



Makes Perfect  
Degree of Separation

# 10 Steps to Lock Down Wireless LANs

You can get a thoroughly secure wireless infrastructure, provided that you conduct a rigorous planning cycle and take the steps necessary to fortify your network. Here's how.

Since their advent in the early 1990s, there's been considerable debate about the security of wireless local area networks (WLANs). Specific concerns have revolved around WLANs' data transmission based on radio frequency (RF) signals traveling through the air, the relative strength of various security protocols and the general rise in malicious activity by hackers.

But WLANs have made significant security strides in recent years, both in terms of their underlying technology and in the sophistication of how organizations deploy and secure them. When planned, configured, used and monitored properly, WLANs — and the access point (AP) hardware through which wireless users communicate — can be very secure. But it's critical that businesses keep up with current best practices on exactly how to lock down their networks.

With that in mind, here are 10 specific steps companies should take as they move to wireless or combined wireless/wired networks.

## 1 Planning Makes Perfect

Wireless vendors and other experts recommend that businesses conduct a detailed planning and analysis process before deploying wireless technology. For instance, wireless survey products — such as Fluke Networks' InterpretAir — can help you determine optimal placement for wireless APs based on environmental conditions and other factors in a given building. In conducting this analysis, an administrator or network engineer first imports a map of a facility that will house

the wireless network. That is followed by the addition of information on building construction — brick, glass or steel walls, for instance. Then an administrator will place access points in certain locations and see a simulation of radiated RF energy in the configurations being tested. The goal: ensuring the minimal amount of radio signals leaking out, thereby avoiding major security issues that could occur if those signals are accessible and get intercepted.

As a second step in the analysis phase, InterpretAir can be used to conduct post-installation verification tests. "At the conclusion of the physical installation, you want to validate that RF performance is living up to what you expect — in terms of data rate, interference and different criteria to evaluate the quality of the install," explains Eric Anderson, marketing manager at Fluke Networks.

For customers in an office park, InterpretAir can also detect APs in other companies in the area. "From a security standpoint, you can start looking at whether there are other wireless networks in the vicinity that are potential risks," Anderson says.

## 2 One Degree of Separation

When your company has a wireless and a wired network, the optimal approach to network configuration is to physically separate the wireless LAN from the wired LAN by placing the former on its own network segment, separate from the trusted, wired LAN, explains Corey Nachreiner, network security analyst for WatchGuard Technologies. "Wireless is a little less secure; you don't want any hacker to jump right on your trusted network," he says.

Taking that separation between LAN and wireless LAN further, WatchGuard recommends using an approach called "forced VPN [virtual private network]" »



that the firm supports in its firewalls. In this configuration, even if a user is established and authorized to access the wireless network, the user still must establish a virtual private network connection through the access point to the wired LAN. “When you use forced VPN, you use our mobile IP [Internet Protocol] security client, along with our mobile VPN user client, and that turns our wireless access point into a VPN server,” Nachreiner says.

A similar recommendation comes from SofaWare, a Check Point company. SofaWare CEO Liran Eshel recommends that even when isolating wireless and wired networks on separate segments, placing a network firewall between them. A Check Point Safe@Office firewall, for instance, is set on a default basis to prevent access to the wired network for users that have wireless network access, Eshel explains.

### 3 Understand the Danger in Defaults

A smart network administrator needs to be well versed in the dangers of sticking with default settings and factory-set passwords. At several levels, default settings need to be changed, in some cases regularly, to make wireless networks harder to hack. Specifically:

- Every AP comes set for an administrator to gain access and tinker, but generally the initial log-on requires either no password or a known password. This should be changed from the outset. Apply your company's password policy — at minimum, an alphanumeric and special character code of no fewer than eight characters. For high-security environments, turn to automated password generators or two-factor access codes to authenticate users.
- Vendors often create default key sets for shared-key authentication between the AP and wireless devices trying to access the network. You'll want to change these from their default settings and continue changing them on a regular basis to keep the bad guys out.
- Beware of the reset function, as it generally reverts a device to the factory defaults — making your network vulnerable to intrusion. Make sure this function is off-limits to everyone but systems administrators. This requires two things: physical security for the devices — because APs often have depressed buttons to invoke the reset function — and software-controlled access for devices that allow remote reset.
- Every AP will come with what is essentially a default name — the service set identifier (SSID) — that then becomes the 32-byte ID for your WLAN. The defaults used by vendors are well known so you need to change the SSIDs on your APs. While smart hackers can easily sniff SSIDs and compromise this type of security, the change will keep out random unwanted users and less-sophisticated hackers. “You should just name it something different, that’s meaningful to you,” Nachreiner advises.

## 4 The Benefits of Encryption

An AP will arrive from a vendor ready to handle a few preset encryption levels. Go for the highest level a product allows — typically, no more than 128-bit shared keys on current APs. It's crucial to keep in mind that for a network with multiple APs, you must set them all at the same level of encryption. An older product that tops out at 104-bit keys won't work with one set to 128-bit; you'll have to go with 104-bit throughout.

The latest wireless security standard, Wi-Fi Protected Access (WPA), offers more robust encryption than its predecessor, Wired Equivalent Privacy (WEP). Over time, WEP was found to have weaknesses that have been overcome in WPA, experts say. Still, even with WPA, it's important that administrators set strong passwords to control access to a given AP. "Use greater than 10 characters; it's good to throw number and character combos," says Nachreiner. "We recommend people pick some sentence with full grammar and capitalization."

That said, even if your AP supports only WEP, it should be turned on; a large percentage of APs don't even utilize the encryption that's built into them. Experts say that war-driving activities — where people go out seeking open, unsecured access points — typically identify a high percentage of completely unprotected APs. According to Scott Pinzon, editor-in-chief of WatchGuard's LiveSecurity service, tests consistently find that approximately 30 percent of detected wireless APs have no encryption turned on.

## 5 Create Unique Addresses and Control Them

You can create unique addresses for end-user devices that you will allow to access your network, and enter those addresses into your AP. By assigning these Media Access Control (MAC) protocol addresses, you will know who is trying to get on, who is on, and if someone who isn't authorized to access your AP is trying to do so. The system administrator can then create an access control list (ACL) of MAC addresses that the AP would use to accept or reject would-be users.

## 6 Keep a Low Profile

Each AP sends a signal so wireless devices can find it to gain access. But you can maximize the timing between blasts from your signal beacon so that your AP's not blaring overly frequently, as if to announce, "Here's a wireless node, everybody come on in." It will be much tougher for scanning hackers to passively hone in on your network if you set the beacon signal as high as possible — typically 67 seconds.

## 7 Manage Under Control

Only keep Simple Network Management Protocol agents functional on your AP if they are at SNMP Version 3. Versions 1 and 2 make it possible for attackers to manipulate the agents and hack their way around the AP and onto your network. SNMP 3 will let you monitor activity and your WLAN and troll for intruders.

## 8 Security by Avoidance

You can block breaches to your wired networks via your WLAN by foregoing use of Dynamic Host Control Protocol (DHCP) servers. A DHCP server automatically assigns temporary IP addresses to devices that have gained access so that users can access other networks. But the DHCP server can't validate the users to which it gives IP addresses. So if a hacker gets through your first line of defense, your other systems become vulnerable. Instead, systems administrators should set the addresses for your users' wireless devices.

## 9 Robust Analysis

If your network has both wired and wireless segments, you should have a tool capable of analyzing both. A WLAN/LAN analyzer can help your system administrator quickly isolate urgent problems on your wired/wireless network as well as issues that may be keeping it from performing at an optimal level. An analyzer can help discover virtual LANs (VLANs), measure RF signals, analyze network traffic, identify top talkers, discover unauthorized devices and locate rogue devices.

Such analysis, using tools such as Fluke's EtherScope, will detect where there's an unprotected access point that doesn't have encryption enabled, Anderson explains.

## 10 Audit and Analyze

Experts recommend regular audits of a wireless network once it has been established. Specific tests that can and should be run include testing to see where a given AP's signal can be received from. They also suggest testing the signal strength of AP antennas to determine the best orientation for those antennas, and to determine how to prevent APs being available beyond the walls of a building. In addition, administrators should "look over firewall logs periodically, and if they see things that don't make sense based on what they installed, that's a tip-off," says WatchGuard's Pinzon.

If you follow these 10 recommendations, you can cast aside the hype and fear surrounding wireless LANs and operate your networks with the confidence that you won't suffer a security breach. ♦

Short on time and staff?  
Ask about CDW technology services  
to bolster your IT effort.