



Sicurezza delle reti¹

Mattia Monga

Dip. di Informatica e Comunicazione
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2010/11

¹ © 2011 M. Monga. Creative Commons Attribuzione-Condividi allo stesso modo 2.5 Italia License.
<http://creativecommons.org/licenses/by-sa/2.5/it/>. Materiale derivato da © 2010 M. Cremonini.



Lezione X: Sicurezza perimetrale



IPTables/Netfilter

- Linux 2.2 ipchains solo stateless filtering
- Linux 2.4 netfilter (kernel mode) permette di scrivere regole stateful, organizzate in *catene* e *tabelle* da iptables (user mode)



Tabelle

Il kernel di Linux mantiene alcune tabelle di regole da esaminare nella manipolazione dei pacchetti di rete. Il numero e la natura delle tabelle dipende dalla configurazione del kernel. Ogni tabella contiene *catene* di regole: con iptables si possono alterare le regole e aggiungere/togliere catene.

filter Tabella di default. Catene di regole: INPUT, FORWARD, OUTPUT;

nat Tabella consultata quando si **crea** una nuova connessione. PREROUTING, OUTPUT, POSTROUTING

mangle Tabella usata in manipolazioni particolari. PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING

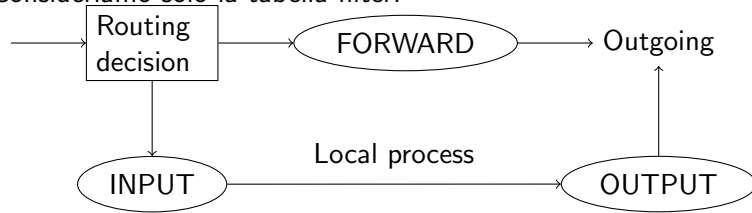
raw Tabella ad alta priorità. PREROUTING, OUTPUT

Per vedere il contenuto di filter: `iptables -t filter -L`

Filtrare un pacchetto



Consideriamo solo la tabella filter:

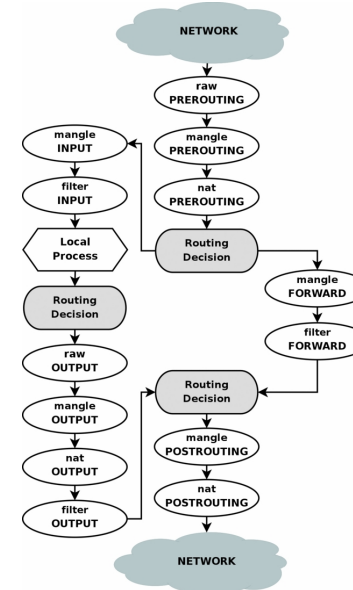


- 1 Arriva un pacchetto (p.es. dalla scheda di rete)
- 2 Si decide dove deve essere consegnato (routing)
- 3 Se è locale, passa per la INPUT chain (ACCEPT/DROP)
- 4 Altrimenti DROP, ma se il forwarding è abilitato, si passa per la FORWARDING chain (ACCEPT/DROP)
- 5 Se un processo locale produce un pacchetto si passa per la OUTPUT chain (ACCEPT/DROP)

113

Scuola delle
reti
Monga
IPTables/Netfilter

Il percorso di un pacchetto



La *routing decision* determina se il pacchetto ha destinazione locale o esterna: deve essere ripetuta più volte perché il filtro potrebbe alterare i campi rilevanti del pacchetto.

114

Scuola delle
reti
Monga
IPTables/Netfilter

Esempio



- ```
1 # First of all delete any existing rules.
2 iptables -t filter -F # -t filter (default)
3 iptables -t filter -X
4
5 # Block all access to port 22 (ssh)
6 # BUT allow host 10.49.165.18
7 iptables -A INPUT --source 10.49.165.18 -p tcp --dport 22 -j ACCEPT
8 iptables -A INPUT -p tcp --dport 22 -j DROP
```

115

Scuola delle  
reti  
Monga  
IPTables/Netfilter