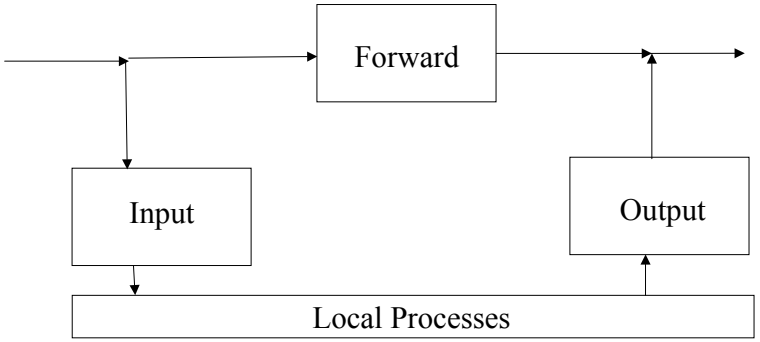
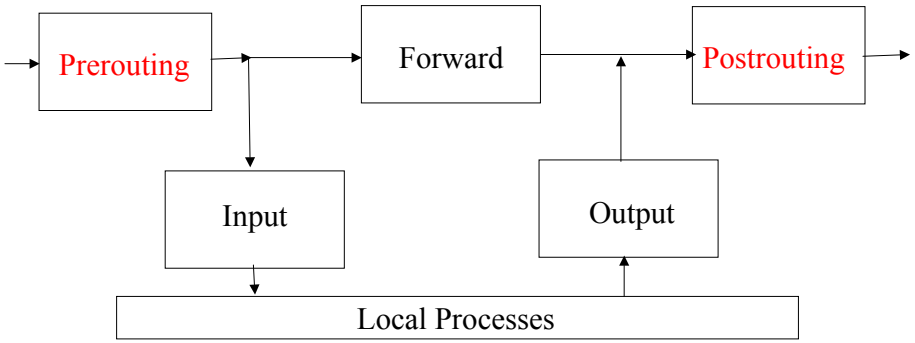
Linux Configuration for NAT and Firewall

- Iptables
  - Several different "tables"
    - Filter
    - NAT
    - Mangle – not talking about this one
  - Each table has several built-in "chains"
  - Each chain has several "rules"
  - Each rule has a "match part" and a "target" part
- Filter table chains
  - Input
  - Forward
  - Output
- NAT table chains
  - Prerouting
  - Postrouting
- User-defined chain
  - Add to any table
  - Use as subroutine in pre-defined chains

Filter table chains



NAT table chains



Rule format

- iptables [-t table] –L –v
  - List the chains (and their rules) in the named table, defaults to the filter table
- iptables [-t table] –A <chainname> <match> -j <target>
  - If the packet matches the <match> condition then do <action>
- Within each chain, rules are checked in order
- If the end of a built-in chain is reached the action taken is specified by the **chain policy**.
- If the end of a user-defined chain is reached, continue with the next rule in the calling chain

Iptables - targets

- DROP
  - Silent drop
- ACCEPT
- REJECT
  - Like DROP but sends ICMP
- RETURN
  - Same as falling off the end of the chain
    - Built-in chain: apply chain policy
    - User-defined chain: return to calling chain
- <chain-name>
  - "call" the named chain

Creating a user-defined chain

- iptables [-t table] –N <chain-name>
  - Note that the chain "belongs to" a particular table, (default: the filter table) and is usable only from that table
- User-defined chains, like functions in a program, help organize the rules

Stateless match elements

- source
  - -s [!] <source-ip or name>
- Destination
  - -d [!] <dest-ip or name>
- Protocol
  - -p (tcp|udp|icmp)
- After –p tcp or –p udp
  - Source port: --sport [!] <portnum or name>
  - Dest port: --dport [!] <portnum or name>

Stateful match elements

- -m state –state [!] <statelist>
- statelist: a comma-separated list of
  - NEW
    - Packet creates a new connection
  - ESTABLISHED
    - Packet on an existing connection
  - RELATED
    - ICMP related to an existing connection
  - INVALID
    - Packet not classifiable

Stateful match elements (cont'd)

- -m limit [-limit num1[/(s|m|h|d)] [-limit-burst num2]
  - matches num1 times per second, minute, hour or day
  - After an initial burst of num2 matches
  - Default: num1=3/h, num2=5
- Uses:
  - Reduce the rate of log messages
  - Avoid DoS attacks

Example filter rules

- iptables –A INPUT –s ! localhost –p tcp --dport 5801 –j DROP
- iptables –A INPUT –s ! localhost –p tcp --dport 5901 –j DROP
- iptables –A INPUT –s localhost –p tcp --dport 6001 –j ACCEPT
- iptables –A INPUT –s poipu.eecs.wsu.edu –p tcp --dport 6001 –j ACCEPT
- iptables –A INPUT –p tcp --dport 6001 –j REJECT --reject-with icmp-port-unreachable
- Policy is ACCEPT

Rules for the nat table

- Rules in the PREROUTING and POSTROUTING chains
- Matches approximately the same as in the filter table
- Targets
  - SNAT
    - Allows "protected" host to use internet services
    - iptables -t nat –A POSTROUTING -j SNAT --to <ip address range>:<port range>
  - DNAT
    - Allows internet host to contact servers on "protected" hosts
    - iptables -t nat –A PREROUTING –d <> -p tcp --dport <> -j DNAT --to <ip address range>:<port>