OpenBSD Firewall Reports Using Fwanalog Installation "Cookbook"

Abstract:

The purpose of this document is to show a firewall administrator using OpenBSD 2.9 with IPF how to setup and automate a reporting tool called Fwanalog to send emails on a daily and weekly basis. Fwanalog is a tool that generates some graphical HTML reports by analyzing your firewall logs. Target audience is beginning level OpenBSD firewall administrators possessing some basic Unix skills, including using vi and the ability to move around the file system. This article starts by covering benefits for automating log analysis and why to use Fwanalog as a reporting tool. Then we go into the "Cookbook" with step by step instructions for installing and configuring Fwanalog and some scripts that will send a summary report each day. Finally, I touch briefly on what you can do with your reports, including a few resources for additional help in reporting incidents and some suggestions for improvement on this particular reporting tool.

Logs and what they can do for you

In OpenBSD the logging of events are put in a file called /var/log/ipflog and daily rotated to a gzipped file in the same directory with a ipflog.X.gz extension . These logs are pretty useless by themselves and not much fun to read. By logging events and using log analysis tools to pull out the useful and significant events, we can get useful data, find problems, and fix them. In addition to using these analysis tools when you need to troubleshoot something, you can automate analysis tools and have reports sent to you on a nightly basis so you can establish long term trending. A good analysis tool doesn't have to be a very fancy, rather a quick and dirty summary in simple text is usually best for the busy administrator. Another good feature to have in an analysis reporting tool is some graphical charts in a web based HTML layout that is good for presenting to managers and executives. After searching for tools to do analysis on ipflogs there were many analysis tools that would analyze Checkpoint, Cisco, and system logs, but only a few free tools looked promising for ipflog analysis. Many did not report enough of the things that are important and many more were so fancy and difficult to install they were almost impossible to install.

Before going on to the tool that I chose I want to mention one promising tool that I looked at getting to work, fwlogwatch (http://cert.uni-stuttgart.de/projects/fwlogwatch/). Fwlogwatch is unique because it can be scheduled to look at the logs and send an alert or script a response to information in a log. Fwlogwatch's automated alerts were more geared towards Linux IPChains, so it was unreasonably difficult to configure it for OpenBSD and IPF. Fwlogwatch was not documented very well and would not install with the notes available. I would not recommend fwlogwatch for those of us who want something that will work without a major amount of tweaking. Fwlogwatch is worth keeping an eye on as it evolves for OpenBSD because of the alerting capabilities.

The tool that actually worked and fulfilled the basic requirements above is Fwanalog (http://freshmeat.net/projects/Fwanalog/). Fwanalog has graphs in HTML formatted reports as well as simple daily text file summaries, and was much easier to get running with only 1 prerequisite. The 1 pre-requisite, Analog, is the core program used by the Fwanalog reporting tool. Fwanalog is a script that uses the binaries of Analog, which was originally designed as a web server analysis and reporting tool. While Fwanalog creates adequate basic reports, it does not automate sending the report via email and still needs someone to manually log in, generate, and copy off reports. Fwanalog uses Analog, which was designed to be run on a web server.

Analog normally places the html reports in a published web folder. This works great if you are running a web server, but we are running these tools on a firewall and firewalls should not be running web servers on them.

Daily log reports are a very valuable tool. You can look at trends and have baselines to compare to when you think there may be a problem. In order to fulfill the basic requirement of having logs emailed on a daily basis we will setup to automatically send these reports. While this may sound simple, it has many steps which I have outlined below in a "Cookbook" style format with minimal fluff in between the steps, so you can get right in and configure your own firewall reporting tools.

HOW TO: Installing Fwanalog

Prerequisites:

- Have a method of getting the files from the Internet to your firewall. I prefer to run an interim ftp site to place the downloaded files since most locations only have them available on a http download site. I run Windows 2000 professional and I enabled ftp on it and download the files to a directory that is published to the ftp server. Getting ftp to work is outside the scope of this paper, but you will need to have ftp or another method to get the files from a http site on to your firewall.
- Have sudo enabled (to do this create the file /etc/sudoers and add a username ALL=(ALL) ALL line at the top for each user you want to have super user "root" access without logging in as root.
- User configuring Fwanalog must log in and have sudo rights

Download the Files needed:

Download Analog from the Analog home page. The default Analog that comes with OpenBSD (ver 4.1.6) did not work during my testing, so download the most current version which does work. At the time of this paper it the current version of Analog is 5.1.

Tar/GZ:
http://www.Analog.cx/Analog-5.1.tar.gz

While we are downloading our tools, lets get Fwanalog downloaded as well:

Tar/GZ:
http://tud.at/programm/Fwanalog/Fwanalog-0.4.1.tar.gz

(I had to put both of these on my PC first then Ftp it from my PC. You may skip this step if you download these directly to your firewall using another method. Once you have the two files downloaded above go ahead and log into your OpenBSD firewall and move the files to the firewall in the steps below. Be sure to read below to see where to place these files if you are downloading them directly to your firewall.)

Let's create a work environment for to get place fwanalog. This is where I placed my files, you may choose a different directory location or partition but be sure to modify all the rest of this document to match your location. Let's go ahead and make our working directory

```
sudo mkdir /home/common
sudo chmod 777 /home/common
sudo mkdir /home/common/Fwanalog
```

```
cd /home/common/Fwanalog
```

Then after creating and changing to that directory download from the ftp server:

```
ftp ftp.yourserver.com
username
password
cd /directory-where-file-Analog-5.1.tar.gz-is
bin
hash
get Analog-5.1.tar.gz
cd /directory-where-file-Fwanalog-0.4.1.tar.gz-is
get Fwanalog-0.4.1.tar.gz
exit
```

Install Analog-Step-by-Step

Analog must be installed for Fwanalog to run. Fwanalog uses the binary (executable program) files of Analog to process the data, passing in a modified log format, which then gets manipulated and output to a report based on IPF log security information rather than web server logs.

Extract Analog-5.1.tar.gz so we can compile and install it.

```
tar –xzvf /home/common/Fwanalog/Analog-5.1.tar.gz
```

This extracts Analog-5.1.tar.gz to the ./Analog-5.1 folder so if you are in /home/common it should be as below. We will need to type **make** to compile the program so we can install it.

```
cd /home/common/Fwanalog/Analog-5.1/src
make
```

(At this point you will see a bunch of gcc commands scroll down the screen ending in something that looks like this below)

```
gcc -O2  -DUNIX -c trees.c
gcc -O2  -DUNIX -c zutil.c
gcc -O2 -o ../Analog alias.o Analog.o cache.o dates.o globals.o hash.o init.o
init2.o  input.o macinput.o macstuff.o output.o output2.o process.o  settings.o
sort.o tree.o utils.o win32.o libgd/gd.o  libgd/gd_io.o libgd/gd_io_file.o
libgd/gd_png.o  libgd/gdfontf.o libgd/gdfonts.o libgd/gdtables.o  libpng/png.o
libpng/pngerror.o libpng/pngmem.o libpng/pngset.o  libpng/pngtrans.o
libpng/pngwio.o libpng/pngwrite.o  libpng/pngwtran.o libpng/pngwutil.o
pcre/pcre.o  zlib/adler32.o zlib/crc32.o  zlib/deflate.o zlib/trees.o zlib/zutil.o -lm
***
***IMPORTANT: You must read the license before using Analog
***
```

Now move the extracted files to the /usr/local/bin so the paths all work properly and we can actually run the program just by typing Analog without the full path.

```
sudo cp -r  /home/common/Fwanalog/Analog-5.1/* /usr/local/bin
        enter your password for sudo to work
```

Lets verify that the path Analog works. (need to run this as sudo since that is how you will call the command later)

```
sudo which Analog
```

Should get a response /usr/local/bin. If not, go back and make sure the **sudo cp** above worked.

Install-Fwanalog Step-by-Step

We first need to extract the file we downloaded earlier and put it /home/common/Fwanalog:

```
tar –xzvf /home/common/Fwanalog/Fwanalog-0.4.1.tar.gz
```

Change to the directory where it extracted:

```
cd /home/common/Fwanalog/Fwanalog-0.4.1
```

You can view the readme by typing:

```
more README
```

Since this is and OpenBSD box we type to copy the options file to the right spot:

```
cp Fwanalog.opts.openbsd Fwanalog.opts
```

Edit our output directory and create that directory so we are ready to run the script:

```
vi Fwanalog.opts
----change  line 10
outdir="/root/Fwanalog.out"
to
outdir="/home/common/reports/Fwanalog/Fwanalog.out"
----change lines for full path only if necessary for Analog, zegrep, and perl
(save and exit)
:wq!
Mkdir /home/common
mkdir /home/common/reports
mkdir /home/common/reports/Fwanalog
```

Testing the script manually:

We are ready to test the script manually before we schedule it to run automatically. Plan on the script running for 10 minutes if you have some large logs and a slow processor. I ran this on a Pentium II 266, with 30Mb of logs, and it took between 5-10 minutes. Of course, an Athlon 1.5Ghz with a fast IDE ATA U100 or SCSI hard drive will process these logs much more quickly.

Run script manually

```
sudo /home/common/Fwanalog/Fwanalog-0.4.1/Fwanalog.sh
```

When it returns you back to the command prompt, look for any errors and correct them as needed. If there are no errors you will just be returned to the command prompt and reports will be in the report directory.

View the Report

The report, or in this case reports, are output to:

```
/home/common/reports/Fwanalog/Fwanalog.out
```

there are a bunch of reports in this directory, but you need to read more of this document to make sure you know how to access them.

So how do I view my reports?

If you were running a web server on your firewall, it would be pretty easy to view these files, since the reports are in html format. I suggest you do not run a web server on your firewall for security reasons, so we need to move these files off the firewall to view them some other way. There are three main other ways to go about this. We could use ftp and copy them off, Secure Copy (scp) to copy them to another Unix box that has a web server running, or the third way and my preferred way is to email them off on a scheduled basis. You may choose to copy them to a secure web server for long term trending that can be shared by an IT team. I tend to read my email more regularly than I check web site reports, so I prefer email reports.

Weekly and Summary Reports

Weekly and summary reports are different than daily reports. Daily reports, as we mentioned during the introduction, were simple text files and are not what you would usually give to managers or executives that prefer a graph. Weekly summaries are the graphs and html reports that are viewable in a web browser.

Scheduling fwanalog reports to be sent out via email is a several part process, but it is worth the effort compared to doing this manually. We will first create a script to automate the running of the Fwanalog.sh script then tar and gzip (compress) all the files so we have a single attachment to send. Then at the bottom of the script, there is a line that sends the email. Finally, we must edit the crontab to scheduled the job.

Create the script Fwanalog.automate.weekly.sh

```
vi /home/common/Fwanalog/ Fwanalog.automate.weekly.sh
```

Enter the following into this script:

```
# the following line calls Fwanalog.sh to run
/home/common/Fwanalog/Fwanalog-0.4.1/Fwanalog.sh
# the following will tar and gzip the output of Fwanalog.sh
sudo tar -c -f /home/common/reports/Fwanalog/Fwanalog.report-all.tar.gz -z
/home/common/reports/Fwanalog/Fwanalog.out/*
# the following will email Fwanalog.report-all.tar.gz
# I used references from:
# http://www.shelldorado.com/articles/mailattachments.html
# to do this:
uuencode /home/common/reports/Fwanalog/Fwanalog.report-all.tar.gz
Fwanalog.report-all.tar.gz | mail -s Fwanalog.report.firewallname
user@yourdomain.com
```

Exit and save **:wq!**

We will put this script in a crontab later so it gets run on a schedule routine. At this point you should run the script you just created to verify it works.

```
sudo sh /home/common/Fwanalog/ Fwanalog.automate.weekly.sh
```

Be patient. If you have a large log file it will take a while. Just like the weekly reports fwanalog is going through a large file and it may take 10 or more minutes. If you have problems try the same steps to find the problem as you did on the Weekly section.

Preparing Preferences for Sending Email:

Before sending mail modify who the email will appear to be sent from. This will help if you have several firewalls or systems with IPF running. Having a unique from address in the email makes it much easier to sort your email and find reports from a specific firewall. The default from address for OpenBSD is Charlie Root. Having 2 or 3 emails from Charlie Root is pretty meaningless if you have several firewalls sending information everyday. It is much better when the reports coming from a firewall called FWNEWYORK to appear in the email from column as “root@fwnewyork” . To change this setting we need to modify the user comments of root, this is also know as GECOS field (some important reason I am sure…historically speaking that is).

```
sudo usermod -c "root@fwspare " -v root
```

Scheduling Weekly Summary Reports

We have to edit the crontab, which is the Unix version of what Microsoft Windows calls the scheduler. I will not explain a whole lot of how this all works but I will let you know you can get more information about it by typing:

```
man –a crontab
```

This will show you all the manual pages for crontab. The second man page is the important one because it tells you the options for crontab. For this job we will run it on Sunday night at 2350hours. Try to choose the best time to run fwanalog depending on the size of your logs. If you have a small log file normally run it before Midnight on Sunday because it is the last day of the week. If it takes 10 or more minutes to run the script you might end up with a blank report when Monday arrives and the logs are switched and are now empty. Here is how you edit the crontab to add the script above:

```
sudo crontab –e
```

This starts the vi editor. There are 6 important columns you will see.

Minute	Hour	Day of Month	Month	Day of Week	Command to Run
50	**23**	*****	*****	**7**	**/bin/sh /home/common/Fwanalog/Fwanalog.automate.weekly.sh**

Put the following in each column:

Minute=50
Hour=23
DayofMonth=*
Month=*
DayofWeek=7
Command to run= /bin/sh /home/common/Fwanalog/ Fwanalog.automate.weekly.sh

This will run our script every Sunday night at 11:50 p.m. If you want to test it before it actually runs on Sunday, change the time to run about 5 minutes ahead or your current time and day of the week, let it run and check your email. Then remember to switch the crontab back to run at 11:50 p.m.

Daily Reports

The html report is nice, but it requires some effort to view it once you get it. You need to use a tool like winzip and uncompress the file and change to a directory to view it . This takes time and effort. Looking at log reports needs to be done more frequently than 1 time per week and very easy to do. The daily report is easy to view if it is a text based email attachment. Scheduling daily reports requires a simple script and a crontab entry similar to the Weekly reports.

Setting up the script for Daily Reports

We need to create a script file and edit it to setup the process.

```
vi /home/common/Fwanalog/Fwanalog.automate.daily.sh
        # Run the Fwanalog.sh script with the -t option to only run today's results.
        sudo /home/common/Fwanalog/Fwanalog-0.4.1/Fwanalog.sh –t
        #  THIS LINE WILL TAKE THE TODAY.TXT OUTPUT OF
        FWANALOG.SH AND SENDS IT AS AN EMAIL ATTACHMENT TO
        THE EMAIL ADDRESS BELOW EDIT YOUR EMAIL ADDRESS AS
        NEEDED
        uuencode /home/common/reports/Fwanalog/Fwanalog.out/today.txt
        daily.Fwanalog.report.txt | mail -s daily.Fwanalog.report.fwname
        user@yourdomain.com
Save and Exit ( :wq!)
```

We will put this script in a crontab later so it gets run on a schedule routine. At this point you should run the script to see what kind of output you will get:

```
sudo sh /home/common/Fwanalog/ Fwanalog.automate.weekly.sh
```

Be patient, if you have large log files it will take a while. It is running the entire script and may take 10 or more minutes. This one is slightly faster since you put the **–t** option on the Fwanalog.sh script which tells the script you are only interested in parsing today's logs. Any email problems should have been fixed in the steps above, so if you skipped to this section go back and read.

Scheduling Daily Reports in Crontab

Again, we have to edit the crontab which is the Unix version of what Microsoft Windows calls the scheduler. We will run /home/common/Fwanalog/ Fwanalog.automate.daily.sh every night except Sunday at 2350hours. Here is how you edit the crontab to add the script above.

```
sudo crontab –e
```

Again this starts the vi editor.

Minute	Hour	Day of Month	Month	Day of Week	Command to Run
50	**23**	*****	*****	**0-6**	**/bin/sh /home/common/Fwanalog/ Fwanalog.automate.daily.sh**

Put the following in each column:

Minute=50
Hour=23

```
DayofMonth=*
Month=*
DayofWeek=0-6
Command to run= /bin/sh /home/common/Fwanalog/ Fwanalog.automate.daily.sh
```

This will run the script every night at 11:50 p.m. Monday through Saturday. If you want to test it before it actually runs change the time to run about 5 minutes ahead of your current time, let it run. Go check your email and make sure you have a report there. When you get it working, remember to switch the schedule time in crontab back to run at 11:50 p.m.

Setting permissions on the report directory:

I bet you almost forgot about setting the permissions back on the directory where we create our reports, /home/common. Before we are done we need to set the permissions so only root or super users have access to the information in this directory. Type the following command:

```
sudo chmod 440 /home/common
```

That should do it. You can go back up and test your cron job again to make sure you still get an emailed report.

Customizing the Report

There is a file /home/common/Fwanalog/Fwanalog-0.4.1/Fwanalog.Analog.conf.local that has a few settings that you can change to modify how much data you get from each analysis. Read the entire document because it tells you what each of the lines does. This config file is how Fwanalog is able to get Analog to report on firewall logs. This is done in a general sense by substituting information for normal web server log information.

Limitations of Fwanalog

In looking at various reporting tools that do similar reporting, a few things came out that Fwanalog doesn't do. Fwanalog does not look at the 8th field in the ipflog that says whether it is a "b" for blocked packet or a "p" for passed packet. Another limitation is the flexibility of parsing more than one set of logs. This had to be setup manually as two separate reports which will probably work most of the time. For those of you who are using this tool as a logging tool to locate use of network protocols it would be nice to know the top 10 protocols in use on the network (passed traffic). As with most open source tools, Fwanalog has many steps for setting up and getting it configured to do what you need it to do. It took more than 3 hours to come up with the working configuration process to create the reports and send them via email using crontab to schedule the task.

.

What Fwanalog does well

Fwanalog does generate a easy to read quick text based daily report and a HTML report with some nice graphs. No matter how useful the text base report is to the technical firewall engineers, the managers and executives really like the graphs and HTML reports. The top 10 reports are good for identifying the top rejected packets, if the firewall is only logging blocked traffic.

What to do with the Report

The report helps us find a pattern in the massive amount of information the logs hold in raw format. No longer are we trying to find our own patterns out of some 240,000 log entries. The report tells us which protocol/host is being logged 34% of the total traffic. Next you have to use experience and some research to know what to do with your new information. I suggest the first few weeks you look at the reports and go look at the logs and research what you are dropping. Don't get too carried away by accusing others of doing something wrong just yet. Let the reports help point out things that you or your Internet neighbors are doing wrong. For instance, I noticed that port 123 (Network Time Protocol) was getting dropped on one of my firewalls. I went and looked at the firewall rules /etc/ipf.rules and found that I had a syntax error that made my permit rule not work. I fixed my configuration error and no longer see dropped packets on port 123.

The other key thing to remember is to double-check your results. Make sure you are seeing what you think you see and verify it with someone else before you make false accusations. If for instance you see a ton of TCP port 25 traffic and think that someone is trying to telnet or hack your system, look to see if there is a DNS error or if the box is supposed to be a mail server. I have had people tell me that port 25 is telnet and it is actually SMTP for email. The point is, check your services and know what your systems are supposed to be doing.
If you are sure you see someone doing something they should not be doing, you should follow some guidelines and use the resources listed below:

SANS Reading Room Incident Handling http://rr.sans.org/incident/incident_list.php
NIPC FBI Cyber Incident Reporting Guidelines http://www.nipc.gov/incident/cirr.pdf
IANA Port Assignments http://www.iana.org/assignments/port-numbers

After looking into all the Official sites that have port-numbers, you need to check out some "unofficial" sites for those common unwanted protocols that you may or may not want to see crossing your firewall.

Unofficial Port to Application Usage http://www.chebucto.ns.ca/~rakerman/port-table.html
Snort does a good job of letting you enter a TCP or UDP port number and tell you what application is running on that port. Ports DB http://snort.sourcefire.com/ports.html.

It is not reasonable to hunt out all problems and probes. Instead use this tool to watch for probes and traffic that one day become abnormal, and choose the highest risk events and biggest threat to fix first. In order to do find patterns you need to have a history of logs and reports to compare to (a baseline). This is another reason why automating this process is so important, if you only do it manually you may not have a good baseline trend. If you have a long history of logs and know you normally get 1,000 dropped packets of ICMP pings and today you see that you are getting 10 times more than you were before and have not done anything to precipitate this new traffic, you may need to dig into the systems and logs and see what is happening. This is an extreme example and many probes will be much less obvious. For real intrusion detection you need to use firewall reporting tools along with other tools like the Open Source Free IDS tool snort (www.snort.org) to supplement your Perimeter Network Security solution.

Summary:

Fwanalog is not the only firewall log analysis reporting tool, nor is it necessarily the best. It does not work as an all inclusive IDS tool, since it does not send alert or trigger actions based on particular information in the logs. If I were to make one major improvement on this tool, I would improve the installation offering an interactive wizard for configuration.

"Cyber Incident Reporting Guidelines". National Infrastructure Protection Center. Federal Bureau of Investigations. Online. 19 January 2002
http://www.nipc.gov/incident/cirr.pdf

Sonnenreich, Wes and Yates, Tom. Building Linux and OpenBSD Firewalls. New York, NY: Wiley Computer Publishing, 1999. 211-247

SANS Institute. Intrusion Detection The Big Picture – Part II. Oakland, CA: Hal Pomeranz, 2001. 23

"Setting up a Firewall with IPF, IPNAT and OpenBSD". SANS Information Security Reading Room. Online. 17 March 2002
http://rr.sans.org/firewall/IPF.php

"Port Numbers." Internet Assigned Numbers Authority. Online. 19 January 2002
http://www.iana.org/assignments/port-numbers

"Ports DB." Snort The Open Source Network Intrusion Detection System, Snort.org Marty Roesch. Online 17 March 2002
http://snort.sourcefire.com/ports.html

"Fwlogwatch – Rus-Cert". Rus-Cert Universität Stuttgart. Online 17 March 2002.
http://cert.uni-stuttgart.de/projects/fwlogwatch/

"Fwanalog". Project of Balázs Bárány. Online 17 March 2002
http://freshmeat.net/projects/Fwanalog/

"Analog". Stephen Turner. Online 17 March 2002
http://www.Analog.cx/

"Sending files as mail attachments". Heiner's Shelldorado. Online 17 March 2002
http://www.shelldorado.com/articles/mailattachments.html

"Snort" Snort.org Marty Roesch. Online 17 March 2002.
http://www.snort.org