A solution which is faster, smarter and more flexible. PALLADION Fraud Detection & Prevention uses a technology difficult to scam - automated behavioural analysis. Built upon PALLADION’s real-time network intelligence it can detect and stop toll fraud immediately.

Fraud Detection & Prevention makes use of the fact that all fraud attacks have similar symptoms, namely the deviation of current calls from the corresponding user’s usual behavioural pattern.

Fraud Detection & Prevention monitors all calls on a VoIP network and over time it learns the behavioural pattern of individual users as well as user groups such as enterprise customers, trunks etc.

If the call patterns do not match the pattern of the corresponding user or user group then the Fraud Detection & Prevention system generates incidents that can trigger actions to detect fraud.
Scoring

Any deviation from the user’s behavioural pattern may suggest that the network is facing a fraud attack. However, relying on just one metric can cause false alerts to be raised.

The Fraud Detection & Prevention system uses rules to calculate values from multiple metrics, enabling a more accurate assessment of the situation. It combines these values into a score for each user and for each user group.

Fraud Detection & Prevention comes with a set of pre-defined rules available for immediate use. Plus the ability to extend with customized sets of rules.

Metrics

Fraud Detection & Prevention comes with a library of metrics to measure the basic attributes of users’ and user groups’ behaviour.

Example Metrics
- Minutes spoken
- Parallel Calls
- Unusual call destinations
- Unusual source IP

Rules

The rules are used to determine what call behaviour is considered fraudulent and at what severity (with a rating system). A rule can make use of any number of metrics.

Example Metrics

Score

The score is the accumulation of the values and is used to determine whether or not a user has surpassed a threshold.

Threshold

Surpassing a defined threshold causes an alarm to be raised. Thresholds can be either static values or dependent on a counter or KPI. Most powerful are fully automatic thresholds depending on previous behavioural patterns.