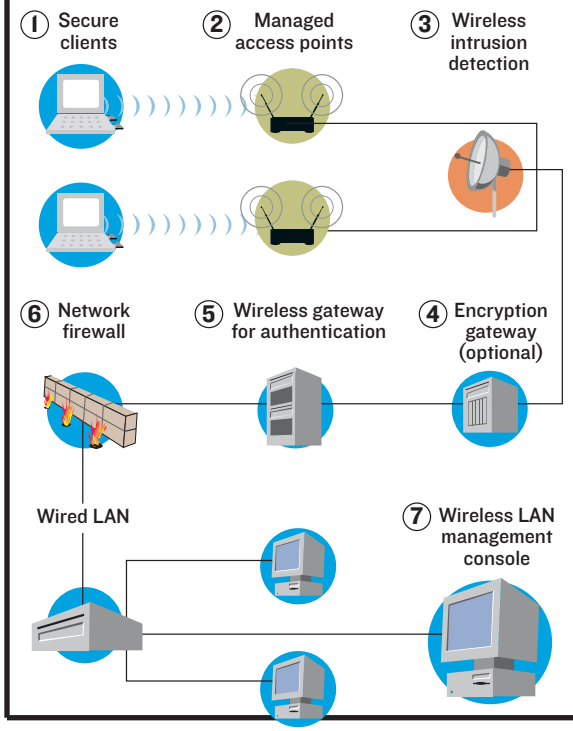
Visions of a secure WLAN



1 At minimum, a secure wireless client should be running firewall and virtual private networking private software. You might also want to deploy software agents for ensuring that remote clients adhere to security policies.

2 Managed access points, sometimes called "lightweight" APs, don't inclued a lot of intelligence and can be controlled from a central management console. Set up the APs to minimize signal leakage.

3 Wireless intrusion detection system sensors sit out along the WLAN perimeter scanning for rogue APs and other security breaches. They report back to a management server. Think roughly one WIDS sensor per five to 10 APs.

4 An encryption gateway can offer additional security beyond typical VPN services. The Joint Futures Lab added such a gateway to its WLAN when it discovered IPSec was leaving some information unprotected.

5 The wireless gateway can handle authentication, role-based access control and several other WLAN security functions.

6 Keep your WLAN outside your firewall. For additional security, you can also run the WLAN on separate switches, putting more distance between it and the wired network.

7 Centralized wireless network management software helps admins configure APs, monitor traffic, enforce policy and more.