Firewall

Cosa e’ un firewall...

- Letterelmente e’ un "muro di fuoco" tra un host e il mondo esterno...
- ...in realta e’ un sw/hw per la protezione da traffico indesiderato
- E’ spesso implementato a livello kernel (interagisce con lo stack TCP/IP)
- E’ facilmente configurabile con applicativi a livello user
-

Funzioni di un firewall

- Monitorare il traffico in transito tra due o piu’ reti
- Prevenire connessioni indesiderate
- Rilevare ed evitare alcuni tipi di attacchi remoti
- Implementare politiche granulari per l’accesso a risorse di rete
- NAT (Network Address Translation)
- PAT (Port Address Translation)

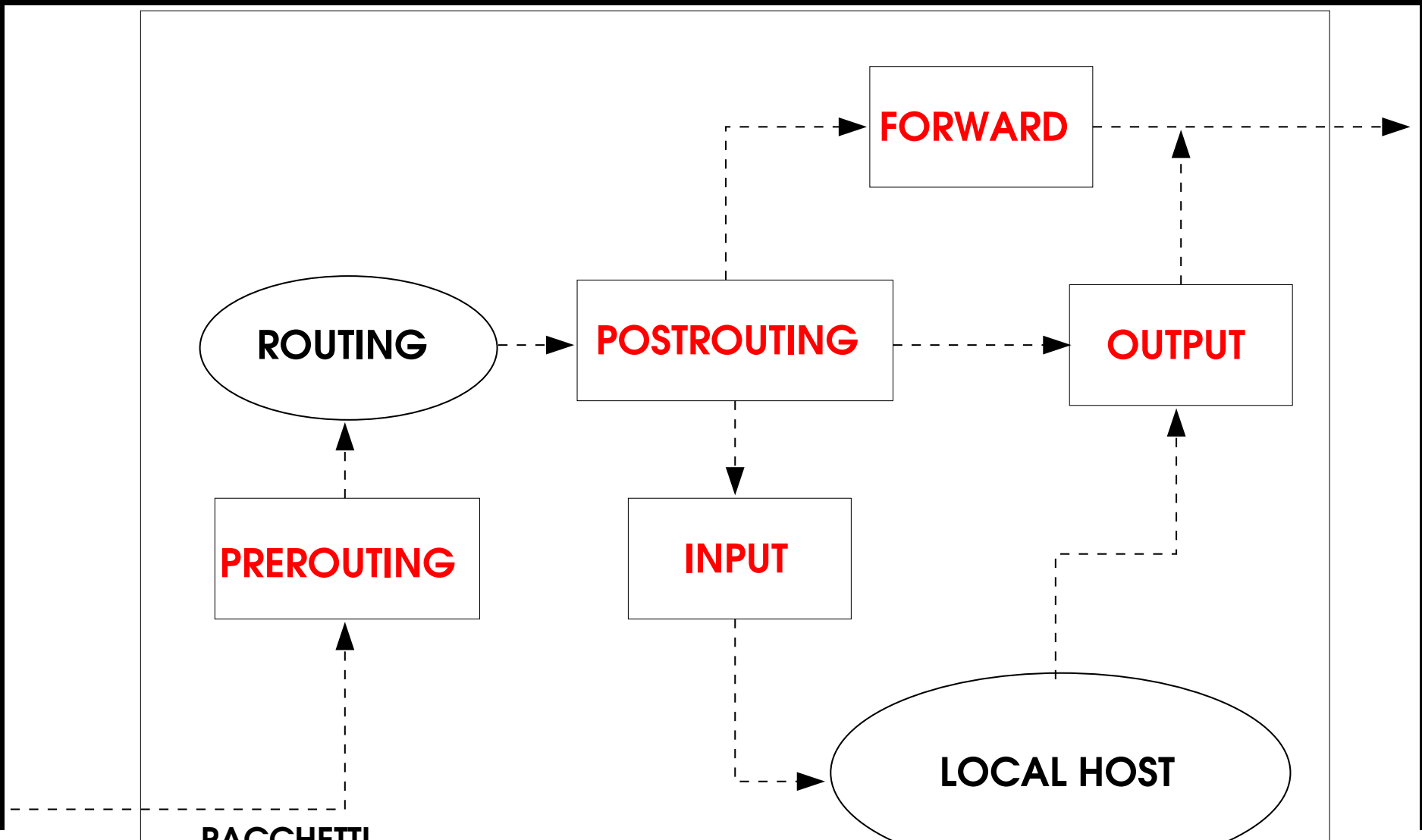
Tipi di firewall

- In base al tipo di utilizzo che se ne fa, i firewall si suddividono in:
  - Personal Firewall (filtrano il traffico di un solo host)
  - Traditional Firewall (filtrano il traffico tra due o piu' reti)
- In base al tipo di funzionalita' implementate, possono essere:
  - Stateless Firewall (Orientati al pacchetto)
  - Stateful firewall (Orientati alla connessione)

Netfilter

- Il sistema di firewalling di Linux si chiama Netfilter
- E’ il firewall di default sui kernel 2.4.X e 2.6.X
- Funzionalita’:
  - Stateless firewall
  - Stateful firewall
  - NAT/PAT
  - Logging
  - Masquerading
  - Moduli e plug-in aggiuntivi
-

Struttura di Netfilter



Funzionamento di Netfilter (1)

- Netfilter elabora i pacchetti utilizzando delle "tabelle" (table)
- Ciascuna tabella contiene diverse "catene" (chain)
- Ogni catena e’ una raccolta di "regole" (rule)
- Ogni regola specifica una determinata azione da effettuare su un pacchetto

Le tabelle di netfilter

- Netfilter supporta, di base, tre tabelle:
  - filter: La tabella di default.
  - nat: usata per i pacchetti che creano nuove connessioni
  - mangle: usata per l’alterazione dei pacchetti

La tabella "filter"

- La tabella filter viene utilizzata per il normale processamento dei pacchetti
- Contiene tre catene di default:
  - INPUT: usata per i pacchetti destinati all’host
  - OUTPUT: usata per i pacchetti generati dall’host
  - FORWARD: usata per i pacchetti in transito

La tabella "nat"

- E’ utilizzata per le operazioni di NAT / PAT
- Contiene tre catene di default:
  - PREROUTING: per manipolare i pacchetti prima del routing
  - OUTPUT: per manipolare i pacchetti generati dall’host
  - POSTROUTING: per manipolare i pacchetti a seguito del routing

La tabella "mangle"

- Viene utilizzata per alterare i pacchetti in uscita/transito
- Contiene cinque catene di default:
- PREROUTING
- POSTROUTING
- INPUT
- FORWARD
- OUTPUT

Le regole

- Ogni catena e’ un insieme di regole
- Ciascuna regola e’ suddivisa in due parti:
  - Descrizione dei pacchetti ai quali si applica
  - Azione da effettuare (target)
- Esistono quattro target di default:
  - ACCEPT, DROP, QUEUE, RETURN

Le regole vengono analizzate una dopo l’altra, fino a quando non avviene un "match". Se un pacchetto verifica una regola, le regole successive vengono ignorate.

Un semplice esempio di firewall

- Obiettivo: impedire le connessioni al nostro host dall'esterno della LAN
- Regola in metalinguaggio:
  - 10 AGGIUNGI alla catena INPUT
  - 20 per ogni pacchetto PROVENIENTE dalla LAN
  - 30 ACCETTA il pacchetto

Moduli di Netfilter e IPTABLES

- Netfilter e’ una architettura firewall a livello kernel
- Molte delle funzionalita’ sono fornite da "moduli" aggiuntivi
- Per la sua configurazione si utilizza di solito IPTABLES
- IPTABLES e’ un applicativo utente a riga di comando
- La sintassi e’:
  - iptables [-t table] <azione> <specifica_pacchetto> <target>

Iptables: azioni

- -A: Aggiunge una regola alla fine di una catena
- -D: Rimuove una regola
- -I: Inserisce una regola in una certa posizione
- -R: Sostituisce una regola
- -F: Cancella tutte le regole di una catena
- -P: Stabilisce la policy di default di una catena
- -L: Visualizza tutte le regole di una catena

Esempi:

- iptables -P INPUT DROP

Stabilisce per la catena di INPUT la policy DROP. Cio' significa che se un pacchetto attraversa tutte le regole della catena di INPUT senza soddisfarne alcuna, alla fine viene ignorato.

- iptables -F OUTPUT

Elimina tutte le regole della catena di OUTPUT

- iptables -L INPUT

Visualizza tutte le regole della catena di INPUT

Sorgente e destinazione

- E’ possibile specificare l’indirizzo sorgente e distinazione di un pacchetto
  - -s: specifica l’indirizzo/rete sorgente
  - -d: specifica l’indirizzo/rete destinazione
- -s 192.168.0.1

Indica tutti i pacchetti provenienti da 192.168.0.1

- -d 192.168.1.0/24

Indica tutti i pacchetti destinati ad un host della rete 192.168.1.0

Protocolli

- E’ possibile specificare il protocollo utilizzato dal pacchetto:
- -p tcp: indica il protocollo tcp
- -p udp: indica il protocollo udp
- -p icmp: indica il protocollo icmp
- Quindi : " -s 192.168.0.1 -p tcp"

Indica tutti i pacchetti TCP provenienti da 192.168.0.1

Porte

Nel caso di pacchetti appartenenti a connessioni TCP o a flussi UDP e’ possibile specificare anche la porta sorgente/destinazione:

- --source-port: indica la porta o il range di porte sorgenti
- --destination-port: indica la porta o il range di porte di destinazione

Esempio:

- -p tcp --source-port 80

Indica tutti i pacchetti TCP provenienti dalla porta 80

- -p udp --destination-port ! 1:1024

Indica tutti i pacchetti UDP destinati a porte superiori alla 1024

Flag TCP

Per i pacchetti TCP e’ possibile anche indicare i flag settati

- --tcp-flags <mask> <set>: indica i pacchetti che abbiano posti a uno tutti i flag di <mask> che compaiono in <set>, e i rimanenti posti a zero
- -p tcp --tcp-flags SYN,ACK SYN

Indica tutti i pacchetti TCP che abbiano il bit SYN posto a 1 e il bit ACK posto a 0

- -p tcp --tcp-flags FYN,ACK,RST RST

Indica tutti i pacchetti TCP che abbiano il flag RST settato e i flag FYN e ACK a 0

Esempio 1: firewall conservativo (F1)

Obiettivo: consentire connessioni tcp/udp solo da/a host della stessa LAN; Consentire il ping

```
iptables -F INPUT
iptables -P INPUT DROP
iptables -A INPUT -s 127.0.0.0/8 -j ACCEPT
iptables -A INPUT -s 192.168.0.0/24 -p tcp -j ACCEPT
iptables -A INPUT -s 192.168.0.0/24 -p udp -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

LOG

E’ possibile effettuare logging dei pacchetti che attraversano il firewall

Esiste un apposito target, chiamato LOG, che scrive sui log di sistema

Le opzioni principalo sono:

- --log-level: indica il livello di LOG
- --log-prefix: consente di specificare un prefisso per i log
- --log-tcp-options: riporta nel log anche le opzioni TCP
- --log-ip-options: riporta nel log anche le opzioni IP

Esempio di LOG (F2)

Obiettivo: aggiungere al firewall precedente una regola che imponga il LOG dei tentativi di connessione indesiderati

....si usano le stesse regole di F1, aggiungendo:

iptables -A INPUT -p tcp -s ! 192.168.0.0/24 -j LOG --log-prefix "Undesired "
--log-ip-options --log-tcp-options

In tal modo tutti i pacchetti che provengono da host esterni alla rete 192.168.0.0/24 vengono riportati nel log di sistema, assieme alle relative opzioni IP e TCP (indirizzi s/d, porte s/d, flag...)

NAT

- Solitamente un router si occupa di inoltrare pacchetti
- In alcuni casi e’ utile o necessario alterare i pacchetti in transito
- Per esempio nel caso del passaggio da una rete locale verso internet...
- ...e’ necessario modificare l’indirizzo sorgente dei pacchetti in uscita...
- ... per poter ricevere correttamente i pacchetti di risposta....
- In questi casi si effettua un NAT (Network Address Translation)

Source NAT

- Per il NAT ti utilizza la tabella "nat"
- Il NAT piu’ utilizzato e’ il Source NAT (SNAT)
- Viene modificato l’indirizzo sorgente, DOPO il routing

Esempio:

- iptables -t nat -A PORTROUTING -s 192.168.0.0/24 -j SNAT --to-source 151.97.6.18

Converte l’indirizzo sorgente di tutti i pacchetti che provengono dalla LAN in 151.97.6.18

Destination NAT

- E’ possibile cambiare anche l’indirizzo destinazione di un pacchetto
- Il Destination NAT (DNAT) si effettua PRIMA del routing
- Ad esempio per smistare il traffico tra i server di una LAN:
- iptables -t nat -A PREROUTING -s ! 192.168.0.0/24 -p tcp --destination-port 80 -j DNAT --to-destination 192.168.10.1

Redirige i pacchetti HTTP provenienti dall’esterno all’host 192.168.10.1

-

Masquerading

- Il masquerading e’ un particolare tipo si SNAT
- Viene spesso utilizzato per le connessioni on-demand
- Serve a mascherare l’indirizzo sorgente in maniera automatica

Esempio 1: modem

Obiettivo: firewall personale. Connessione tramite modem. Impedire connessioni dall'esterno. Solo navigazione web.

```
iptables -F INPUT
iptables -P INPUT DROP
iptables -A INPUT -s 127.0.0.0/8 -d 127.0.0.0/8 -j ACCEPT
iptables -A INPUT -p udp --source-port 53 -j ACCEPT
iptables -A INPUT -p tcp --source-port 80 --tcp-flags SYN,ACK SYN,ACK -j ACCEPT
iptables -A INPUT -p tcp --source-port 8080 --tcp-flags SYN,ACK SYN,ACK -j ACCEPT
iptables -A INPUT -p tcp --source-port 443 --tcp-flags SYN,ACK SYN,ACK -j ACCEPT
iptables -A INPUT -p tcp --state RELATED,ESTABLISHED -j ACCEPT
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

Esempio 2: semplice router adsl

Vari esempi. Logging, forwarding, hardening