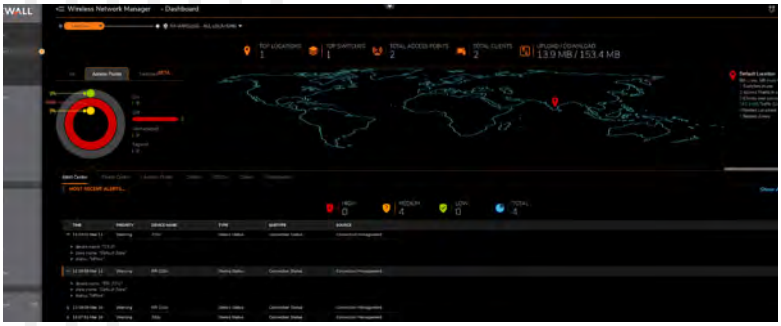
Wireless Network Manager

Tableau de bord unifié basé sur le cloud pour la gestion des points d'accès et des commutateurs

Adaptable aux organisations de toute taille, SonicWall Wireless Network Manager (WNM) est un système intuitif et centralisé de gestion de réseau sans fil et de commutation. Il fournit des analyses approfondies, des fonctionnalités performantes et une intégration facilitée depuis un écran unique.

Son infrastructure basée sur le cloud simplifie l'accès, le contrôle et le dépannage en unifiant plusieurs utilisateurs, emplacements et zones. WNM prend en charge des milliers de points d'accès SonicWave et de commutateurs SonicWall, sans le coût des systèmes de gestion de superposition complexes.



AVANTAGES

- Prise en charge des clés privées pré-partagées (PPSK)
- Authentification SAML
- Lecteur d'empreintes digitales DHCP
- Prise en charge du service de filtrage de contenu
- Gestion intégrée des points d'accès SonicWave et des commutateurs SonicWall
- Visibilité et contrôle unifiés grâce à un tableau de bord unique basé sur le cloud
- Intégration transparente avec Capture Security Center
- Configuration unifiée des règles pour le réseau filaire et sans fil
- Déploiement Zero-Touch pour une intégration et un provisioning rapides
- Mises à jour automatiques des firmwares et de la sécurité
- Analyses de données approfondies en temps réel
- Rapports détaillés, journaux et alertes
- Fiabilité des opérations, stabilité du cloud et sécurité
- Cartographie optimisée de la topologie du réseau
- Outil de mesure de site sans fil avancé intégré
- Interface intuitive
- Coût total de possession plus faible

Passez à une solution de gestion de réseau filaire et sans fil intégrée et sécurisée :

sonicwall.com/wnm

FICHE TECHNIQUE

Créez une règle unifiée et gérez aussi bien quelques points d'accès et commutateurs que des milliers, le tout via un tableau de bord unique basé sur le cloud.

Gestion depuis un écran unique

WNM vous permet de gérer facilement des réseaux mondiaux depuis un écran unique. Partie intégrante de l'écosystème SonicWall Capture Security Center, son tableau de bord intuitif offre une visibilité et un contrôle unifiés. La hiérarchie du réseau vous permet d'afficher les règles uniques créées au niveau de l'utilisateur qui sont répercutées dans divers emplacements et zones. Zoomez sur les appareils gérés pour obtenir des données granulaires. WNM est hautement évolutif, d'un site unique aux réseaux d'entreprise mondiaux avec des dizaines de milliers d'appareils gérés prenant en charge plusieurs utilisateurs.

L'intégration et le déploiement sont automatiques. Votre réseau est opérationnel en quelques minutes.

Clé pré-partagée

Les clés privées pré-partagées (PPSK) sont un outil important pour protéger les réseaux. Chacune est constituée d'une longue série aléatoire de chiffres et de lettres combinés qui est générée lorsqu'un appareil rejoint un réseau. Étant donné que chaque appareil client possède sa propre PPSK, les clés privées pré-partagées constituent un moyen efficace de sécuriser un réseau d'invités ou de désactiver l'accès d'une personne au réseau lorsqu'elle quitte une organisation. Les PPSK permettent de faciliter l'utilisation et la gestion du réseau, la compatibilité avec les clients existants et la prise en charge de différents VLAN.

Prise en charge de l'authentification SAML

Le langage SAML (Security Assertion Markup Language) est une norme qui permet d'authentifier des données entre des parties, notamment entre un fournisseur d'identité et un fournisseur de services. Il permet à un utilisateur d'accéder à plusieurs applications Web en utilisant des identifiants uniques. En résumé, SAML est un moyen d'indiquer aux applications externes qu'un utilisateur est bien celui qu'il prétend être. Cette authentification unique se traduit par une meilleure expérience pour l'utilisateur et peut également améliorer la sécurité, car c'est le fournisseur d'identité et non le fournisseur de services qui est responsable du stockage des identifiants de l'utilisateur.

Lecteur d'empreintes digitales DHCP

Avec la prolifération du BYOD (Bring Your Own Device) sur le lieu de travail, les administrateurs réseau sont au défi de détecter et d'identifier dynamiquement ces appareils pour s'assurer qu'ils sont conformes. Le lecteur d'empreintes digitales DHCP est une technique de vérification de l'identité

qui permet de suivre les appareils, et surtout, de bloquer ceux qui ne sont pas autorisés.

Service de filtrage de contenu

Il est essentiel de protéger votre réseau contre les malwares, les virus et les infections. C'est précisément ce que fait le service de filtrage du contenu (CFS) en inspectant l'accès aux pages Web et en prenant des mesures lorsqu'une menace est détectée. CFS fournit aux administrateurs les outils pour créer et appliquer les règles qui autorisent ou refusent l'accès aux sites selon l'identité d'un individu/groupe ou l'heure de la journée pour plus de 56 catégories prédéfinies.

Fiabilité des opérations

WNM offre la stabilité et la fiabilité du cloud. En cas de panne d'Internet, les points d'accès et les commutateurs peuvent continuer de fonctionner sans WNM, assurant ainsi la continuité des activités. L'authentification à deux facteurs et le chiffrement des paquets renforcent la sécurité, tandis que la mise à jour automatique des firmwares et de la sécurité permet de maintenir à jour les appareils gérés. WNM autorise les administrateurs à appliquer de manière sélective des firmwares de production, bêta ou correctifs sur chaque appareil géré selon les besoins, et permet l'envoi automatique de rapports à plusieurs destinataires simultanément.

Déploiement Zero-Touch

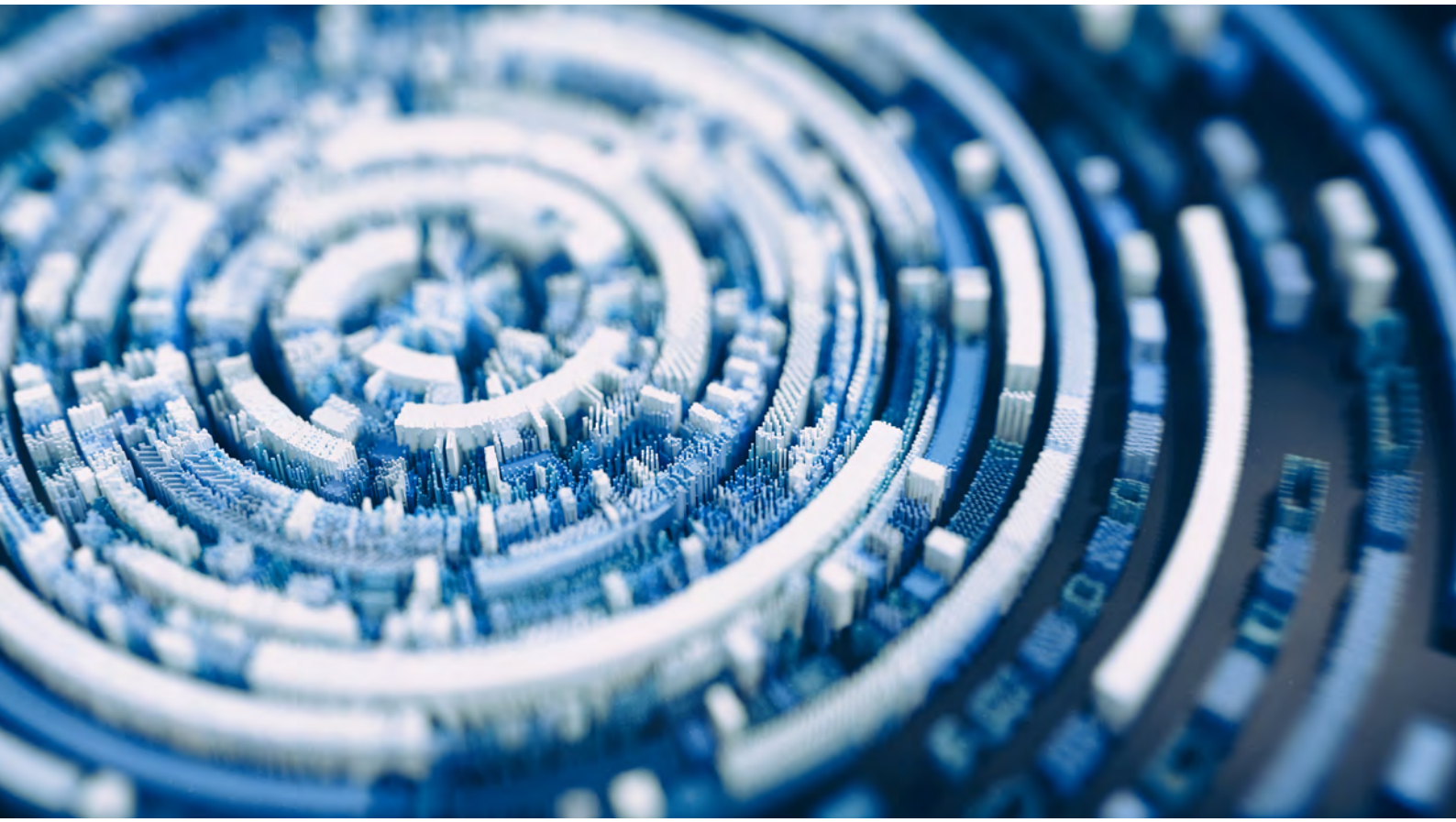
Avec le déploiement Zero-Touch, vos points d'accès et commutateurs SonicWall sont opérationnels en quelques minutes. Et vous pouvez les enregistrer et les intégrer partout grâce à l'application SonicExpress.

Outils d'analyse avancée

Une étude du site sans fil avant le déploiement des points d'accès peut contribuer à garantir les performances et la productivité. L'outil WiFi Planner de WNM vous aide à déployer stratégiquement les points d'accès pour optimiser l'expérience des utilisateurs du Wi-Fi et éviter les erreurs coûteuses. WiFi Planner analyse l'emplacement, les matériaux de construction, la puissance, la force du signal, la largeur du canal et les bandes radio. Cela vous permet d'optimiser la couverture dans les réseaux nouveaux ou existants avec le minimum de points d'accès. L'affectation automatique des canaux évite les interférences. L'outil de topologie de WNM fournit une cartographie de la topologie du réseau et des statistiques sur les appareils gérés.

Coût total de possession plus faible

La solution WNM basée sur le cloud permet de réduire le coût total de possession en déplaçant les dépenses d'investissement (CAPEX) vers les dépenses d'exploitation (OPEX). WNM élimine le coût et la maintenance des contrôleurs matériels redondants et optimise l'encombrement des centres de données. Son interface intuitive réduit les coûts de formation et administratifs.



Pour en savoir plus sur l'évolutivité et la fiabilité extrêmes de cette plateforme de gestion basée sur le cloud, consultez :

SonicWall Wireless Network Manager

À propos de SonicWall

SonicWall offre une solution de cybersécurité sans limites pour l'ère de l'hyper-distribution, dans une réalité professionnelle où tout le monde est mobile, travaille à distance et sans sécurité. En connaissant l'inconnu, en offrant une visibilité en temps réel et en permettant de véritables économies, SonicWall comble le fossé commercial en matière de cybersécurité pour les entreprises, les gouvernements et les PME du monde entier. Pour plus d'informations, rendez-vous sur www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour de plus amples informations.
www.sonicwall.com

SONICWALL

Datasheet-WirelessNetworkManager-JK-US-6800