Podstawowe funkcje zapory

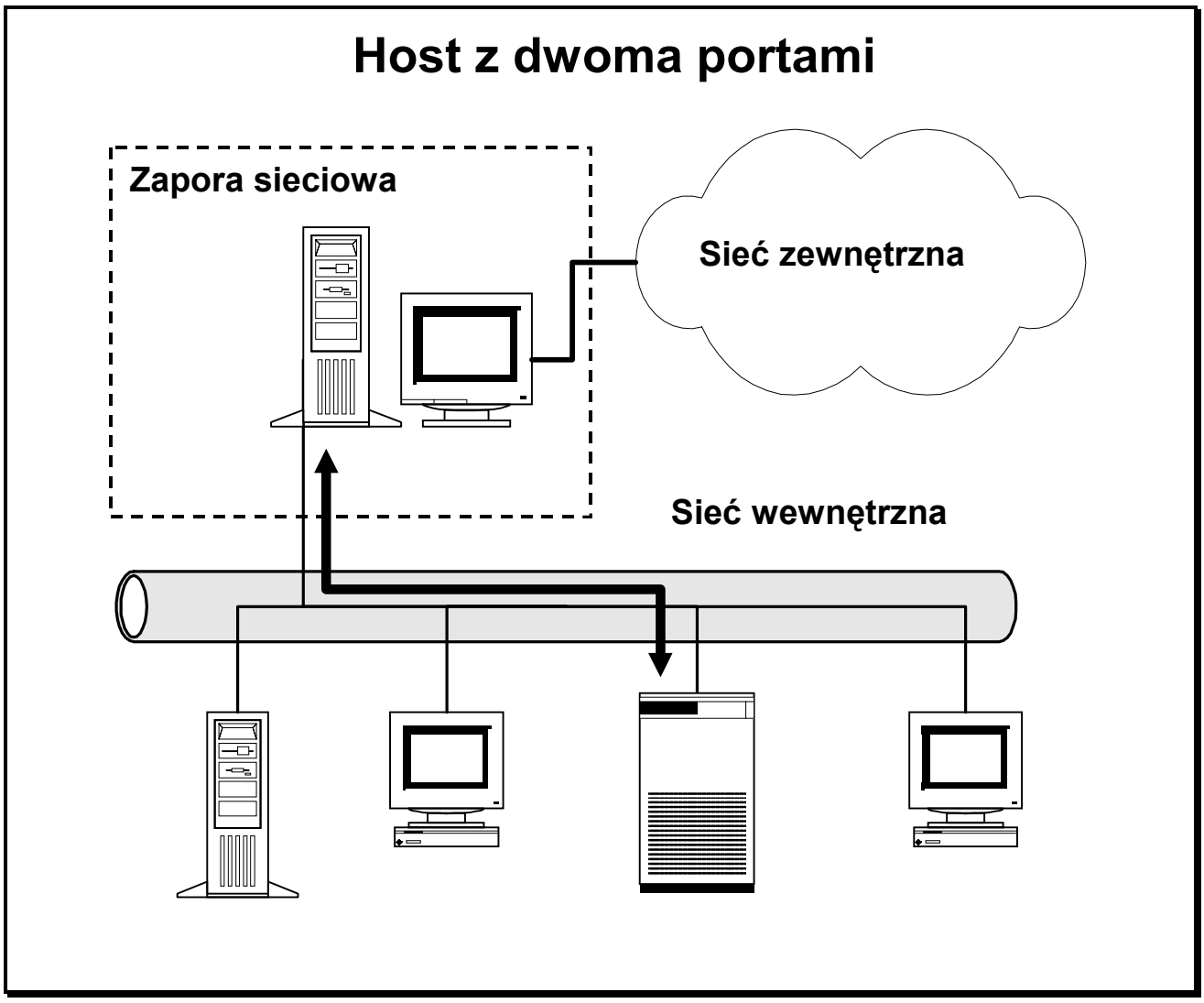
- Blokowanie dostępu
- Monitorowanie komunikacji
- Wykrywania intruzów
- Tunelowanie (*Virtual Private Network*).
- Uwierzytelnianie

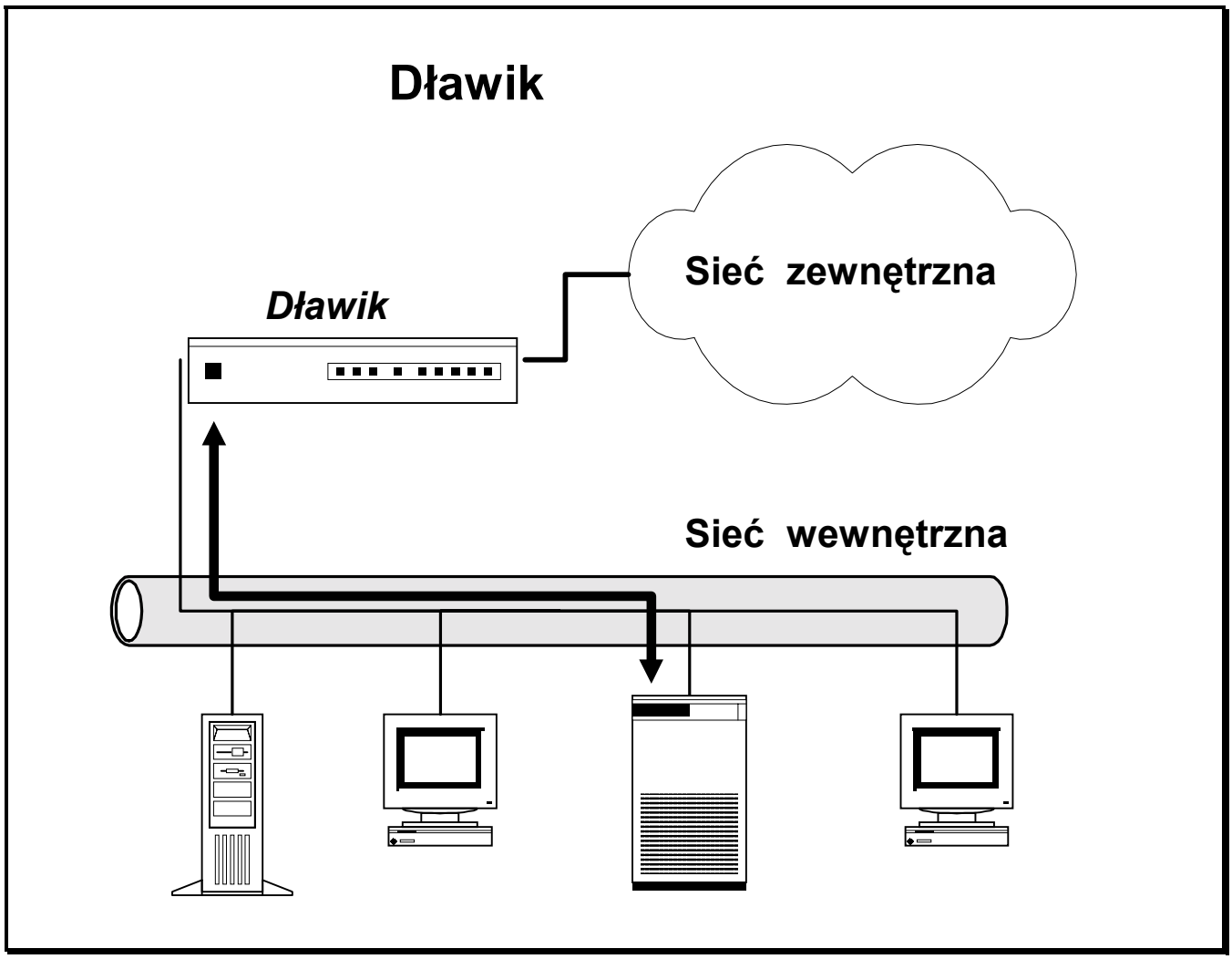
Podstawowe mechanizmy zapory

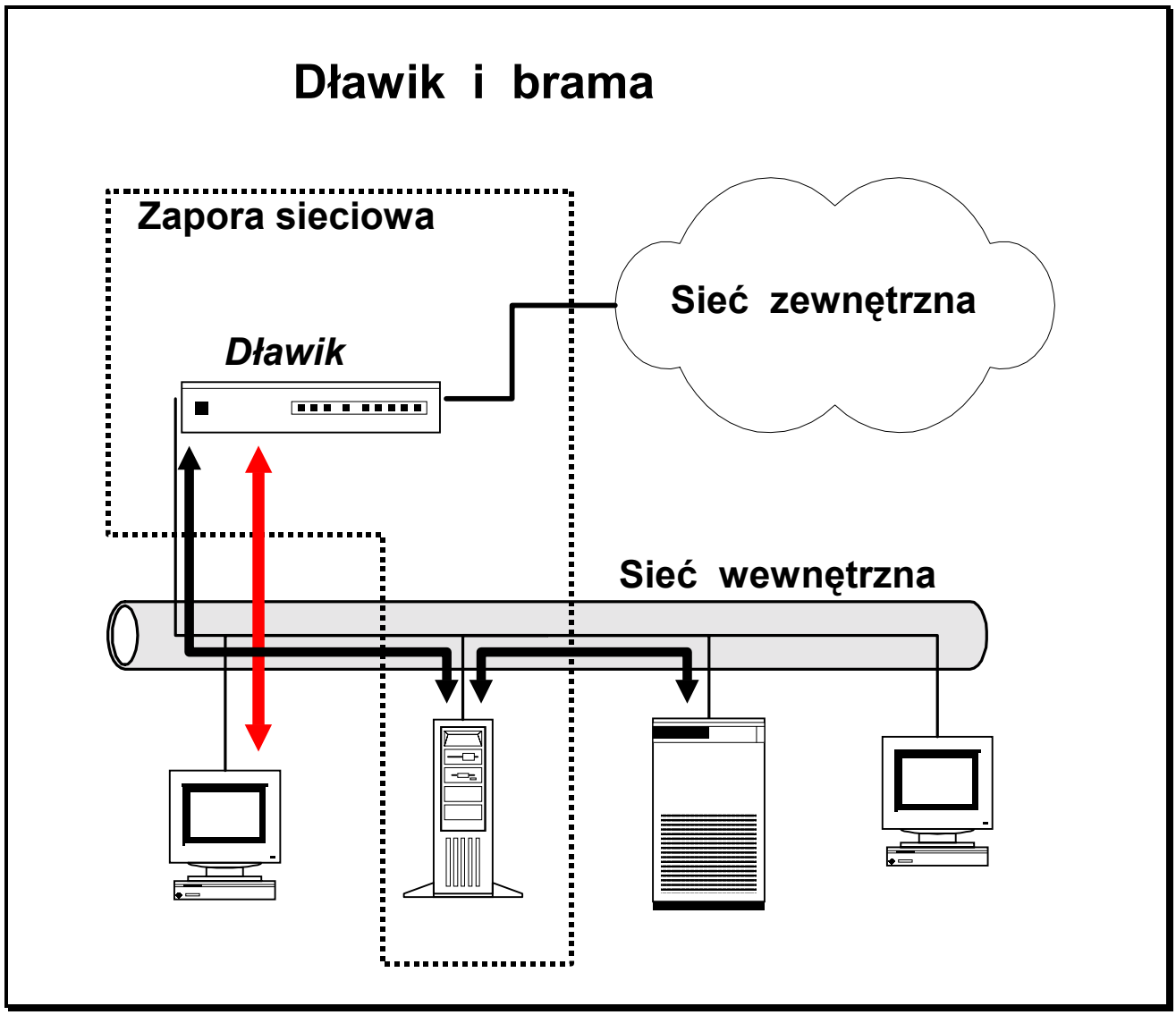
- Filtrowanie pakietów (*packet filtering*)
- Translacja adresów (*network address translations*)
- Usługi proxy (*proxy serwers*)

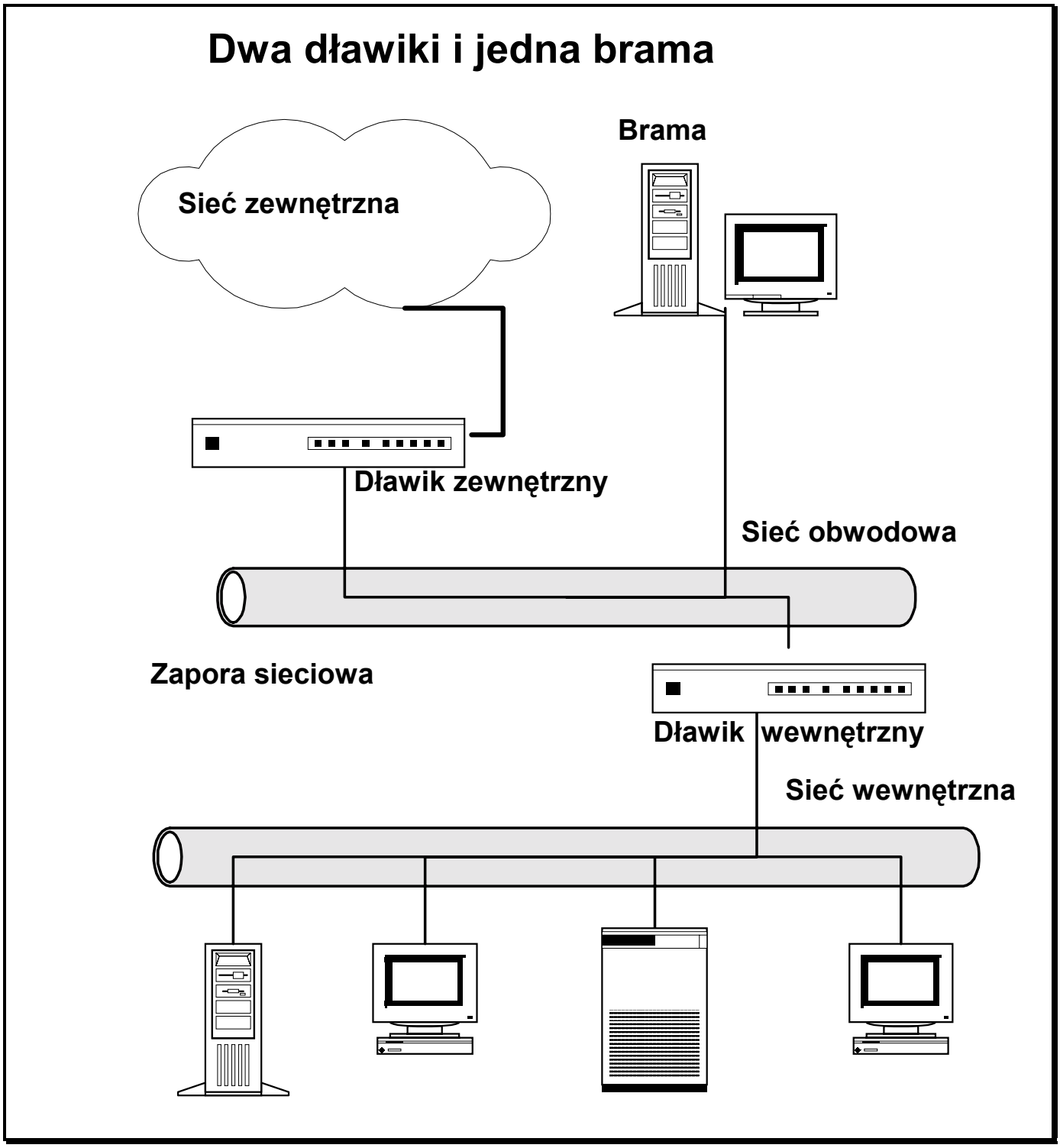
Komponenty zapory

- Dławiki
- Bramy


Host z dwoma portami
Zapora sieciowa
Sieć zewnętrzna
Sieć wewnętrzna


Dławik
Sieć zewnętrzna
Dławik
Sieć wewnętrzna

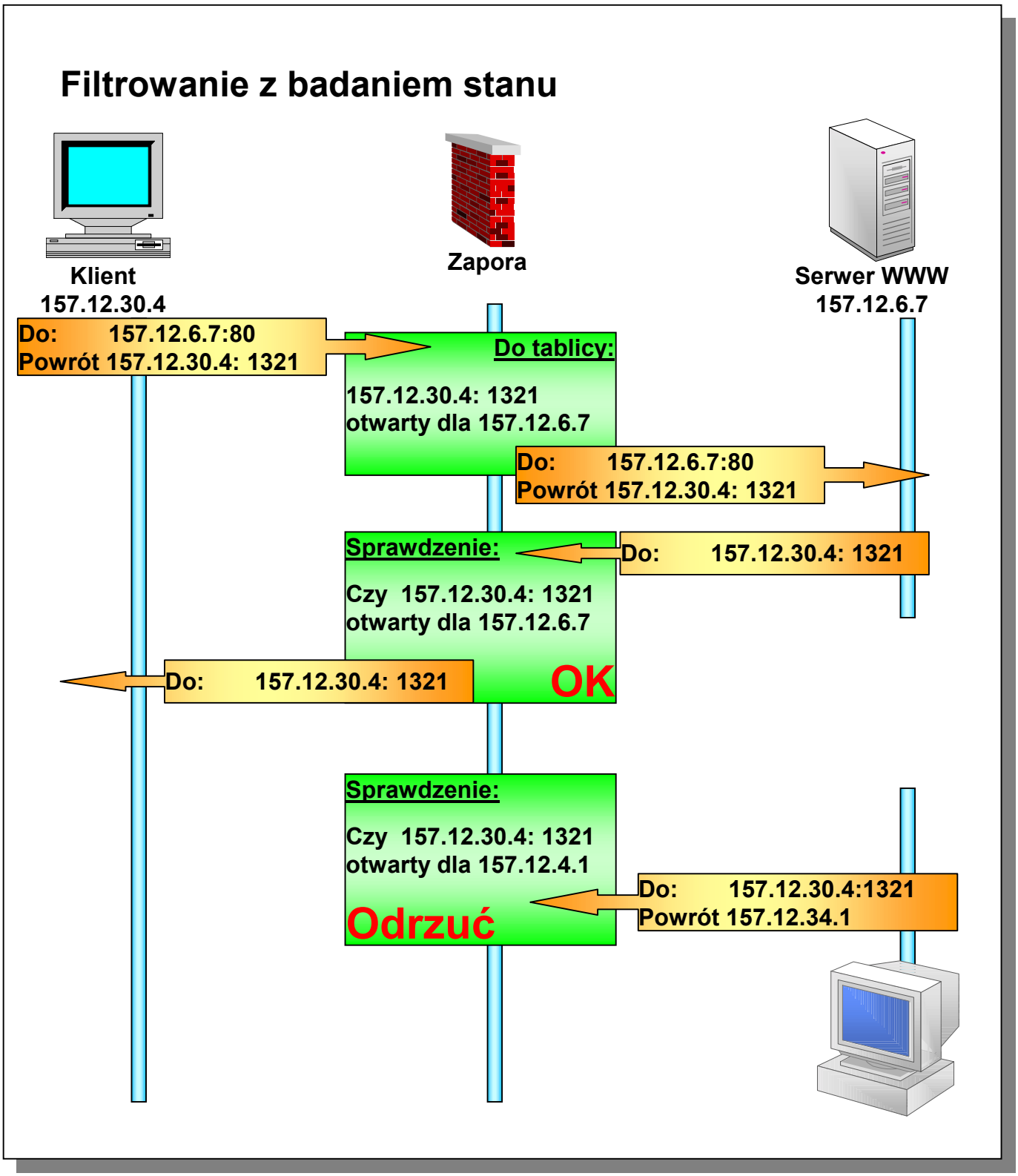

Dławik i brama
Zapora sieciowa
Sieć zewnętrzna
Dławik
Sieć wewnętrzna


Dwa dławiki i jedna brama
Brama
Sieć zewnętrzna
Dławik zewnętrzny
Sieć obwodowa
Zapora sieciowa
Dławik wewnętrzny
Sieć wewnętrzna

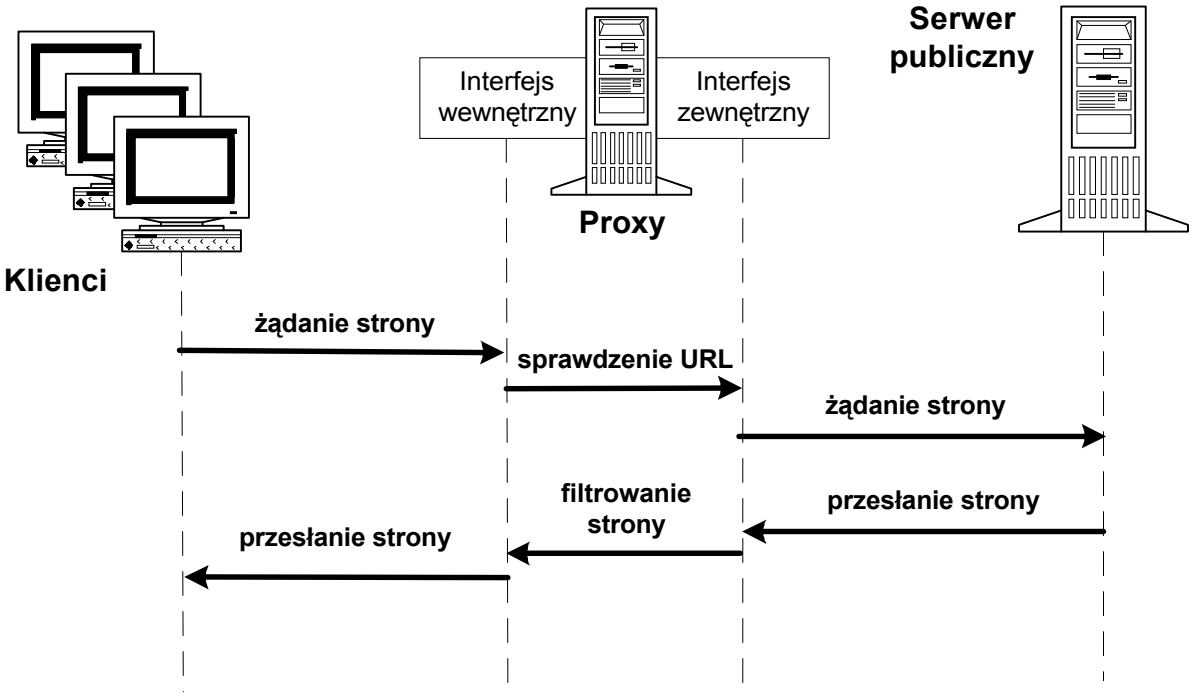
Bezstanowe filtrowanie pakietów

Filtry bezstanowe

- **Filtrowanie adresów IP**
- **Filtrowanie portów**
  - ***Telnet,***
  - ***NetBIOS Session***
  - ***POP***
  - ***NFS***
  - ***X Windows.***
- **Routing źródłowy**
- **Fragmentacja**


Filtrowanie z badaniem stanu
Klient
157.12.30.4
Zapora
Serwer WWW
157.12.6.7
Do: 157.12.6.7:80
Powrót 157.12.30.4: 1321
Do tablicy:
157.12.30.4: 1321
otwarty dla 157.12.6.7
Do: 157.12.6.7:80
Powrót 157.12.30.4: 1321
Sprawdzenie:
Czy 157.12.30.4: 1321
otwarty dla 157.12.6.7
Do: 157.12.30.4: 1321
Do: 157.12.30.4: 1321
OK
Sprawdzenie:
Czy 157.12.30.4: 1321
otwarty dla 157.12.4.1
Odrzuć
Do: 157.12.30.4:1321
Powrót 157.12.34.1

Usługa proxy



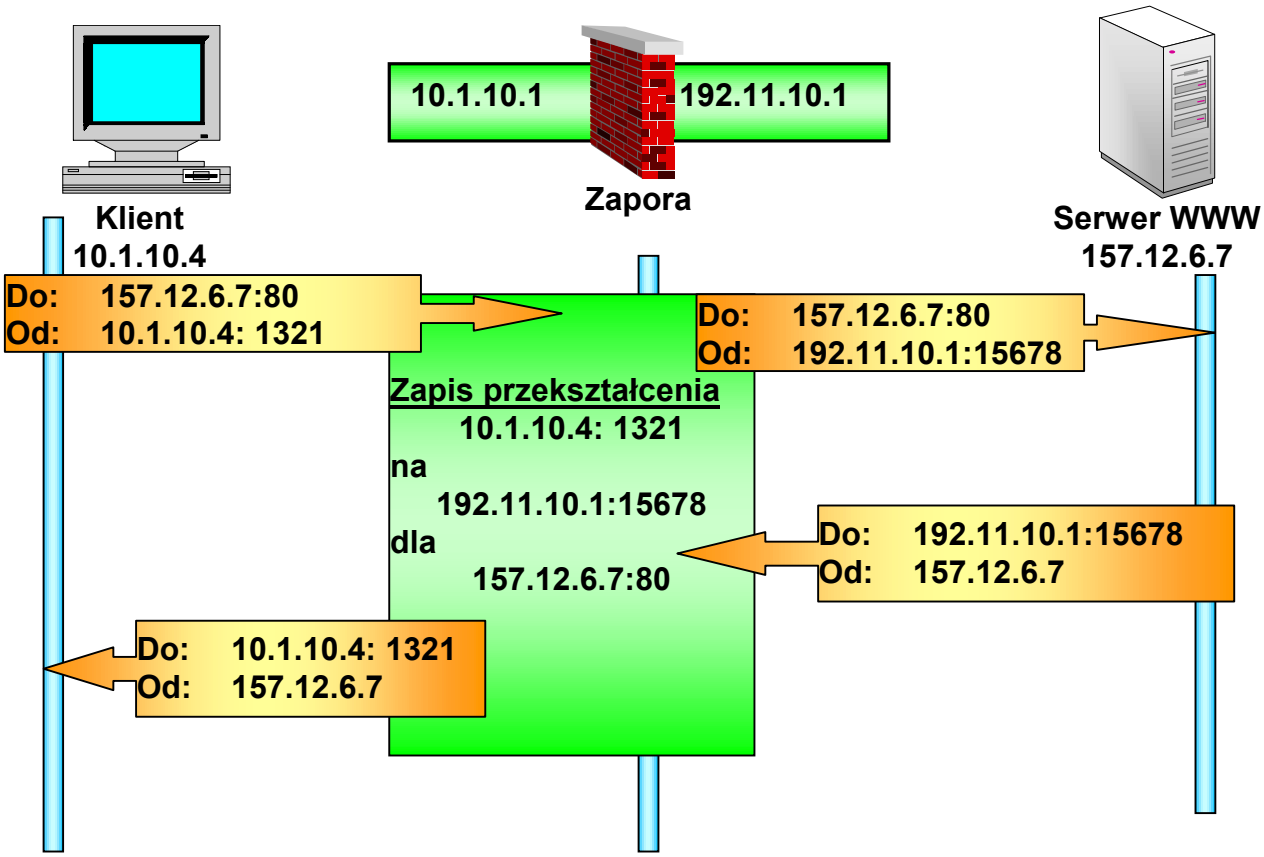
Zalety proxy

- Ukrywanie klienta przed światem zewnętrznym
- Blokowanie niebezpiecznych URL
- Filtrowanie niebezpiecznej zawartości (wirusy, konie trojańskie)
- Badanie spójności przesyłanej informacji
- Eliminacja routingu między sieciami
- Zapewnienie pojedynczego punktu dostępu (nadzorowanie i rejestracja zdarzeń)

Wady proxy

- pojedynczy punkt - wrażliwość na awarie
- oprogramowanie klienckie musi współpracować z proxy
- każda usługa musi mieć proxy
- proxy nie chroni systemu operacyjnego
- małe bezpieczeństwo konfiguracji domyślnych
- zatory

Translacja adresów (NAT)



Translacja statyczna
(*static translation*)

Translacja dynamiczna
(*dynamic translation*)

Translacja ze zrównoważonym obciążeniem
(*load balancing translation*)

Translacja ze zwielokrotnionymi połączeniami
(*network redundancy translation*)

Etapy budowy zapory sieciowej

1. Planowanie konfiguracji
    - Co chronić ?
    - Jaka jest topologia ?
    - Jakie są potrzeby w zakresie aplikacji i protokołów ?
    - Jakie są zależności służbowe ?
    - Jaka powinna być konfiguracja zapory ?
    - Kupić czy budować ?
2. Zdefiniowanie reguł dostępu do zasobów sieciowych
3. Znalezienie odpowiedniej zapory
4. Instalacja i konfiguracja zapory
5. Drobiazgowe testowanie zapory

Podsumowanie:

Przed przystąpieniem do wyboru lub budowy zapory należy odpowiedzieć na pytania

- **jakie zasoby w naszej sieci powinny być chronione,**
- **przed kim należy chronić naszą sieć,**
- **czy jest konieczna ochrona sieci od wewnątrz,**
- **co nam grozi w razie włamania, jakie straty możemy ponieść w wyniku włamania,**
- **jakie serwisy i na jakich zasadach chcemy udostępnić na zewnątrz,**
- **czy potrafimy określić strefy, które wymagają różnych poziomów ochrony,**
- **czy koszty związane z ochroną zasobów nie przewyższają wartości chronionych dóbr.**

Zakres funkcji *firewalli*:

- **filtrowanie pakietów na różnym poziomie,**
- ***statefull inspection* - sprawdzanie pakietów w kontekście pakietów uprzednio badanych,**
- ***application-level gateway* - analiza pakietów warstw aplikacyjnych,**
- **translacja i ukrywanie adresów - NAT (*Network Address Translation*), *IP masquering,***
- **tworzenie sieci wirtualnych VPN wraz z metodami szyfrowania,**
- **wyszukiwanie wirusów - CVP (*Central Virus Protection*),**
- **serwery *proxy* dla różnych protokołów,**
- **uwierzytelnianie dostępu do korzystania z konkretnych protokołów,**
- **tworzenie tzw. strefy zdemilitaryzowanej DMZ (*Demilitarized Zone*) - wydzielonej sieci z serwerami o publicznym dostępie,**
- **możliwość budowy zapór hybrydowych i rozproszonych,**
- **alarmowanie o przypadkach naruszenia bezpieczeństwa i tworzenie stosownych raportów.**

Literatura:

1. S.Garfinkel, G.Spafford. *Practical Unix and Internet Security.* O'Reilly & Associates 1996 (*tłum*. RM 1997).
2. V.Ahuja. *Network & Internet Security.* Academic Press 1996 (*tłum*. MIKOM 1997).
3. D.Atkins. *Internet Security: Professional Reference.* New Riders Publishing 1997 (*tłum*. LT&P 1997).
4. M. Kaeo. *Designing Network Security. Cisco Press 1999 (tłum.* MIKOM 2000*).*
5. L.Klander. *Hacker Proof*. Jamsa Press, 1997 (*tłum.* MIKOM 1998).
6. M. Strebe, Ch. Perkins, *Firewalls*. SYBEX, Inc. 2000, (*tłum* MIKOM 2000).
7. Z. Suski, P. Kołodziejczyk. *Ochrona sieci lokalnej za pomocą zapory sieciowej,* Biuletyn Instytutu Automatyki i Robotyki WAT nr 14/2000. Warszawa 2000.