Best practices:

1. Connection security with the SSL certificate. SSL (Secure Sockets Layer) is a cryptographic protocol that implies a more secure connection. It uses asymmetric cryptography to authenticate exchange keys, symmetric encryption to maintain confidentiality, message authentication codes for message integrity.
2. Use the access key instead of the login / password. It is considered a standard of network security:
    - The access key is generated automatically, has a sufficiently crypto-stable length and a set of characters (the user's password can be very simple)
    - The access key is bound to a specific device, i.e. key hacking will not allow an attacker to access the entire account
    - The access key can be reset without requiring a password change, you only need to re-login
3. Advanced Encryption Standard (AES-256), symmetric block cipher algorithm (block size - 128 bits, 256 bit key). In June 2003, the US National Security Agency decided that the AES cipher is sufficiently reliable to use it to protect classified information. Up to the level of SECRET it was allowed to use 128-bit keys, for the TOP SECRET level, keys of 192 and 256 bits were required. To date, AES is one of the most common symmetric encryption algorithms.