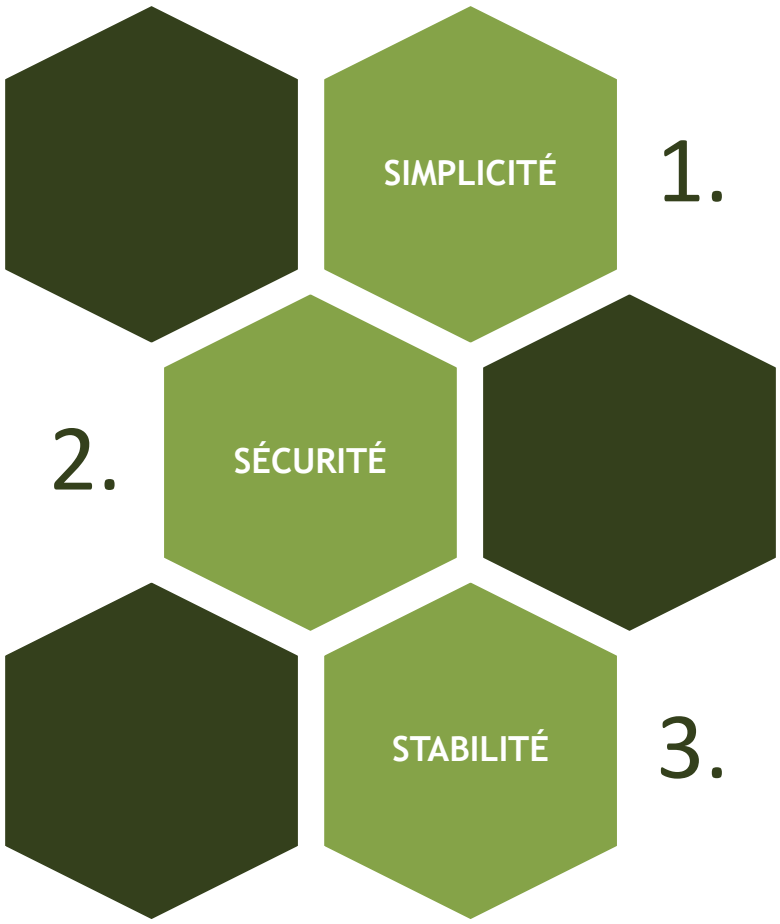
SECURE ACCESS SERVICE EDGE

SECURE ACCESS SERVICE EDGE : DÉFINITION

Gartner a décrit pour la première fois le secure access service edge, ou SASE (prononcer "sassy"), dans son étude d'août 2019 intitulée The Future of Network Security in the Cloud, puis l'a développé dans sa feuille de route stratégique 2021 pour la convergence SASE.

Avant d'entrer dans les détails du SASE, il est important de comprendre ses bases. Les méthodes et technologies de réseau traditionnelles ne peuvent tout simplement pas fournir le type de gestion d'identités et de la sécurité dont les entreprises numériques ont besoin. En effet, ces dernières s'attendent à ce que leurs utilisateurs aient des liens rapides et directs, où qu'ils se trouvent. Compte tenu de l'éloignement des clients et des applications, de la circulation du contenu entre le centre de données et les systèmes d'exploitation, et du fait que davantage de données circulent vers le cloud public et les centres de services qu'elles ne retournent vers le centre de données, une nouvelle approche de la sécurité réseau est nécessaire.

SASE est un modèle de service fourni dans le nuage qui combine un réseau étendu (WAN) et des services de sécurité réseau tels que CASB, FWaaS et Zero Trust. Selon Gartner, les fonctionnalités SASE sont fournies en tant que service sur la base de l'identification de l'entité, du contexte pertinent, des règles de sécurité/conformité de l'entreprise et de l'évaluation continue des risques/de la confiance au cours des sessions Les personnes, les catégories de personnes (succursales), les équipements, les apps, les services, les systèmes IoT et les emplacements d'edge computing peuvent tous être associés aux identités des entités.



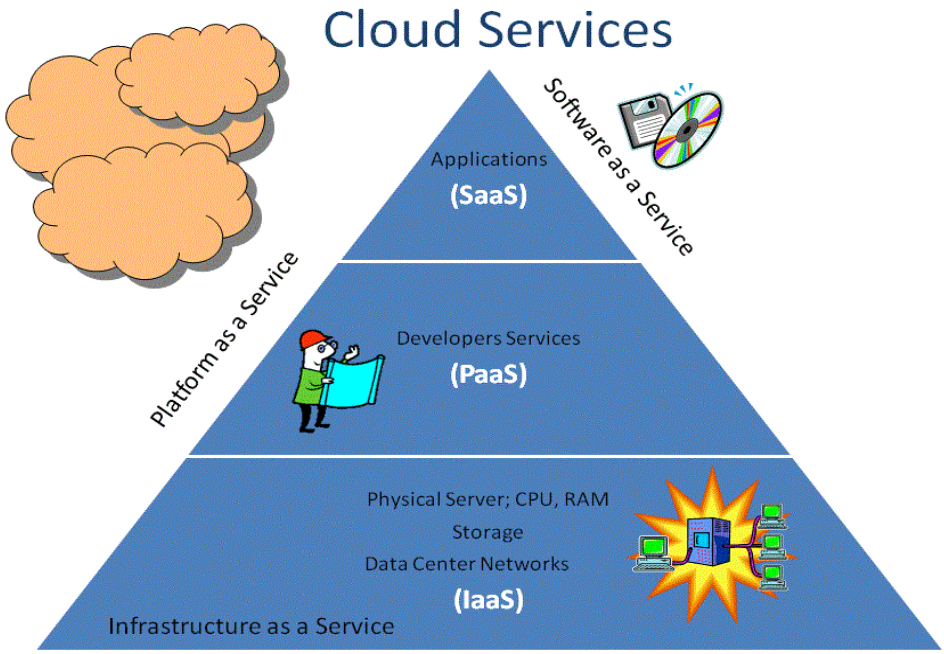
COMMENT ÇA MARCHE ?

À mesure que le nombre d'employés à distance augmente, la dépendance aux services SaaS s'accroît, ce qui entraîne de nouvelles vulnérabilités plus importantes. En termes simples, la protection des consommateurs à la périphérie est plus difficile : il faut maintenir des connexions transparentes qui augmentent la productivité sans causer de problèmes de performance qui réduisent le confort des utilisateurs.

Le service d'accès sécurisé edge (SASE) est une solution architecturale à la sécurité basée sur le centre de données qui offre une alternative. Pour faciliter le déploiement et la maintenance du cloud, SASE combine des capacités de mise en réseau avec des fonctions de sécurité conçues pour le cloud.

SASE combine la hiérarchisation du trafic réseau et de la protection, la sécurité des risques et des données importants, ainsi que la communication réseau-cloud ultra-rapide et transparente. Alors que SASE était autrefois un choix

entre performance et contrôle, la nouvelle technologie permet désormais aux organisations d'avoir les deux. SASE est un concept qui permet aux experts en sécurité des entreprises d'utiliser l'identification et le contexte pour déterminer le niveau exact de performance, de fiabilité, de sécurité et de coût pour chaque session réseau. Les organisations qui utilisent le cadre SASE peuvent atteindre une échelle et une portée plus élevées dans le cloud tout en réglant les problèmes de sécurité supplémentaires qui en découlent.

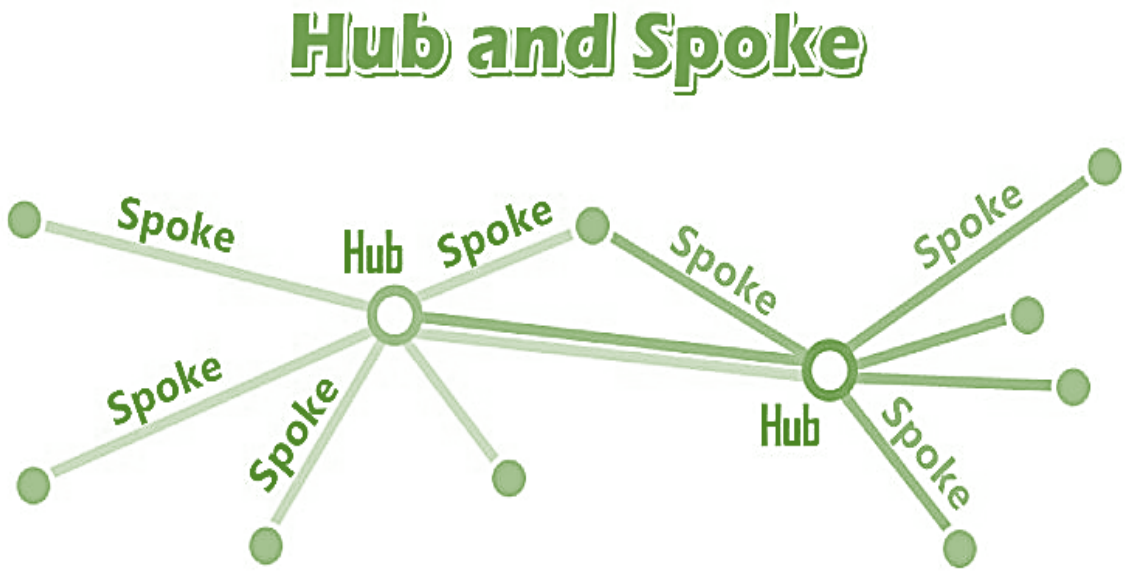


LE MODÈLE HUB AND SPOKE ET SES INCONVENIENTS

Le modèle hub-and-spoke est simple en théorie. En revanche, ce paradigme est incapable de faire face aux subtilités des solutions basées sur le cloud, telles que les logiciels en tant que service (SaaS) et l'augmentation du nombre d'employés à distance. Les organisations doivent réévaluer où et comment le trafic Internet est analysé, ainsi que la façon dont les restrictions d'accès des utilisateurs protégés sont gérées, car de plus en plus de postes de travail, d'applications et de données sensibles des clients migrent vers le cloud.

Lorsque plusieurs logiciels et services sont stockés dans le cloud, il est impossible de reconfigurer tout le trafic dans un seul centre de données. Les

utilisateurs distants peuvent subir une latence lorsqu'ils se connectent à un réseau d'entreprise à l'aide d'un VPN, ce qui aggrave le problème. Il est fréquent que des employés mécontents exploitent une connexion non protégée pour accéder au réseau de l'entreprise.

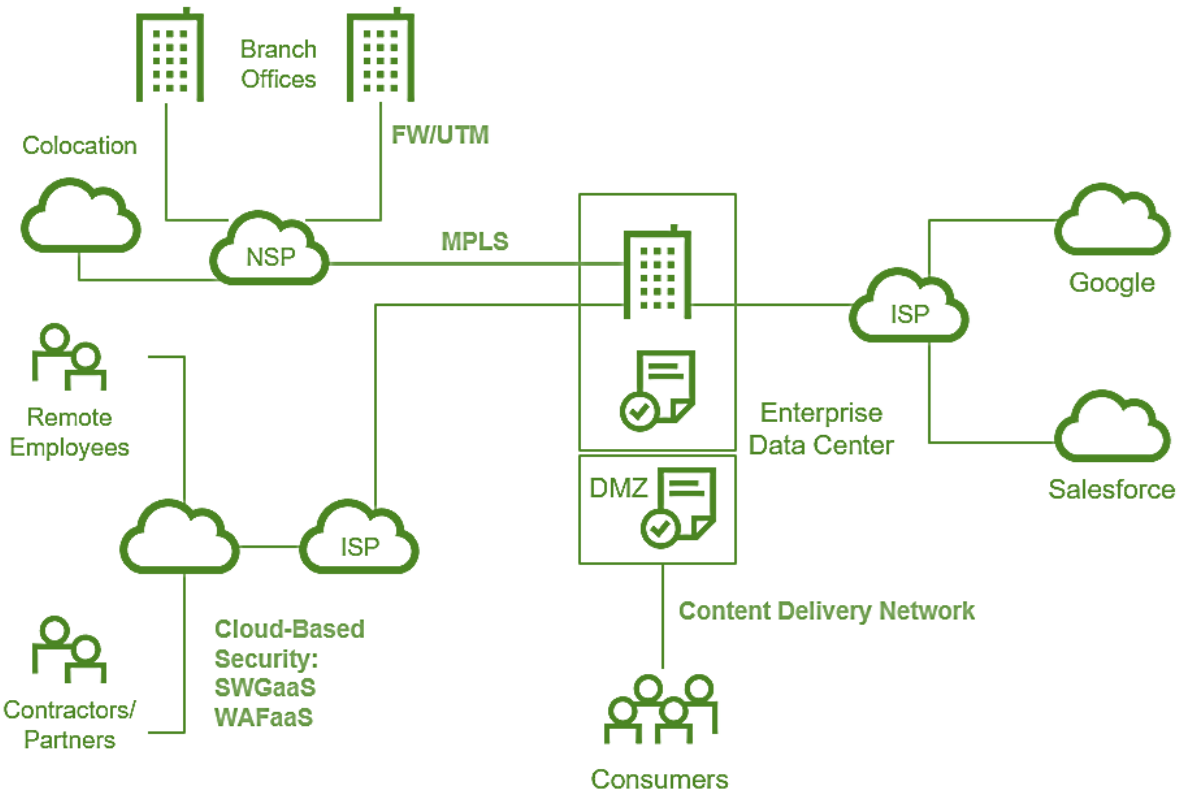


LA SOLUTION SASE SAUVE LA MISE

Avec SASE, par exemple, les contrôles réseau sont déplacés du centre de données de l'entreprise vers la périphérie du cloud, ce qui les rapproche du service utilisé. SASE élimine les services cloud en couches qui nécessitent une mise en œuvre et une gestion distinctes, ce qui permet de combiner les services de réseau et de sécurité afin de fournir une périphérie de réseau sûre et constante.

Une des principales caractéristiques de SASE consiste en la mise en œuvre de restrictions d'accès fondées sur l'identité et la confiance zéro, en particulier sur le réseau périphérique. Les entreprises peuvent l'utiliser pour accorder aux utilisateurs un accès limité aux seuls programmes et données dont ils ont besoin pour effectuer leur travail, sans avoir à se connecter à un réseau via un VPN. Les réglementations en matière de sécurité du réseau sont contrôlées de manière plus granulaire et le matériel existant, comme les VPN et les pare-feu, peut être éliminé.

Traditional Data Center-Centric, Hub and Spoke Network and Network Security Architecture
Data-Center-Centric Networking and Security Model



LES OBJECTIFS DU SASE

L'objectif principal du modèle SASE est de contribuer à la modernisation des réseaux et de la protection afin de répondre aux besoins en constante évolution des entreprises. SASE y parvient en assurant une sécurité constante entre les utilisateurs, quel que soit l'endroit où ils exercent leurs activités, ainsi que la connaissance et la transparence de ce qui peut être accessible.

- Un contrôle automatisé des appareils et une transparence complète des appareils
- Une micro-segmentation du réseau pour limiter les mouvements relatifs et prévenir les violations.
- Les risques cybernétiques et logistiques sont surveillés, évalués et corrigés en permanence.
- Des produits et solutions de plusieurs fabricants, avec des degrés d'orchestration, d'automatisation et de réponse sans précédent.

- La gestion des terminaux IoT et des technologies connexes de manière sécurisée et efficace (systèmes OT).
- Les appareils virtuels et physiques, ainsi que l'infrastructure et les charges de travail du réseau, sont découverts, évalués et réparés/contrôlés.

LES AVANTAGES DU SASE

Le modèle SASE combine de nombreuses tâches de mise en réseau et de sécurité, qui étaient auparavant proposées sous forme de solutions ponctuelles distinctes, en un service cloud unique et intégré. Les entreprises peuvent ainsi tirer profit de la consolidation de SASE de la manière suivante :

- Les coûts et la complexité sont réduits.
- Permet aux utilisateurs de bénéficier d'un accès fluide en fournissant une orchestration centralisée et une optimisation des applications en temps réel.
- Renforcer la sécurité de l'accès à distance et mobile.
- L'accès est restreint en fonction de l'identification de la personne, du dispositif et de l'application.
- Renforcer la sécurité en assurant la cohérence des politiques.
- Grâce à l'administration centralisée, vous pouvez améliorer l'efficacité de vos employés chargés du réseau et de la sécurité.

LES COMPOSANTS DU SASE

	Traditional networking models	SASE model
REMOTE ACCESS TO ON-PREMISES RESOURCES	Most traditional models largely rely on VPN technology through SSL/TLS browser access or a dedicated endpoint client.	SASE acts as a VPN replacement. Users connect to a SASE to access on-premises resources and cloud services. Policy is defined and applied through the SASE console.
ACCESS TO CLOUD RESOURCES	On-premises network access to cloud resources treats these like any other online properties, using traditional firewalls, proxies and routing controls.	SASE provides optimized, streamlined, cloud-aware network access for SaaS, PaaS and IaaS. These rely on API integration and request introspection for end-user requests.
NETWORK ACCESS CONTROLS	Most on-premises environments rely on switching, routing, firewalls and proxies for access control.	SASE services aggregate a number of network security and access controls—including firewalls as a service—into one unified fabric.
SD-WAN, WAN OPTIMIZATION, BANDWIDTH AGGREGATION	These controls and capabilities usually require several vendors and products to function, and they may lack in integration.	A SASE service integrates SD-WAN access and traffic optimization capabilities into a single brokering service for all access types.
WEB APPLICATION SECURITY	WAFs are usually separate appliances or platforms, or are achieved through brokering to a content delivery network or in-cloud service.	SASE platforms integrate WAF policies and services into the same brokered approach, although policies and capabilities may not be as mature yet.
NETWORK THREAT DETECTION	Network threat detection is accomplished using NGFWs, malware detection sandboxes or CASB brokering.	SASE services combine numerous network threat detection capabilities into one service fabric.

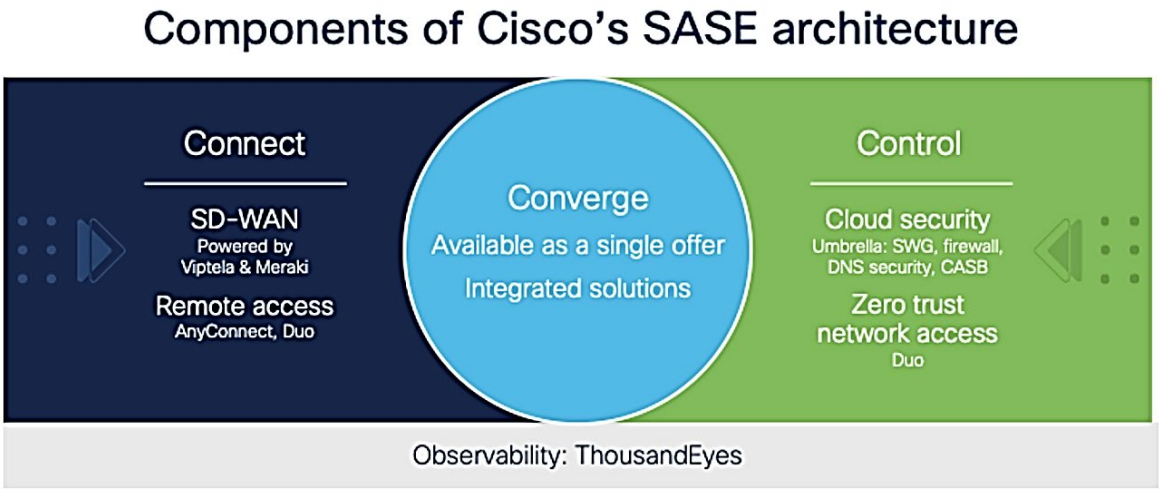
TOP 5 DES ENTREPRISES FOURNISSANT DES SASE :

Akamai	Akamai Technologies, Inc. est un fournisseur de solutions de sécurité numérique et en ligne, ainsi qu'un réseau mondial de distribution de médias, de sécurité des données et de services de cloud.
CATO NETWORKS	Le SD-WAN et le système de sécurité sont combinés à une solution de stockage dans le cloud dans l'offre principale de l'organisation.
CLOUDFLARE	Cloudflare, Inc. est une entreprise de sécurité informatique et d'infrastructure en ligne basée aux États-Unis. Elle est spécialisée dans les réseaux de distribution de médias et dans la mitigation des DDoS.
Forcepoint	Forcepoint est une entreprise de programmes basée au Texas et spécialisée dans les technologies de cybersécurité et la sécurité des informations, ainsi que dans les courtiers de contrôle accessibles dans le cloud, les pare-feu et les services inter domaines.
McAfee	McAfee Corp. est une société internationale de programmes de cybersécurité basée en Californie.

POURQUOI ADOPTER LA SOLUTION CISCO POUR SASE ?

Nombre d'entreprises sont aujourd'hui confrontées à un sérieux dilemme : Comment le personnel chargé de la sécurité et du réseau peut-il garantir l'accessibilité aux programmes pour une main-d'œuvre toujours plus nombreuse sans poser de difficultés ? Pour ce faire, il faut revoir l'architecture réseau standard, ce qui aboutit à la conception d'un secure access service edge (SASE). En clair, la solution SASE correspond aux fonctions de connectivité et de sécurité du cloud. Pour Cisco, la technologie SASE n'est pas unique.

Depuis deux ans et demi, Cisco aide les entreprises du monde entier à établir une connexion pour leur société. Et ces mêmes entreprises ont participé à leur défense contre les cyberdangers croissants. Il s'est développé au fil du temps, de sorte que son expertise est plus simple et plus efficace. Cisco innove encore en vous fournissant un réseau sécurisé adapté au cloud.



L'architecture SASE de Cisco sécurise et optimise votre connexion, ce qui vous permet de fournir les meilleurs engagements possibles aux utilisateurs. Dans ce cas, l'observabilité est considérée comme un élément crucial dans la création de cet environnement. De plus en plus de connexions échappent à votre gestion ou à votre contrôle total à mesure que votre dépendance à l'égard de l'Internet et des services du cloud se développe.

Bien qu'elles n'exploitent pas les infrastructures ou n'aient pas de contrôle sur la façon dont les opérateurs de réseau dirigent le trafic, les entreprises

doivent s'assurer de l'efficacité et de la qualité du transport sous-jacent. Cisco fournit une vue complète, du client au logiciel, de tous les réseaux et du cloud computing, ainsi que des informations significatives sur les problèmes de performance, ce qui vous permet de détecter, de rectifier ou de signaler rapidement les progrès afin de maintenir votre expérience numérique à niveau.

Si Cisco n'est pas le premier fournisseur à proposer un système SASE, il offre néanmoins l'ensemble de services le plus complet. Cisco SD-WAN 17.2 combine des solutions issues des lignes de produits de connectivité et de protection de l'entreprise. Ainsi, on trouve des éléments de connectivité, d'IDS/IPS et de filtrage des URL de Viptela et Meraki, ainsi que des fonctions de portail en ligne sécurisé, de sécurité DNS, de cloud access security broker (CASB) et de pare-feu d'Umbrella.

Cisco combine également les fonctions de sécurité de ses solutions de confiance zéro. En raison de son envergure, Cisco présente certainement plusieurs caractéristiques distinctives fascinantes. Les fonctionnalités de cybersécurité doivent être disponibles dans le cloud. Tous les fournisseurs actuels de SASE dépendent du cloud public, des centres de données ou de fournisseurs tiers pour fournir leurs services.

Malgré la multitude de concurrents SASE, nombre de fournisseurs proposent des fonctions de sécurité et de connectivité. Cisco est l'entreprise leader dans le domaine des réseaux et de la cybersécurité, et elle peut apporter ses connaissances en matière de communications unifiées tout en offrant un avantage stratégique.

Cisco a introduit un système qui offre des choix aux clients au lieu de les contraindre à utiliser un système qui ne s'adresse qu'à une partie de l'entreprise.