Ruckus
Simply Better Wireless.

white paper

SmartSec™ for PCI Compliance

RUCKUS ZONEFLEX™ HELPS RETAILERS TO MEET PCI DATA SECURITY STANDARDS

Introduction

In an effort to stem security threats and secure the credit card data of consumers, a consortium of five credit card companies founded the PCI Security Standards Council in 2004. They jointly agreed to establish and adopt a common set of guiding principles, and created a set of very specific requirements for meeting them. These principles have become known as the “Payment Card Industry Data Security Standard” or “PCI DSS”.

The PCI DSS includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. PCI compliance is mandatory for all merchants that store, process or transmit credit card data through retail stores, mail order, telephone order and online sites. Merchants must therefore pay particular attention when establishing, testing, and maintaining all components of their information system’s infrastructure relating to cardholder data.

Due to the dynamic nature of retail businesses, wireless technology has been well received and has become ubiquitous throughout those organizations. From business offices to warehouses, and all the way to the POS, the need to quickly change has made the technology essential. This dependence requires network managers to carefully consider the implications of the wireless exposure to their network security.

Ruckus Wireless understands that the procurement guidelines for many retailers, hotels, and other corporations require them to meet PCI guidelines. As the inventor of Smart Wi-Fi, Ruckus Wireless is committed to providing solutions that meet PCI requirements.

SmartSec™ for PCI Compliance

RUCKUS ZONEFLEX™ HELPS RETAILERS TO MEET PCI DATA SECURITY STANDARDS

To that end, Ruckus Wireless joined the PCI Security Standards Council as a participating organization. Ruckus Wireless is actively working with the Council to evolve the PCI DSS principles and other payment card data protection standards.

This paper will present a summary of PCI DSS security requirements for wireless LAN (WLAN) deployments, and will discuss how the Ruckus Smart Wireless LAN system meets and exceeds PCI DSS compliance.

Achieving Compliance with PCI Requirements

The PCI Data Security Standard Requirements and Security Assessment Procedures (https://www.pcisecuritystandards.org) consists of a group of principles and very specific corresponding requirements that must be met by all retailers processing credit card information. Some of these requirements directly impact wireless LAN selection and configuration.

PCI v2.0 was most recently released in October of 2010 requiring mandatory implementation starting January 1, 2012. Version 2.0 further extends the existing requirement to "track and monitor all access to network resources" to specifically include:

"Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis."

The methods that the organization allows:

"…includes but are not limited to wireless network scans, physical / logical inspections of system components and infrastructure, network access control (NAC) or wireless IDS/IPS."

Ruckus provides tracking of all nearby APs and their SSIDs via ZoneDirector, which in turn can classify as Rogues, Evil Twin APs, Ad-hoc networks, and Neighbor networks and send an immediate alert appropriately. If a more sophisticated attack with the potential to compromise the network is detected, such as a DoS attack, the attack is immediately remediated to ensure normal operation.

The following are the initial 12 requirements which have not changed:

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

"All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employees' Internet access through desktop browsers, employees' e-mail access, dedicated connection such as business to business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network."

While wireless data networks require additional security measures available on the ZoneFlex product, it is important that firewall configuration applies to both wireline and wireless network segments. This consistent approach to network security simplifies configuration and enhances security. The ZoneFlex products are particularly friendly to such network architecture as traffic is directed to the wired router/firewall directly from the access points without first traversing through the ZoneDirector. Additional security can be applied to wireless traffic using access control lists at the access points and ZoneDirector. It is also recommended that user groups be organized into different WLANs, and then mapped to different VLANs for complete separation. Each WLAN can be configured to use a different set of security policies such as authentication method.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

"Malicious individuals (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information."

There is only one local Administrator account for system management. The IT manager must enter the administrator user name and password twice to setup this account. There is no password recovery option. If the Administrator password is lost, the ZoneDirector must be reset to factory default configuration to regain access. Multiple administration user accounts are allowed when authenticated via a remote authentication server.

ZoneDirector provides a single configuration and monitoring tool to simplify the administration of the network. Newly added access points will automatically join the ZoneDirector managed cluster and be configured with the best security practices enforced on the ZoneDirector. It is a good practice to change the administrator credentials periodically as well as the authentication and encryption keys for your wireless network. Using DynamicPSK makes this much easier by enforcing a unique key per user, as well as a periodic key refresh policy.

SmartSec™ for PCI Compliance

RUCKUS ZONEFLEX™ HELPS RETAILERS TO MEET PCI DATA SECURITY STANDARDS

Protect Cardholder Data

Requirement 3: Protect stored cardholder data.

"Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails."

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

"Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Mis-configured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments."

Once authorized clients are connected to the network and transfer traffic, this traffic is encrypted during transmission to ensure that information is hidden from prying eyes. Encryption techniques continuously evolve to provide stronger encryption schemes. Ruckus Wireless ZoneFlex products support all the latest encryption standards authorized by IEEE, and the Wi-Fi Alliance for use in wireless networks, as well as legacy standards, for backward compatibility.

The Ruckus Wireless solution provides strong authentication and encryption with WPA/WPA2 (TKIP and EAP) for WLAN access. Using Dynamic PSK, the perfect balance is achieved between strong encryption, limited distribution of keys, built-in authentication, and simplicity of management and administration.

Furthermore, the unique BeamFlex antenna technology used by all Ruckus products enhances security by limiting propagation of RF signals to their intended destination. A hacker would find it difficult to eavesdrop from a location outside the directional RF beam, which clearly does not replace the need for encryption but enhances the security of the network

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs.

"Malicious software, commonly referred to as 'malware'—including viruses, worms, and Trojans—enters the network during many business approved activities including employees' e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats."

Requirement 6: Develop and maintain secure systems and applications.

"Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software."

As a best practice, Ruckus Wireless always recommends that your IT department supply and maintain the latest versions of virus definitions, software patches, and software/firmware upgrades, for your network clients.

In an effort to keep abreast of new security issues as they arise, Ruckus Wireless maintains a support site (http://support.ruckus-wireless.com) with the latest available updates and upgrades for all of its products. The administrator menu has a clearly displayed upgrade function that checks for and downloads the latest firmware updates. ZoneDirector applies the upgrades to each of the APs in the WLAN automatically.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know.

"To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. 'Need to know' is when access rights are granted to only the least amount of data and privileges needed to perform a job."

SmartSec™ for PCI Compliance

RUCKUS ZONEFLEX™ HELPS RETAILERS TO MEET PCI DATA SECURITY STANDARDS

Requirement 8: Assign a unique ID to each person with computer access.

"Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users."

Given the nature of the wireless environment, unauthorized clients such as laptops, dual-mode smart-phones and PDAs are very likely to legitimately exist within the Wi-Fi radio environment. They of course should not be allowed onto the network. In other words, the network must separate authorized clients from unauthorized clients, using authentication and access control procedures. Ruckus ZoneFlex Smart Wi-Fi products implement a variety of authentication and access control options for maximum security and flexibility to meet the requirements of every retailer. This includes built-in support for standard Pre-Shared Key (PSK), enterprise-class 802.1x EAP authentication, Dynamic Pre-Shared Key (PSK), and web-based guest pass authentication (i.e. Captive Portal) via Microsoft ActiveDirectory, RADIUS, or a Local Database, as well as Layer 2 and Layer 3 access control lists (ACL).

The first option, pre-shared encryption key (PSK involves configuring a key or passphrase on every client device. While this option is perceived to be secure, it's not. Using the same PSK for all employees and all devices means that the key can be easily compromised. The commonly used PSK also tends to be a relatively short string that can be easily compromised. And for every new employee, IT staff must configure the laptop with the SSID and the key. If there's a need to replace the key (eg. employee leaves), every laptop must be reconfigured.

The second option is using an enterprise-class solution 802.1X, which is highly secure but very complex for small-to-medium retailers. It requires having the RADIUS server and 802.1X supplicants on each client. Configuring and maintaining 802.1X is burdensome for merchants, who do not have the time or resources to manage the system. Ruckus Wireless' Dynamic Pre-Shared Key (PSK) offers a third option. Dynamic PSK is a patent pending technology developed to provide robust and secure wireless access while eliminating the arduous task of manually configuring each individual laptop with the requisite wireless SSID and the tedious management of encryption keys. Dynamic PSK automates and centralizes this process within the network. Once enabled for the entire system, a new user simply connects to the Ethernet LAN and authenticates via a captive portal hosted on the Ruckus ZoneDirector. This information can be checked against any standard back-end authentication system, such as Active Directory, RADIUS, or an internal user database on the ZoneDirector. Upon successful authentication, the ZoneDirector generates a unique 63-byte encryption key for each first time user. A temporary applet with a unique user key and configurable lifetime, plus other wireless configuration information is then pushed to the client. This applet automatically configures the user's device without any human intervention. The user then detaches from the LAN and connects to the wireless network. Once associated, the Dynamic PSK is bound to the specific user and the end device being used.

The Ruckus Guest Pass solution simplifies the setup and management of WLAN access for guests and other temporary WLAN users on the ZoneDirector. Guest Pass authentication generates time-limited guest access passes for guests customized to their time of stay. Unique Guest Pass keys are dynamically generated by the ZoneDirector for the reception staff, and are entered by the guest into the captive portal to gain secure access to the WLAN. The guest WLAN is separate and secure from the organizations' traffic, and guest devices are protected by restricted communications between devices connected to it. Wireless client isolation is a security feature that is automatically configured to prevent communications between clients on the guest WLAN.

Requirement 9: Restrict physical access to cardholder data.

"Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted."

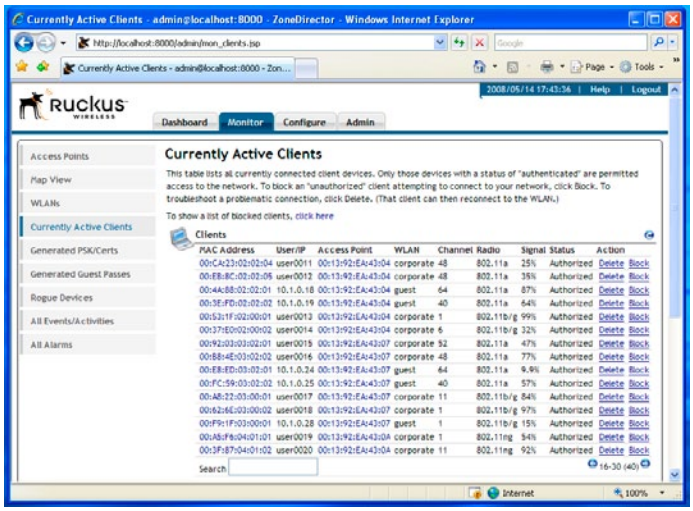
Physical access to ZoneFlex access points is preventable by physically locking them. In a ZoneDirector configuration, even if an access point is stolen, security information and certainly user information are not stored on it, as authentication is always performed against the ZoneDirector. All management information between the ZoneDirector and access points is within a secure management tunnel and cannot be intercepted from the network or otherwise manipulated.

The ZoneFlex products can be integrated within a network's VLAN architecture, allowing the segregation of user traffic. It can then be deployed to work with secure Network Admission Control (NAC) systems using its VLAN capability to quarantine devices that do not match security policies regarding the operating system level, personal firewall settings or anti-virus definition files. Use of access control lists can block users from going to "disallowed" networks or devices.

SmartSec™ for PCI Compliance

RUCKUS ZONEFLEX™ HELPS RETAILERS TO MEET PCI DATA SECURITY STANDARDS

Figure 1: View, monitor and authorize/block connecting devices.



ZoneDirector web UI assists in monitoring the status of all clients on the network.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

"Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs."

ZoneDirector provides simple-to-use tools to view, monitor, and authorize/block connecting devices (**Figure 1**). In addition, each event on the wireless network (such as client association and authentication) can be sent to a centralized Syslog server for detailed logging of all network events. For example, if the client has repeatedly failed authentication attempts, the client will be temporarily blocked to protect against dictionary password attacks.

The FlexMaster Dashboard View provides a quick reference about the condition of the Wi-Fi network. System Alerts actions include monitoring the activity and status of your managed Ruckus Wireless devices, and generating reports based on events. The Reports option under System Alerts enables reporting on system events related to connectivity and hotzone association as reported by the managed Ruckus APs. The Events option displays a detailed event timeline that provides trend and historical records of all important events that have occurred over the previous period. The network administrator can quickly return to a specified time to troubleshoot and analyze any abnormal conditions. The Events table displays the most current events for all managed devices.

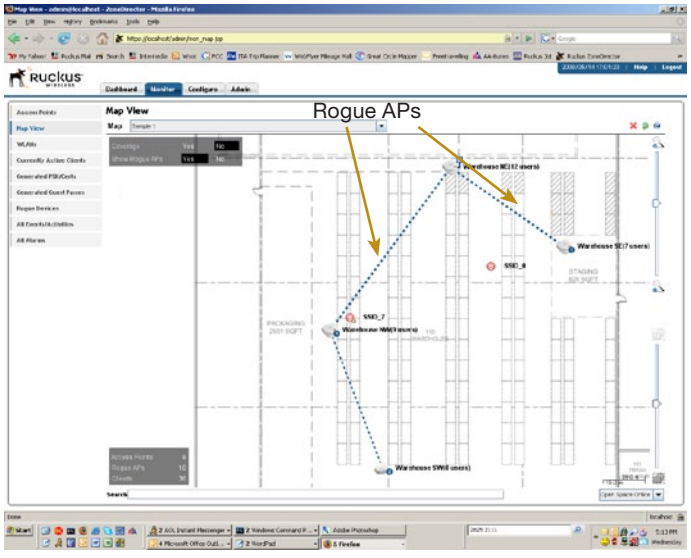
A common attack is when an illegitimate access point is placed nearby and lures unsuspecting clients to connect to it. This may be done by a hacker attempting to steal information or even by a careless employee not adhering to security regulations. Ruckus Wireless ZoneDirector keeps track of all nearby access points and their SSIDs. As seen in **Figure 2**, the ZoneDirector maps the unknown APs in the environment and classifies them as Rogue APs, Evil Twin APs, Ad-hoc networks, and Neighbor networks. Upon detection of a security threat, the ZoneDirector can send e-mail alerts to maintenance personnel.

DoS attacks present a threat to the normal operation of the wireless network, and by extension, to the normal operation of the business. Typical DoS attacks involve excessive messages originating from a hacker's machine. The ZoneFlex products monitor for such situations and ensure that excessive messages are dropped early in the processing to ensure that only minimal resources are consumed.

Requirement 11: Regularly test security systems and processes.

"Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment."

Figure 2: Maps unknown APs in the environment.

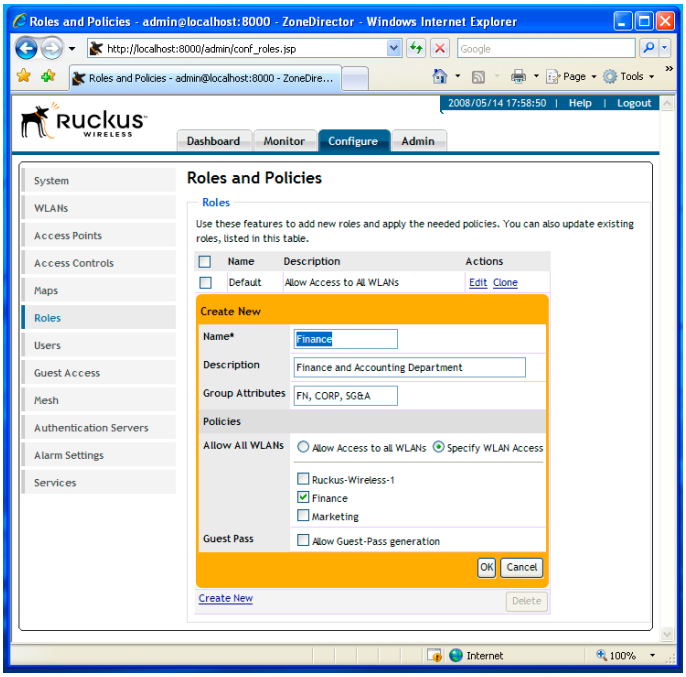


ZoneDirector map view provides visibility to the existence and position of rogue APs.

SmartSec™ for PCI Compliance

RUCKUS ZONEFLEX™ HELPS RETAILERS TO MEET PCI DATA SECURITY STANDARDS

Figure 3: Add and modify roles and policies.



ZoneDirector allows sophisticated policies separating traffic and access privileges for different user groups.

ZoneDirector's customizable dashboard provides a comprehensive at-a-glance network snapshot. Giving the user ability to monitor power levels, change configuration, reboot, control access, and view clients on the WLAN. All from one centralized location.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

"A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of this requirement, "employees" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the company's site."

Highly detailed security policies are fundamental to the protection of wireless data. The ZoneDirector product presents simple, coherent, and consistent policies and reports that allow retailers to enforce, validate, and document their security policy (Figure 3).

In Closing

Current retail environments require businesses to move quickly, work efficiently, and do it securely. Wi-Fi has become a necessary tool to help merchants achieve success in that competitive marketplace. Along with these changes, come opportunities for malicious threats, and new concerns for the business infrastructure.

In response Ruckus Wireless developed the ZoneFlex Smart Wireless LAN (WLAN) system, the first enterprise WLAN solution to deliver hardened security to identify and eliminate threats, robust and easily expandable at an unmatched total cost of ownership. Unlike conventional wireless LAN systems that are costly, complex and cumbersome to deploy, the Smart WLAN system is ideal for organizations that require high-performance, easy deployment and management.

Ruckus Wireless is credited with pioneering "Smart Wi-Fi" technology, and the company's patented hardware and software technologies deliver predictable performance, extended range and real-time adaptability to changing Wi-Fi environments. The ZoneFlex line includes high-density ZoneFlex 802.11a/b/g/n Smart Wi-Fi access points for indoor/outdoor and meshed designs, and the ZoneDirector line of Smart WLAN controllers that manages up to 250 ZoneFlex APs. Completely standards-based, all products integrate advanced features such as adaptive beam forming and steering for highly reliable Wi-Fi with extended range, adaptive meshed connections for eliminating Ethernet cabling to all APs, and power of Ethernet support for eliminating external power supplies while delivering unprecedented performance and reliability.

Designed for simplicity and ease of use, ZoneFlex can be deployed and operated by non-wireless experts. Any organization with little or no IT staff and a limited budget can quickly use the web-based configuration to easily deploy a robust and secure multimedia WLAN in 5 minutes or less.

With ZoneFlex's next generation Smart Wi-Fi technology, merchants are assured that the integrity of their networks will remain uncompromised, secure, and highly reliable in compliance with PCI standards.

Ruckus Wireless, Inc.
350 West Java Drive
Sunnyvale, CA 94089 USA
(650) 265-4200 Ph \ (408) 738-2065 Fx

Ruckus® Simply Better Wireless.

www.ruckuswireless.com