LIVRE BLANC

Une solution SASE flexible avec Fortinet

Résumé

L'innovation digitale, l'adoption du Cloud, la récente et rapide migration vers le télétravail, sont autant de facteurs qui ont transformé le réseau. Avec une dépendance plus marquée aux ressources du Cloud comme les applications Software as a Service (SaaS) et donc aux données qui migrent du data center vers des environnements multi-cloud, il devient clair qu'une nouvelle approche s'impose pour sécuriser les accès réseau. Il s'agit notamment de remettre en cause la confiance implicite accordée aux utilisateurs et dispositifs accédant au réseau.

Les entreprises actuelles exigent un accès immédiat, permanent et en toutes circonstances au réseau et aux ressources/données dans le Cloud. Le défi est que nombre des problématiques qui résultent de l'innovation digitale (modification dynamique des configurations réseau, expansion rapide de la surface d'attaque, etc.) ne peuvent être résolues par des solutions traditionnelles de sécurité, ces dernières ne pouvant offrir le niveau de sécurité et de contrôle d'accès qu'exigent les entreprises et les utilisateurs.

« Les demandes de nos clients en matière de simplicité, d'évolutivité, de faible latence, de flexibilité et de sécurité encouragent la convergence des marchés du WAN Edge et de la sécurité réseau. »[1]

Le SASE (Secure Access Service Edge) est une stratégie d'entreprise émergente qui combine les fonctions de sécurité des réseaux avec les capacités du WAN. L'objectif est de répondre aux besoins des entreprises en matière d'accès sécurisé et dynamique, dans le droit fil de la stratégie réseau orientée sécurité qui constitue le cœur de métier de Fortinet. Le SASE joue un rôle critique pour s'assurer que la sécurité peut être fournie en tous lieux et notamment sur l'Edge du WAN, l'Egde Cloud, l'Edge du data center, le cœur de réseau et les terminaux utilisés par les collaborateurs à distance, très mobiles aujourd'hui.

Une définition précise du SASE

À l'instar de toute nouvelle technologie, le SASE doit être défini avec précision. S'agit-il d'une offre 100% Cloud ? Ou faut-il faire appel à des solutions matérielles également ? Quelles sont les technologies impliquées dans le SASE ?

Si le SASE est généralement catégorisé en tant que service fourni à partir du Cloud, il est parfois nécessaire d'associer solutions physiques et Cloud pour favoriser une intégration efficace au réseau. Il peut s'agir d'associer une connectivité SASE avec des fonctions de contrôle d'accès au réseau et des dispositifs de sécurité Edge à l'intention des télétravailleurs. Le SASE peut ainsi se coupler avec un dispositif SD-WAN (Software-Defined Wide-Area Networking) qui propose également des fonctions de sécurité, ou s'intégrer avec des technologies de type contrôleur de réseau LAN sans fil ou des accès WI-Fi distants.

Ainsi, au-delà de ses fonctions de protection fournies à partir du Cloud, une solution SASE robuste doit également assurer une segmentation du réseau et des outils de mise en conformité qu'une sécurité Cloud ne peut proposer, sauf à devoir acheminer le trafic en dehors du Cloud à des fins d'inspection. C'est la raison pour laquelle Fortinet propose les solutions les plus complètes et flexibles pour les environnements SASE à l'intention des environnements et intégration entre les dispositifs matériels et le Cloud.

Le SASE, un accès sécurisé avant toute chose

D'un point de vue conceptuel, le SASE répond aux défis de sécurité créés par les constructeurs de solution SD-WAN qui ont certes su proposer une solution réseau innovante, mais n'ont pas intégré la sécurité dans leur offre. De son côté, Fortinet propose une solution intégrée de SD-WAN sécurisé, qui bénéficie d'un solide panel de fonctions de sécurité et réseau, une offre intégrée qui se veut unique sur le marché. Ceci s'inscrit dans la stratégie de réseau orienté sécurité et de la plateforme Security Fabric de Fortinet, que nous proposons à nos clients depuis des années.

Fortinet propose une solution SASE totalement intégrée, dans un format matériel ou depuis le Cloud avec les modules essentiels de sécurité:

- **Une solution SD-WAN totalement fonctionnelle. Composante essentielle de la solution SASE, le SD-WAN doit pouvoir proposer des fonctions telles que la sélection dynamique des chemins de routage, des capacités d'auto-restauration du WAN, ainsi qu'une expérience applicative et utilisateur cohérente pour les applications métiers.**
- **Un pare-feu matériel nouvelle-génération (NGFW) ou un service Cloud Firewall-as-a-Service (FWaaS).** Le SASE doit également proposer un panel complet de services de sécurité, lorsque fourni à partir d'une appliance matérielle ou depuis le Cloud. À titre d'exemple, les entreprises qui ont adopté une stratégie de télétravail ont besoin de sécuriser leur Edge et assurer une

segmentation interne pour empêcher les menaces liées aux accès invités ou à l'Internet des objets (IoT) de se mouvoir vers des ressources corporate sensibles. Au-delà, une sécurité Cloud est également nécessaire pour protéger les accès aux ressources dans le Cloud. Des appliances matérielles performantes et une sécurité évolutive Cloud-native peuvent offrir le même niveau élevé et évolutif de performance, ce qui assure une flexibilité et une sécurité optimale pour l'entreprise.

- **Zero-Trust Network Access (ZTNA)** est une technologie utilisée pour identifier les utilisateurs ou les dispositifs et permettre leur authentification lorsqu'ils se connectent aux applications. Le ZTNA, qui est en réalité davantage une stratégie qu'un produit, fait collaborer différentes technologies entre elles. L'authentification à facteurs multiples (MFA) identifie tous les utilisateurs. Sur son volet matériel, le ZTNA propose un contrôle d'accès réseau sécurisé, l'application des règles d'accès et une intégration avec une segmentation réseau dynamique qui limite les accès aux ressources réseau. Du côté Cloud, le ZTNA propose une micro-segmentation avec inspection du trafic interne entre les utilisateurs, ainsi qu'une sécurité permanente des dispositifs connectés au réseau ou pas. En associant des services ZTNA physiques et Cloud, les entreprises peuvent assurer un accès sécurisé et la stricte application des règles, que les utilisateurs et dispositifs soient sur ou hors site.
- **Une passerelle de sécurité Web** est utilisée pour protéger les utilisateurs et dispositifs contre les menaces de sécurité. Cette plateforme applique des règles de sécurité et de conformité Internet, tout en assurant le filtrage du trafic malveillant. Elle peut également appliquer des règles d'utilisation pour les accès au web, assurer le respect de la réglementation et prévenir les fuites de données.
- **Un service CASB** Cloud permet aux entreprises de prendre le contrôle de leurs applications SaaS. Il s'agit notamment de sécuriser les accès applicatifs et de maîtriser le Shadow IT. Pour être optimale, cette approche doit être associée à une prévention des fuites de données (DLP).

Schéma 1 : SASE

Renforcer le SASE à l'aide de technologies complémentaires

Le SASE est conçu pour renforcer l'innovation digitale. Pour autant, il s'agit de prendre en compte le SASE de manière globale, pour éviter de créer une nouvelle solution de sécurité cloisonnée, gérée de manière distincte du reste de l'architecture. Ceci pèse lourdement sur la visibilité et le contrôle de l'ensemble du réseau. Donc, au-delà de fournir les composants essentiels à une solution SASE robuste, Fortinet propose également des outils optionnels conçus pour étendre et améliorer la sécurité des utilisateurs et des dispositifs faisant appel à la solution SASE. Ces outils s'assurent également que la solution dans sa globalité s'intègre en toute transparence au sein de Securty Fabric.

À titre d'exemple, les technologies de sécurité des terminaux (endpoints), à l'image de l'EPP (Endpoint Protection Platform) et de l'EDR (Endpoint Detection and Response), s'assurent que les dispositifs qui tirent parti du SASE sont eux-mêmes sécurisés. Un VPN sophistiqué sécurise la transmission des données et des transactions, tout en maîtrisant la complexité résultant de centaines ou de milliers de terminaux et utilisateurs distants qui doivent s'interconnecter. Enfin, le déploiement de contrôleurs LAN et Wi-Fi sécurisés assure que le trafic sortant ou entrant sur le réseau est de nouveau inspecté.

Certes chaque entreprise a des besoins spécifiques. Mais il serait peu logique de n'adopter que les technologies dites « essentielles » pour le SASE, alors qu'une solution de sécurité et réseau plus globale offre des résultats business bien meilleurs.

Un potentiel important mais un nombre trop restreint d'éditeurs qualifiés

Alors que le SASE est conçu pour relever les défis actuels en matière de contrôle d'accès et de WAN sécurisé, force est néanmoins de constater la pénurie d'éditeurs qui se sont positionnés sur ce marché et donc capables d'offrir une solution SASE complète. Pour exemple, rares sont leurs outils, de sécurité notamment, à avoir été testés ou certifiés. Ainsi, les clients n'ont pas vraiment les moyens de savoir si les services de sécurité dans lesquels ils investissement les protègeront réellement sur le terrain.

Certains éditeurs rechignent à faire appel à des laboratoires de test indépendants pour valider si leurs solutions répondent aux attentes du secteur. Cette problématique est d'autant plus critique que certains fournisseurs, peu expérimentés, offrent des solutions dites « SASE » dont les promesses relèvent plus du discours marketing que de la réalité.

L'atout Fortinet

Chez Fortinet, nos clients nous interrogent souvent : « quelle est votre stratégie SASE ? ». Pour que le SASE fonctionne correctement, toutes ses composantes (connectivité, réseau et sécurité) doivent pouvoir interopérer en tant que système étroitement intégré. Chez Fortinet, nous proposons toutes les composantes SASE nécessaires (et bien davantage d'ailleurs) depuis déjà de nombreuses années, dans le cadre de notre plateforme intégrée de sécurité et de notre architecture Security Fabric. Ceci favorise la convergence des fonctions de sécurité et réseau, dans le cadre d'une approche réseau orienté sécurité qui encourage et sécurise l'innovation digitale. Nombre de nos clients qui souhaitent déployer le SASE se rendent souvent compte qu'il suffit de quelques ajustements mineurs pour bénéficier d'une solution SASE qui existe déjà au sein de la Security Fabric.

Le SASE s'attache à résoudre un vrai problème, mais il s'agit d'une problématique à laquelle Fortinet a déjà répondu par le passé.

- Nous avons été le tout premier éditeur de solutions de sécurité à proposer un SD-WAN avec des fonctions natives de sécurité, car nous avons pu concevoir une solution unique et unifiée qui bénéficie d'années d'expérience en matière de sécurité et de réseau.
- Nous sommes ensuite passés à l'étape suivante en élaborant le premier processeur SD-WAN conçu pour accélérer les fonctionnalités réseau et sécurité et offrir le niveau de performances qu'exigent les environnements réseau les plus exigeants.
- D'autre part, les outils de sécurité de Fortinet sont les plus testés, validés et certifiés du secteur.

Aussi, fournir la solution SASE la plus adaptée à votre entreprise fait déjà partie de notre approche réseau et sécurité. Nous pouvons personnaliser cette solution en y intégrant des technologies évoluées de connectivité et de sécurité, pour s'assurer que votre solution SASE sera capable de suivre l'évolution de vos besoins. La Security Fabric de Fortinet peut également s'intégrer et s'interconnecter avec les autres solutions déployées sur site ou dans le Cloud. Tous ces éléments sont pilotés à partir d'une interface de gestion unifiée qui apporte une visibilité élargie et un contrôle granulaire sur l'ensemble de votre réseau, environnement SASE inclus.

Fortinet propose une solution SASE qui apporte une sécurité de manière cohérente sur l'ensemble du réseau : edges WAN et Cloud, edge du data center, cœur du réseau et endpoint, pour assurer une connectivité, une visibilité et un contrôle transparent.

Nous constatons une accélération des ventes de notre offre SASE sur le marché, venant ainsi valider l'approche de Security Fabric et souligner ce que nous affirmons depuis des années. À l'ère de la connectivité Cloud et de l'innovation digitale, la convergence entre réseau et sécurité doit s'opérer. Un retour vers des architectures cloisonnées est tout simplement impossible. Fortinet est totalement prêt pour l'ère du SASE, et bien plus.

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

FORTINET

www.fortinet.fr

mars 5, 2021 12:54 PM

742476-0-0-FR

wp-FA-fortinet-delivers-the-most-flexible-sase-solution-7312020-A4_FR