Powering Mobile Innovation

Filtering Engine

Protect your network, subscribers and brand image

Key Benefits

Maximise network usage and reliability
Protect the network through blocking unwanted and fradulent traffic and efficiently reducing associated direct and indirect costs

Highly flexible and comprehensive security solution
Consolidate network-wide security policy through multiple channels onto a single solution with an extensive rules-based platform

Provide a safer network and earn subscriber loyalty
Enhance the subscriber experience and earn loyalty by providing a safer network and by putting subscribers in control of the content they want to receive

Market Dynamics

Messaging spam and virus traffic is booming and consuming an increasing amount of valuable network resources, as well as impacting mobile subscribers and the operators' brand image. In order to protect the network, optimise its usage, and enhance the customer experience to build loyalty, mobile operators need to deploy comprehensive and effective anti-malware tools and messaging filtering capability to detect and block unwanted traffic.

Product Overview

The Jinny Filtering Engine is designed to help protect the reputation of your network and your subscriber's experience. It analyses messaging traffic, detects fraudulent elements and blocks undesirable text and multi-media content from both on and off-network sources to ensure that the network handles only desirable traffic. The Jinny Filtering Engine is built around a sophisticated and highly customisable rules-based engine providing the operator with flexibility in factoring in both the network operator's and subscriber's policy. It consolidates network and subscriber preferences inside this highly flexible framework and can integrate easily into multiple back-office systems.

Engineered for best performance with an intuitive user interface, the Jinny Filtering Engine provides operators with a reliable solution to implement SMS, MMS and HTTP traffic screening for anti-spam, anti-flood, anti-fraud and anti-virus on the same platform. It enables you to consolidate a comprehensive security preference for the following requirements:

Network-level Control - Protect the network from malware, virus, malicious and fraudulent traffic, helping to maximise network usage, decrease costs and increase reliability and customer satisfaction.

Subscriber-level control - Protect the subscriber from spam and unwanted traffic helping to build operator loyalty, reduce customer care costs and enhance the end-user experience. New customer-centric control services can also be introduced to generate additional revenue.

Key Features

Highly Flexible
A high performance rules-based engine with a wide set of criteria for maximum flexibility in message content and parameter filtering, fraud evaluation and associated decision actions. The Filtering Engine acts as the Policy Decision Point for messaging traffic, relying on Jinny's messaging proxies or legacy ones.

Wide Spectrum for Security and Policy Control
Provides anti-spam, anti-fraud, anti-flood, anti-virus, plus the Policy Control Function to block unwanted content and traffic.

Sophisticated Filtering
A sophisticated and advanced filtering capability including pattern matching, repeated content and addressing, anti-flooding and content filtering. Capabilities include:

- Filtering out messages identified as spam or phishing attacks against a subscriber
- Malware and spam detection through traffic analysis, filtering of messages based on mobile spam signatures and spam detection algorithms
- Content filtering through signature and specialised 3rd party analysis engines

Operator and Subscriber In-Control
Consolidate the network policies defined by the operator and its subscribers. Collectively the Jinny Filtering Engine solution offers:

- Mobile operator-defined network control and throttling rules
- Mobile operator-defined anti-fraud rules and anti-spam
- Subscriber-defined acceptable or unwanted content

Messaging and IP Traffic Control
Supports SMS, MMS, SMTP and HTTP traffic control for all traffic interfaces, with adherence to 3GPP, OMA, IETF standards.

Filtering Engine Architecture