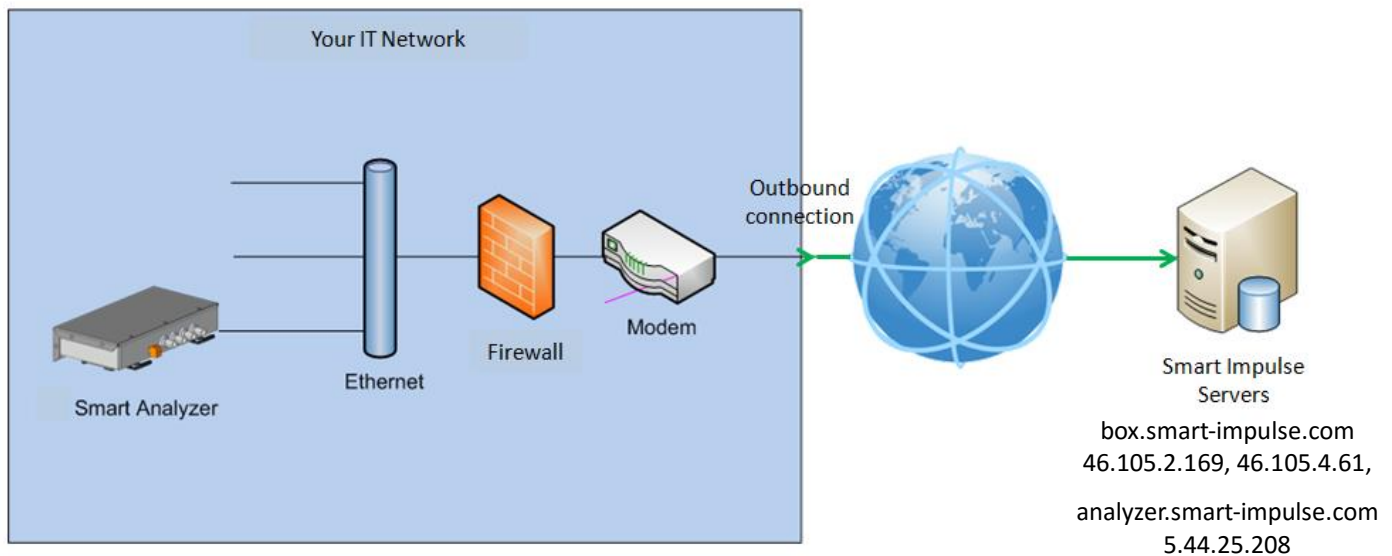


Information on the communication of the Smart Analyzer®



Ports 80, 123, 443

Security and authentication

The Smart Analyzer® sends its data to our servers by using the HTTPS protocol. With the SSL certificates, it confirms it is communicating with the Smart Impulse servers, and encrypts the data exchange with them.

The Smart Analyzer® initiates all communications; no inbound connection needs to be accepted.

Connection through a proxy is possible.

Traffic and communication failure

The order of magnitude of the traffic generated by the Smart Analyzer® is 2 GB/month, with connections made every 5 minutes.

In case of communication failure, the Smart Analyzer® has a data retention capacity of 3 months by USB Flash Drive. As soon as it recovers its connection, it restarts the data transmission. Smart Impulse monitors these communication failures.

Network configuration

In order to ensure the proper functioning of the Smart Analyzer® and the data recovery, the following configuration is necessary:

- Outbound connection towards the host names box.smart-impulse.com, analyzer.smart-impulse.com, vps10891.ovh.net (46.105.2.169) and vps11295.ovh.net (46.105.4.61) and the IP 5.44.25.208.
- Towards the ports 80 and 443 (HTTP and HTTPS, according to the level of protection of the exchanged information), and towards the port 123 (NTP).

Please configure the network in order to allow through the packets issued by the Smart Analyzer and provide us with the network parameters assigned to it (DHCP or static IP, IP address, subnet mask, gateway, proxy, DNS servers, NTP server).

Information on data and Web platform security

Data security and continuity

The data is stored and backed-up in well-secured databases: no direct access from the Internet, storage redundancy on drives in RAID configuration, continuous back-ups and archiving, daily and weekly, protected on site and off-site.

Web platform security

The users' passwords and data access tokens through the API are stored by using a storage algorithm recommended by the NIST (with a unique salt and password hashing).

The platform is only accessible in HTTPS: no data is transmitted without being encrypted between the customer's browser and Smart Impulse's server. The SSL certificate and the server configuration have the highest grade "A" on the validator proposed by [SSL Labs](#).

The used tools, frameworks and technologies are adapted and kept up to date according to the security measures against the standard known Web vulnerabilities listed by the [Open Web Application Security Project](#).

Security of the servers

The servers used for the Smart Impulse infrastructure are kept up to date, and protected according to the best practices against intrusions. Access is secure and restricted to the administrators