Increased cyber security through distributed firewall strategy

Industrial networks or production environments can no-longer rely on the old concept of “Security by Obscurity”. Those who are now looking to disrupt companies or a nation’s day to day operation have discovered that the industrial telemetry and automation networks are soft targets. Government organisations have long been warning about the dangers of Cyber-attacks and have been issuing guidance on counter measures. The UK government (NCIP), US Department of Homeland Security (NERCIP) and other international governmental bodies are all advocating the use of cyber security counter measures. The US government takes this so seriously that it is backed by federal law. The industrial environment has been slow to adopt cyber security and has seen it as an expensive option. A very good reference document “Control Systems Cyber Security: Defence in Depth Strategies” www.inl.gov/technicalpublications/Documents/3375141.pdf written in 2006 describes in some detail how an in-depth Cyber security model should be approached. Some of the points are a little dated now but the message is very clear, without any protection networks are vulnerable to attack.

The vulnerability of today’s systems is partly our own fault. The relentless drive to save costs, get away from bespoke industrial busses and vender lock-in, has meant that the natural choice is IP (Internet Protocol). This is the very same communications system that the world now relies on, from ordering a pizza on line to the control of a nuclear reactor. This is not a wrong or poor choice but it does mean that industrial networks now need the same cyber security counter measures, as we would automatically use on our corporate networks. However the counter measures that we now have to consider for industrial networks should go further than normal corporate security. This is due to the distributed topology of the networks and the very often unmanned locations the networks are installed. This is particularly true for utilities with assets spread over a wide geographic area ranging from a single RTU to a complete unmanned water treatment or substation installation.

There is a misconception that first needs to be dealt with;

Good network security is aimed at stopping entry in to the network from unauthorised sources- it is NOT a virus protection system. There is no substitute for up to date anti-virus software on the client and host machines. Most viruses and malware infect systems after legitimate entry has been gained. The intrusion is invited by simply clicking the OK button to download something off the internet without considering the consequences or by using portable media such as a USB memory device.

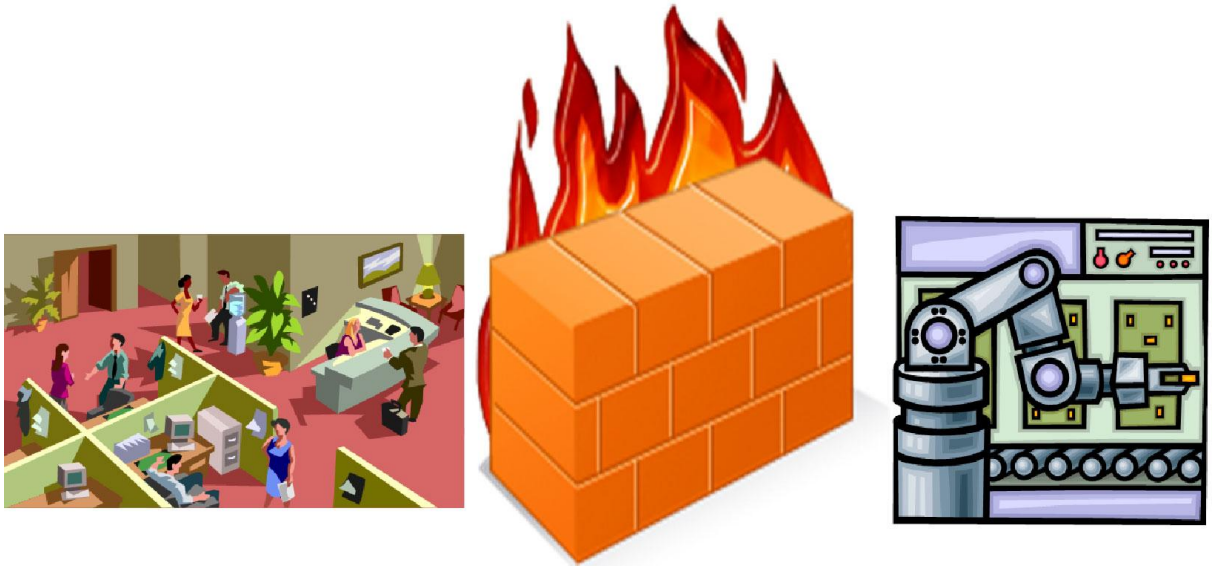
A well configured distributed firewall system will offer some protection against the spread of a virus, as the vectors or protocols the virus hides within will not pass though the firewall unless the protocol is specifically allowed. The firewall will act like an isolation ward in a hospital it will stop the spread of the infection but will not cure the patient.

Westermo Teleindustri AB
SE-640 40 Stora Sundby, Sweden
Tel. +46 (0)16 42 80 00 I Fax. +46 (0)16 42 80 01
info@westermo.com I www.westermo.com

Corp ID No: 556361-2604
VAT: SE556361260401

Network security

The traditional view of how a firewall should be applied is to place the firewall between the industrial network and the SCADA system or interface to the administrative network. This is not a wrong approach. The industrial/automation network should always be protected from any problems on the administration network whether malicious or otherwise!



The application of one big high availability firewall between the networks is good practice, but is not the whole answer. This approach does leave the industrial network vulnerable to attack or accidental damage. A more comprehensive approach is to place a firewall at every junction of the network. This sounds like overkill but this is the way that enterprise or office networks are protected.

Consider the network you are probably connected to at the moment. This will comprise of a large internet facing firewall, firewalls at satellite or branch offices as well as server, laptop and desktop machines on the network all with their own firewall. On a large LAN it is not unusual to find firewalls between departments and floors of a building.

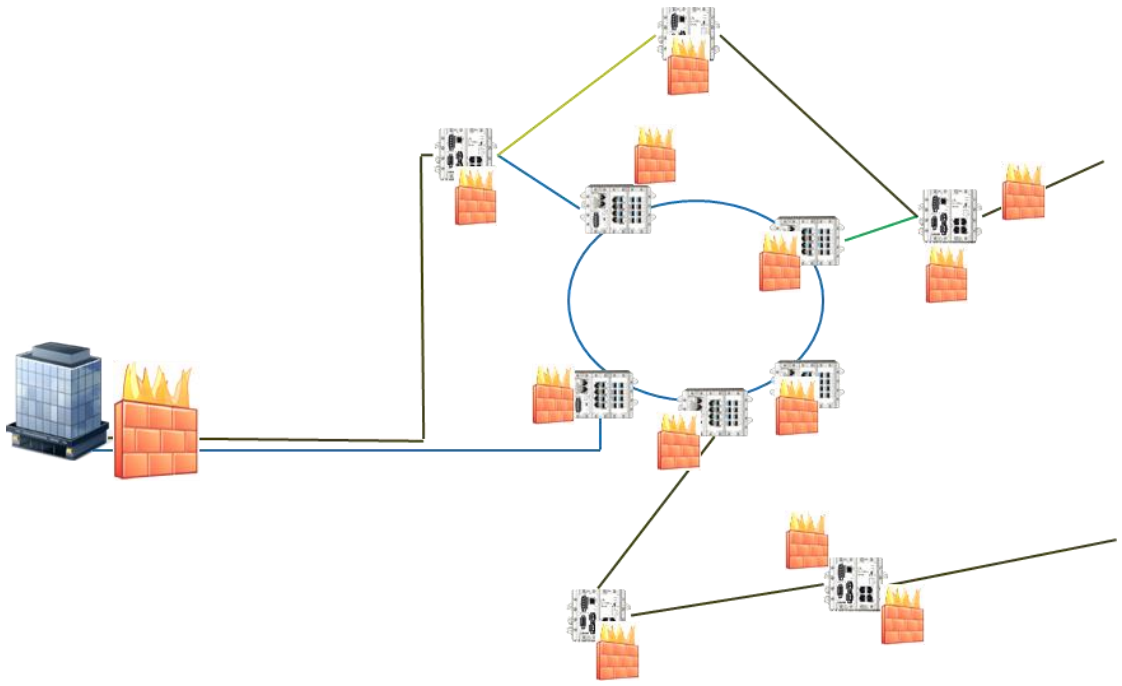
Until recently this has been an expensive option for industrial networks as most of the industrial firewalls have been discrete standalone devices and often fitted as an afterthought. If we were to implement a true in-depth security model using this technology the cost would soon get to the point of being prohibitive. Consider the number of network nodes on a large manufacturing complex such as a chemical plant or distributed down the side of a railway track.

The industrial switch/router market is now addressing this issue by including cyber security counter measures as part of the network switch operating system. The Westermo WeOS operating system has from the beginning included a suite of cyber security features that go far beyond just adding a firewall. It is beyond the scope of this particular white paper to cover all the cyber security features of WeOS.

Westermo Teleindustri AB
SE-640 40 Stora Sundby, Sweden
Tel. +46 (0)16 42 80 00 I Fax. +46 (0)16 42 80 01
info@westermo.com I www.westermo.com

Corp ID No: 556361-2604
VAT: SE556361260401

The application of a distributed firewall does mean that causal hacker or those with a more sinister objective will find it difficult to gain entry to any part of the industrial network and carry out their planned attack. A distributed firewall in effect puts barrier after barrier of tightly controlled access right out to the edge of the network. So even if physical access is gained to a switch on the industrial LAN access will be limited to just the IP addresses, protocol, and ports the firewall rules will allow to pass though the physical port to the rest of the network.



How does this make it difficult for the hacker to access the network?

To understand this we need to look at the way IP communications works at a fundamental level i.e IP address, protocol, and port. The IP address is the 4 octet address used in IPV4 to address the devices on the network i.e. 192.168.0.99. The protocol and port number are not normally visible but are part of the way IP communications select which interface the communications are destined for.

Westermo Teleindustri AB
SE-640 40 Stora Sundby, Sweden
Tel. +46 (0)16 42 80 00 I Fax. +46 (0)16 42 80 01
info@westermo.com I www.westermo.com

Corp ID No: 556361-2604
VAT: SE556361260401

The protocol refers to the message type being TCP or UDP. The port number is the virtual port the application will be listening on e.g.

Port	Protocol	Use
23	TCP	Telnet
22	TCP	SSH
69	UDP	TFTP
20 & 21	TCP	FTP
502	TCP or UDP	Modbus IP
80	TCP	Hypertext Transfer Protocol (HTTP) (web traffic)
443	TCP	HTTPS (Hypertext Transfer Protocol over SSL/TLS) (secure WEB traffic)

It is beyond the scope of this white paper to list all the official port assignments and protocols. A full list of the officially assigned port numbers and protocol can be found at protocols and port numbers. For unofficial protocol and port assignments refer to the equipment supplier's documentation. If no information is available on the protocol and port assignment then it is possible to use an Ethernet dissector such as Wireshark http://www.wireshark.org/ to look for the protocol and port assignment within the datagrams. For a more complete understanding of how Ethernet and IP works Westermo run a series of courses designed for automation professionals Westermo Ethernet Training.

The ability to control or filter the traffic using both IP addresses and ports is important when limiting the extent of any access to the network e.g. if the physical port being accessed will only allow MODBUS IP traffic on Port 502 it will not be possible to try and access the TELNET port of a device and change its configuration, for instance. Some protocols use two or more ports to communicate. WeOS allows for this by providing a list of protocols that are known to use multiple ports.

Ideally a distributed fire wall cyber security system should be designed in to the network from the start. When designing the security system consideration should be given to the commissioning phase. If the security level is raised too soon during commissioning the whole commissioning process can be halted and the plant or process misses its deadline for completion. Security appliances like the Westermo WeOS operating system allow for this by letting the users run with no security and allow the staged implementation switch by switch on the network until the desired security level has been reached.

By distributing firewalls around the whole system we also realise some other benefits. Typically a high availability central firewall has a huge bandwidth able to process packets at or near full wire speed. There would be no point putting in a firewall on a gigabit network that could only support a fraction of that speed when processing packets through the firewall. On an industrial network we can use switches and routers equipped with firewalls at many locations. Each switch such as the Westermo Lynx or Redfox will be able to process the packets locally and therefore do not need huge amounts of processing power at each of the locations. The aggregate processing power of all Lynx or Redfox L3

Westermo Teleindustri AB
SE-640 40 Stora Sundby, Sweden
Tel. +46 (0)16 42 80 00 I Fax. +46 (0)16 42 80 01
info@westermo.com I www.westermo.com
Corp ID No: 556361-2604
VAT: SE556361260401

switches is far in excess of the maximum bandwidth available on the interconnecting backbone network.

The distribution of the firewall brings a second benefit, that of resilience or redundancy within the network. By distributing the FW around the system any failure or breach of security remains local. The rest of the system will remain connected assuming there are backup pathways though the networks. It is beyond the scope of this white paper to cover the routing or backup resilience consideration, for more information on this visit http://westermo.com/.

Conclusion

The cyber security threats to industrial networks are present here and now and cannot be ignored. The trend will be to increase the level of cyber security from the boardroom through to the RTU in a middle of a field. The tools to address this issue are becoming more widely available and more importantly integrated into the industrial switches and routers that are used to create the industrial networks. Using a distributed strategy means that the security can be pushed out to the very edge of the network and there is less reliance on large centralised firewalls. Attacks can be stopped at the very edge of the network rather than having to deal with the problem once the intruder has reached the centre.

Ray Lock
Network Technology Director
Westermo Group

For more information on Westermo and the WeOS operating systems cyber security features please visit http://westermo.com/.

Westermo Teleindustri AB
SE-640 40 Stora Sundby, Sweden
Tel. +46 (0)16 42 80 00 I Fax. +46 (0)16 42 80 01
info@westermo.com I www.westermo.com

Corp ID No: 556361-2604
VAT: SE556361260401