

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?

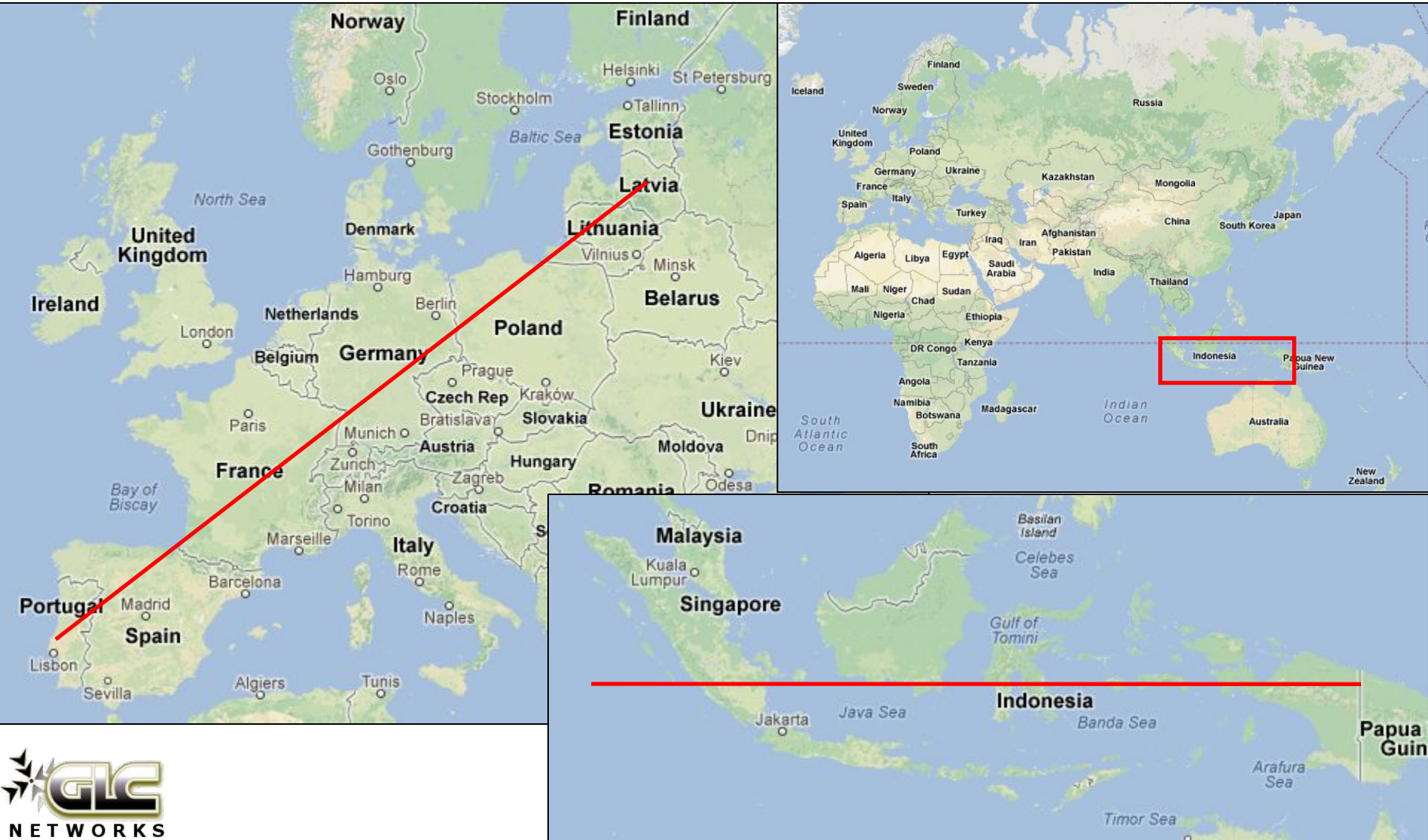
- Garda Lintas Cakrawala (www.glcnetworks.com)
- Based in Bandung, Indonesia
- Areas: Training, IT Consulting
- Mikrotik Certified Training Partner
- Mikrotik Certified Consultant
- Mikrotik distributor

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

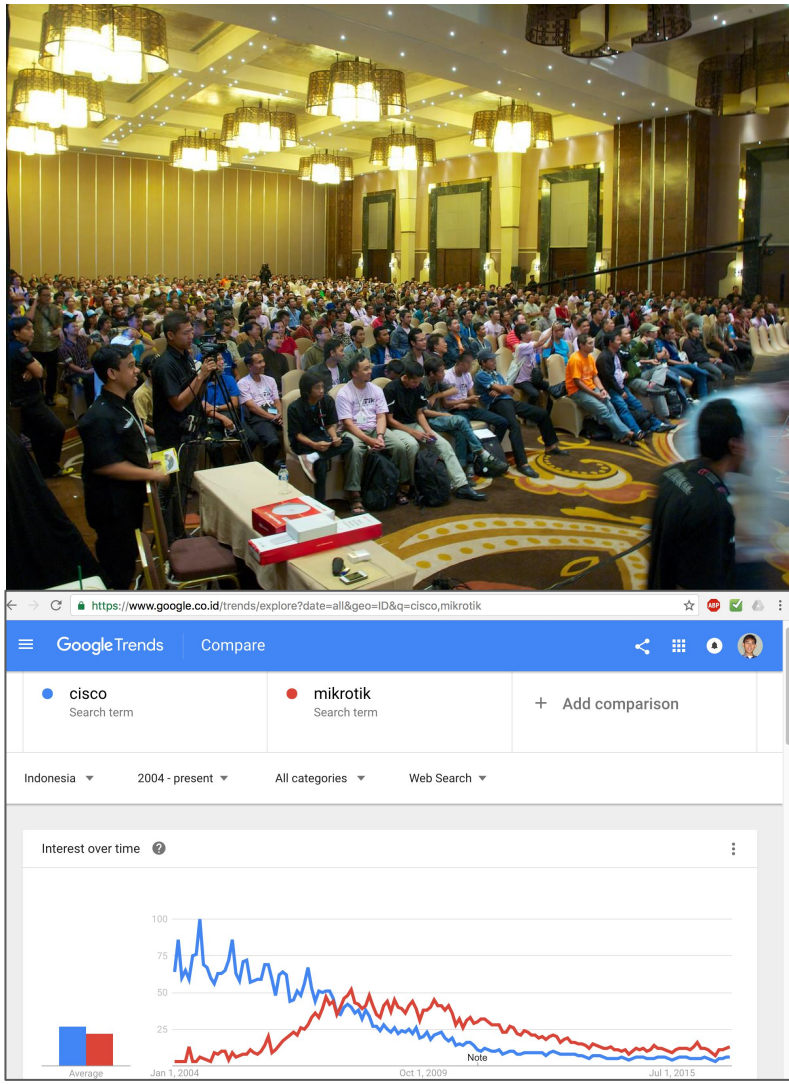






Mikrotik in Indonesia

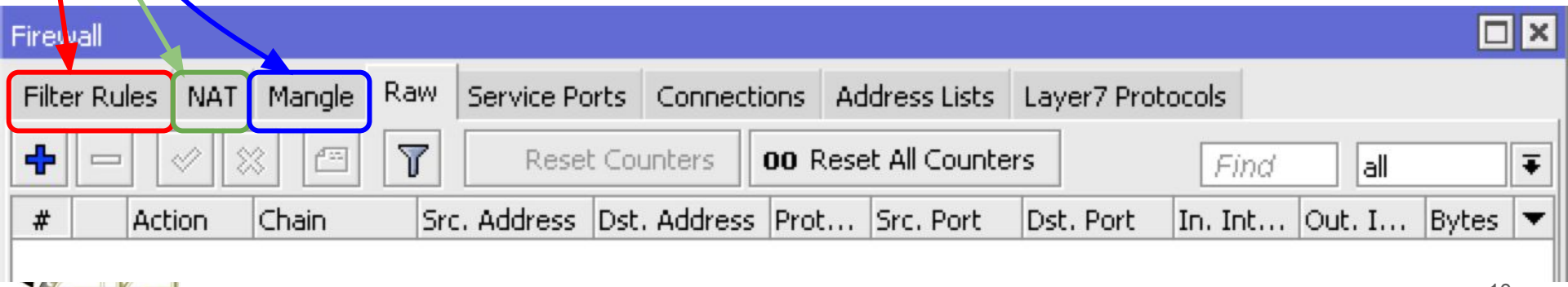
- Very popular product for networking
- Early adoption (beginning of 2000)
- Many schools already join Mikrotik Academy programs
- Lots of training classes
- Biggest MUM in the world (2500+ participants, 2-day event)
- Very active community (facebook, telegram, forum, etc)
- What..? you dont know Mikrotik?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



Firewall

What is Mikrotik firewall?

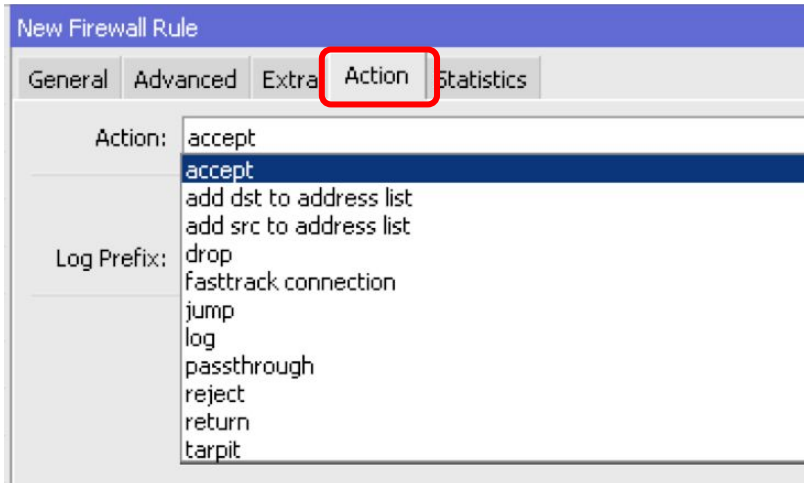
- Is a feature to
  - Control network access (filter)
  - Modify network header (NAT)
  - Marking packet for further processing (mangle)
- Developed from linux
- Consist of 2 parts: matcher & action
- Executed sequentially
- Netadmin must understand the application's characteristics in order to build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

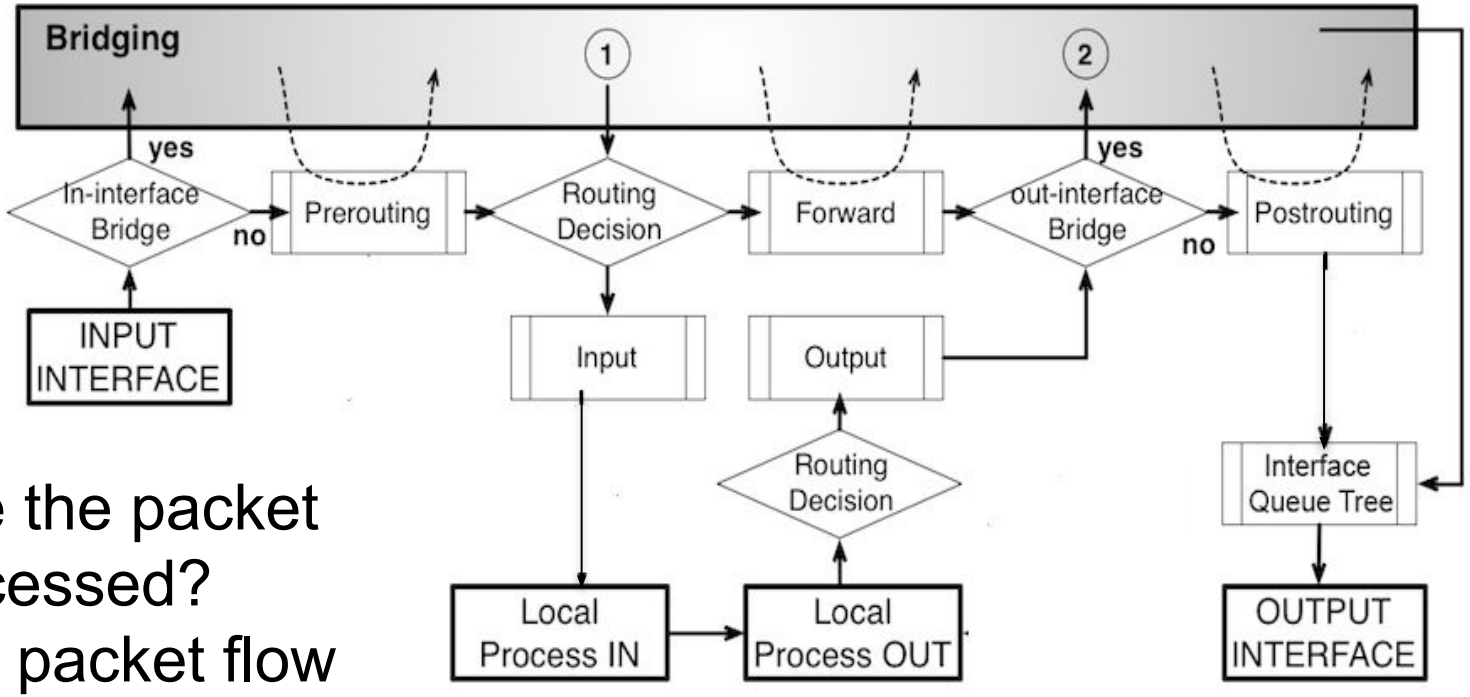




How firewall works?

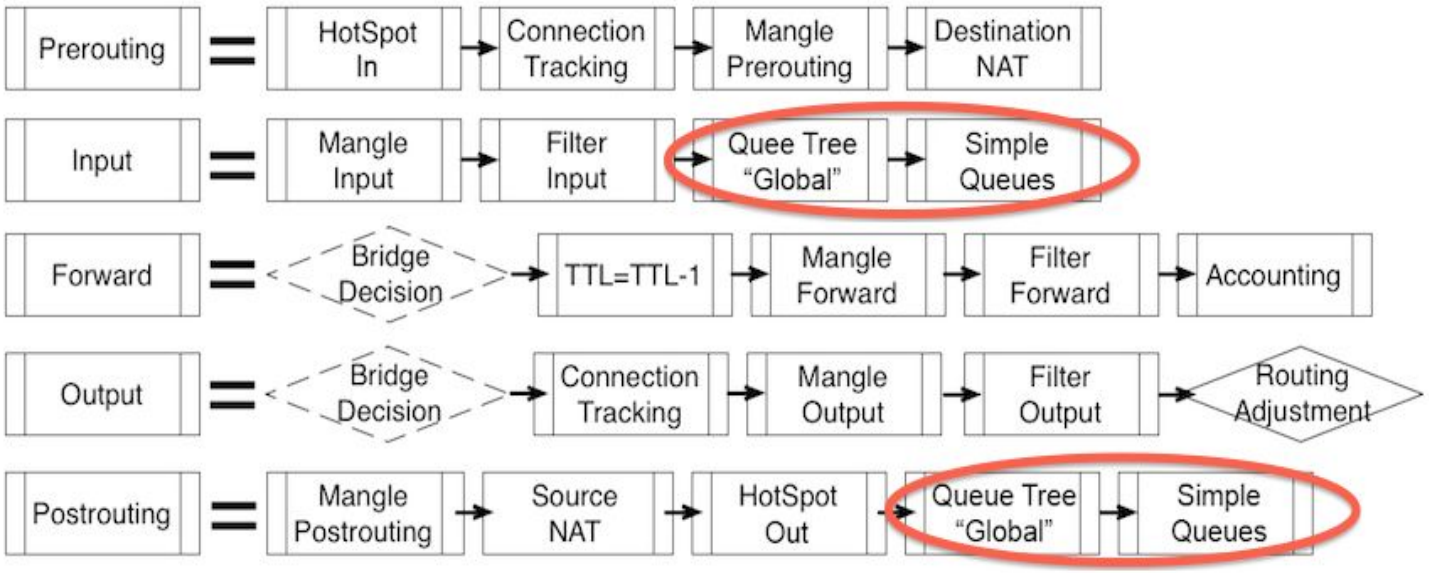
- Setup matcher -> then action
- Mikrotik has lots of options for matcher -> very flexible
- Matcher + Action = Firewall rule
- Rule is executed sequentially

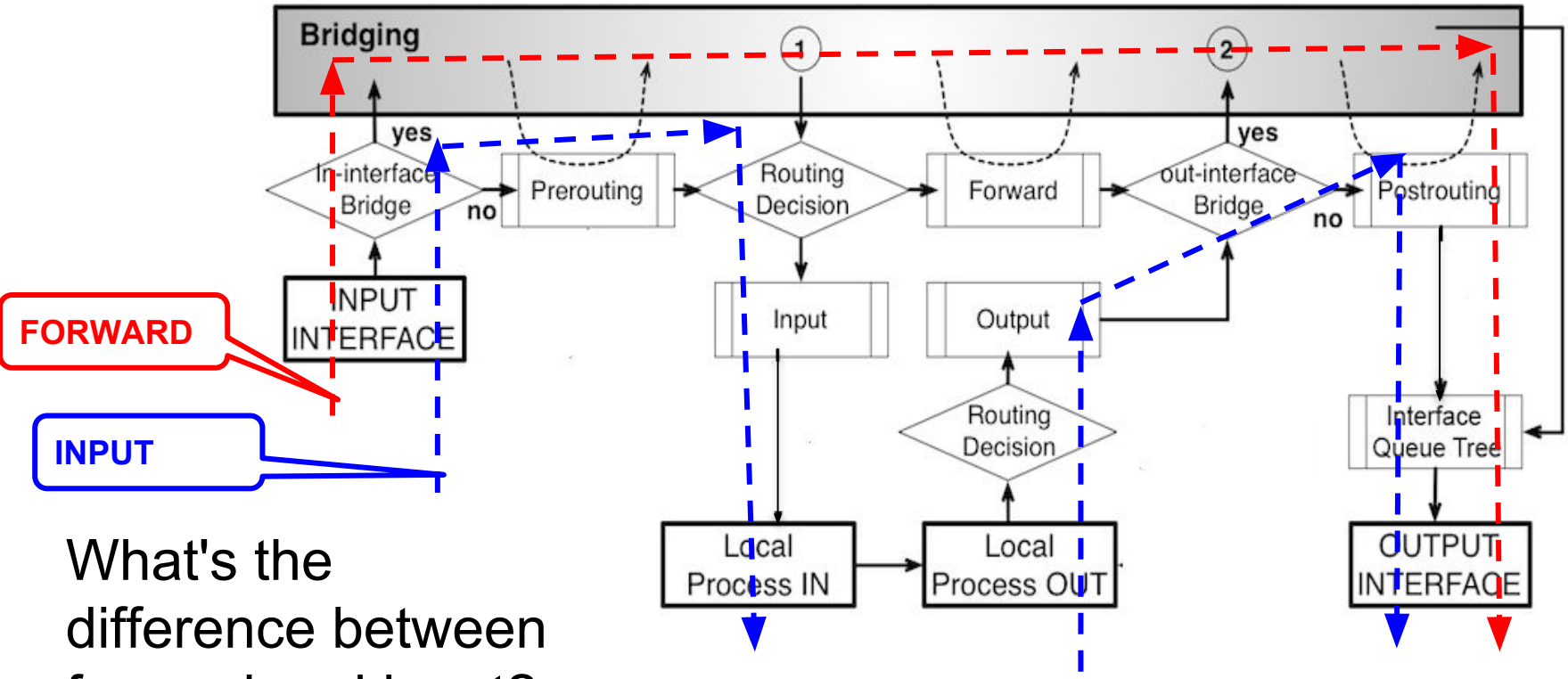




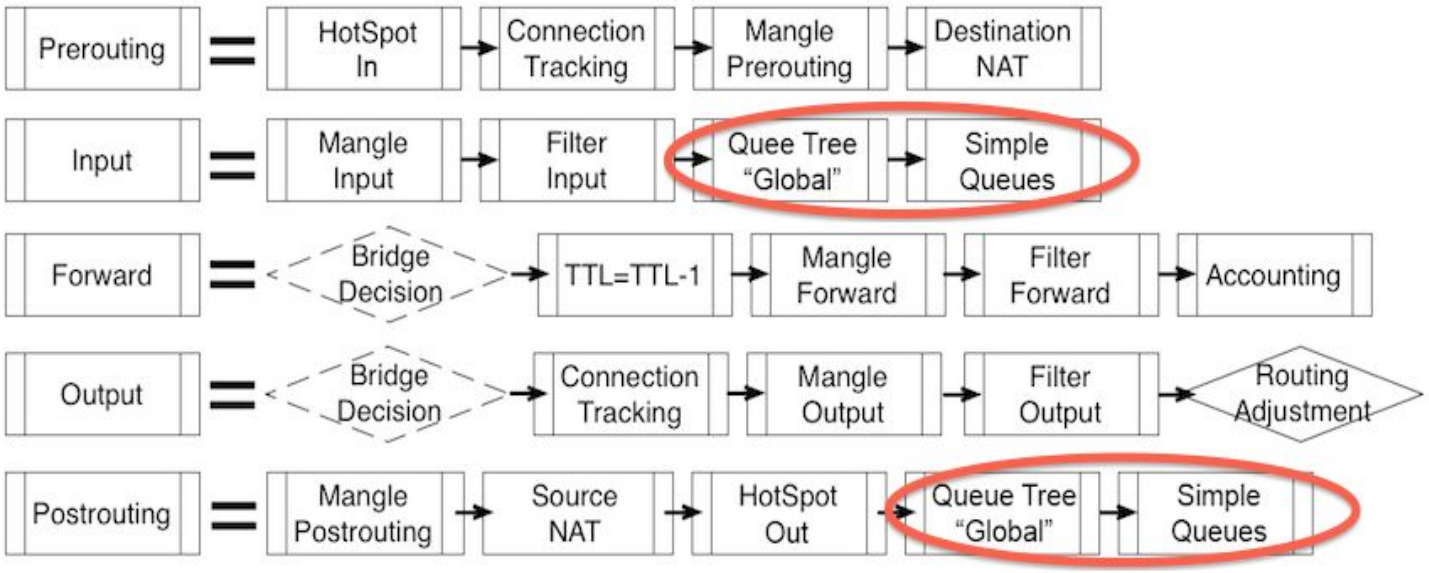
Where the packet is processed?
A: see packet flow

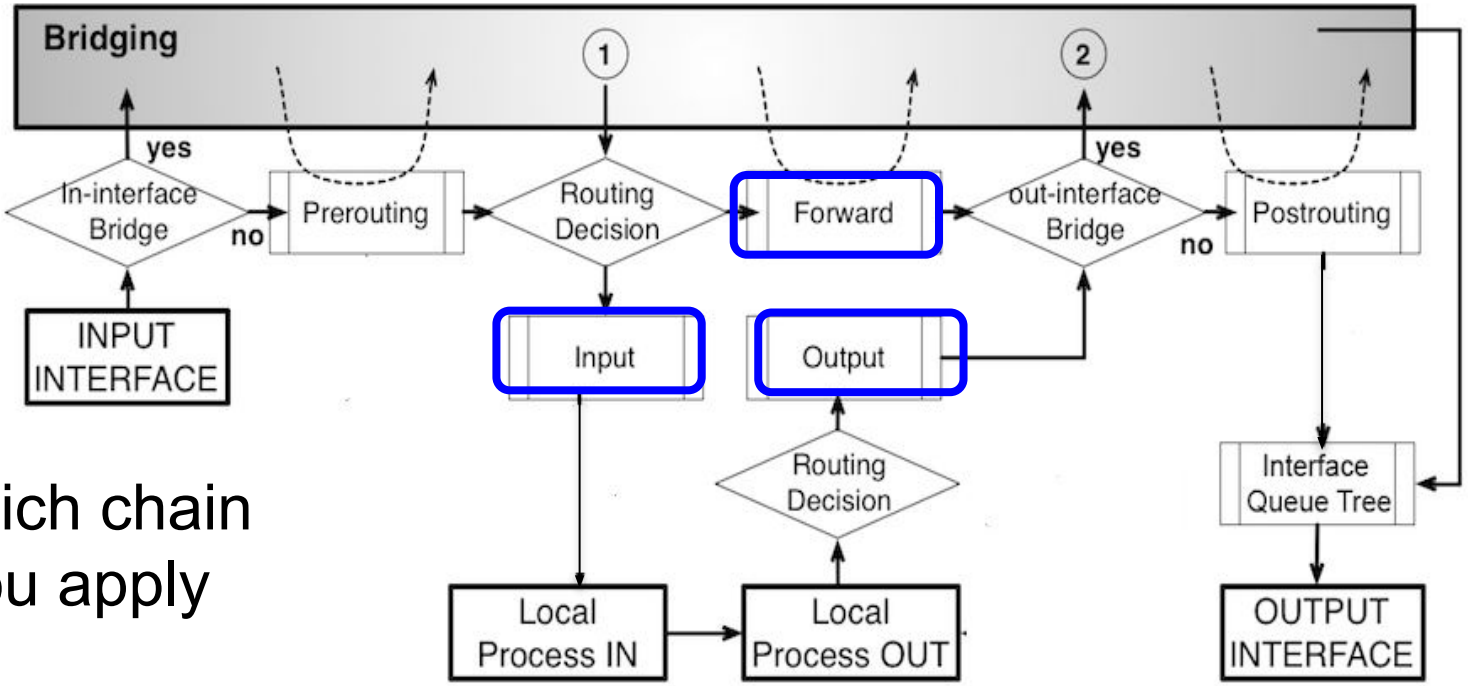
Note: ipsec is removed in this diagram



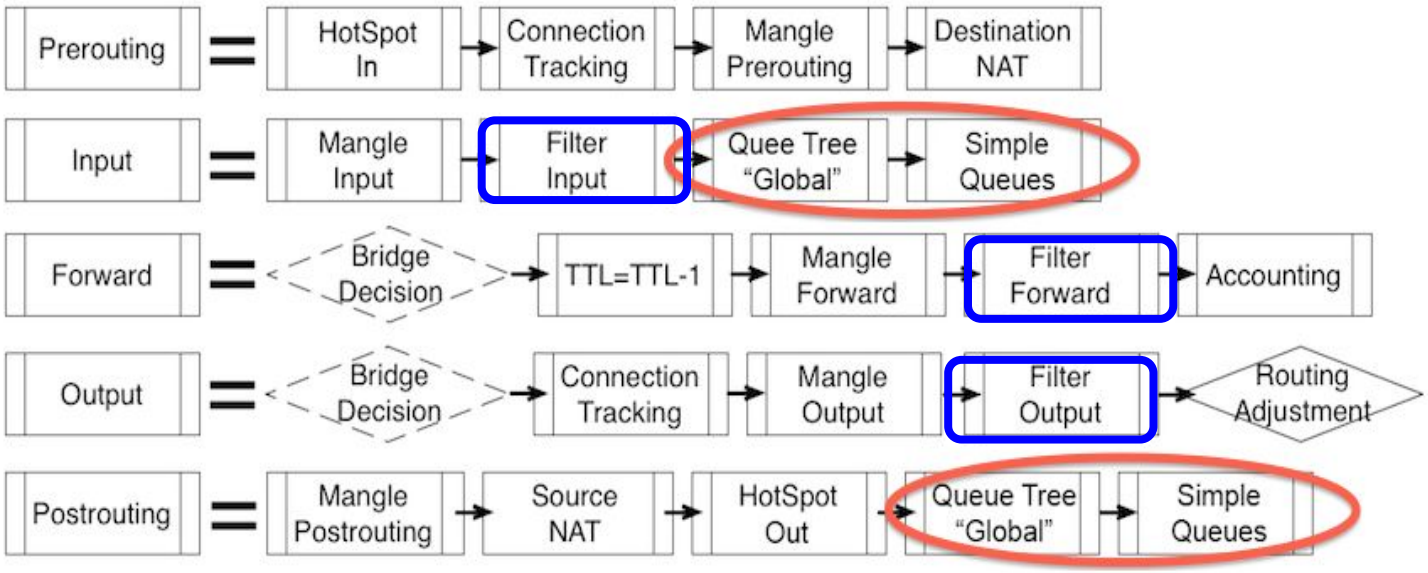


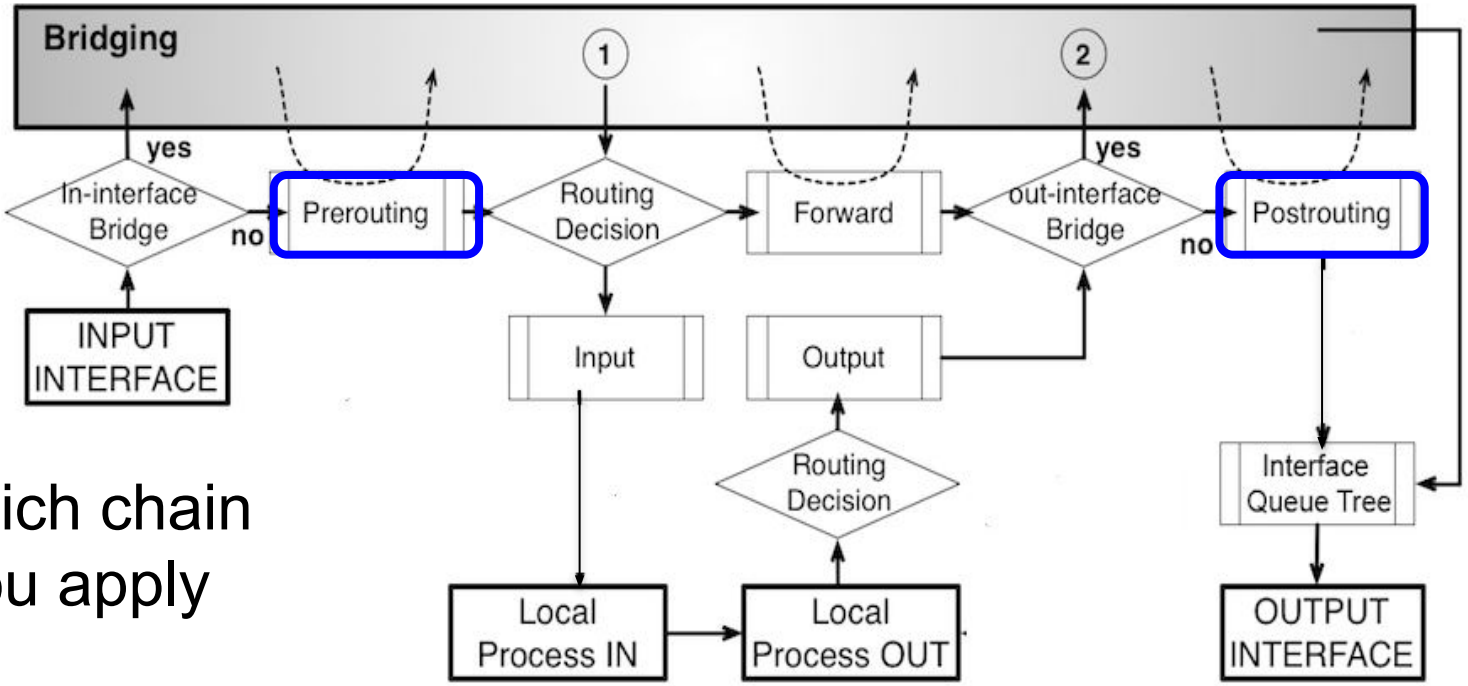
What's the difference between forward and input?



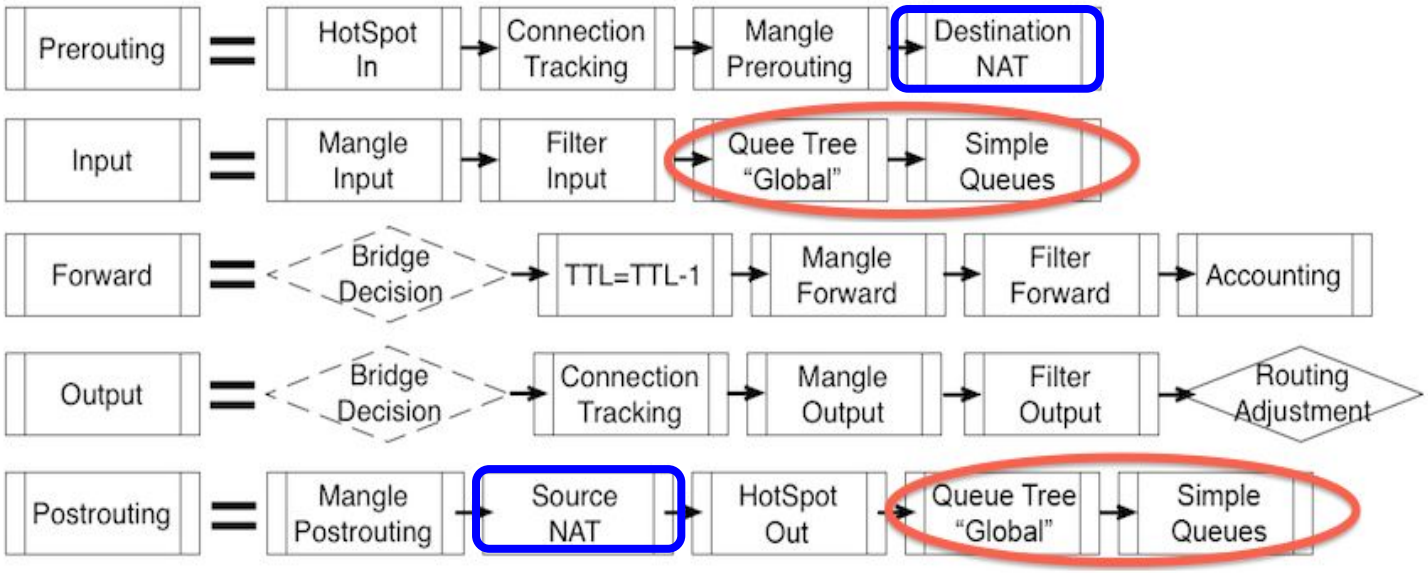


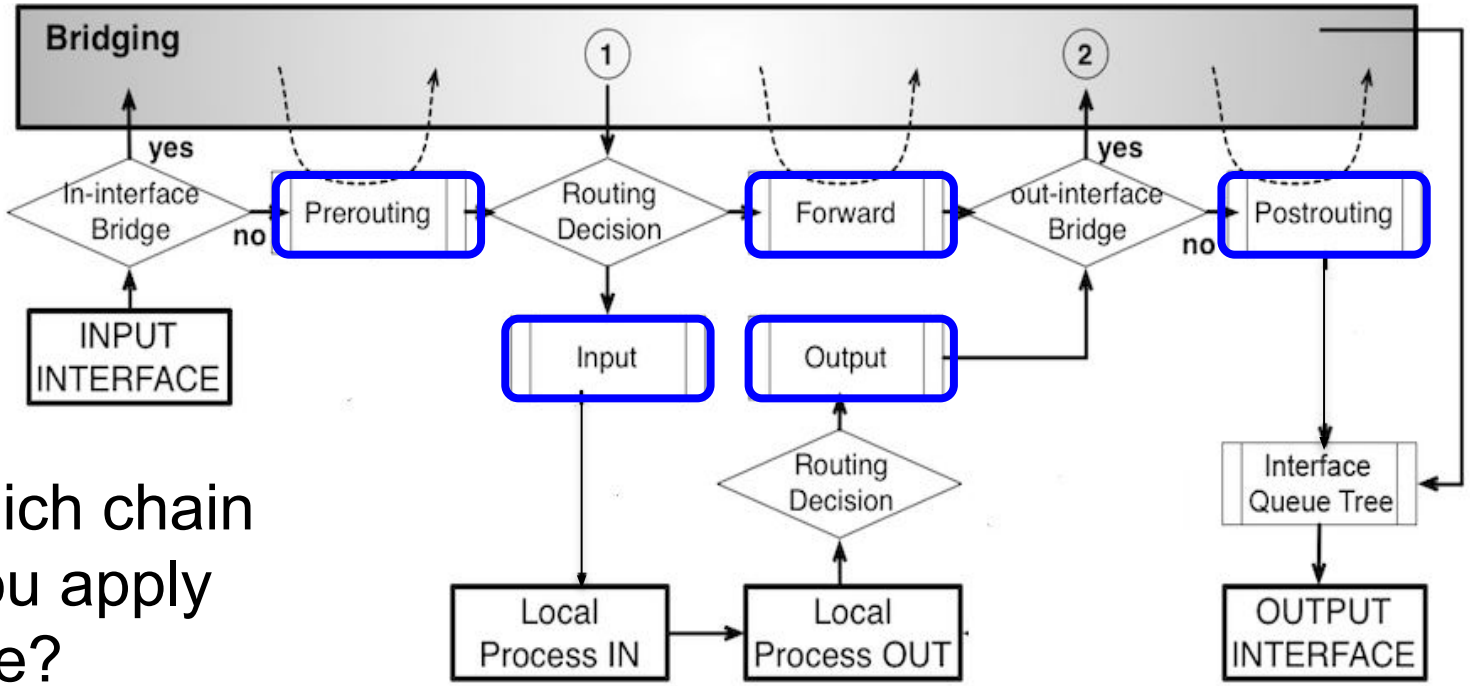
On which chain can you apply filter?



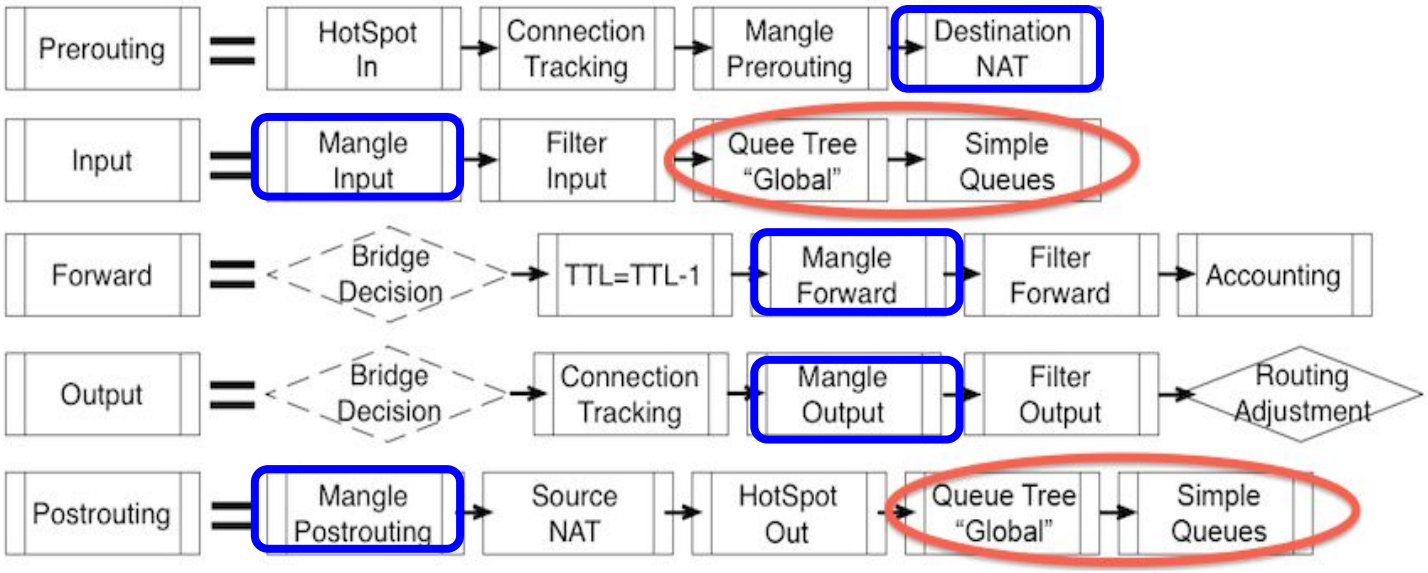


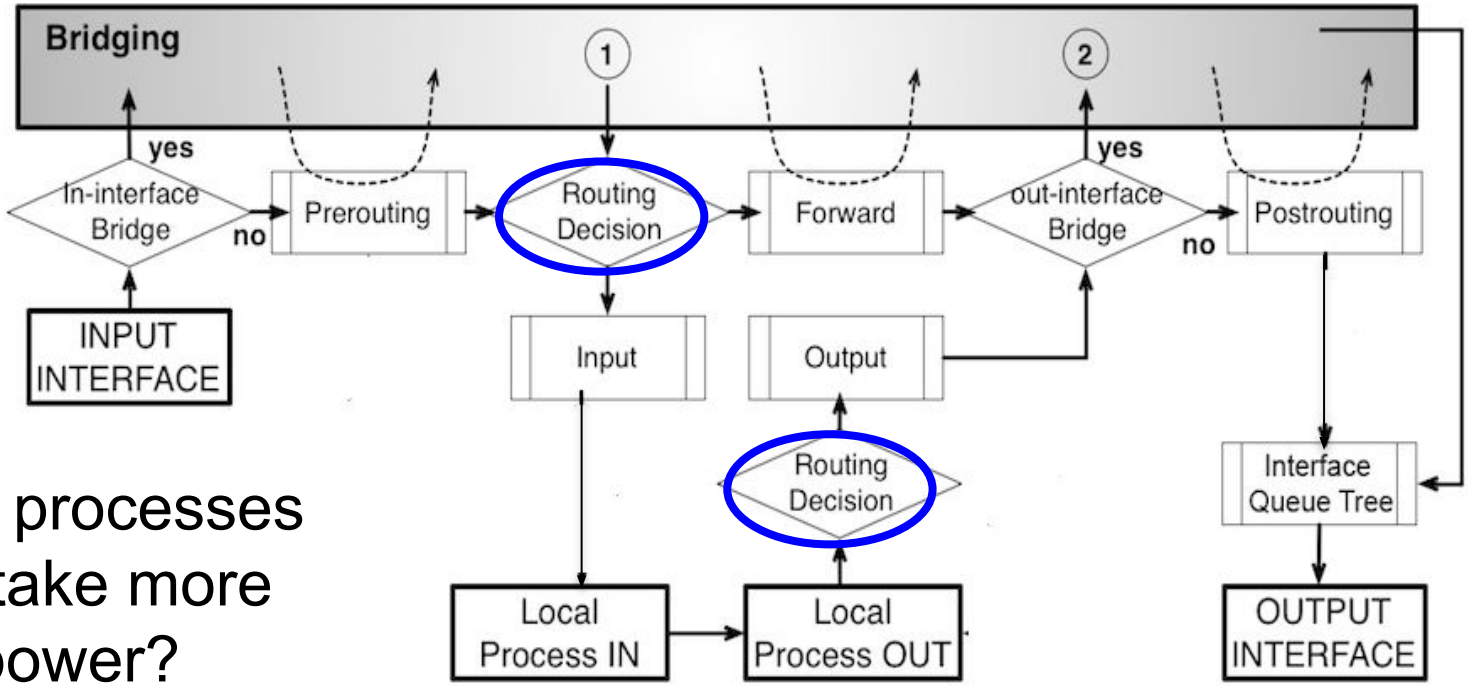
On which chain can you apply NAT?



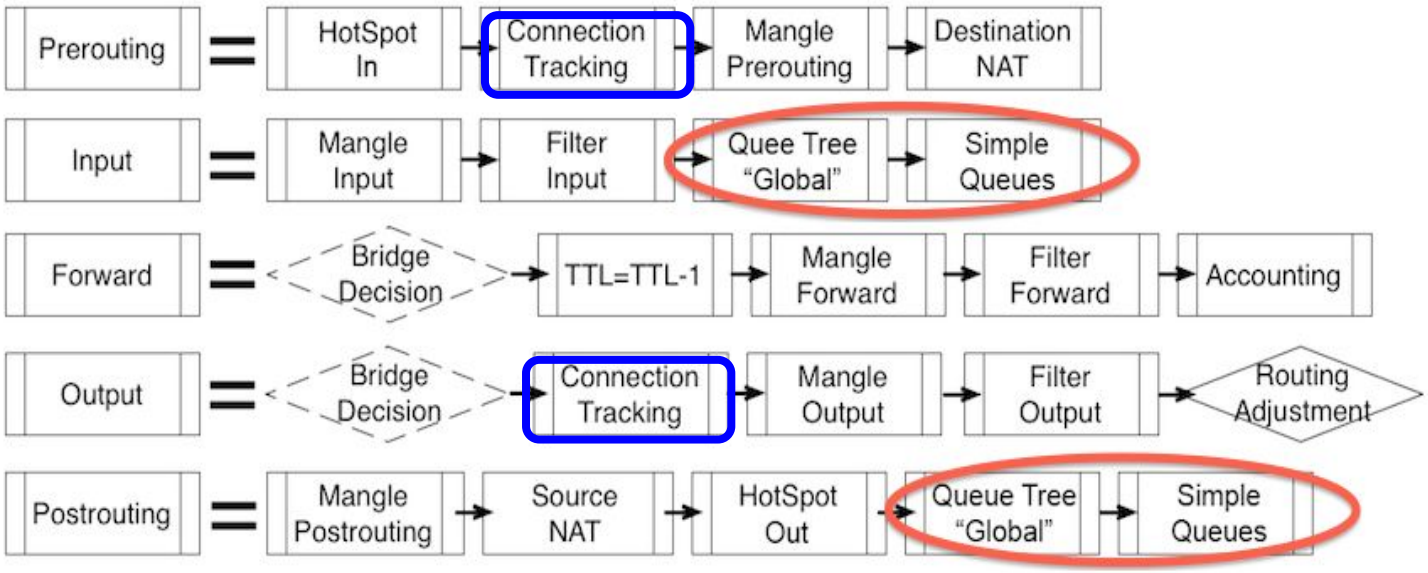


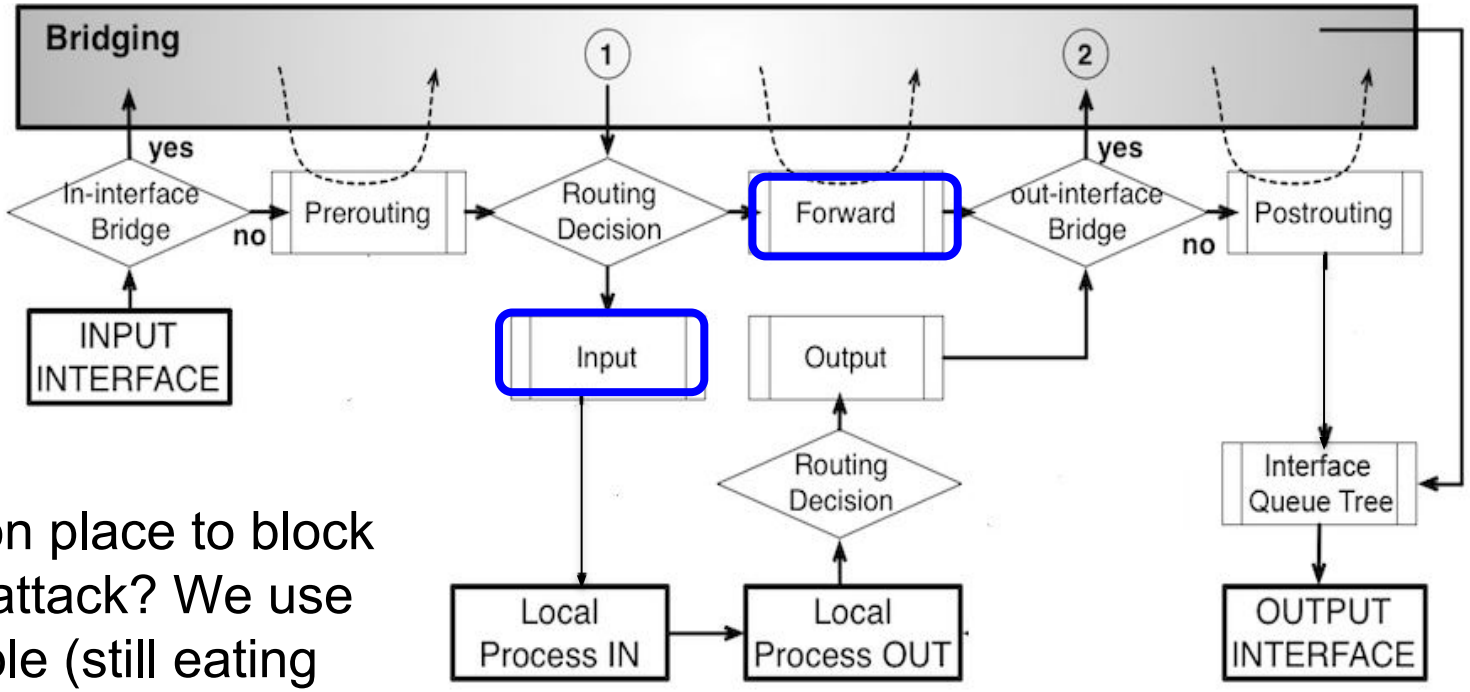
On which chain can you apply mangle?



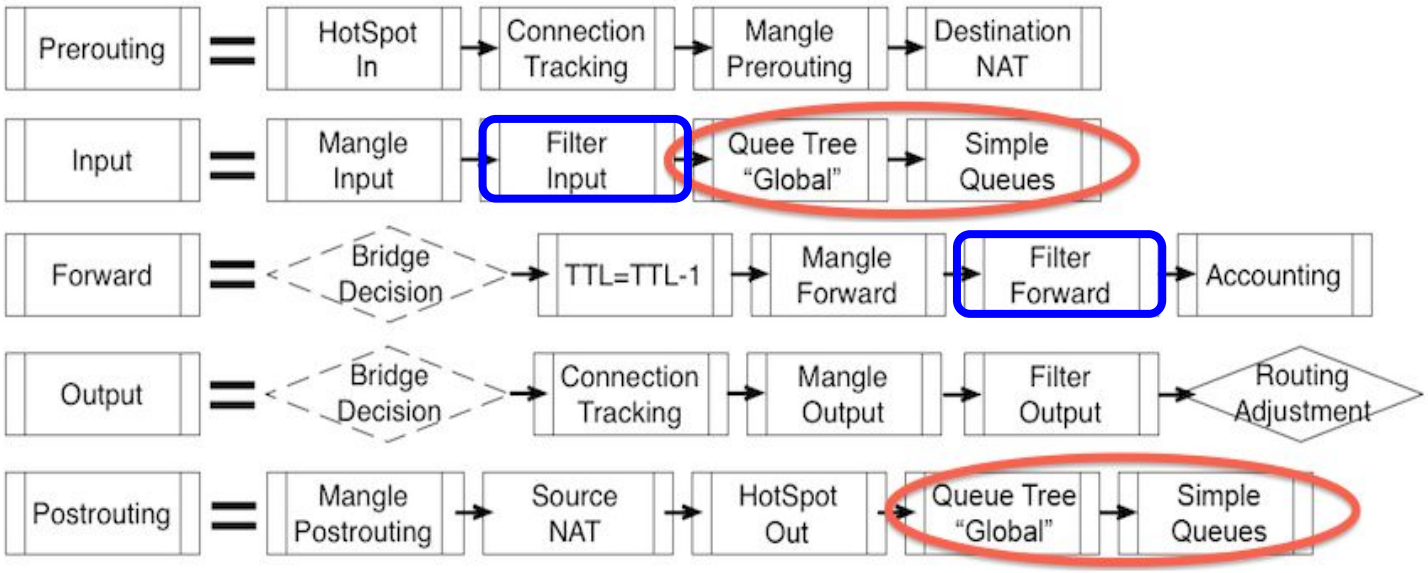


Which processes could take more CPU power?





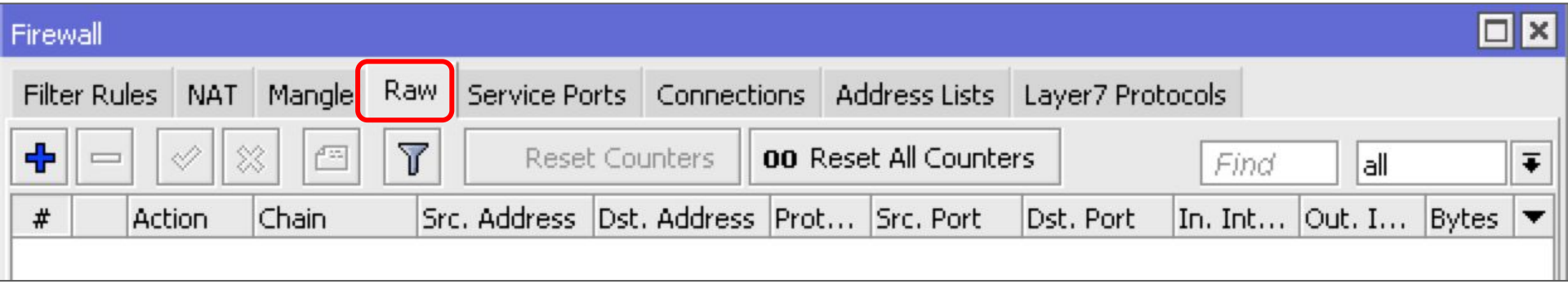
Common place to block DDOS attack? We use filter table (still eating CPU power)



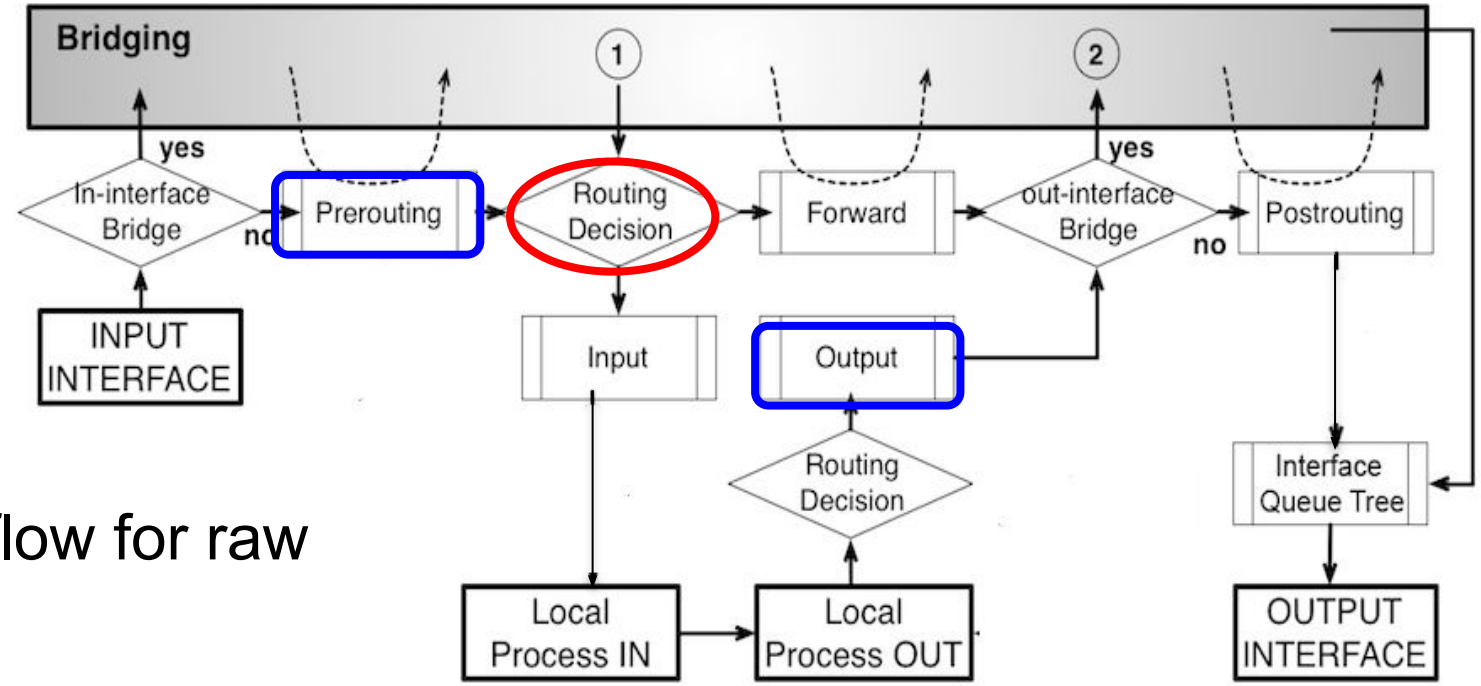
Raw table

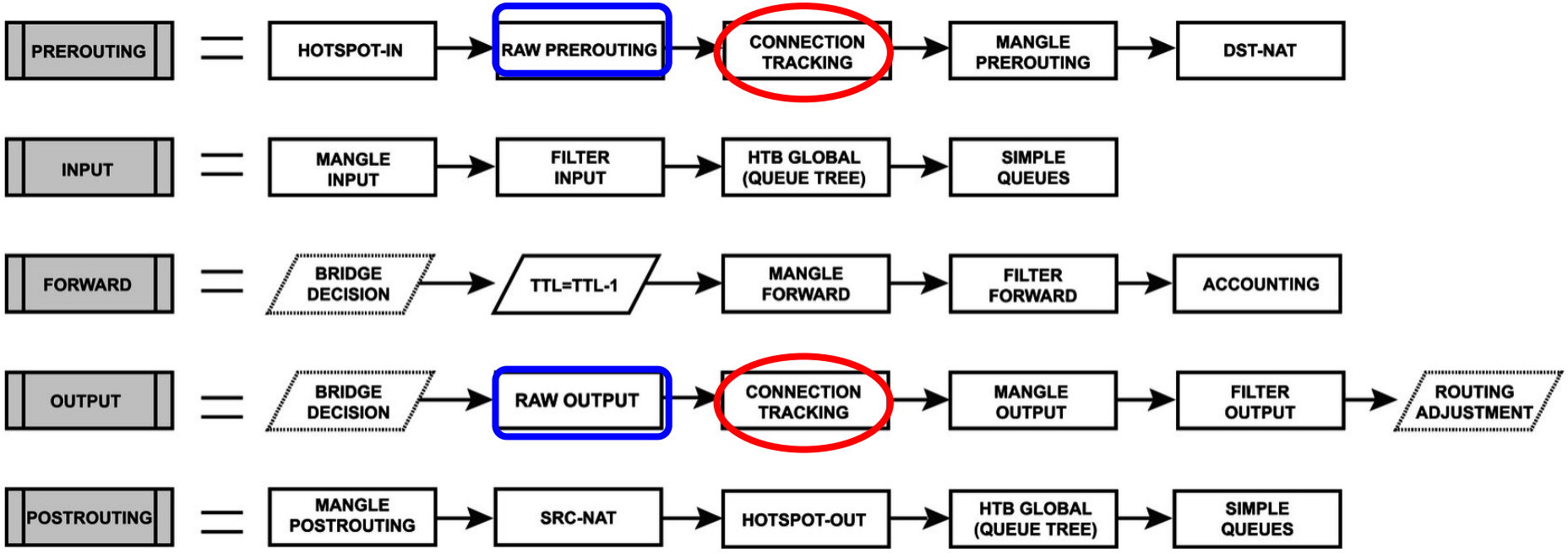
Raw table

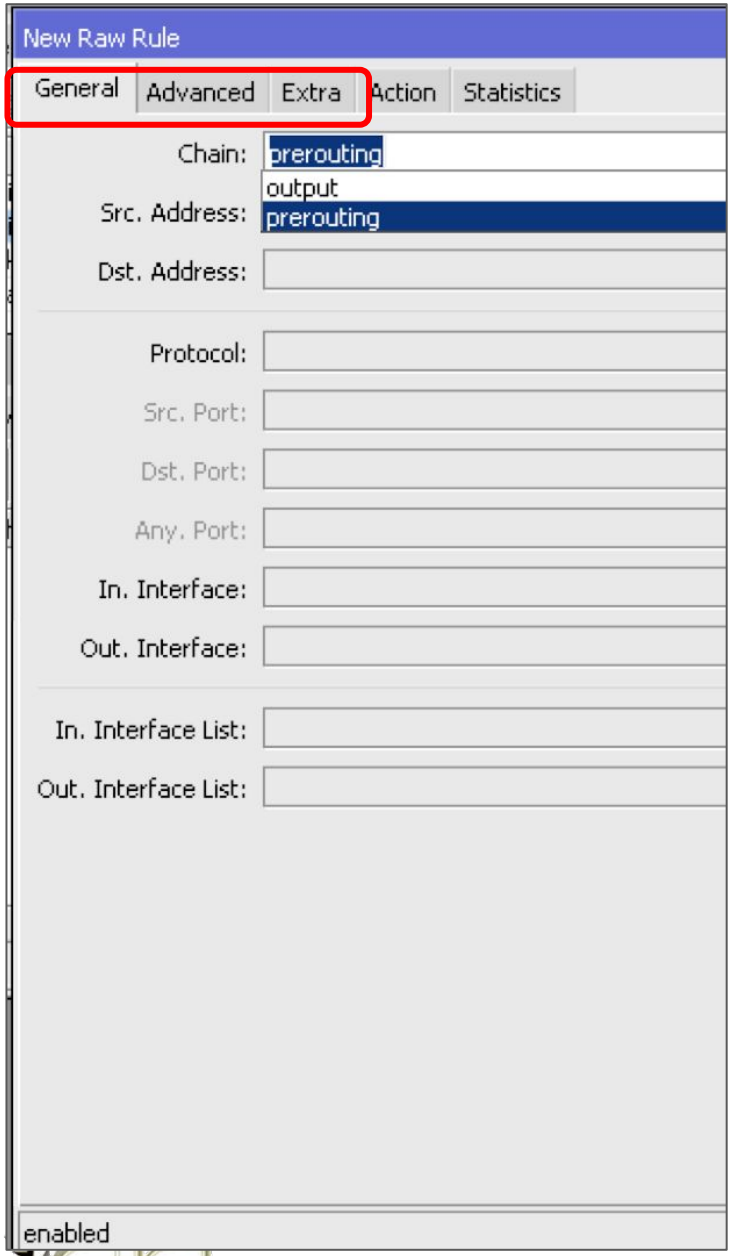
- allows to selectively bypass or drop packets before connection tracking
- does not have matchers that depend on connection tracking (like connection-state, layer7 etc.)
- If packet is marked to bypass connection tracking, packet de-fragmentation will not occur



Packet flow for raw table

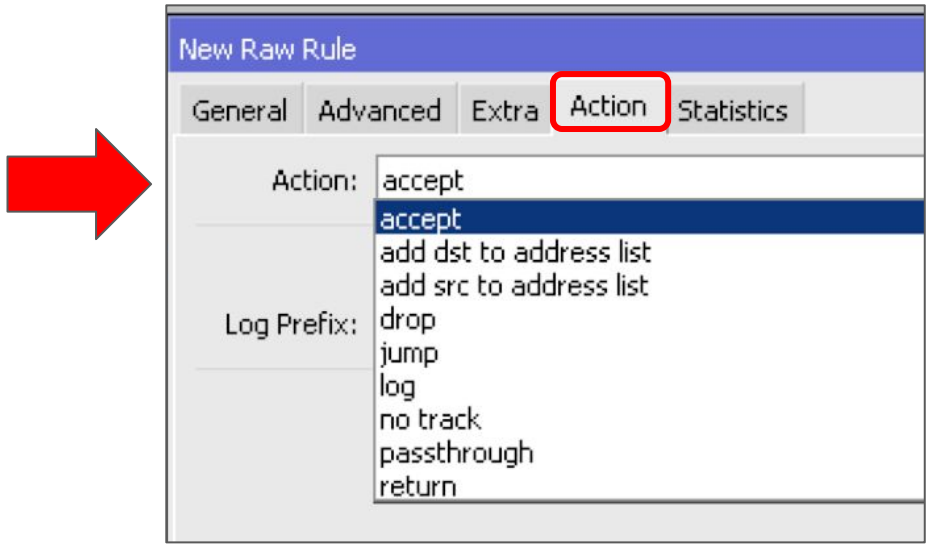




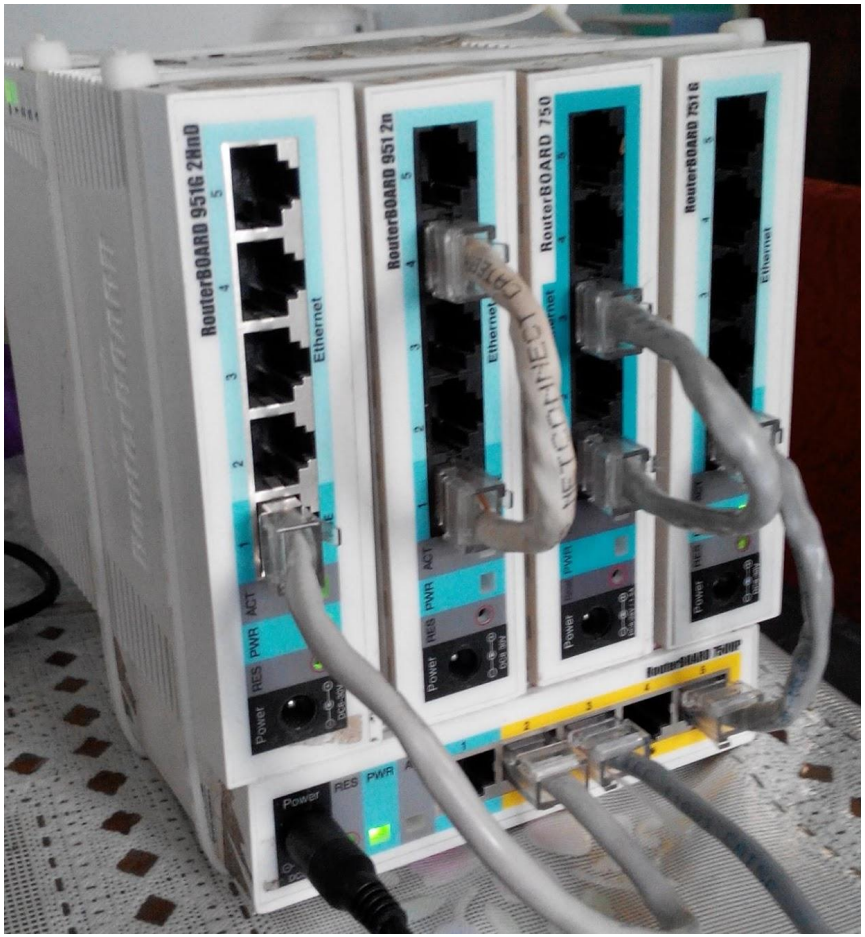


Raw table matchers and action

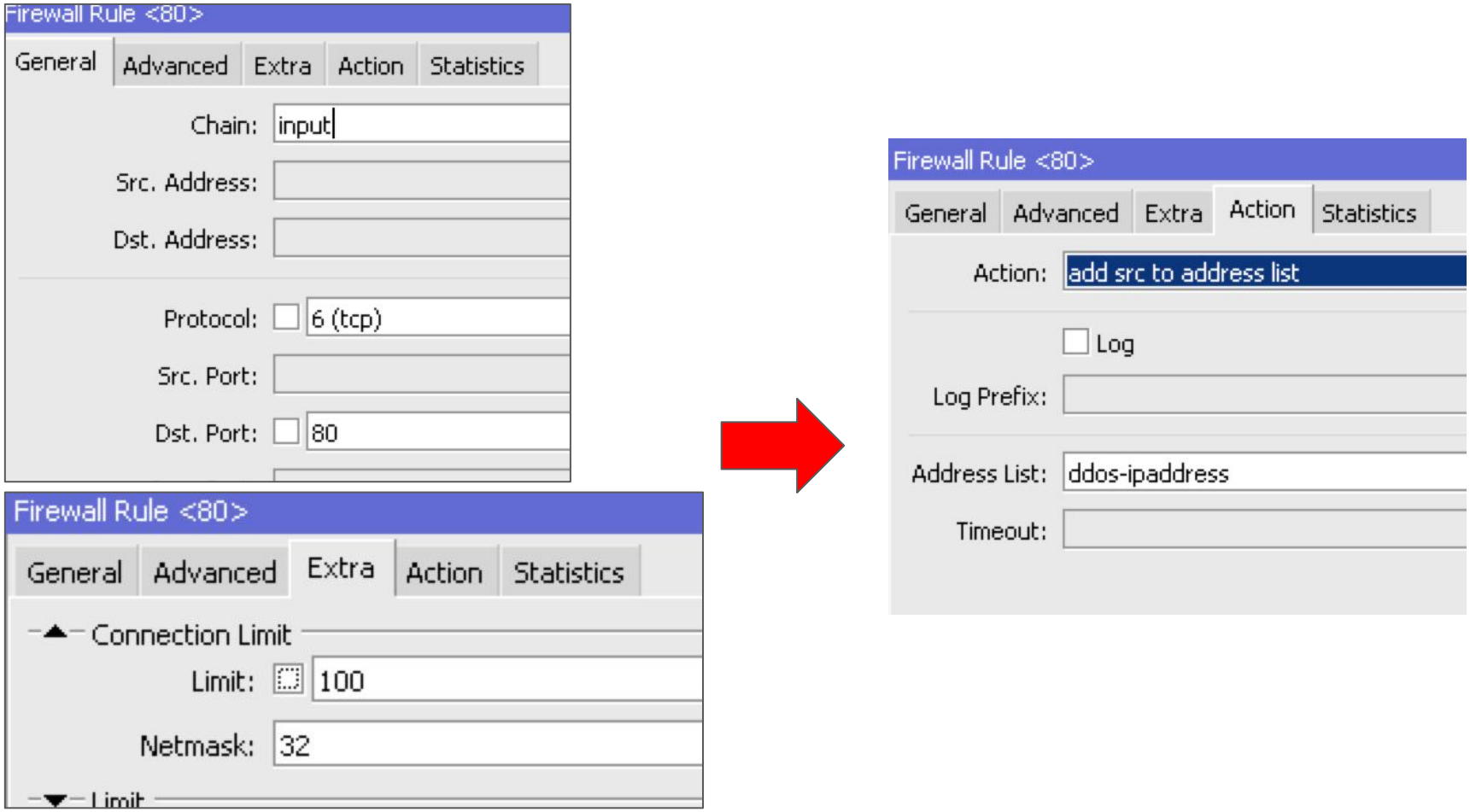
- No paramaters related to connection tracking (l7-filter, conn-mark, bytes, etc)



demo


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

Combined with connection-limit and address list



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