netskope

Livre blanc

Le réseau de demain

Les quatre principes d'une conception moderne des réseaux

Flexible

Sécurisé

Table des matières

Table des matières

Préface : Note à l'attention des lecteurs

Aujourd'hui, beaucoup de nos clients sont à un tournant décisif quant à l'utilisation de leurs réseaux. Ils recherchent des solutions pour moderniser leur infrastructure actuelle et l'adapter aux enjeux futurs. Notre expérience auprès de milliers d'entreprises nous a permis d'identifier quatre principes essentiels, décrits dans ce guide, pour vous aider à créer votre réseau de demain.

Une entreprise ne saurait survivre sans l'information. Pour rester compétitives, les organisations mettent en œuvre des réseaux performants qui permettent d'accéder rapidement et efficacement aux données stockées dans leurs applications.

Notre monde évolue à toute vitesse. La réussite ne dépend plus seulement de l'efficacité des processus, mais surtout de notre capacité à nous adapter rapidement aux changements, qu'ils soient internes ou externes. C'est une vraie rupture avec le passé, où seule la rentabilité comptait en matière d'optimisation. Pour réussir aujourd'hui, les entreprises ont besoin de solutions informatiques à la fois économiques et agiles, capables de suivre le rythme effréné des affaires.

Ces dernières années ont révélé les limites d'une approche rigide. Au début du travail hybride, beaucoup d'entreprises ont tardé à s'adapter. Leurs réseaux étaient conçus pour un usage local, avec des utilisateurs et des applications sur site. Confrontées à ce nouveau défi, elles ont dû se réinventer dans l'urgence.

Les réseaux doivent évoluer, c'est une évidence. Mais par où commencer ? Ce guide vous aide à identifier les actions prioritaires pour moderniser votre infrastructure, l'objectif étant d'avoir un réseau performant, sécurisé et robuste, parfaitement adapté aux besoins de vos utilisateurs et de vos applications.

LES TENDANCES DE FOND À LA BASE DE CE CHANGEMENT

Pour bien transformer le réseau, nous devons d'abord comprendre les raisons qui nous poussent à le faire évoluer. Notre façon de vivre et de travailler est en pleine mutation sous l'effet de plusieurs tendances de fond qui influencent directement les missions des équipes IT. Chacun de ces facteurs exige une refonte complète du réseau, bien au-delà de simples ajustements progressifs. Conjugués, ces changements nous imposent de transformer radicalement nos systèmes.

La transformation numérique est désormais une réalité bien ancrée dans la plupart des organisations du monde entier. D'après une étude récente menée auprès des directeurs des systèmes d'information, 60 % des entreprises prévoient de maintenir des investissements conséquents dans leur transformation numérique. L'objectif est triple : renforcer leur compétitivité, gagner en agilité et optimiser leur processus décisionnel. [1]

Adoption du cloud

L'une des principales évolutions concerne la migration des applications et des données d'entreprise vers le cloud, hors des réseaux internes et des centres de données. D'après Gartner, en 2023, 70 % des charges de travail d'entreprise sont hébergées sur des plateformes cloud, contre seulement 40 % en 2020. [2] Cette tendance se reflète également dans le trafic réseau, puisque plus de 80 % des échanges d'entreprise transitent par Internet, dont plus de la moitié est directement liée aux services cloud. [3]

> Plus de 80 % du trafic des entreprises passe par Internet, et 53 % du trafic web provient d'activités liées au cloud.

Expansion des données

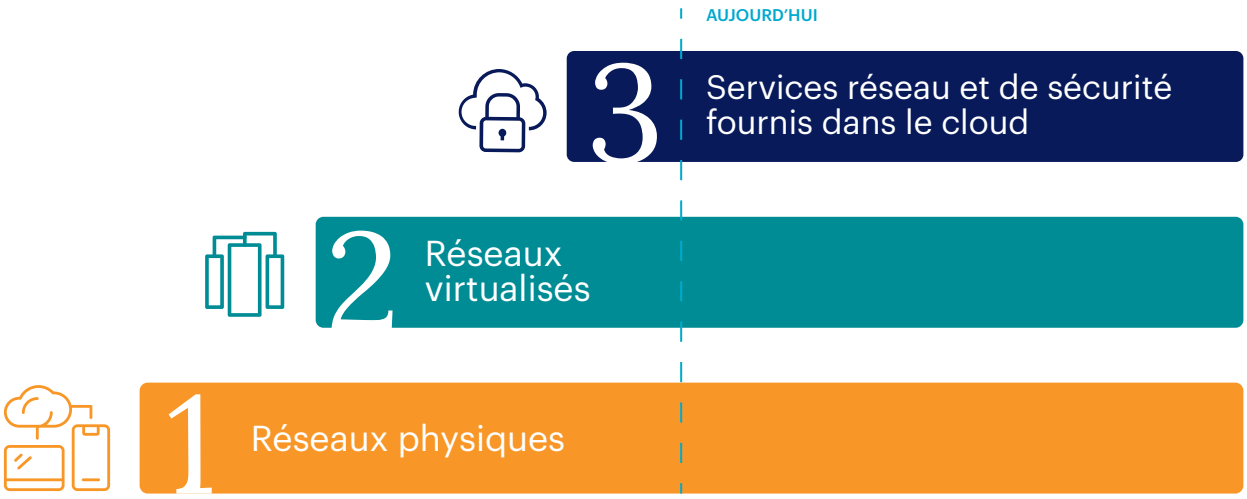
Un autre défi majeur réside dans l'explosion du volume de données générées. Entre 2020 et 2025, la quantité de données mondiales passera de 57 à 175 zettaoctets (Zo). [4] Jamais autant d'informations n'ont été collectées et partagées à travers autant de points d'accès. Ces innombrables données sont dispersées sur les réseaux, dans le cloud et sur une multitude d'appareils, qu'ils soient gérés ou non. Sans protection adaptée, cette dispersion les rend particulièrement vulnérables : l'an dernier, 40 % des entreprises ont subi une violation de données dans le cloud. [5]

Travail hybride

Un troisième facteur clé réside dans l'évolution des modes de travail. Une part importante des employés continuera à travailler en dehors des bureaux traditionnels et souhaite avoir un accès fluide aux informations, qu'importe l'appareil ou le lieu, sans compromis sur la sécurité. Aux États-Unis, 50 % de la main-d'œuvre devrait adopter le télétravail sur le long terme. [6]

Ces tendances de fond nous permettent maintenant de mieux comprendre les défis à relever. C'est dans ce contexte que le réseau d'entreprise entre dans sa troisième ère de conception et qu'on doit en redéfinir l'utilisation et les modes de déploiement. De toute évidence, nos réseaux actuels sont conçus pour répondre à des besoins d'une autre époque et doivent évoluer rapidement face aux défis actuels. En fait, si nous nous accrochons aux anciennes architectures réseau et de sécurité, nous risquons non seulement de nous priver des avantages du cloud et du travail hybride, mais aussi de compromettre la protection des données à l'échelle de l'entreprise.

LES TROIS ÈRES DE LA CONCEPTION DES RÉSEAUX D'ENTREPRISE



La conception des réseaux a traversé trois grandes évolutions majeures :

1. Réseaux physiques (hiérarchie à 3 couches / commutation Spine-Leaf)
2. Réseaux virtualisés
3. Services réseau et de sécurité dans le cloud

L'architecture de base de la plupart des réseaux d'entreprise repose sur un modèle à 3 couches et ses variantes qui utilisent la commutation Spine-Leaf. Ce modèle, qui a fait ses preuves et est largement maîtrisé pour déployer des services réseau, demeure toujours d'actualité.

La deuxième ère de conception des réseaux (réseaux virtualisés) en est maintenant à son apogée. Elle répond à la nécessité croissante d'intégrer des services réseau et de sécurité pour le trafic est-ouest. Plutôt que d'acheminer ce trafic vers le cœur du réseau, la virtualisation exécute les fonctions de commutation, de routage et de sécurité directement dans l'hyperviseur ou via un pare-feu virtualisé en mode bridge. Cette approche allège alors la charge du cœur du réseau sans la supprimer ni la remplacer.

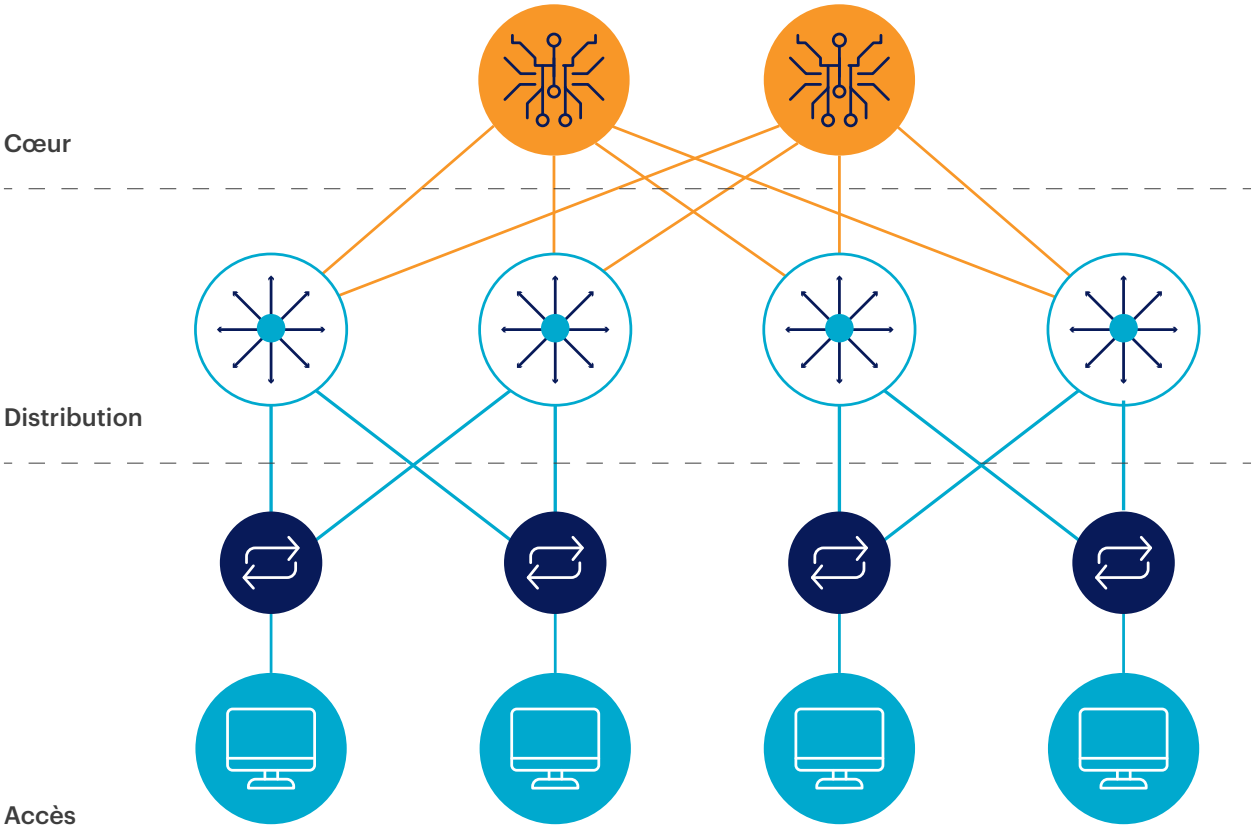
Un point intéressant à noter est que les deux premières phases de l'évolution des réseaux ne s'excluent pas mutuellement. Les réseaux virtualisés fonctionnent en parallèle avec les infrastructures physiques traditionnelles, sans pour autant diminuer ou supprimer leurs fonctionnalités. Ainsi, bien que la virtualisation des réseaux apporte des avantages significatifs, elle vient simplement se superposer aux réseaux physiques existants qui demeurent essentiels.

L'essor des services réseau et de sécurité fournis dans le cloud marque l'entrée dans la troisième ère de la conception des réseaux. Contrairement aux modèles précédents, cette approche offre aux entreprises une opportunité unique pour simplifier leurs réseaux. Elles n'ont plus besoin d'assumer seules les lourdes charges d'investissement et d'exploitation de leur infrastructure réseau. En effet, le cloud permet désormais d'enrichir le réseau étendu avec des services externalisés. Cette transition vers le cloud apporte de nombreux avantages, notamment une efficacité accrue, une meilleure fiabilité et une sécurité renforcée. Elle réduit également la complexité globale. Ceci est possible, car l'intégration transparente des services réseau et de sécurité dans le cloud s'effectue sans bouleverser l'architecture existante du réseau étendu.

Dans ce guide, nous allons examiner les différentes étapes de l'architecture réseau et proposer des recommandations pour permettre aux entreprises d'optimiser leur infrastructure informatique.

La première ère : réseaux physiques (3 couches / commutation Spine-Leaf)

Le concept fondamental du réseau à 3 couches consiste à concentrer les services réseau les plus puissants au cœur du réseau, tout en utilisant différentes couches de distribution pour établir la connectivité partout où l'organisation est présente. Cette architecture, largement éprouvée, garantit une connectivité efficace et fiable.



Exemple de réseau physique

L'architecture réseau traditionnelle à 3 couches cherche à diminuer les coûts en optimisant l'utilisation de routeurs et de pare-feux centraux performants, bien que coûteux, au cœur de l'infrastructure. La couche centrale assure ainsi la connexion entre les différents segments du réseau étendu tout en établissant une frontière claire entre les sections qui sont sécurisées et celles qui ne le sont pas.

L'intégration de la sécurité dans un réseau à 3 couches ajoute une complexité importante. Les contrôles de sécurité doivent être appliqués sans affecter les performances du réseau, mais on doit alors relever de nouveaux défis en matière d'architecture et notamment savoir où les insérer au sein de l'infrastructure physique. À mesure que les besoins évoluent, l'ajout de solutions comme les pare-feux, la protection contre les intrusions ou la prévention des pertes de données alourdit davantage la conception du réseau. Cette approche multiplie également les contraintes opérationnelles et les points de défaillance potentiels.

Avec le développement des centres de données et la demande croissante d'accès aux applications, le réseau physique des entreprises a évolué vers une architecture Spine-Leaf. Ce modèle réduit la latence du trafic est-ouest en interconnectant les commutateurs Leaf dans un maillage complet. En pratique, il simplifie un aspect de l'architecture (en passant de trois couches à deux), mais reste tout aussi complexe, voire plus, en ce qui concerne la sécurité. Malgré les avancées en matière de commutation, une question demeure : comment réaliser l'inspection du trafic pour garantir une protection efficace ?

La première génération des réseaux d'entreprise a été conçue avant tout pour assurer la connectivité, et ce, au détriment de la sécurité. Son architecture privilégie l'accès plutôt que la restriction, ce qui facilite l'isolation des hôtes, mais complique leur connexion sécurisée et l'application de contrôles précis avec inspection du contenu. C'est ce besoin accru d'isolation qui marque le début de la deuxième génération de réseaux d'entreprise.

La première génération des réseaux d'entreprise a été conçue avant tout pour assurer la connectivité, et ce, au détriment de la sécurité. Son architecture privilégie l'accès plutôt que la restriction.

La deuxième ère : Réseaux virtualisés

Plusieurs avancées majeures ont joué un rôle clé dans l'émergence de ce qu'on peut appeler l'ère des réseaux virtualisés. Premièrement, la virtualisation a profondément transformé l'architecture des centres de données, ce qui a augmenté la densité des hôtes tout en générant un trafic entre machines qui ne passe jamais par le câble physique. Ensuite, le risque des menaces internes ou de l'exploitation des machines compromises par des pirates a mis en lumière le problème des mouvements latéraux entre systèmes de confiance similaire. Enfin, les principes du Zero Trust ont entraîné des exigences d'isolation et des contrôles d'accès plus précis que ceux offerts par un réseau plat ou une segmentation traditionnelle.

La virtualisation des réseaux a marqué le début de la deuxième ère de la conception des réseaux. Au lieu de contraindre tout le trafic à traverser le cœur du réseau, les organisations ont commencé à utiliser diverses technologies de superposition pour intégrer des contrôles réseau, comme la segmentation, sans modifier le réseau sous-jacent. De plus, grâce à ces superpositions, la virtualisation a enrichi le réseau physique en permettant d'insérer des inspections de sécurité dans le trafic est-ouest sans obliger ce dernier à passer par une liaison physique. Ces services peuvent être mis en œuvre en utilisant le réseau virtualisé pour diriger le trafic à travers des pare-feux virtualisés ou en ajoutant des services de sécurité directement liés à l'hyperviseur.

La virtualisation des réseaux a considérablement renforcé la capacité des entreprises à déployer différentes mesures de sécurité. Cependant, elle reste confrontée à un défi majeur : la complexité. En effet, la virtualisation des réseaux s'ajoute aux services de mise en réseau physique, et la complexité de ces deux types de réseaux persiste.

La troisième ère : Services réseau et de sécurité dans le cloud

Les deux premières ères de conception des réseaux reposaient entièrement sur une approche interne : le service informatique concevait, déployait et gérait l'infrastructure qui fournissait les services réseau. Mais que se passe-t-il lorsque les ressources à connecter ne font plus partie du réseau de l'entreprise ? C'est exactement le défi posé par l'essor du cloud et du travail hybride, qui ont profondément transformé la nature des connexions et des exigences en matière de sécurité.

Ces évolutions posent une question essentielle : les principaux services réseau et de sécurité peuvent-ils être fournis depuis le cloud tout en fonctionnant simultanément avec le réseau traditionnel de l'entreprise ?

La plupart des applications d'entreprise s'appuient, d'une manière ou d'une autre sur le cloud. Faire passer le trafic par le réseau de l'entreprise pour accéder aux applications cloud pose problème, car l'organisation dispose de peu de points de sortie et d'une capacité de pare-feu limitée. Dans bien des cas, ce détour par l'infrastructure de sécurité interne entraîne un routage inefficace, allonge la latence et dégrade l'expérience des utilisateurs, agacés de devoir attendre les réponses de leurs applications.

Grâce aux services réseau et de sécurité du cloud, les entreprises peuvent permettre aux utilisateurs d'accéder aux applications où qu'ils soient, sans avoir à rediriger le trafic vers les ressources sur site. Toutefois, plutôt que de considérer l'accès au cloud comme un cas d'utilisation distinct, il est important de comprendre que cette troisième ère offre la possibilité de simplifier grandement la complexité héritée des deux premières ères de la conception des réseaux.

Traiter le cloud comme une extension du réseau de l'entreprise, c'est-à-dire comme un réseau pair en termes de services et de sécurité, permet d'éliminer la complexité du réseau local. En fait, les services réseau et de sécurité fournis dans le cloud évitent d'ajouter des éléments supplémentaires, car vous n'avez plus besoin de diriger le trafic vers une appliance pour implémenter de nouveaux services.

Le modèle cloud simplifie la gestion du réseau en réduisant le problème à un premier saut vers le centre de données du fournisseur. Une fois ce cap franchi, des microservices de sécurité peuvent être activés sans nécessiter de modifications supplémentaires de l'infrastructure. Grâce à la séparation de la sécurité et du réseau, les entreprises gagnent en flexibilité et peuvent déployer des réseaux plus légers, plus fiables et optimisés grâce aux services de sécurité fournis dans le cloud.

Les principaux services réseau et de sécurité peuvent-ils être fournis depuis le cloud tout en fonctionnant simultanément avec le réseau traditionnel de l'entreprise ?

SASE : UNE IMPLÉMENTATION PRATIQUE DES SERVICES RÉSEAU ET DE SÉCURITÉ FOURNIS DANS LE CLOUD

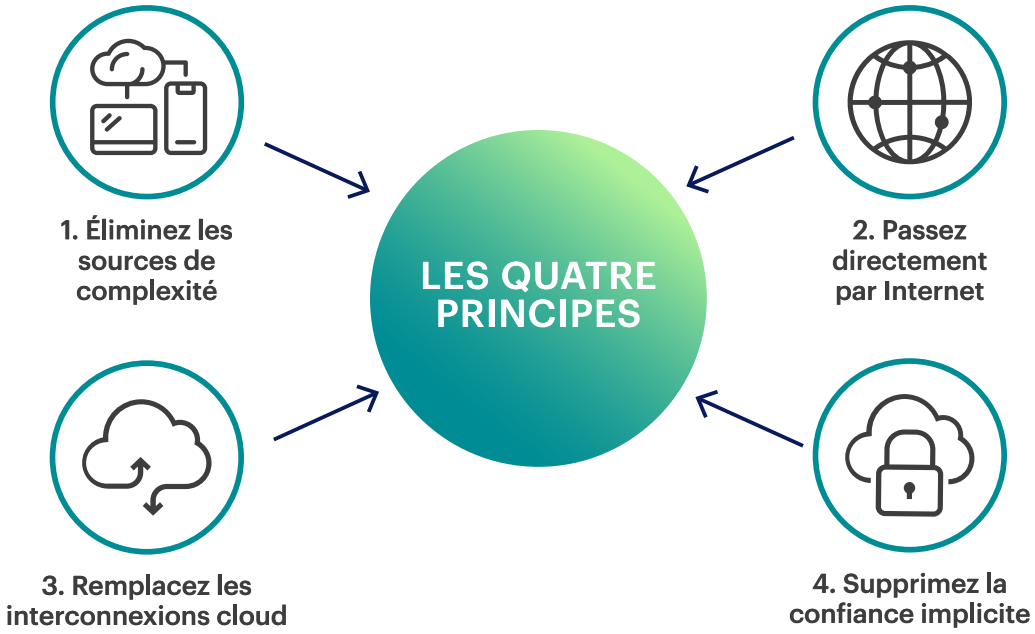
L'architecture Secure Access Service Edge (SASE), prononcée « sassy », repose sur le cloud pour offrir des services réseau et de sécurité visant à protéger les utilisateurs, les applications et les données. Avec de nombreux utilisateurs et applications qui ne sont plus généralement présents ni actifs sur le réseau d'entreprise, les solutions d'accès et de sécurité ne peuvent plus se baser sur les équipements matériels traditionnels du centre de données de l'entreprise.

Le SASE offre les fonctionnalités réseau et de sécurité requises sous forme de services cloud. Au lieu de rediriger le trafic vers un équipement de sécurité, les utilisateurs se connectent directement au service cloud SASE, ce qui garantit un accès sécurisé aux applications, aux services web et aux données. Cette approche permet d'appliquer une politique de sécurité de manière cohérente, quel que soit l'emplacement ou l'appareil utilisé.

LES QUATRE PRINCIPES DE L'IMPLÉMENTATION DES SERVICES RÉSEAU ET DE SÉCURITÉ DANS LE CLOUD

Alors que nous entrons dans la troisième ère des réseaux d'entreprise, comment les architectes réseau doivent-ils envisager les réseaux à venir ?

Ce guide vous accompagnera dans votre démarche. Les quatre principes suivants aident les organisations à identifier où apporter des changements significatifs pour améliorer leurs services réseau :



1ER PRINCIPE : ÉLIMINEZ LES SOURCES DE COMPLEXITÉ

Le SASE révolutionne la conception des réseaux et ouvre la porte à de nouvelles opportunités.

Simplifiez votre architecture

Un réseau bien conçu doit toujours avoir une capacité supplémentaire, car fonctionner près du point de rupture conduit inévitablement à des défaillances. Un réseau résilient doit pouvoir s'adapter aux fluctuations de l'activité, qu'il s'agisse d'un afflux temporaire de collaborateurs au siège pour une conférence ou d'une transition entre travail sur site et télétravail. Même en temps normal, certains sites du réseau restent sous-utilisés pendant de longues heures en dehors des horaires de bureau. Cependant, cette capacité supplémentaire a un coût, car les réseaux sous-utilisés nécessitent quand même des équipements, des services et du personnel qui devraient dans l'idéal, rester inutilisés.

De la même manière, garantir la fiabilité implique un coût supplémentaire. La redondance entraîne un doublement des investissements en équipements réseau et en services de basculement, qui, dans le meilleur des cas, restent inactifs lorsqu'ils sont configurés comme solutions de secours à froid ou en mode basculement passif.

Par conséquent, chaque service ajouté au réseau exige un surprovisionnement et une expertise technique avancée pour garantir sa stabilité, sa convivialité, sa fiabilité et son évolutivité. Ce n'est pas forcément une mauvaise chose, car les organisations doivent s'assurer que la capacité et la fiabilité sont intégrées dès la conception. Cependant, la vraie question reste de savoir si l'intégration de ces services directement dans le réseau constitue la meilleure méthode d'implémentation. En transférant cette capacité excédentaire et l'expertise technique associée vers la couche SASE, les entreprises peuvent bénéficier d'une approche plus flexible, et ne payer que les ressources réellement utilisées au moment où elles en ont besoin.

Un réseau bien conçu doit toujours avoir une capacité supplémentaire, car fonctionner près du point de rupture conduit inévitablement à des défaillances.

La simplification renforce la disponibilité et la résilience du réseau. Avec moins de composants susceptibles de tomber en panne, il devient plus facile d'atteindre un niveau de fiabilité et d'élasticité comparable à celui des infrastructures opérateurs.

Pour moderniser leur infrastructure réseau, les entreprises gagneraient à repenser leur architecture de fond en comble. Ce processus passe par une conception plus rationnelle, un déploiement plus rapide des services et une meilleure capacité à intégrer de nouveaux sites ou collaborateurs, qu'ils soient au bureau ou en télétravail. En privilégiant une connexion directe au réseau, les organisations peuvent réduire leurs dépenses tout en optimisant l'accès aux applications cloud. Des solutions comme le SD-WAN apportent également plus de souplesse dans la gestion du réseau. L'objectif est clair : un réseau d'entreprise simple, rapide et fiable, s'appuyant sur la couche SASE pour garantir une connectivité sécurisée au cloud.

Modernisez les conceptions obsolètes

Dans les deux premières générations des réseaux d'entreprise, la mise en place des services de sécurité nécessitait le déploiement d'équipements physiques et virtuels en ligne. Avec le temps, l'accumulation de ces services a complexifié le routage, ce qui a entraîné des problèmes d'efficacité, comme le chaînage proxy des anciennes solutions de sécurité ou l'obligation de tunneliser le trafic vers une pile de sécurité distante. Ces pratiques restent courantes aujourd'hui, car de nombreux fournisseurs continuent à proposer des solutions qui reposent sur un chaînage et un transfert inefficaces en arrière-plan.

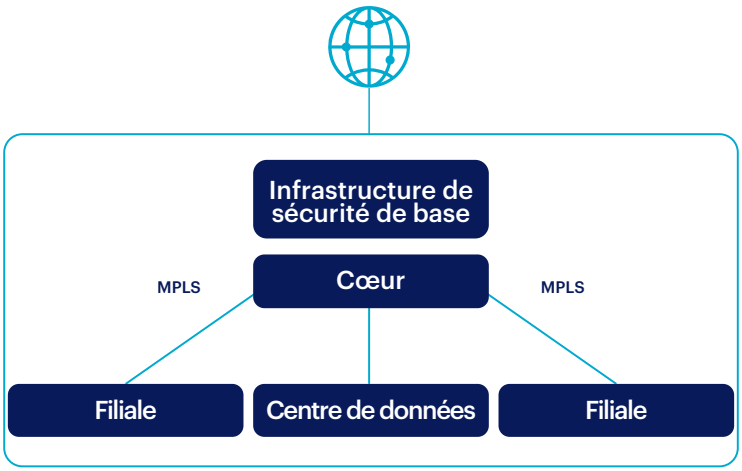
Pour moderniser l'architecture, utilisez le SASE comme un réseau pair à pair pour déployer des services et éviter de devoir constamment recâbler le réseau. Par exemple, au lieu d'installer plusieurs passerelles alignées pour gérer les différentes voies du trafic Internet, web et cloud, la couche SASE offre le SWG, le pare-feu dans le cloud et le CASB, tous accessibles dès le premier saut. Une fois le premier service déployé, l'ajout de nouvelles fonctionnalités se fait simplement par activation, sans avoir à insérer des équipements de sécurité supplémentaires dans le réseau.

À mesure que les services de sécurité sont transférés vers la couche SASE, le réseau sous-jacent gagne en sécurité en éliminant les itinéraires complexes et les exceptions aux règles. Autrefois, les contrôles d'accès s'appuyaient sur des décisions stratégiques directement intégrées au réseau, tandis que les architectures modernes les externalisent vers le SASE. Par exemple, les anciennes approches reposaient sur des règles de pare-feu appliquées aux segments ou aux zones du réseau, chaque « autorisation » pouvant involontairement créer des vulnérabilités en raison du niveau de granularité limité de la segmentation. En déplaçant ces décisions vers la couche SASE, la surface d'attaque se réduit considérablement. Elle offre ainsi un contrôle plus précis pour renforcer la sécurité globale.

À mesure que les entreprises intègrent de nouvelles fonctionnalités de sécurité, comme la protection des données et la protection contre les menaces, ces services peuvent être activés directement depuis la plateforme SASE.

2E PRINCIPE : PASSEZ DIRECTEMENT PAR INTERNET

Les réseaux étendus adoptent une architecture en étoile pour plusieurs raisons. Autrefois, tout le trafic devait passer par le cœur du réseau pour accéder aux centres de données internes. Cette conception offrait également un point de contrôle stratégique, ce qui facilitait l'intégration des mesures de sécurité aux quelques points de sortie disponibles.

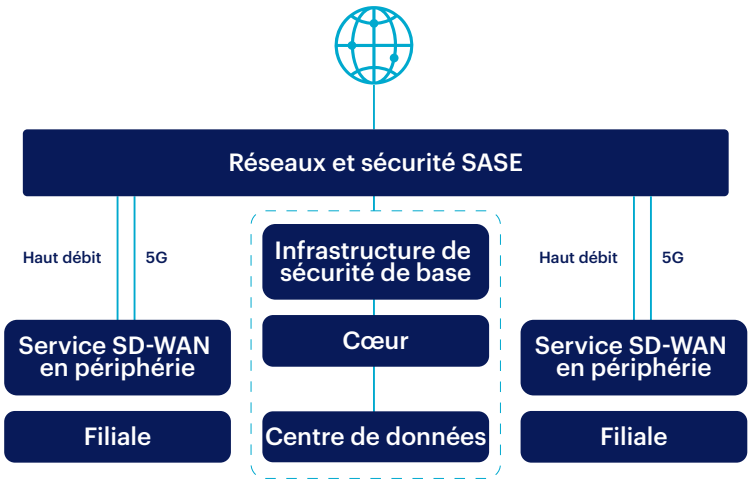


Avec le passage des applications vers le cloud, les entreprises ont cherché à adopter un accès direct à Internet. Grâce à une connexion Internet au niveau des filiales, le trafic vers le cloud et l'Internet peut être déchargé du réseau MPLS. Cependant, les pare-feux utilisés dans les filiales, souvent moins performants que ceux du siège, rendent l'application des stratégies de sécurité incohérente. Même si l'organisation décide d'installer le même pare-feu périmétrique dans les filiales, la maintenance de ces équipements pèse lourdement sur des équipes réseau déjà surchargées. Pire encore, cette tâche est souvent confiée à du personnel non technique, sans réelle expertise en gestion de pare-feu ou en sécurisation des équipements. Ainsi, une solution visant à optimiser le réseau peut paradoxalement engendrer de nouveaux défis opérationnels, parfois encore plus complexes.

Utiliser SASE pour l'accès direct à Internet

Le modèle SASE apporte des solutions clés pour simplifier, moderniser et optimiser le réseau des filiales en facilitant l'accès direct à Internet. Deux obstacles majeurs freinent le remplacement du MPLS : d'une part, l'instabilité et le manque de fiabilité de l'Internet public, et d'autre part, la difficulté d'assurer une sécurité cohérente sans recourir à des équipements coûteux et difficiles à gérer sur chaque site. Le SASE permet de surmonter ces défis en intégrant à la fois la connectivité réseau et la sécurité.

Pour faire face aux soucis de stabilité et de fiabilité d'Internet, la meilleure solution consiste à utiliser plusieurs connexions simultanées, notamment des accès Internet à bas coût, le tout géré et optimisé par le SD-WAN. Cette technologie garantit la stabilité des sessions même en cas de congestion ou de panne d'une liaison. De plus, elle ajuste automatiquement le routage pour maintenir des performances optimales. Ces ajustements étant effectués de manière transparente, les connexions SD-WAN assurent un accès direct à Internet sans interruption. Les applications peuvent ainsi s'exécuter continuellement, sans dégrader l'expérience utilisateur.



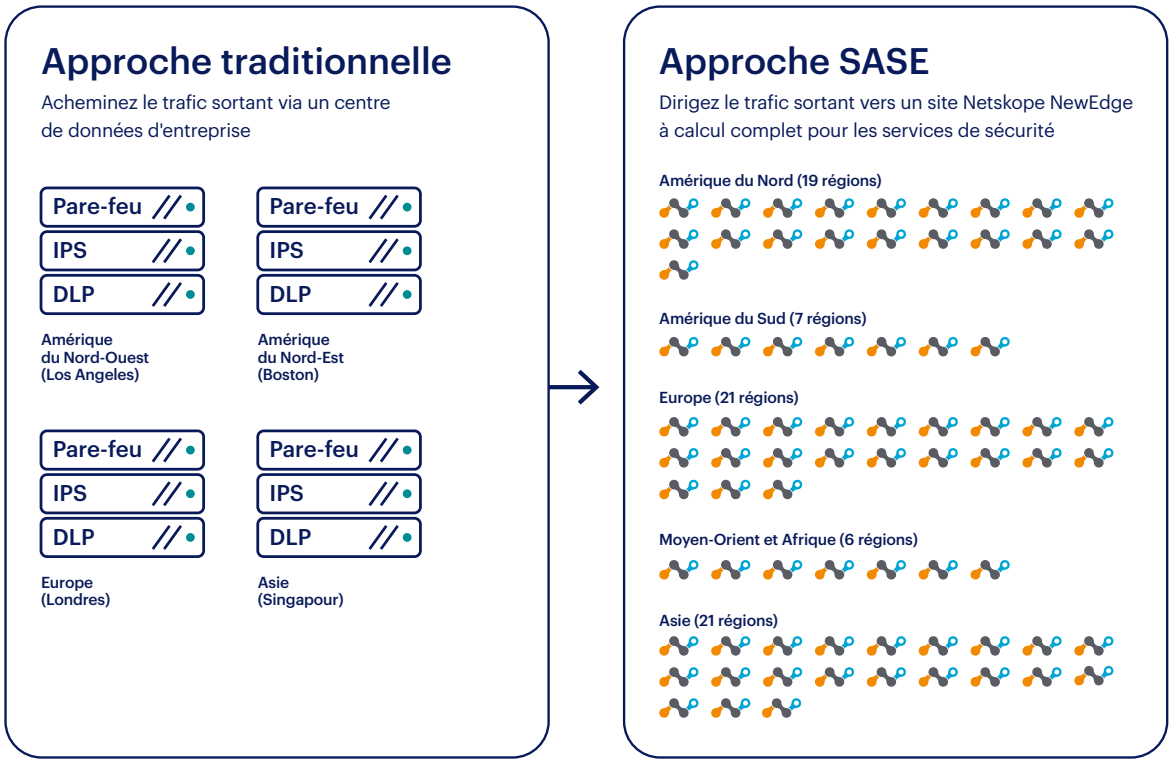
Pour résoudre les problèmes d'incohérence de la sécurité sans dépendre des pare-feux sur site, les entreprises associent le SD-WAN à l'architecture SASE. Cette solution offre l'avantage de transférer les fonctions de sécurité vers le cloud tout en facilitant l'administration du matériel sur site. Le rôle principal de l'appareil SD-WAN se limite alors à établir la connectivité au premier saut et à diriger le trafic vers le cloud SASE, où la visibilité et la sécurité sont appliquées en temps réel, au fur et à mesure de l'utilisation des applications. Grâce à cette architecture, les entreprises n'ont plus besoin de gérer des pare-feux coûteux dans chaque filiale.

L'utilisation des technologies SD-WAN ne se limite pas aux filiales. Avec la montée en puissance des applications cloud, en particulier celles qui reposent sur des communications en temps réel, comme la collaboration et la visioconférence, la connectivité des utilisateurs en télétravail devient un enjeu majeur. Votre organisation évalue le SD-WAN ? Demandez-vous s'il est judicieux d'utiliser plusieurs connexions entre le terminal et Internet (par exemple en combinant une connexion haut débit avec un modem 5G) pour renforcer la stabilité des applications stratégiques.

Distribuer l'accès aux services de sécurité pour réduire la latence

La plupart des entreprises font face à des contraintes physiques et financières qui limitent le nombre de centres de données qu'elles peuvent utiliser et le nombre de points de sortie qu'elles peuvent gérer. Par exemple, une grande entreprise peut déployer 4 centres de données stratégiques pour couvrir le monde entier (deux en Amérique du Nord, un en Europe et un en Asie) et exiger que toutes ses filiales s'y connectent. L'ajout d'un cinquième ou d'un sixième site représente un coût prohibitif, ce qui crée un plafond de couverture. Dans ce contexte, l'entreprise se résigne souvent à un routage sous-optimal jusqu'à ce qu'elle puisse justifier l'ouverture d'un nouveau centre de données pour alléger la charge.

Le plafond de couverture implique que seule une partie des collaborateurs bénéficie d'un point de sortie proche, tandis que les autres doivent composer avec une latence plus ou moins importante. Plus un utilisateur ou une filiale est éloigné du centre de données, plus l'impact sur les performances est notable, ce qui devient particulièrement problématique pour une main-d'œuvre mobile.



Le décompte le plus récent est disponible à l'adresse https://trust.netskope.com/

Fournisseurs de services SASE

Avec le SASE, la responsabilité de la couverture réseau et de son provisionnement est transférée au fournisseur, qui déploie une infrastructure étendue pour ses clients. Cette approche permet de dépasser les limitations liées au plafond de couverture, car un fournisseur SASE opère généralement dans un plus grand nombre de régions que n'importe quelle entreprise. Par conséquent, l'organisation bénéficie d'une couverture mondiale bien supérieure à ce qu'elle pourrait avoir à elle seule, sans avoir à gérer directement des centres de données dans le monde entier.

3E PRINCIPE : REMPLACEZ LES INTERCONNEXIONS CLOUD

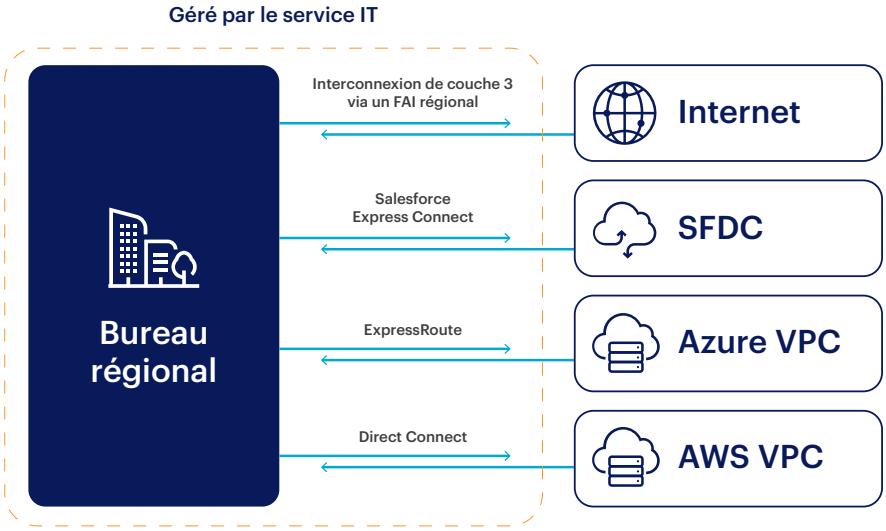
Les services réseau utilisés par les entreprises pour se connecter à Internet, créer leur réseau étendu (WAN) et accéder au cloud dépendent des fournisseurs locaux. Cependant, ces services varient considérablement à travers le monde. D'un marché à l'autre, les fournisseurs varient, les niveaux de service diffèrent et les écarts de prix créent des contraintes à la fois techniques et financières. Ces disparités limitent la capacité des organisations à étendre efficacement leur réseau sur différentes zones géographiques.

La connexion à Internet reste l'option la plus économique, mais elle n'offre ni la fiabilité ni la confidentialité d'une liaison dédiée. Avec la généralisation du cloud, de plus en plus d'applications stratégiques se trouvent hors du réseau de l'entreprise. Face à l'incertitude liée à l'utilisation d'Internet pour accéder à ces services, les interconnexions cloud, comme ExpressRoute pour Azure, Direct Connect pour AWS ou Express Connect pour Salesforce, se sont imposées comme des solutions privilégiées, qui permettent d'assurer une connectivité plus stable et sécurisée pour les applications stratégiques.

L'objectif initial était de créer une continuité entre le cloud et le centre de données, en adoptant un modèle similaire à celui des communications entre les centres de données.

La première vague d'interconnexions cloud a ouvert la voie à l'architecture hybride, où le cloud public devient un prolongement naturel du centre de données local disponible via un cloud privé. L'objectif initial était de créer une continuité entre le cloud et le centre de données, en adoptant un modèle similaire à celui des communications entre les centres de données.

Avec le temps, l'usage des interconnexions cloud s'est élargi. Par exemple, Salesforce est devenu aussi stratégique qu'une application sur site pour les entreprises qui gèrent leurs interactions clients, et qui ont donc besoin d'une liaison dédiée pour garantir rapidité et fiabilité sur le réseau étendu. Cependant, les organisations utilisent une multitude d'applications SaaS, qui jouent un rôle stratégique. La question se pose alors : quelles sont celles qui nécessitent une interconnexion dédiée et celles qui peuvent fonctionner via l'Internet public ? La couverture mondiale complique encore ce problème. Si un bureau régional ne dispose pas d'une option locale pour une interconnexion cloud, l'entreprise doit-elle rediriger son trafic en interne vers un site équipé ou opter pour une connexion directe via Internet ?



Interconnexion cloud traditionnelle, gérée par le service IT sur des liaisons dédiées à haute disponibilité

L'argument de la sécurité est souvent avancé pour justifier l'ajout de liaisons d'interconnexion cloud. Par exemple, grâce à l'acheminement de la totalité du trafic d'une application via une liaison dédiée, l'accès direct à Internet peut être éliminé pour réduire l'exposition des comptes sans préauthentification ou les tentatives d'accès à l'aide d'identifiants compromis. Lorsque le trafic provient exclusivement du réseau étendu interne plutôt que d'Internet, le niveau de sécurité de l'application devient au moins équivalent à celui du réseau étendu lui-même.

Cette sécurité reste toutefois relative, car un acteur malveillant présent sur le réseau étendu peut toujours se déplacer latéralement jusqu'à l'interconnexion cloud. Pour renforcer la protection, de nombreuses entreprises ont complexifié leur architecture en ajoutant des hôtes bastion en amont de l'interconnexion et en imposant aux utilisateurs externes de passer par un VPN avant d'y accéder.

Nous savons désormais que relier le WAN au cloud via des interconnexions n'offre ni une solution évolutive ni une approche optimale sur le plan architectural. Une alternative plus efficace consiste à s'appuyer sur la couche SASE, qui intègre à la fois la sécurité et le réseau au niveau applicatif. Cette approche garantit un accès performant et sécurisé aux applications cloud, quel que soit l'endroit où elles sont hébergées dans le monde.

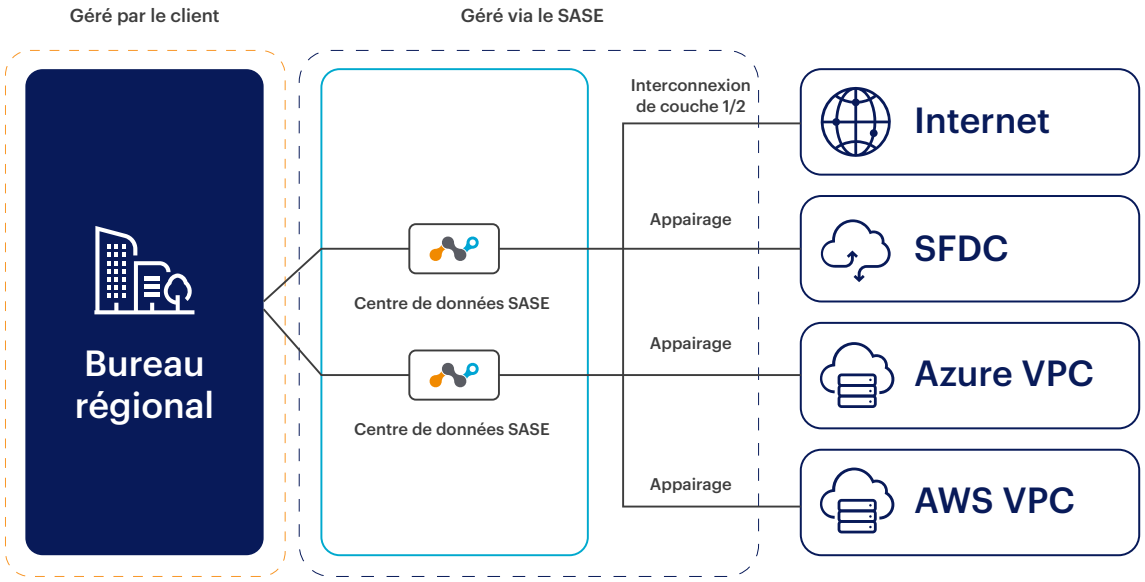
Avec la généralisation du cloud, de plus en plus d'applications stratégiques se trouvent hors du réseau de l'entreprise.

Utiliser le peering SASE comme alternative aux interconnexions cloud

Plutôt que d'investir dans des interconnexions cloud auprès de nombreux fournisseurs de services régionaux, pensez à utiliser l'interconnexion directe SASE avec les fournisseurs cloud pour un accès fiable, sécurisé et à faible latence aux applications cloud. Vous pourrez ainsi réduire considérablement les coûts et la complexité en déléguant la gestion de l'architecture des services au fournisseur SASE.

Tous les fournisseurs SASE ne se valent pas sur ce point. Par exemple, certains optimisent uniquement le temps de traitement à l'intérieur de leurs propres centres de données, sans prendre en compte le temps de transit global jusqu'à l'utilisateur final. Par conséquent, toutes les sorties d'un centre de données SASE n'offrent pas les mêmes performances. Vous devez donc choisir un fournisseur qui optimise à la fois la sécurité et la performance du réseau.

Lorsqu'elle est bien mise en œuvre, cette approche permet aux services IT d'acheminer le trafic vers le centre de données d'un fournisseur SASE afin de tirer parti de ses interconnexions et de son interconnexion directe avec les principaux fournisseurs cloud et le reste d'Internet. Cette stratégie garantit une couverture étendue et des performances constantes. Elle évite également les fluctuations habituelles rencontrées avec les fournisseurs de services réseau régionaux.



4E PRINCIPE : SUPPRIMEZ LA CONFIANCE IMPLICITE

La sécurité périmétrique établit une séparation entre les entités externes non fiables d'Internet et les ressources internes de l'entreprise. Ce modèle reste pertinent pour une segmentation de niveau élémentaire (interne contre externe), car il permet d'appliquer des stratégies de contrôle aussi bien sur les interactions entre les utilisateurs externes et les ressources internes que sur celles des utilisateurs internes qui accèdent à des services externes.

Cependant, une fois qu'un utilisateur a franchi le périmètre, les contrôles d'accès aux ressources internes sont souvent limités. Le réseau interne repose alors sur un niveau de confiance implicite excessif, qui suppose que tous les utilisateurs internes sont « dignes de confiance ». Or, cette confiance est purement présumée et non garantie, ce qui crée une faille de sécurité potentielle. Rien n'empêche qu'un utilisateur interne, intentionnellement ou non, puisse compromettre l'entreprise.

Pour remédier aux problèmes liés à la confiance implicite, de nombreuses entreprises ont intégré diverses technologies de sécurité directement dans le réseau afin d'en renforcer le contrôle :

1. Le NAC pour renforcer l'authentification des appareils et appliquer des stratégies de contrôle d'accès au niveau L2
2. Les VPN pour connecter des appareils distants au réseau local par l'intermédiaire d'un tunnel
3. La segmentation du réseau pour une séparation élémentaire des différentes fonctions et zones de sécurité, comme la distinction entre le centre de données et le réseau local, ou encore entre un serveur web et un serveur de base de données
4. Les réseaux virtuels ou VLAN pour assurer une séparation logique des groupes fonctionnels au sein du réseau, par exemple en isolant le service marketing du service comptabilité
5. Des stratégies de contrôle des hôtes pour vérifier la configuration des appareils et le niveau des correctifs
6. Une authentification à deux facteurs pour réduire le risque posé par le vol d'identifiants

Bien que ces technologies visent à réduire la confiance implicite, elles ajoutent un niveau de complexité important au réseau sans éliminer totalement les risques de sécurité. Pire encore, certaines failles persistent. Par exemple, si l'authentification des appareils et les stratégies d'identification des utilisateurs sont appliquées séparément, un appareil contrôlé à distance peut toujours scanner les ports du réseau et identifier des serveurs vulnérables, même sans aucun identifiant. De plus, de nombreuses solutions, comme le NAC ou les VPN deviennent inefficaces lorsqu'il s'agit d'accéder aux applications cloud.

Cette démarche permet non seulement d'améliorer la sécurité, mais aussi de simplifier et d'optimiser le fonctionnement du réseau à plusieurs égards.

Aujourd'hui, nous savons parfaitement qu'ajouter toujours plus de sécurité ne suffit pas pour éliminer la confiance implicite. La véritable solution consiste à concevoir le réseau dès le départ pour qu'aucune confiance implicite ne subsiste. Cette démarche permet non seulement d'améliorer la sécurité, mais aussi de simplifier et d'optimiser le fonctionnement du réseau à plusieurs égards.

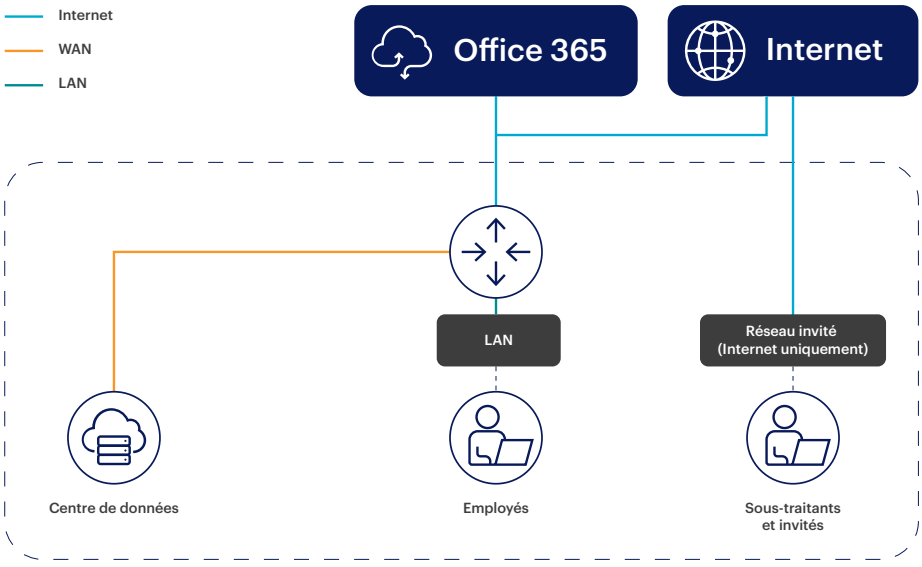
- Les règles de sécurité peuvent être gérées directement au niveau de la couche de protection, sans avoir besoin d'intégrer les mécanismes d'autorisation dans l'infrastructure réseau.
- Le réseau est plus fiable lorsqu'il y a moins d'équipements ou de services de sécurité à gérer.
- De multiples connexions sortantes vers plusieurs réseaux et applications peuvent être centralisées via un point d'accès unique menant à la couche de sécurité.
- De multiples points d'entrée peuvent être éliminés afin de minimiser les vulnérabilités et de réduire les risques liés aux mauvaises configurations, aux stratégies de sécurité mal déployées ou au vol d'identifiants.

Les équipes chargées des réseaux peuvent prendre des mesures pour éliminer les sources de confiance implicite :

- Moderniser le réseau local pour réduire ou éliminer l'accès externe et ne pas accorder de droits supplémentaires aux connexions internes
- Acheminer tout le trafic des applications gérées via SASE
- Contrôler l'accès et renforcez l'authentification / identification via SASE sans utiliser les technologies NAC, 802.1X ou VPN
- Repenser la DMZ

Moderniser le réseau local

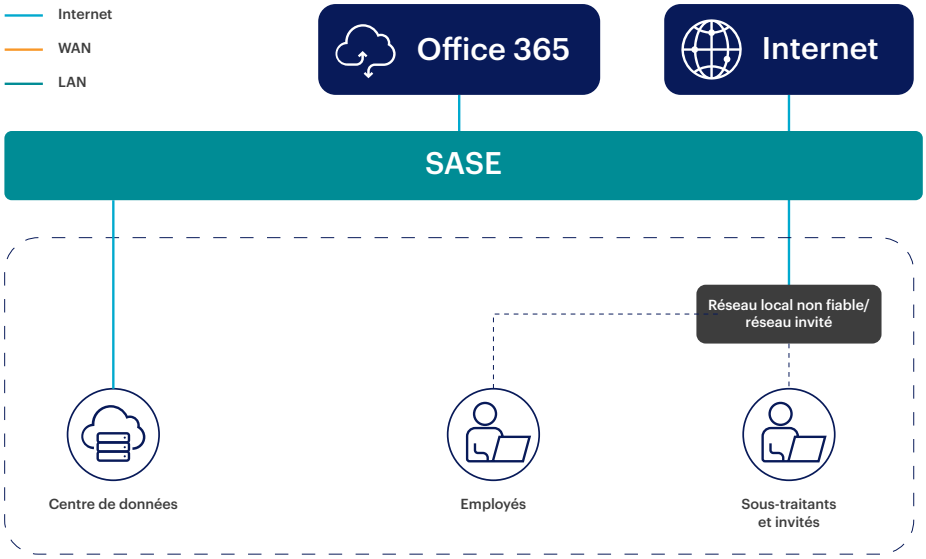
Le réseau local permet aux appareils internes d'accéder au réseau et au centre de données de l'entreprise, mais il demeure une source majeure de confiance implicite. Pendant des années, la seule véritable barrière de protection reposait sur le contrôle physique des accès, assuré par un lecteur de badge et un accueil sécurisé. Une fois à l'intérieur du bâtiment, un appareil pouvait se connecter au réseau local avec des droits souvent bien supérieurs aux besoins réels de l'utilisateur. Bien que des mesures aient été prises pour mieux contrôler les accès, de nombreux réseaux d'entreprise restent très vulnérables aux attaques internes, qu'elles proviennent d'un collaborateur malveillant ou d'un attaquant exploitant un appareil compromis. Une fois connecté au réseau local, un intrus rencontre peu d'obstacles pour cartographier l'infrastructure, identifier des cibles vulnérables et compromettre d'autres systèmes.



Les accès étendus au réseau local sont-ils toujours indispensables de nos jours ? Autrefois, le réseau local était indispensable pour accéder aux applications hébergées dans le centre de données et prendre en charge des fonctionnalités de groupe de travail, comme le partage de fichiers, les outils de collaboration et les communications en temps réel. Aujourd'hui, ces services ont largement migré vers le cloud. L'architecture étendue et permissive du réseau local est donc désormais inutile.

Repenser le réseau local pour le transformer en un réseau invité pour tous les utilisateurs

Heureusement, il existe déjà dans de nombreuses entreprises un modèle qui permet d'éliminer la confiance implicite du réseau local : le réseau invité. Traditionnellement conçu pour offrir une connectivité Internet aux visiteurs et sous-traitants, ce réseau ne donne aucun accès direct au centre de données ni aux autres ressources internes.



Aujourd'hui, la majorité des collaborateurs sur site ont uniquement besoin d'une connexion Internet pour accéder à leurs applications. Le développement du travail hybride a réduit la frontière entre bureau et domicile, les outils professionnels étant maintenant accessibles dans le cloud.

Il n'est donc plus nécessaire d'accorder aux utilisateurs un accès plus étendu au réseau simplement parce qu'ils sont au bureau. Avec l'essor du travail hybride, le réseau d'entreprise s'apparente de plus en plus à un espace de travail partagé, où des collaborateurs de différentes organisations utilisent une infrastructure commune, sans aucune confiance implicite entre les hôtes.

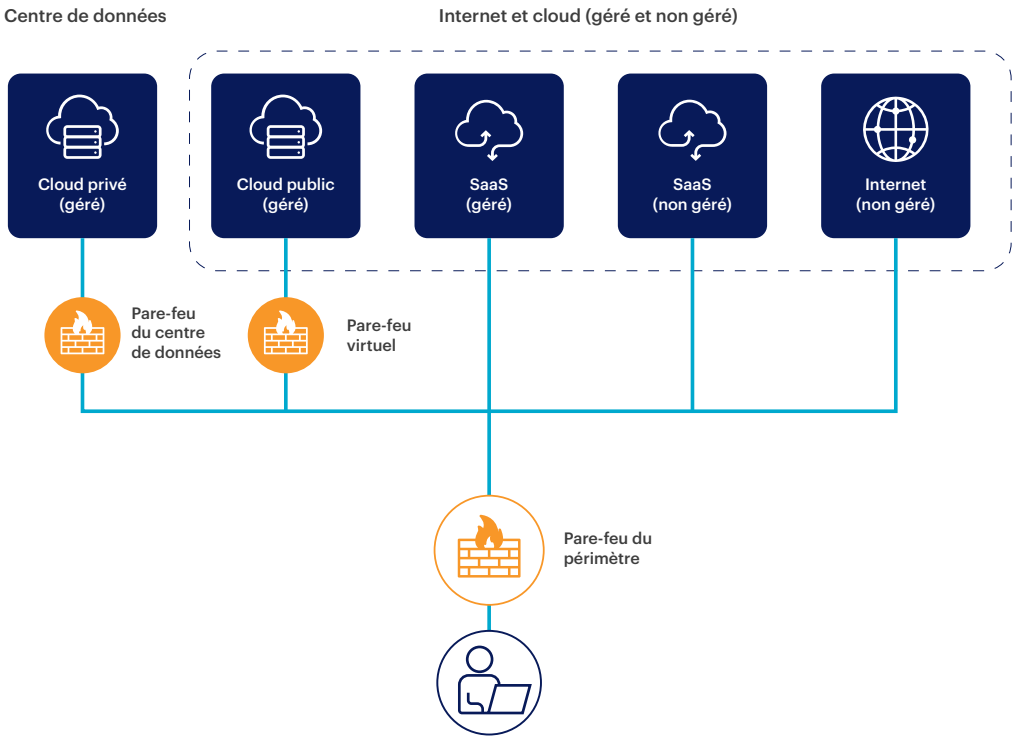
Face à l'essor du télétravail, la frontière entre réseaux sécurisés et non sécurisés devient de plus en plus floue.

Face à l'essor du télétravail, la frontière entre réseaux sécurisés et non sécurisés devient de plus en plus floue. Qu'une collaboratrice travaille depuis chez elle, un café ou un espace de coworking, elle passe la majeure partie de son temps sur des réseaux considérés comme non fiables. Dans ce contexte, le fait de la placer sur un réseau invité ou un réseau local non fiable au bureau ne change rien.

Mélange d'applications gérées et non gérées

Autrefois, le périmètre de sécurité se situait à la frontière entre le réseau fiable et le réseau non fiable. Aujourd'hui, avec la dispersion des données et des applications, ce périmètre s'est déplacé pour contrôler les interactions entre les applications fiables et non fiables. L'enjeu principal n'est plus seulement de protéger le réseau, mais de garantir que les données ne se retrouvent pas dans des environnements où leur sécurité et leur contrôle ne sont plus assurés.

Cependant, les équipements de sécurité traditionnels ne sont pas conçus pour distinguer efficacement une application gérée d'une autre non gérée. Avec l'augmentation des exceptions à la visibilité, cette limitation crée un risque majeur : il devient impossible de différencier les applications autorisées de celles qui ne le sont pas, et aucun contrôle efficace n'est en place pour empêcher les déplacements indésirables de données.



Utiliser le SASE comme périmètre pour les applications gérées

Vous devez d'abord vous concentrer sur les besoins réels en sécurité des applications gérées et sur leur emplacement avant de chercher à rediriger tout le trafic vers le pare-feu du centre de données.

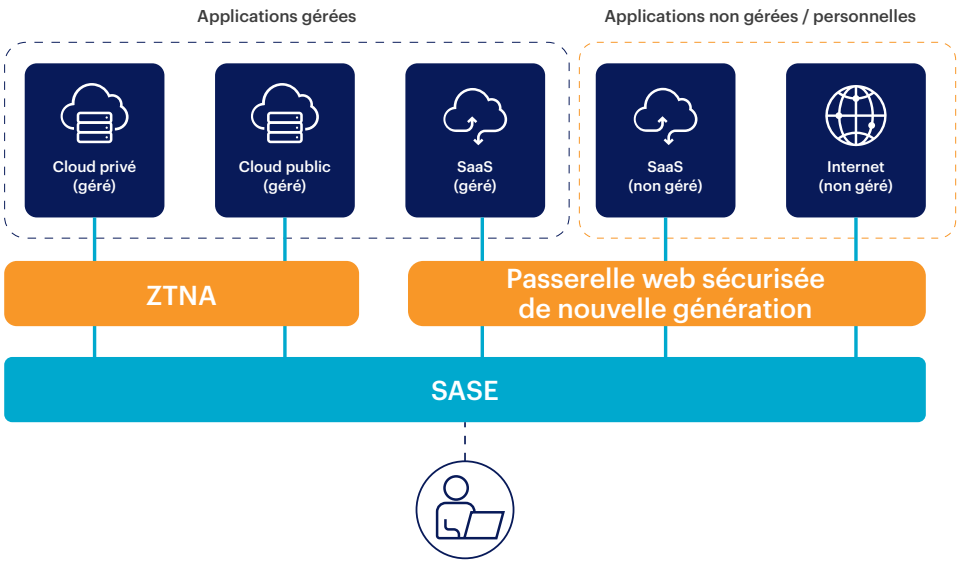
Par exemple, en classifiant les applications comme gérées ou non gérées, il devient évident que les services de sécurité doivent être déployés sur le centre de données, le cloud public et les applications SaaS.

Avec l'augmentation des exceptions à la visibilité, cette limitation crée un risque majeur : il devient impossible de différencier les applications autorisées de celles qui ne le sont pas, et aucun contrôle efficace n'est en place pour empêcher les déplacements indésirables de données.

Exemple de mappage : applications gérées et non gérées

TYPE D'APPLICATION	EMPLACEMENT	EXEMPLE D'APPLICATIONS	PRINCIPALES EXIGENCES DE SÉCURITÉ
APPLICATIONS GÉRÉES	Centre de données	Base de données Oracle	• Accès sécurisé • Protection des données • Analyse comportementale
	Cloud public	AWS / Azure	
	Saas	Office 365 Google Workspace Salesforce Workday GitHub	
APPLICATIONS NON GÉRÉES / PERSONNELLES	Saas	Microsoft 365 Google Workspace Dropbox Zippyshare	• Évaluation des risques • Règles basées sur les risques • Détection d'instance • Protection contre les menaces • Protection des données • Analyse comportementale • Encadrement des utilisateurs finaux
	Internet	Web Non web (FTP, SSH, RSH, etc.)	

La meilleure approche consiste à contrôler les données dans les applications gérées et à déployer la sécurité là où elle est nécessaire. Grâce à l'acheminement de toutes les applications gérées via SASE, vous pouvez appliquer des contrôles d'accès sécurisés, une protection des données et une analyse comportementale en temps réel. Parallèlement, tout le reste du trafic applicatif peut être considéré comme non géré ou personnel, avec des règles spécifiques pour empêcher le déplacement de données non autorisé.



Contrôler l'accès et renforcer l'authentification / identification via le SASE sans utiliser les technologies NAC, 802.1X ou VPN

L'intégration de l'identité et des réseaux a toujours été semée d'embûches. Aujourd'hui, les réseaux appliquent des stratégies d'identité à différentes couches de la connexion, mais sans réelle coordination entre elles. Chaque mesure de sécurité fonctionne de manière indépendante, comme une porte qui autorise l'accès sans savoir quels contrôles ont été appliqués avant ou après la vérification. Par exemple, le NAC peut décider si un appareil est autorisé à accéder à la couche d'accès réseau. Cependant, au niveau de la couche 2, il ne peut pas déterminer si l'utilisateur de cet appareil a le droit d'accéder à une application particulière. Le NAC peut donc confirmer qu'un appareil est autorisé à accéder au réseau, mais il ne peut pas déterminer ce qu'il est en droit d'y faire.

En effet, ces technologies tentent de réduire la confiance implicite en ajoutant des barrières supplémentaires aux ressources protégées, mais elles présentent plusieurs limites :

1. Tout niveau d'accès non contrôlé expose le réseau aux abus. Par exemple, le fait d'être connecté sans authentification ouvre la porte à la surveillance, au balayage des ports d'autres hôtes, à l'exploitation de logiciels non corrigés, au vol d'identifiants et aux attaques préauthentification sur des systèmes vulnérables.
2. Les contrôles d'identité au niveau du réseau deviennent inutiles si ni l'utilisateur ni l'application ne s'y trouvent. Acheminer le trafic via le réseau uniquement pour appliquer ces contrôles est inefficace. Il est donc essentiel de concevoir des contrôles d'identité qui sécurisent les applications gérées, peu importe où se trouvent les utilisateurs.

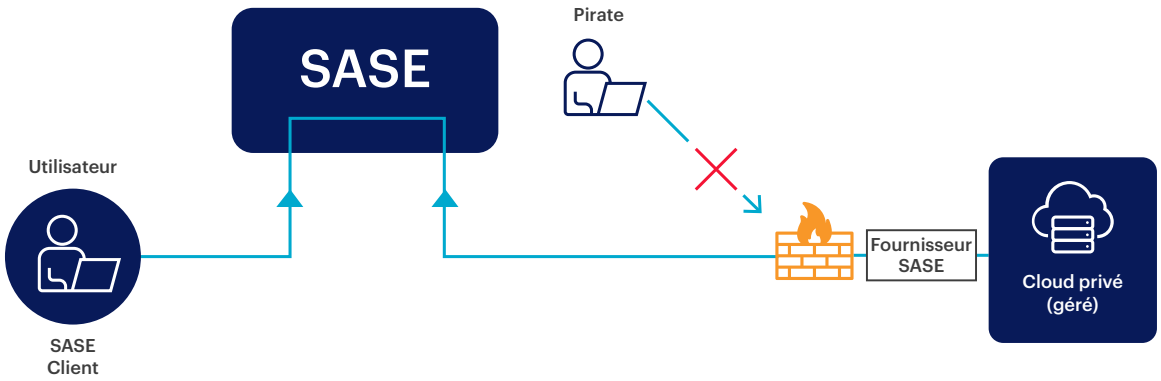
Utiliser le SASE pour appliquer des règles basées sur l'identité

Au lieu de restreindre les connexions réseau à une application spécifique, il est plus efficace d'adopter l'accès réseau Zero Trust (ZTNA). Cette approche établit des connexions basées sur l'identité pour assurer un contrôle précis de l'accès entre l'utilisateur et l'application grâce à l'infrastructure SASE.

Comme mentionné précédemment, limiter la confiance accordée au réseau local (LAN) interne réduit considérablement la surface d'attaque. Il n'y a pas lieu de réutiliser la confiance implicite lorsque l'accès des utilisateurs est uniquement limité à Internet, sans routage interne vers les applications gérées.

La superposition du SASE sert de pont entre les utilisateurs et les applications, ce qui facilite la mise en œuvre du ZTNA. Ce modèle ne se contente pas de vérifier l'identité et d'appliquer les stratégies d'accès, il établit également une connexion sécurisée en reliant deux flux sortants. L'un des grands avantages de l'accès réseau Zero Trust est la simplification des stratégies de pare-feu au niveau du centre de données. Du côté des applications, il suffit de bloquer tout le trafic entrant. Avec cette approche, il n'y a plus de passerelle à sonder, plus de serveur exposé et plus de ports ouverts à balayer. En l'absence de trafic entrant, la surface d'attaque disparaît.

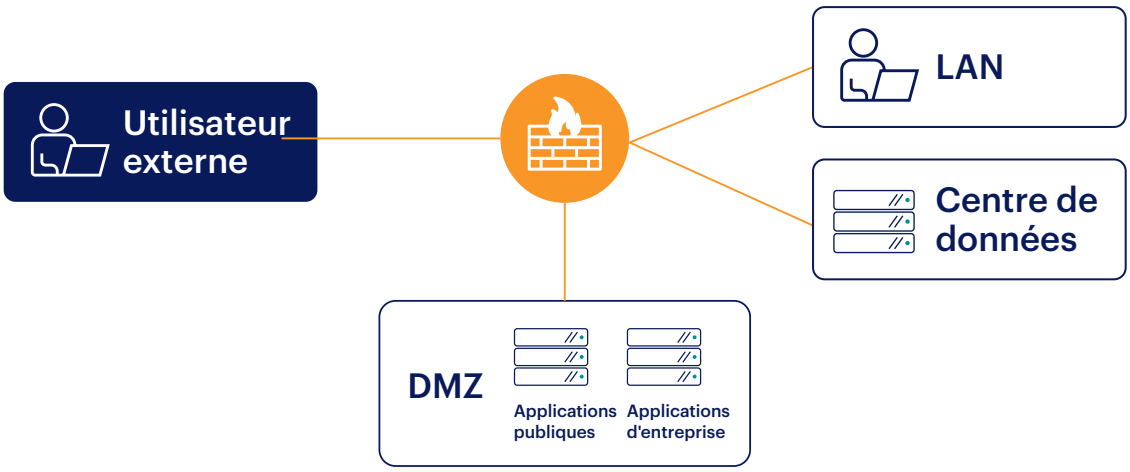
L'un des grands avantages de l'accès réseau Zero Trust est la simplification des stratégies de pare-feu au niveau du centre de données.



Repenser la DMZ

La zone démilitarisée (DMZ) a longtemps permis d'exposer certaines ressources internes à Internet, mais est-elle encore indispensable aujourd'hui ? Autrefois, elle offrait une solution utile, mais imparfaite, pour connecter un réseau géré à Internet afin de répondre à plusieurs besoins, notamment :

- **Pour les applications personnalisées publiques :** les serveurs web et les serveurs d'applications placés dans la DMZ étaient accessibles au public.
- **Pour les applications d'entreprise utilisées par les collaborateurs et les sous-traitants :** applications exécutées dans la zone démilitarisée (DMZ) ou qui offrent un accès limité au centre de données.



Cependant, la zone démilitarisée (DMZ) représente un point de vulnérabilité majeur. En effet, celle-ci crée une exposition directe aux menaces, car elle permet au public d'interagir avec des serveurs qui ont accès à des ressources internes. La moindre faille de sécurité ou erreur dans la configuration d'une stratégie d'accès publique peut servir de porte d'entrée à une cyberattaque. Les organisations doivent donc investir des capitaux importants pour configurer et gérer la DMZ :

- Une ou plusieurs paires de pare-feux à haute disponibilité sont nécessaires pour structurer le réseau DMZ
- Équilibreurs de charge pour gérer et distribuer le trafic légitime
- Mise en place d'un filtrage DDoS à la fois au niveau du réseau et en amont, afin de bloquer les tentatives de saturation des interfaces des serveurs hébergés dans la DMZ
- Prévention des intrusions pour empêcher les tentatives d'exploitation d'une vulnérabilité non corrigée
- Pare-feux applicatifs pour filtrer les entrées malveillantes dans les applications, telles que les injections SQL et les scripts intersites

Même une DMZ bien gérée, surveillée en permanence et configurée selon les meilleures pratiques, reste vulnérable. Tout système situé dans cette zone fait partie de la surface d'attaque et est vulnérable aux tentatives d'exploitation par des utilisateurs non authentifiés venant de l'extérieur.

Alternatives à la DMZ en matière d'architecture

Au lieu de continuer à gérer et à sécuriser une DMZ, vous devriez vous demander si vos applications doivent vraiment s'y trouver. L'essor du cloud a profondément transformé le rôle des applications DMZ traditionnelles, notamment celles accessibles au public. Aujourd'hui, des services spécialisés, comme les applications hébergées ou SaaS offrent des fonctionnalités équivalentes, voire supérieures, sans nécessiter la gestion d'un environnement d'exploitation dédié.

Mais qu'en est-il des applications d'entreprise destinées aux collaborateurs et aux sous-traitants ? Si les applications personnalisées peuvent être migrées vers un cloud public ou privé, leur accès nécessite toujours une méthode de connexion exposée au public, comme un VPN, un hôte bastion, un proxy ou un serveur de terminal. Bien que ces solutions aient pour objectif de sécuriser l'accès aux serveurs internes, elles introduisent des passerelles visibles qui restent vulnérables aux balayages de ports, aux erreurs de configuration ou aux exploits ciblés.

L'essor du cloud a profondément transformé le rôle des applications DMZ traditionnelles.

Grâce à l'application des mêmes principes que ceux de l'accès réseau Zero Trust (ZTNA) et du SASE, les entreprises peuvent offrir un accès sécurisé aux applications privées sans avoir recours à une DMZ. Contrairement aux VPN traditionnels, qui établissent une connexion entre l'appareil de l'utilisateur et l'ensemble du réseau de l'entreprise, le ZTNA crée un accès sécurisé uniquement entre l'utilisateur et des applications spécifiques.

Dans un scénario optimal, vous devrez supprimer totalement le trafic entrant afin de maximiser les gains en sécurité et en coûts. Cette approche n'est pas toujours applicable selon les besoins de l'entreprise, mais réduire le nombre de systèmes hébergés dans la DMZ reste une stratégie efficace. En effet, moins de ressources exposées signifient une surface d'attaque réduite et une gestion simplifiée du réseau.

À PROPOS DE LA PLATEFORME NETSKOPE ONE

Netskope One est une plateforme unifiée de sécurité et de gestion réseau en mode service. Grâce à son moteur Zero Trust unique et breveté, ses innovations en IA et son impressionnant cloud de sécurité privé, cette solution offre une protection optimale des données et des opérations tout en garantissant une expérience utilisateur conviviale.

La puissance de Netskope One

Réduisez vos coûts et simplifiez vos opérations grâce à notre solution tout-en-un qui combine un moteur central, une interface unique, une protection renforcée et un cloud privé sécurisé.

Visibilité et protection grâce à l'IA

Grâce à des technologies d'IA brevetées, nous vous permettons d'avoir une vision claire et détaillée de toutes les activités de vos utilisateurs sur le cloud, les applications SaaS et le web. Notre moteur Zero Trust offre une précision et une visibilité exceptionnelles pour détecter les menaces et prévenir les fuites de données en temps réel.

Une expérience utilisateur conviviale

Adoptez un environnement de travail hybride plus performant grâce à une infrastructure cloud privée ultra-sécurisée, reconnue comme la plus rapide et la plus fiable du marché. Optimisez l'expérience utilisateur de bout en bout, de l'application jusqu'aux composants intermédiaires, avec une gestion proactive complète.

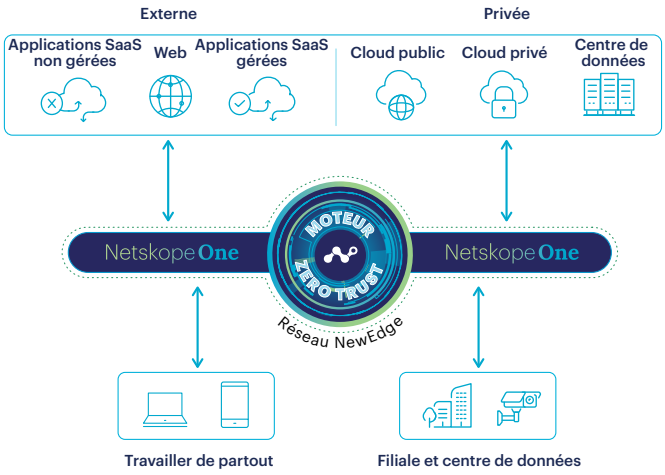
COMPOSANTS DE LA PLATEFORME NETSKOPE ONE

Moteur Zero Trust

La solution Netskope One s'appuie sur un moteur Zero Trust sophistiqué qui adapte intelligemment les niveaux de confiance. Grâce à l'évaluation constante des risques associés aux utilisateurs, appareils, applications, échanges et données, il offre une protection optimale et évolutive. Cette technologie assure ainsi une sécurité rigoureuse sans compromettre la fluidité de l'expérience utilisateur.

Réseau NewEdge

Netskope NewEdge propose une infrastructure cloud privée de sécurité inégalée, avec des centres de données haute performance répartis dans le monde entier. Son architecture permet une connexion directe des utilisateurs et des sites au système Zero Trust, tout en tirant parti de solides partenariats avec les grands acteurs du web et du cloud. Les utilisateurs profitent ainsi d'une expérience optimale, à la fois fluide et rapide, quelle que soit leur localisation.



Netskope One Client

Netskope One Client se démarque comme la première solution SASE du marché qui réunit en un seul outil l'accès distant aux ressources web, clouds et applications internes. En plus d'intégrer les fonctionnalités de protection des données (DLP) et de SD-WAN pour les terminaux, cet outil propose une solution tout-en-un pour répondre aux besoins SASE et Zero Trust. Il facilite ainsi grandement l'administration des postes afin de garantir une meilleure expérience aux utilisateurs.

Netskope One Gateway

Grâce à Netskope One Gateway, la transformation des filiales en sites légers devient simple et efficace. Cette solution propose une connectivité optimale et sécurisée via le Borderless SD-WAN tout en assurant un accès transparent à Intelligent SSE. Elle consolide enfin plusieurs équipements distincts en une seule solution intégrée.

Utiliser Netskope pour votre réseau de demain

Netskope SASE permet aux entreprises de créer leur réseau de demain en appliquant les principes détaillés dans ce guide. Cette solution intègre des services réseau et de sécurité pour garantir une couverture complète, quel que soit l'endroit où l'entreprise opère. Le cloud privé Netskope NewEdge se trouve au cœur de cette solution. Il représente l'infrastructure de sécurité privée la plus importante et la plus performante au monde, qui alimente également la plateforme Netskope One. Conçu par des experts ayant contribué au déploiement et à l'évolution des plus grands services cloud et réseau de diffusion de contenu, NewEdge repose sur une architecture hyperscale optimisée pour le SASE. Cette approche offre aux entreprises une couverture étendue, des performances exceptionnelles et une résilience incomparable.

Grâce à l'intégration de toutes ces capacités de traitement et de ces fonctionnalités de sécurité dans plus de 75 régions et 100 centres de données (depuis août 2024), NewEdge assure des performances optimales sans compromis. Cette approche permet de déployer la sécurité au plus près des collaborateurs et des appareils, sans dépendre de points de présence virtuels ni du backhauling. Résultat ? Une connectivité accélérée vers toutes les applications et une expérience utilisateur optimale.

Notre modèle de service cloud offre un traitement du trafic ultrarapide avec une disponibilité exceptionnelle. Grâce à un SLA de 99,999 %, nous garantissons un accès continu à nos services en ligne. Netskope surprovisionne massivement le réseau NewEdge, capable d'atteindre 2 térabits par seconde dans chaque centre de données et plus de 100 térabits par seconde à l'échelle mondiale. Cette architecture fait partie intégrante de la conception de NewEdge. Elle a pour objectif de permettre aux entreprises de simplifier leur réseau.

L'approche SASE, telle qu'elle est proposée par Netskope, offre un certain nombre d'avantages par rapport aux réseaux d'entreprise traditionnels :

Avantages des réseaux

1. **Simplification des opérations :** si vous confiez la gestion de votre réseau back-end à Netskope, votre organisation n'aura plus qu'à gérer les tunnels vers le centre de données NewEdge. Cette opération est d'autant plus simple grâce à Netskope Client qui gère automatiquement les connexions aux tunnels pour les utilisateurs. De plus, le Borderless SD-WAN assure et optimise en permanence la connectivité des utilisateurs et des sites grâce à des stratégies personnalisées.
2. **Hauts débits :** grâce à NewEdge, votre organisation bénéficie d'une connectivité cloud inégalée et d'un réseau haute performance, sans avoir à rediriger le trafic vers le centre de données de l'entreprise pour la sortie.
3. **Couverture étendue des applications cloud :** la plupart des organisations gèrent un nombre limité d'interconnexions cloud. Par exemple, une société qui utilise AWS peut choisir Direct Connect pour répondre aux besoins de son équipe de développement, tout en se contentant d'une connexion Internet standard, moins fiable, pour accéder à d'autres clouds ou applications SaaS. Netskope offre une solution plus complète pour l'accès aux applications cloud, alliant performance, sécurité et stabilité.
4. **Couverture géographique étendue :** le service Internet reste fragmenté à l'échelle mondiale, avec des débits variables et une qualité de service imprévisible selon les fournisseurs et les régions. Pour améliorer leur connectivité globale, les entreprises peuvent s'appuyer sur NewEdge comme point d'entrée.
5. **Recours à un seul fournisseur :** selon la région, les fournisseurs diffèrent, ce qui rend la tâche plus difficile pour les entreprises qui doivent gérer leurs réseaux. La qualité du service fluctue considérablement, y compris dans une zone géographique donnée, particulièrement dans des territoires aussi variés que l'Europe ou l'Amérique du Sud. Grâce à Netskope, les entreprises offrent une expérience utilisateur optimale dans le monde entier, sans avoir à gérer plusieurs fournisseurs dans chaque région.
6. **Une meilleure sécurité :** grâce à Netskope, les entreprises peuvent optimiser leur protection au lieu de jongler avec une multitude d'équipements réseau et d'exceptions aux règles de sécurité. Netskope SASE propose une solution complète de sécurité qui regroupe plusieurs fonctionnalités essentielles : la protection contre les menaces, la protection des données et l'accès réseau Zero Trust, le tout sous forme de services unifiés. Grâce au regroupement de ces mesures de sécurité sur Netskope, les entreprises peuvent gérer leur réseau plus facilement et réduire leur surface d'attaque, comme l'explique ce guide.

Pour en savoir plus sur Netskope, rendez-vous sur http://www.netskope.com. Suivez également cette série pour obtenir d'autres informations sur la création du réseau de l'avenir.

INDEX

[1] « CIOs, CTOs and technology leaders: Latest findings from PwC's Pulse Survey », PwC, 27 janvier 2022.

[2] « Gartner, Hype Cycle™ for Cloud Security, 2021 », par Tom Croll et Jay Heiser, 27 juillet 2021.

[3] « Cloudy With a Chance of Malice », Netskope, 23 février 2021.

[4] « Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025 », Statista, 18 mars 2022.

[5] « 40% of organizations have suffered a cloud-based data breach », Security Magazine, 29 octobre 2021.

[6] « A Stanford Economist Who Studies Remote Work Says Half of All Workers Will Make This Big Change in 2022 », Inc., 8 janvier 2022.

Vous souhaitez en savoir plus ?

Demander une démo

Netskope, un leader de la sécurité et des réseaux modernes, répond aux besoins des équipes de sécurité et de mise en réseau en fournissant un accès optimisé et une sécurité contextuelle en temps réel pour les utilisateurs, les appareils et les données, où qu'ils se trouvent. Des milliers de clients, dont plus de 30 parmi les entreprises du Fortune 100, font confiance à la plateforme Netskope One, à son moteur breveté Zero Trust Engine et à son puissant réseau NewEdge pour réduire les risques et obtenir une visibilité et un contrôle complets sur l'activité du cloud, du SaaS, du web et des applications privées, en assurant la sécurité et en accélérant les performances, sans sacrifice ni compromis. Pour en savoir plus, rendez-vous sur netskope.com.