Zapory ogniowe

Zapora ogniowa

- Umieszczana:
  - w punkcie przejścia między siecią lokalną lub korporacyjną a siecią rozległą
  - Pomiędzy segmentami sieci LAN
- Utworzona z jednego lub wielu urządzeń i/lub specjalistycznego oprogramowania.
- Podstawowa zasada działania to filtrowanie ruchu przychodzącego i wychodzącego oraz ruchu wewnątrz chronionej sieci lokalnej

Funkcje zapór ogniowych

- Ochrona przed włamaniami z zewnątrz
- Filtrowanie pomiędzy podsieciami
- Informowanie o potencjalnych zagrożeniach

Technologie kontroli ruchu

- Filtrowanie pakietów (*Packet Filtering*) Selekcja pakietów na podstawie nagłówków warstwy sieciowej i transportowej
- Translacja (maskowanie) adresów sieciowych (*Network Address Translation*)
- Filtrowanie w warstwie aplikacji Selekcja pakietów na podstawie danych
- Brama warstwy aplikacji (*Proxy Service*) - usługi pośredniczące

Filtrowanie pakietów

- w. sieciowa: identyfikacja i filtrowanie w zależności od adresów źródłowych i docelowych (IP), fragmentacji
- w. transportowa: filtrowanie na podstawie portów (TCP, UDP), parametrów sesji (TCP), kierunków połączeń
- brak filtrowania danych (w. aplikacji)
- duża szybkość

Filtrowanie pakietów

- Na podstawie informacji z nagłówka każdego pakietu następuje podjęcie decyzji o przepuszczeniu (*allow*) bądź odrzuceniu (*drop, deny*) badanego pakietu

Filtr bezstanowy (*Stateless*)

- Przetwarza każdy pakiet indywidualnie, bez brania pod uwagę innych pakietów, stanu sesji TCP, itp.
- Nie zapamiętuje stanu połączenia, ponieważ nie przechowuje informacji o porcie usługi związanej z przesyłanymi pakietami
- *Zapora pierwszej generacji*

Filtr z badaniem stanów (*Stateful Inspection*)

- Zasada działania filtra z badaniem stanów polega na bieżącym monitorowaniu przechodzących przez dany węzeł połączeń (zwłaszcza sesji TCP), co pozwala na skuteczniejszą kontrolę ich legalności i poprawności.
- *Zapora drugiej generacji*

Filtr z badaniem stanów

- Przechowuje informacje o stanie całego przechodzącego ruchu pakietów na poziomie warstwy sieciowej oraz transportowej
- Wie jakie kolejne stany zostały dozwolone z punktu widzenia protokołu oraz polityki bezpieczeństwa
- Kojarzy pakiety wychodzące z przychodzącymi

Filtr z badaniem stanów

- Automatycznie weryfikuje kolejne etapy nawiązania oraz późniejszy przebieg połączenia
- Odrzuca pakiety błędne bądź nie należące do danej sesji
- Blokuje ataki polegające na wprowadzanie sfałszowanych pakietów
- Blokuje próby skanowania portów

Translacja adresów w zaporach ogniowych

- Mechanizm NAT pozwala zmieniać adresy IP znane wewnątrz chronionej sieci na unikatowe adresy wykorzystywane w Internecie
- Struktura i adresy sieci wewnętrznej są niewidoczne w sieci publicznej

Filtr w w. aplikacji

- Filtrowanie na wyższych warstwach umożliwia ustalanie związków między pakietami tego samego połączenia
- Ułatwia implementację uwierzytelniania i szyfrowania
- *Zapora trzeciej generacji*

Zalety filtrów w. aplikacji

- Blokują dostęp do wybranych adresów WWW w oparciu o ich adres URL
- Filtrują dane pod kątem podejrzanej zawartości, wyszukują wirusy, konie trojańskie, niechciane treści
- Badają spójność przesyłanej informacji pod kątem nieprawidłowo sformatowanych danych

Web Application Firewall

- zapora wyspecjalizowana do filtrowania ruchu do/z aplikacji webowych
- reguły pozwalają rozpoznać ataki na aplikacje webowe, typu: cross-side-scripting, SQL injection
- często umieszczana w reverse-proxy
- liczne rozwiązania różnych producentów

Email Gateway

- Wyspecjalizowana zapora do ochrony poczty
- Mechanizmy:
  - filtry antyspamowe
  - ochrona przed malware, phishingiem
  - określanie reputacji nadawcy
  - DLP w poczcie wychodzącej
- Dostępne jako oprogramowanie lub dedykowane urządzenie

Poziom aplikacji - proxy

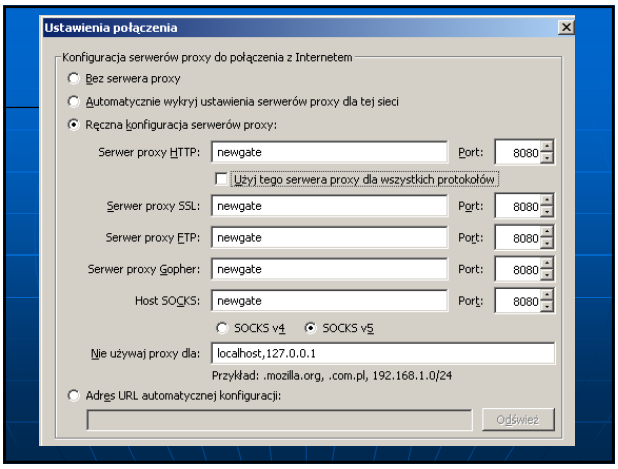
- Proxy początkowo służyły do przechowywania w pamięci podręcznej często przeglądanych stron WWW
- Obecnie używa się ich do ukrywania użytkowników sieci za pojedynczym komputerem
- Serwery proxy zwykle umieszcza się pomiędzy wewnętrznym użytkownikiem sieci lokalnej, a daną usługą w Internecie

Zalety serwerów proxy

- Proxy ukrywa użytkownika przed dostępem z Internetu. Sieć lokalna jest widziana jako jeden komputer. Hosty zewnętrzne nie mogą łączyć się z usługami dostępnymi na wewnętrznych komputerach.
- Zapewnia pojedynczy punkt dostępu, nadzorowania oraz rejestrowania zdarzeń.

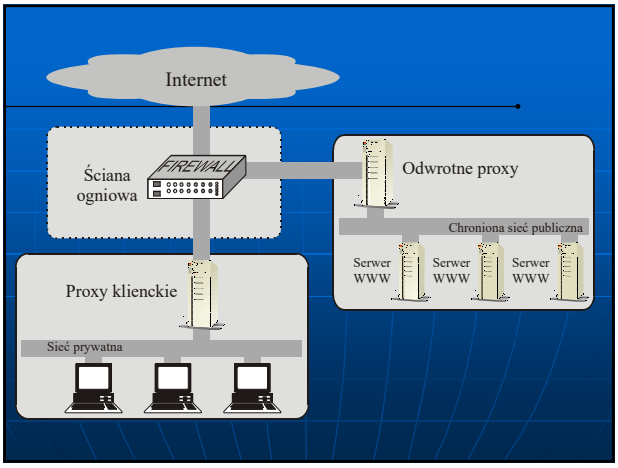
Wady serwerów proxy

- Proxy stanowi pojedynczy punkt w sieci lokalnej, który w każdej chwili może ulec awarii
- Oprogramowanie klienckie musi współpracować z proxy
- Każda usługa musi posiadać swoje własne proxy

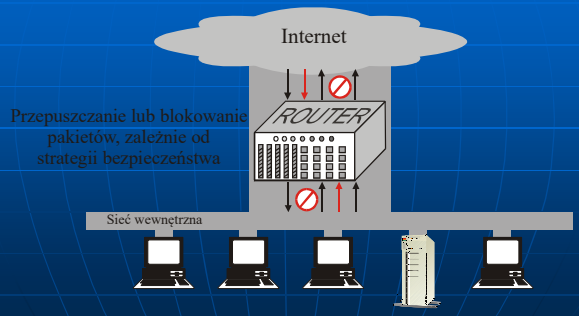


Proxy odwrotne

- Proxy odwrotne (*Reverse Proxy*) – Internet jest widoczny dla farmy serwerów jako pojedyncze urządzenie generujące zapytania
- W połączeniu z systemem wykrywania intruzów proxy odwrotne stanowi skuteczną obronę przed przejęciem kontroli nad serwerem



Zapora ogniowa zbudowana z routera filtrującego

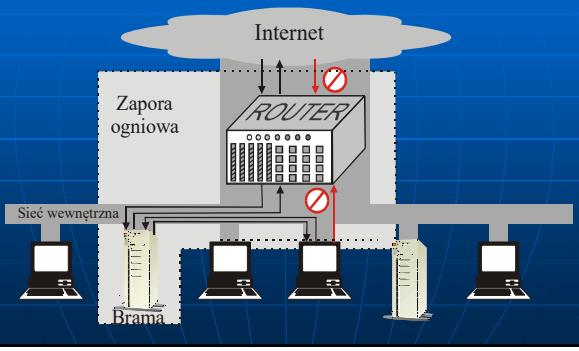


Zapora ogniowa zbudowana z routera filtrującego

Rozwiązanie jest funkcjonalne gdy:

- Hosty umieszczone w chronionej sieci są dobrze zabezpieczone.
- Używana jak niewielka liczba protokołów o niskiej złożoności.
- Priorytetową cechą zapory ma być wysoka wydajność.

Ekranowany host (*Screened Host Gateway*)



Ekranowany host

Zadania routera:

- Blokowanie nie wykorzystywanych usług
- Blokowanie routingu źródłowego
- Blokowanie pakietów innych niż z/do bramy wewnętrznej

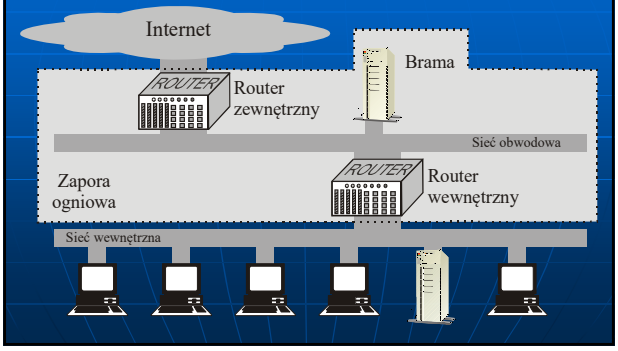
Zadania bramy (hosta bastionowego):

- serwer proxy
- filtr w. aplikacji

Ekranowany host - wady

- Intruz, który złamał zabezpieczenia hosta bastionowego uzyskuje łatwy dostęp do wszystkich wewnętrznych hostów
- Sieć jest dostępna, gdy intruz złamie zabezpieczenia routera
- W bastionie nie należy uruchamiać ryzykownych usług

Ekranowana podsieć



Ekranowana podsieć

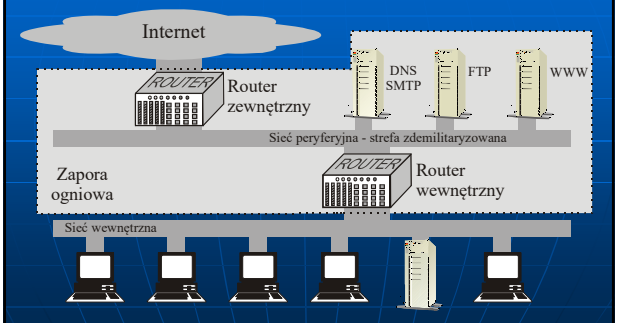
Nowe zadania routera zewnętrznego:

- Blokowanie pakietów z/do routera wewnętrznego

Zadania routera wewnętrznego:

- Blokowanie niewykorzystywanych usług
- Blokowanie routingu źródłowego
- Blokowanie pakietów z/do routera zewnętrznego
- Przepuszczanie pakietów z/do bramy

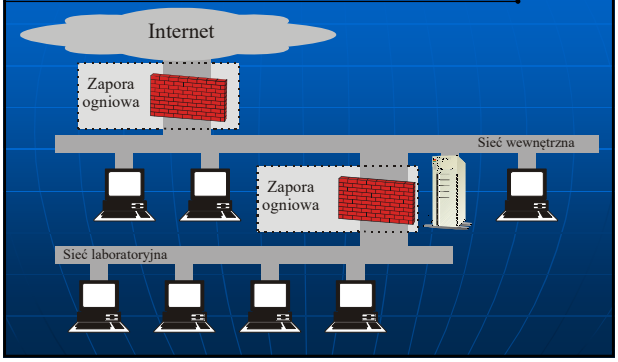
Architektura z użyciem większej liczby bram



Architektura z użyciem większej liczby bram

- Zamiast jednej wspólnej bramy, można użyć po jednej dla każdego protokołu
- Użycie kilku hostów bastionowych zamiast jednego można wykorzystać do:
  - Zwiększenia wydajności usługi intensywnie wykorzystywanej
  - Wprowadzenia redundancji. Hosty można tak skonfigurować, aby w razie awarii inny host mógł przejąć świadczone usługi

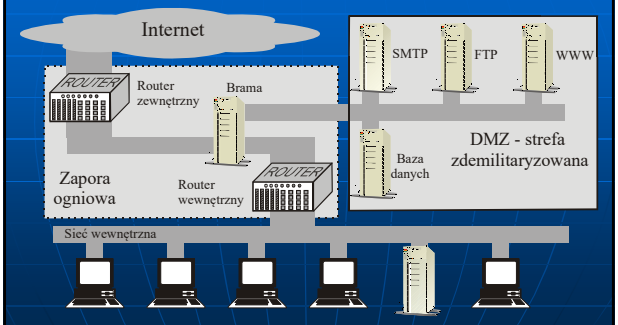
Wewnętrzne zapory sieciowe



Zalety wewnętrznych zapór sieciowych

- Tworzą bariery dla włamywaczy z zewnątrz (Internetu) i z wewnątrz (z sieci lokalnej)
- Ograniczają zasięg i skutki awarii i błędów w sieci wewnętrznej
- Ograniczają liczbę hostów, które mogą być podatne na ataki przez uniemożliwienie działania

Strefa zdemilitaryzowana DMZ



Zapory ogniowe - wyzwania

- Sieci VPN – filtrowanie zaszyfrowanych treści
- Brak możliwości blokowania niektórych portów (np. TLS)
- Omijanie zapór (tunelowanie, błędy w konfiguracji i kolejności reguł)

Firewall ACL

- Filtrowanie polega na dopasowaniu pakietu do jednej lub wielu reguł
- Listy reguł nazywane są Listami Kontroli Dostępu (ACL)
- Zadaniem ACL jest dopasowanie pakietu do wzorca, na podstawie informacji protokołowych

Dzikie maski

- *Widlcard masks* wykorzystywane są do tworzenia reguł ACL
- Jedynka w masce oznacza dowolną wartość na odpowiadającym bicie adresu, zero wartość określoną adresem
- W przeciwieństwie do maski IP, dzikie maski rozpoczynają się zerami, kończą jedynkami

Budowa ACL

- Reguły przeglądane sekwencyjnie, według kolejności na liście
- Każda reguła nakazuje dopuścić (*allow*) bądź odrzucić (*deny*) pakiet
- Po dopasowaniu pakietu do reguły przetwarzanie w ACL kończy się
- Domyślne zakończenie odrzuca wszystkie pakiety

Budowa ACL

- Kolejność reguł na liście jest ważna

1.xyz.com -> deny
2.All -> allow

1.All -> allow
2.xyz.com -> deny

Optymalizacja ACL

- Listy ACL mogą liczyć po kilkaset a nawet kilka tysięcy reguł
- Przetwarzanie pakietu dopasowanego do ostatniej reguły trwa kilka tysięcy razy dłużej niż pakietu dopasowanego do pierwszej reguły

Optymalizacja ACL - uwagi

- Reguły o największym współczynniku dopasowania – na początek listy

ale...

- Nie można dowolnie zmieniać kolejności reguł, jeśli dotyczą tych samych pakietów

Optymalizacja ACL - uwagi

- Proces powinien być cykliczny – obserwacja ruchu i okresowe modyfikacje reguł i ich kolejności
- Optymalizacja ACL wykonywana jest *offline*
- Stosowane mogą być różne algorytmy optymalizacji

Wykrywanie

IDS/IPS, HoneyPot

Filtrowanie ruchu

Firewall

- przepuszcza uprawniony ruch – podejmuje decyzje na podstawie reguł
- weryfikuje adresy, porty, stan połączenia, treści
- kluczowe znaczenia ma szybkość działania
- nie alarmuje w przypadku niedozwolonych pakietów (może je zapisywać w logach)

Czy filtrowanie wystarczy ?

- Nowe rodzaje ataków mogą przenikać przez reguły zapór ogniowych
- Ataki mogą być prowadzone z sieci wewnętrznej
- Ruch dozwolony może być wykorzystany w pewnych kombinacjach przez atakującego
- Nie da się przewidzieć wszystkich scenariuszy ataków
- Zbyt szczelne zapory ogniowe mogą uniemożliwiać działanie pożytecznych usług

Intrusion Detection System

- Analizuje (nie mylić z 'filtruje') ruch sieciowy, działania użytkowników i procesów, wykorzystanie zasobów, itp.
- Wykrywa próby ataku / nieautoryzowanego dostępu do sieci lub systemu
- Ostrzega o atakach, nie zapobiega
- System pasywny
- Szybkość nie jest parametrem kluczowym (chociaż nadal istotnym)

Zadania systemu IDS

- Monitorowanie systemu
  - monitoring ruchu w sieci i zdarzeń na hostach
- Wykrywanie ataków
  - analiza informacji, rozpoznawanie potencjalnie niebezpiecznych sekwencji czynności
- Podjęcie działań
  - zapisanie informacji o ataku
  - powiadomienie administratora (konsola, e-mail, sms)

Etapy działania systemu IDS

- Monitoring
- Przetwarzanie wstępne
- Analiza
- Reakcja
- Dostrajanie

Typy IDS

- Host-based IDS (HIDS)

  monitorowanie hostów
- Network-based IDS (NIDS)

  monitorowanie sieci
- Hybrydowe

HIDS

- Aplikacja zainstalowana na hoście lub agent na hoście i zewnętrzny system
- Możliwość analizy:
  - Ruchu sieciowego związanego z hostem
  - Zachowania procesów/usług na hoście (np. wykorzystywania luk systemu operacyjnego)
  - Działań użytkowników na hoście – w tym prób włamań bez wykorzystania sieci

NIDS

- Podłączony do segmentu sieci lub połączenia *uplink* (np. za lub przed routerem)
- Możliwość analizy:
  - Ruch sieciowy
- Zarządzanie centralne lub rozproszone
- Nie zużywa zasobów hosta (procesora, pamięci)

Podłączenie sond NIDS

- Port SPAN przełącznika lub koncentratora
  - problemy w środowisku przełączanym, gdy przełącznik nie dysponuje takim portem
- Urządzenie przechwytujące - most (in-line IDS)
- TAP

Techniki detekcji

- Wykrywanie nieprawidłowości (anomalii)
  - Wyszukiwanie nietypowych zachowań sieci
  - A jakie zachowania są ”typowe” ???
- Wykrywanie nadużyć
  - Na podstawie znanych wzorców ataków (sygnatur)

Wykrywanie nieprawidłowości

- Wymaga tworzenia i przechowywania dzienników zdarzeń w sieci i systemach operacyjnych
- Na podstawie dzienników ustala się zdarzenia i zachowania ”typowe”
- Zachowania ” typowe” mogą być również zdefiniowane przez operatora
- Odchylenie od zdarzeń ”typowych” jest interpretowane jako nieprawidłowość i powoduje alarm

Opis zachowań ”typowych”

- Krzywe parametryczne
  - Opisują dane historyczne zapisane w dzienniku
  - W celu przygotowania optymalnych krzywych przeprowadza się proces uczenia na podstawie danych z dzienników
  - Odchylenie od krzywej oznacza nieprawidłowość
  - Można regulować ‘czułość’ systemu – jako dopuszczalny stopień odchylenia

Opis zachowań ”typowych”

- Reguły statystyczne
  - Określają przedziały i progi dla zdarzeń normalnych, np. utylizację procesora, natężenie ruchu w sieci, liczbę jednocześnie otwartych sesji, liczbę operacji na pliku w ciągu godziny, itp.
  - Bardzo dobre do wykrywania ataków DoS
- Modelowanie za pomocą sztucznej inteligencji (sieci neuronowe, algorytmy ewolucyjne)

Definicje zachowań ”nietypowych”

- Ruch na porcie nie używanym w sieci
- Aktywność po godzinach pracy
- Aktywność lokalna zewnętrznego serwera
- Sesje przychodzące do sieci lokalnej
- Nielogiczne dane w nagłówkach (np. Xmass tree)

Wykrywanie nadużyć

- Przechowywanie wzorców ataków (np. sekwencji czynności)
- Wyszukiwanie wzorców

Np.: sekwencja czynności **A D K A** oznacza atak

Obserwowana sekwencja:

B F F G H A C M U D M C K K B A S

Sygnatury a anomalie

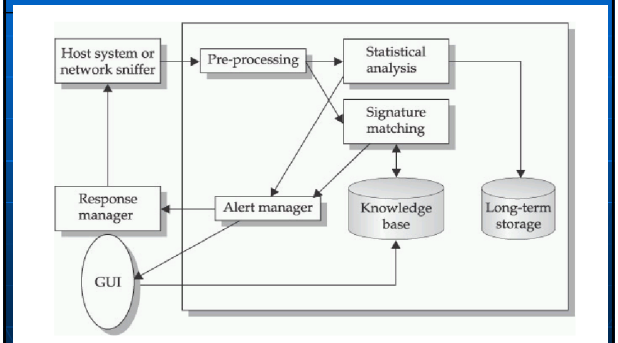
Badanie sygnatur

- Mało fałszywych alarmów
- Problem z wykrywaniem ataków rozciągniętych w czasie
- Tylko ataki o znanych sygnaturach
- Bazy sygnatur specyficzne dla różnych systemów

Analiza anomalii

- Dużo fałszywych alarmów
- Adaptacja do nowych warunków
- Wykrywanie ataków rozciągniętych w czasie
- Możliwy atak podczas nauki
- Niezależne od specyfiki systemu

Standardowy IDS



Wady systemów IDS

- Brak przeciwdziałania
- Fałszywe alarmy / niewykrycie ataku
- Wąskie gardła szybkich sieci
- Generują wielkie ilości danych do analizy
- Wykwalifikowany personel do obsługi
- Ograniczona obsługa ruchu szyfrowanego
- Cena

Intrusion Prevention System

Aktywnie przeciwdziała atakom w czasie rzeczywistym – np. poprzez dodawanie reguł zapory ogniowej, rekonfiguracje przełączników, zamykanie sesji, itp.

Połączenie zapory ogniowej i IDS

IDS/IPS - problemy i wyzwania

- Bardzo szybkie sieci LAN, MAN (kilkaset Gb/s):
  - Czas analizy
  - Rozmiar bazy danych
- Środowisko przełączane:
  - Wymagane specjalne porty monitorujące

Garnki miodu

- HoneyPot – przynęta na włamywacza
- Cel ochronny: zapobieganie, wykrywanie, reakcja na atak
- Cel badawczy: gromadzenie informacji o nowych rodzajach zagrożeń
- Z niską lub wysoką interakcją

Data Loss Prevention (DLP)

- Ochrona przed wyciekami informacji
- Techniki:
  - filtrowanie – wyszukiwanie chronionych treści w przesyłanych danych
  - systemy klasyfikacji dokumentów – twórca dokumentu (maila) określa typ zawartości i stopień poufności (w metadanych). Systemy tego typu są zintegrowane z pakietami biurowymi i programami pocztowymi. Następnie systemy DLP blokują wyciek na podstawie metadanych.

Systemy DLP

- Chronione kanały wycieku:
  - Poczta elektroniczna (także webmail)
  - Urządzenia we/wy (drukarki, faksy)
  - CD/DVD, pamięci przenośne
  - P2P
  - Komunikatory (np. Skype)
  - Protokoły: HTTP, FTP
  - Technologie: WiFi, Bluetooth

UTM

Unified Threat Management:

- Zapora ogniowa
- IDS/IPS
- Ochrona antywirusowa
- Ochrona antyspamowa
- Filtrowanie treści i zapytań
- Autoryzacja użytkowników
- Tunele VPN

SIEM

Security Information and Event Management:

- systemy gromadzenia, filtrowania, normalizacji i korelacji informacji
- wyewoluowały z systemów:
  - *Security Event Management* – systemy 'wczesnego ostrzegania'
  - *Security Information Management* – systemy wnioskowania na podstawie logów historycznych

SIEM

- przetwarzają głównie informacje z logów (np. dzienniki zdarzeń Windows, syslog, ODBC)
- wtyczki i agenty dla aplikacji o nietypowych formatach logów
- odczyt informacji również bezpośrednio z protokołów zarządzania sieciami (netflow, SNMP)