WE MAKE **COMMUNICATIONS EASY**

SAIWALL

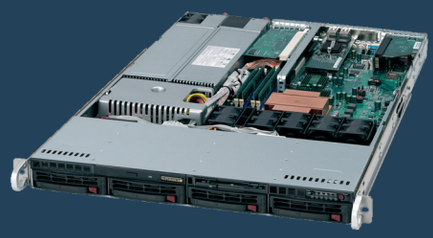
SAIMA Sistemas Global VPN Manager

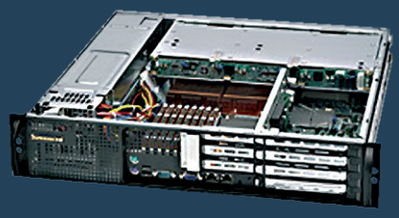
SAIMA sistemas

SAIWALL

In order to offer a better service, SAIMA SISTEMAS places at the client's disposal the SAIWALL "global VPN manager" for the VPN connection with national and international delegations or remote national and international users with connection to the Internet.
This management platform allows all those clients who want it to join all nodes of their network with a cost-cutting (reduction) and with total scalability, further delegations can be added as their enterprise grows without the need of investment of new equipments.

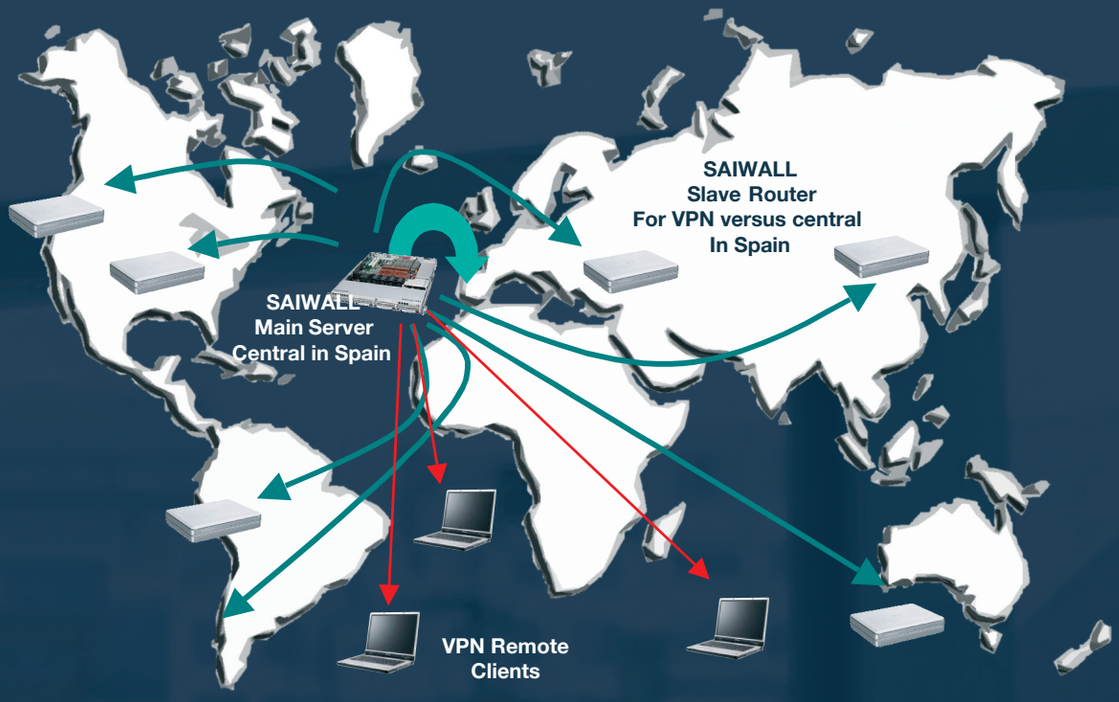
Our network connection proposal (i.e. offices or delegations) is 100% independent from the supplier as well as of the type of connection to the Internet. For example, if your office is connected to the Internet with an ADSL line, you will be able to use the internet access exactly the same way as now. Simultaneously this connection will be valid for a secure VPN connection to the other offices.





SAIWALL Server Main Server
With Supermicro 1U,2U,4U

SAIWALL Slave Router



SAIWALL

SAIWALL

The SAIWALL central server includes an SPI (Stateful Packet Inspection) Firewall based on Linux. This system allows controlling the traffic by ports, IP directions, subnets, as well as blocking or accepting the traffic in the filters. The system is designed for easy and centralized management of filters and firmwares globally, as well as by groups, subgroups or individuals.

The system is based on a virtual private network created between the remote points and the client's central. It is created with the SSL VPN by UDP security protocol by using 2048 bit security certificates. For the encryption AES with 128bit symmetric keys is used which are automatically updated every hour.

The system supports any kind of Routing protocol. It is designed for constant growing networks.

The system allows functionabilities adaptation according to the client's needs. For example, protocols and own applications is supported.

SYSTEM BENEFITS

Centralized installation / Proprietary Self Configuration System.

Centralized management of firewall, which allows firewalling the delegations groups, subgroups or individuals from the central SAIWALL.

Automatic Management of the Slave Routers Firmware.

No need to update or reconfigure Adsl routers.

It allows Load Balancing in the central SAIWALL equipment in order to upgrade the bandwidth easily (i.e. to use 2 Adsl + 1Point-to-point + Radio Link, etc. with fixed IPS).

It allows SAIWALL-SR CLUSTER in each delegation + Load Balancing like the central server.

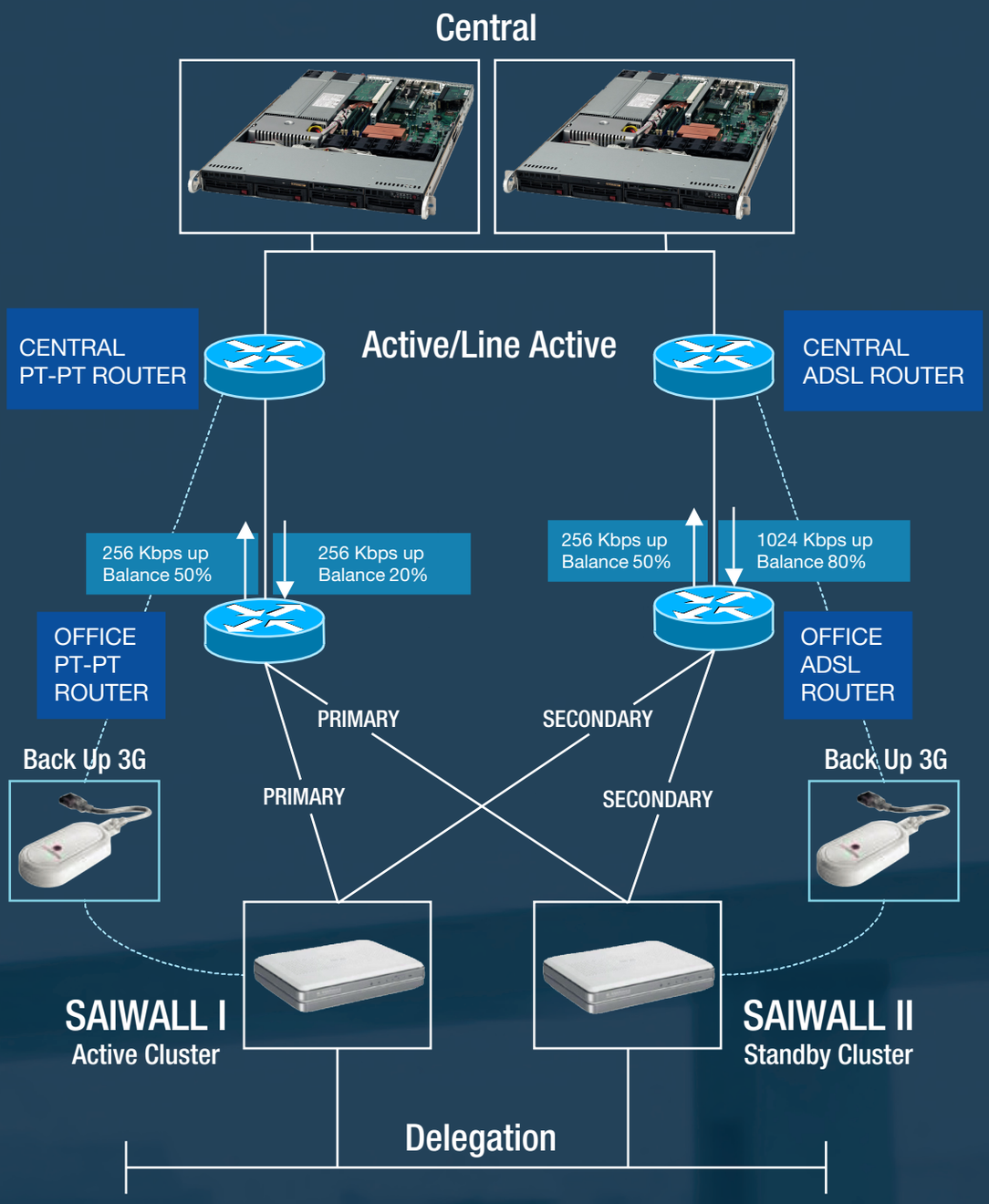
No need of fixed IPS in the delegations. The system also works with dynamic IPS, so that fixed IP costs are saved.

The Saima Sistemas WISE system manages in an intelligent, automated way the percentage of volume of flow used for the upstream and downstream of the lines data flow through an ACTIVE– ACTIVE system.

High security VPN which prevents any kind of SPOOFING attack either at destination or source.

SAIWALL

Saima Sistemas WISE data flow System



SAIWALL

COMPARISON WITH OTHER VPN SOLUTIONS

	VPN SAIWALL	VPN INTERNET SUPPLIER (1)	VPN HARDWARE (2)	NO VPN (3)
FIXED IP OBLIGATORY AT DELEGATION	☒	☑	☑	☑
FIXED CENTRAL IP	☑	☒	☑	☑
MANAGEMENT				
FIREWALL MANAGEMENT	☑	☒	☑	☑
CENTRALIZED FIREWALL MANAGEMENT (5)	☑	☒	☒	☒
MULTILANGUAGE	☑	☒	☒	☒
CENTRALIZED INSTALLATION (5)	☑	☒	☒	☒
AUTOMATIC UPDATE OF THE DELEGATION EQUIPMENTS	☑	☒	☒	☒
RECONFIGURATION OBLIGATION OF THE SUPPLIER'S ROUTER	☒	☒	☑	☑
CONNECTIVITY				
LOAD BALANCING CENTRAL VPN	☑	☒	☒(4)	☒
LOAD BALANCING DELEGATION VPN	☑	☒	☒(4)	☒
LOAD BALANCING CENTRAL INTERNET	☑	☒	☒(4)	☒
LOAD BALANCING INTERNET DELEGACION	☑	☒	☒(4)	☒
CENTRAL CLUSTER	☑	☒	☑(4)	☒
DELEGATION CLUSTER	☑	☒	☑(4)	☒
ANY INTERNET CONNECTION	☑	☒	☒	☑
3G/UMTS	☑	☒	☒	☑
BACKUP 3G/UMTS	☑	☒	☒	☒
UNIFIED AND CENTRALIZED CONFIGURATION (5) OF THE CENTRAL CLUSTERS	☑	☒	☒	☒
UNIFIED AND CENTRALIZED CONFIGURATION (5) OF THE DELEGATION CLUSTERS	☑	☒	☒	☒
WISE SYSTEM, ALLOWS DEFINING % OF LINES DATA FLOW DEPENDING ON THE NEED	☑	☒	☒	☒

NOTE: ☑ = YES
☒ = NO

SAIWALL

	VPN SAIWALL	VPN INTERNET SUPPLIER (1)	VPN HARDWARE (2)	NO VPN (3)
SECURITY				
SECURITY AGAINST SPOOFING ATTACKS (ID THEFT)	☑	☑	☑	☒
HIGH SECURITY AES 128 BIT ENCRYPTION PROTOCOL	☑	☒	☒	☒
COMPATIBILITY WITH ALL ROUTERS TO BE USED SSL	☑	N/A	☒	N/A
AUTOMATIC ENCRYPTED PASSWORD UPDATE EVERY HOUR	☑	N/A	☒	N/A
UDP ENCAPSULATED TUNNEL	☑	N/A	☑	☒
FIREWALL				
CENTRALIZED MANAGEMENT OF ROUTES (5)	☑	☒	☒	☒
CENTRALIZED MANAGEMENT OF NAT	☑	☒	☒	☒
CENTRALIZED MANAGEMENT OF ROUTES	☑	☒	☒	☒
DATA PACKET FLOW MONITORING	☑	☒	☑	☒
LATENCIE MONITORING	☑	☒	☒	☒
BANDWIDTH MONITORING	☑	☒	☑	☒
LINE MONITORING	☑	☒	☑	☒
GROWTH SCALABILITY				
UNLIMITED NATIONAL DELEGATIONS	☑	☑	☒	☑
UNLIMITED INTERNATIONAL DELEGATIONS	☑	☒	☒	☑

NOTE: ☑ = YES
☒ = NO

(1) VPN Internet Supplier: Telecommunications Company I.e. Telefónica (netlan), BT, C&W
(2) VPN Hardware: Generic VPN Router Equipments I.e. Cisco, Zyxel
(3) No VPN: Direct connection without VPN.
(4) Solutions which are handled by a minority of the equipments suppliers, but which have very high prices.
(5) Centralized management: This function allows groups, subgroups or individuals management from the Central control panel of the delegations equipments.

SAIWALL

COSTS	VPN SAIWALL	VPN INTERNET SUPPLIER (1)	VPN HARDWARE (2)	NO VPN (3)
HARDWARE COSTS	☑	☒	☑	☒
HARDWARE AMORTIZATION	☑	☒	☑	N/A
DELEGATION'S VPN MONTHLY COSTS	☒	☑	☒	☒
DELEGATION'S FIXED IP MONTHLY COSTS	☒	☑	☑	☑
CENTRAL MONTHLY COSTS	☑	☑	☒	☒
SLA POSSIBILITY	☑	☑	☒	☒
8/5 SUPPORT	☑	☑	☑	☒
POSSIBILITY OF 24/7 SUPPORT	☑	☑	☒	☒
INCIDENCE MANAGEMENT	☑	☑	☒	☒

NOTE: ☑ = YES
☒ = NO

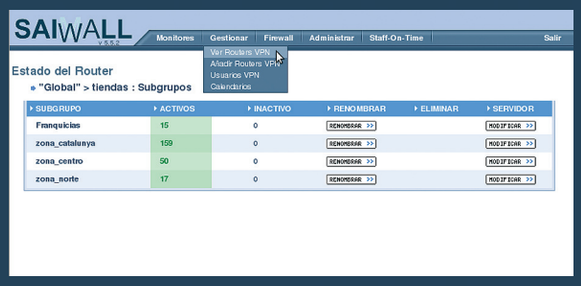
SAIWALL

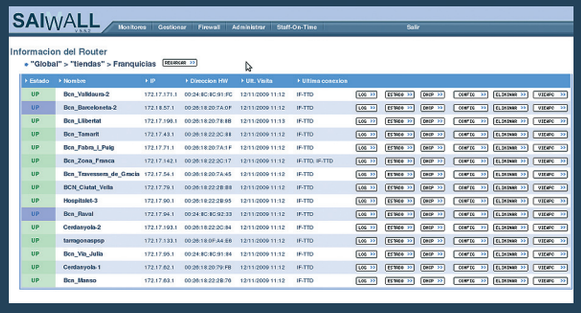
INTERFACE FEATURES

SAIWALL SR REMOTE EQUIPMENTS STATE

· The interface shows the groups and subgroups which form the VPN. It is possible to navigate them by clicking on their name. If we enter as an administrator, then this section allows us to execute following actions on the groups / subgroups:

- Control the on and/or off routers.
- Modify names.
- Erase empty groups and subgroups.
- Modify the VPN server of a group/subgroup by default.





INTERFACE VPN USERS

· It manages VPN users who are connected to the system. Here we can see each user: details, IP of the VPN, and so on. We can also gain access to the state of connection and to the connection Log.

ADDING SAIWALL-SRs

· It is used to add Saiwall-SR to the system. It is done as follows:

In MAC we select the MAC address of the Saiwall-SR we want to add, we give it a NAME, and we select a group / subgroup for it. If we lack the group or subgroup that we need, we can create a new one with the right side buttons.

We choose the IP that the saiwall-sr will have in the VPN. We can choose whether to force an IP Configuration of the WAN in the router. Afterwards, we choose the DHCP, DNS and WINS parameters according to the needs for that network. Finally, we decide whether the router will allow access through Wireless or not. Once these parameters are configured, we click the “add” button.

SAIWALL

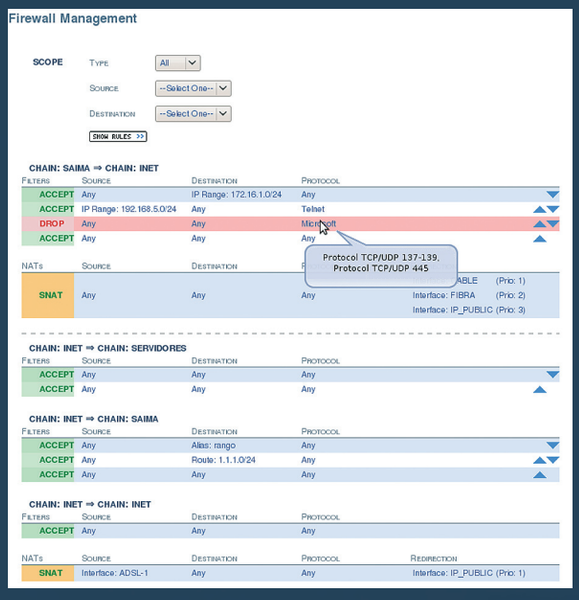
ADDING VPN USERS

· It is used to add users to the VPN server. These users get connected directly to the client's SAIWALL VPN Server.

FILTERS ADMINISTRATION

· In this section we can filter all connections that take place in our network, either at the remote VPN routers or those that are sent through the central server. With that aim we should:

- Choose a 'Source' and a 'Destination' for the packets.
- Select the protocol where we want to add the filter.
- Define what kind of filter we want to add. If we want it to be a permissive one, then we must select ACCEPT. Otherwise, we must select DROP.
- Finally we must specify in which position should the filter be added.
- When we press the Add Rule button, this is added to the data base. then we must press the Apply button that we find at the right hand side of the page in order to apply the rules .



LOCAL ROUTES

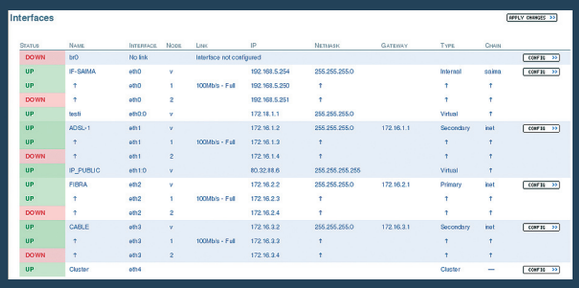
· This section allows us to add routes to the local server in order to interconnect networks. These routes will also be sent automatically to the routers that are connected to the VPN for them to be able reach that network.

· In order to add a route we must:

- Place the network / host IP that we want to define in the route, as well as the network mask that it has.
- Specify what sort of gateway is used to reach that network. Gateways can be whether an IP address , or an Aliaswe have added.
- Finally the network's gateway must be chosen.

SAIWALL

LOCAL NATS ADMINISTRATION



· This section is used to add NATs . NATs are used to redirect connections from the public IP addresses to a server in private network. In order to add a NAT we must:

- Choose the type of NAT that we want.
- A DNAT is used to redirect incoming connections, while the SNAT is used to mask outgoing connections to internet .
- Once we have selected the type we must choose source, destination and the NAT protocols.

REMOTE ROUTES

· It is used to add routes which are located in remote routers.

- First of all, we choose the router where we want to add the route.
- Secondly, we place the network/host IP that we want to define in the route as well as the network mask that it has.
- Finally we have to choose the network gateway.

REMOTE NAT

· It allows us adding NAT rules to a remote router. The procedure is the following:

- To choose the router where we want to add the NAT.
- To choose the type of NAT that we want. A DNAT is used to redirect connections, while the SNAT is used to mask connections to interconnect networks.
- Once we have selected the type we must choose the source, the destination and the NAT protocols.

INTERFACES CONFIGURATION

· This section allows to modify the server IP Configuration and the Bridge configuration of all physical and virtual Interfaces.

SAIWALL

USERS ADMINISTRATION

From this section we can add, eliminate or modify the users who have access to the Saiwall's administration page.
User's name, login, web's language by default and role in the web page can be chosen.

USER'S ROLES ADMINISTRATION

Here user's roles can be created, modified or eliminated. A role has all functionalities for which a user has permission. It also can be done with the VPN groups / subgroups that can be seen / administered.

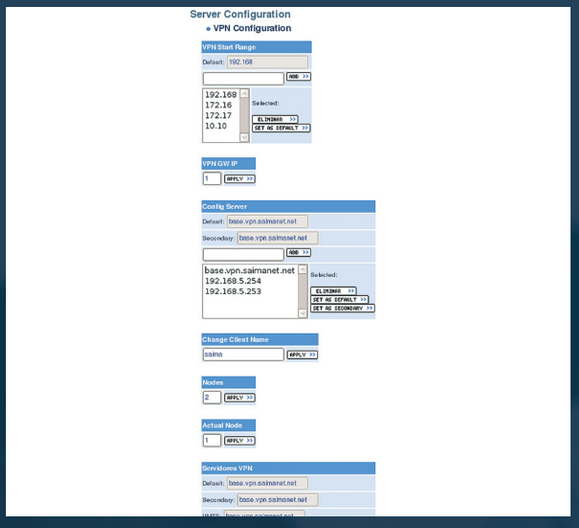
LANGUAGE ADMINISTRATION

From this section translations can be added, copied, modified and removed.
Translations make Saiwall's administration a Multi-language system.

VPN SERVER ADMINISTRATION

From this section several VPN server variables can be modified. We can modify:

- VPN Range
- Last Byte by default of the IP routers
- Configuration server
- Client's and digital certificates name
- VPN Servers Available



IP ALIAS ADMINISTRATION

From this section IP Aliasescan be added and modified. These aliasesare used to refer to network equipment without having to remember the IP.

IP ALIAS GROUPS ADMINISTRATION

From this section IP AliasGroups are added and modified. These alias groups are used to refer to Aliases In a grouped manner to make firewall administration easier.

CORPORATIVE CLIENTS

email: ventas@saimasistemas.com
email: info@saimasistemas.com
Calle Varsovia 115-117, Local 19
08206 Sabadell - Barcelona
Tel.: +34.902.36.58.96
www.saimasistemas.com