SonicWave 432o Outdoor Wireless Access-Point

Secure Wireless Solution

Die drahtlosen Access-Points (APs) der SonicWave-Serie von SonicWall kombinieren IEEE 802.11ac Wave 2-Drahtlostechnologie mit flexibler Implementierung. Diese Hochsicherheits-APs können via Cloud mit dem SonicWall Wireless Network Manager (WNM) oder mithilfe der marktführenden Next-Gen-Firewalls von SonicWall verwaltet werden. Das Ergebnis ist eine von der Firewall unabhängige Lösung, die eine bessere Erfahrung für Wi-Fi-Nutzer ermöglicht und genauso sicher ist wie eine Kabelverbindung.

Montageoptionen.
Alle technischen Daten anzeigen »

Outdoor

SonicWave 432o

HIGHLIGHTS

Intuitives Cloud-Management

- Integriertes Switch-Management
- Warnmeldungen und umfangreiche Analysen
- Automatisierte Firmware-Updates
- Integriertes WiFi Planner-Tool
- Einfacher Wechsel zu Firewall-Management

Hoher Benutzerkomfort

- 802.11ac Wave 2
- Automatische Kanalauswahl
- Anwendungskontrolle und -transparenz
- Analyse des HF-Spektrums
- AirTime-Fairness und schnelles Roaming

Ausgezeichnete Wireless-Sicherheit

- Dritte Funkeinheit speziell zur Prüfung von Paketen
- WPA3-Unterstützung
- Capture ATP und Content-Filtering-Service
- Deep Packet Inspection-Technologie

Vollautomatische Implementierung mit der SonicExpress-App

- Einfache Registrierung und Einführung
- Automatische Erkennung und Bereitstellung
- App erhältlich für iOS und Android

Robustes Outdoor-Design

- Robustes Gehäuse mit IP67-Zertifizierung

Mit SonicWall die richtige Lösung für Ihr Unternehmen finden:

sonicwall.com/secure-wireless

DATENBLATT

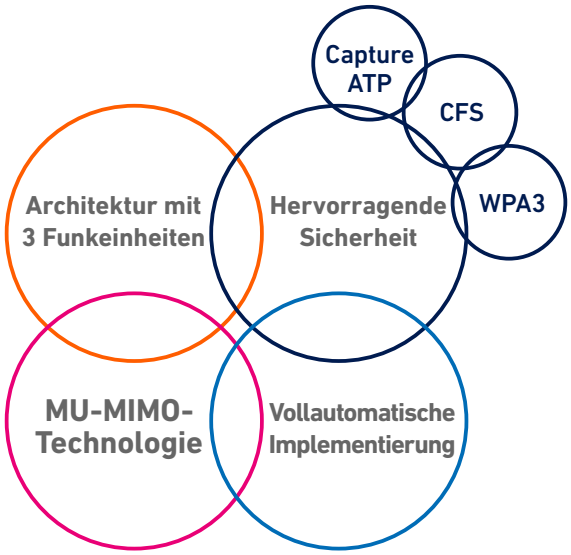
Intuitives Cloud-Management

SonicWall WNM bietet über das SonicWall Capture Security Center (CSC) eine intuitive Benutzeroberfläche für die Verwaltung aller SonicWave-APs von einer zentralen Konsole aus. Zusätzlich ermöglicht das Dashboard mit integriertem SonicWall Switch-Management die zentralisierte Verwaltung der Switches und APs. Mit Warnmeldungen und umfangreichen Echtzeit-Analysen können Sie Netzwerke ganz einfach im Blick behalten und verwalten. Die Features und Firmware werden laufend aktualisiert und verbessert. APs werden automatisch aktualisiert, um manuelle Updates und menschliche Fehler zu vermeiden.

Hoher Benutzerkomfort

Die SonicWave-APs nutzen die Vorteile von 802.11ac Wave 2 und HF-Funktionen, um eine hohe Wireless-Performance sicherzustellen. Mithilfe der MU-MIMO-Technologie können APs zeitgleich mit mehreren Client-Geräten kommunizieren und dadurch die gesamte Netzwerk-Performance, Effizienz und Benutzererfahrung verbessern. Zusätzlich ermöglicht die auf SonicWave 432o-APs unterstützte Mesh-Technologie eine einfache Installation und Implementierung. Mesh-Netzwerke sind leicht in Betrieb zu nehmen, können extrem einfach erweitert werden und benötigen für die Implementierung weniger Kabel und Arbeitsaufwand, wodurch die Installationskosten gesenkt werden.

Mit mehreren Sende- und Empfangsantennen optimieren die SonicWave-APs die Signalqualität, -reichweite und -zuverlässigkeit für drahtlose Geräte. Die SonicWave-APs unterstützen schnelles Roaming, sodass Benutzer nahtlos zwischen verschiedenen Standorten wechseln können. Das funktionsreiche Portfolio umfasst Airtime Fairness, Band-Steering und Signalanalyse-Tools zur Überwachung und Problembehebung.



Ausgezeichnete Wireless-Sicherheit

Die SonicWall-Firewalls scannen den gesamten ein- und ausgehenden drahtlosen Netzwerkverkehr mittels Deep Packet Inspection-Technologie und beseitigen anschließend Bedrohungen wie Malware und Eindringversuche selbst bei SSL-/TLS-verschlüsselten Verbindungen. Weitere Sicherheits- und Kontrollfunktionen wie Content-Filtering, Anwendungskontrolle, Application Intelligence und Capture Advanced Threat Protection (ATP) bieten eine zusätzliche Sicherheitsschicht.

Capture ATP ist unser preisgekrönter Multi-Engine-Sandbox-Dienst mit zum Patent angemeldeter SonicWall Real-Time Deep Memory Inspection (RTDMI™)-Technologie. Die RTDMI-Engine von Capture ATP ist durch eine direkte Prüfung des Speichers in der Lage, massive Zero-Day-Bedrohungen sowie unbekannte Malware proaktiv aufzudecken und abzuwehren. Aufgrund ihrer Echtzeitarchitektur arbeitet die RTDMI-Technologie von SonicWall präzise, reduziert die Anzahl von Falschmeldungen und hilft, ausgeklügelte Angriffe zu identifizieren und abzuwehren, wenn Malware nur für Sekundenbruchteile Schwachstellen zeigt.

SonicWave-APs unabhängig verwalten – auch ohne Firewalls.

Die SonicWave 432o APs beinhalten drei Funkeinheiten, wobei die dritte Funkeinheit für den Bereich Sicherheit ausgelegt ist und passive Scans sowie Prozesse zur Erkennung unberechtigter APs und zur Erfassung von Paketen durchführt. Die SonicWave-Lösung umfasst auch zusätzliche Sicherheitsfeatures wie Erkennung und Vermeidung von Wireless-Angriffen, Segmentierung mithilfe virtueller APs, Wireless Guest Services, HF-Monitoring und Erfassung von Wireless-Paketen.

Einfaches Firewall-Management

Die Implementierung und Einrichtung von APs ist denkbar einfach und trägt dazu bei, die Gesamtbetriebskosten zu verringern. Alternativ können SonicWave-APs auch über SonicWall Next-Gen Firewalls verwaltet werden. Jede SonicWall-Firewall verfügt über einen integrierten Wireless Controller, der SonicWave-APs im gesamten Netzwerk automatisch erkennt und bereitstellt.

Die Verwaltung und Überwachung der Wireless- und Sicherheitssysteme erfolgen zentral über die Firewall. So können Administratoren über eine einzige Konsole alle Aspekte des Netzwerks verwalten.

Vollautomatische Implementierung mit der SonicExpress-App

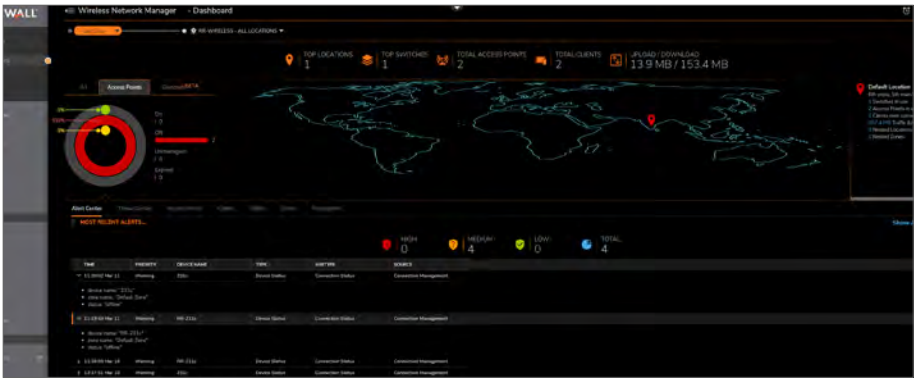
Mithilfe der SonicWall SonicExpress-App können Sie SonicWave-APs ganz einfach registrieren und einführen. Die APs werden mithilfe vollautomatischer Implementierung erkannt und bereitgestellt. Die SonicExpress-App ist für iOS und Android erhältlich und ermöglicht Netzwerkadministratoren die Überwachung und Verwaltung von Netzwerken.

Netzwerkdesign mit WiFi Planner

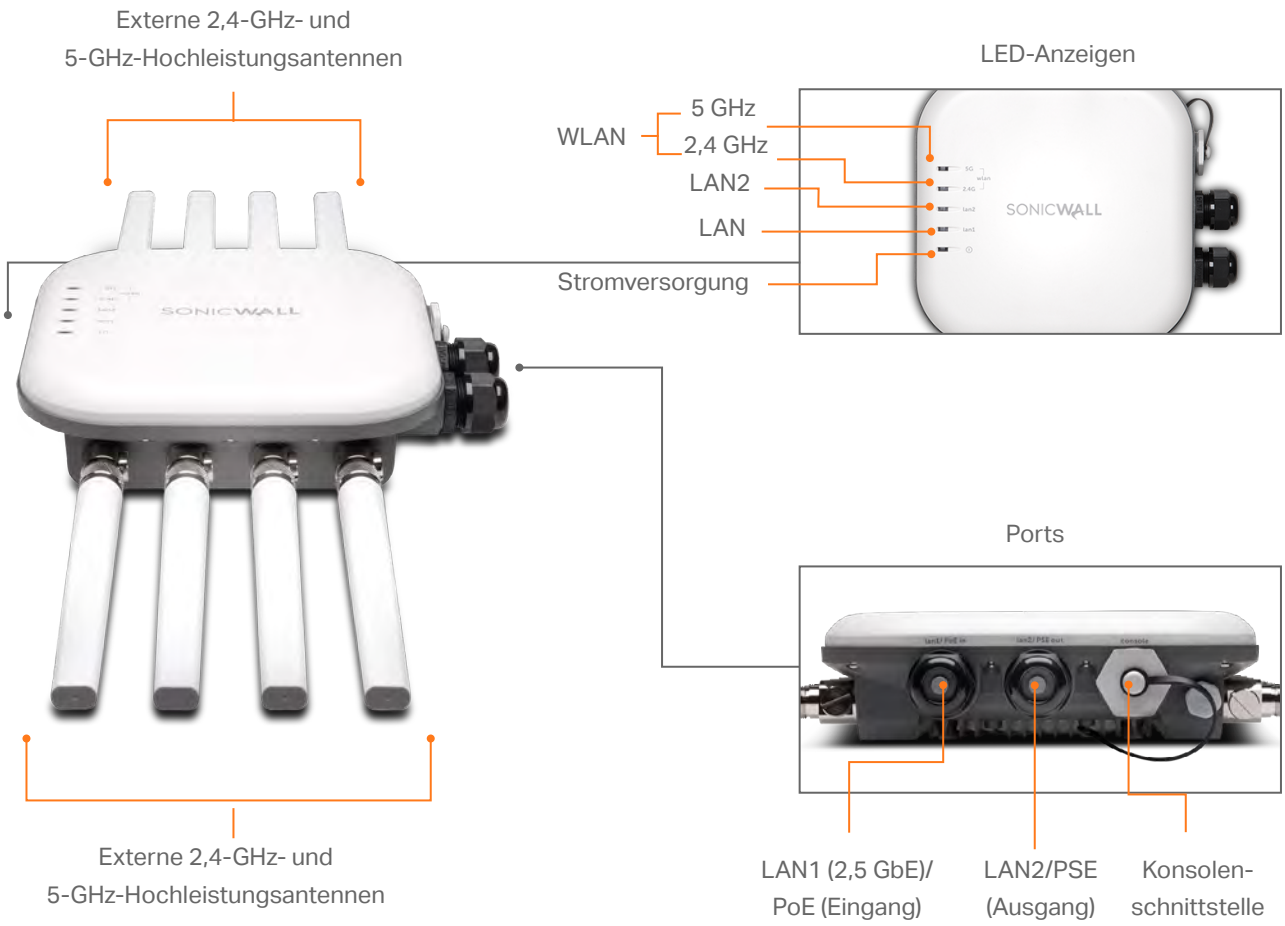
Der SonicWall WiFi-Planner ist ein cloudbasiertes, fortschrittliches Wireless-Site-Survey-Tool. Es ermöglicht ein optimales Design und ein einfache Implementierung von Drahtlosnetzwerken mit hohem Benutzerkomfort.

Robustes Outdoor-Design

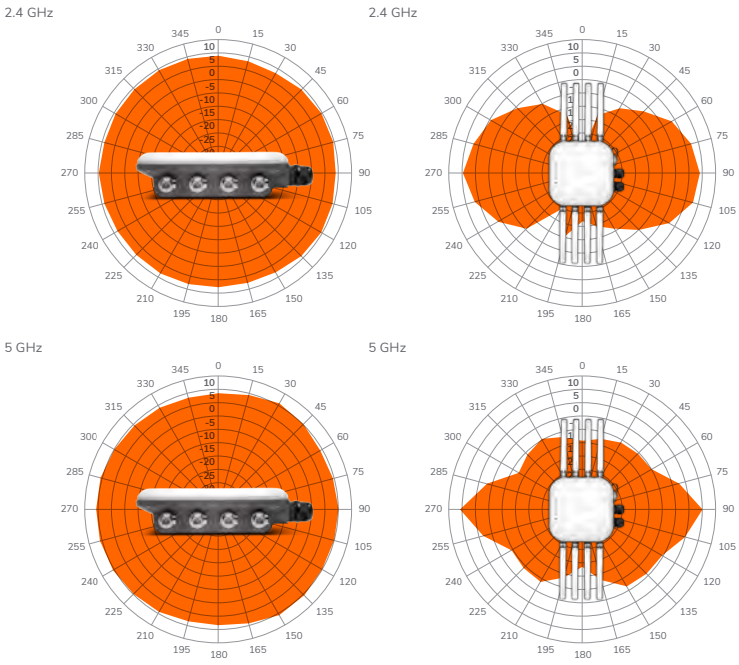
Durch Ihr robustes Gehäuse sind harte Outdoor-Bedingungen kein Problem für SonicWave Outdoor-APs. Diese APs verfügen über die IP67-Zertifizierung und bieten Schutz vor Staub und Wasser.



SonicWave 432o – der Outdoor-AP



Karten mit HF-Abdeckung



SonicWave 400 Series – Systemdaten

HARDWARE	SONICWAVE 432o
Ort	Outdoor
Abmessungen	24,1 (W) x 23,6 (D) x 6,1 (H) cm
Gewicht	2,2 kg
WEEE-Gewicht	4,1 kg
Versandgewicht	4,7 kg
PoE-Injektor	802.3at
Maximaler Stromverbrauch (W)	21,2 W
Statusanzeigen	Sechs (6) LEDs (WLAN/Link) (LAN/Link), Stromversorgung, Test
Antennen	8 Dipolantennen, N-Typ
Netzwerkanschlüsse	(1) 10/100/1000 Autosensing RJ-45 für Ethernet und Power over Ethernet (PoE); (1) 100/1000/2,5-GbE-Autosensing RJ-45 für Ethernet; (1) RJ-45-Konsole
5G/4G/LTE-USB-Modem-Unterstützung	Ja
Im Lieferumfang enthaltenes Zubehör	Masthalter-Set
Virtual Access Points/ SSID-Gruppe	Bis zu 8 pro Access-Point
Gehäuse	UL 1024, feuerfest
Sicherheitsklemme für USB-WAN-Karte	-

STANDARDS UND RICHTLINIEN	SONICWAVE 432o
IEEE-Standards	802.11ac Wave 2, 802.11ac, 802.11n, 802.11g, 802.11b, 802.11a, 802.11e, 802.11i, 802.11r, 802.11k, 802.11v, 802.11w
Compliance	IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11e, IEEE 802.11i, IEEE 802.3at, IEEE 802.3bz, WPA, TKIP, AES, IEEE 802.11r, IEEE 802.11k, IEEE 802.11v, IEEE 802.11w
Zertifizierungs-ID der WiFi Alliance	WFA74189
Richtlinien	FCC/ICES Class B, CE, RCM/ACMA, VCCI Class B, TELEC, BSMI, NCC, MSIP, ANATEL, Customs Union, RoHS (Europa/China), WEEE
Sicherheits-Zertifizierungen	UL E211396, UL 62368-1, UL 60950-1 cUL CAN/CSA C22.2 No. 62368-1-14, CAN/CSA C22.2 No. 62368-1-14, EN 60950-1 oder EN 62368-1, IEC 60950-1, IEC 62368-1, Europa: EN 60950-1, EN 62368-1, Taiwan: CNS 1336-1
Genehmigungen Funkeinheit	USA: FCC Part 15C, 15E, Kanada: ISED RSS-247, Europa: (RED) EN 300 328, EN 301 893, Aus/NZ: AS/NZs 4268, Taiwan: NCC LP002, Zusätzliche Landesgenehmigungen für Japan, Korea, China, Indien, Brasilien
EMI-Genehmigungen	USA: FCC P15B, Kanada: ICES-003, Europa: EN 301 489-1, -17, EN 55032, EN 55024, Aus/NZ: CISPR 32, Japan: VCCI, Taiwan: CNS 13438
Einhaltung der Emissionsgrenzwerte von Funkanlagen	USA: FCC Teil 2, Kanada: RSS-102, Europa: EN 50385, Aus/Nz: ASNZS 2772
MIMO	MU-MIMO 4x4 (4 Streams)
Max./empfohlene Anzahl verbundener Clients pro Funkeinheit	128/48
Sicherheit	UL, cUL, TÜV/GS, CB, CE, BSMI, Mexico CoC, Customs Union
USB WAN Failover und Lastverteilung	-

UMWELTVORSCHRIFTEN	SONICWAVE 432o
Temperaturbereich	-40 bis 60 °C
Luftfeuchtigkeit	10–95 %, nicht kondensierend

FUNKDATEN	SONICWAVE 432o
Funkeinheiten	2: 4x4 11n + 4x4 11ac MU-MIMO; dritte Funkeinheit speziell zur Prüfung von Paketen; Bluetooth-Low-Energy-Funkeinheit
Frequenzbänder	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
Verwendete Kanäle	802.11a: USA und Kanada 12, Europa 11, Japan 4, Singapur 4, Taiwan 4, 802.11b/g: USA und Kanada 1–11, Europa 1–13, Japan 1–14 (Kanal 14 nur nach 802.11b-Standard), 802.11n (2,4 GHz): USA und Kanada 1–11, Europa 1–13, Japan 1–13 802.11n (5 GHz): USA und Kanada 36–48/149–165, Europa 36–48, Japan 36–48, Spanien 36–48/52–64 802.11ac: USA und Kanada 36–48/149–165, Europa 36–48, Japan 36–48, Spanien 36–48/52–64
Sendeleistung	Basierend auf dem vom Systemadministrator angegebenen Geltungsbereich
Steuerung der Sendeleistung	unterstützt
Unterstützte Datenübertragungsraten	802.11a: 6, 9, 12 ,18, 24 ,36, 48, 54 MBit/s pro Kanal, 802.11b: 1,2, 5,5 und 11 MBit/s pro Kanal, 802.11g: 6, 9, 12 ,18, 24 ,36, 48, 54 MBit/s pro Kanal, 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 MBit/s pro Kanal, 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, 1040, 1170, 1300, 1560, 1733,4 MBit/s pro Kanal
Modulationstechnologie/ Frequenzspreizung	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)

SICHERHEIT	SONICWAVE 432o
Datenverschlüsselung	WPA3, WPA2, IPSec, 802.11i, WPA, 64/128/152 Bit WEP, TKIP, AES, SSL VPN**
SSL-VPN Client*	NetExtender, Verbindungstunnel
Erweiterte Security-Services	Capture-ATP, CFS, Geo-IP, Botnet, Antivirus (Cloud)

AUTHENTIFIZIERUNG	SONICWAVE 432o
Authentifizierung	RADIUS, Active Directory, Single-Sign-on (SSO), lokaler Nutzer
Captive Portal	Klick, externer Server, soziale Medien (Facebook, Google, Twitter und LinkedIn), Anmeldung
Anmeldung Captive Portal	Lokale Nutzer, RADIUS, LDAP, OTP, AD

REPORTS	SONICWAVE 432o
Warnmeldungen	Dringende Warnmeldungen per SMS

*SonicWave ist ein SSL-VPN-Client
**Bei Einsatz mit einer SonicWall-Appliance der Secure Mobile Access Series

Die SonicWave-Funktionen im Überblick

ÜBERRAGENDE BENUTZERERFAHRUNG

Funktion	Beschreibung
Highspeed-Wireless-Performance und -Reichweite	Die SonicWave-Access-Points basieren auf dem 802.11ac-Wave-2-Standard, der eine PHY-Rate von bis zu 2,34 GBit/s erreichen kann. Gleichzeitig stellt er je nach Umgebungsbedingungen eine höhere Performance bei größerer Reichweite sicher.
Bessere Signalqualität	Der 802.11ac-Standard ist für das 5-GHz-Frequenzband ausgelegt. Hier ist die Dichte der Wireless-Geräte geringer, weshalb es seltener zu Interferenzen kommt.
Verbesserte Wireless-Zuverlässigkeit	Die verbesserte Bandbreiten-Kapazität und die größere Menge räumlicher Streams in Verbindung mit MU-MIMO und der optimierten Datenverarbeitung durch 802.11ac sorgen für eine zuverlässigere Drahtlos-Netzabdeckung.
MU-MIMO	Die MU-MIMO-Technologie (Multi-User, Multiple-Input, Multiple-Output) ermöglicht eine Übertragung vom Access-Point an mehrere Wireless-Clients gleichzeitig (und nicht nur an einen).
Band-Steering	Durch Band-Steering werden Dual-Band-Clients automatisch mit dem weniger belasteten 5-GHz-Frequenzband verbunden, während das 2,4-GHz-Frequenzband für veraltete Clients verwendet wird. Auf diese Weise wird die Benutzererfahrung deutlich verbessert.
Beamforming	Beamforming verbessert die Wireless-Performance und -Reichweite durch die gezielte Ausrichtung des Funksignals auf einen einzelnen Client, anstatt die Datenübertragung gleichmäßig in alle Richtungen zu verteilen.
AirTime-Fairness	AirTime-Fairness teilt die Übertragungszeit gleichmäßig unter den verbundenen Clients auf und stellt sicher, dass schnellere Clients in derselben Zeit einen höheren Datendurchsatz erreichen als langsamere Clients.
Drahtloses Mesh-Netzwerk	Ein drahtloses Mesh-Netzwerk ermöglicht umgehend eine höhere WiFi-Reichweite ganz ohne Kabel.
FairNet-Wireless-Bandbreitenzuordnung	FairNet garantiert jedem Wireless-Client eine Mindestbandbreite, um zu verhindern, dass einzelne Benutzer überproportional viel Bandbreite beanspruchen.

UMFASSENDE WIRELESS-SICHERHEITSFUNKTIONEN

Funktion	Beschreibung
Reassembly-Free Deep Packet Inspection-Technologie	Die SonicWall-Next-Gen-Firewalls verwenden Reassembly-Free Deep Packet Inspection® (RFDPI)-Technologie zum Scannen des gesamten ein- und ausgehenden Datenverkehrs in allen Netzwerken und blockieren Eindringversuche, Ransomware, Spyware, Viren und andere Bedrohungen vor dem Eintritt ins Netzwerk.
Real-Time Deep Memory Inspection (RTDMI)	Diese zum Patent angemeldete, cloudbasierte Technologie ist in der Lage, Malware, die kein bösartiges Verhalten zeigt oder ihre Mechanismen durch Verschlüsselungsmethoden verschleiert, zu identifizieren und zu blockieren. Die RTDMI-Engine zwingt Malware dazu, ihre Wirkmechanismen im Speicher offenzulegen. So ist sie in der Lage, die in großer Zahl vorkommenden Zero-Day-Bedrohungen sowie unbekannte Malware aufzudecken und abzuwehren.
SSL-/TLS-Entschlüsselung und -Inspektion	Die SonicWall-Firewalls entschlüsseln und prüfen den SSL-/TLS-Verkehr on the fly und ohne Proxy auf Malware, Eindringversuche und Datenlecks. Dabei werden Anwendungs-, URL- und Content-Kontrollregeln angewendet, um das Netzwerk vor Bedrohungen zu schützen, die im SSL-/TLS-verschlüsselten Verkehr lauern.
Dritte Funkeinheit speziell zur Prüfung von Paketen	Die meisten SonicWave-Access-Points umfassen eine spezielle Funkeinheit, die den drahtlosen Datenverkehr kontinuierlich auf unberechtigte Access-Points prüft und zusätzliche Sicherheitsfunktionen bietet, die die Einhaltung der PCI-Compliance fördern.
Erkennung und Vermeidung von Wireless-Angriffen	Bei der Erkennung und Vermeidung von Wireless-Angriffen wird das Drahtlosnetzwerk auf unautorisierte (unberechtigte) Access-Points überprüft. Bei Bedarf leitet die Verwaltungsfirewall automatisch Abwehrmaßnahmen ein, wie z. B. die Unterbindung sämtlicher Verbindungen zum Gerät.
Wireless Guest Services	Mit Wireless Guest Services können Administratoren Gastbenutzern einen Zugriff nur für das Internet gewähren. Dieser Zugriff ist vom internen Zugriff getrennt. Gastbenutzer müssen sich sicher an einem Virtual Access Point authentifizieren, bevor sie einen Zugriff erhalten.
Lightweight Hotspot Messaging	Lightweight Hotspot Messaging erweitert das SonicWall Wireless Guest Services-Modell des differenzierten Internetzugriffs für Gastbenutzer und erlaubt so eine umfassende Personalisierung der Authentifizierungsoberfläche und eine Nutzung beliebiger Authentifizierungsverfahren.
Captive Portal	Captive Portal veranlasst Benutzergeräte dazu, eine Seite aufzurufen und sich über einen Webbrowser zu authentifizieren, bevor ein Internetzugang bereitgestellt wird.
Segmentierung mithilfe virtueller Access-Points	Administratoren können bis zu acht SSIDs auf demselben Access-Point mit eigenen Authentifizierungs- und Datenschutzeinstellungen erstellen. Dies ermöglicht eine logische Segmentierung des sicheren drahtlosen Netzwerkverkehrs und einen sicheren Kundenzugriff.
Cloud-ACL	Als Ergänzung zur lokalen ACL wird eine Cloud-ACL eingesetzt und über einen zentralisierten RADIUS-Server in der Cloud verwaltet. Dies löst Skalierbarkeitsprobleme mit der lokalen ACL und ermöglicht Organisationen die Konfiguration von Authentifizierungskonten basierend auf ihren spezifischen Anforderungen. Zusätzlich kann MAC-Authentifizierung auf allen WiFi-fähigen Geräten durchgeführt werden, selbst wenn diese 802.1x nicht unterstützen. Dies sorgt für eine weitere Schutzschicht für das drahtlose Netzwerk.
Multi-RADIUS-Authentifizierung	Die Multi-RADIUS-Authentifizierung bietet Redundanz der Unternehmensklasse, indem sie Unternehmen eine hohe Verfügbarkeit durch den Einsatz mehrerer RADIUS-Server im Aktiv- bzw Passiv-Modus ermöglicht. Die SonicWall-Verwaltungsfirewall erkennt, wenn der primäre RADIUS-Server ausfällt, und schaltet dann auf den zweiten Server. So wird sichergestellt, dass sich Wireless-Geräte weiterhin authentifizieren können. Außerdem kann die Multi-RADIUS-Authentifizierung auf jedem Virtual-Access-Point unterstützt und für den WPA-Enterprise-, WPA2-Enterprise- oder WPA2-Auto-Enterprise-Modus konfiguriert werden.
Durchsetzung granularer Sicherheitsregeln	Netzwerkadministratoren können Firewall-Regeln auf den gesamten drahtlosen Datenverkehr implementieren und durchsetzen und die drahtlose Client-Kommunikation mit drahtlosen bzw. kabelgebundenen Hosts steuern.

EINFACHE IMPLEMENTIERUNG UND ZENTRALE VERWALTUNG

Funktion	Beschreibung
Einfache Einrichtung und zentrale Verwaltung	Die SonicWave-Access-Points werden automatisch von der Cloud oder durch SonicWall-Next-Gen-Firewalls erkannt, bereitgestellt und aktualisiert. Auch die WLAN-Administration wird direkt von der Verwaltungsfirewall übernommen, was die Einrichtung vereinfacht und die laufende Verwaltung zentralisiert.
Integriertes Switch-Management	Der SonicWall Wireless Network Manager bietet integrierte Steuerung von SonicWave-Access-Points und SonicWall-Switches für einheitliche Netzwerkverwaltung und -transparenz.
WiFi-Planner	Um schon vor der Implementierung eine optimale Positionierung der Access-Points zu ermöglichen, bietet WiFi-Planner eine umfassende Visualisierung des WiFi-Netzwerks, einschließlich Hindernissen, die das Signal stören, sowie abgedeckter und nicht abgedeckter Bereiche.
Floor Plan View	Bei Floor Plan View handelt es sich um ein WiFi-Planungstool, mit dem Benutzer einen Raumplan hochladen oder erstellen und dann SonicWave-Access-Points entsprechend platzieren können, um die erforderliche Funkversorgung sicherzustellen.
Topology View	Topology View ist ein WiFi-Tool, das automatisch Geräte und ihre Vernetzung in der drahtlosen Netzwerkarchitektur abbildet. Dies ist sehr nützlich für die Problembehebung.
Feuerfestigkeit	Die SonicWave-Access-Points sind feuerfest, sodass sie sich sicher in Lüftungskanälen oder innerhalb bzw. oberhalb abgehängter Decken installieren lassen.
Verschiedene Optionen für die Stromversorgung	Die SonicWave-Access-Points werden von SonicWall-PoE-Injektoren (Power over Ethernet) oder Fremdgeräten gespeist, um einen unkomplizierten Einsatz an Stellen zu gewährleisten, an denen Steckdosen schwer zugänglich sind.
Lichtsteuerung	Mit dimmbaren LEDs (außer Betriebsanzeige) eignen sich die SonicPoints perfekt für Umgebungen, in denen eine diskrete Wireless-Abdeckung erwünscht ist.
Umfassende Unterstützung von Standards und Protokollen	Die SonicWave-Access-Points unterstützen eine große Bandbreite an Wireless-Standards und Sicherheitsprotokollen, einschließlich 802.11 a/b/g/n/ac, WPA2 und WPA. Auf diese Weise können Organisationen Geräte, die keine höheren Verschlüsselungsstandards unterstützen, weiterhin nutzen.

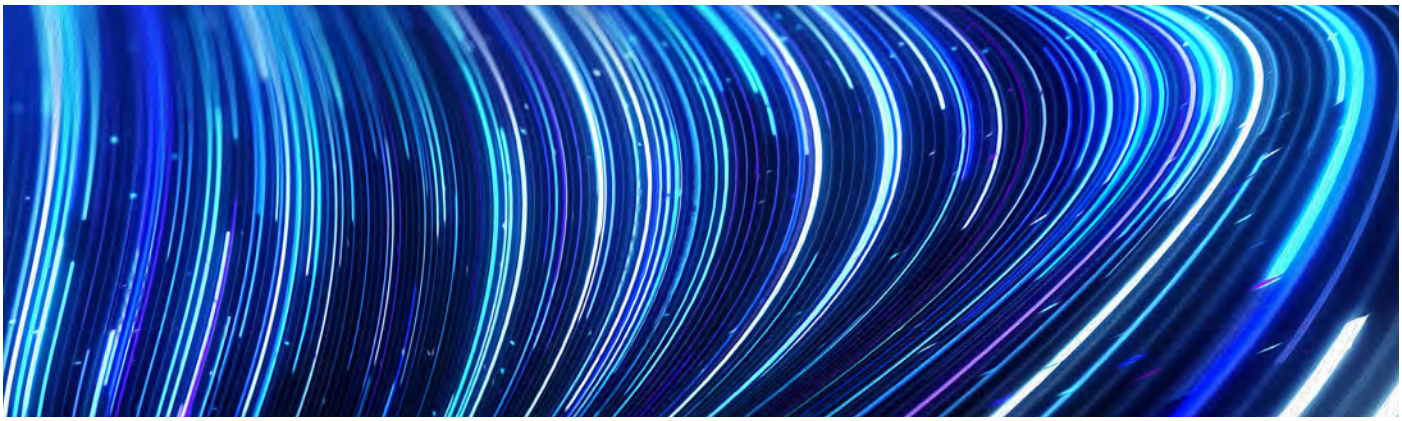
GERINGE TOTAL COST OF OWNERSHIP

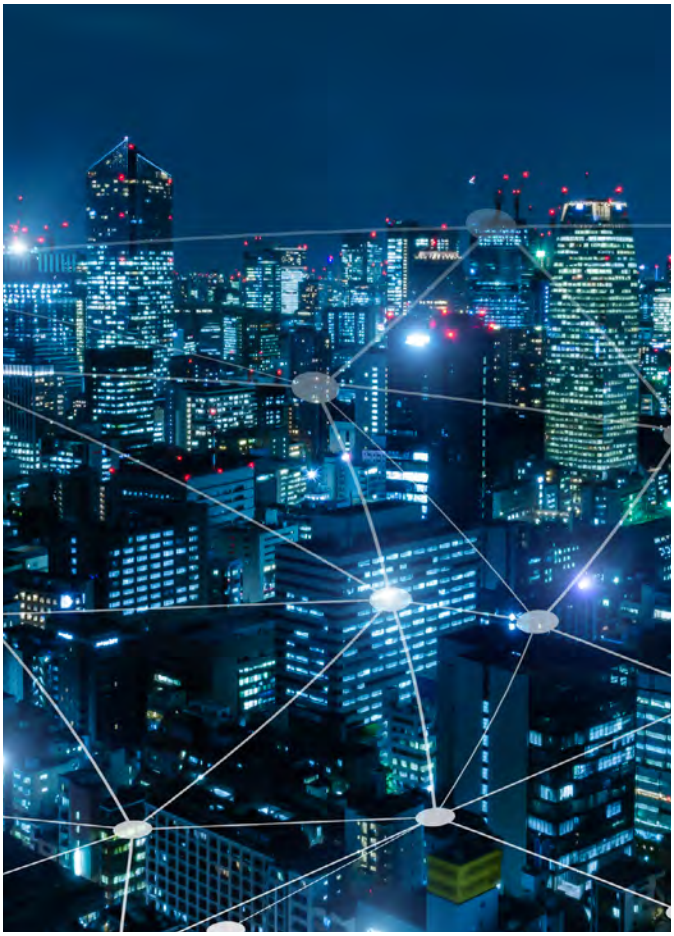
Funktion	Beschreibung
Niedrige TCO	Die Lösung kommt ohne separate Wireless Controller aus, lässt sich einfach implementieren und ermöglicht die Verwaltung von Wireless- und Sicherheitsfunktionen über eine einzige Konsole. Dies reduziert die Kosten für die Implementierung einer Wireless-Lösung in eine neue oder bestehende Netzwerkinfrastruktur um ein Vielfaches.
MiFi-Extender	MiFi-Extender ermöglicht die Anbindung eines 3G-/4G-/LTE-Modems an einen SonicWave-Access-Point und kann entweder als primäres WAN oder als sekundäres Failover-WAN eingesetzt werden, um die Business-Continuity sicherzustellen.
Bluetooth Low Energy	Die SonicWave-Access-Points umfassen eine Bluetooth-Low-Energy-Funkeinheit für die Nutzung von ISM-Anwendungen (ISM = industrial, scientific and medical) für Healthcare, Fitness, Beacons für den Einzelhandel, Sicherheit und Home-Entertainment über eine Bluetooth-Verbindung, die wenig Strom verbraucht.
USB-Ports	Access-Points mit USB-Port unterstützen 3G/4G-Failover. Bei Ausfall des WiFi-Netzwerks wird ein Dongle an den Port angeschlossen, um die Mobilfunkverbindung im Netzwerk herzustellen.
Green Access-Points	Die SonicWave-Access-Points unterstützen sogenannte Green Access-Points. Diese sorgen dafür, dass beide Funkeinheiten in den Sleep-Modus schalten, wenn keine Clients aktiv verbunden sind. So kann man Strom sparen und gleichzeitig auch die Kosten reduzieren. Der Access-Point beendet den Sleep-Modus, sobald ein Client versucht, eine Verbindung aufzubauen.

Für mehr Informationen zu älteren SonicPoint-APs hier klicken.

MODELLNUMMERN (ZULASSUNG)

432o	APL42-0C1





PARTNER ENABLED SERVICES

Brauchen Sie Hilfe bei der Planung, Implementierung oder Optimierung Ihrer SonicWall-Lösung? Die SonicWall Advanced Services Partners sind darauf spezialisiert, Ihre Anforderungen mit erstklassigen Lösungen zu erfüllen. Weitere Informationen:

www.sonicwall.com/PES

Unsere sichere Wireless-Lösung können Sie hier testen:

www.sonicwall.com/products/secure-wireless/live-demo

Über SonicWall

SonicWall bietet grenzenlose Cybersicherheit in einer extrem dezentralen Arbeitswelt, in der jeder remote, mobil und potenziell gefährdet ist. Durch die Identifizierung unbekannter Bedrohungen, moderne Echtzeit-Überwachungsfunktionen und eine herausragende Wirtschaftlichkeit hilft SonicWall Unternehmen, Behörden und KMUs weltweit, die Cybersicherheitslücke zu schließen. Weitere Informationen erhalten Sie unter www.sonicwall.de.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

SONICWALL

Datasheet-SonicWave-US-JK-6931