ECE 671 – Lecture 14

Transport Layer Systems
Firewalls and NAT

Transport layer systems

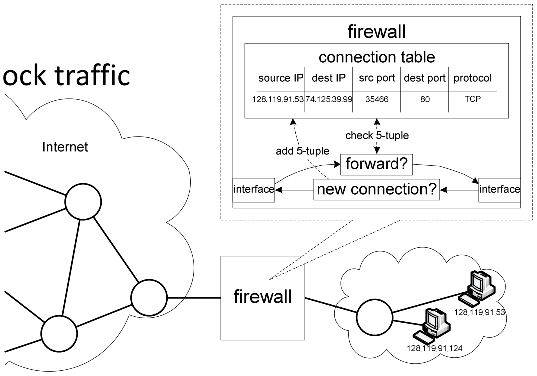
- Traffic handling at level of connections or flows
  - Firewall
  - Network Address Translator

Firewall

- Firewall distinguishes between traffic sources
  - “Inside” traffic is let through
  - “Outside” traffic is blocked
- How to achieve duplex communication?

Firewall

- Firewall keeps record of connections from inside
  - Traffic with reverse 5-tuple is let through from outside
- Additional feature
  - Rules to allow or block traffic
- How can a firewall be circumvented?

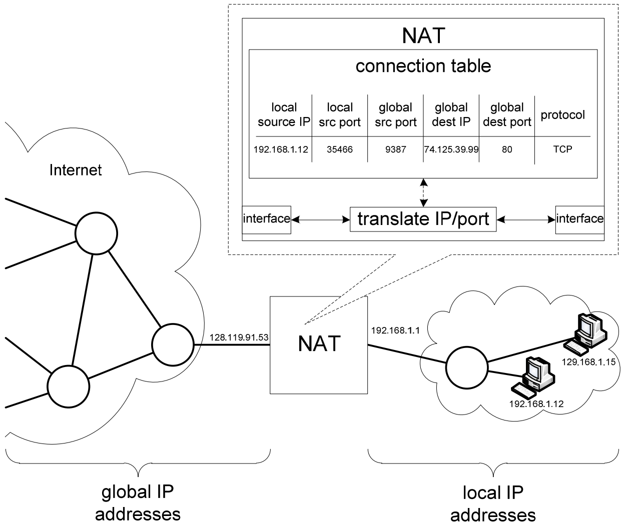


source IP	dest IP	src port	dest port	protocol
128.119.91.53	74.125.39.99	35466	80	TCP

Network Address Translation

- Limited IP address space
  - Use reserved space for home/corporate networks: 192.168/16 or 10/8
  - Use only one IP address toward Internet
- NAT translates between outside and inside addresses
  - How can multiplexing/demultiplexing be achieved?

Network Address Translation

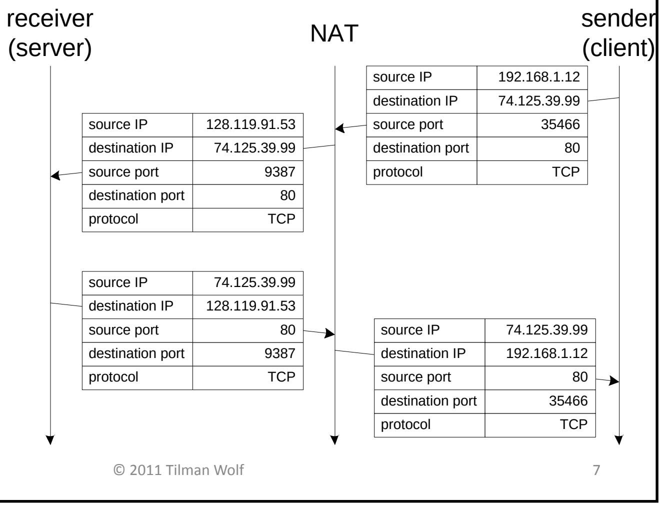


connection table

local source IP	local src port	global src port	global dest IP	global dest port	protocol
192.168.1.12	35466	9387	74.125.39.99	80	TCP

Network Address Translation

- NAT box tracks connections
  - Port number identifies connection
  - NAT box overwrites layer 3/4 headers



source IP	192.168.1.12
destination IP	74.125.39.99
source port	35466
destination port	80
protocol	TCP

source IP	128.119.91.53
destination IP	74.125.39.99
source port	9387
destination port	80
protocol	TCP

source IP	74.125.39.99
destination IP	128.119.91.53
source port	80
destination port	9387
protocol	TCP

source IP	74.125.39.99
destination IP	192.168.1.12
source port	80
destination port	35466
protocol	TCP

Transport layer systems

- Firewall and NAT keep track of similar information
  - Functionality often combined in same system
  - Home gateways typically implement firewalls, NAT, DHCP
- More sophisticated firewalls also use content filter
  - Requires application layer system