SOPHOS
Cybersecurity delivered.

Sophos Firewall

Présentation de la solution

Sommaire

Sophos Firewall

Sophos Firewall a été conçu dès le départ pour répondre aux principaux problèmes des pare-feux actuels, tout en fournissant une plateforme de nouvelle génération conçue pour faire face aux flux chiffrés d'Internet et à l'évolution du paysage des menaces. Sophos Firewall apporte une nouvelle approche dans la manière dont vous identifiez les risques cachés, vous protégez contre les menaces et répondez aux incidents, tout en offrant des performances optimales. Notre architecture Xstream pour Sophos Firewall utilise une architecture de traitement des paquets qui offre des niveaux exceptionnels de visibilité, de protection et de performance.

Sophos Firewall offre une visibilité incomparable sur les utilisateurs à risque, les applications indésirables, les charges virales suspectes et les menaces persistantes. Il intègre étroitement un ensemble complet de technologies modernes de protection contre les menaces, faciles à mettre en place et à maintenir. Et contrairement pare-feux traditionnels, Sophos Firewall communique avec d'autres systèmes de sécurité sur le réseau. Cela lui permet de devenir votre point d'application de confiance pour contenir les menaces et empêcher les malwares de se propager ou d'exfiltrer des données hors du réseau, automatiquement et en temps réel.

Sophos Firewall possède 4 avantages clés par rapport à d'autres pare-feux réseau :

1. **Il expose les risques cachés** – Sophos Firewall est beaucoup plus efficace pour exposer les risques cachés que d'autres solutions, grâce à un tableau de bord visuel, des rapports détaillés intégrés basés dans le Cloud et une visibilité unique sur les risques.
2. **Il bloque les menaces inconnues** – Avec Sophos Firewall, bloquer les menaces inconnues est plus simple, plus rapide et plus efficace qu'avec tout autre pare-feu, grâce à une suite de capacités de protection avancées faciles à installer et à administrer.
3. **Il répond automatiquement aux incidents** – Avec la Sécurité Synchronisée, Sophos Firewall répond automatiquement aux incidents sur le réseau grâce à la fonction Sophos Security Heartbeat™ qui partage en temps réel des informations entre vos postes et votre pare-feu.
4. **Il optimise votre réseau SD-WAN** – Les fonctionnalités Xstream SD-WAN de Sophos Firewall simplifient la configuration de réseaux SD-WAN superposés complexes, en quelques clics de type pointer-cliquer. Vous pouvez également profiter de la sélection automatique des liaisons WAN en fonction des performances, avec des transitions instantanées sans impact entre les liaisons pour optimiser les performances de vos applications, la fiabilité du réseau et la continuité des activités tout en réduisant les coûts de connectivité.

Exposer les risques cachés

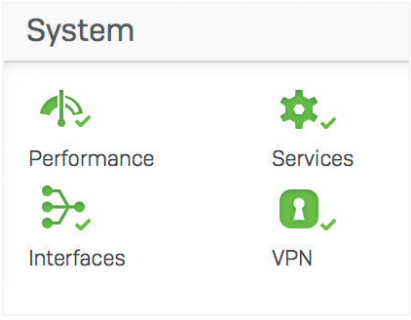
Il est vital qu'un pare-feu moderne puisse analyser les montagnes d'informations collectées, corréler ces données autant que possible et ne signaler que les informations les plus importantes qui nécessitent une action, idéalement avant qu'il ne soit trop tard.

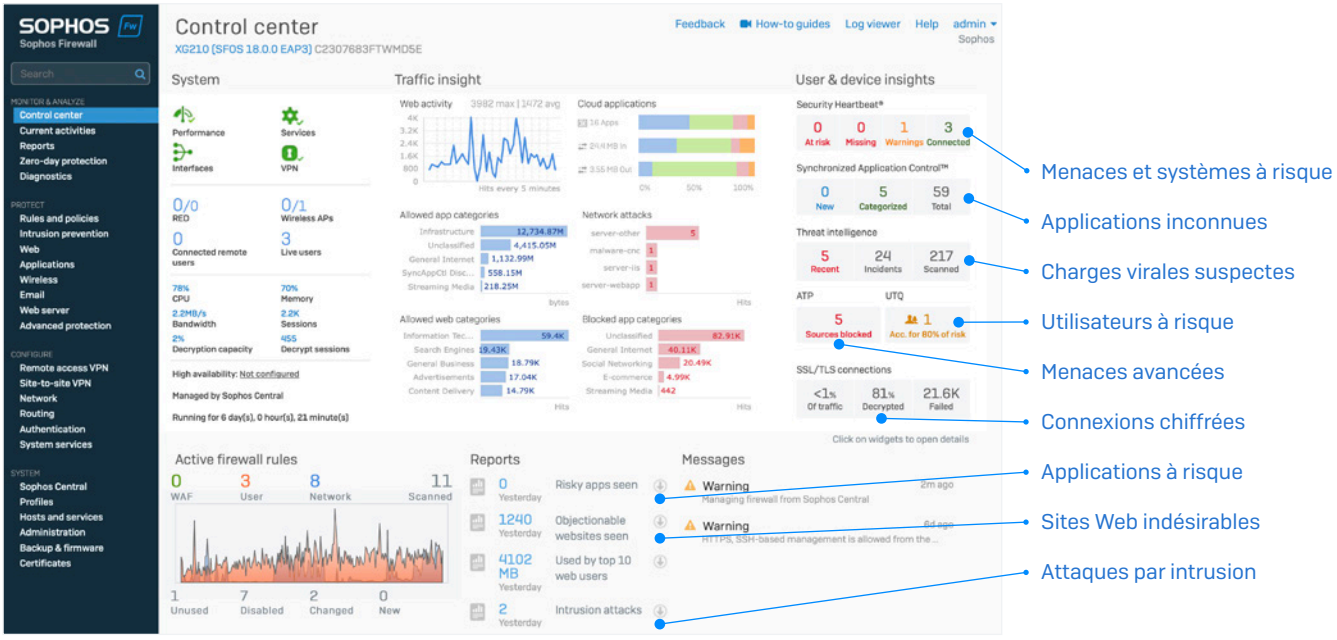
Centre de contrôle

Le centre de contrôle de Sophos Firewall offre un niveau de visibilité sans précédent sur les activités, les risques et les menaces qui ciblent votre réseau.

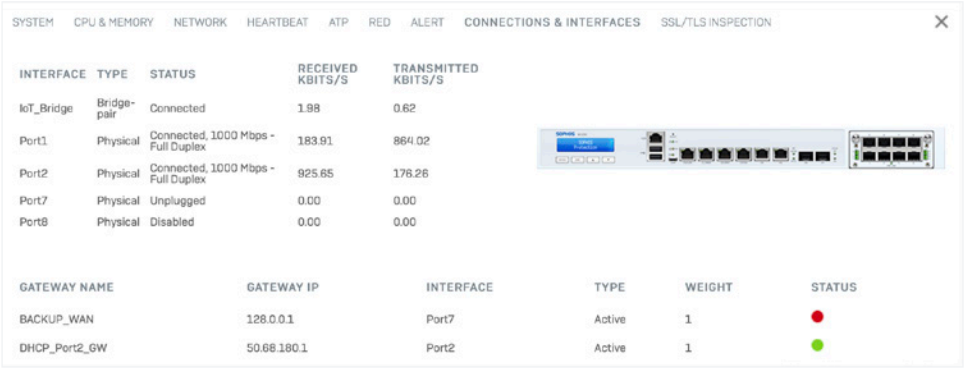
Il utilise des indicateurs tricolores (vert/orange/rouge) pour attirer votre attention sur ce qui est important pour vous.

Un indicateur rouge requiert une action immédiate. Un indicateur jaune indique un problème potentiel. Et un indicateur vert indique qu'aucune action n'est nécessaire.

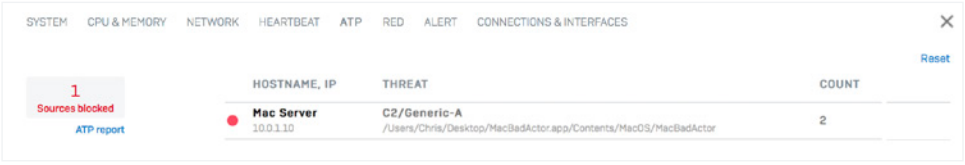




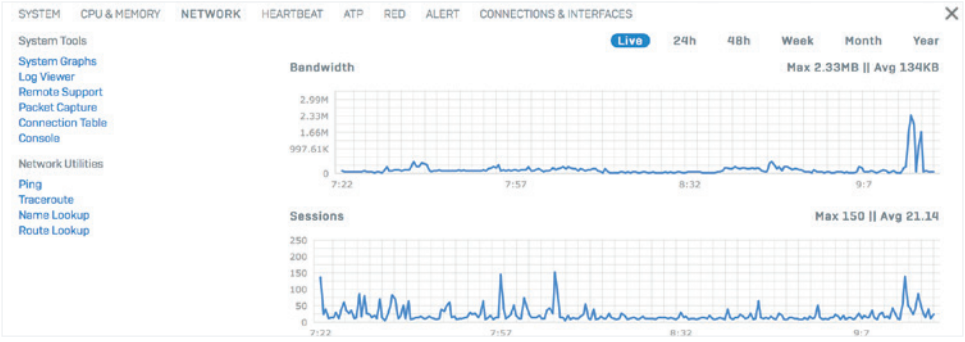
Chaque widget affiché dans le centre de contrôle révèle des informations supplémentaires lorsque l'on clique dessus. Par exemple, il est possible d'obtenir le statut des interfaces de l'appareil en cliquant sur le widget « Interfaces ».



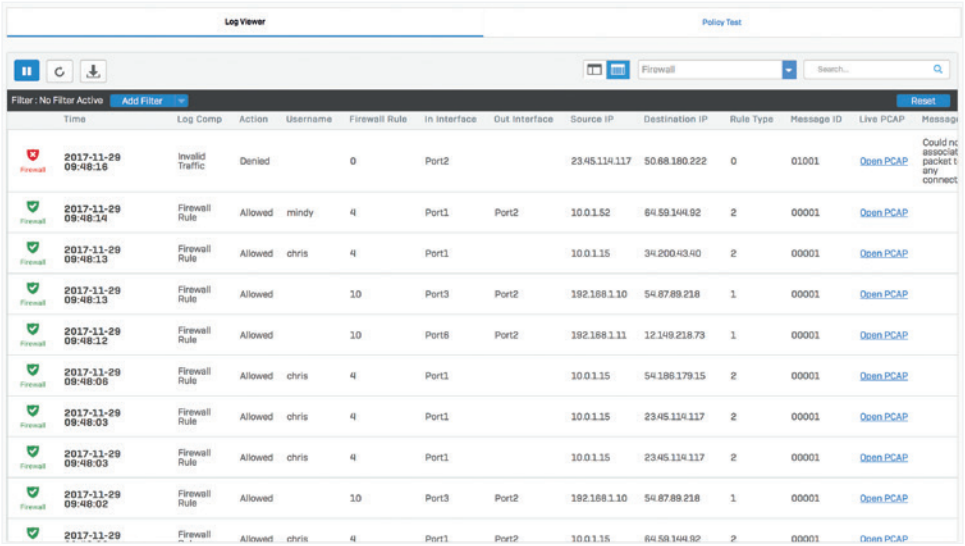
Le widget « ATP » (Advanced Threat Protection) révèle quant à lui l'hôte, l'utilisateur et la source de la menace avancée.



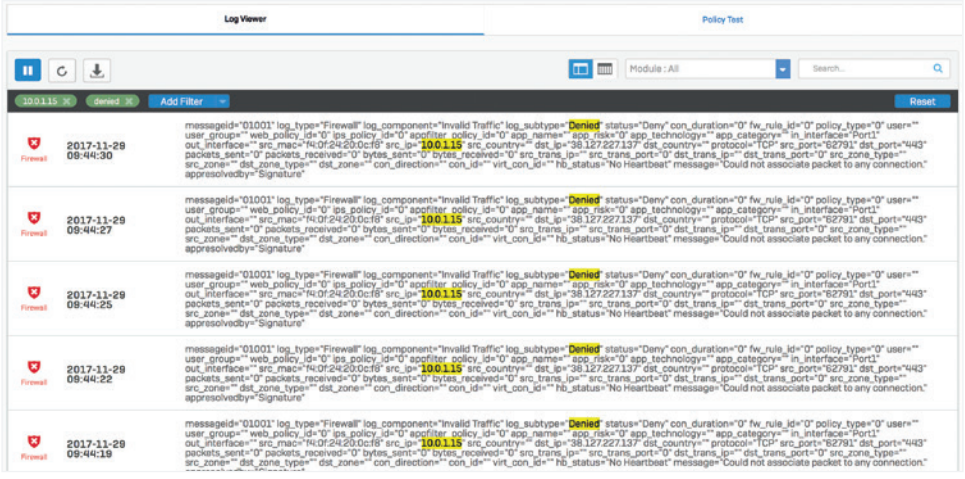
Les systèmes graphiques affichent également à la demande les performances sur une période donnée, que ce soit sur les deux dernières heures, le mois dernier ou l'année passée. Et ils offrent un accès rapide aux outils de dépannage les plus couramment utilisés pour résoudre les incidents.



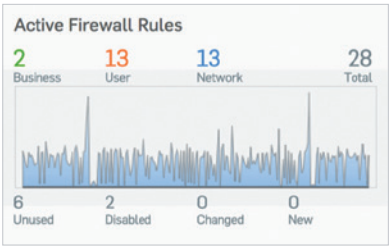
La Visionneuse de journaux est accessible depuis n'importe quel écran, en un seul clic. Elle s'ouvre dans une nouvelle fenêtre, pour garder un œil sur les journaux importants tout en travaillant sur la console. Les journaux peuvent être affichés selon deux vues : standard et détaillée. La vue standard affiche les différents modules du pare-feu sous forme de colonnes, tandis que la vue détaillée est unifiée et est dotée de puissantes options de filtres et de tri et compile les logs de l'ensemble du système en une seule vue en temps réel.



Si vous êtes comme la plupart des administrateurs réseau, vous vous demandez probablement si vous avez trop de règles de pare-feu, et parmi celles-ci, lesquelles sont vraiment nécessaires et lesquelles ne sont pas utilisées. Avec Sophos Firewall, plus besoin de vous poser la question.



Le widget « Règles de pare-feu actives » montre le graphique en temps réel du trafic traité par le pare-feu, par type de règle : Application métier, Utilisateur et Réseau. Il montre également le nombre de règles actives par statut, y compris les règles inutilisées, vous donnant ainsi l'occasion de faire un peu de « nettoyage ». Comme avec les autres widgets du centre de contrôle, en cliquant sur une règle, vous obtiendrez le tableau détaillé des règles triées par type ou par statut.

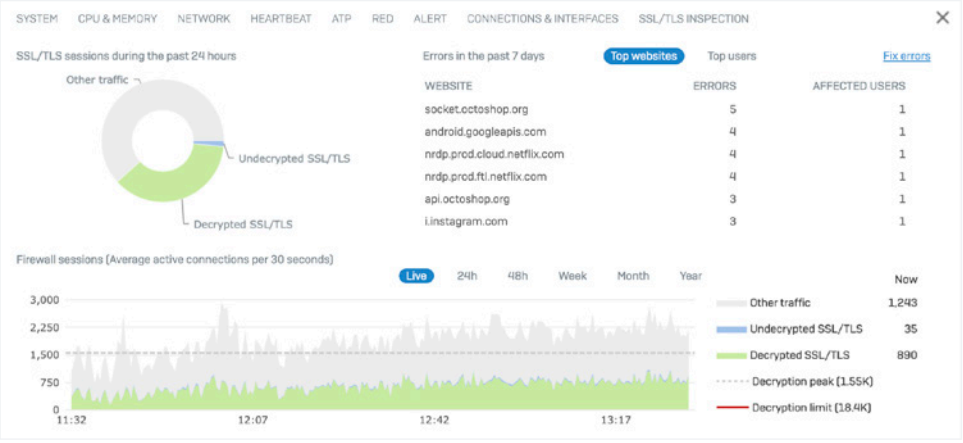


Inspection TLS Xstream

Une véritable tempête se prépare autour du trafic chiffré. Selon Google, le volume de trafic chiffré sur les réseaux est aujourd'hui supérieur à 90 %. Et les cybercriminels y voient une formidable opportunité pour lancer des attaques cachées et donc difficiles à détecter. En effet, on ne peut pas bloquer ce que l'on ne voit pas. Et malheureusement, la plupart des entreprises ne peuvent rien y faire, car leur pare-feu actuel n'a pas les capacités nécessaires pour utiliser l'inspection TSL/SSL sans subir un ralentissement considérable.

Sophos Firewall, avec son nouveau moteur d'inspection SSL Xstream, est doté de capacités beaucoup plus élevées pour les connexions simultanées et offre des outils de création de politiques de sécurité qui lui permettent de prendre des décisions intelligentes sur ce qui doit et peut être analysé, en se déchargeant le cas échéant. À l'aide des outils consacrés aux politiques SSL, les entreprises peuvent créer des politiques TLS/SSL de haut niveau relatives au trafic non déchiffrable, aux certificats, aux protocoles, aux options d'application du chiffrement, et bien plus encore. Sophos Firewall prend en charge le protocole TLS 1.3 et toutes les suites de chiffrement moderne sur chaque port et application du système.

Des outils supplémentaires placés dans le tableau de bord permettent aux administrateurs de voir exactement la proportion de trafic chiffré sur le réseau, et comment celui-ci est traité. Sophos Firewall fait un bien meilleur travail pour faire apparaitre ces informations que d'autres solutions, notamment par la façon dont il signale les erreurs rencontrées au moment de la validation des certificats ou des sites Web qui ne prennent pas en charge les dernières normes de chiffrement.



Sophos Firewall fournit des informations sur les flux de trafic chiffrés et sur tout problème lié à l'inspection TLS, directement dans le centre de contrôle.

Les administrateurs peuvent aussi ouvrir une fenêtre détaillée pour voir exactement quels sont les sites problématiques et pourquoi, ainsi que les utilisateurs qui rencontrent des problèmes. De là, ils peuvent agir directement pour empêcher le déchiffrement de l'application ou du site afin d'éviter d'autres incidents. Aucune autre solution d'inspection SSL n'offre la même accessibilité à ces informations.

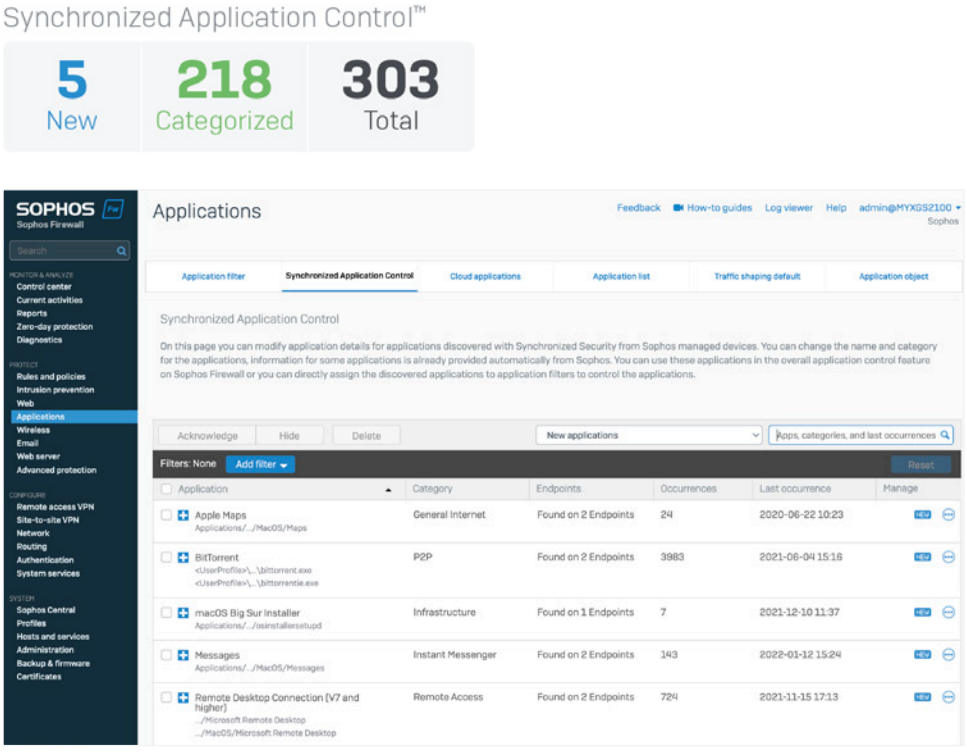
Contrôle synchronisé des applications

Le problème du contrôle des applications dans les pare-feux Next-Gen d'aujourd'hui est que la majorité du trafic des applications n'est pas identifié. Il est soit non catégorisé, soit marqué comme inconnu, HTTP générique ou HTTPS générique.

Il existe une raison simple à cela : tous les moteurs de contrôle des applications des pare-feux reposent sur les signatures et les modèles viraux pour identifier les applications. Et comme on peut s'y attendre, les applications personnalisées destinées aux marchés verticaux, telles que les applications médicales et financières, n'auront jamais de signatures. D'autres applications évasives, comme les clients BitTorrent et la VoIP, ainsi que les applications de messagerie, changent constamment leur comportement et leur signature pour échapper à la détection et au contrôle. Un certain nombre utilise le chiffrement pour échapper à la détection, tandis que d'autres ont simplement recourt à des connexions génériques de type navigateur Web pour communiquer via le pare-feu, car les ports 80 et 443 ne sont généralement pas bloqués sur les pare-feux.

Le résultat est un manque de visibilité total sur les applications sur le réseau, et malheureusement, vous ne pouvez pas contrôler ce que vous ne pouvez voir. La solution à ce problème est très simple, mais pourtant très efficace : le contrôle synchronisé des applications de Sophos, qui utilise notre connexion unique de Sécurité Synchronisée entre les différents postes administrés par Sophos.

Découvrez son fonctionnement. Lorsque Sophos Firewall découvre un trafic issu d'une application qu'il ne peut identifier, il demande au système d'extrémité quelle est l'application à l'origine du trafic.



Les applications inconnues découvertes par le Contrôle synchronisé des applications peuvent être catégorisées automatiquement ou manuellement.

Le système d'extrémité peut alors partager avec le pare-feu les informations sur le fichier exécutable, le chemin du fichier et souvent sa catégorie. Dans la plupart des situations, le pare-feu peut alors utiliser ces informations pour classer et contrôler automatiquement l'application.

Si Sophos Firewall ne peut déterminer la catégorie adéquate de l'application, l'administrateur peut créer une catégorie ou attribuer cette application à une politique existante.

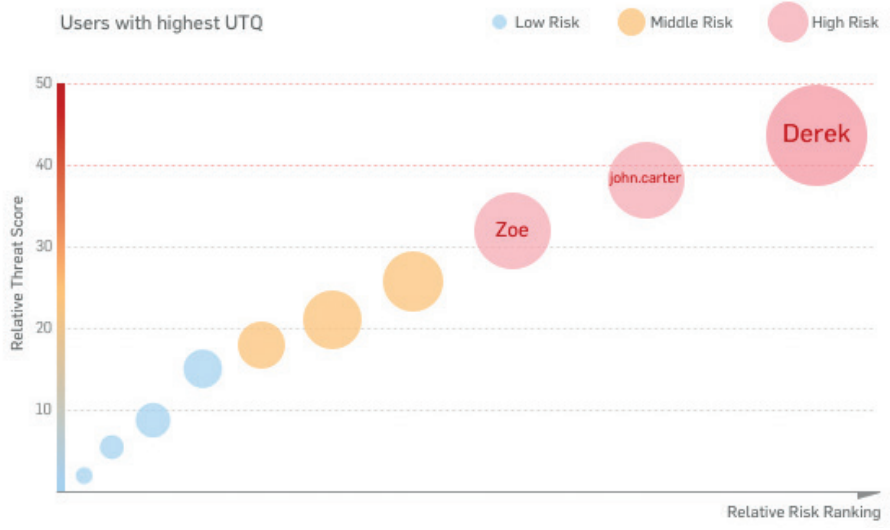
Une fois l'application classée, automatiquement ou par l'administrateur réseau, celle-ci est soumise aux mêmes contrôles de politiques que les autres applications de cette catégorie. Cela facilite le blocage des applications non identifiées et non désirées, et permet de prioriser celles que vous souhaitez utiliser.

La fonction de contrôle synchronisé des applications est une percée dans la visibilité et le contrôle des applications. Elle permet une clarté absolue sur chaque application exécutée sur le réseau, y compris celles auparavant non identifiées et non contrôlées.

Utilisateurs les plus à risque

Des études ont montré que les utilisateurs sont le maillon faible de la chaine de sécurité. La bonne nouvelle est que les modèles de comportement humain peuvent être analysés et utilisés pour prévoir et prévenir les attaques. De plus, les habitudes d'utilisation peuvent aider à illustrer comment les ressources de l'entreprise sont utilisées et si les politiques de l'utilisateur ont besoin d'être affinées.

Le Quotient de menace utilisateur (QMU) de Sophos aide les administrateurs réseau à repérer les utilisateurs qui présentent un risque de sécurité, en fonction de leurs comportements suspects sur le Web et de leur historique d'infection et de menaces. Un utilisateur ayant un QMU élevé peut être le signe d'un acte non intentionnel résultant d'un manque de sensibilisation à la sécurité, d'une infection par un malware ou d'un acte de négligence volontaire.

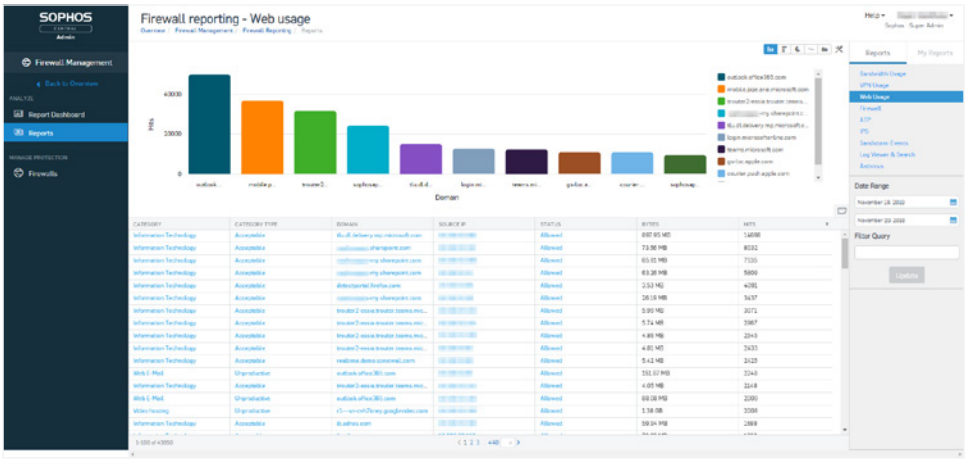


Sophos Firewall met en évidence vos utilisateurs les plus à risque en un coup d'œil.

Identifier l'utilisateur et les activités à l'origine du risque aide les administrateurs réseau à prendre les mesures nécessaires. Ils peuvent alors décider de former les utilisateurs les plus à risque ou d'appliquer des politiques de sécurité plus strictes ou plus adéquates afin de maîtriser ces comportements.

Création de rapports flexible

Sophos Firewall est unique parmi les produits NGFW et UTM. Il offre des options flexibles et intégrées de reporting dans le Cloud, avec un degré élevé de personnalisation, sans frais supplémentaires. Sophos Central Firewall Reporting (CFR) permet aux entreprises de mieux comprendre l'activité grâce aux analyses. Grâce à son ensemble complet de rapports intégrés et aux outils permettant de créer des centaines de rapports différents, CFR offre des informations exploitables sur le comportement des utilisateurs, l'utilisation des applications, les événements de sécurité, etc. Grâce aux rapports interactifs et au tableau de bord des rapports, les administrateurs explorent en un coup d'œil les données syslog stockées dans votre compte Sophos Central. Ils obtiennent ainsi une vue détaillée qui est présentée sous un format visuel pour une compréhension aisée. Les données peuvent ensuite être analysées pour identifier des tendances témoignant de lacunes dans la posture de sécurité et mettant en lumière la nécessité de modifier une politique de sécurité.



Sophos Firewall offre de nombreuses options embarquées et centralisées de reporting dans le Cloud.

Sophos Firewall fournit également des rapports intégrés. Choisissez parmi un ensemble complet de rapports, organisés de manière pratique par type, avec plusieurs tableaux de bord intégrés. Il existe des centaines de rapports avec des paramètres personnalisables pour tous les domaines du pare-feu : activité du trafic, sécurité, utilisateurs, applications, Web, réseaux, menaces, VPN, messagerie et conformité. Vous pouvez facilement programmer l'envoi de rapports périodiques à des destinataires spécifiques et sauvegarder ceux-ci aux formats HTML, PDF ou CSV.

Bloquer les menaces inconnues

Protéger contre les dernières menaces réseau demande une symphonie de technologies fonctionnant en synergie, et dirigées par un chef d'orchestre : l'administrateur réseau. Malheureusement, la plupart des pare-feux ont plutôt tendance à jouer en solo, avec des règles de pare-feu paramétrés pour un secteur, des politiques Web pour un autre, des inspections TLS/SSL ailleurs et le contrôle des applications dans une partie différente du produit.

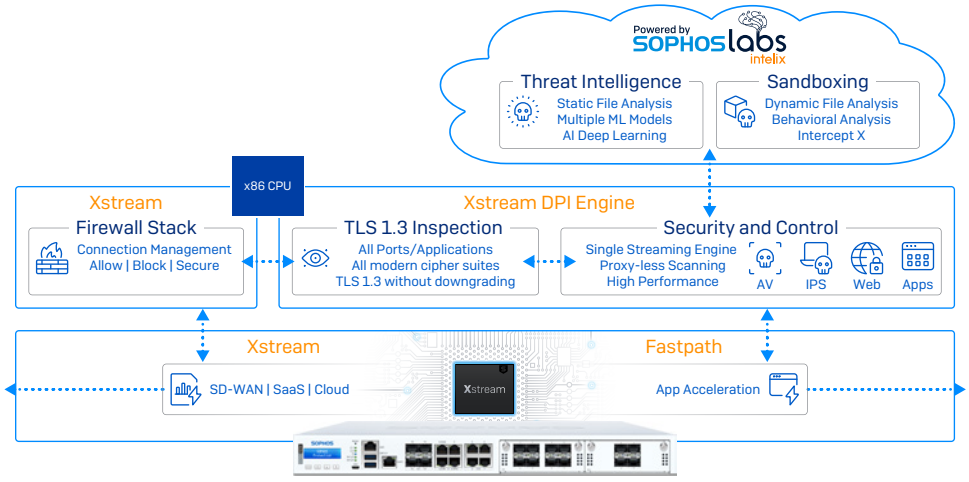
Chez Sophos, non seulement nous pensons qu'il est nécessaire d'avoir la technologie de protection la plus avancée disponible, mais nous comprenons également que celle-ci doit être simple à configurer, à déployer et à administrer au quotidien, car une protection mal configurée est souvent pire que de ne pas avoir de protection du tout.

La simplicité est au cœur de l'ADN de Sophos. Mais peut-être plus important encore pour Sophos est sa volonté d'embrasser le changement et de prendre les décisions nécessaires pour faire les choses différemment dans le but d'offrir une meilleure protection et donc une meilleure expérience aux utilisateurs.

Sophos Firewall fait les choses différemment, et cela fait toute la différence.

Visibilité, protection et performances

Les performances du pare-feu ne devraient pas être diminuées lorsque vous activez la sécurité dont vous avez besoin pour protéger votre réseau. L'un des principaux composants de l'architecture de traitement des paquets Xstream de Sophos Firewall est un moteur DPI (Deep Packet Inspection) à haut débit. Ce moteur DPI fournit une analyse sans proxy en un seul passage pour l'IPS (Intrusion Prevention System), l'antivirus et le contrôle du Web et des applications, ainsi que notre inspection SSL Xstream.



L'architecture Xstream de Sophos Firewall avec les processeurs de flux Xstream programmables offre une protection et des performances puissantes.

Lorsqu'une nouvelle connexion est établie, elle est traitée par la pile du pare-feu qui décide alors d'autoriser, de bloquer ou d'analyser le trafic à la recherche de menaces. Si le trafic nécessite une analyse de sécurité, il transmet les paquets au moteur DPI de streaming sans proxy qui analyse les paquets, même si ceux-ci sont chiffrés. Ce moteur n'est utilisé que pour les quelques paquets initiaux. Ensuite, la pile du pare-feu se décharge complètement du traitement sur le moteur DPI. Ce qui améliore considérablement la latence et les performances.

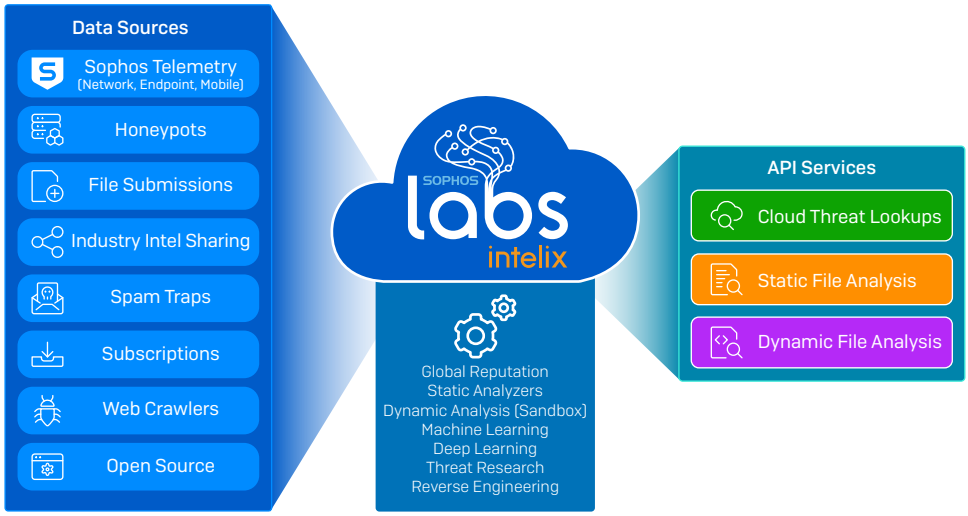
Ensuite, si le flux est considéré comme sécurisé et ne nécessite plus d'inspection supplémentaire, le moteur DPI peut complètement décharger le flux vers Sophos Network Flow FastPath qui fournit un chemin accéléré pour le trafic de confiance. Cela augmente considérablement les performances en libérant les ressources qui inspectent le trafic.

Protection contre les menaces Zero-day

Avec les menaces avancées de type ransomware qui deviennent de plus en plus ciblées et évasives, il est primordial d'identifier et de se protéger contre les menaces Zero-day. La solution ultime à ce problème consiste en 2 types d'analyse :

1. **Analyse statique par Machine Learning** – Cette méthode permet d'analyser et de détecter les menaces Zero-day de manière prédictive grâce à de multiples modèles de Machine Learning, associés à des données de réputation globale et à une analyse approfondie des fichiers, le tout sans avoir besoin d'exécuter le fichier en temps réel.
2. **Analyse dynamique en temps réel (Sandboxing)** – Cette méthode exécute en temps réel les malwares dans un environnement de sandboxing dans le Cloud. Cela permet d'obtenir des informations précieuses sur l'activité des fichiers afin de révéler la véritable nature et les capacités d'une menace inconnue.

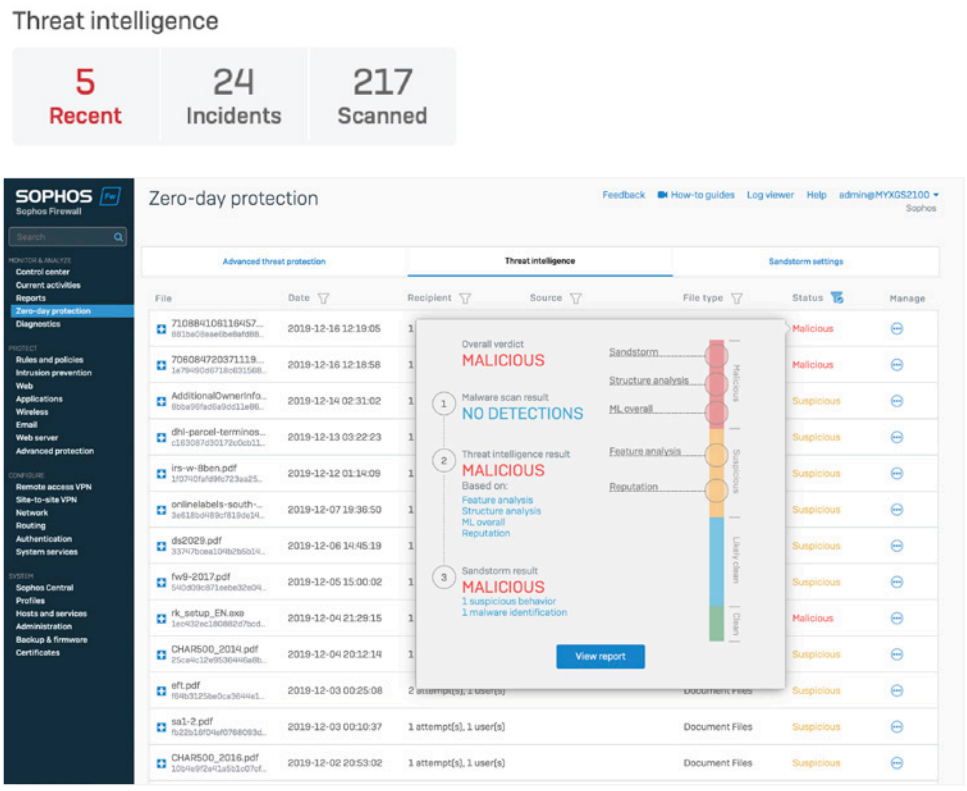
Sophos Firewall inclut ces deux technologies de protection importantes, fournies par notre plateforme SophosLabs Intelix. SophosLabs, notre réseau de laboratoires de recherche sur les menaces de cybersécurité, a développé avec SophosLabs Intelix la plateforme ultime d'analyse et d'intelligence sur les menaces. Celle-ci mobilise la technologie de Machine Learning la plus récente, des décennies de recherche sur les menaces et des pétaoctets de données de renseignements pour fournir une protection inégalée contre les dernières menaces inédites.



La protection Zero-Day de Sophos Firewall est optimisée par les analyses par Machine Learning fournies par SophosLabs Intelix.

Lorsque le moteur Xstream DPI de Sophos Firewall effectue une analyse antivirus d'un fichier entrant sur le réseau et identifie du code actif, il conserve le fichier temporairement et l'envoie au service SophosLabs Intelix pour une analyse statique et dynamique dans le Cloud. Une synthèse des résultats apparait dans le centre de contrôle de Sophos Firewall via le widget 'Intelligence sur les menaces' qui vous amène d'un clic vers le rapport complet (ci-dessous). Le fichier n'est libéré vers le téléchargeur ou le destinataire de l'email que s'il est considéré comme sain.

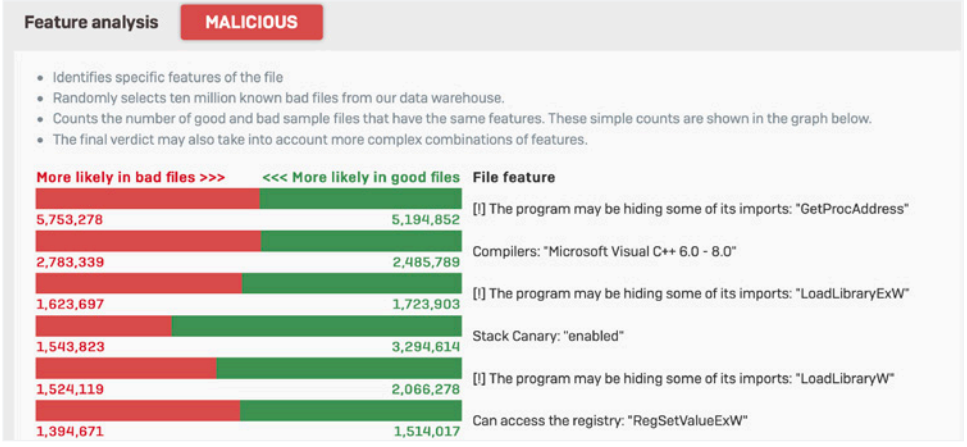
Cette dernière étape est importante, car de nombreuses solutions anti-malware de pare-feux libèrent et envoient le fichier vers l'utilisateur final avant que l'analyse ne soit véritablement terminée. Cela peut entraîner un nettoyage compliqué et coûteux si le fichier s'avère être bel et bien malveillant.



La protection Zero-Day de Sophos Firewall identifie les nouvelles menaces jusqu'alors inédites avant qu'elles ne pénètrent sur votre réseau.

Analyse statique par Machine Learning

L'analyse statique des fichiers utilise plusieurs modèles de Machine Learning pour analyser les différentes caractéristiques, fonctionnalités, ADN et réputation du fichier, en le comparant aux millions de fichiers inoffensifs ou malveillants connus intégrés dans la base de données des SophosLabs. L'analyse rend ainsi un verdict en quelques secondes sur tout nouveau fichier. Cette approche est remarquablement rapide et efficace pour identifier les nouvelles menaces et les nouvelles variantes de menaces existantes, en particulier celles qui ne soumettent pas facilement au sandboxing, tels que les documents protégés par mot de passe contenant des malwares.



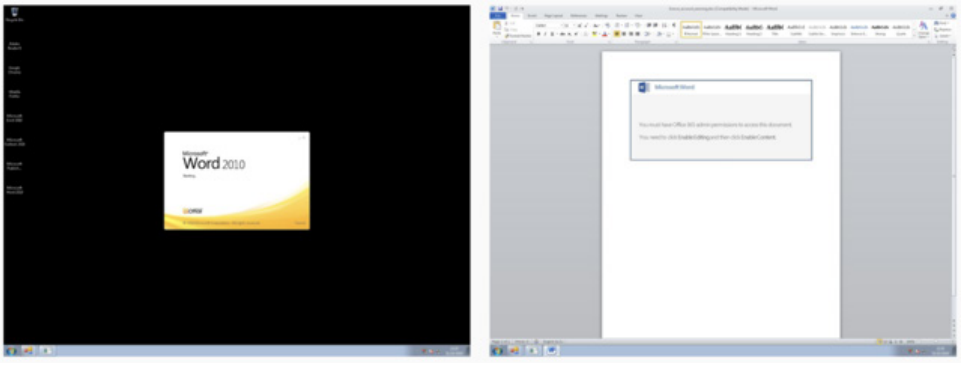
Plusieurs modèles de Machine Learning sont utilisés pour analyser les fichiers suspects afin de détecter les menaces de type Zero-Day.

Analyse dynamique runtime par la technologie de sandboxing

Quand la technologie de sandboxing est apparue, seules les plus grandes entreprises avaient les moyens de se la procurer. Mais aujourd'hui, grâce aux solutions de sandboxing basées dans le Cloud, elle est devenue tout à fait abordable, même pour les plus petites entreprises. Pour la première fois, les PME ont accès à la technologie de sandboxing avec Deep Learning, propulsant la solution bien au-delà de toute autre solution de sandboxing dédiée installée en local, dont le déploiement coûtait il y a encore peu des millions d'euros.

Comme elle est basée dans le Cloud, aucun logiciel ou matériel supplémentaire n'est nécessaire, et il n'y a aucun impact sur les performances du pare-feu. Si le moteur Xstream DPI détermine qu'un fichier contient du code actif (pièce jointe, téléchargement Web, etc.) celui-ci est automatiquement envoyé et exécuté dans l'environnement de sandboxing de SophosLabs Intelix en parallèle de l'analyse statique (ci-dessus) pour déterminer son comportement en temps réel avant d'être autorisé à pénétrer votre réseau.

Pour identifier les menaces, les SophosLabs ont intégré dans la protection Zero-Day les dernières technologies de protection intégrées dans Intercept X, notre produit Endpoint Next-Gen de pointe : Deep Learning, détection des exploits et CryptoGuard (qui détecte en temps réel les ransomwares actifs qui chiffrent des fichiers). Pour rendre un verdict, la technologie de sandboxing surveille également l'activité des fichiers, de la mémoire, du registre et du réseau afin de détecter les caractéristiques d'une intention malveillante. Aucun autre pare-feu n'offre une analyse de type runtime (environnement d'exécution) en combinaison avec la meilleure protection contre les menaces au monde, à savoir Intercept X. Et aucun autre pare-feu n'offre le niveau d'information et de reporting proposé par Sophos Firewall, dont un ensemble de captures d'écran montrant ce qui s'est passé pendant l'exécution du fichier.

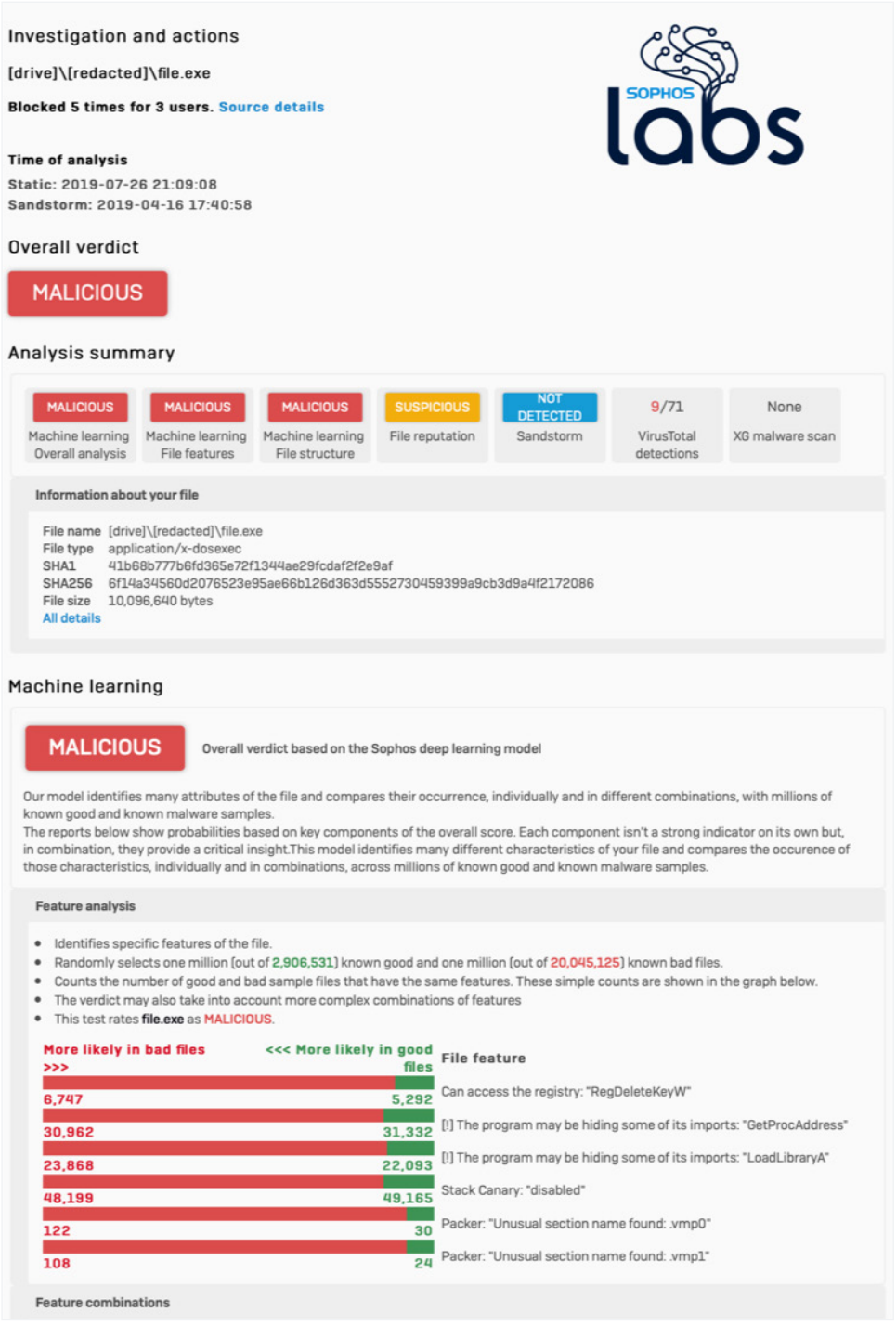


L'analyse runtime par la technologie de sandboxing exécute les fichiers dans un environnement sécurisé pour déterminer leur comportement et fournit des captures d'écran pour examen.

Le sandboxing est particulièrement efficace pour détecter les menaces qui se cachent dans des fichiers normalement inoffensifs et qui peuvent être dépourvues de caractéristiques malveillantes évidentes. Par exemple des fichiers MS Office avec des macros, ou des exécutables bénins ou des mises à jour d'applications qui ont été corrompues.

Reporting complet

Chaque fichier analysé par Sophos Firewall est accompagné d'un rapport complet affichant les résultats détaillés des différentes analyses et des verdicts. Le rapport comporte 6 éléments différents, dont les diverses analyses par Machine Learning, la réputation des fichiers, le sandboxing et même les données VirusTotal issus de tiers.



Investigation and actions

[drive]\[redacted]\file.exe

Blocked 5 times for 3 users. Source details

Time of analysis
Static: 2019-07-26 21:09:08
Sandstorm: 2019-04-16 17:40:58

Overall verdict

MALICIOUS

Analysis summary

Machine learning Overall analysis	Machine learning File features	Machine learning File structure	File reputation	Sandstorm	VirusTotal detections	XG malware scan
MALICIOUS	MALICIOUS	MALICIOUS	SUSPICIOUS	NOT DETECTED	9/71	None

Information about your file

File name	[drive]\[redacted]\file.exe
File type	application/x-dosexec
SHA1	41b68b777b6fd365e72f1344ae29fcdaf2f2e9af
SHA256	6f14a34560d2076523e95ae66b126d363d5552730459399a9cb3d9a4f2172086
File size	10,096,640 bytes

All details

Machine learning

MALICIOUS Overall verdict based on the Sophos deep learning model

Our model identifies many attributes of the file and compares their occurrence, individually and in different combinations, with millions of known good and known malware samples.
The reports below show probabilities based on key components of the overall score. Each component isn't a strong indicator on its own but, in combination, they provide a critical insight.This model identifies many different characteristics of your file and compares the occurence of those characteristics, individually and in combinations, across millions of known good and known malware samples.

Feature analysis

- Identifies specific features of the file.
- Randomly selects one million (out of 2,906,531) known good and one million (out of 20,045,125) known bad files.
- Counts the number of good and bad sample files that have the same features. These simple counts are shown in the graph below.
- The verdict may also take into account more complex combinations of features
- This test rates **file.exe** as MALICIOUS.

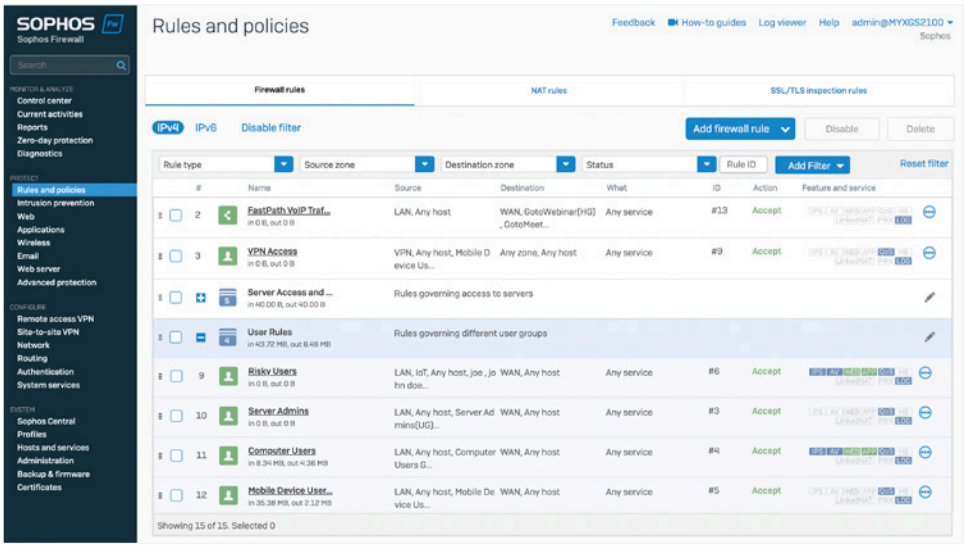
More likely in bad files >>>	<<< More likely in good files	File feature
6,747	5,292	Can access the registry: "RegDeleteKeyW"
30,962	31,332	[!] The program may be hiding some of its imports: "GetProcAddress"
23,868	22,093	[!] The program may be hiding some of its imports: "LoadLibraryA"
48,199	49,165	Stack Canary: "disabled"
122	30	Packer: "Unusual section name found: .vmp0"
108	24	Packer: "Unusual section name found: .vmp1"

Feature combinations

Gestion unifiée des règles

La gestion d'un pare-feu peut être incroyablement complexe. Il faut généralement jongler entre de multiples règles, politiques et paramètres de sécurité qui s'appliqueront à différents domaines fonctionnels, et souvent plusieurs règles différentes seront nécessaires pour obtenir une protection adéquate.

Avec Sophos Firewall, nous avons complètement repensé la façon dont les règles de pare-feu sont organisées et dont votre stratégie de sécurité est gérée. Au lieu d'avoir à chercher dans la console d'administration les politiques qui vous intéressent, nous avons réuni toute la gestion et l'application des règles de pare-feu dans une seule et même interface unifiée. Vous pouvez désormais visualiser, filtrer, rechercher, modifier et organiser toutes les règles de pare-feu au même endroit.



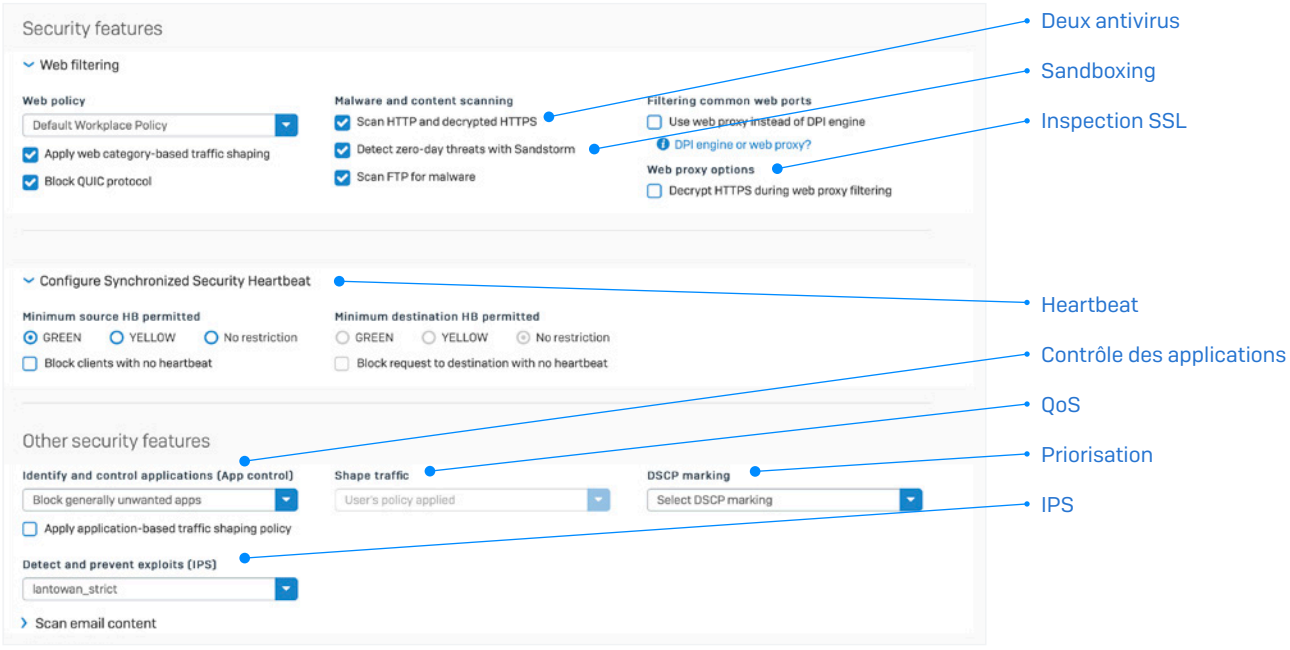
Sophos Firewall regroupe toutes vos règles de politique d'accès, de NAT et d'inspection TLS en un seul endroit, ce qui en facilite la gestion.

Les règles pour les utilisateurs, les applications métier, le NAT, l'inspection TLS/SSL et les réseaux permettent de voir plus facilement les politiques dont vous avez besoin, le tout affiché sur un seul écran.

Les icônes des différents indicateurs permettent d'accéder aux informations importantes sur les politiques, telles que le type, le statut, l'application et bien plus encore.

Gestion de votre stratégie de sécurité en un clin d'œil

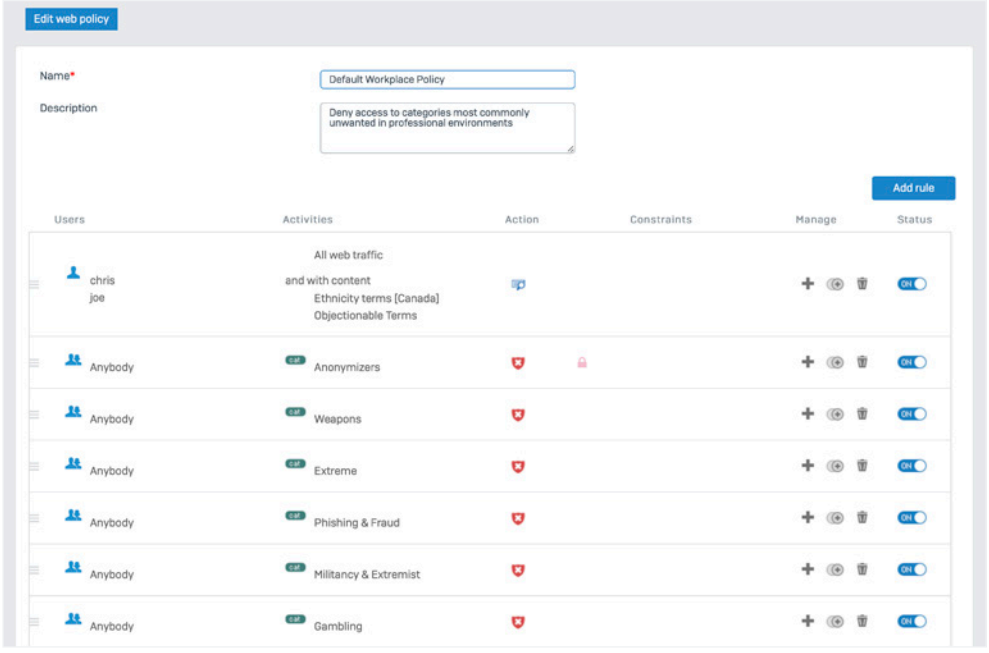
Avec Sophos, il est extrêmement aisé de configurer et de gérer tous les éléments nécessaires à une protection moderne, et ce depuis un seul écran, que ce soit via votre compte Sophos Central dans le Cloud ou via l'interface utilisateur de Sophos Firewall.



Configurez l'ensemble de votre posture de sécurité depuis un seul écran en utilisant des politiques prédéfinies ou personnalisées.

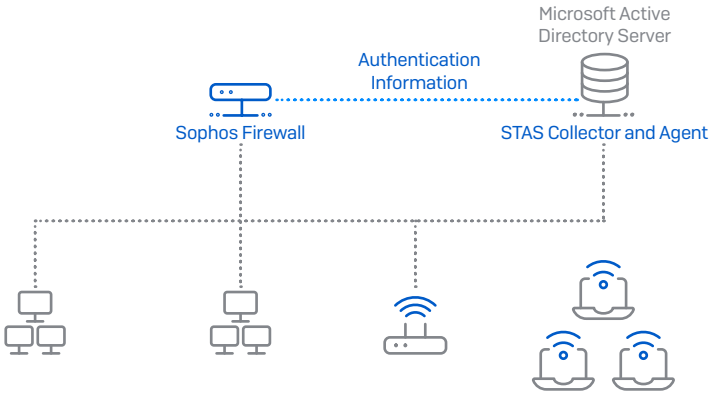
Vous pouvez paramétrer et activer les contrôles de sécurité pour l'antivirus, l'inspection TSL/SSL, la technologie de sandboxing, l'IPS, la régulation du trafic, le contrôle du web et des applications, le Security Heartbeat, le NAT, et hiérarchiser les politiques au même endroit… Le tout déterminé par règle, par utilisateur ou par groupe.

Et si vous souhaitez afficher le détail de vos politiques activables ou les modifier, vous pouvez le faire à la volée, sans avoir à quitter la page des règles de pare-feu pour vous rendre sur une autre page du produit.



Visualisez les détails de la politique en un coup d'œil et apportez des modifications sans quitter l'écran des règles du pare-feu.

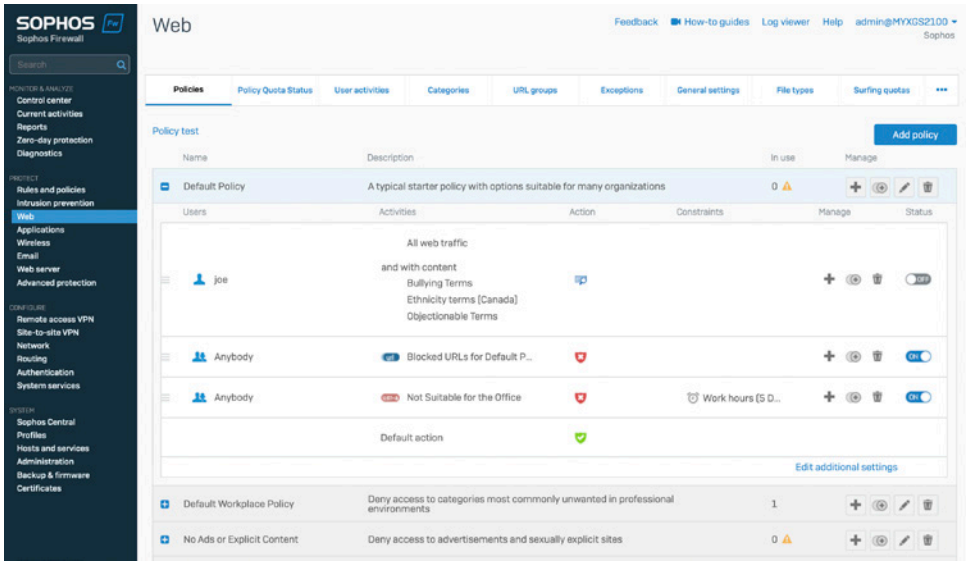
Les options flexibles d'authentification permettent de savoir facilement qui est qui, et d'inclure des services de répertoire tels qu'Active Directory, eDirectory et LDAP ainsi que NTLM, Kerberos, RADIUS, TACACS+, RSA, les agents clients ou un portail captif. Et Sophos Transparent Authentication Suite (STAS) offre une intégration avec des services de répertoire, tels que Microsoft Active Directory, pour une authentification unique fiable et transparente.



No client required on devices for SSO

Protection de pointe de la passerelle Web

Le contrôle et la protection du Web sont des fonctionnalités essentielles des pare-feux, mais elles ne sont souvent pas implémentées de base. Notre expérience dans la conception de solutions professionnelles de protection Web nous a permis d'acquérir les compétences et le savoir-faire nécessaires pour déployer le type de contrôle de politiques de sécurité que l'on retrouve habituellement dans les solutions de passerelle Web sécurisée (SWG) pour grandes entreprises, qui ont un coût dix fois plus élevé. Nous avons implémenté un modèle de politiques par héritage descendant, ce qui permet de créer des politiques sophistiquées de manière simple et intuitive. Des modèles prédéfinis de politiques, utilisables de suite, sont proposés pour la plupart des déploiements courants (environnements de travail classiques, éducation, conformité CIPA pour le secteur de l'éducation, etc.). Cela vous permet d'être opérationnel et conforme immédiatement avec des options de personnalisation et de peaufinage à portée de main.



De puissantes politiques Web de niveau entreprise offrent des contrôles granulaires.

Nous savons que la politique Web est l'un des éléments les plus souvent modifiés au quotidien dans votre pare-feu ; c'est pourquoi nous avons investi beaucoup d'efforts pour faciliter la gestion et le paramétrage des politiques de sécurité en fonction des besoins de vos utilisateurs et de votre entreprise. Vous pouvez aisément personnaliser les utilisateurs/groupes, les activités (URL, catégories et types de fichiers), les actions (bloquer, autoriser ou avertir), et ajouter ou ajuster des contraintes selon l'horaire ou le jour de la semaine.

Fonctionnalités pour le secteur de l'éducation

Sophos Firewall offre de nombreuses fonctionnalités parfaitement adaptées aux environnements du secteur de l'éducation, où les politiques de sécurité Web et la conformité sont des exigences primordiales. Les fonctionnalités spécifiques à l'éducation incluent :

- Politiques Web prédéfinies pour la protection des mineurs sur Internet, conformité CIPA (Children's Internet Protection Act)
- Filtrage du contenu et rapports sur les mots clés
- Paramètres de SafeSearch et du mode restreint de YouTube sur la base d'une politique utilisateur/groupe
- Dérogations à la page de blocage, qui peuvent être gérées par les enseignants
- Des rapports complets intégrés pour identifier rapidement les problèmes potentiels

Les politiques Web incluent désormais des options pour consigner, surveiller et même appliquer des politiques relatives aux contenus dynamiques en fonction de listes de mots clés. Cette fonction est particulièrement importante dans les environnements éducatifs pour garantir la sécurité des jeunes en ligne et identifier les étudiants effectuant des recherches inappropriées. Les listes de mots clés peuvent être envoyées au pare-feu et appliquées à n'importe quelle politique de filtrage Web comme critère supplémentaire, avec des actions pour consigner, surveiller ou bloquer les résultats de recherche ou les sites Web contenant des mots clés spécifiques.

Des rapports complets sont fournis pour identifier les concordances de mots clés et les utilisateurs qui recherchent ou utilisent des mots clés spécifiques. Cela permet d'intervenir de manière proactive auprès de l'utilisateur à risque avant que la situation ne s'aggrave.

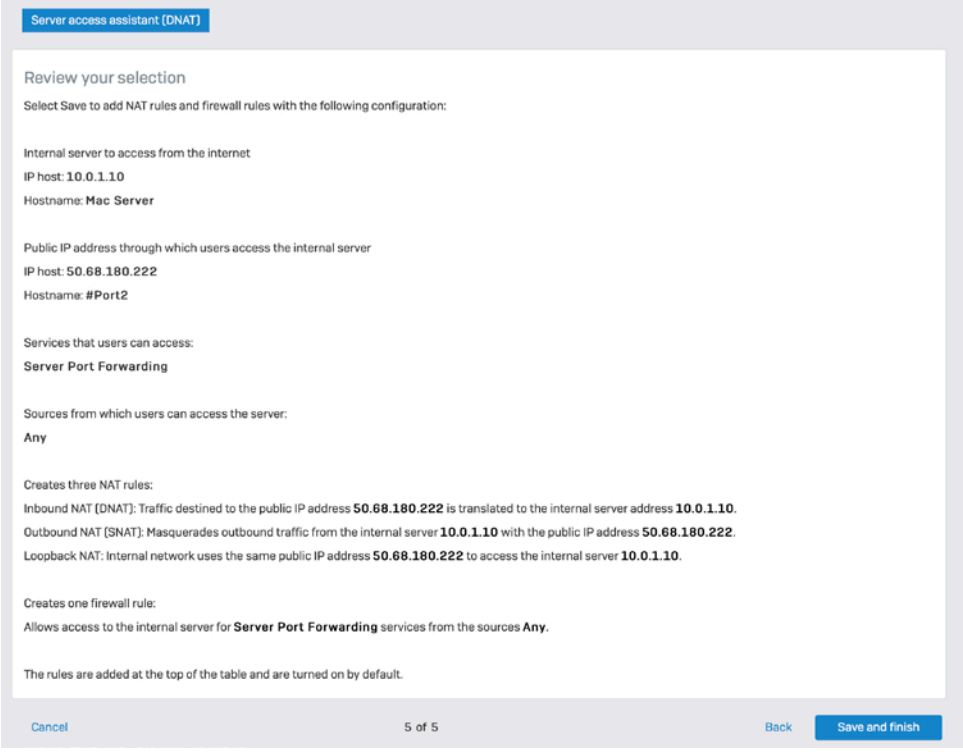
Sophos Firewall permet de se conformer dès le départ à la norme CIPA, pour une mise en conformité rapide. Il offre également des contrôles souples et puissants sur les restrictions SafeSearch et YouTube en fonction de la politique utilisateur/groupe. Les enseignants ont également la possibilité de mettre en place et de gérer leurs propres politiques de dérogation pour permettre à leurs classes d'accéder à des sites Web qui seraient normalement bloqués dans le cadre du programme scolaire.

Vous obtenez ainsi des politiques Web puissantes, en toute simplicité.

Configuration simplifiée du NAT

Tous ceux qui ont essayé de configurer des règles de NAT (Network Address Translation) savent combien cela peut être difficile. Mais il peut en être autrement. Sophos Firewall comprend des capacités de NAT professionnelles complètes pour des configurations de NAT puissantes et flexibles, y compris Source NAT (SNAT) et Destination NAT (DNAT) dans une seule règle avec des critères de sélection détaillés. Pour simplifier les DNAT complexes, un assistant simple d'utilisation vous guide dans le processus de création d'une configuration de NAT complète en quelques clics seulement.

Les administrateurs peuvent également profiter de l'option pratique 'Règle NAT associée' lors de la création d'une règle de pare-feu. 'Règle NAT associée' créera automatiquement une règle de configuration NAT correspondante, ce qui réduira encore le temps passé à créer et à configurer les règles de NAT.

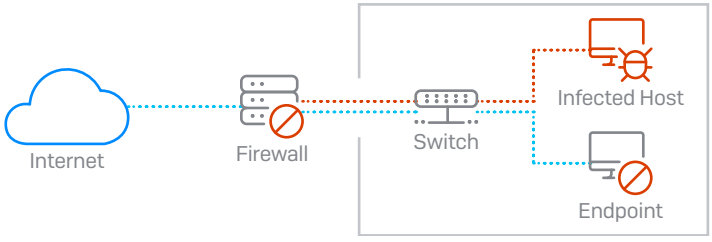


Profitez de l'assistant de règles NAT puissant mais intuitif pour créer des contrôles d'accès complexes en quelques clics seulement.

Réponse automatique aux incidents

Une des fonctions de pare-feu les plus demandées par les administrateurs réseau est la capacité de répondre automatiquement aux incidents de sécurité sur le réseau.

Sophos Firewall est la seule solution de sécurité des réseaux capable d'identifier totalement la source d'une infection sur votre réseau et, en réponse, de limiter automatiquement l'accès de l'appareil infecté aux autres ressources du réseau. Cela est possible grâce à notre fonction Security Heartbeat™ qui partage des données télémétriques et l'état de sécurité entre les systèmes d'extrémité protégés par Sophos et le pare-feu.



Sophos Firewall et Security Heartbeat peuvent isoler automatiquement les hôtes infectés sur votre réseau.

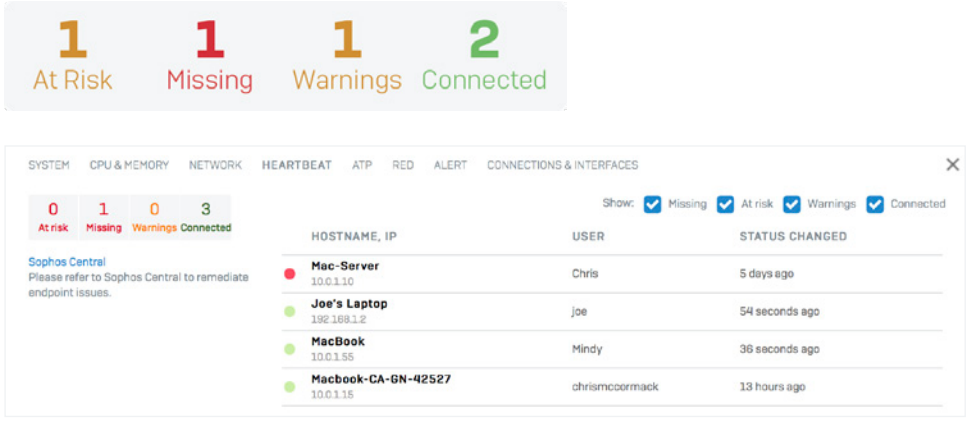
Sophos Firewall intègre de manière exclusive l'état de sécurité des hôtes connectés dans vos règles de pare-feu, vous permettant de limiter automatiquement l'accès aux ressources réseau sensibles de n'importe quel système compromis, jusqu'à ce que ce dernier soit décontaminé.

Non seulement Sophos Firewall isole du réseau les systèmes d'extrémité compromis au niveau du pare-feu, mais il peut également demander à tous les systèmes d'extrémité sains de les isoler au niveau du système d'extrémité.

Cette protection contre les mouvements latéraux isole et empêche les menaces ou les attaquants de se déplacer latéralement sur le réseau vers d'autres systèmes, même s'ils se trouvent sur le même segment de réseau ou domaine de diffusion où le pare-feu ne peut normalement pas intervenir. Il s'agit d'une solution extrêmement simple et efficace pour faire face aux adversaires actifs qui opèrent sur votre réseau. Et cela n'est possible que si vos systèmes d'extrémité et votre pare-feu travaillent ensemble pour coordonner ou synchroniser les défenses.

Security Heartbeat

La fonction Security Heartbeat de Sophos partage des informations en temps réel grâce à une connexion sécurisée entre vos systèmes d'extrémité et votre pare-feu. La synchronisation entre les produits de sécurité qui fonctionnaient auparavant de manière indépendante crée une protection plus efficace contre les malwares avancés et les attaques ciblées.



Le statut Security Heartbeat™ de votre réseau est visible dans le centre de contrôle.

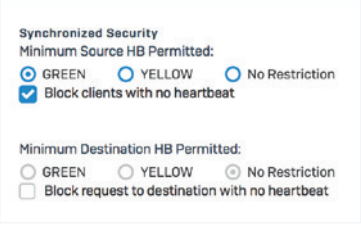
Security Heartbeat non seulement identifie la présence de menaces avancées instantanément, mais il peut aussi être utilisé pour communiquer d'importantes informations sur la nature de la menace, le système hébergé et l'utilisateur. Plus important encore, Security Heartbeat peut aussi agir automatiquement pour isoler ou limiter l'accès aux systèmes compromis jusqu'à disparition du malware. Sa technologie a révolutionné la façon dont les solutions de cybersécurité identifient et répondent aux menaces avancées.

Le Security Heartbeat pour les systèmes administrés derrière votre pare-feu peut être de 3 couleurs selon son statut :

Un **Heartbeat vert** indique que le système est sain et peut accéder à toutes les ressources réseau disponibles.

Un **Heartbeat orange** est un avertissement que l'appareil peut avoir une application potentiellement indésirable (PUA), qu'il n'est plus en conformité ou qu'il fait l'objet d'un autre problème. Vous pouvez limiter l'accès d'un appareil marqué d'un Heartbeat orange aux ressources du réseau, et ce jusqu'à la résolution du problème.

Un **Heartbeat rouge** signale qu'un appareil risque d'être infecté par une menace avancée et qu'il peut tenter de se connecter à un botnet ou à un serveur C&C. Grâce aux paramètres de la politique du Security Heartbeat dans votre pare-feu, vous pouvez facilement isoler les systèmes avec un statut rouge jusqu'à leur nettoyage, afin de réduire les risques de fuite de données ou d'empêcher la propagation de l'infection.



Définissez les exigences du Security Heartbeat dans le cadre de toute règle de pare-feu.

Seul Sophos est capable d'offrir une solution telle que Security Heartbeat, grâce à notre position de leader aussi bien sur le segment des solutions Endpoint que des solutions Réseau. Alors que d'autres éditeurs commencent à réaliser son importance dans la sécurité réseau et peinent à mettre au point de telles solutions, ils sont tous en situation de désavantage : ils n'ont aucune solution leader à intégrer, ni pour le système d'extrémité ni pour le réseau.

Un monde de confiance zéro

Dans le monde des technologies de l'information, la « confiance » est devenue un mot dangereux, surtout lorsqu'elle est implicite. Nous savons que créer un grand périmètre d'entreprise hermétiquement fermé et faire confiance à tout ce qui se trouve à l'intérieur est une conception fondamentalement imparfaite.

Le Zero Trust (Confiance zéro) est une approche globale de la sécurité qui prend en compte ces changements et la façon dont les entreprises travaillent et répondent aux menaces. Il s'agit d'un modèle et d'une philosophie sur la manière de penser et de mettre en œuvre la sécurité.

Il ne faut faire confiance à personne ni à rien de façon automatique, que ce soit à l'intérieur ou à l'extérieur du réseau de l'entreprise. Cependant, il faut bien finir par faire confiance à quelque chose. Avec le Zero Trust, la confiance reste temporaire et est établie à partir de multiples sources de données, et elle est constamment réévaluée.

Le Zero Trust nous permet de contrôler l'ensemble du parc informatique, depuis l'intérieur du bureau jusqu'aux plateformes Cloud utilisées. Fini le manque de contrôle en dehors du périmètre de l'entreprise, ou les difficultés avec les utilisateurs à distance.

Comment évoluer vers le Zero Trust et profiter de tous les avantages qu'il offre ? Bien que personne ne puisse proposer le Zero Trust comme une solution unique, Sophos dispose d'un large portefeuille de technologies et de contrôles de sécurité qui accélère et simplifie votre cheminement vers le Zero Trust.

Sophos Central – La plateforme de cybersécurité la plus fiable sur le marché regroupe ces technologies variées et complémentaires dans une seule console de gestion dans le Cloud, pour vous aider à orchestrer et à surveiller votre réseau Zero Trust.

Sécurité Synchronisée – La cybersécurité qui partage en permanence des informations entre les postes, les accès réseau Zero Trust (ZTNA), les pare-feux et d'autres systèmes, en se fournissant mutuellement des informations et une visibilité.

Sophos ZTNA – Fournit une véritable solution d'accès réseau Zero Trust pour connecter en toute sécurité les utilisateurs aux applications et aux données.

Sophos Firewall – Créez des segments ou des micropérimètres autour des utilisateurs, des appareils, des applications, des réseaux, etc.

Server Protection et Intercept X – Attribuez un état de sécurité à chaque appareil afin que, dans le cas où l'un d'entre eux serait compromis, cet appareil puisse être automatiquement isolé et ne puissent pas se connecter aux autres appareils.

Service Managed Threat Response (MTR) – Le service MTR surveille toutes les activités des utilisateurs sur le réseau et identifie les identifiants des utilisateurs potentiellement compromis.

Optimisation du réseau SD-WAN

Peu de termes auront généré autant de buzz que le SD-WAN (ou Software Defined Networking in a Wide Area Network), noyant l'information dans une masse de données utiles ou bien contradictoires. Le SD-WAN signifie ainsi différentes choses pour différentes personnes, et certains essaient encore de comprendre exactement ce qu'il signifie.

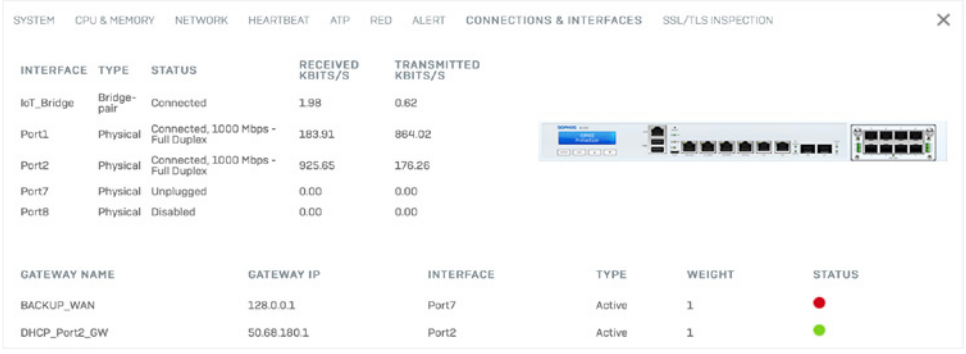
Fondamentalement, le SD-WAN a souvent pour but d'atteindre un ou plusieurs de ces 4 objectifs de mise en réseau :

- **Réduction des coûts de connectivité** – Les connexions MPLS (Multi-Protocol Label Switching) traditionnelles étant coûteuses, les entreprises se tournent vers des options WAN haut débit plus abordables, telles que le câble, l'ADSL et la 3G/4G/LTE.
- **Continuité des activités** – Les entreprises ont besoin de solutions qui assurent la redondance, le routage, le basculement et la préservation des sessions en cas de panne ou de défaillance du réseau WAN.
- Garantir un fonctionnement optimal des applications critiques – Les entreprises exigent une visibilité en temps réel du trafic et des performances des applications afin de maintenir la qualité des sessions des applications professionnelles critiques.
- **Orchestration VPN simplifiée pour les succursales** – L'orchestration VPN entre différents bureaux est souvent complexe et chronophage, c'est pourquoi il est essentiel d'avoir des outils capables de simplifier et d'automatiser le déploiement et la configuration.

Sophos Firewall avec Xstream SD-WAN vous permet d'atteindre vos objectifs SD-WAN les plus ambitieux de manière simple et abordable grâce à un ensemble complet d'options d'orchestration, de gestion et d'optimisation des performances et de la fiabilité du SD-WAN.

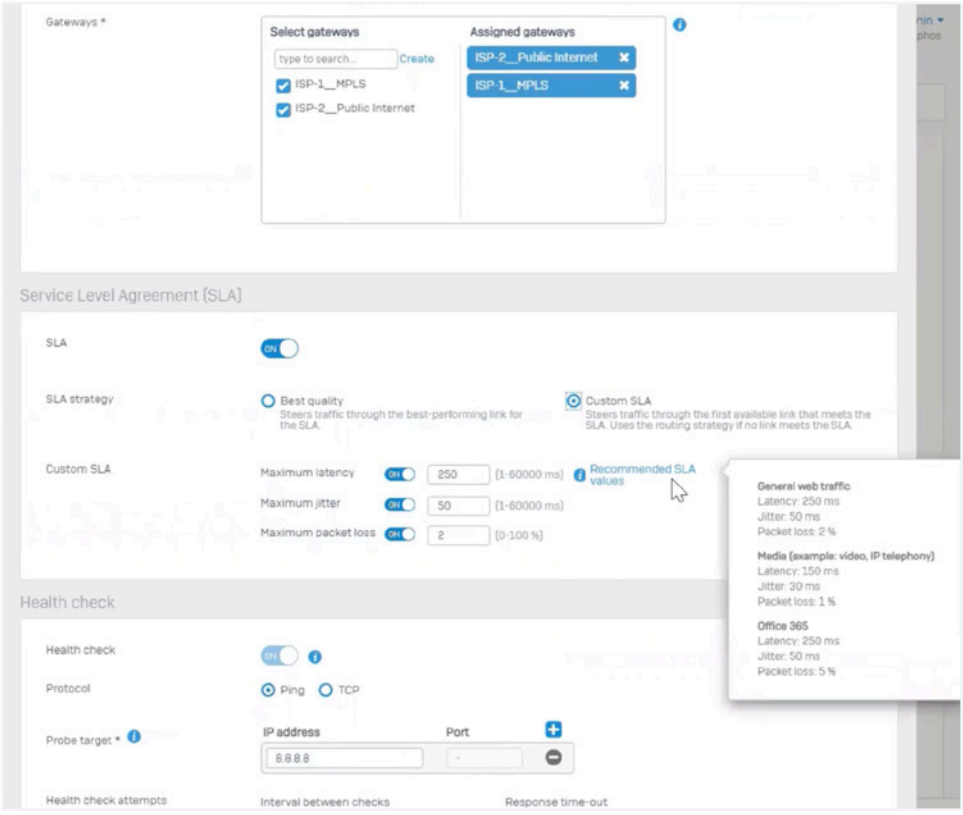
Xstream SD-WAN

La gestion du routage du trafic applicatif sur plusieurs liaisons WAN est un principe clé du SD-WAN, et Sophos Firewall avec Xstream SD-WAN fournit une solution de gestion des liaisons puissante et flexible, que vous utilisiez plusieurs connexions MPLS, DSL, câble ou cellulaires.



L'état de la liaison WAN apparait en bas du widget d'état de l'interface, qui est affiché dans le tableau de bord.

Les profils SD-WAN définissent une stratégie de routage sur plusieurs passerelles de liaison WAN permettant un reroutage transparent et efficace des connexions d'application en fonction des performances de la liaison WAN. Les transitions entre les liaisons se font instantanément, sans impact sur les sessions d'application et sans perturbation, ce qui assure une continuité sans faille, des performances d'application et la meilleure expérience de l'utilisateur final, même dans les environnements Internet les plus perturbés ou instables.



La configuration des profils SD-WAN basés sur les performances est intuitive et facile.

Les stratégies de routage des profils SD-WAN peuvent être basées sur des critères de liaison de type « premier disponible » ou « performances ». Les critères de surveillance des performances comprennent la gigue, la latence et la perte de paquets et peuvent utiliser plusieurs cibles de vérification pour les vérifications PING et TCP.

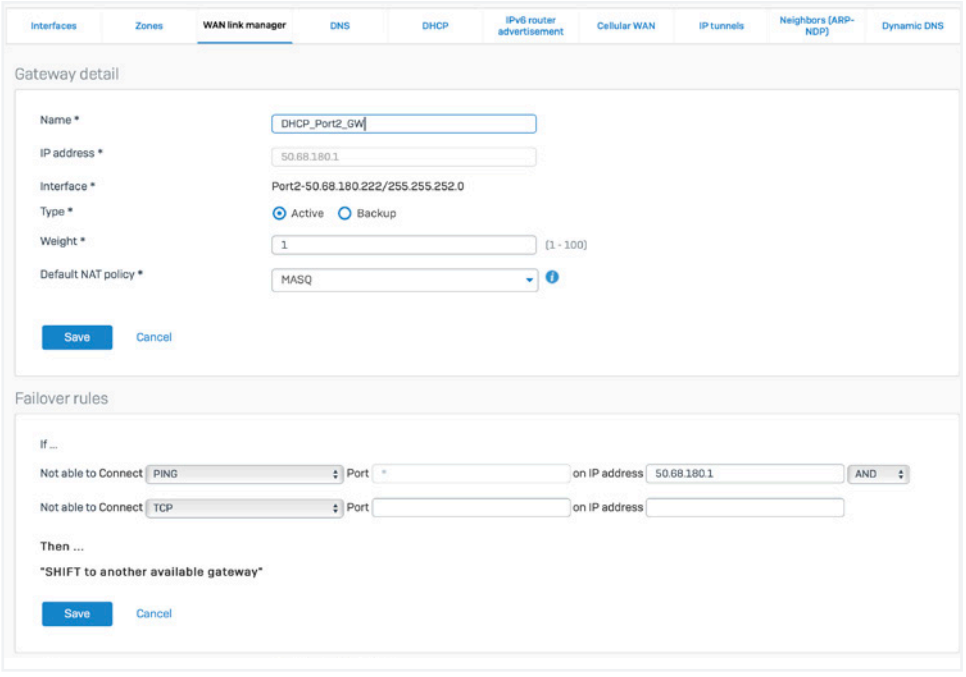
Les profils SD-WAN sélectionnent automatiquement la meilleure liaison en fonction des performances ou selon vos politiques SLA personnalisées qui définissent des valeurs spécifiques pour la gigue, la latence ou la perte de paquets maximales acceptables avant le reroutage sur une liaison plus performante.

Le contrôle des performances de votre réseau SD-WAN est aisé à l'aide de graphiques en temps réel et historiques pour la latence, la gigue et la perte de paquets. Les sélections chronologiques comprennent le temps réel, les dernières 24 ou 48 heures, ou encore la semaine ou le mois derniers. Une journalisation avancée des performances et du routage SD-WAN est également incluse.

Surveillez les performances de vos différentes liaisons WAN en temps réel.

Accélération Xstream FastPath du trafic VPN SD-WAN

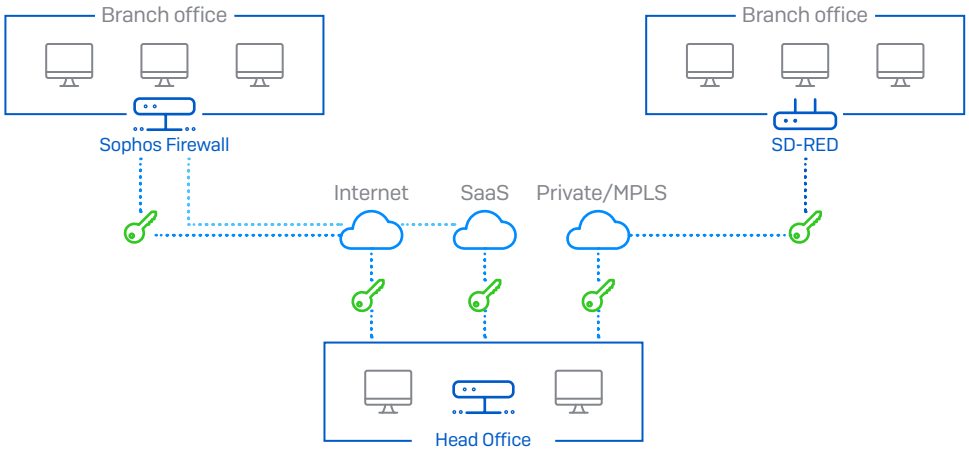
Sophos Firewall utilise les processeurs de flux Xstream intégrés dans les appliances de la série XGS pour fournir une accélération matérielle du trafic des tunnels VPN IPsec. Cela améliore considérablement les performances, en déplaçant vers le processeur de flux Xstream une partie du traitement intensif du CPU requis pour les tunnels IPsec, comme le protocole ESP (Encapsulating Security Payload) pour l'encapsulation/chiffrement et la décapsulation/déchiffrement. Cette nouvelle fonction tire pleinement parti des capacités cryptographiques matérielles du processeur de flux Xstream et présente l'avantage supplémentaire de libérer les ressources du processeur pour d'autres tâches, comme l'inspection profonde des paquets (DPI) du trafic qui en a besoin. L'accélération Xstream FastPath pour le trafic IPsec fonctionne à la fois pour le trafic VPN de site à site et pour l'accès à distance.



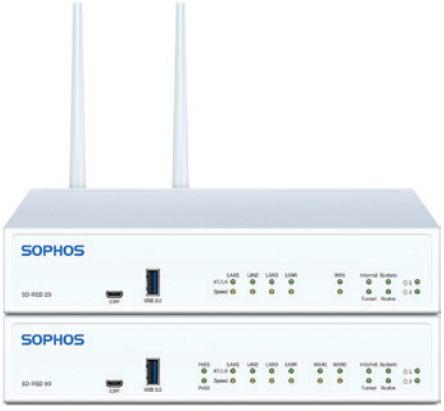
Gestion des liaisons WAN dans Sophos Firewall, avec règles de basculement et d'équilibrage.

Connectivité SD-Branch des bureaux

Avec nos périphériques SD-RED uniques, Sophos est depuis longtemps un pionnier dans le domaine du déploiement et de la connectivité zero-touch. Ils peuvent même être déployés aisément par une personne sans connaissances techniques, et permettent d'établir un tunnel de couche 2 sécurisé entre le périphérique et le pare-feu central.

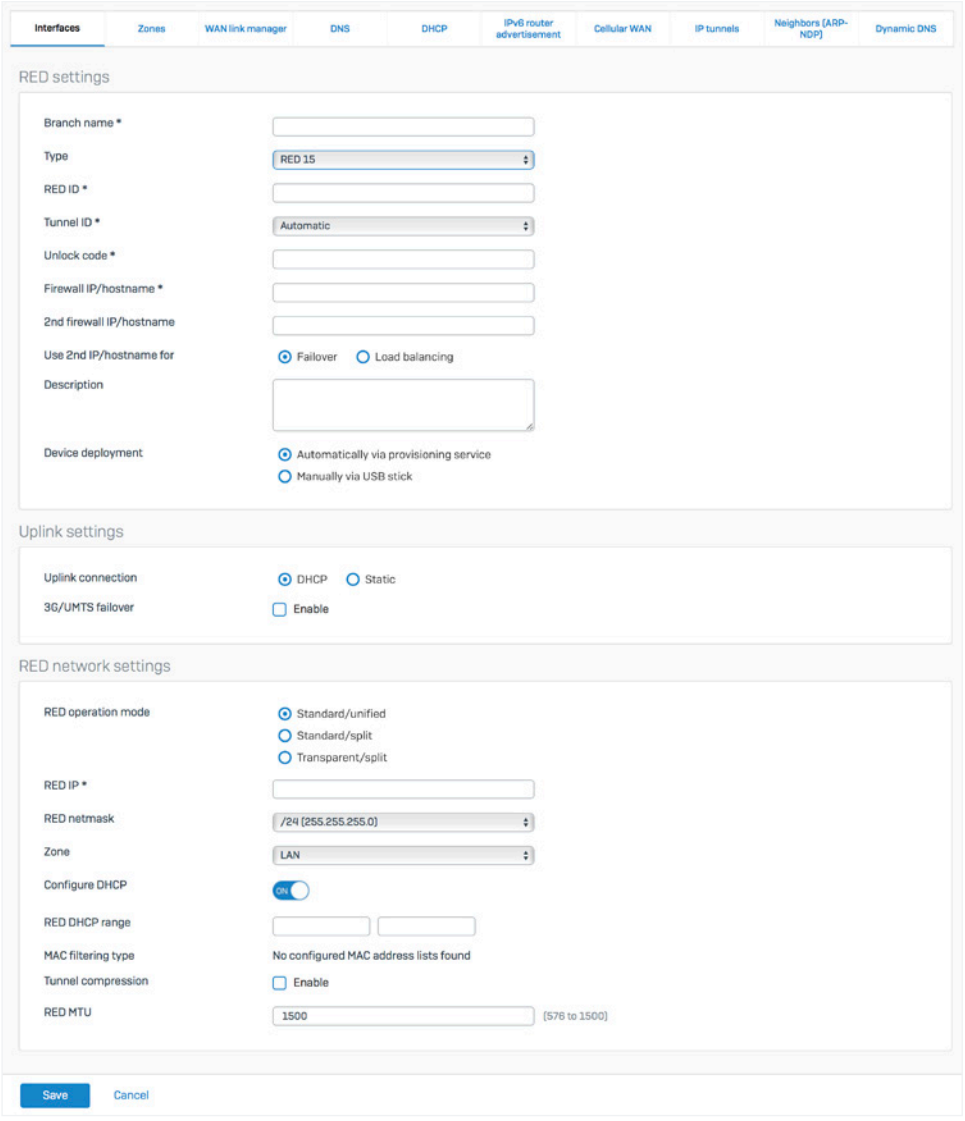


Sophos Firewall et les périphériques SD-RED offrent des options de tunnels pour connecter les succursales via la technologie SD-WAN.



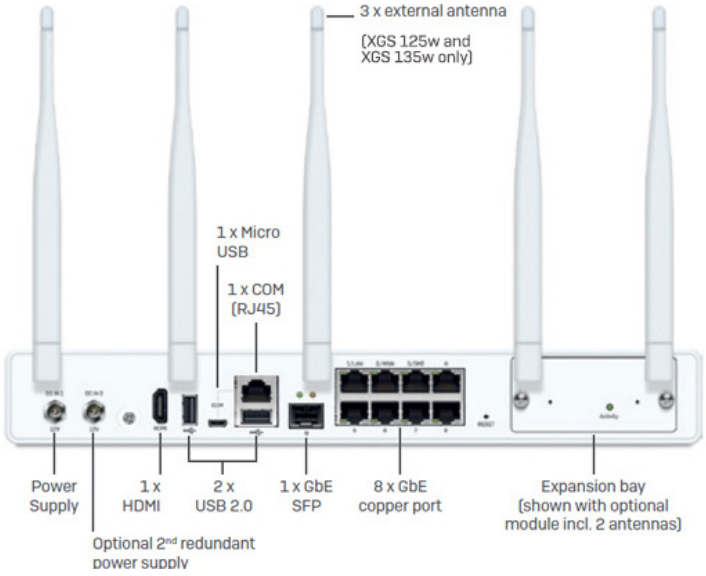
Les périphériques SD-RED offrent une solution de connectivité SD-WAN zero-touch abordable.

Déployer des périphériques SD-RED n'a jamais été aussi simple : Notez tout simplement le numéro de série du boitier dans votre pare-feu et expédiez-le au bureau de destination. Une fois reçu par le site distant, l'installation n'exige aucune connaissance technique : le boitier se connecte automatiquement au service d'approvisionnement Cloud pour établir un tunnel sécurisé avec Sophos Firewall.



Sophos SD-RED est une solution de connectivité entre succursales flexible, sécurisée et abordable.

Nos appliances de bureau de la série XGS sont également d'excellentes solutions de connectivité SD-WAN entre succursales, avec des options de connectivité flexibles, notamment les interfaces cellulaires et VDSL, compatibles avec les connexions en cuivre et la fibre optique. Elles prennent en charge nos tunnels SD-RED sécurisés.

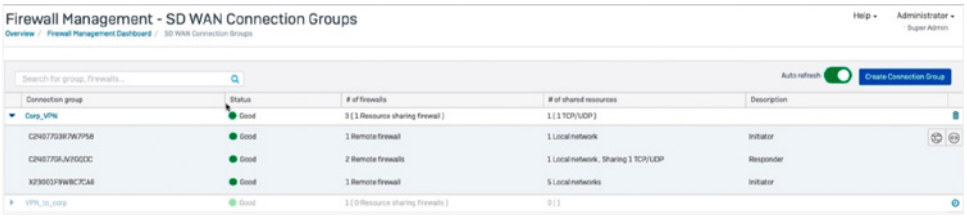


Certains modèles de bureau, tels que XGS 135w (ci-dessus), offrent des options de connectivité WAN LTE/cellulaire, VDSL, cuivre ou fibre optique.

Prise en charge et orchestration VPN

Si vous avez déjà configuré plus de deux tunnels VPN entre différents pare-feux, vous savez à quel point ce processus peut être long et fastidieux. Sophos Firewall prend en charge l'orchestration SD-WAN dans Sophos Central, pour faciliter l'interconnexion de plusieurs tunnels entre plusieurs pare-feux.

Il vous suffit de sélectionner les pare-feux gérés qui doivent participer au groupe de connexion SD-WAN, puis sélectionnez les ressources réseau auxquelles vous souhaitez que chaque site ait accès. En un tour de main, votre réseau superposé VPN SD-WAN prend vie, car toutes les règles d'accès et les tunnels de pare-feu nécessaires, dont la redondance, sont créés automatiquement pour vous.



Configurez rapidement des réseaux superposés SD-WAN complexes en quelques clics et surveillez-les depuis Sophos Central.

Que vous ayez besoin d'un réseau maillé complet, d'une topologie en étoile ou d'un mix des deux, Sophos Central s'occupera automatiquement de tous les tunnels nécessaires et de la configuration du pare-feu pour activer votre réseau SD-WAN superposé.

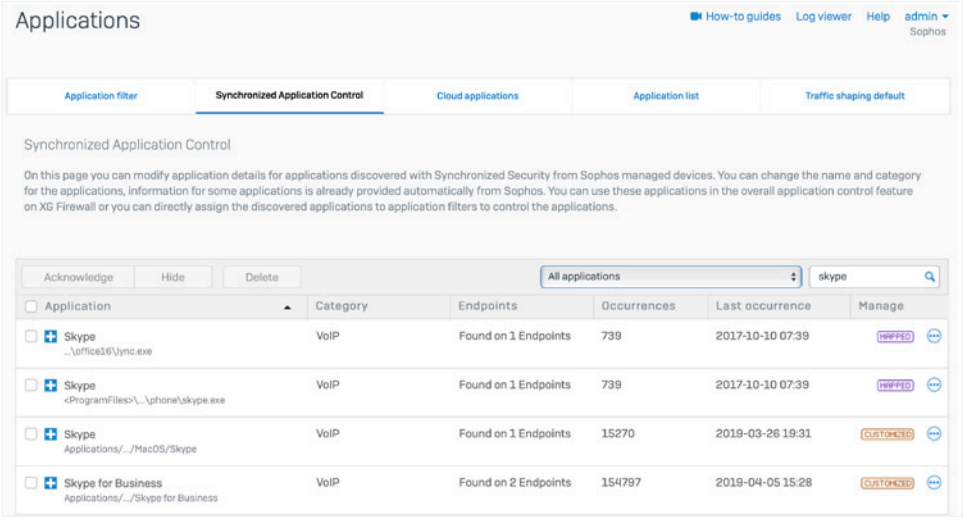
Bien sûr, Sophos Firewall est compatible avec toutes les options VPN de site à site classiques, telles que IPsec et SSL. Il prend même en charge notre tunnel SD-RED de couche 2 ; le routage est très robuste et se montre fiable dans des situations de forte latence telles que les liaisons satellites.

Visibilité et routage des applications

Une autre fonctionnalité qui permet de remplir les objectifs SD-WAN est la sélection et le routage du chemin de l'application, qui sont utilisés pour assurer une qualité suffisante et réduire la latence pour les applications critiques telles que la VoIP.

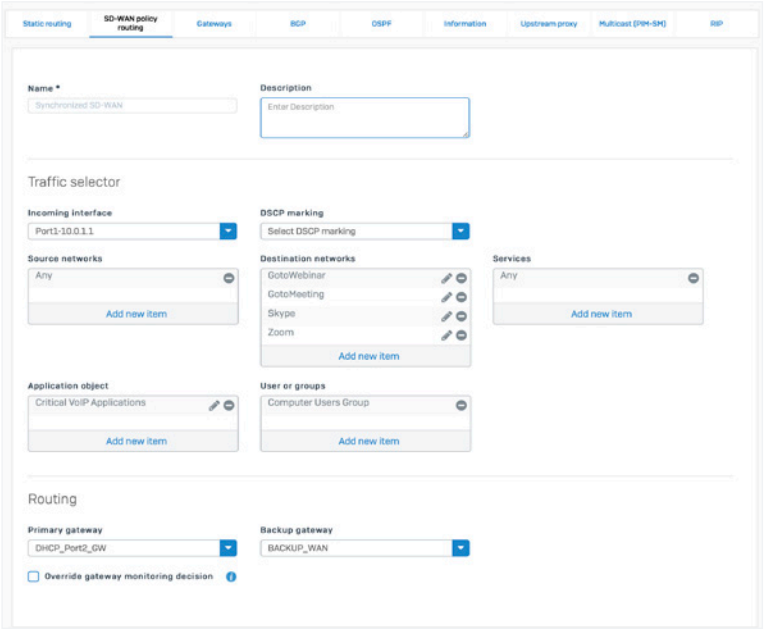
Il est bien évidemment impossible de router ce qui n'a pas été identifié. Il est donc crucial d'avoir une visibilité claire sur les applications et de pouvoir les identifier de manière fiable. C'est un domaine où Sophos Firewall et la Sécurité Synchronisée de Sophos offrent un avantage incroyable. Le contrôle synchronisé des applications offre une visibilité complète sur toutes les applications connectées au réseau ; cela permet d'identifier les applications critiques pour l'entreprise, notamment les applications complexes et personnalisées.

Le SD-WAN synchronisé, une fonctionnalité de la Sécurité Synchronisée, offre d'autres avantages grâce au routage des applications SD-WAN. Le SD-WAN synchronisé 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. Désormais, les applications jusque-là non identifiées peuvent également être ajoutées aux politiques de routage SD-WAN, offrant ainsi un niveau inégalé de contrôle et de fiabilité du routage des applications.



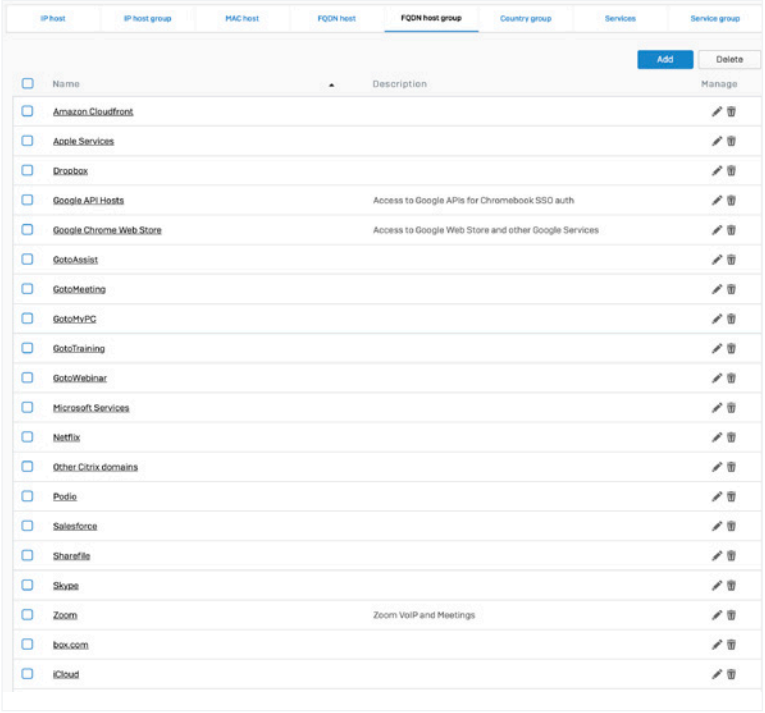
Le contrôle synchronisé des applications identifie 100 % des applications connectées au réseau, permettant ainsi de router et de prioriser les applications critiques.

Sophos Firewall permet également le routage et la sélection du chemin en fonction des applications dans chaque règle de pare-feu, y compris par utilisateur et par groupe. Des contrôles granulaires du routage selon la politique (Policy-Based Routing - PBR) permettent de définir le routage via la connexion WAN de la passerelle principale ou de secours, et de le configurer pour la direction des replay. Ensemble, ces caractéristiques permettent de diriger facilement le trafic des applications importantes vers l'interface WAN optimale.



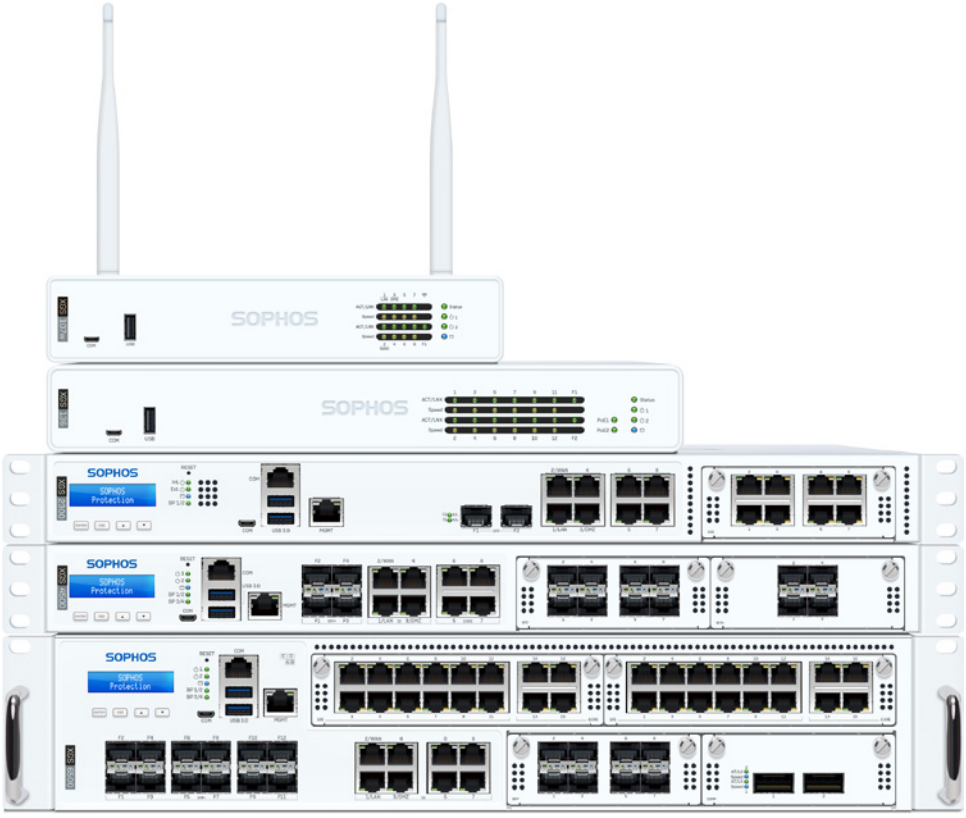
Le routage SD-WAN selon la politique offre des outils flexibles pour diriger le trafic généré par les applications critiques.

Sophos Firewall offre non seulement la possibilité de configurer vos propres objets FQDN (Fully Qualified Domain Name), mais inclut également des milliers de noms de domaine prédéfinis correspondant aux services Cloud SaaS les plus courants.



Les objets hôtes FQDN prédéfinis simplifient la sélection du chemin et le routage basé sur les applications.

Ajoutez Sophos Firewall à n'importe quel réseau - en toute simplicité



Nos appliances matérielles Sophos Firewall offrent des options de déploiement au choix avec l'intégration de ports bypass en série sur tous les modèles 1U et en option dans les modules Flexi Port de nos appliances 2U. Les ports bypass permettent d'installer Sophos Firewall en mode relais conforme avec des pare-feux déjà en place. Si Sophos Firewall doit être arrêté ou redémarré pour mettre à jour le firmware, les ports bypass assurent la continuité des activités en permettant au trafic de continuer à circuler sans perturber le réseau. Cette fonction permet de nouvelles options de déploiement qui sont totalement sans risque, et ne nécessitent pas le remplacement de l'infrastructure de réseau existante. De plus, notre protection Next-Gen Endpoint, Intercept X, fonctionne en complément de tout autre antivirus de bureau existant, permettant le déploiement complet de la sécurité synchronisée de Sophos sur n'importe quel réseau, sans avoir besoin de remplacer quoi que ce soit.

Sophos Firewall : La cybersécurité en toute simplicité.

Demande de tarif

Demandez un devis personnalisé selon vos besoins sans obligation d'achat sur sophos.fr/firewall-quote

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

22-03-30 FR (DD)

SOPHOS