B2B gateways were introduced in 2003, marking the first time IT professionals could deploy best-of-breed managed file transfer tools without sacrificing their larger investment in enterprise business applications. Today, that value proposition has an added advantage: gateways have become building blocks for a secure information strategy.

The intent of this article is to provide even-handed criteria for evaluating B2B gateways within the context of overall information security. "Information security" refers to all activities—physical, electronic, social—related to corporate information protection. This includes, but is not limited to, physically securing the premises, encrypting and backing up data, and developing, publishing and promoting an enterprise-wide security policy.

Data transfer over public networks: risks and rewards

The appeal of a B2B gateway is based, in no small measure, on cryptographic attributes that allow data to be transmitted securely over public networks rather than proprietary VANs. Although the cost savings are attractive, any enterprise choosing to transport data across a public network assumes responsibility for protecting its infrastructure against risks posed by the public network itself. The basic factors to consider are network reliability, load capacity, in-transit data protection, and shielding the enterprise from viruses, worms, and other malware.

As Gartner points out, centralization is one of the explicit virtues of the B2B gateway. A single, secure data portal is advantageous for many reasons, particularly for firms that must demonstrate robust data security for compliance audits. This consolidated port of entry defines the "edge" of the corporate domain and clarifies accountability for data moving into and out of the enterprise.

Security-related gateway evaluation factors

Gateway technology is specifically designed to address the data security risks described above.

But gateways entail risks of their own that that must be factored into any system evaluation. These risks can be divided into two categories: absolute (functionality-driven) and relative (cost/value-driven).

Absolute risks

• *Capability*: How effectively will the gateway handle the functions most important to your operation? How well will it conform to your enterprise's published performance standards?
• *Platform support*: How efficient will the technology be within your hardware/operating system environment? Is it certified to meet your corporate production requirements?
• *Compliance*: If you must comply with corporate or industry regulations—HIPAA, GLB, Sarbanes-Oxley, and PCI, for example—does the system meet those standards and support timely, efficient compliance reporting?

Relative risks

Relative risk factors relate to the cost of acquiring, installing, operating and maintaining the system. The right gateway choice for your company is the one that delivers the most value per dollar compared to 1.) other options in the marketplace; and 2.) the importance of the following factors within your operation:

• *Performance*: Better-performing systems consume less CPU, disk and memory resources. They are typically a better long-term buy for two more reasons: corporate traffic almost always increases rather than decreases, and a robust gateway can reduce (or redistribute) overall loads so your existing infrastructure can accommodate more traffic.
• *Reliability*: By definition, gateways are expected to be highly available. How well will the system scale in large, clustered implementations? How quickly can it recover from exceptional conditions, including component failure?
• *Ease of implementation*: The more quickly the gateway can be installed and put into production, the better the odds for rapid adoption and support by the enterprise.
• *Ease of use*: The most vocal proponents (or critics) of any system are usually the people responsible for its day-to-day operation. Usability promotes user adoption and delivers tangible benefits such as fewer input errors and faster, more effective reporting. From an operations standpoint, a system that can be readily modified and reconfigured requires shorter maintenance windows.

Typical stages of corporate information security

The fundamentals of securing corporate data don't change. At the most basic level, they boil down to restricting access, applying safety measures to the data itself, and making duplicates in case the original is lost or corrupted.

The operational context for these fundamentals, however, is constantly evolving. Most enterprises go through four stages of integrating information security into their core business processes.

Stage #1: The Fortress
At this stage, the enterprise protects data by building a wall around it. Information within this fortress is not encrypted, and the data transfer mechanisms aren't necessarily secure. Protection consists of restricting physical access to campuses and data centers and requiring passwords for log-in. Database passwords are often left at default values or are widely known and rarely changed, since all the data is "internal" anyway. In this scenario, the safety of all data is essentially equivalent and completely dependent on physical safeguards. Security is not intrinsic to either the data or business process.

Stage #2: The Private Line
At this stage, the company embraces the "private line" or "secure tunnel" for inter-enterprise data exchange. This link is secure, but no assumptions are made about protection beyond the link, and a breach in the link will expose all in-transit data. Business processes at either end of the link expect data in its native format. Security is not intrinsic to either the data or business processes.

Stage #3: Security Off the Wire
The third evolutionary stage infuses protection higher in the protocol stack. The application-layer software encrypts data using features within a broader software suite, or through a separate security product integrated into the overall business information process. Data transformation for the sake of security is only applied when necessary.

This stage takes security "off the wire" and allows the use of non-dedicated (but intrinsically less secure) networks like the Internet. Data protection may be oriented toward the document itself, treating each discrete document as an independently secured message, or toward the session layer (SSL and TLS). In the latter case, security parameters are established between two end-points and applied to one or more discrete documents passing over the session.

At this stage, data protection is disengaged from the lower, physical or data-link layers. This takes the safety burden off the network's shoulders. But engaging security at the application layer makes information safety beholden to the prerogatives of the business process. Disparate applications may provide different, and possibly wholly incompatible, data security schemes.

These differences make secure data transfer between heterogeneous systems across a public network a formidable integration challenge.

Stage #4: The B2B Gateway
At this stage the corporation recognizes the value of a single subsystem for reliable, interoperable, secure data transfer over relatively low-cost public networks. Within the centralized architecture, all applications conform to the corporate security policy. Adaptive gateway interfaces make application integration relatively simple. Ongoing gateway operations can be easily monitored and exceptional conditions reported immediately.

B2B gateways that understand multiple application-layer transfer protocols—HTTPS, S/FTP, and so forth—can be configured to adapt to changes in the way the enterprise arranges its communications with others. By disengaging the secure communications aspect from the business process infrastructure, the company can tune components without tearing down and starting over.

ANY ENTERPRISE PREPARING TO EXPAND INTER- OR INTRA-COMPANY DATA EXCHANGE MUST HAVE AN UPDATED, WRITTEN CORPORATE INFORMATION SECURITY POLICY

Choose technology to support your security policy—not vice versa

Any enterprise preparing to expand inter- or intra-company data exchange must have an updated, written corporate information security policy. (The SANS Institute provides useful guidelines and templates at www.sans.org/resources/policies.) Well-crafted policies are clear about the company's standards and procedures in the following areas.

Asset protection: Reducing or preventing data loss with measures such as eliminating single points of failure in critical data processing paths. Other examples: appropriate data backup, in-place redundant systems, and ongoing hardware maintenance.

Access control: Installing authentication controls at both human and external system access points; requiring and enforcing the use of security credentials.

Vulnerability detection: Establishing mechanisms to detect compromised and/or vulnerable systems. For example, a digital certificate approaching its expiry date represents a definite vulnerability. A user account that hasn't been accessed for a long period represents a potential vulnerability.

Monitoring and reporting: Creating procedures to record and report access to sensitive information. Reports showing usual-and-customary access patterns are helpful for operators on the alert for unusual, and potentially harmful, activity.

PAIN: the elements of secure data transfer
Secure electronic data transfer has four attributes: Privacy, Authentication, Integrity, and Non-repudiation. Prudent business practices—and increasingly, government and industry mandates—require these attributes in electronic data exchange of all types, including gateways.

Privacy: Encrypted data is intelligible only to those with the proper security credentials. Typically a public-key encryption scheme is used to ensure that only the intended recipient of the data can decipher the message.

Authentication: Secure credentials identify the originator or sender of the information. This is typically accomplished by attaching a digital signature to the message. The signature, encrypted with security credentials held only by the sender, can be authenticated by any recipient in possession of the sender's public key.

Integrity: A relatively short sequence of bits, known as a message digest, is produced using an algorithm with a very high probability of generating a different digest should any single bit in a message be altered. By sending an encrypted digest along with the message, a recipient can compare a locally computed digest to verify that the message was not altered in transit.

Non-repudiation: To prove non-repudiation (a receipt which the receiver cannot effectively deny), the data recipient digitally signs and returns an acknowledgment to the sender that includes the matching digest of the message, thereby providing both a certain identification of the recipient and proof that the message was successfully decrypted and received intact.

A B2B gateway evaluation matrix

In summary, B2B gateways represent the consolidation of secure communication services accessible to various internal systems through adaptive interfaces. Endpoint configuration is relationship (trading partner) oriented, given the underlying assumption that endpoint management requires handling protocols or connections that vary by endpoint. Gateway activity is driven through interfaces to a business process management (BPM) system and integrated with information gathered throughout the enterprise.

David Walling is Chief Technology Officer for nuBridges. He can be reached at dwalling@nubridges.com.