SIG

Serveur VPN - Routeur - Firewall

GUIDE UTILISATEUR

La famille de Serveurs VPN industriels SIG est fabriquée par

ETIC TELECOM

405 rue Lavoisier
38330 MONTBONNOT SAINT MARTIN
FRANCE

En cas de difficulté dans la mise en œuvre du produit, vous pouvez vous adresser à votre revendeur, ou bien contacter notre service support :

TEL : + (33) (0)4-76-04-20-05
E-mail : hotline@etictelecom.com
web : www.etictelecom.com

DECLARATION OF CONFORMITY

The manufacturer, ETIC Telecom – 13 chemin du vieux chêne – 38240 Meylan – France, Hereby declares under sole responsibility that the listed devices conform to

- the Radio Equipment Directive (RED) 2014/53/UE,
- the Restriction of the use of certain Hazardous Substances (RoHS) Directive 2011/65/UE.

Type of device: VPN Server
Models:
SIG-E-400, SIG-A-400, SIG-EC-400

The harmonized standards to which these devices comply are:

Standard	Title
EN 61000-6-2 2006	Immunity: EN61000-4-2 Electrostatic Discharge EN61000-4-3 RF Radiated Immunity EN61000-4-4 EFT/Burst Immunity EN61000-4-5 Surge Immunity EN61000-4-6 RF Conducted Immunity EN61000-4-8 Power Frequency Magnetic Field Immunity
EN 61000-6-4 2007 A1/2011	Emission: EN55022 Radiated and conducted emission
EN 301 489-1 V1.9.2 EN 301 489-3 V1.6.1 EN 301 489-7 V1.3.1 EN 301 489-17 V2.2.1 EN 301 489-24 V1.5.1	Radio - EMC
EN 301 511 V9.0.2 EN 301 908-1 V6.2.1 EN 301 908-2 V6.2.1 EN 300 328 V1.9.1 EN 301893 V1.8.1	Radio - Spectrum
EN 60950-1/A2 2014 EN 62311 2008	Safety and Health

Date : 18th October 2017

Philippe Duchesne
Technical Director

PRESENTATION 7

1 But du document 7
2 Identification des produits 7
3 Spécifications 8
4 Présentation des produits 11
4.1 Applications 11
4.2 Fonctions principales 12

INSTALLATION 15

1 Description 15
1.1 Dimensions 15
1.2 Face avant 15
1.3 Face arrière 16
1.4 Connecteurs 16
1.5 Boutons poussoirs 17
1.6 Voyants 18
2 Instructions de sécurité 19
3 Ventilation 19
4 Mise à la terre 19
5 Raccordement à la ligne ADSL 20
6 Raccordement au réseau cellulaire 21
6.1 Contrôles avant installation 21
6.2 Antenne 21
6.3 Déport de l'antenne 21
6.4 Choix de l'abonnement au réseau cellulaire 21
6.5 Installation ou extraction de la carte SIM (ou des 2 cartes SIM) 22
6.6 Contrôle de la conformité de la connexion 23

PREPARER LE PARAMETRAGE 25

1 Connexion du PC en vue de la configuration 25
1.1 Introduction 25
1.2 Première configuration 26
1.3 Modification ultérieure de la configuration 26
2 Accès au serveur d'administration par l'interface WAN 27
3 Opérations avec HTTPS 27
4 Retour temporaire à la configuration usine 28
5 Restitution de la configuration usine 28
6 Protection de l'accès au serveur d'administration 29
7 Etapes de configuration 29

PRESENTATION

1 But du document

Le présent document décrit la mise en œuvre de la famille de serveurs VPN industriels SIG présentés sous la forme d'un boîtier matériel, à l'exclusion des serveurs VPN SIG virtuels dont la mise en œuvre est décrite dans une documentation à part.

Dans la suite du document ces produits sont désignés simplement par le mot « SIG ».

2 Identification des produits

Cette famille de serveurs VPN industriels se compose de ces modèles :
SIG-E-400, SIG-A-400, SIG-EC-100

Les principales particularités sont résumées ci-dessous :

Modèles			
SIG-	E-400	A-400	EC-400
WAN Ethernet	•		•
WAN ADSL		•	
WAN Cellulaire (-HG, -HW : 3G+, -LE : 4G)			•
LAN Ethernet 10-100 Mb/s	4	4	4
USB	•	•	•
Redondance de liaison			•
Alimentation VAC	110-230	110-230	110-230
2 lecteurs SIM			•

3 Spécifications

Caractéristiques générales	
Dimensions	Avec pied : 50 X 220 X 220 mm (h, l, p) Sans pied : 44 X 220 X 220 mm (h, l, p)
Poids	Max 0.65 kg
Boitier	Métallique IP20 – IEC60529
Température	Stockage : -40°/ + 85°C Fonctionnement : -20°/ + 60°C (sans ventilateur)
Humidité	10 à 95 % relative (sans condensation)
Alimentation	110 à 230 VAC
Consommation	SIG-E : 2W SIG-A, SIG-C et SIG-EC : 5W
CEM	Immunité EN61000-6-2 : EN61000-4-2 : ESD : 4 kV contact – 8kV air EN61000-4-3 : RF rayonnées : 10V/m < 2 GHz EN61000-4-4 : Burst EN61000-4-5 : Surge : 4KV line / earth EN61000-4-6 : RF conduites EN61000-4-8 : Champs magnétiques Emission EN61000-6-4 : EN 55022 : RF conduites et rayonnées
Sécurité électrique	EN 60950-1
Substances dangereuses	2011/65/UE (RoHS) REACH

Réseau WAN	
Ethernet	RJ45 Auto : 10/100 full & half duplex MDI/MDI-X
ADSL	ADSL2+ et RE-ADSL ITU G992.5 (ADSL2+ et Reach Extended ADSL) Débit max : UL : 1 Mbps, DL : 24 Mbps PPPoE : PPP over Ethernet PPPoA : PPP over ATM EoA : Ethernet over ATM RFC2684 Bridged IPoA : Routed IP over ATM, RFC2684 Routed
4G/3G+	-LW : 4G LTE monde Bandes LTE-TDD : B34, B38, B39, B40, B41 Bandes LTE-FDD : B1, B2, B3, B4, B5, B7, B8, B12, B13, B18, B19, B20, B25, B26, B28, B66 Bandes WCDMA : B1, B2, B4, B5, B6, B8, B19 Bandes GSM : 850/900/1800/1900 -LE : 4G LTE Europe Bandes LTE : B1, B2, B3, B4, B5, B7, B8, B20 Bandes WCDMA : B1, B2, B5, B8 Bandes GSM : 850/900/1800/1900 -CH : 4G LTE Chine Bandes LTE : B1, B3, B8, B38, B39, B40, B41 Bandes WCDMA : B1, B5, B8, B9 Bandes GSM : 900/1800 -HG : 3G+ HSPA monde (sauf Amérique du nord) Bandes WCDMA : B1, B2, B5, B8 Bandes GSM : 850/900/1800/1900 -HW : 3G+ HSPA monde Bandes WCDMA : B1, B2, B4, B5, B6, B8, B19 Bandes GSM : 850/900/1800/1900 Puissance d'émission max LTE : 25 dBm Puissance d'émission max WCDMA : 25 dBm Puissance d'émission max GSM 850/900 : 33 dBm Puissance d'émission max GSM 1800/1900 : 31 dBm Débit max LTE : UL @ 50 Mbps et DL @ 100Mbps Débit max HSPA : UL @ 5,7 Mbps et DL @ 21 Mbps Débit max EDGE : UL @ 237 Kbps et DL @ 237 Kbps Connecteur d'antenne type SMA femelle 2 porte-cartes mini SIM selon modèle

Réseau LAN	
Ethernet	RJ45 : 4 ports Auto : 10/100 full & half duplex MDI/MDI-X

PRESENTATION

Routage / @IP /	
Routage IP	Tables de routage Routes statiques RIP ou OSPF Translation d'adresses (DNAT, SNAT, NAT 1:1)
Attribution d'@IP	Interface WAN : DHCP client ou IP fixe Interface LAN : DHCP serveur
DNS	Interface WAN : compatible DYNDNS, No-IP ou ETIC DNS Interface LAN : relai & serveur DNS
Redondance	Protocole VRRP RFC 3768 WAN de backup sur certains modèles

Sécurité	
Tunnel VPN	OpenVPN (TLS/SSL), IPSEC, L2TP/IPSEC, PPTP Clé partagée ou Certficat X509 Cryptage 3DES & AES 128-192-256 Authentification : MD5 & SHA-1 Jusqu'à 100 tunnels VPN (mix OpenVPN IPSEC possible)
Firewall	Stafeful packet inspection (SPI : 50 règles) Filtrage @ IP et n° de ports
Accès distant	Jusqu'à 25 utilisateurs Login, Mot de passe et certificat (optionnel) Droits d'accès aux équipements individualisés
Journal	Horodaté Evènements : connexion, restart, alarmes

Divers	
SNMP	MIBs supportées : RFC1213-MIB (MIB-2) ADSL-LINE-MIB Traps SNMP
Configuration	Serveur web
Management	Sauvegarde des configurations Reset produit pour retour à la configuration usine

4 Présentation des produits

Le SIG est à la fois un serveur VPN, un routeur, un firewall et un serveur d'accès distant pour les systèmes industriels.

Il permet de réaliser des systèmes de télé contrôle entre un réseau de supervision et des équipements distants (systèmes mobiles, automatismes, équipements de mesure...).

Il intègre selon le modèle :

- SIG-E : Une interface WAN Ethernet
- SIG-A : Un modem ADSL
- SIG-EC : Une interface WAN Ethernet et modem cellulaire 3G/4G

4.1 Applications

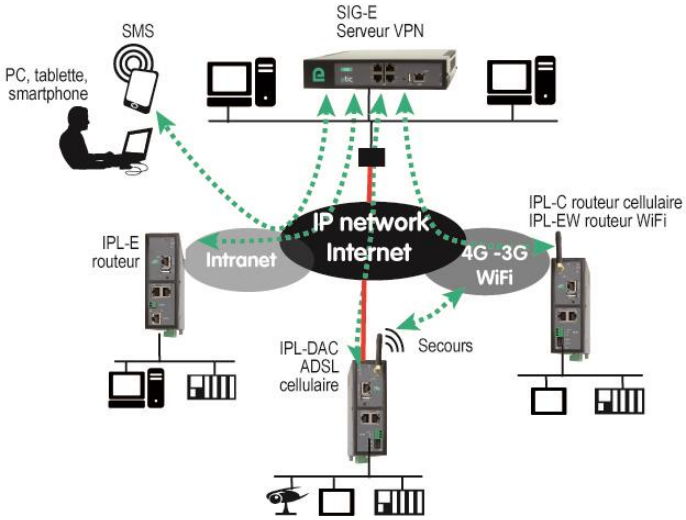
Système de télé contrôle de haute sécurité jusqu'à 100 sites
Le SIG-E permet d'interconnecter 100 sites équipés de routeurs IP au moyen de VPNs en offrant un niveau élevé de sécurité.

Haute disponibilité
Le SIG-E prend en compte les chemins de secours ; un site éloigné peut être équipé d'un routeur ADSL avec secours 3G, par exemple ; en cas de défaillance de la ligne ADSL, le VPN sera rétabli par le réseau cellulaire.

De plus, 2 SIG-E peuvent être placés en redondance l'un de l'autre; en cas de panne de l'un, l'autre prend le relais automatiquement.

Serveur d'accès distant pour la télé-exploitation
Un opérateur autorisé peut se connecter à distance à l'un quelconque des équipements du système au moyen d'un PC, d'une tablette ou d'un smartphone.
Ses droits peuvent être limités en fonction de son identité.

Filtrage des échanges (Firewall)
Le SIG-E placé entre deux réseaux filtre les trames IP et concourt à la sécurité du système.



4.2 Fonctions principales

VPN IPSec et OpenVPN pour la sécurité
La connexion VPN garantit un niveau élevé de performance et de sécurité :

Transparence : Etabli entre deux routeurs, le VPN assure l'interconnexion transparente des deux réseaux en sorte que toute machine de l'un des réseaux peut communiquer avec une machine de l'autre réseau.

Authentification : Le routeur qui établit le VPN est authentifié par celui qui l'accepte et toute autre connexion est rejetée.

Confidentialité : Les données sont cryptées.

Le SIG permet d'établir simultanément des tunnels VPN de type IPSec et OpenVPN (100 au total).

Bien que le SIG soit conçu pour réaliser la fonction de concentrateur de VPNs (on dit aussi serveur VPN), il peut aussi bien se comporter en serveur ou en client VPN.

Le SIG contient 4 modules serveurs VPN OpenVPN indépendants ; chacun de ces modules OpenVPN peut être réglé différemment pour répondre aux nécessités techniques (période de rafraichissement des clés, type de cryptage …).

Le paramétrage d'IPSec peut être différent pour chaque VPN.

Ces différentes caractéristiques permettent d'accepter des VPNs OpenVPNs ou IPSec provenant de routeurs de constructeurs différents et aussi de prendre en compte des chemins de secours (backup) afin de construire des systèmes de télé contrôle de haute disponibilité.

Serveur d'accès distant pour PC, tablette et smartphone
Le SIG fait également fonction de serveur d'accès distant permettant à un groupe d'utilisateurs distants enregistrés dans la liste d'utilisateurs d'accéder aux machines du réseau avec des droits maîtrisés.

De plus, le portail HTTPS accueille les utilisateurs de PC, tablettes et smartphones en mode HTTPS pour les rediriger en sécurité vers les serveurs HTTPS ou HTML que leur identité autorise.

Routage
Le SIG offre une large gamme de solutions de routage qui peuvent être mises en œuvre selon le besoin pour assurer la communication entre les machines de chaque réseau à connecter :
Routes statiques, pour atteindre des réseaux nichés,
Translation d'adresse (NAT, DNAT, port forwarding),
Protocole automatique d'échange de table de routage (RIP),
Gestion de nom de domaine DNS et DynDNS.

Firewall
Le SIG dispose d'un firewall « SPI » qui inspecte les paquets en permanence.

Il permet de rejeter les tentatives de connexions non authentifiées sur l'Internet.

Il permet également d'attribuer des droits maîtrisés (@IP et N° de port de destination autorisés) aux trames IP reçues au travers d'un tunnel VPN.

Redondance VRRP en cas de panne du routeur :
En cas de panne, le SIG peut se déclarer en stand-by en sorte qu'un autre routeur prenne le relais avec un fonctionnement identique.

Secours automatique d'un réseau privé VPN par un réseau cellulaire
LE SIG-EC possède une interface WAN Ethernet et une interface cellulaire.
Il permet de véhiculer les données par l'interface la plus prioritaire tant qu'elle fonctionne normalement (Ethernet en général) ou bien par l'autre interface (le réseau cellulaire en général, en secours).

SNMP
Le SIG est agent SNMP; il répond à la MIB2 standard et transmet un trap SNMP lorsque des événements paramétrables surviennent.

DNS
Le système DNS permet au SIG d'établir une connexion avec un autre routeur même si l'un, l'autre ou les deux routeurs ne possèdent pas une adresse IP connue.
Le principe du DNS consiste à désigner un routeur destinataire d'une connexion par un nom de domaine (par exemple « eticelecom » est un nom de domaine) plutôt que par son adresse IP.

Serveur DHCP
Sur l'interface LAN, le SIG peut se comporter en serveur DHCP.

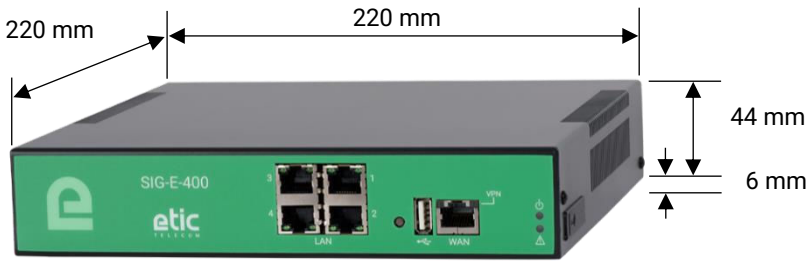
Configuration
Le SIG se configure au moyen d'un navigateur HTML (HTTP ou HTTPS).

EticFinder
Le logiciel EticFinder permet de détecter simplement tous les produits de marque ETIC connectés à un segment Ethernet pour afficher leur adresse MAC ainsi que l'adresse IP qui leur est attribuée sur le réseau.

INSTALLATION

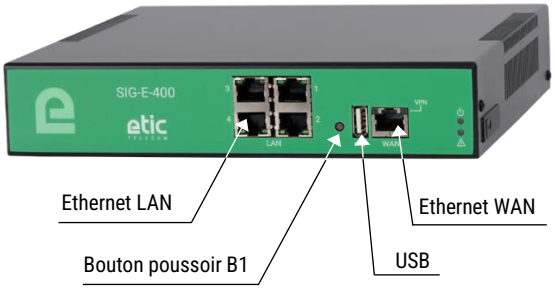
1 Description

1.1 Dimensions

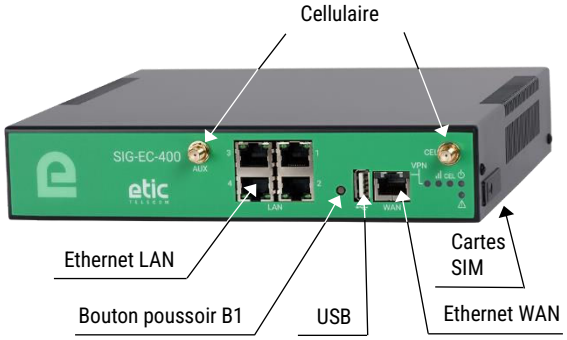


1.2 Face avant

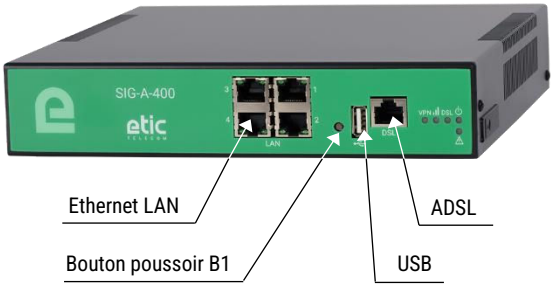
SIG-E-400



SIG-EC-400

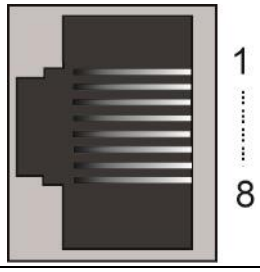


SIG-A-400

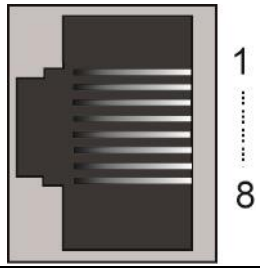


1.3 Face arrière

1.4 Connecteurs

Connecteur RJ45 Ethernet			
Broche	**Signal**	**Fonction**	**RJ45**
1	Tx +	Emission polarité +	
2	Tx -	Emission polarité -	
3	Rx +	Réception polarité +	
4	N.C	-	
5	N.C	-	
6	Rx -	Réception polarité -	
7	N.C.	-	
8	N.C.	-	

SIG-EC-400 Connecteurs d'antennes			
Antenne	**Réseau**	**Type**	**Observation**
CEL	Cellulaire	SMA femelle	3G et 4G
AUX	Cellulaire	SMA femelle	2 antennes peuvent être connectées pour améliorer la transmission 4G

SIG-A-400 Connecteur RJ45 ADSL			
Broche	**Signal**	**Fonction**	**RJ45**
1	N.C.	-	
2	N.C.	-	
3	N.C.	-	
4	TIP	Ligne ADSL	
5	RING	Ligne ADSL	
6	N.C.	-	
7	N.C.	-	
8	N.C.	-	

1.5 Boutons poussoirs

Bouton poussoir de face avant B1		
Appui sur BP	**Voyant**	**Fonction**
10 secondes	5 impulsions	La hotline d'ETIC TELECOM est autorisée à établir une connexion distante vers le SIG dans un délai de 1 heure.

Bouton poussoir de face arrière B2		
Appui sur BP	**Voyant**	**Fonction**
Pendant le fonctionnement	Clignotement rouge	Retour temporaire à la configuration Usine. (adresse IP 192.168.0.128) La configuration courante est conservée.
Simultanément avec la mise sous tension	Clignotement rouge	Retour permanent à la configuration Usine. La configuration courante est perdue sauf si elle a été sauvegardée dans un fichier.

1.6 Voyants

VOYANTS Selon modèles		
Fonction	**Voyant**	**Description**
Opération		Eteint — Hors tension Vert fixe — En fonction Vert clignotant lent — Occupé Rouge fixe — Démarrage (30s) – Sinon défaut grave matériel ou logiciel ou carte SIM absente ou media d'enregistrement absent Rouge clignotant rapide — Chargement du firmware en cours
Alarme application		Réservé
Connexion ADSL	**DSL**	Eteint — Interface ADSL désactivé Impulsion 4 s — Pas de détection de signal ADSL / Ligne non connectée Clignotant lent 2 s — Connexion en cours 1ere étape (adsl) Clignotant rapide 0,5 s — Connexion en cours 2eme étape (mot de passe et @ IP) Vert fixe — Connecté / léger clignotement en présence de données
Qualité du signal ADSL		Eteint — Pas de signal mesuré 1 impulsion — Insuffisant ou faible 2 impulsions — Suffisant 3 impulsions — Bon ou très bon signal
Connexion Cellulaire	**CEL**	Eteint — Carte SIM absente - code PIN erroné - interface cellulaire inactive Impulsion toutes les 4 s — Interface active - non connecté Clignotant lent 2 s — Connexion en cours (1ere étape) Clignotant rapide 0,5 s — Connexion en cours (mot de passe et @ IP) Vert fixe — Connecté / léger clignotement en présence de données
Qualité du signal cellulaire		Eteint — Pas de signal mesuré 1 impulsion — Insuffisant ou faible 2 impulsions — Suffisant 3 impulsions — Bon ou très bon signal
Connexion VPN	**VPN**	Eteint — Aucun VPN connecté Clignotant lent 2 s — Connexion en cours Vert fixe — Au moins un VPN connecté
Ethernet WAN	**Voyant gauche**	Eteint — Non connecté ou interface désactivée Vert — Connecté / léger clignotement en présence de données
Ethernet LAN x 4	**Voyant gauche**	Eteint — Non connecté ou interface désactivée Vert — Connecté / léger clignotement en présence de données

2 Instructions de sécurité

Le produit doit être installé par un opérateur qualifié, dans un coffret ou baie informatique assurant une enveloppe contre le feu.

Le produit doit être connecté uniquement à des équipements conformes aux normes IEC60950-1 ou IEC62368-1 respectant les classifications suivantes :

- IEC60950-1 : source à puissance limitée et circuit d'interconnexion du type TBTS – §2.2 et 2.5
- IEC62368-1 : ES1 & PS2

⚠ Pour éviter tout risque de brûlure, il est vivement recommandé de porter des gants pour manipuler le produit en fonctionnement lorsque la température ambiante dépasse 30°C.

Modèles Cellulaire :

- L'antenne doit être installée de façon à garder une distance minimale de 20 cm entre la source de rayonnement et toute personne.
- L'antenne ne doit pas être colocalisée ni fonctionner conjointement avec une autre antenne ou un autre émetteur.

3 Ventilation

Le produit est conçu pour être installé dans une armoire ou une baie informatique.
Pour éviter tout échauffement, en particulier lorsque la température ambiante peut s'élever dans l'armoire, on veillera à ménager un espace de 1 cm de chaque côté et 2,5 cm au-dessus et au-dessous du produit pour faciliter l'écoulement de la chaleur.

4 Mise à la terre

Pour des raisons de sécurité et de compatibilité électromagnétique, le boitier doit être connecté à la terre de protection de l'installation au moyen de son câble d'alimentation.

5 Raccordement à la ligne ADSL

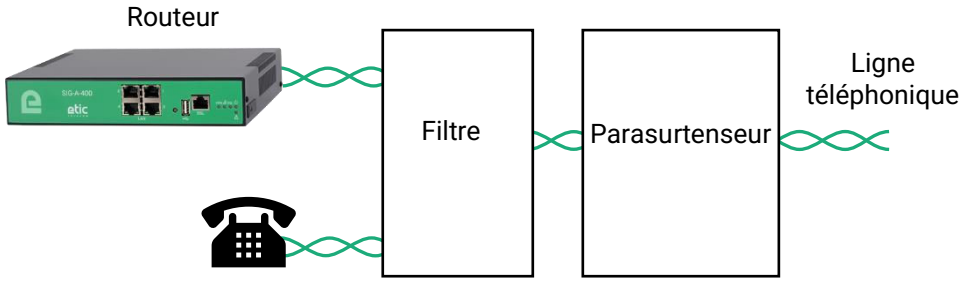
Longueur de ligne / niveau de signal :
Le SIG-A se raccorde à une ligne téléphonique de type analogique à 2 fils ou bien à une ligne « dégroupée » dont l'opérateur garantit une atténuation meilleure que 63 dB.

Cependant, lorsque le niveau de réception est voisin de ce minimum (parce que la ligne est très longue), le nombre de déconnexions intempestives s'accroît.

Dans ce cas, Il est conseillé de demander à l'opérateur de transmettre au moyen de **la technique « RE-ADSL»** (reach extended ADSL) qui accroît la puissance du signal et diminue le débit pour obtenir une augmentation de la portée.

Filtre ADSL :
Si le SIG est connecté à une ligne analogique et que le service de téléphonie est fourni par l'opérateur, il est possible de connecter un poste téléphonique en parallèle au routeur.
Pour ce faire, on doit connecter un filtre ADSL sur l'arrivée de la ligne.

Parasurtenseur :
Le SIG est protégé contre les surtensions provenant de la ligne, dues en particulier aux orages ; néanmoins, si la ligne est notoirement exposée à l'orage – ligne aérienne, câble non blindé, régions orageuses - nous conseillons d'équiper les extrémités de la paire torsadée avec un parasurtenseur relié à la terre.



Adresse IP publique :
L'adresse IP publique attribuée par l'opérateur sur l'Internet peut être fixe ou dynamique.

Néanmoins, si l'adresse attribuée au SIG est dynamique, elle change à chaque connexion du routeur à l'Internet ; elle n'est donc connue d'aucun autre abonné de l'Internet.

En conséquence, un routeur disposant d'une adresse IP dynamique doit être configuré pour être à l'initiative d'une connexion, c'est à dire « client » ; ou bien publier sur un serveur DNS dynamique l'adresse provisoire qui lui est attribuée à chaque connexion à l'Internet.

6 Raccordement au réseau cellulaire

6.1 Contrôles avant installation

Autorisation d'utilisation
On vérifiera auprès de la personne habilitée que l'utilisation d'un routeur cellulaire est autorisée.

Contrôle préalable du niveau de réception au moyen des cartes de couverture des opérateurs
Les cartes de couverture de réseau publiées par les opérateurs sur l'Internet permettent de vérifier grossièrement la disponibilité du service sur le lieu où l'installation du routeur est envisagée.

La consultation des cartes de couverture permet de choisir l'opérateur télécom le plus adapté.

Contrôle de la réception sur site
Si la réception semble possible après avoir consulté la carte de couverture, il est utile de confirmer la faisabilité sur le site lui-même.

Le contrôle doit être effectué à l'emplacement où il est prévu d'installer le routeur, tout particulièrement dans le cas où il doit être installé à l'intérieur d'un bâtiment.

Le contrôle doit être effectué en utilisant le même opérateur de réseau cellulaire que celui qui est prévu pour le routeur.

Une bonne solution, si le routeur n'a pas encore été commandé ou livré, est de réaliser le test au moyen d'un smartphone ; les menus « paramètres » ou « diagnostic » de tous les smartphones permettent d'afficher le niveau de réception.

Il est également possible d'utiliser le routeur pour mesurer le niveau de réception ; le voyant de niveau de champ et le menu diagnostic permettent d'afficher le niveau de réception.

6.2 Antenne

L'antenne est fournie séparément. Utiliser uniquement une antenne appropriée.

Nous proposons un catalogue d'antennes permettant les installations dans les cas les plus variés.

6.3 Déport de l'antenne

L'antenne ne doit pas être installée à l'intérieur d'un coffret métallique.

L'antenne peut être déportée ; cependant, le câble coaxial absorbe le signal reçu ou émis.

Si l'on utilise un câble de diamètre 6 mm, le niveau de réception du signal est diminué de 0,4 dB par mètre soit 4 dB environ tous les 10 mètres.

Pour obtenir le niveau de réception effectif, on retranche la perte dans le câble du niveau de réception affiché par le smartphone ; on veillera à ce que le rallonge ne dégrade pas le signal en dessous de la valeur minimale requise pour une connexion fiable (- 90 dBm).

On peut aussi utiliser du câble coaxial de diamètre 10 mm environ pour diminuer la perte dans le câble (0,2dB/m au lieu de 0,4dB/m).

Nous fournissons les rallonges à notre catalogue.

6.4 Choix de l'abonnement au réseau cellulaire

Un abonnement autorisant la transmission de données 4G-3G ou GPRS-EDGE doit être souscrit.
On pourra choisir, par exemple, un abonnement fait pour les tablettes ou pour les sticks USB
Il est inutile de souscrire un abonnement autorisant la téléphonie.

On choisira un abonnement qui autorise un volume mensuel suffisant au regard de l'application envisagée.

On vérifiera le coût du MO supplémentaire transmis au-delà du volume mensuel forfaitaire.

On souscrira de préférence l'abonnement dans le pays où le SIG doit être installé afin d'éviter les sur-coûts de « roaming ».

6.5 Installation ou extraction de la carte SIM (ou des 2 cartes SIM)

Ce modèle dispose de deux porte-cartes SIM. Si on utilise qu'une seule carte SIM, celle-ci doit être installée dans le porte-carte n° 1 (en haut sur les photos).

Installation de la carte SIM :

- Placer le SIG hors tension.
- Dégager la trappe située sur la face latérale droite.
- Insérer la carte SIM dans l'un des 2 porte-cartes ; la puce de la carte SIM doit être face au circuit imprimé (voir schéma).
- Pousser la carte jusqu'à ce qu'elle se verrouille.

Extraction de la carte SIM :

- Placer le SIG hors tension.
- Dégager la trappe située sur la face supérieure.
- Appuyer sur la carte SIM pour la déverrouiller ; elle remonte de quelques millimètres afin de faciliter son extraction.

6.6 Contrôle de la conformité de la connexion

Après installation, il est conseillé de vérifier la conformité du fonctionnement de la liaison avec le réseau cellulaire en transmettant des PING vers un serveur.
Il faut vérifier qu'aucun PING n'est perdu et que le temps de réponse est satisfaisant.

Si la connexion n'est pas conforme, il faut impérativement améliorer les conditions de réception pour rendre la connexion fiable soit en modifiant le type ou la position de l'antenne, soit en sélectionnant un autre réseau : 3G, voire GPRS, par exemple, au lieu de 4G.

La conformité de la liaison se mesure au moyen des paramètres suivants :

Voyant de réception du signal cellulaire		
Etat	**Description**	**Niveau de réception dBm**
3 flashs	Bonne réception Le SIG capte le réseau ; le niveau de réception est bon.	-50 à - 80
2 flashs	Réception suffisante Le SIG capte le réseau ; le niveau de réception est suffisant pour assurer une liaison fiable. Cependant, le débit pourra être diminué en cas d'erreurs de transmission.	-81 à –90
1 flash	Réception insuffisante Le SIG capte le réseau. Le niveau de réception est faible ; des déconnexions plus ou moins fréquentes et des erreurs peuvent survenir. Il faut améliorer la réception.	-91 à -110
Eteint	Pas de réception Contrôler le connecteur d'antenne et la présence de la carte SIM.	< -111

Pour contrôler en permanence le niveau du signal de réception au moyen du serveur html :

- Dans le menu, choisir **Diagnostics > Etat réseau > Interfaces**.

PREPARER LE PARAMETRAGE

1 Connexion du PC en vue de la configuration

1.1 Introduction

Le SIG se configure au moyen d'un PC équipé d'un navigateur Web. Aucun logiciel complémentaire n'est nécessaire.

Aide en ligne :
Pour la plupart des pages du serveur d'administration une aide est accessible en cliquant le **?** situé en haut à droite de la page.

Adresse du serveur d'administration :
A la livraison, l'adresse IP du serveur Web d'administration est 192.168.0.128.

Configuration :
La première configuration s'effectue de préférence en connectant le PC directement au connecteur LAN Ethernet.
Les modifications ultérieures peuvent être en plus effectuées à distance.

Restitution de l'adresse IP usine :
L'adresse IP usine 192.168.0.128 peut être restituée en enfonçant le bouton poussoir placé sur la partie supérieure du produit.

Protection d'accès au serveur d'administration :
Si vous ne parvenez pas à accéder au serveur d'administration, c'est probablement que l'accès en a été limité pour des raisons de sécurité ou pour d'autres raisons.

Format des adresses réseau :
Dans la suite du texte on appelle « adresse réseau », l'adresse IP de valeur la plus basse du réseau.
Par exemple si le netmask est 255.255.255.0, l'adresse réseau est X.Y.Z.0.

Caractères autorisés :
Les caractères accentués ne peuvent être saisis.

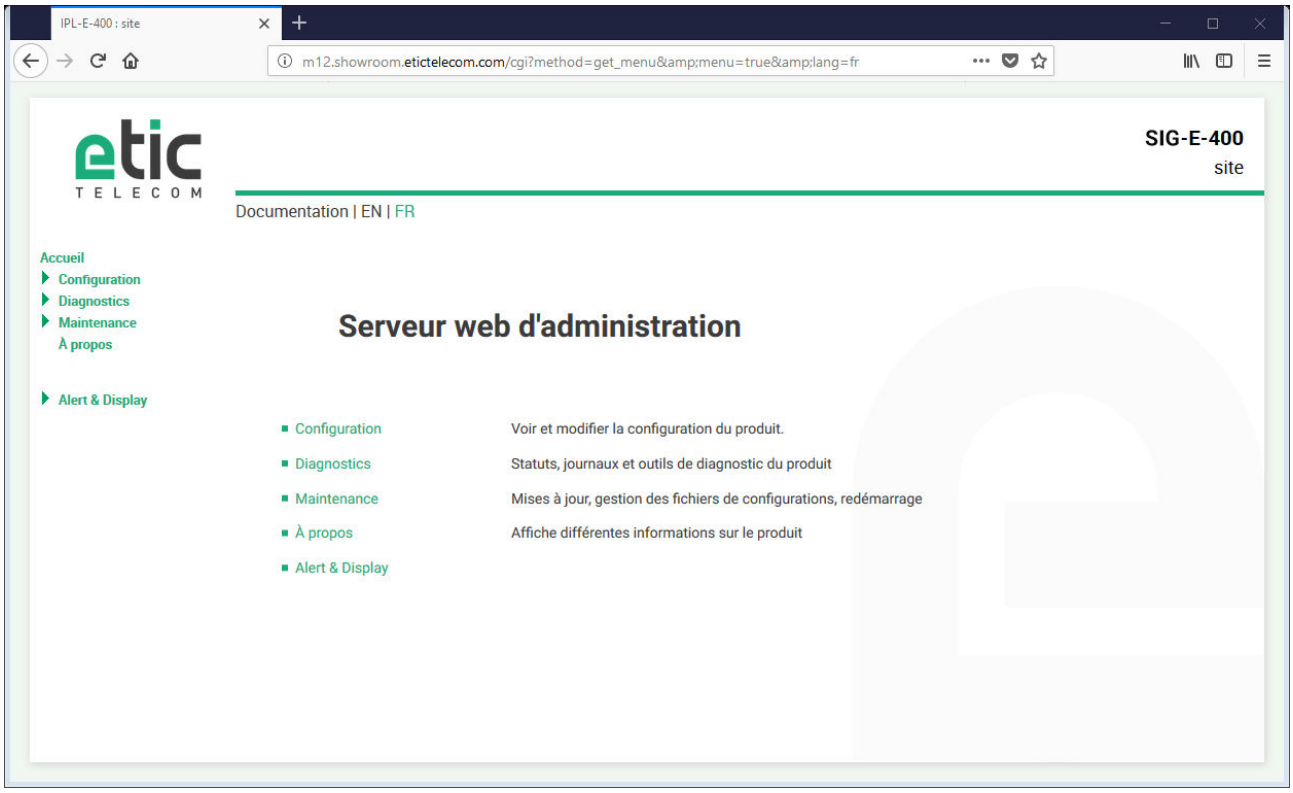
1.2 Première configuration

Etape 1 : Créer ou modifier la connexion TCP/IP du PC
Attribuer au PC une adresse IP différente mais cohérente avec l'adresse IP usine du SIG ; par exemple, l'adresse 192.168.0.1 pour le PC.

Etape 2 : Connecter le PC au SIG
Connecter directement le PC au SIG au moyen d'un câble Ethernet droit ou croisé.

Etape 3 : Lancer le navigateur
Lancer le navigateur puis saisir l'adresse IP du SIG : 192.168.0.128

La page d'accueil du serveur d'administration s'affiche.



Note : A la première configuration, l'accès au serveur d'administration n'est pas protégé.

1.3 Modification ultérieure de la configuration

Par la suite, le serveur d'administration du SIG est accessible depuis l'interface LAN à l'adresse IP attribuée au produit ou à travers une connexion distante.

Par défaut, l'accès au serveur d'administration depuis l'interface WAN n'est pas autorisé.

2 Accès au serveur d'administration par l'interface WAN

Pour autoriser l'accès au serveur d'administration par l'interface WAN,

- Dans le menu, choisir **Configuration > Sécurité > Droits d'administration**.
- Saisir le nom d'utilisateur et le mot de passe.
- Sélectionner le protocole à utiliser pour la configuration **HTTPS seulement** ou **HTTP et HTTPS**.
- Cocher la case **Activer l'accès par le(s) WAN**.

Le serveur d'administration est accessible au moyen d'un navigateur dans le mode HTTPS par l'interface WAN ou l'interface LAN.

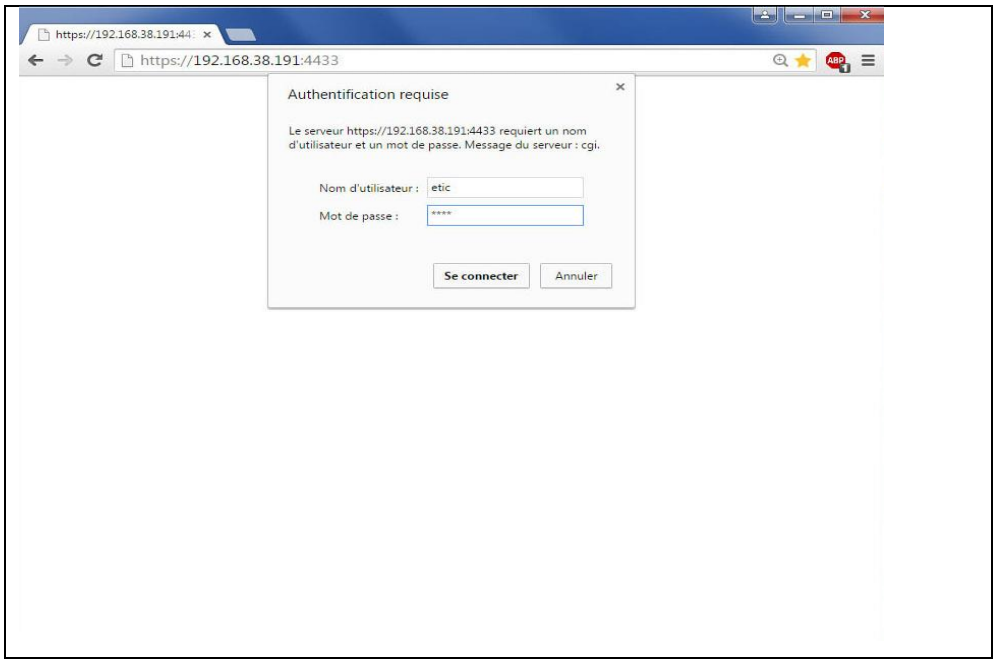
3 Opérations avec HTTPS

Une fois que le mode HTTPS a été sélectionné, procéder comme indiqué ci-dessous :

Le N° de port attribué au serveur d'administration est le N°4433

- Ouvrir le navigateur et saisir l'adresse IP du serveur d'administration du SIG :
- Exemple : https://192.168.38.191:4433.

- Cliquer **Continuer** lorsque le navigateur affiche un message d'avertissement.
-
- Saisir le nom d'utilisateur et le mot de passe qui ont été programmés pour protéger l'accès au serveur d'administration.



La page d'accueil du serveur d'administration s'affiche.

4 Retour temporaire à la configuration usine

Au cas où l'adresse IP du SIG ne pourrait être identifiée, ou bien en cas d'impossibilité d'accéder au serveur d'administration à la suite d'une d'erreur de configuration ou parce que le mot de passe a été oublié, il est possible de restituer la configuration Usine sans pour autant perdre la configuration courante.

- Appuyer sur le bouton poussoir B2 situé à l'arrière du produit,
- Maintenir le bouton-poussoir enfoncé pendant environ 3 secondes
- Le voyant clignote rapidement en rouge.
- Le serveur d'administration devient accessible à l'adresse IP Usine (192.168.0.128), en HTTP et sans mot de passe. La configuration appliquée temporairement est la configuration Usine. Cependant la configuration courante n'est pas perdue et c'est celle qui est toujours visible dans les pages du serveur d'administration.
- Après avoir pris connaissance de l'adresse IP ou changé des paramètres de la configuration enregistrée, appuyer à nouveau sur le bouton-poussoir ou bien mettre le produit hors tension puis à nouveau sous tension.
- Le produit devient à nouveau accessible à l'adresse IP enregistrée.

Note :
Si l'adresse IP du SIG n'est pas connue, on peut utiliser le logiciel **EticFinder**.
Ce logiciel détecte tous les produits de marque ETIC sur un réseau local. Après avoir lancé le logiciel, cliquer sur le bouton « Search », puis, lorsque la liste de produits s'affiche, double-cliquer sur l'adresse du produit pour accéder à son serveur html.

5 Restitution de la configuration usine

Il est possible de restituer définitivement la configuration Usine au moyen du bouton poussoir B2 de la face arrière, ou bien en utilisant le serveur d'administration. Dans ce cas, la configuration courante sera perdue, sauf si elle a été sauvegardée dans un fichier.

Pour restituer la configuration Usine au moyen du bouton poussoir,

- Mettre le SIG hors tension,
- Appuyer sur le bouton poussoir B2 situé à l'arrière du produit,
- Mettre sous tension tout en maintenant le bouton poussoir enfoncé 10 secondes.

Le voyant passe au rouge ; le SIG s'initialise et la configuration Usine est restituée.

Note : On peut aussi restituer la configuration Usine depuis le menu **Maintenance > Gestion des configurations** du serveur d'administration.

6 Protection de l'accès au serveur d'administration

- Dans le menu, choisir **Configuration > Sécurité > Droits d'administration**
- Saisir le nom d'utilisateur et le mot de passe qui protègent l'accès au serveur d'administration.
- Cocher la case **Protéger l'accès au site web par mot de passe**

En cas de perte du nom d'utilisateur et du mot de passe d'accès au serveur d'administration, il faut revenir temporairement à la configuration usine ; l'accès au serveur d'administration est alors libre.

7 Etapes de configuration

Pour configurer le produit, nous conseillons de procéder comme suit :

- Configurer l'interface LAN
- Configurer l'interface WAN
- Configurer les fonctions de routage
- Configurer les VPN
- Configurer l'accès distant
- Configurer le pare-feu

Pour le détail du paramétrage et les diagnostics, se référer au guide de configuration des routeurs :
Reference : « DOC_DEV_Guide de configuration des routeurs_x »

405 rue Lavoisier
38330 Montbonnot Saint Martin
France

Tel : +33 (0)4 76 04 20 00
contact@etictelecom.com

www.etictelecom.com