4

Zapora sieciowa

Wprowadzenie – jak chronić lokalną sieć komputerową, czyli rola zapory sieciowej

Zapora sieciowa (ściana ogniowa) ma za zadanie chronić komputer lub sieć komputerową przed nieautoryzowanym dostępem. Funkcję zapory sieciowej pełnią w systemie informatycznym serwery NAT i proxy. Bardzo częstą praktyką wykorzystywaną we wdrożeniu zapory sieciowej jest stosowanie strefy ograniczonego zaufania (strefa zdemilitaryzowana). Jest to w sieci komputerowej wydzielony obszar o swobodnym dostępie z sieci zewnętrznej oraz braku dostępu do sieci wewnętrznej.

W tym rozdziale nauczysz się:

- rozróżniania typów zapór sieciowych,
- konfigurowania zapory sieciowej,
- stosowania serwerów NAT i proxy.

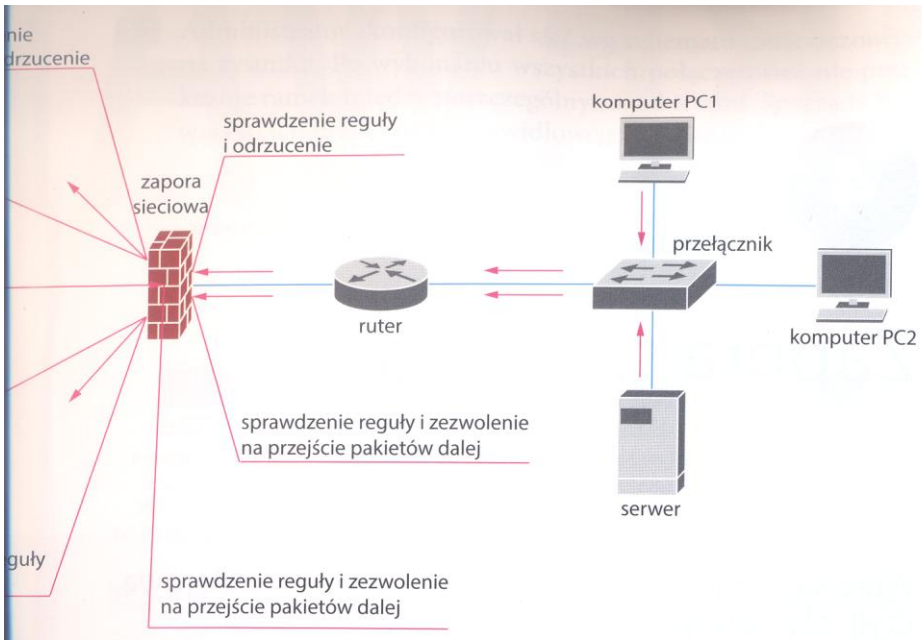
4.1 Zasada działania zapory sieciowej

Zapora sieciowa (ang. *firewall*) filtruje ruch w lokalnej sieci komputerowej, przychodzący i wychodzący, przepuszczając tylko pakiety danych spełniające **ustanowione reguły**. Pakiety, które tych reguł nie spełniają, są odrzucane (rys. 4.1). Zapora sieciowa pracuje we wszystkich warstwach modelu OSI/ISO (rys. 4.2), przy czym w warstwie:

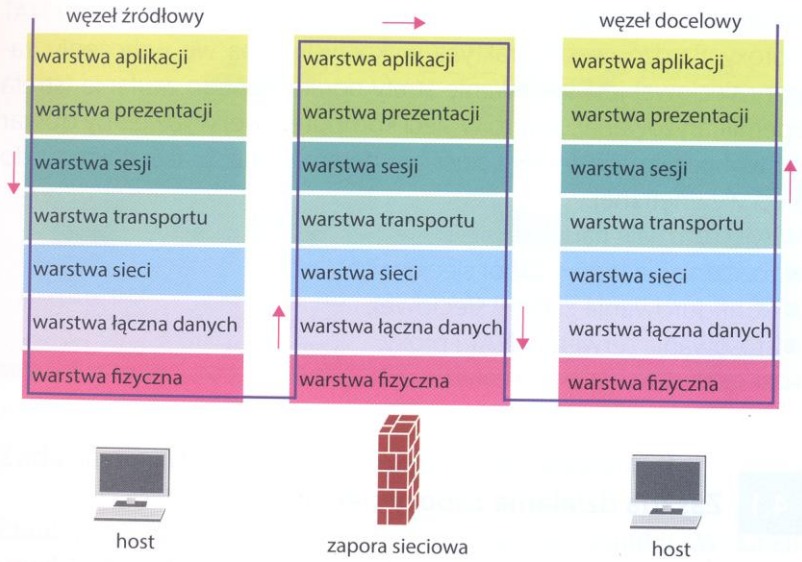
- fizycznej i łącza danych – filtruje po adresie MAC,
- sieciowej – filtruje po adresach IP,
- transportowej – filtruje po portach,
- sesji, prezentacji i aplikacji – ochrona antywirusowa, serwer proxy.

zapora sieciowa

ustanowiona reguła



Rys. 4.1. Schemat działania zapory sieciowej



Rys. 4.2. Zasada działania zapory sieciowej w modelu OSI/ISO

Ze względu na sposób filtrowania danych przez zaporę sieciową rozróżniamy:

e ruchu
owego

- **filtrowanie ruchu sieciowego** – umożliwia administratorowi systemu definiowanie tabel zawierających łańcuchy reguł stosowanych dla pakietów; filtrowanie pakietów przebiega w trzeciej i czwartej warstwie modelu OSI/ISO; przykładem zapory tego typu jest aplikacja IPtables w systemie Linux,

- **filtrowanie przez sprawdzanie stanu komunikacji sieciowej** (ang. *stateful firewall*) – umożliwia nadzorowanie stanu wszystkich połączeń przechodzących przez zaporę sieciową i analizowanie nagłówków pakietów pod kątem, czy pakiety te są przesyłane przez aplikacje dopuszczone do ruchu sieciowego; filtrowanie pakietów przebiega w trzeciej i czwartej lub tylko w czwartej warstwie modelu OSI/ISO,
- **maskowanie adresów sieciowych w lokalnej sieci komputerowej (wewnętrznej)** – usługa NAT,
- **zapora pośrednicząca** – serwer proxy.

filtrowanie przez sprawdzanie stanu komunikacji sieciowej

maskowanie adresów sieciowych w lokalnej sieci komputerowej (wewnętrznej)

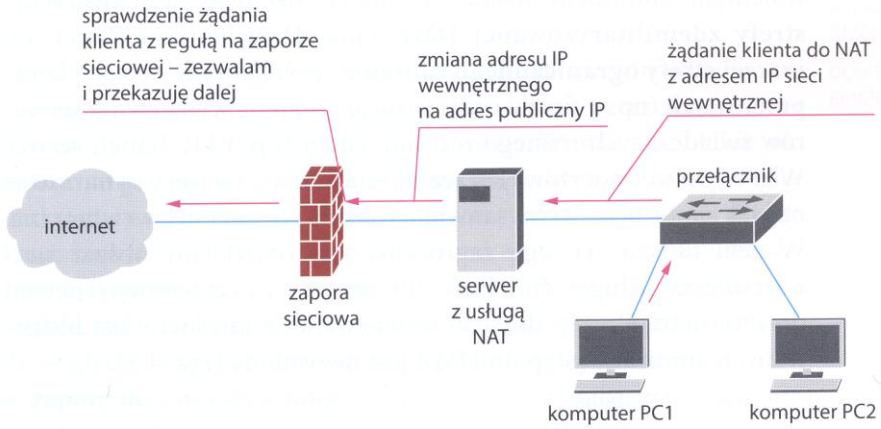
zapora pośrednicząca

usługa NAT

Działanie **usługi NAT** (ang. *Network Address Translation*) jest realizowane (na serwerach bądź ruterach) w dwóch etapach (rys. 4.3) w czwartej warstwie modelu OSI/ISO:

- żądanie klienta jest kierowane do usługi NAT, która zmienia prywatny adres IP w sieci LAN na adres publiczny w internecie,
- żądanie klienta zostaje sprawdzone, czy jest zgodne z regułami ustawionymi na zaporze sieciowej; jeśli tak, to żądanie jest przesyłane do internetu.

Przekazanie żądania z internetu jest realizowane w odwrotnej kolejności.



Rys. 4.3. Usługa NAT na zaporze sieciowej

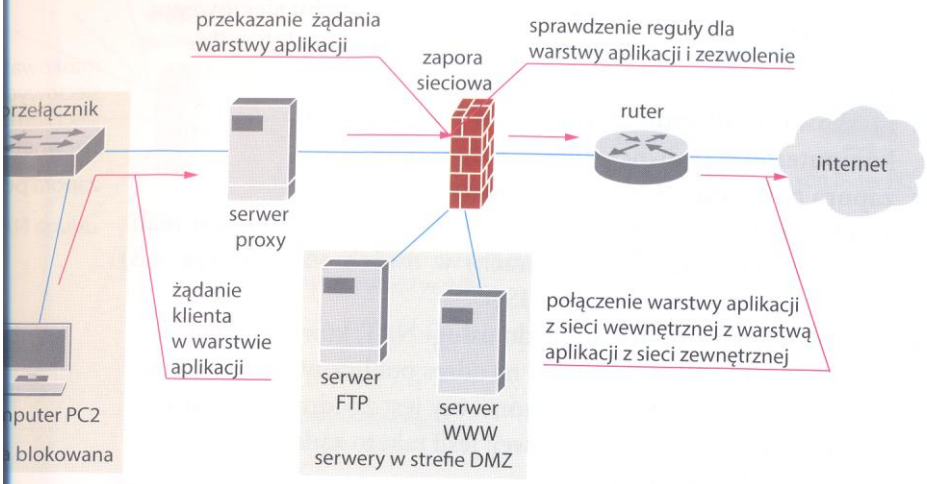
W blokowaniu ruchu sieciowego na poziomie warstwy aplikacji wykorzystuje się **serwer pośredniczący** (ang. *proxy*), nazywany **serwerem proxy** lub **bramką warstwy aplikacji** (rys. 4.4). Wykonuje on połączenia w imieniu użytkownika. Serwer proxy fizycznie oddziela sieć wewnętrzną od sieci zewnętrznej (internet), pełniąc rolę pośrednika między tymi sieciami. Wymiana danych między nimi jest możliwa tylko przez warstwę aplikacji. Takie działanie powoduje, że hosty w sieci wewnętrznej nie są widoczne z internetu. Działanie na poziomie aplikacji pozwala nie tylko serwerowi proxy sprawdzać nagłówek pakietu, ale również zajrzeć do danych zawartych w aplikacji danych, nawet zaszyfrowanych.

serwer pośredniczący

serwer proxy

bramka warstwy aplikacji

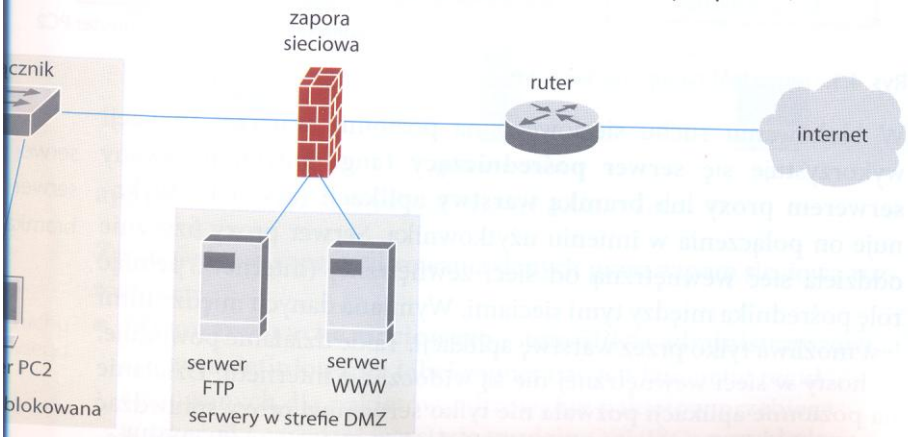
Więcej informacji na ten temat znajduje się na stronach:
http://students.mimuw.edu.pl/SO/Projekt04-05/temat5-g2/sikora--kobylinski/firewall.html
http://wazniak.mimuw.edu.pl/images/1/1c/Bsi_09_wykl.pdf



Rys. 4.4. Serwer proxy w funkcji zapory sieciowej

yzowana DMZ
czonego zaufania

Kolejnym sposobem działania zapory sieciowej jest tworzenie **strefy zdemilitaryzowanej DMZ** (ang. ***DeMilitarized Zone***) lub inaczej **strefy ograniczonego zaufania**. W lokalnych sieciach komputerowych (np. w firmowych) istnieje potrzeba wydzielenia serwerów świadczących różnego rodzaju usługi (np. FTP, Telnet, serwer WWW, serwer pocztowy) przez internet. Takie serwery są narażone na atak z internetu, a tym samym narażona jest cała sieć wewnętrzna. W celu uniknięcia tego zagrożenia jest wydzielany obszar sieci z serwerami usługowymi, który nie należy do sieci wewnętrznej ani do internetu. Dostęp do sieci wewnętrznej z internetu jest blokowany, natomiast dostęp do DMZ jest dozwolony (rys. 4.5).



Rys. 4.5. Schemat podziału lokalnej sieci komputerowej na sieć wewnętrzną blokowaną i strefą DMZ

4.2 Rodzaje zapór sieciowych

Zapory sieciowe możemy podzielić ze względu na metodę filtrowania pakietów danych. Są to:

- **filtr pakietów** – filtr statyczny dodany przez administratora sieci, może dotyczyć adresów, numerów portów, protokołów (np. TCP, UDP); wadą tego rozwiązania jest brak możliwości analizy warstwy aplikacji oraz niski poziom bezpieczeństwa, — filtr pakietów
- **filtr sprawdzający stan komunikacji sieciowej** – analizuje nagłówki pakietów, sprawdzając czy pochodzą z zaufanych aplikacji bądź adresów; wymaga częstej ingerencji administratora sieci, ale ma wyższy poziom bezpieczeństwa niż filtr pakietów, — filtr sprawdzający stan komunikacji sieciowej
- **filtr proxy aplikacyjny** – umożliwia szczegółową analizę poszczególnych protokołów aplikacji (np. http, ftp, smtp, pop3, imap); analiza warstwy aplikacyjnej jest zdecydowanie łatwiejsza niż w poprzedniej metodzie, ponadto zapewnia bardzo wysoki poziom bezpieczeństwa, ale jest mniej wydajna, — filtr proxy aplikacyjny
- **filtr hybrydowy** – stanowi połączenie poprzednich metod; zapewnia wysokie bezpieczeństwo i wydajność, lecz wiąże się z wysokim kosztem. — filtr hybrydowy

Dobierając zaporę sieciową, należy uwzględnić specyfikę ruchu sieciowego oraz systemu operacyjnego, który będzie przez daną zaporę chroniony. Zapora może mieć dodatkowe funkcjonalności, takie jak: system antyspamowy, system konfiguracji z wykorzystaniem przeglądarki internetowej, tunele VPN, system antywirusowy. Każda dodatkowa funkcjonalność może jednak powodować spadek przepustowości i wydajności zapory. Dlatego też należy rozważyć, czy dodatkowe funkcjonalności będą wykorzystywane czy będzie to zbędny dodatek. Ze względu na sposób filtrowania oraz budowę wyróżniamy:

- **zaporę sieciową sprzętową** (hardwarową) – samodzielne urządzenie pełniące rolę zapory lub część innego urządzenia (np. rutera), — zapora sieciowa sprzętowa
- **zaporę sieciową programową** (softwarową) – oprogramowanie pełniące rolę zapory. — zapora sieciowa programowa

Do zapór sprzętowych zaliczamy zaporę dedykowaną i ruter z wbudowaną zaporą sieciową.

Zapora sieciowa dedykowana to specjalistyczne urządzenie wyposażone w podstawowe mechanizmy, które zapewniają ochronę ruchu sieciowego. Do jej podstawowych zadań należą: — zapora sieciowa dedykowana

- filtrowanie ruchu sieciowego przychodzącego i wychodzącego, uwzględniające wykrywanie i usuwanie niebezpiecznego kodu,
- tworzenie bezpiecznych **wirtualnych połączeń VPN** (ang. *Virtual Private Network*) z wykorzystaniem zintegrowanego serwera VPN, — wirtualne połączenie VPN

- kontrola dostępu do zasobów i aplikacji,
- autoryzacja użytkowników,
- zarządzanie szerokością pasma dla aplikacji,
- ochrona antyspamowa i antywirusowa,

adres URL

- filtrowanie stron internetowych po **adresach URL** (ang. ***Uniform Resource Locator***), co umożliwia blokowanie użytkownikom dostępu do wybranych stron internetowych.

ruter z wbudowaną zaporą sieciową

W małych sieciach lokalnych zapora sieciowa sprzętowa może być również realizowana jako jedna z usług świadczonych przez ruter. Jest to **ruter z wbudowaną zaporą sieciową** (ang. *router with a built-in-firewall*), w którym stosuje się listę kontroli dostępu ACL filtrującą ruch sieciowy przechodzący przez urządzenie. Filtrowanie tego ruchu może odbywać się z wykorzystaniem następujących atrybutów pakietów IP:

- protokoły warstwy trzeciej (np. IP, IPX),
- interfejs sieciowy rutera,
- kierunek ruchu pakietów (wejściowe i wyjściowe pakiety),
- adres źródłowy i docelowy IP,
- typ warstwy transportowej TCP lub UDP,
- analiza warstwy sesji, prezentacji i aplikacji.

Przykładowa reguła dla ACL ustawiona na ruterze Cisco z wiersza poleceń interfejsu CLI to:

```
R2(config)# access-list 109 deny tcp host 192.168.1.2
host 192.168.2.15 eq 80
```

Reguła ta blokuje ruch protokołu TCP między hostem źródłowym o adresie IP 192.168.1.2 a hostem o adresie docelowym 192.168.2.15 na porcie 80.

4.3 Konfiguracja zapory sieciowej

Konfigurację zapory sieciowej omówimy na przykładzie systemu MS Windows 8.1 oraz rutera sprzętowego Cisco RV320.

procedura konfiguracji zapory sieciowej systemu MS Windows 8.1

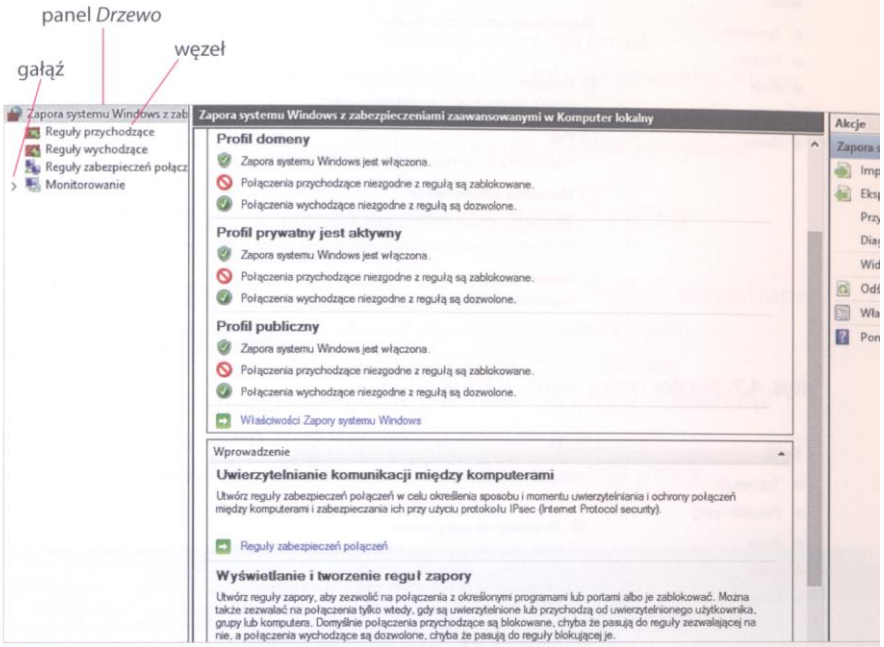
Procedura konfiguracji zapory sieciowej systemu MS Windows 8.1 jest następująca:

KROK 1 Wywołanie menu *Start* systemu MS Windows 8.1 przez naciśnięcie prawego klawisza myszy na ikonie logo systemu MS Windows.

KROK 2 Wybranie z menu *Start* systemu MS Windows 8.1 opcji *Panel sterowania*.

KROK 3 Wywołanie okna konfiguracji zapory sieciowej przez wybranie ścieżki *Panel sterowania* → *Zapora systemu Windows* → *Ustawienia zaawansowane*.

KROK 3 W oknie ustawień zapory systemowej w panelu *Akcje* (rys. 4.6) należy przystąpić do konfigurowania danego węzła w drzewie konfiguracyjnym. Wykonuje się to przez dodanie nowej reguły dla ruchu przychodzącego lub wychodzącego (rys. 4.7). Można również modernizować zapisy w istniejących regułach.



Rys. 4.6. Okno konfiguracji zapory sieciowej w MS Windows 8.1

Aby dodać regułę należy wykonać **procedurę dodawania reguły**, która jest następująca:

KROK 1 Wybranie opcji *Dodaj nową regułę* (rys. 4.7). Zostanie uruchomiony kreator, w którym można konfigurować typ reguły, tj. czy dotyczyć będzie ona programu zainstalowanego w systemie operacyjnym, portu lub wcześniej zdefiniowanej reguły. W tym przykładzie posłużymy się portem.

KROK 2 Zaznaczenie rodzaju protokołu warstwy transportowej, z jakiego korzysta dana usługa. Może to być: *protokół UDP* (protokół bezpołączeniowy) lub *protokół TCP* (protokół połączeniowy). Wpisanie numeru portu usługi lub wybór wszystkich portów.

KROK 3 Konfigurowanie akcji. Możliwe są ustawienia: *Zezwalaj na połączenie*; *Zezwalaj na połączenie, jeśli jest bezpieczne*; *Zablokuj połączenie* (rys. 4.8). Pierwsza opcja pozwala na połączenie, gdy połączenia są chronione przez bezpieczny protokół IPsec; druga – gdy użyto uwierzytelnienia za pomocą protokołu IPsec; ostatnia opcja blokuje dostęp do usługi lub portu. Dla ułatwienia zablokujemy całkowicie dostęp do portu.

KROK 4 Wybranie profilu, czyli w jaki sposób ma ta reguła funkcjonować (rys. 4.9): dla domeny (wszystkie komputery z domeny