

## 6. Firewall, il buttafuori digitale

### Cos'è un firewall? E soprattutto, come cavolo si pronuncia?

**Un firewall è l'equivalente informatico di un buttafuori.** Serve a tenere fuori gli indesiderati e a far entrare e uscire soltanto i dati che autorizzate a circolare. E là fuori, su Internet, ci sono tanti individui e virus indesiderati e indesiderabili.

E visto che me lo chiedete, si pronuncia "faier-uool". Be', più o meno.

#### Pericolo!

**Navigare in Internet con Windows senza firewall significa cercarsi guai.**

**Windows XP è dotato di un firewall, ma è normalmente disattivato** (verrà attivato automaticamente nelle prossime versioni). Il che è profondamente stupido, come mettere una porta blindata in casa e non chiuderla a chiave, ma tant'è.

**Non perdetevi tempo ad attivare il firewall integrato in Windows:** per ammissione della stessa Microsoft, è un colabrodo<sup>11</sup> e comunque non blocca il traffico *uscende* dal vostro computer, per cui un virus che vi infetta può lanciare attacchi dal vostro PC verso altri utenti senza che il firewall Microsoft lo fermi in alcun modo.

Le cose migliorano leggermente se usate il firewall aggiornato, denominato *Windows Firewall*, presente nel Service Pack 2, come descritto a fine capitolo.

Installare un firewall è un'esperienza rivelatrice. Potreste pensare che non vi serva, perché tanto non vi capita mai di essere attaccati: non avete nemici così ostili. La realtà è ben diversa: siamo *tutti* sotto attacco quasi continuamente, solo che non ce ne accorgiamo perché Windows non ce lo fa vedere.

Virus e vandali della Rete, infatti, tentano a casaccio di accedere a tutti i computer che trovano connessi. Niente di personale: è un procedimento casuale, chi capita, capita. Il firewall rivela questo brulichio incessante di tentativi d'accesso, e il primo impatto è scioccante.

Tuttavia lo stupore iniziale di vedersi sotto continua aggressione diventa molto presto scocciatura, per cui si tende a disattivare le notifiche (ma non l'efficacia) del firewall, in modo che ci protegga silenziosamente, senza disturbarci ogni volta per dirci "*Ehi! Ho bloccato un altro intruso! Come sono bravo!!*".

La sorpresa successiva nasce quando ci si accorge di quanti dei nostri normalissimi programmi tentano di *uscire* dal nostro computer, anche se apparentemente non hanno ragione di farlo. Windows Media Player, per esempio, tenta spesso di uscire quando vediamo un filmato o ascoltiamo una canzone presente sul nostro computer. Lo fa anche Acrobat. Ho colto in flagrante sia Word, sia programmi alternativi come OpenOffice, sia programmi di elaborazione audio come SoundForge. Perché vogliono uscire? Con chi vogliono comunicare, e cosa vogliono dirgli? Non so voi, ma l'idea che ci siano queste comunicazioni a mia insaputa non mi lascia tranquillo. Nel dubbio, è decisamente meglio impedirle.

<sup>11</sup> [support.microsoft.com/default.aspx?scid=kb;EN-US;Q306203](http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q306203)

Impedire il traffico *uscente* è importante anche per un'altra ragione. Molti virus si insediano nel computer senza fare danno apparente, "zombificandolo", ossia trasformandolo in uno schiavo che ubbidisce segretamente agli ordini del suo misterioso padrone (spesso si tratta di *spammer* o di altri truffatori). Una volta insediati, questi devono comunicare col proprio padrone e devono tentare di inviare copie di se stessi ad altri utenti. Un firewall si accorge di questi tentativi di comunicazione da parte di un programma non autorizzato e li blocca. In altre parole, il firewall impedisce che l'infezione che vi ha colpito si possa estendere ad altri utenti.

### **Ma perché serve un firewall oltre all'antivirus?**

Perché la sicurezza non si ottiene mai mediante una singola soluzione; si conquista combinando vari ingredienti. È un po' come mettere la cintura e anche le bretelle: un po' scomodo, ma riduce moltissimo le probabilità di trovarsi con le braghe calate nel momento meno opportuno.

A parte questo, il firewall agisce contro pericoli diversi da quelli sorvegliati da un antivirus. L'antivirus ci difende contro i *file* ostili recapitati al nostro computer; il firewall ci protegge dalle *intrusioni* perpetrate direttamente via Internet o tramite la rete locale.

Fra le due forme di attacco c'è una certa sovrapposizione, per cui può capitare per esempio che un firewall blocchi un virus che tenta di infettarci e che un antivirus fermi un intruso che cerca di farci visitare una pagina Web infetta, ma grosso modo la suddivisione dei compiti è questa: bloccare i file ostili spetta all'antivirus, fermare gli attacchi diretti è compito del firewall.

### **Come funziona un firewall**

---

Il firewall è un programma perennemente attivo, che osserva tutto il traffico di dati che entra ed esce tramite le connessioni di rete (connessioni alla rete locale e connessioni a Internet di qualunque tipo). Quando rileva traffico di tipo anomalo o sospetto, lo segnala all'utente oppure lo blocca direttamente.

La maggior parte dei firewall è in grado di capire quale programma sta generando il traffico anomalo e comportarsi di conseguenza. Per esempio, per inviare un e-mail è abbastanza ovvio che il vostro programma di posta deve poter trasmettere dei dati verso Internet; il firewall riconosce il programma che genera la trasmissione e gli consente di effettuarla. Il firewall controlla insomma quali programmi sono autorizzati a comunicare col mondo esterno.

Viceversa, il firewall è anche in grado di capire che tipo di traffico sta *ricevendo* dalla rete locale o da Internet e di riconoscere e bloccare il traffico ostile, lasciando passare quello sicuro. Per esempio, per scaricare la posta dovete ricevere dati da Internet: il firewall riconosce che si tratta di e-mail e lascia passare i dati. Se invece un vandalo cerca di entrare nel vostro computer, il firewall rileva il tentativo e lo blocca.

Un firewall permette anche di essere selettivi nell'accettare comunicazioni da altri computer. Normalmente un computer accetta messaggi da qualunque altro computer, ma questo significa che li accetta anche dagli utenti ostili. Il firewall consente di creare una "lista nera" di computer indesiderati, oppure di creare una "lista bianca" che specifica gli unici computer dai quali si accettano comunicazioni.

I firewall più astuti usano la *modalità di occultamento* (*stealth mode* in gergo). In sostanza, rendono invisibile su Internet il vostro computer, in modo tale che un aggressore non si accorga affatto della vostra esistenza e quindi non pensi neppure di prendervi di mira.

---

## Come agisce un aggressore

---

Per capire quanto sia importante e utile un firewall bisogna conoscere un pochino la psicologia degli aggressori informatici e il loro modo di operare.

Come già accennato, se non siete individui particolarmente in vista o non vi siete fatti troppi nemici, è difficile che un attacco vi prenda di mira personalmente. L'aggressore medio non fa altro che gironzolare per Internet alla ricerca di qualche preda, quasi sempre senza curarsi di chi sia la persona che aggredisce. Come un predatore nella savana, prende di mira preferibilmente i soggetti più deboli e vulnerabili, lasciando perdere quelli meglio difesi o così ben mimetizzati da sfuggire alla sua perlustrazione.

È un paragone molto poetico, perlomeno per un libro d'informatica, ma all'atto pratico come funziona la cosa? A ogni computer collegato a Internet viene assegnato un *indirizzo* permanente o temporaneo, chiamato *indirizzo IP* e solitamente espresso sotto forma di quattro numeri in serie, per esempio 212.162.1.47. È grosso modo l'equivalente del numero telefonico assegnato al vostro cellulare. Usando appositi programmi, l'aggressore "chiama" tutti gli indirizzi compresi in una certa gamma e vede chi risponde, esattamente come un molestatore telefonico può comporre una rosa di numeri a caso alla ricerca di una vittima dalla voce promettente.

Se l'aggressore trova un indirizzo che gli risponde, passa alla seconda fase dell'attacco: trovare un varco. Per snellire il traffico, un computer collegato a Internet suddivide la connessione in *porte*: la posta inviata passa da una determinata porta, quella ricevuta entra da un'altra, le pagine Web arrivano da un'altra ancora, e così via. Per ogni servizio di Internet c'è una porta corrispondente (o più d'una).

L'aggressore "bussa" a ciascuna di queste porte per vedere se per caso dall'altra parte c'è una risposta, e controlla se la porta è chiusa a chiave o aperta. La risposta può provenire da un virus precedentemente insediatosi oppure da un programma (per esempio uno di quelli usati per scambiare musica) o da un difetto del sistema operativo. Se quel programma o sistema operativo ha una falla, l'aggressore può usarla come appiglio per far danni: è il suo varco.

Lo scopo del firewall è prevenire tutto questo. Innanzi tutto, il firewall "chiude a chiave" tutte le porte lasciate incautamente aperte dai programmi e da Windows, e rifiuta di rispondere a chi "bussa" da fuori, in modo da non offrire appigli. Successivamente, il firewall previene l'aggressione nascondendo l'esistenza del vostro computer con un semplice espediente: quando un aggressore bussa al vostro indirizzo IP, il firewall non solo non gli risponde, ma gli fa credere che quell'indirizzo non sia assegnato. Per tornare al paragone telefonico, è come se il molestatore componesse il vostro numero telefonico e invece di sentire il tono di libero, sentisse la voce della Telecom che annuncia che il numero chiamato è inesistente. In entrambi i casi, il rompiscatole desisterà e andrà a cercare altrove.

È per questo che siamo tutti sotto attacco ripetutamente nell'arco della giornata e dobbiamo difenderci con un firewall. Là fuori ci sono migliaia di vandali sfigati che non hanno niente di meglio da fare che cercare computer vulnerabili e a bussare alle loro porte in cerca di qualche pertugio dal quale intrufolarsi per fare danni o spiare.

## Scegliere un firewall

---

Esistono due grandi famiglie di firewall: quelli *software*, ossia costituiti da programmi-sentinella da installare nel computer, e quelli *hardware*, vale a dire apparecchi separati dal computer che contengono un programma-sentinella.

I firewall hardware sono mediamente molto più efficaci di quelli software, perché sono

---

apparecchi autonomi e quindi immuni alle falle di Windows, ma sono anche assai più costosi. Se potete, investite in un firewall hardware, specialmente se dovete proteggere più di un computer. È quello che fanno tutte le aziende che hanno un minimo di riguardo per la sicurezza. Talvolta il firewall hardware è integrato nell'apparecchio che usate per collegarvi a Internet, specialmente nel caso di connessioni ADSL. Date un'occhiata al manuale del vostro modem ADSL: può darsi che contenga un firewall e non lo sappiate.

Se non potete permettervi la spesa di un firewall hardware, potete ricorrere a un firewall software. Ve ne sono molti gratuiti che funzionano benissimo; se volete maggiore versatilità e assistenza tecnica, potete rivolgervi ai firewall a pagamento. In questo capitolo vi presenterò soltanto i firewall software, perché sono la soluzione di gran lunga più diffusa.

## Firewall a scelta

Ecco una breve rassegna dei più gettonati firewall software.

Nome	Produttore	Prezzo	Lingua
BlackICE PC Protection	Internet Security Systems (blackice.iss.net/product_pc_protection.php)	A pagamento.	Inglese.
F-Secure Internet Security	F-Secure (www.f-secure.com)	A pagamento. Versione dimostrativa scaricabile.	Italiano.
McAfee Personal Firewall Plus	McAfee (it.mcafee.com)	A pagamento.	Italiano.
Norton Personal Firewall	Symantec (www.symantec.it/region/it/product/npf_index.html)	A pagamento.	Italiano.
Outpost Firewall Pro	Agnitum (www.agnitum.it)	A pagamento. Versione dimostrativa scaricabile.	Italiano.
Panda Platinum Internet Security	Panda Software (us.pandasoftware.com/com/it/)	A pagamento.	Italiano.
Sygate Personal Firewall	Sygate (smb.sygate.com/products/spf_standard.htm)	Gratuito per uso personale. La versione Pro è a pagamento.	Inglese.
Tiny Personal Firewall	Tiny (www.tinysoftware.com/home/tiny2?la=IT)	A pagamento.	Inglese.
Zone Alarm	Zone Labs (www.zonelabs.com)	Gratuito per uso personale. La versione Plus/Pro è a pagamento.	Inglese.

## Configurare un firewall

Molti pensano che configurare un firewall sia un'impresa complicatissima, e che i firewall siano grandi scocciatori che gridano continuamente *"al lupo, al lupo"* senza motivo, causando falsi allarmi e intralciando l'uso del computer.

Tutto dipende dal firewall che si sceglie e da come lo si configura. L'errore che si commette spesso è di lasciare attivate le notifiche dei tentativi di intrusione. A prima vista questo può sembrare il modo giusto di procedere, ma in realtà i tentativi sono talmente frequenti che ciò che conta non è esserne informati, ma esserne protetti. Il firewall va configurato in modo che agisca silenziosamente contro le minacce provenienti dall'esterno. Salvo casi rari, cercare di

scoprire chi sta dietro i tanti tentativi di penetrazione è solo una perdita di tempo.

La vera difficoltà sta nel saper rispondere agli allarmi generati dai programmi che tentano di uscire. Ma alla fine basta applicare un criterio di base abbastanza semplice:

**Se un programma chiede di andare su Internet o accedere alla rete locale, chiedetevi perché. Se non c'è un motivo più che valido, non importa che programma è, glielo si deve vietare. Nel dubbio, non autorizzate.**

In altre parole, se non siete veramente sicuri di cosa fa un certo programma che chiede l'autorizzazione, non autorizzatelo; autorizzatelo soltanto se l'uso di Internet è impossibile senza quest'autorizzazione. Tenete sempre presente che i vandali della Rete non aspettano altro che un vostro passo falso. Ricordate inoltre che **il firewall da solo non basta**: deve far parte di un **insieme** di contromisure difensive che vedremo nei capitoli successivi.

## Firewall in pratica: installare e configurare Zone Alarm

---

Sicuramente gli esperti storceranno il naso, additando firewall ben più potenti di quello che vi propongo, ma ho scelto Zone Alarm perché è un compromesso sensato di prezzo, difficoltà d'uso ed efficacia. Anche nella sua versione gratuita, è sempre meglio che esporre a Internet un computer indifeso. È come un casco per la moto: non vi salverà la vita se vi centra un carro armato, ma vi proteggerà dagli incidenti più comuni. Le protezioni più pesanti ci sono, ma sono anche più difficili da gestire. E se sono difficili, finisce che non vengono usate.

E' abbastanza spontaneo dubitare di qualsiasi cosa ci venga offerta gratuitamente. Dove sta la fregatura? Be', in questo caso la fregatura non c'è: Zone Labs, la società produttrice di Zone Alarm, ha realizzato due versioni del proprio firewall. Una è gratuita, l'altra no. Quella gratuita serve come oggetto promozionale per invogliarvi a comperare la versione a pagamento, più ricca di funzioni, denominata *Zone Alarm Pro*.

La versione gratuita è comunque sufficiente per l'uso normale, e potete usarla tranquillamente senza dover passare a quella commerciale se rispettate le condizioni di licenza (uso gratuito per utenti privati, non per lavoro) e se sopportate un pochino di promozione pubblicitaria della versione a pagamento. Anche i programmatori devono guadagnarsi la pagnotta in qualche modo.

## Scaricare Zone Alarm

---

Procurarsi la versione gratuita di Zone Alarm non è difficile; la si trova spesso distribuita nelle riviste d'informatica, o la si può scaricare direttamente dal sito di Zone Labs ([www.zonelabs.com](http://www.zonelabs.com)).

Con ovvie intenzioni promozionali, il sito non fornisce un accesso immediato e intuitivo alla versione gratuita, mentre quella a pagamento è propagandata con insistenza. Cercate un collegamento intitolato "*Zone Alarm (free)*" e seguitelo, cercando la parola magica *download* (scaricamento). A un certo punto vi verrà chiesto se volete salvare nel vostro computer un file che ha un nome del tipo *zlsSetup\_45\_594\_000.exe* o simile: fatelo.

## Installare Zone Alarm

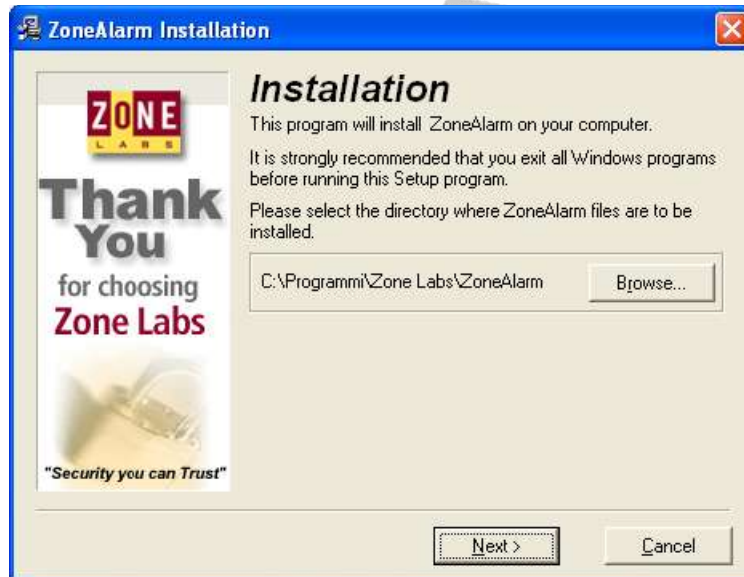
---

Per primissima cosa, scollegatevi da Internet. Avete già rischiato abbastanza sin qui,

---

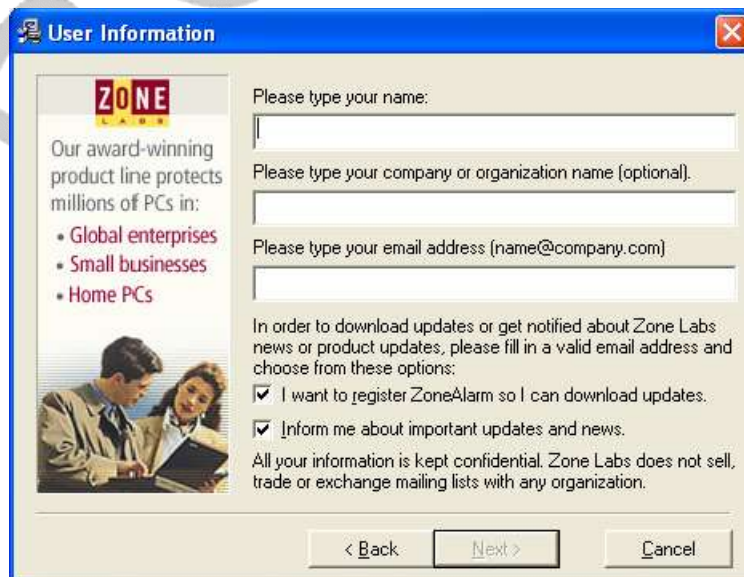
collegando Windows a Internet senza protezione: non è il caso di rischiare ulteriormente, specialmente nel momento in cui state installando un nuovo programma.

Lanciate il programma di installazione di Zone Alarm, ossia il file che avete appena scaricato o trovato nella rivista d'informatica.



**Figura 6-1. La scelta della cartella dove installare Zone Alarm.**

La prima finestra di dialogo (Fig. 6-1) vi chiede dove volete installare il firewall. Potete tranquillamente accettare la cartella proposta, oppure cambiarla cliccando su *Browse*. Al termine, cliccate su *Next*.



**Figura 6-2. Immettere i dati personali e attivare gli avvisi di aggiornamento in Zone Alarm.**

Nella finestra di dialogo successiva (Fig. 6-2), intitolata *User information*, immettete il vostro nome e (facoltativamente) quello della vostra ditta: tenete presente che Zone Alarm è gratuito soltanto per uso personale. Immettete anche il vostro indirizzo di e-mail, in modo che possiate ricevere le notifiche degli aggiornamenti (e, ahimè, un po' di pubblicità).

Lasciate attivate le caselle *I want to register Zone Alarm so I can download updates* e *Inform me about important updates and news*, che servono per consentire a Zone Alarm di ricevere un avviso automatico quando esce una nuova versione del firewall che magari tura qualche falla di quella corrente. Cliccate su *Next*.

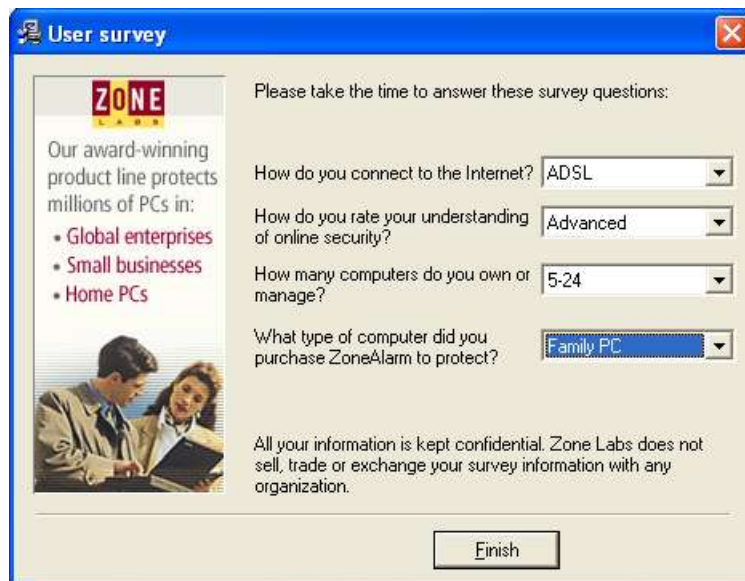
Nella schermata *License agreement* (Fig. 6-3) viene presentato l'accordo di licenza (in inglese). Leggetelo, se potete, e poi accettatelo attivando la casella *I accept the terms of the preceding License Agreement*. Avviate l'installazione cliccando su *Install*. Sembra non succedere nulla, ma attendete con fiducia.



**Figura 6-3. La schermata di licenza di Zone Alarm.**

Dopo una breve pausa, inizia la copia dei file. Poi parte un sondaggio (Fig. 6-4): rispondete scegliendo le risposte più pertinenti alle domande su come vi collegate a Internet, come pensate di cavarvela in fatto di sicurezza, quanti computer possedete o gestite e che tipo di computer proteggerete con Zone Alarm. Al termine, cliccate su *Finish*.

Compare la richiesta *Setup is complete. Do you want to start ZoneAlarm now?* In altre parole, l'installazione vera e propria del firewall è finita, e Zone Alarm vuole sapere se lo vogliamo attivare subito. Rispondete cliccando su *Yes*.



**User survey**

Please take the time to answer these survey questions:

Our award-winning product line protects millions of PCs in:

- Global enterprises
- Small businesses
- Home PCs

How do you connect to the Internet? ADSL

How do you rate your understanding of online security? Advanced

How many computers do you own or manage? 5-24

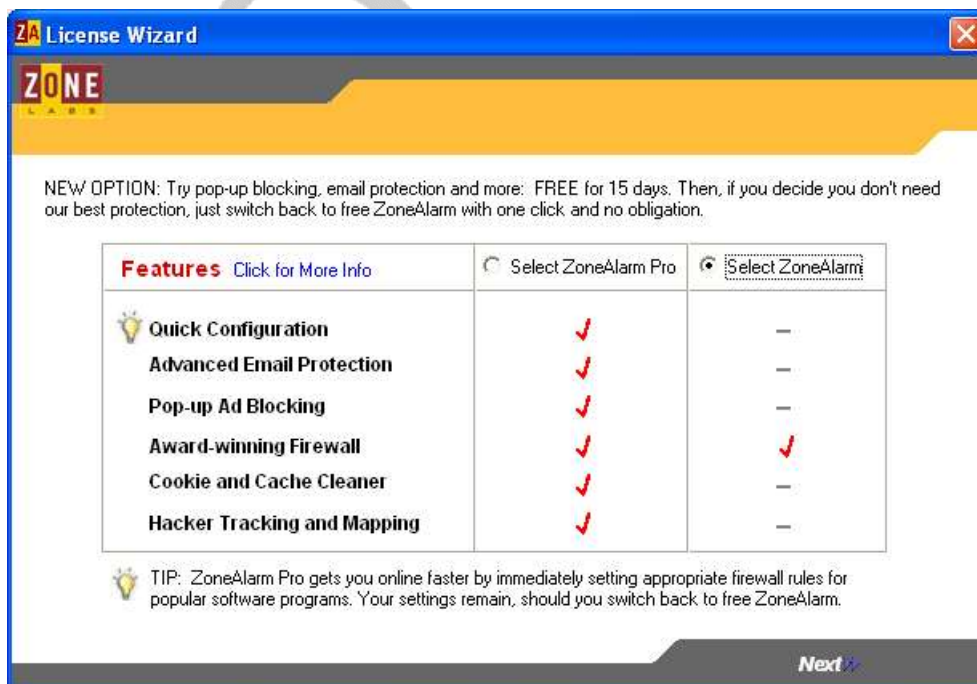
What type of computer did you purchase ZoneAlarm to protect? Family PC

All your information is kept confidential. Zone Labs does not sell, trade or exchange your survey information with any organization.

Finish

**Figura 6-4. Il sondaggio fra gli utenti.**

## Configurare Zone Alarm



**License Wizard**

NEW OPTION: Try pop-up blocking, email protection and more: FREE for 15 days. Then, if you decide you don't need our best protection, just switch back to free ZoneAlarm with one click and no obligation.

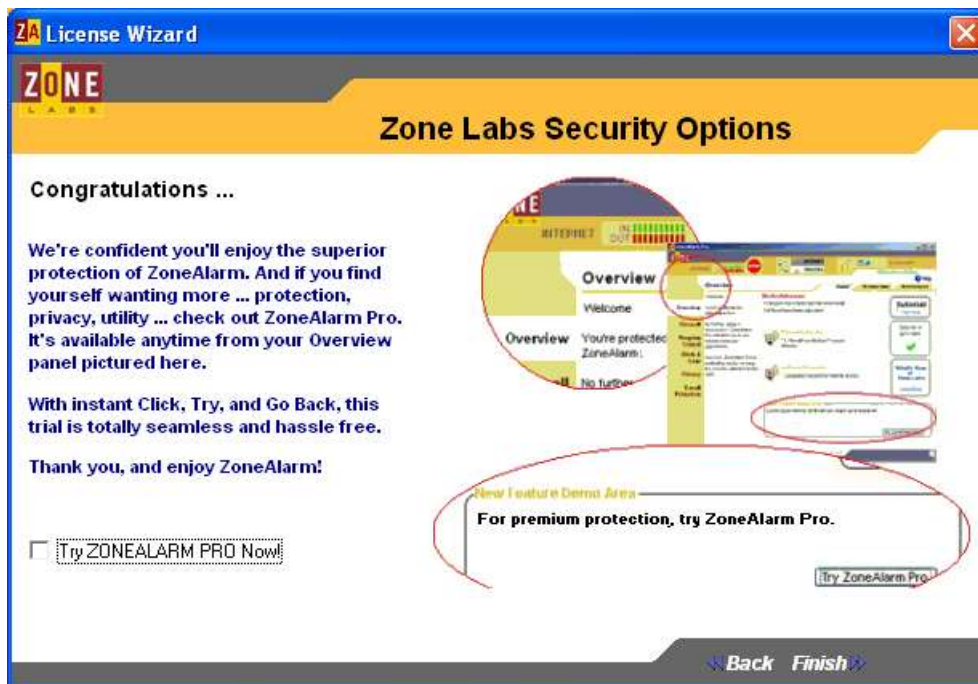
Features <a href="#">Click for More Info</a>	<input type="radio"/> Select ZoneAlarm Pro	<input checked="" type="radio"/> Select ZoneAlarm
Quick Configuration	✓	—
Advanced Email Protection	✓	—
Pop-up Ad Blocking	✓	—
Award-winning Firewall	✓	✓
Cookie and Cache Cleaner	✓	—
Hacker Tracking and Mapping	✓	—

TIP: ZoneAlarm Pro gets you online faster by immediately setting appropriate firewall rules for popular software programs. Your settings remain, should you switch back to free ZoneAlarm.

Next

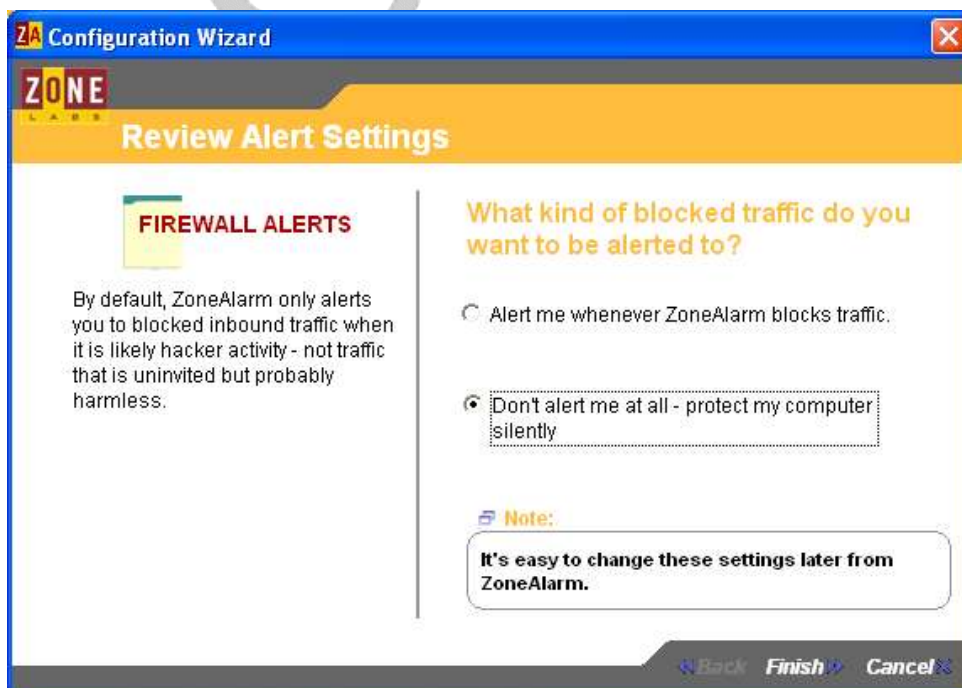
**Figura 6-5. Un po' di promozione per la versione a pagamento.**

A questo punto tocca sorbirsi un po' di pubblicità. La finestra di dialogo che compare (Fig. 6-5) è intitolata *License Wizard*; se non volete provare la versione Pro gratuitamente per quindici giorni e vi accontentate della versione gratuita, attivate *Select ZoneAlarm* e cliccate su *Next*.



**Figura 6-6. Ancora pubblicità per la versione a pagamento.**

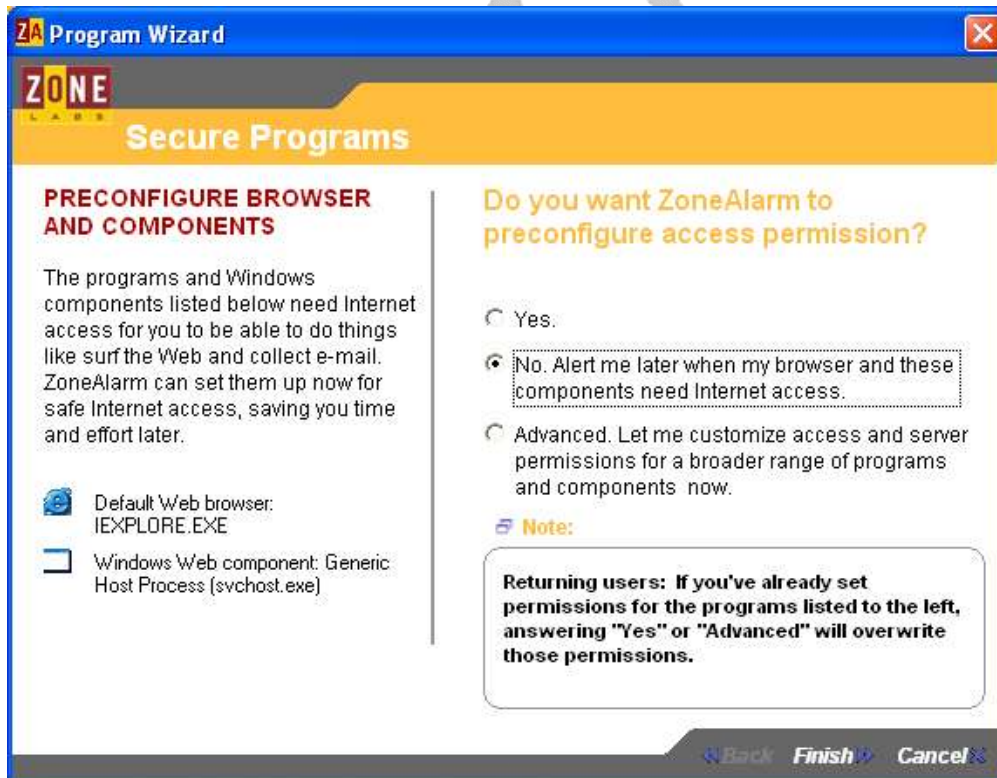
Coraggio, ancora uno spot promozionale e poi è finita (Fig. 6-6). Non attivate *Try ZoneAlarm Pro Now*, a meno che vogliate provare la versione Pro, e cliccate su *Finish*. Nella schermata successiva non vi resta che cliccare ancora su *Next* per proseguire.



**Figura 6-7. Scegliere se farsi avvisare o no a ogni sospetto di tentata intrusione.**

Nella schermata *Firewall Alerts* (Fig. 6-7) cominciate finalmente a impostare Zone Alarm. Più precisamente, scegliete se Zone Alarm deve avvisarvi o no ogni volta che rileva e blocca del traffico sospetto. Se volete farvi un'idea di quanto siano frequenti i tentativi d'intrusione, lasciate attivata l'opzione *Alert me whenever ZoneAlarm blocks traffic*; ma vi garantisco che vi stuferete molto presto di ricevere allarmi in continuazione.

E' sufficiente una protezione silenziosa, come quella offerta dall'altra opzione, ossia *Don't alert me at all - protect my computer silently*. Una volta fatta la vostra scelta (modificabile in seguito), cliccate su *Finish*.

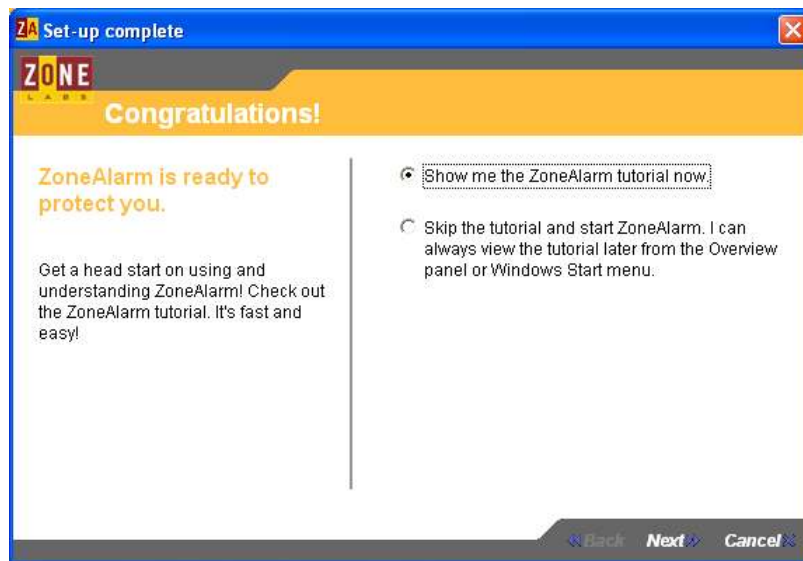


**Figura 6-8. Pre-autorizzare le applicazioni.**

La finestra di dialogo *Preconfigure browser and components* (Fig. 6-8) vi permette di scegliere subito alcuni programmi da autorizzare: tipicamente propone Internet Explorer e un componente di Windows chiamato *Generic Host Process*, identificato dal file *svchost.exe*. Dato che in realtà Internet Explorer è un rischio sicurezza, è decisamente più saggio non farlo uscire salvo rari casi di necessità (siti che funzionano soltanto con Internet Explorer, per esempio); *svchost.exe*, invece, va autorizzato ad uscire, perché altrimenti Windows non funziona correttamente con Internet.

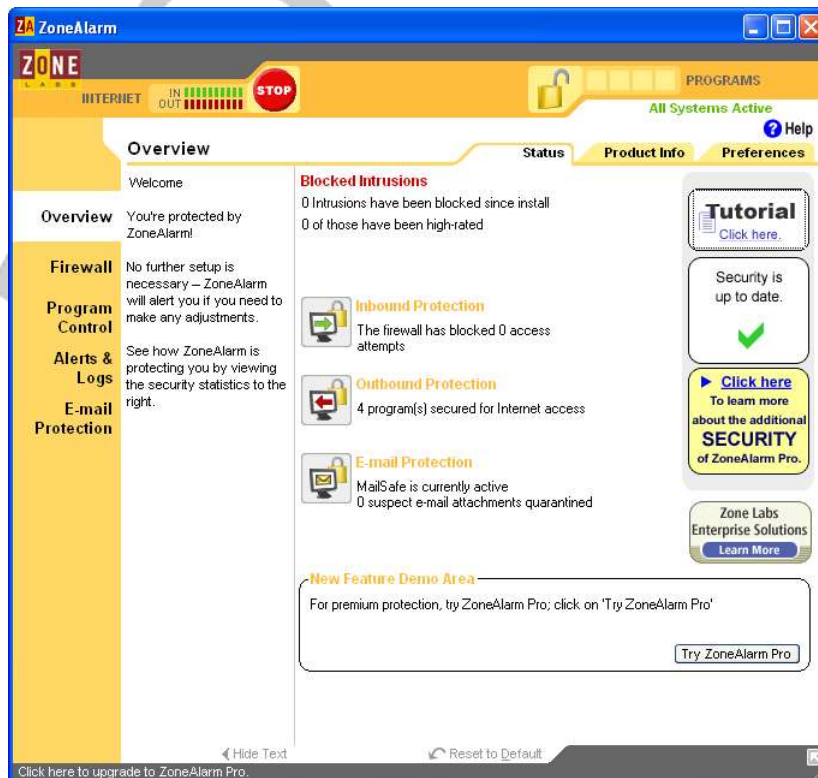
Se volete la massima sicurezza e personalizzazione del firewall, il mio consiglio è scegliere *No*. In questo modo, ogni programma che cercherà di uscire dovrà superare il nostro vaglio prima di essere autorizzato *una tantum* o permanentemente. Al termine, cliccate su *Finish*.

La schermata successiva, intitolata *Ebay fraud prevention*, riguarda, come avrete intuito, il celeberrimo sito di aste online Ebay. Zone Alarm può proteggere la vostra password di Ebay. Se non ne avete una, lasciate attivato *No thank you* ("no grazie") e cliccate su *Next*.



**Figura 6-9. Scegliere se vedere o meno un piccolo corso introduttivo (tutorial) a Zone Alarm.**

A questo punto (Fig. 6-9) potete scegliere se vedere un'animazione (*tutorial*) che spiega come funziona Zone Alarm. Se non vi interessa e vi fidate della mia descrizione sommaria, attivate *Skip*. Una volta fatta la vostra scelta, cliccate su *Finish*.



**Figura 6-10. La schermata iniziale di Zone Alarm.**

Ora finalmente siete a tu per tu con la schermata principale di Zone Alarm. Come noterete, è organizzata in modo diverso dalle tradizionali schermate dei programmi per Windows: non c'è una barra menu in alto. L'equivalente della barra menu è la banda gialla a sinistra, dove trovate le sezioni *Overview*, *Firewall*, *Program Control*, eccetera.

Ciascuna sezione è suddivisa in sottosezioni, identificate dalle linguette cliccabili in alto a destra. Per esempio, nella sezione *Overview* potete cliccare su *Preferences* per regolare le impostazioni preferite di Zone Alarm.

## Gioco a zone

Il nome *Zone Alarm* deriva dal fatto che il firewall divide l'universo in due *zone*. C'è la zona *Trusted*, dove risiedono i computer di cui Zone Alarm si fida, e la zona *Internet*, in cui viene relegato tutto il resto dell'infido mondo dei computer, Internet compresa.

Per esempio, se avete un altro computer nella vostra rete locale e volete permettergli di condividere i file e le stampanti del computer sul quale avete installato il firewall, dite a Zone Alarm di mettere l'altro computer nella zona *Trusted*. Se non volete dare quest'autorizzazione e anzi volete impedire agli altri utenti della rete locale di sbirciare nei vostri file, non dovete fare nulla: Zone Alarm parte dal saggio presupposto che se non gli dite specificamente "*fidati, questo è un amico*", non si fida di nessuno.

Se cliccate su *Firewall* e scegliete la scheda *Main*, troverete due cursori che consentono di regolare il livello di paranoia delle due zone: l'impostazione normale della zona *Internet* è *High* (alta), per rendere il vostro computer totalmente invisibile agli utenti ostili di Internet, mentre l'impostazione standard della zona *Trusted* è *Medium* (media), in modo che possiate condividere file e stampanti con altri computer della rete locale. Se non volete condividere a livello di rete locale, potete impostare a *High* anche questa zona.

L'altra sottosezione di *Firewall*, denominata *Zones*, è quella in cui si indicano a Zone Alarm i computer di cui si può fidare. Se non avete altri computer, non avete nulla da configurare in questa sottosezione. Se invece avete uno o più altri computer collegati in una rete locale e volete consentire loro di superare il firewall e condividere file e stampanti, procedete come segue:

- Scoprite l'indirizzo IP del computer che volete indicare come fidato: se avete una rete locale probabilmente già sapete come si fa, ma comunque ve lo ricordo lo stesso. Scegliete Start > Esegui. Se usate Windows XP, digitate **cmd** e cliccate su OK, poi digitate **ipconfig** e prendete nota dei dati visualizzati; infine digitate **exit** per terminare. Se usate Windows 98, digitate **winipcfg** e cliccate su OK.
- Nel computer sul quale avete installato Zone Alarm, aprite la finestra del firewall e scegliete la sezione *Firewall* e la sottosezione *Zones*.
- Cliccate su *Add* e scegliete *IP address*. Digitate l'indirizzo IP nella casella *IP address* e una descrizione a vostro piacimento in *Description*, poi cliccate su *OK* e *Apply*. Il computer che avete indicato verrà ora considerato come fidato.

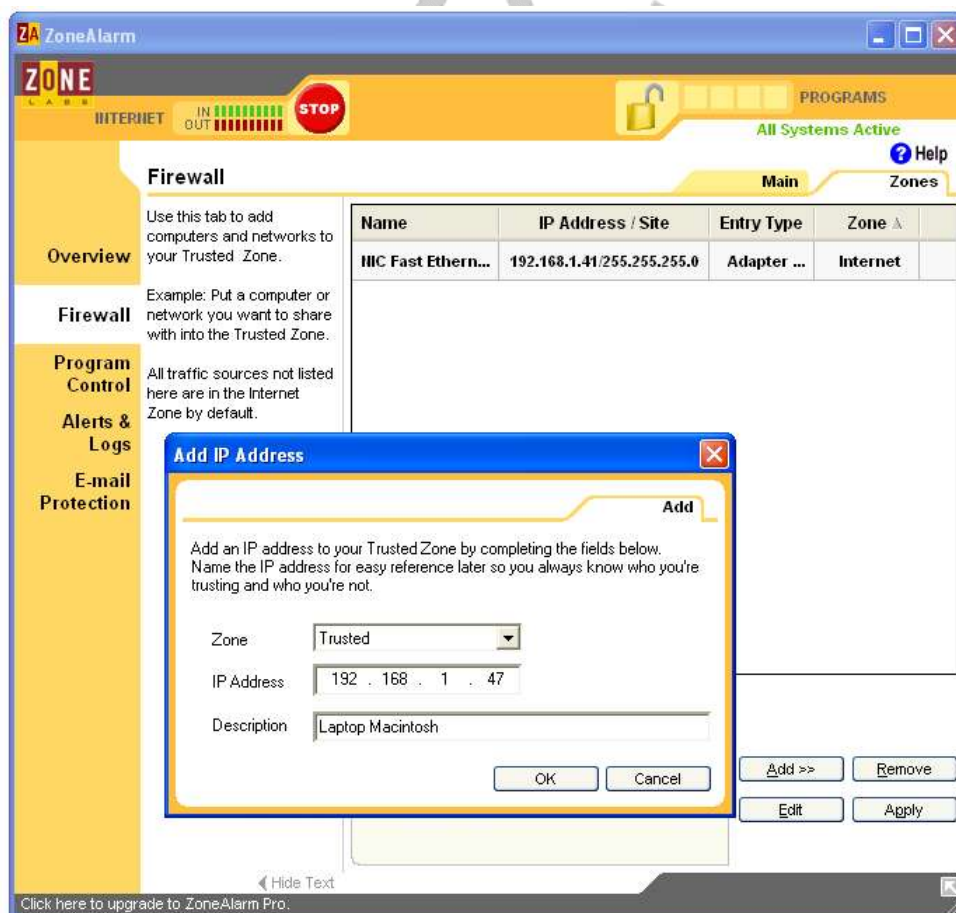
Se avete molti computer da rendere fidati, invece di specificare i loro indirizzi uno per uno potete specificare una gamma di indirizzi IP: quando cliccate su *Add*, scegliete *Range* e immettete l'indirizzo IP di partenza e quello finale della gamma che volete autorizzare.

---

**Pericolo!**

**Siate molto circospetti nel concedere fiducia.** Anche i computer della rete locale possono essere una fonte di infezione o di attacco, sia perché possono infettarsi e poi tentare di infettare voi, sia perché i loro utenti possono essere incompetenti o addirittura ostili. Capita più spesso di quanto possiate pensare che un collega faccia dispetti o venga a sbirciare o sabotare.

In particolare, tenete presente che **i dispositivi tramite i quali accedete a Internet non vanno considerati fidati.** Non è necessario mettere nella zona Trusted il modem, la scheda di rete, il router o l'access point (se non sapete cosa sono, fa niente); anzi, è altamente sconsigliabile.



**Figura 6-11. Aggiungere un indirizzo IP fidato.**

## Protezione dell'e-mail

Un'altra sezione da configurare subito è *E-mail protection*. Il suo scopo è filtrare gli allegati che vi arrivano nella posta e tentare di eliminare quelli potenzialmente pericolosi. Dico *tentare* perché nella versione gratuita di Zone Alarm questa funzione è molto limitata: in pratica blocca soltanto alcuni tipi di allegati pericolosi (gli script VBS, se volete i dettagli tecnici).

Tuttavia, dato che la sicurezza è una questione di difese multiple, tutto fa brodo, per cui ben venga anche questa piccola protezione in più. Il grosso delle difese contro gli allegati infetti, comunque, spetta all'antivirus. Morale della favola: attivate la voce *On* di questa sezione.

## Passi conclusivi

Bene! Le altre sezioni del programma possono attendere: è il momento di terminare la configurazione iniziale di Zone Alarm.

Riducete a icona Zone Alarm, poi cliccate col pulsante destro del mouse sul pulsante di Zone Alarm nella barra delle applicazioni e scegliete *Send to Tray*. Compare una finestra di dialogo di promemoria, nella quale potete tranquillamente attivare *Don't show this message again* e poi cliccare su OK. Tutto questo fa in modo che Zone Alarm sparisca dalla barra delle applicazioni e ricompaia come icona nell'area di notifica.

Chiudete XP e riavviate. Durante la chiusura, Zone Alarm può chiedere di salvare dei dati: in tal caso, accettate. Ora, finalmente, potete ricollegarvi a Internet in sicurezza: Zone Alarm si avvia automaticamente e vi protegge.

Adesso entra in gioco l'arma fina: il cervello.

## Autorizzazione dei singoli programmi

Provate a collegarvi a Internet e fare quello che fate normalmente al computer: inviare la posta, navigare nel Web, chattare con gli amici, eccetera. Noterete subito che la musica è cambiata e che il vostro nuovo buttafuori digitale è molto attivo e sospettoso.

La prima volta che lanciate per esempio Internet Explorer, infatti, Zone Alarm fa comparire un fumetto che avvisa di un tentativo di comunicazione non autorizzato (o per meglio dire non ancora autorizzato) e vi chiede se consentire la comunicazione o bloccarla.



**Figura 6-12. Zone Alarm blocca Internet Explorer.**

L'allerta arancione, con la dicitura *New Program*, indica che Zone Alarm ha rilevato che sta tentando di uscire un programma che a lui è sconosciuto (per forza di cose, visto che abbiamo appena installato il firewall). Notate che Zone Alarm, a differenza del firewall integrato (ma normalmente spento) in Windows, sorveglia anche i tentativi di uscita, anziché soltanto quelli di entrata.

Sappiamo che si tratta di Internet Explorer perché Zone Alarm ne indica il nome dopo *Do you want to allow* ("Vuoi autorizzare...") e specifica il nome del relativo file eseguibile accanto ad *Application* (in questo caso *iexplore.exe*). Ma il firewall ora vuole sapere cosa fare del programma che ha bloccato. A voi la scelta:

- **autorizzarlo, ma solo per questa volta:** cliccate su *Yes*. La prossima volta che Internet Explorer tenta di uscire, Zone Alarm lo bloccherà ancora, segnalerà con la dicitura *Repeat program* che si tratta di un nuovo tentativo da parte di un programma che ha già incontrato, e vi chiederà di nuovo che fare.
- **autorizzarlo permanentemente:** cliccate prima nella casella *Remember* eccetera e poi su *Yes*. Zone Alarm si ricorderà per sempre quest'impostazione (salvo vostro contrordine) e non vi disturberà più con questa domanda la prossima volta che quel programma tenta di uscire.
- **vietarlo, ma solo per questa volta:** cliccate su *No*. Alla prossima esecuzione di Internet Explorer, Zone Alarm lo bloccherà di nuovo dicendo che non è la prima volta che il programma tenta di uscire e chiedendovi ancora una volta cosa fare.
- **vietarlo permanentemente:** cliccate prima nella casella *Remember...* e poi su *No*. Il firewall si ricorderà della vostra scelta, e la prossima volta che Internet Explorer tenterà di uscire, lo bloccherà immediatamente senza assillarvi con fumettoni.

La scelta della risposta dipende ovviamente dalla natura del programma che sta tentando di uscire. Per esempio, se è il vostro programma di posta che sta tentando di collegarsi a Internet, vi conviene autorizzarlo in via definitiva: in sostanza, tutti i programmi che usate normalmente per Internet vanno autorizzati permanentemente, così Zone Alarm non vi assilla.

Se si tratta invece di un programma che non conoscete, è meglio che partiate dal presupposto che ciò che non conoscete è malvagio fino a prova contraria: cominciate a vietarne l'uscita temporaneamente, e nel frattempo indagate (per esempio immettendone il nome in Google) per scoprire di cosa si tratta.

Molto spesso si tratta di componenti legittimi di Windows, per esempio programmi come *svchost.exe*, *spoolsv.exe*, *jucheck.exe*, *explorer.exe*, *cmd.exe*, *rundll.exe* e altri: in tal caso, dopo aver appurato che si tratta effettivamente di programmi regolari, vi conviene autorizzarli (meglio se in modo non permanente, così ne tenete sotto controllo le attività).

---

**Consiglio**

Nella scelta di cosa autorizzare e cosa vietare, Internet Explorer (*iexplore.exe*) è un caso un po' particolare. L'abitudine e l'istinto probabilmente vi suggeriscono di dargli un'autorizzazione permanente, visto che lo usate spessissimo, ma permettetemi di sconsigliarvelo in favore di un'autorizzazione di volta in volta.

Internet Explorer è infatti uno dei principali veicoli di infezione degli aggressori. Visualizzare un sito ostile con Internet Explorer può essere sufficiente per contaminare e devastare il vostro computer. Per questo la navigazione con Internet Explorer va ridotta al minimo indispensabile, usando al suo posto un programma alternativo, come descritto nei capitoli successivi.

Ci sono però dei siti che per ragioni particolarmente stupide funzionano soltanto con Internet Explorer (alla faccia dell'universalità di Internet; è come aprire un negozio di scarpe che fa entrare soltanto clienti taglia 42). Siti che magari non potete ignorare, come quelli di banche o istituzioni governative. In tal caso, potete tirar fuori Internet Explorer e fargli fare un giretto, ma mi raccomando: usatelo soltanto su siti di reputazione più che cristallina. Troverete maggiori dettagli nei prossimi capitoli.

**Server traditore**

A volte il fumetto di Zone Alarm ha una banda blu e reca la dicitura *Server program*, come in Fig. 6-13. In tal caso, la prudenza deve essere massima. Un *server* è infatti (in questo contesto) un programma che accetta comandi dall'esterno. Internet Explorer o il vostro programma di posta, per esempio, non sono server, perché sono loro a prendere l'iniziativa di chiedere dati all'esterno o di spedirli (in gergo tecnico sono *client*).

Un programma server, invece, rimane in ascolto in attesa di un'iniziativa esterna. Molti componenti regolari di Windows si comportano in questo modo, ma lo fanno anche praticamente tutti i programmi ostili: restano in attesa di ordini dal loro oscuro padrone.



**Figura 6-13. Un programma chiede l'autorizzazione come server. Attenzione!**

In altre parole, avere un programma che è permanentemente in attesa di comandi dall'esterno è sempre e comunque una Pessima Idea, perché offre un appiglio agli aggressori. Nel caso mostrato nella Fig. 6-13, il programma server è un componente di Windows, per cui non ci sarebbe troppo da preoccuparsi, ma se domani si scopre una falla nella sicurezza di quel componente (e capita anche troppo spesso), vi trovate con un programma vulnerabile pronto a ricevere ordini dal vandalo di turno.

Ricordate pertanto di prestare moltissima attenzione a questi avvisi, perché possono fare un'enorme differenza in termini di sicurezza. Anche qui vale il principio generale già citato prima: **bloccare qualsiasi programma che richiede l'autorizzazione come server fino a che si dimostra che è innocuo e soprattutto necessario.**

Se un programma fa comparire l'allarme Server, provate a negargli temporaneamente il permesso di comunicare, anche se si tratta di un componente di Windows. Se il computer funziona lo stesso, rendete pure permanente il divieto: se non serve, perché correre rischi superflui? Se il computer non funziona, concedete l'autorizzazione, ma soltanto dopo aver esaminato bene il caso, magari chiedendo lumi ad amici esperti.

#### Regola

A volte uno stesso programma può far comparire sia l'allarme normale, sia quello Server. In questo caso, ciascuno degli allarmi va indagato separatamente, e l'autorizzazione come server va concessa soltanto con estrema riluttanza.

Tutto questo vi può sembrare complicato e paranoico, ma in realtà dopo qualche giorno di navigazione imparerete a riconoscere la manciata di programmi e componenti di Windows che hanno effettivamente bisogno di accedere a Internet e darete ordini permanenti a Zone Alarm.

A quel punto, Zone Alarm smetterà di interpellarvi e diventerà un guardiano silenzioso ma sempre pronto a scattare se gli si presenta di fronte una faccia nuova. Scoprirete, fra l'altro, che molti programmi tentano di andare su Internet senza alcun motivo apparente. Installare un firewall vi farà capire quante cose avvengono alle vostre spalle, e non sempre per ragioni positive.

#### Consiglio

Se cambiate versione di un programma oppure lo reinstallate o lo spostate a una cartella diversa, Zone Alarm è abbastanza furbo da accorgersene. Questo firewall, infatti, non si limita a guardare il nome del programma prima di concedere o meno l'autorizzazione a passare: se così fosse, a un intruso basterebbe ricorrere al vecchio trucco di attaccare il proprio virus a un programma molto diffuso e apparentemente innocuo (per esempio *iexplore.exe*), oppure dare al proprio software ostile il nome di quel programma.

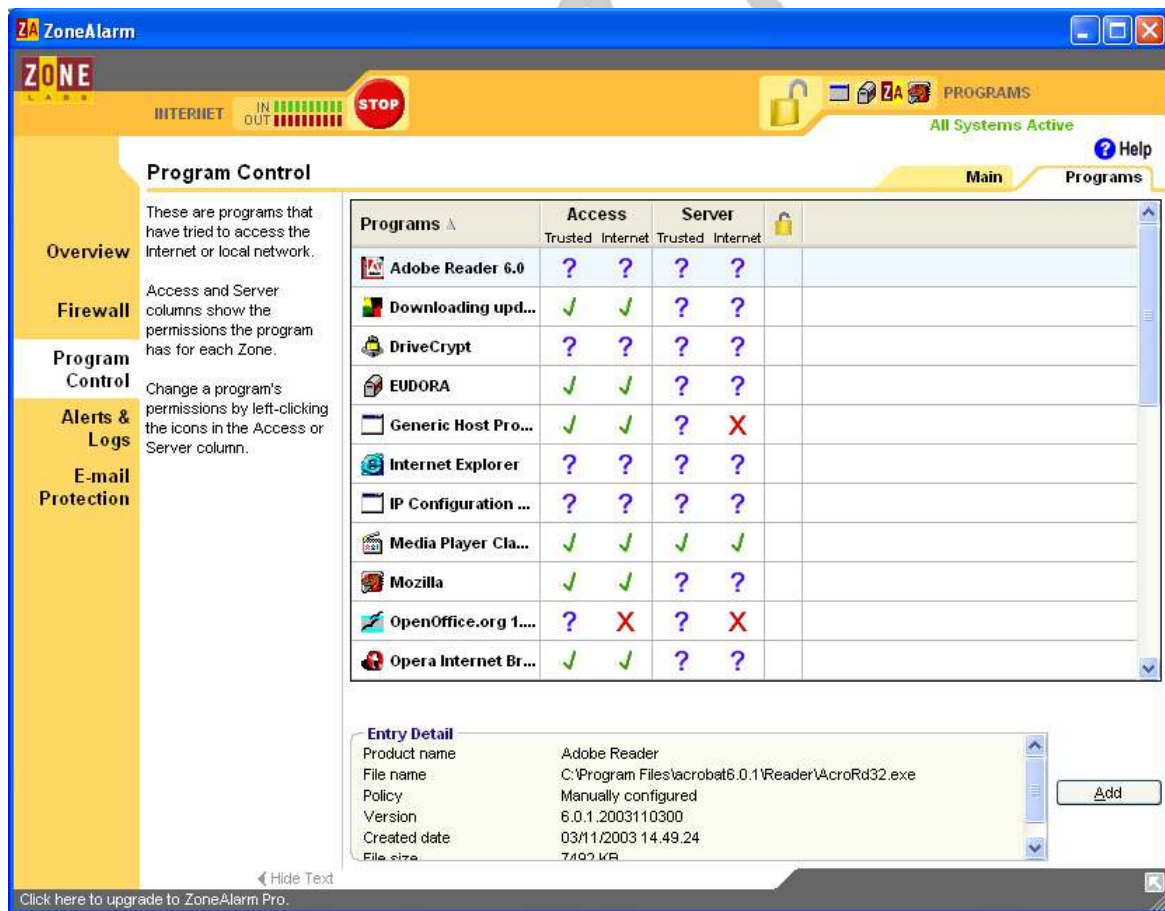
Zone Alarm genera una sorta di "impronta digitale" di ciascun programma autorizzato o meno. In questo modo, se anche un solo bit viene modificato, il firewall se ne accorge e segnala il possibile problema.

Questo però comporta che cambiando versione di un programma, Zone Alarm si inquieta, perché dal suo punto di vista un programma familiare ha cambiato impronte digitali: brutto segno. Sta a voi verificare se il suo sospetto è fondato o meno.

## Cambiare le autorizzazioni

Niente è per sempre, specialmente in informatica, per cui i programmi che autorizzate oggi potrebbero essere diversi da quelli di domani; potreste cambiare idea, o rendervi conto che un programma al quale avete vietato l'uscita ha in realtà ragioni legittime per uscire. In questo caso ricorrete alla sezione *Program Control* di Zone Alarm.

Assicuratevi che nella scheda *Main* di questa sezione il cursore sia impostato su *Medium* (*High*, ossia il controllo più rigoroso, è disponibile soltanto nella versione a pagamento). Poi date un'occhiata alla scheda *Programs*: è qui che Zone Alarm compila l'elenco dei programmi che gli si sono presentati e hanno tentato di passare il varco.



**Figura 6-14. Un elenco di programmi sorvegliati da Zone Alarm.**

La Fig. 6-14 mostra l'elenco di programmi di un computer piuttosto vissuto (uno dei miei). Ogni riga riporta il nome di un programma (non il nome del suo file eseguibile, ma il nome con il quale si presenta a Zone Alarm) e i permessi che gli sono stati accordati e negati:

- segno di spunta verde: permesso permanente
- punto interrogativo blu: il programma deve sempre chiedere il permesso
- X rossa: il programma ha ricevuto un divieto permanente.

Ogni programma ha quattro autorizzazioni distinte, a seconda del tipo di accesso richiesto e della zona a cui vorrebbe accedere. La colonna *Access* indica i permessi di semplice uscita, mentre la colonna *Server* elenca i permessi di agire appunto come server e quindi ricevere ordini dall'esterno. Le suddivisioni *Trusted* e *Internet* indicano a quale zona si riferiscono le autorizzazioni di semplice uscita e di azione come server.

Per esempio, nella Fig. 6-14, Internet Explorer ha quattro punti interrogativi: vuol dire che deve sempre chiedere il mio permesso prima di uscire, sia per fare un'uscita normale, sia per comportarsi da server, e lo deve chiedere sia per andare su Internet, sia per raggiungere la rete locale. Ebbene sì, non mi fido proprio.

Altro esempio: il *Generic Host Processor*, che è un componente di Windows, ha diversi gradi di libertà. Ha due segni di spunta nelle colonne *Access*, per cui è libero di contattare Internet e la rete locale senza impedimenti, ma la colonna *Server* rivela che ha il divieto assoluto di fare da server e rispondere a comandi provenienti da Internet, mentre può rispondere a comandi provenienti dalla rete locale.

## Aggiornamenti

Come gli antivirus, anche i firewall richiedono aggiornamenti periodici, anche se non così frequenti. Ogni tanto, infatti, viene scoperta qualche falla anche nei firewall,<sup>12</sup> che in fin dei conti sono comunque programmi e quindi per definizione imperfetti. Un difetto del firewall potrebbe consentire a un aggressore particolarmente deciso di scardinare questo elemento della vostra sicurezza informatica.

Per sapere quando occorre aggiornare il firewall è spesso disponibile un'opzione di notifica automatica. Per esempio, Zone Alarm contatta la propria casa produttrice ogni volta che vi collegate a Internet e lo avviate e chiede se ci sono aggiornamenti; se ce ne sono, compare sullo schermo l'invito a scaricarli.

A differenza degli antivirus, i firewall vengono in genere aggiornati in blocco: in altre parole, invece di scaricare un file di aggiornamento, si scarica un'intera versione nuova del programma.

Dopo aver scaricato la nuova versione del firewall, la prima cosa da fare è **scollegarsi da Internet e dalla rete locale**. Durante l'aggiornamento, infatti, il computer si troverà momentaneamente privo della protezione offerta dal firewall, e siccome la sfiga ci vede benissimo, è facile che qualche virus dei tanti in giro per la Rete (e magari anche nella rete locale) approfitti di questa temporanea vulnerabilità per tentare un attacco.

### Aggiornare Zone Alarm

L'aggiornamento di Zone Alarm è un procedimento piuttosto semplice. Dopo aver scaricato la nuova versione del programma ed esservi staccati da Internet e dalla rete locale, lanciate il programma, che trova automaticamente la cartella dell'installazione precedente. Cliccate su *Next*.

Nella schermata delle informazioni utente compaiono automaticamente le informazioni che avevate immesso nella versione precedente. Modificatele, se necessario, poi cliccate su *Next*.

Alla domanda *Upgrade or clean install*, che vi chiede di scegliere fra aggiornamento e reinstallazione da zero, rispondete con *Upgrade*. Cliccate su *Next*.

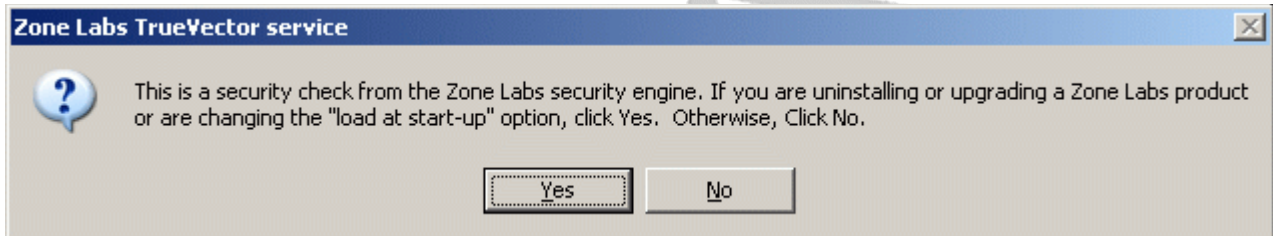
---

12 È successo con BlackIce e RealSecure ([www.theregister.co.uk/content/56/36413.html](http://www.theregister.co.uk/content/56/36413.html)) e il worm Witty.

---

Nella schermata *License agreement*, che presenta la licenza d'uso, cliccate su *I accept* per accettarla. Infine cliccate su *Install*.

Zone Alarm si chiude e mostra l'annuncio perentorio di Fig. 6-15. In sintesi, Zone Alarm si chiede perché lo state chiudendo e si augura che abbiate una buona ragione per farlo. Dato che l'avete, cliccate su *Yes*.



**Figura 6-15. Zone Alarm chiede conferma prima di disattivarsi.**

Inizia la reinstallazione, che è molto simile all'installazione che avete fatto la prima volta che avete adottato Zone Alarm. I dati del sondaggio sugli utenti (*User Survey*) sono precompilati attingendoli da quelli che avete dato a suo tempo: accettateli e cliccate su *Finish*.

Zone Alarm chiede di riavviare Windows: accettate cliccando su *OK*. Dopo il riavvio, fa un po' di pubblicità per la versione a pagamento; se non vi interessa, attivate *Select Zone Alarm* e cliccate su *Next*. Dopo un'ulteriore schermata pubblicitaria potete cliccare su *Finish* per completare l'aggiornamento.

Fatto questo, non vi resta che ridurre a icona Zone Alarm e cliccare col pulsante destro nella barra delle applicazioni, sul pulsante di Zone Alarm, e scegliere *Send to tray*. Nell'area di notifica compare l'icona di Zone Alarm aggiornato. Missione compiuta: tutte le impostazioni della versione precedente vengono acquisite automaticamente nella nuova versione.

## Zone Alarm non finisce qui

Chiaramente Zone Alarm ha molte altre opzioni e funzioni che permettono di affinarne ulteriormente il funzionamento. Tuttavia non voglio tediarvi con dettagli che normalmente non sono indispensabili per il buon uso del firewall. Se volete saperne di più, usate un motore di ricerca (Google, per esempio) per sfogliare le tante guide all'uso approfondito di Zone Alarm che trovate su Internet anche in italiano.

## Come collaudare un firewall

### DA FINIRE

**Per verificare l'integrità del vostro firewall**, potete ricorrere ai test non distruttivi offerti da siti come Grc.com (in particolare le pagine *ShieldsUp!* e *LeakTest*) oppure HackerCheck ([www.hackercheck.com/?mode=c](http://www.hackercheck.com/?mode=c)) di Trend Micro, o anche ai miei piccoli test nel Browser Challenge.

<http://security.symantec.com/default.asp?productid=symhome&langid=it&venid=sym> (test in italiano)

Descrivere in dettaglio. Spiegare Stealth mode (già accennato in introduzione capitolo).

## Cosa cambia col Service Pack 2

---

Una delle novità di maggiore spicco del Service Pack 2 è la presenza di una versione potenziata del firewall già presente in XP, ribattezzato *Windows Firewall* e soprattutto attivato automaticamente, a differenza dell'originale.

Se adottate Zone Alarm, noterete molte somiglianze nel firewall Microsoft: per esempio, è possibile scegliere quali programmi sono autorizzati a comunicare con l'esterno. A differenza di Zone Alarm, invece, Windows Firewall è interamente gestibile dal prompt dei comandi.

Come molti suoi concorrenti, Windows Firewall consente di consentire soltanto il traffico dei dati generati localmente, per esempio da altri computer della rete locale, come nel caso classico della condivisione di file e stampanti.

Per le situazioni di panico generale, per esempio in occasione di un attacco virale massiccio o di una vulnerabilità scoperta in un'applicazione o in un componente di Windows, il firewall del Service Pack 2 include anche una modalità "chiudere i boccaporti" facilmente attivabile, chiamata *On with no exceptions*<sup>13</sup>, nella quale ogni connessione iniziata dall'esterno verrà rifiutata e saranno ammesse soltanto quelle in partenza dalla macchina locale.

Tutto questo non significa che si possono buttar via Zone Alarm e gli altri firewall prodotti da terzi. A parte il fatto che Windows Firewall è concepito per convivere con questi altri firewall piuttosto che sostituirli, il prodotto Microsoft ha al momento, anche nella sua incarnazione nel Service Pack 2, una limitazione non presente nei concorrenti: consente automaticamente tutte le connessioni *in uscita*, a prescindere dal programma che le genera.<sup>xvii</sup> Questo significa che se un utente viene infettato, i tentativi del software ostile di raggiungere il proprio padrone o di disseminarsi non verranno fermati come avviene invece con i firewall alternativi.

---

13 Al momento della pubblicazione di questo testo non è ancora nota la traduzione italiana.

---