Sieci komputerowe

Wykład 9
Brakuje adresów? NAT

IPv4

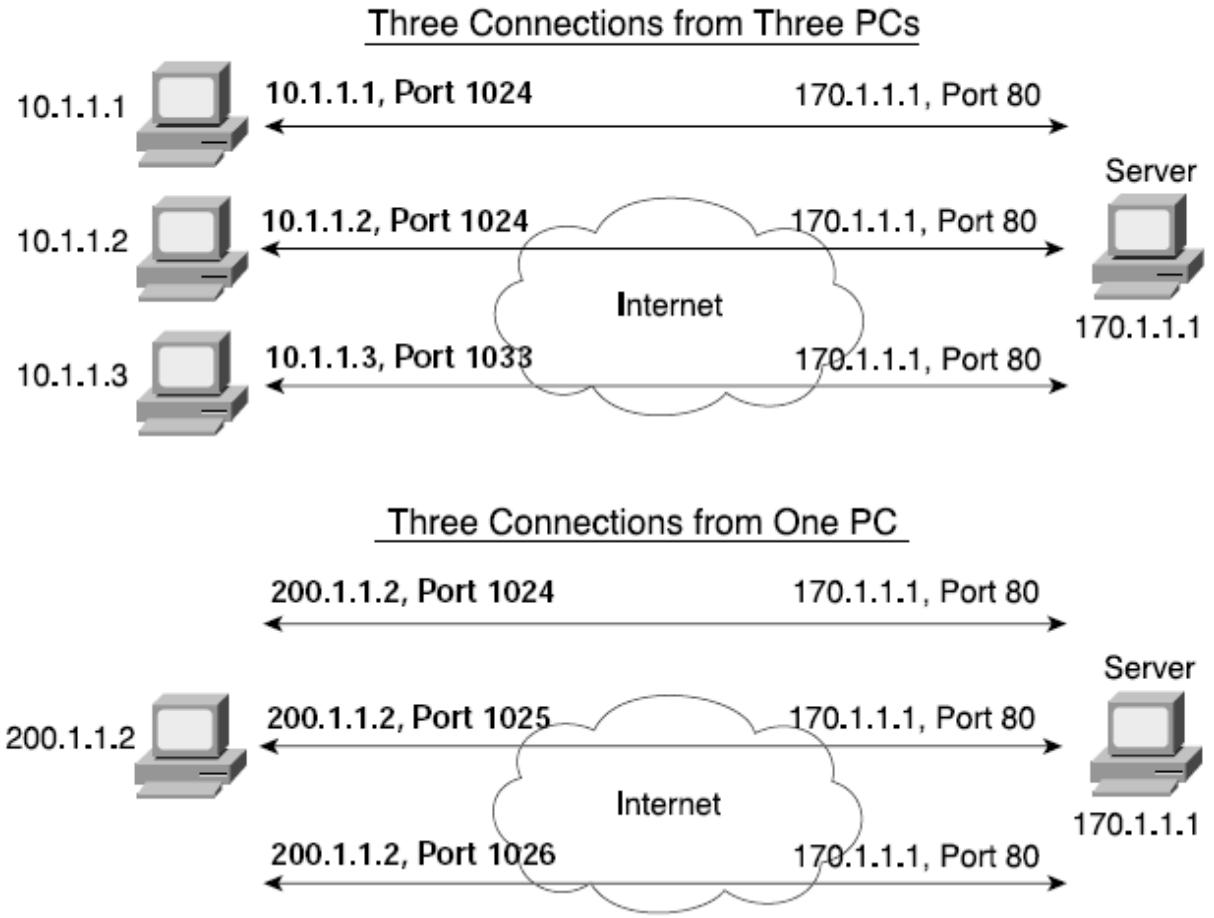
Źródło: http://www.nic.ad.jp/en/ip/ipv4pool/

Translacja adresów (NAT)

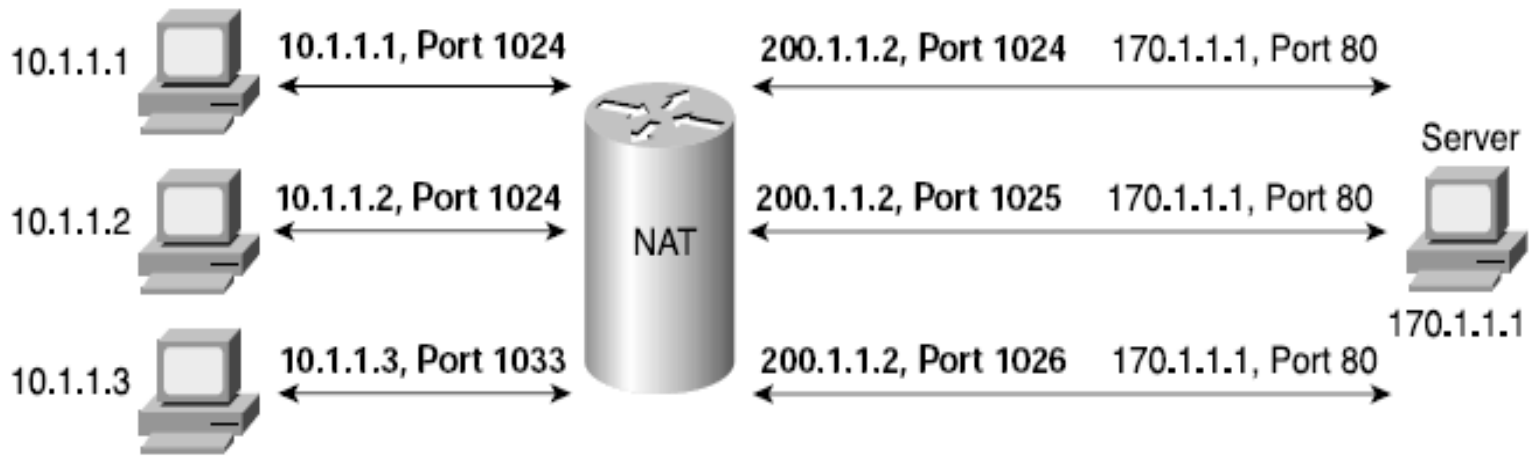
- NAT (ang. Network Address Translation) umożliwia używanie adresów nierutowalnych (niepublicznych)
- Polega na „maskowaniu” połączeń z wielu adresów nierutowalnych jednym publicznym adresem IP
- Nie można wykonywać połączeń bezpośrednio do adresów niepublicznych, wpływa to na zwiększenie bezpieczeństwa
- NAT został wprowadzony ze względu na brak adresów IP

Połączenia bez użycia NAT

Three TCP Connections: From Three Different Hosts, and from One Host



Połączenia z użyciem NAT



Dynamic NAT Table, With Overloading

Inside Local	Inside Global
10.1.1.1:1024	200.1.1.2:1024
10.1.1.2:1024	200.1.1.2:1025
10.1.1.3:1033	200.1.1.2:1026

- Zmieniany jest adres IP i/lub port
- Powyższy rysunek ilustruje technikę SNAT (zmiana adresu źródłowego)
- Stosuje się także DNAT (zmiana adresu docelowego)

Serwery proxy

- Serwer proxy (pośredniczący) wykonuje połączenia w imieniu użytkownika
- Użytkownik „zleca” wykonanie połączenia za pomocą oprogramowania klienckiego – zwykle przeglądarki internetowej
- Użytkownik nie musi posiadać publicznego adresu IP
- Proxy wykona za niego połączenia do sieci zewnętrznych i przekaże odpowiedź
- Proxy działa w warstwie aplikacji – wadą jego jest obsługa niewielu protokołów (głównie FTP i HTTP)

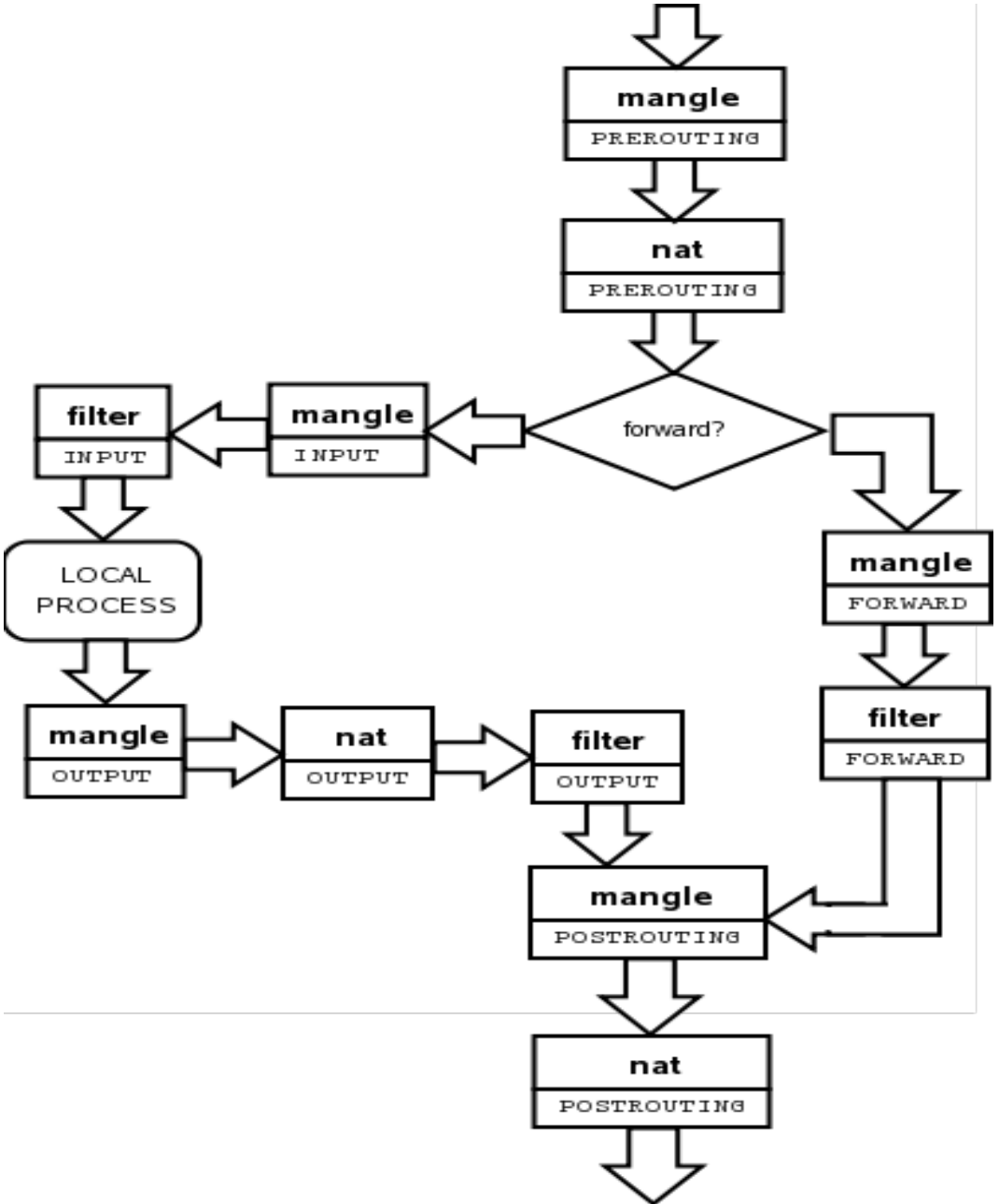
Ściany ogniowe

- Ściany ogniowe (ang. firewall) filtrują adresy
- Mogą też obserwować stany połączeń
  - firewall stanowy
  - firewall bezstanowy (nie śledzi stanu połączeń)
- Konfiguracja za pomocą reguł

Iptables

- Iptables to program do obsługi filtru (firewalla) wbudowanego w jądro systemu operacyjnego Linux
- http://www.netfilter.org

Iptables – diagram przepływu



Iptables

- Dodawanie reguły
  - iptables [-t tablica] komenda [wzorzec] [akcja]

Iptables - przykład

```
# Adres IP hosta
ip=”10.1.1.134”

# Domyślna akcja tablicy filter: DROP
iptables -P INPUT DROP   # ustawia domyślną akcję
iptables -F INPUT        # usuwa wszystkie reguły
iptables -P OUTPUT DROP
iptables -F OUTPUT
iptables -P FORWARD DROP
iptables -F FORWARD
iptables -F -t nat

# Wpuszczamy nawiązane połączenia
iptables -A INPUT -i eth0 -s 0.0.0.0/0 -d $ip \
  -m state --state ESTABLISHED,RELATED -j ACCEPT

# Wypuszczamy wszystko z naszego hosta
iptables -A OUTPUT -o eth0 -s $ip -d 0.0.0.0/0 -j ACCEPT
```

Iptables – przykład c.d.

```
iptables -A INPUT -i eth0 -j DROP
iptables -A OUTPUT -o eth0 -j DROP


iptables -A INPUT -i eth0 -j REJECT
iptables -A OUTPUT -o eth0 -j REJECT \
  --reject-with icmp-host-unreachable
```

Iptables, NAT

```
# cat /etc/sysctl.conf
net.ipv4.ip_forward = 1
# sysctl -p /etc/sysctl.conf

iptables -t nat -A POSTROUTING -s 10.0.0.0/16 -j SNAT \
--to-source 193.0.96.15

iptables -t nat -A PREROUTING -d 193.0.96.200 -j DNAT \
--to-destination 10.1.1.20

iptables -t nat -A PREROUTING -p tcp -d 193.0.96.201 \
--dport 222 -j DNAT -to-destination 10.1.1.212:22
```

Demo