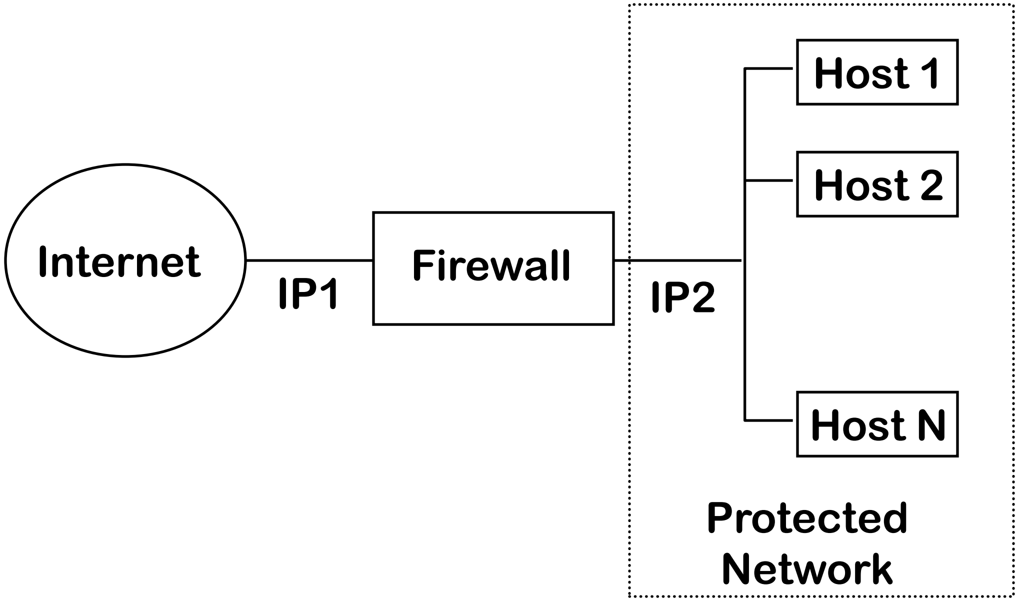
H.O. #11

Winter 98-99

IP Firewalling and Masquerading

Purpose



- Machines in the "Protected Network" can access the Internet normally.
- Packets coming from the "Protected Network" appear to be all coming from IP1.
- Addresses in the "Protected Network" are in the private range.

Implementation

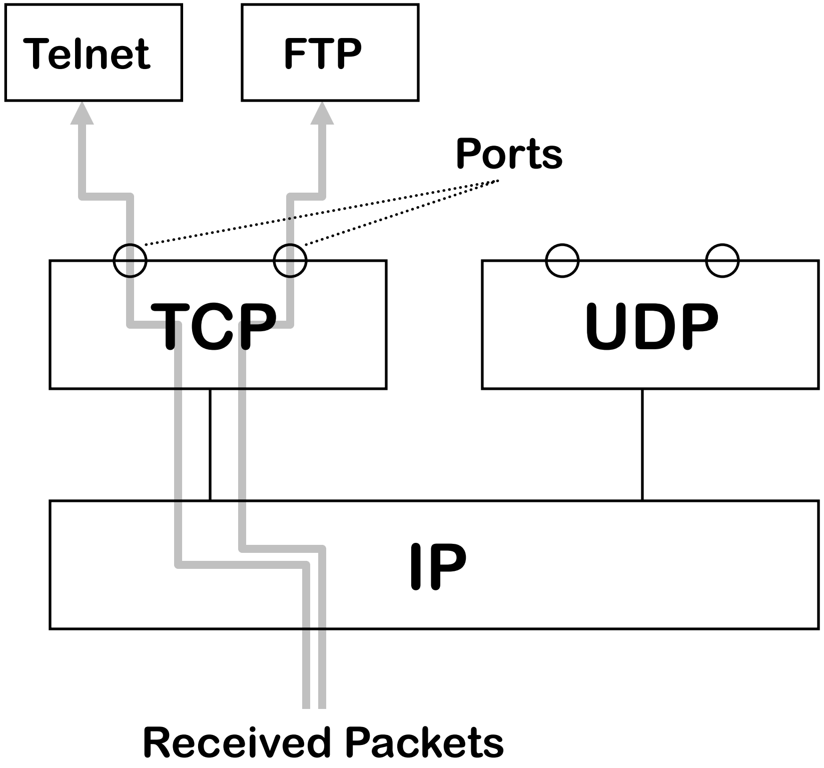
- Hosts inside the Private Network are configured to use the Firewall (IP2) as their gateway.
- The Firewall rewrites the IP header for the outbound packets, replacing the original source IP address with its own (IP1) address. This way, all the packets “seem” to be coming from IP1.
- The destination IP address in the incoming packets (from the Internet to the Private Network) is rewritten, replacing IP1 with the internal IP address of the destination.
- Problem: how to figure out the right destination inside the Protected Network?

Demultiplexing Incoming Packets

- There is not enough information in the IP header to demultiplex incoming packets and decide to which host in the Protected Network each packet is destined.
- It is necessary to use information from the next protocol layer (transport layer) to perform this function.
- Common transport layers over IP: UDP and TCP.
- Transport layer has the concept of a “Port”, which identifies ***which process*** in the host should finally get the packet.

Ports

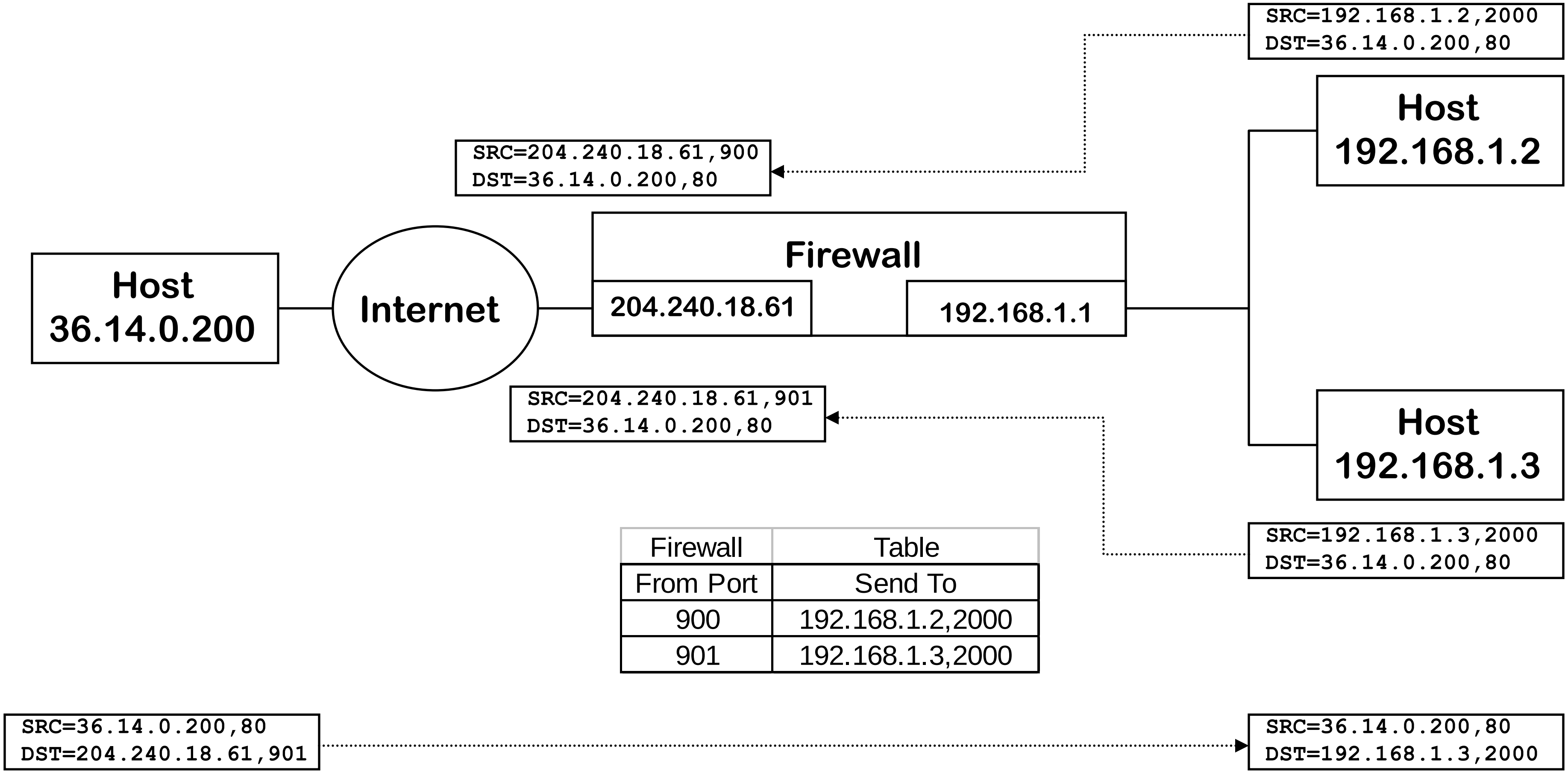
- Ports are 16-bit numbers that identify which process should get the packet.
- UDP and TCP ports exist in different spaces.
- Each packet carries two port numbers:
  - The “source port” of the process who generated it in the source host
  - The “destination port” of the process who should get it in the destination host



Implementation, Revisited

- Upon receiving an outbound packet from a host in the Protected Network, the firewall:
  - rewrites the packet's source IP address as its own address (IP1)
  - generates a local source port and rewrites the packet's source port as this local source port; makes a record of this port
- Upon receiving an inbound packet from the Internet, the firewall checks whether the packet's destination port is in its list of local ports:
  - If the port is in the list, the firewall knows where to send the packet, and rewrites its destination IP and destination port.
  - If the port is not in the list, the packet is dropped.
- Internet hosts cannot start connections

Example



SRC=192.168.1.2,2000
DST=36.14.0.200,80

Host
192.168.1.2

SRC=204.240.18.61,900
DST=36.14.0.200,80

Firewall

204.240.18.61

192.168.1.1

Host
36.14.0.200

Internet

SRC=204.240.18.61,901
DST=36.14.0.200,80

Host
192.168.1.3

SRC=192.168.1.3,2000
DST=36.14.0.200,80

Firewall	Table
From Port	Send To
900	192.168.1.2,2000
901	192.168.1.3,2000

SRC=36.14.0.200,80
DST=204.240.18.61,901

SRC=36.14.0.200,80
DST=192.168.1.3,2000