SonicWALL Clean Wireless Networking Solutions

High-performance clean wireless networking solutions

- **Comprehensive wireless security**
- **Exceptional wireless performance**
- **Central WLAN management**
- **Enhanced wireless reliability**
- **Flexible wireless deployment options**
- **Virtual Access Point (VAP) segmentation**
- **Broad protocol support**
- **Granular security policy enforcement**

The demands on an organizations' wireless network, more connections, increased bandwidth consumption, seamless roaming, extended perimeters, tax the performance and complicate the management of existing 802.11 wireless networks. The challenge faced by many businesses is to preserve compatibility with legacy 802.11 technologies, while still seeking to optimize their wireless network through centralized management and control across all nodes of the WLAN, and do all this while maintaining security.

The SonicWALL® Clean Wireless solutions integrate 802.11n performance with enterprise-class network security appliances to dramatically simplify wireless network set-up and management delivering unmatched wireless network security and enforcement for any 802.11-based wireless network.

The solution starts with SonicWALL SonicPoint-N Dual-Band access points, which support the IEEE 802.11a/b/g/n standards, to provide secure, faster access to data, voice and video over high-bandwidth wireless LANs. Scalable to networks of any size, SonicPoint-N Dual-Band access points require no pre-configuration, as they are centrally configured and managed by any SonicWALL Network Security Appliance – no additional wireless access controller is required. The seamless integration of wireless access points with best-in-class Unified Threat Management (UTM) security and advanced Application Firewall technology ensures that wireless traffic is scrutinized with the same intensity as wired network traffic. As a result, IT administrators can build and easily manage high-performance, distributed wireless networks with unified policy management across both the wireless and wired networks.

Features and Benefits

Comprehensive wireless security features include Wireless Intrusion Detection Services (WIDS), wireless firewalling, secure Layer 3 wireless roaming, IEEE 802.11d multi-country roaming, and integrated Wireless Guest Services (WGS) to enforce password access for customers and other third-party guests.

Exceptional wireless performance features include 40 MHz channels and packet aggregation to support physical data rates of up to 300 Mbp. Dual-Band supports either operation of 2.4 GHz or 5.0 GHz networks.

Central WLAN management can be administered using any SonicWALL TZ, NSA or E-Class NSA solution, and requires no pre-configuration of the SonicPoint devices.

Enhanced wireless reliability is delivered using Multiple-Input Multiple-Out (MIMO) technology that uses multiple antennas at both the transmitter and the receiver to enhance throughput and reliability.

Flexible wireless deployment options include three external antennas and TNC connectors for external next-generation antennas; wall or ceiling mounting; and 802.3af Power over Ethernet (PoE) for easy deployment where electrical power is not readily accessible.

Virtual Access Point (VAP) segmentation enables up to 8 SSIDs to have dedicated authentication and privacy settings while sharing the same physical infrastructure, providing logical segmentation of secure wireless network traffic and secure customer access.

Broad protocol support includes 802.11/a/b/g, WPA2 and WPA, allowing businesses to leverage prior investments in devices that are incapable of supporting higher encryption standards, while easing migration to 802.11n.

Granular security policy enforcement allows the implementation of firewall rules to all wireless traffic, and controls all wireless client communications to any host on the network—wired or wireless.

SONICWALL

PROTECTION AT THE SPEED OF BUSINESS™

Scenario 1: Small Retail Shop/Medical or Dental Office

Retail, medical or dental businesses can combine SonicPoints-N Dual-Band with SonicWALL network security appliances to quickly extend wireless network access, while providing Unified Threat Management (UTM) scanning of both wired and wireless traffic at the gateway, before allowing access to sensitive resources. SonicWALL Wireless Guest Services (WGS) offers password-enforced customer access to the Internet, while SonicWALL Virtual Access Points (VAPs) provide logical segmentation of secure wireless networks traffic and in-the-clear customer access.

- SonicPoints-N Dual-Band with 802.11n provide faster wireless access with greater range and better reliability

- SonicWALL allows employees to securely access network resources from the wireless network using SSL VPN or WPA2

- Virtual Access Points (VAPs) create secure segmentation between trusted and un-trusted wireless users by allowing broadcast of up to eight unique SSIDs

- SonicWALL UTM scans all wireless traffic for vulnerabilities and threats

- SonicWALL Wireless Guest Services (WGS) allows customers to take advantage of wireless network access

- Provides auto-provisioning and centralized management for all SonicPoints deployed in the network

Retail Deployment

Wireless Guest Services

Secure wireless zone with Reassembly-free Deep Packet Inspection scanning

Comprehensive Gateway Security Suite includes gateway anti-virus, gateway anti-spyware, intrusion prevention, content filtering and 24x7 support.
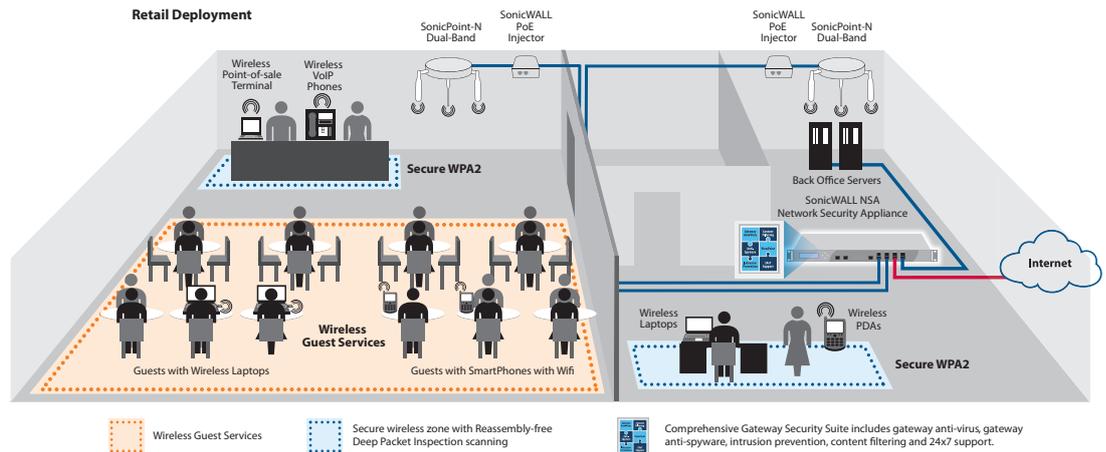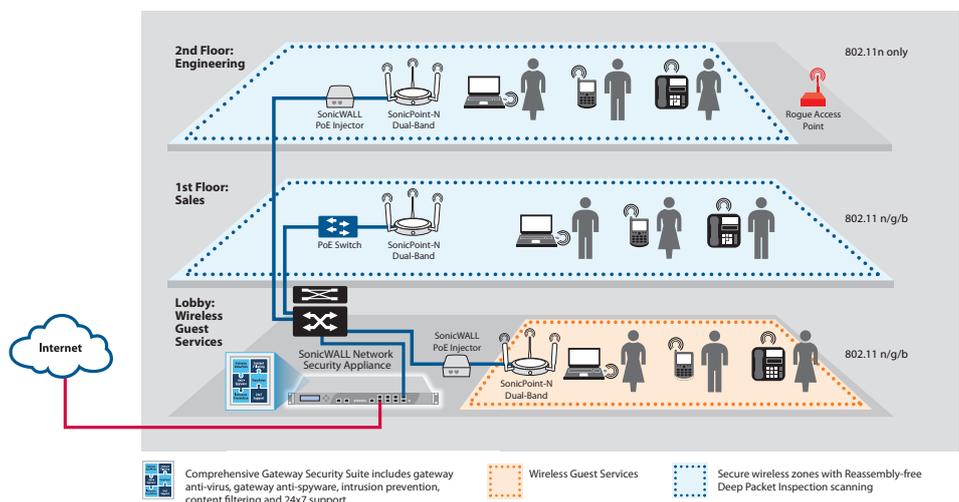
Scenario 2: Clean Wireless Solution

In distributed organizations, SonicPoints-N Dual-Band automatically contact SonicWALL Network Security Appliances (NSAs) to auto-provision the latest firmware and configurations, easing rapid deployment. SonicWALL NSAs offer a single point of wireless monitoring and management, lowering total cost of infrastructure ownership. SonicPoints-N Dual-Band come with built-in wireless Intrusion Detection Systems (IDS) to scan for rogue access points and prevent unauthorized access.

- SonicPoints-N Dual-Band with 802.11n provide faster wireless access with greater range and better reliability

- SonicPoints-N Dual-Band auto-discover the central management gateway, easing deployment

- SonicWALL allows employees to securely access network resources from the wireless network using SSL VPN or WPA2

- SonicWALL UTM comprehensively scans all wireless traffic for vulnerabilities and threats

- Virtual Access Points (VAPs) create secure segmentation between trusted and un-trusted wireless users by allowing broadcast of up to eight unique SSIDs

Enterprise Deployment

Comprehensive Gateway Security Suite includes gateway anti-virus, gateway anti-spyware, intrusion prevention, content filtering and 24x7 support.

Wireless Guest Services

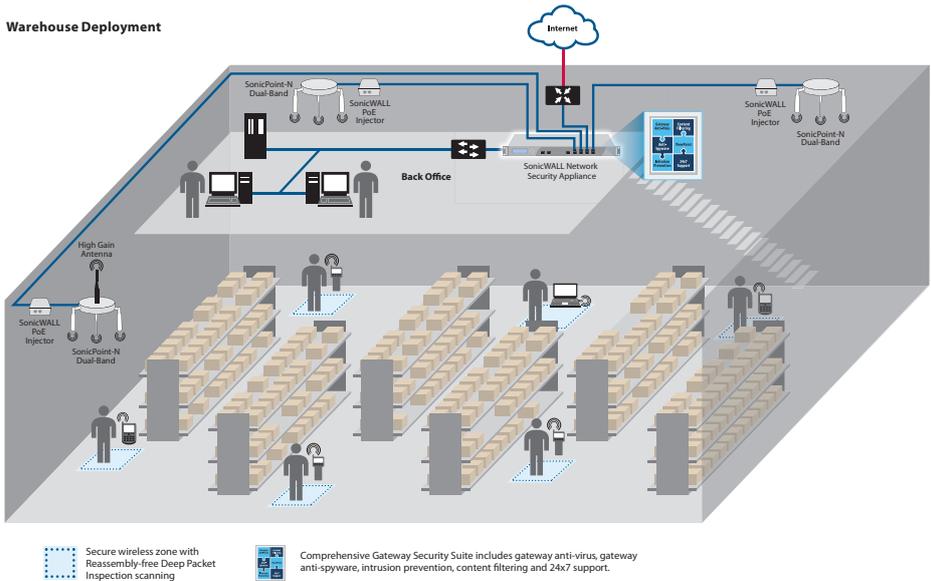Secure wireless zones with Reassembly-free Deep Packet Inspection scanning

Scenario 3: Warehouse Deployment

In warehouse deployments, SonicPoints-N Dual-Band automatically contact a SonicWALL Network Security Appliance (NSA) to auto-provision the latest firmware and configurations, simplifying rapid wireless deployment. SonicWALL NSAs offer a single point of wireless monitoring and management, lowering total cost of infrastructure ownership. SonicPoints-N Dual-Band come with built-in wireless IDS to scan for rogue access points and prevent unauthorized access.

- SonicPoints-N Dual-Band with 802.11n provide faster wireless access with greater range and better reliability

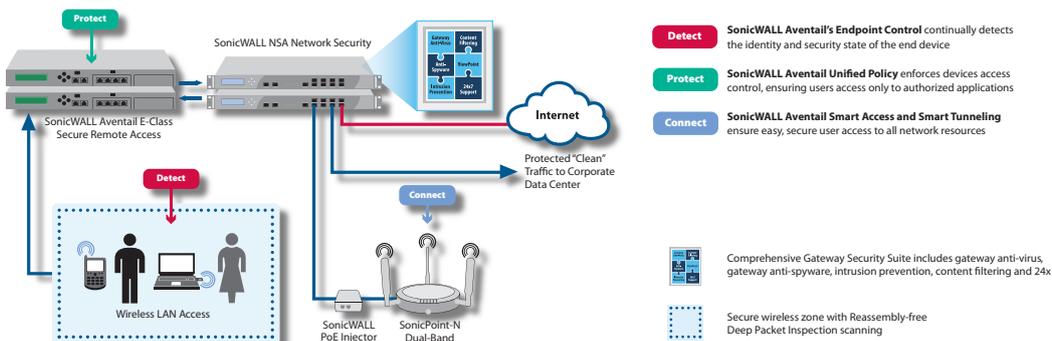- SonicPoints-N Dual-Band auto-discover the central management gateway, easing deployment

- SonicWALL allows employees to securely access network resources from the wireless network using SSL VPN or WPA2

- SonicWALL UTM comprehensively scans all wireless traffic for vulnerabilities and threats

- Virtual Access Points (VAPs) create secure segmentation between trusted and un-trusted wireless users by allowing broadcast of up to eight unique SSIDs

- External TNC Connectors enable third party antennas to boost direction and range of the 802.11 signal

- Provides auto-provisioning and centralized management for all SonicPoints deployed in the network

Warehouse Deployment

Secure wireless zone with Reassembly-free Deep Packet Inspection scanning

Comprehensive Gateway Security Suite includes gateway anti-virus, gateway anti-spyware, intrusion prevention, content filtering and 24x7 support.

Scenario 4: Enterprise Wireless and SonicWALL Aventail E-Class SRA

In distributed wireless environments where there's a need to support additional endpoint security and Network Access Control (NAC), network administrators can deploy SonicPoints-N Dual-Band in conjunction with an E-Class NSA appliance and SonicWALL Aventail E-Class Secure Remote Access (SRA) appliance. The combined solution not only provides distributed wireless connectivity and centralized SonicPoint management, but also provides endpoint enforcement and interrogation ensuring that all wireless users systems have the proper system configuration before gaining access to secure network resources.

- Enforces policy across disparate points of entry, allowing granular access control for collaboration and compliance

- Easy-to-use, providing the core elements of Network Access Control (NAC) today and a foundation for NAC initiatives for the future

- SonicWALL 802.11n solutions provide faster wireless access with greater range and better reliability

- Virtual Access Points (VAPs) create secure segmentation between trusted and un-trusted wireless users by allowing broadcast of up to eight unique SSIDs

- Provides auto-provisioning and centralized management for all SonicPoints deployed in the network

SonicWALL Aventail's Endpoint Control continually detects the identity and security state of the end device

SonicWALL Aventail Unified Policy enforces devices access control, ensuring users access only to authorized applications

SonicWALL Aventail Smart Access and Smart Tunneling ensure easy, secure user access to all network resources

Comprehensive Gateway Security Suite includes gateway anti-virus, gateway anti-spyware, intrusion prevention, content filtering and 24x

Secure wireless zone with Reassembly-free Deep Packet Inspection scanning

Specifications

SonicPoint-N Dual-Band
Bundled with PoE Injector
01-SSC-8571

4-pack SonicPoint-N Dual-Band
without PoE Injector
01-SSC-8572

8-pack SonicPoint-N Dual-Band
without PoE Injector
01-SSC-8573

PoE Injector 802.3af Gigabit N
01-SSC-5544

SonicPoint-N Dual-Band		
Hardware Specifications		
Dimensions	7.5 in (L) x 7.5 in (W) x 1.5 in (H); 19.1 cm (L) x 19.1 cm (W) x 5.8 cm (H)	
Weight	1.25 lbs; .56 kg	
PoE Power Only	802.3af/0.35A	
Status Indicators	Six (6) LED (WLAN, Link/ Act) (LAN, Link/ Act) Power, Wrench	
Antennas	3 Detachable External Antennas, TNC antenna interfaces	
Wired Network Ports	1 10/100/1000 auto-sensing RJ-45 port for Ethernet and Power over Ethernet (PoE) 1 RJ-45 console port	
Mechanical	Wall or ceiling mount kit	
Virtual Access Points	Up to 8 per SonicPoint	
Maximum Managed Devices		
Security Appliance	Per WLAN Interface	Per Appliance
TZ 100/100 Wireless-N	1	1
TZ 200/200 Wireless-N	2	2
TZ 210/210 Wireless-N	16	16
NSA 240/240 Extended License	16	16
NSA 2400	32	32
NSA 3500	48	48
NSA 4500	64	64
NSA 5000	64	64
NSA E5500	96	96
NSA E6500	128	128
NSA E7500	128	128
Standards		
Compliance	IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n draft 2, IEEE 802.11i, IEEE 802.3af, WPA, TKIP,AES	
Regulatory	FCC/ICES CE, C-Tick, RoHS, WEEE	
Safety	UL, cUL, TUV-GS, CB, CE	
Environmental		
Temperature Range	32 to 104°F, 0 to 40°C	
Radio Specifications		
Frequency Band	802.11a, 5.180-5.825GHz; 802.11b/g, 2.412-2.472GHz; 802.11n, 12-2.472Ghz, 5.180-5.825Ghz	
Operating Channel	802.11a, US & Canada 12 , Europe 11, Japan 4, Singapore 4, Taiwan 4 channels 802.11b/g, US & Canada 1-11, Europe 1-13, Japan 14, Spain 2, France 4	
Dynamic Frequency Selection	Not supported	
Transmit Output Power	Based on the regulatory domain specified by the system administrator	
Transmit Power Control	Supported	
Data Rates Supported	802.11a; 6,9,12,18,24,36,48,54 Mbps per channel; 802.11b; 1,2,5.5,11 Mbps per channel; 802.11g; 6,9,12,18,24,36,48,54 Mbps per channel 802.11n; 6,9,12,18,24,36,48,54, 72, 84, 150 300 Mbps per channel	
Modulation Technology	802.11a; Orthogonal Frequency Division Multiplexing (OFDM), BPSK, QPSK, 1-QAM, 64-QAM 802.11b; Direct Sequence Spread Spectrum (DSSS), CCK, DBPSK, DQPSK 802.11g; Orthogonal Frequency Division Multiplexing (OFDM), BPSK, QPSK, 16-QAM, 64-QAM 802.11n; 802.11n draft 2.0	
Security		
Data Encryption	IPSec, 802.11i, WPA; 64/128/152-bit WEP, TKIP, AES, SSL VPN*	
Authentication		
Authentication	RADIUS, Active Directory, Novell e-Directory, SAMBA, Single Sign-on (SSO)	

PoE Injector	
Hardware Specifications	
Number of Ports	2: (1) Data In; (1) Data & Power Out
Dimensions	1.22(H) in x 2.30(W) in x 5.71(D) in; 31(H) mm x 58.5(W) mm x 145(D) mm
Weight	1.0 lbs (450g)
Connectors	Shielded RJ-45, EIA 568A and 568B
Indicators	System Indicator: AC Power (Green); User Indicator: Channel Power Active (Green)
Data Rates	10/100/1000 Mbps
Power over LAN Output	
Pin Assignment and Polarity	4/5 (+), 7/8 (-)TZ 210/210W
Output Power Voltage	-48 VDC
User Port Power	15.4 W minimum
Input Power Requirements	
AC Input Voltage	90 to 264 VAC
AC Frequency	47 to 63 Hz
AC Input Currency	0.5A at 100-240 VAC
Standards and Compliance	
Regulatory Compliance	CE, RoHS, WEEE; Electromagnetic Emission and Immunity; EN 55022, CISPR 22, FCC Part 15, (Class B with FTP cabling); EN 55024, CISPR 24
Safety Approvals	UL 60950-1; EN 60950; IEC 60950-1
Environmental Conditions	
Operating Ambient Temperature	32 to 104 °F, 0 to 40 °C
Operating Humidity	Maximum 90%, non-condensing
Storage Temperature	-4 to 158 °F, -20 to 70 °C
Storage Humidity	Maximum 93%, non-condensing
Operating Altitude	-1,000 to 10,000 ft. (-304.8 to 3,048 m)

*When used with SonicWALL SSL VPN appliance.

For more information on SonicWALL secure wireless networking solutions, please visit **www.sonicwall.com**.

SonicWALL, Inc.

2001 Logic Drive   T +1 408.745.9600   www.sonicwall.com
San Jose, CA 95124   F +1 408.745.9300

SONICWALL®

PROTECTION AT THE SPEED OF BUSINESS™