Secure Crossing Research and Development Inc.
6 Parklane Boulevard Suite 545
Dearborn, Michigan 48126
248-535-3800   www.securecrossing.com

Industrial Protocol Filtering?

How is it better than a Firewall and Intrusion Prevention?

Industrial Protocol Actions Whitelisting

At Secure Crossing Research & Development, Inc., we have developed a new advanced way to protect "Industrial Control Systems" with an emphasis on protecting "Critical Infrastructure."

Our world-leader, innovative product filters Industrial Protocols including CIP (Common Industrial Protocol) delivered over EtherNet/IP and developed by Rockwell Automation and Cisco Systems. Other filtered protocols are DNP3 (Distributed Network Protocol) primarily used by the power industry to control substations; Modbus (Serial Communication Standard developed by Modicon and updated to work over TCP/IP and UDP/IP) used in many control systems; OPC (OLE for Process Control) with two standards OPC classic originally developed to bind with Windows COM/DCOM and OPC UA (Unified Architecture) that is an open standard. Now, we added Profinet which is the open industrial Ethernet standard of PROFIBUS & PROFINET International (PI) for industrial automation.

Traditionally, firewalls do not allow any inbound traffic by default and allow one-way or round trip traffic by rules. More sophisticated systems can allow or disallow traffic by protocol, for example to allow CIP or Modbus, but do not understand anything within those protocols. This would only allow all actions or disallow all actions within that protocol. Today, this is an inadequate means of controlling security on complex industrial networks!

Intrusion Detection and Intrusion Prevention Systems (IDS/IPS) normally rely on signature comparisons such as the wildly popular Snort (owned by Sourcefire). Currently, most vendors use this in some "flavor" where they have modified or tuned it for their specific product offering.

Digital Bond took it one step further with the "Quick Draw" project originally funded by a Department of Homeland Security (DHS) grant to provide "Preprocessors" for Industrial Protocols as an add on to Snort. This approach of comparing a known signature to multiple packets that have been parsed and reassembled for comparison is a major problem. Some of the "Objects" within CIP (Common Industrial Protocol) for example have multiple embedded "Objects," and thus **cannot** be properly handled by a signature comparison even with the use of a "Preprocessor." This method is very inaccurate and easily evaded, leading to considerable false positives and false negatives – completely unsuitable in the Industrial Automation and Critical Infrastructure arena.

The "Scan Engine" (ZenD) in Secure Crossing's Zenwall line of products was built from the ground up with one purpose in mind – to filter Industrial Protocols! Secure Crossing's products are built on top of the FreeBSD operating system which is much more secure than Linux or Windows and handles the parsing of data packets with a different method more suitable for fast Industrial Protocol filtering.

The protocol filters (one for each Industrial Protocol) parse, assemble and look at the respective protocols based on the standards that each protocol conforms. At this level of inspection, we are able to precisely set filters to allow specific traffic into the control system environment. By controlling, as a basic example (Reads, Writes, Stops, Resets sent to the PLCs, RTUs, etc.,) threats to the Industrial Control's zone/cell/ junction box can be eliminated.

Also, the "Scan Engine" (ZenD) will analyze the complete data stream and pull out only the protocol the customer selects to be confirmed as legitimate actions, and then ZenD will auto write the filter for you! This greatly accelerates implementation of new filters and saves time for the customer!

Secure Crossing's methodology is to use the "whitelisting" approach. By disallowing all traffic and allowing only the selected protocols and specific actions within those protocols, Zenwall provides the level of filtering needed for a customer to solve SCADA, Remote Location or Zone Level Security. Where other products attempt to detect the bad, we can specifically allow the known good and block everything else. This is a win in any security context, as the number of bad possibilities almost always vastly outweigh the legitimate known good traffic. Along with source/destination authentication, advanced reporting, remote connectivity and audit tools, you have a winning solution to securing your critical infrastructure!