Five-Step Plan for Securing your Enterprise WLAN

by Lisa Phifer, Core Competence Inc.

Wi-Fi has spread like wildfire, leveraging consumer popularity and business benefits to penetrate corporate networks. As a result, many business assets are now routinely exposed to wireless threats, without corporate awareness or intervention. Wi-Fi misuse, abuse, or attack can cause financial harm, including direct costs associated with investigation, response, down-time, and recovery; indirect losses due to decline in competitiveness and market value; and directed remedies and penalties caused by non-compliance with data privacy regulations.

Given these internal and external pressures to audit and prevent unauthorized network use, every company – even those that ban wireless – must manage the business risks posed by Wi-Fi. Conventional measures used to secure applications, systems, and wired traffic are still essential. However, lack of physical control over the airwaves means that wired defenses can be bypassed. Employees often connect, accidentally or intentionally, to neighbor WLANs, ad hoc peers, or malicious honeypots. Rogue or misconfigured access points can open long-term, unprotected, invisible back doors into corporate networks.

Existing security policies, implementations, and practices must evolve to address these new threats. An effective network defense now requires the ability to control all wireless activity that impacts your business. This paper decomposes the challenge of securing an enterprise wireless LAN (WLAN) into five essential steps. From safeguarding wireless clients and data to auditing and controlling Wi-Fi connections, this paper recommends best practices to ensure the safety and integrity of today's enterprise networks.

Step 1: Protect wireless clients

Over 95 percent of laptops now ship with Wi-Fi, as do many handheld devices. Whether your company bans Wi-Fi or embraces it, these ubiquitous client devices must be protected from wireless-borne threats, ranging from over-the-air viruses and TCP/IP exploits to unsafe, unauthorized, or accidental Wi-Fi connections, initiated by inexperienced or unaware users.

Conventional defenses commonly deployed on Internet hosts, including file encryption, anti-virus, and personal firewall programs, should also be used on Wi-Fi clients. These measures help insulate Wi-Fi clients from TCP/IP intrusions, like accidental file sharing and worm propagation at wireless hotspots.

However, these measures cannot stop risky Wi-Fi connections. New client defenses are needed to prevent employees from associating with neighbor WLANs, ad hoc peers, or malicious honeypots. Some out-of-policy connections are intentional, used to bypass corporate bans on personal email or P2P. Most are accidental, launched silently by promiscuous "zero config" software. Either way, unauthorized Wi-Fi connections jeopardize corporate assets by exposing confidential data and bridging between networks.

To regain control over employee Wi-Fi, configure all clients to associate only with authorized Service Set Identifiers (SSIDs). Unless required for business, deny all ad hoc connections. For best results, use centrally-administered policies -- for example, Windows Wi-Fi connection parameters can be configured via Active Directory Group Policy Objects. To stop employees from adding their own connections, use a third-party connection manager that supports lock-able Wi-Fi client configurations.

To automatically disconnect unsafe associations, deploy a host-resident Wi-Fi Intrusion Prevention program on every client. A Host WIPS can keep an eye on corporate laptops used at home and hotspot WLANs, taking action as needed to enforce your defined Wi-Fi policy. Controlling where and how clients are permitted to connect over Wi-Fi, inside and outside the corporate network, is the only reliable way to protect your workforce against both malicious attack and all-too-common wireless mistakes.

Step 2: Secure data in transit

Wireless networks lack the physical security inherent to wired Ethernet. Since walls, doors, and floors cannot effectively contain Wi-Fi transmissions, new defenses are required to deter eavesdropping, forgery, and replay attacks on business data sent over the air.

If your company already uses a Virtual Private Network to protect business data on the public Internet, leverage that VPN to secure Wi-Fi traffic sent over home and hotspot WLANs. This ensures consistent protection for off-site traffic, independent of any measures used by WLANs that lie beyond your control.

Some companies also use VPNs to protect on-site Wi-Fi -- particularly early adopters who were limited to the cracked Wired Equivalent Privacy (WEP) found in Wi-Fi products through mid-2003. Fortunately, all Wi-Fi-certified products now offer two vastly-improved data protection alternatives:

- Wi-Fi Protected Access (WPA) uses the Temporal Key Integrity Protocol (TKIP) to deter eavesdropping, forgery, and replay of Wi-Fi data. This interim measure resists WEP cracking, but is slower than its successor, WPA2. Today, WPA should be used in WLANs with legacy products.

- WPA Version 2 (WPA2), supported by all Wi-Fi products since late 2004, uses 802.11i and the Advanced Encryption Standard (AES) to secure data in a stronger, more efficient manner. Most enterprise WLANs should now upgrade to WPA2 for robust data privacy and integrity.

Of course, VPNs can still be used inside office WLANs today. However, VPNs add overhead and impede roaming. Most companies will find it best to secure data using VPN off-site and WPA2 on-site.

Step 3: Control corporate network use

To prevent network breach, every element exposed to Wi-Fi, from the APs and switches used to deliver access to the corporate networks reached via wireless, must be insulated against unauthorized use.

Start by applying conventional perimeter defenses to the wireless edge of your network. For example, harden APs and switches by updating patches, closing unused ports, and using secure management interfaces. Extend the VLANs and firewalls already used to control traffic flow inside your wired network to segregate all traffic that enters over Wi-Fi, based on SSID or user identity.

This is a good start, but simply not enough. Rogue or misconfigured APs plugged into your wired network bypass your firewall, providing long-term external access to internal servers and data. Without further controls, neighbors, guests, and intruders can all use your WLAN to steal Internet service, send phishing emails or spam, or even attack your wired network.

You can reduce accidental Wi-Fi connections by configuring your APs with non-default SSIDs. But don't stop there -- deploy Wi-Fi access controls to explictly deny connections from unauthorized clients:

- Due to ease of address spoofing, never depend on MAC address filters for Wi-Fi security.

- If you offer guest access, use a captive portal to track use and enforce time/bandwidth limits.

- In small WLANs, use WPA or WPA2 with a Pre-Shared Key (PSK) to grant access only to authorized clients that present a long, random group password. This is largely intended for home WLANs.

- In enterprise WLANs that need stronger-than-password control over individual users, deploy 802.1X to authorize and audit Wi-Fi connections permitted to reach the corporate network. When used with server certificates, 802.1X can also help clients avoid connecting to fake honeypot APs.

Finally, it is essential to enforce your Wi-Fi data protection and access control choices. A centralized WLAN manager can help to reduce AP misconfiguration and speed recovery after failure or attack.

Step 4: Audit wireless activity

In the end, no matter how carefully you deploy these network, client, and over-the-air security measures, unexpected and unauthorized wireless activity is still quite likely. To meet the internal and external audit requirements that face most businesses today, you will need to monitor and report on the actions taken by all Wi-Fi devices operating within your corporate airspace.

When it comes to wireless traffic, conventional audit resources like firewall logs and wired Network Intrusion Detection Systems are insufficient. Those systems can only monitor traffic inside your wired network. They simply cannot see wireless activity like out-of-policy Wi-Fi connections to neighbors and honeypots. They miss attacks aimed at the WLAN itself, like 802.11/802.1X Denial of Service (DoS) floods and Wi-Fi password-cracking. And they cannot be used to document compliance with defined Wi-Fi security policies or to assess corporate exposures caused by wireless misuse or abuse.

Every company -- including those without authorized WLANs -- should be able to discover and document wireless devices and their locations, activities, policy violations, and attacks. This can be accomplished by deploying a Wireless Intrusion Prevention System (WIPS) for 24/7 surveillance of all Wi-Fi activity that has the potential to impact your business. A WIPS uses a distributed network of sensors to scan the radio channels used by Wi-Fi, analyzing traffic to detect unauthorized connections, misconfigurations, and malicious actions. A WIPS will alert you to potential threats and help you visualize Wi-Fi activity in real-time. The database maintained by the WIPS will let you easily generate regulatory compliance reports.

Step 5: Enforce wireless policy

Of course, passive monitoring is not really enough. By the time a human responds to a WIPS alert, considerable damage may have been done, and intruders may have disappeared. *Proactive prevention* is required by corporate policies and industry regulations that mandate network and data security.

Deploy a WIPS that gives you the ability to immediately enforce defined rules, disconnect unauthorized rogue APs, stop client misbehavior, impede out-of-policy communication, and neutralize DoS attacks. To accomplish these goals, choose and configure your WIPS with care. For example:

- Plan sensor placement to avoid "blind spots" -- and then verify expected coverage.

- Look for a WIPS that automatically and accurately classifies newly-discovered devices, so that any action taken to "contain" them is always appropriate and never intrudes on your neighbor's WLAN.

- Test the effectiveness of your WIPS to quickly and correctly identify rogue APs, ad hoc connections, misbehaving clients, and other Wi-Fi threats of importance to your business.

- Watch out for systems that generate false alerts and inaccurate location estimates -- they waste time and resources by sending you on a wild goose chase.

- To comply with data privacy mandates that require strict policy enforcement, choose a WIPS that can contain multiple security threats at once in a real-time, scaleable fashion.

- Finally, review alerts and reports to understand whether and how the WIPS is enforcing your policies. A WIPS gives you the power to control your airspace, but using that power wisely is still up to you.

Conclusion

Although every company is different, most eventually find that a comprehensive defense requires all five of these steps, working in concert to mitigate common Wi-Fi threats. However, any security measure is most effective when deployed within a risk management context.

Whether your company bans Wi-Fi or plans to adopt Wi-Fi campus-wide, start by assessing the threats that face your business and their potential impact. Define your Wi-Fi needs: who, what, where, and when should Wi-Fi be used to support business activities, on-site and off-site? Examine all devices that will be exposed to Wi-Fi and how they might be accidentally misused or intentionally attacked.

Next, consider the likelihood of each security incident and the associated cost or damage that might be incurred by your business. You cannot mitigate every possible threat. Nor can you really know how much time and money to spend on threat mitigation unless you have a good handle on business risk. Completing a Wi-Fi vulnerability assessment and business risk analysis can help you focus your security budget on the measures that will have the greatest impact.

Once you have defined a security policy designed to mitigate your business' top-priority Wi-Fi threats, use the five steps outlined in this paper to implement your policy and manage your business risk. While Wi-Fi security isn't automatic or easy, it can certainly be accomplished through policy definition and enforcement with readily available tools. In this era of ubiquitous Wi-Fi, applying the best practices described herein can help you to ensure the safety and integrity of your corporate network.

About the Author
Lisa Phifer has been involved in the design, implementation, and evaluation of network technologies for over 25 years. As the owner of Core Competence Inc., an Internet security consulting firm, she has advised companies large and small regarding business needs, product assessment, and the use of emerging technologies and best practices. Before joining Core Competence, Lisa won a Bellcore President's Award for her work on ATM. She has taught numerous wireless LAN, mobile security, and VPN workshops, and writes extensively for industry publications, including Wi-Fi Planet, Business Communications Review, Information Security, and SearchNetworking. Lisa's monthly Wireless Advisor and Mobile Innovator columns are published by searchMobileComputing.