▶ Firewall

Proteggete il vostro computer dalle intrusioni via Internet

Fino a qualche tempo fa strumenti per utenti più evoluti, i firewall oggi possono essere utilizzati al meglio anche senza grandi competenze tecniche. Ecco come funzionano e quali sono i migliori, gratuiti e a pagamento

Ogni computer collegato a Internet è identificato mediante un numero composto da quattro gruppi di cifre (ad esempio: 123.456.789.123) detto *Indirizzo IP*. Tale indirizzo numerico indica esclusivamente con quale fornitore di accesso Internet siamo collegati e quale macchina del provider stiamo utilizzando per navigare in Rete.

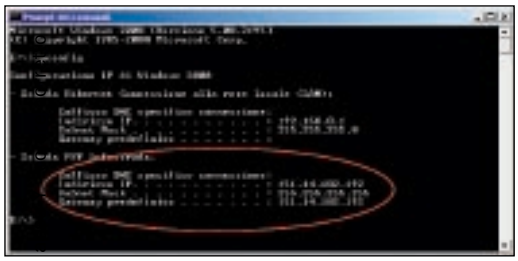
Internet connette, tra loro, milioni di persone in tutto il mondo ed ogni computer è quindi raggiungibile utilizzando l'indirizzo IP che, di volta in volta, ad ogni connessione, gli viene attribuito.

E come in qualunque altra grande comunità è quindi sempre più facile incappare in qualche rompiscatole che tenti di accedere indisturbato e senza autorizzazione al nostro personal, solo per il piacere di far danni.

Se si dispone poi di una connessione a larga barda o di una connessione a Internet pressoché permanente (lo sono oggi le connessioni ADSL ma in molti casi anche quelle di tipo flat), ancora più elevato è il rischio di vedere violato il proprio personal computer. Teniamo a sottolineare che assai raramente chi tenta di entrare nel nostro personal computer è un hacker: a meno che sui vostri sistemi non siano memorizzati dati di grande importanza a livello nazionale ed internazionale oppure che possediate una grande azienda, è assai difficile che un hacker rivolga su di voi la sua attenzione. I "nemici" più comuni sono invece coloro che, armandosi di utility "preconfezionate", tentano di sferrare un attacco verso un qualunque sistema collegato in Rete. In inglese tali persone sono state battezzate *lamer*: spesso trattasi di utenti con scarse competenze tecniche. Tuttavia, possono risultare pericolosi facendo uso di appositi programmi che permettono di mettere a nudo le deficienze in fatto di sicurezza, di un qualunque sistema collegato ad Internet.

Il modo più sicuro per evitare problemi è quello di tenere il proprio computer completamente scollegato dalla rete Internet: una possibilità del tutto

DA SAPERE



In Windows 2000 il comando *ipconfig*, eseguibile dal *Prompt* dei comandi, permette di controllare l'indirizzo IP assegnato in fase di connessione ad Internet. Nelle altre versioni di Windows digitate *winipcfg* in *Start, Esegui...* e premete il pulsante *Ok*.

Sia la versione 2001 di Norton Personal Firewall che la versione 2002 permettono di bloccare o consentire l'accesso a Internet da parte di una qualunque applicazione installata.
È possibile impostare anche delle regole personalizzate che permettano di stabilire il comportamento futuro del firewall.
Norton Personal Firewall 2002 offre informazioni estese sul programma che ha tentato l'accesso alla Rete.

I FIREWALL CHE TROVATE NEL CD ROM DI *PC OPEN*

Firewall	Costo	Sito Internet	Note
Norton Personal Firewall 2002 **Internet Security 2002**	L. 116.400 (60,12 €) L. 193.200 (99,78 €)	www.symantec.it	In italiano. Disponibile anche il pacchetto Internet Security 2002 che include, oltre al firewall, Norton Antivirus e funzionalità per il controllo della privacy e per una navigazione sicura da parte dei bambini.
ZoneLabs ZoneAlarm	Gratuito	www.zonealarm.com/products/za/freedownload2.html	Disponibile anche la versione Professional a pagamento (scaricabile in versione di prova per 30 giorni): essa permette di controllare tutti gli allegati alla posta elettronica e cerca di stabilire chi ha tentato l'attacco al nostro computer e tanto altro ancora.
Sygate Personal Firewall	Gratuito	www.sygate.com/free/spf_download.htm	Esiste anche una versione Professional a pagamento con funzionalità per importare/esportare le regole firewall tra i vari computer, maggiore disponibilità di aggiornamenti.
Tiny Personal Firewall	Gratuito	www.tinysoftware.com	Dotato di manualistica online, in formato PDF e HTML in inglese

impraticabile considerata la sempre maggior importanza che Internet sta oggi acquistando e la sempre maggiore nostra dipendenza dai servizi messi a disposizione online.

Come rendere invisibile il vostro computer

La soluzione che ci proponiamo di mettere in pratica consiste nel rendere il proprio personal computer "nascosto" durante le connessioni Internet.

I *firewall* sono software che fanno da filtro tra le connessioni in entrata e quelle in uscita dal proprio personal computer. Essi consentono, quindi, essenzialmente, di rilevare ciò che avviene durante la connessione Internet, monitorando tutti i dati in uscita ed in entrata. In questo modo è possibile difendersi da tentativi di attacco rivolti verso il nostro personal computer o, più semplicemente, identificare e rendere innocua l'azione di un *trojan virus* che tenti di comunicare informazioni personali attraverso la Rete.

L'utilizzo dei software firewall, unitamente ad un buon antivirus (software dei quali abbiamo parlato nello scorso numero), vi permetterà di proteggere i dati memorizzati sul vostro computer rendendolo immune ad attacchi esterni.

Il vostro obiettivo primario deve essere quello di rendere difficoltoso (meglio se praticamente impossibile) l'accesso alla vostra macchina da parte di persone non autorizzate. In questo modo i vostri "nemici" si rivolgeranno verso altri lidi.

Coloro che installano un firewall rimangono spesso scioccati dal numero di messaggi d'allerta che il programma, a seconda delle caratteristiche specifiche, restituisce loro dopo l'installazione e dopo essersi collegati ad Internet.

In realtà è sufficiente analizzare le informazioni che il firewall stesso fornisce per capire quale situazione più o meno pericolosa si sia determinata. La buona notizia è comunque quella che se il firewall fornisce un messaggio d'allerta, significa che il personal computer è protetto.

La scelta di un firewall deve orientarsi, in primo luogo, su quelli che offrono un controllo adeguato anche sul traffico in uscita: ciò significa che non appena, per la prima volta, un programma tenterà di inviare informazioni via Internet o comunque cercherà di collegarsi ad un sito Internet con lo scopo di prelevare o trasmettere dati, il firewall "metterà in attesa" il tentativo di accesso alla Rete segnalandolo prontamente all'utente.

Questi avrà essenzialmente tre possibilità:

1 - bloccare la comunicazione di rete
2 - consentire la comunicazione di rete
3 - impostare una regola per i tentativi di accesso futuri

Quest'ultimo caso consente di impostare un criterio che permetta di stabilire le azioni che il firewall deve automaticamente compiere qualora, in futuro, dovesse presentarsi un tentativo di accesso alla Rete da parte dello stesso programma installato.

Fino a qualche tempo fa l'utilizzo dei firewall era una prerogativa degli utenti più evoluti: solitamente i vari software non fornivano, infatti, informazioni dettagliate sulle applicazioni che tentavano di accedere a Internet, visualizzando esclusivamente il nome del file eseguibile associato al programma. Oggi invece, i software che vi proponiamo vengono in aiuto all'utente, anche a quello meno esperto, informandolo, in modo esaustivo, sull'applicazione che ha richiesto di accedere alla Rete. I vari firewall dispongono anche di un archivio interno delle varie applicazioni che permette di segnalare quali applicazioni sono fidate, quali lo sono meno od addirittura pericolose.

Nonostante le ultime versioni dei software che abbiamo scelto (**ZoneAlarm**, **Norton Personal Firewall**, **Sygate Personal Firewall** e **Tiny Personal Firewall**) rendano estremamente più semplice, rispetto al passato, l'impostazione di regole firewall personalizzate, è sempre bene assicurarsi di comprendere bene per quale motivo un software tenti di accedere ad Internet e chiedersi se l'azione che esso desidera compiere è stata da noi preventivamente richiesta. Qualora si avessero dei dubbi il nostro consiglio è quello di bloccare il tentativo di accesso: avrete così modo di rendervi conto dell'accaduto. n

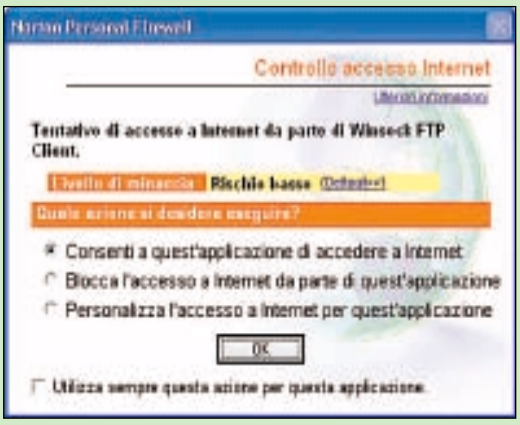
Michele Nasi

IMPOSTAZIONI & CONTROLLI

Sono essenzialmente tre i punti da ricordare per l'utilizzo ottimale di un software firewall

- massimo controllo sulle applicazioni che si installano e che tentano di accedere ad Internet
- rispondere adeguatamente ai messaggi di allerta restituiti dal firewall
- aggiornare periodicamente il firewall

La funzione *Controllo accesso Internet* di Norton Personal Firewall e gli strumenti inclusi in ZoneAlarm, consentono di mettere a nudo tutti i tentativi di accesso alla Rete da parte di una qualunque applicazione. Queste funzionalità sono in grado di scovare le operazioni dannose che tentano di eseguire eventuali *trojan virus* o software *spyware* (applicazioni che mandano in giro attraverso Internet informazioni riguardanti le proprie preferenze e le proprie abitudini).
Quando il firewall visualizza un messaggio d'allerta non si deve cadere in preda al panico: è cosa del tutto normale ed, anzi, evidenzia il corretto funzionamento del firewall stesso.
Nel caso in cui un'applicazione tenti di guadagnare l'accesso alla Rete, viene visualizzata una finestra contenente informazioni dettagliate sul programma.
Il più preciso è Norton Personal Firewall che, rispetto alle precedenti versioni, indica chiaramente di che programma si tratta e viene specificato il livello di minaccia (Norton è infatti in grado di stabilire se il programma sia stato sviluppato da un'azienda conosciuta e fidata nonché di capire se la connessione che sta tentando è sicura o meno). Cliccando sulla voce *Dettagli* è possibile ottenere informazioni ancora più precise: in particolare citiamo l'indirizzo Internet cui l'applicazione cerca di connettersi, la porta utilizzata, il nome dell'azienda che ha sviluppato il programma e tanto altro ancora.
A questo punto l'utente può scegliere se consentire la comunicazione, bloccarla o personalizzarne l'accesso. Attivando la casella *Utilizza sempre questa azione per questa applicazione* la scelta operata dall'utente verrà memorizzata dal firewall nelle impostazioni del controllo accesso Internet: in questo modo se si avvierà in futuro, di nuovo, l'applicazione, il firewall applicherà sempre la scelta selezionata da parte dell'utente, senza mostrare una finestra d'allerta.
In ogni caso, se avete dubbi, bloccate sempre l'accesso ad Internet: avrete il tempo di verificare di che cosa si tratti.



Un esempio di un messaggio di allerta di Norton Personal Firewall 2002. In questo caso un'applicazione che fa uso del servizio FTP per il trasferimento di file ha richiesto di accedere ad Internet. Poiché si tratta di un'applicazione "fidata" che abbiamo eseguito per amministrare il nostro sito Internet via FTP, in questo caso consentiamo la comunicazione di Rete