Communicating With Sam

Mobility Next Generation: Bringing the Enterprise to the Business

Sam Johnston

Question:

Our Company is investigating deploying sales force and technician field automation solutions. Currently, our key databases reside on the iSeries and we are investigating end-to-end solutions from an access and security standpoint that will enable our employees to have virtually anytime, anywhere access to our core system for real-time transactions. Currently, our application security scheme has assumed only local authentication and thus password protection is all that we have used. What are our gaps in system and network functionality and security that we have to overcome to successfully deploy this technology?

Answer:

Quietly and rapidly, there is a new revolution that is quickly taking hold within our industry. This perfect storm of sorts is actually the merging of two "tornado" markets, on one hand the ubiquitous presence of the Internet, and on the other hand the pervasive use of cellular devices. We are talking about more than getting e-mail and the Web on a Blackberry. The two technologies are working together to deliver business applications anywhere and anytime to virtually any device. In essence, it is enabling enterprise business applications to perform transactions outside of the four walls of offices, factories and warehouses, and letting businesses perform these transactions where and when the customer demands. While this has the sales and marketing executives jumping for joy over competitive differentiation, the CIOs and more importantly security officers are having endless sleepless nights over the management challenges this new world will bring.

We'll assume that your business has gone through the business impact of this new model, and the ROI is there, so let's turn to some of the technical issues you will need to deal with. There are a number of components that you need to consider in providing anytime, anywhere access to your enterprise databases. These include:

- Definition of the devices that you intend to use as access endpoints
- Determination of the Network you require to operate your applications
- Development of Portals for access to your enterprise application
- Ensuring a secure computing environment both internally and externally
- Management of the infrastructure once implemented

The first point you need to understand is what devices you are planning to mobilize. The most common data interface endpoints would be laptops and/or PDAs, which now come in many forms with numerous peripheral devices. We will assume that your applications port to these endpoints for the benefit of the discussion, or that at the very least there are practical middleware solutions that will integrate to your ERP solution to enable the solution. Both of these solutions present organizations with numerous options in mobile connectivity. The laptop will provide you with enhanced capacity and performance, and the most flexibility with providing support for LAN connectivity, 802.11a/b/g wireless, or 1X or equivalent data networks. The PDA can provide similar functionality in a more portable solution. Regardless of the solution you choose you will need to also select a network or networks to support your solution.

Mobilizing your workforce within the enterprise typically involves the implementation of an 802.11a/b/g network infrastructure to support roaming within your walls. The implementation of the network will require deployment of Access Points into your facilities. These Access Points need to be deployed to provide a wireless coverage range to meet your business requirements. Density of the deployment will also need to vary depending upon your traffic density. An additional deployment consideration will be whether to deploy "smart" Access Points or "dumb" Access Points with a centralized management strategy. This decision alone could be a detailed discussion, so it is best to assume that one or the other will best suit your environment.

Once you reach beyond your enterprise, there are typically three modes of access to your enterprise. The two most common forms are either LAN or wireless based VPN from a remote network node (home, hotel, hotspot) or dial-up remote access solutions. Another option that is growing in popularity is connectivity to a wireless 1X or equivalent data network which essentially provides a mobile device anywhere connectivity, similar to cell phone coverage, to the enterprise via a portal. This solution is typically more costly and has some bandwidth limitations but is the most mobile solution available. What all of these remote-access solutions have in common is that you need a way to connect to your enterprise network and/or enterprise system to process data, and this is where portals come in.

There are a number of ways to connect into your enterprise, with some of the most common solutions being:

1. VPN Concentrator for Internet based access
2. RAS gateway for PSTN based call termination
3. Web Server/Secure Portal Server in DMZ
4. Direct Gateway Termination into Enterprise

Terminating mobile clients onto VPN concentrators can happen in a number of ways, with IPSEC client termination and SSL VPN termination being the most common. IPSec client termination does require that a client be installed onto the mobile device. This solution is the most OS and CPU intensive connection option but is also the most secure. The SSL VPN option, with newer technical enhancements, is a secure solution with more flexibility. In permitting SSL VPNs it is important that you manage the flow of data since non-corporate endpoints can connect to this solution.

RAS gateway termination has been in place for many years and early mobile solutions leveraged dialup connectivity to establish connections. Shortcomings of this solution are bandwidth and performance. Web Server or Secure portal Server solutions are also popular for terminating client sessions on mobile devices. These servers usually act as the interface to the mobile client and have connections inbound to middleware servers or in some cases database servers to complete the transactions. It is critical that these application servers are hardened and secured.

Sending data over shared, public networks and in some cases deploying data to mobile devices has many security considerations.

Another option is a direct connection gateway termination into the enterprise. This solution is not as popular as it once was and usually does not provide the flexibility of some of the standard based networks. However, if the solution can be designed to meet your performance needs, it is often easier to manage. With any of these mobility solutions and enterprise connection options, security is a key consideration. Unlike extending data into your enterprise, sending data over shared, public networks and in some cases deploying data to mobile devices has many security considerations.

Firstly, physical security is paramount, as it is readily known that mobile devices are much more prone to loss or theft than internal enterprise devices. Any solution that includes mobile data computing outside the enterprise should consider controlling the amount and type of information that gets propagated or stored on the mobile device. Tools such as disk encryption combined with complex 2-factor authentication schemes can help secure access to the device. The best security is to design your applications to minimize the amount of information that goes to the client.

...anywhere and anytime can ultimately lead your business to competitive advantage

However, this may have some bandwidth considerations. Another physical security consideration is when a device is lost or stolen that the security and authentication parameters cannot be mined and used as an overt threat to the enterprise.

Secondly, the data session, if traveling over a public network, should be encrypted between the endpoints. This is also a good idea on some private networks. Additionally, the mechanisms for security authentication and providing identity control should be current to the industry standards.

For Web Server and Portal applications the servers themselves should be hardened and secured into a DMZ behind a firewall with IDS schemes in place. Additionally, the enterprise facing communications channels should be secured and managed with additional levels of firewalls and IDS technology. For SSL solutions with large client deployments, hardware SSL termination devices are recommended.

A third concern is to ensure that the device connected to the network has itself been properly secured and possesses the necessary anti-virus, security settings and code level to operate. Solutions like Cisco's Network Admission Control can assist in this area.

The final consideration is management of your devices. If you thought inventory tracking of stationary devices was difficult, the problems are compounded in a mobile world. Not only are you trying to manage the availability of the devices to ensure high productivity of the end users but you are also trying to manage and protect the asset. Additionally, for mobile users, updates to firmware and applications on the go must be considered and a help desk in place to manage and support the end users. There are also a number of challenges with this offering as many solutions are still emerging and standards are being set. Do not forget strong policy to help manage deployments.

The prospect of enabling business transactions to be processed anywhere and anytime can ultimately lead your business to competitive advantage by allowing business to go to customers with real time responsiveness. However, like any transformational solution, success will be in the execution. The challenge is enormous and the complexity will increase dramatically, as will the number of networks and points of failure. The potential for security holes and financial black holes is large. While all these challenges are known, and will be acknowledged as important by stakeholders, ultimately most organizations generally will focus more on the client interface and middleware solution, leaving limited resources for other aspects of the project. Successful organizations will understand that the key to success will be in developing a strong management framework for all aspects of the solution, including asset, security and network management.

***Sam Johnston** is a partner and Chief Technology Officer of Intesys Network Communications Ltd., providing value-added networking and e-commerce solutions to the iSeries community. He can be reached at (416) 438-0002 or via e-mail at sjohnston@intesys-ncl.com. Any TUG member wishing to submit a question to Sam can forward their typewritten material to the TUG office, or to Intesys. The deadline for our next issue is Friday December 2, 2005.*