VoIPLogic

Fraud Monitor: Protection and Mitigation using SDReporter

Fraud Monitor: Protection and Mitigation using SDReporter

Overview

VoIP Logic's Hosted VoIP Platform collects data on every call that flows through your partition, but how do you use that data to protect and optimize performance? VoIP Logic's Fraud Monitor for Protection and Mitigation: SDReporter* - is designed to specifically use the data that the Hosted VoIP Platform collects related to your customers and your services, and to allow you to create detailed fraud assessment alarms, mitigation configurations, reports and analysis, based on parameters that you define and control.

*The SDReporter is a product offering of VoIP Logic partner TransNexus

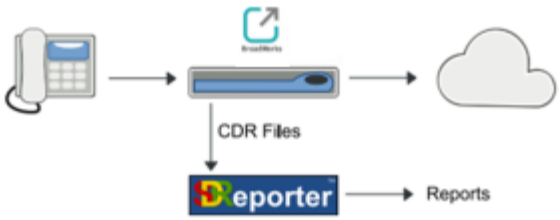

Figure 1: SDReporter Data Flow example

Fraud Detection

With the increase of toll fraud attacks in the industry, it is now more important than ever for Service Providers to implement an efficient telecom fraud management solution to protect your revenue, networks and customers. VoIP Logic's Fraud Monitor solution can significantly reduce problems of traffic pumping fraud, PBX hacking, revenue sharing fraud, along with Blind Transfer and Call Forwarding fraud – all activities that result in revenue loss through unauthorized access. Fraud Monitoring includes smart monitoring features that work with the parameters that Service Providers can set and control. With reports generated for each five-minute traffic interval, VoIP Logic's Service Provider Partners (SPPs) can determine when an unusual spike in traffic has occurred that falls outside the norm, based on the settings you have indicated in the profiles that you have established for your customers. The system can then provide a transmittable alarm and can, in certain instances, dynamically blacklist a Trunk or a User, ensuring that fraud losses are kept to an absolute minimum, without interrupting legitimate calls. Fraud Monitor fraud detection features also include analysis tools including: User definable blacklists, fraud scoring, call diversion, and call blocking.

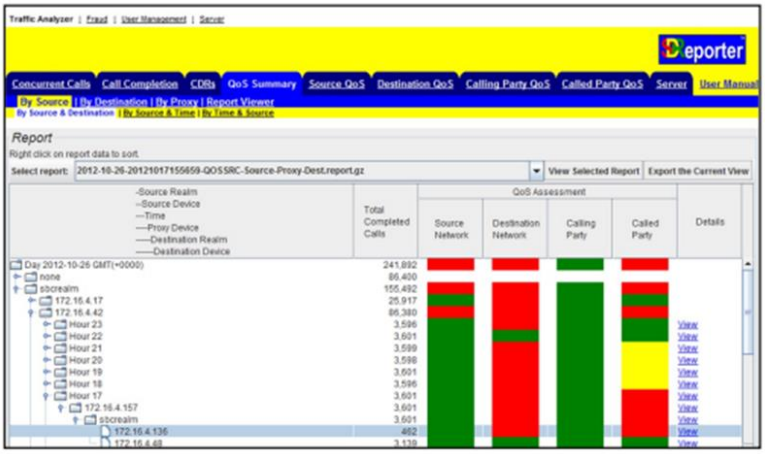

Figure 2: SDReporter Screen Reports example

SDReporter works by managing call termination services through a system that allows SPPs to set and maintain fraud thresholds based on the usage patterns of their own users. Calls from the source network (calling party) are routed to one or more possible SPP designated destination networks.

Inserting SDReporter at this point in the call flow allows the SPP to control the potential for fraud across their VoIP Logic Platform partition(s) by monitoring the call transit across the Platform Infrastructure and sending SNMP Traps and Alarms for traffic that deviates from the standards customized by the Service Provider. This allows the SPP to mitigate any fraudulent or abnormal traffic in near-real time.

Partitioning Deployment Methodology

In order to provide the maximum in flexibility and control, each of VoIP Logic's SPPs will be deployed on their own SDReporter instance. Root level control of the software technology allows SPPs to do the following:

- Analyze the Call volumes and patterns on your Platform partitions and Enterprises to determine the effective instance sizing.
- Define Dial codes and Dialing plans that fit your customers specifically.
- Specify Email or SNMP secure alarm transmission methods exclusively for your NOC team.
- View and assess only your CDR Reporting and Analysis needs.

The SDReporter Platform is fully scalable. It can be easily upgraded to support SPP growth by working with VoIP Logic TAC Support .

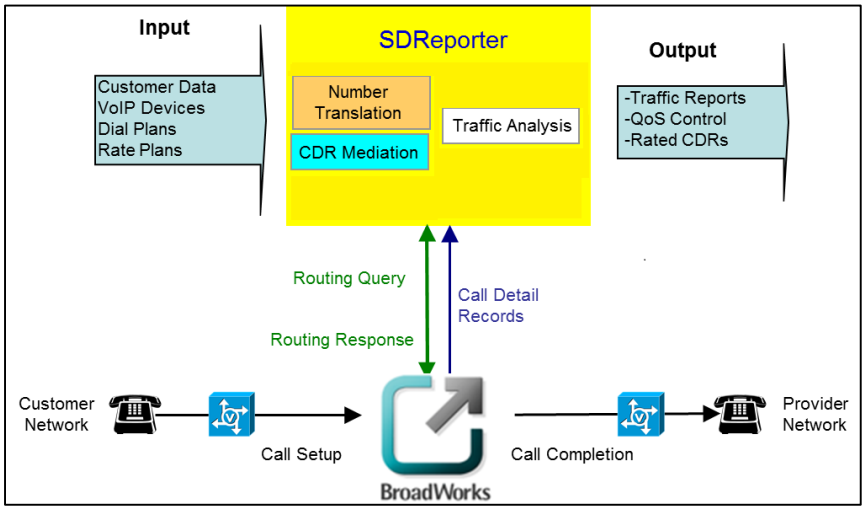

Figure 3: SDReporter Process Flow example

Additional documents related to the implementation of VoIP Logic SDReporter Platform can be found at The VoIP Logic SPP Portal on the TransNexus SDReporter Configuration, Implementation and Administration Guides Page. Please contact your VoIP Logic Account Manager for information on pricing, specifications and implementation process.