



Mergulhe fundo nos logs do seu firewall

Abrindo a caixa preta

Firewalls baseados em Netfilter produzem registros de eventos (os famosos *logs*) tão monstruosos e gigantescos que ninguém em sã consciência quer (ou consegue) digeri-los manualmente. Para nos tirar desse lodaçal lançamos mão das ferramentas de análise de logs. Este mês testamos o IPTables Log Analyzer, o Wallfire wflogs e o FWlogwatch, que pretendem auxiliar os administradores no desenvolvimento e manutenção de suas regras de firewall. Será que dão conta do recado? **POR RALF SPENNEBERG**

Em ambientes protegidos por firewalls, o administrador precisa manter um controle rígido sobre como estão definidas as regras de filtragem e a quantas anda o tráfego dos clientes. Entretanto, megabytes de arquivos de registro (*logfiles*) podem afogar até os profissionais mais competentes, arrastando-os numa fenomenal enxurrada de informações que eles enfrentam sem proteção apenas para ter certeza de que não deixaram nenhuma pista para trás. É uma vida dura...

Os amigos do syslog

Ferramentas de análise de protocolo podem ser de grande ajuda para sair desse espinhoso dilema. Felizmente, os usuários de Linux possuem muitas opções de programas para análise de firewalls. Neste artigo analisaremos três alternativas: IPTables Log Analyzer [1], wflogs do projeto Wallfire [2] e fwlogwatch [3]. Todos os três reconhecem uma variedade bastante grande de protocolos e apresentam os resultados em relatórios HTML muito bonitos. O wflogs e o fwlogwatch possuem, além disso, modos de visualização em tempo real. O IPTables Log Analyzer é a única ferramenta que usa um banco de dados para armazenar os resultados.

Correndo em direção contrária, o IPTables Log Analyzer é calcado no subsistema Ulogd [4] de Harald Weltes, que substitui o subsistema padrão do kernel, o syslog. Infelizmente, ferramentas de análise gratuitas que reconheçam o banco de dados do Ulog são raríssimas. Uma delas é o Ulogd-php [5]. Ao contrário de todos os outros sistemas de registro de eventos, o Ulogd pode registrar incidentes em seu banco de dados.

IPTables Log Analyzer

O IPTables Log Analyzer é um servidor que gera logs do IPTables (kernels 2.4 e 2.6) artisticamente formatados em lindas páginas HTML (ver figura 1). A ferramenta tem três componentes. O gerenciador de saída (*database feeder*) armazena cada evento registrado nos logs em um banco de dados MySQL. Os administradores podem consultar os resultados em uma interface web. O gerenciador, o banco de dados e a interface web podem rodar tanto na mesma máquina como em máquinas separadas. Nesse segundo caso, o banco de dados pode recolher logs de múltiplos firewalls.

Depois de decidir-se sobre a arquitetura a ser implementada, o administrador precisa criar um banco de dados

MySQL chamado *iptables*, liberando acesso para que os usuários *iptables_admin* e *iptables_user* possam manipulá-lo. Depois, é preciso gerar as tabelas dentro do banco de dados (veja a listagem 1). Obviamente, depois de tudo isso deve-se escrever as regras para o IPTables. Duas cadeias definidas pelo usuário nos parece ser a melhor abordagem (veja a listagem 2).

Criando cadeias

Em vez do tradicional *-j ACCEPT*, o IPTables usará, agora, *-j LOG_ACCEPT*. Essas modificações não são necessárias se usarmos o Shorewall [6] ou o SuSE Firewall em CD [7]. Isso posto, temos que informar também que a SuSE não vai mais oferecer suporte ao seu firewall comercial. Essa é mais uma razão para que os administradores reflitam e passem a usar *apenas* ferramentas e atualizações provenientes do universo do Software Livre. Ficar na mão de fornecedores comerciais é isso mesmo: ficar na mão...

O próximo passo é instalar a interface web. Para isso, o administrador precisa simplesmente copiar (ou mover) o diretório *web* para dentro da área de documentos HTML (chamada normalmente de *document root*) do servidor web que

The screenshot shows the 'iptables logs' web interface. At the top, there are navigation tabs for 'Reports', 'Admin', and 'Help'. Below the title, it says 'Last packets filtered by chain ALL younger than any :'. The main content is a table of log entries with columns: Chain, Date, Proto., Src IP, Dest IP [HIDE], and Dest. port. The entries are mostly 'ACCEPT' for TCP connections to 'spenneberg.com' on port 80. There is one 'DROP' entry for a connection to 'p508C2039.dip.t-dialin.net' on port 1433. To the right of the main table are several panels: 'Packet selection [HIDE]' with dropdowns for 'Current chain' (set to 'ALL'), 'Nb packets / page' (set to '20'), and 'Packets date' (set to 'any'); 'Database stats [HIDE]' showing '1601 packets in database', '1601 packets younger than any', and '1601 packets today'; 'Top Hosts [ALL] [any] [HIDE]' listing hosts like 'proxy.rba.ch' and 'p09557F2.dip.t-dialin.net'; and 'Top Proto [ALL] [any] [HIDE]' showing 'TCP' with a count of '1601'.

Figura 1: O IPTables Log Analyzer oferece uma visão geral bem clara sobre o estado dos firewalls.

estiver usando (provavelmente o Apache) e modificar o arquivo *configure.php* para refletir as configurações reais do banco de dados e do servidor web (usuário, senha, URL). A última etapa é instalar e ativar o gerenciador de saída (*database feeder*). Talvez seja preciso alterar novamente as credenciais de usuários do banco de dados.

O IPTables Log Analyzer possui três variantes: *feed_db.pl*, *feed_db-shorewall.pl* e *feed_db-suse.php*. Para rodar o feeder automaticamente durante o boot, é preciso copiar o script de inicialização *scripts/iptableslog* para o diretório */etc/init.d* e criar os links simbólicos apropriados nos diretórios *rc*.

wflogs

O wflogs é a ferramenta de análise do projeto Wallfire [2], embora possa ser usada independentemente dos outros módulos. O programa interpreta e processa arquivos de log dos firewalls baseados em Netfilter, IPchains, IPfilter, Cisco PIX, Cisco IOS e do sistema de detecção de intrusos (IDS - *Intrusion Detection System*) Snort. Os relatórios de evento podem ser produzidos em texto puro, HTML e XML, além de um interessante modo interativo, em que os eventos são mostrados em tempo real. O

wflogs não guarda as informações processadas em um banco de dados, mas pode converter entre os formatos de arquivo do Netfilter, IPchains e IPfilter.

Instalar o wflogs em um sistema Debian é tarefa simples; basta usar o APT. O Debian versão *Sid* inclui o wflogs nos repositórios oficiais. Para o Debian estável (*Woody*) o programa pode ser baixado de [8]. Usuários de outras distribuições têm a opção de compilar o wflogs a partir dos fontes – quem gosta de RPM não terá sorte desta vez. Será necessário, antes, instalar a biblioteca *Wfnetobjs*, outro componente do Wallfire [2]. Recomenda-se ainda a instalação da biblioteca alternativa de DNS, *adns* [9], para que seja possível fazer resolução de nomes por DNS assíncrono.

Para compilar o wflogs, siga as etapas de sempre, com os comandos: *./configure; make; make install*. Talvez seja preciso especificar, no script *configure*, o diretório onde a biblioteca *WFnetobjs* se encontra.

De Netfilter a HTML em poucos passos

O wflogs pode processar logs de firewall tanto online quanto offline. O comando a seguir cria um relatório simplificado formatado em HTML e gerado a partir de um arquivo de log do Netfilter (figura 2):

```
wflogs -i netfilter -o html >
netfilter.log > logs.html
```

No modo *real time*, o wflogs analisa cada novo evento registrado no log e, depois de processados, joga todos na tela. Os administradores podem usar um shell para mudar o comportamento do wflogs interativamente. Por exemplo, o comando a seguir diz ao wflogs para monitorar o arquivo */var/log/warn* em tempo real:

```
wflogs -RI -o human >
/var/log/warn
```

A opção *-P* obriga o wflogs a processar mensagens antigas no arquivo. O wflogs ignora mensagens que não sejam específicas de firewall.

The screenshot shows the 'wflogs summary' page. At the top, it says 'Generated on Fri Apr 30 12:29:37 CEST 2004 by spenneb.'. Below is a table with columns: #, start, end, interval, loghost, chain, input interface, output interface, proto, and source. The table contains several rows of log entries, including:

- Row 13: start Apr 30 10:45:24, end Apr 30 10:46:26, interval 00:00:01:02, loghost P15097491, chain ACCEPT: HTTP-Zugriff, input interface eth0, output interface -, proto tcp, source 62.52.55.227
- Row 15: start Apr 30 10:34:17, end Apr 30 10:34:20, interval 00:00:00:03, loghost P15097491, chain ACCEPT: HTTPS-Zugriff, input interface eth0, output interface -, proto tcp, source 62.59.233.212
- Row 2: start Apr 30 11:25:51, end Apr 30 11:25:52, interval 00:00:00:01, loghost P15097491, chain ACCEPT: HTTPS-Zugriff, input interface eth0, output interface -, proto tcp, source 62.94.244.202
- Row 6: start Apr 30 10:26:56, end Apr 30 10:27:37, interval 00:00:00:41, loghost P15097491, chain ACCEPT: HTTP-Zugriff, input interface eth0, output interface -, proto tcp, source 62.101.126.222
- Row 15: start Apr 30 10:44:47, end Apr 30 10:47:02, interval 00:00:02:15, loghost P15097491, chain ACCEPT: HTTPS-Zugriff, input interface eth0, output interface -, proto tcp, source 62.108.18.44
- Row 18: start Apr 30 10:45:01, end Apr 30 10:47:10, interval 00:00:02:09, loghost P15097491, chain ACCEPT: HTTP-Zugriff, input interface eth0, output interface -, proto tcp, source 62.108.18.44
- Row 38: start Apr 30 10:27:03, end Apr 30 10:50:29, interval 00:00:23:26, loghost P15097491, chain ACCEPT: HTTP-Zugriff, input interface eth0, output interface -, proto tcp, source 62.159.148.131
- Row 55: start Apr 30 10:35:06, end Apr 30 10:38:14, interval 00:00:03:08, loghost P15097491, chain ACCEPT: HTTP-Zugriff, input interface eth0, output interface -, proto tcp, source 62.159.226.12
- Row 8: start Apr 30 10:22:12, end Apr 30 10:22:42, interval 00:00:00:30, loghost P15097491, chain ACCEPT: HTTP-Zugriff, input interface eth0, output interface -, proto tcp, source 62.238.255.223

Figura 2: A página wflogs Summary (resumo do wflogs) mostra quantos pacotes foram registrados para cada origem.

Listagem 1: Banco de dados MySQL

```
# mysql -u root -p
mysql> create database iptables;
mysql> grant create,select,insert on iptables.* to iptables_admin@localhost identified by 'g3h31m';
mysql> grant create,select on iptables.* to iptables_user@localhost identified by 'auchgeheim';
mysql> quit
# cat sql/db.sql | mysql -u iptables_admin -p iptables
```

Filtrando mensagens

Há opções de filtragem extremamente poderosas que podem restringir a exibição de mensagens a tipos bastante específicos. O filtro a seguir foi retirado da documentação do wflogs. Ele lista apenas as conexões bloqueadas de Telnet e SSH ocorridas nos últimos três dias e vindas da rede 10.0.0.0/8:

```
wflogs -f '$start_time >= 3
this 3 days ago] && $start_time < [this 2 days ago] && $chainlabel =~ /(DROP|REJECT)/ && $sipaddr == 10.0.0.0/8 && $protocol == tcp && ($dport == ssh || $dport == telnet) && ($tcpflags & SYN)' -i netfilter -o text --summary=no
```

fwlogwatch

Boris Wesslowski desenvolveu o fwlogwatch para o RUS-CERT na Universidade de Stuttgart, Alemanha. A versão 1.0 do programa [3] foi, finalmente, liberada sob a licença GPL.

O fwlogwatch possui três modos de operação: Log Summary Mode (modo de relatório resumido), Interactive Report Mode (modo interativo de relatórios)

e Realtime Response Mode (modo interativo em tempo real). No modo Log Summary, o programa gera relatórios em texto puro ou HTML com os resumos da análise dos logs (figura 3). No Report Mode, o fwlogwatch automaticamente cria relatórios de incidentes que os administradores podem enviar às pessoas afetadas pelo incidente sempre que necessário.

No Realtime Mode, o fwlogwatch responde a ataques executando scripts, enviando mensagens de email ou automaticamente modificando as regras do firewall. Os administradores podem usar o servidor web embutido (não há necessidade de um Apache) para monitorar o estado do fwlogwatch.

O programa reconhece os arquivos de log de firewalls baseados em IPchains (opção *i*), Netfilter (*n*), IPfilter (*f*), IPFW (*b*), Cisco IOS (*c*), Cisco PIX (*p*), Netscreen (*e*), Windows XP (*w*), Elsa Lancom (*l*) e o IDS Snort (*s*). A instalação é feita com um simples `make && make install` e `make install-config`. Boris Wesslowski possui pacotes para Red Hat Linux e Debian no site oficial do fwlogwatch.

Os administradores podem configurar

o comportamento do fwlogwatch usando como base o arquivo exemplo de configuração, bem documentado e com comentários informativos, ou pela linha de comando. A página de manual explica a sintaxe e funcionamento de todas as opções. Por exemplo, o comando mostrado a seguir executa o fwlogwatch em *Summary Mode*:

```
ureserver.info) port 80 (http) with TCP flags SYN
at Apr 30 12:28:48, 1 packet logged on host P15097491: chain IPTABLES ACCEPT: HT
IP-Zugriff, on input interface eth0, source mac address 00:00:5a:9d:10:ba, desti
nation mac address 00:20:ed:2f:ed:68, protocol tcp, from 80.58.0.172 (unknown ho
stname) (80.58.0.0/16 RIMA (Red IP Multi Acceso) AS3352 Internet Access Network
of IDE) port 50651 (unknown service name) to 217.160.128.61 (p15097491.pureserve
r.info) port 80 (http) with TCP flags SYN
at Apr 30 12:28:52, 1 packet logged on host P15097491: chain IPTABLES ACCEPT: SS
H-Zugriff, on input interface eth0, source mac address 00:00:5a:9d:10:ba, desti
nation mac address 00:20:ed:2f:ed:68, protocol tcp, from 212.204.17.133 (id4cc118
5.versanet.de) port 64541 (unknown service name) to 217.160.128.61 (p15097491.pu
reserver.info) port 22 (ssh) with TCP flags SYN
/var/log/messages:3250: warning: line format matches none of the specified modul
e(s): netfilter
wflogs> help
help          Display this text.
?             Synonym for 'help'.
quit         Quit.
exit         Synonym for 'quit'.
beep         Set beep mode: [on/off?]. Beep for every log entry displayed.
filter       Set filter expression: [expression/unset].
realtime     Set realtime mode: [on/off?]. Monitor new log entries..
verbose      Set verbosity level: [level].
wflogs>
```

Figura 3: No *Summary Mode* o fwlogwatch dá aos administradores uma visão geral da atividade nos arquivos de log.



Figura 4: O servidor web embutido no fwlogwatch permite que o administrador monitore o estado atual do firewall.

```
fwlogwatch -b -Pn -U
'Spenneberg.Com' -p -n -N -o
output.html -t -w
/var/log/messages
```

A opção `-Pn` ativa o interpretador para os logs do Netfilter. Já `-U` permite que o usuário especifique um cabeçalho para o relatório. A opção `-o` especifica o arquivo de saída; `-w` estipula que o relatório será gerado no formato HTML. `-n` e `-N` ativam a resolução de nomes para máquinas e serviços. Como resultado, obtemos um belo relatório formatado em HTML, mostrando toda a atividade de nosso firewall.

Resposta imediata

A opção de rodar o fwlogwatch em modo real time permite que os administradores reajam com ações e comandos às mensagens do arquivo de log. Ao mesmo tempo, o estado do firewall é mostrado em uma janela de navegador. O fwlogwatch roda em segundo plano como um daemon e monitora o arquivo de log. Se o daemon receber um sinal *SIGHUP*, o arquivo de configuração é lido novamente. Já o sinal *SIGUSR1* ordena ao daemon que reabra o arquivo de log. Esse recurso é bastante útil com arquivos de log rotativos.

Listagem 2: IPTables Log Analyzer

```
iptables -N LOG_DROP
iptables -A LOG_DROP -j LOG --log-tcp-options --log-ip-options --log-prefix '[IPTABLES DROP] : '
iptables -A LOG_DROP -j DROP
iptables -N LOG_ACCEPT
iptables -A LOG_ACCEPT -j LOG --log-tcp-options --log-ip-options --log-prefix '[IPTABLES ACCEPT] : '
iptables -A LOG_ACCEPT -j ACCEPT
```



Figura 5: Os administradores podem usar o navegador para configurar o fwlogwatch. O **Alert Threshold** (Limiar de Alerta) especifica o número de mensagens necessárias para disparar uma contramedida.

Os administradores podem especificar valores que definam qual a gravidade necessária nas mensagens para que o fwlogwatch reaja, emitindo alertas ou executando scripts de retaliação. Há duas opções importantes: *recent* (-l) define o período de tempo a monitorar, enquanto *alert_threshold* (-a) define, dentro desse período, o número de eventos que dispara uma resposta. A listagem 3 mostra um exemplo que configura o fwlogwatch em modo *Real Time* com o interpretador para arquivos de log do Netfilter. O processo roda como o usuário *fwloguser*.

Listagem 3: fwlogwatch Realtime Mode Analyzer

```
realtime_response = yes
parser = n
run_as = fwloguser
recent = 600
alert_threshold = 5
notify = yes
notification_script = /usr/sbin/fwlw_notify
server_status = yes
bind_to = 127.0.0.1
listen_port = 8888
status_user = ralf
status_password = i0Q1Am0g4PrAA
refresh = 10
```

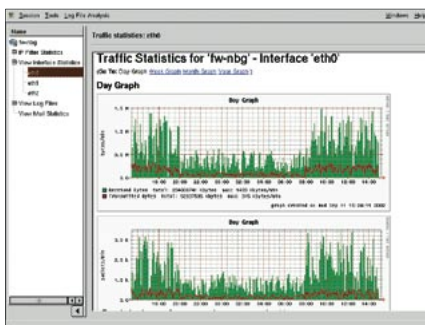


Figura 6: Apesar de ser uma ferramenta interessante, o *SuSE Firewall* não será mais mantido.

Se o limiar de cinco conexões em 600 segundos (dez minutos) é excedido, o fwlogwatch dispara uma ação configurável. O servidor web interno roda no endereço 127.0.0.1:8888, no qual o usuário *ralf* pode “logar-se” com a senha *password*. As senhas são criptografadas com o algoritmo DES, que podem ser geradas com o comando *htpasswd -nb usuário senha*. Quando o usuário registra-se na página, depara-se com algo parecido com a figura 4. Uma grande quantidade de opções pode ser alterada nessa interface web (figura 5).

Escolhas

O fwlogwatch possui um vasto cardápio de recursos, desde a exibição de resumos simplificados ao poderoso modo em tempo real com respostas configuráveis. Mas as outras ferramentas mostradas no artigo também merecem ser consideradas e testadas. Se você precisa de uma filtragem fenomenal, o wflogs pode ser sua melhor

opção. O IPTables Log Analyzer é interessante porque usa um banco de dados para guardar as informações recolhidas. Para quem conhece, a opção de usar declarações na linguagem SQL para fazer pesquisas nas mensagens do firewall baseadas em critérios arbitrários é bem interessante e poderosa. Muito mais poderosa do que depender do *front-end* via web oferecido pelas outras ferramentas. ■

INFORMAÇÕES

- [1] IPTables Log Analyzer: <http://www.gege.org/iptables/>
- [2] Projeto Wallfire (wflogs e Wfnetobjs): <http://www.wallfire.org>
- [3] FWlogwatch: <http://fwlogwatch.inside-security.de>
- [4] Ulogd: <http://gnumonks.org/projects/ulogd>
- [5] Ulogd PHP: <http://www.inl.fr/download/ulog-php.html>
- [6] Shorewall firewall: <http://shorewall.sourceforge.net>
- [7] SuSE firewall: http://www.suse.de/en/business/products/suse_business/firewall/
- [8] Pacotes do wflogs para o Debian Woody. Coloque, em seu sources.list, a linha *deb http://people.debian.org/~kelbert/stable main*
- [9] GNU adns: <http://www.chiark.greenend.org.uk/~ian/adns/>

SOBRE O AUTOR

Ralf Spenneberg é um instrutor freelance de Unix e Linux. Em 2002 publicou o livro “Intrusion Detection for Linux Servers”, rapidamente seguido de “VPNs on Linux”. Em breve, mais um livro seu, “Intrusion, Detection and Prevention with Snort and Co.”, estará nas livrarias.

