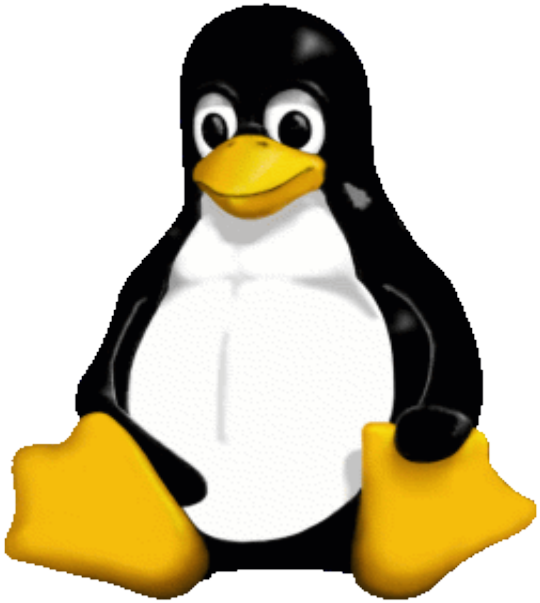
Bezpieczny serwer sieciowy Linux



Jacek Lach
jlach@star.iinf.polsl.gliwice.pl

Plan wykładu

- Terminologia
- Zasady bezpieczeństwa
- Architektura firewalli
- Testowanie

Terminologia

- Firewall - komponent lub zestaw komponentów ograniczających wymianę danych między różnymi sieciami
- Host bastionowy - bardzo dobrze zabezpieczony system komputerowy, do którego istnieje dostęp z zewnętrznej sieci (-> brak zaufania)
- Translacja adresów sieciowych (NAT) - działanie polegające na zamianie adresów sieciowych w pakietach (podłączenie wielu hostów przy użyciu jednego adresu, ukrycie adresów)

Terminologia - cd.

- Filtrowanie pakietów - ograniczenie ruchu pakietów z/do chronionej sieci na podstawie zdefiniowanych reguł zgodnych z polityką bezpieczeństwa sieci
- Router ekranujący (router brzegowy) - router filtrujący pakiety, posiadający dwa interfejsy sieciowe
- Pośrednik (proxy) - program realizujący wybrane żądania w imieniu klientów, ukrywając ich adresy sieciowe

Terminologia - cd.

- Strefa zdemilitaryzowana (DMZ, sieć peryferyjna) - sieć pomiędzy chronioną siecią wewnętrzną a siecią zewnętrzną stanowiąca dodatkową warstwę zabezpieczeń, miejsce podłączania serwerów publicznych
- Wirtualna sieć prywatna (VPN) - sieć prywatna, której poszczególne elementy są połączone przy pomocy sieci publicznej, ochrona danych przesyłanych w ramach sieci realizowana jest poprzez szyfrowanie

Zadanie firewalla

- Ochrona przed zagrożeniami pochodzącymi z sieci zewnętrznej poprzez:
  - wymuszenie dostępu do zasobów chronionej sieci w ściśle określonym punkcie
  - wymuszenie dostępu do sieci zewnętrznej w ściśle określonym punkcie
  - kontrolę ruchu wchodzącego i wychodzącego

Możliwości firewalla

- Skupienie środków bezpieczeństwa - efektywniejsze i tańsze niż rozproszenie zabezpieczeń
- Wymuszenie polityki bezpieczeństwa poprzez ograniczenie dostępu do niebezpiecznych usług
- Rejestracja wydarzeń
- Separacja segmentów sieci - ograniczanie rozprzestrzeniania się problemów w sieci

Ograniczenia firewalli

- Nie chronią przed użytkownikami wewnętrznymi
- Chronią jedynie połączenia, które przez nie przechodzą
- Nie chronią przed nowymi rodzajami zagrożeń
- Nie mogą stanowić jedynej (skutecznej) ochrony antywirusowej
- Wymagają poprawnej konfiguracji
- Ograniczają swobodę współpracy z siecią zewnętrzną

Zasady bezpieczeństwa

- Minimalne przywileje - tylko naprawdę potrzebne
- Złożona ochrona - stosowanie kilku wspierających się zabezpieczeń
- Zróżnicowana ochrona - stosowane zabezpieczenia powinny pochodzić z różnych źródeł
- Najsłabszy punkt - niestety zawsze istnieje
- Współpraca - nie można ochronić sieci, gdy użytkownicy “o bchodzą” zabezpieczenia

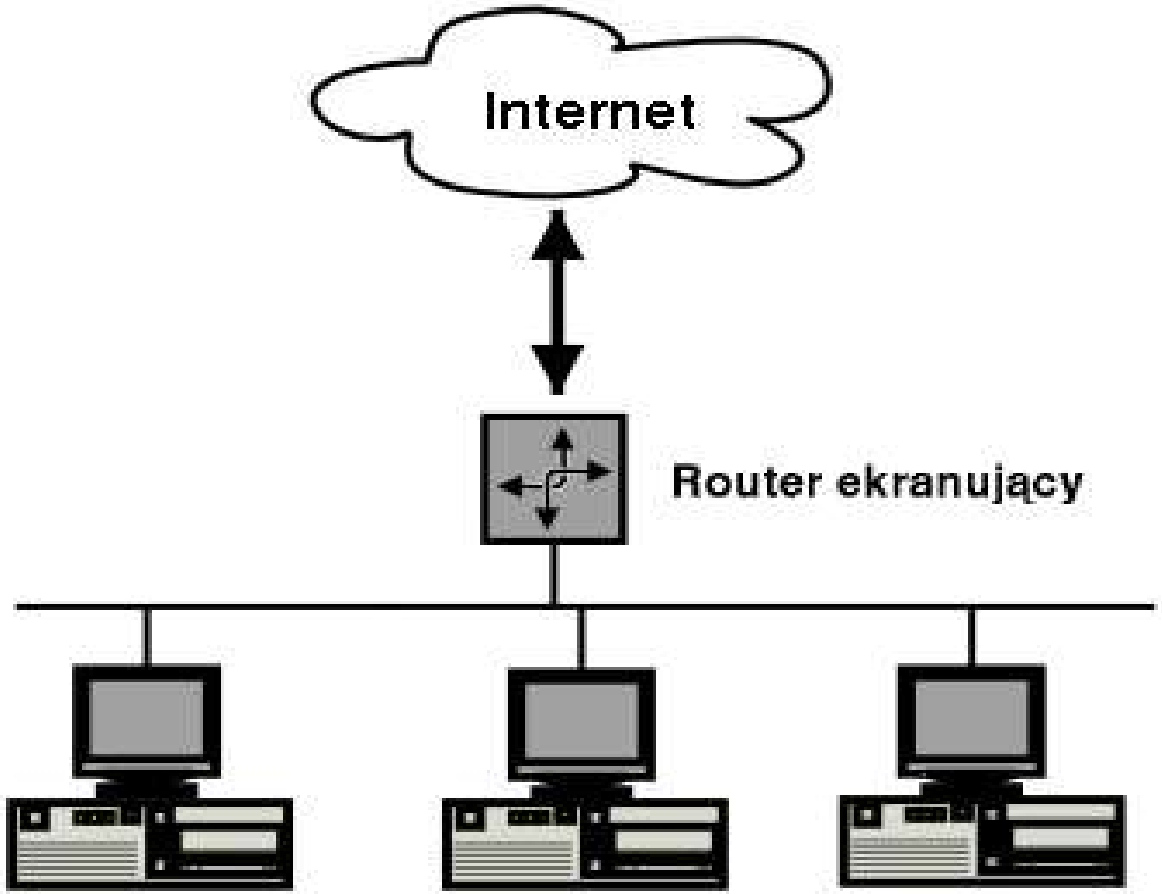
Zasady bezpieczeństwa - cd.

- Wąskie gardło - wymuszenie ruchu przez wskazany, kontrolowany punkt sieci
- Strategie działania:
  - co nie jest dozwolone, jest zabronione
  - co nie jest zabronione, jest dozwolone
- Zabezpieczenie przez utajnienie - nie stanowi dobrego zabezpieczenia, jednak nie należy ułatwiać życia włamywaczowi

Architektury firewalli

- Architektura routera ekranującego
- Architektura hosta dwusieciowego
- Architektura ekranowanego hosta
- Architektura ekranowanej podsieci
- Architektura ekranowanej podsieci - modyfikacje

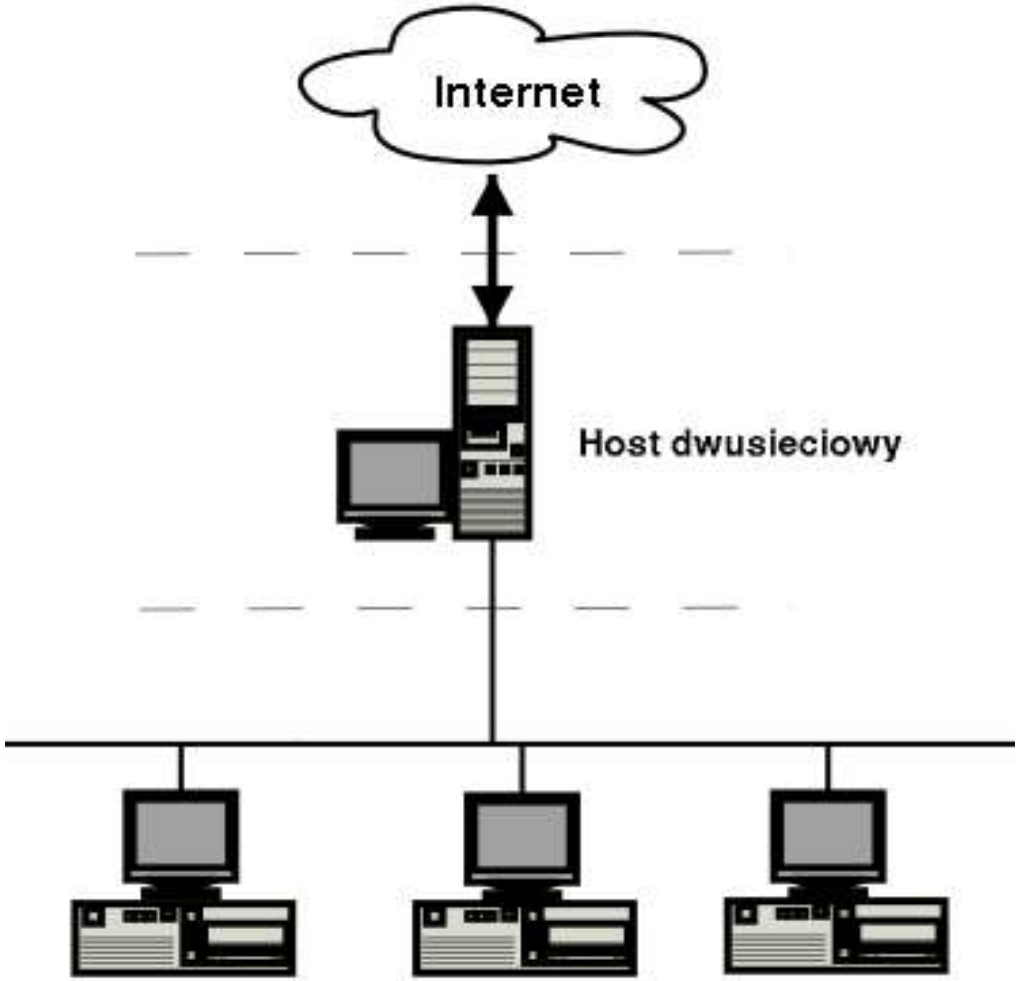
Architektura routera ekranującego



Architektura routera ekranującego

- Stosowana, gdy:
  - Hosty w chronionej sieci są dobrze zabezpieczone
  - Liczba używanych protokołów jest ograniczona
  - Wymagana jest duża wydajność
- Wady:
  - brak drugiej linii obrony
  - możliwości filtrowania ruchu ograniczone możliwościami routera

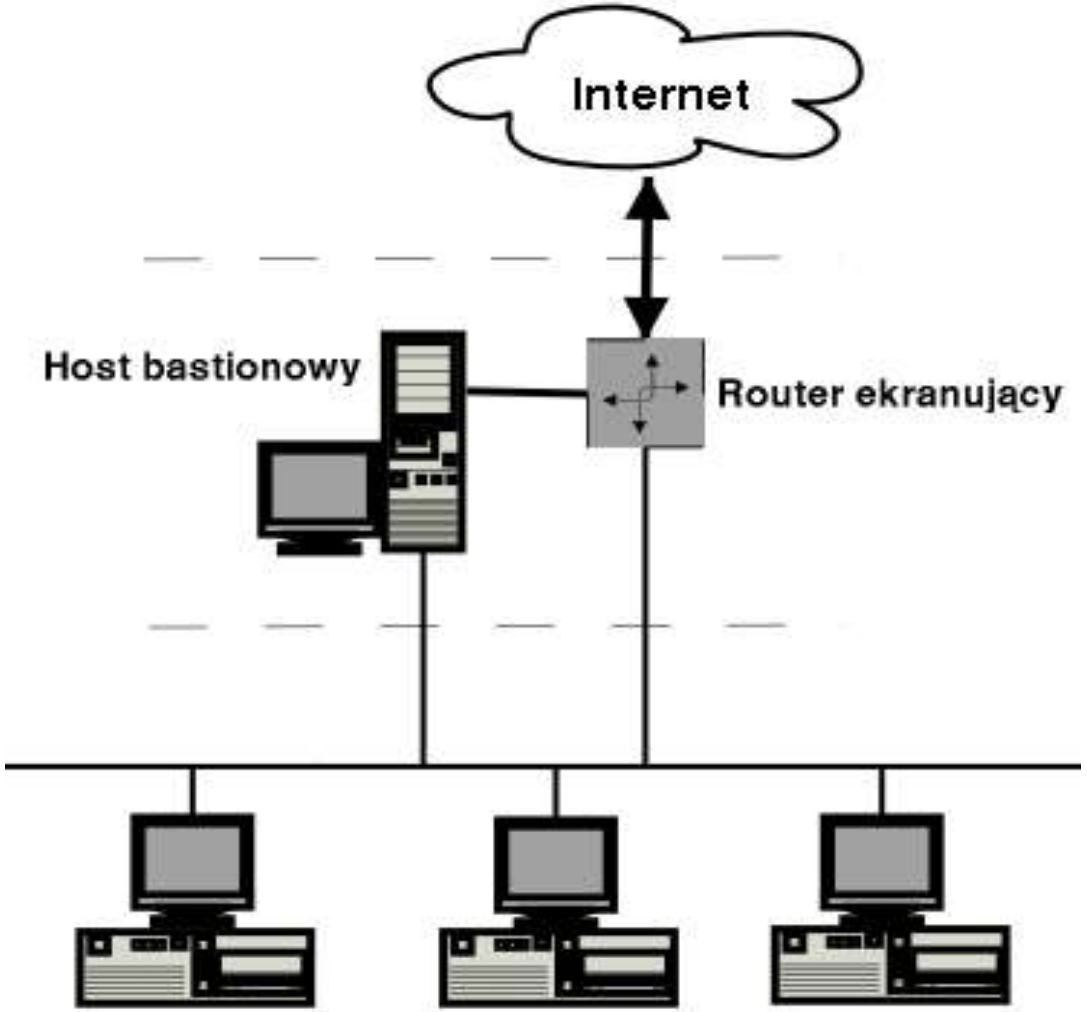
Architektura hosta dwusieciowego



Architektura hosta dwusieciowego

- Stosowana, gdy:
  - Ruch do Internetu jest niewielki
  - Łączność z internetem nie jest krytyczna
  - Użytkownicy internetu mają dostęp do ograniczonego zestawu usług (wymaganie pośrednika na hoscie dwusieciowym)
  - Chroniona sieć nie zawiera bardzo ważnych danych

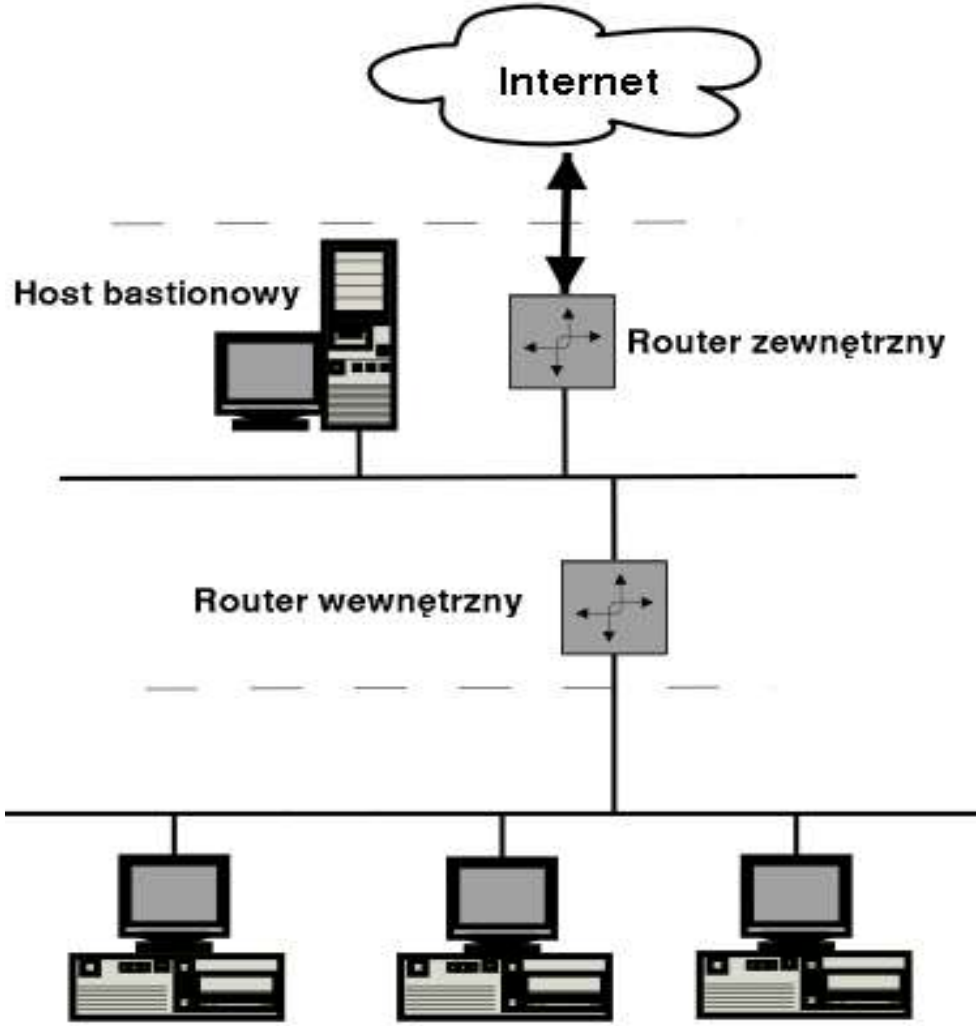
Architektura ekranowanego hosta



Architektura ekranowanego hosta

- Stosowana, gdy:
  - nie jest wymagane udostępnianie zaawansowanych wersji usług sieciowych
  - hosty w chronionej sieci mają dobre zabezpieczenia

Architektura ekranowanej podsieci



Architektura ekranowanej podsieci

- Wieloczęściowa sieć ekranowana
- Z wieloma sieciami peryferyjnymi
- Połączenie hosta bastionowego:
  - z routerem zewnętrznym
  - z routerem wewnętrznym

Testowanie firewalli

- Zagadnienia wymagające rozpatrzenia przy testowaniu:
  - potrzeba przeprowadzenia testu
  - zgoda instytucji, do której sieć należy
  - awarie sieci i systemów komputerowych
  - powiadamianie adminstratorów
  - nadzór
  - opracowanie wyników
  - zabezpieczanie raportu

Cele testowania

- Zgodność implementacji firewalla z polityką bezpieczeństwa
- Weryfikacja ochrony przed atakami sieciowymi
- Weryfikacja poprawności działania logowania zdarzeń
- Zbadanie skuteczności ochrony informacji o sieci wewnętrznej

Przeprowadzenie testu

- Wybór osoby testującej (doświadczenie, niezależność, zaufanie)
- Dobry raport powinien:
  - być czytelny dla osób “niewtajemniczonych”
  - zawierać opis zastosowanych testów i ich wyników
  - być dokładny - wskazówki dla personelu technicznego
  - zawierać propozycje rozwiązania problemów