Securing Cellular Data Over The Internet

Cellular technology has changed from being used primarily for telephone service to being utilized for broadband data travelling over the Internet.

Problem

Over the last twenty years, cellular technology has changed from being used primarily for telephone service to being utilized for broadband data travelling over the Internet. Cellular data transfer started as basic M2M (Machine-To-Machine) file transfer or polled data. Initially this was based on analog technology, but as frequency spectrum became scarce due to increased demand, carriers incorporated digital technologies including EVDO and HSDPA. With the advent of these technologies, data transfer rates have increased from 56Kbps to over 1Mbps. These technologies have led to where data links are carrying more than raw M2M data but also carrying IP based applications such as VoIP.

To insure cellular data security and reliability, a VPN (Virtual Private Network) must be incorporated. A simple VPN client with a plug-in air card will suffice for casual data, but for privacy and security concerns the need goes beyond PC based traffic.

The Encore Solution

Encore Networks addresses today's cellular data networking requirements and challenges with the BANDIT™ line of environmentally hardened (rugged) routers. The BANDIT™ includes the features required for secure business applications like firewall, VPN encryption, and DHCP server capabilities and provides fully featured routing which supports VoIP, Internet and Intranet access for remote and mobile offices. For cellular data networking, the BANDIT™ integrates a hardened modem which can withstand a wide range of temperatures found in many M2M applications such as utility service providers (electric, gas and water), construction sites, industrial environments, lottery terminals, ATM machines and point-of-sale locations.

The BANDIT™ offers legacy M2M protocol conversion such as DNP, Conitel, PGE and
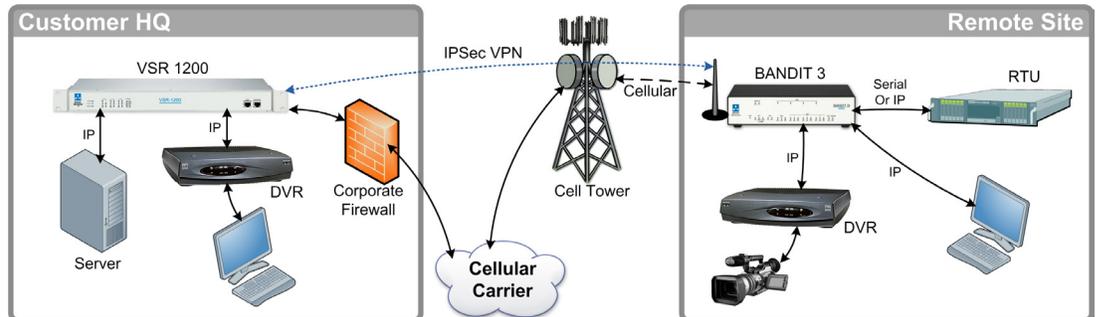
M2M requires a router, a VPN appliance and, at times, legacy protocol conversion.

The function of a router is to convert IP-based data from one addressing scheme to another, for example, public to private addressing. All routers do this but very few incorporate a cellular modem designed to meet commercial and industrial grade requirements. A router supporting VPN in various encryption modes like 3DES or AES is fairly common, but again finding one with a cellular modem, not just a PCMCIA card, further limits your selection. Also, most routers encapsulate legacy protocols by bundling them into IP packets for file transfer over a cellular data link. This creates unacceptable latency and efficiency problems.

CDC. By converting legacy protocols locally for encrypted IP transport, the data packet is more efficient and can carry more data in the packet payload which greatly reduces the effect of network latency. Encore's central site solution, the VSR-1200™, supports multiple host sites for redundancy which further reduces latency and increases network reliability.