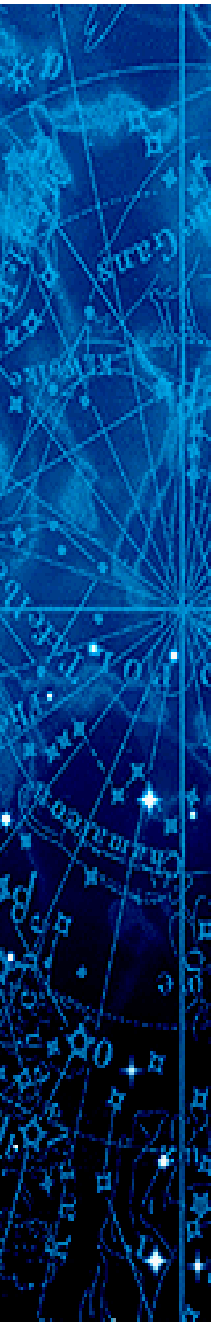


Systemy Firewall

Grzegorz Blinowski

"CC" - Open Computer Systems

Grzegorz.Blinowski@cc.com.pl

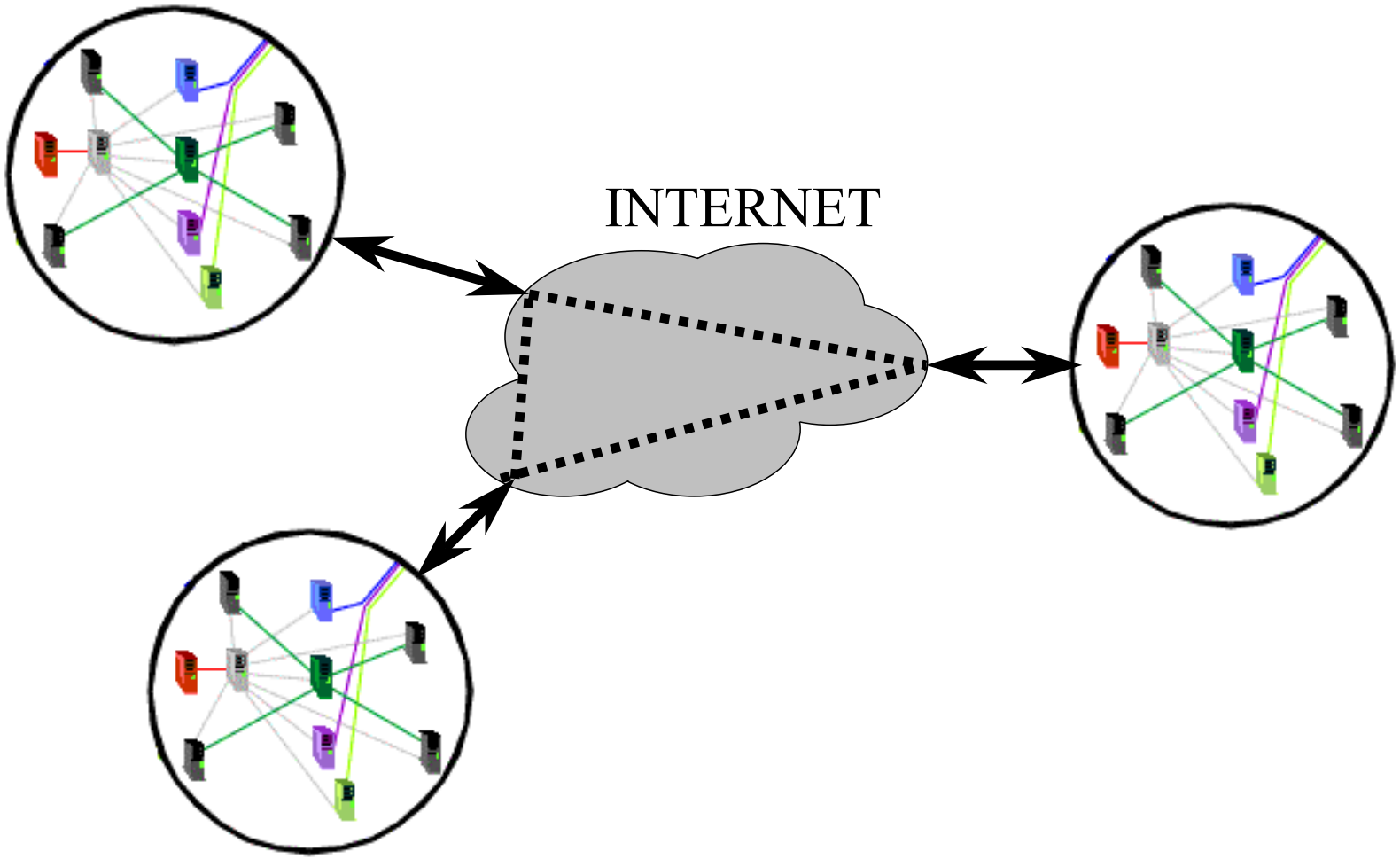
Plan wykładu

- Zastosowanie systemów Firewall w Intranecie
- Rodzaje systemów Firewall
- Główne koncepcje stosowania
- Filtry pakietowe
- Proxy
- Przegląd rynku

Korzyści z połączenia Intranetu z Internetem

- Wykorzystanie tych samych narzędzi w dostępie do danych
- Swobodna wymiana informacji (od e-mail'u do video-konferencji)
- Szybki i tani dostęp do danych na całym świecie (serwisy informacyjne, finansowe)
- Dostęp do danych konkurencji
- Ekstranet - połączenie Intranetów firm

Ekstranet - połączenie Intranetów firm

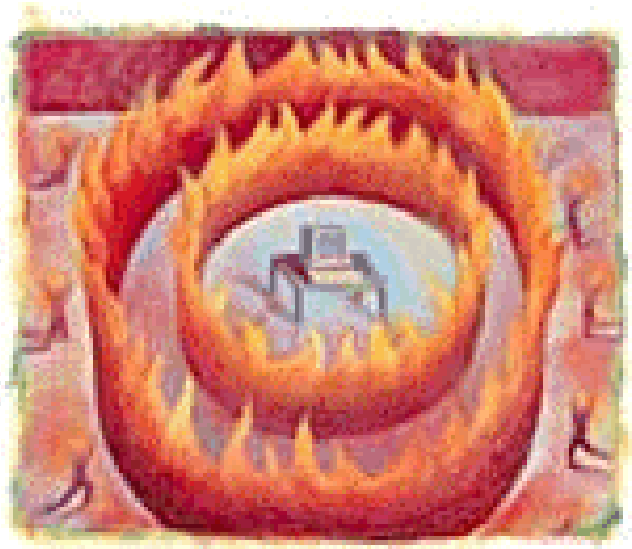


Intranet i Internet - zagrożenia

- Podsłuchiwanie - poufność danych
- Modyfikacja przesyłanych danych - integralność
- Podszywanie się - autoryzacja
- Włamanie i kradzież danych
- Włamanie i modyfikacja danych
- Włamanie i zniszczenie danych
- Denial of Service - uniemożliwianie pracy

Firewall - "ściana ognia" ?

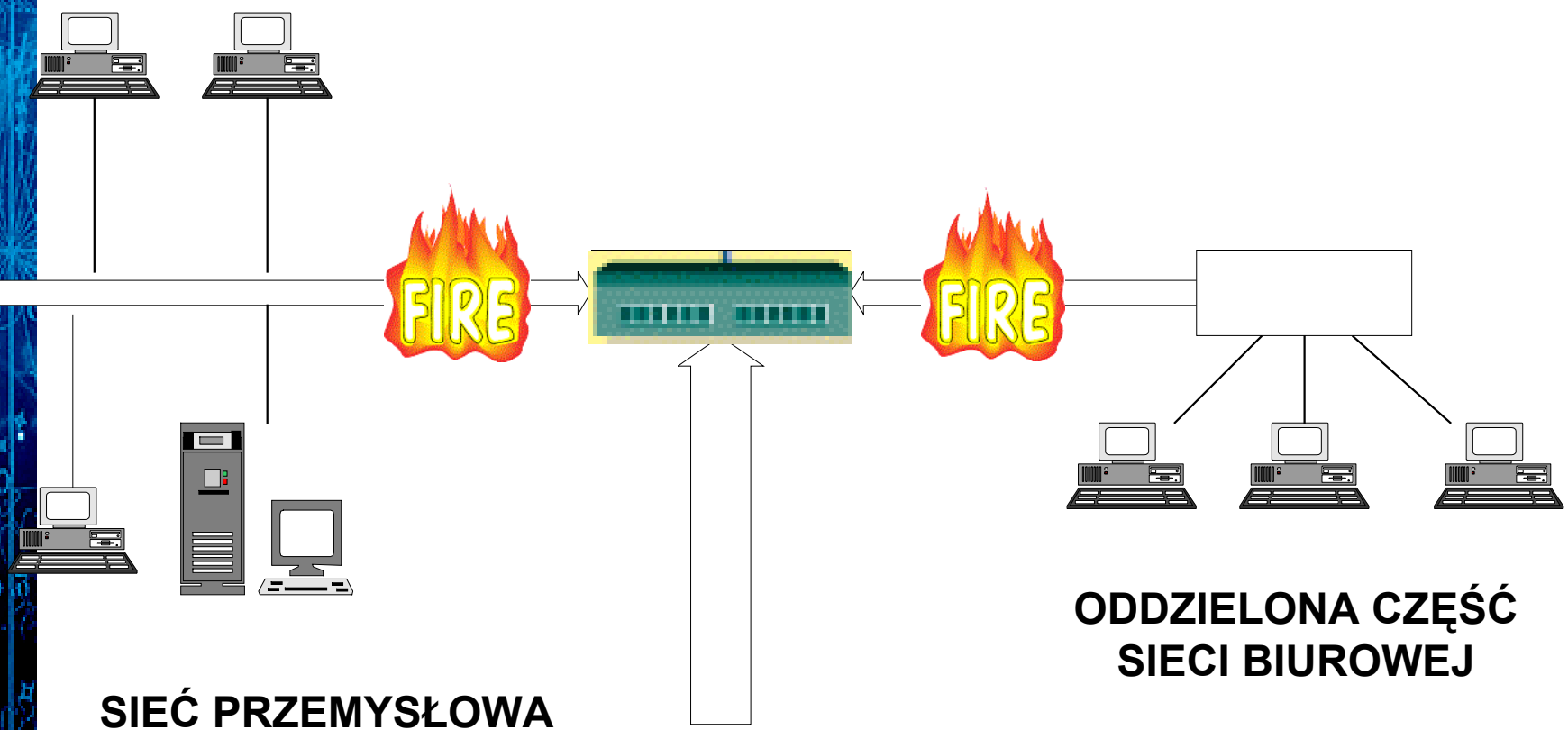
- Firewall = sprzęt + oprogramowanie + polityka bezpieczeństwa
- Kontrola dostępu
- Pełen audyt - logowanie
  - autoryzacja
  - szyfrowanie
  - cache
  - zarządzanie adresami



Firewall wewnątrz intranetu - po co ?

- Ograniczenie dostępu do części zasobów (podsieci) firmy ze względu na poufność danych - ochrona danych
- Ograniczenie dostępu do części przemysłowej Intranetu np. część sieci zajmująca się monitorowaniem i sterowaniem produkcji - bezpieczeństwo
- Kontrola ruchu i audyt w Intranecie - ochrona przed własnymi pracownikami

Firewall wewnątrz Intranetu

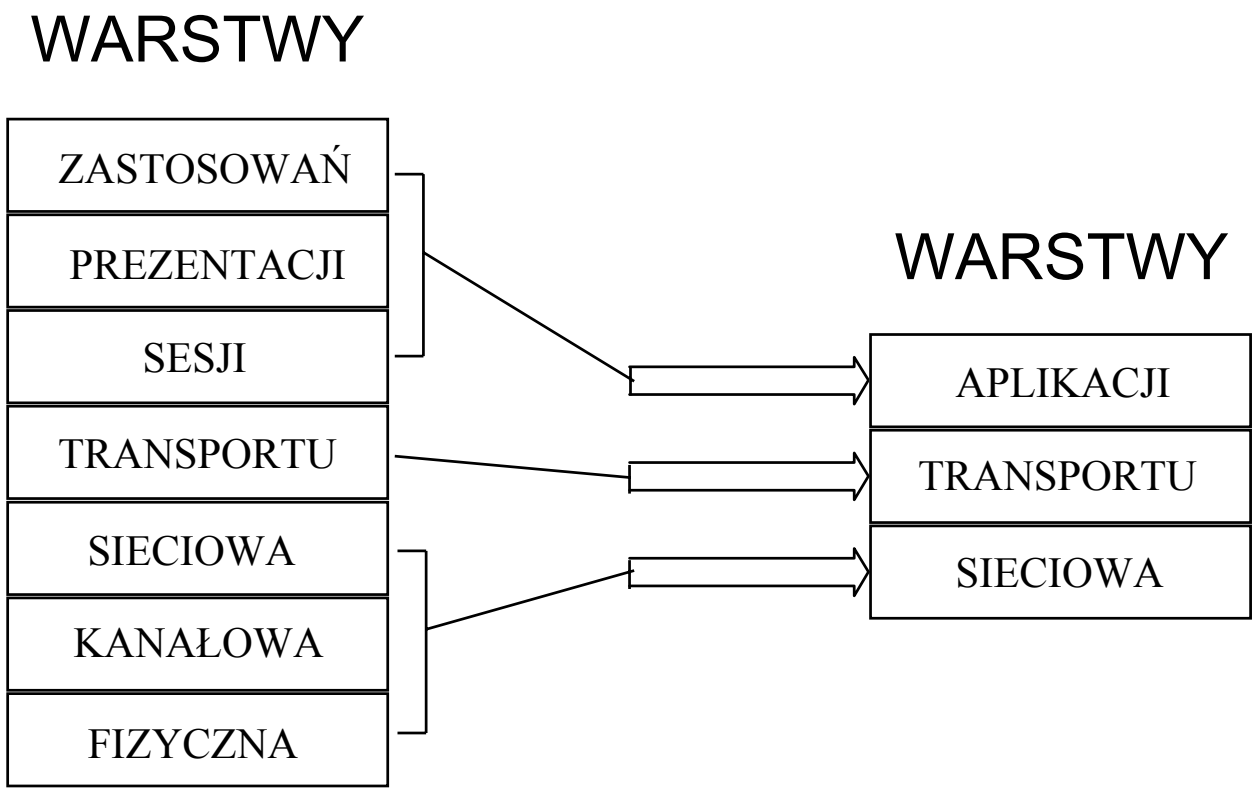


Rodzaje systemów Firewall

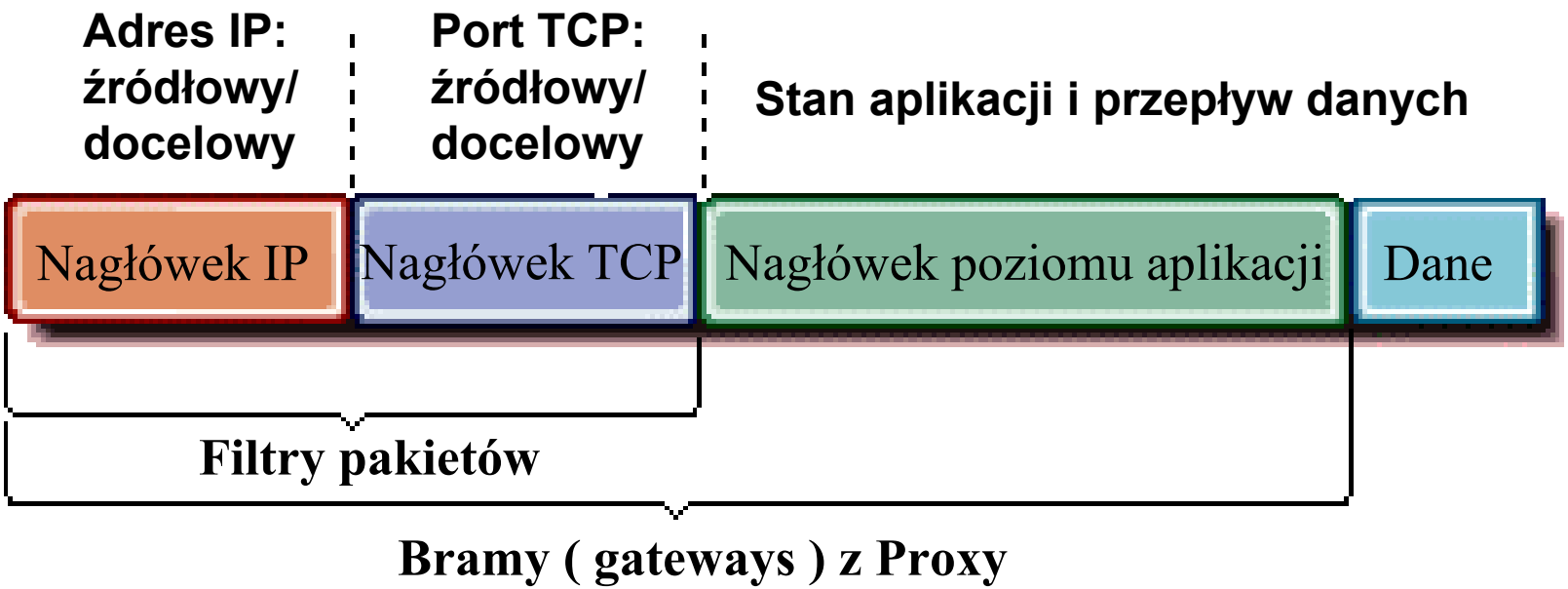
- Model OSI - w którym miejscu jakie informacje ?

- Filtrowanie pakietów (packet filtering)
- Analiza stanu połączeń (circuit level firewall)
- Proxy (application level firewall)

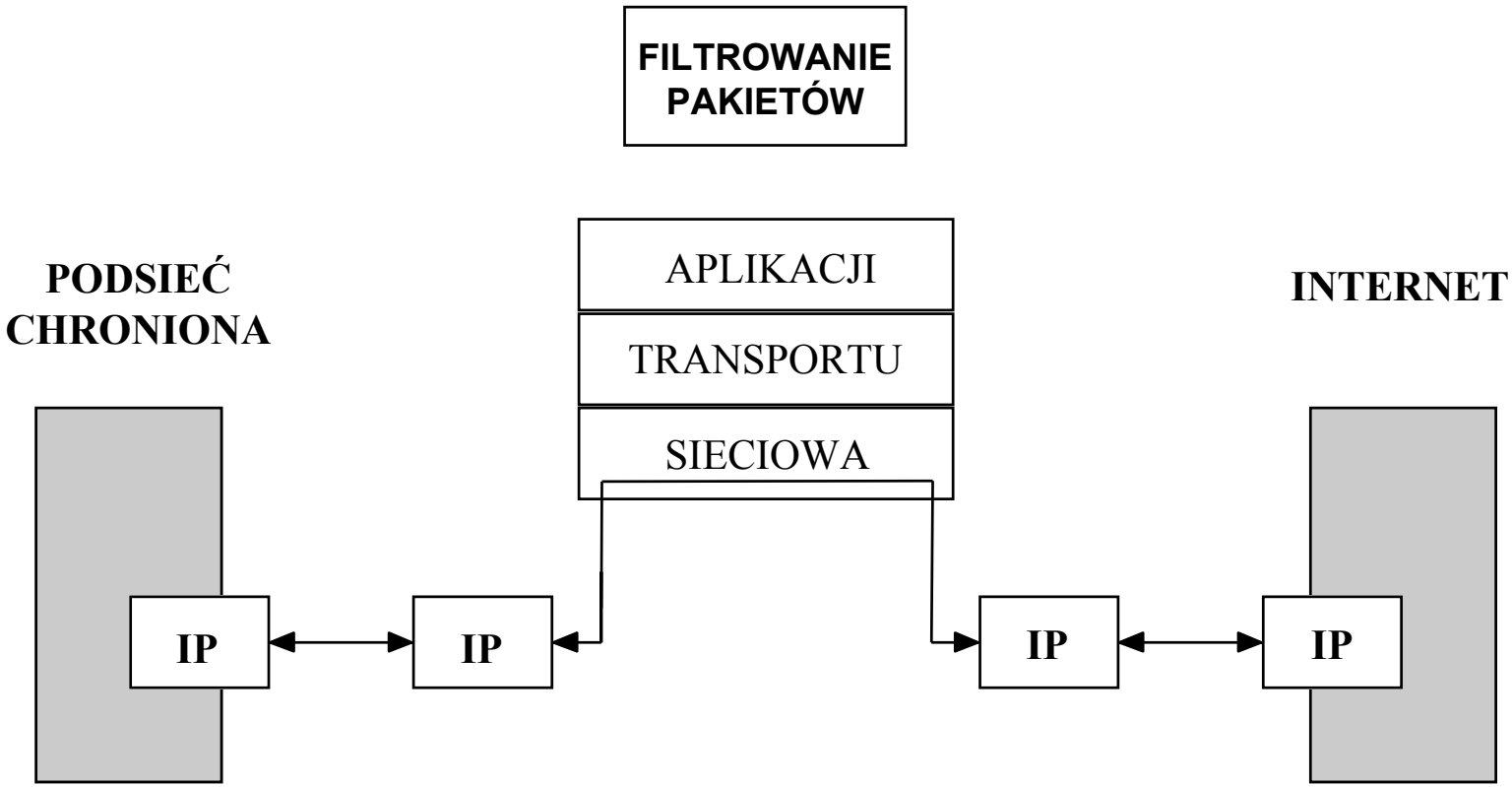
Model OSI - uproszczenie



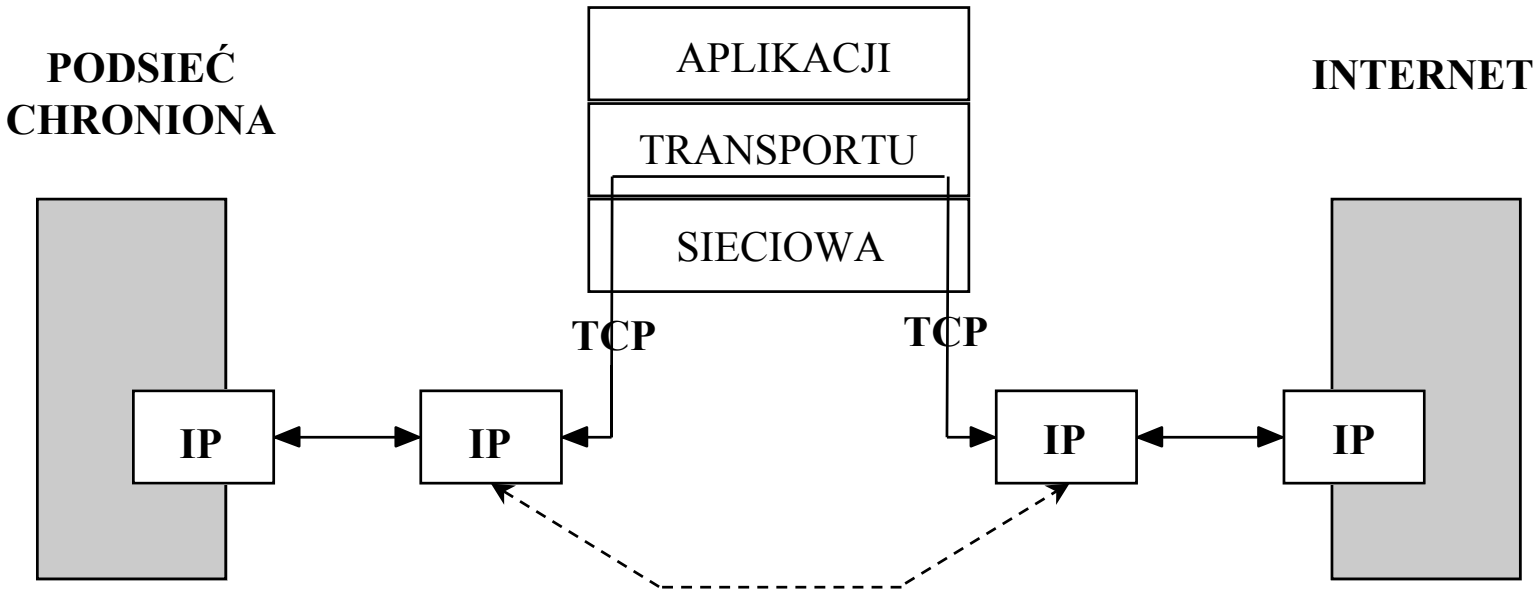
Model OSI - w którym miejscu jakie informacje ?



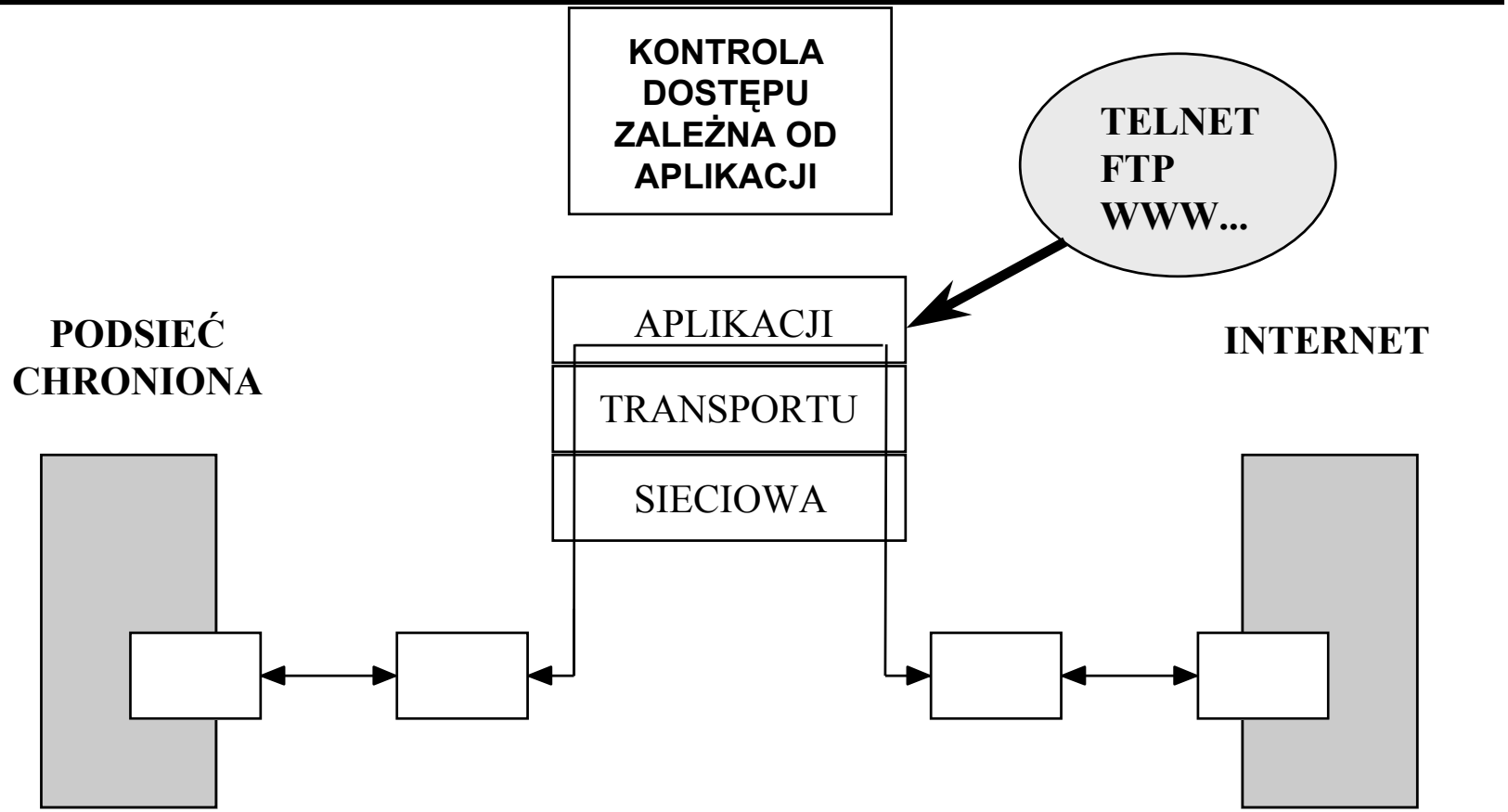
Filtrowanie pakietów (packet filtering)



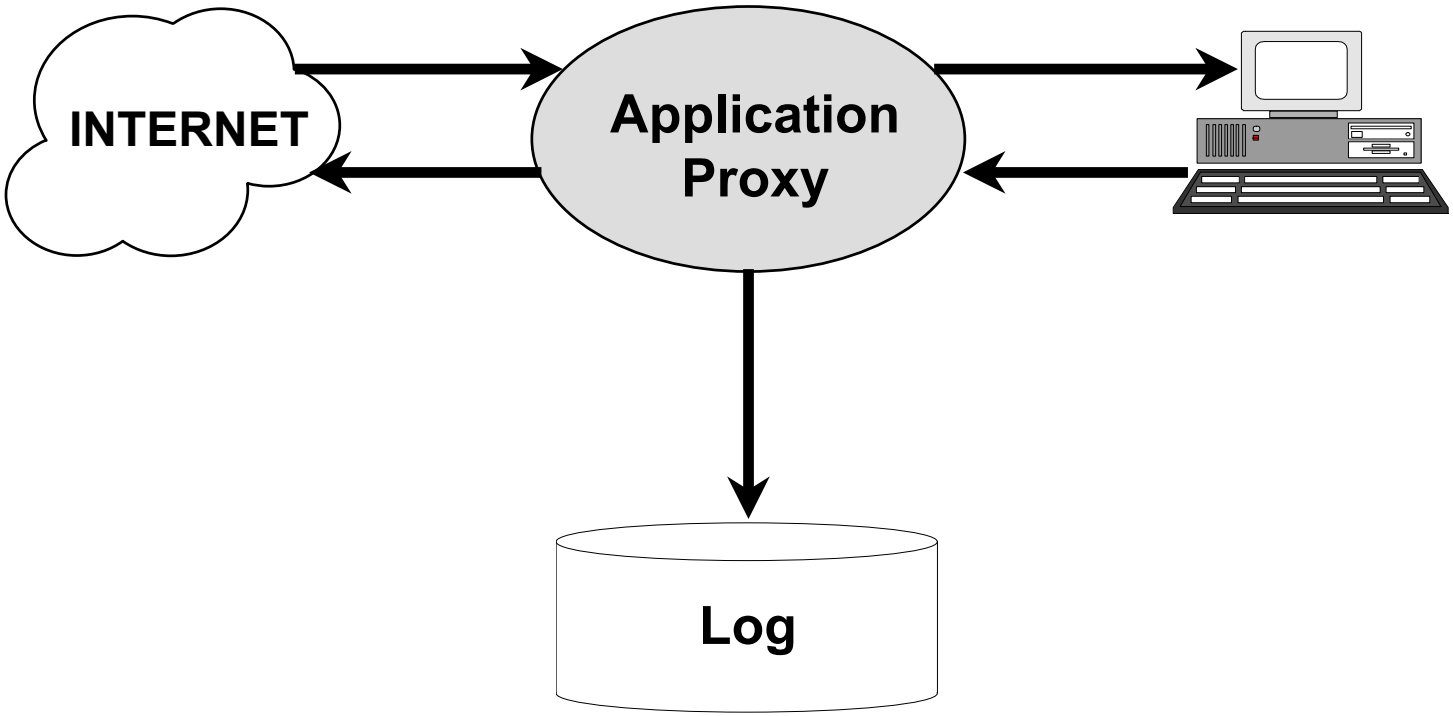
Analiza stanu połączeń (circuit level firewall)



Proxy (application level firewall)



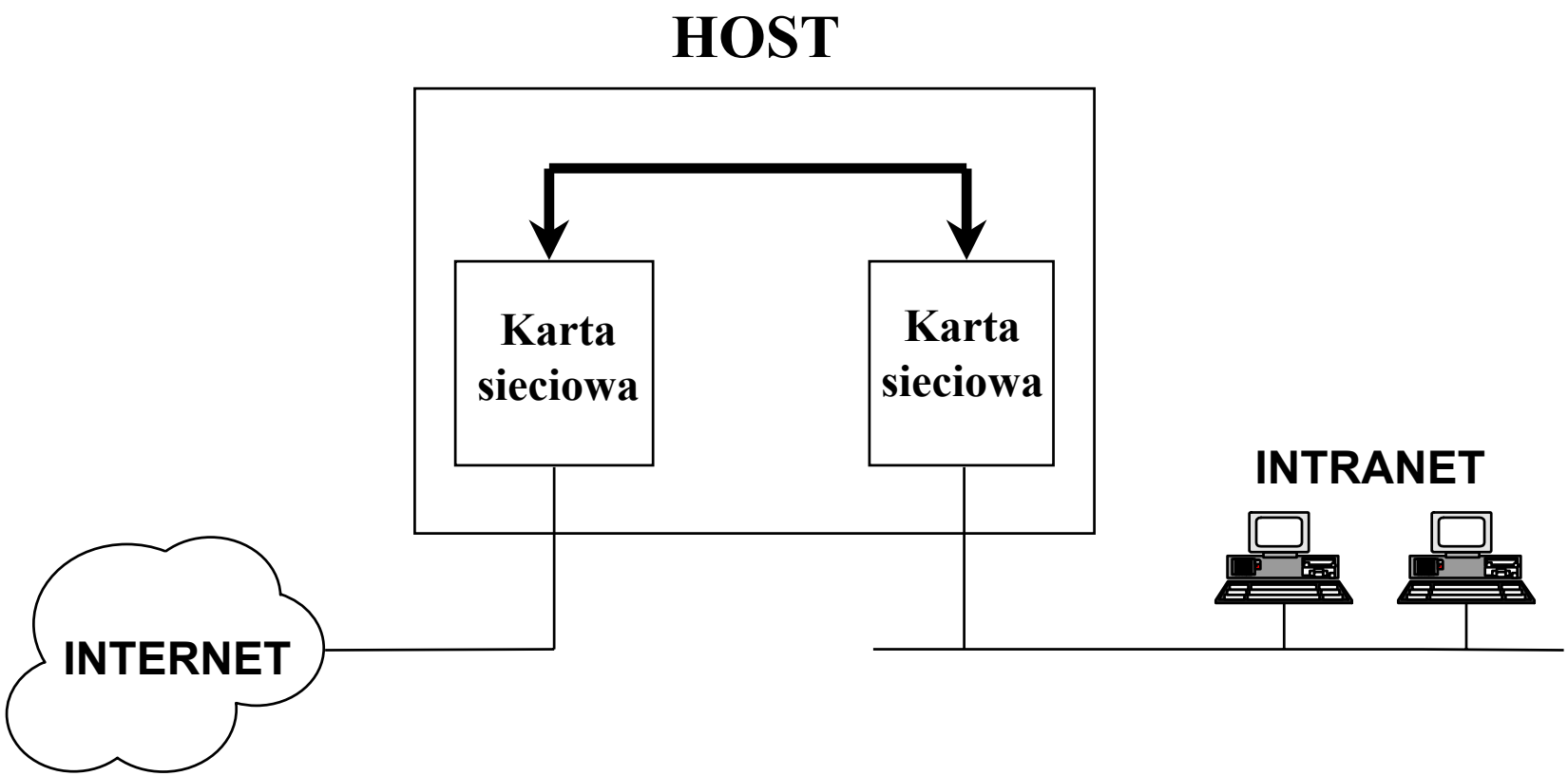
Proxy (application level firewall)



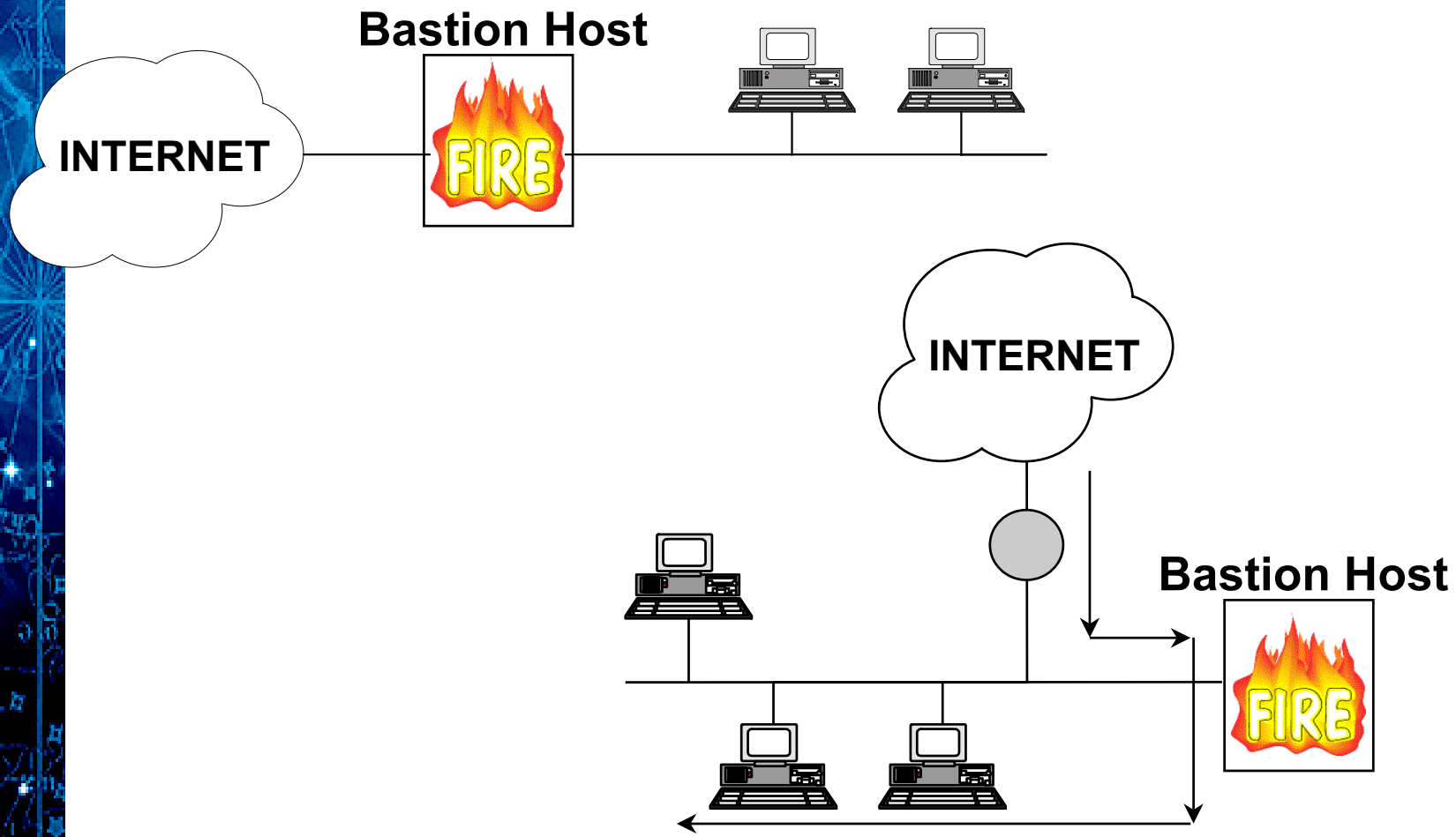
Główne koncepcje stosowania

- Dual-Homed Host
- Bastion Host
- Demilitarized Zone (DMZ)
- Screening router
- Screened subnet

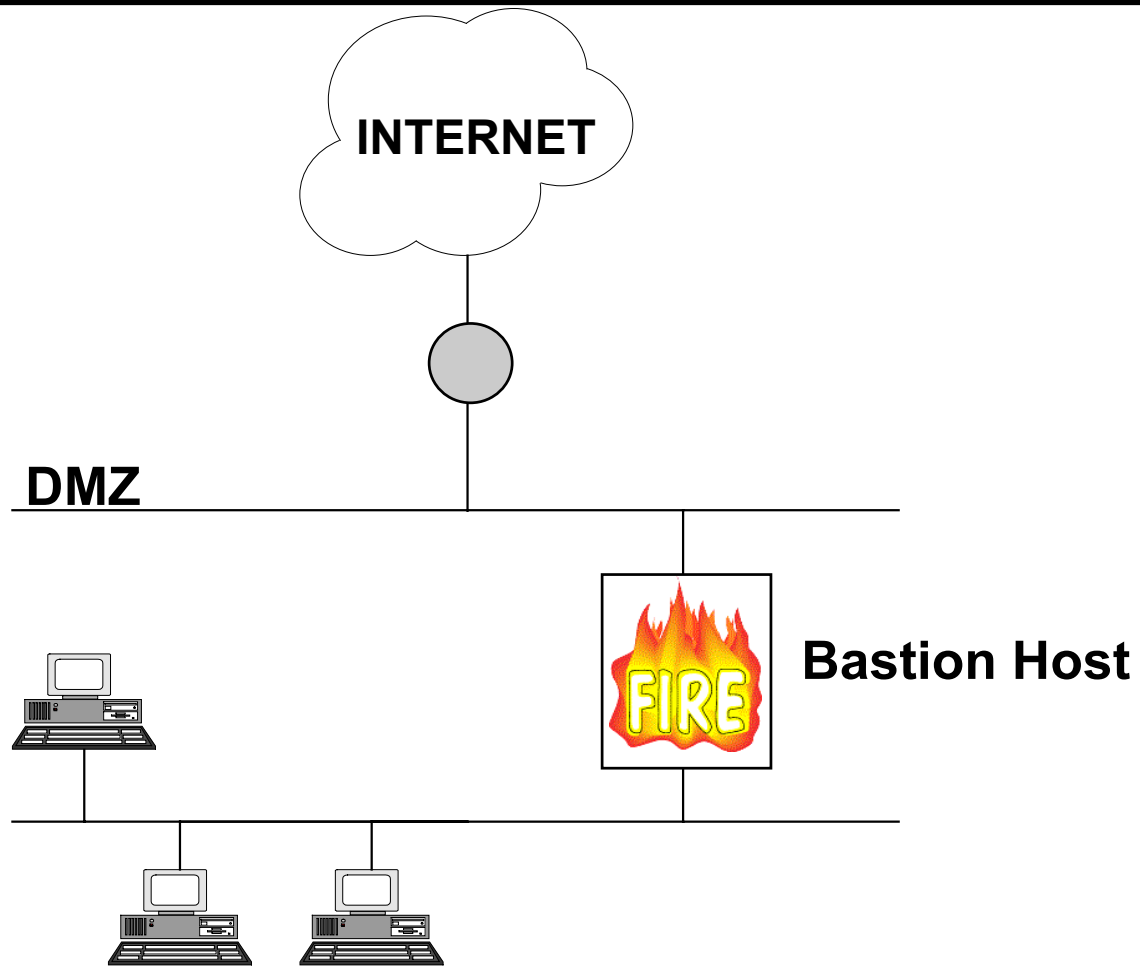
Dual-Homed Host



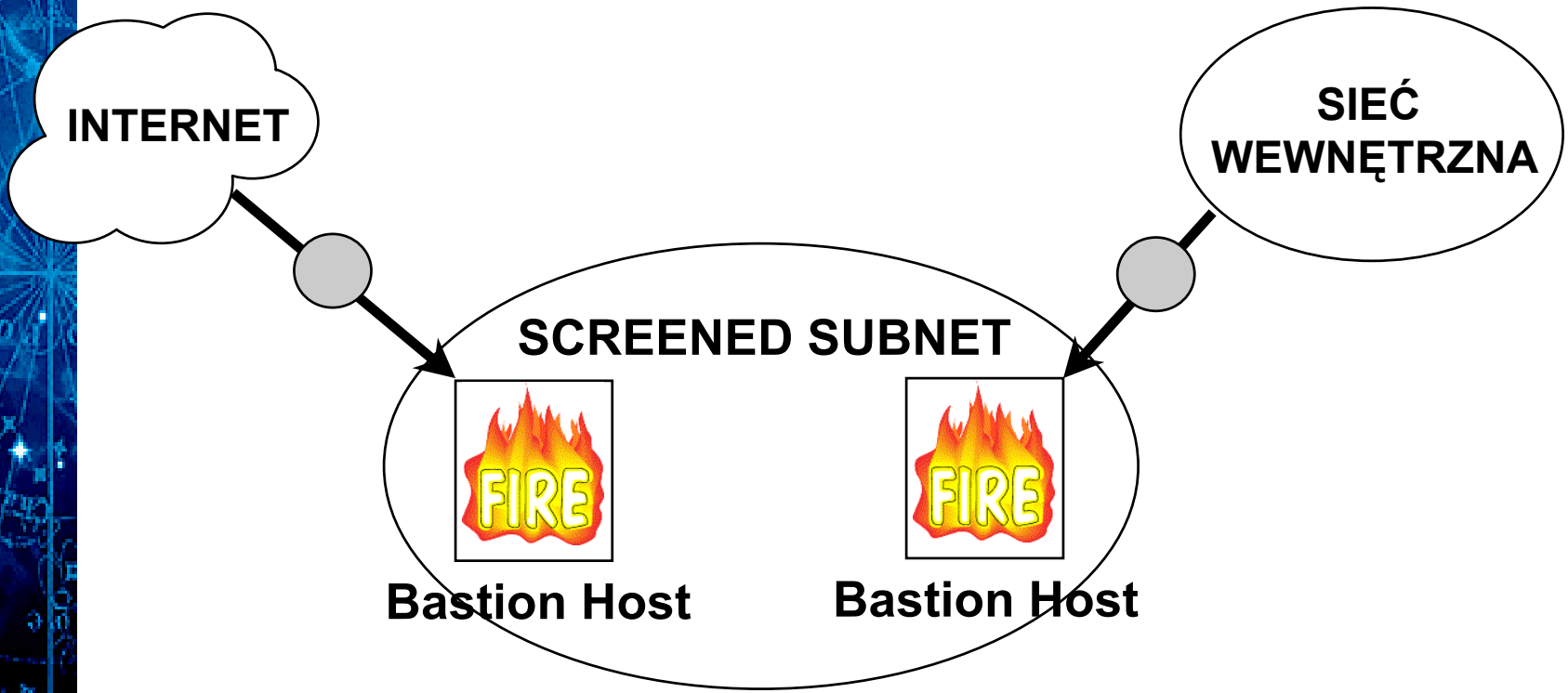
Bastion Host



Demilitarized Zone (DMZ)



Screened Subnet



Filtrowanie pakietów - zalety i wady

- ✓ Szybkość
- ✓ "Przeźroczystość"

- ✗ Trudna konfiguracja
- ✗ Mała elastyczność
- ✗ W przypadku rozwiązań sprzętowych kłopotliwe i drogie upgrade'y

Proxy - zalety i wady

- ✓ Z zasady nie przepuszcza żadnych pakietów
- ✓ Pozwala wymusić dodatkową autoryzację
- ✓ Operuje na poziomie konkretnego protokołu
- ✓ Umożliwia wymuszenie surowych reguł bezp.

- ✗ Uzależnienie od protokołu (zmiany, upgrade'y)
- ✗ Słaba wydajność
- ✗ Ograniczenie ilości usług

Firewall - wybór systemu operacyjnego

- **DOS** (niektóre filtry pakietowe: KarlBridge, Drawbridge)
- **Unix** - systemy komercyjne (praktycznie wszystkie Firewalle)
- **Windows NT** (tak, pod warunkiem, że wymieniana jest część SO)
- **Unix** - systemy niekomercyjne: Linux, BSD. Dostępne są narzędzia darmowe.

Firewall - wybór platformy sprzętowej

Skrajności:

- od PC 386
- do potężnego komputera RISC

Czynniki:

- enkrypcja
- logowanie
- przepustowość sieci (10 Mbit/s, 100 Mbit/s)

Systemy Firewall - cechy produktów

- NAT (Network Address Translation)
- IP-Masquerading
- filtrowanie z kojarzeniem z wyższymi warstwami OSI
- filtracja dla DNS
- filtrowanie ActiveX/ Java
- stateful inspection

Systemy Firewall - ekonomia

- ceny i polityka licencyjna producentów

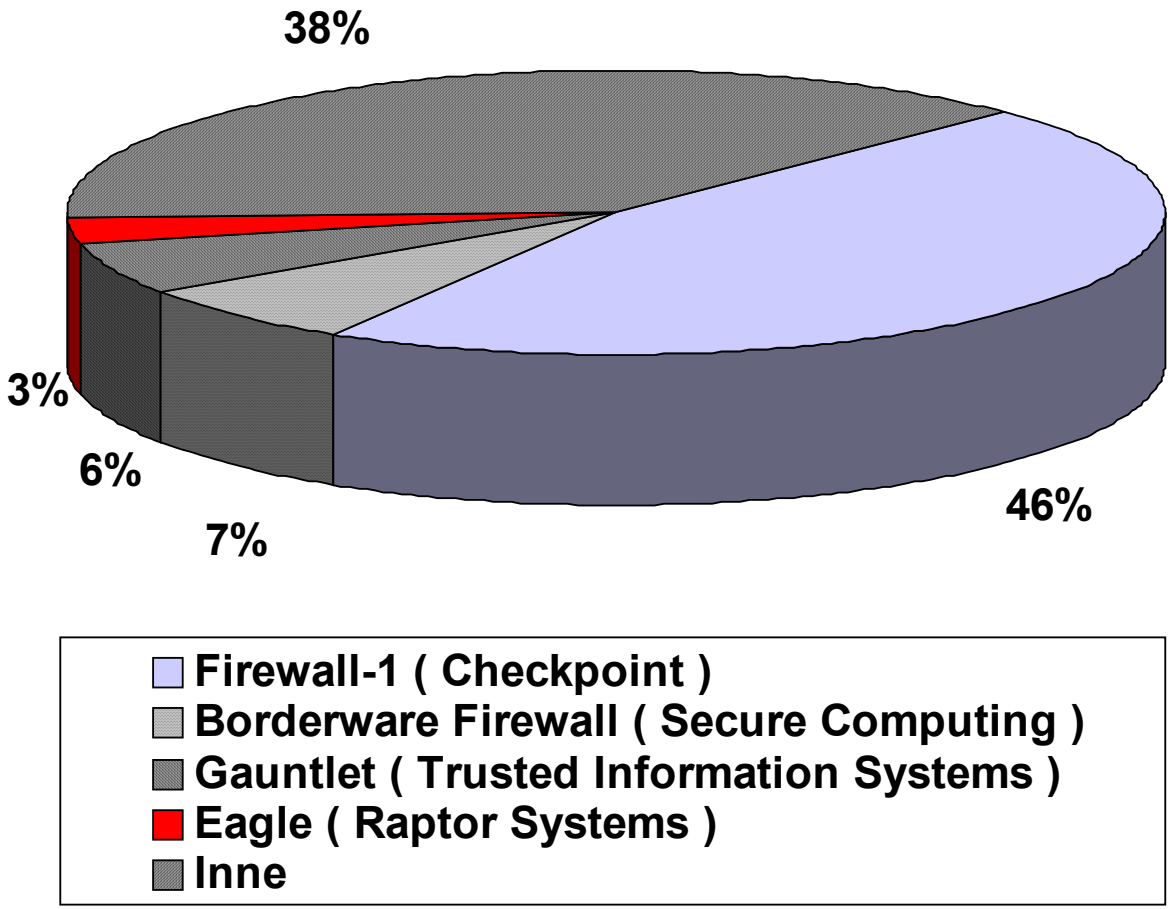
Koszty stworzenia systemu Firewall:

- zakup sprzętu
- zakup oprogramowania
- szkolenia
- zarządzanie
- ograniczenie niektórych usług

Systemy Firewall - producenci

- producenci niezależni (np. CheckPoint, Raptor, Secure Computing, Trusted Information Systems)
- producenci dostarczający Firewall ze swoim sprzętem i oprogramowaniem:
  - rozwiązania zamknięte (np. IBM)
  - rozwiązanie otwarte (np. Digital)
- oprogramowanie freeware/shareware/GNU

Systemy Firewall - podział rynku



Produkty - BorderManager

- centralne zarządzanie siecią (plus NDS, LDAP)
- routing, w tym RAS (Remote Access Service)
- filtrowanie pakietów + NAT (IPX, IP)
- analiza stanu połączeń i proxy
- hierarchiczny cache w proxy
- VPN
- ceny od 2500 USD (dla 5 użytkowników)

Produkty - Cisco PIX

- system typu black-box
- analiza stanu połączeń
- cut-through proxy
- NAT i PAT (Port Address Translation)
- filtrowanie appletów Java
- "przeźroczysty" dla użytkownika
- ceny od 9000 USD