

FORTRESS APPLICATION GUIDE



FORTRESS™
TECHNOLOGIES
Absolute Security for Intelligent Networks

Notice

Copyright © 2005 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.

Fortress and the AirFortress logos 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 © 2005, 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.

Overview

Wireless networks are enabling new types of enterprise applications, providing mobility for existing applications and enhancing productivity. With wireless networks come new security challenges. When providing network services to wireless users, steps must be taken to ensure privacy, enforce policies, and prevent unauthorized users from accessing protected network services. Just as the security risks differ from traditional wired security issues, the security solutions for wireless differ from those designed to provide wired security. A security solution should work across the full range of applications and network environments deployed in enterprises to ensure unrestricted growth and avoid obsolescence. A well-designed security system further enhances the viability of wireless networks.

Fortress Technologies has designed an integrated network security system that addresses the specific needs of enterprise wireless networks as well as supports scalability and ease of management. This overview will examine typical wireless networks, describe how the Fortress system components seamlessly deploy in each network to provide strong security, and note the capabilities and benefits of this system.

Wireless Environments

Wireless networks deployed today fall into one of the following categories:

- Wireless LAN – Wireless devices connect to each other and to the wired network through infrastructure equipment (access points and switches). This could include 802.11 a, b, g, WiFi or vendor-proprietary networks such as OpenAir.
- Point-to-Point – Multiple networks, such as buildings interconnecting on a campus, are connected through wireless links. These network links could include 802.11 bridges, 802.16 WiMAX, Free-space optics or even microwave.
- Peer-to-Peer – Wireless devices connect to each other directly without the presence of an access point or other network infrastructure.

Wireless LAN

Wireless LAN (WLAN), shown in Figure 1a, is the most popular application for wireless networking. Wireless devices connect to each other and the wired network through infrastructure equipment such as wireless access points (APs) and switches. IEEE 802.11 is the industry standard for enterprise WLANs.

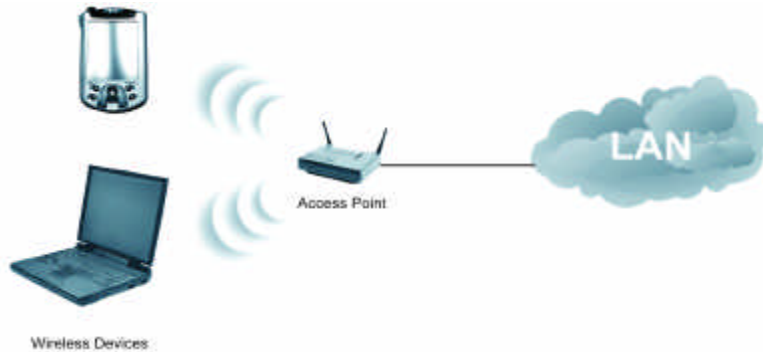


Figure 1a: Simple WLAN

Applications

WLANs are deployed for many applications: offices, warehousing, healthcare, and private hotspots, to name a few. In an office, a WLAN provides mobility for notebook computers between offices and meeting rooms, provides network access for visiting guests, and extends the network to locations that are difficult or expensive to wire. In a warehouse, a WLAN provides mobility for devices such as barcode scanners as their users move around the warehouse floor. In a hospital or medical office, a WLAN provides mobility for medical equipment and handheld computers containing patient and treatment information as healthcare staff move between patient rooms.

Protecting WLANs

The Fortress security system provides robust protection for WLANs. The Fortress Security Gateway is placed between the wireless and wired networks and authenticates and encrypts all traffic on the wireless network. The Fortress Secure Client software is installed on each wireless device and manages the secure connection between the device and the Security Gateway. The Fortress Access Control Server (ACS) authenticates devices and users according to the security policies of the company. This system provides the following:

- **Strong privacy** – All wireless traffic is encrypted at layer 2, thus network addresses, protocol information, and application data are protected from eavesdropping. Fortress uses proven cryptographic mechanisms including AES for encryption and a strong key management system to protect credentials.
- **Device authentication** – Each Secure Client has a unique, system-generated Device ID that is used to ensure that only authorized devices are allowed to connect to the protected network. If a rogue device attempts to masquerade as an authorized device by spoofing its MAC address, communications will fail because the unspoofable Device ID is incorrect. If a secure device is lost or stolen, it can easily be denied access to the network based on its Device ID.
- **User authentication** – Users can be authenticated before being granted access to the network. The Fortress solution works with your existing Windows® NT Domain, Active Directory, LDAP, RADIUS or RSA SecurID® authentication server.
- **Secure network roaming** – Wireless users can roam seamlessly between APs that are connected to separate Security Gateways or IP subnets.
- **Trusted device access** – For devices that cannot host Secure Client software, the ACS can enable a policy to allow access to specific devices based on MAC address, IP address, protocol, and port number. Devices can also be authenticated via the 802.1X standard.

- **Leverage existing infrastructure** – The Fortress system provides security as an overlay onto your existing wireless network, meaning that it will work with any combination of 802.11 standards (a, b, g, and other standards in development) or even legacy WLAN standards and protocols.
- **Ease of use** – The Secure Client is completely transparent to users and applications.
- **Centralized management** – Multiple Security Gateways can authenticate users and devices through a single ACS.
- **VLAN support** – The Security Gateway can pass or translate VLAN tags, allowing separation of wired and wireless VLANs.

Figure 1b shows a Fortress-protected WLAN. A single AP is connected to one Ethernet interface of the Fortress Security Gateway, and the other Ethernet interface is connected to the wired LAN. Fortress Secure Client software, installed on the wireless devices, encrypts the traffic on the wireless network and sends traffic through the AP to the Security Gateway. The Security Gateway decrypts the traffic and forwards it to the LAN. Reply traffic is then encrypted by the Security Gateway and sent to the wireless device. The Access Control Server, connected to the wired LAN, authenticates Secure Clients and manages security policy enforcement on the Security Gateway.

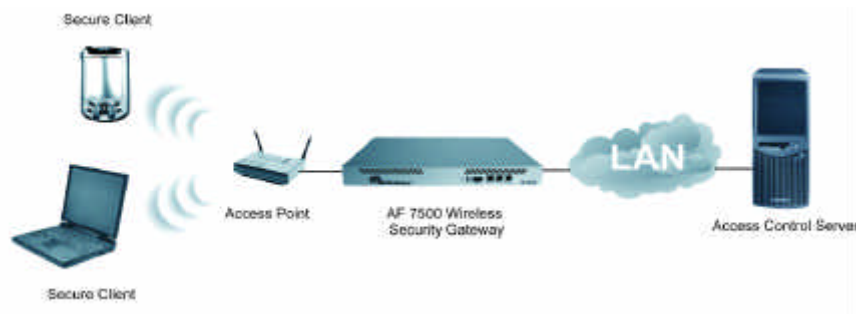


Figure 1b: Simple Fortress-protected WLAN

One Security Gateway can support many APs in a wireless LAN. The number of APs per Security Gateway is a function of the application and bandwidth requirements. Multiple APs can be connected to the Security Gateway through a simple switch or hub as shown in Figure 1c. Users can roam seamlessly between APs connected to a single Security Gateway or even between APs connected to different Security Gateways.

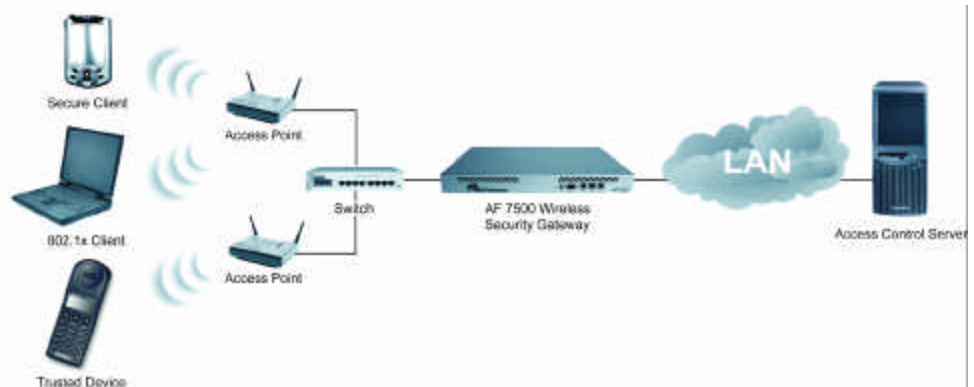


Figure 1c: Fortress-protected WLAN with multiple wireless access points

Devices without Secure Client software can also be authenticated via the 802.1X port-based authentication standard. The Security Gateway monitors 802.1X authentication packets between an AP or switch and the ACS and grants access to devices that successfully authenticate. The Security Gateway can also allow access to trusted devices, such as IP phones, that do not have the Secure Client software installed.

Point-to-Point

Wireless point-to-point and point-to-multipoint networks are commonly used to connect multiple buildings or locations using wireless links. IEEE 802.11 is often used in this environment, but IEEE 802.16 (WiMAX), free-space optics, or satellite links can also be used. Figure 2a shows a typical point-to-point wireless network diagram.



Figure 2a: Typical point-to-point wireless network

Applications

Hospitals, military bases, and corporate and educational campuses often need to connect networks between separate buildings. Wireless networks provide the ideal alternative to running wires between these locations. Wireless networks are also well-suited for providing broadband network connectivity to locations that cannot get traditional wired broadband service. With wireless networks, however, special care must be taken to assure that the security of the networks are as good as, if not better than, that of wired networks.

Protecting Point-to-Point & Multipoint

The Fortress system provides security for wireless point-to-point and point-to-multipoint networks. A Fortress Security Gateway is placed at each location and is configured to protect traffic to and from the other locations, providing the following benefits:

- **Privacy** – All wireless traffic is encrypted at layer 2 to protect from eavesdropping.
- **Device authentication** – Each Security Gateway has a unique Device ID that is used to ensure that only traffic from other authorized Gateways are allowed to pass to the protected network.
- **Point-to-multipoint support** – A single Security Gateway can simultaneously protect traffic between multiple buildings and wireless devices.
- **Leverage existing infrastructure** – The Fortress solution provides security as an overlay onto your existing wireless network, meaning that it will work with most wireless standards, including 802.11 and 802.16.

Figure 2b shows a Fortress-protected wireless point-to-point network. Security Gateways are placed behind the wireless bridges in each building. Traffic between buildings is encrypted by one Security Gateway, sent over the wireless link, and then decrypted and forwarded to the LAN destination by the other Security Gateway.



Figure 2b: Fortress-protected wireless point-to-point network

Fortress Security Gateways can also support point-to-multipoint connections with multiple buildings and wireless devices as shown in Figure 2c. In this scenario, all three building LANs can communicate with each other securely. All LANs can also be reached by a wireless device with Secure Client software roaming between buildings.

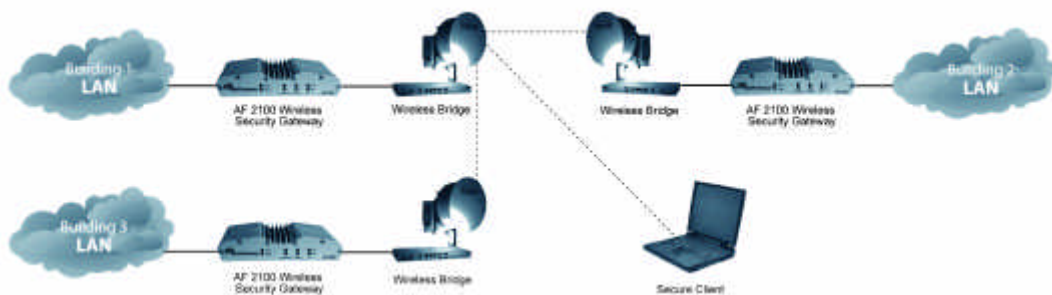


Figure 2c: Fortress-protected wireless point-to-multipoint network

Peer-to-Peer

Wireless networks can also operate in peer-to-peer mode without any wireless infrastructure (APs or switches). Also called “ad hoc mode,” wireless devices communicate directly with each other. This deployment is useful in field environments where no infrastructure is present. Figure 3a shows a typical peer-to-peer network diagram.



Figure 3a: Typical peer-to-peer network

Protecting Peer-to-Peer

The Fortress Secure Client provides complete security for peer-to-peer networks. Each wireless device uses the Secure Client to secure communications with other devices. This provides the following benefits:

- **Privacy** – All wireless traffic is encrypted at layer 2 to protect from eavesdropping.
- **Leverage existing equipment** – The Fortress Secure Client provides security in networks using any variety of 802.11 (a, b, g, and others) wireless network interface.

Figure 3b shows a Fortress-protected peer-to-peer network. Fortress Secure Client software is installed on each wireless device. The devices create an ad hoc network and then traffic between them is encrypted and decrypted by the Secure Client software.



Figure 3b: Fortress-protected wireless peer-to-peer network

When communicating with multiple peers, as shown in Figure 3c, the Secure Client negotiates unique encryption keys with each peer. Therefore, traffic between one pair of devices cannot be decrypted by other devices.

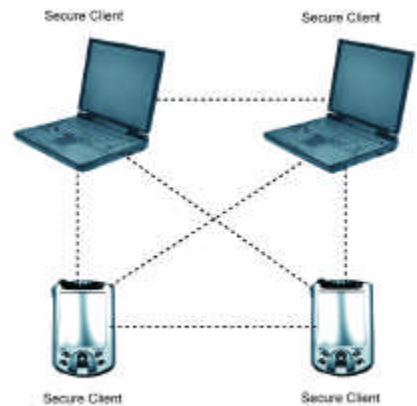


Figure 3c: Fortress-protected wireless peer-to-peer network with multiple peers

Fortress Security System

Having looked at how the Fortress security system works in a variety of wireless network environments, let's now consider in greater detail each component.

Secure Client: Network Protection Starts at the Edge

The Fortress Secure Client manages privacy and authentication while protecting the device from intrusions. It is a software client module for securing laptops, PDAs, tablet PCs and industrial equipment such as barcode scanners and portable terminals. It provides secure wireless connectivity to enterprise LANs protected by Fortress Security Gateways and to other secured devices. It encrypts and decrypts data transmitted to and from the computer on which it is installed, tracks communication with partners, and supports identification and tracking of that computer on the wireless network.

The Fortress Secure Client provides:

- **Privacy** – Provides layer 2 encryption for Ethernet and WLAN interfaces (up to 256-bit AES)
- **Ease of use** – Works transparently to users
- **Device lock-down** – Allows configuration changes to be password protected
- **Compatibility** – Works with third-party firewall and VPN products
- **Single sign-on** – Authenticates to network and operating system simultaneously
- **Always-on device protection** – Blocks unauthorized communications at all times
- **Flexibility** – Works in WLAN infrastructure and peer-to-peer (ad hoc) environments

Platforms

- Microsoft® Windows® 98, NT 4, 2000, XP, 2003
- Microsoft® Windows® CE, Pocket PC 2002, Pocket PC 2003
- DOS handheld devices
- Linux
- Palm OS® (Tungsten™ C)

Security Gateway: Foundation for Secure Networks

The Fortress Security Gateway integrates networking services with robust security and policy enforcements. It is a security appliance that provides a secure edge to the enterprise network by protecting communications between wireless devices and the rest of the network. Because the Security Gateway encrypts at the link layer, not only does it protect important network information, it also functions as a bridge thus it can be quickly and transparently integrated into an existing network. Operation is automatic, requiring no administrator intervention as it protects data transmitted on wireless networks and between wireless devices and the wired network.

The Fortress Security Gateway provides:

- **Privacy** – Provides layer 2 encryption (up to 256-bit AES)
- **Authentication** – Enforces network, device and user authentication
- **Access control** – Allows access to only secure and trusted devices
- **Mobility** – Provides secure Layer 2/Layer 3 mobility services for seamless roaming
- **VLAN Support** – Translates or passes VLAN tags
- **Flexibility** – Allows support for many wireless environments and leverage existing wireless infrastructure
- **Simple deployment** – Employs an Ethernet bridge architecture for simple integration with an existing network
- **Role-based access control** – Manages access policies for individual users
- **Ease of use** – Provides a simple, browser-based, graphical user interface

Access Control Server: Centralized Administration & Control

The Fortress Access Control Server (ACS) is a system for centralized administration and control. It provides wireless network authentication and policy management. A server-based application, the ACS enables device and user authentication, integrating with existing back-office authentication services including RADIUS, NT Domain, LDAP, Active Directory and RSA SecurID.

The Fortress Access Control Server provides:

- **Centralized management** – Provides visibility and control over Security Gateways and Secure Clients from a central console
- **Adaptive authentication** – Supports device and user authentication and integrates with existing authentication infrastructure

Summary

While wireless networks enable new applications, greater mobility and productivity, they also create new security challenges. A well-designed security system mitigates risk and integrates seamlessly with infrastructure investments, purposefully avoiding additional complexity. The security system must protect all wireless environments: WLANs, point-to-point, multipoint and peer-to-peer. As shown, the Fortress security system deploys seamlessly in each of these environments and provides a true wireless security solution that addresses the security concerns for enterprise wireless networks.

CORPORATE HEADQUARTERS
Fortress Technologies, Inc.
4023 Tampa Road, Suite 2000
Oldsmar, FL 34677
Phone: 813.288.7388 or
1.888.4Privacy (477-4822)
www.fortresstech.com

About Fortress Technologies

Fortress Technologies' is the leading provider of security products for enterprise networks. The Fortress security system provides security services, networking services, policy management and monitoring in a scalable, easy to use product suite. It seamlessly integrates with corporate wired assets and systems to ensure the business integrity demanded by commercial and government organizations. Providing the highest level of commercially available wireless security, Fortress meets the government's rigorous standards for wireless network security under the Federal Information Processing Standards (FIPS 140) validation program. Fortress also is one of the only companies to offer end-to-end security consistent with the Department of Defense's new directive for wireless devices and use.

Achieving market-leader status through securing over 10,000 enterprise networks, Fortress has received SC Magazine's coveted "Readers Trust" award for best wireless security solution for two consecutive years. Fortress accolades also include being named one of the "Fierce 15" top 15 emerging WLAN companies for 2005, as well as receiving Frost and Sullivan's 2004 "Market Leadership of the Year" award for wireless LAN security.