FRAFOS Monitor

Strong security for VoIP networks and critical infrastructure

The FRAFOS Monitor provides administrators with an aggregated view of user activity based on usage data collected from various sources such as the FRAFOS SBC, FRAFOS traffic probe as well as VoIP components of other vendors such as Oracle or Cisco. This highly interactive, near real-time view can be used for the analysis of both short-term and long-term use patterns, troubleshooting, auditing server policies, and identifying misconducting users.

Key Features

Daily overview

A daily overview of conducted calls, service interruptions, service quality. Such reports can be received over mail or retrieved from the customers personal area in the web interface.

Alarms

Inform administrators about certain events such as the failure of a component or a fraud attempt. Alarms can be communicated in the form of email, message or using REST API to external SIEM platforms.

Availability monitoring

Detect and report on the availability of the customer's VoIP solutions as well as SIP trunks.

Detailed Security reviews

Provide the customers with comprehensive monitoring and security service tools based on machine learning and big data analysis.

Advanced Fraud Detection policies

On the one side the solution will offer intelligent policies to indicate events such as service disruption or well-known fraud patterns, e.g., mid night calls to suspicious numbers. On the other side, customers can customize additional alarms to indicate malicious behavior such as non-authorized calls.

FRAFOS Monitor at a Glance

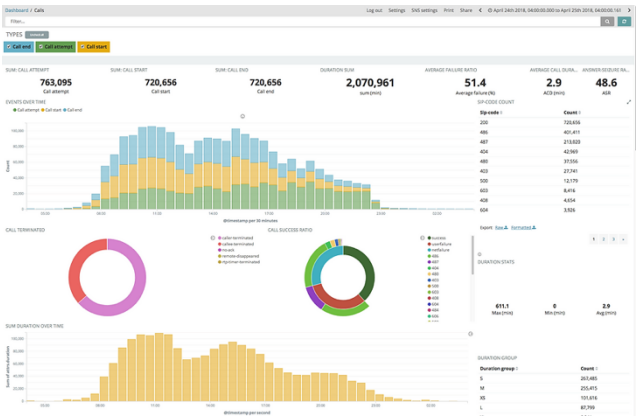
- Fraud detection
- DoS identification
- Call Statistics
- Alarms
- Daily Reports
- Availability monitoring
- Call flow analysis
- Call log history
- Data feed from FRAFOS SBC and different other sources

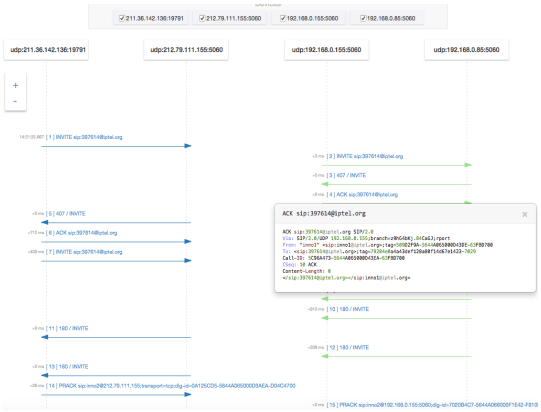
Denial of Service and fraud detection

Using specialized VoIP analysis algorithms and machine learning tools, the FRAFOS Monitor provides fraud and DoS detection and generate alarms when malicious behaviour is identified.

Focused View

The FRAFOS Monitor offers the administrator several dashboards that provide summaries for different aspects of their VoIP service. Administrators inspect these statistics and can narrow down the observed events by specifying event filters. For example, they can limit the events to a window of time that displays only calls that were rejected, filter out events with the IP address of the most intensive senders, and eventually inspect the sender's call-flows in detail.





Comprehensive Data Overview

The FRAFOS Monitor summaries different aspects of the collected data in separate dashboards:

- **Overview Dashboard** displays all events that have been collected by the Monitor.
- **Call Dashboard:** Information about the call duration, number of call attempts, successful call establishments, and terminations and important KPIs like ASR or MOS statistics.
- **Registrations Dashboard** displays events related to registrations and the geographic location of the users.
- **Diagnostics Dashboard** provides administrators with a troubleshooting vehicle that gathers detailed information about the monitored SIP traffic.
- **Security Dashboard** analyzes situations when a FRAFOS SBC instance identifies offending traffic and chooses to reject it by shaping or entirely dropping it. Which packets to ignore and how the traffic limits are set are defined in the FRAFOS SBC rules. A related "Blacklisting Dashboard" identifies often-repeating security events so that repeating offenders may be found.

Centralized Monitoring

The FRAFOS Monitor collects data from multiple SBCs, probes and VoIP components and displays them from one central web application.

VoIP Analysis

The Session Initiation Protocol (SIP) has become increasingly complex with many options and different call flows. With years of experience, the FRAFOS team has developed SIP analysis and processing mechanisms that enable detailed investigation of SIP issues as well as detecting interoperability issues and signaling problems.

Call Sequence Diagrams

Display a "ladder chart" with message details to show the call flow and root causes of call failures.

Network Connectivity Details

The FRAFOS Monitor displays the topology and visualizes statistics for monitored calls. This helps to discover situations such as a destination Call Agent failing abnormally often to complete calls, or SIP compatiblity issues on a link from one CA to another.

Directed cyclic relationship graphs show the flow between call agents. The stronger the lines, the more traffic the events represent on this route.

Flexible deployment

The FRAFOS Monitor is delivered as a container that can be deployed on a virtualization environment, off-the-shelve hardware, or a cloud solution.

FRAFOS GmbH

Member of the Frequentis Group
Askanischer Platz 4
10963 Berlin, Germany

www.frafos.com