



WHITE PAPER

**Bringing Secure Communications
Anywhere at Anytime**
Fortress Secure Wireless Communications System
FORTRESS TECHNOLOGIES INC.

Notice

Copyright © 2009 Fortress Technologies, Inc. All rights reserved.

This white paper contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, without written permission of Fortress Technologies, Inc. 4023 Tampa Road, Suite 2000, Oldsmar FL 34677.

FORTRESS TECHNOLOGIES, INC., MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THE INFORMATION IN THIS DOCUMENT.

AirFortress and the Fortress logo are registered trademarks; MaPS, Unified Security Model, Wireless Link Layer Security, Fortress Mesh and Multi-factor Authentication are trademarks of Fortress Technologies, Inc. The technology behind Wireless Link Layer Security™ enjoys U.S. and international patent protection under patent number 5,757,924.

All company names, products, or trademarks mentioned in this document are the property of their respective owners.

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY	4
2 DESIGN.....	6
2.1 FORTRESS ES520 AND SECURE CLIENT – PLATFORM DESIGN	6
2.1.1 <i>Radio Technology</i>	7
2.1.2 <i>Fortress Mesh</i>	8
2.1.3 <i>Security</i>	10
2.1.4 <i>Hardware – Physical Attributes</i>	12
2.1.5 <i>Configuration</i>	13
3 APPLICABILITY.....	14
3.1 POLICY COMPLIANCE	14
3.2 PAST PERFORMANCE	15
3.3 SUMMARY	16

1 Executive Summary

With a solid history of delivering reliable, policy-compliant solutions that are rugged, proven, and easily deployed, Fortress has established itself as a clear leader in secure wireless networking. Across the public sector, both military and civilian customers rely on Fortress to securely deliver mission related information that supports critical decision making, situational awareness and force protection.

Fortress products extend the reach of networks with industry-leading wireless and security technologies, bringing applications and information to those who need it, when and where they need it. Currently deployed in some of the world's most demanding environments, Fortress products support vital operations that rely on secure, high performance deployable networking, outdoor network extensions and vehicle based networking.

Whether the need is to get real-time logistics information to a forward area, to provide streaming video, voice and data to soldiers on the move, or to securely extend the reach of outdoor networks, gaining operational efficiencies through wireless networking technologies is an imperative for forward looking organizations. These solutions require wireless communications at the edge of the network that offer the best performance in terms of radio range, throughput and reliability.

Any solution must be balanced by the need for security appropriate for the specific threat environment in which it operates. In many cases these solutions must comply with strict government guidelines in both civilian and military organizations such as those within the Department of Defense (DoD). Fortress satisfies this demand while ensuring that security policies and best practices are met by integrating strong, policy compliant security into communications products that are designed to operate in harsh environments.

Fortress products were designed from the ground up to create a versatile wireless communications platform that government customers can rely on in a wide range of applications. The design centered on customer requirements for maximum wireless range, broadband performance, network resilience and policy compliant security in an integrated and rugged solution.

Supporting soldiers, officers and agents in the field is challenging. Whether it is border control agents, first responders or the lower echelon battle command, supporting the "tactical edge", requires true innovation. Today's centralized hub and spoke architecture simply doesn't meet the communication needs of our military, law enforcement and first responders. Fortress' approach integrates numerous technologies and capabilities into a single communication platform built on a secure peer-to-peer architecture. Fortress utilizes its Fortress Mesh technology to create wireless networks with self-forming, self-healing, path-optimizing capabilities that can support thousands of wireless mesh nodes in a highly mobile network. To accomplish this, Fortress Mesh incorporates both proactive and reactive routing algorithms into a layer 2 meshing protocol that requires less than 5% of the bandwidth for control traffic regardless of the network size. In addition, Fortress has implemented FIPS certified Layer 2 AES encryption to protect both the data in transit and the network itself, complying with the various government wireless and security policies. Fortress has

implemented these technologies into both wireless infrastructure, such as the ES520 Secure Wireless Bridge, and client software products.

The Fortress ES520 Secure Wireless Bridge enables organizations to rapidly establish a high-performance wireless mesh network by combining the functions of an access point, switch, wireless bridge and security gateway in a form factor engineered specifically for harsh outdoor environments. The ES520 weighs less than 5 lbs and uses less than 12 watts of power while providing superior performance in distance and throughput. Coupled with industry leading client support, Fortress offers an end-to-end solution that supports robust communications from the vehicle to the warfighter or first responder under high tempo mobility.

Fortress has extensive experience providing tactical wireless solutions that provide broadband quality networking (voice, video and data) in environments where there is little or no centralized control, no available infrastructure and no reliance on aerial relay nodes. Fortress products are currently deployed in many of the world's most demanding environments. The U.S. Army selected Fortress to provide secure wireless communications for the largest installed and operational wireless network in DoD. The Texas National Guard is relying on next generation "Rapid Response Communications Kits" from Fortress to quickly establish communications in dynamic environments which have no existing infrastructure. Supporting operations in these environments has required an innovative and integrated approach.

2 Design

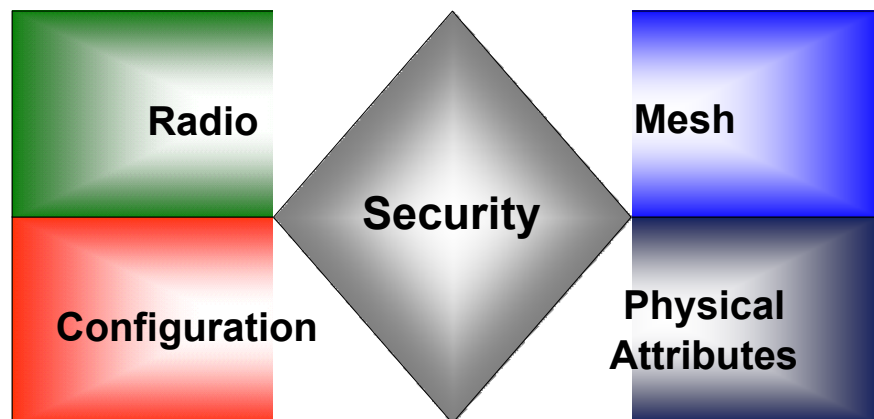
2.1 Fortress – Platform Design

The Fortress Secure Wireless Bridges was designed from the ground up to be a highly integrated and versatile wireless communications platform that our government customers could rely on in fixed, portable or mobile environments. The design centered on our customers' needs for Maximum RF Range, Broadband Performance, Network Resilience and Security in a solution that could rapidly be deployed in harsh environments across dynamic network topologies. The platform philosophy allows for flexible integration of a number of applications. Interoperability and Federal policy compliance are additional design criteria persistent throughout the development life cycle.

The Fortress Secure Wireless Bridge enables organizations to rapidly establish a high-performance wireless mesh network by combining the functions of an access point, switch, wireless bridge and security gateway in a form factor engineered specifically for harsh outdoor environments.

There are five main attributes of the Fortress Secure Wireless Bridge are:

1. Radio Technology
2. Meshing Architecture
3. Security Capabilities
4. Physical Attributes
5. Flexible Configuration



These attributes in the Fortress Secure Wireless Bridge, along with the broad client support, work seamlessly to create an end-to-end solution that supports challenging deployment environments.

This section describes the design methodology used to implement the five design attributes outlined above. Some of the features described in this section are planned features, and some features are optional in the operation of the product.

2.1.1 Radio Technology

Radio performance is perhaps the most visible attribute of the Fortress Secure Wireless Bridge. The Fortress Secure Wireless Bridge LOS performance using omni-directional antennas allows use of the product in true mesh and ad-hoc configurations without reliance on directional antennas which limit such configurations.

The table below shows the radio performance of the ES520 Fortress Secure Wireless Bridge in the 5.8GHz frequency band (802.11a) for a variety of antennas and LOS distances. All results are obtained using 400mW radios and without the use of any external amplifiers.

Radio Technology design methodology of the ES520:

- ✓ **Provides the highest throughput and range** by utilizing the best radios available, combined with a high quality PCB design to reduce noise which provides industry leading radio performance. Not only does the low level optimization done at the MAC and PHY level result in greater radio sensitivity, the ES520 is very light and pole-mountable to decrease signal loss through cables.
- ✓ **Uses standard socket interfaces** to allow for best of breed COTS, semi-custom and full custom radio design. This flexibility allows the ES520 to keep up with the rapidly-changing radio technologies and support customer-specific configurations of radios.
- ✓ **Aggressively follows radio technology** using standard and custom radio designs. This radio technology roadmap includes 802.11n multiple-input multiple-output (MIMO), 4.9GHz Wi-Fi and WiMAX.

Distance (miles)	User Throughput (Mbps)	Antennas	Cable Length (feet)
1.0	21	9dBi Omni + 9dBi Omni	2
2.8	11.8	9dBi Omni + 9dBi Omni	2
7.0	8.5	9dBi Omni + 12dBi Omni	2

* These are average range distances based on actual field tests performed by Fortress during ideal environmental conditions with minimal interference from both manmade and natural objects.

2.1.2 Fortress Mesh

The ES520 supports mesh networking technology which provides the self-forming and self-healing capabilities core to any mesh architecture. Fortress Mesh supports fixed infrastructure or portable networks where the infrastructure is relatively static, and is also designed to support large, dynamic networks with more emphasis on mobility and scalability. Fortress Mesh also offers significant advantages in terms of scalability and resiliency, which is particularly important in highly mobile environments.

Fortress Mesh possess attributes of scalability, mobility, low overhead and dynamic self-configuration and self-administration that are unique.

Fortress Mesh supports:

- ✓ Large scale networks
- ✓ Highly mobile networks - including 'fast mover' nodes
- ✓ Extremely low bandwidth networks
- ✓ Networks spanning vehicles, and fixed wired installations

All current self forming, self-healing networks are extremely limited in size and their ability to organize mobile networks. This fundamental problem exists because the amount of control bandwidth required to keep the network 'whole' grows at an exponential rate with network size. This means that by the time even a small mesh network is deployed it requires all of the available bandwidth just to maintain itself.

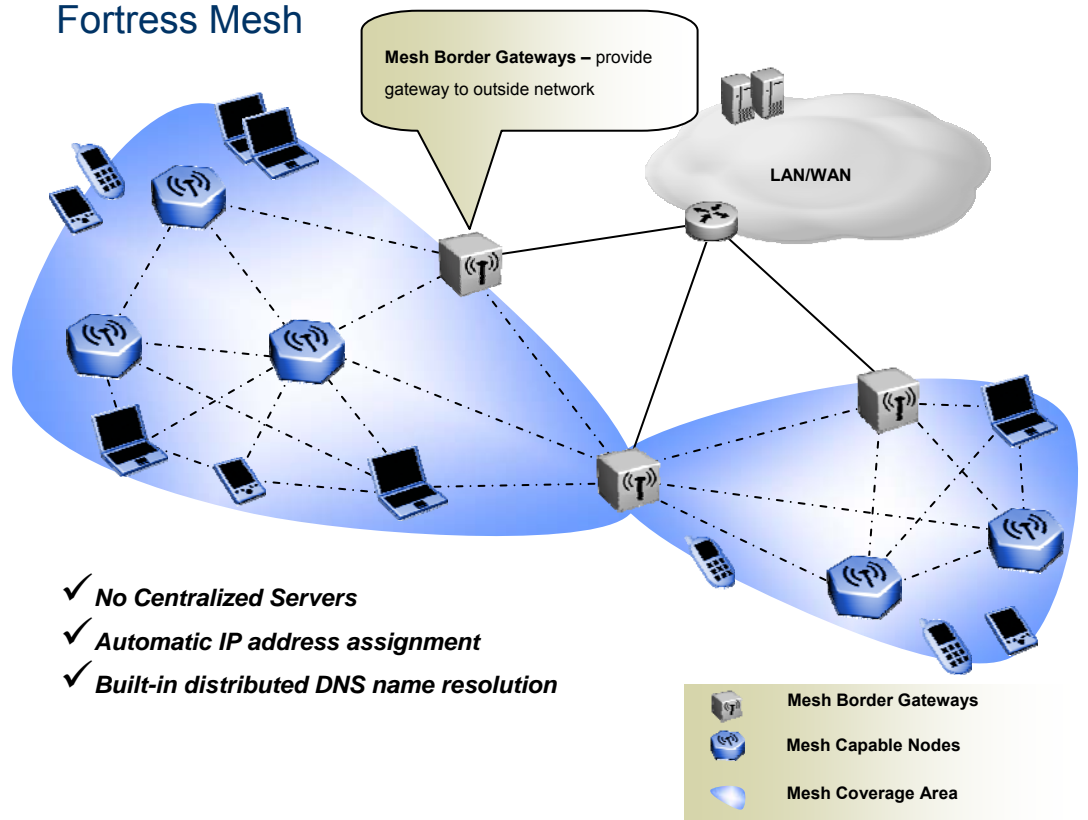
Fortress Mesh overcomes this serious problem. Regardless of network size, or network bandwidth Fortress Mesh will use less than 5% of available bandwidth.

Category	Fortress Mesh	All Other Approaches
Maximum network size	Highly scalable	Limited
Mobility support	Highly mobile networks are fully supported	Limited mobility support only
Control bandwidth	Low percentage of network bandwidth	Exponential with network size.
Low capacity nodes	Fully Supported	No
Network partitioning required to allow scaling	No	Yes
The same algorithm runs on all devices	Yes	Only very small networks
End to End Encryption	Yes	No
Multicast Optimizations	Yes	No

Fortress Mesh features are well suited for highly mobile tactical edge environments because of the following attributes:

- ✓ **Scalability** – Fortress Mesh is designed to support thousands of nodes and an equally large network diameter. Fortress Mesh is designed from the ground up for large mesh networks and incorporates both proactive and reactive routing algorithms. Proactive algorithms are necessary to sustain a high level of mobility, while reactive protocols are utilized to support very large networks.
- ✓ **Enhanced Network Mobility** – Fortress Mesh supports automatic configuration of IP addresses and distribution of node names without reliance on any centralized server such as DNS or DHCP. This is critical to supporting a large resilient mobile network.
- ✓ **Administrative Flexibility** – Fortress Mesh provides significant enhancements to support highly efficient multicast mechanisms. In addition, network segregation allows the network operator to segment the network into multiple administrative domains to put better control mechanisms in place.

Fortress Mesh



2.1.3 Security

The ES520 builds upon Fortress' extensive experience in providing policy compliant security products to the government for over a decade. The ES520 and Fortress Secure Clients incorporate a multi-layer security architecture critical to ensure the protection of the network and communication. The Fortress security foundation is built-on a Layer 2 peer-to-peer architecture which adheres to the Federal Government's stringent security policies. Another compelling aspect of Fortress Security is that as a Layer 2 protocol, it supports and works across Layer 2 mesh architectures.

Multiple layers of security:

- ✓ Encryption
 - NIST FIPS 140-2 AES 128, 192 & 256
 - IEEE 802.11i (WPA2)
 - Fortress media independent layer-2 Mobile Security Protocol (MSP)
 - Suite B implementation is available as a value-added module
- ✓ Multi-factor Authentication™
 - Network, Device, and User (including DoD Common Access Cards or tokens)
 - Internal or external authentication server including: RADIUS, DoD PKI
- ✓ Rugged, tamper-evident enclosure

Multiple levels of security:

- ✓ Commercial
 - Highest level COTS product available
- ✓ Government
 - Sensitive But Unclassified (SBU) – NIST FIPS validation
 - Classified – Suite B module available. NOTE: Prior NSA approval required for use in classified applications.

All these security standards are built and evaluated against the rigorous FIPS 140-2 Level 2 and Common Criteria WLAN Protection Profile.

The ES520 utilizes advanced security functions which are implemented in a reconfigurable, field upgradeable custom FPGA. This particular implementation, which is unique to the ES520, provides a number of significant advantages including:

- ✓ **Fast cryptography:** high performance AES encryption
- ✓ **Protection against timing attacks:** where the timing of cryptographic operations is data-dependent. Dan Bernstein showed that the AES key is vulnerable to timing attacks using a fairly simple Cache Timing attack.
- ✓ **True Random Number Generator (TRNG):** The cornerstone of good cryptography is the reliance on random numbers. Appliances such as an ES520 have no way to

gather entropy because there is no direct user interaction with the device (such as mouse moves and keyboard input). Thus, for a truly secure implementation, the ES520 includes True Random Number Generators.

- ✓ **Upgradeability:** The ES520 platform built on FPGA technology allows the security subsystem to support emerging security standards with in-field upgrades without compromising the strength of the implementation.
- ✓ **Hardware compression:** The ES520 implements hardware compression before encryption. In addition to the added security benefits, it helps preserve valuable wireless bandwidth. Depending on the data mix, up to a 400% increase in throughput is possible.

2.1.4 Hardware – Physical Attributes

The ES520 Secure Wireless Bridge is designed as a highly integrated, flexible, lightweight and rugged platform designed for harsh environments:

ES520 hardware attributes include the following:

- ✓ Dual radios (support for a third radio)
- ✓ 8x LAN ports, 1x WAN port, USB port and serial port
- ✓ Integrated lightning arrestors, a grounding strap and variable voltage input of 9VDC-36VDC and 48VDC
- ✓ Maximum power draw of 13 Watts
- ✓ Can be powered by Power over Ethernet (POE) and power other devices using POE PSE mode over the 8 LAN ports
- ✓ Lightweight (5lbs) and highly compact (8.8" x 2.66" x 8.22") form factor
- ✓ NEMA-4 and MIL-STD 810F certification
- ✓ Custom design of PCB and enclosure provides higher resilience to power glitches while isolating the radio from unclean power sources.



2.1.5 Configuration

The ES520 Secure Wireless Bridge was designed to support rapid deployment hence significant emphasis and effort was placed on simplifying and automating the configuration:

- ✓ The ES520 utilizes a single user interface to configure a multitude of functions (security, radios, authentication, etc.). This greatly reduces the learning curve for the product.
- ✓ The ES520 securely propagates the configuration from one node to other nodes over both the wired and the wireless interfaces. The operator is able to take new ES520 (slave) units and have these units receive their configuration securely from other nodes (master) in the network without using the CLI or GUI on the slave units. Simultaneous configuration of multiple slave units is also supported.
- ✓ Using the external recessed keys the ES520 can be zeroized to bring it back to a factory-fresh configuration. This affords the operator the flexibility to zeroize the keys for security reasons, or repurpose a box for a different application with little effort.

3 Applicability

3.1 Policy Compliance

The Fortress ES520 Secure Wireless Bridge platform is compliant with the DoD 8100.2 Directive for wireless security. The table below outlines key policy components and how Fortress addresses them:

DOD 8100.2 Policy Directive and Fortress ES520 Secure Wireless Bridge

Policy Element	Fortress Policy Element Description	Meets Policy Directive (√)
802.11i	Fortress has validated the ES520 is interoperable with standards-based 802.11i clients	√
FIPS 140-2	Fortress has leveraged its media independent FIPS validated crypto modules for integration into the ES520	√
Authentication	The ES520 platform provides standards-based 802.1x port based authentication and allows for easy integration with RADIUS and DOD CAC PKI based on EAP-TLS protocol	√
Common Criteria	Submitted for Common Criteria EAL 4	√

3.2 Past Performance

Fortress has provided secure wireless network devices for a wide variety of applications including:

- ✓ **Battlefield Support** – U.S. Army CAISI (largest installed and operational wireless network in DoD)
- ✓ **Tactical Edge** – Marine Corps (Afghanistan) 802.16/802.11
- ✓ **Rapid Response Communications Kits** – National Guard, South Carolina National Guard
- ✓ **Mobile “Go-Kits”** – Department of Homeland Security (FEMA)
- ✓ **Wireless Infrastructure** – Joint Forces Command
- ✓ **Outdoor Wireless Reachback** – Marine Corps
- ✓ **Perimeter Security** – U.S. Air Force
- ✓ **Secure Mobility for Maintenance & Logistics** – U.S. Air Force SATS Project
- ✓ **Defense Medical Logistics Support (DMLSS)** – U.S. Navy, U.S. Army, U.S. Air Force
- ✓ **Engineering Logistics Center** – U.S. Coast Guard, DHS
- ✓ **Patient Care and Medication Tracking** – Veterans Administration, VHA & VBA wide deployment
- ✓ **Wireless LAN Security** – U.S. Army Reserve
- ✓ **Outdoor Mesh NIPRNET access** – U.S. Air Force
- ✓ **Building to Building Connectivity** – U.S. Air Force

3.3 Summary

With a solid history of delivering reliable, policy-compliant solutions that are rugged, proven, and easily deployed, Fortress has established itself as a clear leader in secure wireless networking. Fortress' strong past performance is an indicator of our ongoing commitment to excellence.

Fortress solutions are designed for the tactical edge to support the needs of the warfighters and first responders. Meeting our customer's operational requirements in these environments required applying a new approach to wireless network technologies, design and architectures. Fortress' solutions address our customer's needs for Maximum RF Range, Broadband Performance, Network Resilience and High Assurance Security in a solution that could rapidly be deployed in harsh environments across dynamic network topologies.

The Fortress approach creates an end-to-end solution that addresses the need for secure, scalable, high-performance, robust communications in the field. The Fortress solution provides the following key attributes:

- ✓ **RF Range** – Field tested over 7 miles with omni-directional and 32 miles with directional antennas
- ✓ **Throughput** – Supports up to 40Mbps with AES-256 encryption
- ✓ **Fortress Mesh** – self-forming, self-healing and path optimization allows for scalable dynamic network topologies which include highly mobile nodes
- ✓ **ES520 Hardware Design** – 5 lbs, variable power (9vdc – 48vdc), NEMA-4 certified, MIL-STD 810F
- ✓ **Security** – FIPS Layer 2 AES-256 encryption, TRNG and protection against timing attacks – a solution designed to be DoD policy compliant
- ✓ **Modularity** – The ES520 can incorporate additional types of radios to meet customer requirements
- ✓ **Media independence** – The ES520 can utilize integrated 802.11 radios or external media including 802.3, 802.16, satellite or other wireless technology

About Fortress Technologies

Fortress Technologies designs, develops and manufactures products that allow our customers to deploy secure wireless networks that comply with stringent government policies. Fortress provides industry-leading security and wireless technologies that extend the reach of networks, bringing applications and information to those who need it, when and where they need it. Fortress enables immediate “on demand” secure voice, video and data communications virtually anywhere and across all wired or wireless transports including Wi-Fi (802.11), WiMAX (802.16), free space optics (FSO) and Military RF. Fortress products are currently deployed in some of the world’s most demanding environments, supporting vital operations that include deployable communications, disaster recovery and continuity of operations (DR COOP), perimeter and border security, outdoor wireless networks, wireless sensor networks, wireless video surveillance and vehicle networks.

For more information, visit www.fortresstech.com or call 813-288-7388.

www.fortresstech.com

CORPORATE HEADQUARTERS

**Fortress Technologies, Inc.
4023 Tampa Road, Suite 2000
Oldsmar, FL 34677**

Phone: 813.288.7388 or
1.888.4Privacy (477.4822)



© 2009 Fortress Technologies Inc. All rights reserved
