

CASE STUDY Federal Government



Navy Secures Perimeter with Wireless Security Application Model for Homeland Security & Public Safety Applications

Secure Monitoring and Surveillance Systems

The United States Navy has almost 70 bases in the U.S. and several more overseas. Because of increased concern over protecting vital assets and infrastructure including ships, munitions, docks, airstrips and buildings, the Navy needed to implement a monitoring and surveillance system that was both flexible and secure.

Realizing their need for constant surveillance, the Navy deployed sensors and surveillance cameras to monitor and protect infrastructure assets such as bridges, tunnels, airfields and entryways. Wireless surveillance cameras, which are ideal for mobile applications such as police, security and command vehicles as well as stationary assets, proved to be an integral component of the Navy's perimeter security application. Instrumental to operating these cameras is an innovative wireless infrastructure that uses various wireless technologies and a mix of commercially available wireless products.

As part of the Federal Government, Navy networks are mandated to be secure. When government-validated wireless security that would not limit vendor or technology options was required, the Navy turned to Fortress' suite of products to protect communications for its wireless surveillance systems.

Perimeter Security Application Requires Low Latency Solution

By deploying wireless-enabled cameras, the Navy increases security and saves money by not having to run wires to every camera. By selecting Fortress, the Coast Guard was able to implement FIPS-validated security for their wireless networks. Fortress offers a very low latency solution that is well-suited for high-bandwidth data streams sent by video cameras.

The sensitive nature of the Navy's mission requires that extreme care be given to the privacy of any network used to transmit information related to perimeter security. This includes the need to secure data distributed across wireless local area networks as well as to control who can access these networks. The Navy selected the Fortress family of products to protect its wireless perimeter security application because Fortress offers strong FIPS 140-2 validated security that is flexible enough to protect both legacy and future investments in wireless technology.



Challenges

- Provide strong security for surveillance application
- Secure both video cameras and sensor systems
- Meet requirements for FIPS validation
- Provide transparent operation for users

Solution

- Commercially available wireless access points
- Mix of video cameras, sensor systems and mobile computers
- 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
- All applications are supported
- Transparent operation for users
- Perimeter security and surveillance application continues to provide security



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