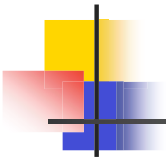
Filtraggio del traffico IP in linux

Corso di Amministrazione di Reti

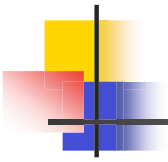
AA 2002/2003

Fabio Bucciarelli - DEIS



Cos'è un firewall?

- E' un dispositivo hardware o software, che permette o nega la comunicazione fra 2 reti diverse (es. Internet – Lan aziendale).
- E' posizionato sulla frontiera fra le 2 reti e ha lo scopo di proteggere la rete interna consentendo le attività lecite

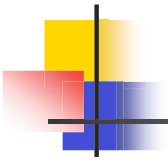


Packet filter firewall

Analizzano gli header dei pacchetti che vi transitano fino al livello di trasporto.

Discriminano in base a:

- Livello fisico (es. interfaccia di rete)
- Livello data link (es. mac sorgente o destinazione)
- Livello rete (es. IP sorgente o destinazione)
- Livello trasporto (es. porta sorgente o destinazione)



Proxy firewall

- Sono in grado di interpretare le informazioni del pacchetto fino al livello applicativo

Es. firewall http inoltra o scarta pacchetti in funzione dell'URL

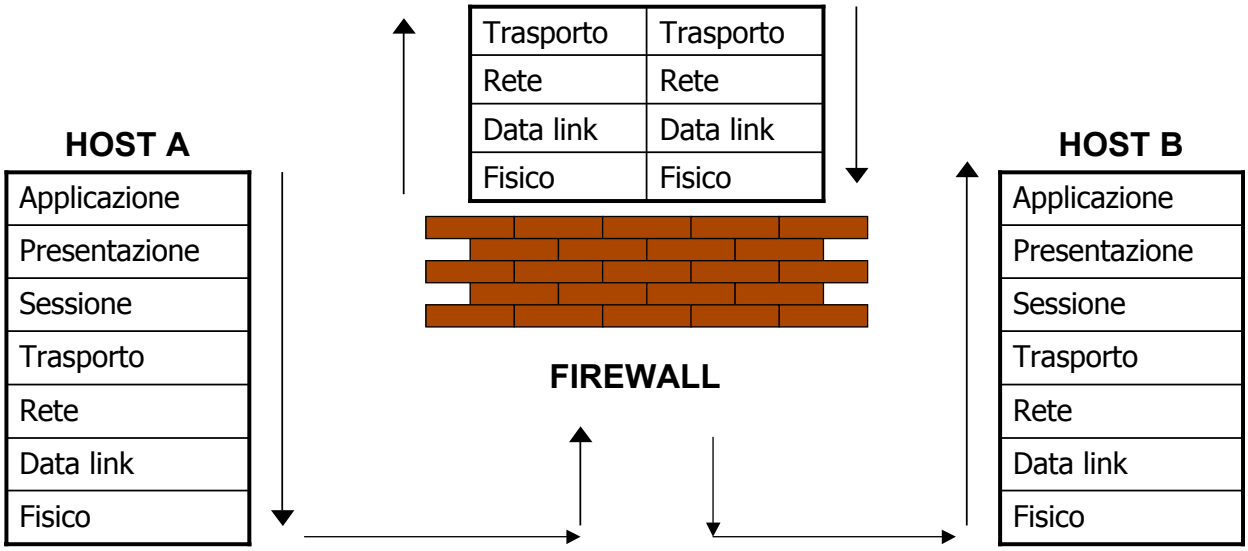
- Proxy generici (es. socks)
- Proxy dedicati (es. squid)

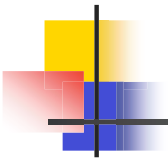
Packet filter vs. Proxy firewall

Packet filter	Proxy firewall
+ veloce	+ potente
Kernel space	User space
Indipendente dal protocollo applicativo	Richiede hardware + veloce

Firewall di linux

E' di tipo packet filter

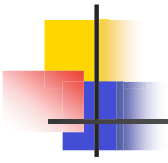




Firewall di linux (2)

E' integrato nel kernel di linux, quindi rappresenta la soluzione più semplice e veloce. Il kernel deve essere predisposto in fase di compilazione , oppure devono essere caricati gli appositi moduli.

- Kernel 2.0.* -> ipfwadmin
- Kernel 2.2.* -> ipchains
- Kernel 2.4.* -> iptables

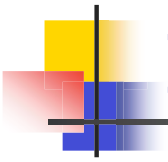


Firewall di linux (3)

- L'attraversamento dei pacchetti tra un'interfaccia ed un'altra deve essere abilitata espressamente nel kernel, attraverso il comando:

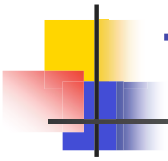
```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

- Possibilità di estensioni (moduli), che possono essere incluse o meno in fase di compilazione



Iptables

- Si basa sui concetti di tabelle, catene e regole
- Una tabella è formata da catene (punti di controllo) e una catena da regole



Tabelle

- Filter
- NAT
- Mangle

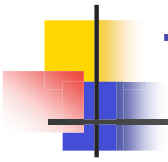


Tabella filter

Contiene le regole di filtraggio vere e proprie dei pacchetti che il firewall origina e riceve o che transitano dal firewall

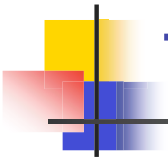


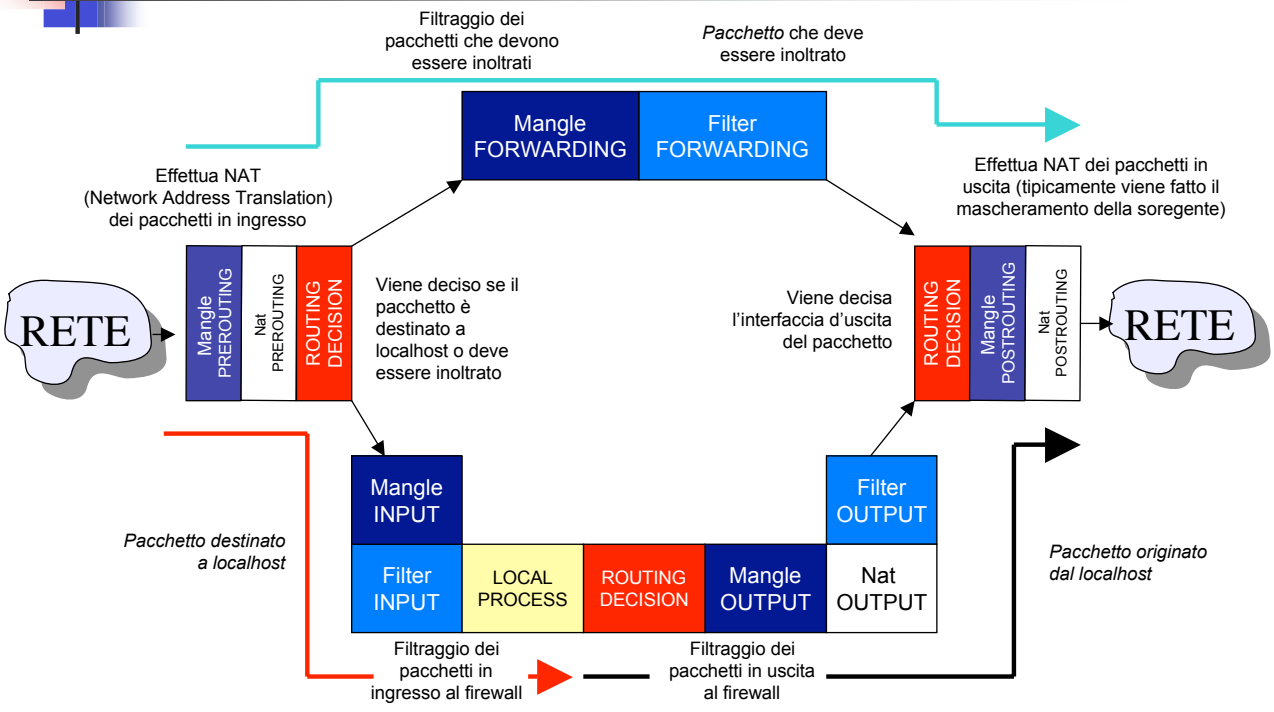
Tabella NAT

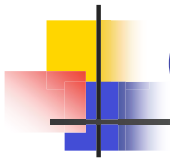
Consente di effettuare il NAT (Networking Address Translation) degli indirizzi IP o del valore della porta sorgente o di destinazione

Tabella mangle

- Usata per effettuare alterazioni particolari dell'header IP (TTL, TOS, MARK)
- Particolarmente interessante è il target MARK, che permette di marcare il pacchetto, in modo da essere trattato diversamente nei successivi punti di controllo o da altri programmi

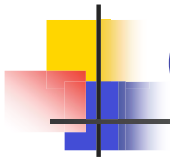
Come i pacchetti attraversano i filtri





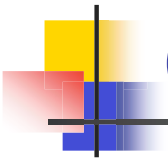
Catene della tabella filter

- INPUT
  operazioni di filtraggio di pacchetti appena gunti al firewall e diretti all'host
- FORWARD
  operazioni di filtraggio di pacchetti che transitano dal firewall
- OUTPUT
  operazioni di filtraggio di pacchetti generati localmente che stanno per uscire dal firewall



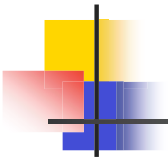
Catene della tabella NAT

- PREROUTING
  operazioni di nat di pacchetti appena giunti al firewall
- OUTPUT
  operazioni di nat di pacchetti generati localmente
- POSTROUTING
  operazioni di nat di pacchetti che stanno per uscire dal firewall



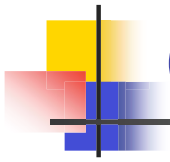
Catene della tabella mangle

- PREROUTING
- INPUT
- FORWARD
- OUTPUT
- POSTROUTING



Le regole

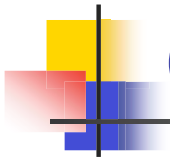
- Hanno la forma di ACL
- Ogni catena ha una policy di default
- L'elenco delle regole viene scorso dall'inizio alla fine
- Al primo match si stabilisce cosa fare del pacchetto e, salvo casi particolari si interrompe l'analisi delle regole della catena
- Se per nessuna regola c'è il match, si esegue la policy di default



Come si costruisce una regola

```
#iptables [table] command
  [match] [target]
```

- [table] selezione della tabella
- [match] criteri per la selezione del pacchetto
- [target] destino del pacchetto che soddisfa il match



Comandi sulle catene

- Creare una nuova catena (-N)
- Cancellare una catena vuota (-X)
- Cambiare lapolicy di default di una catena (-P)
- Elencare le regole presenti in una catena (-L)
- Svuotare una catena delle sue regole (-F)
- Azzerare i contatori

Comandi per manipolare le regole di una catena

- Appendere una nuova regola alla catena (-A)
- Inserire una regola in una determinata posizione (-I)
- Sostituzione di una regola presente in una certa posizione (-R)
- Cancellazione di una regola presente in una certa posizione (-D)
- Cancellazione della 1° regola di una catena (-D)

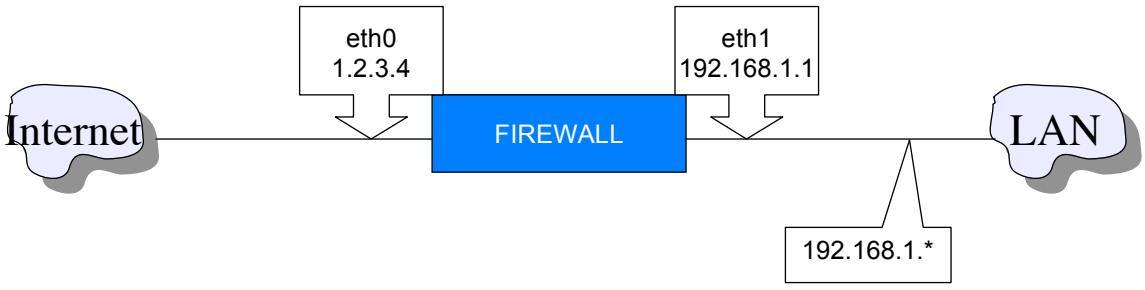
I target (1)

- ACCEPT
  il pacchetto viene accettato
- DROP
  il pacchetto viene scartato
- REJECT
  stesso effetto di DROP, ma viene inviato in risposta un messaggio di errore ICMP di tipo "port unreachable"
- Catena creata dall'utente

I target (2)

- RETURN
  termina la catena; se è una catena predefinita, viene eseguita la tattica, se è definita dall'utente, esegue la regola successiva sulla catena precedente
- QUEUE
  accoda i pacchetti per elaborazioni userspace

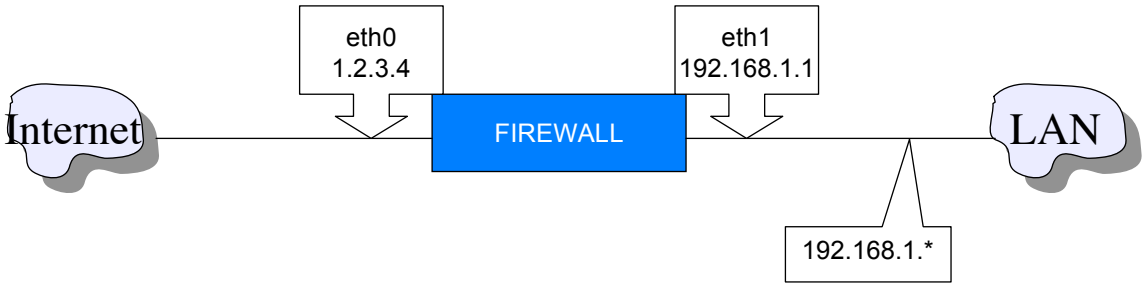
Esempi




```
#iptables -A FORWARD -i eth1 -j DROP
```

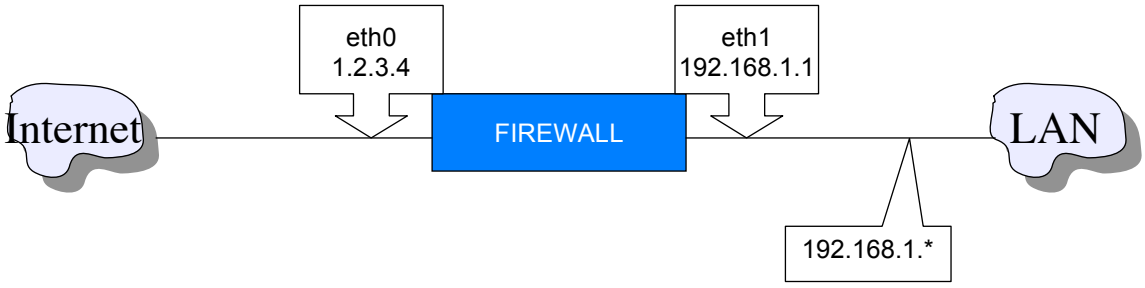
Tutte le opzioni di match possono essere negate attraverso il simbolo !

Esempi




```
#iptables -A FORWARD -i eth1 -s
  192.168.1.0/24 -d 0/0 -j DROP
```

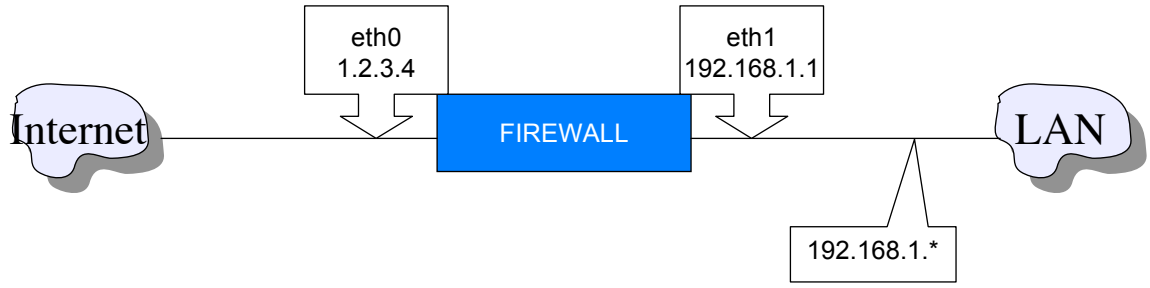
Esempi




```
#iptables -A INPUT -p tcp -s 1.2.3.5 -d
1.2.3.4 --dport 22 -j ACCEPT

#iptables -A INPUT -p tcp -s 0/0 -d 1.2.3.4 --
dport 22 -j DROP
```

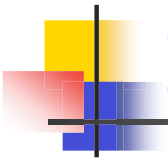
Esempi




```
#iptables -A FORWARD -mac-source
00:60.08:91:CC:B7 -s 192.168.1.5 -d 0/0 -j
ACCEPT
```

I frammenti IP (1)

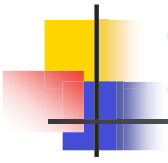
- A volte il pacchetto generato dall'host mittente è troppo grande per attraversare alcune reti, viene quindi frammentato
- Il frammento contiene un sottoinsieme dell'header, non è quindi possibile verificare le intestazioni TCP, UDP e regole come –p tcp, --sport non possono essere verificate



I frammenti IP (2)

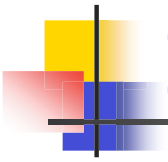
- C'è la possibilità di dare una regola specifica per i frammenti, attraverso l'opzione –f
- Esempio:

```
#iptables -A OUTPUT -f -d 192.168.1.69
-j DROP
```



I flag TCP

- Si possono filtrare i pacchetti attraverso i flag specifici di TCP
- --tcp-flags seguita da 2 stringhe di flag:
  - la prima stringa è la maschera:lista di flag che si vogliono esaminare
  - la seconda indica quali flag devono essere impostati

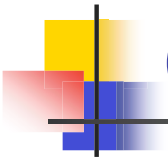


I flag TCP (esempio)

Voglio fare il log di tutte le connessioni TCP che passano dal firewall

```
#iptables -A FORWARD -p tcp -tcp-flags
  ALL SYN,FIN -j LOG
```

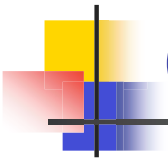
--syn è un'abbreviazione di –tcp-flags SYN,RST,ACK SYN



Connection tracking (1)

Capacità per un firewall di mantenere memoria dello stato delle connessioni.

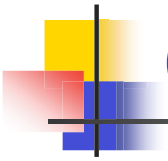
Si usa l'opzione --state seguita da una lista di stati da confrontare.



Connection tracking (2)

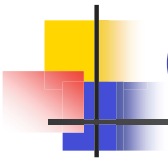
Questi stati sono:

- NEW
  un pacchetto che crea una nuova connessione
- ESTABLISHED
  un pacchetto che appartiene a una connessione esistente



Connection tracking (3)

- RELATED
  pacchetto relativo a una connessione esistente di cui non fa parte (es. errore ICMP, FTP data)
- INVALID
  pacchetto che non può essere identificato (in genere va scartato)



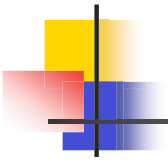
Connection tracking (esempi)

```
#iptables – A FORWARD –d 192.168.0.0/16
  –m state –-state ESTABLISHED, RELATED
  –j ACCEPT
```

Consente il transito verso 192.168.* per connessioni già realizzate o correlate a connessioni precedenti

```
#iptables – A FORWARD –d 192.168.0.0/16
  –m state –-state INVALID –j DROP
```

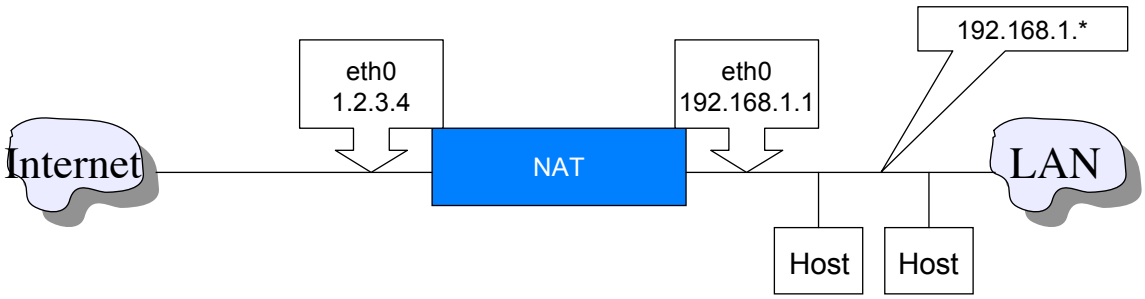
Elimina i pacchetti non identificabili



Network Address Translation (NAT)

- Tecnica descritta nell'RFC 1631, con la quale un nodo di rete speciale acquista funzionalità simili a quelle di un router, allo scopo di sostituire indirizzi IP reali con altri indirizzi più convenienti
- E' possibile riutilizzare dinamicamente gli indirizzi IP privati, permettendo a tali reti di accedere all'esterno, pur non essendo questi univoci a livello globale

NAT

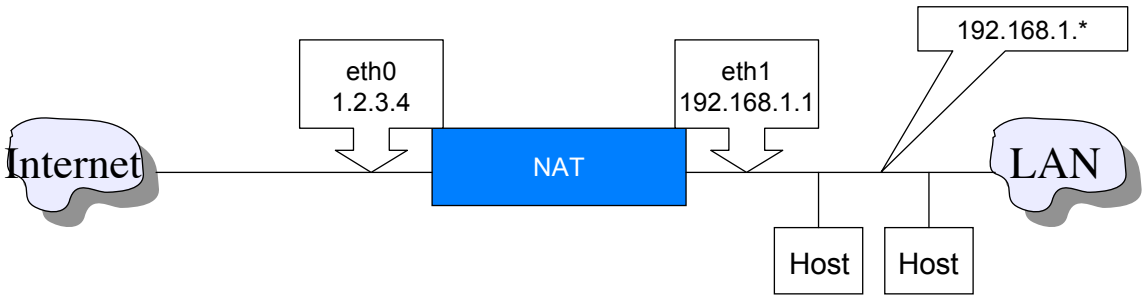


- Normalmente gli indirizzi IP 192.168.1.* non hanno la possibilità di essere riconosciuti univocamente all'interno della rete globale, pertanto non è possibile accedere all'esterno. Si può ottenere attraverso il NAT

NAT

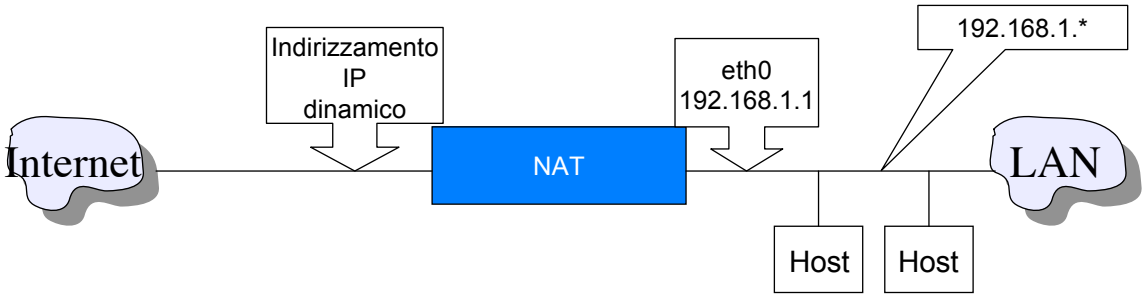
- Souce NAT (SNAT)
  si ha quando si altera l'indirizzo sorgente del pacchetto. E' effettuata in fase di post-routing
- Destination NAT (DNAT)
  si ha quando si altera l'indirizzo di destinazione, ossia si cambia dove la connessione è diretta. Si effettua in fase di pre-routing

SNAT



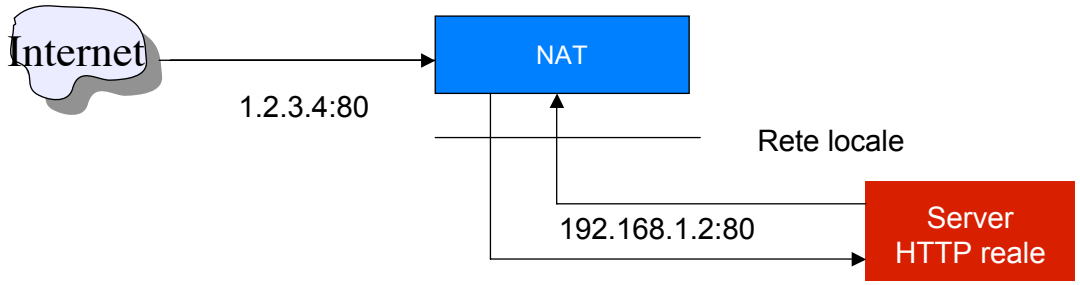

```
#iptable -t nat -A POSTROUTING -o eth0 -j
  SNAT -to-source 1.2.3.4
```

SNAT (mascheramento)



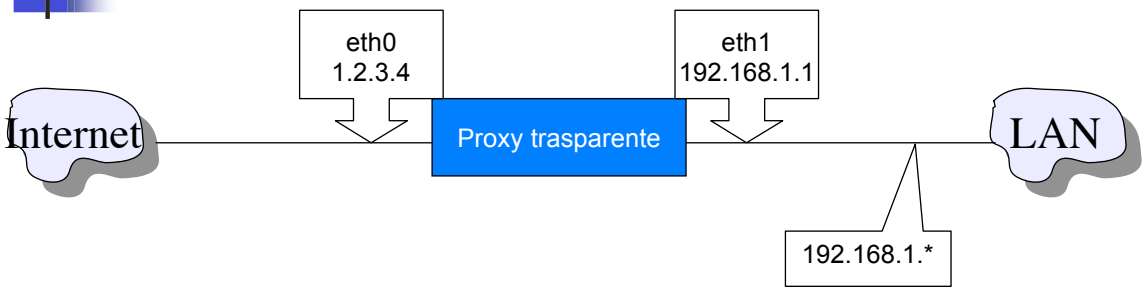

```
#iptables -t nat -A POSTROUTING -o ppp0
  -j MASQUERADE
```

DNAT



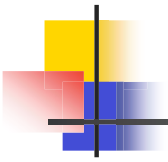

```
#iptables -t nat -A PREROUTING -p tcp --
  dport 80 -i eth0 -j DNAT -to-
  destination 192.168.1.2
```

DNAT (redirect)



Si vuole che tutte le richieste di servizi HTTP, da parte della rete locale, siano dirottati verso il proxy, sullo stesso computer che ospita il NAT, alla porta 8080

```
#iptables -t nat -A PREROUTING -p tcp
  -dport 80 -i eth1 -j REDIRECT -to-port
  8080
```



Bibliografia

- Rusty Russel, Linux 2.4 Packet filtering HOWTO
  http://www.netfilter.org/documentation/HOWTO/packet-filtering-HOWTO.html
- Rusty Russel, Linux 2.4 NAT HOWTO
  http://www.netfilter.org/documentation/HOWTO/NAT-HOWTO.html
- Oskar Andreasson, Iptables tutorial
  http://iptables-tutorial.frozentux.net/
- Manpage di iptables