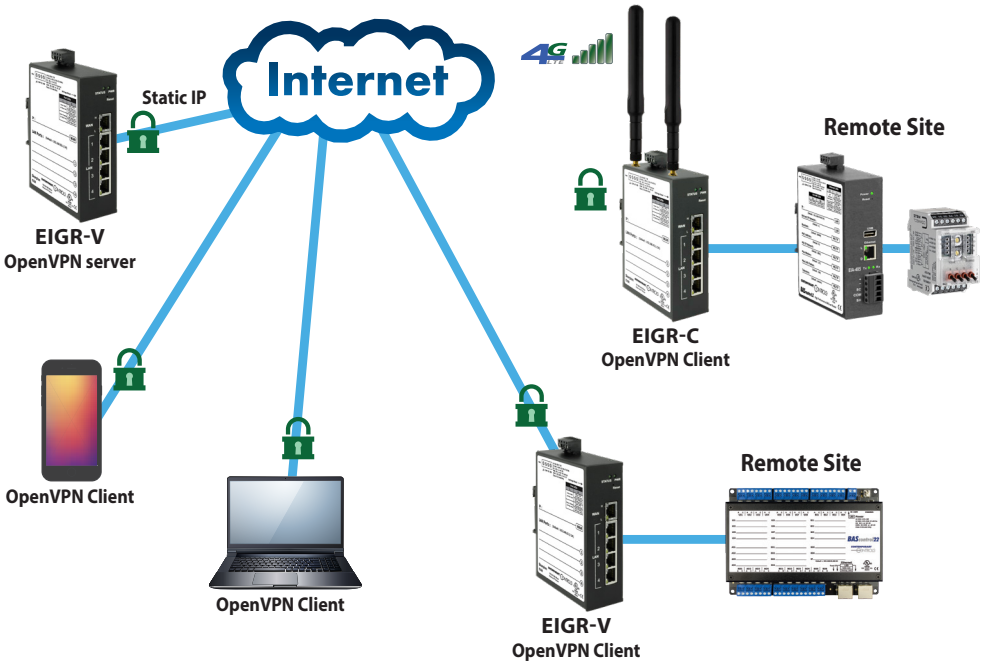
Self-HostedVPN – Secure, Remote Communications over the Internet

Utilizing the Internet for remote commissioning provides convenience while saving time and money. However, accessing equipment at remote sites can be difficult because firewalls block messages that originate from the Internet. Although it is possible to open ports in firewalls using port forwarding, IT professionals are often reluctant to compromise the security of their networks and usually decline this type of request. Without support from the IT department, the system integrator is usually left with very few options.



One solution to this problem is to incorporate a Virtual Private Network (VPN). A simple VPN can exist between two end points, called a VPN tunnel, between a client and a server. One end point (server) is you at your office, and the other (client) is at the remote job site. Communication is encrypted – so only authorized devices can communicate over the VPN.

A VPN service, such as Contemporary Controls' RemoteVPN subscription service, provides secure communication and the convenience of remote access without the burden of having to maintain the VPN server.

However, for network savvy customers, Contemporary Controls offers a Self-HostedVPN solution which allows users to set up and maintain their own secure, remote access without subscription fees and without the need for a cloud-based VPN server.

Contemporary Controls' EIGR-V Skorpion Gigabit IP router can be configured to operate in OpenVPN server mode which allows the router to act as the VPN server with the ability to support our wired and cellular routers as VPN clients. OpenVPN® is a well-supported open-source VPN technology that incorporates SSL/TLS security with encryption. Any IP program (TCP or UDP) can communicate via Self-HostedVPN. Once the VPN connection is established, messages can originate from either side –eliminating the need for port-forwarding.

How it works

Setting up an OpenVPN server on your own is not trivial. It typically involves setting up a root certificate authority and generating certificates and keys for the OpenVPN server and for each client device that intends to connect to this server. However, the EIGR-V router has a built-in webpage interface to generate certificates and keys for VPN client devices, without requiring users to download software or having to learn the complexities of setting up a VPN.

For Self-HostedVPN, users are responsible for setting up a fixed public IP address for the EIGR-V operating as the OpenVPN server. The OpenVPN server router can also be connected behind an existing firewall/router with a public IP and use port forwarding to access the OpenVPN server. This OpenVPN server can reside at the client site or any other convenient site and uses the Internet for communicating to OpenVPN clients without any cloud service involved. This specification differs from our RemoteVPN solution, where there is no requirement of a static public IP address because the OpenVPN server is provided by RemoteVPN. Both the Self-HostedVPN and RemoteVPN solutions work for legacy IP devices where it is not possible to configure an IP gateway address on the device.

One EIGR-V in OpenVPN server mode can support up to 15 IP routers in OpenVPN client mode, allowing access to 15 remote sites via cellular (EIGR-C) or wired VPN routers (EIGR-V /EIPR-V). Additionally, 15 PC/tablet/phone OpenVPN clients are supported with access control permissions configurable via the EIGR-V's built-in webpage. These PC clients can be located anywhere that has Internet connectivity. With this arrangement, PC/tablet/cell phone clients and client routers in remote locations can communicate securely using the services of this one EIGR-V OpenVPN server to devices behind the VPN client routers. An additional benefit is that each PC client can be configured to communicate with one or more router clients independent of each other.

The Self-HostedVPN solution provides secure, remote access to any IP device by just using the VPN IP address for a device. There is no additional requirement to setup Network Address Translation (NAT) or port forwarding on the client routers as they initiate outbound connections to the OpenVPN server.

Furthermore, the OpenVPN client devices only require internet access – there is no requirement for a static or public IP address. Only the EIGR-V router running the OpenVPN server needs to be publicly accessible on a single IP port.

Features and Benefits

- Wired or wireless operation over the Internet
- Secure encrypted communication tunnels
- Free download of OpenVPN client software for Windows, Linux, iOS, and Android
- Internet communication to clients at remote site or any convenient site with Internet connectivity without cloud service
- Support for up to 15 Cellular/VPN routers and 15 clients on PC/tablet/cell phone
- Secure remote accessibility to any IP device using its VPN IP address and without NAT or Port Forwarding for individual devices
- Static or public IP address not required for client devices
- Accessible behind firewall/router with a public IP
- Independent client communication with one or more router
- Applicable to both permanent and temporary remote access
- Flexible man-machine and machine-machine applications
- Quick realization of a remote access project
- Simultaneous access to multiple, remote sites

Self-HostedVPN is a VPN solution that uses Contemporary Controls' EIGR-V IP router operating as an OpenVPN server. The Self-HostedVPN server allows EIPR-V, EIGR-V and EIGR-C IP routers in OpenVPN client mode to communicate at remote sites. Any Windows, Mac, Linux, Android, or iOS device can run the open-source OpenVPN client software. OpenVPN client software – running behind the scenes – allows any program to communicate via Self-HostedVPN. The OpenVPN client can be downloaded from OpenVPN.net, via Google Play store (for Android devices), or via the Apple App store (for iOS devices)

Available on the App Store

Google play

Application 1 – Automation System using Wired Remote Access

Here we have a PC sitting in your office running OpenVPN client software behind a firewall. It connects to your Self-HostedVPN EIGR-V OpenVPN server over the Internet. At the remote site is an EIGR-V or EIPR-V OpenVPN client with its WAN port connected to the Internet as well via an existing Internet router. It can communicate via its LAN ports to any IP device used in building automation systems, such as BACnet routers, and industrial automation systems, such as HMI, PLC, and drives. Ethernet switches can be added to add more devices. The two clients communicate through the existing Internet infrastructure without the need for NAT or port forwarding for individual devices.

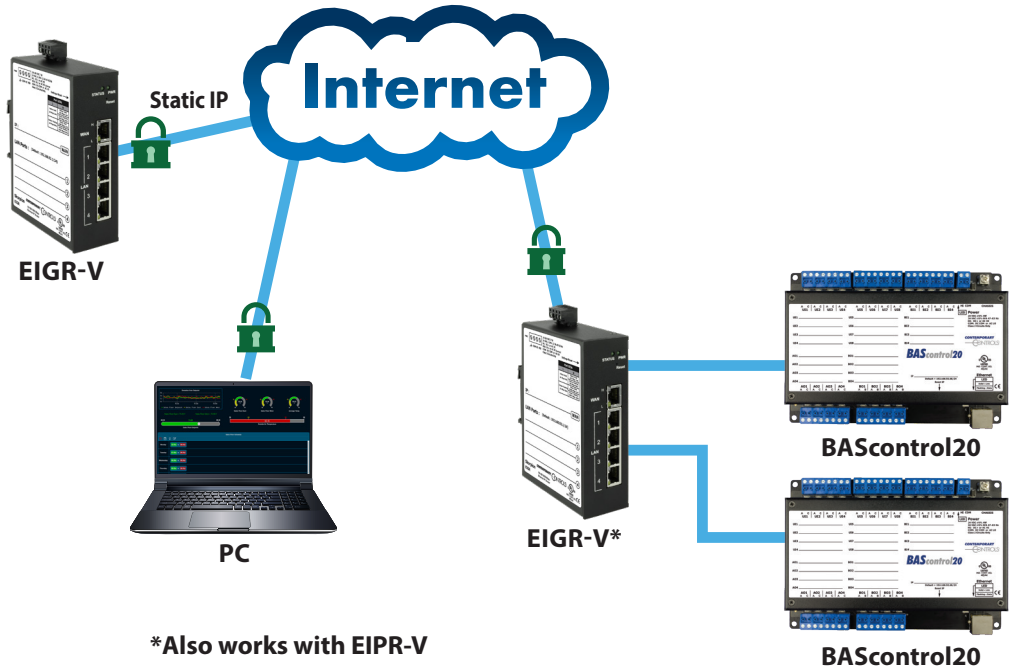


Figure 1 Wired Remote Access for Building Automation System

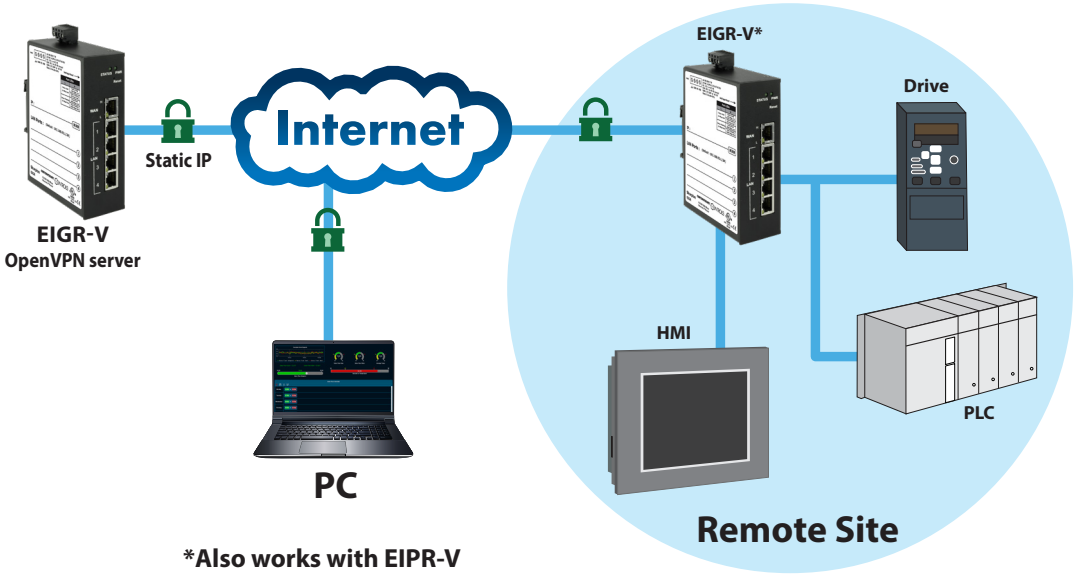
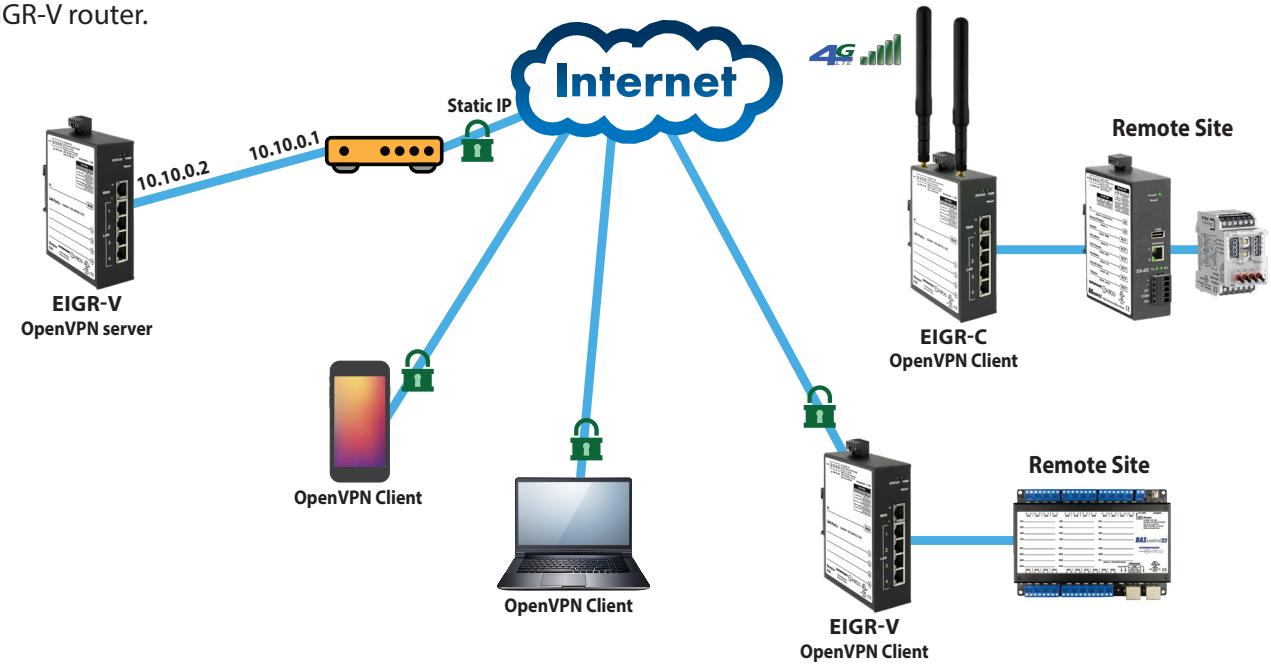


Figure 2 Wired Remote Access for Industrial Automation System

Application 2 – Connecting the OpenVPN Server Router Behind an Enterprise Router/Firewall

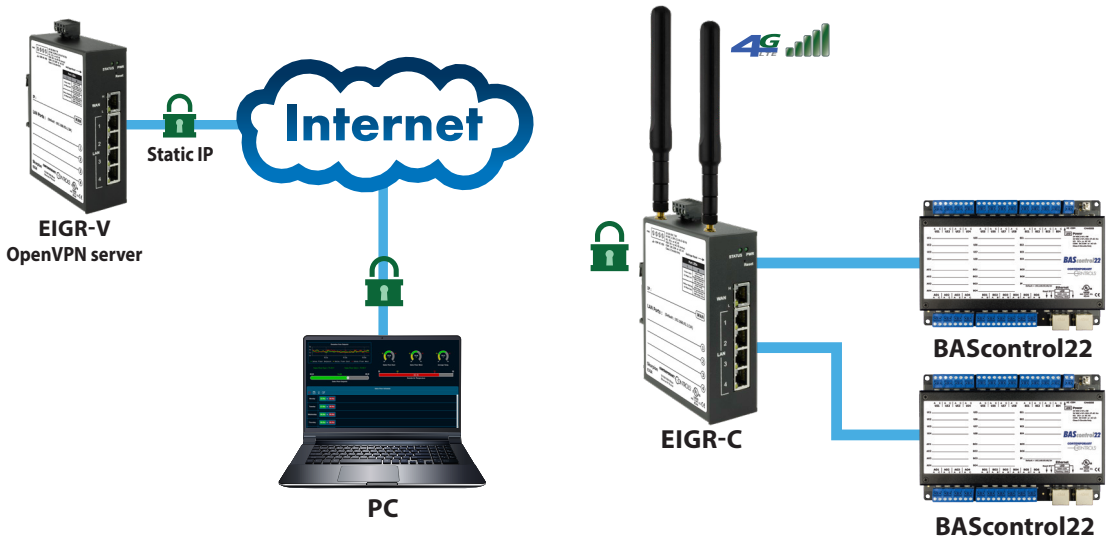
This application shows the ability to connect the EIGR-V OpenVPN server behind an existing enterprise router/firewall that has a static IP address. The EIGR-V doesn't have to be connected directly to the internet with a static IP for the Self-HostedVPN solution. The enterprise router needs to have a Port Forwarding entry for the OpenVPN port to the IP address of the EIGR-V router.



In the example above, if UDP port 5845 is being used as the OpenVPN port, the enterprise router/firewall at 10.10.0.1 will have a Port Forward entry for UDP port 5845 going to EIGR-V router at 10.10.0.2 at UDP port 5845. The EIGR-V will use the Static IP of the enterprise router for OpenVPN configuration setup webpage.

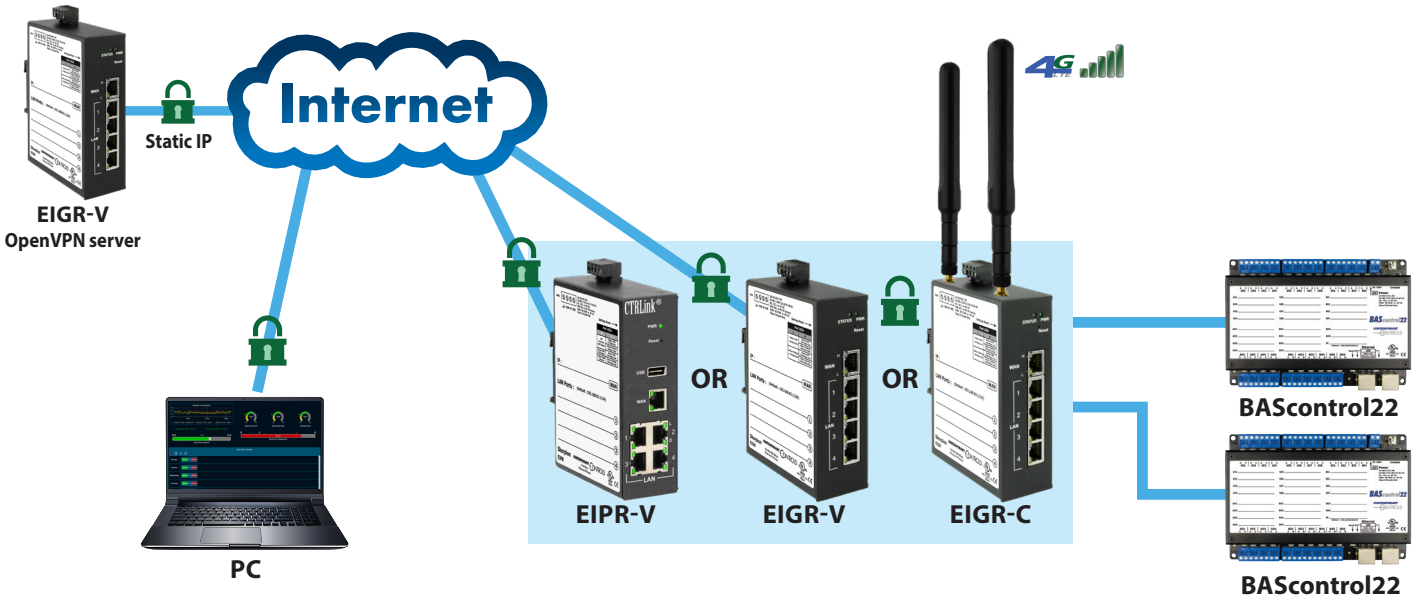
Application 3 – Automation System using Cellular Remote Access

This application is almost the same as Application 1. The difference is that an EIGR-C is utilized as the OpenVPN client to connect to the Internet via its internal cellular modem. All communication occurs with secure VPN connections even though an Ethernet link to the Internet at the remote site is not being utilized.



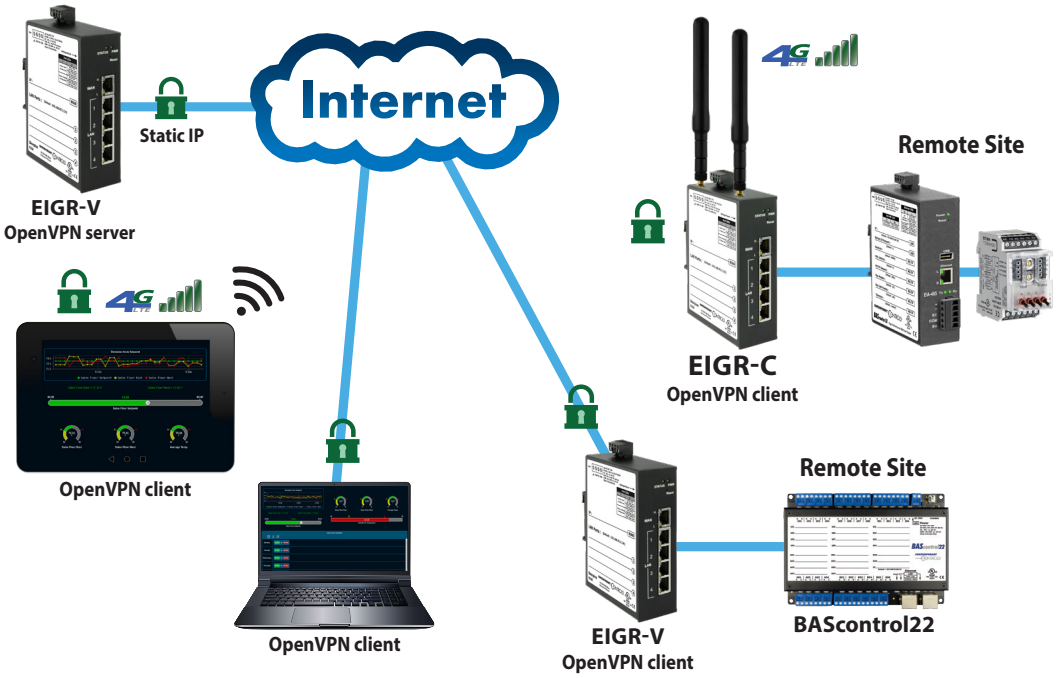
Application 4 – Remote Site Startup Before the Infrastructure is Completed

This application is similar to Application 2. Remote equipment startup is desired before an on-site Ethernet link is completed. The EIGR-C is utilized to establish secure equipment communication for commissioning, and then it is swapped out for an EIPR-V or EIGR-V when the Ethernet infrastructure becomes available. The EIGR-C can then be reused for startup at future locations.



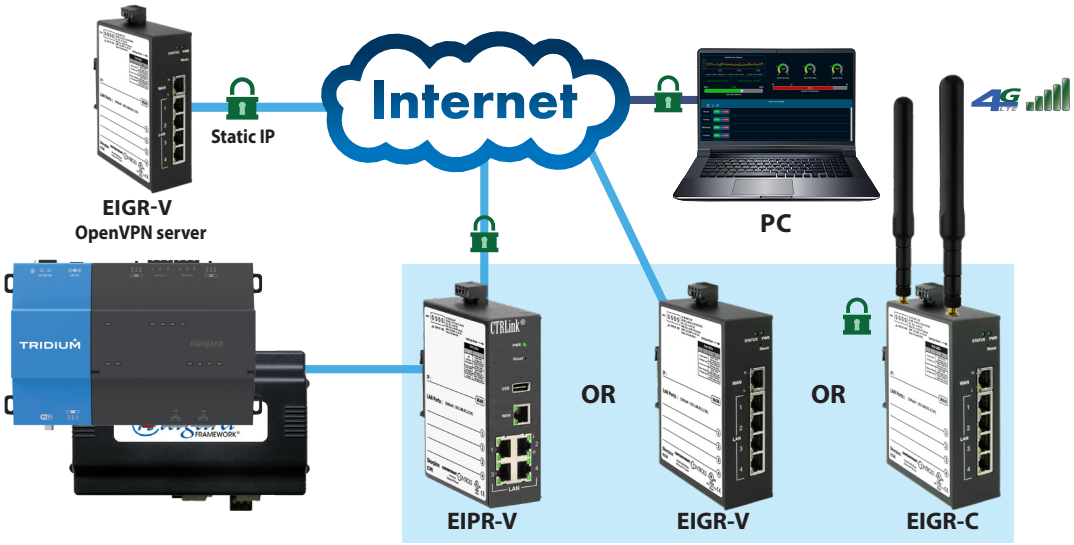
Application 5 – Cellular Access at Multiple Sites

In this application, in addition to having an EIGR-V OpenVPN server and a workstation with an OpenVPN client, you also have an OpenVPN application on your cellular device (your phone or tablet) and an EIGR-C at the job site. Both devices communicate directly to the EIGR-V via the Internet and secure VPN communication occurs. One EIGR-V can support up to 15 Cellular/VPN router clients at remote sites and 15 clients on PC/tablet/phone. These PC clients can be located anywhere that has Internet connectivity.



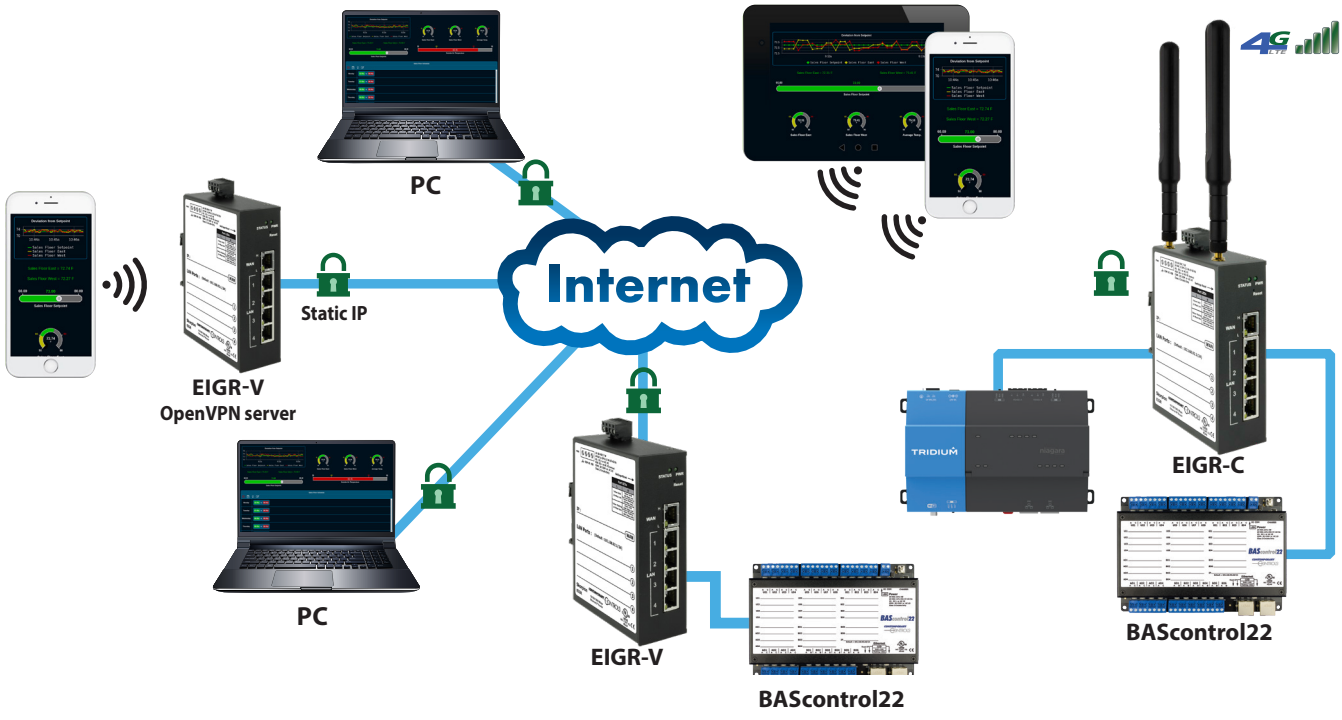
Application 6 – Remote Access to an Existing Automation System such as a JACE

Here we can isolate our remote communications to one device in an automation system such as a JACE®, which is frequently used in building automation systems. In this example you can have all the automation devices connected to one port of the JACE while the EIPR or EIGR connects to another JACE port. Either wired or wireless communication can be utilized. Remote access, even though it is encrypted and secure, can thus be isolated to one device for an added layer of security. Self-HostedVPN also supports the ability to communicate to the JACE using its secondary port if the JACE primary port is communicating to an existing network on a different subnet.



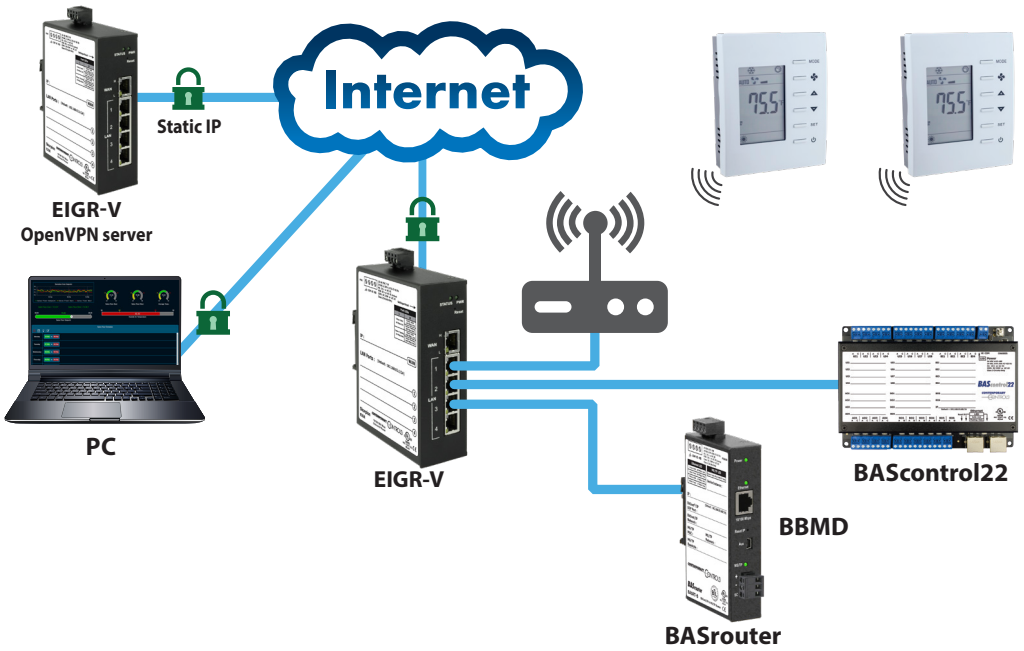
Application 7 – Varied Clients

In the previous examples we only showed one EIPR-V, EIGR-V or EIGR-C being used at a time with one workstation or mobile device. With Self-HostedVPN, you can interconnect up to 15 cellular/VPN routers and 15 clients on PC/tablet/ cell phone and communicate to all the connected systems from all your devices. As in previous examples, many control devices can connect to the LAN ports of an EIPR or EIGR. All of these can then be accessed within the VPN.



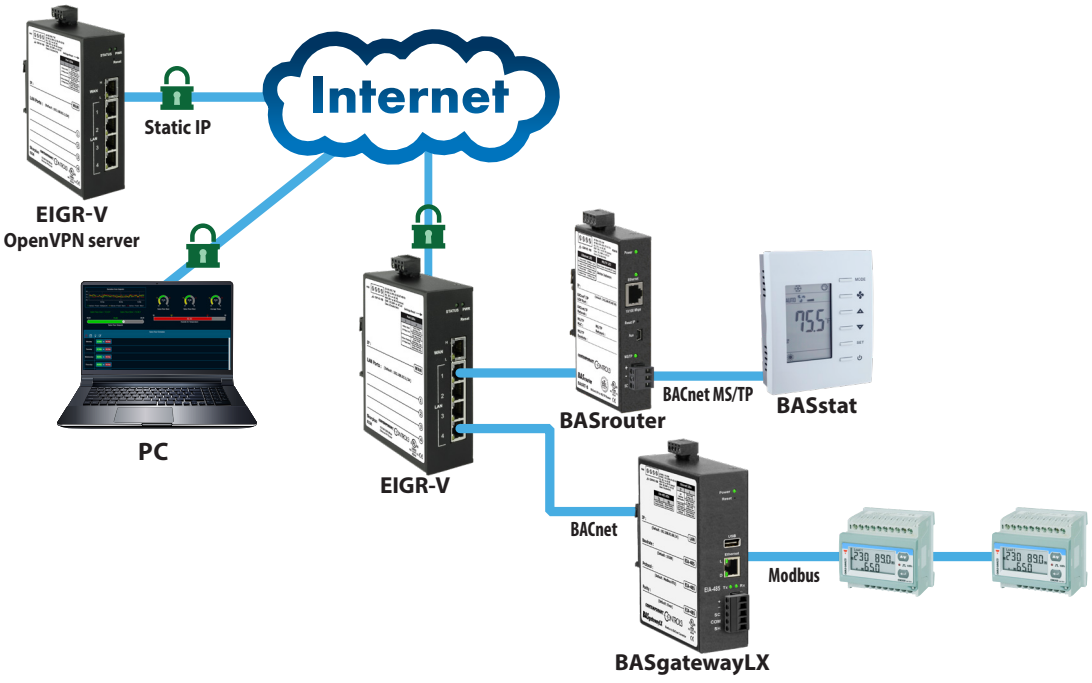
Application 8 – Using Wi-Fi with Wired or Wireless Internet Connections

Wi-Fi enabled devices, such as our BASstat thermostats, can communicate within a Wi-Fi infrastructure that in turn communicates with our Skorpion router via a LAN port. Our router then communicates securely via the Internet or wirelessly to your office, device, or alternate location as discussed in previous applications. This allows Wi-Fi devices to communicate via Self-HostedVPN.



Application 9 – Interconnect to Other Topologies

There are numerous data communication protocols that utilize Ethernet, but we focus our efforts on BACnet. In this application we utilize a BASrouter to interconnect BACnet Ethernet to a BACnet MS/TP network and a BASgatewayLX to interconnect BACnet to a Modbus serial network. The EIPR-V, EIGR-V or EIGR-C located on the Ethernet side of these networks allows secure Internet access to these devices using Self-HostedVPN.



What is the Difference Between Self-HostedVPN and What I have Today?

If you have Internet access through a firewall and you want to achieve remote access to a facility without using Self-HostedVPN, you will need to enable port forwarding in your firewall for the ports used in your communications.

Opening Ports

Typically, port 80 is used for web browsers, and port 47808 is used for BACnet communications. In this case, you would need to set up your firewall to do port forwarding for these ports. When you open a port, you must indicate which device is to receive this communication. Each port typically only allows you to remotely access one device so multiple ports will be required. Plus, you have now exposed these devices to malicious Internet activities. With Self-HostedVPN there is no need to change firewall configurations, and you do not need to expose your devices to the Internet. Your devices remain safe and can easily communicate with the Internet using our secure Self-HostedVPN solution.

Fixed IP Address

Also, many internet connections have changing IP addresses. You might need to configure your firewall to use DynDNS – giving you a permanent public IP address for your internet-exposed devices. The Self-HostedVPN solution provides secure, remote access to any IP device using the VPN IP address for the device. The OpenVPN client devices do not need fixed or public IP addresses, they only require internet access. The only requirement for a fixed public IP applies to OpenVPN server router.

Security Exposure

Many wireless providers are offering wireless routers to their customers. These devices may offer Wi-Fi or wired connections. However, in most cases when using these devices your own devices will still be behind a firewall, and you won't be able to reach them remotely over the Internet. In rare cases, the wireless provider will offer a fixed public IP address (usually for an extra fee). In this case your devices are now directly exposed to the Internet. Using our Self-HostedVPN solution, the EIGR-V router in OpenVPN server mode resides at the client site or any convenient site and is assigned a fixed public IP address. The OpenVPN server router itself can be connected behind an existing firewall/router with a public IP and use port forwarding to access the OpenVPN server.

Computer Emulation

Some people tell us they have a PC on-site at the remote location and they just use an application like TeamViewer or GoToMyPC to access the site. There are a couple of issues with this arrangement. One is that you are relying on this device to be running when you need it to perform your remote access. You need to keep it up to date with security patches, anti-virus programs, etc. This PC must also contain all the tools you use when troubleshooting your network. This could be very expensive with licensing requirements for these programs. With Self-HostedVPN you only have an EIPR or EIGR onsite (mounted securely in a control panel) and you can have all your tools installed on your access devices back at the office.

To learn how to configure the EIGR-V as a VPN server, see the **Application Note, Configuring an EIGR-V Gigabit IP Router as an OpenVPN Server**.

United States
Contemporary Control Systems, Inc.
Tel: +1 630 963 7070
Fax:+1 630 963 0109
info@ccontrols.com

China
Contemporary Controls (Suzhou) Co. Ltd
Tel: +86 512 68095866
Fax: +86 512 68093760
info@ccontrols.com.cn

United Kingdom
Contemporary Controls Ltd
Tel: +44 (0)24 7641 3786
Fax:+44 (0)24 7641 3923
info@ccontrols.co.uk

Germany
Contemporary Controls GmbH
Tel: +49 341 520359 0
Fax: +49 341 520359 16
info@ccontrols.de

www.ccontrols.com