squire technologies

CLOSING DOWN ILLEGAL BYPASS FRAUD IN SOUTH AFRICA

Introduction

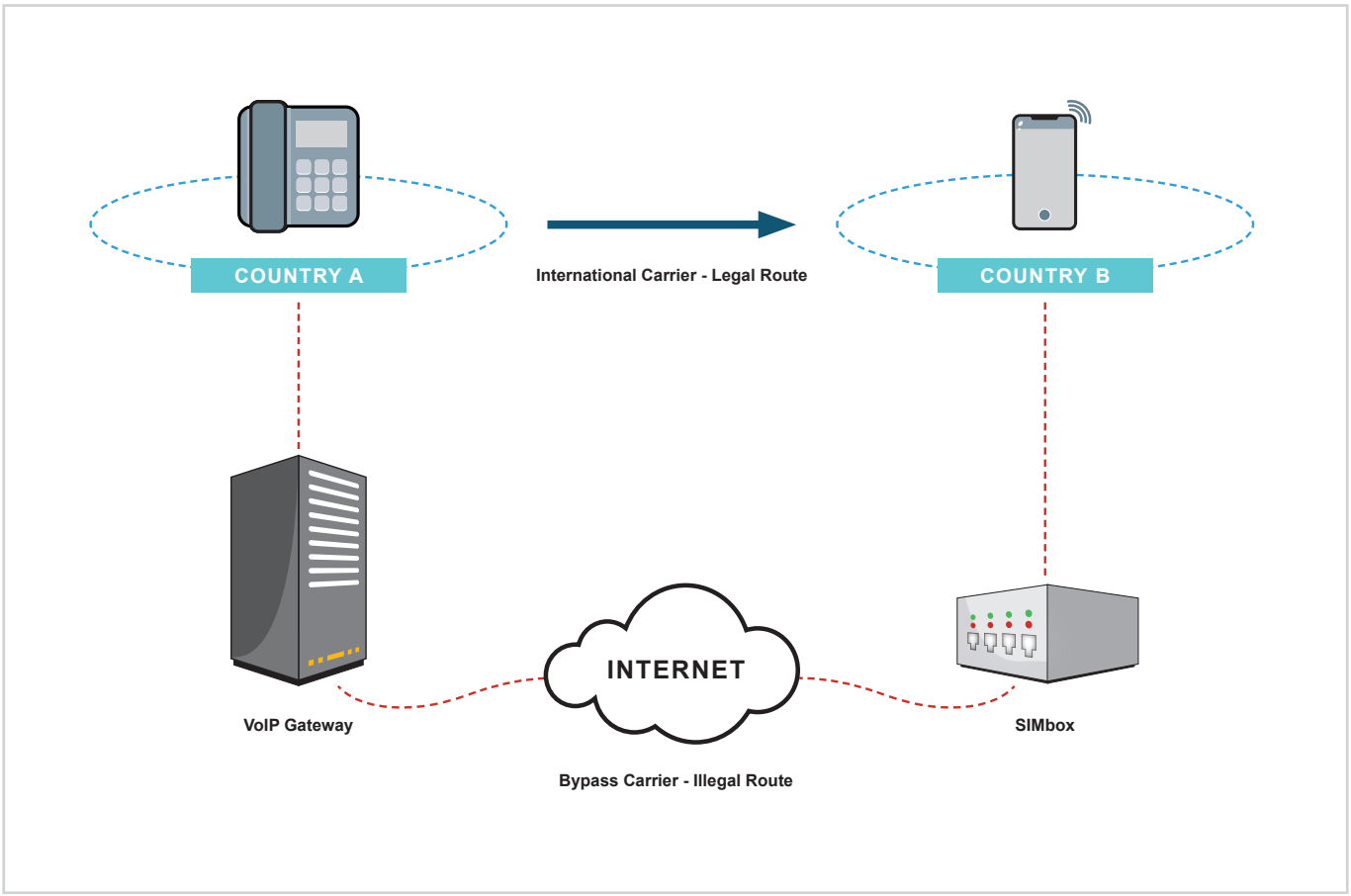
Working with a South African Tier 1 telecoms operator struggling to deal with the impact of international bypass fraud, Squire Technologies' MavenShield Fraud Prevention Solution was integrated and deployed as part of a comprehensive Network Protection System.

Background

In some countries, including South Africa telecom operators are taxed on the international communications that are made in and out of the country.

This taxation has seen the rates charged by operators for international calls escalate, which in turn has driven an industry in international bypass fraud.

SIMbox or Bypass Fraud is when fraudsters set up SIMboxes with multiple low-cost prepaid SIM cards that are used to terminate international calls through local phone numbers to make them appear as if they're local calls.

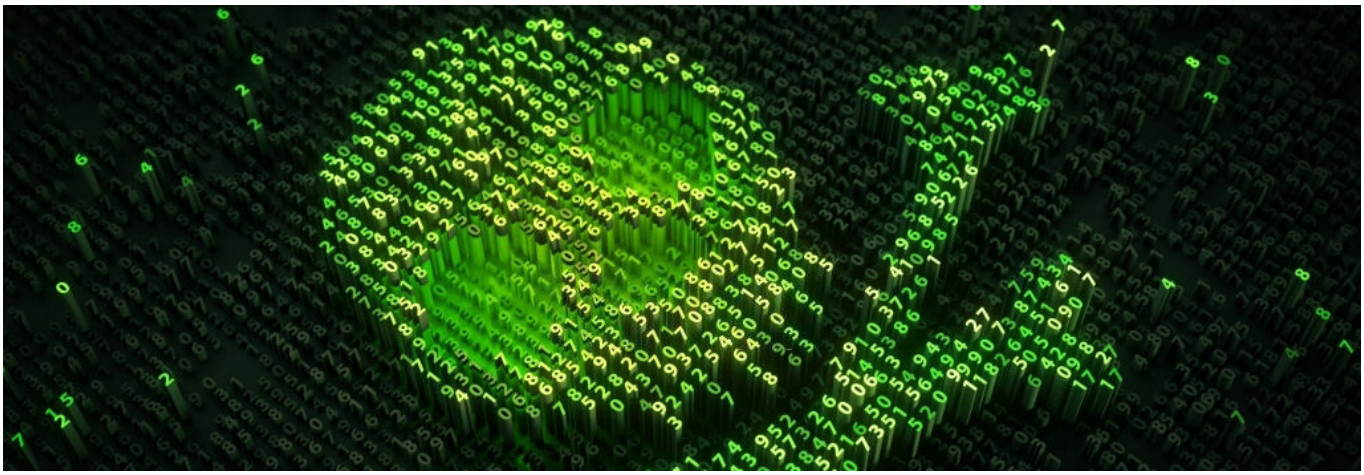


Here fraudsters bypass all international interconnect and termination charges while the operators count the cost in lost revenue as calls bypass their legitimate international gateways.

Fraudsters have become increasingly more sophisticated teaming up with international partners to route significant volumes of international calls through (off-net) the internet using VoIP networks and terminating these through illegal SIMboxes.

Scope and Challenges

The operator runs a Network Protection System which combines a Big Data platform with an 'Intermediate' product that provisions their HLR and routing server. Here the Big Data platform detects fraudulent on-net calls routed through illegal SIMboxes.



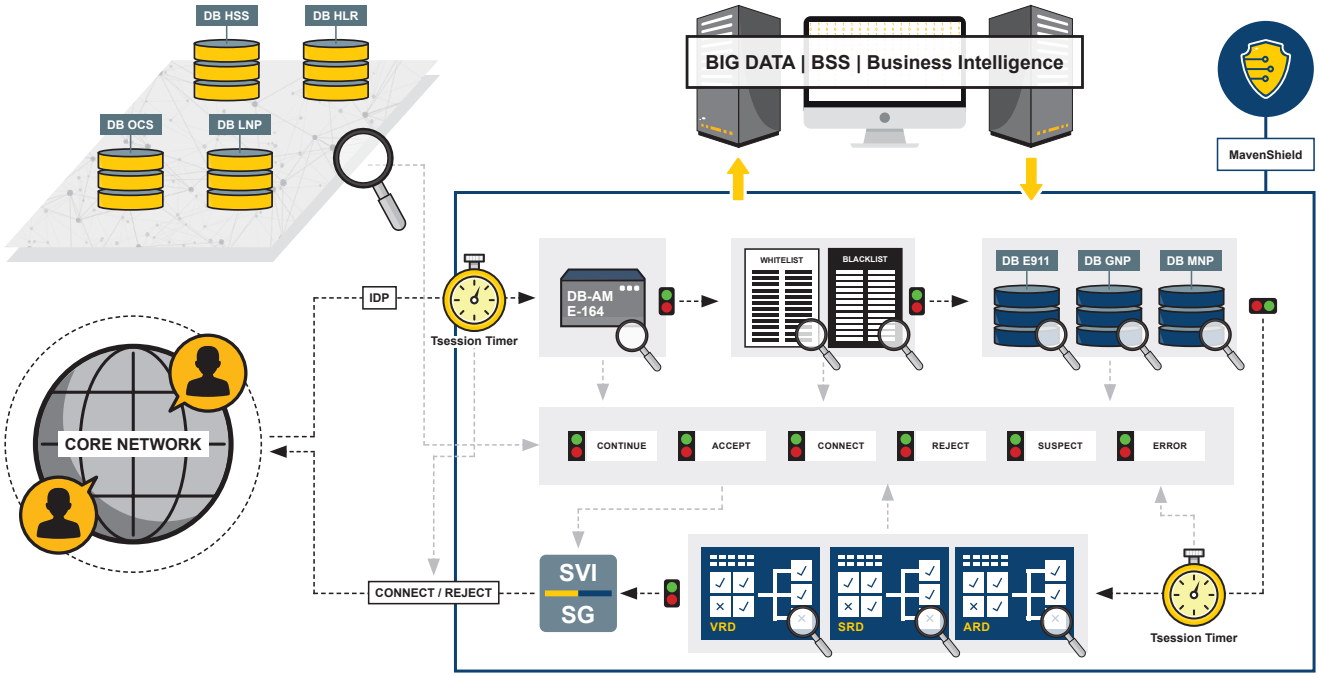
While the operator was utilising their own products for active and passive fraud detection within their own network, they faced challenges in terms of being able to detect and block fraudulent off-net (other local operator) calls in real-time.

The Solution

Our MavenShield fraud prevention gateway is a highly adaptable product designed to integrate with existing BSS, Fraud Prevention and Revenue Assurance solutions.

It provides a means of rapidly taking proactive measures, in this case call blocking upon the detection of suspect traffic.

The operator integrated MavenShield, making it an integral part of their Network Protection System (referring to it as a routing server), to facilitate real-time call blocking of fraudulent off-net calls. Here MavenShield pulls down a regular data stream from the Intermediate product including up to the minute Blacklist and Whitelist databases.



Connected directly to the operators STP's MavenShield receives CAMEL IDP triggers, and based upon the INAP IDP message content it either accepts or rejects calls.

MavenShields' appeal is in its high degree of flexibility, with network managers and engineers able to configure any number of rules to identify fraudulent traffic, including database lookups to outside network components. Here the operator has set up rules including screening of E.164 numbers (to comply with South African numbering plan regulations), rules to identify whether the calling party number belongs to the correct service provider and whether they're using assigned or unassigned numbers.

The decision to block calls is based upon a combination of the data stream from the Intermediate and the configured set of rules within MavenShields business logic. This particular deployment also sees MavenShield set to export all the transaction data records from off-net calls for provisioning into the operators HLR.

The Results

Seamlessly integrated into the operators Network Protection System MavenShield has resulted in the South African operator deploying a comprehensive and future proof fraud prevention solution aimed at stopping fraudsters from finding an easy way to defraud the network out of valuable interconnect and termination revenue.

This holistic approach to an increasing threat to operators and their customers illustrates how telecoms operators require a multi-layered approach to combating network fraud.

Bypass fraud and other illegal activity on our telecoms networks is an increasing issue that brings with it a host of problems for operators, namely huge losses in revenue, but also the potential of considerable fines from regulators and the resulting loss of brand value and customers. For more information about MavenShield and Squire Technologies fraud prevention solutions visit www.squire-technologies.com or call us today on +44 (0)1305 757 314