Pendant longtemps, protéger le réseau interne de l'entreprise suffisait. Un firewall comme fondation, un VPN pour les accès distants, quelques règles de filtrage bien pensées... et l'essentiel était couvert.

Ensuite sont arrivés le cloud, la multiplication des applications SaaS et la généralisation du télétravail. La frontière mise en place au sein de l'entreprise doit maintenant s'étendre à cette nouvelle population de nomade. Notre rôle et notre but est d'assurer la sécurité dans

quoi sert réellement cette architecture ? Et surtout, comment répond-elle concrètement à vos **besoins de sécurité** ?

Pourquoi le modèle de sécurité traditionnel a atteint ses limites

Le travail hybride a profondément modifié l'équation de sécurité. Les collaborateurs alternent entre bureau, domicile et déplacements. Les applications critiques sont désormais réparties entre **data centers, clouds publics et plateformes SaaS**.

Autrement dit, le réseau est devenu *multi-edge*. Et chacun de ces *edges,* ou points d'accès, représentent un risque potentiel : un poste de travail mal configuré, un réseau Wi-Fi public ou un terminal compromis peuvent servir de porte d'entrée vers votre système d'information. Dans ce contexte, continuer à raisonner uniquement en termes de périmètre interne devient insuffisant.

Le cas VPN

Le Virtual Private Network, longtemps considéré comme la solution standard pour l'accès distant, montre aujourd'hui des **limites**. Conçu pour un usage ponctuel et centralisé, il accorde souvent un accès au réseau trop large par rapport aux besoins réels. En cas de compromission d'identifiants, il facilite les **déplacements latéraux** à l'intérieur du SI.

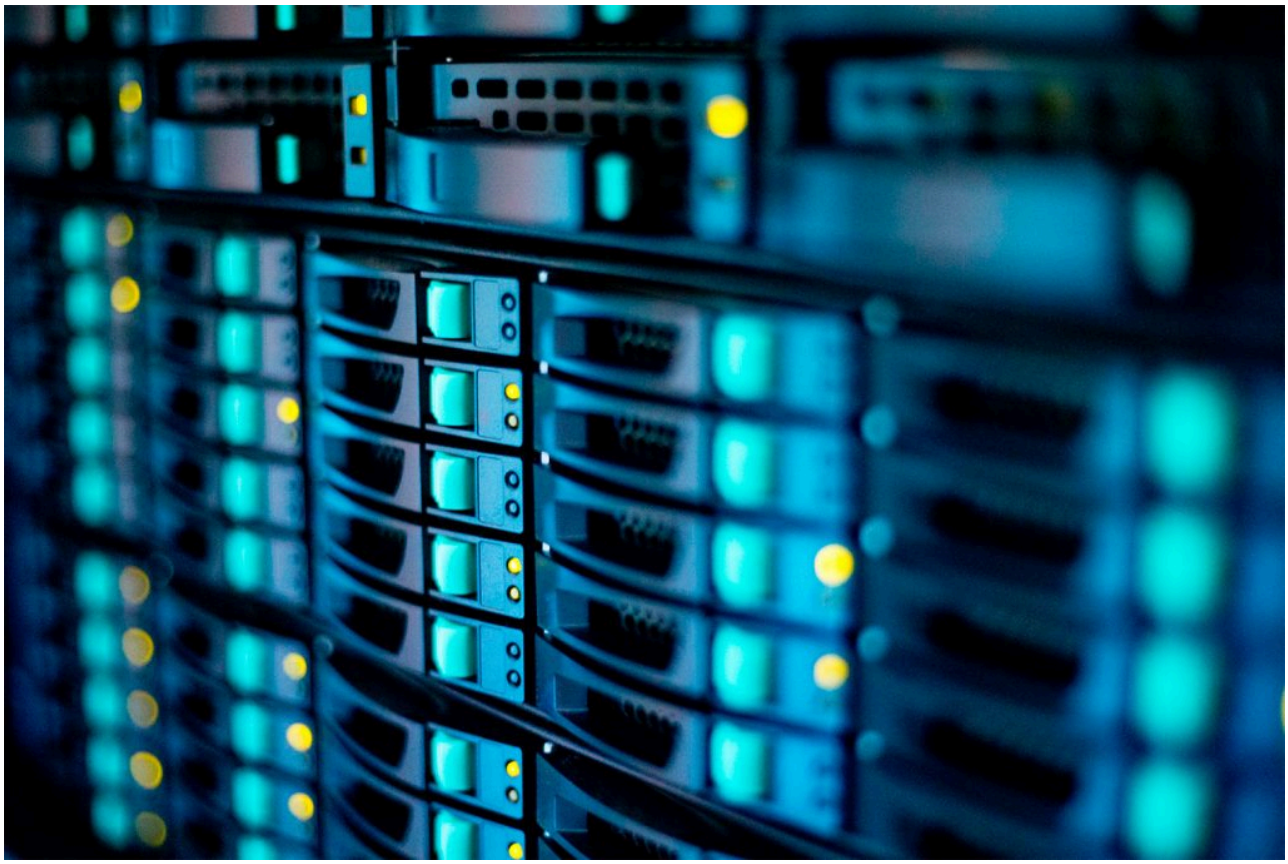
Pour compenser ces faiblesses, beaucoup d'organisations ont ajouté des couches successives de sécurité. Proxy web, firewall nouvelle génération, CASB, DLP, outils de supervision… La sécurité s'est enrichie, mais surtout **complexifiée** avec l'apparition de consoles multiples, les politiques de sécurité non-uniformes et une **visibilité fragmentée**.

Au final, les équipes IT doivent gérer un écosystème hétérogène, parfois difficile à piloter de bout en bout.

Le SASE, concrètement, c'est quoi ?

Le SASE est une architecture qui vise à faire **converger réseau et sécurité** dans un modèle largement orienté cloud.

Il repose sur l'association de deux grandes dimensions. D'un côté, la connectivité, souvent portée par le **SD-WAN** pour relier efficacement sites distants et utilisateurs. De l'autre, un ensemble de services de sécurité délivrés depuis le cloud, regroupés sous l'appellation **SSE**, Security Service Edge.



Pourquoi cette association ?

L'objectif est simple sur le papier : fournir un accès sécurisé, cohérent et performant aux applications, quel que soit l'endroit où se trouvent les utilisateurs et les ressources.

Dans une architecture SASE complète, on retrouve généralement des fonctions telles que :

- le ZTNA pour remplacer le VPN par un accès applicatif basé sur l'identité
- une passerelle web sécurisée pour protéger l'accès Internet (SSE – Security Service Edge)
- un firewall délivré en mode service (FWaaS – Firewall as a Service)
- un contrôle des usages cloud (CASB – Cloud Application Security Broker)
- ainsi qu'une prévention des pertes et fuites de données (DLP – Data Loss Prevention).

Le SD-WAN vient compléter l'ensemble pour optimiser et sécuriser la connectivité des sites distants.

La promesse du SASE ne réside pas seulement dans l'addition de ces briques, mais dans leur **intégration cohérente au sein d'une plateforme unifiée.**

Les cas d'usage concrets du SASE

Au-delà du concept, le SASE répond à des problématiques très opérationnelles :

1

Remplacer le VPN par du ZTNA, afin de fournir un accès strictement limité aux applications nécessaires, basé sur l'identité et avec un contrôle continu de la posture de sécurité.

2

Sécuriser l'accès internet des collaborateurs hybrides, en inspectant les flux, y compris chiffrés, et en bloquant les menaces avancées indépendamment de la localisation de l'utilisateur.

3

Maîtriser le Shadow IT et sécuriser le SaaS, en apportant de la visibilité sur les applications utilisées et en protégeant les données sensibles via des mécanismes de contrôle et de DLP.

4

Moderniser la connectivité des sites distants, grâce à un SD-WAN sécurisé capable d'acheminer intelligemment le trafic vers des ressources.

5

Consolider des solutions réseau et sécurité parfois dispersées, pour réduire la complexité et améliorer la cohérence des politiques de sécurité.

Ces cas d'usage illustrent bien que le SASE n'est pas une solution nouvelle ou une architecture supplémentaire à déployer, mais une tentative d'uniformisation globale de la gestion du réseau.

SASE : tendance ou évolution incontournable ?

Le SASE n'est pas une mode éphémère. Il traduit une transformation profonde des usages IT.

Les utilisateurs et les applications sont éclatés sur différentes réseaux, serveurs, localisations, etc. Continuer à sécuriser uniquement un périmètre interne n'a plus vraiment de sens.

Le SASE apporte une réponse cohérente à cette réalité, à condition d'être envisagé comme une **architecture globale**.

La vraie question n'est donc pas de savoir si le SASE est pertinent. Elle est de déterminer comment l'intégrer intelligemment dans votre stratégie de cybersécurité, en **tenant compte de votre maturité**, de vos contraintes et de vos priorités.

Besoin d'accompagnement pour déployer un modèle SASE ?

Pour étudier le sujet avec vous et commencer à dessiner une architecture SASE cohérente, contactez-nous directement. SNS Security dispose d'ingénieurs certifiés sur le sujet qui peuvent vous aider à configurer, installer et surveiller toutes les briques qui composent le SASE. Le tout, avec un chef de projet dédié pour vous accompagner dans la durée.

Contactez nos experts

Partager sur Linkedin

RÉSEAU

INSIGHTS

Découvrir tous nos articles

PROTÉGER ENTREPRISE

Au cœur de notre SOC de Saintes : là où la cybersécurité se vit au quotidien

À quelques kilomètres de La Rochelle, au cœur de la Charente-Maritime, se trouve l'un des piliers opérationnels de SNS Security...

TECHNO RÉSEAU

SASE : est-ce le bon moment pour faire la bascule ?

Pendant longtemps, protéger le réseau interne de l'entreprise suffisait. Un firewall comme fondation, un VPN pour les accès distants, quelques...

Voir tout →

Plan du site

Protéger mon infrastructure
Surveiller mes actifs informatiques
Évaluer ma maturité
Assistance Technique
Santé
SOS
À propos de nous
Rejoignez notre équipe
Nos articles de blog
Fortinet
Sentinelone
Vectra

Contact

381 av. du Mas d'Argelliers – Le New Work 1, étage 2 | 34000 Montpellier, France | +33 (0)4 67 63 97 14

Contactez-nous

Télécharger notre plaquette

Rejoignez notre newsletter !

E-mail*

Mentions légales & CGU
Charte de protection des données