

email Security & Archiving delivered by ScanSafe, powered by Postini (a Google Company)

Contents

email Security & Archiving delivered by ScanSafe, powered by Postini (a Google Company).....	1
Management Overview	2
Technical Overview	3
Connection Manager	3
Filter Manager	3
Delivery Manager	4
Populating email Accounts	4
Resiliency and Continuity.....	4
Archiving.....	5
Service Description	6
Spam Filtering.....	6
Real-Time Virus Protection.....	6
Connection Manager with Threat Detection and Blocking	6
Delivery Manager with Throttling and Load Balancing	6
Event-Based Alerts	6
Real-Time Monitoring and Reports	7
Inbound Content Filtering	7
Inbound Attachment Filtering	7
Content and Transport Heuristics.....	7
Quarantine Summary Email (Sent to End Users).....	7
Outbound Content Filtering	8
Outbound Attachment Filtering	8
Outbound Virus Blocking.....	8
Outbound Compliance Footer	8
Basic Transport Layer Security	8
Directory Synchronisation (Directory Synchronisation Activation).....	8
Disaster Recovery (Disaster Recovery Upgrade may be purchased	8
Pricing	9
Disclaimer	9

Management Overview

The ever increasing importance of email to businesses and the ever increasing threats to the service have resulted in a great deal of focus on how best to manage this critical resource. According to a number of organisations dealing with inbound traffic from the Internet, over 90% of all emails are spam, some of which include a variety of viruses, graphics images and 'phishing' attempts. Stopping spam from entering the customer's corporate system reduces the bandwidth requirements and can significantly reduce the storage requirements for unwanted email.

There are two approaches to solving the problems: firstly an appliance based solution requiring hardware and software to be implemented and maintained in-house; secondly a Managed Service which intercepts email before it gets to the intended receiving system.

Because of the surges that occur within the Internet relating to spam and other forms of attacks, plus the potential growth of the number of email users within the customer, appliance based solutions may require upgrading from time to time. The Managed Service from ScanSafe guarantees no loss of emails nor degradation of service regardless of what is happening in the Internet or the growth in the customer's user base.

The guarantees that can be made when a customer takes on this service are:

- 100% virus elimination
- 98% spam blocked
- 0.0003% false positives
- 99.999% availability
- 100% delivery assurance
- 100% real time control
- Maximum of 60 second latency for delivery of email

The flexibility of the service means that the management of the system can be centralised or distributed, the policy can be set globally, by group or at an individual user level and that all changes made are immediately effective.

A major business benefit of the architecture means that delivery is guaranteed from sender to receiver because there is no intermediate storing of the email within the managed service. This means that once the senders system has reported that the email has gone, it will have been received at the intended address. It will not be somewhere in between which can happen with systems that use a 'store and forward' architecture. There is one exception to this rule and that is an option for the managed service to enter 'spooling' mode should the customer's receiving server become unavailable. Enough storage is available to provide up to seven days worth of email in this event.

Technical Overview

Putting the control of email in 'the cloud' provides a number of advantages over an in-house design, but the advantages of the Postini service don't stop there. A key differentiator is the 'Pass Through' technique that this solution provides whereby emails are not stored on disk but are dealt with in memory in real time. In other words the service acts as a proxy, forwarding connection requests between the sender and the receiver, rather than storing the email and handling it as two separate transactions (receive from sender, send to receiver).

This 'Pass Through' architecture derives a number of advantages such as guarantee of delivery, minimal latency and fail-over of system without the loss of emails as they are not stored in any intermediate repository.

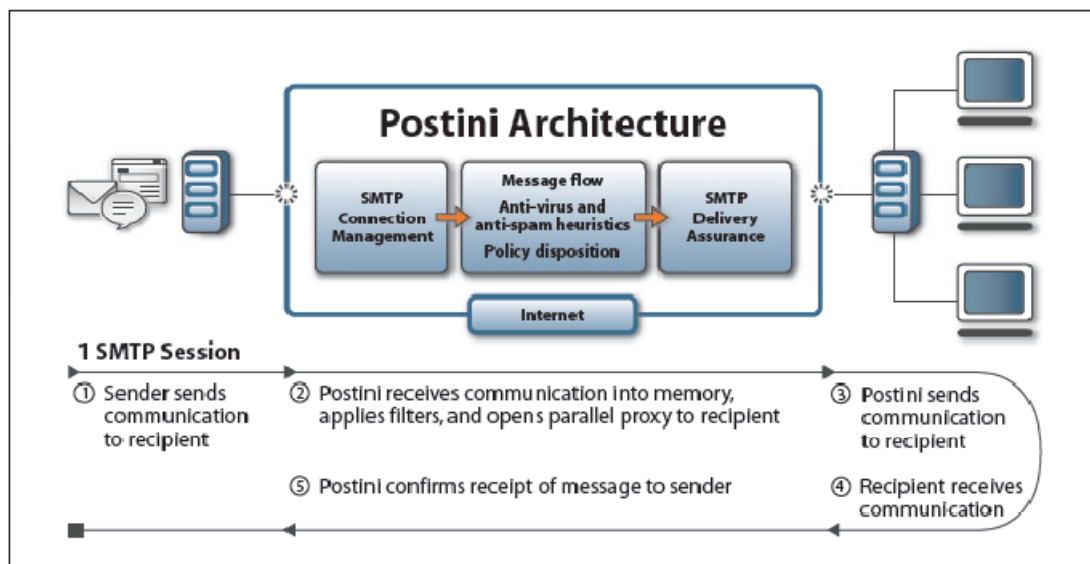


Figure 1 Service Architecture

Connection Manager

Shown in Figure 1, the front end of the service is the Connection Manager which monitors a number of pieces of information relating to individual IP addresses. By building up a state table over time, the connection manager can spot IP addresses that are sending out unwanted content and ultimately will refuse connection requests to these sites. Over 50% of emails are blocked from entering the system using this facility.

Filter Manager

Once the Connection Manager allows an email to progress through, the next stage of the process is the Filter Manager. This checks the email by passing it through two separate virus checkers, anti spam filters and checks the policy for attachments and lexical rules. The process takes from 50-150ms to complete and results in one of two actions. Either the email is allowed to be delivered or it will be sent to a quarantine area

where it is stored for up to 28 days. A notification is passed to the recipient at the customer that an email has been quarantined and is available for inspection.

Delivery Manager

If the email passes all the tests and checks, then it is allowed to complete delivery to the recipient and an acknowledgement of this completion is proxied through the system between recipient and sender.

A feature of the delivery manager is its ability to deliver to specific locations usually with knowledge of primary and secondary sites. This is advantageous to organisations that have multiple delivery points and back-up systems. Delivery locations are held for each individual email account providing very granular flexibility for managing any WAN configuration.

Populating email Accounts

There are a variety of ways for the email user information to be populated within the managed service. The most common way is to synchronise with one or more LDAP directories or Active Directories but for small numbers of users simply cutting and pasting the information is common. Once the user information is in place a hierarchical system of management is used to define policy, produce reports and manage quarantine. This provides the ability for an organisation to define multiple points of administration with defined limits of what the sub-administrators can see or do. For organisations with separate in-country IT management, this allows policy to be handled differently in accordance with local requirements and practices but governed by overall company policy.

Resiliency and Continuity

Postini has multiple pairs of data centres that act in active/passive mode and are configured such that each pair of processors within each data centre are only loaded to 40% of their capability. This means that any unexpected increase in workload will not overload an individual server and that all the customer configuration and policy information is replicated across servers and paired sites. As all connections are proxied live between sender and receiver, if a loss of service occurs during an email transfer then that email will remain 'unsent' by the sender i.e. no final acknowledgement will have occurred unless the email has been fully delivered. Once the secondary site takes over the email can be retransmitted.

Archiving

Legislation is forcing the hand of many organisations to record and maintain, for several years, all correspondence. With so many different forms of communications available both email and instant messaging are used as a matter of general business procedure. An additional facility available through ScanSafe is archiving. This allows archiving of all valid emails and can be applied to internal email through the use of the journaling facility. Storage times are for 10 years.

A key component of an archiving system is the ability to retrieve stored information easily and this is achieved by an advanced indexing system. Importantly, all information can be stored in immutable storage, making it valid for legal purposes.

Access to all stored material is fully configurable and carefully controlled.

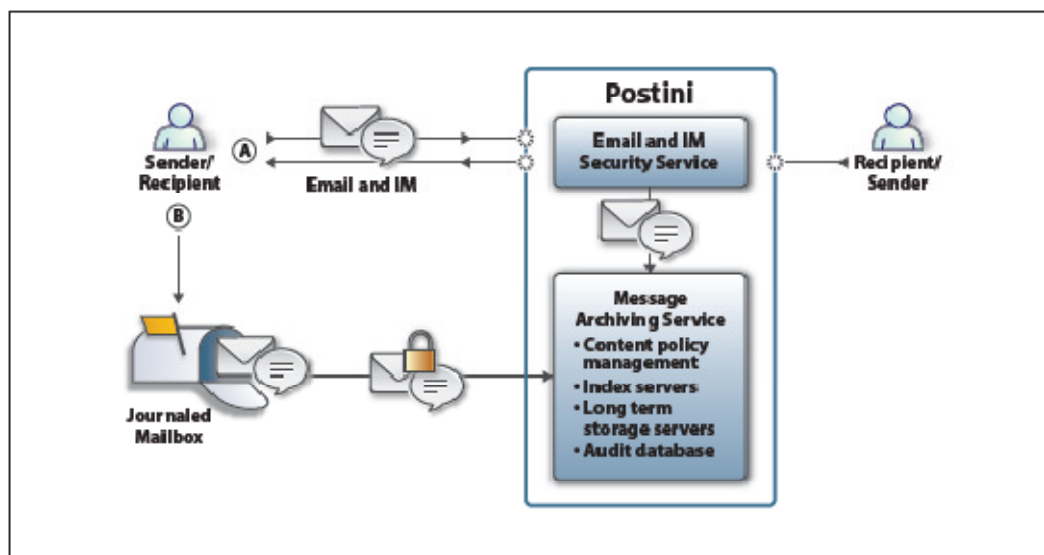


Fig 2 – email and IM Archiving

Service Description

This section provides a synopsis of the specific services that are provided through this managed service.

Spam Filtering

- Evaluates the components of each message to determine if the message is spam, using a heuristics-based anti-spam engine.
- Quarantines inbound email messages that may be spam, and makes these messages accessible to the individual user through the web-based Postini Message Centre (the "Message Centre") for review and disposition for a period of up to 28 days from the receipt of such email.
- Can be customised at an organisation and/or user group level, using the Postini Administration Console, including creating unique settings at the user group and/or individual user levels and establishing controls based on job function and responsibilities.
- Can be configured by individual users, who can specify their own filters, as permitted by the administrator.

Real-Time Virus Protection

- Evaluates the components of each message to determine if the message contains a virus using a heuristics-based virus engine.
- Quarantines inbound email messages that may be infected with a virus and makes these messages accessible to the individual user through the Message Centre for review and disposition for a period of up to 28 days from the receipt of such email.

Connection Manager with Threat Detection and Blocking

- Monitors SMTP traffic to identify patterns of behaviour that are associated with SMTP attacks, such as directory harvest attacks (DHA), denial-of-service (DoS) attacks and statistically significant spikes in spam or virus activity, and automatically rejects such attacks.

Delivery Manager with Throttling and Load Balancing

- Regulates the delivery of inbound email messages across destination servers regardless of operating system and/or geographic server location.
- Balances inbound email message load by automatically redirecting delivery of email messages to fail-over resources in the event a destination server becomes unavailable.

Event-Based Alerts

- Monitors status of inbound and outbound email traffic and notifies designated individuals within the organisation by email, telephone or pager during SMTP attacks and system outages.

Real-Time Monitoring and Reports

- Monitors status of inbound and outbound email messages and can provide usage reports on an hourly, daily, or weekly basis, as specified by the administrator.
- Includes usage audit record for policy enforcement and capacity planning.
- Makes reports available through a web interface or for downloading for further analysis and distribution by the administrator.

Inbound Content Filtering

- Allows an organisation to create and enforce email usage policies for inbound email messages using flexible content filters based on sender and recipient addresses, key words, and attachments.
- Allows an organisation to define content-based exceptions to spam filters.
- Allows an organisation to monitor email usage through a log of detailed filter activity.

Inbound Attachment Filtering

- Enables companies to block or re-route inbound email messages containing unwanted email attachments.
- Allows administrators to use productivity filters to create inbound email policies based on attachment type, such as music, sound and movie files.
- Allows designated senders, such as the customer's designated partners, customers, and associates, to bypass specified email policies through an optional "approved sender list" feature.

Content and Transport Heuristics

- Content Heuristics are designed to identify common traits and characteristics of the legitimate business email for specific industries and job functions, which can reduce the possibility of falsely quarantining legitimate email.
- Transport Heuristics are designed to identify communication networks by industry and job function and to authenticate inbound email from these networks, which can reduce the possibility of falsely quarantining legitimate email.

Quarantine Summary Email (Sent to End Users)

- Automatically alerts end users to the presence of messages in their personal quarantine areas with a Quarantine Summary email.

Outbound Content Filtering

- Allows an organisation to create and enforce email usage policies for outbound email messages using flexible content filters based on sender and recipient addresses, key words, and attachments.

Outbound Attachment Filtering

- Enables companies to block or re-route outbound email messages containing large or harmful email attachments.
- Allows administrators to use productivity filters to create outbound email policies based on attachment type, such as music, sound and movie files.

Outbound Virus Blocking

- Scans outbound email messages for virus and blocks these, which can assist the customer in protecting recipients of its email from viruses.

Outbound Compliance Footer

- Creates a standard organisation-wide email compliance footer to be automatically inserted into all outbound email messages.

Basic Transport Layer Security

- Basic Transport Layer Security allows inbound messages to the Postini system and outbound messages from the Postini system to be encrypted with the standard email encryption protocol TLS. In order for messages to be encrypted, the customer is responsible for ensuring that the email servers that are sending messages to the Postini system and receiving messages from the Postini system have TLS capabilities enabled.

Directory Synchronisation (Directory Synchronisation Activation Support may be purchased for an additional fee)

- Automatically synchronises the customer's enterprise directory with Perimeter Manager.

Disaster Recovery (Disaster Recovery Upgrade may be purchased for an additional fee)

- Spools inbound email continuously in the event of an outage of the customer's network or servers for the period of time that is determined by the number of Mailboxes/Units set forth in the Coverage Selection Sheet.
- Automatically delivers spooled email messages once the customer's mail server(s) and connection have been re-established, at a regulated rate to allow new inbound messages to be delivered concurrently.

Pricing

Pricing for the Managed Email Service is based on the number of committed email boxes that are required. Aliases are considered as one email rather than multiple email addresses. Additional email addresses identified through the running of the service will be notified to the customer and an additional charge made based on a pro-rata charge for the contracted period.

In comparing the cost of a managed service with running the service in-house there are many factors to consider, such as:

- Cost of hardware (multiple site instances may be required)
- Cost of software and any annually renewable charges
- Cost of external support and maintenance
- Implementation cost
- Upgrade requirements
- Failover and Disaster Recovery requirements
- Cost of providing and monitoring tight SLA's
- On-going training and internal support costs
- Server capacity for storage of inbound emails (inc spam)
- Replication of storage space for resilience and DR
- Cost of wasted bandwidth
- Downtime if in-house service is unavailable (loss of connection, server issues, scheduled maintenance etc)
- Remote support

Return on investment calculations will generally prove the case for a managed service, but the principle aim is to take away a growing, ongoing problem from the IT team. In particular, planning for increases in capacity requirements and second guessing the next level of threat are no longer required when using the managed service.

Disclaimer

Vioptim Ltd is not responsible for changes in the Postini service or terms and conditions that may impact the above information which is provided as a guide only. The Postini service, now part of Google, is delivered through ScanSafe and managed through ScanSafe's management portal. Terms and Conditions of any resulting contract will be those provided by ScanSafe