**NETWORK REQUIREMENTS FOR HACKATION**

**RASPBERRY PI INBOUND NEEDS**

USERS NEED TO BE ABLE TO ACCESS PI ON PORT 22/TCP FOR FILE TRANSFER AND SHELL ACCESS

USERS NEED TO BE ABLE TO ACCESS PI ON PORT 5900/TCP FOR VNC/RDP LIKE ACCESS FOR DESKTOP CONTROL

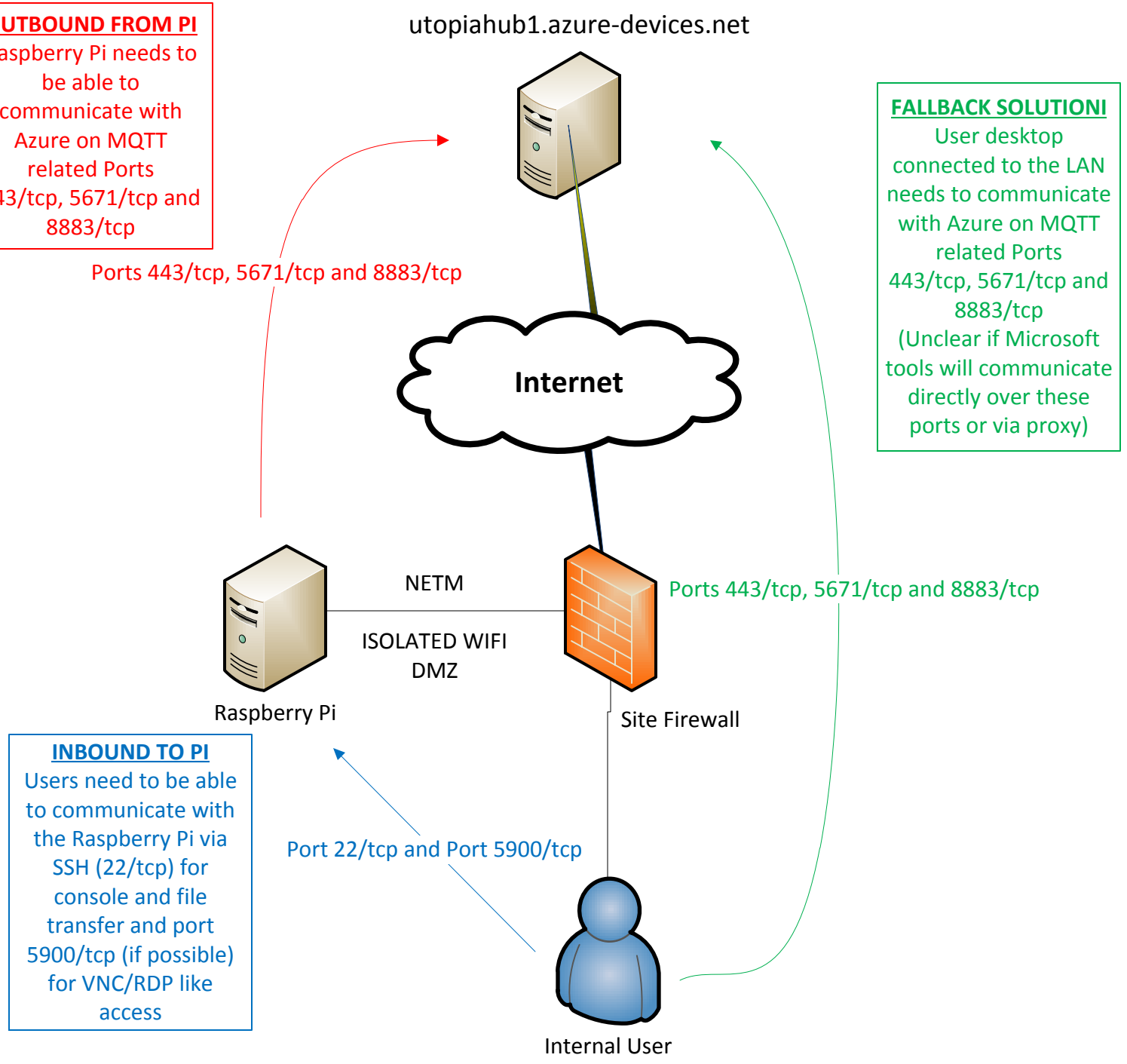
**RASPBERRY PI OUTBOUND NEEDS**

THE PI NEEDS TO BE ABLE TO COMMUNICATE ON MQTT PORTS TO AZURE IOT HUB ON PORTS 443/TCP, 5671/TCP and 8883/TCP

**FALLBACK OUTBOUND NEEDS (EXCLUDING PI)**

THE USER DESKTOP NEEDS TO BE ABLE TO COMMUNICATE ON MQTT PORTS TO AZURE IOT HUB ON PORTS 443/TCP, 5671/TCP and 8883/TCP
(MAY BE ABLE TO USE PROXY TO WORK AROUND DIRECT ACCESS ISSUES)

**OUTBOUND FROM PI**
Raspberry Pi needs to be able to communicate with Azure on MQTT related Ports 443/tcp, 5671/tcp and 8883/tcp




**FALLBACK SOLUTIONI**
User desktop connected to the LAN needs to communicate with Azure on MQTT related Ports 443/tcp, 5671/tcp and 8883/tcp
(Unclear if Microsoft tools will communicate directly over these ports or via proxy)

**INBOUND TO PI**
Users need to be able to communicate with the Raspberry Pi via SSH (22/tcp) for console and file transfer and port 5900/tcp (if possible) for VNC/RDP like access