Cisco Meraki

White Paper

Air Marshal

SEPTEMBER 2013

This document discusses potential security threats in a WiFi environment, and outlines how enterprises can use a best-in-class Wireless Intrusion Prevention System (WIPS) such as Meraki's Air Marshal to create a secure network with preemptive protection policies and security alerts.

Table of Contents

Introduction

Wireless Security Threats in an Enterprise Environment

Secure WiFi access has become a critical component of enterprise networking. WiFi Internet access is critical for corporate communication in verticals including financial services, retail, and distributed enterprise. Due to the widespread use of WiFi and variety of use cases (e.g., point-of-sale (POS) communications, corporate access, warehouse inventory, asset tracking, WiFi services for targeted advertising), the wealth of information transmitted across the wireless medium has skyrocketed. Data transmitted over wireless increasingly contains sensitive personal and financial data. Unfortunately, the tremendous growth in wireless has been accompanied with an increasingly widespread ability to obtain open-source hacking tools that can compromise a wireless network through impersonation of client devices and access points.

Examples of common threats in a modern WiFi environment include:

Network impersonation: achievable by purchasing any consumer-grade access point and copying an SSID, "tricking" clients into thinking that this SSID is available and snooping on their information transactions.

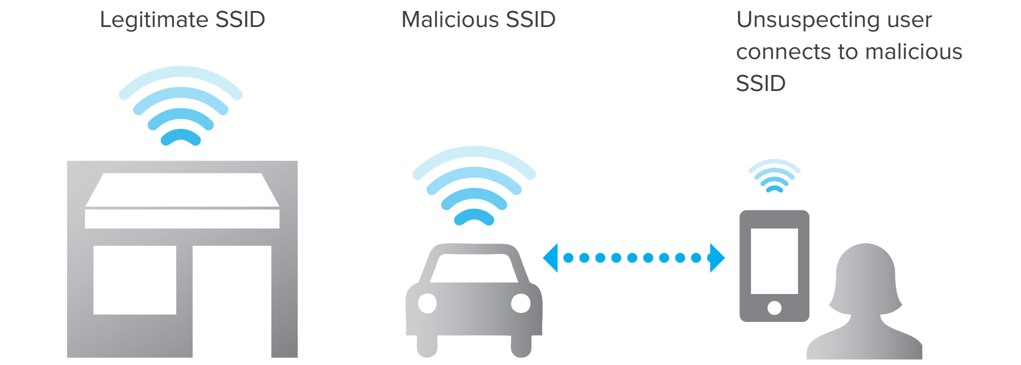


Figure 1: Example of SSID spoofing threat in a retail environment

Wired network compromise: achieved by an unsuspecting employee or student plugging in a consumer-grade access point into the wired infrastructure and exposing the LAN to hackers.

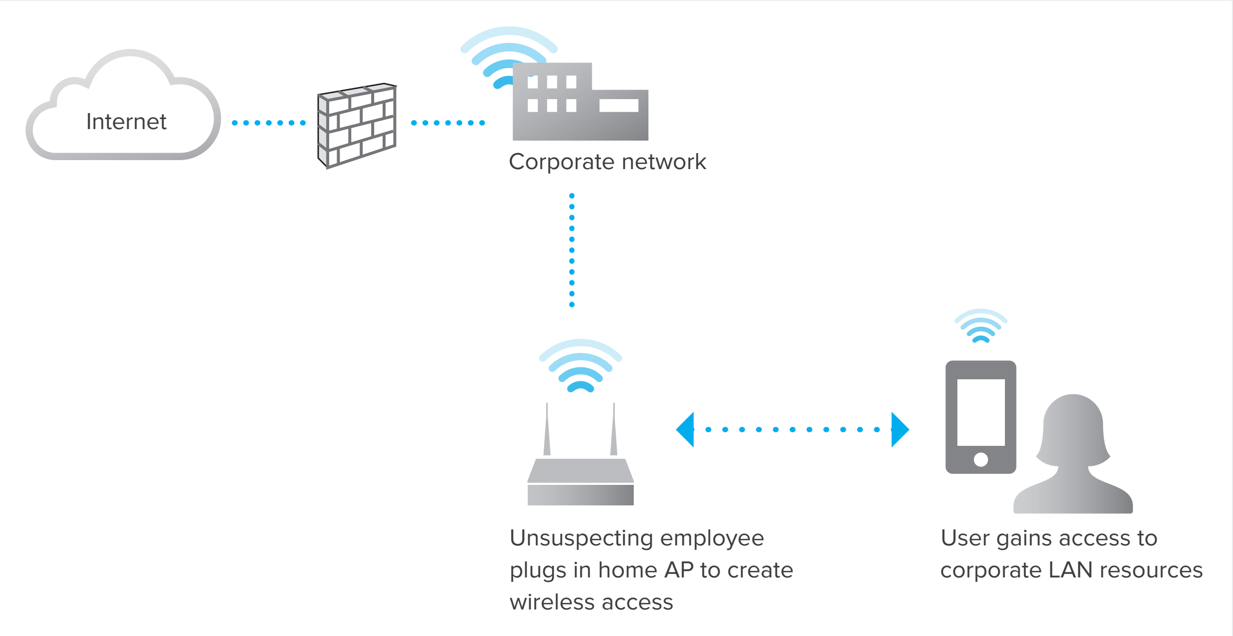

Internet
Corporate network
Unsuspecting employee plugs in home AP to create wireless access
User gains access to corporate LAN resources

Figure 2: Example of accidental wired LAN compromise in corporate environment

To successfully protect an enterprise network, a Wireless Intrusion Prevention System (WIPS) should provide powerful wireless intrusion scanning capabilities, enabling detection and classification of different types of wireless threats, including rogue access points and wireless hackers. Access points can be put in either dedicated scanning mode or sensor mode for real-time intrusion detection and threat remediation. Additionally, a WIPS system should be configurable with intuitive auto-containment policies to facilitate pre-emptive action against rogue devices. Once a threat has been detected, the WIPS platform should kick into gear to enact powerful policies, including intelligent auto-disablement of APs matching a pre-defined criteria and generating different tiers of e-mail alarms based on the type of threat in your airspace.

In addition to protecting airspace against hackers with malicious intent, it is valuable to be able to mark or group high-value 'VIP' wireless clients into a special category, where they can be tracked, to ensure they never leave the wireless network. Examples of VIP clients include high-value corporate assets — these devices belong to the organization and should never associate to a wireless network other than your own (e.g., corporate issued laptops, point-of-sale registers or barcode scanners in a retail environment, etc.) These VIP clients should only associate to the corporate network. If they do stray to a foreign network, it would be classified as an 'accidental association.' The ability to detect and generate alerts when a VIP client strays over to a rogue infrastructure can be invaluable in security conscious environments.

Cisco Meraki's Air Marshal mode allows network administrators to meet these requirements and design an airtight network architecture that provides an industry-leading WIPS platform in order to completely protect the airspace from wireless attacks. The remainder of this document describes in greater depth wireless threats and the necessary security measures required to remediate against these threats; the conclusion then summarizes the setup and configuration process for Meraki's Air Marshal WIPS platform in order to achieve the highest security protection possible.

Wireless Threats

Understanding the wireless airspace around you can help to take effective measures, both preventive and reactive, to ensure that the wireless airspace is secure and interference-free from other wireless networks. A number of different threats exist in the modern enterprise environment, facilitated by easy access to cheap consumer-grade 802.11 equipment, along with open-source hacking tools that can be used to simulate and spoof devices and generate traffic floods. Leading enterprise WLAN providers such as Cisco provide built-in WIPS features to ensure detection and remediation against these threats.

Threat classifications

Visibility and classification of potential wireless threats is an important first step in securing the wireless network and network infrastructure as a whole. Once classified, remediation can be taken against confirmed threats and innocuous alerts can be dismissed. Cisco Meraki Air Marshal automatically classifies threats into the following categories to provide the greatest visibility and overall protection for your network.

Rogue SSIDs

SSID and AP spoofs: the malicious impersonation of a legitimate AP by either spoofing the SSID name or, even worse, the SSID name and the BSSID (the wireless MAC address, which makes it indistinguishable from the original AP).

Rogue SSID seen on LAN: SSIDs that are broadcast by rogue APs and seen on wired LAN; this could suggest compromise of the wired network.

Other SSIDs

Interfering SSIDs: wireless networks that are broadcasting and could be causing RF interference, as well as attracting accidental associations from clients who are supposed to be connecting to your own network.

Ad-Hoc SSIDs: modern smartphones and mobile devices are capable of associating to WiFi networks and then re-broadcasting the SSID, essentially acting as a wireless bridge. Devices in ad-hoc mode can connect to a client AP and create a gateway for wireless hackers.

Malicious Broadcasts

Denial of Service (DoS) attacks are attempts to prevent clients from associating to the legitimate AP by sending an excessive number of broadcast messages to clients. DoS attacks could be from malicious clients, APs, or even another WIPS system in the area that considers the corporate network a threat and is attempting to remediate.

Packet Floods

Clients or APs that are sending an excessive number of packets to your AP. Packets are monitored and classified based on multiple categories including beacon, authentication and association frames. An excessive number of any category of packets seen within a short time interval will be marked in Air Marshal as a packet flood.

Client Straying Threats

Accidental associations: client devices that belong to your infrastructure associating to a wireless network in your airspace that has not been sanctioned by your corporation. Straying clients could accidentally connect to Rogue SSIDs or spoofed SSIDs if proper action is not taken to protect the wireless airspace.

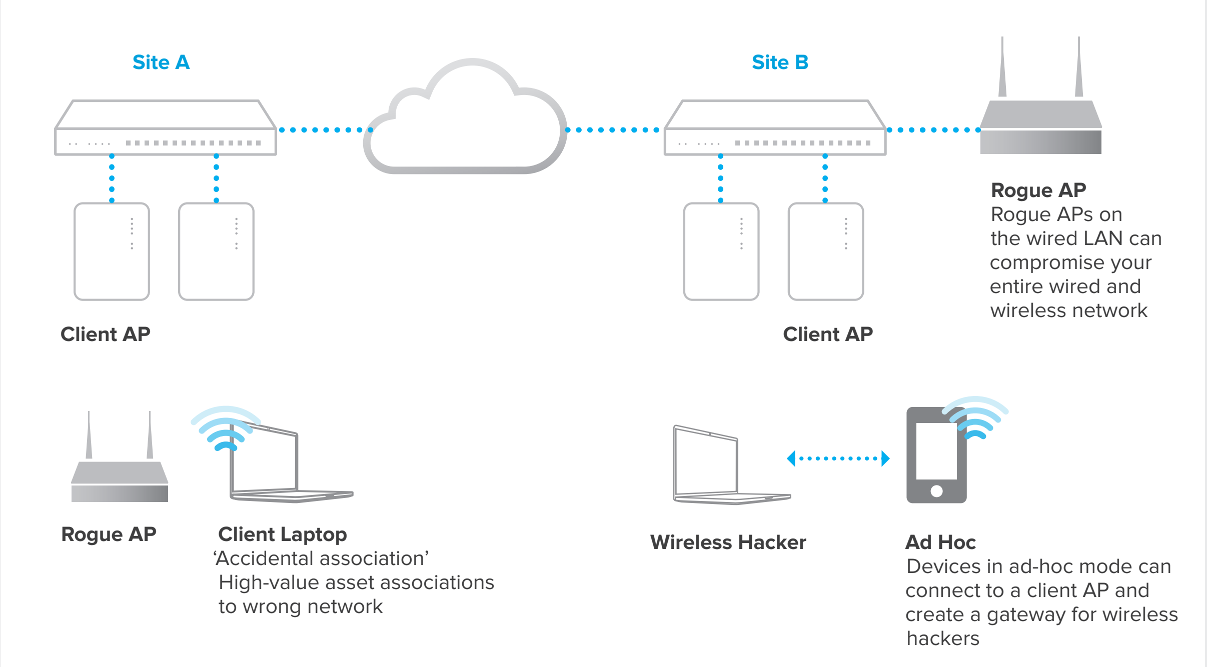

Site A
Site B
Client AP
Client AP
Rogue AP
Rogue APs on the wired LAN can compromise your entire wired and wireless network
Rogue AP
Client Laptop
'Accidental association'
High-value asset associations to wrong network
Wireless Hacker
Ad Hoc
Devices in ad-hoc mode can connect to a client AP and create a gateway for wireless hackers

Figure 3: Security threats in an enterprise environment

PCI Compliance

Understanding and remediating against wireless threats is also a requirement under the Payment Card Industry Data Security Standard (PCI DSS), a standard required for retailers to follow when processing credit card data over WLAN networks. Examples of WIPS requirements under PCI DSS include:

Section 9.1.3 Physical Security: Restrict physical access to known wireless devices.

Section 10.5.4 Wireless Logs: Archive wireless access centrally using a WIPS for 1 year.

Section 11.1 Quarterly Wireless Scan: Scan all sites with card dataholder environments (CDE) whether or not they have known WLAN APs in the CDE. Sampling of sites is not allowed. A WIPS is recommended for large organizations since it is not possible to manually scan or conduct a walk-around wireless security audit of all sites on a quarterly basis

Section 11.4 Monitor Alerts: Enable automatic WIPS alerts to instantly notify personnel of rogue devices and unauthorized wireless connections into the CDE.

Section 12.9 Eliminate Threats: Prepare an incident response plan to monitor and respond to alerts from the WIPS. Enable automatic containment mechanism on WIPS to block rogues and unauthorized wireless connections.

Threat Remediation using Meraki's Air Marshal WIPS platform

A careful study of the common wireless security threats has led to the development of Meraki's Air Marshal platform, which allows access points to be turned into dedicated WIPS sensors called 'Air Marshal' APs. Air Marshal is a WIPS platform which comes equipped with security alerting and threat remediation mechanisms. This includes the following:

a. Monitoring and alerting: a robust and intuitive display of all of the threats for a particular network, including auto-alerting based on the network administrator's preferences. Monitoring techniques include:

i. Rogue AP monitoring: Meraki APs scan across all 2.4 GHz and 5 GHz channels to build a list of rogue access points in the nearby vicinity. In addition, further mechanisms are in place to track APs on the wired LAN network by inspecting traffic on the wired port of the Meraki AP, and using this to build a list of rogue APs that may be on the wired LAN. E-mail alerts will be triggered and sent based on parameters predefined by the network admin.

ii. Tracking 'client straying' of VIP clients: Air Marshal allows tagging of VIP clients and an alert is sent if those clients connect to a unsanctioned SSID. Air Marshal does this by monitoring traffic with the source MAC address of the VIP clients. Wireless devices communicate with three types of 802.11 frames: management frames are used during the probing and association process. Control and data frames are used when the client is actually connected. If Air Marshal sees data frames originating from VIP clients which are not connected to the corporate wireless network, an alert can be sent to administrators for remediation.

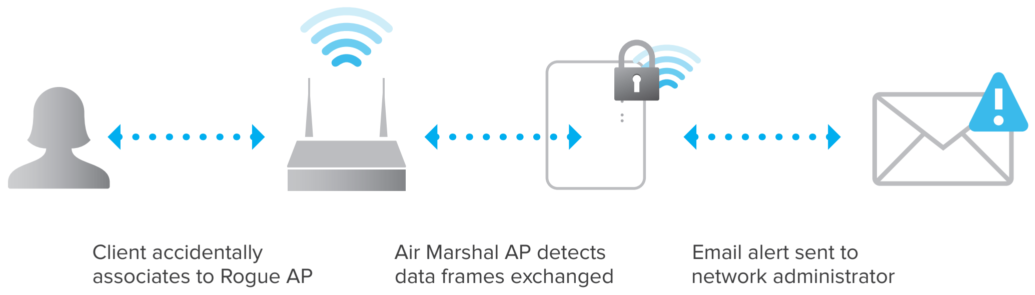

Client accidentally associates to Rogue AP
Air Marshal AP detects data frames exchanged
Email alert sent to network administrator

Figure 4: Tracking accidental associations

b. Remediation mechanisms: Air Marshal APs come equipped with the ability to automatically 'contain' rogue APs and alert on rogue APs and accidental associations, allowing for administrators to take physical action to remove rogue APs and recover straying devices.

What is containment?

‘Containment’ is a common mechanism that calls for the Air Marshal AP to impersonate or spoof the rogue AP in order to render it ineffective. Air Marshal does this by generating a large number of 802.11 packets and using the BSSID of the rogue AP as the the source MAC address. Air Marshal APs also provides more sophisticated containment methods including spoofing clients attempting to associate to the rogue by generating packets with the source MAC of the clients; this allows for a ‘two-way’ spoof and ensures a fool-proof shutdown of the rogue AP.

Packet types generated by WIPS during containment:

1. 802.11 Broadcast deauthorizations with source = Rogue AP, destination = broadcast
2. 802.11 Deauthorization messages with source = Rogue AP, destination MAC = client
3. 802.11 Deauthorization and disassociate messages with source = client, destination = Rogue AP

#3 ensures that more sophisticated 802.11 clients with battery-saving capabilities are also unable to connect to the rogue, as they may ignore deauthorization messages from the Rogue AP if they are ‘sleeping’ in order to save battery life.

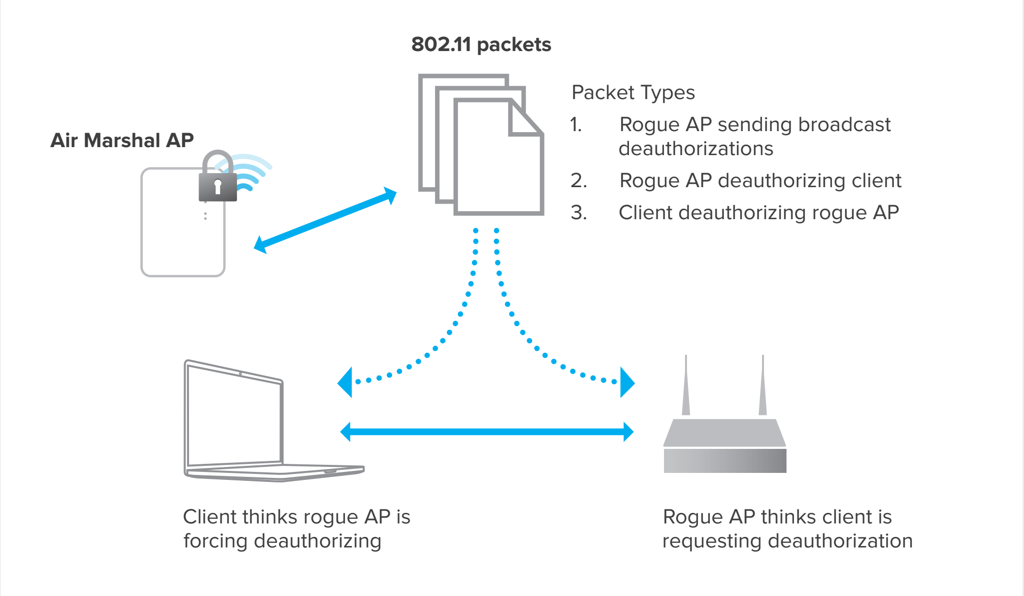
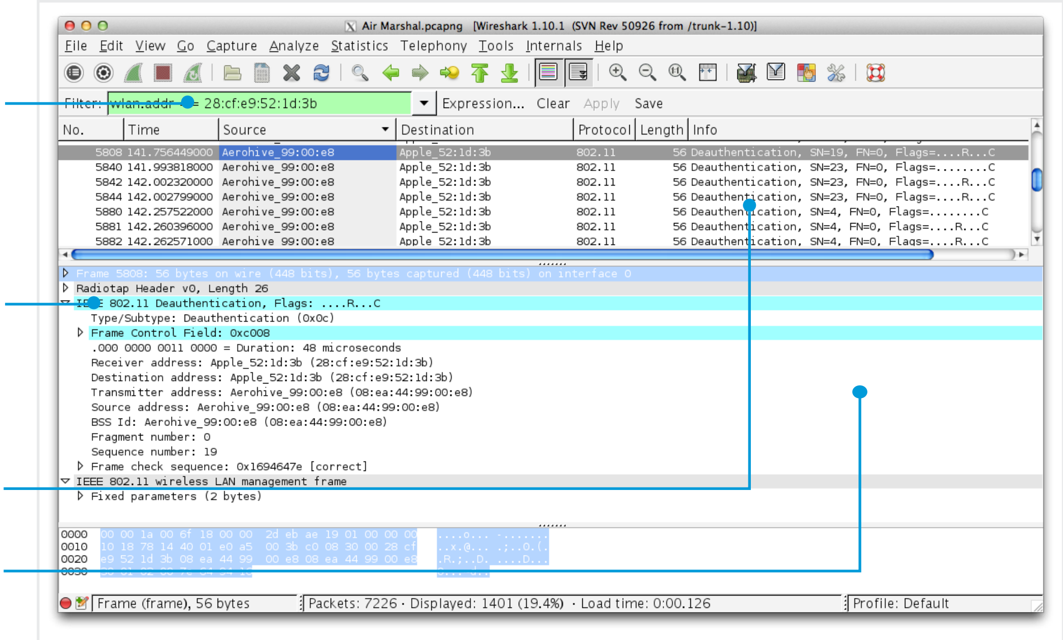

802.11 packets
Air Marshal AP
Packet Types
1. Rogue AP sending broadcast deauthorizations
2. Rogue AP deauthorizing client
3. Client deauthorizing rogue AP
Client thinks rogue AP is forcing deauthorizing
Rogue AP thinks client is requesting deauthorization

Figure 5. Rogue AP ‘Containment’ explained

[2] As containment renders any standard 802.11 network completely ineffective, extreme caution should be taken to ensure that containment is not being performed on a legitimate network nearby and, action should only be taken as a last resort. Please see the Cisco Guidance Note on de-authentication technology for more information.
http://wnbu-press.cisco.com/files/2015/01/Cisco_Guidance_Note.pdf



Air Marshal.pcapng [Wireshark 1.10.1 (SVN Rev 50926 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: wlan.addr == 28:cf:e9:52:1d:3b
Expression... Clear Apply Save

```
No.  Time           Source               Destination        Protocol Length Info
5808 141.756449000  Aerohive_99:00:e8    Apple_52:1d:3b     802.11   56 Deauthentication, SN=19, FN=0, Flags=....R...C
5840 141.993818000  Aerohive_99:00:e8    Apple_52:1d:3b     802.11   56 Deauthentication, SN=23, FN=0, Flags=........C
5842 142.002320000  Aerohive_99:00:e8    Apple_52:1d:3b     802.11   56 Deauthentication, SN=23, FN=0, Flags=....R...C
5844 142.002799000  Aerohive_99:00:e8    Apple_52:1d:3b     802.11   56 Deauthentication, SN=23, FN=0, Flags=....R...C
5880 142.257522000  Aerohive_99:00:e8    Apple_52:1d:3b     802.11   56 Deauthentication, SN=4, FN=0, Flags=........C
5881 142.260396000  Aerohive_99:00:e8    Apple_52:1d:3b     802.11   56 Deauthentication, SN=4, FN=0, Flags=....R...C
5882 142.262571000  Aerohive_99:00:e8    Apple_52:1d:3b     802.11   56 Deauthentication, SN=4, FN=0, Flags=....R...C

▷ Frame 5808: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
▷ Radiotap Header v0, Length 26
▽ IEEE 802.11 Deauthentication, Flags: ....R...C
    Type/Subtype: Deauthentication (0x0c)
  ▷ Frame Control Field: 0xc008
    .000 0000 0011 0000 = Duration: 48 microseconds
    Receiver address: Apple_52:1d:3b (28:cf:e9:52:1d:3b)
    Destination address: Apple_52:1d:3b (28:cf:e9:52:1d:3b)
    Transmitter address: Aerohive_99:00:e8 (08:ea:44:99:00:e8)
    Source address: Aerohive_99:00:e8 (08:ea:44:99:00:e8)
    BSS Id: Aerohive_99:00:e8 (08:ea:44:99:00:e8)
    Fragment number: 0
    Sequence number: 19
  ▷ Frame check sequence: 0x1694647e [correct]
▽ IEEE 802.11 wireless LAN management frame
  ▷ Fixed parameters (2 bytes)

0000  00 00 1a 00 6f 18 00 00  2d eb ae 19 01 00 00 00   ....o... -.......
0010  10 18 78 14 40 01 e0 a5  00 3b c0 08 30 00 28 cf   ..x.@... .;..0.(.
0020  e9 52 1d 3b 08 ea 44 99  00 e8 08 ea 44 99 00 e8   .R.;..D. ....D...
0030  30 01 02 00 7e 64 94 16                            0...~d..

Frame (frame), 56 bytes   Packets: 7226 · Displayed: 1401 (19.4%) · Load time: 0:00.126   Profile: Default
```

iPhone client accidentally associating to Rogue AP

802.11n packet type is deauthentication, source is Rogue AP and destination is client

Repeated deauthentications sent within short time period

Dummy packet is generated by our WIPS sensor, looks like it came from Rogue AP

Figure 6 - Example of containment technique - 802.11 Deauthentication packet

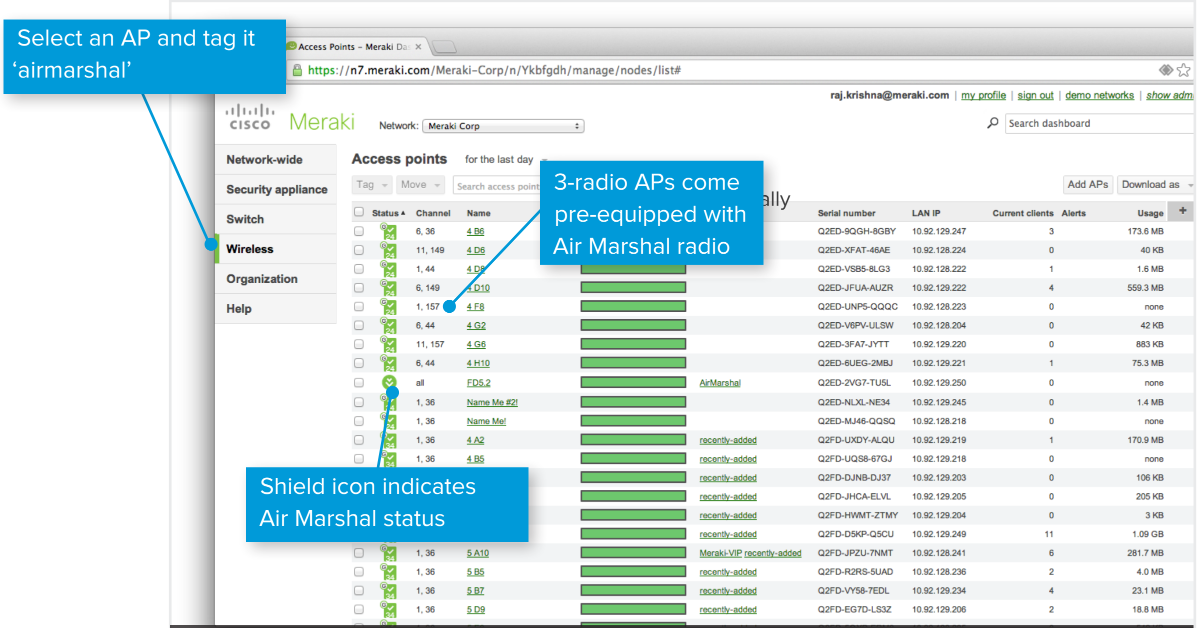
Configuring Meraki's Air Marshal WIPS platform

Dual-radio Meraki APs will run wireless scans opportunistically while also serving clients; this means they will scan the channel on which they are serving clients. It is possible to schedule 'mandatory' scans to be run at pre-specified time intervals that can be set as frequently as once a day. For users requiring more accurate and real-time wireless threat assessments, it is possible to place an AP in Air Marshal mode. While acting as an Air Marshal, an AP will use its radios as dedicated scanners to monitor its surrounding environment in real-time. For the dual-radio APs, this includes both the 2.4GHz and 5GHz frequencies. Newer Meraki APs include a third radio which comes pre-configured for permanent Air Marshal scanning. These APs do not require any Air Marshal configuration and will scan and remediate against threats in real-time.

Air Marshal mode can be switched on by selecting the relevant APs on the Access Points page. By clicking the relevant AP and selecting 'On' under the Air Marshal scanning section, it is possible to designate this AP as a dedicated WIPS scanner. This Air Marshal AP will now be a dedicated sensor performing scans of the surrounding environments for threats, the results of which will be displayed on the WIPS page in real-time.

A note on hybrid vs. dedicated scanners

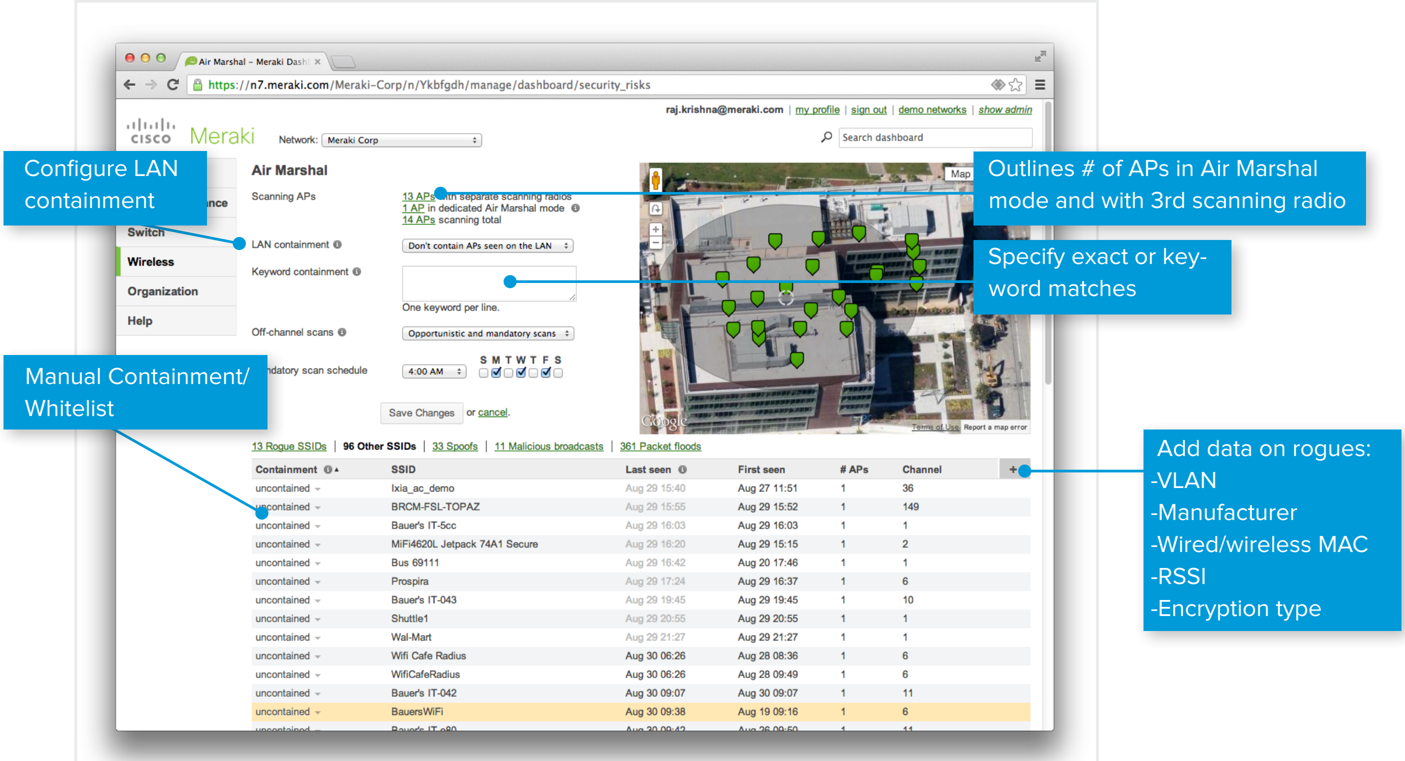
APs with two radios running in client-serving mode will only scan the airspace opportunistically; this means they will scan the client-serving channel in real-time, and will scan across all channels either once a day or when no clients are being served. Most WLAN vendors recommend having dedicated scanning sensors (with no clients being served) in security-conscious environments, to ensure real-time security alerting and protection. Some vendors offer 'time slicing' which allows cross-channel scans while serving clients, but this sacrifices performance of latency-sensitive applications such as VoIP and is generally not recommended in the industry. For this reason, Meraki recommends placing an AP in dedicated Air Marshal mode (or utilizing newer 3-radio APs) for real-time scanning.


Select an AP and tag it 'airmarshal'
3-radio APs come pre-equipped with Air Marshal radio
Shield icon indicates Air Marshal status
Access Points – Meraki Da
https://n7.meraki.com/Meraki-Corp/n/Ykbfgdh/manage/nodes/list#
raj.krishna@meraki.com | my profile | sign out | demo networks | show adm
cisco Meraki
Network: Meraki Corp
Search dashboard
Network-wide
Security appliance
Switch
Wireless
Organization
Help
Tag
Move
Search access point
Add APs
Download as
+

Access points for the last day

Channel	Name		Serial number	LAN IP	Current clients	Alerts	Usage
6, 36	4 B6		Q2ED-9QGH-8GBY	10.92.129.247	3		173.6 MB
11, 149	4 D6		Q2ED-XFAT-46AE	10.92.128.224	0		40 KB
1, 44	4 D8		Q2ED-VSB5-8LG3	10.92.128.222	1		1.6 MB
6, 149	4 D10		Q2ED-JFUA-AUZR	10.92.129.222	4		559.3 MB
1, 157	4 F8		Q2ED-UNP5-QQQC	10.92.128.223	0		none
6, 44	4 G2		Q2ED-V6PV-ULSW	10.92.128.204	0		42 KB
11, 157	4 G6		Q2ED-3FA7-JYTT	10.92.129.220	0		883 KB
6, 44	4 H10		Q2ED-6UEG-2MBJ	10.92.129.221	1		75.3 MB
all	FD5.2	AirMarshal	Q2ED-2VG7-TU5L	10.92.129.250	0		none
1, 36	Name Me #2!		Q2ED-NLXL-NE34	10.92.129.245	0		1.4 MB
1, 36	Name Me!		Q2ED-MJ46-QQSQ	10.92.128.218	0		none
1, 36	4 A2	recently-added	Q2FD-UXDY-ALQU	10.92.129.219	1		170.9 MB
1, 36	4 B5	recently-added	Q2FD-UQS8-67GJ	10.92.129.218	0		none
		recently-added	Q2FD-DJNB-DJ37	10.92.129.203	0		106 KB
		recently-added	Q2FD-JHCA-ELVL	10.92.129.205	0		205 KB
		recently-added	Q2FD-HWMT-ZTMY	10.92.129.204	0		3 KB
		recently-added	Q2FD-D5KP-Q5CU	10.92.129.249	11		1.09 GB
1, 36	5 A10	Meraki-VIP recently-added	Q2FD-JPZU-7NMT	10.92.128.241	6		281.7 MB
1, 36	5 B5	recently-added	Q2FD-R2RS-5UAD	10.92.128.236	2		4.0 MB
1, 36	5 B7	recently-added	Q2FD-VY58-7EDL	10.92.129.234	4		23.1 MB
1, 36	5 D9	recently-added	Q2FD-EG7D-LS3Z	10.92.129.206	2		18.8 MB

Figure 7 - Configuring Air Marshal APs on the Wireless > Access points page



Air Marshal – Meraki Dash

https://n7.meraki.com/Meraki-Corp/n/Ykbfgdh/manage/dashboard/security_risks

raj.krishna@meraki.com | my profile | sign out | demo networks | show admin

Network: Meraki Corp

Search dashboard

Air Marshal

Scanning APs: 13 APs with separate scanning radios
1 AP in dedicated Air Marshal mode
14 APs scanning total

LAN containment: Don't contain APs seen on the LAN

Keyword containment: One keyword per line.

Off-channel scans: Opportunistic and mandatory scans

Mandatory scan schedule: 4:00 AM S □ M ☑ T □ W ☑ T □ F ☑ S □

Save Changes or cancel.

13 Rogue SSIDs | 96 Other SSIDs | 33 Spoofs | 11 Malicious broadcasts | 361 Packet floods

Containment	SSID	Last seen	First seen	# APs	Channel
uncontained	Ixia_ac_demo	Aug 29 15:40	Aug 27 11:51	1	36
uncontained	BRCM-FSL-TOPAZ	Aug 29 15:55	Aug 29 15:52	1	149
uncontained	Bauer's IT-5cc	Aug 29 16:03	Aug 29 16:03	1	1
uncontained	MiFi4620L Jetpack 74A1 Secure	Aug 29 16:20	Aug 29 15:15	1	2
uncontained	Bus 69111	Aug 29 16:42	Aug 20 17:46	1	1
uncontained	Prospira	Aug 29 17:24	Aug 29 16:37	1	6
uncontained	Bauer's IT-043	Aug 29 19:45	Aug 29 19:45	1	10
uncontained	Shuttle1	Aug 29 20:55	Aug 29 20:55	1	1
uncontained	Wal-Mart	Aug 29 21:27	Aug 29 21:27	1	1
uncontained	Wifi Cafe Radius	Aug 30 06:26	Aug 28 08:36	1	6
uncontained	WifiCafeRadius	Aug 30 06:26	Aug 28 09:49	1	6
uncontained	Bauer's IT-042	Aug 30 09:07	Aug 30 09:07	1	11
uncontained	BauersWiFi	Aug 30 09:38	Aug 19 09:16	1	6
uncontained	Bauer's IT-e80	Aug 30 09:42	Aug 26 09:50	1	11

Configure LAN containment

Outlines # of APs in Air Marshal mode and with 3rd scanning radio

Specify exact or keyword matches

Manual Containment/ Whitelist

Add data on rogues:
-VLAN
-Manufacturer
-Wired/wireless MAC
-RSSI
-Encryption type

Figure 8 - Monitoring Air Marshal Page

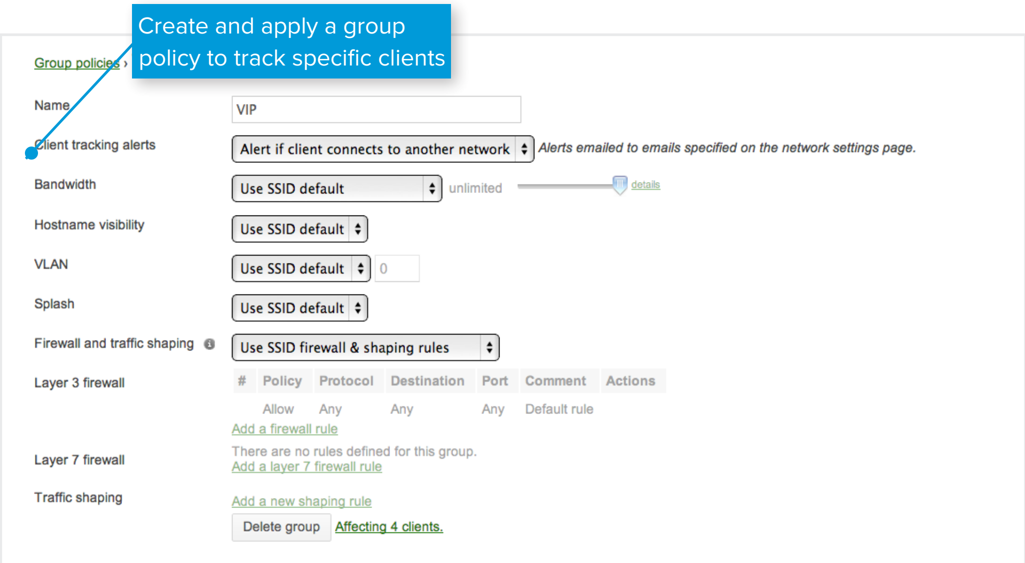
On the Wireless > Air Marshal page, a number of manual actions of automated policies can be set as a response to the detection of certain types of wireless threats based on administrator preferences:

1. Manual rogue containment: when choosing to 'contain' a rogue SSID, the Meraki AP will perform containment (as described in 'Threat Remediation' section of this document) to render the rogue AP ineffective. Certain rogue SSIDs known as friendly APs can also be whitelisted to avoid confusion in the future.

2. Automated LAN and Keyword Containment: automated policies can also be set to contain rogues seen on the wired network, as well as rogue APs matching a certain keyword. For example, if "Acme" is specified as a keyword and a Rogue SSID begins broadcasting an SSID named "AcmeCorp", it will automatically be contained and clients will not be able to associate with it. This can be helpful in detecting people who are trying to copy the network with similar names and 'trick' clients into associating with their own AP.

3. Mandatory scan schedule: set time and days of the week where non-Air Marshal APs should scan all channels to ensure daily scanning.

4. On the Wireless > Group policies page, a special policy can be created to track accidental associations by VIP clients; simply select the 'track clients straying' policy attribute and save the policy. The policy can then be applied to specific clients on the Clients page, and devices can also be pre-staged with their MAC addresses to have this policy automatically applied upon association by using the 'Add devices' function on the page.



Create and apply a group policy to track specific clients

Group policies ›

Name	VIP
Client tracking alerts	Alert if client connects to another network *Alerts emailed to emails specified on the network settings page.*
Bandwidth	Use SSID default unlimited details
Hostname visibility	Use SSID default
VLAN	Use SSID default 0
Splash	Use SSID default
Firewall and traffic shaping	Use SSID firewall & shaping rules

Layer 3 firewall

#	Policy	Protocol	Destination	Port	Comment	Actions
	Allow	Any	Any	Any	Default rule	

Add a firewall rule

Layer 7 firewall: There are no rules defined for this group. Add a layer 7 firewall rule

Traffic shaping: Add a new shaping rule

Delete group Affecting 4 clients.

Figure 9 - Creating a Client tracking group policy

5. Generic alerts for Rogue APs can be set on the 'Alerts and Administration' page, allowing administrators to receive automatic alerts when rogue APs are detected that either match specified keywords or are seen to be on the wired LAN.

Creating a WIPS response plan

By configuring alerts and utilizing Meraki's Air Marshal view to monitor these threats retroactively and in real-time, it is possible to build a robust security plan that can be enforced. An example of a complete security methodology is as follows:

1. Create a WIPS plan as per your company's security policies
   (i) Configure mandatory scanning intervals or designate APs to run in Air Marshal mode
   (ii) Configure auto-containment policies for rogue SSID keyword matches or rogues on the wired LAN
   (iii) Configure client straying policies to track batches of VIP clients
   (iv) Configure WIPS alerts

2. Proactive monitoring of Air Marshal
   (i) Visit Air Marshal page weekly or quarterly and mark known rogues as 'whitelisted', contain dangerous rogues
   (ii) Physically contain rogues that may be a threat

3. Reactive monitoring of Air Marshal alerts
   (i) Receive alert and react accordingly (set containment, find and contain rogue, etc).

Conclusion

By understanding the spectrum of wireless security threats in today’s environment and creating a comprehensive response plan, network administrators can preclude the possibility of a serious compromise of critical network assets — including access to secure network devices that belong to the enterprise. A best-in-class WIPS platform should be capable of delivering intuitive reporting and monitoring, along with a robust suite of tools allowing for automatic alerts and security enforncement.

Meraki’s Air Marshal system includes real-time detection, remediation and alerting capabilities, including the ability to define pre-emptive policies that will intelligently take action to contain rogue APs using sophisticated containment mechanisms. Meraki’s wireless portfolio contains both dual-radio APs which can be converted into full-time sensors running in Air Marshal mode, and three-radio APs with dedicated scanning radios permanently running as Air Marshal scanners. By utilizing Meraki access points and Meraki’s intuitive web-based Dashboard interface, network administrators can create a robust WIPS policy plan, and easily deploy an airtight network to deliver enterprise-grade security in a WLAN environment.