The introduction of Ethernet to the plant floor brings with it lots of benefits, notably a more open architecture that allows connectivity to plant devices and management tools from pretty much anywhere. But with that openness also comes an issue that plant network operators must address: security.

When automation systems are attached to Ethernet networks, it’s not all that different from connecting a computer to the Internet. Somewhere in the plant and certainly in the enterprise network an Internet connection exists. Given that, organizations must take steps to protect the plant environment from the same sort of threats that any Internet-connected computer is facing, including hackers, worms, trojans and various other forms of malware.

In short, the plant environment needs the same sort of security tools that their IT counterparts use, albeit tools built with the plant environment in mind. The tools must allow authenticated access to the plant environment from other areas within the facility as well as from remote locations. That enables remote administrators to handle tasks such as configuration and diagnostics, initialization of nodes, and gain access to on-board Web and FTP servers to glean information from devices.

Siemens customers can get all these security tools as part of the SCALANCE S family of security modules, which offer firewalls, virtual private networks over both bridged and routed networks, and network address translation technology (NAT). What’s more, the Siemens Softnet Security Client enables a remote engineer located anywhere to connect to any VPN-connected site via a single VPN connection to the headquarters site.

It all adds up to an automation environment that is at once open, with the ability to communicate with other networks as needed and be managed from anywhere, while remaining safe and secure from Internet-borne threats.
Firewalls – the first line of defense

Firewalls are one of the oldest security tools and still a crucial piece of the security puzzle. A firewall sits between the internal and external networks. Its main purpose is to help ensure only legitimate trafficpasses from the external side to the internal side.

In an industrial environment, firewalls protect a cell that may include several Ethernet-attached automation devices, such as Industrial PCs and PLCs. In such a case, companies can install a Siemens SCALANCE S602, a simple device with one Ethernet connection coming from the automation network side and another going out to the larger network. Any traffic passing between the two is subject to whatever firewall rules are established for the device.

The S602 uses stateful packet inspection technology, which enables it to essentially assess traffic in context. It will only allow incoming traffic that it knows is a legitimate response to a request from the internal network. If an external source sends data that was not requested, it is blocked.

To ensure all traffic is legitimate, stateful packet inspection firewalls control the traffic based upon pre-determined filter rules. For example, if an internal node sends data to an external target device, the firewall will dynamically allow the response packet for a limited period of time. After the time window has expired, the firewall will block the traffic again.

NAT and NAPT

Another technology that helps provide security for automation environments is network address translation (NAT), which is implemented in devices including the SCALANCE S602 and SCALANCE S612/S623 modules. NAT essentially hides the actual IP addresses of devices on the internal network from view to those on the public, external-facing side of the network. It presents a public IP address to external-facing nodes but translates that address to a different IP address that’s used on the internal side of the network.

Network address and port translation (NAPT) takes the NAT concept a step further by adding a port number into the mix. With NAPT, only a single IP address need be presented to the public. Behind that, packets are addressed to particular devices by adding port numbers. A NAPT table, which typically resides on a router, maps private IP address ports to the ports of the public IP address.

If a device from the external network wants to send a packet to an internal device, it uses the security device's public address with the specified port as the destination address. This IP address is translated to a private IP address with port address by the router. The source address in the IP header of the data packet remains unchanged. But, since the sending address is in a different subnet from the receiving address, the response must go through the router, which forwards it to the external device, all the while protecting the actual IP address of the internal device from public view.

Building secure tunnels with VPNs

Yet another way to provide a secure connection over an inherently insecure network such as the Internet is to use a virtual private network (VPN). A VPN is essentially an encrypted tunnel formed by security devices at each end of the connection, which must generate digital certificates – digital IDs, essentially – to identify one another. The certificates also enable the devices to encrypt the data at one end, send it over the Internet (or other network) in encrypted form, then decrypt it at the other end before passing it to the end device.

Devices such as the Siemens SCALANCE S612/S623 work using digital certificates and can create VPNs in two basic configurations: bridging and routing mode.

Bridging mode can be used to enable devices to communicate securely in a virtually "flat" network while they are located further apart or when their communication has to pass an insecure section of the network. In addition, this is used for communication types that can't be routed and/or have to be in the same subnet.
The SCALANCE S612 and S623 also support a routing mode, which is used to create a VPN between devices on separate subnets. The router, operating at Layer 3 of the OSI model, has the intelligence and awareness of surrounding networks required to route packets to the appropriate destination address. Again, the packet travels over a secure, encrypted VPN tunnel, making the communications secure even over a public network such as the Internet.

Sample use cases
The various security tools available in the plant environment can be configured in different ways depending on exactly what kind of access you need to provide, and to whom. Following are a few examples.

User-specific firewall
Say you've got a contractor doing some work on some of the automation devices in one of your plants. When he's away from the plant, it's useful if he can log in, such as to troubleshoot issues. In such a case, you can create a user-specific rule in the firewall enabling the remote user to gain access. You can also create different levels of authorization, to ensure different remote users gain access only to the devices for which they are authorized.

It's a simple matter of creating a username and password for the remote user. He can then connect to the IP address of the SCALANCE S602 or SCALANCE S612/S623 module and log in using those credentials. By default, he'll have access for 30 minutes, after which he'll be logged out — to protect against him walking away from his computer and leaving the connection open for an extended period of time. If the contractor needs more than 30 minutes, he can renew the connection before it runs out using a Web-based form.

Site-to-site VPN
In an instance where a company has a central site and maybe two satellite facilities, a site-to-site VPN is likely more appropriate. A site-to-site VPN is essentially a secure encrypted connection between two sites that, depending on how it's configured, could allow users at each site to access any resource at the other — assuming they have appropriate authorization, of course.

This setup requires a SCALANCE S612/S623 module at each location to create the encrypted VPN tunnel. A firewall can also be used to provide more fine-grained access control, such as to enable certain users to access some resources but not others.

Point-to-point VPN
A point-to-point VPN enables a user to access devices at any site from any other site that has an Internet connection. This is useful for, say, an administrator working from home after hours who needs to log in to a remote location to troubleshoot a device.

This setup requires a SCALANCE S612/S623 module at the target location along with Softnet Security Client software, which runs on the administrator’s laptop or desktop. The Softnet Security Client enables him to establish an encrypted VPN connection with any site that has the SCALANCE S612/S623 module. From there, with the proper permissions, he can log in to whatever device he needs to.

Multipoint VPN connections
Now say that same administrator has to access another five or 10 sites from his home. Rather than establish individual VPN connections to each of them, he can connect to a central SCALANCE S612/S623 that already has VPN connections established to each of the remote sites and essentially piggyback on those connections.

That's a great benefit for service engineers, for example, who spend much of their time traveling. With a single connection to the central site, they can now easily but securely access any other site as needed — saving valuable time in the process.

Siemens Makes Security Simple
These are just a few of the tools Siemens has to ensure Ethernet-enabled automation environments are just as secure as their field-bus based predecessors — and their IT counterparts. Siemens also has additional tools to secure computers themselves as well as wireless connections (see next page).

While firewalls and VPNs are an important piece of the puzzle, and crucial for providing secure access to remote users, it takes additional layers of security to ensure a true, defense in depth security model. Siemens has tools, built with automated plant networks in mind, to address each of these layers: the plant and network layers as well as password protection to ensure system integrity. In short, Siemens knows what it takes to not only build a fast, reliable plant network based on open Ethernet standards, but to make sure it is secure as well.

To learn more, visit: www.siemens.com/industrialsecurity
Siemens offers a complete lineup of security offerings

The SCALANCE S modules and Softnet Security Client are just a few of the products Siemens offers to keep an industrial environment secure. Others include:

• The CP 1628 communications processor, a module for industrial PCs that provides them with a stateful inspection firewall and VPN capabilities for secure communication without special operating system settings. In this manner, computers equipped with the module can be connected to protected cells in a plant network.

• M875 router for connecting networks via mobile 3G wireless connections including UMTS and HSPA. The M875 likewise provides firewall and VPN functions, enabling secure communications via cellular phone networks, for instances when a Wi-Fi or wired Internet connection is not available.

• CP343-1 Advanced and CP 443-1 Advanced are communications processors that can be plugged directly on the backplane of the PLC and securely connect Siemens SIMATIC S7-300 and S7-400 controllers, respectively, to Industrial Ethernet networks. Each offers firewall and VPN functions, plus network protection via an IP access control list that protects the controllers against access from unauthorized computers.