Outpost Firewall Pro GUIDA

installazione
impostazione
utilizzo

Riferimento versione del software: **Pro 2.5** **data**: **Apr 2005**

Gli autori

MaxZ (**Massimo Z.**)
Rici (**Riccardo F.**)

In collaborazione con

IlSoftware.it
www.ilsoftware.it
Michele Nasi

DISCLAIMER
– Leggere con attenzione prima di consultare la guida –

SOMMARIO S

INTRODUZIONE 1.0

Cos'è un firewall e perché utilizzarlo 1.1

Un firewall è un dispositivo software o hardware preposto al controllo ed al filtraggio del traffico di rete proveniente dall'esterno (rete locale o Internet) nonché di quello eventualmente generato dall'interno.

Spieghiamo questa definizione con parole più semplici. Ogni computer collegato ad Internet è e rimane un 'nodo' della rete mondiale per tutta la durata della connessione. Esso è in grado di comunicare con gli altri computer sfruttando un **protocollo** di comunicazione ed utilizzando dei **pacchetti** (o *datagrammi*) transitanti attraverso determinate **porte** (semplici numeri usati per identificare il tipo di comunicazione). In questa immensa rete di sistemi il firewall può essere paragonato ad una **dogana**: il suo compito è quello di analizzare i pacchetti in entrata o in uscita su una porta, permettendone o bloccandone il transito dopo averli confrontati con un insieme di regole predefinite e/o definite dall'utente. E' quindi facilmente comprensibile come un firewall impedisca l'intrusione nel nostro pc da parte di utenti non autorizzati e ci tenga costantemente informati sui tentativi di accesso ad Internet da parte delle applicazioni installate nel nostro computer.

L'utilità di un firewall non sta però solo in questa funzione: generalmente permette anche di conservare la propria privacy bloccando i cookies ed i referers dai siti Internet e di velocizzare l'apertura e la visualizzazione delle pagine web impedendo il caricamento di animazioni, pop-up e banner pubblicitari indesiderati (che è un grosso vantaggio per chi ha una connessione lenta!).

Dopo questa breve descrizione, è di fondamentale importanza fare una piccola precisazione. I firewall **non sono autonomi**: per funzionare nel pieno delle loro potenzialità (e quindi per fornire la massima protezione) **devono essere settati ed istruiti correttamente** da parte di chi li utilizza.
E' bene evitare di servirsi di questi software se non si è in grado di configurarli in maniera ottimale: in questi casi infatti la loro efficacia risulterebbe nulla o quasi, generando nell'utente un falso senso di sicurezza.

Peculiarità di Outpost Firewall Pro 2.5 1.2

Come ogni software che si rispetti, anche Outpost Firewall si differenzia dai suoi 'colleghi' per aspetti positivi e negativi. Se da una parte sono sempre state note la sue scarse intuibilità e semplicità d'uso, dall'altra è senza dubbio un firewall superiore agli altri per almeno tre aspetti.

- **Plug-In**. Outpost è attualmente l'unico firewall studiato e realizzato con una mentalità 'aperta': è costituito infatti da un programma centrale che avvia a sua volta altre piccole utilità indipendenti (plug-in appunto), ciascuna delle quali ha un compito ben preciso. Questa interessante caratteristica permette di ampliare in maniera semplice le funzionalità di Outpost: infatti, oltre alle plug-in già incluse nel pacchetto di installazione (intercettazione degli attacchi, salvaguardia della privacy, blocco di siti con contenuti specifici, ecc...), ne esistono diverse altre realizzate da sviluppatori di terze parti: è possibile consultare la lista completa delle plug-in esistenti su http://www.agnitum.com/products/outpost/plugins.html.
- **Creazione manuale delle regole**. Questo procedimento è molto interessante e senza dubbio consente di costruire delle regole molto precise. Dopo aver scelto l'applicazione da monitorare, possiamo selezionare ed impostare uno ad uno il protocollo (TCP/IP o UDP), la direzione (in entrata o in uscita) la porta (sia locale che remota) ed eventualmente anche un indirizzo Internet o IP specifico; alla fine basterà soltanto scegliere se permettere o bloccare questo tipo di comunicazione per l'applicazione. Attraverso una casella di testo specifica, Outpost provvederà a visualizzare la descrizione della regola, consentendone la sua modifica in qualunque momento.
- **Salvataggio di più configurazioni**. Dopo aver impostato e salvato durante il setup la prima configurazione (vedremo poi come), è sempre possibile 'costruirne' altre, salvandole poi in file differenti: in questo modo è possibile caricare in ogni momento la configurazione più congeniale.

Dove scaricare Outpost Firewall 1.3

Outpost Firewall è di proprietà della Agnitum, azienda esperta nella sicurezza informatica. Attualmente ne esistono due versioni: una **free** (obsoleta e non più aggiornata) e una **Pro** (concessa in prova per un periodo della durata di 30 giorni).

- Home Page Outpost Firewall http://www.agnitum.com
- Download Outpost Firewall Free http://www.agnitum.com/download/outpost1.html
- Download Outpost Firewall Pro http://www.agnitum.com/download/outpostpro.html

Al momento della stesura della presente guida, le ultime versioni disponibili per il download sono la **1.0** per Outpost Firewall Free e la **2.5.375.374** per quanto riguarda Outpost Firewall Pro.

Installazione di Outpost Firewall Pro 2.5 1.4

Dopo aver lanciato il setup scaricato dal sito della Agnitum, l'installazione procederà come segue:

1. scelta della **lingua**;
2. lettura del **contratto di licenza** e relativa **accettazione**;
3. scelta della **cartella di destinazione** nel disco rigido;
4. scelta del **tipo di configurazione**. Prima di installare Outpost Firewall nel disco fisso, il setup raccoglie informazioni sul sistema e precisamente sull'eventuale presenza di una rete LAN (rilevando gli indirizzi IP dei computer che la compongono) e sulle applicazioni installate (con relativi componenti) che potrebbero richiedere accesso ad Internet. Scegliendo **Configurazione Automatica** questo processo verrà effettuato in maniera autonoma, impostando il firewall di conseguenza; **Assistente Configurazione** vi permetterà invece di inserire manualmente gli indirizzi IP dei computer di un'eventuale rete LAN, di scegliere per quali applicazioni il firewall dovrà creare una regola di accesso (attraverso il pulsante Dettagli) e di abilitare o meno il Controllo componenti per le suddette applicazioni;
5. eventuale modifica delle **opzioni generali** del programma con il pulsante Avanzato (quali l'avvio automatico con il sistema operativo, la protezione delle impostazioni con una password, ecc...);
6. scelta del **file** per il salvataggio della configurazione corrente;
7. ravvio del computer.

Complimenti, l'installazione è completa! E' possibile iniziare ad usare Outpost Firewall.

Menù 'File' 2.1

Nuova configurazione: si accede ad una configurazione guidata del firewall che si divide in due opzioni, Configurazione automatica e Assistente configurazione.

Configurazione automatica

Scegliendo questa opzione Outpost creerà da sé una configurazione in base al software che è presente nel nostro sistema. Si tratta di un tipo di configurazione che si basa su una serie di regole predefinite sia a livello generale che più specificatamente per le singole applicazioni che sono presenti sul nostro sistema.
E' una soluzione che si rivolge agli utenti meno esperti ed esigenti ma che comunque è pur un buon inizio per prendere confidenza con il firewall.

Assistente configurazione

Con questa opzione verrà avviata una procedura guida sulla configurazione del firewall.
In questa procedura verranno proposte le medesime regole ed impostazioni della Configurazione automatica con la differenza però che vi sarà da parte dell'utente la possibilità di intervenire nelle varie fasi per decidere o meno se tali regole e impostazioni sono adatte al nostro sistema.

Le due procedure guidate accessibili tramite Nuova configurazione rendono questo firewall adatto anche a chi lo usa per la prima volta o a chi non ha dimestichezza con questo genere di software. Si tratta comunque di due soluzioni delle quali si può far a meno: spiegheremo infatti nel proseguo della guida come si può configurare il firewall in modo più professionale.

Importa configurazione: tramite questa funzione potremo importare una configurazione di Outpost precedentemente salvata: si tratta di un file con estensione **.cfg**. Per configurazione di Outpost si intende il salvataggio delle regole generali, delle applicazioni e delle impostazioni delle varie plug-in.

Salva configurazione come: tramite questa funzione possiamo salvare la configurazione del firewall che attualmente stiamo utilizzando. Il percorso predefinito è all'interno della directory di installazione del firewall, ma possiamo tranquillamente scegliere la cartella di destinazione che meglio crediamo.

Esci e chiudi: chiude definitivamente il firewall, chiedendo prima conferma.

Menù 'Visualizza' 2.2

Raggruppa per: questa funzione serve per raggruppare per tipo le voci che sono presenti nella struttura ad albero nel pannello di sinistra. Per fare un esempio pratico, se con il mouse evidenziamo il ramo Porte aperte e dal sottomenù Raggruppa per scegliamo la voce Processi, tutte le voci presenti sul ramo Porte aperte verranno raggruppate secondo il nome dei processi.

Filtra per tempo: questa funzione ha il compito di filtrare i dati presenti nei contatori nel pannello di destra.
Ø I contatori non sono presenti sui rami Attività rete e Porte aperte.
I report posso essere filtrati con le opzioni Sessioni corrente, Oggi e Tutto. Con Sessioni corrente vedremo il riepilogo dei conteggi effettuati dall'ultima volta che abbiamo avviato Outpost fino ad ora, con Oggi verrà visualizzato il conteggio su tutta la giornata corrente mentre con Tutto verranno visualizzati tutti i conteggi disponibili.

Colonne: disponibile solo per i rami Attività rete e Porte aperte, questa opzione permette di scegliere quali colonne saranno visualizzate all'interno del pannello di destra.

Avanzate: in questa finestra sarà possibile scegliere in che modo saranno visualizzati i dati indirizzo locale/remoto, identificazione della porta e dati inviati/ricevuti.

Sempre in primo piano: se spuntiamo questa opzione la schermata di Outpost resterà in primo piano e non sarà sovrapposta da altre finestre di altre applicazioni.

Aspetto: in questa finestra possiamo decidere la visualizzazione o meno di alcune barre e voci presenti nel pannello di sinistra.

Azzera contatori: resetta tutti i contatori.

Lingua: scelta della lingua.

Menù 'Utilità' 2.3

Aggiornamento Agnitum: viene avviata la procedura manuale per verificare la disponibilità di nuovi aggiornamenti on-line.

Controlla automaticamente aggiornamenti: se spuntiamo questa opzione Outpost controllerà in automatico la presenza di nuovi aggiornamenti.

Abilita aggiornamento notizie e Abilita aggiornamento su informazioni plug-in: se attiviamo queste funzioni ci verranno notificate informazioni riguardo i prodotti Agnitum e i plug-in di Outpost.

Abilita rapporto: se attiviamo questa opzione tutte le attività di rete verranno riportate all'interno dei report. Consiglio di lasciare abilitata questa opzione.

Visualizzatore rapporto Outpost Firewall Pro: apre il visualizzatore rapporti.

Prova il mio pc on-line: si viene indirizzati al sito www.pcflank.com per effettuare dei test sullo stato di sicurezza del nostro pc.

Menù 'Opzioni' 2.4

La spiegazione dei contenuti di questo menù verrà affrontata nel proseguo della guida in quanto **si tratta di un passo molto importante per la configurazione del firewall che richiede un capitolo a parte**.

Menù 'Aiuto' 2.5

Contenuti e indice: si accede alla guida (in inglese) di Outpost.

Informazioni aiuto: guida rapida: basterà fare clic sull'oggetto di cui cerchiamo informazioni.

Outpost Firewall Pro sul Web: si accede a vari contenuti sul Web riguardanti Outpost Firewall e la casa Agnitum che lo produce.

Novità: vengono presentate le novità della versione 2.5.

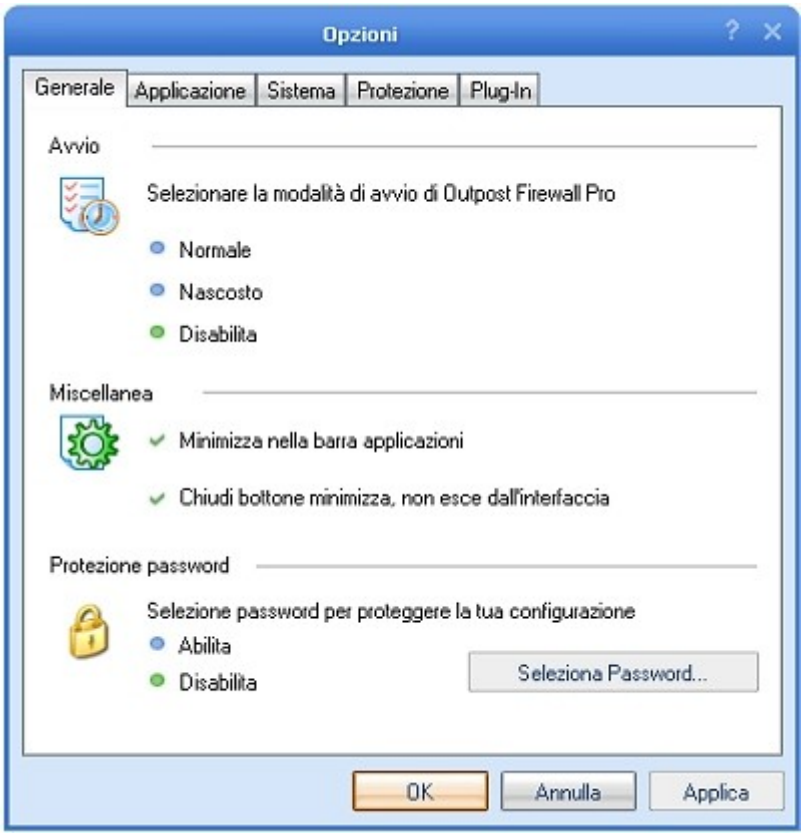
Informazioni su Outpost Firewall Pro: alcune informazioni sulla licenza e sui moduli che fanno parte del software.

CONFIGURAZIONE DEL FIREWALL (MENÙ 'OPZIONI') 3.0

Introduzione 3.1

Il menù Opzioni è senza dubbio quello più importante di Outpost Firewall: attraverso di esso infatti è possibile accedere a tutti gli aspetti funzionali del programma. Le schede a cui possiamo accedere sono: Generale, Applicazione, Sistema, Protezione e Impostazioni Plug-In. Vediamole in dettaglio una ad una.

Scheda 'Generale' 3.2



Attraverso questa scheda possiamo:

1. **Selezionare la modalità di avvio**.
   Normale: il programma viene caricato all'avvio del sistema e la sua icona è visibile in basso a destra.
   Nascosto: il programma viene caricato all'avvio ma a differenza della soluzione precedente l'icona non sarà visibile. E' una protezione: se su un pc accedono più persone, solo chi è al corrente di questa impostazione potrà intervenire per disabilitare Outpost.
   Disabilita: il programma non verrà eseguito automaticamente all'accesso di Windows. Sarà comunque possibile caricarlo manualmente quando ci si connette ad Internet.
2. **Impostare due opzioni**.
   Minimizza nelle barra delle applicazioni: il programma verrà sempre iconizzato in basso a destra e inoltre non verrà abilitata la possibilità di tenere la finestra aperta di Outpost. Mi sembra chiaro che convenga mettere il flag su questa opzione.
   Chiudi bottone minimizza, non esce dall'interfaccia: abilitandola, nel momento in cui cliccheremo sulla **X** in alto a destra il programma verrà minimizzato e non chiuso. Mi sembra chiaro che anche in questo caso conviene tenere abilitato il flag.

3. **Abilitare una password**.
   E' una funzione utilissima nel caso in cui il computer sia utilizzato da più persone: è possibile impostare una password per la protezione della configurazione del firewall, per l'esecuzione del Visualizzatore Rapporto e per l'uscita dal programma. Senza questa password non si potranno modificare le impostazioni.

Scheda 'Applicazione' 3.3

Nel riquadro Impostazioni troviamo tre intestazioni:

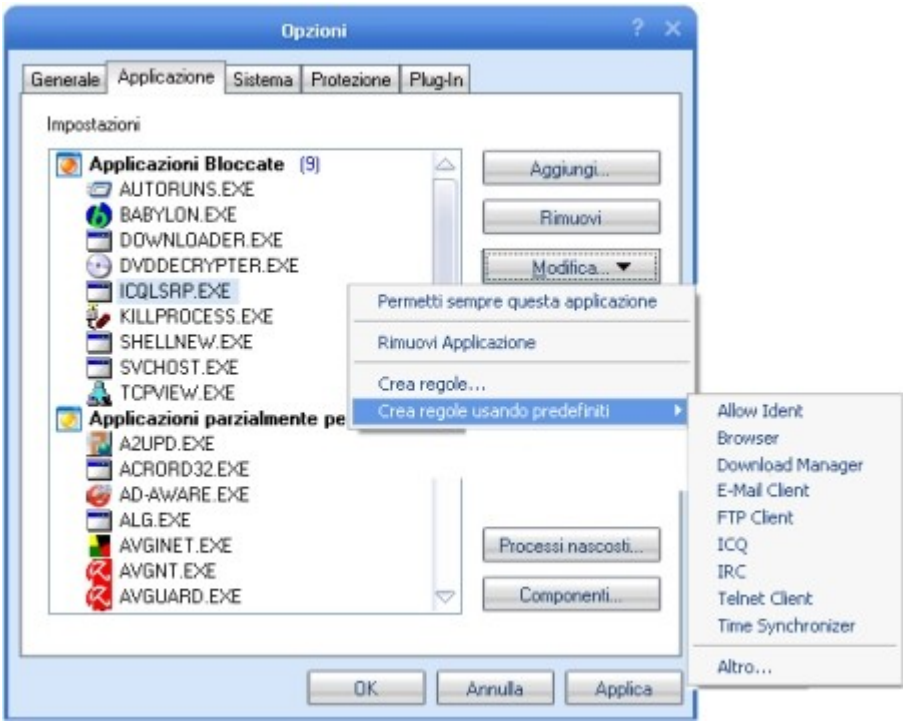
- **Applicazioni bloccate**. Sotto questa voce troveremo tutti quei programmi a cui abbiamo deciso di impedire l'accesso ad Internet: perciò non potranno comunicare con nessun server remoto.
- **Applicazioni parzialmente permesse**. Sotto questa voce verranno visualizzati i programmi ai quali è permessa una libertà limitata: saranno delle regole (rules) a stabilire cosa gli è permesso e cosa no.
- **Applicazioni permesse**. Sotto questa voce verranno visualizzati i programmi ai quali è concessa la libertà massima: potranno perciò comunicare tramite Internet con qualsiasi server remoto e tipo di dati. Per fare un esempio banale, se poniamo ICQ sotto questa voce esso si connetterà anche ad IP che non hanno nulla a che fare con il login, ma solo per visualizzare banner o pagine Web.

Ø Pulsante Aggiungi: possiamo, tramite Esplora Risorse, selezionare un'applicazione per la quale vogliamo impostare delle regole.

Ø Pulsante Rimuovi: selezionando un'applicazione all'interno di una delle tre intestazioni, è possibile rimuoverla con questo pulsante.

Ø Pulsante Modifica: premendolo, comparirà un menù a tendina comprendente voci diverse a seconda dell'intestazione in cui ci troviamo (vedi figure seguenti).

Intestazione Applicazioni Bloccate



Intestazione Applicazioni parzialmente permesse

Intestazione Applicazioni permesse

Questo è il significato delle voci presenti nel menù a tendina:

Permetti sempre questa app: serve a porre l'applicazione selezionata nella sezione Applicazioni Permesse.
Blocca sempre questa app: serve a porre l'applicazione selezionata nella sezione Applicazioni Bloccate.

Modifica regole: serve per modificare le regole già presenti dell'applicazione selezionata.

Crea regole: serve per creare delle regole per una applicazione che non ne abbia.

Crea regole usando predefiniti: serve per attribuire al programma selezionato delle regole predefinite per tipo di applicazione (browser, download manager, ecc...).

Rimuovi applicazione: serve a rimuovere l'applicazione e le sue regole dalla lista.

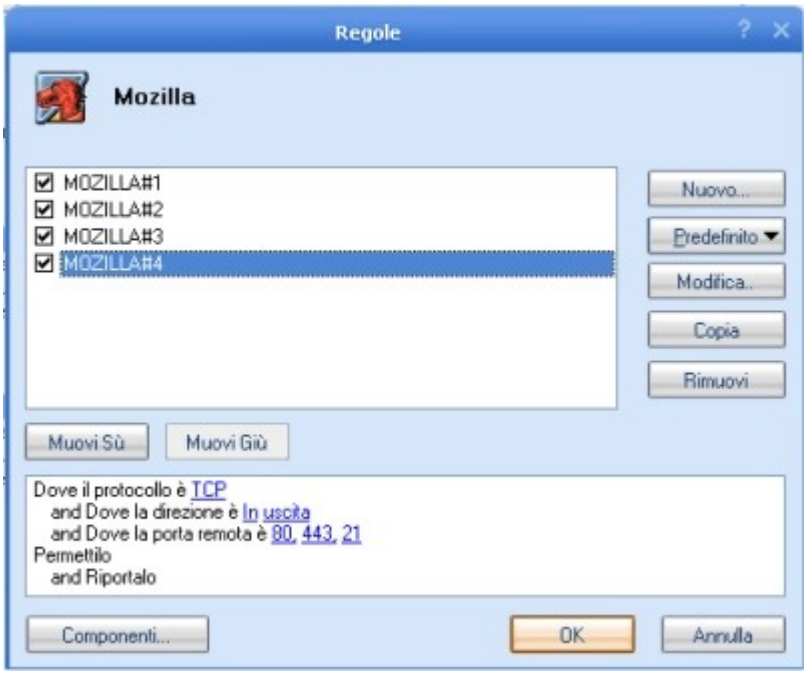
Attraverso il pulsante Processi Nascosti abbiamo la facoltà di scegliere il comportamento di Outpost nei confronti questi processi. Si tratta di una tecnica mediante la quale un'applicazione avvia un processo secondario al suo interno facendolo passare per proprio ed eludendo il controllo del firewall: se da un lato è una tecnica sfruttata a fini benevoli (come ad esempio il controllo automatico degli aggiornamenti), dall'altro può essere utilizzata da software maligni per tentare, ad esempio, di inviare informazioni personali dell'utente attraverso la Rete. E' bene lasciare questa impostazione su Chiedi: avremo così sempre sotto controllo qualsiasi attività da parte delle applicazioni, potendo scegliere l'azione da intraprendere.

Il pulsante Controllo Componenti ci permette invece di impostare il livello di questa funzione. Le applicazioni sono generalmente composte da più moduli (ad esempio le librerie .DLL), alcuni dei quali possono richiedere accesso alla Rete, sempre risultando parte integrante dello stesso programma. Esistono dei software maligni che sono in grado di sostituirsi a questi moduli, tentando di avere libero accesso alla Rete sfruttando il fatto che l'applicazione a cui si sono 'agganciati' è considerata sicura dal firewall.
Il livello Normale è il miglior compromesso tra funzionalità e sicurezza. Il pulsante Modifica lista... apre una finestra nella quale si può consultare la lista dei componenti sotto controllo: è possibile aggiungerne o rimuoverne e ricostruire la lista con un nuovo controllo su disco da parte di Outpost (Ricostruisci database). Selezionando un componente dalla lista, nella sezione Dettagli Componente in basso Outpost fornisce svariate informazioni sul modulo: utilissime per capire se è legittimo e conosciuto oppure potenzialmente pericoloso.

Molto importante è infine lasciare il flag sull'opzione Apri Controllo Processo: è un'interessante funzionalità di Outpost volta a bloccare la cosiddetta **vulnerabilità CopyCat**, ovvero un'operazione attraverso la quale un programma (spesso maligno) tenta di alterare il codice di un'applicazione benigna residente in memoria inserendovi il proprio, con lo scopo di eludere il controllo del firewall.

3.3.1 - Gestione delle regole

E' bene dedicare un piccolo approfondimento a parte per ciò che riguarda la gestione delle regole per le applicazioni. Esse possono essere create/modificate/rimosse attraverso due finestre: alla prima possiamo accedere premendo il pulsante Modifica e scegliendo Crea regole:

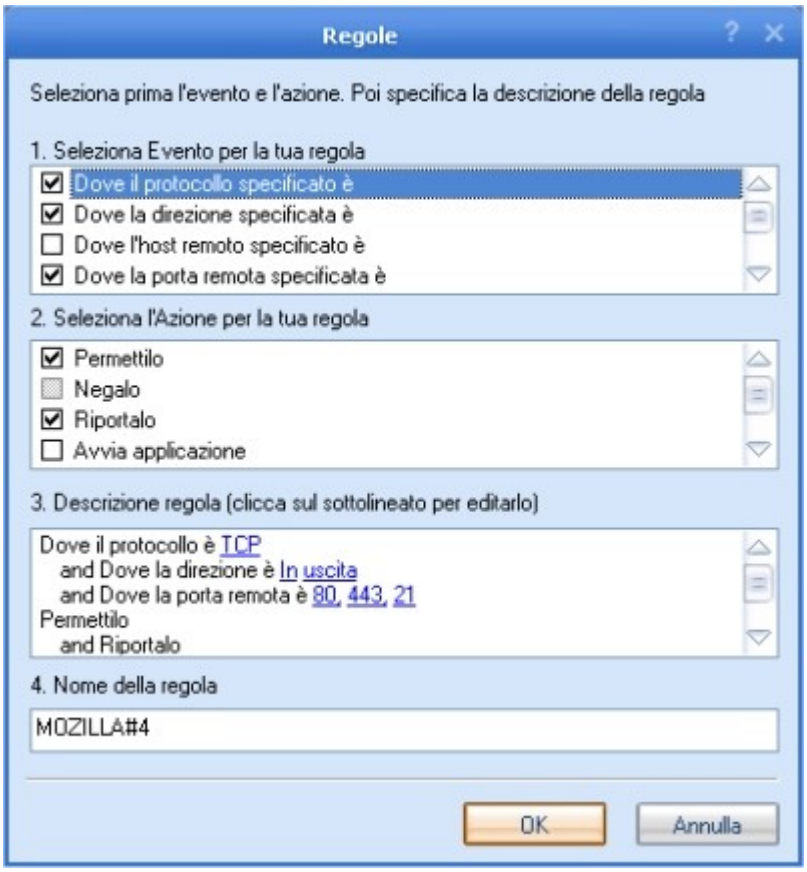


descriviamo brevemente le funzioni dei singoli pulsanti.

Nuovo: serve per creare una nuova regola dell'applicazione scelta.
Predefinito: serve per scegliere tra le regole preconfigurate di Outpost.
Modifica: serve per modificare una regola già creata.
Copia: serve per fare una copia della regola evidenziata.
Rimuovi: serve per eliminare una regola esistente.
Muovi su: serve per spostare in su la regola.
Muovi giù: serve per spostare in giù la regola.
Componenti: serve per accedere alla lista dei componenti presenti nel Database di Outpost. Sarà possibile eliminare quelli che riteniamo sospetti, aggiungerne degli altri ed anche inserire una nuova applicazione ed i componenti che utilizza tramite il pulsante Aggiungi.

Nota: non bisogna sottovalutare l'importanza dell'ordine con cui sono posizionate le regole.

Nel momento in cui andremo a premere Nuovo o Modifica per creare da zero o modificare una regola, ci apparirà invece una finestra simile alla seguente:



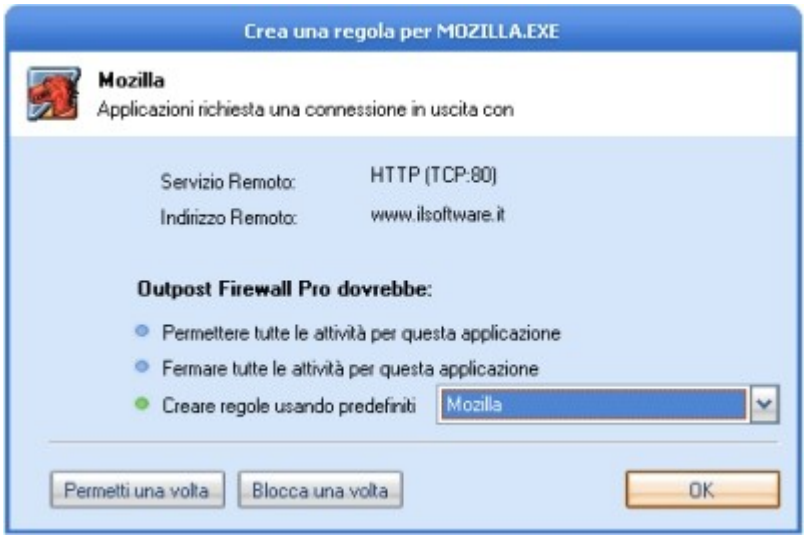
all'interno vi sono quattro sezioni che sono:

1) **Seleziona evento per la tua regola**: si imposta in quali condizione ad una determinata applicazione è permesso o negato comunicare su Internet. Queste sono le possibili scelte:
   - Dove il protocollo specificato è
   - Dove la direzione specificata è
   - Dove l'host remoto specificato è
   - Dove la porta remota specificata è
   - Dove la porta locale specificata è
   - Dove l'intervallo di tempo specificato è
   - Dove la porta locale è uguale alla porta remota

2) **Seleziona azione per la tua regola**: si seleziona quale tipo di permesso è concesso in relazione a ciò che abbiamo impostato su Selezione evento per la tua regola. Queste sono le possibili scelte:
   - Permettilo: permette all'applicazione di comunicare tramite Internet, rispettando sempre le impostazioni date in Selezione evento per la tua regola.
   - Negalo: nega all'applicazione di comunicare tramite Internet, rispettando sempre le impostazioni date in Selezione evento per la tua regola; inoltre, **non notifica** alla fonte che il pacchetto è arrivato a destinazione.
   - Riportalo: verrà riportato tramite una finestra pop-up (vicino alla tray bar) e sul Rapporto Eventi della sezione Riportato l'utilizzo di questa regola da parte dell'applicazione.
   - Avvia applicazione: sarà possibile eseguire una determinata applicazione quando questa regola viene applicata da Outpost. Un esempio potrebbe essere quello di dover lanciare un software per la traduzione di testi dall'inglese all'italiano una volta che accediamo ad una determinata pagina web.
   - Stato di ispezione: se spuntata, sarà attivata una speciale tecnologia del firewall che tiene traccia delle sessione attive TCP ed UDP, consentendo il passaggio del traffico di Rete attraverso percorsi più piccoli e quindi più facilmente controllabili. E' una funzione che garantisce maggior sicurezza rispetto al classico filtraggio dei pacchetti, ma richiede più tempo per il controllo ed un maggior impegno del firewall.
   - Ignora Controllo Componenti: se mettiamo il flag su questa opzione verrà ignorata la funzione Controllo Componenti nel caso in cui l'applicazione che sfrutta questa regola dovesse usufruire di componenti quali spesso sono le librerie .DLL per il suo corretto funzionamento.
3) **Descrizione regola**: in questo riquadro viene riassunta la regola creata. Se poi si clicca nelle impostazioni evidenziate in blu (collegamenti) si accederà direttamente alla loro modifica.
4) **Nome della regola**: si immette il nome della regola creata che può essere ben differente dal nome che le viene affibbiato di default da Outpost.

Creazione regole durante la navigazione.

Fino adesso sono state spiegate quali opzioni vengono offerte per poter configurare dei ruoli ad hoc per un'applicazione. L'utente però si trova a dover configurare spesso in modo dinamico le regole per un'applicazione: per 'in modo dinamico' intendo dire mentre naviga su Internet.
Vediamo ora quali sono le finestre che compaiono all'utente quando naviga: la prima è nella foto seguente,



e ci fornisce numerose indicazioni.
Mozilla applicazioni richiesta una connessione in uscita con: Outpost segnala all'utente che un programma che si chiama Mozilla sta tentando di effettuare una comunicazione in uscita. Sarà banale, però specifico

che esistono due tipi di comunicazione: in **uscita** ed in **entrata**. Generalmente si ha a che fare con comunicazioni in uscita. Comunicazioni in entrata possono ad esempio apparire quando si usa un programma Peer-to-Peer (come WinMX e Kazaa Lite): infatti, in queste situazioni, si deve dare il permesso anche agli altri utenti di poter scaricare dal vostro hard disk.

Continuando con le informazioni che Outpost fornisce all'utente, noteremo che viene data indicazione della porta che Mozilla vuole utilizzare (*Servizio* remoto: HTTP (TCP:80)) e del relativo protocollo (TCP).

Viene anche segnalato verso quale indirizzo vuole comunicare (Indirizzo remoto: www.ilsoftware.it).

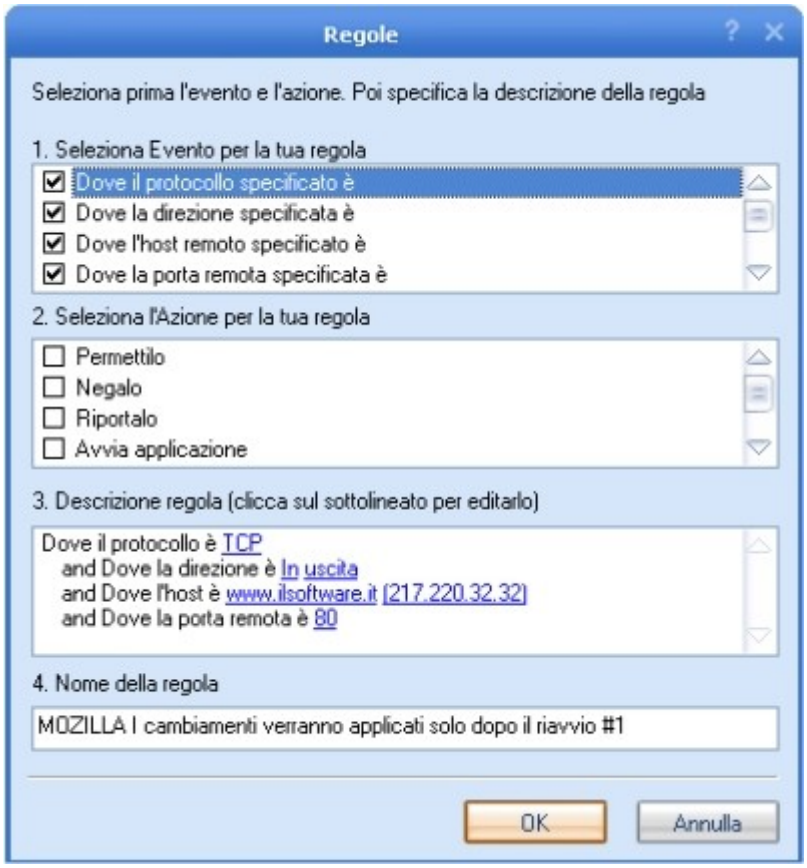
Una volta raccolte queste informazioni e fatti un'idea di cosa sta succedendo (l'applicazione è pulita oppure si tratta di uno spyware ad esempio), dovremo decidere come comportarci nei confronti di questa richiesta.

Outpost come al solito ci viene incontro, dicendoci: Outpost Firewall Pro dovrebbe:

- Permettere tutte le attività per questa applicazione: in questo caso Outpost collocherà l'applicazione in questione tra quelle totalmente permesse. Quindi, d'ora in poi, questo programma avrà accesso su tutte le porte. Vi faccio notare che questa è una cattiva soluzione in quanto consente all'applicazione di fare quello che vuole.
- Fermare tutte le attività per questa applicazione: Outpost collocherà definitivamente nelle applicazioni bloccate Mozilla che quindi non potrà comunicare in nessun modo. L'unica soluzione, se volessimo utilizzare l'applicazione, sarà quella di rimuovere l'applicazione da quelle totalmente bloccate. State attenti quindi quando configurate l'accesso per un'applicazione (ovviamente fidata) a non mettere il flag su questa opzione altrimenti non riuscirete a farla funzionare su Internet.
- Crea regole usando predefiniti: significa che Outpost ha una serie di regole predefinite per le applicazioni più conosciute. In questo caso il firewall ha riconosciuto l'applicazione e segnala all'utente che esistono già delle regole preconfigurate per Mozilla. Se abilitiamo questa opzione, l'applicazione verrà collocata nella categoria parzialmente permesse con un pacchetto di regole predefinito.
  Questa soluzione può essere utile per un utente con poca esperienza sulla configurazione di un firewall, in quanto vengono di default abilitate svariate possibili comunicazioni. Il vantaggio è che abbiamo già finito, lo svantaggio è che spesso è permesso più di quanto serva realmente a questa applicazione. Mi sembra palese quale soluzione preferisco: consiglio, se si utilizza la prima opzione (regole predefinite) di andare a verificare quali regole sono state create ed eventualmente modificarle in un secondo momento.
- Permetti una volta e Blocca una volta sono comandi importanti ed utilissimi: consentono infatti di permettere o bloccare, ogni volta che un'applicazione ne faccia richiesta, una comunicazione. Vedrete che andando avanti vi spiegherò perché sono così importanti.

Siamo arrivati ad un punto in cui Outpost ci ha dato delle informazioni e ci ha detto cosa può fare. A questo punto, agiamo scegliendo l'opzione Altro (dal menù a tendina), vedi immagine qui sotto.

La finestra che comparirà successivamente permetterà di entrare nel dettaglio di una specifica regola (vedi foto seguente):



ancora una volta Outpost ci viene incontro, indicando in Descrizione regola com'è strutturata la regola: Dove il protocollo è il TCP e dove la direzione è in uscita e dove l'host remoto è 217.220.32.36 e dove la porta remota è HTTP (cioè la porta 80). Come potete notare tutte queste informazioni erano già presenti nella finestra iniziale: Outpost ora le dispone semplicemente in un ordine attraverso il quale recepisce una regola per un'applicazione specifica.

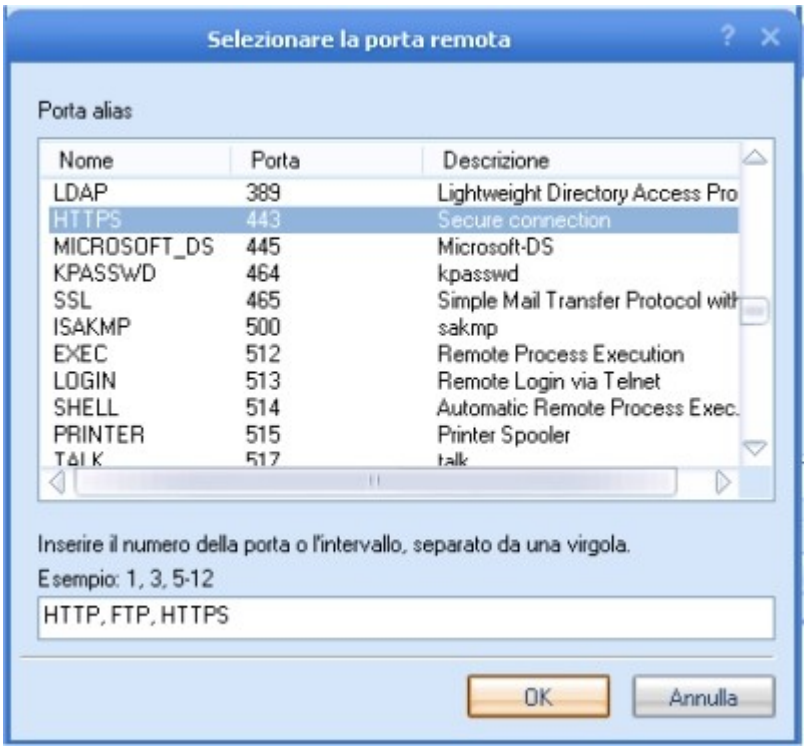
Entriamo ora un po' di più nel dettaglio. Il protocollo è il TCP (tutto ok), la porta remota è HTTP (è una porta standard) e l'host è un indirizzo specifico. Viste le premesse TCP e porta 80 e considerato poi che il 90% dei siti sono consultabili attraverso la porta 80, perché vincolare questa regola ad un sito specifico considerato poi il fatto che ci piace usare Mozilla? La soluzione a questo problema è semplice: basterà togliere nel campo Seleziona Evento per la tua regola il flag Dove l'host remoto specificato è ed il gioco è fatto.

A questo punto la nostra regola sarà cambiata in 'TCP - Outbound - HTTP' . Pensiamo che la regola sia perfetta: allora dovremmo scegliere il tipo di azione da intraprendere quando Outpost si trova in questa situazione e, nel riquadro Seleziona l'azione per la tua regola, metteremo il flag su Permettilo.

Per un attimo immaginiamo di essere degli utenti un po' di più smaliziati: noi sappiamo quindi che Mozilla non avrà bisogno solo della porta HTTP (80) per comunicare, ma sarebbe meglio abilitare fin dall'inizio la possibilità di navigare su un sito FTP (porta 21) e di poter fare degli acquisti su Internet HTTPS (porta 443).

Come facciamo?

Sarà sufficiente cliccare sul link 80 (HTTP) e quindi apparirà una nuova finestra (vedi foto seguente).



In fondo a questa finestra c'è una voce che dice *Inserire* il numero della porta o intervallo, separato da una virgola. Come noterete dalla foto, io ho inserito tre porte separate dalla virgola: HTTP, FTP, HTTPS (che sono rispettivamente la 80, 21, 443): sono le porte che ci interessavano.

Quando vogliamo inserire una serie di porte che non sono contigue dovremo usare la virgola come ho indicato nell'esempio precedente. Se invece volessimo abilitare delle porte che sono contigue, allora dovremo utilizzare il trattino: ad esempio, scrivendo 137-139, saranno abilitate le comunicazioni sulle porte 137, 138 e 139.

Per riprendere il filo logico del discorso, ricordiamoci che tutto questo è stato fatto per abilitare Mozilla a comunicare sulle porte 21, 80 e 443. Forse il numero delle porte vi sembrerà ristretto: io penso di no, in quanto dapprima è meglio abilitare poche porte per poi verificare durante le nostre navigazioni su Internet se abbiamo realmente bisogno di altre porte oltre a quelle già inserite.

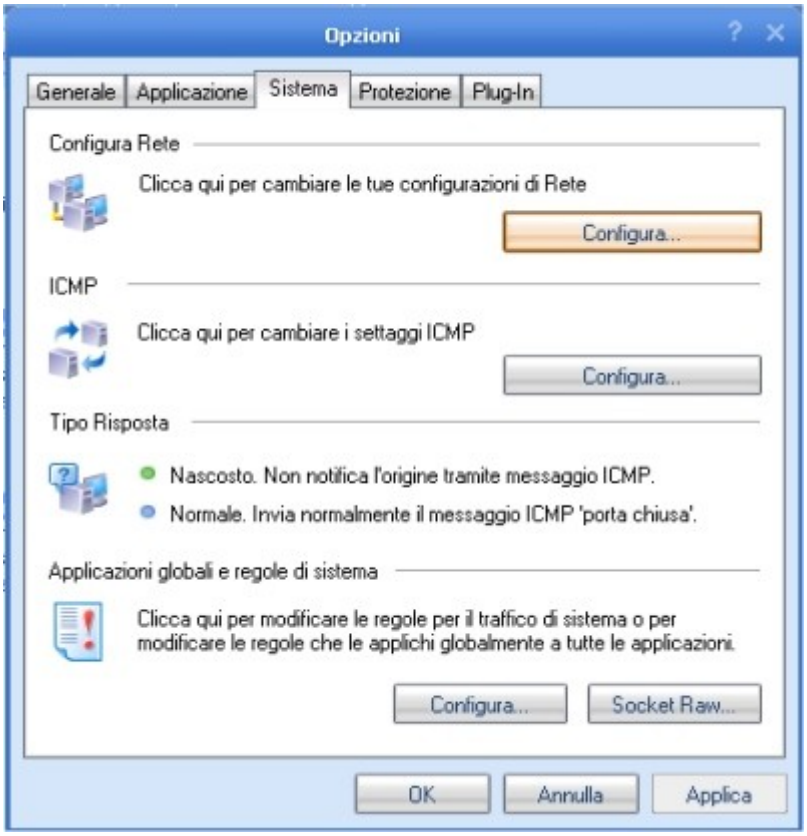
La cosa migliore è partire con delle regole ristrette e molto rigide; poi a mano a mano che si naviga su Internet si verifica se le regole create sono adatte in base alle nostre abitudini. Non ha senso all'inizio abilitare l'apertura di porte che non sappiamo neanche se utilizzeremo. In più considerate anche quest'aspetto: se noi abilitiamo subito anche tante altre porte oltre quelle qui suggerite, non sapremo mai con quale frequenza apriremo queste porte durante la navigazione (salvo consultazioni giornaliere dei log, dico giornaliere perché dopo un po' i dati vengono cancellati). Questo non va assolutamente bene perché stiamo utilizzando delle maglie troppo larghe e perché non sappiamo se effettivamente ne abbiamo bisogno.

Altra considerazione. Ricordo sempre che abbiamo abilitato solo le porte 21, 80 e 443: vogliamo però visualizzare una pagina che richiede una connessione sulla porta 8080 oppure sulla porta 5000, oppure su un'altra porta. Outpost ci segnala questo tentativo di comunicazione: cosa fare? Potremmo come al solito aspettare e vedere cosa succede (a volte si fanno delle scoperte interessanti), permettere una volta la comunicazione su questa porta (Permetti una volta) oppure creare una regola.

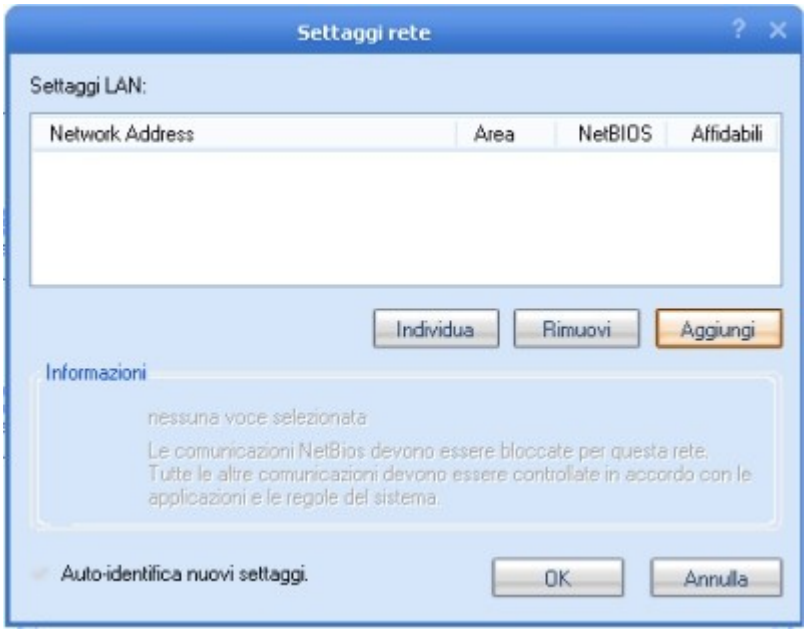
A questo punto è utile chiedersi: la regola che voglio creare, la creo solo per questo sito oppure per tutti i siti? La risposta è la prima, la creo solo per questo sito. Solo il tempo ci dirà se abbiamo fatto bene oppure no. Mi spiego meglio. Se durante le nostre navigazioni sul Web incontreremo poche o nessuna richiesta per questa porta generica, di cui parlavo prima, allora avremo fatto benissimo. Se viceversa tutti i giorni ci troviamo a confrontarci con richieste di questo tipo (ad ogni richiesta deve corrispondere un sito diverso), beh allora forse è meglio cambiare la regola ed abilitarla per tutti i siti.

Scheda 'Sistema' 3.4

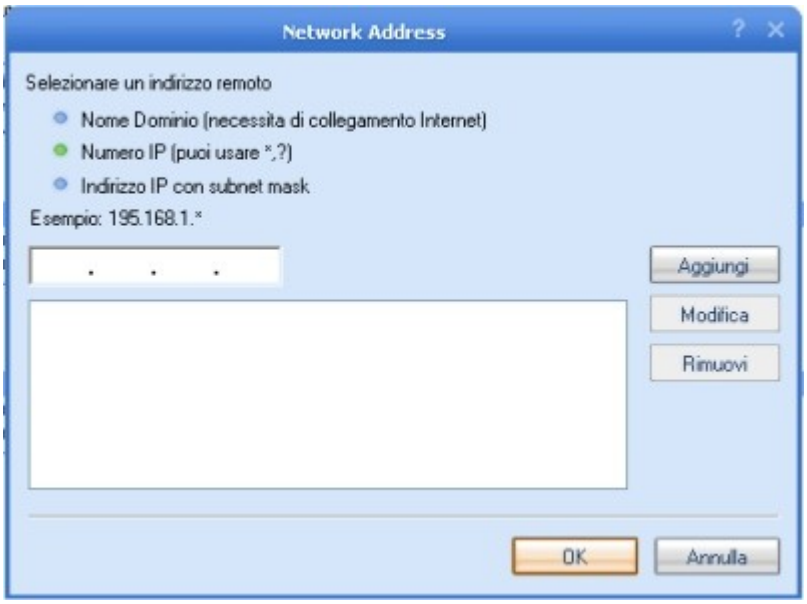
Da questa scheda è possibile configurare diversi componenti di Outpost: Rete, ICMP, Tipo risposta, Applicazioni globali e regole di sistema.



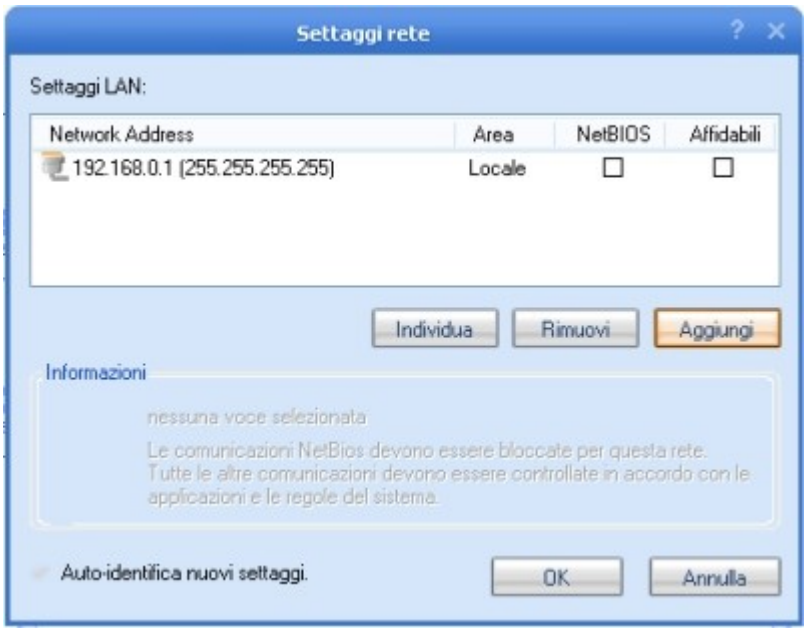
- **Configura Rete**: serve per tutti gli utenti che hanno due o più pc collegati tra loro mediante una scheda di rete. Se premiamo sul pulsante Configura apparirà una maschera dove è possibile inserire un indirizzo o un range di IP (tutti identificativi delle altre macchine che sono in rete):



da questa maschera sarà sufficiente cliccare sul pulsante Aggiungi: comparirà un'altra maschera dove è possibile indicare gli indirizzi IP:



dovremo a questo punto inserire l'IP dell'altro computer, cliccare sul pulsante Aggiungi ed infine sul pulsante OK. A questo punto ci troveremo in questa situazione:

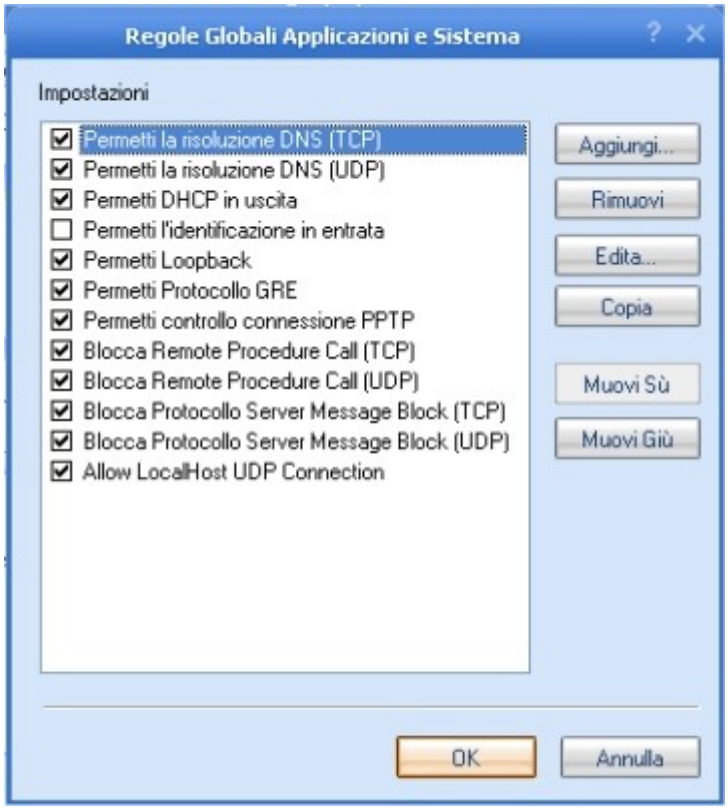


come si può notare, ci sono ancora delle opzioni che dovremmo abilitare: NetBIOS ed Affidabili. Con il flag su NetBIOS, verranno abilitate tutte le comunicazioni NetBIOS indispensabili per condividere risorse piuttosto che stampanti. Con il flag Affidabili (diciamo che si tratta di un opzione rafforzativa della prima) tutte le comunicazioni di rete saranno permesse.
Se mettiamo la spunta anche su Auto-identifica nuovi settaggi, eventuali nuovi pc collegati alla rete locale verranno rilevati in modo automatico.

- **ICMP**. Qui si tratta di settare i permessi di Outpost in presenza di determinati pacchetti che vengono inviati dall'esterno. Per configurarli sarà sufficiente cliccare sul pulsante Configura: comparirà una maschera di questo tipo:

nella prima colonna vengono indicati tipi di ICMP, nella seconda il numero universale che li identifica ed infine nelle ultime due colonne Ingresso ed Uscita possiamo impostare il permesso di accettarli e inviarli. Io ho sempre **disabilitato tutto**: meno facciamo sapere che ci siamo e meglio è. Sottolineo il fatto che navigo tranquillamente; presumo comunque che alcuni di questi ICMP possono essere utili se siamo in presenza di due o più computer collegati in rete.

- **Tipo Risposta**: Nascosto significa che Outpost non permette di inviare pacchetti in risposta ad altri pacchetti che arrivano dalla rete. Ad esempio, facciamo un ping su un IP: se a quell'indirizzo corrisponde un computer, in una situazione normale (senza Outpost) la macchina risponderà inviando un pacchetto: tutto ciò vuol dire che potremmo aver trovato un computer da attaccare. Consiglio quindi di utilizzare questa opzione, Nascosto. E' consigliabile utilizzare Normale in presenza di due o più pc collegati in rete.



- **Applicazioni globali e regole di sistema**: qui è possibile configurare delle regole che valgono per tutte le applicazioni e per il sistema. Di default sono già impostate alcune regole (vedi figura a destra).
  Le regole che hanno il flag sono regole attive, vale a dire che vengono applicate da Outpost sia che si tratti di applicazioni di terzi parti che di applicazioni del sistema operativo.

E' un aspetto del firewall che risulta essere estremamente utile ma anche soggettivo, nel senso che l'abilitazione o la creazione di nuove regole può variare da sistema a sistema in base alle esigenze personali.
Nel mio specifico caso (un pc desktop per uso home e senza rete LAN), ho tolto tutti i flag sulle regole con Permetti lasciato quelli su Blocca. Poi ho aggiunto le seguenti regole:

- **Dove il protocollo è protocollo sconosciuto**
- **Negalo e Riportalo**

- **Dove il protocollo è IP e tipo è RAWSOCKET, ICMP, IGMP, GGP, IPIIP, ST, CBT, EGP, NVP, TMUX, HMP, RDP, IRDP, NETBLT, SDRP, GRE, ESP, AH, NARP, MEP, SKIP, ICMPv6, VMTP, OSPF, MTP, IFMP, PIM, IPPCP, VRRP, PGM, PTP, SCPTP**
- **Dove la direzione è in uscita e tipo di pacchetto è Locale, Transito, NAT**
- **Negalo e Riportalo**

- **Dove il protocollo è IP e tipo è RAWSOCKET, ICMP, IGMP, GGP, IPIIP, ST, CBT, EGP, NVP, TMUX, HMP, RDP, IRDP, NETBLT, SDRP, GRE, ESP, AH, NARP, MEP, SKIP, ICMPv6, VMTP, OSPF, MTP, IFMP, PIM, IPPCP, VRRP, PGM, PTP, SCPTP**
- **Dove la direzione è in arrivo**
- **Negalo e Riportalo**

A proposito di DNS Resolving.

Nel sistema operativo XP, il resolving DNS è gestito dal servizio **Client DNS** che sfrutta le molteplici funzioni del file **svchost.exe**. Se vogliamo che il resolving DNS non venga fatto da **svchost.exe** ma da ogni singola applicazione, dobbiamo dapprima impostare su Disabilitato il servizio **Client DNS**, togliere poi il flag da Permetti la risoluzione DNS (impostazioni regole globali) e porre **svchost.exe** tra le applicazioni **bloccate**.
Per regolare il Resolving DNS, con un po' di pazienza si crea una regola per ogni singola applicazione. Appena eseguiamo un'applicazione vergine (senza nessuna regola ancora formata) la prima cosa che ci verrà richiesta da Outpost sarà di creare una regola per il Resolving DNS. Nel mio caso è questa:

- **Dove il protocollo specificato è UDP**
- **Dove l'host remoto specificato è HOST del proprio provider**
- **Dove la porta remota specificata è DNS (53)**
- **Permettilo**

Si tratta di creare una regola per la risoluzione del DNS per ogni applicazione, indicando come host il DNS del proprio provider. E' una scelta di sicurezza, e non di piacere: la regola che Outpost mette a disposizione è troppo generica e potenzialmente pericolosa per il sistema.

- **Socket Raw**: tutte le applicazioni aggiunte all'interno della finestra Socket Raw avranno un accesso illimitato alla rete. Le regole globali per le applicazioni non hanno alcun effetto sui programmi che sono stati aggiunti in Socket Raw.

Scheda 'Protezione' 3.5

Qui è possibile settare il comportamento generale di Outpost attraverso 5 opzioni:

1. **Modalità Disabilitata**: disabilita il firewall e quindi permette tutte le comunicazioni senza imporre alcuna restrizione. Ovviamente non è consigliabile utilizzare questa opzione.
2. **Modalità Blocco totale**: blocca tutte le connessioni sia in entrata che in uscita: non sarà possibile navigare su Internet. Potremmo utilizzarla in caso di pericolo o per ragioni di sicurezza.
3. **Modalità Blocca di più**: vengono bloccate tutte le attività delle applicazioni che non sono permesse. Sarà necessario creare manualmente delle regole di permesso per queste applicazioni senza poter sfruttare alcuna procedura guidata e andare ad analizzare il file di log per verificare le comunicazioni bloccate.

4. **Regole Assistite**: si abilita una procedura guidata per la creazione di regole per ogni tipo di comunicazione che non è coperta da una regola esistente. Installiamo ad esempio un nuovo client di posta elettronica: Outpost metterà a disposizione una procedura guidata per creare delle regole così che in futuro quest'applicazione possa comunicare. Se fosse stata abilitata l'opzione Modalità Blocca di più, Outpost avrebbe immediatamente bloccato qualsiasi comunicazione dell'applicazione, rendendo necessario creare delle regole manuali senza usufruire della procedura guidata.
5. **Modalità Permetti di più**: permette a tutte le applicazioni di comunicare, a parte quelle che sono state inserite in Applicazioni bloccate. Non è un'opzione interessante poiché troppo permissiva: la sconsiglio.

Scheda 'Plug-In' 3.6

Questa scheda raccoglie l'elenco delle plug-in di Outpost installate e ne permette la configurazione. Quelle presenti e funzionanti di default: Blocco pubblicità, Cache Nomi Dominio (DNS), Filtro Contenuti, Filtro Contenuti Attivi, Individuazione Attacchi e Quarantena Allegati. Vediamole di seguito una ad una.

Blocco pubblicità

La sua funzione è quella di consentire il blocco di banner pubblicitari ed immagini contenute in una pagina web. Questo consentirà di caricare più velocemente certe pagine.
Entrando nel setup del Plugin, incontreremo 4 schede che sono: Stringa HTML, Dimensione Immagine, Miscellanea e Impostazioni.

Scheda Stringa HTML

La scheda *Stringa HTML* presenta parecchie stringhe inserite di default. E' possibile aggiungere altre stringhe in due modi:

- copiando una nuova stringa da inserire nell'apposita casella e quindi con il comando Aggiungi inserendola fra quelle già in lista.
- abilitando il Trashcan (cestino) cioè un cestino sul desktop: questo cestino spazzatura consente di configurare in modo più flessibile il blocco delle immagini.
  E' necessario fare una premessa: **il suo utilizzo differisce a seconda del browser che utilizziamo**.
  Con Internet Explorer è possibile utilizzare la tecnica del 'drag and drop'. Per esempio, apriamo una pagina Internet con Explorer: ci sono parecchie immagini nella pagina web, decidiamo che alcune non ci interessano perché rappresentano soltanto pubblicità. Spostiamo il cursore sull'immagine che non ci interessa e, tenendo cliccato il pulsante sinistro, la trasciniamo nel cestino. Se la procedura è corretta vi accorgerete che quando siete sopra il cestino ci sarà la freccia del mouse con un piccolo documento linkato. Se vogliamo verificare il blocco delle immagini appena impostato, basterà pulire la cache di Explorer (Strumenti/Opzioni Internet/Elimina file mettendo il flag su elimina tutto il contenuto non in linea) e ricaricare la pagina Internet.
  Dicevo che il Trashcan funziona in modo diverso a seconda del browser che si utilizza. Ad esempio con Netscape è necessario copiare il link e quindi incollarlo nel cestino. Con Mozilla Firebird funziona il 'drag and drop' come con Internet Explorer.
  Se clicchiamo sull'iconcina a forma di foglio, si aprirà una nuova finestra per aggiungere un'ulteriore lista di stringhe da bloccare: tale lista la possiamo poi modificare o eliminare utilizzando i pulsanti Rimuovi, Modifica e Aggiungi.

Scheda Dimensioni Immagine

Si può abilitare questa funzione mettendo la spunta nell'apposita casella. Qui sono inserite le dimensioni di immagini che vengono bloccate nei vari siti. Ovviamente ne possiamo inserire anche noi utilizzando gli appositi pulsanti Aggiungi , Rimuovi, Modifica.
Il primo campo rappresenta la larghezza dell'immagine, mentre il secondo la lunghezza.

Scheda Miscellanea

In questa scheda possiamo stabilire se nello spazio dell'immagine che non viene caricata deve essere vi-

sualizzato il testo [AD] oppure un'immagine trasparente.

Nella sezione Siti Affidabili, tramite il pulsante Modifica lista possiamo accedere ad una finestra in cui sarà possibile creare una lista di siti considerati affidabili.

Se mettiamo la spunta su Oggetti Pubblicitari Outpost bloccherà in base alle dimensioni ed alle parole chiavi stabilite certe animazioni, quali ad esempio Macromedia Flash movies.

Scheda Impostazioni

Abbiamo la possibilità tramite i due pulsanti presenti in questa scheda di importare od esportare una determinata configurazione memorizzata in un file con estensione **.ad*.

Cache Nomi Dominio (DNS)

E' un plugin che ha poco a che fare con la sicurezza ma che comunque presenta degli aspetti interessanti.

Il suo compito è quello di fare il resolving DNS di tutti gli indirizzi che stabiliscono una connessione con il nostro pc, sia che si tratti dei siti che visitiamo che di immagini con collegamenti esterni alle pagine web che apriamo; viene ad esempio fatto il resolving DNS anche ai server su cui andiamo a scaricare gli aggiornamenti per i vari Antivirus e Antitrojan.

Personalmente la considero una comodità sapere che abbiamo stabilito una connessione con dl2.avgate.net piuttosto che con 62.146.66.182.

Nella scheda Generale di questo plugin consiglio di mettere i flag su tutte le opzioni e di settare il numero dei record e la loro scadenza in modo che il log non assuma dimensioni troppo grandi.

Non mi dilungo sulla spiegazione delle due opzioni presenti nella scheda Varie in quanto sono di per se non molto importanti e di facile comprensione.

Filtro Contenuti

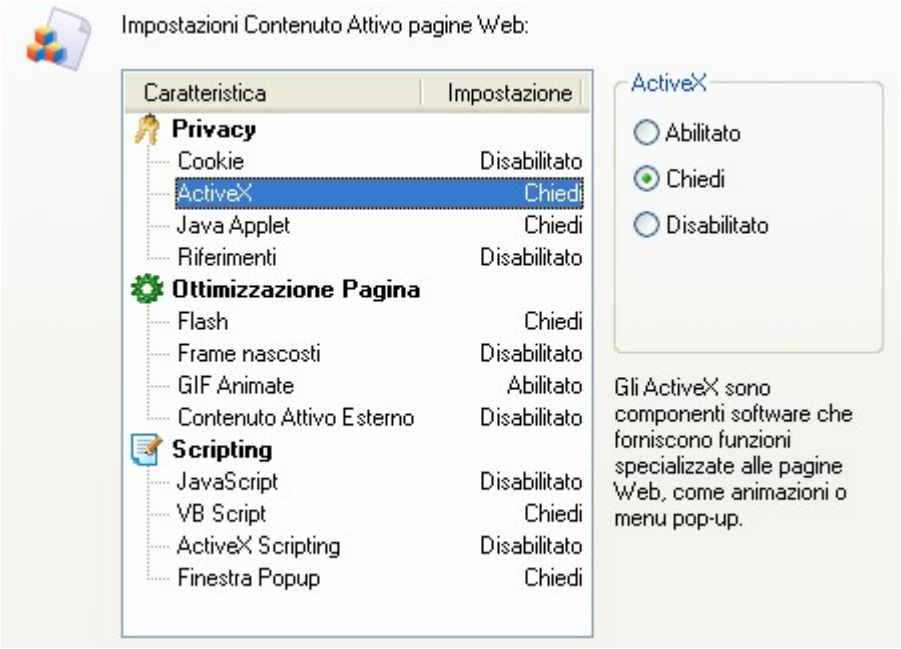
L'utilizzo di questo plugin consente di:

1. bloccare l'apertura di certe pagine web che contengono al loro interno determinate parole (una specie di parental control) che dovremo inserire noi (es. sex, drug) preferibilmente sia in inglese che in italiano.
2. bloccare determinati siti che non vogliamo visualizzare;
3. stabilire quale messaggio verrà visualizzato sulla pagina web di cui verrà bloccato il contenuto;
4. stabilire una lista di siti affidabili dei quali Outpost non bloccherà il contenuto;
5. importare od esportare un file con all'interno la lista dei siti o delle parole bloccate.

Filtro Contenuti Attivi

E' il plug-in più importante per la navigazione sicura su Internet. Consente infatti di bloccare tutta una serie di applicazioni che possono interagire con il browser per l'apertura e visualizzazione di una pagina web.

Una volta entrati nel setup, il layout della configurazione è diviso in tre schede che sono: Pagine Web, Posta e News e Esclusioni.



Scheda Pagine Web

Evidenziando un contenuto attivo possiamo tramite le tre opzioni presenti a destra de-cidere quali azione Outpost deve applicare (vedi figura).

Sono quindi disponibili tre tipi di azioni per ogni tipo di contenuto attivo: con il flag su Abilitato sarà permessa l'esecuzione del contenuto attivo, con Chiedi sarà chiesto all'utente quale sia l'azione da intraprendere e con Disabilitato il contenuto attivo sarà bloccato da Outpost.

Se come opzione per un determinato contenuto attivo scegliamo Chiedi, durante la navigazione Outpost con la prima finestra pop-up ci chiederà di impostare le regole per il determinato host a cui stiamo accedendo. Vedi figura:

se mettiamo il flag su una delle prime due opzioni non ci verrà chiesto nient'altro poiché avremmo deciso in questo caso di permettere l'esecuzione del contenuto oppure di bloccarlo.

Se invece come opzione scegliamo Modifica Regole per Host, nel momento in cui carichiamo la pagina web potrebbe comparire una seconda finestra pop up che indica il tipo di contenuto attivo rilevato e ci chiede quale azione vogliamo eseguire. Vedi figura.

Nel caso specifico che ho riportato il contenuto attivo che viene rilevato è il JavaScript. In questa finestra possiamo scegliere diverse opzioni, che saranno poi applicate una volta premuto il pulsante OK. Vi riporto qui sotto il loro significato:

Permetti JavaScript da questo sito: il contenuto attivo del sito verrà eseguito.

Blocca JavaScript da questo sito: il contenuto attivo del sito verrà bloccato.

Flag Rendi l'impostazione sopra il default per questa opzione: se mettiamo la spunta su questa opzione i contenuti JavaScript saranno permessi per tutti gli host.

Permetti una volta: il contenuto attivo verrà permesso per una sola volta e se si ripresenterà ci sarà chiesto nuovamente di effettuare una scelta.

Blocca una volta: il contenuto attivo verrà bloccato per una sola volta e se si ripresenterà ci sarà chiesto nuovamente di effettuare una scelta.

Scheda Posta e News

Questa scheda presenta analoghe opzioni della scheda Pagine Web con la differenza che verranno applicate sulla visualizzazione dei contenuti attivi presenti all'interno delle e-mail.

Scheda Esclusioni

Personalmente ritengo che il nome di questa scheda non sia azzeccato in quanto non si tratta di una lista di host esclusi dalle impostazioni applicate per questo plug-in, ma semplicemente della lista di tutti quei siti che abbiamo visitato e di cui abbiamo deciso tramite le finestre pop-up di memorizzarne le impostazioni applicate la prima volta.

E' importante mettere il flag su Aggiungi siti web alla lista delle esclusioni durante la prima visita: in questo modo quando visiteremo per la prima volta un determinato sito le impostazioni che sceglieremo tramite le due finestre pop-up delle due figure precedenti verranno memorizzate su questa lista e saranno applicate in modo silenzioso la volta seguente che visiteremo il sito web. In questa scheda abbiamo la possibilità tramite gli appositi pulsanti che troviamo sulla destra di modificare le impostazioni per ogni singolo sito, di rimuovere il sito dalla lista e di aggiungerne manualmente uno senza doverci navigare.

Per modificare le impostazioni di un sito è sufficiente evidenziarlo e poi premere il pulsante Proprietà: comparirà un'altra finestra con le impostazioni che sono applicate per questo sito. Le impostazioni in grigietto sono quelle che avete stabilito di default, mentre quelle contrassegnate con il blu sono impostazioni che differiscono da quelle di default.

Quarantena allegati

È possibile fare in modo che determinati file allegati vengano o rinominati (flag Rinominala) o vengano segnalati come pericolosi all'utente (flag Riporta).

Di default sono previste determinate estensioni e l'azione prevista è quella di rinominare l'estensione (ad esempio *pippo.exe* in *pippo.exe.save*). E' possibile aggiungerne delle altre attraverso il pulsante Nuovo: nel primo campo si dovrà inserire l'estensione mentre nel secondo campo una descrizione dell'estensione o meglio del programma che utilizza file con quell'estensione.

A questo punto si dovrà stabilire, per l'estensione appena creata, che tipo di azione Outpost deve applicare. Il mio consiglio è quello di rinominare l'estensione stessa mettendo il flag su Rinominala.

Individuazione Attacchi

Questo plug-in serve, come dice il termine stesso, per prevenire o meglio per bloccare attacchi provenienti dall'esterno.

Outpost analizza tutti i pacchetti che provengono dalla Rete e, in base a quelle che si chiamano signatures, individua i pacchetti sospetti e blocca automaticamente l'IP dell'eventuale aggressore.

Nella scheda Allarmi consigliamo di posizionare su Massimo il livello di allarme e di mettere tutti i flag sulle opzioni presenti settando a 30 minuti il tempo di blocco dell'IP di un eventuale intruso.

Nella scheda Avanzato abbiamo tre parti che sono, rispettivamente, Lista Attacchi, Porte Vulnerabili ed Esclusioni.

Lista Attacchi

Qui tramite il pulsante Modifica lista... possiamo impostare quali tipi di attacchi Outpost deve individuare e bloccare. Il consiglio è quello di mettere la spunta su tutti i tipi di attacchi in modo d'avere una protezione più ampia possibile.

Porte Vulnerabili

Abbiamo la possibilità di inserire delle porte di sistema o solitamente utilizzate dai trojan che Outpost controllerà i modo più vigile per prevenire eventuali attacchi. Un esempio sarebbe quello di inserire la 12345 per il NetBus e la 27374 per il SubSeven.

Premete il pulsante Specifica per accedere alla finestra per l'inserimento delle porte da controllare.

Esclusioni

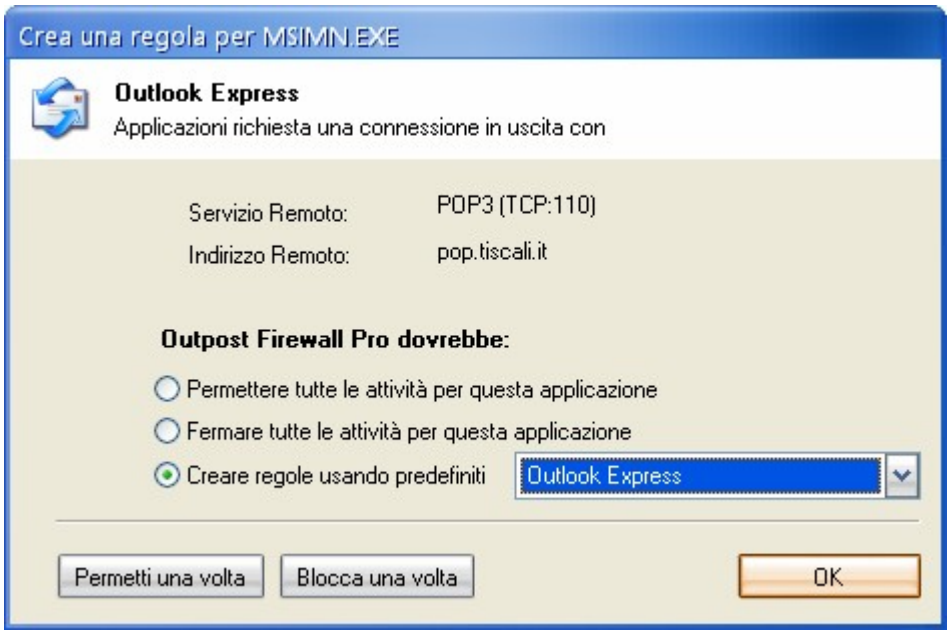
E' possibile inserire degli host o delle singole porte che Outpost considererà affidabili: fatte attenzione poiché una volta inserito l'host o la porta, Outpost considererà **lecito** tutto ciò che proviene da quell'IP o che transita su quella porta.

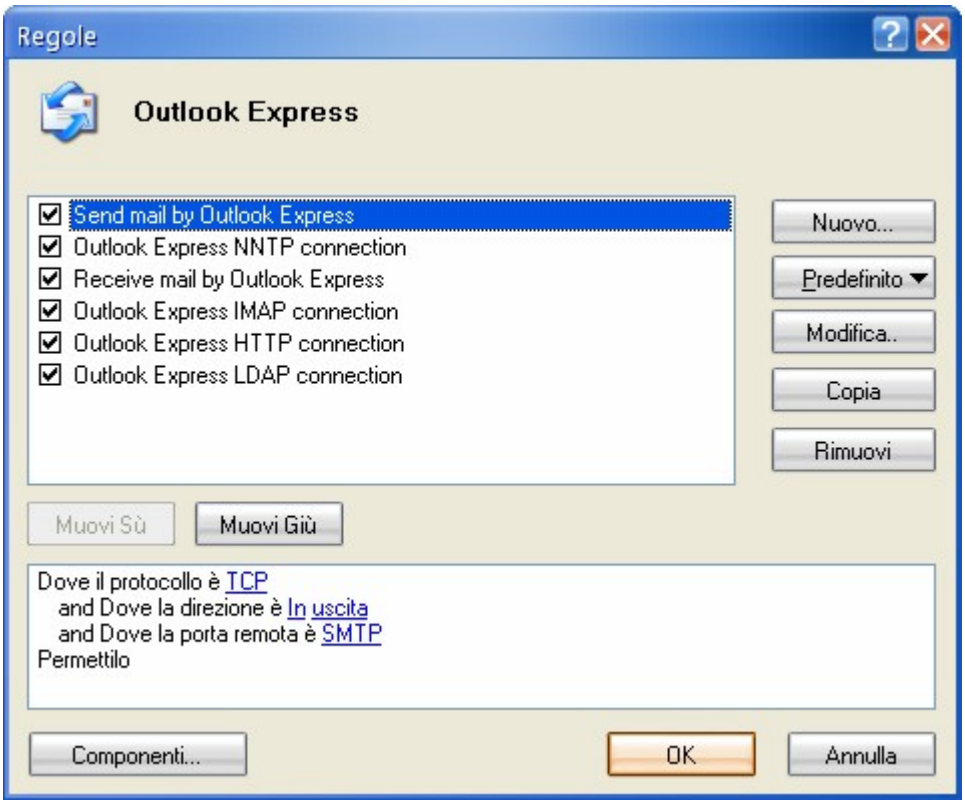
Una puntualizzazione è doverosa. Potrebbe capitare che durante uno scanning test di un sito non riusciate più a visualizzare la pagina di quel sito. Questo avviene perché l'IP dell'aggressore viene bloccato correttamente e quindi non è più possibile comunicare con quell'IP.
Se eventualmente vi rendete conto che non riuscite ad accedere ad un determinato sito potete in questo caso controllare il Visualizzatore Rapporti nella sezione Intercetta Attacco.

Esempio di configurazione per un client e-mail 4.1

Una delle applicazioni che richiedono accesso ad Internet più utilizzate (oltre al browser che abbiamo già avuto modo di vedere) è senza dubbio il client e-mail. Vediamo un esempio cu come configurare correttamente le regole per Outlook Express.

Nel momento in cui l'applicazione richiederà accesso alla Rete, se non esiste alcuna regola Outpost ci avviserà immediatamente, proponendoci di creare una regola preimpostata per l'applicazione:





basta premere OK ed il gioco è fatto... ma c'è una piccola considerazione da fare.

Se provate a controllare le regole che sono state create (scheda Applicazione -> Modifica -> Modifica regole) noterete che esse sono svariate (seconda figura nella pagina precedente).

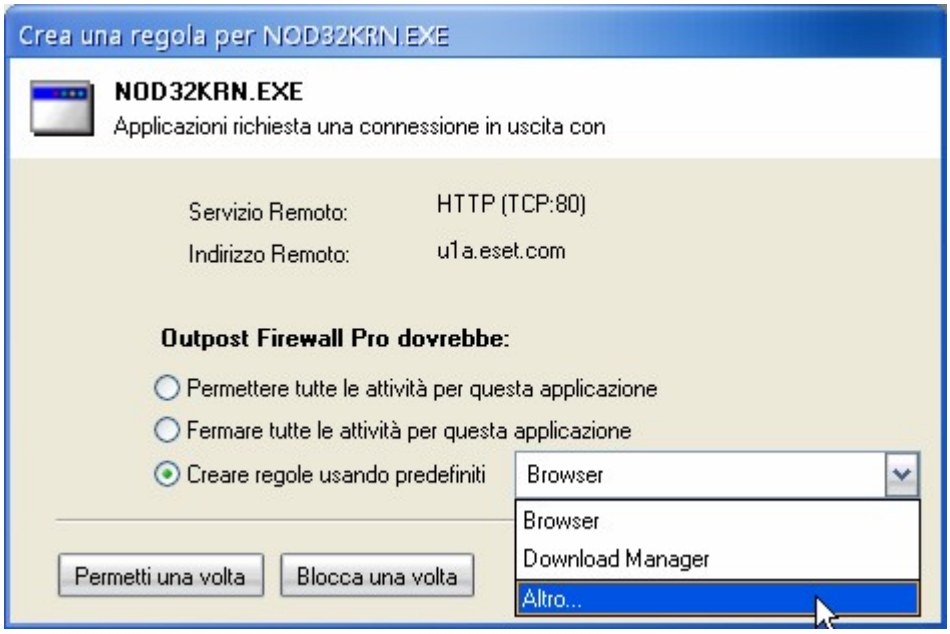
E' bene allora capire bene come utilizzate l'applicazione: se vi serve solo per spedire e ricevere posta (senza bisogno di autenticazione da parte del server) potete lasciare la spunta solo su Send mail by Outlook Express e Receive mail by Outlook Express: l'applicazione potrà quindi comunicare solo attraverso la porta **110** (per la ricezione delle e-mail) e la porta **25** (per l'invio delle e-mail). Le altre regole a cui toglierete la spunta saranno disattivate, ma potrete riattivarle nuovamente in caso di necessità: per il controllo della posta via HTTP (Outlook Express IMAP connection) e per le Newsgroup (Outlook Express NNTP e LDAP connection).

Conoscendo a priori il tipo di comunicazione che richiede l'applicazione, saremmo in grado anche di creare la regola adatta manualmente e senza essere connessi alla Rete. Possiamo sfruttare l'esempio del browser descritto alle pagg. 12-13, oppure semplicemente cliccare sul pulsante Aggiungi della scheda Applicazione, inserire Outlook Express (**msimn.exe**) ed impostare una regola predefinita per il client e-mail (Modifica -> Crea regole usando predefiniti -> E-Mail Client).

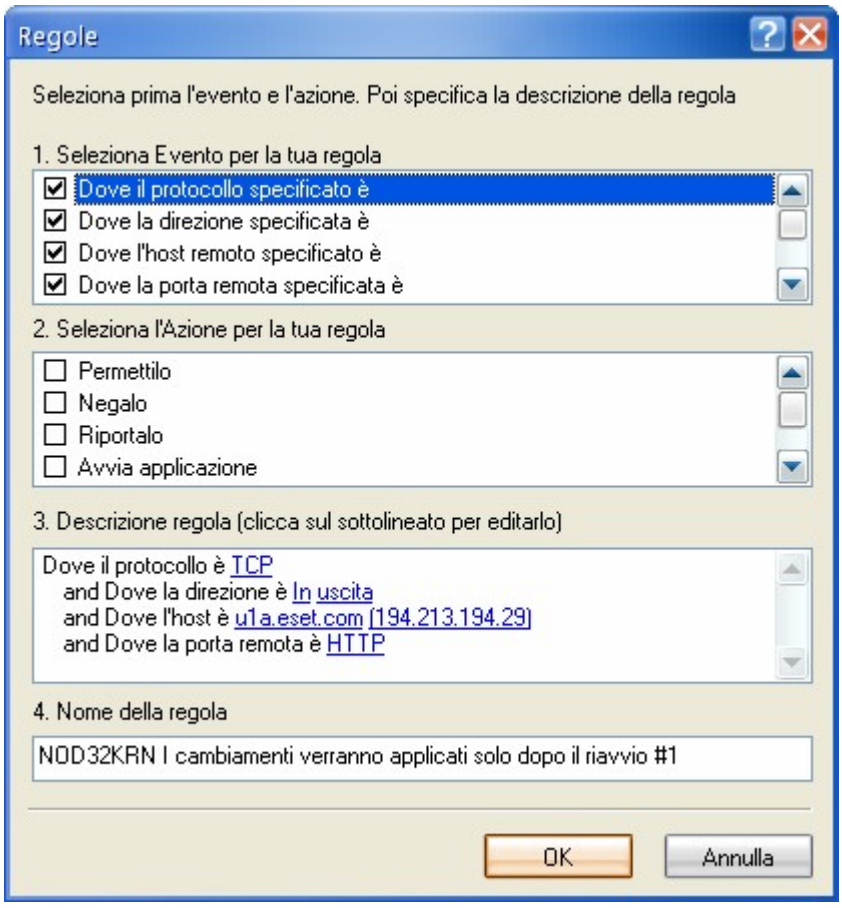
Esempio di configurazione di un'applicazione che richiede update periodici 4.2

Diverso invece è il discorso per applicazioni di cui non possiamo conoscere il tipo di comunicazione di cui necessitano (porta ed host remoto) a priori: in questo caso è sempre bene lasciare che sia il firewall a guidarci per la creazione di una regola precisa.

Nell'esempio che segue, riporto il tentativo di accesso ad Internet da parte del modulo **NOD32KRN.EXE**: si tratta di un componente dell'antivirus NOD32 il cui compito è quello di aggiornare periodicamente il database delle definizioni dei virus:



è facile evincere che il tentativo di connessione avviene verso l'host **u1a.eset.com**, sulla porta **HTTP** (**80**): considerata proprio la porta, Outpost propone, come regola predefinita, quella per i Browser e per i Download Manager: visto che l'applicazione in questione non è né l'una né tantomento l'altra, conviene fare clic su Altro (come in figura) per impostare una regola in modo manuale. Ci comparirà la finestra Regole che abbiamo già incontrato nei capitoli precedenti:



nel punto **3.** possiamo controllare l'esatta costruzione della regola: basterà quindi solamente darle un nome appropriato al punto **4.** , mettere la spunta su Permettilo (e su altre opzioni de lo desideriamo) al punto **2.** e premere OK: la nostra regola è registrata!

Nel caso specifico di NOD32, dopo questa prima connessione atta ad accertare la presenza o meno di aggiornamenti, in caso positivo il modulo richiederà un'ulteriore connessione per procedere al download del nuovo database. Basterà seguire lo stesso procedimento appena descritto e permettere la comunicazione.

Faccio notare anche che l'host remoto per il controllo ed il download degli aggiornamenti viene in genere scelto automaticamente da NOD32 tra alcuni indirizzi: durante gli aggiornamenti successivi, quindi, potrebbero essere richieste connessioni verso host diversi. Sta a voi decidere se modificare le regole in modo che diventino 'universali' per tutti gli host oppure se creare più regole precise (ovviamente la seconda soluzione sarebbe la più sicura, anche se la più dispendiosa in fatto di tempo e di pazienza).

In alternativa, potete scegliere di negare di volta in volta la connessione verso host diversi da quello impostato nella regola oppure settare il firewall su Blocca di più: in tal caso NOD32 continuerà i tentativi di connessione verso gli host della sua lista fino a raggiungere u1a.eset.com.

Cos'è e a cosa serve il Visualizzatore Rapporto 5.1

Il Visualizzatore Rapporto è una piccola utilità inclusa in Outpost che può essere avviata in due modi:

- scegliendo Visualizzatore Rapporto Outpost Firewall Pro dal menù Utilità;
- facendo clic sul pulsante  visibile nella barra principale.

Durante il suo funzionamento, Outpost compie una serie di operazioni e di azioni che vengono salvate in un apposito registro nel disco fisso. Il Visualizzatore Rapporto suddivide per categorie e per tipo di azione intrapresa tutte queste operazioni, permettendo all'utente di consultarle in qualsiasi momento. La visualizzazione delle informazioni avviene attraverso due pannelli.

Nel pannello di sinistra (Console percorso) nella maschera Percorsi, sono elencate le categorie in uno schema ad albero stile Gestione Risorse. Esse sono:

- **Controllo componenti**. Se è stato abilitato nelle opzioni del firewall, verranno fornite informazioni circa il controllo dei moduli delle applicazioni che tentano l'accesso ad Internet.
- **Plug-In**. Visualizza le azioni intraprese da ogni singola plug-in (blocco di siti web, di pubblicità, cookies, attacchi intercettati, ecc...).
- **Rapporto allarmi**. Fornisce informazioni dettagliate sugli attacchi intercettati provenienti dalla Rete.
- **Rapporto sistema**. Registra e visualizza la data di ogni avvio/chiusura del programma, di ogni modifica al tipo di protezione (Blocca di più, Regole Assistite, Permetti di più) e di ogni cambiamento apportato alla configurazione ed alle opzioni del programma.
- **Storico traffico bloccato**. Visualizza tutti i tentativi bloccati di accesso ad Internet da parte delle applicazioni installate nel computer.
- **Storico traffico permesso**. Visualizza tutti i tentativi permessi di accesso ad Internet da parte delle applicazioni installate nel computer.

Per una maggior rapidità di consultazione, è possibile aggiungere diverse categorie nella maschera Preferiti (un po' come si fa con gli indirizzi internet nei Preferiti del browser). Basta fare clic destro con il mouse sulla categoria desiderata e scegliere Aggiungi a preferiti....

Nel pannello di destra vengono visualizzate informazioni dettagliate relative alla categoria selezionata nella Console percorso. In genere è sempre fornita l'ora in cui è avvenuto un evento; quindi, a seconda della categoria, l'applicazione processata, l'IP verso il quale ha richiesto una connessione e l'azione intrapresa dall'utente, il tipo di attacco intercettato e l'IP da cui è partito, gli elementi attivi bloccati ed i siti nei quali erano contenuti, gli indirizzi internet più utilizzati, ecc....

Per facilitare la lettura del log in base alle proprie preferenze è possibile applicare dei filtri: basta fare clic sul pulsante Aggiungi filtri (*fig. 1/a*) presente sempre nel pannello di destra, in alto. Il procedimento per la creazione di un filtro è del tutto analogo a quello per le regole delle applicazioni: potrete visualizzare così il log relativo ad un'applicazione processata, ad un lasso di tempo specificato, ad un indirizzo IP, ad un evento, ecc.... Ovviamente il filtro che andrete ad aggiungere sarà valido solo per il tipo di categoria selezionata; sarà sempre visibile nel pannello di sinistra (Console percorso) nonché editabile e cancellabile in qualsiasi momento (con i pulsanti Edita filtri (*fig. 1/b*) e Rimuovi filtri (*fig. 1/c*) in alto nel pannello di destra).

fig. 1/a

fig. 1/b

fig. 1/c

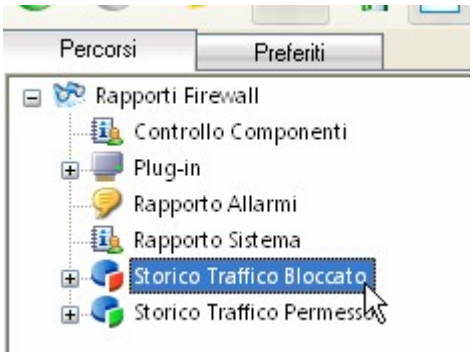

fig. 2

Infine, con il pulsante Esporta (*fig. 2*) nella barra principale del Visualizzatore, Outpost vi offre la possibilità di salvare le informazioni della categoria correntemente selezionata nella Console percorso in un file .LOG su disco fisso, consultabile semplicemente tramite il Blocco Note.

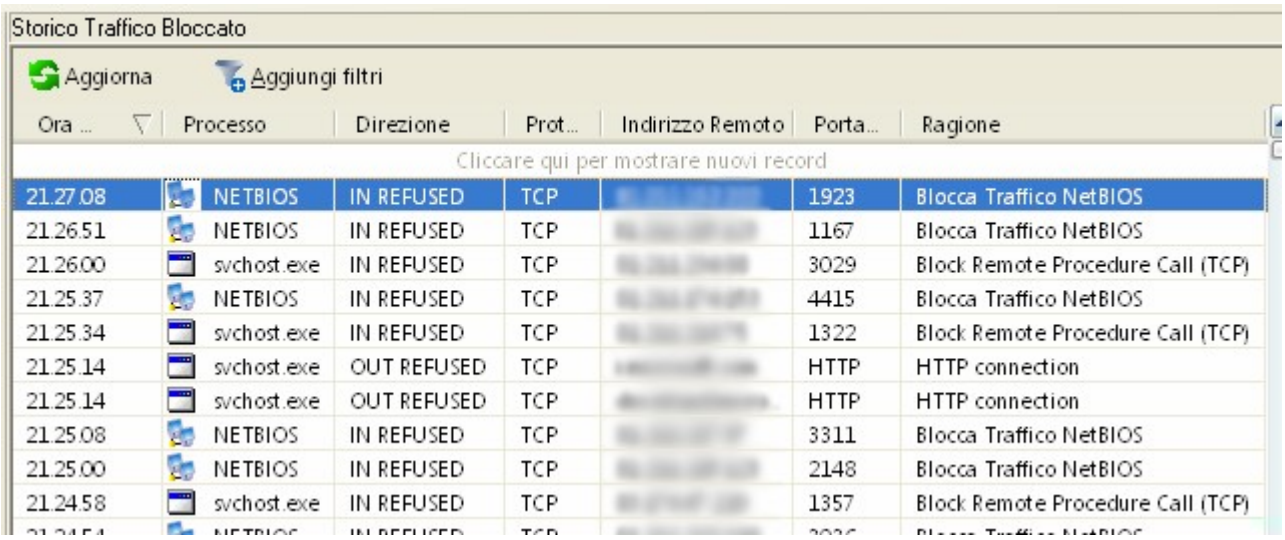
Esempi di lettura del Rapporto 5.2

Vediamo ora un paio di esempi su come si leggono e si visualizzano le informazioni del Rapporto.

1. Supponiamo di voler consultare le ultime applicazioni/processi a cui è stato impedito l'accesso da/al nostro computer (secondo le regole impostate). Nella Console percorso andremo quindi a cliccare sulla categoria Storico Traffico Bloccato così come di seguito mostrato:



conseguentemente, nel pannello di destra, il Visualizzatore riporterà le informazioni registrate per questa categoria (di seguito un'immagine di esempio, in cui sono stati opportunamente oscurati gli indirizzi IP).

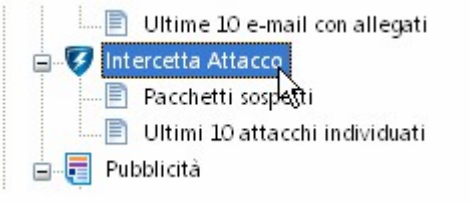


Prendiamo come esempio la prima riga, quella selezionata in blu. Possiamo evincere i seguenti dati:

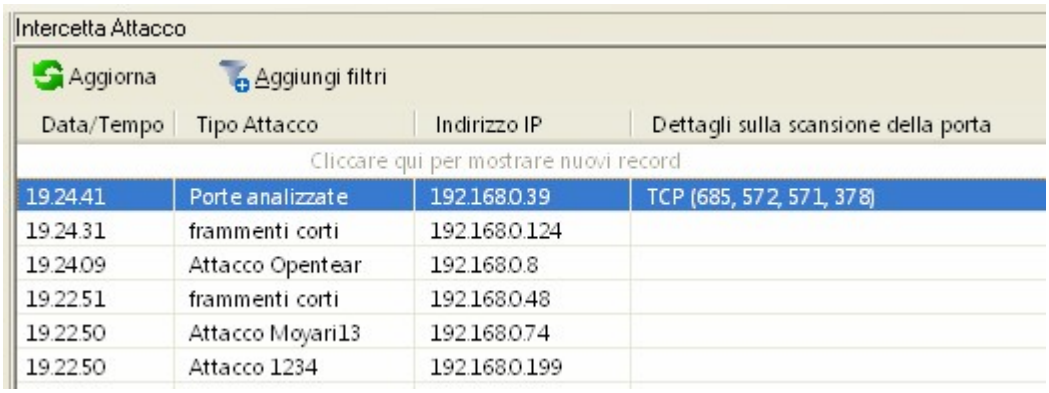
- **Ora d'inizio**. Il momento in cui si è verificato l'evento (21.27.08).
- **Processo**. Il processo o l'applicazione che ha posto in essere l'evento (connessione NetBIOS).
- **Direzione**. IN (proveniente dalla Rete) REFUSED (bloccato). OUT REFUSED indica il blocco di un evento dal nostro computer verso la Rete.
- **Protocollo**. Il tipo di protocollo riguardante l'evento (TCP/IP).
- **Indirizzo Remoto**. L'indirizzo IP dal quale/verso il quale proviene/è diretto l'evento.
- **Porta remota**. La porta remota dalla quale/verso la quale proviene/è diretto l'evento (1923).
- **Ragione**. Il motivo per il quale l'evento è stato bloccato (regola Blocca Traffico NetBIOS).

N.B.: facendo clic destro con il mouse sul titolo di una colonna, potete scegliere di visualizzarne altre (come Indirizzo Locale, Porta Locale, ecc...).

2. Supponiamo invece di voler visualizzare informazioni riguardanti gli ultimi attacchi intercettati dalla Rete: nella Console percorso dobbiamo in questo caso andare a selezionare la categoria Intercetta Attacco (vedi figura a destra) che è situata all'interno del gruppo Plug-in, (poiché è proprio una plug-in a svolgere questo compito).



Come nel caso precedente, nel pannello di destra verranno visualizzati subito i relativi dettagli. Nell'immagine di esempio che segue, il risultato dopo aver effettuato un test dal sito PC Flank.



Analizziamo anche questa volta la riga evidenziata in blu.

- **Data/Tempo**. Il momento in cui si è stato intercettato l'attacco (19.24.41). Nel caso in cui venga mostrata solo l'ora, la data è quella odierna; in caso contrario sarà visualizzata anche quest'ultima.
- **Tipo Attacco**. La metodologia utilizzata per tentare di portare un attacco al nostro computer. In questo caso, un portscanning (Porte analizzate).
- **Indirizzo IP**. L'indirizzo IP dal quale è stato lanciato l'attacco (in questo caso tutti gli indirizzi IP sono di PC Flank).
- **Dettagli sulla scansione della porta**. Questa colonna contiene l'elenco delle porte oggetto di scansione in caso di attacco portscanning. In questo caso le porte 685, 572, 571, 378.

Opzioni 'Ripara database' e 'Opzioni di pulizia' 5.3

Queste due opzioni possono essere scelte dal menù File del Visualizzatore Rapporto.

Ripara database consente di scegliere se il database contenente tutte le informazioni registrate debba essere riparato oppure sostituito con uno nuovo all'avvio del sistema operativo nel caso in cui sia danneggiato.

Opzioni di pulizia permette invece di impostare la dimensione massima su disco del database oltre la quale verrà effettuata la pulizia. I record vengono eliminati a seconda della loro 'vecchiaia' oppure della loro quantità: siete voi a dover scegliere. E' anche possibile impostare opzioni di pulizia differenti a seconda delle categorie. Se la casella Mostra allarmi è spuntata, una finestra di dialogo vi avviserà nel momento in cui sarà avviato il processo di pulizia.

I siti dove si possono effettuare i test 6.1

Una volta che avremo configurato e preso confidenza con Outpost Firewall sarebbe opportuno effettuare dei test su Internet in modo da verificare la reale affidabilità della nostra configurazione.

Ci sono alcuni siti web che offrono servizi per effettuare test sul nostro pc per verificare quanto esso sia vulnerabile agli attacchi provenienti dall'esterno. Di seguito ne riporto alcuni:

http://www.pcflank.com/
http://stealthtests.lockdowncorp.com/
http://www.it-sec.de/
http://scan.sygate.com/
http://www.securitymetrics.com/portscan.adp
http://www.jtan.com/resources/winnuke.html
http://bcheck.scanit.be/bcheck/
http://security.symantec.com/ssc/
http://www.t1shopper.com/tools/port-scanner/

Il consiglio è di effettuare i test su più di un sito, così da verificare la loro affidabilità: a volte può succedere infatti che i risultati di due o più test effettuati su diversi siti non corrispondano fra loro.

Inoltre è bene ricordare che quando si effettua un Trojan test, come ad esempio quello accessibile dal link http://www.pcflank.com/trojans_test1.htm, sarebbe opportuno che le porte analizzate risultassero invisibili:

3128	stealthed	Masters Paradise and RingZero	Trojan horses
12345	stealthed	NetBus	NetBus is one of the most widespread trojans
12348	stealthed	BioNet	BioNet is one of the most widespread trojan
27374	stealthed	SubSeven	SubSeven is one of the most widespread trojans

e **non** chiuse.

Trojan:	Port	Status
GiFt	123	closed
Infector	146	closed
RTB666	623	closed
Net-Devil	901	closed
Net-Devil	902	closed

Se malauguratamente le porte analizzate dovessero risultare **Closed** o peggio **Open** è bene che rivediate la vostra configurazione.

LE PORTE COMUNEMENTE UTILIZZATE DAI PROCESSI DI WINDOWS E DAI TROJAN 7.0

Qui di seguito riporto due tabelle con le porte utlizzate dai più comuni processi di Windows e dai trojan.

Faccio notare che molti trojan, se adeguatamente impostati da chi vuol farne uso, possono operare anche su porte differenti (anche su quelle solitamente utilizzate da un servizio): qui vengono riportate quelle di default.

Processo/Servizio	Porta
Sincronizzazione ora	13
FTP	20, 21
Telnet	23
SMTP (invio e-mail)	25
WhoIs	43
HTTP	80, 8080
POP (ricezione e-mail)	110
Servizio autenticazione	113
DCOM	135
NetBIOS (condivisione in LAN)	135-139
SMB (condivisione in LAN)	445
RPC – servizi diversi	1025 e seguenti
Firewall della connessione Internet (ICF)/Condivisione connessione Internet (ICS), Servizio gateway di livello applicazione (ALG), ClientDNS (Dnscache)	3001 e seguenti

Trojan	Porta/e
Deep Throat	41, 2140, 3150
Rasmin	531, 1045
Net-Devil	901, 902
SubSeven	1243, 6711-6713, 27374
Master's Paradise	3128, 3129, 40422-40426
Back Orifice	8787, 8879
NetBus	12345
BioNet	12348
NetSphere	30100-30102
Hack`a'Tack	31787-31791
ProRat *	5110

* **ProRat** è un tool di amministrazione remota molto sofisticato che, per le caratteristiche che ha, può essere considerato un trojan. Ha al suo interno una funzione che gli consente di disabilitare Windows Firewall oltre a molti altri di terze parti.
Molto pericoloso.

Link utili 7.1

Un'interessante pagina dedicata da Microsoft ai servizi di Windows e relative porte utilizzate:
http://www.microsoft.com/italy/technet/security/guidance/ref_net_ports_ms_prod.mspx

Sul sito PcFlank, che si occupa di sicurezza, sono consultabili invece due utilissimi database:

Porte (ricerca per numero di porta o per servizio)
http://www.pcflank.com/ports_services.htm

Trojan (ricerca per porta utilizzata o per nome)
http://www.pcflank.com/database.htm

CONCLUSIONI E CONSIDERAZIONI 8.0

Abbiamo redatto questa guida con lo scopo di fornire una traccia su come utilizzare al meglio Outpost Firewall Pro. A seconda delle idee, abitudini ed esperienze dell'utente, questa traccia può (anzi deve) essere riadattata per l'uso personale: non pretendiamo certo che quel che abbiamo scritto debba forzatamente andar bene per chiunque legga...

Ci rivolgiamo in particolar modo a quegli utenti che non sono così pignoli e restrittivi nella configurazione di un firewall e che non sono pazienti nel ricevere ed istruire finestre relative a componenti, contenuti attivi, applicazioni; a coloro che, per le loro abitudini ed esigenze, preferiscono allargare le maglie del firewall in modo che risulti meno invasivo possibile.

E' importante capire che un firewall complesso come Outpost va **scoperto**; non si possono intuirne e comprenderne tutte le funzionalità solo leggendo questa guida, ma è di fondamentale importanza **provare**, **sperimentare** di proprio pugno.
Seguire meccanicamente i procedimenti illustrati in questa guida è utile, ma non indispensabile: chiedetevi sempre il perché di una richiesta, di un avviso, di una finestra da parte di Outpost e, soprattutto, imparate a pensare agli effetti che avrà la vostra risposta o il pulsante che premerete. Vedrete che ben presto questo firewall non apparirà più così complicato!

Infine, un ringraziamento sentito è doveroso: va a **Michele Nasi**, direttore del sito www.ilsoftware.it.
Grazie al suo appoggio ed alla sua disponibilità abbiamo sempre potuto lavorare al meglio alla stesura di questa guida per poi renderla pubblica.

Gli autori

MaxZ - Rici