**Sophos dévoile la nouvelle série de pare-feu XGS, dotée de performances accrues pour le traitement des flux chiffrés**

*Une nouvelle étude de Sophos montre une hausse continue du nombre d’attaques menées par des cybercriminels utilisant le chiffrement des flux*

Oxford, le 21 avril 2021 – [**Sophos**](https://www.sophos.com/fr-fr.aspx) **dévoile la nouvelle série de pare-feu XGS qui offre des performances inégalées et fournit une protection avancée contre les cybermenaces. Les nouveaux dispositifs matériels sont dotés des meilleures fonctionnalités d’inspection de la couche de transport sécurisée (ie : TLS : Transport Layer Sercurity) du marché, intégrant un support natif du protocole TLS version 1.3. Ces modèles sont jusqu’à cinq fois plus rapides que ceux actuellement disponibles sur le marché.**

«  Les dispositifs pare-feu Sophos de la série XGS sont une nouvelle étape dans notre histoire et constitue une énorme opportunité pour le marché EMEA, » déclare Kevin Isaac, senior vice-président chez Sophos. « L’année écoulée a vu une incroyable accélération de la numérisation des échanges. Le recours massif au télétravail a engendré à la fois de nouveaux risques, mais également de nouvelles opportunités. Les entreprises ont besoin de protections puissantes et de dernière génération capables de les défendre au quotidien contre des menaces telles que les ransomwares et autres malwares. »

« Auparavant, les équipes en charge de la sécurité du système d’information ignoraient l’inspection des flux de données chiffrées par crainte d’écrouler les performances de fonctionnement de leurs équipements intermédiaires ou le dysfonctionnement d’un flux de communication. Aujourd’hui, les entreprises peuvent compter sur la nouvelle série XGS conçue pour répondre aux nouveaux enjeux de l’Internet où transitent des flux chiffrés. Les équipes d’exploitation peuvent aisément inspecter ces flux et détecter ce qui était auparavant obfusqué, sans réduction de performance, » déclare Dan Schiappa, Chief Product Officer chez Sophos.

**Les cybercriminels utilisent de plus en plus les mécanismes de chiffrement offerts par la couche de transport sécurisée TLS ( Transport Layer Security) pour échapper à la détection.**

Selon [le rapport publié par Sophos](file:///C%3A%5CUsers%5CBarbara.Coumaros%5CAppData%5CLocal%5CMicrosoft%5CWindows%5CINetCache%5CContent.Outlook%5CJRWT1YRG%5Cxxxx), près de 45 % des malwares détectés par Sophos entre janvier et mars 2021 ont utilisé des mécanismes de chiffrement pour dissimuler des communications malveillantes. Il s’agit d’une augmentation drastique par rapport aux [23 % mentionnés par Sophos](https://news.sophos.com/en-us/2020/02/18/nearly-a-quarter-of-malware-now-communicates-using-tls/) dans le cadre d’une étude publiée début 2020.

Sophos a également constaté l’utilisation de couches de communication sécurisée (TLS) pour mener des attaques de rançongiciel, durant l’année écoulée ; en particulier lorsque ces ransomwares sont déployés manuellement par un attaquant. La majorité des malwares de compromission initiaux de type *loader*, *dropper,* ou encore *installer* contenus dans des documents, utilise des flux chiffrés, comme l’a montré BazarLoader, GoDrop ou ZLoader.

« La démocratisation des mécanismes de chiffrement a contribué à l’amélioration de la protection des communications sur Internet. Mais ces mécanismes ont rendu la tâche plus facile aux attaquants lorsqu’ils téléchargent et déploient des modules malveillants ou exfiltrent des données sensibles.  » déclare Dan Schiappa. « Les attaquants tirent parti de services web et cloud protégés par les mécanismes de chiffrement pour installer des malwares, leur transmettre des commandes et les contrôler.  »

**Une protection renforcée contre les menaces**

La protection est alimentée par la recherche sur les menaces issue de SophosLabs Intelix, et basée sur des PetaOctets de données traitées par les SophosLabs. Les fichiers suspects sont exécutés dans un environnement virtuel sécurisé de SophosLabs Intelix, afin d’en analyser le comportement et de collecter des informations sur ceux-ci.

Les nouveaux processeurs réseau Xstream intégrés à l’appliance accélèrent automatiquement les flux de données de confiance. Par exemple, les flux liés aux solutions logicielles ‘as-a-Service’ (SaaS), au SD-WAN et aux applications hébergées dans le cloud, libérant d’avantages de ressources pour les flux nécessitant une inspection profonde des paquets (*deep packet inspection*). Ceci réduit la latence et améliore les performances des applications métiers et des applications essentielles, en particulier celles nécessitant des flux de communication en temps réel. De plus les processeurs réseau Xstream sont reprogrammables, ce qui permet à Sophos de mettre à jour la politique d’identification des flux. La modularité et les nouvelles interfaces permettent aux dispositifs d’évoluer tout au long du cycle d’exploitation, selon les besoins du client, garantissant ainsi une meilleure pérennité de l’investissement.

Grâce à son tableau de bord, Sophos Firewall offre la possibilité aux administrateurs de voir l’ensemble des flux chiffrés et d'implémenter, d'un simple clic de souris, des exceptions pour les flux ne nécessitant pas de déchiffrement. Afin d’optimiser la performance, les SophosLabs alimentent la liste des flux à exclure du déchiffrement.

Le nouveau matériel et le logiciel de la série Sophos Firewall XGS intègrent les solutions de cybersécurité next-gen de Sophos dès aujourd’hui. Ils s’administrent depuis [Sophos Central](https://www.sophos.com/fr-fr/products/sophos-central.aspx) basée dans le cloud. Grâce à la sécurité synchronisée, l'ensemble des briques fonctionnelles de cybersécurité s'intègre dans un écosystème complet. Il permet de détecter des menaces et de réagir dynamiquement pour les circonscrire et les éradiquer. Leur intégration aux services [Sophos Managed Threat Response](https://www.sophos.com/fr-fr/products/managed-threat-response.aspx) (MTR) contribue à renforcer encore la protection au moyen d’analyses effectuées par des êtres humains afin de bénéficier d’une détection des menaces et d’une réponse apportée en cas d’incident 24h/24 et 7j/7.

**Disponibilité**

Les appliances pare-feu de la série XGS et la plupart des dispositifs 1U montées sur rack de Sophos sont disponibles dès aujourd’hui, exclusivement via le réseau de distribution de Sophos, qui se compose de plus de 53 000 partenaires et fournisseurs de services managés (MSP). Ces modèles conviennent parfaitement aux petites, moyennes et grandes entreprises. Ils constituent une solution de sécurité réseau tout-en-un avec un excellent rapport prix/performance et diverses options de connectivité additionnelles. Des modèles supplémentaires conçus pour les environnements périphériques de grandes entreprises, qui nécessitent un rendement maximal pour des configurations réseau plus complexes, seront disponibles à l’achat au cours des semaines à venir. Le système de licences simplifiées inclut une offre groupée qui comprend la protection associée à un support renforcé afin d’offrir une protection optimale au meilleur prix.

**À propos de Sophos**

En tant que leader mondial en solution de cybersécurité Next-Gen, Sophos protège plus de 400 000 entreprises, de toutes tailles et dans plus de 150 pays, contre les cybermenaces actuelles les plus avancées. Développées par les SophosLabs, une équipe présente dans le monde entier et spécialisée dans le renseignement sur les menaces et la science des données, les solutions Cloud-Native et basées sur l'IA de Sophos protègent les systèmes endpoint (les ordinateurs portables, les serveurs et les périphériques mobiles) ainsi que les réseaux contre les techniques de cyberattaque évolutives, notamment les ransomwares, les malwares, les exploits, l'exfiltration de données, le phishing, et bien plus encore. Sophos Central, la plateforme de management Cloud-Native, intègre l'ensemble des produits Next-Gen de Sophos, y compris la solution Intercept X endpoint et le pare-feu XG Next-Gen, via un système unique de « sécurité synchronisée » accessible via un ensemble d'API. Sophos commercialise ses produits et services exclusivement par l’intermédiaire d’un réseau mondial regroupant plus de 53 000 partenaires et fournisseurs de services gérés (MSP : Managed Service Provider). Sophos met également ses technologies commerciales innovantes à la disposition des particuliers via Sophos Home. Le siège de l’entreprise est basé à Oxford, au Royaume-Uni. Plus d'informations sont disponibles sur [www.sophos.com](http://www.sophos.com).

**Contact presse :**

Square Egg Communications, Sandra Van Hauwaert, sandra@square-egg.be, GSM 0497251816.