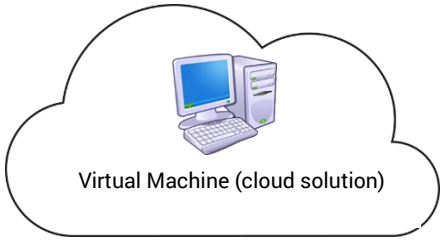
VPN CONCENTRATOR FOR INDUSTRIAL SCADA SYSTEM

The range of VPN SIG servers is used to interconnect remote IP devices via the Internet, an Intranet or a cellular network providing a high level of availability and security.



SECURITY

The SIG VPN concentrator manages from 100 up to 500 VPN connections with IPSec or OpenVPN (via X509 certificates or shared key). A Virtual Machine release of the SIG allows to offer up to 1,000 VPN.

REDUNDANCY

The server is a critical part of a SCADA.Therefore, two SIG servers can be placed in redundancy; in case of default of the first, the second takes over.

VIRTUAL MACHINE

Etic Telecom does offer a turnkey solution of the SIG SW porting onto the HW platform of the customer.

MARKETS

- **Water**: Water distribution and management
- **Energy**: Dam, pipe line, Wind turbine, photovoltaic…
- **Industry**: Quarry, mines, building, factory
- **Transport**: Subway, canals, port, airport, road, traffic control …
- **Infrastructure**: Lighting, Video, display panels …

CHARACTERISTICS

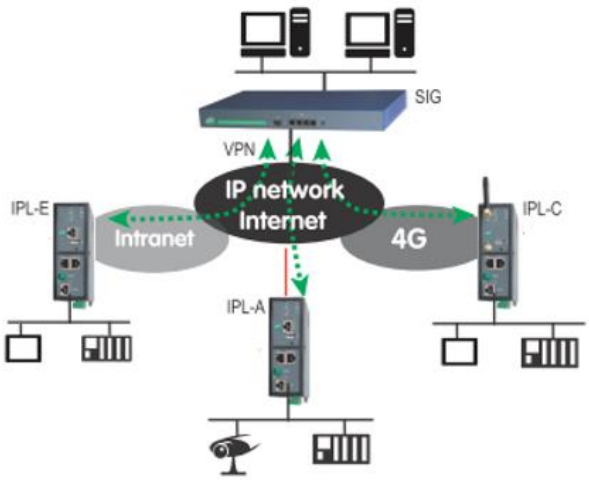
- VPN OpenVPN / SSL server and client
- VPN IPSec
- Up to 500 VPN (depending on model)
- Redundancy
- Modularity (addition of a second SIG to aggregate the number of VPN tunnels)
- Firewall (Stateful Packet Inspection)
- IP router
- Remote Access Server capability
- Secured Portal for Smartphone, Tablet, PC

SIG

SIG FAMILY FOR REMOTE SCADA

OPENVPN OR IPSEC VPN SERVER

The SIG router can collect up to 500 VPN tunnels (mix of OpenVPN & IPSec tunnels possible) across a factory IP network or Internet.
The transfer rate is up to 100 Mb / s which makes it a suitable tool for systems made of several hundred sites.

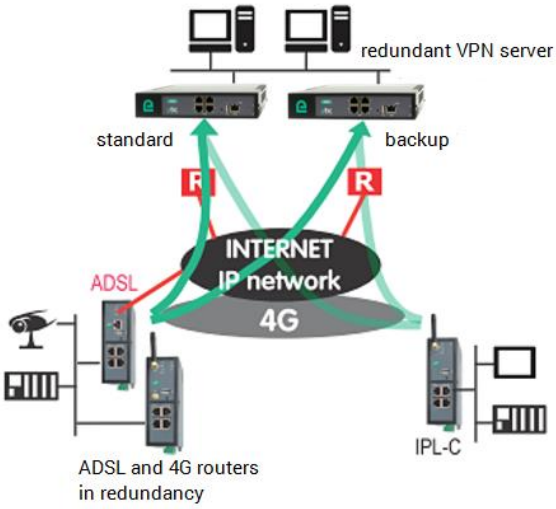


REDUNDANCY

Because it is the network node, the SIG router is a critical equipment: His failure interrupts the operation of the system.

This is why it is able to operate redundantly with another identical equipment.

The redundancy algorithm overcomes the failure of one of the VPN server and the failure of the Internet connection.



LOAD BALANCING

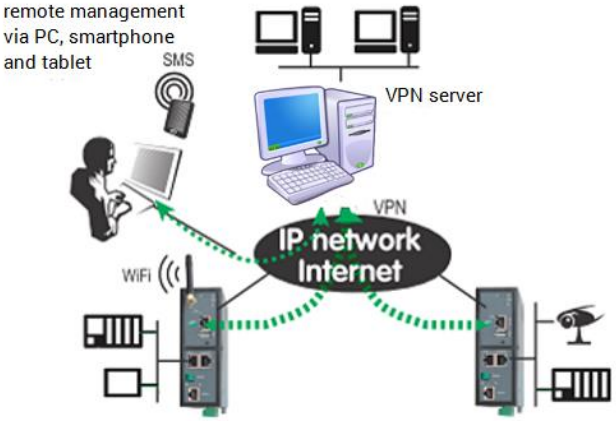
The SIG allows you to build a scalable architecture. A SIG-E-400 or A-400 supports up to 100 VPN tunnels. Beyond 100 tunnels, simply add a second SIG.

REMOTE ACCESS SERVER FOR SMARTPHONE, TABLET OR PC

The SIG server is also aimed for remote access server for remote operations.

Once authentified, a remote user access only to authorized facilities.

When logging with a smartphone, tablet or PC, an individualized directory of machines appears, a simple click is requested to access to embedded servers in a network device.






SIG	SIG-E	SIG-A	SIG-V1	SIG-VM
WAN network	Ethernet	ADSL	Ethernet	Ethernet
LAN RJ45	4	4	4	Non applicable
Number of VPN tunnels	100	100	500	1000
Throughput (Mbps)	50	50	100	Depending on the HW
Dimensions	45 x 240 x 240 mm (h, l, p)	45 x 240 x 240 mm (h, l, p)	45 x 430 x 250 mm (h, l, p)	Non applicable
Weight	1,3 Kg	1,3 Kg	5,2 Kg	Non applicable
Temperature	-40°C /+ 60°C	-40°C /+ 60°C	0°C /+ 40°C	Non applicable
Humidity	5 up to 95 %	5 up to 95 %	5 up to 95 %	Non applicable
Consumption	110/230VAC – 10W	110/230VAC – 10W	110/230VAC – 60W	Non applicable
Tropicalization	Option	Option	Non	Non applicable
Protection	IP20	IP20	IP20	•

SIG

SIG FAMILY FOR REMOTE SCADA

General Characteristics

EMC	• ESD : EN61000-4-2 : Discharge 6 KV • Radiation: EN61000-4-3 : 10V/m<2GHz • Transients : EN61000-4-4 • Choc : EN61000-4-5 : 4KV ligne / ground
Electrical security	EN 60950
Hazardous substances	2002/95/CE European standard «RoHS»

IP Router IP/management

IP Router	• Static routes • RIP V2 on LAN & WAN interface • Source address translation (NAT, SNAT) • Destination address translation (DNAT)
IP @	• WAN : DHCP client or @ fixed IP • LAN : DHCP client or server @ fixed IP
DNS	• WAN interface: DynDNS Compatible • WAN interface: NoIP Compatible • LAN interface: DNS Relay & server
Management	SNMP V1/V2/V3 MIB II & Traps
Qualité de service	QoS DiffServ
Redundancy	VRRP RFC3768

VPN OpenVPN

Server	• 4 independent VPN servers • For each server : TCP & UDP • Port number configurable • Route transmission at VPN connexion
Authentication	Certificat X509
Encryption	3DES & AES 128-192-256 & Blowfish
Hash	MD5 & SHA-1

VPN IPSec

Authentication	• Preshared key • Certificat X509 • Main mode or aggressive mode
Encryption	3DES & AES 128-192-256
Hash	MD5 & SHA-1

FireWall

Type	• Stateful packet inspection
Strategy	• Multicast filtering • Prevention of attacks "Deny of service"
IP address filtering	• Filtering @IP and source & destination ports • 50 rules

Remote Access Server

Users	• List of 25 users • Identification with Login + password
Access rights	Individualized access to equipment via login and PWD
https Portal	Provides access to embedded html server using a smartphone, tablet or PC
connection	VPN PPTP or L2TP/IPSEC or TLS or HTTPS

Configuration and System

Diary	• Horodating • Events: Connection-disconnection. VPN, alarms
Log	• Horodating • Events: Connection-disconnection. Reset, alarms
Configuration	HTTPS/HTTP

RoHS CE MADE IN FRANCE

Made in France by ETIC TELECOM