TransNexus®

2014 TMC INTERNET TELEPHONY PRODUCT OF THE YEAR

TRANSNEXUS DATA SHEET

NexOSS-FC

TRAFFIC PUMPING FRAUD AND THEFT OF SERVICE

Each year, billions of dollars are lost to telephone traffic pumping fraud. The fraud targets are business telephone systems. Hackers break into poorly secured business telephone systems and generate thousands of expensive international calls in just a few hours. The fraud losses can quickly exceed $100,000. Every telephone and user account is a potential intrusion path for phone hackers and achieving 100% security is impossible. Active monitoring of telephone calls is the only certain protection for preventing huge fraud losses for business and service providers.

For decades, telecom fraud detection solutions have relied on analysis of Call Detail Records (CDRs) to detect fraud. CDR analytics work well, but fraudulent calls must be completed and CDRs must be collected before fraud can be detected. This is a major weakness. Fraudsters can make hundreds of long calls and tens of thousands of dollars can be lost before the first CDR is collected.

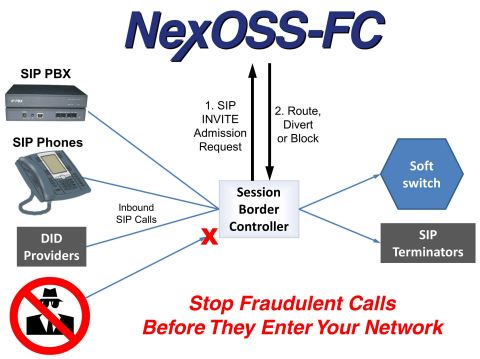
SIP ANALYTICS™

NexOSS-FC solves this problem by using SIP Analytics to detect fraudulent calling trends before calls are made. NexOSS-FC scores each SIP INVITE for fraud potential before it enters your network. SIP Analytics uses the same techniques as CDR analytics, such as historical analysis and adaptive learning. However, SIP Analytics is much faster and uses SIP header information, not available in CDRs, for smarter fraud detection with fewer false positives.

HOW IT WORKS

NexOSS-FC can complement any Session Border Controller (SBC) or softswitch. Since NexOSS-FC is entirely SIP based, it can provide fraud detection for any SIP device. When a SIP call arrives at the SBC, the SBC forwards the call to NexOSS-FC. NexOSS-FC responds in less than a millisecond with instructions to:

1. Route the call as normal
2. Block the call
3. Divert the call



EASY TO DEPLOY, EASY TO USE

NexOSS-FC is very easy to deploy. Packaged as a virtual machine, it can be installed within minutes and protect your network. An out-of-the-box installation with default settings will protect your network from a significant fraud event. As the software learns the traffic patterns of your users, fraud detection triggers will be automatically optimized for each source IP address and calling number for each hour of the week.

FEATURES

- Real time fraud detection by source IP address, calling number and user agent
- Automatic blocking or call diversion
- Blacklist of over 50,000 high risk number ranges
- A single NexOSS-FC provides fraud detection for multiple SBC's from any vendor

BENEFITS

- Peace of mind - eliminates the risk of a major fraud loss
- For service providers, fraud detection and insurance for customers is a value added feature which can be sold for additional revenue
- Savings from stopping one fraud event will pay for the software

ASK FOR A FREE TRIAL

TransNexus will install the NexOSS-FC software in your network for a 30-day evaluation trial. Begin protecting your network from fraud immediately.

HOST SERVER SPECIFICATIONS

- 64-bit Redhat Enterprise Server V6, CentOS V6, or VMware Esxi V5
- Eight CPU cores
- 8-32 GB of RAM depending on calls per second

ABOUT TRANSNEXUS

TransNexus is a software development company specializing in applications for managing wholesale VoIP networks. TransNexus provides its Operations and Billing Support System (OSS/BSS) software platform to major VoIP carriers worldwide. Important carrier features offered by TransNexus are least cost routing, number portability, fraud detection, profitability analysis and QoS controls.

75 Fifth Street NW, Suite 313, Atlanta, GA 30308 • 1404.526.6053 • info@transnexus.com • www.transnexus.com