Firewall RAW table

Mikrotik User Meeting London, November 14, 2016

Achmad Mardiansyah
achmad@glcnetworks.com
GLC Networks, Indonesia

Agenda

- Introduction
- Firewall
- Raw table
- Demo
- Q & A

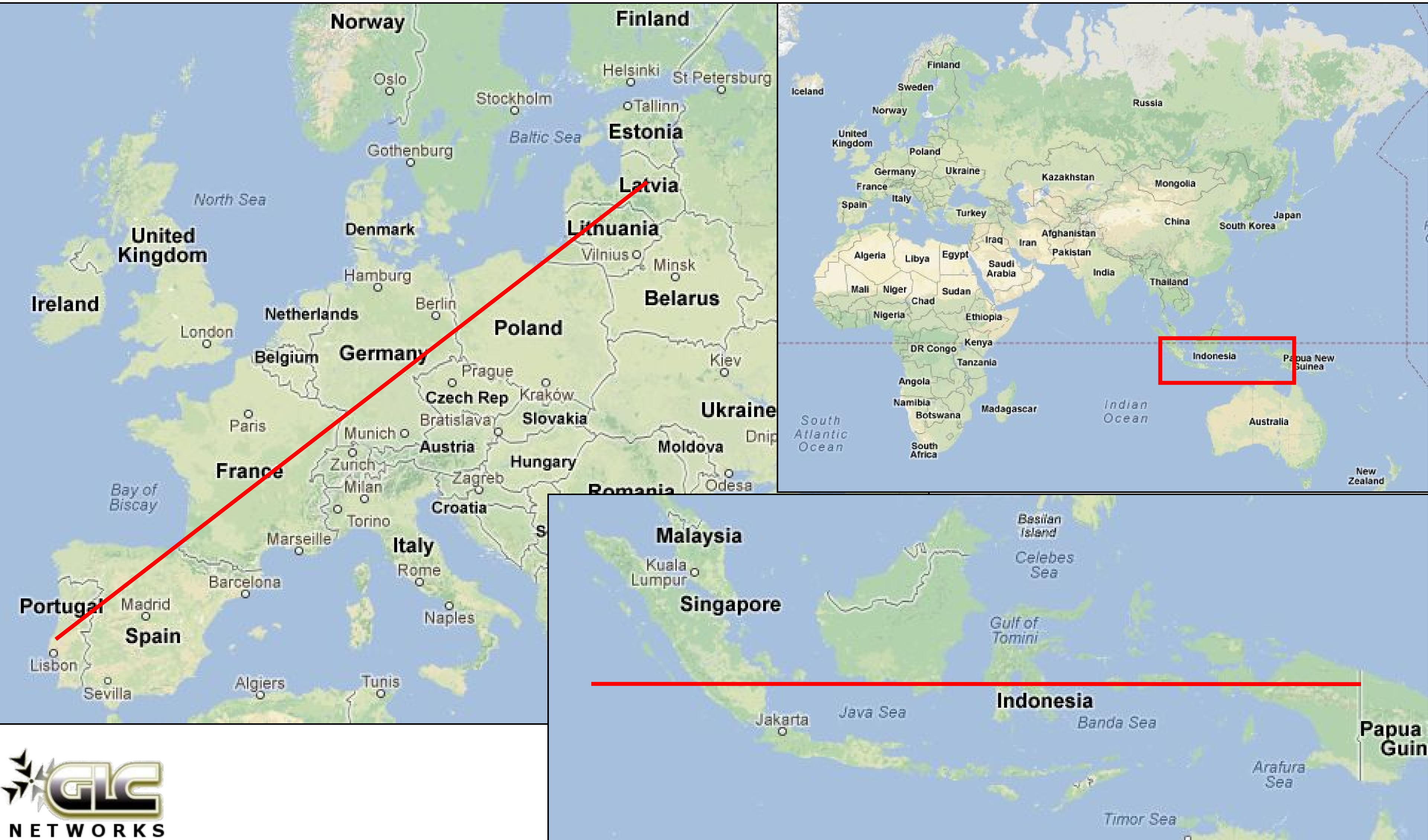
What is GLC?

- Garda Lintas Cakrawala (www.glcnetworks.com)
- Based in Bandung, Indonesia
- Areas: Training, IT Consulting
- Mikrotik Certified Training Partner
- Mikrotik Certified Consultant
- Mikrotik distributor

Trainer Introduction

- Name: Achmad Mardiansyah
- Base: bandung, Indonesia
- Linux user since ’99
- Certified Trainer (MTCNA/RE/WE/UME/INE/TCE)
- Mikrotik Certified Consultant
- Work: Telco engineer, Sysadmin, PHP programmer, and Lecturer at Telkom University
- Personal website: http://achmad.glcnetworks.com
- More info: http://au.linkedin.com/in/achmadmardiansyah

Where is Indonesia?



GLC NETWORKS

About Telkom University

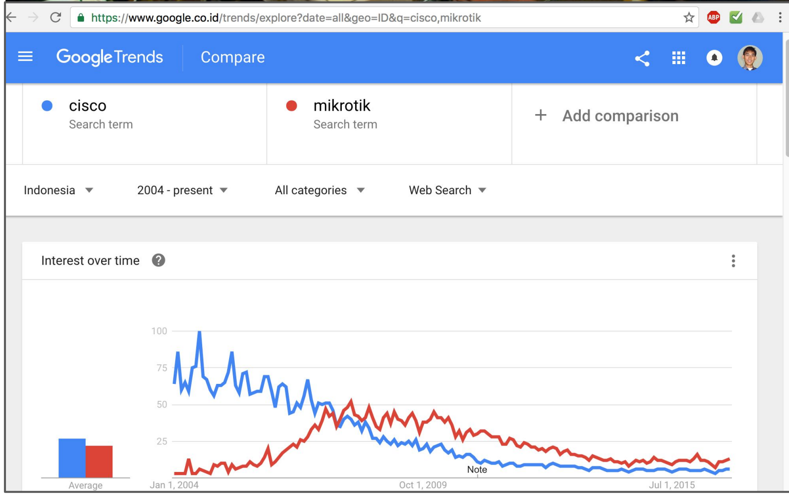
- Located in Bandung, Indonesia
- 7 Faculties, 27 schools
- Areas: Engineering, Communications, Computing, Bussiness and management, Arts
- 650+ Academic staff, 400+ Administration staff, 20000+ students
- An exchange program
- Runs mikrotik academy program

Mikrotik academy @ TEL-U

- Started in 2013
- Embedded into schools curricula
- 100% hands-on
- Get MTCNA certification

Mikrotik in Indonesia

- Very popular product for networking
- Early adoption (beginning of 2000)
- Many schools already join Mikrotik Academy programs
- Lots of training classes
- Biggest MUM in the world (2500+ participants, 2-day event)
- Very active community (facebook, telegram, forum, etc)
- What..? you dont know Mikrotik? Where have you been?



https://www.google.co.id/trends/explore?date=all&geo=ID&q=cisco,mikrotik

Google Trends Compare

● cisco
Search term

● mikrotik
Search term

+ Add comparison

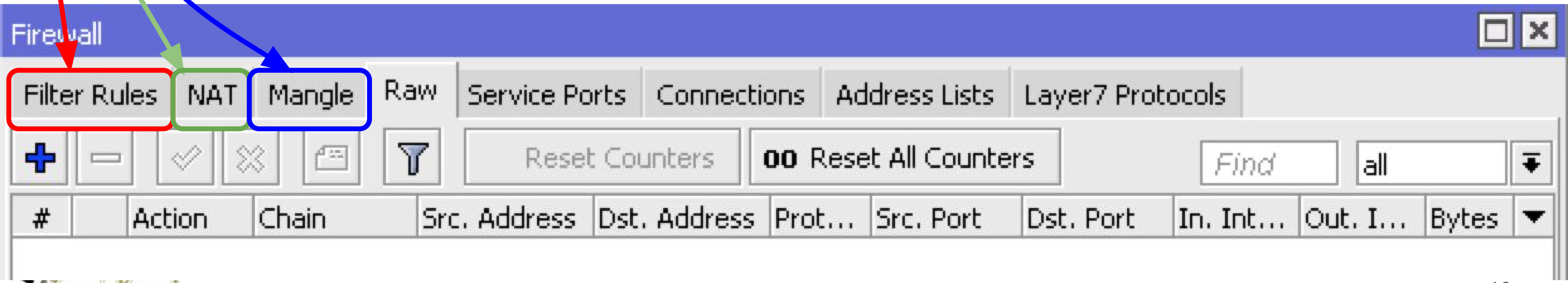
Indonesia ▾ 2004 - present ▾ All categories ▾ Web Search ▾

Interest over time

Firewall

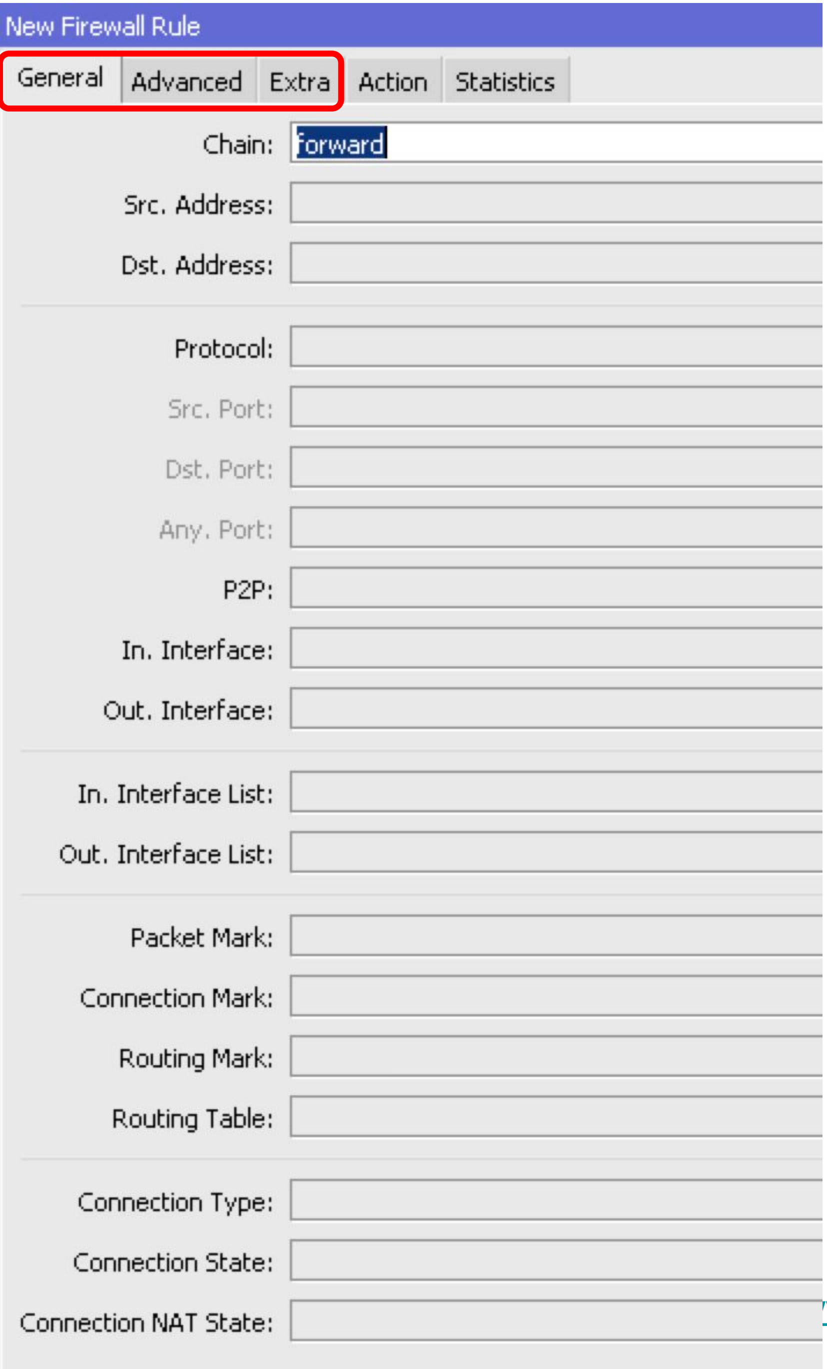
What is Mikrotik firewall?

- Is a feature to
  - Control network access (filter)
  - Modify network header (NAT)
  - Marking packet for further processing (mangle)
- Developed from linux
- Consist of 2 parts: matcher & action
- Executed sequentially
- Netadmin must understand the application’s characteristics in order to build a matcher (e.g. browsing -> using TCP port 80)



How firewall works?

- Setup matcher -> then action
- Mikrotik has lots of options for matcher -> very flexible
- Matcher + Action = Firewall rule
- Rule is executed sequentially



Chain: forward

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

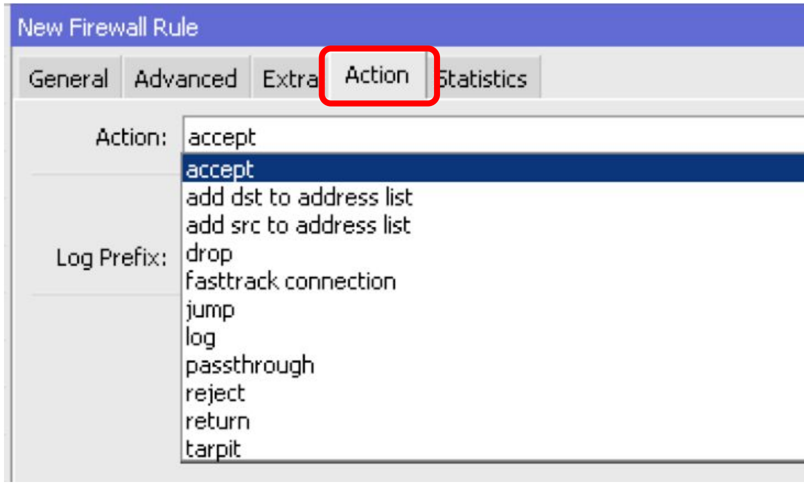
Routing Mark:

Routing Table:

Connection Type:

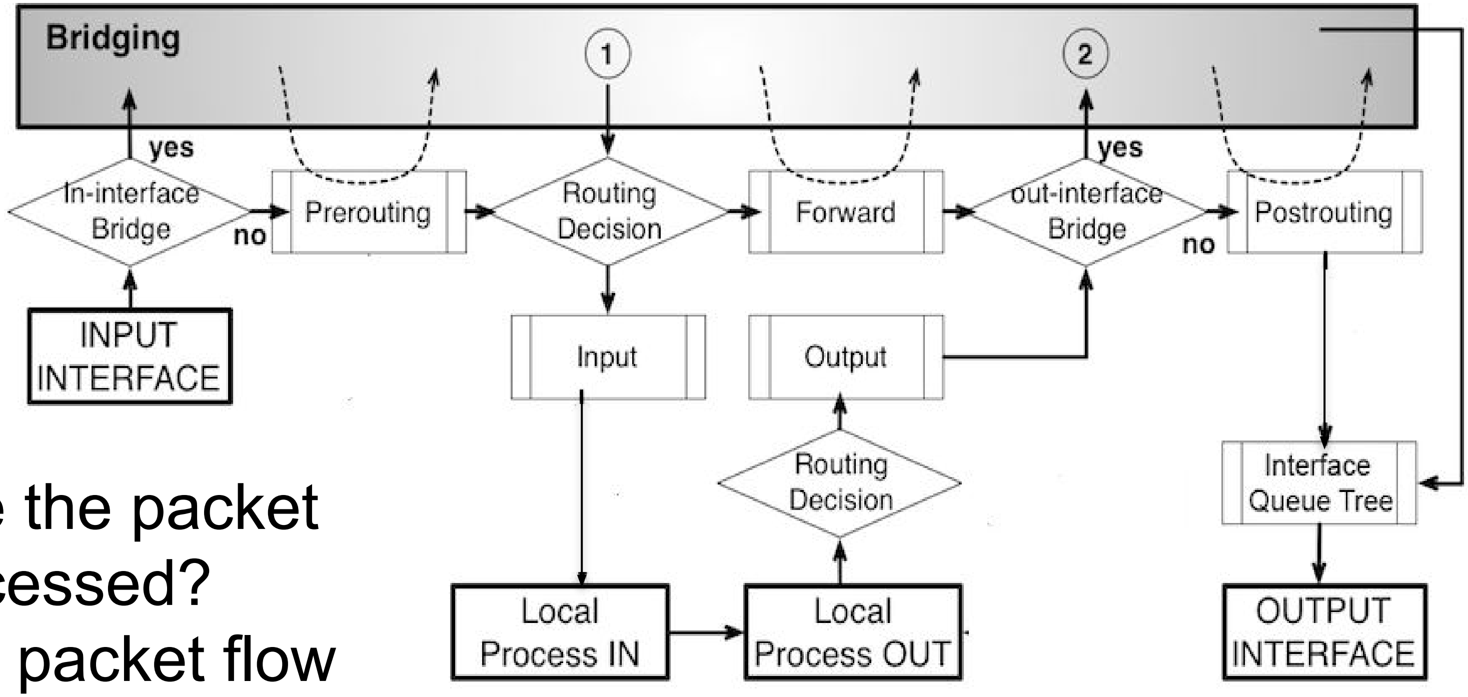
Connection State:

Connection NAT State:



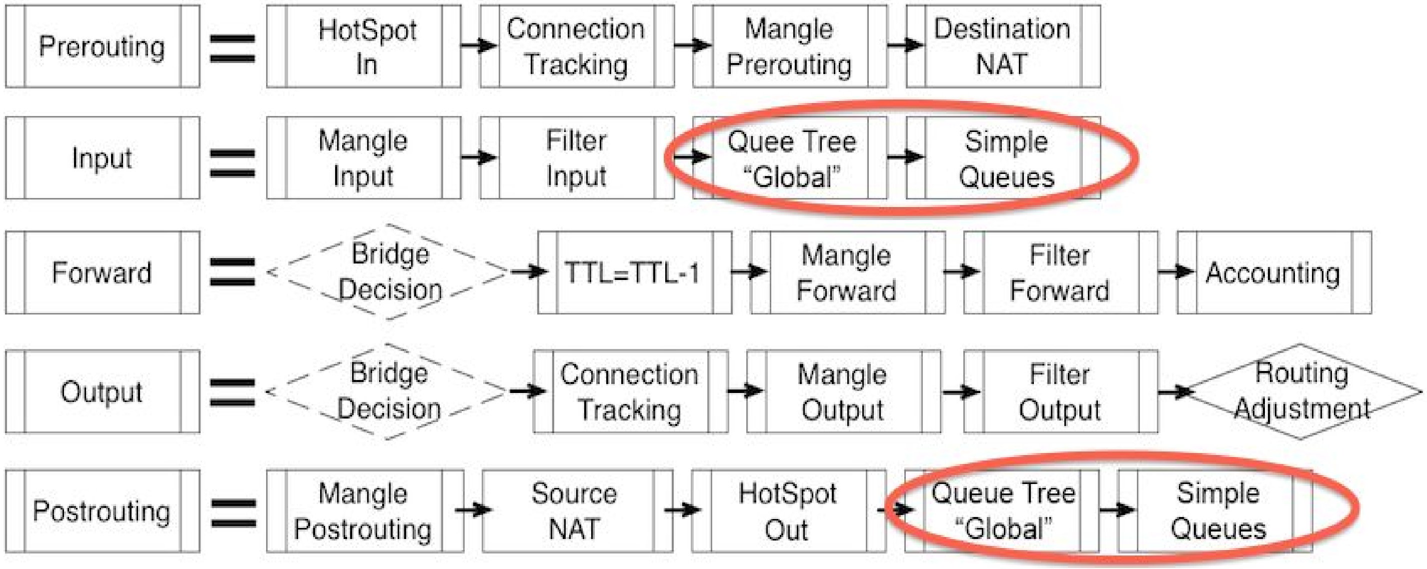
Action: accept

Log Prefix:



Where the packet is processed?
A: see packet flow

Note: ipsec is removed in this diagram



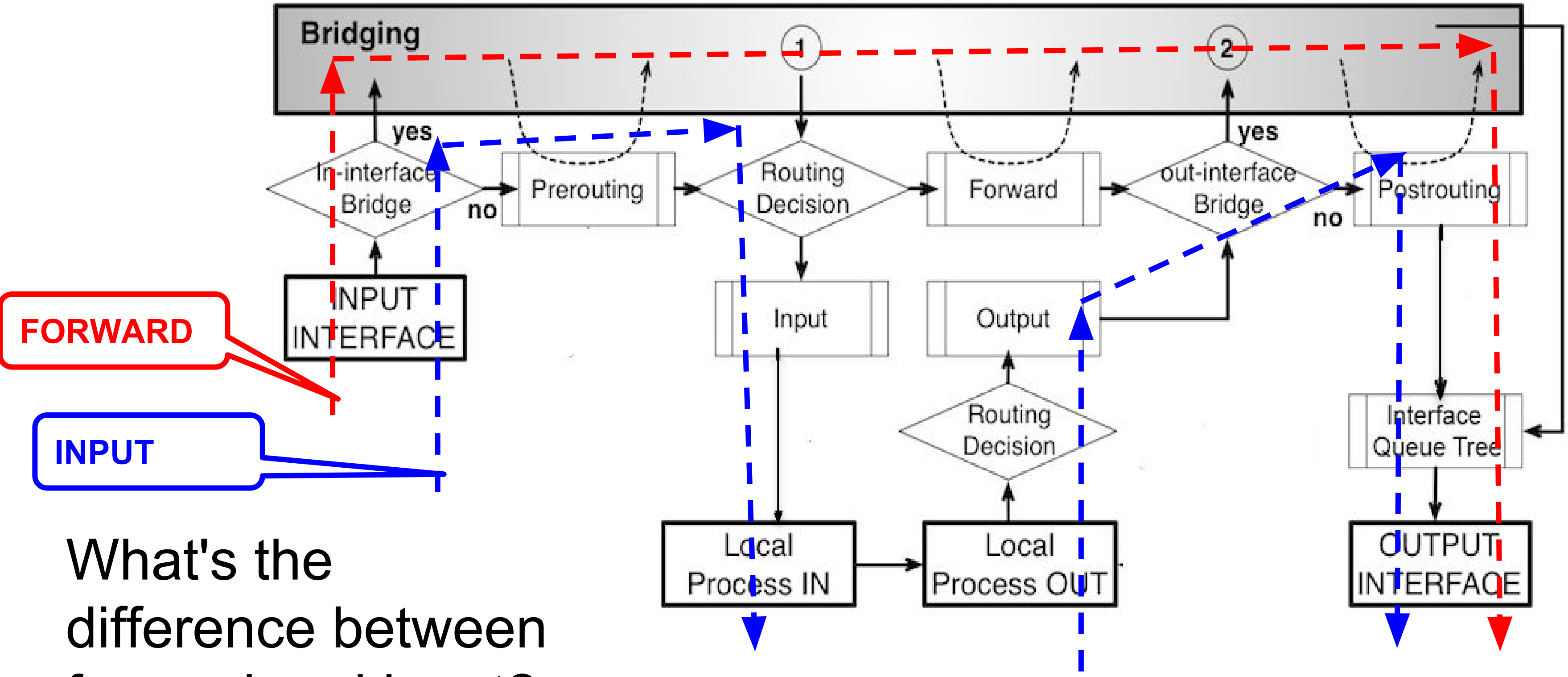
Prerouting = HotSpot In → Connection Tracking → Mangle Prerouting → Destination NAT

Input = Mangle Input → Filter Input → Quee Tree “Global” → Simple Queues

Forward = Bridge Decision → TTL=TTL-1 → Mangle Forward → Filter Forward → Accounting

Output = Bridge Decision → Connection Tracking → Mangle Output → Filter Output → Routing Adjustment

Postrouting = Mangle Postrouting → Source NAT → HotSpot Out → Queue Tree “Global” → Simple Queues



Bridging

1

2

yes

In-interface Bridge

no

Prerouting

Routing Decision

Forward

out-interface Bridge

yes

no

Postrouting

INPUT INTERFACE

Input

Output

Routing Decision

Interface Queue Tree

Local Process IN

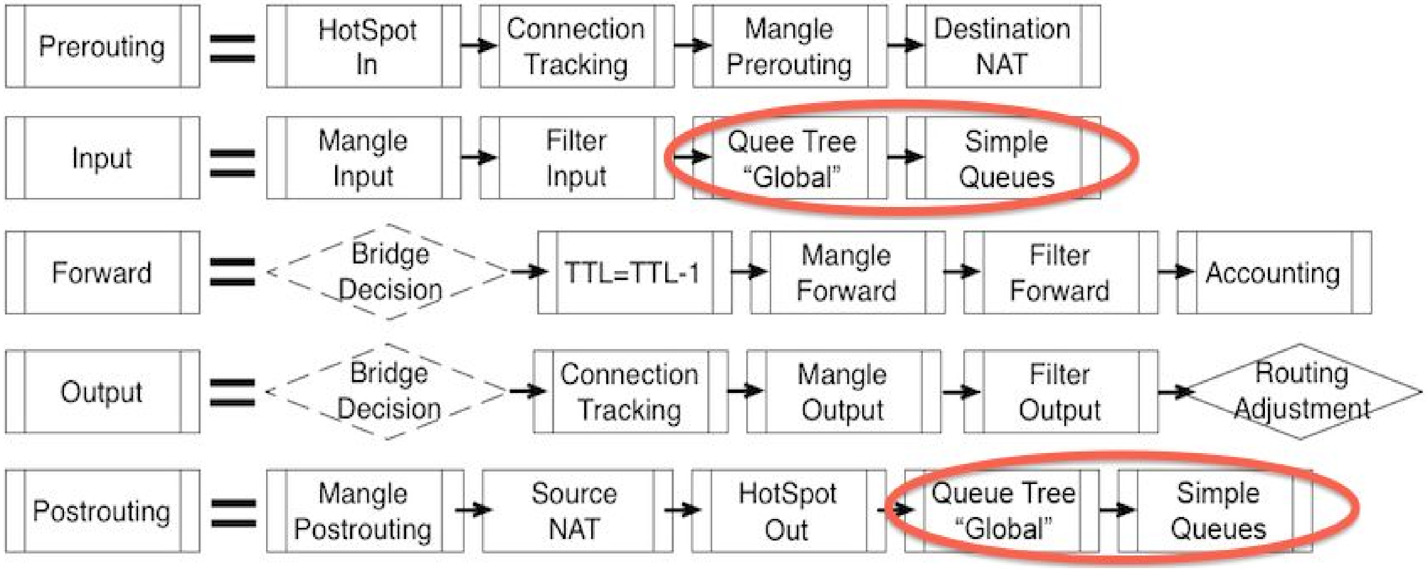
Local Process OUT

OUTPUT INTERFACE

FORWARD

INPUT

What's the difference between forward and input?



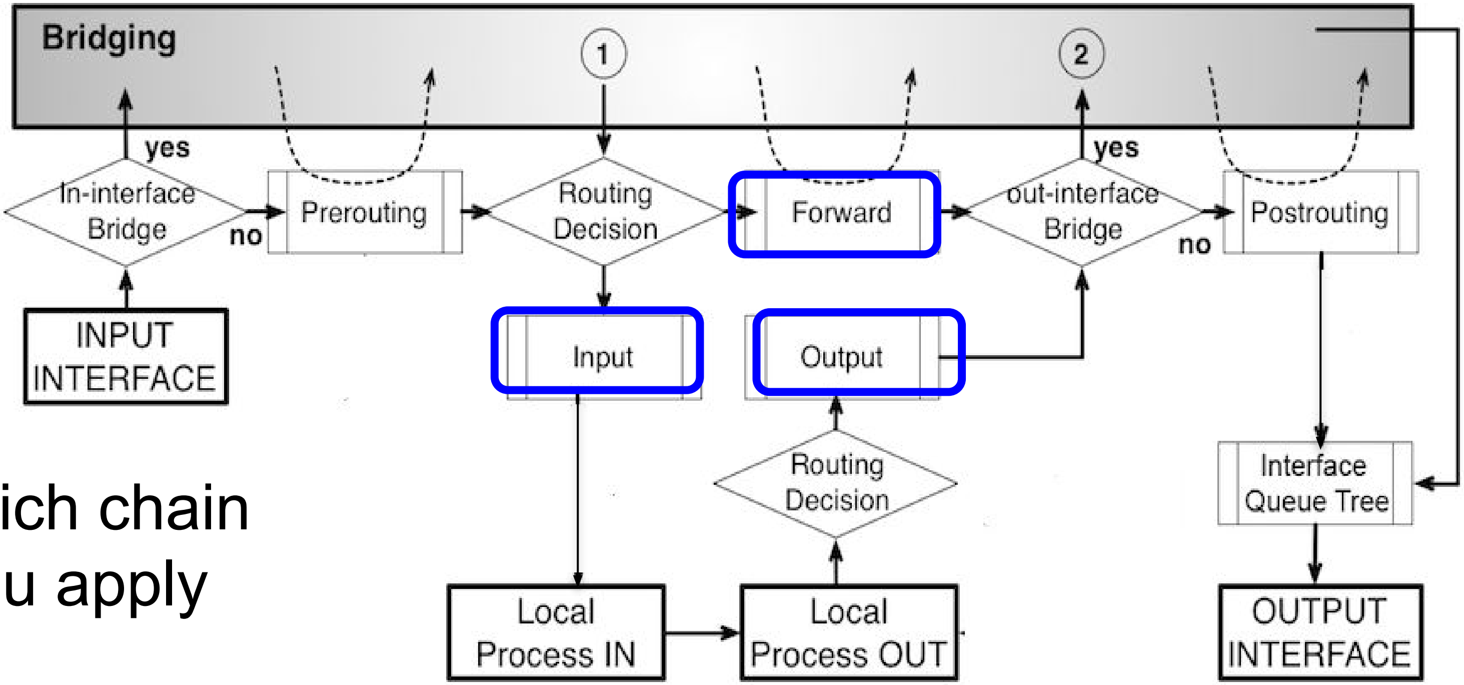
Prerouting = HotSpot In → Connection Tracking → Mangle Prerouting → Destination NAT

Input = Mangle Input → Filter Input → Quee Tree "Global" → Simple Queues

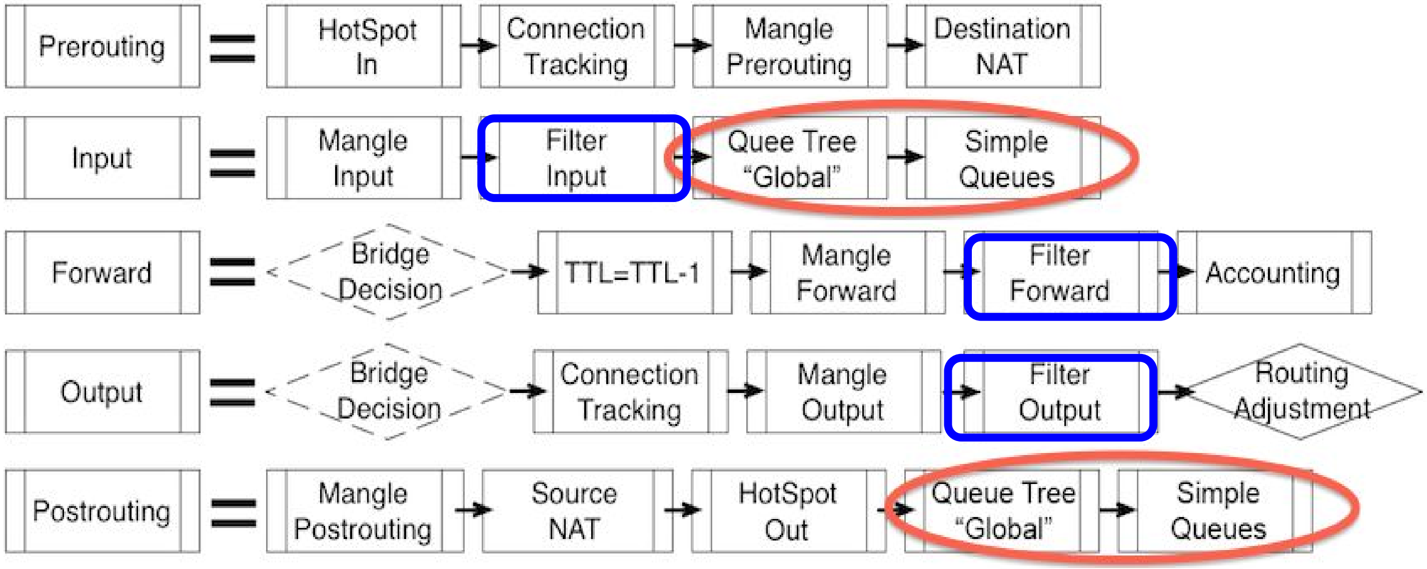
Forward = Bridge Decision → TTL=TTL-1 → Mangle Forward → Filter Forward → Accounting

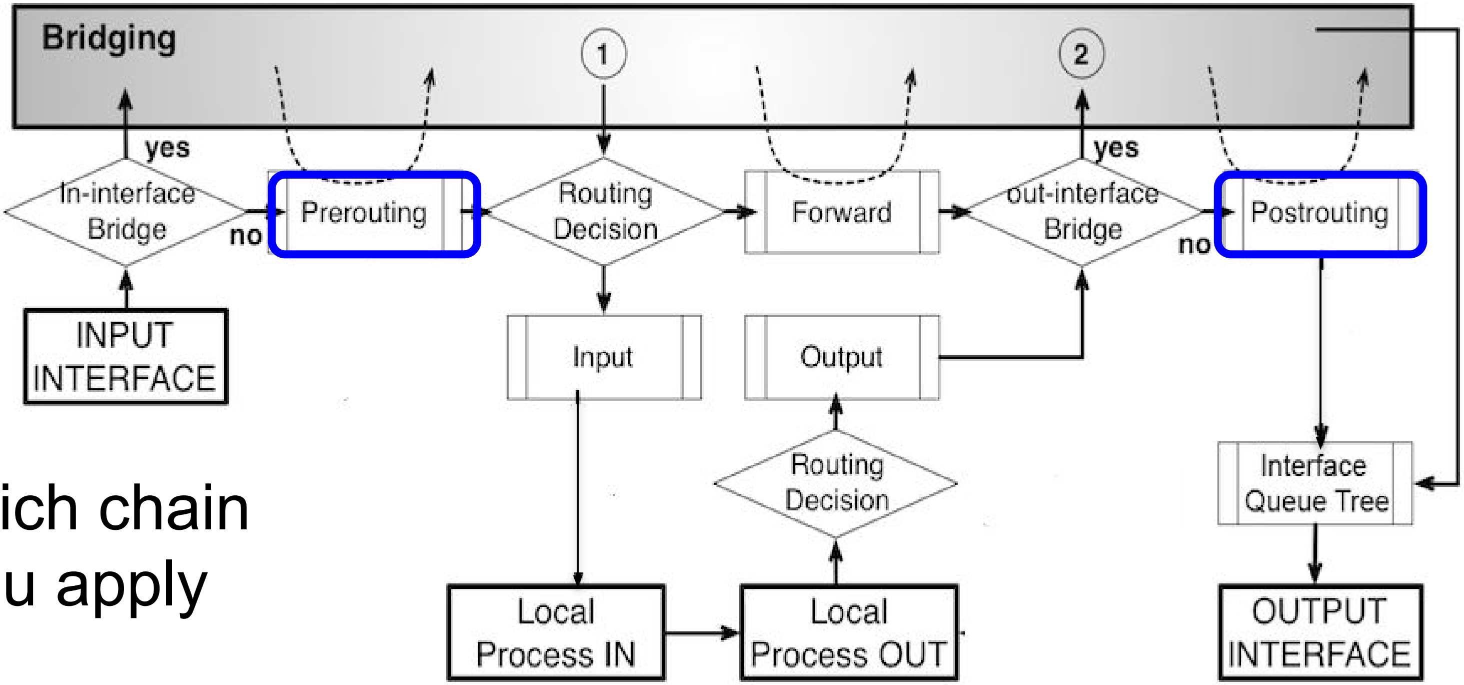
Output = Bridge Decision → Connection Tracking → Mangle Output → Filter Output → Routing Adjustment

Postrouting = Mangle Postrouting → Source NAT → HotSpot Out → Queue Tree "Global" → Simple Queues

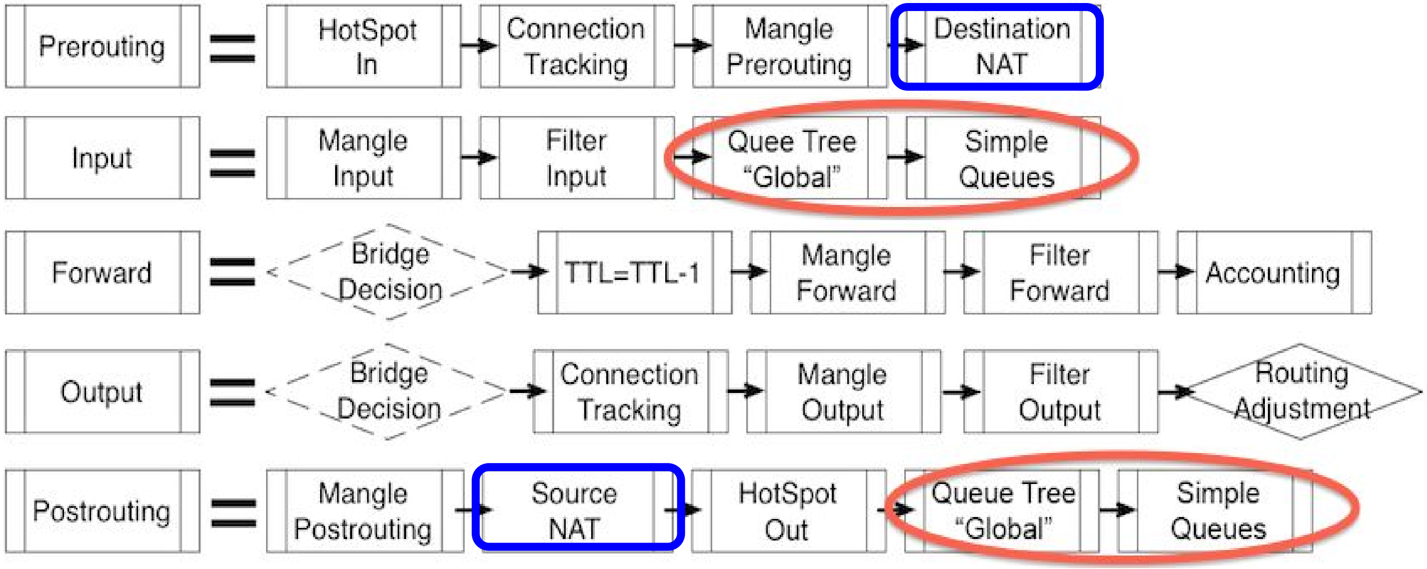


On which chain can you apply filter?


Prerouting = HotSpot In → Connection Tracking → Mangle Prerouting → Destination NAT
Input = Mangle Input → Filter Input → Quee Tree "Global" → Simple Queues
Forward = Bridge Decision → TTL=TTL-1 → Mangle Forward → Filter Forward → Accounting
Output = Bridge Decision → Connection Tracking → Mangle Output → Filter Output → Routing Adjustment
Postrouting = Mangle Postrouting → Source NAT → HotSpot Out → Queue Tree "Global" → Simple Queues



On which chain can you apply NAT?



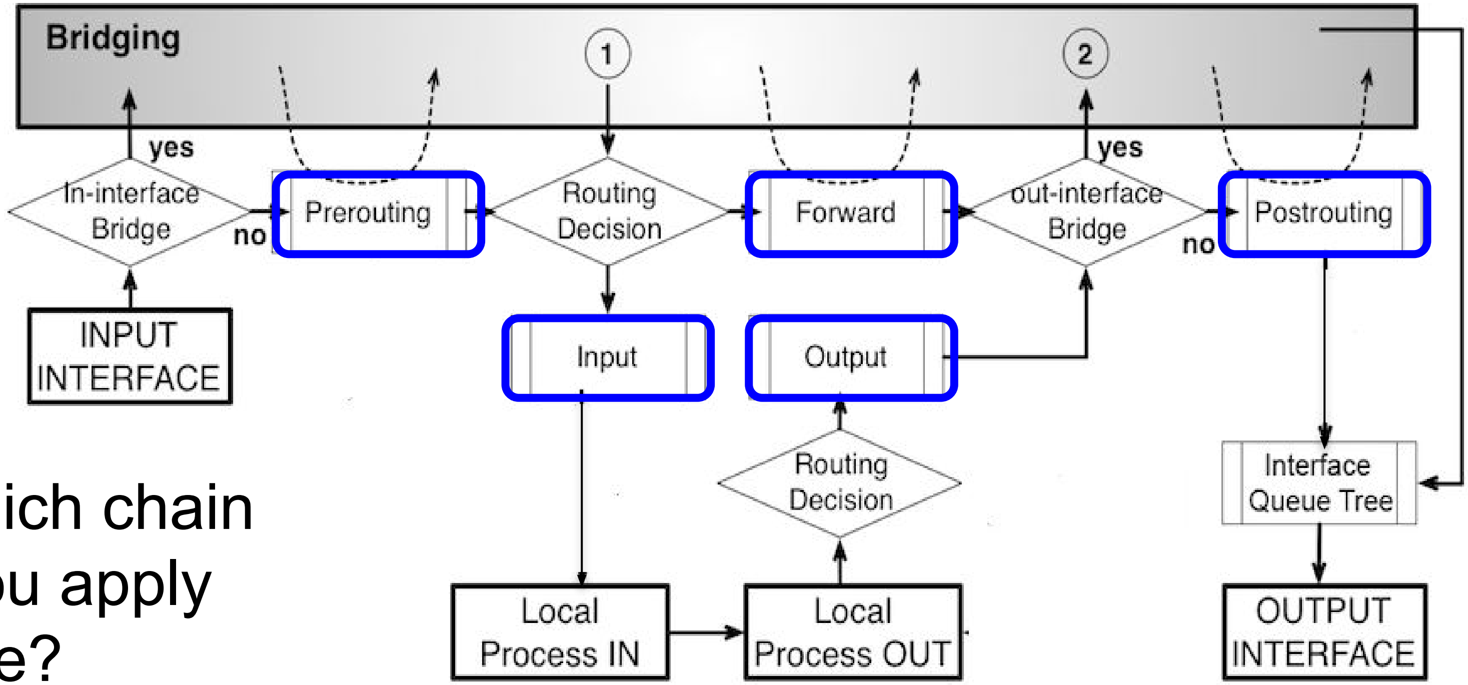
Prerouting = HotSpot In → Connection Tracking → Mangle Prerouting → Destination NAT

Input = Mangle Input → Filter Input → Quee Tree “Global” → Simple Queues

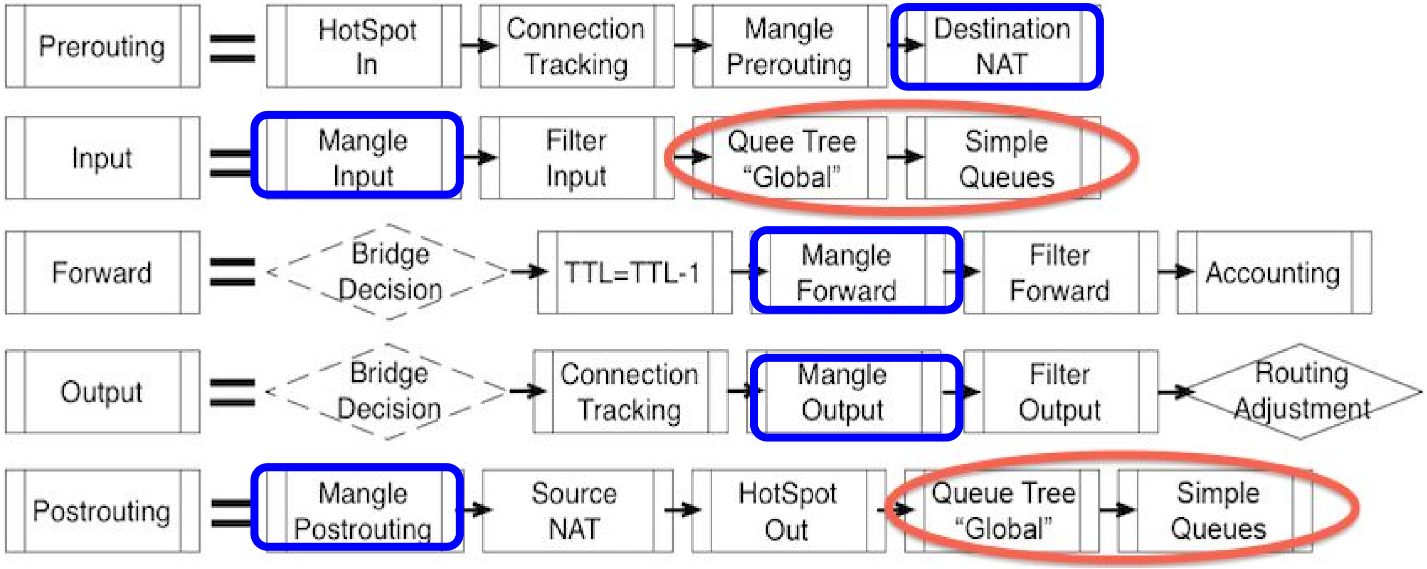
Forward = Bridge Decision → TTL=TTL-1 → Mangle Forward → Filter Forward → Accounting

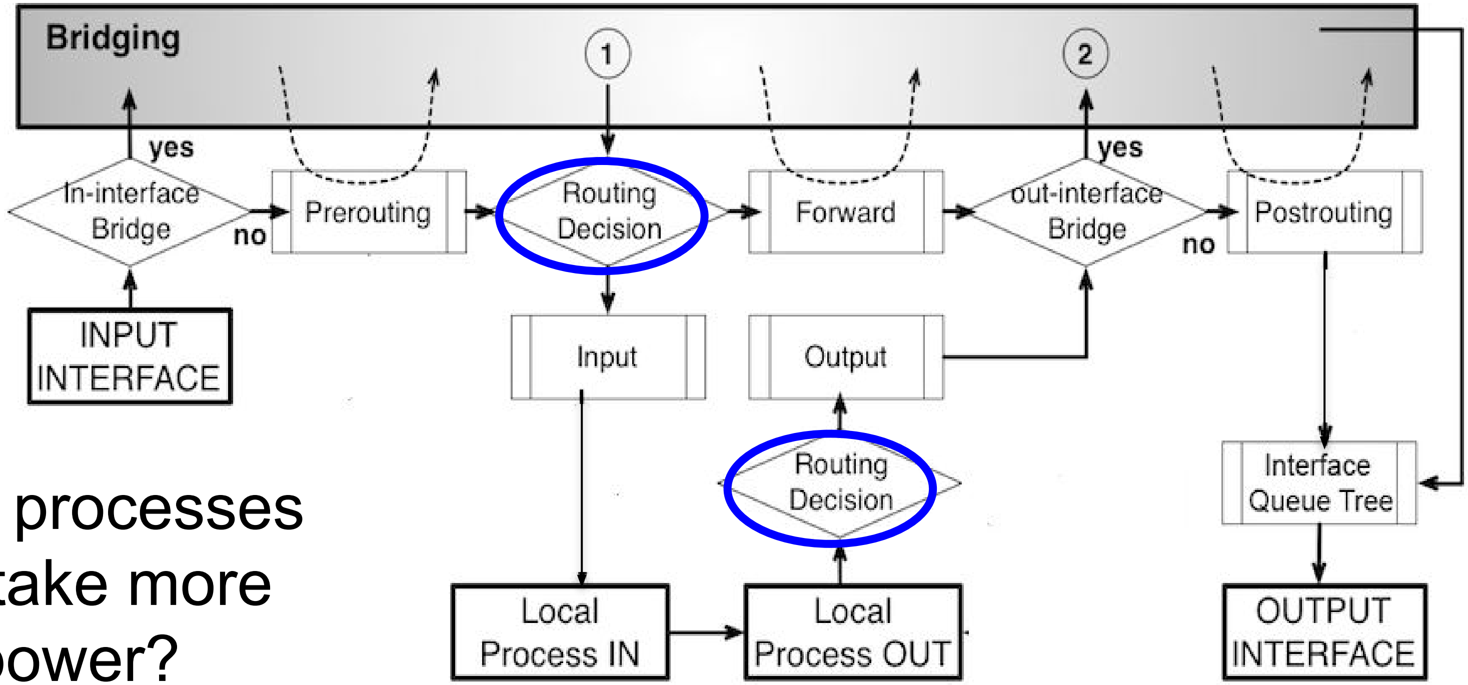
Output = Bridge Decision → Connection Tracking → Mangle Output → Filter Output → Routing Adjustment

Postrouting = Mangle Postrouting → Source NAT → HotSpot Out → Queue Tree “Global” → Simple Queues

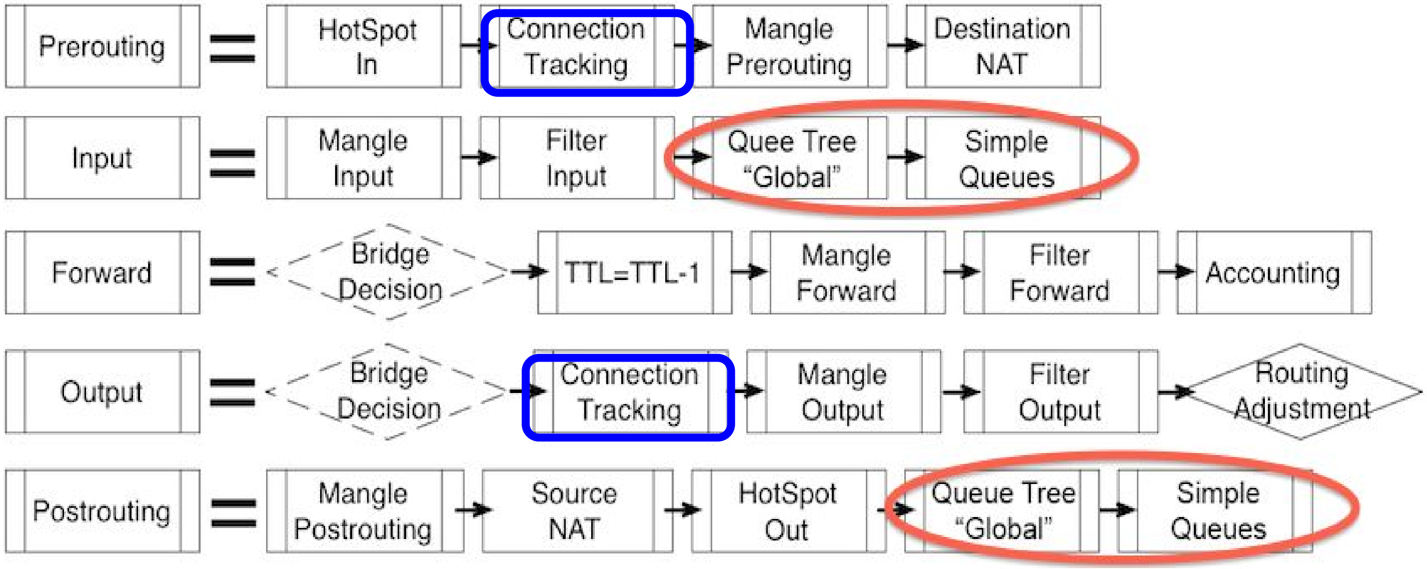


On which chain can you apply mangle?


Prerouting = HotSpot In → Connection Tracking → Mangle Prerouting → Destination NAT
Input = Mangle Input → Filter Input → Quee Tree "Global" → Simple Queues
Forward = Bridge Decision → TTL=TTL-1 → Mangle Forward → Filter Forward → Accounting
Output = Bridge Decision → Connection Tracking → Mangle Output → Filter Output → Routing Adjustment
Postrouting = Mangle Postrouting → Source NAT → HotSpot Out → Queue Tree "Global" → Simple Queues



Which processes could take more CPU power?



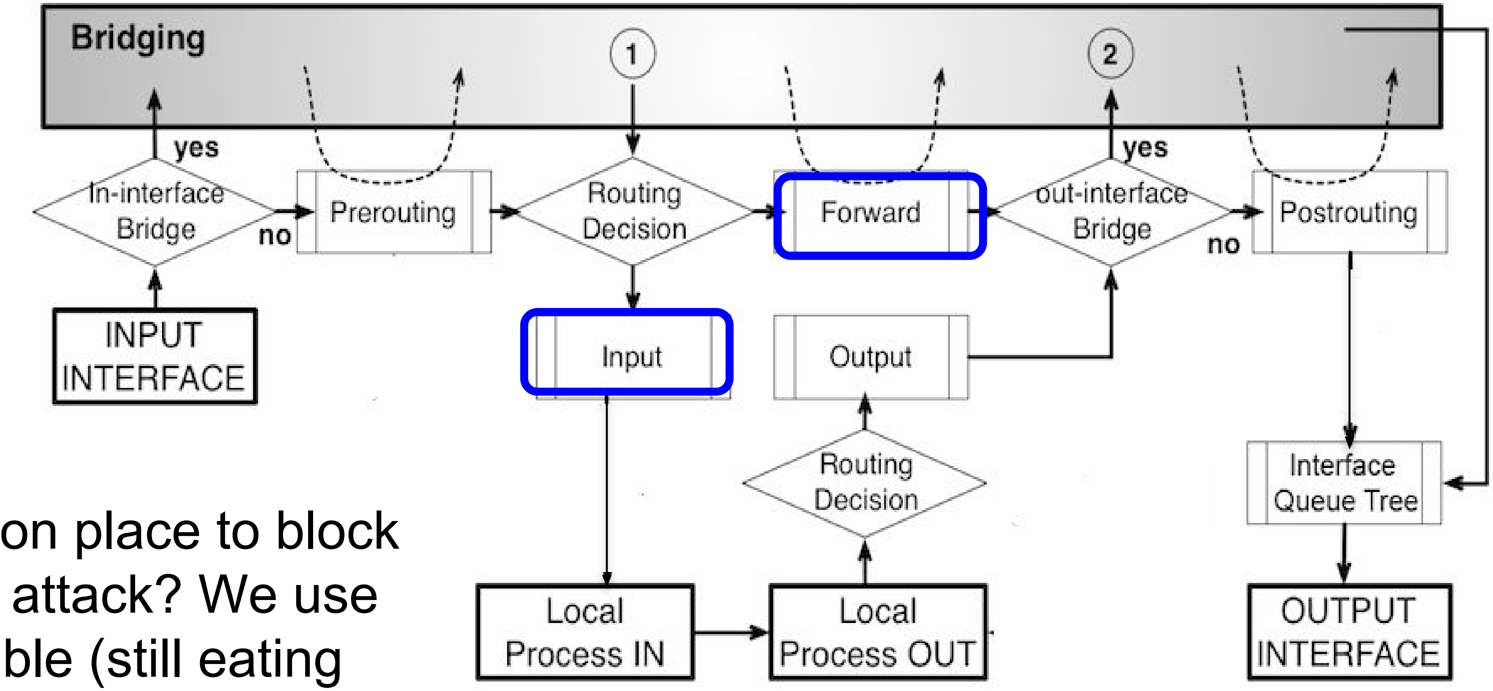
Prerouting = HotSpot In → Connection Tracking → Mangle Prerouting → Destination NAT

Input = Mangle Input → Filter Input → Quee Tree "Global" → Simple Queues

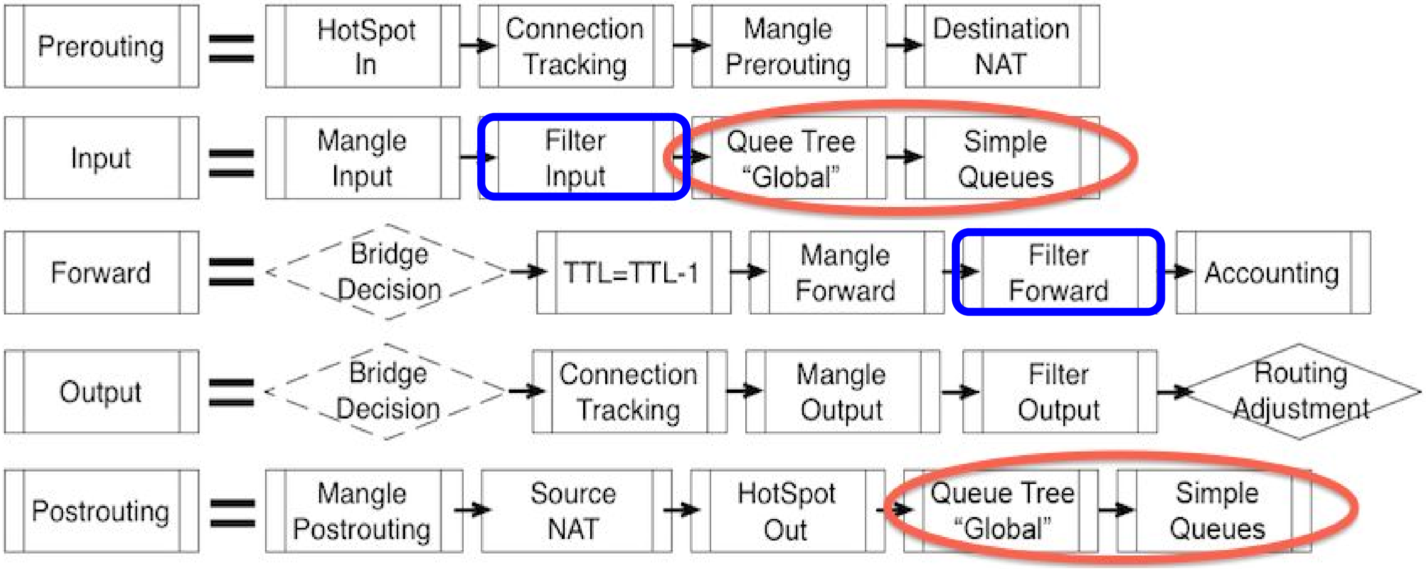
Forward = Bridge Decision → TTL=TTL-1 → Mangle Forward → Filter Forward → Accounting

Output = Bridge Decision → Connection Tracking → Mangle Output → Filter Output → Routing Adjustment

Postrouting = Mangle Postrouting → Source NAT → HotSpot Out → Queue Tree "Global" → Simple Queues



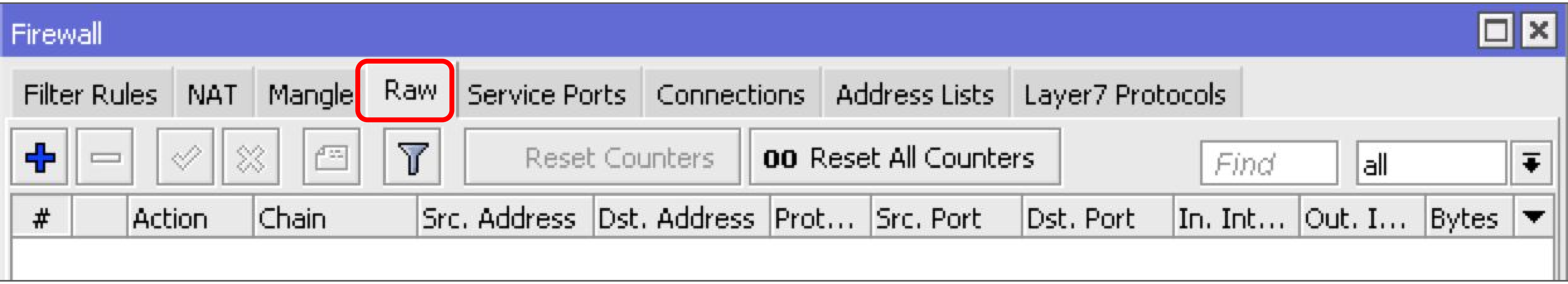
Common place to block DDOS attack? We use filter table (still eating CPU power)


Prerouting = HotSpot In → Connection Tracking → Mangle Prerouting → Destination NAT
Input = Mangle Input → Filter Input → Quee Tree "Global" → Simple Queues
Forward = Bridge Decision → TTL=TTL-1 → Mangle Forward → Filter Forward → Accounting
Output = Bridge Decision → Connection Tracking → Mangle Output → Filter Output → Routing Adjustment
Postrouting = Mangle Postrouting → Source NAT → HotSpot Out → Queue Tree "Global" → Simple Queues

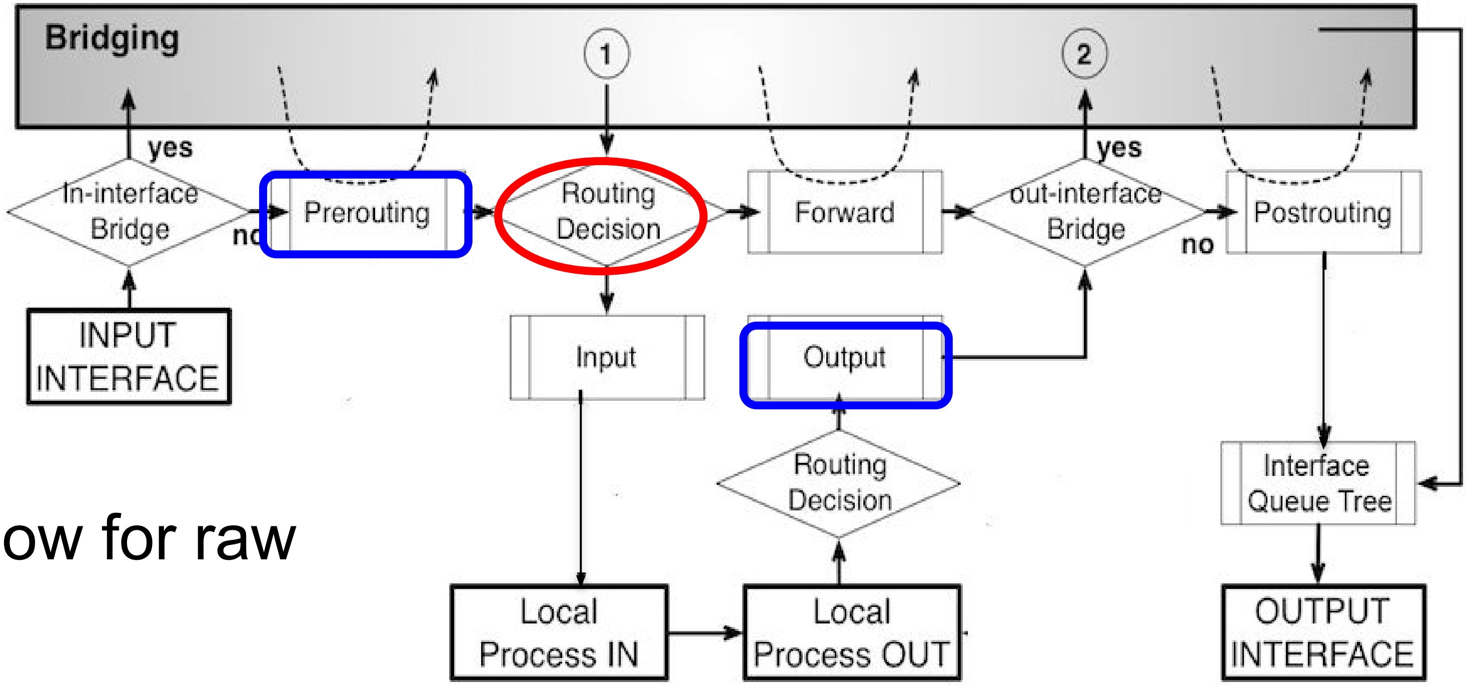
Raw table

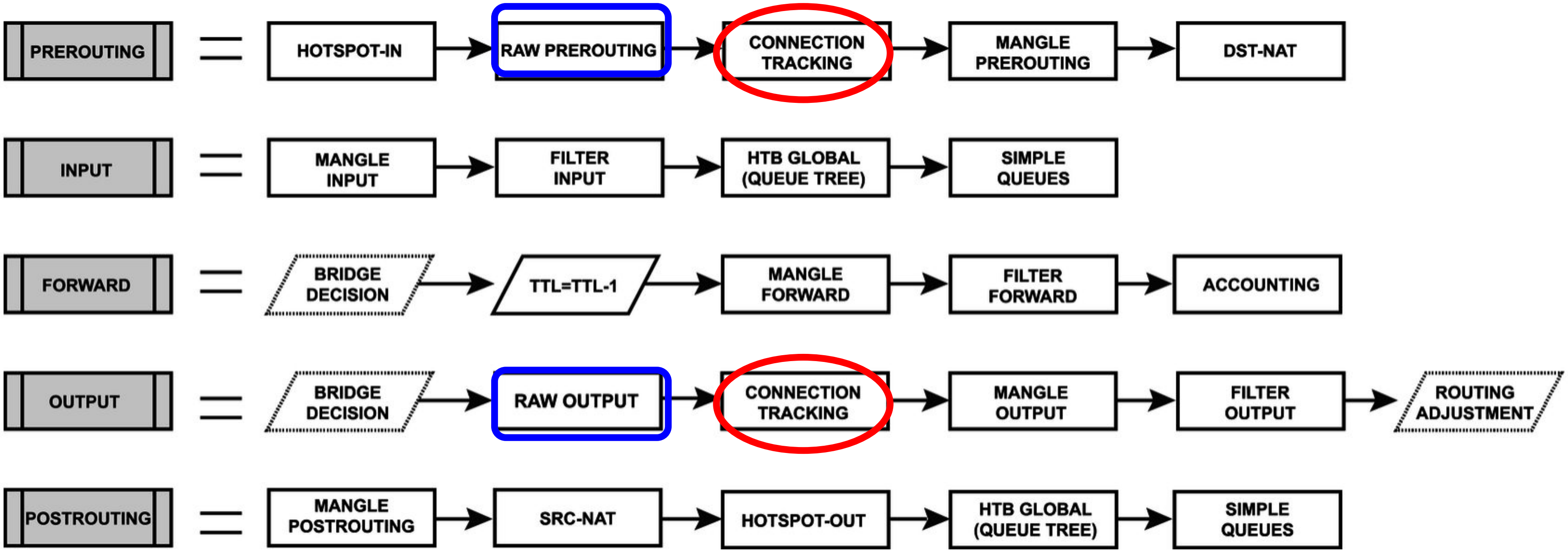
Raw table

- allows to selectively bypass or drop packets before connection tracking
- does not have matchers that depend on connection tracking (like connection-state, layer7 etc.)
- If packet is marked to bypass connection tracking, packet de-fragmentation will not occur



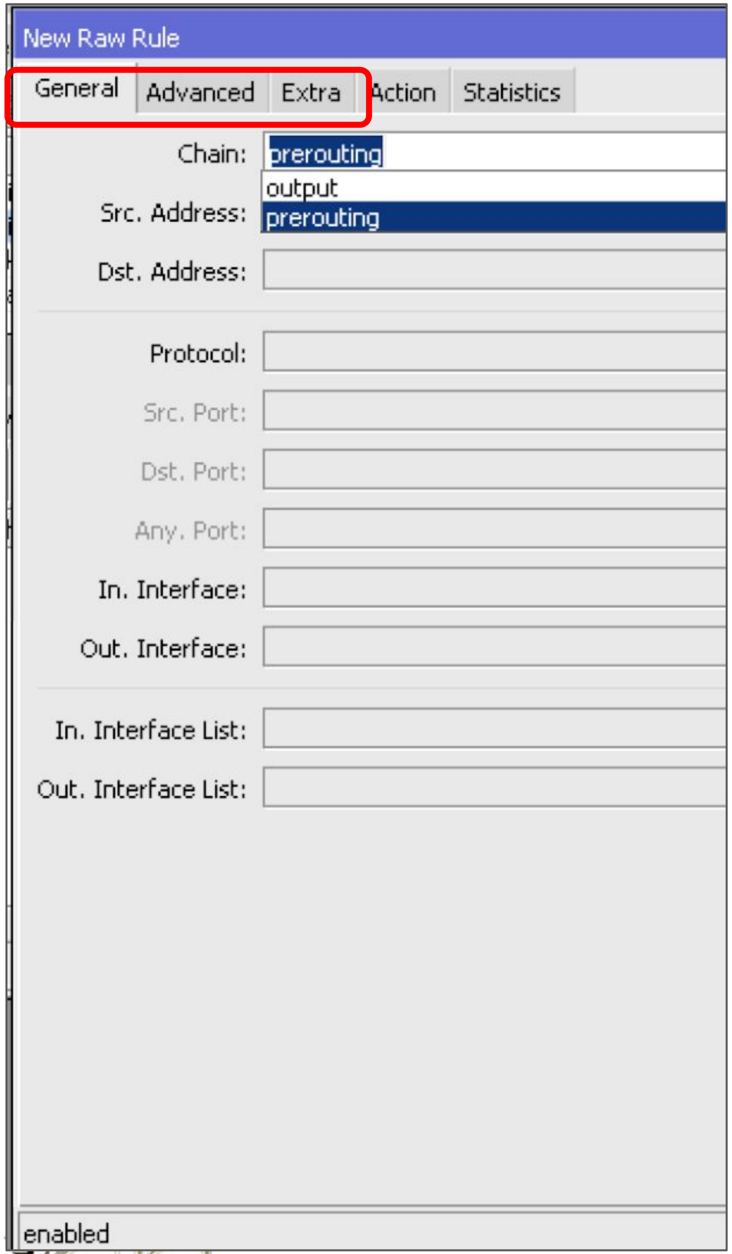
Packet flow for raw table




PREROUTING = HOTSPOT-IN → RAW PREROUTING → CONNECTION TRACKING → MANGLE PREROUTING → DST-NAT
INPUT = MANGLE INPUT → FILTER INPUT → HTB GLOBAL (QUEUE TREE) → SIMPLE QUEUES
FORWARD = BRIDGE DECISION → TTL=TTL-1 → MANGLE FORWARD → FILTER FORWARD → ACCOUNTING
OUTPUT = BRIDGE DECISION → RAW OUTPUT → CONNECTION TRACKING → MANGLE OUTPUT → FILTER OUTPUT → ROUTING ADJUSTMENT
POSTROUTING = MANGLE POSTROUTING → SRC-NAT → HOTSPOT-OUT → HTB GLOBAL (QUEUE TREE) → SIMPLE QUEUES

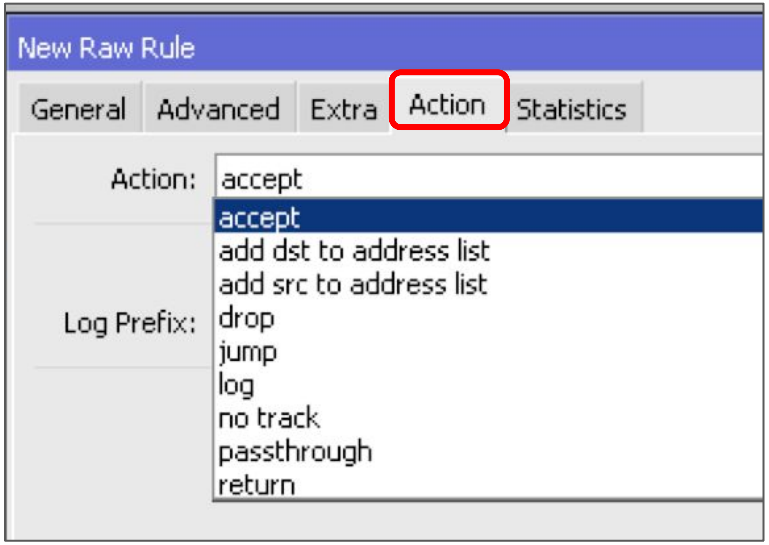
Raw table matchers and action

- No paramaters related to connection tracking (l7-filter, conn-mark, bytes, etc)



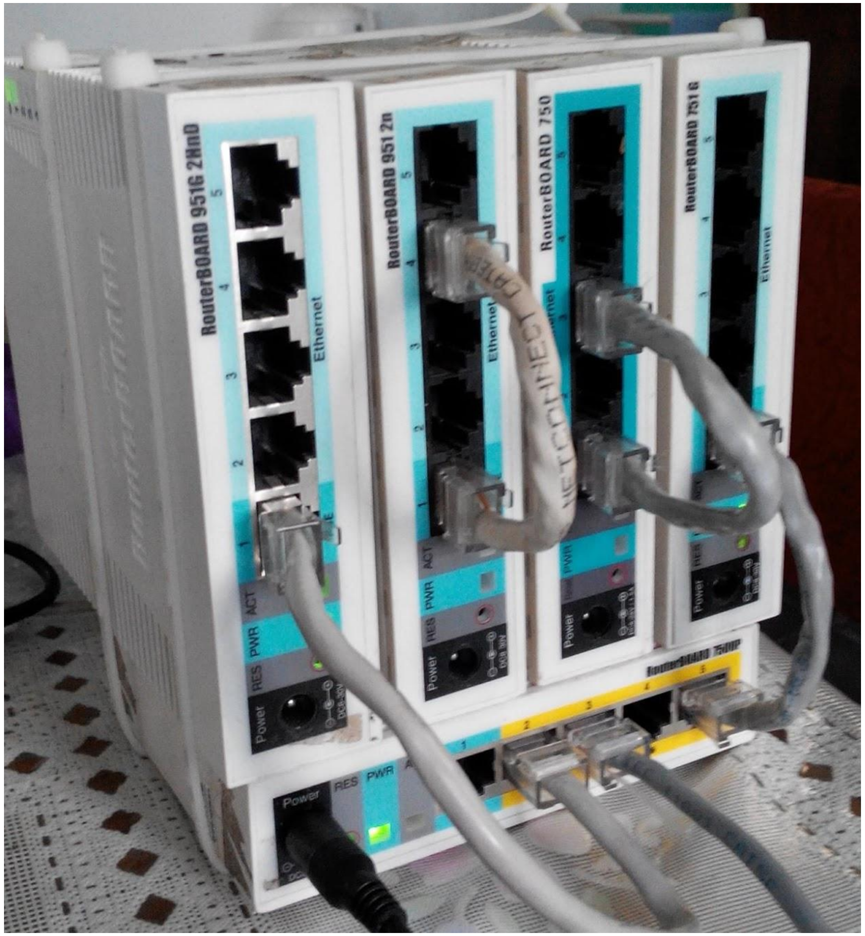
Chain: prerouting

enabled

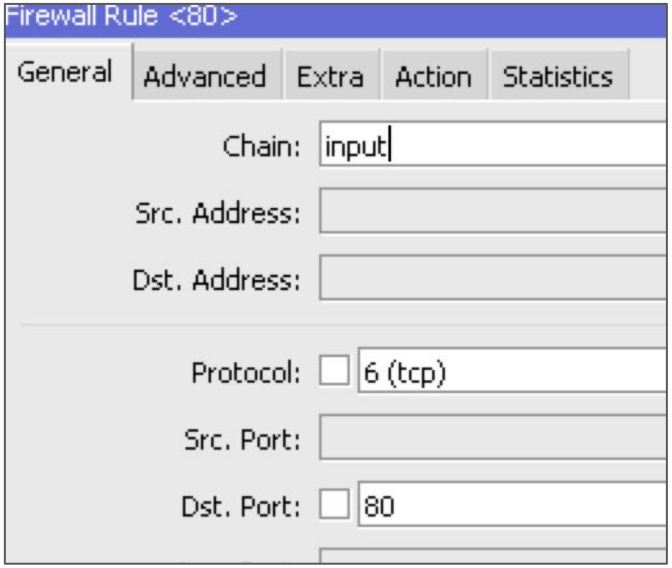


Action: accept

demo


RouterBOARD 951G 2HnD
RouterBOARD 951 2n
RouterBOARD 750
RouterBOARD 751G
RouterBOARD 750UP
Ethernet
Power
RES
PWR
ACT

Combined with connection-limit and address list



Chain: input

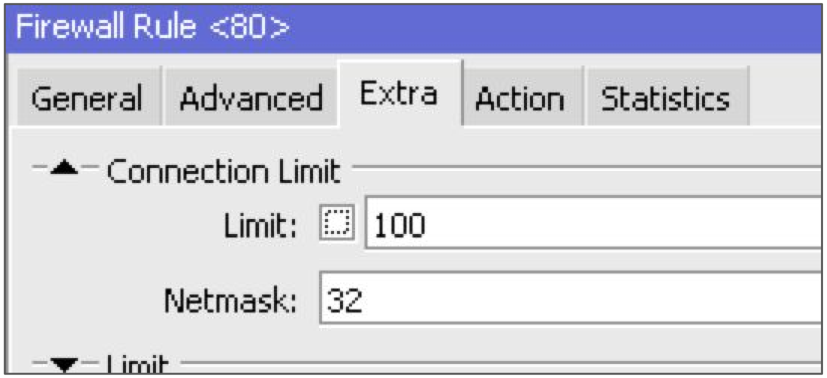
Src. Address:

Dst. Address:

Protocol: □ 6 (tcp)

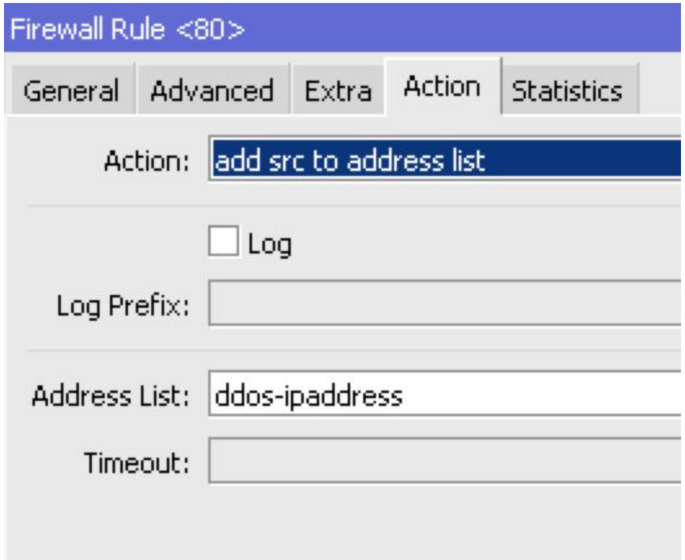
Src. Port:

Dst. Port: □ 80



Limit: □ 100

Netmask: 32



Action: add src to address list

□ Log

Log Prefix:

Address List: ddos-ipaddress

Timeout:

QA

End of slides

- Thank you for your attention
- Please submit your feedback: http://bit.ly/glcfeedback
- Like our facebook page: “GLC networks”
- Stay tune with our schedule