Qosmos DeepFlow®: Subscriber Analytics Use Case

Qosmos DeepFlow configured for Subscriber Analytics is a passive probe that analyses IP traffic in real-time. It identifies protocols and applications behind each flow and reveals events generated by the transactions to feed value-added analytics solutions. Analytics information is delivered for IP-based services, per user and per transaction. Qosmos DeepFlow Subscriber Analytics is based on the DeepFlow Application Component Suite (ACS).

**Key Facts**

- Layer 2-7 IP flow analysis in real-time
- Supports 3G (GTP) networks and LTE (SCTP) networks
- Passive probe, designed for analytics without impact on network operations
- No reporting, no storage: designed to feed third party big data systems
- Up to 20 Gbps per probe, stackable
- Powered by Qosmos ixEngine®, the market leading DPI and metadata engine
- Data aggregation per minute, per user, per application
- Fully customizable data queries
- Data exports using standard formats like CSV and IPFIX
- Available as appliance, software or virtual machine

Qosmos DeepFlow probes identify applications behind each IP session and deliver detailed flow metadata in real-time. In a typical integration, this data is forwarded to a third party big data analytics systems that delivers reports and dashboards about subscribers mobile data consumption. Layer 7 flow analysis is carried out in real time, at core networks speed up to 20 Gbps per box. Virtualizing or stacking several DeepFlow probes enables monitoring of hundreds of Gbps and millions of subscribers.

**High-resolution visibility into traffic flows**

- Identification of protocols and applications associated with every network flow
- Layer 7 traffic analysis using a combination of Deep Packet Inspection (DPI), statistical and behavioral analysis
- Detection of encrypted and obfuscated applications like P2P or Skype
- Identification of applications embedded in Facebook
- Identification of services like VoIP, chat, file transfer within complex applications like Skype or Instant Messaging
- Delivery of application metadata like HTTP URL, Facebook user profile, relation details in Twitter (following, followed by, etc.)
- Up to 50 metadata available for each protocol, for a total of thousands metadata available for application aware analytics and subscriber profiling
- Analysis of wireline networks, 3G and LTE mobile networks
- Correlation of data and signaling information (inheritance)

**Pre-defined probe configurations**

DeepFlow for Subscriber Analytics comes with 4 pre-defined configurations that enable instant deployment. Users can select what configuration to activate depending on their requirements.

- ISA: Analysis of web browsing and media streaming (VoIP and video)
- MSA: Analysis of web browsing and search engine with data and signaling correlation
- CMSA: Analysis of 3G mobile network with data and signaling correlation

Users can also create their own custom analytics probes based on DeepFlow ACS, with the assistance of Qosmos Professional Services. For more information, see the DeepFlow ACS datasheet.

**Maximum Accuracy**

- 2000+ protocol and application plugins providing comprehensive service coverage
- On-demand addition of new plug-ins for specific regional needs
- 100% reliability (does not use TCP or UDP ports classification)
Continuous protocol plug-in updates
Operates even in the case of complex network behavior like HTTP pipelining or HTTP proxy
Automatic de-capsulation of all tunnels (GTP, L2TP, GRE, HTTP tunnels, Teredo etc.)
Advanced mechanisms to ensure high quality of data delivered

**Performance and scalability even under heavy metadata load**
- Real-time analysis of flows up to x 20Gbps
- Range of probes from 1U to 4U
- Flexible probe provisioning enables users to tune the ratio between maximum packet rate and the details of information extracted
- Scalable throughputs: one DeepFlow probe can monitor up to 20 Gbps. Several DeepFlows can be stacked for further scalability
- Designed to maintain performance when flow metadata extraction is activated.

**Actionable data and easy integration**
- Passive probe (port mirroring or tap). No overhead on the network
- Streaming of data in standard format (e.g. CSV over FTP)
- Multiple variants of local and remote communications are supported

**Features**
- Classification of network flows using stateful Deep Packet Inspection
- Statistical and behavioral analysis for encrypted and obfuscated flows
- 2,000+ protocol and application plug-ins typically provides near 100% classification rate in typical traffic environments
- Identification of services like VoIP, video call, chat, file sharing, desktop sharing, posting, etc. within Skype, Facebook, Twitter, and all the most popular applications
- Automatic detection of all URLs
- Real-time extraction of metadata and content from traffic flows
- Over 50 metadata available for many applications (e.g. 83 for HTTP) for a total set of thousands metadata
- Example of application metadata: call duration with Tango (video calls), gender of user in Facebook
- Real-time, event-based analytics
- Examples of events tracked: user is clicking on the “like” button in Facebook, user is sending a tweet
- Correlation at flow, session, application, service and user levels
- GTP-C / GTP-U correlation
- De-capsulation of tunnels (GRE, L2TP etc.)
- Operates on fragmented, duplicated, de-sequenced packets
- Operates both on bidirectional and unidirectional traffic
- User-defined protocol and application plugins for any type of applications including URLs, and also more complex binary applications requiring advanced heuristics.

**Deployment**
- Plug & play probe to feed an analytics system
- Passive probe connected in port mirroring/TAP mode with no impact on traffic
- For wireline and mobile networks
- Supports 3G networks (GTP) and LTE networks (SCTP, all possible links)
- Delivers the result of traffic analysis in the form of CSV data records
- The structure of data records is fully customizable
- Advanced data filtering capabilities
- Once defined, the structure of the data provided by the probe will always remain the same, irrespective of the types of devices present in the network infrastructure
- On-demand addition of plug-ins for specific/regional applications and protocols
- Scalable features: start small with basic flow classification and upgrade to more advanced features such as metadata extraction per application and per user

**Range of DeepFlow probes**

<table>
<thead>
<tr>
<th>Feature</th>
<th>DF 100 Series</th>
<th>DF 1000 Series</th>
<th>DF 10 000 Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>1</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Network interface</td>
<td>Multiple 1 GE or 10 GE interfaces</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max throughput</td>
<td>4 Gb/s</td>
<td>10 Gb/s</td>
<td>20 Gb/s</td>
</tr>
</tbody>
</table>

**Robustness**
- Red Hat guarantee and Linux best practices. Red Hat security and identity management
- Qosmos role-based management
- Built-in protection against attacks (e.g. DDOS)

**Export capabilities and formats**
- Real-time streaming of Session Detail Records (SDR) in CSV format
- Streaming of SDRs over FTP or HTTP
- Flow buffering to preserve data integrity
- Optional anonymization and encryption of exports

**Hardware or software probe**
DeepFlow is available in multiple configurations:
- DeepFlow hardware probe based on COTS Servers and RHEL
- DeepFlow software only
- Virtualization ready: DeepFlow can be virtualized for deployment in cloud architectures

Qosmos is the leader in embedded Deep Packet Inspection and L7 Network Intelligence for use in physical, virtualized and SDN architectures. The company’s software development kit and probes are embedded by vendors into their products sold to telcos and enterprises. www.qosmos.com