

Real-World Scenario 9-2: Securing a Wireless Device

Scenario: You have a new client, a small marketing office with six computers and a SOHO router/WAP. The client wants you to secure the device so that the internal computers will be safe and the wireless network will be difficult to attack.

Define eight ways in which you can protect this wireless network.

Real-World Scenario 9-2 Solution

There are a host of things you can do to secure a wireless network. The following eight-step list should be incorporated into most plans to secure a WAP, but you will undoubtedly add your own zest to the mix!

- Step 1.** Update firmware. Download the latest firmware, install it, and test it before implementation. Any hotfixes and updates (if the device accepts them) should be installed as well. Check for updates automatically, and have the device's manufacturer e-mail you if new updates are released.
- Step 2.** Set passwords! Enter separate, complex passwords for the administrator and the user accounts.
- Step 3.** Disable remote administration. If it is not necessary, remove this functionality by disabling it. Or, if it is necessary, consider changing the port from the commonly used 8080 to something less well known.
- Step 4.** Disable SSID broadcasting. Once all computers have been connected, make the wireless network invisible by disabling the SSID. Computers can still connect, in a manual, step-by-step fashion, but at least it will be more difficult to scan for the SSID.

NOTE Before anyone ever connects to the WAP, change the SSID from the default name to something less common.

- Step 5.** Enable encryption. As of the writing of this book, WPA2 and AES are the best options. (But anything is better than nothing.) Select a complex preshared key. If possible, use a RADIUS server for authentication.
- Step 6.** Reduce the output transmitting power of the WAP. Sometimes, the wireless network is too powerful and reaches far beyond the physical perimeter of the office. Antennas are set to a specific output power by default (for example, 90 mW). This can be

reduced on some WAPs, which will ultimately reduce the range of the wireless network.

Step 7. Enable MAC filtering. This configuration enables you to allow or deny specific MAC addresses.

Step 8. Configure other rules and ACLs. This might include inbound filters, access control policies, application rules, and so on. Depending on your organization's function, you might decide to implement other options, such as captive portals and secure VPN.

In Steps 7 and 8, be sure that you don't lock down your WAP too tightly, or you might end up restricting access to clients that legitimately need to access your wireless network.

Video Solution: Watch the video solution "9-2: Securing a Wireless Device."