Bezpieczeństwo systemów komputerowych

Ściany ogniowe, translacja adresów

Aleksy Schubert (Marcin Peczarski)

Instytut Informatyki Uniwersytetu Warszawskiego

18 grudnia 2018

Na podstawie materiałów Michała Szychowiaka
z *http://wazniak.mimuw.edu.pl*

Dlaczego potrzebne są ściany ogniowe?

- Niebezpieczeństwo związane z atakiem sieciowym wzrasta wraz z liczbą udostępnianych usług sieciowych.
- W sieci lokalnej istnieje potrzeba udostępniania wielu usług.
- Większość z usług dostępnych lokalnie nie powinna być dostępna z zewnątrz.
- Sieć lokalna może być bardzo duża, zawierać tysiące komputerów, wyposażonych w bardzo różnorodne oprogramowanie.
- Zwykle wystaczy jedna dziura w bezpieczeństwie na jednym z komputerów, aby agresor wtargnął do sieci lokalnej.
- Jest praktycznie niemożliwie nadzorowanie wszystkich systemów w dużej sieci lokalnej.
- Sieć lokalną należy odseparować od sieci publicznej.
- Cały ruch między sieciami lokalną a publiczną powinien odbywać się przez nadzorowane kanały.
- W miejscu każdego styku sieci lokalnej z publiczną należy zainstalować silny punkt obrony.

Co to jest ściana ogniowa?

- Ściana ogniowa (ang. *firewall*) – gruba, ognioodporna zapora zapobiegająca rozprzestrzenianiu się ognia w budynku.
- Ściana ogniowa, zapora sieciowa wg Wikipedii:
  - sposób zabezpieczania sieci i systemów komputerowych przed intruzami;
  - dedykowany sprzęt wraz ze specjalnym oprogramowaniem lub samo oprogramowanie blokujące niepowołany dostęp do komputera;
  - ochrona wewnętrznej sieci lokalnej przed dostępem z zewnątrz;
  - ochrona przed nieuprawnionym wypływem danych z sieci lokalnej na zewnątrz;
  - filtrowanie połączeń wchodzących i wychodzących oraz odmawianie żądań dostępu uznanych za niebezpieczne.

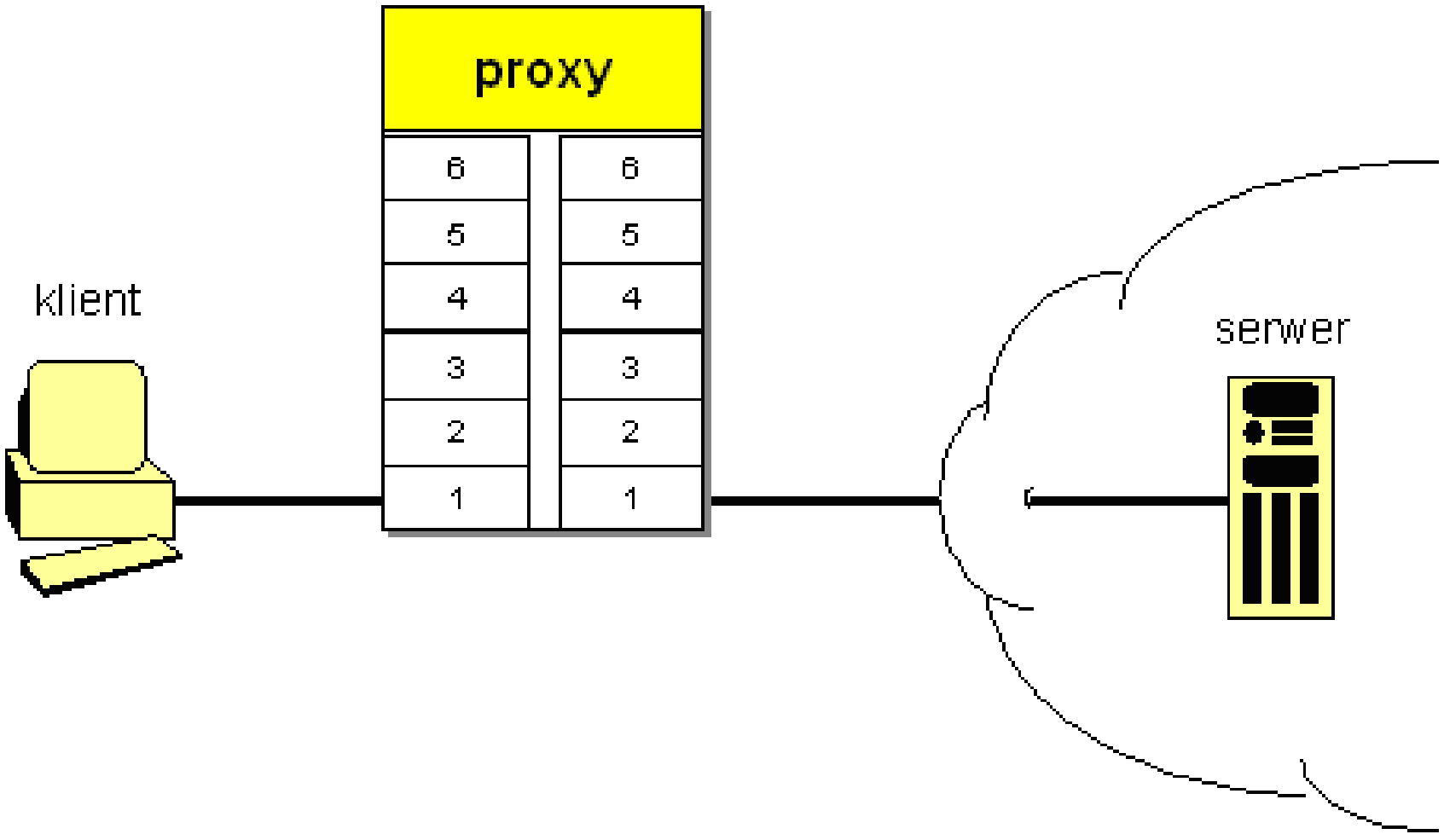
Jakie są podstawowe funkcje ściany ogniowej?

- Dzieli intersieć na dwie części: wewnętrzną i zewnetrzną.
- Filtruje ruch sieciowy.
- Filtracja polega na analizie parametrów w nagłówkach pakietów wartwy sieciowej (warstwa 3 modelu ISO/OSI), a czasem też warswy łącza (2) i transportowej (4).
- Możliwa jest filtracja pakietów
  - wchodzących,
  - wychodzących,
  - propagowanych, rutowanych w węzłach międzysieciowych.
- Decyzja o przepuszczaniu lub blokowaniu ruchu jest podejmowana na podstawie zdefiniowanych reguł filtracji.

Jakie są dodatkowe funkcje ściany ogniowej?

- Pośredniczy w dostępie do usług sieciowych.
- Sieć lokalna może być całkowicie odseparowana od sieci publicznej – brak możliwości rutingu – komunikacja jest możliwa tylko w warstwie aplikacji (7).
- Na zaporze uruchamia się pośrednika (ang. *proxy*), który pośredniczy w komunikacji aplikacji użytkowej działającej w modelu klient-serwer.
  - Klient, uruchomiony w sieci wewnętrznej, nie może nawiązać połączenia bezpośrednio z serwerem pracującym w sieci zewnętrznej.
  - Może tylko nawiązać połączenie z pośrednikiem.
  - Ruch może przechodzić przez zaporę, jedynie gdy zostanie pozytywnie sklasyfikowany przez pośrednika.
  - Zaakceptowane połączenie od klienta jest następnie w jego imieniu zestawiane z serwerem przez pośrednika.
  - Zatem utrzymywane są dwa połączenia: klient – pośrednik i pośrednik – serwer dolecowy.

Proxy

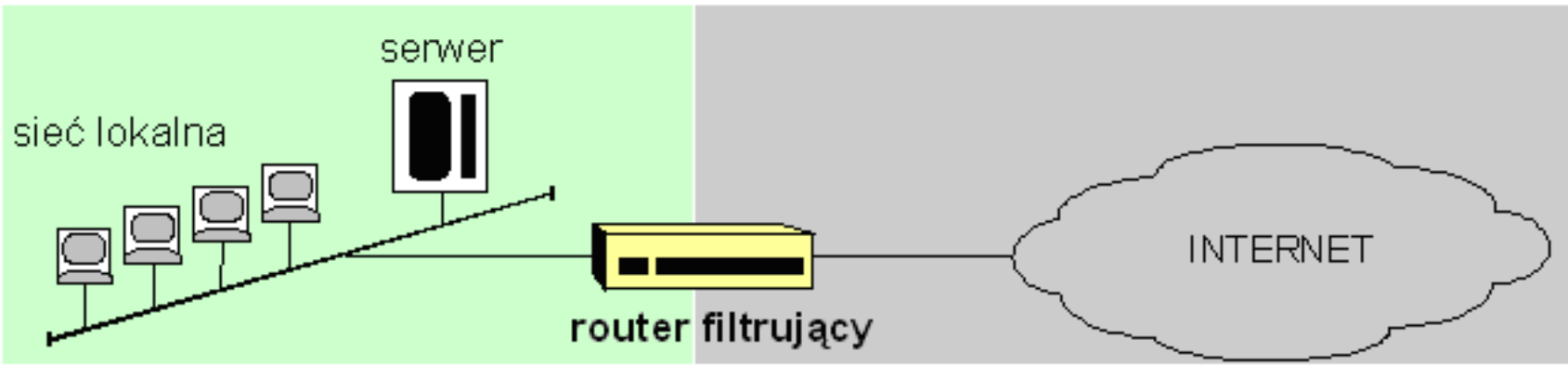


Jakie są podstawowe komponenty ścian ogniowych?

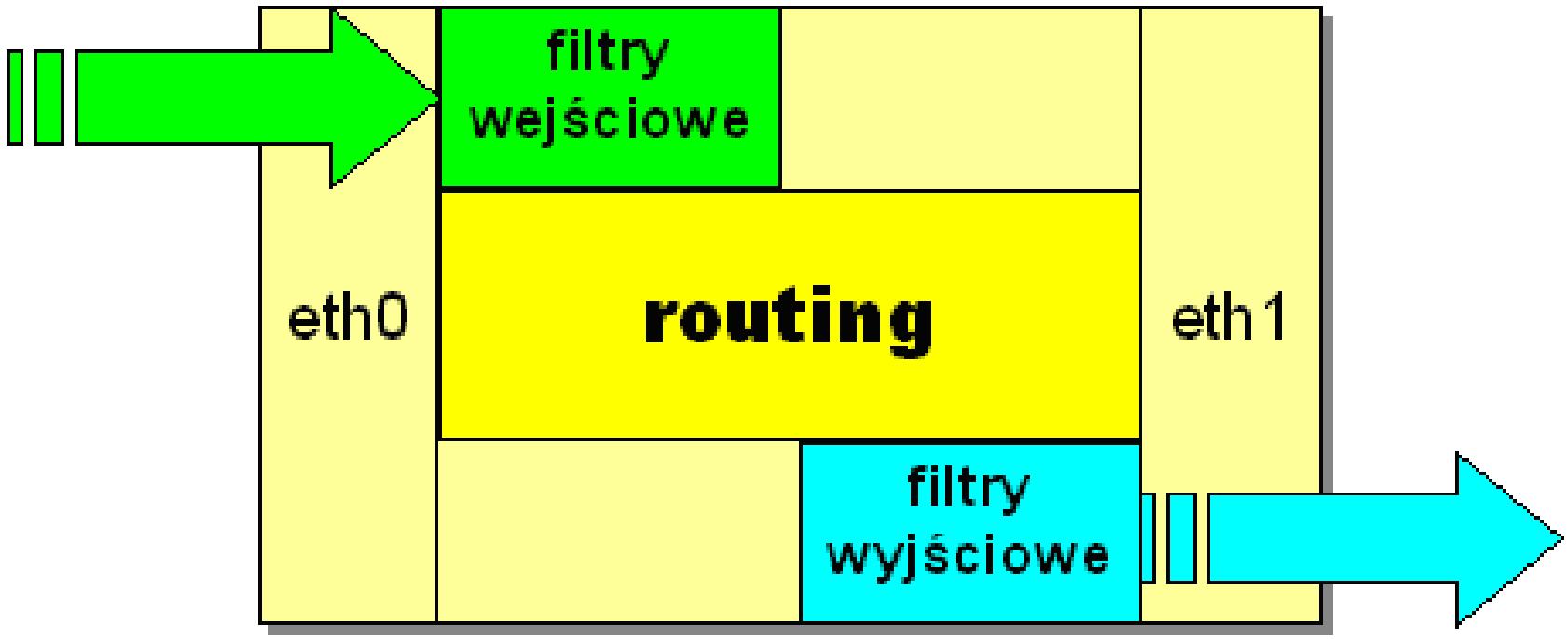
- Specjalizowany węzeł międzysieciowy (ruter) – rozwiązanie najprostsze i najłatwiejsze w utrzymaniu, możliwe do zrealizowania za pomocą następujących urządzeń:
  - ruter filtrujący (ang. *screening router*),
  - ruter szyfrujący (ang. *ciphering router*),
  - komputer twierdza (ang. *bastion host*) – dedykowany komputer lub węzeł międzysieciowy, na którym uruchomione są usługi pośredniczące (ang. proxy).
- Strefa zdemilitaryzowana, DMZ (ang. *demilitarized zone*)
  - dedykowana podsieć obejmująca jedno lub kilka stanowisk o złagodzonych wymaganiach względem ochrony;
  - typowo umieszcza się tam stanowiska oferujące pewne wybrane informacje publicznie, w odróżnieniu od stacji sieciowych pracujących wewnątrz chronionej sieci.

Jak działa ruter filtrujący?

- Podstawowym zagadnieniem dotyczącym realizacji zapory sieciowej tego typu jest kwestia definicji reguł filtracji.
- Reguły filtracji operują na parametrach analizowanych pakietów:
  - adresy z nagłówka protokołu sieciowego (źródłowy i docelowy),
  - typ protokołu warstwy wyższej, przenoszonego w polu danych,
  - rodzaj usługi (np. numer portu z nagłówka protokołu transportowego).



Schemat filtracji

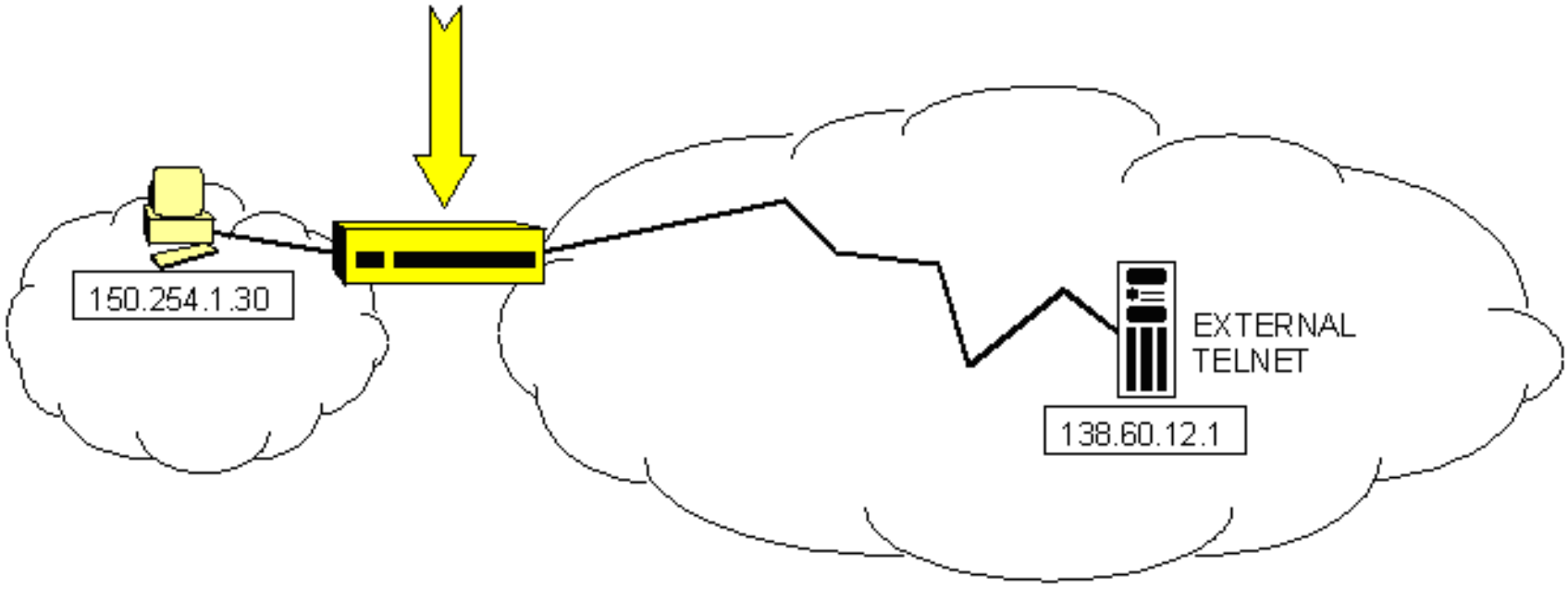


Jak się definiuje reguły filtracji?

- Filtry statyczne – reguły filtracji są definiowane przez administratora i obowiązują aż do jawnej ich zmiany.
- Filtry kontekstowe, SPF (ang. *stateful packet filtering*) – stosują dynamiczne reguły filtracji:
  - w trakcie pracy zapamiętywane są informacje o połączeniach (sesjach);
  - decyzje o filtracji pakietów podejmowane są z uwzględnieniem stanu połączenia (sesji), do którego należą.
- Filtracja nieliniowa – elastyczne definiowanie wyrażeń warunkowych (zagnieżdżone reguły logiczne).

Przykład reguł filtracji

reguła	kierunek ruchu	nadawca pakietu	odbiorca pakietu	protokół transportowy	port nadawcy	port odbiorcy	flagi	działanie
1.	na zewnątrz	150.254.*.*	138.60.12.1	TCP	>1023	23	*	przepuść
2.	do wewnątrz	138.60.12.1	150.254.*.*	TCP	23	>1023	ACK=1	przepuść
3.	do wewnątrz	138.60.12.1	150.254.*.*	TCP	23	>1023	ACK=0	odrzuć
(default)	*	*.*.*.*	*.*.*.*	*	*	*	*	odrzuć



Jakie są podstawowe zasady pisania reguł filtracji?

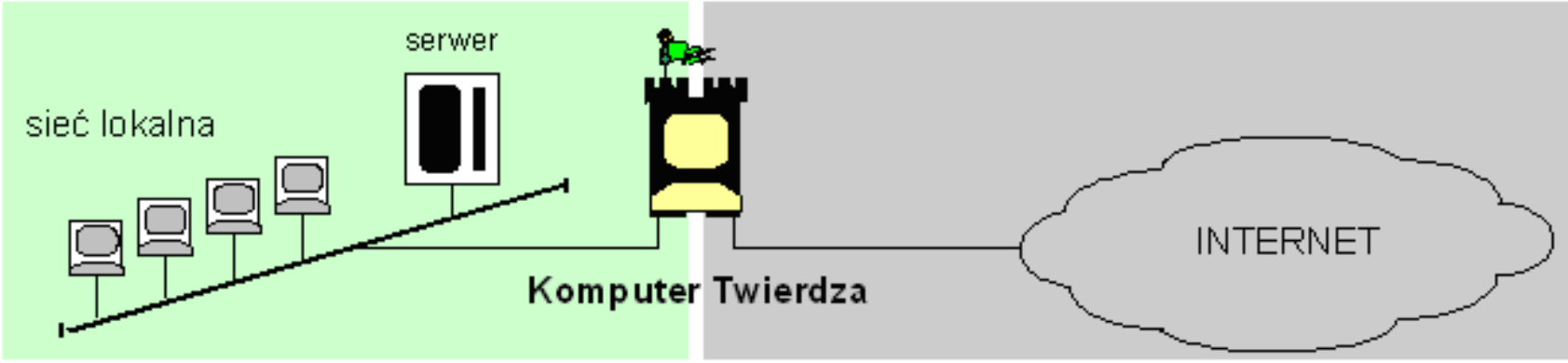
- Należy stosować regułę, że odrzucana jest każda komunikacja, która nie została jawnie dopuszczona.
- Domyślna reguła powinna odrzucać wszystkie pakiety.
- Należy odrzucać pakiety przychodzące z sieci zewnętrznej z adresem źródłowym pochodzącym z sieci wewnętrznej.
- Należy odrzucać pakiety przychodzące z sieci wewnętrznej z adresem źródłowym pochodzącym z sieci zewnętrznej.

Jakie są wady statycznych reguł filtracji?

- Niektóre usługi trudno poddają się filtracji statycznej, np. FTP, X11, DNS.
- Jak w trybie aktywnym FTP chronić się przed oprogramowaniem, podszywającym się pod serwer, próbującym nawiązać połączenie z komputerem wewnątrz chronionej sieci?
- Coraz powszechniej wprowadza się i stosuje tryby pracy zmodyfikowane pod kątem usprawnienia filtracji, np. tryb pasywny w FTP (skądinąd użyteczny także np. przy korzystaniu z dostępu xDSL).

Komputer twierdza, bastion

- Stacja wyposażona w co najmniej dwa interfejsy sieciowe (ang. *dual homed host gateway*).
- Pełni rolę węzła międzysieciowego.
- Oferuje fizyczną i logiczną separację prywatnej sieci lokalnej od zewnętrznej sieci publicznej.
- Dzięki separacji interfejsów tylko on jest widoczny z sieci publicznej.
- Aby wtargnąć do sieci prywatnej, trzeba go najpierw sforsować.

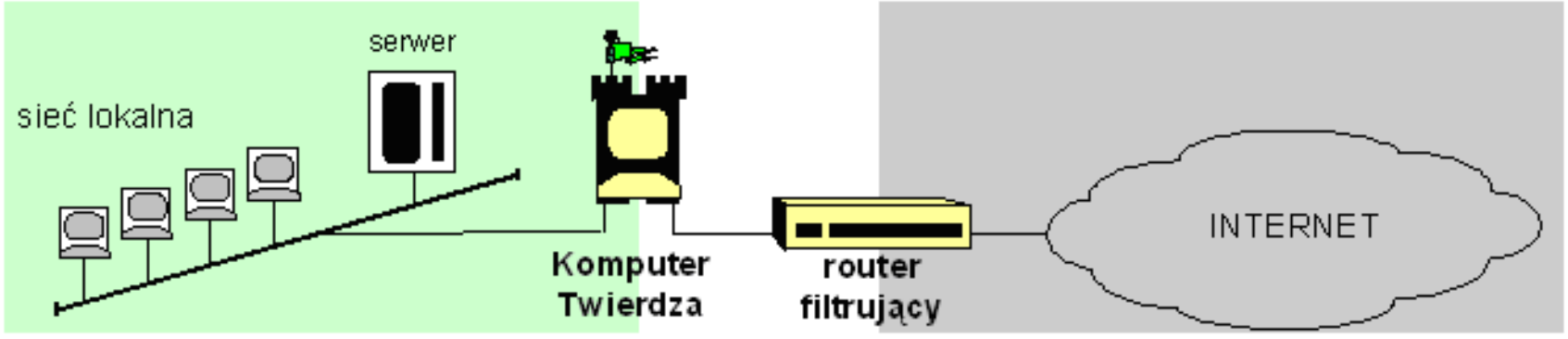


Komputer twierdza, cd.

- Pełni rolę bramy aplikacyjnej – usługi pośredniczące i zastępcze (proxy) rozwiązują problem usług trudnych do filtracji.
- Dzięki temu, że jest on pełnym stanowiskiem komputerowym, potencjalnie wyposażonym w praktycznie nieograniczone zasoby pamięci masowej, możliwa jest szczegółowa rejestracja zdarzeń, ułatwiająca diagnozowanie ewentualnie pojawiających się nowych zagrożeń i niedoskonałości konfiguracji.

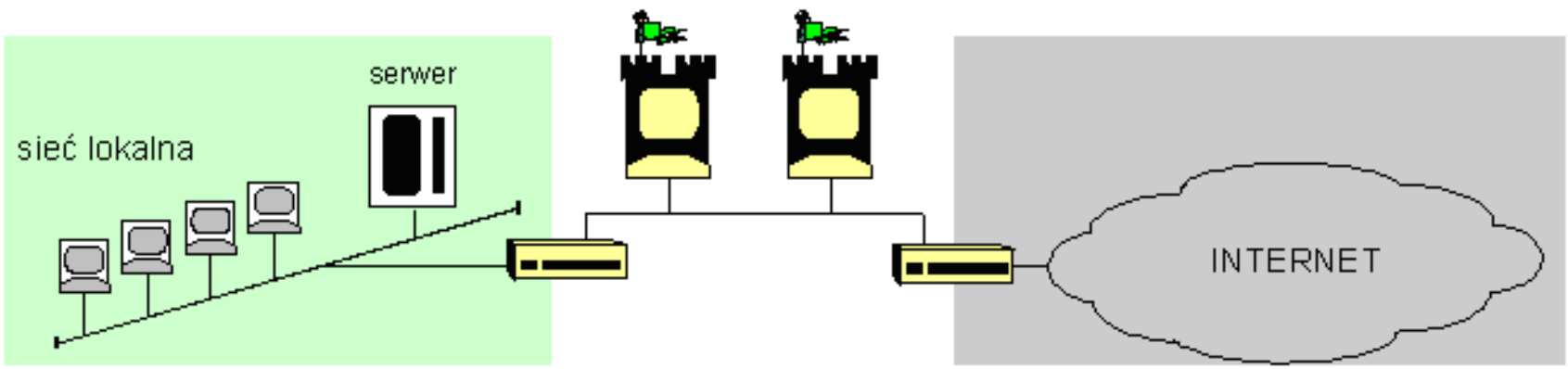
Filtracja podwójna

- W jedną linię obrony można połączyć różne typy ścian ogniowych.
- Bramę aplikacyjną można poprzedzić ruterem filtrującym (ang. *screened host gateway*).



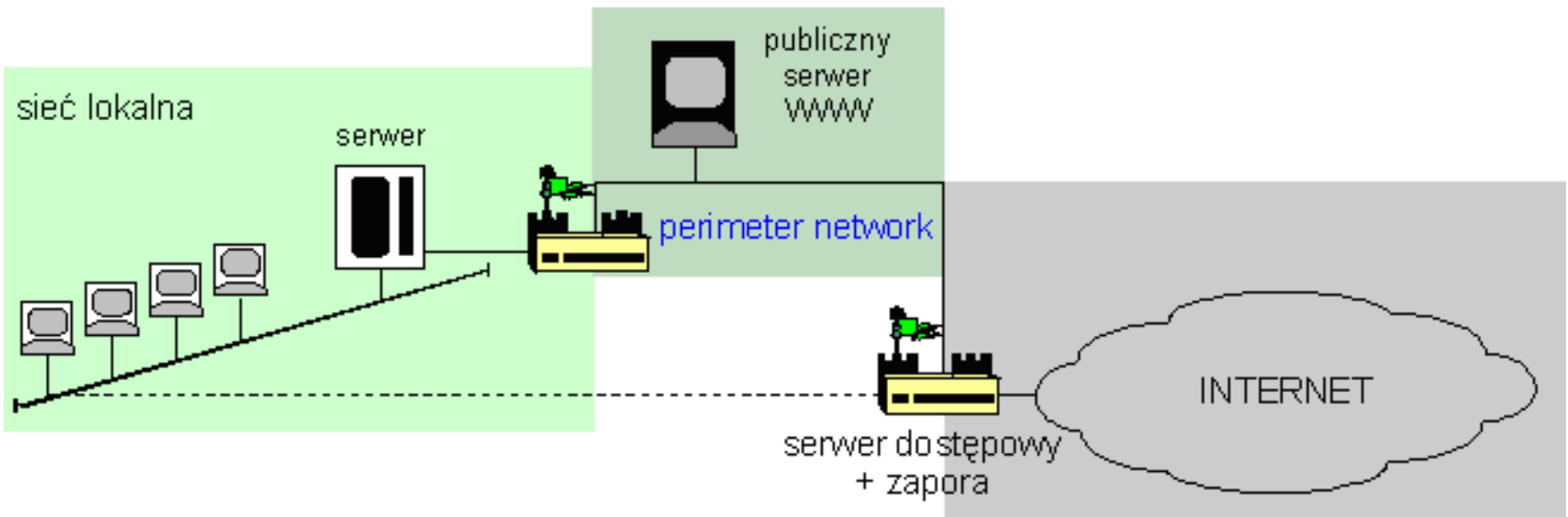
Podsieć ochronna

- Możliwe jest „rozciągnięcie” twierdzy na całą dedykowaną podsieć (ang. *screened network*), a nawet kaskadę podsieci.
- Taka sieć jest często nazywana krótką siecią (ang. *stub network*).
- Chroni sieć wewnętrzną przed zalaniem pakietami nadchodzącymi z zewnątrz.



Strefa zdemilitaryzowana

- DMZ – demilitarized zone
- Wydzielona podsieć zawierająca komponenty świadomie wyjęte spod kontroli obejmującej całą resztę sieci wewnętrznej:
  - zasoby publiczne, np. ogólnodostępny serwis www,
  - przynęty, pułapki.
- Na rysunku przerywaną linią zaznaczono ręczne obejście, które pozwala na tymczasowe przepuszczanie całości lub części ruchu, np. w celach testowych.



Translacja adresów

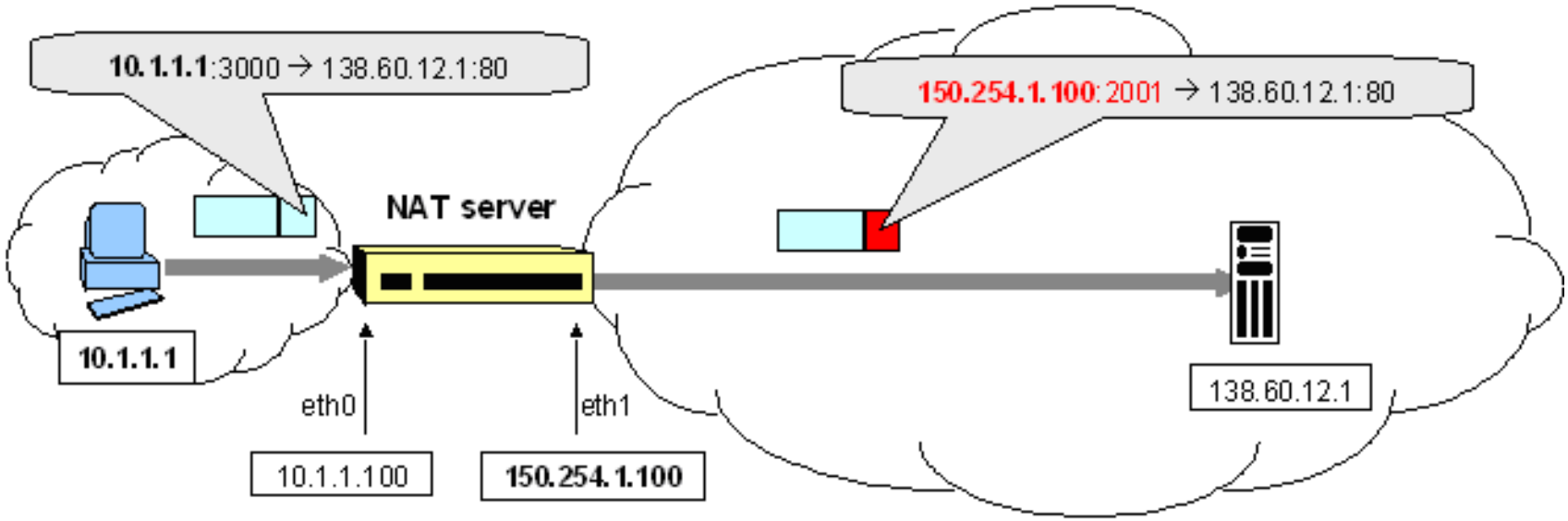
- NAT – Network Address Translation
- Rozszerza dostęp do sieci publicznej na stanowiska nie posiadające przydziału adresów publicznych (posiadające tylko adresy prywatne).
- Umożliwia korzystanie wewnątrz sieci z nieprzydzielonych adresów publicznych.
- Ukrywa wewnętrzną strukturę sieci przed światem zewnętrznym.
- Metody odwzorowania adresów są ustandaryzowane i opisane:
  - RFC 1631 (translacja na pojedynczy adres, tj. N:1),
  - RFC 1918 (translacja na pulę adresową, tj. N:M).

Translacja adresów, cd.

- Może być wykonywana na poziomie warstwy
  - sieciowej, zmieniany jest tylko adres IP – klasyczny NAT,
  - transportowej, zmieniane są adres IP i numer portu – NAPT (Network Address Port Translation), PAT (Port Address Translation).
- Wyróżnia się translację adresów
  - źródłowych – Source NAT (SNAT),
  - docelowych – Destination NAT (DNAT).

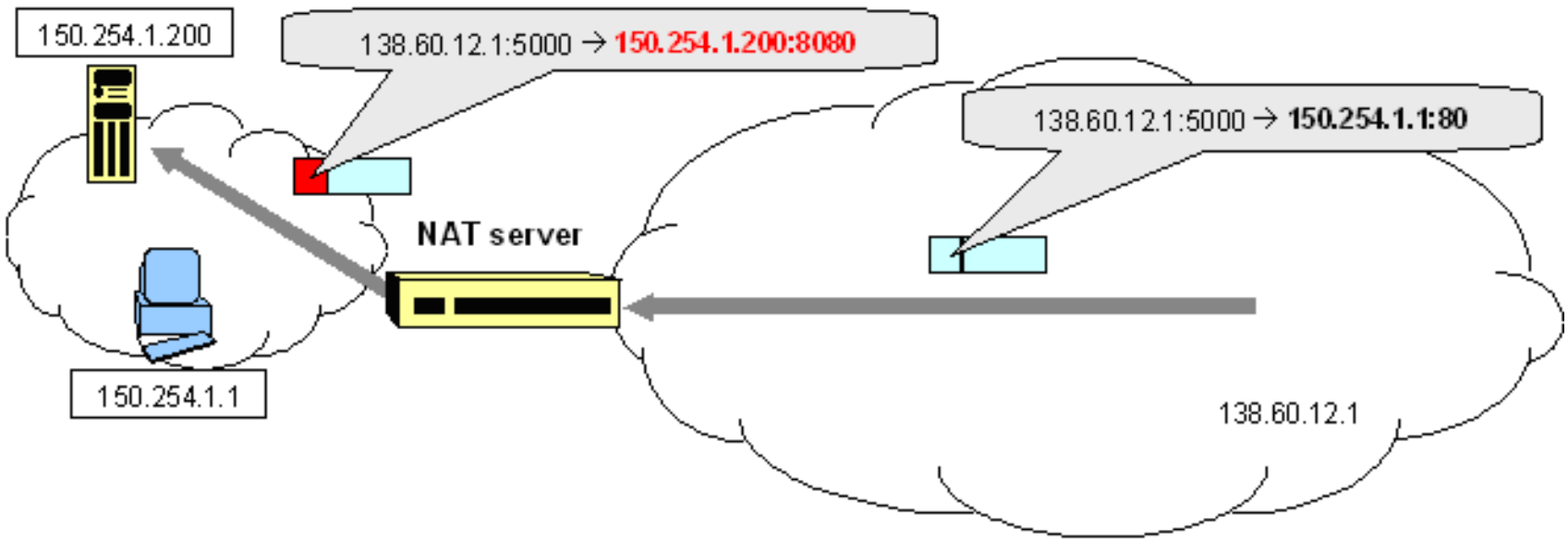
Translacja adresów źródłowych

- Chcemy umożliwić komputerom z sieci prywatnej inicjowanie komunikacji do sieci publicznej.
- W poniższym przykładzie pakiet wychodzący z maszyny o adresie 10.1.1.1 otrzymuje po translacji adres źródłowy 150.254.1.100 należący do serwera translacji, którym jest brzegowy węzeł międzysieciowy.
- Numer portu źródłowego też może ulec zmianie.



Translacja adresów docelowych

- Chcemy umożliwić komputerom z sieci publicznej komunikację do komputerów w sieci prywatnej.
- Pakiety pochodzące z sieci zewnętrznej otrzymują nowy adres docelowy.
- Na rysunku publiczny adres serwera to 150.254.1.1, podczas gdy rzeczywisty adres to 150.254.1.200.
- Numer portu docelowego też może ulec zmianie.
- Jest konieczna, gdy chcemy udostępnić publicznie usługę zlokalizowaną w sieci prywatnej.



Dodatkowe funkcje zapór sieciowych

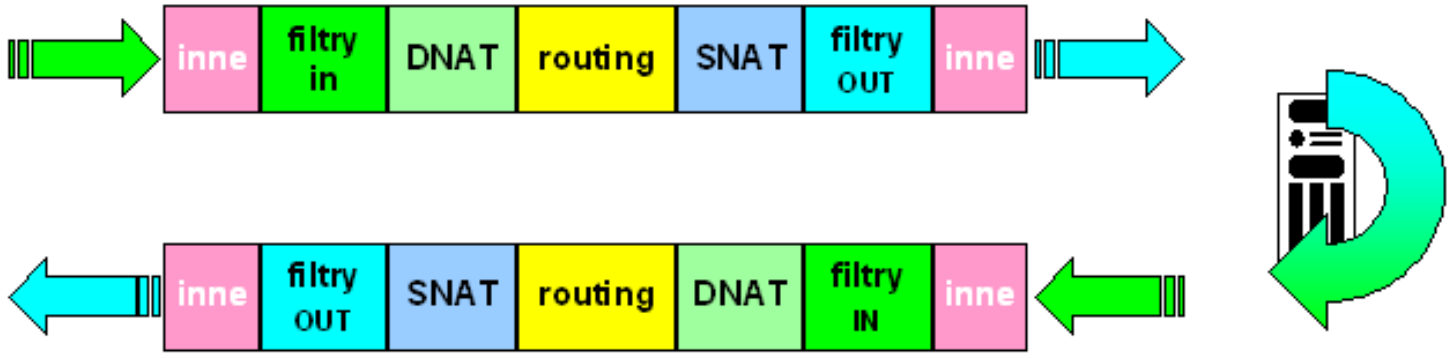
- Ściana ogniowa może realizować jedynie funkcje podstawowe.

- Może realizować również funkcje dodatkowe:

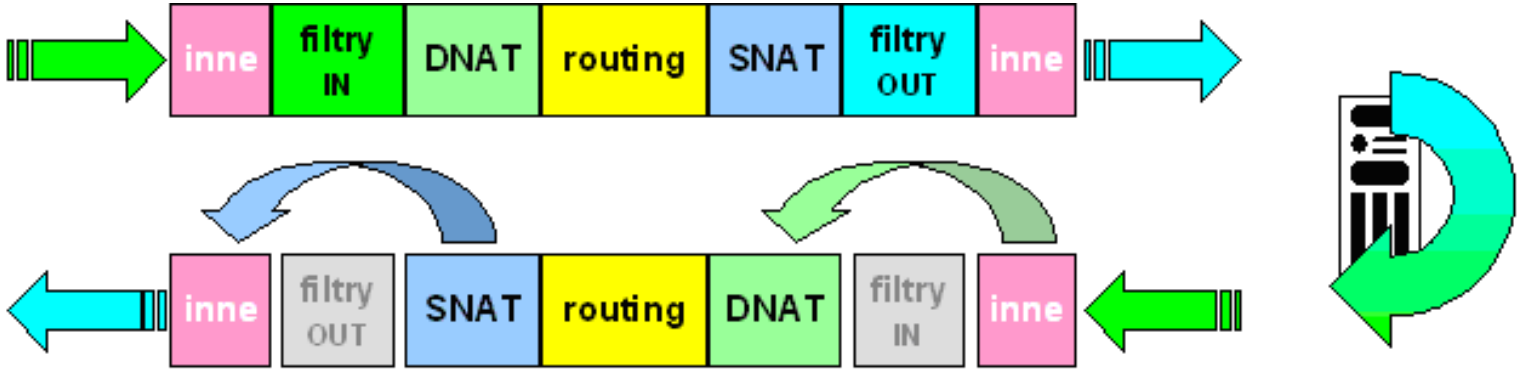
  - obrona przed atakami DoS – specyfikowanie dopuszczalnego strumienia ruchu wejściowego, np. w pakietach na sekundę;
  - kontrola fragmentacji IP i śledzenie numerów sekwencyjnych TCP (sprawdzanie, czy znajdują się w oczekiwanym zakresie);
  - wsparcie dla IPv6, fragmentacja, ICMPv6, ochrona przed atakami DoS analogicznymi jak dla IPv4;
  - filtry IPv6, np. ipf (FreeBSD), rozpoznawanie tunelowania IPv6 w IPv4 (tzn. takich protokołów jak 6to4, 6over4, Toredo);
  - integracja z aplikacjami zewnętrznymi, np. antywirusowymi, rodzicielskiego ograniczania dostępu (ang. *parental control*), systemami detekcji intruzów (IDS).

Filtry kontekstowe

- Standardowy przepływ ruchu poddawanego filtracji



- Filtr kontekstowy podejmuje decyzję na podstawie weryfikacji kontekstu, stanu:
  - każda zainicjowana poprawnie sesja jest pamiętana;
  - w drodze powrotnej pakiet jest sprawdzany na przynależność do zapamiętanej sesji – filtracja może być pominięta.



Jakie są problemy w realizacji zapór sieciowych?

- Filtrowanie usług takich jak FTP:
  - czy będzie naruszeniem polityki bezpieczeństwa, jeśli filtr kontekstowy w zaporze obsłuży komendę PORT 23 protokołu FTP?
- Filtracja pofragmentowanych pakietów:
  - odrzucanie tylko pierwszych fragmentów umożliwia wyciek informacji w strumieniu wyjściowym;
  - istnieją narzędzia do tak perfidnego fragmentowania, aby flagi ACK i SYN nagłówka TCP nie pojawiały się w pierwszym fragmencie;
  - można scalać fragmenty na zaporze – uwaga na błędy przy scalaniu;
  - można narzucić wymóg, aby pierwszy fragment zawierał co najmniej 16 bajtów danych, a najlepiej cały nagłówek TCP.

Problemy realizacji zapór sieciowych, cd.

- Bardzo trudno jest sprawnie pielęgnować duży zbiór reguł.
- Częste zmiany personelu i brak dokumentacji umożliwiającej pielęgnację starych reguł (odziedziczonych po poprzednim administratorze) powiększa trudności.
- Duże organizacje posiadają złożoną politykę bezpieczeństwa, co implikuje wielość nachodzących na siebie domen bezpieczeństwa i trudności w zdefiniowaniu i pielęgnacji spójnych reguł filtracji.
- Autoryzowane tunele wirtualne mogą być potencjalnym nośnikiem nieautoryzowanych treści poza kontrolą zapór sieciowych.
- Propagowanie połączeń (ang. *port forwarding*) może przyczynić się do skutecznego ominięcia kontroli na zaporze.

Problemy realizacji zapór sieciowych, cd.

- Trudności sprawia dość rozpowszechniony protokół SOAP (Simple Object Access Protocol), służący do tunelowania jakiegokolwiek ruchu w HTTP.
- Pod tym względem skrajnie wywrotowe są programy typu httptunnel czy Socks2http.
- Stworzono je, aby umożliwić tunelowanie blokowanej komunikacji (np. peer-to-peer) i obchodzić restrykcje wprowadzane przez zapory sieciowe – ruch HTTP prawie nigdy nie jest blokowany.
- Milcząco zakłada się, że komputery w chronionej sieci wewnętrznej są godne zaufania. Nawet jeśli ich użytkownicy są godni zaufania, to laptopy podłączane do Internetu podczas podróży służbowych mogą przenieść złośliwe oprogramowanie do sieci lokalnej.
- Zapory sieciowe chronią przed atakami z zewnątrz. Czy powinny także chronić sieć publiczną przed atakami wychodzącymi z ochranianej sieci?