# Eksploatacja i bezpieczeństwo systemów

**dr inż. Mirosław Mazurek**

Zakład Systemów Złożonych
**Bud. F, pok. 305, tel. 17 865 11 04**

# Zapora sieciowa

**Zapora sieciowa jest umieszczana między siecią wewnętrzną organizacji i siecią zewnętrzną.**

**Dostarcza ona prostego mechanizmu kontroli ilości i rodzaju ruchu sieciowego między obydwoma sieciami.**

**Podstawowym jej zadaniem jest ograniczenie przepływu danych między sieciami.**

**Podstawowe strategie definiowania zapory:**

**Domyślne przepuszczanie polega na określeniu zbioru warunków, których spełnienie będzie powodowało blokowanie danych. Każdy host lub protokół nie objęty tą polityką będzie przepuszczany.**

**Domyślne blokowanie polega na określeniu protokołów, które będą mogły przechodzić przez zaporę oraz hostów, które będą mogły przesyłać przez nią dane i z którymi komputery w sieci wewnętrznej będą się mogły komunikować. Wszystkie elementy nie objęte definicjami będą blokowane.**

# Zadania zapory sieciowej

**Do podstawowych działań realizowanych przez zaporę należy zaliczyć:**

**Blokowanie dostępu do całej sieci z określonych miejsc w sieci zewnętrznej.**

**Blokowanie dostępu do wybranych serwerów i usług określonym użytkownikom.**

**Monitorowanie komunikacji między sieciami (np. rejestracja końcowych punktów połączeń i ilość przesyłanych danych)**

**Podsłuchiwanie i rejestrowanie komunikacji między sieciami w celu badania przypadków penetracji sieci, wykrywania intruzów i wewnętrznych sabotażystów.**

**Tunelowanie. Automatyczne szyfrowanie i deszyfrowanie pakietów.**

**Uwierzytelnianie. Użytkownicy sieci zewnętrznej muszą uwierzytelnić się wobec zapory.**

# Zadania zapory sieciowej

**Podstawowe mechanizmy spotykane w implementacjach zapór:**

**Filtrowanie pakietów (packet filtering)- odrzucanie pakietów nie spełniających reguł zapory.**

**Translacja adresów (network address translations) - dokonywanie zamiany adresu hosta wewnętrznego w celu ukrycia go przed zewnętrznym monitorowaniem.**

**Usługi proxy - dokonywanie połączenia na poziomie aplikacji w imieniu hosta wewnętrznego. Przerywa połączenie na poziomie warstwy sieciowej.**

# Filtrowanie pakietów

**Filtrowanie pakietów oparte jest na badaniu nagłówków pakietów i odrzucaniu pakietów, które nie odpowiadają określonej specyfikacji.**

**Istnieją dwa podstawowe typy filtrów pakietów:**

filtry bezstanowe (stateless),
filtry z badaniem stanów (statefull inspection).

**Filtry bezstanowe**

**Najczęściej filtrowanie oparte jest na takich polach jak:**

adres IP,
typ protokołu (UDP, TCP, ICMP) - ta informacja jest jednak na tyle ogólna, że zwykle dopuszcza się wszystkie protokoły,
port TCP/UDP,
informacja o wyborze trasy,
znacznik fragmentu.

# Filtrowanie pakietów

**Filtrowanie adresów IP może mieć sens, jeżeli dopuścimy tylko połączenia z zaufanych hostów. Może to być lista komputerów własnych, komputerów klientów i pracowników zdalnych.**

**Zwykle nie jest możliwe powiązanie listy adresów IP z listą portów (protokołów) - a byłoby to bardzo dobre rozwiązanie. Taki filtr ogranicza ruch na podstawie pola adresowego.**

**Jednak podany w nagłówku adres nie musi być prawdziwy (mógł zostać sfałszowany). Taka sytuacja może wystąpić podczas ataku, gdy nie jest potrzebna informacja zwrotna, np. atak typu DoS. Informacja zwrotna nie jest potrzebna również wtedy, gdy adres zwrotny jest zawarty dodatkowo w polu danych (np. w FTP).**

# Filtrowanie pakietów

**Filtrowanie portów nazywane jest również filtrowaniem protokołów wyższych warstw. Do najważniejszych protokołów, które należy zablokować należą:**

Telnet,

NetBIOS Session (usługi Windows i SMB) - możliwe jest podłączenie się do serwera plików w charakterze lokalnego klienta,

POP - jawne hasła dostępowe do poczty,

NFS - podobnie jak w przypadku NetBIOS możliwe jest podłączenie się do serwera plików w charakterze lokalnego klienta,

X Windows.

**Blokować się również powinno porty obsługujące każde oprogramowanie pozwalające na zdalny dostęp lub zdalne nadzorowanie sieci (np. PC Anywhere).**

# Filtrowanie pakietów

**Fragmentacja - umożliwia przesyłanie dużych pakietów IP (przekraczających dozwolone wymiary ramek). Pakiet jest dzielony i przesyłany po kawałku. System odbierający składa je w całość. Najbardziej użyteczne do filtrowania dane (numery portów TCP/UDP) są na początku - we fragmencie zerowym. Z tego powodu dalsze fragmenty nie mogą być filtrowane w oparciu o numery portów i przechodzą przez filtry mimo, że fragment zerowy został odrzucony. Niektóre błędne implementacje TCP/IP składają te fragmenty zamiast je odrzucić. Oznacza to, że jeżeli wysyłane fragmenty będą numerowane od 1, a nie od 0, to filtrowanie takie zostanie oszukane.**

**Problemy filtrowania bezstanowego:**

**Brak możliwości dokładnego sprawdzania ładunków danych. Decyzja jest podejmowana jedynie na podstawie zawartości nagłówka.**

**Brak pamiętania stanu połączenia. Istnieje wobec tego problem określenia ruchu zwrotnego do portów, z których nawiązywano połączenie. Faktycznie nie istnieje możliwość filtrowania ruchu do portów wysokich (powyżej 1024).**

# Filtrowanie pakietów

**Filtry z badaniem stanu**

**Przechowują informację o stanie całego ruchu przechodzącego przez filtr. Wykorzystują ją do określania czy pojedynczy pakiet powinien być odrzucony.**

**Filtry takie działają na poziomie warstwy sieciowej oraz sesji.**

**Informacja jest pobierana z pakietów przepływających podczas nawiązywania sesji. Gdy host wewnętrzny łączy się z hostem zewnętrznym, w pakiecie inicjującym umieszczony jest adres gniazda zwrotnego (adres IP i numer portu) na którym oczekuje na odpowiedź. Informacje te są zapamiętywane przez filtr. Umożliwiają potem odróżnienie poprawnych pakietów zwrotnych od niepoprawnych prób połączeń lub włamań.**

**Kiedy przychodzi odpowiedź, sprawdzane są zapisy w tablicy filtra w celu sprawdzenia, czy pakiet ma zostać przepuszczony. Jeżeli z zewnątrz przychodzi pakiet, który nie ma pozycji w tablicy stanów, to jest odrzucany. Zapisy w tablicy stanów są usuwane gdy przesyłane są pakiety związane z zamknięciem sesji lub po upływie określonego czasu. Wyjątki określają pakiety:**
**które zawsze będą odrzucane,**
**których nigdy nie należy odrzucać,**
**usługi z zewnątrz do określonych hostów.**

# Translacja adresów

**Translacja adresów (Network Address Translation - NAT) umożliwia przydzielenie komputerom z sieci wewnętrznej adresów z puli adresów nie rejestrowanych w sieci Internet (pula adresów prywatnych) oraz zapewnienie tym komputerom możliwości dwustronnego komunikowania się z komputerami w sieci Internet.**

**Sprawia wrażenie, że ruch pochodzi z pojedynczego adresu IP. Jest to adres zapory. NAT jest implementowany tylko w warstwie transportowej. Czyli aby zapobiec naruszeniom bezpieczeństwa w warstwach wyższych, trzeba używać np. proxy.**

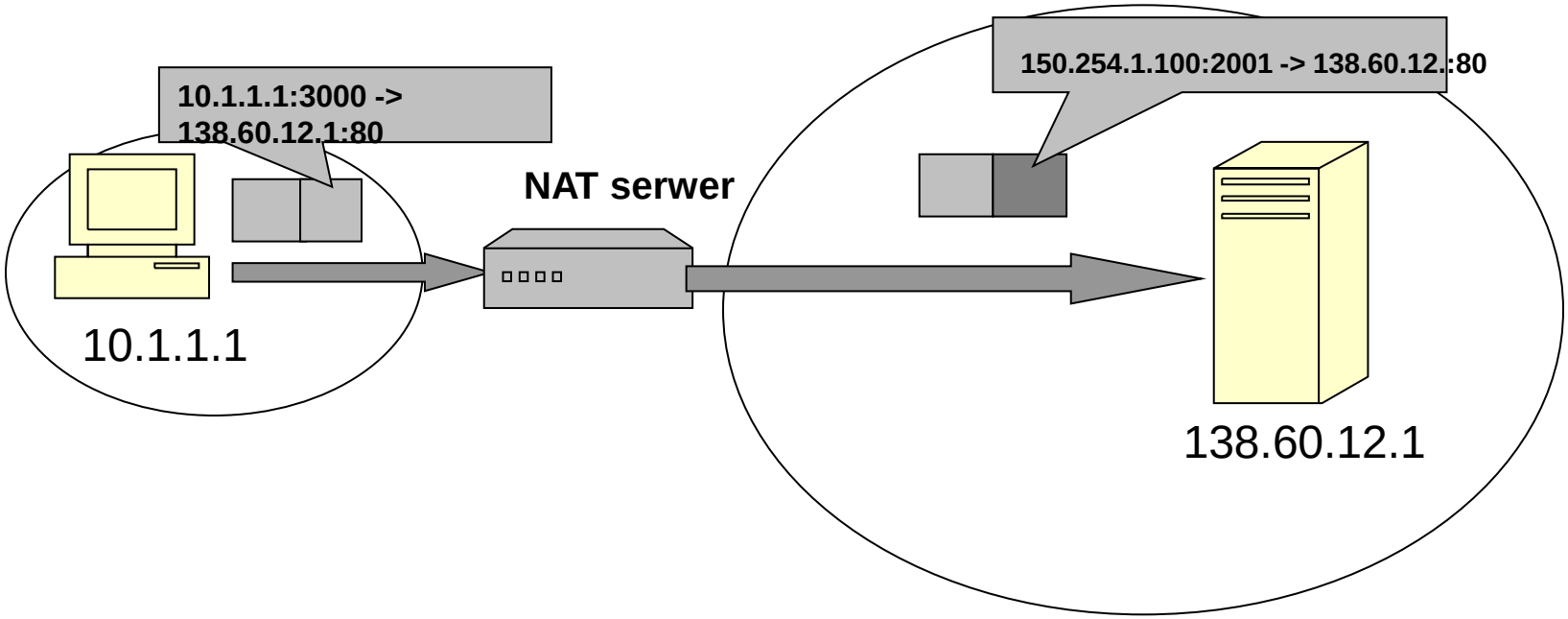
**Stacja kliencka powinna traktować bramę NAT jako swój gateway. Jeżeli tak nie jest, to brama NAT powinna funkcjonować jako serwer proxy arp. Pakiet pochodzący od klienta otrzymuje nowy numer portu źródłowego i adres źródłowy. W takiej postaci jest wysyłany. Brama zapamiętuje zrealizowane przekształcenie.**

**Gdy przychodzi odpowiedź, to musi zostać rozpoznana i pakiet przekształcony. Przywracany jest adres klienta i pakiet trafia do klienta.**

# Translacja adresów

**Zakresy adresów prywatnych:**

**10.0.0.0 - 10.255.255.255 - pojedynczy numer sieci klasy A;**
**172.16.0.0 - 172.31.255.255 - 16 ciągłych numer sieci klasy B;**
**192.168.0.0 - 192.168.255.255 - 255 ciągłych numer sieci klasy C.**



# Typy translacji adresów

**Translacja statyczna (static translation) inaczej przekierowanie portów (port forwarding) - określony zasób ma przypisane stałe przekształcenie. Stosujemy gdy udostępniamy hosty wewnętrzne dla połączeń z hostów zewnętrznych. Np. serwer pocztowy.**

**Translacja dynamiczna (dynamic translation) inaczej automatyczna (automatic), tryb ukrywania (hide mode), maskowanie IP (IP masqerade) - stosowana gdy duża grupa klientów wewnętrznych współużytkuje adres lub grupę adresów wewnętrznych. Adresy tych klientów zastępowane są adresem zapory. Klienci są identyfikowani numerem portu połączenia przechodzącego przez zaporę. Host zewnętrzny nie ma możliwości zainicjowania połączenia z wewnętrznym.**

**Translacja ze zrównoważonym obciążeniem (load balancing translation) - pojedynczy adres i numer portu są przekształcane na jeden z adresów identycznie skonfigurowanych serwerów. W efekcie jeden adres jest obsługiwany przez kilka serwerów. Z puli dostępnych serwerów zapora za każdym razem wybiera jeden.**

**Translacja ze zwielokrotnionymi połączeniami (network redundancy translation) - zwielokrotnione połączenia z Internetem są przyłączone do pojedynczej zapory NAT i wykorzystywane w oparciu o obciążenie i dostępność. Za każdym razem gdy host wewnętrzny łączy się z zewnętrznym, podejmowana jest decyzja, którą droga skierować jego pakiety.**

# Usługi Proxy

**1. Przechowywanie w pamięci podręcznej często przeglądanych stron WWW (przyśpieszenie dostępu do informacji).**

**2. Serwery proxy pośredniczą w przekazywaniu żądań klientów sieci wewnętrznej do sieci zewnętrznej. Pozwala to ukrywać klientów przed badaniem z zewnątrz.**

**3. Proxy nasłuchuje zleceń usługi od klientów wewnętrznych i przesyła je w ich imieniu do sieci zewnętrznej. Po otrzymaniu odpowiedzi z zewnątrz zwraca ją do rzeczywistego klienta.**

# Usługi Proxy

**Zalety:**

**Ukrywanie klienta jest możliwe ponieważ proxy generują żądania warstwy usługowej w imieniu swoich klientów.**

**Nie jest to jedynie zmiana nagłówków. Klienci zwracają się do proxy jak do serwera docelowego. Przez proxy przesyłane są tylko komunikaty warstwy usługowej (np. HTTP) a nie pakiety TCP czy IP.**

**Pakiety protokołów warstw niższych są ponownie generowane przez proxy.**

**Blokowanie URL jest realizowane poprzez porównywanie URL z listą adresów zakazanych.**

**Badanie spójności to sprawdzanie zgodności z protokołem. Eliminuje się w ten sposób, lub przynajmniej ogranicza użycie nieprawidłowo sformatowanych danych do wykorzystywania luk w systemie.**

**Blokowanie routingu. Żaden pakiet TCP/IP nie jest przesyłany pomiędzy sieciami, więc eliminuje się wiele ataków typu DoS oraz wykorzystujących luki TCP/IP.**

# Usługi Proxy

**Wady proxy**

**Pojedynczy punkt kontroli - pojedynczy punkt awarii powoduje duże zagrożenie w przypadku jego awarii. Sam proxy powinien być dodatkowo chroniony przez filtry lub ścianę ogniową.**

**Klienci muszą współpracować z proxy. Klienci niewłaściwie skonfigurowani nie będą korzystać z proxy.**

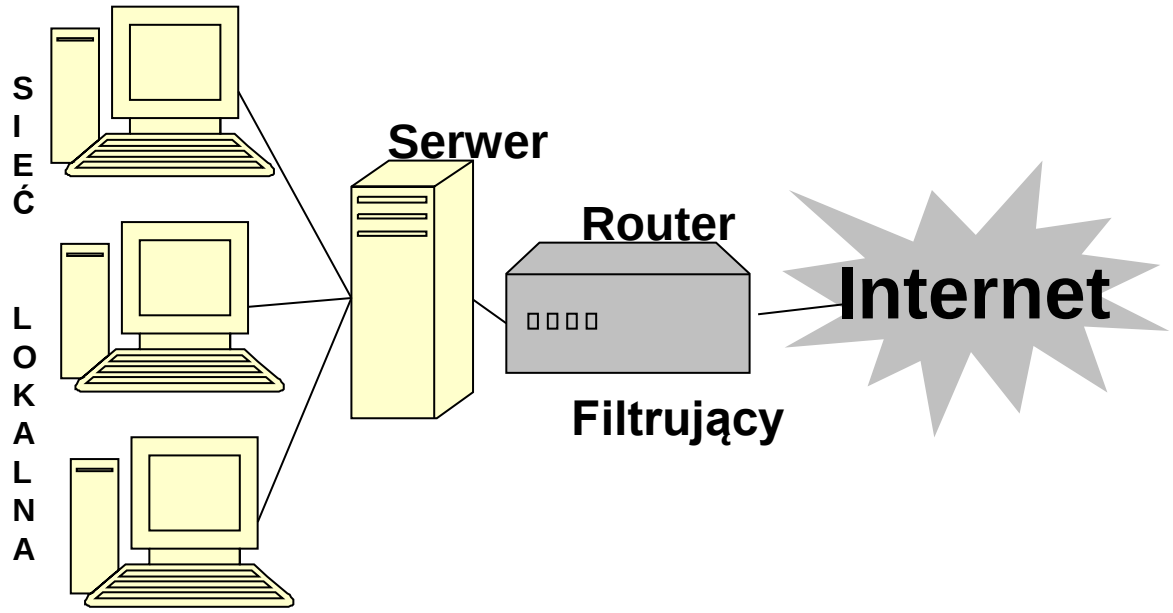
**Oddzielne proxy dla każdej usługi. Dla niektórych usług trudno jest zbudować proxy, ponieważ wymagają one kanału zwrotnego. Dla niektórych usług nie ma skutecznych filtrów zawartości. Np. usługi strumieniowe typu RealVideo lub RealAudio wymagają przepływu skompresowanego strumienia w czasie rzeczywistym. Jego przerwanie uniemożliwia zwykle dalsze dekodowanie. Niemożność filtrowania powinna implikować konieczność blokowania.**

**Ochrona systemu operacyjnego ma decydujące znaczenie dla funkcjonowania proxy.**

**Zatory to wada powodująca spadek wydajności.**

# Modele ścian ogniowych

**System z zaporą sieciową typu router filtrujący**

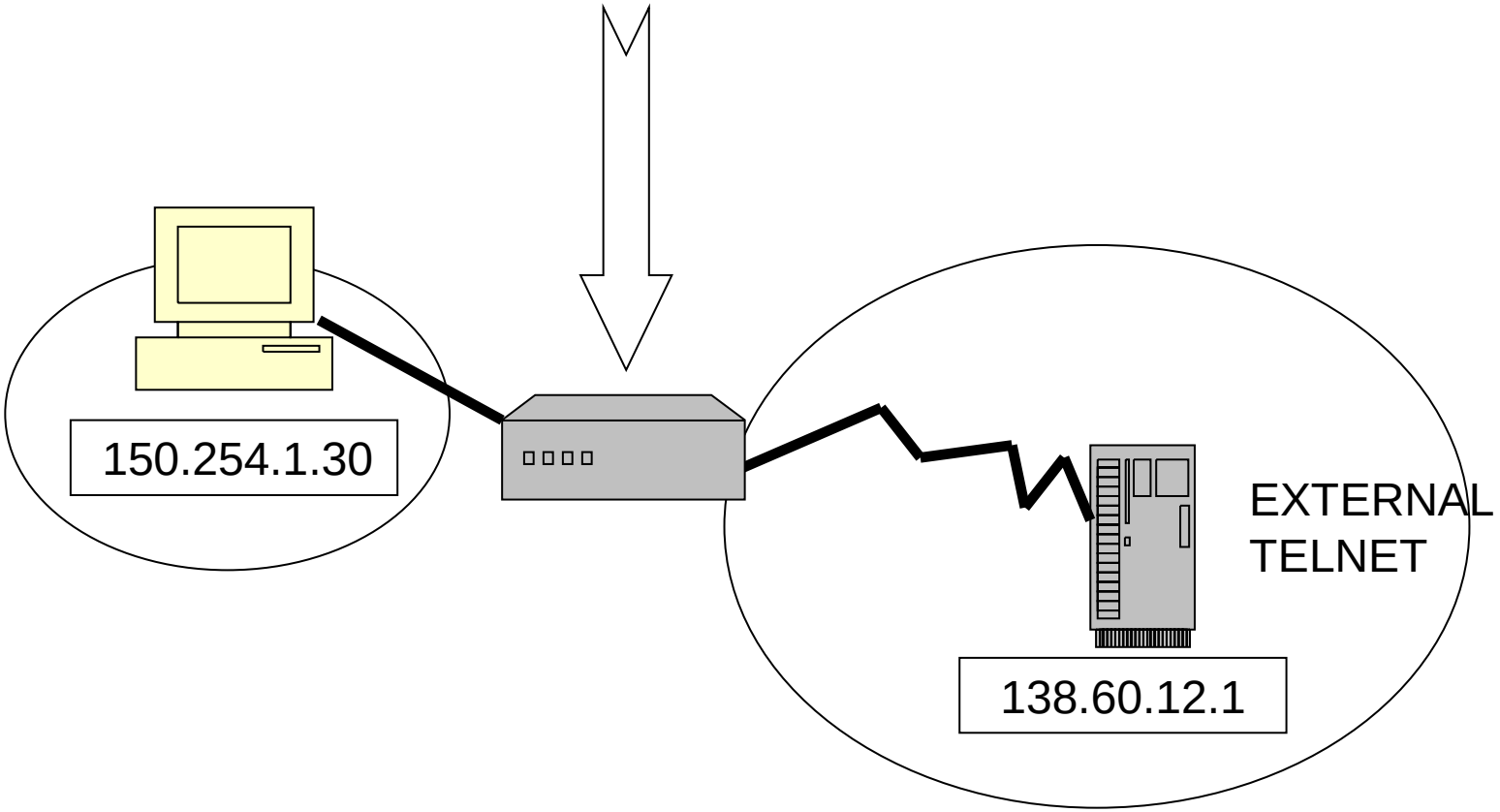



- Możliwość utrzymania oddzielnych list filtracji dla ruchu wchodzącego i wychodzącego

- Filtracja statyczna, kontekstowa (dynamiczne reguły filtracji), filtracja nieliniowa (elasty
definiowanie wyrażeń warunkowych)

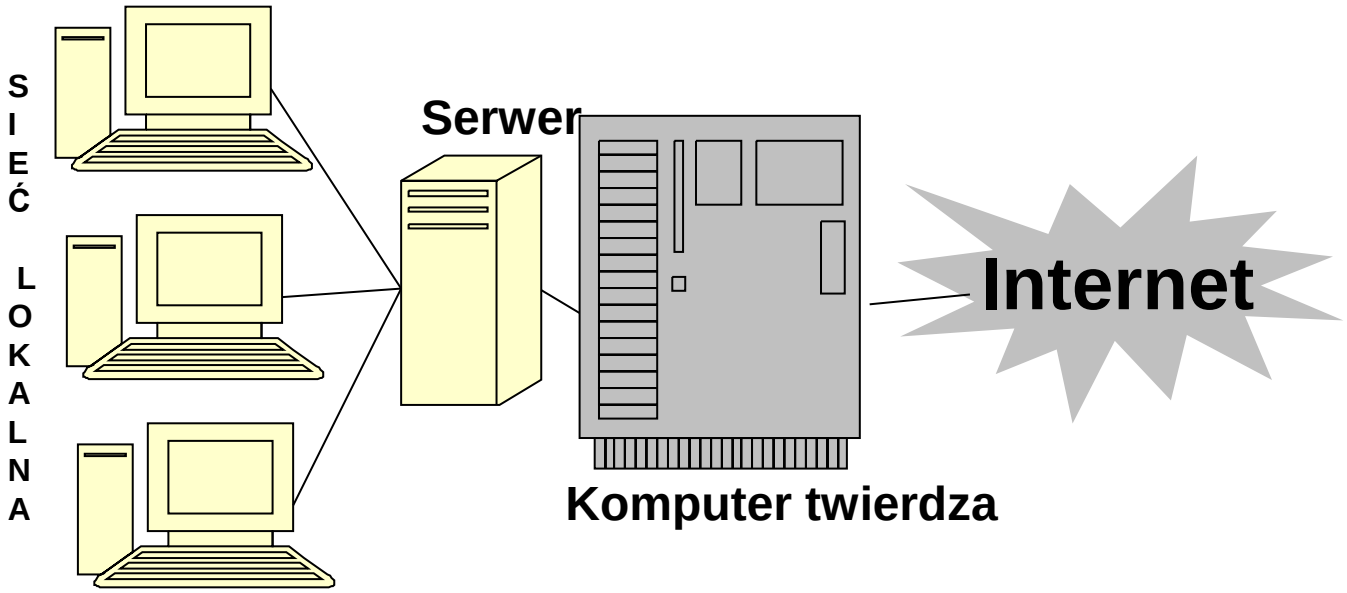
# Modele ścian ogniowych

**Definicja statycznych reguł filtracji**



# Modele ścian ogniowych

**Model systemu z zaporą typu Komputer Twierdza**



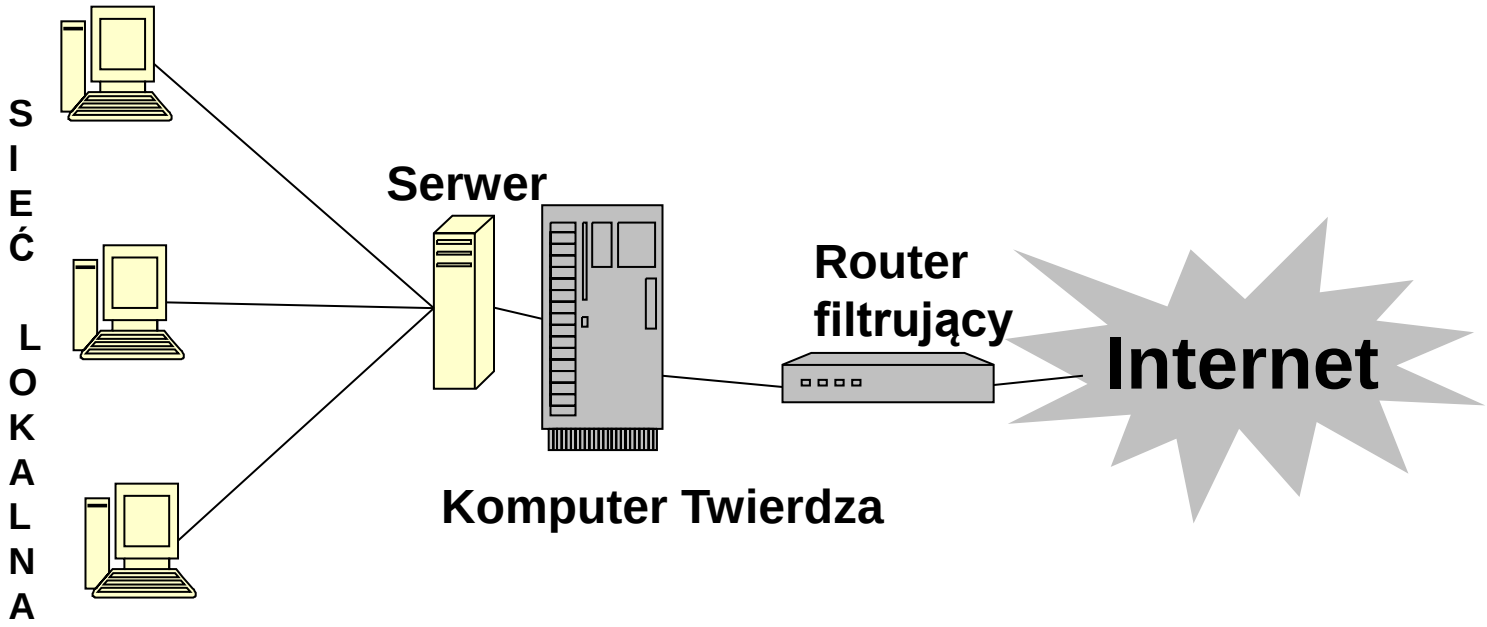

- Komputer Twierdza – stacja z odseparowanymi interfejsami sieciowymi, zajmująca miejsce węzła międzysieciowego.

- Oferuje fizyczną i logiczną separację prywatnej sieci lokalnej od zewnętrznej sieci publicznej.

- Możliwa rejestracja zdarzeń (auditing), ułatwiająca diagnozowanie ewentualnie pojawiających się nowych zagrożeń.

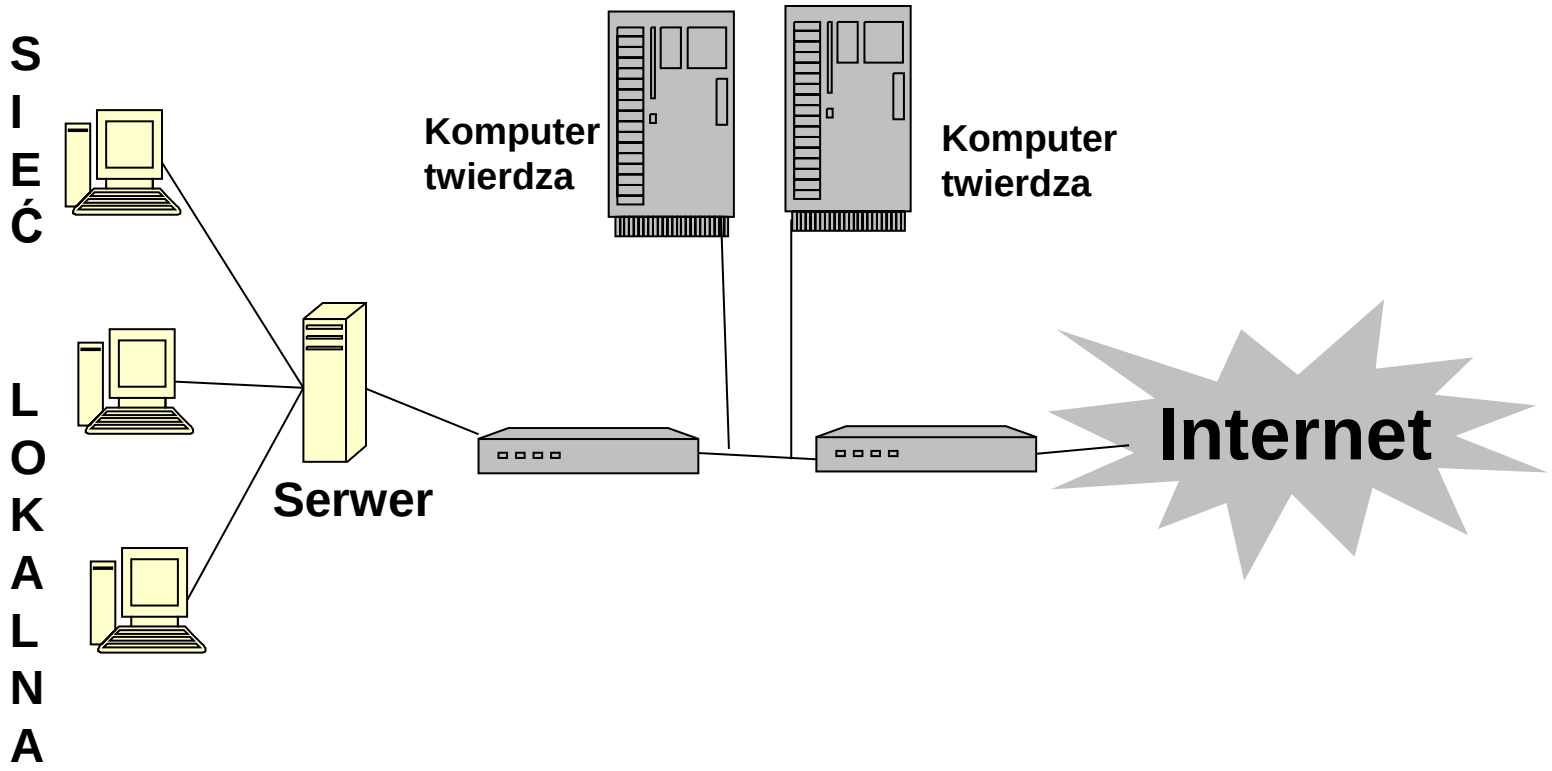
# Modele ścian ogniowych

**Model systemu z filtracją podwójną**



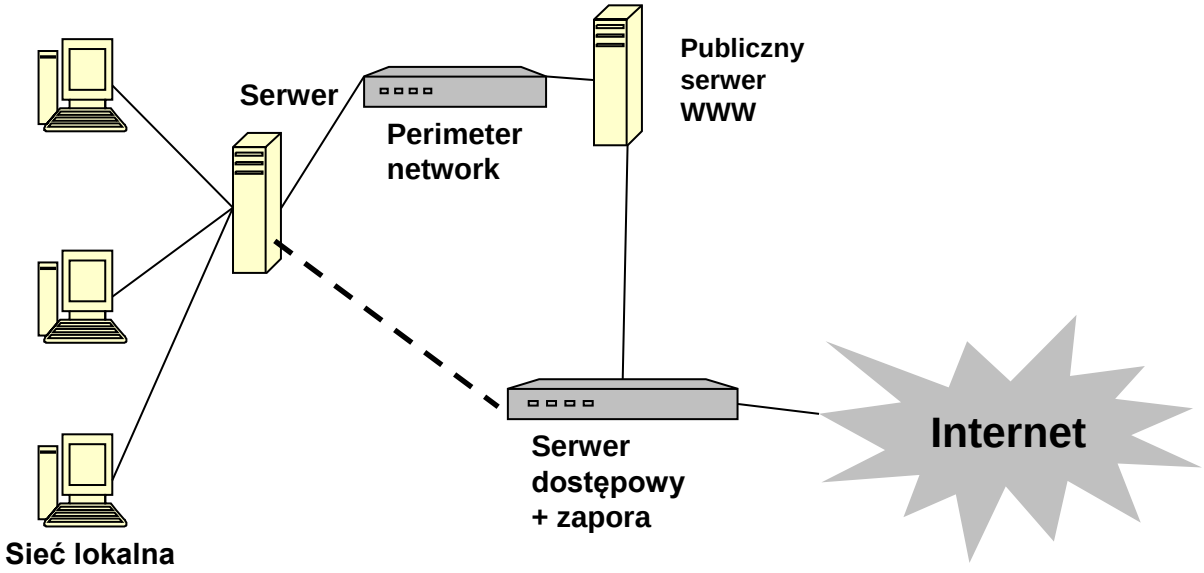
# Modele ścian ogniowych

## Model systemu z podsiecią ochronną

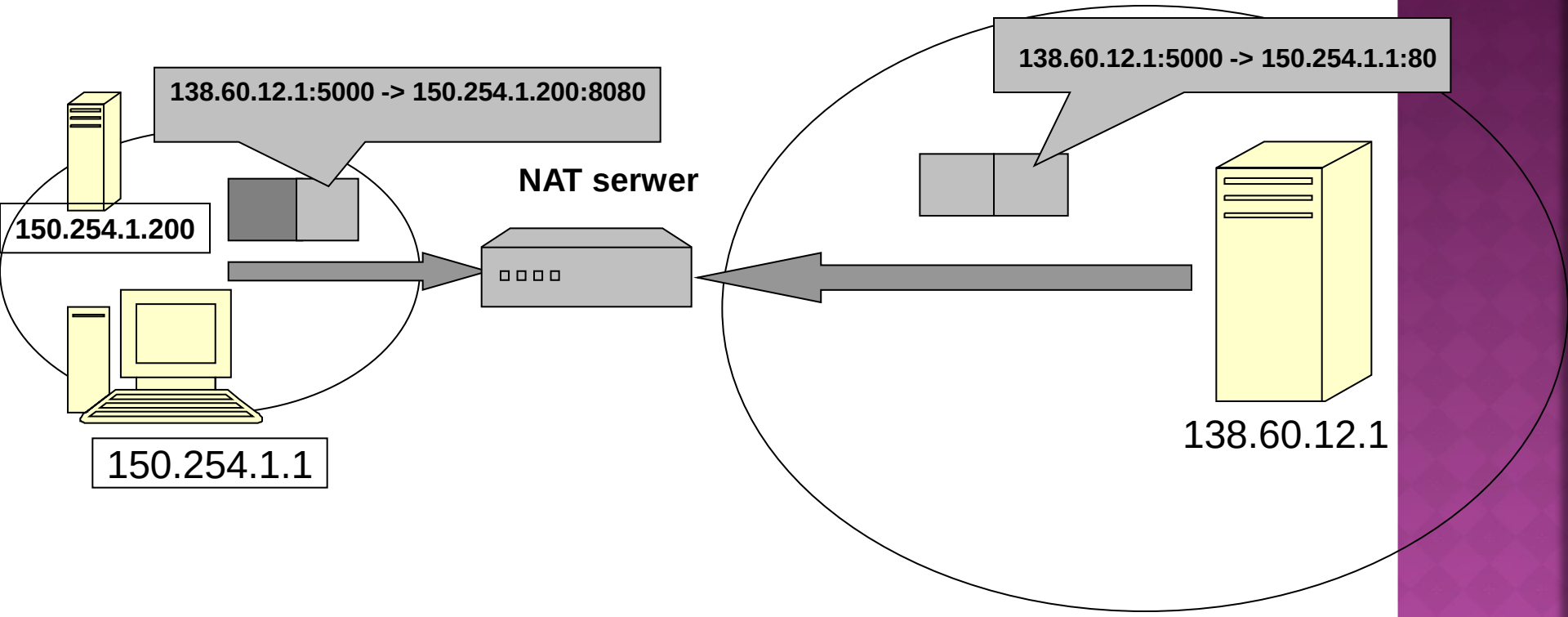


# Modele ścian ogniowych

## Model systemu ze strefą zdemilitaryzowaną




- Strefa Zdemilitaryzowana – wydzielona podsieć zawierająca komponenty świadomie wyjęte spod kontroli obejmującej całą resztę sieci wewnętrznej, np. publiczne zasoby, pułapki,


138.60.12.1:5000 -> 150.254.1.200:8080
NAT serwer
138.60.12.1:5000 -> 150.254.1.1:80
150.254.1.200
150.254.1.1
138.60.12.1