PCI v2.0 Compliance for Wireless LAN

November 2011

This white paper describes how to build PCI v2.0 compliant wireless LAN using Meraki.

Copyright

Trademarks

meraki

www.meraki.com

660 Alabama St.
San Francisco, California 94110

Phone: +1 415 632 5800
Fax: +1 415 632 5899

1. The PCI Standard

The Payment Card Industry Data Security Standard is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments prevent credit card fraud through enhanced security measures. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

The first version of the standard, PCI DSS v1.0, went into effect in January 2005. On January 1, 2007, PCI DSS v1.1 was put in place, replacing PCI DSS v1.0 and the VISA CISP standard. PCI DSS v1.1 reflected changes in the security landscape and offered alternatives in the form of merchant “compensating controls” to make compliance more practical.

On October 1, 2008, the PCI SSC released PCI DSS v1.2. The new standard supersedes v1.1 starting January 1, 2009, and all new audits conducted after this date must adhere to the PCI DSS v1.2 specification. PCI DSS v1.2 clarifies v1.1 requirements that were previously open to interpretation. The new standard also updates requirements based on what the industry has learned about security breaches in the intervening years since v1.1 was issued.

On October 28, 2010, the PCI SSC released PCI DSS v2.0, which became effective on January 1, 2011 and becomes mandatory starting January 1, 2012. This latest version once again provides greater clarity and flexibility to facilitate improved understanding of the requirements and ease implementation for merchants.

2. Network Segmentation and PCI Compliance

PCI audits can be expensive and time-consuming, especially when the audit scope includes your entire network infrastructure. PCI DSS security requirements apply to all system components, where “system components” are defined as “any network component, server, or application that possesses cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access point, network appliances, and other security appliances.

Meraki’s cloud hosted WLAN controller is out of band, meaning that wireless traffic (including cardholder data) does not flow through Meraki’s cloud-hosted controller or any other Meraki infrastructure not behind your firewall. Meraki’s datacenters are SAS 70 type II certified, feature robust physical and cyber security protection, and are regularly audited by third parties. While Meraki’s datacenters are considered out of scope for any WLAN networks PCI audit, Meraki has taken the additional step to obtain PCI certification for our datacenters. Meraki datacenters have passed the Level 1 PCI audit, the most rigorous level for PCI compliance.

One way that the scope of a PCI audit can be reduced is through network segmentation. Network segmentation, or isolation of the cardholder data environment (CDE), from the remainder of the corporate network is <u>not</u> a PCI DSS requirement. However, it is recommended as a means of reducing the scope and cost of a PCI DSS assessment as well as a means of reducing general risk to the organization. If your wireless network is not being used to transmit sensitive cardholder data, then the wireless network can potentially be segmented from the CDE, removing the wireless network from the scope of a PCI audit. There are two ways to achieve this segmentation; locating the WLAN on a completely separate wired network infrastructure that is not connected to the CDE, and using firewall segmentation.

2.1 Wireless Network Not Connected to CDE

Segmentation can be achieved by locating the wireless network on a completely separate, parallel wired network that is not connected to the CDE at all. The access points cannot be connected to any switches, routers or other wired infrastructure that is connected even peripherally to the CDE. In addition, the wireless network must have its own Internet connection (ie. it cannot share a modem or firewall with the CDE network).

2.2 Firewall-Segmented Wireless Network Connected to CDE

If the wireless LAN is connected to the CDE, it can still be segmented from the CDE if it is separated from the CDE with a firewall according to the following PCI-DSS requirement:

> **1.2.3** Install perimeter firewalls between any wireless networks and the CDE, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the CDE.

Meraki's built-in firewall (LAN Isolation) can be used to effectively deny any wireless traffic into the local LAN or CDE. To provide complete segmentation of the wireless LAN from the CDE, LAN isolation must be turned on for *all* SSIDs.

A simple flow chart documenting how a network administrator can ensure that their Meraki wireless network is compliant with these requirements is included in Appendix A. In addition, an example of how to configure a segmented network in Dashboard is included in Appendix B.

2.3 VLANs and Network Segmentation

Virtual local area networks (VLANs) cannot be relied upon for network segmentation (eg. having the CDE on one VLAN and the WLAN on separate VLANs) and will not necessarily take the wireless out of the PCI DSS scope. Hackers can potentially hop across VLANs using known techniques if adequate access controls between VLANs are not put in place.

3. PCI Compliance for a Non-Segmented Meraki Wireless LAN

The following table lists the PCI requirements that are applicable to wireless networks that are part of the CDE (ie. are not segmented from the CDE and/or are transmitting sensitive cardholder data) and how a Meraki wireless LAN can be used to satisfy each requirement:

PCI Requirement	Meraki Meets	How Meraki Helps
1.2.3 Install perimeter firewalls between any wireless networks and the CDE, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the CDE.	✓	This requirement is considered a best practice even for non-segmented networks to limit traffic from the wireless network into the CDE to only that required for business purposes from authorized users and devices. Meraki's built-in firewall (LAN Isolation) and Identity Policy Manager (IPM) can be used to effectively deny or control any wireless traffic into the local LAN or the Internet. LAN isolation should be used for guest SSIDs and IPM custom firewall rules should be used for other SSIDs to limit access to the LAN to business-necessary traffic only.
2.1.1 For wireless environments connected to the CDE or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.	✓	Meraki does not ship with default keys that need to be changed. Meraki supports the latest strong security standards and makes it easy to ensure they are setup correctly.

4.1.1 Ensure wireless networks transmitting cardholder data or connected to the CDE, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.	✓	Meraki supports the strongest encryption standards, including WPA2-PSK, and WPA2-Enterprise (802.11i) with AES encryption.
6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	✓	Meraki can automatically install the latest firmware on APs via the cloud.
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	✓	Meraki provides full, read-only, and lobby ambassador roles. Access can be further restricted to a specific wireless network within an organization.
9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices.	✓	Meraki enterprise access points feature have 3 different physical security mechanisms, including padlock and security screw, that restrict physical access. Meraki APs can also be placed in the plenum to make them more secure.
10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN…verify that logs for external-facing technologies are offloaded or copied onto a secure centralized internal log server media.	✓	Meraki network logs are automatically stored in a centralized environment and backed up in geographically redundant data centers.
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers.	✓	Meraki provides centralized monitoring and logging of all wireless access attempts in a detailed event log.
11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.	✓	Meraki includes IDS, also known as rogue AP detection, which reduces the need for manual scans.

12.3 Develop usage policies for critical employee-facing technologies (for example, remote – access technologies, wireless technologies...) to define proper use of these technologies for all employees and contractors.	✓	Implementer’s responsibility
12.9.5 Include alerts from intrusion detection, intrusion-prevention, and file-integrity monitoring systems.	✓	Meraki’s wireless intrusion detection system generates automatic alerts to warn of potential security threats.

A simple flow chart documenting how a network administrator can ensure that their Meraki wireless network is compliant with these requirements is included in Appendix A. In addition, an example configuration of a PCI-compliant network configuration for a Meraki network that is part of the CDE is contained in Appendix C.

Additional detail on the PCI requirements can be found in [2].

4. Summary

The PCI DSS v2.0 standard describes clear requirements for building compliant wireless LANs.

Meraki's secure wireless solutions offer a simple, cost-effective means of achieving PCI compliance. Meraki's integrated mapping, logging, and rogue AP detection tools eliminate the need to build a solution from component parts. In addition, centralized control of geographically distributed networks makes it easy to implement the same PCI-compliant architecture across large numbers of retail locations.

You can learn more about Meraki solutions for retail at http://www.meraki.com.

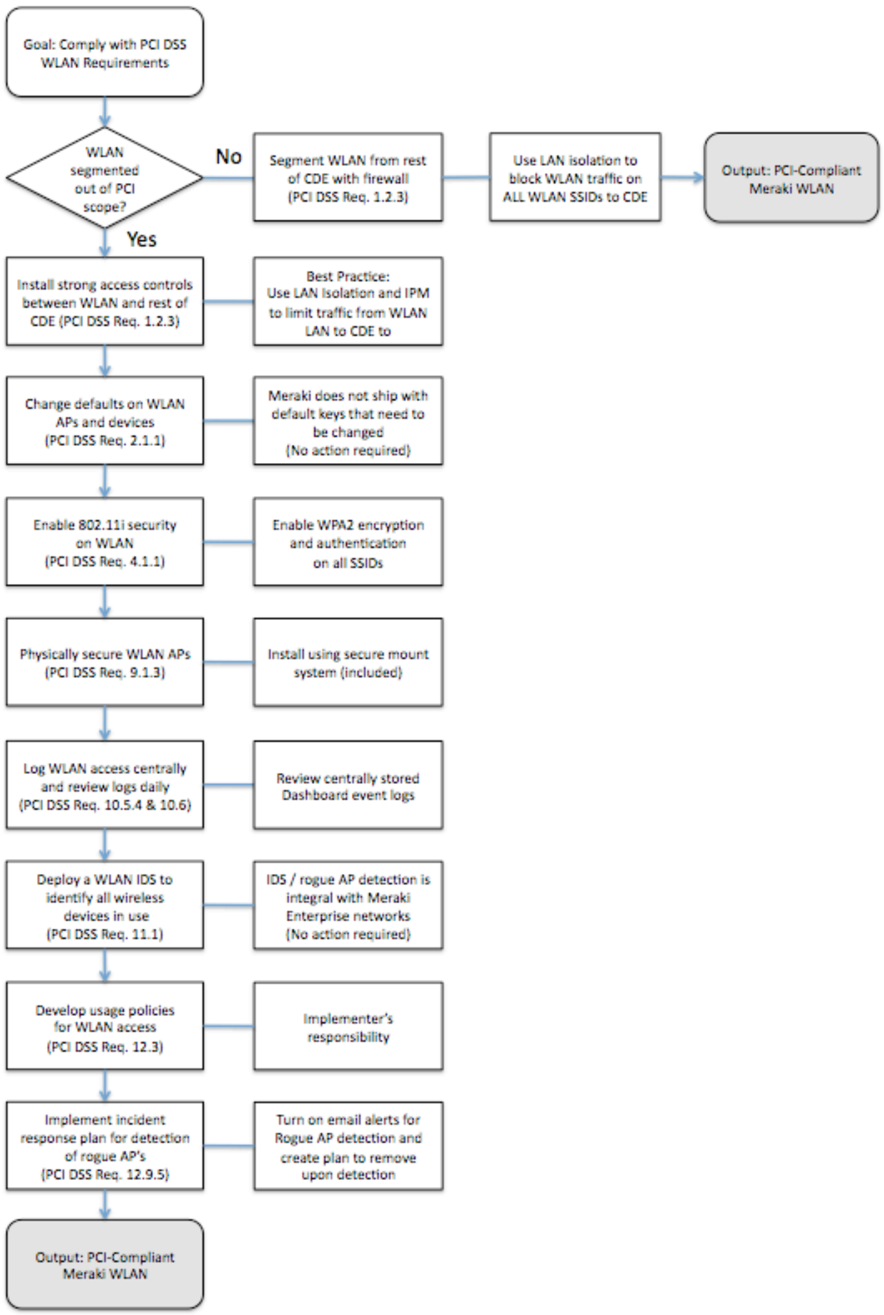
5. References

[1] PCI DSS v1.2 Wireless Guideline, https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

[2] PCI DSS v1.2, https://www.pcisecuritystandards.org/pdfs/pr_080930_PCIDSSv1-2.pdf

[3] PCI DSS v2.0, https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

Appendix A: Meraki PCI-Compliant Network Deployment Flowchart

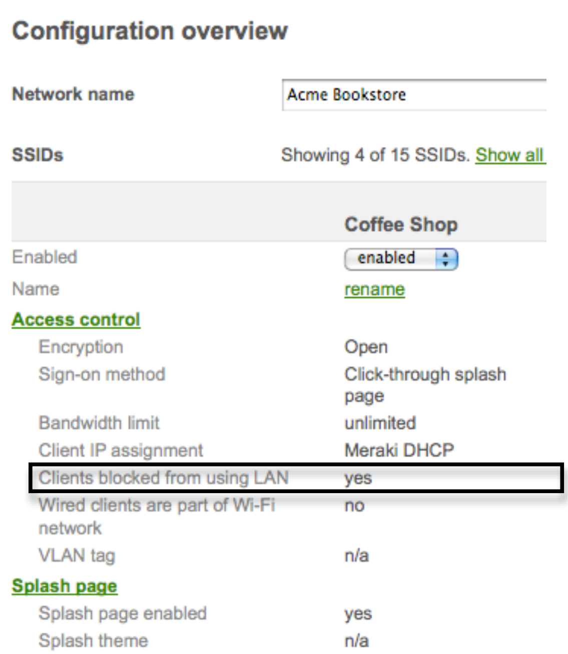


Appendix B: Example PCI-Compliant Configuration of Segmented WLAN

The following is an example of how to configure a Meraki wireless LAN in Dashboard, Meraki's web-based management console, such that it is segmented out of the CDE using the built-in firewall. This example network is in a coffee shop that is located inside a retail bookstore, where a wireless network is installed in the coffee shop to provide guest access to customers. In other words, the network is not used for any business purposes and does not transmit any sensitive cardholder data. However, the wireless access points are plugged into a router that is part of the CDE so the wireless LAN is not on a completely separate infrastructure and can be considered connected to the CDE. The wireless network will be segmented out of CDE using the built-in Meraki firewall so that it is removed from the scope of a PCI audit and is not subject to PCI requirements.

In Figure 1, the configuration of the coffee shop SSID (the only SSID in this network) can be seen. As can be seen under the "Clients blocked from using LAN" feature, the built-in LAN isolation firewall has been turned on to block all access from the wireless network into the CDE. When LAN isolation is enabled, all traffic from the wireless network to any private IP address (10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16) is blocked. This segments the wireless network out of the CDE and out of the scope of a PCI audit.

Figure 1: Dashboard Configuration for Segmented Wireless Network

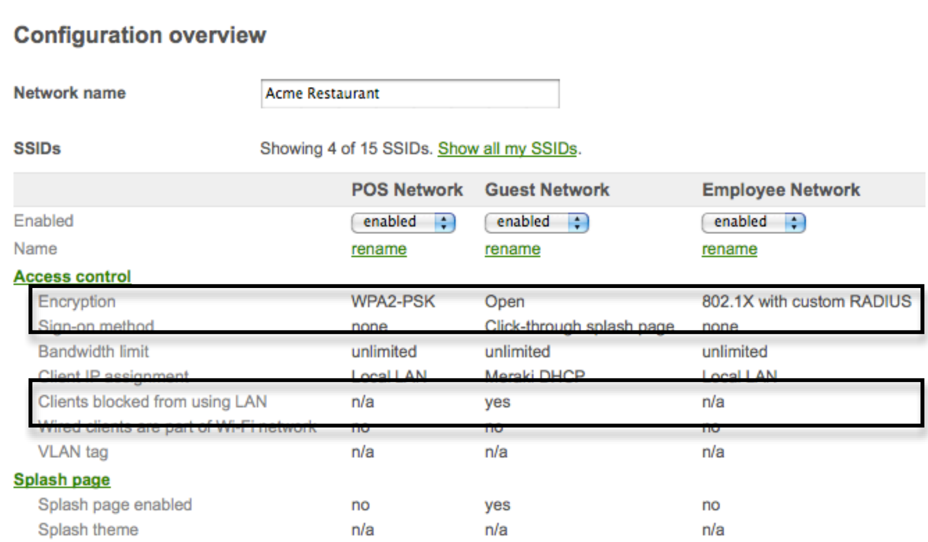


Appendix C: Example PCI-Compliant Multi-use Network Configuration

The following is an example of how a multi-use Meraki wireless LAN can be configured to be PCI-compliant in Dashboard. This network is deployed in a restaurant that is using the wireless network for employees in the back office, for wireless POS devices used by the servers at the tables, and for Internet access for their guests. They have configured three SSIDs, one for each user group: POS Network, Employee Network and Guest Network. In this case the network is part of the CDE since sensitive cardholder data (e.g., credit card numbers) are being transmitted over the network.

Figure 2 shows an overview of how the network's SSIDs have been configured in Dashboard to assure PCI compliance. The use of 802.11i strong security (PCI-DSS Req. 4.1.1) is satisfied using WPA2-PSK on the POS Network and WPA2-Enterprise with 802.1x authentication and encryption on the Employee Network (seen under the "Encryption" setting). The installation of a perimeter firewall between the wireless and the CDE (PCI-DSS Req. 1.2.3) to control access between the wireless LAN and the CDE can also be seen in the Figure 2 under the "Clients blocked from using LAN" setting. This follows the best practice to limit access to the CDE to that required for business purposes.

Figure 2: Dashboard Configuration Overview for All SSIDs



In Figure 3, which shows custom firewall rules that have been put in place on the POS Network SSID, it can be seen that CDE access has been limited to the server running the POS application software and that access to all other areas of the CDE have been blocked.

Figure 3: Firewall Settings for POS Network

Firewall: Custom firewall rules
What is this?

Firewall rules *

#	Policy	Protocol	Port	Destination *	Comment	Actions
1	Allow	TCP	any	172.16.30.231/32	Allow POS Device access to Server	
2	Deny	TCP	any	172.16.0.0/16	Block TCP access to rest of CDE	
3	Deny	UDP	any	172.16.0.0/16	Block UDP access to rest of CDE	
4	Allow	Any	Any	Any	Default rule	

Add a rule

In Figure 4, which shows the Dashboard firewall settings for the Employee Network SSID, it can be seen that employees are allowed access only to a printer in the CDE and that access to the rest of the CDE has been blocked.

Figure 4: Firewall Settings for Employee Network

Firewall: Custom firewall rules
What is this?

Firewall rules *

#	Policy	Protocol	Port	Destination *	Comment	Actions
1	Allow	TCP	any	172.16.30.230/32	Allow access to office printer	
2	Deny	TCP	any	172.16.0.0/16	Block TCP access to rest of CDE	
3	Deny	UDP	any	172.16.0.0/16	Block UDP access to rest of CDE	
4	Allow	Any	Any	Any	Default rule	

Add a rule

Finally, Figure 5 illustrates how the built-in firewall's LAN isolation feature has been turned on to block all access to the CDE from the Guest Network SSID.

Figure 4: Firewall Settings for Guest Network

#	Policy	Protocol	Destination	Port	Comment	Actions
1	Deny	Any	Local LAN	Any	Wireless clients accessing LAN	

These Dashboard configuration settings, in addition to complying with the other steps in the flowchart in Appendix A will ensure a PCI-compliant Meraki wireless network.