VisNetic MailPermit
Enterprise Anti-spam Software

VisNetic MailPermit

permission-based email system

Best of Class

VisNetic MailPermit is on-premise anti-spam software that combines SpamAssassin's sophisticated Bayesian and rules-based anti-spam technology with a proprietary challenge-response system to provide an optimum barrier against spam. The product, which installs easily onto all popular email servers, can virtually eliminate the daily spam that clogs email infrastructures, drains employee productivity and increases legal exposure in organizations.

Best of Class Anti-spam Technologies

VisNetic MailPermit combines Best of Class anti-spam technologies to effectively eliminate spam before it reaches your mailbox. These technologies include (in order of processing):

❑   Whitelists and Blacklists

❑   Rules-based filtering and Bayesian analysis

❑   Permission-based email

Individualized Whitelists and Blacklists

A whitelist is a list of email addresses or domain names from which email-blocking software will allow messages to be received. Whitelists ensure that email from pre-approved senders (e.g. partners, vendors or investors) is automatically delivered to recipients in your organization. A blacklist is a list of email addresses or domain names used by email blocking software to reject email. Blacklists ensure that email from addresses or domains, identified by your organization and/or users as known sources of spam, is automatically deleted before it reaches the recipient's mailbox.

VisNetic MailPermit features whitelist and blacklist capabilities at the system, domain and user levels, with the user level taking precedence. Whitelists and blacklists at the user level allow for the most effective use of this technology to combat spam. For example, your IT staff may not wish to receive messages from an apparel supplier while your purchasing staff welcomes email from the same supplier. In this example, purchasing agents include the supplier's email address or domain in their whitelists and IT staff relegates the address or domain to their blacklists. Consequently, your IT staff is protected from unwanted email while your purchasing agents continue to receive this vendor's messages.

VisNetic AntiSpam

VisNetic MailPermit includes a tightly integrated implementation of VisNetic AntiSpam, a rules-based filtering tool powered by SpamAssassin technology. VisNetic AntiSpam subjects each email message to over 400 tests and assigns a numerical value or score to each message based on the likelihood that it is spam These scores are determined by a series of time-tested checks on the headers and body of a message, including: Bayesian Heuristic Classification, rDNS and MX lookups, and Header, Body and HTML filtering.

VisNetic AntiSpam also includes a mechanism (Bayesian analysis) by which the software learns what is or is not spam by referencing the highest scored non-spam emails. This learning tool is enabled by default and as the number of email messages filtered increases, so does the accuracy of VisNetic Anti-Spam. Also included is a utility that allows administrators the ability to designate good and bad (spam) messages and then instruct the learning mechanism to utilize them.

Permission-based Email

VisNetic MailPermit's challenge-response system checks the From and To address combination on each email. If the unique combination has never been encountered (i.e. this is the first time this sender has emailed this recipient), VisNetic MailPermit immediately dispatches an email or permission slip to the sender requiring him to go to a URL and perform a task that can only be completed by a human being.

When a challenge is issued, the sender's original email is placed in a pending file stored and available for review at the user (recipient) level. Once the sender responds to the challenge, his original email is delivered to the recipient and all subsequent emails from this sender to this recipient will be delivered without delay.

If the sender never completes the challenge, the email is automatically deleted from the pending folder after a specified period of time. At any time, the recipient may access his or her pending folder via a simple web interface and manually approve or reject email.

How does it work?

Upon receipt of each email, VisNetic MailPermit verifies that the intended recipient is a valid user on the mail server. If the recipient is not a valid user, the email is rejected. The From address on email sent to valid users is subsequently verified against whitelists and blacklists established in VisNetic MailPermit, starting with lists defined at the agent level, then domain and system level. Mail from whitelisted addresses is forwarded directly to the mail server. Mail from blacklisted addresses is deleted.
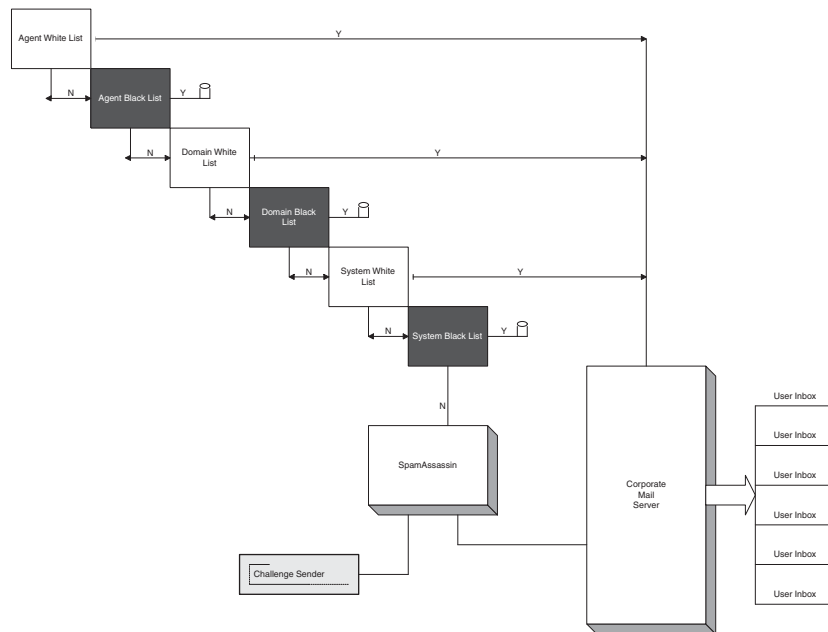
If the From address does not exist on a whitelist or blacklist in VisNetic MailPermit, the email is passed to VisNetic AntiSpam, a rules-based filtering tool powered by SpamAssassin technology. VisNetic AntiSpam assigns a numerical value or score to each message based on the likelihood that it is spam.

- ❑ Email receiving a score of 2* or less has a low likelihood of being spam and is forwarded to the mail server for processing.

- ❑ Email scoring 10 or greater has a high likelihood of being spam and is rejected.

- ❑ Email scoring between 2 and 10 is passed to VisNetic MailPermit's challenge-response system.

* These are default score thresholds. VisNetic MailPermit allows for user-definable thresholds at system, domain and user levels.

Additional Features

User-based Verification of Suspect Email

VisNetic MailPermit brings efficient spam management to the user level, reducing IT burden and increasing the accuracy of your anti-spam solution. Via a simple web interface, users may access email stored in their pending folder. This granular control ensures that legitimate emails are never lost and protects IT administrators from a stream of employee inquiries about missing email.
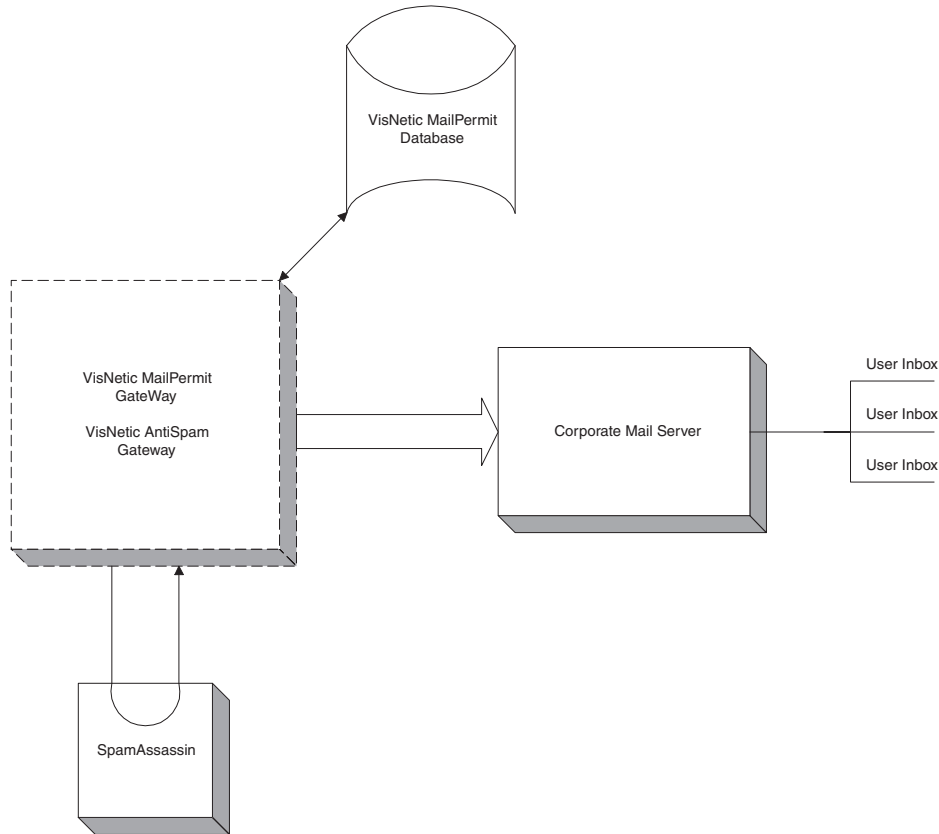
Aliases

VisNetic MailPermit features support for aliases. This means that each unique sender must complete the verification step, granting himself permission to email a recipient on your mail server, only once. For example, the first time Joe S. (joes@hisdomain.com) emails John B. (johnb@yourdomain.com) he will be issued a permission slip and must complete the challenge. Once Joe completes the challenge, his email is delivered to John instantly. All subsequent email from Joe S (jsmith@hisdomain.com) will automatically be delivered to John B. at this address and any one of John's aliases on your mail server-- johnb@yourdomain.com, john.brown@yourdomain.com, jbrown@yourdomain.com.

Flexible, Web-based Administration

The VisNetic MailPermit system administrator controls system, domain and user level settings and determines login rights for domain administrators and users. If granted access, domain administrators can maintain settings for their domains and users can modify their individual settings. This flexibility allows for more granular control, benefiting users by allowing them more control over inbound email and IT personnel by reducing their spam management burden. For the most accurate filtering, user-level whitelists take precedence over domain and system whitelists and blacklists.whitelists and blacklists.

VisNetic MailPermit
Database

VisNetic MailPermit
GateWay

VisNetic AntiSpam
Gateway

Corporate Mail Server

User Inbox

User Inbox

User Inbox

SpamAssassin

❑ **Take control of mission critical email**

Rather than outsource anti-spam to an ASP or third party vendor, VisNetic
MailPermit interoperates with your corporate mail server to identify and overcome
spam.

❑ **Secure email messages**

Unlike outsourced solutions, VisNetic MailPermit helps to ensure the security of your
mission-critical business email correspondence by keeping the process under your
direct control.

❑ **Control the availability of your service**

Hosted locally with minimal initial configuration and no ongoing routine
maintenance, VisNetic MailPermit is as reliable and available as your own mail
server.

Licensing and Availability

Initially, VisNetic MailPermit will be available as a plug-in to VisNetic MailServer. A Gateway for SMTP version for use with any SMTP server will be released next. Anticipated public availability for both is August, 2003.

License sizes for the plug-in include a 6-49 user license and a 50-unlimited user license. Gateway licensing will simply include a single domain license and a multiple domain license. Prices start at $99.95 US for the plug-in and $499.95 US for the Gateway.

Contact

Deerfield Communications, Inc.

P.O. Box 851. Gaylord, MI 49735

Telephone 989.732.8856

Fax 989.731.9299

www.deerfield.com

sales@deerfield.com

feedback@deerfield.com