PSTgateways

autek

Overview - Technical Specifications

Secure cross-domain gateways

PSTgateways

autek

OVERVIEW

PSTgateways is a family of boundary protection devices which allow controlled data transfer between security domains. PSTgateways products based on this technology share a common architecture and differ in the supported data flows, called 'services'. Its layout, software and security features support the main goal of preserving the security properties of the HIGH security domain while allowing controlled data transfer in both directions independently (bidirectional scenarios). The impossibility of any type of traffic between the two networks, apart from the data transferred by the system itself, is guaranteed.

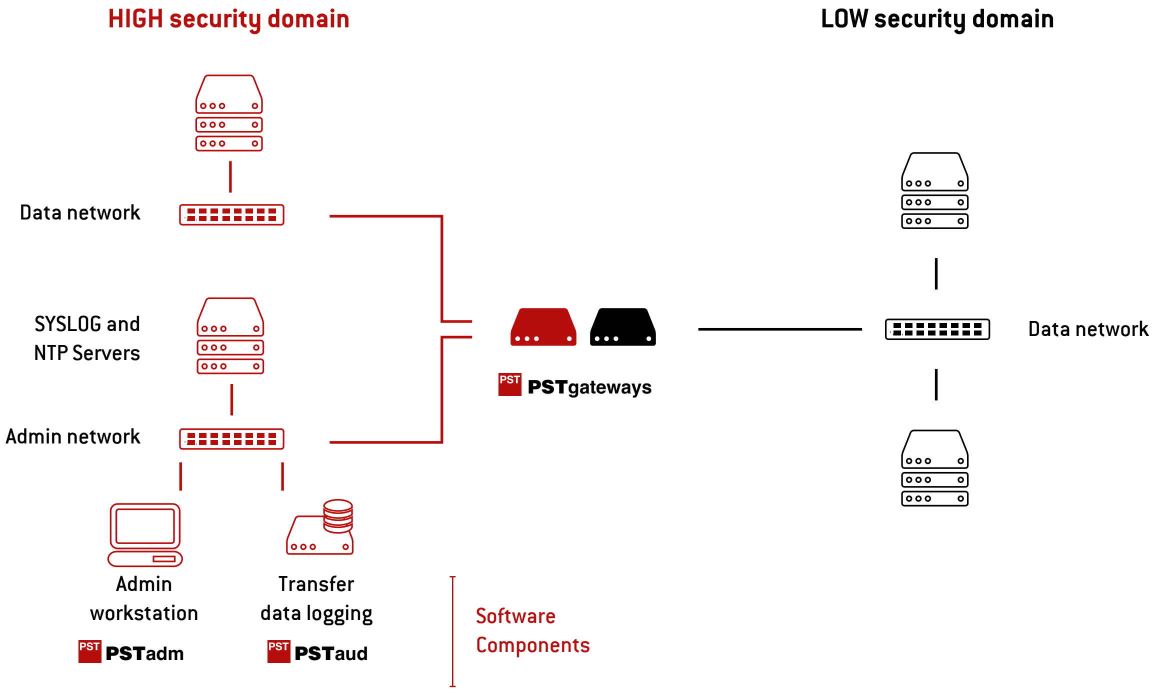
TRUE NETWORK SEPARATION

PSTgateways architecture provides true network separation. Its key points are a 2 host layout and a complete TCP/IP protocol break enforcement. Both appliances act as protocol endpoints and communicate using standard protocols with nodes on each domain.

APPLICATION LEVEL GATEWAYS

Data elements of the application layer (files, email messages, etc.) are extracted and automatically transferred to the other domain. Protocol headers of all stack layers are discarded and new packets are created on the other network for sending the extracted data.

EASE OF DEPLOYMENT AND USE



PSTgateways devices are composed of two 19" appliances with all the necessary software installed (firmware). Each appliance is deployed on one security domain and communicates with the other through a passive device. From the security point of view the solution is asymmetrical; it is exclusively administered from the HIGH security domain. Two additional software components are included, one for the remote administration of the system (PSTadm) and another for transfer data logging (PSTaud). These are installed in general purpose computers.

PSTgateways

autek

‘INBOUND FILE’ SERVICE

The ‘Inbound File’ service allows transferring files between two isolated security domains automatically. This service transfers files from the less secure network (or external) to the more secure network (or internal).

AUTOMATIC FILE TRANSFER

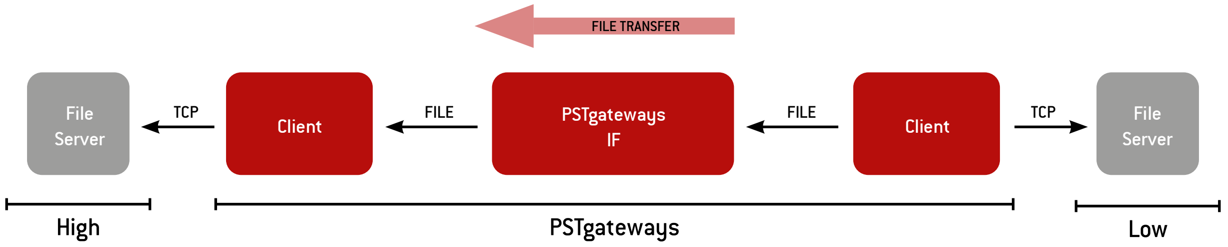
File transfers are defined through channels. A channel is the correspondence between the data source location (server, path) and the data destination location (server, path). Files are automatically moved or copied from the external to the internal network.

The system integrates with the existing infrastructure; each appliance accesses file servers through standard protocols (FTP, FTPS, SFTP or SMB).

The external appliance periodically accesses the file server as a client of the protocol and then transfers the files to the internal appliance. The internal appliance uploads the files to the configured destination folders, also as a client of the protocol.

The system allows different transfer options to be configured for each channel:

- Recursive mode: Subfolders in the source location are also checked.
- Mirror Mode: Allows replication of folder and file structures on the destination file server.
- Automatic delete: Performs the deletion of the correctly transferred files.
- File filter: File name, extension and size filtering.



FEATURES

Channels	Data flows are arranged in communication channels. Channels allow visual and intuitive monitoring. The channels work in parallel and can be enabled and disabled independently.
Channel priority	Channel priority determines the resources dedicated to the channel (server access frequency and the number of files transferred per cycle) and can be set to three different levels: high, medium and low.
Supported protocols	FTP, FTPS, SFTP and SMB.
Maximum number of channels	250
Maximum file size	20 GB
Filtering capabilities	File name, extension and size filtering.

'OUTBOUND FILE' SERVICE

The 'Outbound File' service allows transferring files between two isolated security domains automatically. This service transfers files from the more secure network (or internal) to the less secure network (or external), as long as there is a digital signature authorising the transfer for each file.

AUTOMATIC AUTHORISED FILE TRANSFER

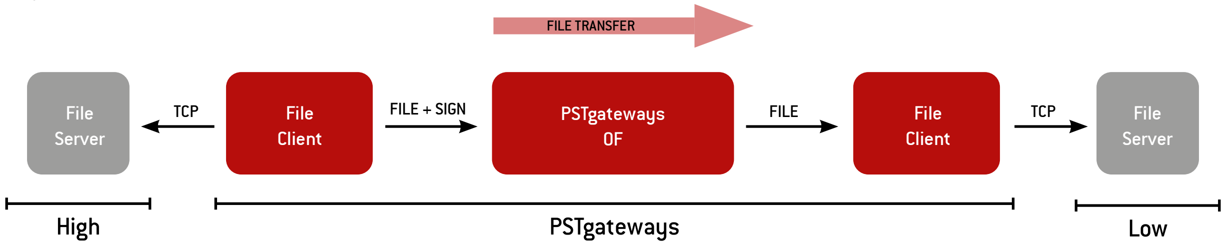
File transfers are defined through channels. A channel is the correspondence between the data source location (server, path) and the data destination location (server, path). Files are automatically moved or copied from the internal to the external network.

The system integrates with the existing infrastructure; each appliance accesses file servers through standard protocols (FTP, FTPS, SFTP or SMB).

The internal appliance periodically accesses the file server as a client of the protocol and checks the validity of the authorisation. It transfers the files to the external appliance, if they are properly authorised. The external appliance uploads the files to the configured destination folders, also as a client of the protocol.

The system allows different transfer options to be configured for each channel:

- Recursive mode: Subfolders in the source location are also checked.
- Mirror Mode: Allows replication of folder and file structures on the destination file server.
- Automatic delete: Performs the deletion of the correctly transferred files.
- File filter: File name, extension and size filtering.



FEATURES

Channels	Data flows are arranged in communication channels. Channels allow visual and intuitive monitoring. The channels work in parallel and can be enabled and disabled independently.
Channel priority	Channel priority determines the resources dedicated to the channel (server access frequency and the number of files transferred per cycle) and can be set to three different levels: high, medium and low.
Supported protocols	FTP, FTPS, SFTP and SMB.
Maximum number of channels	250
Maximum file size	20 GB
Filtering capabilities	File name, extension and size filtering.

PSTgateways

autek

‘INCOMING MAIL’ SERVICE

The ‘Incoming Mail’ service allows transferring mail between two isolated security domains automatically. This service transfers emails from the less secure network (or external) to the more secure network (or internal).

AUTOMATIC MAIL TRANSFER

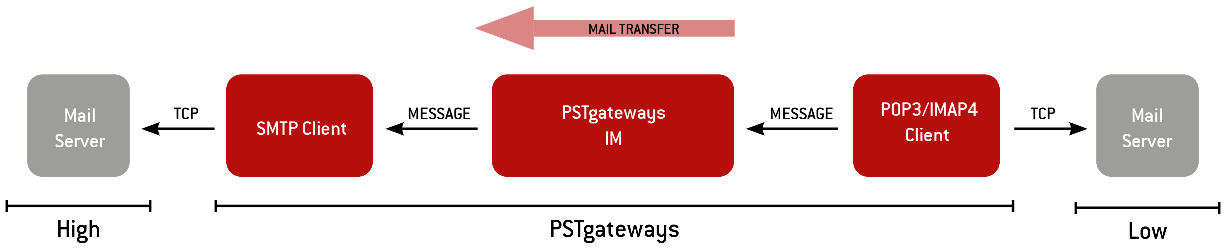
Mail transfers are defined through channels. A channel is the correspondence between an email address on the external network and one or more email addresses on the internal network. Messages are automatically transferred from the external to the internal network.

The system integrates with the existing infrastructure; both appliances access mail servers through standard protocols (SMTP, POP3 or IMAP4).

The external appliance periodically accesses the mail server as a client of the protocol (POP3 or IMAP4) and then transfers the messages to the internal appliance. The internal appliance transfers the messages to the configured mail server, as a client of the protocol (SMTP).

The system allows different transfer options to be configured for each channel:

- Messages can be sent to one or more recipients on the internal network.
- Rejection filter: The system does not transfer a message to the internal network unless it meets certain conditions: number of attachments, attachments type, number of recipients, etc.
- Selection filter: The system allows sending a message to alternative recipients if the message meets certain conditions, including a specific ‘From:’ address, certain texts in the subject or MIME type/subtype.



FEATURES

Channels	Data flows are arranged in communication channels. Channels allow visual and intuitive monitoring. The channels work in parallel and can be enabled and disabled independently.
Channel priority	Channel priority determines the resources dedicated to the channel (server access frequency and the number of messages transferred per cycle) and can be set to three different levels: high, medium and low.
Supported protocols	SMTP, POP3 and IMAP4 (Secure versions supported).
Maximum number of channels	25, 250 or 2500
Maximum message size	50 MB
Filtering capabilities	Selection and rejection filter by MIME type, size, attachment, etc.

‘OUTGOING MAIL’ SERVICE

The ‘Outgoing Mail’ service allows transferring mail between two isolated security domains. This service transfers emails from the more secure network (or internal) to the less secure network (or external), as long as it is digitally signed (S/MIME format).

AUTHORISED MAIL TRANSFER (S/MIME)

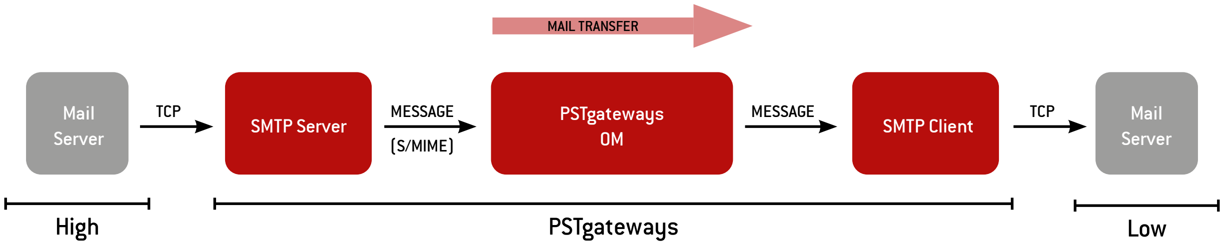
Mail transfers are defined through channels. A channel is defined by an email address on the external network.

The system integrates with the existing infrastructure; both appliances communicate with mail servers through SMTP. It is necessary to configure the internal mail server to relay messages addressed to the external domain through the internal appliance.

The internal appliance works as a SMTP server in the internal network. It receives the relayed messages, analyses them and verifies the signature (S/MIME format). Properly authorised messages are transferred to the external appliance. The external appliance sends the messages to the configured external mail server, as a client of the protocol (SMTP).

The system allows different transfer options to be configured for each channel:

- One or more supervisors can be configured per channel to authorise outgoing messages.
- An internal user can be configured to use different external “From:” addresses (channel).
- Internal copy: Allows forwarding a copy of the outgoing message to an email account on the internal network.
- Rejection filter: The system blocks a message that does not comply with a specific MIME format or does not meet certain configurable conditions, including number of attachments, attachments type, number of recipients, etc.



FEATURES

Channels	Data flows are arranged in communication channels. Channels allow visual and intuitive monitoring. The channels work in parallel and can be enabled and disabled independently.
Channel priority	Channel priority determines the resources dedicated to the channel and can be set to three different levels: high, medium and low.
Supported protocols	SMTP (TLS supported)
Maximum number of channels	25, 250 or 2500
Maximum message size	50 MB
Filtering capabilities	Rejection filter by MIME type, size, attachment, etc.

‘INBOUND UDP’ SERVICE

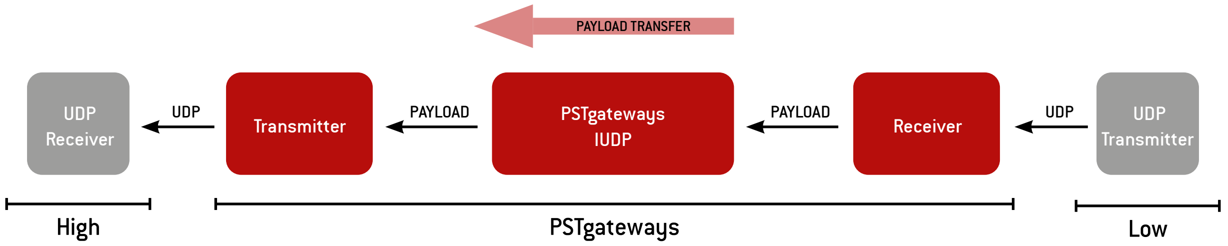
The ‘Inbound UDP’ service allows transferring the payload of UDP packets between two isolated security domains. This service transfers the payload from the less secure network (or external) to the more secure network (or internal). It is suited for ‘real time’ applications due to its low latency (streaming).

UDP PAYLOAD TRANSFER

Transfers are arranged in channels. A channel defines the correspondence between a listening port on the external appliance and a UDP packet destination (server, port) on the internal network.

The external appliance receives UDP packets in the configured listening port and transfers the payload to the destination appliance. The destination appliance makes a new packet and sends it to the configured destination.

The system allows the administrator to configure size and source filtering by channel. Unicast and multicast reception and transmission are also supported.



FEATURES

Channels	Data flows are arranged in communication channels. Channels allow visual and intuitive monitoring. The channels work in parallel and can be enabled and disabled independently.
Channel priority	Channel priority determines the resources dedicated to the channel and can be set to three different levels: high, medium and low.
Supported protocols	UDP
Maximum number of channels	10
Typical mean delay	150 milliseconds
Filtering capabilities	Size and source filtering.
Content control filter	SYSLOG format (BSD or RFC-5424).

FEATURE OVERVIEW

Topology	Two appliances, one on each security domain, which communicate through a passive device.
Deployment	Ready to use appliances. The system is configured remotely once PKI and network parameters are set on the HIGH domain appliance through a local interface.
Administration	The system is monitored remotely, with PSTadm, from the HIGH domain. Several gateways can be administered from the same console (PSTadm). One gateway can be simultaneously administered from several consoles.
Administration Roles	Four remote administration roles are supported and enforced through PKI: • Root Administrator • Security Administrator • Services Administrator • Monitoring Administrator
Status and error notifications	Operation and security events can be sent to separate SYSLOG servers.
Transferred data logging	With PSTaud, installed on a computer on the HIGH domain, information from all transfers can be logged to a database or saved as XML files.
Automatic time synchronisation	The system allows configuring time synchronisation via NTP servers on the HIGH domain.
High Availability (optional)	Complete hardware redundancy. Automatic switch to the secondary system in case of primary system failure.
Maximal bandwidth	130 Mbps (each direction).

SECURITY

Topology	Dedicated and independent management network interface that allows separation of all management traffic from data traffic on the HIGH domain.
Application layer endpoint on both sides	Only data elements of the application layer are extracted and transferred to the other domain.
Boundary network protection	Minimal attack surface. Only used ports available. Communication only with configured hosts allowed.
Administrative communications	The system can only be administered by authorised administrators, enforced through PKI. All communications between the software components and the appliances are protected by TLS with remote peer authentication. All system access and operations performed by administrators are reported.
Transferred data logging	Information from all transfers can be logged for audit purposes.
Appliance software integrity	All software (OS included) executes from a RO partition, the integrity of which can be verified with the supplied tool.

PSTgateways

autek

APPLIANCES TECHNICAL DATA

Connectors	
Video interface	15-pin VGA
Keyboard interface	USB type A
Data network interface	RJ45 (Ethernet 10/100/1000 Mbps)
Administrative network interface	RJ45 (Ethernet 10/100/1000 Mbps)

AC Power Supply	
Connector	IEC-60320-C14
Wattage	450W
Heat dissipation	1725 BTU/hr
Voltage	100-240 V AC, 50/60 Hz

Physical	
Dimensions	4,28 cm (1U) x 48,2 cm (19") x 57,36 cm
Weight	9,20 kg

Temperature	
Operating	From 0ºC to 45ºC
Storage	From -40°C to 65°C

IDENTIFICACIÓN

Referencia (Part Number)	*NSN*	
PSTgateways S6	5895-33-219-0475	Complete system. External Appliance and Internal Appliance are included.
PSTi-S6	5895-33-219-0477	Internal Appliance (red bezel).
PSTe-S6	5895-33-219-0476	External Appliance (black bezel).

Autek Ingeniería, S.L.
Av. Burgos 9, of.1. E-28036 Madrid (España)
Tel. +34 915 974 629
info@autek.es I www.autek.es