TLC WirelessWall Architecture

White Paper

This document describes the architecture and internals of WirelessWall.

Rev 1.0
4/15/2012

Phil Smith, phil@tlcsecure.com

Contents

Acronyms

AES	Advanced Encryption Standard
CA	Certificate Authority
COTS	Commercial Off The Shelf
DES	Data Encryption Standard
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
HIPAA	Health Insurance Portability and Authorization Act
HMAC	Hashed Message Authentication Code
LDAP	Lightweight Directory Access Protocol
OSI	Open Systems Interconnect
PKI	Public Key Infrastructure
PMS	Pre-Master Secret
RADIUS	Remote Authentication Dial-In User Service
SHA	Secure Hash Algorithm
TTLS	Tunneled Transport Layer Security
TLS	Transport Layer Security
VLAN	Virtual Local Access Network
WAC	WirelessWall Access Controller
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

Introduction

TLC WirelessWall is the industry's premier FIPS 140-2 validated software-based solution for protecting wireless networks at Layer 2 of the OSI model. Based on an open, non-proprietary architecture, the system extends existing Wi-Fi component-level standards to solve specific system-level issues. WirelessWall provides a tightly integrated framework enabling interoperability with existing identity management, policy, and security applications while providing broad-based support for a wide variety of wireless devices. The system runs on standard, commercially available off-the-shelf (COTS) hardware. As WirelessWall is **independent of the type of radio technology being deployed,** the system can support any mix of 802.11a, b, g. j or n access points from any vendor, and supports newer 802.11 standards like 802.11n, and operating across long-haul bridges such as 802.16 (WiMAX). The architecture fulfills four objectives:

1. It enforces uniform high (WPA2-Enterprise) security-only across heterogeneous networks.
2. It protects existing infrastructure investment by enabling strong security on legacy devices which may not support WPA2-Enterprise mode.
3. It improves end-to-end security by extending encryption from the client to the data center instead of at the access point, which may otherwise leave the distant bridge from datacenter to AP vulnerable.
4. It centralizes firewall and port-management policies for large clusters of access points, simplifying management that would otherwise have to be replicated to each access point.

WirelessWall has three main components as shown in Figure 1:

WirelessWall Manager – The WirelessWall Manager is a secure browser-based application providing centralized configuration, monitoring, and management of the secure wireless network. The Manager utilizes credentials and group information stored in existing enterprise identity management systems (e.g., Active Directory, LDAP, RADIUS) for authentication, authorization, and policy selection.

WirelessWall Access Controller – The WirelessWall Access Controller (WAC) allows enterprises to integrate wireless users into their wired LAN architecture and enforces all policies created on the WirelessWall Manager. The WAC runs on COTS hardware and physically separates the wireless network from the wired network. Acting as the gatekeeper to the wireless network, WirelessWall enforces all policies created on the Manager and performs all session management tasks required for secure wireless LAN operation, including secure authentication tunneling, data encryption and decryption, firewall filtering, and mobility services.

WirelessWall Client – The WirelessWall Client is a zero-configuration thin client that runs on each WirelessWall-enabled mobile device connected to the wireless network. The Client communicates with the WirelessWall Access Controller to ensure secure authentication, to encrypt and decrypt wireless traffic. The Client incorporates a simple, easy-to-use interface for both login and for cryptographic bypass, for use when a WirelessWall infrastructure is not available.

Easy Integration with Existing Network Infrastructure

WirelessWall is designed to integrate with existing wired switching/routing infrastructure as an overlay, minimizing the need for reconfiguration of the wired network. Enterprise networks and enterprise-grade access points are typically carry different classifications of traffic over different VLANs. WirelessWall supports VLAN tagging, providing network architects significant flexibility in the integration of wireless into existing wired networks by using VLAN trunks.

WirelessWall provides significant capability for high availability. WirelessWall Access Controllers can be used in parallel to provide hot standby. As the WAC is a software application on COTS hardware, the cost to deploy redundant systems is significantly lower than using proprietary hardware appliances. WirelessWall provides local directory caching—a significant capability for large enterprises, where communication with enterprise directories may be lost from time to time. Using local directory caching WirelessWall maintains an updated local copy of the directory at the WirelessWall Manager; if communication between the Manager and the enterprise directory is lost, users can still be authorized to use the wireless network. Directory caching also speeds the user authorization process, ensuring a smooth login process for authorized users.

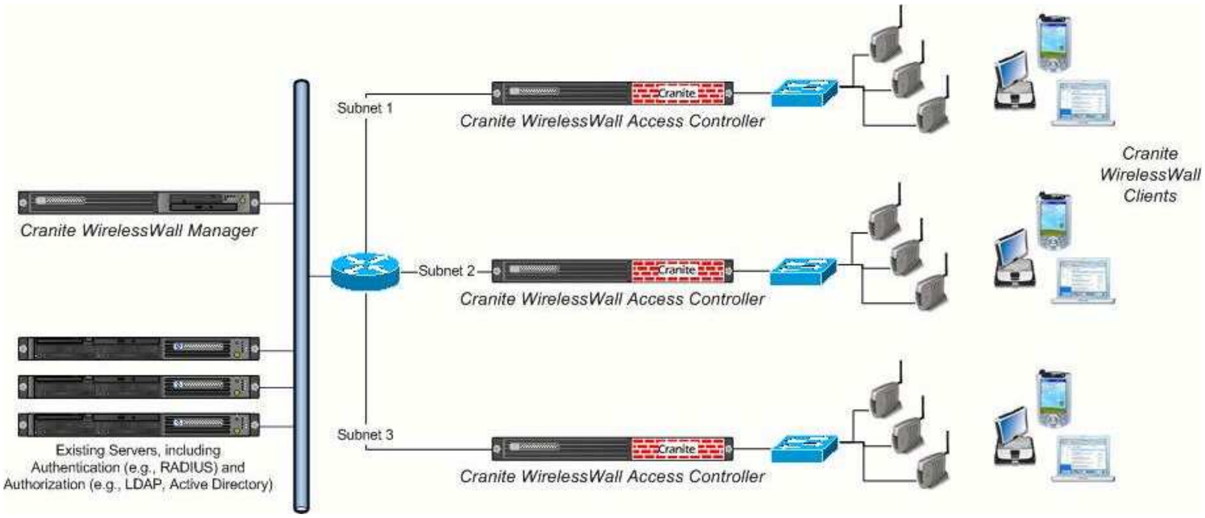
Subnet 1
Cranite WirelessWall Access Controller
Cranite WirelessWall Clients
Cranite WirelessWall Manager
Subnet 2
Cranite WirelessWall Access Controller
Existing Servers, including Authentication (e.g., RADIUS) and Authorization (e.g., LDAP, Active Directory)
Subnet 3
Cranite WirelessWall Access Controller

Figure 1: WirelessWall reference architecture

The WirelessWall Client also provides a powerful unified login option. In typical FIPS-certified solutions, a user logs into the local machine using cached credentials, then logs into the wireless network using domain credentials. While efficient from a security standpoint, two logins mean two challenges to the user. First, a user must log in twice, which is inconvenient. More importantly, two logins means that administrator-defined login scripts do not run at the time of attachment to the network, preventing the download of virus updates, software patches, etc. WirelessWall clients using unified login enjoy wireless network and domain authentication with a single login, ensuring execution of login scripts and further mitigating risk.

Role-Based Access Control and Policy Enforcement

A powerful feature of WirelessWall is its ability to enforce policies unique to each connection, including a policy allowing guest Internet access, enabling 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 enterprise network from unauthorized access.

WirelessWall implements its role-based firewall with robust policy capabilities based on highly granular network traffic filtering. A simple secure browser-based 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.

WirelessWall provides a number of parameters for policy editing and enforcement, including Membership, Per-frame characteristics and Duration.

Membership

Administrators apply policies based on the user’s group membership within the enterprise directory; WirelessWall supports integration with Microsoft’s Active Directory and NT Domain Server, as well as with LDAP. Integration with Active Directory and NT Domain Server is automatic, simply by installing the WirelessWall Directory Connector, a small application which runs on any Windows machine that is a member of the domain; integration with LDAP requires minor schema integration, dependent on the ownership LDAP architecture. This greatly simplifies ongoing management while lowering total cost of by ensuring that user moves, adds and changes within the enterprise directory automatically propagate throughout wireless access policies.

Per-frame characteristics

WirelessWall provides for significantly enhanced security versus typical wireless security solutions by enabling filtering of all traffic to and from the WirelessWall Client. This capability allows security and network administrators to segment and filter traffic based on user identification, network, protocol, and type of frame; these filters can be applied uni-directionally, providing for the creation of extremely granular network access policies. Policies are enforced at each WAC, even when a user roams between WACs on different subnets.

Duration

Administrators can configure session duration using two different methods—session length timeout and idle timeout. Administrators typically set session length to be slightly longer than the typical duration of the user’s workday; after this pre-defined period of time, the user will be prompted to re-enter his/her credentials to continue as an authorized user. The session length timer considers the mobile user roaming throughout the secure wireless network, ensuring that the user cannot bypass the session length timer simply by moving from subnet to subnet. Contrast session timeout, which is used as part of all policies, with idle timeout, which some enterprises may choose to not implement. Idle timeout is typically used in those environments requiring the utmost security; examples include healthcare, financial, and government applications. Administrators can configure very short idle timeout values to ensure that a user who leaves the mobile device idle is not placing the device (or network resources) at undue risk. For instance, a healthcare worker who leaves an authorized PC/PDA connected during a lunch break may be placing the enterprise at risk of violating HIPAA security guidelines. The ability for the session to automatically time out after an administrator -defined period of time is a powerfully elegant mechanism to provide additional security and management without compromising the user experience.

WirelessWall Session Model

Session Creation

WirelessWall's authentication process is managed using an IEEE 802.1x framework and TLC-specific protocol extensions to prevent session hijacking or denial of service attacks. A unique 802.1x port is created on the WAC for each active connection. By using two-way EAP-TTLS to protect the authentication process (see figure 2), administrators are assured that the user's credentials are immune to attack and compromise. As part of the authentication process, a TLS master secret is derived, which is used in the dynamic generation of per-user, per-session AES data privacy and HMAC SHA-1 message integrity keys. FIPS 140-2 validation ensures that this process occurs according to rigorous, defined guidelines, providing administrators with mutual authentication.

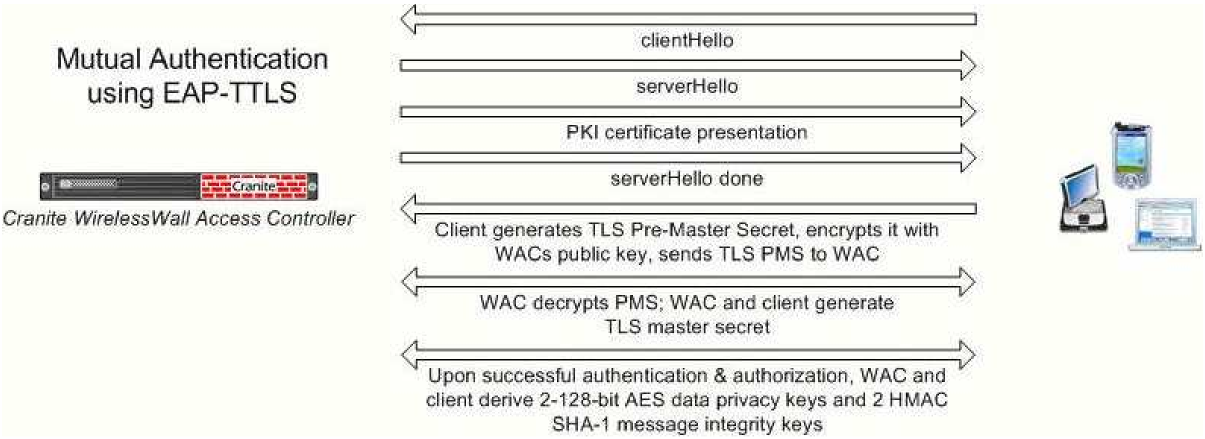
Mutual Authentication using EAP-TTLS
Cranite
Cranite WirelessWall Access Controller
clientHello
serverHello
PKI certificate presentation
serverHello done
Client generates TLS Pre-Master Secret, encrypts it with WACs public key, sends TLS PMS to WAC
WAC decrypts PMS; WAC and client generate TLS master secret
Upon successful authentication & authorization, WAC and client derive 2-128-bit AES data privacy keys and 2 HMAC SHA-1 message integrity keys

Figure 2 – Sessions and 802.1x states

Maintaining Sessions

Once the secure session is established, the Client and the WAC fully authenticate each frame by 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.

Ending Sessions

All WirelessWall sessions expire after an administrator-defined period of time, configurable per policy. Ten minutes prior to the session's scheduled expiration, the user is prompted to provide authentication credentials so the session can continue without interruption. If the user is not available to provide credentials, the session expires on all WACs simultaneously, and all session keys are erased.

Mobilizing Sessions

WirelessWall supports three types of secure mobility. The basic mechanism for re-establishing a connection between the Client and a new WAC is the same for all three mobility modes. Upon the successful creation of a new session, the Manager downloads the security context to all available WACs. This information is used to facilitate low-latency handoffs as users roam between WACs. When the Client roams from one WirelessWall-secured subnet to another and establishes a new radio connection, the new WAC uses the Client's session context (pushed to each WAC when the user originally established the session) to complete an abbreviated TLS handshake. In doing so, the Client is securely authenticated on the new WirelessWall-secured 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. As noted, WirelessWall provides three options for robust mobility support—the option for a user to maintain an IP address as he/she roams between subnets, ensuring application integrity; the option for a user to always attach to a given subnet, appropriate for those enterprises using static IP addresses; and the option for a user to receive a new IP address each time he/she roams between subnets. The first option is the option used in the vast majority of cases.

Encryption

The Advanced Encryption Standard (AES)

WirelessWall utilizes AES to protect sessions and networks from attack and compromise. AES is a Federal Information Processing Standard (FIPS) which 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 using WirelessWall. In particular, AES is ideal for lightweight hardware devices such as PDAs, ensuring maximum battery life and throughput by minimizing processing needed to execute encrypted sessions. Contrast AES with Triple DES, which can suffer overhead of 30% or more; further, the processor-intensive nature of Triple DES will drain battery life at a much greater rate than will AES.

Due to its performance characteristics, AES is specified as the data privacy algorithm in the 802.11i security standard. However, since existing 802.11a/b/g/j/n network interface cards and access points employ encryption mechanisms (WEP, Dynamic WEP, WPA) using hardware-based RC4, the vast majority of existing access points will need to be replaced (either in whole or in part via a firmware and/or radio card upgrade) to support 802.11i. WirelessWall offers all the benefits of AES-based data encryption today , while adding significant enterprise-level management and mobility features which are not 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 to move to 802.11i; standards-based products can be used in a "mix and match" environment, further increasing return on investment while lowering total cost of ownership.

Future Standards Architecture Today

WirelessWall deviates from 802.11-2007 in some aspects to overcome deficiencies that are corrected in future, upcoming standards in IETF Working Groups:

1. 802.11-2007 calls for Security identification and negotiation in 802.11 *management frames*. WirelessWall is compliant with the RSNA (AES-CCMP, 1x), but does not use management frames because:

Supporting this requirement literally would require the ability to control / override firmware logic in existing Access Points. This is vendor specific. The lack of a vendor neutral way of configuring and provisioning access points is a well **known deficiency** in the current 802.11 standard. IETF is developing a standard called the Control And Provisioning of Wireless Access Points (**CAPWAP**) to rectify this deficiency.

WirelessWall delivers the only solution to support everything TODAY, given the state of the standards and industry.

WirelessWall supports standards-compliant key negotiation, encryption and authentication, but only after the Discovery Phase of 802.11 protocols and after association. This provisioning approach does not compromise security in any way, and allows WirelessWall to provide RSN (WPA2-Enterprise class) security even to APs that do not support it. In fact, it does not require the AP to be preprovisioned for security at all.

2. 802.11-2007 calls for key material and 1x authenticator support on the AP. WirelessWall does not do this because:

This is a **known weakness** in the standard because it offers no security between the AP and the Data Center, only between the user and AP. In CAPWAP terminology, this is a **Local AP**. The AP is often connected to the Data Center via long haul wireless bridge, or wire. The LocalAP secures the perimeter but leaves the AP vulnerable to wiretap or physical penetration (i.e., the AP can be stolen, hacked and spoofed).

The **CAPWAP Taxonomy** extends the security boundary by also allowing a **Split AP** architecture such that the data plane between the AP and AC to be encrypted for end-to-end protection.

WirelessWall provides a Split AP architecture with end-to-end security protection TODAY.

3. WirelessWall does not publish the security method in the beacon or probe response. Again, this is primarily because it must operate after Discovery to a) support legacy devices and b) retain vendor neutrality. The secondary reason is to provide *obfuscation* of to **cloak** the security method, which leave conventional APs vulnerable to future attacks.

Conclusion

Wireless LANs are a dynamic, unique and popular technology. IT professionals who grasp the tenets of holistic security design will understand that common wireless LAN security solutions which treat the wireless LAN as a hostile entity are not sufficient for truly secure enterprise-wide deployment . IT professionals will also understand that a well-designed solution for securing, mobilizing and managing wireless LANs should integrate seamlessly into existing enterprise network design and network management principles.

WirelessWall is a unique solution to treat security, mobility and management with equal importance without compromising any of the three:

1. Security – WirelessWall operates at Layer 2 of the OSI stack, providing the utmost level of protection against attacks end-to-end, protecting the crucial distance between the APs and data centers that conventional networks expose.

2. Mobility – WirelessWall supports a highly mobile, vastly scalable enterprise user community with simple, elegant, secure roaming that provides a seamless user mobility experience while making the IT administrator's job easier.

3. Management – WirelessWall enables administrators to utilize existing enterprise directories to manage and secure wireless LAN connections, regardless of the access infrastructure protocol or vendor.

WirelessWall is ahead of 802.11-2007, and in the spirit of the IETF CAPWAP Taxonomy, which permits key material and configuration currently done at the AP to be done at either the AP or the AC (Access Controller). Besides more flexible provisioning and security management in the AC, the CAPWAP architecture improves security by allowing the data plane between the AP and AC to be encrypted for end-to-end security. This is precisely what WirelessWall can accomplish today.

About TLC Secure, Inc.

TLC Secure, Inc. secures enterprise wireless local area networks by providing WirelessWall, the industry's only FIPS 140-2 certified Layer 2 software security solution. WirelessWall encrypts full Ethernet frames, rather than just IP payloads, hiding vital information such as IP addresses, applications and ports from unauthorized listeners. Frame-level encryption also protects non-data network traffic, including DHCP requests or ARP messages, which can be compromised and used to attack the network. This approach helps protects both the user's data and the organization's network, while enabling users to securely roam across subnets without needing to re-authenticate or reboot, saving time and minimizing frustration.

Response to JSIC Questions

Joint Forces Command (JFCOM), Joint Systems Integration Command (JSIC) has a multi-vendor testbed that configures WirelessWall to provide uniform security to a combination of many vendors' Access Points. On 23 April 2008, TLC received a list of several questions regarding the use and architecture of WirelessWall. The following is an initial response to those questions.

1) WPA2: You are not WPA2. Is this because you have not gone through WiFi Alliance certification? Why haven't you?

Answer: WirelessWall offers L2 security in software and Wifi Alliance does NOT certify software -- only WiFi hardware devices.

WirelessWall best meets the “Wireless Gateway/Firewall“ description in section 2.2.2.1 of the DoD Wireless STIG v5 Release 2: http://iase.disa.mil/stigs/stig/wireless_stig_v5r2.pdf ; it should not be considered WiFi hardware, but is a FIPS 150-2 certified a Gateway/Firewall which complements WiFi certified devices such that it can secure, manage and filter content on those devices.

2) 802.11i: Do you consider yourself compliant with IEEE-2007 clause 8 (formerly 802.11i)? Why or why not? (Very technically specific would be most helpful)

Answer: Yes (qualified). However 802.11i supports four modes in the table below, we exclusively support the strongest WPA2 Enterprise Mode. The gray shaded blocks are those we do NOT support.

Mode	**WPA**	**WPA2**
Enterprise Mode **(Business, Education, Government)**	**Authentication:** IEEE 802.1X/EAP **Encryption:** TKIP/MIC	**Authentication:** IEEE 802.1X/EAP **Encryption:** AES-CCMP
Personal Mode **(SOHO, Home/Personal)**	**Authentication:** PSK **Encryption:** TKIP/MIC	**Authentication:** PSK **Encryption:** AES-CCMP

802.11i (IEEE 802.11-2007) modes

We represent the Robust Security Network (RSN) and do not support the interim TKIP Message Integrity Check, or Pre-Shared Keys (Personal Mode) since those offer weaker security. We do not use TKIP because even with larger IV it still uses the RC4 has numerous weaknesses exploiting the correlation between keystream and the key. The FMS attack (see http://en.wikipedia.org/wiki/Fluhrer%2C_Mantin%2C_and_Shamir_attack) and Klein attacks are well known and exploited with freeware hacking tools. WPA-PSK was not supported due to vulnerability of the passphrase to brute-force dictionary attacks. WirelessWall uses AES CRR with CBC-MAC (CCMP) as described in Clause 8.3.3.

WirelessWall goes *beyond* 802.11-2007 Local AP model to provide a Split AP taxonomy similar to the forthcoming IETF CAPWAP, which corrects weaknesses by supporting storage of key material and 1x Authenticator codes on the AC instead of the AP. Conventional APs merely secure the AP to STA (clients) and leave the backend vulnerable and unencrypted. WirelessWall uniquely provides **end-to-end** security and protects against physical compromise of the AP or tapping of the critical AC-to-AP link across wire or long-haul wireless bridges.

3) CCMP: I believe that I've seen in your documentation that your cipher & key management is AES with CCMP. The FIPS certificate specifies AES (along with other algorithms), but does not mention CCMP. On the other hand, it doesn't mention any other key management methods either. So the question is : ARE you using CCMP, or is it an older RC4 technology or ???

Answer: Yes, WirelessWall uses CCMP, not RC4. The details about WPA2 and AES-CCMP boil down to WirelessWall being ahead of the standards and NIST. Please note:

The original WirelessWall certificates are at:
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#311 and
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#635
The Security Policy details what was tested and certified:
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp311.pdf

Please refer to section 6 , where it specifically lists **AES modes ECB, CTR and CBC**. What is called AES-CCMP today is (CTR mode CBC).

WirelessWall was tested and certified in 2003, **before** the 802.11i standard and WPA2 mode became a standard. It was also **before** NIST began testing AES-CCMP (aka the CCM Validation List), which are based on NIST Special Publication 800-38C, published in May 2004:
http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf

It is compliant, but released well before there was any certification for CCM.

4) EAP-TTLS: Your documentation states that's the encapsulation you are using. It appears that EAP-TTLS can be set up as either one-way or two-way authentication. Is WirelessWall EAP-TTLS method set up as 1-way or 2-way? Please explain why you say it is 1-way or 2-way.

Two-way. Certificates are installed on both the WAC and all clients. WirelessWall requires mutual authentication.

5) Proprietary Frames: Where are proprietary Cranite frames used? (Not asking for trade secrets, only what you can publicly share.)

In encrypted mode, Ethertype **0x0c0c** is used. Over the air, that is encapsulated.

6) Initial login: During initial login between client and AC, before an IP address is acquired from the DHCP server, what technique is used to communicate between the client and the AC?

802.1X is the authentication protocol. The 1X state machine is handled between the three entities: 1) the **Supplicant** built into the WirelessWall client, 2) the **Authenticator** on the WirelessWall Access Controller and 3) the (RADIUS client) and the **Authentication Server** (external RADIUS Server) on the trusted network. The state machine dictates the Port Access Entry (PAE) to determine whether the client stays in a cryptographically secure state (WirelessWall on) or goes into an unsecure (WirelessWall off) state.

7) ARPs: When logging into the system and running Air Magnet, Air Magnet is picking up some ARPs, which contain IP addresses of both the client and the internal network server, in the clear, over the air. Thoughts?

This should not be possible when in encrypted mode. We assume you're using AirMagnet to do wireless sniffing. We provided Wireshark sniffer output of a typical exchange and see no visible IPs. ARP would not occur until encrypted session establishment and DHCP is renewed. Our tests confirm this.

8) PKI: Some on your team there have told us before that WirelessWall is not PKI capable. However, we have found a Whitepaper with TumbleWeed and Cranite logos explaining that by using the two products together one can enable PKI (CAC card) logins? Confused, what's ground truth and why are there 2 stories going around?

Version 3.4 of the client and 4.1 of the server support CAC Smartcard and Single-Sign-On. They support OCSP and encapsulate smartcard certificates in the EAP-TTLS authentication TLVs. However, these changes to the client and server is not part of the certification.

The vendor is currently in discussions with the certifying laboratory (Infogard) to obtain a approval as an update, since the new TLVs change the content of the user credentials passed through the tunnel, and not the cryptographic boundary itself or the user roles. This would therefore be a version update not requiring full revalidation.

9) Interoperability with Meru: We have reported to you an interoperability problem we encountered between WirelessWall and Meru. Any new developments there?

The JSIC testing was reported to be done with the Meru Networks AP200 and the MC1000 controller. It was reported that the test configuration, the network switch permits access to the AP200 directly to the WAC, versus through the MC1000. The vendor suggested setting the adapter on the client to a static IP address in case there is a DHCP fragmentation issue on the Meru, since DHCP uses larger packets. This has yet to be confirmed.

Support Capability

The JSIC testing center inquired about support capability for support. TLC offers a range of support options that can be tailored to meet your specific needs. When 24x7 Platinum is purchased, we provide the customer with their own unique telephone number for first response, manned by human operators, and an escalation process for rapid technical/engineering support. Platinum is detailed below, compared with Gold Support:

TLC Customer Support Programs		
Customer Support Key Features	24x7 Platinum Support	8x5 Gold Support
Support Service (Email and Web Portal)	X	X
Support Services (Telephone)	X	X
Call Response & Escalation Procedures		
Number of Service Requests	Unlimited	Unlimited
Access to FAQs on Website	X	X
Maintenance Update & Upgrade Releases	X	X
Authorized Contacts	(Five)	(Two)
Product Security Advisories	X	X
Quarterly Customer Newsletter	X	X

TLC Product Training Discount	(10%) 1	
Severity Levels 2	X	X
Round-the-clock Customer Support *	X	
Configuration Analysis	X	
Priority Call Response	X	
Critical Problem Alerts	X	X
Support Access	24x7	11x5

1 Subject to availability.
2 See Severity Levels chart.
* Production down calls only for after-hours only.

We use the following guide for assigning severity levels and the targeted initial response times as shown below.

Severity Levels		
Severity	Service Request Description	Response Time
Severity 1	Production Issue - System down; virtually complete interruption rendering the product inoperative.	2 hours
Severity 2	Production Issue - Serious impact to business.	6 hours
Severity 3	Production or Pre-production Issue - Minor impact.	1 business day
Severity 4	Configuration - Environment or product (e.g. how-to), general inquiries.	2 business days