

n a firewall-protected environment, the administrator must keep track of developments by logging as many transactions as possible. At the same time, admins want to avoid wading through megabytes of logfiles just because they are worried about missing a clue.

Logfile Helpers

Protocal analysis tools provide a solution to this dilemma. Linux users have many options for firewall analysis programs. In this article, we'll look at three alterna-

Analysis Tools for Firewall Logfiles For the Record

Netfilter firewalls create highly detailed logfiles that nobody really wants to inspect manually. Logfile analysis tools like IPtables Log Analyzer, Wallfire Wflogs, and FWlogwatch help administrators keep track of developments and filter for important messages. **BY RALF SPENNEBERG**

tives: IPtables Log Analyzer [1], WFlogs from the Wallfire project [2], and FWlogwatch [3]. All three programs support a wide range of protocol formats and serve up the results as neatly formatted HTML pages; WFlogs and FWlogwatch additionally have realtime modes. IPtables Log Analyzer is the only tool to use a database for message storage.

IPtables Log Analyzer relies on a special feeder. Harald Weltes' Ulogd [4] handles this natively, replacing the legacy syslog system. Unfortunately, free analysis tools that support the Ulog database are rare. Ulogd-php [5] is one of the first. In contrast to all other logging systems, Ulogd can log events that caused a firewall alert in its database.

IPtables Log Analyzer

IPtables Log Analyzer serves up IPtables logs for Linux 2.4 or 2.6 in the form of

neat HTML pages (see Figure 1). The tool includes three components. The database feeder stores logfile entries in a MySQL database; admins can then use a web interface to access the database. The database feeder, the database, and the web interface can run either on the same machine or on separate machines. In the latter scenario, the database can collect logfiles from multiple firewalls.

After deciding on the architecture, the administrator needs to create a MySQL database called *iptables*, allow the users *iptables_admin* and *iptables_user* access, and generate tables within the database (Listing 1). Of course you also need to define IPtables rules. Two user-defined chains are the best approach (Listing 2).

Creating Chains

Instead of *-j ACCEPT*, IPtables will now use *-j LOG_ACCEPT*. These modifications

iptables log	5	wflogs summary Generated on Fis Apr 30 12:29:37 (2037) 2034 by spenade.								
Card particle Blood by chain ALL prompt Non-ray :	towardse RA H		-	Invest	lagtand	and a	iqui acceler	erps and an	-	-
ATTER 200-04 01110 110 105 201 200-04 200-06	Martin yar 2 S	13 Apr 3	Apr 30 4 10/16/28	00.00.01.12		ACCEPT: HTTP-Zagar	#1M3	-	17	42.52.55.217
ACTER 204-0-0-0214FTP 14220100.22 operating con 800pp ACTER 204-4-0-0214FTP 14220100.22 operating con 800pp	The second second second	12 4010	Arr.20	00.00.00.01		ACCEPT. HTTPS Zapat	-		-	
ACTIFY 2014-0 10/10 TP 10/2010.22 operating on 900pp ACTIFY 2014-0 10/10 TP 10/20108.22 operating on 900pp	provide a state of the state of	3 Apr 1	Apr 30			ACCEPTI HTTPS-Zaget				
ACTEPT 2004-04 90.11 (0 TEP 145 2014)02.20	Anne Marian Anne Marian Anne Marian	 Apr.2 10.263 	Apr.20	0.0010-41		ACCEPT: HTTP: Zapett	100		47	
ACTERY 2004-04-10 102116 TEP 145-251-106-22 sponstory and 903000 ACTERY 2004-04-10 102116 TEP 142-251-108-22 sponstory and 903000	ALL ALL OF BUILD AND ALL AND A	15 April	Apr 30 T 10-4750			ACCEPT: HTTPS-Zageif				
ATTIP 2014 0112 IN TO 0221 IN 2 OPPORT OF BUILD	anna ann an a	11 Apr 1	Apr 30 1047-10	0010012-04	P13377411	ACCEPT: HTTP Zaget	100		17	42118-18-84
ACTED V. 2004-04-06 (02112) TEP (45-23) (06.22	14-01-0003-00 B	3 Apr 34 10.270	Apr 30 5 10:50(25			ACCEPT: HTTP-Zogrift	+00			
Datas Sanat another TTP proc Strapping and provide an electron of the second	10	55 Apr 3	Apr 20	10-00-01-04	PERMITAN	ACC1PT HTTP-ZapidT	1919		17	41.191.2512

Figure 1: The IPtables Log Analyzer gives administrators a clear view of firewall logfiles.

Figure 2: The WFlogs Summary page shows how many packages have been logged for each source.

COVER STORY

are not required for Shorewall [6] or Suse Firewall on CD [7]. This said, Suse will not be supporting its commercial firewall product in the future, which is yet another reason for administrators to choose tools and updates from the world of open source.

The next step is to install the web interface. To do so, the admin user needs to move the *web* directory to the web server's document root and modify *config.php* to reflect the database and web server settings (user, password, URL). The final step is to install and enable the database feeder. Again, you will need to modify the database user credentials.

IPtables Log Analyzer has three feeder variants called *feed_db.pl*, *feed_db-shore-wall.pl*, and *feed_db-suse.php*. To launch the feeder automatically, the admin user needs to move the start script, *scripts/iptablelog*, to */etc/init.d* and create links in the *rc*.

WFlogs

WFlogs is the analysis tool belonging to the Wallfire project [2], although it can be used independently. The modular program parses and processes Netfilter, IPchains, IPfilter, Cisco PIX, Cisco IOS and Snort logfiles, serving up the results as text, HTML, XML, or an interactive realtime mode. WFlogs does not have database support, but it can additionally convert between the Netfilter, IPchains, and IPfilter logfile formats.

Installing WFlogs on Debian is really simple. Debian Sid includes WFlogs, and packages for Woody are available from [8]. Users of other distributions can

Listing 1: MySQL Database

- 01 # mysql -u root -p
 02 mysql> create database
 iptables;
- 03 mysql> grant create,select,insert on iptables.* to iptables_admin@localhost identified by 'g3h31m';

04 mysql> grant create,select on iptables.* to iptables_user@localhost identified by 'auchgeheim';

```
05 mysql> quit
```

```
06 ∦ cat sql/db.sql | mysql -u
iptables_admin -p iptables
```

build WFlogs from the source code. WFlogs also requires the WFnetobjs library, another Wallfire component [2]. The alternative DNS library, *adns* [9], is also recommended for asynchronous DNS name resolution.

To build WFlogs, follow the typical ./configure; make; make install, steps; you may need to specify the WFnetojbs directory in the configure step.

Netfilter to HTML

WFlogs can process firewall logs offline or online. The following command creates an HTML-formatted overview from a Netfilter logfile(Figure 2):

wflogs -i netfilter -o html **2** netfilter.log > logs.html

In realtime mode, WFlogs analyzes new entries in the logfile and outputs these entries on the screen. Administrators can use a shell to interactively modify WFlogs' behavior. The following command tells WFlogs to monitor a file called /var/log/warn interactively in realtime:

```
wflogs -RI -o human 2
/var/log/warn
```

The *-P* option tells WFlogs to process older messages in the file. WFlogs is not thrown by non-firewall messages.

Filtering

Powerful filtering options can restrict output to specific messages. The following filter is from the WFlogs documentation; it lists denied Telnet and SSH connections for the last three days for the 10.0.0.0/8 network:

areierver, in	ful port 00 (brttp) with TCP flags 57%
at Apr 30 12	20:40, 1 parket lagged on host F15007401: chain IFTARLES ACCEPT: HT
TP-Degriff.	m imput interface eth0, swares max address 00:00:3ar80:30:ba, denti
sation sat a	Advess Middleduffiedies, protocol top, from \$5,58.0.177 (uninces he
straine) (80.1	18.0.0/16 klish (Red IF Skilti Access) slikiti internet Access Betwerk
of THE PART	50651 (unknown service tune) to 217,180,128,61 (u15007481, pureserve
r infal part	80 (brttp) with DT flags 50h
et der 30 12 n-Degriff, o atice mac ab 5. vernamet.d venerver.ind /war/log/wen o(s): metfil	(20:52, 2 parter lapped on host T1300740): chain DFIARLES ACCEPT: 55 1 input interface outp, searce mat address 00-00:51;51;91(Drbm.,destin breas 00:20:00:11;71(d);80, pertool top, from 22:20:17:1301 (DeStTint pert 44541 (minimum service none) to 217:100.120.61 (pi5097401.pe pert 44541 (minimum service none) to 217:100.120.61 (pi5097401.pe pert 22 (mak) with T07 flags 209 organ:2500: warning: line format matches none of the specified metal pert
aflogs: belp	
help	Bisplay this text.
	Synamyn for 'belg',
1100	Quin.
RELT.	Synamym Ever upit!.
bwege -	ter boop mide: [onisff17], hosp for every log ontry displayed.
filter	Set filter expression: [expressionitanert].
realtime	Bet realtime mode: [onjuff[2]. Monitur new leg entries
warboas	Set verhealty lavel: [lavel].
aflogas I	APT IN THE APPLICATION AND A STOCKARD

Figure 3: In Summary Mode, FWlogwatch gives administrators an overview of firewall logfile activity.

> netfilter -o text **2** --summary=no

FWlogwatch

Boris Wesslowski developed FWlogwatch for RUS-CERT at the University of Stuttgart, Germany. Version 1.0 [3] of the analysis tool has now been released under the GPL.

FWlogwatch has three operating modes: Log Summary Mode, Interactive Report Mode, and Realtime Response Mode. In Log Summary Mode, the program generates text or HTML pages with the summaries of the firewall logfile analysis (Figure 3). In Report Mode, FWlogwatch automatically generates incident reports that administrators can then forward to whoever has been affected by the incident.

In realtime mode, FWlogwatch responds to attacks by running scripts, sending email messages, or automatically modifying the firewall rules.

Listing 2: IPtables Log Analyzer

Listing 3: Fwlogwatch Realtime Mode

```
01 realtime_response = yes
02 parser = n
03 run_as = fwloguser
04 recent = 600
05 alert_threshold = 5
06 notify = yes
07 notification_script = /usr/
sbin/fwlw_notify
08 server_status = yes
09 bind_to = 127.0.0.1
10 listen_port = 8888
11 status_user = ralf
12 status_password =
i0QlAmOg4PrAA
13 refresh = 10
```

Admins can use the integrated web server for browser-based status monitoring of FWlogwatch.

FWlogwatch supports the IPchains (*i* option), Netfilter (*n*), IPfilter (*f*), IPFW (*b*), Cisco IOS (*c*), Cisco PIX (*p*), Netscreen (*e*), Windows XP (*w*), Elsa Lancom (*l*) and Snort (*s*) formats. The install is a simple make && make install && make install-config process. Boris Wesslowski has packages for Red Hat Linux and Debian on the Fwlogwatch homepage.

Admins can configure FWlogwatch's behavior using the configuration file, which has extremely informative comments. You can also configure FWlogwatch via the command line. The manpage explains the options. For example, the following command launches FWlogwatch in summary mode:

fwlogwatch -b -Pn -U ₽ 'Spenneberg.Com'-p -n -N -o ₽

fwlog	watch status
(before a start (Chillers)	Cardinatashi: thest second Carbook
In	formation
Darmor significant	Freing April 10 2010 IN CEUT 2004
Current line	Facing April 20 20 IN 48 CENT 2004
Farming time:	08080238
Faspens mode	Lop
Lines stars	1000
14ig	24
Obligischule ditruitionnact	19667
Epones in packet carbo	1
Entered in face makes	4
Determinent Opposite 1	Electrotroteche Christophene Dialesel
federate 18-3	CONTRACT IN CASE MANAGEMENT

Figure 4: The integrated FWlogwatch web server allows admins to monitor the current status of the firewall.

32

output.html -t -w ₽ /var/log/messages

The -Pn option enables the Netfilter parser. -U allows the user to specify a heading for the summary. The -o option specifies the output file; -w stipulates HTML output. -n and -N enable name resolution for hosts and services. The result is an HTML-formatted summary of the firewall logfiles.

Quick Response

The option of running FWlogwatch in realtime mode allows admins to react to logfile messages and simultaneously displays the current status in a browser window. FWlogwatch runs in the background as a daemon and monitors the logfile, reparsing the configuration file if it receives a *SIGHUP*. *SIGUSR1* tells the daemon to reopen the logfile. This feature is useful for rotating logfiles, for example.

Administrators can specify threshold values that define when FWlogwatch will react to logfile messages by launching alerts or response scripts. There are two important configuration options: *recent* (-*l*) defines the period of time to monitor, and *alert_threshold* (-*a*) defines the number of events within this time scope needed to trigger a response. Listing 3 shows a sample configuration. The example configures FWlogwatch for real-time mode with the Netfilter parser. The process runs under the user ID *fwloguser*.

If the threshold of five connections in 600 seconds is exceeded, Fwlogwatch performs a customizable action. Fwlogwatch sets up a web server on 127.0. 0.1:8888, where a user *ralf* can log in

Internation Operant Marcian	autor I these	same fictor	all i
Optic	Ins		
Parameter	Detrease	Carrent	Increases.
Alert Breckeld		4	
Discard impost.	1.14	80.00.20.00	
Measure count is public out to		1	
They arrise and a providers for publication and we			
Rollwork lane			
Industration Options Eacharts	asta i then	atoma i Maka	121

Figure 5: Admins can use a browser to configure FWlogwatch. The Alert Threshold specifies the number of messages needed to trigger the FWlogwatch response. with a password of *password*. FWlogwatch uses DES-encrypted passwords, which you can generate by typing *htpasswd -nb user password*. When the user logs in to this page, the view shown in Figure 4 appears. This page leads to other pages with a wide range of browser-based Fwlogwatch configuration options (Figure 5).

Choices

FWlogwatch has an enormous range of features, from a simple summary to a realtime mode with customizable responses. But the other tools we discussed in this article are well worth considering also. If you need powerful filtering, WFlogs may be a better option for your network. The IPtables Log Analyzer is an interesting choice for some situations because of its database support. The IPTables Log Analyzer gives system administrators the option of using SQL statements to search through firewall messages, rather than having to launch their searches from a web frontend.

	INFO			
[1]	IPtables Log Analyzer: http://www.gege.org/iptables/			
[2]	Wallfire project (WFlogs und 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]	WFlogs, Debian Woody packages: http://people.debian.org/~kelbert/			
[9]	GNU adns: http://www.chiark.greenend. org.uk/~ian/adns/			
HOR	Ralf Spenneberg is a freelance Unix/Linux trainer and author. Last year saw the			

AUT

ш

Ξ

release of his first book: "Intrusion Detection Systems for

Linux Servers". Ralf

materials.

has also developed various training