FIREWALL - Como funcionam ...

Antes de mais nada é preciso entender alguns **Conceitos de Redes** que estão diretamente envolvidos no funcionamento e operação de um Firewall.

- *Conexões de entrada (**INPUT**), de saída (**OUTPUT**) e de redirecionamento (**FORWARD**)Conexões de entrada são as que vem de fora com destino direto ao seu micro. Conexões de saída são exatamente o inverso, partindo de seu micro com destino a um **host** (servidor) remoto. Já as conexões de redirecionamento são um pouco diferentes: elas vem de fora (lembrando que "de fora", pode ser tanto da web como de sua rede interna) e entram no seu micro, porém elas devem ser encaminhadas a outro host. O encaminhamento de pacotes geralmente aparece em redes internas, onde o acesso à web é feito via **NAT** (*Network Address Translation*). Quando o acesso é compartilhado por **proxy** (http://pt.wikipedia.org/wiki/Proxy), ou quando a estação tem acesso direto à web, esta lógica ocorre de forma diferente.*

- ***Portas TCP e UDP***

Na realidade, o popular protocolo TCP/IP é composto por um conjunto de outros protocolos os quais provêm os mais variados serviços de rede. Tanto o **protocolo de rede** TCP (muito utilizado) quanto o UDP (usado muito em conteúdo streaming, entre outras funções) oferecem uma série de portas lógicas para que os diferentes "sub" **protocolos de transmissão de dados** (HTTP, FTP, POP, etc.) possam operar. **São 65535 portas TCP + 65535 portas UDP**! Cada protocolo de dados usa uma porta específica - exemplos: HTTP usa a porta 80; TCP e FTP usam as portas 20 (em modo FTP ativo) e 21 TCP (tanto no modo Ativo quanto Passivo); POP usa a porta 110 TCP; e assim por diante. Para que um aplicativo servidor de páginas Web funcione (Apache, IIS, Tomcat, etc), por exemplo, é necessário configurar o sistema de forma que a porta 80 aceite conexões de entrada; se você quer configurar o Terminal Services do Windows Server, terá que liberar conexões entrantes na porta 3389 TCP; e assim por diante. Não é possível se conectar em portas fechadas, a não ser que você se aproveite de alguma vulnerabilidade do protocolo TCP/IP. Lembrando que o protocolo TCP é aberto, e cada sistema operacional usa uma compilação que seja adequada à sua arquitetura de software/hardware, e por isso certas vulnerabilidades que existem na implementação TCP de um sistema operacional podem não existir em outro.

- ***Portas abertas*, *Fechadas* e *Filtradas***

Como já foi dito, para que determinada tarefa de servidor aceite *conexões entrantes*, é necessario que a porta correspondente ao serviço esteja aberta (OPEN). Quando ela está fechada (CLOSED), não é permitido conexões de entrada. O modo filtrado (FILTERED, ou STEALTHED ou ainda BLOCKED) não só fecha a porta como impede que um micro externo consulte a situação dela ou tente realizar conexões, ou seja, os pacotes que chegam com destino a uma porta filtrada são efetivamente descartados. Um firewall confiável deve filtrar as portas não usadas, visto que mesmo que elas estejam fechadas, é possível se aproveitar de alguma vulnerabilidade do protocolo TCP/IP para forçar a entrada. Com elas filtradas, isto se torna uma tarefa virtualmente impossível.

- ***Escopo***

Define o **campo de atuação** de uma determinada **regra de firewall**. Suponhamos que você queira liberar apenas uma porta específica à web, e as demais deverão ser visíveis apenas à rede interna. Ou ainda, digamos que o acesso à porta 23 (telnet) deverá ser liberado apenas ao IP do administrador. Para atingir este objetivo, basta definir o escopo para cada uma das regras de seu firewall. Ele é composto pelo número IP, e pode ser acrescido a máscara de rede, de forma a abrir o acesso à todos os micros daquela faixa de IP. Exemplos de IPs e suas respectivas máscaras são: 192.168.0.0/16 (o mesmo que 192.168.0.0/255.255.255.0), 172.16.0.0/24 (ou 172.16.0.0./255.255.0.0) e 10.0.0.0/32 (ou 10.0.0.0/255.0.0.0). Para liberar/bloquear a porta a todos, geralmente não é necessário especificar o escopo, ou deve-se usar 0.0.0.0/0.0.0.0.

- ***Firewall*** *– Conceito e Exemplo de Utilização Prática*

O **Firewall** (*"parede de fogo"*, em Inglês) é basicamente um bloqueador de conexões entrantes. Ou seja, ele por padrão impede qualquer tipo de conexão entrante via portas TCP e UDP, e pode também restringir ou até barrar todas as solicitações ICMP (o exemplo mais conhecido de requisição ICMP é a de ping). Se seu micro não atua como servidor de absolutamente nada, então não há o menor motivo para permitir estes tipos de conexões. Porém, em certos casos, é necessário abrir execções - se o firewall bloquear as portas 139 (NetBIOS) e 445 (protocolo de rede MS), por exemplo, nenhum micro de sua rede interna conseguirá ver os arquivos e impressoras de sua estação. Ao criar **exceções**, você pode definir o escopo delas, de forma a definir exatamente quem pode acessar as portas de seu micro.

Num cenário real, onde há um servidor Conectiva Linux distribuindo serviços web, *visível* ao mundo todo (internet), além de servir impressão e arquivos para uma rede interna, as exceções seriam tratadas da seguinte forma:

- **Web (80):** todo mundo;
- **Servidor de arquivos e impressão (139, 445 e 631):** apenas rede interna;
- **Serviços administrativos, como SSH, SWAT e Webmin (22, 901 e 10000):** apenas para o IP do administrador.

Para saber quais portas estão abertas em seu micro, há vários meios: você pode usar sites que fazem esse serviço, como o da Sygate, ou pode usar softwares, como o **Local Port Scanner** ou **CurrPorts.** Quem usa Linux pode usar o "Todo-Poderoso" **nmap**, que além de realizar scan (varredura) em qualquer host acessado pelo seu micro, o **nmap** incorpora técnicas bem avançadas de *escaneamento*, que podem revelar brechas que muitos **port scanners** (*http://pt.wikipedia.org/wiki/Port_scanner*) não identificam. Alguns usuários podem dizer: *"Bem, eu fiz um scan com algum programa específico e ele não achou nenhuma porta aberta! Todas as portas não utilizadas foram identificadas como CLOSED"*. Pois muito bem, sabemos que cada porta requer um programa "*escutando*" a mesma, ou seja, não há como a porta 23 (telnet) estar aberta se não há um servidor telnet rodando no seu micro! Porém, lembre-se das portas fechadas e filtradas (conceito determinante como já vimos!). A partir do momento que a porta está apenas como CLOSED, ainda há meios de se conectar à ela. E mais: os **worms** (*http://pt.wikipedia.org/wiki/Worm*), pragas que podem comprometer o computador, precisam abrir uma porta no seu micro para "escutar" por conexões de entrada (o worm NetBus abre a porta 12345) provenientes de um vândalo digital remoto - cracker. Com um firewall devidamente configurado, não há como qualquer software em sua máquina abrir uma porta a não ser que você autorize - **aí está a grande vantagem de segurança do firewall para um micro doméstico**. O firewall complementa a ação do antivirus, impedindo que diversos tipos de praga funcionem. Porém, é bom lembrar que existem tipos **worm** capazes de desabilitar o firewall, nesse caso o programa de proteção antivírus deverá ser capaz de *barrá-lo*. Uma outra questão comum é: *"se eu tenho firewall, como eu ainda posso ser infectado por worms?!"*. Simples: um firewall não previne a infecção do computador, ele somente atua como bloqueador de conexões de entrada. Isso quer dizer que, em geral, o firewall não analisa o tráfego que entra e sai do micro; ele apenas impede que alguém se conecte ao seu micro.

A análise dos pacotes que trafegam num servidor de rede ou estação de trabalho pode ser realizada através do emprego da tecnologia **IDS** ***I****ntrusion* ***D****etection* ***S****ystem* (http://pt.wikipedia.org/wiki/Sistema_de_detec%C3%A7%C3%A3o_de_intrusos). Disponível na forma de software (o antivirus **avast!** inclui um IDS) ou hardware – *Appliance*; é consideravelmente caro e, provavelmente por isso, utilizado com mais frequência por empresas de médio e grande porte. Algumas soluções de firewall também permitem fazer análise de pacotes. O IDS é capaz de olhar pacote por pacote em busca de código malicioso, identificar o risco e bloquear / descastar o pacote. Para que o IDS funcione adequadamente, a constante atualização é fundamental; exatamente como nos antivirus e antispywares, visto que surgem novas pragas a cada dia, digo a cada hora.

- ***Que FIREWALL Utilizar ?***

Quem usa Linux tem um firewall *matador*. Com o **IPTables** é possível customizar quaisquer regras consolidando um ambiente seguro. Um bom nível de conhecimento e experiência são necessários. Para nós "pobres mortais, servos do Windows", sugerimos as seguintes soluções:

Windows Firewall ➔ Embutido no Windows XP SP2, ele é bem básico, já que é um firewall inbound (apenas lida com conexões de entrada). Eficiente em sua função, tem interface bastante amigável. É uma opção sábia mediante a ausência de outra solução qualquer de firewall.

ZoneAlarm ➔ Este é um firewall interessante, pois além de tratar das conexões entrantes, ele permite fazer restrições de várias outras situações. Há uma versão freeware disponível, no entanto a versão paga tem recursos adicionais relevantes.

Sygate Personal Firewall ➔ Similar ao ZoneAlarm, com a vantagem de ser mais customizável.