CYLENTIUM

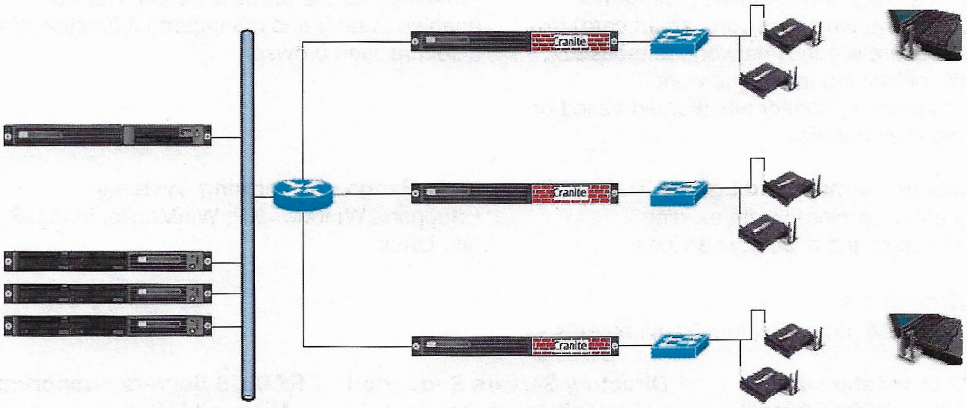
WirelessWall® • *Technology Solutions Brief*

WirelessWall Integration with the Harris SecNet 11 Plus

WirelessWall® is a robust, FIPS 140-2 certified wireless LAN security software solution that enables government agencies, healthcare organizations, and enterprises to enjoy the productivity benefits of wireless LANs without the security risks. WirelessWall combines enterprise-class wireless network protection, end-to-end cross-subnet mobility support, and integrated system management.

Harris' SecNet 11® family is the only 802.11 wireless solution approved by NSA for the protection of Secret data. Based on the IEEE 802.11b protocol, the SecNet 11Plus combines an extremely lightweight & compact form factor with NSA Type 1 (Baton) encryption to provide the utmost in security for Secret tactical and enterprise networks. With drivers for Windows, WinMobile, Mac, and Linux clients, the SecNet 11 Plus enables secure communications for military, the intelligence and joint communities, and first responder customers on multiple platforms in multiple environments.

The use of WirelessWall in conjunction with the SecNet 11 Plus provides significant additional functionality well above and beyond data encryption. WirelessWall is a software solution designed to provide secure, mobile computing in enterprise and tactical wireless networks. WirelessWall is best known for providing FIPS 140-2 validated data encryption (superseded in this application by the SecNet 11's encryption); however, its user-based authentication & authorization, seamless subnet mobility, and enterprise integration capabilities are unmatched, and make it a perfect complement for the SecNet 11 Plus.



WirelessWall adds significant capability to the SecNet 11 product family, at an incremental cost per seat of less than 5% of the SecNet 11 Plus product itself. WirelessWall's software-based approach also provides significant flexibility in terms of hardware platforms—enterprises can deploy on servers from existing vendors such as HP, Dell, or IBM, while tactical deployments can use ruggedized or specialized servers already certified to operate in hazardous or difficult environments.

TLC-Chamonix

TLC-Chamonix, LLC
120 Village Square, Suite 11
Orinda, CA 94563

For more information, call +1 (877) 479-4500, sales@tlc-chamonix.com, or on the Web at wirelesswall.com

The combination of WirelessWall and SecNet 11 products enables true enterprise integration of 802.11 wireless networking into the Secret environment. By adding WirelessWall's user-based authentication to the SecNet 11 Plus, administrators and commanders are assured their networks will not be breached in the event of a device compromise. WirelessWall integrates with existing authentication solutions such as RADIUS to provide user-based authentication, above and beyond the device-based authentication provided by the SecNet 11 Plus. WirelessWall also provides authorization and role-based access control by integrating with enterprise directory applications such as Active Directory and LDAP, a feature not provided by the SecNet 11 by itself.

The combined solution also enables users to roam seamlessly between subnets—a requirement for scaling any 802.11 network, but one not provided by the SecNet 11 itself. In a typical network scenario using the SecNet 11, a user roaming from one subnet to another would be able to do so in a secure fashion; however, crossing a subnet boundary brings the additional burden of maintaining an IP address across that boundary without affecting application integrity. Typical scenarios require the user to log off applications before crossing the subnet boundary, request a new IP address via DHCP once attached to the roamed subnet, then restart (and perhaps re-authenticate to) applications. Such a scenario is burdensome in the enterprise, and defeats wireless' inherent mobility. WirelessWall enables the user to seamlessly roam between subnets while maintaining a secure connection by managing all IP addresses, attachment locations, and network state with no user input or need to re-authenticate.

Features and Benefits of the Combined Solution

NSA Validated Type 1 Wireless Encryption
• Meets DoD's strict requirements for wireless transmission of both classified (Secret) and unclassified information.

User-based Authentication and Authorization
• Requires entry of credentials (username/ password, one-time password, smart card) to access secure wireless network; role-based access control; authorized network administrators to monitor all enforced based on directory membership.

Protects Investment and Lowers TCO
• integrates seamlessly with existing authentication and directory services.

End-to-End, Secure Mobility
• Securely tracks and maintains all user authentication and authorization information, ensuring seamless, uninterrupted sessions users roam across subnets.

Centralized Monitoring and Management
• Intuitive, secure browser-based interface enables system and management functions from a secure web browser.

Wide Range of Operating Systems
• Supports Windows XP, WinMobile, Mac OS X, and Linux.

Specifications

WirelessWall Minimum System Requirements

Intel P2 or greater with:
• Two 10/100/1000 Ethernet network interfaces; USB
• 20 GB Hard Disk
• 800 MHz processor
• 1GB Memory

Directory Servers Supported
• Microsoft Active Directory
• Microsoft NT Domain Server
• OpenLDAP
• Other LDAP-compliant servers

RADIUS Servers Supported
• Microsoft IAS
• FreeRADIUS
• Other RADIUS-compliant servers