STAP 1 – CHECK OF VOLGENDE COMMUNICATIEFLOWS OPEN STAAN (VIA IT)

- HTTPS verbinding voor het versturen van data richting Renson (data.ri4stat.eu)
- HTTPS verbinding voor het ophalen van updates voor het toestel (update.ri4stat.eu)
- NTP om de tijd van het toestel in te stellen
- Een UDP server op poort 49152 om toestellen in het netwerk te vinden (discovery)

Dit zijn standaard protocollen die door de meeste firewalls standaard worden toegelaten. Enkel de UDP server zou eventueel moeten toegelaten worden via een aparte uitzondering. Dit laatste is enkel benodigd om de instellingen van het toestel te wijzigen op het lokale netwerk.

TROUBLESHOOTER 1

DHCP problemen: Sense krijgt geen IP adres van de router
Bv MAC whitelist:

- STAP 1: vraag de MAC adressen aan via Renson (sensesupport@renson.be)
- STAP 2: IT kan deze MAC adressen 'whitelisten' op de router. De toestellen zullen nu worden toegelaten in het network.

TROUBLESHOOTER 2

Extra FIREWALL is aanwezig op de router. Dit wordt gemanaged door IT beheerder

- STAP 1: vraag de IT beheerder om de communicatieflows, MAC adressen en andere firewall specificities te bekijken

TROUBLESHOOTER 3

Alle communicatieflows lijken open te staan die nodig zijn om de Sense toestellen te verbinden aan het netwerk. Volgende zaken kunnen de connectie ook doorbreken:

- Is het netwerk open? Een gastennetwerk of openbaar netwerk zonder wachtwoord wordt niet toegelaten.

SOLUTION

OPLOSSING FIREWALL:

- Opzetten **Hidden WPA2 personal netwerk**
- Om geen complexe firewall op te zetten kan er ook een apart WPA2 personal netwerk opgezet worden voor de Sense toestellen. Dit WPA2 personal kan dan ook optioneel MAC filtering implementeren.
  Dit in combinatie met het "hidden" zetten van dit netwerk kan een veilig alternatief zijn om zo de Sense toestellen afgescheiden te houden van het klantennetwerk.
- Het linken van toestellen aan een "hidden" Wifi netwerk kan enkel via **de embedded pagina**

RENSON®
Creating healthy spaces