PSTgateways

autek
A GMV COMPANY

Introducción - Especificaciones técnicas

Pasarelas seguras cross-domain

PSTgateways

autek
A GMV COMPANY

VISIÓN GENERAL

PSTgateways es una familia de dispositivos de protección de perímetro que permiten transferir información entre dos dominios de seguridad diferentes. Los productos PSTgateways comparten una arquitectura común y se diferencian entre sí en los flujos de datos -llamados 'servicios'- que soportan.

Permiten el intercambio de información en ambos sentidos de manera independiente (escenarios bidireccionales) garantizando la imposibilidad de cualquier tipo de tráfico entre las dos redes, distinto del transferido por el propio sistema.

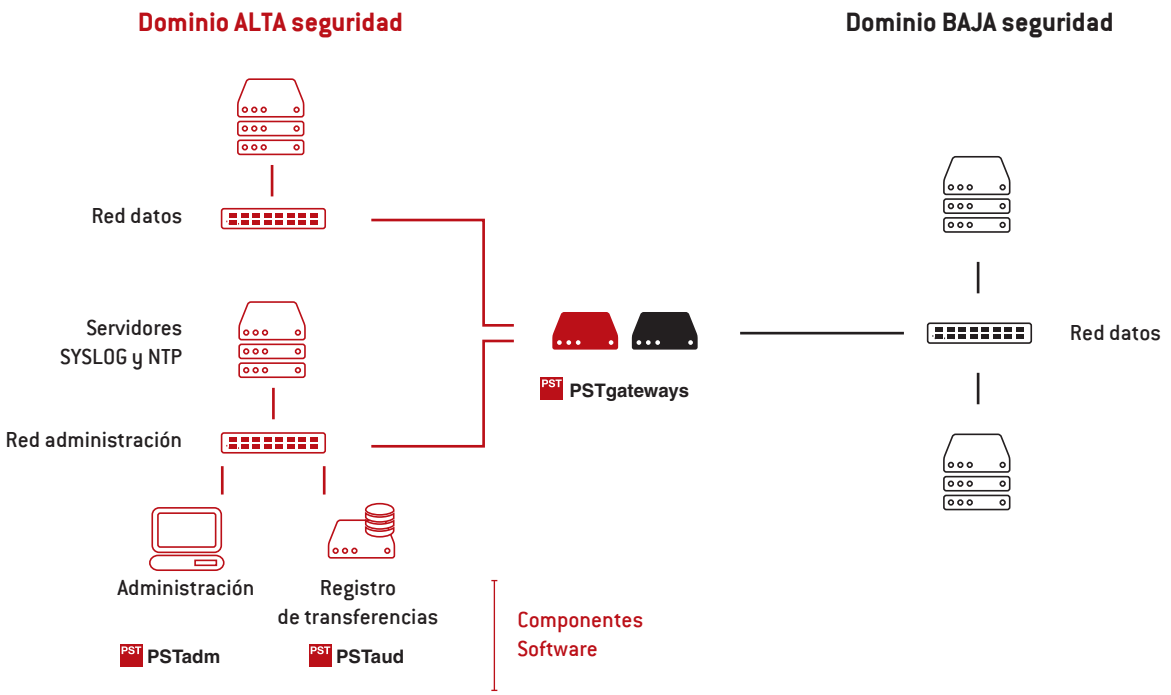
SEPARACIÓN DE REDES

La arquitectura de PSTgateways proporciona separación real de redes. Sus fundamentos son la separación en dos *appliances* y la rotura total de la pila de protocolos TCP/IP. Cada uno de los *appliances* actúa como extremo de la comunicación en un dominio.

PASARELA DE NIVEL DE APLICACIÓN

Las pasarelas intercambian, de manera automática, elementos de alto nivel (ficheros, mensajes, etc.) que se extraen del nivel de aplicación y se transfieren al otro dominio. Las cabeceras de todos los niveles de la pila de protocolos se descartan y se crean nuevos paquetes en la otra red para enviar los datos transferidos.

FACILIDAD DE DESPLIEGUE Y ADMINISTRACIÓN



Los dispositivos PSTgateways están formados por dos *appliances* de 19" con todo el software necesario instalado (*firmware*). Cada uno se despliega en un dominio y se comunican entre sí mediante un dispositivo de intercambio pasivo. Desde el punto de vista de la seguridad, la solución es asimétrica: se administra exclusivamente desde del dominio de ALTA seguridad. Se incluyen dos componentes software adicionales, uno para la administración (PSTadm) y otro para el registro de transferencias (PSTaud), que funcionan en ordenadores de propósito general.

PSTgateways

autek
A GMV COMPANY

SERVICIO "ENTRADA DE FICHEROS"

El servicio "Entrada de ficheros" transfiere ficheros en un único sentido, de manera activa, entre dos dominios de seguridad aislados. Este servicio transfiere ficheros desde la red menos segura (o externa) a la red más segura (o interna).

TRANSFERENCIA AUTOMÁTICA DE FICHEROS

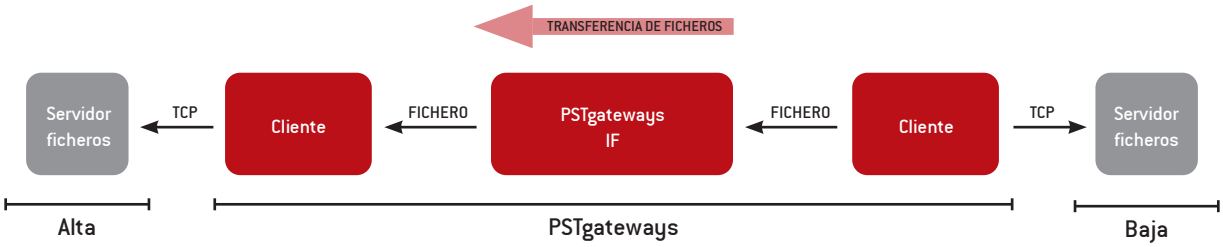
La transferencia de ficheros se define mediante canales. Un canal establece la correspondencia entre un origen de datos (servidor, ruta) y un destino (servidor, ruta). Los ficheros se mueven o copian de manera automática desde la red externa a la red interna.

El sistema se integra con la infraestructura existente. Cada uno de los *appliances* accede a servidores de ficheros mediante protocolos estándar (FTP, FTPS, SFTP ó SMB).

El *appliance* externo accede a los servidores de ficheros periódicamente, como cliente del protocolo, y transfiere los ficheros al *appliance* interno. El *appliance* interno los transfiere al servidor de ficheros de la red interna, también como cliente del protocolo.

El sistema permite configurar diferentes opciones de transferencia por canal:

- Modo recursivo: Se comprueban los directorios y subdirectorios dentro de la ruta especificada del servidor de ficheros origen.
- Modo espejo: Permite replicar una estructura de directorios y ficheros en el servidor de ficheros destino.
- Borrado automático: Permite borrar los ficheros en el servidor de ficheros origen una vez transferidos correctamente.
- Filtrado de ficheros: Capacidad de filtrar por nombre, extensión o tamaño.



CARACTERÍSTICAS

Organización en canales	El flujo de datos se configura mediante canales de comunicación. Los canales permiten una monitorización visual e intuitiva. Los canales trabajan en paralelo y pueden ser activados y desactivados independientemente.
Prioridad de los canales	La prioridad de los canales permite establecer los recursos dedicados (frecuencia de acceso al servidor, número de ficheros por ciclo, etc.) al canal mediante tres niveles: alto, medio y bajo.
Protocolos soportados	FTP, FTPS, SFTP y SMB.
Número máximo de canales	250
Tamaño máximo de fichero	20 GB
Capacidades de filtrado	Filtrado por nombre del fichero, extensión o tamaño.

PSTgateways

autek
A GMV COMPANY

SERVICIO "SALIDA DE FICHEROS"

El servicio "Salida de ficheros" transfiere ficheros en un único sentido, de manera activa, entre dos dominios de seguridad aislados. Este servicio transfiere ficheros desde la red más segura (o interna) a la red menos segura (o externa), siempre y cuando exista una firma digital autorizando la transferencia para cada fichero.

TRANSFERENCIA AUTOMÁTICA DE FICHEROS AUTORIZADOS

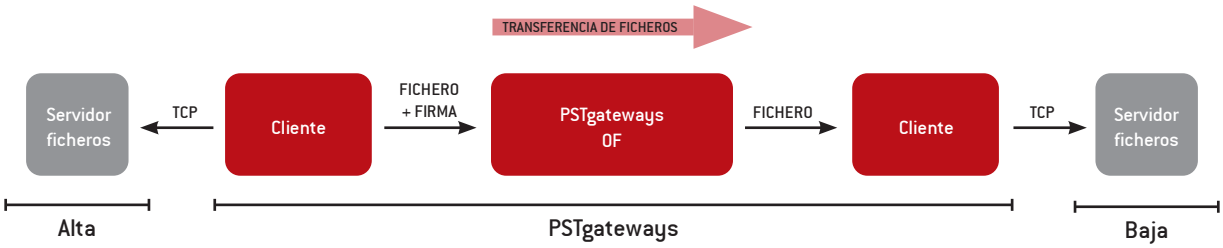
La transferencia de ficheros se define mediante canales. Un canal establece la correspondencia entre un origen de datos (servidor, ruta) y un destino (servidor, ruta). Los ficheros autorizados se mueven o copian de manera automática desde la red interna a la red externa.

El sistema se integra con la infraestructura existente. Cada uno de los *appliances* accede a servidores de ficheros mediante protocolos estándar (FTP, FTPS, SFTP ó SMB).

El *appliance* interno accede a los servidores de ficheros periódicamente, como cliente del protocolo, y comprueba la validez de la autorización. Sí está correctamente autorizado transfiere el fichero al *appliance* externo. El *appliance* externo los transfiere al servidor de ficheros de la red externa, también como cliente del protocolo.

El sistema permite configurar diferentes opciones de transferencia por canal:

- Modo recursivo: Se comprueban los directorios y subdirectorios dentro de la ruta especificada del servidor de ficheros origen.
- Modo espejo: Permite replicar una estructura de directorios y ficheros en el servidor de ficheros destino.
- Borrado automático: Permite borrar los ficheros en el servidor de ficheros origen una vez transferidos correctamente.
- Filtrado de ficheros: Capacidad de filtrar por nombre, extensión o tamaño.



CARACTERÍSTICAS

Organización en canales	El flujo de datos se configura mediante canales de comunicación. Los canales permiten una monitorización visual e intuitiva. Los canales trabajan en paralelo y pueden ser activados y desactivados independientemente.
Prioridad de los canales	La prioridad de los canales permite establecer los recursos dedicados (frecuencia de acceso al servidor, número de ficheros por ciclo, etc.) al canal mediante tres niveles: alto, medio y bajo.
Protocolos soportados	FTP, FTPS, SFTP y SMB.
Número máximo de canales	250
Tamaño máximo de fichero	20 GB
Capacidades de filtrado	Filtrado por nombre del fichero, extensión o tamaño.

PSTgateways

autek
A GMV COMPANY

SERVICIO "ENTRADA DE CORREO"

El servicio "Entrada de correo" transfiere mensajes de correo electrónico en un único sentido, de manera activa, entre dos dominios de seguridad aislados. Este servicio transfiere mensajes desde la red menos segura (o externa) a la red más segura (o interna).

TRANSFERENCIA DE CORREO ELECTRÓNICO

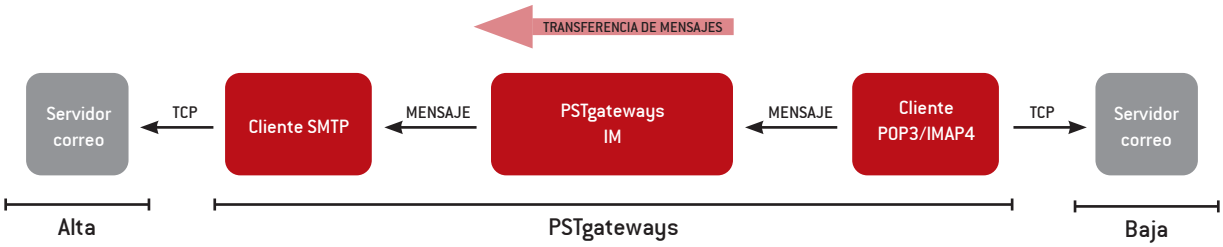
La transferencia de mensajes se define mediante canales. Un canal establece la relación entre una dirección de correo en un servidor en la red externa y una o más direcciones de correo en un servidor en la red de interna.

El sistema se integra con la infraestructura existente, cada uno de los *appliances* accede a servidores de correo mediante protocolos estándar (SMTP, POP3 ó IMAP4).

El *appliance* externo accede a los servidores de correo periódicamente, como cliente del protocolo POP3 ó IMAP4, y transfiere los mensajes al *appliance* interno. El *appliance* interno los transfiere al servidor de correo de la red interna, como cliente del protocolo SMTP.

El sistema permite configurar diferentes opciones de transferencia por canal:

- Permite enviar el mensaje a uno o más destinatarios en la red interna.
- Filtro de rechazo: El sistema no transfiere a la red interna un mensaje que no cumpla determinadas condiciones configurables: número de adjuntos, tipo de adjunto, número de destinatarios, etc.
- Filtro de selección: El sistema permite enviar un mensaje a un destinatario alternativo en la red interna si se cumplen determinadas condiciones: dominio del remitente, determinado texto en el asunto, tipo /subtipo MIME, etc.



CARACTERÍSTICAS

Organización en canales	El flujo de datos se configura mediante canales de comunicación. Los canales permiten una monitorización visual e intuitiva. Los canales trabajan en paralelo y pueden ser activados y desactivados independientemente.
Prioridad de los canales	La prioridad de los canales permite establecer los recursos dedicados (frecuencia de acceso al servidor, número de mensajes por ciclo, etc.) al canal mediante tres niveles: alto, medio y bajo.
Protocolos soportados	SMTP, POP3 e IMAP4 (Soporta versiones seguras).
Número máximo de canales	25, 250 ó 2.500
Tamaño máximo del mensaje	50 MB
Capacidades de filtrado	Filtrado y selección de mensajes por tipo MIME, tamaño, adjuntos, etc.

PSTgateways

autek
A GMV COMPANY

SERVICIO "SALIDA DE CORREO"

El servicio "Salida de correo" transfiere mensajes de correo electrónico, en un único sentido, entre dos dominios de seguridad aislados. Este servicio transfiere mensajes desde la red más segura (o interna) a la red menos segura (o externa), siempre y cuando cada mensaje este autorizado mediante una firma digital (formato S/MIME).

TRANSFERENCIA DE CORREO ELECTRÓNICO AUTORIZADO (S/MIME)

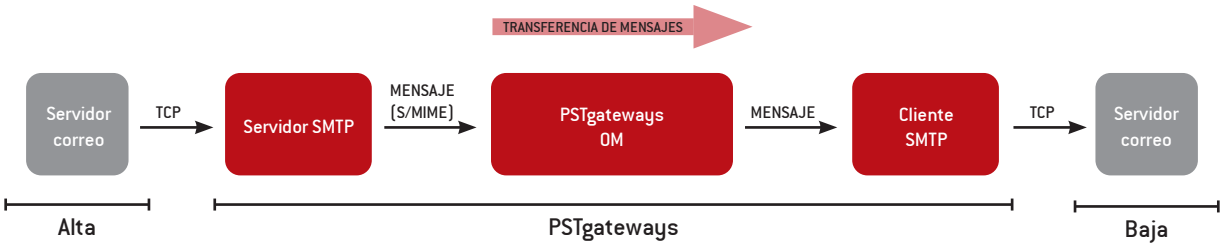
La transferencia de mensajes se organiza mediante canales. Un canal se define por una dirección de remite de correo en la red externa.

El sistema se integra con la infraestructura existente. Cada uno de los *appliances* se comunica con servidores de correo mediante el protocolo estándar SMTP. Es necesario configurar el servidor de correo interno para que reenvíe al *appliance* interno los mensajes destinados al dominio externo.

El *appliance* interno actúa como servidor de correo en la red interna. Recibe los mensajes reenviados, los analiza y verifica la firma (formato S/MIME). Si está correctamente autorizado, elimina la firma y cualquier referencia al domino de correo de la red interna, y se transfiere al *appliance* externo. El *appliance* externo envía el mensaje al servidor de correo externo como cliente del protocolo SMTP.

El sistema permite configurar diferentes opciones de transferencia por canal:

- Permite configurar uno o varios supervisores por canal para autorizar la salida de mensajes.
- Permite configurar que un usuario utilice diferentes direcciones de remite externo (canal).
- Copia interna: El sistema permite reenviar una copia del mensaje de salida a una cuenta de correo de la red interna.
- Filtro de rechazo: El sistema no transfiere a la red de externa un mensaje que no cumpla el formato MIME o determinadas condiciones configurables: número de adjuntos, tipo de adjunto, número de destinatarios, etc.



CARACTERÍSTICAS

Organización en canales	El flujo de datos se configura mediante canales de comunicación. Los canales permiten una monitorización visual e intuitiva. Los canales trabajan en paralelo y pueden ser activados y desactivados independientemente.
Prioridad de los canales	La prioridad de los canales permite establecer los recursos dedicados al canal mediante tres niveles: alto, medio y bajo.
Protocolos soportados	SMTP (Soporta TLS)
Número máximo de canales	25, 250 o 2.500
Tamaño máximo del mensaje	50 MB
Capacidades de filtrado	Filtrado por formato MIME, tamaño, adjuntos, etc.

PSTgateways

autek
A GMV COMPANY

SERVICIO "ENTRADA UDP"

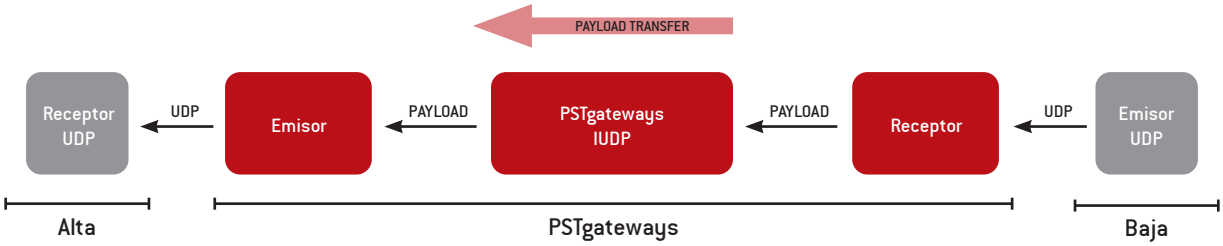
El servicio "Entrada UDP" transfiere el contenido de paquetes UDP (payload), en un único sentido, desde la red menos segura (o externa) a la red más segura (o interna). Su baja latencia permite el uso en aplicaciones de "tiempo real" (streaming).

TRANSFERENCIA "PAYLOAD" UDP

La transferencia de "payload" UDP se define mediante canales. Un canal establece la correspondencia entre un puerto de escucha en el *appliance* externo y un destinatario del paquete UDP (servidor, puerto) en la red interna.

El *appliance* externo espera paquetes UDP en el puerto configurado y transfiere el "*payload*" al *appliance* interno. El *appliance* interno crea un nuevo paquete y envía el "*payload*" al destino configurado.

El sistema permite establecer filtros de tamaño y origen por canal. Además soporta la recepción y envío unicast y multicast.



CARACTERÍSTICAS

Organización en canales	El flujo de datos se configura mediante canales de comunicación. Los canales permiten una monitorización visual e intuitiva. Los canales trabajan en paralelo y pueden ser activados y desactivados independientemente.
Prioridad de los canales	La prioridad de los canales permite establecer los recursos dedicados al canal mediante tres niveles: alto, medio y bajo.
Protocolos soportados	UDP
Número máximo de canales	10
Retardo medio típico	150 milisegundos.
Capacidades de filtrado	Filtrado por tamaño y origen.
Filtro de contenido	Formato SYSLOG (BSD ó RFC-5424).

CARACTERÍSTICAS GENERALES

Topología	Dos *appliances*, cada uno conectado a un dominio de seguridad, comunicados mediante un dispositivo de intercambio pasivo.
Despliegue	*Appliances* listos para usar. El sistema se configura remotamente una vez establecidos los parámetros de red y PKI mediante una interfaz local en el *appliance* del dominio de ALTA.
Administración	La administración remota del sistema se realiza desde el dominio de ALTA. Es posible administrar varias pasarelas desde la misma consola de administración (PSTadm). Una pasarela se puede administrar simultáneamente desde varias consolas de administración.
Roles de administración	El sistema permite definir 4 roles diferentes de administración: • Administrador raíz • Administrador de seguridad • Administrador de servicios • Administrador de monitorización
Estado y notificación de error	El sistema envía eventos de SYSLOG de funcionamiento y seguridad de manera independiente.
Registro de transferencias	Es posible registrar la información de las transferencias realizadas en ficheros o base de datos. Se realiza mediante un componente software separado (PSTaud) que funciona en un ordenador ubicado en el dominio de ALTA.
Sincronización automática de hora	El sistema permite configurar la sincronización de hora a través de servidores NTP en el dominio de ALTA.
Alta disponibilidad (opcional)	Redundancia hardware completa. Recuperación automática en caso de fallo.
Tasa de transferencia	130 Mbps (en cada sentido).

SEGURIDAD

Topología	Interfaz de administración dedicada e independiente que permite separar todo el tráfico de administración del tráfico de datos en el dominio de ALTA.
Extremo de la comunicación en ambos dominios	Sólo se intercambian entre los dominios elementos de información 'por encima' de la capa de aplicación.
Protección perimetral	Superficie de ataque mínima. Sólo los puertos necesarios están disponibles. Sólo se permite la comunicación con los sistemas configurados.
Comunicaciones de administración	Sólo los administradores autorizados, mediante certificados digitales, pueden administrar el sistema. Las comunicaciones de los componentes software con los *appliances* están protegidas mediante TLS con autenticación del extremo remoto. Se registran todos los accesos y operaciones realizados por los administradores del sistema.
Registro de transferencias	Registro de la información de las transferencias realizadas con fines de auditoria.
Garantía de integridad del *firmware*	Todo el software (incluido el sistema operativo) se ejecuta desde una partición de solo lectura, cuya integridad puede ser verificada en cualquier momento.

PSTgateways

autek
A GMV COMPANY

DATOS TÉCNICOS DE LOS *APPLIANCES*

Conexiones	
Interfaz de video	VGA 15 pines
Interfaz teclado	USB tipo A
Interfaz red de datos	RJ45 (Ethernet 10/100/1000 Mbps)
Interfaz red de administración	RJ45 (Ethernet 10/100/1000 Mbps)

Características físicas	
Dimensiones	4,28 cm (1U) x 48,2 cm (19") x 46,1 cm
Peso	9.45 kg

Alimentación	
Conector	IEC-60320-C14
Potencia	700 W
Disipación de calor máxima	2625 BTU/hr
Tensión	200-240 V AC, 50/60 Hz

Temperatura	
Funcionamiento	De 0ºC a 45ºC
Almacenamiento	De -40°C a 65°C

IDENTIFICACIÓN

Referencia (Part Number)	
PSTgateways S7	Sistema completo. Incluye *Appliance* Interno y *Appliance* Externo.
PSTi-S7	*Appliance* Interno (frontal rojo).
PSTe-S7	*Appliance* Externo (frontal negro).

CERTIFICACIONES Y APROBACIONES

Certificado Common Criteria EAL 4+ (AVA_VAN.5, ALC_FLR.3)

Producto STIC aprobado para el manejo de información clasificada

Incluido en el catálogo NIAPC

info@autek.es | www.autek.es