LIVRE COMMERCIAL

aruba
a Hewlett Packard Enterprise company

# LES ARCHITECTURES SD-WAN ET SASE DE PREMIER ORDRE « ZÉRO CONFIANCE » SOUS-TENDENT L'ENTREPRISE NUMÉRIQUE

## TABLE DES MATIÈRES

## SYNTHÈSE

Les entreprises continuent à adopter la transformation numérique dans le but d'accroître l'efficacité, d'améliorer la satisfaction du client, de réaliser de nouvelles opportunités commerciales, de booster leur rentabilité et de conserver un avantage sur la concurrence. La migration des applications d'entreprise vers le cloud est inhérente à une initiative de transformation numérique réussie. Pourquoi ? Aujourd'hui, plus d'applications s'exécutent dans le cloud que dans les datacenters d'entreprise traditionnels, la majorité de ces applications étant utilisées en mode SaaS. En outre, dans un monde axé sur le cloud, les entreprises doivent s'assurer que leurs applications sont accessibles directement et sans risque à tout moment, quel que soit l'endroit où depuis n'importe quel device. Elles doivent également s'assurer que leur réseau offre une expérience optimale à leurs employés comme à leurs clients. Enfin, l'explosion des devices mobiles et IoT dans l'entreprise a radicalement accru la surface d'attaque, exposant les entreprises à des failles de sécurité susceptibles de compromettre les données et de provoquer des temps d'arrêt du réseau.

Les réseaux d'entreprise actuels n'ont jamais été conçus pour un monde axé sur le cloud et ne sont pas capables de relever les défis en termes de cybersécurité liés à la transformation numérique. Il est essentiel que les entreprises non seulement sécurisent leurs applications dans le cloud, mais en plus protègent les utilisateurs se connectant à ces applications sur le réseau WAN. Dans le même temps, la prolifération des devices IoT a significativement accru la surface d'attaque exposant les entreprises à des menaces de cybersécurité croissantes.

De ce fait, l'impératif stratégique consiste à adopter un SD-WAN (Software-Defined Wide Area Network) plus intelligent, plus sécurisé et hautement automatisé, pouvant s'intégrer sans heurts à des services de sécurités fournis via le cloud afin de former une architecture SASE (Secure Access Service Edge) de premier ordre. L'architecture SASE doit être renforcée par une sécurité zéro confiance basée sur l'identité afin d'appliquer une segmentation, de sorte que les utilisateurs et les devices IoT n'aient accès qu'aux parties du réseau qui correspondent à leur rôle au sein de l'entreprise.

Parce que la transformation du WAN et de la sécurité est un parcours, une entreprise peut commencer par moderniser son WAN ou sa sécurité mais, pour réaliser la véritable valeur des investissements dans le cloud, les deux aspects doivent être abordés.

**Les réseaux d'entreprise actuels n'ont jamais été conçus pour un monde axé sur le cloud et ne sont pas capables de relever les défis en termes de cybersécurité liés à la transformation numérique. Il est essentiel que les entreprises non seulement sécurisent leurs applications dans le cloud, mais également protègent les utilisateurs se connectant à ces applications. Dans le même temps, la prolifération des devices IoT a significativement accru la surface d'attaque exposant les entreprises à des menaces de cybersécurité croissantes.**

De plus, il est tout aussi essentiel d'éviter un enfermement propriétaire en choisissant des partenaires de solution technologique offrant flexibilité et liberté de choix. Avec des architectures de réseau et de sécurité transformées, les entreprises peuvent adopter des innovations pertinentes pour accélérer leur productivité, la croissance de leurs revenus et leur rentabilité, le tout en contenant les coûts.

## LES APPLICATIONS SONT FOURNIES DANS LE CLOUD — LA SÉCURITÉ DEVRAIT L'ÊTRE ÉGALEMENT

Traditionnellement, le trafic des applications en provenance des emplacements des filiales était entièrement acheminé via des services MPLS privés vers le datacenter d'entreprise à des fins d'inspection et de vérification de la sécurité (voir figure 1). Cette architecture était sensée lorsque les applications étaient exclusivement hébergées dans le datacenter d'entreprise. À présent que les applications et les services migrent vers le cloud, cette architecture réseau traditionnelle est cependant prise en défaut, surtout parce qu'elle nuit aux performances des applications et fournit une expérience incohérente aux utilisateurs, dans la mesure où le trafic d'abord destiné à Internet passe par le datacenter et le pare-feu de l'entreprise avant d'arriver à destination.

De plus, en raison d'un nombre croissant d'employés travaillant en dehors du réseau de l'entreprise et se connectant directement aux applications cloud, la sécurité traditionnelle basée sur un périmètre ne suffit plus. Le cloud et le SaaS ont transformé à jamais la manière dont les utilisateurs se connectent aux applications et interagissent avec elles. En transformant leurs architectures WAN et de sécurité, les entreprises peuvent garantir un accès direct et sécurisé aux applications et aux services dans des environnements multicloud, indépendamment de l'emplacement ou des devices utilisés pour accéder à ces applications et services.

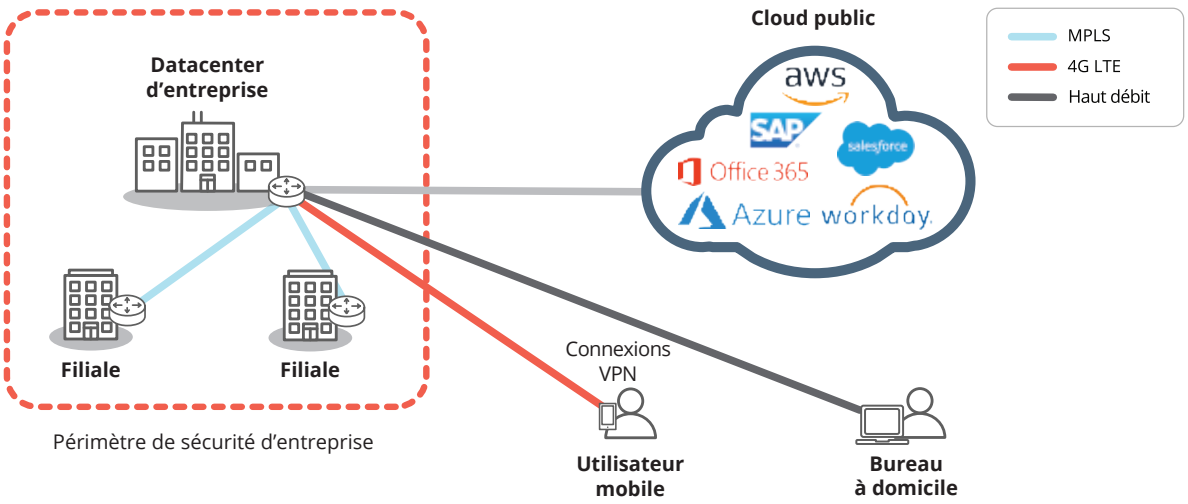


Figure 1 : Les WAN d'entreprise traditionnels et les approches de la sécurité basée sur un périmètre n'ont pas été conçus pour le cloud. Acheminer intégralement le trafic des applications des emplacements des filiales vers le datacenter nuit aux performances et offre une expérience incohérente aux utilisateurs.

En 2019, Gartner a inventé le terme SASE (Secure Access Service Edge) pour un cadre combinant le SD-WAN à des fonctions SSE (Security Service Edge) fournies via le cloud, y compris SWG (Secure Web Gateway), FWaaS (FireWall-as-a-Service), CASB (Cloud Access Security Broker) et ZTNA (Zero Trust Network Access). Il s'agissait auparavant de fonctions uniques et dédiées, mais elles peuvent à présent être fournies à partir du cloud de manière unifiée, comme l'illustre la figure 2.

Certains parmi les premiers à avoir adopté les solutions SSE n'ont pas réussi à mettre en œuvre un SD-WAN capable de mettre en œuvre un breakout Internet adaptatif directement depuis les sites des filiales. Ils n'ont donc pas été en mesure d'orienter le trafic directement du site de la filiale vers le cloud. Sans le composant SD-WAN, le trafic destiné au cloud était encore acheminé vers le datacenter, nuisant aux performances des applications.

Adopter des solutions SSE et le SD-WAN élimine les coûts et la complexité associés à la gestion de plusieurs pare-feu sur site, mais nécessite encore des fonctionnalités de pare-feu au niveau des filiales pour bloquer les menaces entrantes.

Comme le montre la figure 3, grâce à une solution SD-WAN avancée, les entreprises peuvent se connecter directement au cloud via un breakout Internet adaptatif utilisant des connexions Internet haut débit. La capacité de reconnaître les applications sur liste blanche autorise un breakout local depuis la filiale vers le point de présence (PoP) le plus proche, ce qui élimine la latence et offre une expérience optimale pour les applications cloud et SaaS de confiance telles que Microsoft Office 365, 8x8 et RingCentral. La connaissance des applications permet également d'envoyer un autre trafic Internet d'abord à un fournisseur de solutions de sécurité fournies via le cloud en vue d'une inspection avancée, avant de faire suivre ce trafic à un fournisseur SaaS. Des fonctionnalités SD-WAN avancées intégrées à des services de sécurité modernes fournis via le cloud garantissent une mise en œuvre cohérente des politiques et un contrôle d'accès au niveau des utilisateurs, des devices, des applications et de l'IoT. Les entreprises sont ainsi en mesure de mettre en œuvre la conformité, de prévenir les temps d'arrêt et d'atténuer les risques d'atteinte des données liés à une faille de sécurité.

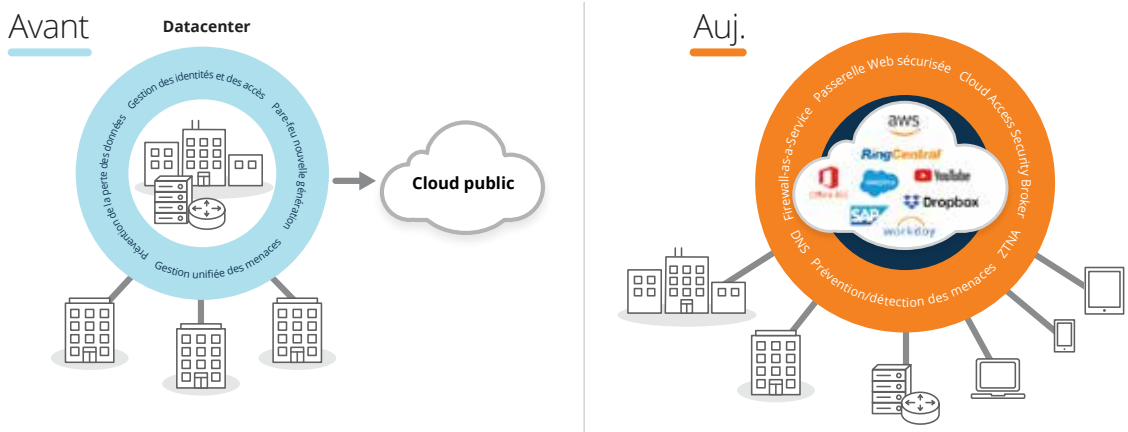


Figure 2 : Auparavant, tout se résumait à sécuriser le datacenter d'entreprise dans lequel les applications étaient exclusivement hébergées. À présent que les applications ont migré vers le cloud et sont fournies à partir du cloud, la sécurité basée sur un périmètre est de moins en moins efficace. Il est impératif de penser différemment et de transférer la sécurité vers le cloud.

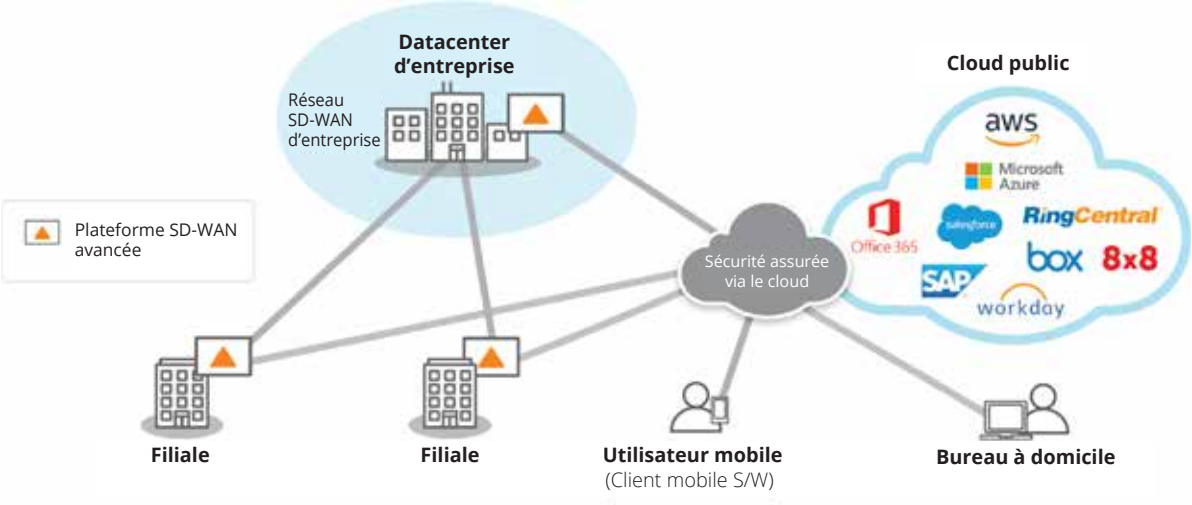


Figure 3 : Un SD-WAN avancé fournit aux entreprises un tremplin sécurisé vers le cloud. Les emplacements de filiale peuvent utiliser des connexions haut débit et un breakout Internet adaptatif pour connecter directement les utilisateurs aux applications cloud, ce qui optimise les performances des applications et l'expérience des utilisateurs. La combinaison d'un SD-WAN avancé et d'une sécurité assurée via le cloud crée une architecture SASE (Secure Access Service Edge) qui garantit la sécurité constante des utilisateurs, des devices et des applications.

## UNE ARCHITECTURE SASE DE PREMIER ORDRE OFFRE LA LIBERTÉ DE CHOIX

Face à l'évolution constante des approches en matière de sécurité du réseau et à la complexité liée à la conception de solutions réseau complexes, il est important d'évaluer les solutions de sécurité et de réseau de premier ordre proposées par des fournisseurs ayant démontré leur expérience et leur expertise. Il n'est pas réaliste de rechercher un fournisseur spécifique capable de fournir des fonctionnalités SASE de premier ordre au niveau de ces deux aspects, et les entreprises ne doivent pas être contraintes d'accepter des compromis dans l'un ou dans l'autre.

Parce que la sécurité est une préoccupation majeure du fait d'un paysage des menaces évoluant en permanence, les entreprises doivent rester agiles pour adopter rapidement et à moindres coûts de nouvelles solutions de sécurité sans s'enfermer dans une solution à un seul fournisseur. Disposer d'une solution de réseau indépendante apporte aux entreprises la tranquillité d'esprit leur permettant de sélectionner et de déployer les solutions de sécurité du cloud s'alignant le mieux sur leurs besoins commerciaux et de sécurité changeants.

Une solution SD-WAN avancée s'intègre étroitement à plusieurs fournisseurs SSE, offrant la liberté de choix qui permet de sélectionner des solutions de fournisseur de premier ordre unifiant le SD-WAN et la sécurité assurée via le cloud par une orchestration automatisée. Avec une architecture SASE de premier ordre, les entreprises construisent une architecture de sécurité cohérente qui bloque l'impact des cyberattaques tout en améliorant l'agilité de l'entreprise et en réduisant la complexité. En définitive, les entreprises peuvent ainsi obtenir un effet multiplicateur à partir de leurs investissements continus dans les applications et les services cloud.

## SÉCURISER L'IOT DE L'ENTREPRISE GRÂCE À UNE APPROCHE ZÉRO CONFIANCE

La prolifération des devices IoT dans les entreprises entraîne des manières nouvelles de surveiller, de signaler, de faire connaître, d'automatiser et d'optimiser les processus commerciaux — des lignes de fabrication à l'automatisation des systèmes CVC et de l'éclairage à des fins d'économie d'énergie. Grâce à l'IoT, les entreprises sont plus efficaces via l'automatisation. Toutefois, l'IoT accroît également la surface d'attaque en ajoutant un nouveau niveau de complexité. Pour relever le défi croissant lié à la sécurité des devices mobiles, l'informatique déploie une solution ZTNA (Zero-Trust Network Access) basée sur le modèle zéro confiance. Une solution ZTNA fonctionne via l'installation d'un agent de point d'extrémité sur un device utilisateur tel qu'un ordinateur portable, une tablette ou un téléphone portable.

Cet agent logiciel s'assure que le trafic en provenance du device est dirigé vers un service de sécurité fourni via le cloud avant d'être dirigé vers une application SaaS ou un fournisseur IaaS. Toutefois, contrairement aux tablettes et aux smartphones, les agents logiciels ZTNA ne peuvent pas s'installer sur des devices IoT car ceux-ci sont sans agent et ne prennent pas en charge l'installation d'agents logiciels tiers. Pour cette raison, les entreprises ont besoin d'une solution de sécurité différente pour les devices IoT afin de protéger leurs réseaux contre les vulnérabilités potentielles susceptibles de provoquer une faille sur le réseau et de perturber les opérations commerciales quotidiennes.

Un SD-WAN avancé prenant en charge une architecture zéro confiance segmente le réseau et applique les principes de l'accès selon le moindre privilège, ce qui permet aux entreprises de limiter le risque associé aux failles lors du déploiement de devices IoT. Il garantit que les utilisateurs et les devices ne communiquent qu'avec des destinations correspondant à leur rôle en fonction de leur statut en termes d'identité, de droits d'accès et de sécurité. Il orchestre la segmentation de bout en bout englobant le datacenter/cloud LAN-WAN-LAN et LAN-WAN, ce qui se traduit par une mise en œuvre des politiques de sécurité cohérente et automatisée avec une plus grande visibilité. Grâce à la segmentation de bout en bout, les entreprises peuvent créer des segments isolés pour le trafic des devices IoT. Une politique de sécurité indépendante peut être définie pour chaque segment définissant les politiques de sécurité à mettre en œuvre pour le trafic des devices. Le trafic existant dans un segment étant isolé du trafic de tous les autres segments, tout accès non autorisé est impossible. Même si une menace devait survenir, son impact serait limité au segment dans laquelle elle se manifeste.

Prenons l'exemple suivant : sur un site distant où des devices IoT sans agent (par exemple, des systèmes PoS et CVC) sont installés (voir la figure 4 ci-dessous), une plateforme SD-WAN avancée identifie les applications utilisées uniquement pas les devices. Une politique système intercepte le trafic PoS et le dirige vers le datacenter d'entreprise dans lequel l'application de traitement des transactions par carte de crédit est hébergée. Dans cet exemple, les services de sécurité de pare-feu existants déployés au sein du datacenter sont exécutés. Par ailleurs, les politiques de système CVC segmentent et dirigent le trafic CVC vers le service de sécurité assuré via le cloud pour une inspection de sécurité supplémentaire avant qu'il ne parvienne au centre de contrôle IoT hébergé dans le cloud public. Puisque le trafic IoT est isolé selon la politique de l'entreprise, une faille dans le segment CVC ne compromet pas ou ne met pas en danger les données personnelles et de carte de crédit dans le segment PoS. La segmentation permet également aux entreprises de se conformer aux exigences de conformité PCI (ou autre). Comme illustré dans cet exemple, un déploiement de sécurité complet intégrant une plateforme SD-WAN avancée peut mieux protéger les entreprises dynamiques d'aujourd'hui dans leur parcours de transformation en adoptant les avantages de l'IoT.

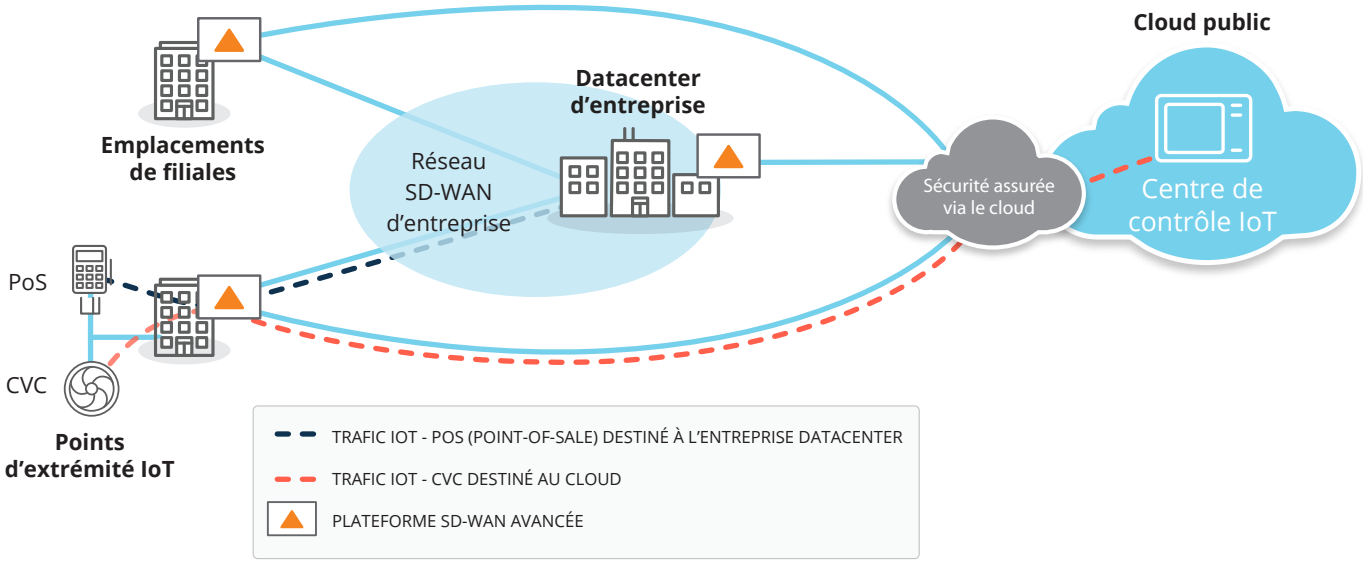


Figure 4 : Les points d'extrémité IoT se multiplient et présentent de nouveaux risques de faille de sécurité. Avec une plateforme SD-WAN avancée, les entreprises peuvent protéger leurs devices IoT en mettant en œuvre une architecture zéro confiance et en segmentant le réseau de manière dynamique. Comme le montre la figure, toutes les données de transaction PoS issues de la filiale sont destinées au datacenter d'entreprise, tandis que le trafic CVC est acheminé vers un centre de contrôle IoT dans le cloud.

## PROTÉGER LES FILIALES CONTRE LES MENACES EXTERNES PAR UN SD-WAN AVANCÉ

Avec la numérisation des entreprises, les risques de cyberattaque ont significativement augmenté au cours de la décennie passée. Dans les environnements de réseau basés sur un routeur traditionnels, les filiales accumulent une diversité d'équipements de réseau et de sécurité, mais ceux-ci sont difficiles à configurer, à gérer et à maintenir à jour en fonction des dernières informations concernant les menaces. Les sites distants manquent également de personnel informatique expérimenté, ce qui les expose à des failles de sécurité potentielles.

En plus de protéger les opérations cloud par une architecture SASE de premier ordre, une solution SD-WAN avancée peut protéger les filiales contre les menaces malveillantes. Cette solution est conçue avec un pare-feu nouvelle génération intégrant des fonctionnalités de défense contre les menaces (par exemple, la prévention et la détection d'intrusion IDS/IPS) et DDoS pour protéger les filiales contre les menaces malveillantes.

Un système IDS basé sur les signatures surveille généralement le trafic réseau pour y rechercher les tendances correspondant à une signature d'attaque spécifique. Lorsqu'une intrusion est détectée, le capteur indique les actions à effectuer (par exemple, abandonner, inspecter ou autoriser le trafic). Les systèmes de prévention des intrusions peuvent opérer en mode strict ou en mode performant. En mode strict, le trafic transite par le capteur et est ainsi immédiatement bloqué en cas d'intrusion. En mode performant, une copie du trafic est envoyée à des fins d'analyse, ce qui améliore l'efficacité sans nuire aux performances du réseau. Une intrusion est bloquée après avoir été détectée. En fonction de leurs exigences en matière de sécurité, les entreprises peuvent choisir entre le mode strict et le mode performant.

Un SD-WAN avancé peut également détecter de manière dynamique des attaques DDoS telles que des attaques de protocole, des inondations ICMP, des inondations SYN et des attaques par usurpation d'adresse IP. Après avoir détecté un comportement anormal du réseau, la solution limite le nombre de requêtes à l'aide d'actions telles que le vieillissement rapide, les excès d'abandon et le blocage de source. En outre, elle peut acheminer le trafic via des liens non affectés en cas d'attaque DDoS pour assurer la continuité de l'activité.

En intégrant des fonctionnalités de réseau et de sécurité avancées en une solution SD-WAN unique telle que le routage, l'optimisation du réseau WAN et le pare-feu nouvelle génération, les entreprises peuvent simplifier considérablement les opérations de réseau dans leurs filiales. De plus, les politiques de sécurité peuvent être automatiquement transmises vers les filiales à partir d'un emplacement central avec un provisionnement sans intervention, ce qui facilite la configuration des politiques de réseau et de sécurité. Les nouvelles filiales sont mises en place rapidement et facilement et les changements apportés à la politique de sécurité peuvent être automatiquement appliqués à des centaines ou à des milliers de filiales en quelques minutes tout en limitant les erreurs.

## LA TRANSFORMATION DU WAN EST ESSENTIELLE À LA RÉUSSITE DE LA TRANSFORMATION NUMÉRIQUE

Outre tous les avantages liés à la migration d'une architecture de sécurité fournie via le cloud moderne, la transformation du WAN pour les entreprises axées sur le cloud actuelles présente une valeur incroyable. Les réseaux WAN centrés sur un routeur traditionnels n'ont jamais été conçus pour le cloud. Les entreprises doivent moderniser leur architecture WAN et repenser la manière de concevoir au mieux les réseaux de leurs filiales afin d'améliorer les performances et la sécurité des applications cloud. Elles font davantage appel au cloud et au SaaS dans le but d'offrir aux utilisateurs une expérience optimale.

La transformation du WAN implique d'offrir un parcours plus efficace et une meilleure expérience entre les utilisateurs et le cloud. Comme décrit précédemment, adopter un breakout Internet adaptatif vers des applications SaaS et hébergées dans le cloud directement à partir des emplacements des filiales optimise la bande passante disponible, mais en plus réduit la latence susceptible d'affecter la productivité des utilisateurs.

De nombreuses entreprises transforment leur périphérie réseau et adoptent le SD-WAN pour connecter les emplacements de leurs filiales via des connexions Internet haut débit. Le SD-WAN permet de sélectionner intelligemment parmi plusieurs liens WAN (MPLS, Internet haut débit, LTE, etc.) les chemins d'accès selon les applications en fonction de politiques définies de manière centrale. Les avantages liés au SD-WAN comprennent les suivants :

- Distribution économique d'applications d'entreprise
- Amélioration des performances des applications, de la disponibilité et de la qualité de l'expérience de l'utilisateur final
- Satisfaction des exigences des sites ou des emplacements distants/de filiales modernes
- Prise en charge des applications et des services SaaS et basés sur le cloud
- Amélioration de l'efficacité informatique des filiales via le provisionnement automatique des services

## RESPECTER LES ACCORDS DE NIVEAU DE SERVICE DES APPLICATIONS

Cela se traduit directement par une amélioration de la productivité et de l'agilité des entreprises. Les entreprises ont besoin d'un réseau haute performance conçu sur une base hautement disponible et capable de prendre en charge des applications critiques de manière fiable. La sécurité ne doit jamais être abordée après coup. La capacité de prendre en charge les fonctionnalités de micro-segmentation et l'application granulaire des politiques permet aux entreprises de sécuriser leur réseau WAN, de se conformer aux exigences de conformité et de se protéger contre les atteintes à la sécurité.

Les entreprises doivent pouvoir déployer de nouvelles filiales en toute flexibilité et ajuster de manière dynamique les règles de politique et de sécurité. La capacité de propager le contexte des politiques est une exigence essentielle à l'automatisation des filiales. Cela rend le concept d'une solution SD-WAN avancée particulièrement intéressant et peut aider les entreprises à éliminer le besoin de disposer de plusieurs appliances exécutant des fonctions de sécurité dédiées, ce qui à son tour peut les aider à simplifier et à consolider — ou « amincir » — l'architecture de périphérie WAN de leurs filiales. Une plateforme de périphérie SD-WAN avancée permet aux entreprises de transformer leur WAN en unifiant le SD-WAN, le routage, l'optimisation du WAN, la segmentation et la sécurité des filiales en une seule plateforme gérée de manière centrale.

Grâce à une orchestration centralisée du WAN et à une approche spécifique aux applications, les priorités de l'entreprise sont toujours reflétées dans le comportement du réseau. Unifier l'orchestration du réseau et les politiques de sécurité garantit que la qualité de service et la sécurité sont appliquées et mises en œuvre de manière cohérente au niveau des applications (ou des catégories d'applications), indépendamment de la manière dont on y accède et de l'endroit où l'on y accède. Les performances et la sécurité des applications peuvent être dictées par des politiques descendantes de l'entreprise, et non par des contraintes technologiques ascendantes. Un SD-WAN avancé surveille en permanence l'état du réseau et des applications, détecte les conditions changeantes et déclenche des réponses automatisées immédiates et en temps réel pour éliminer l'impact des restrictions, des interruptions et des événements de menace pour la sécurité. De plus, automatiser la connectivité des plateformes cloud avec des intégrations via des API (Application Programmable Interface) simplifie les opérations informatiques, ce qui permet aux entreprises d'accéder rapidement aux services de sécurité fournis via le cloud, aux infrastructures IaaS et aux logiciels SaaS. Les réseaux modernes doivent pouvoir être visibles, programmés et automatisés de bout en bout pour assurer de manière dynamique les performances, la sécurité et la qualité d'expérience optimale nécessaires aux environnements multicloud. Un WAN intelligent conçu avec un SD-WAN de premier ordre et des solutions de sécurité fournies via le cloud fait avancer les initiatives de transformation numérique et permet aux entreprises d'évoluer et d'adopter les innovations pertinentes sans restreindre leur productivité et leur croissance, tout cela en minimisant leur exposition aux risques de sécurité.

## CONCLUSION

Alors que les entreprises axées sur le cloud modernes continuent à migrer leurs applications du datacenter vers le cloud, elles doivent adopter la transformation du WAN et de la sécurité afin de réaliser un retour optimal sur leurs investissements dans le cloud. Le SASE (Secure Access Service Edge) oriente l'industrie dans cette nouvelle direction. Comme l'illustre la figure 5, il est important que les entreprises s'intéressent à la transformation du WAN et de la sécurité au moment de concevoir une périphérie de services d'accès sécurisé afin d'offrir une expérience harmonieuse.

Une plateforme SD-WAN avancée permet de se connecter de manière transparente à une variété de services de sécurité cloud d'avant-garde et offre ainsi une architecture SASE de premier ordre. En définitive, aucun fournisseur SASE ne sera capable de fournir seul des technologies de réseau et de sécurité de premier ordre sur une plateforme unique. Le paysage des menaces ne cessant d'évoluer, les entreprises doivent rester agiles pour adopter de nouvelles solutions de sécurité de manière rapide et rentable. Les entreprises sont bien équipées pour évaluer des plateformes offrant la liberté de choix dans l'intégration de solutions SASE de premier ordre. Elles évitent ainsi d'être enfermées dans des solutions à fournisseur unique ou de devoir se contenter de fonctionnalités et de capacités de base.

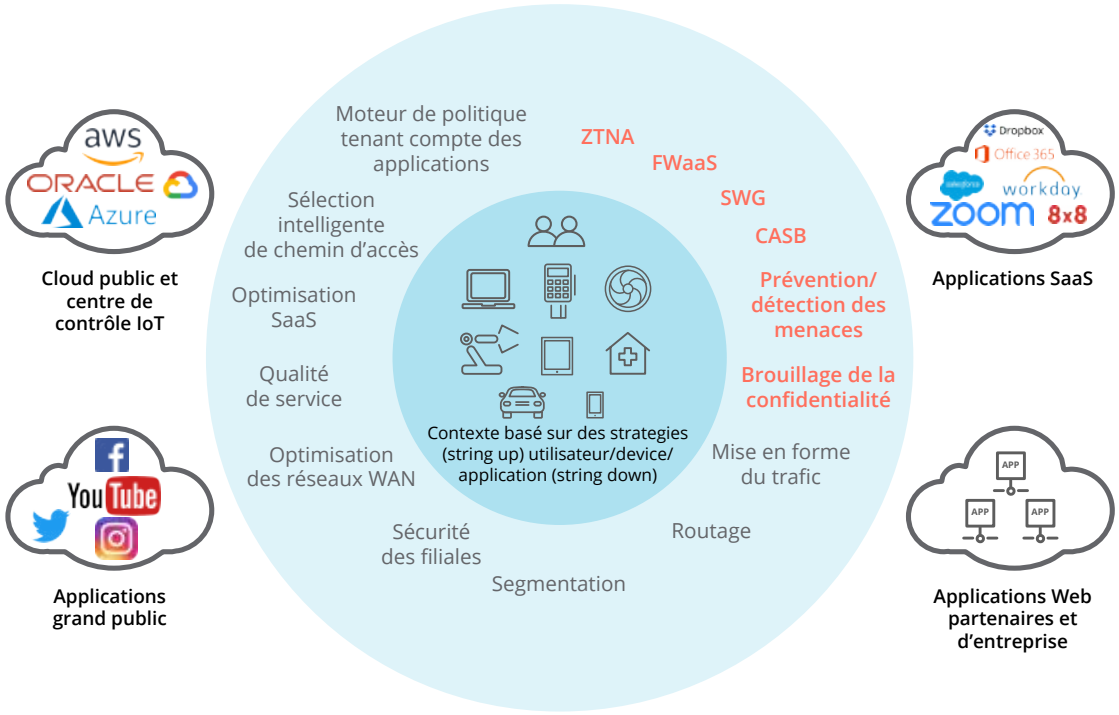


Figure 5 : Une périphérie de services d'accès sécurisé est nécessaire pour soutenir les initiatives de transformation numérique des entreprises, à savoir les besoins liés à la mobilité des équipes et à la stratégie de priorité au cloud. Dans une architecture SASE robuste, des fonctionnalités WAN complètes doivent aller de pair avec des fonctions de sécurité du réseau complètes pour répondre aux besoins d'accès dynamique et sécurisé des utilisateurs, des devices et des applications au sein des entreprises numériques.

De plus, avec la prolifération des devices IoT, le SASE doit être complété d'un cadre de sécurité zéro confiance qui segmente de manière dynamique le trafic en fonction de l'identité, de sorte que les utilisateurs et les devices IoT ne puissent atteindre que les parties du réseau correspondant à leur rôle dans l'entreprise.

Un SD-WAN avancé peut soutenir les fonctions de sécurité fondamentales nécessaires dans la filiale en intégrant un pare-feu nouvelle génération avec des fonctionnalités IDS/IPS, et peut compléter la sécurité assurée via le cloud pour mettre en œuvre de manière transparente les politiques de sécurité dans toute l'entreprise. Les entreprises peuvent ainsi simplifier leur infrastructure réseau en ayant l'opportunité d'adopter à leur propre rythme une architecture WAN moderne, sécurisée et axée sur le cloud, sans compromis.

Enfin, pour les entreprises qui ne sont pas nécessairement prêtes à se débarrasser des pare-feu de filiale et à passer entièrement à un modèle de sécurité fourni via le cloud, il est important de trouver une plateforme SD-WAN avancée offrant la liberté de choix pour soutenir des solutions logicielles UTM (Unified Threat Management) tierces leaders qui s'exécutent aux emplacements des filiales comme une solution intégrée. Cela élimine le coût supplémentaire et la complexité de gestion qui accompagneraient normalement des pare-feu dédiés distincts, mais offre également aux entreprises la flexibilité permettant de déployer des solutions de premier ordre, pour finalement opérer une migration sans heurts vers un modèle de sécurité fourni via le cloud.

Alors que les entreprises poursuivent leurs investissements substantiels dans le cloud, examiner les exigences d'une transformation du WAN et de la sécurité les mènera en définitive à offrir la meilleure qualité d'expérience aux utilisateurs, tout en relevant les défis actuels liés à la cybersécurité. Entamer un parcours sans compromis et bien pensé dans la transformation du WAN et de la sécurité permettra finalement aux entreprises de protéger leurs ressources numériques et d'obtenir un effet multiplicateur à partir de leurs investissements continus dans le cloud.

aruba
a Hewlett Packard Enterprise company



BP_Successful-WAN-and-Security-Transformation_RVK_080422 a00110932fre

Contactez-nous à l'adresse www.arubanetworks.com/contact