TECHNICAL NOTE | FP-TN-NET-CLOUD REV A | 05 AUGUST 2026

Network Requirements for Cloud-Connected Fortress Power Devices

Ports, protocols, and destinations that must be permitted for monitoring, remote support, and firmware updates

AT A GLANCE

Question	Answer
What must be opened inbound?	Nothing. No port forwarding, no inbound NAT rule, no static public IP, no DMZ, no VPN.
What must be allowed outbound?	TCP 8883, TCP 443, UDP 123, UDP 53, and ICMP echo. Full list in Section 1.
Allow by IP or by hostname?	By hostname (FQDN or wildcard). AWS rotates the addresses behind these names.
TLS / SSL inspection?	Must be bypassed for these destinations. Inspection breaks the connection
Typical symptom if blocked	Device shows a healthy local network link, but no data appears in the monitoring app.

1. OUTBOUND ALLOW LIST

All traffic is initiated by the device. Create the following outbound rules on the site firewall and write them against hostnames rather than addresses.

Protocol / Port	Destination	Purpose and impact
TCP 8883	`*.iot.us-west-2.amazonaws.com` `*.iot.us-east-1.amazonaws.com`	MQTT over TLS to AWS IoT Core. Carries telemetry up and commands, setpoints, and configuration down. This is the primary link. **If blocked:** no live data and no remote control. The device is effectively offline.
TCP 443	`*.s3.us-west-2.amazonaws.com` `*.s3.us-east-1.amazonaws.com`	Object storage. Firmware images for over-the-air updates, and bulk log and data file transfer. **If blocked:** no remote firmware updates and no log retrieval for support cases.
UDP 123	`pool.ntp.org`	NTP time synchronization. **If blocked:** clock drift causes TLS certificate validation to fail, which blocks every connection above.
UDP 53 (TCP 53 fallback)	Site DNS resolvers issued by DHCP, or a permitted public resolver	Name resolution for every destination in this table. **If blocked:** nothing resolves and the device never reaches the cloud.

ICMP echo	`8.8.8.8`	WAN reachability self-test used by the device diagnostics. **If blocked:** cloud traffic still works, but the device may report the internet as unavailable.

> **RULE OF THUMB**
>
> If the rule is outbound, written against a hostname, and exempt from TLS inspection, it will work. All three conditions have to hold.

2. INBOUND REQUIREMENTS

> **INBOUND: NONE**
>
> The device opens every session itself. A stateful firewall already permits the return traffic on those sessions, so no inbound rule is needed.

Specifically, none of the following are required for cloud monitoring, and none should be configured on the customer's behalf:

- Port forwarding or destination NAT to the device.
- A static public IP address or dynamic DNS registration.
- Placement in a DMZ.
- An inbound VPN tunnel or any remote-access service.

Commissioning and local access are separate from the cloud path. Where the installer app or a local web interface is used on site, traffic stays on the local network and is covered in the product installation manual.