

CASE STUDY Federal Government



Secure Wireless Communication Ensures Patient Confidentiality

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 failover mode to bridge traffic between the encrypted VLAN and the LAN. The Fortress Management and Policy Server (MaPS™) that manages device authentication and user authentication is also deployed to help administrators easily control and maintain the Fortress secured network on the LAN. MaPS is configured to use the existing NT Domain to authenticate the wireless users.



Challenges

- Secure both legacy devices and newer platforms
- Meet requirements for FIPS validation
- Ensure patient confidentiality (HIPAA)
- Maintain maximum availability of wireless network
- Provide transparent operation for users

Solution

- Bar Code Medication Application (BCMA)
- Mobile devices running Windows® 2000 Professional, Windows 95 or Windows XP
- Fortress Security Gateways
- Fortress Management and Policy Server
- Fortress Secure Clients

Results

- Fortress's overlay security model integrates with all existing technologies and equipment
- FIPS validated security in place for wireless network
- Failover provided for redundancy on the wireless network
- User experience remains unchanged
- Leading Healthcare application kept alive with secure wireless



For more information about the Fortress product suite for Federal Government:

phone: 813.288.7388

visit: www.fortresstech.com

email: info@fortresstech.com

Fortress Technologies Inc.
4023 Tampa Rd., Ste. 2000
Oldsmar, FL 34677