



## Vending Machine Network connectivity

The following document outlines the recommended procedure for connecting IVM vending machine equipment to the end-user computer network. The intent is to guide the computer network specialist in their effort to configure the various network components.

### Background

The fundamental issue with using a LAN connected supply vending machine is to link a vending machine in one location to an IVM server in another location. The recommended solution is akin to a web browser on a desktop looking at a web page.

### TCPIP Client Connection

A web browser works by the web browser sending a message packet to the web server and waiting for a packet to come back. Once the packages have been exchanged, the connection is dropped and the web browser is isolated from the outside world.

In the case of the supply vending, the machine generates a message packet and sends it to the IVM server for validation. IVM looks at the packet and replies with a positive or negative response. Once the packet has been exchanged, the connection between the vending machine and IVM is disconnected.

### Discussion

The TCPIP client connection has the significant advantage of not requiring any additional work on the part of the location to implement an on line vending solution. Furthermore, since the vending machine connects to IVM to approve each and every transaction, the IVM database contains a real time snap shot of what is going on at all times. The only requirement as of this writing is open access to the internet outbound for TCP port *\*hidden\** thru *\*hidden\**. The machine network hardware is capable of both manual and DHCP for configuring a network TCPIP address.

If a proxy server is implemented at the client site additional intervention will be required. The client must allow the vending machine to circumvent the proxy otherwise the machine will not be able to authenticate for connecting outbound to access the internet. A proxy server by its nature is designed to meet connectivity, control and security for business networks. The design of the supply vending machine by its nature is well within the confines of the control and security aspects for business network applications. There is no opportunity for a rogue connection to threaten network security.



## Alternatives to a wired network

The advent of wireless networking has broken down barriers for organization whose IT policies strictly forbid 3<sup>rd</sup> party devices on the corporate infrastructure.

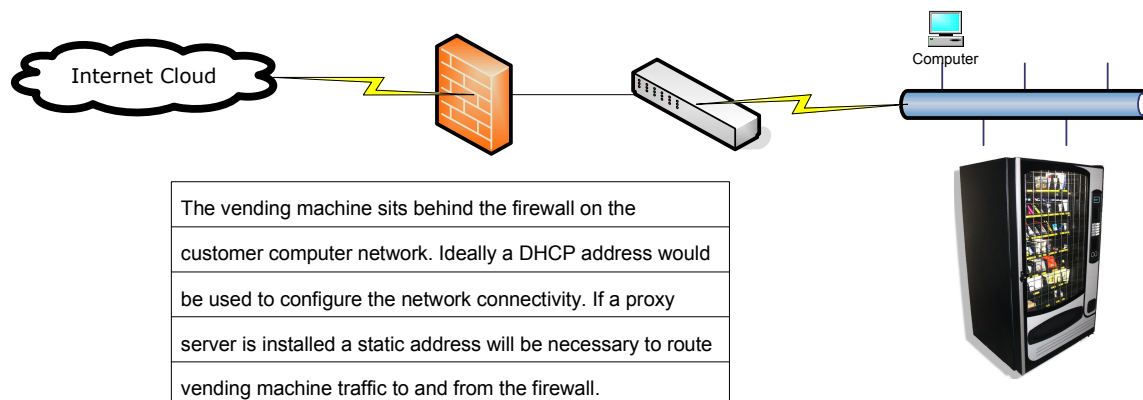
## Security

Foremost in implementing any LAN solution has to be network security and integrity. The TCPIP client solution achieves security through the following means:

- The TCPIP client initiates an outward connection to the IVM server when required. The NAT router only allows an inwards communication in response to an outgoing connection.
- The message through which the data is sent is encrypted using both 128 bit Advanced Encryption Standard (AES) encryption as well as RSA Cryptography schemes.

The IVM hardware is a special purpose controller that does not use any Windows, Linux or other PC based software. Furthermore, the IVM vending controller is designed in such a way as to require manual intervention on the vending machine before any configurations or programming can be sent to the vending controller. In this way, it is impossible for hacker to download a virus into the terminal.

The vending machine is equipped with a TCPIP compatible network adapter that can be customized to accommodate most any typical Internet Protocol network. I'm sure the initial reaction to the thought of a third party IP device on your computer network brings some concern and anxiety. The IP device manufacturer utilizes a proprietary architecture that is simply not compatible with any general purpose computer operating system including: Microsoft Window®, Unix and its variations or Novell®. This decision is yours whether or not to allow the equipment to share space on your computer network.





Lance M. Candia  
Director, Information Technology

9901 East 30<sup>th</sup> Street, Suite A  
Indianapolis, Indiana 462229  
317-899-xxxx

**Summary:**

1. A Local Area Network (LAN) connection must be available.
2. TCP Ports *\*hidden\** thru *\*hidden\** must be open to access outbound.
3. Proxy server authentication is not supported. A proxy server workaround must be implemented.

Questions or concerns, Please contact:

Lance Candia  
Director, Information Technology  
Int*\*hidden\**ent  
(317) *\*hidden\**