**Secure the air for Payment Card
Industry Data Security
Standard 2.0 compliance**

ARUBA®
n e t w o r k s

Table of Contents

Retail security threats are rising

The 2007 TJ Maxx network breach, which resulted in the theft of nearly 96 million credit card records, stood as the high-water mark for credit card theft for years. But in April 2011, a massive breach in Sony's PlayStation Network led to the theft of names, addresses and possibly credit card data belonging to 100 million user accounts.

A month later, the personal and account information, including names and e-mail addresses, of 200,000 Citibank cardholders in North America, was stolen. Citibank downplayed the severity of the theft, but it nevertheless issued replacement cards to affected cardholders.

Cyber-crime against enterprises and government agencies is escalating faster than ever before. Criminals are using advanced threats to breach corporate networks. More than 12 million records were compromised in nearly 600 data breaches in 2010, according to the Privacy Rights Clearinghouse. The pace of data thefts shows no signs of slowing.

At the same time that the threat is rising, retailers are increasingly using wireless LANs in stores. Smartphones and tablets are becoming an essential part of retail operations, and bring new efficiencies to inventory management and point of sale.

More and more retailers are using in-store mobile marketing tactics to engage shoppers in the store. And digital signage brings up-to-the-minute advertisements to shoppers. Merchants want to take advantage of the productivity and efficiency gains of mobility, but above all, they need to protect their stores – and their customers' sensitive credit and debit card data – to meet their industry compliance requirements and to protect their brands.

A quick PCI 2.0 refresher

The Payment Card Industry (PCI) Data Security Standard (DSS) is designed to enhance cardholder data security and facilitate the adoption of consistent data security measures around the world.

PCI DSS is one of a series of security standards from the PCI Security Standards Council that apply to manufacturers of payment devices, applications, infrastructure and users. The PCI Council was formed by the major payment card brands, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI DSS applies to all entities in the payment card process, including merchants, processors, acquirers, issuers and service providers, as well as any other entities that store, process or transmit cardholder data.

While PCI DSS is commonly regarded as applying to the retail industry, it can also impact healthcare, service provider, education, hospitality and financial services organizations as well as any company that processes credit and debit card transactions.

The PCI DSS standard applies wherever account data – both cardholder and authentication data – is stored, processed or transmitted. The PCI Council refers to this as the cardholder data environment or CDE. Cardholder data includes the primary account number (PAN), cardholder name, expiration date, and service code. Sensitive account data includes full magnetic stripe data or equivalent on a chip, the card validation value, and the PIN.

PCI DSS Version 2.0 was released in October 2010 and is in effect for 2011 audits. PCI 2.0 adds guidance and clarifications to version 1.2, but most notably, version 2.0 adds network access control (NAC) as a method to detect rogue wireless access points (APs). Figure 1 shows the 12 requirements of PCI DSS which serve as the baseline of technical and operating requirements that protect cardholder data.

Goal	PCI DSS Requirement
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software or programs
	6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need to know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data environment
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel

Figure 1: The 12 requirements of PCI DSS 2.0

Mitigate risks with PCI DSS 2.0

Complying with the PCI DSS standard is mandatory for any organization that stores, processes or transmits credit card data. However, many merchants have been slow to comply with PCI. According to a Gartner survey in June 2011, 89 percent of Level 1 merchants are already PCI compliant.

However, for Level 2 through 4 merchants, only 57 percent are PCI compliant.[1] Most non-compliant retailers are actively working on being compliant, which can take several years.

There are several compelling reasons to fully comply with PCI, including:

- Protect the merchant's brand – A security breach has a negative impact on a merchant's brand name and customer loyalty. Consumers perceive identity theft as a real threat, and they expect that merchants that accept credit and debit cards to protect their private information.
- Mitigate risk of a security breach – Companies that do not comply with PCI experience more data breaches than PCI-compliant merchants, according to a Ponemon Institute study.[2]
- Avoid costs associated with remediation – Fewer breaches means less remediation. Gartner estimates that a security breach costs $300 per record, which includes the costs of analyzing the extent of the breach as well as cleanup and recovery, client notifications, lawsuits, regulatory fines and brand recovery.

  In contrast, Gartner estimates that PCI compliance costs $16 per record, which includes the cost of using firewalls to separate the cardholder data environment as well as for data encryption, intrusion prevention, audit logging and security audits.

---

[1] "Gartner Survey: PCI Compliance Activity Shifts Downstream as Aggressive Enforcement Continues," Gartner, June 2011.
[2] "67% Of Companies Fail Credit Card Security Compliance," InformationWeek, April 20, 2011

- Fines for out-of-compliance merchants – Increasingly, the card brands are enforcing PCI compliance more aggressively, and retailers, payment terminal providers, and payment processors can be subject to fines if they are out of compliance with PCI.

  Visa may levy fines of up to $500,000 per incident for any merchant or service provider that is compromised and not compliant at the time of the incident. If a Visa member doesn't notify the company's fraud control group of a suspected or confirmed loss or theft of any Visa transaction information, the member is subject to a $100,000 fine per incident. Similarly, MasterCard may levy PCI non-compliance fines up to $200,000 per year. MasterCard has been stepping up its enforcement practices of late.

- Safe harbor for PCI-compliant merchants in the event of a breach – If a merchant loses cardholder data because of a security breach, but is PCI compliant at the time of the breach, then the merchant is exempt from the charges relating to credit and debit card replacements. Otherwise, the merchant is liable for $80 to $320 per credit or debit card number lost and replaced. As an example, the TJX Companies paid $40.9 million to Visa for such fines.

- Access to lower interchange per transaction rates for PCI-compliant merchants – Merchants can qualify for lower tiers of per-transaction card brand fees if they are PCI compliant.

While the specifics of the compliance process depends on the card brand and the number of transactions that the merchant processes annually, the rule of thumb is the more transactions, the more involved the certification process will be.

Merchants may need to engage with independent scan vendors or auditors to validate compliance. And a merchant that has suffered a breach that resulted in data compromise may be escalated to a higher validation level. Figure 2 outlines the requirements for Visa and MasterCard.

Merchant Level	Selection Criteria	Visa Validation Actions	MasterCard Validation Actions	Validated By
1	Any merchant, regardless of acceptance channel, processing more than 6,000,000 credit/debit transactions per year. Any merchant that has suffered a hack or an attack that resulted in an account data compromise. Any merchant identified as Level 1 by any card association.	Annual On-Site Security Audit Quarterly Network Scan	Annual On-Site Security Audit Quarterly Network Scan	Independent Security Assessor or internal audit if signed by an officer of the company. Qualified Independent Scan Vendor
2	1 million – 6 million credit/debit transactions per year	Annual PCI Self-Assessment Questionnaire Quarterly Network Scan	Annual PCI Self-Assessment Questionnaire Quarterly Network Scan At merchant discretion: Annual onsite assessment	Merchant Qualified Independent Scan Vendor
3	20,000 – 1 million credit/debit or e-commerce transactions per year	Annual PCI Self-Assessment Questionnaire Quarterly Network Scan	Annual PCI Self-Assessment Questionnaire Quarterly Network Scan	Merchant Qualified Independent Scan Vendor
4	Less than 20,000 Visa credit, debit or e-commerce transactions per year, and all other merchants processing up to 1 million transactions per year.	Annual PCI Self-Assessment Questionnaire Quarterly Network Scan	Annual PCI Self-Assessment Questionnaire Quarterly Network Scan	Merchant Qualified Independent Scan Vendor Validation requirements and dates for Level 4 merchants are determined by the merchant's acquirer. Submission of scan reports and/or questionnaires by level 4 merchants may be required.

Figure 2: Visa and MasterCard's PCI-compliance levels

Specific requirements for wireless LANs

While the cardholder associations require different levels of compliance based on transaction volumes or past non-compliance, using wireless LANs (WLANs) brings on another layer of requirements. The WLAN-focused requirements of the PCI DSS standard are organized into three categories, which simplify the task of identifying and meeting the requirements.

Depending on whether merchants do not use WLANs at all (Category 1); use WLANs but not for cardholder data (Category 2); or transmit cardholder data over the WLAN (Category 3), merchants will need to meet increasingly stringent requirements. Figure 3 summaries the three categories and their requirements.

Category 1 No WLAN	Category 2 No cardholder data over WLAN	Category 3 Cardholder data over WLAN
11.1 Wireless Scanning/NAC	11.1 Wireless Scanning/NAC	11.1 Wireless Scanning/NAC
	1.1.2 Inventory WLAN 1.2.3 Firewall WLAN 9.1.3 Physical Security	1.1.2 Inventory WLAN 1.2.3 Firewall WLAN 9.1.3 Physical Security
		2.1.1 Don't Use Defaults 2.2 Standard Config 4.1.1 Better than WEP 6.1 Get Latest Patches 7.2 Role-based Access 10.3 Monitor Access

Figure 3: PCI 2.0 requirements pertaining to WLANs

Category 1

Merchants that do not use WLANs must still monitor for the presence of wireless APs. At first glance, this requirement may seem unnecessary, but APs can be accidentally or intentionally introduced in stores and other locations.

For example, an employee could bring in an AP from home to support a smartphone or tablet, and that Wi-Fi may extend to where it can be used by others. An unauthorized, or rogue, device may introduce malware to the retailer's network or be a stepping stone to a larger network breach.

Merchants can use physical inspections, wireless scans, network access control or wireless intrusion detection and prevention (WIDS/WIPS) to test for the presence of wireless APs and detect unauthorized APs.

Category 2

Merchants that use WLANs but do not send cardholder data over the Wi-Fi must meet Category 2 requirements. Category 2 is inclusive of the Category 1 requirements, plus requirements for maintaining an inventory of the WLAN, using a firewall to segment the WLAN from the wired network, using strong encryption and authentication, and using appropriate physical security measures.

Category 3

Merchants that use the WLAN to transmit cardholder data must meet the most stringent requirements. Category 3 is inclusive of Category 1 and 2 requirements as well as additional requirements, not using default passwords and configurations, regular patching, role-based access, and monitoring access.

Aruba's solution for retail networks

Retailers that deploy an enterprise-grade Aruba Networks® WLAN solution benefit from the freedom and ease of a mobile access network that deepens customer engagement and improves employee productivity.

Aruba provides multiple levels of security protection to allow merchants to meet PCI requirements and even exceed the standard using identity-based networking, mobile device fingerprinting, and advanced cryptography.

Merchants can leverage Aruba to provide secure, end-to-end mobility in stores, distribution centers, and corporate headquarters. Aruba consolidates wired, wireless and remote networks on a single, centralized architecture, and this architecture – called the Aruba Mobile Virtual Enterprise (MOVE) architecture – ultimately unifies security, network access and management services and delivers higher levels of operational efficiency and lower cost.

Aruba delivers strong, comprehensive security, including an integrated stateful firewall, strong authentication and encryption, and virtual private network services, so that retailers can benefit from the productivity benefits of mobility while confidently enforcing their corporate and industry security policies.

With Aruba's retail network solution, merchants can provide secure, consistent access to users and devices – no matter where employees or customers are, what devices they use, or how they connect to the network. Aruba takes a role-based, approach to security where the user's identity is validated through strong authentication as well as the device, physical location and application.

Identity-based networking is designed for the way people work today. It's the opposite of the legacy old model in which networks assumed that because you are plugged into a particular port, you must be User A. Today's users are mobile and can connect anywhere in the building or even at another store or office location. With Aruba, users are defined based on who they are and where they are. Access can be controlled by time of day, by application and even device.

In addition, Aruba's device fingerprinting technology automatically classifies a wide variety of wired and Wi-Fi enabled devices, such as barcode scanners, smartphones, mobile point of sale (POS), and laptops. Retailers can then enforce different network access and quality-of-service (QoS) policies for different mobile devices.

Aruba simplifies the challenge of allowing employees – and even customers – to use personally-owned mobile devices on in-store networks. Many retailers are rolling out bring-your-own-device (BYOD) initiatives to allow employees to be more productive and to support in-store mobile marketing campaigns. Aruba Amigopod™ software automatically detects mobile devices such as iPads, smartphones and tablets, and allows users to self-register and be assigned the appropriate network access policy.
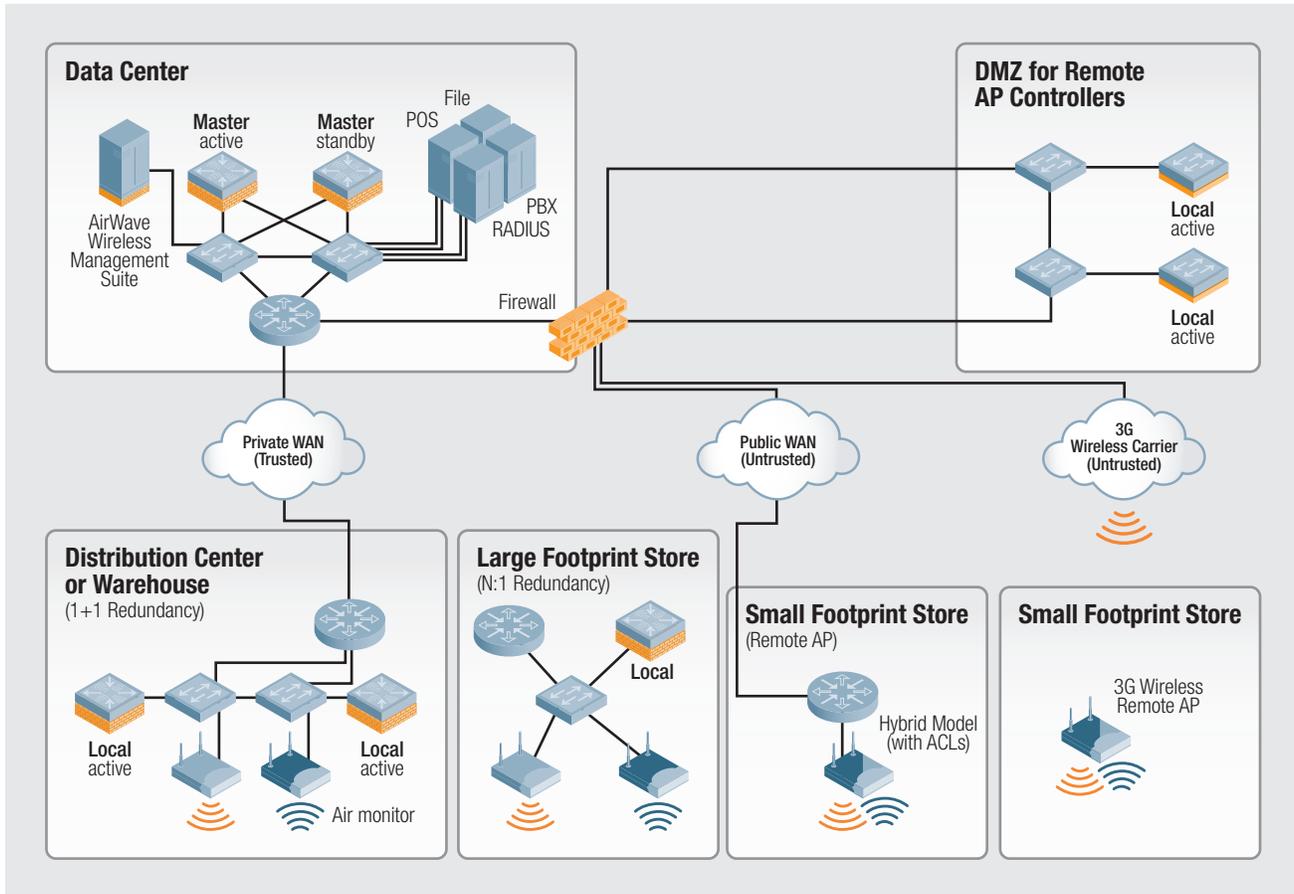
*Figure 4: The key components of the retail physical architecture include master controllers at headquarters,
local controllers at each retail site that has more than four APs, APs deployed throughout the retail space,
air monitors either via a hybrid AP or a dedicated air monitor, and AirWave network management.*

Aruba's solutions are designed for operational efficiency in a retail environment (see Figure 4). Aruba's mobility services are delivered centrally from the data center across thin access networking devices or on-ramps. Aruba Mobility Controllers are deployed in the data center to provide context-aware networking across wireless and wired LANs, VPN connections, and remote offices.

Aruba provides a wide range of access on-ramps, including 802.11n APs, Mobility Access Switches, outdoor wireless mesh routers, virtual branch networking, and the Virtual Intranet Access™ (VIA™) agent for secure remote connectivity.

Amigopod access management software is an easy-to-use visitor management solution that delivers secure network access to guests, employees and their mobile devices. AirWave™ network management is the only multi-vendor network management software that manages everything affecting service quality, including the RF environment, controllers, wired infrastructure and APs.

Achieving PCI compliance with Aruba

With Aruba, merchants can meet the requirements for the categories of WLAN usage for PCI – no WLAN, no cardholder data over the WLAN, and cardholder data over the WLAN (see Figure 5.) And retailers can easily migrate to a higher category of protection as their use of Wi-Fi expands while protecting their investment.

Category 1 No WLAN	Category 2 No cardholder data over WLAN	Category 3 Cardholder data over WLAN
• APs for scanning only • Network access control with S3500 switch • Wireless intrusion detection and prevention • AirWave to log and report	• APs in hybrid mode • Built-in firewall segments the WLAN • Identity-based networking with strong authentication and encryption • AirWave to log and report	• APs in hybrid mode • Supplement with dedicated air monitors • Built-in firewall segments WLAN • Identity-based networking with strong authentication and encryption • AirWave to mitigate rogues, log and report

Figure 5: Aruba Meets PCI Security Controls for WLANs

Aruba's solution for Category 1: No WLAN

Merchants that do not use WLANs must monitor for the presence of unauthorized wireless APs. They can meet this requirement by installing Aruba APs as air monitors and using AirWave network management for rogue detection and reporting. Merchants can also use Aruba Mobility Access Switches to enforce network access control on the wired network.

Wireless scanning and rogue containment

Aruba APs can function as air monitors, periodically scanning the air for unsanctioned wireless devices. In air monitor mode, Aruba APs identify and record other wireless devices in the area, including Wi-Fi clients, APs and bridges. If unauthorized Wi-Fi devices are detected, detailed reporting and even a full packet capture is collected.

Aruba can contain rogues using tarpitting or wireless de-authentication. With tarpitting, the AP or AM answers the client and allows the connection, but does so using a false BSSID, a false channel, or both.

After the client station associates to the false AP, the AP or air monitor ignores the traffic from that client. When a client is successfully tarpitted, most client drivers report that the client is connected. Users can see that their device did not get an IP address, cannot pass data, and may attempt to reconnect to the rogue network.

However, without user intervention the client remains in the tarpit. The client eventually stops trying to send data to the fake AP. If the user tries to connect to the rogue AP again, the client is contained again. This method is very efficient, because each AP or air monitor near the client can participate without spending much time on the channel.

Wireless de-authentication can also be used. De-auth messages indicate that the Aruba AP or air monitor is attempting to disconnect a client from a rogue network. The AP impersonates the MAC address of the rogue APs when it sends the de-auth messages to the client.

The AP also impersonates the MAC address of the client when it sends de-auth messages to the rogue AP. Though this procedure is effective, it is also disruptive to the nearby stations.

Network access control

Aruba Mobility Access Switches can enforce network access control (NAC) so that wired connections are authenticated before any device is allowed to connect to the network. The Mobility Access Switch S3500 can correlate potential wireless rogues with data from the wired network and mitigate potential threats.

If a threat is identified, the S3500 can shut off the affected port, or contain the device through de-authentication or by delaying network connections via tarpitting. Shutting off access reduces business risk and enables the IT security team to focus its efforts on the real threats.

Wireless IDS/IPS

Aruba RFProtect™ combines Aruba wireless intrusion protection software and with additional spectrum capabilities to provide an integrated system that detects and mitigates threats.

The RFProtect module provides a patented containment method for rogue APs and an intrusion detection system for infrastructure and clients. In addition, network dashboards and configuration wizards make it easy to manage these features and simplify the challenges of managing network security.

AirWave RAPIDS™ leverages Aruba air monitors to scan the RF environment for unauthorized devices in range. If the merchant does have any wireless APs on the premises, existing Wi-Fi laptops can be used for wireless scanning.

RAPIDS also scans the wired network to determine if wirelessly detected rogues are physically connected to the local network and to look for other unauthorized devices in the area without wireless coverage.

RAPIDS aggregates scanning data from multiple sources and correlates the data for a more accurate threat assessment (see Figure 6). Administrators can easily classify security threats according to their organization's security policies, so that they can focus on the most important threats.

With RAPIDS, retailers have a complete view of the wireless environment and an efficient, effective process for rogue detection, correlation, classification, alerting, reporting and containment.
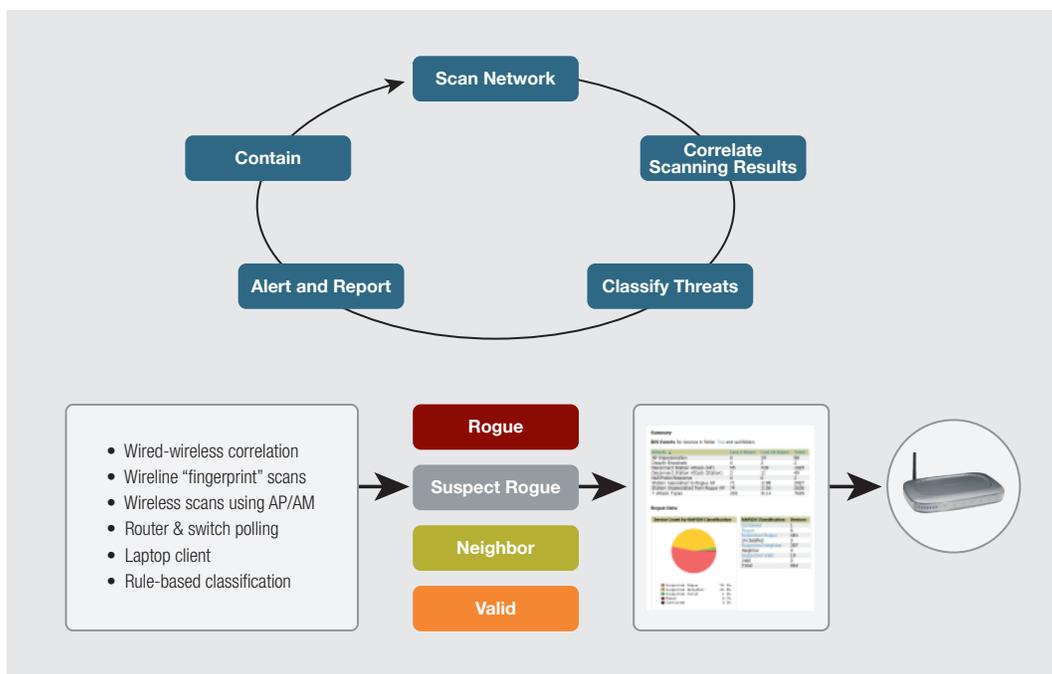

Figure 6: Merchants can use AirWave RAPIDS module to detect rogues and prevent intrusions.

Aruba's solution for Category 2: No cardholder data over the WLAN

Merchants that have wireless networks but do not use the Wi-Fi to store, process or transmit cardholder data must meet Category 2 requirements for WLAN usage. Aruba can help merchants meet these requirements with hybrid APs that provide Wi-Fi access to users as well as periodically scan the air.

Merchants can use Aruba's integrated firewall to segment the wireless network from the cardholder data environment. In addition, Aruba provides capabilities to allow administrators to inventory the WLAN components and enforce physical security.

Wireless IDS/IPS and dedicated air monitors

Aruba APs can be configured as dedicated air monitors that constantly scan the RF spectrum, or as devices that provides both AP and air monitor functions simultaneously (known as a hybrid mode or scanning AP). Dedicated air monitors are recommended for both security and performance advantages.

Wireless IDS/IPS services can be provided by AirWave RAPIDS in conjunction with the Mobility Controller RFProtect software module. APs installed in stores and other remote locations send all traffic to a Mobility Controller in the merchant's data center via an encrypted connection. The Mobility Controller analyzes wired and wireless traffic, and identifies any rogue devices or attacks. With the right policies, Aruba can mitigate rogues and denial-of-service attacks.

Firewall the WLAN from the wired network

Aruba's integrated ICSA-certified stateful firewall can segment the wireless traffic from the wired network. A merchant can apply the appropriate firewall rules to explicitly allow traffic based on corporate policies; the Aruba firewall denies all traffic from the wireless network by default.

Policies governing access rights, quality of service, bandwidth limits, time-of-day and location restrictions can be controlled by user and device. Unauthorized devices that attempt to penetrate the Aruba network can be blacklisted as well.

In addition, merchants can use Aruba's stateful firewall to isolate traffic from barcode scanners that do not support modern encryption and authentication methods. PCI 2.0 strictly forbids the use of wired equivalent privacy (WEP), the compromised security mechanism, yet many older barcode scanners are only capable of WEP.

Firewalling off WEP-only scanners puts them out of scope of PCI DSS compliance, which shields merchants from the cost and complexity of replacing legacy systems. The alternative is for merchants to replace all of their WEP-based scanners, embedded wireless devices or other devices, which can be a costly proposition.

There are many other scenarios where network segmentation via a firewall is desirable. For instance, a merchant may create a role-based policy for a mobile POS that sends credit and debit card data, inventory status and price updates over the Wi-Fi.

Or a store manager using an iPad may need access to in-store or corporate databases and the Internet, but should not have access to the cardholder data system. Or shoppers can use kiosks that connect to the Internet, but any access to the in-store network is blocked.

Strong encryption for authentication and transmission

PCI requires the use of strong encryption for wireless transmission whether or not credit and debit card data is transmitted. With Aruba, a user's identity is validated through IEEE 802.11X authentication and other information, such as device type, location and even the application being used. This identity is used to apply access controls on the user.

Aruba supports multiple authentication and encryption methods and different methods can be used simultaneously (see Figure 7). This allows, for instance, Wi-Fi Protected Access 2 (WPA2) with 801.1X authentication and AES-CCMP encryption to be the preferred authentication method, but less capable devices, such as IP phones and barcode scanners, can use pre-shared key (PSK). In addition, Aruba Mobility Controllers also support Suite B cryptography for use in classified government and high-security enterprise networks.

Once a user's or device's role is assigned, the corresponding firewall policies are applied to all traffic to and from the device. The firewall policies are tightly bound to the user's identity and authentication state to prevent man-in-the-middle and spoofing attacks.

For devices that lack WPA2 or VPN, Aruba supports a captive portal that identifies the user and restricts access by the specified user, time and location. Captive portal authentication is encrypted by SSL and can support both registered users with a login and password or guest users who only supply an email address.

User/Device Role	Authentication	Encryption
Employees	802.1X	AES
Guest networks	Captive portal	None
Handheld devices	802.1X or PSK as supported by the device	AES if possible, TKIP or WEP if necessary (combine with restricted PEF user role).

Figure 7: Recommended Authentication and Encryption Combinations

Additionally, merchants can use the Aruba Amigopod family of software and appliances to secure wireless network access to guests, employees and their mobile devices. Guests and employees with mobile devices can self-register for network access.

Once registered, Amigopod delivers account login credentials to users via printed message, SMS text message, or email. Accounts can be set to expire automatically after a specific number of hours, days, or data consumed.

Amigopod can manage secure, identity-based access for thousands of concurrent users. Amigopod helps satisfy other compliance and auditing requirements by maintaining user account and login information for up to a year.

Administrative access to the Aruba system is also identity-based. This allows the level of access available to each IT administrator to be tailored to the job function. For instance, the network engineering team may have read-write privileges but the service desk has read-only privileges.

Inventory the network

Merchants can use AirWave to create an inventory of the wireless network. AirWave's device inventory report lists every component of the wireless network, including brand, model, version, IP address, MAC address, SSID, and notes on the physical location. AirWave's VisualRF capability identifies the physical location of every device on a sitemap for documentation purposes.

Physical security

Merchants must also restrict physical access to wireless APs and other networking gear, as physical security is the first line of defense. Aruba APs can be secured using third-party secure enclosure or a Kensington lock or bolted so they cannot be easily moved.

Aruba's solution for Category 3: Cardholder data over the WLAN

Aruba provides an enterprise-grade network solution for merchants that transmit cardholder data over the air. In addition to hybrid APs, merchants may want to add dedicated air monitors to provide additional scanning coverage. Aruba provides multiple layers of security, including a stateful firewall and enterprise-grade authentication and encryption methods. Merchants can use AirWave to mitigate rogues and provide reporting.

Don't use defaults

According to the PCI DSS requirements, default vendor settings for wireless environments that connect to the cardholder data environment or transmit cardholder data must be changed. AirWave allows merchants to centrally configure and manage their networks.

When the Aruba WLAN is first powered up, the network administration must assign passwords, SSIDs, encryption keys and other parameters. For automated deployments at stores and remote locations, the default configurations are automatically changed when synchronized with the master Mobility Controller at headquarters.

Configuration standards for system components

During a PCI audit, merchants are required to explain what configuration standards are used for all system components, including WLANs, and how they are enforced. Aruba provides the tools to help merchants comply with this requirement.

Administrators can use AirWave to centrally define the configuration policies for the Aruba network on a group-by-group basis. This allows different configuration policies to be defined for retail stores, distribution centers and corporate headquarters. As a multi-vendor network management tool, AirWave supports most leading hardware brands and models.

AirWave's automated custom compliance audits check the configuration of every network device against policy. A high priority alarm is generated if a violation is detected, and the administrator can instruct AirWave to automatically correct any violations or to create a complete list of improperly configured devices and settings that do not comply with the established policies.

Get the latest patches

Aruba makes a practice of making patches available as quickly as possible to keep customers protected. Aruba's wireless security incidence Response team automatically alerts customers of any security issues and updates.

In addition, the central configuration of Mobility Controllers simplifies patch management. As system updates are uploaded to the controller, all managed APs are updated without intervention. Retail chains with hundreds or thousands of locations can update their entire Aruba network with the latest software at the same time.

Role-based access

Aruba enforces the principle of least privilege by identifying users or devices, placing them in distinct roles, and permitting or denying access to network resources or protocols based on these roles. This capability allows a POS terminal to be treated differently than a store manager on a laptop or a public kiosk. The Aruba WLAN logically separates all traffic and permits access only to the level granted by the administrator based on business needs.

Monitor access

AirWave provides audit logs for administrative actions for up to two years and maintains detailed audit trails and system logging of all activities on the wireless network. Logs for Aruba's WLAN are stored locally and may be exported in retail time to other syslog servers.

Available logs include:

- Wireless associations, including time, MAC address, AP number and physical address
- Authentication attempts, including time, user name, MAC address, IP address, AP number and physical location
- Network traffic, whether permitted or denied, including time, user name, MAC address, IP address, AP number and physical locations
- All access to the controller management interface, including configuration changes made to the system. Logs include time, IP address, user name and the configuration that was changed.
- Wireless attacks and intrusion attempts, including time, MAC address, AP number and physical location.

Make the right move to protect the store

Petco, Cabelas, Checkers and many other leading retailers use Aruba to provide in-store mobility to optimize store operations and in-store mobile marketing programs while maintaining PCI compliance.

With Aruba, merchants can be confident that their workforce has consistent, secure access to network resources based on who they are – and that the cardholder data environment is protected. Aruba integrates easily into existing retail environments, and the MOVE architecture eliminates the cost and complexity of managing separate wired and wireless access policies.

About Aruba Networks, Inc.

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company's Mobile Virtual Enterprise (MOVE) architecture unifies wired and wireless network infrastructures into one seamless access solution for corporate headquarters, mobile business professionals, remote workers and guests. This unified approach to access networks dramatically improves productivity and lowers capital and operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook.

www.arubanetworks.com

1344 Crossman Avenue. Sunnyvale, CA 94089

1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com