



Aveco s.r.o.
Velešlavínská 39
162 00 Praha 6
Czech Republic
tel: ++420-235366707
fax: ++420-220610728
E-mail aveco@aveco.com

Internet connection



Document history

Revision	Date	Description
v.1.3.1	29.4.2020	Chapter "General requirements for network connection" added
v.1.3	26.4.2017	Document reorganized added TeamViewer based solution
v.1.2	23.6.2006	added VPN solution added description for internet access for period of installation of AVECO products
v.1.1	29.9.2005	Aveco static IP address has changed
v.1.0	21.8.2005	Initial version



Content

1. GENERAL REQUIREMENTS FOR NETWORK CONNECTION	5
2. IP ADDRESSES	5
3. AVECO ENGINEER ON SITE	6
3.1. CONNECTIVITY DURING INSTALLATION AT CUSTOMER'S PREMISES	6
4. AVECO ENGINEER CONNECTING FROM HEADQUARTER	7
4.1. SOLUTION BASED ON SSH	7
4.2. SOLUTION BASED ON PORT MAPPING	8
4.3. SOLUTION BASED ON VPN	9
4.4. SOLUTION BASED ON TEAMVIEWER	10



This document describes the possible internet connection for maintenance and installation purposes between Aveco headquarter and installed Aveco systems.

There are basically two types of solutions based on where AVECO engineer is, whether in Aveco headquarter (typically remote installation, support engineer) or whether on customer site (typically engineer doing the installation onsite).

One solution from chapter 3 "AVECO engineer on site" on page 6 as well as from chapter 4 "AVECO engineer connecting from headquarter" on page 7 must be implemented by customer to allow for smooth installation/support services.



1. General requirements for network connection

AVECO needs to transfer quite big amount of data (up to gigabytes in case of some packages, 30MB packages on regular basis) as well as edit many of configuration files and therefore there the connectivity between AVECO headquarter and installed Aveco systems needs to fulfill following requirements :

- must be stable (unpredictable disconnection every few hours/minutes is not acceptable - leads to loose of unsaved changes)
- must be available 24/7 during whole period of installation, it is because several people from several time zones can work on system, for maintenance must be available for whole agreed period of time
- reasonable speed to allow upload/download 1GB files - 1MB/s expected (transfer of 1GB package takes 17 minutes)
- reasonable response time that allows smooth editation of text files - less then 1 second expected

2. IP addresses

AVECO have two independent connections to internet (internet gateways) so that in case one connection/provider fails the second one can be used. The AVECO IP addresses are connected to internet are as follows:

Internet gateway 1 (MAIN)	194.149.122.58
Internet gateway 2 (BACK)	194.149.114.50

Both are to be enabled on the TV station's firewall (in case selected solution requires firewall to be configured to AVECO IPs) in case AVECO should have a possibility to connect at any time.

3. AVECO engineer on site

AVECO engineers need to have access to the headquarter because of new version download, log file upload for inspection, etc.

3.1. Connectivity during installation at customer's premises

AVECO engineers use notebook computers during installation of AVECO products at the customer's site.

AVECO engineers need to access internet during the whole period of installation. They need to access internet as well as to access AVECO office via VPN. This internet connection should exist while the connection between AVECO and Astra servers exists as well.

It is necessary that the notebooks are connected at the same time to the automation system being installed and to the internet.

Possible solutions sorted from the best to the worst possible are listed below:

- 1) Full outgoing access to internet

4. 2) Full outgoing access to AVECO IP addresses, see chapter 1

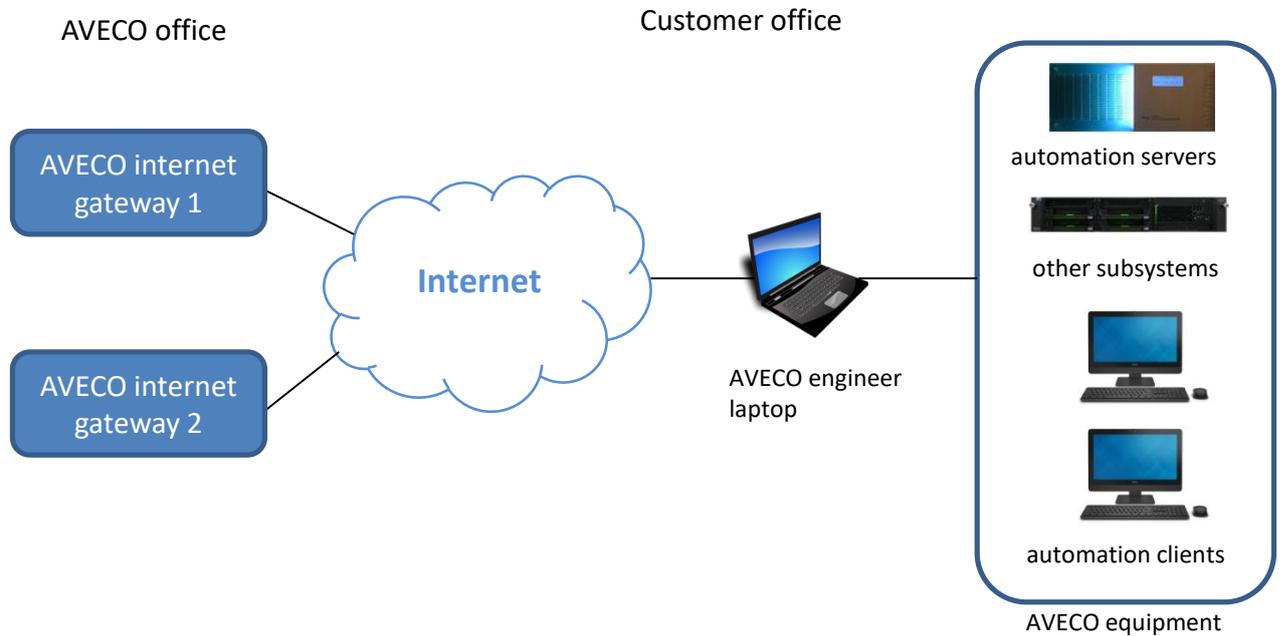
5. General requirements for network connection

AVECO needs to transfer quite big amount of data (up to gigabytes in case of some packages, 30MB packages on regular basis) as well as edit many of configuration files and therefore there the connectivity between AVECO headquarter and installed Aveco systems needs to fulfill following requirements :

- must be stable (unpredictable disconnection every few hours/minutes is not acceptable - leads to loose of unsaved changes)
- must be available 24/7 during whole period of installation, it is because several people from several time zones can work on system, for maintenance must be available for whole agreed period of time
- reasonable speed to allow upload/download 1GB files - 1MB/s expected (transfer of 1GB package takes 17 minutes)
- reasonable response time that allows smooth editation of text files - less then 1 second expected

IP addresses on page 5.

- 3) Outgoing access to AVECO IP addresses via ports 22/TCP, 1194/UDP and 1194/TCP
- 4) Connection to internet via second notebook NIC or via a router (see schematics below)



AVECO notebooks use personal firewalls and regularly updated antivirus software of course.

6. AVECO engineer connecting from headquarter

AVECO engineers need to have connectivity to AVECO equipment to be able to check log files, modify configuration, upload and install bug fixes, install new features etc. It means that there two types of connection and both are needed:

- access to system to see the PC screen - this is to see and analyze the problem
- possibility to upload and download files (FTP preferred) - this is to get log files and upload hot fixes

If not mentioned differently, it is the customer's responsibility to cover the solution completely (which means buy & install solution plus provide a software/client to AVECO team so that AVECO can connect).

Here is a list of TCP/IP ports to be opened for accessing the AVECO equipment:

Automation server	Incoming: <ul style="list-style-type: none"> - port 4868 (UI) - port 80 (HTTP) Outgoing <ul style="list-style-type: none"> - all ports (because of FTP)
Automation client	Incoming: <ul style="list-style-type: none"> - port 3389 (RDP)

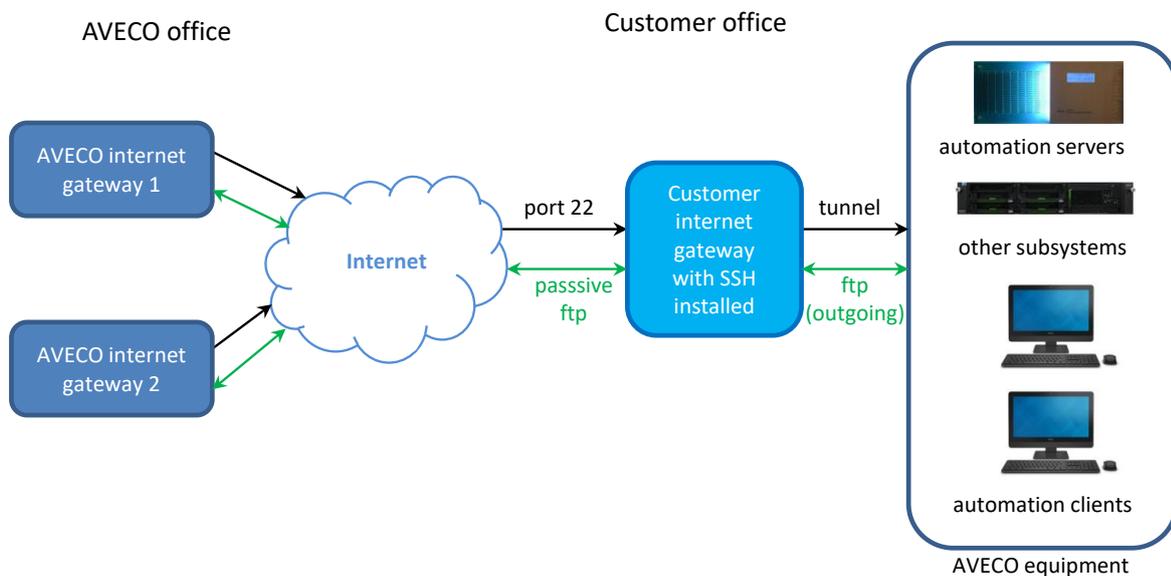
	Outgoing – all ports (because of passive FTP)
Other subsystems	Incoming: – port 3389 (RDP) Outgoing – all ports (because of passive FTP)

It is important to say here that in case AVECO equipment is equipped with more than one network interface, the one labeled EXT (like external) is the one which should be accessible from AVECO internet gateways, never the one marked as INT (like internal).

6.1. Solution based on SSH

SSH (Secure Shell) is a safe way of remote connection. SSH server by default listens on port 22 and allows for connection to amount of AVECO equipment's customer network.

SSH is user/password protected & encrypted.



Customer Internet gateway to provide outgoing FTP connection to AVECO internet gateways, either directly or via proxy ftp.

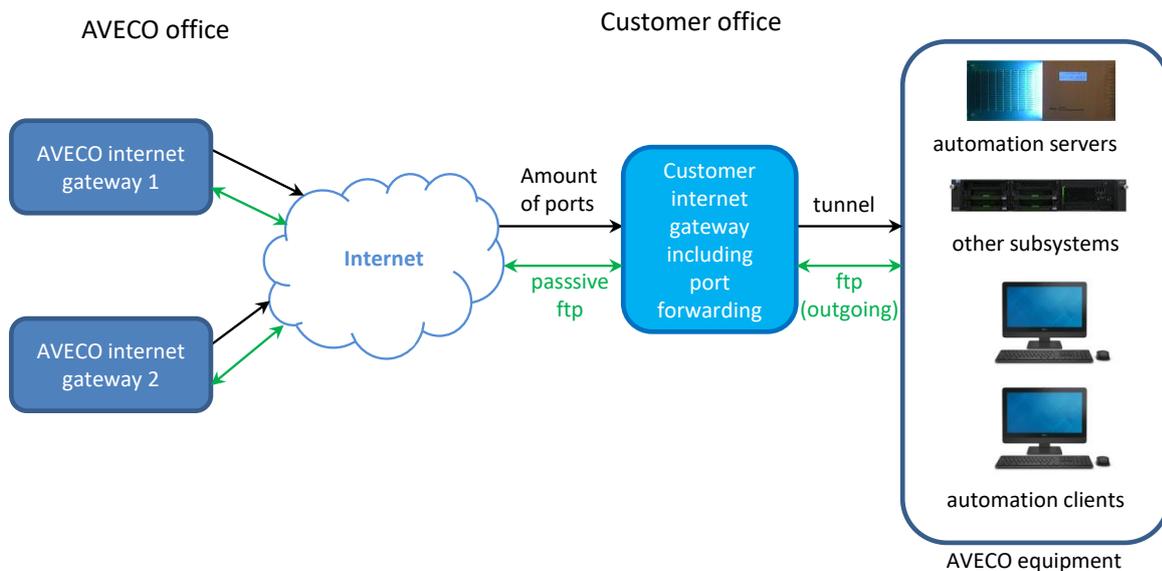
Following information to be provided by customer for connection:

IP/DNS name of Customer internet gateway	
Port SSH server listens on	
Username	

Password	
Table including IP & port to connect to aveco equipment in customer local network (one per AVECO equipment)	
IP of Customer internet gateway used for FTP outgoing connection (to be enabled on AVECO firewall)	

6.2. Solution based on port mapping

Most simple way of connection, it is not encrypted. The main idea of this solution is to receive connection/data on one TCP/IP port and simply forward them to AVECO equipment IP and TCP/IP port. Please note that port "Customer internet gateway" is listening on is typically different then port it is forwarded to (in case access to be provided to more devices it is a must - all listens on same port, typically RDP listens on port 3389)



Customer Internet gateway to provide outgoing FTP connection to AVECO internet gateways, either directly or via proxy ftp.

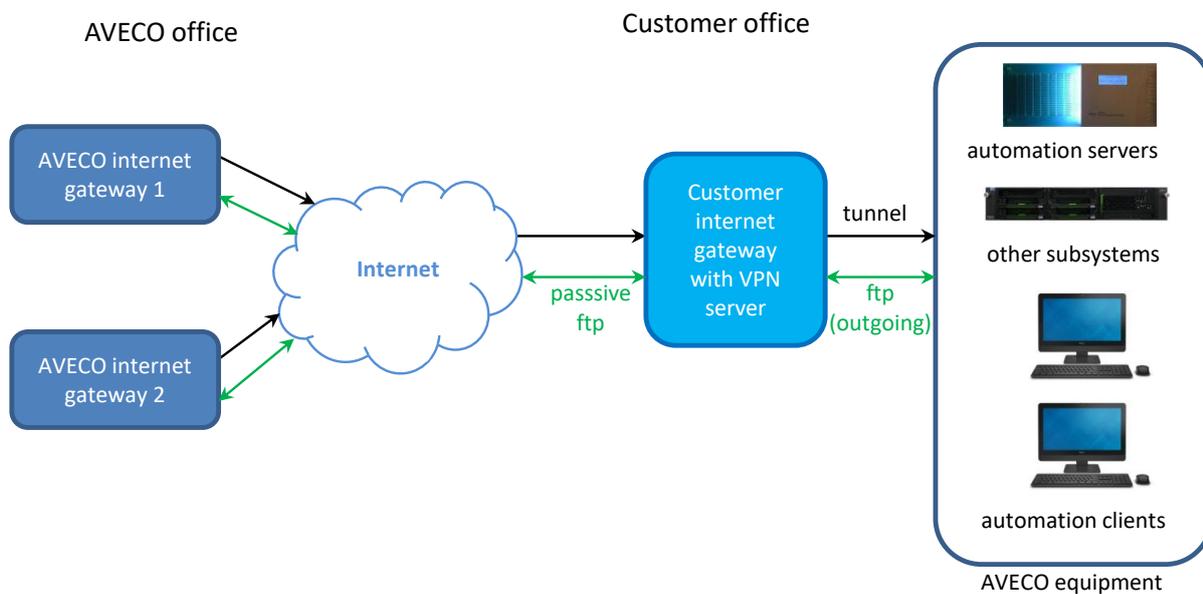
Following information to be provided by customer for connection:

IP/DNS name of Customer internet gateway	
Table including IP & port to connect to aveco equipment in customer local network (one per AVECO equipment), following information needed for each:	

<ul style="list-style-type: none"> – identification of AVECO equipment (like BackOffice MAIN server etc.) – TCP/IP port Customer gateway is listening on – IP of AVECO equipment the connection is forwarded to – TCP/IP port of AVECO equipment the connection is forwarded to 	
IP of Customer internet gateway used for outgoing FTP connection (to be enabled on AVECO firewall)	

6.3. Solution based on VPN

VPN connection is secure connection with an access limited to some network/computers.



AVECO is familiar with several commonly used VPN solutions, here is the list of VPN clients we already have:

- FortiClient VPN
- Cisco VPN
- Cisco AnyConnect VPN
- Windows VPN

- Sophos VPN
- Stone Gate VPN
- Open VPN

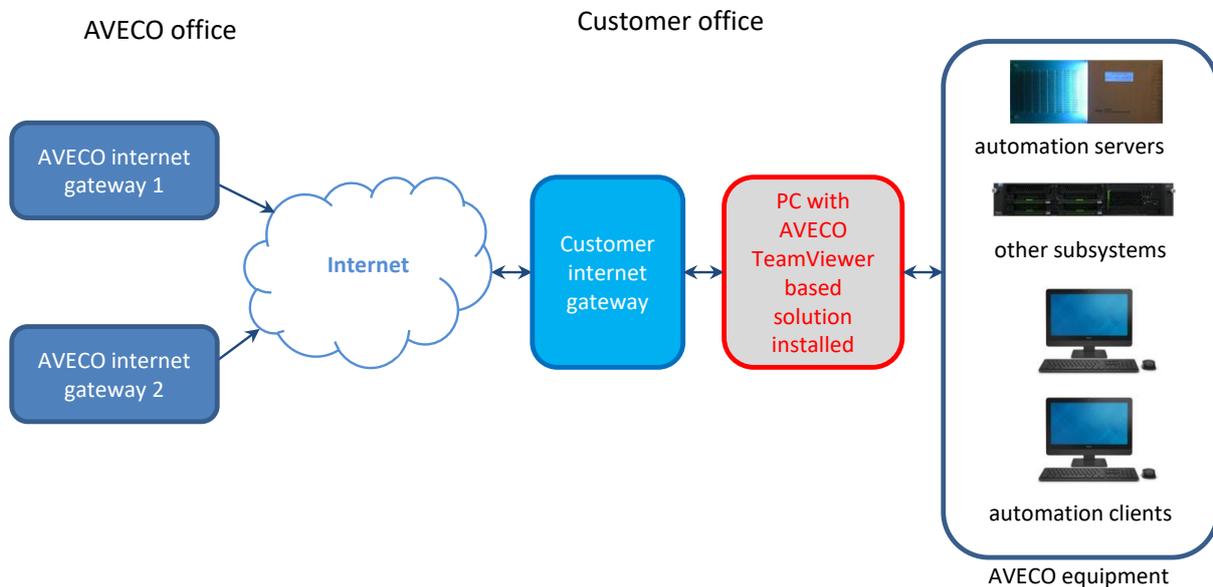
Customer Internet gateway to provide outgoing FTP connection to AVECO internet gateways, either directly or via proxy ftp.

Following information to be provided by customer for connection:

VPN client including all the connection credentials, can be even the hardware token	
IP of Customer internet gateway used for outgoing FTP connection (to be enabled on AVECO firewall)	

6.4. Solution based on TeamViewer

TeamViewer based solution profits from easy way of installation. Customer to prepare Windows PC (physical or virtual) and install AVECO based TeamViewer package (can be downloaded from AVECO web site, this is true for installation manual also) under administrator user.



Once installed, the PC appears in a list of accessible computers, AVECO engineers connect into and can connect to AVECO equipment. Please note that there is a need to install license of Phindows to allow for connection to automation servers, therefore this PC should stay available for remote access forever.