowanego ruchu IP (usługi, protokoły, etc.) oraz duża wydajność pozwalają na budowę sieci, w skład której wchodzą geograficznie rozproszone stacje robocze, serwery, itp. Ponadto w skład pakietu wchodzi moduł *SecuRemote Client* rozszerzający ideę VPN na odległe (przenośne) stacje robocze wyposażone w system Windows 95, dając możliwość połączenia z siecią korporacyjną z "ruchomego" punktu tak bezpiecznie jak z wnętrza własnej sieci, gwarantowane szyfrowanym dostępem do chronionych danych firmy bez potrzeby instalacji Firewall-1.

5. Podsumowanie

Większość przestępstw komputerowych (zwłaszcza tych najbardziej spektakularnych) związanych z włamaniami do systemów komputerowych nie jest raportowana – trochę ze wstydu, trochę z obawy przed utratą wiarygodności i prestiżu. Statystyki są alarmujące – w latach 1985-1993 liczba przypadków naruszania prywatnej własności za pośrednictwem publicznie dostępnych sieci lub połączeń wzrosło o 260%. Według Computer Security Institute z 9832 ataków w 1993 r. 7860 zakończyło się sukcesem, z tego tylko 19 zostało oficjalnie zgłoszonych, zaś roczne straty wynikłe z przestępstw komputerowych w USA osiągają wartość 550 mln dolarów.

Co zatem możemy stracić? W gruncie rzeczy zależy, kim lub czym jesteśmy. Jeżeli wysyłamy jedynie kilka listów na miesiąc, to zapewne nie mamy się czym przejmować. *Ale co się stanie, jeśli nasza działalność oparta jest na poczcie elektronicznej i serwerze WWW?*

LITERATURA

[1] SunSoft - wydawnictwo własne. Solstice. How to Develop a Network Security Policy. An Overwiev of Internetworking Site Security, 1996.

[2] Holbrook J.P., Reynolds J.K.: RFC-1244. The Site Security Handbook, 1991.

[3] Craig Hunt. TCP/IP – Administracja sieci. 1991 (oryginał). ISBN 83-7147-024-X.

[4] James V.: FTP Software – wydawnictwo własne. FTP Software and Intranet Security. What the IT Managers Needs to Know, 1996.

Recenzent: Dr inż. Ryszard Winiarczyk

Wpłynęło do Redakcji 23 grudnia 1997 r.

Abstract

This article describes elements of security in heterogeneous, wide area networks.

First chapter is an introduction to the security problems. Its remarked that most of corporate networks works as local area network (Intranet) connected via public network (Fig.1).

Chapter two is an overview of present basic elements of security methods, such as: user name/password checking, coding with public and private keys, IP Security, electronic signs.

Next chapter describes methods to protect LAN from outside network attack. Packet filters, proxy servers and SMLI are briefly described.

In chapter four, Solstice Firewall-1 is described. The architecture of the system (Fig. 4) and some rules of introducing security are presented. The possible security services are briefly described.

The last chapter is a summary.