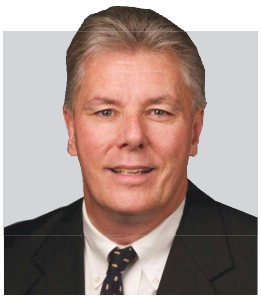
IT Intelligence

CONTENDING WITH ENCRYPTION AND AUTHENTICATION REQUIREMENTS

by Bob Stockwell



Bob Stockwell is Global Technology Leader for STANLEY Security. From 1997-2012, he was Niscayah's Director of Systems Operations.

bob.stockwell@sbdinc.com

In this era of constant connectivity — through Internet, social media platforms and e-commerce sites — Web users are constantly faced with hacking attempts on their computers and network systems. In response to the vulnerabilities brought on by this technological system of open communication and sharing between networks, IT departments using best practices are establishing a series of standardized security measures in order to protect sensitive company and personnel data and network information. These practices often include implementing encrypted connections between locations, blocking ports and limiting access to critical information and resources, based on job role and responsibility.

While these lines of defense are absolutely necessary to guard companies and their employees and networks against hacking attempts, they can cause a huge challenge for today's systems integrator. In order to successfully and efficiently set up a company's security system, an integrator will require access to the customer's network and resources. Since integrators are not technically employees of the customer, they are not bound by the company policies and rules. Therefore, considering the nature of the installation and integration, systems integrators must recognize that these policies may still apply, and be willing to sign documentation stating that all protective protocol and standards will be followed. Every company has its own individual policies that must be adhered to, and many are also governed by state and federal laws. In order to implement a security solution that both continues and enhances these compliance efforts, integrators should familiarize themselves with the details of these standards and governing laws so as to provide customers with the most seamless system integration and transition.

After jumping the compliancy hurdle, integrators then need to work with the company's IT department to acquire authorized access to the correct resources and with the appropriate permissions. Factors, such as ports, permissions, services and communications with other servers can all cause delays in the successful system integration. For example, it doesn't help the integrator much to be able to connect to a system but not be able to make the necessary changes to install and configure it for the customer. That being said, integrators need to make sure they know the application needs of the customer. Many applications and equipment communicate on unique ports, and some use proprietary encryption or may be at a remote location. It is important to be aware of these intricacies and communicate product and equipment requirements to the customer's IT department so the team can configure the equipment to accommodate the new security systems. For instance, many businesses block streaming video, and integrators can end up spending hours troubleshooting why video works in one location, and not another. Knowing the products' requirements beforehand will make achieving the correct access and permissions much easier.

Network encryption can also cause challenges in system integration. The more secure the encryption, the more processing power required to encrypt and unencrypt the data. Sending multiple video streams from one location to another across an encrypted network could quickly overwhelm network equipment. Therefore, even if the network equipment can process the data, it will still add latency to the system. This is not a showstopper, but needs to be clearly understood and communicated to the customer. If acceptable, creating rules-based exceptions can help reduce latency by allowing certain data to bypass the encryption process.

Discovering permissions and encryption challenges in the midst of an installation can delay the process and waste valuable time, increase frustration and contribute to the integrator's loss of confidence.

There are many crucial elements to consider when implementing a security system for a customer. Discovering that there are permissions and encryption challenges while in the midst of an installation can delay the process and waste valuable time, increase frustration and contribute to the integrator's loss of confidence in their ability. Fully documenting and communicating the security system needs with the company's IT department will make the installation process and system performance more efficient and profitable. ■