SonicWALL's Secure & Clean Wireless

SonicWALL's Secure & Clean Wireless solution integrates 802.11n performance with enterprise-class network security appliances to deliver unmatched wireless network security for any 802.11-based wireless network. Some of the key functions are...

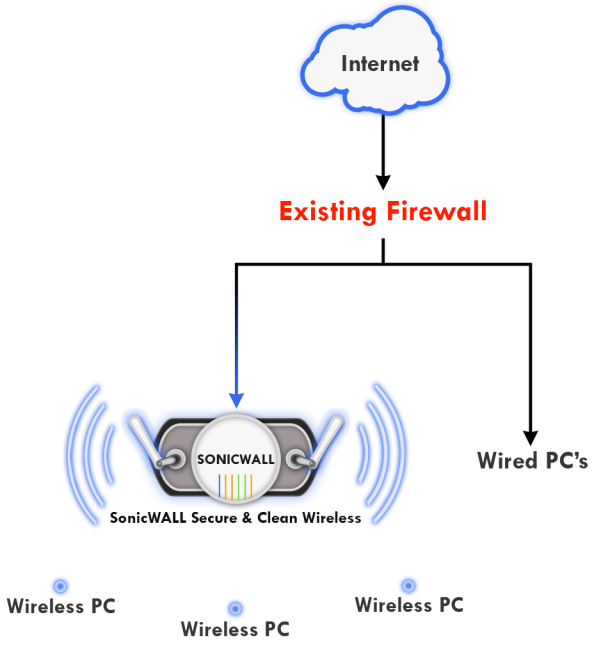
- Antivirus / Antispyware / Intrusion Prevention
- Content Filtering
- Guest Services - enabling the control of guest access and use of the wireless network
- Virtual Access Points - enabling the provision of multiple wireless networks (eg guest & staff) with different security policies on the same access points

The three ways in which a SonicWALL Secure & Clean Wireless solution is typically deployed:

SCENARIO 1

Installing SonicWALL Secure & Clean Wireless into an Existing Network:

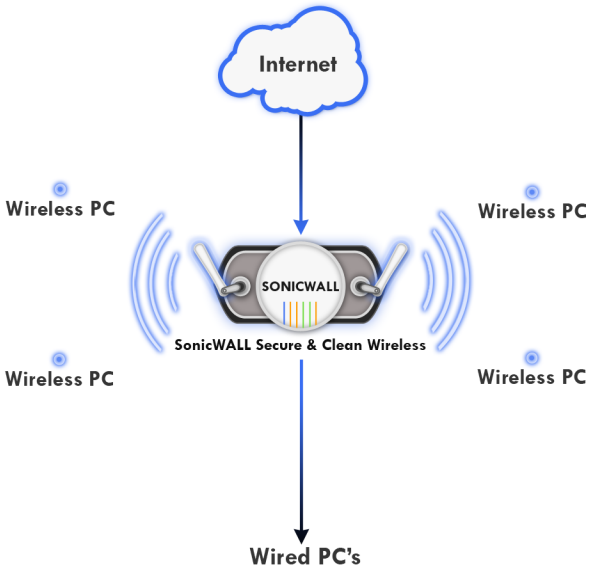
The easiest way to install a SonicWALL wireless solution into an existing network is to configure the SonicWALL for DHCP and connect it to the LAN at a location that is central/nearby to where wireless users work. Once done the unit can be configured to enforce the security services outlined above (eg: Content Filtering, Guest Authentication, etc.) on all wireless traffic.



SCENARIO 2

Installing SonicWALL Secure & Clean Wireless at the Perimeter of the Network:

In this scenario, the SonicWALL becomes the primary security solution for the wired and wireless network. Once installed the unit can be configured to enforce the security services outlined above on all wired and wireless traffic.



SCENARIO **3**

Installing SonicWALL Secure & Clean Wireless into a Multi-Story or Large Physical-Area Network:

This scenario illustrates a SonicWALL wireless deployment into a network that spans multiple stories or a large physical area in which one access point is unable to provide sufficient coverage. Once deployed the SonicWALL can be configured to manage multiple access points (i.e. SonicPoints and enforce the security services outlined above on all wireless traffic).