SOPHOS

Les nouveautés de

Sophos Firewall

Principales nouvelles fonctionnalités de Sophos Firewall OS v21.5

Protection et performances accrues

Intégration de Sophos NDR Essentials avec Sophos Firewall

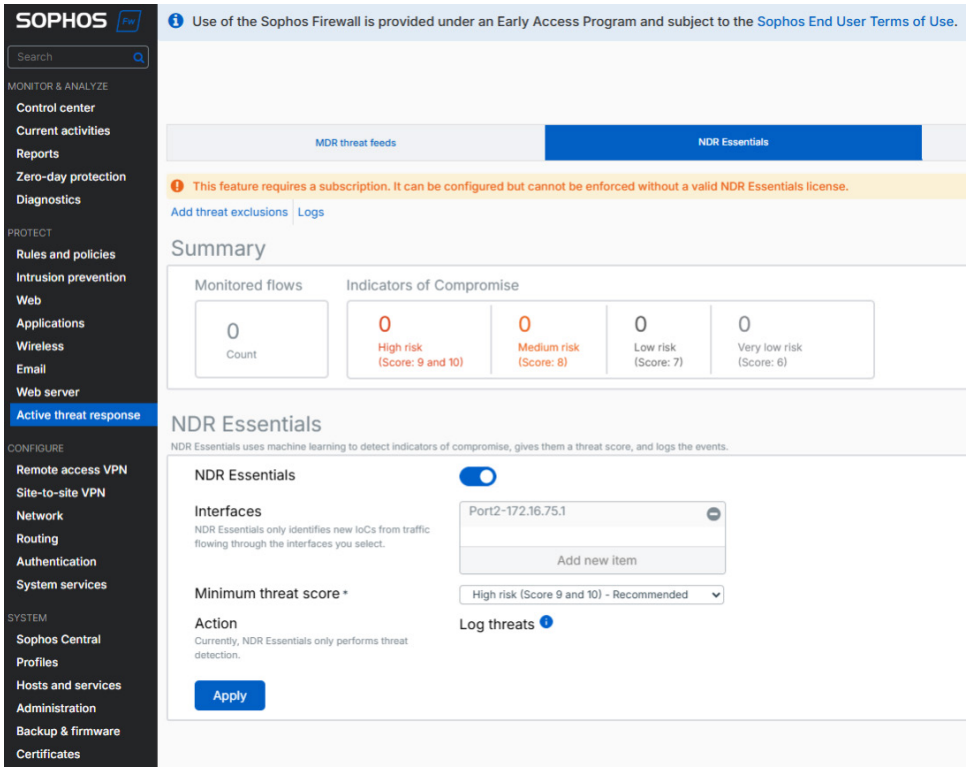
La fonctionnalité NDR (Network Detection and Response) représente une catégorie de produit de sécurité réseau conçue pour détecter un comportement de trafic anormal afin d'aider à identifier les adversaires actifs opérant sur le réseau. Les attaquants expérimentés parviennent aisément à échapper à la détection, mais ils doivent à un moment donné se déplacer ou communiquer hors du réseau pour mener à bien une attaque. La solution NDR est généralement installée au sein du réseau et utilise des capteurs qui surveillent et analysent le trafic réseau afin d'identifier ce type d'activité suspecte.

Les produits NDR existent depuis de nombreuses années et Sophos NDR fait partie de notre gamme de produits MDR/XDR depuis début 2023. Cependant, avec SFOS v21.5, nous intégrons une solution NDR dans Sophos Firewall, une première dans notre secteur, sans frais supplémentaires pour les clients Sophos Firewall doté de l'abonnement Xstream Protection.

L'intégration d'une solution NDR dans un pare-feu Next-Gen peut sembler une évidence, mais le défi consiste à le faire d'une manière qui n'affecte pas les performances du pare-feu, car l'analyse du trafic NDR nécessite une puissance de traitement importante. Par conséquent, nous avons adopté une approche novatrice consistant à déployer une solution NDR dans le Cloud Sophos pour soulager le pare-feu de cette lourde tâche.

Sophos Firewall v21.5 intègre à présent NDR Essentials, notre nouvelle plateforme NDR (Network Detection and Response) fournie depuis le Cloud. La solution utilise les dernières détections basées sur l'IA pour aider à identifier les adversaires actifs et partage ces informations à l'aide de l'API dédiée aux flux de menaces de Sophos Firewall dans le cadre de la fonctionnalité 'Réponse active aux menaces' pour vous tenir informé de toutes les détections et de leurs risques relatifs.

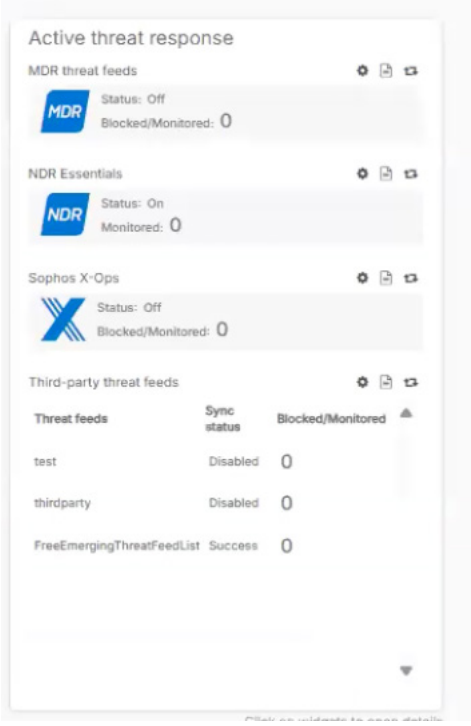
Comment ces nouvelles capacités fonctionnent-elles ? Sophos Firewall capture les métadonnées du trafic chiffré TLS et des requêtes DNS et envoie ces informations à NDR Essentials dans Sophos Cloud. Ensuite, les données sont analysées à l'aide de plusieurs moteurs IA. Il peut détecter les charges virales chiffrées malveillantes sans effectuer de déchiffrement TLS ainsi que les domaines nouveaux et inhabituels générés par des algorithmes qui sont souvent un indicateur majeur de compromission. L'extraction des métadonnées est effectuée par un nouveau moteur léger implémenté au niveau de Xstream FastPath et, par conséquent, elle n'est disponible que sur les pare-feux matériels de la série XGS. Les pare-feux virtuels, logiciels et Cloud pourraient bénéficier de cette capacité d'intégration NDR à l'avenir, mais pas dans la version 21.5.



Configurez et surveillez votre flux NDR Essentials sous « Réponse active aux menaces » en parallèle de vos autres flux de menaces.

Le nouveau flux de menaces NDR Essentials est géré avec vos autres flux de menaces (Sophos X-Ops, MDR et flux tiers) dans la zone dédiée « Réponse active aux menaces » du pare-feu, comme indiqué dans la capture d'écran ci-dessus. L'installation est simple : actionnez le switch approprié pour l'activer, sélectionnez ensuite les interfaces internes à surveiller, définissez un seuil minimum en matière de risque de détection, et le tour est joué !

Les détections NDR Essentials sont notées sur une échelle allant de 1 (risque faible) à 10 (risque le plus élevé). Vous décidez le score de risque qui définit le seuil d'une alerte en fonction de votre environnement. La valeur par défaut recommandée est celle à haut risque (9-10). Toutes les détections dont le score est supérieur ou égal à 6 seront journalisées, mais seules celles qui atteignent ou dépassent votre seuil déclencheront des notifications et seront affichées sous forme d'alertes au niveau du nouveau widget du tableau de bord de votre Centre de contrôle. Les détections notées moins de 6 peuvent être de faux positifs et ne seront donc pas journalisées. Aucune détection NDR Essentials ne sera bloquée pour le moment, mais cette possibilité pourrait être une option proposée à l'avenir. Toutes les détections sont entièrement accessibles via le rapport « Réponse active aux menaces » disponible à la fois en mode on-box et via Sophos Central Firewall Reporting.



Toute détection de NDR Essentials atteignant ou dépassant votre seuil de risque est affichée dans le widget révisé du Centre de contrôle.

Si vous souhaitez des informations plus détaillées en matière de détection et des capacités de chasse aux menaces supplémentaires, nous vous encourageons vivement à consulter Sophos XDR (Extended Detection and Response) avec l'implémentation complète de Sophos NDR avec la nouvelle console d'investigation NDR. Vous pouvez également envisager d'utiliser notre service Managed Detection and Response (MDR) complet 24 h/24 et 7j/7. Tous ces produits et services fonctionneront mieux ensemble avec vos pare-feux Sophos Firewall.

Authentification unique (SSO) pour le VPN d'accès à distance

Authentification unique (SSO) Entra ID (Azure AD) avec Sophos Connect et le portail VPN

L'une des fonctionnalités que vous nous avez le plus demandées facilite l'accès à distance par VPN pour les utilisateurs finaux, leur permettant ainsi d'utiliser les identifiants du réseau de leur entreprise avec le client Sophos Connect et le portail VPN du pare-feu. L'intégration de l'authentification unique (SSO) Entra ID (Azure AD) avec Sophos Connect et le portail VPN est désormais incluse dans SFOS v21.5. Cela offre une intégration Cloud-Native avec les protocoles standard du secteur OAuth 2.0 et OpenID Connect pour une expérience transparente. Une prise en charge du client Sophos Connect 2.4 (et versions ultérieures) au niveau de Microsoft Windows est également disponible.

Autres améliorations au niveau du VPN et de l'évolutivité

Améliorations de l'interface utilisateur et de la convivialité : les types de connexion ont été renommés en passant de « site-à-site » (site-to-site) à « basé sur des stratégies » (policy-based), et les interfaces de tunnel ont été renommées en utilisant désormais le terme « basé sur le routage » (route-based) pour les rendre plus intuitives.

Validation améliorée du pool d'allocation d'adresses IP : accès VPN à distance via SSLVPN, IPsec, L2TP et PPTP pour éliminer les conflits IP potentiels.

Application stricte du profil : sur les profils IPsec qui excluent les valeurs par défaut pour garantir un handshake réussi, éliminant ainsi la fragmentation potentielle des paquets et des tunnels qui ne parviennent pas à s'établir correctement.

Évolutivité du VPN basée sur le routage : la capacité VPN basée sur le routage est doublée avec une prise en charge jusqu'à 3 000 tunnels.

Évolutivité de la solution SD-RED : les produits Sophos Firewall prennent désormais en charge jusqu'à 1 000 tunnels RED site-à-site et jusqu'à 650 périphériques SD-RED.

Sophos DNS Protection :

Sophos DNS Protection en toute simplicité

L'année dernière, nous avons lancé notre service de protection DNS et l'avons rendu gratuit pour tous les clients de pare-feu sous licence Xstream Protection. Avec cette version, Sophos DNS Protection bénéficie d'une intégration plus poussée avec Sophos Firewall sous la forme d'un nouveau widget dans le Centre de contrôle pour indiquer l'état du service, ainsi que de nouvelles informations en matière de dépannage via la journalisation et les notifications, et un nouveau tutoriel pas à pas sur la façon de configurer facilement Sophos DNS Protection.

Améliorations en matière de gestion optimisée et de convivialité

Comme pour chaque nouvelle version de Sophos Firewall, cette édition comprend des améliorations en matière de convivialité qui optimisent la gestion au quotidien.

Des colonnes de tableau redimensionnables : une fonctionnalité demandée depuis longtemps, de nombreux écrans d'état et de configuration du pare-feu prennent désormais en charge des largeurs de colonne redimensionnables qui sont conservées dans la mémoire du navigateur pour les visites ultérieures. De nombreux écrans tels que SD-WAN, NAT, SSL, hôtes et services, et VPN site à site, bénéficient tous de cette nouvelle fonctionnalité.

Recherche en texte libre étendue : les routes SD-WAN permettent désormais de rechercher par nom de route, ID, objets et valeurs d'objet comme les adresses IP, les domaines ou d'autres critères. Les règles ACL locales prennent désormais également en charge la recherche par nom d'objet et valeur d'objet, notamment la recherche basée sur le contenu.

Configuration par défaut : à la demande générale, les règles de pare-feu et le groupe de règles par défaut précédemment créés lors de la configuration d'un nouveau pare-feu ont été supprimés, seules la règle réseau par défaut et les règles MTA étant fournies lors de la configuration initiale. Le groupe de règles de pare-feu par défaut et les sondes de la passerelle par défaut pour les passerelles personnalisées sont tous deux définis sur « Aucun » (None) par défaut.

Nouvelle police : l'interface utilisateur de Sophos Firewall arbore désormais une nouvelle police plus claire, plus propre et plus nette pour une meilleure lisibilité et des performances améliorées.

Autres améliorations

Licences virtuelles, logicielles et Cloud : toutes les licences virtuelles, logicielles et Cloud (BYOL) de Sophos Firewall n'ont plus de limites de RAM. Les licences sont désormais strictement limitées par le nombre de cœurs et n'ont aucune restriction en termes de RAM.

Limite de taille de fichier plus grande dans le WAF : prise en charge d'une limite de taille de fichier de requête (upload) configurable pour le WAF (Web Application Firewall), qui peut désormais analyser des fichiers jusqu'à 1 Go.

La sécurité dès la conception (Secure by design) : nous améliorons continuellement la sécurité de Sophos Firewall et, dans cette version, nous ajoutons une collecte de télémétrie en temps réel pour signaler toute modification inattendue des fichiers principaux du système d'exploitation à l'aide d'une validation de hachage sécurisée. Cette possibilité permettra à nos équipes de surveillance d'identifier de manière proactive les incidents de sécurité potentiels avant qu'ils ne deviennent un véritable problème.

Assouplissement de la délégation du préfixe DHCP : prise en charge désormais des préfixes /48 à /64, améliorant ainsi l'interopérabilité avec les FAI. Les annonces de routeur (RA : Router Advertisements) et le serveur DHCPv6 sont désormais également activés par défaut.

Détection du chemin MTU : cette fonctionnalité résoudra les erreurs de déchiffrement TLS dues à la dernière prise en charge de l'échange de clés ML-KEM (Kyber) dans les navigateurs. Le moteur d'inspection approfondie des paquets (DPI) de Sophos Firewall détectera et ajustera désormais automatiquement le MTU pour chaque flux, garantissant des performances optimales en fonction des conditions spécifiques du réseau.

NAT64 (trafic IPv6 vers IPv4) : NAT64 est pris en charge pour le trafic IPv6 vers IPv4 en mode proxy explicite. Dans ce mode, les clients IPv6 uniquement peuvent accéder aux sites Web IPv4. Le pare-feu prend en charge également un proxy amont IPv4 uniquement pour les clients Ipv6.

Sophos France
Tél. : 01 34 34 80 00
Email : partners@sophos.fr

© Copyright 2025. Sophos Ltd. Tous droits réservés.
Immatriculée en Angleterre et au Pays de Galles N° 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Royaume-Uni.
Sophos est la marque déposée de Sophos Ltd. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.

2025-03-31 FR (DD)

SOPHOS