Esercitazione 7

Sommario

- Firewall
  - introduzione e classificazione
- Firewall a filtraggio di pacchetti
  - Regole
  - Ordine delle regole
- iptables

Introduzione ai firewall

Problema: sicurezza di una rete

- Necessità di proteggere reti collegate ad Internet
  - imporre restrizioni sul tipo di traffico ammesso
  - definire delle policy di sicurezza
  - filtrare il traffico entrante e uscente

Definizione di firewall

- Firewall
  - dispositivo di sicurezza utilizzato in campo informatico per accettare, bloccare o mediare il traffico dati
  - può essere hardware o software
  - è configurato secondo le policy di sicurezza dell'organizzazione in cui si trova

Classificazione dei firewall

- Si possono individuare tre categorie contraddistinte da:
  - modalità di filtraggio delle comunicazioni
    - ⇨ tra un nodo e la rete o tra reti diverse
  - modalità di gestione dei pacchetti
    - ⇨ livello ISO/OSI dello stack di protocolli
  - capacità di tenere traccia dello stato delle connessioni

Classificazione: filtraggio comunicazione

- Personal firewall
  - filtra il traffico che transita tra un singolo nodo e una rete
  - applicazione utilizzata in ambito desktop/office
    - ⇨ in esecuzione sullo stesso PC dell'utente
    - ⇨ esempi: Windows Firewall, Zone Alarm, Kerio PF
- Network firewall
  - filtra il traffico che transita tra le diverse reti che connette insieme
    - ⇨ dispositivo/computer dedicato
    - ⇨ situato al bordo di una rete (collegamento Internet)
    - ⇨ in genere indicato con il solo termine 'firewall'

Classificazione: gestione pacchetti

- Firewall a filtraggio di pacchetto (packet filtering)
  - operano a livello network/transport
    - ⇨ utilizzano gli header dei pacchetti IP/ICMP/TCP/UDP
- Gateway di applicazione (application gateway)
  - opera a livello applicazione
    - ⇨ proxy server, servizio che permette ai client di effettuare connessioni indirette ad altri servizi
  - tutti i dati sono vincolati a passare attraverso il gateway

Classificazione: stato della connessione

- Firewall stateless
  - ogni pacchetto viene trattato considerandolo singolarmente
  - semplice ma poco potente
- Firewall stateful
  - tiene traccia dello stato delle connessioni che lo attraversano
    - ⇨ flussi TCP, comunicazioni UDP
  - potente ma più complesso e lento
    - ⇨ richiede allocazione di risorse in memoria

Firewall a filtraggio dei pacchetti

Firewall a filtraggio dei pacchetti

- Funzionamento
  - accede alle intestazioni dei pacchetti
  - consulta una sequenza di regole (rule chain)
- Insieme delle regole
  - ogni regola
    - ⇨ è individuata da una serie di informazioni
  - specifica l'azione da intraprendere quando le intestazioni dei pacchetti corrispondono alle informazioni specificate
  - azioni possibili:
    - ⇨ accettare
    - ⇨ scartare

Informazioni associate alle regole

- Informazioni fondamentali utilizzate
  - indirizzo e porta mittente
  - indirizzo e porta destinatario
  - esempio

Indice	IP sorgente	IP destinatario	Azione
1	131.114.0.0/16	131.114.29.9	Blocca

- Informazioni aggiuntive
  - numero della regola (ordine)
  - tipo protocollo e stato della connessione (stateful inspection)

Interpretazione delle regole

- Il firewall
  - controlla la corrispondenza delle intestazioni alle regole impostate
  - quando una regola viene soddisfatta allora viene applicata l'azione corrispondente
  - le regole sono processate nell'ordine in cui sono inserite all'interno della catena
  - solo la prima corrispondenza ha effetto

Importanza dell'ordine delle regole (1 di 2)

- L'amministratore di una rete aziendale con indirizzo `222.22.0.0/16` desidera
  - impedire l'accesso da Internet alla rete aziendale
  - consentire l'accesso dalla rete `111.11.0.0/16` alla sottorete interna `222.22.22.0/24`
  - impedire alla singola sottorete `111.11.11.0/24` di poter accedere alla sottorete interna `222.22.22.0/24`

Importanza dell'ordine delle regole (2 di 2)

Errato!

Indice	IP sorgente	IP destinatario	Azione
1	111.11.0.0/16	222.22.22.0/24	Consenti
2	111.11.11.0/24	222.22.0.0/16	Blocca
3	0.0.0.0/0	0.0.0.0/0	Blocca

Corretto

Indice	IP sorgente	IP destinatario	Azione
1	111.11.11.0/24	222.22.0.0/16	Blocca
2	111.11.0.0/16	222.22.22.0/24	Consenti
3	0.0.0.0/0	0.0.0.0/0	Blocca

Regole default

- Caso in cui nessuna regola è soddisfatta
  - firewall inclusivo (inclusive)
    - ⇨ blocca tutto il traffico che non soddisfa le regole
    - ⇨ corrisponde ad avere come ultima regola 'blocca tutto'
    - ⇨ sicuro ma scomodo: senza definire le regole non si può accedere all'esterno
  - firewall esclusivo (exclusive)
    - ⇨ accetta tutto il traffico che non soddisfa le regole
    - ⇨ corrisponde ad avere come ultima regola 'accetta tutto'
    - ⇨ comodo ma insicuro

Netfilter/iptables

Netfilter/iptables

- Suite per la manipolazione dei pacchetti:
  - NetFilter : è parte integrante del kernel
    - ⇨ packet filtering-mangling
  - iptables (user-space) : tool di gestione del firewall
    - ⇨ comunica al kernel le regole per la gestione dei pacchetti

Feature Netfilter

- Feature principali:
  - Packet filtering stateless e stateful
  - Supporto IPv4 e IPv6
  - NAT/PAT
  - Infrastruttura flessibile ed estendibile

Moduli di Netfilter

- Netfilter ha diverse funzioni
- Possono essere abilitate caricando i rispettivi moduli con il comando `modprobe`
- Moduli:
  - iptable_filter (base)
  - iptable_tables (base)
  - iptable_nat
    - ⇨ per il PAT/NAT
  - ipt_state
    - ⇨ per discriminare i pacchetti in base allo stato della connessione

iptables: tabelle

- iptables lavora su 3 tabelle (tables) di default:
  - filter (default) - Regola il filtering: quali pacchetti accettare, quali bloccare
  - nat - Regola le attività di natting
  - mangle - Interviene sulla alterazione dei pacchetti.

iptables: catene

- Ogni tabella è formata da catene (**chains**) predefinite (INPUT, OUTPUT, ..) a cui si possono aggiungere catene custom
- Ogni catena è composta da un elenco di regole (**rules**) che identificano pacchetti di rete secondo criteri diversi

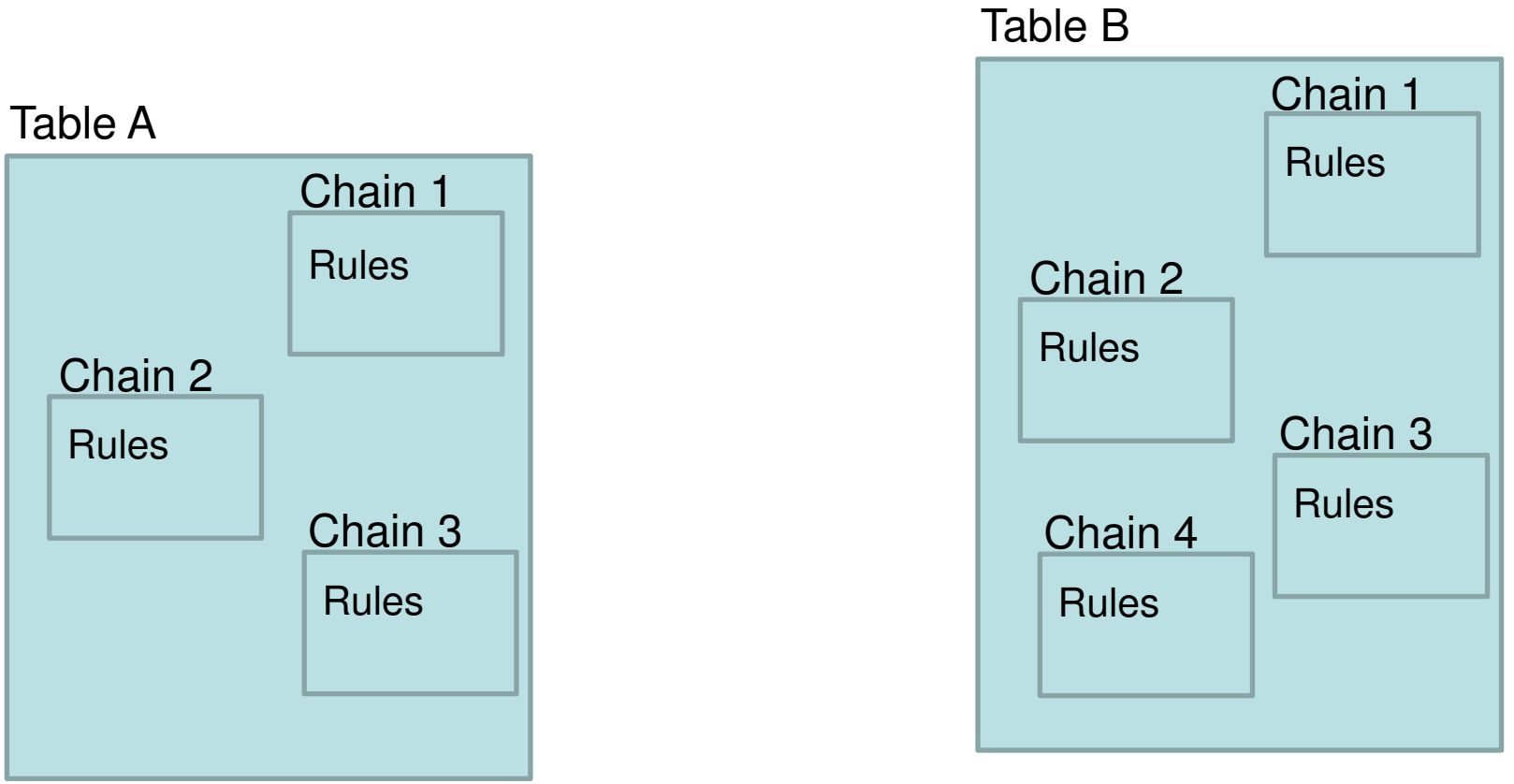
  es: -p tcp –dport 80 -d 10.0.0.45

iptables: regole

- Ogni regola termina con una indicazione (**target**) su cosa fare dei pacchetti identificati dalla regola stessa

  es: -j ACCEPT, -j DROP ...

iptables: strutture



iptables: sintassi e opzioni

- `iptables` è il comando usato per settare, modificare e cancellare regole (se non specificato ci si riferisce alla tabella filter)
  - -P : cambia la politica di una catena esistente: Esempio:
    - ⇨ iptables -P INPUT DROP

  imposta la tattica base, per i pacchetti in ingresso diretti ai processi locali (esaminati quindi dalla catena INPUT), su DROP. Cioè se non si trovano regole che corrispondono al pacchetto in esame, questo viene scartato

iptables: sintassi e opzioni

- -A : appende una regola ad una catena

  Esempio:

  ⇨ iptables -A INPUT -s 192.168.0.1 -j DROP

  aggiungi in coda alla catena input (-A INPUT) la regola per cui tutti i pacchetti con indirizzo sorgente 192.168.0.1 (-s 192.168.0.1) vengano scartati (-j DROP)

- -D: cancella una regola da una catena

  Esempio:

  ⇨ iptables -D OUTPUT 2

  cancella la regola numero 2 dalla catena di output

iptables: sintassi e opzioni

- -L: elenca le regole presenti in una catena (o in tutte le catene se non specificato)

  Esempi:

  ⇨ iptables –L

  elenca le regole delle catene principali (INPUT, OUTPUT,FORWARD)

  ⇨ iptables -L INPUT

  elenca le regole della catena INPUT

  ⇨ iptables -t nat –L

  elenca le regole presenti nelle tre chain della tabella nat

- -F : svuota le regole presenti in una catena
- -p [protocollo]: specifica un protocollo

iptables: regole permanenti

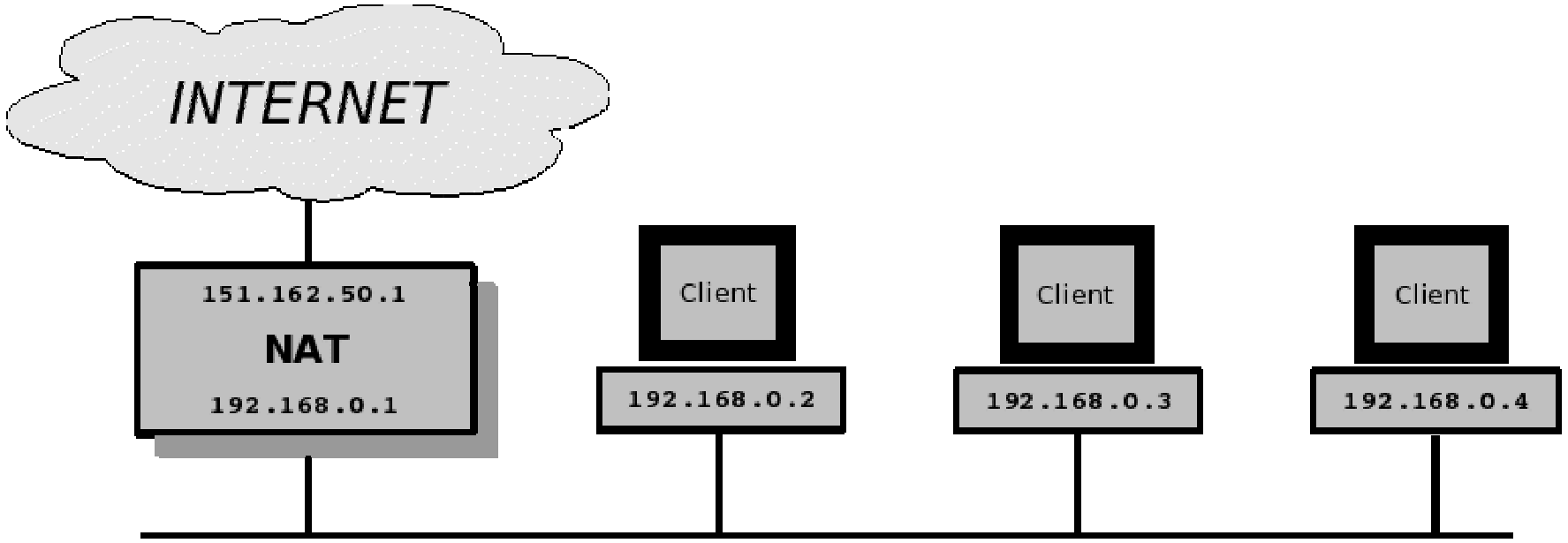
- Le regole non vengono memorizzate in modo permanente
- Al riavvio del PC è necessario reimpostarle
  - Salvare le regole:

    ⇨ `iptables-save > /etc/firew.conf`
  - Caricare le regole salvate

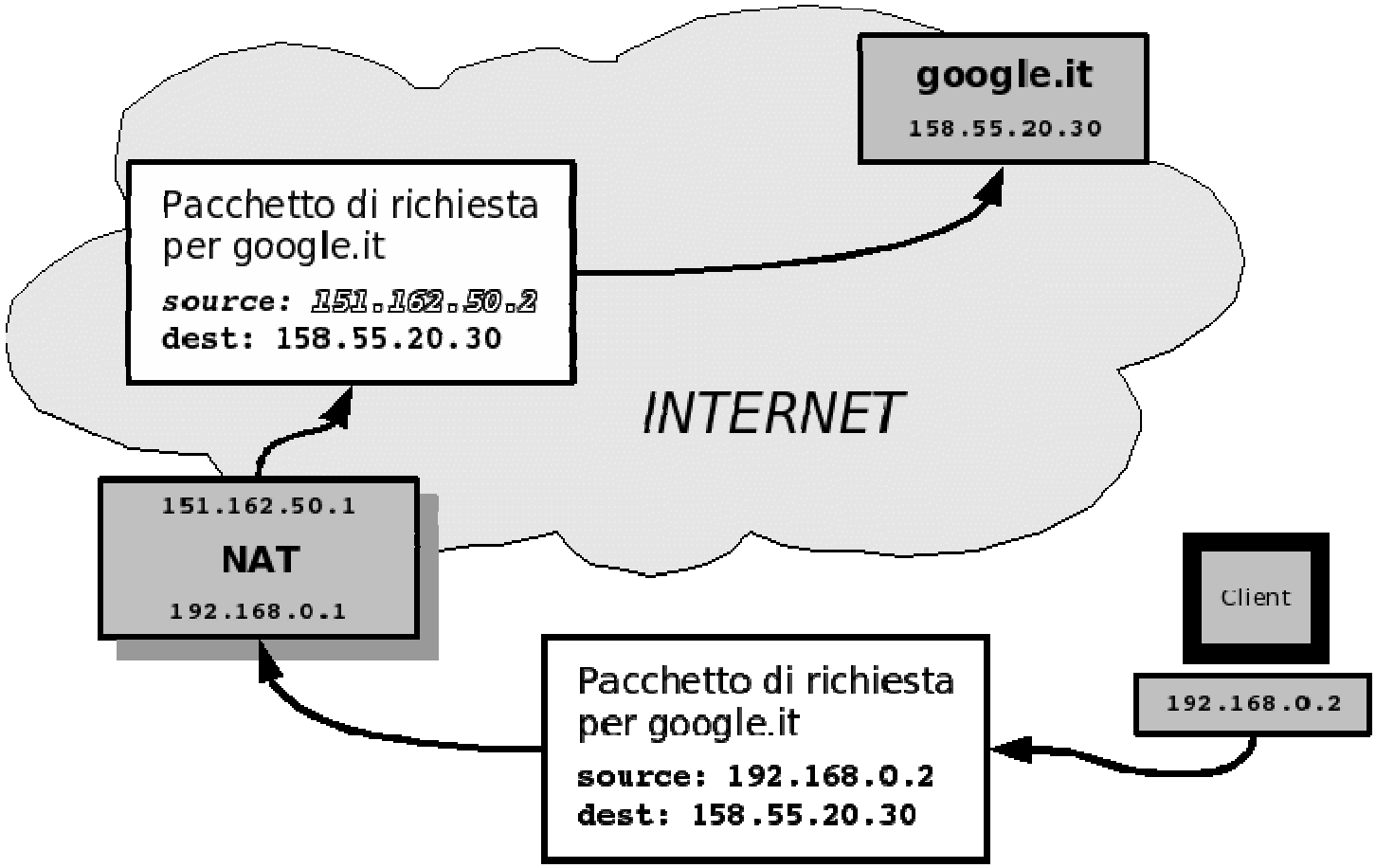
    ⇨ `iptables-restore < /etc/firew.conf`

Funzioni di iptables: NAT

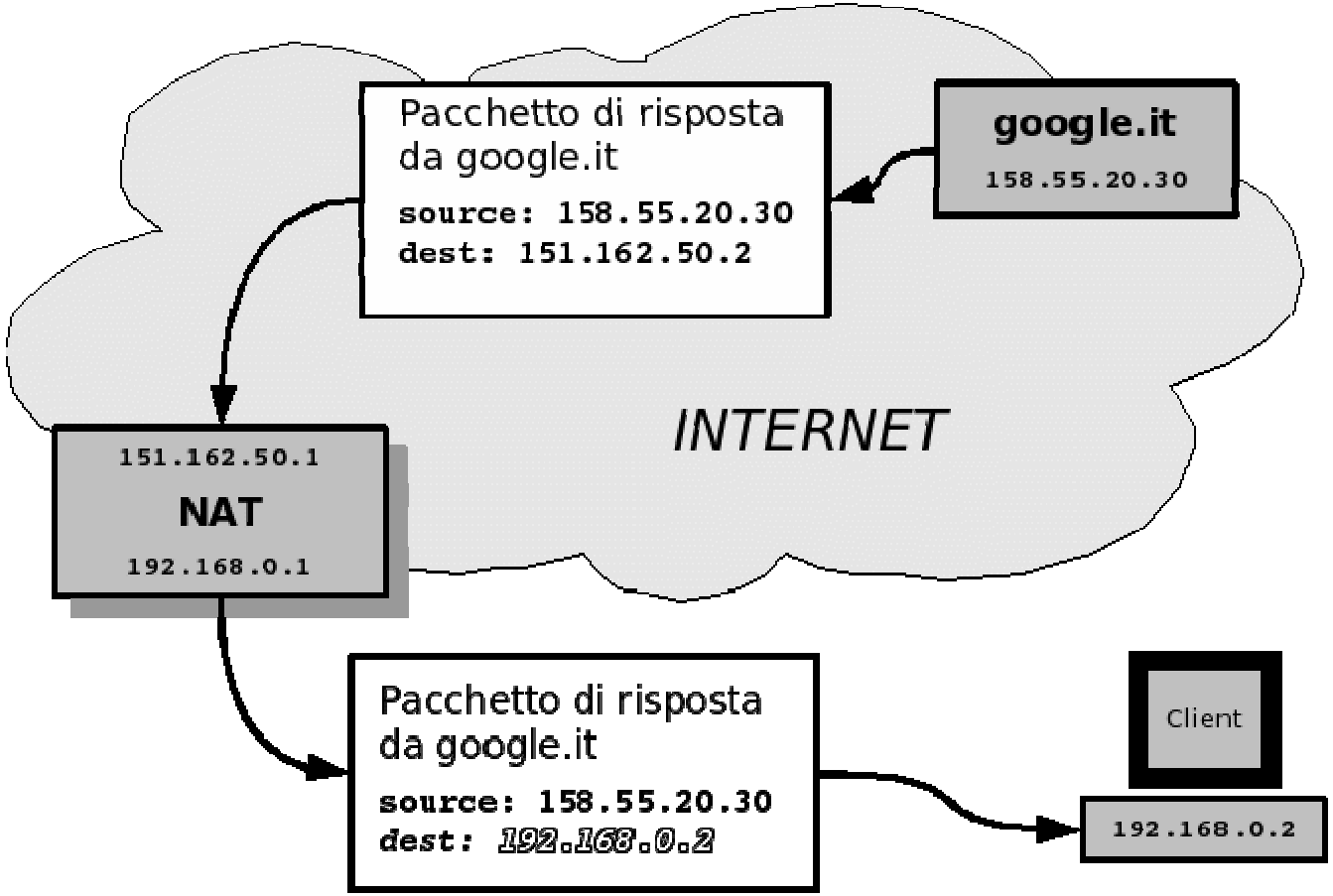
NAT: Network Address Translation



NAT: Network Address Translation



NAT: Network Address Translation



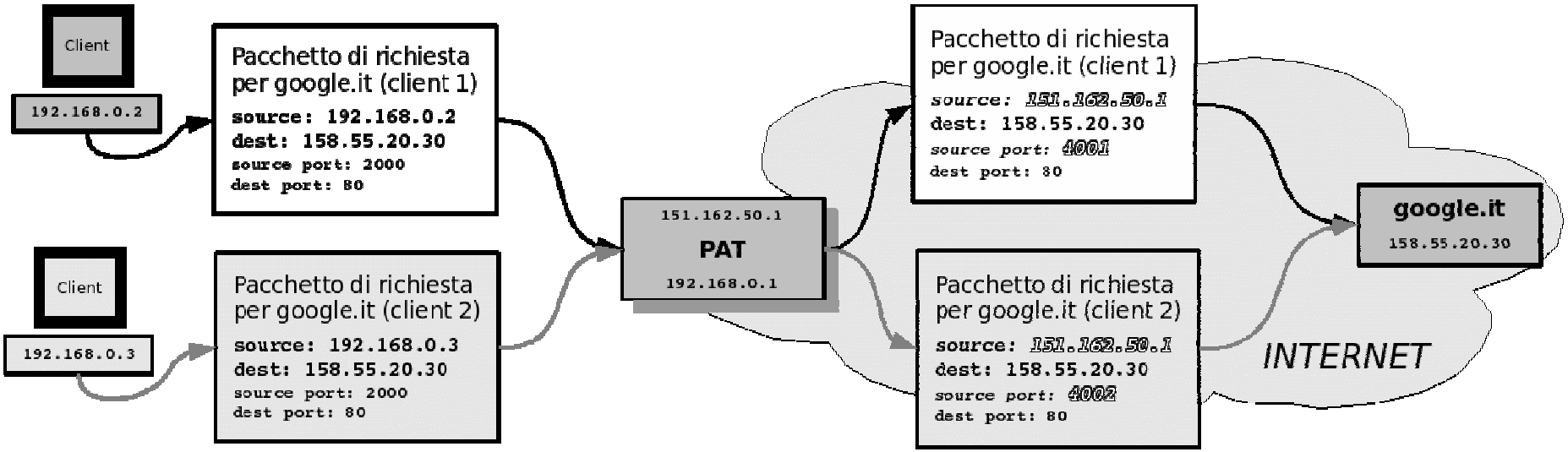
NAT: Network Address Translation

- Generalizzando, il NAT farà conversioni secondo le seguenti tabelle:

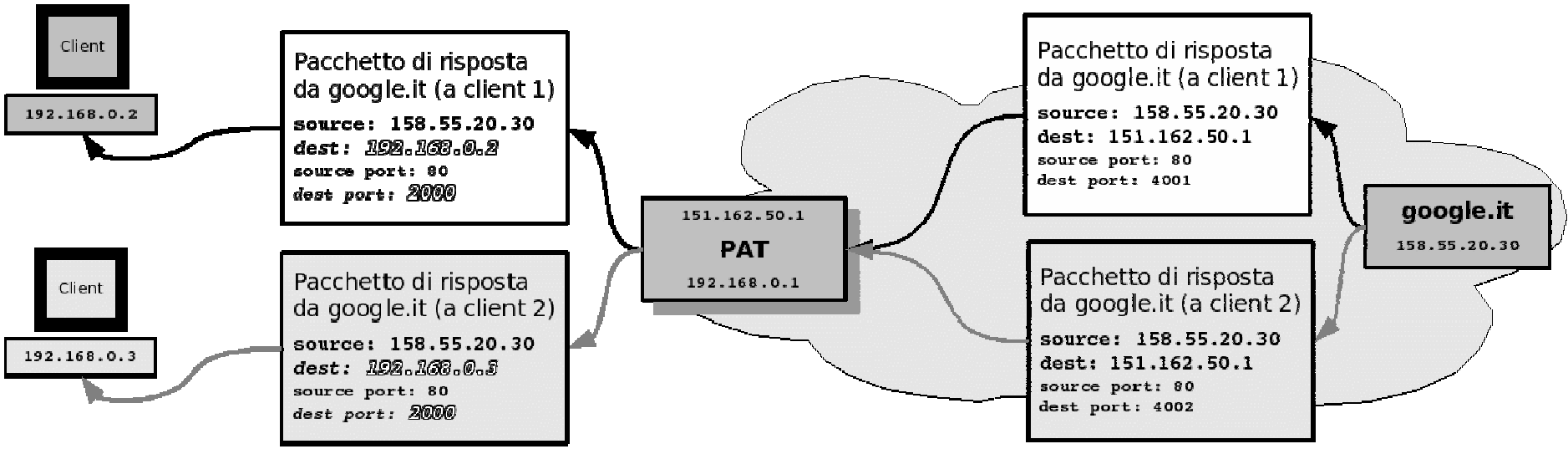
192.168.0.2 –> 151.162.50.2
192.168.0.3 –> 151.162.50.3
192.168.0.4 –> 151.162.50.4

151.162.50.2 –> 192.168.0.2
151.162.50.3 –> 192.168.0.3
151.162.50.4 –> 192.168.0.4

PAT: Port Address Translation

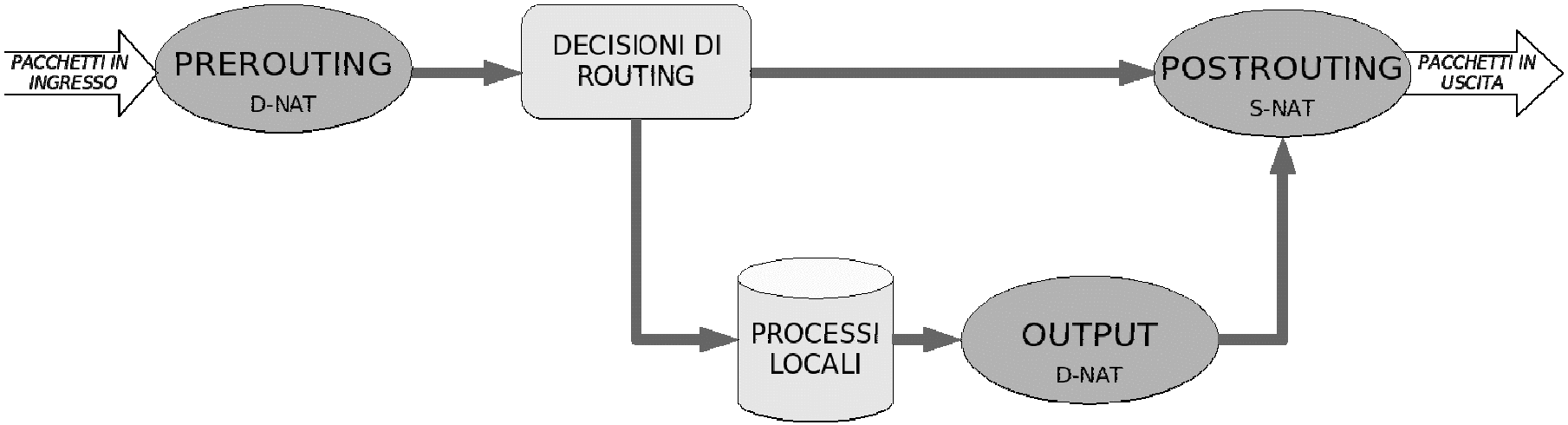


PAT: Port Address Translation



NAT/PAT: iptables

- `iptables` **ha una tabella apposita per gestire le regole per il NAT/PAT. Per modificare tali regole bisogna usare l'opzione** `-t nat`
- **La tabella è formata da 3 chains: PREROUTING, POSTROUTING ed OUTPUT**



NAT: PREROUTING

- I pacchetti in ingresso vengono sottoposti alla catena di PREROUTING appena vengono ricevuti
- In questa chain avviene il DNAT (Destination NAT), cioè la variazione dell'indirizzo destinazione del pacchetto
- L'operazione viene eseguita prima che venga presa una decisione sul routing e sul filtraggio

NAT: POSTROUTING

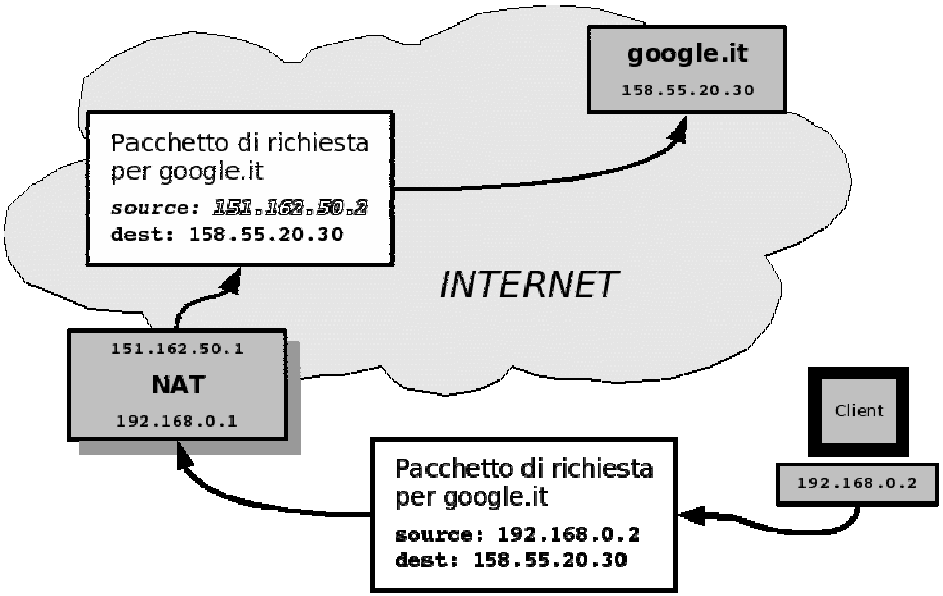
- I pacchetti in uscita passano per la catena di POSTROUTING appena prima di essere inviati sulla rete
- In questa chain avviene il SNAT (Source NAT), cioè la variazione dell'indirizzo sorgente del pacchetto
- L'operazione viene eseguita dopo che venga presa una decisione sul routing e sul filtraggio

NAT: OUTPUT

- I pacchetti generati localmente passano per la catena di OUTPUT prima di passare per quella di POSTROUTING

NAT semplice in pratica (uscita)

- Modifica dell'indirizzo sorgente dei pacchetti ricevuti dagli host interni

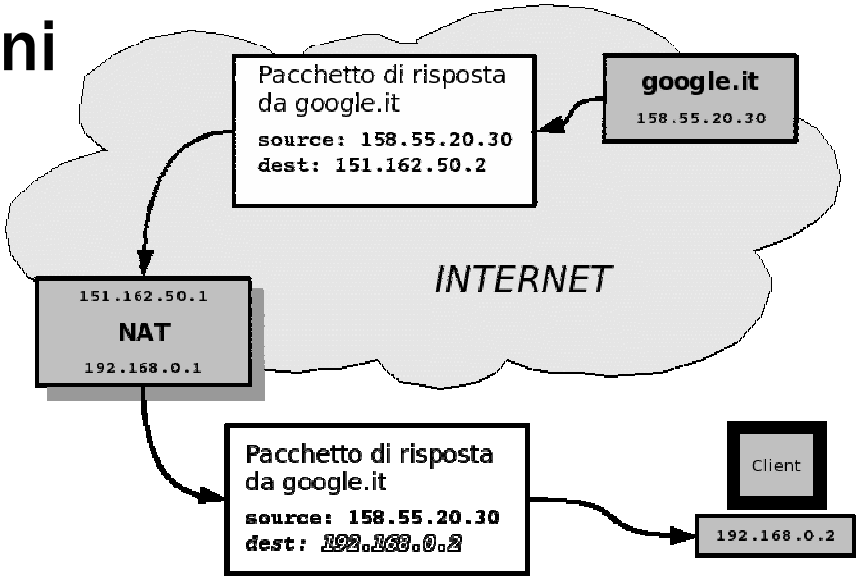


- `iptables -t nat -A POSTROUTING -s 192.168.0.2 -j SNAT --to-source 151.162.50.2`

(Va ripetuto per tutti gli host)

NAT semplice in pratica (entrata)

- **Modifica dell'indirizzo destinazione dei pacchetti ricevuti dagli host esterni**

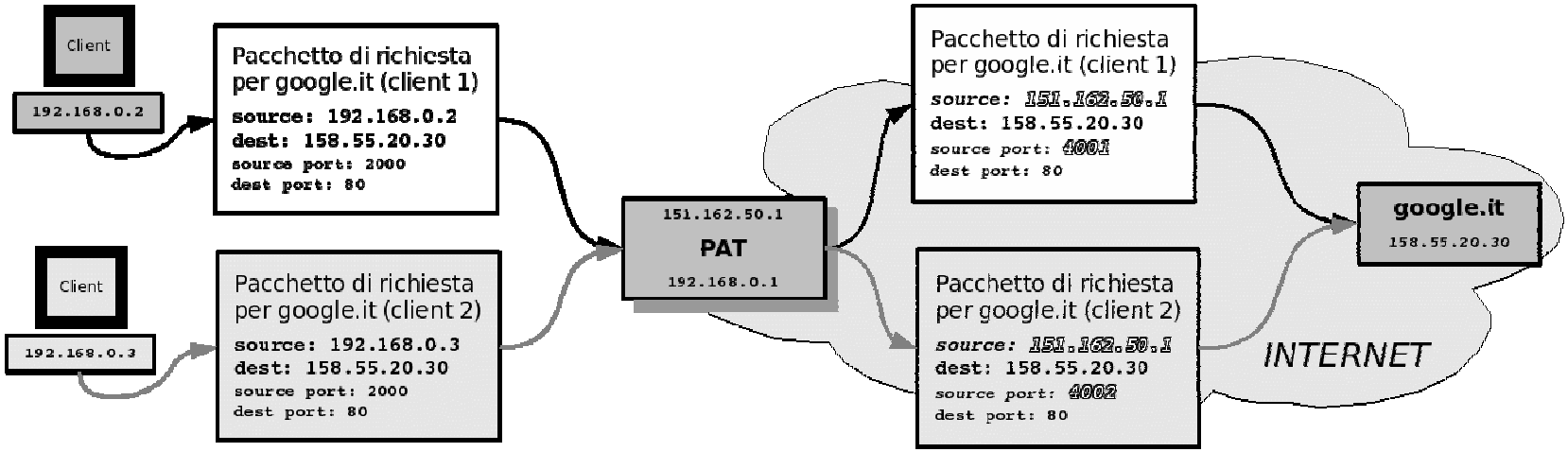


- `iptables -t nat -A PREROUTING -d 151.162.50.2 -j DNAT --to 192.168.0.2`

(Va ripetuto per tutti gli host)

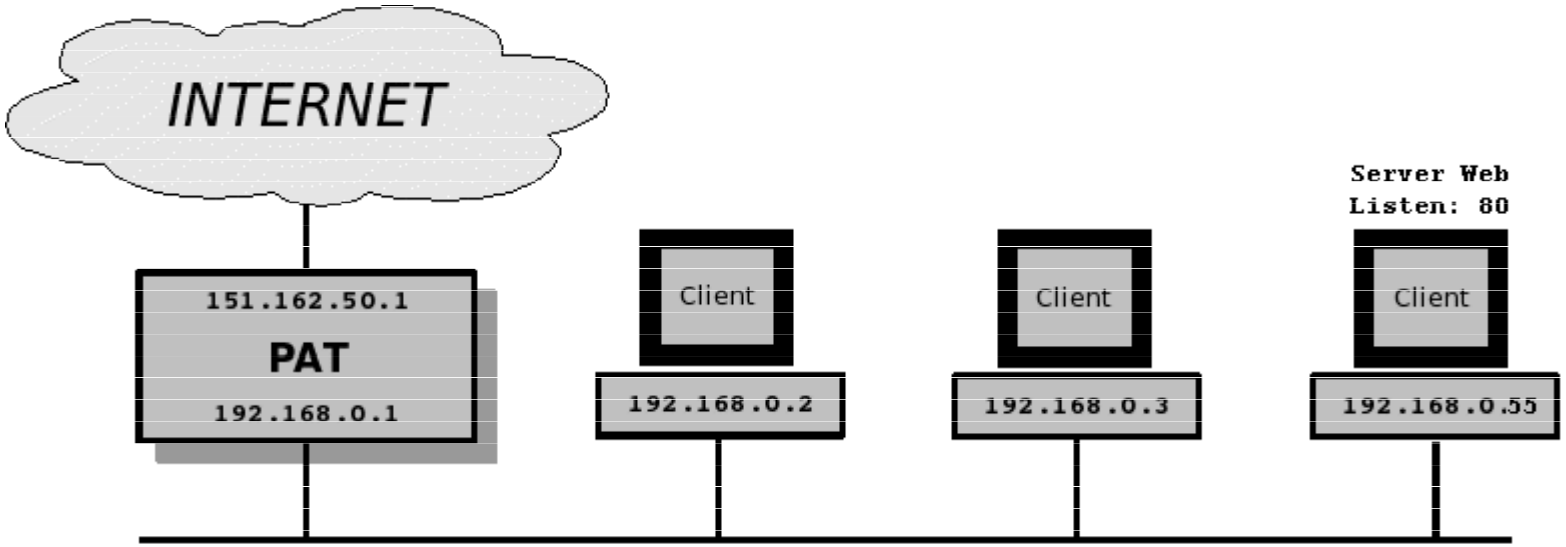
PAT in pratica

- Modifica dell'indirizzo sorgente dei pacchetti ricevuti dagli host interni



- `iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -j SNAT --to-source 151.162.50.1`

Problema della redirezione

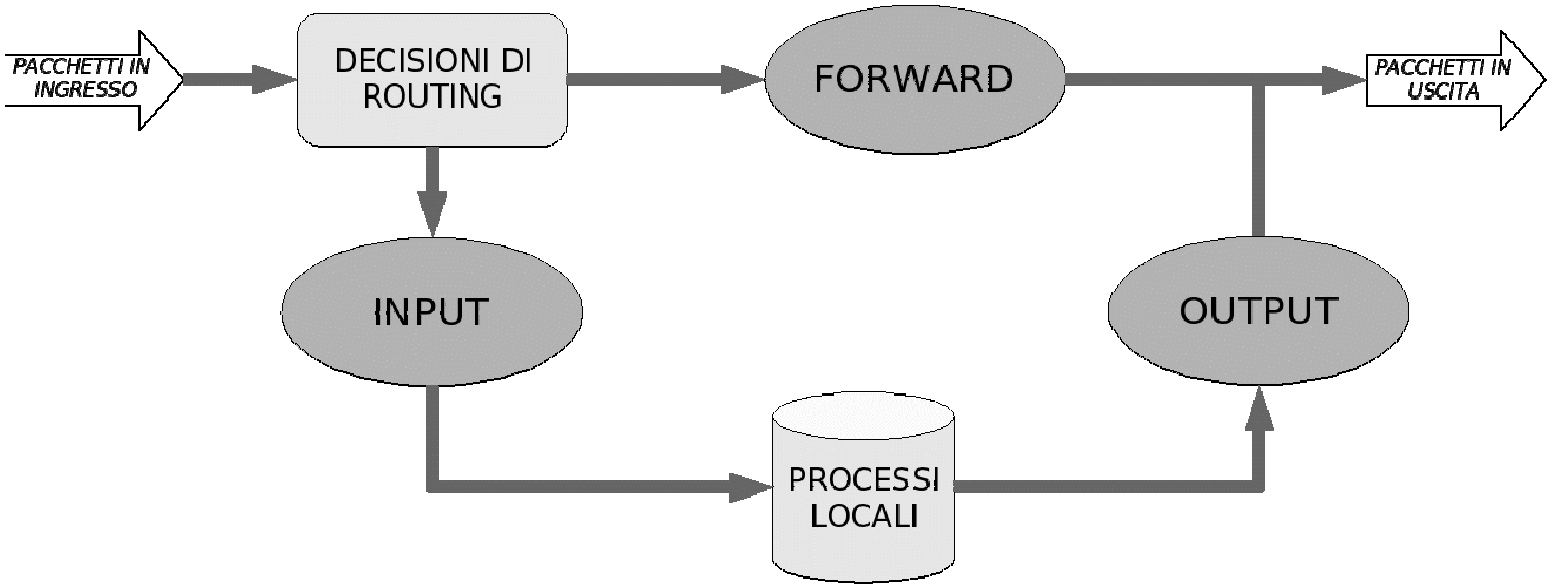


- **Server web all'interno della rete 192.168.0.55:80**
  - `iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to 192.168.0.55:80`

Funzioni di iptables: firewall

Firewall: iptables

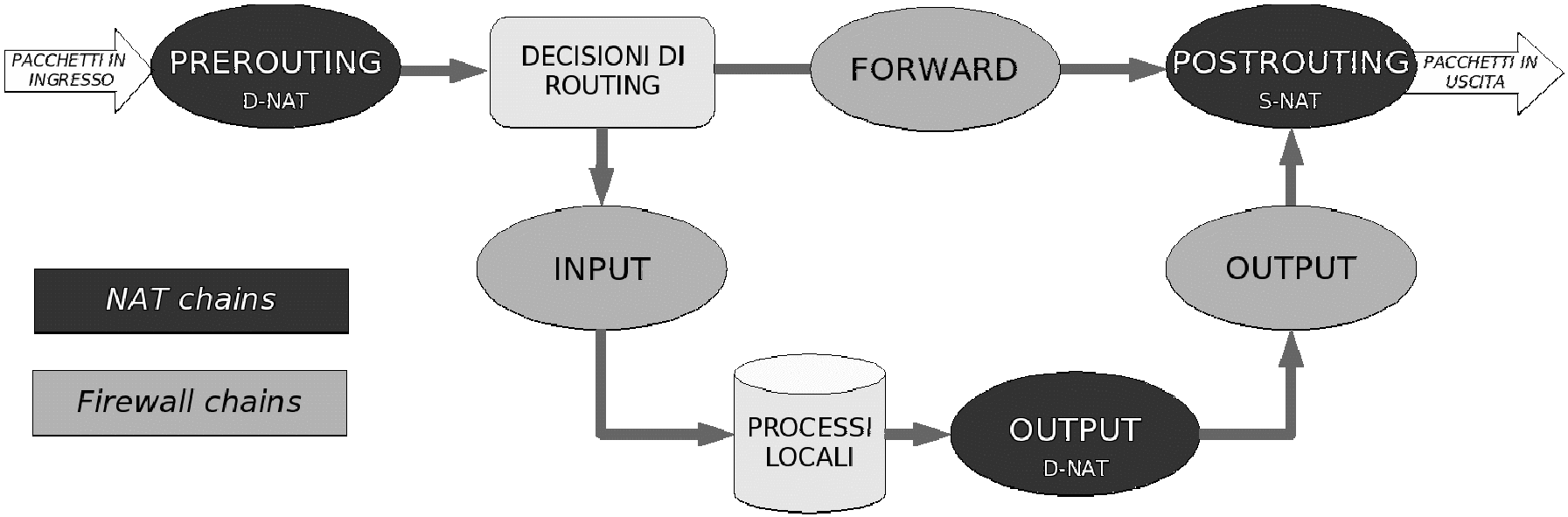
- `iptables` ha una tabella apposita per gestire il filtraggio dei pacchetti (filter). È la tabella sulla quale si lavora se non si specifica nulla attraverso `-t`
- La tabella è formate da 3 chains: INPUT, OUTPUT e FORWARD



Firewall: chains

- I pacchetti in ingresso diretti ai processi della macchina stessa, vengono sottoposti alla catena INPUT
- Quelli in uscita (sempre generati dalla macchina in esame) vengono sottoposti alla catena OUTPUT
- Tutti gli altri pacchetti, cioè quelli in transito sulla macchina che li instrada, vengono analizzati dalle regole della lista FORWARD.

Integrazione di firewall e NAT



- Il firewall e il NAT sono strutturati per funzionare perfettamente insieme
- Le catene del NAT sono disposte in modo che il firewall veda i pacchetti con le destinazioni reali

Firewall in pratica

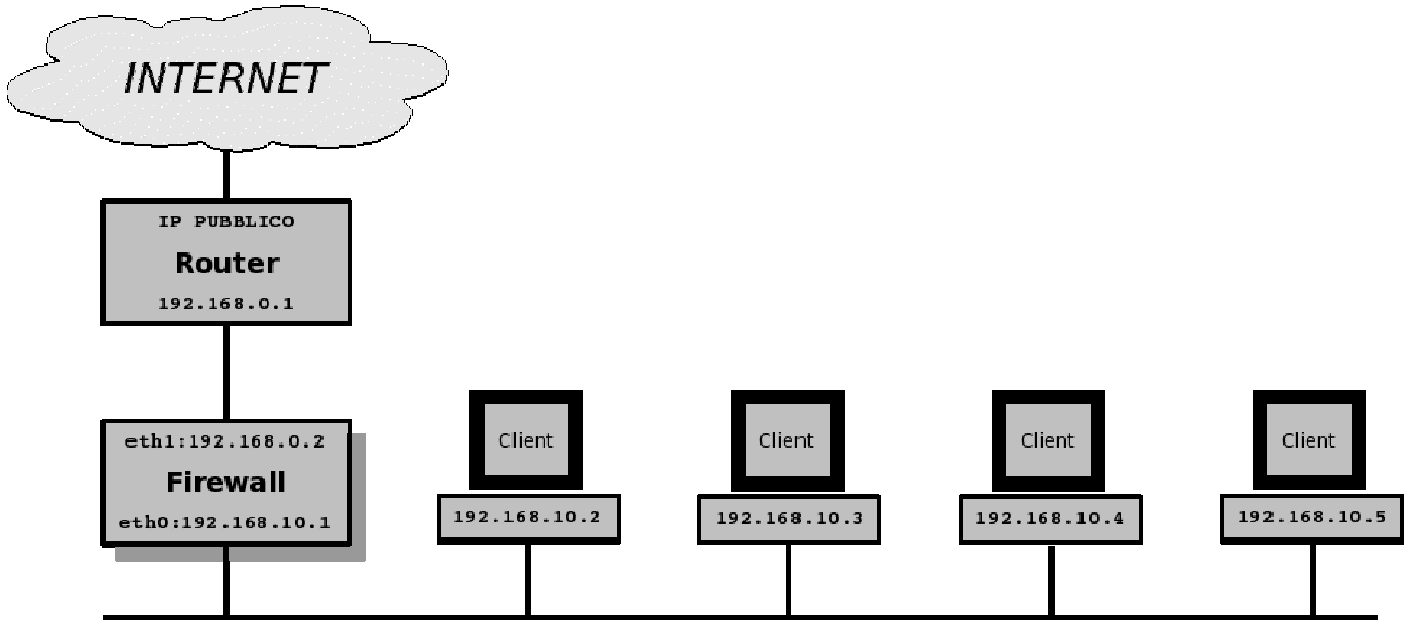


Tabella di routing del firewall

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.10.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
0.0.0.0         192.168.0.1     0.0.0.0         UG    1      0        0 eth1
```

Firewall: regole preliminari

- Il firewall esegue il PAT:
  - ⇨ `iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -j SNAT --to-source 192.168.0.2`
- Di default scartiamo tutto:

  iptables -P INPUT DROP

  iptables -P OUTPUT DROP

  iptables -P FORWARD DROP

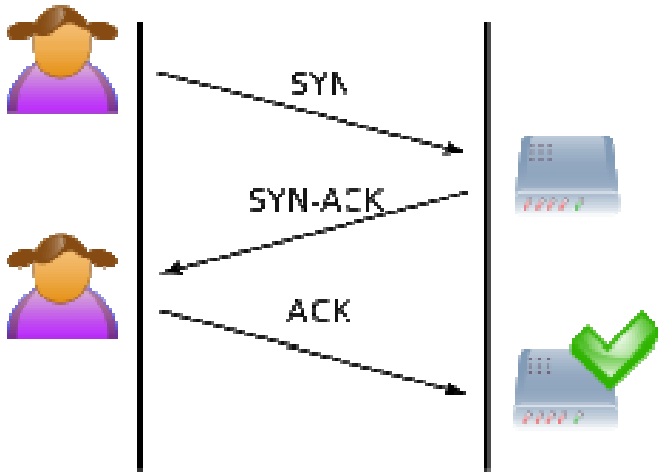
Firewall: regola (1)

- **Vogliamo che la macchina firewall sia accessibile attraverso** `ssh` **dal computer dell' amministratore (192.168.10.5)**
  - `iptables -A INPUT -p tcp -i eth0 -s 192.168.10.5 -d 192.168.10.1 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT`
  - `iptables -A OUTPUT -p tcp -o eth0 -s 192.168.10.1 -d 192.168.10.5 --sport 22 -m state --state ESTABLISHED -j ACCEPT`

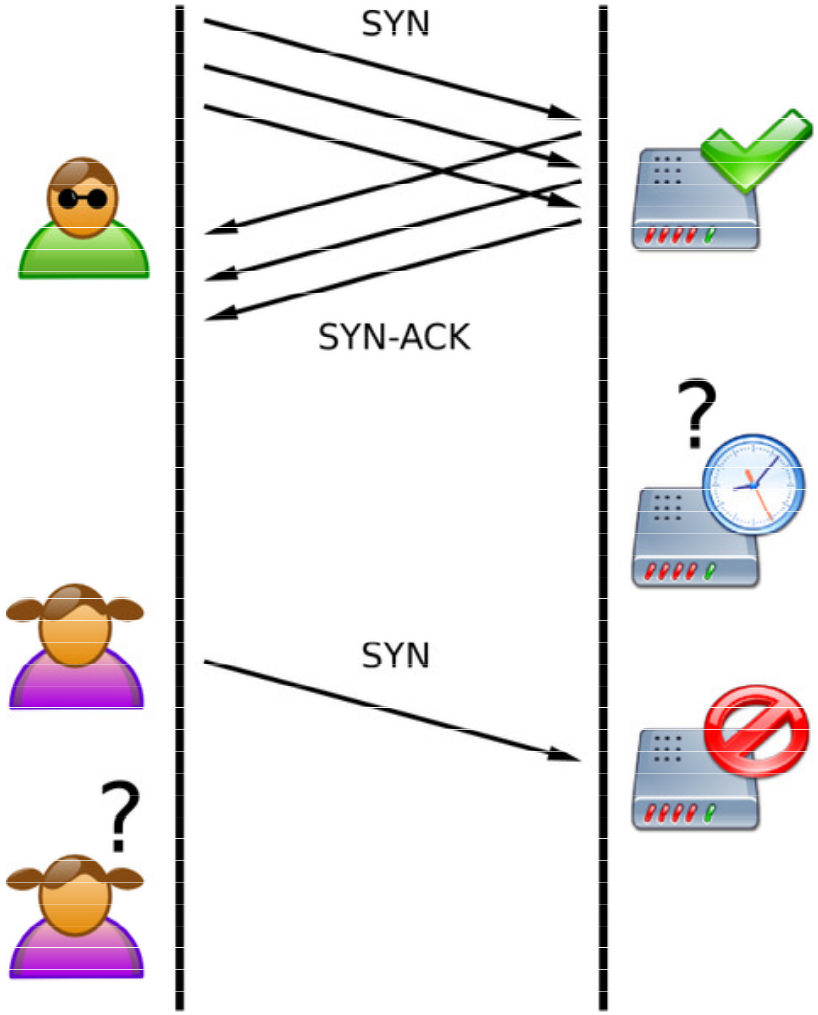
Firewall: regola (2)

- Vogliamo bloccare ogni tentativo di connessione verso i computer interni ma vogliamo permettere connessioni in uscita
  - `iptables -A FORWARD -s 192.168.10.0/24 -i eth0 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT`
  - `iptables -A FORWARD -d 192.168.10.0/24 -i eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT`

Firewall: attacco SYN flood



Firewall: attacco SYN flood



Firewall: protezione dall'attacco

- `iptables -I INPUT -p tcp --syn -m limit --limit 1/s -j ACCEPT`

  - **Aggiungi la regola all'inizio della catena INPUT (-I INPUT) per cui si accettano (-j ACCEPT) connessioni TCP (-p tcp) con il SYN flag settato (–syn) una volta al secondo (-m limit –limit 1/s)**