Proteção ao alcance do usuário comum

Firewall para Leigos

Os Firewalls, dispositivos que controlam o tráfego e bloqueiam acessos indesejados, estão se tornando cada vez mais sofisticados. Entretanto as ferramentas de criação e configuração de firewalls estão ficando cada vez mais simples e acessíveis ao usuário não técnico.

POR JOE CASAD E ACHIM LEITNER

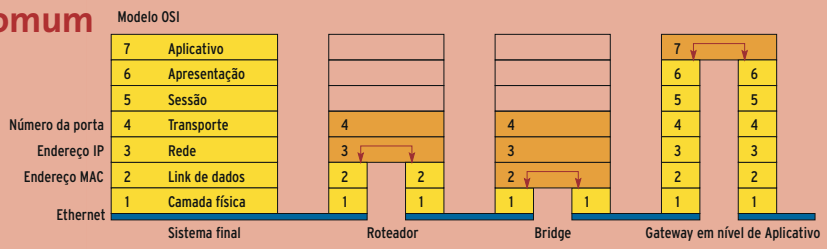

Figura 1: Os firewalls modernos podem operar como pontes ou *bridges* (à esquerda), roteadores (ao centro) ou *gateways* de aplicação (à direita).

Seu computador permite que você tenha uma visão do mundo, mas ninguém quer ter o mundo olhando seu computador. Os invasores estão ficando cada vez mais ousados e tecnicamente mais "afiados". Não é mais aceitável esperar que tais delinqüentes simplesmente não notem sua estação de trabalho "dando sopa". Se você está conectado à Internet, é melhor colocar-se atrás de algum tipo de firewall.

Os firewalls são oferecidos em vários tamanhos, formatos, preços e tecnologias. Um fenômeno curioso vem ocorrendo: o que antes era um simples filtro hoje é um conjunto completo de produtos de segurança. Tradicionalmente, um firewall é um tipo de roteador que fica na camada 3 do modelo de referência OSI. A camada 3 é, justamente, onde residem os protocolos de rede, mais precisamente o protocolo IP. O roteador lê os endereços IP e toma decisões quanto ao destino do datagrama– ou seja, em que direção deve roteá-lo. Um firewall também inspeciona a camada 4 (ou seja, os protocolos de transporte TCP e UDP) para identificar os serviços relevantes e interpretar os avisos presentes nas *flags*.

Produtos modernos de firewall podem operar em outras camadas da pilha de protocolos (figura 1). Esse enfoque multicamada pode ser estendido para baixo até a camada 2 – situação em que temos o famoso *bridgewall*. Da mesma forma como uma bridge (ou um switch) controla o tráfego baseado nos endereços MAC (camada 2), um bridgewall inspeciona os pacotes desde a camada 2 até a camada 4. O bridgewall é um filtro de pacotes tão flexível quanto um switch.

Um *gateway* de aplicação oferece um nível adicional de segurança em uma camada superior. Ele age na conexão TCP como um intermediário entre o cliente e o servidor – é o conhecido *proxy*. Isso permite que o firewall inspecione diretamente os protocolos da camada de aplicação e detecte pacotes ilegais que quebrem as regras estabelecidas pelo administrador de segurança.

Obviamente, os firewalls mais exóticos são produtos dedicados, baseados em hardware e destinados a redes gigantescas e configurações complexas. Estamos mais interessados no que se pode fazer com hardware comum, uma distribuição Linux e alguns programas fáceis de encontrar. Este mês, trazemos uma seleção de ferramentas para construção de firewalls, além de utilitários poderosos que simplificam sua configuração e manutenção. Com elas, você não precisa ser um expert em redes ou segurança para administrar um firewall.

Em um dos artigos, "Cão de Guarda", mostraremos como montar um firewall com IPtables ou IPchains usando o Guarddog. O artigo seguinte, "Ponte Levadiça", discorre sobre as ferramentas necessárias para se construir um firewall do tipo "bridge". Veremos como os "bridgewalls" funcionam e em que situações eles são interessantes.

Um maiores incômodos quando se administra um sistema de segurança é a quantidade de informação acumulada nos registros de eventos, os chamados *logs*. Nosso terceiro artigo mostra ferramentas para ler e analisar tais logs. Nossa matéria final, "Cumprindo Tabela", descreve o Shorewall, abreviação de *Shoreline Firewall* – outra ferramenta que não é um firewall em si, mas que abranda o inferno que é a vida do profissional de segurança.

Nenhum assunto é mais importante que a segurança; da mesma forma, poucos dispositivos são tão importantes na cadeia de segurança quanto os firewalls. O tema deste mês é apenas um lembrete de que firewalls não são apenas para experts: qualquer um conectado à Internet **precisa** de um firewall. Não é uma opção. ■

CAPA