LES RISQUES CACHÉS DES PARE-FEUX MODERNES

Découvrez comment faire en sorte que votre pare-feu ne soit pas utilisé dans le cadre d'une attaque

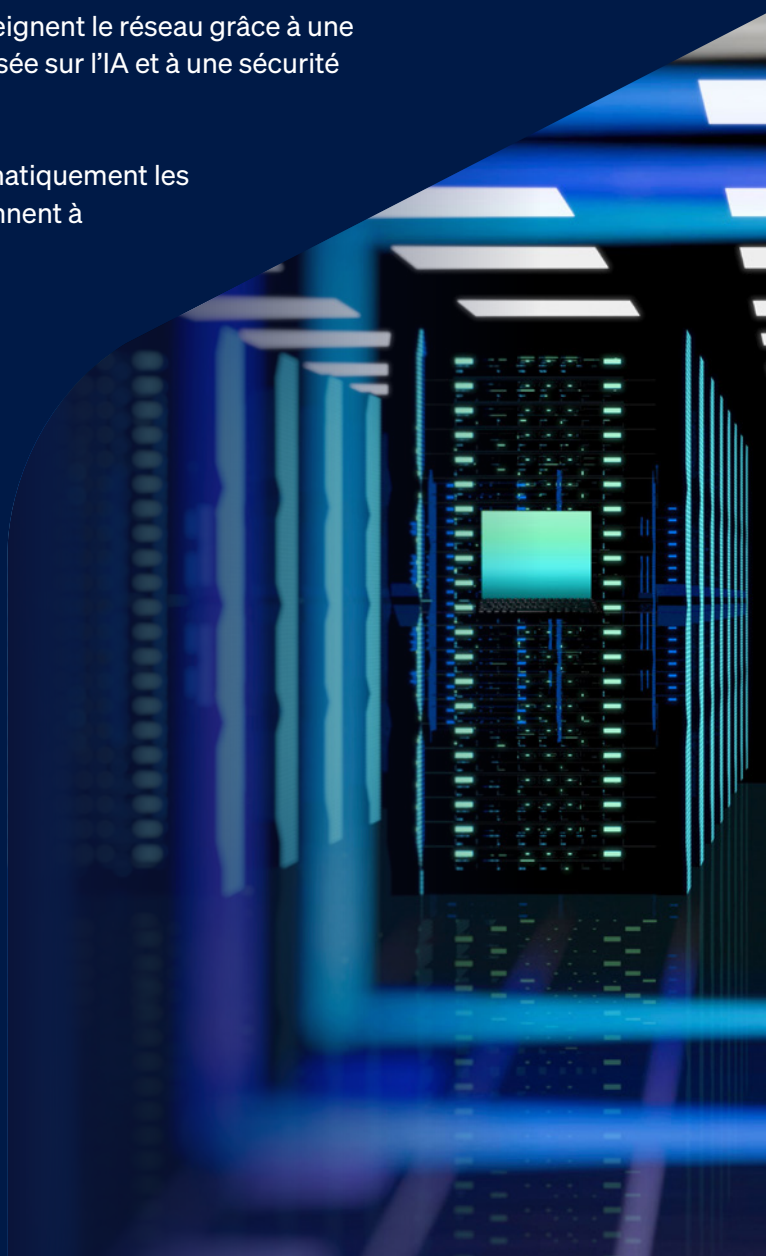
Résumé

Les pare-feux réseau font l'objet d'attaques ciblées d'une ampleur sans précédent. Il ne se passe presque pas un jour sans qu'un article évoque l'exploitation d'une nouvelle faille de pare-feu. Ce constat met en lumière une réalité inquiétante : les pare-feux — ces systèmes précisément conçus pour protéger les réseaux — constituent un risque important et sont devenus des cibles de choix pour des attaquants sophistiqués[1]. Ces attaques exploitent non seulement les failles du logiciel de pare-feu lui-même, mais aussi les vulnérabilités fondamentales dans la manière dont les organisations abordent la sécurité réseau.

Ce livre blanc introduit une approche complète de la sécurité réseau moderne, structurée autour de trois piliers, pour traiter les menaces avant, pendant et après le déploiement :

- **Durcissement :** Réduisez de manière proactive votre surface d'attaque grâce aux principes du « Secure by Design », aux correctifs automatisés, à l'audit des configurations et aux contrôles d'accès Zero Trust.
- **Protection :** Bloquez les menaces avant qu'elles n'atteignent le réseau grâce à une inspection avancée, à une détection des menaces basée sur l'IA et à une sécurité haute performance sans compromis.
- **Détection et réponse :** Identifiez et neutralisez automatiquement les adversaires actifs sur le réseau avant qu'ils ne parviennent à mener leur attaque à bien.

La plupart des solutions de sécurité réseau se concentrent principalement sur la protection, laissant l'infrastructure réseau vulnérable et incapable d'identifier une attaque en cours et encore moins d'y réagir. Ce document propose aux professionnels de la sécurité réseau et aux équipes informatiques une feuille de route pratique pour mettre en œuvre efficacement ces trois piliers.



Le paysage actuel des menaces

Les pare-feux sont pris d'assaut

Les pare-feux réseau se situent à la frontière entre les réseaux internes fiables et le monde extérieur hostile. De par cette position stratégique, ils sont devenus des cibles de grande valeur. Les actualités témoignent d'un flux constant d'attaques ciblant les principaux fournisseurs de pare-feu. Si certaines attaques exploitent des vulnérabilités déjà connues qui n'ont toujours pas été corrigées dans les environnements de production, d'autres ciblent des configurations par défaut inadéquates ou des problèmes de conception qui créent des failles exploitables[2].

Frontier AI a jeté de l'huile sur le feu en ce qui concerne les cyberattaques basées sur l'IA agentique. Le modèle Claude Mythos d'Anthropic a mis au jour plus de 2 000 nouvelles vulnérabilités de type « zero-day » en seulement quelques semaines, marquant un tournant décisif tant pour les attaquants que pour les défenseurs.

Si les gros titres consacrés à Frontier AI ont mis l'accent sur la capacité de l'IA à détecter des vulnérabilités à grande échelle, ce qui importe davantage, c'est la manière dont l'IA réduit le temps de réponse, raccourcissant ainsi le délai entre la découverte d'une vulnérabilité et son impact sur l'activité. En effet, l'IA permet aux attaquants d'agir plus rapidement, à plus grande échelle et avec moins d'obstacles qu'auparavant.

Les conséquences vont bien au-delà des organisations individuelles. Lorsque des acteurs malveillants parviennent à compromettre un pare-feu, ils obtiennent non seulement un accès direct au réseau, mais aussi, potentiellement, des identifiants et un accès aux fournisseurs et aux clients de l'organisation – en d'autres termes, les clés du royaume.

+ 2 000 %

de vulnérabilités « zero-day » découvertes par Mythos en seulement sept semaines

Les trois piliers de la sécurité réseau

Une sécurité réseau efficace nécessite une approche globale qui prend en compte les menaces tout au long de leur cycle de vie : avant, pendant et après le déploiement. Cela donne lieu à trois piliers de défense distincts mais interdépendants :

DURCISSEMENT

RÉDUIRE LA SURFACE D'ATTAQUE

Concevez, développez et maintenez des solutions pour minimiser les risques, réduire l'exposition et renforcer l'infrastructure IT contre les attaques

PROTECTION

BLOQUER LES ATTAQUES AVANT QU'ELLES N'ATTEIGNENT LE RÉSEAU

Déployez la meilleure protection possible pour identifier et bloquer les attaquants et les exploits de pénétrer sur le réseau

DÉTECTION ET RÉPONSE

STOPPER LES ATTAQUES ACTIVES DANS LEUR ÉLAN

Utilisez la détection et la réponse pour identifier et isoler automatiquement les adversaires actifs

L'angle mort de la sécurité

La plupart des pare-feux réseau se concentrent presque exclusivement sur la protection en temps réel, comme le filtrage du trafic, la prévention des menaces et les systèmes de prévention des intrusions. Bien que ces fonctionnalités soient indispensables, le fait de se concentrer uniquement sur l'inspection du trafic en temps réel rend les organisations vulnérables.

L'actualité le montre chaque jour : la plupart des pare-feux et des équipes informatiques ne parviennent pas à sécuriser efficacement leur environnement, c'est-à-dire à réduire la surface d'attaque. Les pare-feux restent vulnérables, la fatigue liée aux correctifs incessants se généralise, des produits en fin de vie restent présents à des points critiques, et les VPN d'accès à distance demeurent largement utilisés, malgré leurs lacunes en matière de sécurité. Dans le même temps, la plupart des pare-feux déployés ne disposent d'aucune capacité de détection et de réponse permettant de contrer les attaques en cours avant qu'elles n'aient des conséquences.

Pour remédier à ce déséquilibre, il faut accorder une attention particulière aux aspects négligés, notamment le durcissement de l'infrastructure, qui constitue le fondement d'une posture de sécurité résiliente.

Durcissement de l'infrastructure réseau — Réduction des risques

Le durcissement consiste à réduire de manière proactive la surface d'attaque, en éliminant les vulnérabilités avant que les attaquants n'aient le temps de les découvrir puis de les exploiter.

Stratégies essentielles de durcissement

1. **Réduire l'exposition au minimum :** Passez régulièrement en revue les systèmes et les infrastructures exposés à Internet, et réduisez le nombre de points d'entrée potentiels.

2. **S'assurer que les systèmes sont « Secure by Design » :** Choisissez des produits conçus dès l'origine autour de la sécurité.

3. **Auditer la configuration et maintenir les logiciels/firmwares à jour :** Assurez le respect des bonnes pratiques de sécurité grâce à une surveillance continue.

4. **Éliminer l'usurpation d'identité en tant que vecteur :** Renforcez la sécurité des accès et de l'authentification. Déployez l'authentification multifacteur (MFA) pour tous les utilisateurs et passez du VPN au principe Zero Trust Network Access (ZTNA).

Réduire l'exposition

Passez régulièrement en revue votre infrastructure réseau et déterminez à quelle étape de son cycle de vie se trouve chaque composant. Remplacez de manière proactive tout élément arrivant en fin de vie. Le coût de la mise à jour d'une technologie vieillissante est bien inférieur à l'impact potentiel d'une attaque par ransomware qui exploiterait des systèmes dont le support a pris fin.

Vous pouvez également en profiter pour simplifier et consolider votre infrastructure réseau. Si vous utilisez des appareils distincts pour le pare-feu, le VPN, le ZTNA, le SD-WAN, le DNS et le filtrage Web, envisagez de regrouper ces fonctionnalités sur une seule et même plateforme. La réduction du nombre d'appareils et de solutions dans votre environnement peut permettre de réduire la complexité, d'améliorer l'efficacité et de renforcer la résilience globale.

Il est tout aussi important de maintenir votre infrastructure IT à jour. Les mises à jour du firmware et des logiciels comprennent souvent des correctifs de sécurité essentiels destinés à corriger des failles que des attaquants pourraient exploiter. Si cela suppose d'y consacrer du temps, l'impact reste sans commune mesure avec celui d'une attaque par ransomware.

S'assurer que les systèmes sont « Secure by Design »

Le secteur de la cybersécurité doit accepter une réalité fondamentale : Les entreprises ont autant besoin de produits sûrs que de produits de sécurité. Lorsque les adversaires s'attaquent aux outils conçus pour protéger les organisations, celles-ci ont besoin de produits de sécurité qui soient eux-mêmes sécurisés. Les organisations ont donc tout intérêt à faire appel à des fournisseurs qui font preuve d'un engagement sincère en faveur de la sécurité et de la transparence — notamment en communiquant de manière transparente sur les violations de données, ce qui constitue la bonne approche même lorsque cela peut s'avérer délicat.

Les entreprises ont autant besoin de produits sûrs que de produits de sécurité.

Les principes clés du Secure by Design sont les suivants :

- MFA intégrée par défaut dans tous les systèmes.
- Suppression des mots de passe et identifiants par défaut.
- Implémentation de correctifs de sécurité automatisés qui limitent au maximum les perturbations.
- Procédures de divulgation des vulnérabilités rapides et transparentes.
- Audits de sécurité réguliers et des tests d'intrusion.
- Pratiques de cycle de vie de développement sécurisé intégrées à l'ingénierie produit.

Vérifier la configuration et maintenir les systèmes à jour

Les pare-feux réseau sont complexes, ce qui les rend vulnérables aux erreurs de configuration et aux paramètres risqués susceptibles de créer involontairement des failles pour les attaquants. Le défi consiste à identifier les erreurs de configuration et à déterminer où se situent ces vulnérabilités. Parfois, le problème est évident, mais le plus souvent, les failles restent cachées jusqu'à ce que quelqu'un en tire parti. La plupart des pare-feux ne fournissent aucune information concernant les paramètres de configuration à risque. Choisissez-en un qui dispose de cette fonctionnalité.

La lassitude face au ballet incessant des correctifs est bien réelle, mais elle n'est pas une fatalité. Les processus traditionnels de mise à jour des correctifs entraînent une charge opérationnelle importante. Des failles de sécurité peuvent être découvertes à tout moment, et aujourd'hui, grâce à l'IA, à un rythme alarmant. La fréquence des mises à jour requises peut submerger les équipes administratives. La plupart des pare-feu vantent leurs « mises à jour automatiques », mais celles-ci exigent généralement que les administrateurs planifient des temps d'arrêt, installent le firmware et redémarrent les appareils.

Les organisations doivent se poser une question simple : Pourquoi l'application des correctifs n'est-elle pas vraiment toujours automatisée ? La réponse est simple : la plupart des fournisseurs n'ont pas conçu leurs logiciels pour prendre en charge les mises à jour de sécurité en temps réel par OTA. Cependant, les approches architecturales modernes peuvent permettre la mise en place de capacités de correctifs automatisés qui :

- Appliquent automatiquement les correctifs de sécurité sans intervention de l'administrateur.
- Ne nécessitent ni interruption de service ni redémarrage du système.
- Font le lien entre les principales mises à jour du firmware.
- Réduisent la fenêtre de vulnérabilité de plusieurs mois à quelques heures ou quelques jours.

Les mauvaises configurations constituent un autre point d'entrée courant pour les attaquants. Des ensembles de règles de pare-feu complexes, des modifications de politique mal documentées et l'accumulation progressive de changements de configuration peuvent, sans le vouloir, exposer par inadvertance des points d'accès qui devraient être sécurisés.

Le défi réside dans l'identification : Comment les administrateurs peuvent-ils identifier les problèmes de configuration ? Les pare-feux traditionnels ne fournissent aucune information sur la sécurité de la configuration. Les approches modernes intègrent des fonctionnalités de contrôles d'état d'intégrité automatisés qui :

- Vérifient en permanence la configuration du pare-feu par rapport aux bonnes pratiques établies et aux critères de référence du CIS.
- Offrent une vue d'ensemble, via un tableau de bord, des contrôles réussis et échoués.
- Attribuent des niveaux de gravité à chaque élément évalué.
- Permettent d'explorer les détails pour modifier rapidement les paramètres ou documenter les exceptions choisies.

Ces fonctionnalités offrent une visibilité dont les pare-feu traditionnels sont dépourvus, garantissant ainsi que la posture de sécurité reste optimale même lorsque les configurations évoluent au fil du temps.

Éliminer l'usurpation d'identité en tant que vecteur d'attaque

67 % des incidents examinés par Sophos en 2025 ont pour origine une compromission d'identifiants[3], ce qui fait de la lutte contre les attaques ciblant l'identité une priorité absolue en matière de renforcement de la sécurité. Il est ainsi plus que jamais essentiel d'adopter les principes du « Zero Trust » : Ne faites confiance à rien ni personne, vérifiez tout.

Pour les organisations qui dépendent encore des VPN d'accès à distance, la migration vers une solution alternative doit devenir une priorité. Le ZTNA offre une alternative moderne au VPN qui s'inscrit dans les principes du « Zero Trust ». Plutôt que d'accorder un accès général au réseau, le ZTNA offre un accès précis à des applications et ressources spécifiques. Si un appareil est compromis, le ZTNA peut automatiquement limiter ou bloquer son accès jusqu'à sa remédiation.

Ainsi, si un attaquant parvient tout de même à compromettre un appareil connecté via ZTNA, il n'aura accès qu'aux applications spécifiques auxquelles l'utilisateur était autorisé à accéder — et non à l'ensemble du réseau. Le périmètre de sécurité se déploie là où il est réellement nécessaire : Autour des applications et données critiques.

67 %

des incidents examinés par Sophos en 2025 ont pour origine une compromission d'identité

Le ZTNA présente six avantages majeurs par rapport au VPN :

1. **MFA systématique :** L'authentification multifacteur (MFA) est obligatoire pour tous les accès, sans exception, ce qui élimine les identifiants compromis et les attaques par force brute en tant que vecteurs d'attaque potentiels.

2. **L'état d'intégrité de l'appareil fait partie de la politique d'accès :** La conformité et l'état d'intégrité des appareils sont évalués en permanence dans le cadre des décisions d'accès.

3. **Fonctionne partout :** Le ZTNA fonctionne aussi bien lorsque les utilisateurs sont connectés au réseau de l'entreprise que lorsqu'ils travaillent à distance, garantissant ainsi une sécurité constante, quel que soit leur emplacement.

4. **Connectivité transparente :** Les implémentations ZTNA modernes offrent des connexions transparentes et fiables, tout en évitant les problèmes de connexion qui affectent souvent les VPN.

5. **Meilleure visibilité :** Les organisations bénéficient d'une visibilité claire sur les ressources auxquelles les utilisateurs accèdent, ce qui facilite la planification des capacités et la gestion des licences.

6. **Administration simplifiée :** L'ajout et la suppression d'utilisateurs, le déploiement de nouvelles applications et la gestion des politiques d'accès sont tous plus simples avec le ZTNA qu'avec un VPN traditionnel.

Les stratégies de renforcement de la sécurité doivent inclure la suppression des VPN d'accès à distance et le déploiement d'une architecture « Zero Trust » avec l'application systématique de l'authentification multifacteur (MFA).

Protection – Blocage des menaces au niveau de la passerelle

Déployez une protection complète pour détecter et bloquer les menaces avant qu'elles n'atteignent le réseau. Cela comprend une inspection TLS avancée, une détection des menaces « zero-day » optimisée par l'IA et une analyse intelligente du trafic qui garantit des performances élevées sans compromettre la sécurité.

Exigences actuelles en matière de protection

- **Inspection TLS 1.3 haute performance :** La majeure partie du trafic Web est désormais chiffrée, et les attaquants dissimulent de plus en plus souvent leurs logiciels malveillants et leur trafic de commande et de contrôle au sein de canaux chiffrés. Les pare-feux doivent déchiffrer et analyser le trafic TLS de manière intelligente, en appliquant des règles basées sur des politiques qui concilient exigences de sécurité, considérations relatives à la confidentialité et impact sur les performances.

- **Accélération matérielle :** Les opérations cryptographiques et l'analyse du trafic sont des tâches très gourmandes en ressources informatiques. Dans les architectures de pare-feu modernes, les applications fiables et les opérations cryptographiques devraient être prises en charge par accélération matérielle, afin de libérer des ressources pour les tâches d'inspection approfondie du trafic non fiable.

- **Protection contre les menaces Zero-day optimisée par IA :** La détection basée sur les signatures reste utile, mais s'avère insuffisante face aux nouvelles menaces. L'analyse des fichiers statiques optimisée par l'IA, associée à un environnement de sandboxing dynamique en temps réel, permet d'identifier et de bloquer les menaces de type « zero-day » avant qu'elles n'atteignent le réseau — des menaces qui passent complètement sous les radars des systèmes traditionnels basés sur les signatures.

Les capacités de protection ET les performances devraient s'améliorer avec le temps, et non se dégrader. Les pare-feux basés sur des architectures programmables peuvent bénéficier à la fois de mises à niveau de sécurité et d'améliorations de performances grâce à des mises à jour logicielles, ce qui prolonge la durée de vie effective des investissements matériels. Contrairement aux pare-feux traditionnels, dont les performances diminuent à mesure que de nouvelles fonctionnalités de sécurité sont ajoutées, les architectures modernes maintiennent ou améliorent leurs performances grâce à une optimisation continue.

Détection et réponse – Mettre fin aux attaques en cours

Lorsque des adversaires parviennent à franchir les défenses, leur présence est rapidement détectée et la menace automatiquement contenue. Une solution NDR (Network Detection and Response), associée à une coordination entre les différentes solutions, permet d'identifier et d'isoler des systèmes compromis avant que les attaquants n'atteignent leurs objectifs.

Network Detection and Response (NDR)

La détection et la réponse sur le réseau s'appuient sur l'intelligence artificielle et l'analyse comportementale pour identifier les adversaires actifs déjà présents sur le réseau. Contrairement aux solutions de défense périmétrique qui analysent le trafic entrant, le NDR examine les schémas de trafic au sein du réseau à la recherche d'indicateurs de compromission :

- Mouvements latéraux anormaux entre les systèmes.
- Communications de type « command and control » vers des hôtes externes suspects.
- Modèles d'accès aux données anormaux.
- Tentatives d'élévation des privilèges.
- Activités de reconnaissance visant à analyser les ressources internes.

Le NDR a toujours été une fonctionnalité haut de gamme nécessitant des produits distincts et des investissements importants. Les organisations avant-gardistes intègrent désormais des fonctionnalités NDR directement dans leurs plateformes de pare-feu, rendant ainsi cette fonctionnalité essentielle à la portée des entreprises de taille moyenne.

Réponse automatisée

Une détection sans intervention revient simplement à signaler aux administrateurs qu'une compromission a eu lieu, souvent trop tard pour prévenir les dommages. A contrario, les capacités de réponse automatisée permettent de maîtriser immédiatement la situation.

Lorsqu'une menace est détectée n'importe où dans l'infrastructure de sécurité — que ce soit par le pare-feu, la protection Endpoint, la sécurité des messageries ou par un analyste MDR —, vous avez besoin d'une solution de sécurité capable de coordonner une réponse automatisée sur l'ensemble des produits de sécurité intégrés. Cette approche permet d'empêcher un appareil compromis de communiquer avec d'autres systèmes, de lui bloquer l'accès aux applications et aux données, et d'éviter tout déplacement latéral.

Cette réponse automatisée s'avère particulièrement utile en dehors des heures de bureau, période durant laquelle 88 % du déploiement des attaques par ransomware a lieu[4]. Considérez le « scénario du vendredi soir » suivant : Vendredi soir, à une heure avancée, un attaquant parvient à compromettre un appareil alors que les équipes sécurité sont absentes. Sans aucune réponse automatique, l'acteur malveillant a devant lui tout le week-end pour se déplacer latéralement, effectuer des élévations de privilèges et déployer son ransomware. L'organisation découvrira la violation le lundi matin, avec l'apparition de fichiers chiffrés et de demandes de rançon.

Si une réponse automatisée sur l'ensemble des produits est prévue, la première intrusion déclenche immédiatement l'isolement. L'attaquant se retrouve en quarantaine, isolé dans un segment, incapable d'avancer ou de se déplacer. Le lundi matin, les équipes sécurité font face à une alerte active sur une menace déjà contenue, plutôt qu'à un incident de ransomware généralisé.

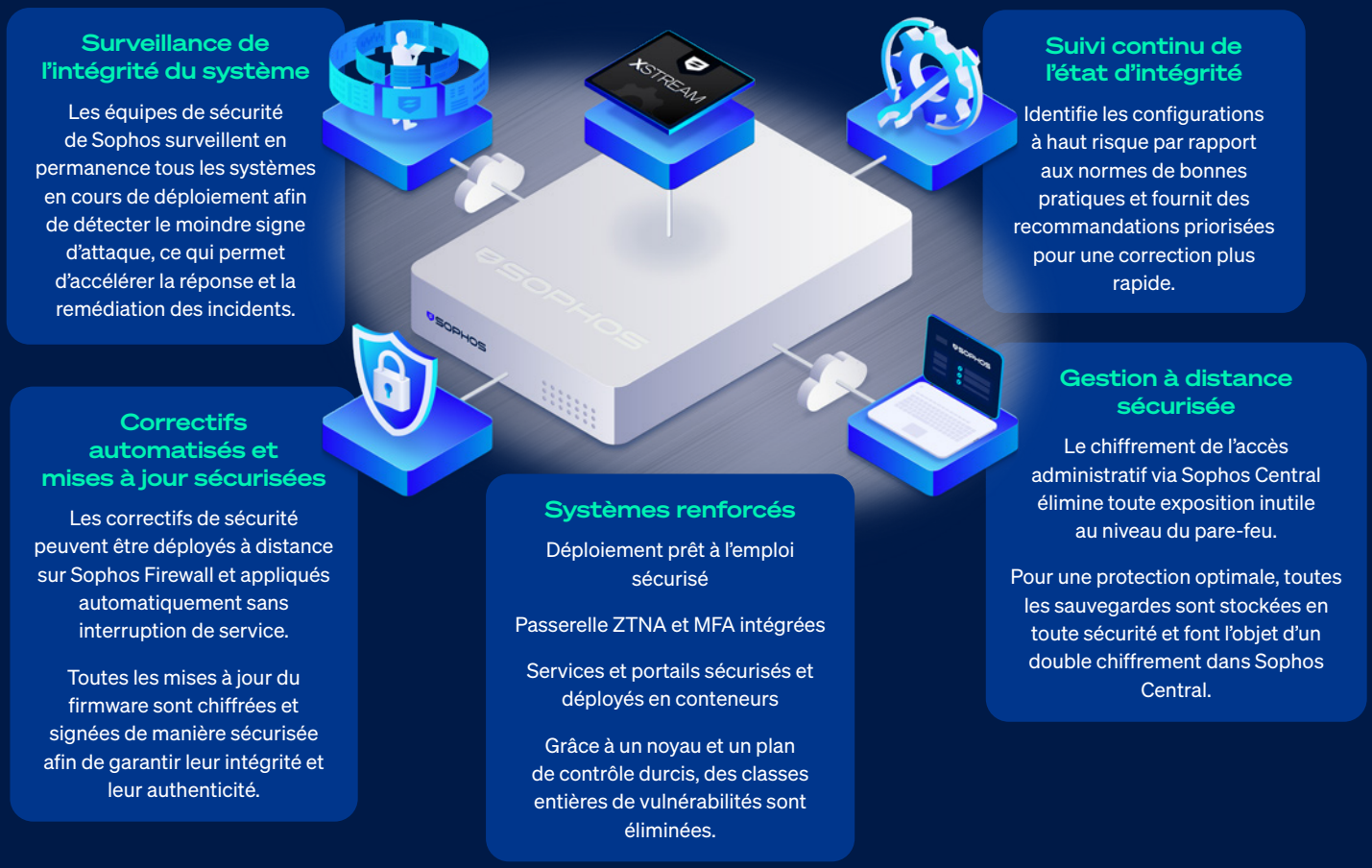
88 %

des attaques de ransomware sont déployées en dehors des horaires de bureau classiques

Sophos Firewall : Une solution complète

Si le cadre à trois piliers présenté ci-dessus correspond aux bonnes pratiques en matière de sécurité, sa mise en œuvre efficace nécessite de choisir une infrastructure suffisamment avancée pour prendre en charge chacun des piliers.

Sophos Firewall se distingue comme l'une des rares solutions à avoir réalisé des investissements considérables dans ces trois domaines, offrant ainsi de nombreuses fonctionnalités que les acheteurs ne trouveront nulle part ailleurs.



Secure by Design (la sécurité dès la conception)

Sophos Firewall répond aux exigences en matière de durcissement de la posture de sécurité grâce à une approche globale « Secure by Design » qui élimine la charge de travail généralement associée à la maintenance d'une infrastructure sécurisée.

Installation automatique des correctifs : Élimine la fatigue liée aux correctifs

La fonctionnalité unique d'installation automatique des correctifs de Sophos Firewall réduit radicalement la durée d'exposition aux vulnérabilités :

- Les correctifs de sécurité sont déployés directement (mises à jour OTA) dès que Sophos les a développés et validés.
- Les correctifs s'appliquent sans aucune intervention de l'administrateur.
- Aucune interruption de service ni aucun redémarrage n'est nécessaire.
- Les correctifs assurent la continuité entre les versions majeures du firmware, garantissant ainsi une protection continue.

Cet avantage architectural réduit la fenêtre de vulnérabilité de plusieurs mois à quelques heures ou quelques jours. Lorsque Sophos détecte et corrige une vulnérabilité, tous les clients de Sophos Firewall sont immédiatement protégés, sans qu'il soit nécessaire d'attendre que les administrateurs bousculent leur emploi du temps ou planifient des fenêtres de maintenance.

Sophos est le seul grand fournisseur de pare-feu à proposer des mises à jour de sécurité véritablement automatiques et sans interruption de service. À elle seule, cette fonctionnalité constitue une avancée décisive dans le domaine de la sécurisation.

Contrôle d'état d'intégrité : Audit continu de la configuration

La fonctionnalité de contrôle d'état d'intégrité de Sophos Firewall offre une visibilité sans précédent sur la configuration :

- Vérifie en permanence la conformité de dizaines de paramètres de configuration de pare-feu par rapport aux critères CIS et aux bonnes pratiques du secteur.
- Présente les vérifications réussies et ratées directement sur le tableau de bord du centre de contrôle.
- Attribue un niveau de gravité à chaque élément évalué (critique, élevé, moyen, faible).
- Permet d'explorer les détails pour modifier rapidement les paramètres ou documenter les exceptions choisies.
- Se met à jour automatiquement pour suivre l'évolution des bonnes pratiques.

Cette surveillance proactive des configurations garantit le maintien d'une posture de sécurité optimale, même lorsque les configurations évoluent au fil du temps. Les administrateurs reçoivent des alertes immédiates concernant les paramètres potentiellement à risque avant que les attaquants ne puissent les détecter et les exploiter.

Surveillance de l'intégrité à distance

Sophos est le seul à assurer la surveillance de l'ensemble de son parc de Sophos Firewalls. Grâce au capteur Linux intégré à la solution Sophos Extended Detection and Response, nous pouvons surveiller l'intégrité du système, notamment :

- Tout changement de configuration non autorisé.
- Toute exportation de règles.
- Toute altération de fichiers.
- 'Toute tentative d'exécution de programmes malveillants.

Ce capteur intégré permet aux équipes de sécurité de Sophos de surveiller de manière proactive l'ensemble du parc de clients à la recherche de signes d'attaque — une couche de sécurité supplémentaire qu'aucun autre fournisseur de pare-feu n'offre actuellement. Lorsque des menaces sont détectées, Sophos peut réagir immédiatement pour aider ses clients a mener à bien les tâches de remédiation, tout en déployant simultanément des correctifs automatisés afin de protéger l'ensemble de ses autres clients.

Authentification multifacteur et Zero Trust Network Access intégrés

Sophos Firewall intègre l'authentification multifacteur (MFA) à tous les points d'accès administratifs et comprend une passerelle ZTNA intégrée, ce qui facilite l'adoption et le déploiement de la technologie ZTNA ainsi que le remplacement des VPN d'accès à distance vulnérables.

Protection ET performances puissantes

Si de nombreux fournisseurs proposent des fonctionnalités de protection performantes, Sophos Firewall se distingue par son approche : il est le seul à garantir une sécurité complète sans perte de performances, ce qui évite aux organisations de devoir désactiver des fonctionnalités de sécurité essentielles.

Architecture Xstream FastPath

L'architecture Xstream programmable de Sophos Firewall gère intelligemment le trafic afin d'offrir à la fois une sécurité et des performances **optimales.** Cette approche garantit que l'activation de fonctionnalités de sécurité complètes — notamment l'inspection TLS, le sandboxing et l'IPS — n'entraîne aucune baisse de performances. Sophos Firewall intègre également une protection Zero-Day optimisée par l'IA afin d'identifier les menaces les plus récentes.

Améliorations constantes en matière de performances et de sécurité

Contrairement aux pare-feux traditionnels, dont les performances diminuent à mesure que de nouvelles fonctionnalités de sécurité sont ajoutées, l'architecture programmable de Sophos Firewall permet à la fois d'améliorer la protection **et** d'optimiser les performances grâce à des mises à jour logicielles. Ainsi, les clients bénéficient d'améliorations continues de leurs investissements matériels sans avoir à remplacer leur équipement : une protection et des performances qui s'améliorent avec le temps au lieu de se dégrader.

Détection et réponse inégalées

La plupart des pare-feux réseau n'offrent pratiquement aucune fonctionnalité de détection et de réponse. Une fois qu'un attaquant a franchi les défenses périmétriques, les pare-feux traditionnels ne disposent d'aucun mécanisme permettant de détecter l'intrusion ou d'y réagir. Cela constitue une faille majeure qui expose les organisations aux attaques les plus sophistiquées.

Sophos Firewall se distingue par ses capacités de détection et de réponse automatisées.

NDR (Network Detection and Response) intégré

L'approche NDR a longtemps été l'apanage des grandes entreprises car elle nécessitait des produits spécifiques et des investissements considérables. Sophos Firewall intègre la fonctionnalité NDR en standard dans l'abonnement de protection de base :

Cette intégration met à la disposition des organisations de toutes tailles une capacité de détection des menaces de niveau entreprise, garantissant ainsi que les attaquants qui parviennent à franchir les défenses périmétriques puissent être identifiés avant d'atteindre leurs objectifs.

Sécurité synchronisée : Réponse automatisée entre produits

Détecter sans intervenir revient simplement à signaler aux administrateurs qu'une compromission a eu lieu, souvent trop tard pour prévenir les dommages. La fonctionnalité Sécurité Synchronisée de Sophos Firewall assure une réponse automatisée et coordonnée à l'échelle de toute l'infrastructure de sécurité.

Lorsqu'un produit Sophos détecte une menace, que le signal provienne de Sophos Firewall, Sophos Endpoint, Sophos Email Security, Workspace Protection ou d'un analyste du service MDR, Sécurité Synchronisée effectue automatiquement les opérations suivantes :

- Empêche l'appareil compromis de communiquer avec d'autres systèmes.
- Empêche l'accès aux applications et aux données.
- Empêche les mouvements latéraux au sein du réseau.
- Contient la menace jusqu'à ce que les équipes de sécurité puissent investiguer et assurer la remédiation.

Le « scénario du vendredi soir » montre combien il est important de disposer d'un système de réponse automatisée :

Sans réponse automatique : Vendredi soir, à une heure avancée, un attaquant parvient à compromettre un appareil alors que les équipes sécurité sont absentes. L'acteur malveillant a devant lui tout le week-end pour se déplacer latéralement, effectuer des élévations de privilèges et déployer son ransomware. L'organisation découvrira la violation le lundi matin, avec l'apparition de fichiers chiffrés et de demandes de rançon.

Grâce à la Sécurité Synchronisée : La première intrusion déclenche immédiatement une mise en quarantaine automatique. L'attaquant se retrouve isolé dans un segment, incapable d'avancer. Le lundi matin, les équipes sécurité font face à une alerte active sur une menace déjà contenue, plutôt qu'à un incident de ransomware généralisé.

Cette capacité de réponse automatisée est particulièrement utile pour les organisations qui ne disposent pas d'une couverture de sécurité 24 heures sur 24, 7 jours sur 7 — c'est-à-dire précisément les entreprises de taille moyenne que les fournisseurs traditionnels de solutions NDR ont longtemps négligées.

Conclusion

Mon pare-feu réduit-il les risques ou en crée-t-il ?

Les pare-feux réseau sont confrontés à une pression sans précédent de la part des attaquants. La mise sous les projecteurs de failles touchant plusieurs grands fournisseurs révèle une réalité préoccupante : Les systèmes conçus pour la protection réseau sont désormais des cibles de choix pour les adversaires dotés de capacités avancées.

Le cadre en trois volets présenté dans ce livre blanc — durcissement de la posture de sécurité, protection, ainsi que détection et réponse aux menaces — offre une approche globale de la sécurité réseau qui permet de faire face aux menaces avant, pendant et après leur survenue. Malheureusement, la plupart des fournisseurs de pare-feu se concentrent presque exclusivement sur le volet « Protection », laissant ainsi des lacunes importantes en matière de renforcement de la sécurité ainsi que de capacités de détection et de réponse.

Pour mettre en œuvre efficacement ce cadre, il est nécessaire de choisir une infrastructure qui accorde une importance égale à ces trois piliers. Les organisations ont intérêt à évaluer les fournisseurs de pare-feu en fonction des critères suivants :

- **Un engagement** en faveur de l'approche Secure by Design, étayé par des preuves de l'implémentation, et non par de simples promesses.
- **Des fonctionnalités de correctifs automatisés** qui éliminent les temps d'arrêt et la lassitude liée à l'accumulation de mises à jour.
- **Des fonctionnalités d'audit de configuration** qui offrent une visibilité sur la posture de sécurité.
- **Des fonctionnalités Zero Trust intégrées**, MFA, ZTNA, etc.
- **Network Detection and Response** pour identifier les menaces actives.
- **Des capacités de réponse automatisée** permettant de contenir les menaces sans intervention humaine.

Le coût du remplacement d'infrastructures vieillissantes ou inadéquates est nettement inférieur à celui de la remise en état après une attaque par ransomware exploitant des vulnérabilités connues. C'est maintenant qu'il faut agir, avant que votre organisation ne se retrouve sous les projecteurs pour de mauvaises raisons.

La sécurité est une responsabilité partagée. Il appartient aux fournisseurs de concevoir des produits sécurisés. Il appartient aux organisations de les déployer correctement, de les entretenir avec soin et de les mettre hors service lorsqu'ils arrivent en fin de vie. C'est en assumant chacune leurs responsabilités que les organisations et les fournisseurs bâtiront un écosystème beaucoup plus sûr.

La question essentielle que vous devez vous poser : **Mon pare-feu réduit-il les risques ou en crée-t-il ?**

Pour répondre à cette question, il faut savoir si votre infrastructure repose sur les trois piliers de la sécurité réseau moderne — ou si elle présente des failles critiques que les attaquants ne manqueront pas d'exploiter.

1, 2, 3 ,4 Rapport Sophos Active Adversary 2026

Pour en savoir plus sur Sophos Firewall, rendez-vous sur sophos.com/firewall

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