# SANS Institute
## Security Consensus Operational Readiness Evaluation

This checklist is from the SCORE Checklist Project. Reposting is not permited without express, written permission.

# Enterprise Wireless Audit Checklist

Prepared by: Dean Farrington
Version: 1.0

## *References:*

1. NIST, Special Publication 800-48, "Wireless Network Security – 802.11, Bluetooth, and Handheld Devices", 2002

2. Center for Internet Security, "Wireless Networking Benchmark (version 1.0)", April 2005

3. Planet3 Wireless, "Certified Wireless Network Administrator, Official Study Guide (3rd Edition)", Berkeley, Ca. Osborne, 2005

4. Planet3 Wireless, "Certified Wireless Security Professional, Official Study Guide", Berkeley, Ca. Osborne, 2003

5. Gast, Matthew , "802.11 Wireless Networks, the Definitive Guide" 2nd Edition, Sebastopol, Ca. O'Reilly, 2005

6. Potter, Bruce and Fleck, Bob, 802.11 Security", Sebastopol, Ca. O'Reilly,2002

7. Edney,Jon and Arbaugh,William, "Real 802.11 Security", Addison-Wesley Professional, 2003

8. Cisco Press, "Cisco Wireless LAN Security", Cisco Press, Indianapolis, In, 2004

9. National Security Agency, "Guidelines for the Development and Evaluation of IEEE 802.11 Intrusion Detection Systems (IDS)"
http://www.nsa.gov/snac/downloads_wireless.cfm?MenuID=scg10.3.1

10. DISA, "Wireless Security Checklist"
http://www.ncrdoim.army.mil/ia/documents/wireless-chklstv2r11-073003.doc

## *Introduction:*

The purpose of this paper is to offer guidance to Enterprise Architects on creating a secure 802.11 wireless network environment. Wireless networks, with their promise of increased productivity have become a requirement of managers and executives. At the same time that 802.11 wireless networking is increasing the productivity of workers, it is also forcing a shift in traditional network design strategies. Because wireless is based on Radio Frequency (RF) technology, it means your internal network is no longer confined to the inside of your building and you may well have a new avenue for network access that bypasses your carefully placed perimeter firewalls and perimeter defenses. Now more than ever, network architecture needs to embody the principal of Defense in Depth.

When designing wireless networks you need to build your security measures in overlapping rings, like the concentric defense of a medieval castle. Should one security measure be proven weak or flawed, several other layers of you defensive strategy should still offer protection to your network. The overall goal is to ensure that no single failure can cause a collapse of all your defenses.

Enterprise level wireless networks require complex and painstaking research and evaluation. Due to the number of points of difference between any two enterprise networks, few ready made "one size fits all" solutions exist today. However many wireless vendors tend to market their solutions in this manner. If you are familiar with securing home WLAN installations you will discover some of the security mechanisms you are accustomed to in small scale wireless networks do not scale effectively to Enterprise level deployment.

The following document can not outline all possible design and deployment considerations for the deployment of Enterprise Wireless Networks in detail. That would require a document the size of one or more of the books listed in the references. For that level of detail I refer you to those references. This document will however attempt to provide you a reference to what are essential considerations for design and deployment of an Enterprise WLAN.

## *Checklist*

| No. | Control |
|-----|---------|
| 1 | **Policy** – Before you start doing network designs or start evaluating authentication mechanisms, create your corporate policy on Wireless use and deployment. You will want to address many things in your policy such as:<br><br>• **Acceptable use of wireless** – Outline appropriate and inappropriate uses of the WLAN environment and possible consequences for non-compliance. Have an end-user agreement document that the user must sign showing they know and understand the policy for wireless use. Spell out in your documentation what services and uses are permitted on the WLAN. Have a policy on Hot Spot use for internet access and for remote connectivity (VPN).<br>• **Sources of Authorized WLAN installations** – It is a good idea to clearly state what part of the organization is the only source authorized to provide WLAN services. This can help prevent users or groups from feeling that since WLANs are approved for use they can provide their own access if it is not available where they would like it. It is a good idea to have a statement dealing with how user installed (rouge) WLAN devices will be dealt with. If the policy states these devices will be confiscated then the user should understand the consequences of enabling such a device. |

| | |
|---|---|
| | • **Allowed hardware** – If you are requiring certain specific hardware for your WLAN define it in policy. It is advisable to prohibit the use of personally owned equipment.<br>• **Wireless IDS** – Document a requirement for deploying Wireless IDS to monitor your WLAN environment.<br><br>Even if you do not have a WLAN deployment, you ought to have a policy governing the deployment of WLANs to ensure that users do not decide to provide their own, the policy should also give you official backing when removing unauthorized access points. |
| 2 | **WLAN Architecture** – Have an overall architecture for Enterprise WLAN deployments. This creates standardization of hardware and configuration for multi site WLAN deployments and allows for reuse of components of the WLAN back end such as authentication servers.<br><br>Determine appropriate placement of WLAN networks in response to the needs of the organization. Should they be placed on the internal network backbone, in a DMZ, only in non-sensitive areas, should an Enterprise Wireless Gateway be used to perform VPN functions over 802.11? These are all issues for the overall corporate architecture to consider since the answers will be different for every company or organization based on their risk tolerance, regulatory requirements, budget, and support capabilities.<br><br>• The architecture should also take into account the Authentication and Encryption schemes to be used. Again these are going to be driven based on local requirements but having them documented should allow for the possible reuse of some of these components across multiple WLAN installations, especially the backend authentication servers.<br><br>• Physical security of the Access Points and related infrastructure should also be considered as part of the infrastructure. Determine appropriate controls to physically secure the hardware such as installation in secured wiring closets or mounting access points in lock boxes.<br><br>• Consider architecting the WLAN is such a way that the wireless network is separated from the LAN through the use of segmentation devices. This can provide additional security and a choke point between the WLAN and the Enterprise LAN backbone.<br><br>• Will the clients use a VPN on top of the Wireless LAN? If the additional security is needed or desired determine how this will be implemented, through the use of a VPN concentrator or an Enterprise Encryption Gateway. |

| 3 | **Configuration Management-** Ensure a system for configuration management is in place and is used for all changes in Access Point configuration. Document, test and record all changes so a history is kept for fault isolation.<br><br>Periodically audit the AP configuration against the configuration recorded in the configuration management system to detect unauthorized modifications. |
|---|---|
| 4 | **Ensure a proper Site Survey is preformed prior to WLAN Deployment**- A Site Survey is needed in order to determine proper placement of Access Points to give the required connectivity and throughput, however it is also an ideal time to take plan for some security concerns.<br><br>1) Placement of Access Points to provide adequate data rates to associated clients may also cause a lot of signal to spread beyond the boundary of the building itself. Look for opportunities to shape the RF footprint of the network by careful use of power levels and directional antennas to minimize the RF in areas outside of your physical control.<br><br>2) At the same time you are placing your access points, identify the locations for placing Wireless IDS sensors. Even if you are not planning to deploy a Wireless IDS  now, you can save time and money later by doing some of the planning now. |
| 5 | **End User Training** - Ensure the end users are properly trained in the use of all security features of the Enterprise WLAN. Train the users about the proper and improper uses of the wireless access they are being provided. Reinforce the corporate policies on use of Hot Spots and personal wireless networks in the course of the training as well. |
| 6 | **Ensure the Security of all WLAN clients** – All workstations that are to be WLAN clients should be properly secured. Some things to ensure:<br>• Proper patch level is maintained<br>• An Anti-Virus client is installed, running, and regularly updated<br>• Ensure a personal firewall is installed and active on the wireless connection.<br>• Ensure appropriate system security settings are in place<br>• Ensure that the supplicant does not have the setting "Validate server certificate" disabled. If this is disabled you can loose all of the security of the connection as any certificate presented can be trusted. |
| 7 | **Ensure Strong Authentication and Encryption is required on the WLAN** – Encryption is the topic that has garnered the most attention in relationship to wireless technology. The choice of encryption and authentication schemes is one of the most important decisions you will need to make when planning your wireless network. This checklist cannot cover all the issues involved in |

| | |
|---|---|
| | selection of an appropriate mechanism for your enterprise since every enterprise has unique requirements, but we will attempt to raise some of the issues you need to consider in your selection.<br><br>• Use the strongest encryption practical, 128 bits should be considered the minimum acceptable level.<br>• Use AES encryption with WPA2 if possible<br>• Select a mechanism that uses centralized authentication<br>• Select a mechanism that supports PKI certificates if you have the infrastructure to support it.<br>• If you are using EAP look to your vendors to comply with RFC3748 which obsoletes RFC2284. RFC3748 calls for binding the inner and outer authentication protocols to help mitigate Man-in-the-middle attacks.<br>• Use a scheme that allows for mutual authentication if possible<br>• Assume that WEP provides no real protection, and only use it as a last resort<br>• Avoid using authentication protocols that have been broken |
| 8 | **Change default passwords**- All Access Points on the market come preconfigured with a default password. The default passwords are well known to the hacking community and allow for easy exploitation of your network. Change them immediately. |
| 9 | **Change default configuration settings** – All Access Points on the market come preconfigured with some form of default settings for the SSID and the administrative passwords. These are well known to the hacking community. Change them before connecting any APs to your production network. |
| 10 | **Configure devices on an non-production network if possible** – Because of the issues with the well known defaults settings it is a good practice to establish your initial configuration of WLAN components on an isolated "configuration LAN" . This reduces the possibility of someone attacking your device by trying to exploit its default configuration, and if the did succeed they would have access to nothing critical. |
| 11 | **Disable all unused management interfaces**- All enterprise class Access Points come with multiple management interfaces, disable any that are not actively being used to manage the device since it can become an avenue of attack. |
| 12 | **Manage the APs Out-of-band if possible** – If possible use an out-of-band network or separate VLAN to handle the management of the Access Points. This further protects the management interfaces from attack. |

| 13 | **SSID Construction** – Do not use the name of the company, the address, phone number in the SSID. Stick to things that will not give away excess information about whose WLAN the SSID is from. "Room 212" is a reasonable SSID as it does not give away too much information, "Accounting Department" is not a good choice as it tells anyone in range exactly what that network connects to. Avoid using the names of individuals as this information is just an invitation to social engineering attempts.<br><br>Security measures like not broadcasting the SSID are not a foolproof measure, the SSID can still be obtained by an attacker, so keep the SSID something you do not mind them knowing. |
|----|----|
| 14 | **Do not broadcast the SSID** – While not a foolproof measure, it does cut down on the availability of information. It is a good idea to not broadcast your SSID information and simply configure you corporate clients with the correct information in their profile. |
| 15 | **Logging & Monitoring** – Most enterprise level networks already have a mechanism in place for both remote logging and for monitoring of network devices. These may be the same tool, as with a SNMP manager or it may be separate solutions for logging to a syslog server and monitoring health with a SNMP manager. In either way having some sort of answer for both requirements is important for your WLAN. Real time monitoring of health can alert you to problems that are happening on the WLAN, but being able to refer to logs of past events is often needed to diagnose issues such as persistent authentication failures. |
| 16 | **Wireless IDS/IPS** – Few Enterprise networks are without an IDS/IPS solution for security monitoring. In the same vein, most any enterprise class WLAN deployment should have some form of Wireless IDS (WIDS) or IPS (WIPS) solution to ensure the safety of the RF environment.<br><br>WIDS solutions normally come in two deployment modes:<br>  1) The overlay network – dedicated WIDS sensors are deployed that are separate from the wireless LAN. These sensors send alerts back to a central manager for event de-duplication and alerting.<br>  2) The Integrated solution – The integrated solution uses the AP's themselves as sensors, this saves the cost of a separate sensor network deployment and generally uses the same management interface as the WLAN management application to monitor security.<br><br>Within these deployment options there are a whole range of variable features. These include IPS capabilities, Policy based station/AP suppression, Performance monitoring, and security monitoring.<br><br>Each deployment mode has its own strengths and weaknesses, all of which |

| | |
|---|---|
| | need to be given careful consideration as part of the evaluation process to ensure the system you select most fully meets your needs. |
| 17 | **<u>Institute a session timeout</u>** – To help mitigate the risk of abandoned authenticated sessions being hijacked, be sure to set a reasonable session timeout. |
| 18 | **<u>Wireless client isolation</u>** – Unless there is a compelling business reason to allow wireless stations to communicate directly with one another, enable wireless client isolation. |
| 19 | **<u>Radius Server security</u>** – If your authentication infrastructure includes a radius server there are some security concerns to keep in mind:<br>• Use a strong Radius shared secret at least 16 characters long<br>• Do not use the same Radius shared secret for all devices on the network, either set the shared secrets per device or at minimum per group of devices.<br>• Ensure only the authentication type(s) being used is enabled on the Radius server to help mitigate Man-in-the-middle attacks. |
| 20 | **<u>Perform regular security assessments of your WLAN</u>** – Perform regular audits of the configurations and security mechanisms of your WLAN. Keep up on developments in WLAN authentication and authorization schemes, replace schemes that become broken. |

# Upcoming SANS Training
### Click Here for a full list of all Upcoming SANS Events by Location

| | | | |
|---|---|---|---|
| **SANS London November 2017** | **London, GB** | **Nov 27, 2017 - Dec 02, 2017** | **Live Event** |
| **SANS San Francisco Winter 2017** | **San Francisco, CAUS** | **Nov 27, 2017 - Dec 02, 2017** | **Live Event** |
| **SIEM & Tactical Analytics Summit & Training** | **Scottsdale, AZUS** | **Nov 28, 2017 - Dec 05, 2017** | **Live Event** |
| **SANS Khobar 2017** | **Khobar, SA** | **Dec 02, 2017 - Dec 07, 2017** | **Live Event** |
| **European Security Awareness Summit & Training 2017** | **London, GB** | **Dec 04, 2017 - Dec 07, 2017** | **Live Event** |
| **SANS Austin Winter 2017** | **Austin, TXUS** | **Dec 04, 2017 - Dec 09, 2017** | **Live Event** |
| **SANS Munich December 2017** | **Munich, DE** | **Dec 04, 2017 - Dec 09, 2017** | **Live Event** |
| **SANS Frankfurt 2017** | **Frankfurt, DE** | **Dec 11, 2017 - Dec 16, 2017** | **Live Event** |
| **SANS Bangalore 2017** | **Bangalore, IN** | **Dec 11, 2017 - Dec 16, 2017** | **Live Event** |
| **SANS Cyber Defense Initiative 2017** | **Washington, DCUS** | **Dec 12, 2017 - Dec 19, 2017** | **Live Event** |
| **SANS Security East 2018** | **New Orleans, LAUS** | **Jan 08, 2018 - Jan 13, 2018** | **Live Event** |
| **SANS SEC460: Enterprise Threat Beta** | **San Diego, CAUS** | **Jan 08, 2018 - Jan 13, 2018** | **Live Event** |
| **SEC599: Defeat Advanced Adversaries** | **San Francisco, CAUS** | **Jan 15, 2018 - Jan 20, 2018** | **Live Event** |
| **Northern VA Winter - Reston 2018** | **Reston, VAUS** | **Jan 15, 2018 - Jan 20, 2018** | **Live Event** |
| **SANS Amsterdam January 2018** | **Amsterdam, NL** | **Jan 15, 2018 - Jan 20, 2018** | **Live Event** |
| **SANS Dubai 2018** | **Dubai, AE** | **Jan 27, 2018 - Feb 01, 2018** | **Live Event** |
| **SANS Las Vegas 2018** | **Las Vegas, NVUS** | **Jan 28, 2018 - Feb 02, 2018** | **Live Event** |
| **SANS Miami 2018** | **Miami, FLUS** | **Jan 29, 2018 - Feb 03, 2018** | **Live Event** |
| **Cyber Threat Intelligence Summit & Training 2018** | **Bethesda, MDUS** | **Jan 29, 2018 - Feb 05, 2018** | **Live Event** |
| **SANS London February 2018** | **London, GB** | **Feb 05, 2018 - Feb 10, 2018** | **Live Event** |
| **SANS Scottsdale 2018** | **Scottsdale, AZUS** | **Feb 05, 2018 - Feb 10, 2018** | **Live Event** |
| **SANS Southern California- Anaheim 2018** | **Anaheim, CAUS** | **Feb 12, 2018 - Feb 17, 2018** | **Live Event** |
| **SANS Secure India 2018** | **Bangalore, IN** | **Feb 12, 2018 - Feb 17, 2018** | **Live Event** |
| **GridEx IV 2017** | **Online** | **Nov 15, 2017 - Nov 16, 2017** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |