iAcuity
Telco

IP Logger

DataSheet

The exponential growth of smartphone adoption has driven up demand for mobile data. Through these devices, mobile subscribers now consume more mobile data in more places. This huge demand for content/information by smart communication devices like phones, tablets, etc. has led to a constant increase in IP traffic. GSMA foresees that, by 2018, the revenue generated by data traffic will exceed that generated by voice traffic by US$12 billion worldwide. Mobile operators must make a number of important changes in order to successfully adapt to new data driven demand

Regulatory authorities and lawful agencies also need to adapt to this data driven transformation so that they can intercept crucial information. The rise of data now encourages lawful agencies to seek ways of acquiring required details from operators in a quick and automated manner. To safeguard public interests against threats of cybercrime, regulators are recommending providers to granulate intercepted information by location, time zone, APN for a prescribed period of time of a year or more.

This is where the challenges of the operators are galore as IP data records (IPDRs) may range from IP-Packets to System Logs from different hardware, and hence result in huge amount of data as compared to the traditional telephone CDR's. The challenge lies in effective storage of this huge amount of IP log data in a powerful and secure data warehouse and extracting the required data at near real time when needed by a lawful or investigating authority.

iAcuity Telco Solutions IP Logger Benefits:

- Carrier Grade Reliability and Proven Performance
- Investigation teams and vigilance authorities can view complete information of users
- High performance indexing leading to Flexibility in search logic, ensuring faster search results
- High performance indexing leading to Flexibility in search logic, ensuring faster search results
- Provides capability to filter, analyze and generate reports based on log messages
- Optimum storage for huge data traffic supporting millions of PDP sessions
- Manage long-term Log data storage in database file system for over a year
- Highly customized Software Application based solution

IP-Logger Features

IAcuity Telco Solutions' IP-Log Management System provides easy & fast Implementation with hassle free configuration. IP-Logger can be deployed on any OS and can support multiple databases. Quick search results and a user-friendly interface allow users to collect and analyze information such as Private IP, Gateway IP, Public IP, and MSISDN with end–to-end IP details.

The key features of IAcuity Telco Solutions' IP Log Management solution are:

1. Fully automated solution that collects, stores, correlates and analyses large volume of network and security event logs for auditing and reporting purposes. Log information is immediately available for near real-time security investigations and incident response.

2. Collects IP data (IPDR) and subscriber data from any telecommunications network.

3. IP-Logger collects information from various CGNAT devices. The CGNAT device pushes the information to IP-Logger's Collector Engine. The Collector engine is designed to support a high volume TPS (100K to 300K) on the basis of different protocols on a single CPU server.

4. IP-Logger NAT Log Parsing & Processing Engine enriches and converts NAT Logs to the required format and storing it, thus enabling run time correlation to initiate faster queries on the data. It parsesand processes different types of file formats like Net flow. Binary, CSV, Zip, ASN.1 and supports the processing of EDRs as well as firewall logs with millions of PDPs that can be stored for a year.

5. The system can be used to administer warrants and search requests for multiple network operators and service providers. User management can be configured to securely segregate between networks, users, and authorities and thus supports various business models.

6. The system ensures maximum security for the retained data through authentication & encryption.

7. The system provides capability to filter, analyze and generate reports based on log messages.

8. Automates request processing and delivers data to authorized agencies by fax, e-mail, or secure IP interfaces.

File Collection

This module is responsible for collecting log files from SGSN, GGSN and from Router based on configuration. The module supports protocols such as ftp, sftp, and web services etc. for collecting files. This module also validates for duplicate files. The names of the files collected will be stored in the data base for a specific period so that file audit can be done. Users can configure various sources from where the application can retrieve data using ftp/sft etc. Any renaming of files also needs to be configured in this module. This module also provides option to view the collection status from different sources.

Transformation, Conversion and Correlation

The files collected will be optionally converted to text format based on configuration. This is based on modular adapter architecture where in different types of adapters can be installed and configured for each source. Based on the configuration IP-Logger will apply correlation on the contents of the files and store combined records in the database for specific time for query purpose. The user can query the data using different query parameters like on specific time frame and other filters like MSISDN, IMSI, IMEI, session id etc. provided that information exists in the files collected.

User Management

User management module is responsible for configuring users and assigning them with various roles.
It has following functionality:

• Access to web application based on user name and password

• User creation, deletion modification and password management

• Assigning access to various modules based on roles

• User Audit management where in all user edit actions and logins are captured and can be viewed by admin user

Query, Reports and Alerts

Users with the right privileges can query the data based on the following criteria:

• End time

• MSISDN

• IMSI

• IMEI

• URL

• IP Address

The results will be stored in a file and can be downloaded by the user. The result will be stored for preconfigured number of days. IP-Logger's built in reporting functionality allows users to export analysis and information into sharable reports. Users can select which reports to create and the required format. In addition, users can also configure alerts allowing them to be notified of certain activities in near real time.

India

360 Kalyandas Udyog Bhavan,
Prabhadevi,
Mumbai - 400025.

Email: info@iacuitytelco.com   www.iacuitytelco.com