

ZONEALARM

ZoneAlarm é um Firewall que provê segurança para qualquer computador que seja conectado à uma rede-local ou , e principalmente, à Internet. Isso é mais verdade ainda para aquelas conexões do tipo ADSL ou cable modem (TV à Cabo). ZoneAlarm protege contra programas maliciosos, tipo Spyware e Trojans (Cavalo-de-Tróia), permitindo que o usuário controle os tráfego de e para a Internet, e como as aplicações acessam a Internet.

ZoneAlarm's **Dynamic Firewall** bloqueia tentativas de conectar seu computador pela Internet. **High Security Level** faz com que seu computador fique invisível para a Internet (ou Rede Local) deixando assim de ser um alvo para hackers e invasores. **Security levels** é o modo mais indicado para configurar seu firewall, sem requerer de você conhecimentos maiores sobre protocolos e portas.

Quando alguma aplicação - de dentro de seu computador - tentar acessar a Internet, ZoneAlarm se assegura de ter a **sua permissão**. Assim nenhum programa conseguirá enviar dados de seu computador para a internet, à não ser aqueles que você autorizar.

ZoneAlarm aparece como um painel em seu desktop, como na figura abaixo. Você também poderá interagir com o ZoneAlarm usando o **Desk Band Toolbar**.



1.0 PRINCIPAIS CARACTERÍSTICAS

1.1 O Internet Lock

O denominado ZoneAlarm's Internet Lock controla se os dados podem trafegar entre seu computador e a Internet ou a Rede Local. Ligando a "trava" para as aplicações que estiverem rodando em seu computador de enviar e receber dados, para ou da Internet ou Rede Local.

Para ligar ou desligar a trava, pressione o botão **LOCK**.

1.2 A Automatic Lock

A trava **Automatic** liga a trava quando você não estiver usando o computador, ou não estiver acessando a Internet. Você pode configurar ZoneAlarm para ligar automaticamente a trava quando seu screen saver for ativado, ou após um período de inatividade.

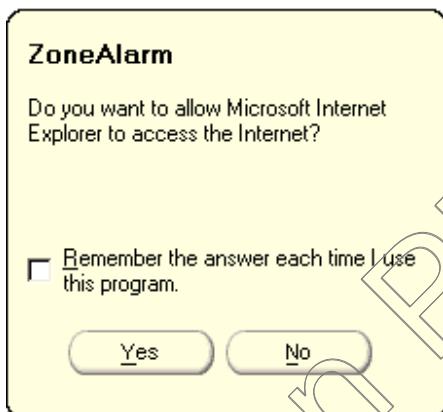
ZoneAlarm permite optar por dar a uma aplicação a permissão para bypassar a Trava. Por exemplo para permitir que um programa de e-mail possa checar mensagens mesmo quando o acesso à Internet estiver trancado para todas as demais aplicações.

1.3 Zona Local e Zona Internet

ZoneAlarm divide a rede em duas zonas: a Zona Local e a Zona Internet. A Zona Local consiste dos computadores da Rede Local, que estejam conectados ao seu computador. A Zona Internet inclui todo o restante do mundo (a Internet) que não esteja em sua Zona Local.

ZoneAlarm permite setar os níveis de segurança independentemente na Local Zone e na Internet Zone, permitindo conexões com serviços confiáveis na Internet, ao mesmo tempo que mantém todo o restante da Internet fora de seu computador.

1.4 Permissões do Programa



Quando um programa tenta acessar a Internet pela primeira vez, **ZoneAlarm vai perguntar** se você deseja que ele acesse realmente a Internet. Selecionando "Yes" permite que o programa acesse a Internet **até que você encerre** tal programa; Selecionando "No" nega tal acesso **até que você encerre** tal programa.

O **modo de acesso default à Internet** para todas as aplicações é solicitar sua permissão a cada vez que você rodar o programa.

Checando a opção "Remember answer" a aplicação receberá ou não tal acesso à Internet sem solicitar a cada vez a sua permissão para tal. Isto é útil para as aplicações, como seu browser ou seu e-mail, que você sempre necessita usar para acessar à Internet. Você pode alterar tais **configurações de acesso** indo no painel **Programs**.

O painel **Programs** permite especificar diferentes permissões de acesso para cada programa em cada Zona. Por exemplo, você pode querer que um programa de FTP acesse totalmente a Internet, mas restringir seu programa de e-mail para a Local Zone.

Program		Allow connect	Allow service
Microsoft Outlook	9.0.2416	Local: ✓ · · Internet: · ✗ ·	<input type="checkbox"/>
WS_FTP 95	6.0.1.1	Local: ✓ · · Internet: ✓ · ·	<input type="checkbox"/>

1.5 Atividade de Servidor

ZoneAlarm permite que você **detecte e controle programas que trabalhem como Internet server** - tais programas ficam no estado de **LISTENING** para requisições vindas de outros computadores. A maioria dos Trojans agem como servidores, esperando por instruções vindas de clientes remotos (dos hackers).



O painel **Programs** destaca as aplicações que estão escutando a Internet com o símbolo de uma mão segurando o ícone de tais programas.

O painel **PROGRAMS** permite que você escolha quais programas são permitidos agir como servers. ZoneAlarm negará acesso à Internet, e mostrará uma janela popup, quando um programa sem permissão de agir como um server começar a escutar ativamente alguma conexão.

Aplicações de Comunicação como o ICQ, ou o NetMeeting, requerem direitos de servidor para poder funcionar adequadamente com o ZoneAlarm.

1.6 Alertas do Firewall

Quando o firewall bloqueia comunicações da Internet ele mostra uma janela de Alerta, para seu conhecimento do bloqueio efetuado.

O padrão é o ZoneAlarm uma notificação de Alerta na forma de uma janela pop-up amarela. Este Alerta contém a origem, o destino, o protocolo, a porta, a data e a hora da comunicação bloqueada. No caso da comunicação bloqueada for para fora do micro, o Alerta irá incluir qual foi a aplicação que foi bloqueada.

Os Alertas **podem ser logadas** num arquivo texto for ser checados posteriormente, e para reportar as tentativas hacker bloqueadas. Podem-se desligar as notificações de Alerta.

1.7 ZoneAlarm MailSafe - Email Attachment Protection

ZoneAlarm **intercepta anexos do tipo Visual Basic Script** em e-mails que você recebe enquanto ZoneAlarm estiver rodando e isola tais anexos, e você é avisado ANTES de pensar em executar tais anexos.

Scripts anexados são programas que podem causar dano aos seus arquivos no computador, violando sua privacidade, ou infectando outros computadores com vírus perigosos. Exemplos disso inclui os recentes vírus "Love Letter" e o "Funny Joke".

ZoneAlarm MailSafe na verdade não deleta esses scripts, porém protege seu PC de danos através da identificação dos scripts e permitindo que você escolha cancelar o script antes dele poder rodar.

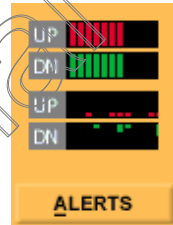
ZoneAlarm MailSafe é ativado por default mas pode ser habilitado ou desabilitado no Painel **Security**.

O copyright do produto pertence à empresa **Zone Labs, Inc.** Este material foi baseado em partes do Help On-Line do programa **Zone Alarm**, e foi adaptado e formatado pelo consultor **Francisco Panizo Beceiro.**

Não é, nem pretende ser um substituto ao Help original, porém é de extrema valia para todos os iniciantes, e para aqueles com poucos conhecimentos da língua inglesa.

2.0 O PAINEL ALERTS

As barras vermelhas mostram dados sendo enviados para fora de seu micro (upload) para a Internet enquanto a barra verde mostra dados sendo recebidos (download). A diferença entre os dois conjuntos de barras é que o conjunto superior mostra o tráfego atual; o conjunto de barras inferior mostra um histórico dos últimos segundos de tráfego pela conexão.



Para visualizar o painel de Alertas expandido, clique no botão **Alerts**.



O painel de Alertas expandido mostra um sumário das atividades da Internet e os alertas desde que o ZoneAlarm foi executado:

- o total de dados enviados (sent) e recebidos (received), por todas as aplicações;
- uma lista dos Alertas Atuais, com a opção de submeter o alerta para o Alert Analyzer;
- a opção de Log Alerts e das Notificações de Alerta.

Current Alerts mostra as seguintes informações: o endereço IP, porta, protocolo e a data e a hora da tentativa de conexão; uma curta mensagem descreve se o Alerta é uma comunicação incoming ou outgoing, e possivelmente a aplicação que causou o alerta.

Se você desejar traçar o endereço IP de alguma conexão bloqueada do tipo incoming, você pode usar ou um **whois** ou um **traceroute** para encontrar o dono do endereço IP utilizado.

Se em **logging the alerts**, o log é arquivado no arquivo ZALog.txt na pasta de instalação do ZoneAlarm, numa pasta chamada Internet Logs. O tamanho do log é mostrado próximo do nome do log, e o log pode ser deletado quando você achar apropriado, evitando assim que se torne muito grande.

As entradas do Log têm a seguinte aparência:

```
"FWIN,2000/03/07,14:44:58,-8:00 GMT, Src=192.168.168.116:0, Dest=192.168.168.113:0, Incoming, ICMP"
```

FWIN indica que o firewall bloqueou uma conexão incoming para o seu computador. Essa entrada também inclui a seguinte informação:

- Data e Hora
- Endereço IP de origem e o número da porta
- Endereço IP de destino e o número da porta
- indicação se o transporte foi através de TCP, UDP, ICMP, ou IGMP

```
"FWOUT,2000/03/07,14:47:02,-8:00 GMT,QuickTime Player Application tried to access the Internet. Remote host: 206.80.6.45:53"
```

FWOUT indica que o firewall bloqueou uma conexão inbound para o seu computador. Essa entrada também inclui a seguinte informação:

- Data e Hora
- Endereço IP de origem e o número da porta
- Endereço IP de destino e o número da porta
- indicação se o transporte foi através de TCP, UDP, ICMP, ou IGMP

```
"PE,2000/03/22,17:17:11 -8:00 GMT,Netscape Navigator application file,206.80.6.45:53"
```

A entrada "PE" informa que uma aplicação em seu computador tentou acessar a Internet. Essa entrada também inclui a seguinte informação:

- Data e Hora
- A aplicação do seu computador que tentou acessar a Internet
- O endereço IP e o número da Porta que a aplicação estava tentando se conectar.

3.0 O PAINEL LOCK

O painel LOCK é um botão que permite se parar os acessos à Internet por aplicações normais. Clicando em **lock** altera o acesso de **off** para **on** e vice-versa.



Quando a trava está aberta e a barra timer está **verde**, o acesso à Internet está permitido e aberto.

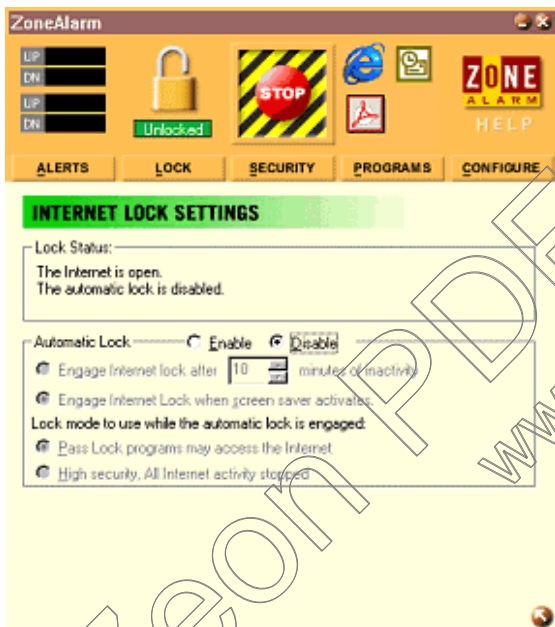
Se a barra timer mostrar um contador de tempo, este significa o tempo restante antes do **automatic lock** ser ativado.



Quando o acesso à Internet estiver bloqueado, a trava se mostrará fechada. A barra timer muda para **vermelho** e o timer mostrará quanto tempo já se passou desde que a trava foi fechada.

Para visualizar o Painel **Lock Expandido** clique sobre o botão **Lock** sob a barra timer.

Quando expandido, o painel de configuração LOCK permite configurar como se deseja que a **Automatic lock** opere.



Você pode escolher travar o acesso à Internet de forma automática quando o **screen saver** se ativar ou após um **período de inatividade na Internet**.

Se o acesso à Internet for bloqueado pela ativação do **screen saver**, ele será desbloqueado assim que o screen saver for desativado.

Entretanto se o Automatic Lock for disparado por **período de inatividade**, você terá que clicar no botão **Lock** para desbloquear o acesso à Internet.

O **Lock Mode** pode ser configurado para que programas "**Pass Lock**" possam acessar a Internet. Esta configuração permite que certos programas possam acessar a Internet, tais como clientes de e-mail, para que eles possam checar e-mails enquanto todas as demais aplicações continuam bloqueadas.

O modo **High Security** PARA toda atividade de acesso, para todas as aplicações, independentemente da configuração dos programas.

4.0 O BOTÃO STOP

Pressionando o botão **STOP** cessa imediatamente **TODO o tráfego Internet**. Pressione esse botão se você imaginar que um programa pode estar sendo usado para acessar a Internet, nesse momento, de modo suspeito e não autorizado.

O botão STOP para com todo e qualquer acesso à Internet, independentemente da configuração **Pass Lock** existente no painel **Programs**. Muito útil para parar um Trojan ou outro programa que esteja para ganhar acesso à suas informações privadas.



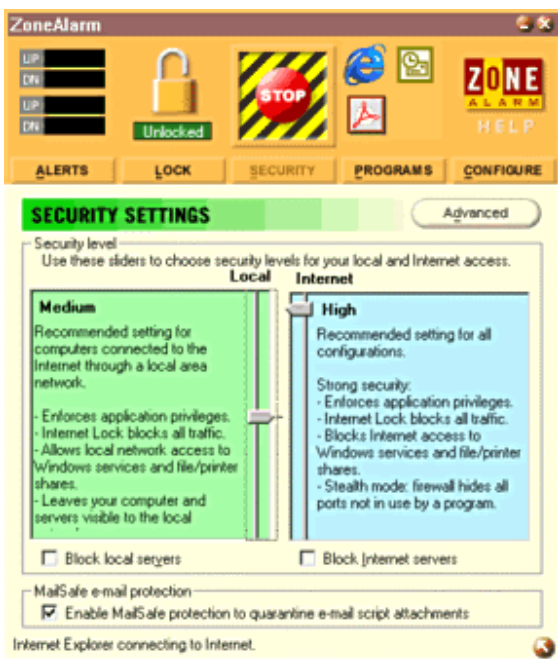
Para **reativar** o acesso à Internet pressione novamente o botão **STOP**.

Note que ao usar o botão de emergência serão cortados completamente **todas as conexões** com a Internet. Conexões e dados sendo transferidos por qualquer programa em seu computador, terão que ser posteriormente reinicializadas.

5.0 O PAINEL SECURITY

O **painel Security** mostra o nível de segurança e as permissões gerais de servidor para as Zonas Local e Internet.

ZoneAlarm divide os computadores em duas zonas: a Local Zone e a Internet Zone. A Local Zone inclui computadores que estão conectados ao seu através de uma LAN (Local Area Network) A Internet Zone inclui tudo na Internet que **não** esteja na Local Zone.



Cada zona tem um seletor **security level**, permitindo que se possa selecionar um diferente nível de segurança para cada uma. As configurações default são **medium** para a Local Zone e **high** para a Internet Zone. Com o incremento dos níveis de segurança, o **firewall dinamicamente coloca mais restrições de acesso** para o seu computador, protegendo você de ameaças potenciais.

O **block servers checkbox** para cada zona permite que se previna contra a tentativa de qualquer programa agir como servidor para aquela zona. Checando esta opção, nenhuma aplicação terá permissão de ficar na escuta de conexões entrantes para tal zona - mesmo se tiver checada a opção "Allow Server" no **Programs panel**. Isto permite que o usuário bloqueie, temporariamente, toda a atividade de servidores para essa zona,

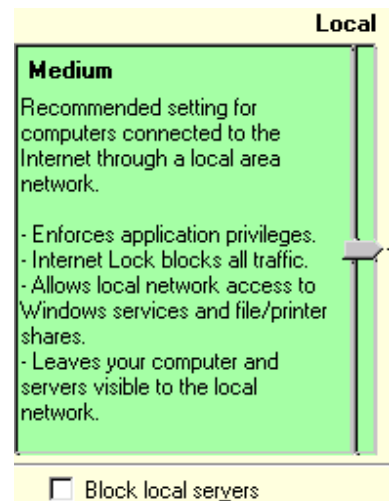
sem que se necessite modificar as configurações de forma permanente.

Atenção: o nível de segurança da Internet Zone deve ser **igual ou superior** ao nível selecionado para a Local Zone.

5.1 Local Zone

O padrão para a Local Zone é **Medium**. As opções possíveis são as seguintes:

- **Low (baixa)** - Define privilégios de aplicações e de Internet Lock somente. Deixa seu computador visível aos outros computadores da Local Zone. O firewall não bloqueia compartilhamento de arquivos ou impressoras ou o tráfego **para e desde** a Local Zone.
- **Medium (média)** - **O padrão para a configuração da Local Zone**. Compartilhamento de Arquivos e Impressoras, além de serviços do Windows são permitidos para computadores pertencentes à Local Zone. A trava automática é incrementada pelo firewall que bloqueia todas as portas. O computador é visível para a Local Zone.
- **High (alta)** - **Alta segurança e flexibilidade de aplicação**. O firewall bloqueia o acesso de dentro da Local Zone para o Windows (serviços NetBIOS) além do compartilhamento de Arquivos e Impressoras. Seu computador fica no Modo Stealth (Invisível): todas as portas, não usadas por um programa durante sua execução, são bloqueadas e não são visíveis para a Local Zone. Este modo automaticamente abre as portas somente quando um programa aprovado necessita delas.

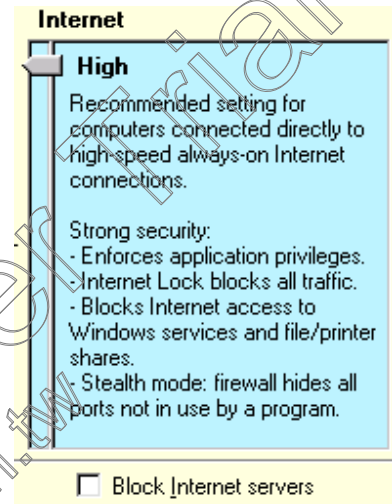


Por default, nenhum computador pertence à Local Zone. Veja na seção 5.3 como adicionar computadores à sua Local Zone de confiança.

5.2 Internet Zone

O padrão para a Internet Zone é **High**. Como na Local zone, o aumento do nível de segurança implica em maiores restrições. As opções possíveis são as seguintes:

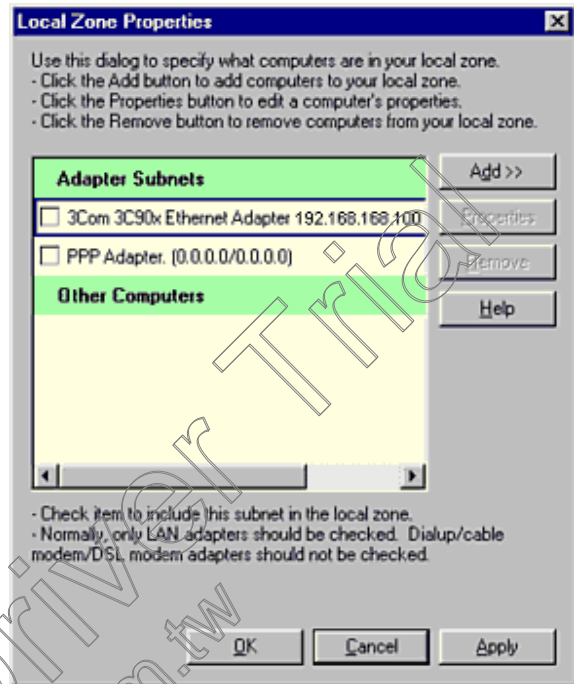
- **Low (baixa)** - Define privilégios de aplicações e de Internet Lock somente. Deixa seu computador visível aos outros computadores da Internet Zone. O firewall não bloqueia compartilhamento de arquivos ou impressoras ou o tráfego **para e desde** a Internet Zone.
- **Medium (média)** - Compartilhamento de Arquivos e Impressoras, além de serviços do Windows são permitidos para computadores pertencentes à Internet Zone. O firewall bloqueia o acesso da Internet Zone para o Windows (serviços NetBIOS). A trava automática é incrementada pelo firewall que bloqueia todas as portas. O computador é visível para a Internet Zone.
- **High (alta)** - **O padrão para a configuração da Internet Zone.** O firewall bloqueia o acesso de fora, da Internet Zone, para o Windows (serviços NetBIOS) além do compartilhamento de Arquivos e Impressoras. Seu computador fica no Modo Stealth (Invisível): todas as portas, não usadas por um programa durante sua execução, são bloqueadas e não são visíveis para a Internet Zone. Este modo automaticamente abre as portas somente quando um programa aprovado necessita delas.



5.3 Propiedades Advanced Zone

A caixa de diálogo **Advanced Properties** permite expandir o alcance de sua Local Zone. Permite que você configure a segurança da Internet Zone num nível mais alto, mas permitindo ainda que computadores selecionados possam se conectar com o seu computador em seu nível de segurança Local Zone.

A seção **Adapter Subnets** lista todos os seus adaptadores de rede e de dial-up. Checando um adaptador automaticamente adiciona todos os outros computadores dessa subnet local à local zone. Se a sua rede for uma pequena LAN, isto automaticamente adicionará todos os computadores de seu grupo à sua local zone.



Se o seu computador é parte de uma **Local Area Network (LAN)**, você tem que colocar uma marca próxima da network adapter cards sob **Adapter Subnets**. Isto garante que você terá acesso aos recursos necessários da sua Local Area Network.

Nota importante para usuários de Cable modem: Se você usa uma placa de rede, conectada diretamente a um cable modem para sua conexão à Internet, você deverá deixar as subnets do cabo desmarcadas, para prevenir que seus vizinhos fiquem habilitados a acessar o seu computador.

A caixa de diálogo **Advanced Zone Properties** permite adicionar outros computadores à sua Local Zone. Pressionando o botão **Add** permite escolher adicionar um host (ou site) por nome, um endereço IP, uma faixa de endereços IP, ou uma subnet IP.

Host/Site Adiciona um nome de computador a sua Local Zone. Você deverá digitar o nome do computador, e poderá entrar ou um nome no estilo domain-style name (tal como "ftp.zonelabs.com") ou um nome Windows-style (tal como "FTPSERVER").

IP Address Adiciona um único endereço IP que se refere a um único computador a sua Local Zone.

IP Range Adicionando uma faixa de IP adiciona uma série de endereços IP consecutivos a sua Local Zone.

IP Subnet Adiciona uma subnet a sua Local Zone. Útil em escritórios onde a Local-Area Network seja dividida em múltiplas subnets. Por exemplo, se a impressora da rede está numa subnet diferente do seu computador, a Dynamic Firewall bloqueará o acesso à impressora. Adicionando a subnet da impressora, à sua Local Zone permite que você utilize a impressora da rede desde o seu computador, tanto quanto quaisquer outros computadores da subnet da impressora.

6.0 O PAINEL PROGRAMS



O painel **Programs** provê um indicador **visual** das mais recentes aplicações que acessaram/acessam a Internet. O painel Programs mostra um ícone piscante para uma aplicação que esteja recebendo ou enviando dados da Internet. Um servidor (na verdade uma aplicação servidora) que esteja **listening** é indicada por uma mão sob o ícone.

Clique no botão Programs para visualizar o painel expandido de Program.

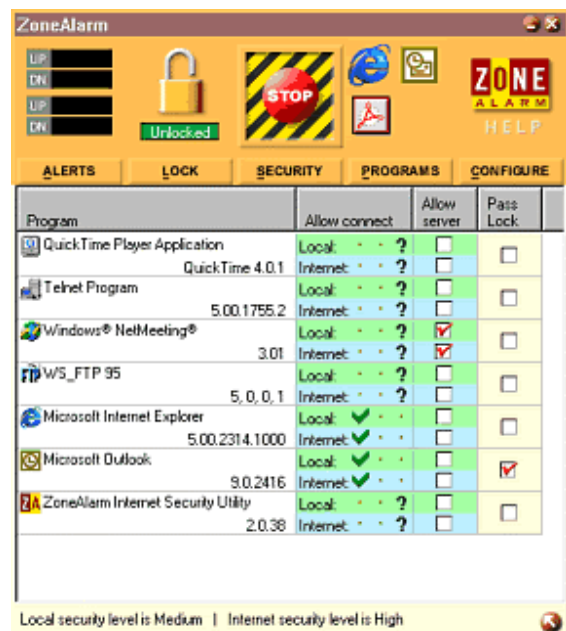
O painel program contém uma lista de todos os programas que já tiveram, ou tentaram, acesso à Internet. Você pode rever e reconfigurar cada direito de acesso, para cada programa na sua **Local Zone** e/ou na **Internet Zone**. Os checkboxes **Allow server** permitem que você controle quais aplicações podem executar funções de servidores.

A coluna **Pass Lock** permite você decidir se uma aplicação pode conectar-se mesmo se a trava lock estiver ligada. Qualquer aplicação da lista pode ser **removida**.

6.1 A Lista de Programas

Sob a coluna **Program**, ZoneAlarm mostra o nome e a versão do programa. Deixando o cursor do mouse pousado sobre uma aplicação mostrará:

- Nome do Produto;
- O nome do arquivo usado para acessar a Internet;
- A localização do arquivo;
- Versão do Produto;
- Data de Criação e tamanho do arquivo.



6.2 Direitos de Acesso

A coluna **Allow Connect** mostra cada direito de acesso de cada aplicação para cada uma das zonas. Para alterar os direitos de acesso, clique num dos três botões na coluna Allow Connect:

- A marca **green check** permite um programa se conectar sempre, sem necessitar de sua confirmação a cada vez. Se você permitir que um programa sempre conecte-se à Internet Zone, ZoneAlarm também permitirá que o programa sempre se conecte à Local Zone.
- O **X vermelho** previne acesso à Internet até você alterar para uma check mark ou uma question mark (marca de interrogação). Se você nega acesso de uma aplicação à Local Zone, ZoneAlarm não permitirá também que tal programa acesse a Internet Zone. A Internet Zone não pode possuir direitos de acesso superiores ao da Local Zone.
- A **question mark** (marca de interrogação - que é a configuração default) alertará você e te pedirá permissão a cada vez que um programa tentar acessar a Internet.

Programas não podem ter direitos de acesso maiores à Internet zone do que a definida para a Local zone. Por exemplo, um browser não pode ter acesso à Internet zone se ele não possuir direitos de acesso à Local zone.

	Allow connect	Allow server
Local:	✓ . .	<input type="checkbox"/>
Internet:	. X .	<input type="checkbox"/>
Local:	✓ . .	<input checked="" type="checkbox"/>
Internet:	. . ?	<input type="checkbox"/>

6.3 Allow Server

ZoneAlarm controla as aplicações servidoras. Tais aplicações ficam escutando por requisições de conexão externas (incoming connection requests) e respondem à essas requisições. Com o ZoneAlarm você pode limitar as aplicações servidoras de serem acessíveis.

Um exemplo é quando você executa uma aplicação que precisa de aceitar conexões entrantes, você será apresentado a opção de permitir essa aplicação de agir como servidora. Aplicações de comunicação, tipo ICQ e NetMeeting, tipicamente requerem direitos de servidoras para conseguir funcionarem propriamente sob o ZoneAlarm. ZoneAlarm identifica tais aplicações logo em seguida à sua execução, permitindo que você temporariamente assinale direitos delas agirem como tal.

A maioria dos Trojans (trojan horse ou Cavalos de Tróia) são, de fato, aplicações servidoras que permitem a hackers controlar seu computador remotamente. ZoneAlarm dá a você controle dessas aplicações, permitindo que você especifique quais podem agir como um servidor. Para um maior controle, ZoneAlarm deixa que você indique se um servidor pode se comunicar com a Internet Zone, ou se ele é restrito à Local Zone. Se uma aplicação, em seu computador, tentar responder à uma requisição remota, sem a sua prévia permissão, ZoneAlarm detectará tal comportamento e emitirá um aviso para seu conhecimento.

6.4 Pass Lock

Checando a check-box **Pass Lock** permite que um programa bypassse a **Automatic Lock**.

Program	Allow connect	Allow server	Pass Lock
Norton AntiVirus Utilities 6.0.2.22	Local: . . ? Internet: . . ?	<input checked="" type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Outlook 9.0.2416	Local: ✓ . . Internet: . . ?	<input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/>

Use esta característica para permitir programa de e-mail checar novos e-mails mesmo quando o acesso para todas as zonas estiver bloqueado.

Se um de seus programas gerar erros ligados a uma conexão Internet, é possível que ele tenha tentado acessar a Internet quando a Automatic Lock tenha sido acionada. Se você desejar permitir isso, tenha certeza de checar o checkbox Pass Lock.

6.5 Remoção de Programa e Menu Local

Para **remover um programa da lista** clique com o botão direito do mouse e selecione a opção **Remove**.

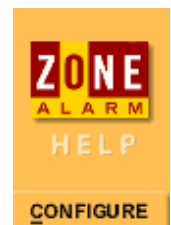
Program	Allow connect	Allow server	Local Network
Microsoft Internet Explorer 5.00.2314.1000	Local: . . ? Internet: . . ?	<input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> Allow <input checked="" type="checkbox"/> Disallow <input type="checkbox"/> Ask <input type="checkbox"/> Allow server
ZoneAlarm Internet Security Utility 2.0.8	Local: . . ? Internet: . . ?	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> Allow <input checked="" type="checkbox"/> Disallow <input type="checkbox"/> Ask <input type="checkbox"/> Allow server
Norton AntiVirus Utilities 6.0.2.22	Local: . . ? Internet: . . ?	<input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> Allow <input checked="" type="checkbox"/> Disallow <input type="checkbox"/> Ask <input type="checkbox"/> Allow server
Microsoft Outlook 9.0.2416	Local: ✓ . . Internet: . . ?	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> Allow <input checked="" type="checkbox"/> Disallow <input type="checkbox"/> Ask <input type="checkbox"/> Allow server

Remover um programa da lista não previne ZoneAlarm de monitorá-lo. ZoneAlarm irá detectar o programa na próxima vez que ele tentar acessar a Internet.

Você também pode alterar os direitos de acesso de um programa à Internet usando esse menu (clcando com o botão direito do mouse, como indicado na figura abaixo).

7.0 O PAINEL CONFIGURATION

Clicando no logotipo **ZoneAlarm** traz a você a página **ZoneAlarm's Online Information**. Lá se encontram links para o ZoneAlarm help file, frequently asked questions, e para o Zone Labs Support and ZoneAlarm News.



Clique no botão **Configure** para visualizar o painel de configuração expandida. Esse painel Configuration permite que se configure como o ZoneAlarm deve trabalhar.

ZoneAlarm's **version number** e o TrueVector service version number são mostrados. O driver TrueVector deve estar carregado para que o ZoneAlarm possa trabalhar adequadamente.



ZoneAlarm pode alertar de qualquer atividade da Internet abrindo uma **popping window** sobre qualquer janela do Windows que estiver aberta. Você habilita esse comportamento checando o checkbox "On top during Internet activity".

A configuração default habilita que o ZoneAlarm seja carregado a cada vez que um boot for dado no computador. Esta característica pode ser desabilitada se for desmarcado o checkbox "Load ZoneAlarm at startup". Fazendo isso entretanto fará com que apenas os programas carregados **após a execução do ZoneAlarm** sejam efetivamente controlados.

8.0 A BARRA DE FERRAMENTAS DESK BAND TOOLBAR



ZoneAlarm pode ser minimizado como uma "docking toolbar", o que permite uma referência visual rápida da atividade da Internet. Acesso rápido ao ZoneAlarm com mínimo espaço de tela perdido.

Para **restaurar** a janela principal do ZoneAlarm, clique o botão ZoneAlarm na toolbar.

Quando o acesso à Internet for bloqueado com o High Security, o botão central **STOP** mudará para um botão **GO verde**. Clicando no botão **GO** novamente restaura o acesso à Internet.

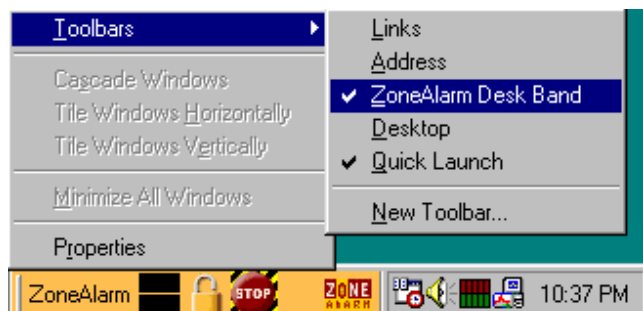
Se o **Automatic Lock** foi acionado o ícone **Lock** mostrar-se-á com um **X vermelho** sobre ele. Clique sobre o ícone **Lock** para travar / destravar o acesso à Internet.



Se o **Automatic Lock** foi acionado o ícone **Lock** mostrar-se-á com um **X vermelho** sobre ele. Clique sobre o ícone **Lock** para travar / destravar o acesso à Internet.

Ativando a Desk Band

No Windows 98, Windows 2000 ou qualquer Windows com o Internet Explorer 4 Shell Update, clique com o botão direito do mouse sobre a Barra de Ferramentas do Windows e selecione "Toolbars" (ou então "Barra de Ferramentas") e então "ZoneAlarm Desk Band".



Quando rodando sob o Windows 95 ou Windows NT 4.0 sem o Internet Explorer 4 Shell Update, vá até o **Painel de Configuração** e clique em "Show shell toolbar" para ativar a Desk Band toolbar. Note que nesta configuração, a pequena toolbar pode apenas flutuar pelo desktop e em muitos casos poderá cobrir ícones no system tray.

O nome da Desk Band pode ser removida clicando com o botão direito sobre o nome, e deselecionando a opção Show Title. Você poderá então alterar o tamanho da Desk Band movendo o lado esquerdo em relação ao lado direito.

9.0 KEYBOARD SHORTCUTS (ATALHOS DE TECLADO)

O teclado pode ser utilizado para acessar quase todos os comandos do **ZoneAlarm**. Abaixo um pequeno resumo dos comandos que podem ser acessados através de simples combinações de teclas:

Ctrl+L	Trava / Destrava
Ctrl+S	Parada de Emergência
Ctrl+H	Zone Labs Information Overview
Alt+A	Expande/Fecha o Painel Alerts
Alt+L	Expande/Fecha o Painel Lock
Alt+S	Expande/Fecha o Painel Security
Alt+P	Expande/Fecha o Painel Programs
Alt+C	Expande/Fecha o Painel Configure
Alt+Z	Zoom/Unzoom -- Expande/Fecha o painel atual
ESC	Unzoom -- Fecha o painel aberto
F1	Acessa o arquivo de Ajuda (Help File)
PgUp	Alerta Aberto Anterior
PgDn	Alerta Aberto Seguinte
Home	Primeiro Alerta Aberto
End	Último Alerta Aberto