Proposé par :

netskope

Réseau SD-WAN moderne avec SASE

pour les nuls
A Wiley Brand

Connectez, optimisez et sécurisez tout

Fournissez une politique et une expérience cohérentes partout

Surveillez les réseaux en temps réel avec l'AIOps

Édition spéciale Netskope

Muhammad Abid
Parag Thakore

À propos de Netskope

Netskope, leader mondial dans le domaine du SASE, accompagne les organisations dans l'intégration harmonieuse de leur réseau et de leur sécurité. L'entreprise met l'accent sur l'utilisation de l'AIOps, l'application des principes Zero Trust, ainsi que sur l'exploitation des innovations en IA/ML, afin de sécuriser les données tout en assurant une connectivité haute performance et une protection exhaustive contre les menaces. Grâce à sa plateforme rapide et conviviale, Netskope offre un accès sécurisé et en temps réel aux utilisateurs, aux appareils et aux données, où qu'ils se trouvent. Avec Netskope, les clients bénéficient d'une réduction des risques, d'une amélioration des performances et d'une visibilité inégalée sur l'activité de toutes les applications cloud, web et privées. Des milliers de clients font confiance à Netskope et à son puissant réseau NewEdge pour faire face à l'évolution des menaces, aux nouveaux risques, aux changements technologiques, aux changements organisationnels et réseau, ainsi qu'aux nouvelles exigences réglementaires. Pour découvrir comment Netskope accompagne ses clients tout au long de leur parcours SASE, visitez le site netskope.com.

Nous tenons à remercier un certain nombre de personnes qui ont rendu possible la publication de ce livre :

Chez Netskope : Amanda Anderson, Robert Arandjelovic, Madhavan Arunachalam, Chad Berndtson, Jason Clark, Fan Gu, Kathy Jacobsen, Jessica Jostes, Naveen Palavalli, Gerry Plaza, Carolyn Robinson, James Yokota

Chez Evolved Media : Shay Ben-Dov, Theresa Ingles, David Penick, Karen Queen, Vincent Rossmeier, Evan Sirof, Lauren Wagner, Dan Woods

Réseau SD-WAN moderne avec SASE

pour les nuls®

Réseau SD-WAN moderne avec SASE

Édition spéciale Netskope

par Muhammad Abid et Parag Thakore

pour les nuls®

Réseau SD-WAN moderne avec SASE pour les Nuls®, Édition spéciale Netskope

Publié par
John Wiley & Sons, Inc.
111 River St., Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-21945-2 (pbk) ; ISBN 978-1-394-21946-9 (ebk)

Remerciements de l'éditeur

Cet ouvrage a été réalisé avec la participation des personnes suivantes :

Éditeur : Elizabeth Kuball

Rédacteur chargé des acquisitions : Traci Martin

Responsable éditorial : Rev Mengle

Responsable de compte client : Jeremith Coward

Éditeur de production : Saikarthick Kumarasamy

Assistance spéciale : Nicole Sholly

Table des matières

Introduction

Depuis des années, les réseaux informatiques sont le moteur de nos entreprises, dynamisent nos communautés et enrichissent notre quotidien. Tandis que l'informatique et le numérique progressent à pas de géant, les infrastructures réseaux de nos entreprises peinent à suivre le rythme. La mise en réseau n'est pas statique ; elle évolue en fonction des besoins des entreprises, des avancées technologiques et de la créativité humaine. Parfois, les réseaux devancent même leurs applications, et à d'autres moments, une technologie obsolète cède la place à des innovations plus actuelles.

Ce livre se penche sur le passé et le futur des réseaux d'entreprise, et vous indique comment rester au diapason dans un monde où le cloud, l'Internet des objets (IoT) et la mobilité sont rois. Bien sûr, les anciennes méthodes de mise en réseau ont eu leurs mérites, mais ces modèles et technologies ne suffisent plus pour les entreprises d'aujourd'hui qui évoluent dans l'ère du sans-frontières.

Il nous faut non seulement un nouveau type de réseau, mais aussi une nouvelle mentalité. Les prouesses techniques ne suffiront pas pour relier des individus équipés d'une panoplie d'appareils à une vaste gamme de destinations et d'applications. Pour un monde hyperconnecté et sans frontières, nous avons besoin d'une vision de réseaux tout aussi illimités.

À propos de ce livre

Le réseau étendu défini par logiciel (SD-WAN) sans frontières, ou *Borderless SD-WAN*, nous offre une architecture réseau plus solide, fiable et efficace, parfaitement adaptée à notre monde actuel, fortement axé sur le cloud et dispersé. Ce livre vous guide pour concevoir un plan d'action afin d'implémenter cette solution réseau adaptée au monde moderne. Et comme cette solution est « définie par logiciel », elle s'adapte facilement aux besoins changeants de votre entreprise. Mieux encore, elle booste votre productivité tout en vous faisant économiser de l'argent.

Quelques suppositions idiotes

Vous avez déjà une bonne idée des bases des réseaux d'entreprise et du rôle central de l'Internet. Il est donc logique que les entreprises délaissent les anciens réseaux WAN MPLS (Multiprotocol Label Switching) au profit des SD-WAN plus modernes. Mais qu'en est-il de la suite ? Avec l'évolution des lieux de travail, l'essor des appareils mobiles et de l'IoT, ainsi que la prolifération des applications SaaS et des services cloud, le paysage change constamment. Il est temps d'arrêter de jouer les seconds rôles avec votre architecture réseau et d'exploiter pleinement le potentiel du Borderless SD-WAN pour vous adapter à ce monde en perpétuel changement.

Icônes utilisées dans ce livre

Nous utilisons des icônes dans la marge pour attirer l'attention sur les informations importantes.

CONSEIL

Tout le contenu en regard de l'icône Conseil est un raccourci pour faciliter une tâche spécifique.

RAPPEL

L'icône Rappel signale les faits qu'il est particulièrement important de connaître.

JARGON TECHNIQUE

Lorsque nous proposons des informations très techniques que vous pouvez ignorer sans risque, nous utilisons l'icône Jargon technique.

ATTENTION

Tenez bien compte de tout ce qui se trouve en regard de l'icône Attention pour vous épargner des maux de tête.

Au-delà de ce livre

Bien que ce livre regorge d'informations, si vous vous retrouvez à la fin à vous demander « Où puis-je en savoir plus ? », rendez-vous sur `www.netskope.com/fr/`.

DANS CE CHAPITRE

- **Suivre l'évolution du réseau étendu (WAN)**
- **Découvrir comment le réseau étendu défini par logiciel (SD-WAN) a amélioré le réseau étendu (WAN)**
- **Comprendre le défi que représente le télétravail pour les réseaux SD-WAN traditionnels**
- **Comprendre pourquoi les réseaux SD-WAN ne parviennent pas à atteindre l'efficacité dont nous avons besoin**

Chapitre 1
Pourquoi les réseaux sont en retard par rapport à l'informatique moderne

L'évolution des réseaux informatiques a traversé plusieurs moments cruciaux : les anciennes solutions sont remplacées par de nouveaux outils. Les réseaux locaux (LAN) ont cédé la place aux réseaux étendus (WAN), qui à leur tour ont remplacé les réseaux étendus définis par logiciel (SD-WAN) ; et maintenant, cette ère des SD-WAN touche à sa fin. À la place, les réseaux Borderless SD-WAN émergent comme la prochaine grande tendance pour les réseaux d'entreprise. Cette évolution permet d'offrir une connectivité « *Anywhere-to-Anywhere* » sécurisée et contextuelle, spécifiquement conçue pour une époque tournée vers le cloud et le travail hybride. Les organisations s'engageant rapidement dans ce processus de modernisation peuvent surpasser leurs concurrents en bénéficiant d'une infrastructure informatique plus souple, plus sécurisée et plus efficace.

Le monde des connexions « One-to-One »

Il y a longtemps, dans un monde très similaire au nôtre, les entreprises devaient toutes survivre dans un environnement statique axé sur le matériel. La mise en réseau a d'abord relié les utilisateurs et les appareils par le biais de réseaux locaux (LAN) à l'intérieur d'un bâtiment : généralement le siège social d'une entreprise ou ses filiales. À l'époque, chaque collaborateur venait au bureau tous les jours. Les réseaux locaux permettaient à toute personne se trouvant au même endroit physique de travailler ensemble sur le même réseau. Toutes les applications destinées à ces utilisateurs devaient être connectées à un centre de données unique, situé dans un endroit précis, et par lequel toutes les activités réalisées sur le réseau transitaient. Cela fonctionnait bien... jusqu'à ce que cela ne soit plus le cas.

RAPPEL

Les réseaux locaux avaient leurs limites, notamment le fait qu'ils exigeaient que tous les utilisateurs se trouvent au même endroit.

Le passage des réseaux locaux (LAN) aux réseaux étendus (WAN) a permis à plus d'appareils d'être répartis dans plus d'endroits, connectés à des centres de données reliés à Internet et protégés par un pare-feu. Chaque appareil se trouvait dans un périmètre physique donnant accès au réseau.

Avec les WAN, les collaborateurs des filiales qui souhaitaient se connecter aux applications de l'entreprise devaient passer par le réseau privé de l'entreprise, généralement via des connexions MPLS (Multiprotocol Label Switching), pour revenir ensuite au centre de données centralisé. Le MPLS est une technologie largement utilisée pour les réseaux privés. Placer des applications dans chaque installation distante était tout simplement trop difficile et peu pratique. La centralisation a permis d'uniformiser le contrôle et la sécurité des applications et du réseau. Ainsi, toutes les filiales ont dû se connecter au centre de données ou au siège social de l'entreprise via le WAN.

Si un accès à Internet était nécessaire, les utilisateurs étaient redirigés vers toutes les applications métiers hébergées sur Internet depuis le bureau central. Cette méthode, appelée *backhauling* ou *hairpinning*, était fastidieuse.

Même les entreprises d'envergure mondiale, y compris les institutions financières internationales, les réseaux de santé comprenant plusieurs hôpitaux et les chaînes de restauration possédant des points de vente, comme Taco Bell ou McDonald's, étaient concernées.

Dans les années 2000, les connexions MPLS ont permis aux opérateurs de faire converger la voix, la vidéo et les données sur le même réseau. Aujourd'hui encore, le MPLS fournit des connexions réseau fiables, soutenues par des accords de niveau de service (SLA), mais il coûte cher et sa

planification et sa mise en service peuvent prendre des mois (voir la figure 1-1).

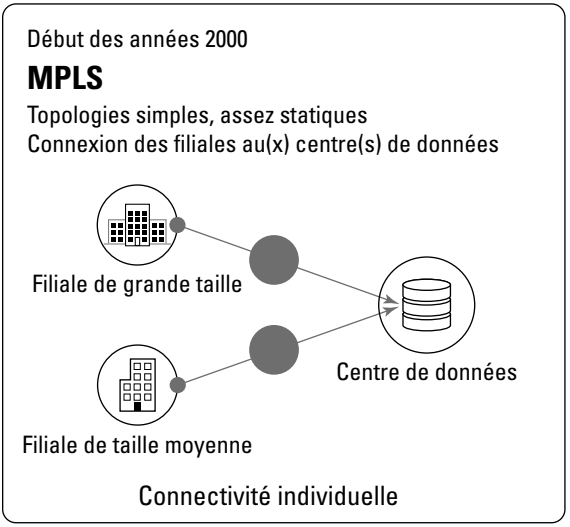


FIGURE 1-1 : Dans le monde des connexions « One-to-One », les filiales utilisent les liaisons MPLS pour se connecter à un emplacement centralisé appelé centre de données, où toutes les applications sont hébergées.

Cependant, lorsque les entreprises ont commencé à utiliser des applications plus immersives comme la vidéo, le protocole MPLS n'a tout simplement pas pu fournir une bande passante suffisante pour les filiales. En outre, le déploiement et la maintenance du MPLS coûtaient cher, et l'utiliser pour satisfaire la demande en bande passante importante liée à la consommation de vidéos s'accompagnait d'un coût prohibitif. Les entreprises étaient donc à la recherche d'une autre solution de transport plus rentable. Elles l'ont découvert sous la forme du protocole bien connu de *transport Internet*.

L'avènement du monde des connexions « One-to-Many »

Le coût de la bande passante MPLS et la lenteur de la mise en service d'un réseau étendu (WAN) ont été les premiers signes que les structures réseau du passé ne répondaient plus aux besoins actuels. Mais, de nombreux autres signes faisaient également leur apparition.

Les entreprises faisaient face à un nouveau défi dans un monde où les logiciels et le stockage ont basculé en ligne, un modèle basé sur le cloud computing et le SaaS (Software-as-a-Service). Elles devaient s'assurer qu'elles pouvaient fournir et garantir des applications – comme Microsoft 365 pour la productivité, Amazon Web Services (AWS) pour la puissance de calcul et le stockage des données, et Google Cloud pour Google Docs et d'autres services cloud – en toute sécurité et avec des performances fiables. Au fur et à mesure que la dépendance envers les applications vidéo immersives basées sur le cloud et le SaaS se développait et que la nature des applications évoluait, l'augmentation de la bande passante MPLS devenait extrêmement coûteuse. Que devaient faire les entreprises ? Elles avaient besoin qu'un héros vêtu d'une armure numérique étincelante arrive rapidement.

Heureusement, le SD-WAN est arrivé juste à temps, offrant la prochaine évolution logique de l'architecture WAN. Le SD-WAN était une technologie moderne qui permettait un contrôle centralisé au sein d'une infrastructure distribuée, résolvant bon nombre des pressions exercées par les applications cloud sur les réseaux étendus traditionnels.

Le SD-WAN promettait de tirer parti d'une variété de canaux différents (MPLS, Internet, cellulaire) et de fournir des performances optimisées sur une ou plusieurs connexions. En faisant abstraction de la couche réseau et en acheminant le trafic sur la base de politiques définies et gérées de manière centralisée, le SD-WAN a optimisé l'acheminement et la hiérarchisation du trafic des applications. Le SD-WAN a assuré la connectivité entre les utilisateurs des filiales, le centre de données et les applications cloud (voir figure 1-2).

Plus précisément, le SD-WAN :

- Permet une connexion sécurisée et chiffrée via l'Internet public, les réseaux cellulaires et les liaisons MPLS vers des applications/données à la fois sur site et dans le cloud
- Permet de connecter un site central, tel qu'un centre de données, à de nombreux sites distribués, tels que des filiales
- Permet aux entreprises d'acheminer et de hiérarchiser le trafic en fonction du type d'application utilisée et des données qu'il contient

Le SD-WAN a donné aux entreprises plus de choix et de contrôle. Il leur a permis d'utiliser le transport par Internet de manière dynamique et efficace, tout en conservant la possibilité d'utiliser des liaisons MPLS si nécessaire. L'utilisation de connexions Internet étant beaucoup moins onéreuse que le MPLS, cette démarche a permis de réduire considérablement les coûts.

L'utilisation du SD-WAN a également apporté des avantages en termes de performances. Bien que l'Internet public puisse parfois être moins

fiable que le MPLS, le SD-WAN dispose de fonctionnalités qui améliorent l'expérience utilisateur et assurent une grande fiabilité. Par exemple, il peut fournir des fonctions de qualité de service (QoS), qui donnent la priorité aux données. Il dispose également de capacités de correction des liaisons, telles que la correction des erreurs de transfert, qui permettent de résoudre les problèmes et d'améliorer la connexion.

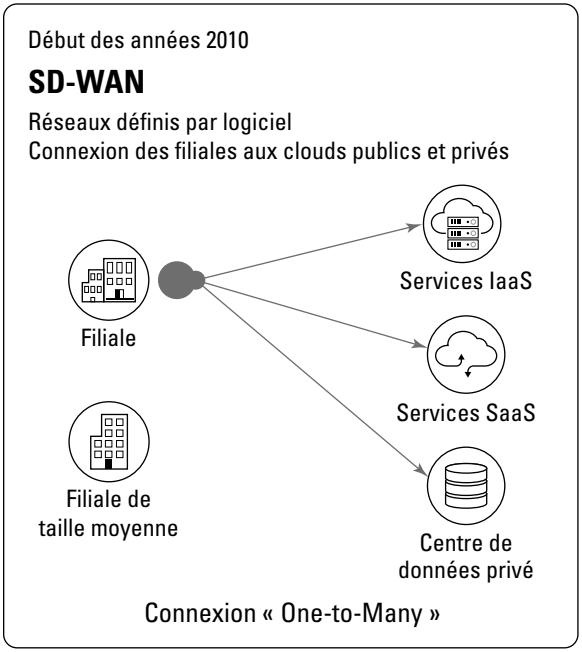


FIGURE 1-2 : Dans le monde des connexions « One-to-Many », les filiales acheminent le trafic non seulement vers le centre de données centralisé à l'aide du protocole MPLS, mais aussi vers de multiples clouds à l'aide du MPLS et de l'Internet via un SD-WAN à faible coût.

Résultat ? Dès que les entreprises ont découvert la puissance et la simplicité des applications SaaS basées sur le web (au lieu de celles résidant dans le centre de données), le retour en arrière est devenu impossible.

On aurait pu penser que cela aurait conduit à un monde utopique dans lequel chaque entreprise serait en mesure d'exploiter pleinement la puissance du cloud grâce à un réseau souple et abordable, n'est-ce pas ?

Cela *aurait pu* être le cas... mais le monde a encore changé.

Le challenge des connexions « Many-to-Many » : le SD-WAN à un carrefour décisif

Aujourd'hui, nous sommes entrés dans une nouvelle ère, celle de l'entreprise sans frontières (voir figure 1-3), dans laquelle les utilisateurs, les appareils, les sites et les clouds sont tous connectés de multiples façons. Le télétravail s'est considérablement développé, nous permettant de quitter l'espace confiné du bureau traditionnel. L'expansion du périmètre réseau de l'entreprise s'illustre par la croissance des micro-filiales, l'adoption du multicloud, la popularité du travail à distance, l'essor de la télésanté, la gestion des flottes mobiles et l'intégration d'appareils liés à l'Internet des objets (IoT).

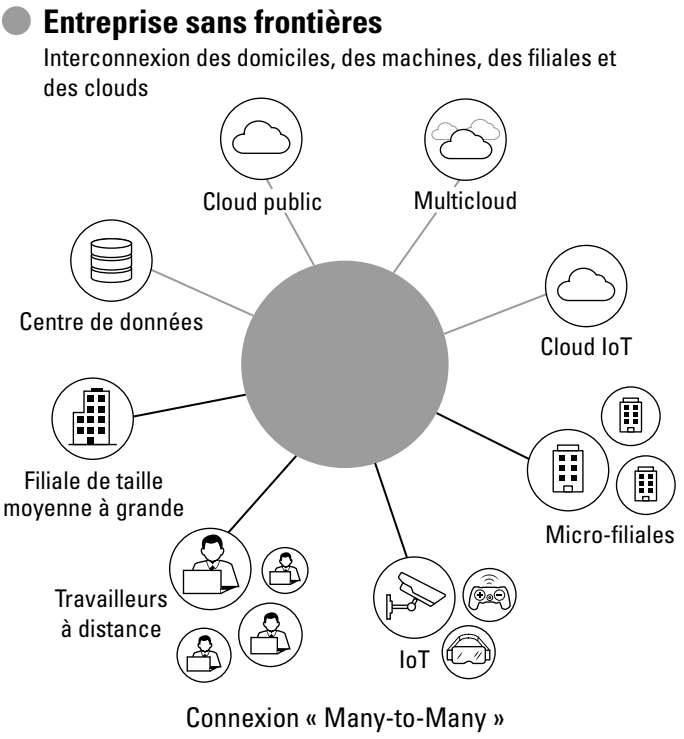


FIGURE 1-3 : Dans l'univers des connexions « Many-to-Many », l'entreprise sans frontières exige une connectivité simple, flexible, sécurisée et performante en tout lieu, englobant diverses filiales, les collaborateurs en télétravail, les appareils IoT, les centres de données et une variété de services cloud.

L'intérêt du SD-WAN résidait dans le fait qu'il permettait à une entreprise de contrôler le trafic des utilisateurs dans les filiales vers les

destinations auxquelles ils souhaitaient se connecter. Mais l'ensemble du système était lié à un ensemble d'hypothèses qui ont commencé à s'effondrer au fur et à mesure que de multiples vagues d'innovation transformaient le monde. Les sections suivantes offrent un aperçu des principales tendances qui ont réduit l'efficacité du SD-WAN.

La prolifération des applications et des appareils IoT

Le SD-WAN traditionnel pouvait prendre en charge quelques milliers d'applications, ce qui était suffisant à ses débuts. Mais avec l'explosion du volume des applications cloud et des appareils IoT, ses capacités ont été remises en question. Le SD-WAN n'a pas été élaboré pour identifier et classer ces applications et appareils innovants selon un contexte approfondi ni pour établir des règles judicieuses les concernant. Il est impossible d'établir des priorités ou de sécuriser ce qui ne peut être compris et classé dans des catégories significatives.

La prolifération des appareils IoT est plus importante que jamais. Les architectures réseau actuelles ne sont pas conçues pour la convergence de l'IoT, de la technologie opérationnelle (OT) et de la technologie de l'information (IT). Le manque de visibilité détaillée et de contrôle précis des appareils IoT présente des risques pour le réseau. Pour cela, une segmentation précise reposant sur l'intelligence artificielle (IA) et l'apprentissage automatique (ML) s'avère indispensable, contrairement à la méthode traditionnelle fondée sur le protocole Internet (IP).

Travail hybride

De nos jours, les personnels ne sont pas confinés aux bureaux des filiales et ne peuvent pas être protégés par les réseaux SD-WAN qui ont été conçus en pensant aux collaborateurs qui se trouvent au bureau. Aujourd'hui, chaque utilisateur et chaque appareil est une filiale à lui tout seul. En outre, suite à la pandémie de COVID-19, l'effectif œuvrant hors des locaux a connu une hausse spectaculaire, dépassant les capacités de gestion initialement prévues pour le SD-WAN. Les collaborateurs s'attendent à une expérience utilisateur de haute qualité et sécurisée, comparable à celle d'un siège social, peu importe où ils travaillent.

Au début de la pandémie, quand les collaborateurs ont dû retourner chez eux, les architectes IT se sont surtout focalisés sur la sécurisation des connexions à distance. Souvent, la planification de l'architecture à long terme n'a pas fait l'objet d'une réflexion approfondie. C'est pourquoi de nombreuses entreprises se retrouvent aujourd'hui à gérer difficilement plusieurs solutions de connectivité à distance ponctuelles, notamment les réseaux privés virtuels (VPN) d'accès à distance, le SSE (Security Service Edge), l'accès réseau Zero Trust (ZTNA), les passerelles web sécurisées (SWG), les agents de sécurité d'accès au cloud (CASB), la prévention des pertes de données (DLP) et les appliances SD-WAN.

Connecter les utilisateurs à plusieurs clouds et créer des réseaux entre ces clouds

Établir des connexions entre les utilisateurs, les appareils et les sites vers un ou plusieurs clouds n'est pas chose simple. Ce processus se révèle fréquemment très complexe, car il inclut des éléments tels que la sécurité, la rapidité et la performance du réseau qu'il est essentiel d'intégrer naturellement, au lieu de les incorporer ultérieurement. Cette démarche nécessite une évolution progressive de la conception des architectures. Les cas d'utilisation, entre autres, visent à :

- Permettre aux utilisateurs de bénéficier d'un accès sécurisé et optimisé aux applications sur site ou dans le cloud via une connexion Internet peu fiable
- Permettre aux entreprises de faciliter les communications sécurisées entre les applications, le tout conformément à des règles, via divers services cloud
- Permettre aux filiales réparties dans le monde entier d'accéder aux applications via des connexions réseau intermédiaires peu fiables

Le fil conducteur de ces cas d'utilisation est la nécessité d'un réseau dispersé de points de présence (PoP) dans le cloud, positionnés stratégiquement pour fournir sécurité et optimisation au plus près des utilisateurs, des appareils, des sites et des différents environnements cloud. Cet arrangement stratégique garantit une expérience utilisateur de plus grande qualité. Par exemple, un PoP situé à San Francisco ne peut pas fournir une expérience satisfaisante aux utilisateurs situés à Bangalore.

Priorité au sans-fil (4G/5G)

Un monde de connexions « Many-to-Many », où les personnes doivent pouvoir travailler n'importe où et n'importe quand, nécessite une capacité sans fil/cellulaire intégrée plus importante que celle fournie par le SD-WAN. Une connectivité rapide et fiable est nécessaire en tout lieu, qu'il s'agisse d'un véhicule de terrain en mouvement constant ou d'un site de construction ou d'exploration, en particulier là où le haut débit n'est pas disponible ou prend beaucoup de temps à configurer. Ainsi, les connexions sans fil s'avèrent indispensables dans diverses situations. Il faut donc privilégier et prioriser la gestion élargie des réseaux 4G/5G, plutôt que de les considérer comme une solution de secours.

Micro-filiale

Le sens du mot *filiale* a changé depuis sa première introduction. Au début, les filiales étaient presque toujours de grands ensembles d'utilisateurs. Dans notre monde massivement distribué, une filiale peut comprendre

cinq ou dix personnes travaillant dans un petit bureau, dans une agence bancaire ou sur un chantier de construction. Le SD-WAN traditionnel est trop lourd et volumineux pour gérer rapidement un grand nombre de micro-filiales.

Ce qu'il faut, c'est une petite passerelle mobile « tout-en-un » qui intègre le SD-WAN, la sécurité, l'informatique en périphérie, le cellulaire, les points d'accès et la commutation. Les micro-filiales ou les agences décentralisées doivent prendre en charge les applications légères de calcul en périphérie développées par les entreprises elles-mêmes ou par des partenaires ; ceci, afin d'éliminer le besoin de serveurs supplémentaires et de réduire les dépenses d'investissement en matériel (CapEx) et d'exploitation (OpEx). Pensez-y comme à un magasin d'applications qui vous permet d'exécuter vos propres applications personnalisées ou l'une des applications du catalogue d'un partenaire.

Convergence de l'IT/OT

La prolifération des périphériques IoT, des outils de production intelligents et des actifs de grande valeur a complètement transformé la filiale dans le monde sans frontières. Il n'est plus question d'imaginer des humains accéder avec une expérience utilisateur optimale à des applications grâce au SD-WAN. La nouvelle filiale est composée d'actifs de grande valeur qui ont besoin d'accéder aux applications de manière similaire. Ces machines peuvent être un distributeur automatique de billets (DAB), une grue, un robot dans une usine ou tout autre capteur IoT recueillant des données qui doivent être transportées efficacement et analysées automatiquement à l'aide de techniques d'IA pour maximiser les bénéfices commerciaux et prédire les éventuelles pannes.

L'exécution d'opérations efficaces nécessite des capacités de calcul à la périphérie du réseau, afin d'alimenter n'importe quelle application conteneurisée peu volumineuse, spécifiquement adaptée à l'usage prévu. Par exemple, dans un champ pétrolier, un câble à fibre optique ne signale au service cloud d'analyse que la température en fonction d'un seuil prédéfini. Il est tout aussi important de gérer efficacement les opérations Day 1. Imaginez une usine de fabrication intelligente dotée d'une machine à commande numérique par ordinateur (CNC) qui communique en permanence ses valeurs de contrôle d'intégrité à un outil alimenté par l'IA, capable d'anticiper un problème avant qu'il ne se produise. Le personnel chargé de l'exploitation du réseau peut se connecter à distance à l'appareil, résoudre tout problème et effectuer une maintenance prédictive, ce qui permet d'économiser les coûts liés aux déplacements. Ces capacités innovantes permettent de faire converger les technologies de l'information et les technologies opérationnelles.

Les limites du SD-WAN traditionnel face au monde moderne

Les architectures réseau classiques peinent à suivre les besoins actuels et représentent un fardeau pour les entreprises. L'adoption massive du télétravail n'était pas prévue lors de la conception des réseaux d'entreprise. Nous devons repenser la manière dont nous créons les réseaux modernes afin de permettre une intégration étroite des réseaux et de la sécurité et de fournir une protection dans le cloud sur la base des principes du Zero Trust. Ces principes stipulent qu'au lieu de supposer que tout ce qui se trouve derrière le pare-feu de l'entreprise est sûr, le système de sécurité devrait toujours vérifier et ne jamais faire confiance. Les technologies réseau et de sécurité actuelles ressemblent à d'anciennes briques dans un édifice moderne en verre. Intégrées tant bien que mal aux infrastructures des entreprises, elles bouleversent l'architecture au lieu de l'optimiser. Elles sont à l'origine des défis actuels, ou ne sont pas conçues pour les surmonter. Et c'est un problème.

Tous les défis mentionnés ci-dessus pèsent sur le SD-WAN. De la même manière, le SD-WAN s'est développé, car le WAN ne pouvait pas gérer un monde de filiales, il a atteint un tournant majeur (certains pourraient même dire un point de rupture), car il ne peut pas gérer un monde de connexions « Many-to-Many ».

Les sections suivantes exposent les raisons pour lesquelles le SD-WAN a atteint ses limites.

Vous ne pouvez pas améliorer votre réseau en appliquant des correctifs

Le SD-WAN n'a pas été conçu pour le monde moderne, et aucune mise à jour mineure n'y changera quoi que ce soit. Imaginez que vous ayez une appliance SD-WAN « lourde » pour chaque travailleur à distance, chaque appareil IoT ou chaque application en périphérie. C'est comme si tous les passagers d'un vol essayaient d'embarquer avec une valise démodée et surdimensionnée, trop grande et trop encombrante pour les compartiments à bagage des avions modernes. Ce n'est tout simplement pas possible. Les équipes chargées des réseaux ont traditionnellement répondu aux besoins émergents des entreprises en ajoutant de nouvelles solutions individuelles et personnalisées. Autrefois, chaque nouvelle idée recevait une nouvelle boîte noire ; aujourd'hui, chaque idée se voit attribuer une nouvelle machine virtuelle (VM). Les appliances SD-WAN, les passerelles cellulaires dans les filiales pour la connectivité, les produits supplémentaires pour la connectivité multicloud d'application à application, et les clients VPN traditionnels correspondent tous à ce modèle. Cette approche a créé des silos technologiques, constitués de solutions ponctuelles faiblement intégrées et gérées séparément.

Au final, le service IT doit garantir des performances stables et une protection robuste pour l'ensemble des ressources de l'entreprise à l'échelle mondiale, tout en garantissant un coût abordable pour chaque connexion. Il s'agit d'un défi architectural, et non d'un problème fonctionnel, qui nécessite l'élimination des silos informatiques et des solutions ponctuelles pour répondre aux nouvelles exigences des entreprises. Le modèle qui consiste à « ajouter un autre boîtier ou une autre machine virtuelle » n'est pas compatible avec les nouveaux modes de fonctionnement des entreprises.

Le SD-WAN n'est pas évolutif

Le SD-WAN ne peut pas évoluer pour gérer le volume d'utilisateurs, d'applications et d'appareils. Les filiales varient en taille, allant de quelques personnes à quelques centaines, voire quelques milliers d'individus. Dans le haut de cette fourchette, les solutions SD-WAN doivent être exécutées dans un grand cluster d'équilibrage de charge pour pouvoir fonctionner efficacement. Imaginez une entreprise avec des dizaines de milliers de travailleurs à distance répartis dans le monde entier, ou un environnement de production comportant plus de 100 000 machines connectées à l'IoT à gérer. Dans ces cas, le SD-WAN peine à gérer l'énorme volume de trafic, la multitude de connexions ou la complexité des politiques et des règles de qualité de service à définir et à appliquer.

Le SD-WAN est dépourvu d'une fonctionnalité essentielle

Si nous regardons la façon dont le monde fonctionne aujourd'hui, il est clair que le point de contrôle ne réside plus à la frontière d'une filiale. La capacité de définir et de gérer un réseau ne peut pas être liée à un périmètre physique. Et nous devons en savoir beaucoup plus sur chaque connexion pour pouvoir gérer le réseau et la qualité de service.

Le SD-WAN ne peut pas prendre en compte le contexte. Il ne peut pas comprendre les applications auxquelles les utilisateurs tentent d'accéder et les risques qu'elles présentent, ni la gamme d'appareils utilisés et leur risque de compromission. Les entreprises ont besoin de ces informations approfondies pour pouvoir prendre des décisions informées sur la priorisation des applications. En pratique, cela signifie qu'un ensemble beaucoup plus riche d'informations est nécessaire sur les utilisateurs, les applications et les appareils. Cette compréhension permet aux administrateurs de créer des règles particulières non seulement pour des utilisateurs et des appareils spécifiques, mais aussi qui permettent de gérer les risques dans des catégories plus larges en appliquant les principes Zero Trust.

Dans le SD-WAN traditionnel, la sécurité était ajoutée de manière indépendante et non intégrée. Le SD-WAN traditionnel permettait aux filiales

de communiquer directement sur Internet avec plusieurs clouds, ouvrant ainsi une énorme faille de sécurité dans le processus. Plusieurs sociétés ont choisi d'implémenter une sécurité distribuée au sein de chaque filiale, rendant ainsi sa gestion et son adaptation compliquées. En outre, cela ne permet pas à l'équipe de sécurité de suivre les utilisateurs mobiles et les applications où qu'ils se trouvent. Les fournisseurs de services SD-WAN emploient désormais le terme de « *sécurité adéquate* » pour évoquer le niveau au sein des filiales. La sécurité réseau « adéquate » ne peut pas remplacer la sécurité optimale fournie par une plateforme SASE (prononcez « sassy »), une architecture basée sur le cloud qui offre des services réseau et de sécurité destinés à protéger les utilisateurs, les applications et les données, quel que soit leur emplacement. Le temps a prouvé que la sécurité fournie par le cloud constitue la bonne approche à adopter. Le SASE d'un fournisseur unique permet une architecture unifiée avec une simplification et un partage du contexte entre le SD-WAN et la sécurité fournie par le cloud. (Nous parlerons du SASE plus en détail dans le chapitre 5.)

Le SD-WAN n'exploite pas l'IA/ML

Le SD-WAN traditionnel n'a pas su tirer parti de l'apprentissage automatique (ML) ni de l'analyse prédictive avancée, qui pourraient permettre des opérations performantes et automatisées, apportant aisance et efficacité aux équipes réseau. Celles-ci cherchent à anticiper les problèmes avant qu'ils ne se produisent et à fournir une expérience utilisateur exceptionnelle dans toutes les applications. Le SD-WAN actuel doit rassembler toutes les informations nécessaires sur l'intégralité du réseau (pour chaque utilisateur à distance, filiale et charge de travail dans le cloud) et exploiter l'intelligence artificielle et l'apprentissage automatique pour offrir des prévisions à l'échelle de l'entreprise. Ainsi, les ingénieurs réseau peuvent améliorer davantage les performances du réseau, et les utilisateurs finaux gagnent en productivité.

Le SD-WAN ne peut pas offrir une expérience de qualité pour plus de 60 000 applications

Une mise en œuvre typique d'un réseau SD-WAN pouvait concerner près de 3 000 ou 4 000 applications, mais le paysage moderne en compte au moins 60 000. Connaître les caractéristiques et le caractère stratégique de ces applications permet de prioriser les solutions afin d'améliorer l'expérience utilisateur. Par exemple, la connexion réseau d'une personne utilisant Zoom à des fins professionnelles doit être optimisée, contrairement à celle d'un collaborateur qui regarde des vidéos sur YouTube ou joue à des jeux au travail.

Le SD-WAN ne simplifie pas l'utilisation du plan de contrôle

Le SD-WAN a progressé en dissociant le plan de données et le plan de contrôle. Cependant, le fait que le plan de contrôle soit bricolé sur site n'a pas facilité son utilisation. Les entreprises doivent privilégier un contrôleur entièrement basé sur le SaaS, qui gère l'acheminement avancé, notamment via les protocoles BGP (Border Gateway Protocol) et OSPF (Open Shortest Path First). Les entreprises doivent aussi se pencher sur l'infrastructure soutenant les fonctionnalités SSE, en s'assurant qu'elle propose une présence internationale, une protection intégrale pour chaque emplacement, une interconnexion étendue avec les prestataires de services cloud et une latence minimale. Ainsi, les clients n'auront pas à faire de compromis entre l'efficacité de la sécurité et les performances – un problème très difficile à résoudre. La configuration en un seul clic des capacités de type SSE pour un boîtier SD-WAN dans une filiale permet de trouver automatiquement le point de présence le plus proche.

Le sans-fil 4G/5G a été pensé après coup

La prise en charge élargie de la technologie sans fil 4G/5G ne doit pas être envisagée après coup. Au contraire, elle doit être prise en charge de différentes manières : en tant qu'alternative de transport intégrée à l'équipement SD-WAN et comme solution WAN sans fil élargissant la portée de la passerelle SD-WAN qui s'exécute en arrière-plan. Les filiales peuvent avoir besoin d'un accès sans fil, mais il en va de même pour les équipements mobiles tels que les camions ou les robots. Le sans-fil joue un rôle différent dans chacun de ces contextes.

L'architecture n'est pas née dans le cloud

La complexité écrasante des réseaux cloud conduit les organisations à éprouver une immense frustration lorsqu'il s'agit de connecter les utilisateurs, les appareils et les sites au cloud ou à plusieurs clouds. L'architecture doit évoluer de manière à ce que la sécurité, la vitesse et l'optimisation du réseau soient intégrées comme des éléments essentiels de la connectivité, et non comme des composants secondaires. Les utilisateurs peuvent profiter d'un accès sécurisé et amélioré aux applications, qu'elles soient hébergées localement ou dans le cloud, même avec une connexion Internet peu fiable. De plus, des filiales situées aux quatre coins du globe peuvent accéder aux applications en toute sécurité, malgré une connectivité intermédiaire incertaine entre elles ou entre différents services cloud. Mais une connexion cloud nécessite également de rapprocher le point de présence du réseau de l'utilisateur afin de garantir des performances et une expérience utilisateur de haute qualité.

Le SD-WAN n'est pas extensible

Aujourd'hui, les réseaux se déplacent vers le cloud et les opérations de calcul se produisent plus près de la périphérie. Au départ, de nombreux fournisseurs de services SD-WAN ont commencé par enchaîner les VM SD-WAN avec les VM de sécurité des partenaires sur site, hébergées sur une grande appliance. Toutefois, une grande partie de ces fonctions de sécurité et de mise en réseau ont maintenant été transférées dans le cloud. Par conséquent, il est de plus en plus nécessaire d'avoir des fonctions de calcul légères plus proches de la source de données. Imaginez un détaillant qui souhaite qu'un système de point de vente soit disponible à 100 % ; il déplacera ce système sous forme d'une application en périphérie pour maintenir une haute disponibilité ou, dans le monde de l'IoT, exécutera le moteur d'exécution Azure IoT Edge à la périphérie de l'entreprise. D'autres exemples peuvent inclure vos propres applications personnalisées.

Le SD-WAN est rigide et non pertinent

Le succès d'une technologie quelconque dépend de sa pertinence dans le paysage technologique actuel. Tout est une question de contexte. Malgré ses atouts d'antan, le SD-WAN ne prend tout simplement pas en charge les connexions « Any-to-Any » ou « Many-to-Many » comme l'exigent les entreprises actuellement. Il n'est pas non plus très évolutif, ce qui est indispensable pour tout secteur d'activité.

RAPPEL

Le SD-WAN a eu son heure de gloire. Toutefois, sa rigidité et son inflexibilité excessives entravent la transformation dans ce monde hyperconnecté. Il passera à l'arrière-plan et sera dépassé par la prochaine génération de technologies. Ainsi va le cycle de l'innovation.

ATTENTION

À un moment donné, le manque d'expérience confirmée dans les applications ou l'absence de sécurité, de visibilité et de gestion uniforme des applications se transforme en un barrage dont les fissures s'élargissent, menant à une débâcle désastreuse. Les utilisateurs et les appareils se retrouvent pris dans un déluge en aval, incapables d'accéder aux ressources distantes avec le niveau de performance ou les politiques de cybersécurité appropriés. Alors, que doit faire un architecte IT pour endiguer cette avalanche de nouvelles exigences ? Les organisations de toutes formes et de toutes tailles ont désormais besoin d'un SD-WAN conçu pour les connexions « Many-to-Many » et « Any-to-Any ». Heureusement pour ceux d'entre nous qui s'intéressent à la technologie, cette forme de SD-WAN est arrivée. Netskope l'appelle le *Borderless SD-WAN*, et il va au-delà de ce que le SD-WAN traditionnel offre actuellement.

DANS CE CHAPITRE

- **Comprendre les avantages de Netskope Borderless SD-WAN**
- **Sécuriser un réseau étendu défini par logiciel (SD-WAN)**
- **Répondre aux besoins de la micro-filiale**
- **Accompagner les utilisateurs finaux, peu importe leur localisation**
- **Une connectivité rapide et fiable grâce à la 4G/5G**
- **Tirer pleinement parti des capacités de l'Internet des objets (IoT)**
- **Découvrir ce que le Borderless SD-WAN peut apporter**

Chapitre **2**

Une vision concrète pour un SD-WAN abouti : l'avenir sans frontières

Le SD-WAN s'est imposé, car les utilisateurs des filiales réclamaient un support plus efficace pour gérer leur trafic et leur qualité de service, en combinant des connexions Internet économiques et le MPLS (Multiprotocol Label Switching). Comme indiqué dans le chapitre 1, le monde a évolué dans des directions que le SD-WAN peinait à suivre. Tous les domaines abordés dans le chapitre 1, à savoir l'essor de la mobilité, la multiplication des applications et des appareils IoT, et l'univers multicloud, nécessitent un réseau sans fil, une informatique en périphérie et une sécurité gérée depuis le cloud. Ces exigences mettent à rude épreuve le SD-WAN traditionnel et les solutions conçues pour le soutenir, parfois jusqu'à leur point de rupture.

Dans ce chapitre, nous examinons ces problèmes plus en détail et montrons comment la solution Borderless SD-WAN de Netskope peut apporter des réponses.

Borderless SD-WAN : les réseaux dans un monde de connexions « Many-to-Many »

Dans le contexte actuel, où utilisateurs et appareils se retrouvent à la dérive dans l'océan numérique, interagissant avec plusieurs clouds et une multitude d'applications, ils peuvent se sentir comme des marins errant dans un vaste espace sans boussole ni carte – trouver protection et optimisation peut être aussi difficile que de chercher un phare en pleine tempête. Quand on tente de les secourir, on leur jette en fait un enchevêtrement de solutions qui tourne au casse-tête administratif. Ce n'est pas ce que recherchent les organisations.

Le but du Borderless SD-WAN, c'est d'offrir à quiconque ou à n'importe quel appareil une connectivité à la fois sécurisée et performante, où que vous soyez. C'est une bonne idée, n'est-ce pas ? Mais comment cela fonctionne exactement ? Comment cette vision peut-elle devenir réalité ?

Pour bien comprendre le Borderless SD-WAN (voir figure 2-1), il nous faut analyser comment six scénarios actuels dans le domaine de l'informatique, des réseaux et de la sécurité mettent à mal le SD-WAN traditionnel :

- SD-WAN sécurisé
- Micro-filiale
- SD-WAN des terminaux
- Passerelle WAN sans fil
- Accès intelligent à l'IoT
- Réseaux multicloud

À mesure que nous explorons chacun de ces éléments, nous expliquons ce qui est nécessaire dans le monde du « Many-to-Many », pourquoi le SD-WAN et les solutions actuelles ne font pas le poids, et comment le Borderless SD-WAN peut vous aider.

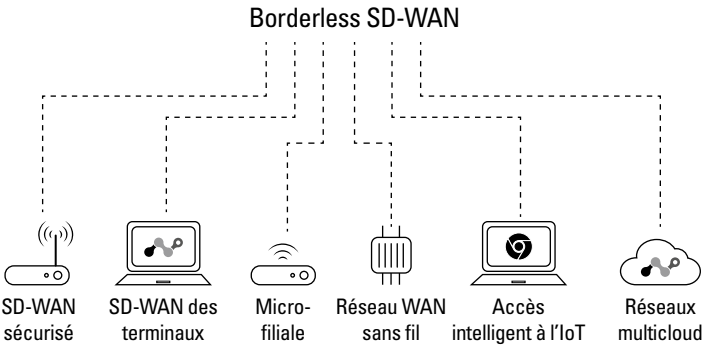


FIGURE 2-1 : Borderless SD-WAN gère les logiciels sur les ordinateurs portables, les passerelles mobiles ainsi que les appliances se trouvant dans des micro-sites, des grandes filiales ou des centres de données. Il fait office de passerelle virtuelle pour les réseaux multicloud.

SD-WAN sécurisé

Sécurité et réseaux ont toujours été étroitement liés. Comme nous l'avons vu précédemment, les connexions MPLS étaient chères, rigides et manquaient de visibilité et de contrôle applicatif. Le SD-WAN a vu le jour comme une alternative moins coûteuse au MPLS. Cette technologie est venue compléter le MPLS en utilisant des connexions Internet haut débit et économiques, permettant aux utilisateurs de filiales de se connecter directement aux applications sur site et aux applications SaaS. L'objectif du SD-WAN était de fournir des performances et une sécurité équivalentes sur des connexions haut débit standard, ce qu'il a réussi grâce à une visibilité et à un contrôle orientés applications. Ainsi, les administrateurs ont pu établir des politiques pour faire passer Zoom avant Netflix, par exemple.

RAPPEL

Nous voici à un nouveau tournant où il est temps de dépasser le SD-WAN traditionnel. L'explosion du nombre d'applications cloud et d'appareils IoT a mis les solutions SD-WAN traditionnelles à rude épreuve. Leur contrôle basé sur des règles centrées sur les applications n'est plus suffisant, surtout si la solution SD-WAN en question n'adopte pas une approche Zero Trust.

L'entreprise moderne a maintenant besoin d'un SD-WAN Zero Trust contextuel pour garantir un accès rapide, fiable et sécurisé à toutes les applications et tous les appareils, partout, tout en offrant une visibilité complète et des contrôles appropriés. Cela est possible grâce à des politiques contextuelles qui tiennent compte des applications, des utilisateurs, des appareils, ainsi que des risques associés, rendant ainsi la gestion du réseau plus intelligente et plus sécurisée.

Les solutions SD-WAN actuelles permettent aux administrateurs réseau de créer des politiques pour quelques milliers d'applications, ce qui est dérisoire face aux dizaines de milliers d'applications qui pullulent sur le web et dans le cloud. Si vous ne pouvez même pas identifier ces applications, comment espérer les gérer ? Certaines sont adaptées aux besoins professionnels, d'autres pas du tout. Attribuer automatiquement des priorités de trafic à toutes les applications prises en charge s'avère donc très complexe. Le personnel en charge du réseau doit configurer ces applications une à une, manuellement. C'est un processus lent, propice aux erreurs et totalement inadapté à la gestion de milliers d'applications.

La solution Borderless SD-WAN gère une base de données de plus de 60 000 applications. Inutile pour les administrateurs IT de configurer manuellement les politiques de qualité de service pour chaque application. À la place, un indice de confiance dans le cloud (CCI, Cloud Confidence Index) évalue la fiabilité de chaque application. Cet indice donne un score en fonction de la préparation de l'application pour un usage en entreprise, et ce score définit des paramètres de priorité automatiques pour le trafic. Ainsi, l'équipe réseau est libérée de toute manipulation manuelle, rendant les opérations plus fluides. Par exemple, Zoom a un CCI de 82 et est donc prioritaire par défaut, tandis que SureVoIP, avec un CCI de 38, est relégué en bas de la liste dès le départ.

Les entreprises veulent avoir un contrôle en temps réel de la qualité de leurs connexions aux applications, et la capacité de basculer vers une meilleure connexion en une fraction de seconde. Elles cherchent aussi à corriger et à optimiser le protocole TCP en temps réel.

Le SD-WAN traditionnel se limite à segmenter le réseau en fonction des adresses IP ou des sous-réseaux. La sécurité repose sur la connaissance et le contrôle du réseau, ce qui marchait bien auparavant. Mais comment gérer des appareils IoT compromis en périphérie, qui offrent un accès au réseau de l'entreprise ? Le SD-WAN traditionnel ne nous donne pas de vue claire sur ces appareils IoT, et avec leur multiplication, c'est plus crucial que jamais. Grâce à l'intelligence artificielle et à l'apprentissage automatique, des fonctionnalités contextuelles détectent et segmentent tous les appareils IoT, qu'ils soient gérés ou non, pour minimiser les risques liés aux appareils compromis. Par exemple, si une caméra IoT envoie des vidéos à une application non autorisée, la micro-segmentation permet de la bloquer rapidement pour limiter les dégâts en cas de compromission et y remédier.

Le Borderless SD-WAN répond à ces besoins en collectant une vaste gamme de données sur les utilisateurs, les appareils, les applications et les réseaux. Cette richesse de contexte permet une application précise de politiques granulaires.

Micro-filiale

Le terme *micro-filiale* désigne un petit espace comme un bureau, un café ou une boutique où l'on peut travailler à l'ère du télétravail. Même si ces lieux accueillent seulement quelques utilisateurs ou appareils, leurs exigences en termes de connectivité, de qualité de service et de sécurité sont tout aussi cruciales que dans une grande filiale. Ce qu'il leur faut, c'est une passerelle efficace, abordable, qui garantit à la fois une excellente connectivité et une sécurité fiable.

Le Borderless WAN facilite la gestion des micro-filiales en utilisant un logiciel léger sur une passerelle SASE (Secure Access Service Edge) compacte, à savoir un équipement physique situé soit dans une grande filiale soit dans une micro-filiale. Cette architecture intègre les services réseau et de sécurité. Une passerelle SASE unifiée s'avère être la solution la plus efficace pour déployer un Borderless SD-WAN. Elle regroupe diverses fonctionnalités comme la connectivité cellulaire, le SD-WAN, le Wi-Fi, la sécurité et le traitement des données en périphérie, le tout contrôlé via une seule console et géré par une politique unique. La configuration optimale consiste en une intégration simplifiée via une console unique, appuyée par un SSE (Security Service Edge) intelligent pour assurer une protection complète. D'ailleurs, Netskope, en tant que fournisseur unique, propose justement cette solution complète en matière de SASE.

RAPPEL

Le Borderless SD-WAN distribué permet une expérience de haute qualité partout, que vous soyez dans un petit bureau ou dans un véhicule de terrain sur un site pétrolier au Texas. Pour y parvenir, l'idéal est un appareil unique, compact et léger capable de gérer plusieurs services. La plupart des fournisseurs de SD-WAN n'offrent pas cette flexibilité et se limitent aux solutions pour les filiales traditionnelles.

SD-WAN des terminaux

De nos jours, c'est souvent un équipement SD-WAN combiné à des logiciels VPN qui assure un accès à distance sécurisé et efficace. Cependant, cette solution n'est pas idéale pour les collaborateurs à distance, qui ne jouissent pas de la même qualité de connexion que ceux qui se trouvent au bureau. De plus, la nécessité de combiner SD-WAN et VPN oblige les entreprises à jongler entre différents fournisseurs, équipements et budgets, rendant cette approche difficile à faire évoluer.

S'appuyer uniquement sur un logiciel VPN sans le soutien d'un équipement SD-WAN est source de nombreux problèmes. Les VPN souffrent notamment d'un manque de visibilité, de connexions statiques point à point, de latence accrue et d'une gestion inefficace du trafic voix/vidéo. Cette absence de clarté sur qui accède à quoi et d'où, ajoutée à des fluctuations de performance réseau souvent ignorées, peut nuire directement à la productivité des utilisateurs.

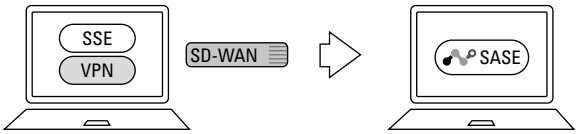
Les VPN traditionnels sont conçus pour acheminer le trafic vers des concentrateurs, ce qui génère des latences supplémentaires à cause d'une sélection de chemin peu efficace. Les solutions SD-WAN peuvent résoudre certains de ces problèmes, mais elles sont liées à un équipement spécifique et n'intègrent pas la sécurité Zero Trust. De ce fait, vous ne pouvez pas les personnaliser pour chaque utilisateur à distance.

De nos jours, le personnel souhaite bénéficier d'une sécurité Zero Trust et d'une connectivité fiable, quel que soit l'endroit où il se trouve. Les équipes IT, de leur côté, recherchent simplicité et clarté pour gérer efficacement les utilisateurs à distance. Paradoxalement, bien qu'étiqueté comme étant « défini par logiciel », le SD-WAN utilise surtout du matériel spécialisé ou des serveurs dédiés, en particulier dans les filiales.

L'installation d'un SD-WAN sur un ordinateur portable peut améliorer considérablement l'expérience utilisateur, peu importe le lieu de connexion. Les opérateurs réseau bénéficient ainsi d'une visibilité totale sur toutes les applications et connexions, ce qui simplifie le dépannage. Même dans les zones avec un Internet capricieux, un SD-WAN installé sur un ordinateur portable optimise la qualité en ajustant des politiques de service pour donner la priorité aux applications sensibles à la latence.

Le SD-WAN physique devient un casse-tête à mesure que les connexions à distance se multiplient. Prenons l'exemple d'une grande compagnie d'assurance : elle a dû envoyer des appareils SD-WAN à plus de 25 000 téléconseillers. Un taux de roulement plus important du personnel a entraîné le non-retour de plus de 500 appareils par mois, provoquant des problèmes de sécurité, une hausse des coûts et des complications logistiques. Ce scénario souligne l'importance d'une solution telle que le Borderless SD-WAN, qui peut être mise en œuvre directement sur l'ordinateur portable d'un collaborateur.

Quant aux autres voies d'accès à distance, comme les systèmes Zero Trust / ZTNA (Zero Trust Network Access), elles présentent également des inconvénients. La majorité des clients Zero Trust / ZTNA ne bénéficient pas des avantages de l'optimisation SD-WAN, et la plupart des prestataires SD-WAN peinent à intégrer les éléments Zero Trust et ont besoin de matériel. Une solution logicielle unifiant les capacités Zero Trust et les avantages de l'optimisation des applications SD-WAN peut fournir le meilleur des deux mondes sans aucun matériel. Le paysage professionnel moderne exige aujourd'hui un client SASE unifié basé à 100 % sur logiciel (voir figure 2-2).



Traditionnel
Solutions ponctuelles
non intégrées

Client SASE unifié
Agent unique pour le SD-WAN
des terminaux et le SSE

FIGURE 2-2 : Le Borderless SD-WAN intègre un client SASE unifié, qui combine l'optimisation SD-WAN et la sécurité SSE pour satisfaire aux besoins de la main-d'œuvre hybride actuelle.

RAPPEL

L'accès à distance n'est efficace que lorsqu'il offre une expérience utilisateur de qualité et une sécurité Zero Trust partout où l'utilisateur travaille. Certaines solutions spécialisées peuvent également fournir cette fonctionnalité, mais le problème devient alors de devoir gérer une multitude de produits plutôt qu'une unique solution Borderless SD-WAN.

Réseau WAN sans fil

Pour travailler efficacement dans un monde où tout est interconnecté, le SD-WAN traditionnel ne suffit pas en matière de connexion sans fil. Ce dont vous avez vraiment besoin, c'est d'une connexion rapide et fiable partout, que vous soyez dans un véhicule constamment en mouvement ou devant un point d'accès fixe en entreprise qui émet un signal puissant depuis la salle serveur.

Le SD-WAN traditionnel a ses limites, mais le Borderless SD-WAN les dépasse. Du côté des utilisateurs, nous pouvons distinguer deux cas d'utilisation ou applications typiques.

Le premier cas d'utilisation vise les organisations qui cherchent un appareil tout-en-un. Ce dispositif unifie des fonctions comme le SD-WAN, la sécurité, l'informatique en périphérie et la passerelle sans fil, simplifiant ainsi la gestion de réseaux et de budgets compliqués. Cette passerelle doit être compatible avec les opérateurs du monde entier et offrir une qualité d'expérience (QoE) en permettant des ajustements dynamiques de la bande passante pour réduire les coûts des connexions cellulaires coûteuses. Par exemple, si une connexion haut débit est disponible en parallèle d'une connexion cellulaire, il peut être acceptable que Netflix ait une priorité moyenne. Mais si la connexion haut débit n'est plus disponible, une politique de qualité de service dynamique peut bloquer Netflix sur le réseau cellulaire.

Le deuxième cas d'utilisation met en jeu le Borderless SD-WAN comme passerelle WAN sans fil. Vous pouvez monter la passerelle cellulaire Netskope sur un mur ou un plafond et la connecter via un câble Ethernet

PoE (Power over Ethernet) qui fournit aussi l'alimentation. Elle transmet un signal robuste à la passerelle Borderless SD-WAN SASE située dans votre salle serveur. Avec cette configuration, votre entreprise peut gérer tous ses appareils depuis une seule console, éliminant le besoin de jongler entre différents fournisseurs et tableaux de bord. Cette capacité permet de réaliser des économies et de contourner les limites des antennes externes, dont la puissance diminue avec la distance, les rendant presque inutilisables si le routeur de la salle serveur est trop éloigné du toit.

Réseaux multicloud

Le SD-WAN traditionnel peine à gérer efficacement les environnements multicloud et les opérations automatisées. Alors que les entreprises utilisent des dizaines de clouds différents pour des tâches variées, elles recherchent un réseau capable de les connecter de manière sécurisée tout en facilitant la communication entre applications selon des règles établies. Certains nouveaux venus sur le marché offrent bien une solution de réseau cloud avec de la visibilité pour gérer les connexions entre différents clouds grâce à des stratégies et à des configurations automatisées. Ces fournisseurs de services multicloud résolvent un problème important : ils offrent aux entreprises la possibilité de transférer leurs charges de travail vers ces clouds grâce à un tableau de bord unifié fournissant les données essentielles pour une orchestration efficace. C'est un bon début, mais cela ne va pas assez loin. Le Borderless SD-WAN, lui, pousse le concept encore plus loin en intégrant sécurité et optimisation pour chaque utilisateur, chaque appareil, chaque site et chaque cloud. Avec cette solution, les clients profitent d'un accès instantané à une sécurité SSE en un seul clic, assurant ainsi une protection totale sur tous les types de cloud.

Par exemple : vous gérez des milliers de serveurs répartis dans divers clouds, et ces serveurs doivent régulièrement télécharger des mises à jour sur Internet. Étant donné que ces serveurs sont exposés aux cybermenaces, comment garantir leur sécurité ? Le Borderless SD-WAN a la solution. Grâce à sa profonde compréhension du contexte et à son intégration facile avec des outils d'automatisation cloud comme Terraform, il applique des règles précises pour gérer la connectivité entre les clouds, optimiser le réseau et renforcer la sécurité. Toute cette complexité de gestion multicloud disparaît grâce à une console unique. Depuis cette interface, vous pouvez déployer facilement le logiciel léger de Borderless SD-WAN sur tous vos environnements cloud. À partir de cette console, des opérations cloud automatisées permettent à ces instances du logiciel Borderless SD-WAN d'interagir de manière fluide avec des services clés tels qu'Amazon Web Services (AWS) Transit Gateway, Azure Virtual Router et Google Cloud Platform (GCP) Cloud Router. Pour couronner le tout, un simple clic vous donne accès à Netskope Intelligent SSE, vous offrant ainsi une couche de sécurité intégrée pour vous prémunir contre toute forme de cyberattaque.

Le Borderless SD-WAN élargit le réseau WAN de votre entreprise et vous donne la possibilité de vous connecter à plusieurs services cloud. Il vous permet aussi d'intégrer facilement un cloud public dans votre architecture Borderless SD-WAN. De cette façon, les utilisateurs peuvent faire fonctionner les applications sur leurs appareils et accéder de manière sûre et efficace à des services cloud comme l'IaaS (infrastructure en tant que service).

Résultat : le Borderless SD-WAN unifie réseau et sécurité de bout en bout.

CONSEIL

Les entreprises peuvent définir des stratégies uniformes pour tout leur réseau, touchant chaque appareil et utilisateur sur n'importe quel cloud, grâce à la sécurité et l'optimisation intégrées. Peu importe le cloud auquel vous vous connectez, les stratégies resteront les mêmes. Les paramètres d'optimisation, d'autorisation et de restriction demeurent constants, quel que soit le type de cloud utilisé. Chaque cloud peut non seulement dialoguer avec les autres – par exemple, AWS avec GCP et GCP avec Azure – mais ces échanges se font aussi de manière sécurisée dans des environnements multicloud. C'est de cette manière que vous devez réaliser des réseaux multicloud pour pouvoir respecter les meilleures pratiques actuelles.

Accès intelligent à l'IoT

Aujourd'hui, les entreprises ont besoin d'un accès intelligent à l'IoT depuis leur SD-WAN. Elles souhaitent que leurs ressources IoT/opérationnelles (OT) se connectent au cloud afin que l'informatique en périphérie puisse s'exécuter sur ces ressources, en ne transférant vers le cloud que les données nécessaires pour analyser un problème et déterminer de manière proactive une solution. Elles doivent également pouvoir tirer parti des capacités de l'IoT pour la surveillance à distance, le dépannage, la collecte de données et la maintenance prédictive en réduisant ainsi les visites sur site des techniciens, ce qui permet de diminuer les coûts liés à la main-d'œuvre, au carburant et à d'autres frais. Sans ces fonctionnalités, il sera difficile d'obtenir le retour sur investissement (ROI) souhaité de leur écosystème d'actifs IoT.

L'objectif est de fournir à un actif IoT une connectivité sécurisée de haute qualité avec des fonctionnalités sans fil et d'edge computing.

Par exemple, pour une machine à commande numérique par ordinateur (CNC) dans une usine, les appareils Borderless SD-WAN robustes fournissent non seulement une connexion Wi-Fi pour les capteurs, mais prennent également en charge l'edge computing pour collecter des informations telles que les données de température et de vibration des capteurs. Ils recueillent également de manière sélective les données utiles en fonction de seuils prédéfinis, ce qui permet d'améliorer l'efficacité opérationnelle tout en réduisant considérablement les coûts.

La passerelle SASE de Netskope prend en charge le provisionnement sans intervention et l'edge computing intégré afin de rapprocher le calcul de la source de données. Elle peut collecter et extraire des données à partir de capteurs IoT et ne transmettre au cloud IoT que les données dépassant des seuils prédéfinis, en utilisant des connexions cellulaires ou d'autres moyens de transmission de son choix. Grâce à la gestion évolutive du cycle de vie des applications (ALM), elle fournit des services de conteneurs prêts à l'emploi tels que le runtime Azure IoT Edge, ainsi que la possibilité d'exécuter d'autres services à partir d'un catalogue de services pour les appareils mobiles. Les clients peuvent également utiliser leurs applications personnalisées. La passerelle SASE de Netskope est dotée d'un kit de développement logiciel (SDK) facile à utiliser pour les développeurs, ainsi que d'interfaces de programmation d'applications (API). Cet ensemble offre une grande flexibilité et une multitude d'options, permettant aux entreprises d'intégrer leurs propres applications.

La passerelle Borderless SD-WAN assure un support post-implémentation et une maintenance continue en prenant en charge l'accès à distance via son gestionnaire IoT intégré. Cela permet d'accélérer la résolution des incidents et de fournir un support efficace aux actifs de grande valeur. Cette fonction permet d'éviter les interventions chez le client car l'informaticien peut dépanner et diagnostiquer à distance. En anticipant le dysfonctionnement d'un appareil, ils peuvent envoyer rapidement la bonne pièce pour résoudre le problème, ce qui permet d'éviter ou de minimiser les interruptions d'activité.

Que peut-on attendre de ces nouvelles capacités ?

Les entreprises doivent être exigeantes quant aux nouvelles capacités que le Borderless SD-WAN peut leur apporter. Voici une liste de ce que le Borderless SD-WAN doit faire pour assurer la sécurité et les performances, y compris les éléments que nous avons déjà abordés, parmi d'autres :

- **Fournir une visibilité pour une prise de conscience contextuelle.** Il est impossible de contrôler, de hiérarchiser ou de défendre ce qui n'est pas visible. Une solution Borderless SD-WAN doit offrir autant de visibilité que possible sur les utilisateurs, les appareils, les applications et les réseaux tout au long du flux de trafic. Dans la mesure du possible, ces informations doivent être contrôlées et mises à jour en temps réel.
- **Fournir un accès et un routage intelligents qui éliminent la complexité de l'administration.** Trouvez une solution simple pour configurer les fonctionnalités SSE et SD-WAN sur un appareil

SD-WAN dans différents environnements tels que les filiales, les utilisateurs distants, les appareils IoT et les environnements multicloud. Cette solution doit permettre de localiser automatiquement le point de présence (PoP) le plus proche. En outre, recherchez un contrôleur cloud évolutif capable d'interagir avec des routages avancés tels que les protocoles BGP (Border Gateway Protocol) et OSPF (Open Shortest Path First).

- **Offrir une sécurité cloud fondée sur les principes Zero Trust.** La sécurité doit être flexible et réactive pour s'adapter à la connectivité croissante et aux conditions en évolution constante. Les pare-feux intégrés aux systèmes SD-WAN traditionnels ne permettent pas à la sécurité de suivre les utilisateurs et les applications mobiles où qu'ils soient, même s'ils ont commencé à résoudre ce problème. Une solution Borderless SD-WAN, étroitement intégrée à un SSE intelligent, offre un SASE à fournisseur unique. Elle fournit une architecture unifiée avec une sécurité réseau hybride, offrant une sécurité sur site comme un pare-feu est-ouest, un système de prévention/détection des intrusions (IPS/IDS) et une segmentation au niveau de la filiale ainsi qu'une sécurité complète via des solutions cloud.
- **Proposer des opérations évolutives et pilotées par l'IA.** Le Borderless SD-WAN s'appuie sur des opérations pilotées par l'IA pour surveiller le réseau à tous les niveaux, y compris l'activité au niveau des utilisateurs, des filiales et des clouds, afin de permettre un dépannage proactif et des analyses complètes. L'identification précoce des anomalies et des signes avant-coureurs à l'aide de l'IA et de l'apprentissage automatique (ML) contribue à réduire le nombre de tickets d'assistance et le temps moyen de résolution, ce qui permet aux clients d'exploiter des réseaux à grande échelle. L'IA et le ML permettent également de rectifier automatiquement les mauvaises conditions du réseau afin d'offrir des performances optimales.
- **Fournir une expérience applicative et une sécurité garanties pour des dizaines de milliers d'applications et d'appareils IoT.** Une implémentation SD-WAN classique peut comprendre les caractéristiques de 3 000 ou 4 000 applications, mais l'explosion des applications cloud et de l'IoT exige une solution Borderless SD-WAN capable de détecter et de hiérarchiser automatiquement 60 000 applications ou plus et de micro-segmenter automatiquement les appareils IoT à risque.
- **Proposer une compatibilité étendue avec les technologies sans fil 4G/5G, avec fiabilité et de différentes manières.** Avec le Borderless SD-WAN, les utilisateurs peuvent accéder aux réseaux 4G et 5G en toute sécurité là où une connexion haut débit n'est pas disponible ou prend du temps à s'établir. Cette capacité est cruciale non seulement pour les filiales, mais aussi pour les flottes mobiles de machines et de robots.

- **Fournir une rampe d'accès au cloud qui réunit le cloud, le réseau et la sécurité.** Les entreprises éprouvent une immense frustration lorsqu'il s'agit de connecter des utilisateurs, des appareils et des sites à un ou plusieurs clouds, en raison de la complexité écrasante de la mise en réseau dans le cloud. L'architecture doit évoluer pour que la sécurité, la vitesse et l'optimisation du réseau fassent partie intégrante de la connectivité, plutôt que d'être des éléments ajoutés après coup. Afin de proposer une solution Borderless SD-WAN avec une sécurité intégrée, il est essentiel d'avoir une connectivité de qualité et accessible aux utilisateurs et aux appareils, peu importe leur localisation. Un réseau mondial cloud avec des points d'accès répartis offre une fonctionnalité périphérique et une connectivité de qualité pour la rampe d'accès au cloud.
- **Fournir des applications de calcul en périphérie pour permettre la mise en place de nouveaux services.** De plus en plus d'applications conteneurisées sont déployées à la périphérie du réseau. Les architectures SD-WAN actuelles ne sont pas suffisamment équipées pour gérer les défis importants posés par cette évolution. Par exemple, un administrateur informatique peut vouloir utiliser une application de contrôle de l'expérience numérique de son choix dans une filiale.

DANS CE CHAPITRE

- **Comprendre l'importance de l'architecture « cloud first »**
- **Création de plans de gestion, de contrôle et de données plus sophistiqués**
- **Utilisation de l'apprentissage automatique (ML) et de l'intelligence artificielle (IA) pour surveiller les réseaux en temps réel**

Chapitre 3
Comment fonctionne le Borderless SD-WAN

Dans le domaine technologique, un adage souvent attribué à Thomas Edison affirme que sans mise en œuvre, une vision n'est qu'une illusion. Comme on dit au Texas, sans mise en œuvre, c'est juste du vent. Netskope a entièrement conçu son réseau étendu sans frontières (borderless) défini par logiciel (SD-WAN) pour offrir une expérience exceptionnelle aux utilisateurs de la technologie et aux personnes chargées de la configurer, de l'exécuter, de l'optimiser et de la déboguer. En bref, Netskope se concentre sur la mise en œuvre ou l'exécution. Ils ont la substance.

Le Borderless SD-WAN de Netskope doit être innovant, car il élargit les capacités et la portée du SD-WAN traditionnel, créant ainsi un nouvel ensemble d'exigences qui transforment l'architecture et les fonctions administratives habituelles du réseau SD-WAN. De ce fait, l'architecture réseau doit évoluer pour garantir une expérience optimale aux utilisateurs, peu importe l'endroit où ils se trouvent dans le monde.

La diversité des services offerts à une large population d'utilisateurs, de filiales, d'appareils IoT et dans le cloud nécessite une révision de la façon dont les plans de gestion, de contrôle et de données sont conçus et mis en œuvre. Les configurations traditionnelles, centrées sur les filiales, sont

désormais remplacées par des politiques basées sur un contexte beaucoup plus détaillé, prenant en compte l'utilisateur, l'appareil, l'application, les données et le réseau. Pour ces raisons, le Borderless SD-WAN de Netskope opère d'une manière complètement inédite, s'appuyant sur une architecture cloud native. Ce chapitre examine ce que cela signifie en pratique.

Pourquoi le Borderless SD-WAN doit-il avoir une architecture « cloud first » ?

Dans notre monde actuel, caractérisé par de multiples interactions et connexions, un nombre croissant d'utilisateurs, d'appareils, de sites et de clouds ont besoin de la connectivité sécurisée et optimisée du Borderless SD-WAN. Prenons l'exemple d'une entreprise qui relocalise des milliers de collaborateurs de centres d'appels vers un modèle de travail à domicile ; dans ce cas, la fonction SD-WAN doit s'adapter à grande échelle. Pour assurer un service de qualité à ces collaborateurs, il est indispensable d'avoir un point de présence (PoP) fiable à proximité de chacun d'eux. La seule manière d'atteindre cet objectif est de déplacer l'implémentation vers le cloud et d'adopter une stratégie de connectivité innovante. C'est précisément l'approche adoptée par le Borderless SD-WAN.

Bien que de nombreux fournisseurs affirment proposer une architecture cloud native pour le Borderless SD-WAN, en réalité, peu y parviennent. Ils prétendent que leur plan de gestion, de contrôle et de données est hébergé dans le cloud. Cependant, la réalité est qu'ils se contentent souvent d'exécuter leur logiciel sur des serveurs actifs de secours dans le cloud. Cette méthode présente un inconvénient : dès que la capacité maximale est atteinte, les fournisseurs doivent constamment activer des serveurs de secours supplémentaires dans le cloud pour répondre aux besoins changeants des clients. Avec l'augmentation des appareils, des sites et des utilisateurs à connecter, cette architecture et cette méthode ne sont pas durables à long terme. Le fait de simplement déplacer un logiciel pour l'exécuter dans le cloud ne signifie pas qu'il exploite pleinement le potentiel évolutif de la technologie cloud.

Pour maximiser les avantages du cloud, le Borderless SD-WAN utilise des conteneurs logiciels et des microservices, chacun pouvant être mis à l'échelle indépendamment grâce à la flexibilité des ressources cloud. Cette architecture permet au Borderless SD-WAN de déployer et de gérer efficacement des milliers de sites, d'appareils IoT et de terminaux utilisateurs.

JARGON TECHNIQUE

Plus spécifiquement, le Borderless SD-WAN de Netskope repose sur une plateforme cloud distribuée intégrant plusieurs niveaux de redondance, des instantanés de sauvegarde et un basculement automatique. Tous les éléments de l'architecture du Borderless SD-WAN sont hébergés dans un cluster redondant et résistant aux pannes, où les services sont déployés en mode actif-actif pour assurer à la fois l'équilibrage de charge et une haute disponibilité.

Cette configuration permet au Borderless SD-WAN de garantir non seulement une haute disponibilité de manière autonome, mais aussi d'auto-évoluer chaque service régulièrement. Chaque service est installé derrière un ensemble d'équilibreurs de charge conçus pour la haute disponibilité (HA), et la charge de chaque groupe est surveillée grâce à divers indicateurs.

En cas de surcharge dans un groupe, des machines supplémentaires sont ajoutées pour mieux répartir la charge. Les services du Borderless SD-WAN sont conçus pour être sans état, ce qui leur permet de s'adapter de manière élastique, aussi bien entre les instances de serveurs au sein d'un même centre de données qu'entre différents centres de données, sans interruption ni impact sur les performances.

Remodeler les plans de gestion, de contrôle et de données

L'architecture Borderless SD-WAN rend les plans de gestion, de contrôle et de données plus intelligents et sophistiqués. Dans cette section, nous décrivons les nouvelles approches pour chaque plan et leurs nouvelles capacités.

Le plan de gestion

Le *plan de gestion* du SD-WAN provient d'un service centralisé, généralement situé sur une machine virtuelle (MV) dans un centre de données ou potentiellement dans le cloud. Sa fonction principale était de gérer les dispositifs SD-WAN des filiales, en veillant à leur mise à jour, approvisionnement et contrôle, pour que le logiciel SD-WAN fonctionne correctement sur le matériel de l'entreprise. Cette approche était efficace jusqu'à l'émergence de nouveaux défis.

Aujourd'hui, les entreprises doivent gérer une multitude d'appareils IoT et personnels, ainsi que des ordinateurs portables qui se connectent au réseau et à des environnements multicloud. Le Borderless SD-WAN est conçu pour prendre en charge tous ces cas d'utilisation, ainsi que la gestion des données qu'ils génèrent et la configuration des applications.

C'est pourquoi le plan de gestion dans le Borderless SD-WAN a été entièrement transformé. Il s'agit désormais d'un système cloud natif, hautement redondant, multitenant et accessible via une interface web intuitive et facile à utiliser. Cette transformation était cruciale puisque le Borderless SD-WAN remplit plusieurs rôles essentiels :

- **Gestion de logiciels sur des cas d'utilisation distribués :** il est nécessaire d'assurer des performances élevées et une connectivité sécurisée pour tous les utilisateurs, tous les appareils, toutes les filiales et dans des environnements multicloud. Le Borderless SD-WAN doit orchestrer le logiciel dans ces contextes élargis, une responsabilité bien plus grande que la simple gestion de quelques dispositifs SD-WAN traditionnels.
- **Gestion des données et de la télémétrie :** le Borderless SD-WAN est chargé de traiter toutes les données et informations de télémétrie que le réseau reçoit, ce qui est réalisable grâce à sa capacité d'évolution.
- **Gestion d'un nouveau modèle de travail à distance :** il doit gérer efficacement et en toute sécurité le travail à distance à grande échelle, où le défi n'est plus de gérer 400 bureaux distants, mais plutôt des milliers d'utilisateurs à distance, chacun générant et consommant des données.

CONSEIL

Grâce au Borderless SD-WAN, les entreprises profitent d'une configuration et d'une visibilité totales sur tous leurs dispositifs réseau via le plan de gestion. Le Borderless SD-WAN offre aussi des informations sur l'état de santé des applications, ainsi que des mises à jour logicielles automatisées et sécurisées pour tous les appareils du réseau simultanément. Contrairement aux produits SD-WAN traditionnels, le Borderless SD-WAN permet une vue de gestion exhaustive de l'intégralité du réseau d'une entreprise et de l'ensemble de ses appareils.

Le plan de contrôle

Le *plan de contrôle* donne aux entreprises la capacité de créer et de gérer la topologie de leur réseau, permettant ainsi à une filiale de se connecter avec une autre. Dans les versions antérieures du SD-WAN, ce plan de contrôle était généralement exécuté sur un dispositif matériel physique, sur lequel se trouvait aussi le plan de données du SD-WAN. Si le plan de données subissait une panne, le plan de contrôle était également affecté, ce qui entraînait un manque de résilience. Parfois, quand le plan de contrôle atteignait sa limite de capacité d'adjacence (par exemple, si le plan utilisait le protocole BGP qui atteignait sa limite d'adjacence), il était nécessaire d'ajouter plus de dispositifs SD-WAN, car le plan de contrôle

et le plan de données cohabitaient sur le même matériel. De plus, le plan de contrôle dans le SD-WAN traditionnel n'était pas conçu pour gérer le volume élevé d'utilisateurs, d'appareils, de filiales et d'environnements multicloud.

Avec le Borderless SD-WAN, le plan de contrôle est déplacé dans le cloud et fourni comme un service SaaS. Il fonctionne en parallèle avec un plan de contrôle sur site comme BGP et OSPF, mais le contrôleur n'est plus physiquement présent dans l'environnement de l'entreprise. Ce service est utilisé par les organisations de la même manière que d'autres services SaaS tels que Salesforce ou Workday. La migration du plan de contrôle vers un modèle SaaS permet au Borderless SD-WAN de s'adapter facilement à la demande. Cela offre également l'avantage aux entreprises de ne plus avoir à investir dans du matériel supplémentaire pour augmenter la capacité du plan de contrôle lors de l'expansion de nouvelles filiales.

CONSEIL

Le transfert du plan de contrôle vers le cloud permet au Borderless SD-WAN de gérer la topologie réseau de façon plus précise et avancée qu'auparavant. Cette évolution est devenue indispensable en raison de l'expansion des réseaux, de l'augmentation du nombre d'appareils personnels et IoT, et de la multiplication des connexions aux passerelles sans fil.

Le Borderless SD-WAN place l'ensemble de ses contrôleurs dans le cloud, offrant ainsi des degrés de contrôle, de facilité d'utilisation et d'extensibilité inaccessibles auparavant dans le SD-WAN traditionnel.

Le plan de données

Grâce à un contrôleur entièrement basé sur SaaS qui offre une visibilité complète du réseau et de tous les appareils connectés, les entreprises bénéficient d'une perspective inédite sur les données transitant sur leur réseau, éliminant ainsi la nécessité de contrôleurs complexes et improvisés sur site.

Le *plan de données* a lui aussi subi des changements majeurs dans le cadre du Borderless SD-WAN. Alors que le MPLS se concentrait sur le routage de paquets, le SD-WAN traditionnel représentait une avancée significative en établissant des décisions et politiques de routage basées sur les applications, sans toutefois tenir compte du contexte lié aux applications, aux utilisateurs et aux appareils. En d'autres termes, le SD-WAN traditionnel n'était pas en mesure de supporter des politiques basées sur les risques associés aux applications, aux interactions utilisateurs ou aux appareils. La sécurité, bien qu'intégrée au SD-WAN, comme le montre la figure 3-1, était soit « adéquate », soit mal incorporée, rendant son fonctionnement opérationnel complexe et incapable de partager le contexte entre le réseau et la sécurité.

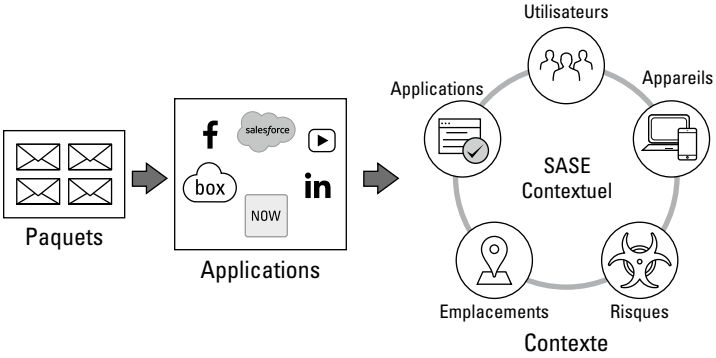


FIGURE 3-1 : Les politiques contextuelles du Borderless SD-WAN prennent en compte la compréhension des applications, des utilisateurs, des appareils, ainsi que des risques qu'ils présentent, rendant ainsi les opérations réseau (NetOps) à la fois intelligentes et sécurisées.

Dans le contexte actuel, illustré par la figure 3-1, les entreprises doivent établir des politiques uniformes concernant les performances des applications, l'accès Zero Trust et la sécurité pour chaque utilisateur à distance, chaque site, chaque appareil et chaque cloud. Le Borderless SD-WAN élève ces fonctionnalités à un niveau supérieur :

- **Un simple clic vers Security Service Edge (SSE) automatise la connexion entre le Borderless SD-WAN et le SSE.** De plus, il facilite l'accès aux services sans nécessiter de configurations de routage du trafic ou l'usage de fichiers PAC (Proxy Auto-Configuration).
- **Le Borderless SD-WAN enrichit le contexte autour de l'utilisateur, de l'appareil, des données et de l'application, ce qui permet de définir et d'appliquer des politiques beaucoup plus efficaces et sophistiquées.** L'évaluation des solutions pour des décisions de sécurité et de routage du trafic contextuelles dans le cloud améliore la gestion des risques pour les utilisateurs, ainsi que la détection et la réponse aux risques liés aux appareils, grâce à des politiques segmentées en temps réel. Imaginez une détection, une priorisation et une optimisation automatiques de plus de 60 000 applications, ou une identification des risques liés aux appareils IoT grâce à l'IA/ML.
- **Le Borderless SD-WAN permet aussi aux utilisateurs, sites, appareils et environnements multicloud distants de rester connectés à un réseau mondial de points de contact.** Combiné avec le SSE, le Borderless SD-WAN s'intercale entre les utilisateurs et les applications à ces points de contact. C'est ainsi qu'il opère sa magie et fournit les services nécessaires pour l'application de

politiques et l'amélioration de la qualité de service (QoS) avec une sécurité intégrée. Cependant, pour que cela soit efficace, la connectivité réseau et les services Borderless SD-WAN doivent être proches de l'utilisateur en termes de réseau. Si toutes les fonctionnalités Borderless SD-WAN et SSE sont centralisées dans un centre de données à Seattle, alors que vos utilisateurs ou filiales sont à Mumbai ou Berlin, l'expérience sera lente et de niveau inégal.

C'est pourquoi Netskope a développé NewEdge, un réseau mondial de points d'accès (PoP).

Netskope NewEdge est un cloud privé spécialement conçu qui intègre des services réseau et de sécurité à grande échelle, offrant des connexions à faible latence dans plus de 70 régions du monde. Le réseau NewEdge permet une intégration transparente des services Borderless SD-WAN et SSE, assurant que les utilisateurs, les filiales, les sites, les appareils et les environnements multicloud à l'échelle mondiale soient à proximité de ces services convergents. Le SSE de NewEdge propose divers services tels que la passerelle web sécurisée de nouvelle génération (NG-SWG), la passerelle d'accès cloud sécurisé (CASB), l'accès réseau Zero Trust (ZTNA), la gestion de la posture de sécurité SaaS (SSPM), la gestion de la posture de sécurité du cloud (CSPM), le pare-feu en tant que service (FWaaS) et la protection contre la perte de données (DLP). Le Borderless SD-WAN de NewEdge assure un routage optimisé pour les applications SaaS et les services intermédiaires dans le cloud. Globalement, NewEdge associé à SSE et Borderless SD-WAN garantit ainsi une connectivité sécurisée et performante pour les applications cloud, web, SaaS et privées.

Faire de la place à l'intelligence artificielle

Dans les plans de gestion du Borderless SD-WAN, il est désormais possible de mettre en place davantage d'opérations pilotées par l'intelligence artificielle (IA) par rapport au SD-WAN traditionnel. Les entreprises bénéficient d'une vue d'ensemble de leur réseau où l'IA peut contrôler en temps réel la qualité et la sécurité des liens pour les appareils externes se connectant au réseau. L'IA est capable d'identifier un lien défectueux et peut aussi se servir des données historiques et du contexte pour anticiper les éventuelles défaillances futures d'un lien. L'apprentissage automatique (ML) et l'IA peuvent offrir des solutions automatisées en cas de problèmes, comme la correction proactive d'erreurs ou la *remédiation automatisée des liens*, permettant un basculement automatique vers une meilleure connexion disponible. Le ML et l'IA sont également capables de détecter automatiquement les appareils IoT et leur comportement, et de mettre en quarantaine ceux qui posent problème.

Le Borderless SD-WAN intègre aussi des analyses de flux détaillées sur les performances des applications à travers le réseau. Ces analyses permettent aux entreprises de visualiser chaque appareil utilisant une application et son expérience utilisateur, et d'exploiter ces données pour établir des lignes de base automatiques. Ces lignes de base définissent ce que sont des performances réseau « normales » en termes de perte de paquets ou de statistiques de flux d'application ; elles tiennent aussi compte du temps et de l'activité du réseau qui varient selon les heures d'ouverture pour les différentes filiales et les utilisateurs distants.

Le Borderless SD-WAN offre également une fonction de suivi intégrée qui surveille chaque utilisateur et chaque filiale, à chaque minute, identifiant les problèmes liés au niveau de service et signalant les violations des accords de niveau de service (SLA) du fournisseur. Ce système de suivi simplifie la gestion en fournissant des détails sur les flux de trafic (et où se trouve la défaillance), signalant les violations de politiques et détectant les anomalies.

En plus, le Borderless SD-WAN va au-delà en fournissant des données exploitables basés sur le ML pour le dépannage réel des appareils au sein des filiales. Par exemple, ses capacités de découverte automatique identifient les appareils accédant aux applications en entreprise ou à domicile, ce qui permet aux services informatiques distants de dépanner ces appareils via un gestionnaire IoT intégré, en réduisant ainsi significativement le temps moyen de résolution des problèmes.

DANS CE CHAPITRE

- Examiner les avantages du Borderless SD-WAN pour les entreprises
- Explorer les avantages pour l'utilisateur final
- Identifier les avantages pour les experts réseau
- Faire des économies avec le Borderless SD-WAN

Chapitre 4
Les avantages du Borderless SD-WAN pour les entreprises

Le Borderless SD-WAN de Netskope propose une gamme de fonctionnalités réseau adaptées aux exigences du monde actuel. Ce réseau étendu défini par logiciel (SD-WAN) est conçu pour satisfaire les besoins contemporains en matière de mobilité, flexibilité, sécurité intégrée et accessibilité permanente de n'importe quel lieu, à tout moment, sur tout appareil. Alors que le SD-WAN a révolutionné le WAN en adoptant un modèle « One-to-Many », le Borderless SD-WAN transforme le réseau vers une approche « Many-to-Many ».

Les avantages de cette évolution ne sont pas exclusivement réservés aux spécialistes des réseaux, car ils sont concrets et se ressentent au quotidien dans l'ensemble de l'entreprise. Si cette perspective n'éveille pas l'enthousiasme de l'aficionado des réseaux en vous, alors qu'est-ce qui le fera ?

Ce chapitre couvre ces avantages au quotidien pour tous les utilisateurs, en plus de certains atouts plus sophistiqués destinés aux professionnels des réseaux responsables de la gestion de la technologie et de l'infrastructure réseau. La lecture de ce chapitre vous fera réaliser que le Borderless SD-WAN ne se limite pas à une fonction de mise en réseau ; il

assure également une connectivité de haute performance et intègre la sécurité de manière fluide. Il représente donc un élément crucial pour les entreprises, en garantissant une expérience homogène à chaque utilisateur, où qu'il se trouve.

Une approche unique : une seule plateforme, un seul logiciel, une seule politique

Avant de poursuivre, examinons le changement de philosophie que le Borderless SD-WAN introduit au sein des entreprises. Cette perspective façonne le reste de l'analyse présentée dans ce chapitre. De nombreuses séries télévisées citent un proverbe populaire, selon lequel chaque individu se doit de suivre un code, une philosophie personnelle (ceci est particulièrement visible dans les représentations de gangs criminels et de clans nobles d'extraterrestres). Il en va de même pour la connectivité. Le principe directeur du Borderless SD-WAN se concentre sur le pouvoir de l'uniformité (voir figure 4-1) et sur la manière dont cette méthode assiste les entreprises dans l'optimisation de leurs processus opérationnels.

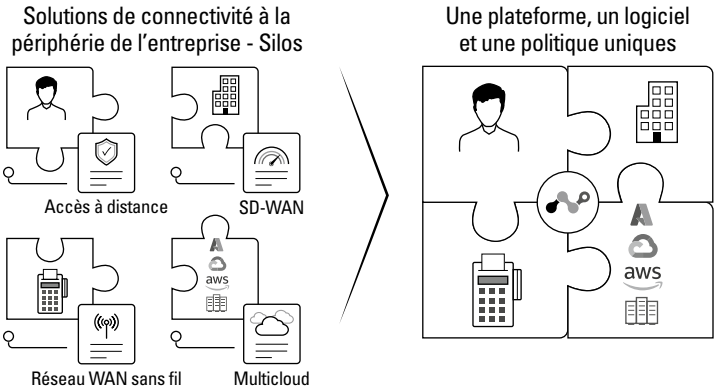


FIGURE 4-1 : L'architecture basée sur le pouvoir de l'uniformité est capable de s'adapter à divers scénarios d'utilisation, d'unir aisément réseau et sécurité, de diminuer les dépenses et de simplifier les procédures opérationnelles.

Ce pouvoir de l'uniformité se manifeste de différentes manières :

- **Il s'agit de créer une expérience utilisateur cohérente, régie par des politiques qui suivent les utilisateurs indépendamment de leur localisation.** Cette uniformité est garantie par un logiciel léger qui fournit un ensemble uniforme de fonctionnalités SD-WAN partout, que ce soit dans une filiale de toute taille ou sur un ordinateur

portable en déplacement. Le même logiciel offre également des fonctionnalités WAN sans fil, une mise en réseau multicloud pour faciliter la connectivité entre applications à travers différents clouds, un accès intelligent à l'Internet des objets (IoT) pour exploiter la valeur commerciale de diverses sources de données, ainsi qu'une surveillance et un dépannage à distance des équipements intelligents.

- **Toutes les solutions Borderless SD-WAN sont gérées à partir d'une console unique.**
- **Cette plateforme intègre de manière transparente le réseau et la sécurité, offrant un accès sécurisé et optimisé et une expérience unifiée qui réduit les coûts et simplifie les opérations.**

Une expérience utilisateur homogène est assurée par une plateforme intégrale qui repose sur un moteur Zero Trust partagé, la gestion de l'expérience numérique et l'interconnexion entre réseau et sécurité. C'est de cette manière que le principe d'uniformité offre finalement un cadre complet de services d'accès sécurisé à la périphérie (SASE) provenant d'un unique fournisseur (plus de détails suivront dans ce chapitre).

Intéressant, n'est-ce pas ? Ce n'est que le début. Abordons d'abord les avantages pour les utilisateurs finaux, avant de discuter des avantages plus étendus des solutions Borderless SD-WAN pour les équipes de gestion des réseaux et les entreprises.

Faciliter la vie des utilisateurs finaux grâce au Borderless SD-WAN

Le Borderless SD-WAN profite à tous les utilisateurs où qu'ils travaillent, y compris un collaborateur dans une filiale, un analyste chez lui utilisant son ordinateur portable pour accéder à des applications d'entreprise à travers le monde, ou un conseiller en centre d'appels cherchant à offrir un service de qualité à un client. Cette technologie dessert même un ingénieur sur le terrain dans un site pétrolier, opérant depuis un véhicule. Voici les avantages du Borderless SD-WAN pour les utilisateurs professionnels au quotidien :

- **Flexibilité et liberté de choix :** les utilisateurs ont la capacité de travailler depuis n'importe quel lieu, que ce soit une filiale ou un site distant, à domicile, dans un café, un véhicule de loisir ou un hôtel, tout en ayant partout accès aux mêmes fonctionnalités SASE (SD-WAN et Security Service Edge [SSE]).
- **Connectivité optimisée :** les utilisateurs peuvent profiter d'un accès hautement efficace à divers clouds et centres de données. Les soucis liés à la performance et à la qualité de service (QoS) sont désormais

résolus. Même les applications gourmandes en ressources telles que Zoom et Microsoft Teams fonctionnent efficacement avec des connexions fluctuantes.

- **Continuité de l'activité :** une protection intégrale, assurée par une passerelle SASE et un client SASE unifié, prévient toute interruption due à des cyberattaques. La sécurité accompagne les utilisateurs, que ce soit sur les sites des filiales ou en télétravail.
- **Accès Zero Trust :** le même accès contextuel Zero Trust est disponible en tout lieu, ce qui permet aux utilisateurs de rester en conformité avec les politiques de l'entreprise. Le système garantit que les politiques suivent les utilisateurs et s'adaptent à leur contexte.
- **Résolution aisée des problèmes :** l'utilisation de l'intelligence artificielle (IA) et de l'apprentissage automatique (ML) donne aux administrateurs informatiques la capacité de diagnostiquer à distance les problèmes des utilisateurs finaux, de diminuer le temps moyen nécessaire pour résoudre les tickets d'assistance et d'améliorer la productivité des utilisateurs finaux.

L'expérience utilisateur est nettement améliorée grâce au Borderless SD-WAN. Pour les utilisateurs mobiles, tels que ceux dans les flottes de camions, la passerelle SASE combine SD-WAN, commutation, routage, Wi-Fi et technologie sans fil, s'intégrant parfaitement avec le SSE. Cela garantit un accès sécurisé et performant à toutes les applications d'entreprise, indépendamment de l'emplacement des utilisateurs.

Les travailleurs à distance profitent d'une productivité améliorée grâce à une connexion fiable, même en présence de connexions instables. Le Borderless SD-WAN optimise constamment la connexion de l'utilisateur à n'importe quelle application, y compris les applications de communication vocale/vidéo exigeantes où le facteur temps est important, telles que Zoom et RingCentral. Par exemple, lorsque ces applications sont utilisées, si des problèmes de latence, de gigue ou de perte de paquets surviennent, le Borderless SD-WAN corrige ces soucis si efficacement que l'utilisateur ne se rend même pas compte d'un éventuel problème. Cette expérience uniforme, de qualité, et cette connectivité sécurisée se produisent entre l'utilisateur et n'importe quel cloud ou centre de données, peu importe l'appareil utilisé et l'emplacement géographique de l'utilisateur.

De plus, avec le SD-WAN et le SSE, les utilisateurs profitent d'une sécurité constante et de politiques d'optimisation réseau au niveau des terminaux, intégrées dans un client SASE unifié sur l'ordinateur portable de l'utilisateur, offrant ainsi la même expérience que les filiales aux sites distants. Leur accès et leur productivité ne sont pas entravés, qu'ils soient au bureau, à domicile, dans un camping-car ou à la plage. Ils jouissent de la même sécurité et d'une connectivité efficace, où qu'ils soient (cela

vous rappelle-t-il quelque chose ?). L'expérience est toujours la même dans l'application.

L'utilisateur bénéficie maintenant d'une plus grande souplesse et d'un plus large éventail de choix concernant le mode et le lieu de travail. Il n'a plus à se préoccuper de sa localisation ou de l'appareil utilisé. Il peut accéder aux applications et travailler comme s'il était physiquement dans un bureau. Voilà une fonctionnalité impressionnante ! Si vous êtes dans une chambre d'hôtel avec une connexion Internet et que vous devez animer une réunion sur Zoom, votre ordinateur portable peut se transformer en un appareil SD-WAN qui gère l'optimisation du dernier kilomètre pour vous fournir automatiquement une expérience vidéo de qualité.

La gestion de la posture de sécurité des logiciels en tant que service (SaaS) dans l'approche SSE (SSE SSPM) surveille constamment les environnements Zoom pour détecter et corriger toute configuration inappropriée qui pourrait compromettre la sécurité, garantissant ainsi la conformité avec les standards de l'industrie et les cadres réglementaires.

Le plus remarquable est que l'utilisateur ne se rend même pas compte que des processus d'optimisation et de sécurisation sont actifs. Il bénéficie simplement d'une connexion stable, sécurisée, optimisée et d'une portée inédite grâce à une connectivité omniprésente. Le Borderless SD-WAN est adapté au monde actuel, caractérisé par de fréquentes connexions « Many-to-Many ».

Ce que les experts en réseau retirent du Borderless SD-WAN

Abordons maintenant les aspects plus techniques et avancés pour les experts en réseau (c'est-à-dire vous !), qui identifient huit avantages principaux dans le Borderless SD-WAN.

Renforcer la confiance opérationnelle grâce à l'AIOps

Les architectes réseau et les équipes d'exploitation disposent de fonctions d'administration qui harmonisent et pérennisent l'optimisation, la sécurité et la visibilité du réseau. Une interface unique (ou, en d'autres termes, une console unique) permet de définir les politiques, de surveiller et d'assister dans la résolution de problèmes pour tous les sites, utilisateurs et appareils du réseau. Les filiales et les utilisateurs jouissent de la même expérience et sont gérés de manière identique. La même orchestration Borderless SD-WAN et SSE utilisée pour les filiales – y

compris les politiques Zero Trust contextuelles mises en œuvre et gérées par les équipes réseau aujourd'hui – peut désormais être appliquée aux utilisateurs individuels utilisant le client SASE unifié. Cette prise en charge unifiée s'étend également aux solutions de réseau multicloud, de réseau étendu sans fil et d'accès intelligent à l'IoT.

Avec le provisionnement sans contact, vous pouvez déployer votre réseau entier, incluant les utilisateurs, les appareils, les sites et le cloud, en quelques minutes seulement. Les politiques peuvent être établies pour l'ensemble du réseau, puis relayées via toutes les passerelles Borderless SD-WAN et tous les terminaux, en utilisant les mêmes fonctionnalités SD-WAN et SSE. Pour la surveillance et l'optimisation du réseau, l'intelligence artificielle (IA) et l'apprentissage automatique (ML) ravissent les experts réseau en identifiant les anomalies dans l'utilisation de la bande passante, en permettant un dépannage automatisé, en apportant un soutien proactif et en fournissant des aperçus sur les flux de trafic et les politiques.

Les effets sont concrets. Disposer d'une vue unifiée de vos solutions réseau clés via une seule console permet aux équipes de gestion du réseau de simplifier tous les aspects de la surveillance, du rapport et de la gestion du réseau. Elles utilisent ainsi leur temps de manière plus efficace, en se concentrant sur des projets à long terme plus stratégiques qui contribueront à la croissance globale de l'entreprise.

Gagner en efficacité et en agilité grâce au SD-WAN contextuel

Le Borderless SD-WAN assure une transparence totale sur les données et les applications au sein d'un réseau hybride, reliant chaque site, utilisateur à distance, appareil IoT et environnement multicloud. Cette visibilité sur les applications est essentielle pour soutenir des utilisateurs qui utilisent une multitude d'applications, y compris des applications SaaS ainsi que diverses applications personnelles et professionnelles, que ce soit dans le cloud ou sur site. L'entreprise moderne a maintenant besoin d'un SD-WAN Zero Trust contextuel pour garantir un accès rapide, fiable et sécurisé à toutes les applications et tous les appareils, partout, tout en offrant une visibilité complète et des contrôles appropriés.

Le Borderless SD-WAN est capable de catégoriser le trafic par application sur tous les ports en standard. L'objectif est d'assurer une qualité de service optimale pour les applications essentielles, tout en évitant de gaspiller des ressources, de la bande passante et du temps d'exploitation sur des applications moins critiques. Avec des dizaines de milliers d'applications SaaS existantes, il est irréalisable pour les équipes de gestion de réseau de configurer des politiques de qualité de service pour chacune d'entre elles. La solution SASE de Netskope intègre une base de données de plus de 60 000 applications (comme nous l'expliquons au chapitre 1 et ailleurs), classées par un indice de confiance dans le cloud (CCI) qui

évalue la préparation de l'application pour un usage en entreprise. Le CCI facilite l'ajustement automatique des applications au niveau approprié de politiques de qualité de service. Nous aborderons ce sujet plus en détail dans le cadre de l'adoption du SASE au chapitre 5.

Netskope possède une base de données de politiques de qualité de service qui sont attribuées aux applications selon l'indice de confiance dans le cloud (CCI) et d'autres facteurs. Ce système d'attribution automatique allège significativement le travail manuel de l'équipe en charge de l'exploitation du réseau, ce qui conduit à des opérations nettement plus efficaces.

Les capacités contextuelles de Netskope peuvent également inclure la détection automatique de tous les appareils IoT, qu'ils soient gérés ou non, ainsi que les micro-segments pour contrôler les risques liés à un appareil compromis.

Augmenter la productivité et améliorer l'expérience des utilisateurs grâce à des performances applicatives garanties

Le Borderless SD-WAN contribue à augmenter la productivité et à renforcer la collaboration en assurant un accès optimisé et extrêmement fiable à toutes les applications, y compris les services de communication unifiée en tant que service (UCaaS). Avec un effort minimal, les spécialistes des réseaux peuvent améliorer l'expérience des utilisateurs, qu'ils travaillent à domicile, dans une filiale ou dans un lieu autre qu'un bureau traditionnel, chez eux, dans un hôtel ou un café. Ceci est possible grâce à des fonctionnalités SD-WAN actives dans les filiales, dans le cloud et sur les ordinateurs portables des utilisateurs. Le Borderless SD-WAN peut également rehausser les performances du réseau avec un basculement en moins d'une seconde dans des situations de liaisons multiples, ou une correction proactive, même sur une connexion Internet large bande unique et instable.

Pérenniser votre investissement avec un contrôleur 100 % SaaS

Autrefois, les contrôleurs SD-WAN devaient être installés manuellement sur place par les administrateurs informatiques. Cette méthode, assez artisanale, était complexe à mettre en place et à développer. Avec les contrôleurs Borderless SD-WAN 100 % SaaS, qui gèrent le routage avancé tel que le protocole BGP (Border Gateway Protocol) et OSPF (Open Shortest Path First), les entreprises peuvent rapidement établir de nouveaux sites et connecter des sites distants. Cette fonctionnalité de contrôle basée sur le cloud signifie que les experts en réseau peuvent aisément passer d'un à des milliers de sites et gérer des centaines de milliers d'utilisateurs et d'appareils IoT, le tout avec une configuration, une

gestion et une visibilité sans complication sur tous les sites à l'échelle mondiale.

Les experts peuvent laisser leurs réseaux s'étendre autant que nécessaire. Ils n'ont plus à anticiper la capacité requise (mesurée en nombre de sites supportés par le réseau SD-WAN). Une passerelle ou un client SASE peut être ajouté à chaque fois qu'une nouvelle filiale ou un utilisateur distant doit être connecté. L'évolutivité devient illimitée, car le contrôleur opère comme un service SaaS. Le réseau peut ainsi s'étendre selon les besoins. Et voilà ! Une solution pérenne.

Étendre la portée et la flexibilité grâce au réseau étendu sans fil

Le monde des affaires dépasse largement les limites des réseaux câblés traditionnels. Cependant, la simple disponibilité de la connectivité sans fil ne garantit pas la connectivité, la qualité de service et la sécurité requises pour le fonctionnement d'une entreprise moderne. Avec les passerelles sans fil Borderless SD-WAN gérées dans le cloud, vous pouvez convertir la connectivité sans fil en un réseau robuste, sécurisé et optimisé, que ce soit pour établir un réseau ad hoc sur un site distant ou dans un bureau temporaire, ou pour fournir une connectivité sans fil rapide, fiable et sans complication.

La passerelle sans fil Borderless SD-WAN peut s'intégrer à votre infrastructure existante et être couplée à toute solution SD-WAN, pour une prise en charge cellulaire principale ou de secours. Cela facilite la création rapide de services réseau, augmentant ainsi la productivité et la flexibilité des entreprises.

Transformer votre entreprise avec le SASE hébergé dans le cloud

Le SD-WAN traditionnel a du mal à offrir une visibilité complète et un accès optimisé depuis n'importe quel utilisateur ou site vers n'importe quel cloud, service SaaS ou application privée. Même en utilisant des méthodes « créatives » avec des installations de hubs SD-WAN bricolées, les environnements de fournisseurs souffrent de latences et ne garantissent pas une connectivité performante. C'est dans ce contexte que la qualité de l'infrastructure réseau devient cruciale.

Netskope NewEdge est le réseau privé de sécurité le mieux connecté dans le monde, avec une présence dans plus de 70 régions, et il fusionne les services de réseau et de sécurité à grande échelle. Il offre des points d'accès au trafic à faible latence distribués mondialement, est soigneusement surveillé et dispose d'une puissance de traitement complète dans chaque région pour le traitement du trafic. Avec une disponibilité cinq neufs et les meilleurs accords de niveau de service (SLA) du secteur, il se démarque

nettement. Le réseau NewEdge signifie que chaque utilisateur, filiale, site, appareil et environnement multicloud partout dans le monde sera proche du Borderless SD-WAN intégré aux services SSE. Les hubs WAN cloud du Borderless SD-WAN et le SSE au sein de l'infrastructure NewEdge distribuée mondialement offrent de multiples niveaux d'avantages :

- **Netskope Borderless SD-WAN dans NewEdge étend la structure SD-WAN des sites locaux à toutes les ressources SaaS et cloud.** Par exemple, en utilisant le SD-WAN avec un client SASE unifié, le trafic de Zoom peut être optimisé pour un utilisateur en télétravail de la même manière qu'il le serait pour un utilisateur dans une filiale de l'entreprise utilisant la passerelle SASE de Netskope. Un autre exemple serait l'utilisation d'un service intermédiaire pour connecter des filiales réparties géographiquement à une application située au siège de l'entreprise sur un autre continent.
- **Grâce à une intégration transparente avec le SSE, le Borderless SD-WAN offre une protection complète contre toutes les menaces de cybersécurité et un réseau hautes performances, garantissant des opérations commerciales ininterrompues.**
- **Le Borderless SD-WAN peut être utilisé pour relier les ressources d'entreprise dispersées sur plusieurs environnements cloud, comme Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP), dans le cadre d'une architecture réseau unifiée.** Avec son routage avancé et son intégration native auprès des fournisseurs de services cloud, le Borderless SD-WAN facilite l'interconnexion entre différentes régions au sein de ces fournisseurs cloud et permet une intégration simplifiée en un clic avec Netskope Intelligent SSE pour les charges de travail déployées dans le cloud.

En offrant ces fonctionnalités, le Borderless SD-WAN permet aux entreprises d'accélérer leur transition vers le cloud, offrant à la fois une connectivité de haute performance et une sécurité appropriée. La gestion d'actifs hébergés à la fois sur site et dans le cloud ne pose plus de problème. Le passage progressif d'une partie plus importante de l'infrastructure vers le cloud est entièrement soutenu, sans se soucier des contraintes du paysage SD-WAN existant. Les limitations fréquentes du SD-WAN traditionnel dans la prise en charge de multiples environnements cloud entraînent souvent des défis logistiques importants – une situation que nous souhaitons éviter pour les experts en réseau.

RAPPEL

Avec le Borderless SD-WAN, les entreprises peuvent contrôler la manière dont chaque cloud communique et interagit avec les autres, ce qui constitue une stratégie d'entreprise efficace pour la gestion du cloud.

Protéger votre entreprise avec une solution de sécurité SASE complète

Le Borderless SD-WAN offre une gamme complète de fonctionnalités de sécurité intégrées. Sur le plan du réseau, il garantit la sécurité du réseau hybride à la périphérie en incorporant des services tels qu'un pare-feu et un système de prévention des intrusions (IPS) pour une segmentation est-ouest. En s'intégrant à Netskope Intelligent SSE, il propose une protection complète avec des capacités de passerelle web sécurisée (SWG), de passerelle d'accès cloud sécurisé (CASB), d'accès réseau Zero Trust (ZTNA), de protection contre la perte de données (DLP), de gestion de la posture de sécurité du cloud (CSPM), de pare-feu cloud et d'autres services de sécurité.

Les services réseau et de sécurité inclus dans le modèle SASE de Netskope sont construits sur NewEdge, une plateforme cloud native rapide, fiable et convergente qui offre la couverture géographique la plus étendue de son secteur, avec plus de 70 régions. Cela se traduit par un faible temps de latence pour la grande majorité des professionnels du savoir dans le monde. Les entreprises bénéficient d'une protection complète contre tous types de cyberattaques et de fuites de données, ce qui contribue à éviter les perturbations et à préserver la réputation de la marque. Les passerelles et les clients SASE sélectionnent automatiquement le point de présence (PoP) SSE le plus pertinent pour la sécurité et l'optimisation. Les professionnels réseau s'enthousiasment de pouvoir déployer le SSE en un simple clic, que ce soit pour les filiales ou les utilisateurs distants. Résultat : une nouvelle approche de la connectivité, entièrement basée sur le cloud, offrant une agilité exceptionnelle aux entreprises.

Exploiter la valeur commerciale des données grâce à l'edge computing

Le Borderless SD-WAN offre une prise en charge native des capacités de calcul en périphérie, permettant ainsi l'exécution de services de conteneurs prêts à l'emploi tels que le runtime Azure IoT Edge, ainsi que la gestion de l'expérience numérique, et bien plus encore. Les administrateurs informatiques ont le choix entre une variété de services disponibles dans un catalogue ou peuvent même intégrer leurs propres applications personnalisées. Avec des fonctionnalités avancées de gestion du cycle de vie des applications (ALM), les entreprises sont en mesure de déployer ces services à grande échelle et de les distribuer sur des milliers de passerelles SASE en un simple clic.

Réduire les coûts informatiques globaux

Les avantages offerts par le Borderless SD-WAN se traduisent par une empreinte réseau consolidée, remplaçant ainsi la configuration multi-fournisseurs du SD-WAN par un seul produit provenant d'un unique fournisseur. Cette simplification conduit à des économies significatives en matière de coûts de support réseau. La formation du personnel opérationnel à une multitude de produits de différents fournisseurs peut rapidement devenir une dépense considérable, dépassant parfois même les coûts d'investissement et d'exploitation des produits eux-mêmes.

Le Borderless SD-WAN permet d'éliminer ces solutions cloisonnées et non intégrées, en réduisant ainsi les coûts et en offrant un meilleur retour sur investissement. En remplaçant plusieurs produits et consoles par un logiciel unique et léger qui répond aux besoins essentiels des clients, le Borderless SD-WAN réduit la complexité. Les experts en réseau acquièrent un nouveau contrôle, ce qui est essentiel pour leur métier. De plus, la gestion centralisée et native de l'ensemble du réseau réduit la charge administrative.

Le Borderless SD-WAN permet aux entreprises d'économiser sur les dépenses d'investissement (CapEx) et sur l'ensemble des opérations informatiques. Avec une seule console, une seule automatisation et un seul logiciel pour gérer l'ensemble du réseau, les entreprises réalisent des économies substantielles et augmentent leur retour sur investissement (ROI). Par exemple, leBorderless SD-WAN de Netskope a permis à ses clients d'obtenir des économies d'au moins dix fois le coût total de possession (TCO) grâce à son architecture convergente et ses technologies.

DANS CE CHAPITRE

- Surmonter les défis de sécurité du réseau étendu défini par logiciel (SD-WAN)
- Utiliser le SASE (Secure Access Service Edge) pour fusionner le réseau et la sécurité
- Naviguer dans le parcours SASE

Chapitre 5
Accélérer l'adoption du SASE

Examinons maintenant comment intégrer la sécurité dans le Borderless SD-WAN de Netskope au sein d'une architecture SASE étendue. Les entreprises, en quête d'innovations numériques distinctives, ont accéléré l'adoption du SASE. Cette évolution a suscité un besoin pour de nouvelles compétences numériques, comme le cloud computing et la fusion de la sécurité et des réseaux à travers les produits, l'architecture et l'organisation.

Le SASE combine plusieurs concepts, notamment Zero Trust, SD-WAN et Security Service Edge (SSE), pour nous guider vers une politique de sécurité et de mise en réseau qui protège et régit le cloud et le nouvel environnement de travail à distance. Pour réaliser pleinement le concept de SASE (Secure Access Service Edge), il est impératif que le réseau et la sécurité soient définis par logiciel et déployés via le cloud. Cette approche repose en partie sur la consolidation et l'intégration des fonctionnalités de sécurité, qui constituent le cœur de la stratégie SASE.

Le SSE délocalise les points de contrôle et d'inspection stratégiques vers le(s) cloud(s) où votre entreprise exerce ses activités. Cette évolution place la sécurité à proximité de l'endroit où les données, les applications et les personnes opèrent – là où se trouve le danger. Le SSE, en synergie avec le Borderless SD-WAN, offre une efficacité remarquable car il est piloté par logiciel et ses services essentiels sont nativement hébergés dans le cloud. Cette configuration améliore la connectivité pour chaque

utilisateur, appareil, site, application et composant de l'infrastructure d'entreprise, sans compromettre la performance.

L'association du Borderless SD-WAN avec le SSE est donc cruciale pour l'implémentation réussie d'un SASE. Ce chapitre se penche sur les défis de sécurité inhérents à un environnement Borderless SD-WAN traditionnel et examine comment l'émergence de nouvelles technologies permet aux entreprises de renforcer leur sécurité dans une architecture orientée cloud.

Le problème de la sécurité dans les réseaux SD-WAN avant l'avènement du SASE

Le Borderless SD-WAN a pour but de faciliter le travail mobile du personnel moderne, en permettant de travailler de n'importe où et sur tout appareil. Les utilisateurs doivent pouvoir accéder aisément à toutes les applications. Ils doivent être assurés que, où qu'ils se trouvent et quelles que soient les applications utilisées, ils bénéficient d'une expérience uniforme et que les fonctionnalités clés de l'entreprise sont à leur portée. Toutefois, la sécurité demeure primordiale pour ces utilisateurs, appareils, sites et applications. Ainsi, il est crucial d'intégrer le Borderless SD-WAN à une infrastructure de sécurité robuste, assurant la protection de chaque élément du réseau d'entreprise.

Pour saisir les enjeux de l'intégration de la sécurité au Borderless SD-WAN, il est utile de comparer la situation actuelle avec celle du SD-WAN traditionnel.

Dans ce dernier, les connexions partent d'une filiale physique vers divers fournisseurs d'infrastructure en tant que service (IaaS), de plateforme en tant que service (PaaS) ou de logiciel en tant que service (SaaS), ainsi que vers tout fournisseur de communications unifiées en tant que service (UCaaS). Ces connexions sont adaptées aux exigences spécifiques des utilisateurs et aux applications qu'ils souhaitent utiliser. Un défi majeur avec le SD-WAN traditionnel réside dans la gestion efficace de la sécurité. En effet, la sécurité est devenue le point faible, le talon d'Achille, du SD-WAN traditionnel. Il est important de noter que, concernant les applications, le SD-WAN traditionnel a été conçu pour identifier, prioriser et sécuriser uniquement un nombre limité d'applications, de l'ordre de quelques milliers. Cette limitation est particulièrement contraignante dans le contexte actuel où les applications se multiplient rapidement.

Initialement, cette configuration fonctionnait bien, mais elle est rapidement devenue insuffisante.

Dans le monde actuel, où les entreprises transcendent les frontières géographiques, le périmètre de réseau s'est élargi bien au-delà des filiales

classiques. Il englobe désormais des micro-filiales, des sites distants utilisés par les collaborateurs et des appareils connectés à l'Internet des objets (IoT), s'étendant à travers divers environnements multicloud. La nécessité impérative est de sécuriser tous ces éléments. Face à ces nouveaux périmètres, les architectes réseau ont commencé à intégrer diverses solutions ponctuelles pour la sécurité et la connectivité. Cette démarche a abouti à un réseau hétérogène, composé de technologies variées et souvent incompatibles, obligées de fonctionner conjointement. Cette complexité s'est souvent avérée problématique, tant pour les utilisateurs finaux que pour les équipes de gestion informatique (ITOps). Une telle architecture fragmentée peine à appliquer uniformément les politiques de sécurité et de qualité de l'expérience (QoE) sur l'ensemble du réseau, incluant utilisateurs, appareils, sites et clouds. De plus, avec l'apparition de dizaines de milliers de nouvelles applications dans le cloud, un modèle auquel le SD-WAN traditionnel n'était pas adapté, les défis se sont intensifiés. Comme le dit le proverbe, il est impossible de prioriser ou de sécuriser ce qui n'est pas détecté. Le SD-WAN traditionnel s'est donc heurté à un obstacle majeur avec l'incapacité de détecter ces nouvelles applications.

En outre, la faible visibilité et le manque de contrôle détaillé sur les appareils de l'Internet des objets (IoT) représentent une menace sérieuse pour la sécurité des entreprises. Le SD-WAN traditionnel, limité dans sa capacité à gérer l'impact des appareils IoT compromis, s'est avéré insuffisant. Face à cette lacune, il est devenu crucial d'enrichir le modèle de sécurité avec une approche Zero Trust. Cette intégration vise à fournir des services SD-WAN adaptés aux exigences contemporaines des entreprises, à la fois à la périphérie du réseau et sur l'ensemble du réseau WAN.

Pour garantir une sécurité complète contre les cyberattaques dans le cadre du SD-WAN, certaines organisations ont choisi de rediriger l'ensemble du trafic vers un site central, comme un centre de données. De ce point central, elles se connectent à l'Internet et à différents clouds pour accéder aux services IaaS, PaaS et SaaS. Or, malgré le renforcement de la sécurité, l'expérience utilisateur a été affectée là encore par des problèmes de latence et de performance dus à ce routage centralisé. Pour contourner ces problèmes de backhauling et la latence associée, d'autres entreprises ont adopté une approche de sécurité distribuée sur chaque site. Certaines ont ajouté des dispositifs de sécurité individuels à leurs solutions SD-WAN existantes. D'autres ont recouru à des solutions plus complexes, appelées solutions SD-WAN « lourdes », impliquant des chaînages de services au sein des mêmes dispositifs. Ces approches, bien qu'efficaces, se sont révélées coûteuses et complexes à gérer et à échelonner. Certains fournisseurs de SD-WAN, proposant des fonctionnalités de pare-feu de base, ont prétendu offrir une *sécurité suffisante* au niveau des filiales. Cependant, une sécurité réseau jugée « suffisante » ne pouvait pas remplacer une sécurité de haut niveau, nécessaire pour répondre aux exigences de sécurité globales de l'entreprise.

Affirmer que l'harmonisation du réseau et de la sécurité pour chaque utilisateur distant, chaque filiale, chaque appareil IoT et chaque environnement multicloud représente un exercice d'équilibrage complexe est un doux euphémisme. Cela équivaut à essayer de nettoyer une plage en retirant chaque grain de sable individuellement – une tâche herculéenne, presque aussi ardue que celle de Sisyphe. (Nous avons relevé le défi de condenser un maximum de métaphores dans ces deux phrases, et nous croyons avoir réussi.)

La sécurité cloud a ouvert la voie au SASE

L'avènement et la popularité croissante de la sécurité via le cloud ont initié un tournant dans les stratégies des fournisseurs de SD-WAN. Ils se sont orientés vers des collaborations avec des fournisseurs de solutions de sécurité cloud pour pallier les risques liés à l'autorisation d'accès direct à Internet via le cloud. Cette évolution marque une rupture avec les méthodes antérieures, où le trafic SD-WAN était routé à travers les centres de données de l'entreprise pour l'inspection de sécurité, provoquant des boucles de trafic réseau et des latences élevées, ou bien la nécessité de déployer une pile de sécurité complète dans chaque filiale.

Avec le temps, il est devenu évident que la sécurité basée sur le cloud était la voie à suivre, ce qui a préparé le terrain pour le SASE. Les entreprises sont maintenant en quête d'une unification de leurs architectures réseau et de sécurité, pour simplifier les opérations tout en permettant un partage de contexte entre le SD-WAN et les solutions de sécurité cloud. Ceci vise à améliorer les contrôles de sécurité, en les rendant plus efficaces et plus détaillés.

Le SASE : conçu pour unifier les réseaux et la sécurité

Le SASE et le SSE incarnent la façon dont la sécurité migre vers le cloud et devient plus efficace que toutes les solutions utilisées auparavant. Le SSE est la manière dont tous les services de sécurité nécessaires au SASE (qui étaient auparavant des applications, des produits ou des services distincts, émanant souvent de fournisseurs différents) sont réunis sous une forme unifiée et intégrée qui offre une capacité et une efficacité accrues, et réduit la complexité et les coûts. Le SASE est une vision globale de la transition des fonctionnalités réseau et de sécurité vers le cloud. Le SSE regroupe l'ensemble des fonctionnalités de sécurité nécessaires, alors que le Borderless SD-WAN rassemble toutes les capacités réseau essentielles. Le SASE, quant à lui, fusionne ces deux domaines, en combinant réseau et sécurité.

Il propose un ensemble de services unifiés de réseau et de sécurité et devient le point central d'inspection pour l'ensemble du trafic, en assurant une protection constante et uniforme pour tous les utilisateurs, données, appareils, sites et applications. Le SASE fonctionne comme le cerveau central de votre réseau et de votre sécurité, reliant et coordonnant tous les « sens » ou aspects de ces systèmes. Il connecte et optimise, interprète les données, évalue l'ampleur des risques et détermine le niveau d'accès approprié en tout temps, quel que soit le scénario.

Netskope Intelligent SSE tire pleinement parti du cloud en intégrant des fonctions de sécurité clés pour les entreprises, telles que la passerelle d'accès cloud sécurisé (CASB), la passerelle web sécurisée (SWG), l'accès réseau Zero Trust (ZTNA), la protection contre la perte de données (DLP), la gestion de la posture de sécurité dans le cloud (CSPM), la gestion de la posture de sécurité SaaS (SSPM), la gestion de l'expérience numérique (DEM), et le pare-feu en tant que service (FWaaS). Cette intégration assure une synergie entre ces différentes fonctions. Avec l'intégration en un clic et grâce à Netskope NewEdge, le Borderless SD-WAN peut faciliter la fourniture de ces services SSE au plus près du point d'accès des utilisateurs, des données et des applications. Les points de présence (PoP) de NewEdge, répartis à travers le monde, garantissent une latence minimale permettant aux utilisateurs d'accéder à toutes les applications, de n'importe où, en assurant ainsi des performances élevées et une connectivité de qualité supérieure, favorisant l'adoption du SASE. Netskope NewEdge joue également un rôle crucial en sécurisant avec le SSE et en offrant un accès optimal à tous les services cloud via le Borderless SD-WAN, y compris l'optimisation des applications UCaaS essentielles aux entreprises.

Qu'en est-il de la périphérie de l'entreprise, où se trouve la passerelle SASE et d'où partent les utilisateurs et les appareils ? Cette configuration intègre nativement un pare-feu avancé de couche 7 et un système de prévention des intrusions (IPS), offrant ainsi une sécurité renforcée à la frontière du réseau.

Les prochains paragraphes aborderont en détail les fonctionnalités de sécurité intégrées de Netskope SASE :

- **Classification :** identifie les informations sensibles, idéalement lorsqu'elles sont créées, mais également par le biais d'analyses périodiques des banques de données.
- **CASB :** sert de point d'application de la stratégie de sécurité placé entre les consommateurs de services cloud et les fournisseurs de services cloud pour appliquer les stratégies de sécurité de l'entreprise lors de l'accès aux ressources basées sur le cloud.

- **SWG :** contrôle l'accès et protège uniquement contre les menaces du Web. La passerelle web sécurisée de nouvelle génération (SWG) de Netskope s'attaque aux menaces et aux risques liés aux données dans le cloud pour les instances personnelles des applications gérées, des milliers d'applications informatiques virtuelles et des services cloud.
- **ZTNA :** applique le principe selon lequel personne ne jouit d'une confiance aveugle et n'est autorisé à accéder aux actifs de l'entreprise avant d'avoir été vérifié comme légitime et autorisé. L'accès avec le minimum de privilèges permet d'accéder uniquement aux ressources dont les utilisateurs ont besoin, rien de plus.
- **Isolement du navigateur à distance (RBI) :** sépare les appareils des collaborateurs de l'acte de navigation sur Internet en hébergeant et en exécutant toute l'activité de navigation dans un conteneur distant basé dans le cloud. Ce « sandboxing » protège les données, les appareils et les réseaux contre toutes sortes de menaces provenant de sites web malveillants.
- **FWaaS :** garantit la sécurité de tous les ports et protocoles sortants pour un accès direct à Internet, soit via un agent installé sur un appareil géré, soit par l'intermédiaire des protocoles GRE (Generic Routing Encapsulation) et Ipsec (Internet Protocol Security) pour les bureaux.
- **DLP :** la protection contre la perte de données (DLP) de Netskope prévient l'exfiltration de données, qu'elle soit intentionnelle ou accidentelle, résultant d'une utilisation inappropriée, délibérée ou non. Netskope DLP garantit une identification précise de toutes les données sensibles, sous n'importe quelle forme, tout en maintenant un taux d'erreur le plus bas possible.
- **La sensibilisation aux menaces et leur neutralisation (également appelée protection contre les menaces avancées ou [ATP]) :** identifie les signes indiquant qu'un environnement a été compromis et prend des mesures pour réduire ou éliminer la probabilité de nouvelles attaques.
- **CSPM :** identifie et corrige les problèmes de mauvaise configuration entre les organisations et les environnements IaaS des fournisseurs de services cloud (CSP) comme Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).
- **SSPM :** évalue la configuration des applications SaaS et élimine les erreurs de configuration qui pourraient permettre l'exfiltration, l'usurpation d'identité ou d'autres types d'attaques.
- **Sécurité sur site :** les services de sécurité peuvent aussi être déployés sur site. Le trafic interne, ou trafic est-ouest, bénéficie également des avantages d'un pare-feu de nouvelle génération (NGFW), d'un système de détection d'intrusion (IDS), entre autres, mis en place localement via la passerelle SASE Borderless SD-WAN.

Le SASE est un parcours : comment s'orienter dans ce paysage ?

Une architecture SASE efficace, incorporant le Borderless SD-WAN, peut adopter différentes configurations, adaptées aux besoins spécifiques de chaque entreprise. Par définition, un déploiement SASE réussi se caractérise par un nombre réduit de fournisseurs, une simplification des opérations, une diminution de la complexité, une réduction des coûts, ainsi que des performances réseau améliorées, plus rapides et fluides, le tout assorti d'une sécurité complète. Cependant, une telle amélioration ne se réalise pas instantanément.

RAPPEL

Le SASE est un processus évolutif, plutôt qu'une simple opération de remplacement. Dans la majorité des cas, la consolidation des fournisseurs s'effectuera progressivement, au fil du temps.

De nombreuses entreprises utilisent déjà des solutions de sécurité cloud fournies par des prestataires SSE et pourraient opter pour un SD-WAN qui s'harmonise au mieux avec leurs systèmes de sécurité existants. Inversement, si une entreprise est déjà équipée d'un produit Borderless SD-WAN, elle a la possibilité de l'intégrer avec la solution de sécurité cloud de son choix. Il n'existe pas d'approche universellement meilleure ou moins bonne ; l'essentiel réside dans les besoins spécifiques de l'organisation et dans la stratégie qui lui permettra d'atteindre ses objectifs commerciaux de la manière la plus efficace.

Les prochaines sections détaillent les avantages spécifiques d'une solution SASE provenant d'un fournisseur unique. Nous vous suggérons de considérer attentivement ces aspects avant de commencer ce parcours et de choisir la direction à prendre. Il est important de se rappeler que, parfois, l'union de deux éléments (1 + 1) peut apporter plus de valeur que leur somme individuelle, surpassant ainsi le chiffre 2.

Le Zero Trust, un SASE tenant compte du contexte

Dans le contexte du cloud, la simple visibilité n'est plus suffisante. Même avec les images les plus détaillées et de la plus haute résolution, il est possible de passer à côté d'éléments cruciaux si l'on ne sait pas où regarder, comment observer, ou ce que l'on cherche précisément. Pour élaborer des politiques SASE efficaces et détaillées, un contexte enrichi, centré sur les utilisateurs, les appareils, les applications et les risques associés, est indispensable. Ce même contexte est également vital pour l'application des principes de sécurité Zero Trust.

Pour les capacités de réseau et de sécurité du SASE de Netskope, le contexte est fourni par Netskope Cloud XD (Xtreme Definition), qui alimente le moteur Zero Trust. Le SSE de Netskope, intégré dans son

architecture SASE, utilise le même moteur Zero Trust que le Borderless SD-WAN. Cette configuration permet un partage efficace du contexte entre les services de sécurité convergente et du réseau. Elle inclut l'application de politiques granulaires basées sur la détection et l'évaluation des risques associés aux applications, aux appareils et aux utilisateurs.

Par exemple, Netskope SSE et Borderless SD-WAN partagent une base de données d'applications commune qui répertorie plus de 60 000 applications. Netskope évalue chaque application en utilisant un Indice de confiance dans le cloud (CCI), qui aide à déterminer la pertinence d'une application pour un usage en entreprise. Avec Netskope SSE, les administrateurs informatiques peuvent s'appuyer sur le CCI pour identifier et évaluer les risques associés à différents services cloud, et prendre des décisions informées quant à l'autorisation ou au blocage de certaines applications dans leur environnement. Ceci permet un contrôle précis de l'utilisation des services cloud et assure la conformité aux exigences de sécurité et de gouvernance. Le Borderless SD-WAN utilise les informations contextuelles du CCI pour établir des valeurs de qualité de l'expérience (QoE) intelligentes par défaut pour la passerelle SASE de Netskope. Cela élimine la tâche complexe et fastidieuse de la configuration manuelle des règles QoE pour des dizaines de milliers d'applications. En tirant parti des données du CCI, le Borderless SD-WAN peut allouer dynamiquement des ressources réseau, telles que la bande passante et la priorité, pour garantir des performances optimales pour les applications critiques (voir figure 5-1).

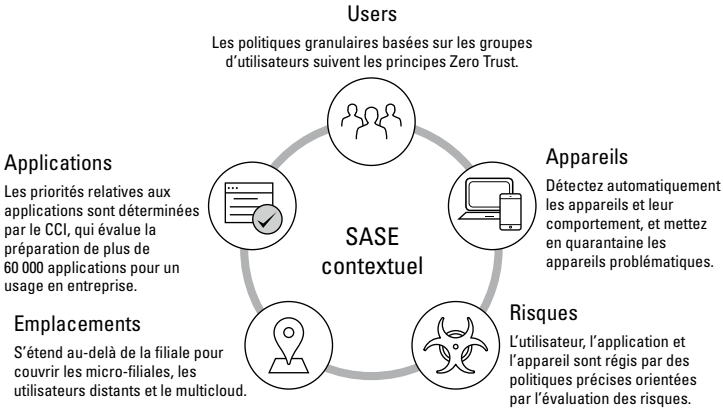


FIGURE 5-1 : Pour élaborer des politiques SASE efficaces et détaillées, un contexte enrichi, centré sur les utilisateurs, les appareils, les applications et les risques associés, est indispensable.

Une politique unifiée et une expérience cohérente en tout lieu

Dans le paysage actuel où évoluent la plupart des entreprises, les filiales et les utilisateurs distants ne bénéficient pas d'une gestion unifiée. La prise en charge traditionnelle du SD-WAN pour les filiales ne considère pas pleinement le contexte ni la sécurité Zero Trust. Cependant, la passerelle SASE Netskope Borderless SD-WAN permet d'implémenter un SD-WAN avec des politiques Zero Trust contextuelles et granulaires. En parallèle, les réseaux privés virtuels (VPN) habituellement utilisés pour les utilisateurs distants souffrent d'un manque de visibilité et d'optimisation, alors que Netskope Endpoint SD-WAN remédie à ces lacunes. Avec les capacités d'intégration du Borderless SD-WAN et du SSE de Netskope, une entreprise moderne est en mesure de fournir un SD-WAN performant et adapté au contexte, aussi bien pour les utilisateurs en filiale que pour les utilisateurs distants (voir figure 5-2).

Le cadre politique unifié qui en résulte assure une expérience utilisateur cohérente et une sécurité qui accompagne les utilisateurs où qu'ils soient. Les architectes réseau et les équipes opérationnelles bénéficient de la plateforme unifiée, de la console et de la politique uniques du Borderless SD-WAN pour configurer et gérer les politiques des filiales. Ces politiques peuvent désormais être étendues aux utilisateurs individuels sur des sites distants. Peu importe la localisation des utilisateurs, des applications et des services, les services informatiques des entreprises peuvent désormais gérer à la fois les filiales et les utilisateurs distants à partir d'une plateforme unifiée, en appliquant une politique uniforme de Zero Trust et de performance réseau sur toute l'infrastructure de l'entreprise. Cette approche intégrée offre une architecture évolutive, des opérations simplifiées, une connectivité de haute performance, et une sécurité renforcée, basée sur des principes Zero Trust contextualisés.

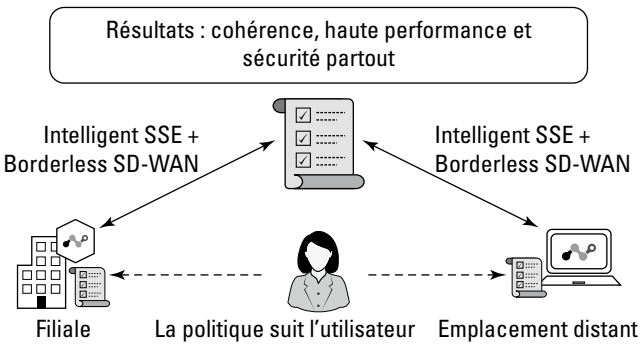


FIGURE 5-2 : À partir d'une seule plateforme unifiée, les équipes informatiques peuvent désormais gérer les filiales et les utilisateurs distants à l'aide d'une politique uniforme de sécurité et de performance du réseau qui suit l'utilisateur.

SASE fourni par le cloud avec une portée mondiale inégalée

Historiquement, les ingénieurs en sécurité et en réseau ont souvent dû jongler entre deux priorités contradictoires : renforcer la sécurité ou améliorer les performances. Selon une règle tacite dans le domaine de la sécurité des réseaux, il est impossible d'atteindre l'excellence dans tous les domaines simultanément : des compromis entre performances, disponibilité et sécurité sont toujours nécessaires. Toutefois, la plateforme NewEdge de Netskope fait exception à cette règle, en répondant efficacement à ces trois critères sans nécessiter de compromis.

Comme mentionné dans le chapitre 3, Netskope NewEdge se positionne actuellement comme le principal cloud privé pour la sécurité, bénéficiant d'une couverture mondiale étendue dans plus de 70 régions. Il réussit l'exploit de combiner des services de réseau et de sécurité à grande échelle, offrant ainsi des itinéraires de trafic à faible latence à travers le monde. Grâce à ses nombreux accords de peering et à une infrastructure informatique robuste dans chaque région, NewEdge traite le trafic de manière efficace. De plus, il assure une disponibilité exceptionnelle, avec un taux de disponibilité cinq neuf, et respecte les accords de niveau de service (SLA) les plus exigeants du secteur. Cette solution garantit donc des performances et une fiabilité optimales.

Avec le réseau NewEdge de Netskope (voir figure 5-3), chaque utilisateur, filiale, site, appareil et environnement multicloud partout dans le monde a accès de manière fluide au Borderless SD-WAN de Netskope, intégré avec les services SSE. Les services SSE disponibles sur NewEdge couvrent une vaste gamme de solutions, incluant la passerelle web sécurisée de nouvelle génération (NG-SWG), CASB, ZTNA, SSPM, CSPM, FWaaS et DLP. Le service Borderless SD-WAN de Netskope au sein du réseau NewEdge étend l'envergure du SD-WAN pour englober les ressources SaaS et cloud. Il optimise le trafic cloud pour les utilisateurs distants et les filiales, facilitant ainsi l'accès et l'utilisation. De plus, il propose un service « mid-mile » qui assure une connectivité fiable entre les filiales dispersées géographiquement et des applications centralisées situées sur un autre continent.

L'association du réseau NewEdge, des services SSE et du Borderless SD-WAN assure une connexion sécurisée et efficace pour l'accès aux applications cloud, web, SaaS et privées. Cette combinaison permet aux organisations de bénéficier d'une infrastructure solide, offrant des performances élevées et un accès sécurisé aux ressources essentielles dans différents environnements.

70 régions
Rampes d'accès au trafic à faible latence et réparties dans le monde entier

Plus de 100 zones de localisation
Pour une plus grande résilience grâce à une expérience locale

Plus de 2 000 adjacences réseau
Les services Microsoft et Google ont fait l'objet d'une surveillance approfondie dans toutes les régions possibles

Calcul complet
Dans chaque région pour le traitement du trafic via la pile SASE complète

Les meilleurs SLA du secteur
Temps de disponibilité à 5 neufs, traitement 10 fois plus rapide, taux de capture des logiciels malveillants de 100 %

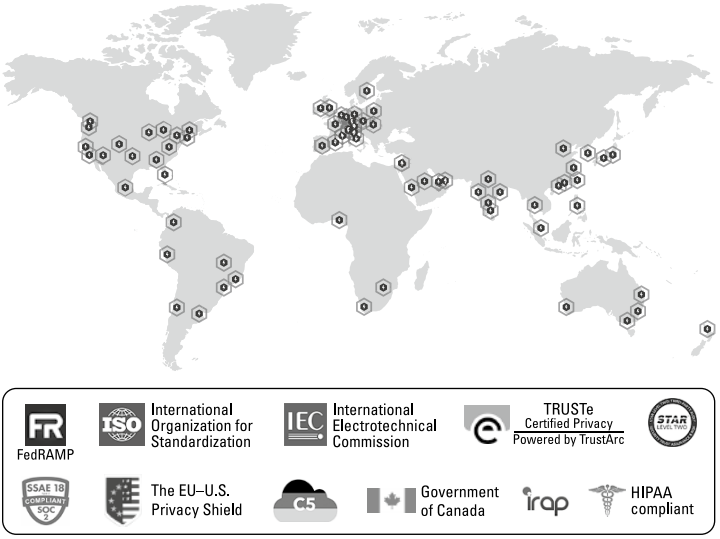


FIGURE 5-3 : NewEdge associe des services réseau et de sécurité à grande échelle, offrant ainsi des itinéraires de trafic à faible latence à travers le monde.

Unifier et simplifier les opérations informatiques (ITOps)

Les utilisateurs, appareils, sites et environnements cloud nécessitent des connexions à la fois sécurisées et performantes. Les approches traditionnelles conduisent souvent à l'utilisation de multiples produits ponctuels disparates, augmentant ainsi les coûts et la complexité. Le SASE, avec

son approche intégrée des services de sécurité et de réseau, offre des avantages significatifs en termes d'efficacité et de rentabilité.

Du côté réseau, un logiciel Borderless SD-WAN unique et allégé peut remplacer plusieurs produits distincts (comme le SD-WAN de filiale, les VPN d'accès à distance, les passerelles sans fil, l'infrastructure multicloud, etc.), réduisant ainsi la complexité (voir figure 5-4). Le SSE de Netskope consolide plusieurs fonctionnalités de sécurité en une seule solution, éliminant le besoin de produits multiples qui ne partagent pas les informations sur les menaces et affaiblissent ainsi la posture de sécurité. En outre, comme mentionné précédemment, le Borderless SD-WAN et le SSE de Netskope s'intègrent de manière transparente et partagent le même moteur Zero Trust. Cette consolidation des fournisseurs SASE simplifie la surveillance et la maintenance des systèmes, améliore la conception du réseau et réduit les dépenses d'exploitation. En exploitant l'intelligence artificielle pour piloter les opérations et en automatisant une grande partie de l'activité de détection et de réponse, il est possible de réduire le volume des tickets d'assistance et de diminuer significativement le temps moyen nécessaire à la résolution des problèmes.

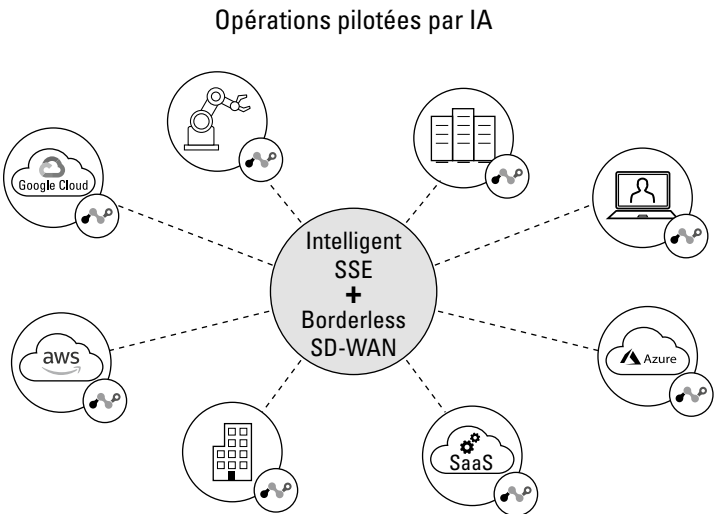


FIGURE 5-4 : Le SASE permet de regrouper plusieurs fournisseurs, de diminuer le nombre de systèmes nécessitant une surveillance, de simplifier la conception des réseaux et de réaliser des économies significatives.

DANS CE CHAPITRE

- **Dynamiser votre entreprise grâce à des architectures réseau diversifiées**
- **Utiliser une solution conçue pour le cloud**
- **Sécuriser et optimiser la connectivité**
- **Explorer l'accès au réseau intelligent et le routage avancé**
- **En savoir plus sur la sécurité globale des réseaux hybrides**
- **Offrir une expérience applicative de premier ordre en tout lieu**
- **Mieux connaître le contexte**
- **Exploiter la puissance des opérations pilotées par l'intelligence artificielle (IA)**
- **Mettre en œuvre une stratégie donnant la priorité au sans fil**
- **Atteindre flexibilité et efficacité grâce à l'orchestration de conteneurs**

Chapitre 6
Les dix principales fonctionnalités nécessaires à l'adoption par les entreprises d'un réseau Borderless SD-WAN

Si vous êtes arrivé jusqu'ici, vous envisagez sûrement de mettre en place le Borderless SD-WAN de Netskope, que ce soit maintenant ou dans un futur proche. Vous vous interrogez probablement aussi sur les capacités spécifiques à rechercher dans une solution Borderless

SD-WAN pour vous assurer qu'elle corresponde parfaitement aux besoins de votre entreprise, surtout après avoir vu comment le Borderless SD-WAN surpasse le SD-WAN traditionnel.

Dans le chapitre 5, nous avons pu explorer comment une solution SASE (Secure Access Service Edge) provenant d'un fournisseur unique peut simplifier votre parcours, en offrant une connectivité sécurisée, fiable et optimisée pour chaque site, cloud, utilisateur distant ou appareil IoT. Ainsi, l'ensemble de votre entreprise pourra bénéficier des avantages d'une plateforme SASE vraiment convergente, qui simplifie les opérations, assure une sécurité uniforme, maintient les performances du réseau et garantit le succès de l'implémentation du SASE.

Les entreprises optant pour la solution SASE à fournisseur unique de Netskope peuvent rationaliser leur architecture grâce à la stratégie de « l'uniformité » (voir chapitre 4), qui repose sur une plateforme unique, un logiciel léger et une politique unique pour gérer à la fois le réseau et la sécurité. Pour mieux cerner les avantages du Borderless SD-WAN, nous proposons une liste de dix fonctionnalités essentielles qui peuvent guider une organisation dans son parcours vers l'adoption du Borderless SD-WAN.

CONSEIL

Si vous êtes du genre à lire les livres de manière non conventionnelle (la curiosité de connaître la fin en premier est parfois irrésistible, n'est-ce pas ?) et que vous lisez ce chapitre en premier, gardez en tête que ces fonctionnalités définissent le cadre approprié pour l'implémentation des solutions Borderless SD-WAN présentées tout au long du livre. Bien que ces dix fonctionnalités soient *primordiales*, elles ne représentent pas la *totalité* de ce que le Borderless SD-WAN peut offrir ; en réalité, la gamme des possibilités offertes par le Borderless SD-WAN est bien plus vaste et s'adapte facilement aux besoins spécifiques de chaque entreprise. Utilisez cette liste comme contexte utile pour les décisions plus stratégiques que vous aurez à prendre dans le cadre de l'adoption d'une solution Borderless SD-WAN.

Dynamisez votre entreprise avec la convergence du SASE

Il n'existe pas d'approche unique pour développer votre architecture Borderless SD-WAN et de sécurité. L'essentiel est qu'elle réponde aux exigences spécifiques de votre entreprise, en contribuant à la réalisation de vos objectifs techniques et métiers. En adoptant une stratégie unifiée à travers le Borderless SD-WAN et l'Intelligent Security Service Edge (SSE) de Netskope, les entreprises peuvent se défaire de la nécessité d'avoir plusieurs produits isolés et parvenir à une efficacité opération-

nelle optimale. Cette fusion de la connectivité et de la sécurité couvre une variété de cas d'usage, y compris les environnements multicloud, les filiales de toutes tailles, les utilisateurs distants et l'IoT. Grâce à une unique solution logicielle allégée, le Borderless SD-WAN s'intègre aisément avec Netskope Intelligent SSE, créant ainsi un réseau à la fois sécurisé, optimisé et performant pour chaque utilisateur, appareil, site et cloud distant. Cette méthode intégrée simplifie la gestion et diminue la complexité, permettant ainsi aux organisations de rationaliser efficacement leurs opérations.

Bénéficiez de toute la puissance du cloud grâce à une solution « cloud first »

Pour une mise en œuvre efficace de services SSE performants, il est essentiel d'adopter une stratégie privilégiant le cloud pour les services SD-WAN et SSE, assurant ainsi flexibilité et évolutivité.

Le Borderless SD-WAN, avec sa gestion centralisée dans le cloud, simplifie les opérations en offrant un contrôle centralisé et en facilitant une connexion rapide des utilisateurs, appareils, sites et ressources cloud, souvent en quelques minutes seulement. Avec une visibilité totale et des données basés sur l'IA et l'apprentissage automatique (ML) sur l'ensemble du réseau (comme détaillé au chapitre 4), les problèmes peuvent être rapidement identifiés et résolus, ce qui contribue à réduire les tickets d'assistance et à minimiser le temps de résolution des incidents. Cette efficacité contribue à maintenir la productivité pour les clients.

En outre, le Borderless SD-WAN distingue clairement le plan de données du plan de contrôle, offrant ainsi évolutivité et résilience. Le plan de contrôle, compatible avec des protocoles de routage tels que BGP (Border Gateway Protocol) et OSPF (Open Shortest Path First), est fourni en tant que SaaS, éliminant ainsi les complexités liées à l'installation improvisée de contrôleurs sur site et simplifiant la gestion. Nous examinons ce point en détail au chapitre 3.

Le Borderless SD-WAN établit une superposition sécurisée, indépendante du transporteur et du mode de transport, créant un réseau conscient du contexte qui relie les utilisateurs distants, les appareils IoT, les filiales, les centres de données et les environnements multicloud. De plus, les services Borderless SD-WAN et SSE sont hébergés sur Netskope NewEdge, avec des points de présence (PoP) stratégiquement répartis. Cette proximité avec les utilisateurs et les applications offre un accès sécurisé et optimisé aux clouds publics et privés, avec des optimisations pour des applications exigeantes comme Zoom et Microsoft 365.

Accès au cloud : sécurisation et optimisation des connexions « Any-to-Any »

Le Borderless SD-WAN offre une visibilité complète et une rampe d'accès optimisée pour chaque utilisateur ou site, facilitant une connectivité transparente à une variété d'applications cloud, SaaS et privées.

Avec les hubs cloud répartis de Netskope NewEdge, le Borderless SD-WAN étend la portée du réseau SD-WAN de l'entreprise depuis les sites physiques (tels que les filiales, les sites régionaux, les campus, les centres de données, les sites distants et les bureaux mobiles) et les rapproche au maximum des services SaaS et cloud pour améliorer les performances.

Par exemple, que ce soit un utilisateur accédant à Zoom depuis un emplacement distant avec un SD-WAN de terminal ou depuis une filiale d'entreprise utilisant la passerelle Netskope SASE, le trafic est optimisé pour assurer une expérience utilisateur de qualité. De la même manière, le Borderless SD-WAN via NewEdge offre un service intermédiaire hautement optimisé et à faible latence qui relie des filiales géographiquement éloignées à des applications situées dans des sièges sociaux sur différents continents.

L'intégration étroite du Borderless SD-WAN avec le SSE, dans le cadre d'une solution SASE complète, assure une protection exhaustive contre les cybermenaces, réduisant ainsi le risque de perturbation de l'activité.

En plus de ses capacités SD-WAN pour les filiales et les utilisateurs distants, le Borderless SD-WAN peut aussi connecter les ressources d'entreprise réparties dans divers environnements cloud, y compris Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP), au sein d'une architecture réseau unifiée. En exploitant un routage avancé et une intégration native avec les fournisseurs de cloud, le Borderless SD-WAN établit aisément des connexions entre différentes régions au sein de ces plateformes cloud. De plus, il permet une intégration facile avec Netskope Intelligent SSE pour les charges de travail dans le cloud, en un simple clic.

Accès au réseau intelligent et routage avancé

La flexibilité est un critère crucial pour les entreprises dans le choix d'un produit. Le Borderless SD-WAN de Netskope excelle en matière de flexibilité, se fondant aisément avec Netskope Intelligent SSE grâce à un accès

intelligent et simplifié en un seul clic. Cette intégration fluide permet de connecter le Borderless SD-WAN à une gamme étendue de services de sécurité, incluant la passerelle web sécurisée (SWG), la passerelle sécurisée d'accès au cloud (CASB), l'accès réseau Zero Trust (ZTNA), la protection contre la perte de données (DLP), la gestion de la posture de sécurité SaaS (SSPM), la gestion de la posture de sécurité cloud (CSPM), le pare-feu en tant que service (FWaaS), et d'autres, offrant ainsi une protection intégrale contre les cyberattaques.

L'intégration de la sécurité est accessible tant au niveau des filiales, via la passerelle SASE, que dans n'importe quel emplacement distant grâce à un logiciel client SASE unifié et léger, qui fonctionne sur les ordinateurs portables des utilisateurs et s'adapte aux environnements multicloud. Ceci assure la mise en place de mesures de sécurité cohérentes et robustes, indépendamment du lieu ou de l'appareil utilisé. Le Borderless SD-WAN prend également en charge des protocoles de routage avancés comme OSPF et BGP, ce qui permet une intégration harmonieuse avec l'infrastructure existante de l'entreprise. Par ailleurs, la distinction entre le plan de contrôle et le plan de données, ainsi que la distribution des clés à l'échelle du cloud, assurent simplicité et évolutivité du plan de contrôle, qui peut être fourni de manière efficace depuis le cloud.

Sécurité complète du réseau hybride

Voici la situation : choisir un SD-WAN sans sécurité intégrée peut engendrer une complexité extrême. Les entreprises se retrouvent souvent à gérer deux systèmes distincts, ce qui peut se transformer en véritable casse-tête logistique. Non seulement cela complique la gestion, mais cela peut aussi affaiblir l'efficacité des composants de sécurité et SD-WAN.

Mais pas de panique ! Le Borderless SD-WAN de Netskope adopte une approche hybride en matière de sécurité réseau, combinant la sécurité sur site et celle basée sur le cloud. Il intègre des services de sécurité essentiels, tels qu'un pare-feu de nouvelle génération (NGFW) et un système de prévention/détection des intrusions (IPS/IDS), directement dans sa passerelle SASE. Votre trafic est-ouest est ainsi sécurisé là où c'est nécessaire.

Et ce n'est pas tout ! Le Borderless SD-WAN va plus loin, en offrant une protection complète à 360 degrés avec des services de sécurité avancés déployés depuis le cloud. Imaginez des outils tels que la passerelle web sécurisée de nouvelle génération (NG-SWG), le CASB, le ZTNA, le SSPM, le CSPM, le FWaaS, et bien plus encore. C'est comme si une véritable forteresse de sécurité entourait votre réseau et le défendait sous tous les angles.

Offrez une expérience applicative hors pair à n'importe quelle application, où qu'elle se trouve

Les entreprises doivent toujours prioriser la fourniture d'une expérience applicative cohérente, fiable et de haute performance à leurs utilisateurs. C'est là que réside l'importance cruciale d'adopter un SD-WAN Borderless. Cette technologie permet aux entreprises de repenser et de réinventer leurs stratégies en matière de mise en réseau, de sécurité et d'optimisation pour atteindre cet objectif.

Le SD-WAN Borderless propose une gamme de fonctionnalités avancées, telles que la sélection dynamique des itinéraires, le basculement ultra-rapide, une qualité d'expérience (QoE) adaptative et granulaire basée sur le contexte, la correction des problèmes de liaison, ainsi que l'optimisation des protocoles TCP/UDP. Ces fonctionnalités travaillent de concert pour garantir des performances et une expérience utilisateur optimales. Il est essentiel pour les entreprises de ne pas faire de compromis sur ces capacités. En adoptant le Borderless SD-WAN, elles peuvent radicalement transformer leur approche de la mise en réseau, en la rendant plus efficace pour offrir une expérience applicative hors pair.

Connaissance contextuelle des risques liés à l'identité de l'utilisateur, à l'appareil et à l'application pour de meilleurs contrôles

Le Borderless SD-WAN de Netskope est conçu pour être sensible au contexte, validant en temps réel l'identité de l'utilisateur, les informations sur l'appareil et les risques liés à l'application. Cette connaissance contextuelle établit un véritable cadre Zero Trust au sein du réseau. De plus, le Borderless SD-WAN se distingue par sa capacité à simplifier la configuration des politiques de Qualité de Service (QoS). Les solutions SD-WAN traditionnelles ne détectent que quelques milliers d'applications, et les administrateurs informatiques doivent configurer individuellement les politiques de qualité de service pour ces applications, ce qui peut prendre beaucoup de temps.

Le moteur Netskope Zero Trust peut aujourd'hui identifier plus de 60 000 applications, attribuant à chacune un indice CCI (Indice de confiance dans le cloud), comme expliqué au chapitre 2. Cet indice CCI sert à évaluer la préparation d'une application pour un usage en entreprise. Avec le Borderless SD-WAN, Netskope utilise ces évaluations CCI

pour appliquer des paramètres intelligents de QoS par défaut, simplifiant ainsi le processus. Cela signifie que les équipes opérationnelles réseau n'ont plus à configurer manuellement les politiques de QoS pour chaque application, économisant ainsi un temps et un effort précieux.

Les capacités contextuelles de Netskope vont au-delà de la simple identification des utilisateurs et des applications. Elles incluent également la détection automatique de tous les appareils IoT, qu'ils soient gérés ou non, permettant à Netskope d'identifier et de gérer les risques associés aux appareils IoT compromis. Grâce à cette connaissance approfondie du contexte, Netskope peut micro-segmenter le réseau en se basant sur l'IA/ML, en isolant et en régulant l'accès et le comportement des appareils IoT. Cela aide à minimiser l'impact potentiel d'un appareil compromis, réduisant ainsi les risques d'accès non autorisés ou de violation de données.

Opérations simplifiées, automatisées et pilotées par l'IA

Imaginez que la solution Borderless SD-WAN de Netskope soit votre assistant dévoué, toujours prêt à vous aider. Elle agit comme un assistant personnel, s'occupant des tâches répétitives pour que vous puissiez vous concentrer sur l'essentiel. En automatisant les processus et en exploitant des opérations pilotées par l'intelligence artificielle, le Borderless SD-WAN apporte une facilité de gestion sans précédent. Que ce soit pour intégrer de nouveaux clients, configurer des passerelles SASE, gérer le SD-WAN des terminaux, ou naviguer dans des environnements multicloud, tout cela devient facile grâce à une plateforme de gestion centralisée.

Mais ce n'est pas tout. L'intelligence de l'apprentissage automatique (ML) rend cette solution Borderless SD-WAN véritablement remarquable. Elle apprend de votre réseau, analyse les flux de trafic, et s'adapte à vos politiques, permettant ainsi d'identifier et de résoudre proactivement les problèmes avant qu'ils ne se manifestent. C'est comme si vous aviez une équipe d'experts travaillant sans relâche pour assurer le bon fonctionnement de votre réseau.

Et n'oublions pas les économies de temps significatives. Avec une surveillance autonome, les anomalies sont détectées rapidement, et vous pouvez anticiper les éventuelles violations des accords de niveau de service (SLA) avant qu'elles ne surviennent. Vous pouvez donc résoudre les problèmes plus rapidement, minimiser les interruptions et reprendre vos activités normales en un temps record.

Prise en charge d'une stratégie donnant la priorité au sans-fil

Une solution complète Borderless SD-WAN vous assiste en termes de connectivité, offrant une conception indépendante du mode de transport qui s'adapte à vos besoins spécifiques. Elle intègre la possibilité d'ajouter des options de connectivité 4G/5G, assurant ainsi une connexion fiable et sans tracas, où que vous soyez. Un des principaux atouts de cette solution est son aptitude à optimiser la force du signal cellulaire. Ainsi, même dans un bureau éloigné ou dans un espace de travail temporaire dépourvu d'accès à la large bande câblée, vous bénéficiez toujours d'une connexion stable et robuste. Elle est particulièrement utile dans des contextes où une connexion filaire à large bande n'est pas disponible, idéale, ou même envisageable.

De plus, le Borderless SD-WAN est conçu pour assurer une interopérabilité globale avec divers opérateurs télécoms. Cette compatibilité étendue à travers le monde vous permet de choisir l'opérateur qui répond le mieux à vos exigences ou qui est le plus performant dans votre région. Que vous ayez besoin d'équiper des microfiliales, des bureaux de taille moyenne, ou de grandes entreprises, cette solution vous offre la flexibilité et l'évolutivité requises pour satisfaire vos besoins de connectivité.

Prise en charge complète de l'edge computing

Le Borderless SD-WAN se distingue avant tout par sa flexibilité et son efficacité, et c'est là que l'orchestration des conteneurs fait toute la différence. Elle vous permet de gérer et de déployer facilement de nouveaux services au niveau de la passerelle sans qu'il soit nécessaire de maintenir un grand nombre de serveurs dans chaque filiale. Imaginez par exemple avoir un conteneur de gestion de l'expérience numérique sur votre passerelle SASE – le suivi en temps réel de l'expérience utilisateur devient alors extrêmement simple ! De plus, cette orchestration facilite grandement l'analyse des données IoT. Elle prend en charge des environnements multicloud comme AWS IoT Greengrass et Azure IoT Hub, vous permettant ainsi d'explorer et d'analyser ces riches données IoT directement à la périphérie du réseau. Cela représente un avantage considérable pour rester à la pointe de la technologie.

La figure 6-1 présente les dix fonctionnalités abordées dans ce chapitre.

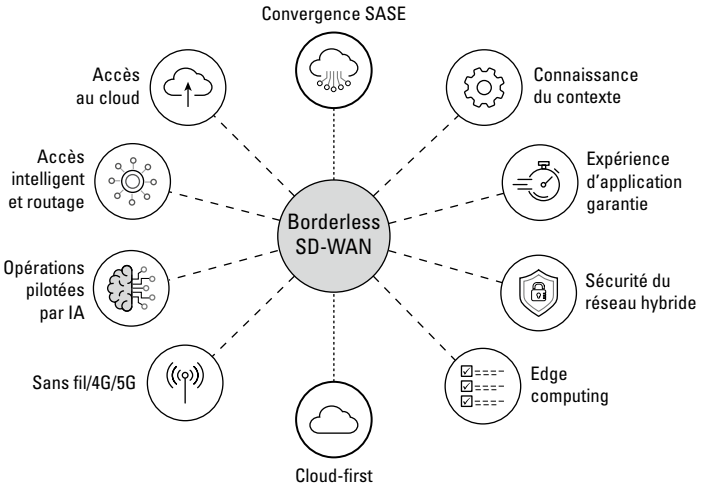


FIGURE 6-1 : Dix fonctionnalités qui peuvent aider une entreprise à démarrer son parcours vers l'adoption du Borderless SD-WAN.

Ready for Anything

Netskope, leader mondial du SASE, permet aux organisations d'intégrer le réseau et la sécurité de manière transparente, de tirer parti d'AIOps, d'appliquer les principes Zero Trust et les innovations AI/ML pour sécuriser les données, grâce une connectivité haute performance et une protection complète contre les menaces. Rapide et facile à utiliser,la plateforme Netskope offre un accès optimisé et une sécurité en temps réel pour les utilisateurs, les appareils et les données, où qu'ils se trouvent. Des milliers de clients font confiance à Netskope et à son puissant réseau NewEdge pour faire face à l'évolution des menaces, aux nouveaux risques, aux changements technologiques, aux changements d'organisation et de réseau, ainsi qu'aux nouvelles exigences réglementaires. Pour savoir comment Netskope aide ses clients à être prêts à tout au cours de leur parcours SASE, **visitez netskope.com/fr/**

netskope

Répondez aux exigences de l'entreprise sans frontières avec le réseau Borderless SD-WAN

Le périmètre réseau des entreprises a considérablement évolué avec l'expansion des microfiliales, du multicloud, du travail à distance, de la télésanté, des flottes mobiles et de l'Internet des objets (IoT). Dans ce contexte, utilisateurs, appareils, sites et environnements cloud sont dispersés, mais interconnectés de multiples manières. C'est dans ce cadre que s'inscrit le Borderless SD-WAN, enrichi de nouvelles capacités offrant une connectivité sécurisée, fiable et rapide. Fondé sur les principes Zero Trust, il intègre des opérations évolutives et pilotées par l'IA, garantissant une expérience applicative et une sécurité renforcée pour plus de 60 000 applications. Il propose également une meilleure prise en charge du sans-fil 4G/5G, et bien d'autres avancées significatives.

À l'intérieur...

- Bénéficiez d'une connectivité rapide et fiable
- Intégrez le réseau et la sécurité de manière transparente et accélérez votre adoption du SASE
- Découvrez six solutions et dix fonctionnalités pour l'entreprise sans frontières
- Réduisez les coûts informatiques et gérez les budgets
- Simplifiez les architectures et exécutez des opérations efficaces

Parag Thakore et **Muhammad Abid,** dirigeants chez Netskope, sont des experts reconnus dans les domaines du cloud computing, de la cybersécurité et des réseaux, possédant de nombreux brevets dans ces secteurs. Avec des décennies d'expérience acquises au sein d'organisations internationales telles que Cisco, VeloCloud/VMware, Infiot, Fortinet et T-Systems, ils ont joué un rôle déterminant dans la transformation du WAN d'entreprise et l'adoption des technologies SD-WAN et SASE.

Allez sur Dummies.com®
pour voir des vidéos, des exemples pas à pas, des articles pratiques, ou pour faire des achats !

ISBN: 978-1-394-21945-2

pour les nuls®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.