Will My Customers Let Me Connect?

How to Overcome Remote Connectivity Security Concerns

Many Original Equipment Manufacturers (OEMs) love the idea of remotely connecting their equipment but are worried about the complexity of managing connections, and dealing with end-user security concerns. The biggest hang-up tends to be around establishing a VPN connection and dealing with firewall and routing issues. Fortunately, there is a better alternative to VPN for remotely connecting.

The Pros and Cons of VPN

VPN (Virtual Private Network) is designed to connect an external user to a network. VPN works great for telecommuting, but is not the best option for connecting to remote equipment. For example, if you work from home, you can make a VPN connection to your company's network and access all the files and data you normally would at the office. It is understandable that end-user IT groups refuse to allow that same type of network access to an outsider. IT can limit the remote user to specific devices, but this means that IT has to do additional time-consuming configuration work. VPN has somehow become the de facto standard for remote connectivity to automation equipment, but it is certainly not the best solution.

A Better Solution: Connect Out, Not In

Incoming VPN connections require the end user to open an incoming port, essentially creating a hole in their firewall. A better solution is to have the equipment make an outgoing connection to a specific cloud-hosted server. Most locations allow an outgoing connection to allow users to access the internet from behind their firewall, so typically no changes to firewall settings or security policies are required. Connecting out to a specific trusted server helps alleviate concerns about connectivity to the public internet.

RRAMAC
CONNECTED SYSTEMS

(844) 4RRAMAC • 763.544.6638
www.rramac.com • info@rramac.com

Why use a Cloud based solution from RRAMAC?

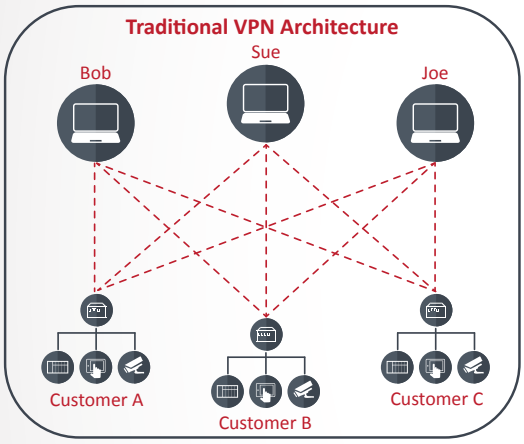
RRAMAC has been implementing cloud hosted data solutions for nearly a decade. We not only simplify the remote connectivity aspect of the Industrial Internet of Things (IIoT), but we also have the expertise to help you get the right data from your controllers, drives, embedded devices, or other equipment. Our cloud hosted solutions include predictive maintenance, downtime analysis, inventory tracking, and other custom reports. Your information is available on web based dashboards, historical trends, text and email notifications, and custom mobile apps.

Encryption and Security Certificates

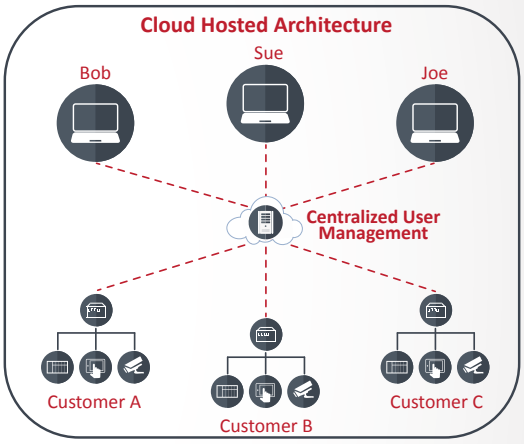
When connecting out to a cloud hosted server, data encryption is used to prevent unauthorized access to data. Security certificates are used to make sure that the data goes only to the specified server. Encryption and Security Certificates are used by banks and credit card companies for internet transactions. This same technology can be used to make sure that the outgoing connection from a customer's equipment can connect only to the designated cloud server. When an authorized user wants to access the data, encryption and security certificates are used to validate that user's connection to the cloud server.

User Account Management

A cloud-hosted connectivity architecture is far more secure and easier to manage than traditional VPN when it comes to managing user login accounts. Suppose that an OEM has three people that need to connect to three customer sites.



In this scenario Bob, Sue, and Joe, would need usernames and passwords on each remote customer site. Adding and deleting users from each individual site is tedious, so many OEMs end up having a single login for all users. This means former employees often still have access.



In this scenario, the user accounts are created and managed on the cloud server. If Joe leaves the company, his login can be deleted for all sites with a few mouse clicks.

Network Isolation and IP Conflicts

The other inherent problem with using VPN for data collection is that it is difficult to connect to multiple customer sites simultaneously. Since VPN is designed to connect you to a remote network, you cannot use a single VPN if you want to connect to multiple customers simultaneously. The VPN would interconnect the customer sites and would result in IP conflicts as well as security concerns. Here again, a cloud hosted server with security certificates is a much better solution. Multiple sites can connect into the same cloud server simultaneously just like multiple bank customers can do online banking at the same time.

RRAMAC
CONNECTED SYSTEMS

15400 Medina Road
Plymouth, MN 55447

(844) 4RRAMAC • 763.544.6638
www.rramac.com • info@rramac.com