Requirements for a Security-Driven Networking Strategy, from SD-WAN to SASE

L'innovation digitale impose à chaque entreprise de repenser ses réseaux et d'offrir une meilleure expérience utilisateur aux collaborateurs et aux clients. Le périmètre, autrefois un simple point d'accès vers l'edge réseau, s'étend désormais sur la totalité de l'infrastructure IT, et impose de nouvelles exigences au data center, au réseau WAN, au réseau LAN et au edge cloud. La pandémie actuelle de COVID-19 a mis en exergue l'intérêt de disposer de plans de continuité métier qui permettent des accès distants sécurisés, flexibles, évolutifs et disponibles en tous lieux.

De leur côté, les menaces de sécurité sont toujours aussi sophistiquées et fréquentes. Plus d'un tiers des piratages en 2020 résulte de techniques d'ingénierie sociale.[1] C'est la raison pour laquelle une amélioration de la sécurité et un redesign du réseau s'imposent pour toutes les entreprises.

Une **stratégie réseau orientée sécurité** accélère la convergence du réseau et de la sécurité sur l'ensemble de l'environnement connecté (tous les edges et utilisateurs), du cœur de réseau jusqu'aux sites distants et le cloud. Cette stratégie permet aux entreprises de défendre leurs environnements réseau en temps réel tout en optimisant l'expérience utilisateur à l'intention des collaborateurs et des clients.

Avec la sécurité positionnée au niveau du cœur de réseau, les réseaux peuvent évoluer, s'étendre et adapter leur innovation digitale avec simplicité, pour ainsi répondre aux défis des nouvelles tendances majeures : hyperscale, multicloud, 5G, etc. La convergence du réseau et de la sécurité implique une sécurité qui soit flexible et omniprésente.

Une stratégie réseau orientée sécurité accélère la convergence du réseau et de la sécurité sur l'ensemble de l'environnement interconnecté (tous les utilisateurs et les edges), depuis le cœur de réseau, jusqu'aux sites distants et le cloud.

Les éléments clés d'une stratégie réseau orientée sécurité

Une stratégie réseau orientée sécurité répond à trois besoins spécifiques :

- **La gestion des risques externes et internes pour les utilisateurs sur le réseau**
- **La capacité à offrir une sécurité flexible et cloud-native pour tous les utilisateurs sur le réseau**
- **L'amélioration de l'expérience utilisateur et la maîtrise des coûts**

La première étape pour bâtir un réseau orienté sécurité consiste à **utiliser des processeurs de sécurité personnalisés**, ou ASIC, qui permettent aux équipes de piloter le réseau de manière rapide, tout en **consolidant les fonctions de sécurité :** contrôle applicatif, pare-feu, prévention d'intrusion. Cette consolidation s'effectue au sein d'une solution comme un pare-feu réseau, sans peser sur les performances. Les cas d'utilisation portent sur le SD-WAN (software-defined wide-area networking), le pare-feu nouvelle-génération (NGFW), l'IPS, l'inspection du trafic SSL, le contrôle applicatif, le filtrage web, l'antivirus/antimalware, le sandboxing et la segmentation accélérée. Ce dernier point est d'ailleurs extrêmement important pour une stratégie de réseau orienté sécurité, puisque nombre de pare-feux ne peuvent gérer les tâches de traitement nécessaires à une segmentation interne dynamique.

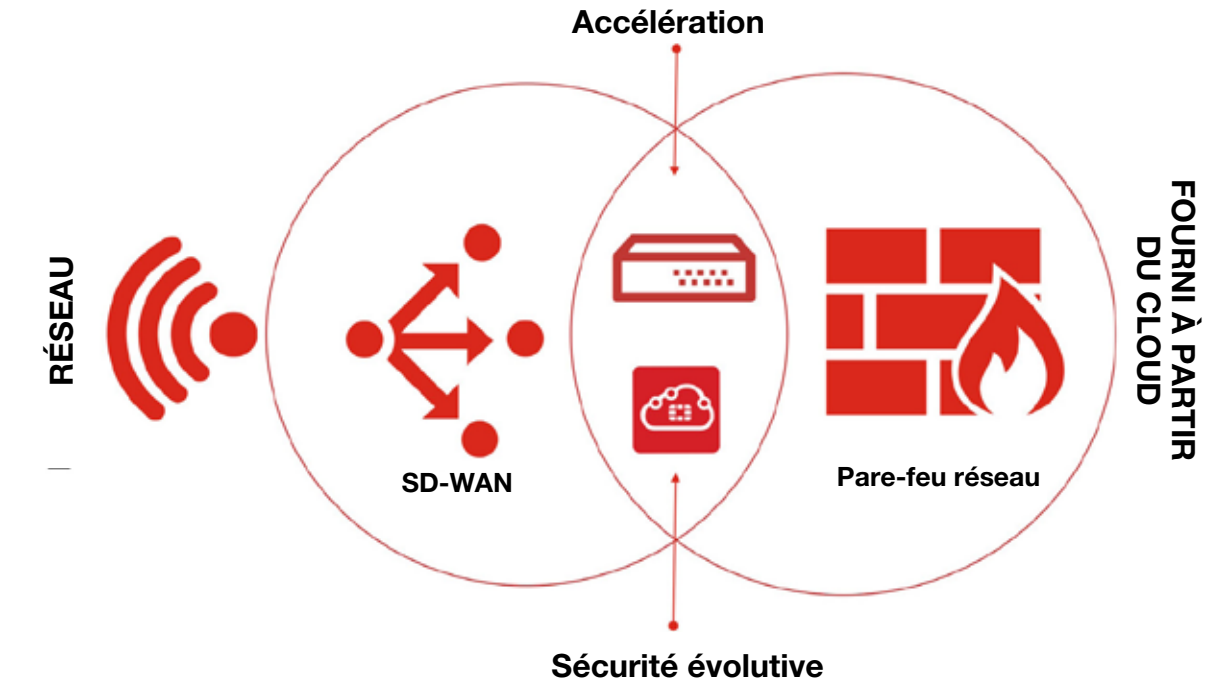
Une architecture cloud conçue sur mesure permet la convergence de la sécurité et du réseau à l'intention des utilisateurs du cloud qui recherchent de la flexibilité pour déployer leurs solutions.

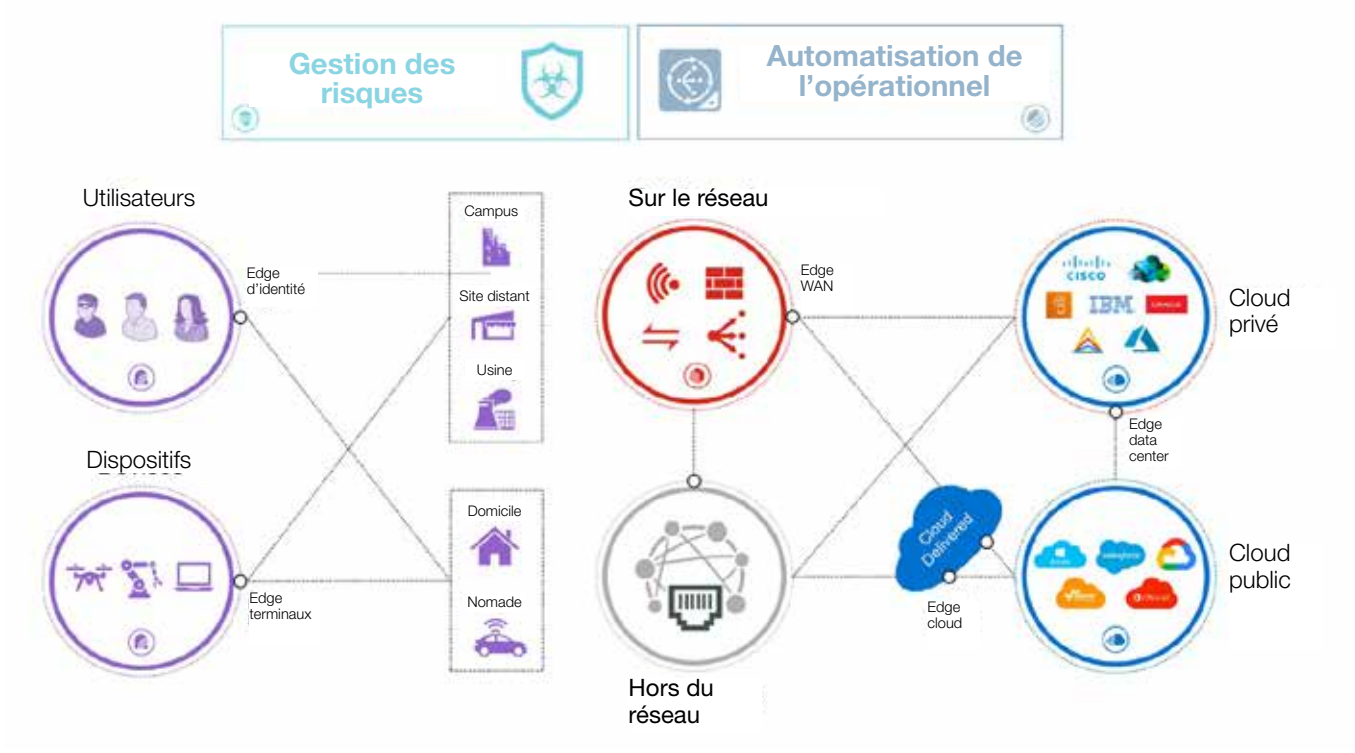
Dans l'avenir, les pare-feux réseau devront également **être compatibles avec les data centers hyperscale et les performances de la 5G**. Les innovations comme le trafic de type Elephant flows, l'edge computing, la protection de la HDTV et des médias riches, les réseaux 5G et la segmentation dynamique du cœur de réseau, nécessiteront des niveaux de performances sans précédent de la part du NGFW. Mais parce que des pare-feux n'ont pas été conçus dans cette optique de performances, certaines solutions ne seront tout simplement pas capables de répondre aux exigences de demain, sauf à investir de manière massive... Et parfois à perte !

Une stratégie de réseau orienté sécurité transforme le edge WAN en le migrant vers un SD-WAN d'entreprise, totalement intégré au dispositif NGFW. Cette intégration permet de sécuriser le **SD-WAN**, et se substitue à un SD-WAN qui requiert une sécurité en tant que couche supplémentaire. Une approche robuste au SD-WAN intègre également des techniques d'intelligence artificielle, pour ses traitements analytiques prédictifs, une orchestration intuitive et une capacité d'auto-restauration.

Au final, les entreprises doivent étendre la sécurité aux réseaux filaires et sans fil, de manière étroitement intégrée, ce qui assure une protection cohérente et intégrale des edges du LAN. C'est la condition essentielle pour des **réseaux sains et réactifs**, qui étendent la sécurité vers les edges d'accès et réseau.

Tous ces edges doivent être **gérés de manière centralisée** à des fins de simplification et d'automatisation, rendant ainsi le réseau plus agile.





Le SASE pour sécuriser l'edge cloud

En 2020 et au-delà, tout intérêt porté à un réseau orienté sécurité doit également englober le SASE (secure access service edge). Le SASE est un framework d'entreprise qui associe les fonctions de sécurité réseau avec des capacités WAN, afin de prendre en charge les besoins des entreprises en matière d'accès sécurisé, en totale conformité avec une stratégie de réseau orienté sécurité. Le SASE joue un rôle essentiel pour s'assurer que la sécurité peut être fournie en tous endroits, notamment sur l'edge cloud, pour sécuriser les utilisateurs distants et mobiles.

Le SASE est généralement considéré comme faisant parti du cloud computing, mais certains contextes exigent des solutions physiques et cloud pour que le SASE soit parfaitement intégré au réseau. Ceci peut impliquer d'associer la connectivité SASE avec le contrôle d'accès réseau et les dispositifs de sécurité edge, en support d'une appliance SD-WAN physique disposant d'un ensemble de fonctionnalités de sécurité, ou lorsqu'il s'agit de s'intégrer avec des technologies à l'image des contrôleurs LAN sans fil ou des points d'accès Wi-Fi au niveau des sites distants. Le SASE permet aux entreprises de **sécuriser les utilisateurs distants** de manière pertinente, quelle que soit leur localisation, pour ainsi définir une expérience utilisateurs robuste et des gains de productivité, grâce à un edge cloud qui propose des chemins à faible latence.

Une offre SASE et une stratégie de réseau orientée sécurité ne signifient pas la même chose. Au-delà des protections essentielles cloud telles que définies par le SASE[2], un SASE robuste doit pouvoir également permettre la segmentation du réseau et assurer la conformité réglementaire qu'une sécurité cloud ne peut prendre en charge sans devoir assurer l'inspection du trafic en dehors du cloud.

C'est dans ce contexte que le SASE devient partie intégrante d'une stratégie réseau orientée sécurité, pour offrir le niveau de sécurité et de performances qu'exigent les entreprises actuelles.

[1] "2020 Data Breach Investigations Report," Verizon, mai 2020

[2] "The Future of Network Security Is in the Cloud," Gartner, 13 septembre 2019.

FORTINET

www.fortinet.fr

Copyright © 2020 Fortinet, Inc. Tous droits réservés. Fortinet®, FortiGate®, FortiCare®, FortiGuard® et certaines autres marques sont des marques déposées de Fortinet, Inc., et les autres noms Fortinet mentionnés dans le présent document peuvent également être des marques déposées et/ou des marques de droit commun de Fortinet. Tous les autres noms de produit ou d'entreprise peuvent être des marques commerciales de leurs détenteurs respectifs. Les données de performances et autres indicateurs de mesure figurant dans le présent document ont été obtenus au cours de tests de laboratoire internes réalisés dans des conditions idéales, et les performances et autres résultats réels peuvent donc varier. Les variables de réseau, les différents environnements réseau et d'autres conditions peuvent affecter les performances. Aucun énoncé du présent document ne constitue un quelconque engagement contraignant de la part de Fortinet, et Fortinet exclut toute garantie, expresse ou implicite, sauf dans la mesure où Fortinet conclut avec un acheteur un contrat écrit exécutoire, signé par le directeur des affaires juridiques de Fortinet, qui garantit explicitement que les performances du produit identifié seront conformes à des niveaux de performances donnés expressément énoncés et, dans un tel cas, seuls les niveaux de performances spécifiques expressément énoncés dans ledit contrat écrit exécutoire ont un caractère obligatoire pour Fortinet. Dans un souci de clarté, une telle garantie sera limitée aux performances obtenues dans les mêmes conditions idéales que celles des tests de laboratoire internes de Fortinet. Fortinet rejette intégralement toute convention, déclaration ou garantie en vertu des présentes, qu'elle soit expresse ou implicite. Fortinet se réserve le droit de changer, de modifier, de transférer ou de réviser par ailleurs la présente publication sans préavis, et c'est la version la plus à jour de la publication qui est applicable. Fortinet rejette intégralement toute convention, déclaration ou garantie en vertu des présentes, qu'elle soit expresse ou implicite. Fortinet se réserve le droit de changer, de modifier, de transférer ou de réviser par ailleurs la présente publication sans préavis, et c'est la version la plus à jour de la publication qui est applicable.

mars 2, 2021 11:01 AM

745599-0-1-FR

POV-requirements-for-SDN-strategy-A4_FR