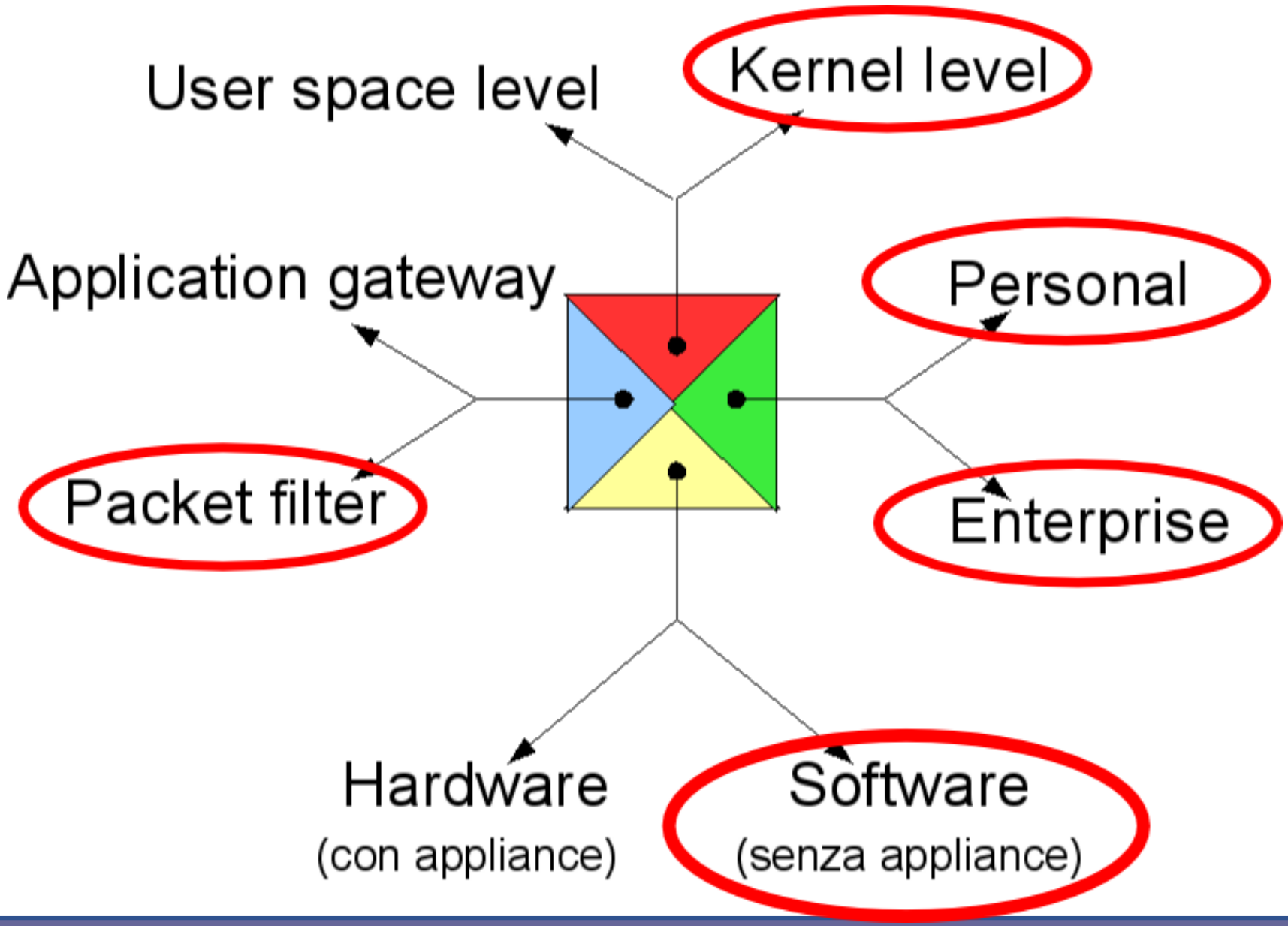
PARTE 8

Elementi di Sicurezza Informatica per reti di calcolatori

Modulo 3 – iptables

IPtables - Classificazione



IPtables

- **Iptables è un software per implementare funzionalità di Packet Filtering (sia statico che dinamico), di Inspection, di NAT e di marking dei pacchetti.**
- **Presente in tuttte le maggiori distribuzioni Linux a partire dal Kernel 2.4**
- **È il successore di IPchains (Kernel 2.2.x).**

- **Grazie alle caratteristiche di Stateful Firewall, permette di bloccare/rilevare molte scansioni “stealth” e di contrastare diversi attacchi DoS.**

IPtables

- **Il Kernel Linux, il modulo del Kernel Netfilter, ed il software applicativo IPtables sono tutti software Open Source, scaricabili, uilizzabili e modificabili liberamente.**

- **IPtables e Netfilter consentono di realizzare un firewall (eventualmente con funzioni di routing) senza costi di licenza per il software ed utilizzando dispositivi hardware standard, economici e facilmente reperibili.**

Netfilter - Installazione

- **Netfilter è un modulo del Kernel di Linux, pertanto deve essere opportunamente selezionato al momento della configurazione del Kernel (prima della compilazione)**

- **In tutte le maggiori distribuzioni di Linux, il kernel contiene già tutti i componenti di Netfilter (tipicamente come moduli), pertanto non sono necessarie ricompilazioni**

IPtables - Installazione

- **L'applicazione IPtables è installata di default in tutte le maggiori distribuzioni di Linux**

- **Qualora non fosse presente, può essere facilmente installata utilizzando i pacchetti binari, previsti per tutte le maggiori distribuzioni. Può inoltre essere installato a partire dai sorgenti.**

- **Sorgenti reperibili all' URL**
- **http://ftp.netfilter.org/pub/iptables/**

IPtables - Netfilter

- **IPtables consente la realizzazione di regole per filtrare i pacchetti.**
- **Lo stack TCP/IP è gestito dal sistema operativo, quindi Iptables deve potersi interfacciare con il Kernel Linux.**

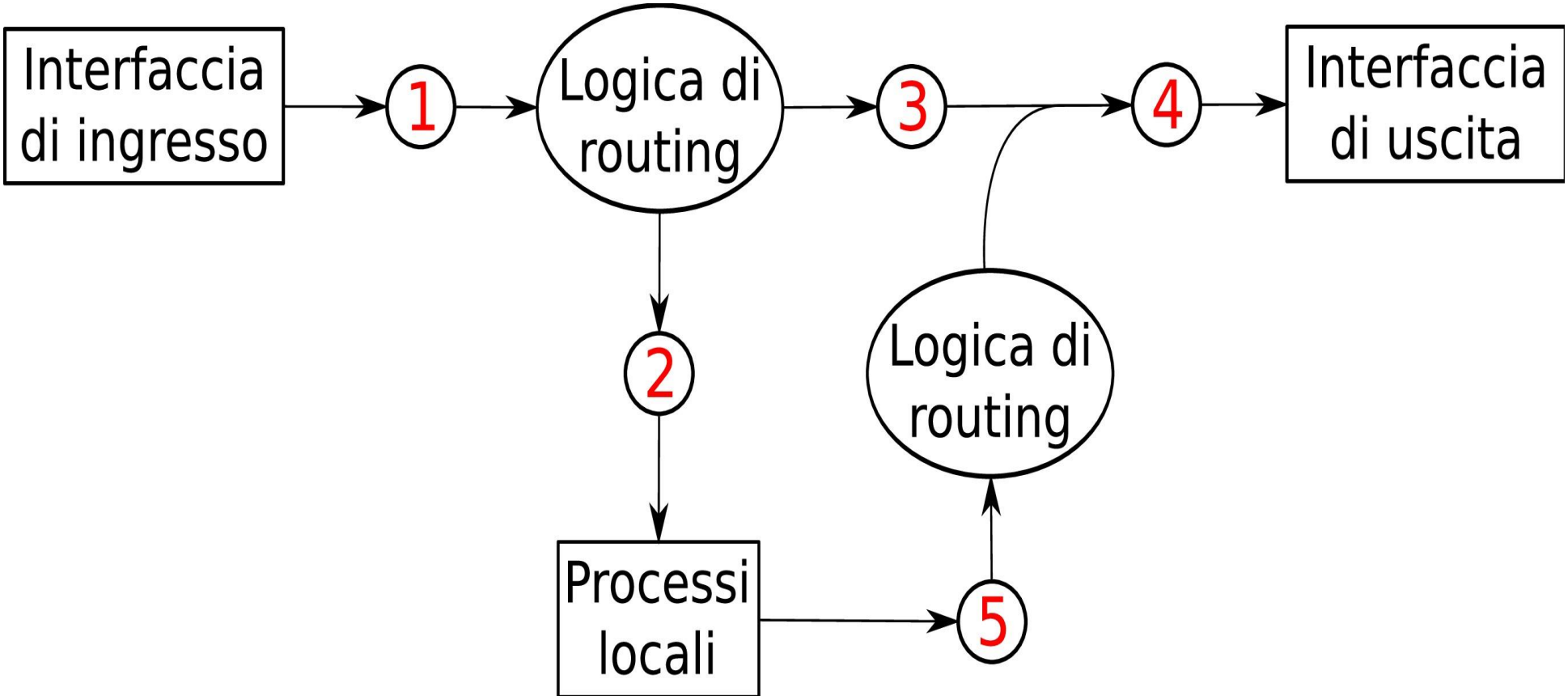
- **Per interfacciarsi con il Kernel Linux, IPtables sfrutta il modulo Netfilter.**
- **Tale modulo opera fornendo agganci (hooks) al sistema operativo utilizzabili per intercettare i pacchetti in transito.**

IPtables - Netfilter

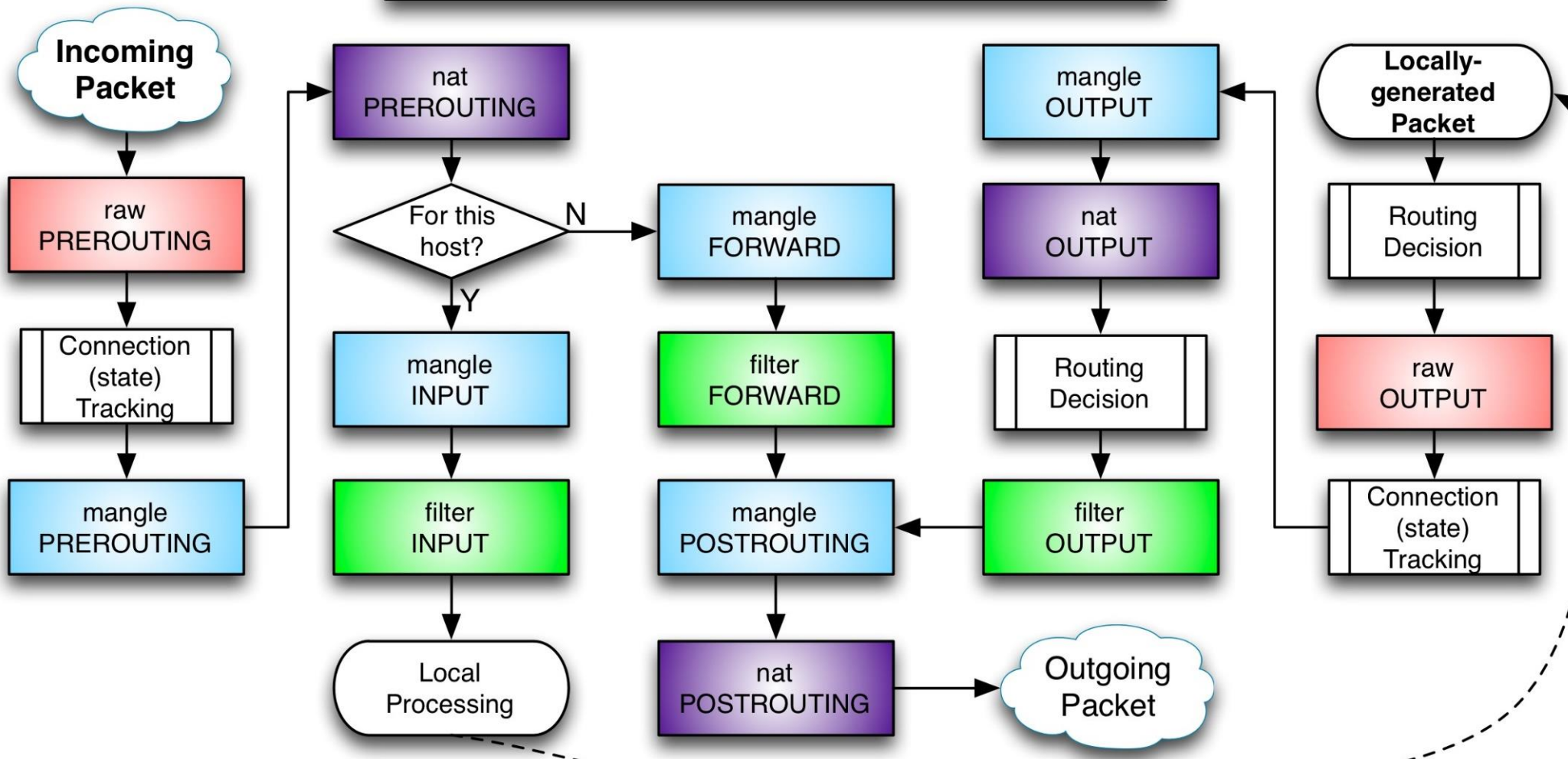
- **Le regole definite con IPtables permettono di implementare delle funzioni di gestione, associate ad un determinato hook.**

- **Ogni volta che un pacchetto attraversa un hook, Netfilter controlla se a quel determinato punto è stata assegnata una funzione di gestione.**
- **Se sì il pacchetto viene passato alla funzione. Se no il pacchetto passa all'hook successivo.**

IPtables - Netfilter



iptables Process Flow



Created by Phil Hagen (ver 2014-09-25)
for SANS FOR572: Advanced Network Forensics and Analysis
See http://sans.org/for572 for more information

Derived from : http://www.iptables.info/en/structure-of-iptables.html

IPtables - Netfilter

- **(1)NF_IP_PREROUTING: è raggiunto dai pacchetti in ingresso attraverso una interfaccia di rete, e prima di essere sottoposti a routing (hook per DNAT)**
- **(2) NF_IP_LOCAL_IN: è raggiunto solo dai pacchetti diretti alla macchina locale**
- **(3) NF_IP_FORWARD: è raggiunto solo dai pacchetti provenienti da una interfaccia di rete e diretti verso un'altra interfaccia (pacchetti in transito)**
- **(4) NF_IP_POSTROUTING: è raggiunto dai pacchetti già sottoposti a routing e che stanno per uscire dalla macchina locale (hook per SNAT)**
- **(5) NF_IP_LOCAL_OUT: è attraversato dai pacchetti generati localmente prima di essere sottoposti alla logica di routing**

- **Ogni volta che un pacchetto raggiunge un hook deve essere possibile informare il sistema sulle azioni da intraprendere.**

IPtables - Netfilter

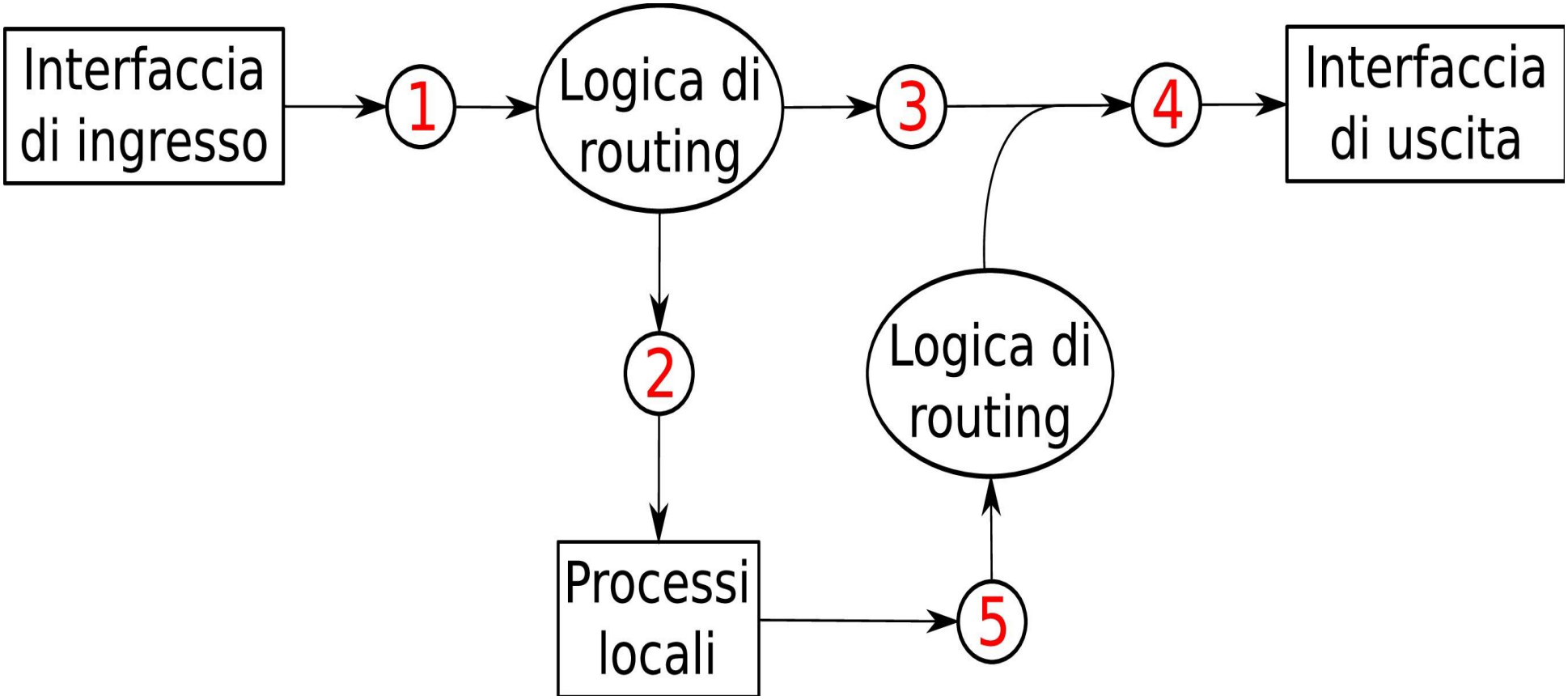
- **Netfilter mette a disposizione cinque principali valori di ritorno:**

- **NF_ACCEPT: accetta il pacchetto**
- **NF_DROP: nega l'accesso al pacchetto**
- **NF_STOLEN: preleva il pacchetto dal Kernel per manipolazioni in kernel space**
- **NF_QUEUE: accoda il pacchetto che viene reso disponibile per una gestione in ambito user space**
- **NF_REPEAT: provoca un nuovo transito del pacchetto nel medesimo hook**

IPtables

- **Sono presenti tre tabelle alle quali si possono associare un numero arbitrario di catene.**
- **Filter: per operazioni di filtraggio. Agganci agli hook NF_IP_LOCAL_IN, NF_IP_LOCAL_OUT e NF_IP_FORWARD**
- **Nat: per le funzioni di Masquerading (SNAT), Port Forwarding e Transparent Proxy (DNAT). Si aggancia agli hook NF_IP_PREROUTING, NF_IP_POSTROUTING, NF_IP_LOCAL_OUT**
- **Mangle: per le funzionalità di marking dei pacchetti e per effettuare modifiche ai campi TOS e TTL. Prevede agganci a tutti gli hook**

IPtables - Netfilter



IPtables – Packet Filtering

- **Per le operazioni di packet filtering si usa la tabella Filter, che contiene tre catene:**
- **INPUT: contiene le regole per i pacchetti destinati ad un processo locale**
- **OUTPUT: contiene le regole per i pacchetti diretti verso l'esterno**
- **FORWARD: contiene le regole per i pacchetti in transito**

IPtables – Packet Filtering

- **Per ciascuna catena occorre impostare la politica (accesso o negazione implicita) utilizzando l'opzione -P**
- **Il comando per impostare la politica ha la seguente struttura:**
- **iptables [-t tabella] -P catena { ACCEPT | DROP }**

- **Esempi:**
- **iptables –t filter –P INPUT DROP iptables –t filter –P FORWARD ACCEPT**

IPtables – Packet Filtering

- **A ciascuna catena possono essere aggiunte regole con l'opzione –A. Ogni regola ha un obiettivo, introdotto con l'opzione -j**

- **Il comando utilizzabile per aggiungere delle regole ha la seguente struttura:**
- **iptables [-t tabella] -A catena espressione -j obiettivo [opzioni]**

- **Tutti i pacchetti conformi all'espressione vengono inviati verso l'obiettivo**

IPtables – Packet Filtering

- **I possibili obiettivi sono:**
- **DROP: scarta il pacchetto (silenziosamente)**
- **REJECT: scarta il pacchetto inviando un messaggio ICMP o un TCP RST al mittente**
- **ACCEPT: autorizza il pacchetto ad attraversare l'hook**
- **QUEUE: rende il pacchetto disponibile per elaborazioni in user space**
- **LOG: effettua registrazione delle informazioni relative a pacchetti conformi alle regole specificate**
- **Il nome di un'altra catena di regole creata dall'utente: utile per organizzare logicamente le regole**

IPtables – Packet Filtering

- **Esempi di regole statiche:**

- **iptables –t filter –A INPUT –s 192.168.1.0/24 –j DROP**

- **iptables –t filter –A FORWARD –p tcp –i eth+ –d 192.168.1.0/24 --dport 80 –j ACCEPT**

- **iptables –t filter –A INPUT –p icmp –s !192.168.1.0/16 --icmp-type echo-request –j DROP**

IPtables – Packet Filtering

- **IPtables può essere usato per impostare delle regole dinamiche (stateful o state aware) utilizzando il modulo state.**
- **Tale modulo utilizza vari qualificatori utilizzabili all'interno delle espressioni di confronto. I più importanti sono:**
- **NEW: pacchetti necessari per l'apertura di una nuova connessione**
- **ESTABLISHED: pacchetti appartenenti a connessioni già stabilite in precedenza**
- **RELATED: pacchetti correlati a connessioni già stabilite (ICMP utili o nuove connessioni nel caso di FTP attivo)**

IPtables – Packet Filtering

- **Esempio di regole dinamiche per la gestione di FTP attivo:**

[connessione di controllo]

iptables –t filter –A FORWARD –p tcp - -dport ftp –m state --state NEW, ESTABLISHED –j ACCEPT

iptables –t filter –A FORWARD –p tcp - -sport ftp –m state --state ESTABLISHED -j ACCEPT

[connessione dati]

iptables –t filter –A FORWARD –p tcp - -sport ftp-data –m state --state RELATED,ESTABLISHED –j ACCEPT

iptables –t filter –A FORWARD –p tcp - -dport ftp-data –m state --state ESTABLISHED –j ACCEPT

IPtables – Packet Filtering

- **L'utilizzo del modulo state implica il tracciamento delle connessioni per riconoscere i pacchetti che fanno parte, o che sono correlati, a connessioni già esistenti**

- **Il tracciamento delle connessioni viene effettuato mediante moduli di Netfilter. Nel caso del protocollo FTP si utilizza il modulo ip_conntrack_ftp**

IPtables – Packet Filtering

- **Un'ulteriore esempio di regole dinamiche consiste nell'utilizzo del modulo limit**

- **limit consente di porre dei limiti alla frequenza con cui determinati tipi di pacchetti attraversano il firewall**

- **Utile per contrastare portscans, ping sweeps, alcuni tentativi di attacchi DOS, come syn floods**

IPtables – Packet Filtering

- **Esempio: regola di iptables per limitare l'efficacia di ping sweep**

iptables -t filter -A FORWARD -i eth+ -p icmp -m limit

--limit 4/minute --limit-burst 3 -j ACCEPT

- **Accetta una media di 4 pacchetti ICMP al minuto. Se la policy di default è DROP, i pacchetti ICMP in eccesso sono eliminati.**

IPtables – NAT

- **IPtables può essere utilizzato per funzioni di Network Address Translation (NAT) utilizzando la tabella nat**
- **In particolare, è possibile realizzare le seguenti funzionalità:**

- **Source NAT (SNAT): alterazione dell'indirizzo IP sorgente dei pacchetti**

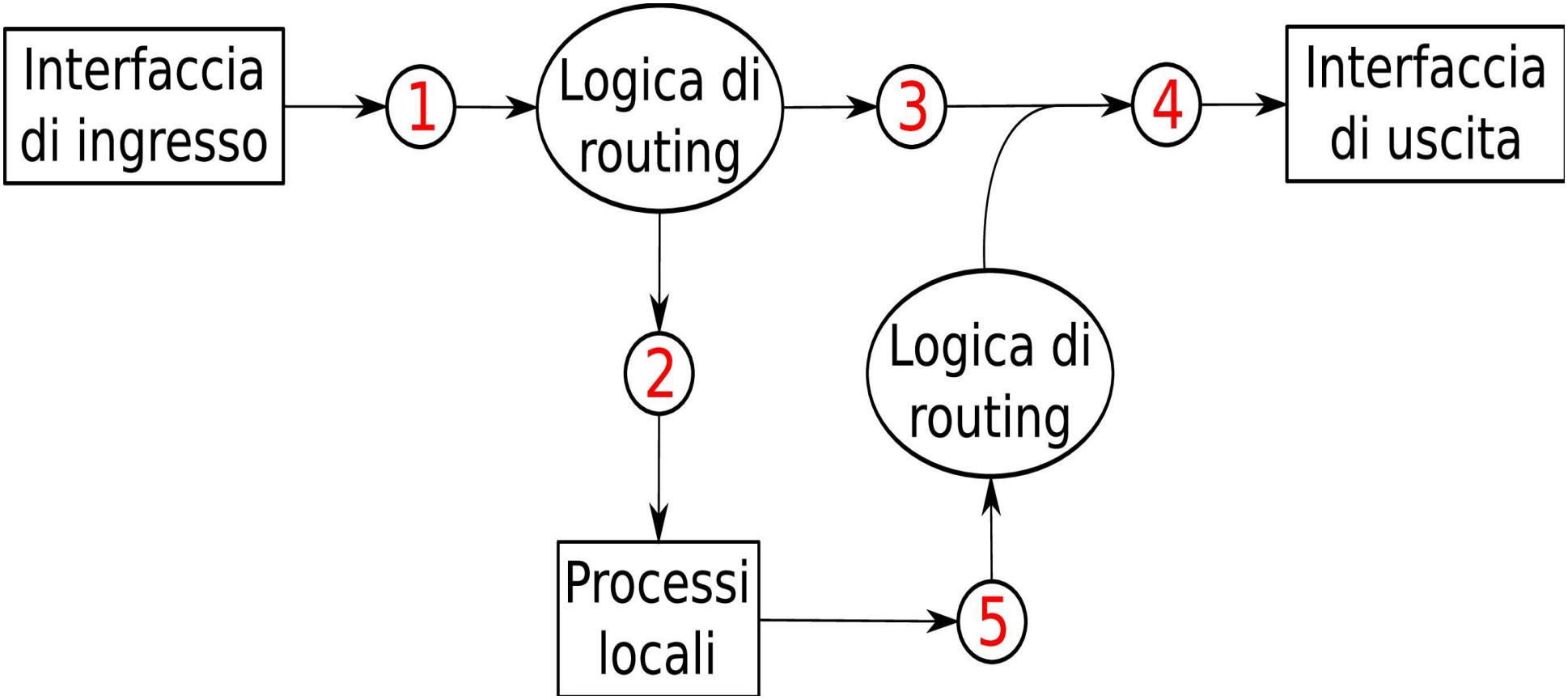
- **Destination NAT (DNAT): alterazione dell'indirizzo IP destinazione dei pacchetti**

IPtables – NAT

La tabella nat prevede tre catene di default:

- **PREROUTING: consente manipolazioni sull’indirizzo di destinazione (DNAT) dei pacchetti provenienti dall’esterno**
- **OUTPUT: consente manipolazioni sull'indirizzo di destinazione (DNAT) dei pacchetti generati localmente**
- **POSTROUTING: consente manipolazioni sugli indirizzi sorgente (SNAT) di tutti i pacchetti in uscita**

IPtables - NAT



IPtables – NAT

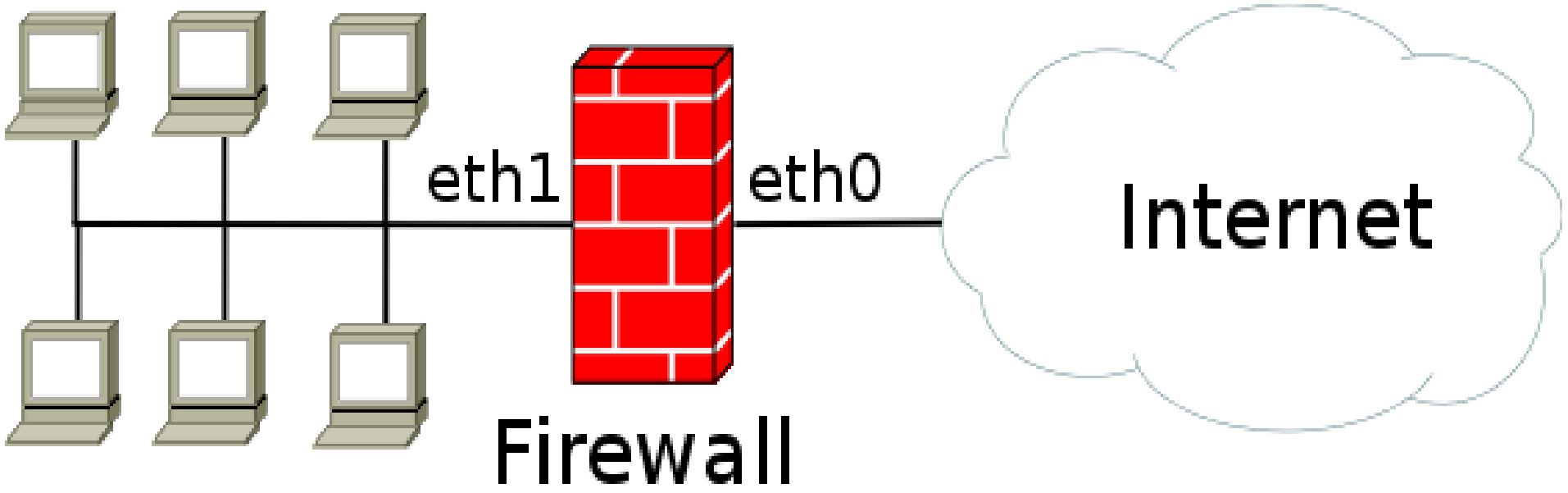
Gli obiettivi utilizzabili nelle regole delle catene sono:

- **SNAT: modifica l'indirizzo IP e la porta sorgente di un pacchetto**
- **MASQUERADE: sostituisce l'indirizzo IP sorgente di un pacchetto con quello dell'interfaccia di rete a cui è destinato (caso particolare di SNAT)**
- **DNAT: modifica l'indirizzo IP e la porta di destinazione di un pacchetto**
- **REDIRECT: sostituisce l'indirizzo IP destinazione di un pacchetto con quello dell'host che si occupa del NAT (caso particolare di DNAT)**

Perché effettuare NAT?

- **Per condividere un solo indirizzo IP (assegnato al firewall) con tutti gli host della rete locale**
- **Per consentire l'accesso da Internet ad un servizio presente su un host della rete locale con indirizzo privato**
- **Per nascondere la struttura della rete, facendo in modo che tutti i pacchetti sembrino generati dal firewall**
- **Per realizzare un Transparent Proxy**

IPtables – NAT



IPtables – NAT

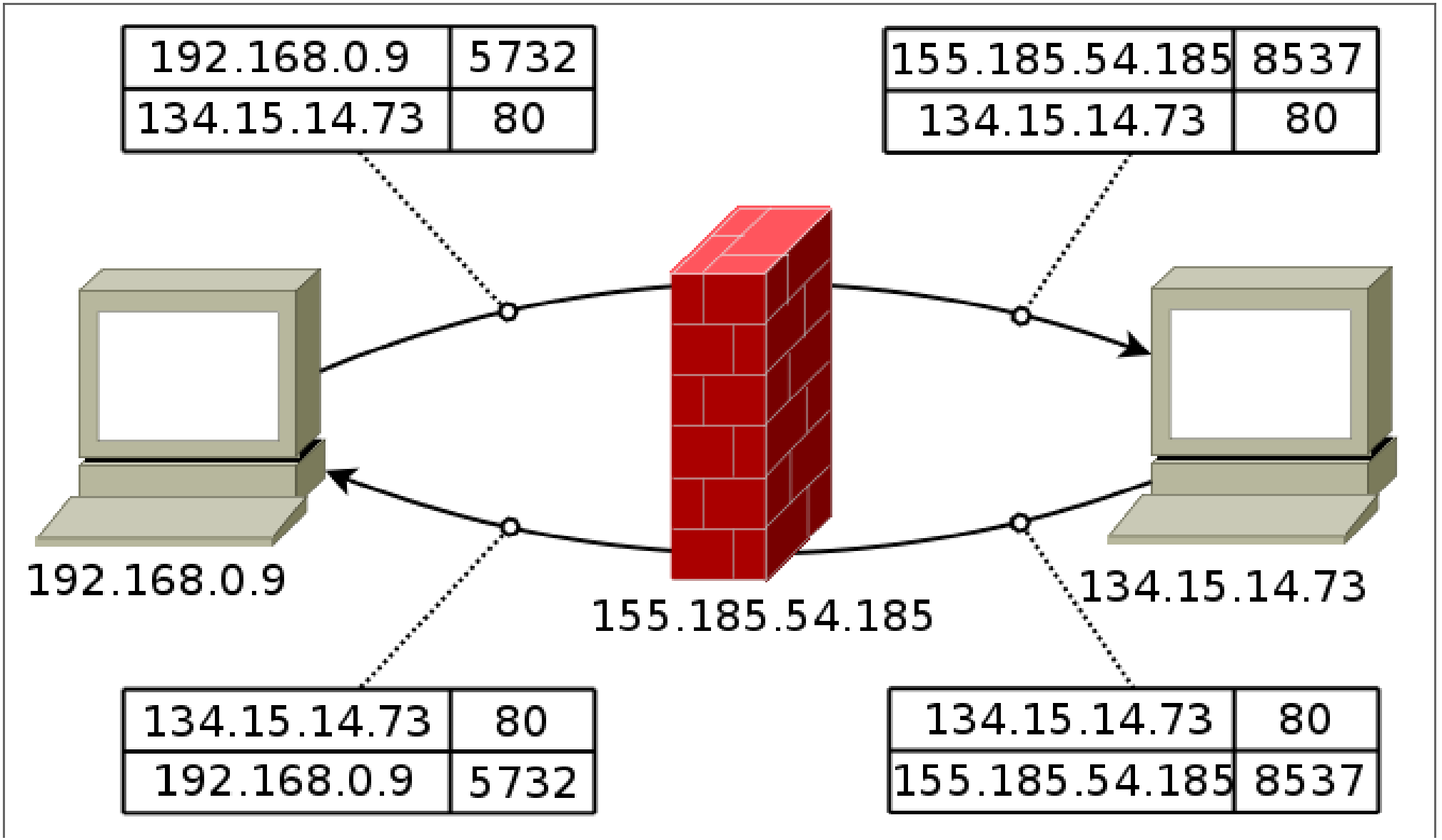
- **Per condividere l'unico indirizzo IP pubblico con tutte le macchine della rete locale è possibile utilizzare la seguente regola di IPtables:**

iptables –t nat –A POSTROUTING –o eth0 –j SNAT --to-source 155.185.54.185

Dove 155.185.54.185 rappresenta l'indirizzo IP pubblico della interfaccia di rete eth0 del firewall

Come funziona: ogni connessione tra un nodo della LAN e un nodo in Internet viene rimappata su un numero di porta libero dell'indirizzo IP 155.185.54.185

IPtables – NAT



IPtables – NAT

- **Questa regola non può essere utilizzata nel caso in cui l'indirizzo IP pubblico del firewall sia impostato dinamicamente (ad esempio nel caso di una connessione DSL).**
- **In questo caso si usa l'obiettivo MASQUERADE**

iptables –t nat –A POSTROUTING –o ppp0 –j MASQUERADE

- **L'obiettivo MASQUERADE sostituisce l'indirizzo IP sorgente con l'indirizzo IP attualmente posseduto dall'interfaccia ppp0**

IPtables – NAT

- **Se all'interno della LAN esiste un server web con un indirizzo IP privato, tale server non è direttamente raggiungibile dai nodi in Internet**

- **Per far fruire un servizio all'esterno di una rete locale con indirizzi privati occorre utilizzare il seguente comando:**

iptables –t nat –A PREROUTING –p tcp –d 155.185.54.185 --dport 80 -j DNAT --to-destination 192.168.1.1

- **Dove 192.168.1.1 è l'indirizzo privato del web server**

IPtables – NAT

- **Mediante le regole della tabella nat è possibile implementare un Transparent Proxy, cioè un proxy contattato dai client in modo trasparente, senza la necessità di impostazioni particolari**

iptables –t nat –A PREROUTING –p tcp –i eth1 --dport 80 –j DNAT --to-destination 192.168.1.1:8080

- **Questo comando redirige tutti i pacchetti tcp diretti alla porta 80 verso la porta 8080 dell'host 192.168.1.1, che ospita un web proxy**

IPtables – NAT

- **Se il transparent proxy risiede sullo stesso host che implementa i meccanismi di NAT è possibile usare l'obiettivo REDIRECT**

iptables –t nat –A PREROUTING –p tcp –i eth1 --dport 80

–j REDIRECT --to-port 8080

IPtables – Packet Marking

- **Attraverso la tabella mangle di Netfilter, IPtables può implementare funzionalità di "marcatore di pacchetti".**
- **Si intende la tecnica di manipolazione degli header dei pacchetti per utilizzare avanzate metodologie di routing, modificare i valori dei campi TOS, TTL, ecc.**

Cinque catene per questa tabella:

- **PREROUTING: per manipolare pacchetti prima della logica di routing**
- **OUTPUT: per manipolare pacchetti generati da processi locali prima della logica di routing**

IPtables – Packet Marking

- **INPUT: per manipolare pacchetti diretti ad un processo locale (dal Kernel 2.4.18 in poi)**

- **FORWARD: per manipolare pacchetti instradati da una interfaccia all'altra**

- **POSTROUTING: per manipolare pacchetti già sottoposti alla logica di routing**

IPtables – Packet Marking

Gli obiettivi delle regole associate alle catene sono:

- **MARK: utilizzato per impostare il valore dei marcatori di Netfilter**
- **TOS: usato per impostare il valore del campo TOS**
- **DSCP: sfruttato per alterare il valore del campo DSCP (sei bit all'interno del campo TOS)**
- **ECN: permette di settare a 0 tutti i bit del campo ECN dei pacchetti TCP**
- **TCPMSS: consente di modificare il valore del MSS dei pacchetti TCP SYN**

IPtables – Packet Marking

Per impostare un valore ai marcatori di Netfilter:

iptables –t mangle –A PREROUTING –p tcp –i eth0 –j MARK --set-mark mark

Per alterare il valore del TOS di un pacchetto:

iptables –t mangle –A OUTPUT – p tcp –dport 3045 –j TOS --tos tos

Per modificare il valore della Maximum Segment Size:

iptables –t mangle –A POSTROUTING –p tcp –j TCPMSS --clamp-mss-to-pmtu

IPtables

- **In tutte le tabelle di IPtables è possibile definire delle nuove catene (opzione -N), in aggiunta a quelle presenti di default. Le catene definite degli utenti possono essere utilizzate come obiettivo all'interno delle regole**

iptables -t filter -N catena_tcp

iptables -t filter -A FORWARD -p tcp -j catena_tcp

- **Definendo nuove catene è possibile separare le regole relative a diversi tipi di pacchetti**

IPtables

- **L'opzione -L stampa a schermo una schermata contenente le catene contenute in una tabella e le regole appartenenti a ciascuna catena**

iptables -t filter -L

- **L'opzione -D consente di eliminare selettivamente una regola da una catena**

iptables -t filter -D FORWARD 2

elimina la seconda regola dalla catena FORWARD

IPtables

- **L'opzione -F (flush) elimina tutte le regole contenute in una determinata catena. Se nessuna catena viene specificata, sono eliminate tutte le regole appartenenti a tutte le catene della tabella**

iptables -t filter -F FORWARD iptables -t nat -F

- **L'opzione -X consente di eliminare una catena. Possono essere eliminate solo le catene definite con l'opzione -N**

iptables -t filter –X catena_tcp

IPtables - Configurazione

- **La creazione di un firewall, eventualmente con funzionalità di NAT integrate, può richiedere l'utilizzo di numerose regole, e quindi di un numero elevato di comandi**

- **Tipicamente tutti i comandi vengono raggruppati all'interno di uno script, che viene eseguito automaticamente all'avvio del firewall**

- **Gli script di configurazione possono essere scritti manualmente o possono essere generati automaticamente mediante l'utilizzo di appositi programmi**