

Using and understanding zalog.txt

Here is an example of the file *zalog.txt* if you have done a default installation of ZoneAlarm it should be found in C:\WINDOWS\Internet Logs

ZoneAlarm Logging Client v4.5.538.000

Windows XP-5.1.2600-Service Pack 1-SP These three lines are the header and just tell you about ZoneAlarm, Windows and how the information is formatted

type,date,time,source,destination,transport

FWROUTE,2004/02/01,19:34:40 -5:00 GMT,209.254.50.93:1027,192.42.93.32:53,UDP

FWOUT,2004/02/01,19:34:40 -5:00 GMT,209.254.50.93:1027,192.52.178.30:53,UDP

FWIN,2004/02/01,20:05:26 -5:00 GMT,209.251.126.1:0,209.254.50.93:0,ICMP (type:8/subtype:0)

FWIN,2004/02/01,20:42:20 -5:00 GMT,127.0.0.1:80,209.254.50.93:1349,TCP (flags:AR)

PE,2004/02/01,20:31:46 -5:00 GMTGMT, Download Accelerator Plus,66.94.216.250:53,N/A

ACCESS,2004/02/01,19:35:36 -5:00 GMTGMT, The firewall rules for named.exe allow an outgoing UDP connection to 208.185.54.61:DNS.,N/A,N/A

This is the the part of the entry that tells you what kind of information was blocked or logged. Below there are some definitions

FWIN: indicates that the firewall blocked an inbound packet of data coming to your computer. Some, but not all, of these packets are connection attempts.

FWOUT: indicates that the firewall blocked an outbound packet of data from leaving your computer.

FWROUTE: the firewall blocked a packet that was not addressed to or from your computer, but was routed through it.

FWLOOP: the firewall blocked a packet addressed to the loopback adapter (127.0.0.1)

LOCK: the firewall blocked a packet due to a lock violation

PE: indicates that a popup appeared asking for permission for a program to access the network.

ACCESS: an application was blocked because it did not have access permission

MS: MailSafe quarantined a file attachment

Next you have the date and time. Some people have asked why a 24 hr clock is used instead of the 12hour clock.

The reason is that using the 24 hr clock puts everyone on the same clock and geography doesn't matter. This way services that use these logfiles can use the times to help crunch the data. If everyone reports a ping from a

single computer but the times are all one hour apart on the 12 hr clock, no report will be sent. But using the 24 hr

clock, it will be seen that all the pings actually came at the same instant, but across many timezones, so a report

will be sent.

Next you have where the packet originated from. Either an IP address, a program, or in the case of the Pro and Plus versions of ZoneAlarm, an Expert rule. If it is an IP address there are two parts to it. First is the IP address then there is a colon ":" and then there is a port number. First for the IP address. There are a few IP address's that belong to you and do not go out over the internet. They are

- 0.0.0.0 this is your computer and there seem to be a debate if this is actually a valid address. I just know it shows up
- 127.0.0.1 this is the loopback address
- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255 These three ranges are reserved for LAN use. Everyone has them and they are private.
- 192.168.0.0 - 192.168.255.255

There are others but you will see these most

You can lookup the IP at [Domain Dossier](#)

The ports can be looked up at [IANA Port Assignments](#). Just be aware that some applications can be made to use any port, regardless of what its intended to be used for.

Then you have the destination. For the most part this will be your computer, unless its an outbound (FWOUT) or Routed (FWROUTE) packet. You can use the same tools as the inbound packets.

And lastly you have the protocol that was used. Mostly you will see TCP or UDP but you can see many others. A full list is [Here](#)

Some of the flags are listed below for the different protocols.

The TCP flags are:

- S (SYN),
- F (FIN),
- R (RESET),
- P (PUSH),
- A (ACK),
- U (URGENT),
- 4 (low-order unused bit),
- 8 (high-order unused bit)

The SYN-flag is only set in the first packet initiating a TCP connection. This happens only when trying to make a connection.

The FIN-flag is when you terminate a connection

ICMP types:

- 0 - Echo Reply
- 3 - Destination Unreachable
- 4 - Source Quench
- 5 - Redirect

- 8 - Echo Request
- 9 - Router Advertisement
- 10 - Router Solicitation
- 11 - Time Exceeded
- 12 - Parameter Problem
- 13 - Timestamp Request
- 14 - Timestamp Reply
- 15 - Information Request
- 16 - Information Reply
- 17 - Address Mask Request
- 18 - Address Mask Reply

That pretty much explains how to read the logfile. Now on how you can use it.

First there are a few programs that will help in this. One is [ZoneLog](#) and another is [VisualZone](#)

Anything that says FWROUTE you can pretty much ignore, unless you are getting alot of them. If you are, then you are probably behind a router, and if you turn off the Broadcast / Multicast in it, they will probably stop.

If you see PE, then that is a request for a program that is wanting access. If it happens over and over for the same program, you might want to consider letting it remember, or making some rules for it.

Access usually tells you a program was blocked, but it can also be used to tell you an expert rule made this entry mandatory.

Also look at the number of attempts from a single IP address, it could mean someone is trying to hack into your system or that you have a connection that you are blocking that you keep trying to use.

You can also use this list when you are creating expert rules for programs. If you have no idea where to start, create a rule that blocks everything, then try to access the net. Look in here and find out where it was going (destination IP address) and look it up at Domain Dossier and see if it needs to connect there. If it does, then add it to a new expert rule (before the blocking one) and let that traffic through, both to that IP address and to the port.

Then try the program again. If it fails look in the log for a new entry, and go through the process again. This is kind of cumbersome, but most companies will not give you the information that you need to do this easily. Some do, so go to their home page and look in the FAQ's for port numbers and or IP address's that you need to allow first. Then if you don't find it go through this process.