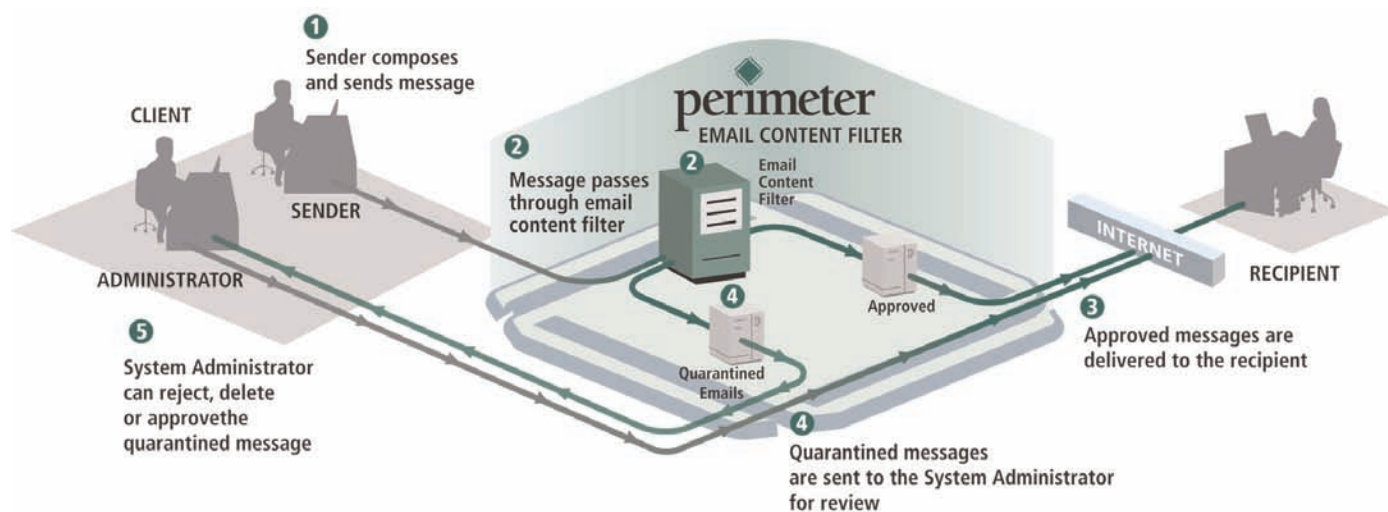


Email Content Filtering Service

Service Overview

Although the use of email technology has changed the way companies do business, it also brings with it many potential risks. Without visibility and control over the information leaving corporate email networks, organizations risk legal liability, regulatory violations and penalties, abuse of email resources, competitive threats and loss of priceless information – all resulting in significant costs and exposure. Enforcing an organization's Acceptable Use Policy with regard to email can be difficult without the right solution. At Perimeter, we make it easy to implement and manage corporate communications policies that protect against these threats. By utilizing our Email Content Filtering Service, organizations can enforce communication policies that ensure compliance with government regulations (GLBA, HIPPA, SOX) and defined corporate policies, reduce legal liability by identifying risky language, protect confidential information from leaving the network, and cut operational costs by reducing the need for manual review and auditing.

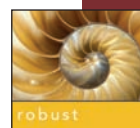
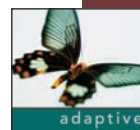


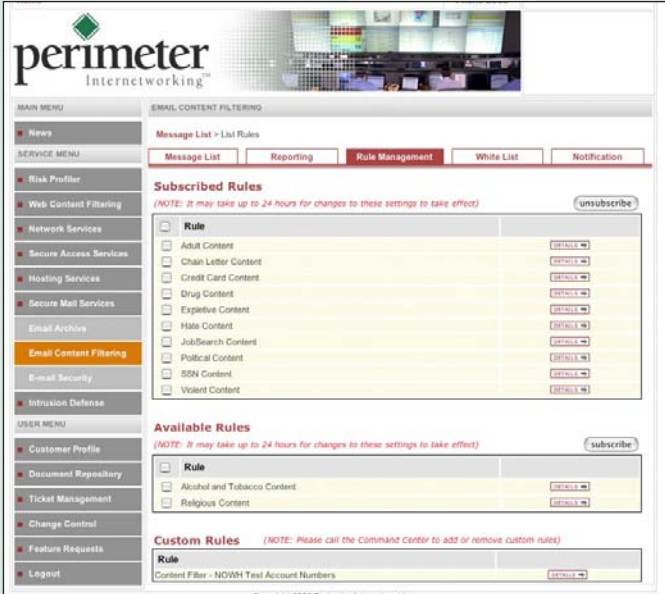
Service Highlights

Perimeter's Email Content Filtering Service scans your outbound email communications including attachments for certain criteria set forth by your organization. The engine automatically identifies emails that do not meet your organization's policy and the emails with violations are quarantined, processed based upon handling rules, and then delivered or returned for modification. Administrators have flexibility in establishing the criteria, determining handling procedures and establishing custom rules. The client also has the ability to view summary reports, and subscribe to or unsubscribe from standard rules through the online portal.

Key Features & Benefits

Feature	Benefit
Scans email for SSN, CCN, and custom numbers	Prevents inadvertent or intentional loss of confidential or non-public information.
Scans email for inappropriate words & phrases.	Protects company from legal liability and damage to reputation caused by offensive language.
Administrator can set options for notification	Provides flexibility in timing of notification.





Email Content Filtering Rule Management page in Viewpoint portal.

Problem Addressed

Perimeter's Email Content Filtering Service helps organizations implement company policies associated with compliance, liability, reputation, and protection of confidential information:

- Intentional or unintentional communication of company confidential and non-public information.
- Communication of inappropriate information or language exposing the company to legal liability and damage to reputation.

Technical Overview

Perimeter's Email Content Filtering Service scans and filters all outbound email for categories of words, phrases, and numbers using dictionaries and rules preset according to best practices. Categories can be turned off and on, rules can be modified, and dictionaries can be added to or modified according to an individual company's policies. When a rule violation is detected, the specific email is quarantined by reason – word/phrase, number or custom rule. Then according to the handling policy set for the user that sent the specific email, the administrator has the ability to either approve the email for delivery, return to the user for modification with violating information highlighted (optionally copied to others for internal review), or delete the offending email. Management reports are compiled by period (this month, last month, year-to-date, all time) and summaries by rule violation, offenders, and message volume are available.

Categories/Types Scanned Including:

Words/Phrases

Numbers

Adult	ATM/Client Card
Alcohol/Tobacco/Drugs	Bank Account
Confidential (Custom)	Credit Card
Gambling	Patient Identifier
Hate Speech	Social Security
Violence/Weapons	Trade Account

Known Dependencies/Limitations:

Company's outbound mail traffic routed to Perimeter

ECF service is hosted in Perimeter's NOC.

All SMTP traffic requires authentication for relay outside of Perimeter's network

