

Taking Control Of Your Airwaves

Edwin E. Mier, David C. Mier and Robert B. Tarpley

Four leading packages show great restraint in tethering your wireless environments.

Ed Mier is an industry analyst, consultant and author, and also founder of Miercom, a network consultancy and product test center based in Cranbury, NJ. Dave Mier is a senior technical engineer, and Robert Tarpley is a test engineer at Miercom. They can be reached at edmier@miercom.com, dmier@miercom.com and rtarpley@miercom.com.

One early casualty of the Wi-Fi revolution has been security. Unmonitored and unchecked, wireless may be extending your network to locations you never knew or intended, leaving security holes big enough to drive a bus through.

A new class of “wireless security systems” has emerged in response. And that’s what *BCR* and Miercom, in this latest Best-in-Test review, sought to evaluate.

So what do these products do? Our research distilled five key wireless-oriented, security-related functions that these systems address, albeit to varying degrees:

1. Authenticating wireless users; that is, making

sure wireless clients are authorized, and are who they say they are.

2. Defending the “wired” network from threats that may enter through wireless LAN access points (APs).


3. Protecting the integrity of wireless transmissions, typically through encryption, from unauthorized interception.

4. Detecting, monitoring—and to some extent locating—unauthorized wireless APs.

5. Counterattacking by disabling such “rogue” APs—what the industry calls “containment” or “mitigation.”

We identified nearly a dozen vendors with packages claiming to address three or more of these functions, and invited them to submit their wares to Miercom’s main lab test facility in central New Jersey for this review. Several candidly admitted their packages weren’t yet ready for competitive review. A few others declined, saying

TABLE 1: Scorecard—Wireless Security Systems

					
	Percent Weighting	Aruba 2400 Wireless LAN Security System	Bluesocket WG-2100 Wireless Gateway	Chantry BeaconMaster 1200	Meru Networks MC 1100 Controller
Configuration (1)	20	85	85	90	80
Security Features (2)	30	90	83	75	84
Management and Administration (3)	25	88	86	88	82
Performance (4)	25	90	81	80	75
The Bottom Line	100	89	84	83	80

(1) Product package, including: capacity (number of Access Points, or APs, supported), radio technologies supported, whether APs offered and third-party APs supported, architecture, throughput capacity and up-link options and other deployment characteristics.

(2) Includes: rogue-AP detection and containment, encryption implementation, integral support for Intrusion Detection/Prevention Systems (IPS/IDSs), firewall features, VPN handling and other security features and aspects.

(3) Includes: Special wireless and security-oriented applications, such as for AP placement, Web GUI navigability, configuration and management applications, wizards, usage and security reports, audit and alerting features, and related management and administrative aspects.

(4) Throughput for unsecured versus secure environments; latency and jitter, for single versus multiple clients and for unsecured versus secure environments; roaming hand-over times; rogue-AP detection and containment effectiveness; controller reboot and failover times and other metrics.

the timing of our summer testing wasn't right for their next releases.

Four vendors accepted and were tested:

■ **Aruba Networks**, which submitted its 2400 Wireless LAN Security System, featuring an appliance-type server with an integral 24-port switch. We tested the system using Aruba's own APs, although popular 3rd party APs are supported as well.

■ **Bluesocket**, which sent us its WG-2100 Wireless Gateway, an appliance-type server, and its just-released BlueSecure add-on monitoring subsystem. Bluesocket doesn't offer its own APs, but works with popular 3rd party APs. The package was tested with Cisco Aironet 1100 APs.

■ **Chantry**, which provided its BeaconMaster 1200 appliance. We tested the package using Chantry's own APs, though it, too, supports popular 3rd party APs.

■ **Meru Networks**, which submitted its MC 1100 Controller, an appliance similar to the other systems. However, unlike the others, Meru's package works only with the vendor's own APs; third-party APs are not supported.

As the scorecard (Table 1) shows, Aruba emerged a clear Best-in-Test winner. Aruba's overall score of 89 reflects the vendor's top ratings in two of the four criteria categories: Security Features and Performance.

As usual, the scorecard reflects this particular set of competitors and the test methodology Miercom developed and applied. Your mileage could vary, based on your short list of competitors and the relative weighting of criteria you consider the most important to your environment.

Configuration

All the systems feature an "appliance"—a pre-loaded, pre-packaged hardware and software platform, which views all the traffic passing between your wireless access points and your wired network (see Table 2, pp. 26–27).

It's important, however, that these devices not become network bottlenecks. And as Table 2 shows, all the products tested support at least one Gigabit Ethernet uplink, to alleviate this concern.

Another key "configuration" component is access points (APs), and in particular, the number and type of APs supported. Aruba, Chantry and Meru offer their own special brand of APs. That can be useful, because with their own APs, these vendors can carefully control the flow of data between the AP and the controller appliance. Aruba, for example, extends wireless encryption from the AP all the way back to the controller appliance. Normally, wireless-link encryption stops at the AP, and traffic travels from AP to controller appliance unencrypted. Encrypting all the way to the controller—the border with the wired network—is a plus. Bluesocket does not offer its own APs, and thus does not support this extended encryption capability.

Support for leading third-party APs is also useful because then you can deploy the wireless-security system with whatever APs you may already be using. Aruba and Chantry support leading third-party APs, in addition to their own. Bluesocket supports only third-party APs, as noted. And Meru supports *only* its own APs.

Another plus is AP support for the latest, high-speed 802.11g wireless-radio specification—featuring 54-Mbps transmission and full backward compatibility with the widely deployed 11-Mbps 802.11b. So is support for 802.11a, which provides better re-use of radio frequencies and so better overall scalability.

On this account, Bluesocket's system is transparent to radio technology, supporting whatever your third-party APs support. Aruba's and Chantry's APs handle the full gamut: 802.11a, 11b and 11g. Meru's APs supported only 11b when tested. This, as discussed later in "performance," turned out to be a major competitive drawback. Meru said it plans to add 802.11g support to its APs by the end of this year.

Capacity is another configuration point of comparison. Aruba's \$9,000 controller supports 24 directly-connected APs, or up to 48 APs indirectly connected to the controller (i.e., via some portion of the wired network, but isolated on the wired network from non-WLAN traffic). Uniquely among the products tested, Aruba's controller appliance includes a 24-port switch, which can even deliver in-line power to up to 24 directly-connected Aruba APs. A small drawback for Aruba, however, is that its system requires fairly dense deployment of APs, which equates to more APs, overall, than competitors require in order to cover the same terrain.

Bluesocket's \$13,000 controller has no fixed limit as far as number of supported APs. The system is constrained only by processing power and bandwidth to/from the wired network, which, as noted, can be up to 1 Gbps. Practically speaking, it seems the Bluesocket system would be able to handle a couple dozen or so APs, depending, of course, on AP type and speed and cumulative traffic load. Meru's \$8,000 system, as tested, supports up to 50 of Meru's 802.11b APs.

Chantry's \$45,000 system, by far the highest-priced, also supports by far the most APs, up to 200, and so a considerably broader wireless topology than competitors. Chantry also offers the mid-sized BeaconMaster 1100 system, which supports 100 APs—still more than double the competitors' capacity—for \$26,000.

How much does this work out to per AP? Prices generally range from about \$400 to \$700. Coverage areas vary per AP, though, and users should carefully scrutinize the vendor's specifications on this point.

Our testing found that, in some cases, such as with Aruba, which requires fairly dense AP spacing, you will not connect effectively with



Scrutinize the access point density you'll need for adequate coverage; products vary

802.11g if you go even a little beyond the vendor's recommended 50-foot distance.

One final note on configuration: Bluesocket and Meru were tested with a switched, Layer-2 and VLAN-based topology connecting APs to their respective security controller, while Aruba and Chantry IP-routed all traffic from their APs to controller. IP-based connectivity is generally better for broader, geographically dispersed wireless networks, while switched and VLAN-based connectivity favors a local area. From our testing, however, we cannot conclude that one offered any compelling advantages over the other.

Overall, we thought Chantry's package offers the strongest "configuration" suit, earning it an impressive 90 rating in this category (Table 1). With all factors considered, we viewed Aruba and Bluesocket as roughly equivalent, configuration-wise, each garnering an 85 rating. And Meru, with a few noted configuration issues, followed with an 80 score.

Security Features

Table 3 (pp. 28–29) shows a thumbnail comparison of key "security features" supported by the

packages reviewed. This was a key component of the evaluation, accounting for 30 percent of the overall score. The products all supported some security features to roughly the same extent—such as 802.1x authentication, and the ability to turn off AP broadcasting of the wireless network's identity (SSID).

We tested 802.1x authentication using an external RADIUS server, which took a little set-up time for most of the packages, but then worked very reliably (see "Testing Wireless Security" pp. 28). The initial authentication time for a client entering the network varied among the products, from about 8 to 15 seconds. The variation seemed based more on the wireless laptop-client's operating system than on the particular wireless security system. (We tested with clients based on Win2000 and XP Professional).

In one case, we found that the vendor goes well beyond 802.1x authentication capabilities. Bluesocket offers a large number of authentication techniques in addition to 802.1x, likely to match almost any customer's existing authentication environment. This useful feature earned Bluesocket extra points in the evaluation.

TABLE 2 Wireless Security Systems Tested

	Aruba www.arubanetworks.com	Bluesocket www.bluesocket.com	Chantry www.chantrynetworks.com
Product, version	2400 Wireless LAN Security System, v2.2.2.0	WG-2100 Wireless Gateway v4.0 (late beta tested); BlueSecure, v2.1.1	BeaconMaster 1200, v2.06
Main controller unit, as tested	Appliance, w/built-in 24 port switch; one 10/100 uplink	Appliance; one 10/100 uplink; optional BlueSecure runs on a Win 2000 server	Appliance; one gigabit fiber uplink
Other uplink options	Two Gigabit (via GBIC)	One Gigabit (copper is integral, fiber optional)	Four 10/100 or two Gigabit
Vendor offers own APs	Yes	No, tested with Cisco (Aironet 1100) APs	Yes
Supports 3rd party APs	Yes	Yes	Yes
Wireless technologies supported	802.11a,11b, and 11g	All; controller (gateway) is independent of APs	802.11a,11b, and 11g
AP-to-controller connectivity in test bed	IP routed to controller	L2-switched to controller via VLAN, to isolated switch port	IP-routed to controller
How many APs supported	Directly connected: 24, Indirectly connected: 48	Not fixed; limited only by max traffic through gateway	200
QoS, Class of service, SVP (Spectralink Voice Priority) support	Based on appl'n classification; can ID and expedite SVP VOIP streams	DiffServ supported; either direction; bandwidth by class and priority (high, med, low)	TOS, DiffServ supported on a per-class (VNS) basis; separate VNS for SVP and voice traffic
Management access	In-band, Web GUI supports SSL/HTTPS optionally	In-band, SSL-based Web GUI	Out-of-band (dedicated 10/100 mgt port), SSL-based Web GUI
High availability configurations; controller redundancy	Yes; excellent; active-active or active-passive; synchronized (6 sec avg.)	Yes; good; active-passive, permanent failover (30 sec avg.)	Yes; fair; active-active; some delay (90 sec avg.)
Price, US list	Controller: \$8,995 AP (model AP52): \$495 each	Controller: \$12,995 AP (Cisco Aironet 1100): \$425; opt BlueSecure: \$2,995 server software, \$695 per sensor	Controller: \$44,995 (lower-end model BeaconMaster 1100 does 100 APs, costs \$25,995); AP (model BP200e): \$395

We also examined how the wired network could be defended from threats originating on the wireless network. We found Aruba and Bluesocket particularly strong here: Each comes with an integral, full-featured intrusion detection system (IDS) that also actively suppresses many attacks, in a manner akin to an intrusion prevention system (IPS). Both also include integral firewalls, along with the ability to “rate-limit” flows—which Miercom has found is a most effective tool against denial-of-service attacks.

Meru offers a full-featured IPS and firewall, too, but as an optional third-party plug-in blade—bearing an extra \$10,000 price tag. Chantry does not include or offer an integrated IDS/IPS option. And as far as firewall goes, Chantry’s package is designed to integrate with a separate firewall system from Check Point. This was not tested.

Another useful security feature—an alternative to 802.1x—is “captive portal.” That’s the industry’s name for wireless-client username/password-controlled access, often employed for “guest”-type users. The 802.1x standard is good for a relatively static and long-term user base, like permanent employees in an office; but with a lot of tran-

sient users—like in hotels, airports, etc.—a one-time user login, kept in local database with password, is the way to go. The security system can maintain a local database of clients, or pass off password verification to an external authentication server. The packages tested all provided this capability except Meru, which said it plans to add “captive portal” in late 2004.

As far as protecting the integrity of wireless transmissions from unauthorized interception, two main security features apply: VPN gateway and encryption support. All the packages except for Chantry include integral “VPN gateway” support. Aruba’s is the most extensive, supporting up to 4,000 concurrent individual wireless-client VPN tunnels, in either termination or pass-through mode, and working with popular VPN client software including Cisco and Nortel.

In termination mode, the wireless-security controller is the VPN gateway: It terminates VPN tunnels, and then passes on, unsecured and unencrypted, all data to the wired network. In pass-through mode, the controller recognizes that wireless clients are using encrypted tunnels, and simply passes these encrypted streams through, bidirectionally to *another* VPN gateway (like a Nortel Contivity), that is somewhere deeper inside the customer’s wired network.

Meru similarly offers full VPN gateway capabilities, featuring a Windows-based VPN client that the Meru controller dynamically downloads to wireless clients. An optional accelerator card (\$3,000) is offered for encryption processing in large deployments—it handles up to 2,000 concurrent VPN tunnels. Bluesocket supports up to about 200 concurrent VPN tunnels, and supports many third-party VPN software clients. In Chantry’s case, the vendor said that, as with firewalling, its BeaconMaster 1200 controller is designed to work with a separate device, in this case a Check Point VPN gateway.

Apart from encrypted VPN tunnels, the Wi-Fi standards bodies—most notably the IEEE—have also adopted a continuum of wireless encryption standards. These have evolved from the original Static Wired Equivalent Privacy (WEP), to Dynamic WEP, to Wi-Fi Protected Access (WPA), and soon to be finalized WPA2 (see “Wireless Security Alphabet Soup,” p. 31).

Aruba and Chantry support all these, with support for the latest WPA2 due out as of September 2004. Meru does WEP and most aspects of WPA, and expects to add enhanced AES encryption—a WPA2 component—by year-end. Bluesocket relies on third party APs, and so doesn’t get directly involved in wireless encryption.

The last set of wireless security features we examined involve finding and neutralizing unauthorized, or “rogue,” APs, which clutter the airwaves of large enterprises with increasing frequency these days. This is an area in which Aruba distinguishes itself.

VPN tunnels and wireless encryption standards protect the privacy of traffic

**Meru Networks
www.merunetworks.com**

MC 1100 Controller, v2.0.2

Appliance; one 10/100 or gigabit copper uplink

Optional dual-port 10/100 or gigabit copper

Yes

No

802.11b; 11g support planned for 4Q04

AP traffic was L2-switched to controller via VLAN

50 (100+ planned in 4Q04)

Special dynamic bandwidth allocation, by AP, for SIP and H.323 traffic

In-band, SSL-based Web GUI

Yes; good; active-passive (24 sec avg.)

Controller: \$7,995 AP (model AP100): \$695; opt IPS blade: \$10,000 opt VPN accelerator: \$3,000

All the packages offer the ability to detect rogue APs. It is integral with Aruba, Chantry and Meru, and an optional subsystem with Bluesocket, called BlueSecure (\$3,000 for Windows server-based software and \$695 per special detection sensor).

Aruba's detection of rogue APs is impressive. Its APs triangulate on the rogue AP and show you graphically, on a site map, where it is located. Chantry's detection capability is also very effective, and in fact its APs were the most sensitive in identifying the existence of rogue APs. Its location information is more limited than Aruba's, however. Bluesocket's and Meru's rogue-AP detection was also effective but, like Chantry, location data was limited—in general, showing which sensor or AP detected the rogue, and the relative signal strength that was picked up.

The ability to disable rogue APs—called “containment” or “mitigation” within the industry—was best shown by Aruba. Their system employs several techniques, including a form of denial-of-service attack, to effectively and immediately disable rogues. Meru also showed that it, too, could effectively isolate rogue APs from the network. However, neither Bluesocket nor Chantry currently offers the ability to render a rogue AP incommunicado. They can both identify rogues, but can take no further disabling action.

With all security features considered, Aruba emerged with the highest rating in this category, an impressive 90. Bluesocket and Meru came in next, earning scores of 83 and 84, respectively. With no integral or optional IDS/IPS or VPN gateway, Chantry garnered a 75 rating for the security features category.

Management And Admin

Ratings in the management and administration category ended up fairly close. However, while all the tested packages offer useable Web browser-based management interfaces, each vendor's package exhibits some noteworthy positive aspects, and some drawbacks.

Aruba and Chantry tied for the highest management rating with an 88. Aruba's Graphical Planner, which assesses the customer's environment and prescribes AP placement, is a strong, unique plus among the systems tested. Other Aruba positives include: an auto-configure tool to set up APs, a configuration audit trail, good SNMP support, and very good integral reports. Overall, though, we consider the rich Aruba graphical user interface (GUI) overwhelming and fairly tedious to use.

Chantry doesn't offer the useful, automated set-up aids that Aruba does. In fact, the vendor recommends you have a third-party site survey done before you deploy their system. Chantry does, however, offer good bulk AP configuration, with audit trail, SNMP support and integral reports.

Testing Wireless Security

The wireless-security test bed consisted of a “core” network, a “Site-A” network and a “Site-B” network, each a different subnet, interconnected via an Extreme Summit 48 L2/L3 switch/router.

The core network included Windows 2003-based Domain Controller, DNS server and DHCP server. For IEEE 802.1x authentication of wireless clients, which all the tested products supported, we used Funk Software's Steel Belted Radius server, ver. 4.71, running on a Windows 2000 (SP4) Compaq Deskpro. The Steel Belted Radius worked in conjunction with Active Directory.

We tested each wireless security package using a mix of Dell and Compaq laptops. Two of our four test laptops ran Microsoft XP; the other two ran Microsoft Windows 2000. We intentionally employed a different wireless adaptor in each laptop. These included: a Broadcom 54g MaxPerformance 802.11g adaptor; a Proxim Orinoco Silver 802.11a/b/g adaptor; a Cisco Aironet 802.11a/b/g adaptor; and a Linksys Wireless-G notebook adaptor using the Funk Odyssey client v 3.02.

We used Ixia's IxChariot ver. 5.0 traffic-generation package to test throughput. In every case, the traffic that was passed between wireless laptops and a server on the wired core network consisted of 40 percent VOIP streams (RTP/UDP) and 60 percent TCP connections and streams, by traffic volume.

Each laptop-to-server throughput test was run for two minutes, first in unsecured mode and then in secure mode. In secure mode each laptop client was first RADIUS-authenticated via 802.1x (using PEAP and MS-Chap ver. 2 protocols), and then all traffic was encrypted using “Dynamic WEP.” In unsecured mode, not even a login was required. The tests were first run using a single client, in unsecured and secure modes. Then four concurrent clients were tested, also in both modes.

TABLE 3 Security Features

	Aruba
IDS/IPS Support	Integrated IDS with IPS responses; protects wireless side
Firewall Support	Integrated stateful firewall; dynamic port limiting; policies and rules; bandwidth limiting
802.1x authentication	Yes
Other authentication	Yes; local database; “captive portal”
VPN gateway	Yes; integral; downloads VPN client onto clients; controller supports up to 4,000 VPN tunnels concurrently; Nortel, Cisco VPN clients supported; termination or pass-through
WEP, WPA, WPA2 encryption	WEP, WPA; WPA2 planned Sept '04
Rogue AP detection	Excellent; can triangulate to locate rogue APs; good location info; very effective containment, automatically or after notification
Disable SSID broadcast	Yes

For the “roaming handoff” tests, we placed two of the vendors’ access points (APs) 120 feet apart, one situated in Site-A and the other in Site-B. Then a laptop that was wireless-connected to one AP was slowly moved, over the same path and at the same speed in all cases, to the other AP, forcing a handoff.

A steady stream of UDP traffic was generated and sent from a server on the core network out to the test laptop, using a software tool called ZTI Telecom’s LanTraffic V2, while the laptop was “roaming.” During the same time, a continuous Ping stream was run from the laptop to measure the elapsed “down” time it took for the roaming handoff.

Azimuth’s W-Series Test Platform (version 2.2.2) was also employed, to conduct AP “association” tests on each system. The Azimuth system ran the AP Association Capacity test and the AP Association Performance test. Association Capacity tested whether the AP could handle up to 127 concurrent wireless clients. All the products tested could. Association Performance measured how many attempts it took for the 127 wireless clients to successfully register with the AP. Most connected on the first attempt, and any remaining ones registered in two or three attempts.

For “rogue AP detection,” we inserted undefined Avaya AP-3 AE and AP-4 Access Points into the network, and then carefully noted each system’s ability to identify, locate and issue notification that the rogue APs had been detected.

We also then exercised the abilities of Aruba and Meru systems to “mitigate” the connections and traffic of the rogue APs and clients connected to them. The Bluesocket and Chantry systems do not now support rogue-device containment or “mitigation.”

Denial-of-service attacks were also launched against each tested system over the wired network, to see how vulnerable each was to such attacks. No firewall was in place. The attacks were run from a Dell PC running Debian GNU/Linux (Linux kernel 2.4.18).

For wireless network monitoring and analysis, we used WildPackets’ AiroPeekNX (ver. 2.0.5) package.

All tests run on Meru Networks’ system were done using 802.11b (11 Mbps) radio transmission, since the Meru system did not yet support 802.11g. The higher-speed 11g enabled all of Meru’s competitors to achieve considerably better throughput (see Figure 1)□

Bluesocket	Chantry	Meru Networks
Integrated IDS with IPS responses; worm, DoS detection	None	Optional, 3rd party IPS blade (\$10,000); worm detection; 1,000+ signatures; separately managed
Same as above; also does bandwidth limiting, per class or per user	Configurable filters; special integration with Check Point firewall	Same as above; can also do URL filtering; anti-virus for email attachments
Yes	Yes	Yes
Yes; local database; “captive portal;” coord w/ Windows domain login; add'l Active Directory or LDAP lookup; policy based access; others	Yes; “captive portal;” other 3rd party authentication systems supported	Other authentications planned for late 2004 include “captive portal”
Yes, integral; about 200 VPN tunnels concurrently; supports a dozen third-party VPN clients; termination or pass-through	None integral; works with Check Point	Yes; integral; up to 2,000 tunnels concurrently; this Windows client dynamically downloaded; optional (\$3,000) accelerator card; termination or pass-through
Handled by APs; not addressed by Bluesocket package	WEP, WPA; WPA2 planned Sept '04	WEP, WPA (except no TKIP); TKIP and AES planned for late '04
Very good rogue AP detection via optional BlueSecure, but no containment capability; some location info	Excellent; most sensitive detection of rogue APs, but no disabling capability (containment); some location info	Very good; detects, notifies and effective containment; some location info
Yes (an AP setting)	Yes	Yes

Bluesocket's management package similarly offers good reports and a configuration audit trail. There are no set-up or automated planning tools in the package, however.

What's more, Bluesocket's add-on security subsystem, BlueSecure, while a very useable and impressive wireless monitoring and rogue AP-detection system, is totally separate from the vendor's main Wireless Gateway system. The vendor plans to integrate the two.

Meru's GUI is generally easier to navigate than competitors', but that's in part because there aren't as many supported features and functions. For example, there are no site-planning tools, and very limited integral reports. We do credit Meru with a nice configuration wizard.

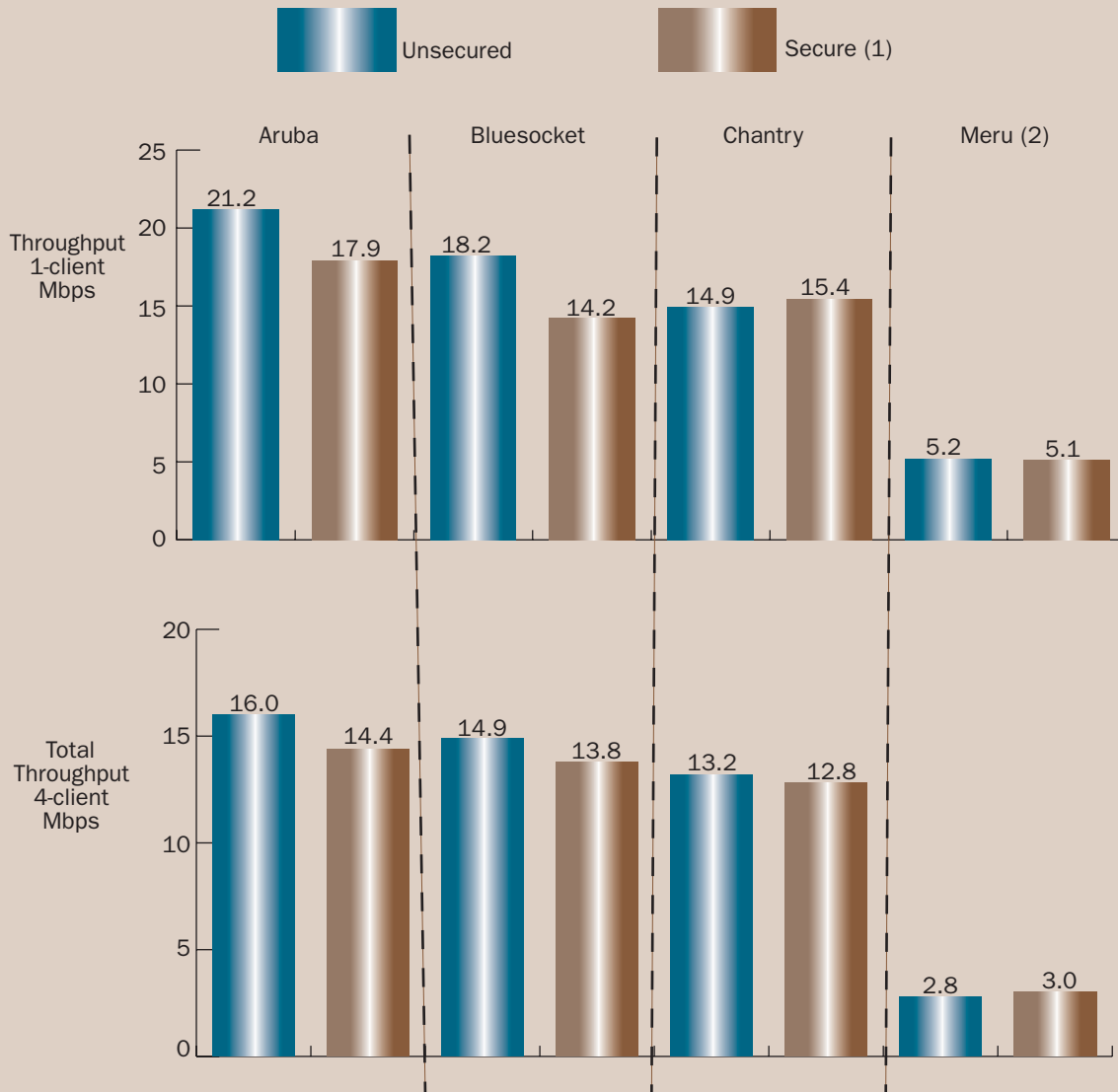
Performance

We deliberated for months about what performance metrics to apply to a review of wireless security systems. We concluded that the best tests would compare the performance that wireless clients experience with, and without, full security parameters applied.

What we didn't expect, though, was that many factors affecting traditional network performance—such as jitter, delay and packet loss—varied noticeably between these products, and security settings didn't seem to matter.

We conducted most tests by first operating a single wireless client, and then compared the same metrics with four wireless clients connected via the same AP (see "Testing Wireless Security").

FIGURE 1 Throughput—Unsecured vs. Secure



(1) Additionally, employed 802.11x authentication via RADIUS server, and Dynamic WEP, 128-bit encryption.

(2) Vendor tested with 802.11b, 11-Mbps radio. Others were all tested with 802.11g, 54-Mbps radio, which Meru did not support when tested.

Wireless Security Alphabet Soup

Speaking the language can enhance your prospects of acquiring and effectively deploying the right wireless security system. Here are some key industry buzzwords and acronyms, in alphabetical order:

802.1x: A popular IEEE standard, included in the latest wireless-security specifications, that defines how to authenticate the identity of wireless (and wired) clients, such as via an external RADIUS server, as well as other authentication methods (see EAP).

AES: Advanced Encryption Standard, the latest U.S. government-endorsed encryption algorithm, detailed in the FIPS 197 specification. Supports encryption keys of 128, 196 and 256 bits. AES is a required component of WPA2 (IEEE 802.11i) wireless security (see WPA2).

Dynamic WEP: An incremental security improvement over basic Static WEP (the Wired Equivalent Privacy protocol), Dynamic WEP entails regeneration of a new encryption key for each new user session, along with 802.1x authentication support.

EAP: Extensible Authentication Protocol, per IETF RFC 3748, and variations; a protocol used by 802.1x that lets various external authentication methods—digital certificates, usernames and passwords, secure tokens, etc.—be incorporated into wireless security environments.

IV: Initialization Vector; a 24-bit “starting

point” value, appended to basic-WEP 40- and 104-bit encryption keys, yielding 64- and 128-bit composite key values.

MIC: Message Integrity Check, called “Michael;” a component of WPA wireless security (see WPA), which ensures messages are not tampered with, or captured and replayed.

Static WEP: The original Wired Equivalent Privacy wireless protocol, generally considered insecure; features a 40- or 104-bit key, which, when manually entered and applied, is not typically changed.

TKIP: Temporal Key Integrity Protocol; an encryption-key-management protocol and required component of WPA (see below) wireless security. WPA2 retains support of TKIP for backward compatibility.

WPA: Wi Fi Protected Access; an enhanced wireless-security environment, generally replacing Dynamic WEP (which generally replaced Static WEP). WPA prescribes 802.1x authentication support, full 128-bit and TKIP or PSK (pre-shared key) encryption-key support, backward compatibility for WEP.

WPA2: WiFi Protected Access, version 2, embodied in the recently-adopted IEEE 802.11i specification; latest-generation wireless security environment, to enhance and supplant WPA; features AES encryption, 802.1x authentication and backward support for TKIP□

Security techniques do deliver a hit to throughput

The same wireless client platforms were used in all cases, and their positioning relative to the test AP was the same.

To begin with, consider packet loss. We noted almost no data loss for any of the products when testing a single wireless client, whether in the “secure” or “unsecured” environments. However, with four concurrent clients, packet loss occurred in almost all cases. Bluesocket (which doesn’t offer its own APs and was tested with Cisco Aironet 1100 APs) exhibited the highest packet loss, on average, across the board. Chantry and Meru exhibited the least.

Jitter—defined as variation in packet delay—was minimal in almost all cases and never exceeded more than a couple of milliseconds (ms). However, fixed delay varied by vendor. With a single client and no added security enabled, one-way delay ranged from 10 ms with Bluesocket to 24 ms with Aruba.

With Bluesocket and Chantry, security added roughly 20 ms to the one-way delay for both single- and multiple-client connectivity, likely due to their encryption implementations. Using four con-

current wireless clients on the same AP resulted in considerably higher one-way delay with Meru—in some cases over 100 ms.

We also checked the ability of the main controller to fail over to a hot standby unit, a feature which all the vendors supported. Aruba showed the best here with a 6-second failover. Chantry was the longest, nearly 90 seconds.

Another metric we applied was throughput—how much data traffic the clients can deliver via the wireless network, using our standard mix of 40 percent voice over IP (VOIP) and 60 percent TCP-based data streams. These results are shown in Figure 1.

Aruba took the top prize here, too, for delivering the highest throughputs—for single- and multiple-client, and secure and unsecured environments. Bluesocket placed a close second, with Chantry not far behind. Meru’s throughput was so much less because its APs supported only 11-Mbps 802.11b when tested; we tested with 54-Mbps 802.11g wireless clients, which fall back to 11-Mbps with 802.11b APs. It is noteworthy, too, that in almost all cases, throughput drops precipi-



Users must understand the physical attributes and security features of this new class of product

tously—roughly 10 percent across the board—in a secure, encrypted environment versus unsecured. So a price *is* paid for wireless security.

With all performance metrics considered, Aruba emerged a clear winner in this category, earning a 90 rating. Bluesocket and Chantry trailed with 81 and 80 ratings, respectively. Meru, due largely to its much lower, 802.11b throughput, garnered a 75.

Conclusion

The review of four wireless security systems uncovered some dramatic differences between products. These packages all feature an appliance-type controller, which examines all data passing in both directions between the wired and wireless networks.

Users need to understand the product packages' physical attributes with regard to uplinks, APs and coverage, as well as the scope and range of security features supported. As far as detecting and containing rogue APs in an enterprise, we find Aruba's package especially effective, and Meru a solid second place.

As the scorecard shows, Miercom rates all four systems with an overall score of 80 or better, which means they all can be considered solid

products and recommended buys. We view the composite security capabilities and overall performance of Aruba as the clear Best-in-Test for this round□

Companies Mentioned In This Article

- Aruba (www.arubanetworks.com)
- Avaya (www.avaya.com)
- Azimuth (www.azimuth.net)
- Bluesocket (www.bluesocket.com)
- Broadcom (www.broadcom.com)
- Chantry (www.chantrynetworks.com)
- Check Point (www.checkpoint.com)
- Cisco (www.cisco.com)
- Compaq (www.compaq.com)
- Dell (www.dell.com)
- Empirix (www.empirix.com)
- Funk Software (www.funk.com)
- Ixia (www.ixiacom.com)
- Linksys, now a Cisco company (www.linksys.com)
- Meru Networks (www.merunetworks.com)
- Proxim (www.proxim.com)
- WildPackets (www.wildpackets.com)