This brochure explains how Adaptiv can detect fraud. Fraud detection is but one of the many uses for Adaptiv.

Fraud

Fraud usually refers to the unauthorised use of telecommunication facilities, however, it can also extend to include the exploitation of weak spots in rate plans.

With the advent of VoIP, fraud is a growing issue that can be achieved from anywhere in the world using the Internet.

The VoIP-based PBX is a common access point for fraud, as it works via the Internet to manage voice calls. Due to the ease with which the VoIP PBX is setup, it's used not only by companies, but also internally by Telco's and their resellers to route calls.

So what happens when a company's PBX is breached? Typically, a Telco invoices a company either monthly or quarterly, by which time a large amount of fraudulent activity could have occurred. If company support staff has failed to notice fraud early on, the last chance is with the company accountant.

As a Telco, you could gain respect from customers if unusual activity was detected early on. On the other hand, fraudulent activity could increase your revenue. But what happens when a small company is hacked and creates a $5,000 bill and refuses to pay? Well, you would have to take the hit, as legal action is costly and you would risk losing customers. If a $500,000 bill is fraudulently created the company could be forced into bankruptcy and you'd still have to pay your suppliers.

Adaptiv can be used to detect these types of fraudulent activity.

Fraud Detection

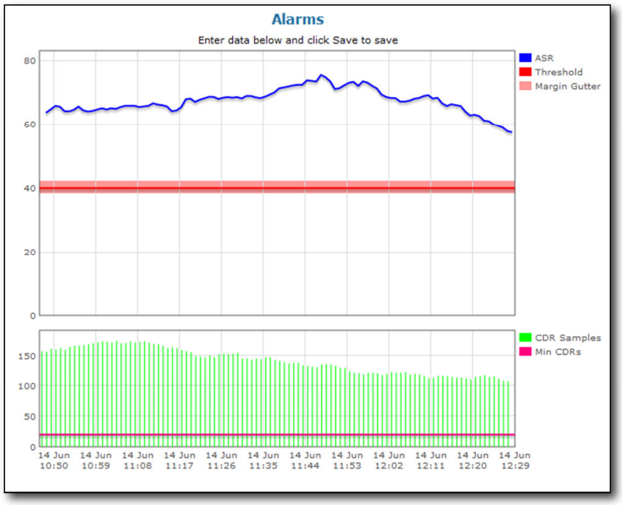
Adaptiv Fraud Detection is based on an alarm system that detects unusual traffic conditions.

Adaptiv can be set up to send a warning message to key support personal so they can further investigate any irregularities, or can be set up to automatically shut down any unusual traffic conditions.

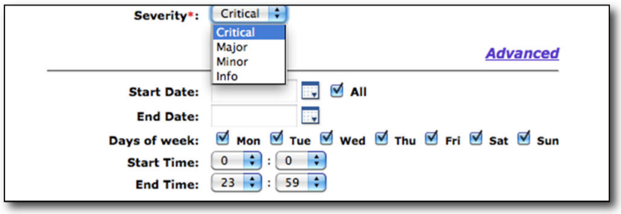
Adaptiv monitors completed calls 'near real time' in order to collect enough data to make intelligent assessments. This means alarms can go off in minutes, as opposed to hours, days, weeks or months.

In order to set up an alarm, you need to know what your traffic typically looks like.

Adaptiv has a feature called an Alarm Graph, which shows trends in traffic, and allows you to set up alarms using appropriate values.



You can fine-tune the alarm to suit specific needs, providing an in depth visualisation of what's been set up. When an alarm is triggered, you will be emailed the Alarm Graph.

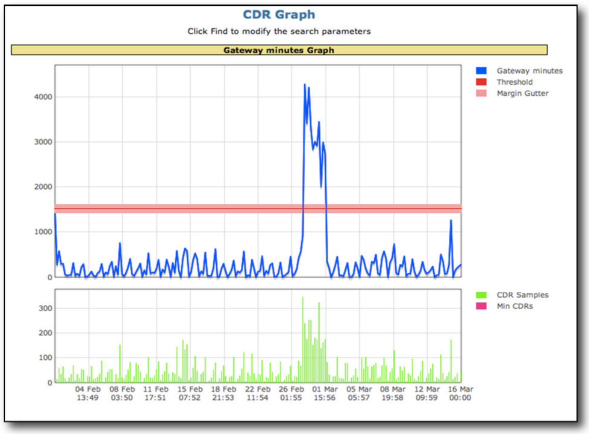


Severity*: Critical

Start Date: ☑ All
End Date:
Days of week: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun
Start Time: 0 : 0
End Time: 23 : 59

Varying traffic patterns are taken into account using Time Periods, which establish alarms for very specific times of the year, week or even each day.

CDR Count is a simple yet effective method for detecting fraud. For example, if overseas calls never exceed a certain number of calls per interval, the alarm threshold can be set to warn you if this number is exceeded.



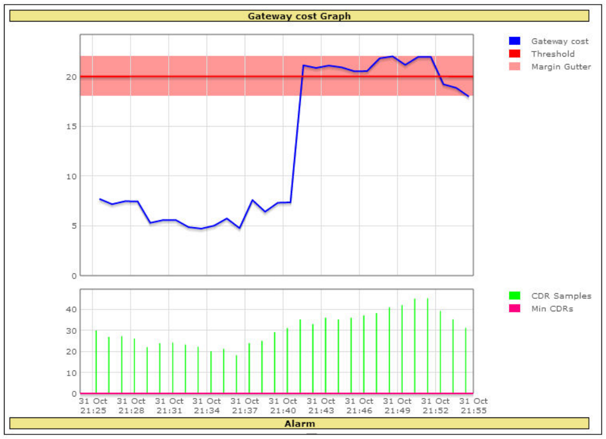
Gateway Minutes monitors the minutes to or from a particular carrier and can be used to detect potential fraudulent activity or alert sales staff of upsell opportunities.

Similarly, Gateway Cost provides an associated dollar amount instead of minutes, often used with new carriers where spend thresholds are set to alert account managers to visit the carrier for additional business or of possible fraud.

There are a number of Operational Alarms that look at the performance of your platform and notify operational staff should the service degrade, and can also indicate a breach or misuse of your system. Alarms can be setup to detect low average call duration (ACD) and poor success rate (ASR) that could potentially indicate fraud. Error Count looks at the reoccurrence of a particular type of call release code, such as ‘not authorised’, indicating someone may be trying to breach your system.

Fraud Notification

When an alarm is triggered, Adaptiv will notify your NOC using SNMP and email key support staff about the detected problem.



Adaptiv will email a copy of the graph that shows what triggered the alarm, allowing your support staff to quickly assess the issue.

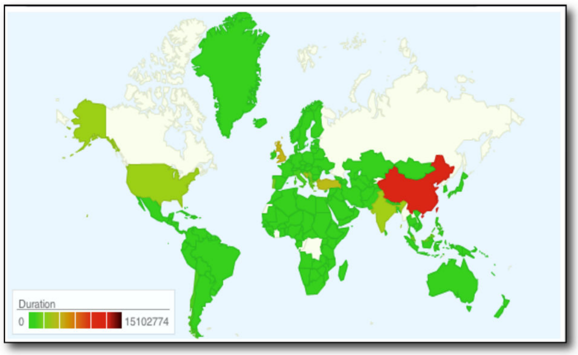
Automatic Blocking

For Adaptiv systems that route as well as monitor, you can set up Adaptiv to automatically block traffic associated with the cause of an alarm. At any time, support can remove the block and restore normal routing. In cases where staff are unable to investigate the problem, Adaptiv will automatically restore routing after a specified period of time and check if the problem is still present.

Fraud Investigation

Adaptiv provides an easy to use web interface, combined with a powerful OLAP database, allowing quick discovery of potential issues and an analysis of traffic patterns in your system.

Graphic representations, such as the World Map, allow you to see a geographical overview of your traffic patterns based on current and past traffic.



Analytical Charts summarises your history of data. You can tailor the data, selecting Total Calls, Successful Calls, Total Minutes, Cost, ASR, ACD, PDD, QOS and turn this data into charts that provide an interactive visualisation.

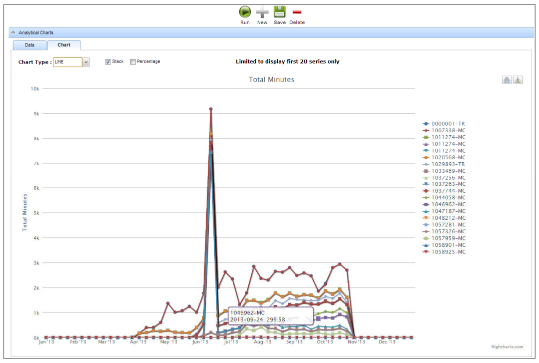
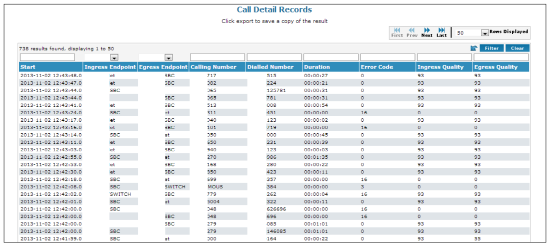


Chart Type : LINE ☑ Stack ☐ Percentage

Limited to display first 20 series only

View CDR allows you to select a range of CDR and drill down to a short list using filters.



Call Detail Records

Click export to save a copy of the result

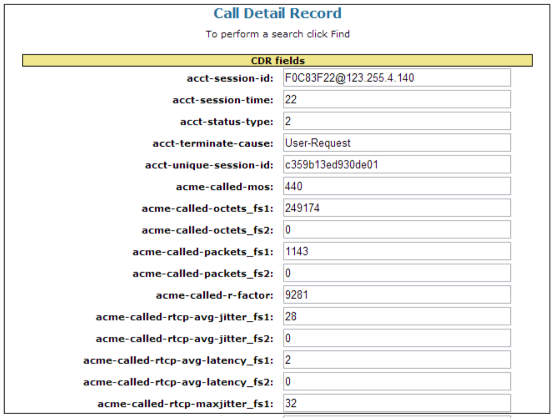
First Prev Next Last | 50 Rows Displayed

738 results found, displaying 1 to 50

Filter Clear

Start	Ingress Endpoint	Egress Endpoint	Calling Number	Dialled Number	Duration	Error Code	Ingress Quality	Egress Quality
2013-11-02 12:43:48.0	et	SBC	717	515	00:00:27	0	93	93
2013-11-02 12:43:47.0	et	SBC	082	224	00:00:21	0	93	93
2013-11-02 12:43:44.0	SBC		065	125781	00:00:31	0	93	93
2013-11-02 12:43:44.0		SBC	065	781	00:00:31	0	93	93
2013-11-02 12:43:41.0	et	SBC	513	008	00:00:54	0	93	93
2013-11-02 12:43:24.0	SBC	et	311	451	00:00:00	16	0	0
2013-11-02 12:43:17.0	et	SBC	940	123	00:00:02	0	93	93
2013-11-02 12:43:16.0	et	SBC	101	719	00:00:00	16	0	0
2013-11-02 12:43:14.0	SBC	et	050	000	00:00:45	0	93	93
2013-11-02 12:43:11.0	et	SBC	650	231	00:00:39	0	93	93
2013-11-02 12:43:03.0	et	SBC	940	123	00:00:03	0	93	93
2013-11-02 12:42:55.0	SBC	et	270	986	00:01:35	0	93	93
2013-11-02 12:42:53.0	et	SBC	168	280	00:00:22	0	93	93
2013-11-02 12:42:30.0	et	SBC	350	423	00:00:11	0	93	93
2013-11-02 12:42:18.0	SBC	et	599	357	00:00:00	16	0	0
2013-11-02 12:42:08.0	SBC	SWITCH	MOUS	384	00:00:00	3	0	0
2013-11-02 12:42:02.0	SWITCH	SBC	779	262	00:00:04	16	93	93
2013-11-02 12:42:01.0	SBC	et	5004	322	00:00:11	0	93	93
2013-11-02 12:42:00.0	SBC		048	626696	00:00:00	16	0	0
2013-11-02 12:42:00.0		SBC	048	696	00:00:00	16	0	0
2013-11-02 12:42:00.0		SBC	279	085	00:01:01	0	93	93
2013-11-02 12:42:00.0	SBC		279	146085	00:01:01	0	93	93
2013-11-02 12:41:59.0	SBC	et	000	164	00:00:22	0	93	55

With the click of a button, you can select any particular CDR in the list and view all the raw data regarding that call.



Call Detail Record

To perform a search click Find

CDR fields

acct-session-id:	F0C83F22@123.255.4.140
acct-session-time:	22
acct-status-type:	2
acct-terminate-cause:	User-Request
acct-unique-session-id:	c359b13ed930de01
acme-called-mos:	440
acme-called-octets_fs1:	249174
acme-called-octets_fs2:	0
acme-called-packets_fs1:	1143
acme-called-packets_fs2:	0
acme-called-r-factor:	9281
acme-called-rtcp-avg-jitter_fs1:	28
acme-called-rtcp-avg-jitter_fs2:	0
acme-called-rtcp-avg-latency_fs1:	2
acme-called-rtcp-avg-latency_fs2:	0
acme-called-rtcp-maxjitter_fs1:	32

Conclusion

Adaptiv offers powerful and flexible fraud detection software that's easy to use, complete with setup support and visuals, so you can quickly understand the problem at hand.