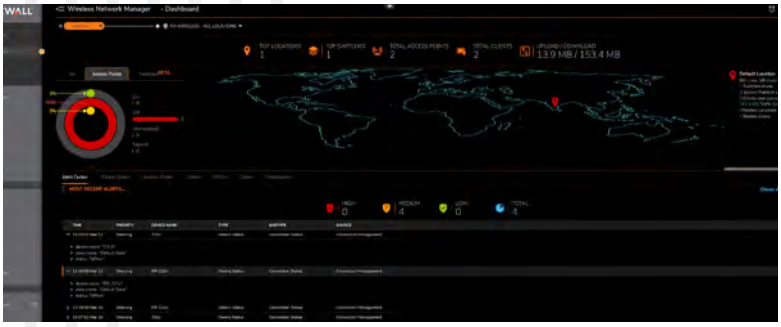
Wireless Network Manager

Zentrales cloudbasiertes Dashboard für die Verwaltung von Access-Points (APs) und Switches

SonicWall Wireless Network Manager (WNM) ist ein intuitives, zentralisiertes Wireless- und Switching-Netzwerkmanagementsystem, das sich für kleine wie große Organisationen flexibel skalieren lässt. Es bietet umfassende Analysefunktionen, leistungsstarke Features und einfaches Onboarding über eine einzige Konsole.

Die cloudbasierte Infrastruktur führt mehrere Nutzer, Standorte und Zonen in einer zentralen Ansicht zusammen und vereinfacht auf diese Weise Zugriff, Steuerung und Troubleshooting. WNM unterstützt Tausende SonicWave-APs und SonicWall-Switches ohne die Kosten komplexer Overlay-Management-Systeme.



HIGHLIGHTS

- Unterstützung von Private Pre-Shared Keys (PPSK)
- SAML-Authentifizierung
- DHCP-Fingerprinting
- Unterstützung von Content Filtering Service
- Integrierte Verwaltung von SonicWave-APs und SonicWall-Switches
- Zentrale Transparenz und Steuerung dank einem einzigen cloudbasierten Dashboard
- Nahtlose Integration mit Capture Security Center
- Zentrale Regelkonfiguration für kabelgebundene und drahtlose Netzwerke
- Vollautomatische Implementierung für schnelles Onboarding und Provisioning
- Automatische Firmware- und Sicherheitsupdates
- Umfassende Datenanalysen in Echtzeit
- Detaillierte Berichte, Protokolle und Warnmeldungen
- Zuverlässiger Betrieb sowie verlässliche Cloud-Stabilität und -Sicherheit
- Leistungsstarkes Netzwerktopologie-Mapping
- Integriertes erweitertes Site-Survey-Tool
- Intuitive Oberfläche
- Niedrigere Gesamtbetriebskosten

Entscheiden Sie sich für eine sichere, integrierte Lösung zur Verwaltung kabelgebundener und drahtloser Netzwerke:

sonicwall.com/wnm

DATENBLATT

Erstellen Sie eine zentrale Regel und verwalten Sie diese überall über ein einziges cloudbasiertes Dashboard – egal ob es sich um ein paar wenige oder Tausende APs und Switches handelt.

Verwaltung über eine einzige Konsole

Mit WNM können Sie globale Netzwerke spielend leicht über eine einzige Konsole verwalten. Als Teil des SonicWall Capture Security Center-Ökosystems sorgt das intuitive Dashboard für eine hohe Transparenz und eine zentrale Verwaltung. Aufgrund der Netzwerkhierarchie können Sie einzelne Regeln einsehen, die auf Nutzerebene erstellt und auf verschiedene Standorte und Zonen angewendet werden. Darüber hinaus können Sie durch einen Drill-down auf verwalteten Geräten detaillierte Daten aufrufen. WNM lässt sich umfassend skalieren, ob für einen einzigen Standort oder für globale Unternehmensnetzwerke mit Zehntausenden verwalteter Geräte und mehreren Nutzern.

Onboarding und Implementierung erfolgen automatisch. Ihr Netzwerk ist in Minutenschnelle eingerichtet.

Pre-Shared Key

Private Pre-Shared Keys (PPSK) sind wichtige Tools zum Schutz von Netzwerken. Jeder dieser Schlüssel besteht aus einer langen Reihe zufällig kombinierter Ziffern und Buchstaben, die generiert wird, sobald ein Gerät mit dem Netzwerk verbunden wird. Da jedes Client-Gerät über einen eigenen einzigartigen Pre-Shared Key verfügt, ist PPSK eine effektive Möglichkeit, ein Gastnetzwerk zu schützen oder den Netzwerkzugriff einer Person bei deren Ausscheiden aus dem Unternehmen zu deaktivieren. PPSK vereinfacht die Nutzung und Verwaltung des Netzwerks, stellt die Kompatibilität für ältere Clients sicher und unterstützt unterschiedliche VLANs.

Unterstützung der SAML-Authentifizierung

Security Assertion Markup Language (SAML) ermöglicht die Authentifizierung von Daten zwischen verschiedenen Parteien, insbesondere zwischen Identitäts- und Serviceprovidern. Mithilfe von SAML können Nutzer über einen einzigen Satz Anmeldedaten auf mehrere Webanwendungen zugreifen. Kurz gesagt: SAML bestätigt externen Anwendungen, dass ein Nutzer wirklich derjenige ist, für den er sich ausgibt. Durch eine solche einmalige Anmeldung (Single-Sign-on) lässt sich nicht nur die Benutzererfahrung verbessern, sondern auch die Sicherheit, da der Identitätsanbieter – und nicht der Serviceprovider – für die Aufbewahrung der Anmeldedaten verantwortlich ist.

DHCP-Fingerprinting

Immer mehr Mitarbeiter nutzen heute ihre eigenen Geräte am Arbeitsplatz (Bring Your Own Device, BYOD). Netzwerkadministratoren brauchen daher eine Möglichkeit, diese Geräte dynamisch zu identifizieren, um sicherzustellen, dass sie den geltenden Vorschriften entsprechen. Mit DHCP-Fingerprinting, einer Methode zur Prüfung der Identität, können Administratoren Geräte nachverfolgen und – ganz besonders wichtig – nicht erlaubte Geräte blockieren.

Content Filtering Service

Es ist extrem wichtig, Ihr Netzwerk vor Malware, Viren und Infektionen zu schützen. Content Filtering Service (CFS) unterstützt Sie dabei: Der Service prüft den Zugriff auf Webseiten und leitet Maßnahmen ein, wenn eine Bedrohung identifiziert wird. Administratoren können Regeln erstellen und anwenden, um den Zugriff auf Sites basierend auf der Nutzer- oder Gruppenidentität bzw. nach Tageszeit für über 56 vordefinierte Kategorien zu erlauben oder zu verweigern.

Zuverlässiger Betrieb

WNM bietet die Stabilität und Zuverlässigkeit der Cloud. Da bei einem Internetausfall die Access-Points und Switches ohne WNM weiterlaufen können, ist die Business-Continuity jederzeit gewährleistet. Die Zwei-Faktor-Authentifizierung und die Verschlüsselung von Datenpaketen verbessern die Sicherheit. Gleichzeitig sorgen automatische Firmware- und Sicherheitsupdates dafür, dass verwaltete Geräte immer auf dem neuesten Stand bleiben. Mit WNM können Administratoren Produktions-, Beta- oder Patch-Firmware bei Bedarf selektiv auf jedem verwalteten Gerät anwenden. Darüber hinaus lassen sich Berichte automatisch an mehrere Empfänger gleichzeitig versenden.

Vollautomatische Implementierung

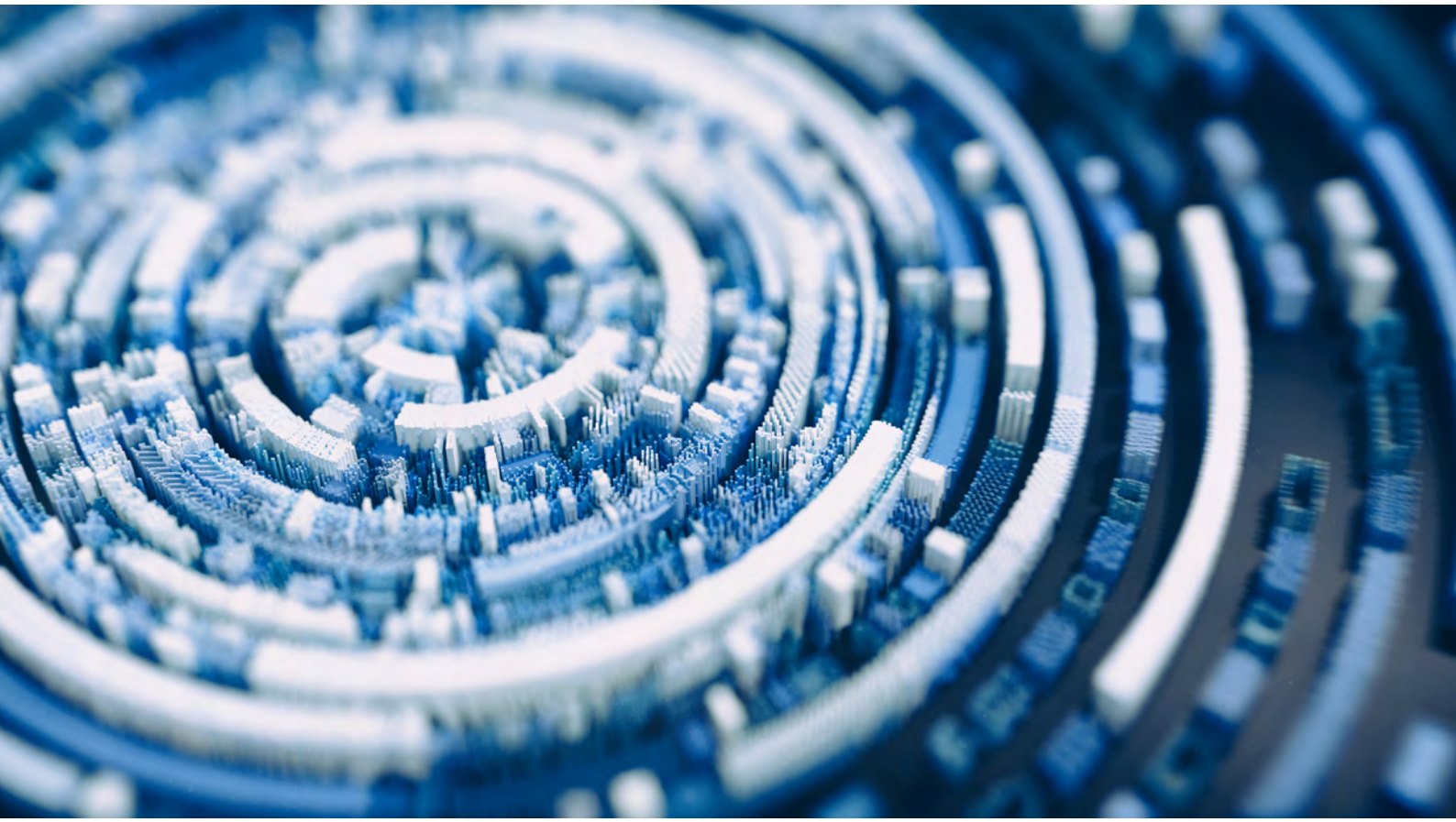
Dank der vollautomatischen Implementierung können Sie Ihre SonicWall-APs und -Switches in nur wenigen Minuten einrichten. Über die SonicExpress-App können Sie diese außerdem von überall aus registrieren und onboarden.

Erweiterte Analysetools

Vor der Implementierung eines Access-Points kann ein Wireless-Site-Survey dabei helfen, eine möglichst hohe Performance und Produktivität sicherzustellen. Das in WNM integrierte Tool „WiFi Planner" ermöglicht die strategische Implementierung von Access-Points, sodass Sie die Wi-Fi-Benutzererfahrung optimieren und kostspielige Fehler vermeiden können. WiFi Planner analysiert Standort, Baumaterialien, Energiebedarf, Signalstärke, Kanalbreite und Frequenzbereiche. So können Sie die Abdeckung in neuen oder bestehenden Netzwerken mit möglichst wenigen APs optimieren. Durch eine automatische Kanalzuweisung lassen sich Interferenzen vermeiden. Zudem bietet das Topologie-Tool von WNM Netzwerktopologiekarten und Statistiken zu verwalteten Geräten.

Niedrigere Gesamtbetriebskosten

Der cloudbasierte WNM reduziert die Gesamtbetriebskosten durch eine Umgliederung der Investitionskosten (CAPEX) in die Betriebskosten (OPEX). WNM eliminiert die Kosten und den Verwaltungsaufwand redundanter hardwarebasierter Controller und optimiert den Rack-Platz im Datencenter. Durch die intuitive Oberfläche fallen außerdem weniger Kosten für Training und Administration an.



Um mehr über die überragende Skalierbarkeit und Zuverlässigkeit dieser cloudbasierten Management-plattform zu erfahren, werfen Sie einen Blick auf:

SonicWall Wireless Network Manager

Über SonicWall

SonicWall bietet grenzenlose Cybersicherheit für eine extrem dezentrale Arbeitswelt, in der jeder remote, mobil und potenziell gefährdet ist. Durch die Identifizierung unbekannter Bedrohungen, moderne Echtzeit-Überwachungsfunktionen und eine herausragende Wirtschaftlichkeit hilft SonicWall großen 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-WirelessNetworkManager-JK-US-6800