



# Linux server sicuro in Azienda

© 2001 Francesco Collini per Collini Consulting s.a.s.

**Linux e...  
l'importanza di  
vedere ciò che "ci si  
mette in casa..."**

In questi ultimi anni stiamo assistendo ad una crescita esponenziale della presenza del software libero "open-source" in ambito enterprise, che ha affiancato e sta ormai superando il classico software commerciale, chiuso e vincolante nella fascia server. L'esempio più eclatante è rappresentato dal sistema operativo Linux, ideato da uno studente finlandese nel 1991 come clone del sistema Unix e sviluppato, aggiornato ed supportato oggi da migliaia e migliaia di programmatori sparsi in tutto il mondo e pienamente supportato dalle major software e hardware mondiali.

Linux è un sistema operativo stabile, scalabile e sicuro ma il suo punto di forza risiede nella grande possibilità di apertura del suo codice sorgente: è infatti possibile vedere, modificare ed analizzare le istruzioni che i programmatori hanno scritto: Linux è free-software, open-source" per eccellenza. Le sue qualità in ambito server non hanno uguali; cioè è stato anche dimostrato da autorevoli analisi e studi condotti mediante l'utilizzo di comprovati strumenti di benchmarking.

## **File Server**

I server Linux con l'implementazione del modulo *Samba* consentono la piena compatibilità, visibilità e integrazione in reti miste con pc che utilizzano i principali sistemi operativi Microsoft Windows, quali 95/98/Me/2000/XP. Samba implementa infatti il protocollo *SMB* per emulare appieno le funzionalità di un PDC Windows NT 4.0 / Windows 2000.

E' così possibile avere un dominio Windows mediante il quale autenticare gli utenti con la propria password all'avvio del pc, utilizzare script di logon e i profili utente in roaming, e mettere in comune programmi, file (ad es. tutti i documenti di videoscrittura) e stampanti di rete.

La gestione dei back-up viene di solito affidata ad una unità nastro ad alte prestazioni che in modo completamente automatico provvede a salvare una copia di tutti gli archivi durante le ore notturne quando il server non viene comunemente utilizzato.

Sono altresì implementati tutti i servizi di rete come DNS, DHCP, WINS ecc. ecc. a tutti i client della LAN.

## **La posta elettronica**

Linux viene ormai utilizzato nella stragrande maggioranza dei server utilizzati per scambiare posta elettronica e da quasi tutti gli Internet Service Provider (ISP).

Il server di posta elettronica *Qmail*, ampiamente utilizzato anche su domini postali ad altissimo traffico, consente di gestire illimitati indirizzi di posta elettronica, mailing-list, autorisponditori e forwarders.

E' inoltre implementata la richiestissima funzionalità di WebMail, mediante la quale un utente può ricevere ed inviare posta elettronica anche se non si trova sulla scrivania del proprio ufficio; basta infatti connettersi via web mediante un comune browser da una qualunque postazione del Globo collegata ad Internet. L'accesso web alla propria mailbox avviene inserendo la propria userid e password crittografate da una trasmissione SSL criptata al riparo da

malintenzionati mentre attraversa Internet.

Ultimamente si possono integrare direttamente all'interno del server postale antivirus di fascia enterprise che controllano ogni messaggio in entrata/uscita dall'Azienda direttamente all'interno del server SMTP, *prima* che esso giunga nel computer dell'utente finale.

## **Fax Server**

Integrato con la posta elettronica è disponibile, sempre in ambito open-source, un server fax estremamente stabile e flessibile, che è in grado di gestire anche più modem sia in invio che in ricezione.

A corredo del motore server fax, che ricordiamo gira in background nativo sotto Linux, l'invio e la ricezione dei messaggi sono supportati da facilissimi programmi client interamente funzionanti sotto Windows 32 ed ora anche funzionanti sotto Macintosh; l'utente finale ha quindi un'interfaccia completamente user-friendly per gestire le proprie comunicazioni fax. La ricezione dei fax e la gestione delle conferme di invio messaggi sono completamente integrati all'interno della propria posta elettronica.

## **GroupWare**

Sempre utilizzando la stabile e robusta piattaforma Linux quale server sono fruibili piattaforme di lavoro di gruppo quali Lotus Notes/Domino con principali funzioni di posta interna/esterna, gestione contatti di gruppo e pianificazione del tempo delle risorse umane dell'Azienda.

Lotus Notes / Domino è leader nel campo delle soluzioni di messaging e piattaforme per il lavoro di gruppo; Lotus supporta pienamente il server Domino sotto server Linux.

## **La sicurezza all'interno dell'Azienda**

Internet è diventato nell'Azienda un indispensabile strumento di lavoro in dotazione a tutto il personale; è importante però valutare anche i rischi che da questo ne conseguono, ovvero l'abuso e la possibilità che vengano commessi illeciti tramite la Rete. Adottando un Proxy Server trasparente ed invisibile all'interno dell'Azienda, il gateway Linux distribuirà la connettività ad Internet secondo le politiche di sicurezza aziendali che il management vorrà comunicarci. Sarà perciò possibile inserire filtri che permettano, ad esempio, di inibire l'accesso a siti a carattere pornografico, limitare l'uso solo in particolari orari, impedire che vengano scaricati files, videogiochi e programmi senza autorizzazione e monitorarne l'attività.

## **La sicurezza all'esterno dell'Azienda**

Sono sempre più richieste ultimamente valide soluzioni di security aziendale. Grazie alla sua estrema versatilità di utilizzo Linux è largamente utilizzato come firewall di una rete; il *muro di fuoco*, traduzione letterale dall'inglese, separa la rete aziendale interna da Internet ed è in grado di accettare e respingere il traffico lecito e quello illecito, mediante funzioni costruite direttamente dentro al kernel (cuore) del sistema operativo Linux.

E' opportuno implementare all'interno del firewall adeguati sistemi di logging e

anti-intrusione che, monitorizzando costantemente i log del sistema (i logs non sono altro che il “diario di bordo” dove è descritta qualunque cosa accada) sono in grado di rilevare comportamenti anomali e bloccare istantaneamente gli indirizzi IP di provenienza delle macchine che hanno tentato un'intrusione, allertando immediatamente gli amministratori del sistema tramite e-mail.

## **Le VPN**

Oggi giorno Internet ci offre una enorme potenzialità: quella di potere scambiare dati con qualunque parte del mondo, ormai a banda larga. Nasce così spontanea l'idea di collegare branchie di reti aziendali remote, distanti fra loro, in modo molto più economico di come si faceva con le costosissime linee dedicate.

Direttamente integrate all'interno del firewall-Linux descritto nel paragrafo sopra sono installabili soluzioni *VPN (Virtual Private Network, rete privata virtuale)* in ambito open-source che permettono di crearsi una rete geografica sicura, un proprio perimetro, all'interno di una rete potenzialmente insicura qual è Internet. La VPN consente anche ai dipendenti di un'Azienda il collegamento alla rete aziendale.

## **L'Assistenza**

Un qualunque prodotto software è sicuro nel momento in cui si fornisce un adeguato monitoraggio e un costante aggiornamento del prodotto ogni qualvolta escano patch e/o bugfix (correzioni) che coprano eventuali buchi di programmazione minacciando la stabilità e la sicurezza del sistema. E' altrettanto importante tenere monitorati i log di sistema al fine di individuare eventuali scansioni da parte di *cracker* (pirati informatici) e/o comportamenti anomali.

Completamente da remoto, tramite shell sicura SSH o via modem, è possibile effettuare le operazioni di ordinaria manutenzione, aggiornamento e monitoraggio del sistema, apportando e segnalando al responsabile CED eventuali modifiche.