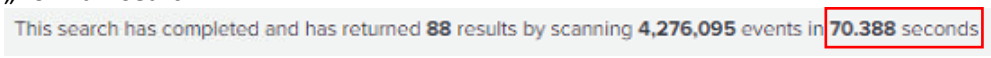
McAfee/SkyHigh Web Gateway – Splunk integration – mcafee:webgateway:custom Log Format - Version 0.3 05.Dec.2023 – https://proxy-test.com/swg_cheatsheet.pdf

Log line structure (an example, your log structure can look different):

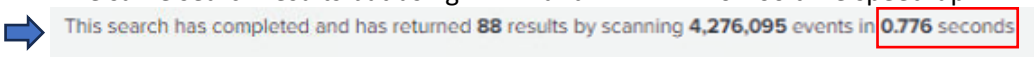
```
2021-02-26 14:36:46.449 -0600 s=200 ac=allowed src=192.168.2.1 p=https m=GET d=s1.googleapis.com dp=443 bi=563 bo=4156 dur=38 rt=17
timestamp                     status action      source_ip       proto   method destination          dest_port bytes_in bytes_out duration runtime

up="/v4/threatListUpdates" ua="FF86-10.0" c=it dip=142.250.185.5 ckex=112 skex=112 cntx
url_path                   user_agent     category dest_ip      client_key_exchange server_key_exchange ssl_client_context_is_applied

scc=1302 ssc=1302 sslcp=1.3 sslsp=1.3 sslicn="GTS CA 1O1,GlobalSign" sslcn="upload.video.google.com" crtdays=-52
ssl_client_cipher ssl_server_cipher ssl_client_proto ssl_server_proto ssl_issuer_common_name        ssl_common_name                cert_remaining_days

srcp=62407 mbmismatch ctmt0                                                                  rul="L" rnf=41 rne=104 conrt=0
source_port magic_bytes_mismatch both_content_type_and_ensured_type_are_empty                last_rule rules_fired rules_evaluated connection_runtime

bfc=524 btc=4418 tunnel psrcip=192.168.2.10 psrcp=42550 rqv=2.0 rsv=2.0 r=0
bytes_from_client bytes_to_client tunnel proxy_source_ip proxy_source_port request_http_version response_http_version reputation

tdns=0 tcon=0 tre=34 text=34 t=18.18.22.11
time_dns time_connect time_rule_engine time_in_externals timers (extended)
```

How to speed-up your searches and reports:

„normal“ search:



The same search results but using TERM and PREFIX – 10-100 time speed-up:



Normal search: based on extracted fields	Improved: fast search/reporting: based on raw TERM –> **3-10 times faster**
src=10.20.30.40 dest=example.com	TERM(src=10.20.30.40) TERM(d=example.com)
src=10.20.30.* dest=*example.com	TERM(src=10.20.30.*) TERM(d=*example.com)
web_reputation > 50	TERM(r=50) OR TERM(r=51) … OR TERM(r=127)
action=blocked	TERM(ac=blocked)

Normal report: based on extracted fields	Improved: based on TERM/PREFIX -> **50-100 times faster**
timechart count by category	| tstats count by PREFIX(c=) _time | rename c= AS categories | timechart sum(count) by categories