LISTE DES FONCTIONNALITÉS

Liste des fonctionnalités Sophos Firewall

Sophos Firewall

Avantages principaux

- L'architecture Xstream offre des niveaux exceptionnels de visibilité, de protection et de performances grâce au traitement des paquets basé sur les flux.
- L'inspection TLS Xstream offre des performances élevées, la prise en charge du protocole TLS 1.3 sans baisse des performances, des stratégies de niveau entreprise indépendantes des ports avec des exceptions prédéfinies, un tableau de bord offrant une visibilité inégalée et des fonctionnalités de résolution des problèmes de compatibilité
- Xstream DPI Engine fournit une analyse du flux (stream scanning) pour IPS, AV, Web, ainsi que le contrôle applicatif et l'inspection TLS dans un moteur à haute performance unique
- Xstream Network Flow FastPath garantit une accélération du trafic fiable intelligente et basée sur des politiques, de manière automatique
- Xstream SD-WAN fournit une sélection des liens basée sur les performances avec re-routage à impact nul, surveillance SD-WAN, outils d'orchestration SD-WAN multi-sites et accélération FastPath du trafic des tunnels VPN IPsec
- Une interface utilisateur spécialement conçue avec un centre de contrôle interactif utilisant des indicateurs tricolores (rouge, jaune, vert) pour repérer instantanément les éléments qui nécessitent une attention particulière
- Le Centre de contrôle offre des informations instantanées sur l'état d'intégrité des endpoints, les applications Mac et Windows non identifiées, les applications Cloud et le Shadow IT, les charges utiles suspectes, les utilisateurs à risque, les menaces avancées, les attaques réseau, les sites Web inappropriés, et bien plus encore
- Une navigation optimisée en deux clics vers n'importe quelle destination grâce à la recherche intelligente
- Le widget des stratégies du Centre de contrôle surveille l'activité des politiques de relatives à l'entreprise, aux utilisateur et au réseau, et assure le suivi des stratégies inutilisées, désactivées, modifiées et nouvelles
- Le modèle de politiques unifié combine toutes les règles d'inspection de pare-feu, NAT et TLS sur un seul écran avec des options de regroupement, de filtrage et de recherche
- Une gestion optimisée des règles de pare-feu pour les grands ensembles de règles avec regroupement automatique et manuel personnalisé, affichage instantané des informations lors du survol du curseur et indicateurs d'application
- Toutes les règles de pare-feu fournissent un résumé clair des mesures de sécurité et de contrôle appliquées pour AV, sandboxing, IPS, web, appli, régulation du trafic (QoS) et Heartbeat
- Les stratégies prédéfinies relatives à l'IPS, au Web, aux applications, au TLS et à la régulation du trafic (QoS) permettent d'accélérer la configuration et de simplifier le paramétrage dans les scénarios de déploiement courants (par exemple, CIPA, politiques types sur le lieu de travail, etc.)
- La fonction Sophos Security Heartbeat™ connecte les postes protégés par Sophos au pare-feu pour partager l'état d'intégrité et les données télémétriques, permettant ainsi l'identification instantanée des postes compromis ou présentant des problèmes d'intégrité
- La fonction de réponse active aux menaces identifie, bloque et répond automatiquement aux adversaires actifs à partir des flux de menaces fournis par les SophosLabs, les analystes MDR ou des tiers
- La fonction de contrôle synchronisé des applications identifie, classe et active automatiquement le contrôle de toutes les applications Mac/Windows inconnues sur le réseau
- La Visibilité sur les application Cloud permet de détecter instantanément les activités de type Shadow IT et offre une régulation du trafic en un clic
- L'outil de simulation de politiques permet de simuler et de tester des règles de pare-feu et des politiques Web par utilisateur, adresse IP et heure de la journée

SOPHOS

- Les principes «Secure by Design» garantissent une protection renforcée du pare-feu contre les attaques
- API de configuration pour toutes les fonctionnalités d'intégration RMM/PSA
- L'intégration NDR dans le cloud améliore la détection des adversaires actifs
- Une passerelle ZTNA est intégrée dans chaque pare-feu pour faciliter l'accès sécurisé aux applications où que vous soyez
- La gestion et le reporting multi-pare-feux dans le Cloud avec Sophos Central permettent de gérer les stratégies de groupe et d'accéder à tous vos produits de sécurité Sophos depuis une seule console
- L'assistant de configuration simplifié permet un déploiement rapide prêt à l'emploi en quelques minutes seulement
- Déploiement et configuration zero touch dans Sophos Central pour les nouveaux pare-feux
- Intégration transparente avec Sophos MDR et XDR

Module 'Base Firewall'

Gestion générale

- Interface utilisateur simplifiée et dédiée, et gestion des règles de pare-feu pour les grands ensembles de règles avec regroupement, fonction de visualisation rapide des règles et indicateurs d'application
- Prise en charge de l'authentification à deux facteurs (mot de passe à usage unique) pour l'accès administrateur, le portail utilisateur, l'IPsec, le VPN SSL et le WAF
- Outils avancés de journalisation et de dépannage dans l'interface graphique (p. ex. capture de paquets)
- Prise en charge de la haute disponibilité (HA) permettant le clustering de deux appareils en mode actif-actif ou actif-passif, avec une configuration HA rapide de type plug-and-play, prenant en charge plusieurs liens de synchronisation redondants
- Interface de ligne de commande (CLI) complète accessible depuis l'interface graphique
- Administration déléguée avec intégration Azure AD pour l'authentification unique (SSO)
- Mises à jour du firmware via SSL avec épinglage des certificats pour une sécurité maximale
- Définitions d'objets système réutilisables et consultables pour les réseaux, services, hôtes, périodes, utilisateurs et groupes, clients et serveurs
- Portail utilisateur en libre-service
- Suivi des changements de configuration
- Contrôle d'accès flexible aux appareils pour les services par zones
- Options de notification par email et d'interruptions SNMP
- SNMP v3 (y compris la surveillance du matériel) et surveillance sFlow/Netflow
- Support pour la gestion centralisée dans Sophos Central (disponible pour les clients avec un abonnement au support valide uniquement)
- Sauvegarde et restauration des configurations : localement, via FTP ou par email ; à la demande, quotidiennement, hebdomadairement ou mensuellement. Possibilité de remapper les ports lors de la mise à niveau des appliances matérielles
- Prise en charge des certificats Let's Encrypt pour : configuration TLS, WAF, SMTP, connexion aux hotspots, console d'administration Web, portail utilisateur, portail captif, portail VPN et portail SPX
- API pour intégration tierce
- Modification du nom de l'interface
- Option d'accès à distance pour le support Sophos
- Gestion des licences dans le cloud via MySophos

Pare-feu, réseau et routage

- Pare-feu à inspection approfondie des paquets avec état
- L'architecture de traitement des paquets Xstream offre des niveaux exceptionnels de visibilité, de protection et de performances grâce au traitement des paquets basé sur les flux
- L'inspection TLS Xstream avec performances élevées, prise en charge du protocole TLS 1.3 sans baisse des performances, stratégies de niveau entreprise, ports indépendants, tableau de bord offrant une visibilité inégalée et fonctionnalités de résolution des problèmes de compatibilité
- Xstream DPI Engine fournit une analyse du flux (stream scanning) pour IPS, AV, Web, ainsi que le contrôle applicatif et l'inspection TLS dans un moteur à haute performance unique
- Xstream Network Flow FastPath garantit une accélération intelligente et basée sur des politiques du trafic des applications fiables, du trafic VPN IPSec et du trafic chiffré TLS de manière automatique
- Stratégies basées sur l'utilisateur, le groupe, l'horaire ou le réseau
- Stratégies relatives aux horaires d'accès par utilisateur/groupe

- Application des politiques selon les zones, les réseaux ou par type de service
- Isolement des zones et prise en charge des politiques basées sur les zones
- Zones par défaut pour LAN, WAN, DMZ, LOCAL, VPN et Wi-Fi
- Zones personnalisées sur LAN ou DMZ
- Politiques NAT personnalisables avec masquage de l'adresse IP et prise en charge complète des objets pour rediriger ou transférer plusieurs services via une seule règle, avec un assistant NAT pratique permettant de créer rapidement et facilement des règles NAT complexes en quelques clics
- Définitions d'objets réseau réutilisables pour toutes les règles grâce à la fonctionnalité de recherche intelligente globale en texte libre
- Protection contre le flooding : DoS, DDoS et blocage de l'analyse des ports
- Blocage pays basé sur l'IP
- Routage : statique, multidiffusion (PIM-SM), et dynamique : RIP, BGP, OSPFv3 (IPv6) BGPv6
- Clonez des routes statiques et activez-les ou désactivez-les, redistribuez les routes BGP dynamiques dans OSPFv3, utilisez les options de route Blackhole et utilisez Equal-Cost Multi-Path (ECMP) pour l'équilibrage de charge
- Prise en charge du mandataire direct (upstream proxy)
- Routage multidiffusion non basé sur le protocole avec surveillance IGMP
- Pontage avec prise en charge STP et transfert de diffusion ARP
- Prise en charge et balisage VLAN DHCP
- Prise en charge du pontage VLAN
- Prise en charge de la trame Jumbo
- Activation/désactivation des interfaces physiques
- Prise en charge du WAN sans fil (non disponible dans les déploiements virtuels)
- Interface d'agrégation de liens 802.3ad
- Configuration complète de DNS, DHCP et NTP
- DNS dynamique (DDNS)
- Certification d'approbation du programme IPv6 Ready Logo
- Délégation du préfixe DHCP IPv6
- Prise en charge du tunneling IPv6, y compris 6in4, 6to4, 4in6 et déploiement rapide IPv6 (6 rd) via IPsec

Xstream SD-WAN

- Les profils Xstream SD-WAN prennent en charge plusieurs options de liens WAN, y compris VDSL, DSL, câble, LTE/cellulaire et MPLS
- Les SLA basés sur les performances sélectionnent automatiquement le meilleur lien WAN en fonction de la gigue, de la latence ou de la perte de paquets
- Équilibrage de charge SD-WAN sur plusieurs liens SD-WAN avec des stratégies de pondération Round Robin ou de persistance de session
- Le reroutage sans impact maintient les sessions d'application lorsque les performances du lien tombent en dessous des seuils et qu'une transition est effectuée vers un lien WAN plus performant
- Les graphiques de surveillance SD-WAN fournissent des informations en temps réel sur la latence, la gigue et la perte de paquets pour tous les liens WAN
- Accélération Xstream FastPath du trafic des tunnels IPsec SD-WAN
- Le SD-WAN synchronisé (une fonctionnalité de Sécurité Synchronisée) s'appuie sur une clarté et une fiabilité optimisées au niveau de l'identification des applications grâce au partage d'informations, en provenance du contrôle synchronisé des applications, entre les systèmes d'extrémité gérés par Sophos et Sophos Firewall
- Routage des applications vers les liens prioritaires prédéfinis par les règles de pare-feu ou selon la politique de sécurité.
- Prise en charge robuste du VPN, y compris IPsec et VPN SSL.
- Tunnel RED de couche 2 unique avec routage

Régulation du trafic et quotas de base

- Régulation du trafic flexible basée sur le réseau ou l'utilisateur (QoS) (options améliorées de régulation du trafic Web et des applications incluses avec l'abonnement Web Protection)
- Définissez des quotas de trafic par utilisateur pour le téléchargement/téléversement ou le trafic total, de manière cyclique ou non cyclique.
- Optimisation de la VoIP en temps réel
- Marquage DSCP

Wi-Fi sécurisé

- Déploiement plug-and-play simple des points d'accès Sophos Wireless (série APX uniquement) – apparaissent automatiquement sur le centre de contrôle du pare-feu
- Surveillance et gestion centralisées des points d'accès et

des clients sans fil grâce au contrôleur sans fil intégré

- Pontez les points d'accès au réseau local, au VLAN ou à une zone distincte avec options d'isolement client
- Prise en charge de plusieurs SSID par radio, y compris les SSID cachés
- Prise en charge de diverses normes de sécurité et chiffrement dont WPA2 Personal et Enterprise.
- Option de sélection de la largeur du canal
- Conforme à la norme IEEE 802.1X (authentification RADIUS) avec prise en charge des serveurs primaire et secondaire
- Prise en charge de la norme 802.11r (transition rapide)
- Prise en charge des hotspots pour les bons d'accès (personnalisés), le mot de passe du jour ou l'acceptation des conditions générales
- Accès Internet invité sans fil avec options d'environnement clôturé
- Accès réseau sans fil basé sur l'horaire
- Mode réseau maillé sans fil avec répétition et pontage, compatible avec les points d'accès pris en charge
- Optimisation automatique de la sélection des canaux en arrière-plan
- Prise en charge des connexions HTTPS

Authentification

- La Synchronisation de l'identifiant utilisateur utilise la Sécurité Synchronisée pour partager l'identifiant utilisateur Active Directory actuellement connecté entre les postes protégés par Sophos et le pare-feu, sans agent sur le serveur AD ou le client
- Authentification via : Active Directory, eDirectory, RADIUS, LDAP et TACACS+
- Agents d'authentification serveur pour Active Directory SSO, STAS, SATC
- Authentification unique (SSO) : Active directory, eDirectory, Comptabilité RADIUS
- Authentification unique Azure AD pour l'accès administrateur à la console Webadmin
- Authentification unique Azure AD permettant aux utilisateurs de s'authentifier pour accéder au Web via le portail captif
- SSO AD transparent avec HSTS appliqué, permettant l'établissement de liaisons (handshakes) Kerberos et NTLM via HTTP ou HTTPS
- Importation de groupes Azure AD et prise en charge du RBAC
- Agents d'authentification client pour Windows, Mac OS X, Linux 32/64
- Authentification SSO par navigateur : Authentification proxy transparente (NTLM) et Kerberos
- Portail captif du navigateur
- Certificats d'authentification pour iOS et Android
- Services d'authentification pour IPsec, SSL, L2TP, PPTP
- Prise en charge de l'authentification Google Chromebook pour les environnements avec Active Directory et Google G Suite
- Intégration de Google Workspace via un client LDAP avec Google Chromebook SSO
- Authentification basée sur les API

Portails VPN et utilisateur libre-service

- SNMP v3 (y compris la surveillance du matériel) et surveillance sFlow/Netflow
- Téléchargement du client d'authentification Sophos
- Téléchargement du client d'accès distant SSL (Windows) et les fichiers de configuration (autres OS)
- Informations d'accès au Hotspot
- Modification du nom d'utilisateur et du mot de passe
- Affichage de l'utilisation personnelle d'Internet
- Accès aux messages mis en quarantaine et gestion des listes d'expéditeurs bloqués/autorisés en fonction des utilisateurs (nécessite Email Protection)

Options VPN de base

- VPN de Site-à-Site : SSL, IPsec, AES/3DES 256 bits, PFS, RSA, certificats X.509, clé pré-partagée (PSK)
- Tunnel VPN de site à site Sophos RED (robuste et léger)
- Accélération Xstream FastPath du trafic du tunnel IPsec (de site à site et pour l'accès à distance)
- Outils de gestion, de surveillance et d'importation VPC d'AWS
- L2TP et PPTP
- VPN basé sur le routage avec sélecteurs de trafic
- Accès distant : Prise en charge du client VPN SSL, IPsec, iPhone/iPad/Cisco/Android
- Prise en charge de IKEv2
- Basculement HA avec état de connexion IPsec pour RBVPN, PBVPN et VPN d'accès à distance sans perte d'événement de session dans les scénarios de basculement HA

- Surveillance de l'état du tunnel VPN IPsec via SNMP
- Prise en charge IPsec avancée pour PSK et DH-Group uniques 27-30 / RFC6954
- Client SSL pour Windows et téléchargement de configuration via le portail utilisateur

Client Sophos Connect

- Authentification : Clé pré-partagée (PSK), ICP (X.509), Token et XAUTH
- Prise en charge de l'authentification unique (SSO) Entra ID (Azure AD)
- Activation de la Sécurité Synchronisée et du Security Heartbeat pour les utilisateurs connectés distants
- Tunnellisation fractionnée (split-tunneling) intelligente pour un routage optimal du trafic
- Prise en charge du NAT-traversal
- Client-moniteur pour un aperçu graphique de l'état de la connexion
- Prise en charge des clients Mac (IPsec) et Windows (SSL/IPsec)

Module 'Network Protection'

Prévention des intrusions (IPS)

- Moteur d'inspection approfondie des paquets (DPI) IPS haute performance et Next-Gen avec des modèles IPS sélectifs pouvant être appliqués sur la base de règles de pare-feu pour des performances et une protection maximales
- Des milliers de signatures
- Sélection granulaire des catégories
- Prise en charge des signatures IPS personnalisées
- Les filtres intelligents de la stratégie IPS permettent la mise en place de politiques dynamiques qui se mettent automatiquement à jour à mesure que de nouveaux modèles sont ajoutés

Réponse active aux menaces et Security Heartbeat™

- La réponse active aux menaces surveille/bloque automatiquement les menaces avancées et persistantes (APT) et toute autre menace identifiée via les Flux de menaces de Sophos-X Ops, afin de garantir une protection avancée contre les bots et les adversaires actifs tentant de contacter des destinations malveillantes à l'aide de détections DNS, AFC et pare-feu multicouches
- La réponse active aux menaces surveille/bloque automatiquement les menaces identifiées par les flux MDR/XDR publiés par un analyste SOC Sophos ou client/partenaire lorsque Sophos Firewall avec Xstream Protection est associé à Sophos MDR/XDR
- La réponse active aux menaces surveille/bloque automatiquement les flux de menaces tiers provenant de sources de renseignements sur les menaces industrielles, verticales ou régionales avec Xstream Protection
- Le Security Heartbeat synchronisé de Sophos signale instantanément par un indicateur d'état Heartbeat rouge les appareils compromis qui tentent de contacter tout indicateur de menace identifié par la réponse active aux menaces et ses flux de menaces associés. L'état du Heartbeat est également surveillé par Sophos Endpoint et partagé avec le pare-feu et comprend des informations telles que l'hôte, l'utilisateur, le processus, le nombre d'incidents et l'heure de la tentative de compromission
- Les conditions du Security Heartbeat peuvent être associées à n'importe quelle règle de pare-feu, afin de limiter automatiquement l'accès aux ressources et aux segments du réseau de tout appareil compromis jusqu'à ce qu'il soit nettoyé
- Sophos Firewall active également automatiquement la protection contre les mouvements latéraux lorsqu'un terminal géré est compromis, en demandant à tous les terminaux Sophos sains de rejeter le trafic provenant de l'appareil compromis, ce qui bloque efficacement cet appareil, même sur le même segment LAN

Gestion des appareils SD-RED

- Gestion dans Central de tous les appareils SD-RED
- Pas de configuration : se connecte automatiquement via un service de provisionnement basé sur le Cloud
- Tunnel chiffré sécurisé utilisant des certificats numériques X.509 et le chiffrement AES 256 bits
- Ethernet virtuel pour un transfert fiable de tout trafic entre les sites
- Gestion des adresses IP avec configuration centralisée des serveurs DHCP et DNS
- Révocation à distance de l'accès des appareils SD-RED après une période d'inactivité déterminée
- Compression du trafic du tunnel
- Options de configuration du port VLAN

VPN sans client

- Portail d'auto-assistance HTML5 chiffré unique de Sophos avec prise en charge de RDP, SSH, Telnet et VNC

Module 'Web Protection'

Contrôle et sécurité du Web

- Protection web DPI en continu ou inspection en mode proxy explicite
- Le mode proxy explicite prend en charge l'authentification par connexion pour plusieurs utilisateurs partageant la même IP source
- Protection contre les menaces renforcée
- Base de données de filtrage URL avec des millions de sites répartis dans 92 catégories, alimentée par les SophosLabs
- Stratégies relatives au temps de navigation par utilisateur/groupe
- Stratégies relatives aux horaires d'accès par utilisateur/groupe
- Contrôle antimalware : bloque toutes les formes de virus, malwares sur le Web, chevaux de Troie, et logiciels espions sur HTTP/S, FTP ainsi que les messageries Web
- Protection antimalware avancée avec émulation JavaScript
- Recherches Live Protection en temps réel et dans le Cloud pour obtenir les derniers renseignements sur les menaces
- Second moteur de détection de malwares indépendant (Avira) pour le double contrôle
- Contrôle en temps réel ou en mode batch
- Protection anti-pharming
- Application des restrictions de locataires pour O365
- Détection et application du tunneling du protocole SSL
- Validation du certificat
- Mise en cache du contenu web haute performance
- Mise en cache forcée pour les mises à jour de Sophos Endpoint
- Filtrage des types de fichiers par type MIME, extension et types de contenu actif (par exemple Activex, applets, cookies, etc.)
- Application de la politique YouTube for Schools (utilisateur/groupe)
- Application de SafeSearch (basée sur DNS) pour les principaux moteurs de recherche par politique (utilisateur/groupe)
- Surveillance et application des mots-clés Web pour enregistrer, signaler ou bloquer les contenus Web correspondant à des listes de mots-clés, avec possibilité d'importer des listes personnalisées
- Blocage des applications potentiellement indésirables (PUA)
- Option de dérogation de la stratégie Web permettant aux enseignants ou au personnel d'autoriser temporairement l'accès à des sites ou catégories bloqués, entièrement personnalisable et gérable par certains utilisateurs
- Alertes instantanées pour tout utilisateur naviguant vers une catégorie Web restreinte (à une fréquence pouvant atteindre 5 minutes)

Visibilité sur les applications Cloud

- Le widget du Centre de contrôle affiche la quantité de données téléchargées et téléversées vers des applications Cloud classées comme nouvelles, autorisées, non autorisées ou tolérées
- Mise en évidence des activités de Shadow IT
- Informations détaillées sur les utilisateurs, le trafic et les données
- Accès en un clic aux politiques de régulation du trafic
- Filtrage de l'utilisation des applications Cloud par catégorie ou volume
- Rapport d'utilisation détaillé personnalisable des applications Cloud pour un reporting historique complet

Protection et contrôle des applications

- Contrôle synchronisé des applications pour identifier, classer et contrôler automatiquement toutes les applications Windows et Mac inconnues sur le réseau grâce au partage d'informations entre les terminaux gérés par Sophos et le pare-feu
- Contrôle des applications basé sur les signatures avec des modèles pour des milliers d'applications
- Visibilité sur les applications Cloud et contrôle pour repérer les activités de Shadow IT
- Les filtres intelligents de contrôle applicatif activent les stratégies dynamiques qui se mettent automatiquement à jour à mesure que de nouveaux modèles sont ajoutés
- Découverte et contrôle des micro-applications
- Contrôle des applications basé sur la catégorie, les caractéristiques (par exemple, consommation de bande passante et de productivité), la technologie (par exemple, P2P) et le niveau de risque
- Application de la stratégie de contrôle des applications par utilisateur ou par réseau

Régulation du trafic du Web et des applications

- Options de Régulation renforcée du trafic (QoS) par catégorie Web ou application pour limiter ou assurer le téléchargement, ou priorité totale du trafic et transfert individuel ou partagé

Module ‘Protection DNS’

Service DNS basé dans le Cloud

- Service de résolution de noms de domaine
- Service DNS haute performance basé dans le Cloud
- Optimisé par SophosLabs et l’IA
- Bloque les URL malveillantes lors de la recherche DNS
- Contrôles de conformité précis pour bloquer les sites Web indésirables par catégorie
- Administré dans Sophos Central

Module ‘NDR Essentials’

Détection et réponse du réseau (Network Detection and Response)

- NDR basé dans le Cloud
- Optimisé par l’IA
- Détecte les communications malveillantes chiffrées sans déchiffrement TLS
- Détecte les algorithmes de génération de domaines
- Évalue les scores des menaces potentielles et alerte sur toute menace dépassant le seuil fixé
- Prise en charge complète des rapports et de la journalisation

Module ‘Zero-Day Protection’

Analyse dynamique par sandboxing

- Intégration complète dans le tableau de bord de votre solution de sécurité Sophos
- Inspecte les fichiers exécutables et les documents comportant du contenu exécutable (y compris les fichiers .exe, .com, .dll, .doc, .docx, docm, .rtf et PDF), ainsi que les archives contenant l’un des types de fichiers mentionnés ci-dessus (y compris les fichiers ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z et Microsoft Cabinet)
- Analyse agressive des comportements, des réseaux et de la mémoire
- Détecte les comportements d’évasion du Sandboxing
- La technologie de Machine Learning avec Deep Learning analyse tous les fichiers exécutables déposés
- Inclut la prévention des exploits et la technologie CryptoGuard Protection de Sophos Intercept X
- Rapports détaillés sur les fichiers malveillants avec captures d’écran et fonctionnalité de libération des fichiers dans le tableau de bord
- Sélection facultative du centre de données et options flexibles de stratégie utilisateur et groupe concernant le type de fichier, les exclusions et les actions lors de l’analyse
- Prend en charge les liens de téléchargement uniques

Analyse statique des renseignements sur les menaces

- Tous les fichiers contenant du code actif téléchargé via le Web ou entrant dans le pare-feu sous forme de pièces jointes à des emails, telles que des fichiers exécutables et des documents comportant du contenu exécutable (y compris .exe, .com et .dll, .doc, .docx, docm et .rtf et PDF) et des archives contenant l’un des types de fichiers énumérés ci-dessus (y compris ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet), sont automatiquement envoyés pour analyse des renseignements sur les menaces
- Les fichiers sont vérifiés par rapport à la vaste base de données de renseignements sur les menaces des SophosLabs et soumis à plusieurs modèles de Machine Learning afin d’identifier les éventuels malwares nouveaux et inconnus
- Les rapports détaillés comprennent un widget des fichiers analysés dans le tableau de bord, une liste détaillée des fichiers qui ont été analysés et les résultats de l’analyse, ainsi qu’un rapport détaillé décrivant les résultats de chaque modèle de Machine Learning

Module ‘Central Orchestration’

Orchestration SD-WAN

- Orchestration SD-WAN et VPN avec création facile et automatisée, à l’aide d’un assistant, de tunnels VPN de site à site entre les emplacements réseau à l’aide d’une architecture optimale (hub-and-spoke, maillage complet ou une combinaison des deux)
- Prend en charge les tunnels VPN IPsec, SSL ou RED S’intègre parfaitement aux fonctionnalités SD-WAN pour la priorisation des applications, l’optimisation du routage et l’exploitation de plusieurs liens WAN pour la résilience et les performances

Sophos Central Firewall Reporting Advanced

- 30 jours de stockage de données dans le Cloud pour les rapports historiques de pare-feu avec des fonctionnalités avancées permettant d’enregistrer, de planifier et d’exporter des rapports personnalisés

Intégration XDR et MDR

- Intégration avec Sophos XDR et MDR pour fournir des données télémétriques et des renseignements sur les menaces à des fins de chasse aux menaces et d’analyse des menaces

- La réponse active aux menaces de Sophos utilise les flux de menaces des analystes MDR et XDR pour identifier, bloquer et isoler automatiquement les menaces actives sur le réseau
- La télémétrie relative aux IoC fournie par la Sécurité Synchronisée recueille des informations importantes sur toute menace, tout utilisateur, tout processus et tout appareil ayant été compromis

Module 'Email Protection'

Protection et contrôle des messageries

- Analyse des emails avec prise en charge SMTP, POP3 et IMAP
- Solution de réputation avec surveillance de la propagation des spams basée sur une technologie brevetée de détection des modèles récurrents
- Blocage des spams et logiciels malveillants pendant la transaction SMTP
- Protection anti-spam DKIM et BATV
- Liste grise anti-spam et protection SPF (Sender Politique Framework)
- Vérification du destinataire en cas de saisie incorrecte d'adresse email
- Second moteur de détection de malwares indépendant (Avira) pour le double contrôle
- Recherches Live Protection en temps réel et dans le Cloud pour obtenir les derniers renseignements sur les menaces
- Mises à jour automatiques des signatures et des modèles
- Prise en charge des hôtes intelligents pour les relais sortants
- Détection/blocage/analyse des types de fichiers des pièces jointes
- Acceptation, rejet ou abandon des messages trop volumineux
- Détecte les URL de phishing au sein des emails
- Utilisez des règles prédéfinies pour le contrôle des contenus ou créez des règles personnalisées en fonction de divers critères, avec des exceptions et des options de politique granulaires
- Prise en charge du chiffrement TLS pour SMTP, POP et IMAP
- Ajout automatique de la signature à tous les messages sortants
- Programme d'archivage des emails
- Listes individuelles de blocage et d'autorisation des expéditeurs basées sur l'utilisateur gérées via le portail utilisateur

Gestion de la quarantaine des emails

- Rapports de quarantaine des spams et options de notification
- Mise en quarantaine des malwares et du spam avec options de recherche et de filtrage par date, expéditeur, destinataire, objet et motif, avec possibilité de libérer ou de supprimer les messages
- Portail utilisateur en libre-service pour consulter et libérer les messages placés en quarantaine

Chiffrement des emails et DLP

- Chiffrement SPX en instance de brevet pour chiffrement unidirectionnel des emails
- Auto-enregistrement des destinataires pour la gestion des mots de passe SPX
- Ajout de pièces jointes aux réponses sécurisées SPX
- Complètement transparent : aucun logiciel ou client supplémentaire requis
- Moteur DLP avec recherche automatique d'éventuelles données sensibles présentes dans les emails et les pièces jointes
- Listes de contrôle de contenu (LCC) préconfigurées pour les données sensibles telles que les informations personnelles identifiables (PII), les données de cartes de paiement (PCI), les données médicales (HIPAA), etc., gérées par les SophosLabs

Module 'Web Server Protection'

Protection du pare-feu d'application Web (WAF)

- Reverse Proxy
- Moteur de durcissement des URL avec prévention des liens profonds et des attaques de traversées de répertoires
- Moteur de durcissement des formulaires
- Protection contre les injections SQL
- Protection contre les attaques XSS
- Double moteur antivirus (Sophos et Avira)
- Déchargement du chiffrement via HTTPS (TLS/SSL)
- Signature des cookies avec des signatures numériques
- Routage basé sur des chemins
- Application des politiques GeoIP

- Configuration personnalisée du chiffrement et application de la version TLS
- Application de HSTS et de X-Content-Type-Options
- Prise en charge du protocole Outlook Anywhere
- Authentification inversée (déchargement) pour l'authentification basée sur formulaire et l'authentification de base pour l'accès au serveur
- Abstraction des serveurs virtuels et des serveurs physiques
- Équilibreur de charge intégré répartissant les visiteurs sur plusieurs serveurs
- Permet d'ignorer les vérifications individuelles de manière granulaire selon les besoins
- Mise en correspondance des requêtes des réseaux sources ou d'URL cibles spécifiées
- Prise en charge des opérateurs logiques *et/ou*
- Assure la compatibilité avec diverses configurations et déploiements non standard
- Options permettant de modifier les paramètres de performance du pare-feu d'application Web (WAF)
- Option de limite de taille d'analyse
- Autorisation/blocage des plages d'adresse IP
- Prise en charge des caractères génériques pour les chemins d'accès et les domaines de serveur
- Ajout automatique d'un préfixe/suffixe pour l'authentification

Reporting et journalisation

Central Firewall Reporting

- Rapports prédéfinis avec options de personnalisation souples
- Reporting pour Sophos Firewall : matériel, logiciel, virtuel et Cloud
- Interface utilisateur intuitive avec représentation graphique des données
- Tableau de bord offrant une vue instantanée des événements des dernières 24 heures
- Identifiez aisément les activités, tendances et attaques potentielles sur le réseau
- Sauvegarde simple des journaux avec récupération rapide en cas d'audit
- Déploiement simplifié sans avoir besoin d'une expertise technique

Sophos Central Firewall Reporting Advanced

- Rapports agrégés multi-pare-feux
- Enregistrez des modèles de rapport personnalisables
- Rapports planifiés
- Exportez des rapports au format PDF, CFV ou HTML
- Jusqu'à un an de stockage de données par pare-feu
- Connecteur MDR/XDR du Data Lake pour la chasse aux menaces

Rapports intégrés

- REMARQUE : Le reporting dans Sophos Firewall est inclus sans frais supplémentaires, mais la disponibilité des journaux, rapports et widgets individuels peut dépendre des licences des modules de protection respectifs.
- Des centaines de rapports intégrés avec des options de personnalisation : Tableaux de bord (Trafic, Sécurité et Quotient de menaces utilisateurs), applications (Risque applicatif, Applications bloquées, Applications synchronisées, Moteurs de recherche, Serveurs Web, Correspondance de mots-clés Web, FTP), réseau et menaces (Réponse active aux menaces et flux de menaces, Security Heartbeat, IPS, Wi-Fi, protection contre les menaces zero day), VPN, email, conformité (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)
- Surveillance des activités en cours : état d'intégrité du système, utilisateurs actifs, connexions IPsec, utilisateurs distants, connexions actives, clients sans fil, quarantaine et attaques DoS
- Surveillance des performances des liens SD-WAN pour la gigue, la latence et la perte de paquets
- Anonymisation des rapports
- Planification de rapports pour plusieurs destinataires par groupe de rapports avec des options de fréquence flexibles
- Exportation de rapports aux formats HTML, PDF et Excel (XLS)
- Rapports favoris
- Personnalisation de la conservation des journaux par catégorie
- Visionneuse de journaux complète avec affichage en colonnes et affichage détaillé, dotée d'options de filtrage et de recherche puissantes, d'un identifiant de règle hyperlié et d'une personnalisation de l'affichage des données

Gestion centralisée

Sophos Central

- La gestion et le reporting multi-pare-feux dans le Cloud avec Sophos Central permettent de gérer les stratégies de groupe et d'accéder à tous vos produits de sécurité Sophos depuis une console unique
- La gestion des politiques de groupe permet de modifier une fois les objets, paramètres et stratégies et de les synchroniser automatiquement avec tous les pare-feux du groupe
- Le Gestionnaire de tâches fournit un historique complet des audits et un suivi de l'état des modifications apportées aux politiques de groupe
- La gestion des sauvegardes de firmware dans Sophos Central stocke les cinq derniers fichiers de sauvegarde de configuration pour chaque pare-feu, dont un peut être épinglé pour un stockage permanent et un accès facile
- La planification des mises à jour du firmware de Sophos Central permet d'appliquer facilement des mises à jour automatisées à tout moment
- Avec le déploiement zero-touch, vous effectuez la configuration initiale du pare-feu dans Sophos Central, puis vous l'exportez sur une clé USB qui sera utilisée pour la charger sur l'appareil au démarrage. L'appareil sera ainsi automatiquement connecté à Sophos Central

Accès réseau Zero Trust (ZTNA)

- Passerelle Sophos ZTNA intégrée pour un accès sécurisé aux applications hébergées derrière le pare-feu
- Administré dans Sophos Central

Secure by Design

- La fonctionnalité de contrôle d'état d'intégrité du compte de Sophos Firewall compare des dizaines de paramètres de configuration aux bonnes pratiques afin d'identifier les risques potentiels, et permet d'explorer facilement les problèmes pour les résoudre
- Fonctionnalité de correctif OTA (over-the-air) zero-touch automatisée pour corriger les vulnérabilités sans temps d'arrêt
- Noyau durci pour une sécurité, des performances et une évolutivité améliorées avec avec un isolement stricte des processus et une atténuation pour les attaques par canaux latéraux
- Surveillance à distance de l'intégrité par Sophos à l'aide d'un capteur XDR intégré permettant une surveillance en temps réel de l'intégrité du système, notamment les configurations non autorisées, l'exécution de codes malveillants, la falsification de fichiers, etc., afin d'identifier rapidement les éventuelles attaques et y répondre rapidement
- Architecture Xstream Next-Gen avec nouveau plan de contrôle pour une sécurité et une évolutivité maximales
- Conteneurisation des limites de confiance clés et des portails utilisateur/VPN
- Gestion centralisée chiffrée et sécurisée via Sophos Central, éliminant tout besoin d'accès administrateur à distance
- L'authentification multifacteur sur tous les systèmes protège contre le vol d'identifiants et les attaques par force brute
- Passerelle ZTNA intégrée pour un accès à distance plus sécurisé et une protection renforcée des applications
- Des déploiements sécurisés prêts à l'emploi garantissent l'implémentation des bonnes pratiques de sécurité avec des contrôles d'accès stricts

Résumé des fonctionnalités de Sophos Firewall par abonnement

	Bundle Xstream Protection							Disponible séparément		
	Bundle Standard Protection					Disponible séparément				
	Base Firewall	Network Protection	Web Protection	DNS Protection	Fonction-nalités exclusives du bundle	Zero-Day Protection	Central Orchestration	Central Firewall Reporting Adv.	Email Protection	Web Server Protection
Gestion générale (y compris HA)	✔									
Architecture Xstream	✔									
Pare-feu, réseau et routage	✔									
Xstream SD-WAN	✔									
Régulation du trafic et quotas de base	✔									
Wi-Fi sécurisé	✔									
Authentification	✔									
Portail utilisateur en libre-service	✔									
VPN (IPsec, SSL, etc.)	✔									
VPN de Site-à-Site RED	✔									
Client VPN Sophos Connect	✔									
Prévention des intrusions (IPS)		✔								
Réponse active aux menaces										
Flux de menaces Sophos X-Ops		✔								
Flux de menaces MDR/XDR					✔					
Flux de menaces tiers					✔					
Security Heartbeat synchronisé		✔								
Gestion des appareils SD-RED		✔								
VPN sans client		✔								
Contrôle des applications synchronisées			✔							
Contrôle et sécurité du Web			✔							
Protection et contrôle des applications			✔							
Visibilité sur les applications Cloud			✔							
Régulation trafic Web et applications			✔							
Sécurité et conformité DNS				✔						
NDR Essentials					✔					
Analyse dynamique par sandboxing						✔				
Analyse des renseignements sur les menaces						✔				
Orchestration SD-WAN							✔			
Données de Central Firewall Reporting*		7 jours	7 jours	7 jours	7 jours	7 jours	30 jours	Jusqu'à 1 an	7 jours	7 jours
Fonctionnalités de CFR Advanced							✔	✔		
Protection et contrôle des messageries									✔	
Gestion de la quarantaine des emails									✔	
Chiffrement des emails et DLP									✔	
Protection du WAF										✔
Journalisation et reporting intégrés	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Gestion dans Sophos Central**		✔	✔	✔	✔	✔	✔	✔	✔	✔
Passerelle ZTNA**		✔	✔	✔	✔	✔	✔	✔	✔	✔
Secure by Design	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

Note : certaines fonctionnalités ne sont pas prises en charge sur les modèles XGS 87 et XGS 88 (rapports intégrés, fonctionnalité MTA (agent de transfert d'emails), double analyse antivirus et analyse antivirus WAF)

Les options de licence MSP diffèrent légèrement de celles indiquées ci-dessus

* La durée de conservation des données est une estimation basée sur l'utilisation moyenne du réseau et peut varier en fonction du volume réel des données enregistrées. Outil d'estimation du stockage.

** Inclus dans tout bundle, support ou abonnement de protection. Les clients disposant uniquement d'une licence Base doivent ajouter un abonnement de support pour bénéficier de ces fonctionnalités.

Liste des fonctionnalités Sophos Firewall

SOPHOS

Résumé des fonctionnalités de Sophos Firewall par abonnement

	Support Enhanced (inclus dans les bundles Standard et Xstream Protection)	Support Enhanced Plus (disponible en tant que mise à niveau du support Enhanced)
Support multicanal 24/7 (téléphone, portail Web, chat), y compris assistance à distance et accès en libre-service à la base de connaissances et aux forums communautaires	✔	✔
Téléchargements, mises à jour et versions de maintenance du firmware **	✔	✔
Gestion dans Sophos Central, reporting et passerelle ZTNA	✔	✔
Remplacement anticipé de matériel pour les appareils actifs	✔	✔
Remplacement anticipé de matériel pour un appareil HA passif*		✔
Remplacement anticipé de matériel pour les appareils SD-RED/APX		✔
Accès VIP (appels transférés vers des ingénieurs seniors)		✔
Consultation à distance (2 à 8 heures par an)		✔

* Pour activer la couverture RMA avancée pour un appareil HA passif, l'appareil actif doit disposer d'une licence de support Enhanced Plus
Pour plus d'informations, consultez le Guide des services de support Sophos.

** Remarque : pour recevoir les mises à jour du firmware un abonnement au support doit être ajouté à tout module individuel acheté.

Sophos France
Tél. : +33 1 34 34 80 00
Email : info@sophos.fr

2025-12-15 FR (DD)