

# Corso reti 2k7

## linuxludus

Lezione 5, netfilter 4 kids

Giuseppe Marocchio (LAN)  
io@giuseppe-marocchio.com

---

---

# Firewall

Un firewall e' un dispositivo HW/SW che ha il compito di filtrare le comunicazioni tra due o più reti di calcolatori. Esso può essere un normale computer o un dispositivo hw sviluppato ad hoc



# firewall (2)

Oggi tratteremo il firewall di linux “netfilter”  
al fine di proteggere una rete e non solo il pc  
locale (come visto la scorsa serata)

---

---

# Tipi di Firewall

Esistono sostanzialmente 3 tipi di firewall.

**StateLess**

**StateFull**

**StateFull DPI**

---

---

# StateLess

E' la modalità primordiale di proteggere una rete. Questo tipo di firewall blocca le porte secondo una logica "scema" Aperta o Chiusa senza aggiungere particolari controlli a cosa è in transito.

E' un modello oramai in disuso.

---

---

# StateFull

Un firewall statefull è in grado di controllare lo “stato” di una connessione TCP. Pertanto è in grado di capire se essa è nuova o già in uso. Pertanto è in grado di tenere traccia di ogni connessione.

---

---

# DPI

DPI e' un tipo di "firewall" che si sta affermando negli ultimi anni, la DPI (Deep Packet Inspection ) è una funzione che permette di aprire i pacchetti in transito per capire effettivamente cosa contengono. E successivamente deciderne le sorti.

E' usato come strumento per limitare i p2p

---

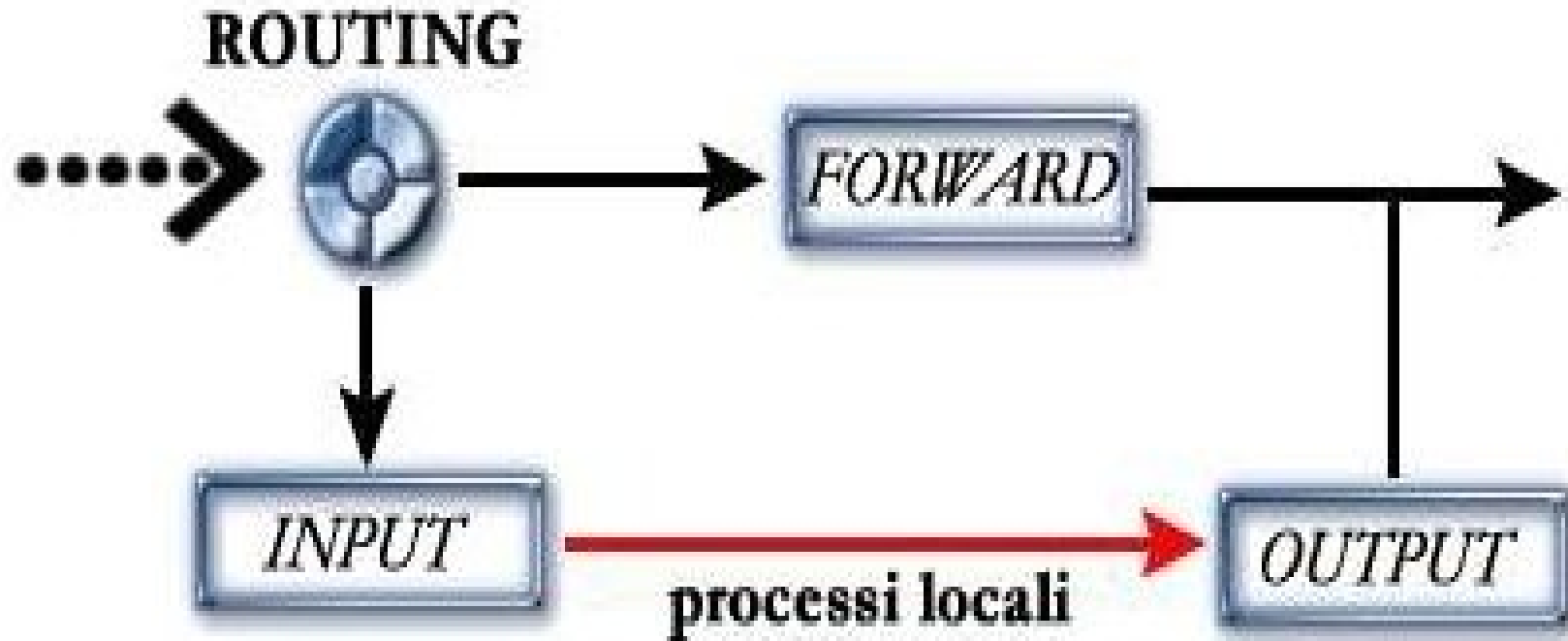
---

# E noi?

Stasera affronteremo il modello Stateless e StateFull. Con particolare enfasi sul tipo StateFull.



# Struttura del firewall



PERCORSO PACCHETTI KERNEL 2.4

**tralasciamo input e output**

# Forward

Forward serve per filtrare i pacchetti in transito TRA il due o più reti.

Input e output sono già stati affrontati la settimana scorsa



# Routing

Routing appartiene alla tabella NAT e serve per abilitare funzionalità “aggiuntive” come la “condivisione della connessione” o il “forward di una porta”



# NAT

Farò spesso riferimento a questa cosa misteriosa, chiamata NAT. il nat è quel meccanismo che serve per nascondere una rete “privata” dietro un singolo ip pubblico.

questo meccanismo consiste in pratica nel cambiamento di alcune parti del pacchetto IP

---

---

# Tabella NAT

la tabella nat si divide in 2 rami.  
il primo e' definito PREROUTING il secondo si  
chiama POSTROUTING

si possono vedere le regole con

```
iptables -t nat -L
```

# PREROUTING

prerouting serve per abilitare le funzionalita' di port forwarding in caso di rete nattata.

Esempio:

```
iptables -t nat -A PREROUTING -p tcp --  
dport 80 -j DNAT --to 192.168.1.3:80
```

---

---

# POSTROUTING

Postrouting serve per abilitare le funzioni di nat su una specifica interfaccia/rete

Esempio:

```
iptables -t nat -A POSTROUTING -o ppp0  
-j MASQUERADE
```

---

---

# Filtrare sulla forward

Filtrare i pacchetti in transito e' relativamente semplice. Basta operare sulla tabella forward, specificando mediante le opzione -o / -i l'interfaccia sorgente e di destinazione. In alternativa è possibile specificare gli indirizzi ip o le classi di ip

---

---

# Abilitare il Forward

Normalmente le funzionalità di forwarding su un pc con linux sono disabilitate di default. in Netkit sono già abilitate. tuttavia per abilitarle e' necessario dare il seguente comando:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

---

---

# Statefull con i flag TCP

La maniera piu' semplice per sperimentare un firewall statefull. E' senzadubbio quella di provare.

i flag sulle connessioni TCP possono essere

NEW, RELATED, ESTABLISHED, INVALID,  
es:

```
iptables -A INTLAN -m state --state  
ESTABLISHED,RELATED -j ACCEPT
```

---

---

# Laboratorio

Configuriamo due macchine virtuali come

PC1-----PC2-----[ PC3 PC4 ]

PC1 oggi simula internet, con un servizio sulla porta 80. PC2 e' il firewall della rete che contiene PC3 e PC4, e necessita di nat

---

---

**All'opera**

**Proviamo ?**



Domande ?

