ARCHITECTURE ET OUTILS DE SÉCURITÉ

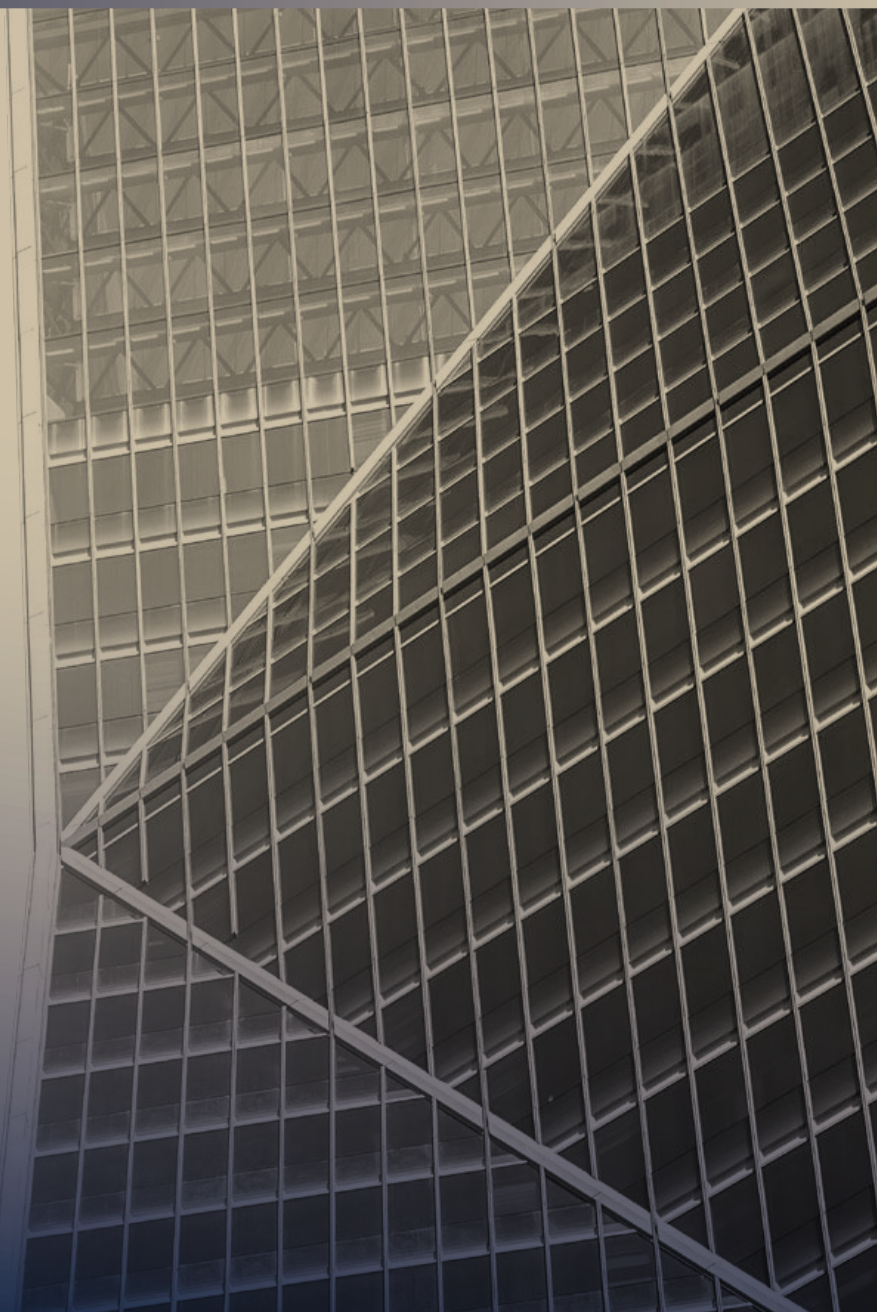
DOSSIER TECHNIQUE

LE **SASE** (SECURE ACCESS SERVICE EDGE)

1 Tous publics 2 Avancé 3 Expert

Mars 2026

Fonctionnalités, promesses et points d'attention autour du Secure Access Service Edge



CLUSIF

L’article L. 122-5 de la propriété intellectuelle n’autorisant pas les représentations ou reproduction intégrale, ou partielle, faite sans le consentement de l’auteur ou de l’ayant droit ou ayant cause, sauf exception stricte (« copies ou reproductions réalisées à partir d’une source licite et strictement réservées à l’usage privé du copiste et non destinées à une utilisation collective », analyses et les courtes citations dans un but d’exemple et d’illustration, etc.), toute représentation ou reproduction, par quelque procédé que ce soit du présent document sans autorisation préalable du Clusif constituerait une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

Table des matières

1 INTRODUCTION 7

1.1 La naissance du SASE 7
1.1.1 Le SSE, tremplin vers le SASE 8
1.1.2 Que permet le SASE ? 9

2 DESCRIPTION DETAILLEE DES DIFFERENTS SERVICES ET COMPOSANTS 10

2.1 Liste des composants du SASE 10
2.1.1 SD-WAN 10
2.1.2 CDN 11
2.1.3 SWG 11
2.1.4 CASB 12
2.1.5 ZTNA 12
2.1.6 Next Gen - Firewall(NG-FW) / Firewall as a Service (FWaaS) 13
2.1.7 DLP 13
2.1.8 RBI 14
2.1.9 DNSS 15

2.2 Composants supplémentaires 16
2.2.1 CNAPP 16
2.2.2 CSPM 16
2.2.3 SSPM 17
2.2.4 CWPP 17
2.2.5 CIEM 17
2.2.6 WAAP 17
2.2.7 EDR, NDR et XDR 18

3 CORRESPONDANCE FONCTIONNALITES/COMPOSANTS 20

4 BENEFICES/RISQUES 21

4.1 Les bénéfices 21
4.1.1 Capacité d'évolutivité 21
4.1.2 Centralisation 21
4.1.3 Modèle de sécurité 21
4.1.4 Disponibilité et performances réseau 21
4.1.5 Adaptabilité des coûts 22
4.1.6 Transfert de risque 22

4.2 Risques 23
4.2.1 Réversibilité 23
4.2.2 Dépendance au fournisseur 23
4.2.3 Réglementaire 23
4.2.4 Exposition accrue aux attaques cyber 24
4.2.5 Difficulté de comparaison 24
4.2.6 Complexité d'implémentation 24
4.2.7 Gestion du changement 25
4.2.8 Partage des responsabilités 25
4.2.9 Temps de réponse 25
4.2.10 Dépendance aux composants du SI hors SASE 25

5 PROPOSITION D'APPROCHE POUR CHOISIR SA SOLUTION SASE/SSE 27

5.1 Infrastructure 27

5.2 Composants proposés par l'éditeur 28

5.3 Intégration (Endpoints/Appliances...) 29

5.4 Administration 30

5.5 Ouverture / Interopérabilité 30

5.6 Engagements / Responsabilités 30

5.7 Protection des données par l'éditeur 31

5.8 Modèle financier 31

5.9 Modèle de gestion 31

6 CAS D'USAGES ET EXEMPLES D'IMPLEMENTATION 32

6.1 Cas d'usages 32

6.1.1 Accès distants sécurisés pour les utilisateurs 32

6.1.2 Gestion des accès aux applications 32

6.1.3 Interconnexion sécurisée des sites distants 32

6.1.4 Contrôle de l'échange des données 33

6.2 Exemples d'implémentation 33

6.2.1 Cas d'implémentation numéro 1 33

6.2.2 Cas d'implémentation numéro 2 34

6.2.3 Cas d'implémentation numéro 3 34

6.2.4 Cas d'implémentation numéro 4 35

7 SYNTHESE MANAGERIALE 37

Remerciements

Le Clusif tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Baptiste	**HAMON**	SSI CONSEIL
Jean-Marc	**JACQUOT**	NEXTAURA

Les contributeurs :

Xavier	**AIT-YAHIATENE**	BANQUE DE FRANCE
Linley	**BRASSE**	L²CD
Romuald	**BLONDEL**	BPIFRANCE
Valentin	**JANGWA**	LEVAS/GS MAG
Laurent	**MARTINET**	INTEGRALE IP
Tristan	**SAVALLE**	ADVENS
Gilles	**ZYCHOWSKI**	OFFICE NATIONAL DES FORÊTS

Le Clusif remercie également les adhérents ayant participé à la relecture.

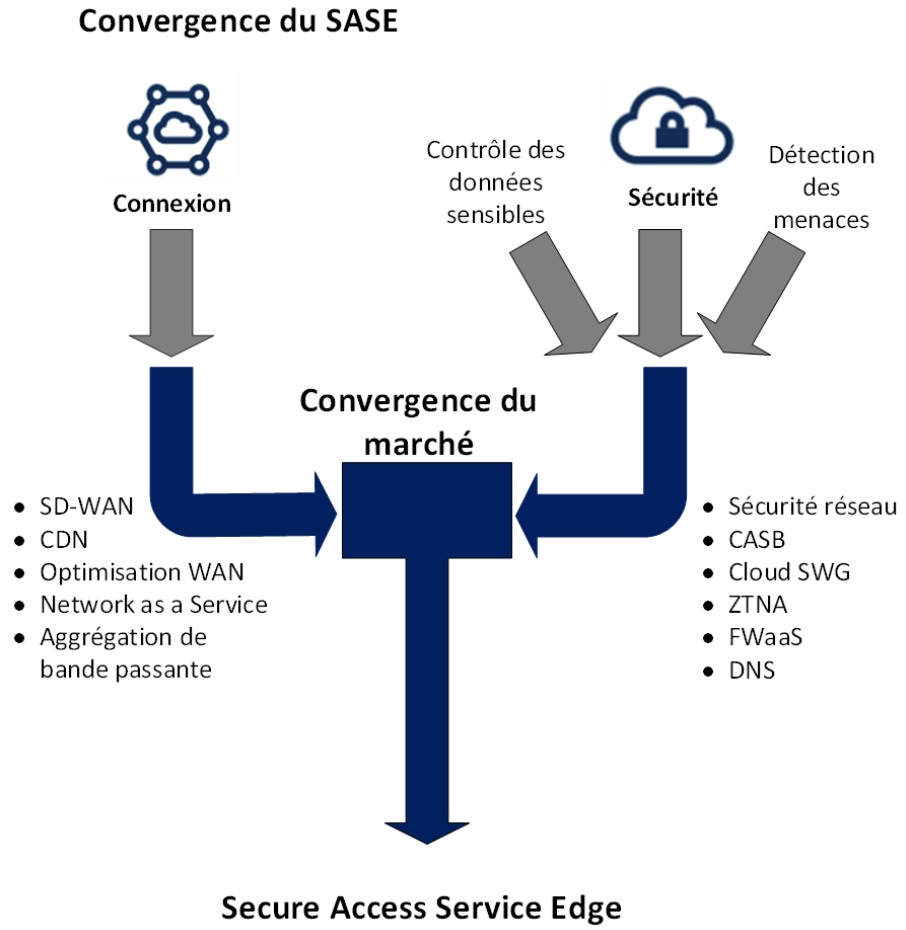
1 Introduction

Le Secure Access Service Edge (SASE) est un terme conceptualisé en 2019 pour décrire un modèle d'architecture faisant converger la connectivité réseau avec les fonctions de sécurité réseau en les proposant sur une plateforme cloud unique. Cette plateforme permet d'assurer une visibilité et des mesures de contrôle cohérentes pour n'importe quel utilisateur sur n'importe quelle application lorsque ces derniers y sont rattachés.

1.1 La naissance du SASE

Le concept de SASE a été formalisé par Gartner, mais s'inscrit dans une évolution amorcée plus tôt : la convergence du réseau (SD-WAN) et de la sécurité (SWG, CASB, ZTNA) aujourd'hui regroupés sous le terme SSE (Security Service Edge). Face à la montée du cloud, à la mobilité des utilisateurs et aux limites des architectures centralisées, certains acteurs historiques à l'origine du FWaaS avaient, dès 2016, commencé à proposer une architecture unifiée, cloud-native et distribuée. Le SASE reprend cette vision en l'élargissant à l'ensemble du WAN, pour rapprocher les fonctions critiques du point d'accès utilisateur via des points de présence (PoP) globalement répartis. La sécurité ne repose plus sur le périmètre réseau, mais sur l'identité et le contexte d'accès. Cette approche s'impose progressivement comme un standard pour répondre aux enjeux de performance, de sécurité et de flexibilité du SI distribué moderne.

1.1.1 Le SSE, tremplin vers le SASE

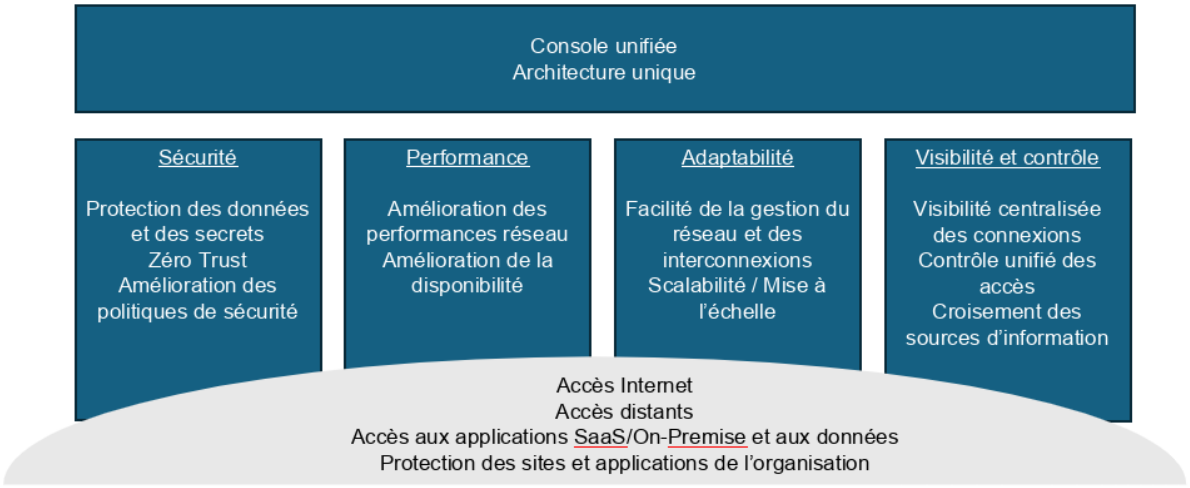


Le Security Service Edge (SSE) représente la composante sécurité du modèle SASE. Il regroupe plusieurs services critiques opérés depuis le cloud, notamment le Cloud Access Security Broker (CASB), le Secure Web Gateway (SWG), le Zero Trust Network Access (ZTNA) et le Firewall as a Service (FWaaS), illustrés à droite sur le schéma ci-dessus. Le SSE vise à sécuriser l'accès aux ressources Internet, aux applications Software as a Service (SaaS) et aux applications privées standards, en s'appuyant sur des politiques centralisées, basées sur l'identité et le contexte.

Quand les organisations ne commencent pas par une refonte réseau de type SD-WAN, la mise en œuvre du SSE constitue souvent une première étape logique. Moins intrusif à déployer, il permet de répondre rapidement aux enjeux de sécurité liés au cloud et au travail à distance. Ce déploiement progressif crée une base cohérente pour intégrer ultérieurement la couche réseau de manière fluide. Le SSE agit ainsi comme un tremplin pragmatique vers une architecture SASE complète.

1.1.2 Que permet le SASE ?

Le SASE ne se limite pas à une simple addition de briques réseau et sécurité : il propose une approche unifiée orientée cloud-native qui transforme la gestion des accès et la sécurisation des ressources. Cette convergence permet d'apporter des fonctionnalités difficilement atteignables avec des architectures traditionnelles.



Les fonctionnalités de sécurité réseau, de filtrage d'URL, de protection contre les menaces, de contrôle d'accès, de prévention de perte des données, de surveillance du Shadow IT, d'analyse du comportement des utilisateurs et des entités (UEBA[1]), et la sécurité des données sont prises en charge par le SASE.

Déployer du SASE n'empêche pas d'avoir à gérer certaines exceptions ou spécificités du système d'information (imprimantes, caméras IP, téléphonie, équipements industriels). Certains éditeurs SASE proposent des solutions spécifiques pour l'OT/IoT.

[1] User and Entity Behavior Analytics.

2 Description détaillée des différents services et composants

2.1 Liste des composants du SASE

Composants principaux :

- Optimisation du réseau :
  - **SD-WAN** :
    - WAN Optimization / SaaS Acceleration
    - Quality of Service
    - Routing
    - Dynamic Path Selection
  - **CDN**
- Sécurisation des données et des usages :
  - **SWG** (Secure Web Gateway)
  - **CASB** (Cloud Access Service Broker)
  - **ZTNA** (Zero Trust Network Access)
  - **NG-FW** / **FWaaS** (Next Generation Firewall / Firewall as a Service)
  - **DLP** (Data Leak/Loss Protection/Prevention)
  - **RBI** (Remote Browser Isolation)
  - **DNSS** (DNS Security)

Composants satellites :

- **CSPM** (Cloud Security Posture Management) / **SSPM** (SaaS Security Posture Management), **CNAPP** (Cloud Native Application Protection Platform)
- **WAAP** (Web Application and API Protection)
- **EDR**, **NDR**, **XDR**

En bleu, les Composants « Coeur » du SASE

2.1.1 SD-WAN

Le SD-WAN (Software-Defined Wide Area Network) est une technologie réseau « logicielle » qui permet de centraliser la gestion des réseaux étendus de type WAN, et d'obtenir une visibilité globale sur son trafic.

Le SD-WAN se base sur des équipements (ou pare-feux, ou routeurs, etc.) capables d'orchestrer et d'optimiser le trafic WAN, en utilisant plusieurs liens d'opérateurs, notamment Internet, à des fins de résilience et de simplification d'architectures de communication.

Techniquement, le SD-WAN est composé d'un « Control Plane » et d'un « Data Plane » :

- Le Control Plane (plan de contrôle) est l'intelligence centralisée. Chargé du pilotage et de l'orchestration, il est responsable de la gestion des configurations du trafic réseau et des décisions de routage, et pilote plusieurs équipements,
- Le Data Plane (plan de données) est le réseau physique porté par les équipements : il est responsable du traitement, du transport et du routage des paquets/informations, selon les instructions reçues du Control Plane.

Le SD-WAN repose sur une séparation claire entre le Control Plane et le Data Plane, le tout piloté par le Management Plane (plan de gestion). Le Control Plane centralisé pilote plusieurs équipements du Data Plane répartis sur différents sites et peut orchestrer leurs communications en temps réel.

Avant le SD-WAN, chaque routeur ou firewall fonctionnait de manière autonome avec son

propre plan de contrôle embarqué, ce qui limitait l'intelligence globale et l'interopérabilité entre équipements de différents sites.

Le SD-WAN introduit également la notion d'*overlay*, qui constitue un réseau logique sécurisé (via IPsec ou autre encapsulation) s'appuyant sur un *underlay*, c'est-à-dire les réseaux physiques sous-jacents (MPLS, Internet, 4G/5G, etc.). Cela permet de superposer une connectivité optimisée et sécurisée sur des liaisons hétérogènes, tout en assurant une gestion centralisée des politiques de routage, de sécurité et de qualité de service. En complément, le SD-WAN permet :

- d'optimiser le trafic, notamment par son analyse et par des prises de décisions (acheminer l'information par un lien plus performant que l'autre à l'instant T, etc.), mais aussi par des mécanismes de hiérarchisation/priorisation de trafic permettant de mettre en œuvre de la QoS (qualité de service) ;
- de redonder ses accès WAN à des fins de haute disponibilité, ou d'améliorer la connectivité jusqu'alors offerte par des solutions MAN/MPLS ;
- de faire évoluer plus facilement son infrastructure WAN suivant ses besoins par l'ajout facilité de nouveaux sites, de bande passante, etc.

En synthèse : le SD-WAN est un type de réseau informatique se basant sur le WAN pour bâtir un réseau virtuel (étendu, agrégé, sécurisé, performant), conçu sur un réseau physique piloté/orchestré centralement, de manière plus souple que des interconnections réseaux historiques (tels que les VPN IPSEC site à site).

2.1.2 CDN

Le CDN (Content Delivery Network) est un réseau de serveurs distribués à maillage global ayant pour finalité de diffuser du contenu Internet plus rapidement et plus efficacement.

Le contenu est stocké « en cache », dans plusieurs serveurs dits POP (Points Of Presence), distribués dans des localisations différentes dans le monde, de manière à réduire la distance entre l'utilisateur et le contenu. Cela se traduit par des temps de chargement plus courts et donc par une meilleure expérience utilisateur.

Au-delà de l'aspect expérience utilisateur, le CDN comporte des avantages du point de vue de la sécurité en jouant le rôle d'intermédiaire entre l'utilisateur et le serveur d'origine, protégeant ainsi le site des attaques DDoS[2] et du trafic malveillant.

2.1.3 SWG

La passerelle web sécurisée (Secure Web Gateway) est un service qui surveille et contrôle l'accès des utilisateurs au web en analysant ce trafic, les applications et les services cloud. L'inspection du trafic web permet de s'assurer qu'il répond aux exigences de sécurité de l'organisation et de filtrer les requêtes malveillantes avant qu'elles n'atteignent leur cible.

En tant qu'intermédiaire entre le client et le serveur, les SWG ont aussi la capacité de déchiffrer le trafic HTTPS. Cette fonctionnalité de déchiffrement nécessite des évaluations préalables au sein de l'organisation en matière de risques et de conformité juridique. Les passerelles web sécurisées réalisent du filtrage d'URL, et de la détection et du filtrage de code malveillant (utilisation de signature d'attaques). Elles peuvent aussi être utilisées pour limiter certaines fonctionnalités d'application web, ou encore pour prévenir la perte de données (DLP). Les passerelles web sécurisées peuvent analyser les mots clés contenus dans une page web et réaliser un filtrage en fonction de la politique de l'organisation ; elles peuvent également bloquer des trafics par catégories de site web, suivant celles maintenues par les éditeurs de solutions.

La complexité liée au déchiffrement dans les solutions traditionnelles perdure au niveau du

[2] Distributed Denial of Service (attaques par déni de service distribué).

SWG (impact sur la performance, angle mort de l'épinglage de certificat, complexité des exclusions, telles que les sites bancaires ou ceux ayant trait à la santé).

L'intégration des SWG dans l'architecture SASE permet de contextualiser l'activité des utilisateurs et des données, afin de mettre en place des règles adaptatives basées sur le risque. L'expérience utilisateur est améliorée en évitant les interdictions générales. De plus, l'intégration des SWG dans le cloud permet de fournir une haute capacité (performance et évolutivité) et une faible latence partout dans le monde (à condition que le SWG soit déployé sous forme distribuée et non sur une instance présente à un seul endroit).

Les SWG peuvent contenir des fonctionnalités de CASB intégrées permettant d'identifier et d'inspecter le trafic des services cloud et des applications, comme détaillé dans le chapitre suivant.

2.1.4 CASB

Le CASB, Cloud Access Security Broker, est une solution de logiciel informatique qui joue le rôle d'un courtier en sécurité d'accès au Cloud. Il s'agit en quelque sorte d'un intermédiaire virtuel qui tend à sécuriser les applications SaaS (Software as a Service / logiciel en tant que service) telles que Slack, Salesforce ou autres, et les applications IaaS (Infrastructure as a Service / infrastructure en tant que service) telles que AWS, Azure ou autres.

Le CASB permet de sécuriser les données de l'organisation de bout en bout depuis le cloud au périphérique et, inversement, que ces données soient statiques ou en mouvement.

Selon les périphériques utilisés, un certain nombre de politiques de sécurité sont établies par l'organisation et appliquées via une plateforme unifiée ou par des agents logiciels installés sur les équipements.

Ces politiques de sécurité sont répertoriées sous la forme de plusieurs services qui sont proposés par les éditeurs de logiciels CASB :

- Alertes sur les menaces de sécurité
- Analyse de comportements
- Contrôle des accès utilisateurs
- Contrôle de conformité sur le fondement des normes et standards avec, par exemple, l'application des politiques de sécurité pour la mise en conformité avec le RGPD
- Détection des menaces
- Surveillance en temps réel et visibilité sur l'utilisation des applications de l'organisation
- Détection du Shadow IT

2.1.5 ZTNA

L'approche Zero Trust Network Access (ZTNA) s'appuie sur les principes Zero Trust[3] et offre à des utilisateurs travaillant de plus en plus fréquemment à distance des facilités de connexion à leur environnement de travail de manière sécurisée. L'utilisateur distant a une connectivité sécurisée à la ressource demandée (une application privée), sans lui donner un accès au réseau ni exposer les applications à Internet.

Cette architecture fonctionne sur un modèle basé sur deux piliers :

Le réseau, premier élément du contrôle des accès :

- Au niveau Firewall ou Next Gen Firewall
- Par identification des adresses IP de sortie dédiées au client et utilisées par les utilisateurs

L'identité, dans lequel la confiance n'est jamais implicite :

- L'accès aux ressources doit être accordé sur le fondement du besoin d'en connaître
- L'accès est accordé sur l'identité et le contexte de l'utilisateur

[3] https://clusif.fr/publications/que-faut-il-savoir-du-zero-trust/

- Le principe du moindre privilège d'accès à la ressource est respecté
- L'accès utilisateur est réévalué continuellement

Le ZTNA est un changement de paradigme par rapport au VPN (Virtual Private Network). Il ne prolonge pas le réseau de l'entreprise vers l'utilisateur, il supprime l'exposition réseau en fournissant un accès applicatif basé sur l'identité, le contexte et une vérification continue. S'il simplifie l'expérience utilisateur et réduit les problématiques de segmentation réseau côté accès distant, il déplace la complexité vers la gouvernance des identités, des politiques d'accès et de la cartographie applicative.

C'est un composant essentiel de la structure de sécurité offerte par SASE. ZTNA et CASB sont notamment en interaction une fois la connexion à une application établie. Une analyse DLP ou de recherche de logiciels malveillants est effectuée, généralement via l'utilisation d'un proxy commun d'inspection du contenu.

Différents modes d'implémentation existent, soit sous forme de « portail des applications », soit en mode reverse proxy, avec ou sans agent, pour prendre en compte le BYOD (Bring Your Own Device).

2.1.6 Next-Generation Firewall (NGFW) / Firewall as a Service (FWaaS)

Ces termes décrivent deux aspects différents d'un pare-feu – ce qu'il peut faire (NGFW) par rapport au lieu et à la manière dont il est déployé (FWaaS). Les FWaaS peuvent avoir des capacités de nouvelle génération, et un NGFW peut être hébergé dans le cloud.

Le NGFW a été introduit il y a plus de dix ans par le rapport Gartner, qui le définit comme un « pare-feu d'inspection approfondie des paquets qui va au-delà du blocage des adresses IP et des ports pour ajouter : l'inspection de la couche application, la prévention des intrusions et l'apport de renseignements depuis l'extérieur du pare-feu ».

Le FWaaS permet de simplifier l'infrastructure informatique des pare-feux tout en conservant leurs capacités de protection historiques. Parmi les avantages, on compte une gestion centralisée des pare-feux et l'absence d'interruption pour le déploiement des correctifs. Le FWaaS aide également les organisations à appliquer des politiques cohérentes, quelle que soit la localisation des infrastructures.

2.1.7 DLP

La prévention contre la perte ou fuite de données (Data Loss/Leak Protection/Prevention) est un ensemble de mesures et de processus utilisés pour s'assurer que les données sensibles ne sont pas perdues, mal utilisées ou consultées par des utilisateurs non autorisés.

La démarche de protection s'articule autour de trois axes :

1. IDENTIFIER les données pour les protéger contre les fuites
2. SURVEILLER les canaux de fuite de données
3. AGIR pour éviter les fuites de données

Dans cette démarche, on doit distinguer trois types de données :

1. Les données en cours d'utilisation : données auxquelles un système accède ou qu'il utilise à un moment donné. Il peut s'agir de données en mémoire temporaire, d'un rapport ouvert ou d'une requête en cours d'exécution sur un poste de travail, d'un fichier en cours de copie sur une clé USB.
2. Les données au repos : données stockées dans l'infrastructure informatique et sur des supports. Les données au repos peuvent également être stockées à l'extérieur auprès de tiers ou par le biais d'extensions externes de l'infrastructure informatique, telles que le stockage en nuage.
3. Les données en mouvement : données en transit, circulant sur les réseaux.

Les outils de prévention de perte de données actuels proposent des mesures de sécurité déclinées autour des trois axes décrits précédemment :

- Identifier : ils classent les données et identifient les violations des politiques. Certaines politiques sont motivées par des exigences de conformité réglementaire.
- Surveiller : ils contrôlent les activités des terminaux, surveillent les réseaux d'entreprise et supervisent les données dans le cloud pour générer une alerte en cas de fuite de données. Ils peuvent aussi fournir des rapports pour répondre aux exigences de conformité et d'audit et identifier les zones de faiblesse et les anomalies pour l'investigation numérique et la réponse aux incidents.
- Agir : ils permettent aussi d'appliquer des mesures préventives (chiffrement, blocage d'envoi de données) ou correctives (filtrage des flux de données). Ceci permet d'empêcher les utilisateurs de partager accidentellement ou de façon malveillante des données susceptibles de créer des risques pour l'organisation.

2.1.8 RBI

Le RBI (Remote Browser Inspection) est une fonctionnalité permettant d'isoler le navigateur du client des codes, des scripts et des charges utiles hautement malveillants qui s'exécutent automatiquement lors de l'accès à la page web. Elle permet notamment de lutter contre l'exploitation des vulnérabilités ciblant les navigateurs. Le RBI peut être vu comme une fonctionnalité avancée du SWG.

Ainsi, cette technologie empêche les infections causées par des logiciels malveillants et d'autres cyberattaques d'affecter les appareils des utilisateurs (et par voie de conséquence les réseaux internes du client) en bloquant l'exécution de codes et de scripts potentiellement malveillants sur le navigateur de l'utilisateur.

Principe de fonctionnement : rupture de flux et bac à sable

- Il s'agit d'un principe de rupture de flux entre le site web et le navigateur du client, via la mise en place d'un navigateur virtuel géré par l'offre SASE, qui retransmet au client uniquement le flux « désinfecté » (exempt de menaces) ; tout le trafic est soumis à inspection de sécurité.
- Un environnement de type bac à sable dans lequel le contenu et le code programmatique du site web consulté sont testés et vérifiés afin d'identifier les attaques de type « zero-day » et d'autres attaques répandues, telles que la publicité malveillante, le détournement de clics, les attaques de redirection, les attaques de navigateur par chemin d'accès, les XSS, etc.

Les téléchargements malveillants sont neutralisés et supprimés avant d'être exécutés sur l'appareil distant.

- Étant donné qu'aucune exécution de code local ne se produit sur l'ordinateur de l'utilisateur, ce dernier est protégé contre les sites web malveillants.
- Les utilisateurs sont en sécurité, quelle que soit la source, puisque les URL sont automatiquement ouvertes dans le navigateur web isolé, qu'il s'agisse de pages web, d'e-mails, de documents, de messageries sociales ou de liens reçus par SMS.
- Les publicités malveillantes et les traqueurs indésirables sont automatiquement bloqués. Pour les publicités légitimes, elles s'affichent en protégeant le point de terminaison distant.

En résumé, et pour l'essentiel, le RBI est un composant important d'une offre SASE permettant aux organisations de fournir un accès Internet « sécurisé » sans avoir à s'inquiéter de la compromission des navigateurs et des appareils des utilisateurs par des codes malveillants sur les sites web, cela en éliminant la plus grande partie des menaces pesant sur les navigateurs.

2.1.9 DNSS

Attention à ne pas confondre DNSSEC (qui correspond à des fonctions de sécurité appliquées au protocole DNS) avec DNSS (qui signifie « DNS Security »). DNSS est généralement utilisé pour définir les mesures prises pour protéger l'infrastructure DNS d'une organisation au sens large du terme. Il englobe aussi bien les serveurs DNS internes sur lesquels les utilisateurs finaux viennent effectuer des requêtes en tant que clients, que les DNS externes (faisant autorité) sur lesquels le monde extérieur vient effectuer des requêtes sur les domaines gérés par et/ou sous la responsabilité de l'organisation.

L'avantage d'intégrer le DNS dans la sécurité globale de l'entreprise réside dans le fait qu'il est généralement le premier élément utilisé par les clients internes de l'organisation, cela aussi bien pour des applications internes que pour les sites et/ou applications externes. En ce sens, on peut dire qu'il sert de premier rempart dans la sécurité d'une infrastructure. Le protocole étant utilisé en standard sur l'ensemble des équipements clients et les serveurs DNS supportant nativement la synchronisation de données, il est assez simple de généraliser la sécurité à toute l'organisation. Par sa place privilégiée dans le contrôle des flux sortants, le DNSS est souvent directement intégré au sein du service SWG chez des éditeurs.

Ci-après une liste non exhaustive des fonctionnalités de sécurité disponibles au travers d'un ou plusieurs proxys DNS :

- Contrôle d'accès et filtrage pour empêcher l'accès à des sites spécifiques et/ou avec une mauvaise réputation
- Contrôle d'intégrité et authentification des réponses DNS (en utilisant le protocole DNSSEC)
- Amélioration de la confidentialité (en évitant la divulgation des IP des clients DNS grâce à la centralisation de l'ensemble des requêtes DNS effectuées au sein de l'organisation)
- Protection contre les différents types d'attaques DNS (déni de service, exploits utilisant le protocole DNS, etc.)
- Identification d'activité anormale, d'attaques en cours et/ou d'indicateurs de compromission (DNS tunneling, serveurs DNS compromis en amont, etc.)
- Journalisation des requêtes DNS (facilite l'analyse en cas de nécessité)

Pour résumer, avec le DNSS on peut réaliser à la fois de la détection de menaces (inspection des paquets, réputation des domaines) et du contrôle des accès réseau (initiés via le DNS), cela sur l'ensemble des périphériques d'une organisation, et ce, quels que soient leur type et leur localisation (au sein ou à l'extérieur des bureaux). Cette facilité de mise en place et de maintenance fait souvent du DNSS un choix privilégié comme brique de départ d'une solution SASE.

2.2 Composants supplémentaires

Certains éditeurs de SASE commencent à proposer des briques supplémentaires pour étendre les capacités de leurs solutions, notamment pour :

- **mieux contrôler ses environnements cloud**, que ce soit en mode cloud native (IaaS, PaaS) ou application (Saas) via des contrôles les plus continus possibles au niveau control plane ou data plane et des actions de remédiation ;
- **protéger ses terminaux** (postes de travail, mobiles, serveurs physiques ou VM), en tentant de détecter les menaces au plus tôt et de manière transverse sur les SI de l'organisation, mais aussi de proposer des capacités de remédiation immédiate (isolation, etc.).

Contrairement aux composants cœur, tous les acteurs du SASE ne proposent pas encore forcément ces éléments dans leur offre.

2.2.1 CNAPP

Les solutions de sécurité du cloud évoluent depuis plusieurs années pour compléter la vision de conformité apportée par les CSPM avec une approche de détection & réaction en « temps continu ». Ces nouvelles solutions portent le nom de **Cloud Native Application Protection Platform** (CNAPP).

Elles regroupent tout ou partie des fonctionnalités de sécurité et de conformité qui seront vues ci-dessous et notamment : CSPM[4], CWPP[5], CIEM[6], parfois également sécurité des pipelines de développement (analyse de code, dépendances, etc.).

2.2.2 CSPM

Une plateforme de Cloud Security Posture Management (CSPM) est une solution visant à identifier les risques relatifs aux infrastructures cloud (IaaS, PaaS...) et à aider les équipes à construire une posture de gestion de ces risques.

Un CSPM analyse de manière régulière (tous les jours, x heures, etc.) les configurations des environnements cloud en cartographiant les ressources pour détecter des défauts d'accès, de configurations ou des vulnérabilités identifiées, et donner une vision des assets et workloads présents.

Les éléments peuvent généralement être consolidés dans une vision orientée risque ou orientée conformité par rapport à un référentiel existant (par exemple, les CIS Benchmarks), une réglementation (RGPD, HIPAA[7]…) ou des normes industrielles, et ainsi identifier si les politiques de sécurité et les contrôles sont correctement mis en œuvre.

Un CSPM recommande des actions de remédiation et peut, dans certains cas, les exécuter en mode automatique ou à la demande des utilisateurs. Il s'adresse typiquement aux équipes en charge des environnements cloud et fonctionne généralement en mode multicloud pour donner une vision la plus globale possible. Il est généralement sans agent, en allant chercher les informations directement depuis les API des fournisseurs cloud, et n'offre donc pas de vision de sécurité continue.

Un CSPM peut contribuer fortement à la maîtrise des environnements cloud. Il s'intègre dans les processus DevSecOps en donnant une vision de la sécurité des environnements déployés.

---

[4] Cloud Security Posture Management.

[5] Cloud Workload Protection Platform.

[6] Cloud Infrastructure Entitlement Management.

[7] Health Insurance Portability and Accountability Act.

2.2.3 SSPM

Une plateforme de SaaS Security Posture Management (SSPM) porte les mêmes objectifs qu'un CSPM, mais en étant dédiée aux applications SaaS :

- elle s'intègre généralement aux applications via API ;
- elle diffère des CASB en apportant une vision globale et, autant que possible, une prévention des défauts de configuration plutôt qu'une surveillance des accès.

La complexité de la mise en œuvre d'un SSPM est souvent liée à l'aspect propriétaire des applications SaaS et la nécessité de mettre en place des modules spécifiques pour chaque application.

CSPM et SSPM peuvent être complémentaires et utilisés ensemble pour une gestion de la sécurité et de la conformité globale dans le cloud (IaaS, PaaS, SaaS).

2.2.4 CWPP

Une plateforme de protection des charges de travail cloud (CWPP – Cloud Workload Protection Platform) est une solution de sécurité qui surveille et détecte en continu les menaces ciblant les *charges de travail* exécutées dans le cloud.

Elle peut permettre de détecter des vulnérabilités, des pertes d'intégrité, des configurations dangereuses, des malwares, des activités malveillantes sur le plus grand nombre possible de *charges de travail* sur différents environnements cloud ou hybrides.

Une *charge de travail* est un actif chargé d'accomplir une tâche au sein des environnements d'exécution. Par exemple, des tâches de type DevOps comme le CI/CD (Continuous Integration/Continuous Delivery) ou du code exécuté sur des machines virtuelles ou containers hébergés dans le cloud, voire simplement des instructions lowcode, nocode.

Contrairement au CSPM, le CWPP travaille donc directement au sein des *charges de travail* et s'appuie souvent sur un agent ou un micro-agent.

2.2.5 CIEM

Une plateforme de gestion des droits sur l'infrastructure cloud (CIEM – **Cloud Infrastructure Entitlement Management**) est une solution de protection du cloud centrée sur l'identité.

Elle assure la gestion des risques liés à l'accès au cloud, au moyen de contrôles ou de surveillance des permissions et des activités au regard de ces permissions.

Elle cherche ainsi à détecter des abus de permissions (utilisateur ou machine, ressource stable ou éphémères), des erreurs de configuration (accès trop permissifs…) et à donner une visibilité globale.

2.2.6 WAAP

Une solution de **Web Application and API Protection** (WAAP) est une plateforme de protection des applications exposées sur Internet et des interfaces de programmation (API). Elle vise à sécuriser les services accessibles publiquement contre les attaques applicatives, telles que les injections, le cross-site scripting, l'exploitation de vulnérabilités connues, les abus d'API ou encore les attaques automatisées (bots).

Le WAAP regroupe généralement plusieurs capacités historiquement distinctes : pare-feu applicatif (WAF), protection des API, mécanismes de lutte contre les bots, et, parfois, protection contre les attaques par déni de service de couche applicative. Il s'appuie sur des analyses comportementales, des signatures, des modèles d'apprentissage et des flux de threat intelligence, afin de détecter des usages anormaux ou malveillants.

Contrairement aux briques de type SWG ou ZTNA centrées sur la sécurisation des accès des utilisateurs, le WAAP protège les applications elles-mêmes lorsqu'elles sont exposées à Internet, indépendamment de l'origine des requêtes. Il constitue ainsi une brique complémentaire

dans une architecture de sécurité globale, en particulier dans les environnements fortement orientés cloud et API.

2.2.7 EDR, NDR et XDR

Les **Endpoint Detection and Response** (EDR) sont des solutions qui surveillent et centralisent les événements de sécurité depuis des terminaux (postes de travail, serveurs, VM, voire téléphones mobiles ou tablettes…), proposent des mécanismes de détection des anomalies et incidents, et permettent une remédiation automatique ou (plus raisonnablement) semi-automatique lorsque cela est possible (depuis la mise en quarantaine d'un fichier ou l'arrêt d'un flux jusqu'à l'isolation du poste).

Contrairement à un antivirus, un EDR ne travaille pas qu'avec des signatures ou des méthodes heuristiques, mais met en œuvre des mécanismes plus avancés d'identification des anomalies (par exemple, comportementales) et des liaisons avec des sources de *Threat Intelligence*.

L'EDR, par nature, ne traite que les signaux provenant des agents installés.

Les EDR s'intègrent souvent dans des suites de protection plus vastes, couvrant également des fonctionnalités antivirales classiques, de protection contre les menaces, voire de détection des vulnérabilités ou des défauts de configuration sur les terminaux ou sur le réseau environnant.

Les **Network Detection and Response** (NDR) assurent les mêmes fonctionnalités qu'un EDR, mais au niveau réseau. Sur un LAN traditionnel, ils se placent en écoute passive derrière un ou plusieurs ports de switch ou derrière des TAP. En environnement cloud, ils peuvent potentiellement s'interfacer avec les modules de gestion des flux. Leur capacité de réponse se fait généralement par interfaçage avec des solutions de filtrage actives (firewall, par exemple).

On parle également de Network Traffic Analysis (NTA), en particulier lorsque les fonctions de remédiations (par nature délicates à implémenter sur un cœur de réseau pour ne pas risquer de perturber le fonctionnement normal de l'entreprise) ne sont pas mises en avant.

L'**Extended Detection and Response** (XDR) est une solution de détection et de réponse aux incidents de cybersécurité qui étend le périmètre de l'EDR pour y inclure le réseau, les annuaires (Active Directories), les outils cloud, les firewalls, les services protégés par un CSPM, etc.

Elle doit intégrer nativement diverses fonctionnalités de sécurité dans un système opérationnel cohérent qui unifie les composants [source Gartner] et qui s'adapte aux enjeux issus de la cartographie des risques. Ses actions corrélées sont donc la promesse de « *tout voir, tout faire, partout* ».

L'objectif de l'XDR est donc l'identification des menaces, notamment complexes, depuis de multiples vecteurs, car il dispose :

1. de diverses capacités de détection (antivirus sur signature, next-gen antivirus sans signature, anti-exploit, anti-ransomware, fileless prevention, vision globale, etc.) ;
2. de sources de Threat Intelligence ;
3. de capacités de détection, voire de corrélation entre sources.

Il doit également permettre d'augmenter la vitesse de réaction via des mécanismes automatiques ou, plus raisonnablement, semi-automatiques, par exemple pour isoler plus vite une menace (isolation de poste, d'utilisateur, suppression de droits d'accès sur les fichiers utilisateurs, coupure des flux, etc.).

En étendant le périmètre de l'EDR, le XDR donne donc une vision globale et sécurise plus en amont et en aval des terminaux. Au niveau des firewalls, il peut par exemple détecter et bloquer les flux provenant de serveurs réputés malicieux. En agissant au niveau des NGAV, il permet également de bloquer un malware présent sur le SI avant que l'attaque ne se déclenche. Enfin, le XDR détecte et atténue les menaces plus tôt dans le cycle (kill chain) en intégrant des outils de supervision e-mail ou DNS.

À ce jour, les composants EDR, NDR, XDR ne sont pas ou très peu inclus dans les approches SASE des éditeurs. Pour autant, les éditeurs de ces solutions tendent à vouloir consolider les fonctions de sécurité (endpoint, cloud, identités, accès…) et pourraient ainsi rejoindre peu à peu les acteurs du SASE (hors fonctionnalités de SD-WAN).

3 Correspondance entre fonctionnalités et composants

Ci-après quelques exemples de fonctionnalités mis en correspondance avec les composants associés, certains étant potentiellement optionnels, ces derniers étant désignés par (X) :

	SD-WAN	**CDN**	**SWG**	**CASB**	**ZTNA**	**NG-FW/ FWaaS**	**DLP**	**RBI**	**DNSS**
Sécurisation de l'accès Internet pour les utilisateurs distants			X		(X)	X		(X)	(X)
Interconnexion des sites distants via Internet	X				X	X			
Sécurisation de l'accès aux applications SaaS/On-Premise depuis des équipements gérés		(X)		X	X	X	(X)		(X)
Sécurisation des accès aux applications de l'organisation depuis des équipements non gérés				X	X		(X)		(X)

4 Bénéfices/Risques

4.1 Les bénéfices

4.1.1 Capacité d'évolutivité

La mise en œuvre d'une solution SASE est un projet d'architecture intégrant à la fois l'infrastructure réseau et l'infrastructure sécurité, se prêtant bien à un déploiement progressif.

À terme, l'infrastructure réseau et sécurité est consolidée, homogénéisée, centralisée. Il est alors plus aisé d'apporter des changements aux capacités du réseau et aux interconnexions (ajout de sites, connectivité des nomades, intégration de nouveaux clouds, etc.), tout en maintenant la même couverture de sécurité.

En résumé, une solution SASE offre une excellente capacité de mise à l'échelle.

4.1.2 Centralisation

Le SASE offre une capacité de gestion centralisée, d'orchestration et d'harmonisation des politiques de sécurité. La réduction du nombre de composants d'infrastructure et de leur disparité permet de simplifier l'administration.

Cette architecture offre une meilleure visibilité, notamment une meilleure gouvernance avec un degré de précision et de maîtrise de l'accès amélioré.

Le SASE permet aussi de contrôler plusieurs solutions cloud (multicloud) et d'avoir une cartographie de tous les services gérés à travers celui-ci.

Le fait de centraliser une solution peut représenter un risque de résilience. Il faudra s'assurer d'avoir une redondance et la tester afin de bénéficier d'une reprise en cas d'incident.

4.1.3 Modèle de sécurité

L'unification d'un ensemble de composants sécurité (ZTNA, CASB, SWG, NG-FW...) permet de passer d'un modèle de sécurité périmétrique à un modèle « Zero Trust » basé sur l'identité et la posture de sécurité des terminaux, très adapté aux usages actuels (cloud, nomadisme, BYOD…).

4.1.4 Disponibilité et performances réseau

Une solution SASE, par ses fonctionnalités SSE/SD-WAN précédemment évoquées, permet de mettre en œuvre une résilience forte des accès WAN (par ex. : plusieurs opérateurs Internet sur chaque site) et d'améliorer de fait la disponibilité de l'accès à l'infrastructure SASE et aux ressources qu'elle protège. Cette disponibilité est également liée au nombre de points de présence « proches » de l'éditeur, pour l'accès à l'infrastructure SASE.

Les éditeurs SASE proposent également des Service Level Agreement (SLA) souvent élevés permettant de s'assurer de la disponibilité permanente de l'infrastructure (par ex. : 99,999 % de disponibilité engage le fournisseur à moins de 6 minutes de temps d'arrêt par an).

Les éditeurs portent une attention particulière à la qualité de la connectivité par l'optimisation et/ou la surveillance des connexions au SASE, l'objectif final étant d'améliorer l'expérience utilisateur pour l'accès aux ressources protégées.

Les améliorations de performance sont mises en œuvre, sous réserve d'une bonne adéquation entre les points de présence du fournisseur et des besoins clients, et sous réserve que l'éditeur SASE mette en œuvre des fonctionnalités techniques pouvant améliorer la performance (QoS, cache, optimisation via agent, etc.). Il est important de noter que seuls les éditeurs disposant de leurs propres backbones inter-POPs (hors Internet) peuvent se prévaloir de maîtriser leurs

SLA de connectivité de bout en bout (débit, latence, etc.).

Ces optimisations doivent cependant prendre en compte les exigences métier liées au niveau de protection, de débit affecté ou de temps de latence escompté par l'application, afin d'aligner les besoins. Sans ces éléments, parfois complexes à définir et à implémenter techniquement, les mesures de sécurité peuvent se retrouver inefficaces, voire dégradées, tout comme les performances réseau.

4.1.5 Adaptabilité des coûts

Du fait de son architecture orientée cloud, le SASE transforme la quasi-totalité des coûts OPEX et CAPEX locaux en OPEX cloud, à l'exception des solutions qui nécessitent des équipements de terminaison sur site.

Ceci, combiné à la flexibilité de gestion (telle que l'allocation dynamique de bande passante pour une période définie, la suspension temporaire d'un site, l'activation ou désactivation d'un service de sécurité optionnelle, etc.), généralement permise depuis la console de supervision, amène une souplesse nouvelle dans le monde du réseau.

Cette flexibilité opérationnelle s'accompagne, selon les offres, d'une gestion dynamique des coûts, offrant ainsi au client un meilleur contrôle (tout en restant conscient de la dépendance associée, voir chapitre « Dépendances au fournisseur »).

4.1.6 Transfert de risque

Les solutions SASE sont par nature fortement, voire totalement, dans le cloud, ce qui revient, dans un grand nombre de cas, à externaliser un ensemble de prestations auparavant réalisées en interne.

De fait, une grande partie des risques est naturellement transférée vers le ou les éditeur(s) choisi(s).

Il est alors essentiel de porter une attention particulière aux conditions contractuelles et aux engagements de service de l'éditeur, afin de vérifier leur alignement avec la matrice de gestion des risques, qu'il faudra réviser en conséquence.

4.2 Risques

4.2.1 Réversibilité

Le regroupement de l'ensemble des fonctions de réseau et de sécurité dans l'offre SASE par un seul fournisseur de services nécessite une vigilance accrue sur les conditions de réversibilité :

- À la fin du contrat, la migration des données et des politiques de sécurité vers d'autres éditeurs implique la reprise de l'ensemble des services de l'offre, ce qui peut induire une forte complexité, en raison notamment du risque de perte de corrélation entre les différentes briques de sécurité.
- Les clauses de réversibilité des contrats proposés dans le cadre des offres SASE doivent donc être étudiées avec attention pour éviter de se retrouver dans une situation de « client captif ».

Il est important de s'assurer que l'ensemble des configurations de la solution SASE soient exportables via des services dans un format standard (type json ou csv). La plupart des éditeurs sont en mesure, moyennant des journées de services, d'analyser, de convertir et d'intégrer tout ou partie des éléments de configuration dans la solution cible.

L'usage de déploiement automatisé (IaC : Infrastructure as Code) est également une bonne pratique pour faciliter la réversibilité.

4.2.2 Dépendance au fournisseur

Le regroupement des services réseau et sécurité chez un seul fournisseur entraîne une dépendance aux difficultés qu'il peut rencontrer, telles qu'une panne de tout ou partie de l'infrastructure ou même la faillite de ce dernier.

Cette dépendance peut aussi se révéler problématique si le fournisseur ne fait pas évoluer son offre dans le sens des besoins du client ou impose une évolution démesurée de ses tarifs.

Le SASE n'implique pas une obligation absolue d'être lié à un fournisseur unique, mais cela permet la simplification de la gestion centralisée des opérations, notamment en cas d'attaque cyber.

Pour réduire ce risque, il peut être envisagé de séparer les services sur plusieurs éditeurs, par exemple SD-WAN séparé du SSE. Cela permet de réduire la dépendance et les risques associés, au détriment de la console unifiée et de certaines automatisations, et, dans un certain sens, du concept SASE.

Pour les plus ambitieux, il peut être envisageable de créer une console d'administration interopérable qui pilotera les services de plusieurs fournisseurs au travers de connecteurs (API). En revanche, ce chantier, si envisagé, ne doit pas être pris à la légère, car il nécessitera des ressources conséquentes disponibles sur la durée.

4.2.3 Réglementaire

En fonction de la nationalité du fournisseur, certaines réglementations peuvent s'appliquer. Par exemple, un fournisseur de SASE américain sera soumis au Cloud Act qui peut contraindre le fournisseur de services à fournir les données stockées sur des serveurs, qu'ils soient situés aux États-Unis ou à l'étranger.

Par ailleurs, le choix de la localisation géographique des points de présence (POPs) doit également être fait avec prudence pour éviter les risques d'ingérence étatique.

Selon le référentiel SecNumCloud de l'ANSSI, la qualification du fournisseur SASE permettrait d'assurer que le fournisseur suit un haut niveau d'exigence, aussi bien au niveau technique, qu'opérationnel ou juridique (conformité avec le droit européen). À noter qu'en 2025, parmi les leaders du marché, il ne figure aucune société européenne.

4.2.4 Exposition accrue aux attaques cyber

L'utilisation de solution cloud entraîne de facto une augmentation de la surface d'exposition. Néanmoins, de manière plus générale, les éditeurs de solution SaaS sont bien conscients de ce risque et consacrent un effort important à la sécurité de leur application (leur réputation et, de fait, leur modèle économique, étant en jeu).

Les solutions SASE sont d'autant plus sensibles qu'elles permettent de gérer le cœur de la sécurité et des accès réseau d'un système d'information. Il est ainsi d'autant plus indispensable de doter les interfaces d'administration des solutions SASE de mesures de sécurité supplémentaires pour éviter tout risque de compromission (authentification multifacteur, limitation des accès aux interfaces d'administration à un nombre restreint de réseaux ou d'adresses IP, etc.).

De plus, le fournisseur SASE doit garantir une sécurité intrinsèque irréprochable, couvrant la disponibilité, l'intégrité et la confidentialité. En effet, toute compromission de sa part entraînerait des conséquences critiques pour ses clients.

4.2.5 Difficulté de comparaison

La complexité technique et la diversité de l'offre SASE rendent difficile la comparaison des fournisseurs, tant sur le plan des fonctionnalités que des offres tarifaires. De plus, la terminologie utilisée varie en fonction des fournisseurs, ce qui n'arrange rien.

Il est essentiel d'analyser l'origine des technologies qui composent l'offre SASE de chaque éditeur (réseaux ou sécurité), ainsi que l'angle sous lequel ils conçoivent ou intègrent leurs fonctionnalités. Cette approche permet d'évaluer la couverture et la maturité de leur solution. En effet, certains éditeurs privilégient l'acquisition de technologies existantes, mais leur intégration n'est pas toujours homogène, ce qui peut impacter la cohérence de l'offre.

4.2.6 Complexité d'implémentation

La migration vers une offre SASE peut s'avérer complexe sur plusieurs axes.

D'abord sur les aspects techniques, notamment :

- Refonte du réseau et des équipements de sécurité
- Déploiement des agents
- Réadaptation des politiques
- Réorganisation de la gestion des identités
- Réécriture de la documentation opérationnelle (procédures, etc.)
- Prévision des impacts métier

À noter que la complexité d'implémentation dépendra directement de la taille du SI et du degré d'hétérogénéité de l'existant. Par exemple, l'ajout de l'agent SASE en cohabitation avec d'autres agents existants (i.e. : EDR/XDR) peut ralentir les postes utilisateurs, créer des conflits, complexifier le diagnostic et surcharger les équipes support.

D'autre part, la complexité est aussi humaine, l'organisation doit évoluer en rapprochant les équipes réseau et sécurité ; les utilisateurs vont devoir s'adapter à un nouveau mode de fonctionnement. (Cela est détaillé dans le chapitre suivant « Gestion du changement ».)

Afin de simplifier le déploiement, il est recommandé d'effectuer la migration progressivement en fonction de la facilité d'implémentation, des risques identifiés et enfin des contrats en cours (fin de contrat, expiration de licences, etc.).

Par ailleurs, il faut être bien conscient qu'un planning de déploiement SASE se déroule généralement sur plusieurs années.

4.2.7 Gestion du changement

Afin d'anticiper et de minimiser la résistance au changement, il est important d'impliquer dès le départ les équipes réseau et les équipes sécurité dans le projet SASE.

Par ailleurs, afin de faciliter la communication entre ces mêmes équipes, il est important de se mettre d'accord sur un vocabulaire commun et d'assimiler les termes spécifiques du SASE.

Un projet SASE nécessite l'établissement d'une feuille de route commune réseau et sécurité pour une meilleure collaboration, en complément d'une coordination efficace avec les métiers.

Pour minimiser les effets secondaires potentiels d'un projet de cette envergure et prévenir d'éventuels mécontentements, une communication claire et une formation adaptée des utilisateurs de la DSI et métier sont essentielles.

4.2.8 Partage des responsabilités

Comme pour tout déploiement de projet cloud, la sous-traitance redéfinit le partage des responsabilités entre le client et le prestataire.

Dans le cadre d'un projet SASE, ce partage peut engendrer des failles de sécurité et des impacts opérationnels majeurs si les rôles ne sont pas clairement définis. En effet, une erreur de configuration, une réponse inadéquate aux incidents ou une absence de redondance peuvent compromettre la continuité des activités.

Les contrats doivent préciser clairement les engagements du fournisseur en matière de surveillance, de gestion des incidents et de reprise d'activité. Il est conseillé de valider avant contractualisation, lors d'un pilote, les impacts d'un fonctionnement sans tout ou partie de la solution SASE.

Il paraît important, pour pallier les éventuelles pannes du SASE et assurer la continuité d'activité, d'intégrer au projet l'étude de scénarios de sinistres et des solutions de contournement adaptées.

Enfin, une gouvernance claire et une matrice RACI garantiront une réponse coordonnée et efficace en cas de crise.

4.2.9Temps de réponse

Certains facteurs, tels que la localisation et le type de connectivité, influent fortement sur les temps de réponse du réseau avec un impact sur les performances solutions.

En effet, certains fournisseurs possèdent leurs propres infrastructures et sont donc théoriquement plus à même de contrôler les performances de bout en bout. Les points de présence utilisent parfois une connectivité passant par Internet plutôt que des liaisons dédiées, ce qui empêche le contrôle de la latence et donc des temps de réponse.

Dans le cas d'applications sensibles à la latence, il est d'autant plus important de prendre en compte les délais de réponse dès la phase d'étude des solutions.

Enfin, le diagnostic lié à des lenteurs peut s'avérer difficile sans solution de surveillance de la performance réseau de bout en bout (poste et lien utilisateur compris). Ce module est parfois embarqué au sein du SASE sous le nom de DEM (Digital Experience Monitoring) qui permet de faire des analyses poussées et de générer des rapports.

4.2.10 Dépendance aux composants du SI hors SASE

Le SASE s'intégrant fortement avec le SI, il va s'appuyer sur des composants existants de ce dernier (DNS, fournisseur d'identité, etc.). Dans certains cas, ils peuvent devenir des points de dépendance critiques.
Par exemple, le module ZTNA opère une bascule fondamentale : la décision d'accès n'est plus basée sur le réseau, mais sur l'identité et le contexte.

En cas de panne, d’erreur de configuration ou de compromission du fournisseur d’identité (IdP), les utilisateurs perdent l’accès à toutes les ressources protégées par le SASE (interne avec le ZTNA, ou externe avec le SWG).

5 Proposition d'approche pour choisir sa solution SASE/SSE

L'objectif de ce chapitre est d'aider à poser les bonnes questions et avoir des éléments d'analyse pour choisir son éditeur déclinant le modèle SASE/SSE.

5.1 Infrastructure

Questions	Proposition d'analyse
Infrastructure serveurs en propre ou managée par un tiers (si tiers, merci de préciser) ?	La gestion d'un composant de l'infrastructure en propre permet une maîtrise de celui-ci et l'absence de dépendance à un tiers (ou permet en tout cas d'aller au-delà du respect d'engagements contractuels avec des sous-traitants). Le fait de posséder l'ensemble des composants en propre peut permettre de garantir un excellent niveau de service (disponibilité, latence, etc.) sur l'ensemble de la chaîne, ainsi que de répondre plus facilement aux problématiques réglementaires et de souveraineté. Point d'attention : est-ce que l'infrastructure réseau inter-POPs est basée sur un réseau privé (WAN) indépendant d'Internet (cela pouvant avoir un impact notable sur la latence) ? IPv 6 est-il supporté ?
Infrastructure réseau « Core » en propre ou managée par un tiers (si tiers, merci de préciser) ?	
Infrastructure réseau « POPs » en propre ou managée par un tiers (si tiers, merci de préciser) ?	
Nombre de POPs et fonctionnalités rattachées (avec détail par région [Amérique du Nord, Amérique latine, EMEA, APAC]) ?	Le nombre de points de présence est important pour permettre une haute disponibilité, une faible latence en fonction de la localisation des sites et/ou des utilisateurs. Cela permet aussi d'améliorer la résilience d'accès à l'infrastructure SASE. S'assurer que les POPs réalisent directement les opérations de calculs (i.e. : CASB) ou, à défaut, que la redirection soit faite vers un POP relativement proche.

5.2 Composants proposés par l'éditeur

Questions	Proposition d'analyse

Quels sont les composants couverts par la solution ?
 	
Ci-après une liste « de base » à date :
• SD-WAN
  ○ WAN Optimization / SaaS Acceleration
  ○ Quality of Service
  ○ Routing
  ○ Dynamic Path Selection
• CDN *(Content Delivery Network)*
• SWG *(Secure Web Gateway)*
• CASB *(Content Access Broker)*
• ZTNA *(Zero Trust Network Access)*
• NG-FW / FWaaS *(Next Generation Firewall / Firewall as a Service)*
• DLP *(Data Leak/Loss Protection)*
• RBI *(Remote Browser Isolation)*
• DNSS *(DNS Security)*
	Certains éditeurs ne couvrent qu'un périmètre limité des composants SASE, il est donc important de s'assurer que les fonctionnalités qui correspondent à vos besoins métier soient couvertes.

5.3 Intégration (Endpoints/Appliances…)

• La solution nécessite-t-elle l'installation d'un agent pour tout ou partie des composants ? • Comment sont gérés les endpoints non managés (BYOD) ? • La solution nécessite-t-elle l'installation d'appliances physiques sur les sites ? • Quels sont les flux déchiffrés par la solution ? Comment le déchiffrement est-il réalisé ? Quelle granularité ?	Définir la stratégie relative aux agents (sans agent, restriction sur le nombre d'agents installés, certification/qualification des agents). Vérifier pour chaque composant ou service si l'agent est obligatoire, ainsi que les différents types de endpoints couverts (PC, MAC, smartphones, etc.). Il est également intéressant de savoir comment le primodéploiement de l'agent doit être réalisé (tant pour les postes maîtrisés que pour le BYOD) et comment les mises à jour de l'agent sont réalisées (tant pour le logiciel que pour la configuration de l'agent). Demander des schémas détaillés de l'architecture de connexion vers l'infra de l'éditeur montrant les appliances (physiques ou virtuelles), les agents, les URL/IP/ports de connexions et le rôle de chacun des équipements ou composants commercialisés par l'éditeur. Pour le déchiffrement, demander quels flux sont déchiffrés (https, ftps, ssh, etc.), par quelles ressources (agents, appliances, etc.), et quel est le degré de paramétrage du déchiffrement sur le périmètre (source, destination, protocole, port, application, etc.) ou sur la sécurité (gestion des certificats racines, suites de chiffrement) ? Vous devez pouvoir décider suivant votre politique de déchiffrement (penser notamment, pour le surf web qui transite via l'infra SASE, à ne pas déchiffrer les sites de type santé, etc.).

5.4 Administration

Questions	Proposition d'analyse
• La solution est-elle ouverte et pilotable via une API sécurisée ? Si oui, quelle est la couverture (notamment SOAR et administration…) ? • La console d'administration est-elle réellement unifiée ou s'agit-il de multiples consoles accessibles en SSO ? • Est-il possible de créer des zones d'administration restreintes au sein de la même console (i.e. : accès uniquement à l'administration d'un pays sans voir les autres) ?	La solution permet-elle une interconnexion fluide avec mes outils existants ? Sera-t-il facile de l'intégrer dans mes processus existants et d'adapter les permissions avec l'organisation des équipes opérationnelles ?

5.5 Ouverture / Interopérabilité

Questions	Proposition d'analyse
• Quel est le degré de maturité de la solution en matière d'interopérabilité (avec des composants d'autres éditeurs SASE) ? • Quelles sont les possibilités d'intégrations/interactions avec des composants existants du SI (i.e. : IdP, IAM, SCIM, SIEM, EDR/XDR…) ?	La solution s'intègre-t-elle à mon écosystème ? Il s'agit de s'assurer qu'il existe une réelle interopérabilité permettant une utilisation optimale des fonctionnalités par rapport aux besoins métier de l'organisation.

5.6 Engagements / Responsabilités

Questions	Proposition d'analyse
• Quel est le niveau de disponibilité, RTO et RPO garantis pour la solution dans son ensemble ? Existe-t-il une solution de secours permettant aux utilisateurs d'accéder aux ressources de l'organisme en cas de panne de la solution SASE ? Si oui, merci de détailler. • L'offre bénéficie-t-elle de certifications ? Si oui, lesquelles ?	Les niveaux proposés par les éditeurs sont-ils conformes aux exigences de disponibilité de mon organisation ? Peu de solutions de secours permettent de maintenir un niveau de service équivalent en dehors de la duplication de l'infrastructure. La solution classique consiste à choisir entre désactiver la sécurité (fail-open) en cas d'indisponibilité de la plateforme ou d'empêcher toute communication (fail-close). Les certifications permettent de garantir un niveau minimum de conformité avec des standards.

5.7 Protection des données par l'éditeur

Questions	Proposition d'analyse
• Les équipes techniques de l'éditeur ont-elles accès aux données du client ? Si oui, lesquelles (données en transit, journaux d'événements, etc.) et dans quelles conditions (accès direct, bastion) ? Où sont situées les équipes techniques de l'éditeur ? • Quels sont les mécanismes d'isolation entre les clients (réseau, serveurs, base de données, applicatifs, etc.) ?	Comme toute solution, les composants SASE doivent s'intégrer dans la politique de sécurité de votre organisation. Par nature, des composants sont externalisés et les politiques cloud de l'organisation s'appliquent. Il convient d'avoir une vue précise des engagements de sécurité de l'éditeur et d'avoir conscience qu'il peut techniquement avoir accès aux données transitant par sa plateforme. En effet, ce n'est qu'au travers de protections logicielles et de procédures que l'accès peut être limité. De plus, l'infrastructure SASE est partagée avec d'autres clients et le cloisonnement est logiciel uniquement. La confiance dans l'éditeur est primordiale, dans la mesure où il est le garant de la sécurité de l'organisation. Une démarche plus complète d'analyse de la sécurité de l'éditeur pourra être un complément utile à mener lors de la phase amont du projet SASE.

5.8 Modèle financier

Questions	Proposition d'analyse
• Modèle de tarification ?	Le modèle de tarification de la solution est-il suffisamment clair et permet-il de faire des projections dans le temps afin d'établir un budget réaliste ?

5.9 Modèle de gestion

Questions	Proposition d'analyse
• Modèle de gestion souhaité ?	Actuellement, le marché est composé de deux types d'acteurs offrant des solutions SASE : • Éditeur • Fournisseur de services managés (ESN, intégrateur, opérateur télécom, etc.) Selon le modèle choisi, le prestataire offrira plus ou moins de contrôle sur la partie logicielle ou sur la connectivité réseau. Quoi qu'il en soit, il convient d'être vigilant quant au partage des rôles et responsabilités.

6 Cas d’usage et exemples d’implémentation

6.1 Cas d’usage

Les cas d’usage sont donnés à titre indicatif et ne sont pas classés par ordre d’importance.

6.1.1 Accès distants sécurisés pour les utilisateurs

Contrairement aux VPN classiques (IPSec/TLS) qui fournissent un accès plus large aux réseaux de l’entreprise, le ZTNA (Zero Trust Network Access) donne un accès granulaire uniquement aux applications via un tunnel chiffré (TLS) une fois l’identité de l’utilisateur et la conformité de son poste de travail vérifiées.

Composant important de l’approche SASE, le ZTNA permet la centralisation des flux de communication et augmente la visibilité du SOC pour identifier rapidement les tentatives d’intrusion et y répondre. Sa position de concentrateur lui permet également de fournir les éléments de télémétrie permettant de contrôler l’expérience utilisateur et de faire de la maintenance préventive.

En complément, SWG (Secure Web Gateway) et RBI (Remote Browser Isolation) permettent l’inspection des flux de navigation, le filtrage et la détection d’éléments malveillants dans le trafic.

Les principaux composants utilisés sont : SWG, ZTNA, RBI.

6.1.2 Gestion des accès aux applications

L'objectif consiste à identifier et interdire l'accès à certaines applications internes ou SaaS qui présentent des risques, tels que le non-respect des lois, des problèmes de sécurité, un faible niveau de confiance ou une non-conformité avec les politiques de l'entreprise (Shadow IT). Certaines applications peuvent également être restreintes à des profils d'utilisateurs spécifiques en raison de leur sensibilité.

L'entreprise pourra appliquer ces règles d'autorisation et d'interdiction de manière contextuelle et granulaire selon les catégories d'utilisateurs, les terminaux utilisés, la géolocalisation, etc., tout en garantissant la traçabilité.

Les principaux composants utilisés sont : SWG, CASB, ZTNA, NG-FW, UEBA.

6.1.3 Interconnexion sécurisée des sites distants

À travers la mise en place d'équipements adaptés dont la gestion est centralisée, le SASE permet d'interconnecter, de sécuriser et de gérer facilement les sites distants, même les plus modestes. La redondance des accès, souvent prise en charge nativement, renforce la disponibilité et la résilience des connexions, contribuant ainsi à une meilleure continuité de service. Les liens Internet sur lesquels passe l’interconnexion vers le SASE ne sont pas détenus par le fournisseur SASE, il faut être vigilant aux engagements de service proposés par le fournisseur d’accès Internet.

Composants utilisés : SD-WAN, ZTNA, NG-FW/FWaaS.

6.1.4 Contrôle de l'échange des données

Le CASB (Cloud Access Security Broker) permet à l'organisation d'avoir une visibilité et un contrôle sur l'utilisation et les échanges des données au sein des ressources informatiques. Le travail collaboratif et l'augmentation incessante des données sont source de risques de fuite des données ou de compromission. C'est la raison pour laquelle le rôle d'intermédiaire de cette fonctionnalité permet une meilleure gestion des droits d'accès aux documents partagés et une optimisation du contrôle. Le DLP permet de compléter utilement en apportant une couche de contrôle supplémentaire.

Composants utilisés : CASB, DLP.

6.2 Exemples d'implémentation

Nous avons regroupé dans ce chapitre quelques exemples d'approches SASE à différents stades allant de l'étude de viabilité à une implémentation en production.

6.2.1 Cas d'implémentation numéro 1

- **Contexte :** Société de 200 collaborateurs, dont une centaine de collaborateurs en nomadisme ; quatre sites répartis dans la même région en France, dont un datacenter historique hébergeant les applications métier ; utilisation de trois applications SaaS.
- **Objectifs :**
  - Simplifier la gestion des interconnexions et des accès aux ressources internes et SaaS, ainsi que le nomadisme.
  - Améliorer la sécurité des accès aux applications.
  - Homogénéiser la politique de filtrage d'accès aux sites Internet.
- **Déroulé projet :**
  - Réflexion sur le besoin SASE : avec quatre sites dans la même région en France, l'atout du SASE de se connecter à un « point de proximité » (ou POP) pour bénéficier de la qualité des interconnexions « inter-POP » est inexistante.
  - En revanche, tous les sujets d'homogénéisation et d'agrégation des connexions pour appliquer des politiques globales, tant pour les utilisateurs internes que pour les nomades, sont des atouts.
  - Il a donc été décidé de se faire présenter trois offres d'éditeurs, puis de définir des critères différenciants pour ne retenir qu'une offre.
  - À date, une offre est retenue, les designs de transformations d'architecture sont en cours.
- **Éléments clés/difficultés/enseignements :**
  - Le budget devient une OPEX, il a fallu montrer les différences de coûts par rapport à une solution permettant d'homogénéiser de manière plus traditionnelle les politiques de sécurité.
  - Incompréhension concernant la sécurité des réseaux locaux : expliquer les différences entre la sécurisation purement locale wifi et filaire (Network Access Control (NAC / 802.1X), etc.), par rapport aux sécurités apportées par l'agent SASE de poste de travail.
  - Anticiper les plans de transformation d'infrastructure et les changements (nouvelles installations techniques, éventuelles modifications de chartes informatiques, etc.).

- Pour un éditeur, il n'a jamais été confirmé qu'il était en mesure de commercialiser son offre SASE du fait de la « petite taille » du client et de la présence des sites uniquement en Île-de-France.

6.2.2 Cas d'implémentation numéro 2

- **Contexte :** Etude pour l'implémentation de la solution SASE dans un grand groupe international réparti sur 40 pays, avec trois datacenters dans le monde.
- **Objectifs :**
  - L'objectif de l'étude est de définir la trajectoire à 10 ans avec un éclaircissement sur les coûts prévisionnels de la solution SASE.
  - Le choix de la solution SASE permet de rationaliser le nombre d'agents installés sur le poste de travail. L'EDR n'est pas intégré dans l'étude.
  - Les problématiques de la latence et de l'expérience utilisateur pour l'accès aux datacenters mondiaux de l'entreprise ont été étudiées en particulier.
- **Éléments clés/difficultés/enseignements :**
  - Un découpage des fonctionnalités du SASE a été réalisé sur les parties télécommunication (SD-WAN), accès aux ressources de l'entreprise (ZTNA, SWG, CASB), protection des applications (DDoS, API protection, WAF) prévention de la perte des données (DLP), pare-feux (FWaaS) et canaux de communication (mails, Teams, Slack).
  - Les risques identifiés pour l'implémentation du SASE sont la durée de mise en œuvre, le nombre de partenaires et la collaboration avec l'ensemble des équipes.
  - La réversibilité du SASE a aussi été étudiée pour permettre une récupération des configurations par API.
  - Un accent a été mis sur le niveau de granularité des permissions et le renforcement du contrôle de l'administration (administration à quatre yeux).

6.2.3 Cas d'implémentation numéro 3

- **Contexte :** Projet de déploiement SASE au sein d'une entreprise avec environs 6000 collaborateurs répartis sur des dizaines de sites géographiques, en France et DROM-COM.
- **Objectifs :**
  - Améliorer la posture globale de sécurité grâce à une gestion centralisée de politiques de sécurité sur tous les utilisateurs, appareils et applications, indépendamment de leur localisation géographique.
  - Cartographier l'ensemble des applications.
  - Améliorer l'expérience utilisateur et la productivité en fournissant un accès sécurisé, rapide et fiable aux ressources cloud et aux applications privées.
  - Répondre aux exigences réglementaires en matière de conformité.
  - Minimiser les risques liés à la fuite ou aux violations de données et aux accès non autorisés.
  - Gestion de l'obsolescence (des solutions actuelles VPN client et Proxy de navigation).
- **Éléments clés/difficultés/enseignements :**

  Le projet s'est déroulé en deux temps dissociés avec deux appels d'offres :

- Phase 1 : Le projet SD-WAN sur 10 mois
  - Être conscient du support Internet qui introduit de la latence et pas de garantie de SLA.
  - Nécessite une bonne synchronisation entre réception du matériel et la mise en service.
- Phase 2 : L'étude et contractualisation SSE sur 18 mois
  - Les offres éditeurs évoluant régulièrement, il est important de définir une phase d'étude des solutions fixes.
  - Prévoir un temps adapté pour finaliser la partie contractuelle.
  - Prévoir un pilote (1 à 2 mois) sur un périmètre restreint en production en intégrant les cas d'usage significatifs avant le choix final.
  - Le pilote permet également d'anticiper de nombreux écueils en termes de flux à autoriser ou à interdire. Il donne également un aperçu significatif de la cartographie des applications utilisées et des usages.
- Déploiement global en production par composants (*délai/planning à compléter par la suite pour chaque composant)*
  - Bascule du proxy historique vers le nouveau proxy SWG.
    - Retrait des flux vidéo de Teams (latence excessive).
  - Suppression progressive du VPN pour les utilisateurs, au profit du ZTNA.

6.2.4 Cas d'implémentation numéro 4

- **Contexte :** Projet de déploiement SASE dans un groupe international (une centaine de sites sur plusieurs plaques) et quelques milliers de collaborateurs, dans le cadre de la refonte de l'infrastructure IT.
- **Objectifs :** Sécuriser les accès, améliorer les performances réseau et simplifier la gestion, dans un contexte marqué par une croissance externe via l'acquisition régulière de nouvelles entités.
- **Éléments clés/difficultés/enseignements :**
  - La solution SASE déployée intègre les briques SD-WAN, ZTNA, FWaaS et Secure web Gateway, avec une architecture cloud-native s'appuyant sur des points de présence au plus proche des sites et utilisateurs. Cette approche a permis d'harmoniser les connexions depuis une console de management unique, d'offrir une sécurité unifiée, quel que soit le lieu de connexion, et de remplacer les VPN traditionnels par un accès conditionnel basé sur l'identité et le contexte.
  - Amélioration de l'expérience utilisateur, avec des accès plus rapides et plus fiables aux ressources internes et au cloud.
  - Renforcement de la sécurité grâce à une inspection en ligne du trafic, une segmentation dynamique et une visibilité complète sur les usages.
  - Réduction de la complexité opérationnelle, avec une gestion centralisée des politiques réseau et sécurité.
  - Agilité accrue permettant de connecter rapidement de nouveaux sites ou utilisateurs.
  - Le projet a nécessité une phase d'audit approfondie, une cartographie des flux applicatifs et une intégration avec l'annuaire d'entreprise. Les principales difficultés (notamment l'adhésion des équipes locales et l'optimisation des

performances sur certains sites avec leurs propres spécificités) ont été levées grâce à une approche progressive, des pilotes ciblés et un accompagnement personnalisé.

- Ce projet illustre parfaitement la valeur ajoutée d'une approche SASE : une convergence efficace entre réseau et sécurité, au service de la performance, de la flexibilité et de la résilience de l'entreprise. La gestion projet de l'intégrateur a été structurante dans la réussite du projet.

7 Synthèse managériale

Le modèle Secure Access Service Edge (SASE), conceptualisé en 2019, s'impose progressivement comme une réponse aux transformations profondes des systèmes d'information : généralisation du cloud, mobilité croissante des collaborateurs, limite des architectures centralisées. En combinant les fonctions réseau et sécurité au sein d'une plateforme cloud unifiée, le SASE vise à offrir une gestion cohérente des accès et une sécurité homogène, quel que soit l'utilisateur, le terminal ou la localisation.

Pour les organisations, le SASE représente une promesse d'agilité et de simplification. Ses principaux bénéfices sont :

- une évolutivité qui accompagne la croissance, les acquisitions et le travail à distance, sans refonte complète des infrastructures ;
- une simplification grâce à la centralisation des politiques réseau et sécurité, réduisant la complexité opérationnelle ;
- une meilleure disponibilité et performance via une connectivité résiliente et optimisée ;
- une optimisation des coûts, avec le passage d'investissements matériels lourds (CAPEX) à un modèle plus flexible basé sur la consommation (OPEX) ;
- un renforcement de la posture de sécurité, en appliquant des contrôles homogènes et contextualisés sur l'ensemble des usages numériques.

Cependant, cette promesse s'accompagne de points de vigilance majeurs. Les risques à anticiper concernent :

- la dépendance au fournisseur, avec un risque de verrouillage contractuel et technologique ;
- la réversibilité complexe lors d'un changement de solution ;
- les contraintes réglementaires et de souveraineté, notamment liées aux fournisseurs soumis à des lois extraterritoriales ;
- la complexité d'implémentation, qui requiert un projet pluriannuel, une évolution de l'organisation interne et une communication renforcée ;
- une exposition accrue en cas de compromission de la plateforme SASE (qui concentre des fonctions critiques).

Face à ces enjeux, l'adoption d'une architecture SASE doit rester progressive et maîtrisée. Beaucoup d'organisations choisissent d'abord d'implémenter le Security Service Edge (SSE), qui constitue une première étape logique et moins intrusive, avant d'intégrer la dimension réseau. Cette trajectoire graduelle permet de limiter les risques, de préparer les équipes et d'assurer un alignement avec les priorités métier et réglementaires.

En conclusion, le SASE constitue une évolution structurante vers des infrastructures plus agiles, performantes et sécurisées. Pour en tirer pleinement parti, il convient toutefois de l'aborder avec discernement : le succès dépendra autant de la technologie retenue que de la gouvernance, du pilotage et de l'accompagnement du changement.



Tour Eria, 5 rue Bellini
92821 Puteaux Cedex
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

clusif.fr