Product Overview

Revision 5

Version 3.0
20/06/2012

Product Overview
Revision 5 31/05/2011
Ref. 521-19

Table of Contents

Introduction

Secure Email Gateway

PSTmail is a system which allows the exchange of e-mail between two TCP/IP networks with various degrees of classification or security policies which would impede their connection through any other means. The two networks are not equivalent: one is considered to have a higher classification degree or security level. PSTmail guarantees the impossibility of any type of traffic between the two networks except the mail transferred by the system itself.

The system is exclusively administered from the securest network.

The supported email protocols are those which are standard in Internet: POP3 and IMAP4 for receiving and SMTP for sending. The gateway does not substitute the mail servers of the two networks but rather uses them as intermediary elements for sending and receiving the messages.

The mail enters a secure network in a transparent way for the users, even though filtering policies, conditional forwarding can be applied and it can be sent to various internal accounts.

The outgoing mail requires authorization by way of an electronic signature of each of the messages in order to leave the secure network.

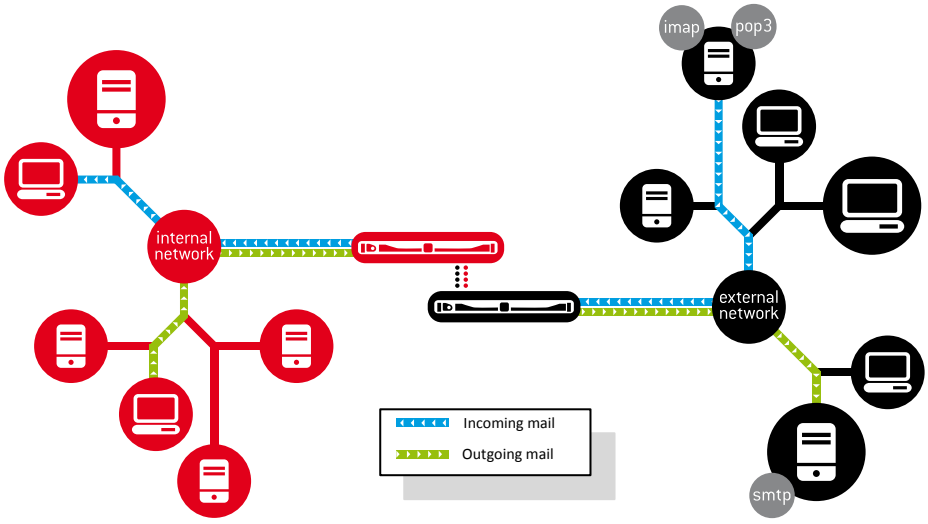

Figure 1. Secure Email Gateway

This Document

This document is intended to provide an overview of the product.

The product and its main functions are described in the first chapter.

The infrastructure required for operating the product is specified in the second chapter.

The subsequent chapters describe the different parts of the product (incoming mail, outgoing mail and administration) in greater detail.

Audience

The document may be used as an introduction to the product and its documentation.

It may also be used by anyone assessing the possibility of rolling-out PSTmail within a company or organization.

References

Throughout the document the following tags are used to indicate a reference to other documents.

[IG] Installation and Deployment Guide, ref 0521-14.

[OG] Operations Manual, ref 0521-15.

Glossary

CA Certification Authority

CN Common Name

1. PSTmail

The Product

The fundamental component of PSTmail consists of two computers called ‘units’. Each unit is connected to one of the networks. The one connected to the internal network is called PSTi and the one connected to the external network is called PSTe. These are dedicated computers; i.e. no software application is executed on them apart from those of PSTmail. They are supplied with all the required software installed.

- **PSTmail element**

  Each pair of PSTi and PSTe units forms an element. The element also includes the hardware device used for communication between the units.

  There are two possible configurations: standard –formed by an element– and high availability –formed by two elements in an active-passive redundancy scheme–.

The system is also formed by the following software components, which will run on general purpose stations or servers located on the internal network:

- **PSTadm**- Administration application

  The administration of the complete system is carried out from a station on the internal network. The unit located on the external network (PSTe) requires no administration.

- **PSTaud**- Audit records reception service

  Activity data (data of the messages transferred through the gateway) is recorded on a database separate from PSTmail. The job of PSTaud is to enter the data it receives from the internal unit into the database.

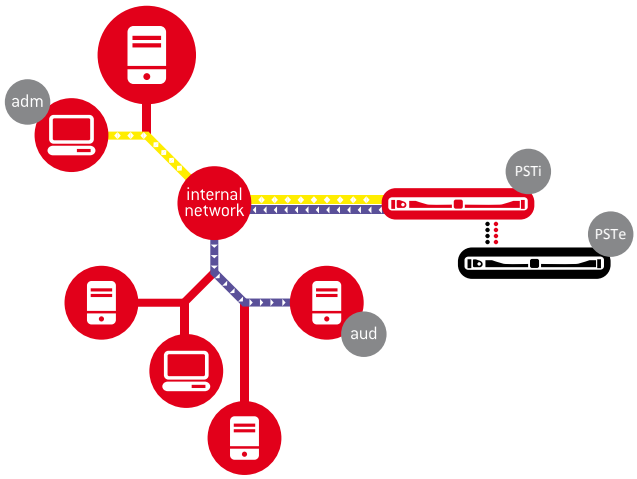

Figure 1.1. PSTmail Components

Incoming Mail

The gateway manages incoming mail transparently: it periodically checks the external network mailboxes which are configured, enters the messages it finds into the internal network and sends them to the destination accounts on the internal network which are established by configuration.

- Incoming mail channel

  This is the name given to the correspondence between an external network mailbox and one or more internal network mailboxes. The simplest case is for each user to have an account on each of the networks and hence for correspondence to be 1 to 1.

  There are also a number of parameters that can be individually specified for each channel, such as, a rejection filter and conditional forwarding.

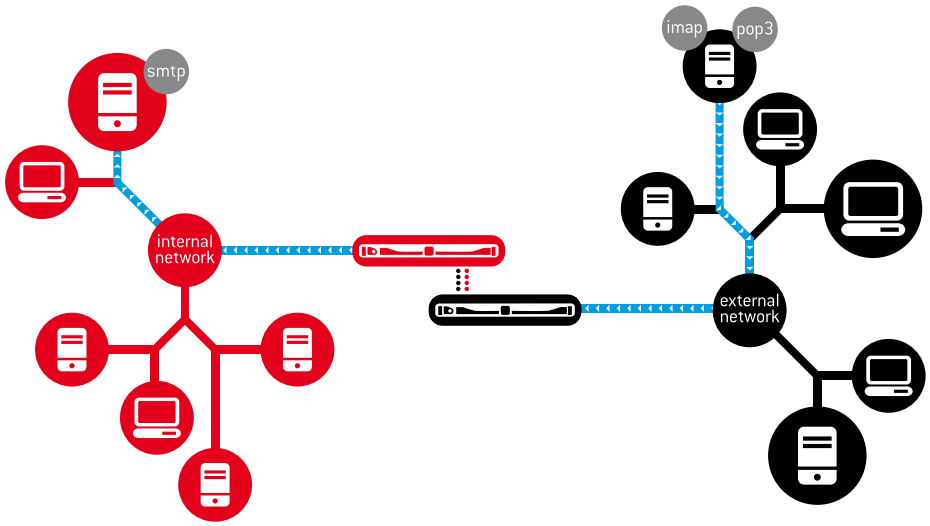

Figure 1.2. Incoming Mail

Outgoing Mail

All outgoing messages need to be authorized by digital signature. PSTi works as a mail server on the internal network and checks the digital signature of each message before sending it to its recipients on the external network.

It also deletes any internal network information contained in the message headers and permits basic filtering of the messages by format.

- Supervisor

  Users of the internal network entitled to authorize the sending of messages are called supervisors.

- Outgoing mail channel

A channel is characterized by the sender's address on the external network. Each channel is assigned a supervisor (or more than one) by configuration.

The filtering features, and other parameters such as the notification of messages sent, can be configured individually for each channel.

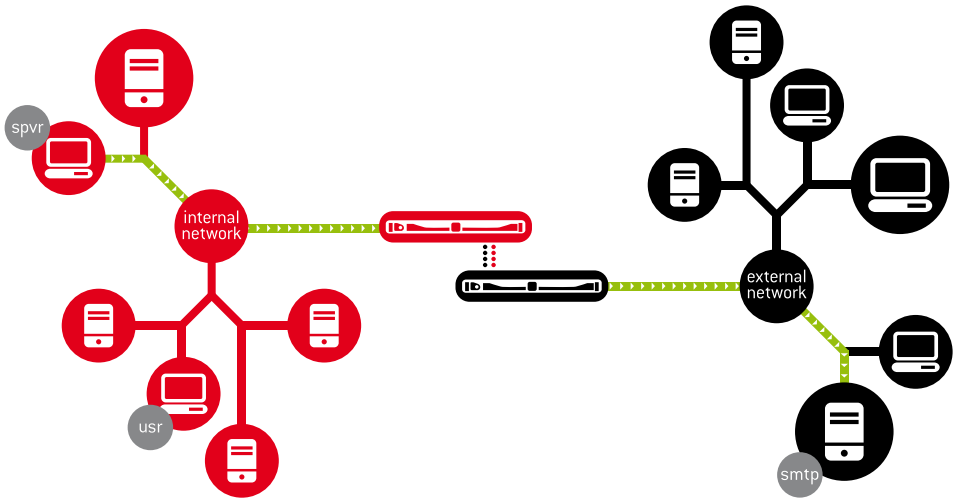

Figure 1.3. Outgoing Mail

Administration

Local administration is only performed with the system down. It is done on the internal units to establish a few initial settings that seldom need to be modified.

Administration takes place from a station on the internal network, through the PSTadm application, which connects via SSL to the internal unit, PSTi. The gateway also sends system events via the 'syslog' protocol to servers located on the internal network.

There are 4 different administration roles with their respective permissions. You can assign any roles you want to an administrator.

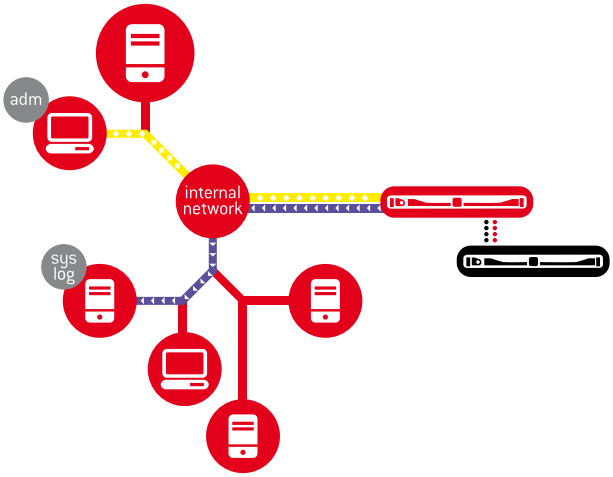

Figure 1.4. Administration

Auditing

Auditing is the recording of information about the transfers made by the system (e.g. messages sent to their recipients on the internal network).

The PSTaud software component, installed in a computer on the internal network, is responsible for entering these records into a database outside the system.

PSTi automatically connects to PSTaud via SSL.

For each service (incoming and outgoing mail), it is possible to configure whether or not auditing information will be sent and the level of detail of the same.

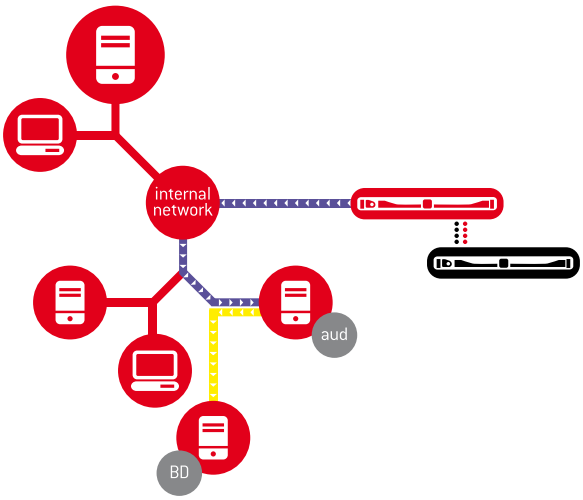

Figure 1.5. Auditing

Technical Features Summary

- Appliances - 19" rack mount, 1U high.

- Incoming mail transfer rate: 20.000 messages per hour.
- Outgoing mail transfer rate: 5.000 messages per hour.
- Maximum message size: 50MB

2. Infrastructure

This chapter is aimed at anyone intending to introduce or considering rolling-out PSTmail within a company or organization.

It includes a description of the infrastructure required in addition to the PSTmail units.

For more detailed information see [IG].

Hardware and Software

As described in the previous chapter, a scenario involving two networks, one of which is considered secure, is assumed. Email services are required in both networks using standard Internet protocols (SMTP for outgoing and POP or IMAP for incoming mail).

The following hardware and software are required for the internal network:

1. Gateway administration requires:
   - For installing PSTadm, a computer running the Windows XP SP3 (or higher) operating system is required. Various machines may be used for PSTadm but only one can be connected to the gateway at any given time.
2. For remote storage of security and operations events, the following equipment is required:
   - Depending on whether the security and operations events are stored together or separately, one or two 'syslog' servers are needed.
3. For remote storage of transfer records, the following configuration is required:
   - A computer running the Windows XP SP3 (or higher) operating system for installing the PSTaud service.
   - A database server accessible via an ODBC connection.

Public Key Infrastructure

A public key infrastructure is required to ensure gateway communications and outgoing mail authorization.

The necessary certificates and their features are described below.

Recipient	*Permissions*
PSTi	Certificate with SSL Server and SSL Client features.
PSTaud	Certificate with SSL Server features.

The private keys and PSTi and PSTaud certificates together with the certification authority (CA) certificate must be available during system installation.

Administrators and Supervisors

A certificate for each administrator and supervisor is required.

Recipient	*Permissions*
Administrator	Certificate with SSL Client features.
Supervisor	Certificate with S/MIME features.

Configuration

Minor changes to the configuration are needed for deploying PSTmail:

- The internal network SMTP server must be configured to resend mail to PSTmail in the following cases:

  1. Mail addressed to the external network.

  2. Mail for PSTmail addressed to a configurable address.

- If a rejection filter is used to resend rejected messages to the external network, one or more external network mail accounts may be configured to receive incoming mail that does not meet the defined rejection filter restrictions.

3. Incoming Mail Details

Configuration

A high level overview of the incoming mail service configuration is given in this section. For further details see [OG].

Basic infrastructure	External incoming mail server (POP / IMAP)
	Internal outgoing mail server (SMTP)
Input channel	External email address
	Internal email destination addresses
	Filtering
	Message forwarding
Advanced infrastructure	External outgoing mail server (SMTP), for sending rejected messages
	Server configuration by channel or channel group

Filtering

The rejection filter consists of checking a series of message format conditions. If a condition is not met, the message is rejected. Rejection may imply sending the message to an external account and sending a rejection notification to the channel recipients. The rejection filter is applied before the message is sent to the internal network.

Conditions can be applied to the following values:

- Limit for the total number of attachments and nesting levels (attachments within attachments).
- Total message or attachment size
- Total number of recipients
- Number of extensions for attachments

Forwarding to Other Accounts

Selection filtering consists of forwarding messages that meet certain conditions expressed as message field rules (sender, name and extension of attachments, subject,

etc.) to an internal network account. As many filters as needed may be configured; the first filter whose condition is met (if any) will determine the message destination address in the internal network. Selection filtering takes place in the internal network before sending the message to the internal recipients.

4. Outgoing Mail Details

Configuration

A high level overview of the outgoing mail service configuration is given in this section. For further details see [OG].

General	Internal domains from within which no information should leave the internal network
Basic infrastructure	External outgoing mail server (SMTP)
	Internal outgoing mail server (SMTP)
	Users
	Supervisors
Output channel	External email address
	Authorization address
	Default users for this channel
	Authorized supervisors
	Filtering
	Notify user and/or supervisor of messages sent
Advanced infrastructure	Server configuration by channel or channel group

Authorization

The following authorization conditions must be met in order for the gateway to send a message to external network recipients:

- The message must be signed correctly
- The key certificate used to sign the message must be included in the message and have been issued by a CA configured in the gateway
- The CN of the message signing certificate must be enabled for the channel through which the message will be sent

Purging Internal Network Information

All header fields, apart from those in the following list, will be deleted from messages. In addition, email addresses belonging to internal domains will be deleted from any remaining fields. Internal domains are specified in the configuration.

```
Bcc:
Cc:
Comments:
Content-Description:
Content-Transfer-Encoding:
Content-Type:
Date:
Disposition-Notification-To:
From:
In-Reply-To:
Keywords:
MIME-Version:
Organization:
Priority:
References:
Reply-To:
Subject:
To:
```

Filtering

Filtering consists of checking a series of message format conditions. If a condition is not met, the message is not sent.

Conditions regarding the following aspects can be imposed:

- Limitation of the total number of attachments and of the nesting level (attachments within attachments)
- Total message or attachment size
- Total number of recipients
- Number of extensions for attachments

User Message Output

1. The user can create the message using any standard mail client, add any required external network recipients and send the message.

2. PSTmail checks that the message has been sent by a defined user and that it meets the defined filtering conditions. If this is the case, the sender is replaced with the corresponding external sender and all internal network information is deleted from the message. The transformed message is attached to an authorization request message which is then sent to the configured channel supervisor mailbox.

3. The supervisor receives the authorization request and can inspect the message contents in the format in which it will be sent (the message is an attachment to the request message). To authorize sending the supervisor has to reply to the message and add their signature to the reply.

4. When the gateway receives a signed message, it checks the signature and ensures that the supervisor is authorized to send messages via that channel. It checks that the filtering conditions have been met and that internal network information cleansing has been performed correctly. If this is the case, the message is accepted for sending to the external network.

Supervisor Message Output

1. The supervisor can create the message using any standard mail client, add any required external network recipients, sign it and send it.

2. When PSTmail receives a signed direct message, it makes sure that it has been sent by a configured supervisor authorized to send mail via the requested channel and checks signature validity.

   A check is then made that the message meets the defined filtering conditions and, if this is the case, replaces the sender with the corresponding external sender, deletes all internal network information from the message and accepts it for sending.

Email Client Requirements

If a user wants to send mail using several accounts, a mail client that has a *Reply-To* field is required.

For supervisors, the mail client must support the S-MIME format and allow attachment of the original message to a reply.

5. Administration

‘Administration roles and permissions’ are explained in this section. For reasons of clarity, administration tasks have been divided into two parts: configuration and monitoring. In day-to-day administrative work, this differentiation is not as pronounced.

Administration Roles and Permissions

PSTmail classifies administration tasks into four different roles. No restrictions are placed on the roles that can be assumed by a single person, identified by their certificate. The roles and a summary of their permissions are described below:

- Root administrator (Root)

  Sets administration permissions for all other roles. ‘Root administrator’ permission can only be established locally in the internal unit when the system is not running.

- Security administrator (Sec)

  Defines the infrastructure configuration: 'syslog' and PSTaud servers and other parameters that affect their operation. Can obtain copies of security events files.

- Services administrator (Srv)

  Configuration and control (starting and stopping) of services. Can obtain copies of operation events files.

- Monitoring administrator (Mon)

  Can obtain information about the status of the general system and the configured services channels.

For practical reasons, it is recommended that security and services administrators are given monitoring administrator permissions as well.

Configuration

The configuration described below is performed remotely from an internal network machine using the PSTadm application.

On completing the deployment as described in [IG] including the installation of the software components PSTadm and PSTaud, the configuration described below must be carried out using the necessary permissions. This configuration must be completed before configuring the incoming and outgoing mail services; this configuration may be altered subsequently at any time.

Root Definition of permissions for the administration and restriction of IP’s from which administration is possible.

Sec Configuration of the 'syslog' infrastructure and related parameters.

Sec Definition of PSTaud connection data and related parameters.

The configuration of each service is described in the section corresponding to the service. Service administrator permissions are required to access these functions.

Monitoring

Monitoring administrator permissions are required to access the monitoring function.

General Status Monitoring

Gateway status monitoring is carried out from the main PSTadm window as described in [OG].

In the event of connection problems between units, connection problems with the audit server and the status of the secondary element for cluster configurations, information about the problem will be provided.

System events with ‘Global’ scope should also be checked in the 'syslog'.

Services Monitoring

Incoming and outgoing mail services are organized in channels; these channels share some common features, thus facilitating administration.

Common channel features

Status ON / OFF	Each channel can be turned on and off as required. If the channel is turned off, no service will be provided through it.
Priority	Three priority levels exist; the system assigns resources to the channel according to priority.
Group tags	Group tags can be allocated to a channel; these tags may be selected in the status display view.
State transitions and notifications	Channels follow a cycle of operational states. It is possible to configure individually some of the state transition conditions and the parameters for notifications using the system events caused by state transitions.