



UNIWARES
Information Security Systems

UNIWARES

LEON ANTI-SPAM SERVER

LEON - Enterprise Anti-Spam Server

LEON - The Anti-Spam Server is responsible for receiving and classifying the E-mails within a clients company or organization. Its principal function is to impede, close to all, unsolicited commercial emails (UCE). In this way, a company that uses LEON will have a significant return on the following areas and therefore on its Return On Investment: Economize on the consumption of the bandwidth; Reduction on administration costs of the corporate network; Gain with user/employee productivity; Reduces the threat of viruses and spywares.

Technical specifications

Leon is built as a proxy mail server. It implements a full RFC 2821/1869 compatible SMTP server and is compatible with any SMTP mail system. Policies can be applied to inbound and outbound mail traffic.

Multi-Language Support

Leon contains full support for currently six languages (English, Portuguese, French, Italian, Spanish and German) through separate dictionaries and language specific Spam filters.

Language Awareness

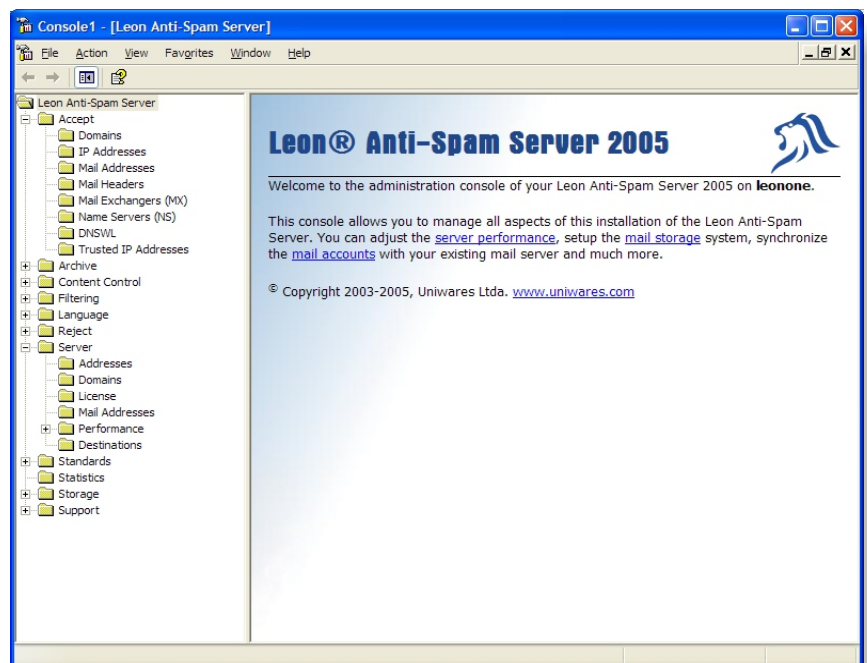
For each supported language, it uses specific algorithms and dictionaries, which handle the languages semantics and rules.

Bayesian Filters

Generic self-adapting filters using multiple algorithms perform in-depth content analysis.

Flexible Filters

Filters like regular expression filters allow filtering of mail elements containing certain keywords, phrases or patterns. Heuristics find variations in Spam techniques. Filters can be separately enabled and changed in order.



Attachment Filtering

Mail attachments can be filtered by type, size, MIME type, etc.

Reporting

Complete reporting options give total transparency of the mail traffic and Spam filtering. Information about major Spam sources, types of attacks, volumes, sizes and bandwidth of mail traffic are easily obtained and can be displayed and exported in a variety of formats.

100% RFC Compliance

In all aspects the compliance with current Internet standards (RFCs, BCPs) is guaranteed and can be made part of the policy (SMTP connections, mail content and formats, etc).

Quarantine

Mails can be automatically quarantined for user and/or administrator access. Through full featured web access quarantined items can be easily managed (remove, forward, deliver, report, view, source, etc). False positives are automatically reported to the Uniwares Spam Catcher team. Administrators can delete single messages, mailboxes or the complete quarantine.

Sender Verification

Verifies the identity of a TCP connection during initial communication. Connections from either blacklisted senders or senders with false or spoofed information can be blocked. Various standard techniques are used to accomplish verification.

TCP information headers

All incoming mail is extended with full connection information about the senders TCP connection. IP address, resolved host name, claimed host name, port and protocol are logged.

Behavior Detection and Retaliation

Sending mail systems are monitored for policy violations according to administrative parameters like number of connections, spam amount sent, etc. Retaliation features like tar pitting and bandwidth throttling reduce the impact of these offending mail systems by severely delaying and limiting connections from such systems.

Attack and DoS protection

Active protection against directory harvesting, denial of service and phishing attacks protect your mail system and network users.

Flexible Targets

Filtered mail may trigger customizable actions, can be forwarded to certain mailboxes, be dropped automatically or can be quarantined until administrative action is taken. Web access allows users and/or administrators to inspect quarantined email.

Real-time Black Hole Lists (RBL)

The filters include full DNS based RBL filtering. Databases are configurable. Databases like MAPS, DUL, Spamhaus, etc. are supported by default. Local DNS queries are supported; subscribed RBL providers (through zone transfers) can be used.

Real-time White Lists (RWL)

The filters include full DNS based RWL filtering. Databases are configurable. Databases like Habeas IP Whitelist are supported by default. Local DNS queries are supported; subscribed RWL providers (through zone transfers) can be used.

White Lists (accept)

White list filtering for mail exchangers (MX), senders, mailing lists, single hosts and recipients allows flexible pass-through configuration for any source or target. White listed items are never filtered out.

Black Lists (reject)

Administrators may manually add certain items to the black list filters. Items on these lists are always filtered out, even if they would pass all other filters.

Pass-through Lists

Mailboxes, domains and mail exchangers can be configured as pass-through items. An administrator can setup Leon to pass-through any mail coming from a certain MX; exclude some mailboxes from filtering; or, for ISP operation, exclude filtering for certain domains.

Administration

All configurations can be performed through Microsoft Management Console (MMC) snap-ins, a web browser, scripts or command line (CLI). All events can be scripted (e.g. notifications, failures, reports, etc.). The user interfaces are available in various languages. This reduces administration costs.

Windows Performance Counters

Using standard Windows mechanisms for performance measuring, Leon does allow easy integration into standard management tools.

Leon Subscription Service

UNIWARES offers a subscription service, which guarantees the constant up grading of the LEON software and up dating of the LEON libraries via an automatic system developed especially for LEON. These libraries are a fundamental requirement for the efficient control of spam on your email service system. For this reason UNIWARES maintains within its environment a team of professionals called "LEON Spam Catchers" trained to up-date the library 24 hours, 7 (seven) days a week with the information gathered from millions of monitored mailboxes worldwide.

Availability

Either as server-installable software or the following appliance types:

L200 - Pentium 4/2.8 GHz, 1 Gb RAM, 40 Gb HD, Height 1U, 19" width

L400 - P4/3.2 GHz, 1 Gb RAM, 80 Gb HD, Height 1U, 19" width

L800 - Dual Xeon 3.2 GHz, 2 Gb RAM, 200 Gb HD, Height 3U, 19" width

LAS500 - 1x PROC. AMD OPTERON 64BITS - SERIE 246 - 2.0 GHZ CACHE L2 1MB, 1GB DDR400 ECC, 2x HD

SCSI ULTRA320 73GB 10K RPM SCA (RAID), redundant power supply (500W) 2 Network adapters

(10/100/1000) LAS2500 - 2x PROC. AMD OPTERON 64BITS - SERIE 246 - 2.0 GHZ CACHE L2 1MB, 2GB

DDR400 ECC, 4x HD SCSI ULTRA320 73GB 10K RPM SCA (RAID), redundant power supply (800W) 2 Network

adapters (10/100/1000), 19" width

Uniwares - Information Security Systems

Uniwares is an information technology company dedicated to the design, development and marketing of advanced core quality software products and added-value solution services in the area of Information, Internet and networks security. Uniwares develops and uses advanced cutting edge technology, offering superior quality services and advantages for organizations that strive to achieve a solution that is continuous and sustainable.

Uniwares has been developing applications since 1996. Recently, we have been developing corporative applications, offering the market products with quality of excellence. Our latest release, the Leon Anti-Spam Server, is the first solution on the market, which supports six different languages.

Other simple applications and tools are available for download. All our products are developed in C++ and some source codes are available.

Uniwares Information Security Systems Ltda.

info@uniwares.com.br

www.uniwares.com.br

