SonicWall Wireless Network Security

Secure, high-speed wireless solutions

SonicWall Wireless Network Security solutions combine high-performance IEEE 802.11ac wireless technology with industry-leading next-generation firewalls. As a result, they deliver enterprise-class wireless performance and security while dramatically simplifying network setup and management.

The solutions are based on:

- SonicWall SonicPoint AC Series wireless access points (SonicPoint ACe and SonicPoint ACi), which support the 802.11 a/b/g/n/ac standards

- SonicWall TZ, NSA and SuperMassive firewalls, which use deep packet inspection technology to detect and eliminate threats over both wired and wireless networks

Enterprise-level performance

SonicWall SonicPoints take advantage of the latest capabilities in 802.11ac to deliver up to 1.3 Gbps of wireless throughput — three times that of 802.11n. This enterprise-level performance enables WiFi-ready devices to connect from greater distances and use bandwidth-intensive mobile apps, such as video and voice, in higher density environments without experiencing signal degradation.

Built-in dual radios allow the SonicPoint ACe and ACi to dedicate one radio to the less crowded 5 GHz frequency band, ensuring minimal interference and a higher signal quality, while the second radio operates at the 2.4 GHz band to support legacy 802.11b/g/n clients. With multiple antennas at the transmitter and receiver and support for 3x3 MIMO,

SonicPoints are engineered to optimize signal quality, range and reliability.

For organizations with a substantial long-term investment in 802.11n, the SonicWall SonicPoint N2 features an enterprise wireless chipset, dual radios, high-speed performance and all the advantages that SonicWall Wireless Network Security solutions offer.

Comprehensive security

In addition to intrusion prevention, SSL decryption and inspection, application control and content filtering, the Wireless Network Security solution also integrates additional security-related features, including wireless intrusion detection and prevention, virtual access points, wireless guest services, cloud access control list and more.

Easy setup and centralized management

SonicWall Wireless Network Security solutions greatly simplify deployment and setup while reducing total cost of ownership (TCO). Integrated into every SonicWall firewall is a wireless controller that auto-detects and auto-provisions SonicPoints across the network.

Ongoing management and monitoring of SonicPoints and security are handled centrally through the firewall or through the SonicWall Global Management System, providing network administrators with a single pane of glass from which to manage all aspects of the network — both wired and wireless.
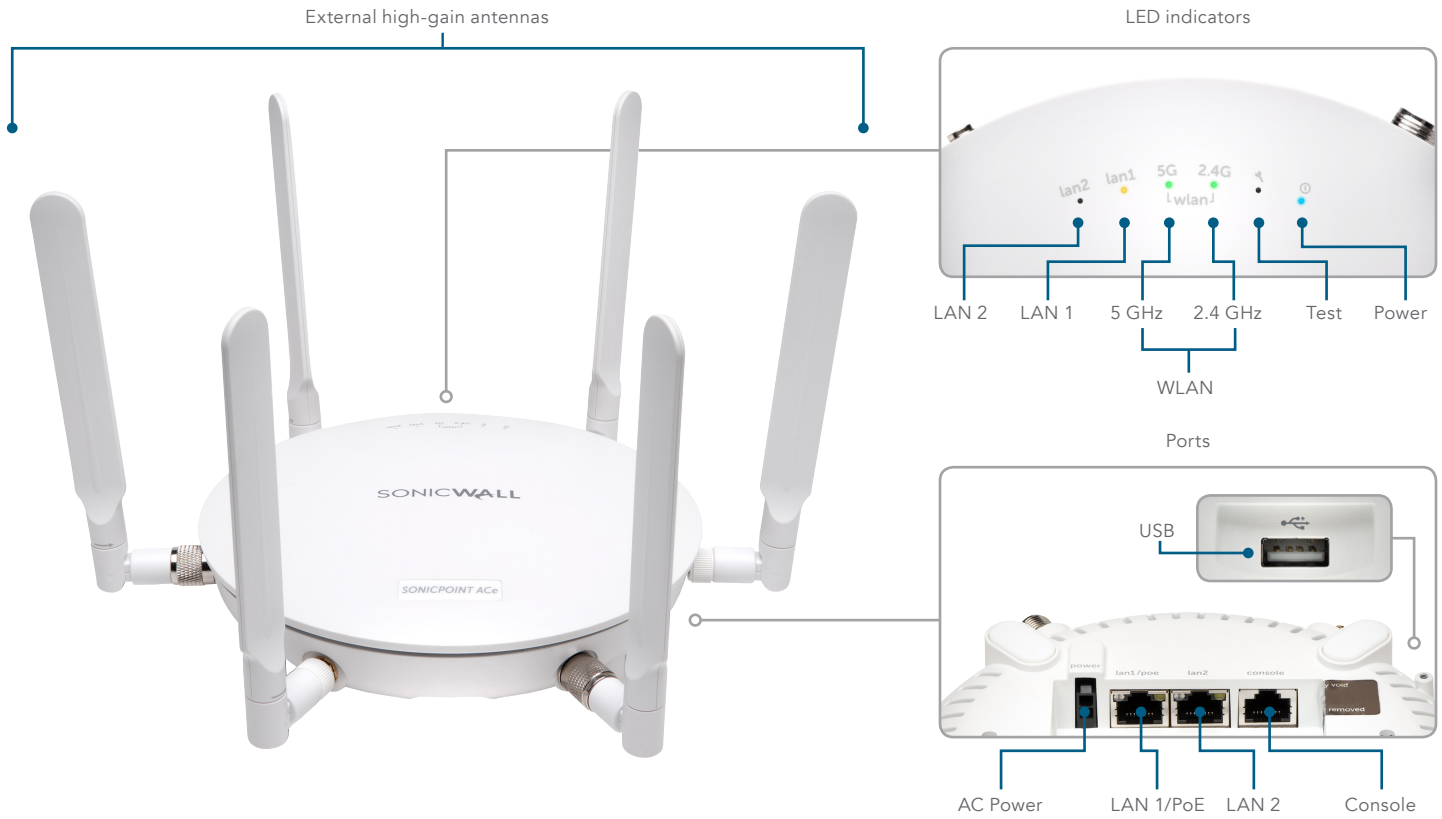

Benefits:

- Superior wireless performance and range
  - Enhanced signal quality
  - Increased wireless reliability
  - FairNet wireless bandwidth allocation
- Comprehensive wireless security
  - Deep packet inspection technology
  - Granular security policy enforcement
  - Virtual access point segmentation
  - Wireless intrusion detection and prevention
  - Cloud access control list
- Easy setup and centralized WLAN management
  - Flexible wireless deployment options
  - Broad standards and protocols support
  - Multiple hardware platforms
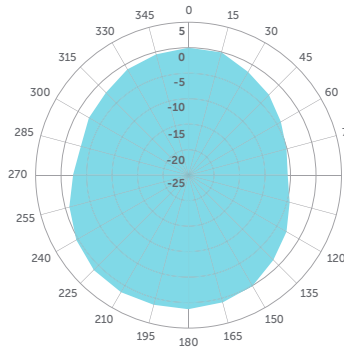- Low total cost of ownership

SonicPoint ACe

External high-gain antennas

LED indicators

lan2 lan1 5G 2.4G
└ wlan ┘

LAN 2   LAN 1   5 GHz   2.4 GHz   Test   Power

WLAN

Ports

USB
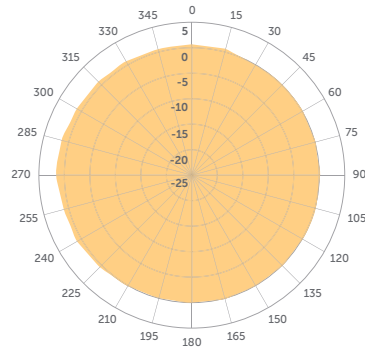
AC Power   LAN 1/PoE   LAN 2   Console
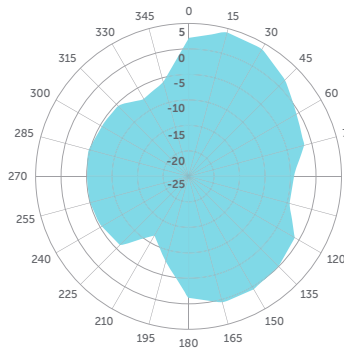
Radio frequency coverage maps

2.4 GHz Vertical

2.4 GHz Horizontal

5 GHz Vertical

5 GHz Horizontal

Vertical plane

Horizontal plane (floor)

SONICWALL®

SonicPoint ACi

Internal antennas

SONICWALL

SONICPOINT ACi

LED indicators

lan2 lan1 5G 2.4G
wlan

LAN 2 | LAN 1 | 5 GHz | 2.4 GHz | Test | Power

WLAN

Ports

USB

lan1/poe lan2 console
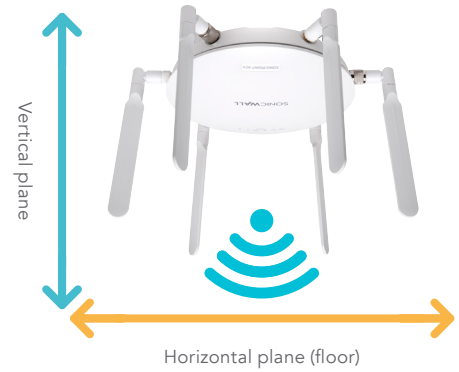
LAN 1/PoE | LAN 2 | Console

Radio frequency coverage maps

2.4 GHz Vertical

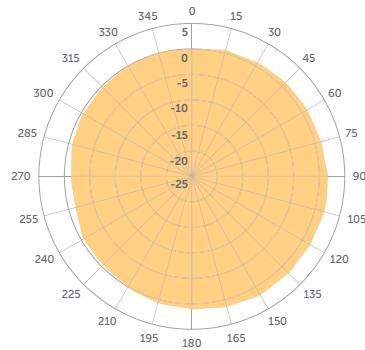2.4 GHz Horizontal

5 GHz Vertical

5 GHz Horizontal

Vertical plane

Horizontal plane (floor)

SONICWALL®

SonicPoint N2

External high-gain antennas

LED indicators

LAN 2   LAN 1   5 GHz   2.4 GHz   Test   Power

WLAN

Ports

USB

LAN 1/PoE   LAN 2   Console

Radio frequency coverage maps
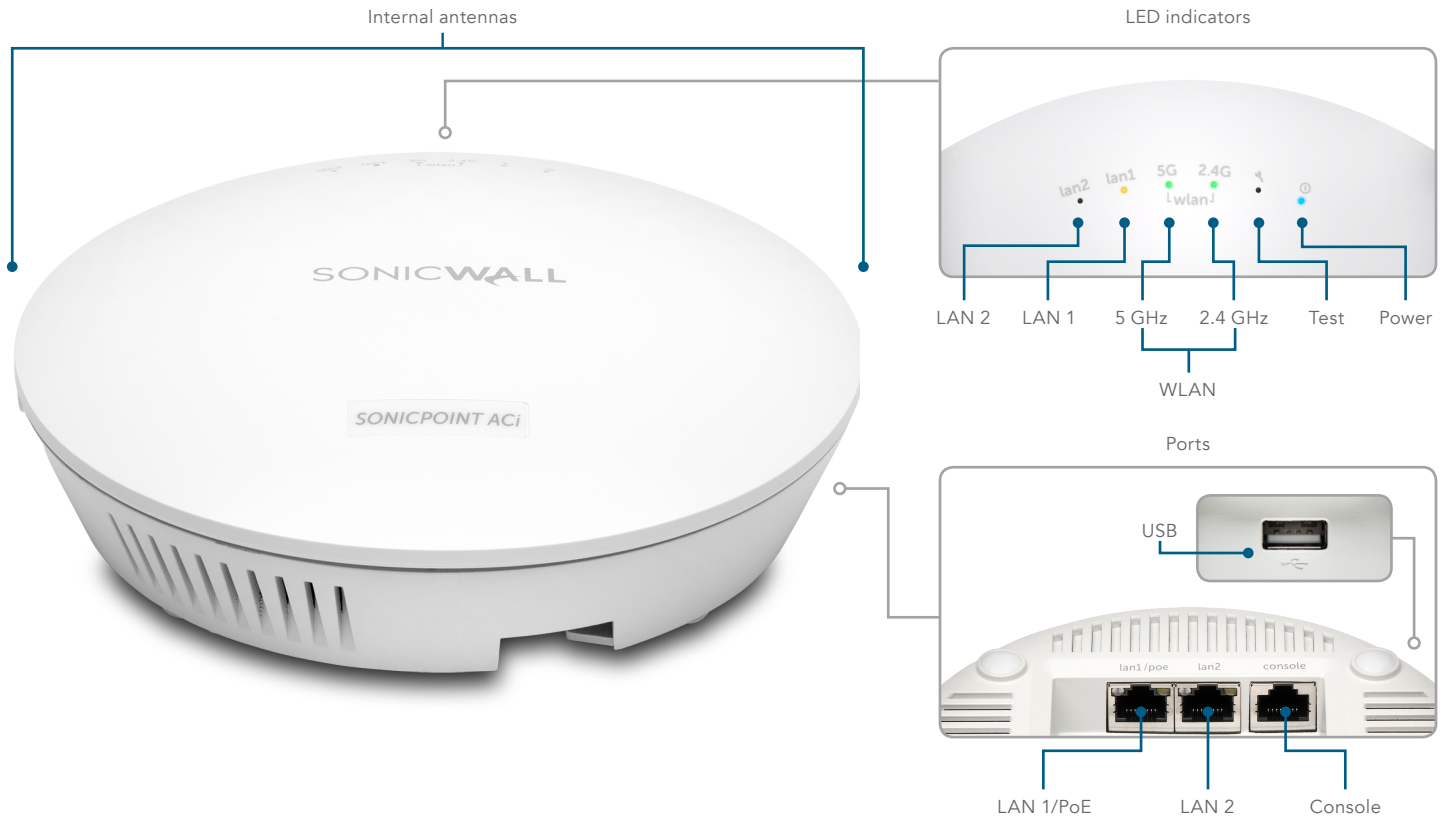
2.4 GHz Vertical
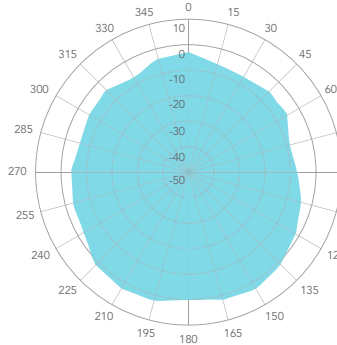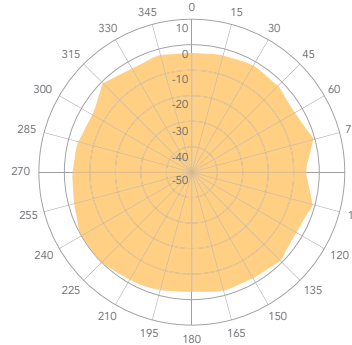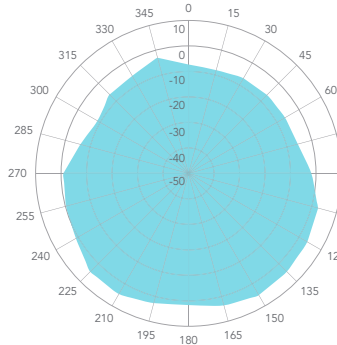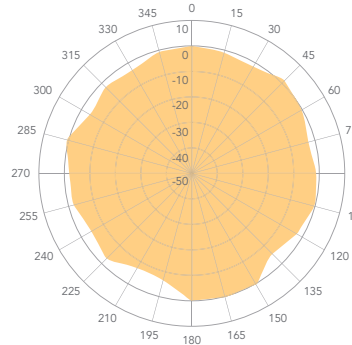
2.4 GHz Horizontal

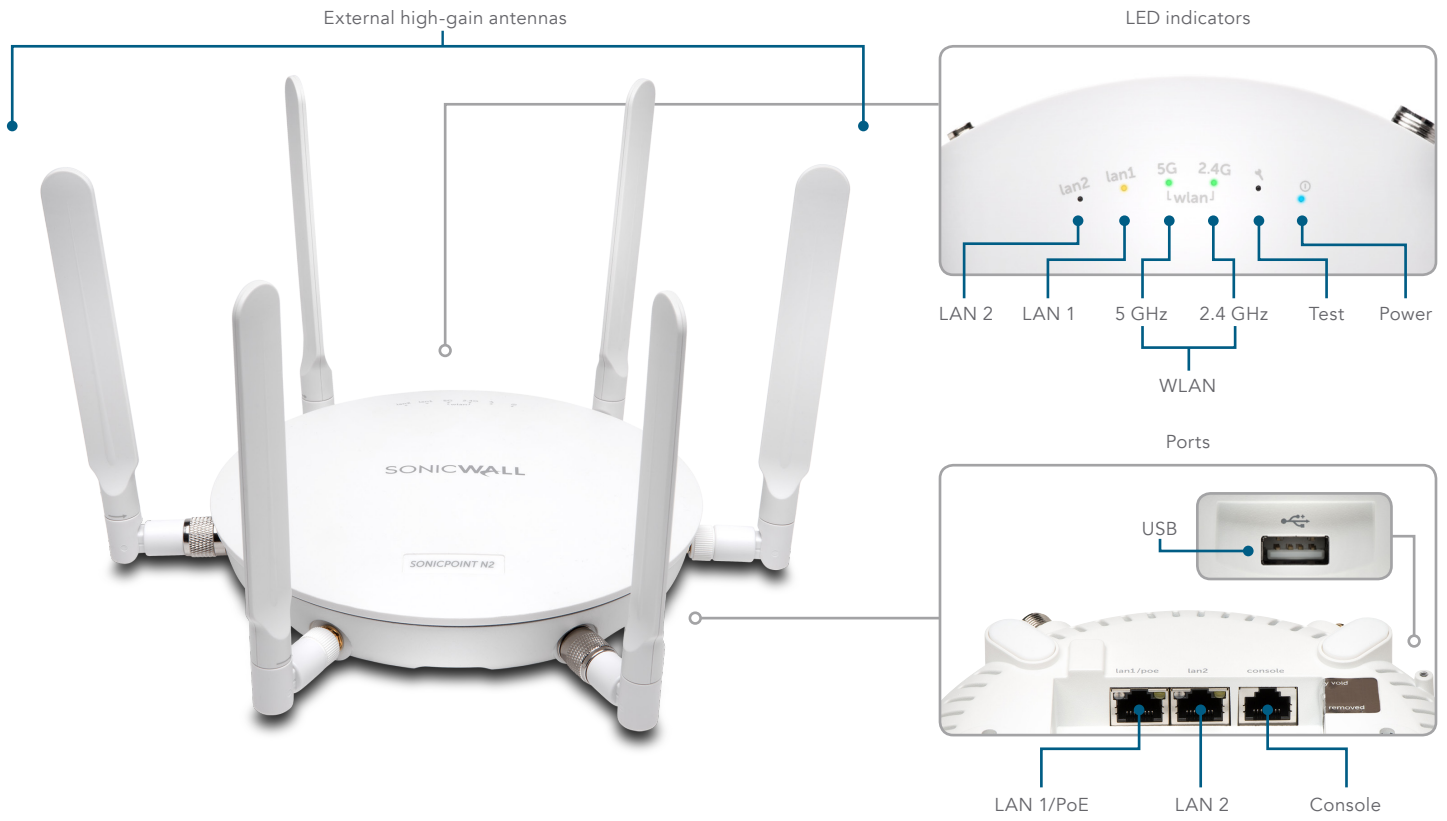5 GHz Vertical

5 GHz Horizontal
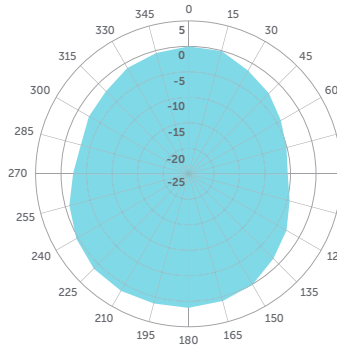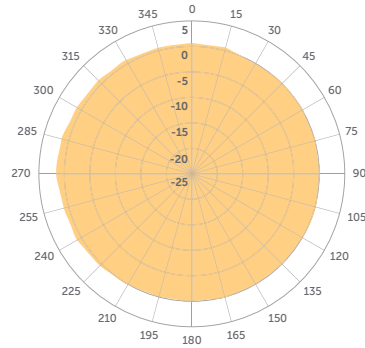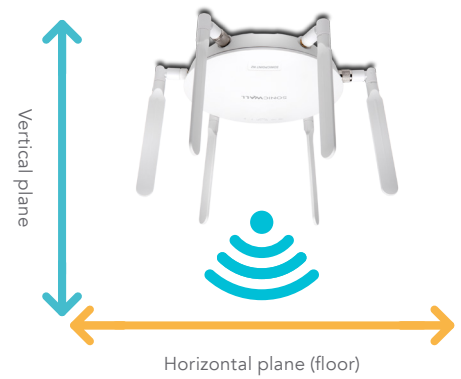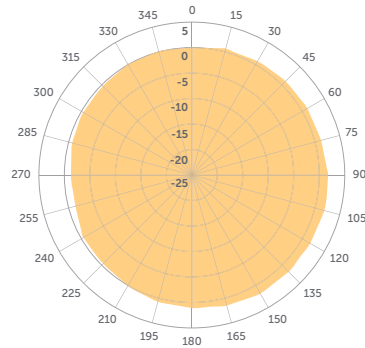
Vertical plane

Horizontal plane (floor)

SONICWALL®

SonicPoint feature summary

Enterprise-level wireless performance, range and reliability	
Feature	**Description**
Superior wireless performance and range	The SonicPoint ACe and SonicPoint ACi are based on the 802.11ac standard, which can achieve a data rate of up to 1.3 Gbps, or 3x that of 802.11n, while maintaining a higher performance level at greater ranges depending on environmental conditions.
Enhanced signal quality	The 802.11ac standard operates in the 5 GHz frequency band, which has fewer wireless devices competing for airspace and is therefore less prone to signal interference. In addition, 802.11ac uses wider 80 MHz channels and has more non-overlapping channels than 802.11n, which operates in the 2.4 GHz frequency band. All of these features combined yield a higher quality signal.
Increased wireless reliability	The increase in bandwidth capacity and greater number of spatial streams combined with 3x3 MIMO and the improved processing offered by 802.11ac, result in more reliable wireless coverage.
FairNet wireless bandwidth allocation	SonicPoints support FairNet, which guarantees a minimum amount of bandwidth to each wireless client in order to prevent disproportionate bandwidth consumption by a single user.
Comprehensive wireless security	
Feature	**Description**
Reassembly-Free Deep Packet Inspection technology	SonicWall next-generation firewalls tightly integrate Reassembly-Free Deep Packet Inspection® (RFDPI) technology to scan all inbound and outbound traffic on wired and wireless networks and eliminate intrusions, spyware, viruses and other threats before they enter the network.
Wireless intrusion detection and prevention	Wireless intrusion detection and prevention scans the wireless network for unauthorized (rogue) access points and then the managing firewall automatically takes countermeasures, such as preventing any connections to the device.
Wireless guest services	Wireless guest services enables administrators to provide internet-only access for guest users. This access is separate from internal access and requires guest users to securely authenticate to a virtual access point before access is granted.
Lightweight hotspot messaging	Lightweight hotspot messaging extends the SonicWall wireless guest services model of differentiated internet access for guest users, enabling extensive customization of the authentication interface and the use of any kind of authentication scheme.
Captive portal	Captive portal forces a user's device to view a page and provide authentication through a web browser before internet access is granted.
Virtual access point segmentation	Administrators can create up to eight SSIDs on the same access point, each with its own dedicated authentication and privacy settings. This provides logical segmentation of secure wireless network traffic and secure customer access.
Cloud ACL	An extension to local ACL, cloud ACL is deployed and managed from a centralized RADIUS server in the cloud. This eliminates local ACL scalability issues, enabling organizations to configure authentication accounts based on their specific requirements. In addition, MAC authentication can be enforced on all WiFi-enabled devices even if they are not capable of 802.1x support. This adds another layer of protection to the wireless network.

SONIC**WALL**®

Comprehensive wireless security con't	
Feature	Description
Multi-RADIUS Authentication	Multi-RADIUS Authentication provides enterprise-class redundancy by enabling organizations to deploy multiple RADIUS servers in active/passive mode for high availability. Should the primary RADIUS server fail, the managing SonicWall firewall discovers the failure and switches to the secondary server, ensuring wireless devices can continue to authenticate. Further, multi-RADIUS authentication can be supported on each virtual access point and configured for WPA-Enterprise, WPA2-Enterprise or WPA2-Auto-Enterprise mode.
Granular security policy enforcement	Network administrators can implement and enforce firewall rules on all wireless traffic and control all wireless client communications to any host on the network — wired or wireless.

Easy setup and flexible, centralized management	
Feature	Description
Simplified setup and centralized management	SonicPoints are automatically detected, provisioned and updated by the wireless controller in the managing SonicWall SuperMassive, NSA or TZ Series firewall. WLAN administration is also handled directly from the managing firewall, simplifying setup and centralizing ongoing management.
Plenum rated	SonicPoints are plenum rated for safe installation in air-handling spaces such as in or above suspended ceilings.
Multiple power options	SonicPoints are powered from a SonicWall IEEE 802.11at Power over Ethernet (PoE) Injector or third-party device for easy deployment where electrical outlets are not readily accessible. The SonicPoint ACe can also be powered directly through an AC adapter.
Light controls	With dimmable LEDs (excluding power), SonicPoints fit perfectly into environments that need discreet wireless coverage.
Broad standards and protocols support	SonicPoints support a wide range of wireless standards and security protocols, including 802.11 a/b/g/n/ac, WPA2 and WPA. This allows organizations to leverage prior investments in devices that are incapable of supporting higher encryption standards while easing migration to 802.11ac.

Low total cost of ownership	
Feature	Description
Low TCO	Features such as simplified deployment, single pane of glass management for both wireless and security, and no need to purchase a separate wireless controller drastically reduce an organization's cost to add wireless into a new or existing network infrastructure.
Green access points	SonicPoints reduce costs by supporting green access points, which enables both radios to enter sleep mode for power saving when no clients are actively connected. The SonicPoint will exit sleep mode once a client attempts to associate with it.
Certified by the Wi-Fi Alliance	SonicPoints are certified by the Wi-Fi Alliance. This validates them as interoperable with a diverse sampling of other certified equipment operating in the same frequency band.

SONIC**WALL**®

Wireless Network Security scenarios

SonicWall Wireless Network Security is the ideal solution for organizations of all sizes and types looking to build a secure, high-speed wireless network. Deploying SonicPoints in combination with a SonicWall next-generation firewall provides enterprise-class wireless performance and security for businesses, schools, hospitals and other organizations.

Small networks — Retail store/medical or dental office deployments

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

SonicWall Wireless Network Security is perfect for small offices, such as retail or point of sale (POS) businesses, school classrooms, medical/dental businesses and banks. By combining SonicPoint ACe and SonicPoint ACi wireless access points with a SonicWall firewall, these organizations can quickly extend wireless network access while providing deep packet inspection for both wired and wireless traffic at the gateway before allowing access to sensitive resources. SonicWall wireless guest services offers password-enforced customer access to the Internet, while virtual access points provide logical segmentation of secure wireless network traffic and in-the-clear customer access.

Features

- SonicPoint ACe and SonicPoint ACi provide gigabit wireless performance with greater signal range and reliability.

- SonicPoint wireless access points are auto-discovered and auto-configured by the central management gateway, easing deployment.

- SonicPoint wireless access points enable employees to securely access network resources from the wireless network using SSL VPN or WPA2.

- Virtual access points create secure segmentation between trusted and un-trusted wireless users by allowing broadcast of up to eight unique SSIDs.

- Deep packet inspection technology detects and eliminates vulnerabilities and threats across all inbound and outbound wireless traffic.

- Key security services, such as application control and content filtering, are enforced over the wired and wireless LANs.

- SonicWall wireless guest services and lightweight hotspot messaging enable organizations to offer customers wireless Internet access from a customized authentication interface.

- SonicPoints allow the dedication of one radio to rogue access detection while the other supports users, helping achieve and maintain regulatory compliance.

SONICWALL®

Wireless Network Security scenarios

SonicWall Wireless Network Security is the ideal solution for organizations of all sizes and types looking to build a secure, high-speed wireless network. Deploying SonicPoints in combination with a SonicWall next-generation firewall provides enterprise-class wireless performance and security for businesses, schools, hospitals and other organizations.

Distributed networks — Enterprise/campus deployments

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

In distributed network environments that have a higher density of client associations, such as businesses with remote and branch offices, college campuses, school districts and healthcare provider networks, SonicPoint wireless access points provide superior wireless signal performance, range and quality. Employees, students and customers can securely access network resources on the wireless network using SSL VPN or WPA2. Using SonicWall GMS, administrators can centrally manage every SonicPoint across the entire network, including creating and enforcing wireless policies, which eliminates the need for a separate wireless controller and reduces the total cost of ownership.
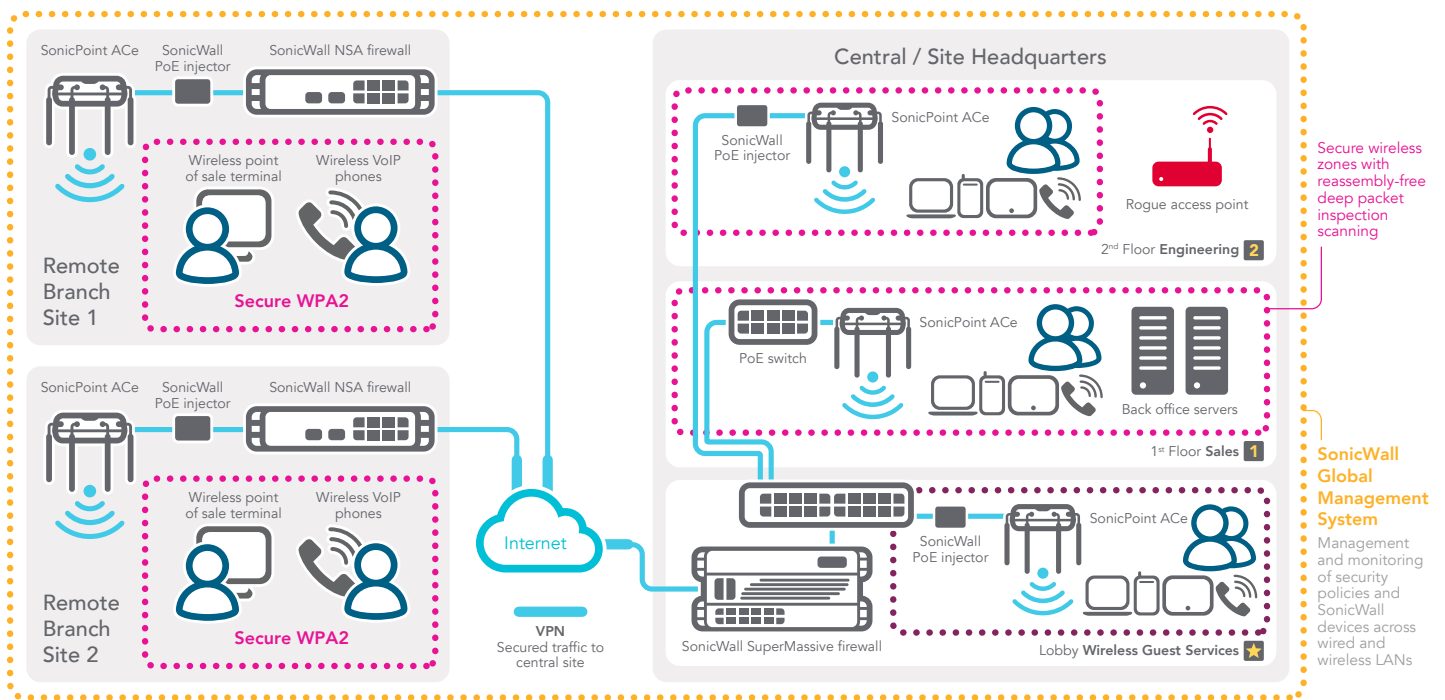
Features

- SonicPoint ACe and SonicPoint ACi provide gigabit wireless performance with greater signal range and reliability.

- SonicPoint wireless access points are auto-discovered and auto-configured by the central management gateway, easing deployment.

- SonicPoint wireless access points enable employees to securely access network resources from the wireless network using SSL VPN or WPA2.

- Virtual access points create secure segmentation between trusted and un-trusted wireless users by allowing broadcast of up to eight unique SSIDs.

- Deep packet inspection technology detects and eliminates vulnerabilities and threats across all inbound and outbound wireless traffic.

- Key security services, such as application control and content filtering, are enforced over the wired and wireless LANs.

- SonicWall wireless guest services and lightweight hotspot messaging enable organizations to offer customers wireless Internet access from a customized authentication interface.

- SonicWall GMS provides central management and monitoring of the wired and wireless LANs, including the firewall and all SonicPoints that are connected to it.

SONIC**WALL**®

Specifications

Hardware Specifications	SonicPoint ACe	SonicPoint ACi	SonicPoint N2
Dimensions	6.9 (D) x 1.5 (H) in 175 (D) x 38 (H) mm	6.7 (D) x 1.5 (H) in 175 (D) x 40 (H) mm	6.9 (D) x 1.5 (H) in 175 (D) x 38 (H) mm
Weight	0.53 kg / 1.2 lbs	0.48 kg / 1.1 lbs	0.53 kg / 1.2 lbs
WEEE weight	1.2 kg / 2.6 lbs	0.53 kg / 1.2 lbs	0.74 kg / 1.6 lbs
Shipping weight	1.74 kg / 3.8 lbs	0.79 kg / 1.8 lbs	1.1 kg / 2.4 lbs
PoE Power requirements	802.3at		
Power supply	802.3at + AC Adapter (12 v)	802.3at PoE	802.3at PoE
Maximum power consumption (W)	15.2 W	15.6 W	13.7 W
Status indicators	Six (6) LED (WLAN/Link) (LAN/Link) Power, Test		
Antennas	3+3 (SMA 2.4 GHz + TNC 5 GHz)	6 fully internal	3+3 (SMA 2.4 GHz + TNC 5 GHz)
Wired network ports	(2) 10/100/1000 auto-sensing RJ-45 for Ethernet and Power over Ethernet (PoE); (1) RJ-45 console; (1) USB 2.0		
Mechanical	Wall or ceiling mount kit		
Virtual access points	Up to 8 per SonicPoint		
Maximum clients supported	256 (128 per radio)		
Chassis	UL 2043 plenum rated		
Standards and compliance			
Compliance	IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11i, IEEE 802.3e, IEEE 802.3i, IEEE 802.3at, WPA/WPA2, TKIP, AES		
Regulatory	FCC/ICES Class B, CE, RCM/ACMA, VCCI Class B, TELEC, BSMI, NCC, MSIP, ANATEL, Customs Union, RoHS (Europe/China), WEEE		
Certifications	WiFi, Dynamic Frequency Selection (DFS)		
Safety	UL, cUL, TUV/GS, CB, CE, BSMI, Mexico CoC, Customs Union		
Environmental			
Temperature range	32 to 104°F, 0 to 40°C		
Humidity	10 - 95%, non-condensing		
Radio specifications			
Radios	Dual: 3x3 11n + 3x3 11ac		Dual: 3x3 11n + 3x3 11n
Frequency bands	802.11a: 5.180-5.825 GHz 802.11b/g: 2.412-2.472 GHz 802.11n: 2.412-2.472 GHz, 5.180-5.825 GHz **802.11ac: 2.412-2.472 GHz, 5.180-5.825 GHz		
Operating channels	802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4 802.11b/g: US and Canada 1-11, Europe 1-13, Japan 1-14 (14-802.11b only) 802.11n (2.4 GHz): US and Canada 1-11, Europe 1-13, Japan 1-13 802.11n (5 GHz): US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64 **802.11ac: US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64		
Transmit output power	Based on the regulatory domain specified by the system administrator		
Transmit power control	Supported		

*When used with SonicWall Secure Remote Access Series appliance
**Available on SonicPoint ACe and SonicPoint ACi only

SonicPoint ACe (includes PoE Injector and 1 year of SonicPoint Support)	01-SSC-0868
4-pack SonicPoint ACe (includes 3 years of SonicPoint Support for each SonicPoint)	01-SSC-0877
8-pack SonicPoint ACe (includes 3 years of SonicPoint Support for each SonicPoint)	01-SSC-0878

SonicPoint ACi (includes PoE Injector and 1 year of SonicPoint Support)	01-SSC-0871
4-pack SonicPoint ACi (includes 3 years of SonicPoint Support for each SonicPoint)	01-SSC-0879
8-pack SonicPoint ACi (includes 3 years of SonicPoint Support for each SonicPoint)	01-SSC-0880

SonicPoint N2 (includes PoE Injector and 1 year of SonicPoint Support)	01-SSC-0874
4-pack SonicPoint N2 (includes 3 years of SonicPoint Support for each SonicPoint)	01-SSC-0881
8-pack SonicPoint N2 (includes 3 years of SonicPoint Support for each SonicPoint)	01-SSC-0882

PoE Injector 802.3at Gigabit AC	01-SSC-0176

Check with your local SonicWall reseller for the specific SonicPoint part numbers in your region.

SONICWALL®

Specifications (continued)

Radio specifications (continued)	
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: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 15, 30, 45, 60, 90, 120, 135, 150 Mbps per channel **802.11ac: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3, 15, 30, 45, 60, 90, 120, 135, 150, 180, 200, 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3, 65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7 Mbps per channel
Modulation technology spectrum	802.11a: Orthogonal Frequency Division Multiplexing (OFDM) 802.11b: Direct Sequence Spread Spectrum (DSSS) 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS) 802.11n: Orthogonal Frequency Division Multiplexing (OFDM) **802.11ac: Orthogonal Frequency Division Multiplexing (OFDM)

Security	
Data encryption	WPA2; 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)

Hardware Specifications	PoE Injector
Number of ports	2: (1) Data In; (1) data and power out
Dimensions	1.22 (H) x 1.97 (W) x 6.30 (L) in; (31 (H) x 50 (W) x 160 (L) mm
Weight	0.5 lbs/(0.3 kg)
WEEE weight	0.85 lbs/(0.38 kg)
Shipping weight	0.87 lbs/(0.4 kg)
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 (-)
Output power voltage	-48 VDC
User port power	30 W minimum

Input power requirements	
AC input voltage	100 to 240 VAC
AC frequency	50 to 60 Hz
AC input current	0.8A at 100-240 VAC

Standards and compliance	
Regulatory compliance	CB, S Mark, RCM, ICES, cUL, CCC, CE, GS, BIS, PSE, MOM, EAC, KCC/MSIP, BSMI, UL, FCC
Electromagnetic emission and immunity	Class B emission level, EN 55022, CISPR 22, FCC Part 15
Safety	IEC/EN/UL 60950-1
Environmental	EU RoHS, China RoHS, EU WEEE, DOE Level VI, MEPS

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 95%, non-condensing
Operating altitude	-1,000 to 10,000 ft. (-304.8 to 3,048 m)

*When used with SonicWall Secure Remote Access Series appliance
**Available on SonicPoint ACe and SonicPoint ACi only

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 global businesses in over 150 countries, so you can do more business with less fear.

SONICWALL®