Cybersecurity (Security+) and P4 Programmable Switches

Overview Cybersecurity Labs

Ali AlSabeh, Jorge Crichigno
University of South Carolina
http://ce.sc.edu/cyberinfra

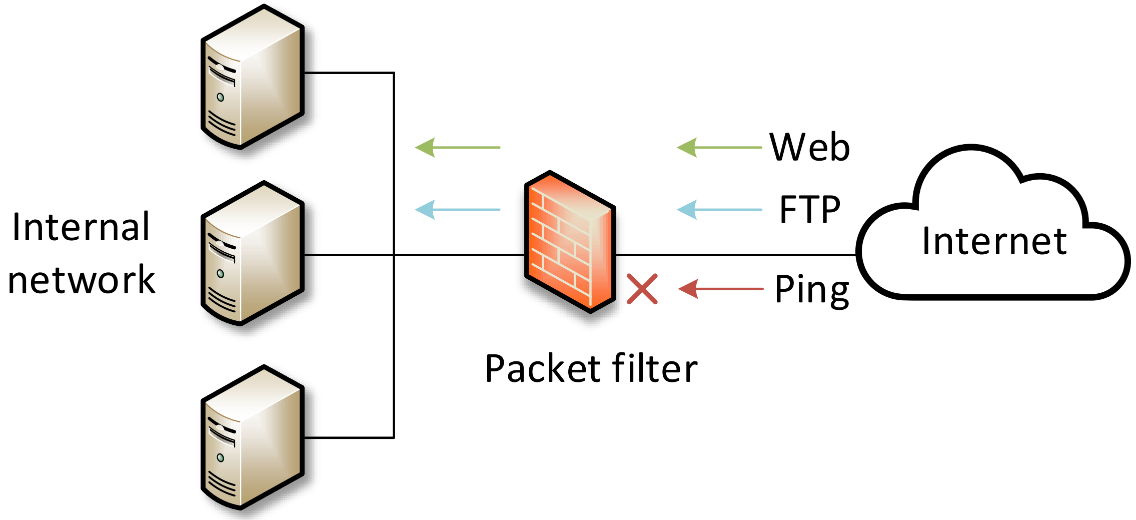
Western Academy Support and Training Center (WASTC)
University of South Carolina (USC)
Energy Sciences Network (ESnet)

June 21st, 2023

Stateful Packet Filters and iptables

Packet Filters

- A packet filter inspects the headers of packets to permit or deny the traffic
- When a packet filter receives a packet, it compares the packet to the preconfigured rule set
  - ➢ At the first matched rule, the packet filter applies the action corresponding to the rule
  - ➢ Typically, an implicit deny is configured if no rule is matched
- Packet filtering firewalls are often deployed at network boundaries
  - ➢ E.g., packet filters may be deployed between a corporate network and the Internet
- Packet filters can also exist as a computer software to protect its network connection



Packet Filters

- Packet filters usually permit or deny network traffic based on the following information:
  - Source and destination IP addresses
  - Protocol, such as TCP, UDP, or ICMP
  - Source and destination ports, ICMP types, and codes
  - Direction (inbound or outbound)
  - Physical interface
- Many rules are often used in conjunction with each other in a set precedence to create an overall policy

Packet Filters

- Rules are listed on the left-hand side of the figure (a)
- The execution logic is displayed on the right-hand side of the figure (b)
- The rules are executed sequentially

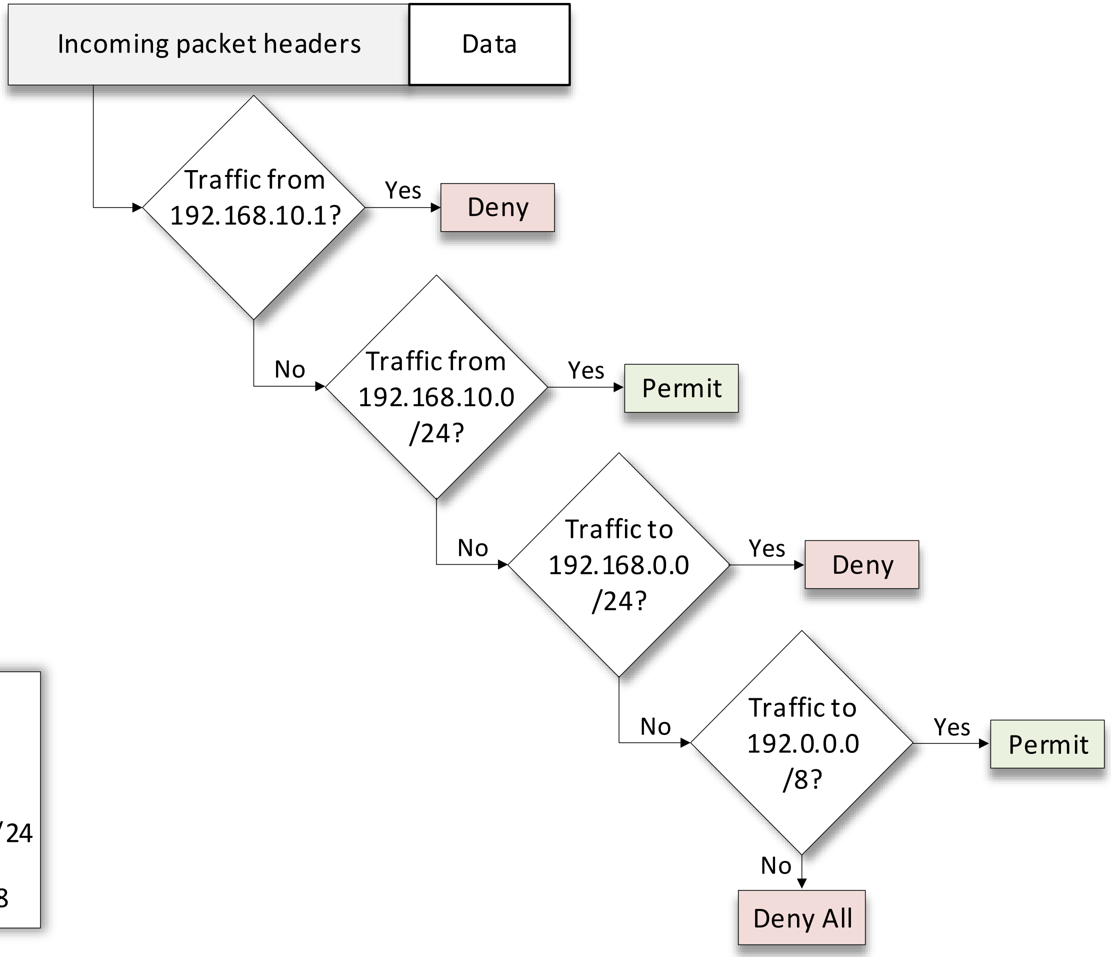
Deny src host 192.168.10.1

Permit src 192.168.10.0/24

Deny destination 192.168.0.0/24

Permit destination 192.0.0.0/8

(a)



(b)

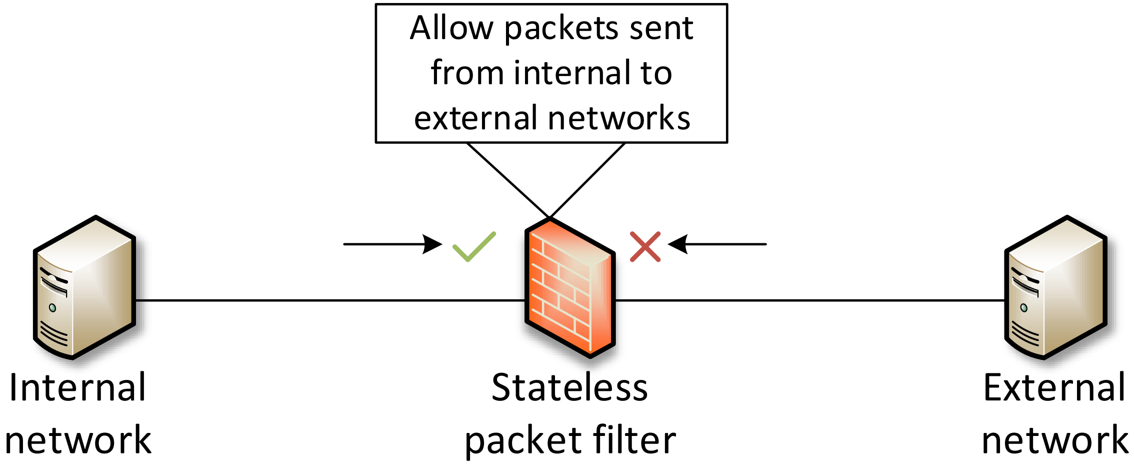
Packet Filters

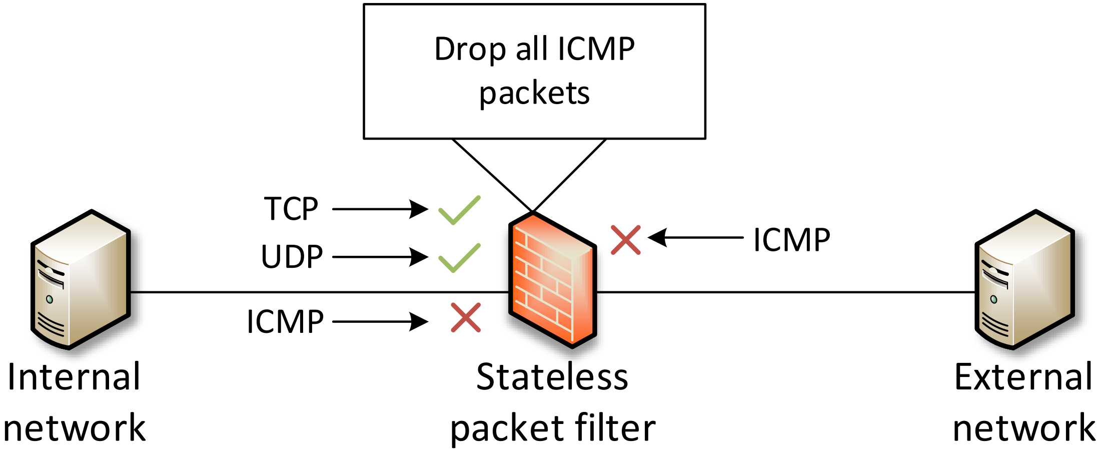
- Traditional packet filtering are limited compared to modern cyber threats
  - Thus, leading to new systems such as Deep Packet Inspection (DPI), next-generation firewalls, etc.
- However, packet filtering remains relevant as simple, low-cost option for implementing security measures
- Types of packet filters mainly include:
  - Stateless packet filter
  - Stateful packet filter

Advantages	Disadvantages
Simple to use	Ineffective against modern attacks
Cost-effective	Can be circumvented
Resource-effective	Cannot make application-based decisions
Fast	Large rules can become hard to maintain

Stateless Packet Filter

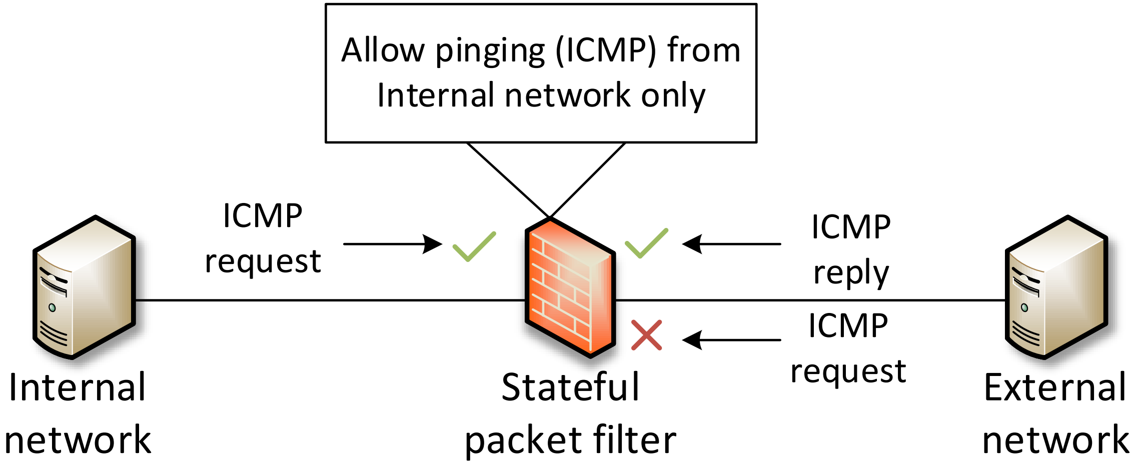
- A stateless packet filter does not save any information about the packet
- It solely takes action based on the header fields of the current packet

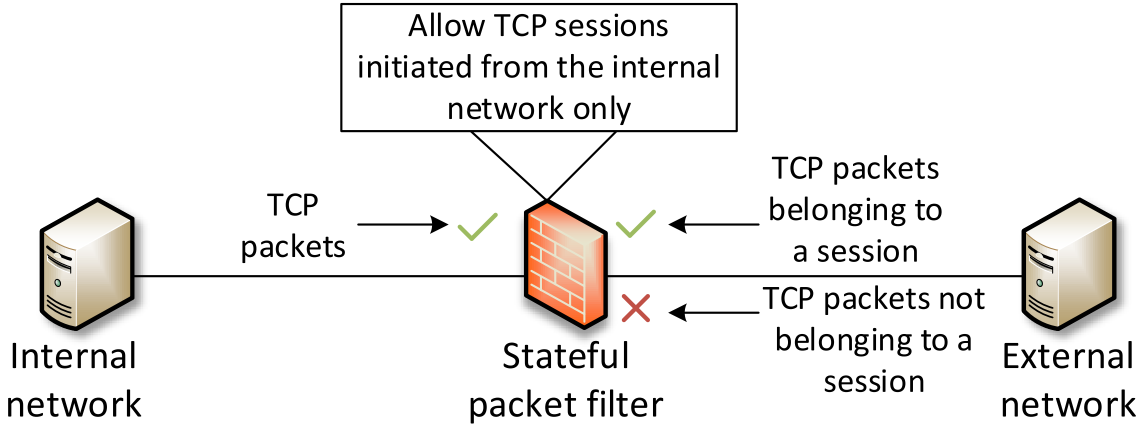




Stateful Packet Filter

- A stateful packet filter can maintain information about connections
  - ➢ i.e., a record of the state of a connection is maintained and tracked
- By maintaining a state, the packet filter can take actions based on the connection




Allow TCP sessions initiated from the internal network only
TCP packets
✓
✓
TCP packets belonging to a session
✗
TCP packets not belonging to a session
Internal network
Stateful packet filter
External network

Differences between Stateless and Stateful Packet Filters

Stateless	Stateful
Protect networks based on static information (source, destination IPs)	Protect networks based on the state and the context of the connection
Less secure	More secure
Cheaper/cost-efficient	More expensive (requires memory)
Less complex	More complex
Faster	Relatively slower
Lower CPU usage	Higher CPU usage
More suitable to individuals and small businesses	More suitable to large enterprises

Packet Filtering in Linux Using iptables

- In Linux, a packet filter can be configured using *iptables*
- *iptables* consists of a collection of tables
  - ➢ *Filter* is the table where all the actions associated with a firewall take place
  - ➢ *NAT* is the table used for Network Address Translation
  - ➢ *Mangle* is used for specialized packet alteration
  - ➢ *Raw* is used for configuration exemptions
- Each table consists of a number of built-in chains and may also contain user-defined chains
  - ➢ E.g., input chain for packets delivered locally, output chain for packets sent from the device
- Each chain may contain a list of rules that can match a set of packets
- Each rule specifies what to do (target) with a packet that matches

Filter iptable

- This is the default table if no other table is selected
- It is used to make decisions about the packet, i.e., whether to accept or deny it
- It contains three built-in chains
  - ➢ Input chain: activated for altering packets delivered locally
  - ➢ Forward chain: activated for altering packets that are routed through the device
  - ➢ Output chain: activated for altering packets sent from the device

NAT iptable

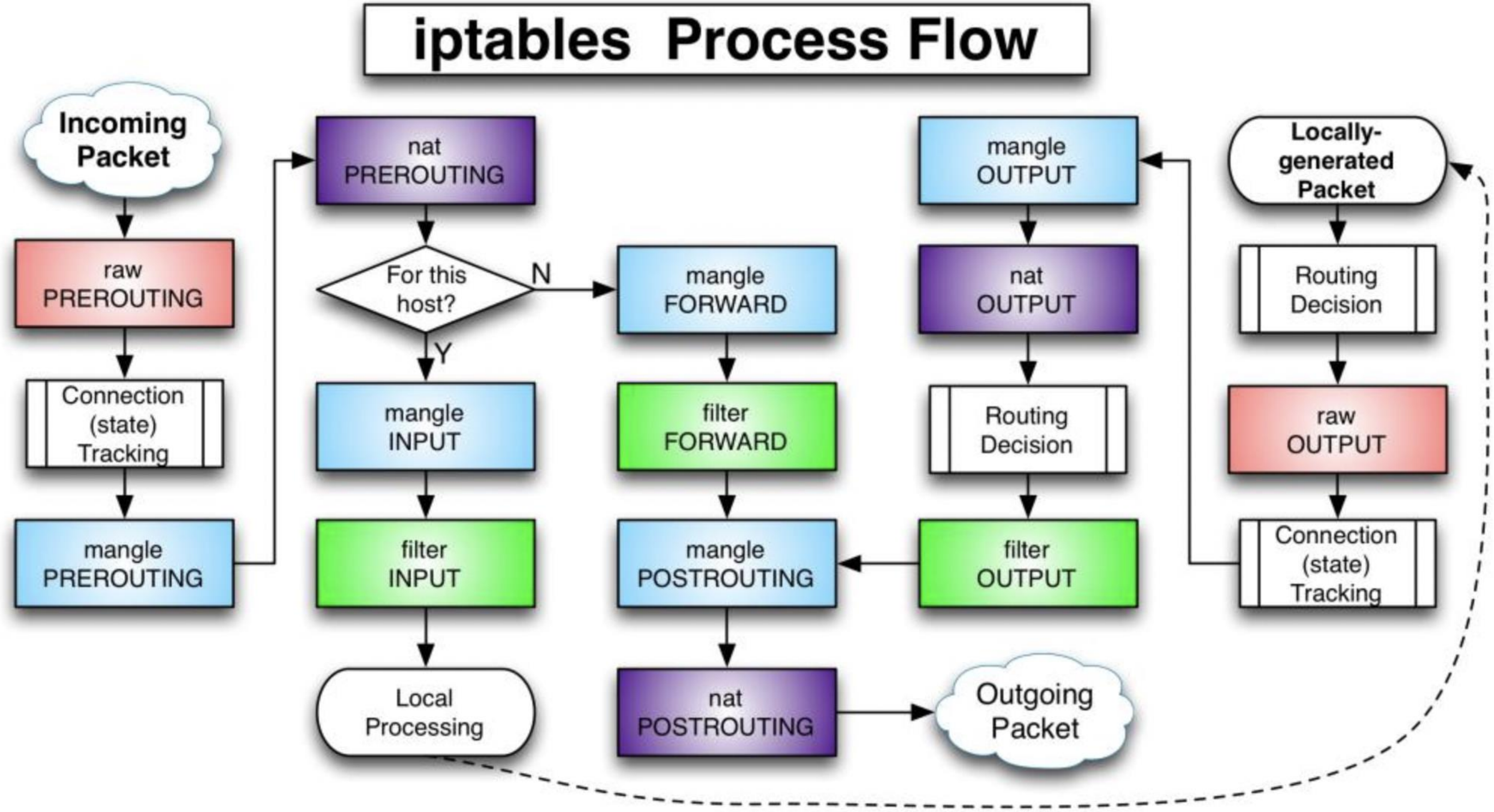
- This table is the used implement Network Address Translation (NAT)
  - As packets the Linux-based router, the rules in the NAT table determine how to modify the packet's source and destination addresses
- It contains three built-in chains
  - Prerouting chain: activated for altering packets as soon as they come in
  - Output chain: activated for altering locally-generated packets before routing
  - Postrouting chain: activated for altering packets as they about to go out

Mangle iptable

- This table is the used for specialized packet alteration
  - ➢ E.g., adjust TCP maximum segment size, modify Time to Live (TTL)
- In recent kernels (2.4.8 and above), it contains five built-in chains
  - ➢ Prerouting chain: activated for altering packets before routing
  - ➢ Input: activated for altering packets delivered locally
  - ➢ Forward: activated for altering packets that are routed through the device
  - ➢ Output chain: activated for altering locally-generated packets before routing
  - ➢ Postrouting chain: activated for packets as they about to go out

Raw iptable

- This table is the used for configuring exemptions
- It has the highest priority, thus, it is called before any other iptables
  - It can mark packets to opt-out of connection tracking
- It contains two built-in chains
  - Prerouting chain: activated for altering packets arriving at any network interface
  - Output chain: activated for altering locally-generated packets before routing



Process flow of iptables. [Figure taken from https://tinyurl.com/697kxhew]

Iptables Rules and Targets

- Rules contain a criteria and a target
- If the criteria is matched, a target is applied
- If the criteria is not matched, it moves on the next rule
- Possible targets include:
  - Accept: accept the packet
  - Drop: drop the packet
  - Queue: pass the packet to the user space
  - Return: stop executing the next rules in the current chain for this packet, and return back to the calling chain