

Securing Wireless Networks

The Benefits of Going Wireless

Wireless networks use radio signals instead of wires to carry digital information. As a result, they provide great flexibility by allowing employees to access network resources without the need of a wired connection. They can also be cheaper to install since wires do not need to be installed every place a user may work and increase productivity since employees can take a laptop anywhere in the office and still have access to network resources.

Most users would enjoy the flexibility of a wireless network, but system administrators cringe at the thought of securing one. With some solid understanding of the technology, a network can be secured. Not every network is the same and should be evaluated carefully so that the best combination of security options is used without hindering your users.

This article addresses some of the modifications you should make to your centralized wireless access point to create a more secure network: change basic configuration settings, control the physical device, scramble your data through encryption and ensure proper access through authentication. The topics discussed here can be complex; you should seek professional assistance if you're unsure.

How to Secure Your Wireless Network

A wireless network has security vulnerabilities that can compromise the security and stability of your business. Improper installation can invite intruders in. Before installing, understand some of the inherent downfalls of going wireless and how to safely integrate a wireless network into your business.

What makes wireless networks insecure? First, data is no longer contained within physical wires and cables. Instead, it's sent through the air as radio signals. Anyone with the right equipment can capture the information without the user ever knowing. Second, many business owners buy a wireless access device, install it on the network with the default settings and walk away thinking they're secure. Unfortunately, most wireless equipment is shipped with default settings that leave the network exposed. Third, using the standard wireless encryption method, which scrambles your data, can be insecure. The method of encryption, known as Wired Equivalent Privacy (WEP), can be easily cracked within a matter of hours.

Basic Configuration Settings

Wireless access points contain two settings to access the network: a broadcast beacon and a unique identifier. The beacon is used to publicize networks so that users can see the wireless network they want to connect to. Public hotspots, like Starbucks's, transmit wireless signals using broadcast beacons. Computer users and hackers alike seek these announcements to connect to a wireless network. Turning off the beacon on your centralized wireless device makes it more difficult for hackers to find and subsequently penetrate your company's network.

The unique network identifier, known as the Service Set Identifier (SSID), announces specific networks. The identifier distinguishes individual wireless networks so that users can select which network they want to connect to. Public hotspots can overlap with more than one network. For instance, if Starbucks and Hotel are located next to each other, you want to be able to discern which network you want to connect with.

Like the broadcast beacon, the unique identifier is a setting that should be configured to prevent easy access. Most wireless access points are shipped with a default SSID pre-configured. For example, Netgear devices come with the default SSID of "netgear". Hackers know all the common ones so they can easily

guess the name of many networks. You should change the default identifier to a unique name. Choose one as you would choose a password, but don't make it simple and easy to guess. Avoid using words like the name of your business or phone number. Instead, add some special characters and numbers to it. If you're unsure how to make specific configuration changes for your device, you can refer to the user manual or hire a professional.

Physically Securing the Wireless Access Point Device

The wireless access point needs to be physically controlled. You need to physically lock up or hide your device; otherwise disgruntled employees could access and reconfigure it. Once reconfigured, anyone can gain unauthorized access into your network where financial, confidential and other sensitive data are stored. Many manufacturers have ways of physically locking down the device, including padlocks and cable locks. If your wireless devices cannot be locked, at least hide it above your ceiling tiles so that people don't know where it's located.

In addition to physical control, you need to control the device's radio signals to prevent wireless waves from traveling outside your office. Radio frequencies travel a certain distance before they fade, just like a radio stations transmit their signals. The distance the wave travels depends on the antenna installed on the device; the more powerful antenna, the greater the range.

If you don't limit your wireless signal, an unnoticed hacker sitting in your parking lot can access your network. To prevent this, mount the device then walk the perimeters of the facility with a laptop until you determine when the signal fades. If the signals travel more than a few feet past your building or office, turn down the bandwidth meter in the device.

Next, you need to determine where you will place you wireless devices on the network. You're likely to already have some security devices on you network that you can take advantage of, like a firewall. Placing your wireless devices on a few

select ports in your firewall allows the firewall to protect your network by monitoring all network traffic.

How to Verify Acceptable Users

You need to decide who is authorized to access your network so that you can verify employees are who they say they are. You can authenticate users in several ways, depending on the size and complexity of your network.

The simplest way is using a computer's unique hardware address. Once you configure the wireless access point to use the hardware address of an employee's workstation, it can verify the workstation and grant, or deny, access to the network. This type of authentication is ideal for home and small businesses because there aren't many workstations to manage. However, a good hacker can get a permitted hardware address and reconfigure his workstation or laptop to use that address. This method of hacking is known as address spoofing. It's not an easy trick to pull off, but it still leaves your wireless network vulnerable.

Another way to authenticate is to use a password. You give authorized users a shared password to access the wireless network. However, if the password is accidentally published, it has to be changed on the wireless device and users need to be told of the new password. Although this approach takes less time to configure on the front end, it can take more time when changes need to be made, especially if employees resign or are terminated. It's a quick solution, but not the most secure solution.

The most secure way of authentication is using an authentication server, where usernames and passwords already exist. The same information used to gain access to network resources is also used to gain access to the wireless network. The advantage of this configuration is that users have their own unique login so their password can be changed without affecting any other users. In addition, this method provides a way of tracking which users log in and when. The biggest

drawback with this configuration is the amount of hardware resources and expense required. A centralized database server and an authentication server are both needed for this particular configuration.

Businesses also can combine any of these three methods of authentication to make their networks more secure. It just takes more time and a little more money. If you're unsure how to make specific configuration changes, either refer to the user manual for your device or hire professional help.

Hiding Your Data From Prying Eyes

To ensure only your intended users can access your data, you need to encrypt it, which is part of the user authentication process. Early encryption technology, called Wired Equivalent Privacy (WEP), was poorly designed and had a repeating pattern. This predictability eventually allowed hackers to break in.

Today, there are two alternative encryption protocols: IP Security (IPSec) and WiFi Protected Access (WPA). IPSec is an encryption formula typically used for securing server-to-server communications and external connections. It's a very difficult protocol to crack, which gives it an enormous advantage. Unfortunately, it requires more bandwidth (a T-1 line instead of dial-up) and costs more to operate.

Another encryption technique, called WiFi Protected Access (WPA), uses information from the user-verification process to uniquely encrypt the data. There are a few requirements for getting WPA working:

- 1) First, verify your users through an authentication process. For small networks, passwords or hardware addresses can be used to authenticate user identity. For large network environments, an authentication server should be configured.

2) For companies that use an authentication server, you need to install digital certificates on the server and all of the workstations. Certificates are another way of verifying who the workstation and user are. Microsoft Windows Server versions 2000 and 2003 provide free certificate software. If neither of these servers is available, you can get a certificate from a company such as Verisign on the internet.

3) The workstation's wireless access cards must be WPA-compliant. If they are not compliant, it's possible the card's device software can be updated from the manufacturer's website, otherwise, a new card will need to be purchased.

New standards for wireless data encryption are emerging. In the meantime, WPA provides good data security. With that said if you have no other means for securing your data due to compatibility issues then at least encrypt your information with WEP. After all, something is better than nothing.

Wireless Implementation Checklist

1. Physical
 1. Ensure the wireless device is physically locked down.
 2. Control how far the wireless signal travels.
 3. Take advantage of other security devices such as firewalls.
2. Basic Configuration
 1. Disable the broadcast beacon from announcing the device
 2. Use a unique Service Set Identifier (SSID)
3. Authentication
 1. Verify users using the workstation hardware address.
 2. Password-protect your wireless network.
 3. Authentication server provides the most robust security.
4. Encryption
 1. The original Wireless Encryption Protocol (WEP) provides basic scrambling capabilities, but can be penetrated due to a repeating pattern.
 2. The IPSec provides better encryption but requires more bandwidth to operate.
 3. The most recent wireless encryption protocol (WPA) offers the most protection, but requires additional hardware to function.

Note: Some of the suggested solutions may not work in every situation.

Dictionary

802.1x A new standard designed to enhance the security of wireless local area networks. 802.1X provides an authentication framework for wireless networks, allowing a user to be authenticated by a central authority, like Verisign or in-house software (Windows).

AES Short for **A**dvanced **E**ncryption **S**tandard. An encryption formula for securing sensitive, but unclassified, material by U.S. government agencies. AES may eventually become the encryption standard for commercial transactions in the private sector.

Algorithm A formula or set of steps for solving a particular problem. To be an algorithm, a set of rules must be unambiguous and have a clear stopping point. We use algorithms every day. For example, a recipe for baking a cake is an algorithm.

DMZ Short for **D**emilitarized **Z**one. A computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.

- Hacker** Someone who tries to break into computer systems with malicious intent, usually to either steal data or use system resources.
- IPSec** Short for **IP Security**. A set of protocols developed to support secure exchange of data. Typically implemented in server-to-server communication and Virtual Private Networks (VPNs).
- MAC** Short for **Media Access Control** address. A hardware address that uniquely identifies each network device of a local area network (LAN) or other network.
- RADIUS** Short for **Remote Authentication Dial-In User Service**, which is an authentication and accounting system. When you dial in to many networks, you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access.
- SSID** Short for **Service Set Identifier**. A 32-character unique identifier sent over a wireless network that acts as a password when a mobile device tries to connect. The SSID differentiates one wireless network from another, so all access points and all devices attempting to connect to a specific network must use the same SSID.
- VPN** Short for **Virtual Private Network** is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.
- WEP** Short for **Wired Equivalent Privacy**. A security protocol for wireless networks.. However, it has been found that WEP is not as secure as once believed.
- WPA** Short for **Wi-Fi Protected Access**. A security standard for users of computers equipped with a wireless connection. It is an improvement on and is expected to replace the original Wi-Fi security standard, Wired Equivalent Privacy (WEP). WPA provides more sophisticated data encryption than WEP and also provides user authentication.