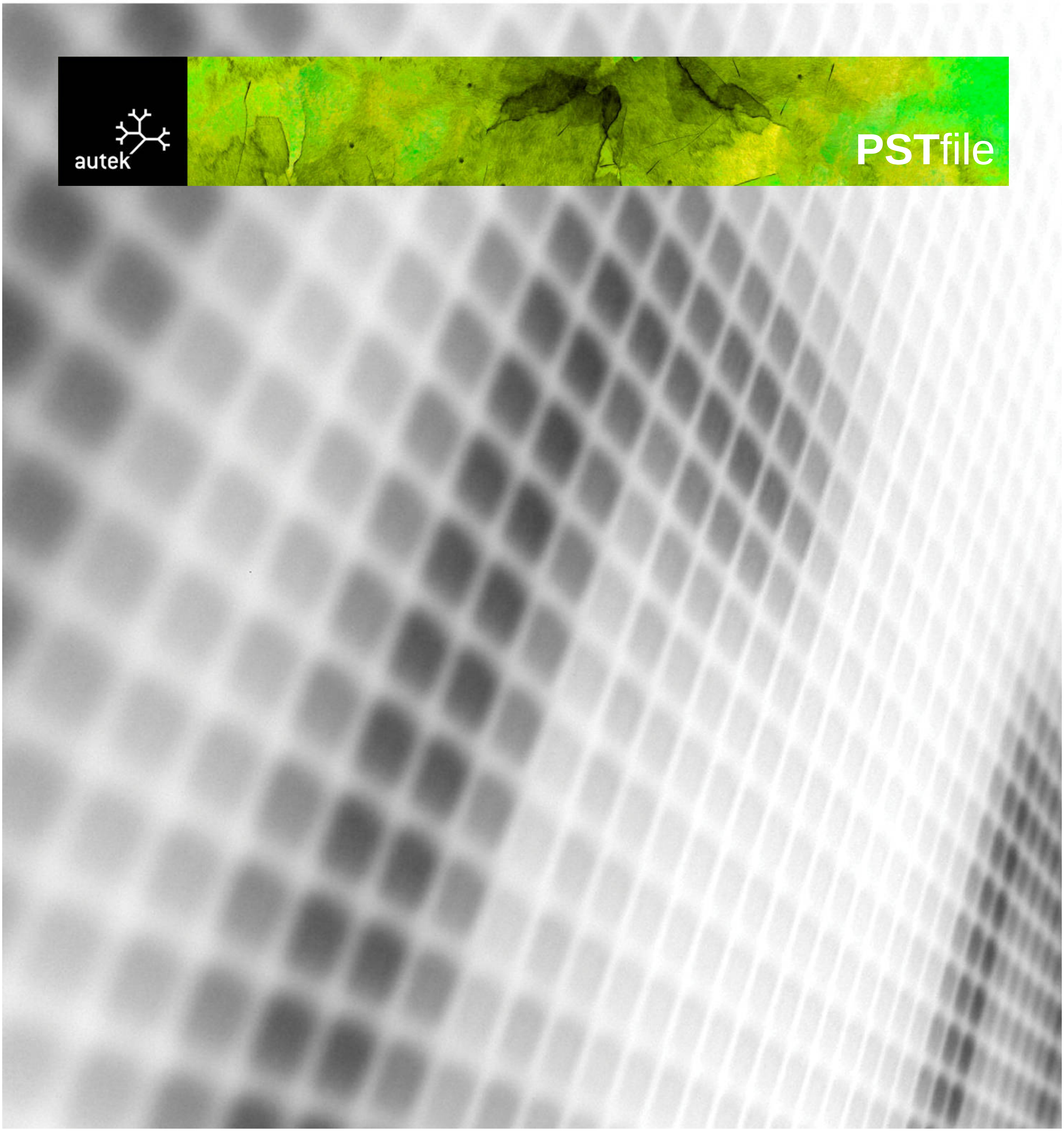

PSTfile

Product Overview

Revision 2

The authors of this document have been very careful in its preparation but we cannot offer any warranty or assume any responsibility for errors, omissions or damages resulting from the use of the information contained herein.

Autek Ingeniería, S.L.	**PST file**

Product Overview
Revision 2 27/06/2013
Ref. 545-19

Table of Contents

Introduction

Secure File Gateway

PSTfile is a system which allows the exchange of files between two TCP/IP networks with different 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. PSTfile guarantees the impossibility of any type of traffic between the two networks except the files transferred by the system itself.

The system is exclusively administered from the securest network.

PSTfile is one of the products of the **PSTgateways** family. All PSTgateways products share the same architecture which provides common administration and security infrastructure. Individual products differ in the supported data flows, called services.

PSTfile comprises two data flow services: **'Inbound File'** (IF) and **'Outbound File'** (OF) transfer services. The supported file transfer protocols are FTP, FTPS and SMB. The gateway does not substitute the file servers on the two networks but rather uses them as intermediary elements for sending and receiving the files. The gateway always plays the client role of the supported protocols. Both services work automatically once source and target have been configured. Their main difference is that outbound files must be digitally signed in order to be transferred by the system.

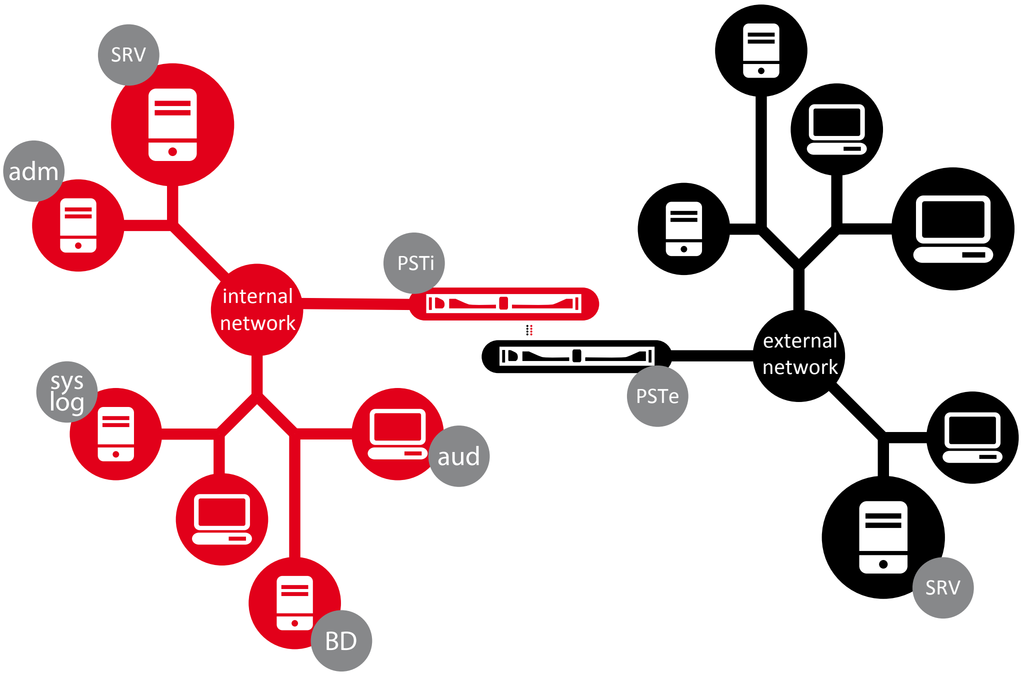

Figure 1. Secure File Gateway

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 (inbound and outbound file services and administration) in greater detail.

Audience

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

It may also be used by anyone assessing the possibility of deploying PSTfile within a company or organization.

References

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

[IG]	PSTgateways - Installation and Deployment Guide, ref 0550-1.
[OG]	PSTgateways - Operation Manual, ref 0550-2.
[PSTSIGN_UM]	PSTsign - User Manual, ref 0550-3.

1. PSTfile

The Product

The fundamental component of PSTfile consists of appliances 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.

- **PSTfile element**

  Each pair of PSTi and PSTe units forms an element. The element also includes the hardware device necessary 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-active 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**- Auditing records reception service

  Activity data (data of the files transferred through the gateway) is recorded on a database separate from the gateway. The job of PSTaud is to enter the data it receives from the internal unit into an external database or alternatively to text files.

  Alternatively, transfer data can be recorded to files on the computer where PSTaud is installed.

  The use of this component is optional but strongly recommended for security reasons.

- **PSTsign**- File sign application

  Windows shell extension application for easily generating detached signature files requiered by the 'Outbound File' service to transfer a file. A command line version is also included.

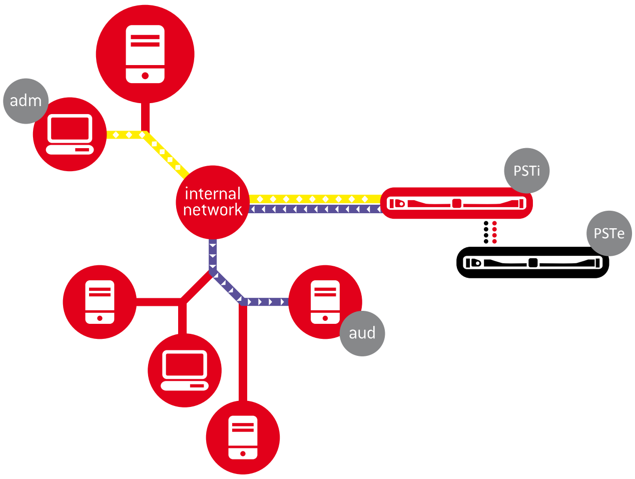

Figure 1.1. PSTfile Components

Inbound File Service

Inbound file transfer works automaticaly: the gateway periodically checks the external network folders which are configured, enters the files it finds into the internal network and sends them to the destination folders on the internal network which are established by configuration.

Inbound File Channel

This is the name given to the correspondence between an external network file server and an internal network one.

There are also a number of parameters that can be individually specified for each channel, such as priority, mirror or recursive mode.

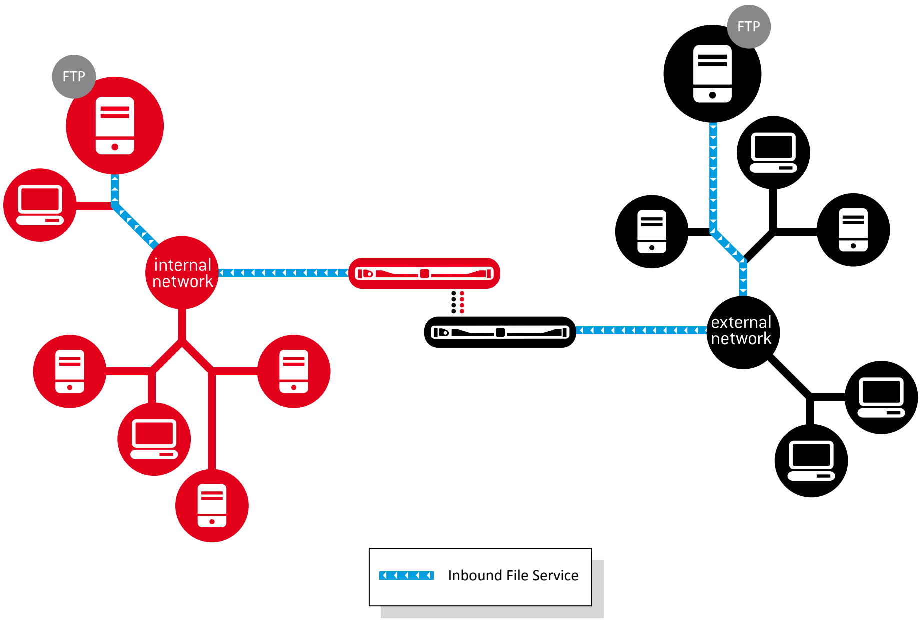

Figure 1.2. Inbound File Service

Outbound File Service

It works in a similar way as the inbound file service, with the source folder being on the internal network and destination folder on the external network. The big difference is that a digital signature is required for the files to be transferred.

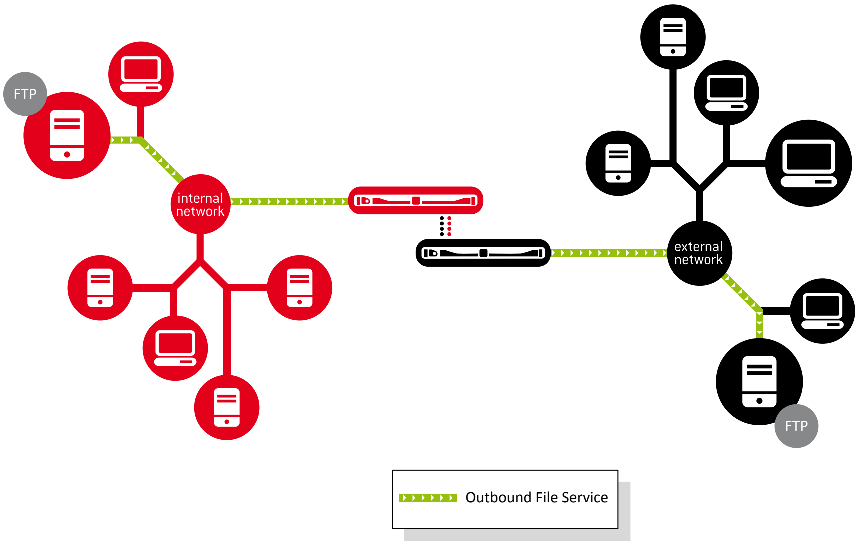

Figure 1.3. Outbound File Service

Administration

Local configuration 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.

Remote administration takes place from a station on the internal network, through the PSTadm application, which connects via TLS to the internal unit, PSTi.

There are 4 different administration roles with their respective permissions. Administrators are identified by means of digital certificates.

In addition, gateways send operation and security events through 'syslog' protocol to the internal network servers configured.

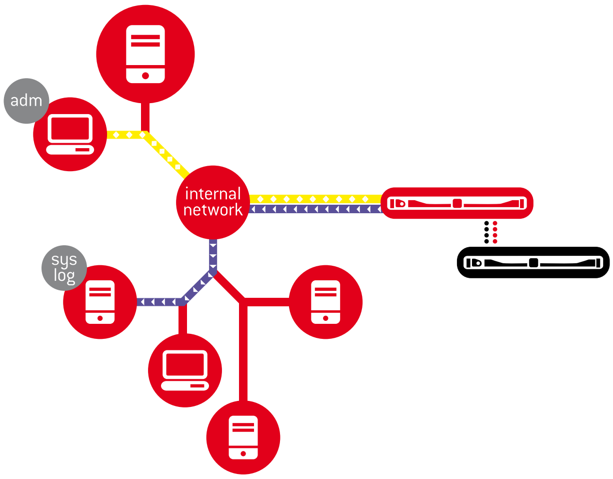

Figure 1.4. Administration

Auditing

Auditing is the recording of information about the transfers made by the system.

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, it is possible to configure whether or not auditing information will be sent.

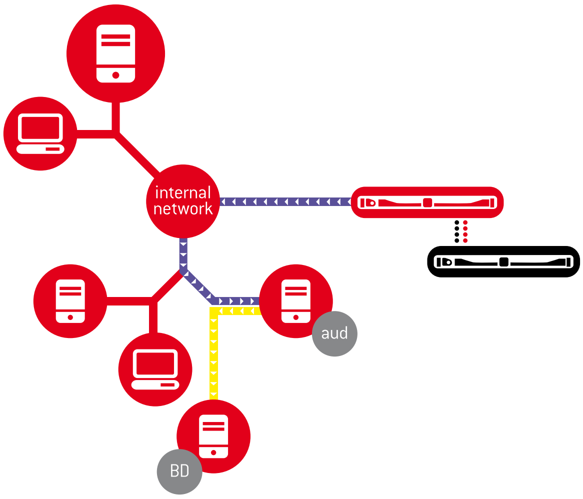

Figure 1.5. Auditing

Technical Features Summary

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

- Transfer rate: 130 Mbps.
- Maximum file size: 20 GB.
- Maximum number of channels: 250.
- Inbound and outbound only systems available
- High availability version (Active - active redundancy scheme).

Security features

- TCP/IP stack interruption at all layers.
- Minimal and securely configured operating system.
- Software integrity at startup is guaranteed.
- External units don't use any persistent data.
- Firmware can be easily upgraded (offline).

2. Infrastructure

This chapter is aimed at anyone intending to introduce or considering deployment of PSTfile within a company or organization.

It includes a description of the infrastructure required in addition to the PSTfile 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. File servers are required in both networks using any of the supported protocols FTP, FTPS or SMB.

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

1. Gateway administration requires:
   - For installing PSTadm, a computer running the Windows XP SP3 (or higher) operating system. PSTadm can be used on various machines and various gateways can be administered from the same PSTadm instance simultaneously.
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.
3. For remote storage of transfer records, the following 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 if it is required to log events in an external database.

Public Key Infrastructure

A public key infrastructure is required for securing gateway communications and for signature verification of outbound files.

The necessary certificates and their features are described below.

Holder	*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

A certificate for each administrator is required.

Holder	*Permissions*
Administrator	Certificate with SSL Client features.

For more detailed information see [IG].

3. File Transfer Services

This section contains a summary of the features of the inbound and outbound file services. For more comprehensive details, see [OG].

Common Features

- Services can be independently enabled and disabled.
- Services are organized into channels (See Inbound File Channel) that can be enabled and disabled independently. Active channels make transfers automatically.
- Supported protocols: FTP, FTPS and SMB.
- *Gateways always* play the client role of supported protocols.
- Files can be *moved or copied* from the source to the target. In the first case once they have been transferred to the target location, they will be deleted from the source location, in the latter they wont.
- Recursive mode: in this mode all folders and their contents are also copied. The folder structure in the source is not deleted.
- File size and file extension restrictions can be configured.
- Configurable transfers log.
- Optionally files can be uploaded with a temporal name and renamed thereafter.
- In high availability versions the administrator can decide in which of the two elements the channel will run.
- The following information is recorded for transfers made by the system : time and date, source and target servers, base directory and *relative directory*, name, size and SHA-256 hash of transferred files.

Outbound File Service

Although signature files can be created with any tool, the product includes **PSTsign**, an easy to use Windows shell extension for this task.

4. 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

PSTfile 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.

  System command for setting system time, reboot and static config query.

- 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 service 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 deployment as described in [IG], including the installation of the PSTadm and PSTaud software components, the configuration described below must be made using the necessary permissions. This configuration must be completed before configuring the inbound and outbound file services; this configuration may be altered subsequently at any time.

Role	Action
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.

Service configuration is separated in service wide and channel configuration. 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 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

Inbound and outbound file services are organized in channels; these channels share some common features, thus facilitating administration. Channels can be turned on and off, their state and transferred and pending file numbers can be monitored.