

IPFW **FIREWALL** su Linux

Corso di Sicurezza su Reti
prof. Alfredo De Santis
Anno accademico 2001/2002



De Nicola Dario
Milano Antonino
Mirra Massimo
Nardiello Teresa Eleonora
Rapoli Ermelinda

56/100081
56/01039
56/100382
56/00395
56/100924

Ipfw Firewall su Linux

Sommario

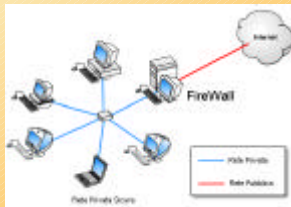
- Che cos'è un firewall
- Architettura di un firewall
- IPFW
- IPFWADM
- IPCHAINS
- IPTABLES
- Installazione
- Configurazione
- Attacchi al firewall



Ipfw Firewall su Linux

Che cos'è un Firewall?

- Firewall: applicazione che ha come scopo la protezione di un singolo sistema posto in rete, un'intera rete o anche più reti interconnesse.



Ipfw Firewall su Linux

Concetto di regola

La regola è la **legge** che stabilisce la possibilità di un pacchetto di entrare nel sistema o di essere scartato.



Ipfw Firewall su Linux

Descrizione di un Firewall

- Consente il passaggio del solo traffico legittimo e blocca ogni eventuale traffico illegittimo.
- Implementato su computer ordinario, oppure su sistemi dedicati



Ipfw Firewall su Linux

Funzione del Firewall...

- Tenere traccia di ogni file che entra o che lascia l'area della rete.
- Controllare l'eventuale sorgente dei virus.



Ipfw Firewall su Linux

Perché dovrei filtrare i pacchetti?

•Controllo

•Sicurezza

•Vigilanza



Ipfw Firewall su Linux

Controllo (1)

- Ci consente di garantire un certo tipo di traffico e di vietarne dell'altro.



Ipfw Firewall su Linux

Controllo (2)

- Guardando l'intestazione dei pacchetti possiamo impedire che quest'ultimi arrivino ad una certa parte della rete esterna.
- Possiamo evitare di accettare materiale inutile proveniente dall'esterno.

Ipfw Firewall su Linux

Sicurezza:

- Possiamo limitare le entrate nella nostra rete (esempio: "Ping della morte").
- Possiamo permettere a qualsiasi cosa di uscire dalla nostra rete.
- Potremmo voler essere solo degli osservatori della rete e non dei server. A tale scopo impostiamo il filtro dei pacchetti in modo che rifiuti i pacchetti usati per la connessione.



Ipfw Firewall su Linux



Vigilanza:

- Può accadere che qualche macchina della rete configurata male possa decidere di "sparare" pacchetti al mondo esterno.
- E' buona norma chiedere al filtro dei pacchetti di avvisarci nel caso accadano tali anomalie.



Ipfw Firewall su Linux

Architettura di un firewall

- Basi di TCP/IP
- Differenze tra Packet Filter e Application Proxy
- Stateful Inspection
- Introduzione al Nat

Ipfw Firewall su Linux

Connessione ad Internet...

- Uso dei protocolli dello stack TCP/IP (HTTP,FTP,Telnet...).
- I protocolli lavorano su un numero specifico di porta. Se gli accessi non sono controllati un hacker potrebbe impadronirsi della nostra macchina.



Ipfw Firewall su Linux

TCP/IP

- Protocollo di comunicazione per connettere Internet e le reti esterne
- Ideato per garantire una comunicazione affidabile
- Non tiene conto di alcuni problemi inerenti alla sicurezza



Ipfw Firewall su Linux

Esempio:Approccio stratificato

Livelli ISO/OSI

7	APPLICATION
6	PRESENTATION
5	SESSION
4	TRANSPORT
3	NETWORK
2	DATALINK
1	PHYSICAL

Ipfw Firewall su Linux

Classificazione dei Firewalls:

- Applicazioni proxy firewalls.
- Packet filtering firewalls.

Ipfw Firewall su Linux

Applicazioni proxy firewalls "Application Gateway"

- Implementano il firewalling a livello 7.

7 APPLICATION

- Sono implementate sui proxy servers.

Ipfw Firewall su Linux

Applicazioni proxy firewalls

- Il firewall proxy garantisce oppure blocca gli accessi tenendo conto di regole predefinite.
- Tali regole possono essere basate su indirizzi IP, protocolli, porte...

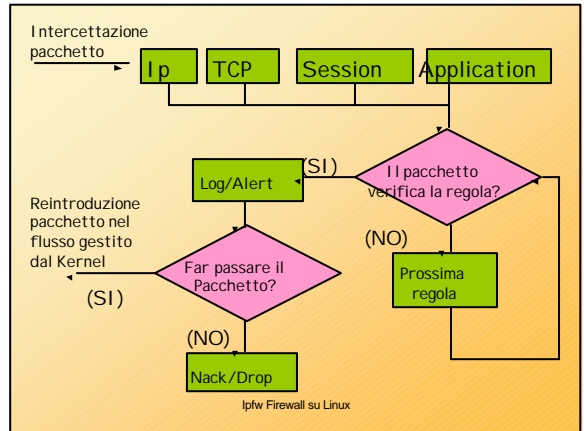


Ipfw Firewall su Linux

Al momento della connessione...

- Il proxy server connette la macchina richiedente la connessione con quella di destinazione.
- Gestisce il trasferimento dei dati da una macchina all'altra.
- Per usare un proxy, tutte le macchine client dovrebbero essere specificatamente configurate per esso.

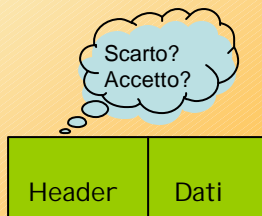
Ipfw Firewall su Linux



Ipfw Firewall su Linux

Packet filtering firewall (filtro dei pacchetti)

- Parte di software che guarda le intestazioni dei pacchetti decidendone il destino.
- In linea di massima può scartare (drop) o accettare (accept).



Ipfw Firewall su Linux

Packet filtering firewall (filtro dei pacchetti)

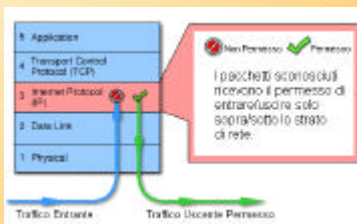
- Se un pacchetto ottiene il permesso viene instradato direttamente a destinazione.
- Non viene controllato il contenuto dei pacchetti!!!



Ipfw Firewall su Linux

Packet filtering firewalls (1)

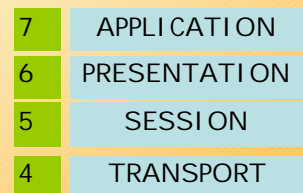
- Lavorano allo strato di rete (livello 3) e sono più veloci dei proxy firewalls.



Ipfw Firewall su Linux

Packet filtering firewalls (2)

- Alcuni Packet Filter ignorano i quattro strati superiori.
- A volte viene controllato anche lo strato di Trasporto



Ipfw Firewall su Linux

Vantaggi

Packet Filter:	Application Proxy:
Economico nelle risorse	Buon livello di sicurezza
Trasparente all'utente della rete	Consapevolezza dell'Application layer
Buone prestazioni	

Ipfw Firewall su Linux

Svantaggi

Packet Filter:	Application Proxy:
Livello sicurezza basso	Proxy dedicato per ogni servizio
Accesso limitato dall'header IP	Poco performante
Manipolazione limitata informazioni	Vulnerabile a bug dell'Application Layer

Ipfw Firewall su Linux

Stateful Inspection (1)

- Tecnologia di firewalling introdotta in tempi piuttosto recenti.
- Ideata per soddisfare i seguenti requisiti:
- Informazioni sulla comunicazione (esamina tutti i layers)
- Esame delle comunicazioni precedenti.

Ipfw Firewall su Linux

Stateful Inspection (2)

- Stato derivato dall'applicazione: mantenimento di una sessione di un utente autenticatosi attraverso un'applicazione.
- Manipolazione dell'informazione: si effettuano valutazioni sulle modifiche che l'informazione subisce dalla comunicazione e dall'applicazione.

Ipfw Firewall su Linux

Network Address Translation

- Consente di "tradurre" dinamicamente uno o più indirizzi IP privati in uno o più indirizzi IP pubblici e viceversa.

Vantaggi:

1. Risparmio spazio indirizzi pubblici
2. Maggiore protezione rete privata
3. Flessibilità nella configurazione di una DMZ.

Ipfw Firewall su Linux

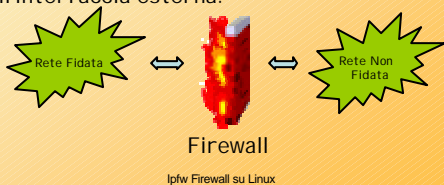
Modalità di setup...

- Dual Homed setup
- De-Militarized Zone setup

Ipfw Firewall su Linux

Dual Homed setup

- I pacchetti che attraversano le due reti passano attraverso il firewall.
- Un pacchetto proveniente dalla rete esterna "non fidata" deve prima approdare all'interfaccia esterna.



Dual Homed setup

- Il firewall confronta il pacchetto con le regole di accesso predefinite.
- Accesso consentito: il firewall instrada il pacchetto alla rete interna privata tramite l'interfaccia interna.



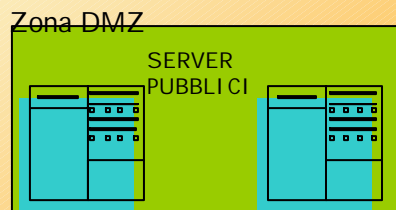
De-Militarized Zone setup (1)

- Facilita le funzioni di accesso al web, posta elettronica....
- Le macchine della rete privata sono protette da regole di accesso molto ferree.



De-Militarized Zone setup (2)

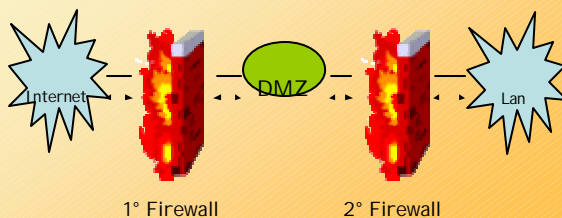
- I server pubblici risiedono in un'area detta "De-Militarized Zone".



De-Militarized Zone (3)

Controlla regole di accesso delle persone che attraversano l'Internet per connettersi ai server pubblici

Controlla le regole degli accessi alla rete privata.



IPFW

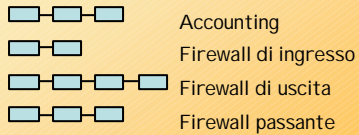
Il firewall IP e le capacità di accounting del kernel Linux offrono:

- conteggio pacchetti IP
- firewall basati sul filtraggio dei pacchetti



Descrizione (1)

La gestione dell'accounting e del firewall IP è basata su 4 liste mantenute nel kernel:



Ipfw Firewall su Linux

Descrizione (2)

Ogni regola specifica:

- indirizzi mittente e destinatario
- protocolli usati
- numeri di porta e altre caratteristiche dei pacchetti

match: corrispondenza tra pacchetto e regola

Ipfw Firewall su Linux

Accounting

Regole di accounting: pacchetti IP trasmessi o ricevuti tramite una delle interfacce di rete locali

Conteggio pacchetti e byte



Ipfw Firewall su Linux

Firewall di ingresso

Gestione pacchetti entranti



Primo match determina il comportamento ("policy") da tenere

Contatori di pacchetti e byte per la regola

Ipfw Firewall su Linux

Firewall di uscita

Gestione pacchetti uscenti



Primo match determina il comportamento ("policy") da tenere

Contatori di pacchetti e byte per la regola

Ipfw Firewall su Linux

Firewall passante

Gestione pacchetti spediti da un host remoto e destinati ad un host remoto



Primo match determina il comportamento ("policy") da tenere

Contatori di pacchetti e byte per la regola

Ipfw Firewall su Linux

Policy (1)

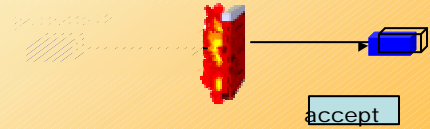
Azione che deve essere intrapresa quando un pacchetto corrisponde ad una regola (non specificata per le regole di accounting)

Nessun match → applica policy di default

Ipfw Firewall su Linux

Policy (2)

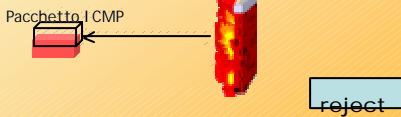
3 differenti comportamenti possibili:



Ipfw Firewall su Linux

Policy (3)

3 differenti comportamenti possibili:



Ipfw Firewall su Linux

Policy (4)

3 differenti comportamenti possibili:



Ipfw Firewall su Linux

Esempi (1)



Il pacchetto passa per le regole di accounting
Poi per il firewall di ingresso
Se viene accettato viene spedito alla destinazione locale

Ipfw Firewall su Linux

Esempi (2)



Il pacchetto passa per le regole di accounting
Poi per il firewall di ingresso
Se viene accettato passa per il firewall di uscita
Se viene accettato passa per le regole di accounting e viene spedito alla destinazione remota

Ipfw Firewall su Linux

Redirect

Ridirezione pacchetti entranti ad un socket locale



Kernel compilato con l'opzione
CONFIG_IP_TRANSPARENT_PROXY attiva

Ipfw Firewall su Linux

Masquerading (1)

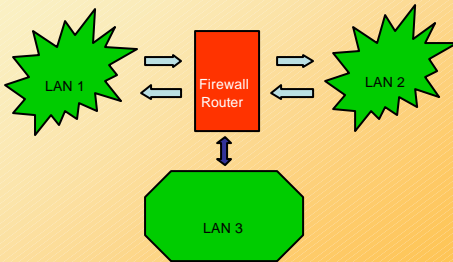
Mascheratura pacchetti entranti destinati ad un host remoto



Kernel compilato con l'opzione
CONFIG_IP_MASQUERADE attiva

Ipfw Firewall su Linux

Masquerading (2)



Ipfw Firewall su Linux

Files

`/proc/net/ip_acct` (regole di accounting)
`/proc/net/ip_input` (regole firewall di ingresso)
`/proc/net/ip_output` (regole firewall di uscita)
`/proc/net/ip_forward` (regole firewall passante)
`/proc/net/ip_masquerade` (sessioni mascherate)

Ipfw Firewall su Linux

setsockopt (funzione C)

La gestione del firewall IP può avvenire tramite chiamate alla funzione:

```
int setsockopt(int socket, IPPROTO_IP, int command,  
void *data, int length)
```

socket IP "raw"

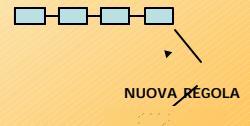
lunghezza di ciò che è puntato da data

Costante: opzione IP

Ipfw Firewall su Linux

Valori di *command* (1)

- IP_ACCT_APPEND
- IP_FW_APPEND_IN
- IP_FW_APPEND_OUT
- IP_FW_APPEND_FWD



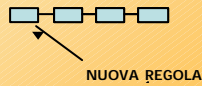
Appendi in coda alla lista

data puntatore ad una struttura **ip_fw**

Ipfw Firewall su Linux

Valori di *command* (2)

- IP_ACCT_INSERT
- IP_FW_INSERT_IN
- IP_FW_INSERT_OUT
- IP_FW_INSERT_FWD



Inserisci all'inizio della lista

data puntatore ad una struttura **ip_fw**

Ipfw Firewall su Linux

Valori di *command* (3)

- IP_ACCT_DELETE
- IP_FW_DELETE_IN
- IP_FW_DELETE_OUT
- IP_FW_DELETE_FWD



Cancella dalla lista la prima corrispondenza con ciò che è puntato da *data*

data puntatore ad una struttura **ip_fw**

Ipfw Firewall su Linux

Valori di *command* (4)

- IP_ACCT_ZERO
- IP_FW_ZERO_IN
- IP_FW_ZERO_OUT
- IP_FW_ZERO_FWD



Azzerata tutti i contatori della lista

data intero (non viene utilizzato)

Ipfw Firewall su Linux

Valori di *command* (5)

- IP_ACCT_FLUSH
- IP_FW_FLUSH_IN
- IP_FW_FLUSH_OUT
- IP_FW_FLUSH_FWD



Rimuovi tutte le regole della lista

data intero (non viene utilizzato)

Ipfw Firewall su Linux

Valori di *command* (6)

- IP_FW_POLICY_IN
 - IP_FW_POLICY_OUT
 - IP_FW_POLICY_FWD
- Cambia il comportamento di default della lista

Valori di *data* :

- IP_FW_F_ACCEPT (accept)
- IP_FW_F_ACCEPT | IP_FW_F_MASQ (accept+masquerading nel firewall passante)
- IP_FW_F_ICMPRPL (reject)
- 0 (deny)

Ipfw Firewall su Linux

Valori di *command* (7)

- IP_FW_MASQ_TIMEOUTS
- Assegna timeout mascheratura



data puntatore ad una struttura a 3 interi:

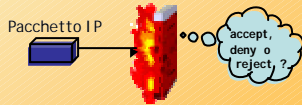
- timeout per sessioni TCP
- timeout per sessioni TCP che hanno già ricevuto FIN
- timeout per sessioni UDP

timeout=0 → non modificare il valore attuale

Ipfw Firewall su Linux

Valori di *command* (8)

- IP_FW_CHECK_IN
- IP_FW_CHECK_OUT
- IP_FW_CHECK_FWD



Controlla come il pacchetto verrebbe gestito dal firewall

data puntatore ad una struttura **ip_fwpkt**

Ipfw Firewall su Linux

Strutture

- **ip_fw** – indirizzi e porte mittente e destinazione, netmasks, indirizzo e nome interfaccia di rete, protocollo, policy, ridirezione, mascheramento, altri flags
- **ip_fwpkt** – header IP, header TCP o UDP o ICMP, indirizzo interfaccia di rete

Ipfw Firewall su Linux

Valore restituito

- **0** (in caso di successo)
- **-1** (in caso di errore)

Con comandi del tipo IP_FW_CHECK_XXX

- **0** (accept senza redirect o masquerading)
- **-1** **errno=ECONNABORTED** (accept+redirect)
- **errno=ECONNRESET** (accept+masquerading)
- **errno=ETIMEDOUT** (deny)
- **errno=ECONNREFUSED** (reject)

Ipfw Firewall su Linux

ipfwadm (comando shell)

Usato per preparare, gestire ed ispezionare il firewall IP e le regole di accounting

Sintassi:

ipfwadm *categoria comando parametri opzioni*

Ipfw Firewall su Linux

Categorie (1)

- **-A**
regole di accounting



- **-M**
amministrazione del masquerading



può essere usata solo in combinazione con il comando **-l** (list) o **-s** (set timeout values)

Ipfw Firewall su Linux

Categorie (2)

- **-I**
regole per il firewall di ingresso



- **-O**
regole per il firewall di uscita



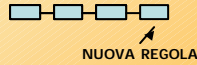
- **-F**
regole per il firewall passante



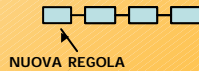
Ipfw Firewall su Linux

Comandi (1)

- **-a**
appende in coda alla lista



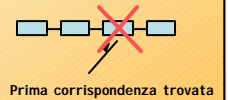
- **-i**
inserisce all'inizio della lista



Ipfw Firewall su Linux

Comandi (2)

- **-d**
cancella dalla lista la prima corrispondenza con la regola specificata



- **-l**
elenca tutte le regole della lista



Ipfw Firewall su Linux

Comandi (3)

- **-z**
azzerata tutti i contatori della lista



- **-f**
rimuovi tutte le regole della lista



Ipfw Firewall su Linux

Comandi (4)

- **-p**
cambia il comportamento di default della lista

- **-s tcp tcpfin udp**
assegna timeout mascheratura



può essere usato solo in combinazione con la categoria **-M**

Ipfw Firewall su Linux

Comandi (5)

- **-c**
controlla come il pacchetto verrebbe gestito dal firewall
può essere usato solo in combinazione con le categorie **-I**, **-O** o **-F**



- **-h**
help sulla sintassi dei comandi



Ipfw Firewall su Linux

Comandi (6)

Se si usano i comandi **-a**, **-i**, **-d** e **-p** per le liste di firewall bisogna specificare di fianco al comando uno dei seguenti comportamenti:

- *accept*
- *deny*
- *reject*

Ipfw Firewall su Linux

Parametri

- **-P**
protocollo
- **-S indirizzo**
indirizzo mittente
- **-D indirizzo**
indirizzo destinatario
- **-V indirizzo**
indirizzo interfaccia di rete
- **-W nome**
nome interfaccia di rete

Ipfw Firewall su Linux

Principali opzioni

- **-m**
masquerading
- **-r**
redirect
- **-e**
output esteso

Ipfw Firewall su Linux

IPCHAINS



- Come passano i pacchetti attraverso i filtri;
- usare ipchains;
- regole di filtraggio;
- cambiare le regole di firewall;

Ipfw Firewall su Linux

Un kernel con il filtraggio dei pacchetti

Lo strumento ipchains dialoga con il kernel e lo istruisce su quali pacchetti filtrare. I pchains inserisce e cancella regole dalla sezione di filtraggio dei pacchetti.

Ipfw Firewall su Linux

Filtraggio dei pacchetti

Il kernel parte con tre elenchi di regole.

firewall chains (catene firewall).

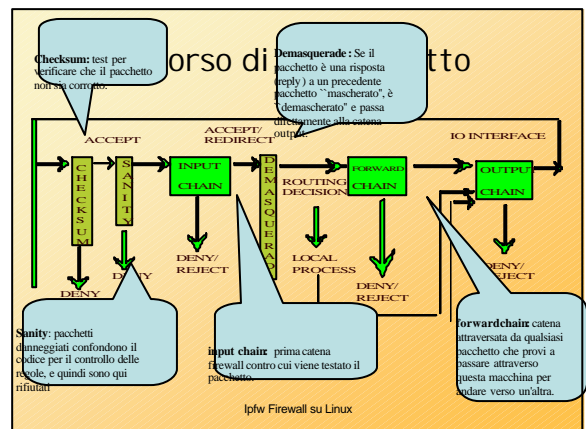
Catene predefinite :

- **input** (ingresso)
- **output** (uscita)
- **forward** (inoltro)

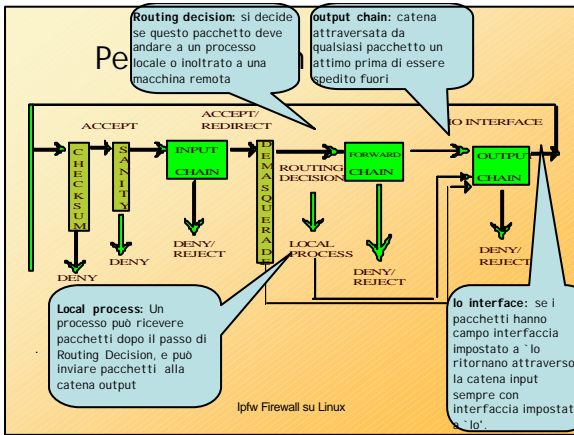
Una catena è una lista di **regole**. Ogni regola dice :

<<se l'intestazione del pacchetto è fatta così, allora questo è quello che si deve fare con il pacchetto>>.

Ipfw Firewall su Linux



Ipfw Firewall su Linux



Usare il tool IPCHAINS

La sintassi del comando IPCHAINS è data dalla seguente scrittura:

```
ipchains <opzione-di-comando> <filtro> | <regola> | <obiettivo>
```

- N: creazione nuova chains.
- X: cancellazione chains vuota.
- F: cambio della politica di default.
- L: elenco di una rules.
- F: cancellazione di tutte le rules.
- Z: azzeramento del contatore dei byte e dei pacchetti.
- A: inserisce in coda una nuova regola.
- I: inserisce una nuova regola.
- R: rimpiazzamento regola.
- D: cancellazione di una regola.
- M-L: elenco delle connessioni mascherate.
- M-S: impostazione valore di timeout per masq.

ACCEPT DENY REJECT REDIRECT MASQ (come ipfwadm) RETURN: passa alla catena chiamante.

Indicato attraverso un nome: input, forward output.

Regole di filtraggio

- Esempio :
voglio bloccare tutti i pacchetti che arrivano da un certo indirizzo ip della rete.

La regola alla chains di input si basa su questi parametri:

- IP sorgente;
- IP destinazione;
- porta sorgente;
- porta di destinazione;
- tipo di protocollo;
- interfaccia;
- TCP SYN flag attivo

ipfw Firewall su Linux

- La riga di comando sarà del tipo:

```
ipchains -A input -p UDP -s 149.32.227.0/24 -d 0.0.0.0 -j REJECT
```

protocollo mittente destinatario

ipchains -L
avremo questo output:

```
Chain input (policy ACCEPT):
target prot opt source destination ports
REJECT udp ----- pc2.mi.it anywhere any -->any

Chain forward (policy ACCEPT):
Chain output (policy ACCEPT):
```

ipfw Firewall su Linux

Creare una nuova catena

La chiameremo test.

```
ipchains -N test
```

Si possono ora inserire le rules in test.

ipfw Firewall su Linux

Si consideri un pacchetto TCP proveniente da 192.168.1.1 e destinato a 1.2.3.4.

- Entra nella catena input e viene controllato rispetto alla Regola 1:
- La Regola 2 è soddisfatta e il suo obiettivo è Test. Quindi la successiva regola a essere esaminata è la prima di Test. La Regola 1 in Test è soddisfatta ma non specifica un obiettivo, quindi la Regola 2 di Test sarà la
- Questa non è soddisfatta e si è così raggiunta la fine delle catena Test. Si ritorna alla catena input, dove l'ultima regola esaminata era la Regola 2 e quindi ora si passa alla Regola 3.

Cancellare una catena

```
ipchains -X <nomecatena>
```

Non è possibile cancellare nessuna delle tre catene predefinite.

Svuotare una catena

```
ipchains -F <nomecatena>
```



Se non si specifica una catena, saranno svuotate tutte le catene.

Ipfw Firewall su Linux

Specificare un protocollo

Il protocollo viene specificato con l'opzione `-p`.
Nomi dei protocolli:

TCP, UDP o ICMP.

I nomi dei protocolli possono essere preceduti da un `^!` per negarli, con ad esempio `-p !TCP`.

I codici più importanti dei pacchetti ICMP sono:

- 0 echo-reply : ping
- 3 destination-unreachable : traffico UDP/TCP
- 5 redirect : instradamento dei pacchetti
- 8 echo-request : ping
- 11 time-exceeded : traceroute

Ipfw Firewall su Linux

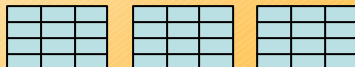
IPTABLES

È molto vicino ad IPCHAINS ma si differenzia da esso per la possibilità di manipolare il pacchetto in diversi punti della macchina.

Una **tabella** rappresenta un punto particolare del cammino del pacchetto

È composto di tre tabelle principali:

- FILTER
- NAT
- MANGLE



FILTER

Composta da tre catene predefinite uguali a quelle di ipchains.

- diretti all'userspace



- uscenti



- passanti



NAT (1)

È consultata per i pacchetti che stanno per creare una nuova connessione (i pacchetti SYN) anche qui ci sono tre catene:

Prerouting: serve a stabilire le regole sui pacchetti appena arrivati. Il controllo avviene prima della "routing decision".

Output: si riferisce ai pacchetti che sono in uscita e sono stati generati in locale.

Postrouting: regola i pacchetti che stanno per lasciare la macchina. Il controllo avviene dopo la routing decision.

MANGLE

Serve a manipolare i pacchetti in entrata o in uscita infatti ha due catene:

- PREROUTING

altera i pacchetti in entrata prima della decisione del routing

- OUTPUT

interviene sui pacchetti in uscita dalla macchina prima del routing decision

TARGET delle REGOLE

Come in IPCHAINS occorre stabilire delle regole tramite le quali il firewall decide la sorte del pacchetto. Le regole di una catena hanno un target che stabilisce cosa fare del pacchetto, esistono quattro target fondamentali:

- ACCEPT
 - DROP
 - REJECT
 - RETURN
 - QUEUE
- come IPCHAINS
- solo IPTABLES

Accoda il pacchetto nella coda dell'userspace

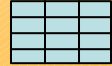
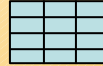


SINTASSI (1)

La sintassi di iptables è molto simile a quelle viste per ipfwadm e ipchains.

Tuttavia per gestire le tabelle sono presenti delle opzioni aggiuntive.

-t <tabella>: permette di gestire le regole delle catene di "tabella"



SINTASSI (2)

--tcp-flags <flags1 flags2>

flags1: indica l'insieme dei flag da esaminare;
flags2: indica quali dovrebbero risultare impostati.

i flag sono SYN, ACK, FIN, RST, URG, PSH.

Esempio:

```
iptables -t FILTER -A INPUT -p tcp  
--tcp-flags ALL SYN,ACK -j DROP
```

--syn si può utilizzare solo con il protocollo tcp, ed è molto utile per impedire i tentativi di connessione verso la propria rete locale.

Installazione del firewall IPFW

Ipfw Firewall su Linux

I kernel Linux hanno da sempre il packet filtering

- Kernel 1.1 - ipfw (ip-firewall) 1994 (Alan Cox – UK)
- Kernel 2.0 - ipfwadm (Jos Vos – NL)
- Kernel 2.2 - ipchains (1998) (Paul Russel – AU)
- Kernel 2.4 - iptables (1999) gestisce oltre al packet filtering, SNAT, DNAT, connection tracking, load balancing, log

Ipfw Firewall su Linux

Esiste il file /proc/net/ip_fwchains?

Sì



Procedere con la configurazione

No



Ricompilare il Kernel

Ipfw Firewall su Linux

Ricompilazione del Kernel

Per i kernel 2.0.x le voci da includere nel file di configurazione della compilazione sono:

```
options CONFIG_EXPERIMENTAL=y
options CONFIG_FIREWALL=y
options CONFIG_IP_FIREWALL=y
options CONFIG_IP_FIREWALL_CHAINS=y
```

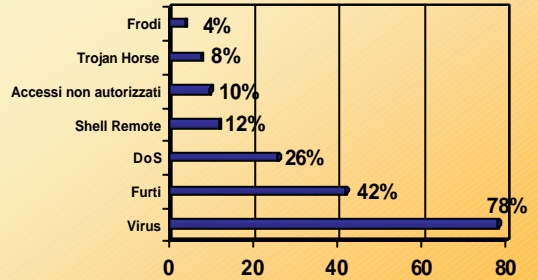
Altrimenti

Per i kernel 2.1.x e 2.2.x è necessario includere:

```
options CONFIG_FIREWALL=y
options CONFIG_IP_FIREWALL=y
```

Ipfw Firewall su Linux

Statistiche



Fonti:


* <http://www.poliziadistato.it/pds/primapagina/virus/virus.html>

* Rivista Network Word Febbraio 2002

Ipfw Firewall su Linux

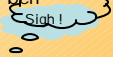
Ci metteremo ora nei panni di chi attacca il firewall. Ci baseremo su alcuni concetti:



- Non esiste il firewall perfetto 
- Ogni anno si scoprono punti vulnerabili in quasi tutti i firewall sul mercato
- In rete esistono innumerevoli firewall:
 - mal configurati
 - non controllati
 - spesso non soggetti a manutenzione

Ipfw Firewall su Linux

Sia ben chiaro!!! Un firewall ben congegnato, ben configurato e tenuto sotto controllo è:



- praticamente impenetrabile 

Quindi è di norma preferibile aggirare il firewall piuttosto che attaccarlo direttamente.

Ipfw Firewall su Linux

Gerarchia degli Attacchi



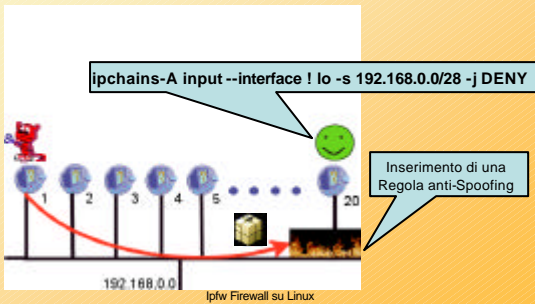
Ipfw Firewall su Linux

Azione del Firewall

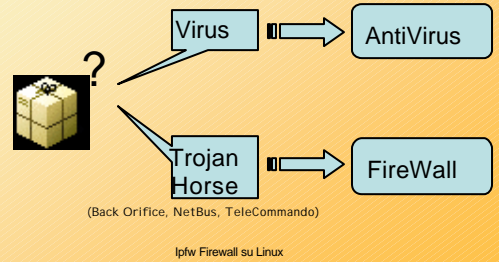


Ipfw Firewall su Linux

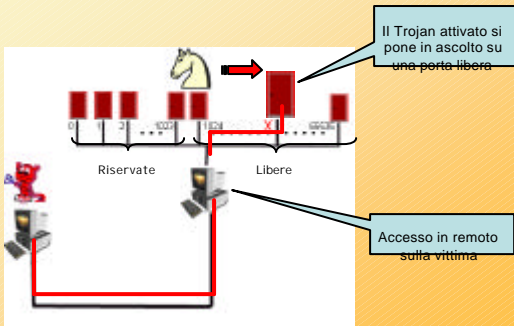
IpChains contro Spoofing



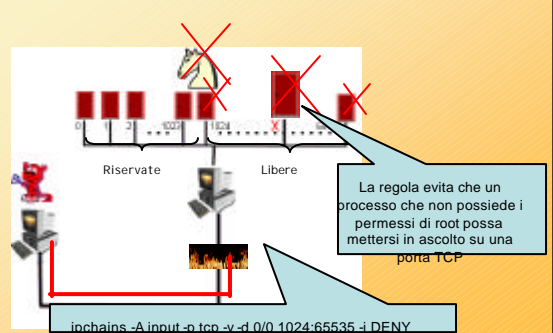
Cosa contiene il pacchetto?



Attacco Trojan Horse (1)

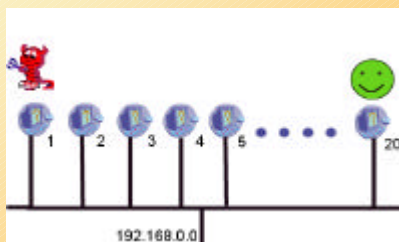


Attacco Trojan Horse (2)



Difesa dagli attacchi "DoS" (1)

Attacco Smurf (ICMP)
Attacco Fraggle(UDP)



Difesa dagli attacchi "DoS" (2)

Attacco Smurf (ICMP)
Attacco Fraggle(UDP)

