Spam Filtering Service

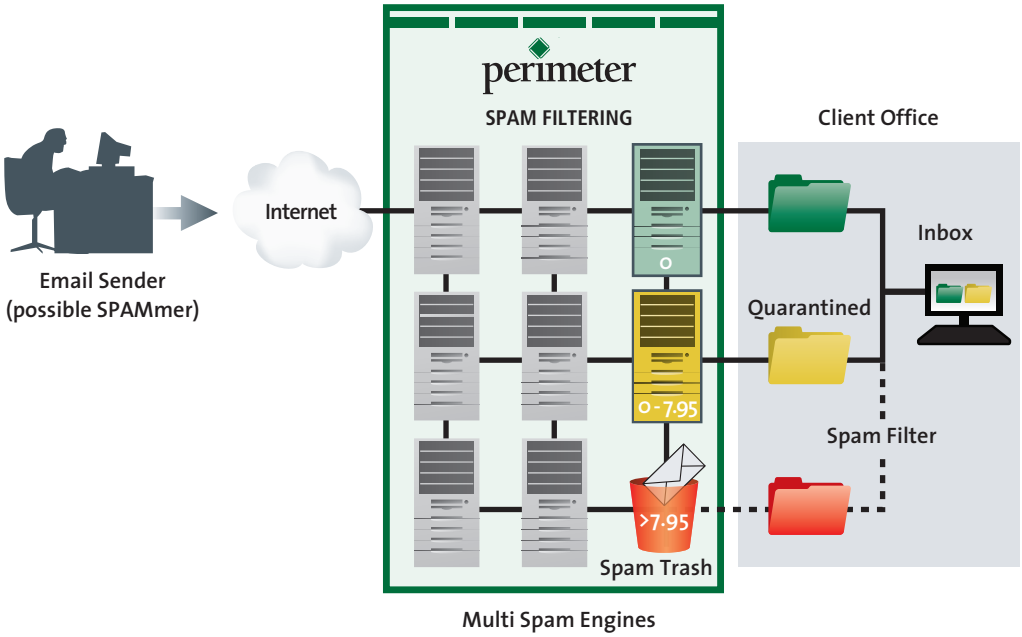
THE PROBLEM OVERVIEW

Perimeter's Spam Filtering service addresses significant problems associated with unwanted incoming email:

- Huge volume of SPAM overwhelming users' inboxes with emails that have to be directed to collection folders by email client software or manually deleted
- Emails that can distract employees from productive work or manipulate employees into behavior that can cause corporate reputational damage, legal liability, or security threats

Perimeter's SPAM-filtering service "pushes" all incoming email through a multi-layered SPAM filtering system that blocks, identifies and/or quarantines inbound SPAM or potential SPAM. This processing takes place outside your network, reducing network traffic and email server processing. Since most known SPAM email is blocked before it reaches your network, your users experience a significant reduction in unidentified SPAM that they must sort through and delete in their inboxes, and thus a significant increase in daily email productivity.

Since Perimeter is a fully-managed service, implementation of the SPAM Filtering service requires only that you make a simple change to the MX record for your domain. There is no interruption in your email services during the implementation period. There is no software or hardware required. Once the MX record change is made, email will start flowing through the Perimeter security infrastructure where each message is inspected by our multi-layered SPAM filters. Clean email is delivered to your email server, and identified SPAM is deleted, tagged or quarantined depending on your preference.



perimeter eSecurity™

Complete. On Demand. Affordable.

perimeter eSecurity™

Complete. On Demand. Affordable.

THE PERIMETER SOLUTION

Perimeter's SPAM Filtering service starts blocking known SPAM and black-listed domains to drop emails before they get to your inbox. Then we apply the white and black lists created by our customer. The SPAM service applies hundreds of filters and algorithms, including Bayesian statistical inference methods, to calculate a SPAM score for each email. SPAM scores range from 0 (unlikely) to over 8 (very likely). You have the option to configure your level of SPAM delivery by determining what gets deleted, quarantined, tagged or delivered without tagging. These four levels determine how emails are sent to individual employees. The quarantine level provides a method to hold all SPAM messages with a specific score range on Perimeter's SMTP platform. System administrators can access the quarantine and release emails they choose. In addition, you have the option to provide employee access to the corporate SPAM quarantine, where each employee would see their own list of SPAM emails and can take action for themselves.

THE BENEFITS OF PERIMETER'S SOLUTION

Key Features	Benefits
Multi-layered Protection • Domain Black List • Lexical Analysis • Bayesian Algorithms	Significant increase in accurate identification of SPAM
Multiple SPAM Processing Options • Delete or Release • Quarantine or Tag & Deliver	Significant reduction in quantity of SPAM
Unwanted Emails Dropped at Gateway	Increased server and network efficiency
Implementation with MX Record Change	Immediate productivity increase upon easy service deployment
Online Web Portal	Ability to view system status any time and anywhere you have an internet connection