Secomea Hosted Solution

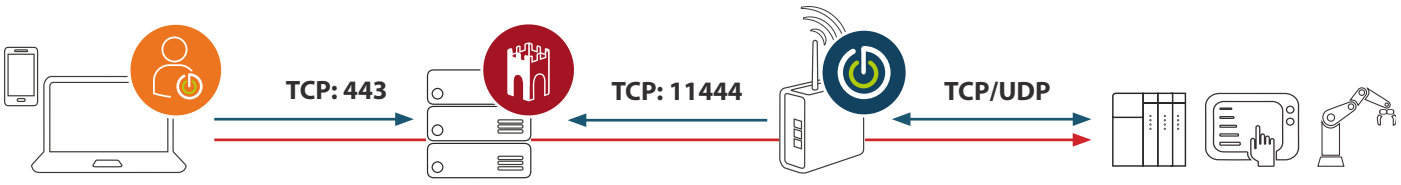
INFORMATION FOR THE IT DEPARTMENT

Introduction to the Secomea Products:

LinkManager (Referred to as **LM**) is the software/client used to gain remote access to industrial equipment connected to the SM.

GateManager (Referred to as **GM**) is the central server that facilitates the encrypted connection between the LinkManager and the SiteManager.

SiteManager (Referred to as **SM**) is the hardware IOT Gateway (Or embedded software) typically installed along with a PLC/ HMI or other industrial equipment where remote access is needed.



LinkManager
(Client)

GateManager
(Hosted by Secomea)

SiteManager
(IIoT Gateway)

Industrial Equipment
(PLC, HMI, etc.)

SiteManager connection information

The SM initiates the connection towards the public IP/DNS of the hosted GM.
The connection is outbound on port 11444 (TCP), alternatively port 80 (TCP) or 443 (TCP) can be used instead of 11444 (TCP).
Preferred connection method can be defined in the SM configuration.

The first time a SM connects to a GM, the SM will request the "Appliance TLS X.509 Certificate" from the GM. This is a unique self-signed certificate.

The SM initiates a TLS handshake with the GM. After a successful first handshake the SM will be locked to that GM's unique "Appliance TLS X.509 Certificate".
As the SM is now locked to the unique GM "Appliance TLS X.509 Certificate" it is secure against MITM/re-direct attacks.

LinkManager software connection information

The LM software initiates the connection towards the public IP/DNS of the hosted GM.
The connection is outbound on port 443 (TCP).

The first time a LM connects to a GM, the LM will request the "Appliance TLS X.509 Certificate" from the GM. This is a unique self-signed certificate.

The LM software initiates a TLS handshake with the GM. After a successful first handshake the LM will request the unique ID of the "Appliance TLS X.509 Certificate" and store it in its configuration files.
As the LM is now locked to the unique serial contained in the "GM Appliance TLS X.509 Certificate" it is secure against MITM/ re-direct attacks.

The LM software must installed on the user's PC and when installed installs a TAP network adapter, when a user is connected to a remote device via the GM, the software automatically creates the network routes needed in the windows routing table while the LM remote connection is active.

Hosted GateManager information

The GM is the proxy or the "facilitator" for the connection between the LM and the SM.
This means that the GM does not initiate the connection towards either the LM or the SM.
GMs hosted by Secomea have a public DNS name I.e. Gm14.secomea.com.
The web interface of the GM is the entry point for all users of the Secomea solution.
The GM uses a normal TLS web certificate to ensure that the https connection is secure.
The GM is where users and their access to specific SM and specific devices are administered.

There are the following login authorization methods:
- Certificate / Password (recommended & default)
- Certificate / Password + SMS code (recommended for additional security)
- Username / Password + SMS code
- Username / Password

For more details about our solution and Cybersecurity, see:
https://www.secomea.com/info-for-it-experts/