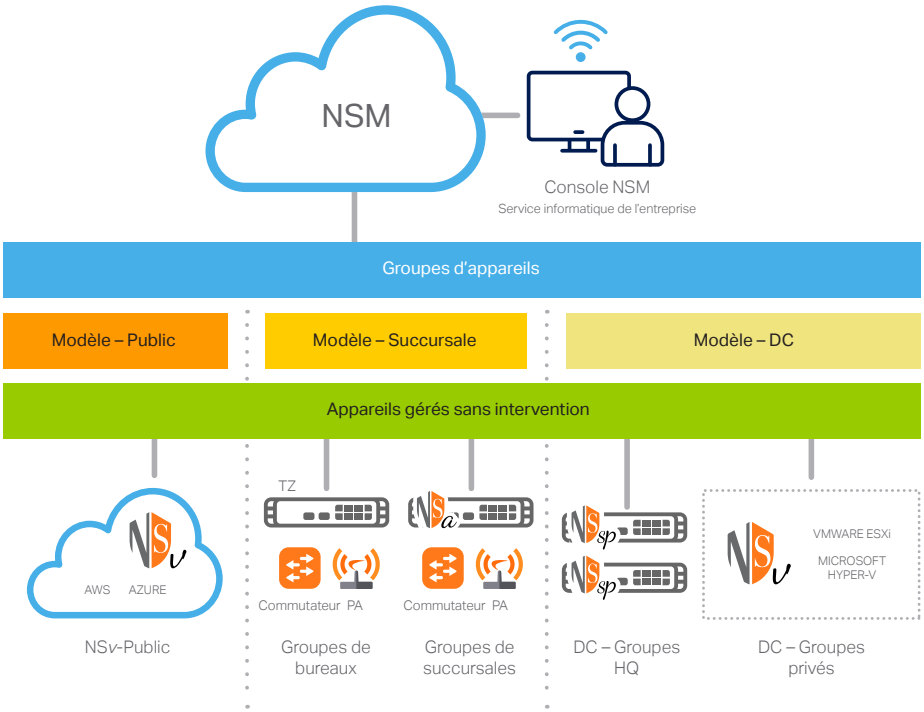
SONICWALL

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 ou plusieurs entreprises, 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-feu 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.

SonicWall Network Security Manager (NSM), un gestionnaire de pare-feu centralisé multi-locataires, vous permet de gérer de manière centralisée toutes les opérations de pare-feu sans erreur en respectant des flux de travail vérifiables. Son moteur analytique natif offre une visibilité sur une interface unique et vous permet de surveiller et de détecter les menaces en unifiant et en mettant en corrélation les journaux de tous les pare-feu. La solution NSM vous aide également à rester en conformité grâce à une piste d'audit complète 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 milliers de pare-feu déployés sur de nombreux sites, et tout cela plus rapidement et avec moins d'efforts.



Avantages :

Entreprise

- Réduction des frais généraux de gestion de la sécurité
- Connaissance du paysage des menaces et de la stratégie de sécurité
- Réduction des dépenses d'investissement avec SaaS

Opérations

- Aucun matériel/logiciel à déployer
- Élimination des silos de gestion des pare-feu
- Intégration facile de n'importe quel nombre de pare-feu à distance
- Visibilité sur toutes les opérations de sécurité

Sécurité

- Audit, engagement et application de règles de sécurité cohérentes dans tous les environnements
- Identification et réaction rapides aux problèmes et aux risques
- Prise de décisions éclairées en matière de règle de sécurité

Gardez le contrôle : orchestrez les opérations de pare-feu d'une manière centralisée

La solution NSM vous offre tout ce qu'il vous faut pour un système de gestion de pare-feu unifié. Elle vous donne une visibilité au niveau des locataires, un contrôle des appareils basé sur le groupe et une évolutivité sans limites pour gérer et fournir de manière centralisée vos opérations de sécurité réseau SonicWall. Cela comprend le déploiement et la gestion de tous les pare-feu, groupes d'appareils et locataires, la synchronisation et l'application de règles de sécurité cohérentes dans vos environnements avec des contrôles locaux flexibles, et une surveillance complète à partir d'un tableau de bord dynamique avec des rapports et des analyses détaillés. La solution NSM vous permet de faire tout cela à partir d'une seule console cloud native conviviale, à laquelle il est possible d'accéder depuis n'importe où en utilisant n'importe quel appareil compatible avec le navigateur.

Gestion multi-locataires
À mesure que votre environnement de pare-feu se développe avec des locataires multi-cloud et multi-sites complexes ayant des besoins de sécurité différents pour chaque segment réseau, 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 des groupes d'appareils
La gestion des groupes d'appareils constitue une méthode efficace pour créer et gérer des pare-feu en tant que groupes ou groupes hiérarchiques et appliquer et déployer des modèles de configuration sur des groupes de pare-feu. 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-feu 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-feu 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.

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 et des tâches administratives.

Déploiement sans intervention et sans effort
Intégré à la solution NSM, le service de déploiement sans intervention vous permet de déployer et de mettre en service sans effort les pare-feu, 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 déballés, enregistrés, connectés au réseau et mis sous tension, 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, l'examen et l'approbation des règles avant déploiement. Les groupes d'approbation sont flexibles, ce qui permet de respecter les diverses procédures d'autorisation et d'audit des différents types d'organisations. La solution NSM déploie de manière programmée des règles de sécurité entièrement validées et vérifiées pour améliorer l'efficacité opérationnelle, atténuer les risques et éliminer les erreurs de configuration et les erreurs humaines.

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 locataires, 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

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

Voir tout et partout
Le tableau de bord de reporting, d'analyse et de surveillance des risques de la solution NSM vous donne jusqu'à sept jours de visibilité continue à 360° de l'ensemble de votre écosystème de sécurité SonicWall au niveau des locataires, des groupes ou des appareils. Il fournit des analyses statiques quasi en temps réel de tout le

trafic réseau et des communications de données qui transitent par l'écosystème de pare-feu. Toutes les données du journal sont automatiquement enregistrées, agrégées, contextualisées et présentées d'une manière significative, exploitable et facilement consommable qui vous permet de découvrir, d'interpréter, de hiérarchiser et de prendre des mesures défensives et correctives appropriées basées sur la connaissance des données et de la situation. Le reporting programmé vous permet de personnaliser entièrement vos rapports avec n'importe quelle combinaison de données vérifiables. Il présente jusqu'à 365 jours de journaux enregistrés au niveau des appareils pour les analyses historiques, la détection des anomalies, la découverte des failles de sécurité, et plus encore. Cela vous aidera à suivre, à mesurer et à 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 les problèmes cachés avec une meilleure précision et un plus grand niveau de confiance. En utilisant une combinaison de rapports historiques, d'analyses basées 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.

Résumé des fonctionnalités

Gestion

- Gestion au niveau des groupes de locataires et d'appareils
- Modèles de configuration
- Regroupement des appareils
- Assistant d'application et de déploiement
- Audits de configuration
- Différences de configuration
- Gestion et planification hors ligne
- Gestion des règles de sécurité des pare-feu
- Gestion des règles de sécurité des VPN
- Gestion SD-WAN
- Gestion des services de sécurité à valeur ajoutée
- Redondance et haute disponibilité
- Sauvegarde des fichiers de préférences pour les pare-feu
- API RESTful
- Mise à niveau du firmware
- Administration basée sur les rôles
- Gestion des points d'accès et des commutateurs

Surveillance

- État et santé des appareils
- État des licences et support
- Résumé des réseaux/menaces
- Centre d'alerte et de notification
- Journaux des événements
- Vue topologique

Analyse

- Activités basées sur les utilisateurs
- Utilisation des applications
- Visibilité entre les produits avec Capture Client
- Visualisation dynamique en temps réel
- Fonctionnalités d'exploration approfondie et de pivotement

Reporting

- Rapports PDF programmés - Niveau des locataires/groupes/appareils
- Rapports personnalisables
- Journalisation centralisée
- Rapport sur plusieurs menaces
- Rapport centré sur l'utilisateur
- Rapport sur l'utilisation des applications
- Rapports sur la bande passante et les services
- Reporting sur la bande passante par utilisateur

Licences et formules

Fonctionnalités	Essentielle	Avancée
Gestion de centaines d'appareils par locataire	Oui	Oui
Gestion multi-locataires	Oui	Oui
Inventaire des appareils	Oui	Oui
Envoi de règles au niveau du groupe	Oui	Oui
Groupe d'appareils	Oui	Oui
Modèles	Oui	Oui
Application et déploiement	Oui	Oui
Audit de configuration	Oui	Oui
Différences de configuration	Oui	Oui
Automatisation des flux de travail	Oui	Oui
API	Oui	Oui
Déploiement sans intervention	Oui	Oui
Planification des tâches	Oui	Oui

Fonctionnalités	Essentielle	Avancée
Sauvegarde/restauration	Oui	Oui
Mises à niveau du firmware	Oui	Oui
Gestion des points d'accès et des commutateurs	Oui	Oui
Nombre de jours de reporting des données	7 jours	365 jours
Tableau de bord au niveau des groupes/locataires	Oui	Oui
Capture ATP (au niveau des appareils)	Oui	Oui
Capture Threat Assessment (au niveau des appareils)	Oui	Oui
Visibilité et reporting au niveau des groupes	Oui	Oui
Rapports programmés (niveau des groupes d'appareils)	Oui	Oui
Analyse basée sur les utilisateurs	Non	Oui
Analyse des applications	Non	Oui
Analyse des menaces	Non	Oui
Exploration approfondie et pivotement	Non	Oui

Produit	Référence
SOLUTION NSM ESSENTIELLE POUR SOHO 250 1 AN	02-SSC-5219
SOLUTION NSM AVANCÉE POUR SOHO 250 1 AN	02-SSC-5213
SOLUTION NSM ESSENTIELLE POUR TZ 350 1 AN	02-SSC-5239
SOLUTION NSM AVANCÉE POUR TZ 350 1 AN	02-SSC-5231
SOLUTION NSM ESSENTIELLE POUR TZ 400 1 AN	02-SSC-5263
SOLUTION NSM AVANCÉE POUR TZ 400 1 AN	02-SSC-5257
SOLUTION NSM ESSENTIELLE POUR TZ 500 1 AN	02-SSC-5183
SOLUTION NSM AVANCÉE POUR TZ 500 1 AN	02-SSC-5177
SOLUTION NSM ESSENTIELLE POUR TZ 570 1 AN	02-SSC-4975
SOLUTION NSM AVANCÉE POUR TZ 570 1 AN	02-SSC-4963
SOLUTION NSM ESSENTIELLE POUR TZ 600 1 AN	02-SSC-5201
SOLUTION NSM AVANCÉE POUR TZ 600 1 AN	02-SSC-5195
SOLUTION NSM ESSENTIELLE POUR TZ 670 1 AN	02-SSC-5011
SOLUTION NSM AVANCÉE POUR TZ 670 1 AN	02-SSC-4999
SOLUTION NSM ESSENTIELLE POUR NS*a* 2600/NS*a* 2650 1 AN	02-SSC-5281
SOLUTION NSM AVANCÉE POUR NS*a* 2600/NS*a* 2650 1 AN	02-SSC-5275
SOLUTION NSM ESSENTIELLE POUR NS*a* 3600/NS*a* 3650 1 AN	02-SSC-5299
SOLUTION NSM AVANCÉE POUR NS*a* 3600/NS*a* 3650 1 AN	02-SSC-5293
SOLUTION NSM ESSENTIELLE POUR NS*a* 4600/NS*a* 4650 1 AN	02-SSC-5325
SOLUTION NSM AVANCÉE POUR NS*a* 4600/NS*a* 4650 1 AN	02-SSC-5319
SOLUTION NSM ESSENTIELLE POUR NS*a* 5600/NS*a* 5650 1 AN	02-SSC-5347
SOLUTION NSM AVANCÉE POUR NS*a* 5600/NS*a* 5650 1 AN	02-SSC-5341
SOLUTION NSM ESSENTIELLE POUR NS*a* 6600/NS*a* 6650 1 AN	02-SSC-5365
SOLUTION NSM AVANCÉE POUR NS*a* 6600/NS*a* 6650 1 AN	02-SSC-5359

Des références pluriannuelles et des contrats de support sont également disponibles. Pour une liste complète, veuillez contacter votre revendeur préféré ou contacter l'équipe commerciale SonicWall.

Navigateurs Internet

- Microsoft® Internet Explorer 11.0 ou une version ultérieure et la dernière version de Microsoft Edge, Mozilla Firefox, Google Chrome ou Safari.

Appareils gérés par NSM[1]

- Appliances de sécurité réseau SonicWall : SuperMassive 9000 Series[2], E-Class NSA, NS*sp* 12000 Series[2], NS*a* Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- Appliances virtuelles de sécurité réseau SonicWall : NSv Series
- SonicWall SonicWave, SonicPoint
- Commutateur SonicWall

[1] Prend en charge les pare-feu exécutant SonicOS version 6.x ou 7.x.
[2] 365 jours de reporting et 30 jours d'analyse non pris en charge.

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 en savoir plus, rendez-vous sur www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035 - États-Unis
Consultez notre site Internet pour plus d'informations.
www.sonicwall.com

Datasheet-NSM-US-COG-2114