



# **LEON**

**Enterprise Anti-Spam Server**

**and**

**Enterprise Anti-Spam Engine**

Technical Specification

## Leon – The Anti Spam Server

Leon incorporates a multitude of techniques to combat SPAM and uses the concept of DPR – Detection, Prevention and Retaliation. Leon is built as a proxy mail server and it implements a full RFC compatible SMTP server.

Leon acts as a mail proxy and is simply added between the internet, the firewall and the normal mail server. Due to its architecture, the receiving part of Leon can be separated from the filtering and delivering part.



## Feature List

Product Type	Server-based; SMTP Proxy for any SMTP mail server
Operating Systems	Windows 2000 Server, Windows XP Pro, Windows 2003 Server
Features	Spam Filtering; Policy compliance filtering for incoming mail; e-mail management (reporting, archiving, etc.); e-mail relay; Attachment handling (deconstruction / analysis of attachments, extraction, blocking), Quarantine (with user access through web)
Management tools	MMC based, Windows Automation (Scripting), Web Based.

## Anti-Spam Techniques

Subject keyword search	●
Subject RegEx or Pattern search	●
Body keyword search	●
Body RegEx or Pattern search	●
MIME deconstruction	●
Keyword search in deconstructed content	●
RegEx. search in deconstructed content	●
Message format analysis	●
MIME specific format analysis	●
Statistical analysis	●
Bayesian Filtering, generic auto-updating, multiple algorithms	●
Linguistic analysis	●
Header analysis	●
Header RFC compliance analysis	●
Content RFC compliance analysis	●
Header-chain verification	●
Date/Time sequence verification	●
Attachment deconstruction	●
Attachment analysis	●
Attachment blocking by type (name/extension/MIME)	●
Attachment blocking by size	●
MTA blacklist	●
IP blacklist	●
Domain blacklist	●
Sender blacklist	●
DNS blacklist (DNSBL, RBL)	●
DNS whitelist (DNSWL, RWL)	●
Reverse MTA IP verification	●
SMTP standard compliance enforcement	●
MTA whitelist	●
IP whitelist	●
Domain whitelist	●
Sender whitelist	●
Habeas Support	●
Habeas Whitelist Support	●
Multiple Language Support	6 Languages + Generic
Language specific algorithms for every supported language	●
Language detection and filtering	●
Directory harvest attack (DHA) protection	●
MTA behavior analysis and blocking	●
automatic MTA blocking when Spam level exceeds threshold	●

Spam technique detection	●
contained URL blocking	●
Open proxy lists	●
Mail Header Whitelist	●
Mail Header Blacklist	●
Nameserver Whitelist	●
Nameserver Blacklist	●
Mailing List detection and filtering	●
URL Nameserver Whitelist	●
URL Nameserver Blacklist	●
Country Whitelist	●
Country Blacklist	●
Spoofing protection	●
Bypass lists	Sender, Domain, Recipient, HELO, IP, Trusted MTA, Maillists
Customizable SMTP reply codes	with variable replacement
Rate Limiting of Spam Sources	●
Mail Quota	Soft, Hard
DNS Caching	DNS, blacklists, whitelists
Grey-listing	●
SPF support (Sender Policy Framework)	●
SenderID support	Leon 2006
DKIM	Leon 2006
Event notifications	by mail
Activity reports	by mail
Restricted Mode Operation	●
Active Directory Support to synchronize user database	●
Detailed connection history	●
Message Archive	●
Reputation Filtering	●
User import	Automatic, Textfile, Database, Windows, Active Directory

## General Features

Compatibility	TCP/IP, SMTP, RFC's – 974, 1123 §5, 1741, 1766, 1806, 1869, 1872, 2045, 2046, 2047, 2076, 2110, 2183, 2635, 2821, 2822
Multiprocessor Support	Yes, unlimited
Retaliation Support	Tarpitting (utilizing the RFC SMTP specifications); Delaying SMTP connections for detected Spam Sources;
Performance	Single Processor P4/2.4 Ghz: ~50 Mails/Sec., min. 600 Kbyte/Sec.
Attack/Hijack protection	Split-Server architecture; Behavior-based MTA blocking; Flood blocking; Connection limiting;
Phishing Protection	Yes, Automatic Update
Logging	Real-time logging of incoming connections; Real-time logging of filtered mail; Real-time logging of all filtering processes;
General Spam reduction	~99.3% with standard configuration; more can be achieved
Options for identifying Spam	Tagging subject with [SPAM] tag; Tagging headers with detailed filter results; Quarantine in system; Log; Pass-through after tagging; Delete;
Quarantine Features	User access through Web; Periodic notifications; Automatic deletion after time; Mail inspection through administrator; Search by any attribute; Administrative quarantine;
Spam engine update	Multiple daily updates from vendor over the Internet through encrypted and signed mail messages (optional per FTP); Auto-learning (via Bayesian Filter); Automatic Engine updates with administrative confirmation; Server does not need to be restarted for data updates;
Spam levels supported	Positive yes/no indication; weight system (0-100) with administrator defined threshold.
Adjustment of Spam engine	System global settings; Group/User specific settings; IP specific settings; Domain specific settings;
Message formats scanned	Text; All MIME formats (including HTML)
Scriptable	Yes, VBS, JavaScript, VB, C#, etc.
Spam activity reports	Yes; daily, monthly, yearly; Reports can be exported as HTML, XML, Graphic; Reports are customizable by the user
Licensing	License bound to number of users, domains and licensing time

## Availability

Appliance	L200 - Pentium 4/2.8 GHz, 1 Gb RAM, 40 Gb HD, Height 1U L400 - P4/3.2 GHz, 1 Gb RAM, 80 Gb HD, Height 1U L800 - Dual Xeon 3.2 GHz, 2 Gb RAM, 200 Gb HD, Height 3U
Software	On CD for installation on customer supplied hardware

### *Additional notes*

Product includes all features in the base configuration. Additional, specialized dictionaries for the Bayesian filters are available on request. Compatible with every SMTP based mail server, independent of operating system.