

White Paper

A Web Broker Architecture for Remote Access

A simple and cost-effective way to remotely maintain and service industrial machinery worldwide

Francis Vander Ghinst – Head of Sales & Marketing Ops. - fvt@ewon.biz

eWON sa
Avenue Robert Schuman, 22
1400 Nivelles
Belgium
tel. +32 (0)67 895 800

The industrial remote access world

Providing industrial remote access systems for machine builders and OEMs has become a critical requirement for enterprises, often making the difference between companies that are successful and those that are not. Regardless of whether maintenance engineers work in the office or at home, they need easy and seamless access to machines and industrial assets in order to do their job, which primarily involves remote maintenance.

In the early 1990s, there were only limited options for worldwide access to machines and industrial assets. A modem communicating via the public switched telephone network was the prevalent option. Unfortunately, this required making long-distance calls, and the available throughput was so low that it was difficult to service machines in practice. As the Internet grew, it provided an opportunity for free or public long distance communication for remote access. Now combined with cellular technologies that provide wireless communication or DSL based technologies, this offers the market new communication media for accessing devices. However, DSL based technologies require installing a dedicated line to the machine location, while cellular technologies requires that wireless receivers are available in the vicinity of the machine providing adequate coverage for good communication.

An alternative approach is for machine builders to utilize the network infrastructure of their customers, assuming that the customer's machine can be connected to the Internet via a LAN connection point. This is the preferred way to access the machine, since it provides the lowest-cost connection, high throughput, and almost no deployment effort on the media side.

Using Internet implies the use of virtual private networks (VPNs) to ensure secure IP connections. Using a LAN connection point requires the integration of these VPNs into the corporate LANs of the machine builders' customers.

With a remote access turnkey system approach, the machine builder must assume responsibility for the integration activities and will probably need to collaborate with the customer's IT staff in order to perform the integration. Although this is a viable approach, it has some drawbacks. For instance, each customer may require a different VPN configuration, which increases the complexity of the integration process and extends the installation and commissioning period, which of course impacts the cost of the machine installation.

It is therefore important to choose technologies which allow the installation cost to be kept to a reasonable level by minimizing the integration factor as much as possible.

VPNs: a challenge for machine builders and OEMs

VPN technologies offer machine builders and OEMs an alternative way to supply high performance connectivity for communication between service or maintenance engineers and the machines they have to service, located on the sites or in the factories of their customers. They can also start thinking about new applications, such as diagnosing machine faults (for example by using a webcam), benchmarking machines by obtaining key performance indicators for the machines, establishing maintenance plans by monitoring machine life cycles, and so on.

The technical challenge is different here. With dial-up modems, the essential requirement was to have a phone line connected to the PSTN and pair of modems (one at each end), while VPN technology demands IP expertise and familiarity with the Internet.

VPN technology provides a combination of encryption and tunneling functions. Data is encapsulated in an IP “wrapper” that travel over the Internet. When data is sent, it must be wrapped and encrypted by a gateway, which is a hardware device or a software program, using a sophisticated encryption mechanism. At the other end of the communication link, the destination gateway must “unwrapped” the data, decrypt it, and route it to the recipient. In this way, the traffic originating from the VPN gateway is handled the same as data originating from another user in the LAN.

Network layer VPN versus application layer VPN

Network layer VPNs generally provide their users permanent external access to their company networks via the Internet, as though they were internally connected to the corporate LAN. This is the best solution for geographically distributed users who need to share the same resources in a seamless way, without losing any productivity compared to internal users connected directly to the LAN.

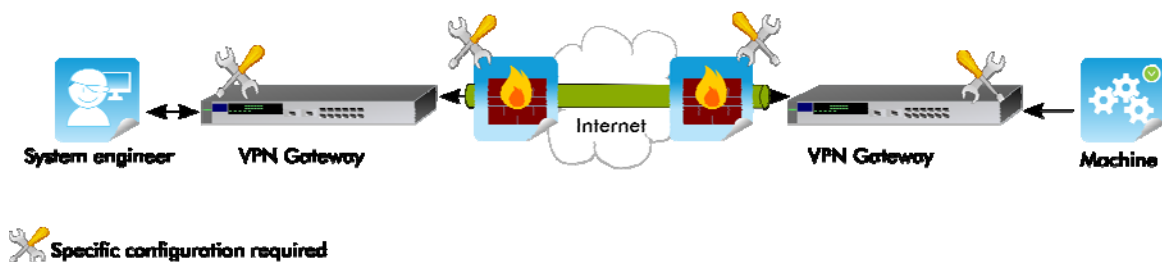
However, this level of access can create security gaps if the connection point that the user is using is in reality unsecure or can easily be compromised. While it is possible to secure a PC that is actually within a LAN, such precautions are difficult and expensive to implement with remote PCs in unmanaged networks.

In the world of machine builders and OEMs, this means that on the machine side the connection point should be put under the control of machine builder’s organization. This is never possible because the connection point is located inside another IT network organization: the customer’s LAN. This implies that the connection point is managed by the customer’s IT department and complies with customer security policies, which could differ from those of the machine builder. Access could also be restricted to the machine IP devices and applications, but this requires additional configuration settings and effort. Another way to avoid security problems is to have the connection point to the Internet be dedicated and separate from the LAN. This could be achieved by using an additional physical medium, such as a PSTN line, an ADSL line, or a cellular link.

Another consideration with network level VPNs is the level of skilled resources needed for deployment and maintenance, which is high. For organizations such as machine builders or OEMs trying to provide remote access to hundreds or thousands of machines, it can be costly and time-consuming to deploy, update and manage all of these machines, especially if they cannot be on site physically to configure the equipment. If the customers with their own security policies and configuration settings are also taken into account, the difficulties are multiplied. There is thus a risk that the machine builders will quickly be faced with an unrealistic level of investment in order to meet the needs of these numerous remote access connection configurations and settings.

Traditionally, network layer VPNs rely on the IPSec protocol. Some vendors also use a combination of a Layer 2 tunneling protocol (L2TP) and a point-to-point tunneling protocol (PTPP).

Fig. 1 : Network VPN



Application layer VPNs such as SSL VPNs – the secure transport mechanism – use a different method to transport private data across the public Internet. They use the same path as a web connection, thereby minimizing the necessary configuration settings on all passthrough devices. This is the first advantage of SSL VPNs, since whenever a web browser application is available, there is already a path (from the user's perspective) to the external world (the web), and the SSL VPNs can use the same path.

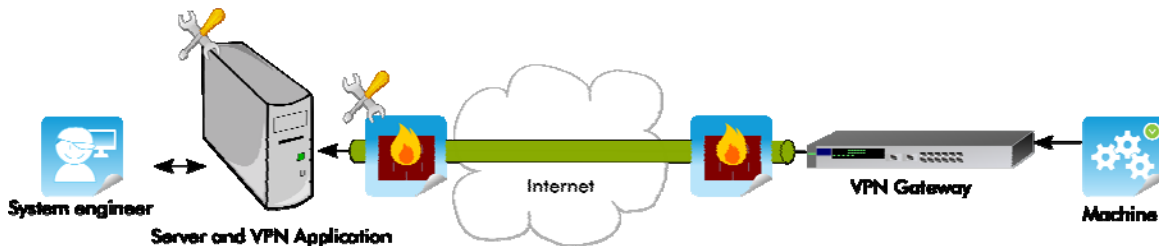
Translated to the world of machine builders and OEMs, this means that the connection between the maintenance engineer and the machine takes place using VPN encryption, utilizing the same path as the web connection to establish the VPN connection (alias tunnel). If users or machines are able to act as web clients inside their networks (in other words, if they can browse the web), they can also establish SSL VPN connections. Because SSL VPNs operate at the application layer, it is possible to provide controlled access to applications instead of controlled access to the entire corporate LAN, which inherently limits the security gaps in the network. It is thus ideal for accessing machines within other network infrastructures or machines that initiate a connection from an insecure endpoint, and it minimizes integration effort because the VPN tunnels follow the same paths as existing web connections that already pass through the firewall.

It also makes the technology more familiar to the users, even those without strong technical backgrounds. Configuration is less labor intensive and can be done by IT employees with lower skill levels. When deploying hundreds or thousands of machines, having a VPN system that is easier to configure and integrate in other network infrastructures reduces the investment burden, reduces risks, and keeps the integration cost reasonable.

Why use a web hosted architecture?

The next question is how to establish VPN communication between the system engineer (the user) and the machine. At the user location, we could install a component to serve as the endpoint of the VPN tunnel initiated by the machine. This could be a hardware component or a software component. In our case, the idea is to install a software application called a SSL VPN server that collects all incoming VPN connections originating from various machines – a typical server concept. However, this requires installing the VPN server on a PC and configuring it. This is not straightforward, since it requires IT knowledge and skills, but hopefully once the setup has been configured for a machine builder, only maintenance activities have to be taken into account afterward. With a server application, users can also connect to the same servers as the machine, and the VPN server is responsible for the internal establishment of the ultimate link between the user and the machine (see Figure 2).

Fig. 2 : Application VPN



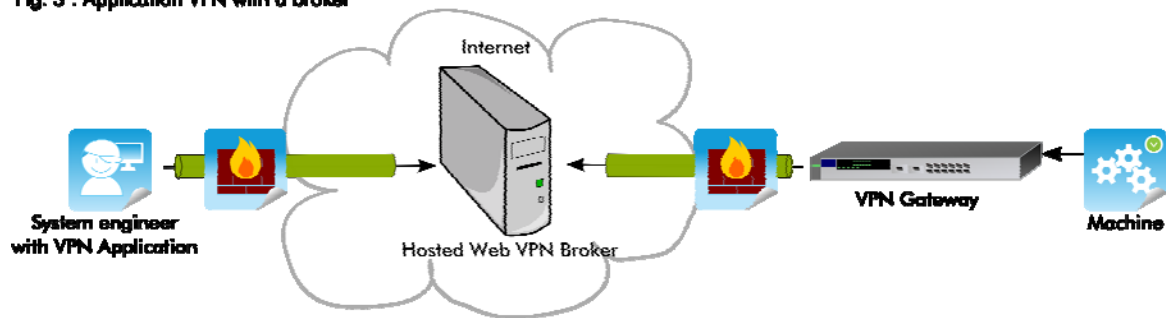
 **Specific configuration required**

The next step is to transform the internal VPN server architecture into an external web architecture. With this web architecture, the machines and users can still connect in a seamless way, while the machine builders no longer need to install, configure and maintain the VPN servers; this can be delegated to a specialized third party organization (see Figure 3).

In fact, if the VPN server is hosted by an independent organization, it can be shared among several machine builders, each having a private account, and they can individually configure their users and machines. This reduces the web infrastructure cost for individual machine builders and OEMs or spreads the cost over several machine builders.

A web based architecture inherently provides better scalability than a pure hardware architecture based on hardware gateways or internal software applications. In fact, the web architecture can provide a load balancing function that can distribute the number of necessary VPN connections or tunnels over several servers. It can also provide redundancy to ensure the business continuity of the remote access services.

Fig. 3 : Application VPN with a broker



Security

Both technologies – network layer VPN and application layer VPN – effectively secure network traffic, and both have associated strengths and weaknesses that make them appropriate for different needs.

With regard to the needs of machine builders, the two approaches offer the same level of security, although the protocol implementations differ greatly. They have many similarities, including strong encryption, authentication, and protocol session keys that are specified in a conceptually similar manner. The two protocols thus offer similar support for leading encryption, data integrity and authentication technologies, which means that they can provide the necessary security.

The web server architecture inherently adds an additional authentication mechanism to ensure that machine builder users cannot use the accounts of other machine builders. SSL can also be used to ensure the privacy of user accounts.

On-demand connections

What machine builders need is the ability to connect to their machines anytime and anywhere. Instead of going on site, machine builders need to have reliable connections that allow them to access their machines for support, service, and maintenance.

Unlike remote asset management where the ability to control the asset is essential, which means that permanent access to the asset is necessary, machine builders do not always need permanent connections. This of course depends on the application, but remote access for machine troubleshooting, maintenance or service could be provided by an on-demand connection. In fact, the customer may want to prevent continual remote access to the machine, which means that the machine is usually disconnected from the LAN and only connected for a certain period when this is necessary or requested by the machine builder.

Disconnecting the machine from LAN is not essential for security, but it gives the customer the feeling of having physical control over when the machine is accessed and for how long.

With a dedicated line using a medium other than LAN access, temporary connections may also be desirable due to the pricing model of the medium that is used. This is not necessary with flat-rate pricing, such as a DSL line, but with volume-dependent pricing (such as cellular media) it could be attractive to establish the connection only when necessary. In fact, established VPN connections send dummy messages called "keep-alive" messages periodically, even if they are not transporting any IP messages, in order to keep the connection open and inform the destination that there is activity. Although these messages are short, they may be exchanged several times a minute, and at end of the month they can amount to a significant volume, especially if hundreds of machines are involved.

The "interruptible" aspect of the connection thus needs to be taken into account in the design of the remote access system, so that the VPN connection can be restored after a sudden break or a connection can be established if the device is not already online (on the web). Watchdog mechanisms should also be implemented in the remote access system, either in software or in hardware, to reestablish the connection when the medium is restored or back on the air.

Conclusion

A web hosted broker system relays VPNs of web based communication originated by users on one side to VPNs of web based communication originated by machines on the other side. This system thus offers several benefits in case of deployment of hundreds or thousands of machines among several customers by:

- using web technologies to provide connections;
- reducing the integration time at the customer site;
- reducing the maintenance time for the server at the system engineer site;
- making worldwide deployment easier;
- making provisions for temporary connections.

It has also been shown that the design of the proposed system takes into account an approach that allows the cost structure to be kept minimal while enabling quite predictable budgetary cost estimation.