THE TOLLY GROUP

No. 204144 November 2004

Aruba Wireless Networks

Aruba 5000 WLAN Security System

Competitive Security Evaluation

1989 - 2004 15 Years TOLLY

Test Summary

Premise: *There are inherent advantages in blending the power of Layer 2/3 switching, authentication and firewalling into the same device primarily since a stateful firewall collocated on the same device that controls the WLAN can help secure voice communications to mobile users. Such a dual-function device can assign a "role" to a user on the basis of various factors such as the SSID, the authentication method, RADIUS attributes and then apply firewall policies on a per-user basis.*

Aruba Wireless Networks commissioned The Tolly Group to evaluate its Aruba 5000 WLAN switch that combines 10/100/1000 Mbps Ethernet switching with stateful LAN-speed firewalling, VPN concentrator features and a variety of wireless security services.

The four-slot Aruba 5000 WLAN switch centralizes administration and processing of features such as 802.1X authentication, authorization and access control, encryption/decryption and mobility management. It represents one of the few systems that centralizes all encryption thereby providing device-to-data center privacy.

Aruba asked The Tolly Group to compare the security features/functions of the Aruba 5000 against the Airespace 4012 WLAN switch. As per its Fair Testing Charter, The Tolly Group invited Airespace to participate in the test, review test methodology and comment on test results. The company responded by threatening legal action if The Tolly Group tested its product without explicit permission which it ultimately declined to give. The Tolly Group did not test the

Test Highlights

- Provides enhanced security by mapping security policies to the state/role assigned to each user as opposed to mapping policies to an IP address or a subnet, which can be compromised
- Secures voice over wireless communication through traffic flow classification and stateful packet inspection facilities
- Guards against man-in-the-middle attacks by performing all encryption/decryption at the switch, thus securing traffic between the access point and the switch
- Implements a stateful firewall on the switch to blacklist immediately any misbehaving clients which prevents AP-to-switch links from becoming congested with malicious traffic

WLAN Switch Security Comparison

Feature	Aruba 5000 WLAN Switch	Airespace 4012 WLAN Switch
	Tested	Vendor refused to test
Stateful firewall integrated on the WLAN switch	Yes	No[1]
Point of encryption/decryption	Switch	Access point[1]
WLAN switch can automatically blacklist a misbehaving client	Yes	No[1]
IP spoofing / ARP poisoning can enable wireless client assuming additional privileges	No	Yes[1]

[1]Since Airespace threatened legal action if the company's product was tested, their "results" are derived from correspondence with them, as well as publicly available product documentation.

Source: The Tolly Group, August 2004 *Figure 1*

Tolly Verified LAN & WLAN Certifications Earned – Aruba 5000		
Certification ID	**Certification**	**Category**
10508	10/100 Auto-negotiation	LAN Connectivity
10514	Auto MDI/MDIX	LAN Switch Core
10515	Port Mirroring	LAN Switch Core
10532	VLAN Support (IEEE 802.1Q)	LAN Switch Core
10564	Virtual Router Redundancy Protocol (VRRP)	LAN Switch Core
10574	Cisco Fast EtherChannel support	LAN Switch Core
10594	Redundant Power Supply - (hot swappable)	High-Availability Core (Product-type Independent)
10638	Power over Ethernet Provider/Recipient	WLAN Switch/Radio Core
10715	Different Security Policy per SSID	WLAN Switch/Radio Core

Source: The Tolly Group, August 2004 *Figure 2*

Airespace 4012 but instead relied upon publicly available information and on-the-record Airespace comments to make comparisons between the products (for a deeper understanding of the interaction between The Tolly Group and Airespace, see the report section, "Equipment Acquisition and Support." Readers may also view a complete copy of Airespace's official position statement to The Tolly Group by following a link at: http://www.tolly.com/DocDetail.aspx?DocNumber=204144.)

Tolly Group engineers exposed the Aruba 5000 switch to three security scenarios to determine its effectiveness at securing communications between the switch and various access points (APs). The Aruba 5000 was subjected to three security tests:

- A secure voice test,
- A variant of the "man-in-the-middle" attack, and
- A wireless intrusion prevention scenario.

In every test instance, the Aruba 5000 demonstrated its security effectiveness. (See Figure 1.) The Tolly Group also validated more than 20 key functions on the Aruba 5000 WLAN switch under its Tolly Verified certification program. Testing was conducted in August, 2004

Results and Analysis

Secure Voice Scenario

In this scenario, engineers used SIP-based phones and a discrete SSID for voice traffic to verify the capability of the Aruba 5000 to allow only SIP voice traffic and ensure that a second device could not access the same SSID to transmit data traffic.

Testing demonstrated that the Aruba 5000 does not utilize IP subnet addresses to distinguish between traffic from different SSIDs. Instead, the system integrates packet inspection hardware and software to distinguish between different traffic and application types. The Aruba system assigns a "role" or policy to each SSID and manages traffic via the SSID. Since Aruba integrates a stateful firewall into its Aruba 5000 WLAN switch, it retains complete knowledge of the state of the client including the SSID to which the client is associated. Therefore, the switch never grants a client associated to a voice SSID more permissions (and bandwidth, if so configured) than required.

By contrast, publicly available information shows that the Airespace 4012 does not provide any integrated stateful firewalling function within the switch. In fact, not only does Airespace not claim to implement such a firewall feature but the company has gone on record stating that such a design is a bad idea and has even published a white paper to this effect – Integrating Firewalls into Enterprise WLANs (http://www.airespace.com/technology/integrating_firewalls_into_enterprise_wlans.php). Thus, it is clear that they do not have this feature.

Instead, Airespace's security solution must depend on an external firewall to provide the security. However such an implementation doesn't allow firewalling functions to retain user context. By the time traffic reaches an external firewall, users have been authenticated.

In such a security solution, the differentiation between the two types of users (voice and data) occurs at the external firewall, not at the switch. Generally, the only information that the firewall

utilizes to differentiate between users is their IP addresses or their subnets. In a typical scenario, an SSID is mapped to a VLAN/subnet and thus different types of users will be using IP addresses from different IP address pools.

If a client on the voice SSID spoofs an IP address from the subnet belonging to the data SSID, the firewall does not have any means to detect this and thus allows complete access to the client. This is especially relevant as the WLAN security policies are often less secure for voice clients (as the phones often cannot perform 802.1X or implement a VPN endpoint etc.).

Airespace acknowledges that the security vulnerability stems from the fact that almost all current handsets use WEP for security and generate a constant stream of packets, according to Alan Cohen, Airespace's vice president of product marketing and product management. "The movement of 802.11i into the VoWLAN market is coming and will play a big role here. Firewalls are a potential component, but not the only one to providing advanced security in voice," Cohen said in Airespace's official statement to The Tolly Group (See Equipment Acquisition and Support section.)

Man-in-the-Middle Attack Variant

This test was designed to examine how the centralized encryption model of the Aruba 5000 protects against an attack that intercepts the data between an access point and the WLAN switch/controller. Engineers attempted to demonstrate the Aruba 5000's centralized encryption model by securing the communications between the WLAN switch and the AP by using Aruba's encryption to avoid a man-in-the-middle attack from inside the firewall.

Engineers inserted a LAN analyzer between a downstream AP and the Aruba 5000 and tried to capture packets using a hub attached to the test network. (While today's networks are switched, those switches implement "mirror ports" which allow technicians visibility into traffic on any port.) The laptop-based analyzer attached to the hub successfully captured packets from the link between the switch and the AP. But analysis of those packets determined that data was encrypted via the Dynamic WEP encryption scheme. Engineers tested packets flowing from the Aruba 5000 to the AP, and also from the AP to the switch. In both cases, traffic was encrypted to thwart

Aruba Wireless Networks

Aruba 5000

Enterprise Security Effectiveness

Aruba Wireless Networks
Aruba 5000
Product Specifications*

- Integrated crypto hardware provides high-speed, centralized encryption (WEP, AES, 3DES, TKIP etc.)
- Modular chassis-based WLAN switch with a built-in stateful firewall and VPN concentrator
  - Supports up to 256 access points, 4,096 simultaneous wireless users
  - Accepts native 802.11 traffic for processing
- Integrated RF management and optimization
- ICSA-certified firewall
  - Flow classification and identification
  - Application aware (eg. FTP, SIP etc.)
  - Bandwidth contracts per user
- Integrated crypto hardware provides high-speed, centralized encryption (WEP, AES, 3DES, TKIP etc.)
- Subscriber management using stateful firewall.
- Up to 4,096 VPN IPSec, L2TP and PPTP tunnel terminations
- 8 Gbps clear text throughput, and 3.6 Gbps 3DES encrypted IPSec throughput
- QoS using per-user bandwidth contracts, 802.1p support and DSCP tagging.
- Clientless inter-subnet and inter-switch mobility using proxy Mobile IP and proxy DHCP
- 802.11 Transport, Authentication and Encryption
- Three-dimensional RF site survey
- Distributed and centralized AP calibration
- Wireless RMON and packet capture
- Complete wireless IDS
- Rogue AP detection and containment
- Man-in-the-middle attack detection and prevention
- Station and AP classification
- Wireless bridge detection
- Other wireless IDS functionality such as detection of Weak WEP IVs, ad-hoc network detection etc.

For more information contact:
Aruba Wireless Networks
1322 Crossman Avenue
Sunnyvale, CA 94086
Phone: (408) 227-4500
Fax: (408) 227-4550
URL: http://www.arubanetworks.com

**Vendor-supplied information not verified by The Tolly Group*

man-in-the-middle attacks. The Aruba 5000 also supports additional encryption schemes including 820.11i, PPTP and L2TP over IPSec.

While Airespace would not permit testing of its Airespace 4012 switch, we can still consider the relative effectiveness of its implementation approach. In a security solution like the Airespace 4012, encryption/decryption takes place at the AP rather than at the WLAN switch. The inherent assumption behind doing encryption/decryption on the AP is that the wired network to which the AP is connected to is secure. However, this is not always true. A hacker (who can also be an insider) can corrupt the ARP cache of the AP and its gateway and sniff any packets traversing the connection between the AP and the switch. This scenario leads to a security hole where VoIP traffic can be sniffed to snoop on voice calls as the packets are still in the clear. The same argument applies to data traffic between the AP and the WLAN switch, and the traditional approach of using distributed encryption/decryption presents security weaknesses to man-in-the-middle attacks.

While Airespace acknowledges support for IPSec communications[2], the company also has promoted a non-standardized AP-to-switch communications mechanism called the Lightweight Access Point Protocol (LWAPP). LWAPP governs how access points and other devices communicate with each other. LWAPP has had limited acceptance from a handful of other vendors.

Wireless Intrusion Prevention Scenario

In this test, engineers examined the capability of the Aruba 5000 to blacklist a station automatically that is misbehaving at the TCP level.

[2]Airespace white paper: WLAN Security: Top 10 Checklist, December 10, 2003 http://www.airespace.com/technology/wlan_security_checklist.php#three

Management & Security Tolly Verified Certifications Earned – Aruba 5000

Certification ID	Certification	Category
10518	Dual firmware images	System Management
10519	Dual configuration images	System Management
10526	Save/Load Configuration to Text File	System Management
10555	System Upgrade via Trivial File Transfer Protocol (TFTP)	System Management
10572	Embedded Web Management	System Management
10788	System Upgrade via File Transfer Protocol (FTP)	System Management
10559	User Authentication via IEEE 802.1X	Systems Security and User Management
10570	User Authentication via Local User Database	Systems Security and User Management
10746	802.1X - Single-port, "Per-MAC" Authentication	Systems Security and User Management
10748	Web Browser-based Authentication	Systems Security and User Management
10749	URL "Hijacking"	Systems Security and User Management
10750	URL Automatic Redirect After Authentication	Systems Security and User Management

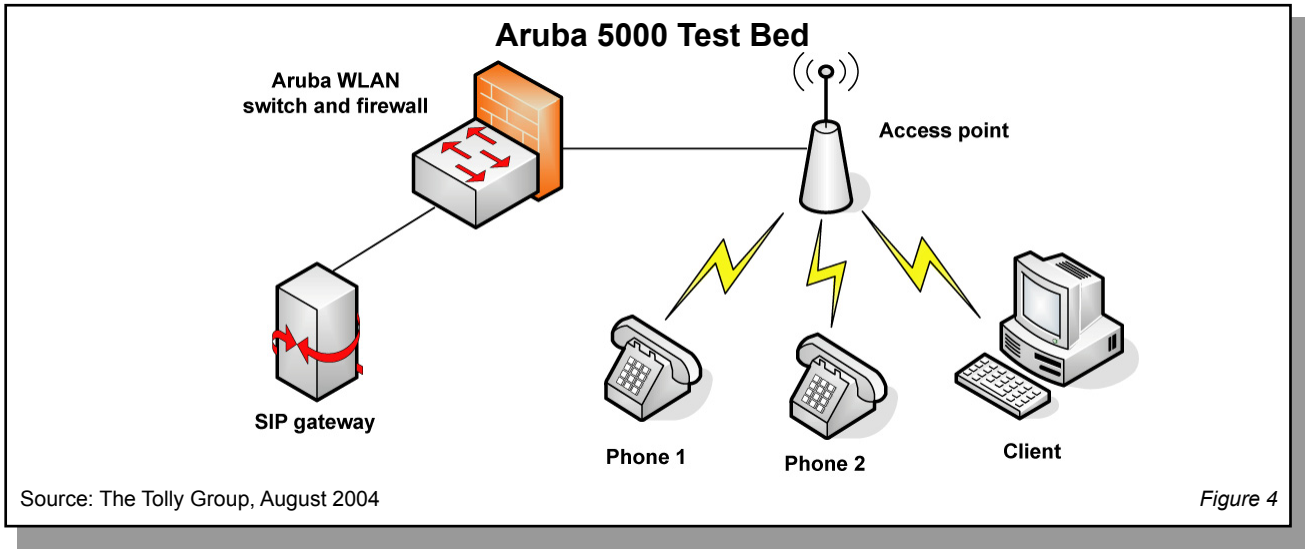
Source: The Tolly Group, August 2004 *Figure 3*

The Wireless Intrusion Prevention test was verified through screen captures of the Aruba 5000 console that the WLAN switch automatically blacklisted a client that violated the role assigned to the SSID with which it associated with the WLAN switch. Engineers confirmed that a misbehaving client was blocked or blacklisted by verifying that the client could not send any traffic through the WLAN switch and by verifying that the management console screen of the Aruba 5000 shows that this misbehaving client had been blacklisted.

This test shows the additional actions that can be taken when detecting a misbehaving client due to the presence of a stateful firewall integrated with the switch on the WLAN infrastructure. If the firewall detects a policy violation (such as TCP traffic on a port known to be a part of a malicious attack on a SSID/role only for VoIP phones), it can immediately blacklist this client. Not only does this shut down the malicious client but it also ensures that the misbehaving client cannot clog up the channel between the AP and the switch.

In a traditional WLAN solution, such as the Airespace 4012, the firewall functionality has to be implemented in a separate device. As a result, there is no possibility to take any such action when such a policy violation is detected. Even though the traffic from the misbehaving client is dropped at the firewall, the malicious/misbehaving client can congest the communication channel between the AP and the switch, thereby denying service to legitimate wireless clients.

Airespace does not endorse automatic blacklisting. In fact, the company says blacklisting was never designed to keep "different types of traffic" off



Source: The Tolly Group, August 2004

Figure 4

an SSID, according to Cohen. "That is what ACLs are used for," he said[3].

Tolly Verified Certifications

Tolly Group engineers certified more than 20 features/functions of the Aruba 5000 WLAN switch. (See Figures 2 & 3.) These 20 certifications are in addition to 16 earned during an earlier test. For a detailed explanation of specific Tolly Verified tests, visit on the Web at http://www.tolly.com/TVDetail.aspx?ProductID=105.

Test Configuration and Methodology

For all performance tests, The Tolly Group tested an Aruba 5000 WLAN switch running software version: 2.2.1.0.

The switch was connected to a Layer2/3 network that linked to an Aruba AP52 access point, running boot code 1.2 software. The switch also provided connectivity to a corporate network.

For the secure voice test, engineers used a wireless client to attempt to authenticate and associate using a particular SSID with the wireless AP. Engineers used screen captures of the Aruba 5000's management console to verify success/failure of the association attempt. They then verified through the Aruba 5000 management console that the switch denied traffic from a client which spoofed the IP address corresponding to a different SSID. (See Figure 4.)

For the man-in-the-middle attack variation test, engineers used an Airopeek NX analyzer to capture packets on the wireless network (AP to wireless client) and also used an Ethereal analyzer to capture packets on the wired network between the WLAN switch and the AP. In Aruba's case, Airopeek NX packet captures and Ethereal packet captures indicated the presence of encryption in both directions. (See Figure 5.)

For the intrusion detection test, engineers utilized screen captures from the Aruba 5000 console to show that the WLAN switch automatically blacklisted a client that violated the role assigned to the SSID with which it associated. It was confirmed that the misbehaving client had been blocked and blacklisted by verifying that the client could not send any traffic through the WLAN switch and by verifying that the management console screen of the Aruba 5000 showed that the misbehaving client had indeed been blacklisted.

Equipment Acquisition and Support

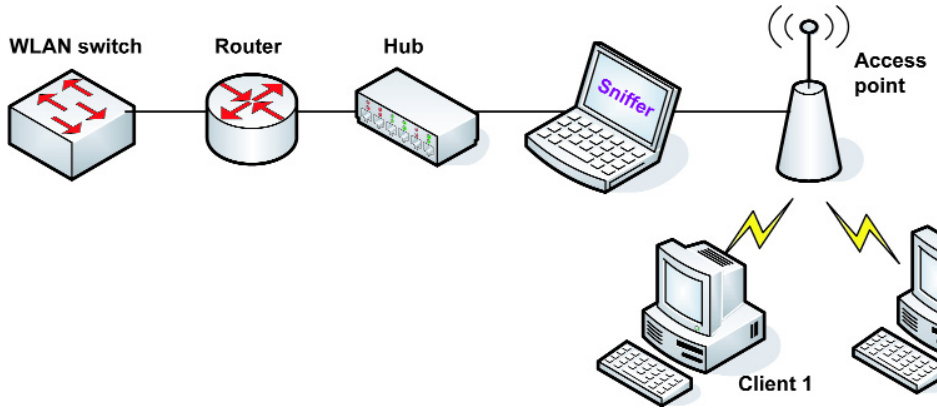
In accordance with its Fair Testing Charter, The Tolly Group approached Airespace and invited the company to participate in the testing project. Airespace immediately declared that any testing of the company's product in any way without its explicit permission would violate the end-user license.

As stated by Airespace VP Alan Cohen in E-mail correspondence to The Tolly Group's Operations Manager on Wednesday, 11 August 2004 4:03 p.m.: "As we went through the prior time, our end-user license explicitly cites that our equipment cannot be used for any purpose except for the purpose it was intended, which is WLAN services in the enterprise. Any use of our equipment, without our explicit written consent, violates the license. Violation of our license will result in us going to a judge and getting an injunction to get Tolly to cease and desist (this provision is the EULA). We we (sic) prosecute violation of our license to the full extent of the law."

The Tolly Group offered to conduct the test at Airespace's site using the company's own equipment. After reviewing the test plan, Cohen pro-

[3]Airespace's Alan Cohen comment from an E-mail correspondence to Kevin Tolly, dated Thursday, 28 October 2004 10:15 a.m.

Aruba 5000 Secure Voice Test Bed



Source: The Tolly Group, August 2004

Figure 5

vided a critique and renewed the company's statement that any test would result in Airespace seeking an injunction. The Tolly Group notified Airespace that it intended to publish a document related to this project which would reflect the stance that Airespace took. Furthermore, The Tolly Group invited Airespace to provide an official position statement, which it did.

Readers may view a complete copy of Airespace's official position statement to The Tolly Group by following a link at http://www.tolly.com/DocDetail.aspx?DocNumber=204144.

The Tolly Group gratefully acknowledges the providers of test equipment used in this project.

Vendor	Product	Web address
Ethereal	Ethereal Ver 0.10.6	http://www.ethereal.com
WildPackets	AiroPeek NX Ver 2.0	http://www.wildpackets.com

Tolly Group Services

With more than 15 years of testing experience of leading-edge network technologies, The Tolly Group employs time-proven test methodologies and fair testing principles to benchmark products and services with the highest degree of accuracy. Plus, unlike narrowly focused testing shops, The Tolly Group combines its vast technology knowledge with focused marketing services to help clients better position product benchmarks for maximum exposure. The company offers an unparalleled array of reports and services including: Test Summaries, Tolly Verifieds, performance certification programs, educational Webcasts, white paper production, proof-of-concept testing, network planning, industry studies, end-user services, strategic consulting and integrated marketing services. Learn more about The Tolly Group services by calling (561) 391-5610, or send E-mail to sales@tolly.com.

For info on the Fair Testing Charter, visit: http://www.tolly.com/Corporate/FTC.aspx

Project Profile

Sponsor: Aruba Wireless Networks

Document number: 204144

Product class: WLAN switch

Products under test:

- Aruba 5000 software version: 2.2.1.0

Testing window: August 2004

Software status:

- Generally available

For more information on this document, or other services offered by The Tolly Group, visit our World Wide Web site at http://www.tolly.com, send E-mail to sales@tolly.com, call (561) 391-5610.

The Tolly Group doc. 204144 rev. clk 18 Nov 04