

Proofpoint Email Firewall

First Line of Defense Against Spam and Malicious Connections

Proofpoint Email Firewall™ provides enterprise-grade, real-time content filtering for email. Whether deployed on-premises or in the cloud, Proofpoint includes powerful email firewall and email policy enforcement features (included as part of both the Proofpoint Enterprise Privacy™ and Proofpoint Enterprise Protection™ Suites).

About Proofpoint Email Firewall

An integral component of both Proofpoint Enterprise Suites, Proofpoint Email Firewall detects sensitive information in message content and subject line.

Proofpoint Enterprise Privacy Suite

- Email Firewall
- Regulatory Compliance
- Digital Asset Security
- Encryption

Proofpoint Enterprise Protection Suite

- Dynamic Reputation
- Email Firewall
- Spam Detection
- Zero-Hour Anti-Virus
- Virus Protection

Proofpoint Email Firewall

Proofpoint Email Firewall allows enterprises to define and enforce acceptable-use policies for message content and attachments. A convenient point-and-click interface simplifies the process of defining complex rules related to file types, message size and message content. These features can be used to identify and prevent a wide variety of inbound and outbound policy violations, including offensive language, harassment, file sharing and many more.

Proofpoint Email Firewall	
Feature	Benefit
Connection-level defense	Serves as a first level of defense against email-borne threats and malicious connections
Message abuse prevention	Prevents message abuse by supporting advanced features, such as attachment scanning and verification, support for custom or proprietary document types, and message disposition flexibility
Meet corporate requirements	Quick creation of default and custom acceptable-use policies, giving administrators a powerful and rapidly deployable policy enforcement tool to quickly deliver on unique corporate requirements
Localized policy enforcement	Enables enforcement of policies in multiple languages, thereby developing policies unique to a geography or language

Connection-level defense

The Proofpoint Email Firewall provides a stateful, first line of defense against spam and malicious connections by testing numerous connection-level data points including DNS, MX record verification, sender policy framework (SPF), recipient verification and Proofpoint Dynamic Reputation (included in the Proofpoint Enterprise Protection Suite) data.

Acceptable-use policies

The Proofpoint Email Firewall includes common filters and standard dictionaries to quickly establish corporate messaging policies or support existing policies, giving organizations an immediate benefit in proactively controlling the most frequently encountered issues with messaging abuse.

Proofpoint Email Firewall

Key messaging analysis functions provided by the Proofpoint Email Firewall include:

- **Policy definition:** Easily define a specific set of policies for different groups, email routes and compliance areas. The Proofpoint Enterprise Suites provide a 100% web-based, graphical user interface for managing all types of messaging policies and simplifies the process of defining complex logical rules.
- **Real-time monitoring:** Monitor inbound/outbound email message flow, including attachments, for compliance throughout the enterprise.
- **Enterprise classification:** Filtered messages can be categorized into any number of compliance or content-related classifications.
- **Flexible message handling options:** Proofpoint Email Firewall rules allow organizations to take action on messages that violate policies. For example, any suspected or noncompliant email is flagged and can be quarantined for further review or audit before exposing the company to any liability.

Meet internal policy requirements

Proofpoint Email Firewall rules can compare message content with dictionaries in order to protect businesses from the use of inappropriate or offensive content and other issues that can surface through email usage. A variety of built-in dictionaries are supplied with Proofpoint Email Firewall, such as an offensive language dictionary that can be employed to discourage the use of improper or abusive language.

Unique customized policies

In situations where Proofpoint Enterprise Suites' preconfigured dictionaries do not meet a company or department's needs, custom dictionaries can be created to manage specific policies. In addition, pre-existing databases can be imported to leverage policies and information already used elsewhere in an organization.

Custom policies are easily created using a graphical user interface, which allows messages to be analyzed and processed, based on a comprehensive list of message attributes:

- **Attachment attributes:** File size, filename, file extension, number of files, number of files in archive, file depth in archive, presence of protected files and presence of corrupt archives.
- **Message attributes:** Text in message body, dictionary scores, message size, presence of encryption, MIME type and HTML tags.
- **Message header, envelope and routing attributes:** Email headers, envelope recipient, envelope sender, sender hostname, sender IP address, recipient, number of recipients, DNS block list status, message route (e.g., inbound or outbound) and more.
- **System attributes:** Total concurrent connections, total connections, and total messages.
- **Recipient group membership:** Different policies can be defined and enforced for different groups of users or domains. As with all of Proofpoint's policy enforcement features, policies can be defined at the global, group or individual end-user level.

Attachment scanning and support for custom or proprietary document types

Built-in attachment scanning capabilities allow organizations to apply Proofpoint Email Firewall policies to the contents of message attachments. Policies can be enforced on content in more than 300 types of attachments, including word processing documents (such as Microsoft Word), spreadsheets (such as Microsoft Excel worksheets), Adobe Acrobat PDF documents, presentation formats (such as Microsoft PowerPoint) and documents included in archives (including ZIP, GZIP, TAR, and TNEF formats).

Apply multi-lingual policies

Proofpoint Enterprise Suite's policy and content scanning engines detect and 'understand' text in any language, including multi-byte languages. Acceptable use policies can match non-English keywords and dictionary terms written in international character sets including Japanese, Chinese and Cyrillic.

About Proofpoint

Proofpoint focuses exclusively on the art and science of cloud-based email security, eDiscovery and compliance solutions. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against spam and viruses, safeguard privacy, encrypt sensitive information, and archive messages for easier management and discovery. Proofpoint's enterprise email solutions mitigate the challenges and amplify the benefits of enterprise messaging.

Proofpoint, Inc.
892 Ross Drive
Sunnyvale, CA
94089

1.877.647.6488