Best Practice Checklist Series - Issue 7

Wi-Fi Deployment and Security

Understanding the basics: A layperson's guide and checklist for overseeing IT.



Best Practice Checklist Series

An exclusive publication of Sandbox Technologies, Inc.

3868 W Carson St, Suite 316
Torrance, CA 90503
Tel. (424) 207-5130
www.sandboxtech.com

SANDBOX TECHNOLOGIES

Small Business Solutions
Enterprise GrowthPath®
EGP Secure®
EGP Cloud™
ConstructIT®

Wi-Fi Deployment and Security

The relative simplicity of deploying consumer wireless products often contributes to misconceptions about the configuration of Wi-Fi networks in a manner that optimizes both security and performance.

Because implementations can vary considerably based on the unique needs of different organizations, the level of planning and the selection of equipment also varies. As such, some of the recommendations in the “Deployment” section of this publication may or may not apply to every situation. Unlike the deployment checklist items, those recommendations in the “Security” section are likely to apply to most network implementations and should be reviewed carefully to ensure adherence when applicable.

Before selecting or implementing any new Wi-Fi solution or installing structured cabling in preparation for an installation, it is always recommended that organizations consult with an experienced Wi-Fi specialist to identify the optimal solution, the appropriate number of access points and the proper placement of equipment.

As always, should you wish to discuss your current settings and protections, or the implementation of a new Wi-Fi solution, your Sandbox Technologies Engineer, Account Manager, or Consulting CIO will be happy to answer any questions you may have.

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Table of Contents

Wi-Fi Deployment 4
Wi-Fi Security 6

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Wi-Fi Deployment

Equipment Suitability Analysis

Has a professional requirements analysis been conducted prior to the selection of a Wi-Fi solution and any supporting hardware?

Security features, the maximum number of concurrent devices supported per access point, access point power requirements, the number of antennas per access point, the access point's multiplexing capabilities, signal tuning capabilities, interoperability with core networking equipment and firewalls, and ability to support single credentials for multi-site implementations when necessary are just a few of the important things to consider before committing to a particular solution.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Equipment Placement Analysis

Has a professional site survey been conducted prior to commencing the installation of any structured cabling intended to support the Wi-Fi solution?

The proper placement of access points is essential for optimal performance. Coverage area requirements, construction materials and other elements can affect signal penetration and performance if not taken into consideration. A few examples of potential impediments to Wi-Fi signal include vintage sheetrock, dense wallboard, plaster or "stucco" and the underlying metal lath or "chicken wire" it binds to, concrete subfloors, magnetic paint, mirrors, glass, steel I-beams, dense wooden beams, and even certain types of water features.

When multiple access points are being implemented, it's a common misconception that closer is better. Unfortunately, that isn't always the case. Positioning access points too close to one another, or too close to connected devices can also contribute to performance problems. Placement is also important when considering newer "wireless mesh" based equipment that communicates without individual cable connections to each access point. While hardwired access points remain the preferred means of implementation, when mesh-based solutions must be deployed, organizations are cautioned to account for the performance degradation that occurs each time an additional access point is "chained" to another access point to extend signal. It is also worth noting that because Wi-Fi communication is bi-directional, strong signal strength from the nearest access point to an associated device does not always guarantee optimal performance if the associated device is incapable of broadcasting a return signal with suitable strength.

For complex implementations, the optimal recommended practice is to procure professional floor plans in CAD or .PDF formal (optimally CAD), import them into professional site-survey software, tag signal impediments and assign broadcast signal strength variables to devices to produce a formal report that can be used to determine the optimal placement locations.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Tuning and Optimization

Has the Wi-Fi solution been properly tuned and optimized for the environment?

The ubiquity of consumer and low-end Wi-Fi solutions often causes business managers to react with surprise when they learn that professional Wi-Fi equipment can be professionally tuned to optimize communication and mitigate various sources of signal interference from competing wireless networks that have been configured to communicate on the same channel or channels. Higher frequencies travel farther and faster but are less capable of penetrating obstructions than lower frequencies, which cover smaller distances and travel at a slower rate of speed. Truly understanding how wireless technology works is essential to ensuring optimal performance.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Wi-Fi Security

Perimeter Firewall Protection

Has perimeter firewall protection been implemented to segment wireless access from the organization's corporate network resources or "LAN"?

Wi-Fi networks can be susceptible to multiple vectors of attack, including MITM (man-in-the-middle) attacks, traffic sniffing, and DDOS attacks. For this reason, wireless networks should only be allowed access to LAN resources when used in conjunction with a VPN client or approved remote access solution on mobile devices and laptops.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Minimum Encryption Requirements

Has the organization's wireless network been configured to communicate using the minimum acceptable communication protocol?

At the time of this writing, WPA2 Enterprise is the minimum recommended communication protocol for most Wi-Fi networks. WPA2 Enterprise (not to be confused with WPA2-PSK, which will typically pass the scrutiny of security auditors but is still subject to eavesdropping) is the second generation of enterprise encryption for wireless communication. Its precursors, WEP and WPA should be regarded as obsolete, and their use can subject an organization to a number of vulnerabilities. NO wireless solution should be considered entirely secure (even when the minimum recommended WPA2 protocol is employed) and as such, it is a recommended best practice that organizations employ the latest generation of encryption available to deter potential attacks.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Implement an Enterprise-Class, Controller-Based Wireless Network.

Is the organization employing the use of an enterprise grade, controller-based wireless network solution?

The foregoing solutions are typically comprised of access points and an internal or Cloud-based controller. As a general rule, professional solutions tend to provide more granular configuration, optimization and security capabilities, centralized control, and a simplified means of deploying critical security and other updates. (Often automatically or with minimal IT intervention required.)

Controller-based Wi-Fi solutions are typically more reliable and provide enhanced performance and visibility into network anomalies. Their centralized control often plays a key role in the rapid identification and mitigation of security flaws that can result from the improper configuration of individual access points.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Guest Network Segmentation

Does the organization maintain a unique, Internet access-only Wi-Fi network that is reserved solely for use by guests and employee-owned devices that are not authorized for use within the company's network?

Guests and/or employees bringing personal mobile devices and laptops on premises creates the potential for unauthorized access to company-owned devices that are authorized for Wi-Fi use. There can be no assurances that devices not owned and actively managed by the organization are being actively managed and protected and are not infected with trojans or other malware that could be used as a pivot point to attack company-owned devices.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Unauthorized Wi-Fi Equipment

Have policies and provisions been put in place to prevent employees or other individuals from installing unauthorized wireless access points?

Organizations often overlook the fact that without suitable protections and established policies prohibiting such, tech savvy employees (often with no malicious intent) have been known to bring unauthorized wireless access points into the workplace and configure them for their own use. Even when this is done with the best of intentions, it can create enormous potential for exposure. In more extreme cases, without protections in place, malicious individuals gaining physical access to an active network port within an organization's office location can do the same for the purpose of breaching an organization's network.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Password Security

Are any default passwords removed from Wi-Fi equipment, and are user and administrative passwords changed periodically in accordance with an established schedule?

Although this should go without saying, any default passwords for wireless access points, controllers, network switches and other related devices should be removed immediately at the time of deployment. Unfortunately, when this simple, yet very critical step is overlooked, the results can be devastating. Similarly, all Wi-Fi passwords should be changed periodically and conform the organization's minimum standards for password length and complexity.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Wireless Flood Protection

Has wireless flood protection been implemented?

While less commonly encountered, wireless flood attacks are a vector that malicious individuals can use to cause network problems and disruption of service. This is done by using software that rapidly and repeatedly attempts to authenticate to one or more wireless access points, often using "spoofed" MAC address identifiers to give the false appearance that each attempt is being made by a different device and thus legitimate.

Status ☐ ✓ ☐ − ☐ ?

NOTES: _____

_____

_____

Prohibit Automatic Connections

Have policies been instituted to prohibiting employees from automatically connecting to wireless networks?

Although this policy is undeniably bothersome, for optimal security, company-owned devices should not be permitted to automatically connect or re-connect to wireless networks. When this is allowed, malicious actors targeting an organization can deploy rogue access points using a network SSID (name) that is identical to that of the company's network. Specialized devices exist for this purpose, and the malicious actors simply amplify the signal strength of their access point and accept any password transmitted by user devices and allow them to connect. User devices interpret the rogue device as legitimate and because the signal is stronger, the device assumes it is a closer access point and attempts to connect to it, rather than connecting to the legitimate network. Unaware that this happening, users devices can be attacked, or their unencrypted Internet activities observed and recorded.

Status ☐ ✓ ☐ − ☐ ?

NOTES: _____

_____

_____

This document is protected by US and International copyright laws. Reproduction or distribution of this document for commercial advantage and without written permission from Sandbox Technologies, Inc. is strictly prohibited. Any distribution must retain attributions and this notice.

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.