Virtual Private Network

Secure Remote Access to machines through VPN

SCOPE

With PLC's and Machine Controllers having Ethernet ports supporting the TCP/IP protocol it is very easy to access these devices remotely. The technology used for this is generally known as Virtual Private Networks (VPN). A VPN connection assures the secure transfer of data from one network or device to another network or device over shared or public networks like the Internet.

CONTENT

WHITEPAPER

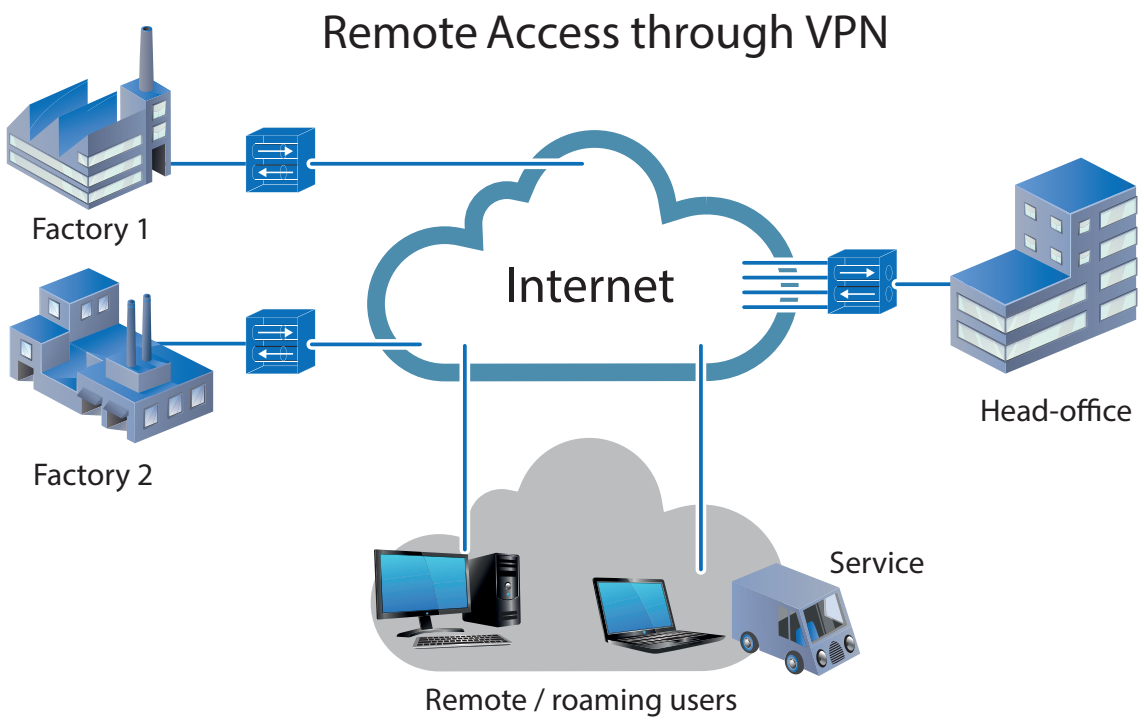
Executive Summary

Business Benefits

When using remote access through VPNs both the machine builder and the end user have big benefits. The machine builder can quickly diagnose problems on the machine, even before they happen. He can inform the end user to take on time preventive actions or help him to solve the issue by remote assistance. Also the end user will benefit from remote access, as the machine is easily accessible and can provide real time production information.

The way Virtual Private Networks function any IP-type of communication can be done. Even communicate to those devices that do not have an Ethernet connection like serial device by using IP to serial conversion. There is almost no limit on the type of communication. Possibilities are endless.

Having remote access to a machine is the same as standing next to it, but still being on a distance.



VPN establishes a connection between two sites. The connection is secured by username and password plus the data transferred is encrypted. This makes it unlikely that outsiders can interfere with the operation of the machine or access production data. A VPN connection is also called a VPN tunnel as what goes in one side comes out at the other side without any changes.
To establish a connection between different sites various standard products are available.
In this paper an overview is given of the products and technologies used, the principle of operation and an explanation of terminology.

High Level Solution

Modern machine control systems can provide a wealth of information about the process they are controlling. This can be production data as well as data indicating the electrical and mechanical health of the machine.

For instance the machine controller is registering and reporting the power consumption of a drive. At design time of the machine the load of a drive is calculated and during commissioning a threshold is defined. The controller of the machine monitors the current consumption of the drive against the threshold and triggers an alarm when the current exceeds this threshold. An additional threshold could be set for a pre-alarm, warning that inspection or maintenance must be planned for this drive.

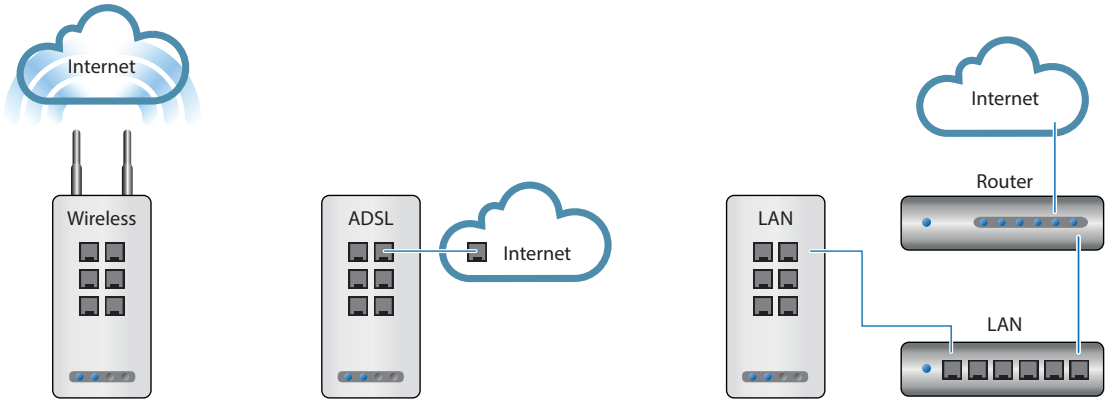
This information is of importance to the user of the machine in order to prevent unintended production stops. And in case the machine manufacturer has a maintenance contract with his end-user to maintain the machine and prevent production loss caused by standstill, a pre-alarm can prevent costly repairs.

Monitoring machine response times or vibrations can help to detect wear of mechanical parts. This can trigger the machine builder to pre-emptively send spare parts to the end-user site, so the worn parts can be replaced at the next scheduled maintenance stop.
In the end the end-user will benefit from a reduction in breakdowns and emergency repairs.

Ways of access

With the current communication technologies there are many possibilities to create a connection to the machine. To name a few:

- Wireless connection through a UMTS or GPRS connection.
- The machine plugs in into the local factory network.
- There is a direct connection to the Internet by means of an ADSL, cable, fiber or similar connections.

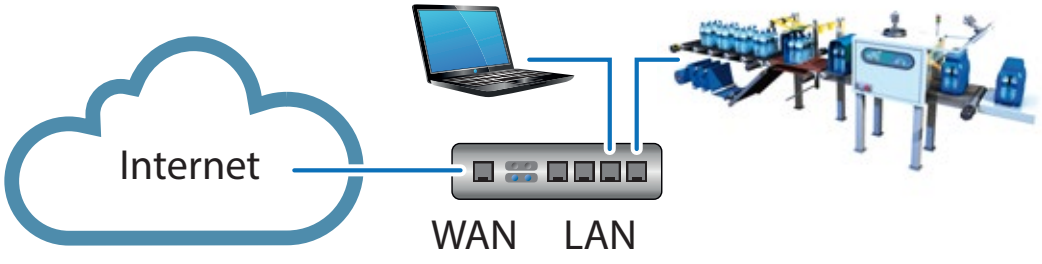


Wireless *ADSL / Cable* *Local network*

Whichever connection type is used data can be directly transferred between the machine and the machine builder's office, independent of the connection between the two. The products pictured are all router devices and connect their local network to a bigger network. This bigger network can be the Internet or a factory network.

Remote access through VPN

The general technology used for remote access is called Virtual Private Network (VPN).
This is a connection between two devices where they start a connection by first finding each other, then authenticate and negotiate an encryption. When the connection is active the two devices can transfer data in a safe way, protected against intruders.

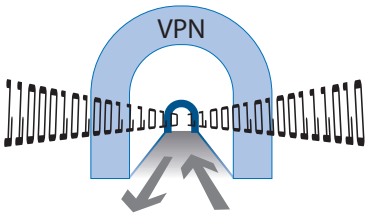


From a users point of view it is just like he is sitting next to the machine. However that machine can physically be on the other side of the world.

Imagine such a device having a WAN (Wide Area Network) port to connect to a bigger network or the Internet and a couple of LAN (Local Area Network) ports to create a local network. Through the routing capabilities of the devices the two distant LAN networks are connected to each other and act as one. A device connected to the LAN side of the router can reach other devices on the other sides LAN. This is very convenient as a machine controller on one side can directly be accessed from the other side. Instead an endpoint (router) being a box with WAN and LAN ports it could also be a PC that connects to the other network.

Security

Sending data over the Internet or other networks implies a security risk. Of course it is a must to prevent that somebody can intercept the data send across the network and start tampering with the system.
VPN creates a secure tunnel. Secure in the sense that there is authentication when the connection is opened and that the data transferred is encrypted.
The authentication can be based on username/password, pre-shared keys or certificates. Or a combination of the three is used. Often a username plus a certificate is used.



Encryption can be from a simple to a very high level. Keep in mind that encrypting and decrypting data takes time. The higher the encryption is the more time it takes to prepare the data and thus the slower the transfer. An option when a high level of encryption is used could be using a device that has enough processing power to do the encryption/decryption quickly. Faster devices have often a higher price. There is no golden rule to decide which encryption level to use. It depends on the level of security and communication speed needed.

Type of data transferred

In principal any type of IP-data can be send across the VPN connection. But some practical examples are:

- Alarms and warnings from machine to OEM.
- Bidirectional communication between remote-SCADA or HMI and the machine.
- Recipe or production information to and from a remote database server (for example Oracle or Microsoft).
- New control programs uploaded to the machine to deploy modifications or upgrades.
- Status monitoring to assist in faultfinding when there is malfunction in the machine. Could be as simple as checking if a sensor signal is active and learn that the sensor needs to be re-aligned.

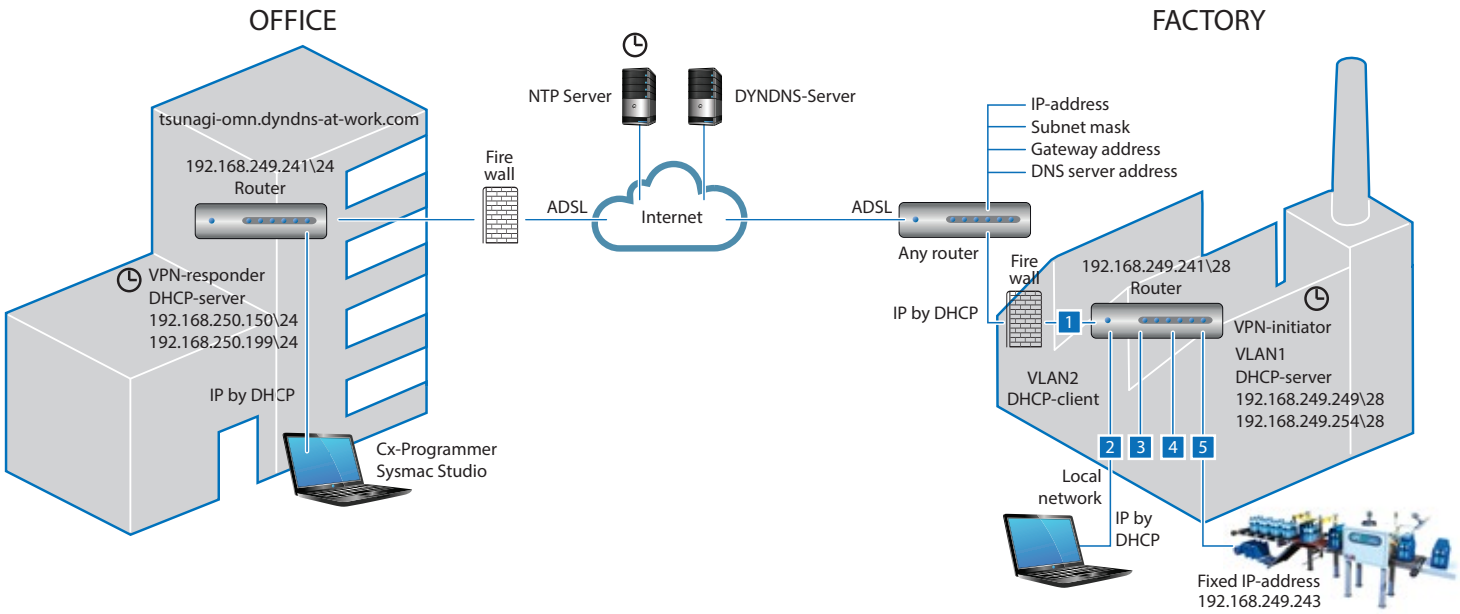
Client/server, initiator/responder

There is a distinct role for each device in the setup of this VPN connection. One of the devices acts as the initiator or client of the connection and the other is the responder or server. The server is waiting for a client to connect. And being a server it is not only servicing one but multiple clients.
The routers in machines have the role of client and they connect to the server at the office of the machine builder. The machine builder has all his machines online.

Machines can then report their status directly and continuously and the machine builder has the opportunity to react immediately on events. Like when there are problems but also to plan scheduled maintenance or send consumables on information the machine provides.

Solution Details

In a network setup there are often products from different manufacturers used. But these devices must understand each other. Thus standardization of protocols is need.
Also in VPN technology there is a lot of standardization. There is not one VPN standard but there are several. The two mainstream ones are IPsec and OpenVPN (also known as SSL).
These two standards made their way to commonly available products and services. With Common Of The Shelve (COTS) products anybody can set up his own VPN infrastructure.



VPN use case walkthrough

The drawing above is an example of a machine controller connecting to the office network of a machine builder. The drawing shows the components that are used to set up a VPN tunnel between two sites.
At the left side is the machine builder's office (VPN server). On the right is the network in a machine that is installed in a factory at a distant location (VPN client). The machines network is connected via the VPN tunnel to the machine builders' office network so there is instant access to the machine.

The machine is hooked up to a bigger factory network that has an Internet connection available. The router in the machine is configured to create a local network LAN in the machine itself and connect one of its ports (WAN) over the Internet out to the office network.

These local services are:

- VLAN, (Virtual Local Area Network) this is used to divide the routers Ethernet ports in two separate networks. Traffic cannot move from one network to the other and vice versa. One VLAN (the local network) has its own IP-address range and is one end-point of the VPN connection. The other VLAN (WAN) is part of the factory network and gets its IP-address and other settings from a DHCP server on the network. For the factory network this machine is represented as a single device with only one IP-address.
- Routing, forwards messages from one VLAN to the other depending on the destination address. It also stops broadcasts and multicast message on the factory network entering the local machine network.
- Firewall, when there is an attack from the factory network this is stopped by the firewall. It is also possible to open up the firewall for certain types of messages. But this is totally application specific.
- DHCP server is there to assign IP-addresses to devices on the local network. Normally controlling devices have fixed IP-addresses. But it could be that a service engineer connects his laptop to this local network and then it is convenient that he gets the correct IP-address assigned.

As the machine is part of the factory bigger network it cannot be accessed from outside the factory. The factory router that connects to the Internet has a firewall and will block off all incoming traffic. Therefore the router in the machine needs to be the initiator of the VPN connection. To let the VPN connection be established successfully the VPN initiator (the router in the machine) must have some following set up.

- Time synchronization. In the negotiation and encryption process also the date and time is used. Both the initiator and responder must have the same time and date. The exact date and time can be derived from so-called timeservers (NTP-servers). A timeserver can be on the Internet or on the factory network. With a timeserver the date and time is automatically set and adjusted regularly.
- Domain Name Server. For the VPN initiator to get to the VPN responder it needs to know its address on the Internet. However fixed IP-addresses on the Internet are scarce and quite costly. It is easier to have a domain name. Then a DNS server resolves the domain to an IP-address. The router knows only the name (office.machinebuilder.com) but by requesting a DNS server, which IP-address is linked to this name, the responder can be reached. And it doesn't matter how often the IP-address of the responder changes. It is always reachable through its name.

On the responder site the following must be set:

- As with the VPN initiator also in the responder the time must be set correctly. It can use the same timeserver as the VPN initiator is using.
- As the VPN initiator is searching for the VPN responder per name the router must announce his name and IP-address regularly at a DNS-server on the Internet. This DNS service is called Dynamic DNS. There are a couple of companies that offer this service like DYNDNS.

- VPN connection settings of the initiator must be registered at the responder.

If there is a connection request coming in it credentials will be checked and if correct the connection is accepted and the tunnel is up. The machines network is now connected to the office network and data can be exchanged between them directly.

For the direct wireless or wired connections the way of connection is a little simpler but still largely the same.

Connection technology

When creating a VPN tunnel a connection must be established from the client to the server. In many cases this connection is over the Internet. There are several ways to connect to the Internet depending on what is available at that location.
In general there are three variants. This can be wired or wireless, directly connected or via a bigger local network.

Wireless

There are locations where only wireless access is possible. For instance on a remote site where there is no ADSL or cable connection. However there is a mobile network with data communication available. To get access to this mobile network a subscription at a service provider and a SIM-card are needed.

There are different types of wireless data communication but the most commonly known are GPRS and UMTS. GPRS is older and less performing technology then UMTS. UMTS has communication speeds well into the Megabit per second range. GPRS throughput is limited to a couple of hundred kilobits per second.
To ensure that data communication is always possible GPRS functions as a fallback when it is not possible to establish a UMTS link. For both UMTS and GPRS the cost of the connection is based on the amount of data transferred, not on connection time. Therefore the connection can be up and running all the time.

Wired, directly connected to the Internet.

The machine's router is connected directly to the Internet. This connection is an ADSL, cable or fiber connection. A local service provider installs the connection and the Internet is directly accessible from the machine

Wired, connected to a bigger local network.

The router in the machine is connected to a larger local (Factory) network. From within this larger network a connection can be made to the Internet. The router in the machine must know how to route out of this larger onto the Internet. But normally these routing settings are available from a DHCP server on the larger network.

All the above-mentioned connection types feature that they are up and running all the time so there is instance access from one side to the other.

Routing

An essential part in VPNs is the routing. For a device on one network to reach a device on the other side there shouldn't be to many hurdles in setting up the connection at the device. For the device it is only important to know to which router address his message should be sent when it is not on the local network. It is then up to

the router to handle the rest of the communication.
When a message arrives at the router it needs to forward it to a known address. If this is router is in a bigger network it will send to another router. The message is forwarded till goes out on the Internet. Or the addressed device on the bigger network is reached. In case of a direct connection to the Internet (wired or wireless), the Internet will take care of getting the message to the addressee.
When the Router is VPN capable and the tunnel is up then the message is forwarded over this tunnel and ends up at the other side.

VPN technology

There are many implementations of VPN. But currently two are in use as be proven reliable and save. These are IPsec and OpenVPN (or SSL). Both make use of the same kind of technologies in compression and encryption. There is one difference that IPsec uses a kind of username/password for authentication while OpenVPN uses certificates that need to be generated at the server. Also OpenVPN uses the same way of communication https:// secure websites use. This makes it easier to let OpenVPN traffic pass Firewalls in routers as the Firewalls judge this traffic to be regular web-traffic.

Summary

A Virtual Private Network is a secured connection between two devices/routers/networks. The connection can be established over local and public networks. Security is by authentication and encryption.

There are clients and servers or initiator or responders. The clients initiate the connection to the server and the server can accept connections from multiple clients. The VPN connection between the client and the server is a transparent link between the two. Any type of data can be sent over. And it doesn't matter on which side of the VPN connection you are. And how far apart the two networks are.

Addressing

IP-address	An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.
Subnet Mask	A Subnet mask is a logically visible subdivision of an IP address in a network address and a node address. The practice of dividing a network into two or more networks is called subnetting. If an addressed IP-address is not inside the local network the message will be send to the router or gateway.
DHCP	The Dynamic Host Configuration Protocol is a network protocol used to configure devices that are connected to a network so they can communicate on that network using the Internet Protocol (IP). The protocol is implemented in a client-server model, in which DHCP clients request configuration data, such as an IP address, a default route, and one or more DNS server addresses from a DHCP server.
Local and remote network address	The Local network address is determined by combining the IP-address with the Subnet mask. A logical AND is performed. With the IP-address 192.168.250.12 and a subnet mask 255.255.255.0 The local network address is 192.168.250.0 and has a range from 1 to 254. If a IP-address is not within this range then it is a remote address. Through VPN it also could be a remote network address.
Gateway address	The Gateway address (or default gateway) is a router interface connected to the local network that sends packets out of the local network.
DNS Server Address	The Domain Name System (DNS) translates easily memorized domain names to the numerical IP addresses. A DNS Server does the translation from name to address. The DNS server itself has a fixed IP-address. Example the name www.omron.com translates to 202.232.86.142

Components

Router/Gateway	A Router is a device that forwards data packets between computer networks. These can be two networks but also a local network and the Internet. If the Router forwards to a larger network it is also called a Gateway.
Servers for DHCP, DNS and NTP	A Server is accessible locally or on the Internet and delivers a service. A DHCP server assigns IP-addresses. A DNS server translate names to IP-addresses A NTP server delivers a time to a device.
VPN-initiator and responder	In VPN a connection is always initiated from one side. Therefore one side is waiting to respond to a request from an initiator. Comparable is a Client/Server principle of operation.
UMTS, ADSL, Cable and Fibre	Different technologies to connect to the Internet. This can be wireless, wired or optical.
LAN and WAN	Local Area Network versus Wide Area Network. A LAN is a network where all devices are at the same location like an office or a factory. The WAN is the bigger network where the LAN is connected to via a router.

Services

VLAN	The Virtual Local Area Network is a technology where certain ports on a managed switch are combined to a kind of "physical network". Traffic on other ports of the same or other switches will not appear on the ports assigned to the VLAN. A VLAN can span over multiple switches in a LAN. The reason to do this is traffic separation.
Routing	Routing is the process of selecting paths in a network along which to send network traffic
Firewall	A Firewall is a software or hardware-based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on a rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted.
VPN protocol	VPN (Virtual Private Network) is a general term. However there are many different implementations/protocols. One is more secure then others. Currently most used implementations are IPsec and OpenVPN.

Omron Corporation

- 50 years in industrial automation
- Over 35.000 employees
- Support in every European country
- Over 1.800 employees in 19 European countries
- 800 Specialised field engineers
- 7% of turnover invested in R&D
- More than 200.000 products
- More than 6.950 patents registered to date

Omron Industrial Automation

Headquartered in Kyoto, Japan, OMRON Corporation is a global leader in the field of automation. Established in 1933 and headed by President Hisao Sakuta, Omron has more than 35,000 employees in over 35 countries working to provide products and services to customers in a variety of fields including industrial automation, electronic components industries, and healthcare. The company is divided into five regions and head offices are in Japan (Kyoto), Asia Pacific (Singapore), China (Hong Kong), Europe (Amsterdam) and US (Chicago). The European organisation has its own development and manufacturing facilities, and provides local customer support in all European countries. For more information, visit Omron's Web site at www.omron.com.

AUTHOR

René Heijma
Product Specialist Industrial Communication

- Omron Europe B.V.
  Product Marketing
  Automation department
- Zilverenberg 2,
  5234GM, 's-Hertogenbosch,
  The Netherlands
- Tel. +31 (0)73 6481 950
- rene.heijma@eu.omron.com
- industrial.omron.eu

Starting his career as a PLC and SCADA engineer René Heijma worked on many different projects in the process and machine automation. From the early specification of the project, the programming of the PLCs and SCADA systems, till the commissioning of the electrical installation.

He joined Omron in 2001 as a Field Network Specialist. In those years DeviceNet and PROFIBUS where the prominent field networks which needed support. But since then Ethernet based control networks appeared, René specialized in these network technologies also and specifies new products and supports them thereafter in the Omron organisation.

VPN-technology is not really belonging to the control network domain but is a very nice extension. René investigated how to apply this VPN-technology in Omron applications and this whitepaper is an abstract of this investigation.

Visit us @ www.myOMRON.com, the engineering portal.