Global Information Assurance Certification Paper

A Secure Approach to Deploying Wireless Networks

GIAC GSEC Gold Certification

Author: Joseph F. Matthews, joseph.mathews@pccairfoils.com

Advisor: Dr. Johannes B. Ullrich

Accepted: August 1st 2016

Abstract

Enterprise wireless networks are an important component of modern network architecture. They are required to support mobile devices and provide connectivity to various devices where wired connections are not practical or cost prohibitive. But the missing physical control of the medium does require additional precautions to control access to wireless networks. Most books and papers present the problem and the risks, but do not provide a fully secure solution with examples. The 802.11 standard for wireless networks does offer encryption and authentication methods like WPA. But in an enterprise environment, these controls have to be implemented in a scalable and manageable way. This paper presents a hands-on guide to implementing a secure wireless network in an enterprise environment and provides an example of a tested secure solution.

1. Risks and Planning

1.1 Risks

Attacking wired networks in buildings requires physical access. Wireless offers great convenience and many benefits, but it also comes with a great many risks. An attacker can sit in a company's parking lot or with amplified equipment several blocks away and break into the network using wireless signals that bleed out into the open. With wardriving, warwalking or warflying the attacker is not locked into one physical location, they are continually on the move. This movement makes the attacker a harder target to pinpoint and to prevent their attacks (Cole, E., 2015).

Insecure wireless networks are easily attacked. Even relatively inexperienced attackers can attack them without much effort. Wi-Fi attacks are a real and ongoing threat. Three attackers used wardriving to steal over $750,000 from several businesses in the Seattle area. Attackers will look for any means possible to infiltrate network systems to gain access to data for their illicit purposes ("Dark Reading - Wardriving Burglars Hacked Business Wi-Fi Networks," 2011).

1.2 Planning

Without proper planning and Defense in Depth, most wireless networks can be breached in a matter of minutes. Utilization of Defense in Depth is essential. Proper planning and configuration need to be integrated early into the security plan (Cole, E., 2015). The sooner security decisions are made in the planning process, the more economical and easier they will be to implement. Companies need to identify the risks, the businesses assets, and the steps necessary for mitigation and protection.

At a minimum, data should be classified as public or private with an emphasis placed on protecting all private data. Signal bleed is a risk presented by wireless. Access points should be placed to minimize signal bleed and control the signal. Utilization of directional antennas and shielding on external walls helps to localize the signal and to contain private data within the expected locations. Planning and protection of the wireless network must occur at all layers of the Open Systems Interconnect (OSI) model. Once the wireless system is in place and secure,

enact stringent change control policies to avoid inadvertently weakening security ("Center for Internet Security," 2015).

2. Tools and Attacks

2.1 Kali Linux Wireless Penetration Testing Beginner's Guide

Even though wireless networks have been around for several years, and the encryption and security have improved, the human element is still the main weakness. Poor planning and configuration allow attackers to break into banks, businesses, and government agencies. The tool of choice for Hackers is Kali Linux. Step by step guides shows how Kali Linux is used by attackers to break into wireless networks. Guides like this are designed to help educate administrators, and to help close the security gaps in wireless networks. But, in the wrong hands, these books allow almost any skill level attacker to breach wireless networks. Encryption methods have improved, but so have the attacks. Administrators need to continue their education because without proper configuration and planning no matter what encoding method is selected the attacker can break it. Many attack vectors are shown, but no one resource can cover protecting against all of them (Buchanan, C., Ramachandran, V., 2015).

2.2 Attacks

Over 40% of the world is now using the internet, and a large portion of the population is accessing it wirelessly. The inherent weaknesses in wireless security open it up to malicious and criminal activity. Implementation of wireless security is typically at the upper OSI layers. Attackers are starting to target the physical layer utilizing multiple types of attacks on a variety of Wireless LANs (Gan, D., Waliullah, M., 2014).

Different attacks against IEEE 802.11 are still common. Many open source tools are available freely to attackers. Attacking wireless is very easy. Kismet and SMAC are both used to sniff traffic on wireless networks to identify legitimate Media Access Control addresses (MAC addresses). The addresses are then spoofed allowing the attacker to bypass MAC filtering. Aircrack-NG suite was then used to gain access. Aircrack-NG is a suite of tools used for denial of services (DOS) attacks, Wired Equivalent Privacy (WEP) cracking attacks. The toolset aides

in many attack scenarios. Multiple issues are still present in IEEE 802.11. Knowledge and following the good practices of the industry is the best current solution (Moniruzzaman, A., Rahman, S., Waliullah, M., 2015).

3. Defense in Depth for Wireless Networks

Defense in Depth is one of the first steps to securing wireless. Each layer of security slows the attacker; examples include using Wi-Fi Protected Access 2 (WPA2) protection, enabling Wireless Intrusion Detection Systems (WIDS), actively scanning and monitoring for rogue devices. Understanding the types of adversaries' aids in selecting the proper layers of defense to apply determines how to prioritize their deployment (Cole, E., 2015).

Defense in Depth comes from the military strategy of utilizing multiple levels of defense to make the enemies' job harder and more complex. These same countermeasures need to be used to protect assets in an enterprise. The National Security Agency (NSA) "recommends a balance between the protection capability and cost, performance, and operational considerations" (Defense in Depth, n.d., p01). Per the NSA People, Technology and Operations are the three primary elements for Information Assurance. The graphic below shows examples of layered defenses suggested by the NSA.

Class of Attack	*First Line of Defense*	*Second Line of Defense*
Passive	Link & Network Layer Encryption and Traffic Flow Security	Security Enabled Applications
Active	Defend the Enclave Boundaries	Defend the Computing Environment
Insider	Physical and Personnel Security	Authenticated Access Controls, Audit
Close-In	Physical and Personnel Security	Technical Surveillance Countermeasures
Distribution	Trusted Software Development and Distribution	Run Time Integrity Controls

Fig 1. Examples of Layered Defenses

Knowing what types of adversaries and their motivations a business will face is one of the first steps to a successful Defense in Depth strategy. Adversaries could include Insiders, Hackers, Nation States, Criminals, Competitors or Terrorists. Motivations could be as simple as pride or

bragging rights to theft or denial of service. Without a basic understanding of the types of attackers and their motives, businesses have no idea what to attempt to protect (Cole, E., 2015).

4. The Controls

4.1 Critical Security Control #15: Wireless Access Control

The first step in securing wireless networks is to identify and control all wireless devices connected to the network. Wireless devices connected to the network should have a documented business case and owner. The device configuration must match the approved company security profile. Devices that do not meet the documentation and configuration requirements should be denied access to the network. It is impossible to protect the unknown. A good and current network diagram is a must to aid in controlling the environment. Change control is required to ensure that no unknown changes occur that may jeopardize the environment's security.

Rogue access points should be actively tested for and removed as quickly as possible (Cole, E., 2015). Vulnerability scanning tools should be set to detect wireless access points that are connected to the wired network. Reconciliation of identified devices and authorized devices should occur frequently. Any unauthorized access points should be deactivated. Without a current and updated authorization list and proper detection methods in place, users can install their own wireless devices bypassing all approved security measures.

Wireless intrusion detection systems (WIDS) help to identify rogue wireless devices, detect attempted and successful compromises. Traffic should be monitored as it passes through the wired network. WIDS will monitor and alert on attacks and compromises, but it is a detection system, not a prevention system. A detection system allows the attack to occur and alerts to aid in reducing the time that the attacker is in the network. Without active monitoring and immediate response, WIDS, like all other detections systems, start to lose their value. Ensure that before implementing WIDS total cost of ownership is taken into consideration. The physical hardware is a small portion of the cost involved (Cole, E., 2015).

Before any implementation of hardware or software, the business' benefits and costs must be considered. If the business case is justified then, the clients wireless should be configured only to allow access to authorized networks. Wireless should be disabled in the hardware

configuration if an approved business case does not exist. Most new laptops are delivered with wireless network cards built into the motherboard and enabled by default. A suggested good practice would be to create group policies to disable these devices and only allow approved exceptions.

WEP is insecure and easy to breach. Tutorials are readily available on the internet to lead the attacker through the process of defeating WEP security. Wi-Fi Protected Access 2 (WPA2) and Advanced Encryption Standard (AES) should be used for all wireless traffic.

Without mutual authentication, the client is verified by the access point, but the client does not confirm the identity of the access point. Spoofing of an access point is easy with the "Evil Twin" as a well-known example of this type attack. Extensible Authentication Protocol-Transport Layer Security (EAP/TLS) provides mutual authentication and credential protection.

Allowing unknown access can and will lead to information leaks and successful attacks. Peer-to-peer wireless network capabilities should be disabled on wireless clients. Peer-to-peer wireless allows a client to connect directly to another without going through the normal network security and monitoring devices, thus circumventing security measures.

Business need should determine allowed access. Without an approved and documented business case, all wireless peripherals including Bluetooth should be disabled. Maintain updated approval documents. Periodically audit to ensure no unknown access has been enabled or provided.

Segregation and separation of trust levels help to secure the business environment. Virtual Local Area Networks (VLANs) are used segregate one physical network into multiple virtual networks. VLANs reduces traffic within a segment. Bring Your Own Device (BYOD) or other untrusted devices should reside on a separate VLAN. Internet traffic from this VLAN should go through the same border security devices as corporate traffic. Enterprise access should be filtered and treated as untrusted. ("Center for Internet Security," 2015).

4.2 Recommendations

Follow the steps and recommendations outlined in Center for Internet Security (CIS) Critical Security Controls Version 6.0, control number 15, Wireless Device Control. Figure 7 below

shows the recommended preventative controls.

The Center for Internet Security Critical Security Controls Version 6.0		
Family	**Control**	**Control Description**
Critical Security Control #15: Wireless Access Control		
Network	**15.1**	Ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Organizations should deny access to those wireless devices that do not have such a configuration and profile.
Network	**15.2**	Configure network vulnerability scanning tools to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points should be deactivated.
Network	**15.3**	Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises. In addition to WIDS, all wireless traffic should be monitored by WIDS as traffic passes into the wired network.
Network	**15.4**	Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface).
Network	**15.5**	Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.
Network	**15.6**	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication.
Network	**15.7**	Disable peer-to-peer wireless network capabilities on wireless clients.
Network	**15.8**	Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.
Network	**15.9**	Create separate virtual local area networks (VLANs) for BYOD systems or other untrusted devices. Internet access from this VLAN should go through at least the same border as corporate traffic. Enterprise access from this VLAN should be treated as untrusted and filtered and audited accordingly.

Fig 2. Critical Security Control #15

Experts from all sectors and roles developed the controls. "Offense informs defense: Use knowledge of actual attacks that have compromised systems to provide the foundation to continually learn from these events to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks ("Center for Internet Security," 2015).

No network is 100% secure; layering defenses make it harder for the adversaries. Each layer may only stop 30% to 40%. Achieving a safe environment requires utilizing multiple layers.

By following the recommended preventative controls, the first steps in locking down and securing wireless networks are accomplished. Prevention and detection both are required to combat the attacker successfully (Cole, E., 2015).

5. Implementation and Setup

5.1 Implementation

Before implementing Control 15 and its subsections, a business case and a site survey should be completed. The business case will determine if the wireless environment is justified.

The site survey will aid in determining what equipment is needed. Below is an example configuration plan.

The reference configuration contains two Cisco 2504 Wireless controllers and thirty 802.11G/N Fixed Unified Access Points with Internal Antenna. These devices are setup with Remote Authentication Dial-In User Service (RADIUS) Authentication for Securing Management access. Figure 3 shows the configuration choices for setting up RADIUS Authentication; figure 4 shows the completed server settings. Their configuration is managed and controlled. The controllers are setup for failover to eliminate a single point of failure. Routing all traffic through a firewall and a network intrusion detection system (NIDS) helps to enhance security.

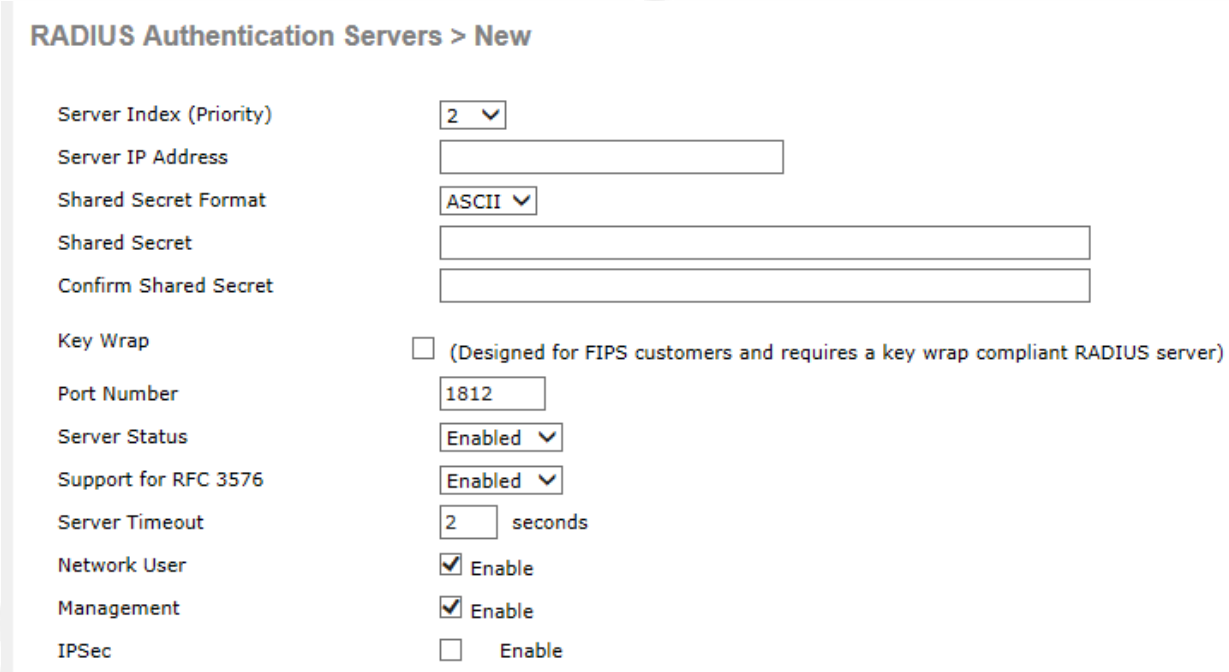

Fig 3. Radius Authentication Server Setup

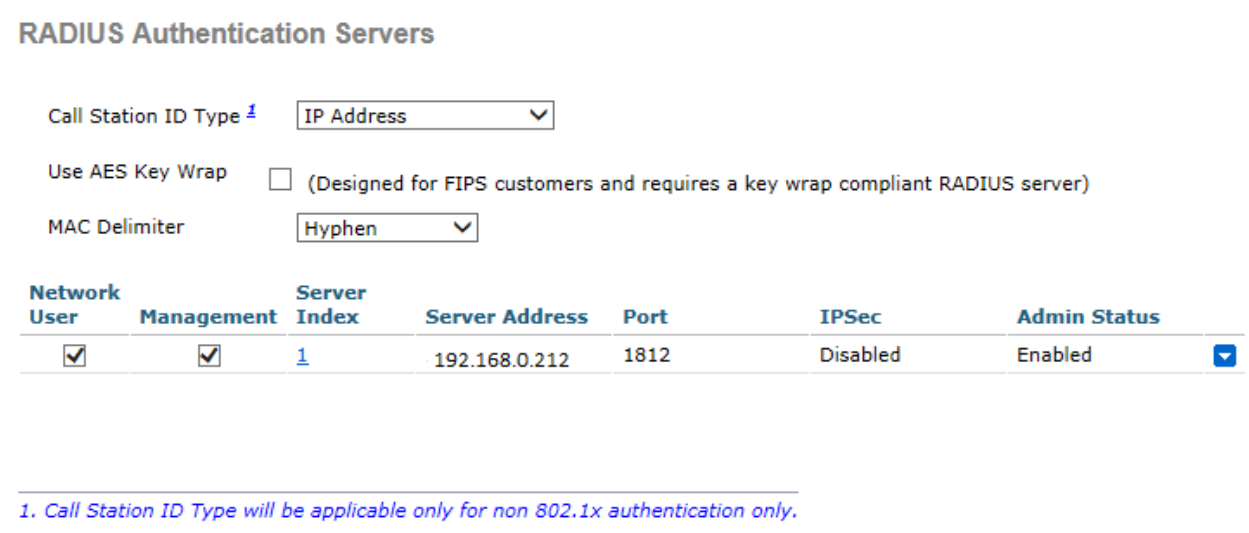

Fig 4. Radius Authentication Server Settings

Using commercial grade wireless access points allows them to perform two functions. The access points can be used to supply a wireless network signal and to act as wireless intrusion detection systems (WIDS). The Access points are configured to search for rogue access points and clients. They also are set to identify any rogue wireless devices and successful or attempted attacks and compromises. See below for the rogue summary screen on the Cisco 2500 series controller.

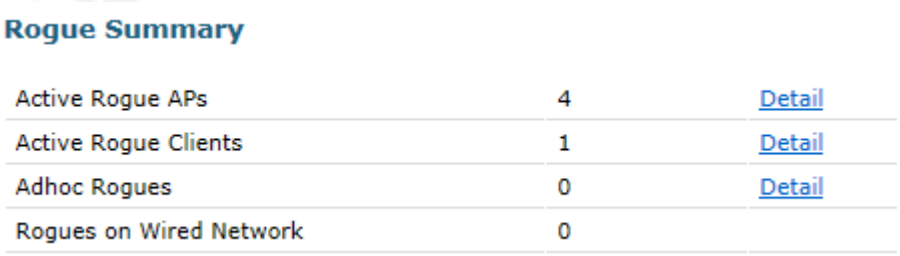

Fig 5. Rogue Summary

Office guest, factory, and jet-direct all have separate Wireless Local Area Networks (WLANs). Separation is critical for control and security of the wireless traffic. Each WLAN is then routed into VLANs as shown below in figure 6. Then all of the wireless traffic goes through the same security stack and firewall as wired network traffic. Routing the traffic through the

security stack allows filtering and auditing of the traffic. Figure 7 below shows that Wi-Fi Protected Access 2 (WPA2) protection is in use. Additionally, MAC filtering is used to ensure that only know and approved clients can gain access to the Office, Factory and Jet Direct networks. Active Directory stores the approved MAC addresses. The RADIUS server controls their authentication and verification. The approved credentials are passed to the controller using Cisco ACS. Control of guest network access is by Web Authentication (Web-Auth). Guests receive a Username, and password that expires after a 24-hour period. When connecting to the Guest Service Set Identifier (SSID), all users are forced into a web portal that requires them to provide their credentials.

WLANs

Current Filter: None [Change Filter] [Clear Filter] Create New Go

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	office-network	office-network	Enabled	[WPA2][Auth(802.1X)], MAC Filteri
2	WLAN	guest-network	guest-network	Enabled	Web-Auth
3	WLAN	factory-network	factory-network	Enabled	[WPA2][Auth(802.1X)], MAC Filteri
4	WLAN	jetdirect-network	jetdirect-network	Enabled	[WPA2][Auth(PSK)], MAC Filtering

Fig 6. Wireless LAN Examples

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
guest_egress	802	192.168.1.5	Dynamic	Disabled
intranet_egress	2	10.60.48.5	Dynamic	Disabled
management	10	10.17.69.5	Static	Enabled
virtual	N/A	1.1.1.1	Static	Not Supported

Fig 7. Interfaces

Advanced Encryption Standard (AES) encryption is used to encrypt the traffic, and Protected Extensible Authentication Protocol (PEAP/TLS) provides mutual authentication. Both the encryption and authentication are setup on the controller and the client. The configurations must match to allow successful communication. PEAP/TLS was chosen to add a layer of security. PEAP encapsulates the EAP protocol within an encrypted TLS tunnel.

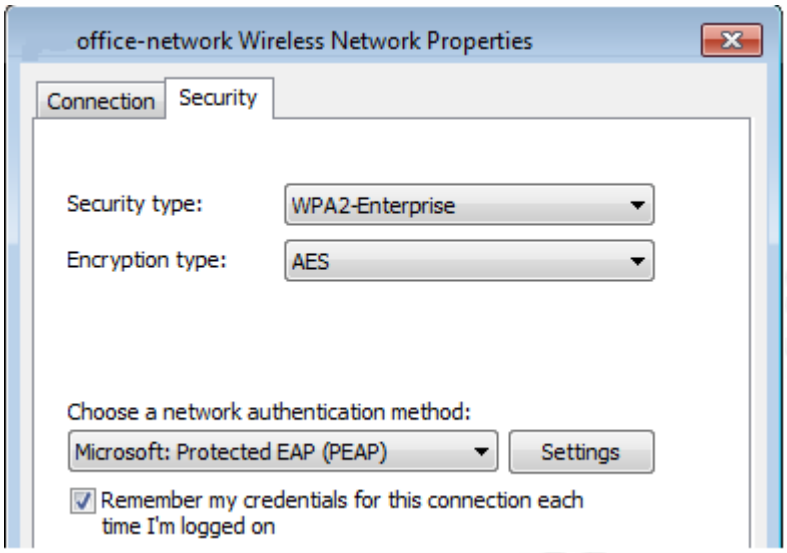

Fig 8. Network Properties

Figure 9 below shows a reference network diagram. Power over Ethernet (POE) Switches provides power and route the wireless traffic to the core switch then into the wireless controller. From the wireless controller, the traffic travels through the firewall and the NIDS. Once the traffic traverses the security checks, it reaches its destination either the network or out through the Point of Presence (POP) to the Internet.

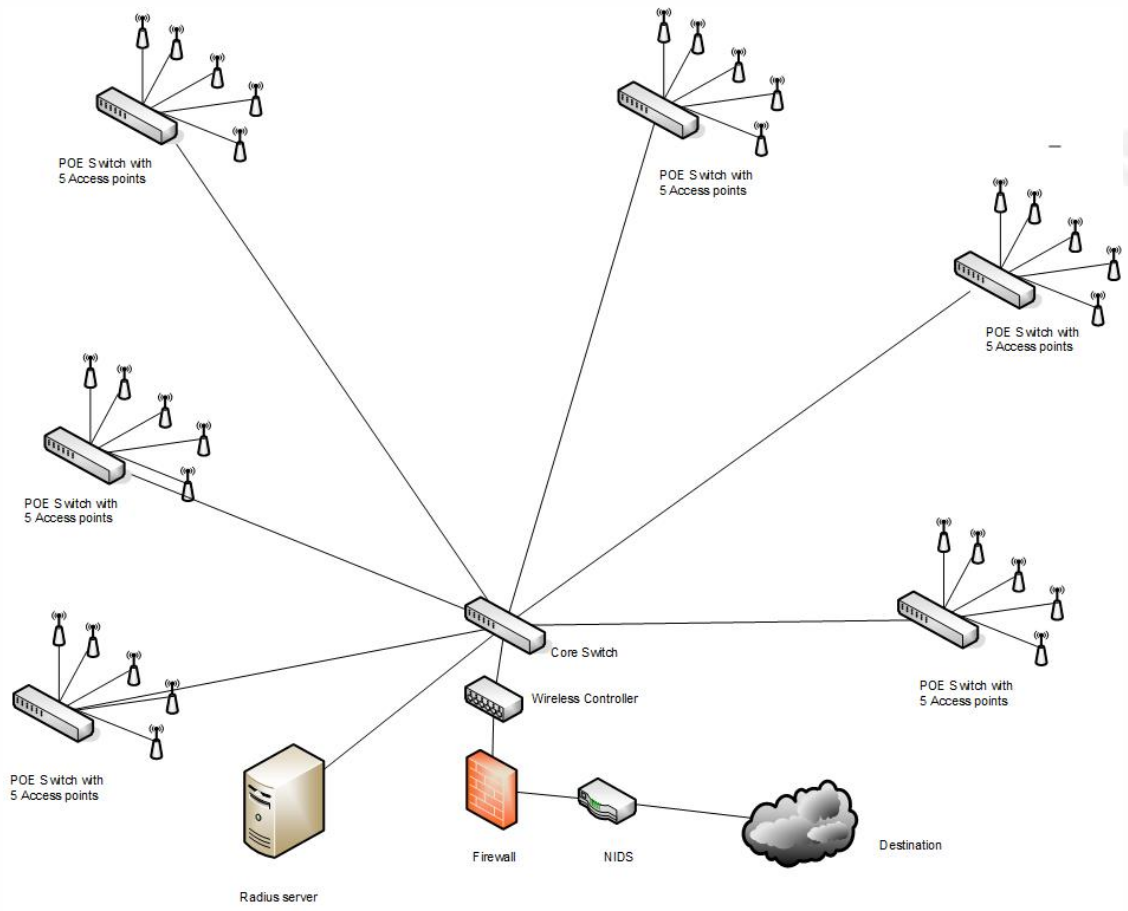

Fig 9. Wireless Network Diagram

5.2 Setup

Before setup and configuration, the parameter information in figure 10 is required. It is important to note that the username and password cannot be the same. ("Cisco 2500 Series Wireless Controllers - Install and Upgrade Guides - Cisco," 2011) Network and administrator access control are through RADIUS. Verification of usernames and passwords occurs against the backend database before permitting access. For added security, disable any unneeded wireless networks. As an example, if all devices use 802.11g and 802.11n disable 802.11a and 802.11b. The virtual gateway IP address must be the same for all controllers in a mobility group.

- A system (controller name), such as *controller*. The system name can contain up to 32 printable ASCII characters.
- An administrative username and password, which can contain up to 24 printable ASCII characters.
- A management interface (DS Port or network interface port) IP address, such as ***10.40.0.4***.
- A management interface netmask address, such as ***255.255.255.0***.
- A management interface default router IP address, such as ***10.40.0.5***.
- A VLAN identifier if the management interface is assigned to a VLAN, such as ***40*** or ***0*** for an untagged VLAN.
- A management interface port, such as ***1***.
- A management interface DHCP server IP address, such as ***10.40.0.6*** (the IP address of the default DHCP server that will supply IP addresses to clients and the management interface.
- A virtual gateway IP address (a fictitious, unassigned IP address, such as ***1.1.1.1***, used by all Cisco wireless controller Layer 3 security and mobility managers).
- A Cisco wireless controller mobility or RF group name, such as ***rfgrp40*** if required. An RF group name can contain up to 19 printable ASCII characters.
- An 802.11 network name (SSID), such as ***wlan1***. An SSID can contain up to 32 printable, case-sensitive ASCII characters.
- DHCP bridging
- Whether or not to allow static IP addresses from clients, either ***Yes*** or ***No***.
  - *Yes* is more convenient, but has lower security (session can be hijacked).
  - *No* is less convenient, but has higher security and works well for Windows XP devices.
- RADIUS server IP address, communications port, and secret if you are configuring a RADIUS server, such as ***10.40.0.3***, ***1812***, and ***mysecretcode***.
- The country code for this installation. Enter **help** to see a list or refer to the *Cisco Wireless LAN Controller Configuration Guide* for country code information. This guide is available at cisco.com.
- Status of the 802.11a, 802.11b, 802.11g, or 802.11n networks, either ***enabled*** or ***disabled***.
- Status of Radio Resource Management (RRM), either ***enabled*** or ***disabled***.

Fig. 10 Cisco 2500 Configuration Settings

After collecting the required information connect a computer to the controller's management port. Run VT-100 emulation with Hyper Terminal, Putty or another emulator. Configure the emulator settings for 9600 baud, 8 data bits, No flow control, 1 stop bit, No parity. Power on the controller. The controller will run a boot-up script and perform a power-on-self-test. Below is a boot display example.

```
CISCO SYSTEMS
WLCNG Boot Loader Version 1.0.15 (Built on Nov 23 2010 at 07:51:36 by cisco)
Board Revision 0.0 (SN: PSJ143302MT, Type: AIR-CT2504-K9) (P)
Verifying boot loader integrity... OK.
OCTEON CN5230C-SCP pass 2.0, Core clock: 750 MHz, DDR clock: 330 MHz (660 Mhz data
rate)
CPU Cores:  4
DRAM:  1024 MB
Flash: 32 MB
Clearing DRAM........ done
Network: octeth0', octeth1, octeth2, octeth3
  ' - Active interface
  E - Environment MAC address override
CF Bus 0 (IDE): OK
IDE device 0:
 - Model: 1GB CompactFlash Card Firm: CF B612J Ser#: C181101244A1Yb3A5QNU
 - Type: Hard Disk
 - Capacity: 977.4 MB = 0.9 GB (2001888 x 512)
Press <ESC> now to access the Boot Menu...

Continue booting the controller or press Esc to access the following menu:
============================================================
 Boot Loader Menu
============================================================
 1. Run primary image (7.0.114.76) - Active
 2. Run backup image (7.0.114.75)
 3. Change active boot image
 4. Clear configuration
 5. Format FLASH Drive
 6. Manually update images
 ------------------------------------------------------------
Enter selection:
```

Fig. 11 Boot display

The full boot-up process takes two to three minutes. During the boot process, the controller runs Posts test and initializes the bootup scripts. The boot script starts the Setup Wizard for basic configuration using the previously collected information.

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_d9:16:24]:
```

Fig 12. Cisco Wizard Configuration Tool

After initial configuration is complete log into the controller to perform the additional setup, security configuration and begin connecting access points. Figure 13 shows a Cisco external

connection example, and figure 14 shows access points connected to a controller. The controller will automatically record the MAC address of all access points that connect and the Radio Resource Management (RRM) will auto configure the access points.

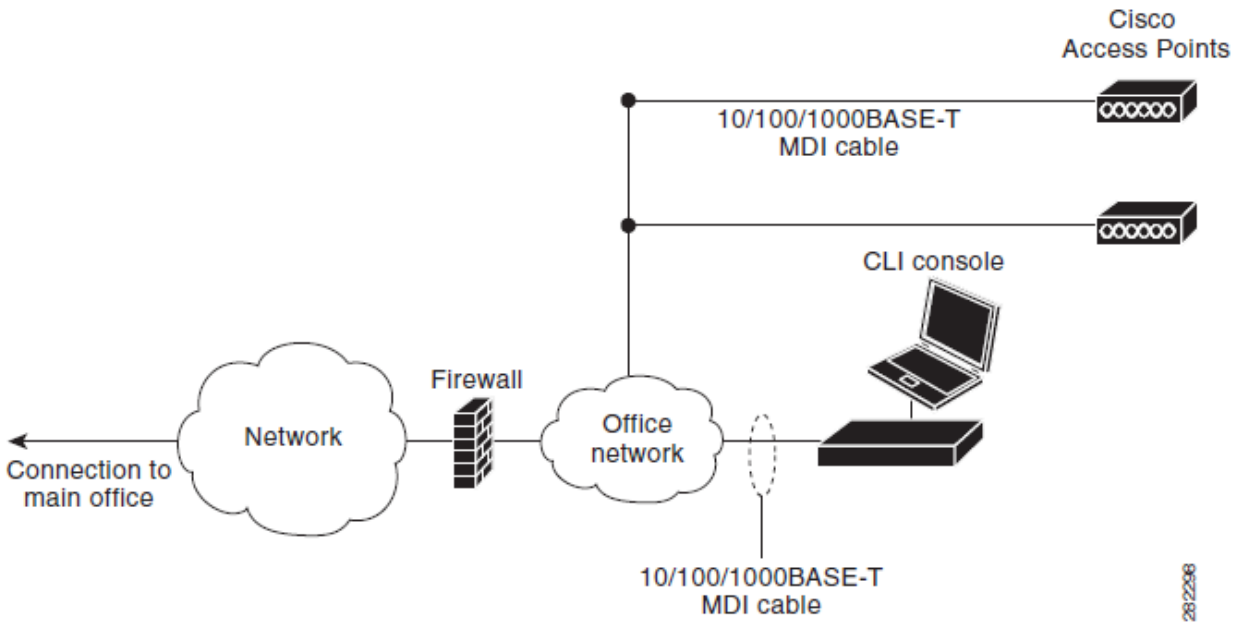

Fig. 13 External network equipment connection to the controller

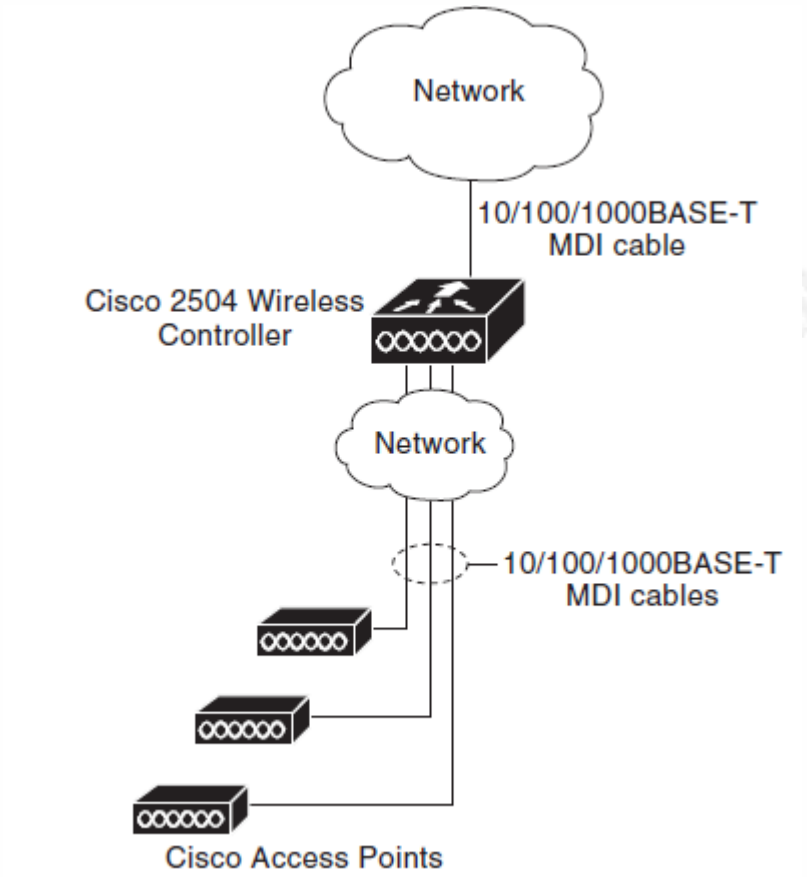

Fig. 14 Access points connected to a controller

6. Conclusion

6.1 Recap

Research articles and papers continue to show that using one or two levels of protection are not enough. Wireless administrators have to take a wider view and follow the Defense in Depth steps to make their networks as secure as possible. Applying multiple layers of protection delays the attacker and requires more effort and experience to break through. Every minute during an attack puts the attacker at risk of discovery (Cole, E., 2015).

There is no foolproof way at this time to secure wireless completely. Even the most secure protocols for wireless still have their flaws. Proper configuration and Defense in Depth are still the best and strongest methods of protection. The tools and knowledge to attack and

break into wireless networks are freely available. Criminals and hackers attack businesses every day to access or steal their data and money. The critical controls from the Center for Internet Security provide 20 different controls broken up into Systems, Networks, and Application controls. "The CIS Controls are a set of internationally recognized measures developed, refined, and validated by leading IT security experts from around the world. The CIS Controls represent the most important cyber hygiene actions every organization should implement to protect their IT networks. In fact, a study by the Australian government indicates that 85% of known vulnerabilities can be stopped by deploying the Top 5 CIS Controls. This includes taking an inventory of IT assets, implementing secure configurations, patching vulnerabilities, and restricting unauthorized users" ("Center for Internet Security," 2015).

Businesses need to maintain current updated network diagrams. Configuration control is a must. Once configurations are in place audits should be periodically performed to ensure no unauthorized changes occur. It is impossible to protect a network with unknown devices providing access and connecting. Security professions have to find and secure all avenues; all the attacker has to do is find one, to steal the companies' data and information. Reports of new and larger breaches occur almost daily. In the past, a small breach was major news, today when a breach of millions of records occurs it is barely a shock. Society is becoming numbed to the effects of attackers.

6.2 Further suggestions

Technology is constantly changing. It is important to investigate and stay current with technology and security improvements. One way to remain apprised of new security improvements is by subscribing to security newsletters such "SANS NewsBites", is a semiweekly high-level executive summary. It covers the most important news articles published on security during the last week. "@RISK," is a weekly summary of newly discovered attack. It presents the vectors, vulnerabilities of how the attacks work. "OUCH!" is a monthly newsletter aimed at educating the average computer user. SANS provides these at http://www.sans.org/newsletters/. Cipher is IEEE's monthly newsletter is accessible at http://www.ieee-security.org/cipher.html. Microsoft's Security newsletter is available at https://technet.microsoft.com/en-us/security/security-newsletter.aspx To ensure security best

practice awareness, companies need to check periodically for updated security controls recommendations at https://www.cisecurity.org/critical-controls.cfm.

Network Administrators, System Administrators, Active Directory Administrators, Programmers and Managers all need to be involved in security awareness and training. These are the people in charge of the assets and information, so they need to be aware of the dangers and the solutions to ensure the protection of the business. Security is not just the security teams' responsibility; it is everyone's.

References

Buchanan, C., Ramachandran, V. (2015). Kali Linux Wireless Penetration Testing Beginner's Guide (2nd ed.). Birmingham B3 2PB, UK: Packt Publishing Ltd.

Center for Internet Security. (2015, October 15). Retrieved from https://www.cisecurity.org/critical-controls.cfm

Cisco 2500 Series Wireless Controllers - Install and Upgrade Guides - Cisco. (2011, May). Retrieved from http://www.cisco.com/c/en/us/support/wireless/2500-series-wireless-controllers/products-installation-guides-list.html

Cole, E. (2015). SEC401: Security Essentials Bootcamp Style [Slides].

Dark Reading - Wardriving Burglars Hacked Business Wi-Fi Networks. (2011, September 23). Retrieved from http://www.darkreading.com/attacks-and-breaches/wardriving-burglars-hacked-business-wi-fi-networks/d/d-id/1100324?print=yes

Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments. (n.d.). Retrieved from National Security Agency website: https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Gan, D., Waliullah, M. (2014). Wireless LAN Security Threats & Vulnerabilities: A Literature Review. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, (2014), pp. 176-183. Retrieved from http://thesai.org/Downloads/Volume5No1/Paper_25-Wireless_LAN_Security_Threats_Vulnerabilities.pdf

Hanzo, L., Wang, X., Zou, Y. (2015). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. Proceedings of the IEEE. Retrieved from http://arxiv.org/abs/1505.07919

Lampoudis, D., Tsekleves, E., Tsitroulis, A. (2014). Exposing WPA2 security protocol vulnerabilities, Int. J.

Many Wireless Security Breaches Reported At Security Conference. (2005). Retrieved from http://www.informationweek.com/many-wireless-security-breaches-reported-at-security-conference/d/d-id/1030499

Moniruzzaman, A., Rahman, S., Waliullah, M. (2015). An Experimental Study Analysis of Security Attacks at IEEE 802.11 Wireless Local Area Network. International Journal of Future Generation Communication and Networking Vol. 8, No. 1, (2015), pp. 9-18. Retrieved from http://www.sersc.org/journals/IJFGCN/vol8_no1/2.pdf

Wi-Fi Security: Securing Yourself against Practical Wireless Attacks – InfoSec Resources. (2015, March 19). Retrieved from http://resources.infosecinstitute.com/hacking-your-neighbors-wi-fi-practical-attacks-against-wi-fi-security/

Last Updated: January 20th, 2019

Upcoming Training

SANS Miami 2019	Miami, FL	Jan 21, 2019 - Jan 26, 2019	Live Event
SANS Las Vegas 2019	Las Vegas, NV	Jan 28, 2019 - Feb 02, 2019	Live Event
SANS Security East 2019	New Orleans, LA	Feb 02, 2019 - Feb 09, 2019	Live Event
Security East 2019 - SEC401: Security Essentials Bootcamp Style	New Orleans, LA	Feb 04, 2019 - Feb 09, 2019	vLive
SANS Anaheim 2019	Anaheim, CA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Northern VA Spring- Tysons 2019	Tysons, VA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Dallas 2019	Dallas, TX	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Secure Japan 2019	Tokyo, Japan	Feb 18, 2019 - Mar 02, 2019	Live Event
SANS Reno Tahoe 2019	Reno, NV	Feb 25, 2019 - Mar 02, 2019	Live Event
Open-Source Intelligence Summit & Training 2019	Alexandria, VA	Feb 25, 2019 - Mar 03, 2019	Live Event
Mentor Session @Work - SEC401	Raleigh, NC	Feb 27, 2019 - Mar 06, 2019	Mentor
SANS Baltimore Spring 2019	Baltimore, MD	Mar 02, 2019 - Mar 09, 2019	Live Event
Baltimore Spring 2019 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Mar 04, 2019 - Mar 09, 2019	vLive
Community SANS Indianapolis SEC401	Indianapolis, IN	Mar 04, 2019 - Mar 09, 2019	Community SANS
SANS Secure India 2019	Bangalore, India	Mar 04, 2019 - Mar 09, 2019	Live Event
SANS St. Louis 2019	St. Louis, MO	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Secure Singapore 2019	Singapore, Singapore	Mar 11, 2019 - Mar 23, 2019	Live Event
SANS London March 2019	London, United Kingdom	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS San Francisco Spring 2019	San Francisco, CA	Mar 11, 2019 - Mar 16, 2019	Live Event
Mentor Session - SEC401	Fredericksburg, VA	Mar 12, 2019 - May 14, 2019	Mentor
SANS Munich March 2019	Munich, Germany	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Secure Canberra 2019	Canberra, Australia	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Norfolk 2019	Norfolk, VA	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201903,	Mar 19, 2019 - Apr 25, 2019	vLive
SANS 2019 - SEC401: Security Essentials Bootcamp Style	Orlando, FL	Apr 01, 2019 - Apr 06, 2019	vLive
SANS 2019	Orlando, FL	Apr 01, 2019 - Apr 08, 2019	Live Event
Community SANS Raleigh SEC401	Raleigh, NC	Apr 01, 2019 - Apr 06, 2019	Community SANS
SANS London April 2019	London, United Kingdom	Apr 08, 2019 - Apr 13, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KY	Apr 11, 2019 - Apr 18, 2019	Live Event