# Meraki White Paper:
# Wireless LAN Security

**Version 1.0, March 2009**

Robust security is a requirement for many companies deploying a wireless network. However, creating a secure wireless network has often been difficult and time-consuming. This paper describes the security requirements for most companies and how Meraki can help them meet those challenges easily and at a low cost.

**Copyright**

**Trademarks**

Meraki® is a registered trademark of Meraki, Inc.

www.meraki.com

660 Alabama St.
San Francisco, California 94110

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

# Table of Contents

# 1    The Need For Security

While security is important for all networks, wireless LANs deserve special consideration since they are subject to an increased level of risk. First, since wireless extends beyond the walls of an organization, physical security is less effective than with wired networks. Second, wireless network abuse has become more common, with tools that assist wireless hacking widely available, and companies are a target. Finally, 802.11 protocols operate on unlicensed spectrum using well-understood protocols, resulting in a proliferation of devices that are able to access a corporate network.

Wireless networks are also subject to several regulations that mandate the high security networks, including PCI, HIPAA, and SOX. The credit card industry requires those processing credit card transactions to comply with PCI standards, in order to mitigate the chances of card number theft and fraud. All merchants using payment cards must build and maintain a secure network, protect and encrypt cardholder data, and regularly monitor and test their networks, including wireless networks.

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996. Many health care institutions are covered by it and are required to maintain administrative, technical, and physical safeguards to ensure integrity and confidentiality of patient data. Wireless networks are potentially vulnerable and must be secured in order to comply.

Finally, public companies are subject to the Sarbanes-Oxley act (SOX) and similar measures outside the U.S. SOX requires companies to maintain and assess internal control structures and procedures for financial reporting and to assess the effectiveness of these internal control structures. Network security is typically part of the control review.

Thus, a combination of regulatory requirements, as well as common sense, make wireless security an important consideration.

## 2    What Doesn't Work

There are many possible methods to implement wireless security. An understanding of which methods are ineffective, and why, is necessary in order to avoid them.

Some companies have attempted to contain the wireless signal within the physical perimeter of the coverage area. Specialized directional antennas might be used for this purpose. In reality, RF propagation is highly unpredictable. WiFi signals reflect off of walls, as well as furniture and other everyday objects, which may be moved as an office is reconfigured. It is inevitable that some wireless signal will penetrate beyond the confines of most buildings, so it is best to assume that outsiders will have a signal strong enough to attempt to access the network.

Service Set Identifier (SSID) cloaking is another ill-advised security strategy. Software that allows non-technical users to find and associate with hidden SSIDs is readily available on the Internet. While hiding SSIDs may deter the most casual intruder, it is not sufficient to protect the network. Worse, it can impair usability as the trusted user may struggle to associate with the network.

Each 802.11 client has a unique MAC address assigned at the time of manufacture. It is possible to restrict access to a network to only approved MAC addresses. Unfortunately, this approach has a number of drawbacks. First, it is difficult to administer: keeping track of long lists of MAC addresses is error-prone and cumbersome. Second, it is fundamentally insecure. Software is commonly available that allows a client to change (or "spoof") its MAC address. An intruder can simply listen to the wireless traffic, identify an authorized MAC address, and set his MAC address accordingly. This exploit requires just a few minutes to execute.

Wireless Equivalency Protocol, or WEP, was the 802.11 group's first security mechanism. Unfortunately, it proved very easy to break WEP, and tools to do so are widely available. As a result, WEP is typically not considered secure enough for corporate use. Worse, it may give users a false sense of security.

# 3    Recommended Security Architectures

While there are many ways to set up a secure wireless system, we will describe three that are applicable to a wide variety of environments. This section describes the security configuration of an employee or trusted network. Later, we discuss how to treat guests through the use of a separate Virtual Access Point (also known as a separate SSID).

## 3.1    Open with VPN

An "open with VPN" approach starts with the assumption that all wireless data is insecure. Neither encryption nor authentication is performed before users are allowed to get on the network. Typically, users who get on the network are able to access the Internet but not able to access the LAN. Those who need LAN access must VPN into the corporate network, as if they were coming in from outside the building.

There are at least three ways to prevent traffic on the open network from accessing the corporate LAN. A common approach is usage of VLAN tagging to isolate all wireless traffic outside the firewall. This approach is simple and effective, but does require that the company's switches support VLANs and, depending on the given wired infrastructure, can be difficult to configure and maintain. Alternately, Meraki provides an integrated LAN Isolation feature. LAN Isolation causes wireless routers to drop all packets destined for the LAN, and only allow Internet traffic to proceed. The final approach is to use a separate wired network and Internet connection. This approach is expensive but simple and highly secure.

The major advantage of the open architecture is its simplicity. No special client configuration is necessary. In addition, the security principle is straightforward: all wireless traffic is untrusted. Anyone wishing to access corporate resources is treated as if they are coming from outside the firewall and must VPN.

There are drawbacks to this approach. First, VPN access can be inconvenient to users and deter them from using the wireless network. Second, not all clients support VPN, especially devices like PDAs and scanners. Finally, load on the VPN server will likely increase, which can add cost.

### 3.2    Shared Key (WPA2-PSK)

In the shared key approach, all authorized clients receive a secret key. The key might be provided to employees or installed on their machine by an IT administrator. While there are three shared key mechanisms (WEP, WPA, and WPA-2), Meraki recommends WPA-2 since it is the most secure. As mentioned above, WEP is not secure and should be avoided.

All traffic that comes in through WPA2-PSK is typically allowed access to the corporate LAN.

The shared key approach can be highly effective for small to midsize organizations. It is simple and supported by almost all clients, including PDAs and scanners.

The most significant drawback of the shared keys is that they can be difficult to administer. If an employee who knows the key leaves the organization, the key might need to be changed for everyone in order to keep the network secure. In addition, knowledge of the key may leak outside the organization, enabling outsiders to access the corporate network.

### 3.3    User Authentication (WPA2-Enterprise)

WPA2-Enterprise, also known as 802.1x, is considered by many to be the "gold standard" of wireless security. In this architecture, each client (known as a supplicant) uses a unique username and password to authenticate on the wireless network. The client's username and password are checked against any Active Directory or LDAP server that supports the RADIUS protocol (and most do). Meraki supplies an integrated RADIUS server that companies can use instead of a stand-alone server if they wish.

The primary advantages of WPA2-Enterprise are that it is highly secure and scales well. IT administrators can re-use their existing authentication infrastructure, so as employees come and go they are automatically added and removed from the wireless network. There is also no need to VPN.

Since 802.1x is a relatively new standard, client support is still evolving. As of 2009, support is common on most laptop and PC operating systems. However, support for PDAs, scanners, and other devices still varies. In addition, client configuration can sometimes be complex.

While implementation of 802.1x has often been highly complex, Meraki has simplified the process significantly. 802.1x takes just a few clicks to deploy, and is no more difficult than implementing WPA2-PSK.

### 3.4    Hybrid Approaches

Meraki allows modular use of the features of any of the recommended architectures described above in a "mix and match" manner. For example, one might offer a WPA2-Enterprise solution for all Windows and Mac users using the standard corporate image. Clients that lack 802.1x support would use the open network and VPN back in if needed.

### 3.5    Summary

The following table summarizes the advantages and disadvantages of the approaches described above.

|  | Open / VPN | Pre-Shared Key | User Auth (802.1x) |
|---|---|---|---|
| **Client support** | 3 | 3 | 2 |
| **Scalability** | 4 | 1 | 4 |
| **Employee convenience** | 1 | 3 | 3 |
| **Security** | 4 | 3 | 4 |

# 4    Guest Access

Guests, consultants, and contractors frequently need to connect to the company's network. These people typically need access to the Internet only, or more rarely, to a limited number of network resources such as printers and file shares. Meraki recommends creating a separate Virtual Access Point for use by guests, with its own SSID and security policies.

There are a number of security strategies that can be applied to guests, including open and registered. In the open scenario, any client can associate with and use the network. Administrators might choose to display a splash page with terms of service. In the registration scenario, guests are given a username and password, perhaps provided to them by their host or the receptionist. The username might be static, e.g., "guest," or could be unique to that specific guest. Meraki provides a tool for receptionists and other non-technical staff to easily add guests to the guest network. This way, the company knows exactly who is accessing its network.

Once authorized, guest traffic is typically placed on a separate VLAN using the Meraki LAN Isolation feature. For more details on guest access, please see the Meraki Guest Access White Paper.

# 5    Example Configuration

Meraki's virtual network isolation feature allows companies to run multiple networks that have completely different security policies. The following table shows a typical security configuration for a corporate network featuring guest access and wireless VOIP phones.

| Service Parameter | Virtual AP 1 | Virtual AP 2 | Virtual AP 3 |
|---|---|---|---|
| **Users** | Employees | Guests | Phones |
| **SSID** | Corp | Guest Access | Corp – VOIP |
| **Network Access** | LAN & Internet | Internet only | LAN & Internet |
| **Client bandwidth** | Unlimited | 5 mbit/s | Unlimited |
| **Quality of service** | Normal | Normal | High |
| **Authentication** | 802.1x / LDAP | Open | WPA2-PSK |

# 6    The Meraki Edge

Meraki offers some unique benefits when building a secure, scalable wireless system. The key advantages include extreme ease of use, consistent management across multiple sites, and cost effectiveness.

While many systems tout ease of use, field deployment interviews suggest that the reality differs from the sales talk. Many systems still feature archaic command-line interfaces, require multi-day training courses and certification programs, and publish 500-page manuals. Effective security need not have such extensive requirements. Further, when security is made complex to this degree, the chances of configuration errors and unintended consequences increase.

Meraki offers a powerful yet streamlined security interface. The system is managed entirely through a modern, hosted graphical web interface. In addition, there are very few moving parts. The only pieces of hardware on the company's site are the access points. There are no controllers in the DMZ or complex multi-site tunnels to create.

Meraki also makes it easy to ensure that security policies are applied consistently throughout organizations with multiple sites. All networks for the organization are visible from a single account. For example, a company might have a corporate headquarters, branch offices, and manufacturing plants. Reports for the networks at each location can be received by both the centralized IT team as well as local administrators. Finally, because the networks are so easy to establish, it is possible to create secure networks in employee homes, or on a temporary basis (e.g., at a sales conference).

Finally, Meraki does not place an undue burden on the existing wired network infrastructure. For example, VLANs can be used to segregate wireless traffic, but Meraki also provides an integrated traffic segregation facility. Meraki also includes a number of other integrated security services, such as integrated bandwidth limits (for guests), or integrated adult content filters (for compliance).

# 7    Conclusion

Companies deploying a wireless network need to take security into consideration. However, security does not need to be difficult and time-consuming. Meraki makes it easy to implement the security policy that works best for a particular organization, whether it has ten clients or tens of thousands.

# 8    References

1.   Meraki Guest Access White Paper

2.   Meraki Network Design Guide

These documents are available for download at meraki.com.