Configure seu firewall com o Guarddog

Cão de guarda

O Guarddog, um programa do KDE, promete um "firewall fácil" no Linux com uns poucos cliques. Mais importante: auxilia usuários inexperientes a proteger seus computadores – ou mesmo redes inteiras – contra os perigos da Internet. POR HOLGER JUNGE

Os subsistemas ipchains (kernel Linux 2.2) e iptables (kernel Linux 2.4 e 2.6) configuram o kernel do Linux para agir como firewall. Entretanto, sua operação por linha de comando pode parecer um tanto "cifrada" para neófitos do Linux. Em meio a essa confusão, Simon Edwards desenvolveu o Guarddog [1] para tornar as coisas mais fáceis. O Guarddog é uma ferramenta gráfica de configuração e manutenção de firewalls. Protegida sob a licença GPL, roda tanto no KDE 2 como no KDE 3.

A versão estável mais atual (2.4.0) saiu em dezembro de 2004 e pode ser obtida em [2]. Como os nossos testes foram feitos antes dessa data, experimentamos com as versões 2.2.0 (estável) e 2.3.2 (desenvolvimento). Além dos códigos fonte, o site possui binários prontos para o Mandrake e o SuSE. Há binários para o Red Hat também, mas apenas para a versão 2.2.0. Há também a indicação de um repositório APT para o Debian Woody com a versão 2.2. Se você usa Debian Sarge ou Sid, os repositórios oficiais da distribuição possuem, respectivamente, as versões 2.3.2 e 2.4.0. Usuários do Sarge que preferirem instalar a versão instável em lugar da disponível para o Sid devem estar cientes dos prós e contras mencionados no quadro "Aos Corajosos".

O Guarddog foi projetado para o usuário doméstico, seja em uma única máquina ou em uma pequena rede local. Embora as distribuições mais importantes como Conectiva, Red Hat, Mandrake e SuSE possuam suas próprias ferramentas gráficas para montagem de firewalls, tais ferramentas padecem de uma certa dose de granularidade – em outras palavras, costumam ser "oito ou oitenta". Alguns usuários precisam de uma configuração simples de fazer, mas um pouco mais detalhada. O Guarddog pode ser a ferramenta ideal para isso.

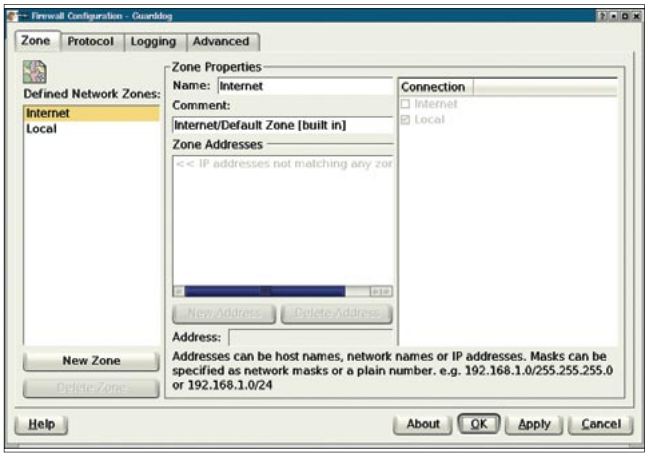

Figura 1: A interface gráfica do Guarddog depois de iniciado. Observem as duas zonas pré-configuradas, *Internet* e *Local*.

Figura 2: A aba *Protocol* permite informar ao firewall quais protocolos deve liberar e quais bloquear. O usuário não precisa se preocupar com números de porta e outros bichos.

Armadilhas de Segurança

Os usuários inexperientes precisam ter bastante cuidado ao montar um firewall. A facilidade com que a "empurração de mouse" habilita e desabilita opções pode estimular – erroneamente! – o usuário a deixar mais portas abertas do que o necessário. No outro extremo, é bem fácil criar uma muralha tão intransponível que deixaria alguns serviços importantes inacessíveis.

Além disso, o Guarddog é um programa do KDE e não deve ser rodado em uma máquina servidora, que muitas vezes roda apenas em modo texto. É preferível usar o Guarddog em uma máquina cliente para gerar a configuração do firewall e, depois, copiar o script resultante para seu servidor dedicado.

Como o Guarddog é baseado em ipchains ou iptables, os usuários precisam certificar-se de que os módulos apropriados do kernel estão disponíveis no servidor. Muitas distribuições encarregam-se automaticamente disso. Na remotíssima possibilidade de a sua não tomar essas providências, será necessário recompilar o kernel para incluir os módulos de ipchains ou iptables.

O Guarddog usa comandos de filtragem que levam em conta os protocolos dos pacotes em trânsito. os usuários não precisam se preocupar com os números de porta, o que evita erros de configuração. É possível ainda determinar grupos de máquinas – as chamadas zonas – o que permite, entre outras coisas, criar redes periféricas, as chamadas Zonas Desmilitarizadas (DMZ).

A interface

O Guarddog deve ser executado com privilégios de superusuário (root) para que o programa possa colocar imediatamente as novas regras de filtragem em ação. A figura 1 mostra o Guarddog no momento em que é chamado. Infelizmente, a GUI não é muito intuitiva em alguns pontos. O Guarddog possui quatro abas: a guia *Zone* permite que os usuários agrupem máquinas em zonas.

Em *Zone properties* (propriedades da zona) deve-se digitar os endereços IP (únicos ou em faixas) para a zona. Há duas já configuradas, uma delas chamada de *Internet* e a outra de *Local*. Nenhuma delas pode ser apagada. A zona *Internet* automaticamente inclui qualquer endereço IP que não faça parte de nenhuma outra zona. Já a zona *Local* compreende os endereços da rede interna. Uma máquina sozinha ficará contente apenas com essas duas zonas.

Pode-se usar a aba *Protocol* (ver figura 2) para permitir ou bloquear protocolos específicos. A estrutura em árvore à direita organiza os protocolos por categoria. Sem sombra de dúvida, o DNS é o primeiro serviço que você deverá permitir; ele está na categoria *Network*. Ao ativar a opção *DNS - Domain Name Server* aparecerá uma marca para indicar a liberação do serviço. Para aplicar as alterações, pressione o botão *Apply* (aplicar). Um segundo clique na opção mostra um X, indicando que o firewall irá, explicitamente, rejeitar qualquer conexão que use o protocolo. Se nenhuma marca estiver aparecendo, o firewall simplesmente bloqueará o tráfego baseado nesse protocolo.

Além do DNS, você pode precisar (ou, melhor dizendo, certamente precisará) de HTTP, HTTPS (HTTP seguro), FTP (presente na categoria *File transfer*) e os protocolos de email SMTP e POP3 (na categoria *Email*).

"Fichando" protocolos

A aba *Logging* (ver figura 3) permite que configuremos o Guarddog para registrar eventos no sistema *syslog*. Isso pode ser usado para, por exemplo, detectar "crackers" varrendo suas portas em busca de falhas. O Guarddog pode ajustar a taxa de verificação (*logging rate*) para limitar a bagunça criada por eventos do firewall nos logs do sistema. É importante impor um limite para isso; do contrário, seu computador pode ser derrubado por Negação de Serviço (DoS

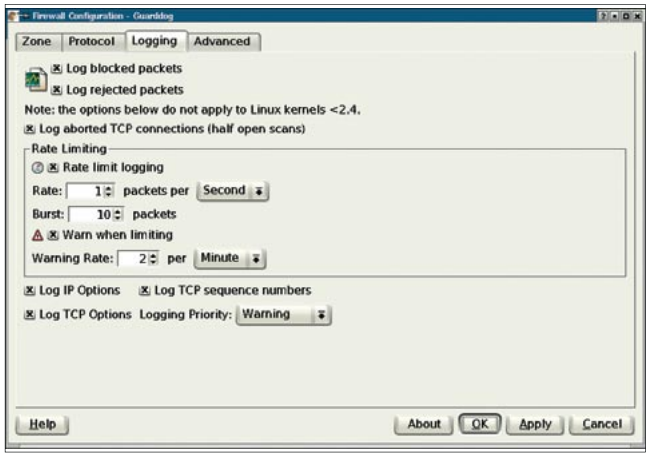

Figura 3: Os administradores podem usar a aba *Logging* para especificar o tipo de registro de eventos (log) que o firewall deve fazer.

– Denial of Service). Uma enxurrada de pacotes IP malformados poderia rapidamente abarrotar os arquivos do syslog e sobrecarregar seu disco rígido.

Se, por algum motivo qualquer, for preciso um nível maior de detalhe sobre os pacotes IP e TCP que entram, é possível ativar a opção de mostrar o fluxo de dados na parte de baixo da tela.

A aba *Advanced* (avançado – ver figura 4) oferece opções avançadas para ajuste fino do firewall. É de especial interesse para administradores experientes. Se algo der errado, não entre em pânico: clique em *Restore to factory defaults...* (restaurar valores iniciais) para usar os padrões do software. Os padrões para *Local Dynamic Port Range* também são suficientes na maioria dos casos. Elas especificam a faixa de portas que o Linux pode usar para iniciar conexões de dentro para fora da rede.

Se algum protocolo não estiver listado na aba *Protocol*, é possível clicar em *New Protocol* (novo protocolo) e digitar o nome, o transporte usado (TCP ou UDP) e as portas usadas por ele.

O Guarddog possui um útil recurso de importação e exportação dos scripts de firewall. É possível, por exemplo, exportar as regras já criadas para um script simples em shell e armazená-lo em */etc/rc.firewall*. Como não é comum servidores rodarem o ambiente KDE, os administradores podem, simplesmente, pressionar o botão *Export* para criar o script. Depois, basta copiá-lo para o servidor e rodá-lo.

Uma porta para o mundo

Nem sempre os firewalls Linux são usados para proteger apenas a máquina em questão. Pelo contrário, é comum usar sistemas Linux como parte da estrutura de segurança de redes inteiras. Nesse caso, o computador rodando Linux funciona como um "porteiro" – o chamado *gateway* – e possui duas interfaces (placas) de rede: uma voltada para a Internet, a outra conectada à rede interna. (ver figura 5). É bastante simples configurar o Guarddog para o papel. A única ressalva: isso só funciona com iptables, por isso é necessário kernel 2.4 ou 2.6. Será preciso configurar o mascaramento de IP *antes* de usar o Guarddog para gerar as regras do firewall. Embora o Guarddog não possa auxiliá-lo nesse passo, seu primo Guidedog pode [4].

O primeiro passo é criar uma nova zona no Guarddog para a rede local. Para isso, clique em *New Zone* na aba *Zone*. Qualquer nome serve – LAN, por exemplo. Depois clique em *New Address* para configurar os endereços IP, que podem ser únicos, faixas ou redes inteiras (como, por exemplo, *192.168.1.0/24*).

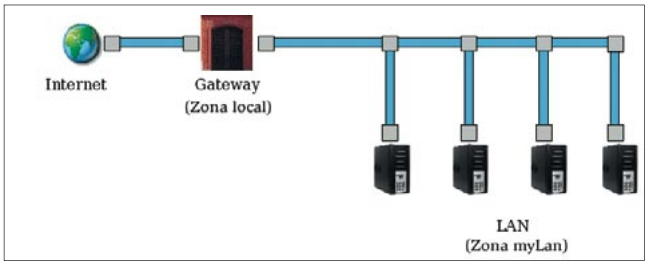

Figura 5: O computador rodando Linux e atuando como firewall também é um gateway para a rede interna acessar a Internet.

Agora clique em *Internet* e *Local* sob o ramo *Connection* para certificar-se de que a zona LAN está conectada à Internet e à máquina local. Na aba *Protocol* escolha *Internet* e habilite (ou bloqueie) os protocolos apropriados na coluna LAN. Finalmente, clique em *Apply* para armazenar as regras no script */etc/rc.firewall* e ativar o firewall. ■

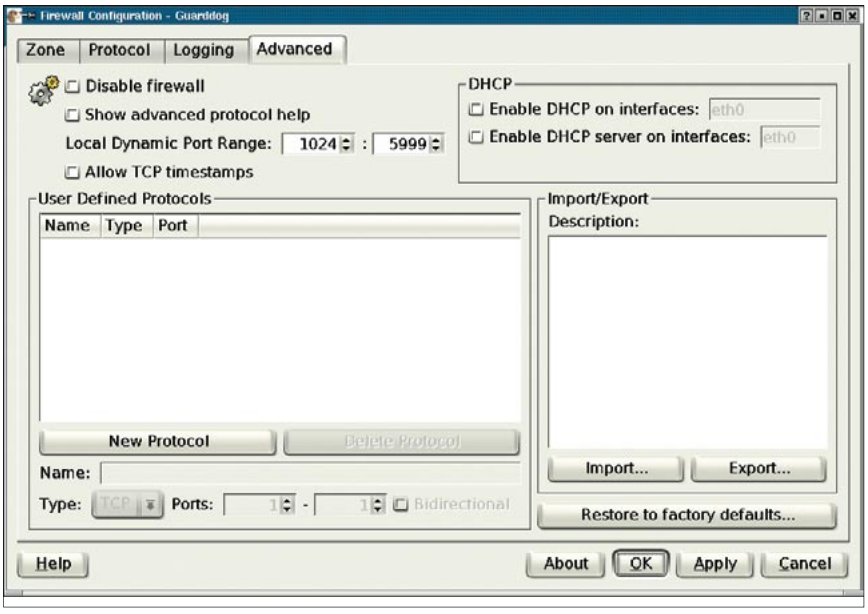

Figura 4: O Guarddog permite que muitos detalhes do firewall sejam configurados. Por exemplo, é possível definir novos protocolos e importar ou exportar scripts.

Aos Corajosos

Apesar da versão estável ser a 2.4.0, muitas distribuições (como a Debian Sarge) ainda disponibilizam apenas a versão instável anterior, a 2.3.2. Há alguns problemas em usar essa versão em ambientes de produção. Há, é claro, vantagens em relação à 2.2, como a definição, pelo usuário, de protocolos desconhecidos. Há também o suporte ao kernel 2.6, recurso ausente no Guarddog 2.2, e a adição de muitos protocolos novos como RSync, Distcc, GKRellm, Bittorrent, Servidor de Chaves PGP, Jabber sobre SSL e o Microsoft Media Server. Todas essas vantagens podem ser usufruídas também com o Guarddog 2.4.0, portanto desaconselhamos o uso da versão instável.

INFORMAÇÕES

[1] Página oficial do Guarddog: *http://www.simonzone.com/software/guarddog*

[2] Download do programa: *http://www.simonzone.com/software/guarddog/#download*

[3] Manual Online do Guarddog: *http://www.simonzone.com/software/guarddog/#manual*

[4] Guidedog: *http://www.simonzone.com/software/guidedog/*

SOBRE O AUTOR

Holger Junge trabalha para a Lifemedien (*www.lifemedien.de*) onde, como bom pastor, apascenta servidores de domínio e de web além de bancos de dados MySQL e Oracle. Obviamente, todos rodando Linux.