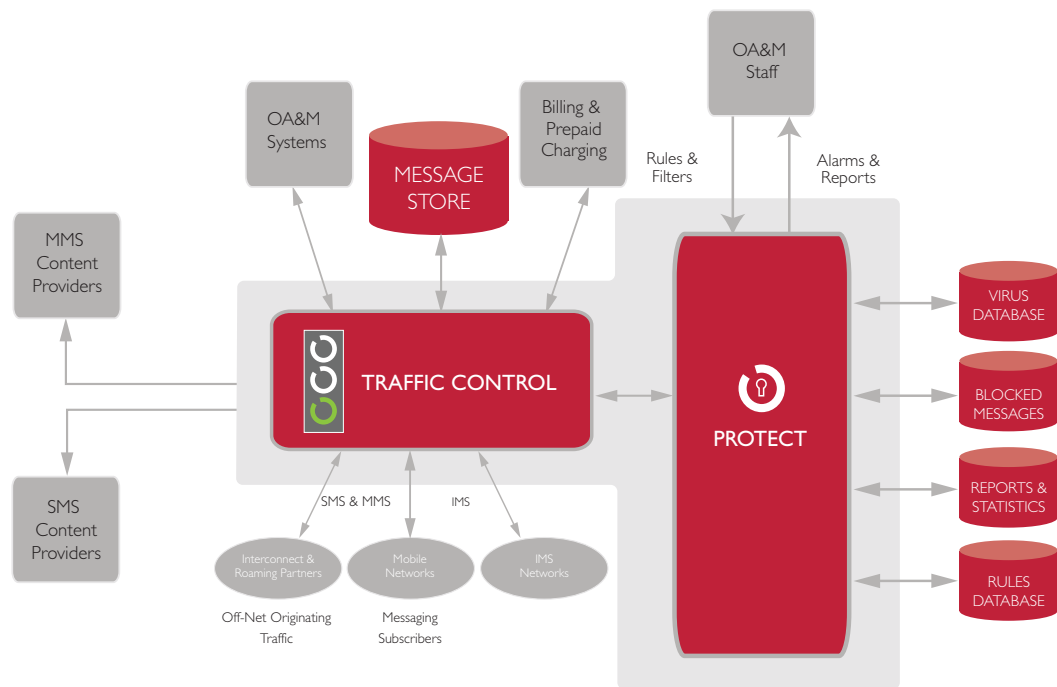


The Protect Module: Securing Messaging

As operators open up more interconnection points, and support new interfaces for message submission from applications, they are also giving fraudsters and spammers new opportunities for targeting subscribers via the messaging service. New service concepts including m-commerce, mobile banking, and e-wallets would be rendered unworkable if vital messaging bearer technologies become compromised.



Protect filters out undesirable messages that seek to attack or defraud subscribers or network infrastructure and underpins revenue assurance initiatives to prevent leakage. The system stops spoofed and faked messages that are impossible to bill, ensuring that network bandwidth is freed up for revenue generating traffic. As many fraud threats originate outside of the home network, operators can use Protect to intercept mobile terminating traffic entering the network via interconnect partners or roaming partners.



SMS Spam

SMS Flooding

SMS Faking

MMS Viruses

SMS Spoofing

Key Features

1. Eliminate threat of spam & fraud to integrity of the network

- 100% inspection of all traffic
- All protocol layers examined

2. Fully integrated with Symantec anti-virus engine for blocking MMS traffic containing viruses



The Protect Module: Securing Messaging



Key Features

Configuring the System

The Protect module uses a combination of Filters, Rules and Execution Plans to identify security and spam threats and to determine what steps to take. Filters, Rules and Execution Plans can all be created and defined by an operator through a web interface.

Filter Creation

The operator can define filters to select messages, for example Spam or Spoof messages that has been previously detected on the operators network. Messages that match the filter criteria are then subject to possible subsequent actions, for example, they can be blocked or quarantined, or they can trigger a warning message to be sent to the originator.

Filters are classified into the following types:

Address Filters allow the operator to screen messages based on addressing information within the message such as, the OA, DA, SCCP Called or Calling addresses, Service Centre address, IMSI etc.

Content Filters allow you to screen intercepted messages based on the content type or a specific text string. One default Content filter is available from start up, which can be modified to suit requirements however additional content filters can be provisioned as required

Spoofing Filters check that the address data in the message correctly matches the address data supplied at the SCCP layer.

Spam Filters The nature of Spam messages is that they are sent repeatedly to many different destinations and since there are many Spammers sending these messages it is a challenge to define filter criteria to detect such messages



Protect provides a two-stage mechanism to detect Spam messages:

Spam Traps – they detect Spam activity and log a record of it in either the Candidate list or the Active list. These lists are placeholders for storing copies of detected Spam activity

Spam Filters - Subsequent messages that match the messages in the Candidate or Active list can then be filtered out using specific Spam filters that use the messages in these lists.

Meta Filter

Meta Filter allows you to screen intercepted messages based on a combination of the other four filtering mechanisms (Address, Content, Spam and Spoof).



Openmind Networks

4 Westland Square, Dublin 2, Ireland Tel: +353-1-633-0070 Email: info@openmindnetworks.com

www.openmindnetworks.com