



CASE STUDY WIRELESS SECURITY

HEALTHCARE

Secure Wireless Communication Ensures Patient Confidentiality

Leading Healthcare Application Kept Alive with Secure Wireless

Benefits

- Stringent Security
- Comprehensive Management
- Proven Performance
- Investment Protection
- Easy to Deploy
- Transparent to User

The healthcare market today can tap into the freedom and productivity of a wireless workforce. However, wireless networks open doors to the possibility of intrusions, network vulnerabilities and an unintended lack of privacy. The lack of physical boundaries on wireless users creates new security challenges for information technology managers and administrators.

Healthcare Market Demands Privacy

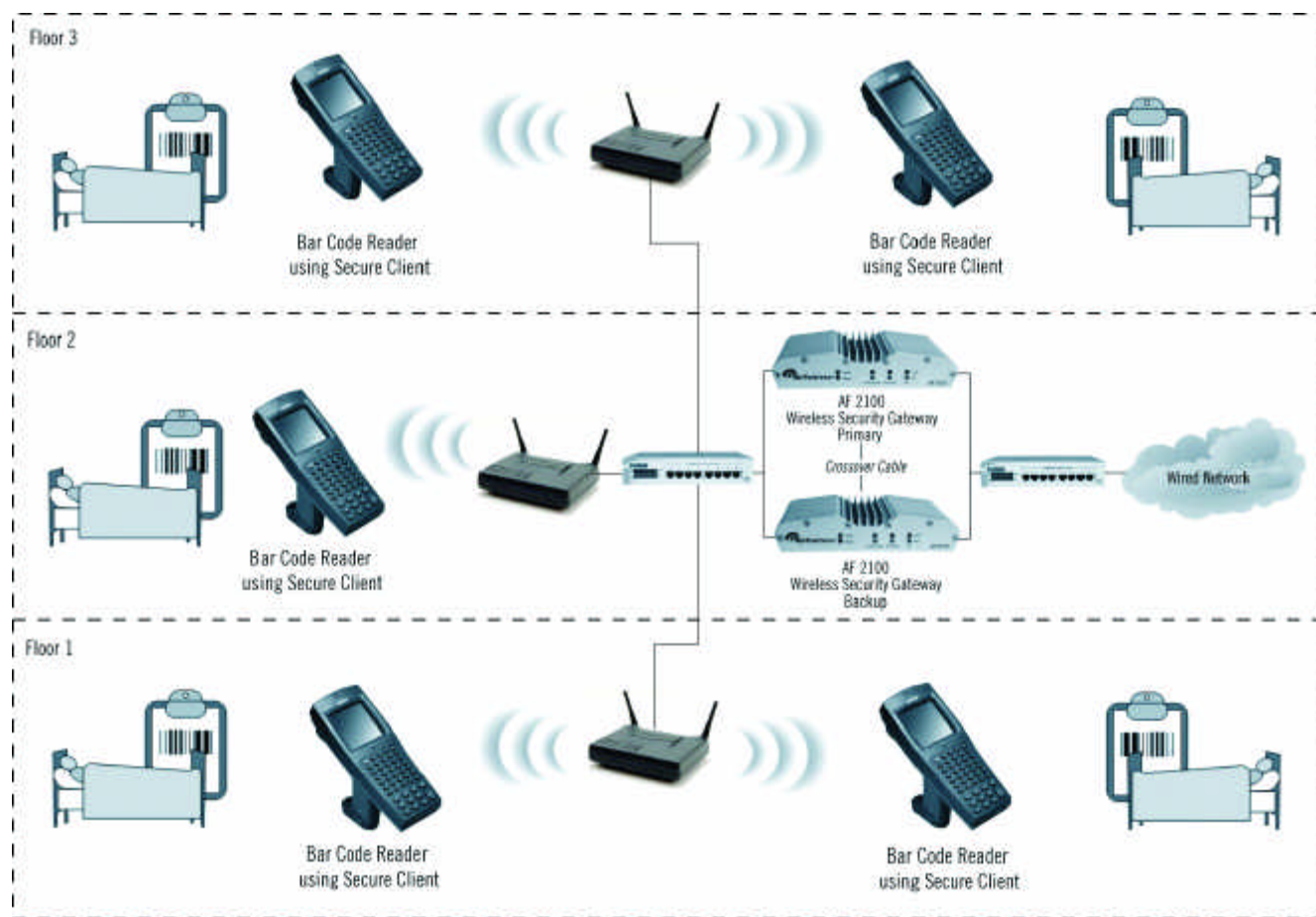
With Federal legislation requirements, government agencies such as the Department of Veterans Affairs (VA), along with the general healthcare market have taken steps to ensure the integrity and privacy of its patients. The Federal Health Insurance Portability and Accountability Act (HIPAA) requires that all hospitals in the country take the steps necessary to protect the privacy of patient information including securing data distributed across wireless local area networks.

The VA has taken measures to secure its wireless networks. The VA has selected Fortress Wireless Security Gateways to protect both the medical networks and wireless communications in 167 hospitals and medical centers. The Fortress products will secure the VA's wireless application used for real-time retrieval of patient information. The application provides the healthcare providers with medical information at the patient's bedside. It is the primary application used to support inpatient medication administration and has become a key component of quality assurance. This application is deployed on inpatient

wards across VA's healthcare system. A typical VA site has five wards with anywhere from 10 to 12 (802.11b) wireless access points per ward. The VA's Bar Code Medication Application runs on six to 10 mobile clients in each ward. The application runs on Windows® 2000 Professional, Windows 95 or Windows XP; all are configured with 802.11b NICs. The access points are wired into a single VLAN in a network switch and then two Fortress Gateways are configured in fail over mode to bridge traffic between the encrypted VLAN and the LAN. The Fortress Access Control Server (ACS) that manages device authentication and user authentication is also deployed to help administrators easily control and maintain the Fortress secured network on the LAN. The ACS is configured to use the existing NT Domain to authenticate the wireless users.

Tested & Proven Security

Fortress offers the most flexible, market-proven security products that address the inherent risks and vulnerabilities of 802.11 and other wireless networks. The security products offer a trusted and easy-to-use solution that ensures the business integrity demanded by Global 1000 companies, government agencies and healthcare organizations. Fortress was the first wireless security product to meet the U.S. government's rigorous standards cryptographic security, certified by the National Institute of Standards and Technologies (NIST) and the Department of Defense, among others.



The Fortress Security Gateway installs seamlessly between wireless access points and the corporate network. One of the unique attributes of the Fortress Gateway is that it can be used to secure any vendor's access points. Multiple Fortress Gateways can then be managed by the Fortress Access Control Server and/or tied into existing directory and policy servers such as RADIUS, LDAP or NT Domain services.

Fortress Products

Fortress products are sold and co-marketed through a growing list of authorized platform partners, systems integrators and resellers including a select group of Fortress Solution Providers who are extensively trained in the planning and deployment of secure wireless networks.

www.fortresstech.com

Fortress Technologies Inc.
 4023 Tampa Road, Suite 2000
 Oldsmar, FL 34677
Phone: 813.288.7388
1.888.4Privacy (477-4822)

