IPTABLES

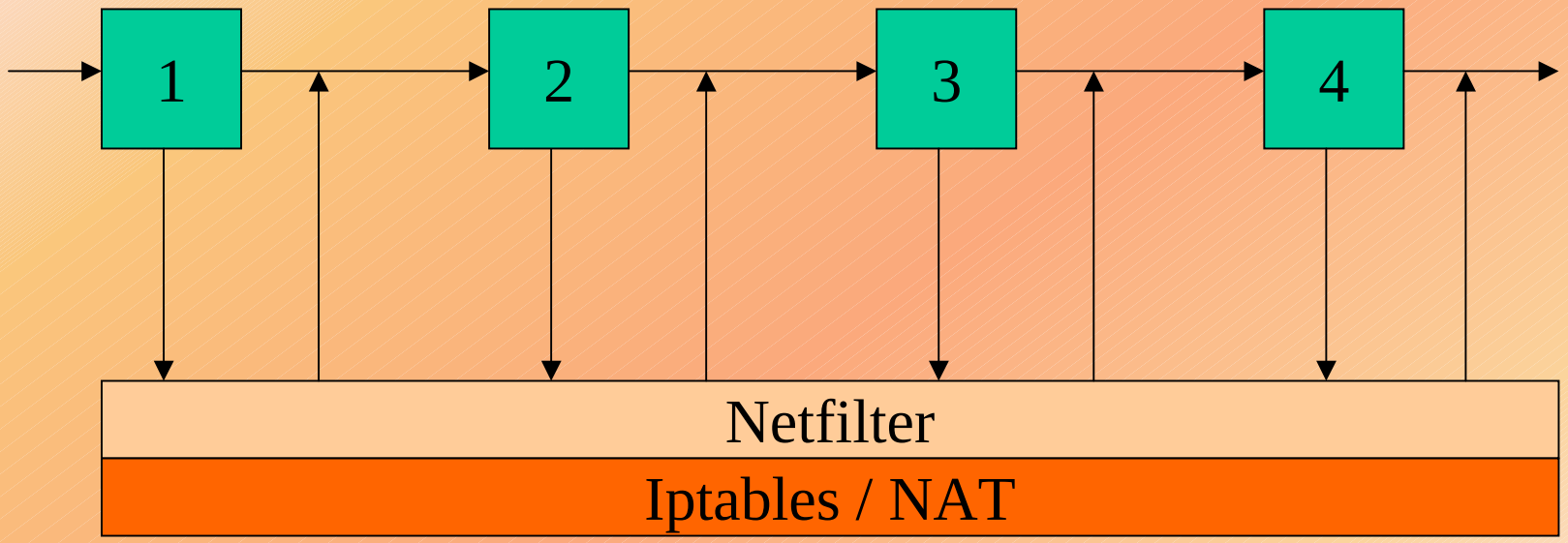
Un’Introduzione

NETFILTER (1)

- netfilter è un framework per il manipolamento dei pacchetti, esterno alla normale interfaccia socket Berkeley. Consta dei seguenti punti:
  1. ogni protocollo definisce degli "hook" (IPv4 ne definisce 5) i quali sono punti ben definiti in una traversata dei pacchetti nel protocol stack. In ciascuno di questi punti, il protocollo richiamerà il framework netfilter fornendo il pacchetto e il numero dell'hook.
  2. porzioni del kernel possono registrarsi per "ascoltare", per ogni protocollo, differenti hook. Perciò quando un pacchetto è passato al framework netfilter, esso controlla se qualcuno si è registrato per quel determinato protocollo e hook; se sì, a ciascuno di essi è data, in ordine, una chance per esaminare (ed eventualmente alterare) il pacchetto, per scartarlo, per lasciarlo proseguire, o per chiedere a netfilter di accodarlo per lo userspace (spazio utente).

NETFILTER (2)

3. i pacchetti che sono stati accodati sono sistemati per essere inviati allo userspace; questi pacchetti sono gestiti in modo asincrono.
4. La parte finale consiste di splendidi commenti sul codice e di una ottima documentazione.



Pacchetto che attraversa il sistema netfilter

NETFILTER (3)

- In aggiunta a questo framework grezzo sono stati realizzati vari moduli che forniscono funzionalità simili ai kernel precedenti (pre-netfilter), in particolare un sistema NAT e uno di filtraggio dei pacchetti (iptables) entrambi estendibili.

IPTABLES

- Iptables e' l'interfaccia utente per l'impostazione di filtri eseguiti da netfilter a livello di Kernel (disponibile in tutte le versioni di Linux)
- E' l'evoluzione di ipchains, entrambi sviluppati da Rusty Russell
- Si raccomanda, ovviamente, di scegliere la versione più aggiornata di questo modulo per non incorrerre in vulnerabilità ormai pubblicamente riconosciute da cui sono affette le vecchie versioni.
- In grado di effettuare filtering su protocolli IPv4, IPv6, Decnet, etc.

Tipologie di filtri

- Controlla e verifica 3 tipi diversi di flussi attraverso la definizione di altrettante tabelle o chains:
  - **Input**
  - **Output**
  - **Forward**
- Oltre alle 3 tabelle citate se ne possono creare altre personalizzate per scopi specifici
- E’ in grado di effettuare i LOG

Tipologie di filtri

- All’ interno di ciascuna tabella effettua il controllo su:
  - Input e Output Interface
  - Source MAC Address
  - Source e destination IP Address
  - Invalid Packets (CRC error, frammenti, etc)
  - Protocol (IP, TCP, UDP, ICMP, etc.)
  - Source e destination port (TCP e UDP)
  - Flag TCP (SYN, FIN, ACK, RST, URG, PSH, ALL, NONE)
  - Rate limit
  - Etc.

Politiche applicabili

- Per ogni pacchetto analizzato, iptables e' in grado di applicare le seguenti politiche:
  - **ACCEPT** (accetta il pacchetto)
  - **DROP e REJECT** (scarta il pacchetto)
  - **QUEUE** (passa il pacchetto allo userspace)
  - **RETURN** (esce dalla access list della attuale tabella e passa il controllo alla successiva tabella)
- La sintassi e' di tipo command line per la costruzione di ACL (Access Control List) sequenziali (per ciascun pacchetto l'esecuzione termina al primo match).

Iptables.acl (1)

```
#!/bin/sh
#

#
#Esegue il  Flushing ed il  Reset di tutti i filtri
#
iptables -F -t filter
iptables -X

#
# Inizializza le tabelle INPUT, OUTPUT, FORWARD ed  esegue il DROP su tutti i pacchetti FORWARD
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP

#
# Costruisce ed esegue il Flushing di una nuova tabella per i pacchetti SYN
#
iptables -N SYN
iptables -F SYN
```

Iptables.acl (2)

```
#
# Accetta tutto dall'interfaccia di loopback
#
iptables -A INPUT -i lo -j ACCEPT

#
# ------ FILTRI Globali------
# Porre qui tutti i filtri che si vogliono sempre in DROP#

# DROP dei pacchetti non validi
#   iptables -A INPUT -i eth0 -m state --state INVALID -j LOG --log-prefix "INVALID PACKETS: "
   iptables -A INPUT -i eth0 -m state --state INVALID -j DROP

# DROP dei pacchetti frammentati
#   iptables -A INPUT -i eth0 -f -j LOG --log-prefix "FRAGMENTS PACKETS: "
   iptables -A INPUT -i eth0 -f -j DROP

#
# DROP dei pacchetti provenienti da reti sospette (spoofing)
   iptables -A INPUT -i eth0 -s 127.0.0.0/8 -j DROP
   iptables -A INPUT -i eth0 -s 224.0/8 -j DROP
   iptables -A INPUT -i eth0 -s 172.16.0.0/16 -j DROP
   iptables -A INPUT -i eth0 -s 10.0.0.0/8 -j DROP
```

Iptables.acl (3)

```
# DROP dei pacchetti provenienti dall'esterno con indirizzi appartenenti alla rete interna
#
  # iptables -A INPUT -i eth0 -s 192.168.0.0/16 -j LOG --log-prefix SPOOFING
  # iptables -A INPUT -i eth0 -s 192.168.0.0/16 -j DROP
  #

# REJECT di tutti i pacchetti provenienti dall'esterno con indirizzo di loopback  (quence source attack)
#
  iptables -A INPUT -i eth0 -d 127.0.0.0/8 -j DROP

# REJECT di tutte le nuove connessioni TCP che non seguano il normale handshake e quindi non inizino con un pacchetto SYN
#
  iptables -A INPUT -i eth0 -p tcp ! --syn -m state --state NEW -j REJECT

# ------ FILTRI per il protocollo ICMP ------
  #
  # ACCEPT di ogni Ping provenienti dalla rete interna (xxx.xxx.xxx.0/21), ACCEPT dei Ping provenienti dalla rete WAN con un
      rate di 2/sec, DROP di tutto il resto  #
  iptables -A INPUT -i eth0 -p icmp --icmp-type echo-request -s  xxx.xxx.xxx.0/21 -j ACCEPT
  iptables -A INPUT -i eth0 -p icmp --icmp-type echo-request -m limit --limit 2/s -s ! xxx.xxx.xxx.0/21 -j ACCEPT
#   iptables -A INPUT -i eth0 -p icmp --icmp-type echo-request -j DROP  (redundant)
#
# ------ FINE  ICMP ------
```

Iptables.acl (4)

```
# ------ FILTRI ------
  # ACCEPT di tutte le connessioni TCP ESTABLISHED
  #
  iptables -A INPUT -i eth0 -p tcp -m state --state ESTABLISHED -j ACCEPT

  # ACCEPT di tutte le connessioni UDP ESTABLISHED
  #
  iptables -A INPUT -i eth0 -p udp -m state --state ESTABLISHED -j ACCEPT

  # ACCEPT di tutte le nuove connessioni TCP ed invio alla tabella SYN per il filtraggio   #
  iptables -A INPUT -i eth0 -p tcp --syn -j SYN

  # Caratteristiche della tabella SYN::
  # ACCEPT di tutte le nuove connessioni alla porta 2 solamente se provenienti dalla rete interna LAN con un rate di 3/sec   #
      ACCEPT di tutte le nuove connessioni alla porta 80  provenienti da qualsiasi rete
      ACCETT di tutte le nuove connessioni alla porta 3128 solamente dalla rete interna LAN   #
  iptables -A SYN -p tcp --destination-port 80 -j ACCEPT
  iptables -A SYN -p tcp --destination-port 3128 -s  xxx.xxx.xxx.0/21 -j ACCEPT
  iptables -A SYN -p tcp --destination-port 22 -s  xxx.xxx.xxx.0/21 -m limit --limit 3/s --limit-burst 2 -j ACCEPT

  # REJECT di tutto il resto
  #
  iptables -A SYN -j REJECT
```

Iptables.acl (5)

```
#REJECT di tutto il TCP
#
   iptables -A INPUT -i eth0 -p tcp -j REJECT

# ACCEPT di tutti i pacchetti UDP indirizzati alla porta 7001 #
   iptables -A INPUT -i eth0 -p udp --destination-port 7001 -j ACCEPT

# REJECT di tutti i pacchetti UDP
#
   iptables -A INPUT -i eth0 -p udp -j REJECT
#
# ------ FINE  FILTERS ------

# SALVA tutta la configurazione nel file /etc/sysconfig/iptables
#
iptables-save -c > /etc/sysconfig/iptables

# Riavvia il servizio iptables
#
/etc/rc.d/init.d/iptables stop && /etc/rc.d/init.d/iptables start
```

- Riferimenti:
  - http://www.iptables.org/