

## MANUALE ZONE ALARM - FIREWALL

Benvenuti nella guida del programma Zone Alarm, per chi non lo sapesse è un programma che viene usato per difendere il nostro pc da sguardi indiscreti, in sostanza controlla tutto il traffico in entrata e in uscita verso il nostro pc. Può essere usato per uso personale ed in questo caso è freeware, altrimenti ne esiste una versione per uso professionale ed in tal caso è a pagamento. Il sito ufficiale da cui scaricarlo è <http://www.zonelabs.com/>

All'avvio il programma si presenta con un interfaccia nella quale trovate nella prima scheda Overview (sguardo di insieme). Come vedete i nomi delle schede si trovano alla vostra sinistra nel riquadro arancione, cliccandoci potete accedere alla scheda desiderata. Accanto compare del testo esplicativo, potete nascondere cliccando su Hide text in basso, se invece cliccate su Reset to default tornate alle impostazioni che avevate prima di fare dei cambiamenti. In alto avete tre schede, cliccate su status, adesso al centro vi compare un riepilogo:

1. Blocked intrusion: (Intrusioni bloccate);
2. Inbound protection:(Protezione dei flussi di dati verso il pc), vedrete un scritta simile a questa >> **The firewall has blocked 4 attempts**, cioè il programma ha bloccato 4 tentativi;
3. Outbound intrusion:(Protezione dei flussi dal pc verso l'esterno);
4. E-mail protection:(Protezione e-mail);

### Product info

Adesso se andate nella scheda product info vi vengono date delle informazioni sulla versione del programma in Version information, sotto avete la possibilità di scaricare la versione pro come prova per 30 giorni, cliccando sul pulsante Try now. Se volete una guida direttamente on-line cliccate dove dice click here accanto alla scritta For on-line help self, mentre se volete registrare la copia cliccate su change register.

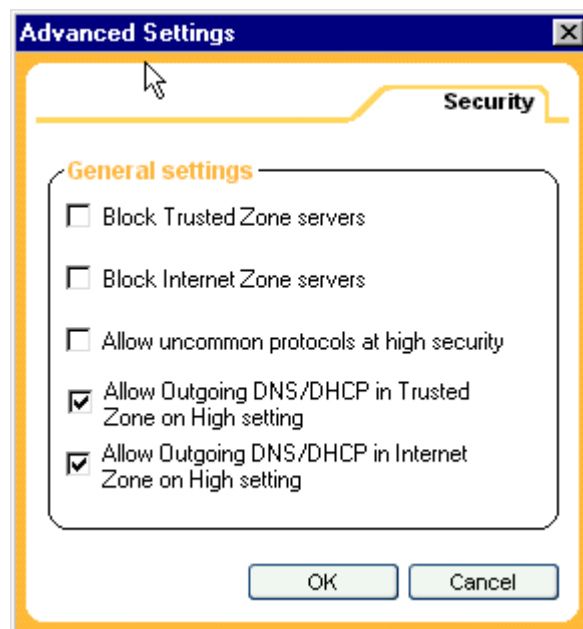
### Preferences

In alto dovete specificare se volete ricercare delle versioni aggiornate del programma automaticamente o manualmente, cioè automatically o manually, cliccando su check for update vi collegate ad internet per la ricerca. Se volete che Zone alarm venga sempre visualizzato in primo piano anche se avete altri programmi aperti allora cliccate su Show Zone alarm on top during internet activity. Mentre se volete che venga avviato insieme a window (scelta consigliata) allora spuntate Load zone on start up. Quando tornate ad un pannello (cioè firewall, overview, program control, etc..) potete anche visualizzare l'ultima scheda visitata in precedenza, dovete spuntare l'opzione Remember the last tabs visited in the panel. Se volete nascondere il testo che compare accanto ai pannelli allora accanto alla scritta, explanatory text within, dovete spuntare hide text altrimenti l'altra. In color scheme potete scegliere il colore dei pannelli, per la versione free c'è solo orange (arancione). Alle volte durante un avviso di zone alarm compare una finestra che vi dà la possibilità di richiedere informazioni aggiuntive attraverso il tasto more info, in questi casi potete fare in modo che prima che avvenga il

contatto con il sito di zone alarm vi venga visualizzata una finestra pop-up, e potete anche far nascondere il vostro ip quando possibile, dovete spuntare le due opzioni di sotto.

### **Pannello Firewall - MAIN**

Passate alla scheda main, adesso vi viene spiegato nel testo a sinistra che Alarm vi difende da traffico pericoloso tramite due zone, la internet zone e la trusted (fidata). La prima comprende i pc sconosciuti che sono collegati ad internet e che potrebbero entrare nel vostro pc, mentre la seconda riguarda i pc trusted (fidati) con i quali potete anche scambiare file, per esempio condividere documenti, stampanti, cartelle. Impostiamo prima la internet zone security, per default dovreste spostare la barra fino a High che è la configurazione consigliata, così il vostro pc è invisibile e non è permesso lo scambio di files, o condivisione di risorse con altri pc, per esempio non dovreste usare questa opzione quando state usando dei files sharing, tipo gnutella, napster, anche se a volte questi programmi permettono la modalità passiva nel trasferimento quindi delle funzioni sono permesse. Se impostate su medium gli altri computer possono vedere il vostro pc ma non condividere risorse, e gli attacchi net-bios sono bloccati, ovvio che low non è consigliata. Ora passate alla trusted zone security, qui potete impostare su high, però così il vostro pc è invisibile e non è consentito condividere risorse, per esempio se avete una rete lan, questa è formata da pc trusted cioè fidati, perchè appartengono alla vostra rete, e vorreste poter accedere alle stampanti sugli altri pc o intervenire a distanza per guasti, quindi dovreste posizionarvi su medium. Quindi la configurazione finale è high per internet zone e medium per trust zone. Adesso cliccate su advanced avrete questa scheda:



se avete una rete aziendale potete cliccare su Block trusted zone server, cioè bloccare quei programmi che richiedono di attivarsi come server per funzionare correttamente, per esempio chat program, mail client, browser per navigare, però alle volte sono programmati dagli hacker per accedere al vostro pc, cioè ad un certo punto voi avete sul pc dei programmi per navigare, per gestire la posta o per chattare non ci sono problemi, perchè vi verrà chiesto dal programma se volete dargli il permesso, potrete consentirlo perchè si tratta di programmi che senza il permesso non potrebbero

funzionare. Ma sul vostro pc potreste aver installato qualche programma realizzato da malintenzionati che una volta attivati come server possono fare della vostra macchina quello che vogliono, allora è meglio spuntare l'opzione così zone alarm li blocca automaticamente. La seconda opzione dovete spuntarla di sicuro perchè riguarda la internet zone. La terza opzione non la spuntate perchè riguarda il permesso da dare a quei protocolli di rete non comuni (quelli comuni sono tcp/ip, dns, udp, ed icmp, ed altri). Le ultime due potete spuntarle perchè riguardano le comuni comunicazioni che avvengono mentre siete collegati, attraverso le porte comuni, per esempio quando siete nella internet zone e siete collegati ad un sito la porta aperta è la 80, sul pc avete 65635 porte di comunicazione, in genere quando state scaricando la posta siete collegati alla 119, mentre alla 25 quando la state spedendo.

## **Add**

In questa scheda potete aggiungere dei siti o dei computer connessi in rete o anche una vostra sottorete ed una serie di ip alla vostra trusted zone, per scambiare risorse con essi. Se avete una Lan, rete locale, ogni pc collegato ha un suo host name, per sapere il vostro andate nel pannello di controllo e cliccate su rete, ora nella scheda identificazione potete inserire il nome host che è un nome che permette di ricordarvi più facilmente di un pc, per esempio pc per marketing, un altro potrebbe essere pc scambio posta, e sotto potete inserire una breve descrizione. Per impostare i dati per gli altri computer cliccate su add in zone alarm, ora scegliete host/sites, ora in host name inserite il nome host e sotto la descrizione. Se volete potete anche aggiungere una serie di ip che contraddistinguono la vostra rete, in genere in caso di rete si ha un ip statico cioè non cambia mai durante i collegamenti, cliccate su add e scegliete ip address, adesso inserite le 4 cifre che formano un indirizzo ip, e continuate così fino ad aggiungere tutti gli ip che volete siano aggiunti alla zona trusted (cioè sicura). Per fare un altro esempio, se avete impostato la zona internet come high e quella trust come medium in sostanza per gli altri pc collegati ad internet siete invisibili nel senso che voi potete connettervi ad essi sfruttando la porta 80 o anche per scaricare la posta se si tratta del vostro provider, ma loro non possono entrare nel vostro pc, mentre i pc della vostra eventuale rete d'ufficio possono condividere le risorse se avete impostato come medium la zona trusted. Però potreste voler usare dei programmi tipo napster durante i quali vi possono fare la richiesta di scaricare da una cartella del vostro pc delle canzoni, in questi casi il pc host che sta tentando di farlo riceve un rifiuto perchè il vostro firewall lo reputa tentativo di ingresso, allora conoscendo il suo host (che in genere viene visualizzato dal programma napster o simili con accanto l'ip) potete inserirlo con il tasto add, e scegliere host. Oppure Immaginiamo di avere degli amici amministratori di un sito con ip statico, e di voler condividere delle risorse con loro possiamo aggiungere il loro ip nella trusted zone sempre al solito modo. In genere per conoscere l'ip, il nome host di un pc collegato ad internet basta per esempio digitare in ms-dos il comando Tracert <http://www.nomesito> e premere invio, vi dirà tutto il tragitto per arrivare a comunicare con quel sito e alla fine vi darà il nome del sito, il nome host ed il suo ip.







## **Program controls - MAIN**

Ponete program control su medium, così ogni volta che un programma vuole accedere ad internet vi verrà chiesto il permesso tipo: "Do you allow internet explorer access to the internet?" e voi rispondete yes, poi sotto spuntate remember this answer, così in futuro non vi verrà più richiesto in quanto se I.E è il programma che usate spesso per collegarvi diventa fastidioso che ogni volta ve lo chieda, fate lo stesso col programma

per chattare o per scaricare la posta. C'è da dire che il messaggio di sopra riguarda i programmi che vogliono accedere ad internet ma ce ne sono di altri che chiedono l'accesso come server, allora il messaggio potrebbe diventare "do you allow front page access as act server?" e rispondete se si o no. Sotto in automatic lock spuntate on così il lucchetto al pc verrà inserito automaticamente mentre per esempio sono passati tot minuti di inattività o si è attivato lo screen saver. Cliccate su custom, ora dovete specificare se il lucchetto deve essere impostato quando lo screen saver è attivo, seconda opzione, oppure quando sono passati tot minuti di inattività (durante i quali non muovete nemmeno il mouse). Ora potete decidere se i programmi ai quali avete dato il permesso in precedenza, possono accedere a internet o se tutte le attività sono bloccate. Cioè quando ogni volta vi viene fatta la domanda se consentire o meno ad un programma di accedere, se rispondete yes quel programma potrebbe anche accedere ad internet durante il lucchetto (cioè blocco delle attività) oppure potete decidere che niente possa accedere.

## Programs

In questa scheda avete il riepilogo dei permessi o dinieghi che avete attribuito ai programmi. Ecco una tipica situazione:

Programs ▲	Access		Server		
	Trusted	Internet	Trusted	Internet	
 Download Accelerator	?	?	?	?	
 Internet Explorer	✓	✓	?	?	
 Microsoft Word for	?	?	?	?	
 Outlook Express	✓	✓	?	?	
 WS_FTP 95	✓	✓	?	?	

il segno ? vuol dire che ogni volta vi viene chiesto se consentire o meno l'accesso, mentre la V vuol dire che ha il permesso e la X non può accedere, ovvio che potete cambiare la situazione cliccando sul simbolo col sinistro del mouse e scegliere fra allow (consenti), block (blocca) e ask (chiedi), potete impostare sia per la colonna access (accesso ad internet) che per server(programmi che funzionano come server). Pannello alert and logs Zone alarm vi avvisa con delle finestre quando vi deve chiedere il permesso per un programma ma anche quando ci sono tentativi di accesso dall'esterno, in questo caso potrebbe diventare fastidioso ricevere il solito suono che il programma emette in questi casi allora impostate su off nella scheda alert events shown. Adesso cliccate su advanced, se volete che zone alarm registri tutto giornalmente in un log file spuntate la prima opzione, ora sotto dovete cliccare su browse per stabilire dove si trova il file log, in genere in c:\windows\internetlogs. Per cancellarlo premete delete logs, mentre sotto impostate su tab l'opzione in modo che il log venga mostrato nel formato di default. Nell'ultima scheda e-mail protection spuntate su on, così sarete protetti da eventuali allegati di posta maligni.