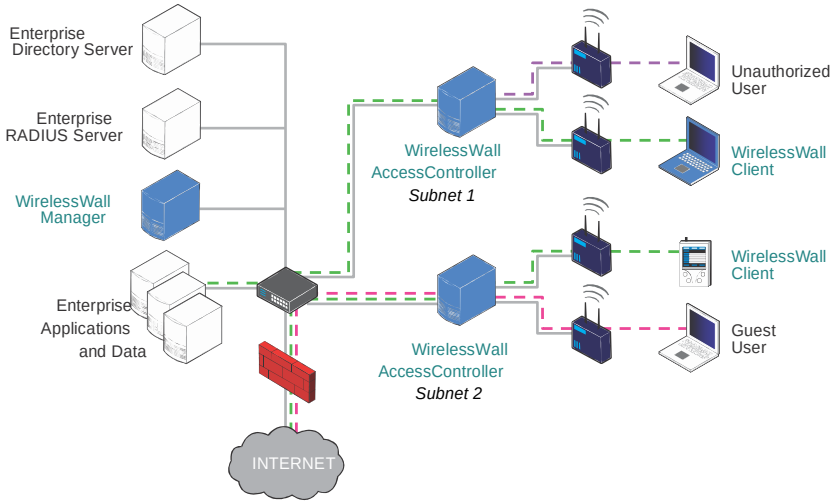
TLC Datasheet

WirelessWall®



Award-winning FIPS 140-2 validated **end-to-end security** and mobility software for sniffer-proof wireless networks.

Robust FIPS 140-2 Certifed WLAN Security System

WirelessWall® is a robust, FIPS 140-2 certified wireless LAN security software solution that enables government agencies, financial and healthcare organizations, and commercial enterprises to preserve wireless infrastructure investment. WirelessWall combines enterprise-class wireless network protection, seamless cross-subnet mobility support, and integrated system management. Strong security is uniform, even over older Access Points and WLAN devices that don't support WPA2-grade AES encryption. 4G WiMAX and Mesh ready for long distance.

WirelessWall Manager:

Provides centralized configuration, monitoring, and management of large secure wireless networks. Enables the creation and maintenance of access policies for mobile users. Allows administrators to monitor performance and usage of an entire wireless network with multiple access points in real-time and make necessary adjustments.

WirelessWall Access Controller:

Enforces access policies, performs session management tasks required for secure wireless LAN operation, encryption decryption, firewall filtering, and secure mobility services.

WirelessWall Access Client:

Zero-configuration thin client that operates on each mobile device. Encrypts and decrypts all data at each user's connection.

Features and Benefits

Layer 2 Encryption

- Encrypts the 802.11 data payload using FIPS 140-2 certified Advanced Encryption Standard (AES) cryptography.
- Hides sensitive information such as IP addresses, ports, and protocols from unauthorized listeners.

Seamless, Secure Mobility

- Securely tracks and maintains all user authentication and authorization information, ensuring seamless, uninterrupted sessions as users move between locations and across subnets.
- Supports multiple options of robust mobility providing different levels of security. Prevents all wireless sniffing.

FIPS 140-2 Certified

- NIST certified as meeting rigorous FIPS 140-2 requirements.
- Complies with DoD and civilian agency security requirements.

Centralized Monitoring and Management

- Intuitive, browser-based interface enables authorized network administrators to monitor all system and management functions from a secure web browser.

Protects investment and lowers TCO

- Open architecture, seamlessly integrates with existing authentication and directory services.
- 4G WiMAX Ready and MotoMesh Certified. Supports any mix of 802.11a, b, g, h, j or n from any vendor.

TLC-Chamonix, LLC, 120 Village Square suite, 11 Orinda, CA 94563, USA Tel: +1 (877) 479-4500 • E-mail: info@wirelesswall.com. • http://wirelesswall.com

WirelessWall: Flexible Layer 2 Software Architecture

WirelessWall's software-only architecture enables flexible, secure WLAN deployments using a wide range of commercial of-the-shelf hardware. Extensive client operating system support facilitates seamless and secure wireless connectivity anytime, anywhere.

Unlike VPN or SSL based systems, WirelessWall protects customer networks by encrypting all network data, including sensitive IP header and user payload data.

WirelessWall is the only Layer 2 software based FIPS 140-2 certified product that mitigates the wide range of vulnerabilities and attacks common to Layer 3 (e.g., IPSec VPN) and SSL-based products. WirelessWall protects against the following attacks:

- Access Point / MAC address spoofing
- Dictionary attacks
- Man-in-the-middle
- ARP connection/redirection
- WEP, WPA weaknesses

Specifications

WirelessWall Access Controller/Manager Minimum Requirements:

Intel Pentium® Server or VMWare with:

- Two 10/100 Ethernet network interfaces
- 20 GB Hard Disk
- 800 MHz Intel-based processor
- 256 MB Memory
- CD-ROM drive

WirelessWall Clients

- Linux
- Microsoft Windows 2000, XP and Vista
- Windows Mobile, Pocket PC
- Mac OS X Panther, Tiger and Leopard

Directory Servers

- Microsoft Active Directory
- Microsoft NT Domain Server
- OpenLDAP

RADIUS Servers

- Microsoft IAS
- FreeRADIUS
- Other RADIUS-compliant

Compare

	WirelessWall	Proprietary-Hardware Solution	802.11i Solution	IPSec/SSL-Solution
FIPS 140-2	Yes	Maybe	No	Maybe
Use Existing Hardware	Yes	No	No	Yes
Meets Military Policy Mandates	Yes	Maybe	No	No
Prevents MAC Spoofing	Yes	Maybe	No	No
Seamless Roaming Across Subnets	Yes	Maybe	No	Maybe
Secures gap between data center and APs	Yes	No	No	Yes

In addition, WirelessWall supports advanced features such as Virtual LAN tagging and directory caching, providing significant network performance enhancement and flexibility.

For more information, contact TLC-Chamonix at
Tel:+1 (877) 479-4500,
E-Mail: info@wirelesswall.com
Web at http://wirelesswall.com