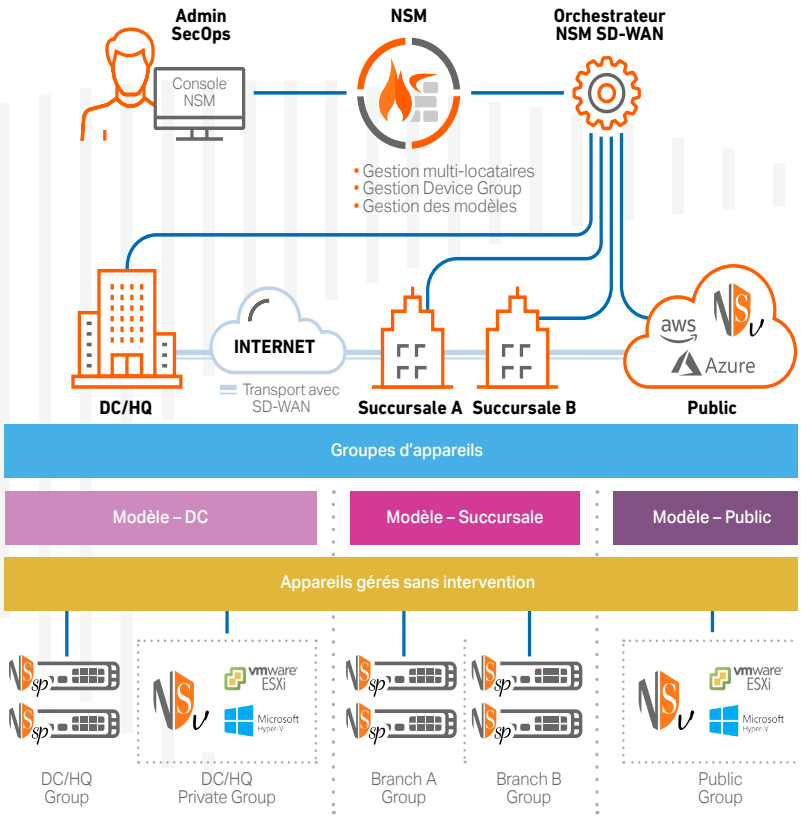
SONICWALL

Network Security Manager

Système de gestion de pare-feu unifié évolutif qui s'adapte à tout environnement

Que vous cherchiez à protéger une petite entreprise, une entreprise distribuée, plusieurs entreprises ou un réseau fermé, la sécurité de votre réseau peut être submergée par des dysfonctionnements opérationnels, des risques invisibles et des exigences réglementaires. Historiquement, les bonnes pratiques de gestion des pare-feux se sont principalement appuyées sur un système robuste et fiable et des mesures de contrôle opérationnel. Cependant, les erreurs courantes, les mauvaises configurations et peut-être même les violations de ces contrôles restent des défis constants pour les centres de sécurité opérationnels (SOC) bien gérés.



AVANTAGES

Entreprise

- Réduction des frais généraux de gestion de la sécurité
- Connaissance du paysage des menaces et de la stratégie de sécurité
- Efficacité de la DSI et réduction du surmenage des administrateurs
- Prévention des interruptions d'activité et incidents de sécurité coûteux

Exploitation

- Élimination des silos de gestion des pare-feux
- Intégration facile de n'importe quel nombre de pare-feux à distance
- Réponse rapide aux problèmes de système critiques, garantissant des performances réseau optimales
- Instauration d'une configuration et d'une stratégie cohérentes pour l'ensemble des appareils gérés
- Simplification du déploiement rapide des réseaux SD-WAN

Sécurité

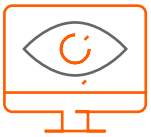
- Audit, engagement et application de règles de sécurité cohérentes dans tous les environnements
- Instauration de configurations SD-WAN cohérentes pour l'ensemble des sites
- Reconnaissance et réaction rapides aux problèmes et aux risques
- Surveillance et suivi des résultats des actions stratégiques avec davantage de clarté
- Prévention des authentifications d'utilisateurs non autorisés, y compris des menaces internes

Gestion centralisée. Sécurité renforcée.

www.sonicwall.com/nsm

FICHE TECHNIQUE

SonicWall Network Security Manager (NSM), une solution de gestion centralisée de pare-feux multi-locataires, vous permet de gérer de manière centralisée et sans erreur l'ensemble des opérations de pare-feu en adoptant des flux pouvant être contrôlés. Les fonctionnalités de reporting et d'analyse[1,2] vous offrent une visibilité sur une interface unique afin de surveiller et d'identifier les menaces grâce à l'unification et à la mise en corrélation des journaux de tous les pare-feux. La solution NSM vous aide également à rester en conformité grâce à l'application de règles cohérentes sur tous les pare-feux, à une piste d'audit détaillée de chaque changement de configuration et à un reporting granulaire. La solution NSM s'adapte à toutes les tailles d'organisation gérant des réseaux avec des centaines de pare-feux déployés entre différents locataires ou sur plusieurs sites – le tout plus rapidement et avec moins d'efforts.



Restez maître de la situation : orchestrez les opérations de pare-feu depuis une seule interface

La solution NSM vous offre tout ce dont vous avez besoin pour un système de gestion de pare-feu unifié. Elle vous apporte une visibilité au niveau locataire, un contrôle des appareils reposant sur les groupes et une évolutivité illimitée afin de centraliser la gestion et l'exécution de vos opérations de sécurité du réseau SonicWall. Ces dernières incluent le déploiement et la gestion de l'ensemble des pare-feux, groupes d'appareils et locataires, la synchronisation et l'application de règles de sécurité cohérentes, y compris le filtrage DNS et de contenu, au sein des environnements avec des contrôles locaux flexibles et la surveillance de tous les éléments essentiels depuis un tableau de bord dynamique avec rapports et analyses détaillés. NSM assure également le contrôle des accès au réseau via l'intégration d'Aruba ClearPass. La solution NSM vous permet par ailleurs d'administrer l'ensemble des éléments depuis une seule console conviviale accessible de partout à l'aide d'un appareil avec navigateur.

Gestion multi-locataires

À mesure que votre environnement de pare-feu se développe, vous aurez besoin d'un système de gestion de pare-feu capable d'évoluer avec cet environnement. La solution NSM fournit une gestion complète multi-locataires et un contrôle indépendant des règles sur l'ensemble des locataires gérés. Cette séparation englobe toutes les caractéristiques et fonctions de gestion de la solution NSM qui dictent le fonctionnement du pare-feu pour chaque locataire. Vous pouvez construire chaque locataire pour qu'il dispose de son propre ensemble d'utilisateurs, de groupes et de rôles pour effectuer la gestion des groupes d'appareils, l'orchestration des règles et toutes les autres tâches administratives dans les limites du compte de locataire attribué.

Gestion Device Group

Device Group constitue une méthode efficace pour créer et gérer des pare-feux en tant que groupes ou groupes hiérarchiques et pour appliquer et déployer des modèles de configuration sur des groupes de pare-feux. Cela vous permet de synchroniser et d'appliquer des règles, des objets et/ou des exigences de configuration communs à tous les groupes de pare-feux sélectionnés d'une manière à la fois cohérente et fiable. Tous les changements de règle approuvés dans le modèle sont automatiquement appliqués à tous les groupes d'appareils liés à ce modèle. Le regroupement des appareils peut être défini de manière granulaire en fonction de caractéristiques telles que le type de réseau, la localisation, le département, la structure organisationnelle ou une combinaison d'attributs relatifs pour faciliter la gestion, l'identification et l'association.

Gestion, application et déploiement des modèles

Les flux de travail simplifiés de la solution NSM vous permettent de concevoir, de valider, de vérifier et d'appliquer facilement et rapidement des modèles de configuration pour gérer un ou des milliers de pare-feux sur de nombreux sites géographiques. Les modèles comprenant divers règles, paramètres et objets de pare-feu associés sont définis indépendamment de l'appareil et envoyés automatiquement et de manière centralisée par la solution NSM vers les appareils ou groupes d'appareils qui nécessitent des configurations similaires.

Lorsqu'ils sont combinés aux variables de modèles, les modèles vous permettent de déployer et d'exécuter de manière centralisée des centaines de pare-feux distants et d'instaurer une configuration unifiée tout en conservant des valeurs spécifiques aux différents appareils comme les IP d'interface, la configuration du DNS, le nom d'hôte de pare-feu, etc. Les entreprises distribuées peuvent aisément intégrer et sécuriser de nouveaux sites et succursales distants avec un seul modèle, éliminant ainsi les configurations manuelles séparées pour chaque appareil et pour les différents sites.

Orchestration et surveillance SD-WAN

La solution NSM simplifie le déploiement de réseaux SD-WAN à tous les niveaux de l'entreprise via un flux intuitif et auto-guidé. Elle centralise l'instauration et l'application d'un

trafic fondé sur les applications et autres configurations de gestion du trafic dans et entre plusieurs centaines de sites, par ex. succursales et points de vente. En outre, la solution NSM vous permet de surveiller la santé et les performances de tout votre environnement SD-WAN afin de garantir la cohérence des configurations, de garantir le fonctionnement optimal des applications et de donner les outils nécessaires aux équipes en charge de l'infrastructure réseau pour dépanner et solutionner rapidement les problèmes.

Orchestration et surveillance VPN

La solution NSM simplifie les configurations et règles VPN grâce à une procédure de configuration étape par étape simple faisant appel à un assistant. Les administrateurs système peuvent ainsi établir rapidement et sans erreur la connectivité et la communication d'un site à l'autre à l'aide d'un flux reproductible et auto-guidé. Par ailleurs, la fonction de surveillance VPN vous aide à garder un œil sur vos VPN, vous offrant une visibilité intégrale sur les activités, la santé et les performances de votre environnement VPN. Les administrateurs réseau peuvent exploiter ces informations afin de surveiller le statut de connexion, les données transférées et la bande passante consommée sur ces tunnels VPN. Des alertes aident les administrateurs à garantir de manière proactive l'intégrité des connexions VPN pour une connectivité continue entre les sites.

Soyez plus efficace : travaillez plus intelligemment et prenez des mesures de sécurité plus rapidement avec moins d'efforts

La solution NSM est un outil de gestion de la productivité qui vous permet de travailler plus intelligemment et de prendre des mesures de sécurité plus rapidement avec moins d'efforts. Sa conception est guidée par des processus opérationnels et repose sur le principe de simplification et, dans certains cas, d'automatisation des flux de travail afin d'améliorer la coordination de la sécurité tout en réduisant la complexité, le temps et les frais généraux liés à l'exécution des opérations de sécurité quotidiennes et des tâches administratives.

Zero-Touch Deployment sans effort

Intégré à la solution NSM, le service Zero-Touch Deployment vous permet de déployer et de mettre en service sans effort les pare-feux, les commutateurs et les points d'accès SonicWall sur les sites distants et dans les succursales. L'ensemble du processus nécessite une intervention minimale de l'utilisateur et est entièrement automatisé. Les appareils compatibles avec la technologie sans intervention sont expédiés directement aux sites d'installation. Une fois enregistrés et connectés au réseau, tous les appareils connectés sont instantanément opérationnels et la sécurité et la connectivité sont assurées de manière transparente. Une fois les liens de communication établis avec la solution NSM, les modèles d'appareils pré-fournis sont automatiquement envoyés à tous les appareils compatibles avec la technologie sans intervention. Cela élimine le temps, le coût et la complexité associés au processus traditionnel d'intégration sur site.

Gestion des changements sans erreur

La solution NSM fournit un accès immédiat à de puissants flux de travail automatisés qui sont conformes aux exigences de gestion des changements de règle de pare-feu et d'audit des centres de sécurité opérationnels (SOC). Elle assure une gestion sans erreur des changements de règle en appliquant une série de processus de configuration rigoureux comprenant la comparaison, la validation et l'approbation des règles avant déploiement. Les groupes d'approbation sont flexibles, ce qui permet de respecter les diverses procédures d'audit des différentes équipes en charge des opérations. La solution NSM déploie de manière programmée des règles de sécurité entièrement validées pour améliorer l'efficacité opérationnelle, atténuer les risques et éliminer les erreurs de configuration.

Automatisation de la gestion avec l'API RESTful

L'API RESTful de la solution NSM donne à vos opérateurs de sécurité qualifiés une approche standard de la gestion programmatique des fonctionnalités spécifiques à NSM sans interface de gestion Web. Elle facilite l'interopérabilité entre les consoles de gestion NSM et tierces pour augmenter l'efficacité de votre équipe de sécurité interne. Les services API sont utilisés pour automatiser les opérations de pare-feu pour tous les appareils gérés. Cela comprend les tâches courantes quotidiennes telles que la gestion des groupes d'appareils et de locataires, la configuration des audits, les contrôles de santé du système et plus encore.

Soyez mieux informé : analysez les risques cachés avec la surveillance active, le reporting et l'analyse[1,2]

Le tableau de bord interactif de la solution NSM est chargé de données de surveillance, de reporting et d'analyse en temps réel afin de vous aider à résoudre les problèmes, étudier les risques et prendre des décisions et actions intelligentes pour une stratégie de sécurité adaptative renforcée.

Les administrateurs peuvent agir avec précision et rapidité au moyen d'alertes en temps réel afin d'assurer un fonctionnement optimal de leur organisation et d'éviter les interruptions d'activité et incidents de sécurité coûteux.

Voir tout et partout

La solution NSM, lorsqu'elle est combinée à la fonctionnalité d'analyse[1,2], vous donne jusqu'à sept jours de visibilité continue sur l'ensemble de votre écosystème de sécurité SonicWall au niveau des locataires, des groupes ou des appareils. Elle fournit des analyses statiques quasiment en temps réel de tout le trafic réseau et des communications de données qui transitent par l'écosystème de pare-feux. Toutes les données de journal sont automatiquement enregistrées, agrégées, contextualisées et présentées d'une manière claire, exploitable et facilement consommable qui vous permet de découvrir, d'interpréter, de hiérarchiser et de prendre des mesures défensives et correctives appropriées fondées

sur la connaissance des données et de la situation. Le reporting planifié vous permet de personnaliser vos rapports avec n'importe quelle combinaison de données du trafic. Il présente jusqu'à 365 jours de journaux enregistrés au niveau des appareils, des groupes d'appareils ou des locataires pour les analyses historiques, la détection des anomalies, la découverte des failles de sécurité et plus encore. Cela vous aidera à suivre, mesurer et assurer un fonctionnement efficace du réseau et de la sécurité.

Comprendre vos risques

Avec des capacités supplémentaires d'exploration approfondie et de pivotement, vous pouvez analyser et mettre en corrélation les données pour examiner en profondeur et détecter les menaces et problèmes cachés avec une meilleure précision et un plus grand niveau de confiance. En utilisant une combinaison de rapports historiques, d'analyses fondées sur les utilisateurs et les applications et de visibilité des terminaux, vous pouvez analyser en profondeur divers modèles et tendances associés au trafic entrant/sortant, à l'utilisation des applications, à l'accès des utilisateurs et des appareils, aux actions des menaces et plus encore. Vous aurez une meilleure connaissance de la situation et obtiendrez des renseignements précieux pour non seulement identifier les risques de sécurité, mais aussi pour orchestrer les mesures correctives tout en surveillant et en suivant les résultats afin de promouvoir et de favoriser l'application cohérente de la sécurité dans votre environnement.

Optimisez la productivité de vos employés

Les analyses utilisateur[1,2] vous offrent une visibilité globale et transparente de l'utilisation par vos employés des applications Web et d'Internet. Grâce à des capacités de zoom et de rotation, les analystes sont en mesure de facilement et rapidement analyser les points de données intéressants au niveau de l'utilisateur et d'établir des mesures étayées et conformes aux règles en lien avec les utilisateurs et applications à risque au fur et à mesure du processus de découverte. En outre, les rapports de productivité[1,2] mettent à votre disposition des informations relatives à l'utilisation d'Internet et au comportement en ligne de vos employés sur une période déterminée. Cette fonction génère des instantanés performants et des rapports d'analyse approfondie vous permettant de classer les activités en ligne des utilisateurs dans différents groupes de productivité (productif, improductif, acceptable, inacceptable ou personnalisé) afin d'aider l'organisation à mieux comprendre et contrôler l'utilisation d'Internet.

Déploiement flexible

Les clients peuvent déployer la solution NSM de plusieurs manières afin de satisfaire au mieux à leurs besoins en termes de fonctionnement, de réglementation et de budget.

Pour une expérience ne nécessitant pas de maintenance, la solution NSM est disponible dans une version SaaS hébergée par SonicWall et accessible sur Internet. Avec la solution NSM SaaS, vous bénéficiez d'une évolutivité à la demande et d'une réduction de vos coûts opérationnels. Cette solution se caractérise par l'absence de déploiement matériel et logiciel, de programme de maintenance, de personnalisations / configurations / mises à niveau logicielles et de coûts liés à d'éventuels temps d'indisponibilité, une dépréciation et une mise hors service. Toutes ces dépenses sont supprimées et remplacées par un abonnement annuel moindre et prévisible.

Pour un contrôle et une conformité absolus de vos systèmes, vous pouvez déployer la solution NSM dans le cloud public Microsoft Azure ou sous forme d'appliance virtuelle dans un cloud privé sur VMWare, Microsoft Hyper-V ou KVM. Vous bénéficiez ainsi de tous les avantages opérationnels et économiques de la virtualisation, notamment l'évolutivité et l'agilité des systèmes, la rapidité du provisioning des systèmes, une gestion simplifiée et une réduction des coûts.

Fonctions de sécurité

Les institutions fédérales, publiques, sanitaires, pharmaceutiques et autres grandes organisations déploient souvent des réseaux fermés afin de garantir la confidentialité et l'isolement de leurs applications critiques et systèmes d'information les plus sensibles tels que les systèmes de documents confidentiels, les systèmes de contrôle et d'acquisition de données et les centres de recherche. La solution NSM prend en charge les environnements de réseaux fermés en offrant aux administrateurs une méthode hors ligne pour l'intégration, l'activation de licences, la correction et la mise à niveau relatives au système NSM et aux pare-feux qu'il gère sans contacter un gestionnaire de licences SonicWall ou MySonicWall.

Pour une sécurité renforcée, la solution NSM applique plusieurs mesures de contrôle des accès aux comptes afin de prévenir les accès non autorisés à l'interface de gestion NSM. Elle accorde des contrôles administratifs spécifiques en fonction des rôles des utilisateurs et déclenche un verrouillage des comptes en fonction du nombre défini de tentatives de connexion erronées. De même, l'accès des utilisateurs est uniquement permis en cas de connexion depuis une liste spécifiée d'adresses IP sources autorisées et sécurisé via l'authentification à deux facteurs (2FA)[3].

Récapitulatif des fonctionnalités

Gestion

- Contrôle d'accès réseau (NAC) avec Aruba ClearPass
- Gestion au niveau des locataires et Device Group
- Modèles de configuration
- Regroupement d'appareils
- Conversion de la configuration des appareils en modèle
- Assistant d'engagement et de déploiement
- Contrôles des configurations
- Diff. de configurations
- Gestion et planification hors ligne
- Gestion des règles de sécurité des pare-feux
- Gestion des règles de sécurité VPN
- Administration SD-WAN
- Synchronisation des services de sécurité
- Haute disponibilité
- Sauvegardes des configurations
- API RESTful
- Mise à niveau firmware multi-appareils
- Administration fondée sur les rôles
- Gestion des points d'accès et des commutateurs
- Intelligent Platform Monitoring (IPM)[3]
- Gestion des certificats multi-appareils

Surveillance[1,2]

- Santé et statut des appareils
- Statut des licences et de la prise en charge
- Résumé du réseau / des menaces
- Centre d'alerte et de notification
- Journaux d'événements
- Vue topologique

Analyse[1,2]

- Activité par utilisateur
- Utilisation des applications
- Visibilité entre les produits avec Capture Client
- Visualisation dynamique en temps réel
- Capacités de zoom et de pivotement

Reporting[1,2]

- Rapports PDF planifiés – au niveau des locataires, groupes et appareils
- Rapports personnalisables
- Journalisation centralisée
- Rapports multi-menaces
- Rapports axés sur les utilisateurs
- Rapports d'utilisation des applications
- Rapports sur la bande passante et les services
- Rapports sur la bande passante par utilisateur
- Rapports de productivité

Sécurité

- Prise en charge de réseaux fermés
- Verrouillage des comptes
- Contrôle de l'accès aux comptes
- Prise en charge 2FA[3]
- Prise en charge des applications d'authentification 2FA

Licences et packages

Gestion

Fonctionnalité	NSM SaaS Essential	NSM SaaS Advanced	NSM On-Prem[2]
Locataire	Oui	Oui	Oui
Inventaire d'appareils	Oui	Oui	Oui
Règles d'application au niveau du groupe	Oui	Oui	Oui
Device Group	Oui	Oui	Oui
Modèles	Oui	Oui	Oui
Engagement et déploiement (automatisation des flux)	Oui	Oui	Oui
Contrôle des configurations	Oui	Oui	Oui
Diff. des configurations	Oui	Oui	Oui
Automatisation des workflows	Oui	Oui	Oui
API	Oui	Oui	Oui
Déploiement zéro intervention	Oui	Oui	Oui
Orchestration et surveillance SD-WAN	Oui	Oui	Oui
Orchestration et surveillance VPN	Oui	Oui	Oui
Planification des tâches	Oui	Oui	Oui
Sauvegarde / restauration	Oui	Oui	Oui
Mises à jour du firmware	Oui	Oui	Oui
Gestion des points d'accès et des commutateurs	Oui	Oui	Oui
Filtrage DNS avancé	Oui	Oui	Oui
Contrôle d'accès réseau avec Aruba ClearPass	Oui	Oui	Oui
Filtrage du contenu basé sur la réputation	Oui	Oui	Oui

Licences et packages (suite)

Reporting			
Fonctionnalité	**NSM SaaS Essential**	**NSM SaaS Advanced**	**NSM On-Prem[2]**
Tableau de bord au niveau des groupes / locataires	Oui	Oui	Non
Capture ATP (niveau des appareils)	Oui	Oui	Oui
Capture Threat Assessment (niveau des appareils)	Oui	Oui	Oui
Rapports de productivité[5]	Non	Oui	Non
Rapports VPN	Non	Oui	Non
Rapports personnalisés	Oui	Oui	Non
Rapports planifiés (flux, CTA et gestion)	Oui (excepté rapports sur les flux)	Oui	Oui
Jours de données de reporting	7 jours	365 jours	365 jours

Analyse			
Fonctionnalité	**NSM SaaS Essential**	**NSM SaaS Advanced**	**NSM On-Prem[2]**
Analyse par utilisateur	Non	Oui	Oui
Analyse des applications	Non	Oui	Oui
Analyse forensique réseau et chasse aux menaces avec zooms avant et rotations	Non	Oui	Oui
Cloud App Security – détection du Shadow IT	Oui	Oui	Non

Configuration requise

Navigateurs Internet

- Microsoft® Internet Explorer 11.0 ou version supérieure et dernière version de Microsoft Edge, Mozilla Firefox, Google Chrome et Safari

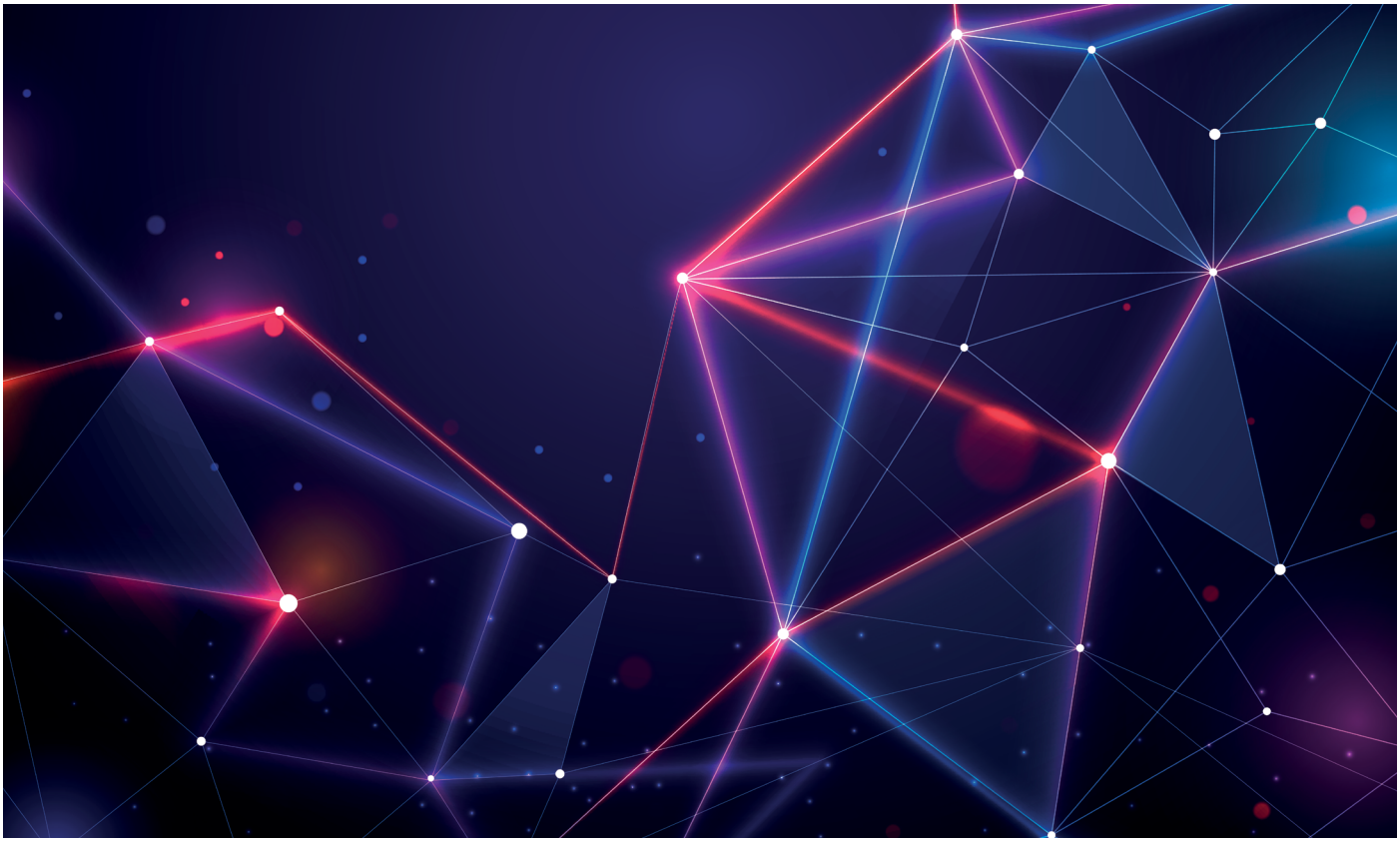
Configuration requise pour NSM On-Prem

- Hyperviseur : ESXi 7.0, 6.7 et Hyper-V 2016, 2019, KVM
- Cloud public : Azure
- Ressources informatiques minimales : 4 vCPU, 24 Go de mémoire pour la gestion de 1 à 500 pare-feux, 250 Go de stockage

Appareils gérés

- NS*sp* 15700, NS*sp* 13700, NS*sp* 12000 Series[4], SuperMassive 9000 Series[4], NSA Series, NS*a* Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- Les appliances et firmwares de 5ème génération, y compris les appareils SOHO qui ne sont pas sans fil et tournant sous SonicOS 5.9, ne sont pas pris en charge.
- Appliances virtuelles de sécurité réseau SonicWall : NS*v* Series
- SonicWall SonicWave[6], SonicPoint
- La prise en charge de SonicWave inclut les points d'accès compatibles Wi-Fi6
- SonicWall Switch

[1] NSM SaaS inclut des fonctionnalités de reporting et d'analyse.
[2] NSM On-Prem nécessite une installation et une licence SonicWall Analytics On-Prem séparée pour les fonctionnalités de reporting et d'analyse.
[3] Disponible uniquement avec NSM On-Prem.
[4] 365 jours de reporting et 30 jours d'analyse non pris en charge.
[5] Nécessite une licence AGSS/CGSS activée sur les pare-feux de génération 6/6.5, une licence Essential Protection sur les pare-feux de 7ème génération.
[6] La prise en charge de SonicWave inclut les points d'accès compatibles Wi-Fi6



Déployez et gérez tous vos pare-feux, commutateurs connectés et points d'accès depuis une interface unique et simple d'utilisation.

www.sonicwall.com/nsm

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-NSM-A4-JK-10177