SONICWALL

Wireless Network Manager

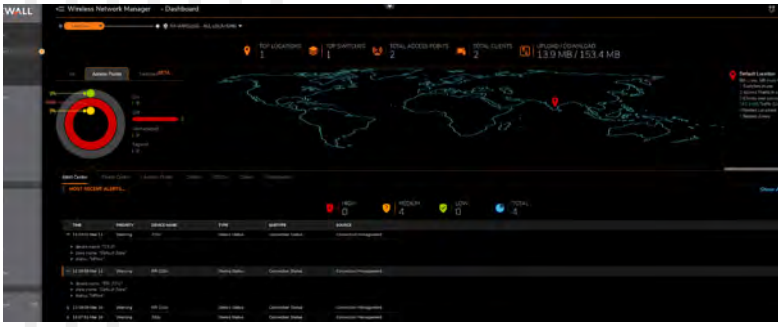
Dashboard unificata basata su cloud per la gestione di access point (AP) e switch

Wireless Network Manager (WNM) di SonicWall è un intuitivo sistema di gestione centralizzata delle reti wireless e degli switch, adatto per aziende di ogni dimensione. Offre analisi avanzate, potenti strumenti e semplici funzioni di onboarding da un unico pannello di controllo.

La sua infrastruttura basata sul cloud semplifica l'accesso, il controllo e la risoluzione dei problemi unificando diversi tenant, sedi e zone. WNM supporta migliaia di AP SonicWave e switch SonicWall, senza la necessità di costosi e complessi sistemi di gestione.

CARATTERISTICHE PRINCIPALI

- Supporto di Private Pre Shared Key (PPSK)
- Autenticazione SAML
- Fingerprinting DHCP
- Supporto di Content Filtering Service
- Gestione integrata di AP SonicWave e switch SonicWall
- Visibilità e controllo unificati grazie a un'unica dashboard basata sul cloud
- Integrazione fluida con Capture Security Center
- Configurazione di policy unificate per reti wireless e cablate
- Implementazione zero-touch per velocizzare l'onboarding e il provisioning
- Aggiornamenti automatici di sicurezza e del firmware
- Analisi completa dei dati in tempo reale
- Report, log e avvisi dettagliati
- Funzionamento affidabile, stabilità e sicurezza nel cloud
- Potenti funzioni di mappatura della topologia di rete
- Tool integrato di analisi avanzata del sito
- Interfaccia intuitiva
- Basso costo totale di proprietà



Scegliete una soluzione di gestione sicura e integrata per reti cablate e wireless:

sonicwall.com/wnm

SCHEDA TECNICA

Una policy unificata per gestire fino a migliaia di AP e switch da qualsiasi luogo, il tutto da un'unica dashboard basata sul cloud.

Gestione da un'unica dashboard

WNM consente di gestire facilmente le reti globali da un unico pannello di controllo. Parte integrante dell'ecosistema Capture Security Center di SonicWall, la sua dashboard intuitiva offre una visibilità e un controllo unificati. La gerarchia di rete consente di visualizzare le singole policy create a livello di tenant che vengono applicate a varie sedi e zone e offre funzionalità di drill-down sui dispositivi gestiti per ottenere dati granulari. WNM è altamente scalabile, da un semplice sito a reti aziendali globali con decine di migliaia di dispositivi gestiti con diversi tenant.

La rete è operativa in pochi minuti grazie all'onboarding e all'installazione automatici.

Chiavi precondivise

Le chiavi private precondivise (Private Pre-Shared Keys, o PPSK) sono uno strumento importante per la protezione delle reti. Ognuna di queste chiavi consiste in una lunga serie di lettere e numeri combinati in ordine casuale che viene generata quando un dispositivo si collega a una rete. Poiché ogni dispositivo client ha una propria chiave precondivisa, PPSK è un metodo efficace per proteggere una rete guest o per disattivare l'accesso di un utente alla rete quando l'utente lascia un'organizzazione. PPSK semplifica l'uso e la gestione della rete e garantisce la compatibilità per i client di vecchia generazione e il supporto per diverse VLAN.

Supporto dell'autenticazione SAML

Lo standard SAML (Security Assertion Markup Language) è un metodo utilizzato per autenticare i dati tra due parti, in particolare tra un provider di identità e un provider di servizi. Consente agli utenti di accedere a più applicazioni web usando un unico set di credenziali di accesso. In poche parole, SAML è un modo per confermare alle applicazioni esterne che un utente è quello che dice di essere. Questo metodo di autenticazione single sign-on (SSO) migliora l'esperienza degli utenti e può anche rafforzare la sicurezza, perché le credenziali degli utenti vengono memorizzate dal provider di identità, e non dal provider di servizi.

Fingerprinting DHCP

Con la diffusione del modello BYOD (Bring Your Own Device) sul posto di lavoro, gli amministratori di rete hanno la necessità di rilevare e identificare dinamicamente i dispositivi degli utenti per assicurarsi che siano conformi. Il fingerprinting DHCP è una tecnica di verifica dell'identità che consente di monitorare i dispositivi e, soprattutto, di bloccare quelli non autorizzati.

Content Filtering Service

Proteggere la rete da malware, virus e infezioni è di importanza vitale. Il Content Filtering Service (CFS) fa esattamente questo: ispeziona l'accesso alle pagine Web e agisce appena viene rilevata una minaccia. CFS fornisce agli amministratori gli strumenti per creare e applicare policy che autorizzano o negano l'accesso a determinati siti in base all'identità del gruppo o dell'utente o in base all'orario, per oltre 56 categorie predefinite.

Funzionamento affidabile

WNM offre la stabilità e l'affidabilità del cloud. In caso di interruzione della connessione Internet, gli access point e gli switch possono continuare a funzionare senza WNM, garantendo la continuità dei servizi. L'autenticazione a due fattori e la cifratura dei pacchetti aumentano la sicurezza, mentre gli aggiornamenti automatici del firmware e delle funzioni di sicurezza mantengono aggiornati i dispositivi gestiti. WNM consente agli amministratori di applicare in modo selettivo firmware di produzione, beta o patch su ogni dispositivo gestito quando necessario e di attivare l'invio automatico di report a più destinatari contemporaneamente.

Implementazione Zero-Touch

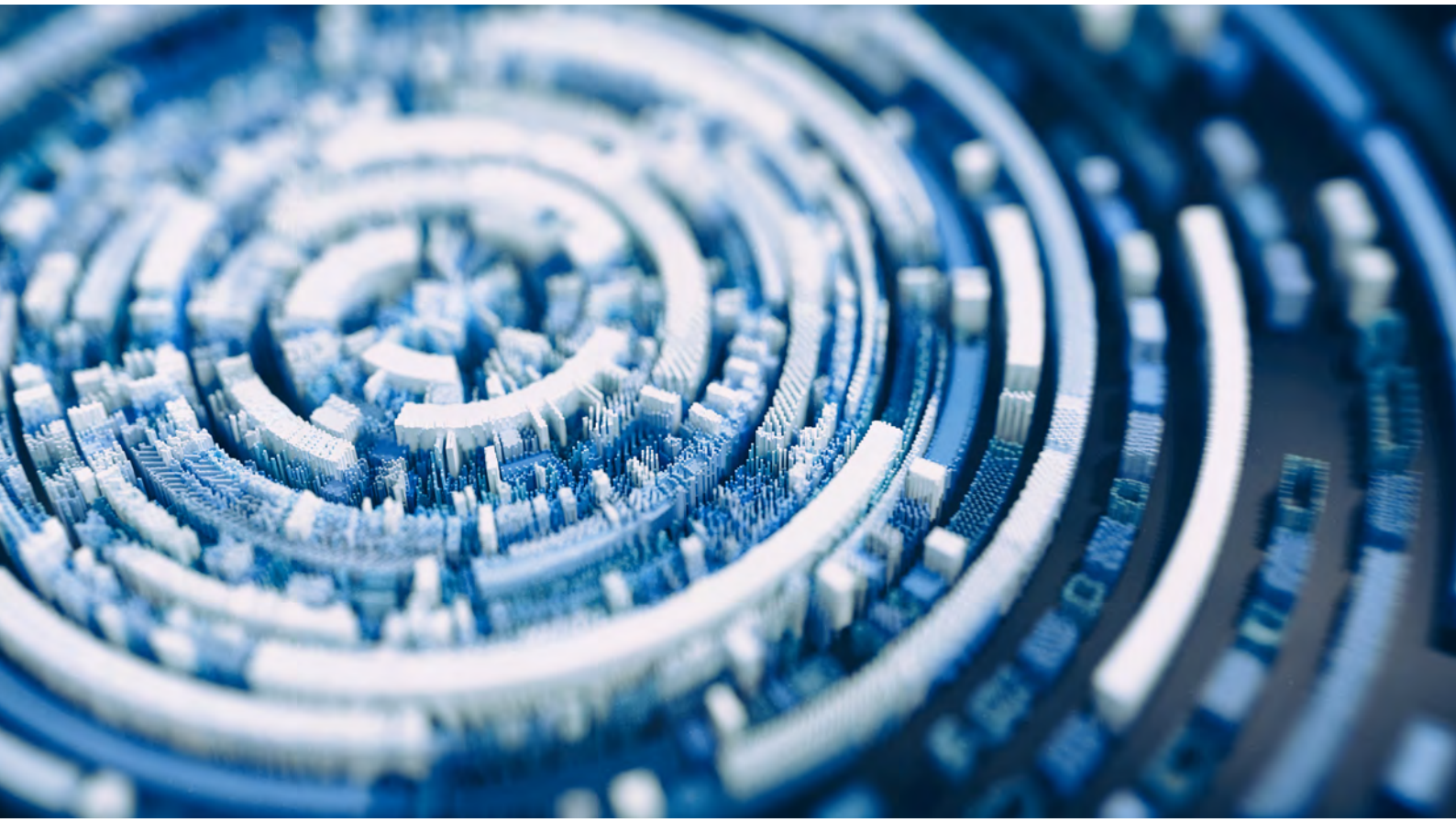
Grazie all'implementazione Zero-Touch, gli AP e gli switch SonicWall sono operativi nel giro di pochi minuti. Con l'app SonicExpress è inoltre possibile registrarli e connetterli da qualsiasi luogo.

Strumenti di analisi avanzati

Un'analisi wireless del sito prima di implementare i punti di accesso può contribuire a migliorare le prestazioni e la produttività. Il tool Wi-Fi Planner integrato in WNM consente di installare gli access point in modo strategico per ottimizzare l'esperienza d'uso del Wi-Fi ed evitare costosi errori. WiFi Planner analizza il posizionamento, i materiali di costruzione, la potenza, la forza del segnale, l'ampiezza del canale e le bande radio. In questo modo è possibile ottimizzare la copertura in reti nuove o esistenti utilizzando il minor numero possibile di AP. L'assegnazione automatica dei canali previene le interferenze. Lo strumento di topologia di WNM fornisce mappe topologiche della rete e statistiche sui dispositivi gestiti.

Basso costo totale di proprietà

WNM basato sul cloud riduce il costo totale di proprietà (TCO), trasformando le spese di capitale (CAPEX) in spese operative (OPEX). WNM riduce i costi e la manutenzione dei controller basati su hardware e ottimizza lo spazio su rack nei data center. La sua interfaccia intuitiva riduce i costi di formazione e di amministrazione.



Per maggiori informazioni sull'ottima scalabilità e affidabilità di questa piattaforma di gestione basata sul cloud, visitare:

SonicWall Wireless Network Manager

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