9. Zapory sieciowe (firewall) i translacja adresów

W dziedzinie zabezpieczeń ruchu sieciowego dużą rolę odgrywają systemy kontroli komunikacji nazywane w języku ang. firewall. W języku polskim ścierają się na ogół dwa terminy: zapora sieciowa oraz ściana przeciwogniowa. Drugi z nich jest tłumaczeniem rdzennego pojęcia amerykańskiego (rysunek 1)

> Def.: **fire wall** – ognioodporny mur używany jako zapora zapobiegająca rozprzestrzenianiu się ognia.
>
> *Słownik dziedzictwa amerykańskiego*

Rysunek 1. Etymologia pojęcia firewall

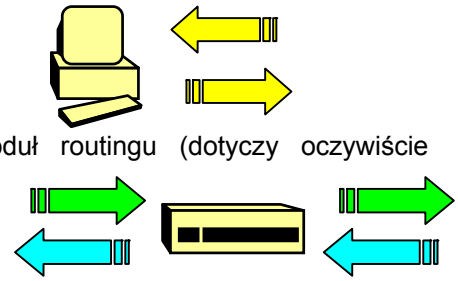
Inną analogią tego pojęcia jest kontrola paszportowa i celna na granicy – w naszym przypadku granicy sieci komputerowej.

Podstawowe funkcje systemów firewall

Podstawowe funkcje systemów firewall obejmują filtrację ruchu oraz pośredniczenie w dostępie do usług sieciowych

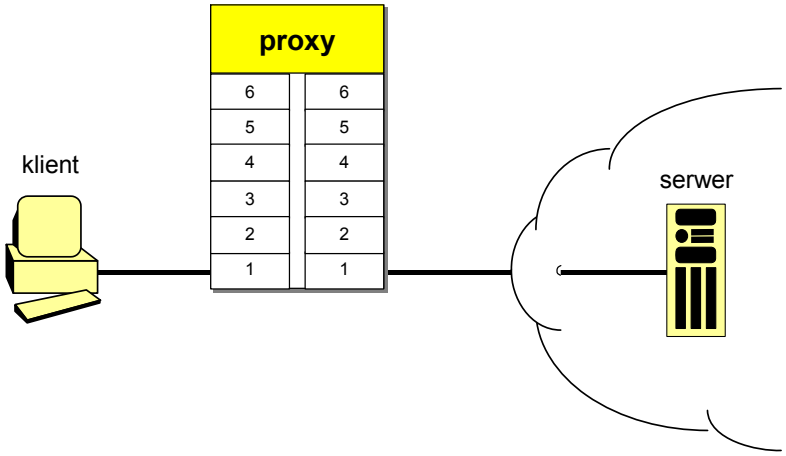
Filtracja pakietów to podstawowa forma zabezpieczenia sieci. Polega na analizie pakietów (a dokładniej parametrów ruchu zawartych w nagłówkach pakietów) warstwa 3 (czasami 2-4) modelu OSI. Możliwa jest:

- filtracja pakietów nadchodzących
- filtracja pakietów wychodzących
- filtracja pakietów propagowanych przez moduł routingu (dotyczy oczywiście wyłącznie węzłów międzysieciowych)



Ruch sieciowy jest filtrowany (przepuszczany lub blokowany) w zależności od decyzji podjętych na podstawie analizy pakietów, przy zastosowaniu zdefiniowanych reguł (reguł filtracji).

Pośredniczenie w dostępie do usług jest realizowane poprzez odseparowanie świata wewnętrznego i zewnętrznego względem zapory sieciowej (brak funkcji routingu). Komunikacja poprzez zaporę nie jest możliwa w żadnej warstwie poza aplikacyjną (warstwa 7 modelu OSI). Na zaporze uruchomione są aplikacje pośredniczące (*proxy services*) w komunikacji końcowych aplikacji użytkowych (np. klient-serwer). Oznacza to, iż klient, uruchomiony – przyjmijmy – w sieci wewnętrznej, nie może nawiązać połączenia bezpośrednio z serwerem pracującym w sieci zewnętrznej. Może tylko nawiązać połączenie z aplikacją proxy. Ruch może przechodzić przez zaporę, jedynie gdy zostanie pozytywnie sklasyfikowany przez aplikację proxy. Zaakceptowane połączenie od klienta jest następnie zestawiane w imieniu klienta przez aplikację proxy z serwerem. W istocie zatem utrzymywane są dwa połączenia: klient-proxy i proxy-serwer dolecowy.



Rysunek 2. Model pośredniczenie w realizacji usług (firewall typu proxy)

Podstawowe komponenty systemów firewall

Systemy firewall konstruowane są ze złożenia wymienionych poniżej komponentów.

- Specjalizowany węzeł międzysieciowy (router)

  Jest to rozwiązanie najprostsze i najłatwiejsze w utrzymaniu. Można je zrealizować przy pomocy następujących urządzeń:

  - router filtrujący (*screening router*)
  - router szyfrujący (*ciphering router*)

- Komputer Twierdza (***Bastion Host***)

  Jest to dedykowana stacja lub węzeł międzysieciowy, na którym uruchomione są usługi proxy.

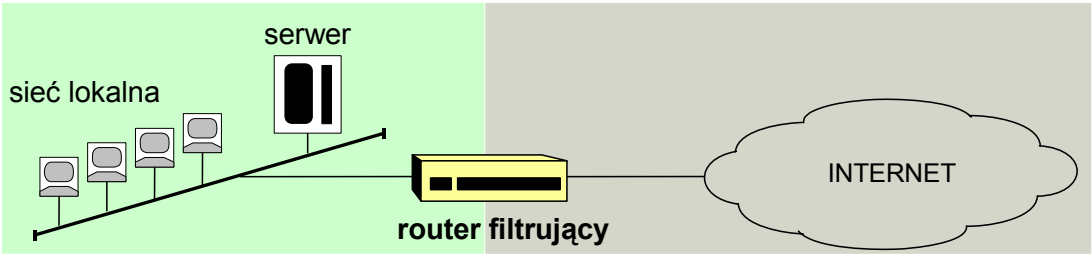
- Strefa Zdemilitaryzowana (***Demilitarized Zone – DMZ***)

  Jest to 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 sieci chronionej.

Router filtrujący

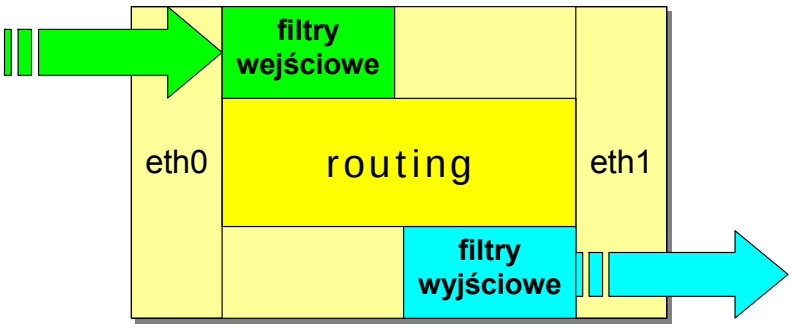
Podstawowym zagadnieniem dotyczącym realizacji zapory sieciowej tego typu jest kwestia definicji reguł filtracji. Reguły filtracji operują w ogólności na parametrach analizowanych pakietów, takich jak:

- adresy z nagłówka protokołu sieciowego (źródłowy i docelowy)
- typ protokołu (PDU i SDU, np. protokołu transportowego)
- rodzaj usługi (numer portu z nagłówka protokołu transportowego)



Rysunek 3. Model systemu z zaporą sieciową typu router filtrujący

Schemat wewnętrznej kompozycji urządzenia filtrującego jest przedstawiony na rysunku 4. Możliwe jest utrzymywanie oddzielnych list filtracji dla ruchu wchodzącego i wychodzącego z zapory sieciowej.



Rysunek 4. Model modułu filtracji

Filtry można zdefiniować na następujące sposoby:

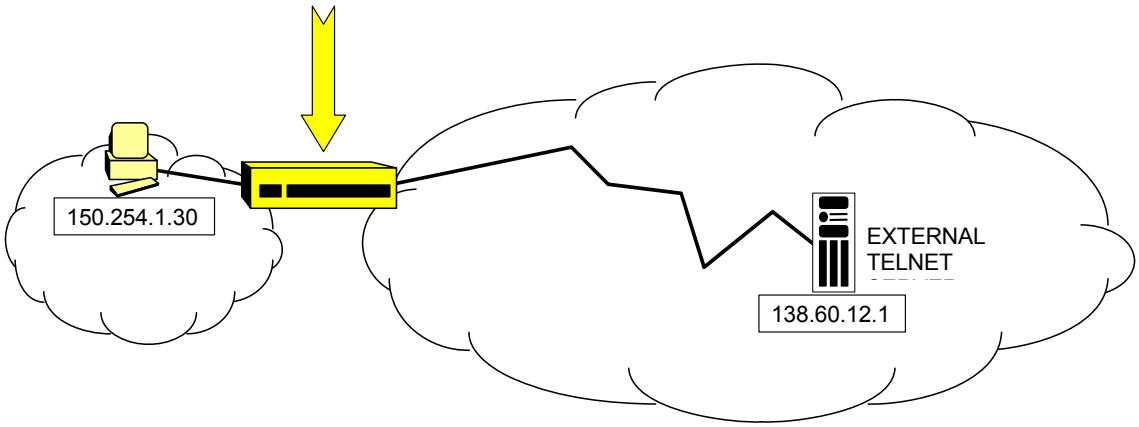
- filtry statyczne – definicje reguł filtracji są dokonane z wyprzedzeniem i obowiązują aż do jawnej ich zmiany
- filtry kontekstowe – realizują dynamiczne reguły filtracji (SPF = Stateful Packet Filtering)
  - w trakcie pracy aktualizowane są informacje o bieżących sesjach (asocjacjach protokołu sieciowego)
  - decyzje o filtracji pakietów podejmowane są z uwzględnieniem stanu sesji, do której przynależą
- filtracja nieliniowa:
  - elastyczne definiowanie wyrażeń warunkowych (zagnieżdżone reguły logiczne)

Przykład statycznych reguł filtracji pokazuje rysunek 5. Opisuje on filtrację przypadku z rysunku 6. Na nim mamy hipotetyczną sieć wewnętrzną, której stacjom zezwala się na nawiązywanie połączeń tylko wybranej usługi (w przykładzie – telnet) i jedynie z wybranym serwerem zewnętrznym.

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

Rysunek 5. Przykładowe statyczne reguły filtracji

Reguły zdefiniowane na statycznej liście filtracji są przeglądane sekwencyjnie do pierwszego trafienia. Dla pasującej reguły jest aplikowane zdefiniowane w niej działanie (na ogół akceptacja lub odrzucenie pakietu). Reguła nr 1 zezwala na ruch wychodzący na zewnątrz jeśli adres nadawcy należy do zakresu adresów sieci wewnętrznej, odbiorcą pakietu jest wyróżniony serwer zewnętrzny, port nadawcy nie jest portem systemowym, a port odbiorcy zgadza się z portem usługi telent. Druga reguła zezwala na ruch w przeciwnym kierunku, pod warunkiem odwrotnej kombinacji parametrów, lecz jedynie pod warunkiem, że w nagłówku TCP ustawiona jest flaga ACK. Natomiast w przypadku, gdy flaga ta jest wyzerowana, ruch wchodzący z serwera jest blokowany. Jest konsekwencją faktu, iż flaga ACK jest wyzerowana jedynie w pierwszym segmencie TCP – nawiązującym połączenie (segment SYN). Nie jest oczywiście naturalne, by serwer usługi telent próbował zestawić połączenie z klientem ochranianej sieci, zatem taką sytuację należy rozpoznać jako podejrzaną i odrzucić pakiet (najprawdopodobniej oprogramowanie podszywające się za serwer próbuje nawiązać połączenie ze stacjami wewnątrz chronionej sieci). Reguła ostatnia jest realizacją zasady domyślnej reguły dostępu – blokuje jakikolwiek ruch, który nie został zdefiniowany w poprzednich regułach.



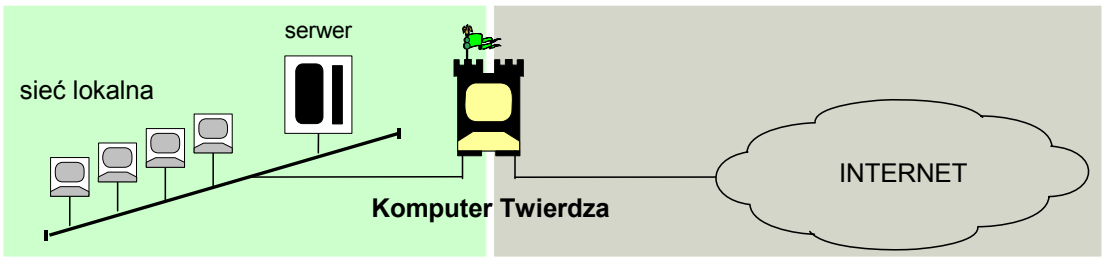
Rysunek 6. Schemat sieci do przykładu definicji statycznych reguł filtracji

Statyczne reguły filtracji posiadają kilka ograniczeń. Przykładowo niektóre usługi trudno poddają się filtracji statycznej (np. FTP, X11, DNS). Rozważmy jak w trybie aktywnym pracy serwera FTP (przypomnij sobie jaki to tryb) ochronić się przed nadużyciem, w którym oprogramowanie podszywające się za serwer próbuje nawiązać połączenie ze stacjami wewnątrz chronionej sieci. Z pomocą przychodzą pewne nowe rozwiązania proponowane w samych protokołach aplikacyjnych. Coraz powszechniej wprowadza się i stosuje tryby pracy zmodyfikowane pod

kątem usprawnienia filtracji, np. tryb *passive* w protokole FTP (skądinąd użyteczny także np. przy korzystaniu z dostępu xDSL)

Komputer Twierdza

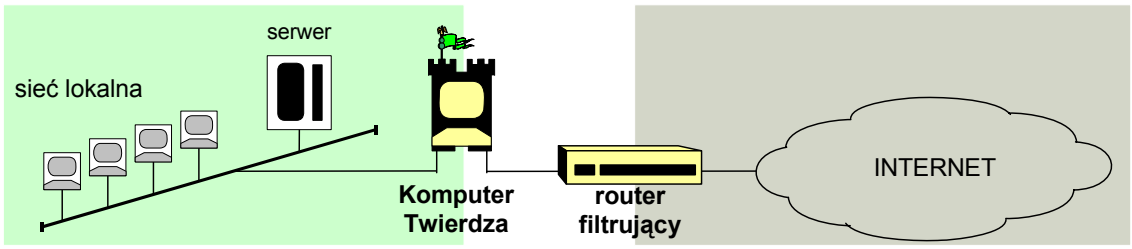
Komputer Twierdza to stacja z odseparowanymi interfejsami sieciowymi (*Dual Homed Host Gateway*) zajmująca miejsce węzła międzysieciowego (rysunek 7). Oferuje fizyczną i logiczną separację prywatnej sieci lokalnej od zewnętrznej sieci publicznej. Dzięki separacji interfejsów tylko Komputer Twierdza jest widoczny z sieci publicznej. Zatem, aby wtargnąć do sieci prywatnej trzeba uprzednio zawładnąć Komputerem Twierdzą. Komputer Twierdza pełni rolę bramy aplikacyjnej – usługi pośredniczące i zastępcze (*proxy*) rozwiązują problem usług trudnych do filtracji. Dzięki temu, iż jest on pełnym stanowiskiem komputerowym, potencjalnie wyposażonym w dowolne żądane oprogramowanie i praktycznie nieograniczone zasoby pamięci masowej, możliwa jest szczegółowa rejestracja zdarzeń (*auditing*), ułatwiająca diagnozowanie ewentualnie pojawiających się nowych zagrożeń i niedoskonałości konfiguracji.



Rysunek 7. Model systemu z zaporą sieciową typu Komputer Twierdza

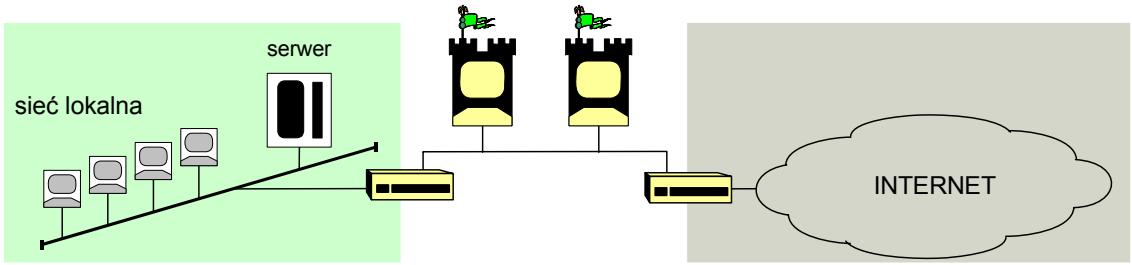
Filtracja podwójna

Rysunek 8 pokazuje schematyczne połączenie w jedną linię obrony różnych typów zapór sieciowych, dokładniej jest to brama aplikacyjna poprzedzona routerem filtrującym (*Screened Host Gateway*).



Rysunek 8. Model systemu z filtracją podwójną

Możliwe jest dalej „rozciągnięcie” Twierdzy na całą dedykowaną podsieć (*Screened Network*), co pokazuje z kolei rysunek 9, a nawet kaskadę podsieci.

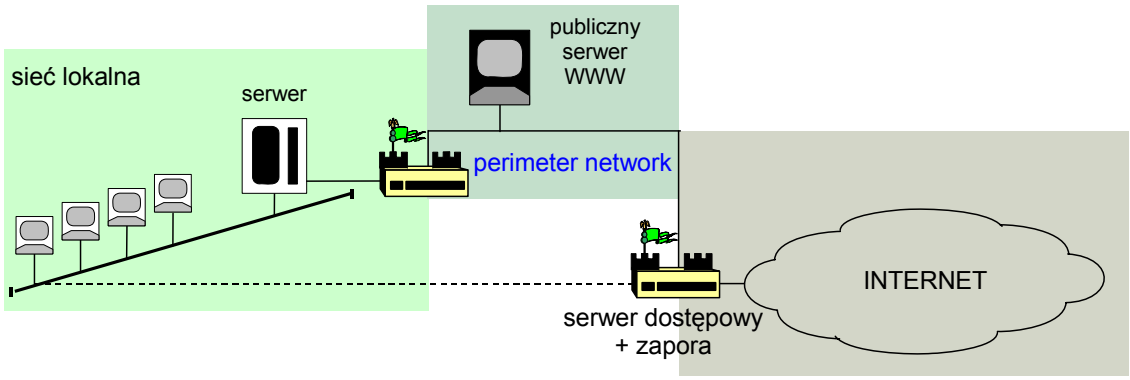


Rysunek 9. Model systemu z podsiecią ochronną

Strefa Zdemilitaryzowana

Konfiguracja która przyjęła się pod nazwą Strefa Zdemilitaryzowana (DMZ = *Demilitarized Zone*) to wydzielona podsieć zawierająca komponenty świadomie wyjęte spod kontroli obejmującej całą resztę sieci wewnętrznej, takie jak np.:

- publiczne zasoby (np. ogólnodostępny serwis WWW)
- przynęty, pułapki



Rysunek 10. Model systemu ze Strefą Zdemilitaryzowaną DMZ

Translacja adresów – Network Address Translation (NAT)

Translacja adresów jest powszechnym w sieciach komputerowych mechanizmem, który ma różne cele, a są to:

- rozszerzenie dostępu do sieci publicznej na stanowiska nie posiadające przydziału adresów publicznych (posiadające tylko adresy prywatne – RFC 1918)

- wykorzystanie wewnątrz sieci nieprzydzielonych publicznych adresów IP (za cenę braku możliwości komunikacji z takimi oficjalnymi adresami)
- ukrycie wewnętrznej struktury sieci przed światem zewnętrznym
- przekierowanie ruchu (portów: NAPT = Network Address Port Translation)

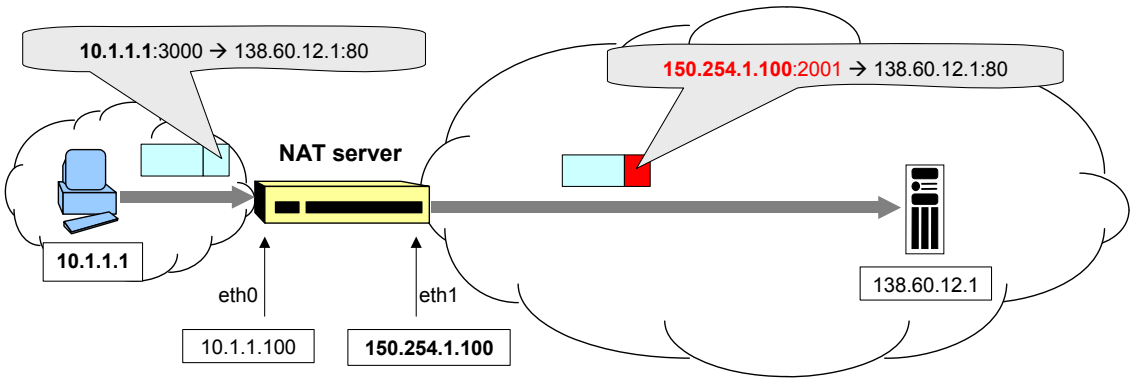
Metody wzajemnego odwzorowania adresów są ustandaryzowane i opisane w dokumentach:

- RFC1631 (translacja na pojedynczy adres, tj. N:1)
- RFC1597,1918 (translacja na pulę adresową, tj. N:M)

Wyróżnia się przy tym translację adresów źródłowych – Source NAT (SNAT) – oraz docelowych – Destination NAT (DNAT).

Translacja adresów źródłowych (SNAT)

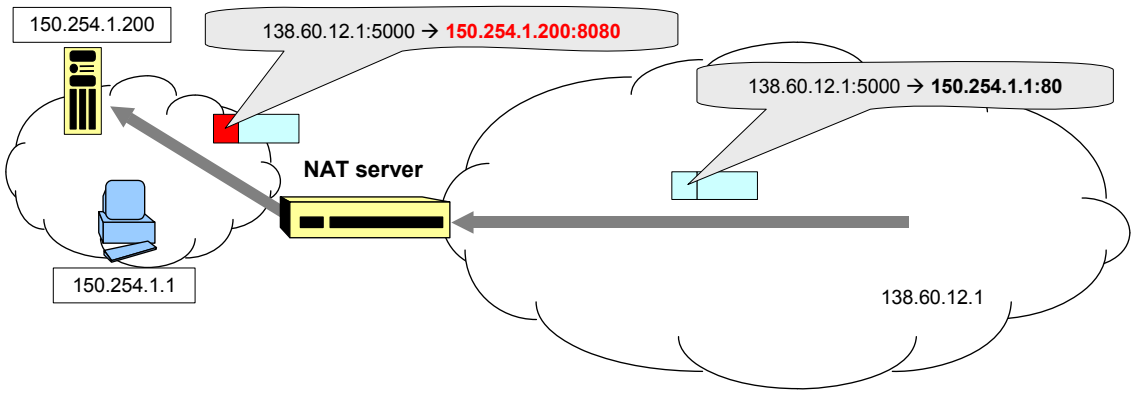
W tym przypadku pakiety wychodzące z sieci wewnętrznej otrzymują nowy adres źródłowy w nagłówku (rysunek 11). W przykładzie, pakiet wychodzący w rzeczywistości z adresu IP równy 10.1.1.1 otrzymuje po translacji adres źródłowy serwera translacji (jest nim brzegowy węzeł międzysieciowy), mianowicie 150.254.1.100. Numer portu źródłowego też ulega zmianie.



Rysunek 11. Schemat translacji adresów źródłowych (SNAT)

Translacja adresów docelowych (DNAT)

W mechanizmie Destination NAT (DNAT) pakiety przychodzące ze strony inicjującej (na ogół – sieci zewnętrznej) otrzymują nowy adres docelowy (w tym w szczególności – port). Celem może być przekierowanie ruchu określonej usługi pod rzeczywisty, nie ujawniany na zewnątrz, adres wewnętrznego serwera tej usługi. Na rysunku 12 adres serwera (o jaką usługę chodzi w tym przykładzie?) upubliczniony na zewnątrz jest równy 150.254.1.1, podczas gdy rzeczywisty adres to 150.254.1.200.



Rysunek 12. Schemat translacji adresów źródłowych (SNAT)

Dodatkowa funkcjonalność zapór sieciowych

Łańcuch funkcji realizowanych przez zapory sieciowe wyglądać może następująco:

jedynie funkcje podstawowe:

również funkcje dodatkowe:

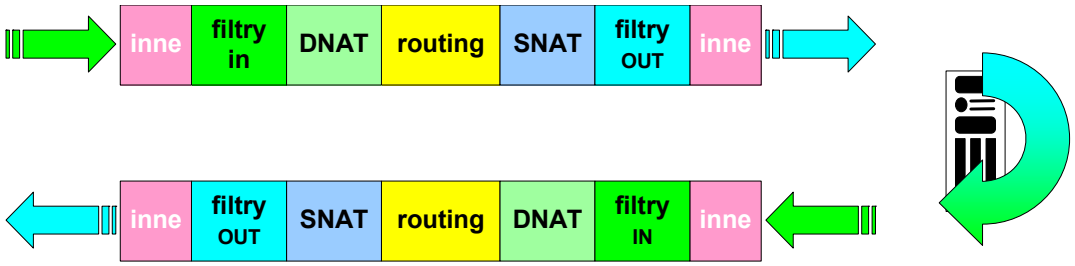
Dodatkowymi funkcjami mogą być

- obrona przed atakami DoS (*flood-wall*) – specyfikowanie dopuszczalnego rozmiaru strumienia wejściowego (np. w pakietach na sek.)
- kontrola fragmentacji IP i śledzenie numerów sekwencyjnych TCP (kontrola 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 różnymi zewnętrznymi modułami, np. systemami antywirusowymi, modułami sieciowej detekcji intruzów (IDS), czy ograniczenia dostępu (*parental control*)

Filtry kontekstowe

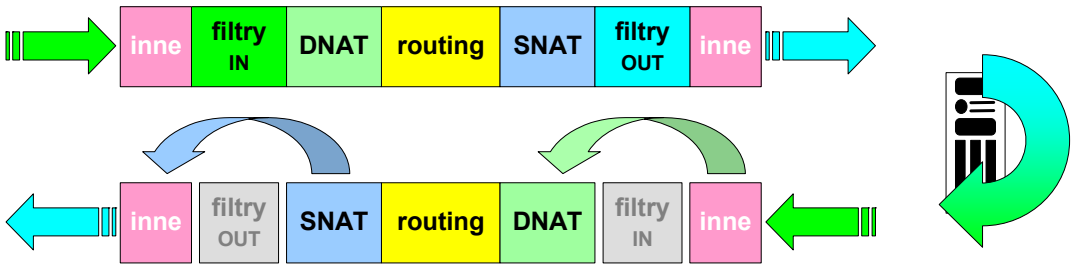
Standardowy przepływ ruchu poddawanego filtracji (*round-trip*) można przedstawić schematycznie postaci poniższej:



Filtry kontekstowe podejmują dynamicznie zmienne decyzje na podstawie weryfikacji kontekstu (*stateful inspection*):

- każda zainicjowana poprawnie sesja jest pamiętana na dynamicznych listach
- w drodze powrotnej pakiet jest sprawdzany na przynależność do zapamiętanej sesji – filtracja może być pominięta:

Przedstawia to poniższy schemat:



Problemy realizacji zapór sieciowych

Zapory sieciowe cierpią na wiele problemów, zarówno technologicznych jak i realizacyjnych. Problemy technologiczne dotyczą np. usług takich jak FTP. Przykładowo, jeśli filtr kontekstowy w zaporze obsłuży komendę PORT 23 protokołu FTP, to czy będzie to naruszenie polityki bezpieczeństwa? Problemy technologiczne związane są również z wykorzystaniem w ruchu sieciowym mechanizmów takich jak fragmentacja IP. Z filtracją pakietów pofragmentowanych związane są następujące problemy:

- odrzucanie tylko pierwszych fragmentów umożliwia wyciek informacji w strumieniu wyjściowym
- istnieją narzędzia do tak perfidnego fragmentowania, by 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 16B danych (a najlepiej cały nagłówek TCP)

Istotne problemy niesie ze sobą pielęgnacja reguł filtracji. Szczególnie trudna jest ona do sprawnego przeprowadzenia w przypadku dużych zbiorów reguł. Dodatkowo potęgują trudności częste na naszym rynku informatycznym zmiany personelu i brak dokumentacji uniemożliwiający pielęgnację starych reguł (odziedziczonych po poprzednim administratorze). Często występują również problemy wewnętrzne: duże organizacje posiadają często złożoną politykę bezpieczeństwa, co implikuje wielość nachodzących na siebie domen bezpieczeństwa i trudności w definicji i pielęgnacji spójnych reguł filtracji.

Ostrożnie należy też postępować z tunelami wirtualnymi. Autoryzowane tunele VPN mogą być potencjalnym nośnikiem nieautoryzowanych treści poza kontrolą zapór ogniowych. Zatem powinny być zaplanowane i zrealizowane w sposób przemyślany. Podobnie jak VPN, również propagowanie połączeń (*port forwarding*) może przyczynić się do skutecznego ominięcia kontroli na zaporze. Podobnie trudności sprawia dość rozpowszechniony protokół SOAP (*Simple Object Access Protocol*), służący, mówiąc kolokwialnie, do tunelowania jakiegokolwiek ruchu w HTTP. Pod tym względem skrajnie wywrotowy jest *httptunnel* (http://www.noccrew.org/software/httptunnel.html)

Pytania problemowe

1. W przykładzie statycznych reguł filtracji z rysunku 5 zdefiniowano 4 reguły. Jedna z nich jest jednak nadmiarowa i można ją usunąć bez żadnych konsekwencji dla przebiegu filtracji. Która to reguła?