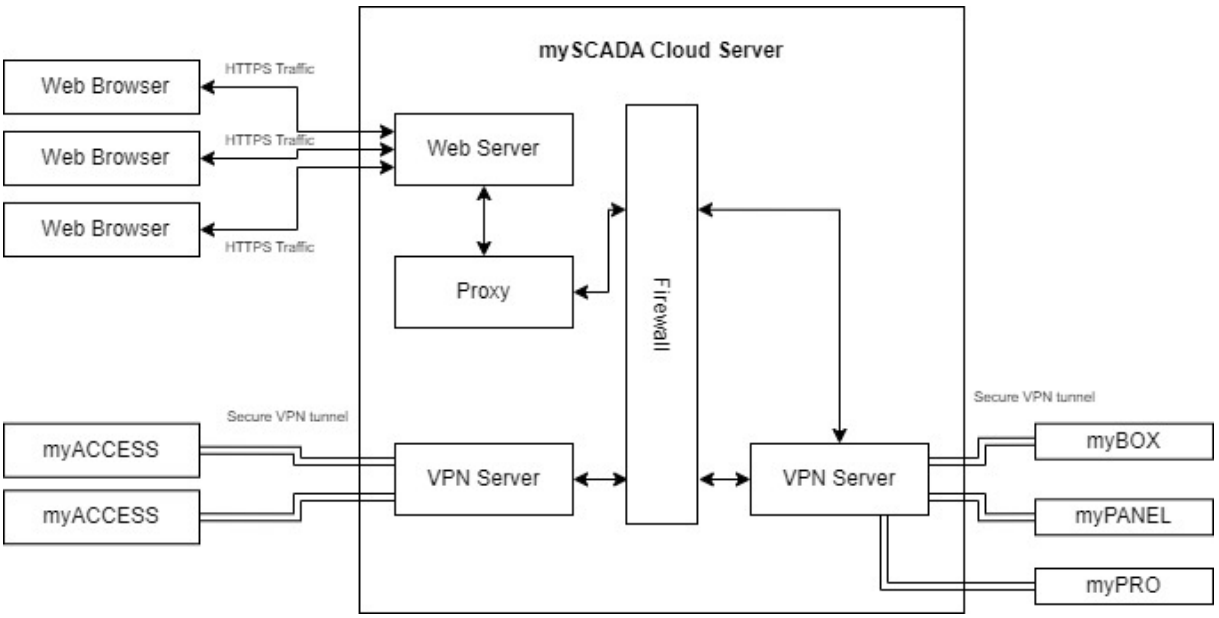
mySCADA

myACCESS

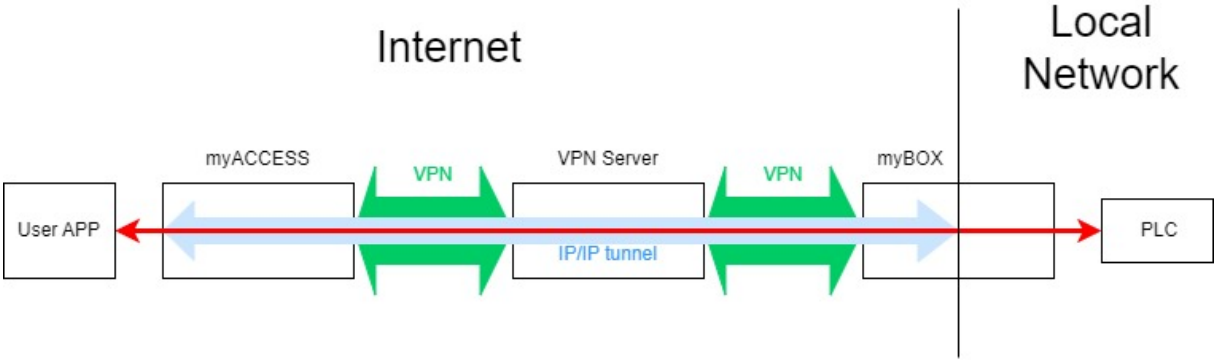
Description of functionality and recommended settings for maximum possible security

Client/facility communication diagram



1. Connecting via myACCESS Windows Application

In this model, the desired outcome is to remotely access the end device (e.g. PLC) connected to the myBOX device on the local network.



Communication schema: the secure VPN tunnel is created between user PC and VPN server and between VPN server and myBOX device.

- Connect the myBOX to myACCESS as follows. All devices on the local network that we need to access must have the default gateway set to myBOX.
- Install and configure myACCESS as follows.

The actual request for a VPN connection takes place in the following stages:

1. In the first phase, a VPN tunnel is set up with the myACCESS server. The setup is secured with X.509 certificates + name and password.

2. In the second phase, an IP/IP tunnel is built inside the encrypted tunnel with the selected myBOX device and the route is set up on the computer from where the VPN is built. The routes are set to all local networks directly connected to myBOX.

3. At this stage, it is already possible to communicate with the individual elements of the remote local network using any application running on a PC with a myACCESS connection established. For example, it is possible to configure a PLC.

2. Remote access via the web browser

In this model, the desired outcome is to access the myBOX/myPRO/myPANELs web interface.

The HTTPS protocol secures the communication between the web client and the web server. End users always access a proxy on the VPN server, which provides content from the desired end device and performs caching to offload traffic to a separate end device.

Diagram for remote access using a web browser:

3. End device security

- A unique hash identifies the end device.
  For example: https://www99.myscada.cloud/rglRGkv9Or13FsiYzWuTss59/

  This identification can be at any time re-generated from the myACCESS portal administrative interface at https://www.myscada.org/en/. Hash change does not break communication with end device as the change is done on the VPN server routing table only.

- In terms of security, we recommend securing the end device with user access levels. See the manual (chapter 2.3.myACCESS Device Limiting access for remote users) in case of accessing the device via a link.

- Once a user tries to access the device via a link, he/she will be prompted with the username/password.

- User password length/complexity requirements are set in the project itself, see the manual (chapter 32.3.User accounts).

The recommended procedure for password safety (which can be made obligatory for end users in the project):

- password length should be at least 12 characters long.
- passwords should contain a combination of upper and lower case letters, numbers and special characters (e.g. @, #, $, %, &).
- Passwords change every 3 months.

4. Administrative interface security (myACCESS portal)

Technical Details

Item	Description
Passwords	passwords stored at the end device are always encrypted using SHA512 algorithm
VPN Technology	OpenVPN
VPN Certificate	X.509v3 (RSA 1024bit)
Incoming channel	AES-128-CBC/SHA1
Outgoing channel	AES-128-CBC/SHA1
Control channel	TLSv1, cipher TLSv1/SSLv3 ECDHE-RSA-AES256-SHA