Access Point wireless SonicWave 432o per esterni

Soluzione wireless sicura

Gli access point (AP) wireless della serie SonicWall SonicWave combinano la tecnologia wireless ad alte prestazioni IEEE 802.11ac Wave 2 con opzioni di implementazione flessibili. Questi punti di accesso altamente sicuri possono essere gestiti via cloud con SonicWall Wireless Network Manager (WNM) o tramite i firewall di nuova generazione leader di settore di SonicWall. Si ottiene così una soluzione che può funzionare indipendentemente dal firewall, offrendo agli utenti Wi-Fi un'esperienza d'uso superiore e con lo stesso livello di sicurezza di una connessione cablata.

CARATTERISTICHE PRINCIPALI

Gestione intuitiva tramite cloud

- Gestione switch integrata
- Avvisi e analisi dettagliate
- Aggiornamento automatico del firmware
- Tool WiFi Planner integrato
- Semplice passaggio alla gestione via firewall

Esperienza d'uso migliore

- 802.11ac Wave 2
- Selezione automatica del canale
- Controllo e visibilità delle applicazioni
- Analisi dello spettro RF
- AirTime Fairness e fast roaming

Sicurezza wireless migliore della categoria

- Terza radio dedicata alla scansione
- Supporto WPA3
- Capture ATP e servizio di filtraggio dei contenuti
- Tecnologia Deep Packet Inspection

Implementazione zero-touch con l'app mobile SonicExpress

- Semplicità di registrazione e connessione
- Rilevamento e provisioning automatici
- App disponibile per iOS e Android

Design robusto per esterni

- Grado di protezione IP67, custodia industriale

Opzioni d'installazione. Specifiche complete »

In Esterno

SonicWave 432o

Trovate la soluzione SonicWall giusta per la vostra piccola azienda o filiale:

sonicwall.com/secure-wireless

SCHEDA TECNICA

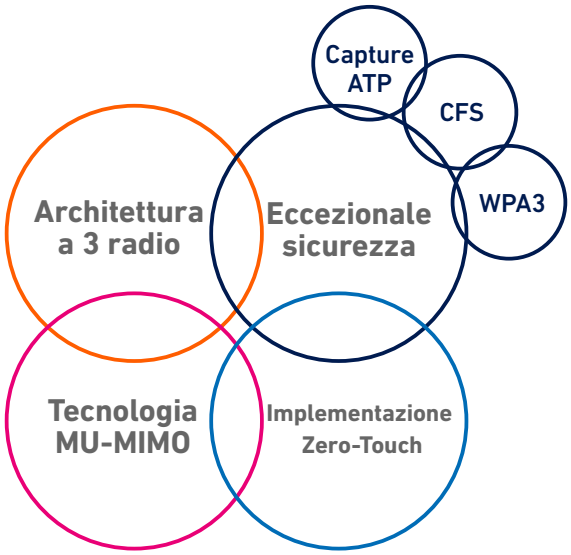
Gestione intuitiva tramite cloud

SonicWall WNM offre un'intuitiva interfaccia utente per gestire tutti gli access point (AP) SonicWave da un unico pannello di controllo tramite SonicWall Capture Security Center (CSC). Inoltre, mediante il dashboard integrato è possibile gestire centralmente tutti gli AP e gli switch SonicWall, per monitorare e controllare facilmente le reti tramite avvisi e analisi dettagliate, aggiornate in tempo reale. Gli aggiornamenti vengono inviati automaticamente agli AP in modo da disporre sempre delle funzionalità e delle migliorie del firmware più recente, eliminando la necessità di aggiornamenti manuali e possibili errori umani.

Esperienza d'uso migliore

Gli AP SonicWave sfruttano le funzionalità offerte dallo standard 802.11ac Wave 2 e caratteristiche RF avanzate per fornire prestazioni wireless ad alta velocità. La tecnologia MU-MIMO consente agli AP di comunicare con più dispositivi client contemporaneamente, migliorando le prestazioni generali della rete, l'efficienza e l'esperienza d'uso. Inoltre, la tecnologia mesh supportata dagli access point SonicWave 432o semplifica l'installazione e l'implementazione. Le reti mesh sono semplici da configurare e da ampliare, e richiedono meno cavi e meno personale, riducendo i costi di installazione.

Grazie a diverse antenne di trasmissione e di ricezione, gli AP SonicWave consentono di ottimizzare la qualità del segnale, la portata e l'affidabilità per i dispositivi wireless. Gli AP SonicWave supportano il fast roaming, che permette agli utenti di spostarsi agevolmente da un luogo all'altro senza perdere la connessione. L'ampia gamma di funzionalità include air-time fairness, band steering e strumenti di analisi del segnale per il monitoraggio e la risoluzione di problemi.



Sicurezza wireless migliore della categoria

I firewall SonicWall eseguono la scansione di tutto il traffico wireless in entrata e in uscita sulla rete tramite la tecnologia Deep Packet Inspection ed eliminano le minacce pericolose, come il malware e le intrusioni, anche su connessioni crittografate con SSL/TLS. Altre funzionalità di sicurezza e controllo come Content Filtering, Application Control and Intelligence e Capture ATP (Advanced Threat Protection), offrono ulteriori livelli di protezione.

Capture ATP è il nostro pluripremiato servizio di sandboxing multi-engine dotato della tecnologia Real-Time Deep Memory Inspection (RTDMI™) in attesa di brevetto di SonicWall. Il motore RTDMI di Capture ATP rileva e blocca in modo proattivo le minacce di massa, le minacce zero-day e i malware sconosciuti mediante l'analisi diretta della memoria. Grazie all'architettura in tempo reale, la tecnologia RTDMI di SonicWall è precisa, riduce al minimo i falsi positivi e identifica e mitiga gli attacchi sofisticati in cui i meccanismi di attacco del malware sono esposti per meno di 100 nanosecondi.

Gli AP SonicWave sono gestibili in modo autonomo, anche senza firewall.

Gli AP SonicWave 432o includono tre radio, di cui la terza è dedicata alla sicurezza e provvede al rilevamento di punti di accesso non autorizzati, alla scansione passiva e all'acquisizione dei pacchetti. La soluzione SonicWave integra ulteriori funzionalità relative alla sicurezza tra cui il rilevamento e la prevenzione di intrusioni wireless, la segmentazione degli AP virtuali, servizi guest wireless, il monitoraggio RF e l'acquisizione di pacchetti wireless.

Gestione semplificata tramite firewall

L'implementazione e la configurazione degli AP sono notevolmente semplificate, riducendo così il costo totale di proprietà. In via opzionale, gli AP SonicWave possono essere gestiti dai firewall SonicWall di nuova generazione. In ogni firewall SonicWall è integrato un controller wireless per il rilevamento e il provisioning automatici degli AP SonicWave sull'intera rete.

La gestione e il monitoraggio della connettività wireless e della sicurezza avvengono a livello centrale attraverso il firewall, fornendo agli amministratori di rete un unico pannello di controllo da cui gestire tutti gli aspetti della rete.

Implementazione zero-touch (ZTD) con l'app SonicExpress

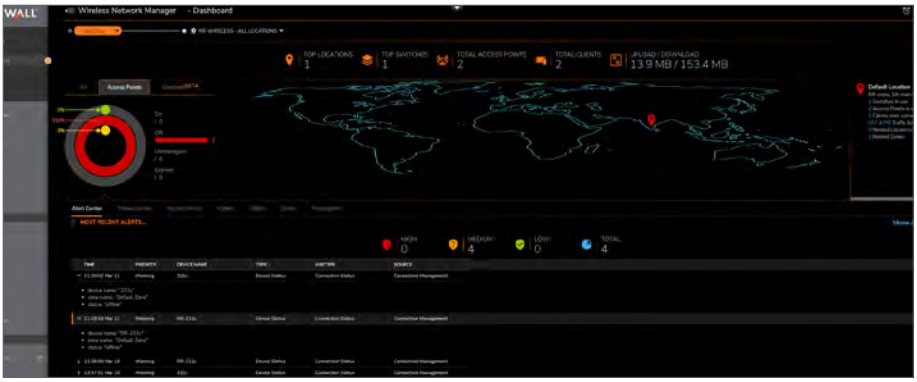
Gli access point (AP) SonicWave possono essere facilmente registrati e connessi mediante l'app SonicWall SonicExpress. Gli AP vengono automaticamente rilevati e configurati con l'implementazione zero-touch. L'app SonicExpress, disponibile per iOS e Android, consente agli amministratori di monitorare e gestire le reti da dispositivi mobili.

Configurazione con WiFi Planner

WiFi Planner di SonicWall è un tool avanzato di analisi wireless del sito, basato su cloud, che consente di progettare e implementare in modo ottimale una rete wireless per offrire agli utenti un'esperienza wireless migliore.

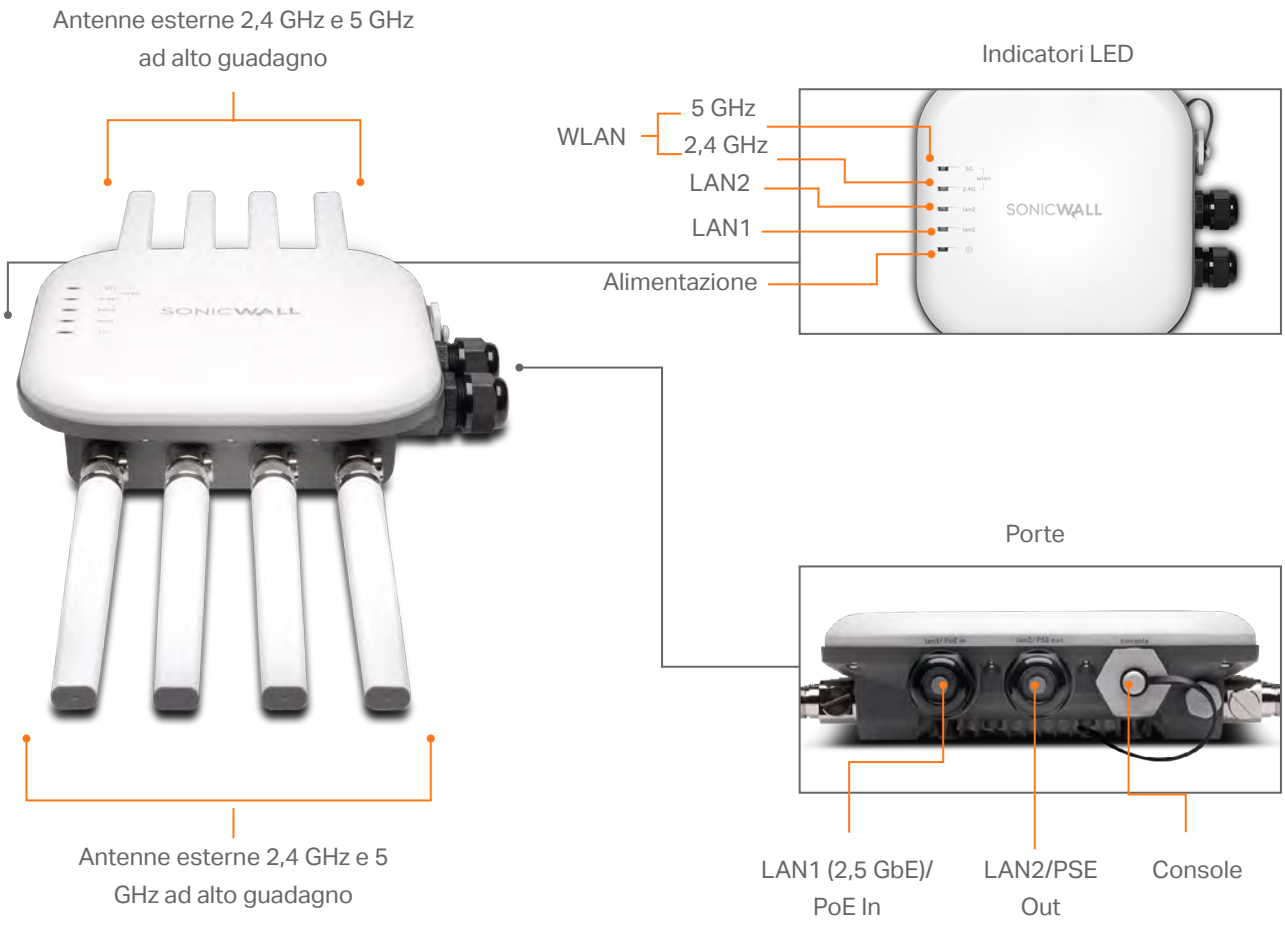
Design robusto per esterni

Gli AP SonicWave per esterni sono creati per resistere a condizioni esterne complesse grazie alla custodia di livello industriale. Questi AP dispongono del grado di protezione IP67, che assicura la protezione dalla polvere e dall'immersione in acqua.

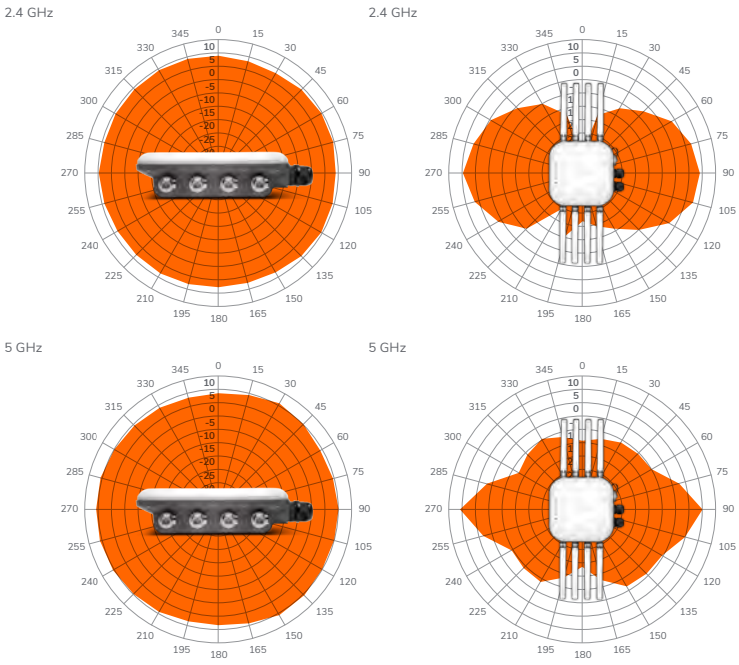


SONICWALL

SonicWave 432o - Access point per esterni



Mappe di copertura RF



Specifiche della serie SonicWave 400

SPECIFICHE HARDWARE	SONICWAVE 432o
Posizione	All'aperto
Dimensioni	24,1 (L) x 23,6 (P) x 6,1 (H) cm 9,5 (L) x 9,3 (P) x 2,4 (H) in
Peso	2,2 kg / 4,9 lbs
Peso RAEE	4,1 kg / 9,1 lbs
Peso con la confezione	4,7 kg / 10,4 lbs
PoE Injector	802.3at
Potenza max. assorbita (W)	21,2 W
Indicatori di stato	Sei (6) LED (WLAN/Link) (LAN/Link) Power, Test
Antenne	8 dipolo tipo N
Porte rete cablata	(1) 10/100/1000 auto-sensing RJ-45 per Ethernet e Power over Ethernet (PoE); (1) 100/1000/2.5 GbE auto-sensing RJ-45 per Ethernet; (1) console RJ-45
Supporto modem USB 5G/4G/ LTE	Sì
Accessori inclusi	Kit di montaggio a palo
Punti di accesso virtuali/gruppo SSID	Fino a 8 per ciascun access point
Chassis	Certificazione Plenum UL 1024
Clip di sicurezza per schede USB WAN	N/D

STANDARD E CONFORMITÀ	SONICWAVE 432o
Standard IEEE	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
Conformità	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
ID certificazione Wi-Fi Alliance	WFA74189
Normative	FCC/ICES Class B, CE, RCM/ACMA, VCCI Class B, TELEC, BSMI, NCC, MSIP, ANATEL, Customs Union, RoHS (Europa/Cina), RAEE
Approvazioni di sicurezza	UL E211396, UL 62368-1, UL 60950-1 cUL CAN/CSA C22.2 N. 62368-1-14, CAN/CSA C22.2 N. 62368-1-14, EN 60950-1 o EN 62368-1, IEC 60950-1, IEC 62368-1, Europa: EN 60950-1, EN 62368-1, Taiwan: CNS 1336-1
Approvazioni radio	USA: FCC Parte 15C, 15E, Canada: ISED RSS-247, Europa: (RED) EN 300 328, EN 301 893, Aus/NZ: AS/NZs 4268, Taiwan: NCC LP002, Approvazioni nazionali aggiuntive per Giappone, Corea, Cina, India, Brasile
Approvazioni EMI	USA: FCC P15B, Canada: ICES-003, Europa: EN 301 489-1, -17, EN 55032, EN 55024, Aus/NZ: CISPR 32, Giappone: VCCI, Taiwan: CNS 13438
Limitazioni alle emissioni	USA: FCC Part 2, Canada: RSS-102, Europa: EN 50385, Aus/Nz: ASNZS 2772
MIMO	MU-MIMO 4x4 (4 flussi)
Numero max./consigliato di client connessi per ciascuna radio	128/48
Sicurezza	UL, cUL, TÜV/GS, CB, CE, BSMI, Mexico CoC, Customs Union
USB WAN fail-over e bilanciamento del carico	N/D

CONDIZIONI AMBIENTALI	SONICWAVE 432o
Campo di temperature	da -40 a 60 °C
Umidità	10 - 95%, non condensante

SPECIFICHE RADIO	SONICWAVE 432o
Radio	Dual: 4x4 11n + 4x4 11ac MU-MIMO; terza radio dedicata alla scansione; radio Bluetooth Low Energy
Bande di frequenza	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
Canali operativi	802.11a: USA e Canada 12, Europa 11, Giappone 4, Singapore 4, Taiwan 4, 802.11b/g: USA e Canada 1-11, Europa 1-13, Giappone 1-14 (solo 14-802.11b), 802.11n (2,4 GHz): USA e Canada 1-11, Europa 1-13, Giappone 1-13, 802.11n (5 GHz): USA e Canada 36-48/149-165, Europa 36-48, Giappone 36-48, Spagna 36-48/52-64, 802.11ac: USA e Canada 36-48/149-165, Europa 36-48, Giappone 36-48, Spagna 36-48/52-64
Potenza di trasmissione in uscita	In base al dominio normativo specificato dall'amministratore di sistema
TPC (Transmit Power Control)	Supportato
Velocità di trasmissione dati supportate	802.11a: 6, 9,12,18, 24, 36, 48, 54 Mb/s per canale, 802.11b: 1, 2, 5,5, 11 Mb/s per canale, 802.11g: 6, 9,12,18, 24, 36, 48, 54 Mb/s per canale, 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 Mb/s per canale; 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 Mb/s per canale
Spettro tecnologia di modulazione	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)

SICUREZZA	SONICWAVE 432o
Crittografia dei dati	WPA3, WPA2, IPSec, 802.11i, WPA, 64/128/152 bit WEP, TKIP, AES, SSL VPN**
Client SSL-VPN*	NetExtender, Connect Tunnel
Servizi di sicurezza avanzati	Capture ATP, CFS, Geo-IP, botnet, anti-virus (cloud)

AUTENTICAZIONE	SONICWAVE 432o
Autenticazione	RADIUS, Active Directory, single sign-on (SSO), utente locale
Captive Portal	Click-through, server esterno, social account (Facebook, Google, Twitter e Linkedin), sign-on
Accesso al Captive Portal	Utenti locali, RADIUS, LDAP, OTP, AD

REPORTISTICA	SONICWAVE 432o
Avvisi	Notifica di allarme critico tramite SMS

*SonicWave funge da client SSL-VPN

**In caso di utilizzo con appliance della serie SonicWall Secure Mobile Access

Riepilogo delle funzionalità di SonicWave

ESPERIENZA D'USO SUPERIORE

Funzionalità	Descrizione
Prestazioni e portata wireless ad alta velocità	Gli access point SonicWave si basano sullo standard 802.11ac Wave 2, che può raggiungere una frequenza PHY fino a 2,34 Gb/s mantenendo un livello prestazionale più elevato a maggiori distanze a seconda delle condizioni ambientali.
Migliore qualità del segnale	Lo standard 802.11ac opera nella banda di frequenze di 5 GHz, che presenta una minore presenza di dispositivi wireless ed è pertanto meno incline alle interferenze di segnali.
Maggiore affidabilità wireless	L'aumento della larghezza di banda e il maggior numero di flussi spaziali, combinati con la tecnologia MU-MIMO e la migliore elaborazione offerta dallo standard 802.11ac, garantiscono una maggiore efficienza della copertura wireless.
MU-MIMO	La tecnologia MU-MIMO (Multi-user, multiple-input, multiple-output) consente la trasmissione simultanea dall'access point a numerosi client wireless anziché a uno solo.
Band steering	Il band steering migliora l'esperienza d'uso, indirizzando i client dual band a connettersi automaticamente alla banda di frequenza a 5 GHz meno trafficata, lasciando la frequenza più affollata di 2,4 GHz per i client legacy.
Beamforming	Il beamforming migliora le prestazioni e la portata wireless focalizzando il segnale wireless su un singolo client, anziché diffondere la trasmissione dei dati in modo uguale in tutte le direzioni.
AirTime Fairness	AirTime Fairness distribuisce in modo uniforme il tempo di trasmissione, per cui i client più veloci ricevono una maggiore quantità di dati, mentre i client più lenti ne ricevono meno nello stesso intervallo di tempo.
Wireless mesh	Una rete wireless mesh consente di estendere la copertura Wi-Fi istantaneamente senza bisogno di cavi.
Distribuzione della banda wireless mediante FairNet	FairNet garantisce una quantità minima di larghezza di banda ad ogni client wireless, in modo da impedire un consumo sproporzionato di banda da parte di un unico utente.

SICUREZZA WIRELESS COMPLETA

Funzionalità	Descrizione
Tecnologia Reassembly-Free Deep Packet Inspection	I firewall SonicWall di nuova generazione integrano la tecnologia Reassembly-Free Deep Packet Inspection® (RFDPI), che analizza tutto il traffico in ingresso e in uscita su reti cablate e wireless per eliminare intrusioni, ransomware, spyware, virus e altre minacce prima che entrino nella rete.
Real-Time Deep Memory Inspection (RTDMI)	Questa tecnologia in attesa di brevetto, basata su cloud, rileva e blocca il malware che non mostra alcun comportamento dannoso e nasconde il proprio armamentario attraverso la crittografia. Obbligando il malware a svelare la sua presenza in memoria, il motore RTDMI rileva e blocca in modo proattivo minacce di massa, zero-day e malware sconosciuto.
Decrittazione e ispezione SSL/TLS	Il firewall SonicWall decifra e ispeziona in tempo reale il traffico SSL/TLS senza proxy alla ricerca di malware, intrusioni e sottrazioni di dati, applicando le policy di controllo delle applicazioni, degli URL e dei contenuti per proteggere la rete dalle minacce nascoste nel traffico crittografato con SSL/TLS.
Terza radio dedicata alla scansione	La maggior parte degli access point SonicWave include una radio dedicata che esegue la scansione continua dello spettro wireless alla ricerca di access point non autorizzati, e comprende funzioni aggiuntive di sicurezza che contribuiscono alla conformità PCI.
Rilevamento e prevenzione di intrusioni wireless	La funzione di rilevamento e prevenzione delle intrusioni wireless esegue la scansione della rete wireless alla ricerca di access point non autorizzati (rogue), dopodiché il firewall applica automaticamente delle contromisure, come il blocco di eventuali connessioni al dispositivo.
Servizi wireless guest	I servizi wireless guest consentono agli amministratori di fornire agli utenti ospiti solamente l'accesso a Internet. Questo accesso è separato dall'accesso interno e richiede agli utenti ospiti di autenticarsi in modo sicuro a un access point virtuale prima di autorizzare l'accesso.
Lightweight HotSpot Messaging	Lightweight Hotspot Messaging estende il modello di servizi wireless guest di SonicWall, basato sull'accesso a Internet differenziato per gli utenti ospiti, offrendo un'ampia personalizzazione dell'interfaccia di autenticazione e l'uso di qualsiasi schema di autenticazione.
Captive portal	La tecnologia Captive Portal obbliga il dispositivo di un utente a visualizzare una pagina web dove l'utente deve autenticarsi per poter accedere a Internet.
Segmentazione degli access point virtuali	Gli amministratori possono creare fino a otto SSID sullo stesso access point, ciascuno con le proprie impostazioni dedicate di autenticazione e privacy. In questo modo si ottiene una segmentazione logica del traffico di rete wireless protetto e dell'accesso sicuro per i clienti.
ACL cloud	ACL cloud, un'estensione della lista di controllo accessi locale, è implementata e gestita da un server RADIUS centralizzato nel cloud. In questo modo si eliminano eventuali problemi di scalabilità dell'ACL locale, permettendo alle aziende di configurare gli account di autenticazione in base alle loro esigenze specifiche. Inoltre è possibile applicare l'autenticazione MAC a tutti i dispositivi Wi-Fi, anche se non sono in grado di supportare lo standard 802.1x. In questo modo si aggiunge un ulteriore livello di protezione alla rete wireless.
Autenticazione Multi-RADIUS	L'autenticazione Multi-RADIUS fornisce una ridondanza di livello aziendale che consente alle imprese di implementare più server RADIUS in modalità attiva/passiva per un'elevata disponibilità. In caso di guasto del server RADIUS primario, il firewall SonicWall a cui spetta la gestione rileva il guasto e passa al server secondario, mantenendo possibile l'autenticazione dei dispositivi wireless. Inoltre, l'autenticazione multi-RADIUS può essere supportata su ciascun access point virtuale e configurata per le modalità WPA-Enterprise, WPA2-Enterprise o WPA2-Auto-Enterprise.
Applicazione granulare delle policy di sicurezza	Gli amministratori di rete possono implementare e applicare regole firewall all'intero traffico wireless e controllare tutte le comunicazioni tra client wireless e qualsiasi host della rete, sia wireless che cablata.

IMPLEMENTAZIONE SEMPLIFICATA E GESTIONE CENTRALIZZATA

Funzionalità	Descrizione
Configurazione semplificata e gestione centralizzata	Gli access point SonicWave vengono automaticamente rilevati, configurati e aggiornati via cloud o dai firewall SonicWall di nuova generazione. Anche l'amministrazione della WLAN viene gestita direttamente dal firewall incaricato della gestione, semplificando la configurazione e centralizzando le normali attività di gestione.
Gestione integrata degli switch	SonicWall Wireless Network Manager offre la gestione integrata degli access point e degli switch SonicWall, garantendo una visibilità e una gestione unificata della rete.
WiFi Planner	Per ottimizzare il posizionamento degli access point prima dell'installazione è possibile utilizzare WiFi Planner, che offre una visione completa dell'ambiente Wi-Fi, compresi gli ostacoli che limitano le prestazioni del segnale e le zone coperte e non coperte.
Vista planimetrica	Uno strumento di pianificazione Wi-Fi consente agli utenti di caricare o creare un disegno in pianta, in modo da posizionare gli access point SonicWave nella maniera più adatta per garantire la copertura wireless richiesta.
Visualizzazione della topologia	Uno strumento Wi-Fi mappa automaticamente i dispositivi e il modo in cui sono connessi nell'architettura della rete wireless, semplificando così la risoluzione di eventuali problemi.
Certificazione Plenum per installazione a soffitto	Gli access point SonicWave sono dotati di certificazione per l'installazione sicura all'interno o al di sopra di controsoffittature, ad esempio negli spazi per il trattamento dell'aria.
Diverse opzioni di alimentazione	Gli access point SonicWave sono alimentati da un iniettore PoE (Power over Ethernet) SonicWall o da dispositivi di altri produttori per facilitare l'implementazione in luoghi dove le prese elettriche non sono facilmente accessibili.
Controlli luminosi regolabili	Grazie ai LED a luminosità regolabile (escluso il LED dell'alimentazione), i SonicPoint si adattano perfettamente agli ambienti in cui è richiesta una maggiore discrezione nella copertura wireless.
Ampio supporto di standard e protocolli	Gli access point SonicWave supportano un'ampia gamma di standard wireless e protocolli di sicurezza, tra cui 802.11 a/b/g/n/ac, WPA2 e WPA. Le aziende possono così sfruttare al meglio i precedenti investimenti in dispositivi che non sono in grado di supportare standard di crittografia di livello superiore.

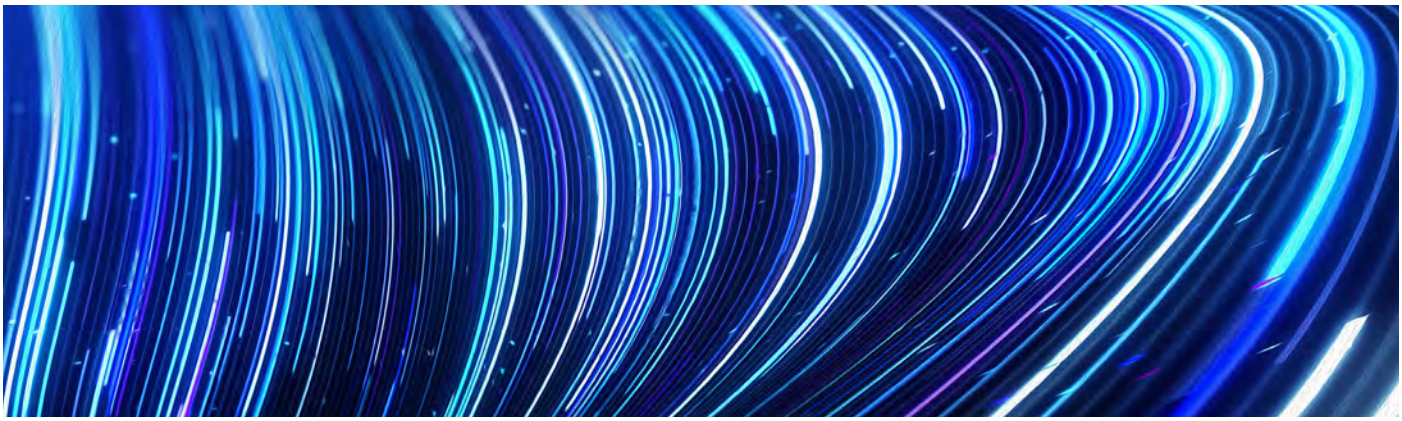
BASSO COSTO TOTALE DI PROPRIETÀ

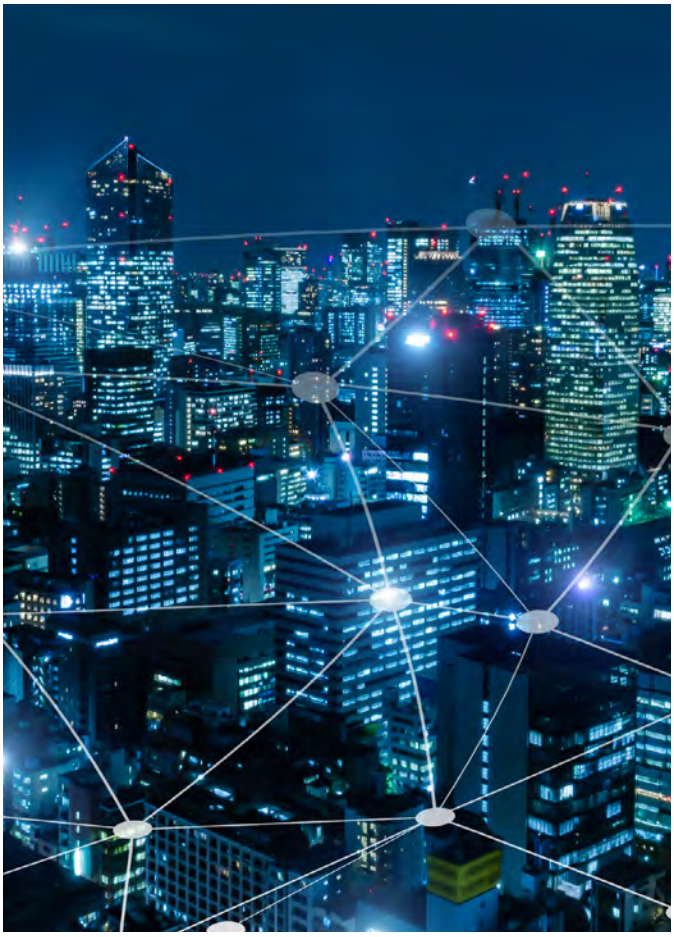
Funzionalità	Descrizione
Basso TCO	Funzionalità come l'implementazione semplificata e un unico pannello di gestione per i dispositivi wireless e per la sicurezza, senza la necessità di acquistare un controller wireless separato, riducono drasticamente i costi a carico delle aziende per aggiungere la connettività wireless in un'infrastruttura di rete nuova o esistente.
MiFi Extender	MiFi Extender consente di aggiungere a un access point SonicWave un modem 3G/4G/LTE da utilizzare come WAN primaria o come collegamento WAN di failover secondario per garantire la continuità operativa.
Bluetooth Low Energy	Gli access point SonicWave includono una radio Bluetooth Low Energy che consente di utilizzare applicazioni industriali, scientifiche e mediche (ISM) per ambito sanitario, fitness, beacon nei punti vendita, sicurezza e intrattenimento domestico con un collegamento a basso consumo energetico.
Porta USB	Gli access point con porta USB supportano il failover 3G/4G. Collegando un dongle alla porta, in caso di interruzione della rete WiFi la rete continua a funzionare tramite connessione cellulare.
Risparmio energetico	Gli access point SonicWave riducono i costi grazie alla funzionalità di risparmio energetico, che consente alle due radio di entrare in modalità sleep per risparmiare energia quando nessun client è connesso attivamente. L'access point esce quindi dalla modalità sleep appena un client tenta di associarsi ad esso.

Per informazioni sugli AP SonicPoint della generazione precedente, fare clic qui.

CODICE RMN

432o	APL42-0C1





SERVIZI OFFERTI DAI PARTNER

Serve aiuto per pianificare, ottimizzare o installare una soluzione SonicWall? I SonicWall Advanced Services Partner sono qualificati per fornire servizi professionali di altissimo livello. Per maggiori informazioni:

www.sonicwall.com/PES

Per provare la nostra soluzione wireless sicura, visitare:

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

SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative per la nuova normalità iperdistribuita, in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. Con la sua capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale, SonicWall rende possibili economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni visitare www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

SONICWALL

Datasheet-SonicWave-US-JK-6931