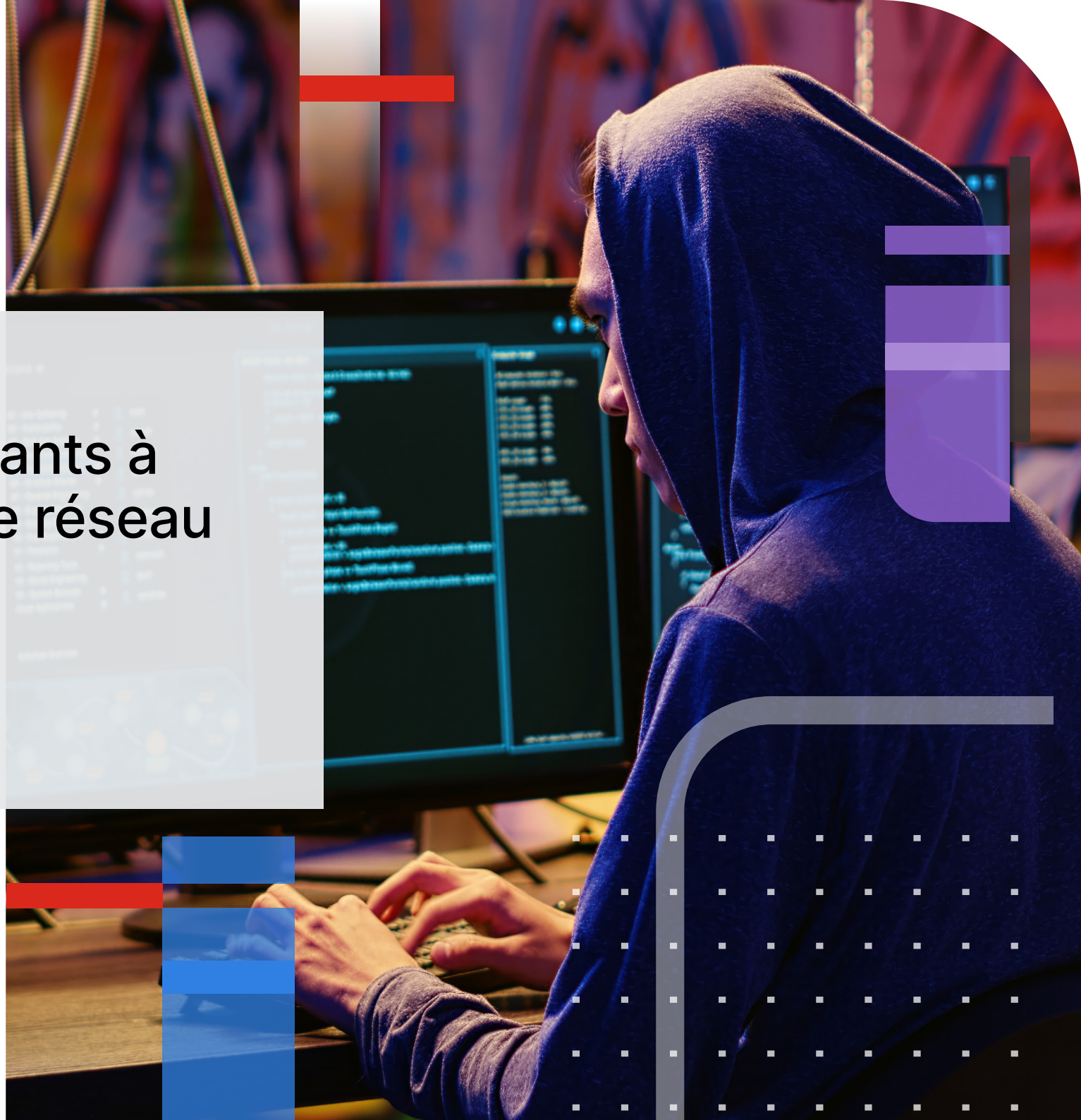


FORTINET

Tenir les assaillants à
l'écart de l'Edge réseau



Sommaire

Avant-propos	3
Nouveaux problèmes	4
Nouvelles solutions	7
Protéger	8
Converger	9
Scalabiliser	11
Sécurité réseau pilotée par IA : la réponse aux enjeux actuels	12



Avant-propos

Aujourd'hui, les utilisateurs ont besoin d'un réseau capable de les connecter à n'importe quelle ressource, n'importe où et sur n'importe quel type d'appareil. Dans le même temps, les réseaux de campus et de data center doivent opérer sur une nouvelle architecture hybride composée de sites distants, de réseaux multiclouds (publics et privés), de réseaux domestiques des télétravailleurs et de solutions Software-as-a-Service (SaaS) dans le cloud. Résultat : les équipes de sécurité peinent de plus en plus à assurer une visibilité totale sur cet environnement réseau distribué et en perpétuelle mutation, ce qui explique en partie leur difficulté à sécuriser et à surveiller chaque utilisateur et chaque appareil accédant aux données, aux applications et aux workloads. Côté cybercriminels, cette situation offre une excellente occasion d'infiltrer votre réseau depuis la périphérie. Une fois dans votre environnement, ces hackers peuvent créer des dégâts considérables.

Malheureusement, les pare-feux d'ancienne génération et autres outils de sécurité traditionnels ont été conçus pour des points de contrôle réseau statiques, sur des workflows et des types de données très prévisibles. Ce qu'il faut aux équipes de sécurité, c'est une sécurité réseau unifiée, pensée pour les infrastructures hybrides intégrant tous les pare-feux nouvelle génération (NGFW), sous toutes leurs formes et sur tout le réseau. Elles pourront ainsi assurer à la fois une gestion centralisée et une réponse coordonnée à chaque menace. Cette unification de la sécurité doit permettre de protéger les actifs et les utilisateurs situés n'importe où, de converger et de consolider les solutions distribuées afin de réduire les charges informatiques, de simplifier la gestion, de permettre l'automatisation et d'adapter dynamiquement les services et la bande passante pour répondre à l'évolution constante des besoins de l'entreprise.





Nouveaux problèmes

Le data center reste certes un rouage essentiel, mais il n'est plus le principal hébergeur des applications d'entreprise. Ces dernières sont désormais déployées sur les plateformes les plus diverses. Ainsi, une transaction ou un workflow donné pourra s'étendre à de multiples environnements et applications, si bien que la source, la destination et le chemin de données pourront parfois changer plusieurs fois en cours de route. Comment, dans ces conditions, assurer le suivi et la sécurité d'une transaction de bout en bout ?

Force est de constater que les pare-feux traditionnels sont dépassés par l'adoption de la 5G – et ce à l'heure où 95 % du trafic est chiffré¹ au moyen des protocoles SSL/TLS, garants de la sécurité des transactions et des accès à distance. Le problème, c'est que les cybercriminels recourent eux aussi au chiffrement pour masquer leurs activités malveillantes (exfiltration de données d'entreprise, vol de secrets commerciaux, attaques de ransomware, etc.). Or, la plupart des pare-feux sont incapables de déchiffrer et d'inspecter ce trafic sans impacter sérieusement la performance et l'expérience utilisateur. Au final, la plupart du trafic – notamment celui à très haut débit – ne fait l'objet d'aucune inspection.

En parallèle, l'avènement des environnements multiclouds et des modes de travail hybrides redéfinit en profondeur les impératifs de sécurité. On le sait, le cloud facilite l'approche de développement Agile et son extrême scalabilité permet d'absorber l'explosion des accès distants aux applications métiers. Cependant, les data centers on-prem doivent encore héberger certains de ces applicatifs pour diverses raisons : conformité réglementaire, confidentialité, protection de la propriété intellectuelle ou caractère hautement sensible des données. C'est là que les choses se compliquent car les pare-feux traditionnels n'ont pas été conçus pour les data centers hybrides, notamment les différents modèles d'interconnexion : utilisateur à data center, data center à cloud, utilisateur à cloud, et data center à data center.

Les directions des systèmes d'information finissent alors par bricoler des solutions de fortune pour assurer une interopérabilité toute relative de solutions disparates. Serveurs, switches, routeurs, pare-feux, équilibreurs de charge et autres équipements interconnectés agissent de concert pour assurer le flux constant des données entre différents systèmes et applications, ce qui complexifie grandement l'infrastructure du data center. Idem pour le réseau qui voit le nombre d'appareils connectés et le volume de trafic exploser, rendant particulièrement difficile la gestion, le suivi et la résolution des problèmes.





Le data center reste certes un rouage essentiel, mais il n'est plus le principal hébergeur des applications d'entreprise. Ces dernières sont désormais déployées sur les plateformes les plus diverses.

Nouvelles solutions

La gestion et la sécurité des architectures hybrides passent par une visibilité centralisée sur la totalité du réseau distribué, c'est-à-dire une parfaite connaissance de chaque utilisateur et chaque appareil connecté au réseau, ainsi que des applications et ressources auxquels ils accèdent. Côté sécurité, le moindre comportement anormal et la moindre activité malveillante doivent être détectés en tout point du réseau. Vous devez également pouvoir mobiliser toutes les ressources de sécurité nécessaires pour coordonner la réponse aux menaces. Alors que les réseaux s'étendent et que les environnements de périphérie (Edge) se multiplient, de nombreuses entreprises adoptent le triptyque SASE (Secure Access Service Edge), SD-WAN (Software-Defined Wide Area Network) et ZTNA (Zero-Trust Network Access). Outre la complexité d'un tel montage, les angles morts qu'il laisse apparaître ont un impact direct sur l'expérience utilisateur et la capacité de réponse aux attaques.

À l'inverse, l'intégration de ces fonctionnalités dans vos NGFW vous aide à renforcer vos défenses et la résilience de votre réseau. Quant à la gestion centralisée, elle vous permet de déployer en temps réel des politiques homogènes depuis une console unifiée. Résultat, vous réduisez les risques de défaillances internes mais aussi d'attaques externes dans tout votre environnement. Grâce à son interopérabilité native, cette approche simplifie les opérations, assure la conformité et facilite l'automatisation d'une grande partie des tâches pour améliorer l'efficacité opérationnelle des modèles hybrides. Que vos pare-feux soient 100 % on-prem, 100 % cloud ou en configuration hybride, la gestion unifiée et centralisée de tout votre parc vous fait gagner sur tous les tableaux.

Campus, data center, réseau multicloud, sites distants, télétravail... quels que soient les environnements à protéger, les cas d'usage restent sensiblement les mêmes et peuvent être abordés en articulant la sécurité sur un schéma en trois temps : **protéger, converger, scalabiliser**. Maîtriser ces trois concepts, c'est implémenter une stratégie de sécurité garante d'une expérience client et d'une protection en phase avec les objectifs métiers.



Protéger

L'objectif n°1 : bloquer toute menace avant qu'elle ne s'introduise sur le réseau. Si cela ne peut être empêché, intervenir aussi rapidement que possible pour neutraliser l'attaque et réduire les perturbations de l'activité. De même, un NGFW doit être orienté applications, notamment par sa capacité à interagir avec d'autres outils pour accélérer l'accès et l'utilisation d'applications prioritaires, et en bloquer d'autres. Cela comprend par exemple un filtrage web renforcé par des fonctionnalités de reconnaissance d'image avancée et de filtrage des contenus vidéo pour garantir le respect des politiques d'usage acceptable.

Une solution NGFW doit aussi intégrer des solutions de sécurité de pointe, de type anti-malware et système de prévention des intrusions (IPS), pour prévenir les attaques connues et inconnues. Côté Threat Intelligence, elle doit pouvoir ingérer les flux CTI de produits complémentaires (sécurité de la messagerie électronique, sandboxes, etc.) pour détecter et prévenir les dernières menaces.

Enfin, il est essentiel que votre NGFW agisse en synergie avec les solutions de détection et réponse sur les terminaux (EDR), les pare-feux d'applications web (WAF), et d'autres systèmes de sécurité. Ensemble, les fonctionnalités intégrées de protection et les intégrations à d'autres technologies garantissent la sécurité du réseau face aux menaces présentes et émergentes.



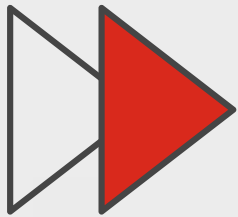
Converger

Un NGFW digne de ce nom doit assurer une visibilité totale pour débusquer les attaques sophistiquées se fondant dans le trafic HTTPS chiffré pour exfiltrer des données ou déployer un ransomware. À cela s'ajoute une intégration parfaitement transparente de fonctionnalités réseau et sécurité au sein d'une solution unifiée. Peu importe qu'il s'agisse d'un NGFW on-prem ou d'une plateforme SASE dans le cloud, vous bénéficierez d'une sécurité dynamique alliée à des fonctionnalités de connectivité et de routage avancées.

Côté contrôle, il est indispensable d'identifier tout utilisateur, appareil ou application demandant un accès, puis de l'assigner automatiquement au segment réseau approprié. Or, cela passe par l'intégration native de services de proxy. Concrètement, lorsqu'un appareil effectue sa première demande d'accès, le pare-feu doit interagir avec les clients des terminaux (pour le cas de serveurs et d'utilisateurs) et des solutions de contrôle d'accès au réseau (pour les objets et équipements IoT ou IIoT). L'authentification multifacteur (MFA) est également indispensable pour déterminer le rôle d'un utilisateur ou d'un appareil, l'assujettir aux politiques associées, et ne lui octroyer l'accès que pour l'application ou le segment du réseau dont il a strictement besoin dans le cadre de ses missions.



Pour les applications et workflows naviguant constamment entre différents environnements, le NGFW doit comprendre quelle politique déclencher, puis l'appliquer partout. Pilotée depuis une console de gestion centralisée, cette approche homogène de l'orchestration et de l'application des politiques permet à la sécurité de suivre les applications, les workflows et les transactions de bout en bout.



Pour les applications et workflows naviguant constamment entre différents environnements, le NGFW doit comprendre quelle politique déclencher, puis l'appliquer partout.

Scalabiliser

Peu importe son lieu et son mode de déploiement, un pare-feu doit agir vite aujourd'hui. Et encore plus vite demain. Les data centers génèrent et brassent d'énormes quantités de données à vitesse transactionnelle pour toutes sortes de cas d'usage : modélisation avancée sur du Big Data, transactions financières à ultra-faible latence, environnements multi-utilisateurs massifs exigeant de la performance, etc.

Par « vitesse », nous entendons la rapidité avec laquelle un pare-feu inspecte les données et sa capacité à prendre en charge l'automatisation. En ce sens, un pare-feu doit assurer une sécurité avancée et parfaitement coordonnée pour protéger le réseau des attaques éclairs qu'il subit. De même, il lui faut être opérationnel rapidement, sans provisionnement manuel chronophage. Qui dit opérations manuelles, dit ralentissement des opérations et erreurs de configuration pouvant ouvrir la porte aux ransomwares et autres types d'attaque.

Le problème, c'est que la plupart des pare-feux traditionnels fonctionnent déjà à 100 % de leurs capacités. Autrement dit, ils ne disposent d'aucune marge de scalabilité pour répondre aux exigences des métiers. Rien d'étonnant à cela : ils n'ont pas été



conçus pour l'hyper-performance. Leur plus grande faiblesse vient du fait qu'ils embarquent des processeurs standard, alors que tout fonctionne désormais sur des processeurs sur mesure – des cartes graphiques aux smartphones, en passant par les serveurs cloud. Qu'on ne s'y trompe pas : la sécurité exige énormément de puissance processeur. Toutefois, la scalabilité des pare-feux ne doit s'opérer ni aux dépens des fonctionnalités de sécurité, ni aux dépens de la performance et des budgets alloués.

Sécurité réseau pilotée par l'IA : la réponse aux enjeux actuels

Les pare-feux constituent le premier rempart contre les hackers qui ciblent votre réseau. Les SPU (Security Processing Units) brevetés de Fortinet sont les seuls processeurs du marché à réunir des fonctionnalités réseau et de sécurité dans un seul et même produit. Composants essentiels de son architecture NGFW pilotée par l'IA, ils sont conçus pour renforcer votre protection et l'efficacité de votre réseau. Grâce à la plateforme de sécurité unifiée de Fortinet, les entreprises gèrent l'intégralité de leur infrastructure depuis une seule et même interface, quels que soient le format et l'emplacement de leurs pare-feux. Cette approche d'intégration évolutive améliore la coordination et accélère la détection et la réponse aux menaces sur tous les edges.

¹ « [HTTPS encryption on the web](#) », Google Transparency Report, consulté le 1er juin 2023.



www.fortinet.com/fr

Copyright © 2024 Fortinet, Inc. Tous droits réservés. Fortinet®, FortiGate®, FortiCare®, FortiGuard® et certaines autres marques sont des marques déposées de Fortinet, Inc. D'autres noms Fortinet utilisés dans le présent document peuvent également être des marques commerciales, déposées ou non, de Fortinet. Tous les autres noms de produit et d'entreprise peuvent être des marques commerciales de leurs détenteurs respectifs. Les performances et autres métriques mentionnées dans le présent document ont été obtenues lors de tests internes en laboratoire, réalisés dans des conditions idéales. Les performances et autres résultats pourront varier en conditions réelles. Les variables réseau, les différents environnements réseau et d'autres paramètres pourront influencer sur les performances. Rien de ce qui précède ne constitue un engagement contraignant de la part de Fortinet. Fortinet décline toute garantie, expresse ou tacite, sauf dans le cadre d'un contrat à force contraignante conclu avec un acheteur, signé par le directeur juridique de Fortinet ou toute autre personne dotée de pouvoirs supérieurs, et qui garantit expressément que le produit concerné fonctionnera à un niveau de performance clairement défini et quantifié. Dans ce cas, seules les métriques de performance clairement identifiées dans ledit contrat écrit constitueront un engagement contraignant de la part de Fortinet. À des fins de clarté absolue, de telles garanties se limiteront aux seules performances obtenues dans les mêmes conditions idéales que celles des tests internes en laboratoire de Fortinet. En vertu des présentes, Fortinet décline toute obligation, déclaration et garantie expresse ou tacite. Fortinet se réserve le droit de changer, modifier, transférer ou autrement réviser cette publication sans préavis. Dans ce cas, la version la plus récente s'applique.