



Security & Management for Wireless Networks

Architecture White Paper



Notice

Copyright © 2004 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 AirFortress logo are registered trademarks; the Fortress Technologies corporate logo, Unified Security Model, Wireless Link Layer Security and Three Factor Authentication (TFA) 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.

Copyright © 2004, PalmSource, Inc. PalmSource, Palm OS, Palm Powered, Palm, HotSync and certain other trademarks and logos appearing on this website, are trademarks or registered trademarks of PalmSource, Inc. or its affiliates in the United States, France, Germany, Japan, the United Kingdom, and other countries. These marks may not be used in connection with any product or service that does not belong to PalmSource, Inc. (except as expressly permitted by a license with PalmSource, Inc.), in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits PalmSource, Inc., its licensor, its subsidiaries or affiliates. Other brands used herein may be trademarks of their respective owners. While all content is believed to be correct at the time of publication, it is provided solely for general-purpose information. The content, including without limitation, descriptions of third party products, features, functions or specifications, is supplied "As-Is" and with no express or implied warranties whatsoever made by PalmSource, Inc. or its third party suppliers or licensees, including but not limited to warranty for accuracy, merchantability, fitness for purpose or titles. All other brands and trademarks used herein are or may be trademarks of, and are used to identify other products or services of, their respective owners. All rights reserved.

palmOne and Tungsten are among the trademarks or registered trademarks owned by or exclusively licensed to palmOne, Inc.

Microsoft and Windows are registered trademarks of the Microsoft Corporation.

The SecurID is a registered trademark of RSA Security Inc. in the U.S. and/or other countries.

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

Abstract

Wireless networking introduces new security challenges for the enterprise network administrator or systems integrator. Efforts to address these unique challenges and inherent vulnerabilities have spawned much debate in the industry. At odds are approaches that implement security at different layers of the OSI networking model - Layers 2, 3 or higher. From the initial work on wireless security and the continued design efforts of the IEEE, clearly Layer 2, the Data Link Layer, is the appropriate point for integrating security into a network. This white paper discusses the advantages of Data Link Security and how by providing a mix of cryptography, access control and authentication methods, Fortress Technologies' AirFortress architecture provides the most comprehensive and robust approach for securing wireless networks.

Table of Contents

I. Executive Overview.....	1
II. Product Overview of AirFortress Solution.....	1
a. AirFortress Family of Wireless Security Gateways.....	3
b. AirFortress Access Control Server (ACS).....	3
c. AirFortress Secure Client.....	4
d. AirFortress Secure Client Supported Devices.....	4
III. Security Architecture of AirFortress Solution.....	5
a. Data and Network Privacy.....	5
b. Three Factor Authentication (TFA).....	5
c. Strong Protection and Policy Control.....	6
1. Strength of AirFortress Architecture.....	6
2. AirFortress Encryption.....	6
3. Device Authentication.....	6
4. Optimized Security Mechanism.....	7
IV. Benefits of AirFortress Architecture.....	9
V. Conclusion.....	10

I. Executive Overview

The off-the-shelf security bundled with wireless equipped laptops, PDAs and network devices may seem to provide adequate protection, but for the enterprise environment the security risks of wireless networking mandate a greater level of protection and manageability than provided by these consumer-grade security solutions. Generic solutions, such as WPA or TKIP, address basic security issues for the average small business or home office user. However, these incremental fixes are based on weak components and are only meant as a temporary solution to keep the WiFi market adoption from stalling due to security concerns. The IEEE-endorsed solution for improved wireless security (802.11i) still only addresses a portion of the market. More sophisticated wireless systems or those protecting sensitive information require a stronger and more comprehensive security model that supports a broad range of devices and security policies. A one-size-fits-all technology decree cannot address the flexibility required to satisfy the numerous regulatory policies or the wide range of network systems configurations.

By striking a balance between protecting critical elements of the wireless network and providing flexible management of wireless users and devices, Fortress Technologies has designed a security and management architecture that is easy to implement yet able to meet the industry's most stringent standards. The AirFortress products integrate features such as a robust key exchange mechanism, strong data encryption, support for EAP authentication and the ability to maintain multiple vendors' equipment in a heterogeneous environment. The AirFortress product family is the most successful wireless security platform available today and has been chosen by some of the world's leading adopters of wireless LANs. The U.S. Army, U.S. Air Force, VA Hospitals, Defense Commissary Agency, and other large customers all have the AirFortress products deployed to protect their wireless LANs.

Much has been written about the risks inherent in wireless networking and the strengths or weaknesses of the various security technologies. This paper does not rehash these topics, but instead it focuses only on Fortress Technologies' approach to providing a comprehensive system for multi-vendor, multi-platform wireless network and device security. It describes in detail the motivation behind the design and the basic architectural components of the AirFortress product line.

II. Product Overview of AirFortress Solution

The AirFortress product family draws on Fortress Technologies extensive network security experience and long track record of producing Federal Information Processing Standard (FIPS) validated security products. By incorporating proven technologies and methods to provide superior privacy, access control, authentication and data integrity, Fortress Technologies delivers reliable, robust security and management specifically designed for enterprise wireless networks.

The AirFortress product family comprises three main components: the AirFortress Wireless Security Gateway, the AirFortress Secure Client and the AirFortress Access Control Server.

**AirFortress®
Product Family**

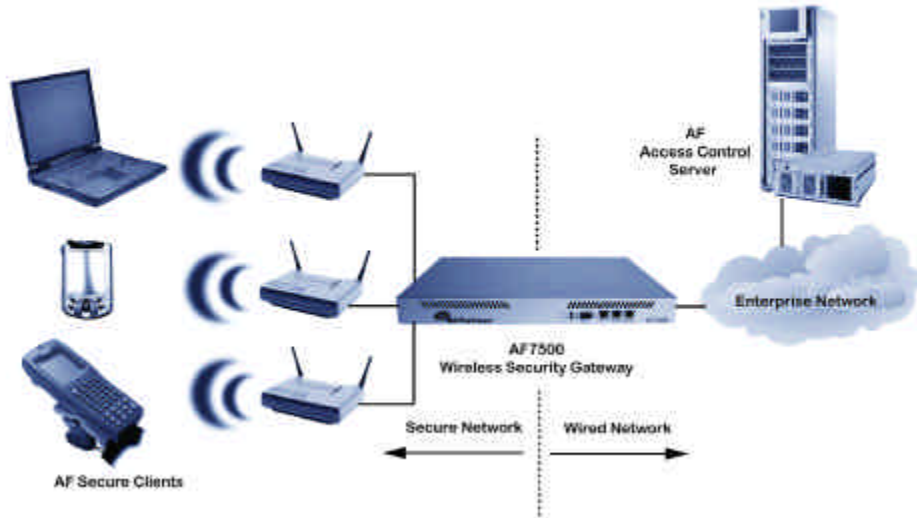
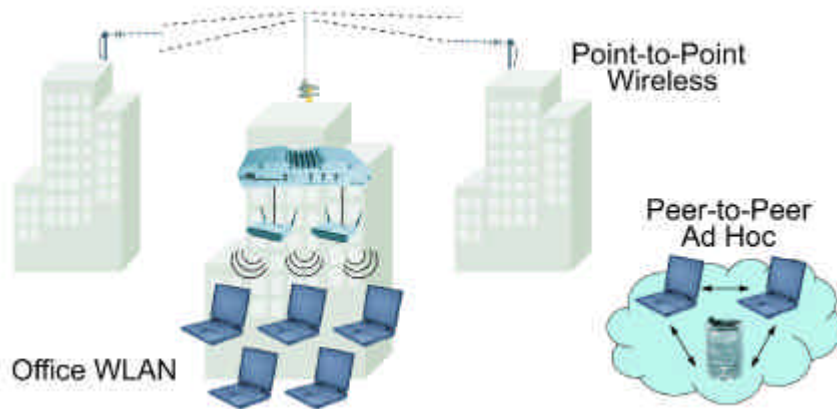


Diagram of Generic LAN Topology

The AirFortress system can also be used to secure point-to-point wireless links such those found on corporate campuses, large healthcare facilities, military bases or building-to-building bridges like those found in metropolitan area networks.

Point-to-Point



a. AirFortress Family of Wireless Security Gateways

The AirFortress Wireless Security Gateway is a network infrastructure appliance that provides a secure edge to the corporate network by allowing only protected communications between wireless devices and the rest of the network.

Designed to install easily into a mixed vendor environment, the AF device sits between the access points at the edge of the LAN and the internal wired network. Not to be confused with Layer 3 gateways or routing devices, the AirFortress Gateway is a Layer 2 bridge that easily integrates in a wide variety of environments without time-consuming reconfiguration of the existing LANs.

The AirFortress Wireless Security Gateways are available in two models:

The **AF2100** provides a small form factor that can be installed on a shelf next to an AP or mounted in a remote wiring closet. This platform is suited for small installations or networks where a distributed campus approach is more appropriate. A single **AF2100** can provide security with no noticeable degradation for up to 50 simultaneous wireless devices (PCs, PDAs or handheld scanners) depending on the applications and overall bandwidth usage. Access points are likely to reach their maximum throughput well before the AirFortress Wireless Security Gateway reaches saturation.

The **AF7500** is designed for large scale wireless LAN deployments where a central facility is available to accommodate a rack mounted chassis. The larger enterprise-grade **AF7500** can protect an even greater number of users spread throughout a large office building, campus or military compound. This appliance provides the greatest flexibility for centrally managing and growing an enterprise wireless LAN. Both the **AF2100** and the **AF7500** can be configured in failover pairs to provide continuity of service for high availability environments.

b. AirFortress Access Control Server

Wireless security is only as good as the policies and controls that are actively managed as part of the overall solution. The AirFortress Access Control Server (ACS) is a high-performance, highly scalable user and device access control platform for coordinating wireless authentication and policy management. The ACS offers centralized command and control for wireless LANs from a browser-based interface that provides administrators with a full view of policies, parameters and usage. With Fortress Technologies' unique Three Factor Authentication™ (TFA) enabled, the device authentication capability allows specific devices to be granted or denied access regardless of user credentials. The AirFortress ACS manages policies as a standalone service or in conjunction with commonly used authentication and directory services deployed in the enterprise. Using the Extensible Authentication Protocol (EAP) and integrated support for NT Domains, Active Directory Service, RADIUS, RSA SecurID or LDAP make the AirFortress ACS a seamless extension to existing network administration and corporate infrastructure.

c. AirFortress Secure Client

Fortress Technologies believes that protecting the device is as important as protecting the network and the data. Corporate laptops and PDAs often contain sensitive intellectual property. Activating wireless can expose the information on these devices to ad-hoc attacks and port scanning. Serious damage can be inflicted on a single device without ever infiltrating the corporate side of the wireless LAN. Some competing security products recommend treating all wireless devices as hostile and focus security strictly on the protection of the LAN using a makeshift assortment of firewall and VPN technologies. This approach is flawed and leaves important assets vulnerable to ad-hoc intrusion. By including the client as a secured component of the wireless LAN, Fortress Technologies creates a trusted relationship between the client device and internal corporate systems.

The AirFortress Secure Client is a lightweight software client module for laptops, PDAs, tablet PCs, thin client devices and industrial equipment such as barcode scanners and portable terminals. Fortress Technologies continues to leverage its partnerships with leading device manufacturers and operating system vendors to provide the broadest array of support for commonly used devices in the enterprise, healthcare and industrial markets. The chart below indicates the breadth of client coverage available on the AirFortress platform.

The AF Secure Client has an extremely small resource footprint, yet there are devices that are unable to accommodate an additional client. Specialized devices such as wireless IP phones, printers, industrial scales, and so forth, can be included as part of the AirFortress network and managed side-by-side with full feature Secure Clients.

AirFortress Secure Client Supported Devices

Enterprise Devices	<i>Windows</i>	<i>CE, CE.Net</i>	<i>Palm*</i>	<i>DOS</i>	<i>Linux</i>
<i>PCs, Laptops, Tablets</i>	●	●		●	●
<i>PDAs</i>		●	●		
Specialized Devices	<i>Windows</i>	<i>CE, CE.Net</i>	<i>Palm</i>	<i>DOS</i>	<i>Linux</i>
<i>Acute Network Technologies</i>		●			
<i>AirSpeak</i>		●			
<i>Neoware</i>		●			
<i>TeleVideo</i>		●			
<i>Wyse</i>		●			
Ruggedized Devices	<i>Windows</i>	<i>CE, CE.Net</i>	<i>Palm</i>	<i>DOS</i>	<i>Linux</i>
<i>HHP</i>		●		●	
<i>Intermec</i>	●	●		●	
<i>LXE</i>	●	●		●	
<i>Psion-Teklogix</i>	●	●		●	
<i>Symbol</i>		●	●	●	

*Tungsten C

III. Advantages of Data Link Security

AirFortress' *wireless* Link Layer Security (wLLS) architecture is independent of the physical and MAC layer allowing the system to function across a broad range of network systems including all 802.11 and most 802.16 point-to-point network systems. It is also independent of data flow above Layer 2 allowing it to support all network or application specific protocols. By implementing a security scheme that resides at the Data Link Layer the system secures the protocol, frame and packet transmissions that other systems leave exposed. A true Layer 2 solution the AirFortress security solution provides seamless integration into any current or future network topology. The following sections detail the components that makeup the security and management features of the AirFortress security solution.

a. Data and Network Privacy

- **Frame Masking** hides header, computer name, protocol and other vulnerable information.
- **Frame Authentication** ensures integrity, preventing session hijacking.
- **Payload Compression** disguises original length of frame and its contents to combat analytical and brute force attacks.
- **Dynamic per Session Keys** are generated using an encrypted dual Diffie-Hellman key exchange to prevent man-in-the-middle attacks and spoofing.
- **Encryption of ARP** packets and unique bridging design prevents ARP poisoning attacks.
- **Replay Protection** guards against data being captured and then being re-injected into the network after it has been compromised.

b. Three Factor Authentication

Three Factor Authentication (TFA) is a pioneering approach to multi-tiered network authentication for wireless enterprises. The three factor approach, unique to Fortress Technologies' AirFortress wireless security solution, enforces secure access at the network, device and user levels.

- **Access ID** used for mutual authentication and prevents unauthorized clients and intruders from initiating a key exchange with the Gateway. Access IDs are the first stage of TFA enforcing controlled access to the network.
- **Device ID** is a unique, non-duplicable, hardware identifier, which is used to distinguish devices protected by the AirFortress Secure Client. The Device ID is automatically generated and bound to a specific device to prevent spoofing.
- **User ID** is the final stage of TFA ensuring that the user presents valid credentials to the system prior to gaining network access.

The diagram illustrates the relations and sequence used in Three Factor Authentication



c. Strong Protection and Policy Control

AirFortress enforces a closed architecture design but supports heterogeneous multi-vendor devices. This design delivers the protection of a firewall without the complexity.

1. Strength of AirFortress Architecture

AirFortress protects data in an IEEE 802.11 frame with a strong encryption and mutual authentication process. The modular design of AirFortress' components results in a much smaller footprint when compared to other client-side VPN utilities or network supplicants. This computationally light design allows the Secure Client to be easily integrated onto many wireless devices or network infrastructure platforms that other technologies could never secure. AirFortress uses recognized encryption algorithms (AES and 3DES) and a dual Diffie-Hellman key exchange to automatically build and maintain security associations. Keys are dynamically generated, which cuts down on system overhead and improves the overall efficiency of this approach versus others more computationally intensive methods. All components used in the AirFortress architecture, including the data hashing algorithm used to provide integrity checking and support for device authentication capability, meet the requirements for FIPS validation.

Data link security protects the communication on the LAN and in the air, but the value of the AirFortress solution is in how Fortress Technologies has integrated technologies behind the scenes to make the AirFortress solution a robust, yet easy to implement security framework. The following design summary explains the various components of AirFortress' architecture.

2. AirFortress Encryption

AirFortress implements cryptographic processes automatically, without direct intervention of the operator except for the initial configuration of parameters such as a unique Access ID. The system provides secure establishment of keys, use of proven cryptographic algorithms (also FIPS approved), efficient processing, and ease of deployment, all with a minimal amount of system administration. Fortress Technologies provides all three NIST approved key lengths of AES (128, 192, 256). This is an important element of the strength and flexibility of the AirFortress system and allows highly sensitive systems environments to achieve an unprecedented level of security.

3. Device Authentication

The Device ID is a unique, system-generated value created for each AirFortress-protected device to ensure that only authorized devices are allowed to connect to a protected network. This ID cannot be copied, modified or spoofed. If a rogue device attempts to masquerade as an authorized device by using the MAC address derived from a known device, the exchange of traffic will be prevented because the unrecognized device will not have correct a Device ID.

4. Optimized Security Mechanism

A central component of AirFortress' efficiency advantage is its key exchange mechanism. Unlike other security protocols, AirFortress requires only two steps and two transmissions in each direction (four frames total) to complete the key exchange.

Secure Frame Handling

The AirFortress packet handling mechanism manages message fragmentation and provides replay protection.

Integrity and Authentication Checking

A keyed hash is calculated using the header, sequence number and encrypted payload. The recipient uses this hash to check the integrity and authenticity of the packet.

AirFortress Key Exchange

The key exchange process allows two nodes on a network to securely establish a dynamic session key by exchanging messages over an open channel. This key will then be used to exchange private communications between the two nodes during a finite period of time. The key exchange method mutually identifies the two nodes, such that each of them is a valid party for the communications that are to follow. This key exchange method maintains a low communication and computational overhead, minimizing the number of mutual authentication messages exchanged between the two parties.

Anatomy of the Key Establishment and Key Exchange

The AirFortress creates and manages several unique keys:

- **Secret (Hard) Key:** Created using the SHA-1 hash of the unique system attributes.
- **Private and Public Static Key Pair:** Used to create the common static secret key.
- **Private and Public Dynamic Key Pair:** Used to create the dynamic session key parameter for key renegotiation can be set to meet customer policy (maximum 24 hours).
- **Common Static Secret Key:** After the initial key negotiation, the static key is used instead of the hard key to generate dynamic session keys for all subsequent transmissions. This key is common to both nodes, eliminating any possibility that another device can impersonate a valid node.
- **Dynamic Session Key:** Encrypts data packets exchanged between nodes.

The Access ID is a 16-digit hexadecimal value chosen by the system administrator, ensuring that keys are unique to a given network.

Private keys are produced using an ANSI X9.31 random number generator as well as device-specific parameters to ensure uniqueness and strength. Public keys are generated using the Diffie-Hellman protocol as defined in the following section.

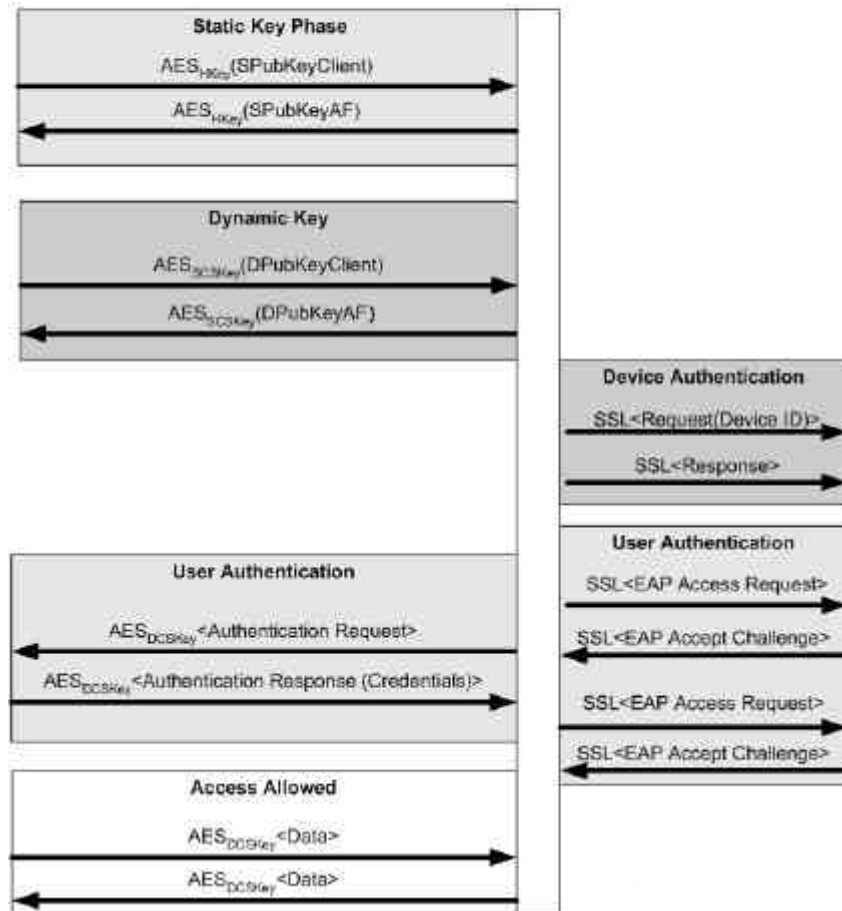
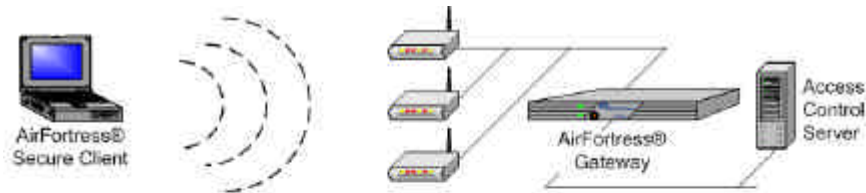
Key Generation Process

The two static keys are negotiated when the AirFortress Secure Client or Gateway is initially powered on. The common static secret key and the dynamic session key are negotiated only when two AirFortress-secured devices initiate a connection.

Key Negotiation

Only two secured nodes using the same Access ID can establish common secret keys. AirFortress uses two successive, Diffie-Hellman encrypted key exchanges to complete key negotiation between two nodes. After power-up, each device possesses a hard key, private and public static keys and private and public dynamic keys. The dynamic keys piggy-back on existing transmissions and do not generate their own unique traffic for the purpose of key exchanges.

Diagram of Key Negotiation



Key Protection

To protect transmission of keys during the authentication process, the dual Diffie-Hellman exchange is used to ensure that the public key exchange cannot be compromised or intercepted. Further, to protect the integrity of the keys, the actual session key determined by encrypt data is never transmitted and is generated by internal calculations within the end-points. These private keys never leave the module and are newly generated each time the AirFortress device initiates a session and at each rekey interval.

The Diffie-Hellman public key exchange protocol provides secure distribution of a common secret key between two nodes of a network (secure from passive attacks, such as eavesdropping). However, unlike the generic Diffie-Hellman key agreement method that has proven to be vulnerable against attacks that intercept, modify, or inject messages, (commonly referred to as "man-in-the-middle" attacks) the AirFortress solution performs a secondary Diffie-Hellman key exchange using dynamically generated public keys. This dual Diffie-Hellman key exchange produces a dynamic session key that is an exclusive common property of the two communicating nodes. This eliminates all known Diffie-Hellman vulnerabilities.

4. Benefits of AirFortress Architecture

- Highly secure in all wireless and mobile environments using industry standard encryption protocols, FIPS-validated implementations of AES and 3DES
- Small footprint supports easy integration with a broad range of devices, NIC cards, access points and specialized industrial devices.
- Data Link Layer works with any IEEE 802 Media Access Control wireless communications protocols such as 802.11a, b or g LANs, 802.16 WAN or any environment that operates using a standard Ethernet transceiver or bridge
- Data compression used to defeat statistical attacks also provides improved throughput
- FIPS validation is platform-independent, allowing broad OEM integration capabilities
- EAP-compliant user authentication will work with any standard EAP authentication
- Easy to install Layer 2 passthrough device requiring no change of IP addressing scheme or reconfiguration of existing network topology.

Customer feedback indicates the following three key advantages are the primary incentive behind the AirFortress' wide acceptance in both government and commercial systems:

a. Ease of Use

Strong security does not have to be difficult to implement and maintain. The AirFortress solution efficiently manages the critical security and management issues associated with wireless networking such as access control, authentication (device and user) and device roaming between access points. By automating the key exchange and all supporting cryptographic processing, the AirFortress security solution operates with little user intervention, reducing setup and management requirements for already overburdened system administrators. Since AirFortress provides a Layer 2 security, it is protocol agnostic, enabling deployment with any vendors' wireless network and supporting most device-level operating systems. Typical installations take less than four hours.

b. Strength of a Closed System

Public networks and hotspots are designed to be open and available to a broad group of potential users. In these situations, security is often left up to the individual user, not handled by the network provider. On the other hand, corporate networks are designed to serve a select group of authorized users and devices. Establishing a closed network system that is available (and visible) only to a finite group of users or device is one more way that Fortress protects network assets. This unequalled wireless network protection is the result of a combination of optimized security components and standard cryptographic methodologies all tightly integrated into one comprehensive solution for providing privacy, access control, authentication and data integrity. Three Factor Authentication provides the unique ability to verify or restrict usage based on network, device and/or user identity. TFA is a logical, tiered approach to authentication that, unlike other methods, tests credentials in a manner that limits the possibility of attacks based on password or user logon guessing.

c. Roaming

The untethered nature of wireless users implies the need for mobility and seamless protection. With the AirFortress solution, when a wireless station moves from one AP to another, an automatic re-association will occur with the new AP. If the new AP is attached to the same AirFortress Gateway as the initial AP (i.e., moving within a building), all security associations and credentials remain intact. If the second AP is connected to a different AirFortress Gateway (i.e., moving to another building), the action of roaming between APs forces a new key exchange to automatically occur between the mobile station and the new AirFortress Gateway. This occurs without any user intervention and no noticeable interruption in connectivity. The new association and the exchange of AirFortress keying information will force the previous credentials and associations to become invalidated on the old AP, all without the wireless user having any awareness of what has occurred.

With Fortress' secure subnet roaming, AirFortress Secure Clients can roam from an AF Gateway on one subnet (home subnet) to an AF Gateway on another subnet (foreign subnet) without having to manually renew their IP address. This ability to maintain a persistent connection during a session improves the interaction and performance with many desktop applications such as email clients that require a consistent IP address. Roamed Secure Clients remain connected to their defined home AF Gateways, meaning that all communication for a Secure Client that has roamed is routed to its home AF Gateway.

5. Conclusion

Early adopters and vendors of wireless networks have been slowly stepping their way through a myriad of legacy security options trying to find one that provides both robust security and offers the best value in terms of administrative costs and enterprise integration. Wireless enrollment and authentication products supplemented their offerings with IPsec and re-branded themselves as security solutions. But time and time again, VPN technologies (IPsec and SSL) have proven to be inefficient and vulnerable. Wireless equipment vendors with their own breed of network protection address security for those customers who are able to commit to a single vendor environment, but even these implementations are proving to be less than secure for environments that must ensure

privacy of sensitive data.

Because off-the-shelf wireless equipment must have some minimal level of protection, the WiFi Alliance and IEEE are working hard to make sure this market can shake off its tarnished image and move ahead with the steady adoption of wireless. While the industry is off contemplating the development of baseline security features, Fortress Technologies has created a family of wireless security products with the ability to consolidate wireless functionality for privacy, access control, authentication and data integrity into one comprehensive, easy-to-manage solution. Designed to go far beyond these minimum requirements and meet the more demanding expectations of corporate and government IT, AirFortress offers a best-of-breed solution. With Layer 2 data link security and Three Factor Authentication protecting against intrusion and denial-of-service vulnerabilities, the AirFortress system allows network administrators to manage the dynamic growth of wireless networks and centrally control security policies, users and devices.

With more than seven years of security systems experience and a large installed base of customers, Fortress Technologies has established itself as the leading supplier of wireless security solutions for the enterprise, industrial, healthcare and government markets.



CORPORATE HEADQUARTERS

Fortress Technologies Inc.
4023 Tampa Road, Suite 2000
Oldsmar, FL 34677 · USA
Phone: 813 288-7388
Fax: +1 813 288-7389
or 888 4PRIVACY (477-4822)

www.fortresstech.com

© 2004 Fortress Technologies Inc. All Rights Reserved.