Mobile Connectivity

Description of the Application

The ability to connect mobile devices, such as a handheld computer or a cellular telephone, to the network is no longer a “nice-to-have”; it is quickly becoming a requirement for organizations worldwide. Although mobile connectivity has matured over the past two years, it continues to be a segmented and fast-changing industry, with new technology constantly being developed. It is certain, however, that mobile communication will have a significant impact on most organizations over the next three years.

Some mobile technology vendors have already been successful in drawing subscribers to colorful and useful content using personal phones. Others offer mobile access to corporate email and other applications from handheld devices. However, no vendor currently offers an end-to-end solution for mobile applications. The challenge for most organizations is to quickly route and deploy a multitude of mobile solutions, with as little impact as possible to the existing networks.

Challenges to the Application Type

Deploying a wide array of mobile connectivity options makes it critical to address the core issues of a mobile infrastructure:

**Providing session direction** - A major concern when deploying new mobile solutions is how incoming traffic will be directed to these mobile solutions. Another concern is how to quickly add new mobile applications without changing the handling of existing mobile applications.

**Providing security** - When users are allowed to connect a mobile device to the network, company resources are exposed to external users. Many enterprises use applications that involve commerce, which require high levels of security and encryption, yet they also need to partner with an external company for these mobile applications. Allowing partner access to the network, yet still keeping data secure, is a major challenge for mobile deployments.

**Enhancing scalability and performance** - Another significant challenge for planning mobile applications is knowing how many users will take advantage of mobile connectivity. The goal is to keep technology and hardware purchases low in order to purchase multiple solutions, yet still allow for scalability. Compounding the issue is that most new mobile applications do not involve large-scale deployments, so scalability concerns have not yet been addressed.

**Usability** - Because mobile devices typically have tiny screens, and limited ability to display images, a network solution must have the ability to dynamically reformat content to fit on the user’s screen, no matter what device is connecting to the network.

F5 Solution Overview

F5 Networks’ BIG-IP® solution solves many of these challenges by addressing critical issues and providing a robust platform to develop or deploy mobile connectivity options. The BIG-IP product includes a number of features to allow organizations to get their mobile applications into the hands of employees or customers today, while helping prepare for future mobile growth.

The Universal Inspection Engine (UIE) on the BIG-IP product can route application specific traffic straight to the appropriate server the moment the traffic enters the network. With the UIE, mobile email traffic is routed to special servers, handheld computer users are routed to specific servers, and SMS (Short Message Service) traffic is routed to different SMSC (Short Message Service Center) gateways, all based on keywords. The UIE examines all of the HTTP or TCP payload and directs traffic based on configurable iRules™. Organizations can add new mobile applications and route traffic to them without disrupting the network or other servers.

When SSL (Secure Sockets Layer) connectivity is required between mobile devices and the network, or the network and a partner’s application, the BIG-IP product first offloads the CPU-intensive SSL processing, then load balances and directs the traffic. The BIG-IP product’s industry leading SSL performance alleviates concerns about overloading servers with new wireless applications or increased usage.

The BIG-IP solution enhances the scalability and performance of any network, including networks with mobile applications. The Extended Content Verification (ECV) feature on the BIG-IP product goes much further than standard health checks to determine if a server is up or down. It allows the administrator to duplicate actual server connections and content requests to product reliably supports employees, partners, and customers. The network can effectively grow with the mobile user base, while reducing initial hardware investments and without limiting future growth.
F5 Solution Overview - continued

With F5’s FirePass controller, organizations are able to extend access to internal resources to their remote workforce, partners, or customers, from any device in any location. The FirePass SSL VPN provides secured, clientless access to off-site users as easily as if they were in the corporate LAN. Once authenticated by the FirePass controller, users pass through the corporate firewall and are able to access applications without having to re-authenticate for multiple resources.

For mobile users, the FirePass controller allows secure access from PDAs (like Palm OS), and cell phones (like WAP and iMode phones) to email and other applications. It dynamically formats email from POP/IMAP/SMTP email servers to fit the smaller screens of mobile phones and PDAs, and supports the sending of network files as email attachments and the viewing of text/Word documents.

The FirePass controller also offers network administrators simplicity and granular control of access to intranet resources on a group basis, improving quality of service for the enterprise while reducing overhead.