High Performance Network Security

FortiAnalyzer - Dataset Reference

VERSION 5.4.1

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

June 29, 2016

FortiAnalyzer 5.4.1 Dataset Reference

05-541-310522-20160629

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-06-29	Updated for version 5.4.1.

Introduction

This document provides information about the various types of FortiAnalyzer datasets.

Understanding Datasets and Macros

FortiAnalyzer datasets are collections of log messages from monitored devices.

Charts in FortiAnalyzer are generated based on the datasets. To create a chart, you can use the predefined datasets, or you can create your own custom datasets by querying the log messages in the SQL database on the FortiAnalyzer unit. Both predefined and custom datasets can be cloned, but only custom datasets can be deleted. You can also view the SQL query for a dataset, and test the query against specific devices or log arrays.

You can create custom reports that contain macros that are created based on predefined and custom datasets. Macros are used to dynamically display the device log data as text in a report. They can be embedded within a text field of a paragraph in a report layout in XML format. Macros display a single value, such as a user name, highest session count, or highest bandwidth, and so on.

For more information about how to create datasets, charts, and macros, see the FortiAnalyzer *Administration Guide.*

Dataset Reference List

The following tables list the available predefined data sets reported by FortiAnalyzer. For documentation and technical support reference purposes, thess tables contain the dataset names, SQL query syntax for each dataset, and the log category of the dataset.

Dataset Name	Description	Log Category
Traffic-Bandwidth-Summary-Day-Of-Month	Traffic bandwidth timeline	traffic

```
select
   $flex_timescale(timestamp) as hodex,
   sum(traffic_out) as traffic_out,
   sum(traffic_in) as traffic_in
from
   ###(select $flex_timestamp as timestamp, sum(coalesce(sentbyte, 0)) as traffic_out, sum
       (coalesce(rcvdbyte, 0)) as traffic_in from $log where $filter and logid_to_int
       (logid) not in (4, 7, 14) group by timestamp having sum(coalesce(sentbyte,
       0)+coalesce(rcvdbyte, 0))>0 order by timestamp desc)### t group by hodex order by
       hodex
```

Dataset Name	Description	Log Category
Session-Summary-Day-Of-Month	Number of session timeline	traffic

```
select
   $flex_timescale(timestamp) as hodex,
   sum(sessions) as sessions
from
   ###(select $flex_timestamp as timestamp, count(*) as sessions from $log where $filter
       and logid_to_int(logid) not in (4, 7, 14) group by timestamp order by timestamp
       desc)### t group by hodex order by hodex
```

Dataset Name	Description	Log Category
Top-Users-By-Bandwidth	Bandwidth application top users by bandwidth usage	traffic

```
select
   coalesce(
      nullifna(`user`),
      nullifna(`unauthuser`),
      ipstr(`srcip`)
   ) as user_src,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth,
   sum(
      coalesce(rcvdbyte, 0)
   ) as traffic_in,
   sum(
      coalesce(sentbyte, 0)
   ) as traffic_out,
   count(*) as sessions
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
group by
   user_src
having
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   )> 0
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
Top-App-By-Bandwidth	Top applications by bandwidth usage	traffic

```
select
   app_group_name(app) as app_group,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth,
   sum(
      coalesce(rcvdbyte, 0)
   ) as traffic_in,
   sum(
      coalesce(sentbyte, 0)
   ) as traffic_out,
   count(*) as sessions
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and nullifna(app) is not null
group by
   app_group
having
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   )> 0
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
Top-User-Source-By-Sessions	Top user source by session count	traffic

```
select
   coalesce(
      nullifna(`user`),
      nullifna(`unauthuser`),
      ipstr(`srcip`)
   ) as user_src,
   count(*) as sessions
```

```
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
group by
   user_src
order by
   sessions desc
```

Dataset Name	Description	Log Category
Top-App-By-Sessions	Top applications by session count	traffic

```
select
   app_group_name(app) as app_group,
   count(*) as sessions
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and nullifna(app) is not null
group by
   app_group
order by
   sessions desc
```

Dataset Name	Description	Log Category
Top-Destination-Addresses-By-Sessions	Top destinations by session count	traffic

```
select
   coalesce(
      nullifna(
         root_domain(hostname)
      ),
      ipstr(dstip)
   ) as domain,
   count(*) as sessions
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
group by
   domain
order by
   sessions desc
```

Dataset Name	Description	Log Category
Top-Destination-Addresses-By-Bandwidth	Top destinations by bandwidth usage	traffic

```
select
```

```
   coalesce(
      nullifna(
         root_domain(hostname)
      ),
      ipstr(dstip)
   ) as domain,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth,
   sum(
      coalesce(rcvdbyte, 0)
   ) as traffic_in,
   sum(
      coalesce(sentbyte, 0)
   ) as traffic_out
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and coalesce(
      nullifna(
         root_domain(hostname)
      ),
      ipstr(`dstip`)
   ) is not null
group by
   domain
having
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   )> 0
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
DHCP-Summary-By-Port	Event top dhcp summary	event

```
drop
   table if exists pre_clt_list;
drop
   table if exists cur_clt_list;
drop
   table if exists allocated_ip; create temporary table pre_clt_list as ###(select concat
       (interface, '.', devid) as intf, mac from $log where $last3day_period $filter and
       logid_to_int(logid) = 26001 and dhcp_msg = 'Ack' group by interface, devid,
       mac)###; create temporary table cur_clt_list as ###(select concat(interface, '.',
       devid) as intf, mac from $log where $filter and logid_to_int(logid) = 26001 and
       dhcp_msg = 'Ack' group by interface, devid, mac)###; create temporary table
       allocated_ip as select distinct on (1) intf, cast(used*100.0/total as decimal
       (18,2)) as percent_of_allocated_ip from ###(select distinct on (1) concat
       (interface, '.', devid) as intf, used, total, itime from $log where $filter and
       logid_to_int(logid)=26003 and total>0 order by intf, itime desc)### t order by
       intf, itime desc; select t1.intf as interface, percent_of_allocated_ip, new_cli_
       count from allocated_ip t1 inner join (select intf, count(mac) as new_cli_count
       from cur_clt_list where not exists (select 1 from pre_clt_list where cur_clt_
       list.mac=pre_clt_list.mac) group by intf) t2 on t1.intf=t2.intf order by interface,
       percent_of_allocated_ip desc
```

Dataset Name	Description	Log Category
Top-Wifi-Client-By-Bandwidth	Traffic top WiFi client by bandwidth usage	traffic

```
select
   coalesce(
      nullifna(`user`),
      nullifna(`unauthuser`),
      ipstr(`srcip`)
   ) as user_src,
   srcssid,
   devtype,
   coalesce(
      nullifna(`srcname`),
      `srcmac`
   ) as hostname_mac,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and (
      srcssid is not null
      or dstssid is not null
   )
group by
   user_src,
   srcssid,
   devtype,
   hostname_mac
having
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   )> 0
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
Traffic-History-By-Active-User	Traffic history by active user	traffic

```
select
   $flex_timescale(timestamp) as hodex,
   count(
      distinct(user_src)
   ) as total_user
from
   ###(select $flex_timestamp as timestamp, coalesce(nullifna(`user`), nullifna
       (`unauthuser`), ipstr(`srcip`)) as user_src from $log where $filter and logid_to_
       int(logid) not in (4, 7, 14) group by timestamp, user_src order by timestamp
       desc)### t group by hodex order by hodex
```

Dataset Name	Description	Log Category
Top-Allowed-Websites-By-Requests	UTM top allowed web sites by request	traffic

```
select
   hostname,
   catdesc,
   count(*) as requests
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and utmevent in (
      'webfilter', 'banned-word', 'web-content',
      'command-block', 'script-filter'
   )
   and hostname is not null
   and (
      utmaction not in ('block', 'blocked')
      or action != 'deny'
   )
group by
   hostname,
   catdesc
order by
   requests desc
```

Dataset Name	Description	Log Category
Top-50-Websites-By-Bandwidth	Webfilter top allowed web sites by bandwidth usage	webfilter

```
select
   domain,
   string_agg(distinct catdesc, ', ') as agg_catdesc,
   sum(bandwidth) as bandwidth,
   sum(traffic_in) as traffic_in,
   sum(traffic_out) as traffic_out
from
   ###(select coalesce(nullifna(hostname), ipstr(`dstip`)) as domain, catdesc, sum
       (coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth, sum(coalesce(rcvdbyte,
       0)) as traffic_in, sum(coalesce(sentbyte, 0)) as traffic_out from $log-traffic
       where $filter and logid_to_int(logid) not in (4, 7, 14) and utmaction!='blocked'
       and ((logver>=52 and countweb>0) or ((logver is null) and utmevent in ('webfilter',
       'banned-word', 'web-content', 'command-block', 'script-filter'))) group by domain,
       catdesc having sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0))>0 order by
       bandwidth desc)### t group by domain, catdesc order by bandwidth desc
```

Dataset Name	Description	Log Category
Top-Blocked-Websites	UTM top blocked web sites by request	traffic

```
select
   hostname,
   count(*) as requests
from
   $log
```

```
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and utmevent in (
      'webfilter', 'banned-word', 'web-content',
      'command-block', 'script-filter'
   )
   and hostname is not null
   and (
      utmaction in ('block', 'blocked')
      or action = 'deny'
   )
group by
   hostname
order by
   requests desc
```

Dataset Name	Description	Log Category
Top-Web-Users-By-Request	UTM top web users by request	traffic

```
select
   coalesce(
      nullifna(`user`),
      nullifna(`unauthuser`),
      ipstr(`srcip`)
   ) as user_src,
   devtype,
   srcname,
   count(*) as requests
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and utmevent in (
      'webfilter', 'banned-word', 'web-content',
      'command-block', 'script-filter'
   )
group by
   user_src,
   devtype,
   srcname
order by
   requests desc
```

Dataset Name	Description	Log Category
Top-Allowed-WebSites-By-Bandwidth	UTM top allowed websites by bandwidth usage	traffic

```
select
   appid,
   hostname,
   catdesc,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth,
   sum(
      coalesce(rcvdbyte, 0)
   ) as traffic_in,
   sum(
      coalesce(sentbyte, 0)
   ) as traffic_out
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and utmevent in (
      'webfilter', 'banned-word', 'web-content',
      'command-block', 'script-filter'
   )
   and hostname is not null
group by
   appid,
   hostname,
   catdesc
having
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   )> 0
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
Top-Blocked-Web-Users	UTM top blocked web users	traffic

```
select
   coalesce(
      nullifna(`user`),
      nullifna(`unauthuser`),
      ipstr(`srcip`)
   ) as user_src,
   devtype,
   srcname,
   count(*) as requests
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and utmevent in (
      'webfilter', 'banned-word', 'web-content',
      'command-block', 'script-filter'
   )
   and (
      utmaction in ('block', 'blocked')
      or action = 'deny'
   )
group by
   user_src,
   devtype,
   srcname
order by
   requests desc
```

Dataset Name	Description	Log Category
Top-20-Web-Users-By-Bandwidth	Webfilter top web users by bandwidth usage	webfilter

```
  select
     user_src,
     sum(bandwidth) as bandwidth,
     sum(traffic_in) as traffic_in,
     sum(traffic_out) as traffic_out
  from
     ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as user_
         src, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth, sum(coalesce
         (rcvdbyte, 0)) as traffic_in, sum(coalesce(sentbyte, 0)) as traffic_out from $log-
         traffic where $filter and logid_to_int(logid) not in (4, 7, 14) and ((logver>=52
         and countweb>0) or ((logver is null) and utmevent in ('webfilter', 'banned-word',
         'web-content', 'command-block', 'script-filter'))) group by user_src having sum
         (coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0))>0 order by bandwidth desc)### t group
         by user_src order by bandwidth desc
```

Dataset Name	Description	Log Category
Top-Web-Users-By-Bandwidth	UTM top web users by bandwidth usage	traffic

```
  select
     coalesce(
        nullifna(`user`),
        nullifna(`unauthuser`),
        ipstr(`srcip`)
     ) as user_src,
     devtype,
     srcname,
     sum(
        coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
     ) as bandwidth,
     sum(
        coalesce(rcvdbyte, 0)
     ) as traffic_in,
     sum(
        coalesce(sentbyte, 0)
     ) as traffic_out
  from
     $log
  where
     $filter
     and logid_to_int(logid) not in (4, 7, 14)
     and utmevent in (
        'webfilter', 'banned-word', 'web-content',
        'command-block', 'script-filter'
     )
  group by
     user_src,
     devtype,
     srcname
  having
```

```
      sum(
         coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
      )> 0
   order by
      bandwidth desc
```

Dataset Name	Description	Log Category
Top-Video-Streaming-Websites-By-Bandwidth	UTM top video streaming websites by bandwidth usage	traffic

```
   select
      appid,
      hostname,
      sum(
         coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
      ) as bandwidth,
      sum(
         coalesce(rcvdbyte, 0)
      ) as traffic_in,
      sum(
         coalesce(sentbyte, 0)
      ) as traffic_out
   from
      $log
   where
      $filter
      and logid_to_int(logid) not in (4, 7, 14)
      and catdesc in ('Streaming Media and Download')
   group by
      appid,
      hostname
   having
      sum(
         coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
      )> 0
   order by
      bandwidth desc
```

Dataset Name	Description	Log Category
Top-Email-Senders-By-Count	Default top email senders by count	traffic

```
   select
      coalesce(
         nullifna(`user`),
         nullifna(`unauthuser`),
         ipstr(`srcip`)
      ) as user_src,
      count(*) as requests
   from
      $log
   where
      $filter
      and logid_to_int(logid) not in (4, 7, 14)
      and service in (
         'smtp', 'SMTP', '25/tcp', '587/tcp',
         'smtps', 'SMTPS', '465/tcp'
      )
   group by
      user_src
   order by
      requests desc
```

Dataset Name	Description	Log Category
Top-Email-Receivers-By-Count	Default email top receivers by count	traffic

```
   select
      coalesce(
         nullifna(`user`),
         nullifna(`unauthuser`),
         ipstr(`srcip`)
      ) as user_src,
      count(*) as requests
   from
      $log
   where
      $filter
      and logid_to_int(logid) not in (4, 7, 14)
      and service in (
         'pop3', 'POP3', '110/tcp', 'imap',
         'IMAP', '143/tcp', 'imaps', 'IMAPS',
         '993/tcp', 'pop3s', 'POP3S', '995/tcp'
      )
   group by
      user_src
   order by
      requests desc
```

Dataset Name	Description	Log Category
Top-Email-Senders-By-Bandwidth	Default email top senders by bandwidth usage	traffic

```
   select
      coalesce(
         nullifna(`user`),
         nullifna(`unauthuser`),
         ipstr(`srcip`)
      ) as user_src,
      sum(
         coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
      ) as bandwidth
   from
      $log
   where
      $filter
      and logid_to_int(logid) not in (4, 7, 14)
      and service in (
         'smtp', 'SMTP', '25/tcp', '587/tcp',
         'smtps', 'SMTPS', '465/tcp'
      )
   group by
      user_src
```

```
having
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   )> 0
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
Top-Email-Receivers-By-Bandwidth	Default email top receivers by bandwidth usage	traffic

```
select
   coalesce(
      nullifna(`user`),
      nullifna(`unauthuser`),
      ipstr(`srcip`)
   ) as user_src,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and service in (
      'pop3', 'POP3', '110/tcp', 'imap',
      'IMAP', '143/tcp', 'imaps', 'IMAPS',
      '993/tcp', 'pop3s', 'POP3S', '995/tcp'
   )
group by
   user_src
having
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   )> 0
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
Top-Malware-By-Name	UTM top virus	virus

```
select
   virus,
   max(virusid) as virusid,
   (
      case when virus like 'Riskware%' then 'Spyware' when virus like 'Adware%' then
          'Adware' else 'Virus' end
   ) as malware_type,
   sum(totalnum) as totalnum
from
   (
      ###(select virus, 0 as virusid, count(*) as totalnum from $log-traffic where $filter
          and logid_to_int(logid) not in (4, 7, 14) and utmevent is not null and virus is
          not null group by virus, virusid order by totalnum desc)### union all ###(select
          virus, virusid, count(*) as totalnum from $log-virus where $filter and
          (eventtype is null or logver>=52) and nullifna(virus) is not null group by
          virus, virusid order by totalnum desc)###) t group by virus, malware_type order
          by totalnum desc
```

Dataset Name	Description	Log Category
Top-Virus-By-Name	UTM top virus	virus

```
select
   virus,
   max(virusid) as virusid,
   (
      case when virus like 'Riskware%' then 'Spyware' when virus like 'Adware%' then
          'Adware' else 'Virus' end
   ) as malware_type,
   sum(totalnum) as totalnum
from
   (
      ###(select virus, 0 as virusid, count(*) as totalnum from $log-traffic where $filter
          and logid_to_int(logid) not in (4, 7, 14) and utmevent is not null and virus is
          not null group by virus, virusid order by totalnum desc)### union all ###(select
          virus, virusid, count(*) as totalnum from $log-virus where $filter and
          (eventtype is null or logver>=52) and nullifna(virus) is not null group by
          virus, virusid order by totalnum desc)###) t group by virus, malware_type order
          by totalnum desc
```

Dataset Name	Description	Log Category
Top-Virus-Victim	UTM top virus user	traffic

```
select
   user_src,
   sum(totalnum) as totalnum
from
   (
      ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as
          user_src, count(*) as totalnum from $log-traffic where $filter and logid_to_int
          (logid) not in (4, 7, 14) and utmevent is not null and virus is not null group
          by user_src order by totalnum desc)### union all ###(select coalesce(nullifna
          (`user`), ipstr(`srcip`)) as user_src, count(*) as totalnum from $log-virus
          where $filter and (eventtype is null or logver>=52) and nullifna(virus) is not
          null group by user_src order by totalnum desc)###) t group by user_src order by
          totalnum desc
```

Dataset Name	Description	Log Category
Top-Attack-Source	UTM top attack source	attack

```
select
   coalesce(
      nullifna(`user`),
      ipstr(`srcip`)
   ) as user_src,
   count(*) as totalnum
from
   $log
where
   $filter
group by
```

```
   user_src
order by
   totalnum desc
```

Dataset Name	Description	Log Category
Top-Attack-Victim	UTM top attack dest	attack

```
select
   dstip,
   count(*) as totalnum
from
   $log
where
   $filter
   and dstip is not null
group by
   dstip
order by
   totalnum desc
```

Dataset Name	Description	Log Category
Top-Static-IPSEC-Tunnels-By-Bandwidth	Top static IPsec tunnels by bandwidth usage	event

```
select
   vpn_name,
   sum(traffic_in + traffic_out) as bandwidth,
   sum(traffic_in) as traffic_in,
   sum(traffic_out) as traffic_out
from
   (
      select
         devid,
         vd,
         remip,
         tunnelid,
         vpn_name,
         max(traffic_in) as traffic_in,
         max(traffic_out) as traffic_out
      from
         ###(select devid, vd, remip, vpn_trim(vpntunnel) as vpn_name, tunnelid, max
             (coalesce(sentbyte, 0)) as traffic_out, max(coalesce(rcvdbyte, 0)) as
             traffic_in from $log where $filter and subtype='vpn' and tunneltype like
             'ipsec%' and (tunnelip is null or (tunnelip='0.0.0.0' and logver is null))
             and action in ('tunnel-stats', 'tunnel-down') and tunnelid is not null group
             by devid, vd, remip, vpn_name, tunnelid)### t group by devid, vd, remip, vpn_
             name, tunnelid) tt group by vpn_name having sum(traffic_in+traffic_out)>0
             order by bandwidth desc
```

Dataset Name	Description	Log Category
Top-SSL-VPN-Tunnel-Users-By-Bandwidth	Top SSL VPN tunnel users by bandwidth usage	event

```
select
   user_src,
   remip as remote_ip,
   from_dtime(
      min(s_time)
   ) as start_time,
   sum(bandwidth) as bandwidth,
   sum(traffic_in) as traffic_in,
   sum(traffic_out) as traffic_out
from
   (
      select
         devid,
         vd,
         remip,
         user_src,
         tunnelid,
         min(s_time) as s_time,
         max(e_time) as e_time,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_in)+ max(max_traffic_
                out) else max(max_traffic_in)- min(min_traffic_in)+ max(max_traffic_out)-
                min(min_traffic_out) end
         ) as bandwidth,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_in) else max(max_
                traffic_in)- min(min_traffic_in) end
         ) as traffic_in,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_out) else max(max_
                traffic_out)- min(min_traffic_out) end
         ) as traffic_out
      from
         ###(select devid, vd, remip, coalesce(nullifna(`user`), ipstr(`remip`)) as user_
             src, tunnelid, min(coalesce(dtime, 0)) as s_time, max(coalesce(dtime, 0)) as
             e_time, min(coalesce(sentbyte, 0)) as min_traffic_out, min(coalesce(rcvdbyte,
             0)) as min_traffic_in, max(coalesce(sentbyte, 0)) as max_traffic_out, max
             (coalesce(rcvdbyte, 0)) as max_traffic_in from $log where $filter and
             subtype='vpn' and tunneltype='ssl-tunnel' and action in ('tunnel-stats',
             'tunnel-down', 'tunnel-up') and coalesce(nullifna(`user`), ipstr(`remip`)) is
             not null and tunnelid is not null group by devid, vd, user_src, remip,
             tunnelid)### t group by devid, vd, user_src, remip, tunnelid) tt group by
             user_src, remote_ip having sum(bandwidth)>0 order by bandwidth desc
```

Dataset Name	Description	Log Category
Top-Dial-Up-IPSEC-Tunnels-By-Bandwidth	Top dial up IPsec tunnels by bandwidth usage	event

```
select
   vpn_name,
   sum(traffic_out + traffic_in) as bandwidth,
   sum(traffic_in) as traffic_in,
   sum(traffic_out) as traffic_out
from
   (
      select
         devid,
         vd,
         tunnelid,
         remip,
         vpn_name,
         max(traffic_in) as traffic_in,
         max(traffic_out) as traffic_out
      from
         ###(select devid, vd, remip, vpn_trim(vpntunnel) as vpn_name, tunnelid, max
             (coalesce(sentbyte, 0)) as traffic_out, max(coalesce(rcvdbyte, 0)) as
             traffic_in from $log where $filter and nullifna(vpntunnel) is not null and
             subtype='vpn' and tunneltype like 'ipsec%' and not (tunnelip is null or
             (tunnelip='0.0.0.0' and logver is null)) and action in ('tunnel-stats',
             'tunnel-down') and tunnelid is not null group by devid, vd, remip, vpn_name,
             tunnelid)### t group by devid, vd, remip, vpn_name, tunnelid) tt group by
             vpn_name having sum(traffic_out+traffic_in)>0 order by bandwidth desc
```

Dataset Name	Description	Log Category
Top-Dial-Up-IPSEC-Users-By-Bandwidth	Top dial up IPsec users by bandwidth usage	event

```
select
   coalesce(
      xauthuser_agg,
      user_agg,
      ipstr(`remip`)
   ) as user_src,
   remip,
   from_dtime(
      min(s_time)
   ) as start_time,
   sum(bandwidth) as bandwidth,
   sum(traffic_in) as traffic_in,
   sum(traffic_out) as traffic_out
from
   (
      select
         devid,
         vd,
         string_agg(distinct xauthuser_agg, ' ') as xauthuser_agg,
         string_agg(distinct user_agg, ' ') as user_agg,
         remip,
         tunnelid,
         min(s_time) as s_time,
         max(e_time) as e_time,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_in)+ max(max_traffic_
                out) else max(max_traffic_in)- min(min_traffic_in)+ max(max_traffic_out)-
                min(min_traffic_out) end
         ) as bandwidth,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_in) else max(max_
                traffic_in)- min(min_traffic_in) end
         ) as traffic_in,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_out) else max(max_
                traffic_out)- min(min_traffic_out) end
         ) as traffic_out
      from
###(select devid, vd, nullifna(`xauthuser`) as xauthuser_agg, nullifna(`user`) as
    user_agg, remip, tunnelid, min(coalesce(dtime, 0)) as s_time, max(coalesce
    (dtime, 0)) as e_time, min(coalesce(sentbyte, 0)) as min_traffic_out, min
    (coalesce(rcvdbyte, 0)) as min_traffic_in, max(coalesce(sentbyte, 0)) as max_
    traffic_out, max(coalesce(rcvdbyte, 0)) as max_traffic_in from $log where
    $filter and subtype='vpn' and tunneltype like 'ipsec%' and not (tunnelip is
    null or (tunnelip='0.0.0.0' and logver is null)) and action in ('tunnel-
    stats', 'tunnel-down', 'tunnel-up') and tunnelid is not null group by devid,
    vd, xauthuser_agg, user_agg, remip, tunnelid)### t group by devid, vd, remip,
    tunnelid) tt group by user_src, remip having sum(bandwidth)>0 order by
    bandwidth desc
```

Dataset Name	Description	Log Category
Top-Dial-Up-IPSEC-Users-By-Duration	Top dial up IPsec users by duration	event

```
select
   coalesce(
      xauthuser_agg,
      user_agg,
      ipstr(`remip`)
   ) as user_src,
   from_dtime(
      min(s_time)
   ) as start_time,
   sum(duration) as duration,
   sum(bandwidth) as bandwidth,
   sum(traffic_in) as traffic_in,
   sum(traffic_out) as traffic_out
from
   (
      select
         devid,
         vd,
         remip,
         string_agg(distinct xauthuser_agg, ' ') as xauthuser_agg,
         string_agg(distinct user_agg, ' ') as user_agg,
         tunnelid,
         min(s_time) as s_time,
         max(e_time) as e_time,
         (
            case when min(s_time)= max(e_time) then max(max_duration) else max(max_
                duration)- min(min_duration) end
         ) as duration,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_in)+ max(max_traffic_
                out) else max(max_traffic_in)- min(min_traffic_in)+ max(max_traffic_out)-
                min(min_traffic_out) end
         ) as bandwidth,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_in) else max(max_
                traffic_in)- min(min_traffic_in) end
         ) as traffic_in,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_out) else max(max_
                traffic_out)- min(min_traffic_out) end
         ) as traffic_out
      from
         ###(select devid, vd, remip, nullifna(`xauthuser`) as xauthuser_agg, nullifna
             (`user`) as user_agg, tunnelid, min(coalesce(dtime, 0)) as s_time, max
             (coalesce(dtime, 0)) as e_time, max(coalesce(duration,0)) as max_duration,
             min(coalesce(duration,0)) as min_duration, min(coalesce(sentbyte, 0)) as min_
             traffic_out, min(coalesce(rcvdbyte, 0)) as min_traffic_in, max(coalesce
             (sentbyte, 0)) as max_traffic_out, max(coalesce(rcvdbyte, 0)) as max_traffic_
             in from $log where $filter and subtype='vpn' and tunneltype like 'ipsec%' and
             not (tunnelip is null or (tunnelip='0.0.0.0' and logver is null)) and action
             in ('tunnel-stats', 'tunnel-down', 'tunnel-up') and tunnelid is not null
             group by devid, vd, remip, xauthuser_agg, user_agg, tunnelid order by
             tunnelid)### t group by devid, vd, remip, tunnelid) tt group by user_src
             having sum(bandwidth)>0 order by duration desc
```

Dataset Name	Description	Log Category
Top-SSL-VPN-Web-Mode-Users-By-Bandwidth	Top SSL VPN web mode users by bandwidth usage	event

```
select
   user_src,
   remip as remote_ip,
   from_dtime(
      min(s_time)
   ) as start_time,
   sum(bandwidth) as bandwidth,
   sum(traffic_in) as traffic_in,
   sum(traffic_out) as traffic_out
from
   (
      select
         devid,
         vd,
         user_src,
         remip,
         tunnelid,
         min(s_time) as s_time,
         max(e_time) as e_time,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_in)+ max(max_traffic_
                out) else max(max_traffic_in)- min(min_traffic_in)+ max(max_traffic_out)-
                min(min_traffic_out) end
         ) as bandwidth,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_in) else max(max_
                traffic_in)- min(min_traffic_in) end
         ) as traffic_in,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_out) else max(max_
                traffic_out)- min(min_traffic_out) end
         ) as traffic_out
      from
         ###(select devid, vd, coalesce(nullifna(`user`), ipstr(`remip`)) as user_src,
             remip, tunnelid, min(coalesce(dtime, 0)) as s_time, max(coalesce(dtime, 0))
             as e_time, min(coalesce(sentbyte, 0)) as min_traffic_out, min(coalesce
             (rcvdbyte, 0)) as min_traffic_in, max(coalesce(sentbyte, 0)) as max_traffic_
             out, max(coalesce(rcvdbyte, 0)) as max_traffic_in from $log where $filter and
             subtype='vpn' and tunneltype='ssl-web' and action in ('tunnel-stats',
             'tunnel-down', 'tunnel-up') and coalesce(nullifna(`user`), ipstr(`remip`)) is
             not null and tunnelid is not null group by devid, vd, user_src, remip,
             tunnelid)### t group by devid, vd, user_src, remip, tunnelid) tt group by
             user_src, remote_ip having sum(bandwidth)>0 order by bandwidth desc
```

Dataset Name	Description	Log Category
Top-SSL-VPN-Users-By-Duration	Top SSL VPN users by duration	event

```
select
   user_src,
   tunneltype,
   sum(duration) as duration,
   sum(traffic_out + traffic_in) as bandwidth,
   sum(traffic_in) as traffic_in,
   sum(traffic_out) as traffic_out
from
   (
      select
         devid,
         vd,
         remip,
         user_src,
         tunneltype,
         tunnelid,
         max(duration) as duration,
         max(traffic_in) as traffic_in,
         max(traffic_out) as traffic_out
      from
         ###(select devid, vd, remip, coalesce(nullifna(`user`), ipstr(`remip`)) as user_
             src, tunnelid, tunneltype, max(coalesce(duration, 0)) as duration, max
             (coalesce(sentbyte, 0)) as traffic_out, max(coalesce(rcvdbyte, 0)) as
             traffic_in from $log where $filter and subtype='vpn' and tunneltype like
             'ssl%' and action in ('tunnel-stats', 'tunnel-down') and coalesce(nullifna
             (`user`), ipstr(`remip`)) is not null and tunnelid is not null and
             tunnelid!=0 group by devid, vd, remip, user_src, tunnelid, tunneltype)### t
             group by devid, vd, remip, user_src, tunnelid, tunneltype) tt group by user_
             src, tunneltype having sum(traffic_out+traffic_in)>0 order by duration desc
```

Dataset Name	Description	Log Category
vpn-Top-Dial-Up-VPN-Users-By-Duration	Top dial up VPN users by duration	event

```
select
   coalesce(
      xauthuser_agg,
      user_agg,
      ipstr(`remip`)
   ) as user_src,
   t_type as tunneltype,
   from_dtime(
      min(s_time)
   ) as start_time,
   sum(duration) as duration,
   sum(bandwidth) as bandwidth,
   sum(traffic_in) as traffic_in,
   sum(traffic_out) as traffic_out
from
```

```
   (
      select
         devid,
         vd,
         remip,
         string_agg(distinct xauthuser_agg, ' ') as xauthuser_agg,
         string_agg(distinct user_agg, ' ') as user_agg,
         t_type,
         tunnelid,
         min(s_time) as s_time,
         max(e_time) as e_time,
         (
            case when min(s_time)= max(e_time) then max(max_duration) else max(max_
                duration)- min(min_duration) end
         ) as duration,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_in)+ max(max_traffic_
                out) else max(max_traffic_in)- min(min_traffic_in)+ max(max_traffic_out)-
                min(min_traffic_out) end
         ) as bandwidth,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_in) else max(max_
                traffic_in)- min(min_traffic_in) end
         ) as traffic_in,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_out) else max(max_
                traffic_out)- min(min_traffic_out) end
         ) as traffic_out
      from
         ###(select devid, vd, remip, nullifna(`xauthuser`) as xauthuser_agg, nullifna
             (`user`) as user_agg, (case when tunneltype like 'ipsec%' then 'ipsec' else
             tunneltype end) as t_type, tunnelid, min(coalesce(dtime, 0)) as s_time, max
             (coalesce(dtime, 0)) as e_time, max(coalesce(duration,0)) as max_duration,
             min(coalesce(duration,0)) as min_duration, min(coalesce(sentbyte, 0)) as min_
             traffic_out, min(coalesce(rcvdbyte, 0)) as min_traffic_in, max(coalesce
             (sentbyte, 0)) as max_traffic_out, max(coalesce(rcvdbyte, 0)) as max_traffic_
             in from $log where $filter and subtype='vpn' and (tunneltype like 'ssl%' or
             (tunneltype like 'ipsec%' and not (tunnelip is null or (tunnelip='0.0.0.0'
             and logver is null)))) and action in ('tunnel-stats', 'tunnel-down', 'tunnel-
             up') and tunnelid is not null group by devid, vd, remip, xauthuser_agg, user_
             agg, t_type, tunnelid)### t group by devid, vd, remip, t_type, tunnelid) tt
             group by user_src, tunneltype having sum(bandwidth)>0 order by duration desc
```

Dataset Name	Description	Log Category
vpn-User-Login-history	VPN user login history	event

```
select
   $flex_timescale(timestamp) as hodex,
   sum(total_num) as total_num
from
   (
      select
         timestamp,
         devid,
         vd,
         remip,
         tunnelid,
         sum(tunnelup) as total_num,
         max(traffic_in) as traffic_in,
         max(traffic_out) as traffic_out
      from
         ###(select $flex_timestamp as timestamp, devid, vd, remip, tunnelid, (case when
             action='tunnel-up' then 1 else 0 end) as tunnelup, max(coalesce(sentbyte, 0))
             as traffic_out, max(coalesce(rcvdbyte, 0)) as traffic_in from $log where
             $filter and subtype='vpn' and (tunneltype like 'ipsec%' or tunneltype like
             'ssl%') and action in ('tunnel-up', 'tunnel-stats', 'tunnel-down') and
             tunnelid is not null group by timestamp, action, devid, vd, remip, tunnelid
             order by timestamp desc)### t group by timestamp, devid, vd, remip, tunnelid
             having max(tunnelup) > 0 and max(traffic_in)+max(traffic_out)>0) t group by
             hodex order by total_num desc
```

Dataset Name	Description	Log Category
vpn-Failed-Login-Atempts	VPN failed logins	event

```
select
   f_user,
   tunneltype,
   sum(total_num) as total_num
from
   ###(select coalesce(nullifna(`xauthuser`), `user`) as f_user, tunneltype, count(*) as
       total_num from $log where $filter and subtype='vpn' and (tunneltype='ipsec' or left
       (tunneltype, 3)='ssl') and action in ('ssl-login-fail', 'ipsec-login-fail') and
       coalesce(nullifna(`xauthuser`), nullifna(`user`)) is not null group by f_user,
       tunneltype)### t group by f_user, tunneltype order by total_num desc
```

Dataset Name	Description	Log Category
vpn-Authenticated-Logins	VPN authenticated logins	event

```
select
   coalesce(
      xauthuser_agg,
      user_agg,
      ipstr(`remip`)
   ) as f_user,
   t_type as tunneltype,
   from_dtime(
      min(s_time)
   ) as start_time,
   sum(total_num) as total_num,
   sum(duration) as duration
from
   (
      select
         string_agg(distinct xauthuser_agg, ' ') as xauthuser_agg,
         string_agg(distinct user_agg, ' ') as user_agg,
         t_type,
         devid,
         vd,
         remip,
         tunnelid,
         min(s_time) as s_time,
         max(e_time) as e_time,
         (
            case when min(s_time)= max(e_time) then max(max_duration) else max(max_
                duration)- min(min_duration) end
         ) as duration,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_in)+ max(max_traffic_
                out) else max(max_traffic_in)- min(min_traffic_in)+ max(max_traffic_out)-
                min(min_traffic_out) end
         ) as bandwidth,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_in) else max(max_
                traffic_in)- min(min_traffic_in) end
         ) as traffic_in,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_out) else max(max_
                traffic_out)- min(min_traffic_out) end
         ) as traffic_out,
         sum(tunnelup) as total_num
      from
         ###(select nullifna(`xauthuser`) as xauthuser_agg, nullifna(`user`) as user_agg,
             devid, vd, remip, (case when tunneltype like 'ipsec%' then 'ipsec' else
             tunneltype end) as t_type, tunnelid, sum((case when action='tunnel-up' then 1
             else 0 end)) as tunnelup, min(coalesce(dtime, 0)) as s_time, max(coalesce
             (dtime, 0)) as e_time, max(coalesce(duration,0)) as max_duration, min
             (coalesce(duration,0)) as min_duration, min(coalesce(sentbyte, 0)) as min_
             traffic_out, min(coalesce(rcvdbyte, 0)) as min_traffic_in, max(coalesce
             (sentbyte, 0)) as max_traffic_out, max(coalesce(rcvdbyte, 0)) as max_traffic_
             in from $log where $filter and subtype='vpn' and (tunneltype like 'ipsec%' or
             tunneltype like 'ssl%') and action in ('tunnel-up', 'tunnel-stats', 'tunnel-
             down') and tunnelid is not null group by xauthuser_agg, user_agg, devid, vd,
             remip, t_type, tunnelid)### t group by t_type, devid, vd, remip, tunnelid
             having max(tunnelup) > 0) tt group by f_user, tunneltype having sum
             (bandwidth) > 0 order by total_num desc
```

Dataset Name	Description	Log Category
vpn-Traffic-Usage-Trend-VPN-Summary	VPN traffic usage trend	event

```
select
   hodex,
   sum(ssl_traffic_out + ssl_traffic_in) as ssl_bandwidth,
   sum(
      ipsec_traffic_out + ipsec_traffic_in
   ) as ipsec_bandwidth
from
   (
      select
         $flex_timescale(timestamp) as hodex,
         devid,
         vd,
         remip,
         tunnelid,
         (
            case when t_type like 'ssl%' then max(traffic_in) else 0 end
         ) as ssl_traffic_in,
         (
            case when t_type like 'ssl%' then max(traffic_out) else 0 end
         ) as ssl_traffic_out,
         (
            case when t_type like 'ipsec%' then max(traffic_in) else 0 end
         ) as ipsec_traffic_in,
         (
            case when t_type like 'ipsec%' then max(traffic_out) else 0 end
         ) as ipsec_traffic_out
      from
         ###(select $flex_timestamp as timestamp, devid, vd, remip, tunnelid, (case when
             tunneltype like 'ipsec%' then 'ipsec' else tunneltype end) as t_type, max
             (coalesce(sentbyte, 0)) as traffic_out, max(coalesce(rcvdbyte, 0)) as
             traffic_in from $log where $filter and subtype='vpn' and (tunneltype like
             'ipsec%' or tunneltype like 'ssl%') and action in ('tunnel-stats', 'tunnel-
             down') and tunnelid is not null group by timestamp, devid, vd, remip, t_type,
             tunnelid order by timestamp desc)### t group by hodex, devid, t_type, vd,
             remip, tunnelid) tt group by hodex order by hodex
```

Dataset Name	Description	Log Category
Top-S2S-IPSEC-Tunnels-By-Bandwidth-and-Availability	Top S2S IPsec tunnels by bandwidth usage and avail	event

```
select
   vpntunnel,
   tunneltype,
   sum(traffic_out) as traffic_out,
   sum(traffic_in) as traffic_in,
   sum(bandwidth) as bandwidth,
   sum(uptime) as uptime
from
   (
      select
         vpntunnel,
         tunneltype,
         tunnelid,
         devid,
         vd,
         sum(sent_end - sent_beg) as traffic_out,
         sum(rcvd_end - rcvd_beg) as traffic_in,
         sum(
            sent_end - sent_beg + rcvd_end - rcvd_beg
         ) as bandwidth,
         sum(duration_end - duration_beg) as uptime
      from
         ###(select tunnelid, tunneltype, vpntunnel, devid, vd, min(coalesce(sentbyte, 0))
             as sent_beg, max(coalesce(sentbyte, 0)) as sent_end, min(coalesce(rcvdbyte,
             0)) as rcvd_beg, max(coalesce(rcvdbyte, 0)) as rcvd_end, min(coalesce
             (duration, 0)) as duration_beg, max(coalesce(duration, 0)) as duration_end
             from $log where $filter and subtype='vpn' and action='tunnel-stats' and
             tunneltype like 'ipsec%' and (tunnelip is null or (tunnelip='0.0.0.0' and
             logver is null)) and nullifna(`user`) is null and tunnelid is not null group
             by tunnelid, tunneltype, vpntunnel, devid, vd order by tunnelid)### t group
             by vpntunnel, tunneltype, tunnelid, devid, vd order by bandwidth desc) t
             group by vpntunnel, tunneltype order by bandwidth desc
```

Dataset Name	Description	Log Category
Top-Dialup-IPSEC-By-Bandwidth-and-Availability	Top dialup IPsec users by bandwidth usage and avail	event

```
select
   user_src,
   remip,
   sum(traffic_out) as traffic_out,
   sum(traffic_in) as traffic_in,
   sum(bandwidth) as bandwidth,
   sum(uptime) as uptime
from
   (
      select
         user_src,
         remip,
         tunnelid,
         devid,
         vd,
         sum(sent_end - sent_beg) as traffic_out,
         sum(rcvd_end - rcvd_beg) as traffic_in,
         sum(
            sent_end - sent_beg + rcvd_end - rcvd_beg
         ) as bandwidth,
         sum(duration_end - duration_beg) as uptime
      from
         ###(select tunnelid, coalesce(nullifna(`xauthuser`), nullifna(`user`), ipstr
             (`remip`)) as user_src, remip, devid, vd, min(coalesce(sentbyte, 0)) as sent_
             beg, max(coalesce(sentbyte, 0)) as sent_end, min(coalesce(rcvdbyte, 0)) as
             rcvd_beg, max(coalesce(rcvdbyte, 0)) as rcvd_end, min(coalesce(duration, 0))
             as duration_beg, max(coalesce(duration, 0)) as duration_end from $log where
             $filter and subtype='vpn' and action='tunnel-stats' and tunneltype like
             'ipsec%' and not (tunnelip is null or (tunnelip='0.0.0.0' and logver is
             null)) and tunnelid is not null group by tunnelid, user_src, remip, devid, vd
             order by tunnelid)### t group by user_src, remip, tunnelid, devid, vd order
             by bandwidth desc) t group by user_src, remip order by bandwidth desc
```

Dataset Name	Description	Log Category
Top-SSL-Tunnel-Mode-By-Bandwidth-and-Availability	Top SSL tunnel users by bandwidth usage and avail	event

```
select
   user_src,
   remote_ip,
   sum(traffic_out) as traffic_out,
   sum(traffic_in) as traffic_in,
   sum(bandwidth) as bandwidth,
   sum(uptime) as uptime
from
   (
      select
         user_src,
         remip as remote_ip,
         tunnelid,
         devid,
         vd,
         sum(sent_end - sent_beg) as traffic_out,
         sum(rcvd_end - rcvd_beg) as traffic_in,
         sum(
            sent_end - sent_beg + rcvd_end - rcvd_beg
         ) as bandwidth,
         sum(duration_end - duration_beg) as uptime
      from
         ###(select tunnelid, coalesce(nullifna(`user`), ipstr(`remip`)) as user_src,
             remip, devid, vd, min(coalesce(sentbyte, 0)) as sent_beg, max(coalesce
             (sentbyte, 0)) as sent_end, min(coalesce(rcvdbyte, 0)) as rcvd_beg, max
             (coalesce(rcvdbyte, 0)) as rcvd_end, min(coalesce(duration, 0)) as duration_
             beg, max(coalesce(duration, 0)) as duration_end from $log where $filter and
             subtype='vpn' and action='tunnel-stats' and tunneltype in ('ssl-tunnel',
             'ssl') and coalesce(nullifna(`user`), ipstr(`remip`)) is not null and
             tunnelid is not null group by tunnelid, user_src, remip, devid, vd order by
             tunnelid)### t group by user_src, remote_ip, tunnelid, devid, vd order by
             bandwidth desc) t group by user_src, remote_ip order by bandwidth desc
```

Dataset Name	Description	Log Category
Top-SSL-Web-Mode-By-Bandwidth-and-Availability	Top SSL web users by bandwidth usage and avail	event

```
select
   user_src,
   remote_ip,
   sum(traffic_out) as traffic_out,
   sum(traffic_in) as traffic_in,
   sum(bandwidth) as bandwidth,
   sum(uptime) as uptime
from
   (
      select
         user_src,
         remip as remote_ip,
         tunnelid,
         devid,
         vd,
         sum(sent_end - sent_beg) as traffic_out,
         sum(rcvd_end - rcvd_beg) as traffic_in,
         sum(
            sent_end - sent_beg + rcvd_end - rcvd_beg
         ) as bandwidth,
         sum(duration_end - duration_beg) as uptime
      from
         ###(select tunnelid, coalesce(nullifna(`user`), ipstr(`remip`)) as user_src,
             remip, devid, vd, min(coalesce(sentbyte, 0)) as sent_beg, max(coalesce
             (sentbyte, 0)) as sent_end, min(coalesce(rcvdbyte, 0)) as rcvd_beg, max
             (coalesce(rcvdbyte, 0)) as rcvd_end, min(coalesce(duration, 0)) as duration_
             beg, max(coalesce(duration, 0)) as duration_end from $log where $filter and
             subtype='vpn' and action='tunnel-stats' and tunneltype='ssl-web' and coalesce
             (nullifna(`user`), ipstr(`remip`)) is not null and tunnelid is not null group
             by tunnelid, user_src, remip, devid, vd order by tunnelid)### t group by
             user_src, remote_ip, tunnelid, devid, vd having sum(sent_end-sent_beg+rcvd_
             end-rcvd_beg)>0 order by bandwidth desc) t group by user_src, remote_ip order
             by bandwidth desc
```

Dataset Name	Description	Log Category
Admin-Login-Summary	Event admin login summary	event

```
select
   f_user,
   ui,
   sum(login) as total_num,
   sum(login_duration) as total_duration,
   sum(config_change) as total_change
from
   (
      select
         `user` as f_user,
         ui,
         (
            case when logid_to_int(logid)= 32001 then 1 else 0 end
         ) as login,
         (
            case when logid_to_int(logid)= 32003 then duration else 0 end
         ) as login_duration,
         (
            case when logid_to_int(logid)= 32003
            and state is not null then 1 else 0 end
         ) as config_change
      from
         $log
      where
         $filter
         and nullifna(`user`) is not null
         and logid_to_int(logid) in (32001, 32003)
   ) t
group by
   f_user,
   ui
having
   sum(login)+ sum(config_change)> 0
order by
   total_num desc
```

Dataset Name	Description	Log Category
Admin-Login-Summary-By-Date	Event admin login summary by date	event

```
select
   $flex_timescale(timestamp) as dom,
   sum(total_num) as total_num,
   sum(total_change) as total_change
from
   ###(select timestamp, sum(login) as total_num, sum(config_change) as total_change from
       (select $flex_timestamp as timestamp, (case when logid_to_int(logid)=32001 then 1
       else 0 end) as login, (case when logid_to_int(logid)=32003 and state is not null
       then 1 else 0 end) as config_change from $log where $filter and logid_to_int(logid)
       in (32001, 32003)) t group by timestamp having sum(login)+sum(config_change)>0
       order by timestamp desc)### t group by dom order by dom
```

Dataset Name	Description	Log Category
Admin-Failed-Login-Summary	Event admin failed login summary	event

```
select
   `user` as f_user,
   ui,
   count(status) as total_failed
from
   $log
where
   $filter
   and nullifna(`user`) is not null
   and logid_to_int(logid) = 32002
group by
   ui,
   f_user
order by
   total_failed desc
```

Dataset Name	Description	Log Category
System-Summary-By-Severity	Event system summary by severity	event

```
select
   (
      case when level in ('critical', 'alert', 'emergency') then 'Critical' when level =
          'error' then 'High' when level = 'warning' then 'Medium' when level = 'notice'
          then 'Low' else 'Info' end
   ) as severity,
   count(*) as total_num
from
   $log
where
   $filter
   and subtype = 'system'
group by
   severity
order by
   total_num desc
```

Dataset Name	Description	Log Category
System-Summary-By-Date	Event system summary by date	event

```
select
   $flex_timescale(timestamp) as dom,
   sum(critical) as critical,
   sum(high) as high,
   sum(medium) as medium
from
   ###(select $flex_timestamp as timestamp, sum(case when level in ('critical', 'alert',
       'emergency') then 1 else 0 end) as critical, sum(case when level = 'error' then 1
       else 0 end) as high, sum(case when level = 'warning' then 1 else 0 end) as medium
       from $log where $filter and subtype='system' group by timestamp order by timestamp
       desc)### t group by dom order by dom
```

Dataset Name	Description	Log Category
Important-System-Summary-By-Date	Event system summary by date	event

```
select
  $flex_timescale(timestamp) as dom,
  sum(critical) as critical,
  sum(high) as high,
  sum(medium) as medium
from
  ###(select $flex_timestamp as timestamp, sum(case when level in ('critical', 'alert',
      'emergency') then 1 else 0 end) as critical, sum(case when level = 'error' then 1
      else 0 end) as high, sum(case when level = 'warning' then 1 else 0 end) as medium
      from $log where $filter and subtype='system' group by timestamp order by timestamp
      desc)### t group by dom order by dom
```

Dataset Name	Description	Log Category
System-Critical-Severity-Events	Event system critical severity events	event

```
select
  msg_desc as msg,
  severity,
  sum(count) as counts
from
  ###(select coalesce(nullifna(logdesc), msg) as msg_desc, (case when level in
      ('critical', 'alert', 'emergency') then 'Critical' when level='error' then 'High'
      when level='warning' then 'Medium' when level='notice' then 'Low' else 'Info' end)
      as severity, count(*) as count from $log where $filter and subtype='system' group
      by msg_desc, severity order by count desc)### t where severity='Critical' group by
      msg, severity order by counts desc
```

Dataset Name	Description	Log Category
System-High-Severity-Events	Event system high severity events	event

```
select
  msg_desc as msg,
  severity,
  sum(count) as counts
from
  ###(select coalesce(nullifna(logdesc), msg) as msg_desc, (case when level in
      ('critical', 'alert', 'emergency') then 'Critical' when level='error' then 'High'
      when level='warning' then 'Medium' when level='notice' then 'Low' else 'Info' end)
      as severity, count(*) as count from $log where $filter and subtype='system' group
      by msg_desc, severity order by count desc)### t where severity='High' group by msg,
      severity order by counts desc
```

Dataset Name	Description	Log Category
System-Medium-Severity-Events	Event system medium severity events	event

```
select
  msg_desc as msg,
  severity,
  sum(count) as counts
```

```
from
   ###(select coalesce(nullifna(logdesc), msg) as msg_desc, (case when level in
       ('critical', 'alert', 'emergency') then 'Critical' when level='error' then 'High'
       when level='warning' then 'Medium' when level='notice' then 'Low' else 'Info' end)
       as severity, count(*) as count from $log where $filter and subtype='system' group
       by msg_desc, severity order by count desc)### t where severity='Medium' group by
       msg, severity order by counts desc
```

Dataset Name	Description	Log Category
utm-drilldown-Top-Traffic-Summary	UTM drilldown traffic summary	traffic

```
select
   srcip,
   srcname
from
   ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as user_
       src, srcip, srcname from $log where $filter and logid_to_int(logid) not in (4, 7,
       14) group by user_src, srcip, srcname)### t where $filter-drilldown group by srcip,
       srcname
```

Dataset Name	Description	Log Category
utm-drilldown-Top-User-Destination	UTM drilldown top user destination	traffic

```
select
   appid,
   app,
   dstip,
   sum(sessions) as sessions,
   sum(bandwidth) as bandwidth
from
   ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as user_
       src, appid, app, dstip, count(*) as sessions, sum(coalesce(sentbyte, 0)+coalesce
       (rcvdbyte, 0)) as bandwidth from $log where $filter and logid_to_int(logid) not in
       (4, 7, 14) and dstip is not null and nullifna(app) is not null group by user_src,
       appid, app, dstip having sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0))>0 order
       by bandwidth desc)### t where $filter-drilldown group by appid, app, dstip order by
       bandwidth desc
```

Dataset Name	Description	Log Category
utm-drilldown-Email-Senders-Summary	UTM drilldown email senders summary	traffic

```
select
   sum(requests) as requests,
   sum(bandwidth) as bandwidth
from
   ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as user_
       src, sender, count(*) as requests, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0))
       as bandwidth from $log where $filter and logid_to_int(logid) not in (4, 7, 14) and
       service in ('smtp', 'SMTP', '25/tcp', '587/tcp', 'smtps', 'SMTPS', '465/tcp') group
       by user_src, sender order by requests desc)### t where $filter-drilldown
```

Dataset Name	Description	Log Category
utm-drilldown-Email-Receivers-Summary	UTM drilldown email receivers summary	traffic

```
select
   sum(requests) as requests,
   sum(bandwidth) as bandwidth
from
   ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as user_
       src, recipient, count(*) as requests, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte,
       0)) as bandwidth from $log where $filter and logid_to_int(logid) not in (4, 7, 14)
       and recipient is not null and service in ('pop3', 'POP3', '110/tcp', 'imap',
       'IMAP', '143/tcp', 'imaps', 'IMAPS', '993/tcp', 'pop3s', 'POP3S', '995/tcp') group
       by user_src, recipient order by requests desc)### t where $filter-drilldown
```

Dataset Name	Description	Log Category
utm-drilldown-Top-Email-Recipients-By-Bandwidth	UTM drilldown top email recipients	traffic

```
select
   recipient,
   sum(bandwidth) as bandwidth
from
   ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as user_
       src, recipient, count(*) as requests, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte,
       0)) as bandwidth from $log where $filter and logid_to_int(logid) not in (4, 7, 14)
       and service in ('pop3', 'POP3', '110/tcp', 'imap', 'IMAP', '143/tcp', 'imaps',
       'IMAPS', '993/tcp', 'pop3s', 'POP3S', '995/tcp') group by user_src, recipient order
       by requests desc)### t where $filter-drilldown and recipient is not null group by
       recipient having sum(bandwidth)>0 order by bandwidth desc
```

Dataset Name	Description	Log Category
utm-drilldown-Top-Email-Senders-By-Bandwidth	UTM drilldown top email senders	traffic

```
select
   sender,
   sum(bandwidth) as bandwidth
from
   ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as user_
       src, sender, count(*) as requests, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0))
       as bandwidth from $log where $filter and logid_to_int(logid) not in (4, 7, 14) and
       service in ('smtp', 'SMTP', '25/tcp', '587/tcp', 'smtps', 'SMTPS', '465/tcp') group
       by user_src, sender order by requests desc)### t where $filter-drilldown and sender
       is not null group by sender having sum(bandwidth)>0 order by bandwidth desc
```

Dataset Name	Description	Log Category
utm-drilldown-Top-Allowed-Websites-By-Bandwidth	UTM drilldown top allowed web sites by bandwidth	traffic

```
select
   appid,
   hostname,
   sum(bandwidth) as bandwidth
from
   ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as user_
       src, appid, hostname, (case when utmaction='blocked' then 1 else 0 end) as blocked,
       sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-traffic
       where $filter and logid_to_int(logid) not in (4, 7, 14) and ((logver>=52 and
       countweb>0) or ((logver is null) and utmevent in ('webfilter', 'banned-word', 'web-
       content', 'command-block', 'script-filter'))) and hostname is not null group by
       user_src, appid, hostname, blocked order by bandwidth desc)### t where $filter-
       drilldown and blocked=0 group by appid, hostname order by bandwidth desc
```

Dataset Name	Description	Log Category
utm-drilldown-Top-Blocked-Web-sites-By-Request	UTM drilldown top blocked web sites by request	traffic

```
select
   appid,
   hostname,
   sum(requests) as requests
from
   (
      ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as
          user_src, appid, hostname, (case when utmaction='blocked' then 1 else 0 end) as
          blocked, count(*) as requests from $log-traffic where $filter and logid_to_int
          (logid) not in (4, 7, 14) and utmevent in ('webfilter', 'banned-word', 'web-
          content', 'command-block', 'script-filter') and hostname is not null group by
          user_src, appid, hostname, blocked order by requests desc)### union all ###
          (select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, 0 as appid,
          hostname, (case when action='blocked' then 1 else 0 end) as blocked, count(*) as
          requests from $log-webfilter where $filter and (eventtype is null or logver>=52)
          and hostname is not null group by user_src, appid, hostname, blocked order by
          requests desc)###) t where $filter-drilldown and blocked=1 group by appid,
          hostname order by requests desc
```

Dataset Name	Description	Log Category
utm-drilldown-Top-Virus-By-Name	UTM drilldown top virus	traffic

```
select
   virus,
   sum(totalnum) as totalnum
from
   (
      ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as
          user_src, virus, count(*) as totalnum from $log-traffic where $filter and logid_
          to_int(logid) not in (4, 7, 14) and utmevent is not null and virus is not null
          group by user_src, virus order by totalnum desc)### union all ###(select
          coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, virus, count(*) as
          totalnum from $log-virus where $filter and (eventtype is null or logver>=52) and
          nullifna(virus) is not null group by user_src, virus order by totalnum desc)###)
          t where $filter-drilldown group by virus order by totalnum desc
```

Dataset Name	Description	Log Category
utm-drilldown-Top-Attacks	UTM drilldown top attacks by name	attack

```
select
   attack,
   sum(attack_count) as attack_count
from
   ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, attack, count(*) as
       attack_count from $log where $filter and nullifna(attack) is not null group by
       user_src, attack order by attack_count desc)### t where $filter-drilldown group by
       attack order by attack_count desc
```

Dataset Name	Description	Log Category
utm-drilldown-Top-Vulnerability	UTM drilldown top vulnerability by name	netscan

```
   select
      vuln,
      sum(totalnum) as totalnum
   from
      ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, vuln, count(*) as
          totalnum from $log where $filter and action='vuln-detection' and vuln is not null
          group by user_src, vuln order by totalnum desc)### t where $filter-drilldown group
          by vuln order by totalnum desc
```

Dataset Name	Description	Log Category
utm-drilldown-Top-App-By-Bandwidth	UTM drilldown top applications by bandwidth usage	traffic

```
   select
      appid,
      app,
      sum(bandwidth) as bandwidth
   from
      ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as user_
          src, appid, app, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth,
          count(*) as sessions from $log where $filter and logid_to_int(logid) not in (4, 7,
          14) and nullifna(app) is not null group by user_src, appid, app order by sessions
          desc)### t where $filter-drilldown group by appid, app having sum(bandwidth)>0
          order by bandwidth desc
```

Dataset Name	Description	Log Category
utm-drilldown-Top-App-By-Sessions	UTM drilldown top applications by session count	traffic

```
   select
      appid,
      app,
      sum(sessions) as sessions
   from
      ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as user_
          src, appid, app, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth,
          count(*) as sessions from $log where $filter and logid_to_int(logid) not in (4, 7,
          14) and nullifna(app) is not null group by user_src, appid, app order by sessions
          desc)### t where $filter-drilldown group by appid, app order by sessions desc
```

Dataset Name	Description	Log Category
Top5-Users-By-Bandwidth	UTM drilldown top users by bandwidth usage	traffic

```
   select
      coalesce(
         nullifna(`user`),
         nullifna(`unauthuser`),
         ipstr(`srcip`)
      ) as dldn_user,
      count(*) as session,
      sum(
         coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
      ) as bandwidth,
      sum(
         coalesce(sentbyte, 0)
      ) as traffic_out,
      sum(
         coalesce(rcvdbyte, 0)
      ) as traffic_in
   from
      $log
   where
      $filter
      and logid_to_int(logid) not in (4, 7, 14)
   group by
      dldn_user
   having
      sum(
         coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
      )> 0
   order by
      bandwidth desc
```

Dataset Name	Description	Log Category
bandwidth-app-Top-App-By-Bandwidth-Sessions	Top applications by bandwidth usage	traffic

```
   select
      app_group_name(app) as app_group,
      sum(
         coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
      ) as bandwidth,
      sum(
         coalesce(rcvdbyte, 0)
      ) as traffic_in,
      sum(
         coalesce(sentbyte, 0)
      ) as traffic_out,
      count(*) as sessions
   from
      $log
   where
      $filter
      and logid_to_int(logid) not in (4, 7, 14)
      and nullifna(app) is not null
   group by
      app_group
   having
      sum(
         coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
      )> 0
```

```
    order by
      bandwidth desc
```

Dataset Name	Description	Log Category
bandwidth-app-Category-By-Bandwidth	Application risk application usage by category	traffic

```
    select
      appcat,
      sum(
        coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
      ) as bandwidth
    from
      $log
    where
      $filter
      and logid_to_int(logid) not in (4, 7, 14)
      and nullifna(appcat) is not null
    group by
      appcat
    order by
      bandwidth desc
```

Dataset Name	Description	Log Category
bandwidth-app-Top-Users-By-Bandwidth-Sessions	Bandwidth application top users by bandwidth usage	traffic

```
    select
      coalesce(
        nullifna(`user`),
        nullifna(`unauthuser`),
        ipstr(`srcip`)
      ) as user_src,
      sum(
        coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
      ) as bandwidth,
      sum(
        coalesce(rcvdbyte, 0)
      ) as traffic_in,
      sum(
        coalesce(sentbyte, 0)
      ) as traffic_out,
      count(*) as sessions
    from
      $log
    where
      $filter
      and logid_to_int(logid) not in (4, 7, 14)
    group by
      user_src
    having
      sum(
        coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
      )> 0
    order by
```

```
         bandwidth desc
```

Dataset Name	Description	Log Category
bandwidth-app-Traffic-By-Active-User-Number	Bandwidth application traffic by active user number	traffic

```
      select
         $flex_timescale(timestamp) as hodex,
         count(
            distinct(user_src)
         ) as total_user
      from
         ###(select $flex_timestamp as timestamp, coalesce(nullifna(`user`), nullifna
             (`unauthuser`), ipstr(`srcip`)) as user_src from $log where $filter and logid_to_
             int(logid) not in (4, 7, 14) group by timestamp, user_src order by timestamp
             desc)### t group by hodex order by hodex
```

Dataset Name	Description	Log Category
bandwidth-app-Top-Dest-By-Bandwidth-Sessions	Bandwidth application top dest by bandwidth usage sessions	traffic

```
      select
         coalesce(
            nullifna(
               root_domain(hostname)
            ),
            ipstr(`dstip`)
         ) as domain,
         sum(
            coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
         ) as bandwidth,
         sum(
            coalesce(rcvdbyte, 0)
         ) as traffic_in,
         sum(
            coalesce(sentbyte, 0)
         ) as traffic_out,
         count(*) as sessions
      from
         $log
      where
         $filter
         and logid_to_int(logid) not in (4, 7, 14)
      group by
         domain
      order by
         bandwidth desc
```

Dataset Name	Description	Log Category
bandwidth-app-Top-Policies-By-Bandwidth-Sessions	Top policies by bandwidth and sessions	traffic

```
      select
         coalesce(
            cast(poluuid as text),
            cast(policyid as text)
         ) as polid,
         sum(
            coalesce(rcvdbyte, 0) + coalesce(sentbyte, 0)
         ) as bandwidth,
         sum(
            coalesce(rcvdbyte, 0)
         ) as traffic_in,
         sum(
            coalesce(sentbyte, 0)
         ) as traffic_out,
         count(*) as sessions
      from
         $log
      where
         $filter
         and logid_to_int(logid) not in (4, 7, 14)
      group by
         polid
      order by
         bandwidth desc
```

Dataset Name	Description	Log Category
bandwidth-app-Traffic-Statistics	Bandwidth application traffic statistics	traffic

```
drop
   table if exists stats_temp; create temporary table stats_temp(
      total_sessions varchar(255),
      total_bandwidth varchar(255),
      ave_session varchar(255),
      ave_bandwidth varchar(255),
      active_date varchar(255),
      total_users varchar(255),
      total_app varchar(255),
      total_dest varchar(255)
   ); insert into stats_temp (
      total_sessions, total_bandwidth,
      ave_session, ave_bandwidth
   )
select
   format_numeric_no_decimal(
      sum(sessions)
   ) as total_sessions,
   bandwidth_unit(
      sum(bandwidth)
   ) as total_bandwidth,
   format_numeric_no_decimal(
      cast(
         sum(sessions)/ $days_num as decimal(18, 0)
      )
   ) as ave_session,
   bandwidth_unit(
      cast(
         sum(bandwidth)/ $days_num as decimal(18, 0)
      )
```

```
  ) as ave_bandwidth
from
  ###(select count(*) as sessions, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as
    bandwidth from $log where $filter and logid_to_int(logid) not in (4, 7, 14))### t;
    update stats_temp set active_date=t1.dom from (select dom, sum(sessions) as
    sessions from ###(select $DAY_OF_MONTH as dom, count(*) as sessions from $log where
    $filter and logid_to_int(logid) not in (4, 7, 14) group by dom order by sessions
    desc)### t group by dom order by sessions desc limit 1) as t1; update stats_temp
    set total_users=t2.totalnum from (select format_numeric_no_decimal(count(distinct
    (user_src))) as totalnum from ###(select coalesce(nullifna(`user`), nullifna
    (`unauthuser`), ipstr(`srcip`)) as user_src, count(*) as count from $log where
    $filter and logid_to_int(logid) not in (4, 7, 14) group by user_src order by count
    desc)### t) as t2; update stats_temp set total_app=t3.totalnum from (select format_
    numeric_no_decimal(count(distinct(app_grp))) as totalnum from ###(select app_group_
    name(app) as app_grp, count(*) as count from $log where $filter and logid_to_int
    (logid) not in (4, 7, 14) and nullifna(app) is not null group by app_grp order by
    count desc)### t) as t3; update stats_temp set total_dest=t4.totalnum from (select
    format_numeric_no_decimal(count(distinct(dstip))) as totalnum from ###(select
    dstip, count(*) as count from $log where $filter and logid_to_int(logid) not in (4,
    7, 14) and dstip is not null group by dstip order by count desc)### t ) as t4;
    select 'Total Sessions' as summary, total_sessions as stats from stats_temp union
    all select 'Total Bytes Transferred' as summary, total_bandwidth as stats from
    stats_temp union all select 'Most Active Date By Sessions' as summary, active_date
    as stats from stats_temp union all select 'Total Users' as summary, total_users as
    stats from stats_temp union all select 'Total Applications' as summary, total_app
    as stats from stats_temp union all select 'Total Destinations' as summary, total_
    dest as stats from stats_temp union all select 'Average Sessions Per Day' as
    summary, ave_session as stats from stats_temp union all select 'Average Bytes Per
    Day' as summary, ave_bandwidth as stats from stats_temp
```

Dataset Name	Description	Log Category
Score-Summary-For-All-Users-Devices	Reputation score summary for all users devices	traffic

```
select
  $flex_timescale(timestamp) as hodex,
  sum(scores) as scores
from
  ###(select $flex_timestamp as timestamp, sum(crscore%65536) as scores from $log where
    $filter and logid_to_int(logid) not in (4, 7, 14) and crscore is not null group by
    timestamp having sum(crscore%65536)>0 order by timestamp desc)### t group by hodex
    order by hodex
```

Dataset Name	Description	Log Category
Number-Of-Incidents-For-All-Users-Devices	Reputation number of incidents for all users devices	traffic

```
select
  $flex_timescale(timestamp) as hodex,
  sum(scores) as scores,
  sum(totalnum) as totalnum
from
  ###(select $flex_timestamp as timestamp, sum(crscore%65536) as scores, count(*) as
    totalnum from $log where $filter and logid_to_int(logid) not in (4, 7, 14) and
    crscore is not null group by timestamp having sum(crscore%65536)>0 order by
    timestamp desc)### t group by hodex order by hodex
```

Dataset Name	Description	Log Category
Top-Users-By-Reputation-Scores	Reputation top users by scores	traffic

```
select
   coalesce(
      nullifna(`user`),
      nullifna(`unauthuser`),
      ipstr(`srcip`)
   ) as user_src,
   sum(crscore % 65536) as scores
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and crscore is not null
group by
   user_src
having
   sum(crscore % 65536)> 0
order by
   scores desc
```

Dataset Name	Description	Log Category
Top-Devices-By-Reputation-Scores	Reputation top devices by scores	traffic

```
select
   devtype,
   coalesce(
      nullifna(`srcname`),
      nullifna(`srcmac`),
      ipstr(`srcip`)
   ) as dev_src,
   sum(crscore % 65536) as scores
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and crscore is not null
group by
   devtype,
   dev_src
having
   sum(crscore % 65536)> 0
order by
   scores desc
```

Dataset Name	Description	Log Category
Top-Users-With-Increased-Scores	Reputation top users with increased scores	traffic

```
drop
   table if exists prd1_usr_tbl;
```

```
drop
   table if exists prd2_usr_tbl; create temporary table prd1_usr_tbl as ###(select
       coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as f_user, sum
       (crscore%65536) as sum_rp_score from $log where $pre_period $filter and logid_to_
       int(logid) not in (4, 7, 14) and crscore is not null group by f_user having sum
       (crscore%65536)>0 order by sum_rp_score desc)###; create temporary table prd2_usr_
       tbl as ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr
       (`srcip`)) as f_user, sum(crscore%65536) as sum_rp_score from $log where $filter
       and logid_to_int(logid) not in (4, 7, 14) and crscore is not null group by f_user
       having sum(crscore%65536)>0 order by sum_rp_score desc)###; select t1.f_user, sum
       (t1.sum_rp_score) as t1_sum_score, sum(t2.sum_rp_score) as t2_sum_score, (sum
       (t2.sum_rp_score)-sum(t1.sum_rp_score)) as delta from prd1_usr_tbl as t1 inner join
       prd2_usr_tbl as t2 on t1.f_user=t2.f_user where t2.sum_rp_score > t1.sum_rp_score
       group by t1.f_user order by delta desc
```

Dataset Name	Description	Log Category
Top-Devices-With-Increased-Scores	Reputation top devices with increased scores	traffic

```
drop
   table if exists prd1_dev_tbl;
drop
   table if exists prd2_dev_tbl; create temporary table prd1_dev_tbl as ###(select
       coalesce(nullifna(`srcname`),nullifna(`srcmac`), ipstr(`srcip`)) as f_device,
       devtype, sum(crscore%65536) as sum_rp_score from $log where $pre_period $filter and
       logid_to_int(logid) not in (4, 7, 14) and crscore is not null group by f_device,
       devtype having sum(crscore%65536)>0 order by sum_rp_score desc)###; create
       temporary table prd2_dev_tbl as ###(select coalesce(nullifna(`srcname`),nullifna
       (`srcmac`), ipstr(`srcip`)) as f_device, devtype, sum(crscore%65536) as sum_rp_
       score from $log where $filter and logid_to_int(logid) not in (4, 7, 14) and crscore
       is not null group by f_device, devtype having sum(crscore%65536)>0 order by sum_rp_
       score desc)###; select t1.f_device, t1.devtype , sum(t1.sum_rp_score) as t1_sum_
       score, sum(t2.sum_rp_score) as t2_sum_score, (sum(t2.sum_rp_score)-sum(t1.sum_rp_
       score)) as delta from prd1_dev_tbl as t1 inner join prd2_dev_tbl as t2 on t1.f_
       device=t2.f_device and t1.devtype=t2.devtype where t2.sum_rp_score > t1.sum_rp_
       score group by t1.f_device, t1.devtype order by delta desc
```

Dataset Name	Description	Log Category
Attacks-By-Severity	Threat attacks by severity	attack

```
select
   (
      case when severity = 'critical' then 'Critical' when severity = 'high' then 'High'
          when severity = 'medium' then 'Medium' when severity = 'low' then 'Low' when
          severity = 'info' then 'Info' end
   ) as severity,
   count(*) as totalnum
from
   $log
where
   $filter
group by
   severity
order by
   totalnum desc
```

Dataset Name	Description	Log Category
Top-Attacks-Detected	Threat top attacks detected	attack

```
select
   attack,
   attackid,
   cve,
   severity,
   sum(attack_count) as attack_count
from
   ###(select attack, attackid, t1.severity, cve, (case when t1.severity = 'critical' then
       1 when t1.severity = 'high' then 2 when t1.severity = 'medium' then 3 when
       t1.severity = 'low' then 4 else 5 end) as severity_level, count(*) as attack_count
       from $log t1 left join ips_mdata t2 on t1.attack=t2.name where $filter and nullifna
       (attack) is not null group by attack, attackid, t1.severity, severity_level, cve
       order by severity_level, attack_count desc)### t group by attack, attackid,
       severity, severity_level, cve order by severity_level, attack_count desc
```

Dataset Name	Description	Log Category
Top-Attacks-Blocked	Threat top attacks blocked	attack

```
select
   attack,
   count(*) as attack_count
from
   $log
where
   $filter
   and nullifna(attack) is not null
   and action in (
      'deny', 'blocked', 'reset', 'dropped'
   )
group by
   attack
order by
   attack_count desc
```

Dataset Name	Description	Log Category
Top-Virus-Source	Threat top virus source	traffic

```
select
   srcip,
   hostname,
   sum(totalnum) as totalnum
from
   (
      ###(select srcip, hostname, count(*) as totalnum from $log-traffic where $filter and
          logid_to_int(logid) not in (4, 7, 14) and utmevent is not null and virus is not
          null group by srcip, hostname order by totalnum desc)### union all ###(select
          srcip , ipstr(`dstip`) as hostname, count(*) as totalnum from $log-virus where
          $filter and (eventtype is null or logver>=52) and nullifna(virus) is not null
          group by srcip, hostname order by totalnum desc)###) t group by srcip, hostname
          order by totalnum desc
```

Dataset Name	Description	Log Category
Intrusion-in-Last-7-Days	Threat intrusion timeline	attack

```
select
   $flex_timescale(timestamp) as hodex,
   sum(totalnum) as totalnum
from
   ###(select $flex_timestamp as timestamp, count(*) as totalnum from $log where $filter
       group by timestamp order by timestamp desc)### t group by hodex order by hodex
```

Dataset Name	Description	Log Category
Virus-Time-Line	Threat virus timeline	virus

```
select
   $flex_timescale(timestamp) as hodex,
   sum(totalnum) as totalnum
from
   (
      ###(select $flex_timestamp as timestamp, count(*) as totalnum from $log-traffic
          where $filter and logid_to_int(logid) not in (4, 7, 14) and utmevent is not null
          and virus is not null group by timestamp order by timestamp desc)### union all
          ###(select $flex_timestamp as timestamp, count(*) as totalnum from $log-virus
          where $filter and (eventtype is null or logver>=52) and nullifna(virus) is not
          null group by timestamp order by timestamp desc)###) t group by hodex order by
          hodex
```

Dataset Name	Description	Log Category
Top-Spyware-Victims	Threat top spyware victims	virus

```
select
   user_src,
   sum(totalnum) as totalnum
from
   ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, virus, count(*) as
       totalnum from $log where $filter group by user_src, virus order by totalnum
       desc)### t where virus like 'Riskware%' group by user_src order by totalnum desc
```

Dataset Name	Description	Log Category
Top-Spyware-by-Name	Threat top spyware by name	virus

```
select
   virus,
   max(virusid) as virusid,
   sum(totalnum) as totalnum
from
   ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, virus, virusid,
       count(*) as totalnum from $log where $filter group by user_src, virus, virusid
       order by totalnum desc)### t where virus like 'Riskware%' group by virus order by
       totalnum desc
```

Dataset Name	Description	Log Category
Top-Spyware-Source	Threat top spyware source	traffic

```
select
   srcip,
   hostname,
   count(*) as totalnum
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and virus like 'Riskware%'
group by
   srcip,
   hostname
order by
   totalnum desc
```

Dataset Name	Description	Log Category
Spyware-Time-Line	Threat spyware timeline	virus

```
select
   $flex_timescale(timestamp) as hodex,
   sum(totalnum) as totalnum
from
   ###(select $flex_timestamp as timestamp, count(*) as totalnum from $log where $filter
       and virus like 'Riskware%' group by timestamp order by timestamp desc)### t group
       by hodex order by hodex
```

Dataset Name	Description	Log Category
Top-Adware-Victims	Threat top adware victims	virus

```
select
   user_src,
   sum(totalnum) as totalnum
from
   ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, virus, count(*) as
       totalnum from $log where $filter group by user_src, virus order by totalnum
       desc)### t where virus like 'Adware%' group by user_src order by totalnum desc
```

Dataset Name	Description	Log Category
Top-Adware-by-Name	Threat top adware by name	virus

```
select
   virus,
   max(virusid) as virusid,
   sum(totalnum) as totalnum
from
   ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, virus, virusid,
       count(*) as totalnum from $log where $filter group by user_src, virus, virusid
       order by totalnum desc)### t where virus like 'Adware%' group by virus order by
       totalnum desc
```

Dataset Name	Description	Log Category
Top-Adware-Source	Threat top adware source	traffic

```
select
   srcip,
   hostname,
   count(*) as totalnum
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and virus like 'Adware%'
group by
   srcip,
   hostname
order by
   totalnum desc
```

Dataset Name	Description	Log Category
Adware-Time-Line	Threat adware timeline	virus

```
select
   $flex_timescale(timestamp) as hodex,
   sum(totalnum) as totalnum
from
   ###(select $flex_timestamp as timestamp, count(*) as totalnum from $log where $filter
       and virus like 'Adware%' group by timestamp order by timestamp desc)### t group by
       hodex order by hodex
```

Dataset Name	Description	Log Category
Intrusions-Timeline-By-Severity	Threat intrusions timeline by severity	attack

```
select
   $flex_timescale(timestamp) as timescale,
   sum(critical) as critical,
   sum(high) as high,
   sum(medium) as medium,
   sum(low) as low,
   sum(info) as info
from
   ###(select $flex_timestamp as timestamp, sum(case when severity = 'critical' then 1
       else 0 end) as critical, sum(case when severity = 'high' then 1 else 0 end) as
       high, sum(case when severity = 'medium' then 1 else 0 end) as medium, sum(case when
       severity = 'notice' then 1 else 0 end) as low, sum(case when severity = 'info' or
       severity = 'debug' then 1 else 0 end) as info from $log where $filter group by
       timestamp order by timestamp desc)### t group by timescale order by timescale
```

Dataset Name	Description	Log Category
Important-Intrusions-Timeline-By-Severity	Threat intrusions timeline by severity	attack

```
select
```

```
    $flex_timescale(timestamp) as timescale,
    sum(critical) as critical,
    sum(high) as high,
    sum(medium) as medium,
    sum(low) as low,
    sum(info) as info
from
    ###(select $flex_timestamp as timestamp, sum(case when severity = 'critical' then 1
        else 0 end) as critical, sum(case when severity = 'high' then 1 else 0 end) as
        high, sum(case when severity = 'medium' then 1 else 0 end) as medium, sum(case when
        severity = 'notice' then 1 else 0 end) as low, sum(case when severity = 'info' or
        severity = 'debug' then 1 else 0 end) as info from $log where $filter group by
        timestamp order by timestamp desc)### t group by timescale order by timescale
```

Dataset Name	Description	Log Category
Top-Intrusions-By-Types	Threat top intrusions by types	attack

```
select
    vuln_type,
    count(*) as totalnum
from
    $log t1
    left join ips_mdata t2 on t1.attack = t2.name
where
    $filter
    and vuln_type is not null
group by
    vuln_type
order by
    totalnum desc
```

Dataset Name	Description	Log Category
Critical-Severity-Intrusions	Threat critical severity intrusions	attack

```
select
    attack,
    attackid,
    cve,
    vuln_type,
    count(*) as totalnum
from
    $log t1
    left join ips_mdata t2 on t1.attack = t2.name
where
    $filter
    and t1.severity = 'critical'
group by
    attack,
    attackid,
    cve,
    vuln_type
order by
    totalnum desc
```

Dataset Name	Description	Log Category
High-Severity-Intrusions	Threat high severity intrusions	attack

```
select
   attack,
   attackid,
   vuln_type,
   cve,
   count(*) as totalnum
from
   $log t1
   left join ips_mdata t2 on t1.attack = t2.name
where
   $filter
   and t1.severity = 'high'
group by
   attack,
   attackid,
   vuln_type,
   cve
order by
   totalnum desc
```

Dataset Name	Description	Log Category
Medium-Severity-Intrusions	Threat medium severity intrusions	attack

```
select
   attack,
   vuln_type,
   cve,
   count(*) as totalnum
from
   $log t1
   left join ips_mdata t2 on t1.attack = t2.name
where
   $filter
   and t1.severity = 'medium'
group by
   attack,
   vuln_type,
   cve
order by
   totalnum desc
```

Dataset Name	Description	Log Category
Top-Intrusion-Victims	Threat top intrusion victims	attack

```
select
   victim,
   sum(cri_num) as critical,
   sum(high_num) as high,
   sum(med_num) as medium,
   sum(cri_num + high_num + med_num) as totalnum
```

```
from
   ###(select dstip as victim, sum((case when severity='critical' then 1 else 0 end)) as
       cri_num, sum(case when severity='high' then 1 else 0 end) as high_num, sum(case
       when severity='medium' then 1 else 0 end) as med_num from $log where $filter and
       severity in ('critical', 'high', 'medium') group by victim)### t group by victim
       order by totalnum desc
```

Dataset Name	Description	Log Category
Top-Intrusion-Sources	Threat top intrusion sources	attack

```
select
   source,
   sum(cri_num) as critical,
   sum(high_num) as high,
   sum(med_num) as medium,
   sum(cri_num + high_num + med_num) as totalnum
from
   ###(select srcip as source, sum(case when severity='critical' then 1 else 0 end) as
       cri_num, sum(case when severity='high' then 1 else 0 end) as high_num, sum(case
       when severity='medium' then 1 else 0 end) as med_num from $log where $filter and
       severity in ('critical', 'high', 'medium') group by source)### t group by source
       order by totalnum desc
```

Dataset Name	Description	Log Category
Top-Blocked-Intrusions	Threat top blocked intrusions	attack

```
select
   attack,
   attackid,
   (
      case when t1.severity = 'critical' then 'Critical' when t1.severity = 'high' then
          'High' when t1.severity = 'medium' then 'Medium' when t1.severity = 'low' then
          'Low' when t1.severity = 'info' then 'Info' end
   ) as severity_name,
   count(*) as totalnum,
   vuln_type,
   (
      case when t1.severity = 'critical' then 0 when t1.severity = 'high' then 1 when
          t1.severity = 'medium' then 2 when t1.severity = 'low' then 3 when t1.severity =
          'info' then 4 else 5 end
   ) as severity_number
from
   $log t1
   left join ips_mdata t2 on t1.attack = t2.name
where
   $filter
   and nullifna(attack) is not null
   and action in (
      'deny', 'blocked', 'reset', 'dropped'
   )
group by
   attack,
   attackid,
   t1.severity,
   vuln_type
order by
```

```
   severity_number,
   totalnum desc
```

Dataset Name	Description	Log Category
Top-Monitored-Intrusions	Threat top monitored intrusions	attack

```
select
   attack,
   attackid,
   (
      case when t1.severity = 'critical' then 'Critical' when t1.severity = 'high' then
          'High' when t1.severity = 'medium' then 'Medium' when t1.severity = 'low' then
          'Low' when t1.severity = 'info' then 'Info' end
   ) as severity_name,
   count(*) as totalnum,
   vuln_type,
   (
      case when t1.severity = 'critical' then 0 when t1.severity = 'high' then 1 when
          t1.severity = 'medium' then 2 when t1.severity = 'low' then 3 when t1.severity =
          'info' then 4 else 5 end
   ) as severity_number
from
   $log t1
   left join ips_mdata t2 on t1.attack = t2.name
where
   $filter
   and nullifna(attack) is not null
   and action not in (
      'deny', 'blocked', 'reset', 'dropped'
   )
group by
   attack,
   attackid,
   t1.severity,
   vuln_type
order by
   severity_number,
   totalnum desc
```

Dataset Name	Description	Log Category
Attacks-Over-HTTP-HTTPs	Threat attacks over HTTP HTTPs	attack

```
select
   attack,
   attackid,
   (
      case when severity = 'critical' then 'Critical' when severity = 'high' then 'High'
          when severity = 'medium' then 'Medium' when severity = 'low' then 'Low' when
          severity = 'info' then 'Info' end
   ) as severity,
   count(*) as totalnum,
   (
      case when severity = 'critical' then 0 when severity = 'high' then 1 when severity =
          'medium' then 2 when severity = 'low' then 3 when severity = 'info' then 4 else
          5 end
   ) as severity_number
```

```
from
   $log
where
   $filter
   and severity in ('critical', 'high', 'medium')
   and upper(service) in ('HTTP', 'HTTPS')
group by
   attack,
   attackid,
   severity,
   severity_number
order by
   severity_number,
   totalnum desc
```

Dataset Name	Description	Log Category
default-AP-Detection-Summary-by-Status-OffWire	Default access point detection summary by status off-wire	event

```
select
   (
      case apstatus when 1 then 'rogue' when 2 then 'accepted' when 3 then 'suppressed'
          else 'others' end
   ) as ap_full_status,
   count(*) as totalnum
from
   (
      select
         apstatus,
         bssid,
         ssid
      from
         ###(select apstatus, bssid, ssid, count(*) as subtotal from $log where $filter
             and apstatus is not null and apstatus!=0 and bssid is not null and
             onwire='no' and logid_to_int(logid) in (43527, 43521, 43525, 43563, 43564,
             43565, 43566, 43569, 43570, 43571, 43582, 43583, 43584, 43585) group by
             apstatus, bssid, ssid order by subtotal desc)### t group by apstatus, bssid,
             ssid) t group by ap_full_status order by totalnum desc
```

Dataset Name	Description	Log Category
default-AP-Detection-Summary-by-Status-OffWire_table	Default access point detection summary by status off-wire	event

```
select
   (
      case apstatus when 1 then 'rogue' when 2 then 'accepted' when 3 then 'suppressed'
          else 'others' end
   ) as ap_full_status,
   count(*) as totalnum
from
   (
      select
         apstatus,
         bssid,
         ssid
      from
```

```
         ###(select apstatus, bssid, ssid, count(*) as subtotal from $log where $filter
            and apstatus is not null and apstatus!=0 and bssid is not null and
            onwire='no' and logid_to_int(logid) in (43527, 43521, 43525, 43563, 43564,
            43565, 43566, 43569, 43570, 43571, 43582, 43583, 43584, 43585) group by
            apstatus, bssid, ssid order by subtotal desc)### t group by apstatus, bssid,
            ssid) t group by ap_full_status order by totalnum desc
```

Dataset Name	Description	Log Category
default-AP-Detection-Summary-by-Status-OnWire	Default access point detection summary by status on-wire	event

```
select
   (
      case apstatus when 1 then 'rogue' when 2 then 'accepted' when 3 then 'suppressed'
          else 'others' end
   ) as ap_full_status,
   count(*) as totalnum
from
   (
      select
         apstatus,
         bssid,
         ssid
      from
         ###(select apstatus, bssid, ssid, count(*) as subtotal from $log where $filter
            and apstatus is not null and apstatus!=0 and bssid is not null and
            onwire='yes' and logid_to_int(logid) in (43527, 43521, 43525, 43563, 43564,
            43565, 43566, 43569, 43570, 43571, 43582, 43583, 43584, 43585) group by
            apstatus, bssid, ssid order by subtotal desc)### t group by apstatus, bssid,
            ssid) t group by ap_full_status order by totalnum desc
```

Dataset Name	Description	Log Category
default-AP-Detection-Summary-by-Status-OnWire_table	Default access point detection summary by status on-wire	event

```
select
   (
      case apstatus when 1 then 'rogue' when 2 then 'accepted' when 3 then 'suppressed'
          else 'others' end
   ) as ap_full_status,
   count(*) as totalnum
from
   (
      select
         apstatus,
         bssid,
         ssid
      from
         ###(select apstatus, bssid, ssid, count(*) as subtotal from $log where $filter
            and apstatus is not null and apstatus!=0 and bssid is not null and
            onwire='yes' and logid_to_int(logid) in (43527, 43521, 43525, 43563, 43564,
            43565, 43566, 43569, 43570, 43571, 43582, 43583, 43584, 43585) group by
            apstatus, bssid, ssid order by subtotal desc)### t group by apstatus, bssid,
            ssid) t group by ap_full_status order by totalnum desc
```

Dataset Name	Description	Log Category
default-Managed-AP-Summary	Default managed access point summary	event

```
select
   (
      case when (
         action like '%join%'
         and logid_to_int(logid) in (43522, 43551)
      ) then 'Authorized' else 'Unauthorized' end
   ) as ap_status,
   count(*) as totalnum
from
   $log
where
   $filter
   and logid_to_int(logid) in (43522, 43551)
group by
   ap_status
order by
   totalnum desc
```

Dataset Name	Description	Log Category
default-Managed-AP-Summary_table	Default managed access point summary	event

```
select
   (
      case when (
         action like '%join%'
         and logid_to_int(logid) in (43522, 43551)
      ) then 'Authorized' else 'Unauthorized' end
   ) as ap_status,
   count(*) as totalnum
from
   $log
where
   $filter
   and logid_to_int(logid) in (43522, 43551)
group by
   ap_status
order by
   totalnum desc
```

Dataset Name	Description	Log Category
default-Unclassified-AP-Summary	Default unclassified access point summary	event

```
select
   (
      case onwire when 'no' then 'off-wire' when 'yes' then 'on-wire' else 'others' end
   ) as ap_status,
   count(*) as totalnum
from
```

```
   ###(select onwire, ssid, bssid, count(*) as subtotal from $log where $filter and
      apstatus=0 and bssid is not null and logid_to_int(logid) in (43521, 43525, 43527,
      43563, 43564, 43565, 43566, 43569, 43570, 43571, 43582, 43583, 43584, 43585) group
      by onwire, ssid, bssid order by subtotal desc)### t group by ap_status order by
      totalnum desc
```

Dataset Name	Description	Log Category
default-Unclassified-AP-Summary_table	Default unclassified access point summary	event

```
select
   (
      case onwire when 'no' then 'off-wire' when 'yes' then 'on-wire' else 'others' end
   ) as ap_status,
   count(*) as totalnum
from
   ###(select onwire, ssid, bssid, count(*) as subtotal from $log where $filter and
      apstatus=0 and bssid is not null and logid_to_int(logid) in (43521, 43525, 43527,
      43563, 43564, 43565, 43566, 43569, 43570, 43571, 43582, 43583, 43584, 43585) group
      by onwire, ssid, bssid order by subtotal desc)### t group by ap_status order by
      totalnum desc
```

Dataset Name	Description	Log Category
default-selected-AP-Details-OffWire	Default selected access point details off-wire	event

```
select
   (
      case apstatus when 0 then 'unclassified' when 1 then 'rogue' when 2 then 'accepted'
         when 3 then 'suppressed' else 'others' end
   ) as ap_full_status,
   devid,
   vd,
   ssid,
   bssid,
   manuf,
   rssi,
   channel,
   radioband,
   from_dtime(
      min(dtime)
   ) as first_seen,
   from_dtime(
      max(dtime)
   ) as last_seen,
   detectionmethod,
   itime,
   onwire as on_wire
from
   $log
where
   $filter
   and apstatus is not null
   and bssid is not null
   and onwire = 'no'
   and logid_to_int(logid) in (
      43521, 43563, 43564, 43565, 43566, 43569,
      43570, 43571
   )
group by
   ap_full_status,
   devid,
   vd,
   ssid,
   bssid,
   manuf,
   rssi,
   channel,
   radioband,
   detectionmethod,
   itime,
   onwire,
   apstatus
```

Dataset Name	Description	Log Category
default-selected-AP-Details-OnWire	Default selected access point details on-wire	event

```
select
   (
      case apstatus when 0 then 'unclassified' when 1 then 'rogue' when 2 then 'accepted'
          when 3 then 'suppressed' else 'others' end
   ) as ap_full_status,
   devid,
   vd,
   ssid,
   bssid,
   manuf,
   rssi,
   channel,
   radioband,
   from_dtime(
      min(dtime)
   ) as first_seen,
   from_dtime(
      max(dtime)
   ) as last_seen,
   detectionmethod,
   itime,
   onwire as on_wire
from
   $log
where
   $filter
   and apstatus is not null
   and bssid is not null
   and onwire = 'yes'
   and logid_to_int(logid) in (
      43521, 43563, 43564, 43565, 43566, 43569,
      43570, 43571
   )
group by
   ap_full_status,
   devid,
   vd,
   ssid,
   bssid,
   manuf,
   rssi,
   channel,
   radioband,
   detectionmethod,
   itime,
   onwire,
   apstatus
```

Dataset Name	Description	Log Category
event-Wireless-Client-Details	Event wireless client details	event

```
drop
   table if exists ip_list; create temporary table ip_list as
select
   ip,
   lower(mac) as lmac,
   sn,
   ssid,
   channel,
   radioband,
   min(dtime) as first,
   max(dtime) as last
from
   $log - event
where
   $filter
   and ip is not null
   and mac is not null
   and sn is not null
   and ssid is not null
group by
   ip,
   lmac,
   sn,
   ssid,
   channel,
   radioband
order by
   ip;
select
   user_src,
   ip,
   lmac,
   sn,
   ssid,
   channel,
   radioband,
   from_dtime(first) as first_seen,
   from_dtime(last) as last_seen,
   cast(
      volume as decimal(18, 2)
   ) as bandwidth
```

```
from
   (
      select
         *
      from
         ip_list
         inner join (
            select
               user_src,
               srcip,
               sum(volume) as volume
            from
               ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr
                   (`srcip`)) as user_src, srcip, sum(coalesce(sentbyte, 0)+coalesce
                   (rcvdbyte, 0)) as volume from $log-traffic where $filter-time and logid_
                   to_int(logid) not in (4, 7, 14) and srcip is not null group by user_src,
                   srcip having sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0))>0 order by
                   volume desc)### t group by user_src, srcip order by user_src, srcip) t
                   on ip_list.ip = t.srcip) t order by volume desc
```

Dataset Name	Description	Log Category
event-Wireless-Accepted-Offwire	Event wireless accepted off-wire	event

```
select
   'accepted' as ap_full_status,
   devid,
   vd,
   ssid,
   bssid,
   manuf,
   channel,
   radioband,
   from_dtime(
      max(last_seen)
   ) as last_seen,
   detectionmethod,
   snclosest,
   'no' as on_wire
from
   ###(select devid, vd, ssid, bssid, manuf, channel, radioband, detectionmethod,
       snclosest, onwire, logid, apstatus, max(dtime) as last_seen from $log where $filter
       and bssid is not null and logid_to_int(logid) in (43521, 43525, 43563, 43564,
       43565, 43566, 43569, 43570, 43571) group by devid, vd, ssid, bssid, manuf, channel,
       radioband, detectionmethod, snclosest, onwire, logid, apstatus order by last_seen
       desc)### t where apstatus=2 and onwire='no' group by devid, vd, ssid, bssid, manuf,
       channel, radioband, detectionmethod, snclosest order by last_seen desc
```

Dataset Name	Description	Log Category
event-Wireless-Accepted-Onwire	Event wireless accepted on-wire	event

```
select
   'accepted' as ap_full_status,
   devid,
   vd,
   ssid,
   bssid,
   manuf,
   channel,
   radioband,
   from_dtime(
      max(last_seen)
   ) as last_seen,
   detectionmethod,
   snclosest,
   'yes' as on_wire
from
   ###(select devid, vd, ssid, bssid, manuf, channel, radioband, detectionmethod,
       snclosest, onwire, apstatus, max(dtime) as last_seen from $log where $filter and
       bssid is not null and logid_to_int(logid) in (43521, 43525, 43563, 43564, 43565,
       43566, 43569, 43570, 43571) group by devid, vd, ssid, bssid, manuf, channel,
       radioband, detectionmethod, snclosest, onwire, apstatus order by last_seen desc)###
       t where apstatus=2 and onwire='yes' group by devid, vd, ssid, bssid, manuf,
       channel, radioband, detectionmethod, snclosest order by last_seen desc
```

Dataset Name	Description	Log Category
event-Wireless-Rogue-Offwire	Event wireless rogue off-wire	event

```
select
   'rogue' as ap_full_status,
   devid,
   vd,
   ssid,
   bssid,
   manuf,
   channel,
   radioband,
   from_dtime(
      max(last_seen)
   ) as last_seen,
   detectionmethod,
   snclosest,
   'no' as on_wire
from
   ###(select devid, vd, ssid, bssid, manuf, channel, radioband, detectionmethod,
       snclosest, onwire, logid, apstatus, max(dtime) as last_seen from $log where $filter
       and bssid is not null and logid_to_int(logid) in (43521, 43525, 43563, 43564,
       43565, 43566, 43569, 43570, 43571) group by devid, vd, ssid, bssid, manuf, channel,
       radioband, detectionmethod, snclosest, onwire, logid, apstatus order by last_seen
       desc)### t where apstatus=1 and onwire='no' group by devid, vd, ssid, bssid, manuf,
       channel, radioband, detectionmethod, snclosest order by last_seen desc
```

Dataset Name	Description	Log Category
event-Wireless-Rogue-Onwire	Event wireless rogue on-wire	event

```
select
   'rogue' as ap_full_status,
   devid,
   vd,
   ssid,
   bssid,
   manuf,
   channel,
   radioband,
   from_dtime(
      max(last_seen)
   ) as last_seen,
   detectionmethod,
   snclosest,
   'yes' as on_wire
 from
   ###(select devid, vd, ssid, bssid, manuf, channel, radioband, detectionmethod,
       snclosest, onwire, apstatus, max(dtime) as last_seen from $log where $filter and
       bssid is not null and logid_to_int(logid) in (43521, 43525, 43563, 43564, 43565,
       43566, 43569, 43570, 43571) group by devid, vd, ssid, bssid, manuf, channel,
       radioband, detectionmethod, snclosest, onwire, apstatus order by last_seen desc)###
       t where apstatus=1 and onwire='yes' group by devid, vd, ssid, bssid, manuf,
       channel, radioband, detectionmethod, snclosest order by last_seen desc
```

Dataset Name	Description	Log Category
event-Wireless-Suppressed-Offwire	Event wireless suppressed off-wire	event

```
    select
      'suppressed' as ap_full_status,
      devid,
      vd,
      ssid,
      bssid,
      manuf,
      channel,
      radioband,
      from_dtime(
        max(last_seen)
      ) as last_seen,
      detectionmethod,
      snclosest,
      'no' as on_wire
    from
      ###(select devid, vd, ssid, bssid, manuf, channel, radioband, detectionmethod,
          snclosest, onwire, logid, apstatus, max(dtime) as last_seen from $log where $filter
          and bssid is not null and logid_to_int(logid) in (43521, 43525, 43563, 43564,
          43565, 43566, 43569, 43570, 43571) group by devid, vd, ssid, bssid, manuf, channel,
          radioband, detectionmethod, snclosest, onwire, logid, apstatus order by last_seen
          desc)### t where apstatus=3 and onwire='no' group by devid, vd, ssid, bssid, manuf,
          channel, radioband, detectionmethod, snclosest order by last_seen desc
```

Dataset Name	Description	Log Category
event-Wireless-Suppressed-Onwire	Event wireless suppressed on-wire	event

```
    select
      'suppressed' as ap_full_status,
      devid,
      vd,
      ssid,
      bssid,
      manuf,
      channel,
      radioband,
      from_dtime(
         max(last_seen)
      ) as last_seen,
      detectionmethod,
      snclosest,
      'yes' as on_wire
   from
      ###(select devid, vd, ssid, bssid, manuf, channel, radioband, detectionmethod,
          snclosest, onwire, apstatus, max(dtime) as last_seen from $log where $filter and
          bssid is not null and logid_to_int(logid) in (43521, 43525, 43563, 43564, 43565,
          43566, 43569, 43570, 43571) group by devid, vd, ssid, bssid, manuf, channel,
          radioband, detectionmethod, snclosest, onwire, apstatus order by last_seen desc)###
          t where apstatus=3 and onwire='yes' group by devid, vd, ssid, bssid, manuf,
          channel, radioband, detectionmethod, snclosest order by last_seen desc
```

Dataset Name	Description	Log Category
event-Wireless-Unclassified-Offwire	Event wireless unclassified off-wire	event

```
select
   'unclassified' as ap_full_status,
   devid,
   vd,
   ssid,
   bssid,
   manuf,
   channel,
   radioband,
   from_dtime(
      max(last_seen)
   ) as last_seen,
   detectionmethod,
   snclosest,
   'no' as on_wire
from
   ###(select devid, vd, ssid, bssid, manuf, channel, radioband, detectionmethod,
       snclosest, onwire, logid, apstatus, max(dtime) as last_seen from $log where $filter
       and bssid is not null and logid_to_int(logid) in (43521, 43525, 43563, 43564,
       43565, 43566, 43569, 43570, 43571) group by devid, vd, ssid, bssid, manuf, channel,
       radioband, detectionmethod, snclosest, onwire, logid, apstatus order by last_seen
       desc)### t where apstatus=0 and onwire='no' group by devid, vd, ssid, bssid, manuf,
       channel, radioband, detectionmethod, snclosest order by last_seen desc
```

Dataset Name	Description	Log Category
event-Wireless-Unclassified-Onwire	Event wireless unclassified on-wire	event

```
select
   'unclassified' as ap_full_status,
   devid,
   vd,
   ssid,
   bssid,
   manuf,
   channel,
   radioband,
   from_dtime(
      max(last_seen)
   ) as last_seen,
   detectionmethod,
   snclosest,
   'yes' as on_wire
from
   ###(select devid, vd, ssid, bssid, manuf, channel, radioband, detectionmethod,
       snclosest, onwire, apstatus, max(dtime) as last_seen from $log where $filter and
       bssid is not null and logid_to_int(logid) in (43521, 43525, 43563, 43564, 43565,
       43566, 43569, 43570, 43571) group by devid, vd, ssid, bssid, manuf, channel,
       radioband, detectionmethod, snclosest, onwire, apstatus order by last_seen desc)###
       t where apstatus=0 and onwire='yes' group by devid, vd, ssid, bssid, manuf,
       channel, radioband, detectionmethod, snclosest order by last_seen desc
```

Dataset Name	Description	Log Category
default-Top-IPSEC-Vpn-Dial-Up-User-By-Bandwidth	Default top IPsec VPN dial up user by bandwidth usage	event

```
select
   coalesce(
      xauthuser_agg,
      user_agg,
      ipstr(`remip`)
   ) as user_src,
   from_dtime(
      min(s_time)
   ) as start_time,
   sum(bandwidth) as bandwidth,
   sum(traffic_in) as traffic_in,
   sum(traffic_out) as traffic_out
from
   (
      select
         devid,
         vd,
         string_agg(distinct xauthuser_agg, ' ') as xauthuser_agg,
         string_agg(distinct user_agg, ' ') as user_agg,
         remip,
         tunnelid,
         min(s_time) as s_time,
         max(e_time) as e_time,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_in)+ max(max_traffic_
                out) else max(max_traffic_in)- min(min_traffic_in)+ max(max_traffic_out)-
                min(min_traffic_out) end
         ) as bandwidth,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_in) else max(max_
                traffic_in)- min(min_traffic_in) end
         ) as traffic_in,
         (
            case when min(s_time)= max(e_time) then max(max_traffic_out) else max(max_
                traffic_out)- min(min_traffic_out) end
         ) as traffic_out
      from
         ###(select devid, vd, nullifna(`xauthuser`) as xauthuser_agg, nullifna(`user`) as
             user_agg, remip, tunnelid, min(coalesce(dtime, 0)) as s_time, max(coalesce
             (dtime, 0)) as e_time, min(coalesce(sentbyte, 0)) as min_traffic_out, min
             (coalesce(rcvdbyte, 0)) as min_traffic_in, max(coalesce(sentbyte, 0)) as max_
             traffic_out, max(coalesce(rcvdbyte, 0)) as max_traffic_in from $log where
             $filter and subtype='vpn' and tunneltype like 'ipsec%' and not (tunnelip is
             null or (tunnelip='0.0.0.0' and logver is null)) and action in ('tunnel-
             stats', 'tunnel-down', 'tunnel-up') and tunnelid is not null group by devid,
             vd, xauthuser_agg, user_agg, remip, tunnelid order by tunnelid)### t group by
             devid, vd, remip, tunnelid) tt group by user_src having sum(bandwidth)>0
             order by bandwidth desc
```

Dataset Name	Description	Log Category
default-Top-Sources-Of-SSL-VPN-Tunnels-By-Bandwidth	Default top sources of SSL VPN tunnels by bandwidth usage	event

```
select
   remip as remote_ip,
   sum(traffic_in + traffic_out) as bandwidth
from
   (
      select
         devid,
         vd,
         remip,
         tunnelid,
         max(traffic_in) as traffic_in,
         max(traffic_out) as traffic_out
      from
         ###(select devid, vd, remip, tunnelid, max(coalesce(sentbyte, 0)) as traffic_out,
            max(coalesce(rcvdbyte, 0)) as traffic_in from $log where $filter and
            subtype='vpn' and tunneltype like 'ssl%' and action in ('tunnel-stats',
            'tunnel-down') and remip is not null and tunnelid is not null group by devid,
            vd, remip, tunnelid order by tunnelid)### t group by devid, vd, remip,
            tunnelid) tt group by remote_ip having sum(traffic_in+traffic_out)>0 order by
            bandwidth desc
```

Dataset Name	Description	Log Category
webfilter-Web-Activity-Summary-By-Requests	Webfilter web activity summary by requests	webfilter

```
select
   $flex_timescale(timestamp) as hodex,
   sum(allowed_request) as allowed_request,
   sum(blocked_request) as blocked_request
from
   (
      ###(select $flex_timestamp as timestamp, sum(case when utmaction!='blocked' then 1
         else 0 end) as allowed_request, sum(case when utmaction='blocked' then 1 else 0
         end) as blocked_request from $log-traffic where $filter and logid_to_int(logid)
         not in (4, 7, 14) and utmevent in ('webfilter', 'banned-word', 'web-content',
         'command-block', 'script-filter') group by timestamp order by timestamp desc)###
         union all ###(select $flex_timestamp as timestamp, sum(case when
         action!='blocked' then 1 else 0 end) as allowed_request, sum(case when
         action='blocked' then 1 else 0 end) as blocked_request from $log-webfilter where
         $filter and (eventtype is null or logver>=52) group by timestamp order by
         timestamp desc)###) t group by hodex order by hodex
```

Dataset Name	Description	Log Category
traffic-Browsing-Time-Summary	Traffic browsing time summary	traffic

```
select
   $flex_timescale(timestamp) as hodex,
   cast(
      sum(delta)/ 60.0 as decimal(18, 2)
   ) as browsetime
from
   ###(select $flex_timestamp as timestamp, sum($browse_time) as delta from $log where
       $filter and logid_to_int(logid) not in (4, 7, 14) group by timestamp having sum
       ($browse_time)>0 order by delta desc)### t group by hodex order by hodex
```

Dataset Name	Description	Log Category
traffic-Browsing-Time-Summary-Enhanced	Traffic browsing time summary enhanced	traffic

```
select
   $flex_timescale(timestamp) as hodex,
   cast(
      sum(delta)/ 60.0 as decimal(18, 2)
   ) as browsetime
from
   ###(select $flex_timestamp as timestamp, sum($browse_time2) as delta from $log where
       $filter and logid_to_int(logid) not in (4, 7, 14) group by timestamp having sum
       ($browse_time2)>0 order by delta desc)### t group by hodex order by hodex
```

Dataset Name	Description	Log Category
webfilter-Top-Web-Users-By-Blocked-Requests	Webfilter top web users by blocked requests	webfilter

```
select
   user_src,
   sum(requests) as requests
from
   (
      ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as
          user_src, count(*) as requests from $log-traffic where $filter and logid_to_int
          (logid) not in (4, 7, 14) and utmevent in ('webfilter', 'banned-word', 'web-
          content', 'command-block', 'script-filter') and coalesce(nullifna(`user`),
          nullifna(`unauthuser`), ipstr(`srcip`)) is not null and utmaction='blocked'
          group by user_src order by requests desc)### union all ###(select coalesce
          (nullifna(`user`), ipstr(`srcip`)) as user_src, count(*) as requests from $log-
          webfilter where $filter and (eventtype is null or logver>=52) and coalesce
          (nullifna(`user`), ipstr(`srcip`)) is not null and action='blocked' group by
          user_src order by requests desc)###) t group by user_src order by requests desc
```

Dataset Name	Description	Log Category
webfilter-Top-Web-Users-By-Allowed-Requests	Webfilter top web users by allowed requests	webfilter

```
select
   user_src,
   sum(requests) as requests
from
   (
      ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as
          user_src, count(*) as requests from $log-traffic where $filter and logid_to_int
          (logid) not in (4, 7, 14) and utmevent in ('webfilter', 'banned-word', 'web-
          content', 'command-block', 'script-filter') and coalesce(nullifna(`user`),
          nullifna(`unauthuser`), ipstr(`srcip`)) is not null and utmaction!='blocked'
          group by user_src order by requests desc)### union all ###(select coalesce
          (nullifna(`user`), ipstr(`srcip`)) as user_src, count(*) as requests from $log-
          webfilter where $filter and (eventtype is null or logver>=52) and coalesce
          (nullifna(`user`), ipstr(`srcip`)) is not null and action!='blocked' group by
          user_src order by requests desc)###) t group by user_src order by requests desc
```

Dataset Name	Description	Log Category
traffic-Top-Web-Users-By-Browsing-Time	Traffic top web users by browsing time	traffic

```
select
   user_src,
   sum(delta) as browsetime,
   sum(bandwidth) as bandwidth,
   sum(traffic_in) as traffic_in,
   sum(traffic_out) as traffic_out
from
   ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, sum($browse_time) as
       delta, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth, sum(coalesce
       (rcvdbyte, 0)) as traffic_in, sum(coalesce(sentbyte, 0)) as traffic_out from $log
       where $filter group by user_src having sum($browse_time)>0 order by delta desc)###
       t group by user_src order by browsetime desc
```

Dataset Name	Description	Log Category
webfilter-Top-Blocked-Web-Sites-By-Requests	Webfilter top blocked web sites by requests	webfilter

```
select
   domain,
   catdesc,
   sum(requests) as requests
from
   (
      ###(select hostname as domain, catdesc, count(*) as requests from $log-traffic where
          $filter and logid_to_int(logid) not in (4, 7, 14) and utmevent in ('webfilter',
          'banned-word', 'web-content', 'command-block', 'script-filter') and hostname is
          not null and utmaction='blocked' group by domain, catdesc order by requests
          desc)### union all ###(select hostname as domain, catdesc, count(*) as requests
          from $log-webfilter where $filter and (eventtype is null or logver>=52) and
          hostname is not null and catdesc is not null and action='blocked' group by
          domain, catdesc order by requests desc)###) t group by domain, catdesc order by
          requests desc
```

Dataset Name	Description	Log Category
webfilter-Top-Allowed-Web-Sites-By-Requests	Webfilter top allowed web sites by requests	webfilter

```
select
```

```
   domain,
   string_agg(distinct catdesc, ', ') as agg_catdesc,
   sum(requests) as requests
from
   (
      ###(select hostname as domain, catdesc, count(*) as requests from $log-traffic where
          $filter and logid_to_int(logid) not in (4, 7, 14) and utmevent in ('webfilter',
          'banned-word', 'web-content', 'command-block', 'script-filter') and hostname is
          not null and utmaction!='blocked' group by domain, catdesc order by requests
          desc)### union all ###(select hostname as domain, catdesc, count(*) as requests
          from $log-webfilter where $filter and (eventtype is null or logver>=52) and
          hostname is not null and catdesc is not null and action!='blocked' group by
          domain, catdesc order by requests desc)###) t group by domain order by requests
          desc
```

Dataset Name	Description	Log Category
webfilter-Top-Video-Streaming-Websites-By-Bandwidth	Webfilter top video streaming websites by bandwidth usage	webfilter

```
select
   domain,
   sum(bandwidth) as bandwidth,
   sum(traffic_in) as traffic_in,
   sum(traffic_out) as traffic_out
from
   ###(select coalesce(nullifna(root_domain(hostname)), 'other') as domain, sum(coalesce
       (sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth, sum(coalesce(rcvdbyte, 0)) as
       traffic_in, sum(coalesce(sentbyte, 0)) as traffic_out from $log-traffic where
       $filter and logid_to_int(logid) not in (4, 7, 14) and ((logver>=52 and countweb>0)
       or ((logver is null) and utmevent in ('webfilter', 'banned-word', 'web-content',
       'command-block', 'script-filter'))) and catdesc in ('Streaming Media and Download')
       group by domain having sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0))>0 order by
       bandwidth desc)### t group by domain order by bandwidth desc
```

Dataset Name	Description	Log Category
webfilter-Top-Blocked-Web-Categories	Webfilter top blocked web categories	webfilter

```
select
   catdesc,
   sum(requests) as requests
from
   (
      ###(select catdesc, count(*) as requests from $log-traffic where $filter and logid_
          to_int(logid) not in (4, 7, 14) and utmevent in ('webfilter', 'banned-word',
          'web-content', 'command-block', 'script-filter') and catdesc is not null and
          utmaction='blocked' group by catdesc order by requests desc)### union all ###
          (select catdesc, count(*) as requests from $log-webfilter where $filter and
          (eventtype is null or logver>=52) and catdesc is not null and action='blocked'
          group by catdesc order by requests desc)###) t group by catdesc order by
          requests desc
```

Dataset Name	Description	Log Category
webfilter-Top-Allowed-Web-Categories	Webfilter top allowed web categories	webfilter

```
select
  catdesc,
  sum(requests) as requests
from
  (
    ###(select catdesc, count(*) as requests from $log-traffic where $filter and logid_
        to_int(logid) not in (4, 7, 14) and utmevent in ('webfilter', 'banned-word',
        'web-content', 'command-block', 'script-filter') and catdesc is not null and
        utmaction!='blocked' group by catdesc order by requests desc)### union all ###
        (select catdesc, count(*) as requests from $log-webfilter where $filter and
        (eventtype is null or logver>=52) and catdesc is not null and action!='blocked'
        group by catdesc order by requests desc)###) t group by catdesc order by
        requests desc
```

Dataset Name	Description	Log Category
traffic-Top-50-Sites-By-Browsing-Time	Traffic top sites by browsing time	traffic

```
select
  hostname,
  string_agg(distinct catdesc, ', ') as agg_catdesc,
  sum(delta) as browsetime,
  sum(bandwidth) as bandwidth,
  sum(traffic_in) as traffic_in,
  sum(traffic_out) as traffic_out
from
  ###(select hostname, catdesc, sum($browse_time) as delta, sum(coalesce(sentbyte,
      0)+coalesce(rcvdbyte, 0)) as bandwidth, sum(coalesce(rcvdbyte, 0)) as traffic_in,
      sum(coalesce(sentbyte, 0)) as traffic_out from $log where $filter and logid_to_int
      (logid) not in (4, 7, 14) and hostname is not null group by hostname, catdesc
      having sum($browse_time)>0 order by delta desc)### t group by hostname order by
      browsetime desc
```

Dataset Name	Description	Log Category
traffic-Top-50-Sites-By-Browsing-Time-Enhanced	Traffic top sites by browsing time enhanced	traffic

```
select
  hostname,
  string_agg(distinct catdesc, ', ') as agg_catdesc,
  sum(delta) as browsetime,
  sum(bandwidth) as bandwidth,
  sum(traffic_in) as traffic_in,
  sum(traffic_out) as traffic_out
from
  ###(select hostname, catdesc, sum($browse_time2) as delta, sum(coalesce(sentbyte,
      0)+coalesce(rcvdbyte, 0)) as bandwidth, sum(coalesce(rcvdbyte, 0)) as traffic_in,
      sum(coalesce(sentbyte, 0)) as traffic_out from $log where $filter and logid_to_int
      (logid) not in (4, 7, 14) and hostname is not null group by hostname, catdesc
      having sum($browse_time2)>0 order by delta desc)### t group by hostname order by
      browsetime desc
```

Dataset Name	Description	Log Category
traffic-Top-10-Categories-By-Browsing-Time	Traffic top category by browsing time	traffic

```
select
   catdesc,
   sum(delta) as browsetime,
   sum(bandwidth) as bandwidth
from
   ###(select catdesc, sum($browse_time) as delta, sum(coalesce(sentbyte, 0)+coalesce
       (rcvdbyte, 0)) as bandwidth from $log where $filter and logid_to_int(logid) not in
       (4, 7, 14) and catdesc is not null group by catdesc having sum($browse_time)>0
       order by delta desc)### t group by catdesc order by browsetime desc
```

Dataset Name	Description	Log Category
traffic-Top-10-Categories-By-Browsing-Time-Enhanced	Traffic top category by browsing time enhanced	traffic

```
select
   catdesc,
   sum(delta) as browsetime,
   sum(bandwidth) as bandwidth
from
   ###(select catdesc, sum($browse_time2) as delta, sum(coalesce(sentbyte, 0)+coalesce
       (rcvdbyte, 0)) as bandwidth from $log where $filter and logid_to_int(logid) not in
       (4, 7, 14) and catdesc is not null group by catdesc having sum($browse_time2)>0
       order by delta desc)### t group by catdesc order by browsetime desc
```

Dataset Name	Description	Log Category
traffic-Top-Destination-Countries-By-Browsing-Time	Traffic top destination countries by browsing time	traffic

```
select
   dstcountry,
   sum(delta) as browsetime,
   sum(bandwidth) as bandwidth,
   sum(traffic_in) as traffic_in,
   sum(traffic_out) as traffic_out
from
   ###(select dstcountry, sum($browse_time) as delta, sum(coalesce(sentbyte, 0)+coalesce
       (rcvdbyte, 0)) as bandwidth, sum(coalesce(rcvdbyte, 0)) as traffic_in, sum(coalesce
       (sentbyte, 0)) as traffic_out from $log where $filter and logid_to_int(logid) not
       in (4, 7, 14) group by dstcountry having sum($browse_time)>0 order by delta
       desc)### t group by dstcountry order by browsetime desc
```

Dataset Name	Description	Log Category
traffic-Top-Destination-Countries-By-Browsing-Time-Enhanced	Traffic top destination countries by browsing time enhanced	traffic

```
select
   dstcountry,
   sum(delta) as browsetime,
   sum(bandwidth) as bandwidth,
   sum(traffic_in) as traffic_in,
   sum(traffic_out) as traffic_out
from
   ###(select dstcountry, sum($browse_time2) as delta, sum(coalesce(sentbyte, 0)+coalesce
       (rcvdbyte, 0)) as bandwidth, sum(coalesce(rcvdbyte, 0)) as traffic_in, sum(coalesce
       (sentbyte, 0)) as traffic_out from $log where $filter and logid_to_int(logid) not
       in (4, 7, 14) group by dstcountry having sum($browse_time2)>0 order by delta
       desc)### t group by dstcountry order by browsetime desc
```

Dataset Name	Description	Log Category
webfilter-Top-Search-Phrases	Webfilter top search phrases	webfilter

```
   select
      keyword,
      count(*) as requests
   from
      $log
   where
      $filter
      and keyword is not null
   group by
      keyword
   order by
      requests desc
```

Dataset Name	Description	Log Category
Top-10-Users-Browsing-Time	Estimated browsing time	traffic

```
   select
      coalesce(
         nullifna(`user`),
         nullifna(`unauthuser`),
         ipstr(`srcip`)
      ) as user_src,
      sum($browse_time) as browsetime
   from
      $log
   where
      $filter
      and logid_to_int(logid) not in (4, 7, 14)
   group by
      user_src
   having
      sum($browse_time)> 0
   order by
      browsetime desc
```

Dataset Name	Description	Log Category
Top-10-Users-Browsing-Time-Enhanced	Estimated browsing time enhanced	traffic

```
   select
      coalesce(
         nullifna(`user`),
         nullifna(`unauthuser`),
         ipstr(`srcip`)
      ) as user_src,
      sum($browse_time2) as browsetime
   from
      $log
   where
      $filter
      and logid_to_int(logid) not in (4, 7, 14)
   group by
      user_src
   having
      sum($browse_time2)> 0
   order by
      browsetime desc
```

Dataset Name	Description	Log Category
Estimated-Browsing-Time	Estimated browsing time	traffic

```
   select
      coalesce(
         nullifna(`user`),
         nullifna(`unauthuser`),
         ipstr(`srcip`)
      ) as user_src,
      sum($browse_time) as browsetime
   from
      $log
   where
      $filter
      and logid_to_int(logid) not in (4, 7, 14)
   group by
      user_src
   having
      sum($browse_time)> 0
   order by
      browsetime desc
```

Dataset Name	Description	Log Category
Estimated-Browsing-Time-Enhanced	Estimated browsing time enhanced	traffic

```
   select
      coalesce(
         nullifna(`user`),
         nullifna(`unauthuser`),
         ipstr(`srcip`)
      ) as user_src,
      sum($browse_time2) as browsetime
   from
      $log
   where
      $filter
      and logid_to_int(logid) not in (4, 7, 14)
   group by
      user_src
```

```
having
   sum($browse_time2)> 0
order by
   browsetime desc
```

Dataset Name	Description	Log Category
wifi-Top-AP-By-Bandwidth	Top access point by bandwidth usage	traffic

```
select
   srcintf,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and (
      srcssid is not null
      or dstssid is not null
   )
group by
   srcintf
having
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   )> 0
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
wifi-Top-AP-By-Client	Top access point by client	traffic

```
select
   srcintf,
   count(distinct srcmac) as totalnum
from
   ###(select srcintf, srcssid, osname, osversion, devtype, srcmac, count(*) as subtotal
       from $log where $filter and logid_to_int(logid) not in (4, 7, 14) and (srcssid is
       not null or dstssid is not null) and srcmac is not null group by srcintf, srcssid,
       osname, osversion, devtype, srcmac order by subtotal desc)### t group by srcintf
       order by totalnum desc
```

Dataset Name	Description	Log Category
wifi-Top-SSID-By-Bandwidth	Top SSIDs by bandwidth usage	traffic

```
select
   srcssid,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth
from
   $log
where
```

```
      $filter
      and logid_to_int(logid) not in (4, 7, 14)
      and srcssid is not null
   group by
      srcssid
   having
      sum(
         coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
      )> 0
   order by
      bandwidth desc
```

Dataset Name	Description	Log Category
wifi-Top-SSID-By-Client	Top SSIDs by client	traffic

```
   select
      srcssid,
      count(distinct srcmac) as totalnum
   from
      ###(select srcintf, srcssid, osname, osversion, devtype, srcmac, count(*) as subtotal
          from $log where $filter and logid_to_int(logid) not in (4, 7, 14) and (srcssid is
          not null or dstssid is not null) and srcmac is not null group by srcintf, srcssid,
          osname, osversion, devtype, srcmac order by subtotal desc)### t where srcssid is
          not null group by srcssid order by totalnum desc
```

Dataset Name	Description	Log Category
wifi-Top-App-By-Bandwidth	Top WiFi applications by bandwidth usage	traffic

```
   select
      appid,
      app,
      sum(
         coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
      ) as bandwidth
   from
      $log
   where
      $filter
      and logid_to_int(logid) not in (4, 7, 14)
      and (
         srcssid is not null
         or dstssid is not null
      )
      and nullifna(app) is not null
   group by
      appid,
      app
   having
      sum(
         coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
      )> 0
   order by
      bandwidth desc
```

Dataset Name	Description	Log Category
wifi-Top-Client-By-Bandwidth	Top WiFi client by bandwidth usage	traffic

```
select
   (
      coalesce(srcname, srcmac, 'unknown') || ' (' || coalesce(devtype, 'unknown') || ', '
          || coalesce(osname, '') || (
         case when osversion is null then '' else ' ' || osversion end
      ) || ')'
   ) as client,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and (
      srcssid is not null
      or dstssid is not null
   )
group by
   client
having
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   )> 0
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
wifi-Top-OS-By-Bandwidth	Top WiFi os by bandwidth usage	traffic

```
select
   (
      coalesce(osname, 'unknown') || ' ' || coalesce(osversion, '')
   ) as os,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and (
      srcssid is not null
      or dstssid is not null
   )
group by
   os
having
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   )> 0
 order by
   bandwidth desc
```

Dataset Name	Description	Log Category
wifi-Top-OS-By-WiFi-Client	Top WiFi os by WiFi client	traffic

```
select
  (
    coalesce(osname, 'unknown') || ' ' || coalesce(osversion, '')
  ) as os,
  count(distinct srcmac) as totalnum
from
  ###(select srcintf, srcssid, osname, osversion, devtype, srcmac, count(*) as subtotal
      from $log where $filter and logid_to_int(logid) not in (4, 7, 14) and (srcssid is
      not null or dstssid is not null) and srcmac is not null group by srcintf, srcssid,
      osname, osversion, devtype, srcmac order by subtotal desc)### t group by os order
      by totalnum desc
```

Dataset Name	Description	Log Category
wifi-Top-Device-By-Bandwidth	Top WiFi device by bandwidth usage	traffic

```
select
  devtype,
  sum(
    coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
  ) as bandwidth
from
  $log
where
  $filter
  and logid_to_int(logid) not in (4, 7, 14)
  and (
    srcssid is not null
    or dstssid is not null
  )
  and devtype is not null
group by
  devtype
having
  sum(
    coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
  )> 0
order by
  bandwidth desc
```

Dataset Name	Description	Log Category
wifi-Top-Device-By-Client	Top WiFi device by client	traffic

```
select
  devtype,
  count(distinct srcmac) as totalnum
from
```

```
   ###(select srcintf, srcssid, osname, osversion, devtype, srcmac, count(*) as subtotal
       from $log where $filter and logid_to_int(logid) not in (4, 7, 14) and (srcssid is
       not null or dstssid is not null) and srcmac is not null group by srcintf, srcssid,
       osname, osversion, devtype, srcmac order by subtotal desc)### t where devtype is
       not null group by devtype order by totalnum desc
```

Dataset Name	Description	Log Category
wifi-Overall-Traffic	WiFi overall traffic	traffic

```
select
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and (
      srcssid is not null
      or dstssid is not null
   )
```

Dataset Name	Description	Log Category
wifi-Num-Distinct-Client	WiFi num distinct client	traffic

```
select
   count(distinct srcmac) as totalnum
from
   ###(select srcintf, srcssid, osname, osversion, devtype, srcmac, count(*) as subtotal
       from $log where $filter and logid_to_int(logid) not in (4, 7, 14) and (srcssid is
       not null or dstssid is not null) and srcmac is not null group by srcintf, srcssid,
       osname, osversion, devtype, srcmac order by subtotal desc)### t
```

Dataset Name	Description	Log Category
Top30-Subnets-by-Bandwidth-and-Sessions	Top subnets by application bandwidth	traffic

```
select
   ip_subnet(`srcip`) as subnet,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth,
   sum(
      coalesce(rcvdbyte, 0)
   ) as traffic_in,
   sum(
      coalesce(sentbyte, 0)
   ) as traffic_out,
   count(*) as sessions
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
```

```
group by
   subnet
having
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   )> 0
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
Top30-Subnets-by-Application-Bandwidth	Top applications by bandwidth	traffic

```
select
   ip_subnet(`srcip`) as subnet,
   app_group_name(app) as app_group,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and nullifna(app) is not null
group by
   subnet,
   app_group
having
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   )> 0
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
Top30-Subnets-by-Application-Sessions	Top applications by sessions	traffic

```
select
   ip_subnet(`srcip`) as subnet,
   app_group_name(app) as app_group,
   count(*) as sessions
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and nullifna(app) is not null
group by
   subnet,
   app_group
order by
   sessions desc
```

Dataset Name	Description	Log Category
Top30-Subnets-by-Website-Bandwidth	Top websites and web category by bandwidth	traffic

```
select
  subnet,
  website,
  sum(bandwidth) as bandwidth
from
  ###(select ip_subnet(`srcip`) as subnet, hostname as website, sum(coalesce(sentbyte,
    0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-traffic where $filter and hostname
    is not null and logid_to_int(logid) not in (4, 7, 14) and ((logver>=52 and
    countweb>0) or ((logver is null) and utmevent in ('webfilter', 'banned-word', 'web-
    content', 'command-block', 'script-filter'))) group by subnet, website order by
    bandwidth desc)### t group by subnet, website order by bandwidth desc
```

Dataset Name	Description	Log Category
Top30-Subnets-by-Website-Hits	Top websites and web category by sessions	traffic

```
select
  subnet,
  website,
  sum(hits) as hits
from
  (
    ###(select ip_subnet(`srcip`) as subnet, hostname as website, count(*) as hits from
      $log-traffic where $filter and hostname is not null and logid_to_int(logid) not
      in (4, 7, 14) and utmevent in ('webfilter', 'banned-word', 'web-content',
      'command-block', 'script-filter') group by subnet, website order by hits
      desc)### union all ###(select ip_subnet(`srcip`) as subnet, hostname as website,
      count(*) as hits from $log-webfilter where $filter and hostname is not null and
      (eventtype is null or logver>=52) group by subnet, website order by hits
      desc)###) t group by subnet, website order by hits desc
```

Dataset Name	Description	Log Category
Top30-Subnets-with-Top10-User-by-Bandwidth	Top users by bandwidth	traffic

```
select
  ip_subnet(`srcip`) as subnet,
  coalesce(
    nullifna(`user`),
    nullifna(`unauthuser`),
    ipstr(`srcip`)
  ) as user_src,
  sum(
    coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
  ) as bandwidth
from
  $log
where
  $filter
  and logid_to_int(logid) not in (4, 7, 14)
  and srcip is not null
```

```
group by
   subnet,
   user_src
having
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   )> 0
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
Top30-Subnets-with-Top10-User-by-Sessions	Top users by sessions	traffic

```
select
   ip_subnet(`srcip`) as subnet,
   coalesce(
      nullifna(`user`),
      nullifna(`unauthuser`),
      ipstr(`srcip`)
   ) as user_src,
   count(*) as sessions
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
group by
   subnet,
   user_src
order by
   sessions desc
```

Dataset Name	Description	Log Category
app-Top-20-Category-and-Applications-by-Bandwidth	Top category and applications by bandwidth usage	traffic

```
select
   appcat,
   app,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
group by
   appcat,
   app
having
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   )> 0
```

```
      order by
         bandwidth desc
```

Dataset Name	Description	Log Category
app-Top-20-Category-and-Applications-by-Session	Top category and applications by session	traffic

```
      select
         appcat,
         app,
         count(*) as sessions
      from
         $log
      where
         $filter
         and logid_to_int(logid) not in (4, 7, 14)
      group by
         appcat,
         app
      order by
         sessions desc
```

Dataset Name	Description	Log Category
app-Top-500-Allowed-Applications-by-Bandwidth	Top allowed applications by bandwidth usage	traffic

```
      select
         from_itime(itime) as timestamp,
         coalesce(
            nullifna(`user`),
            nullifna(`unauthuser`),
            ipstr(`srcip`)
         ) as user_src,
         appcat,
         app,
         coalesce(
            root_domain(hostname),
            ipstr(dstip)
         ) as destination,
         sum(
            coalesce(`sentbyte`, 0)+ coalesce(`rcvdbyte`, 0)
         ) as bandwidth
      from
         $log
      where
         $filter
         and logid_to_int(logid) not in (4, 7, 14)
         and action in ('accept', 'close', 'timeout')
      group by
         timestamp,
         user_src,
         appcat,
         app,
         destination
      order by
```

```
   bandwidth desc
```

Dataset Name	Description	Log Category
app-Top-500-Blocked-Applications-by-Session	Top blocked applications by session	traffic

```
select
   coalesce(
      nullifna(`user`),
      nullifna(`unauthuser`),
      ipstr(`srcip`)
   ) as user_src,
   appcat,
   app,
   count(*) as sessions
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and action in (
      'deny', 'blocked', 'reset', 'dropped'
   )
group by
   user_src,
   appcat,
   app
order by
   sessions desc
```

Dataset Name	Description	Log Category
web-Detailed-Website-Browsing-Log	Web detailed website browsing log	traffic

```
select
   from_dtime(dtime) as timestamp,
   catdesc,
   hostname as website,
   status,
   sum(bandwidth) as bandwidth
from
   ###(select dtime, catdesc, hostname, cast(utmaction as text) as status, sum(coalesce
       (sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-traffic where $filter
       and hostname is not null and logid_to_int(logid) not in (4, 7, 14) and ((logver>=52
       and countweb>0) or ((logver is null) and utmevent in ('webfilter', 'banned-word',
       'web-content', 'command-block', 'script-filter'))) group by dtime, catdesc,
       hostname, utmaction order by dtime desc)### t group by dtime, catdesc, website,
       status order by dtime desc
```

Dataset Name	Description	Log Category
web-Hourly-Category-and-Website-Hits-Action	Web hourly category and website hits action	traffic

```
select
   hod,
   website,
   sum(hits) as hits
from
   (
      ###(select $hour_of_day as hod, (hostname || ' (' || coalesce(`catdesc`, 'Unknown')
          || ')') as website, count(*) as hits from $log-traffic where $filter and
          hostname is not null and logid_to_int(logid) not in (4, 7, 14) and utmevent in
          ('webfilter', 'banned-word', 'web-content', 'command-block', 'script-filter')
          group by hod, website order by hod, hits desc)### union all ###(select $hour_of_
          day as hod, (hostname || ' (' || coalesce(`catdesc`, 'Unknown') || ')') as
          website , count(*) as hits from $log-webfilter where $filter and hostname is not
          null and (eventtype is null or logver>=52) group by hod, website order by hod,
          hits desc)###) t group by hod, website order by hod, hits desc
```

Dataset Name	Description	Log Category
web-Top-20-Category-and-Websites-by-Bandwidth	Web top category and websites by bandwidth usage	traffic

```
select
   website,
   catdesc,
   sum(bandwidth) as bandwidth
from
   ###(select hostname as website, catdesc, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte,
       0)) as bandwidth from $log-traffic where $filter and hostname is not null and
       logid_to_int(logid) not in (4, 7, 14) and ((logver>=52 and countweb>0) or ((logver
       is null) and utmevent in ('webfilter', 'banned-word', 'web-content', 'command-
       block', 'script-filter'))) group by website, catdesc order by bandwidth desc)### t
       group by website, catdesc order by bandwidth desc
```

Dataset Name	Description	Log Category
web-Top-20-Category-and-Websites-by-Session	Web top category and websites by session	traffic

```
select
   website,
   catdesc,
   sum(hits) as hits
from
   (
      ###(select hostname as website, catdesc, count(*) as hits from $log-traffic where
          $filter and hostname is not null and logid_to_int(logid) not in (4, 7, 14) and
          utmevent in ('webfilter', 'banned-word', 'web-content', 'command-block',
          'script-filter') group by website, catdesc order by hits desc)### union all ###
          (select hostname as website, catdesc, count(*) as hits from $log-webfilter where
          $filter and hostname is not null and (eventtype is null or logver>=52) group by
          website, catdesc order by hits desc)###) t group by website, catdesc order by
          hits desc
```

Dataset Name	Description	Log Category
web-Top-500-Website-Sessions-by-Bandwidth	Web top website sessions by bandwidth usage	traffic

```
select
   from_dtime(dtime) as timestamp,
   user_src,
        website,
        catdesc,
        cast(
           sum(dura)/ 60 as decimal(18, 2)
        ) as dura,
        sum(bandwidth) as bandwidth
     from
        ###(select dtime, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as
           user_src, hostname as website, catdesc, sum(coalesce(duration, 0)) as dura, sum
           (coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log where $filter
           and hostname is not null and logid_to_int(logid) not in (4, 7, 14) and action in
           ('accept','close','timeout') group by dtime, user_src, website, catdesc having sum
           (coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0))>0 order by bandwidth desc)### t group
           by dtime, user_src, website, catdesc order by bandwidth desc
```

Dataset Name	Description	Log Category
web-Top-500-User-Visted-Websites-by-Bandwidth	Web top user visted websites by bandwidth usage	traffic

```
     select
        website,
        catdesc,
        sum(bandwidth) as bandwidth
     from
        ###(select hostname as website, catdesc, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte,
           0)) as bandwidth from $log-traffic where $filter and hostname is not null and
           logid_to_int(logid) not in (4, 7, 14) and ((logver>=52 and countweb>0) or ((logver
           is null) and utmevent in ('webfilter', 'banned-word', 'web-content', 'command-
           block', 'script-filter'))) group by hostname, catdesc having sum(coalesce(sentbyte,
           0)+coalesce(rcvdbyte, 0))>0 order by bandwidth desc)### t group by website, catdesc
           order by bandwidth desc
```

Dataset Name	Description	Log Category
web-Top-500-User-Visted-Websites-by-Session	Web top user visted websites by session	traffic

```
     select
        website,
        catdesc,
        sum(sessions) as sessions
     from
        (
           ###(select hostname as website, catdesc, count(*) as sessions from $log-traffic
              where $filter and hostname is not null and logid_to_int(logid) not in (4, 7, 14)
              and utmevent in ('webfilter', 'banned-word', 'web-content', 'command-block',
              'script-filter') group by hostname, catdesc order by sessions desc)### union all
              ###(select hostname as website, catdesc, count(*) as sessions from $log-
              webfilter where $filter and hostname is not null and (eventtype is null or
              logver>=52) group by hostname, catdesc order by sessions desc)###) t group by
              website, catdesc order by sessions desc
```

Dataset Name	Description	Log Category
fct-Installed-Feature-Summary	Installed Feature Summary	fct-event

```
     select
        clientfeature,
        count(*) as totalnum
     from
        $log
     where
        $filter
        and clientfeature is not null
     group by
        clientfeature
     order by
        totalnum desc
```

Dataset Name	Description	Log Category
fct-Device-by-Operating-System	Device by OS	fct-event

```
select
   os,
   count(*) as totalnum
from
   $log
where
   $filter
   and os is not null
group by
   os
order by
   totalnum desc
```

Dataset Name	Description	Log Category
fct-Installed-FortiClient-Version	FortiClient Version	fct-event

```
select
   fctver_short,
   count(distinct hostname) as totalnum
from
   ###(select fctver as fctver_short, hostname from $log where $filter and fctver is not
       null group by fctver_short, hostname)### t group by fctver_short order by totalnum
       desc
```

Dataset Name	Description	Log Category
fct-Endpoint-Profile-Deployment	Endpoint Profile Deployment	fct-event

```
select
   coalesce(
      nullifna(usingpolicy),
      'No Profile'
   ) as profile,
   count(*) as totalnum
from
   $log
where
   $filter
group by
   profile
order by
   totalnum desc
```

Dataset Name	Description	Log Category
fct-Client-Summary	Client Summary	fct-event

```
select
   hostname,
   deviceip,
   os,
   profile,
   hostuser,
   fctver
from
   ###(select hostname, deviceip, os, nullifna(usingpolicy) as profile, nullifna(`user`)
       as hostuser, fctver from $log where $filter and os is not null group by hostname,
       deviceip, os, profile, hostuser, fctver)### t group by hostname, deviceip, os,
       profile, hostuser, fctver
```

Dataset Name	Description	Log Category
fct-Total-Threats-Found	Total Threats Found	fct-traffic

```
select
   coalesce(
      nullifna(utmevent),
      'Unknown'
   ) as utmevent,
   count(*) as totalnum
from
   $log
where
   $filter
group by
   utmevent
order by
   totalnum desc
```

Dataset Name	Description	Log Category
fct-Top10-AV-Threats-Detected	Top AV Threats Detected	fct-traffic

```
select
   threat,
   count(*) as totalnum
from
   $log
where
   $filter
   and threat is not null
   and lower(utmevent)= 'antivirus'
group by
   threat
order by
   totalnum desc
```

Dataset Name	Description	Log Category
fct-Top10-Infected-Devices-with-Botnet	Top Infected Devices with Botnet	fct-traffic

```
select
   hostname,
   count(*) as totalnum
from
   $log
where
   $filter
   and hostname is not null
   and lower(utmevent) in ('webfilter', 'appfirewall')
   and lower(threat) like '%botnet%'
group by
   hostname
order by
   totalnum desc
```

Dataset Name	Description	Log Category
fct-Top10-Infected-Devices-with-Virus-Malware	Top Infected Devices with Virus Malware	fct-traffic

```
select
   hostname,
   count(*) as totalnum
from
   $log
where
   $filter
   and hostname is not null
   and lower(utmevent) in ('antivirus', 'antimalware')
group by
   hostname
order by
   totalnum desc
```

Dataset Name	Description	Log Category
fct-All-Antivirus-Antimalware-Detections	All Antivirus and Antimalware Detections	fct-traffic

```
select
   threat,
   hostname,
   coalesce(
      nullifna(`user`),
      'Unknown'
   ) as hostuser,
   utmaction
from
   $log
where
   $filter
```

```
      and lower(utmevent) in ('antivirus', 'antimalware')
   group by
      threat,
      hostname,
      hostuser,
      utmaction
```

Dataset Name	Description	Log Category
fct-Web-Filter-Violations	Web Filter Violations	fct-traffic

```
   select
      remotename,
      hostname,
      coalesce(
         nullifna(`user`),
         'Unknown'
      ) as hostuser,
      utmaction,
      count(*) as totalnum
   from
      $log
   where
      $filter
      and lower(utmevent)= 'webfilter'
   group by
      remotename,
      hostname,
      hostuser,
      utmaction
```

Dataset Name	Description	Log Category
fct-Application-Firewall	Application Firewall	fct-traffic

```
   select
      threat,
      hostname,
      coalesce(
         nullifna(`user`),
         'Unknown'
      ) as hostuser,
      utmaction
   from
      $log
   where
      $filter
      and lower(utmevent)= 'appfirewall'
   group by
      threat,
      hostname,
      hostuser,
      utmaction
```

Dataset Name	Description	Log Category
fct-Errors-and-Alerts	Errors and Alerts	fct-event

```
select
   msg,
   hostname,
   coalesce(
      nullifna(`user`),
      'Unknown'
   ) as hostuser
from
   $log
where
   $filter
   and level in ('error', 'alert')
group by
   msg,
   hostname,
   hostuser
```

Dataset Name	Description	Log Category
fct-Threats-by-Top-Devices	Threats by Top Devices	fct-traffic

```
select
   hostname,
   count(*) as totalnum
from
   $log
where
   $filter
   and hostname is not null
   and utmevent is not null
group by
   hostname
order by
   totalnum desc
```

Dataset Name	Description	Log Category
fct-vuln-Device-Vulnerabilities	Vulnerabilities Detected by User/Device	fct-netscan

```
select
   vulnseverity,
   count(distinct vulnname) as totalnum
from
   ###(select vulnseverity, vulnname from $log where $filter and nullifna(vulnseverity) is
      not null and nullifna(vulnname) is not null group by vulnseverity, vulnname)### t
      group by vulnseverity order by totalnum desc
```

Dataset Name	Description	Log Category
fct-vuln-Category-Type-Vulnerabilities	Vulnerabilities Detected by Category Type	fct-netscan

```
select
```

```
    vulncat,
    count(distinct vulnname) as totalnum
from
    ###(select vulncat, vulnname from $log where $filter and nullifna(vulncat) is not null
        and nullifna(vulnname) is not null group by vulncat, vulnname)### t group by
        vulncat order by totalnum desc
```

Dataset Name	Description	Log Category
fct-vuln-Vulnerabilities-by-OS	Forticlient Vulnerabilities by OS	fct-netscan

```
select
    os,
    count(distinct vulnname) as totalnum
from
    ###(select os, vulnname from $log where $filter and nullifna(os) is not null and
        nullifna(vulnname) is not null group by os, vulnname)### t group by os order by
        totalnum desc
```

Dataset Name	Description	Log Category
fct-vuln-Vulnerabilities-by-Risk-Level	Number Vulnerability by Device and Risk Level	fct-netscan

```
select
    vulnseverity,
    (
        case when vulnseverity = 'Critical' then 5 when vulnseverity = 'High' then 4 when
            vulnseverity = 'Medium' then 3 when vulnseverity = 'Low' then 2 when
            vulnseverity = 'Info' then 1 else 0 end
    ) as severity_number,
    count(distinct vulnname) as vuln_num,
    count(distinct devid) as dev_num
from
    ###(select vulnseverity, devid, vulnname from $log where $filter and nullifna
        (vulnseverity) is not null and nullifna(vulnname) is not null and nullifna(devid)
        is not null group by vulnseverity, vulnname, devid)### t group by vulnseverity
        order by dev_num desc, severity_number desc
```

Dataset Name	Description	Log Category
fct-vuln-Device-by-Risk-Level	Number Vulnerability by Device and Risk Level	fct-netscan

```
select
    vulnseverity,
    (
        case when vulnseverity = 'Critical' then 5 when vulnseverity = 'High' then 4 when
            vulnseverity = 'Medium' then 3 when vulnseverity = 'Low' then 2 when
            vulnseverity = 'Info' then 1 else 0 end
    ) as severity_number,
    count(distinct vulnname) as vuln_num,
    count(distinct devid) as dev_num
from
    ###(select vulnseverity, devid, vulnname from $log where $filter and nullifna
        (vulnseverity) is not null and nullifna(vulnname) is not null and nullifna(devid)
        is not null group by vulnseverity, vulnname, devid)### t group by vulnseverity
        order by dev_num desc, severity_number desc
```

Dataset Name	Description	Log Category
fct-vuln-Vulnerability-Trend	Vulnerability Trend	fct-netscan

```
select
  $flex_timescale(timestamp) as hodex,
  count(distinct vulnname) as total_num
from
  ###(select $flex_timestamp as timestamp, vulnname from $log where $filter and nullifna
      (vulnname) is not null group by timestamp, vulnname order by timestamp desc)### t
      group by hodex order by hodex
```

Dataset Name	Description	Log Category
fct-vuln-Details-by-Risk-Level-Device	Vulnerability Details for Each Risk Level by Device	fct-netscan

```
select
  devid,
  os,
  vulnseverity,
  count(distinct vulnname) as vuln_num,
  count(distinct products) as products,
  count(distinct cve_id) as cve_count
from
  ###(select devid, os, vulnname, vulnseverity, vulnid from $log where $filter and
      vulnname is not null and vulnseverity is not null group by devid, os, vulnname,
      vulnseverity, vulnid)### t1 left join fct_mdata t2 on t1.vulnid=t2.vid::int group
      by devid, os, vulnseverity order by vuln_num desc, devid
```

Dataset Name	Description	Log Category
fct-vuln-Details-by-Device-User	Vulnerability Details by Device User	fct-netscan

```
select
  devid,
  (
    '
```

' || vulnname || '
'

```
  ) as vulnname,
  vulnseverity,
  vulncat,
  string_agg(distinct products, ',') as products,
  string_agg(distinct cve_id, ',') as cve_list,
  (
    'Remediation Info'
  ) as vendor_link
from
  ###(select devid, vulnname, vulnseverity, vulncat, vulnid from $log where $filter and
      vulnname is not null group by devid, vulnname, vulnseverity, vulncat, vulnid)### t1
      inner join fct_mdata t2 on t1.vulnid=t2.vid::int group by devid, vulnname,
      vulnseverity, vulncat order by devid
```

Dataset Name	Description	Log Category
fct-vuln-Remediation-by-Device	Remediate The Vulnerability Found on Device	fct-netscan

```
        select
           devid,
           (
              '
```

' || vulnname || '

'

```
           ) as vulnname,
           vulnseverity,
           string_agg(distinct vendor_link, ',') as vendor_link
        from
           ###(select devid, vulnname, vulnseverity, vulnid from $log where $filter and vulnname
               is not null group by devid, vulnname, vulnseverity, vulnid)### t1 inner join fct_
               mdata t2 on t1.vulnid=t2.vid::int group by devid, vulnname, vulnseverity order by
               vulnseverity, devid
```

Dataset Name	Description	Log Category
fct-vuln-Remediation-by-Vulnerability	Remediation by Vulnerability	fct-netscan

```
        select
           (
              '' || vulnname || '

                  ' || 'Description
```

' || description || '

' || 'Affected Products

' || products || '

' || 'Impact

' || impact || '

' || 'Recommended Actions

' || vendor_link || '

'

```
           ) as remediation
        from
           ###(select devid, vulnname, vulnseverity, (case vulnseverity when 'low' then 1 when
               'info' then 2 when 'medium' then 3 when 'high' then 4 when 'critical' then 5 else 0
               end) as severity_level, vulnid from $log where $filter and vulnname is not null
               group by devid, vulnname, vulnseverity, severity_level, vulnid order by severity_
               level)### t1 inner join fct_mdata t2 on t1.vulnid=t2.vid::int group by remediation
               order by remediation
```

Dataset Name	Description	Log Category
fct-vuln-Top-30-Targeted-High-Risk-Vulnerabilities	Top 30 Targeted High Risk Vulnerabilities	fct-netscan

```
select
   t3.cve_id,
   score,
   string_agg(distinct products, ',') as products,
   (
      'Mitigation Infomation'
   ) as vendor_link
from
   ###(select vulnid from $log where $filter group by vulnid)### t1 inner join fct_mdata
       t2 on t2.vid=t1.vulnid::text inner join fct_cve_score t3 on strpos(t2.cve_id,
       t3.cve_id) > 0 group by t3.cve_id, score order by score desc, t3.cve_id
```

Dataset Name	Description	Log Category
os-Detect-OS-Count	Detected operation system count	traffic

```
select
   (
      coalesce(osname, 'Unknown')
   ) as os,
   count(*) as totalnum
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
group by
   os
order by
   totalnum desc
```

Dataset Name	Description	Log Category
drilldown-Top-App-By-Sessions-Table	Drilldown top applications by session count	traffic

```
select
   appid,
   app,
   sum(sessions) as sessions
from
   ###(select appid, app, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr
       (`srcip`)) as user_src, dstip, srcintf, dstintf, policyid, count(*) as sessions,
       sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log where
       $filter-exclude-var and logid_to_int(logid) not in (4, 7, 14) group by appid, app,
       user_src, dstip, srcintf, dstintf, policyid order by sessions desc)### t where
       $filter-drilldown and nullifna(app) is not null group by appid, app order by
       sessions desc
```

Dataset Name	Description	Log Category
drilldown-Top-App-By-Sessions-Bar	Drilldown top applications by session count	traffic

```
select
  appid,
  app,
  sum(sessions) as sessions
from
  ###(select appid, app, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr
      (`srcip`)) as user_src, dstip, srcintf, dstintf, policyid, count(*) as sessions,
      sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log where
      $filter-exclude-var and logid_to_int(logid) not in (4, 7, 14) group by appid, app,
      user_src, dstip, srcintf, dstintf, policyid order by sessions desc)### t where
      $filter-drilldown and nullifna(app) is not null group by appid, app order by
      sessions desc
```

Dataset Name	Description	Log Category
drilldown-Top-App-By-Bandwidth-Table	Drilldown top applications by bandwidth usage	traffic

```
select
  appid,
  app,
  sum(bandwidth) as bandwidth
from
  ###(select appid, app, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr
      (`srcip`)) as user_src, dstip, srcintf, dstintf, policyid, count(*) as sessions,
      sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log where
      $filter-exclude-var and logid_to_int(logid) not in (4, 7, 14) group by appid, app,
      user_src, dstip, srcintf, dstintf, policyid order by sessions desc)### t where
      $filter-drilldown and nullifna(app) is not null group by appid, app having sum
      (bandwidth)>0 order by bandwidth desc
```

Dataset Name	Description	Log Category
drilldown-Top-App-By-Bandwidth-Bar	Drilldown top applications by bandwidth usage	traffic

```
select
  appid,
  app,
  sum(bandwidth) as bandwidth
from
  ###(select appid, app, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr
      (`srcip`)) as user_src, dstip, srcintf, dstintf, policyid, count(*) as sessions,
      sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log where
      $filter-exclude-var and logid_to_int(logid) not in (4, 7, 14) group by appid, app,
      user_src, dstip, srcintf, dstintf, policyid order by sessions desc)### t where
      $filter-drilldown and nullifna(app) is not null group by appid, app having sum
      (bandwidth)>0 order by bandwidth desc
```

Dataset Name	Description	Log Category
drilldown-Top-Destination-By-Sessions-Table	Drilldown top destination by session count	traffic

```
select
  dstip,
  sum(sessions) as sessions
from
  ###(select appid, app, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr
      (`srcip`)) as user_src, dstip, srcintf, dstintf, policyid, count(*) as sessions,
      sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log where
      $filter-exclude-var and logid_to_int(logid) not in (4, 7, 14) group by appid, app,
      user_src, dstip, srcintf, dstintf, policyid order by sessions desc)### t where
      $filter-drilldown and dstip is not null group by dstip order by sessions desc
```

Dataset Name	Description	Log Category
drilldown-Top-Destination-By-Bandwidth-Table	Drilldown top destination by bandwidth usage	traffic

```
select
  dstip,
  sum(bandwidth) as bandwidth
from
  ###(select appid, app, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr
      (`srcip`)) as user_src, dstip, srcintf, dstintf, policyid, count(*) as sessions,
      sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log where
      $filter-exclude-var and logid_to_int(logid) not in (4, 7, 14) group by appid, app,
      user_src, dstip, srcintf, dstintf, policyid order by sessions desc)### t where
      $filter-drilldown and dstip is not null group by dstip having sum(bandwidth)>0
      order by bandwidth desc
```

Dataset Name	Description	Log Category
drilldown-Top-User-By-Sessions-Table	Drilldown top user by session count	traffic

```
select
  user_src,
  sum(sessions) as sessions
from
  ###(select appid, app, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr
      (`srcip`)) as user_src, dstip, srcintf, dstintf, policyid, count(*) as sessions,
      sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log where
      $filter-exclude-var and logid_to_int(logid) not in (4, 7, 14) group by appid, app,
      user_src, dstip, srcintf, dstintf, policyid order by sessions desc)### t where
      $filter-drilldown and user_src is not null group by user_src order by sessions desc
```

Dataset Name	Description	Log Category
drilldown-Top-User-By-Sessions-Bar	Drilldown top user by session count	traffic

```
select
  user_src,
  sum(sessions) as sessions
from
```

```
   ###(select appid, app, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr
       (`srcip`)) as user_src, dstip, srcintf, dstintf, policyid, count(*) as sessions,
       sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log where
       $filter-exclude-var and logid_to_int(logid) not in (4, 7, 14) group by appid, app,
       user_src, dstip, srcintf, dstintf, policyid order by sessions desc)### t where
       $filter-drilldown and user_src is not null group by user_src order by sessions desc
```

Dataset Name	Description	Log Category
drilldown-Top-User-By-Bandwidth-Table	Drilldown top user by bandwidth usage	traffic

```
select
   user_src,
   sum(bandwidth) as bandwidth
from
   ###(select appid, app, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr
       (`srcip`)) as user_src, dstip, srcintf, dstintf, policyid, count(*) as sessions,
       sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log where
       $filter-exclude-var and logid_to_int(logid) not in (4, 7, 14) group by appid, app,
       user_src, dstip, srcintf, dstintf, policyid order by sessions desc)### t where
       $filter-drilldown and user_src is not null group by user_src having sum
       (bandwidth)>0 order by bandwidth desc
```

Dataset Name	Description	Log Category
drilldown-Top-User-By-Bandwidth-Bar	Drilldown top user by bandwidth usage	traffic

```
select
   user_src,
   sum(bandwidth) as bandwidth
from
   ###(select appid, app, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr
       (`srcip`)) as user_src, dstip, srcintf, dstintf, policyid, count(*) as sessions,
       sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log where
       $filter-exclude-var and logid_to_int(logid) not in (4, 7, 14) group by appid, app,
       user_src, dstip, srcintf, dstintf, policyid order by sessions desc)### t where
       $filter-drilldown and user_src is not null group by user_src having sum
       (bandwidth)>0 order by bandwidth desc
```

Dataset Name	Description	Log Category
drilldown-Top-Web-User-By-Visit-Table	Drilldown top web user by visit	traffic

```
select
   user_src,
   sum(requests) as visits
from
   (
      ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as
          user_src, hostname, count(*) as requests from $log-traffic where $filter-
          exclude-var and logid_to_int(logid) not in (4, 7, 14) and utmevent in
          ('webfilter', 'banned-word', 'web-content', 'command-block', 'script-filter')
          and hostname is not null group by user_src, hostname order by requests desc)###
          union all ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src,
          hostname, count(*) as requests from $log-webfilter where $filter-exclude-var and
          (eventtype is null or logver>=52) and hostname is not null group by user_src,
          hostname order by requests desc)###) t where $filter-drilldown and user_src is
          not null group by user_src order by visits desc
```

Dataset Name	Description	Log Category
drilldown-Top-Web-User-By-Visit-Bar	Drilldown top web user by visit	traffic

```
select
   user_src,
   sum(requests) as visits
from
   (
      ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as
          user_src, hostname, count(*) as requests from $log-traffic where $filter-
          exclude-var and logid_to_int(logid) not in (4, 7, 14) and utmevent in
          ('webfilter', 'banned-word', 'web-content', 'command-block', 'script-filter')
          and hostname is not null group by user_src, hostname order by requests desc)###
          union all ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src,
          hostname, count(*) as requests from $log-webfilter where $filter-exclude-var and
          (eventtype is null or logver>=52) and hostname is not null group by user_src,
          hostname order by requests desc)###) t where $filter-drilldown and user_src is
          not null group by user_src order by visits desc
```

Dataset Name	Description	Log Category
drilldown-Top-Website-By-Request-Table	Drilldown top website by request	traffic

```
select
   hostname,
   sum(requests) as visits
from
   (
      ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as
          user_src, hostname, count(*) as requests from $log-traffic where $filter-
          exclude-var and logid_to_int(logid) not in (4, 7, 14) and utmevent in
          ('webfilter', 'banned-word', 'web-content', 'command-block', 'script-filter')
          and hostname is not null group by user_src, hostname order by requests desc)###
          union all ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src,
          hostname, count(*) as requests from $log-webfilter where $filter-exclude-var and
          (eventtype is null or logver>=52) and hostname is not null group by user_src,
          hostname order by requests desc)###) t where $filter-drilldown and hostname is
          not null group by hostname order by visits desc
```

Dataset Name	Description	Log Category
drilldown-Top-Website-By-Request-Bar	Drilldown top website by request	traffic

```
select
   hostname,
   sum(requests) as visits
from
   (
      ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as
          user_src, hostname, count(*) as requests from $log-traffic where $filter-
          exclude-var and logid_to_int(logid) not in (4, 7, 14) and utmevent in
          ('webfilter', 'banned-word', 'web-content', 'command-block', 'script-filter')
```

```
            and hostname is not null group by user_src, hostname order by requests desc)###
            union all ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src,
            hostname, count(*) as requests from $log-webfilter where $filter-exclude-var and
            (eventtype is null or logver>=52) and hostname is not null group by user_src,
            hostname order by requests desc)###) t where $filter-drilldown and hostname is
            not null group by hostname order by visits desc
```

Dataset Name	Description	Log Category
drilldown-Top-Email-Sender-By-Volume	Drilldown top email sender by volume	traffic

```
select
   sender,
   sum(bandwidth) as volume
from
   (
      ###(select sender, recipient, count(*) as requests, sum(coalesce(sentbyte,
         0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-traffic where $filter-exclude-
         var and logid_to_int(logid) not in (4, 7, 14) and service in ('smtp', 'SMTP',
         '25/tcp', '587/tcp', 'smtps', 'SMTPS', '465/tcp') and utmevent in ('general-
         email-log', 'spamfilter') group by sender, recipient order by requests desc)###
         union all ###(select `from` as sender, `to` as recipient, count(*) as requests,
         sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-
         emailfilter where $filter-exclude-var and service in ('smtp', 'SMTP', '25/tcp',
         '587/tcp', 'smtps', 'SMTPS', '465/tcp') and eventtype is null group by `from`,
         `to` order by requests desc)###) t where $filter-drilldown and sender is not
         null group by sender having sum(bandwidth)>0 order by volume desc
```

Dataset Name	Description	Log Category
drilldown-Top-Email-Send-Recipient-By-Volume	Drilldown top email send recipient by volume	traffic

```
select
   recipient,
   sum(bandwidth) as volume
from
   (
      ###(select sender, recipient, count(*) as requests, sum(coalesce(sentbyte,
         0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-traffic where $filter-exclude-
         var and logid_to_int(logid) not in (4, 7, 14) and service in ('smtp', 'SMTP',
         '25/tcp', '587/tcp', 'smtps', 'SMTPS', '465/tcp') and utmevent in ('general-
         email-log', 'spamfilter') group by sender, recipient order by requests desc)###
         union all ###(select `from` as sender, `to` as recipient, count(*) as requests,
         sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-
         emailfilter where $filter-exclude-var and service in ('smtp', 'SMTP', '25/tcp',
         '587/tcp', 'smtps', 'SMTPS', '465/tcp') and eventtype is null group by `from`,
         `to` order by requests desc)###) t where $filter-drilldown and recipient is not
         null group by recipient having sum(bandwidth)>0 order by volume desc
```

Dataset Name	Description	Log Category
drilldown-Top-Email-Sender-By-Count	Drilldown top email sender by count	traffic

```
select
   sender,
   sum(requests) as requests
```

```
from
   (
     ###(select sender, recipient, count(*) as requests, sum(coalesce(sentbyte,
        0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-traffic where $filter-exclude-
        var and logid_to_int(logid) not in (4, 7, 14) and service in ('smtp', 'SMTP',
        '25/tcp', '587/tcp', 'smtps', 'SMTPS', '465/tcp') and utmevent in ('general-
        email-log', 'spamfilter') group by sender, recipient order by requests desc)###
        union all ###(select `from` as sender, `to` as recipient, count(*) as requests,
        sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-
        emailfilter where $filter-exclude-var and service in ('smtp', 'SMTP', '25/tcp',
        '587/tcp', 'smtps', 'SMTPS', '465/tcp') and eventtype is null group by `from`,
        `to` order by requests desc)###) t where $filter-drilldown and sender is not
        null group by sender order by requests desc
```

Dataset Name	Description	Log Category
drilldown-Top-Email-Send-Recipient-By-Count	Drilldown top email send recipient by count	traffic

```
select
   recipient,
   sum(requests) as requests
from
   (
     ###(select sender, recipient, count(*) as requests, sum(coalesce(sentbyte,
        0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-traffic where $filter-exclude-
        var and logid_to_int(logid) not in (4, 7, 14) and service in ('smtp', 'SMTP',
        '25/tcp', '587/tcp', 'smtps', 'SMTPS', '465/tcp') and utmevent in ('general-
        email-log', 'spamfilter') group by sender, recipient order by requests desc)###
        union all ###(select `from` as sender, `to` as recipient, count(*) as requests,
        sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-
        emailfilter where $filter-exclude-var and service in ('smtp', 'SMTP', '25/tcp',
        '587/tcp', 'smtps', 'SMTPS', '465/tcp') and eventtype is null group by `from`,
        `to` order by requests desc)###) t where $filter-drilldown and recipient is not
        null group by recipient order by requests desc
```

Dataset Name	Description	Log Category
drilldown-Top-Email-Recipient-By-Volume	Drilldown top email receiver by volume	traffic

```
select
   recipient,
   sum(bandwidth) as volume
from
   (
     ###(select recipient, sender, count(*) as requests, sum(coalesce(sentbyte,
        0)+coalesce(rcvdbyte, 0)) as bandwidth from $log where $filter-exclude-var and
        logid_to_int(logid) not in (4, 7, 14) and service in ('pop3', 'POP3', '110/tcp',
        'imap', 'IMAP', '143/tcp', 'imaps', 'IMAPS', '993/tcp', 'pop3s', 'POP3S',
        '995/tcp') and utmevent in ('general-email-log', 'spamfilter') group by
        recipient, sender order by requests desc)### union all ###(select `to` as
        recipient, `from` as sender, count(*) as requests, sum(coalesce(sentbyte,
        0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-emailfilter where $filter-
        exclude-var and service in ('pop3', 'POP3', '110/tcp', 'imap', 'IMAP',
        '143/tcp', 'imaps', 'IMAPS', '993/tcp', 'pop3s', 'POP3S', '995/tcp') and
        eventtype is null group by `to`, `from` order by requests desc)###) t where
        $filter-drilldown and recipient is not null group by recipient having sum
        (bandwidth)>0 order by volume desc
```

Dataset Name	Description	Log Category
drilldown-Top-Email-Receive-Sender-By-Volume	Drilldown top email receive sender by volume	traffic

```
select
   sender,
   sum(bandwidth) as volume
from
   (
      ###(select recipient, sender, count(*) as requests, sum(coalesce(sentbyte,
          0)+coalesce(rcvdbyte, 0)) as bandwidth from $log where $filter-exclude-var and
          logid_to_int(logid) not in (4, 7, 14) and service in ('pop3', 'POP3', '110/tcp',
          'imap', 'IMAP', '143/tcp', 'imaps', 'IMAPS', '993/tcp', 'pop3s', 'POP3S',
          '995/tcp') and utmevent in ('general-email-log', 'spamfilter') group by
          recipient, sender order by requests desc)### union all ###(select `to` as
          recipient, `from` as sender, count(*) as requests, sum(coalesce(sentbyte,
          0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-emailfilter where $filter-
          exclude-var and service in ('pop3', 'POP3', '110/tcp', 'imap', 'IMAP',
          '143/tcp', 'imaps', 'IMAPS', '993/tcp', 'pop3s', 'POP3S', '995/tcp') and
          eventtype is null group by `to`, `from` order by requests desc)###) t where
          $filter-drilldown and sender is not null group by sender having sum(bandwidth)>0
          order by volume desc
```

Dataset Name	Description	Log Category
drilldown-Top-Email-Recipient-By-Count	Drilldown top email receiver by count	traffic

```
select
   recipient,
   sum(requests) as requests
from
   (
      ###(select recipient, sender, count(*) as requests, sum(coalesce(sentbyte,
          0)+coalesce(rcvdbyte, 0)) as bandwidth from $log where $filter-exclude-var and
          logid_to_int(logid) not in (4, 7, 14) and service in ('pop3', 'POP3', '110/tcp',
          'imap', 'IMAP', '143/tcp', 'imaps', 'IMAPS', '993/tcp', 'pop3s', 'POP3S',
          '995/tcp') and utmevent in ('general-email-log', 'spamfilter') group by
          recipient, sender order by requests desc)### union all ###(select `to` as
          recipient, `from` as sender, count(*) as requests, sum(coalesce(sentbyte,
          0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-emailfilter where $filter-
          exclude-var and service in ('pop3', 'POP3', '110/tcp', 'imap', 'IMAP',
          '143/tcp', 'imaps', 'IMAPS', '993/tcp', 'pop3s', 'POP3S', '995/tcp') and
          eventtype is null group by `to`, `from` order by requests desc)###) t where
          $filter-drilldown and recipient is not null group by recipient order by requests
          desc
```

Dataset Name	Description	Log Category
drilldown-Top-Email-Receive-Sender-By-Count	Drilldown top email receive sender by count	traffic

```
select
   sender,
   sum(requests) as requests
from
   (
      ###(select recipient, sender, count(*) as requests, sum(coalesce(sentbyte,
          0)+coalesce(rcvdbyte, 0)) as bandwidth from $log where $filter-exclude-var and
          logid_to_int(logid) not in (4, 7, 14) and service in ('pop3', 'POP3', '110/tcp',
          'imap', 'IMAP', '143/tcp', 'imaps', 'IMAPS', '993/tcp', 'pop3s', 'POP3S',
          '995/tcp') and utmevent in ('general-email-log', 'spamfilter') group by
          recipient, sender order by requests desc)### union all ###(select `to` as
          recipient, `from` as sender, count(*) as requests, sum(coalesce(sentbyte,
          0)+coalesce(rcvdbyte, 0)) as bandwidth from $log-emailfilter where $filter-
          exclude-var and service in ('pop3', 'POP3', '110/tcp', 'imap', 'IMAP',
          '143/tcp', 'imaps', 'IMAPS', '993/tcp', 'pop3s', 'POP3S', '995/tcp') and
          eventtype is null group by `to`, `from` order by requests desc)###) t where
          $filter-drilldown and sender is not null group by sender order by requests desc
```

Dataset Name	Description	Log Category
drilldown-Top-Attack-Destination	Drilldown top attack dest	attack

```
select
   dstip,
   sum(totalnum) as totalnum
from
   ###(select srcip, dstip, count(*) as totalnum from $log where $filter-exclude-var group
       by srcip, dstip order by totalnum desc)### t where $filter-drilldown and dstip is
       not null group by dstip order by totalnum desc
```

Dataset Name	Description	Log Category
drilldown-Top-Attack-Source	Drilldown top attack source	attack

```
select
   srcip,
   sum(totalnum) as totalnum
from
   ###(select srcip, dstip, count(*) as totalnum from $log where $filter-exclude-var group
       by srcip, dstip order by totalnum desc)### t where $filter-drilldown and srcip is
       not null group by srcip order by totalnum desc
```

Dataset Name	Description	Log Category
drilldown-Top-Attack-List	Drilldown top attack list	attack

```
select
   from_itime(itime) as timestamp,
   attack,
   srcip,
   dstip
from
   ###(select itime, attack, srcip, dstip from $log where $filter-exclude-var order by
       itime desc)### t where $filter-drilldown order by timestamp desc
```

Dataset Name	Description	Log Category
drilldown-Top-Virus	UTM top virus	virus

```
select
   virus,
   max(virusid) as virusid,
   (
          case when virus like 'Riskware%' then 'Spyware' when virus like 'Adware%' then
             'Adware' else 'Virus' end
        ) as malware_type,
        sum(totalnum) as totalnum
      from
        (
          ###(select virus, 0 as virusid, count(*) as totalnum from $log-traffic where $filter
             and logid_to_int(logid) not in (4, 7, 14) and utmevent is not null and virus is
             not null group by virus, virusid order by totalnum desc)### union all ###(select
             virus, virusid, count(*) as totalnum from $log-virus where $filter and
             (eventtype is null or logver>=52) and nullifna(virus) is not null group by
             virus, virusid order by totalnum desc)###) t group by virus, malware_type order
             by totalnum desc
```

Dataset Name	Description	Log Category
drilldown-Virus-Detail	Drilldown virus detail	traffic

```
      select
        from_itime(itime) as timestamp,
        virus,
        user_src,
        dstip,
        hostname,
        recipient
      from
        (
          ###(select itime, virus, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr
             (`srcip`)) as user_src, dstip, hostname, recipient from $log-traffic where
             $filter and logid_to_int(logid) not in (4, 7, 14) and utmevent is not null and
             virus is not null order by itime desc)### union all ###(select itime, virus,
             coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, dstip, cast(' ' as char)
             as hostname, cast(' ' as char) as recipient from $log-virus where $filter and
             (eventtype is null or logver>=52) and nullifna(virus) is not null order by itime
             desc)###) t where $filter-drilldown order by timestamp desc
```

Dataset Name	Description	Log Category
user-drilldown-Top-Blocked-Web-Sites-By-Requests	User drilldown top blocked web sites by requests	webfilter

```
      select
        hostname,
        sum(requests) as requests
      from
        ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, hostname, action,
           count(*) as requests from $log where $filter and hostname is not null group by
           user_src, hostname, action order by requests desc)### t where $filter-drilldown and
           action='blocked' group by hostname order by requests desc
```

Dataset Name	Description	Log Category
user-drilldown-Top-Allowed-Web-Sites-By-Requests	User drilldown top allowed web sites by requests	webfilter

```
      select
        hostname,
        sum(requests) as requests
```

```
from
   ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, hostname, action,
       count(*) as requests from $log where $filter and hostname is not null group by
       user_src, hostname, action order by requests desc)### t where $filter-drilldown and
       action!='blocked' group by hostname order by requests desc
```

Dataset Name	Description	Log Category
user-drilldown-Top-Blocked-Web-Categories	User drilldown top blocked web categories	webfilter

```
select
   catdesc,
   sum(requests) as requests
from
   ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, catdesc, action,
       count(*) as requests from $log where $filter and catdesc is not null group by user_
       src, catdesc, action order by requests desc)### t where $filter-drilldown and
       action='blocked' group by catdesc order by requests desc
```

Dataset Name	Description	Log Category
user-drilldown-Top-Allowed-Web-Categories	User drilldown top allowed web categories	webfilter

```
select
   catdesc,
   sum(requests) as requests
from
   ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, catdesc, action,
       count(*) as requests from $log where $filter and catdesc is not null group by user_
       src, catdesc, action order by requests desc)### t where $filter-drilldown and
       action!='blocked' group by catdesc order by requests desc
```

Dataset Name	Description	Log Category
user-drilldown-Top-Attacks	User drilldown top attacks by name	attack

```
select
   attack,
   sum(attack_count) as attack_count
from
   ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, attack, (case when
       severity in ('critical', 'high') then 1 else 0 end) as high_severity, count(*) as
       attack_count from $log where $filter and nullifna(attack) is not null group by
       user_src, attack, high_severity order by attack_count desc)### t where $filter-
       drilldown group by attack order by attack_count desc
```

Dataset Name	Description	Log Category
user-drilldown-Top-Attacks-High-Severity	User drilldown top attacks high severity	attack

```
select
   attack,
   sum(attack_count) as attack_count
from
```

```
  ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, attack, (case when
     severity in ('critical', 'high') then 1 else 0 end) as high_severity, count(*) as
     attack_count from $log where $filter and nullifna(attack) is not null group by
     user_src, attack, high_severity order by attack_count desc)### t where $filter-
     drilldown and high_severity=1 group by attack order by attack_count desc
```

Dataset Name	Description	Log Category
user-drilldown-Top-Virus-By-Name	User drilldown top virus	virus

```
select
  virus,
  max(virusid) as virusid,
  sum(totalnum) as totalnum
from
  ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, virus, virusid,
     count(*) as totalnum from $log where $filter and nullifna(virus) is not null group
     by user_src, virus, virusid order by totalnum desc)### t where $filter-drilldown
     group by virus order by totalnum desc
```

Dataset Name	Description	Log Category
user-drilldown-Top-Virus-Receivers-Over-Email	User drilldown top virus receivers over email	virus

```
select
  receiver,
  sum(totalnum) as totalnum
from
  ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, `to` as receiver,
     count(*) as totalnum from $log where $filter and subtype='infected' and (service in
     ('smtp', 'SMTP', '25/tcp', '587/tcp', 'smtps', 'SMTPS', '465/tcp') or service in
     ('pop3', 'POP3', '110/tcp', 'imap', 'IMAP', '143/tcp', 'imaps', 'IMAPS', '993/tcp',
     'pop3s', 'POP3S', '995/tcp')) and nullifna(virus) is not null group by user_src,
     receiver order by totalnum desc)### t where $filter-drilldown group by receiver
     order by totalnum desc
```

Dataset Name	Description	Log Category
user-drilldown-Count-Spam-Activity-by-Hour-of-Day	User drilldown count spam activity by hour of day	emailfilter

```
select
  hourstamp,
  sum(totalnum) as totalnum
from
  ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, $hour_of_day as
     hourstamp, count(*) as totalnum from $log where $filter and `to` is not null and
     action in ('detected', 'blocked') group by user_src, hourstamp order by
     hourstamp)### t where $filter-drilldown group by hourstamp order by hourstamp
```

Dataset Name	Description	Log Category
user-drilldown-Top-Spam-Sources	User drilldown top spam sources	emailfilter

```
select
  mf_sender,
  sum(totalnum) as totalnum
```

```
from
   ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as user_src, `from` as mf_sender,
       count(*) as totalnum from $log where $filter and `from` is not null and action in
       ('detected', 'blocked') group by user_src, mf_sender order by totalnum desc)### t
       where $filter-drilldown group by mf_sender order by totalnum desc
```

Dataset Name	Description	Log Category
event-Usage-CPU	Event usage CPU	event

```
select
   hourstamp,
   cast(
      sum(cpu_usage)/ sum(num) as decimal(6, 2)
   ) as cpu_avg_usage
from
   ###(select $hour_of_day as hourstamp, sum(cpu) as cpu_usage, count(*) as num from $log
       where $filter and subtype='system' and action='perf-stats' group by hourstamp)### t
       group by hourstamp order by hourstamp
```

Dataset Name	Description	Log Category
event-Usage-Memory	Event usage memory	event

```
select
   hourstamp,
   cast(
      sum(mem_usage)/ sum(num) as decimal(6, 2)
   ) as mem_avg_usage
from
   ###(select $hour_of_day as hourstamp, sum(mem) as mem_usage, count(*) as num from $log
       where $filter and subtype='system' and action='perf-stats' group by hourstamp)### t
       group by hourstamp order by hourstamp
```

Dataset Name	Description	Log Category
event-Usage-Sessions	Event usage sessions	event

```
select
   hourstamp,
   cast(
      sum(sess_usage)/ sum(num) as decimal(10, 2)
   ) as sess_avg_usage
from
   ###(select $hour_of_day as hourstamp, sum(totalsession) as sess_usage, count(*) as num
       from $log where $filter and subtype='system' and action='perf-stats' group by
       hourstamp)### t group by hourstamp order by hourstamp
```

Dataset Name	Description	Log Category
event-Usage-CPU-Sessions	Event usage CPU sessions	event

```
select
   hourstamp,
   cast(
      sum(sess_usage)/ sum(num) as decimal(10, 2)
   ) as sess_avg_usage,
   cast(
      sum(cpu_usage)/ sum(num) as decimal(6, 2)
   ) as cpu_avg_usage
from
   ###(select $hour_of_day as hourstamp, sum(cpu) as cpu_usage, sum(totalsession) as sess_
       usage, count(*) as num from $log where $filter and subtype='system' and
       action='perf-stats' group by hourstamp)### t group by hourstamp order by hourstamp
```

Dataset Name	Description	Log Category
App-Risk-Top-Users-By-Bandwidth	Top users by bandwidth usage	traffic

```
select
   coalesce(
      nullifna(`user`),
      nullifna(`unauthuser`),
      ipstr(`srcip`)
   ) as user_src,
   srcip,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth,
   sum(
      coalesce(rcvdbyte, 0)
   ) as traffic_in,
   sum(
      coalesce(sentbyte, 0)
   ) as traffic_out
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and srcip is not null
group by
   user_src,
   srcip
having
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   )> 0
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
App-Risk-Top-User-Source-By-Sessions	Application risk top user source by session count	traffic

```
select
   srcip,
   coalesce(
      nullifna(`user`),
      nullifna(`unauthuser`),
      ipstr(`srcip`)
   ) as user_src,
   count(*) as sessions
from
```

```
      $log
   where
      $filter
      and logid_to_int(logid) not in (4, 7, 14)
      and srcip is not null
   group by
      srcip,
      user_src
   order by
      sessions desc
```

Dataset Name	Description	Log Category
App-Risk-Top-Users-By-Reputation-Scores-Bar	Application risk reputation top users by scores	traffic

```
   select
      coalesce(
         nullifna(`user`),
         nullifna(`unauthuser`),
         ipstr(`srcip`)
      ) as user_src,
      sum(crscore % 65536) as scores
   from
      $log
   where
      $filter
      and logid_to_int(logid) not in (4, 7, 14)
      and crscore is not null
   group by
      user_src
   having
      sum(crscore % 65536)> 0
   order by
      scores desc
```

Dataset Name	Description	Log Category
App-Risk-Top-Devices-By-Reputation-Scores	Application risk reputation top devices by scores	traffic

```
   select
      devtype,
      coalesce(
         nullifna(`srcname`),
         nullifna(`srcmac`),
         ipstr(`srcip`)
      ) as dev_src,
      sum(crscore % 65536) as scores
   from
      $log
   where
      $filter
      and logid_to_int(logid) not in (4, 7, 14)
      and crscore is not null
   group by
      devtype,
      dev_src
   having
      sum(crscore % 65536)> 0
   order by
      scores desc
```

Dataset Name	Description	Log Category
App-Risk-Application-Usage-By-Category-With-Pie	Application risk application usage by category	traffic

```
select
   appcat,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and nullifna(appcat) is not null
group by
   appcat
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
App-Risk-App-Usage-by-Category	Application risk application usage by category	traffic

```
select
   appcat,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and nullifna(appcat) is not null
group by
   appcat
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
Top-20-Categories-By-Bandwidth	Webfilter categories by bandwidth usage	webfilter

```
select
   catdesc,
   sum(bandwidth) as bandwidth
from
   ###(select catdesc, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from
      $log-traffic where $filter and logid_to_int(logid) not in (4, 7, 14) and
      ((logver>=52 and countweb>0) or ((logver is null) and utmevent in ('webfilter',
      'banned-word', 'web-content', 'command-block', 'script-filter'))) and catdesc is
      not null group by catdesc order by bandwidth desc)### t group by catdesc order by
      bandwidth desc
```

Dataset Name	Description	Log Category
App-Risk-Key-Applications-Crossing-The-Network	Application risk application activity	traffic

```
select
   app_group_name(app) as app_group,
   appcat,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth,
   count(*) as num_session
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and nullifna(app) is not null
group by
   app_group,
   appcat
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
App-Risk-Applications-Running-Over-HTTP	Application risk applications running over HTTP	traffic

```
select
   app_group_name(app) as app_group,
   service,
   count(*) as sessions,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and nullifna(app) is not null
   and service in (
      '80/tcp', '443/tcp', 'HTTP', 'HTTPS',
      'http', 'https'
   )
group by
   app_group,
   service
having
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
```

```
    )> 0
  order by
    bandwidth desc
```

Dataset Name	Description	Log Category
App-Risk-Top-Web-Sites-Visited-By-Network-Users-Pie-Cha	Application risk web browsing summary category	traffic

```
  select
    catdesc,
    sum(num_sess) as num_sess,
    sum(bandwidth) as bandwidth
  from
    ###(select catdesc, count(*) as num_sess, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte,
        0)) as bandwidth from $log-traffic where $filter and logid_to_int(logid) not in (4,
        7, 14) and ((logver>=52 and countweb>0) or ((logver is null) and utmevent in
        ('webfilter', 'banned-word', 'web-content', 'command-block', 'script-filter'))) and
        catdesc is not null group by catdesc order by num_sess desc)### t group by catdesc
        order by num_sess desc
```

Dataset Name	Description	Log Category
App-Risk-Top-Web-Sites-Visited-By-Network-Users	Application risk web browsing summary category	traffic

```
  select
    catdesc,
    sum(num_sess) as num_sess,
    sum(bandwidth) as bandwidth
  from
    ###(select catdesc, count(*) as num_sess, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte,
        0)) as bandwidth from $log-traffic where $filter and logid_to_int(logid) not in (4,
        7, 14) and ((logver>=52 and countweb>0) or ((logver is null) and utmevent in
        ('webfilter', 'banned-word', 'web-content', 'command-block', 'script-filter'))) and
        catdesc is not null group by catdesc order by num_sess desc)### t group by catdesc
        order by num_sess desc
```

Dataset Name	Description	Log Category
App-Risk-Web-Browsing-Hostname-Category	Application risk web browsing activity hostname category	traffic

```
  select
    domain,
    catdesc,
    sum(visits) as visits
  from
    (
      ###(select coalesce(nullifna(hostname), ipstr(`dstip`)) as domain, catdesc, count(*)
          as visits from $log-traffic where $filter and logid_to_int(logid) not in (4, 7,
          14) and utmevent in ('webfilter', 'banned-word', 'web-content', 'command-block',
          'script-filter') and catdesc is not null group by domain, catdesc order by
          visits desc)### union all ###(select coalesce(nullifna(hostname), ipstr
          (`dstip`)) as domain, catdesc, count(*) as visits from $log-webfilter where
          $filter and (eventtype is null or logver>=52) and catdesc is not null group by
          domain, catdesc order by visits desc)###) t group by domain, catdesc order by
          visits desc
```

Dataset Name	Description	Log Category
Top-Destination-Countries-By-Browsing-Time	Traffic top destination countries by browsing time	traffic

```
select
   dstcountry,
   sum(delta) as browsetime,
   sum(bandwidth) as bandwidth,
   sum(traffic_in) as traffic_in,
   sum(traffic_out) as traffic_out
from
   ###(select dstcountry, sum($browse_time) as delta, sum(coalesce(sentbyte, 0)+coalesce
       (rcvdbyte, 0)) as bandwidth, sum(coalesce(rcvdbyte, 0)) as traffic_in, sum(coalesce
       (sentbyte, 0)) as traffic_out from $log where $filter and logid_to_int(logid) not
       in (4, 7, 14) group by dstcountry having sum($browse_time)>0 order by delta
       desc)### t group by dstcountry order by browsetime desc
```

Dataset Name	Description	Log Category
Top-Destination-Countries-By-Browsing-Time-Enhanced	Traffic top destination countries by browsing time enhanced	traffic

```
select
   dstcountry,
   sum(delta) as browsetime,
   sum(bandwidth) as bandwidth,
   sum(traffic_in) as traffic_in,
   sum(traffic_out) as traffic_out
from
   ###(select dstcountry, sum($browse_time2) as delta, sum(coalesce(sentbyte, 0)+coalesce
       (rcvdbyte, 0)) as bandwidth, sum(coalesce(rcvdbyte, 0)) as traffic_in, sum(coalesce
       (sentbyte, 0)) as traffic_out from $log where $filter and logid_to_int(logid) not
       in (4, 7, 14) group by dstcountry having sum($browse_time2)>0 order by delta
       desc)### t group by dstcountry order by browsetime desc
```

Dataset Name	Description	Log Category
App-Risk-Traffic-Top-Hostnames-By-Browsing-Time	Traffic top domains by browsing time	traffic

```
select
   hostname,
   sum($browse_time) as browsetime,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth,
   sum(
      coalesce(rcvdbyte, 0)
   ) as traffic_in,
   sum(
      coalesce(sentbyte, 0)
   ) as traffic_out
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and hostname is not null
group by
   hostname
having
   sum($browse_time)> 0
order by
   browsetime desc
```

Dataset Name	Description	Log Category
App-Risk-Traffic-Top-Hostnames-By-Browsing-Time-Enhanced	Traffic top domains by browsing time enhanced	traffic

```
select
   hostname,
   sum($browse_time2) as browsetime,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth,
   sum(
      coalesce(rcvdbyte, 0)
   ) as traffic_in,
   sum(
      coalesce(sentbyte, 0)
   ) as traffic_out
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and hostname is not null
group by
   hostname
having
   sum($browse_time2)> 0
order by
   browsetime desc
```

Dataset Name	Description	Log Category
App-Risk-Top-Threat-Vectors-Crossing-The-Network	Application risk top threat vectors	attack

```
select
   severity,
   count(*) as totalnum
from
   $log
where
   $filter
group by
   severity
order by
   totalnum desc
```

Dataset Name	Description	Log Category
App-Risk-Top-Critical-Threat-Vectors-Crossing-The-Network	Application risk top critical threat vectors	attack

```
select
   attack,
   severity,
   ref,
   count(*) as totalnum
from
   $log
where
   $filter
   and severity = 'critical'
   and nullifna(attack) is not null
group by
   attack,
   severity,
   ref
order by
   totalnum desc
```

Dataset Name	Description	Log Category
App-Risk-Top-High-Threat-Vectors-Crossing-The-Network	Application risk top high threat vectors	attack

```
select
   attack,
   severity,
   ref,
   count(*) as totalnum
from
   $log
where
   $filter
   and severity = 'high'
   and nullifna(attack) is not null
group by
   attack,
   severity,
   ref
order by
   totalnum desc
```

Dataset Name	Description	Log Category
App-Risk-Top-Medium-Threat-Vectors-Crossing-The-Network	Application risk top medium threat vectors	attack

```
select
   attack,
   severity,
   ref,
   count(*) as totalnum
```

```
from
   $log
where
   $filter
   and severity = 'medium'
   and nullifna(attack) is not null
group by
   attack,
   severity,
   ref
order by
   totalnum desc
```

Dataset Name	Description	Log Category
App-Risk-Top-Low-Threat-Vectors-Crossing-The-Network	Application risk top low threat vectors	attack

```
select
   attack,
   severity,
   ref,
   count(*) as totalnum
from
   $log
where
   $filter
   and severity = 'low'
   and nullifna(attack) is not null
group by
   attack,
   severity,
   ref
order by
   totalnum desc
```

Dataset Name	Description	Log Category
App-Risk-Top-Info-Threat-Vectors-Crossing-The-Network	Application risk top info threat vectors	attack

```
select
   attack,
   severity,
   ref,
   count(*) as totalnum
from
   $log
where
   $filter
   and severity = 'info'
   and nullifna(attack) is not null
group by
   attack,
   severity,
   ref
order by
```

```
          totalnum desc
```

Dataset Name	Description	Log Category
App-Risk-Top-Virus-By-Name	UTM top virus	virus

```
select
  virus,
  max(virusid) as virusid,
  (
    case when virus like 'Riskware%' then 'Spyware' when virus like 'Adware%' then
        'Adware' else 'Virus' end
  ) as malware_type,
  sum(totalnum) as totalnum
from
  (
    ###(select virus, 0 as virusid, count(*) as totalnum from $log-traffic where $filter
        and logid_to_int(logid) not in (4, 7, 14) and utmevent is not null and virus is
        not null group by virus, virusid order by totalnum desc)### union all ###(select
        virus, virusid, count(*) as totalnum from $log-virus where $filter and
        (eventtype is null or logver>=52) and nullifna(virus) is not null group by
        virus, virusid order by totalnum desc)###) t group by virus, malware_type order
        by totalnum desc
```

Dataset Name	Description	Log Category
App-Risk-Top-Virus-Victim	UTM top virus user	traffic

```
select
  user_src,
  sum(totalnum) as totalnum
from
  (
    ###(select coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`)) as
        user_src, count(*) as totalnum from $log-traffic where $filter and logid_to_int
        (logid) not in (4, 7, 14) and utmevent is not null and virus is not null group
        by user_src order by totalnum desc)### union all ###(select coalesce(nullifna
        (`user`), ipstr(`srcip`)) as user_src, count(*) as totalnum from $log-virus
        where $filter and (eventtype is null or logver>=52) and nullifna(virus) is not
        null group by user_src order by totalnum desc)###) t group by user_src order by
        totalnum desc
```

Dataset Name	Description	Log Category
App-Risk-Data-Loss-Prevention-Type-Events	Application risk DLP UTM event	traffic

```
select
  utmsubtype,
  sum(number) as number
from
  (
    ###(select utmsubtype, count(*) as number from $log-traffic where $filter and logid_
        to_int(logid) not in (4, 7, 14) and utmevent='dlp' and utmsubtype is not null
        group by utmsubtype order by number desc)### union all ###(select subtype::text
        as utmsubtype, count(*) as number from $log-dlp where $filter and subtype is not
        null group by subtype order by number desc)###) t group by utmsubtype order by
        number desc
```

Dataset Name	Description	Log Category
App-Risk-Vulnerability-Discovered	Application risk vulnerability discovered	netscan

```
select
   vuln,
   vulnref as ref,
   vulncat,
   severity,
   count(*) as totalnum
from
   $log
where
   $filter
   and vuln is not null
group by
   vuln,
   vulnref,
   vulncat,
   severity
order by
   totalnum desc
```

Dataset Name	Description	Log Category
App-Risk-Malware-Discovered	Application risk virus discovered	traffic

```
select
   dom,
   sum(totalnum) as totalnum
from
   (
      ###(select $DAY_OF_MONTH as dom, count(*) as totalnum from $log-traffic where
          $filter and logid_to_int(logid) not in (4, 7, 14) and utmevent is not null and
          virus is not null group by dom order by totalnum desc)### union all ###(select
          $DAY_OF_MONTH as dom, count(*) as totalnum from $log-virus where $filter and
          nullifna(virus) is not null and (eventtype is null or logver>=52) group by dom
          order by totalnum desc)###) t group by dom order by totalnum desc
```

Dataset Name	Description	Log Category
App-Risk-Breakdown-Of-Risk-Applications	Application risk breakdown of risk applications	traffic

```
select
   unnest(
      string_to_array(behavior, ',')
   ) as d_behavior,
   count(*) as number
from
   $log t1
   inner join app_mdata t2 on t1.appid = t2.id
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
group by
   d_behavior
```

```
order by
   number desc
```

Dataset Name	Description	Log Category
App-Risk-Number-Of-Applications-By-Risk-Behavior	Application risk number of applications by risk behavior	traffic

```
select
   risk as d_risk,
   unnest(
      string_to_array(behavior, ',')
   ) as f_behavior,
   count(*) as number
from
   $log t1
   inner join app_mdata t2 on t1.appid = t2.id
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
group by
   risk,
   f_behavior
order by
   risk desc,
   number desc
```

Dataset Name	Description	Log Category
App-Risk-High-Risk-Application	Application risk high risk application	traffic

```
select
   risk as d_risk,
   behavior as d_behavior,
   t2.id,
   t2.name,
   t2.app_cat,
   t2.technology,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth,
   count(*) as sessions
from
   $log t1
   inner join app_mdata t2 on t1.appid = t2.id
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and behavior is not null
group by
   t2.id
order by
   risk desc,
   sessions desc
```

Dataset Name	Description	Log Category
Apprisk-Ctrl-Severe-High-Risk-Application	Severe and high risk applications	traffic

```
select
  appcat,
  count(distinct app) as total_num
from
  ###(select appcat, app from $log where $filter and app is not null and appcat is not
     null and logid_to_int(logid) not in (4, 7, 14) and apprisk in ('critical', 'high')
     group by appcat, app)### t group by appcat order by total_num desc
```

Dataset Name	Description	Log Category
Apprisk-Ctrl-Threats-Prevention	Threat Prevention	app-ctrl

```
select
  threat_name,
  count(distinct threats) as total_num
from
  (
    ###(select cast('Malware & Botnet C&C' as char(32)) as threat_name, app as threats
       from $log-app-ctrl where $filter and lower(appcat)='botnet' group by app)###
       union all ###(select cast('Malware & Botnet C&C' as char(32)) as threat_name,
       virus as threats from $log-virus where $filter and nullifna(virus) is not null
       group by virus)### union all ###(select cast('Malicious & Phishing Sites' as
       char(32)) as threat_name, hostname as threats from $log-webfilter where $filter
       and cat in (26, 61) group by hostname)### union all ###(select cast('Critical &
       High Intrusion Attacks' as char(32)) as threat_name, attack as total_num from
       $log-attack where $filter and severity in ('critical', 'high') group by
       attack)###) t group by threat_name order by total_num desc
```

Dataset Name	Description	Log Category
Apprisk-Ctrl-Application-Vulnerability	Application vulnerabilities discovered	attack

```
select
  attack,
  attackid,
  vuln_type,
  cve,
  severity_number,
  count(distinct dstip) as victims,
  count(distinct srcip) as sources,
  sum(totalnum) as totalnum
from
  ###(select attack, attackid, vuln_type, t2.cve, (case when t1.severity='critical' then
     5 when t1.severity='high' then 4 when t1.severity='medium' then 3 when
     t1.severity='low' then 2 when t1.severity='info' then 1 else 0 end) as severity_
     number, dstip, srcip, count(*) as totalnum from $log t1 left join ips_mdata t2 on
     t1.attack=t2.name where $filter and nullifna(attack) is not null and t1.severity is
     not null group by attack, attackid, vuln_type, t2.cve, t1.severity, dstip, srcip
     )### t group by attack, attackid, vuln_type, severity_number, cve order by
     severity_number desc, totalnum desc
```

Dataset Name	Description	Log Category
Apprisk-Ctrl-Breakdown-Of-High-Risk-Application	Severe and high risk applications	traffic

```
select
   appcat,
   count(distinct app) as total_num
from
   ###(select appcat, app from $log where $filter and app is not null and appcat is not
       null and logid_to_int(logid) not in (4, 7, 14) and apprisk in ('critical', 'high')
       group by appcat, app)### t group by appcat order by total_num desc
```

Dataset Name	Description	Log Category
Apprisk-Ctrl-Top-20-High-Risk-Application	Application risk high risk application	traffic

```
select
   d_risk,
   count(distinct f_user) as users,
   id,
   name,
   app_cat,
   technology,
   sum(bandwidth) as bandwidth,
   sum(sessions) as sessions
from
   ###(select risk as d_risk, coalesce(nullifna(t1.`user`), nullifna(t1.`unauthuser`),
       ipstr(t1.`srcip`)) as f_user, t2.id , t2.name, t2.app_cat, t2.technology, sum
       (coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth, count(*) as sessions
       from $log t1 inner join app_mdata t2 on t1.appid=t2.id where $filter and risk>='4'
       and logid_to_int(logid) not in (4, 7, 14) group by f_user, t2.id , t2.name, t2.app_
       cat, t2.technology, risk)### t group by id, d_risk, name, app_cat, technology order
       by d_risk desc, sessions desc
```

Dataset Name	Description	Log Category
Apprisk-Ctrl-High-Risk-Application-Behavioral	Application Behavioral Characteristics	traffic

```
select
   behavior,
   round(
      sum(total_num)* 100 / sum(
         sum(total_num)
      ) over (),
      2
   ) as percentage
from
   ###(select (case when lower(appcat)='botnet' then 'malicious' when lower
       (appcat)='remote.access' then 'tunneling' when lower(appcat) in ('storage.backup',
       'video/audio') then 'bandwidth-consuming' when lower(appcat)='p2p' then 'peer-to-
       peer' when lower(appcat)='proxy' then 'proxy' end) as behavior, count(*) as total_
       num from $log where $filter and lower(appcat) in ('botnet', 'remote.access',
       'storage.backup', 'video/audio', 'p2p', 'proxy') and logid_to_int(logid) not in (4,
       7, 14) and apprisk in ('critical', 'high') group by appcat)### t group by behavior
       order by percentage desc
```

Dataset Name	Description	Log Category
Apprisk-Ctrl-Key-Application-Crossing-The-Network	Key Application Crossing The Network	traffic

```
select
   d_risk,
   count(distinct f_user) as users,
   id,
   name,
   app_cat,
   technology,
   sum(bandwidth) as bandwidth,
   sum(sessions) as sessions
from
   ###(select risk as d_risk, coalesce(nullifna(t1.`user`), nullifna(t1.`unauthuser`),
       ipstr(t1.`srcip`)) as f_user, t2.id, t2.name, t2.app_cat, t2.technology, sum
       (coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth, count(*) as sessions
       from $log t1 inner join app_mdata t2 on t1.appid=t2.id where $filter and logid_to_
       int(logid) not in (4, 7, 14) group by f_user, t2.id, t2.name, t2.app_cat,
       t2.technology, risk)### t group by id, name, app_cat, technology, d_risk order by
       bandwidth desc
```

Dataset Name	Description	Log Category
Apprisk-Ctrl-Risk-Application-Usage-By-Category-With-Pie	Application risk application usage by category	traffic

```
select
   appcat,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and nullifna(appcat) is not null
group by
   appcat
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
Apprisk-Ctrl-Category-Breakdown-By-Bandwidth	Category breakdown of all applications, sorted by bandwidth	traffic

```
select
   appcat,
   count(distinct app) as app_num,
   count(distinct f_user) as user_num,
   sum(bandwidth) as bandwidth,
   sum(num_session) as num_session
```

```
from
   ###(select appcat, app, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr
       (`srcip`)) as f_user, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as
       bandwidth, count(*) as num_session from $log where $filter and logid_to_int(logid)
       not in (4, 7, 14) and nullifna(appcat) is not null group by appcat, app, f_user)###
       t group by appcat order by bandwidth desc
```

Dataset Name	Description	Log Category
Apprisk-Ctrl-Top-Web-Applications-by-Bandwidth	Top 25 Web Categories by Bandwidtih	traffic

```
select
   d_risk,
   id,
   name,
   technology,
   count(distinct f_user) as user_num,
   sum(bandwidth) as bandwidth,
   sum(num_session) as num_session
from
   ###(select risk as d_risk, t2.id, t2.name, t2.technology, coalesce(nullifna(t1.`user`),
       nullifna(t1.`unauthuser`), ipstr(t1.`srcip`)) as f_user, sum(coalesce(sentbyte,
       0)+coalesce(rcvdbyte, 0)) as bandwidth, count(*) as num_session from $log t1 inner
       join app_mdata t2 on t1.appid=t2.id where $filter and logid_to_int(logid) not in
       (4, 7, 14) and nullifna(app) is not null and service in ('80/tcp', '443/tcp',
       'HTTP', 'HTTPS', 'http', 'https') group by risk, t2.id, t2.name, t2.technology, f_
       user)### t group by d_risk, id, name, technology order by bandwidth desc
```

Dataset Name	Description	Log Category
Apprisk-Ctrl-Top-Web-Categories-Visited	Top 25 Web Categories Visited	traffic

```
select
   catdesc,
   count(distinct f_user) as user_num,
   sum(sessions) as sessions,
   sum(bandwidth) as bandwidth
from
   ###(select catdesc, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`))
       as f_user, count(*) as sessions, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0))
       as bandwidth from $log-traffic where $filter and catdesc is not null and logid_to_
       int(logid) not in (4, 7, 14) and ((logver>=52 and countweb>0) or ((logver is null)
       and utmevent in ('webfilter', 'banned-word', 'web-content', 'command-block',
       'script-filter'))) group by f_user, catdesc order by sessions desc)### t group by
       catdesc order by sessions desc
```

Dataset Name	Description	Log Category
Apprisk-Ctrl-Common-Virus-Botnet-Spyware	Common virus disvocered, the botnet communictions and the spyware/adware	traffic

```
select
   virus_s as virus,
   (
      case when lower(appcat)= 'botnet' then 'Botnet C&C' else (
         case when virus_s like 'Riskware%' then 'Spyware' when virus_s like 'Adware%'
             then 'Adware' else 'Virus' end
      ) end
   ) as malware_type,
   appid,
   app,
   count(distinct dstip) as victims,
   count(distinct srcip) as source,
   sum(total_num) as total_num
from
   (
      ###(select app as virus_s, appcat, appid, app, dstip, srcip, count(*) as total_num
          from $log-traffic where $filter and logid_to_int(logid) not in (4, 7, 14) and
          lower(appcat)='botnet' group by virus_s, appcat, appid, dstip, srcip, app order
          by total_num desc)### union all ###(select unnest(string_to_array(virus, ','))
          as virus_s, appcat, appid, app, dstip, srcip, count(*) as total_num from $log-
          traffic where $filter and logid_to_int(logid) not in (4, 7, 14) and virus is not
          null group by virus_s, appcat, appid, dstip, srcip, app order by total_num
          desc)###) t group by virus, appid, app, malware_type order by total_num desc
```

Dataset Name	Description	Log Category
Apprisk-Ctrl-Zero-Day-Detected-On-Network	Zero-day malware detected on the network	traffic

```
       select
          virus_s,
          appid,
          app,
          count(distinct dstip) as victims,
          count(distinct srcip) as source,
          sum(total_num) as total_num
       from
          ###(select unnest(string_to_array(virus, ',')) as virus_s, appid, app, dstip, srcip,
              count(*) as total_num from $log where $filter and logid_to_int(logid) not in (4, 7,
              14) and virus like '%PossibleThreat.SB%' group by virus_s, dstip, srcip, appid, app
              )### t where virus_s like '%PossibleThreat.SB%' group by virus_s, appid, app order
              by total_num desc
```

Dataset Name	Description	Log Category
Apprisk-Ctrl-Files-Analyzed-By-FortiCloud-Sandbox	Files analyzed by FortiCloud Sandbox	virus

```
       select
          $DAY_OF_MONTH as dom,
          count(*) as total_num
       from
          $log
       where
          $filter
          and nullifna(filename) is not null
          and logid_to_int(logid)= 9233
       group by
          dom
       order by
          dom
```

Dataset Name	Description	Log Category
Apprisk-Ctrl-Malicious-Files-Detected-By-FortiCloud-Sandbox	Files detected by FortiCloud Sandbox	virus

```
select
   filename,
   analyticscksum,
   count(distinct dstip) as victims,
   count(distinct srcip) as source
from
   ###(select filename, analyticscksum, dstip, srcip from $log where $filter and filename
       is not null and logid_to_int(logid)=9233 and analyticscksum is not null group by
       filename, analyticscksum, srcip, dstip)### t group by filename, analyticscksum
       order by victims desc, source desc
```

Dataset Name	Description	Log Category
Apprisk-Ctrl-File-Transferred-By-Application	File transferred by applications on the network	app-ctrl

```
select
   appid,
   app,
   filename,
   cloudaction,
   max(filesize) as filesize
from
   $log
where
   $filter
   and filesize is not null
   and clouduser is not null
   and filename is not null
group by
   cloudaction,
   appid,
   app,
   filename
order by
   filesize desc
```

Dataset Name	Description	Log Category
appctrl-Top-Blocked-SCCP-Callers	Appctrl top blocked SCCP callers	app-ctrl

```
select
   srcname as caller,
   count(*) as totalnum
from
   $log
where
   $filter
   and lower(appcat)= 'voip'
   and app = 'sccp'
   and action = 'block'
   and srcname is not null
```

```
        group by
           caller
        order by
           totalnum desc
```

Dataset Name	Description	Log Category
appctrl-Top-Blocked-SIP-Callers	Appctrl top blocked SIP callers	app-ctrl

```
        select
           srcname as caller,
           count(*) as totalnum
        from
           $log
        where
           $filter
           and srcname is not null
           and lower(appcat)= 'voip'
           and app = 'sip'
           and action = 'block'
        group by
           caller
        order by
           totalnum desc
```

Dataset Name	Description	Log Category
security-Top20-High-Risk-Application-In-Use	High risk application in use	traffic

```
        select
           d_risk,
           count(distinct f_user) as users,
           name,
           app_cat,
           technology,
           sum(bandwidth) as bandwidth,
           sum(sessions) as sessions
        from
           ###(select risk as d_risk, coalesce(nullifna(t1.`user`), nullifna(t1.`unauthuser`),
               ipstr(t1.`srcip`)) as f_user, t2.name, t2.app_cat, t2.technology, sum(coalesce
               (sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth, count(*) as sessions from $log
               t1 inner join app_mdata t2 on t1.appid=t2.id where $filter and risk>='4' and logid_
               to_int(logid) not in (4, 7, 14) group by f_user, t2.name, t2.app_cat,
               t2.technology, risk)### t group by d_risk, name, app_cat, technology order by d_
               risk desc, sessions desc
```

Dataset Name	Description	Log Category
security-High-Risk-Application-By-Category	High risk application by category	traffic

```
        select
           app_cat,
           count(distinct app) as total_num
        from
```

```
   ###(select app_cat, app from $log t1 inner join app_mdata t2 on t1.appid=t2.id where
       $filter and risk>='4' and logid_to_int(logid) not in (4, 7, 14) group by app_cat,
       app)### t group by app_cat order by total_num desc
```

Dataset Name	Description	Log Category
security-Top10-Application-Categories-By-Bandwidth	Application risk application usage by category	traffic

```
select
   appcat,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and nullifna(appcat) is not null
group by
   appcat
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
Security-Category-Breakdown-By-Bandwidth	Category breakdown of all applications, sorted by bandwidth	traffic

```
select
   appcat,
   count(distinct app) as app_num,
   count(distinct f_user) as user_num,
   sum(bandwidth) as bandwidth,
   sum(num_session) as num_session
from
   ###(select appcat, app, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr
       (`srcip`)) as f_user, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as
       bandwidth, count(*) as num_session from $log where $filter and logid_to_int(logid)
       not in (4, 7, 14) and nullifna(appcat) is not null group by appcat, app, f_user)###
       t group by appcat order by bandwidth desc
```

Dataset Name	Description	Log Category
security-Top25-Web-Applications-By-Bandwidth	Top Web Applications by Bandwidtih	traffic

```
select
   d_risk,
   name,
   app_cat,
   technology,
   count(distinct f_user) as users,
   sum(bandwidth) as bandwidth,
   sum(num_session) as sessions
from
```

```
   ###(select risk as d_risk, t2.app_cat, t2.name, t2.technology, coalesce(nullifna
       (t1.`user`), nullifna(t1.`unauthuser`), ipstr(t1.`srcip`)) as f_user, sum(coalesce
       (sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth, count(*) as num_session from
       $log t1 inner join app_mdata t2 on t1.appid=t2.id where $filter and logid_to_int
       (logid) not in (4, 7, 14) and nullifna(app) is not null and service in ('80/tcp',
       '443/tcp', 'HTTP', 'HTTPS', 'http', 'https') group by risk, t2.app_cat, t2.name,
       t2.technology, f_user)### t group by d_risk, name, app_cat, technology order by
       bandwidth desc
```

Dataset Name	Description	Log Category
Security-Top25-Web-Categories-Visited	Top 25 Web Categories Visited	traffic

```
select
   catdesc,
   count(distinct f_user) as user_num,
   sum(sessions) as sessions,
   sum(bandwidth) as bandwidth
from
   ###(select catdesc, coalesce(nullifna(`user`), nullifna(`unauthuser`), ipstr(`srcip`))
       as f_user, count(*) as sessions, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0))
       as bandwidth from $log-traffic where $filter and catdesc is not null and logid_to_
       int(logid) not in (4, 7, 14) and ((logver>=52 and countweb>0) or ((logver is null)
       and utmevent in ('webfilter', 'banned-word', 'web-content', 'command-block',
       'script-filter'))) group by f_user, catdesc order by sessions desc)### t group by
       catdesc order by sessions desc
```

Dataset Name	Description	Log Category
security-Top25-Malware-Virus-Botnet-Spyware	Malware: viruses, Bots, Spyware/Adware	traffic

```
select
   virus_s as virus,
   (
      case when lower(appcat)= 'botnet' then 'Botnet C&C' else (
         case when virus_s like 'Riskware%' then 'Spyware' when virus_s like 'Adware%'
             then 'Adware' else 'Virus' end
      ) end
   ) as malware_type,
   count(distinct dstip) as victims,
   count(distinct srcip) as source,
   sum(total_num) as total_num
from
   (
      ###(select app as virus_s, appcat, dstip, srcip, count(*) as total_num from $log-
          traffic where $filter and logid_to_int(logid) not in (4, 7, 14) and lower
          (appcat)='botnet' group by virus_s, appcat, dstip, srcip order by total_num
          desc)### union all ###(select unnest(string_to_array(virus, ',')) as virus_s,
          appcat, dstip, srcip, count(*) as total_num from $log-traffic where $filter and
          logid_to_int(logid) not in (4, 7, 14) and virus is not null group by virus_s,
          appcat, dstip, srcip order by total_num desc)###) t group by virus, malware_type
          order by total_num desc
```

Dataset Name	Description	Log Category
security-Top10-Malware-Virus-Spyware	Malware: viruses, Spyware/Adware	virus

```
select
   virus,
   max(virusid) as virusid,
   malware_type,
   count(distinct dstip) as victims,
   count(distinct srcip) as source,
   sum(total_num) as total_num
from
   ###(select virus, virusid, srcip, dstip, (case when virus like 'Riskware%' then
       'Spyware' when virus like 'Adware%' then 'Adware' else 'Virus' end) as malware_
       type, count(*) as total_num from $log where $filter and nullifna(virus) is not null
       group by virus, virusid, srcip, dstip order by total_num desc)### t group by virus,
       malware_type order by total_num desc
```

Dataset Name	Description	Log Category
security-Top10-Malware-Botnet	Malware: Botnet	appctrl

```
select
   app,
   appid,
   malware_type,
   count(distinct dstip) as victims,
   count(distinct srcip) as source,
   sum(total_num) as total_num
from
   ###(select app, appid, cast('Botnet C&C' as char(32)) as malware_type, srcip, dstip,
       count(*) as total_num from $log where $filter and lower(appcat)='botnet' and
       nullifna(app) is not null group by app, appid, malware_type, srcip, dstip order by
       total_num desc)### t group by app, appid, malware_type order by total_num desc
```

Dataset Name	Description	Log Category
security-Application-Vulnerability	Application vulnerabilities discovered	attack

```
select
   attack,
   attackid,
   vuln_type,
   cve,
   severity_number,
   count(distinct dstip) as victims,
   count(distinct srcip) as sources,
   sum(totalnum) as totalnum
from
   ###(select attack, attackid, vuln_type, t2.cve, (case when t1.severity='critical' then
       5 when t1.severity='high' then 4 when t1.severity='medium' then 3 when
       t1.severity='low' then 2 when t1.severity='info' then 1 else 0 end) as severity_
       number, dstip, srcip, count(*) as totalnum from $log t1 left join ips_mdata t2 on
       t1.attack=t2.name where $filter and nullifna(attack) is not null and t1.severity is
       not null group by attack, attackid, vuln_type, t2.cve, t1.severity, dstip, srcip
```

```
        )### t group by attack, attackid, vuln_type, severity_number, cve order by
        severity_number desc, totalnum desc
```

Dataset Name	Description	Log Category
security-Files-Analyzed-By-FortiCloud-Sandbox	Files analyzed by FortiCloud Sandbox	virus

```
select
   $day_of_week as dow,
   count(*) as total_num
from
   $log
where
   $filter
   and nullifna(filename) is not null
   and logid_to_int(logid)= 9233
group by
   dow
order by
   dow
```

Dataset Name	Description	Log Category
Security-Zero-Day-Detected-On-Network	Zero-day malware detected on the network	traffic

```
select
   virus_s,
   app,
   count(distinct dstip) as victims,
   count(distinct srcip) as source,
   sum(total_num) as total_num
from
   ###(select unnest(string_to_array(virus, ',')) as virus_s, app, dstip, srcip, count(*)
      as total_num from $log where $filter and logid_to_int(logid) not in (4, 7, 14) and
      virus like '%PossibleThreat.SB%' group by virus_s, dstip, srcip, app)### t group by
      virus_s, app order by total_num desc
```

Dataset Name	Description	Log Category
security-Data-Loss-Incidents-By-Severity	Data loss incidents summary by severity	dlp

```
select
   initcap(severity :: text) as s_severity,
   count(*) as total_num
from
   $log
where
   $filter
   and severity is not null
group by
   s_severity
order by
   total_num desc
```

Dataset Name	Description	Log Category
security-Data-Loss-Files-By-Service	Data Lass Files By Service	dlp

```
select
   filename,
   (
      case direction when 'incoming' then 'Download' when 'outgoing' then 'Upload' end
   ) as action,
   max(filesize) as filesize,
   service
from
   $log
where
   $filter
   and filesize is not null
group by
   filename,
   direction,
   service
order by
   filesize desc
```

Dataset Name	Description	Log Category
security-Endpoint-Security-Events-Summary	Endpoint Security Events summary	fct-traffic

```
select
   (
      case utmevent when 'antivirus' then 'Malware incidents' when 'webfilter' then
          'Malicious/phishing websites' when 'appfirewall' then 'Risk applications' when
          'dlp' then 'Data loss incidents' when 'netscan' then 'Vulnerability detected'
          else 'Others' end
   ) as events,
   count(*) as total_num
from
   $log
where
   $filter
   and utmevent is not null
group by
   events
order by
   total_num desc
```

Dataset Name	Description	Log Category
security-Top-Endpoing-Running-High-Risk-Application	Endpoints Running High Risk Application	fct-traffic

```
select
   coalesce(
      nullifna(`user`),
      ipstr(`srcip`),
      'Unknown'
   ) as f_user,
   coalesce(
      nullifna(hostname),
      'Unknown'
   ) as host_name,
   threat as app,
   t2.app_cat as appcat,
   risk as d_risk
from
   $log t1
   inner join app_mdata t2 on t1.threat = t2.name
where
   $filter
   and utmevent = 'appfirewall'
   and risk >= '4'
group by
   f_user,
   host_name,
   t1.threat,
   t2.app_cat,
   t2.risk
order by
   risk desc
```

Dataset Name	Description	Log Category
security-Top-Endpoints-Infected-With-Malware	Endpoints Infected With Malware	fct-event

```
select
   coalesce(
      nullifna(`user`),
      ipstr(`deviceip`),
      'Unknown'
   ) as f_user,
   coalesce(
      nullifna(hostname),
      'Unknown'
   ) as host_name,
   virus,
   file
from
   $log
where
   $filter
   and clientfeature = 'av'
   and virus is not null
group by
   f_user,
   host_name,
   virus,
   file
```

Dataset Name	Description	Log Category
security-Top-Endpoints-With-Web-Violateions	Endpoints With Web Violations	fct-traffic

```
select
   f_user,
   host_name,
   remotename,
   sum(total_num) as total_num
from
   ###(select coalesce(nullifna(`user`), ipstr(`srcip`)) as f_user, coalesce(nullifna
       (hostname), 'Unknown') as host_name, remotename, count(*) as total_num from $log
       where $filter and utmevent='webfilter' and remotename is not null and
       utmaction='blocked' group by f_user, host_name, remotename order by total_num
       desc)### t group by f_user, host_name, remotename order by total_num desc
```

Dataset Name	Description	Log Category
security-Top-Endpoints-With-Data-Loss-Incidents	Endpoints With Data Loss Incidents	fct-event

```
select
   f_user,
   host_name,
   msg,
   sum(total_num) as total_num
from
   ###(select coalesce(nullifna(`user`), ipstr(`deviceip`), 'Unknown') as f_user, coalesce
       (nullifna(hostname), 'Unknown') as host_name, msg, count(*) as total_num from $log
       where $filter and clientfeature='dlp' group by f_user, host_name, msg order by
       total_num desc)### t group by f_user, host_name, msg order by total_num desc
```

Dataset Name	Description	Log Category
content-Count-Total-SCCP-Call-Registrations-by-Hour-of-Day	Content count total SCCP call registrations by hour of day	content

```
select
   $hour_of_day as hourstamp,
   count(*) as totalnum
from
   $log
where
   $filter
   and proto = 'sccp'
   and kind = 'register'
group by
   hourstamp
order by
   hourstamp
```

Dataset Name	Description	Log Category
content-Count-Total-SCCP-Calls-Duration-by-Hour-of-Day	Content count total SCCP calls duration by hour of day	content

```
select
   $hour_of_day as hourstamp,
   sum(duration) as sccp_usage
from
   $log
where
```

```
      $filter
      and proto = 'sccp'
      and kind = 'call-info'
      and status = 'end'
   group by
      hourstamp
   order by
      hourstamp
```

Dataset Name	Description	Log Category
content-Count-Total-SCCP-Calls-per-Status	Content count total SCCP calls per status	content

```
   select
      status,
      count(*) as totalnum
   from
      $log
   where
      $filter
      and proto = 'sccp'
      and kind = 'call-info'
   group by
      status
   order by
      totalnum desc
```

Dataset Name	Description	Log Category
content-Count-Total-SIP-Call-Registrations-by-Hour-of-Day	Content count total SIP call registrations by hour of day	content

```
   select
      $hour_of_day as hourstamp,
      count(*) as totalnum
   from
      $log
   where
      $filter
      and proto = 'sip'
      and kind = 'register'
   group by
      hourstamp
   order by
      hourstamp
```

Dataset Name	Description	Log Category
content-Count-Total-SIP-Calls-per-Status	Content count total SIP calls per status	content

```
   select
      status,
      count(*) as totalnum
   from
      $log
```

```
where
   $filter
   and proto = 'sip'
   and kind = 'call'
group by
   status
order by
   totalnum desc
```

Dataset Name	Description	Log Category
content-Dist-Total-SIP-Calls-by-Duration	Content dist total SIP calls by duration	content

```
select
   (
      case when duration < 60 then 'LESS_ONE_MIN' when duration < 600 then 'LESS_TEN_MIN'
          when duration < 3600 then 'LESS_ONE_HOUR' when duration >= 3600 then 'MORE_ONE_
          HOUR' else 'unknown' end
   ) as f_duration,
   count(*) as totalnum
from
   $log
where
   $filter
   and proto = 'sip'
   and kind = 'call'
   and status = 'end'
group by
   f_duration
order by
   totalnum desc
```

Dataset Name	Description	Log Category
Botnet-Activity-By-Sources	Botnet activity by sources	traffic

```
select
   app,
   coalesce(
      nullifna(`user`),
      nullifna(`unauthuser`),
      ipstr(`srcip`)
   ) as user_src,
   count(*) as events
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and appcat = 'Botnet'
   and nullifna(app) is not null
group by
   app,
   user_src
order by
   events desc
```

Dataset Name	Description	Log Category
Botnet-Infected-Hosts	Botnet infected hosts	traffic

```
select
   coalesce(
      nullifna(`user`),
      nullifna(`unauthuser`),
      ipstr(`srcip`)
   ) as user_src,
   devtype,
   coalesce(srcname, srcmac) as host_mac,
   count(*) as events
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and appcat = 'Botnet'
group by
   user_src,
   devtype,
   host_mac
order by
   events desc
```

Dataset Name	Description	Log Category
Detected-Botnet	Detected botnet	traffic

```
select
   app,
   count(*) as events
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and appcat = 'Botnet'
   and nullifna(app) is not null
group by
   app
order by
   events desc
```

Dataset Name	Description	Log Category
Botnet-Sources	Botnet sources	traffic

```
select
   dstip,
   root_domain(hostname) as domain,
   count(*) as events
from
   $log
where
```

```
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and appcat = 'Botnet'
   and dstip is not null
group by
   dstip,
   domain
order by
   events desc
```

Dataset Name	Description	Log Category
Botnet-Victims	Botnet victims	traffic

```
select
   coalesce(
      nullifna(`user`),
      nullifna(`unauthuser`),
      ipstr(`srcip`)
   ) as user_src,
   count(*) as events
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and appcat = 'Botnet'
   and srcip is not null
group by
   user_src
order by
   events desc
```

Dataset Name	Description	Log Category
Botnet-Timeline	Botnet timeline	traffic

```
select
   $flex_timescale(timestamp) as hodex,
   sum(events) as events
from
   ###(select $flex_timestamp as timestamp, count(*) as events from $log where $filter and
       logid_to_int(logid) not in (4, 7, 14) and appcat='Botnet' group by timestamp order
       by timestamp desc)### t group by hodex order by hodex
```

Dataset Name	Description	Log Category
Application-Session-History	Application session history	traffic

```
select
   $flex_timescale(timestamp) as hodex,
   sum(counter) as counter
from
   ###(select $flex_timestamp as timestamp, count(*) as counter from $log where $filter
       and logid_to_int(logid) not in (4, 7, 14) group by timestamp order by timestamp
       desc)### t group by hodex order by hodex
```

Dataset Name	Description	Log Category
Application-Usage-List	Detailed application usage	traffic

```
select
   appid,
   app,
   appcat,
   (
      case when (
         utmaction in ('block', 'blocked')
         or action = 'deny'
      ) then 'Blocked' else 'Allowed' end
   ) as custaction,
   sum(
      coalesce(sentbyte, 0)+ coalesce(rcvdbyte, 0)
   ) as bandwidth,
   count(*) as num_session
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and nullifna(app) is not null
   and policyid != 0
group by
   appid,
   app,
   appcat,
   custaction
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
PCI-DSS-Compliance-Summary	PCI DSS Compliance Summary	event

```
select
   status,
   num_reason as requirements,
   cast(
      num_reason * 100.0 /(
         sum(num_reason) over()
      ) as decimal(18, 2)
   ) as percent
from
   (
      select
         (
            case when fail_count > 0 then 'Non-Compliant' else 'Compliant' end
         ) as status,
         count(distinct reason) as num_reason
      from
         (
            select
               ftnt_pci_id,
               (
                  sum(fail_count) over (partition by ftnt_pci_id)
               ) as fail_count,
               reason
            from
               ###(select ftnt_pci_id, (case when result='fail' then 1 else 0 end) as fail_
                   count, reason from $log t1 inner join pci_dss_mdata t2 on
                   t1.reason=t2.ftnt_id where $filter and subtype='compliance-check' group
                   by ftnt_pci_id, result, reason)### t) t group by status) t order by
                   status desc
```

Dataset Name	Description	Log Category
PCI-DSS-Non-Compliant-Requirements-By-Severity	PCI DSS Non-Compliant Requirements by Severity	event

```
with query as (
          select
             *
          from
             (
                select
                   ftnt_pci_id,
                   severity,
                   (
                      sum(fail_count) over (partition by ftnt_pci_id)
                   ) as fail_count,
                   reason
                from
                   ###(select ftnt_pci_id, severity, (case when result='fail' then 1 else 0 end)
                       as fail_count, reason from $log t1 inner join pci_dss_mdata t2 on
                       t1.reason=t2.ftnt_id where $filter and subtype='compliance-check' group by
                       ftnt_pci_id, severity, result, reason)### t) t where fail_count>0) select
                       t.severity, count(distinct t.reason) as requirements from (select distinct
                       on (1) reason, severity from query order by reason, (case severity when
                       'high' then 4 when 'critical' then 3 when 'medium' then 2 when 'low' then 1
                       else 0 end) desc) t group by t.severity order by requirements desc
```

Dataset Name	Description	Log Category
PCI-DSS-Compliant-Requirements-By-Severity	PCI DSS Compliant Requirements by Severity	event

```
with query as (
          select
             *
          from
             (
                select
                   ftnt_pci_id,
                   severity,
                   (
                      sum(fail_count) over (partition by ftnt_pci_id)
                   ) as fail_count,
                   reason
                from
###(select ftnt_pci_id, severity, (case when result='fail' then 1 else 0 end)
    as fail_count, reason from $log t1 inner join pci_dss_mdata t2 on
    t1.reason=t2.ftnt_id where $filter and subtype='compliance-check' group by
    ftnt_pci_id, severity, result, reason)### t) t where fail_count=0) select
    t.severity, count(distinct t.reason) as requirements from (select distinct
    on (1) reason, severity from query order by reason, (case severity when
    'high' then 4 when 'critical' then 3 when 'medium' then 2 when 'low' then 1
    else 0 end) desc) t group by t.severity order by requirements desc
```

Dataset Name	Description	Log Category
PCI-DSS-Fortinet-Security-Best-Practice-Summary	PCI DSS Fortinet Security Best Practice Summary	event

```
select
   status,
   num_reason as practices,
   cast(
      num_reason * 100.0 /(
         sum(num_reason) over()
      ) as decimal(18, 2)
   ) as percent
from
   (
      select
         (
            case when result = 'fail' then 'Failed' else 'Passed' end
         ) as status,
         count(distinct reason) as num_reason
      from
         ###(select result, reason from $log where $filter and subtype='compliance-check'
             and result in ('fail','pass') group by result, reason)### t group by status)
             t order by status
```

Dataset Name	Description	Log Category
PCI-DSS-Failed-Fortinet-Security-Best-Practices-By-Severity	PCI DSS Failed Fortinet Security Best Practices by Severity	event

```
select
   status,
   num_reason as practices,
   cast(
      num_reason * 100.0 /(
         sum(num_reason) over()
      ) as decimal(18, 2)
   ) as percent
from
   (
      select
         initcap(status) as status,
         count(distinct reason) as num_reason
      from
         ###(select status, reason from $log where $filter and subtype='compliance-check'
             and result='fail' group by status, reason)### t group by status) t order by
             status
```

Dataset Name	Description	Log Category
PCI-DSS-Passed-Fortinet-Security-Best-Practices-By-Severity	PCI DSS Passed Fortinet Security Best Practices by Severity	event

```
select
   status,
   num_reason as practices,
   cast(
      num_reason * 100.0 /(
         sum(num_reason) over()
      ) as decimal(18, 2)
   ) as percent
from
   (
      select
         initcap(status) as status,
         count(distinct reason) as num_reason
      from
         ###(select status, reason from $log where $filter and subtype='compliance-check'
            and result='pass' group by status, reason)### t group by status) t order by
            status
```

Dataset Name	Description	Log Category
PCI-DSS-Requirements-Compliance-Details	PCI DSS Requirements Compliance Details	event

```
select
   ftnt_pci_id,
   left(
      string_agg(distinct ftnt_id, ','),
      120
   ) as practice,
   (
      case when sum(fail_count)> 0 then 'Non-Compliant' else 'Compliant' end
   ) as compliance,
   pci_requirement
from
   ###(select ftnt_pci_id, ftnt_id, (case when result='fail' then 1 else 0 end) as fail_
      count, pci_requirement from $log t1 inner join pci_dss_mdata t2 on
      t1.reason=t2.ftnt_id where $filter and subtype='compliance-check' group by ftnt_
      pci_id, ftnt_id, result, pci_requirement)### t group by ftnt_pci_id, pci_
      requirement order by ftnt_pci_id
```

Dataset Name	Description	Log Category
PCI-DSS-Fortinet-Security-Best-Practice-Details	PCI DSS Fortinet Security Best Practice Details	event

```
select
   reason as ftnt_id,
   msg,
   initcap(status) as status,
   module
from
   $log
```

```
where
   $filter
   and subtype = 'compliance-check'
group by
   reason,
   status,
   module,
   msg
order by
   ftnt_id
```

Dataset Name	Description	Log Category
DLP-Email-Activity-Details	Email DLP Violations Summary	dlp

```
select
   from_itime(itime) as timestamp,
   `from` as sender,
   `to` as receiver,
   regexp_replace(filename, '.*/', '') as filename,
   filesize,
   profile,
   action,
   direction
from
   $log
where
   $filter
   and (
      service in (
         'smtp', 'SMTP', '25/tcp', '587/tcp',
         'smtps', 'SMTPS', '465/tcp'
      )
      or service in (
         'pop3', 'POP3', '110/tcp', 'imap',
         'IMAP', '143/tcp', 'imaps', 'IMAPS',
         '993/tcp', 'pop3s', 'POP3S', '995/tcp'
      )
   )
order by
   timestamp desc
```

Dataset Name	Description	Log Category
Email-DLP-Chart	Email DLP Activity Summary	dlp

```
select
   profile,
   count(*) as total_num
from
   $log
where
   $filter
   and (
      service in (
         'smtp', 'SMTP', '25/tcp', '587/tcp',
         'smtps', 'SMTPS', '465/tcp'
```

```
            )
            or service in (
               'pop3', 'POP3', '110/tcp', 'imap',
               'IMAP', '143/tcp', 'imaps', 'IMAPS',
               '993/tcp', 'pop3s', 'POP3S', '995/tcp'
            )
         )
      group by
         profile
      order by
         total_num desc
```

Dataset Name	Description	Log Category
DLP-Web-Activity-Details	Web DLP Violations Summary	dlp

```
      select
         from_itime(itime) as timestamp,
         srcip,
         dstip,
         hostname,
         profile,
         filename,
         filesize,
         action,
         direction
      from
         $log
      where
         $filter
         and lower(service) in ('http', 'https')
      order by
         timestamp desc
```

Dataset Name	Description	Log Category
Web-DLP-Chart	Web DLP Activity Summary	dlp

```
      select
         profile,
         count(*) as total_num
      from
         $log
      where
         $filter
         and lower(service) in ('http', 'https')
      group by
         profile
      order by
         total_num desc
```

Dataset Name	Description	Log Category
DLP-FTP-Activity-Details	Web DLP Violations Summary	dlp

```
      select
         from_itime(itime) as timestamp,
         srcip,
         dstip,
         filename,
         profile,
         filesize,
         action,
         direction
      from
         $log
      where
         $filter
         and lower(service) in ('ftp', 'ftps')
      order by
         timestamp desc
```

Dataset Name	Description	Log Category
FTP-DLP-Chart	FTP DLP Activity Summary	dlp

```
select
   profile,
   count(*) as total_num
from
   $log
where
   $filter
   and lower(service) in ('ftp', 'ftps')
group by
   profile
order by
   total_num desc
```

Dataset Name	Description	Log Category
top-users-by-browsetime	Top Users by website browsetime	traffic

```
select
   coalesce(
      nullifna(`user`),
      ipstr(`srcip`)
   ) as user_src,
   coalesce(
      nullifna(hostname),
      ipstr(`dstip`)
   ) as domain,
   sum($browse_time) as browsetime
from
   $log
where
   $filter
group by
   user_src,
   domain
having
   sum($browse_time)> 0
order by
   browsetime desc
```

Dataset Name	Description	Log Category
wifi-usage-by-hour-authenticated	Wifi Usage by Hour - Authenticated	event

```
select
   hod,
   count(distinct stamac) as totalnum
from
   ###(select $HOUR_OF_DAY as hod, stamac from $log where $filter and subtype='wireless'
       and action='client-authentication' group by hod, stamac)### t group by hod order by
       hod
```

Dataset Name	Description	Log Category
wifi-usage-authenticated-timeline	Wifi Usage Timeline - Authenticated	event

```
select
   $flex_timescale(timestamp) as hodex,
   count(distinct stamac) as totalnum
from
   ###(select $flex_timestamp as timestamp, stamac from $log where $filter and
       subtype='wireless' and action='client-authentication' group by timestamp, stamac
       order by timestamp desc)### t group by hodex order by hodex
```

Dataset Name	Description	Log Category
app-top-user-by-bandwidth	Top 10 Applications Bandwidth by User Drilldown	traffic

```
select
   app,
   coalesce(
      nullifna(`user`),
      nullifna(`unauthuser`),
      ipstr(`srcip`)
   ) as user_src,
   sum(
      coalesce(`sentbyte`, 0)+ coalesce(`rcvdbyte`, 0)
   ) as bandwidth
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and nullifna(app) is not null
group by
   app,
   user_src
order by
   bandwidth desc
```

Dataset Name	Description	Log Category
app-top-user-by-session	Top 10 Application Sessions by User Drilldown	traffic

```
select
   app,
   coalesce(
      nullifna(`user`),
      nullifna(`unauthuser`),
      ipstr(`srcip`)
   ) as user_src,
   count(*) as sessions
from
   $log
where
   $filter
   and logid_to_int(logid) not in (4, 7, 14)
   and nullifna(app) is not null
group by
   app,
   user_src
order by
   sessions desc
```

Dataset Name	Description	Log Category
traffic-Interface-Bandwidth-Usage	Interface Bandwidth Usage	traffic

with qry as (

```
   select
      dom as dom_s,
      devid as devid_s,
      vd as vd_s,
      srcintf,
      dstintf,
      total_sent,
      total_rcvd
   from
      ###(select $DAY_OF_MONTH as dom, devid, vd, srcintf, dstintf, sum(coalesce(sentbyte,
          0)) as total_sent, sum(coalesce(rcvdbyte, 0)) as total_rcvd, sum(coalesce
          (sentbyte, 0)+coalesce(rcvdbyte, 0)) as total from $log where $filter and logid_
          to_int(logid) not in (4, 7, 14) and nullifna(srcintf) is not null and nullifna
          (dstintf) is not null group by dom, devid, vd, srcintf, dstintf having sum
          (coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0))>0 order by total desc)### t)
          select dom, unnest(array['download', 'upload']) as type, unnest(array[sum
          (download), sum(upload)]) as bandwidth from (select coalesce(t1.dom_s, t2.dom_s)
          as dom, coalesce(t1.devid_s, t2.devid_s) as devid, coalesce(t1.vd_s, t2.vd_s) as
          vd, coalesce(t1.srcintf, t2.dstintf) as intf, sum(coalesce(t1.total_sent,
          0)+coalesce(t2.total_rcvd, 0)) as download, sum(coalesce(t2.total_sent,
          0)+coalesce(t1.total_rcvd, 0)) as upload from qry t1 full join qry t2 on t1.dom_
          s=t2.dom_s and t1.srcintf=t2.dstintf group by dom, devid, vd, intf) t where
          $filter-drilldown group by dom order by dom
```

Dataset Name	Description	Log Category
360-degree-security-Application-Visiblity-and-Control-Summary	Application Visibolity and Control Summary	app-ctrl

```
select
   appcat,
   count(distinct app) as total_num
from
   ###(select appcat, app from $log where $filter and app is not null and appcat is not
       null and logid_to_int(logid) not in (4, 7, 14) group by appcat, app)### t group by
       appcat order by total_num desc
```

Dataset Name	Description	Log Category
360-degree-security-Threats-Detection-and-Prevention-Summary	Threat Prevention	app-ctrl

```
select
   threat_name,
   count(distinct threats) as total_num
from
   (
      ###(select cast('Malware & Botnet C&C' as char(32)) as threat_name, app as threats
          from $log-app-ctrl where $filter and lower(appcat)='botnet' group by app)###
          union all ###(select cast('Malware & Botnet C&C' as char(32)) as threat_name,
          virus as threats from $log-virus where $filter and nullifna(virus) is not null
          group by virus)### union all ###(select cast('Malicious & Phishing Sites' as
          char(32)) as threat_name, hostname as threats from $log-webfilter where $filter
          and cat in (26, 61) group by hostname)### union all ###(select cast('Critical &
          High Intrusion Attacks' as char(32)) as threat_name, attack as total_num from
          $log-attack where $filter and severity in ('critical', 'high') group by
          attack)###) t group by threat_name order by total_num desc
```

Dataset Name	Description	Log Category
360-degree-security-Data-Exfiltration-Detection-and-Prevention-Summary	Data Exfiltration Summary	dlp

```
select
   data_loss,
   count(*) as total_num
from
   (
      select
         (
            case when severity = 'critical' then 'Critical Data Exfiltration' else (
               case when coalesce(
                  nullifna(`user`),
                  ipstr(`srcip`)
               ) is not null then 'User Associated Data Loss' else NULL end
            ) end
         ) as data_loss
      from
         $log
      where
         $filter
   ) t
where
   data_loss is not null
group by
   data_loss
order by
   total_num desc
```

Dataset Name	Description	Log Category
360-degree-security-Endpoint-Protection-Summary	Endpoint Protection	fct-traffic

```
select
   blocked_event,
   count(*) as total_num
from
   (
      select
         (
            case utmevent when 'antivirus' then 'Malware Deteced and Blocked' when
                'appfirewall' then 'Risk Application Blocked' when 'webfilter' then (
               case when coalesce(
                  nullifna(`user`),
                  ipstr(`srcip`)
               ) is not null then 'Web Sites Violation Blocked' else 'Non User Initiated
                   Web Visits' end
            ) else NULL end
         ) as blocked_event
      from
         $log
      where
         $filter
         and utmaction in ('blocked', 'quarantined')
   ) t
where
   blocked_event is not null
group by
   blocked_event
order by
   total_num desc
```

Macro Reference List

The following table lists the available predefined macros that can be used in a report layout to display the log data as text (XML format) dynamically.

Macro Name	Description	Dataset Used	Log Category
Application Category with Highest Session Count	Application category with the highest session count	App-Sessions-By-Category	Traffic
Application with Highest Bandwidth	Application with the highest bandwidth usage	Top-App-By-Bandwidth	Traffic
Application with Highest Session Count	Applications with the highest session count	Top-App-By-Sessions	Traffic
Attack with Highest Session Count	Attack with highest session count	Utm-Top-Attack-Source	Attack
Botnet with Highest Session Count	Botnet with the highest session count	Detected-Botnet	Traffic
Destination with Highest Bandwidth	Destination with the highest bandwidth usage	Top-Destinations-By-Bandwidth	Traffic
Destination with Highest Session Count	Destination with the highest session count	Top-Destinations-By-Sessions	Traffic
Highest Bandwidth Consumed (Application) Category	Highest bandwidth consumed by application category	App-Risk-App-Usage-By-Category	Traffic
Highest Bandwidth Consumed (Application)	Highest bandwidth consumed by application	Top-App-By-Bandwidth	Traffic
Highest Bandwidth Consumed (Destination)	Highest bandwidth consumed by destination	Top-Destinations-By-Bandwidth	Traffic
Highest Bandwidth Consumed (P2P Application)	Highest bandwidth consumed by P2P application	Top-P2P-App-By-Bandwidth	Traffic
Highest Bandwidth Consumed (Source)	Highest bandwidth consumed by source	Top-Users-By-Bandwidth	Traffic
Highest Bandwidth Consumed ()Web Category)	Highest bandwidth consumed by website category	Top-Web-Category-by-Bandwidth	Web Filter
Highest Bandwidth Consumed (Website)	Highest bandwidth consumed by website	Top-Web-Sites-by-Bandwidth	Web Filter

Macro Name	Description	Dataset Used	Log Category
Highest Risk Application with Highest Bandwidth	Highest risk application with the highest bandwidth usage	High-Risk-Application-By-Bandwidth	Traffic
Highest Risk Application with Highest Session Count	Highest risk application with the highest session count	High-Risk-Application-By-Sessions	Traffic
Highest Session Count by Application Category	Highest session count by application category	App-Sessions-By-Category	Traffic
Highest Session Count by Application	Highest session count by application	Top-App-By-Sessions	Traffic
Highest Session Count by Attack	Highest session count by attack	Utm-Top-Attack-Source	Attack
Highest Session Count by Botnet	Highest session count by botnet	Detected-Botnet	Traffic
Highest Session Count by Destination	Highest session count by destination	Top-Destinations-By-Sessions	Traffic
Highest Session Count by Highest Severity Attack	Highest session count by highest severity attack	Threat-Attacks-By-Severity	Attack
Highest Session Count by P2P Application	Highest session count by P2P application	Top-P2P-App-By-Sessions	Traffic
Highest Session Count by Source	Highest session count by source	Top-User-Source-By-Sessions	Traffic
Highest Session Count by Virus	Highest session count by virus	Utm-Top-Virus	Traffic
Highest Session Count by Web Category	Highest session count by website category	Top-Web-Category-by-Sessions	Web Filter
Highest Session Count by Website	Highest session count by website	Top-Web-Sites-by-Sessions	Web Filter
Highest Severity Attack with Highest Session Count	Highest severity attack with the highest session count	Threat-Attacks-By-Severity	Attack
P2P Application with Highest Bandwidth	P2P applications with the highest bandwidth usage	Top-P2P-App-By-Bandwidth	Traffic
P2P Application with Highest Session Count	P2P applications with the highest session count	Top-P2P-App-By-Sessions	Traffic

FORTINET®

High Performance Network Security

Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.