BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 19, 2003

System ochrony sieci lokalnej zbudowany na bazie routerów Cisco

Marek KWIATKOWSKI, Zbigniew ŚWIERCZYŃSKI

Instytut Teleinformatyki i Automatyki WAT
ul. Kaliskiego 2, 00-908 Warszawa

STRESZCZENIE: W artykule opisany został projekt ochrony sieci lokalnej zbudowanej z wykorzystaniem routerów CISCO. Projekt powstał w ramach pracy dyplomowej, której celem było stworzenie aplikacji monitorującej przesyłanie pakietów przez router pełniący dodatkowo rolę ściany ogniowej pomiędzy przykładową siecią komputerową i Internetem.

1. Wstęp

Zarządzanie współczesnymi sieciami komputerowymi nabiera szczególnego znaczenia ze względu na szybki postęp informatyzacji we wszystkich dziedzinach życia. Konieczność monitorowania i zarządzania dużą ilością urządzeń sieciowych sprawia, że administrator sieci potrzebuje sprawnego systemu kontroli przesyłanych przez sieć danych. Zdarza się, że dostępne na rynku rozwiązania programowe nie spełniają określonych wymogów lub są za drogie. W takich sytuacjach można skonstruować własne zabezpieczenia korzystając z funkcji i narzędzi już posiadanych oraz ogólnie dostępnego w Internecie oprogramowania.

Celem artykułu jest przedstawienie sposobu wykorzystania routerów CISCO do ochrony sieci lokalnej, a w szczególności zaimplementowanie zasad filtrowania pakietów przy pomocy mechanizmu Access Control List (funkcji dostępnej w ramach systemu operacyjnego routerów Cisco) oraz skonstruowanie aplikacji służącej do monitorowania poprawności działania stworzonej zapory ogniowej (określenie zapora ogniowa często stosuje się zamiennie z określeniem ściana ogniowa – ang. firewall). Przed oprogramowaniem postawiono

następujące wymagania: powinna prezentować informacje dotyczące transmisji pakietów przez poszczególne interfejsy routera, a także zwracać uwagę administratora na zdarzenia mające szczególne znaczenie dla poprawnej pracy routera, takie jak zamiany konfiguracji routera czy zmiany stanów interfejsów. Oprogramowanie powinno na bieżąco informować o wszystkich opisanych powyżej zdarzeniach.

2. Zapora ogniowa

Fizyczna izolacja jest najprostszą metodą ochrony sieci komputerowej. W tej sytuacji nikt z zewnątrz nie będzie mógł atakować komputerów, jeśli fizycznie nie włamie się do pomieszczeń, gdzie się one znajdują. Choć takie podejście nie uwzględnia sytuacji, w której szkody może wyrządzić osoba z wewnątrz firmy, jest ona prosta i była stosowana przez wiele lat. W wielu przypadkach jest to wciąż najlepsze rozwiązanie systemu zabezpieczeń.

Obserwowany w ostatnich latach gwałtowny wzrost zainteresowania Internetem powoduje, że coraz trudniej jest utrzymać sieci komputerowe w fizycznej izolacji od świata zewnętrznego. Trudno sobie dziś wyobrazić sieć bez dostępu do poczty elektronicznej, grup dyskusyjnych i oczywiście usługi *World Wide Web*. W celu zapewnienia dostępu do wybranych usług Internetu i jednocześnie zapewnienia niezbędnego stopnia izolacji zaczęto stosować zapory ogniowe.

Zapory pozwalają stworzyć konfigurację, która zapewnia kompromis między siecią fizycznie izolowaną od Internetu i siecią swobodnie do niego podłączoną. Zapora jest umieszczona między siecią wewnętrzną i zewnętrzną, udostępniając mechanizm kontroli rodzaju przesyłanych pakietów między obiema sieciami.

Najprostszą wykorzystywaną architekturą zapory ogniowej jest pojedynczy obiekt działający na styku sieci chronionej i publicznej, który sprawdza rodzaj danych wymienianych pomiędzy tymi sieciami i na podstawie wprowadzonych wcześniej reguł podejmuje decyzję o tym co przepuścić, a co zablokować. Zaletą takiego rozwiązania jest jego centralizacja ułatwiająca monitorowanie i zarządzanie takim systemem. Cechę tę można także traktować jako wadę, ponieważ całe bezpieczeństwo zależy od jednego miejsca i przełamanie go jest równoznaczne z udostępnieniem chronionych zasobów intruzom. Wszystkie rozwiązania mają swoje zalety i wady, a to czy nadają się do pełnienia pewnych funkcji zależy w dużej mierze od wymagań, jakie są przed nimi stawiane przez użytkowników, oraz kryteriów wyboru, którymi kierują się

nabywcy. Tak więc rozwiązanie przedstawiane w niniejszym artykule powinno znaleźć grono użytkowników zainteresowanych wdrożeniem tego typu zabezpieczeń w swoich sieciach komputerowych.

W praktycznych zastosowaniach zaletą architektury bazującej na pojedynczym obiekcie filtrującym ruch na styku sieci chronionej i publicznej nie jest jej bezpieczeństwo, ale względy użytkowe i ekonomiczne. W porównaniu z systemami wielowarstwowymi, taka architektura jest tańsza, łatwiej zrozumiała, bardziej przekonywująca dla użytkowników i łatwiej dostępna. Takie rozwiązanie można określić jako względnie tanie, ponieważ zwykle do kontaktu z Internetem i tak potrzebny jest router, który dodatkowo można wykorzystać jako filtr pakietów. Te same funkcje może także zrealizować programowa zapora ogniowa, jednak w tym przypadku wiąże się to z dodatkowymi kosztami. Firewall na routerze jest więc dobrym rozwiązaniem dla małych ośrodków, jak i dla użytkowników szukających narzędzia, które można szybko skonfigurować i wdrożyć. Należy jednak pamiętać, że nie ma rozwiązań uniwersalnych i każde z nich wymaga podjęcia świadomych decyzji, ostrożnego konfigurowania i utrzymania.

Router ekranujący chroniący sieć wewnętrzną jest przykładem zapory ogniowej działającej jako filtr pakietów. Tego typu firewall posiada wszystkie zalety wymienione wcześniej, a w porównaniu do niedrogich rozwiązań programowych (np. osadzonych na komputerze z dwiema kartami sieciowymi) wyróżnia się jeszcze innymi praktycznymi cechami.

Proste filtrowanie pakietów uważa się za wydajne, ponieważ wymaga zwrócenia uwagi tylko na kilka typów nagłówków. Routery nie będące filtrami pakietów i tak muszą dokonywać w trakcie trasowania analizy niektórych pól nagłówków np. adresów odbiorcy, przez co narzut obliczeniowy, powodowany przez wprowadzenie reguł filtrowania, nie zwiększa się tak bardzo, jak można by się spodziewać.

Kolejną zaletą jest zdolność routera do selektywnego analizowania i przekazywania pakietów różnych protokołów sieciowych. Warunki przepuszczenia i odrzucenia można budować oddzielnie dla protokołów: IP, IPX, TCP, UDP, AppleTalk, IPX SAP, ICMP.

Pomimo powszechności zastosowania routerów na styku różnych sieci tego typu firewall nie jest rozwiązaniem często stosowanym. Zastosowane w routerach filtry nie mają najczęściej zbyt rozbudowanego systemu rejestrowania ruchu przechodzącego przez zaporę, prób włamań czy udzielania użytkownikom różnego rodzaju dostępu. Problem więc stanowi monitorowanie i zarządzanie tego typu zaporą ogniową w czasie rzeczywistym. Przydatne może wydawać się posiadanie narzędzi raportujących zdarzenia zachodzące w routerze i przedstawiania ich w przejrzystej formie na konsoli administratora.

Niektóre współczesne routery mają wbudowaną obsługę rejestrowania naruszeń filtra za pomocą narzędzia *syslog*, jednak sposób prezentacji wyników pozostawia wiele do życzenia.

Programowanie routera mającego pełnić funkcje zapory ogniowej wymaga wykonania następujących czynności:

- zablokowania pakietów nieużywanych usług,
- zezwolenia na połączenia przychodzące z określonych serwerów sieciowych i blokowanie pozostałych,
- zezwolenia komputerom z sieci wewnętrznej na inicjowanie połączeń z komputerami pracującymi w sieci zewnętrznej.

3. Listy dostępu (ang. Access Control List)

Systemy operacyjne routerów Cisco mają wbudowany mechanizm filtrowania ruchu pakietów poprzez listy dostępu. Filtrowanie pakietów jest jednym z podstawowych sposobów zabezpieczenia i ograniczenia ruchu w sieci. Pozwala określić sieci źródłowe i docelowe, między którymi może odbywać się komunikacja, jak również wskazać dopuszczalny lub zabroniony typ pakietów występujących w danym połączeniu. Lista dostępu jest zestawem reguł, na podstawie których router podejmuje decyzję, czy dane pakiety przepuścić, czy odrzucić.

Router przetwarza warunki zapisane na liście dostępu w sposób sekwencyjny. Listy dostępu są zbiorem kryteriów dotyczących typu i kierunku ruchu pakietów. Przetwarzanie ich jest sekwencyjne, co oznacza, że router analizuje warunki po kolei, porównując nagłówek pakietu ze wzorcem zapisanym w liście dostępu. Spełnienie warunku znajdującego się wyżej na liście zamyka proces sprawdzania, a warunek ten decyduje o akceptacji lub odrzuceniu pakietu niezależnie od tego, czy pakiet spełniłby następne warunki. W przeciwnym razie sprawdzane są następne warunki aż do wyczerpania listy. Kolejność kryteriów zapisanych w listach dostępu ma więc zasadnicze znaczenie. Jednym wpisem można zablokować wszystkie pakiety. W każdej liście dostępu występuje końcowy i ostateczny warunek, który odrzuca wszystkie pakiety. Wynika z tego, że w sytuacji gdy pakiet nie spełni żadnego z zadeklarowanych przez administratora warunków, zostanie odrzucony przez warunek *implicit deny any* (odrzucenie wszystkiego), który jest niejawnie dodawany na końcu każdej listy ACL. Przy konstruowaniu listy dostępu należy zawsze pamiętać o dwóch rzeczach: kolejności kryteriów oraz warunku ostatecznym, odrzucającym wszystkie pakiety. Zarządzanie ruchem dotyczy

zwykle konkretnego interfejsu routera i kierunku ruchu. Istotne jest więc to, z którym interfejsem routera skojarzona zostanie lista dostępu oraz czy filtrowanie ma działać na wejściu czy na wyjściu interfejsu. Jeżeli lista dostępu zadeklarowana jest na wejściu, to konfiguracja interfejsu "wejściowego" sprawdzana jest przed przystąpieniem do trasowania pakietu. Natomiast jeżeli lista dostępu przypisana jest do wyjścia przez dany interfejs, to przetwarzanie pakietu odbywa się zgodnie z następującą kolejnością: router sprawdza w tablicy routingu, przez który interfejs należy przesłać dany pakiet, przesyła go do niego, a następnie na podstawie reguł przypisanych do tego interfejsu podejmuje decyzję czy prześle go dalej, czy zablokuje. Istotnym elementem przy konstruowaniu list dostępu jest sposób adresowania zastosowany przy opisywaniu warunków. Router wykorzystuje specyficzne oznaczenia hostów i sieci za pomocą tzw. maski wzorca, nazywanej też *dziką maską* (ang. *wildcard mask*). Jest to zapis maski, w którym bit ustawiony na 0 nakazuje porównanie odpowiadającego mu bitu w adresie analizowanego pakietu z odpowiednim bitem w warunku. W przypadku bitu ustawionego na 1 odpowiadający mu bit w adresie nie jest sprawdzany ze wzorcem, a zatem może być dowolny. Na przykład, chcąc stworzyć regułę dla pakietów kierowanych do hosta o adresie IP 131.108.1.100, maska wzorca w liście dostępu powinna mieć wartość 0.0.0.0, a opis hosta w warunku listy dostępu wyglądać następująco: 131.108.1.100 0.0.0.0. Natomiast dowolny adres w podsieci 131.108.1.0/24 można opisać jako 131.108.1.0 0.0.0.255. Oznacza to, że tylko bity ostatniego bajtu adresu w pakietach IP nie będą porównywane ze wzorcem. Dowolnego adresata w sieci IP można wskazać, za pomocą zapisu 0.0.0.0 255.255.255.255. Przy stosowaniu podsieci, należy uważnie wyliczyć, ile bitów można zignorować podczas porównywania ze wzorcem, a ile bitów dokładnie musi mu odpowiadać. Zakładając, iż planujemy objąć naszym warunkiem każdego adresata w podsieci 192.168.1.64/27 (podsieć ta utworzona jest na 3 bitach ostatniego bajtu), maska wzorca musi powodować analizę trzech pierwszych bajtów adresu oraz dodatkowo trzech bitów ostatniego bajtu w nadesłanych pakietach IP. Pozostałe 5 bitów może być dowolne, np.:

zapis podsieci 192.168.1.64/27,

ostatni bajt w/w adresu - 0 1 0 0 0 0 0 0,

maska wzorca (ostatni bajt) - 0 0 0 1 1 1 1 1 = 31,

zapis adresu podsieci w liście dostępu - 192.168.1.64 0.0.0.31.

Zdarza się, że dla uproszczenia zapisu warunków list dostępu stosuje się tzw. ukryte maski wzorca, pozwalające na wskazanie dowolnego adresu (*any*) lub konkretnego adresata (*host*). Na przykład host o adresie 131.108.1.100 można wskazać na dwa sposoby: „131.108.1.100 0.0.0.0” lub „host 131.108.1.100”.

Identyfikacja list dostępu odbywa się poprzez numer, który jest niepowtarzalny w ramach jednego routera. Numer ten wskazuje jednoznacznie listę dostępu, jej typ oraz protokół, którego ona dotyczy. Zakresy tych numerów są z góry określone, więc posługiwanie się nimi zależy głównie od tego, jaki rodzaj ruchu ma być filtrowany. Zakres obsługiwanych list dostępu różni się, zależnie od wersji systemu operacyjnego routera. W Cisco IOS zostały przyporządkowane następujące zakresy numeryczne dla poszczególnych typów list dostępu:

- ACL IP standardowe – numery od 1 do 99,
- ACL IP rozszerzone – numery od 100 do 199,
- ACL AppleTalk – nr 600 – 699,
- ACL IPX – nr 800 – 899,
- ACL Rozszerzone IPX – nr 900 – 999,
- ACL IPX SAP – nr 1000 –1099.

Standardowe listy dostępu są proste w konfiguracji, ale nie mają możliwości zaawansowanej analizy pakietów. W trakcie konfiguracji warunków jedynym kryterium wyboru pakietu jest adres źródłowy. Standardową listę dostępu tworzy się poleceniem trybu konfiguracyjnego, którego składnia została przedstawiona poniżej:

C2600(config)#access-list *numer_listy_dostępu*{permit|deny}
adres_źródłowy_pakietu maska_wzorca [log].

Numer listy dostępu ma wartość z przedziału od 1 do 99 (dla IP), natomiast adres źródłowy pakietu w połączeniu z maską wzorca tworzy zapis adresu hosta lub sieci nadawcy. W standardowej liście dostępu przy dopasowaniu warunku brany jest pod uwagę tylko adres źródłowy. Lista taka nie odróżnia ruchu związanego z protokołem TCP czy UDP. Podobnie jest z typami aplikacji. Opcja *log* wymusza wysłanie komunikatu dla każdego pakietu dopasowanego do tego wzorca. Listę dostępu przypisujemy do interfejsu poleceniem o następującej składni:

C2600(config-if)#ip access-group *numer_listy_dostępu* {in|out}.

Powyższe polecenie dotyczy filtrowania pakietów na poziomie interfejsu i jest jednym z wariantów wykorzystania list dostępu. Oprócz podania numeru listy kojarzonej z danym interfejsem, należy określić tryb analizowania listy: na wejściu (*in*) czy na wyjściu pakietu z interfejsu (*out*), domyślnie out.

Listy rozszerzone w większym stopniu dają możliwość wyboru ruchu, który ma być filtrowany. Poprzez zastosowanie adresu docelowego i maski wzorca można dodatkowo wskazać konkretny adres odbiorcy, całą sieć, podsieć lub wszystkich potencjalnych odbiorców. Ciekawym rozwiązaniem jest możliwość określenia protokołu, którego ma dotyczyć warunek. W trakcie konfiguracji listy dla protokołów TCP bądź UDP można również wybrać numery portów, na których będą filtrowane pakiety. Konstrukcja warunków dla listy rozszerzonej musi być wykonywana z dużo większą precyzją, ponieważ nieznajomość sposobu działania protokołów może powodować późniejsze błędne działanie routera. Listę rozszerzoną tworzymy następującym poleceniem:

C2600(config)#access-list *numer_listy* {permit|deny} *protokół*
adres_źródłowy [*operator port*] a*dres_docelowy*
[*operator port*] [established] [log]

Adresy źródłowe i docelowe konstruowane są podobnie jak w listach standardowych (adres hosta lub sieci i maska wzorca). Istnieje możliwość korzystania ze słów kluczowych *host* i *any*. Postać komendy access-list zależy od protokołu, którego dotyczy warunek. Dla protokołów warstwy transportowej (TCP czy UDP) można posłużyć się operatorem pozwalającym na wskazanie portów: Lt - mniejsze od, Gt - większe od, Eq - równe, Neq - różne od. Opcję *established* stosuje się tylko dla protokołu TCP i dotyczy ona segmentów, w których ustawiono bit synchronizacji (SYN) podczas zestawiania sesji TCP.

Oprócz IP, TCP i UDP często stosowane jest filtrowanie innych protokołów, takich jak ICMP czy IGMP. Polecenie tworzące listę rozszerzoną dla protokołu ICMP ma następującą składnię:

C2600(config)#access-list *numer_listy* {permit|deny} icmp
adres_źródłowy adres_docelowy [*typ_icmp* [*kod_icmp*] |
komunikat_icmp]

Jeśli, istnieje potrzeba zablokowania wysyłania odpowiedzi do programu ping, należy wskazać odpowiedni typ komunikatu ICMP. Taki efekt można osiągnąć przez wpisanie numeru komunikatu ICMP, w tym wypadku 0, lub nazwy *echo-reply*:

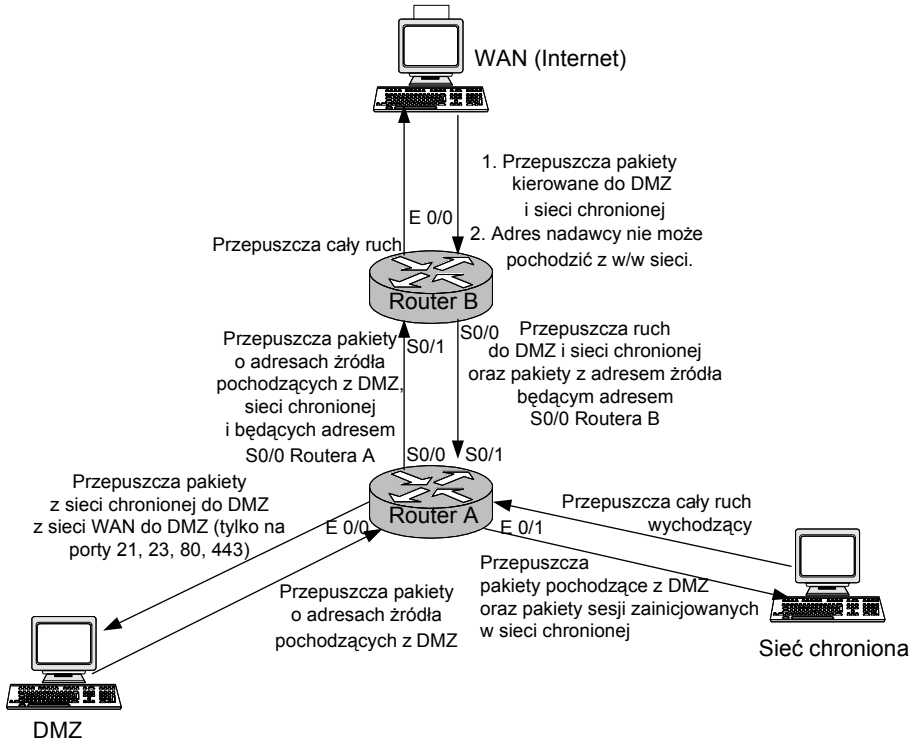
C2600(config)#access-list 133 deny icmp any any echo-reply

Pewnym ułatwieniem jest posługiwanie się nazwami list dostępu zamiast ich numerowania. Należy jednak pamiętać, że nie każdy system operacyjny na to pozwala.

4. Konfiguracja sieci komputerowej

W ramach artykułu został przedstawiony system ochrony sieci lokalnej z wykorzystaniem routerów CISCO. W celu praktycznego sprawdzenia działania zaprojektowanego systemu należało zbudować model sieci testowej z zaimplementowanymi zasadami filtrowania pakietów przy pomocy mechanizmu Access Control List (ACL). Kolejnym etapem tworzenia systemu ściany ogniowej było zaprojektowanie i implementacja aplikacji przetwarzającej pozyskane opisy zarejestrowanych zdarzeń (logi) opisujące działanie routera i na ich podstawie generującej posumowania dotyczące transmitowanych pakietów. Na koniec przeprowadzono testy i sprawdzono poprawność działania zbudowanego systemu.

W trakcie realizacji zadania wykorzystano trzy komputery (dwa symulujące sieci lokalne, jeden sieć Internet) oraz dwa routery Cisco z serii 2600. Konieczne było wykorzystanie dwóch routerów ponieważ żaden z niech nie posiadał trzech interfejsów typu Ethernet. Model badanej sieci wraz z przyjętymi zasadami filtrowania pakietów przedstawia rys. 1:



Rys. 1. Model badanej sieci z zasadami filtrowania pakietów

Zasadniczym elementem projektu było stworzenie aplikacji, wspomagającej pracę administratora sieci, poprzez zbieranie, przetwarzanie i zobrazowanie wybranych informacji pochodzących z routera. Proponowana konfiguracja routera pozwala na otrzymywanie informacji dotyczących:

- ilości przesyłanych i odrzuconych pakietów *TCP*,
- ilości przesyłanych i odrzuconych pakietów *UDP*,
- ilości przesyłanych i odrzuconych komunikatów *ICMP*,
- ilości przesyłanych i odrzuconych pakietów kierowanych na porty: 21 (*FTP*), 23 (*TELNET*), 80 (*HTTP*) i 443 (*SSL*),
- zmian konfiguracji routera,
- zmian stanów interfejsów.

Powyższe informacje uzyskiwane są przy wykorzystaniu mechanizmu *syslog* udostępnianego przez system operacyjny Cisco IOS.

Usługę *syslog* skonfigurowano na Routerze A tak, aby wysyłała potrzebne informacje do jednego z hostów w sieci chronionej, na którym zainstalowano serwer odbierający komunikaty od demona *syslog*. Do tego celu użyto darmowej wersji serwera raportującego o nazwie *Kiwi Syslog Demon* w wersji 7.0.2, pobranego ze strony internetowej: http://www.kiwisyslog.com/links/syslogd_standard_current_kiwitools.htm (stan z dnia 10.11.2002). Istotną zaletą powyższego oprogramowania jest możliwość zapisywania otrzymywanych komunikatów do pliku tekstowego. Właściwość ta jest wykorzystywana przez aplikację generującą statystyki routera.

5. Opis aplikacji wspomagającej pracę administratora sieci

Do stworzenia aplikacji o nazwie „Ststystyki", która wspomaga pracę administratora sieci wykorzystano środowisko programistyczne Borland Delphi w wersji 6.0. Założono, że projektowana aplikacja wspomagająca pracę administratora sieci będzie pracowała pod kontrolą systemu operacyjnego Microsoft Windows.

Aplikacja składa się z dwóch modułów – jednego przetwarzającego informacje dotyczące transmisji poprzez poszczególne interfejsy i drugiego badającego na jakie porty kierowane były przesyłane dane.

Pierwszy moduł ma na celu zobrazowanie informacji o przepuszczonych i odrzuconych pakietach dla wszystkich interfejsów, a także informacji istotnych z punktu widzenia poprawnej pracy routera, do których zaliczono informacje o zmianach konfiguracji routera i informacje dotyczące ewentualnych zmian stanów interfejsów. Ze względu na dużą ilość prezentowanych informacji, interfejs stworzono na tyle duży i przejrzysty, żeby użytkownik nie miał problemów z wyszukaniem interesujących go informacji.

Opisywany interfejs powinien w szczególny sposób informować użytkownika o zaistnieniu wspomnianych wyżej zdarzeń, mających istotny wpływ na poprawną prace routera, tj. o zmianie konfiguracji routera i o ewentualnych zmianach stanów interfejsów. Te informacje można traktować jako krytyczne dla bezpieczeństwa sieci, więc ich wystąpienie należało wyróżnić spośród innych wyświetlanych wyników przeszukiwania pliku dziennika. W związku z tym umieszczono na interfejsie opisywanego modułu elementy graficzne, będące dodatkową informacją, która powinna zwrócić uwagę użytkownika aplikacji wspomagającej pracę administratora sieci na wystąpienie zdarzeń takich jak zmiany konfiguracji routera i zmiany stanów interfejsów.

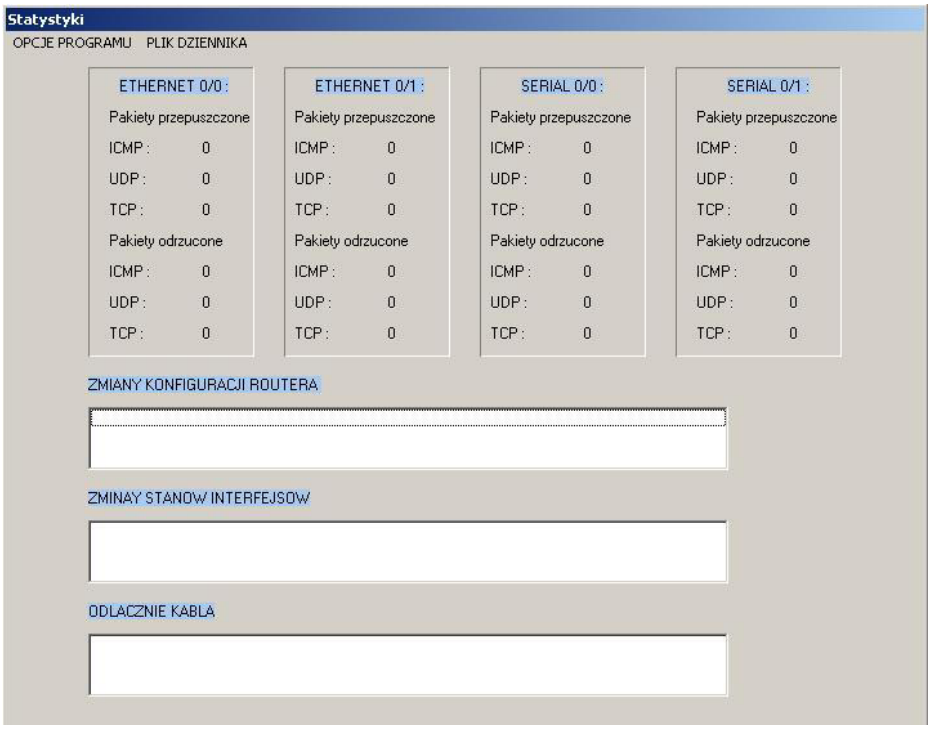
Proponowany interfejs graficzny dla modułu pierwszego przedstawia rys. 2. Opisywane wcześniej elementy graficzne, mające być dodatkową informacją dla użytkownika aplikacji wspomagającej pracę administratora sieci są niewidoczne. Ich działanie zostało przedstawione w dalszej części artykułu.

W zaproponowanym modelu sieci testowej najważniejsza rola przypada routerowi A. Posiada on dwa interfejsy typu Ethernet i dwa interfejsy typu Serial. Dla potrzeb badanej sieci testowej wykorzystuje jedynie dwa interfejsy typu Ethernet i jeden interfejs typu Serial. Aplikacja wspomagająca pracę administratora sieci jest jednak przygotowana do obsługi wszystkich interfejsów, nawet tych, które nie są wykorzystywane w trakcie eksploatacji sieci testowej. Tak więc na interfejsie projektowanego modułu powinno się znaleźć miejsce również dla tego interfejsu, który nie jest wykorzystywany.

Poniżej przedstawiono szczegółowy opis działania modułu pierwszego.

Po uruchomieniu aplikacji wspomagającej pracę administratora sieci, użytkownik ma do dyspozycji interfejs modułu pierwszego, przedstawiony na rys 2. Interfejs oferuje dwa rozwijane menu, o nazwie „OPCJE PROGRAMU” i „PLIK DZIENNIKA”.

Po rozwinięciu menu o nazwie „OPOCJE PROGRAMU” użytkownik ma do dyspozycji opcje: „START”, „STOP”, „FILTR PORTÓW”, „ZEROWANIE LICZNIKÓW” i „WYJŚCIE”.



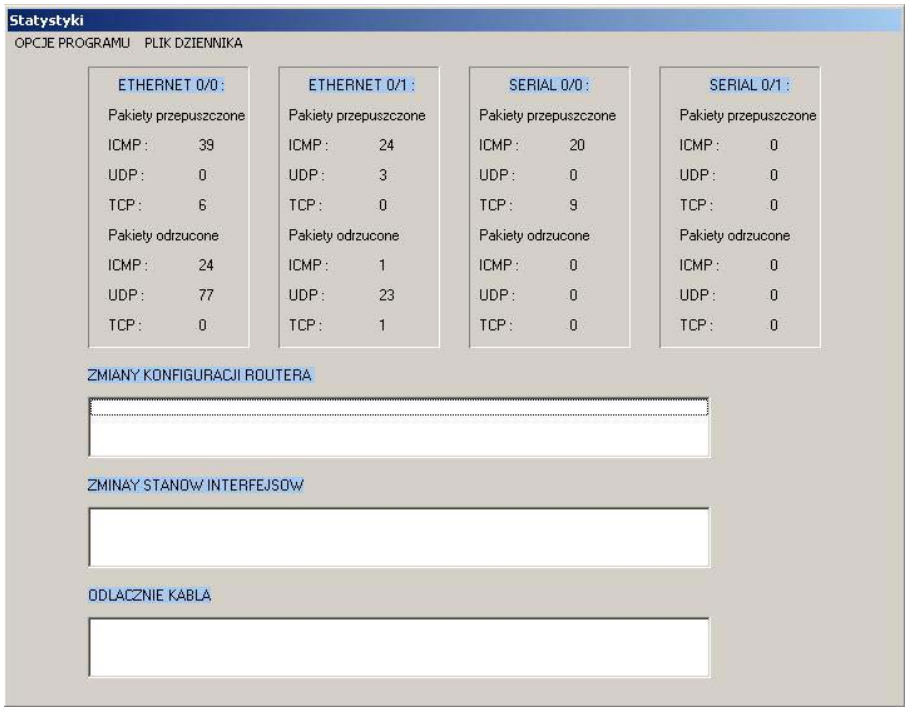
Rys. 2. Interfejs modułu pierwszego

Wybranie opcji „START" rozpoczyna działanie timera, który co pięć sekund przeszukuje plik dziennika serwera *syslog* w celu zdobycia informacji na temat przepuszczonych i odrzuconych pakietów na poszczególnych interfejsach. Pierwszym krokiem w tej procedurze jest otwarcie pliku dziennika, znajdującego się w konkretnym, ustalonym wcześniej miejscu. Przykładowa linia zapisana w tym pliku, odpowiadająca informacji pochodzącej z jednej z zaimplementowanych list dostępu wygląda następująco:

„*2003-02-21 17:09:11 Local7.Info 131.108.110.1 281: 01:36:19: %SEC-6-IPACCESSLOGP: list 101 denied udp 131.108.110.2(138) -> 131.108.110.255(138), 1 packet*".

Moduł pierwszy analizuje linię od początku aż do znaku końca linii. Pierwszym elementem jest data zapamiętywana pod odpowiednią zmienną programu. Zapamiętana zostaje również godzina, będąca drugim elementem analizowanej linii. Kolejne pozycje analizowanej linii aż do znaku – „%" są pomijane, ponieważ nie mają znaczenia dla działania modułu pierwszego.

Wystąpienie tego znaku jest sygnałem, że kolejny ciąg analizowanej linii jest kodem komunikatu wysłanego przez jedną z zaimplementowanych list dostępu. Po rozpoznaniu kodu komunikatu moduł odczytuje numer listy dostępu występujący po słowie „*list*". Lista dostępu numer 101 jest przyporządkowana do interfejsu E0/0, lista numer 102 jest przyporządkowana do interfejsu E0/1, a lista numer 103 jest przyporządkowana do interfejsu S0/0. Na podstawie numeru listy dostępu, opisywany moduł rozpoznaje, którego interfejsu dotyczy komunikat. Następny ciąg analizowanej linii informuje o tym, czy pakiety zostały przepuszczone – „*permitted*", czy też odrzucone – „*denied*". Kolejny ciąg znaków oznacza rodzaj transmisji. Poszukiwane rodzaje transmisji to: „*ICMP*", „*TCP*" i „*UDP*". Po rozpoznaniu rodzaju transmisji, opisywany moduł odczytuje przedostatni ciąg znaków oznaczający ilość pakietów. Adresy nadawcy i odbiorcy są pomijane, jako nie istotne z punktu widzenia poprawnego działania modułu pierwszego. Po znalezieniu znaku końca linii przeszukiwanie pliku dziennika przenosi się do następnej linii. Operacja jest powtarzana aż do znalezienia znaku końca pliku. Przykładowy widok interfejsu modułu pierwszego obrazujący ilość przesłanych i odrzuconych pakietów przez router przedstawiony jest na rys. 3.



Rys. 3. Interfejs modułu pierwszego. Informacje o ruchu pakietów przez router

Drugim typem komunikatu, który może wystąpić w pliku dziennika jest komunikat informujący o zmianie konfiguracji routera. Występują trzy rodzaje takich komunikatów:

- komunikat informujący o zmianie konfiguracji routera za pomocą konsoli bezpośrednio podłączonej do routera:

„*2003-02-21 17:05:48 Local7.Notice 131.108.110.1 273: 01:32:56: %SYS-5-CONFIG_I: Configured from console by console*”,

- komunikat informujący o zmianie konfiguracji routera za pomocą połączenia telnetowego. W tym konkretnym przypadku z komputera o adresie IP 131.108.110.2:

„*2002-10-11 14:33:13 Local7.Notice 131.108.110.1 128: 1d05h: %SYS-5-CONFIG_I: Configured from console by vty0 (131.108.110.2)*”,

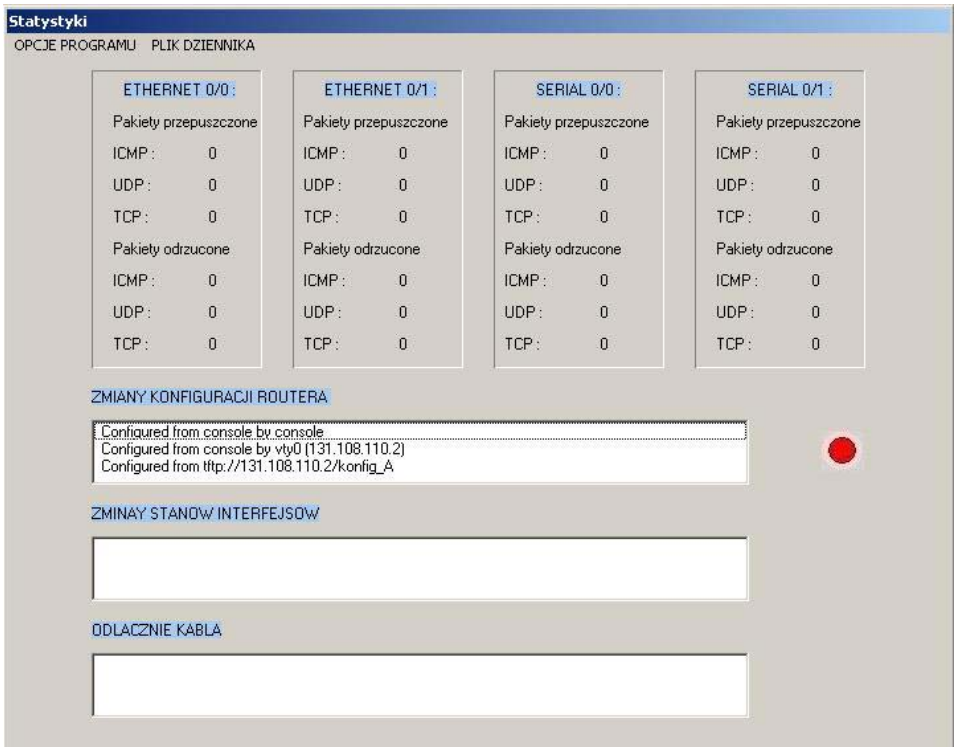
- komunikat informujący o zmianie konfiguracji routera przy użyciu serwera *TFTP*. W tym konkretnym przypadku znajdującego się na komputerze o adresie IP 131.108.110.2, zaś plik konfiguracyjny przesyłany z serwera *TFTP* nazywa się „*konfig_A*”:

„*2002-12-16 14:42:43 Local7.Notice 131.108.110.1 2617: 00:19:52: %SYS-5-CONFIG: Configured from tftp:///131.108.110.2/konfig_A*”.

Do momentu wystąpienia znaku „%” odczytywanie każdej z przedstawionych powyżej linii odbywa się identycznie jak we wcześniej opisanym przypadku zliczania pakietów. Różnice zaczynają się po wykryciu ciągu znaków oznaczających zmianę konfiguracji, ponieważ w tym przypadku pobierana jest cała treść komunikatu dotycząca sposobu zmiany konfiguracji i wyświetlana na interfejsie modułu pierwszego w oknie „ZMIANY KONFIGURACJI ROUTERA”. Wyświetlany jest również element graficzny, mający zwrócić uwagę użytkownika na wystąpienie szczególnie ważnego zdarzenia. Przykładowy widok interfejsu modułu pierwszego po wykryciu wszystkich opisanych rodzajów zmian konfiguracji przedstawiony jest na rys. 4.

Trzecim typem komunikatu występującym w pliku dziennika jest komunikat informujący o zmianach stanów interfejsów routera. Występują dwa rodzaje powyższych komunikatów:

- komunikaty informujące o zmianie administracyjnego stanu interfejsu. Zmiany takie można wywołać przez wydanie polecenia „SHUTDOWN” albo



Rys. 4. Interfejs modułu pierwszego. Ostrzeżenie o zmianie konfiguracji

„NO SHUTDOWN" w trybie konfiguracyjnym interfejsu routera. Linie tych komunikatów wyglądają następująco:

> „*2002-10-11 15:10:57 Local7.Notice 131.108.110.1 172: 1d06h: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down*",
>
> lub
>
> „*2002-10-11 15:11:12 Local7.Error 131.108.110.1 174: 1d06h: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up*",

- komunikaty informujące o zmianie stanu połączenia fizycznego. Zmiany takie można wywołać przez fizyczne odłączenie kabla od interfejsu routera lub jego ponowne podłączenie. Powoduje to jednoczesne wyświetlenie komunikatu opisanego wcześniej, a dotyczącego zmiany stanu interfejsu. Linie tego komunikatu wyglądają następująco:

„*2002-10-11 15:11:12 Local7.Notice 131.108.110.1 175: 1d06h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up*”,

lub

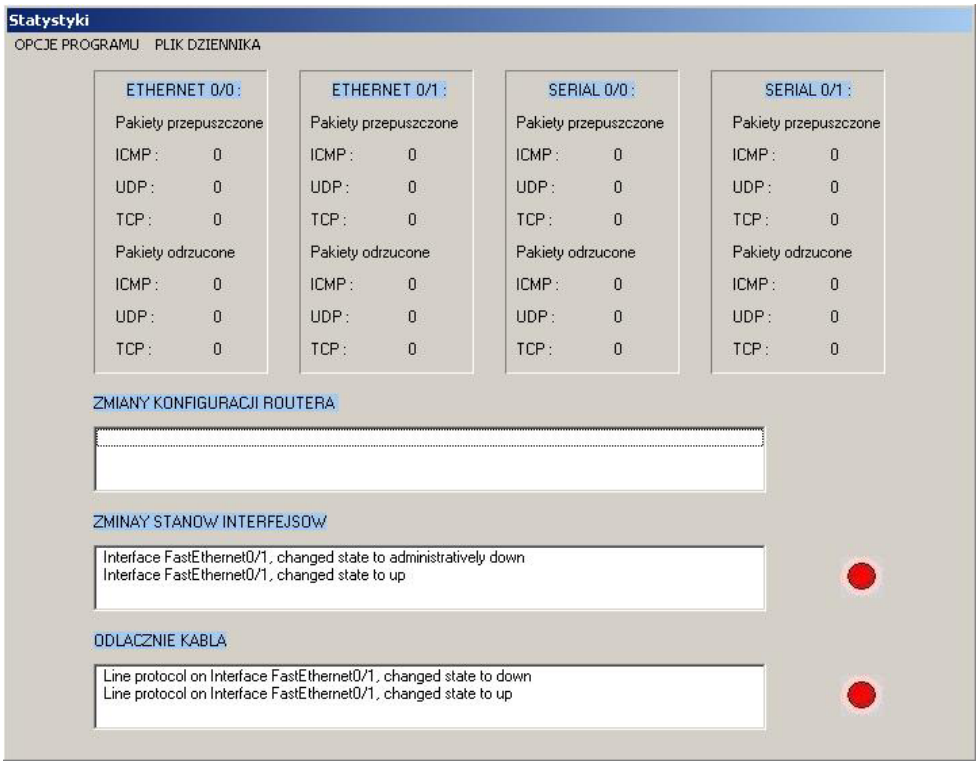
„*2002-10-11 15:10:57 Local7.Notice 131.108.110.1 173: 1d06h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down*”.

Odczytywanie każdej z przedstawionych powyżej linii odbywa się identycznie jak w przypadku omawianych wcześniej komunikatów o zmianie konfiguracji routera i pochodzących z list dostępu. Po odczytaniu kodu oznaczającego zmianę stanu interfejsu pobierana jest cała treść komunikatu dotycząca wspomnianego zdarzenia, aż do znaku końca linii. Jeśli odczytany kod dotyczy zmiany stanu połączenia fizycznego, ciąg informujący o zdarzeniu wyświetlany jest na interfejsie modułu pierwszego w oknie o nazwie „ODŁĄCZENIE KABLA”. Jeśli zaś dotyczy zmiany stanu interfejsu routera, ciąg informujący o zdarzeniu wyświetlany jest na interfejsie modułu pierwszego w oknie o nazwie „ZMIANY STANÓW INTERFEJSÓW”. W obu przypadkach wyświetlany jest również element graficzny, mający zwrócić uwagę użytkownika na wystąpienie szczególnie ważnego zdarzenia. Przykładowy widok interfejsu modułu pierwszego po wykryciu obu opisanych komunikatów przedstawiony jest na rys. 5.

„STOP” jest kolejną opcją dostępną w menu „OPCJE PROGRAMU”. Wybór tej pozycji zatrzymuje pracę timera odpowiedzialnego za przeszukiwanie pliku dziennika. Stan interfejsu po wyborze opcji „STOP” odzwierciedla wyniki ostatnio przeprowadzonego przeszukiwania pliku dziennika. Po wyborze pozycji „STOP” moduł pierwszy aplikacji wspomagającej pracę administratora sieci znajduje się w stanie oczekiwania na polecenie ze strony użytkownika. Ponowne uruchomienie timera następuje po wybraniu pozycji „START” z menu „OPCJE PROGRAMU”.

Opcja „ZEROWANIE LICZNIKÓW” znajdująca się w menu „OPCJE PROGRAMU” powoduje wyzerowanie liczników na interfejsie modułu pierwszego. Opisywana opcja nie powoduje podjęcia przez aplikacje żadnych innych działań i służy jedynie zwiększeniu czytelności interfejsu modułu pierwszego.

„WYJŚCIE” jest poleceniem oznaczającym zakończenie pracy aplikacji „Statystyki” i powoduje zamknięcie zarówno głównego okna modułu pierwszego jak i ewentualnie otwartego okna modułu drugiego.

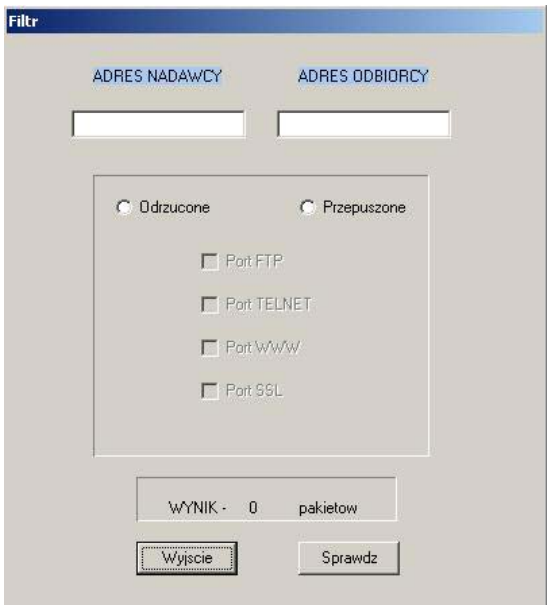


Rys. 5. Interfejs modułu pierwszego. Ostrzeżenie o zmianie stanów interfejsów

Ostatnią pozycją menu „OPCJE PROGRAMU” jest opcja „FILTR PORTÓW”. Powoduje ona wyświetlenie interfejsu modułu drugiego i udostępnia użytkownikowi kolejne warianty przeszukiwania pliku dziennika. Interfejs modułu drugiego przedstawia rys. 6.

Moduł drugi jest odpowiedzialny za przeszukiwanie pliku dziennika pod kątem portów, na które przesyłane są pakiety. Poszukiwane numery portów: 21 (*FTP*), 23 (*TELNET*), 80 (*WWW*) i 443 (*SSL*).

Interfejs modułu drugiego składa się z dwóch pól tekstowych o nazwach „ADRES NADAWCY” i „ADRES ODBIORCY”, dwóch pól jednokrotnego wyboru o nazwach „ODRZUCONE” i „PRZEPUSZCZONE”, czterech pól wielokrotnego wyboru o nazwach „PORT FTP”, „PORT TELNET”, „PORT WWW”, „PORT SSL”. Po uruchomieniu modułu drugiego pola wielokrotnego wyboru są nieaktywne. Zaznaczenie któregoś z pól jednokrotnego wyboru powoduje uaktywnienie wszystkich pól wielokrotnego wyboru. Interfejs modułu drugiego zawiera także pole zobrazowania wyniku i dwa przyciski opisane jako „SPRAWDŹ” i „WYJŚCIE”.



Rys. 6. Interfejs modułu drugiego

Pola tekstowe, opisane jako „ADRES NADAWCY" i „ADRES ODBIORCY" służą do wpisywania adresów IP komputera wysyłającego pakiet i adresu IP komputera odbierającego pakiet. Wypełnienie tych pól nie jest konieczne. Jeśli pozostaną puste, wyniki będą dotyczyć wszystkich adresów IP.

Pola jednokrotnego wyboru opisane jako „PRZEPUSZCZONE" i „ODRZUCONE" określają, czy poszukiwane pakiety zostały zaakceptowane przez listy dostępu, czy też nie. Zaznaczenie któregoś z tych pól umożliwia wybór portu.

Pola wielokrotnego wyboru opisane jako „PORT FTP", „PORT TELNET", „PORT WWW", „PORT SSL" pozwalają użytkownikowi wybrać numer interesującego go portu. Można wybrać więcej niż jedną opcję. W takiej sytuacji wyświetlony wynik będzie dotyczył wszystkich zaznaczonych portów.

Przycisk opisany jako „WYJŚCIE" jest żądaniem zakończenia pracy modułu drugiego.

Przycisk opisany jako „SPRAWDŹ" powoduje przeszukanie pliku dziennika pod kątem zaznaczonych przez użytkownika opcji i wyświetlenie wyników w opisanym polu na interfejsie modułu drugiego. Jako wynik operacji przeszukania pliku dziennika zostaje zwrócona liczba pakietów odpowiadająca zaznaczonym przez użytkownika opcjom. Poszukiwane linie są podobne do linii poszukiwanych przez moduł pierwszy. Różnicą jest jedynie numer portu, na

który kierowany jest pakiet. Przykładowe linie poszukiwane przez moduł drugi wyglądają następująco:

- dla portu 21 (*FTP*):

„*2003-02-21 16:56:17 Local7.Info 131.108.110.1 265: 01:23:25: %SEC-6-IPACCESSLOGP: list 101 permitted tcp 131.108.140.2(1038) -> 131.108.110.2(21), 1 packet*”,

- dla portu 23 (*TELNET*):

„*2003-02-21 16:55:59 Local7.Info 131.108.110.1 264: 01:23:07: %SEC-6-IPACCESSLOGP: list 101 permitted tcp 131.108.140.2(1037) -> 131.108.110.2(23), 1 packet*”,

- dla portu 80 (*WWW*):

„*2003-02-21 16:56:33 Local7.Info 131.108.110.1 267: 01:23:41: %SEC-6-IPACCESSLOGP: list 101 permitted tcp 131.108.140.2(1040) -> 131.108.110.2(80), 1 packet*”,

- dla portu 443 (*SSL*):

„*2003-02-21 16:56:26 Local7.Info 131.108.110.1 266: 01:23:34: %SEC-6-IPACCESSLOGP: list 101 permitted tcp 131.108.140.2(1039) -> 131.108.110.2(443), 1 packet*”.

Przeszukiwanie pliku dziennika odbywa się w identyczny sposób jak w przypadku modułu pierwszego. Różnica polega na tym, że po odczytaniu adresu odbiorcy pobierany jest także ciąg opisujący numer portu przeznaczenia pakietu. Jeśli odczytana linia, tzn. ewentualne adresy nadawcy i odbiorcy, numer portu docelowego i informacja dotycząca odrzucenia bądź przepuszczenia pakietu, zgadzają się z opcjami zaznaczonymi przez użytkownika, ilość pakietów danego typu zostaje zsumowana i wyświetlona w polu wyniku modułu drugiego.

6. Podsumowanie

W artykule została przedstawiona propozycja rozwiązania programowo-sprzętowego ochrony lokalnej sieci komputerowej przed niechcianymi pakietami pochodzącymi z innych sieci.

W efekcie realizacji zamierzonych zadań zbudowano sieć testową, w której wykorzystano dwa routery CISCO, ustalono zasady filtrowania pakietów, na jednym z routerów skonfigurowano mechanizm monitorujący jego

działanie oraz stworzono aplikacje wspomagającą pracę administratora sieci o nazwie „Statystyki".

Jako mechanizm monitorujący pracę routera wybrano mechanizm *syslog*, który skonfigurowano tak, aby wysyłał informacje do komputera znajdującego się w jednej z podsieci. Na tym komputerze osadzono darmowe oprogramowanie – „*Kiwi Syslog Demon*", będące serwerem raportującym dla mechanizmu *syslog*. Po otrzymaniu informacji z routera wspomniany program zapisuje go do pliku dziennika.

Opracowana aplikacja o nazwie „Statystyki" odczytuje dane zapisywane w pliku dziennika i na ich podstawie formułuje istotne informacje dotyczące pracy routera, jak również przesyłanych przez router pakietów. Wybrane informacje są wyświetlane na interfejsie aplikacji wspomagającej pracę administratora sieci.

Zbudowany system ochrony sieci lokalnej przeszedł pomyślnie testy zarówno pod kątem zabezpieczenia chronionej sieci, jak i monitorowania oraz informowania o zdarzeniach mających miejsce w zaporze ogniowej. Można mieć nadzieję, że aplikacja „Statystyki" będzie stanowić cenne narzędzie ułatwiając monitorowanie zdarzeń na routerze Cisco z uruchomionymi funkcjami filtrowania pakietów.

Literatura:

[1] S. Garfinkel, G. Spafford, *Bezpieczeństwo w Unixie i Internecie*, Wydawnictwo RM 1997.

[2] *Akademia Sieci CISCO – pierwszy rok nauki* , MIKOM 2001.

[3] *Akademia Sieci CISCO – drugi rok nauki*, MIKOM 2001.

[4] Merike Keao, *Tworzenie bezpiecznych sieci*, MIKOM 2000.

[5] Elizabeth D. Zwicky, *Internet Firewalls – tworzenie zapór ogniowych*.

[6] Waldemar Pierścionek, Piotr Zejer, *Listy dostępu*, PC Kurier nr 19, 2001.

[7] L. Chappell, *Konfiguracja routerów Cisco: zaawansowane możliwości,* MIKOM 2001.

[8] Marek Kwiatkowski, „*Projekt systemu ochrony sieci lokalnej zbudowanego z wykorzystaniem routerów Cisco*" – praca magisterska. Biblioteka Wojskowej Akademii Technicznej.

Recenzent: prof. dr hab. inż. Marian Chudy

Praca wpłynęła do redakcji 20.09.2003