

## New in v5.4 - two new fields in E2guardian log formats 7 & 8.

### searchterms and extflags

**Searchterms** has the searchterms used in a search that has been detected. This to make it easier to report on searchterms used. Since most users launching point is via a search engine, this is likely be the most useful thing to indicate trends in users' browsing.

### Extflags (extension flags)

The e2guardian access.log has not held the listening port, information on whether the request was proxied or transparent, or an indication of how the 'user' and 'group' has been arrived at.

To add all this information in the normal way would require the addition of at least 4 fields to the log, so to avoid this and keep the log as compact as possible a single 'extflags' field is added in the following format!"

listening#port!flags\$%&'T'()%'S' + )!user#source!group#source

where!"

**listening\_port** is the port number e2g was listening on.

**flags** are!"

first character!

& , proxy request

T , Transparent request

( , (-. & request

second character

\* , \* TT& request

S " SS/ \$\* TT&S0 request

+ , request within + (T +

so!" '&\*' standard proxy http request

'&S' proxy https request \$no + (T + 0

'&+' request within + (T + session over proxied session

'T\*' transparent http request

'TS' transparent https request \$no + (T + 0

'T+' request within + (T + session over transparent session

**user\_source** is the source for the 'user' field

e.g. dnsa, port, ip, ntlm

**group\_source** is the source for the filter group

This maybe hard coded \$e.g. dnsa, def0 or the name of the maplist group defined in e2guardian.conf used to determine the group \$e.g. ipmap, portmap0.

1xamples2

3 4!TS!dnsa!dnsa

3 4!T+!ip!ipmap

3535!&\*!dnsa!dnsa

3535!&+!dnsa!dnsa

3535!T\*!dnsa!dnsa

3535!T\*!!def

353 !&\*!port!portmap

353 !&\*!ip!ipmap