SOPHOS

Les nouveautés de

Sophos Firewall

Principales nouvelles fonctionnalités de Sophos Firewall OS v21

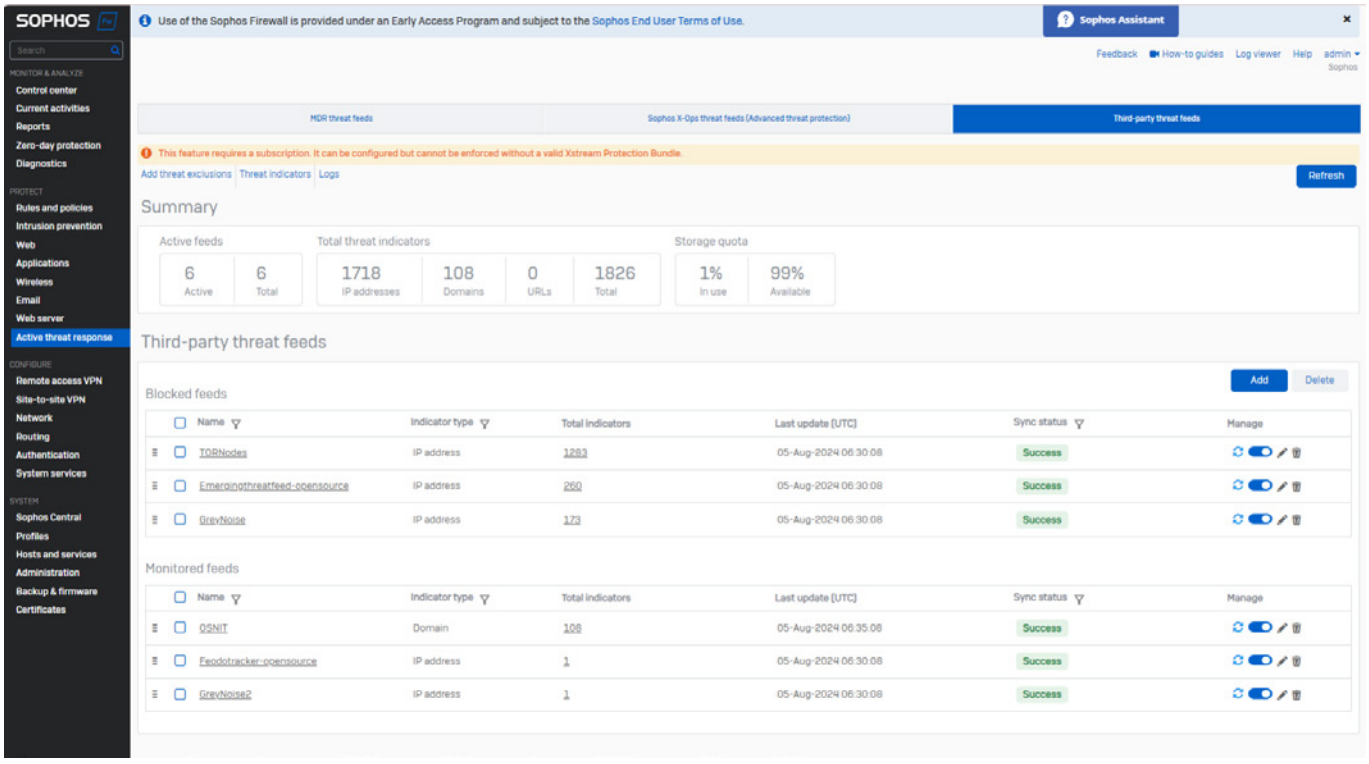
Une protection supplémentaire :

flux de renseignements sur les menaces tiers

La réponse active aux menaces (Active Threat Response), ajoutée dans la version 20, a introduit un nouveau framework de flux de renseignements sur les menaces dans Sophos Firewall. La prise en charge initiale concernait les flux dynamiques de renseignements sur les menaces de Sophos X-Ops, et Sophos MDR permettait au pare-feu de répondre automatiquement en bloquant l'accès à toute menace publiée via ce framework.

Bien qu'il s'agisse là du besoin essentiel de la plupart des clients, il existe néanmoins des régions en particulier et certains marchés verticaux où des flux de renseignements sur les menaces personnalisés et spécifiques sont privilégiés ou requis. Notre communauté de partenaires, nos fournisseurs de centre d'opérations de sécurité (SoC) et de nombreux clients ont également manifesté leur intérêt pour une capacité extensible en matière de flux de menaces afin de prendre en charge les solutions et services de détection et de réponse aux menaces, existants ou nouveaux.

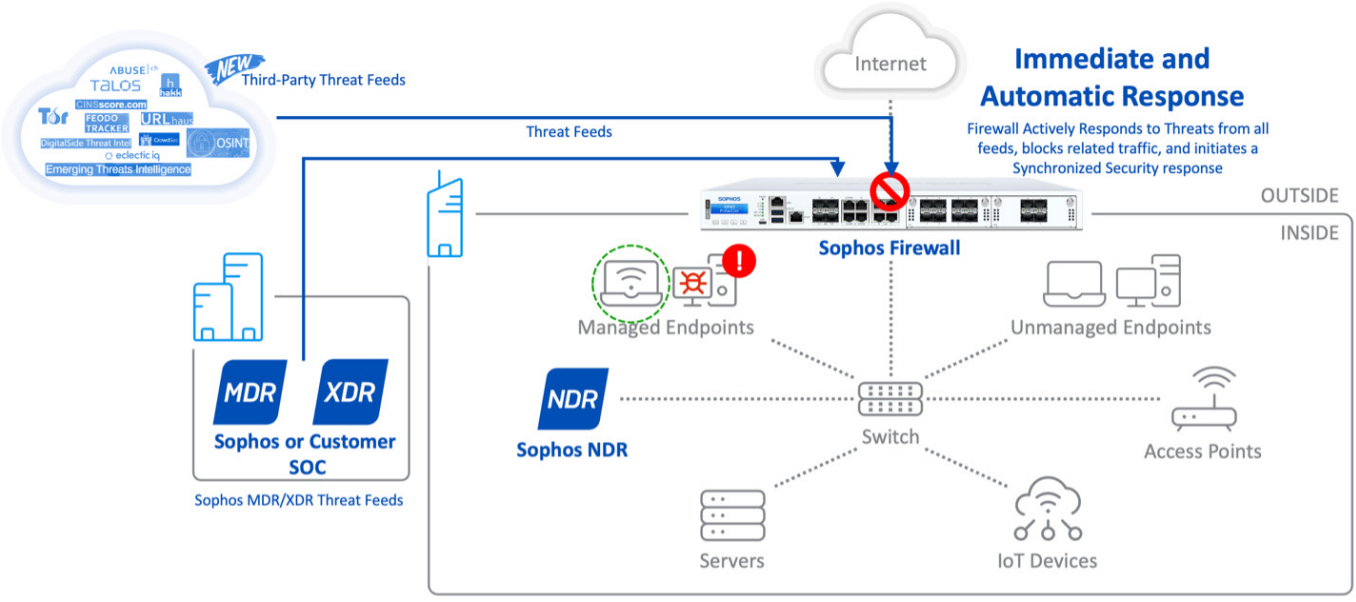
Pour permettre ces cas d'usage, Sophos Firewall v21 étend désormais son framework pour prendre en charge les flux de renseignements sur les menaces tiers. Vous pouvez ainsi facilement ajouter des flux de menaces verticaux ou personnalisés supplémentaires au pare-feu. Ces flux surveilleront et répondront de la même manière automatique, bloquant toute activité associée, au niveau de tous les moteurs de sécurité et ce sans règle de pare-feu supplémentaire.



Configurez et surveillez vos flux de menaces tiers à partir du menu Réponse active aux menaces.

Cette nouvelle version prend également en charge les services MSP, offrant ainsi aux partenaires Sophos la possibilité d'intégrer cette fonctionnalité à leur propre service MDR (Managed Detection and Response), pour en tirer le plein potentiel. Sophos Firewall prend même en charge les solutions MDR concurrentes afin de s'intégrer plus étroitement à l'environnement de détection et de réponse aux menaces des clients.

Par exemple, si le pare-feu identifie un appareil communiquant avec un serveur C2 publié via l'une des sources du flux de menaces, Sophos Firewall lance automatiquement la fonction de Réponse active aux menaces pour bloquer toutes les requêtes et le trafic tentant de contacter ce serveur à partir de n'importe quel hôte du réseau et assignera à l'appareil compromis un statut Security Heartbeat rouge. Aucune configuration de règle de pare-feu n'est nécessaire.



La prise en charge des flux de renseignements sur les menaces tiers étend la réponse aux menaces actives

Une large gamme de flux de menaces spécifiques et verticaux sont pris en charge, notamment ceux fournis par des organismes de sécurité, des consortiums industriels et des sources de renseignements sur les menaces communautaires ou open source.

- Cisco Talos
- GreyNoise Intelligence
- Abuse.ch/URLhaus
- Hakk Solutions
- OSINT (Open-source Intelligence)/DigitalSide
- CINS Score
- CrowdSec
- EclicticIQ
- Feodo Tracker

Et bien plus encore !

Sécurité Synchronisée pour tous les flux de menaces

La Réponse active aux menaces déclenche la même réponse au sein de la Sécurité Synchronisée que toute autre condition de type Security Heartbeat 'rouge'. Cette mesure comprend l'application de toutes les règles de pare-feu qui contiennent des conditions Heartbeat. Le pare-feu coordonne également la protection contre les mouvements latéraux, en informant tous les postes sains protégés par Sophos Endpoint qu'il existe un hôte compromis sur le réseau local afin qu'ils bloquent le trafic provenant de celui-ci.

Évolutivité améliorée

Sophos Firewall v21 inclut une série d'améliorations concernant la mise en réseau, pour offrir des niveaux de performances accrus et une plus grande évolutivité pour de nombreuses entreprises :

Amélioration de la haute disponibilité

Résilience accrue, transitions transparentes et interruptions de service réduites : les déploiements en haute disponibilité sont améliorés grâce au basculement (failover) transparent des routes dynamiques. Le basculement des tunnels SD-RED a également été considérablement perfectionné. Désormais, les tunnels peuvent être rétablis en quelques secondes après un basculement HA, ce qui permet de réduire les interruptions. L'amélioration des interactions avec les domaines Active Directory lors des basculements HA garantit également des transitions plus fluides.

Améliorations VPN IPsec

Niveau de performance IPsec de site-à-site amélioré : les passerelles distantes basées sur FQDN ont été optimisées pour améliorer l'évolutivité des déploiements distribués. En outre, il est désormais possible d'utiliser les relais DHCP au niveau des interfaces XFRM pour le trafic vers les serveurs DHCP déployés derrière un pare-feu. Mais ce n'est pas tout : les déploiements RBVPN bénéficient maintenant d'une disponibilité (up-time) multipliée par 20 (max) au niveau de l'interface XFRM, minimisant ainsi considérablement les perturbations lors de situations de type tunnel flapping et des redémarrages (reboots).

Amélioration de la gestion : les options d'activation et de désactivation groupées sont désormais disponibles pour les connexions. Le filtrage amélioré au niveau de la page de gestion VPN consolide désormais les informations sur plusieurs pages. De plus, une vue spécifique aux interfaces XFRM a été ajoutée sur la page « Interfaces » pour un filtrage aisé des interfaces RBVPN.

Amélioration de l'authentification et de la protection Web

Amélioration de l'authentification : l'intégration de Google Workspace via le client LDAP et le SSO de Google Chromebook sont désormais pris en charge. Les performances en matière de gestion des pics de connexions ont été multipliées par 4 (max) pour Radius SSO, STAS et Synchronized User ID afin de permettre la gestion de milliers de demandes de connexion simultanées, même dans plusieurs environnements SSO (mélange de STAS, Radius SSO et Synchronized User ID). De plus, la prise en charge a été ajoutée pour une expérience AD SSO transparente lorsque HSTS est activé, permettant ainsi des handshakes Kerberos et NTLM via HTTP ou HTTPS.

Amélioration des performances de la protection Web : l'application de SafeSearch, des restrictions YouTube, des domaines de connexion Google App et des restrictions des locataires Azure AD permet désormais de réduire considérablement la charge exercée sur le système, et donc d'améliorer les niveaux de performance.

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.

Prise en charge des certificats Let's Encrypt : la prise en charge des certificats Let's Encrypt, réclamée depuis longtemps, permet le déploiement et le renouvellement automatiques des certificats sur la base des demandes de signature de certificats (CSR). Les certificats Let's Encrypt sont pris en charge pour une diversité d'application : pare-feu d'application web (WAF), protocole SMTP, configuration TLS, connexion aux hotspots, console d'administration web, portail utilisateur, portail captif, portail VPN et portail SPX.

Gestion des routes statiques : les utilisateurs peuvent cloner des routes statiques, les activer ou les désactiver et ajouter des descriptions. Il existe désormais une option de routage blackhole et la prise en charge du multi-chemin à coût égal (ECMP : Equal-Cost Multi-Path) pour l'équilibrage de charge.

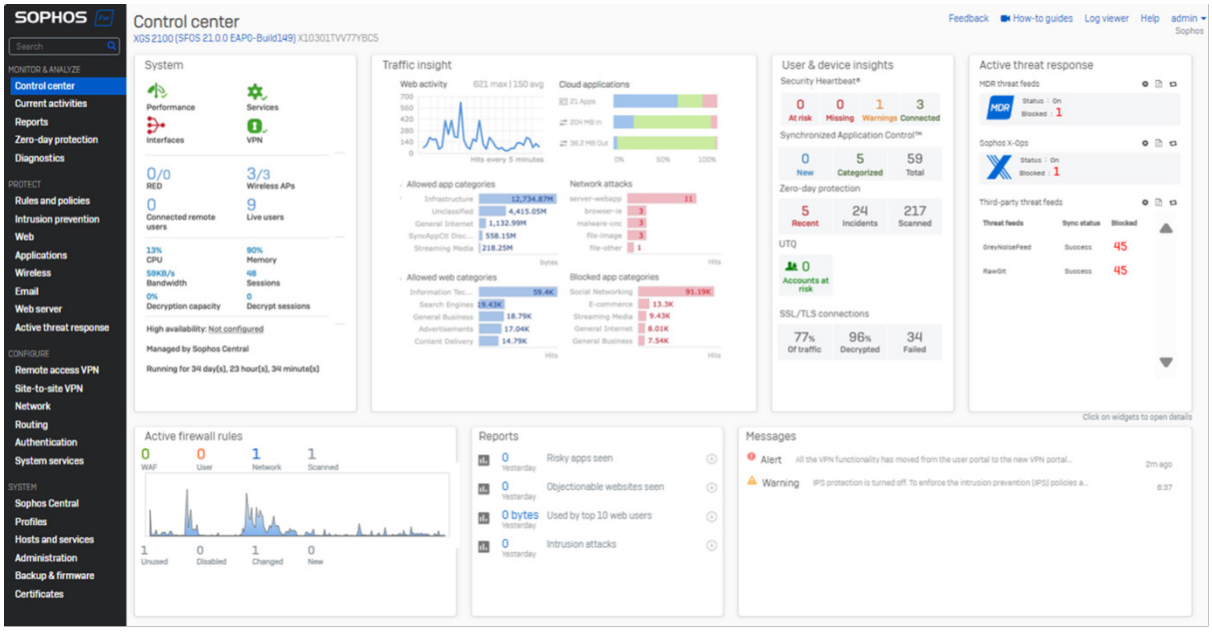
Référence d'objet étendue : offre une visibilité accrue sur les références des objets réseau (utilisation) pour les interfaces, les zones, les passerelles et les profils SD-WAN. Cette fonctionnalité prend également en charge l'API XML pour récupérer le nombre de références d'objets (usage/utilisation), offrant ainsi une visibilité sur les objets inutilisés.

Configuration du VPN améliorée : le pare-feu prend désormais en charge les recherches basées sur du texte libre et de la valeur dans les configurations VPN telles que le réseau, le sous-réseau et les utilisateurs pour l'accès à distance et les VPN de site à site.

Routage dynamique : cette nouvelle option permet de redistribuer les routes BGP dans OSPFv3.

Amélioration du Centre de contrôle avec des affichages par fiche dédiée : le Centre de contrôle de Sophos Firewall a été repensé avec de nouveaux affichages par fiches dédiées pour une meilleure visibilité des événements et des données importantes du réseau. Une toute nouvelle fiche dédiée pour la Réponse active aux menaces consolide les informations sur les menaces provenant de Sophos MDR, de Sophos X-Ops et des flux de menaces tiers dans une section unique et facile à visualiser.

Console d'administration Web repensée et plus réactive : la console d'administration Web de Sophos Firewall intègre le dernier guide de style de Sophos, identique à Sophos Central, ce qui lui confère un nouveau design et une réactivité sensiblement accrue, pour une expérience de gestion optimisée.



Le Centre de contrôle modernisé de Sophos Firewall offre de nouveaux affichages par fiches dédiées et un design rafraichi.

Mises à niveau plus fluides

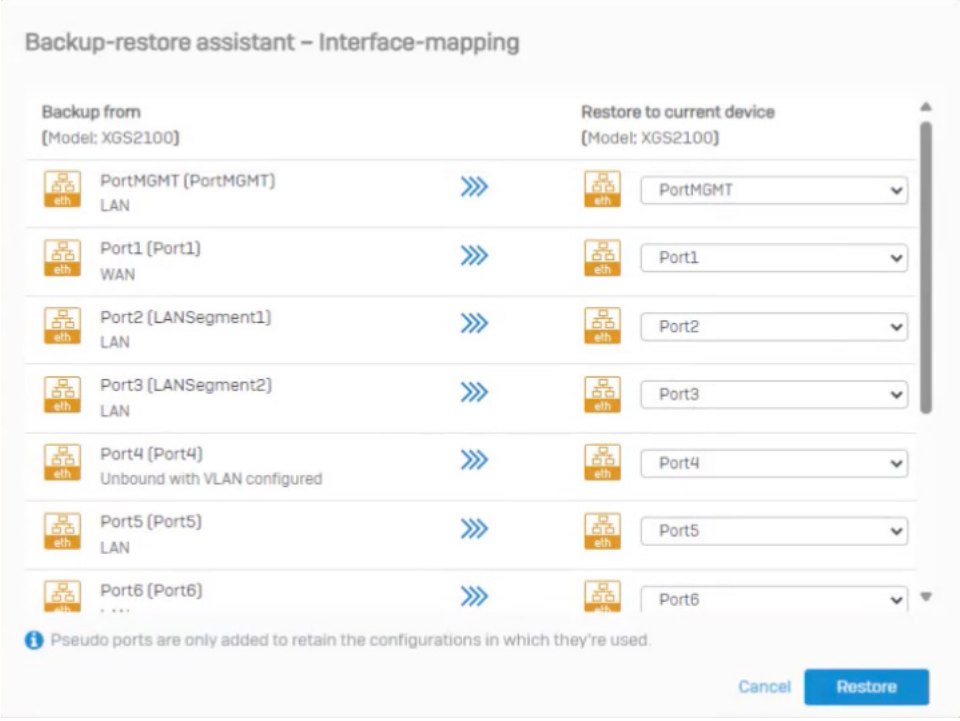
Sophos Firewall v21 inclut des fonctionnalités particulièrement utiles, initialement introduites dans la v20 MR2, qui facilitent les mises à niveau des pare-feux vers les derniers modèles de la série XGS.

Sauvegarde et restauration any-to-any avec mappage des ports

Le nouvel assistant de sauvegarde et de restauration de Sophos Firewall permet de restaurer facilement les sauvegardes de configuration du pare-feu sur une autre appliance de pare-feu grâce à des options de mappage d'interface flexibles.

Il est ainsi facile de mettre à niveau les pare-feux Sophos Firewall de la série XG vers la série XGS, ou un modèle de la série XGS vers un autre modèle de la série XGS, ou encore même de migrer vers ou depuis des appliances logicielles ou virtuelles. Cela signifie également que vous pouvez aisément migrer les interfaces vers des ports à plus haut débit sur un nouveau pare-feu.

Pour alléger votre travail et éviter d'avoir à répéter les mêmes configurations, vous pouvez également exporter un modèle de configuration à partir d'une appliance virtuelle, puis le restaurer sur plusieurs déploiements matériels ou virtuels, afin de simplifier une mise à niveau de multiples appareils.



Mappez aisément les interfaces entre l'ancienne et la nouvelle appliance

Pour plus d'informations sur la mise à niveau et le nouvel assistant de sauvegarde/restauration, consultez cet article de blog.

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

2024-10-16 FR (PC)

SOPHOS