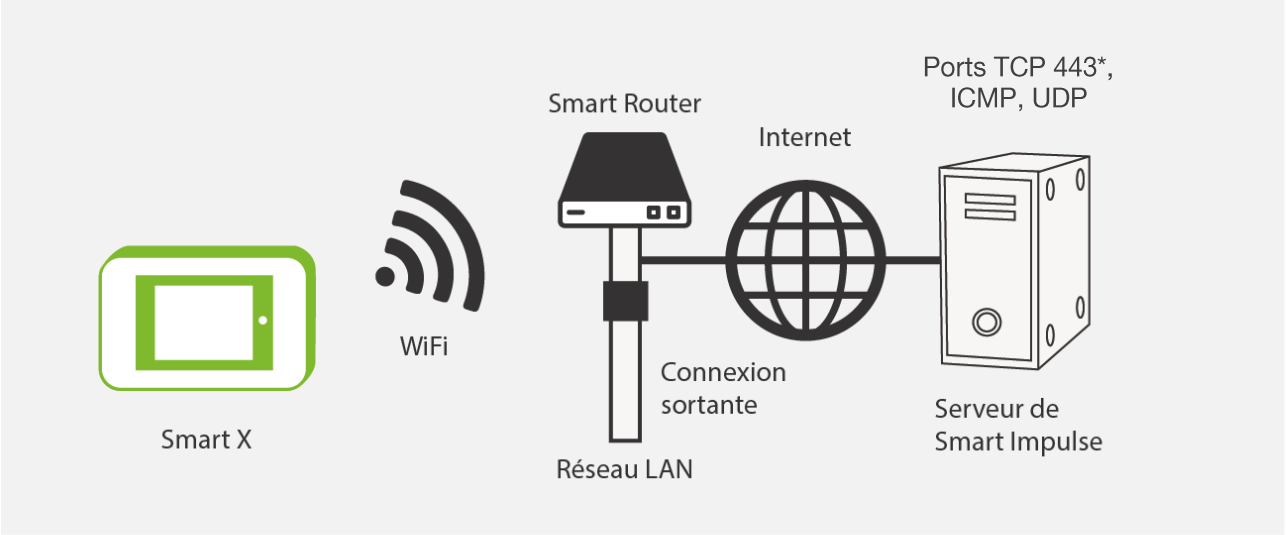
Informations sur la communication d'un Smart X®



Sécurité et authentification

Dès qu'un fichier de données est prêt, le Smart X le crypte avec le cryptage AES avant son stockage interne en cas d'absence de connexion internet, ou son envoi vers nos serveurs. La communication vers les serveurs se fait en HTTPS* (TLS 1.2), via le Smart Router.

Pertes de communication

En cas de perte de communication, le Smart X a une capacité de stockage de données d'environ 1 mois. Dès qu'il retrouve sa connexion, il relance l'envoi des données. Ces pertes de communication sont surveillées par Smart Impulse.

Paramétrage réseau

Pour le bon fonctionnement du Smart X et la récupération des données, **merci de vérifier auprès de votre service informatique** l'autorisation de connexion sortante du Smart Router vers notre serveur :

- Protocole ICMP vers 8.8.8.8 (ping)
- Protocole TCP vers smartx.smart-impulse.com (178.33.106.9), port 443* (HTTPS – TLS 1.2)
  **Port 80 (HTTP) pour les Smart X livrés par Smart Impulse avant Septembre 2024.*
- Protocole UDP vers time.google.com port 123 (NTP)

Merci de configurer le réseau afin d'autoriser le transit des paquets émis par le Smart X et de nous transmettre les paramètres réseau qui lui ont été affectés (DHCP / IP fixe, adresse IP, masque de sous-réseau, passerelle, proxy, serveurs DNS).

Informations sur la sécurité des données et de la plateforme web

Sécurité et pérennité des données

Les données sont stockées et sauvegardées dans des bases de données sécurisées :

- Pas d'accès direct depuis Internet,
- Redondance du stockage sur disques en RAID,
- Sauvegardes et archivages en continu, quotidiens et hebdomadaires, protégés, sur site et hors site.

Sécurité de la plateforme Web

- Les mots de passe utilisateurs et tokens d'accès aux données par l'API sont stockés en ayant recours à un algorithme de stockage recommandé par le NIST (avec salt unique et hashage des mots de passe).
- La plateforme est uniquement accessible en HTTP cryptée : aucune donnée ne transite sans être encryptée entre le navigateur de l'utilisateur et le serveur de Smart Impulse. Le certificat SSL et la configuration du serveur ont la note maximale de « A » sur le validateur proposé par SSL Labs.
- Les outils, frameworks et technologies utilisées sont adaptés et tenus à jour concernant les mesures de sécurité à prendre contre les failles web classiques connues et références par le Open Web Application Security Project.
- Une authentification via SSO peut être proposée en option.

Sécurité des serveurs utilisés

- Les serveurs utilisés pour l'infrastructure de Smart Impulse sont tenus à jour, et protégés selon les bonnes pratiques contre les intrusions.
- L'accès aux serveurs web est restreint et sécurisé pour les administrateurs.
- Les serveurs internes à notre infrastructure ne sont pas joignables de l'extérieur.