LIVRE BLANC

aruba
a Hewlett Packard Enterprise company

UNE TRANSFORMATION RÉUSSIE DES WAN ET DE LA SÉCURITÉ EST INDISPENSABLE À L'ENTREPRISE NUMÉRIQUE

TABLE DES MATIÈRES

SOMMAIRE

Les entreprises continuent d'adopter la transformation numérique afin d'accroître leur efficacité, d'améliorer la satisfaction des clients, de saisir de nouvelles opportunités de marché, de renforcer leur rentabilité et de conserver un avantage concurrentiel. La migration des applications d'entreprise vers le cloud fait partie intégrante de toute initiative de transformation numérique réussie. Pourquoi ? Aujourd'hui, plus d'applications fonctionnent dans le cloud que dans les datacenters traditionnels des entreprises, et la majorité de ces applications sont exploitées comme logiciel as a service (SaaS). De plus, dans le monde du cloud-first, les entreprises doivent s'assurer que les applications sont accessibles directement et en toute sécurité à tout moment, de tout endroit et sur tout appareil. Elles veulent également s'assurer que le réseau offre en permanence une expérience de la plus haute qualité possible aux employés et aux clients. Enfin, l'explosion des appareils mobiles et IoT dans l'entreprise a considérablement augmenté la surface d'attaque, exposant les entreprises à des failles de sécurité qui peuvent compromettre les données et entraîner une interruption du réseau.

Les réseaux d'entreprise d'aujourd'hui n'ont jamais été conçus pour le monde cloud-first, et sont loin d'offrir l'agilité et la sécurité nécessaires pour répondre aux exigences de la transformation numérique. Il est essentiel que les entreprises sécurisent non seulement les applications dans le cloud, mais aussi les utilisateurs qui se connectent à ces applications via le réseau étendu (WAN). Dans le même temps, l'environnement commercial concurrentiel d'aujourd'hui exige des entreprises qu'elles offrent une expérience de la plus haute qualité à leurs clients. Elles ont besoin d'un réseau qui maintient les performances et la disponibilité nécessaires à la poursuite de leurs activités.

Pour que la transformation numérique tienne toutes ses promesses, les entreprises devront transformer à la fois leurs architectures WAN et de sécurité, et pas seulement l'une ou l'autre. Les entreprises ont déjà réalisé d'importants investissements dans le cadre de leur passage au cloud. Le grand défi est donc de savoir comment tirer un effet multiplicateur de leurs investissements dans le cloud. La réponse consiste à moderniser leurs architectures WAN et de sécurité. Par conséquent, il est stratégiquement impératif d'adopter un réseau étendu défini par logiciel (SD-WAN) plus intelligent et hautement automatisé, pouvant être intégré en toute fluidité aux services de sécurité cloud.

La transformation du WAN et de la sécurité étant tout un cheminement, une entreprise peut commencer par les moderniser ; cependant, pour tirer le meilleur parti de ses investissements dans le cloud, elle doit aborder les deux aspects. Il est par ailleurs tout aussi important d'éviter le verrouillage des fournisseurs en choisissant des partenaires de solutions technologiques qui offrent flexibilité et liberté de choix. Grâce à des architectures de réseau et de sécurité transformées, les entreprises peuvent adopter des innovations opportunes pour accélérer la productivité, la croissance des revenus et la rentabilité tout en maîtrisant les coûts.

Pour que la transformation cloud et numérique tienne toutes ses promesses, les entreprises devront transformer à la fois leurs architectures WAN et de sécurité, et pas seulement l'une ou l'autre. Les entreprises ont déjà réalisé d'importants investissements dans le cadre de leur passage au cloud ; le grand défi est donc de savoir comment tirer un effet multiplicateur de leurs investissements dans le cloud.

LES APPLICATIONS SONT FOURNIES DANS LE CLOUD — LA SÉCURITÉ DOIT L'ÊTRE AUSSI

Traditionnellement, tout le trafic d'applications provenant des sites des succursales était réacheminé sur des services MPLS privés vers le datacenter de l'entreprise pour inspection et vérification de la sécurité (voir Figure 1). Cette architecture était justifiée lorsque les applications étaient hébergées exclusivement dans le datacenter de l'entreprise. Cependant, avec la migration des applications et des services vers le cloud, cette architecture réseau traditionnelle n'est pas à la hauteur, principalement parce qu'elle nuit aux performances des applications et offre une expérience utilisateur inégale dans la mesure où le trafic destiné à Internet passe d'abord par le datacenter et le pare-feu de l'entreprise avant d'atteindre sa destination.

En outre, le nombre croissant d'employés travaillant hors du réseau de l'entreprise et se connectant directement aux applications cloud rend la sécurité périmétrique traditionnelle insuffisante. Le cloud et le SaaS ont changé à jamais la façon dont les utilisateurs se connectent et interagissent avec les applications. 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 multiclouds, quels que soient le lieu ou les appareils utilisés pour y accéder.

Une solution de sécurité cloud prend en charge plusieurs fonctions de sécurité réseau qui peuvent inclure une passerelle Web sécurisée (SWG), un pare-feu en tant que service (FWaaS), un agent de sécurité des accès au cloud (CASB) et une architecture de réseau Zero Trust (ZTNA). Ces fonctions étaient auparavant uniques et dédiées sur site. Désormais, elles peuvent être fournies à partir du cloud de manière unifiée, comme le montre la figure 2.

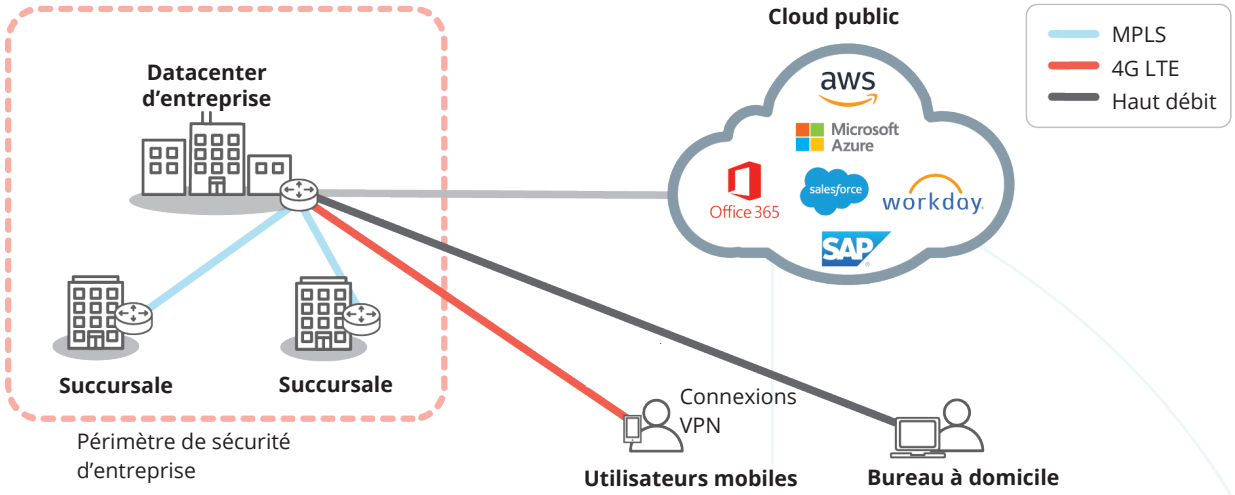

Figure 1 : Les WAN d'entreprise traditionnels et les approches de sécurité périmétriques n'ont pas été conçus pour le cloud. Le renvoi de tout le trafic applicatif des sites de succursales vers le datacenter nuit aux performances et offre une expérience utilisateur inégale.

Certains premiers utilisateurs de solutions de sécurité cloud n'ont pas réussi à mettre en œuvre un SD-WAN capable d'appliquer l'Adaptive Internet Breakout directement à partir des sites des succursales. Ils ne pouvaient donc pas diriger le trafic directement du site d'une succursale vers le cloud. Sans le composant SD-WAN, le trafic destiné au cloud était toujours renvoyé vers le datacenter, entraînant un impact négatif sur les performances des applications.

L'adoption d'une solution de sécurité cloud et d'un réseau SD-WAN élimine le coût et la complexité associés à la gestion de plusieurs pare-feu de nouvelle génération sur site, mais nécessite toujours une fonctionnalité de pare-feu dynamique basé sur une zone sur les sites des succursales pour bloquer toute menace entrante. Comme le montre la figure 3, une solution SD-WAN avancée permet aux entreprises de se connecter directement au cloud via l'Adaptive Internet Breakout en utilisant des connexions Internet haut débit. L'intelligence nécessaire pour reconnaître les applications sur liste blanche permet un routage local depuis la succursale jusqu'au point de présence (PoP) le plus proche, éliminant ainsi la latence et offrant la meilleure qualité d'expérience pour les applications SaaS et cloud de confiance telles que Microsoft Office 365, 8x8 et RingCentral. La connaissance des applications permet également d'envoyer d'autres trafics liés à Internet à un fournisseur de sécurité cloud pour une inspection avancée avant de les transmettre à un fournisseur SaaS. Les capacités SD-WAN avancées intégrées aux services de sécurité cloud modernes garantissent une application cohérente des politiques et un contrôle d'accès pour les utilisateurs, les appareils, les applications et l'IoT. Cela permet aux entreprises de faire respecter la conformité, d'éviter les temps d'arrêt et d'atténuer le risque de compromission des données associé à une faille de sécurité.

SÉCURISER L'IOT DES ENTREPRISES AVEC LE SD-WAN

La prolifération des appareils IoT dans les entreprises apporte de nouvelles façons de surveiller, de signaler, d'alerter, d'automatiser et d'optimiser les processus métier,

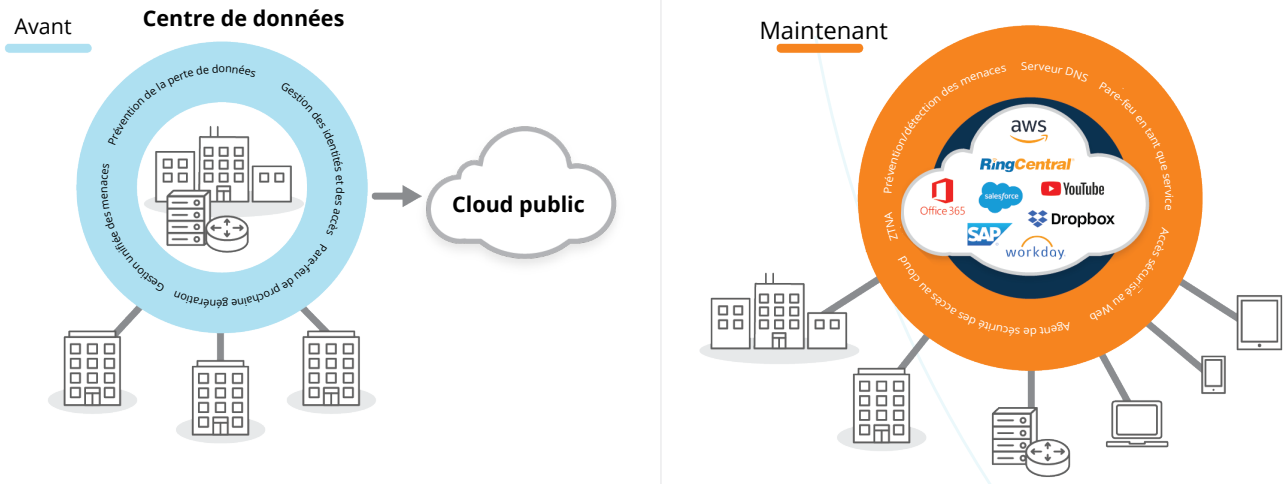

Figure 2 : Dans le passé, il fallait avant tout sécuriser le datacenter de l'entreprise où les applications étaient hébergées de manière exclusive. Maintenant que les applications ont été déplacées vers le cloud et sont fournies à partir de celui-ci, la sécurité périmétrique des entreprises est de moins en moins efficace. Il est impératif de penser différemment et de transférer la sécurité vers le cloud.

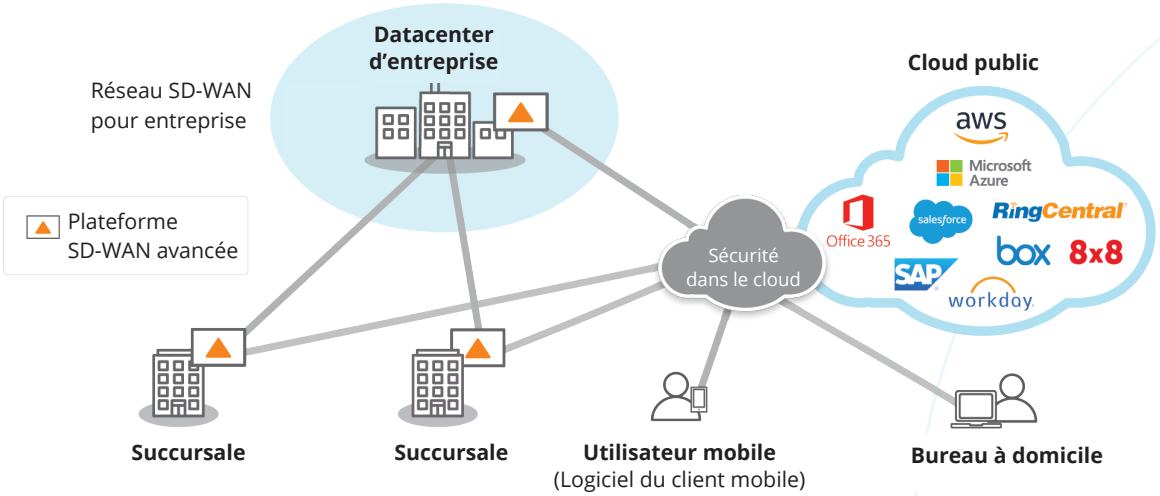

Figure 3 : Un réseau SD-WAN avancé offre aux entreprises une bretelle d'accès sécurisée au cloud. Les sites des succursales peuvent utiliser des connexions haut débit et l'Adaptive Internet Breakout pour connecter directement les utilisateurs aux applications cloud, optimisant ainsi les performances des applications et l'expérience utilisateur. La combinaison d'un réseau SD-WAN avancé et d'une sécurité cloud par le biais d'une approche de réseau Zero Trust (ZTNA) s'appuyant sur des politiques garantit une sécurisation permanente du WAN, des utilisateurs, des appareils et des applications.

des chaînes de fabrication à l'automatisation du système de CVC et de l'éclairage pour réaliser des économies d'énergie. Si l'IoT rend les entreprises plus efficaces grâce à l'automatisation, il augmente également la surface d'attaque en ajoutant une nouvelle dimension de complexité. Pour relever le défi croissant de la sécurité des appareils mobiles, les services informatiques déploient une solution d'accès réseau Zero Trust (ZTNA) basée sur le modèle de confiance zéro. Une solution ZTNA consiste à installer un agent sur un appareil utilisateur tel qu'un ordinateur portable, une tablette ou un téléphone mobile. Cet agent logiciel garantit que le trafic provenant de l'appareil est dirigé vers un service de sécurité cloud avant d'être dirigé vers une application SaaS ou un fournisseur IaaS. Cependant, contrairement aux tablettes et aux smartphones, les agents logiciels ZTNA ne peuvent pas être installés sur les appareils IoT. Dans la mesure où ils sont sans agent, ils ne permettent pas l'installation d'agents logiciels tiers. Pour cette raison, les entreprises ont besoin d'une solution de sécurité différente pour les appareils IoT afin de protéger les réseaux d'entreprise contre les vulnérabilités potentielles qui pourraient ouvrir une brèche dans le réseau et perturber les activités quotidiennes.

Une plateforme SD-WAN avancée et adaptée aux applications permet aux entreprises de réduire les risques liés aux failles lors du déploiement d'appareils IoT. Une plateforme SD-WAN avancée identifie et classe le trafic applicatif du premier paquet, l'intercepte à la périphérie du réseau pour l'orienter vers un segment approprié et le protège des autres trafics du réseau. Une plateforme SD-WAN avancée orchestre une segmentation de bout en bout couvrant le LAN-WAN-LAN et le LAN-WAN-Datacenter/Cloud de l'entreprise, ce qui permet une application cohérente et automatisée des politiques de sécurité avec une meilleure visibilité. La segmentation de bout en bout permet aux entreprises de créer des segments isolés pour le trafic des appareils IoT. Une politique de sécurité indépendante peut être établie pour chaque segment, définissant les politiques de sécurité à appliquer au trafic de l'appareil. Le trafic d'un segment étant isolé du trafic de tous les autres segments, cela empêche tout accès non autorisé. Même lorsqu'une menace survient, son impact est limité au segment dans lequel elle est apparue. En outre, grâce à un pare-feu dynamique unifié basé sur une zone, les entreprises peuvent sécuriser les sites distants et les appareils IoT contre toute menace potentielle entrante inquiétante en les bloquant.

Prenons un exemple. Dans un site distant où sont installés des appareils IoT sans agent, tels que des systèmes de points de vente et de CVC (Figure 4 ci-dessous), une plateforme SD-WAN avancée identifie de manière unique les applications utilisées par ces appareils. Une politique de système intercepte le trafic des points de vente et le dirige vers le datacenter de l'entreprise où est hébergée l'application de traitement des transactions par carte de crédit. Dans cet exemple, les services de sécurité existants du pare-feu de nouvelle génération déployés dans le datacenter sont appliqués. D'autre part, les politiques des systèmes de CVC segmentent et dirigent le trafic CVC vers le service de sécurité cloud pour une inspection de sécurité supplémentaire avant d'atteindre le centre de contrôle IoT hébergé dans le cloud public. Le trafic IoT étant isolé selon la politique de l'entreprise, une faille dans le segment des CVC ne compromet pas ou ne met pas en danger les cartes de crédit et les données personnelles dans le segment des points de vente. La segmentation aide également les organisations à satisfaire aux exigences de conformité PCI (ou autres) pour leur activité. Comme le montre cet exemple, un déploiement de sécurité complet avec plateforme SD-WAN avancée peut mieux protéger les entreprises dynamiques d'aujourd'hui dans leur parcours de transformation à mesure qu'elles adoptent les avantages de l'IoT.

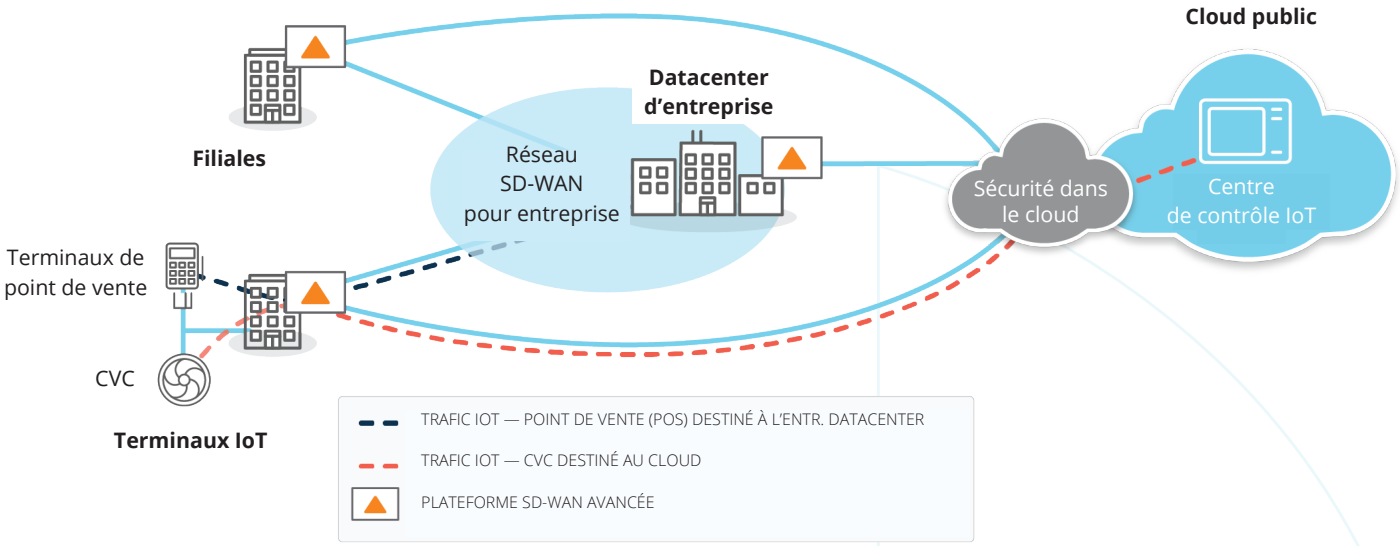

Figure 4 : Les terminaux IoT se multiplient et présentent de nouveaux risques de failles de sécurité. En utilisant une plateforme SD-WAN avancée, les entreprises peuvent protéger les appareils IoT derrière le pare-feu dynamique unifié basé sur zone, en identifiant dynamiquement le trafic des appareils IoT, en appliquant des politiques individuelles et en segmentant le réseau de manière granulaire pour répondre aux exigences de conformité. Un SD-WAN avancé garantit l'interception du trafic IoT à la périphérie du réseau et son envoi vers la bonne destination, y compris le cloud, sans aucun compromis ni risque d'exposition de l'entreprise. Comme le montre le schéma, toutes les données de transaction en point de vente de la succursale sont destinées au datacenter de l'entreprise, tandis que le trafic CVC est acheminé vers un centre de contrôle IoT dans le cloud.

LES SOLUTIONS LES PLUS PERFORMANTES FAVORISENT L'AGILITÉ DES ENTREPRISES

Compte tenu de l'évolution constante des approches en matière de sécurité des réseaux et de la difficulté de la mise en place de solutions réseau complexes, il est important d'évaluer les solutions de sécurité et de réseau les plus performantes auprès de fournisseurs ayant fait leurs preuves. Trouver un fournisseur unique capable de fournir des capacités de premier ordre dans les deux domaines est irréaliste, et les entreprises ne devraient pas avoir à faire de compromis sur des capacités de base d'un côté ou de l'autre.

Avec l'évolution constante du paysage des menaces faisant de la sécurité une préoccupation majeure, les entreprises doivent conserver l'agilité nécessaire pour adopter rapidement et de manière rentable de nouvelles solutions de sécurité sans être limitées à la solution d'un seul fournisseur. Avec une solution réseau indépendante, les entreprises ont l'assurance et la tranquillité d'esprit nécessaires pour sélectionner et déployer les solutions de sécurité cloud correspondant le mieux à l'évolution de leurs activités et de leurs exigences en matière de sécurité.

En ayant la liberté de choisir les solutions des fournisseurs les plus performants qui unifient le SD-WAN et la sécurité cloud grâce à l'automatisation, les entreprises gagnent en agilité et en rapidité ; de plus, elles réduisent la complexité et les coûts en mettant en place une architecture de sécurité cohérente qui bloque l'impact des cyberattaques. À terme, cela permet aux entreprises d'obtenir un effet multiplicateur sur leurs investissements existants et en cours dans les applications et services cloud.

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

Outre tous les avantages de la migration vers une architecture de sécurité cloud moderne, la transformation du WAN pour les entreprises de type « cloud-first » d'aujourd'hui présente un intérêt considérable. Les WAN traditionnels centrés sur les routeurs n'ont jamais été conçus pour le cloud. Les entreprises doivent moderniser leur architecture WAN et repenser la meilleure façon de concevoir leurs réseaux de succursales pour améliorer les performances et la sécurité des applications cloud. Les entreprises ont de plus en plus recours au cloud et au SaaS, en s'attachant à offrir une qualité d'expérience optimale aux utilisateurs.

La transformation du WAN consiste à fournir un chemin plus efficace et une meilleure expérience entre les utilisateurs et le cloud. Comme décrit précédemment, l'adoption de l'Adaptive Internet Breakout pour accéder aux applications hébergées dans le cloud et SaaS directement depuis les sites des succursales permet non seulement d'optimiser la bande passante disponible, mais aussi de réduire toute latence susceptible d'avoir un impact négatif sur la productivité des utilisateurs.

De nombreuses organisations transforment la périphérie de leur réseau et adoptent le SD-WAN pour connecter les sites des succursales à l'aide de connexions Internet haut débit. Le SD-WAN offre une sélection intelligente de chemins d'accès pilotée par les applications sur plusieurs liaisons WAN (MPLS, Internet à haut débit, LTE, etc.) en fonction de politiques définies de manière centralisée. Les avantages du SD-WAN sont les suivants :

- Fourniture rentable d'applications d'entreprise
- Amélioration des performances des applications, de la disponibilité et de la qualité de l'expérience des utilisateurs finaux
- Satisfaction des exigences de la succursale moderne/des sites ou emplacements éloignés
- Prise en charge des applications et services SaaS basés dans le cloud
- Amélioration de l'efficacité de l'informatique des succursales grâce au provisionnement automatisé des services

RÉPONDRE AUX EXIGENCES DES SLA DES APPLICATIONS

Il en découle directement une plus grande productivité de l'entreprise et une plus grande agilité opérationnelle. Les entreprises ont besoin d'un réseau haute performance, reposant sur une base hautement disponible et capable de prendre en charge les applications critiques de manière fiable. La sécurité ne doit jamais être envisagée après coup. La prise en charge des capacités de microsegmentation et l'application granulaire des politiques permettent aux entreprises de sécuriser leur WAN, de satisfaire aux exigences de conformité et de se défendre contre les violations.

Les entreprises ont besoin de l'agilité nécessaire pour créer de nouvelles succursales et ajuster les règles de politique et de sécurité de manière dynamique. La capacité à propager le contexte de politique est une condition essentielle à l'automatisation des succursales. Cela rend très attrayant le concept d'une solution SD-WAN avancée et peut aider les entreprises à éliminer la nécessité de plusieurs appareils exécutant des fonctions de sécurité dédiées et, par conséquent, à simplifier et à consolider ou à « alléger » l'architecture WAN de périphérie de leurs succursales. 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 succursales dans une seule plateforme à gestion centralisée.

L'orchestration centralisée du SD-WAN et une approche spécifique aux applications garantissent la prise en compte permanente des priorités de l'entreprise dans le comportement du réseau. L'unification de l'orchestration des politiques de réseau et de sécurité garantit l'application cohérente de la qualité de service et de la sécurité aux applications, ou aux catégories d'applications, indépendamment de leur mode et de leur lieu d'accès. Les performances et la sécurité des applications peuvent être dictées par des politiques d'entreprise descendantes, 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 immédiates et automatisées en temps réel afin d'éliminer l'impact des coupures, des pannes et des événements menaçant la sécurité. En outre, l'automatisation de la connectivité des plateformes cloud avec des intégrations via des interfaces de programmation d'applications (API) simplifie les opérations informatiques et permet aux entreprises d'accéder en temps voulu aux services de sécurité cloud, IaaS et SaaS.

Le réseau d'aujourd'hui nécessite une visibilité, une programmabilité et une automatisation de bout en bout pour garantir de manière dynamique les performances, la sécurité et la plus haute qualité d'expérience requises pour les environnements multi-cloud. Un WAN intelligent conçu avec des solutions de sécurité SD-WAN et cloud de premier ordre fait avancer les initiatives de transformation numérique et permet aux entreprises d'évoluer et d'adopter des innovations opportunes sans limiter leur productivité et leur croissance, tout en minimisant l'exposition aux risques de sécurité.

CONCLUSION

À mesure que les entreprises modernes de type « cloud-first » continuent de migrer leurs applications depuis le datacenter vers le cloud, elles doivent adopter la transformation du WAN et de la sécurité pour tirer le meilleur parti de leurs investissements dans le cloud. Gartner a inventé le terme SASE, ou Secure Access Service Edge (service d'accès sécurisé Edge), qui fait évoluer le secteur dans cette nouvelle direction. Comme le montre la figure 5, il est important que les entreprises tiennent compte à la fois de la transformation du WAN et de la sécurité lorsqu'elles conçoivent un service d'accès sécurisé Edge pour créer une expérience fluide.

En fin de compte, aucun fournisseur n'aura la capacité de fournir des technologies de réseau et de sécurité de premier ordre sur une seule et même plateforme. Face à l'évolution constante du paysage des menaces, les entreprises doivent conserver l'agilité nécessaire pour adopter rapidement et de manière rentable de nouvelles solutions de sécurité. Les entreprises ont tout intérêt à évaluer les plateformes qui offrent la liberté de choix pour intégrer des solutions de réseau et de sécurité de premier ordre.
Ce faisant, elles peuvent éviter d'être enfermées dans des solutions propriétaires à fournisseur unique ou de devoir se contenter de fonctionnalités et de capacités de base.

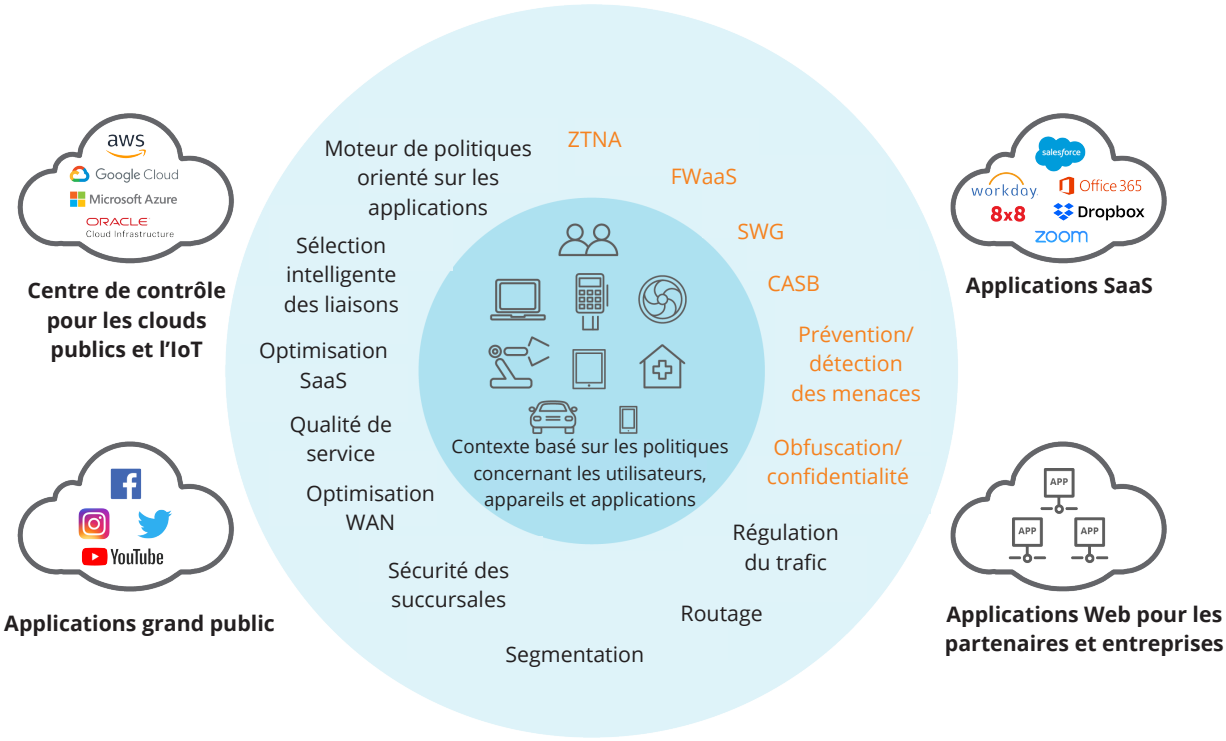

Figure 5 : des capacités Secure Access Service Edge (SASE) sont nécessaires pour soutenir les initiatives de transformation numérique des entreprises, comme les stratégies orientées cloud et les efforts liés à la mobilité du personnel. Dans une architecture SASE robuste, les capacités WAN exhaustives doivent fonctionner de concert avec les fonctions globales de sécurité réseau afin de répondre aux besoins d'accès dynamique et sécurisé des entreprises numériques pour les utilisateurs, les appareils et les applications.

Une plateforme SD-WAN avancée prenant en charge des interfaces de programmation d'applications (API) intégrées peut apporter de nouveaux niveaux d'automatisation aux entreprises, offrant ainsi la possibilité de se connecter à divers services cloud de premier ordre, y compris pour les services de sécurité. Elle peut prendre en charge les fonctions de sécurité de base requises dans les succursales et compléter la sécurité cloud afin d'assurer une application fluide des politiques de sécurité de bout en bout dans toute l'entreprise. Les entreprises qui ne sont pas encore prêtes à transformer complètement leurs architectures WAN et de sécurité ont ainsi la possibilité de passer à leur rythme et sans compromis à une architecture WAN moderne de type « cloud-first ».

Enfin, pour les entreprises qui ne sont pas encore prêtes à retirer les pare-feu de leurs succursales et à passer complètement à un modèle de sécurité cloud, il est important de trouver une plateforme SD-WAN avancée qui offre la liberté de choix par la prise en charge des principales solutions logicielles tierces de gestion unifiée des menaces (UTM) fonctionnant comme une solution intégrée sur les sites des succursales. Cela permet d'éliminer les coûts supplémentaires et la complexité de gestion qui résulteraient normalement de l'utilisation de pare-feu dédiés distincts, mais aussi de donner aux entreprises la possibilité de déployer des solutions de premier ordre, pour finalement offrir une migration en douceur vers un modèle de sécurité cloud.

À l'heure où les entreprises continuent d'investir massivement dans le cloud, la prise en compte des exigences liées à la transformation du WAN et de la sécurité leur permettra d'offrir aux utilisateurs une expérience de la plus haute qualité, d'accroître la productivité et de générer de nouvelles sources de revenus. En s'engageant dans une transformation réfléchie et sans compromis du WAN et de la sécurité, les entreprises obtiendront à terme un effet multiplicateur de leurs investissements existants et en cours dans le cloud.

aruba
a Hewlett Packard Enterprise company

WP_Successful-WAN-and-Security-Transformation_EM_021621 a00110932enw