

# *Sicurezza su linux ... e considerazioni varie*

Gianluca Antonacci  
email: [giaaan@tin.it](mailto:giaaan@tin.it)



# Sommario

## Protezione del PC: firewall e antivirus

- configurazione di Firestarter
- configurazione di ClamAV

## Indicizzazione dei files

- cenni sulla posizione dei files e albero delle directory
- configurazione e utilizzo di Tracker

## Un simpatico e istruttivo filmato

- “Lo gnu, il pinguino e il cerbiatto esuberante” ([www.biasco.ch](http://www.biasco.ch))

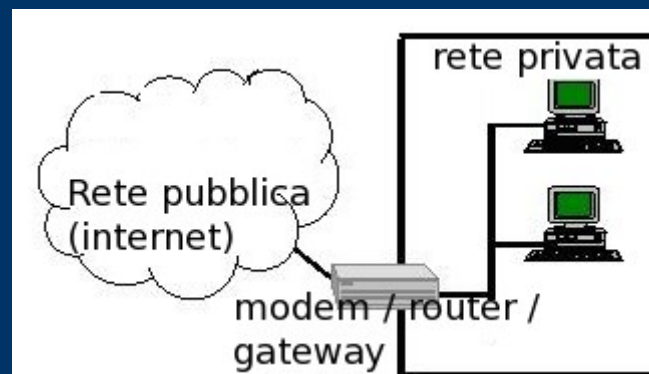


# Sicurezza in rete

Gli indirizzi IP che caratterizzano un PC in una rete possono essere di due tipi: pubblici (= visti da tutto il mondo) o privati (= accessibili dalla cosiddetta rete locale)

Rete pubblica: es. 193.205.203.1

Rete privata: es. 192.168.x.x, 10.0.x.x



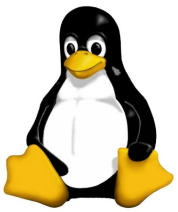
# Sicurezza in rete

Quando navighiamo con un browser nel “mondo selvaggio della rete” ci esponiamo a potenziali pericoli... con un po' di coscienza e prudenza vale comunque la pena di uscire!!!

Un test: <http://browserspy.dk>

Cosa se ne deduce?

Quante informazioni mandiamo in giro a computer sconosciuti? È un problema di sicurezza?



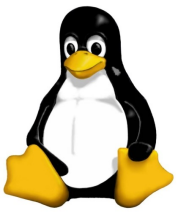
## Iptables e Firestarter

Firestarter è l'interfaccia grafica a iptables, il firewall di linux

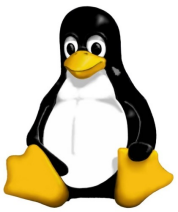
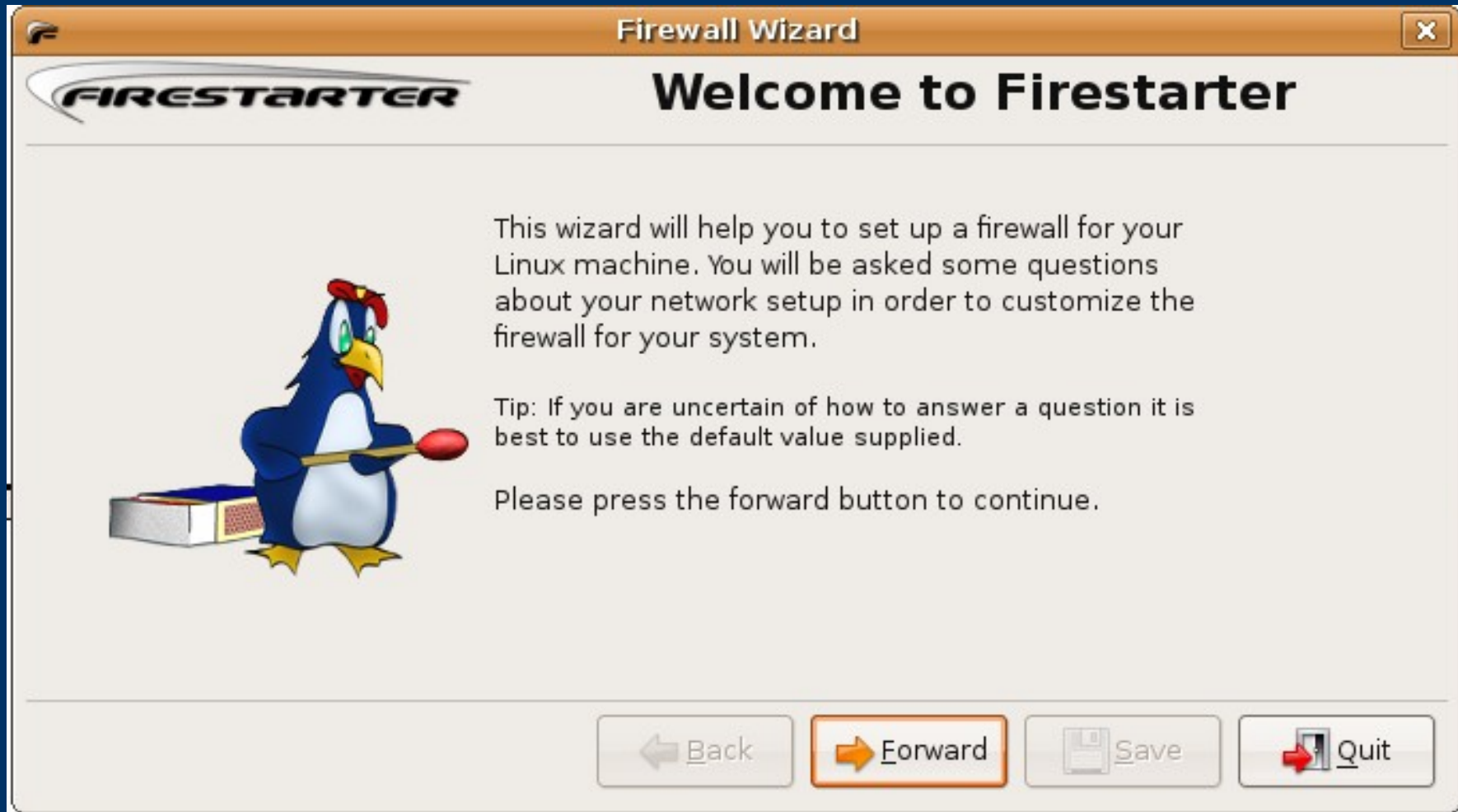
Per installarlo è sufficiente dare il comando

*sudo apt-get install firestarter*

...o alternativamente usare il package manager grafico *synaptic*



# Installazione di Firestarter



# Configurazione di Firestarter

Lanciare Firestarter da System > Administration > Firestarter.

Quando eseguito per la prima volta viene lanciato il processo di configurazione con un wizard. Bisogna scegliere l'interfaccia di rete su cui attivare il firewall e la tipologia di IP assegnato (DHCP o statico)

Si può anche scegliere se condividere la connessione di rete con altri PC

Infine si salva la configurazione e si lancia il programma

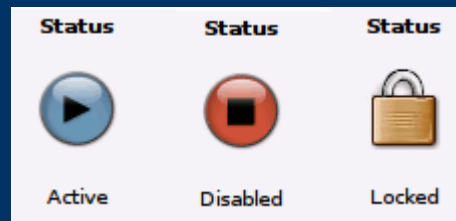


# Opzioni di Firestarter

L'interfaccia grafica ha tre finestre di opzioni: Stato, Eventi e Policy.

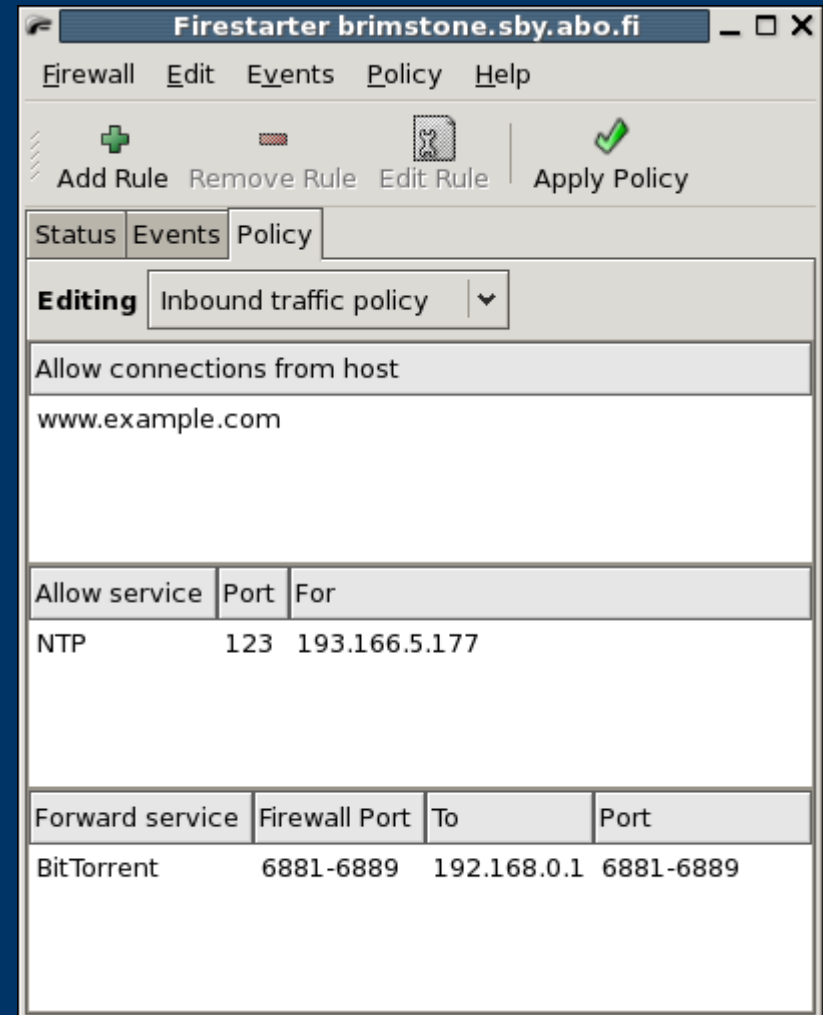
*Stato*: questa finestra dà indicazioni relative allo stato del firewall (attivo = firewall funzionante, disattivo = tutte le connessioni concesse, bloccato = tutte le connessioni sono rifiutate)

*Eventi*: questa finestra dà la lista dei tentativi di connessioni, quelli accettati e quelli rifiutati



# Opzioni di Firestarter

*Policy:* in questa finestra si definiscono le regole per la connessione dall'esterno verso il proprio PC (chi può e chi non può entrare). Queste regole possono essere definite sulla base della porta, del servizio e dell'IP del PC in ingresso



# Linux e virus

*In generale*, GNU/Linux è mediamente al riparo da problemi di virus, perché

- Linux è stato concepito come un sistema multiutente; la suddivisione tra normali utenti e root rappresenta di per sé una protezione contro la manipolazione delle parti più critiche del sistema, pertanto, un virus contratto da un normale utente avrà margini di infezione limitati.
- GNU/Linux è particolarmente attento all'uso dell'hardware; il codice del virus non viene eseguito con la stessa facilità su ogni PC.
- Linux ha ad ora limitata diffusione di questo sistema: se il virus non trova un numero sufficiente di computer da infettare, la sua propagazione sarà necessariamente ridotta, tanto che il tasso di mortalità sarà più elevato del tasso di infezione, con il risultato che il virus si estinguerà.

**Si è, dunque, al sicuro su sistemi GNU/Linux? NO. In linea di principio non vi è nulla che renda GNU/Linux esente da virus, worm, trojan e simili**

Se la diffusione di GNU/Linux in ambito privato continuerà ad aumentare (terzo punto della lista suddetta viene a mancare), ci si dovrà aspettare sempre più attacchi, come nella realtà quotidiana di Windows.

Fonte [wiki.ubuntu-it.org/Sicurezza/](http://wiki.ubuntu-it.org/Sicurezza/)



## Antivirus per linux: ClamAV

Clamav nasce come risposta Open Source ai più che noti antivirus a pagamento. Rilasciato sotto licenza GPL, è in grado di eliminare già a livello dei server di posta o dei gateway, la notevole quantità di virus che oggi giorno prolifera sotto forma di allegati e-mail.

Caratteristiche principali:

scansione di file e directory da linea di comando

- la presenza di un daemon multi-thread molto veloce
- datadase aggiornabile rapidamente con il supporto di firme digitali
- il supporto scansione archivi compressi Rar, Zip, Gzip, Bzip2, Tar
- la gestione diretta della scansione della posta



## Antivirus per linux: ClamAV

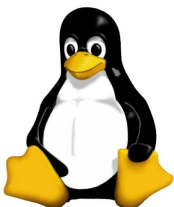
Per l'installazione digitare da terminale:

```
sudo apt-get install clamav
```

Questo installerà il programma in versione applicativo standard; il comportamento della applicazione dipende dalle opzioni della riga di comando.

Esiste, inoltre, la possibilità di far funzionare il programma come daemon (più comoda per un uso orientato a e-mail server oppure se presenti più utenti contemporaneamente)

La configurazione del programma avviene attraverso l' uso del file `clamd.conf` presente nella directory `/etc/clamav`.



## Antivirus per linux: ClamAV

I comandi responsabili della scansione sono rispettivamente:  
clamscan (eseguibile indipendente) o avscan (grafico)  
clamdscan (background)

Alcuni esempi per clamscan:

per effettuare la scansione di tutti i file, directory e sotto directory presenti sul computer:

```
clamscan -r /
```

per effettuare la scansione di tutti i file, cartelle e sottocartelle presenti nella /home:

```
clamscan -r /home
```



# Antivirus per linux: ClamAV

## Aggiornamento definizione dei virus con il comando freshclam

Per esempio

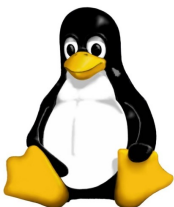
```
user@ubuntu:/etc/clamav # freshclam
ClamAV update process started at Wed Apr 27 00:06:47 2005
main.cvd is up to date (version: 31, sigs: 33079, f-level: 4,
builder: tkojm)
daily.cvd is up to date (version: 855, sigs: 714, f-level: 4,
builder: ccordes)
```

### Proxy

Attenzione nel caso di proxy bisogna cambiare queste righe nel file /etc/clamav/freshclam.conf

```
HTTPProxyServer proxy.unitn.it
HTTPProxyPort 3128
```

Fonte: <http://help.ubuntu.com/community/ClamAV>



## File e alberi delle directory

Il file system di Linux è organizzato in una struttura ad albero gerarchica. Il livello più alto del file system è / o directory root. Nella filosofia di Linux, tutto è considerato un file (inclusi i dischi fissi, le partizioni e i dispositivi rimovibili). Questo significa che tutti gli altri file e directory (inclusi gli altri dischi e partizioni) esistono sotto la directory root . Per esempio, /home/pippo/ubuntu.odt mostra il percorso assoluto al file ubuntu.odt presente nella directory pippo all'interno della directory home che a sua volta è contenuta nella directory root (/). All'interno della directory root (/) è presente un insieme di directory comuni a tutte le distribuzioni Linux.



# File e alberi delle directory

Quello che segue è un elenco delle directory più comuni presenti nella directory root (/):

**/bin** - applicazioni binarie (la maggior parte dei vostri files eseguibili)

**/boot** - i files richiesti per il boot (come il kernel, ecc.)

**/dev** - i vostri dispositivi (dai drives al display)

**/etc** - solo file di configurazione del sistema

**/etc/profile.d** - contiene gli scripts che sono avviati da /etc/profile al login.

**/etc/rc.d** - contiene un numero di scripts di shell che sono avviati al bootup a differenti livelli.

**/etc/rc.d/init.d** - contiene molti scripts di inizializzazione dei sistemi basati su rpm.

**/etc/rc.d/rc\*.d** - dove "\*" è un numero corrispondente al run level preimpostato. Contiene files per i servizi da avviare o terminare in questo run level.

**/etc/skel** - directory contenente molti esempi o strutture di inizializzazione. Spesso contiene sottodirectory e files usati per popolare una home directory di un nuovo utente.

**/etc/X11** - files di configurazione per il sistema X Window

**/home** - files e cartelle personali dell'utente

**/lib** - librerie di sistema (simile ai Program Files)

...continua...



# File e alberi delle directory

... continua:

**/lost+found** - per files perduti

**/media** - dispositivi montati (o caricati) come cdroms, camere digitali, ecc.

**/mnt** - file systems montati

**/opt** - collocazione per programmi installati e “opzionali”

**/proc** - directory dinamica che include informazioni sui processi

**/root** - directory “home” per l’utente di root

**/sbin** - binari solo di sistema

**/sys** - contiene informazioni sul sistema

**/tmp** - files temporanei

**/usr** - applicazioni per utenti

**/var** - principalmente logs, database, ecc.

**/usr/local/bin** - il posto dove inserire i vostri programmi preferiti. Non saranno sovrascritti dagli aggiornamenti.

**/usr/share/doc** - documentazione.



# File e alberi delle directory

Cosa c'è in un pacchetto “deb”?

Dove sono i files del software che ho appena installato?

```
dpkg -L firefox
```

```
/etc/gre.d
```

```
/etc/gre.d/gre64.conf
```

```
/usr/bin/firefox
```

```
/usr/lib64/firefox-2.0.0.19
```

```
/usr/lib64/firefox-2.0.0.19/LICENSE
```

```
/usr/lib64/firefox-2.0.0.19/browserconfig.properties
```

```
/usr/lib64/firefox-2.0.0.19/chrome
```

Ecc...

Ogni file è nella directory con una ben determinata funzione → ordine nella struttura delle directory, ordinate per funzione e non per contenuto



# Indicizzazione dei file

Tracker consente di indicizzare e trovare i file sulla base del nome e del loro contenuto, ovvero posso trovare dei file anche se solo mi ricordo una parola chiave contenuta all'interno, non necessariamente nel titolo.

Installazione di tracker... se già non c'è:

```
sudo apt-get install tracker
```

