Linux Desktop Security

Giuseppe Augiero

Augiero.it

Sicurezza del proprio Destktop

Le cose da fare

Il network

Stack Tcp/IP

- Lo stack Tcp/IP nasce per esigenze militari di affidabilità e non di sicurezza.
- L'attuale versione (v4) dello stack Tcp/ip non offre funzionalità di sicurezza.
- E' facile falsificare informazioni di trasporto di un datagram Ip (ip sorgente, destinazione, tos).
- Il payload può essere letto da chiunque ne venga in possesso.

Nat

- Il Nat permette di modificare l'indirizzo Ip dei pacchetti che transitano su un router.
- Perché utilizzare il nat ?
- **Nat crea un falso senso di sicurezza.**

Firewall

Firewall

- E’ un sistema di protezione perimetrale tra due reti (per esempio: Lan e Internet).
- Un firewall, è un dispositivo che connette una rete fidata “**trusted**” (presumibilmente sicura) con una rete non fidata “**untrusted**” (potenzialmente insicura).
- Tutto il traffico da e verso Internet deve passare da un unico nodo (il firewall).
- Il firewall non deve essere visibile.

Punti di Forza

- Centralizza le politiche di sicurezza.
- Centralizza i log e i messaggi di allarme.
- Previene il foot-printing.
- Permette di usare sistema di strong security.

Tipologie di firewall

- Packet filters e screening routers.
- Application gateways e proxy servers.
- Stateful inspection.
- Soluzioni ibride.

Packet Filter

- Un packet filtering firewall semplicemente esamina l'intestazione di ciascun pacchetto (IP) e decide se lasciarlo transitare o di bloccarlo in funzione delle regole definite dall'amministratore del firewall.

- **Vantaggi:**

- Economicità e funzioni di packet filtering svolte anche a livello di router.

- **Svantaggi:**

- Reporting degli eventi limitato

Stateful Inspection

- I firewall che offrono funzionalità di stateful packet inspection mantengono informazioni sullo stato della connessione.

- Mantenendo una tabella delle connessioni correnti e dei loro eventi, sono in grado di rilevare sequenze anomale che potrebbero rappresentare degli attacchi.

Stateful Inspection (II)

- **Aspetti negativi:**
  - Non effettuano controlli profondi a livello applicazione.
  - Non permettono controlli sull'autenticazione utenti.

Application Gateway

- Utilizzano un set di proxy, uno per ogni applicazione.
- Possono richiedere o no la connessione iniziale.
- Possono forzare l'autenticazione utente.
- Funzionano da intermediari e ogni sessione è sempre il risultato di due connessioni:
  - Client Firewall.
  - Firewall Server.

Application Gateway (II)

- **Vantaggi:**
  - Consente al Firewall di riscrivere l'IP header.
  - Non attaccabile con procedimenti basati su routing.
- **Svantaggi:**
  - Prestazioni condizionate dalla profondità e complessità dei controlli.

Limiti

- Non protegge contro virus e trojan.
- Non protegge contro nuovi (sconosciuti) attacchi.
- Non protegge contro le connessioni che non lo attraversano.
- Non protegge da cattive o inesistenti policy.
- Non protegge da attacchi interni (75%-80%).
- Non protegge da attacchi fisici.
- Non può fungere da unico punto di difesa.

Le regole

- Definizione di una lista in cui ogni elemento (**regola**) definisce se un particolare tipo di traffico deve passare o non passare.
- Possibilità di utilizzare operatori relazionali.
- **E' importante l'ordine delle regole.**

La filosofia del gioco

- Il design delle policy di un firewall può seguire uno dei seguenti approcci:
  - permetto e nego tutto il resto (**+ sicuro**).
  - nego e permetto tutto il resto (**- sicuro**).

Le regole d'oro

- **Stealth rule**:
  - E' buona norma inserire all'inizio della lista, una regola che rende il firewall invisibile.
- **Clean Up rule:**
  - Alla fine della lista occorre inserire una regola che neghi tutto il traffico non permesso (drop su catch-all).
- **Antispoofing e Rfc 1918.**

Architettura di un firewall

- Il firewall può essere un prodotto hardware o software.
- Se il firewall è software occorre “**bastionizzare**” la macchina su cui gira.
- In generale la configurazione di un firewall e’ una operazione complessa.

Netfilter

Iptables

- Iptables e' parte integrante di netfilter.
- **Netfilter** e' il framework di manipolazione dei pacchetti che mette a disposizione il kernel di Linux.
- Supporto kernel 2.4 2.6 e 3.0
- Successore di ipfwadm e ipchains

Come installare iptables

- Iptables e' parte integrante del kernel di Linux.

- Per usare le funzionalità di iptables occorre attivare il supporto di netfilter nel Kernel.

- Ricompilazione del Kernel.

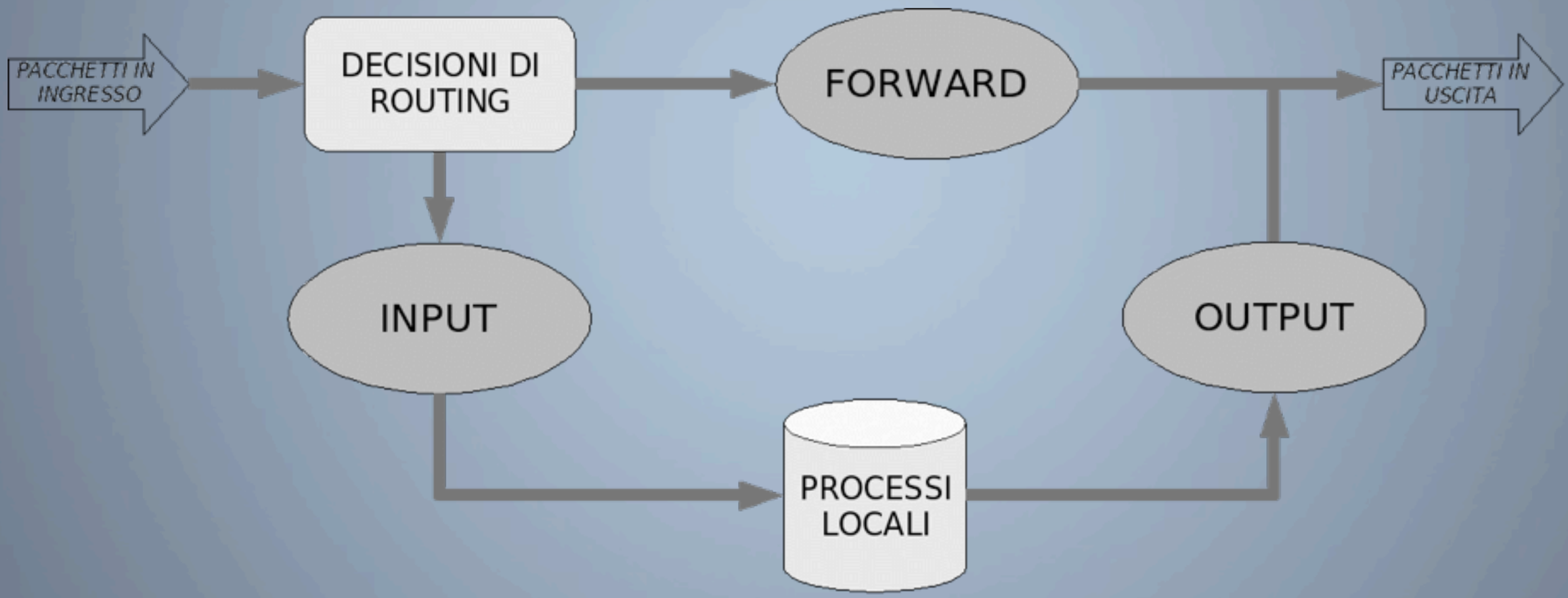
Forwarding

- Per abilitare il forwarding occorre:
  - *echo 1 > /proc/sys/net/ipv4/ip_forward*
  - oppure
  - *editare il file /etc/sysctl.conf*

Struttura del sistema

- Di default iptable e’ composto da tre tabelle:
  - **Filter**
  - **Nat**
  - **Mangle**
- Ogni tabella contiene più catene.
- Ogni catene e’ una lista di regole ordinate.

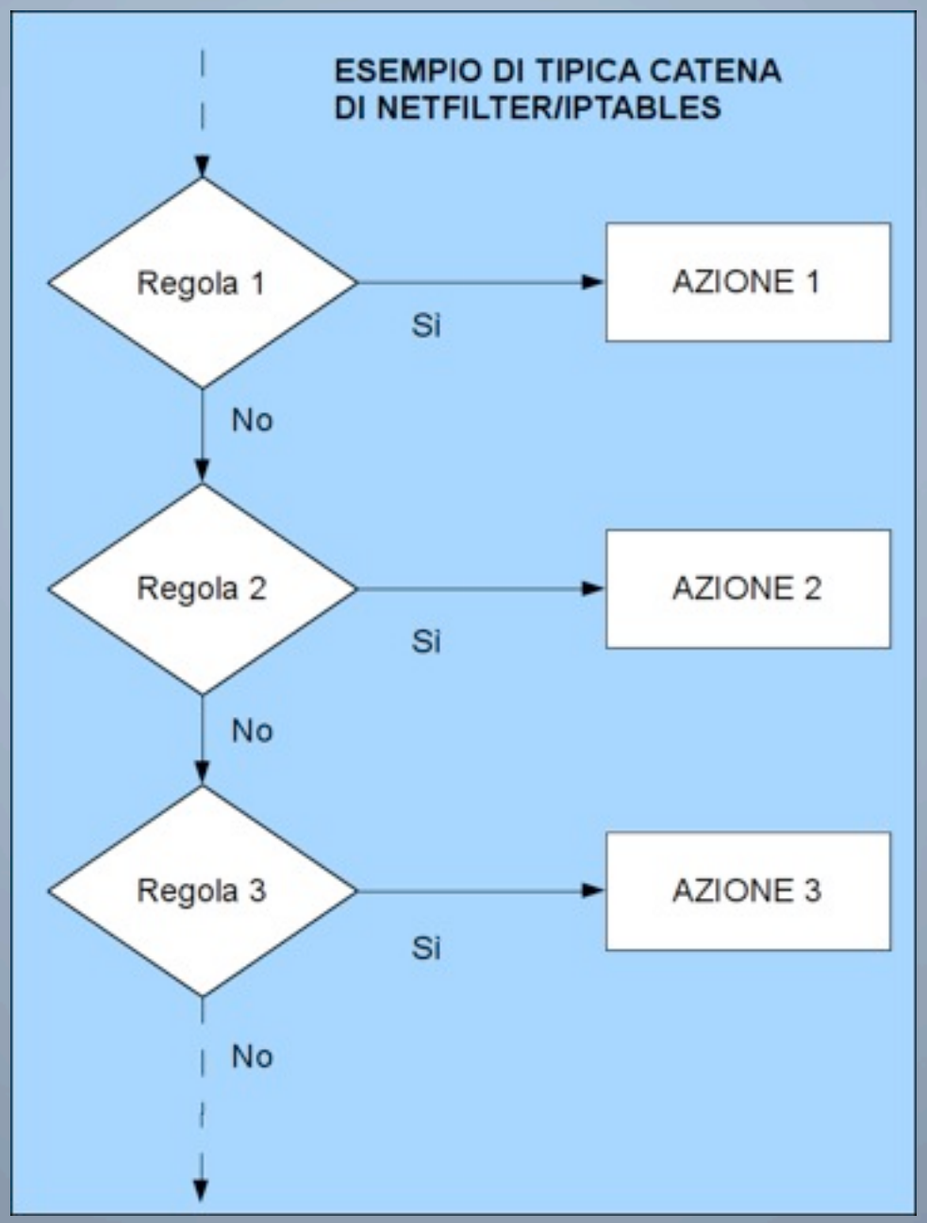
Il percorso


PACCHETTI IN INGRESSO
DECISIONI DI ROUTING
FORWARD
PACCHETTI IN USCITA
INPUT
OUTPUT
PROCESSI LOCALI

Policy

- Di default esistono tre catene (Input/Output/Forward).
- Una catena e’ un insieme di regole
- Ogni regola definisce cosa bisogna fare con il traffico identificato.
- Se non esiste una regola per il traffico viene applicata la policy generale della catena.

Regole



Azioni da intraprendere

- **Accept**
- **Drop (timeout)**
- **Reject**

- Il traffico in drop o reject può essere monitorato e loggato.

Sintassi

Default policy

- L’opzione **-P** permette di definire la policy di default da applicare alla catena:
  - *iptables -P INPUT DROP*

Operazioni sulle catene (I)

- Creare una nuova catena:
  - Opzione `**-N**' oppure `**--new-chain**'
    - *iptables -N test*
- Cancellare una catena:
  - Opzione `**-X**' o `**--delete-chain**'.
    - *iptables -X test*
  - Le catene devono essere vuote.
  - Le 3 catene predefinite non possono essere cancellate.

Operazioni sulle catene (II)

- Svuotare una catena:
  - Il flush della catena viene effettuato con il parametro **-F**
  - *iptables -F forward*
  - Se non si specifica una catena, allora tutte le catene saranno svuotate.
- Consultare una catena:
  - E’ possibile ottenere una lista delle regole di una catena usando il comando `**-L**' (o `**--list**').
  - *iptables -L*

Operazioni sulle regole

- Una regola può essere:
  - Aggiunta a una catena (**--append** oppure **-A**).
  - Cancellata da una catena (**--delete** oppure **-D**).
  - Rimpiazzata in una catena (**--replace** oppure **-R**).
  - Inserita in una catena (**--insert** oppure **-I**).
    - *iptables -A INPUT -s 1.1.1.1 -j DROP*

Definizione di una regola

- **-p** procotollo.
- **-s** source ip address.
- **-d** destination ip source.
- **-i** interfaccia di rete.
- **--sport** porta sorgente.
- **--dport** porta destinazione.
- **--tcp-flags** (Syn/Ack/Fin/Rst).
- **-j** azione da intraprendere.

Nat

- Iptables permette di gestire anche il nat.
- La regola da utilizzare per nattare i pacchetti è :
  - **iptables -t nat -A POSTROUTING -o [wan-int] -j MASQUERADE**

Mangle

- La tabella di Mangle e' un tabella particolare usata per manipolare i pacchetti.
- E' possibile marcare i pacchetti (MARK).
- Modificare il TOS.
- Modificare il TTL.

Catene di mangle

- Le catene che troviamo nella tabella Mangle sono:

- **Pre Routing.**
- **Post Routing.**

Tracking

- Attraverso il modulo **ip_conntrack** è possibile tenere traccia delle connessioni.
- Il tracciamento ci permettete di capire se un dato pacchetto fa parte di una determinata connessione.

Stato delle sessioni

- **NEW** – Il pacchetto non e' correllato a nessuna connessione ed e' teso a creare una nuova connessione.

- **ESTABLISHED** – Il pacchetto appartiene a una connessione (p.es un pacchetto di risposta).

- **RELATED** – Il pacchetto e' correlato ma non appartiene a nessuna connessione esistente (p.es. icmp o ftp).

- **INVALID** - Non e' stato possibile ricavare lo stato del pacchetto.

Sintassi

- Le opzioni di iptables per controllare lo stato del pacchetto sono:

- *iptables -m state –state NEW, ESTABLISHED, RELATED, INVALID*

Ripulire le catene

- *iptables –F INPUT*
- *iptables –F FORWARD*
- *iptables –F OUTPUT*

Esempi pratici

Iptables utility

- Per salvare la regole definite in iptable:
- ***iptables-save > file***

- Per ripristinare le regole salvate:
- ***iptables-restore < file***

Il nostro primo script

- Impostiamo una politica di default.

- ***iptables –P INPUT DROP***
- ***iptables –P FORWARD DROP***
- ***iptables –P OUTPUT ACCEPT***

Traffico ssh

- Vogliamo che il traffico ssh verso la nostra macchina sia consentito:

- ***iptables –A INPUT –p tcp –d 4.4.4.4 –dport 22 –j ACCEPT***

Traffico dalla nostra lan

- Per accettare il traffico in ingresso da una specificata subnet possiamo definire la regola:
- ***iptables –A INPUT –s 4.4.4.0/24 –j ACCEPT***

Bloccare un ip

- Per bloccare tutto il traffico proveniente da un determinato Ip possiamo definire la regola:

- ***iptables –A INPUT –s 1.1.1.1 –j DROP***

Bloccare ssh

- Per bloccare il traffico ssh provenienete da un determinato Ip possiamo definire la regola:

- ***iptables –A INPUT –s 1.1.1.1 –p tcp –dport 22 –j DROP***

Linux Desktop Security

Giuseppe Augiero

Augiero.it