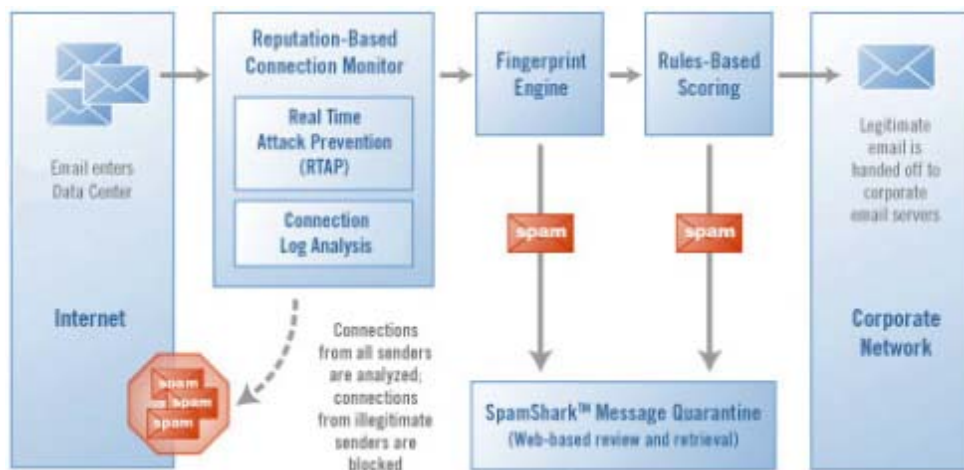




ANS Spam Plus Hassle-Free, Automatic & Accurate

Unwanted email (spam) has evolved from simply being a nuisance to become a significant problem, especially for businesses. Spam affects employees' productivity, it introduces potential legal liability, and there are real costs to the recipients and their corporations. By some estimates, the amount of spam will triple over the next few years. ANS has seen a 1600 percent increase in spam volume since we began managing email for customers in 2000.

ANS Spam Plus, powered by FrontBridge, has distinguished itself as a leading remedy for eliminating spam in the enterprise, winning the eWEEK Labs Analyst's Choice Award in eWEEK's July 14, 2003 edition. ANS Spam Plus leverages the benefits of our network architecture, ensuring that filtered messages are delivered reliably and securely. The following diagram illustrates how the system works:



ANS Spam Plus utilizes three layers of protection to analyze each piece of email and to detect and act on suspected spam.

Blacklisting: ANS uses a proprietary blacklist. We do not use commercial blacklists such as MAPS and ORBZ/S. Most commercial and public blacklists follow a "guilty until proven innocent" approach, which frequently blocks email from legitimate senders. Our blacklist contains only the addresses of the most egregious spammers on the Internet. While conservative, our blacklist can immediately block nearly 10 percent of our customer's inbound spam.

Fingerprinting: Messages not blocked by blacklisting are fingerprinted to detect matches with known spam message characteristics. ANS's fingerprinting technology leverages knowledge gained from filtering mail for our entire customer base. The fingerprinting database aggregates data from all spam blocked by our system allowing the fingerprinting process to become more intelligent and refined as more mail is processed.

Messages identified as spam are fingerprinted and given a unique id based on their content. If these messages come through our system again, the fingerprint is detected and the message is marked as spam.

Messages are analyzed to determine new spamming methods (i.e., base64-encoded spam). Once determined, a dedicated spam team modifies our scoring layer on the fly to catch spam using the same method.



ANS Spam Plus **Hassle-Free, Automatic & Accurate**

Rules-based scoring: Scores are assigned to messages based on more than 20,000 rules that embody and define characteristics of spam and legitimate email. Points are added to the score if a message contains characteristics of spam; and points are subtracted if it contains many characteristics of legitimate email. When a message's score reaches a defined threshold, it is flagged as spam. Message characteristics we evaluate and score include:

- Phrases in the body and subject of the message
- Formation of headers (i.e., Message-ID, Received, random characters)
- Originating mail server / Originating mail agent
- From and SMTP From address

Spam Treatment

Most customers choose to quarantine messages identified as spam outside their network. Quarantined messages are stored and deleted after 15 days. Customers can review quarantined messages and retrieve improperly blocked messages through SpamShark, a Web-based tool.

Unlike most competitors, ANS Spam Plus has a very low incidence of blocking legitimate email - less than one for every 250,000 emails received (less than 0.0004 percent).

As an alternative to quarantining messages, ANS Spam Plus also allows spam to be sent through to customers. When ANS Spam Plus forwards spam, it can modify the message to flag it for internal review. Modifications can include:

- Inserting an X-header for filtering inside the perimeter
- Inserting a new subject line message (i.e., < This is spam >)
- Directing spam to an internal SMTP mailbox

Benefits

Automatic spam filtering – No user interaction is required; and it is not necessary to set up of individual accounts

Highly accurate filtering – Legitimate business email is not blocked.

No white listing – Highly granular and accurate spam filtering technology eliminates the need to white list approved mail senders.

Hassle-free quarantine – Spam quarantined in SpamShark can be reviewed through the Web-based SpamShark interface; quarantined spam automatically expires after 30 days and is deleted.

Improved network efficiency – Eliminating spam outside your network reduces the load on mail servers and results in network usage and storage savings.

Contact us today at 330-645-4266 or email us at sales@anscorp.com to learn more about ANS Spam Plus.