



CASE STUDY WIRELESS SECURITY

TACTICAL NETWORKS

U.S. Army Deploys Wireless for Secure Combat Information Systems

Wireless Security Vital for Sensitive Battlefield Communications

Benefits

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



Today's military relies on mobility and operational flexibility. To further enhance the agility of troop and supply movement, Army logistics specialists have deployed wireless networks that link all the units responsible for providing resources that support the frontline. The U.S. Army is mindful of the inherent risks associated with wireless networking, and nowhere is the threat of intrusions, intercepted communications or network downtime more serious than when dealing with battlefield communications. The lack of physical boundaries and the mobility of wireless users create new security challenges for the Army's information technology managers.

The U.S. Army's equivalent of a corporate supply chain is the Combat Service Support Automated Information System Interface (CAISI). CAISI is a tactical wireless LAN that serves as the "last mile" and is a vital link in supplying soldiers with the equipment and supplies needed to stay equipped, in touch and on the move. Traditional wired networks, or relying on messengers to share supply information to central command, was time consuming, prone to errors and did not provide real-time supply information. The agility provided by wireless networks allows work that used to take hours to be done in minutes.

CAISI serves as a connection to an ever-changing cluster of warehouses and command facilities on the battlefield. If a vehicle needs to be repaired on the battlefield, the parts can be ordered via the CAISI wireless LAN and can be deployed in a truly

responsive fashion from a tent or from the back of a truck.

Vulnerabilities of Wireless Networking

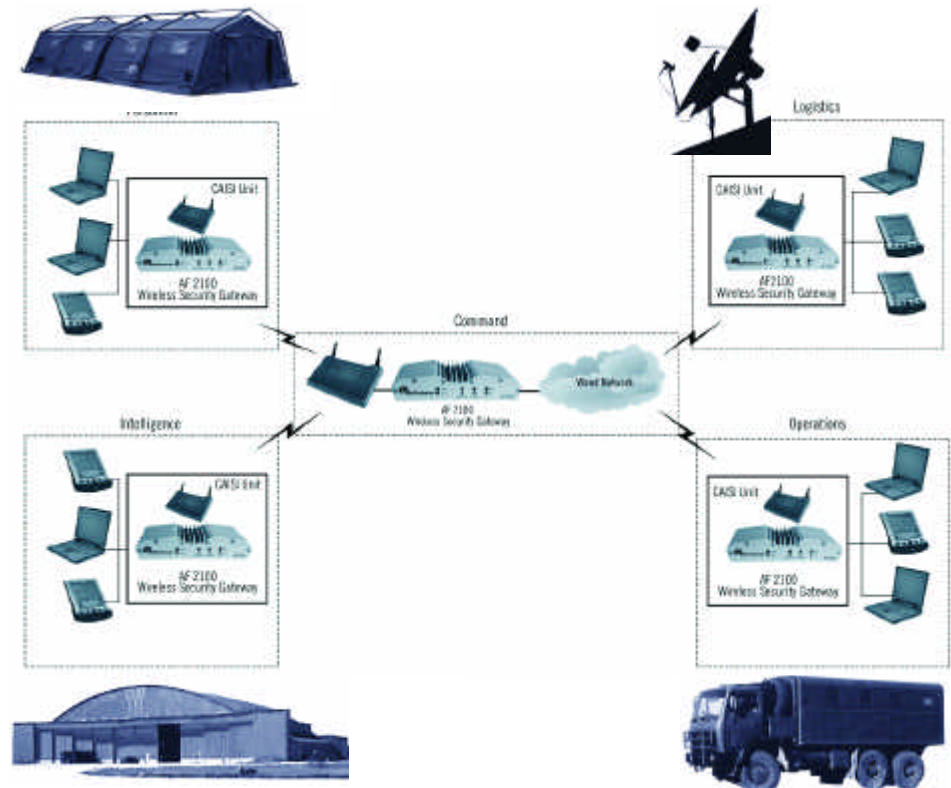
The Army ruled out relying on Wired Equivalent Privacy (WEP) for wireless encryption because of the well-known vulnerabilities associated with it. WEP is typically integrated into wireless access points and NICs by the vendor. Even using rotating key schemes that attempt to reduce the vulnerabilities of WEP was not an acceptable solution because of potential bandwidth consumption of frequent key exchanges. IPSec also couldn't meet the Army's requirements. IPSec, which was developed for use on wired networks, adds an administrative burden as well as overhead to network communications. More importantly, IPSec does not protect vital information such as IP addresses and certain broadcast traffic that can be used by hackers to exploit or deny service to a wireless network. What the Army needed was a low latency solution that was quick and easy to deploy, yet secure enough to protect the Army's vital information assets in the most perilous situations.

The Solution: Fortress® Wireless Security Gateways

The U.S. Army selected Fortress Security Gateways to secure their CAISI battlefield logistics application for more than 11,000 wireless access points serving a potential 85,000 users. Fortress is the leading security solution and has been validated by the National Institute of Standards and Technology (NIST) as FIPS 140 vali-

dated for use in the U.S. and Canadian federal governments. Besides its rock-solid security, the Fortress Gateway was also selected for its ease-of-use and the fact that it can be seamlessly integrated into the network.

A typical deployment will consist of a small network of PCs connected by CAT-5 cable to a standard Ethernet hub for each combat unit. Traffic sent to other field units or back to the main network will pass through the hub to the Fortress Gateway where it is encrypted, protecting not just data but also important network information. The traffic is then sent from an off-the-shelf Cisco wireless access point in the tent to an access point on the network edge and decrypted by a Fortress Gateway on the wired network.



AirTight 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. The Fortress Gateway was the first wireless security product to meet the U.S. government's rigorous standards cryptographic security, certified by NIST and the Department of Defense, among others. The Fortress Security Gateway installs seamlessly between access points and the corporate network. One of the unique attributes of the Fortress product is that it can communicate with

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.

Tested & Proven

The Fortress product family is based on the proven protection of Data

Link encryption and Three Factor Authentication™. These measures are integrated into an optimized edge appliance which seamlessly combines all wireless traffic into a managed and secure wireless system. Fortress offers a trusted and easy-to-use security solution that ensures the business integrity demanded by Global 1000 companies, government agencies and healthcare organizations.

Fortress regularly submits its products for rigorous testing of its security and operational integrity to meet the U.S. government's rigorous standards cryptographic security, certified by the National Institute of Standards and Technologies (FIPS 140) and the Department of Defense, among others.

www.fortresstech.com

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



FORTRESSTECHNOLOGIES™