Zaphire
Technical Sheet

Introduction

Zaphire is a Norwegian company based in Drammen. Since 2018, we have developed solutions for building automation and energy management with a focus on user-friendliness, security, and reliability.

Purpose

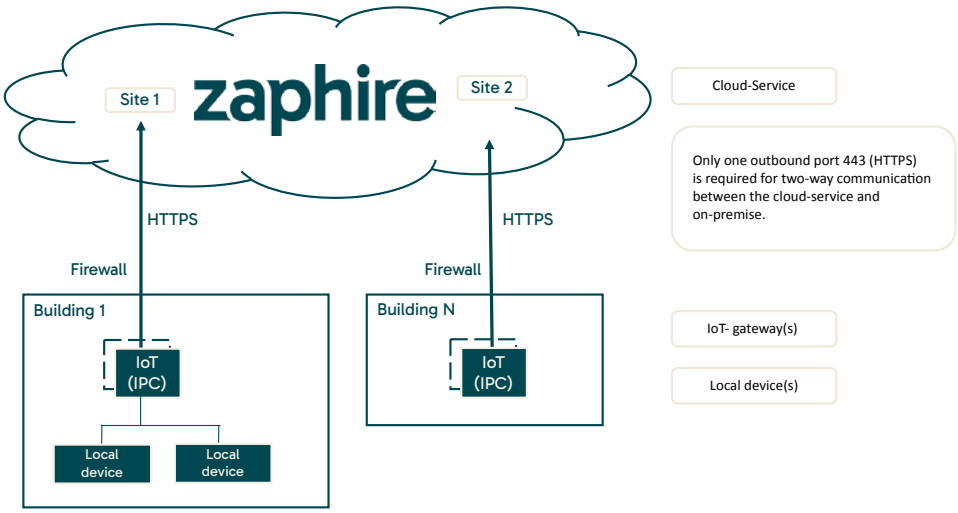
This technical specification provides a simplified description of the architecture and the secure communication between Cloud and On-Premise, as well as providing the implementation details required by system administrators to install Zaphire.

The components of the system

Cloud-service: Term describing the combination of all services behind https://zaphire.io implemented at the cloud- provider.
Location: Cloud location / no physical installation

IoT- coupler: One or more devices capable of establishing a secure two-way HTTPS websocket link between the on-premise automation and the cloud-service.
Location: On-premise

Local device / PLC: One or more autonomous devices located on-premise for automation and process control. The local device must be capable of sharing its data on an open automation protocol.
Location: On-premise



On-premise requirements

A. secure local network
Local devices and IoT- coupler(s) within one building must be connected to a local network behind a firewall. Segmentation into multiple local networks is possible and advised when no direct horizontal communication is required to improve the overall fault tolerance and resilience for network issues.

Network details such as the IP-address, subnet-mask, gateway-IP, and DNS-servers are a local matter and are chosen freely by the on-premise system administrator. Single networks/VLAN's that span over multiple buildings/sites is not recommended. At the very simplest scale, a standard/broadband router with an integrated firewall is sufficient to establish a secure local network.

B. Firewall requirements
All inbound ports should be closed for user and internet traffic for security reasons to protect the automation devices at the local network for external attacks.

Outbound port TCP 443 (HTTPS) must be open for internet traffic to the following DNS:

- zaphire.io
- sso.zaphire.io
- cr.zaphire.io

This can be tested by opening https://zaphire.io from a computer connected to the same network as the IoT coupler and log into Zaphire from there.

IMPORTANT: The IP address of zaphire.io may change at any time in the future without notice. Please use DNS entries, not the cloud service's IP address, if you need to restrict firewall destinations for outbound traffic in the firewall. For highest resilience.

zaphire