Practical Network Defense

Master's degree in Cybersecurity 2018-19

Iptables and NAT

Angelo Spognardi

spognardi@di.uniroma1.it

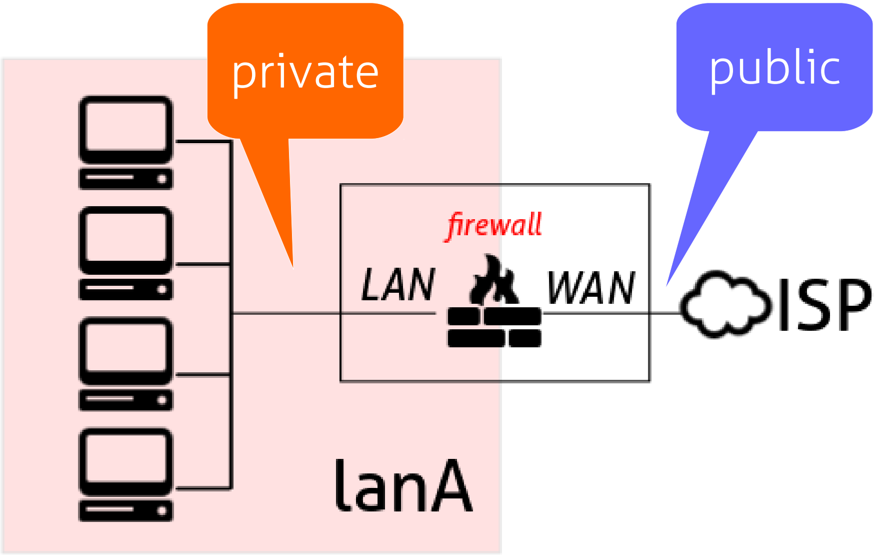
Dipartimento di Informatica

Sapienza Università di Roma

Network Address Translation (NAT)

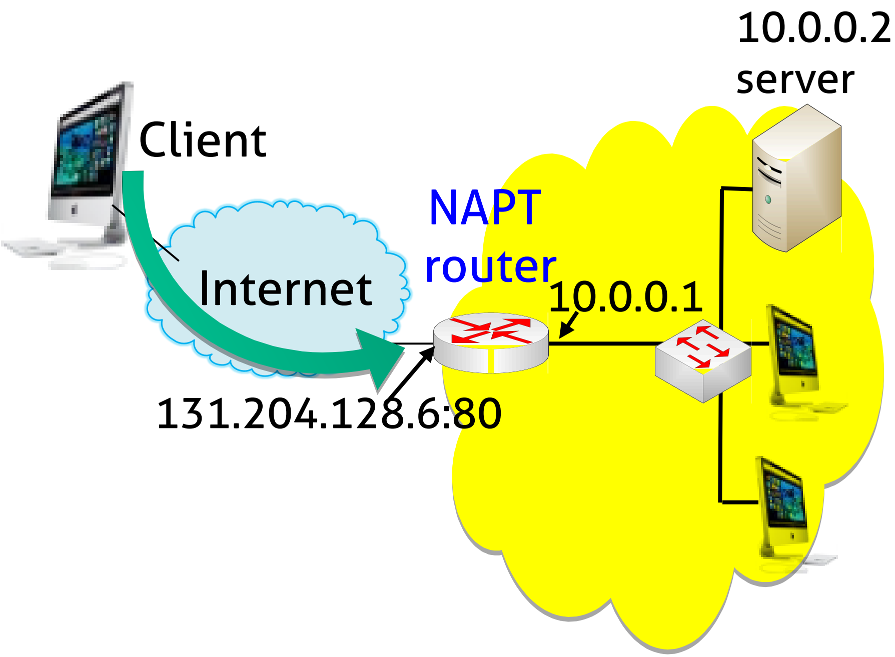
- Translate the address (f.e.: between incompatible IP addressing)
- Informally speaking, connecting to the Internet a LAN using un-routable in-house LAN addresses

- 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



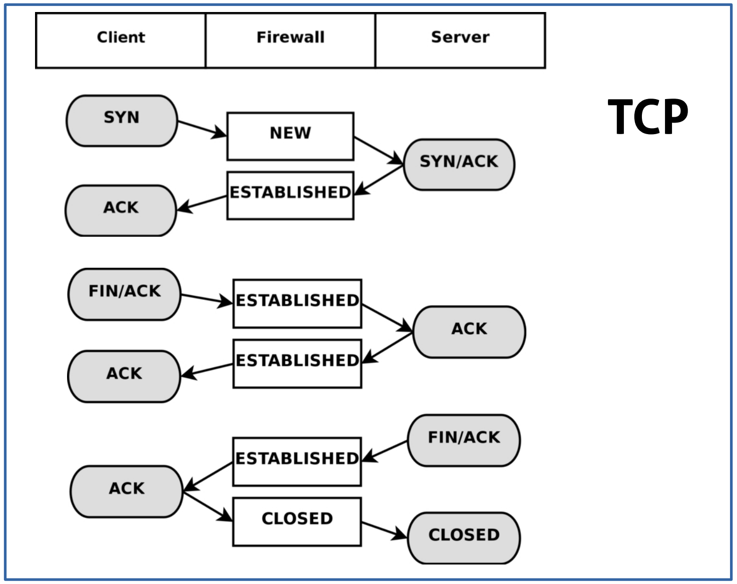
NAPT for Incoming Requests

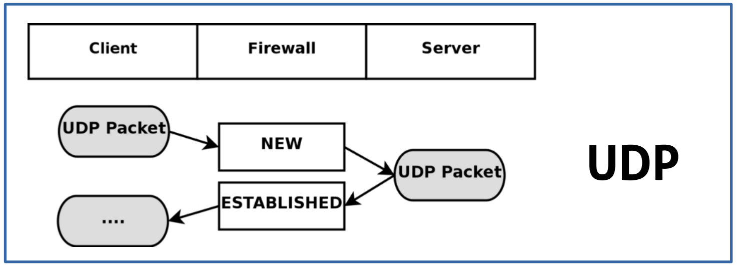
- NAPT router blocks all incoming ports by default
- Many applications have had problems with NAPT in the past in their handling of incoming requests
- Four major methods
  - Application Level Gateways (ALGs)
  - Static port forwarding
  - Universal Plug and Play (UPnP) Internet Gateway Device (IGD)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

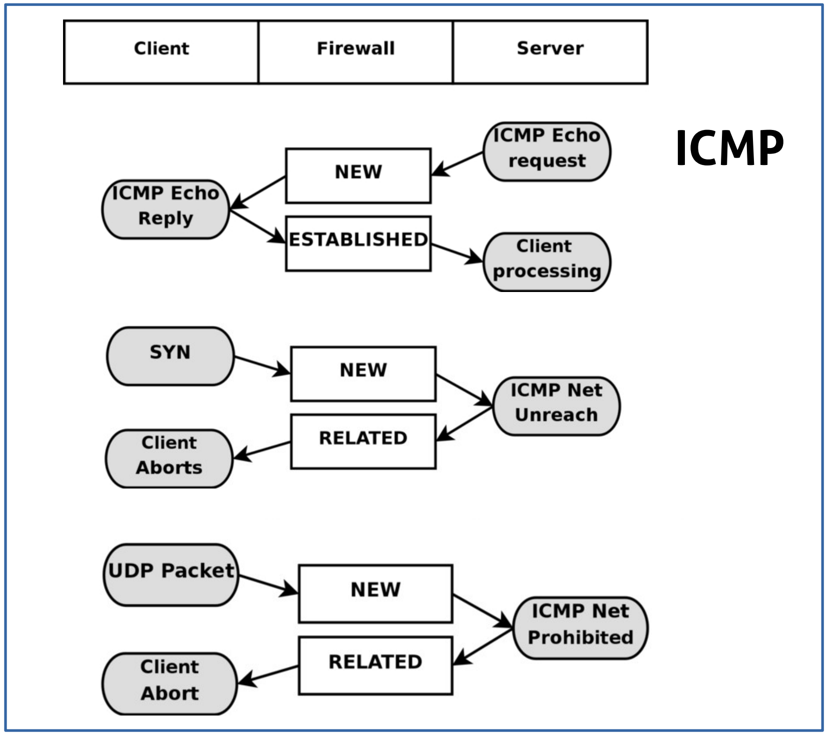


More on the conntrack module

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







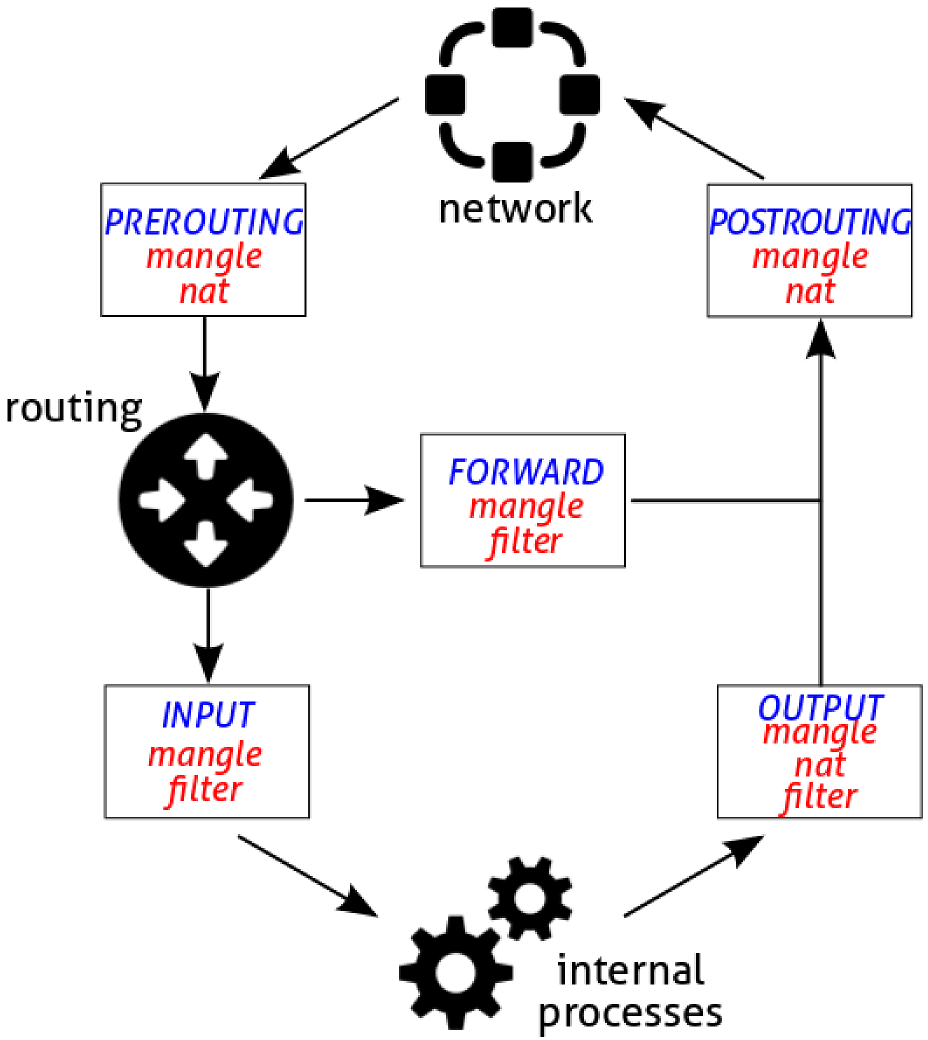
More on this:

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"
  ```

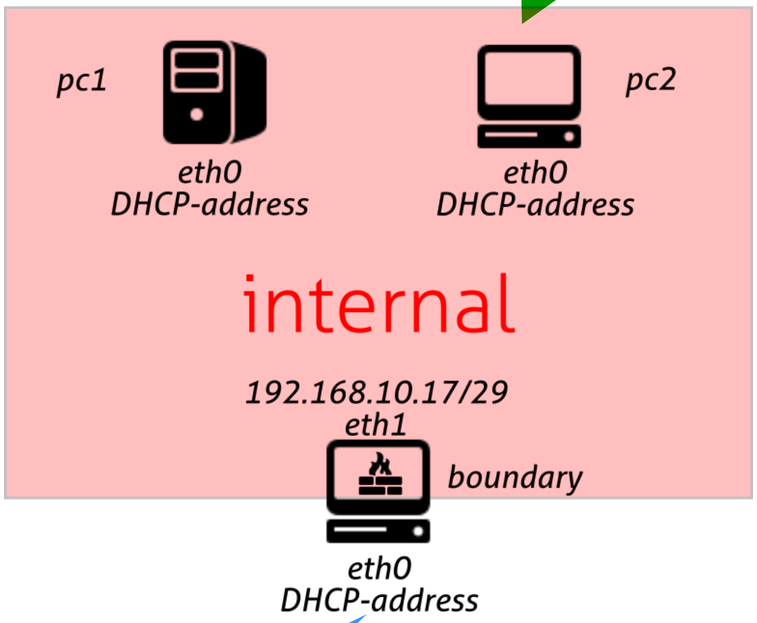
- Log and drop invalid packets

  ```
  - iptables -A INPUT -m conntrack --ctstate \
    INVALID -j LOG --log-prefix "Invalid packet"

  - iptables -A INPUT -m conntrack --ctstate \
    INVALID -j DROP
  ```

Activity 1: Source NAT

- Use the lab2-es1 topology
- Setup boundary to perform NATting with iptables
  - Masquerade to exit
- internal is NOT exposed



I can access external and my IP address is *boundary*

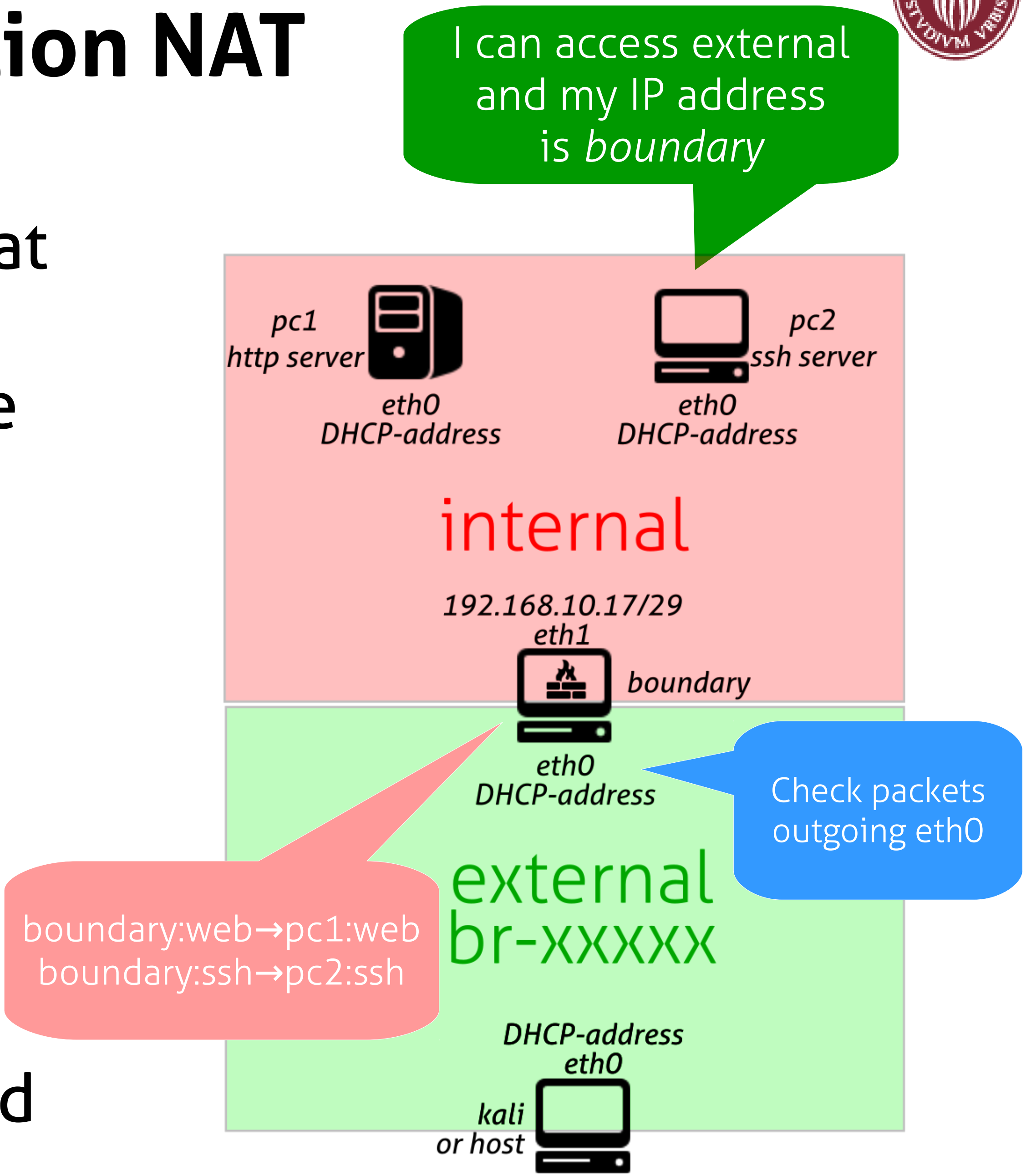
Check packets outgoing this interf.

Activity 1: Policy to protect boundary

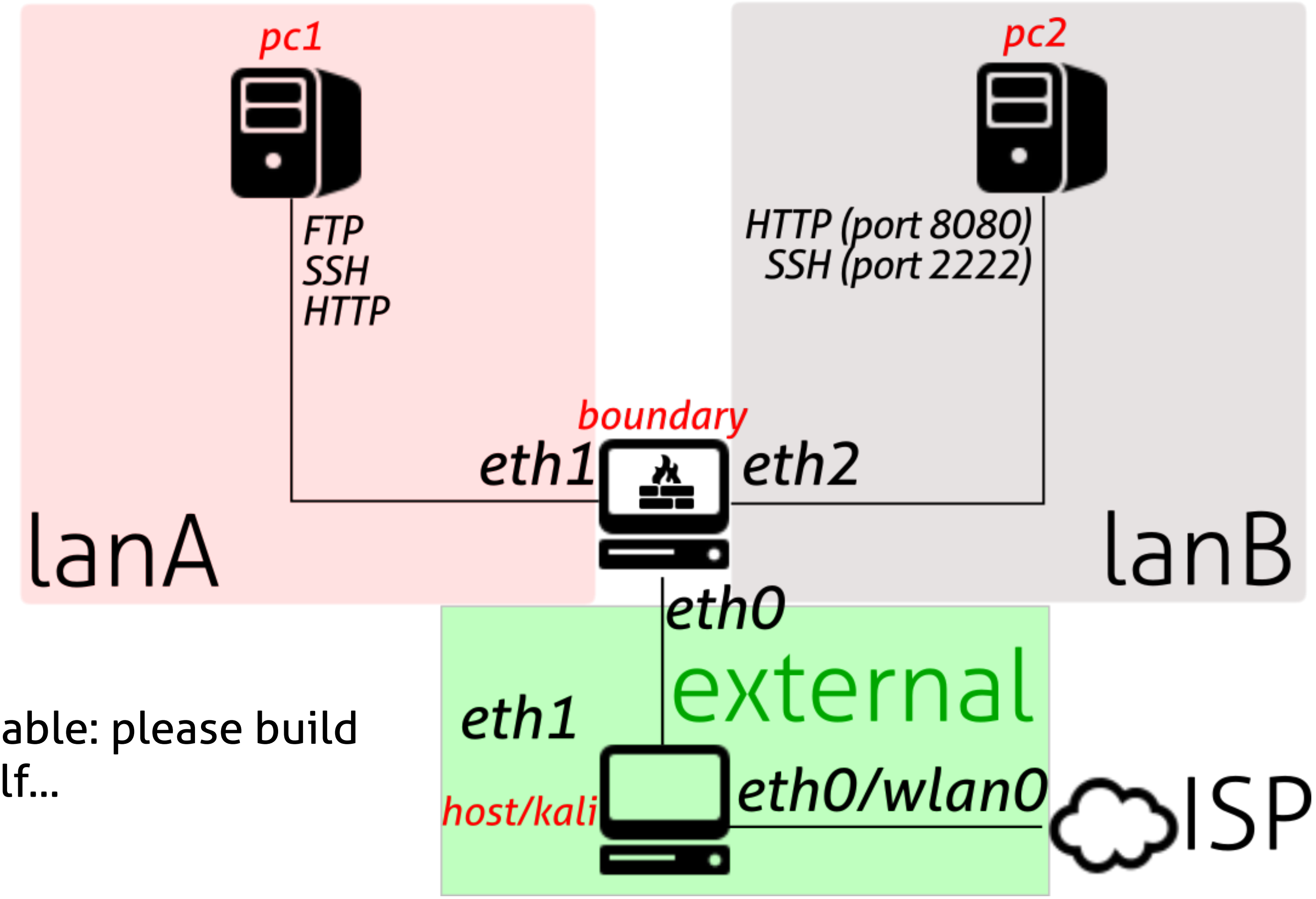
- Accept ICMP echo replies destined to LAN
- Only accept ICMP echo request
- Only allow SSH to the router
- Respond with TCP RST or ICMP Unreachable for incoming requests for blocked ports

Activity 2: Destination NAT

- Modify activity 1 so that internal servers are reachable from outside
  - Start apache on p1 and ssh on pc2
- Setup boundary to perform NATting with iptables
  - Destination NAT
- internal is NOT exposed



Activity 3 (homework if late): NAT with 2 networks and services



No lab available: please build it by yourself...

Activity 3: IP address configuration

- PC1
  - IP 10.0.1.10
  - netmask /28
  - default gateway 10.0.1.1
- PC2
  - IP 10.0.2.20
  - netmask /28
  - default gateway 10.0.2.17
- boundary eth0 (external)
  - DHCP
- boundary eth1
  - IP 10.0.1.1
  - netmask /28
- boundary eth2
  - IP 10.0.2.17
  - netmask /28
- host/kali
  - DHCP
- host/kali should be the router to ISP of boundary

Activity 3: server configuration

- On PC1
  - You can use the vsftp conf of lab3-es1
  - Start apache on port 80
  - Start ssh
- On PC2
  - Start apache on port 8080
  - Start ssh on port 2222
- On boundary
  - Start ssh

Activity 3: policy to implement

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

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
      (I don't know if it is legal… but it is there…)
  - "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