PGL – Piccole Guide Linux

http://lgcrsll.altervista.org/pgi/pgl/index.html

Netfilter e Iptables

Luigi Carusillo

lgcrsll@email.it

P G L

I edizione: 27 ottobre 2005

II edizione: 14 settembre 2012

Indice

Introduzione

Un firewall (letteralmente, muro tagliafuoco) è un software di sicurezza che regola il traffico dei pacchetti, consentendo soltanto il traffico desiderato in arrivo, in transito e in partenza da un computer. Ciò al fine di: a) salvaguardare la riservatezza (*privacy*), e b) evitare il malevolo uso a distanza da parte di estranei di un computer come testa di ponte per danneggiare altri computer.

Il firewall di Linux è costituito da ***Netfilter***, incluso nel kernel, e dal programma ***Iptables***: *Netfilter* e *Iptables* sono funzionalmente inscindibili e rappresentano, rispettivamente, la mente e il braccio del firewall di Linux.

Il firewall

Il firewall è organizzato in tabelle (*tables*), suddivise in catene (*chains*), contenenti le regole.

Le tabelle

Il firewall comprende tre tabelle (attraverso le quali agisce):

- ***filter***, che effettua il filtraggio dei pacchetti, ammettendo alcuni pacchetti e proibendo altri pacchetti: è la tabella principale e si applica al computer singolo;
- ***mangle***, che effettua l'ottimizzazione dei pacchetti in uscita: si applica alle reti locali (LAN);
- ***nat***, che effettua, relativamente ai pacchetti in uscita, il mascheramento o la conversione degli indirizzi d'origine e la conversione degli indirizzi di destinazione: si applica anch'essa alle reti private (LAN).

Le regole

Le regole sono create secondo certi criteri e raccolte in un elenco: in base al criterio con cui è stata creata, ogni regola ha lo scopo di individuare (*match*) un tipo di pacchetti e stabilirne il destino con un'azione (*target*) appropriata.

Il firewall in azione

Tutti i pacchetti sono vagliati dal firewall allo stesso modo. Infatti, per ogni pacchetto:

1. *Netfilter* cerca nell'elenco delle regole una corrispondenza (*match*) tra il pacchetto esaminato e una delle regole elencate;
2. quando trova la regola corrispondente al pacchetto, *Netfilter*, per mezzo di *Iptables*, esegue l'azione (*target*) contenuta in quella regola.

Ciò vale per ciascuna delle tre tabelle.

Nota

Oggetto di questo manuale è la tabella *filter*.

Capitolo 1

Iptables

1.1 Sintassi

La sintassi generale è:

```
iptables -t tabella comando catena opz.-generali azione opz.-specifica
```

ma varia a seconda del comando interno al comando principale:

iptables	-t tabella	comando	catena	opz.-generali	azione	opz.-specifica
iptables	[-t tabella]	-A	catena	[opzioni]	azione	[opzione]
iptables	[-t tabella]	-F	[catena]	[opzioni]		
iptables	[-t tabella]	-L	[catena]	[opzioni]		
iptables	[-t tabella]	-N	catena			
iptables	[-t tabella]	-P	catena		azione	
iptables	[-t tabella]	-X	[catena]			

Gli elementi racchiusi tra parentesi quadre, quando previsti, sono facoltativi.

Ancora diversa è la sintassi del comando di aiuto, che va posto da solo o dopo una delle opzioni relative ai moduli:

iptables	opz.-generali	comando
iptables	[opzioni]	-h

1.2 Tabelle

Come detto nell'**Introduzione**, le tabelle di *Netfilter*, gestite da *Iptables*, sono:

- *filter*, predefinita (si omette);
- *mangle*;
- *nat*.

Poiché la tabella *filter* è predefinita e si omette e poiché le azioni previste dalla tabella non comprendono opzioni specifiche, la sintassi relativa alla tabella *filter* si semplifica in:

```
iptables comando catena opz.-generali azione
```

1.3 Comandi

-A, --append	Aggiunge una o più regole alla fine di una catena.
-F, --flush	Elimina tutte le regole in una catena o in tutte le catene.
-h, --help	Mostra indicazioni d'aiuto.
-L, --list	Elenca tutte le regole di una catena o di tutte le catene.
-N, --new-chain	Crea una nuova catena definita dall'utente.
-P, --policy	Imposta una regola come criterio generale di una catena.
-X, --delete-chain	Elimina una catena definita dall'utente.

1.4 Catene

Ogni tabella contiene delle catene predefinite.

- La tabella *filter* comprende tre catene predefinite:
  - `INPUT`, relativa ai pacchetti in entrata,
  - `FORWARD`, relativa ai pacchetti in transito,
  - `OUTPUT`, relativa ai pacchetti in uscita.
- La tabella *mangle* comprende cinque catene predefinite:
  - `INPUT`, relativa ai pacchetti in entrata,
  - `FORWARD`, relativa ai pacchetti in transito,
  - `OUTPUT`, relativa ai pacchetti in uscita,
  - `PREROUTING`, relativa ai pacchetti in uscita,
  - `POSTROUTING`, relativa ai pacchetti in uscita.
- La tabella *nat* comprende tre catene predefinite:
  - `OUTPUT`, relativa ai pacchetti in uscita,
  - `PREROUTING`, relativa ai pacchetti in uscita,
  - `POSTROUTING`, relativa ai pacchetti in uscita.

Per semplificare l'impostazione delle regole in presenza di una rete privata (LAN), è possibile creare nuove catene.

Per ogni tabella, non specificando alcuna catena si indicano tutte le catene della tabella.

1.5 Opzioni generali

Esistono opzioni generali e opzioni relative ai moduli.

1.5.1 Opzioni generali

`-d`, `--destination`	Precede l'indirizzo di destinazione.
`-f`, `--fragment`	Indica dei pacchetti frammentati tutti i frammenti successivi al primo.
`-i`, `--in-interface`	Precede l'interfaccia d'entrata (o input).
`-j`, `--jump`	Precede un'azione.
`--line-numbers`	In un elenco di regole, numera le regole.
`-m`, `--match`	Precede un modulo generico.
`-n`, `--numeric`	Mostra gli indirizzi IP e le porte nei rispettivi formati numerici.
`-o`, `--out-interface`	Precede l'interfaccia d'uscita (o output).
`-p`, `--protocol`	Precede un modulo indicante un protocollo. Da solo, indica tutti i protocolli.
`-p all`, `--protocol all`	Indica tutti i protocolli.
`-s`, `--source`	Precede l'indirizzo d'origine.
`-v`, `--verbose`	Modalità prolissa: mostra i dettagli.
`-vv`	Modalità molto prolissa: mostra maggiori dettagli.

1.5.2 Opzioni relative ai moduli

Opzioni relative ai moduli dei protocolli

`icmp`	Indica il protocollo ICMP.
`--icmp-type`	Precede un tipo e/o un sottotipo.
`0, echo-reply`	Risposta con un'eco (pong).
`3, destination-unreachable`	Destinazione irraggiungibile.
`0, network-unreachable`	Rete irraggiungibile.
`1, host-unreachable`	Host irraggiungibile.
`2, protocol-unreachable`	Protocollo irraggiungibile.
`3, port-unreachable`	Porta irraggiungibile.
`4, fragmentation-needed`	Frammentazione necessaria.
`5, source-route-failed`	Percorso d'origine respinto.
`6, network-unknown`	Rete sconosciuta.
`7, host-unknown`	Host sconosciuto.
`9, network-prohibited`	Rete proibita.
`10, host-prohibited`	Host proibito.
`11, TOS-network-unreachable`	Rete irraggiungibile in base al tipo di servizio.
`12, TOS-host-unreachable`	Host irraggiungibile in base al tipo di servizio.
`13, communication-prohibited`	Accesso vietato.
`14, host-precedence-violation`	Violazione della precedenza dell'host.
`15, precedence-cutoff`	Interruzione della precedenza.
`4, source-quench`	Attenuazione dell'origine.
`5, redirect`	Dirottamento.
`0, network-redirect`	Dirottamento della rete.
`1, host-redirect`	Dirottamento dell'host.
`2, TOS-network-redirect`	Dirottamento della rete in base al tipo di servizio.
`3, TOS-host-redirect`	Dirottamento dell'host in base al tipo di servizio.
`8, echo-request`	Richiesta di un'eco (ping).
`9, router-advertisement`	Messaggio del router.
`10, router-solicitation`	Richiesta al router.
`11, time-exceeded (ttl-exceeded)`	Tempo scaduto (durata massima superata).
`0, ttl-zero-during-transit`	Durata massima zero durante il transito.
`1, ttl-zero-during-reassembly`	Durata massima zero durante la ricomposizione.
`12, parameter-problem`	Problema relativo ai parametri.
`0, ip-header-bad`	Intestazione IP corrotta.
`1, required-option-missing`	Opzione richiesta mancante.
`13, timestamp-request`	Richiesta di sincronizzazione di data e ora.
`14, timestamp-reply`	Risposta di sincronizzazione di data e ora.
`15, information-request`	Richiesta di informazioni.
`16, information-reply`	Risposta di informazioni.
`17, address-mask-request`	Richiesta della maschera di rete.
`18, address-mask-reply`	Risposta della maschera di rete.
`tcp`	Indica il protocollo TCP.
`--dport, --destination-port`	Indica una porta di destinazione.
`--sport, --source-port`	Indica una porta d'origine.
`udp`	Indica il protocollo UDP.
`--dport, --destination-port`	Indica una porta di destinazione.
`--sport, --source-port`	Indica una porta d'origine.

Riguardo al protocollo ICMP il tipo è indicato da un numero o da un'espressione. Il sottotipo è indicato da due numeri, separati da una barra, o da un'espressione. Esempi:

- `icmp --icmp-type 3` (oppure `icmp --icmp-type destination-unreachable`)
- `icmp --icmp-type 3/3` (oppure `icmp --icmp-type port-unreachable`)

Opzioni relative ai moduli generici

`limit`	Precede un limite massimo.
`--limit`	Indica una frequenza massima. Se non segue alcun valore, il valore predefinito è: `3/day`.
`--limit n/second`	Indica una frequenza massima riferita al secondo.
`--limit n/minute`	Indica una frequenza massima riferita al minuto.
`--limit n/hour`	Indica una frequenza massima riferita all'ora.
`--limit n/day`	Indica una frequenza massima riferita al giorno.
`--limit-burst`	Indica il massimo numero iniziale di corrispondenze (cioè, di pacchetti da individuare), prima che possa agire l'opzione `--limit` descritta precedentemente. Il numero iniziale viene automaticamente e progressivamente aumentato di uno finché non viene soddisfatta l'opzione `--limit`. Il valore predefinito è: `5`.
`multiport`	Precede una serie di porte.
`--sports`, `--source-ports`	Indica una serie di porte d'origine.
`--dports`, `--destination-ports`	Indica una serie di porte di destinazione.
`--ports`	Indica sia una porta d'origine che una porta di destinazione, separate da due punti.
`state --state`	Precede uno stato di connessione o più stati di connessione, separati da una virgola.
`NEW`	Indica un pacchetto che crea una nuova connessione.
`ESTABLISHED`	Indica un pacchetto che appartiene ad una connessione esistente.
`RELATED`	Indica un pacchetto che crea una nuova connessione collegata ad una connessione esistente, ma che non appartiene alla connessione esistente.
`INVALID`	Indica un pacchetto che non appartiene ad alcuna connessione, e che perciò non è identificabile.

1.6 Azioni

Esistono azioni generali e azioni specifiche.

1.6.1 Azioni generali

`LOG`	Registra nel file /var/log/syslog i pacchetti individuati.
`--log-prefix`	Precede un'annotazione (fino a 29 caratteri), per identificare e distinguere i messaggi della registrazione.

L'azione generale `LOG`, in quanto azione di semplice registrazione, non è un'azione finale, cioè non termina la ricerca da parte di *Netfilter*. Perciò, una regola contenente l'azione `LOG` deve sempre precedere la regola corrispondente contenente un'azione specifica finale, per esempio `ACCEPT` (vedere tra gli **Esempi** a pag. 6), che termina la ricerca da parte di *Netfilter*.

1.6.2 Azioni e opzioni specifiche

Le azioni specifiche sono azioni finali, che terminano la ricerca da parte di *Netfilter*.

TABELLA *FILTER*

Azioni	
`ACCEPT`	Ammette (cioè, lascia passare) il traffico.
`DROP`	Proibisce (cioè, blocca ed elimina) il traffico.

Data la natura delle azioni, non esistono opzioni.

TABELLA *MANGLE*

Azione e opzioni		
`TOS`		Indica il tipo di servizio.
`--set-tos`		Precede il valore del servizio.
	`16, Minimize-Delay`	Minimo ritardo.
	`8, Maximize-Throughput`	Massima velocità di trasmissione.
	`4, Maximize-Reliability`	Massima affidabilità.
	`2, Minimize-Cost`	Minimo costo.
	`0, Normal-Service`	Servizio normale.

TABELLA *NAT*

Azioni e opzioni	
`DNAT`	Converte l'indirizzo di destinazione effettivo in un indirizzo IP differente.
`MASQUERADE`	Maschera l'indirizzo d'origine con l'indirizzo IP dinamico.
`SNAT`	Converte l'indirizzo d'origine nell'indirizzo IP statico.
`--to-destination`	Indica l'indirizzo di destinazione.
`--to-source`	Indica l'indirizzo d'origine.

Le azioni `MASQUERADE` e `SNAT` sono alternative fra loro.

1.7 Esempi

Gli esempi si riferiscono alla tabella *filter*.

```
# iptables -L -v
# iptables -L -n -vv

# iptables -N NUOVA-CATENA-1
# iptables -N NUOVA-CATENA-2
# iptables -X NUOVA-CATENA-1
# iptables -X  (sono interessate tutte le nuove catene)

# iptables -h
# iptables -p tcp -h
# iptables -m state -h

# iptables -A INPUT -p icmp --icmp-type 3 -m state --state RELATED
                                                    -j LOG --log-prefix="[I ICMP 3] "
# iptables -A INPUT -p icmp --icmp-type 3 -m state --state RELATED -j ACCEPT
```

Capitolo 2

Configurazione del firewall

2.1 Configurazione hardware

La configurazione hardware considerata in questa sede si riferisce ad un computer (o sistema) singolo, come un computer portatile, connesso ad Internet, che dispone di due interfacce di connessione:

- l'interfaccia localhost (`lo`), presente in ogni sistema, per le connessioni interne al sistema;
- l'interfaccia di rete, per la connessione del sistema ad Internet, che può essere di volta in volta:
  - `ppp0`, attraverso un modem per connessioni Point-to-Point Protocol (PPP), come una chiave USB;
  - `eth0`, attraverso un modem o un router Ethernet;
  - `wlan0`, attraverso un modem o un router WiFi.

2.2 Pianificazione del firewall

2.2.1 Definizione del criterio generale

Prima di tutto bisogna stabilire il criterio generale (*policy*) di protezione del firewall. Due criteri, opposti fra loro, sono possibili:

1. CRITERIO GENERALE TEMERARIO: consentire tutto ciò che non è esplicitamente vietato.
2. CRITERIO GENERALE PRUDENTE: vietare tutto ciò che non è esplicitamente consentito.

Conviene seguire il secondo criterio, proibendo quasi tutto il traffico (in arrivo, in transito e in uscita), ad esclusione di quello strettamente necessario ed esplicitamente ammesso, secondo i criteri particolari.

2.2.2 Definizione dei criteri particolari

Porte e stati di connessione ammessi

Qui si assume che la connessione ad Internet avvenga attraverso un intervallo limitato, ma ampiamente sufficiente, di porte locali, rispetto a tutte le porte disponibili; mentre le porte remote possono essere tutte quelle disponibili.

Inoltre, si assume che le connessioni ammesse ad Internet siano tutte avviate dal computer locale e quindi si nega la possibilità di connessioni iniziate da computer remoti.

Porte locali proibite in entrata e in uscita:	`0:1024` e `6000:65535`
Porte locali ammesse in entrata e in uscita:	`1025:5999`
Porte remote ammesse in entrata e in uscita:	`0:65535`
Stati di connessione proibiti in entrata:	`NEW`

Servizi ammessi

Qui si assume anche che la connessione ad Internet debba soddisfare le esigenze di base: navigazione, prelevamento (*download*) e invio (*upload*) di file, posta elettronica, discussioni su Usenet, aggiornamento dell'ora, ascolto della radio. Pertanto, è ammesso esclusivamente il traffico relativo:

- al protocollo ICMP, limitatamente;
- al servizio DNS;
- ai protocolli: BITTORRENT, FTP, HTTP, HTTPS, IMAPS, NNTP, NTP, POP3, POP3S, RTSP, SMTP, SMTPS.

2.3 Realizzazione del firewall

La realizzazione del firewall, che richiede i privilegi di root, comprende:
1. il caricamento di uno o più moduli del kernel;
2. l'impostazione di alcuni parametri del kernel;
3. l'impostazione di una serie di regole;
4. l'impostazione di un ultimo parametro del kernel.

2.3.1 Caricamento dei moduli del kernel

Almeno un modulo del kernel è necessario e deve essere caricato:

```
# modprobe ip_conntrack_ftp
```

2.3.2 Impostazione dei parametri del kernel (I)

Ai parametri del kernel corrispondono dei file nel file system di Linux, ossia nella directory /proc/. L'impostazione dei parametri del kernel non richiede la ricompilazione del kernel, ma la semplice modifica dei file nella directory /proc/. I nomi dei file indicano la loro funzione.

Di interesse in questa sede sono i file presenti nella directory /proc/sys/net/ipv4/ e nelle subdirectory /proc/sys/net/ipv4/conf/all/ e /proc/sys/net/ipv4/conf/default/: i file in questione contengono un valore numerico o una gamma di valori numerici.

Dunque, è necessario modificare i valori numerici all'interno dei file: il più delle volte si tratta di attivare (con 1) o disattivare (con 0) un parametro, altre volte bisogna attribuire ad un parametro un valore numerico (per esempio: 1024) o una gamma di valori numerici (per esempio: 1025 5999).

Nella directory /proc/sys/net/ipv4/ sono di rilievo i file:

icmp_echo_ignore_broadcasts	Consente di ignorare i ping di broadcast.
icmp_ignore_bogus_error_responses	Consente di ignorare i messaggi d'errore.
ip_forward	Consente l'inoltro IP.
ip_local_port_range	Stabilisce l'intervallo delle porte locali.
tcp_ecn	Consente la notifica esplicita di congestione.
tcp_max_syn_backlog	Stabilisce il massimo numero di connessioni in coda.
tcp_syncookies	Consente l'invio dei syncookies.

Per esempio:

```
# echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
# echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
# echo 0 > /proc/sys/net/ipv4/ip_forward  (disattivazione temporanea)
# echo 1025 5999 > /proc/sys/net/ipv4/ip_local_port_range
# echo 0 > /proc/sys/net/ipv4/tcp_ecn
# echo 1024 > /proc/sys/net/ipv4/tcp_max_syn_backlog
# echo 1 > /proc/sys/net/ipv4/tcp_syncookies
```

L'inoltro IP deve essere prima disattivato e poi attivato (vedere la **Sottosez. 2.3.4** a pag. 12).

Le subdirectory /proc/sys/net/ipv4/conf/all/ e /proc/sys/net/ipv4/conf/default/ contengono file corrispondenti, da modificare allo stesso modo. Di rilievo sono i file:

accept_redirects	Consente di ricevere i reindirizzamenti in genere.
accept_source_route	Consente di ricevere il percorso di provenienza.
forwarding	Consente l'inoltro in genere.
log_martians	Consente di registrare i pacchetti strani.
rp_filter	Consente di filtrare il percorso inverso. Ne deriva la proibizione del traffico con indirizzi IP falsi (IP spoofing), cioè dei pacchetti con indirizzi IP non Internet (in quanto riservati alle reti private) sia d'origine che di destinazione.
secure_redirects	Consente di ricevere i reindirizzamenti sicuri.
send_redirects	Consente di inviare i reindirizzamenti.

Per esempio:

```
# echo 0 > /proc/sys/net/ipv4/conf/all/accept_redirects
# echo 0 > /proc/sys/net/ipv4/conf/all/accept_source_route
# echo 1 > /proc/sys/net/ipv4/conf/all/forwarding
# echo 1 > /proc/sys/net/ipv4/conf/all/log_martians
# echo 1 > /proc/sys/net/ipv4/conf/all/rp_filter
# echo 1 > /proc/sys/net/ipv4/conf/all/secure_redirects
# echo 1 > /proc/sys/net/ipv4/conf/all/send_redirects

# echo 0 > /proc/sys/net/ipv4/conf/default/accept_redirects
# echo 0 > /proc/sys/net/ipv4/conf/default/accept_source_route
# echo 1 > /proc/sys/net/ipv4/conf/default/forwarding
# echo 1 > /proc/sys/net/ipv4/conf/default/log_martians
# echo 1 > /proc/sys/net/ipv4/conf/default/rp_filter
# echo 1 > /proc/sys/net/ipv4/conf/default/secure_redirects
# echo 1 > /proc/sys/net/ipv4/conf/default/send_redirects
```

2.3.3 Impostazione delle regole

L'impostazione delle regole segue un certo ordine. *Netfilter* esamina ciascun pacchetto scorrendo le regole nella sequenza data: quando trova una corrispondenza (*match*) tra il pacchetto esaminato e una regola, ferma la ricerca ed esegue l'azione (*target*) contenuta in quella regola. Come detto nella **Sottosez. 1.6.1** a pag. 5, fa eccezione l'azione `LOG`.

Trattandosi di un computer singolo, l'impostazione delle regole si basa esclusivamente sulla tabella *filter*. Inoltre, poiché nel caso di un computer portatile è frequente cambiare il tipo di connessione (PPP, Ethernet, WiFi), è più pratico non indicare l'interfaccia di rete (non specificando alcuna interfaccia di rete si indicano tutte le interfacce).

Pulizia totale iniziale

Azzeramento di tutte e tre le tabelle, ossia eliminazione sia di tutte le regole impostate in precedenza sia di tutte le eventuali catene definite dall'utente:

```
# iptables -F
# iptables -t mangle -F
# iptables -t nat -F

# iptables -X
# iptables -t mangle -X
# iptables -t nat -X
```

Impostazione del criterio generale

Proibizione di tutto il traffico in entrata, in transito e in uscita, ossia chiusura totale:

```
# iptables -P INPUT DROP
# iptables -P FORWARD DROP
# iptables -P OUTPUT DROP
```

Il traffico consentito dovrà essere esplicitamente ammesso in seguito.

Proibizione del traffico non identificabile

Proibizione di tutti i pacchetti non identificabili in entrata e in uscita, relativi sia alla rete di loopback che ad Internet (non specificando alcuna interfaccia di rete si indicano tutte le interfacce):

```
# iptables -A INPUT -f -j DROP
# iptables -A INPUT -m state --state INVALID -j DROP
# iptables -A OUTPUT -f -j DROP
# iptables -A OUTPUT -m state --state INVALID -j DROP
```

Ammissione del traffico interno al computer

Ammissione del traffico nella rete di loopback in entrata e in uscita:

```
# iptables -A INPUT -i lo -j ACCEPT
# iptables -A OUTPUT -o lo -j ACCEPT
```

Regolazione del traffico destinato e proveniente da Internet

Ammissione dei pacchetti ICMP, limitatamente ai messaggi di controllo indispensabili:

```
# iptables -A OUTPUT -p icmp --icmp-type 8 -m state --state NEW -j ACCEPT
# iptables -A OUTPUT -p icmp --icmp-type 12 -m state --state RELATED -j ACCEPT
# iptables -A INPUT -p icmp --icmp-type 0 -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -p icmp --icmp-type 3 -m state --state RELATED -j ACCEPT
# iptables -A INPUT -p icmp --icmp-type 11 -m state --state RELATED -j ACCEPT
# iptables -A INPUT -p icmp --icmp-type 12 -m state --state RELATED -j ACCEPT
```

Ammissione dei pacchetti relativi al servizio DNS:

```
# iptables -A OUTPUT -p udp --sport 1025:5999 --dport 53:53
                                                -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p udp --sport 53:53 --dport 1025:5999
                                                    -m state --state ESTABLISHED -j ACCEPT
```

Ammissione dei pacchetti relativi al servizio BitTorrent (la porta locale 5000 è presa a caso tra 1025 e 5999):

```
# iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 0:65535
                                                -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp --sport 0:65535 --dport 3000:3000
                                               -m state --state ESTABLISHED,RELATED -j ACCEPT
# iptables -A OUTPUT -p udp --sport 1025:5999 --dport 0:65535
                                                -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p udp --sport 0:65535 --dport 3000:3000
                                               -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Ammissione dei pacchetti relativi al servizio FTP: connessione di controllo, connessione (per il trasferimento dei) dati in modalità attiva e connessione (per il trasferimento dei) dati in modalità passiva.

```
# iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 21:21
                                                -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp --sport 21:21 --dport 1025:5999
                                                    -m state --state ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 20:20
                                                    -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp --sport 20:20 --dport 1025:5999
                                               -m state --state ESTABLISHED,RELATED -j ACCEPT
# iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 0:65535
                                               -m state --state ESTABLISHED,RELATED -j ACCEPT
# iptables -A INPUT -p tcp --sport 0:65535 --dport 1025:5999
                                                    -m state --state ESTABLISHED -j ACCEPT
```

Ammissione dei pacchetti relativi al servizio HTTP:

```
# iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 80:80
                                                -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp --sport 80:80 --dport 1025:5999
                                                    -m state --state ESTABLISHED -j ACCEPT
```

Ammissione dei pacchetti relativi al servizio HTTPS:

```
# iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 443:443
                                                -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp --sport 443:443 --dport 1025:5999
                                                -m state --state ESTABLISHED -j ACCEPT
```

Ammissione dei pacchetti relativi al servizio IMAPS:

```
# iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 993:993
                                                -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp --sport 993:993 --dport 1025:5999
                                                -m state --state ESTABLISHED -j ACCEPT
```

Ammissione dei pacchetti relativi al servizio NNTP:

```
# iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 119:119
                                                -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp --sport 119:119 --dport 1025:5999
                                                -m state --state ESTABLISHED -j ACCEPT
```

Ammissione dei pacchetti relativi al servizio NTP:

```
# iptables -A OUTPUT -p tcp --sport 123:123 -d 193.204.114.105
                                                -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp -s 193.204.114.105 --dport 123:123
                                                -m state --state ESTABLISHED -j ACCEPT
```

Ammissione dei pacchetti relativi al servizio POP3:

```
# iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 110:110
                                                -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp --sport 110:110 --dport 1025:5999
                                                -m state --state ESTABLISHED -j ACCEPT
```

Ammissione dei pacchetti relativi al servizio POP3S:

```
# iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 995:995
                                                -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp --sport 995:995 --dport 1025:5999
                                                -m state --state ESTABLISHED -j ACCEPT
```

Ammissione dei pacchetti relativi al servizio RTSP:

```
# iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 554:554
                                                -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp --sport 554:554 --dport 1025:5999
                                                -m state --state ESTABLISHED -j ACCEPT
```

Ammissione dei pacchetti relativi al servizio SMTP:

```
# iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 25:25
                                                -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp --sport 25:25 --dport 1025:5999
                                                -m state --state ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 587:587
                                                -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp --sport 587:587 --dport 1025:5999
                                                -m state --state ESTABLISHED -j ACCEPT
```

Ammissione dei pacchetti relativi al servizio SMTPS:

```
# iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 465:465
                                                -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp --sport 465:465 --dport 1025:5999
                                                -m state --state ESTABLISHED -j ACCEPT
```

2.3.4 Impostazione dei parametri del kernel (II)

Attivazione dell'inoltro IP (che prima era stato disattivato):

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

2.4 Il file rc.firewall/firewall

Per configurare stabilmente il firewall, in qualità di root bisogna creare lo script **rc.firewall** (o **firewall**) e con un programma di videoscrittura inserirvi tutti i comandi necessari. Il file rc.firewall/firewall è il modo più pratico per configurare il firewall, anche per la possibilità di essere copiato e trasferito in più sistemi Linux. Un file rc.firewall è allegato a questo manuale.

Ecco un esempio, che ricalca i comandi fin qui spiegati.

```
#!/bin/bash

## Caricamento dei moduli del kernel

modprobe ip_conntrack_ftp

## Impostazione dei parametri del kernel (I)

# Intervallo delle porte locali ammesse (in entrata e in uscita): 1025-5999

echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
echo 0 > /proc/sys/net/ipv4/ip_forward
echo 1025 5999 > /proc/sys/net/ipv4/ip_local_port_range
echo 0 > /proc/sys/net/ipv4/tcp_ecn
echo 1024 > /proc/sys/net/ipv4/tcp_max_syn_backlog
echo 1 > /proc/sys/net/ipv4/tcp_syncookies

echo 0 > /proc/sys/net/ipv4/conf/all/accept_redirects
echo 0 > /proc/sys/net/ipv4/conf/all/accept_source_route
echo 1 > /proc/sys/net/ipv4/conf/all/forwarding
echo 1 > /proc/sys/net/ipv4/conf/all/log_martians
echo 1 > /proc/sys/net/ipv4/conf/all/rp_filter
echo 1 > /proc/sys/net/ipv4/conf/all/secure_redirects
echo 1 > /proc/sys/net/ipv4/conf/all/send_redirects

echo 0 > /proc/sys/net/ipv4/conf/default/accept_redirects
echo 0 > /proc/sys/net/ipv4/conf/default/accept_source_route
echo 1 > /proc/sys/net/ipv4/conf/default/forwarding
echo 1 > /proc/sys/net/ipv4/conf/default/log_martians
echo 1 > /proc/sys/net/ipv4/conf/default/rp_filter
echo 1 > /proc/sys/net/ipv4/conf/default/secure_redirects
echo 1 > /proc/sys/net/ipv4/conf/default/send_redirects

## Impostazione delle regole

# Pulizia iniziale totale
iptables -F
iptables -t mangle -F
iptables -t nat -F

iptables -X
iptables -t mangle -X
iptables -t nat -X
```

(Continua)

(Continua)

```
# Impostazione del criterio generale
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

# Proibizione del traffico non identificabile
iptables -A INPUT -f -j DROP
iptables -A INPUT -m state --state INVALID -j DROP
iptables -A OUTPUT -f -j DROP
iptables -A OUTPUT -m state --state INVALID -j DROP

# Ammissione del traffico interno al computer (traffico di loopback)
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Regolazione del traffico destinato e proveniente da Internet

# Porte locali proibite in entrata:             0:1024 e 6000:65535
# Porte locali ammesse in entrata e in uscita:  1025:5999
# Porte remote ammesse in entrata e in uscita:  0:65535
# Stati di connessione proibiti in entrata:     NEW

# ICMP
iptables -A OUTPUT -p icmp --icmp-type 8 -m state --state NEW -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 12 -m state --state RELATED -j ACCEPT
iptables -A INPUT -p icmp --icmp-type 0 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p icmp --icmp-type 3 -m state --state RELATED -j ACCEPT
iptables -A INPUT -p icmp --icmp-type 11 -m state --state RELATED -j ACCEPT
iptables -A INPUT -p icmp --icmp-type 12 -m state --state RELATED -j ACCEPT

# DNS
iptables -A OUTPUT -p udp --sport 1025:5999 --dport 53:53 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p udp --sport 53:53 --dport 1025:5999 -m state --state ESTABLISHED -j ACCEPT

# BITTORRENT
iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 0:65535 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 0:65535 --dport 3000:3000 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -p udp --sport 1025:5999 --dport 0:65535 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p udp --sport 0:65535 --dport 3000:3000 -m state --state ESTABLISHED,RELATED -j ACCEPT

# FTP
# Controllo della connessione
iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 21:21 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 21:21 --dport 1025:5999 -m state --state ESTABLISHED -j ACCEPT
# Connessione (per il trasferimento dei) dati in modalità attiva
iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 20:20 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 20:20 --dport 1025:5999 -m state --state ESTABLISHED,RELATED -j ACCEPT
# Connessione (per il trasferimento dei) dati in modalità passiva
iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 0:65535 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p tcp --sport 0:65535 --dport 1025:5999 -m state --state ESTABLISHED -j ACCEPT

# HTTP
iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 80:80 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 80:80 --dport 1025:5999 -m state --state ESTABLISHED -j ACCEPT

# HTTPS
iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 443:443 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 443:443 --dport 1025:5999 -m state --state ESTABLISHED -j ACCEPT

# IMAPS
```

(Continua)

(Continua)

```
iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 993:993 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 993:993 --dport 1025:5999 -m state --state ESTABLISHED -j ACCEPT

# NNTP
iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 119:119 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 119:119 --dport 1025:5999 -m state --state ESTABLISHED -j ACCEPT

# NTP
iptables -A OUTPUT -p udp --sport 123:123 -d 193.204.114.105 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p udp -s 193.204.114.105 --dport 123:123 -m state --state ESTABLISHED -j ACCEPT

# POP3
iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 110:110 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 110:110 --dport 1025:5999 -m state --state ESTABLISHED -j ACCEPT

# POP3S
iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 995:995 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 995:995 --dport 1025:5999 -m state --state ESTABLISHED -j ACCEPT

# RTSP
iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 554:554 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 554:554 --dport 1025:5999 -m state --state ESTABLISHED -j ACCEPT

# SMTP
iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 25:25 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 25:25 --dport 1025:5999 -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 587:587 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 587:587 --dport 1025:5999 -m state --state ESTABLISHED -j ACCEPT

# SMTPS
iptables -A OUTPUT -p tcp --sport 1025:5999 --dport 465:465 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 465:465 --dport 1025:5999 -m state --state ESTABLISHED -j ACCEPT

## Impostazione dei parametri del kernel (II)

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

2.4.1 Suggerimenti pratici

- Evitare l'impiego dell'opzione `-m multiport`: l'attribuzione di una regola per ogni porta rende più chiara l'elencazione e più semplice aggiungere o eliminare/commentare le singole regole.
- Limitare o evitare l'uso dell'azione `LOG`: la registrazione di tutto il traffico (ammesso e proibito) farebbe assumere dimensioni eccessive al file /var/log/syslog. Un metodo potrebbe essere: i) dapprima, registrare soltanto il traffico ammesso; ii) poi, registrare soltanto il traffico proibito; iii) in seguito, registrare soltanto il traffico da tenere sotto osservazione; iv) infine, ridurre le registrazioni al minimo indispensabile fino addirittura a farne del tutto a meno.

2.4.2 Attivazione

Rendere eseguibile lo script e inserirlo tra i processi che devono essere attivati all'avvio del sistema: a seconda della distribuzione Linux, il file rc.firewall va nella directory /etc/rc.d/, il file firewall va in /etc/init.d/.

Riavviare il sistema: al riavvio il firewall è attivo.

2.4.3 Verifica

La validità della configurazione del firewall può essere verificata in due modi:

- mediante scansione in linea su siti web come **PC Flank** e **Shields Up** (vedere tra gli **Indirizzi** a pag. 17);
- mediante scansione con ***Nmap***.

Scansione in linea

La scansione in linea delle proprie porte richiede che la connessione ad Internet sia effettuata mediante modem, non attraverso un router.

Scansione con *Nmap*

Con ***Nmap*** è possibile effettuare una scansione sufficientemente approfondita delle proprie porte (sconsigliabile una scansione completa di tutte le 65.535 porte, che richiederebbe molto tempo).

Operazioni preliminari

1. In qualità di root, copiare in /usr/local/bin/ lo script **scan**, allegato a questo manuale.
2. Creare nella propria home directory le directory:

   /Nmap/
   /Nmap/frag/
   /Nmap/pack/
   /Nmap/ping/

   Le directory /frag/, /pack/ e /ping/ ospiteranno i file di log prodotti durante la scansione.

Scansione

1. Connettersi ad Internet e con un programma di navigazione (browser) andare ad uno dei siti che mostrano l'indirizzo IP dinamico (come http://www.ilmioip.it/): apparirà l'indirizzo IP assegnato dal proprio fornitore di servizi Internet (provider) per la connessione in atto.
2. In qualità di root, aprire con un programma di videoscrittura in /usr/local/bin/ lo script scan, sostituire provvisoriamente `X.X.X.X` con l'indirizzo IP assegnato e salvare (senza chiudere lo script).
3. In qualità di root, avviare la scansione:

   ```
   $ su
   # scan
   ```

4. Terminata la scansione, tornare a sostituire l'indirizzo IP utilizzato per la scansione con `X.X.X.X`, e salvare. La sostituzione di un indirizzo IP valido con uno non valido è una precauzione indispensabile per evitare, ad una successiva connessione, di effettuare inavvertitamente la scansione ad un indirizzo IP che non è più il proprio.
5. Leggere i risultati della scansione nei file di log. I risultati di ogni scansione parziale vengono registrati in due file di log: le informazioni contenute in entrambi si integrano e si completano.

Bibliografia

[1] Stefano Barni. *Linux in Rete, stop agli intrusi.*
http://www.zeusnews.it/index.php3?ar=stampa&cod=2033

[2] Carlo Contavalli. *IPtables for Fun – Implementare un firewall in linux.*
http://www.masobit.net/people/ccontavalli/docs-it/iptables/iptables4dummies.pdf

[3] Herve Eychenne. *IPTABLES(8).*
`$ man iptables`

[4] Fyodor. *NMAP(1).*
`$ man nmap`

[5] Daniele Giacomini. *a2.*
http://www.informaticalibera.net/

[6] Marco Masetti. *Firewall, netfilter, iptables.*
http://digilander.libero.it/amilinux/doc/netfilter.html

[7] AA.VV. *Documentation about the netfilter/iptables project.*
http://www.hu.netfilter.org/documentation/index.html

Indirizzi

Netfilter–Iptables	http://www.netfilter.org/
Nmap	http://www.insecure.org/nmap/
PC Flank	http://www.pcflank.com/
ShieldsUp!	https://www.grc.com/x/ne.dll?bh0bkyd2

LICENZA PGI – PICCOLE GUIDE D'INFORMATICA

*Le **PGI – PICCOLE GUIDE D'INFORMATICA**, o più brevemente **PGI**, sebbene siano redatte con grande accuratezza, sono sprovviste di qualsiasi forma di garanzia: è sempre opportuno procedere a verifiche.*

Tutte le PGI possono essere riprodotte e/o distribuite totalmente o parzialmente in piena libertà. La ridistribuzione commerciale delle PGI non è vietata, ma neanche incoraggiata.

Tutte le PGI possono essere modificate totalmente o parzialmente in piena libertà. Le modifiche fatte in accordo con l'autore originale rendono l'autore delle modifiche coautore. Le modifiche fatte senza l'accordo con l'autore originale sono ammesse ma non incoraggiate: sarebbe auspicabile che, semplicemente in ossequio al galateo, riportassero il nome dell'autore originale e il nome del revisore.

Lavori derivati dalle PGI o comprendenti parti di PGI sono non solo ammessi ma incoraggiati: sarebbe auspicabile che, semplicemente in ossequio al galateo, riportassero i riferimenti alle PGI da cui derivano o che comprendono.

Tutte le PGI possono essere tradotte in piena libertà: sarebbe auspicabile che le traduzioni, semplicemente in ossequio al galateo, riportassero il nome dell'autore e il nome del traduttore.