Description of the Application

Sales Force Automation (SFA) applications comprise a subset of standard Customer Relationship Management (CRM) solutions. SFA applications are typically software solutions designed to assist an enterprise with coordinating sales activities across inside sales, field sales, channel partners, and online sales channels.

To provide the necessary functionality, SFA applications must deliver features that help improve sales channel effectiveness and efficiency, spanning account management, sales opportunity insight, sales quotes and proposals, product pricing, sales force and channel commission, new order entry, and shipped order tracking. SFA applications can also offer industry-specific capabilities to enhance selling productivity.

Challenges to the Application Type

SFA applications are typically based on application server technology with a common 3-tier architecture. In many cases, these platforms are hidden from the customer, as SFA vendors optimize application server configurations to address some of the more common SFA deployment and operational challenges:

Providing scalability - SFA applications struggle with scalability. To support the needs of multiple users accessing extensive sets of information, SFA applications must perform complex queries, apply business rules and policies, and ultimately apply presentation logic. This complex architecture places a heavy burden on servers supporting the application, resulting in the need for advanced clustering or chaining of multiple servers.

Enhancing performance - Basic SFA applications are designed and developed to provide scalability in a standard deployment. However, the customization required to match the needs of a unique sales force adds solution complexity, and can create major problems for these standard deployments, particularly during peak usage periods such as holidays, company promotions, and end of quarter activities.

Providing security - Sensitive sales forecasting and strategic data requires a high degree of security. As most SFA applications move towards a Web-based architecture, providing security becomes increasingly challenging. If the SFA application utilizes SSL (Secure Sockets Layer) to encrypt traffic, it can compromise the performance and scale of the application servers that support it. This requires additional servers and increases deployment cost and complexity.

Solving implementation complexity - Many SFA applications are difficult to deploy because the implementation is so complex. Every customer has variable selling approaches, so each SFA application must be customized. As a result of this customization, deployments can take significant amounts of time, scalability and performance will vary, and future upgrades become increasingly complex.

Providing for lengthy connections - SFA applications are effectively the primary desktop productivity application of the sales channel. From this one application, they perform nearly all daily tasks. Therefore, most connections to the server exist for long periods of time, requiring session persistence, which can slow application servers (software-based solutions) to an estimated 30-40% of their optimal performance.

Allowing remote users - With most SFA users residing in field offices or channel partner locations, remote user access is essential. While Web architecture can address most scenarios, there is a trend towards providing true mobile access to sales tools from devices like mobile phones and handheld computers. These smaller, mobile clients can require special functionality to ensure users get the important information they need, when they need it.

F5 Solution Overview

With powerful local and global traffic management network products, F5 Networks offers valuable benefits for getting the most out of any SFA application deployment. F5 Networks has established itself as a leader, able to enhance the scalability of enterprise solutions and optimize network performance through intelligent Layer 7 management. As the global leader in SSL for network devices, sensitive customer information is always protected as it travels over the network, with 40-60% better performance than software-based security. F5 Networks provides a solution that works gracefully with SFA application, helping to minimize overall complexity, while still supporting all mission-critical applications.

The BIG-IP system version 9 offers substantial improvement in efficiency with bandwidth reduction and TCP optimization, while enhancing the secure delivery of web applications. And with the FirePass controller SSL VPN, organizations can extend secure access to the enterprise’s SFA applications for all remote and internal users.

TMOS acts as a full TCP/IP proxy with independent optimization of client-side and server-side connections. Utilizing this TCP Express functionality, the BIG-IP system eliminates the need for clients and servers to negotiate the lowest common denominator for communications, dramatically improving network efficiency and end user performance.
TCP Express optimization also enables the BIG-IP system to act as a bridge or translation device between all clients and back end servers. Even when organizations are utilizing legacy servers and applications, the BIG-IP system mediates between non-optimized or otherwise incompatible devices to optimize network communication. This solution provides organizations with tremendous cost savings and scalability as well as an unparalleled ability to translate communication improvement capabilities across their entire infrastructure.

As the global leader in SSL (Secure Sockets Layer) for network devices, F5 Networks provides customers with solutions to ensure that their sensitive information is protected as it travels over the network, with 40-60% better performance than software-based security.

F5 Networks’ FirePass controller SSL VPN extends this level of performance and access securely to remote users. The FirePass device provides access to internal web servers, as easily as from inside the corporate LAN. It also delivers granular access control to intranet resources on a group basis. For example, the FirePass controller can provide employees with access to all intranet sites while partners are restricted to a specific web host.