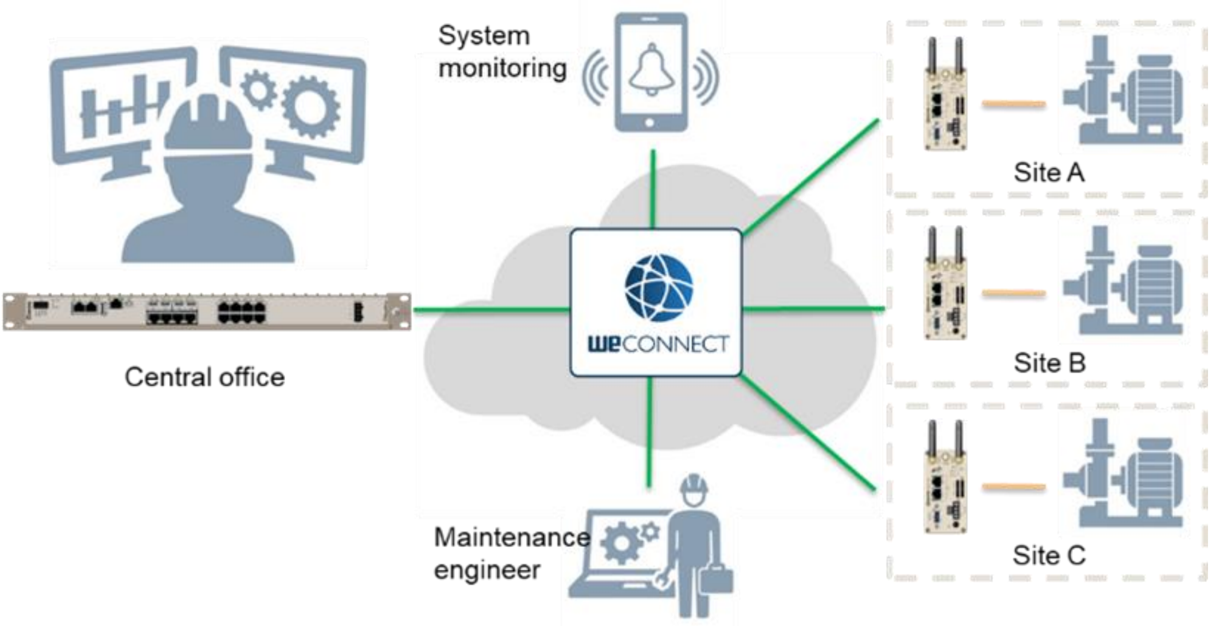
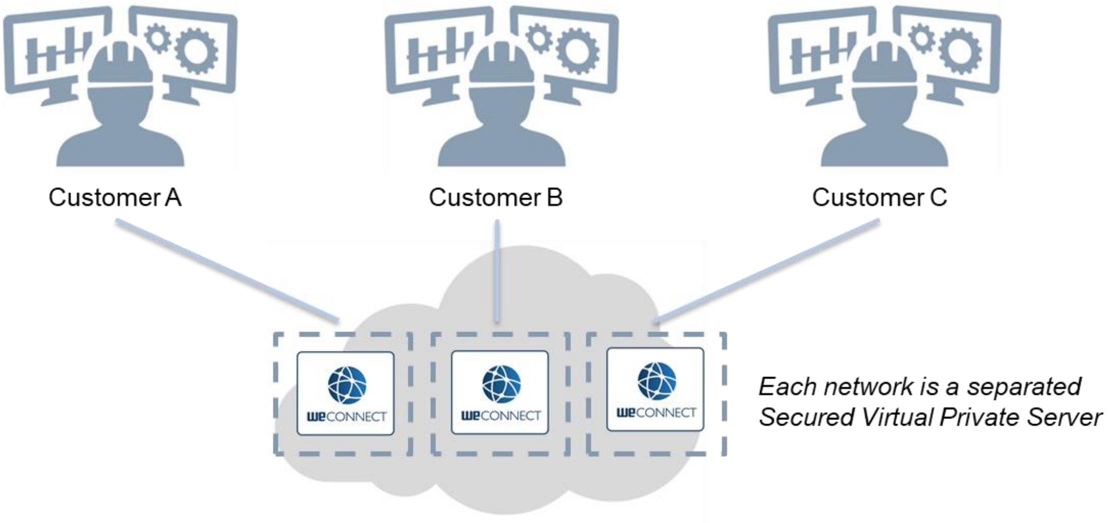
WeConnect high security VPN service



System security

Most VPN concentrator system share a VM server hosted in a Cloud server farm, so all users share the same resources. Sharing the same resources often leads to restrictions on the number of device and clients that can be connected simultaneously and could expose users to a security risk if the virtual isolation in the VM (Virtual Machine) is breached. WeConnect is structured in a way that every Secure server (VPN Concentrator) is isolated from every other secure server in the WeConnect system. To achieve this level of segregation every Secure server is running in its own VM space ensuring that there is no possibility of the Secure server being accessed from any other customer instance in the WeConnect eco system.


Customer A
Customer B
Customer C
WeCONNECT
WeCONNECT
WeCONNECT
Each network is a separated Secured Virtual Private Server

High security VPN (IEC 62443 Data Conduit)

All Nodes (remote routers) and Clients (laptops/servers/iPhone or Android) use high security SSL (OpenVPN) VPNs (IEC-62443 Conduit) running strong AES-256-bit encryption. Each Node and client have a unique certificate from a trusted PKI (Public Key Infrastructure) signed CA (Certificate Authority). There are no shared public certificates, so the loss of a client device or Node does not result in the need to change the certificate in every Node or client connected to the secure sever.

Using a certificate from a trusted CA source mitigates the possibility of a Man in the Middle attack. A Man in the Middle attack occurs when an actor is able to insert a router to terminate the VPN from a Node or client and then spoof a VPN onward to the VPN concentrator and use the access to sniff the traffic or insert new instructions to remote assets. Such attacks are possible when PSK (Pre shared key) typically a password or self-signed certificates is used to secure the VPN.

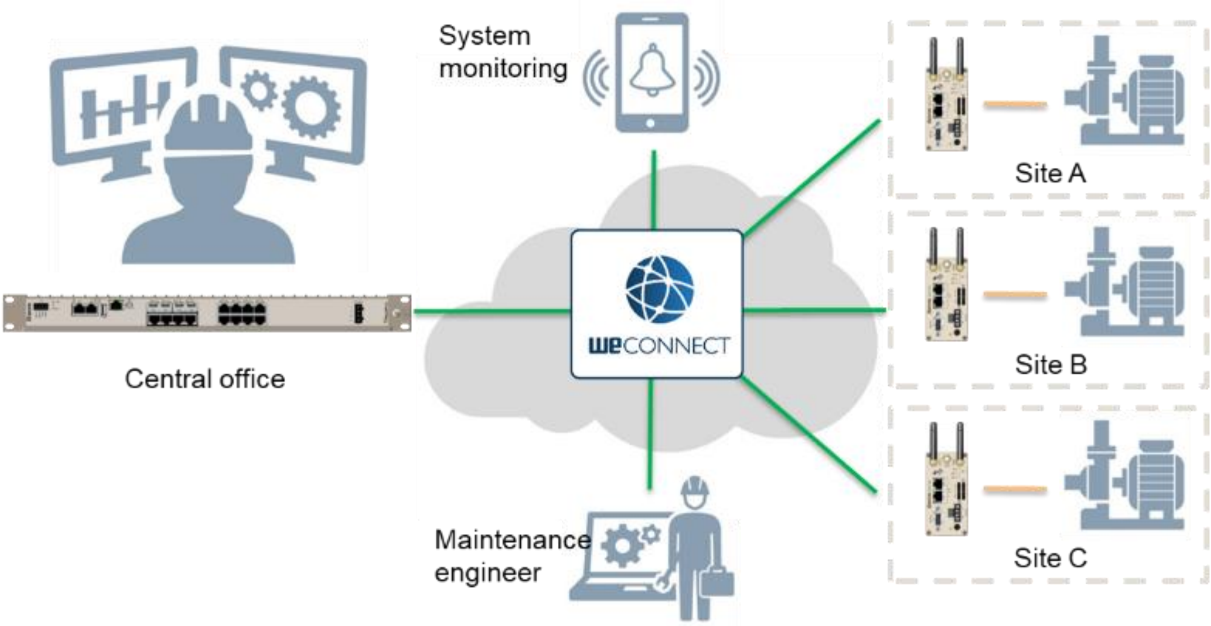
Internet access

The SSL VPN is initiated from the client or Node towards the secure server. This means the Node or client just require internet access to make a secure connection to WeConnect over any available media. The remote Nodes or client **do not** require a static IP address, just access to the internet via LTE/UTMS (using a standard SIM card), broadband connection or access via a 3rd party network such as a satellite link.

Using standard “off the shelf” SIM cards for LTE/UTMS offers an additional level of cyber security. The service providers isolate the user cellular network from the Internet using NAT (Network Address Translation) which allows access out to the internet from the service provider network, but prevents actors on the internet reaching into the service providers network and accessing a device directly. Because the IP address is hidden and effectively isolated from the internet, an actor cannot execute a DoS attack against a remote Node, carry out a port scan to look for vulnerabilities or initiate a brute force attack. The same cannot be said for static IP SIM card with a public IP address.

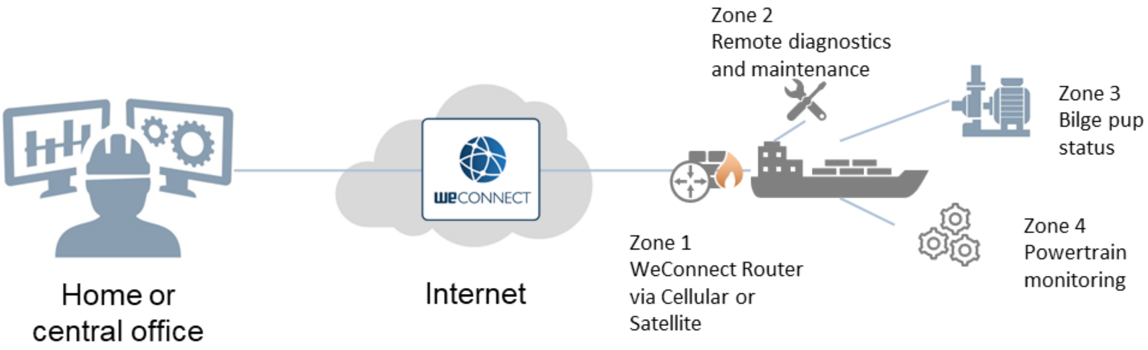
Note: WeConnect is not dependent on roaming SIM cards but, roaming SIM cards give a higher degree of system resilience due to their ability to allow a Westermo LTE/UTMS router to roam between networks should the primary network become unavailable.

Any device which supports SSL VPN can be connected to WeConnect. Laptops (Windows or Linux), iPad, iPhone or Android devices can all be used as clients. The client uses standard protocols and tools to establish the VPN. Typically, a user can download the OpenVPN client software and import the client setup file from WeConnect. Like a Node each client has its own unique certificate that can be cancelled or changed at any time. The client can be secured using two factor authentication using Google Authenticator.



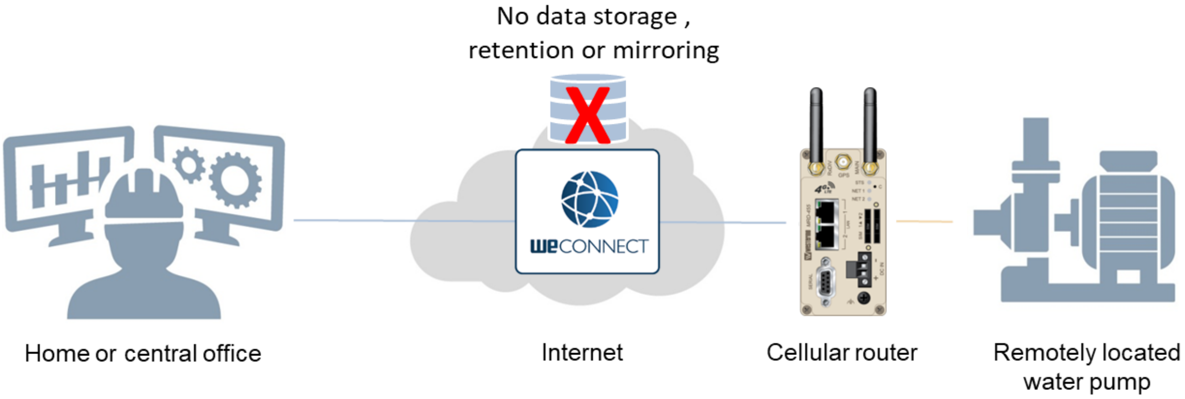
Perimeter Firewall on every node (IEC 62443 Zones)

Every Westermo device used in combination with WeConnect has its own built in perimeter firewall (configured separately). The Perimeter Firewall effectively segregates the remote network from the internet facing media (LTE, xDSL, satellite, or via factory/corporate network). Furthermore, the firewall will filter traffic over the VPN. Working on a principle of zero trust (IEC-62443) the firewall should also be applied, even when connecting to third-party network such a factory or corporate network used as transport to the internet. Depending on the size of the remote network the perimeter firewall may be the only firewall needed to create an IEC 62443 Zone. If required, the firewall can be split into multiple zones for multiple subnets . When using WeOS Layer 3 devices the remote network can be further segregated into Micro segments each of which can have its own firewall rules.



Data in transit (IEC-62443 Data conduit)

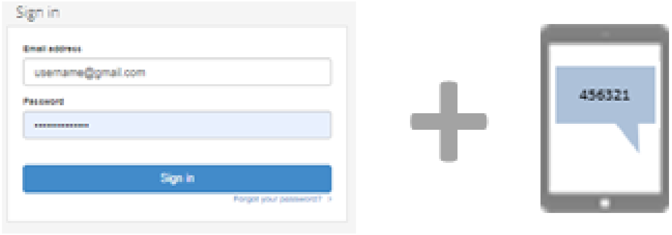
The data/packets passing through the WeConnect system are never stored, subjected to sniffing or mirroring at any point of its journey. Just like a regular router installed in an IT cooperate server room, the data from a Node or Client is received at the secure server and then redirected to the exit VPN (Data Conduit) where the destination IP address can be found.



There is an argument that the data is in unencrypted as it passes through the Secure server and is therefore vulnerable. But this is no different to a router located in the IT room! The reality is somewhat different, the data is not encrypted at the point as it traverses the secure server and exits down the next tunnel. However, to get access to the data an actor would have to gain access physically (break into an AWS data centre) or virtually to the Secure server operating system. The level of knowledge and persistence required would be very high and would be the same regardless of the router being in a cloud location or in an IT server room. The SSL VPNs are the obvious data conduits when reviewing the system against IEC 62443, but a data conduit can also be viewed as the data moving between two firewalls in the system. In effect the first firewall is limiting packets from the node location into the WeConnect VPN. The destination firewall, either a Client or a Node, will equally have a set of rules that will only forward the packet if there is a rule to do so. An example would be communication between a Modbus slave and Modbus master or SCADA system. Since we know the source IP and the destination IP and port the firewall rules can be constructed to only allow traffic through if it matches both firewalls. If traffic originates from elsewhere on the network the packet will be dropped at either firewall. In effect we have a conduit inside a conduit.

Two factor Authentication and user authority

Logging into the WeConnect management portal and the Client VPN can be secured using Two factor authentication using Authenticator apps.



Sign in

Email address

username@gmail.com

Password

••••••••••••••

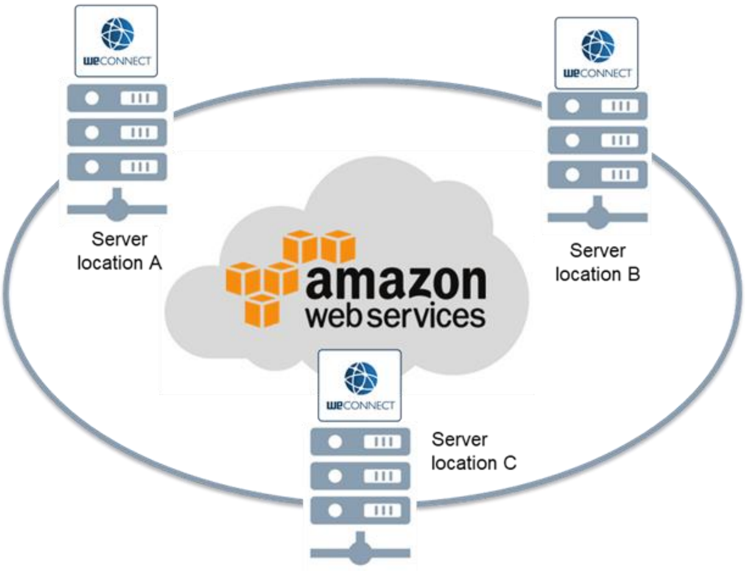
Sign in

Forgot your password?

Two factor authentication ensures that an attacker with stollen credentials still needs access to the user’s authentication device, typically a mobile phone.

System Resilience and physical security

The WeConnect system is hosted on Amazon’s Web Service (AWS), in three geographic locations around the world to reduce the local latency of data passing via the WeConnect system. At each geographic location, the system is replicated on three physically separate server centres. To ensure the maximum possible uptime each server centre has its own UPS and generator capacity in the event of a power outage. WeConnect Secure server monitors the connectivity to the internet as well as its own resources.



Should a server centre become unavailable the WeConnect system automatically replicates the Secure server on the next available server centre. Should the second AWS server centre become unavailable the Secure servers will automatically be moved to the next available AWS server centre. If the third AWS centre become unavailable, we have bigger issues to worry about!

The AWS server centres are all protect by high levels of high security and operation strict access control policies both physical and electronic. The level of integrity is well beyond anything most private or even government organisations can achieve. The list of relevant compliance standards AWS conform to can be found here.

https://aws.amazon.com/compliance/programs/

For further reading on the security infrastructure;

https://d1.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf?did=wp_card&trk=wp_card

CSIQ Compliance (CSA);

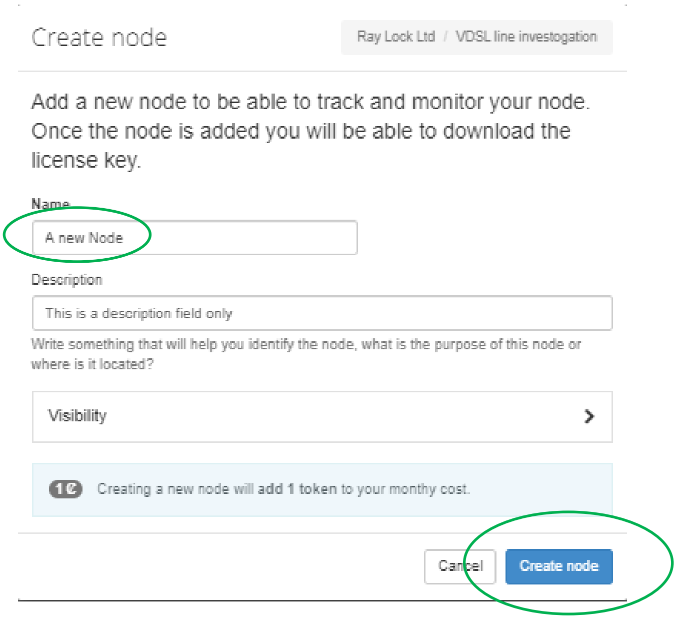
https://d1.awsstatic.com/whitepapers/compliance/CSA_Consensus_Assessments_Initiative_Questionnaire.pdf

Ease of use

WeConnect has been designed from the start as an easy to use platform. No IT or knowledge of routing is required to operate and maintain the system. The addition or deletion of Clients or Nodes is an administrative task and not requiring any IT professional involvement.

When adding a new remote Node to WeConnect, an administrator simply adds a name of the node and a description via the web portal. No other configuration details are required on WeConnect. The WeConnect system automatically create a configuration file and certificate for the new Node. At the Node (remote location) a user follows the steps in the setup Wizard to retrieve and install the configuration file and trusted CA signed certificates.

Note: The WeConnect wizard imports the VPN setup only and adds it to the local configuration of the node.



Create node

Add a new node to be able to track and monitor your node. Once the node is added you will be able to download the license key.

Name: A new Node

Description: This is a description field only

Write something that will help you identify the node, what is the purpose of this node or where is it located?

1 Creating a new node will add 1 token to your monthy cost.

Once a node has activated the WeConnect VPN will automatically upload routes to all subnets from the remote site to the secure server and the route table amended to include this new information. When a client connects all the available subnets are pushed to the clients routing table. This give the user the ability to directly address any device within the secure server. There is no need for NAPT, port forwarding or additional static routing at the node locations. As previously mentioned, the firewall on the node can be used to limit access to only relevant data streams and known addresses.

One of the major features of WeConnect is the Identical Network secure server mode. In many applications, the networks at the remote location could all use the same subnet. This could be due to always using the same configuration or the original systems were standalone. Having the same subnet at each location would cause the routing tables to become confused and devices would be unreachable. Configurating Identical networks enables support for this kind of application and still allows a client to directly address the devices on the remote network.

Scalability

WeConnect has been designed to automatically scale as a user adds clients and Nodes. A system can start with just a few VPNs and grow to many hundreds or thousands over time. There is no limit to the number of VPNs that can be terminated and used simultaneously on a WeConnect secure server. As the need for resources increases so does the VM instance.

The WeConnect system can also scale by adding additional Secure servers. In some instances, it may be desirable to separate an organisations customers to maintain segregation. Again, there are no limits to number of secure servers that can be started in the management portal. There is an additional cost for each Secure server that would need to be factored in.

Data Usage

Each Node and client have a data allotment of 2GB per month. The Nodes and Clients are pooled together . For example, a secure network with 10 Nodes and Clients would share a pool of 20GB a month. Some devices may take more than 2GB a month and others less, if the pool is not exceeded there is no issue. If the pool is exceeded, then extra data can be added at a cost of one token per month for each additional 2GB.

Number of concurrent connections

Unlike most of the cloud-based VPN systems there are no limits to the duration or numbers of clients that can be connected concurrently to WeConnect nor any additional cost for 24/7/365 connectivity. If a system comprises of 20 remote Nodes and 10 engineers all can be connected simultaneously 24/7/365. Furthermore, multiple clients can access the same Node or multiple Nodes can be connected to each other depending on the Secure server type, see modes of operation below.

The always on nature of WeConnect means that wide are SCADA solutions can be implemented in much the same way as legacy leased lines were used to connect SCADA systems to remote locations for data gathering and/or control. Whereas lease lines were dedicated to a single protocol connection, WeConnect will allow multiple conversations to take place simultaneously to the remote site e.g. SCADA control using DNP3 or Modbus and configuration/software update of the devices on site.

Secure server Modes

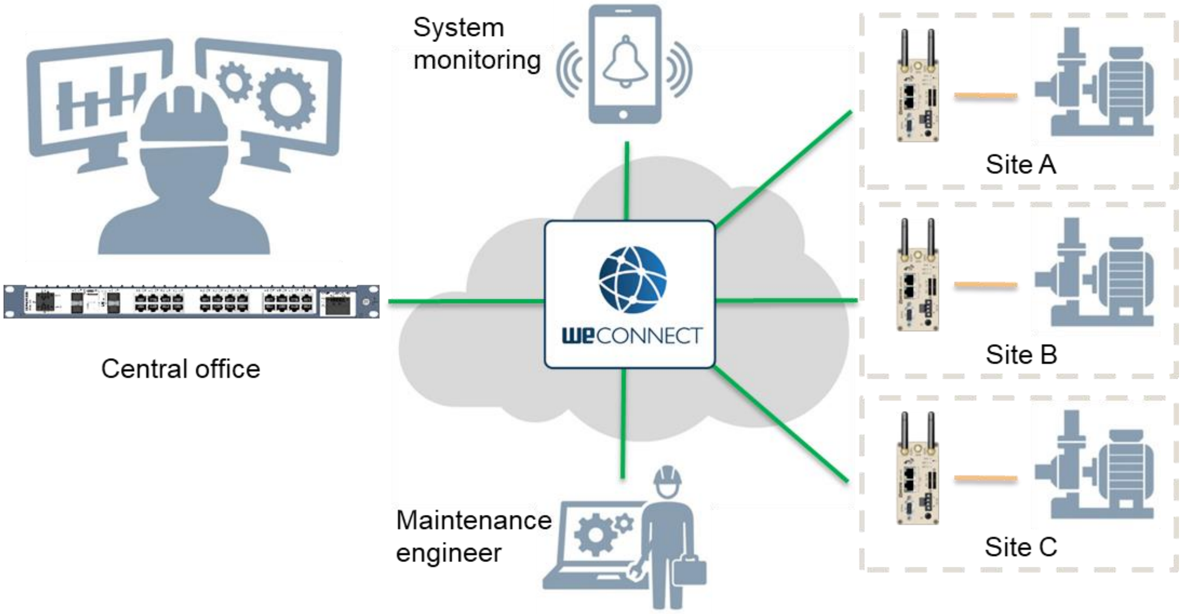
Remote access breaks down into 3 main groups or requirements.

One to Many
Many to Many
Identical networks

The WeConnect system has been designed to make implementing each of these requirements as easy as possible. Simply selecting the server type automatically sets up the routing profiles and rules for the different types of application. See below for a description of each of the Secure server types.

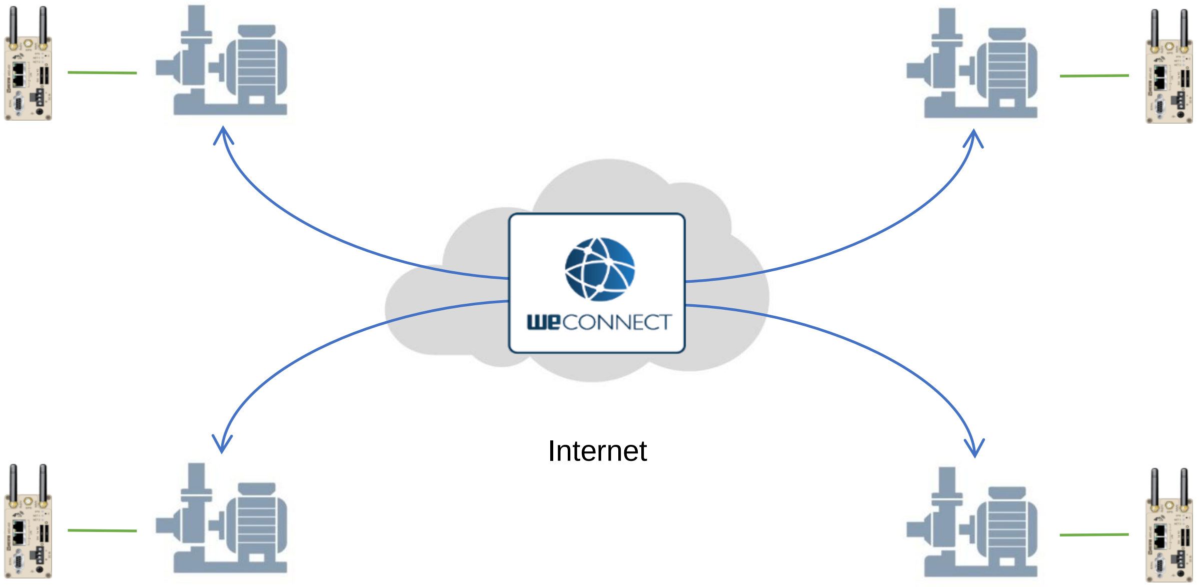
One to Many

One to many is typically used for data gathering e.g. a SCADA polling or remote diagnostics and maintenance. When One to Many is selected Nodes (remote sites) are not allowed to communicate to each other, but any client can connect to any node. All nodes and clients can be connected 24/7/365.



Many to Many

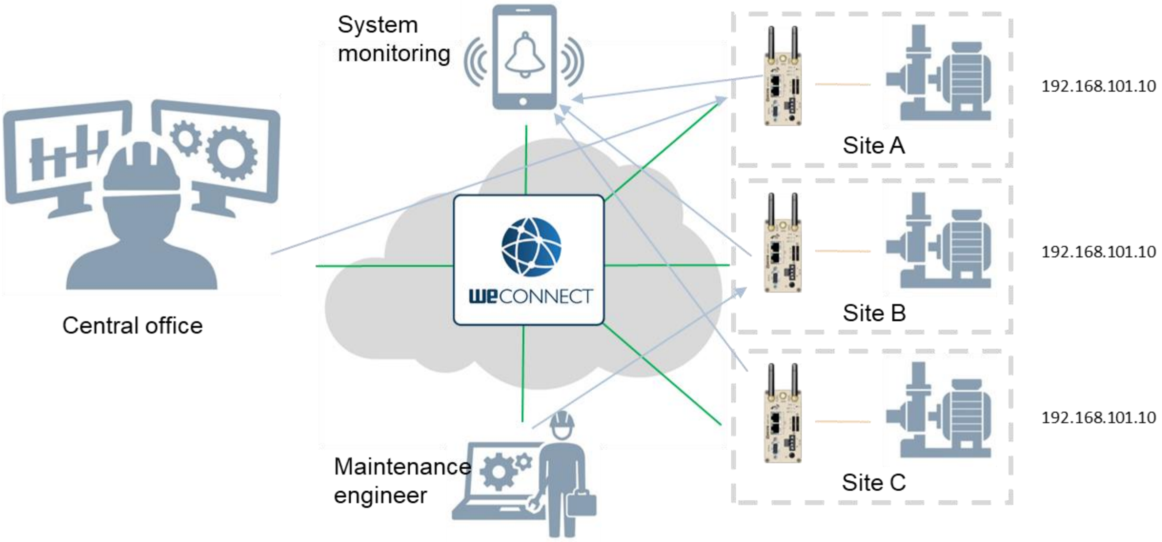
In a Many to Many Secure server, Nodes can connect to each other as well as any client can access any Node. Typical application would be legacy leased line or dialup modem replacement over IP or multiple nodes exchanging data over IP such as controlling water extraction from bore holes or rivers to a holding reservoir. All nodes and clients can be connected 24/7/365.



Identical Networks

In an Identical network application, the remote nodes can all have the same subnet at the remote location. This would normally need some advance routing techniques to work around the issue of the same subnet and possible the same IP addresses being reused on every remote location. A WeConnect user can select which site they would like to access to from the management portal. The system is flexible and can even allow multiple engineers to access the same remote location simultaneously.

Each remote location can have more than one subnet allowing for multiple networks to be accessed. A filter can be applied to each client limiting the nodes and the subnets they can access. For example, a maintenance engineer from a third-party company can only access a single subnet, whereas another engineer can access all the subnets at all locations. If the application requires, each remote system is still able to send data to a Client for example a Historian or SCADA system for event recording.



Conclusion

WeConnect offers end user and organisation a secure and flexible solution for remote access. The COVID-19 pandemic focused attention on remote access in a way that could not have been anticipated pre 2020. There were always arguments and justification based on cost but and reduced carbon footprint. But during the pandemic the argument for remote access changed as getting engineers to site was problematic to say the least and, in some cases, almost impossible. Being able to access device and resources securely and flexibly has been key to successful business operations during whilst movement has been restricted on a national and international level. WeConnect is hosted in the cloud, but this is an advantage due to the resilience afforded by the 24/7 support in the server centres. The levels of physical and electronic security around a server centre make WeConnect a cost effective and secure solution when compared to a home-grown alternatives. The solution is based on industry standard protocols and principles of operation. There are no proprietary protocols or Westermo specific software requirements to use or operate WeConnect. A user is completely free to use any media available just as long as there is access to the internet. There are no requirements for Port forwarding from the internet or the use of static IP SIM cards. Operating WeConnect can be moved to an admin task freeing IT specialists up from the day to day operation.

Author;

Ray Lock

Remote Access solutions Architect

Senior Director

For more information visit;

https://www.westermo.com/solutions/weconnect