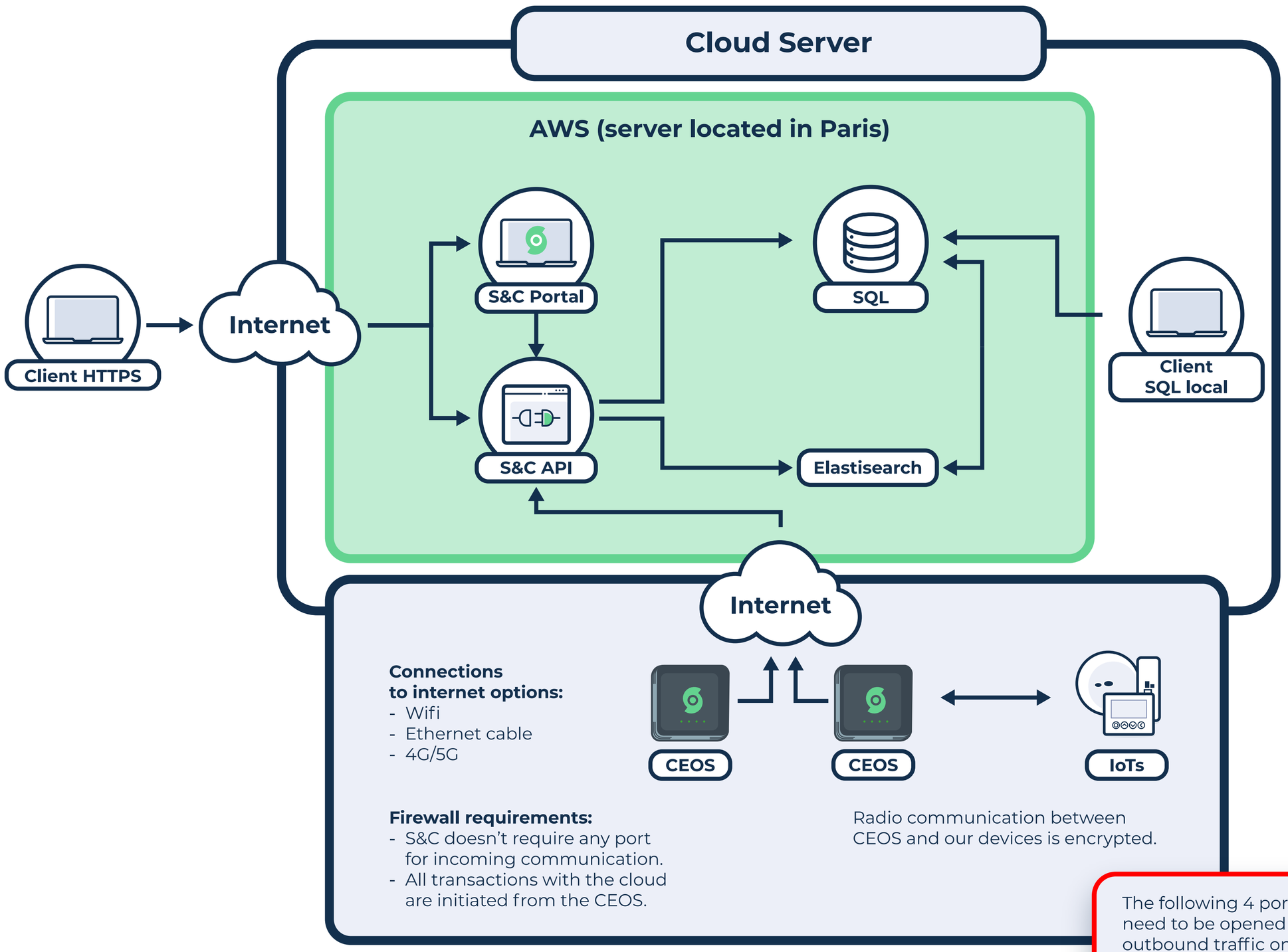
Securing our light BMS

Connection and Cloud Security



Connections to internet options:
- Wifi
- Ethernet cable
- 4G/5G

Firewall requirements:
- S&C doesn't require any port for incoming communication.
- All transactions with the cloud are initiated from the CEOS.

Radio communication between CEOS and our devices is encrypted.

The following 4 ports will need to be opened for outbound traffic only:
- 443 (https)
- 8883 (mqtt)
- 22 (ssh)
- 123 (ntp)

CEOS security keypoints

- The overall risk of a hacked CEOS is limited to its usage

- Each CEOS has unique identity/credentials to access S&C ressources limiting scale of attack if hacked.
- CEOS doesn't contain shared security assets.
- CEOS sensitive identity/credentials are encrypted in the persistent storage.
- Each CEOS has a unique key for the encryption.
- This key can only be used if the CEOS is booted in secure mode.
- Booting in secure mode requires a signed firmware.
- CEOS OTA updates.

- Requires an update bundle signed with a Smart & Connective certificate issued by DigiCert.
- Impossible to push a malicious update.
- The networking architecture is also a protection.
- CEOS are in a local network and not reachable directly from the WAN.
- All communications are initiated from the CEOS.
- REST-API communication is always initiated from CEOS.

- MQTT API:

- CEOS ACL doesn't allow to publish to other topics than its own.
- MQTT user account hacked could be revoked easily.

In the event of an attack, simply disconnect CEOS to regain manual control of the devices.
Our BMS has been deliberately designed to run in parallel with your installation, rather than as a substitute for it, so as to provide simple recourse in the event of an attack.

C3 - Accès confidentiel