



## Firewall su misura. Per tutti

Nell'era preinformatica la parola inglese "firewall" significava solo una cosa: muro, o porta, tagliafuoco, cioè una barriera installata specificamente per impedire il propagarsi di un incendio da una zona a un'altra. I firewall digitali svolgono una funzione analoga nei confronti degli attacchi informatici e sono sempre più indispensabili anche in casa.

Sempre più spesso, oggi, studiamo, lavoriamo e compiamo operazioni delicate (come acquisti online o bonifici bancari) dalle stesse reti domestiche su cui sono sempre più comuni dispositivi niente affatto sicuri. Smart Tv e altre meraviglie del genere funzionano infatti con il protocollo Upnp descritto nel numero scorso, la cui flessibilità ed estrema facilità d'uso hanno un prezzo ben preciso. Nelle sue specifiche mancano funzioni di crittografia e autenticazione, e non per caso. Aggiungerle avrebbe ridotto moltissimo la facilità d'uso *percepita* di Upnp (basti pensare alla reazione dell'utente medio se, per ascoltare con lo smartphone musica archiviata nel suo computer,

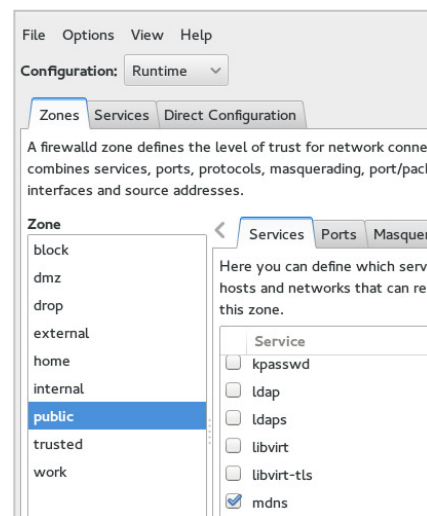
dovesse digitare un'apposita password ogni volta che torna a casa). Per questo, e per non rallentare troppo con algoritmi crittografici troppo pesanti i processori economici di molti prodotti attuali, UPnP poggia sull'ipotesi che tutti i dispositivi e gli utenti di una rete locale siano completamente affidabili. Una condizione sempre meno realistica, in un mondo in cui tutti sono sempre connessi a Internet, spesso senza adeguate conoscenze informatiche. Per questo è indispensabile proteggersi con un firewall (anche se certo non è sufficiente). Sono i firewall

Device	Type	Received	Sent	Activity
eth0	Internet	0.7 MB	0.0 MB	2.2 KB/s
eth1	Local	0.0 MB	0.1 MB	0.0 KB/s
sit0	IPv6 Tunnel	0.0 MB	0.0 MB	0.0 KB/s

Source	Destination	Port	Service	Program
130.232.120.53	66.102.9.99	80	HTTP	firefox-bin
130.232.120.53	204.225.124.69	6667	ircd	xchat
130.232.120.53	216.239.51.104	80	HTTP	firefox-bin

Firestarter è una delle interfacce grafiche a iptables più semplici. Poche schede e pulsanti, ma ben organizzati, e più che sufficienti per le configurazioni più semplici.



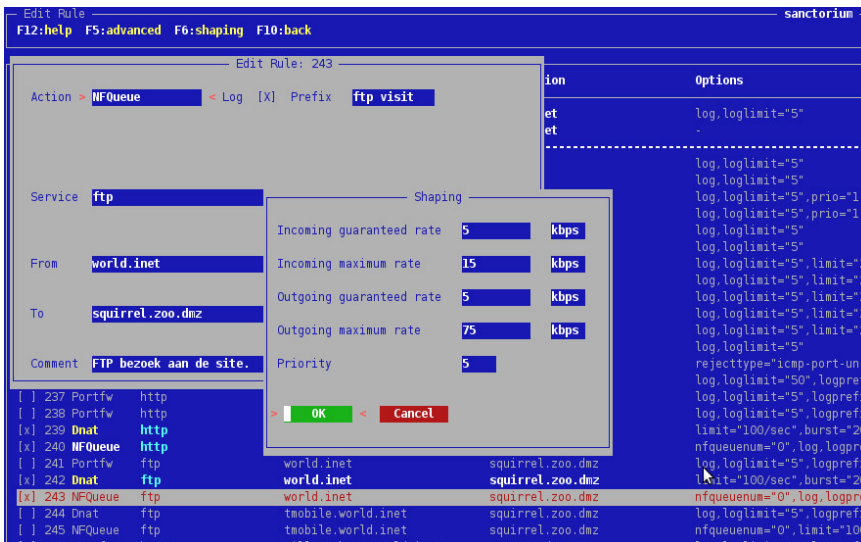
Il Firewall Configurator di Fedora si basa su tre schede corrispondenti a tre modi di lavorare: zone della rete locale, servizi oppure scrittura diretta di comandi iptables.

a filtrare, reindirizzare o semplicemente bloccare i singoli flussi che costituiscono il traffico di Internet, analizzando tutti i pacchetti Ip (Internet Protocol) che li costituiscono, uno alla volta, in tempo più o meno reale.

Oltre al filtraggio in senso stretto, i vari componenti software dei firewall possono anche condividere l'accesso a Internet fra più computer, dando priorità diverse a ogni loro singola connessione, oppure alterare in vari modi (in inglese "mangling") le intestazioni dei singoli pacchetti. Questo mese presentiamo gli strumenti base che svolgono questo lavoro su Linux e alcune delle loro interfacce utente, che vanno da semplici finestre con pochi pulsanti e menu a intere distribuzioni scritte da cima a fondo solo, o quasi, per fare da firewall.

### LE FONDAMENTA DEI FIREWALL LINUX: NETFILTER E IPTABLES

Il software che, sotto Linux, gestisce le operazioni elementari essenziali per un firewall si chiama netfilter (<http://netfilter.org>). Le sue librerie contengono funzioni "agganciabili" direttamente ai vari punti del kernel che gestiscono tutti i pacchetti Ip in transito, per filtrarli come desiderato in base alla loro origine,



L'aspetto (e il nome) di Wuurmuur potrebbero incutere molto più timore rispetto ai programmi concorrenti, ma l'interfaccia a caratteri ha il vantaggio di essere utilizzabile anche in remoto, su connessioni cifrate.

destinazione o natura. Lo strumento che effettua questi "agganci" sotto Linux si chiama iptables. Con questo nome si indicano sia il formato delle tabelle contenenti le istruzioni di filtraggio, sia il programma da riga di comando con cui le si gestisce. Come vedremo nel seguito dell'articolo, non c'è quasi mai bisogno di utilizzarlo direttamente, se non lo si desidera. Anche in quel caso, però, è necessario conoscerne almeno la terminologia e i principi generali di funzionamento per evitare errori.

In ogni computer Linux possono esistere cinque tabelle iptables indipendenti (anche se alcune potrebbero essere utilizzabili solo ricompilando o riconfigurando il kernel). Quella usata più frequentemente si chiama Filter: fra le altre citiamo soltanto, per motivi di spazio, quelle chiamate Nat, Mangle e Security: la prima viene utilizzata quasi esclusivamente per condividere una stessa connessione Internet fra più computer, come descritto nel box in queste pagine. La seconda serve per modificare internamente i pacchetti prima che escano dal computer, e l'ultima applica, a livello Ip, le varie procedure di controllo obbligatorio degli accessi impostate con il sistema SELinux.

Ogni tabella può contenere, oltre alle sue "chain" (letteralmente "catena", in Inglese) predefinite, altre create

dall'amministratore. Le catene predefinite della tabella di filtraggio sono Input (per i pacchetti destinati a programmi locali), Forward (per pacchetti provenienti da altri computer, ma non destinati a quello su cui gira iptables) e Output (per pacchetti generati localmente, ma destinati ad altre macchine).

Una catena iptables non è altro che una sequenza di regole, ognuna contenente certe caratteristiche (classificatori) di una connessione Ip e l'azione da compiere (tramite le funzioni di netfilter) su tutti i pacchetti di ogni connessione di quel tipo.

Ogni pacchetto Ip viene confrontato con tutte le regole delle catene che lo riguardano, una alla volta: se non corrisponde a una regola, si passa a quella successiva, finché non si arriva alla fine della catena, nel qual caso si applica l'azione (policy) di default della catena stessa. Quando la descrizione corrisponde, invece, il kernel compie immediatamente l'azione da essa indicata.

Non esiste una policy o gruppo di policy di default validi per tutti i casi: la maggioranza dei desktop ha una configurazione iptables che lascia passare tutti i pacchetti di connessioni che *nascono* sul desktop stesso, cioè da programmi lanciati dall'utente, ritenuto affidabile fino a prova contraria. Per i server, invece, è molto più frequente il criterio opposto,

### Netfilter

È il nome di un componente fondamentale del kernel di Linux che intercetta e gestisce tutti i pacchetti di dati in transito

## INDIRIZZI, PORTE E LORO TRADUZIONI

Il Simple Object Access Protocol (Soap, [www.w3schools.com/webservices/ws\\_soap\\_intro.asp](http://www.w3schools.com/webservices/ws_soap_intro.asp)) è uno standard per lo scambio di messaggi tra componenti software, formattato secondo la sintassi XML, che sta vivendo una nuova stagione di popolarità proprio grazie al suo uso nei "salotti intelligenti". Normalmente la parte che invia la richiesta iniziale è chiamata client, e quella che la esegue Web Service. La parte "object" della definizione indica che richieste e risposte seguono le regole classiche della programmazione orientata agli oggetti. Soap venne sviluppato nei primi anni duemila per portare su Web le chiamate di procedure software remote, cioè le richieste a un programma, da parte di un altro che gira su un altro computer, di svolgere qualche operazione per conto di quest'ultimo. Questo era possibile anche prima, ovviamente, ma non sempre praticabile attraverso Internet. I messaggi Soap, che sono scritti in Xml, vengono trasmessi con i protocolli Http o Smtpt, cioè viaggiano sugli stessi canali normalmente utilizzati da pagine Web e, rispettivamente, posta elettronica.

per comprensibili ragioni di sicurezza: come default, si inizia dicendo a iptables di bloccare qualsiasi trasmissione di pacchetti in entrambi i versi. Dopo si aggiungono regole per lasciar passare alcuni tipi di traffico, e soltanto quelli.

In generale, una singola azione iptables potrebbe anche essere il passaggio a una nuova catena, definita dall'amministratore di sistema, ma quasi sempre consiste in un Accept, Reject o Drop. Nel primo caso, com'è facile intuire, al pacchetto viene consentito di proseguire per la sua destinazione finale, che potrebbe essere qualche programma sullo stesso computer, o un generico host su Internet. Le altre due opzioni portano invece entrambe alla cancellazione del pacchetto, ma con una differenza importante: Reject notifica l'azione al programma che ha inviato il pacchetto, Drop no. Quest'ultima scelta, comunissima, si fa ogni volta che non si vuole soltanto negare un certo tipo di accesso, ma anche nascondere la stessa presenza sulla rete di un computer in grado di fornirlo. Le opzioni standard di iptables permettono di creare o rimuovere catene in ogni tavola con un solo comando, oppure di aggiungere o cancellare regole in qualsiasi posizione all'interno di catene già esistenti. Per salvare una configurazione appena creata, in modo che venga caricata automaticamente a ogni avvio si deve invece usare un comando separato, chiamato iptables-save. L'ultimo concetto generale di iptables che bisogna conoscere, prima di poter utilizzare con successo questo programma o una qualsiasi delle sue interfacce, è sostanzialmente semplice, anche se ha un nome oscuro. Parliamo del cosiddetto *stateful filtering*, spesso chiamato anche *stateful packet inspection* (Spi).

Di per sé, tutte le procedure generali descritte finora sono senza memoria o, in

Firewall Rules						
New rule						
Firewall Rules						
#	Protocol	Source	Log	Destination	Action	
1	All	Controlling	<input type="checkbox"/>	RED	<input checked="" type="checkbox"/>	
2	All	OVPN-N2N-1	<input type="checkbox"/>	BLUE	<input checked="" type="checkbox"/>	
3	All	PC-1	<input type="checkbox"/>	OVPN-N2N-2	<input checked="" type="checkbox"/>	
4	All	PC-1	<input type="checkbox"/>	IPsecn2n1	<input checked="" type="checkbox"/>	
Policy: Blocked						
Incoming Firewall Access						
#	Protocol	Source	Log	Destination	Action	
1	TCP	Any	<input type="checkbox"/>	RED: 444	<input checked="" type="checkbox"/>	
2	TCP	Any	<input type="checkbox"/>	RED: 222	<input checked="" type="checkbox"/>	
3	All	ovpn11	<input type="checkbox"/>	GREEN	<input checked="" type="checkbox"/>	
Policy: Blocked						

L'interfaccia a tabelle colorate del firewall di IpFire, ognuna corrispondente a un diverso segmento di rete, non è certo all'ultima moda, ma è comunque molto intuitiva ed efficiente.

termini più tecnici, "prive di stato" (in Inglese "stateless"): questa espressione significa semplicemente che ogni singolo pacchetto viene modificato, accettato o respinto solo in base alla sua corrispondenza con almeno una delle regole di una qualsiasi catena iptables. Origine, caratteristiche e storia del flusso di traffico di cui quel pacchetto fa parte non fanno alcuna differenza.

Questo modo di procedere, per quanto semplice, ha però un limite gravissimo che renderebbe iptables inutile se non ci fosse il modo di disattivarlo. Moltissime comunicazioni, infatti (incluse tante fra esseri umani), devono infatti consistere per forza di due flussi, distinti e viaggianti in sensi opposti, fra i due enti che comunicano. A livello dei firewall questo significa che bloccare qualsiasi pacchetto di tipo Ftp in ingresso al computer (per rifiutare di farne un server

Ftp) impedirebbe anche agli utenti dello stesso computer di scaricare file da altri server Ftp su Internet.

La soluzione è appunto un filtraggio che tenga conto dello stato ("stateful", appunto) di ogni singola connessione. In sostanza, si deve poter dire a iptables "blocca tutti i pacchetti di questo tipo in ingresso, da qualunque computer siano arrivati, a meno che non siano risposte a connessioni dello stesso tipo, iniziate da questo stesso computer". Per fare questo bastano due comandi, come mostra questo esempio volutamente incompleto, per ragioni di spazio e semplicità espositiva (ma il Box Risorse elenca diversi tutorial pratici per iptables!):

```
iptables -A OUTPUT --dport ssh
--state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT --sport ssh
--state ESTABLISHED -j ACCEPT
```

## RISORSE

Il wiki italiano della distribuzione Arch Linux include una buona introduzione a vari dettagli dei firewall ([https://wiki.archlinux.org/index.php/Firewalls\\_%28Italiano%29](https://wiki.archlinux.org/index.php/Firewalls_%28Italiano%29)). Una spiegazione più approfondita, sempre in Italiano, si trova su [www.extraordy.com/sicurezza-firewall-basi-e-progettazione-di-iptables-prima-parte](http://www.extraordy.com/sicurezza-firewall-basi-e-progettazione-di-iptables-prima-parte). Il portale Distrowatch mantiene, insieme a tanti altri, anche un elenco aggiornato delle distribuzioni di Linux create apposta per offrire questo servizio (<http://distrowatch.com/search.php?category=Firewall>). Fra i tanti articoli e tutorial online che spiegano l'uso pratico di iptables con esempi concreti segnaliamo <http://openskill.info/topic.php?ID=155> (in Italiano) e le pagine Web [www.cybercity.biz/tips/linux-iptables-examples.html](http://www.cybercity.biz/tips/linux-iptables-examples.html), [www.golinuxhub.com/2014/03/how-to-allow-block-ssh-connection-from.html](http://www.golinuxhub.com/2014/03/how-to-allow-block-ssh-connection-from.html) e [www.thegeekstuff.com/2011/03/iptables-inbound-and-outbound-rules](http://www.thegeekstuff.com/2011/03/iptables-inbound-and-outbound-rules).





Il primo comando appende (-A) alla catena di uscita della tabella di filtraggio la regola di lasciar passare (Accept) tutti i pacchetti appartenenti a connessioni nuove ("new") o già attivate ("established") per la porta Ssh (trasmissioni cifrate) di qualsiasi altro computer. Il secondo comando appende alla catena di ingresso della stessa tabella una regola speculare quasi identica, che lascia entrare pacchetti Ssh, ma solo se appartengono a connessioni già attive. È evidente che in questo modo il computer che usa quel firewall potrà connettersi per primo a qualunque altro computer via Ssh, mentre il contrario sarà impossibile.

## OLTRE I FIREWALL ISOLATI: LE DMZ

Chiunque volesse usare in casa dispositivi Upnp, poco o per niente sicuri, oppure accedere anche da fuori, via Internet, a uno e uno solo dei computer domestici potrebbe aumentare la sicurezza della sua rete locale proprio con un firewall, anche se da solo non basterebbe certo a garantirla.

Configurando opportunamente un firewall si può infatti collocare qualsiasi cosa capace di connettersi a Internet per suo tramite (inclusi console per giochi, Smart Tv e terminali mobili) in due sottoreti locali separate, con scopi e privilegi ben distinti. Nella prima andranno tutti gli oggetti che non devono affatto essere raggiungibili da Internet (anche se potrebbero connettersi ad essa su esplicita richiesta del loro utente locali). L'altra sottorete, fisicamente connessa a una diversa interfaccia (cablata o wireless) del firewall, ospiterà invece tutti e soli i dispositivi che devono per forza essere raggiungibili da Internet, altrimenti sarebbero inutili (si pensi a una webcam con funzioni antifurto). Questa seconda zona viene chiamata "zona demilitarizzata" (Dmz), a indicare che è una sorta di terra di nessuno ad alto rischio. Il firewall filtrerà tutti i pacchetti che lo attraversano in modo che la rete interna sia effettivamente irraggiungibile (nel senso già spiegato) sia dall'esterno, sia dalla stessa Dmz. In questo modo, anche se un cracker riuscisse ad assumere il controllo di un terminale raggiungibile perché "abbandonato" nella Dmz, non potrebbe servirsene per attaccare il resto della rete locale.

## INTERFACCE LINUX PER I FIREWALL

L'interfaccia utente più diffusa, affidabile, portatile e flessibile per configurare firewall Linux è senz'altro uno o più script shell contenenti la giusta sequenza di comandi iptables. Come mostrano le schermate in questo articolo, sono disponibili parecchie alternative con interfacce grafiche per tutti i gusti. Sotto il cofano, prevedibilmente, tutti quei programmi non fanno altro che chiamare iptables, con le opzioni corrispondenti ai pulsanti appena cliccati dall'utente. Le differenze stanno solo nell'aspetto e nella quantità di pulsanti e menu predefiniti, nella varietà di interfacce disponibili e nella documentazione che accompagna ogni applicazione. Ufw, il firewall di default per Ubuntu, lavora sia da riga di comando sia con interfaccia a finestre, così come FireStarter ([www.fs-security.com](http://www.fs-security.com)). Oltre alle funzioni di filtraggio vere e proprie, FireStarter può gestire configurazione Dhcp, Nat/Pat, "liste nere" di siti da interdire a priori e visualizzazione dinamica di tutte le connessioni che blocca.

Shorewall (<http://shorewall.net>) ha funzioni simili, controllabili da browser tramite il server Webmin ([www.webmin.com](http://www.webmin.com)).

L'interfaccia ricca di schede del "firewall configurator" di Fedora/Gnome facilita la creazione di Dmz e tante altre zone su una stessa rete locale, con tutte le opzioni possibili a portata di clic. Meno facile da definire è Vuurmuur ([www.vuurmuur.org](http://www.vuurmuur.org)). La "missione" dichiarata di quest'ultimo è lasciar amministrare firewall anche a chi non ha alcuna conoscenza precedente di iptables, tramite regole con una sintassi "leggibile da esseri umani".

L'interfaccia utente però, anche se dotata di menu e moduli, è a caratteri, quindi accessibile solo dall'interno di un terminale. A compensazione di questa complessità (più apparente che reale) Wuurmuur può essere controllato automaticamente da script, e rende relativamente facile anche impostare velocità e ritardo medio di ogni connessione (traffic shaping), monitoraggio in tempo reale e altre operazioni non proprio per principianti.

**DMZ: zona demilitarizzata**  
Un segmento isolato della rete locale i cui host hanno limitazioni nella connessione verso il resto della rete



## Distribuzioni da firewall: IpFire e gli altri

Qualsiasi distribuzione Linux include almeno una delle interfacce grafiche a Iptables citate nell'articolo principale. D'altra parte, se si vogliono fare le cose sul serio, anche su una semplice rete domestica con 4 o 5 terminali fra computer, tablet e simili non è il caso di configurare (e soprattutto tenere aggiornati) un firewall diverso in ogni singolo computer. Prima di tutto per risparmiare tempo, e in secondo luogo per centralizzare la gestione, cioè per poter imporre gli stessi vincoli e controlli su tutta la propria rete locale. I modem Adsl commerciali hanno tutti un firewall incorporato, ma con opzioni forzatamente limitate. Molto meglio, se appena è possibile, dedicare a firewall e servizi simili un computer separato, che non sia usato per nient'altro. Su questa macchina, che potrebbe essere anche un microcomputer tipo Raspberry Pi o alla peggio una macchina virtuale, si potranno installare distribuzioni ad-hoc come quelle descritte nei paragrafi seguenti.

### IPFIRE ([www.ipfire.org](http://www.ipfire.org))

IpFire fa la parte del leone in questo articolo perché ci sembra una delle più versatili e complete fra le distribuzioni specializzate per "protezione" di reti locali. Il primo motivo d'interesse di IPFire è che è sì una distribuzione Linux, ma completamente autonoma, anziché l'ennesimo fork di prodotti come Fedora o Debian. Ogni singolo pacchetto viene compilato e integrato direttamente dai suoi sorgenti, per ottimizzare tutto senza dipendere da cicli di aggiornamento di terze parti. Solo così, infatti, IPFire

può accoppiare le versioni più stabili e sicure di ogni programma a quelle più recenti, ma sempre aggiornate con le patch grsecurity (<http://grsecurity.net>), del kernel Linux vero e proprio. Il risultato è un nucleo di IPFire sempre allo stato dell'arte, sia come sicurezza che come supporto hardware, senza compromettere la stabilità dell'intero sistema.

**Oltre ai suoi aggiornamenti**, effettuabili con pochi clic grazie al gestore software nativo chiamato Pakfire ([pakfire.ipfire.org](http://pakfire.ipfire.org)), IpFire può anche velocizzare quelli di tutti gli altri computer della sua rete locale! Che si tratti di nuovi pacchetti Linux o di Service Packs di Windows, Pakfire manterrà una copia locale di quei file nella sua cache (archivio locale), per non doverla scaricare di nuovo da Internet quando servirà a un altro client.

Passando al Firewall vero e proprio, l'interfaccia di IPFire facilita la creazione di zone indipendenti ("segmenti") con uno schema di colori tanto semplice quanto flessibile: il verde indica i normali desktop connessi a rete cablata, che possono accedere a Internet, o agli altri segmenti locali, più o meno

come vogliono. All'estremo opposto, i computer a cui non è consentito comunicare con altri segmenti o con Internet vanno nella zona rossa. Per i terminali connessi tramite Wi-Fi, che è per sua natura un tipo di rete meno sicuro, esiste un segmento blu separato, con restrizioni e controlli, predefiniti ma modificabili, intermedi a quelli dei primi due. Ovviamente, è predefinita anche una Dmz classica, riconoscibile dal colore arancio. Ma il bello di IpFire è che il suo gestore di firewall è solo una di una serie di funzioni troppo lunga per riuscire a citare tutte quelle più interessanti.

**Ci limiteremo** a dire che con IpFire si possono facilmente bloccare gli accessi a siti Web indesiderati, con liste nere preimpostate o create dall'amministratore, che contiene un antivirus per le pagine Web, quel che serve per creare reti criptate fra più uffici di una stessa azienda. Può girare anche su un Pentium 1 con 128 MB di memoria e 2 Gbyte di disco.

E se IpFire non piace di distribuzioni specializzate per firewall ce ne sono altre, per ragioni di spazio ne qui ne citiamo solo altre due.

## **IPCOP** ([www.ipcop.org](http://www.ipcop.org))

Lo slogan di questa distribuzione Linux per reti domestiche o di piccole aziende è "I pacchetti cattivi si fermano qui!". Tutte le funzioni di IPCop sono configurabili da qualsiasi browser. Come IpFire, anche qui l'amministratore può valutare sia la configurazione del sistema, sia i grafici che mostrano in tempo reale traffico e altre prestazioni, tramite semplici grafici e schemi a colori.

## **ZEROSHELL** ([www.zeroshell.org](http://www.zeroshell.org))

La differenza fra IpFire, IpCop e Zeroshell è che quest'ultima sembra molto più adatta all'impiego su microcomputer e a gestire reti wireless perdendo meno tempo possibile. Gli sviluppatori forniscono sia una immagine per Cd Live, sia una per memorie Compact Flash. Zeroshell è predisposta per funzionare immediatamente, se installata su computer con chipset Atheros, come Access Point e firewall per reti Wi-Fi 802.11a/b/g, con gestione semiautomatica di tutte le procedure di autenticazione e gestione delle chiavi crittografiche. •

## **LIBREOFFICE** **STA PER SBARCARRE** **SU INTERNET**

**N**ei prossimi mesi LibreOffice Online potrebbe portare la suite per ufficio libera da cui prende il nome anche sul famigerato "cloud". Si potranno quindi finalmente creare o modificare testi, fogli elettronici e presentazioni nel formato aperto OpenDocument (ODF), senza installare nulla sul proprio computer, ma usando comunque un'applicazione Open Source che supporta nativamente ODF. È stato annunciato l'accordo ufficiale fra le aziende IceWarp e Collabora, per sviluppare insieme LibreOffice Online, che si propone come concorrente di Google Docs e Microsoft Office 365.

## **FREEPTO, SOFTWARE LIBERO** **E MASSIMA SICUREZZA SEMPRE IN TASCA**

**F**reepto ([www.freepto.mx](http://www.freepto.mx)) è un sistema GNU/Linux completo, che gira interamente da chiavetta Usb, creando su quest'ultima una cartella cifrata in cui conservare e portarsi sempre dietro tutti i propri documenti riservati. A differenza della maggior parte delle distribuzioni portatili, Freepto è scritta (e mantenuta da un gruppo di sviluppatori italiani) specificamente per navigare online con la massima sicurezza e privacy possibili, senza però rinunciare alla comodità di un sistema operativo tradizionale. Su Freepto si trovano infatti, già installati e preconfigurati, il Tor Browser Bundle, che facilita moltissimo (ma, da solo, non garantisce!) la navigazione automatica sul Web grazie a una versione modificata del browser Firefox, e il cosiddetto "Wipe". Quest'ultimo è uno strumento, attivabile con un clic dal menu del file manager di Freepto, con cui cancellare in maniera sicura singoli file o intere cartelle dalla chiavetta stessa, o dal disco rigido a cui si appoggia. Un altro strumento simile provvede a rimuovere i metadati confidenziali presenti in fotografie e altri documenti digitali, come nome dell'autore o luogo e ora di uno scatto. BleachBit, sempre incluso in Freepto, si occupa di cancellare i dati sensibili dalla cache del browser e nei temporanei generati da altri programmi. La documentazione in Italiano di Freepto si trova su <http://we.riseup.net/freepto-wiki/freepto-docs>.