Proposé par SPIE ICS

Reprendre le contrôle de sa cybersécurité à l'ère du travail hybride : le défi des architectures SASE

Solution unifiée et sur mesure, le modèle SASE (Secure Access Service Edge) s'impose comme le modèle à privilégier dans un contexte de mutation des architectures IT vers le Cloud. A la clé, un enjeu primordial : la protection des données sensibles et des accès utilisateurs qui sont davantage exposés aux cyberattaques avec le développement du travail hybride. Car les architectures de cybersécurité traditionnelles ne permettent plus de maîtriser la sécurité dans ces nouveaux environnements. Avec une architecture SASE, la sécurité des Cloud privés et publics devient accessible à toutes les organisations et leur permet de repenser leur sécurité sur un modèle unifié. Les experts de SPIE ICS partagent leur retour d'expérience.

Maitriser sa sécurité dans un environnement IT dispersé

Auparavant, les DSI des organisations se reposaient sur un modèle d'architecture très centralisée et disposaient d'une certaine forme de contrôle des accès et des usages des collaborateurs. Ils pouvaient localiser les postes de travail, détecter et proposer des solutions « on premise[i] » dans un environnement relativement sécurisé et cloisonné.

Alors que le risque cyber augmente, on assiste aujourd'hui à la diversification des cas d'usages et à l'émergence des applications libres sur internet, sans oublier un recours accru au Cloud hybride. Cela contraint les DSI à repenser la politique d'accès des utilisateurs en fonction des besoins métier et de chaque niveau de responsabilité.

Situés à l'entrée du cloud, les services Edge du SASE apparaissent ainsi comme un moyen sûr et robuste de superviser et de contrôler les usages des collaborateurs. Ainsi, dans un contexte de travail hybride, les premières étapes consistent à veiller à la bonne application de la politique de filtrage des flux internet et à rationaliser les droits d'accès des collaborateurs aux données de l'entreprise.

Ilyès Soltane, expert en cybersécurité chez SPIE ICS, prend l'exemple du filtrage des flux internet et des accès aux applications collaboratives comme Teams, qui ne sont plus forcément développées en interne : « On va pouvoir contrôler si ce qui rentre et sort sur internet est bien légitime. Comme les applications sont remplacées par des souscriptions à des services Cloud, on va pouvoir limiter certaines actions : tel utilisateur donné n'aura pas le droit de réaliser un appel externe via Teams ; tel autre ne pourra pas envoyer des données sensibles à l'extérieur du réseau d'entreprise. »

Ilyes Soltane, expert en cybersécurité chez SPIE ICS

La solution permet ainsi de reprendre la maitrise de sa sécurité dans un environnement IT « hyper décentralisé ». Un tableau de bord unique permet de simplifier l'exploitation de l'environnement et permet une supervision de sécurité unifiée avec des KPI consolidés.

En protégeant le réseau à la source, le modèle SASE réduit significativement la probabilité que des attaques telles que du phishing et du ransomware aboutissent. Il permet aussi de s'adapter aux nouvelles menaces comme des attaques de type « Zero-Day ».

Une migration SASE doit être progressive, accompagnée et sur-mesure

Le datacenter n'est plus au centre du réseau : les architectures de sécurité de type « best of breed » (firewalls, antivirus, VPN, etc.) ne sont plus adaptées pour assurer la protection des données des organisations. Les applications métier et les usages se sont diversifiés, la mobilité et le télétravail se sont généralisés, provoquant des risques de contournement volontaires ou involontaires des bonnes pratiques de sécurité.

Ilyès Soltane insiste sur les avantages d'une architecture SASE : « Elle permet de s'adapter à l'environnement « legacy » de chaque organisation, pour mettre progressivement en œuvre les nouveaux outils de sécurité et maitriser globalement sa cybersécurité ».

Il préconise de commencer par réaliser un schéma directeur Réseau et Sécurité pour déterminer la trajectoire technique et organisationnelle du projet et clarifier les objectifs. Cette étape permet de recenser les premiers jalons techniques et de définir le chemin de migration ». Dans cette perspective, il est judicieux de prévoir une phase pilote qui permettra de tester l'approche et plusieurs cas d'usage avant de déployer la solution à grande échelle.

Le SASE accompagne le développement d'une organisation dans le temps

« La réflexion organisationnelle que nécessite la mise en place d'une architecture SASE est très vertueuse pour l'organisation » précise Pascal Mavric, consultant cybersécurité chez SPIE ICS. Il en énumère les bénéfices :

• L'agilité et l'évolutivité de l'architecture SASE sont à la source même de sa conception : elle permet aux entreprises de s'adapter rapidement aux changements tout en ajustant les politiques de sécurité au besoin

• En fusionnant les fonctionnalités réseau et sécurité, elle réduit la complexité et simplifie la gestion globale des SI. Les routages de trafic optimisés pour plus de performance et les accès sécurisés depuis n'importe quel endroit permet au personnel distant ou mobile de profiter d'une meilleure expérience utilisateur

• Avec l'intégration du SD-WAN et un réseau orienté services, le SASE assure une meilleure gestion de la performance des applications et des services, un point crucial pour l'utilisation efficace des ressources Cloud

Si l'architecture SASE est à la fois structurante et agile, son principal atout est bien sa capacité à évoluer au fil de la vie de l'organisation et du développement des nouveaux usages.

Pallier le manque de ressources et optimiser les couts grâce aux Services Managés

La principale préoccupation des DSI est aujourd'hui d'optimiser les coûts de supervision, d'administration et d'exploitation de leurs infrastructures tout en pilotant leur cybersécurité. Le modèle SASE favorise l'adoption d'un modèle d'externalisation, contribue à la réduction des coûts et leur permet de se concentrer sur l'accompagnement des directions opérationnelles dans leurs enjeux métiers.

Le modèle SASE permet aussi de garantir une disponibilité des services suivant le modèle de disponibilité des cinq neuf (99.999%). « A chaque changement dans le cycle de vie de l'organisation et à chaque « « upgrade », nous garantissons un service sans coupure » précise Ilyes. Sa conception même, en « full SaaS », apporte un niveau de résilience optimum. La garantie de continuité de service est à présent accessible à toutes les organisations.

« La supervision de la sécurité chez nos clients fait partie intégrante de notre expertise, une fois la migration SASE effectuée. Par ailleurs, notre SOC (Security Operations Center) nous permet de repérer les comportements malveillants et d'agir très rapidement. » confirme Ilyès Soltane.

Il insiste également sur l'importance de la veille 24/7 et d'une nouvelle approche de sécurité dynamique pour les ETI ne disposant pas des ressources nécessaires en interne.

« Là où le VPN donnait accès à l'ensemble des données de l'organisation, les nouvelles normes « Zero trust » (confiance zéro) permettent un contrôle différencié des accès et usages pour chaque utilisateur.

Par ailleurs l'architecture SASE est conçue pour optimiser tous les processus de mises à jour et de fournir un niveau de sécurité optimisé » ajoute Ilyès Soltane.

La combinaison gagnante des outils de sécurité du modèle SASE

Pour déployer les services de SSE (Security Service Edge) du modèle SASE, les organisations disposent désormais d'une palette complète de fonctionnalités matures intégrées au sein d'une solution technique unique, leur permettant de construire une bulle de sécurité performante :

• Le Secure Web Gateway (SWG) ou passerelle web sécurisée pour le filtrage du trafic web et la vérification de sa conformité aux exigences de sécurité.

• Le Cloud Access Security Broker (CASB): ce logiciel « courtier en sécurité d'accès au cloud » situé entre les utilisateurs et les applications Cloud permet de surveiller les activités dans le cloud et d'appliquer les politiques de sécurité.

• Le Zero Trust Network Access (ZTNA), modèle de sécurité partant du principe que les menaces sont présentes aussi bien à l'intérieur qu'à l'extérieur du réseau. Cette « confiance zéro » se traduit pas une vérification stricte de chaque utilisateur et de chaque appareil avant de donner une autorisation d'accès aux ressources internes.

• Le Firewall-as-a-Service (FWaaS), la nouvelle génération de pare-feu dans le cloud permettant le filtrage des url, la protection contre les menaces avancées, les systèmes de prévention des intrusions (IPS) et la sécurité DNS.

• Le Data Leak Protection (DLP) qui permet de contrôler les transferts de données sensibles ou critiques en dehors du réseau de l'entreprise

• Le chiffrement des données qui permet de protéger la confidentialité des données échangées via le réseau

Couplé avec une architecture SD-WAN, le modèle SASE offre un accès sécurisé et efficient pour les utilisateurs, indépendamment de leur emplacement, tout en offrant un contrôle global de la sécurité à la DSI.

En conclusion, face à un environnement réglementaire de plus en plus strict, notamment au niveau européen, la mise en place d'une architecture SASE facilite la mise en conformité avec les exigences légales sur la protection des données. La mise en œuvre de nouvelles politiques de sécurité adaptées à l'ère du télétravail et du cloud computing en est facilitée.

Pour Ilyes Soltane, « Dès lors qu'on aborde le SASE de la bonne manière, c'est-à-dire en partant du legacy et des besoins métier et en transformant chaque brique de sécurité de façon progressive, en repensant la sécurité sous l'angle des nouveaux usages, ce modèle offre une combinaison idéale pour offrir une sécurité renforcée sans compromettre la flexibilité ou les performances du réseau. »