Firewall: Howto interpret firewall messages in your system log

How to interpret a message from the firewall in your logs:

Feb 23 07:37:01 - kernel: IP fw-in rej eth0 TCP 12.75.147.174:1633 100.200.0.212:23 L=44 S=0x00 I=540

There is a LOT of information in this just one line. Let break out this example so refer back to the original firewall hit as you read this.

```
    * This firewall "hit" occurred on: "Feb 23 07:37:01"
    * This hit occurred on the "IP" or TCP/IP protocol
    * This hit came IN to ("fw-in") the firewall
      * Other logs can say "fw-out" for OUT or "fw-fwd" for FORWARD
    * This hit was then "rejECTED".
      * Other logs can say "deny" or "accept"
    * This firewall hit was on the "eth0" interface (Internet link)
    * This hit was a "TCP" packet
    * This hit came from IP address "12.75.147.174" on return port "1633".
    * This hit was addressed to "100.200.0.212" to port "23" or TELNET.
      * If you don't know that port 23 is for TELNET, look at your /etc/services file to
see what other
        ports are used for.

    * This packet was "44" bytes long (L=44)
    * This packet did NOT have any "Type of Service" (TOS) set
      --Don't worry if you don't understand this; not required to know
      * divide this by 4 to get the Type of Service for ipchains users
    * This packet had the "IP ID" number of "54054"
      --Don't worry if you don't understand this; not required to know

    * This packet had a 16bit fragment offset including any TCP/IP packet
      flags of "0x0040"
      --Don't worry if you don't understand this; not required to know
      * A value that started with "0x2..." or "0x3..." means the "More Fragments" bit
was set
        so more fragmented packet will be coming in to complete this one BIG packet.
      * A value which started with "0x4..." or "0x5..." means that the "Don't Fragment"
bit is set.
      * Any other values is the Fragment offset (divided by 8) to be later used to
recombine
        into the original LARGE packet

    * This packet had a TimeToLive (TTL) of 254.
      * Every hop over the Internet will subtract (1) from this number. Usually, packets
```

```
will
        start with a number of (255) and if that number ever reaches (0), it means that
realistically
        the packet was lost and will be deleted.
```

Unique solution ID: #1061
Author: Dingetje
Last update: 2004-12-01 20:48