

HACEMOS FÁCILES LAS COMUNICACIONES



SAIWALL

Gestor de VPN Global de SAIMA Sistemas



SAIWALL

SAIMA SISTEMAS, en el afán de ofrecer un mejor servicio a sus clientes, pone a su disposición el SAIWALL "gestor VPN global" para la conexión VPN con delegaciones o usuarios remotos nacionales e internacionales que tengan conexión a Internet. Esta plataforma de gestión permitirá a todos aquellos clientes que lo requieran unir todos los puntos de su red minimizando costes y con una escalabilidad total, ya que podrá ir añadiendo delegaciones a medida que su empresa crezca, sin tener que realizar cambios, ni añadir equipos.

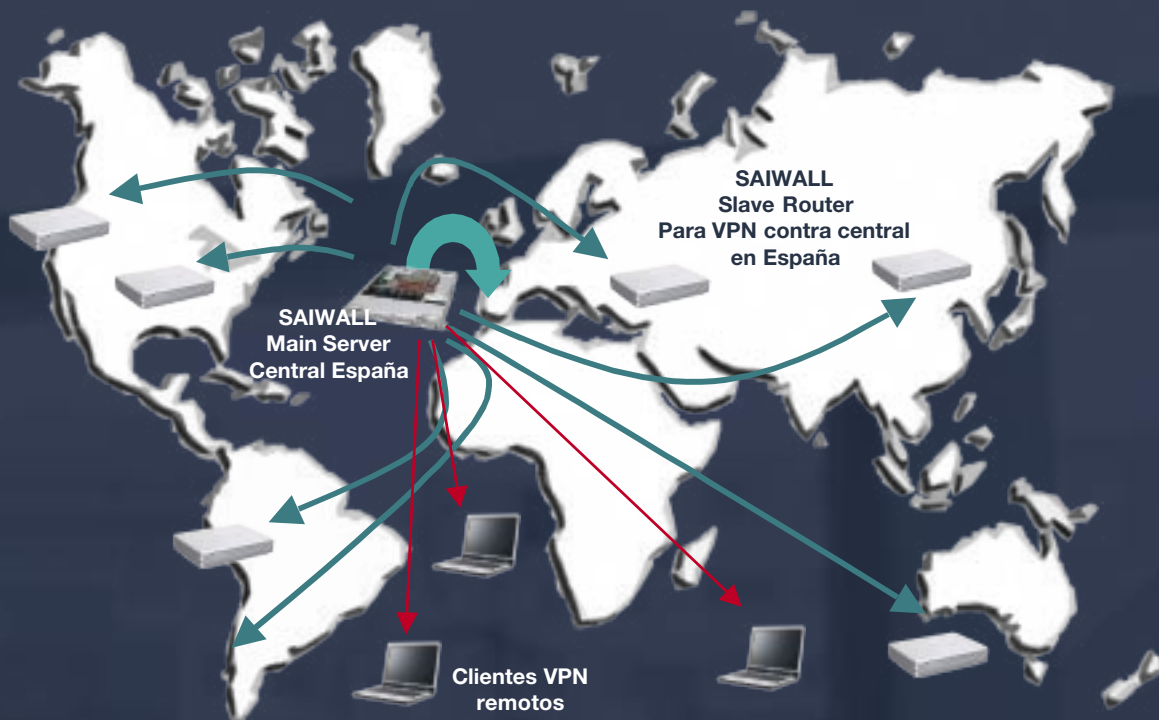
Nuestra propuesta de conexión de redes (por ejemplo la de sucursales o delegaciones) es 100% independiente tanto del proveedor como del tipo de conexión a Internet que tenga. Si por ejemplo su oficina está conectada a Internet por ADSL podrá seguir accediendo a Internet exactamente del mismo modo que lo hace en la actualidad, y simultáneamente, esa misma conexión será perfectamente válida para establecer la conexión segura con otras oficinas.



Servidor SAIWALL Main Server
Con Supermicro 1U,2U,4U



SAIWALL Slave Router



SAIWALL

SAIWALL

El SAIWALL central incluye un Firewall SPI (Stateful Packet Inspection) basado en Linux. Este sistema permite control de tráfico por puertos, direcciones IP, subredes, y permite en los filtros, aparte de bloquear o aceptar el tráfico. El sistema está diseñado para la gestión centralizada de filtros y firmwares a nivel global, de grupos, subgrupos o individuales.

El sistema se basa en una red privada virtual que se crea entre los puntos remotos y la central del cliente, creado con el protocolo de seguridad SSL VPN por UDP utilizando para la encriptación certificados de seguridad de 2048 bits y para la encriptación AES 128 bits simétricos con claves de cifrado que se renuevan automáticamente cada hora.

El sistema soporta cualquier tipo de protocolo de Routing, diseñado para redes con crecimiento constante.

El sistema permite adaptación de funcionalidades a medida del cliente, por ejemplo: protocolos y aplicaciones propias.

BENEFICIOS DEL SISTEMA

Instalación Centralizada / Sistema de Auto configuración Propio.

Gestión centralizada de Filtros global, que permite filtrar desde el SAIWALL central los grupos, subgrupos o individual de las delegaciones.

Gestión Automatizada del Software de los Slave Routers.

Funciona sin actualizar ni reconfigurar routers Adsl.

Permite Load Balancing en el equipo central SAIWALL para añadir ancho de banda fácilmente. (ejemplo para usar 2 Adsl + 1 PtaPt + Radio Enlace, etc., con IPS fijas)

En cada delegación permite CLUSTER de SAIWALL-SR + Load Balancing como la central.

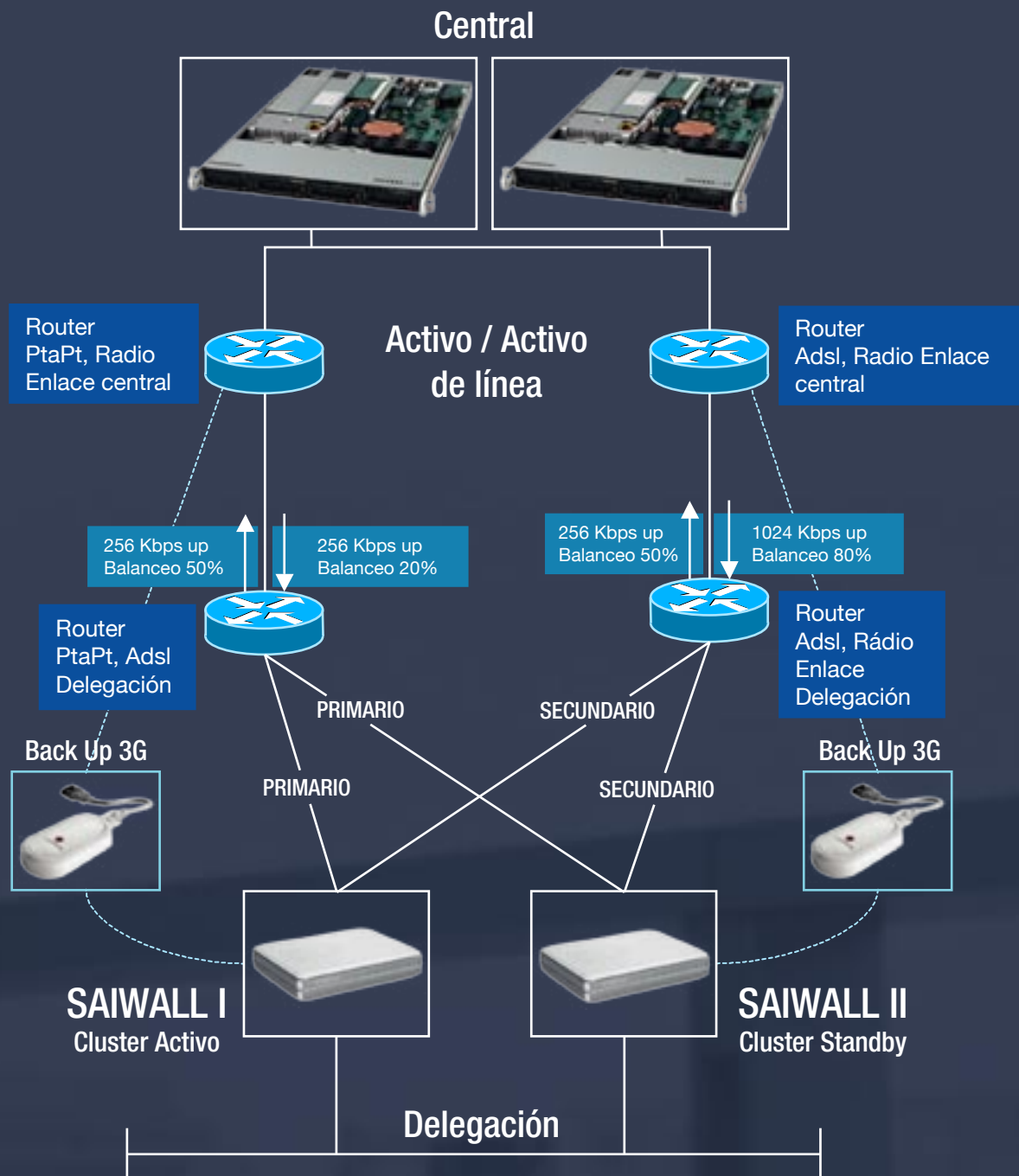
No requiere IPS fijas en las delegaciones, el sistema funciona también con IPs dinámicas ahorrando los costes de las IPs fijas.

Sistema WISE de Saima Sistemas que permite gestionar a través de un sistema ACTIVO - ACTIVO de líneas el porcentaje de caudal que se destina en la subida y bajada del flujo de datos en cada una de las líneas de forma inteligente y automatizada.

VPN de alta seguridad que imposibilita en su totalidad cualquier tipo de ataque de SPOOFING tanto de destino como de origen.

SAIWALL

Sistema WISE de flujo de datos de Saima Sistemas



SAIWALL

COMPARATIVA CON OTRAS SOLUCIONES DE VPN

	SAIWALL VPN	VPN PROVEEDOR INTERNET (1)	VPN HARDWARE (2)	SIN VPN (3)
IP FIJA OBLIGATORIA EN DELEGACION	✗	✓	✓	✓
IP FIJA CENTRAL	✓	✗	✓	✓
GESTION				
GESTION FIREWALL	✓	✗	✓	✓
GESTION FIREWALL CENTRALIZADO (5)	✓	✗	✗	✗
MULTI IDIOMA	✓	✗	✗	✗
INSTALACION CENTRALIZADA (5)	✓	✗	✗	✗
ACTUALIZACION AUTOMATICA DE LOS EQUIPOS DELEGACION	✓	✗	✗	✗
OBLIAGACION RECONFIGURACION DEL ROUTER DEL PROVEEDOR	✗	✗	✓	✓
CONECTIVIDAD				
LOAD BALANCING VPN CENTRAL	✓	✗	✗(4)	✗
LOAD BALANCING VPN DELEGACION	✓	✗	✗(4)	✗
LOAD BALANCING INTERNET CENTRAL	✓	✗	✗(4)	✗
LOAD BALANCING INTERNET DELEGACION	✓	✗	✗(4)	✗
CLUSTER CENTRAL	✓	✗	✓(4)	✗
CLUSTER DELEGACION	✓	✗	✓(4)	✗
CUALQUIER CONEXIÓN A INTERNET	✓	✗	✗	✓
3G/UMTS	✓	✗	✗	✓
BACKUP 3G/UMTS	✓	✗	✗	✗
CONFIGURACION UNIFICADA Y CENTRALIZADA (5) DE LOS CLUSTERS CENTRAL	✓	✗	✗	✗
CONFIGURACION UNIFICADA Y CENTRALIZADA (5) DE LOS CLUSTERS DELEGACION	✓	✗	✗	✗
SISTEMA WISE, PERMITE DEFINIR LOS % DE CAUDAL DE LAS LINEAS SEGÚN NECESIDAD	✓	✗	✗	✗

NOTA: ✓ = SI
✗ = NO

SAIWALL

	SAIWALL VPN	VPN PROVEEDOR INTERNET (1)	VPN HARDWARE (2)	SIN VPN (3)
SEGURIDAD				
SEGURIDAD FRENTE ATAQUES DE SPOOFING (ROBO DE IDENTIDAD)	✓	✓	✓	✗
PROTOCOLO DE ENCRIPCIÓN AES 128 Bits DE MÁXIMA SEGURIDAD	✓	✗	✗	✗
COMPATIBILIDAD CON TODOS LOS ROUTERS POR USAR SSL	✓	N/A	✗	N/A
RENOVACIÓN DE CLAVES DE CIFRADO DE FORMA AUTOMÁTICA CADA HORA	✓	N/A	✗	N/A
TUNEL ENCAPSULADO POR UDP	✓	N/A	✓	✗
FIREWALL				
GESTIÓN CENTRALIZADA (5) DE FILTROS	✓	✗	✗	✗
GESTIÓN CENTRALIZADA (5) DE NAT	✓	✗	✗	✗
GESTIÓN CENTRALIZADA (5) DE RUTAS	✓	✗	✗	✗
MONITORIZACIÓN FLUJOS DE PAQUETES DE DATOS	✓	✗	✓	✗
MONITORIZACIÓN LATENCIAS	✓	✗	✗	✗
MONITORIZACIÓN ANCHO DE BANDA	✓	✗	✓	✗
MONITORIZACIÓN DE LINEAS	✓	✗	✓	✗
ESCALABILIDAD DE CRECIMIENTO				
SIN LÍMITE DE DELEGACIONES NACIONALES	✓	✓	✗	✓
SIN LÍMITE DE DELEGACIONES INTERNACIONALES	✓	✗	✗	✓

NOTA: ✓ = SÍ
✗ = NO

(1) VPN Proveedor de Internet: Operador de telecomunicaciones Ej. Telefónica (netlan), BT, C&W

(2) VPN Hardware: Equipos Router VPN genérico Ej. Cisco, Zyxel

(3) Sin VPN: Conexión directa sin VPN.

(4) Soluciones que solo las tienen una minoría de proveedores de equipos pero con costes muy elevados.

(5) Gestión Centralizada: Es una función que permite realizar la gestión por grupos subgrupos e individuales desde el panel de control de la Central de los equipos de las delegaciones.

SAIWALL

	SAIWALL VPN	VPN PROVEEDOR INTERNET (1)	VPN HARDWARE (2)	SIN VPN (3)
COSTES				
COSTES DE HARDWARE	✓	✗	✓	✗
AMORTIZACION HARDWARE	✓	✗	✓	N/A
COSTES MENSUALES VPN DELEGACION	✗	✓	✗	✗
COSTES MENSUALES IP FIJA DELEGACION	✗	✓	✓	✓
COSTES MENSUALES CENTRAL	✓	✓	✗	✗
POSIBILIDAD SLA	✓	✓	✗	✗
SOPORTE 8/5	✓	✓	✓	✗
POSIBILIDAD SOPORTE 24/7	✓	✓	✗	✗
GESTION DE INCIDENCIAS	✓	✓	✗	✗

NOTA: ✓ = SI
✗ = NO

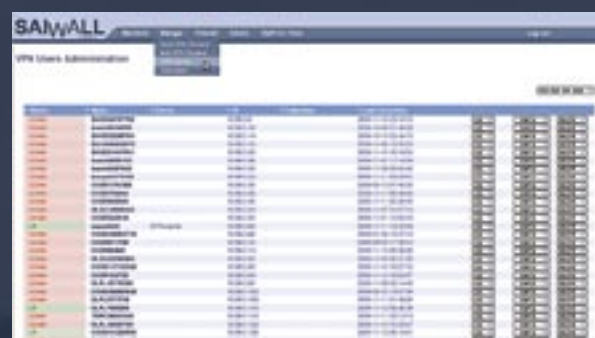
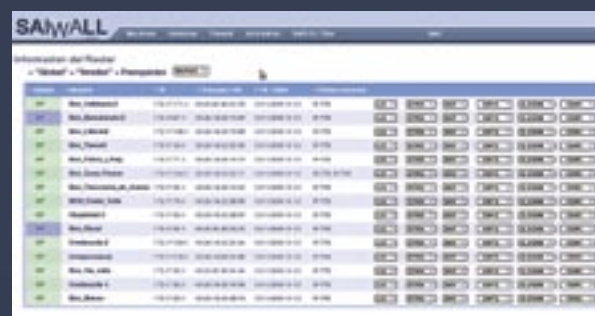
SAIWALL

CARACTERÍSTICAS DEL INTERFASE

ESTADO DE LOS EQUIPOS REMOTOS SAIWALL SR

· La interfaz muestra los grupos y subgrupos que forman la VPN. Pudiendo navegar por ellos apretando encima de su nombre. Si se entra en modo administrador, esta pagina permite ejecutar las siguientes acciones sobre los grupos/subgrupos:

- Controlar los routers encendidos y/o caídos.
- Renombrar los nombres.
- Eliminar grupos y subgrupos vacíos.
- Modificar el servidor VPN por defecto de un grupo/subgrupo.



USUARIOS VPN

· Gestiona los usuarios VPN conectados al sistema. En ella podemos ver cada usuario que tenemos añadido, sus datos, IP dentro de la VPN, etc. A parte también podemos acceder al estado de la conexión y al Log.

AÑADIR SAIWALLS SR

· Se utiliza para añadir Saiwall SR al sistema. Se hace de la siguiente manera:

en MAC seleccionamos el router desconfigurado que queramos añadir, le damos un NOMBRE, Seleccionamos un grupo/subgrupo donde ubicarlo. Si los grupos/subgrupos que hay no nos satisfacen se pueden crear mas con los botones de la derecha.

Escogemos la IP que tendrá el router dentro de la VPN y con ello la de la red que creara, podemos escoger si forzar una Configuración IP en el router, después seteamos los parametros DHCP, DNS y WINS según las necesidades para esa subred. Finalmente decidimos si el router permitirá el acceso mediante Wireless

Una vez configurados estos parametros le damos al botón añadir.

SAIWALL

AÑADIR USUARIOS VPN

· Se utiliza para añadir usuarios al servidor VPN. Estos usuarios se conectan con el SAIWALL cliente VPN directamente al servidor.

ADMINISTRACIÓN DE FILTROS

· En esta pagina podemos filtrar todas las conexiones que se producen en nuestra red. Tanto las de la VPN como las que pasan por el servidor central. Para ello tenemos que:

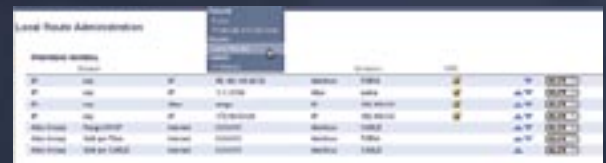
- Escoger un 'Origen' y un 'Destino' para los paquetes
- Seleccionar el protocolo donde queremos añadir el filtro
- Definir de que tipo queremos que sea el filtro. Si queremos que sea de permisión debemos seleccionar ACCEPT, en caso contrario hay que seleccionar DROP.
- Finalmente hay que especificar en que posición debe añadirse el filtro
- Cuando le damos al botón Añadir Regla esta se añade a la base de datos. Si la regla que hemos añadido es local, debemos apretar el botón Aplicar que hay a la derecha de la pagina para aplicar las reglas al servidor.



RUTAS LOCALES

· Esta pagina nos permite añadir rutas al servidor local para interconectar redes. Estas rutas también se añadirán a los routers que se conecten para que sepan que tienen que pasar por el servidor para llegar a esa red.

- Para añadir una ruta se debe:
 - Poner la IP de la red/host que queremos definir en la ruta así como la mascara de red que tiene.
 - Especificar de que tipo es la puerta de enlace para llegar hasta esa red. La puerta de enlace puede ser del tipo IP o bien un Alias que tengamos añadido.
 - Finalmente hay que escoger cual es la Puerta de enlace de la red



SAIWALL

ADMINISTRACIÓN DE LOS NATS LOCALES

· Esta pagina sirve para añadir NATs en las iptables. Los NAT sirven tanto para redirigir conexiones como para interconectar redes haciendo Routing. Para poder añadir un NAT se debe:

- Escoger el tipo de NAT que queremos.
- DNAT se utiliza para redireccionar conexiones y SNAT para enmascarar conexiones para interconectar redes.
- Una vez seleccionado el tipo debemos elegir el origen, destino y los protocolos que queremos Natear.



ID	Nombre	Tipo	Protocolo	Origen	Destino	Acción	Estado
1
2
3
4
5
6
7
8
9
10

RUTAS REMOTAS

- Se utiliza para añadir rutas que se encuentran en los routers remotos.
- Primero se escoge el router donde añadir la ruta.
- Después se pone la IP de la red/host que queremos definir en la ruta así como la mascara de red que tiene.
- Finalmente hay que escoger cual es la Puerta de enlace de la red.

NAT REMOTO

- Nos permite añadir reglas NAT a un router remoto. El procedimiento es el siguiente:
- Escoger el router al que queremos añadirle el NAT.
- Escoger el tipo de NAT que queremos. DNAT se utiliza para redireccionar conexiones y SNAT para enmascarar conexiones para interconectar redes.
- Una vez seleccionado el tipo debemos elegir el origen, destino y los protocolos que queremos natear.

CONFIGURACIÓN DE INTERFACES

- Esta pagina permite modificar la Configuración IP de las 6 interfaces físicas del servidor y de la Interface Bridge.

SAIWALL

ADMINISTRACIÓN DE USUARIOS

Desde esta pagina se pueden añadir, eliminar y modificar los usuarios que tienen acceso a la pagina de administración del Saiwall.

De los usuarios se puede escoger el nombre, contraseña, idioma por defecto en la web y rol dentro de la pagina.

ADMINISTRACIÓN DE ROLES DE USUARIO

Aquí se pueden crear, modificar y eliminar roles de usuario. Un Rol contiene todas las funcionalidades para las cuales un usuario tiene permiso, así como los grupos/subgrupos de la VPN que puede ver/administrar.

ADMINISTRACIÓN DE IDIOMAS

Desde esta pagina se pueden añadir, clonar, modificar y eliminar traducciones.

Las traducciones hacen que la pagina de administración del Saiwall sea Multi-idioma.

ADMINISTRACIÓN SERVIDOR VPN

Desde esta pagina se pueden modificar varias variables del servidor VPN. Se puede modificar:

- Rango de las VPN
- El ultimo Byte por defecto de la IP de los routers
- Servidor de Configuración
- Nombre del Cliente y de los certificados digitales
- Servidores VPN Disponibles.



ADMINISTRACIÓN ALIASES IP

Desde esta pagina se añaden y modifican los Alias de las IP. Estos alias sirven para referirse a PCS sin tener que recordar la IP o PCS que pueden ir cambiando de IP.

ADMINISTRACIÓN DE GRUPOS DE ALIAS IP

Desde esta pagina se añaden y modifican los Grupos de Alias de IP. Estos alias sirven para referirse a grupos de PC sin tener que recordar las IPS o PCS que pueden ir cambiando de IP.

email: ventas@saimasistemas.com
email: info@saimasistemas.com
Calle Varsovia 115-117, Local 19
08206 Sabadell - Barcelona
Tel.: 902.36.58.96
www.saimasistemas.com