

Ten Easy Steps for Wireless LAN Security

Here are some relatively simple, low-cost ways to optimize the security of your wireless LANs. They're not perfect, but they do provide at least the first few lines of defense. They are listed in approximate order of difficulty and cost. Steps 1 through 6 should be considered as essential to creating & maintaining security. Remember that once an intruder has access to your LAN, sniffing passwords and other confidential data becomes much easier than trying to break in from outside the LAN. An attacker will always choose the path of least resistance, so don't be tempted into lax security when it is relatively easy to secure your wireless infrastructure – it also helps you sleep better at night!

1. Enable the highest level of WEP (Wired Equivalent Protocol) that ships with the access point. WEP has several well-known flaws; however it does provide some useful measure of protection. Both 802.11b and 802.11g provide up to 128-bit WEP. Several Wi-Fi products also support proprietary 256-bit WEP extensions. Windows® XP also supports 256-bit WPA (Wi-Fi Protected Access) which is somewhat more secure than WEP. Most modern Wi-Fi equipment supports WPA, although it is usually not possible to use both WEP & WPA simultaneously on the same device.
2. Change the default SSID (Service Set ID) that ships with the access point and/or wireless router. Finding an access point with the default SSID signals an unguarded access point. Change the default device password while you're configuring things. The combination of default SSID & default password is an open invitation to unwanted visitors!
3. Disable the "broadcast" mode in which access points periodically transmit their SSID. Since determined attackers will often know the default names of many access points, they can use freeware utilities or even the tools included in Windows® XP, to find the names of nearby wireless networks (see point 8).
4. Implement infrastructure mode, where all wireless clients on a network link directly via an access point or wireless router. Disable the "Ad-Hoc" mode everywhere, which enables a peer-to-peer network and thus allows an unauthorized user to connect with other wireless LAN cards without any authentication. This opens the door for any attacker in wireless range to access your network through a legitimate wireless user.
5. Set up MAC Address Authentication via access control lists (ACLs). Configure your access points so they allow only clients with specific MAC addresses to access the network, or allow access to only a given number of MAC addresses. Note that this can reduce flexibility in giving access to visitors and others who require ad-hoc access to LAN-hosted services, but unless you are using a more sophisticated authentication method (such as a VPN or RADIUS server), this is a small price to pay for the enhanced security afforded. Some of the high-end APs such as those from Buffalo URL: <<http://www.buffalotech.com/products/wireless.php>> have a RADIUS server built in.
6. Educate your network users about the security risks of wireless networking, then create and enforce a wireless security policy. Look at the logs of your AP regularly to determine if security has been breached or has been threatened by attackers.
7. Place access points on separate subnets and put a firewall between that subnet and the main corporate network. This mimics the architecture of many security tools which put a gateway or other security server between the access points and the wired network.
8. Perform a regular audit for rogue access points. By "rouge", we mean unsecured. For example, a department might be experiencing a dead spot & innocently add another AP to compensate without securing it. We recommend that a scan be performed at least once a

quarter, if not once a month. This can be as easy as walking around with a wireless notebook equipped with free sniffer software such as the excellent NetStumbler program URL: <<http://www.netstumbler.com/>> or Windows® XP, or as ambitious as using SNMP queries to find new devices that have been added to your network. If you do find any rogue access points, you'll need to shut them down or reconfigure them to be secure in line with these guidelines. See also point 6.

9. If you're running SNMP (Simple Network Management Protocol) agents on your access points, assign a non-obvious name to the "community" that identifies which management applications can communicate with those agents. That way, wireless attackers can't just sniff around for the default community names that ship with many management tools.

10. Implement Virtual Private Networking (VPN) over the wireless LAN. This technology makes it possible for users to communicate securely via a VPN tunnel between the client desktop or notebook PC and the wired network. VPNs employ encryption and strong authentication methods as mechanisms for hiding or masking information about the private network topology from potential attackers on the public network. This solution typically requires a separate VPN server and can be relatively costly to implement & maintain.

General Observations

The only sure way of ensuring total security is to disconnect your computers from any source of power & lock them in a bank vault! Given that some level of insecurity must be accepted, the steps outlined above merely place barriers of increasing difficulty in the way of those who want to gain unauthorized access to your network. No security is insurmountable or foolproof, but your aim should be to make your WLAN demand too much effort to break into easily so that the attacker will move on to easier targets.

Windows® XP: In our experience, it is well worth applying Service Pack 2 (SP2) to any machine using a wireless device due to the many improvements to wireless support in SP2. In fact, SP2 should be applied to all machines running Windows® XP if at all possible!

For home and small business: The combination of using a unique SSID + disabling SSID broadcast + MAC Address Authentication + WEP (or preferably WPA) encryption provides an acceptable level of wireless security. Any wireless product you are considering using should support this level of security as a minimum. **Beware: some don't!**

For medium and enterprise business: With centrally managed administration for a large number of users and the ease of deployment and control, VPN or RADIUS is a better choice for wireless security. VPN offers the most powerful methods to ensure that network access is strictly limited to users who can be authenticated via the VPN Server. All the major manufacturers of wireless LAN products that we are aware of support VPN pass-through.

Although "security through obscurity" can confer a false sense of security, an interesting application of this is FakeAP URL: <<http://www.blackalchemy.to/project/fakeap/>>, which employs a wireless card to send out 53,000 fake AP beacon frames. This will make finding your genuine WLAN very much harder for the casual snooper.

Finally: Be careful, the wireless world is full of people who will happily abuse your WLAN if they can find it & use it. Don't let them!