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([P|T|I][H|S|M]:user_source:group_source

where:-

listening_port is the port number e2g was listening on.

flags are:-

first character:
P – proxy request
T – Transparent request
I – ICAP request

second character
H – HTTP request
S - SSL (HTTPS) request
M – request within MITM

so:- 'PH' standard proxy http request
'PS' proxy https request (no MITM)
'PM' request within MITM session over proxied session
'TH' transparent http request
'TS' transparent https request (no MITM)
'TM' request within MITM 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, def) or the name of the maplist group defined in e2guardian.conf used to determine the group (e.g. ipmap, portmap).

Examples–

8443:TS:dnsa:dnsa
8443:TM:ip:ipmap
8080:PH:dnsa:dnsa
8080:PM:dnsa:dnsa
8080:TH:dnsa:dnsa
8080:TH::def
8084:PH:port:portmap
8084:PH:ip:ipmap