Outpost Firewall La configurazione in dettaglio

Il problema
Personalizzare Agnitum Outpost Firewall per proteggersi da attacchi esterni

La soluzione
Creare le regole ideali per configurare il prodotto in base alle proprie esigenze

Nel CD Guida di questo numero (*categoria firewall*) trovate Outpost Firewall

Agnitum Outpost Firewall è un firewall personale che ha conquistato subito il nostro favore.

Nella prova comparativa tra i migliori firewall attualmente disponibili sul mercato (pubblicata nello scorso numero di *PC Open*), Outpost ha particolarmente brillato mettendo in evidenza caratteristiche spesso superiori ai più famosi software commerciali, una semplicità d'utilizzo disarmante, un'efficacia senza uguali.

Dopo aver presentato, nello scorso numero, le principali funzionalità del prodotto, questa volta ci proponiamo di illustrare una serie di semplici indicazioni per configurare il firewall senza fatica e per risolvere i problemi che potrebbero presentarsi durante il suo utilizzo.

Outpost è un software firewall in grado di fare da filtro tra il proprio computer e la rete Internet. Il programma permette, quindi, di ripararsi da tutti i possibili attacchi provenienti dall'esterno e, contemporaneamente, di intercettare tutte le richieste di invio e/o ricezione dati da parte delle applicazioni installate sul PC.

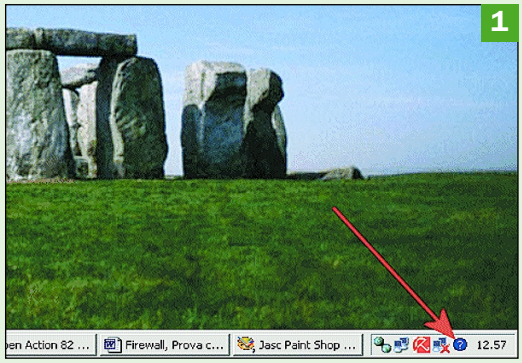
Non appena un programma installato tenta di comunicare con Internet, Outpost visualizza la finestra *Create rule* che consente di impostare una regola personalizzata per l'accesso alla Rete da parte di quella specifica applicazione. Creando una regola personalizzata, Outpost concederà o negherà in futuro, in modo automatico, l'accesso a Internet.

Uno degli errori più frequenti che si commettono durante la configurazione di un firewall consiste nel permettere l'accesso alla Rete ad applicazioni che non si conoscono. In questo modo si può aprire la porta ad attacchi dall'esterno o acconsentire, senza saperlo, alla trasmissione di informazioni personali. Se Outpost segnala il tentativo di connessione ad Internet da parte di un programma che considerate "fidato", le alternative che si prospettano sono essenzialmente due: qualora Outpost riconosca il programma, il consiglio è quello di utilizzare l'opzione *Create rules using preset* ("Crea una regola utilizzando le informazioni disponibili"), altrimenti è meglio provvedere manualmente alla creazione di una regola personalizzata (scegliere *Create rules using preset* e poi *Other* dal menu a tendina).

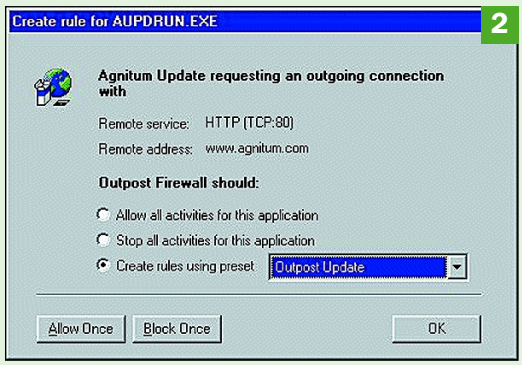
Ove possibile, il nostro consiglio è quello di impostare numerose regole "strette" piuttosto che poche regole

La creazione delle regole

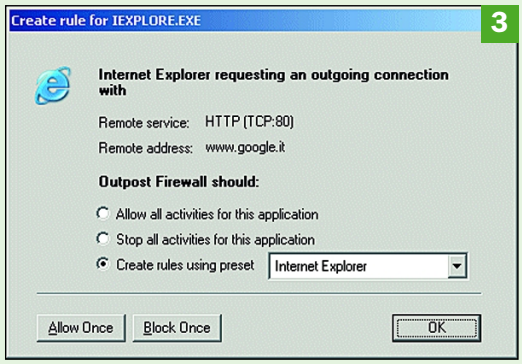
La modalità *Ask mode*
Dopo l'installazione, Outpost si presenta nell'area accanto all'orologio di Windows (*traybar*) con un'icona blu raffigurante un punto interrogativo. Ciò significa che il programma è in *Ask mode*: il firewall visualizza una finestra d'avviso a ogni richiesta di connessione ad Internet da parte di un programma.



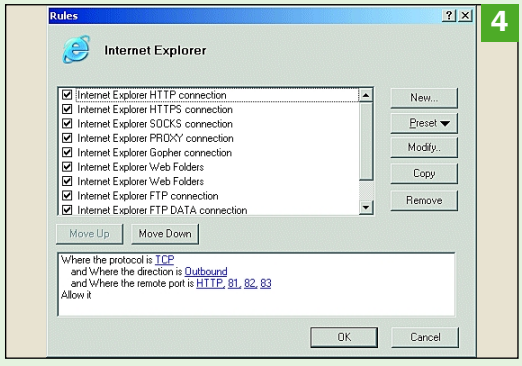
Comunicare con Internet
La finestra *Create rule* che appare a video consente di impostare una regola per la comunicazione con Internet da parte di un'applicazione. La stessa finestra mostra l'icona e il nome del programma che richiede l'accesso alla Rete, il protocollo utilizzato (HTTP, FTP e così via), la porta e l'indirizzo remoto al quale l'applicazione si desidera collegare.



Il modulo di aggiornamento
Una delle prime finestre *Create rule* che compariranno riguarda il programma AUPDRUN.EXE: si tratta del modulo di aggiornamento in automatico del firewall. È sufficiente selezione l'opzione *Create rules using preset Outpost Update*.



La creazione delle regole
Outpost rileverà immediatamente il tentativo di accesso a Internet da parte del browser e vi richiederà che cosa fare. Anche in questo caso è possibile utilizzare una regola reimpostata (*Create rules using preset*): Outpost è infatti in grado di riconoscere tutti i principali browser e di consentire tutte le comunicazioni sicure.



"larghe". In sostanza, sconsigliamo di impostare regole che permettano alle varie applicazioni installate di usare liberamente un gran numero di protocolli, di connettersi a qualsiasi indirizzo remoto, di utilizzare qualsiasi porta.

Tenete presente che Outpost potrebbe segnalarvi spesso tentativi di accesso ad Internet da parte del file SVCHOST.EXE: si tratta di un componente di sistema usato in ambiente Windows 2000/XP. Noi consigliamo di attivare solo il traffico UDP, disabilitando il resto.

Outpost visualizza le connessioni in corso nella finestra *All connections* (*tutte le connessioni*). Per ciascunaconnessione vengono visualizzate informazioni complete sul quantitativo di dati inviati e ricevuti, sul numero di porta aperta, sul protocollo usato, sul software che ha richiesto la connessione, sull'host remoto, sulla durata della comunicazione: si tratta di dati molto utili che altri firewall (compresi quelli professionali) spesso non forniscono.

Cliccando sulle voci *Allowed* e *Blocked*, Outpost mostra, rispettivamente, tutti i tentativi di connessione che sono stati consentiti e quelli negati.

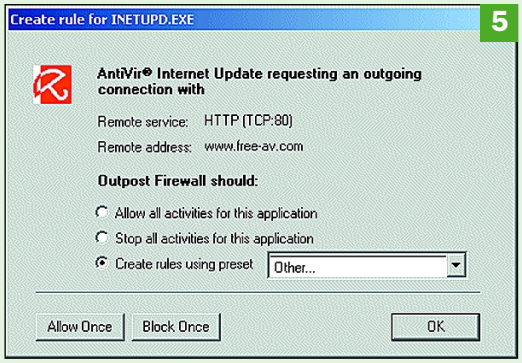
Per quanto riguarda gli attacchi provenienti dall'esterno, cliccando sulla voce *Attack detection*, Outpost visualizza l'elenco di tutti i tentativi di connessione al proprio PC, di eventuali attacchi veri e propri, di tutti i *port scanning* (gli hacker utilizzano spesso sistemi di scansione delle porte per scovare eventuali vulnerabilità).

Il programma è poi in grado di proteggere l'utente anche dai contenuti (potenzialmente pericolosi) che caratterizzano le pagine Web. In questo senso, Outpost consente di impostare delle politiche personalizzate per la gestione di cookie, ActiveX e applet Java. Dalla finestra principale di Outpost, cliccate con il tasto destro del mouse sulla voce *Active Content* s poi su *Properties*. Cliccando su *Mail*, *News* e su *Web Pages*, avrete la possibilità di impostare delle regole generali per la visualizzazione dei siti Web. L'utente può, ad esempio, disattivare l'esecuzione automatica di applet Java o di contenuti ActiveX, la ricezione di cookie, la visualizzazione di finestre a comparsa (pop-up), la comunicazione degli URL visitati in precedenza con il browser (*Referers*). Selezionando *Web Pages* quindi premendo il pulsante *Add*, Outpost offre la possibilità di aggiungere una lista di siti Web, ciascuno caratterizzato da specifiche regole: si può ad esempio consentire l'esecuzione di applet Java, ActiveX e ricezione dei cookie durante la navigazione siti "fidati", negarla su siti particolarmente "invasivi". Outpost Firewall consente, inoltre, di bloccare in modo automatico la visualizzazione di banner pubblicitari, di inibire l'accesso ai siti che contengano materiale "offensivo" (la cernita viene effettuata in base alle parole-chiave inserite manualmente da parte dell'utente), di impedire l'esecuzione degli allegati di posta elettronica potenzialmente pericolosi (Visual Basic Script, file batch, file eseguibili).

Dopo aver installato e configurato il vostro firewall, provate a servirvi del test di sicurezza effettuabile all'indirizzo www.pcflank.com: dal menu di sinistra (*Test your system*) potrete eseguire tutte le prove.

Qualora abbiate domande su Outpost, vi suggeriamo di fare riferimento alla pagina seguente: http://www.il-software.it/forum/topic.asp?TOPIC_ID=5267 (è necessaria una registrazione gratuita per poter inviare i propri messaggi). Outpost Firewall è distribuito in Italia da Future Time (www.nod32.it): nel momento in cui state leggendo queste pagine, l'azienda dovrebbe aver già rilasciato la localizzazione italiana. ■

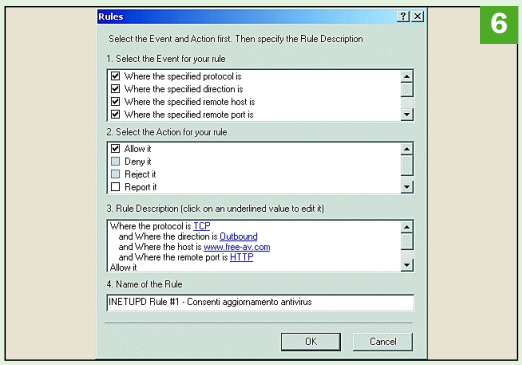
M.N.



5

▶ Il client di e-mail

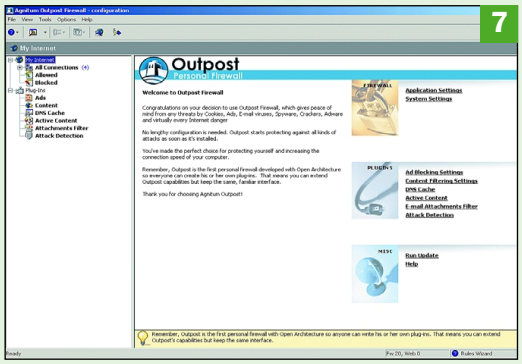
Non si dovrebbero riscontrare problemi configurando, nello stesso modo, il client di posta elettronica. Quando Outpost riconosce un programma permette di creare una regola personalizzata per l'accesso usando le informazioni di cui dispone (*Create rules using preset*).



6

▶ Le applicazioni "fidate"

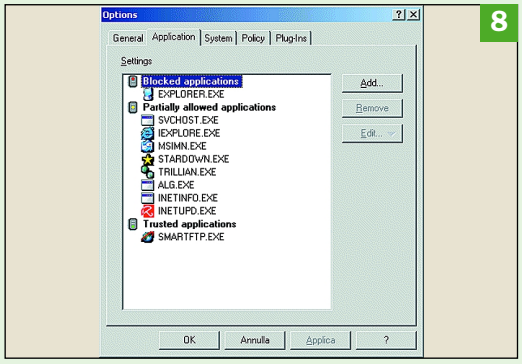
Nel caso di Antivir Internet Update (il programma per l'aggiornamento del software antivirus Antivir PE) possiamo selezionare *Allow all activities for this application* ("Consenti tutte le attività") dato che si tratta di un programma "fidato".



7

▶ I parametri

Nella finestra per la creazione di una regola vengono indicati il protocollo, la direzione della comunicazione (*inbound* significa *in entrata*; *outbound* sta per *in uscita*), l'indirizzo remoto e la porta. Il pulsante *Allow it* consente d'ora in poi alla comunicazione; *Deny it* la nega.



8

▶ Le applicazioni "blocked"

Cliccando sul menu *Options*, *Application*, è possibile visualizzare l'elenco delle applicazioni alle quali è vietato l'accesso a Internet (*Blocked*), quelle a cui è permesso un accesso parziale (*Partially allowed*) e quelle fidate (*Trusted*). Per cambiare una regola, selezionare l'applicazione e premere *Edit*.