Firewall fácil com o Shorewall

Domando o fogo

É verdade que firewalls devem ser administrados por especialistas. Porém, até esses profissionais podem se beneficiar de uma interface prática para essa tarefa.

por Tarcísio Carvalho Espínola

Ramon Gonzalez - www.sxc.hu

Montar um firewall para a proteção de um único servidor não é tarefa das mais simples. Imagine montar um firewall para uma rede inteira, que requer muito mais atenção e conhecimento, tanto dos serviços quanto das ferramentas utilizadas. Qualquer descuido pode comprometer toda a segurança da rede e a reputação do seu administrador.

No caso específico do Linux, trabalhar com o *Iptables* na linha de comando torna as coisas um pouco mais complicadas, principalmente para usuários novatos ou acostumados apenas com cliques na interface gráfica. A criação de regras mais elaboradas requer tantas opções e parâmetros – e em uma rede mais complexa teremos dezenas delas – que é fácil cometer erros.

Não estamos questionando a eficácia dessa poderosa ferramenta; muito pelo contrário, o domínio de seus comandos para uma utilização eficiente e segura, em situações mais avançadas, exige bastante experiência por parte do administrador. Pensando nisso, Thomas M. Eastep teve a brilhante idéia de desenvolver uma ferramenta que funcionasse como uma camada entre o estressado e atarefado administrador de rede e o prolixo, mas poderoso, software Iptables: o *Shorewall*[1].

A forma simples e intuitiva como são desenvolvidas as regras no Shorewall facilita bastante a criação e manutenção do firewall. Na inicialização do serviço, as regras definidas pelo administrador são compiladas e convertidas em regras do Iptables, que será o responsável pelo firewall.

Devido à sua competência, o Shorewall permite também que o administrador aprimore seus conhecimentos na operação do Iptables, estudando as regras criadas pelo programa a partir das instruções passadas de forma gráfica. Quando o administrador adota a definição gráfica de regras pelo Shorewall, geralmente aumenta sua capacidade de criar e gerenciar configurações mais complexas. O poder da interface gráfica, nesse caso, está em permitir a administração de múltiplas regras de forma facilitada.

Para ilustrar a utilização do Shorewall, mostraremos como configurar o firewall de uma rede normalmente utilizada em pequenas e médias empresas (**figura 1**), embora o Shorewall possa ser utilizado em situações bem mais complexas.

Infra-estrutura

Em nossa rede de exemplo, usaremos servidores e estações Linux e Windows® para mostrar que os serviços

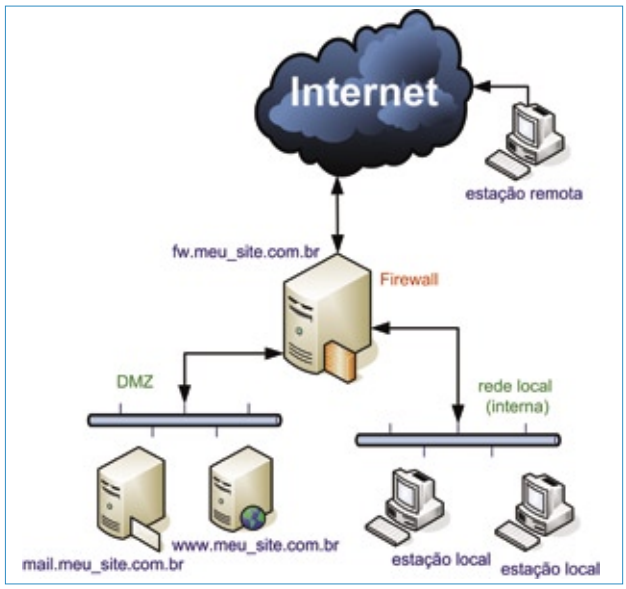

Figura 1 A rede utilizada neste artigo é bastante simples, composta por uma *DMZ*, uma rede local e o firewall conectando ambas à Internet.

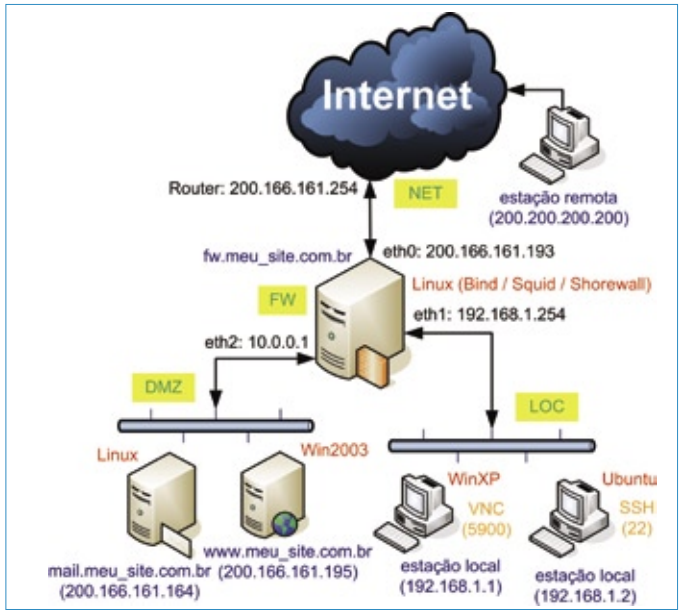

Figura 2 Detalhes da estrutura da rede usada neste artigo.

apresentados não dependem dos sistemas operacionais utilizados, com exceção, claro, do servidor firewall que deverá necessariamente usar Linux.

Para fins de exemplo, suponhamos que nossos 64 IPs pertencem à faixa 200.166.161.192/26, distribuídos da seguinte forma:

- IP da rede: 200.166.161.192;
- máscara: 255.255.255.192;
- IPs utilizáveis: 200.166.161.193 a 200.166.161.254;
- IP broadcast: 200.166.161.255.

A **figura 2** e a **tabela 1** detalham os parâmetros da nossa rede de exemplo.

Em seguida, basta configurar o servidor DHCP da rede local com os parâmetros acima. Na configuração das regras do firewall, consideraremos que o serviço de DHCP será oferecido pelo próprio servidor firewall, como veremos mais adiante, mas a sua configuração foge do escopo deste artigo.

A DMZ (zona desmilitarizada) obviamente fica isolada da rede local. Nela, serão conectados os servidores. Observe que, na **figura 2**, foi definido inclusive o endereço IP da estação remota que terá acesso a alguns serviços nas estações da rede local.

Note que, dos 64 endereços de que dispomos, iremos utilizar apenas seis (um para a rede, outro de broadcast, um no roteador e três nos servidores), e os 58 restantes serão desperdiçados. Isso é muito comum nos contratos com operadoras, ao menos no Brasil. Esse tipo de contrato tem ajudado a agravar a escassez de endereços IP disponíveis na Internet.

Tabela 1: Descrição da rede de exemplo

Roteador	
Interface Ethernet	200.166.161.254/26
Servidor Firewall	
Interface eth0	200.166.161.193/26
Interface eth1	192.168.1.254/24
Interface eth2	10.0.0.1/30 (interface da *DMZ*)
Gateway padrão	200.166.161.254 (IP do roteador)
DNS	200.166.161.193 (o servidor firewall também servirá DNS)
Servidor de email (`mail.meu_site.com.br`)	
Interface eth0	200.166.161.194/26
Máscara	255.255.255.192
Gateway padrão	200.166.161.254
DNS	200.166.161.193
Servidor Web (`www.meu_site.com.br`)	
Interface Ethernet	200.166.161.254
DNS	200.166.161.193
Rede local	
IP da rede	192.168.1.0
Máscara	255.255.255.0
IPs utilizáveis	192.168.1.1 a 254
Broadcast	192.168.1.255
Gateway padrão	192.168.1.254 (eth1 no servidor firewall)
DNS server	192.168.1.254 (eth1 no servidor firewall)

Instalação

Vamos agora instalar a ferramenta que será utilizada na configuração do firewall. Antes de iniciar, no entanto, é importante lembrar que a versão mais recente do Shorewall, no momento da escrita deste artigo, era a 4.08.

O Shorewall funciona da seguinte maneira: ao ser iniciado o programa, as configurações definidas nos arquivos do diretório `/etc/shorewall` são compiladas e convertidas em um arquivo que contenha as regras para o Iptables. Caso não ocorram erros, as regras serão aplicadas e o firewall ativado. Do contrário, o motivo da falha será mostrado e o firewall não será iniciado.

A partir do lançamento da versão 4.0, foram disponibilizadas duas versões de compiladores para as regras do Shorewall: a versão em script de shell,

que é a mais antiga e provavelmente será descontinuada nas próximas versões, e a versão em Perl, bem mais rápida, mas que ainda não está totalmente funcional. Apesar disso, muitos administradores já a utilizam em produção sem qualquer problema, por isso vamos usar essa nova técnica neste artigo.

Como o Shorewall está disponível nos repositórios de pacotes de todas as principais distribuições, não abordaremos a compilação do software a partir dos fontes.

Após a instalação, os arquivos que iremos editar na configuração do firewall serão colocados no diretório `/etc/shorewall/`, sendo eles:

```
interfaces;
masq;
policy;
proxyarp;
rules;
shorewall.conf;
zones.
```

Os pacotes para *Debian* e *Ubuntu*, no entanto, deixam os arquivos de configuração-padrão em `/usr/share/doc/shorewall/default-config/`. Nesse caso, basta copiá-los para `/etc/shorewall/`. Em seguida, já podemos iniciar a configuração do nosso firewall.

Zonas

Definiremos duas zonas para a montagem do firewall: uma para o próprio servidor firewall, que controlará todo o tráfego entre as zonas, e uma para cada rede a que ele estiver conectado. A **tabela 2** mostra como serão definidas essas zonas.

Todas as configurações de zonas no Shorewall deverão ser feitas no arquivo `/etc/shorewall/zones`. O **exemplo 1** ilustra como deve ficar esse arquivo em nossa configuração. Basta ele para definir todas as zonas do firewall. Observe que as zonas `NET`, `LOC` e `DMZ` foram configuradas com o tipo `ipv4`, pois isso é obrigatório. Note também que a zona `FW` foi definida como sendo o próprio firewall. Com o comando `man shorewall-zones`, o administrador pode ler mais informações sobre esse arquivo de configuração.

Interfaces

Cada zona será vinculada a uma interface de rede do servidor, exceto a zona `FW`, que representará o próprio servidor e não estará vinculada a nenhuma interface. Logo, deveremos ter três interfaces em nosso servidor:

- `eth0`: Interface vinculada à zona `NET`. Essa interface será conectada diretamente ao roteador que liga a rede à Internet. Em nosso exemplo, `eth0` receberá o IP 200.166.161.193/26.
- `eth1`: Interface vinculada à zona `LOC`. Essa interface deverá ser conectada ao switch da rede local e será configurada com o IP 192.168.1.254/24. É preciso configurar também o servidor DHCP da rede local, para que ele envie esse endereço como gateway às estações (em nosso exemplo, esse serviço será executado no próprio servidor firewall).
- `eth2`: Interface vinculada à zona `DMZ`. Essa interface tem uma particularidade: seu IP será configurado apenas com o intuito

Exemplo 1: Arquivo de zonas

```
01 #ZONE   TYPE       OPTIONS    IN         OUT
02 #                              OPTIONS    OPTIONS
03 fw      firewall
04 net     ipv4
05 loc     ipv4
06 dmz     ipv4
07
08 # Não apagar esta última linha.
```

Tabela 2: Definição das zonas

Nome da zona	Componentes	Características
Zona *FW*	O próprio firewall	Tem livre acesso às demais zonas, mas o acesso a ela será controlado de acordo com os serviços disponibilizados para cada zona.
Zona *NET*	Internet	Será considerada hostil em nossas configurações. É importante ter muito cuidado com ela.
Zona *LOC*	Rede local	Nesta zona estarão conectadas as estações locais da empresa. Seu acesso às demais zonas será controlado de acordo com os serviços permitidos para essa zona.
Zona *DMZ*	Servidores da empresa que proverão serviços à Internet e à rede local	Essa zona terá dois servidores, um com Linux (*mail.meu_site.com.br*), executando serviços de e-mail, e o outro com Windows Server (*www.meu_site.com.br*), que hospedará o site da empresa (ver **figura 1**).

de ativá-la, mas não pertencerá a nenhuma rede de qualquer zona. Nela, configuraremos o IP 10.0.0.1/30 e vamos conectá-la ao mesmo switch no qual serão conectados os servidores da DMZ.

Não será necessário seguir o padrão acima para montar os seus próprios firewalls; no entanto, é recomendável fazê-lo. Também é possível usar *aliases* de interfaces (`eth0:0`, por exemplo) se necessário. Todas as configurações de interfaces no Shorewall deverão ser feitas no arquivo `/etc/shorewall/interfaces`.

O **exemplo 2** mostra como deve ser feita essa configuração. Observe que esse caso não configura a zona `FW`, uma vez que ela não estará vinculada a nenhuma interface. Além disso, os endereços broadcast foram configurados para serem detectados automaticamente. Já para a interface `eth0`, que terá IP estático, foram definidas as opções `tcpflags`, `routerfilter`, `nosmurfs`, `norcf1918` e `logmartians`.

É interessante consultar o manual do arquivo de configuração de interfaces e descobrir a função de cada uma dessas opções (`man shorewall-interfaces`). Elimine-as, se necessário (não recomendável), ou adicione outras de acordo com as suas necessidades.

Exemplo 2: Arquivo de interfaces

```
01 #ZONE  INTERFACE  BROADCAST  OPTIONS
02 net    eth0       detect     tcpflags,routefilter,nosmurfs,norf
➥c1918,logmartians
03 loc    eth1       detect
04 dmz    eth2       detect
05
06 # Não apagar esta última linha.
```

Exemplo 3: Arquivo de políticas

```
01 #SOURCE  DEST   POLICY   LOG     LIMIT:BURST
02 #                        LEVEL
03 fw       all    ACCEPT
04 loc      all    REJECT   info
05 net      all    DROP     info
06 dmz      all    DROP     info
07 #
08 # THE FOLLOWING POLICY MUST BE LAST
09 #
10 all      all    DROP     info
11
12 # Não apagar esta última linha.
```

Tabela 3: Políticas entre zonas

Zona	Política	Explicação
FW	ACCEPT	Requisições vindas da zona FW com destino às demais zonas (all) serão permitidas e nada será registrado no log.
LOC	REJECT	Requisições vindas da zona LOC; com destino às demais zonas (all), deverão ser bloqueadas. Uma resposta será retornada ao solicitante e os bloqueios serão registrados no log (com a tag info).
NET	DROP	Requisições vindas da zona NET; com destino às demais zonas (all), deverão ser bloqueadas. Nenhuma resposta será retornada ao solicitante e os bloqueios serão registrados no log (com a tag info).
DMZ	DROP	Requisições vindas da zona DMZ; com destino às demais zonas (all), deverão ser bloqueadas. Nenhuma resposta será retornada ao solicitante e os bloqueios serão registrados no log (com a tag info).

Políticas

Definidas as zonas e interfaces, definiremos agora as políticas de acesso entre cada par de zonas. As definições mostradas na **tabela 3** serão adotadas como padrão para qualquer requisição que ocorra entre as zonas.

Para reforçar a segurança, vamos definir, por fim, que todas as requisições vindas de qualquer zona (`all`) com destino a qualquer zona (`all`) serão bloqueadas, e que esses bloqueios sejam registrados no log com a *tag* `info`. Essa regra deverá ser a última no arquivo de configuração.

Todas as configurações das políticas de acesso no Shorewall devem ser feitas no arquivo `/etc/shorewall/policy`, como mostra o **exemplo 3**. Note que a regra geral, ou seja, a que define a política de qualquer pacote, foi a última a ser definida, justamente para ser aplicada apenas se os pacotes não se encaixarem a nenhuma outra regra. Mais uma vez, é importante consultar a página de manual do programa (`man shorewall-policy`) para obter mais detalhes. ■

Mais informações

[1] Shorewall: http://www.shorewall.net/

Sobre o autor

Tarcísio Carvalho Espínola é coordenador de TI do Instituto Centec, onde vem trabalhando na implementação de soluções livres nos servidores da empresa. Em seu tempo livre, ele ainda mantém o site Opção Linux (http://www.opcaolinux.com.br).