

# Fortianalyzer SQL tables list

Reference: <https://docs.fortinet.com/document/fortigate/6.4.0/fortios-log-message-reference/384955/traffic>

Table 1. Table columns for Traffic Log

Column Name	Description
id	Numerical, 28 number, differ per row e.g. 1612273830 epoch time, the rest unclear
bid	Numerical, 9 numbers, same for the table for all rows
dvid	Numerical, 4 numbers,
itime	Numerical, epoch time, e.g. 1612273830, stays the same for all rows (?)
dtime	Numerical, epoch, e.g. 1612281024, changes but not with each row, every few rows, probably end time
euid	Numerical, 1 number
epid	Numerical, varies
dsteuid	Numerical, all = 0
dstepid	Numerical, the same for all rows
logflag	Numerical, differs but not each row, some rows are missing it
logver	Numerical, the same for all rows, e.g. 60
proto	Numerical, IP/TCP protocol number
vrf	Empty
logid	Numerical, log type, e.g. 0000000015, 000000013
type	String, e.g. traffic
subtype	String, e.g. forward
level	String, e.g. notice
action	String, e.g. deny, start, close
policyid	Numerical, e.g. 2
sentbyte	Numerical, variable
rcvdbyte	Numerical
sessionid	Numerical
srcport	Numerical
dstport	Numerical

Column Name	Description
transport	EMpty
trandisp	String, <b>snat</b>
duration	Numerical
sentpkt	Numerical
rcvdpkt	Numerical
utmaction	String, <b>block</b>
slot	Empty
srcip	IP address
dstip	IP address
srcname	Empry
dstname	Empty
service	String, <b>HTTP</b>
user	empty
poluuid	Hex long number
app	String, <b>HTTP, HTTPS, DNS, TeamViewer</b>
appcat	String, <b>unknown, Remote.Access</b>
tranip	{}
unauthuser	{}
unauthusersource	{}
vpn	{}
srcintf	String, <b>bla_INT</b>
dstintf	String, <b>bla_EXT</b>
group	{}
custom_field1	{}
srcintfrole	<b>undefined</b>
dstintfrole	<b>undefined</b>
fctuid	{}
wanoptapptype	{}
wanin	Numerical, <b>3317, 0</b>
wanout	Numerical, differs from <i>wanin</i>
lanin\	Numerical, <b>164</b>
lanout	Numerical, equals to <i>lanin</i>