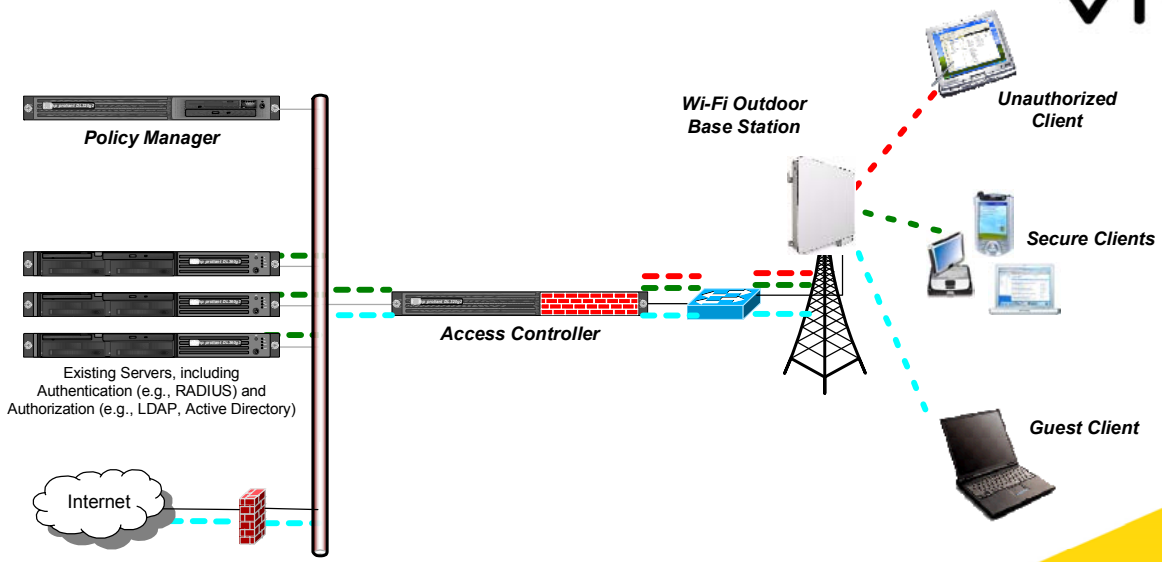

V vato Technical Note: VTN5

FIPS 140-2 Security for Long Range Wireless LAN/MAN

Application: Wi-Fi Base Station

Introduction

802.11 (Wi-Fi) wireless local area networks (WLANs) have enjoyed enormous growth over the last few years. As Wi-Fi swept into private homes and small offices at a record setting pace, enterprises lagged behind, particularly due to the security concerns of enterprise IT managers. These concerns were validated when the standard Wi-Fi security method, Wired Equivalent Privacy (WEP), was compromised. As a result, most enterprise users were denied the inherent productivity of high-speed mobile network computing. Understandably, security concerns excluded the use of WLANs in Department of Defense networks as well as in many healthcare and financial institutions. The vendor community and the IEEE have responded with numerous new cryptographic and authentication standards that address the security concerns of WLAN deployments.

WEP's weak static keying has now been replaced with Temporal Key Integrity Protocol (TKIP) which dynamically changes the encryption key over a period of time, defeating WEP key recovery attacks. Additionally, 802.1x adds a user authentication server that distributes encryption keys. However, the vendor community recognized that the ratification of the IEEE 802.11i security standard would take significant time, and that an interim solution was needed to provide a higher measure of information assurance to the user community. Thus, the Wi-Fi Alliance (which is an organization composed primarily of vendors rather than a standards-making body like the IEEE) introduced Wi-Fi Protected Access (WPA) certfication. WPA incorporated these new methods and standards while adding payload integrity checks to address masquerade and replay attacks. With the June 2004 ratification of IEEE 802.11i, the Wi-Fi Alliance has replaced WPA certification with "WPA2-Enterprise", utilizing 802.1x for authentication and the Advanced Encryption Standard (AES) for security. Even if properly deployed,

these newer technologies fail to adequately protect WLANs. Further, they are not certifiable to the latest government standards and can be misapplied, misconfigured, or simply left in the default "off" state by neglect or as a result of incompatibility with existing equipment. Enterprises and (especially!) governments need and demand more.

The US government has mandated that all purchases of products using cryptography conform to stringent, certifiable requirements. Requirements for WLANs typically mandate the provision of an end-to-end assured channel using FIPS-certified cryptography.[1] Cryptographic solution vendors must submit their products to testing laboratories managed by the National Institute of Standards and Technology (NIST). Products are evaluated by these labs for conformance to a specific set of requirements. These requirements are found in Federal Information Processing Standards (FIPS) publications; FIPS 140-2 specifically addresses cryptography for Sensitive But Unclassified (SBU) applications. [2]

This paper will discuss the application of a FIPS 140-2 validated security system in a long-range, high-coverage wireless network.

Building a Long-Range High-Coverage Secured Network

The inherent productivity improvement from mobile network connectivity becomes obvious soon after initial deployment. Mobile workers and their enterprise managers or military commanders will quickly demand expanded wireless coverage to further enable efficiencies across the entire area of operations. In anticipation of this demand, the network administrator should integrate scalable WLAN into his or her overall network plan.

Wireless LAN Components

As shown in Figure 1, the simplified network would consist of wireless equipment added to the enterprise network. Critical security components must be added, but they should not limit wireless' inherent mobility or burden the user with procedures which reduce efficiency gains. These security components should also be compatible with the existing legacy network equipment to control costs. First, we'll examine the wireless component.

Typical Wi-Fi equipment is limited to a range of 200 to 300 feet between standard access points (APs) using omni-directional antennas and laptop clients in an open environment. This range amounts to a circular coverage area of approximately 250,000 square feet. High-gain omni antennas can be added to increase range and coverage—at the expense of lower throughput due to increased levels of received interference [3]. A high-gain sectored antenna can be added to spatially reduce the effect of interference, but this configuration suffers from decreased coverage area due to the smaller inherent field of view of these devices.

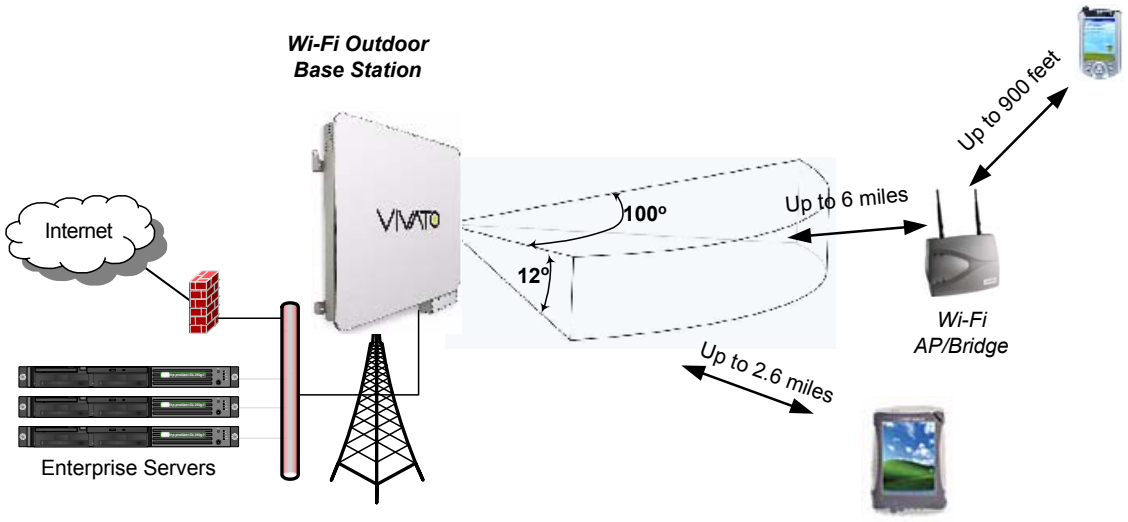

Figure 1 Long Range High Coverage Wi-Fi

Phased array Wi-Fi base stations combine the long range and interference rejection of a high-gain antenna and the coverage advantage of wide field-of-view omni systems by electronically synthesizing many individually-pointed, high-gain antennas. As a result, a single base station mounted on a 60 foot mast can provide service to an open area of over 160 million square feet (6 square miles) for hand held Wi-Fi clients. Unlike conventional Wi-Fi equipment, multiple base stations can be located on the same mast to increase this coverage by a factor of 3.6. The expanded coverage capability from a single location greatly reduces both time to deploy and overall cost of the wireless network.

Wi-Fi AP/Bridges (or “microcells”) can be added where needed to provide either wired Ethernet or wireless connectivity to clients that are out of direct range due to distance, shadow fading, or building wall attenuation [4]. The microcell can be configured with high-gain antennas to increase the range of both the Wireless Distribution System (WDS) backhaul links and links to client devices. The network designer will typically need to add only a few microcells to a network, thus minimizing the total number of wireless devices and associated management needed for full coverage. Such a configuration has the added advantage of limiting the number of wireless backhaul links which introduce unwanted latency which adversely affects applications such as wireless VoIP.

Security Components

Once sufficient wireless coverage is provisioned, the remaining critical network design element is security. The system must integrate advanced WLAN security features in a managed and validated system configuration. If the security implementation places an undue burden on users, it will reduce the effectiveness of the WLAN or, even worse,

discourage its use altogether. The network designer must review the mobile environment, user habits, mobile application, and network resources for requirements that will enhance network functionality. As an example, consider an environment where client devices are utilized by multiple users throughout a multi-shift day. The network designer should address the following questions:

- Will each user's access to network resources be unique?
- Do security requirements dictate that each user has a unique login?
- Will users roam across multiple radios or subnets?
- Are guest users allowed access and to which resources?

A successful implementation of a secure high-coverage Wi-Fi environment meets the resulting requirements while ensuring enhanced network functionality and user productivity.

In addition to understanding user requirements, a thorough understanding of the radio environment, at both initial design and ongoing operation, is a key component of a secure network. As an example, otherwise well intentioned employees, understanding the productivity improvements of mobile networked computing, may have or will soon place unsecured and unmanaged wireless access points (APs) on the network. A secured wireless network should have provisions to initially and continuously scan for these rouge APs. The Vivato Base Station can be enabled to monitor the environment using the built in Rouge Access Point Detection (RAPD) feature as shown in Figure 2. The rogue AP detector screen displays extensive decoded information from these APs to help you identify and locate their source.

- **SSID**: The service set identifier (SSID) is similar to the Wi-Fi Base Station's ESSID - an identifying name that is broadcast to enable users to select the desired Wi-Fi Base Station.
- **MAC Address**: The media access control number of the device or wireless interface transmitting the received signal.
- **Channel**: The 802.11b channel for the detected signal.
- **Pointing Directions (Signal dBm)**: The signal strength for this signal as it is received at each of the 13 wireless interfaces in the Wi-Fi Base Station. The values are ordered from left to right (from behind the Wi-Fi Base Station) to correspond to the pointing direction of the received signal. Note that a zero (0) indicates a signal level too low to affect Wi-Fi operation; it does not mean a signal level of 0 dBm (1mW).

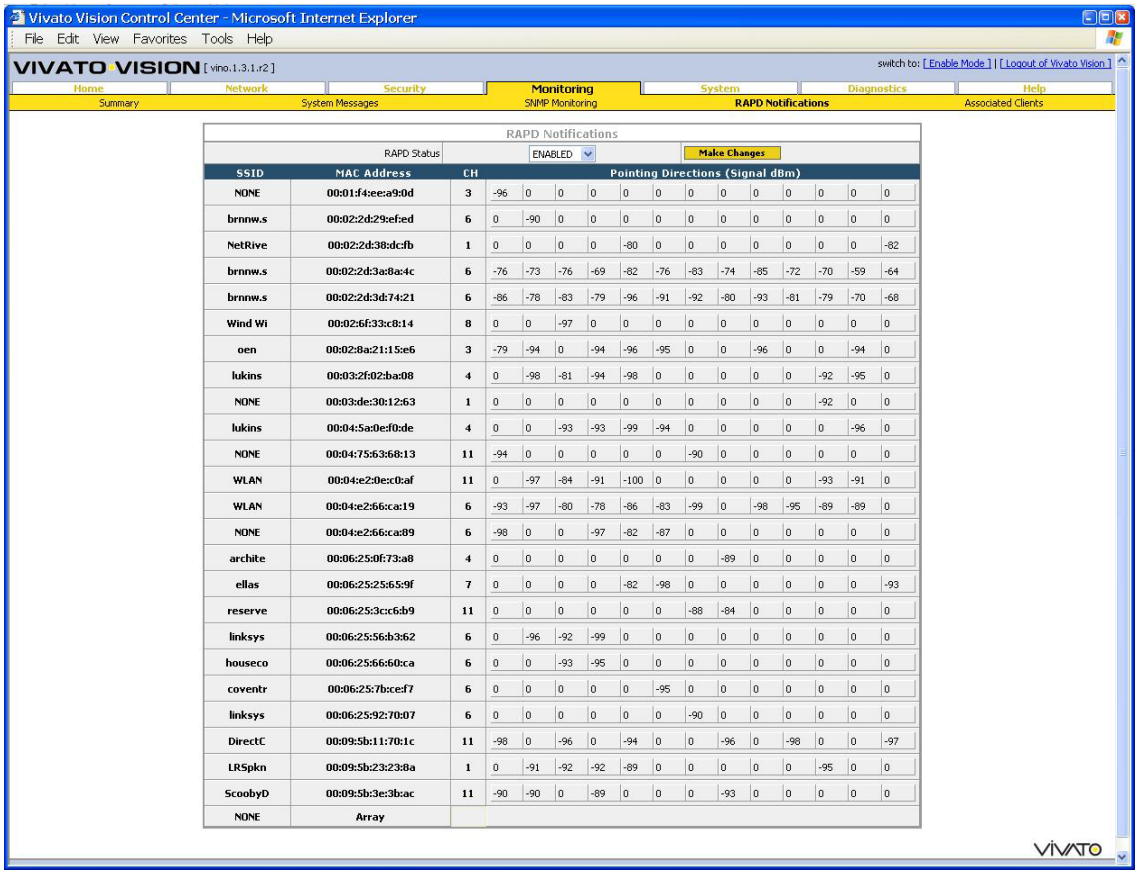

Figure 2 Rouge Access Point Detection (RAPD)

The burden of integrating advanced security features to address strict enterprise-level and DoD security requirements, while meeting the productivity goals of the network designer, has now been greatly reduced. Cranite Systems' WirelessWall® software suite secures and manages the WLAN with features that address true mobility needs.

WirelessWall interoperates with existing policy, management, and security applications, and provides broad-based support for a wide variety of wireless devices, including Vivato Wi-Fi Base Stations and Microcells. Since WirelessWall is independent of the type of radio technology being deployed, it supports any mix of 802.11a, b, g, h, or j products. This ensures compatibility with future Vivato product introductions, as well as in mixed deployments consisting of Vivato products and products from other suppliers. This approach protects existing infrastructure investment and significantly reduces the overall cost of ownership.

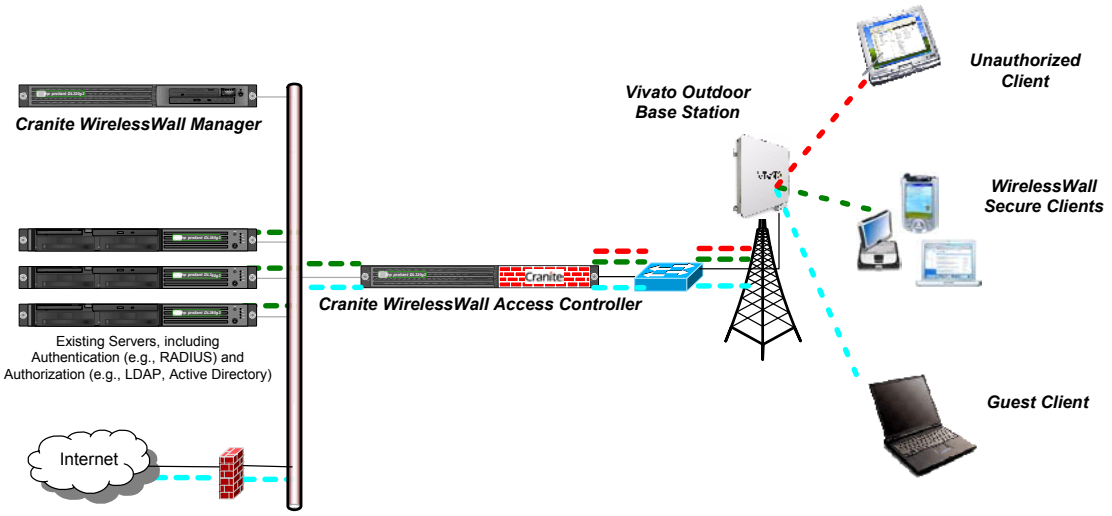

Figure 3 Network Components

WirelessWall has three main components, as shown in Figure 3:

WirelessWall Manager –The Manager is a browser-based application that provides centralized configuration, monitoring, and management, of the secure wireless network. The Manager integrates with existing authentication servers and enterprise directories, enabling network administrators to securely create and maintain local wireless access control policies for mobile users.

WirelessWall Access Controller –The Access Controller allows enterprises to integrate wireless users into their wired LAN architectures and enforces all policies created on the WirelessWall Manager. The Access Controller also performs all session management tasks required for secure wireless LAN operation, such as encryption, decryption, and firewall filtering, to provide a secure mobility service infrastructure.

WirelessWall Client –The Client is a zero-configuration thin client that runs on each mobile device connected to the wireless network. The Client works with the WirelessWall Access Controller to encrypt and decrypt wireless traffic. WirelessWall clients are available for the full range of Microsoft products, including PocketPC and CE.net, as well as Macintosh and Linux.

Authentication Process

The authentication process, as shown in Figure 4, is managed using an 802.1x framework and Cranite-specific protocol extensions to prevent session hijacking or denial of service attacks at any point. An Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) connection is established to protect the users authentication credentials for each login attempt.

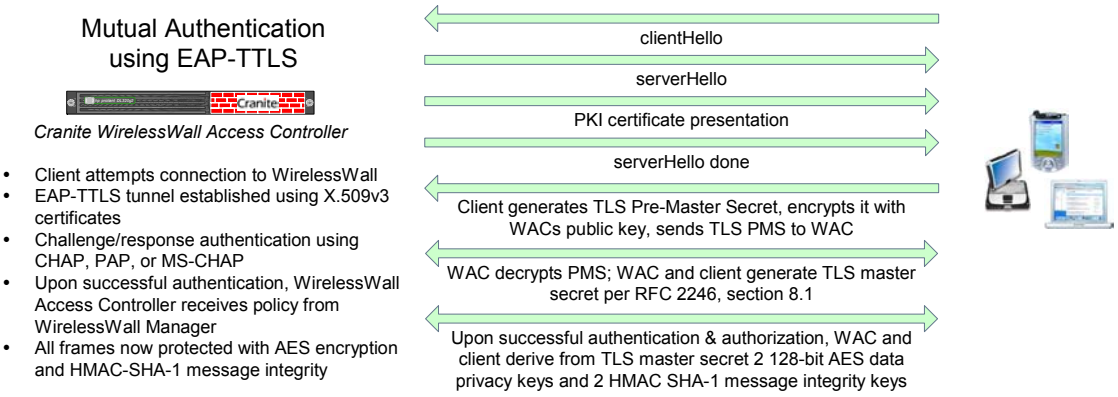

Figure 4 Client Authentication Process

Maintaining Sessions Securely

Once the session tunnel is established, the WirelessWall Client and WirelessWall Access Controller fully authenticate each frame. This process includes validating sender identity, checking for evidence of tampering, ensuring that the frame sequence numbers are correct, and verifying conformance to the policy in place for the connection.

Mobilizing Sessions Securely

WirelessWall supports three mobility types, each executed securely. However, the basic mechanism for re-establishing a connection between the WirelessWall Client and a new WirelessWall Access Controller is the same for all three mobility modes [5].

Basic Roaming and Re-establishing a Session

Upon the successful creation of a new session, the WirelessWall Manager pushes the TLS session ID and master secret to all available WirelessWall Access Controllers. This information is used to facilitate the creation of new connections as users roam between WirelessWall Access Controllers, as shown in Figure 5.

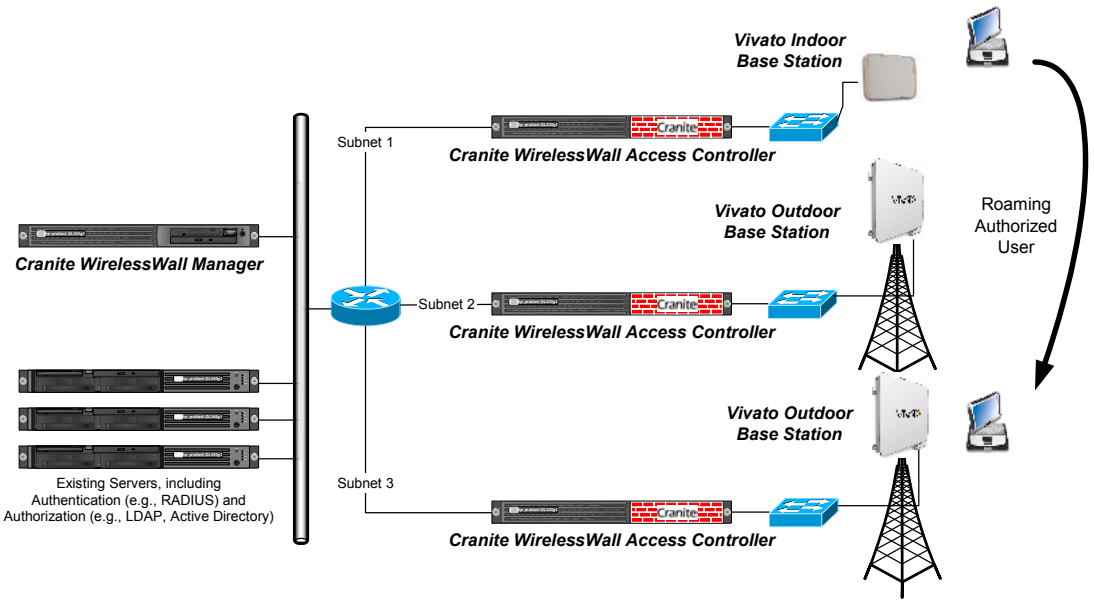

Figure 5 Roaming User

When the WirelessWall Client roams from one WirelessWall-secured subnet to another and establishes a new radio connection, the new WirelessWall Access Controller uses the WirelessWall Client's session context to complete an abbreviated TLS handshake. In doing so, the Client is securely authenticated on the new WirelessWall subnet. No intervention is required on the user's part, making roaming a seamless, transparent process for the user. Each time a user roams between secure subnets, the roam is logged to ensure accounting and ease troubleshooting for the administrator.

Mobility Mode 1: Dynamic Home Mode

For those concerned about application persistence, WirelessWall offers Dynamic Home Mobility Mode. In this mode, when a Client roams between secured subnets, the Client informs the roamed WirelessWall Access Controller of the IP address of its home WirelessWall Access Controller. Upon doing so, the roamed WirelessWall Access Controller registers with the Client's home WirelessWall Access Controller to establish a forwarding relationship. Because Dynamic Home Mode provides application persistence, this mode is employed by the majority of enterprises.

Mobility Mode 2: Static Home Mode

For those concerned about application persistence, and desiring an additional level of management control, WirelessWall offers Static Home Mobility Mode. This mode functions in a technically similar fashion to Dynamic Home Mode. In Dynamic Home Mobility Mode, the WirelessWall Access Controller to which the user initially authenticates is the user's Home WirelessWall Access Controller for the duration of the session. In Static Home Mode, all Client traffic, regardless of initial authentication or origination location, is delivered to the WirelessWall Access Controller which the administrator has defined in the WirelessWall Manager as the user's Home

WirelessWall Access Controller. For this reason, Static Home Mode provides an additional level of management control and is also used if an enterprise is running static IP.

Mobility Mode 3: No Home Mode
For those unconcerned about application persistence, WirelessWall offers No Home Mobility Mode. In this mode, when a Client roams between secured subnets, new AES-CBC and HMAC-SHA-1 keys are derived and the user joins the roamed subnet. Since the user is now a member of the roamed subnet, DHCP requests a new IP address. This mode defeats the purpose of wireless mobility because it forces the user to restart any applications that are dependent upon maintaining an IP address. Hence, this mode is rarely used in enterprise environments.

Ending Sessions
All sessions expire after an administrator-defined period of time, which is configurable per policy. Before a session expires, the user is prompted to provide authentication credentials so the session can continue without interruption. Ten minutes before the session is scheduled to end, the WirelessWall Client sends an EAPoL "Hello" message which initiates the re-authentication process. If the user is not available to provide credentials, the session expires on all WirelessWall Access Controllers simultaneously and all session keys are erased.

Role-Based Policy Enforcement
One of the most powerful features of WirelessWall is its ability to enforce policies unique to each connection, including a policy allowing guest Internet access. This capability enables administrators to deliver differentiated services to mobile users on the same network infrastructure. For example, the role-based firewall can limit traffic to a specific server while simultaneously allowing otherwise broad access to an authenticated mobile user. This capability creates new opportunities for creative network design and infrastructure cost savings. Role-based policy enforcement is also useful to permit guest access while protecting the wired network from unauthorized access. All communication between wireless clients transits the Access Controller insuring policy conformance.

WirelessWall implements its role-based firewall with robust policy capabilities based on highly granular network traffic filtering. A simple web-based instrumentation dashboard allows security and network administrators to associate security policies with specific connections based on each user's existing group/domain associations as defined by the enterprise's directory service.

Encryption
WirelessWall uses the Advanced Encryption Standard (AES) to protect sessions and networks from attack and compromise. AES is a Federal Information Processing Standard (FIPS) – FIPS Publication 197 – that specifies a cryptographic algorithm for use by U.S. government organizations to protect sensitive information. AES' combination of security, performance, efficiency, ease of implementation, and flexibility, make it an appropriate selection for mobile applications and WirelessWall. In particular, AES is ideal for lightweight hardware devices such as PDAs, ensuring

maximum battery life and throughput without compromising any of the typically lightweight processing power on the PDA. Contrast AES with Triple DES, which can suffer overhead of 30%, further, the processor-intensive nature of Triple DES drains battery life at a much greater rate than AES.

Due to its performance characteristics, AES has been specified as the data privacy algorithm in the 802.11i security standard. WirelessWall offers all the benefits of AES-based data encryption today, while adding significant enterprise-level management and mobility features which will not be addressed by the standards bodies. Further, WirelessWall protects the existing investment in access points and network interface cards by eliminating the need for a forklift upgrade now that the 802.11i standard has been ratified. Standards-based products can be used in a "mix and match" environment, increasing return on investment while lowering total cost of ownership.

Conclusion

The rapidly growing Wi-Fi market offers users true high-speed data connectivity, mobility, and network expansion. Security concerns have now been addressed by the vendor community, and augmented by government and military certification programs. Vivato and Cranite Systems have joined forces to test and validate a solution that offers maximum mobility while maintaining strict network security. Vivato's long-range, high-coverage base stations and microcells provide for rapid deployment of high coverage low cost wireless networking, while Cranite's WirelessWall brings a purpose-built solution to treat management, security, and mobility, with equal importance without compromising any of the three:

- *Management* – WirelessWall enables administrators to utilize existing enterprise directories to manage and secure wireless LAN connections, regardless of the access infrastructure protocol or vendor.
- *Security* – WirelessWall operates at Layer 2 of the networking stack, providing the utmost level of protection against radio-based attacks.
- *Mobility* – WirelessWall supports a highly mobile, vastly scalable user community with simple, elegant, secure roaming that provides a seamless user experience while making the IT administrator's job easier.

For more information on deployment and support of combined Vivato/Cranite solutions please contact Vivato at 866-802-1600 (509-343-6059) or Cranite Systems at 888-410-1115 (408-360-4900).

References

[1] Federal Information Processing Standards (www.itl.nist.gov/fipspubs/geninfo.htm)

[2] FIPS publication 140-2 (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf).

[3] Vivato Technical White Paper, “Metropolitan Wireless LAN/Man Deployment”. June 2004, (www.vivato.com/metro/download/MetroWirelessLAN.pdf)

[4] Vivato Wi-Fi Base Station (VP1210) Outdoor Deployment Guide

[5] Cranite Technical White Paper, “Best Practices: Wireless LAN Design, Implementation and Management” Sept. 2003

About Vivato - Vivato delivers a complete family of innovative Wi-Fi infrastructure products, featuring Wi-Fi Base Stations, both indoor and outdoor. Vivato's base stations are packaged as a single integrated unit, including the planar phased array antenna and all of the electronics needed to run the Base Station. Simply supply Ethernet and power, and the Base Station delivers beams of Wi-Fi to a large area. For more information please visit www.vivato.com.

About Cranite Systems, Inc. - Founded in August 2000, Cranite develops purpose-built solutions for managing and securing wireless networks that enable maximum mobility for users with the lowest total cost of ownership. The company is headquartered in San Jose, CA. Please visit www.cranite.com for more information.

VIVATO
Wi-Fi WHERE YOU NEED IT

CORPORATE OFFICE
1820 GATEWAY DRIVE
SUITE 300
SAN MATEO, CA 94404
PHONE (650) 227-0490
www.vivato.net

RESEARCH AND DEVELOPMENT
12610 E. MIRABEAU PKWY
SUITE 900
SPOKANE, WA 99216
PHONE 509-343-6001