BridgeVPN – Secure, Remote Communications for Single-Site Access

Utilizing the Internet for remote commissioning provides convenience while saving time and money. Contemporary Controls' EIGR-VB Gigabit IP router can be configured as a wired bridge VPN server for single-site, remote access solutions. With this configuration, users set up and maintain their own secure remote access without subscription fees and without the need for a cloud-based VPN server.

A VPN can exist between two end points, called a VPN tunnel, between a client and a server. One end point (client) is at your office, and the other end point (server) is at the remote job site. Communication is encrypted, and only authorized devices can communicate over the VPN.

Operating in OpenVPN* server mode, the EIGR-VB supports bridge mode where up to 10 VPN PC clients (Windows/Linux) are bridged to the router's local-area-network (LAN) side and assigned an IP address from the LAN subnet. This provides the same application experience as if the client devices were part of the EIGR-VB's LAN. It also allows passage of multicast and broadcast messages through the VPN tunnel which mitigates the need for a BACnet/IP Broadcast Management Device (BBMD) for access to BACnet systems.

Although the EIGR-VB has many of the same features found in high-end routers, it is simpler to install and commission. A resident DHCP server on the LAN side will provide IP addresses to LAN-side clients, while a DHCP client on the wide-area network (WAN) side will accept IP address assignments from the attached network. Static addressing is accommodated as well. Configuration is via a web browser using authentication.

Features and Benefits

- Wired operation over the Internet
- Secure encrypted communication tunnel
- Free download of OpenVPN client software
- Support for Linux and Windows OpenVPN clients
- Stateful Firewall and Allowlist
- Passage of multicast and broadcast messages eliminates requirement for BBMD
- Internet communication to a client at a remote site or any convenient site with Internet connectivity
- Support for up to 10 PC clients
- Independent client communication with one or more router
- Flexible man-machine and machine-machine applications
- Quick realization of a remote access project
- Individual access to multiple, remote sites

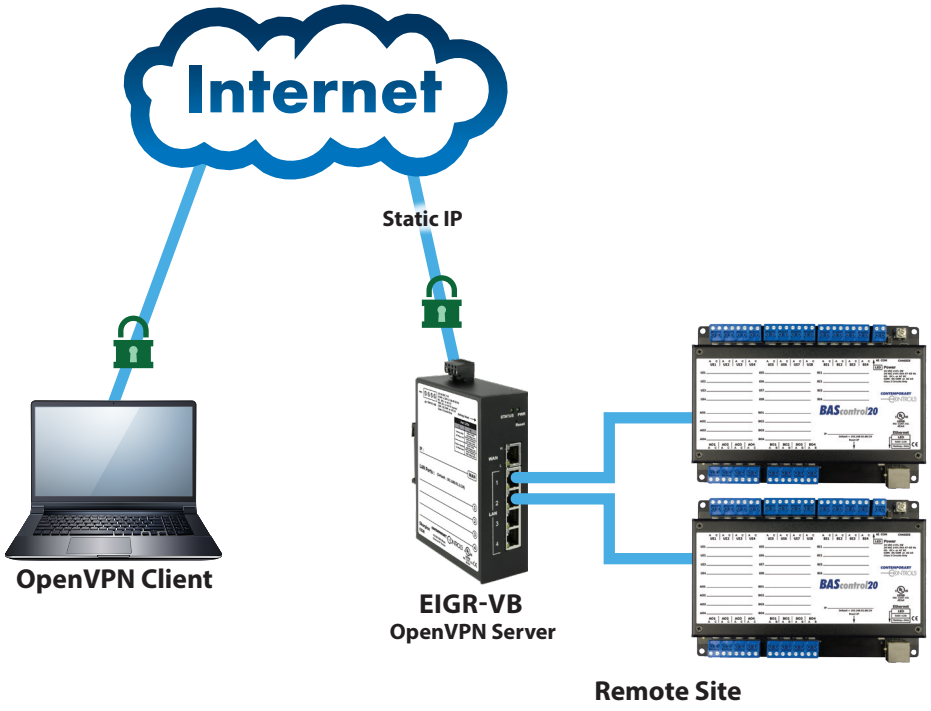
BridgeVPN

*OpenVPN® is a well-supported open-source VPN technology that incorporates SSL/TLS security with encryption.

BridgeVPN — 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-VB 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. One EIGR-VB VPN router set to OpenVPN server mode and assigned a static IP address resides at the client site or any other convenient site and uses the Internet for communicating to OpenVPN clients without any cloud service involved.

The EIGR-VB router can support up to 10 VPN PC clients (Windows/Linux). The VPN clients are bridged to the LAN side and are provided an IP address from the LAN subnet and can easily access the LAN side devices without any special configuration. Any Windows or Linux PC can run the open-source OpenVPN client software. Though OpenVPN client software is available from the Google Store for Android devices and App Store for iOS devices, it doesn't support TAP adapter required for bridge mode. For PCs, OpenVPN Version 2.x is required which corresponds to OpenVPN GUI on Windows. OpenVPN Connect (version 3.x) is not supported with BridgeVPN as it doesn't support the TAP adapter.

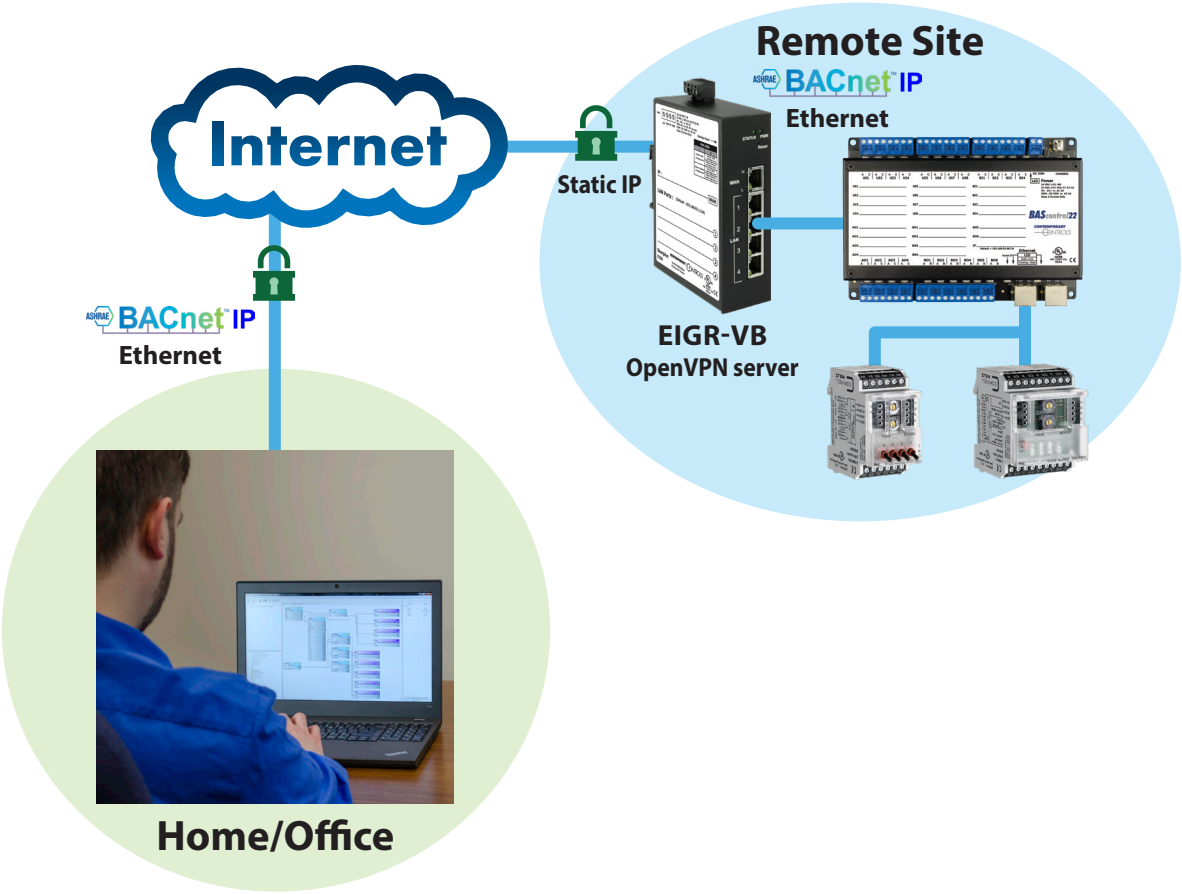


BridgeVPN — System Overview Example

The figure below shows an example of remote monitoring with BridgeVPN. A systems integrator (SI) working from the office must view a recently installed building automation site at the client's location. The SI accesses this remote site with BridgeVPN which consists of an EIGR-VB router set to OpenVPN server mode and connected to the Internet.

Using the local Internet service, the SI first opens up VPN client software (OpenVPN client) on the Windows or Linux PC to provide a VPN tunnel connection to the EIGR-VB router functioning as an OpenVPN server at the remote site. Once this connection is made, the SI can service the remote equipment as if they were physically onsite. The SI can program the Sedona controller using the Sedona Application Editor (SAE) or view the webpage. In this example, the EIGR-VB router is at the remote site and the SI accesses the Internet via a wired connection. BridgeVPN provides an effective, secure means of remote access, using the Internet to communicate with the client at a single location without subscription fees or cloud service requirements.

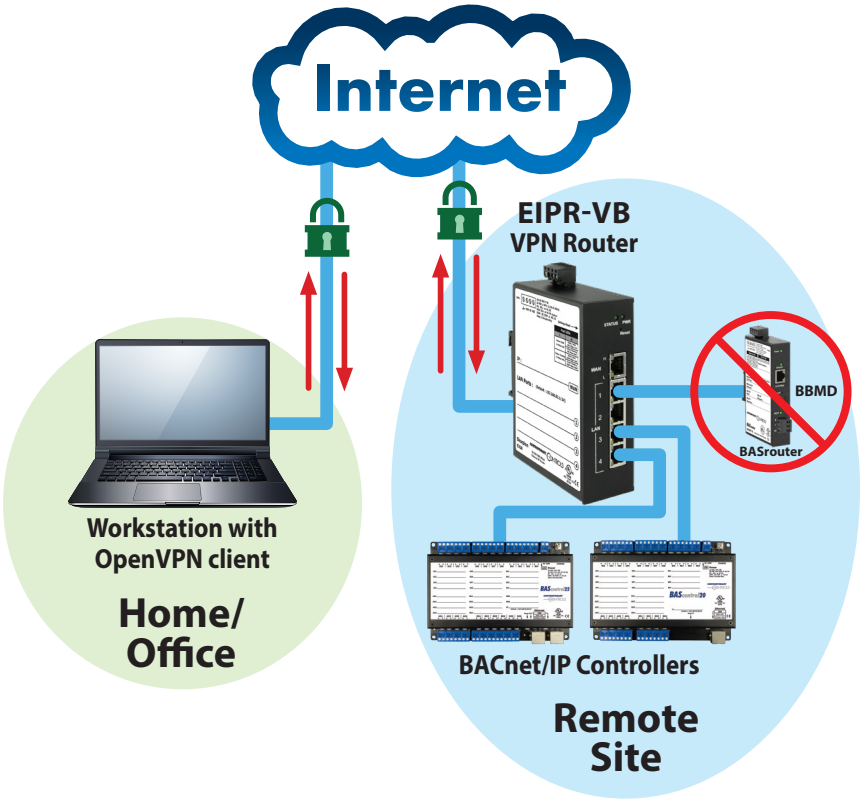
Remote Monitoring via BridgeVPN



Building Automation System using Wired Remote Access

An EIGR-VB OpenVPN server at the remote site can have its WAN port connected to the Internet directly or via an existing Internet router. If the EIGR-VB router is behind an existing Internet router, the Internet router needs to have a Port Forwarding Entry for the OpenVPN port to the IP address of the EIGR-VB router. The EIGR-VB will use the Static IP of the enterprise router for the OpenVPN configuration setup webpage.

A Windows or Linux PC in your office running OpenVPN client software behind a firewall connects to your EIGR-VB OpenVPN server over the Internet. The PC can communicate over BridgeVPN to any IP device used in building automation systems, such as BACnet controllers or routers, on the IP router's LAN ports. Ethernet switches can be used to add more devices. The VPN clients (up to 10 Windows/Linux PCs in OpenVPN client mode) are bridged to the LAN side and are provided an IP address from the LAN subnet which provides the same application experience as if the client device were part of the LAN of the EIGR-VB. This allows passage of multicast and broadcast messages through the VPN tunnel. The PC can easily run BACnet client applications to discover and communicate with BACnet devices at the remote site. Since the PC VPN interface is on the same subnet as the EIGR-VB LAN, there is no need for a BBMD.

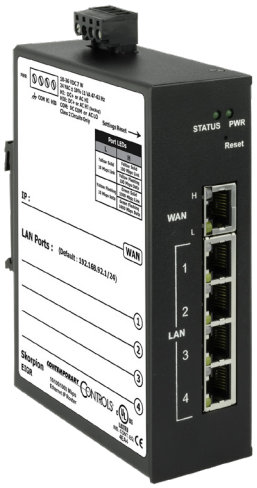


EIGR-VB Series —Skorpion Gigabit IP Router

The EIGR-VB high-speed router links two 10/100/1000 Mbps Internet Protocol (IPv4) networks, passing appropriate traffic while blocking all other traffic. One network is the LAN; the other is the WAN. The built-in stateful firewall passes communication initiated on the LAN side while blocking WAN-side initiated communication. A stateful firewall acts on the structure of the message and who is initiating and who is responding. Originating requests from the LAN side and corresponding responses from the WAN side pass through the firewall. But traffic originating from the WAN side is blocked from the LAN side unless the firewall is adjusted to allow it. This protects the LAN side from unauthorized WAN access

With Port Address Translation (PAT), LAN-side clients can access the Internet. Network Address Translation (NAT) allows a one-to-one translation between LAN-side and WAN-side devices. With Port Forwarding, LAN-side devices can be accessed from the Internet. The EIGR-VB incorporates a four-port Ethernet switch for multiple LAN-side connections. An external Ethernet-based modem—cable or DS—can be used to connect to the Internet. DSL modems connect via Point-to-Point Protocol over Ethernet (PPPoE).

The EIGR-VB includes real-time clock and OpenVPN client/server functionality. It operates over 0 to 60°C temperature range.



The EIGR-VB Gigabit IP router can be configured to operate in OpenVPN server mode as a wired bridge VPN server for single-site, remote access solutions.

Ordering Information

Model	*RoHS*	*Description*
EIGR-VB	✔	Skorpion GigE IP Router with Bridge VPN 0 to 60°C

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