INTRODUCTION

Opengear helps you manage, monitor and remediate your network remotely, even when the primary network is down. Our Network Resilience Platform provides an independent management network, giving you secure access to provision, configure and troubleshoot critical IT infrastructure without sending someone to the site – minimizing downtime, protecting SLAs, and saving money.

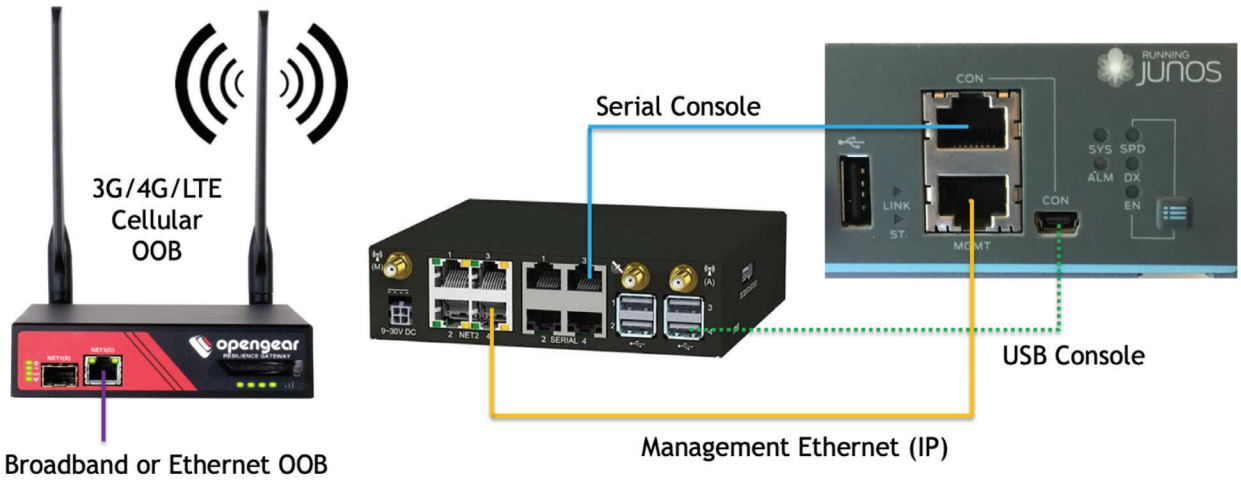
Opengear *Smart* Out-of-Band (*Smart* OOB™) appliances together with Lighthouse management software provide secure, resilient access to critical network and IT infrastructure at remote locations via serial and USB console ports. Our Remote IP Access feature takes this to the next level by providing secure IP access to equipment at edge locations. This enables an engineer or administrator to access critical infrastructure over TCP/IP, typically to equipment connected to an Ethernet management network.

In addition to direct connections to console ports, with Remote IP Access you can reach the Web GUI of remote equipment over HTTP or HTTPS, perform direct file transfers using TFTP, FTP or SCP, SSH into remote systems or virtual machines, and log in to Linux and Windows servers using VNC or Remote Desktop Protocol (RDP). This feature also allows you to use many other services that run over IP, providing emergency access to remote site equipment over the out-of-band network.

PROXIMITY

When a network engineer goes to a remote site to provision, re-configure or troubleshoot a problem, they will typically take a laptop computer, together with a serial console cable and an Ethernet cable. Each deployed Opengear appliance can provide this connectivity - we call this *proximity*.

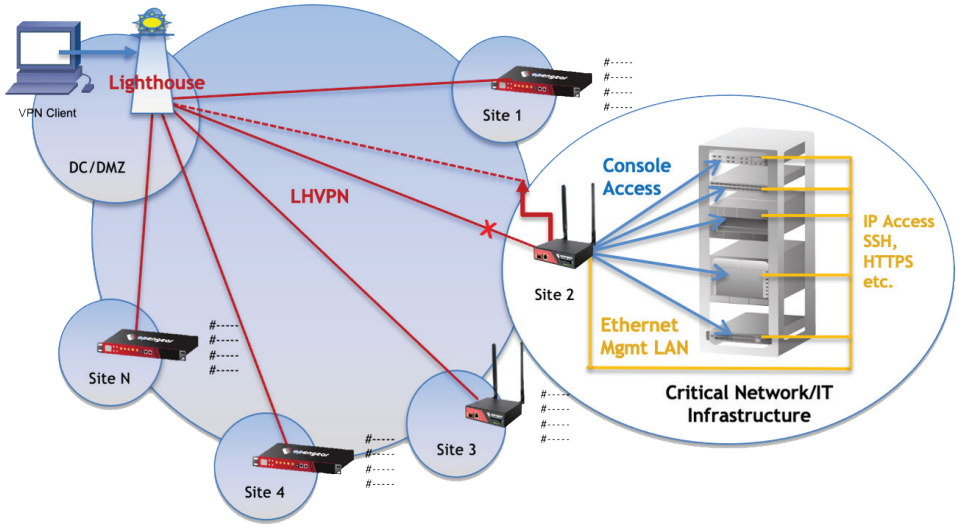
With a number of Opengear appliances deployed on the network, you have secure remote access to the attached console ports and to the management networks from one central platform, Lighthouse, which is the hub of the Opengear *Smart* OOB™ solution.



RESILIENCE

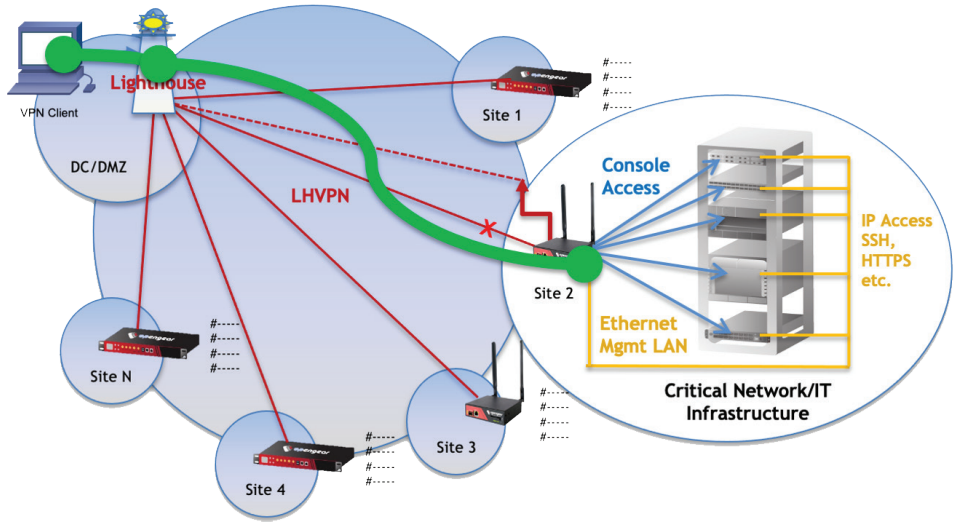
The Opengear appliances are connected to Lighthouse over a resilient fabric, the Lighthouse VPN (LHVPN) network. This fabric is an overlay VPN that uses OpenVPN tunnels with X.509 certificates, strong (AES-256-GCM) encryption and redundant connectivity, which may include failover to 4G/LTE cellular or broadband for true out-of-band connectivity.

Lighthouse management software is the central hub of the LHVPN, and also the central point of access for users to connect to remote equipment. Users connect to Lighthouse, are authenticated, and can then use the Console Gateway quick-search to find and connect to console ports using the built-in Web Terminal or their own SSH client. The resilient LHVPN fabric connects Lighthouse users to the remote Opengear appliances and the equipment they are attached to, ensuring that *Smart* OOB™ access works even if the primary network is down, and that the Opengear appliances automatically fail-over to cellular or broadband.



REMOTE IP ACCESS

Remote IP Access adds client VPN capability to Lighthouse. Engineers can launch a VPN client connection to Lighthouse, be authenticated, then automatically connected to the remote site management network. Now the engineer has a secure VPN tunnel to the remote equipment they need to work on, providing the same TCP/IP access they would get if they travelled to the site and plugged into the management LAN. The massive benefit is that they don't need to physically travel to the site, because they are connected remotely.



EASY-TO USE SECURITY FEATURES

Opengear's Remote IP Access feature makes use of Lighthouse resilient connectivity, and also leverages Lighthouse centralized security. The OpenVPN client connection requires a user to authenticate to Lighthouse with their username and password in the usual way. Lighthouse supports local or remote authentication using AAA (RADIUS, TACACS or LDAP), which may include 2FA/MFA. The Remote IP Access client connection is already multi-factor authenticated: it uses a certificate to authenticate each client, in addition to the username/password combination to map the user into a group from which Lighthouse determines privileges and access to resources - for example, which sites or nodes the user can see and connect to.

The Lighthouse administrator can create new certificates for Remote IP Access users from the Web GUI. These certificates are generated within an OpenVPN config file that the user can easily import into their OpenVPN client as a new connection profile. If a user subsequently leaves the company, the Lighthouse admin can simply revoke their certificate to prevent further VPN client access.

SAMPLE USE CASES FOR REMOTE IP ACCESS

Use Case #1: Customer migrating to Virtual Firewalls

Many customers are migrating from traditional hardware-based firewall appliances to a virtual firewall solution. The hardware firewalls have console ports, but many users prefer to manage them from the Web GUI, so they have Remote IP Access already deployed. They can remotely manage new virtual firewalls using IP Access too, in addition to managing the servers that they are running on.

Use Case #2: Customer with Virtual SD-WAN Appliances running under VMware

Serial console connectivity is very useful for network and security engineers - but not all appliances have serial console ports. We see an increasing number of customers beginning to deploy virtual appliances. These Virtual Machines (VMs) or Virtual Network Functions (VNFs) do not have console ports; they are accessed and managed over IP. This is also true of the operating systems and hypervisors which make up an important part of the software stack, all of which must be working for the virtual appliances to operate. Each component in the stack requires remote access for maintenance and upgrades.

Remote IP Access provides secure remote TCP/IP connectivity to each site that has an Opengear appliance deployed. The Opengear appliance provides console access to connected switches and other devices, but network engineers can also access their servers through the VMWare ESXi environment via Web browser, or using an embedded lights-out management (LOM) technology like iLO5 (HP).The virtual SD-WAN appliance also has a Web GUI providing a status dashboard and admin menus.

Remote IP Access to multiple remote networks and VLANs

Remote IP Access provides secure, remote out-of-band IP access to the management network connected behind each Opengear appliance. We have the ability to push client routes, enabling Remote IP Access users to access the local LAN segment and networks beyond. Data centers and remote sites often have more than one management network. It is not unusual for a data center to have several management VLANs, separated for security reasons - perhaps one VLAN for network management, another for management of security appliances, and several more for different server teams.

For multiple separate management networks or VLANs, Opengear has added mapping capability to the Remote IP Access solution. This feature maps IP Access users, via group membership for scalability, into one or more firewall zones on the remote Opengear appliance. This allows for variation at different sites; each appliance can have different network interfaces, including VLANs, mapped into the appropriate firewall zones. For example, a user who belongs to the Security group gets mapped to the security management zone, and is granted IP access to the firewalls. A member of the Blue Server team is mapped to the blue server zone and has IP access to the blue servers. This solution uses the Lighthouse group and Smart Group mapping, together with the firewall zone capability of Opengear NetOps Console Servers to provide a secure, flexible and scalable solution for remote IP Access to multiple edge networks and VLANs.

Note: OM1200 and OM2200 Series NetOps Console Servers have 802.1Q VLAN support (trunk and access ports)

WHICH OPENGEAR APPLIANCES SUPPORT REMOTE IP ACCESS?

The Opengear ACM7000 and IM7200 Series *Smart* OOB™ console servers support Remote IP Access. The new OM1200 and OM2200 Series NetOps Console Servers also support Remote IP Access, as well as 802.1Q VLANs and L3 segmentation of the built-in switch ports (on models with the built-in switch), enabling connections to multiple management networks or VLANs, as described above.

ACM7000

IM7200

OM1200 & OM2200

SUMMARY

The Remote IP Access feature adds a very powerful capability to the Opengear *Smart* OOB™ solution, giving users the ability to access, manage, troubleshoot and remediate their IT and network infrastructure remotely over IP using the Lighthouse VPN resilient fabric connectivity.

The Opengear solution provides both secure console access and full remote IP network access to critical infrastructure at remote sites, even when the production network is down, allowing fast response for remediation, minimizing downtime, avoiding site visits and delays, and saving money.

OPENGEAR REMOTE IP ACCESS: SECURE, SCALABLE, POWERFUL, RESILIENT EASY-TO-USE

Additional Information

Opengear Remote IP Access is a licensed feature of Lighthouse, included in the Lighthouse Enterprise subscription. It is provided as a NetOps module, called Software Defined Infrastructure (NOM-SDI).

Remote IP Access makes use of the standard OpenVPN protocol, and supports a number of third party OpenVPN clients on platforms including Windows, Mac and Linux:

- Viscosity (macOS, Windows)
- Tunnelblick (macOS)
- Pritunl (cross-platform)`
- Openvpn CLI (Linux, Unix, Windows)

Viscosity - OpenVPN Client for Mac and Windows - SparkLabs

https://www.sparklabs.com/viscosity/

Pritunl Client - Open Source OpenVPN Client

https://client.pritunl.com/

CONTACT US OR SCHEDULE A DEMO

If you are interested in the Opengear *Smart* OOB™ solution, have a question, or would like an IP Access product demo, please contact your local Opengear partner, or contact us directly at the links below:

https://opengear.com/contact-us/

https://opengear.com/schedule-demo/