

## Macintosh: Configurare i requisiti di sicurezza con MacOS X

di Giorgio Ginelli

L'evoluzione del sistema operativo di Apple ha determinato sostanziali cambiamenti nella gestione delle connessioni e dunque nella sicurezza, mantenendone però sempre molto alti i requisiti minimi.

Mac Os X garantisce i più alti livelli di protezione grazie allo sviluppo software open source e all'adozione di standard precisi. Il cuore open source di MacOS X si chiama Darwin e offre Kerberos, Secure Shell (OpenSSH), un framework per transazioni sicure via Internet (OpenSSL) e la protezione dei documenti con permessi UNIX in stile BSD.

Darwin presenta un'architettura a memoria protetta che assegna uno spazio unico a ciascuna applicazione, consentendo in questo modo un uso continuo del computer, senza che il malfunzionamento di un'applicazione vada a bloccare l'intero sistema. Ma al di là dei tecnicismi, l'azione fondamentale è sempre quella di definire lo scenario all'interno del quale ci si deve muovere: computer privato o piattaforma aziendale. Il singolo utente – casalingo o professionale che sia – non deve gestire accessi a livelli diversificati e neppure dover consentire l'accesso alla propria piattaforma ad utenti remoti. In ogni caso, comunque, le attuali versioni del nuovo sistema operativo di casa Apple, hanno tutti gli strumenti di difesa utili a fronteggiare le differenti situazioni.

Cuore di tutto il sistema organizzativo sono comunque le Preferenze di sistema, dove si trova l'impostazione della Condivisione.

### MacOs X 10.2 – Jaguar

In questa versione del MacOS X, la finestra Condivisione ha il compito di attivare e disattivare tutti i servizi principali presenti sulla piattaforma; è composta da tre pannelli differenti che consentono una più che discreta parametrizzazione delle impostazioni di sicurezza.

- **Servizi.** Il pannello Servizi (figura 1a) consente di selezionare i servizi che si vogliono attivare per un determinato utente: Web Server e Server FTP, dunque, ma anche condivisione documenti o stampanti. Per quest'ultima è comunque indispensabile avere sia sulla piattaforma che funge da server di stampa la stessa versione di MacOS esistente sulla piattaforma client; per intenderci, non si può condividere una stampante tra MacOS X e le versioni precedenti.
- **Firewall.** MacOS X ha un firewall integrato (figura 1b) che consente tutti i controlli di base in grado di assicurare un grado di sicurezza più che sufficiente ad un tipo di utilizzo tipico, che può essere l'uso anche professionale di una singola piattaforma. Il firewall integrato in MacOS è di tipo chiuso e può essere anche gestito da terminale, il che potrebbe essere un sollievo per gli utenti Unix, ma un incubo per tutti gli altri;
- **Internet.** Questa scheda (figura 1c) gestisce tutte le configurazioni utilizzate nel caso di connessione condivisa della piattaforma per la navigazione in rete. In pratica la piattaforma diviene un router, ed offre la possibilità a tutta la lan di accedere ad Internet. Ovviamente questa possibilità dovrà essere gestita nella maniera corretta anche nel pannello Network, dove dovranno essere create le opportune connessioni.

## **Il nuovo portachiavi**

Uno dei fulcri del sistema di sicurezza rimane il Portachiavi, che diviene una vera e propria centrale di controllo (figura 2). Nato con la versione 9 del MacOS, la sua funzione era semplicemente quella di tenere traccia delle password delle utenze registrate su un computer.

Con la versione MacOS X, il portachiavi è creato alla prima configurazione del sistema, può essere poi modificato e aggiornato costantemente e viene attivato al momento del login, quando si digita la password dell'utente.

Fondamentalmente la sua funzione è comunque quella di gestire le decine di password e permessi tipici di un utilizzo on-line del computer; in effetti il Portachiavi archivia tutte le informazioni necessarie per accedere a server file, ftp e web, oltre a utilizzare immagini disco criptate (figura 3).

Per sicurezza, infatti, è possibile con MacOS X criptare parte del disco rigido utilizzando un'immagine disco per inviarla ad altri utenti in possesso della password (figura 4). Un disco criptato compare sulla scrivania come un volume, ma l'utilizzo del contenuto è possibile solo sbloccando il Portachiavi con la password adeguata.

È possibile creare portachiavi diversi per conservare password che possono servire a diversi scopi, ad esempio per il lavoro e per lo shopping su Internet; oppure è possibile fare una copia di un portachiavi in modo da poterlo portare su altri computer.

## **Connettersi in una rete mista**

Una delle maggiori preoccupazioni dei progettisti di Cupertino, è stata senz'altro adeguare il supporto del MacOS X per la connettività a reti nelle quali sono presenti piattaforme dotate di diversi sistemi operativi. Anche in questo caso per la sicurezza devono esistere barriere solamente nei punti critici, in modo che il sistema operativo sia uno strumento semplice da utilizzare e sicuro, sia per il server che per il client.

La condivisione inizia selezionando il comando Collegamento al server dal menu Vai posto sulla barra del Finder (figura 5), dopo aver opportunamente impostato i parametri di connessione attraverso il pannello Network in Preferenze di sistema (figura 6), nel quale sono raggruppate tutti i parametri per la connessione con i differenti protocolli.

Scelto il server al quale collegarsi, viene attivato il protocollo SMB, che consente di selezionare una risorsa tra quelle messe a disposizione dall'indirizzo del server (figura 7), alla quale segue la fase di autenticazione Filesystem SMB/CIFS, dove entrano in gioco i privilegi associati all'utente (figura 8).

## **MacOs X 10.3 – Panther**

Anche se a prima vista può non sembrare, la nuova versione del MacOS implementa numerose potenti novità, a cominciare da Samba3 con supporto nativo per il protocollo di condivisione SMB/CIFS, e per finire con l'implementazione VPN con il supporto agli standard L2TP e PPTP, la cui autenticazione (Ipsec o Ms-CHAP) lo rende ancora più compatibile con client Windows e Linux.

A parte tutto quello che un utente normale non coglie, è sotto gli occhi di tutti gli utilizzatori in che misura la nuova versione integri tutte le funzioni di sistema con l'interfaccia del Finder. Ad esempio, invece di avere finestre di lavoro da selezionare attraverso comandi residenti nel dock, molto più semplicemente si ha a disposizione una cartella Network (figura 9) che contiene tutte le risorse legate alla condivisione; le funzioni sono però identiche a quelle presenti in Jaguar, tranne che per l'aggiunta del modulo di Apple Remote Desktop. Nella nuova versione del sistema operativo, Apple ha dotato l'architettura di servizi directory anche di tutte le funzionalità di autenticazione necessarie e che sono gestite da una Authentication Authority. Si tratta di una tecnologia di riferimento ampiamente collaudata sviluppata dal Mit, nella quale le procedure di autenticazione sono gestite mediante un

algoritmo basato su scambio di chiavi, le quali vengono distribuite dal sistema KDC (Kerberos Distributor Center). Una volta avvenuta l'autenticazione il traffico può viaggiare in rete in forma crittografata e può essere monitorata attraverso l'applicazione Accesso Directory presente nella cartella Utility.

## **DIDASCALIE**

Figura 1 (servizi.tif + firewall.tif + internet.tif) – La finestra con i controlli per la Condivisione è composta di tre schede differenti, ognuna delle quali consente l'applicazione di tutti i parametri necessari alle impostazioni di sicurezza.

Figura 2 (KEY10.tif) – Dal Portachiavi di MacOS X è possibile gestire gli attributi degli elementi inseriti al suo interno, definendo un completo controllo dell'accesso.

Figura 3 (ACCESSO.tif) – Qualsiasi elemento inserito nel portachiavi per poter essere utilizzato o letto, ha bisogno di un'adeguata password.

Figura 4 (CRIPTA.tif) – Il massimo della sicurezza è rappresentato dalla criptatura di volumi o di interi dischi, che necessitano poi di essere sbloccati dal Portachiavi per poterne utilizzare il contenuto.

Figura 5 (server1.tif) – Il MacOS X supporta tutti i protocolli in grado di gestire reti miste, che sono così totalmente trasparenti alla piattaforma Macintosh.

Figura 6 (tcpip.tif + jnetwork.tif) – La finestra delle Preferenze Network è in grado di gestire tutte le impostazioni per il collegamento via Tcp/Ip, Ppp, Proxy e Modem, la cui destinazione può essere indirizzata ai dispositivi che si crede opportuno attivare.

Figura 7 (server2.tif) – SMB consente di scegliere fra le risorse messe a disposizione dall'indirizzo al quale ci si vuole connettere.

Figura 8 (server3.tif) – La procedura di autenticazione è il verso passo che rende possibile la connessione al server.

Figura 9 (Pnetwork.tif) – Con Phanter è possibile avere con un solo colpo d'occhio la situazione delle connessioni presenti sulla piattaforma grazie all'applicazione Network, presente in tutte le finestre.