ANALYSIS OF NETWORK TRAFFIC FILTERING

ANALIZA FILTRACJI RUCHU SIECIOWEGO

Piotr Kabala, Dariusz Laskowski,

Wojskowa Akademia Techniczna

e-mail: dlaskowski@wat.edu.pl

Abstract: The article consist of study on concept of Network Obstacle (firewall, FW) using PLD-Linux platform and available tools, implementation selected mechanism of security, also analysis the effectiveness of prepared Network Obstacle. Study on concept of Network Obstacle is based on Screened Subnet architecture. Testing effectiveness of network Obstacle was found in two fundamental parts. In the first part was examining the security of network obstacle, testing the resistance attempts of scanning port and the most common attacks. The second part of the research meant to show the influence of the Network Obstacle on time and delay of the realization of transaction for HTTP movement depending on level of the security and movement intensity generated by internal network users. Testing the effectiveness of FW was verify by testing the resistance in an attempt of scanning ports and attacks refusal of service (ICMP, SYN Flood), providing base of dispersed attacks DDoS. This part of the research had one aim, to show the influence FW on time and on delay of the realization the transaction for motion HTTP, depending on the security level and intensity of movement generated by the users of the internal network.

Keywords: network traffic, web filtering, protocol IP, firewall

Streszczenie: Artykuł przedstawia badania koncepcji Platformy Sieciowej z zaporą Linux PLD wykorzystującą dostępne narzędzia analizy ruchu, implementację wybranego mechanizmu bezpieczeństwa oraz analizę efektywności przygotowanej Zapory Sieciowej (FW). Badania oparto na architekturze ekranowanych podsięci. Testowanie skuteczności zapory wykonano w dwóch etapach. W pierwszej części sprawdzono bezpieczeństwo poprzez testowanie odporności na próby skanowania portów i najczęstsze typy ataku. Druga część badań miała na celu pokazanie wpływu zapory na czas i opóźnienie realizacji transakcji dla ruchu HTTP w zależności od poziomu bezpieczeństwa i natężenia ruchu generowanego przez użytkowników sieci wewnętrznej. Sprawdzenie skuteczność FW zostało zweryfikowane przez badania odporności w próbie skanowania portów i ataków odmowy usługi (tj. SYN Flood i ICMP) zapewniając bazę rozproszonych ataków typu DDoS. Ta część badań miała jeden cel, którym było pokazanie wpływu FW na czas i opóźnienia realizacji transakcji dla ruchu HTTP, w zależności od poziomu bezpieczeństwa i intensywności ruchu generowanego przez użytkowników sieci.

Słowa kluczowe: ruch sieciowy, filtrowanie sieci, protokół IP, zaporę sieciową

1. Wstęp

W dzisiejszych czasach bezpieczeństwo sieci teleinformatycznych ma niebagatelny wpływ na funkcjonowanie wielu organizacji, przedsiębiorstw, służb administracji państwowej i samorządowej oraz służb mundurowych. Coraz częściej sieci zapewniają przesyłanie i przechowywanie w swoich zasobach licznych danych, do których nieautoryzowany dostęp miałby destrukcyjny wpływ na prestiż i stabilność funkcjonowania organizacji. Stale „rośnie” szkodliwe oddziaływanie destruktorów na posiadane zasoby. W związku z tym, konieczne stało się stosowanie mechanizmów i narzędzi utrzymania wymaganego poziomu bezpieczeństwa sieci teleinformatycznych [1,2].

Podstawowym narzędziem bezpieczeństwa umieszczonym na granicy między domenami sieci publicznej i prywatnej organizacji jest Zapora Sieciowa (ang. *firewall*, FW), analizująca strumień pakietów IP (ang. *Internet Protocol*), będąca urządzeniem lub programem. Alternatywą dla komercyjnych produktów są open source’owe rozwiązania FW oparte o systemy klasy Unix i narzędzia pozwalające na dowolność projektowania i dynamiczne skalowanie własności funkcjonalnych pod kątem optymalnego wykorzystania posiadanego potencjału (tj. urządzenia, oprogramowania) adekwatnie do uwarunkowań ruchu sieciowego IP i specyfiki otaczającego środowiska telekomunikacyjnego.

Realizacja dedykowanej Zapory Sieciowej wymaga wyboru platformy systemowej i narzędzi projektowania [3]. W przypadku sieciowych systemów operacyjnych często stosuje się rozwiązania komercyjne rodziny (tj. Windows firmy Microsoft) lub open source’owe - Unix (Linux). Ze względu na fakt, iż występują między nimi różnice zarówno w architekturze systemu jak i poziomie bezpieczeństwa, należy rozważyć te kwestie przed wyborem odpowiedniego systemu operacyjnego, jako platformy do projektu programowej Zapory Sieciowej [4].

2. Metody destrukcyjnego oddziaływania w sieci IP

Sieci teleinformatyczne, wykorzystujące stos protokołów TCP (ang. *Transmission Control Protocol*) / IP (ang. *Internet Protocol*), wspomagają organizacje w realizacji ich zadań statutowych. Przesyłane informacje wymagają zachowania pożądanego poziomu poufności dla „danych wrażliwych” tak, aby uniemożliwić nieupoważnionym osobom do nich dostęp. Poniższa tabela (Tabela 1) zestawia najczęstsze metody ataków na sieci TCP / IP [4].

Dlatego też istnieją sieciowe mechanizmy bezpieczeństwa, które można sklasyfikować do jednego z dwóch zbiorów tj.: monitorujące transmisję danych i nadzorujące dostęp do sieci.

Tabela 1. Metody ataków na systemy komputerowe

Metoda ataku	Opis ataku	Sposób obrony	Funkcja FW
Wykorzystanie „dziur” w programach	Metoda wykorzystuje „luki” w działaniu, czy też brak mechanizmów bezpieczeństwa aplikacji lub usług uruchomionych w systemie operacyjnym.	Wyłączenie wszelkich podatnych na atak usług, czy też aplikacji lub zastosowanie „łat” poprawiających bezpieczeństwo.	Nie są w stanie zabezpieczyć sieci przed tego typu atakiem.
Nieautoryzowany dostęp	Korzystanie z usług przez osoby do tego nieuprawnione.	Precyzyjne określenie uprawnień do udostępnianych w sieci usług.	Potrafia znacznie ograniczyć tego typu atak wykorzystując odpowiednie reguły filtrowania pakietów na podstawie określonego wzorca.
Blokowanie Usługi (atak DDoS)	Atak powoduje zaprzestanie działania usługi, czy też aplikacji lub uniemożliwienie korzystania poprzez jej przeciążenie.	Odrzucanie złośliwych pakietów lub podejrzanych poleceń i żądań.	Umożliwiają obronę przed tą metodą np. wykorzystując filtrowanie z analizą stanu połączeń.
Podszywanie się	Metoda polega na naśladowaniu autentycznego hosta, przesyłając spreparowane pakiety ze sfałszowanym adresem źródłowym IP.	Sprawdzanie integralności i wiarygodności przesyłanych pakietów, wprowadzenie nieprzewidywalności do mechanizmu kontroli połączenia (m.in. losowe porty i numery TCP).	Umożliwiają realizację bezpiecznej transmisji danych.
Podsluchiwanie	Metoda polega na nasłuchiowaniu przez atakującego komunikacji sieciowej nienależącej do niego.	Stosowanie mechanizmów szyfrowania danych (np. IPSec, SSL), detekcja skanowania portów i sniferów.	Zapory Sieciowe umożliwiają realizację bezpiecznej transmisji danych.

W nomenklaturze sieciowej, Zapora Sieciowa jest narzędziem monitorującym i odpowiada za ochronę terminali (hostów) domeny sieci znajdujących się za FW (tj. w sieci prywatnej) przed przesyłaniem nieautoryzowanych danych (Rys. 1).

Rys. 1 Schemat stanowiska testowego

Zapory Sieciowe funkcjonują przede wszystkim w warstwie sieciowej i transportowej modelu odniesienia łączenia systemów otwartych OSI ISO RM (ang. *Open System Interconnection International Organization for Standardization Reference Model*) standardu zdefiniowanego zarówno przez ISO jak i ITU-T (ang. *International Telecommunication Union - Telecommunication Standardization Sector*). FW to także specyficzne interfejsy scalające środowiska sieciowe przy zapewnieniu filtracji strumieni danych ruchu IP a w szczególności oferują one:

- Filtrowanie: adresów i portów oraz zawartości.
- Ochronę: trasowanych pakietów, adresów IP.
- Monitorowanie wybranych relacji, raportowanie i prowadzenie statystyk.

Filtrowanie pakietów IP jest podstawowym mechanizmem umożliwiającym podejmowanie decyzji, które pakiety IP muszą być odrzucone. Statyczna metoda filtrowania pakietów (ang. *state less packet filtering*) umożliwia kontrolowanie przepływu pakietów na podstawie [5]:

- adresu IP źródłowego i docelowego zawartego w nagłówku pakietu;
- typu protokołu transportowego (TCP, UDP, ICMP) i numeru portu nadawcy oraz odbiorcy wykorzystanego do przesyłania danych.

W zależności od ustalonych reguł filtrowania dany ruch jest przepuszczany lub odrzucany. Metoda ta nie dokonuje filtrowania na podstawie zawartości pola danych pakietu. Statyczne filtrowanie pakietów IP jest metodą na tyle prostą i wydajną, że implementowana jest w aplikacjach użytkowych pełniących rolę prostych Zapór Ogniowych, a także w urządzeniach sieciowych (np. routerach w postaci list kontroli dostępu – list *access control list*, ACL).

Istnieje także metoda dynamicznego filtrowania pakietów IP umożliwiająca budowanie reguł filtrowania z wykorzystaniem mechanizmu śledzenia połączeń (ang. *connection tracking*) [7] pozwalającego na analizowanie stanu połączeń TCP przechodzących przez Zaporę Sieciową.

Dynamiczne filtrowanie pakietów IP wykorzystywane jest w tzw. filtrach pakietów z badaniem stanu (ang. *state full packet filtering*). Na podstawie informacji zawartych w nagłówkach pakietów (rodzaju protokołu warstwy transportowej oraz flagi połączenia), mechanizm jest w stanie określić stan danego połączenia. W związku z tym, Zapora Sieciowa utrzymuje bazę danych, w której gromadzone są dane dotyczące każdego z połączeń (m.in. adres źródłowy i docelowy, port źródłowy i docelowy, numery sekwencyjne, flagi i czas bezczynności). Informacje te przechowywane są w postaci wpisów w tzw. tablicy połączeń (ang. *connection table*). Zasadę filtrowania z wykorzystaniem analizy stanu połączeń przedstawia rysunek (Rys 2).

Rys. 2 Filtrowanie z wykorzystaniem analizy stanu połączeń [6]

Z tablicą połączeń związane są określone liczniki, które np. ustalają limit czasu bezczynności zapisanego w tabeli połączenia. Na podstawie przynależności przetwarzanych pakietów do zapisanego połączenia następuje ich przekazywanie lub odrzucenie. Podstawowa zasada obowiązująca podczas filtrowania pakietów z analizą stanu połączeń polega na tym, że pakiety przychodzące z sieci publicznej do sieci prywatnej muszą stanowić część wcześniej utworzonego strumienia danych [7].

3. Koncepcja Zapory Sieciowej z wykorzystaniem platformy Linux

Podstawowym zadaniem projektowanego produktu - FW - jest oddzielenie sieci prywatnej od sieci publicznej (np. Internetu). Użytkownicy sieci chronionej korzystają z zasobów sieci publicznej i wykorzystują lokalne serwery usług: przeglądania stron WWW (ang. *World Wide Web*), przesyłania plików FTP (ang. *File Transfer Protocol*). Ponadto zakłada się, iż sieć chroniona jest siecią bezpieczną tzn. jej użytkownicy nie stanowią źródła ataków.

Niniejsza koncepcja bazuje na systemie klasy Unix - Linux PLD z jądrem (co najmniej) 2.6 ze względu na jego wystarczający poziom bezpieczeństwa, niewielkie wymagania sprzętowe na moc obliczeniową i posiadanie znacznej liczby funkcji programowych umożliwiających zbudowanie efektywnej FW. Ponadto, zakłada się, że środowisko testowe odzwierciedli rzeczywiste relacje występujące w powszechnie eksploatowanych sieciach, wykorzystując (Rys. 3) [8-10]:

- Klasyczną topologię FW - filtr pakietów z pośredniczącym serwerem Proxy.
- Protokoły TCP i IPv4 (odpowiednio w warstwie IV i III modelu OSI ISO RM).
- Architektury *Screened Subnet* pozwalającej na wydzielenie z domeny określonego segmentu sieci (strefy zdemilitaryzowanej, DMZ) z serwerem usług.

Rys. 3 Ogólna architektura Zapory Sieciowej

Zasadniczymi komponentami architektury są routery nadzorujące dostęp do zasobów sieci umieszczony na granicy między siecią publiczną a strefą DMZ oraz router lokalny zlokalizowany między strefą DMZ a siecią prywatną, tj. [11,12]:

1) Router dostępowy:

- Filtrowanie pakietów z analizą stanu połączeń.
- Kontrola dostępu użytkowników sieci publicznej do zasobów DMZ.
- Obrona sieci wewnętrznej przed atakami (DoS, skanowanie portów).
- Translacja adresów i portów z wykorzystaniem mechanizmu NAT (ang. *Network Address Translation*) i PAT (ang. *Port Address Translation*).
- Pełnienie funkcji bramy SSL VPN (ang. *Secure Sockets Layer Virtual Private Network*).

2) Router wewnętrzny:

- Filtrowanie pakietów z analizą stanu połączeń.
- Kontrola dostępu użytkowników sieci prywatnej do zasobów strefy DMZ i sieci publicznej na podstawie adresów MAC.
- Pełnienie funkcji pośredniczącego serwera Proxy dla usługi WWW.

Budowę strefy DMZ oparto o zarządzany przełącznik umożliwiający przydzielanie poszczególnych jego portów do konkretnych sieci VLAN (ang. *Virtual Local Area Network*). Ze względu na fakt, iż zarówno router dostępowy jak i router wewnętrzny wymagają dostępu do różnych sieci VLAN w strefie DMZ, przyłączono je do przełącznika przez port trunkingowy (ang. *trunking port*) wykorzystujący, co najmniej standard enkapsulacji 802.1q. Enkapsulacja 802.1q polega na określaniu przynależności ramek typu Ethernet do określonych sieci VLAN – tzw. tagowaniu.

W tym celu, do każdej ramki dodawane jest dwubajtowe pole TCI (ang. *Tag Control Information*) zawierające pole VID (*VLAN ID*) i określające, do której sieci VLAN należy dana ramka. Aby umożliwić komunikację routerów Zapory Sieciowej z poszczególnymi sieciami VLAN konieczne jest utworzenie logicznych podinterfejsów (ang. *subinterfaces*) należących do określonych sieci VLAN na pojedynczym, fizycznym interfejsie sieciowym. Ponadto, komunikacja pomiędzy sieciami VLAN może odbywać się jedynie poprzez router obsługujący standard 802.1q. Rozwiązanie strefy DMZ w oparciu o sieci VLAN posiada wiele zalet. Najważniejsze z nich to [13]:

- możliwość tworzenia wielu podsieci z wykorzystaniem pojedynczego przełącznika,
- możliwość separacji stacji w strefie DMZ,
- możliwość kontroli dostępu i filtracji ruchu do poszczególnych sieci VLAN, gdyż całkowity ruch przechodzi przez router,
- kontrolowanie ruchu pomiędzy poszczególnymi sieciami VLAN,
- wysoka skalowalność strefy DMZ.

Konfigurację reguł filtrowania w routerze dostępowym i lokalnym zrealizowano z wykorzystaniem opracowanego w języku *Bash* skryptu uruchomieniowego. Skrypt *Bash* zorganizowany został w zbiór plików przechowywanych w katalogu */etc/firewall*. Wykorzystywany jest on do zautomatyzowania procesu odtwarzania konfiguracji Zapory Sieciowej np. w sytuacji restartu systemu operacyjnego (Rys. 4).

Rys. 4 Struktura katalogu */etc/firewall*

4. Badanie efektywność filtracji ruchu sieciowego IP

Przeprowadzenie wiarygodnych testów sprawdzających poprawność zaprojektowanej Zapory Sieciowej postanowiono dokonać w specjalizowanym środowisku badawczym (test bed'zie) z wykorzystaniem popularnych technik i technologii stosowanych w sieciach teleinformatycznych o architekturze przedstawionej na rysunku (Rys. 5).

Rys. 5 Architektura sieci testowej

W ramach niniejszej koncepcji Zapory Sieciowej strefę DMZ oparto na wirtualnych lokalnych sieciach komputerowych VLAN:

- VLAN 10 wykorzystano do przesyłania ruchu między routerami, dzięki czemu zapewniono komunikację użytkowników sieci chronionej z publiczną.
- VLAN 20 zapewnia dostęp użytkownikom sieci publicznej do serwera WWW i ftp.
- VLAN 30 oferuje komunikację autoryzowanym użytkownikom zdalnym z siecią publiczną i dostęp do serwerów poczty SMTP (ang. *Simple Mail Transfer Protocol*) /POP3 (ang. *Post Office Protocol 3*) i lokalnego serwera nazw DNS (ang. *Domain Name System*). Ponadto, dostęp do tych sieci posiadają użytkownicy sieci prywatnej.

Jako przełącznik w strefie DMZ wykorzystano urządzenie Catalyst firmy Cisco wyposażone w 24 interfejsy FastEthernet. Jego funkcjonalność pozwala na przywiązanie fizycznych portów do określonych sieci VLAN. Dwa porty VLAN wykorzystano, jako porty trunking'owe, do których przyłączono routery Zapory Sieciowej (Port Fa0/1 i Fa0/2). Do VLAN'u 20 przywiązano porty Fa0/4 i Fa0/5 a do VLAN'u 30 - porty Fa0/6 i Fa0/7. Aby Zapora Sieciowa w architekturze *Screened Subnet* funkcjonowała prawidłowo niezbędne było wykonanie trasowania pomiędzy poszczególnymi podsieciami. W opracowanej koncepcji wykorzystano routing statyczny ze względu na niezmiennosc tras. Ponadto, tego typu trasowanie nie obciąża routerów oraz sieci pakietami związanymi z rozgłaszaniem tras. Tabela 2 zawiera informacje dotyczące tras statycznych wprowadzonych w urządzeniach sieci testowej poza trasami bezpośrednio przyłączonymi do interfejsów.

Ze względu na fakt, iż użytkownicy sieci prywatnej wymagają dostępu do sieci publicznej, należało w routerach dostępowym i wewnętrznym ustalić trasę domyślnej bramy (ang. *default gateway*). Trasę taką skonfigurowano również w serwerach usług, do których jest wymagany dostęp z sieci publicznej. Ponadto, w routerze dostępowym i serwerach usług ustawiono trasę do sieci prywatnej (192.168.100.0/24).

Tabela 2. Trasy routing 'u w poszczególnych urządzeniach sieciowych

	Sieć docelowa	Maska	Brama lub interfejs wyjściowy
Router dostępowy	0.0.0.0	0.0.0.0	Interfejs zewnętrzny
	192.168.100.0	255.255.255.0	192.168.10.2
Router wewnętrzny	0.0.0.0	0.0.0.0	192.168.10.1
Serwery usług	192.168.100.0	255.255.255.0	192.168.20.2 (VLAN 20) 192.168.30.2 (VLAN 30)
	0.0.0.0	0.0.0.0	192.168.20.1 (VLAN 20) 192.168.30.1 (VLAN 30)

Koncepcja Zapory Sieciowej pozwala realizować połączenia VPN z sieci publicznej do strefy DMZ w celu zapewnienia bezpiecznego dostępu do jej zasobów. Funkcję bramy VPN pełni router dostępowy zapewniając komunikację VPN typu *client-to-site* z wykorzystaniem tuneli SSL VPN. Rozwiązanie to zostało wprowadzone w celu umożliwienia prowadzenia na odległość działań administracyjnych, a także umożliwienia użytkownikom zdalnym bezpiecznego dostępu do serwerów WWW, FTP oraz SMTP/POP3. W związku z tym, zdefiniowano dwie grupy dostępowe: grupa administratorów oraz grupa użytkowników zdalnych. Dla każdej z grup wydzielono tunel SSL VPN, na podstawie którego definiowany jest dostęp do określonych usług. Każdy z użytkowników nawiązujący połączenie przez tunel SSL/VPN musi zostać uwierzytelniony przez bramę VPN. Brama VPN nasłuchuje połączeń na oddzielnych portach dla każdego z tuneli. W koncepcji Zapory wykorzystano oprogramowanie OpenVPN, które udostępnia dwie metody uwierzytelniania użytkowników i szyfrowania komunikacji:

- mechanizm współdzielonego klucza (ang. *pre-shared key*) – strony połączenia współdzielą między sobą tajny klucz. Rozwiązanie proste w konfiguracji, stosowane w przypadku łączenia podsieci.
- z wykorzystaniem certyfikatów cyfrowych SSL X.509 – rozwiązanie stosowane do tworzenia zdalnego dostępu dla użytkowników. Dzięki właściwościom SSL/PKI istnieje możliwość wystawiania certyfikatów na określony czas, unieważniania ich oraz określania dostępu na podstawie właściciela certyfikatu.

Metoda ta została wykorzystana w niniejszej koncepcji Zapory Sieciowej.

Tego rodzaju topologia FW pozwala zestawiać poufne tunele SSL (ang. *Secure Socket Layer*), w ramach wirtualnych sieci prywatnych VPN (ang. *Virtual Private Network*), z sieci publicznej do strefy DMZ. Funkcję bramy VPN pełni router dostępowy zapewniając komunikację VPN typu *client-to-site* z wykorzystaniem tuneli SSL VPN. Rozwiązanie to zostało wprowadzone w celu umożliwienia prowadzenia na odległość działań administracyjnych, a także umożliwienia użytkownikom zdalnym dostępu do serwerów WWW, ftp oraz SMTP/POP3. Dla każdej z grup wydzielono tunel SSL VPN dostępu do usług po pozytywnym uwierzytelnieniu przez bramę VPN monitorującą strumienie danych na zdefiniowanych, dla każdego z tuneli, portach (Rys. 6).

Rys. 6 Realizacja połączeń SSL VPN w sieci testowej

Sieć prywatna oraz strefa DMZ oparte są na technologii FastEthernet z algorytmem dostępu CSMA/CD. Ruch generowany w sieci prywatnej dotyczy głównie usług: WWW, FTP oraz e-mail. W strefie DMZ zlokalizowano cztery serwery usług: WWW, FTP, SMTP/POP3 oraz lokalny serwer DNS. Użytkownicy sieci publicznej mają możliwość nawiązywania wyłącznie ustalonych połączeń TCP do zasobów sieci VLAN 20, w której zlokalizowane są serwery WWW i FTP. Dostęp użytkowników sieci prywatnej do zasobów strefy DMZ i sieci publicznej weryfikowany jest na podstawie adresu MAC. Użytkownicy, których powiązanie adresu MAC i IP nie istnieje w bazie danych routera wewnętrznego, nie są dopuszczani do ruchu poza sieć prywatną. Domyślną polityką traktowania pakietów przez routery Zapory Sieciowej jest *DROP*, zatem pakiety nie pasujące do reguł filtrowania są odrzucane (wszystko, co nie jest jawnie dopuszczone, jest odrzucone).

Pozostałymi składowymi *test bedu* były:

- 1) Oprogramowanie OpenVPN zapewniające uwierzytelnianie użytkowników i szyfrowania transportu danych przez:
 - mechanizm współdzielonego klucza tajnego (ang. *pre-shared key*) to klasyczne rozwiązanie proste w konfiguracji i stosowane w przypadku łączenia podsieci,
 - certyfikaty cyfrowe SSL X.509 stosowane przy zdalnym dostępie.
- 2) Generator ruchu i usług sieciowych (Hping2) i analizator ruchu IP (Wireshark).
- 3) Open-source'owe narzędzie do eksploracji sieci i audytów bezpieczeństwa (Nmap).

Scenariusze badawcze obejmowały analizę przepływu danych realizowaną w ramach:

- 1) Usług sieciowych dla 3-ech wariantów łańcucha funkcjonalnego (Rys. 7) dla 3-ech poziomów bezpieczeństwa (PB1 - bez FW, PB2 - z FW, PB3 – FW i serwer proxy).

Rys. 7 Filtrowanie ruchu

Router dostępowy zezwala na następujący ruch:

- VLAN 10: ruch związany z nowymi połączeniami z sieci prywatnej oraz ruch do sieci prywatnej należący wyłącznie do nawiązanych połączeń, a także ruch ICMP. Pozostały ruch jest blokowany;
- VLAN 20: dla sieci publicznej - dostęp protokołem HTTP/HTTPS do serwera WWW (port TCP/80 i TCP/443), ruch do serwera FTP (port TCP/21), ruch należący do nawiązanych połączeń TCP i UDP, a także ruch ICMP. Pozostały ruch jest blokowany;
- VLAN 30: dla sieci publicznej ruch od/do lokalnego serwera poczty wychodzącej SMTP (port TCP/25 i TCP/465), ruch pakietów *DNS Query* (UDP/53) pomiędzy serwerem DNS, a siecią publiczną oraz pakietów *DNS Zone Transfer* (TCP/53) z serwera *dns.tpsa.pl* (194.204.159.1) w Internecie. Serwer ten pełni funkcję *secondary DNS servera* dla sieci prywatnej. Dopuszcza się również ruch ICMP;
- połączenia na portach UDP/17003 i UDP/17004 wykorzystywanych przez aplikację bramy VPN (pakiety należące do tuneli VPN są szyfrowane i enkapsulowane w pakiety UDP przez aplikację OpenVPN);
- dla zdalnych administratorów sieci zezwala się na dostęp do routerów poprzez zdalny terminal z wykorzystaniem protokołu SSH (port TCP/22);
- dla użytkowników zdalnych zezwala się na dostęp do lokalnych serwerów usług WWW, FTP, SMTP/POP3 wyłącznie na portach, na których one pracują;

Router wewnętrzny zezwala na następujący ruch:

- VLAN 10: ruch TCP, UDP od wyłącznie uprawnionych użytkowników sieci (filtrowanie na podstawie MAC) oraz ruch należący do nawiązanych połączeń. Router blokuje ruch do sieci p2p (ang. *peer-to-peer*), które stanowią „zapychacze” pasma łącza internetowego;
 - VLAN 20: dostęp protokołem HTTP/HTTPS do serwera WWW (port TCP/80 i TCP/443), ruch do serwera FTP (port TCP/21);
 - VLAN 30: ruch pakietów *DNS Query* (UDP/53) od/do serwera nazw DNS, ruch od serwera poczty wychodzącej SMTP (port TCP/25 i TCP/465) do sieci LAN, ruch do serwera poczty przychodzącej POP3 (port TCP/110 i TCP/995) z sieci LAN;
 - ruch WWW do sieci publicznej jest kierowany do pośredniczącego serwera Proxy, który realizuje funkcję filtra zawartości;
 - dla administratorów sieci zezwala się na dostęp do routera wewnętrznego poprzez zdalny terminal z wykorzystaniem protokołu SSH (port TCP/22);
- 2) Badań odporności sieci TCP/IPv4 na wybrane działanie destrukcyjne (ataki) dokonano na wielu wariantach (przykład *test bedu* - Rys. 8).

Rys. 8 Schemat sieci do testowania odporności na wybrane rodzaje ataków

- 3) Pomiarów wydajnościowych dla usługi przeglądania stron WWW wykonano z wykorzystaniem aplikacji ApacheBench i zaleceń IETF [4, 12, 13] (przykład *test bedu* - Rys. 9).

Rys. 9 Ważniejsze komponenty *test bedu* dla testów wydajnościowych

Ważniejsze elementy konfiguracyjne to:

1) *Firewall.conf*:

```
IPTABLES="/usr/sbin/iptables"
MODPROBE="/sbin/modprobe"
# Przestrzeń adresowa sieci prywatnej
EXT_NET="171.16.31.0/24"
EXT_DEV_ADDR_1="171.16.31.1"
# Interfejsy fizyczne
INT_DEV="eth0"
EXT_DEV="eth1"
VLAN_10_DEV="eth0.10"
```

2) *Firewall.nat*:

```
$IPTABLES -t nat -A POSTROUTING -o $EXT_DEV -s 192.168.0.0/16 -j
SNAT--to-source $EXT_DEV_ADDR_1
$IPTABLES -t nat -A PREROUTING -i $EXT_DEV -d $EXT_DEV_ADDR_2
-j DNAT--to-destination 192.168.20.10
$IPTABLES -t nat -A PREROUTING -p tcp -i $EXT_DEV -d
$EXT_DEV_ADDR_1 -m multiport --dports 25,465 -j DNAT --to-destination
192.168.30.10
$IPTABLES -t nat -A PREROUTING -p tcp -i $EXT_DEV -d
$EXT_DEV_ADDR_1 --dport 53
-j DNAT --to-destination 192.168.30.100
```

3) *Firewall.vpn*:

```
$IPTABLES -t filter -N VPN
$IPTABLES -t filter -A FORWARD -i tun+ -j VPN
$IPTABLES -t filter -A VPN -m state --state ESTABLISHED,RELATED -j
ACCEPT
$IPTABLES -t filter -A VPN -i tun0 -s 192.168.50.0/24 -d 192.168.10.0/24 -m
multiport -p tcp --dports 22 -m state --state NEW -j ACCEPT
$IPTABLES -t filter -A VPN -i tun+ -d 192.168.30.100 -p udp --dport 53 -j
ACCEPT
$IPTABLES -t filter -A VPN -i tun1 -s 192.168.60.0/24 -d 192.168.30.10 -m
multiport -p tcp --dports 25,110,465,995 -m state --state NEW -j ACCEPT
$IPTABLES -t filter -A VPN -p icmp -j ACCEPT
$IPTABLES -t filter -A VPN -j DROP
```

5. Wyniki badań

Efektywność Zapory Sieciowej sprawdzono testując, w pierwszej kolejności, jej odporność na próby skanowania portów i najczęściej wykorzystywane ataki odmowy usługi (ICMP i SYN Flood), stanowiące podstawę rozproszonych ataków DDoS. Drugą część badań ukierunkowano na identyfikację i zobrazowanie wpływu FW na parametry ruchu sieciowego, czyli na wartość czasu i opóźnienia realizacji transakcji dla ruchu HTTP w zależności od poziomu bezpieczeństwa (PB-1...3) i natężenia ruchu generowanego przez użytkowników sieci wewnętrznej (pakiety 50 i 200kB). Pomiar wydajności usługi WWW zrealizowano dla trzech poziomów bezpieczeństwa FW, których opis przedstawia tabela (Tabela 3).

Tabela 3. Poziomy bezpieczeństwa Zapory Sieciowej

Oznaczenie	Poziom bezpieczeństwa
Poziom 1	Wyłączona Zapora Sieciowa
Poziom 2	Włączona Zapora Sieciowa bez serwera Proxy WWW
Poziom 3	Włączona Zapora Sieciowa oraz serwer Proxy WWW

Przykładowe wyniki realizowanych pomiarów zaprezentowano graficznie w postaci rezultatów:

- 1) Testu mechanizmu obrony sieci przed atakami ICMP Flood (Rys. 10 i Rys. 11).
Test pozwolił wykazać, iż atak ICMP Flood bez uruchomionego mechanizmu spowodował degradację przepływności do ok. 7Mb/s. W przypadku ataku rozproszonego nastąpiło całkowite wysycenie łącza, co kompletnie uniemożliwiło realizację usługi.

— Chwilowy przepływ ruchu ftp podczas ataku ICMP Flood o natężeniu 1000pps
— Chwilowy przepływ ruchu ftp podczas ataku ICMP Flood o natężeniu 5x1000pps

Rys. 10 Przepływ ruchu FTP podczas ataku ICMP Flood przy wyłączonym FW

Kolejny test zrealizowano w identycznych warunkach sieciowych z tym, że uruchomiono mechanizm *Netfilter* limitujący ruch *ICMP Echo Request* (Rys. 10).

Rys. 11 Flow of the movement FTP during ICMP Flood attacks in function of time

W efekcie zaobserwowano znaczną poprawę przepływności w stosunku do poprzedniego eksperymentu. Degradacja ruchu FTP zmalała do ok. 10% w przypadku ataku o natężeniu 1000pps (ang. *packets per second*). Nawet przeprowadzenie ataku rozproszonego nie spowodowało wysycenia łącza, choć przepływność do ok. 3,5Mb/s.

- 2) Pomiaru i wyznaczenia wartości średnich dla transakcji WWW (http) przy zmiennej liczbie równoczesnych połączeń:

- Czasy realizacji (Rys. 12).
- Czasy opóźnienia (Rys. 13).

Po dokonaniu analizy otrzymanych danych z pomiarów istnieją podstawy do sprecyzowania następujących spostrzeżeń dla przyjętych poziomów bezpieczeństwa:

- PB nr 1: wystąpił proporcjonalny wzrost całkowitego czasu realizacji transakcji WWW przy zwiększaniu natężenia ruchu, co skutkuje utrzymującym się na stałym poziomie średnim opóźnieniem realizacji transakcji dla obu rozmiarów obiektu WWW (dla 50kB średnio 6,8ms, zaś dla 200kB - 23ms). Na wartość tego opóźnienia ma wpływ tzw. opóźnienie na łączy (ang. *serialization delay*) zależne od rozmiaru pakietu oraz przepustowości danego łącza oraz czas przetwarzania pakietów przez router dostępowy i wewnętrzny.

Rys. 12 Wykres średniego czasu realizacji transakcji WWW

Rys. 13 Wykres średniego opóźnienia realizacji transakcji WWW

- PB 2: zaobserwowano blisko (10÷15)% wzrost średniego opóźnienia realizacji transakcji WWW w stosunku do PB 1, co było spowodowane koniecznością przetwarzania przez oba filtry każdego z pakietów w celu znalezienia pasującej reguły filtrowania. Wpływ na wartość opóźnień, w tym przypadku, ma również liczba i kolejność reguł filtrowania uruchomionych w filtrach FW, na co należy zwrócić szczególną uwagę podczas ich konfiguracji. Te parametry natomiast są zależne od zastosowanej domyślnej polityki traktowania pakietów. Podczas implementacji niniejszej koncepcji Zapory Sieciowej starano się tak definiować reguły, aby możliwie zminimalizować czas przeszukiwania reguł filtrowania. Przykładem jest umieszczenie w każdym z łańcuchów filtrowania, jako pierwszej reguły zezwalającej na ruch od już nawiązanych połączeń TCP. Testy wykazały, iż Zapora Sieciowa jest w stanie przenieść ruch WWW od 400 użytkowników jednocześnie z tym, że czasy realizacji transakcji są odpowiednio większe.
- Porównując wyniki badań dla PB1 i 3 widać, iż dodatkowe przetwarzanie pola danych pakietów na poziomie aplikacyjnym realizowanym przez serwer Proxy WWW wprowadza znacznie opóźnienia w realizacji transakcji HTTP. Pomiar wykazały blisko dwukrotny wzrost średniego opóźnienia w stosunku do wariantu realizującego wyłącznie filtrowanie nagłówek pakietów IP [dla 50kb - (16÷20) ms, a dla 200kB -(36÷53) ms]. Różnica ta jest mniejsza w przypadku większych obiektów HTML. Ponadto, zaobserwowano dużo szybszy wzrost czasu transakcji HTTP wraz ze wzrostem liczby jednoczesnych połączeń niż ma to miejsce dla poziomu bezpieczeństwa 1 i 2 Zapory Sieciowej. Szczególnie jest to widoczne, gdy router był zmuszony przetworzyć jednocześnie ruch od znacznej liczby użytkowników (tj. od 400).

Przeprowadzone badania oraz analiza otrzymanych danych wynikowych stały się podstawą do identyfikacji następnych obszarów badawczych z tego zakresu tematycznego. Ważniejszymi z nich jest walidacja, dotrzymania w czasie zbliżonym do rzeczywistego, wymagań w zakresie bezpieczeństwa (tj. poufności) i niezawodności (gotowości technicznej i funkcjonalnej) i jakości (dźwięku i obrazu) w środowisku heterogenicznym systemu antro-po-technicznego. Wybrane aspekty badawcze poddano już fragmentarycznej analizie, a przykładowe wyniki zaprezentowano w publikacjach [14÷18].

6. Wnioski

Meritum opracowania było wykonanie zdecentralizowanej, programowej Zapory Sieciowej z wykorzystaniem dostępnych narzędzi typu open source w architekturze typu *Screened Subnet*. Funkcjonalność FW przebadano z wykorzystaniem adekwatnych do potrzeb dedykowanych mechanizmów bezpieczeństwa tj. filtry pakietów IP z analizą stanów połączeń, serwer Proxy WWW, bramę VPN czy też mechanizmy chroniące sieć prywatną przed destrukcyjnym oddziaływaniem

niepożądanych zagrożeń. Dodatkowo, zrealizowano badania odporności Zapory Sieciowej na skanowanie portów i ataki typu DoS (ICMP Flood, SYN Flood) stanowiące podstawę rozproszonych ataków DDoS, a także sprawdzono wpływ Zapory Sieciowej na czas realizacji transakcji HTTP w test będzie odzwierciedlającym rzeczywiste sieci TCP/IPv4.

Przeprowadzona identyfikacja efektywności FW wykazała jego odporność na współczesne destrukcyjne oddziaływanie. Ponadto FW skutecznie ogranicza możliwości przeprowadzenia ataków ICMP Flood i SYN Flood. Dodatkowo, eksperymenty sprawdzające jej wydajność pozwoliły wykazać różnice czasowe w realizacji transakcji HTTP dla różnych poziomów bezpieczeństwa podczas jednoczesnych połączeń od wielu użytkowników sieci chronionej. Badania udowodniły, iż wzrost liczby przetwarzanych reguł filtrowania przez Zaporę Sieciową, a także dodatkowe przetwarzanie pakietów na poziomie warstwy aplikacji zwiększa opóźnienie realizacji transakcji. Przetwarzanie pakietów przez serwer Proxy WWW zwiększa blisko dwukrotnie opóźnienie i czas realizacji transakcji HTTP. Pomiary pokazały, iż zwiększanie poziomu bezpieczeństwa sieci nie zawsze „idzie w parze” z zwiększeniem jej wydajności w „odczuciu” użytkownika końcowego (abonenta).

7. Literatura

- [1] Laskowski D., Lubkowski, P.: Confidential transportation of data on the technical state of facilities, *Advances in Intelligent Systems and Computing* 286, pp. 313-324, 2014.
- [2] Bajda, A., Laskowski, D., Wrazen M.: Diagnostics the quality of data transfer in the management of crisis situation, *Przegląd Elektrotechniczny* 87 (9 A), pp. 72-78, 2011.
- [3] Bergier B. „Bezpieczeństwo i ochrona danych w sieciach komputerowych opartych o system GNU/LINUX” – praca dyplomowa, 2003.
- [4] Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman: *Building Internet Firewalls – 2nd Edition*, 2000.
- [5] Gouda M. G., Xiang-Yang A. Liu: *Firewall Design: Consistency, Completeness and Compactness*, IEEE, 2004.
- [6] Benjamin H.: *CCIE Security*, Wydawnictwo MIKOM, Warszawa 2004.
- [7] Strony WWW: <http://www.infosecwriters.com>, <http://www.pld-linux.org>, <http://www.openvpn.net>, <http://www.privoxy.org>, <http://www.ipsec-howto.org/ipsec-howto.pdf>, <http://www.iptables.org>, <http://httpd.apache.org>, dostępne IX-X. 2012r.

- [8] Lubkowski P., Laskowski D.: The end-to-end rate adaptation application for real-time video monitoring, *Advances in Intelligent Systems and Computing* 224, pp. 295-305, 2013.
- [9] Lubkowski P., Laskowski D., Pawlak E. Provision of the reliable video surveillance services in heterogeneous networks, *Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference, ESREL 2014* pp. 883-888, 2015.
- [10] Lubkowski P., Laskowski D.: Test of the multimedia services implementation in information and communication networks, *Advances in Intelligent Systems and Computing* 286, pp. 325-332, 2014.
- [11] Serafin M.: *Sieci VPN – Zdalna praca i bezpieczeństwo danych*, Helion, 2008.
- [12] Shimorski J. R., Shinder Littlejohn D., Shinder W. Thomas – „Wielka Księga Firewalli”, HELION, Warszawa 2004.
- [13] Zalecenia IETF: RFC-3193 „Securing L2TP using IPSec”, RFC-3511 “Benchmarking Methodology for Firewall Performance”, 2003.
- [14] Laskowski D., Lubkowski P., Pawlak E., Stańczyk P.: Anthro-po-technical systems re-liability, *Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference, ESREL 2014*, pp. 399-407, 2015.
- [15] Lubkowski P., Laskowski D.: The selected issues of reliable identification of object in transport systems using video monitoring services, *Communication in Computer and Information Science* 0471, pp. 59-68, 2014.
- [16] Laskowski D., Lubkowski P., Kwasniewski M.: Identification of suitability services for wireless networks, *Przegląd Elektrotechniczny* 89 (9), pp. 128-132, 2013.
- [17] Bylak M., Laskowski D.: Assessment of network coding mechanism for the network protocol stack 802.15.4/6LoWPAN, *Advances in Intelligent Systems and Computing* 224, pp. 75-82, 2013.
- [18] Bylak M., Laskowski D.: Diagnosis coding efficiency of network coding mechanism for wireless networks, *Przegląd Elektrotechniczny* 89 (9), pp. 133-138, 2013.

***Dr hab. inż. Dariusz Laskowski** ukończył Wydział Elektroniki Wojskowej Akademii Technicznej, gdzie obecnie pracuje. Zajmuje się wieloaspektową analizą zjawisk determinujących poprawność realizacji usług w heterogenicznych systemach i sieciach oferujących przesył danych. Główne obszary zainteresowania to niezawodność, bezpieczeństwo, jakość i przeżywalność obiektów technicznych w aspekcie ich praktycznego zastosowania w sieciach heterogenicznych.*