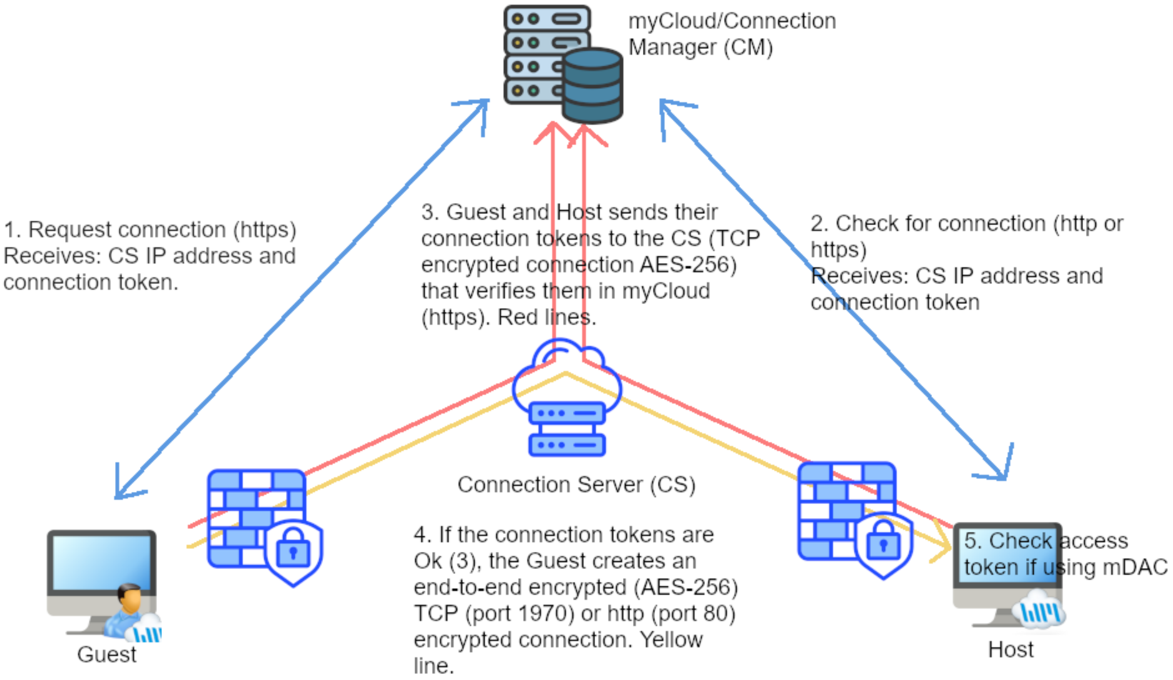
Advanced myCloud Connection Description

The following documents describes the principles for myCloud connections. A myCloud connection is an internet based connection assigned and controlled by WiseMo myCloud.

Please refer to the following diagram:


myCloud/Connection Manager (CM)
1. Request connection (https) Receives: CS IP address and connection token.
3. Guest and Host sends their connection tokens to the CS (TCP encrypted connection AES-256) that verifies them in myCloud (https). Red lines.
2. Check for connection (http or https) Receives: CS IP address and connection token
Connection Server (CS)
4. If the connection tokens are Ok (3), the Guest creates an end-to-end encrypted (AES-256) TCP (port 1970) or http (port 80) encrypted connection. Yellow line.
5. Check access token if using mDAC
Guest
Host

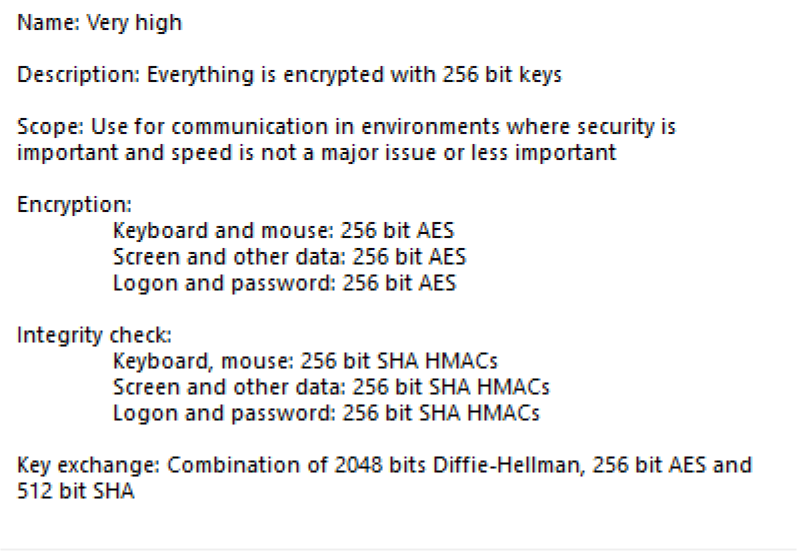
A connection involves the following modules:

- Guest: The module that is installed on the device that should remote control a remote device.
- Host: The module that is installed on the device that should be remotely controlled
- myCloud/Connection Manager (CM): A web service that is in charge of authorizing a connection and where and how a connection should be establish. The Connection Manager is hosted by WiseMo.
- Connection Server (CS): Verifies a connection and acts as a routing point tunneling the connection. There are many Connection Servers around the world hosted by WiseMo. A connection Server for a connection is assigned based on geographical proximity and load. The remote control connection goes through the Connection Server only and is end-to-end encrypted. A customer can Host their own Connection Server(s) free of charge (Private Connection Servers) if they want to assure that no data passes through a WiseMo hosted server.

- Firewalls on customer premises.

This logic assures that:

- All connections from customer locations are made out through the firewalls. No inbound ports should be opened. No hole-punching techniques are attempted to bypass the firewalls.
- All connections to CM and CS are based on https (4k bit certificate). The Host makes http based heartbeats to the CM. These heartbeats can also be made on https if configured in the Host.
- The Guest-Host connection is end-to-end encrypted with AES-256 (lower encryption levels can be configured):



Name: Very high

Description: Everything is encrypted with 256 bit keys

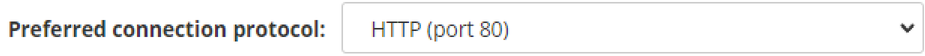
Scope: Use for communication in environments where security is important and speed is not a major issue or less important

Encryption:
Keyboard and mouse: 256 bit AES
Screen and other data: 256 bit AES
Logon and password: 256 bit AES

Integrity check:
Keyboard, mouse: 256 bit SHA HMACs
Screen and other data: 256 bit SHA HMACs
Logon and password: 256 bit SHA HMACs

Key exchange: Combination of 2048 bits Diffie-Hellman, 256 bit AES and 512 bit SHA

- The Guest-CS and Host-CS connections can be made over TCP on port 1970 or on http on port 80. If the connection is made over http, the content of the http packages are AES-256 encrypted.
- The Guest-CS and Host-CS connections will first be attempted on TCP/1970 and then on http/80. If a customer only allows http/80, it is recommended to configure myCloud accordingly (Settings > Connection > Preferred connection protocol):



Preferred connection protocol: HTTP (port 80)

- If using Private Connection Servers, the servers can be configured to other ports.
- After a connection to the Host is established, the Guest user must be authenticated and authorized by the Host. Multiple schemes exist.
- If using myCloud Device Access Control (mDAC, central control of authentication and authorization) the architecture assures that the Connection Server will not get the connection verified if it is not properly authenticated by myCloud (step 3 above).