SAPIENZA
UNIVERSITÀ DI ROMA

Practical Network Defense

Master's degree in Cybersecurity 2020-21

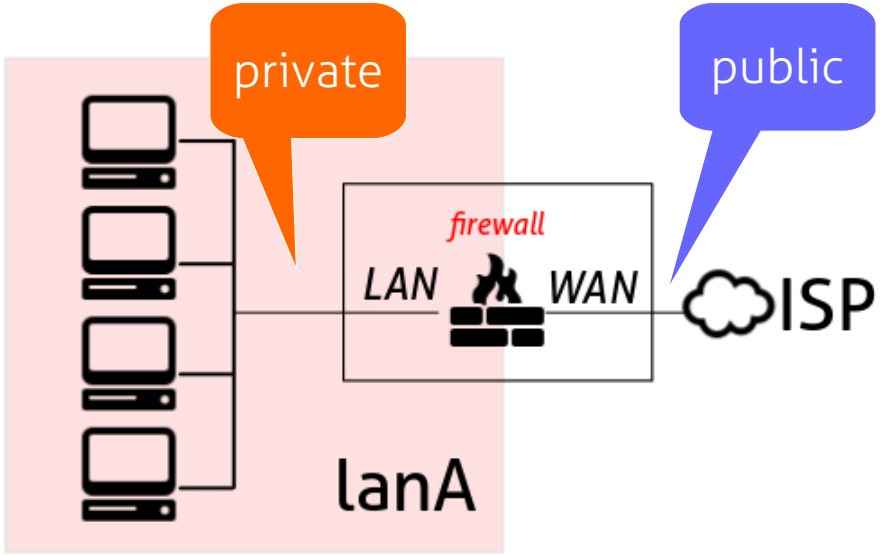
Iptables and NAT

Angelo Spognardi
spognardi@di.uniroma1.it
Dipartimento di Informatica
Sapienza Università di Roma

Network Address Translation (NAT)

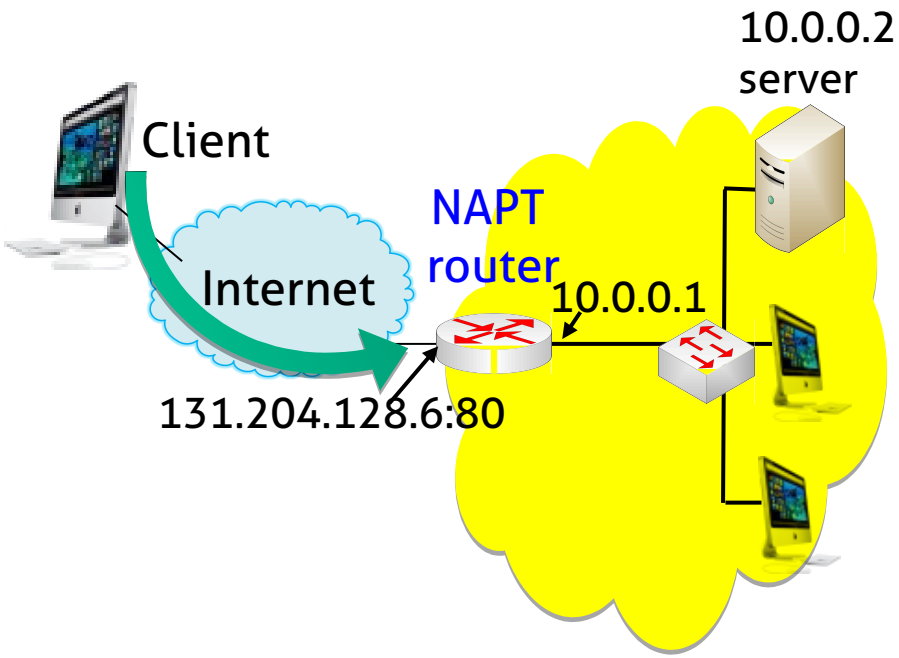
- Translate the address (f.e.: between incompatible IP addressing)
- Informally speaking, connecting to the Internet a LAN using un-routable in-house LAN addresses

- NAT in a routed firewall:
  - Can filter requests from hosts on WAN side to hosts on LAN side
  - Allows host requests from the LAN side to reach the WAN side
  - Does not expose LAN hosts to external port scans



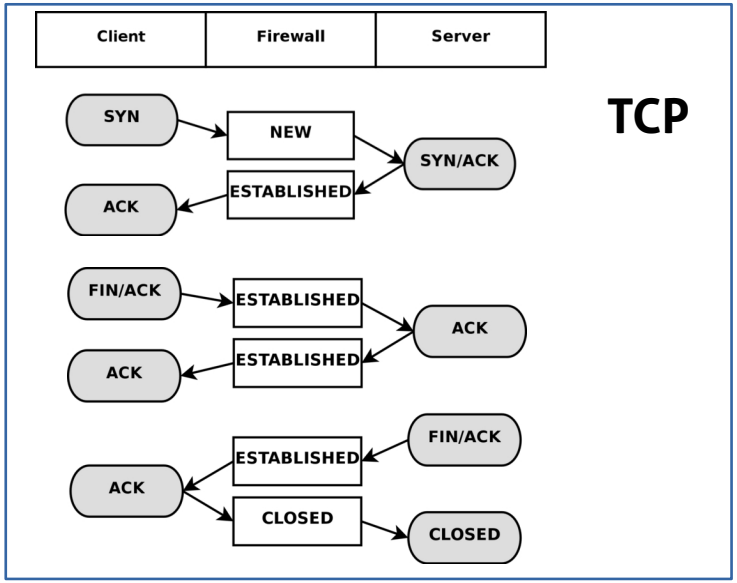
NAPT for Incoming Requests

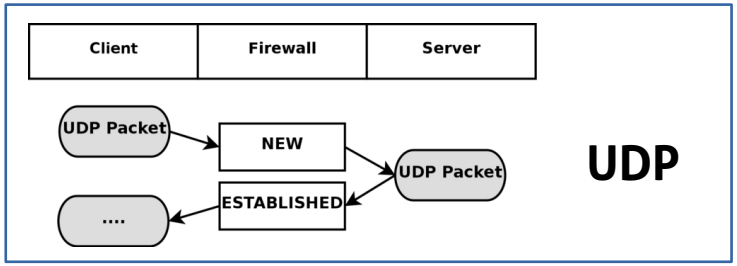
- NAPT router blocks all incoming ports by default
- Many applications have had problems with NAPT in the past in their handling of incoming requests
- Four major methods
  - Application Level Gateways (ALGs)
  - Static port forwarding
  - Universal Plug and Play (UPnP) Internet Gateway Device (IGD) protocol
  - Traversal Using Relays around NAT (TURN)

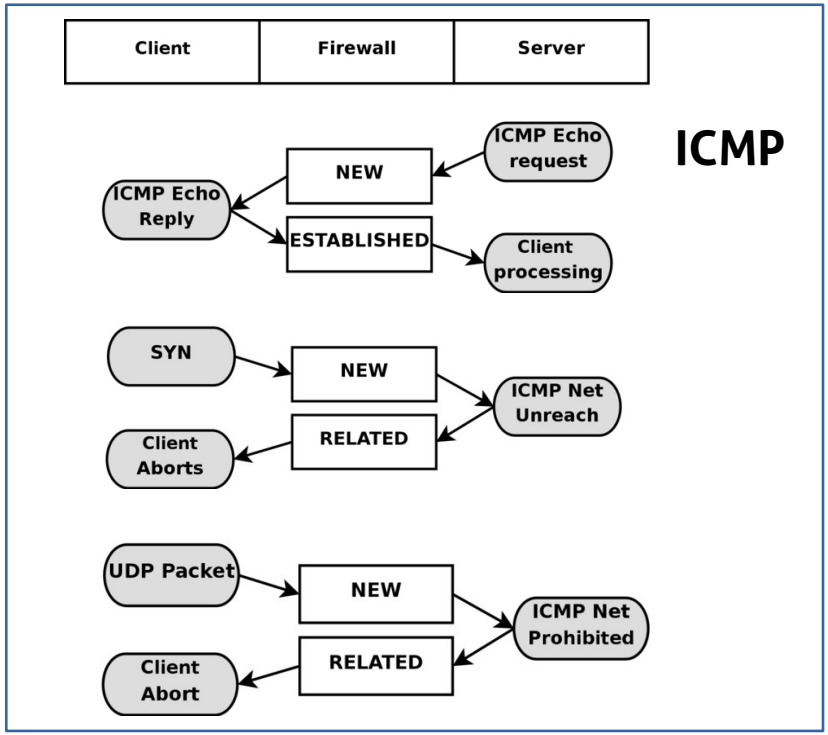


More on the conntrack module

- Clever use of logic to recognize connections, even with connection-less protocols (UDP, ICMP...)







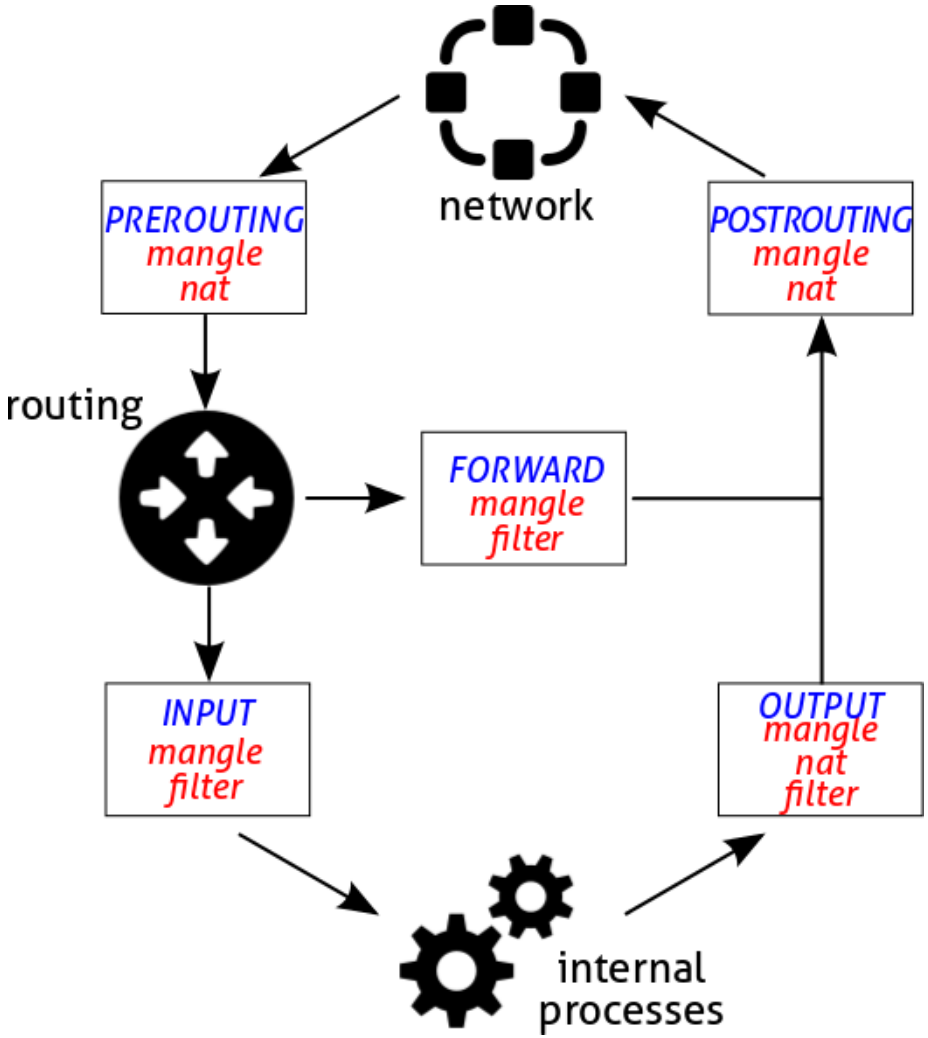
More on this:

https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html#STATEMACHINE

iptables: four built-in tables

1. MANGLE: manipulate bits in TCP header
2. FILTER: packet filtering
3. NAT: network adress translation
4. RAW: exceptions to connection tracking
   - When present RAW table has the highest priority
   - Used only for specific reasons
   - Default: not loaded

Chain and table priorities



- MANGLE>NAT>FILTER
- RAW>MANGLE
  - Not shown in the picture
  - Only used during PREROUTING and OUTPUT

NAT table

- Used for NAT (Network Address Translation): to translate the packet's source field or destination field
  - Only the first packet in a stream will hit this table (the rest of the packets will automatically have the same action)
- Special targets (*packet fates/actions*):
  - DNAT: destination nat
  - SNAT: source nat
  - MASQUERADE: dynamic nat (when fw interface address is dynamically assigned)
  - REDIRECT: redirects the packet to the machine itself

NAT'ing targets

- DNAT: Destination address translation
  - Transform the destination IP of incoming packets
  - Used in PREROUTING chain
- SNAT: Source address translation
  - Transform the source IP of outgoing packets
    - Can be done one-to-one or many-to-one
  - Used in POSTROUTING chain
- MASQUERADE: like SNAT but the source IP is taken form the dynamically assigned address of the interface

iptables logging

- LOG as possible target
  - "non-terminating target", i.e. rule traversal continues at the next rule
  - to log dropped packets, use the same DROP rule, but with LOG target
- When this option is set for a rule, the Linux kernel will print some information on all matching packets (like most IP header fields) via the kernel log (where it can be read with dmesg or syslogd(8))

--log-level level: specifies the type of log (emerg, alert, crit, err, warning, notice, info, debug)

--log-prefix prefix: add further information to the front of all messages produced by the logging action

Log example

- Log fowarded packets
  - `iptables -A FORWARD -p tcp -j LOG \ --log-level info --log-prefix "Forward INFO"`
- Log and drop invalid packets
  - `iptables -A INPUT -m conntrack --ctstate \ INVALID -j LOG --log-prefix "Invalid packet"`
  - `iptables -A INPUT -m conntrack --ctstate \ INVALID -j DROP`

Lab activity

Main tasks

- Iptables and ip6tables
- Reference links:
  - Linux ipv6 configuration: ipv6 sysctl
    - https://www.kernel.org/doc/Documentation/networking/ip-sysctl.txt
  - Iptables reference manual
    - www.frozentux.net/iptables-tutorial/iptables-tutorial.html

To do the activities

- We will use Kathará (formerly known as netkit)
  - A container-based framework for experimenting computer networking: http://www.kathara.org/
- A virtual machine is made ready for you
  - https://drive.google.com/file/d/1W6JQzWVyH5_LKLD20R6XH1ugPDP5LWP5/view?usp=sharing
- For not-Cybersecurity students, please have a look at the Network Infrastructure Lab material
  - http://stud.netgroup.uniroma2.it/~marcos/network_infrastructures/current/cyber/
    - Instructions are for netkit, we will use kathara

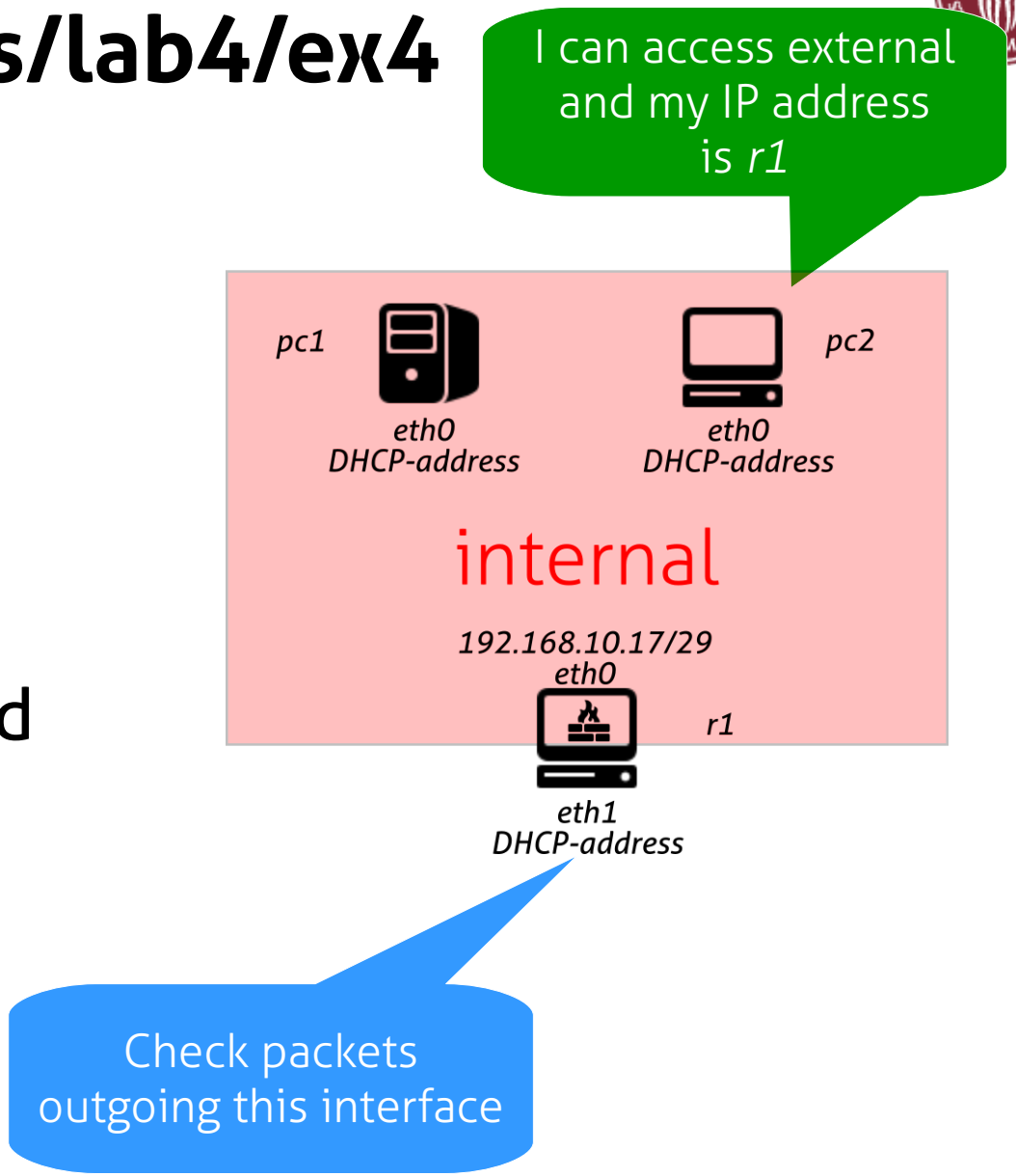
The kathara VM

- It should work in both Virtualbox and VMware
- It should work in Linux, Windows and MacOS
- There are some alias (shortcuts) prepared for you
  - Check with **`alias`**
- All the exercises can be found in the git repository:
  - https://github.com/vitome/pnd-labs.git
- You can move in the directory and run lstart
  - **NOTE**: launch docker first or the first lstart attempt can (...will...) fail

Lab activity: ex4

Exercise 1: pnd-labs/lab4/ex4

- Enable masquerade
- Setup r1 to perform NATting with iptables
  - Masquerade to exit
- internal is NOT exposed



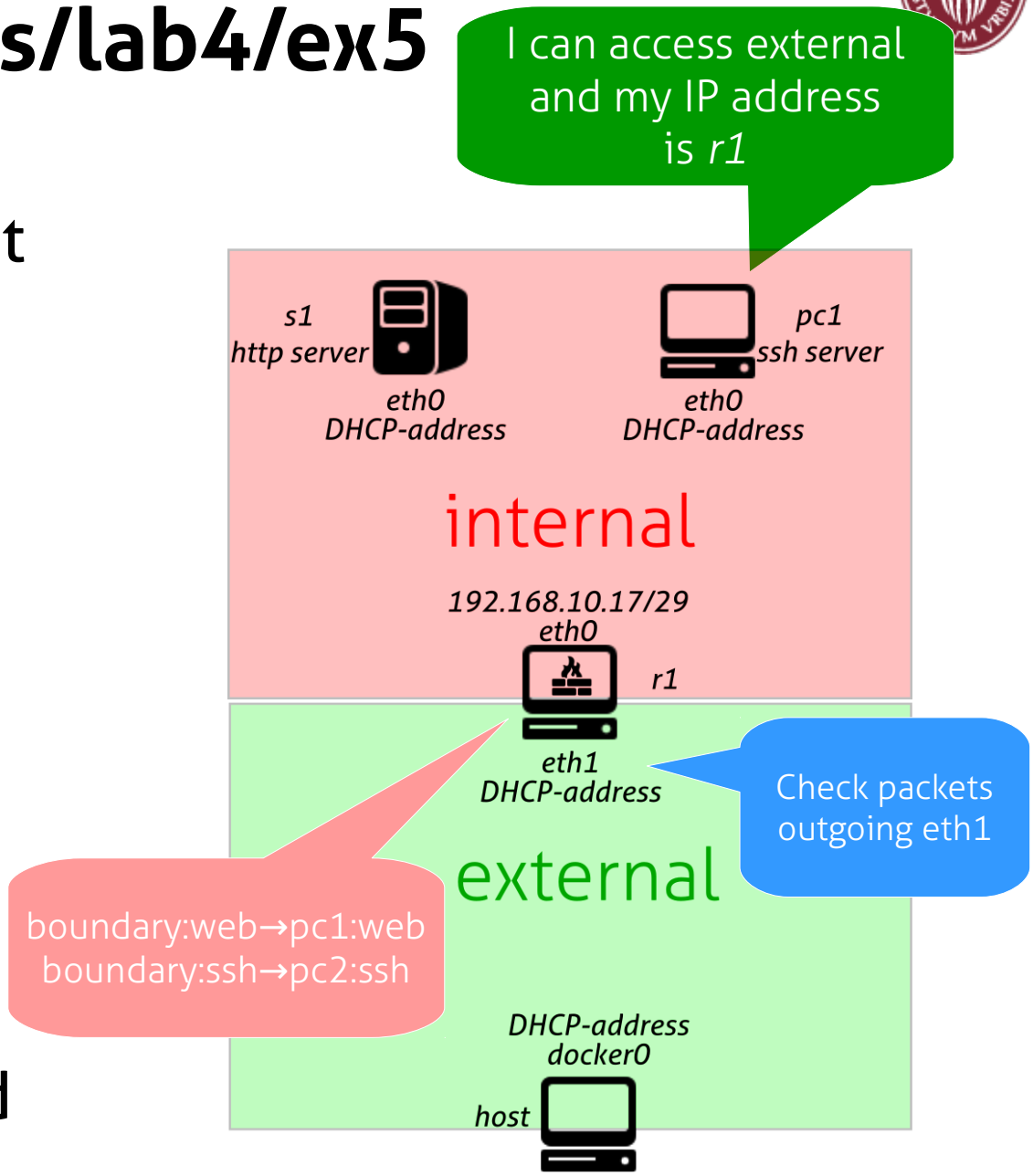
Exercise 1: Policy to protect r1

- Accept ICMP echo replies destined to LAN
- Only accept ICMP echo request from eth1
- Respond with TCP RST or ICMP Unreachable for incoming requests for blocked ports

Lab activity: ex5

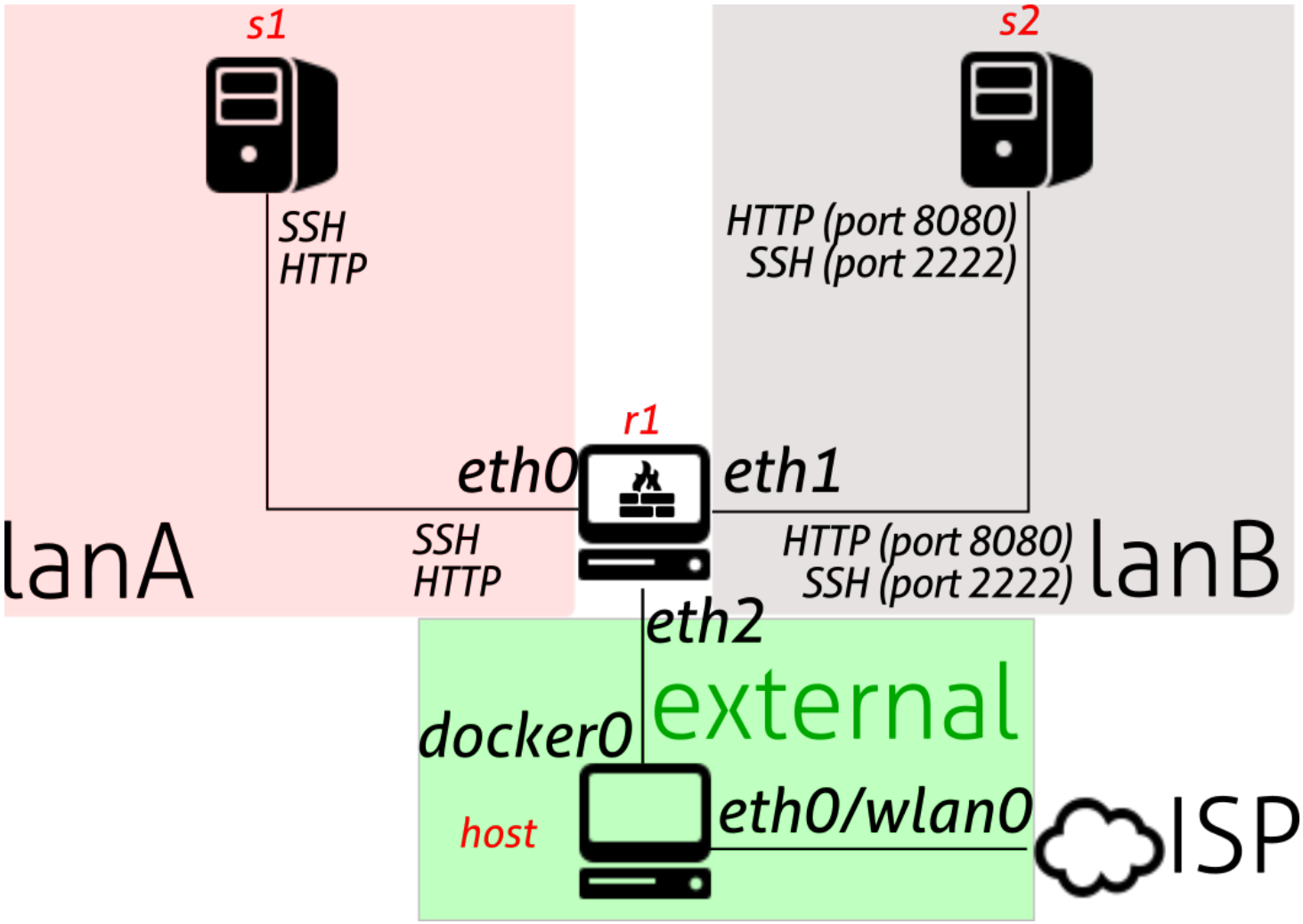
Exercise 2: pnd-labs/lab4/ex5

- Modify activity 1 so that internal servers are reachable from outside
  - http on s1
  - ssh on pc1
- Setup boundary to perform NATting with iptables
  - Destination NAT
- internal is NOT exposed



Lab activity: ex6

Exercise 3: pnd-labs/lab4/ex6
NAT with 2 networks and services

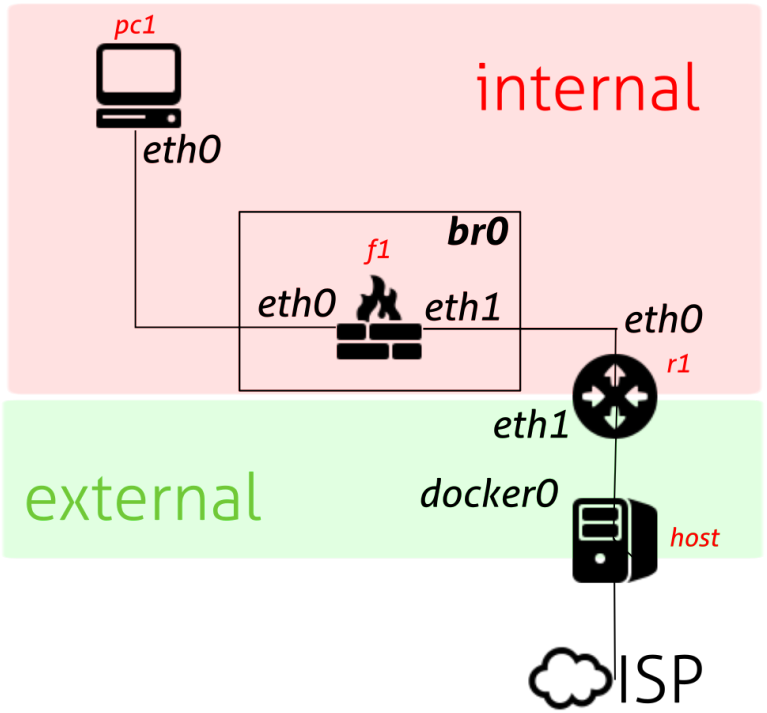


Exercise 3: policy to implement

- Unrestricted internet access from all the machines in the lanA and lanB
- Use NAT to redirect incoming traffic from WAN to the all the services
  - SSH
  - HTTP and HTTPS
- Accept ICMP echo response also for both the lans
- Respond with TCP RST or ICMP Unreachable for incoming requests for blocked ports

Lab activity: ex7

Exercise 4: pnd-labs/lab4/ex7 Transparent firewall



- The lab is ready to have f1 to act as a transparent firewall
- Try to configure it so that you can regulate the type of traffic pc1 can use towards the ISP and the host

That's all for today

- **Questions?**
- See you tomorrow
- Resources:
  - "Building internet firewalls", Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, O'Reilly 2nd ed.
    - https://docstore.mik.ua/orelly/networking_2ndEd/fire/index.htm
  - "Firewalls and Internet security: repelling the wily hacker", William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin, Addison-Wesley 2nd ed.
  - www.frozentux.net/iptables-tutorial/iptables-tutorial.html