

Budujemy „firewall”

Każdego dnia przybywa około 20 000 nowych komputerów podłączonych do sieci Internet. Ta największa publiczna sieć komputerowa przyciąga coraz szersze rzesze użytkowników, oferując im bogate zbiory informacyjne, grupy dyskusyjne, wymianę poczty elektronicznej, gry sieciowe, ... a nawet możliwości prowadzenia rozmów „on line”. Opierając się na danych statystycznych sporządzonych przez Network Wizards (<http://www.nw.com>) można przypuszczać, iż przed zakończeniem naszego stulecia Internet obejmie swoim zasięgiem ponad 50 milionów komputerów. Wraz ze wzrostem liczby użytkowników Internetu rośnie ryzyko utraty prywatności lokalnych sieci komputerowych. Najbardziej skutecznym sposobem zniwelowania potencjalnych zagrożeń bezpieczeństwa, wynikających z podłączenia do sieci publicznej, jest fizyczne odseparowanie wszystkich komputerów wspomagających realizację istotnych zadań organizacji i przechowujących jej strategiczne informacje. W praktyce, oznacza to kompleksową przebudowę fizycznej infrastruktury systemu informatycznego, co w dużej większości przypadków pociąga za sobą poważne wydatki finansowe. Rozwiązaniem tego problemu jest zastosowanie oprogramowania określanego mianem „ściana ognia” (ang. *firewall*), dedykowanego do ochrony systemu lokalnego przed ingerencją zewnętrzną. Określenie „ściana ognia”, jak do tej pory, nie przyjęło się w polskiej terminologii informatycznej i w związku z tym pozostaniemy przy oryginalnej nazwie tego oprogramowania (**firewall**).

Zagrożenia.

Przed przystąpieniem do omówienia zagadnień ochrony sieci prywatnej, należało by ogólnie naświetlić jakie niebezpieczeństwa wynikają z faktu połączenia z siecią publiczną - aby zbudować skuteczny system zabezpieczeń trzeba wiedzieć przed czym się bronić. Zasadniczo, oprogramowanie „firewall” nie zapewnia ochrony systemu przed użytkownikami lokalnymi, można więc ograniczyć rozważania do zagadnienia zagrożeń zewnętrznych, zakładając optymistycznie, że wszystkie osoby posiadające lokalny dostęp do systemu są upoważnione do wykonywanych przez nie operacji. Nie znaczy to jednak, że nie mamy możliwości zbudowania systemu wewnętrznych zabezpieczeń. Wiele produktów nadaje się doskonale i do tego celu poszerzając spektrum zastosowań na sieci Intranet.

Najpowszechniej praktykowaną metodą uzyskiwania dostępu do odległego systemu jest wykonywanie zdalnego logowania **Telnet** (ang. *Network Terminal Protocol*), 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 Telnet 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 („hackera”).

Przechwytywanie hasła może odbywać się za pośrednictwem ukrytego w systemie programu, który odbiera wpisywane przez użytkownika dane (np. fałszywy program *login*) lub poprzez prowadzenie „**nasłuchiwanie sieci**” (ang. *sniffing*) wykonywanego w trakcie zdalnego logowania legalnego użytkownika. „Sniffing” odbywa się za pośrednictwem urządzeń podsłuchowych, podłączonych do sieci na drodze transmisji danych. W najprostszym przypadku może to być zmodyfikowana karta sieciowa umożliwiająca selektywne przechwytywanie pakietów.

„**Sniffing**” to bardzo poważny problem, który nie ogranicza się wyłącznie do przechwytywania hasła - w przypadku prowadzenia nieszyfrowanej transmisji danych „nasłuchiwanie sieci” może prowadzić do całkowitej utraty poufności przesyłanych informacji. Niestety, na dzień dzisiejszy nie ma skutecznych narzędzi przeciwdziałania tej technice - dostępne programy monitorujące pracę sieci komputerowej nie gwarantują wykrycia dobrze zamaskowanego urządzenia podsłuchowego. Nawet zastosowanie łącza światłowodowego nie zapewnia pełnej tajności transmitowanych informacji (więcej informacji można uzyskać w Internecie pod adresem: <http://www.cert.org>).

W momencie pozyskania pliku zawierającego zaszyfrowane hasła użytkowników (w UNIX */etc/passwd* , */etc/shadow*), mogą zostać podjęte próby uzyskania ich jawnej postaci. Najczęściej stosowaną techniką jest tzw. „**atak brutalny**” (ang. *brute force attack*), sprowadzający się do szyfrowania i porównywania wszystkich słów zawartych w przygotowanym do tego celu słowniku.

Potencjalne zagrożenie stanowią wszystkie usługi pozwalające na prowadzenie zdalnej pracy pomiędzy tzw. „zaprzyjaźnionymi” komputerami: **RLOGIN**, **RSH** i **RCP**. Poprzez podstawienie odpowiednio przygotowanych plików konfiguracyjnych *.rhosts* i *hosts.equiv*, osoby nieupoważnione mogą uzyskać uprawnienia legalnego użytkownika systemu. (Pierwszym krokiem administratora powinno być zablokowanie tych aplikacji lub instalacja **SSH (Secure Shell)**, jeżeli stosowanie ich okaże się konieczne.)

Pewne niebezpieczeństwo stanowi usługa transferu plików **FTP (File Transfer Protocol)**. Wykorzystując niewłaściwie administrowany serwer FTP, użytkownik Internetu może wejść w posiadanie ważnych informacji, przechowywanych w systemie plików komputera. Bardzo groźnym zjawiskiem jest wykorzystanie FTP do rozprowadzania tzw. „**złośliwych programów**” (ang. *malicious programs*).

W gronie tych aplikacji możemy wyróżnić:

- „**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 (czasu procesora, pamięci operacyjnej, przestrzeni dyskowej) i doprowadzenia do upadku systemu;
- „**koń trojański**” (ang. *trojan horse*) - program, który udaje pracę innego legalnego programu, a w międzyczasie wykonuje szereg niepożądanych czynności (np. fałszywy program *login* kradnie hasło użytkownika);

- „**bomba czasowa**” (ang. *time bomb*), „**bomba logiczna**” (ang. *logic bomb*) - fragment programu podejmujący działanie tylko w określonym czasie (np. dzień urodzin autora programu) lub w momencie spełnienia ustalonych warunków;
- „**robak**” (ang. *worm*) - program, który powiela samego siebie, wykonuje ustalone czynności (najczęściej niekorzystne dla systemu) i próbuje przenieść się do innego komputera w sieci.

Z uwagi na właściwość samoprzenaszalności, „robak” wydaje się być najbardziej niebezpiecznym członkiem powyżej wymienionej grupy programów. Pierwszy atak „robaka” zarejestrowano w 1988 roku. Program napisany przez Roberta Morrisa przenosił się z komputera na komputer poprzez wykorzystywanie słabych punktów aplikacji SENDMAIL, FINGERD i RHOST.

Inną kategorią zagrożeń są tzw. „**furtki**” (ang. *backdoors*) lub „**włazy**” (ang. *trapdoors*), które stanowią nieudokumentowane wejścia do legalnych programów. Niekiedy, programiści tworzą alternatywne wejście do aplikacji aby ułatwić sobie proces testowania. „Furtką” do programu może być ciąg znaków lub nawet wciśnięcie odpowiedniej kombinacji klawiszy. W momencie odnalezienia „furtki” nieuprawniony użytkownik uzyskuje kontrolę na aplikacją.

Omawiając niebezpieczeństwa związane z wykorzystaniem Internetu nie należy zapominać o dwóch najbardziej popularnych usługach - serwisie wymiany poczty elektronicznej SMTP (*Simple Mail Transfer Protocol*) i serwisie informacyjnym WWW (*World Wide Web*). Najślabszą stroną systemu poczty elektronicznej Internetu okazał się program *sendmail* - w ostatnich latach odnotowano przypadki wykorzystania niedostatecznych zabezpieczeń tego programu do oszukiwania serwera SMTP, który poprzez błędną interpretację nadchodzących przesyłek, traktował je jako programy wykonywalne. Próby rozszerzenia możliwości WWW (np. interfejs CGI, nowe elementy HTML), spowodowały powiększenie pola działania „hackerów”. Administratorzy serwerów WWW często decydują się na korzystanie ze sprowadzonych z Internetu skryptów CGI (*Common Gateway Interface*). Uruchamianie nieznanymi aplikacjami nieuchronnie wiąże się z podejmowaniem ryzyka, uzyskania odmiennego niż zakładano, rzeczywistego rezultatu działania programu. Ostatnie rozszerzenia języka opisu dokumentów hipertekstowych HTML (*HiperText Markup Language*), zmierzają w kierunku wprowadzenia do WWW elementów bezpośredniej interakcji z użytkownikiem. Bez wątplenia najbardziej eleganckim rozwiązaniem jest wzbogacanie stron HTML o aplikacje napisane w języku **Java**. Warto jednak pamiętać, iż Java jest bardzo „młodym” językiem programowania, a zastosowany system bezpieczeństwa może okazać się nie w pełni skuteczny. Informacje na temat ryzyka wynikającego z uruchamiania sprowadzanych z Internetu programów Java można znaleźć pod adresem: <http://www.cs.princeton.edu>.

Chyba najgłośniejszą obecnie techniką oszukiwania zabezpieczeń systemów (w tym systemów chronionych przez niektóre „firewall”) jest „**spoofing**”. Określenie „spoofing” wywodzi się z dziedziny wojskowej i oznacza *przeciwdziałanie elektronicznym przeciwsystemom nieprzyjaciela poprzez nadawanie fałszywych informacji*. W odniesieniu do zagadnienia transmisji danych w sieci TCP/IP, „**IP Source-Address Spoofing**” oznacza proces przesyłania pakietów zawierających nieprawdziwy adres źródłowy (ang. *source address*), przez co komputer odbierający te pakiety błędnie identyfikuje ich nadawcę. Pierwszy poważny atak przeprowadzony z wykorzystaniem tej techniki został odnotowany 22 stycznia 1995 roku w USA.

Zakres przedstawionych powyżej potencjalnych zagrożeń, jakie należy uwzględnić podczas budowy polityki bezpieczeństwa, został świadomie ograniczony tylko do tych zagadnień, którym można przeciwdziałać poprzez „firewall”. Nie ma potrzeby rozważać niebezpieczeństwa przechwytywania zainicjowanych połączeń sieciowych (ang. *connection hijacking*) czy rejestracji fal elektromagnetycznych, emitowanych przez drukarki, monitory komputerów czy przewody instalacji

sieciowej, skoro „firewall” w niczym tu nie pomoże. Należy także pamiętać, iż wymienione zagrożenia obejmują tylko to, co do tej pory zostało wykryte i ujawnione publicznie. Administrator systemu zobowiązany jest na bieżąco zapoznawać się z informacjami dotyczącymi zagadnień bezpieczeństwa i ochrony.

Budowa polityki bezpieczeństwa sieci prywatnej.

Instalacja oprogramowania „firewall” powinna być poprzedzona staranną analizą potrzeb organizacji w zakresie wykorzystania sieci Internet. Należy dokładnie sprecyzować z jakich usług będą korzystać pracownicy organizacji (użytkownicy lokalni), a jakie usługi będą świadczone na rzecz użytkowników zewnętrznych - w ostatnich latach coraz więcej organizacji decyduje 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 punktów 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 sprostą 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.

Opierając się na badaniach laboratoryjnych przeprowadzonych przez *National Software Testing Laboratories* i *Data Communications* (wyniki testów są ogólnie dostępne w sieci Internet pod adresem: http://www.data.com/Lab_Tests/Firewalls.html), można wyłonić pewne wyróżniające się rozwiązania:

- ◆ **Borderware Firewall Server** firmy *Border Network Technologies*;
- ◆ **Firewall-1** firmy *Checkpoint Software Technologies* lub popularna wersja OEM z *SunSoft*
- ◆ **Digital Firewall for Unix** firmy *DEC*;
- ◆ **Cyberguard** firmy *Harris Computer Systems Corporation*.

Najwyższe wyniki testów, spośród wyżej wymienionych produktów, uzyskał **Firewall-1**. Dzięki zastosowaniu algorytmów selektywnej filtracji pakietów, **Firewall-1** bardzo nieznacznie obniża efektywność funkcjonowania całego systemu.

Zestaw potencjalnych możliwości Firewall-1 obejmuje:

- ◆ **filtrację pakietów** (przeciwdziałanie „spoofing”, ...);
- ◆ **aplikacje pośredniczące** (ang. *application proxy*) (prowadzenie identyfikacji, kontroli tożsamości, kontroli uprawnień, ...);
- ◆ **translację adresów internetowych** (ukrywanie wewnętrznych adresów IP, ...);
- ◆ **szyfrowanie i uwierzytelnianie** (tworzenie wirtualnych sieci prywatnych (ang. *virtual private network*)).

Firewall-1 jako jedno z nielicznych rozwiązań prowadzi bieżące monitorowanie stanu wszystkich otwartych sesji komunikacji sieciowej, niezależnie od tego czy transmisja danych prowadzona jest w oparciu o komunikację połączeniową (TCP) czy bezpołączeniową (UDP). Dużą zaletą tego oprogramowania jest także przejrzysty interfejs graficzny użytkownika, który w znacznym stopniu usprawnia proces wdrażania i nadzorowania realizacji przyjętej strategii ochrony.

Wdrożenie polityki bezpieczeństwa

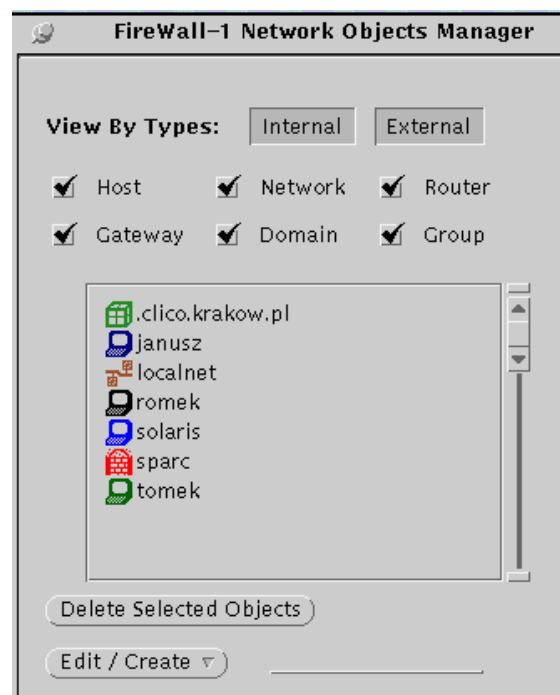
Dysponując zatwierdzonym projektem systemu ochrony można przystąpić do fazy wdrożenia polityki bezpieczeństwa, która sprowadza się do zainstalowania i konfiguracji oprogramowania „firewall”, odpowiedzialnego za egzekwowanie przyjętych ograniczeń. Proces wdrożenia polityki bezpieczeństwa obejmuje następujące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

- I. Definicja obiektów sieciowych.
- II. Definicja użytkowników systemu.
- III. Specyfikacja dodatkowych usług sieciowych. (jeżeli jest taka potrzeba)
- IV. Ustalenie zasad bezpieczeństwa.
- V. Weryfikacja i instalacja.

Pewne wybrane elementy tego procesu zostaną zaprezentowane na przykładzie wspomnianego już wcześniej oprogramowania **Firewall-1** firmy **Checkpoint Software Technologies** (znany w Polsce przede wszystkim w wersji **OEM SunSoft - Solstice Firewall-1**).

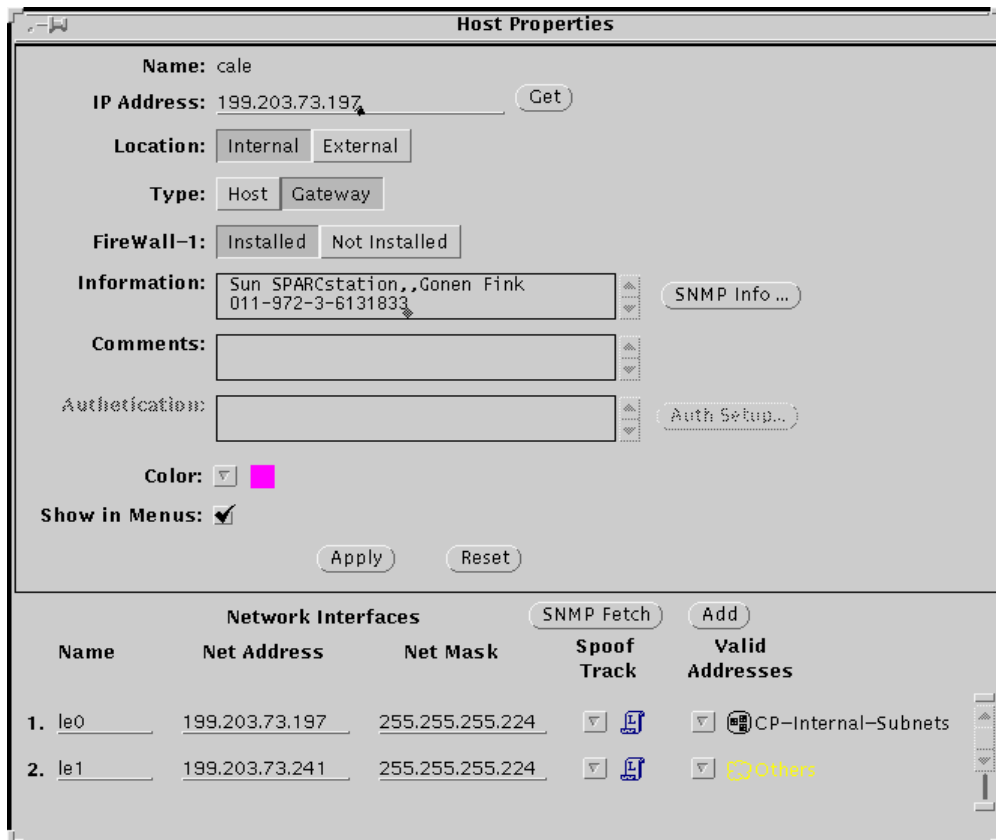
Administrator odpowiedzialny za wdrożenie polityki ochrony sieci prywatnej (niekiedy nazywany inżynierem *Security*) wykorzystuje graficzny interfejs Firewall-1, który obejmuje następujące komponenty:

- **Network Objects Manager** - okno dedykowane do wprowadzania danych o obiektach sieciowych, które podlegają bezpośredniej kontroli Firewall-1;
- **Users Manager** - okno pozwalające na wprowadzanie danych o użytkownikach i grupach użytkowników;
- **Services Manager** - okno umożliwiające definiowanie dodatkowych usług sieciowych;
- **Rule Base Editor** - edytor wykorzystywany do zapisywania reguł bezpieczeństwa;
- **Control Properties** - panel sterowania



Ilustracja 1. Network Objects Manager pozwala na definiowanie obiektów sieciowych, które podlegają bezpośredniej kontroli Firewall-1.

- określający podstawowe zasady funkcjonowania mechanizmu zabezpieczeń;
- **System Status View** - okno pozwalające na śledzenie stanu ochranianego systemu;
 - **Log Viewer** - okno umożliwiające zapoznanie się ze wszystkimi zdarzeniami, jakie zostały zarejestrowane przez Firewall-1.



Ilustracja 2. Definicja obiektu sieciowego typu gateway, który prowadzi przeciwdziałanie „spoofing”.

Definicja obiektów sieciowych odbywa się za pośrednictwem Network Objects Manager (Ilustracja 1). Obiekty sieciowe są reprezentantami fizycznych elementów sieci prywatnej, które podlegają bezpośredniej inspekcji (*host, gateway, router, network, domain, group*). Podczas definiowania obiektu typu *gateway* (Ilustracja 2) należy zaznaczyć czy będzie on prowadził przeciwdziałanie „spoofing”. W przypadku gdy *gateway* łączy sieci LAN, będące elementami jednej sieci zakładowej, prowadzenie przeciwdziałania „spoofing” może okazać się niepotrzebne - Firewall-1 może być użyty do ochrony sieci prywatnej przed niepożądanym oddziaływaniem sieci publicznej, jak również w ramach jednej dużej sieci prywatnej, może rozgraniczać jej podsieci, stosując niekiedy złączone rygory nadzoru.

Definicja użytkowników odbywa się za pośrednictwem Users Manager (Ilustracja 3) i sprowadza się do wprowadzenia informacji, które pozwolą na przeprowadzenie ich późniejszej identyfikacji, kontroli tożsamości i sprawdzenia czy są upoważnieni do korzystania z żądanych usług. Firewall-1 pozwala na prowadzenie kontroli tożsamości wyłącznie względem grup użytkowników, toteż zalecane jest aby wszyscy zdefiniowani użytkownicy zostali połączeni w grupy. Takie podejście sprzyja prowadzeniu bardziej zdyscyplinowanego i przejrzystego zarządzania, administrowania i kontrolowania użytkowników systemu. W procesie potwierdzania tożsamości użytkowników Firewall-1 stosuje zróżnicowane techniki:

Unix Password - hasło użytkownika w systemie UNIX;

Internal Password - wewnętrzne hasło użytkownika w Firewall-1;
S/Key - hasło użytkownika wygenerowane przez Firewall-1;
SecurID - hasło ustalone przez specjalną kartę (*Security Dynamics SecureID card*).

Ustalenie zasad bezpieczeństwa

Pierwsza, naczelną (domyślną) zasada Firewall-1 mówi: **„Wszystko co nie jest jednoznacznie dozwolone jest zabronione !”**. Podczas ustalania zasad bezpieczeństwa należy mieć na uwadze, iż jeżeli pominiemy pewne istotne fakty lub przyjęta koncepcja zabezpieczeń okaże się niekompletna, może to mieć bardzo poważne skutki dla dalszej pracy systemu. Zadanie dokonywania nadzoru przyjętej strategii ochrony spoczywa na module inspekcyjnym Firewall-1 (ang. Inspection Module). Należy pamiętać, iż warunkiem koniecznym skutecznej ochrony sieci prywatnej jest instalacja tego modułu na *gateway*, który łączy tę sieć z Internetem. Zasady funkcjonowania tego modułu ustalane są za pośrednictwem edytora zasad ochrony Rule Base Editor i panelu sterowania Control Properties.

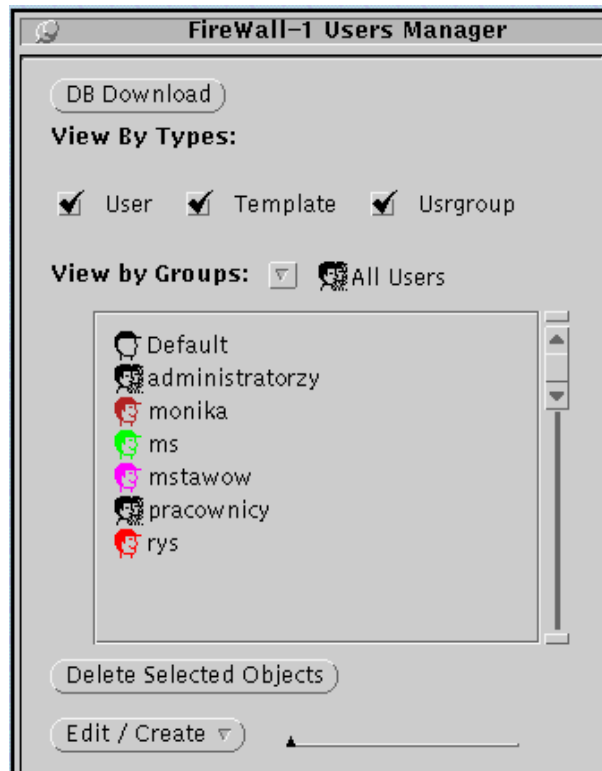
Rule Base Editor jest przeznaczony do zapisywania i weryfikacji poprawności zasad kontroli pakietów. Prowadzona weryfikacja zapewnia utrzymanie ich logicznej spójności i niesprzeczności. Na rysunku (Ilustracja 4) wyszczególniono pytania, na które należy odpowiedzieć przed przystąpieniem do ustalania reguł określających działanie modułu inspekcyjnego Firewall-1. Ilustracja 5 przedstawia przykładową konfigurację Rule Base Editor. Zapis kolejnych reguł odbywa się w analogiczny sposób jak wprowadzanie wierszy do tabeli relacyjnej bazy danych. Pierwsze trzy kolumny tej tabeli identyfikują pakiety, które zostaną poddane inspekcji:

- **Source** - miejsce pochodzenia pakietów;
- **Destination** - miejsce przeznaczenia pakietów;
- **Services** - typ pakietów.

Następne dwie kolumny decydują o reakcji Firewall-1 w przypadku wykrycia pakietów, które spełniają wcześniej określone warunki:

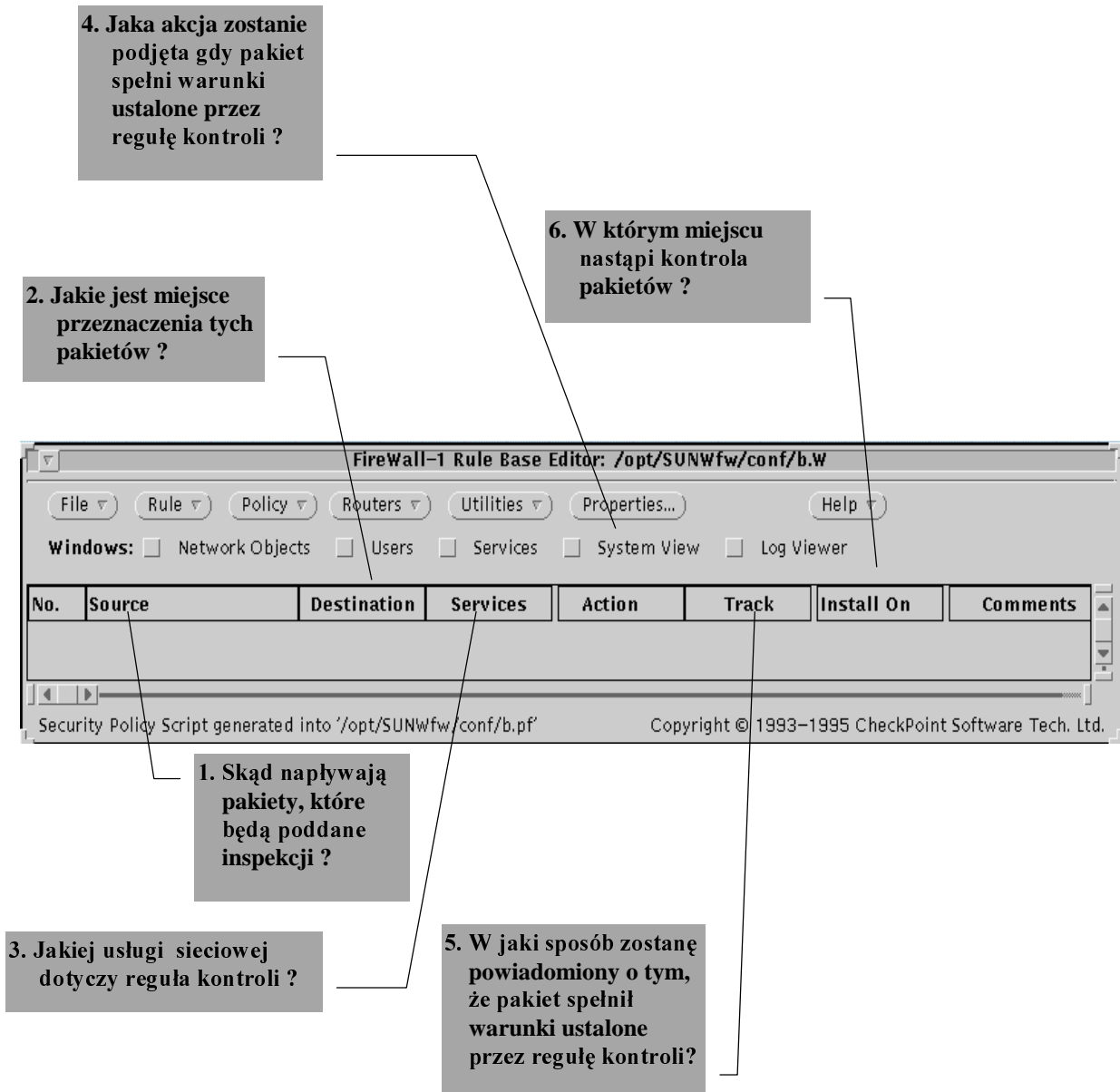
- **Action** - akcja podejmowana względem pakietów (odrzuć, zaakceptuj, wstrzymaj, zaszyfrowaj);
- **Track** - sposób powiadomienia administratora (podniesienie alarmu, zapis informacji o fakcie wystąpienia zdarzenia).

Panel sterowania **Control Properties** ustala wartości podstawowych parametrów systemu bezpieczeństwa, które zostały zgrupowane w pięciu kategoriach tematycznych:



Ilustracja 3. Definicja użytkowników odbywa się za pośrednictwem Users Manager.

- ◆ polityka bezpieczeństwa (**Security Policy**);
- ◆ rejestrowanie zdarzeń i alarmowanie (**Logging and Alerting**);
- ◆ zarządzanie przestrzenią nazw (**Name Resolving**);
- ◆ kontrola pracy router-ów (**Routers**);
- ◆ sprawdzanie tożsamości użytkowników (**Authentication**).



Ilustracja 4. Rule Base Editor jest przeznaczony do zapisywania reguł kontroli pakietów.

Najbardziej istotne ustalenia podejmowane są w grupie Security Policy (rys.6). W trakcie instalacji Firewall-1 wszystkie parametry tej kategorii przyjmują najbardziej typowe wartości domyślne, co znacznie eliminuje ryzyko podjęcia niewłaściwych decyzji, w przypadku gdy administrator nie jest do końca pewny znaczenia parametru. Wprowadzanie jakichkolwiek modyfikacji powinno być poprzedzone dokładną analizą wynikających z tego konsekwencji, nie tylko w aspektach bezpieczeństwa, ale również w odniesieniu do pracy całego systemu. Niedopuszczalnym jest aby wprowadzenie warstwy ochronnej systemu informatycznego zakłóciło jego prawidłowe funkcjonowanie (np. blokada serwera poczty elektronicznej czy serwera WWW). Pierwszy parametr

tej kategorii **Apply Gateway Rules to Interface Direction** określa kierunek przepływu pakietów przez *gateway*, w stosunku do których zostanie przeprowadzona kontrola określonych w Rule Base Editor zasad bezpieczeństwa. Istnieje możliwość wyboru jednej z trzech opcji:

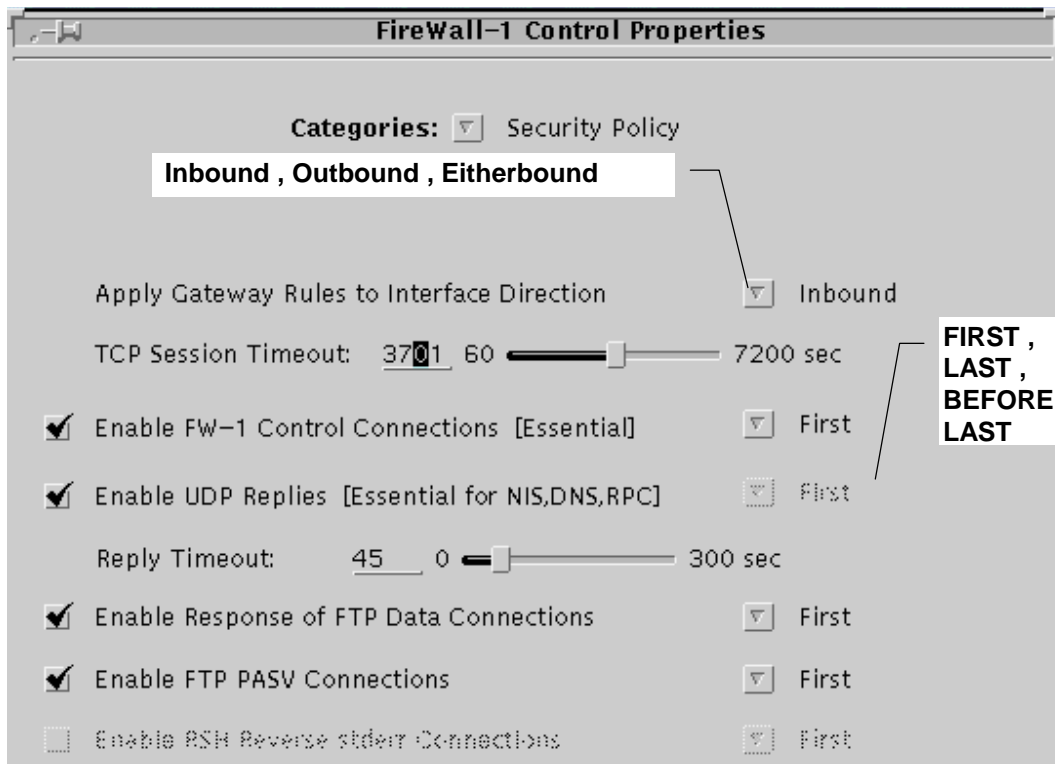
- Inbound** - sprawdzeniu podlegają pakiety napływające z sieci Internet;
- Outbound** - sprawdzeniu podlegają pakiety opuszczające sieć chronioną;
- Eitherbound** - sprawdzeniu podlegają wszystkie pakiety .

No.	Source	Destination	Services	Action	Track	Install On	Comments
1	Any	sparc	Any	reject	Alert	Gateways	ochrona gateway
2	sparc	Any	Any	reject	Short	Src	odrzuca pakiety inicjowane na gateway
3	Any	solaris	smtp	accept	Short	Gateways	uzytkownicy zewnetrzni maja dostep tylko do serwera poczty
4	clico	Any	Any	accept	Short	Gateways	uzytkownicy lokalni maja pelny dostep do Internet
5	Any	Any	Any	reject	Long	Gateways	wszystko co nie jest powyzej dozwolone jest ZABRONIONE

Ilustracja 5. Przykładowa konfiguracja Rule Base Editor.

Oczywiście, najbardziej ostrożnym podejściem jest wybór opcji ostatniej, która pozwala na dokonanie kontroli wszystkich przepływających przez *gateway* pakietów i która ustalona jest jako wartość domyślna. W pewnych okolicznościach, dla podniesienia efektywności funkcjonowania systemu (szczególnie przy dużym obciążeniu *gateway*), można zrezygnować z kontroli pakietów opuszczających sieć prywatną (rzadziej decydujemy się na pominięcie ograniczeń w stosunku do pakietów napływających z zewnątrz). Obniżenie efektywności funkcjonowania chronionej sieci komputerowej jest jednym z podstawowych zarzutów stawianych oprogramowaniu „firewall” - kontrola wszystkich pakietów znacznie obniża szybkość transmisji danych. Aby uniknąć sytuacji, w której warstwa ochronna stanie się „wąskim gardłem” systemu, przyjęta w Firewall-1 technologia **SMLI (Stateful Multi-Layer Packet Filtering)** wykorzystuje algorytmy selektywnej kontroli pakietów. W przypadku transmisji danych opartej o protokół TCP (*Transfer Control Protocol*), sprawdzeniu podlega tylko pierwszy segment sesji. Jeżeli wyniki kontroli okażą się pozytywne, adnotacja o otwartej i zatwierdzonej sesji TCP zostaje zapisana w bazie danych Firewall-1, a każdy następny segment tej sesji swobodnie osiągnie miejsce swojego przeznaczenia. Parametr **TCP Session Timeout** decyduje o tym jak dużo segmentów TCP, należących do zatwierdzonej sesji, może przekroczyć *gateway* bez sprawdzenia zgodności z regułami ustalonymi w edytorze Rule Base Editor. Jeżeli segment napłynie po upływie czasu TCP Session Timeout to traktowany jest przez Firewall-1 jako pierwszy segment nowej sesji. Następne dwa parametry tej kategorii są bardzo ważne dla aplikacji sieciowych, funkcjonujących w oparciu o model komunikacji *request/reply*, które

używają transportu UDP (*User Datagram Protocol*). W gronie tych aplikacji możemy wyróżnić tak istotne usługi TCP/IP jak: RPC (*Remote Procedure Call*), DNS (*Domain Name System*) i NIS (*Network Information Service*). Parametr **Enable UDP Replies** określa czy powracające pakiety dwukierunkowej komunikacji UDP zostaną zaakceptowane. Czas, przez który Firewall-1 toleruje powracające pakiety UDP, określa parametr **Reply Timeout**, mierzony od momentu odnotowania ostatniego pakietu.



Ilustracja 6. Security Policy zawiera podstawowe parametry, określające działanie modułu inspekcyjnego Firewall-1.

Opis pozostałych parametrów kategorii Security Policy, jak również innych elementów Firewall-1, które nie zostały zaprezentowane (translacja adresów IP, VPN, ...), można znaleźć w dostarczonej przez dystrybutora dokumentacji „*Solstice FireWall-1 Administrator's Guide*”.

Po ustaleniu wszystkich reguł funkcjonowania systemu ochrony, administrator powinien dokonać sprawdzenia ich poprawności z uwzględnieniem kolejności, w jakiej moduł inspekcyjny Firewall-1 prowadzi kontrolę pakietów:

1. ustalenia Control Properties -> Security Policy oznaczone jako FIRST;
2. reguły kontroli ustalone w Rule Base Editor;
3. ustalenia Control Properties -> Security Policy oznaczone jako BEFORE LAST;
4. ostatnia reguła w Rule Base Editor;
5. ustalenia Control Properties -> Security Policy oznaczone jako LAST.

Jeżeli wyniki weryfikacji polityki bezpieczeństwa okażą się pomyślne, można je zainstalować i przystąpić do testowania systemu pod względem szczelności i efektywności.

Opisane zagadnienia nie wyczerpują pełnego zakresu problematyki bezpieczeństwa. Intencją tej pracy było jedynie naświetlenie najistotniejszych aspektów procesu budowy systemu zabezpieczeń sieci

prywatnej. Osoby zainteresowane zaprezentowanym oprogramowaniem FireWall-1 mogą uzyskać dodatkowe informacje pod adresem e-mail: *support@clico.krakow.pl*.