aruba
a Hewlett Packard Enterprise company

EBOOK

Sécurité Edge-to-cloud : Un nouveau réseau étendu (WAN) et une nouvelle sécurité

Guide pratique pour l'adoption d'une architecture SASE (service d'accès sécurisé Edge)

La transformation numérique et le WFA (Work From Anywhere ou Travail depuis n'importe quel endroit) ont un impact considérable sur le WAN et la sécurité dans un monde « cloud first ».

Tandis que les organisations s'emploient à résoudre les problèmes que posent la pandémie du COVID-19 et la nouvelle normalité que représente le WFA, l'adoption des services hébergés dans le cloud continue de battre son plein. Cette tendance intensifie la nécessité de transformer de toute urgence le datacenter traditionnel et les réseaux de type MPLS et VPN en service SASE cloud-native offrant un provisionnement plus dynamique de services réseau sécurisés et protégeant les données de bout en bout sur le WAN.

S'agissant de la sécurisation du WAN, les 3 défis les plus importants que les responsables informatiques sont appelés à relever sont :

- Comment sélectionner la bonne architecture SD-WAN pour prendre en charge les applications d'entreprise en toute sécurité dans un environnement cloud-first ?
- Comment l'environnement WFA hybride permanent affectera-t-il les décisions du service informatique concernant l'adaptation d'une architecture de sécurité dans une plateforme SASE ?
- Comment le service IT peut-il gérer les problèmes de sécurité associés à la prolifération des appareils IoT pour la plupart sans agent ?

Voyons comment les exigences en matière de réseau et de sécurité sont en train de changer dans un monde cloud-first.

50 %
des personnes interrogées en 2021 ont affirmé qu'elles sont en train de mettre en œuvre et d'exécuter des initiatives de transformation numérique, comparé à 38 % en 2020[1]

45 %
des entreprises ont mis en place une politique cloud-first[2]

1, 2. ESG IT Technology Intentions Spending Survey, décembre 2020 (en anglais)

Zero Trust, ZTNA et SASE dans un monde cloud-first

Les solutions de sécurité traditionnelles n'ont pas été conçues avec le cloud à l'esprit. Le transport du trafic vers un datacenter centralisé était une bonne idée lorsque toutes les applications y résidaient. Toutefois, en raison de l'augmentation du trafic des utilisateurs dans les succursales et des applications qui passent au cloud, le backhaul du trafic sur un réseau en étoile traditionnel fournit une expérience utilisateur médiocre, augmente les risques de sécurité et coûte cher.

Les solutions de sécurité réseau existantes n'intègrent pas encore le concept Zero Trust, modèle de sécurité informatique pour la gestion des identités et des accès. Ce modèle ne fait confiance à aucun utilisateur ou logiciel s'il n'a pas été authentifié. En d'autres termes, il authentifie tout, puis accorde l'accès uniquement aux applications et données qui sont compatibles avec les rôles des utilisateurs ou des appareils. Dans le cadre de la sécurité Zero Trust, les utilisateurs, appareils et applications doivent prouver leur identité et ce qu'ils prétendent être. Ils sont ensuite autorisés à accéder uniquement aux ressources qui les intéressent, quel que soit leur emplacement à l'intérieur ou à l'extérieur du périmètre du réseau.

ZTNA (Zero Trust Network Access ou Accès réseau Zero Trust) est un ensemble de technologies fonctionnant sur une plateforme Zero Trust qui accorde l'accès selon les principes du moindre privilège et du « besoin de savoir » définis par des politiques granulaires. ZTNA offre aux utilisateurs un accès fluide et sécurisé aux applications privées sans jamais les placer sur le réseau ou les exposer à Internet.

Il y a enfin le service SASE, terme inventé par Gartner. SASE définit une architecture Edge combinant des capacités WAN complètes et des fonctions de sécurité réseau cloud telles que SWG (Secure Web Gateway ou passerelle Web sécurisée), CASB (Cloud Access Security Broker ou agent de sécurité des accès au cloud), FWaaS (Firewall-as-a-Service ou pare-feu en tant que service), ZTNA et bien plus encore.

Défis associés à la sécurité WAN et réseau

Dans l'environnement cloud-first d'aujourd'hui, les besoins en matière de sécurité WAN et réseau sont plus interdépendants que jamais. Pour réaliser toutes les promesses de la transformation numérique, les entreprises doivent transformer leur architecture WAN et leur architecture de sécurité et prendre en charge des applications métier accessibles depuis n'importe quel site et n'importe quel réseau de transport.

Examinons les défis les plus importants en matière de sécurité et WAN auxquels sont confrontées les équipes informatiques et les équipes réseau des entreprises :

- Comment profiter des avantages commerciaux et opérationnels du cloud tout en renforçant la sécurité et en réduisant les risques ?
- Comment garantir une expérience utilisateur cohérente et de grande qualité à toutes les applications métier hébergées dans le cloud sur le WAN ?
- Comment déployer et mettre en application des politiques d'accès réseau cohérentes pour les employés qui travaillent dans un environnement hybride (en partie au bureau ou dans les succursales) ou un environnement WFA (Travail depuis n'importe quel endroit) ?
- Comment gérer la sécurité et la connectivité WAN de tous ces appareils, utilisateurs et applications ?
- Le choix de la bonne plateforme SD-WAN peut-il améliorer l'intégration de la sécurité réseau au WAN ?
- Est-il possible d'obtenir tous les services de sécurité nécessaires auprès d'un seul fournisseur ?

Répondre aux exigences de l'intégration des politiques relatives aux applications SD-WAN et à la sécurité

Face à une économie mondiale qui évolue à un rythme effréné, les entreprises ont besoin d'agilité pour créer de nouvelles succursales et ajuster les politiques et règles de sécurité de manière dynamique. La propagation du contexte des politiques est également un élément important dans l'automatisation des succursales. Cette capacité clé ne peut être fournie que par une solution SD-WAN avancée telle que la plateforme SD-WAN Edge d'Aruba EdgeConnect.

Une solution SD-WAN avancée peut également aider les entreprises à éliminer la nécessité d'avoir recours à plusieurs appliances en unifiant les fonctionnalités WAN Edge des succursales telles que :

- SD-WAN
- Routage
- Pare-feu basé sur une zone et segmentation
- Gestion unifiée des menaces (UTM)
- Contrôle et visibilité du réseau et des applications
- Optimisation WAN

La consolidation de ces fonctionnalités simplifiera le WAN Edge des succursales. En outre, elle améliorera considérablement les opérations informatiques et la mise en application de la qualité de service (QoS) et des politiques de sécurité.

L'orchestration SD-WAN centralisée d'Aruba EdgeConnect unifie la configuration et la gestion. Elle veille également à ce que la qualité de service et la sécurité soient appliquées de manière cohérente aux applications ou classes d'applications quelle que soit la manière dont on y accède. Les performances et la sécurité des applications sont dépendantes de politiques métier hiérarchiques et non pas de contraintes technologiques ascendantes.

SD-WAN offre une sécurité plus cohérente

Combinant une sécurité cloud à une solution SD-WAN avancée, l'architecture SASE élimine le coût et la complexité associés à la gestion sur site de plusieurs pare-feu nouvelle génération ; ce modèle nécessite des fonctionnalités de pare-feu basé sur une zone dans les succursales afin de neutraliser les menaces.

La plateforme EdgeConnect inclut les avantages suivants :

- Intelligence et connaissance des applications permettant d'identifier et autoriser les applications à accéder directement aux ressources hébergées dans le cloud
- Intégration et orchestration automatisées avec les fournisseurs de sécurité cloud de la succursale au PoP (point de présence) de mise en application de la sécurité le plus proche

Les principaux avantages incluent :

- Réduction de la latence
- Optimisation des performances des applications
- Support pour une expérience de la plus haute qualité pour les applications SaaS

L'intégration du système de défense contre les menaces d'Aruba à la plateforme SD-WAN Edge d'Aruba EdgeConnect étend les capacités de détection et prévention des intrusions (IDS/IPS) au SD-WAN. Les appliances physiques et virtuelles d'EdgeConnect s'appuient sur l'architecture des menaces et les flux de menaces d'Aruba Central pour permettre aux entreprises de fournir une sécurité latérale est-ouest et une sortie Internet locale sécurisée depuis les succursales. Elles peuvent être déployées de manière centralisée, sur site ou dans le cloud. La journalisation des menaces fournit des analyses relatives au réseau et à la sécurité à Aruba Central ainsi que des capacités UTM Edge-to-cloud complètes.

Zero Trust : Sécurisation de l'Edge par rôle, contexte et application

Vu la prolifération des appareils mobiles, des forces de travail distantes, des applications hébergées dans le cloud et des appareils IoT, les entreprises doivent aligner leurs politiques réseau basées sur les objectifs commerciaux sur leurs politiques de sécurité.

L'intégration du contrôle d'accès basé sur l'identité d'Aruba ClearPass Policy Manager à la plateforme SD-WAN d'Aruba EdgeConnect renforce l'intelligence des applications en ajoutant les informations sur l'identité des utilisateurs, des appareils, des rôles et de la posture de sécurité pour former la base d'un WAN Edge sécurisé.

Cette nouvelle couche de contexte permet de segmenter de manière très précise les types d'appareils en fonction de leur rôle au sein de l'organisation sans avoir à gérer des milliers de VLAN. Par exemple, une politique de segmentation précise peut être définie pour empêcher les caméras de sécurité d'accéder au traitement des transactions des cartes bancaires ou aux systèmes de gestion HVAC. Elle peut également restreindre le rôle des caméras de sécurité de sorte à ce qu'elles communiquent en direction du centre de contrôle du système de surveillance ou de l'appareil d'enregistrement, mais pas vers d'autres caméras. Elle aide ainsi le service informatique à gérer la conformité à la sécurité ainsi que les audits de sécurité. Elle crée également des journaux de menaces qui peuvent être exportés vers une application SIEM (gestion d'informations et d'événements de sécurité) tierce.

57 %

des personnes interrogées affirment que leurs organisations ont déployé ou déploieront Zero Trust[3]

49 %

des participants affirment que leurs organisations ont déployé ou déploieront des architectures de sécurité SASE.[4]

71 %

des participants sont prêts à choisir un fournisseur jugé être parmi les meilleurs lorsqu'ils déploient la sécurité SD-WAN cloud pour une architecture SASE[5]

3, 4, 5. Ponemon Institute, L'état des architectures de sécurité SD-WAN, SASE et Zero Trust, avril 2021

ClearPass : Sécurisation de l'IoT avec une plateforme SD-WAN avancée

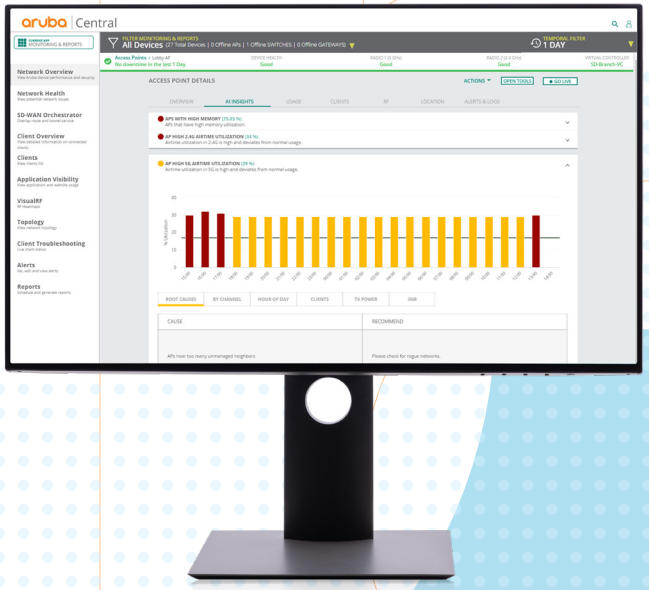
Les téléphones mobiles, ordinateurs portables ou tablettes peuvent être sécurisés avec des agents logiciels ZTNA. Toutefois, il n'est pas possible d'installer des agents logiciels de sécurité sur les appareils IoT puis qu'ils sont sans agent. Il s'agit là d'un problème de sécurité que SASE n'a pas pris en compte.

Une plateforme SD-WAN d'Aruba EdgeConnect peut réduire les risques de violation de la sécurité associés au déploiement des appareils IoT. La plateforme EdgeConnect identifie et classe le trafic des applications dès le premier paquet, l'intercepte à la périphérie du réseau et l'attribue à un segment approprié. Cette segmentation simple le sécurise du reste du trafic du réseau.

L'intégration de ClearPass à EdgeConnect renforce l'intelligence des applications avec des politiques basées sur l'identité des utilisateurs et des appareils et des politiques basées sur les rôles, ce qui contribue à raffiner la segmentation. Ce contrôle d'accès basé sur l'identité permet d'appliquer les politiques de sécurité de manière plus cohérente sur l'ensemble du réseau, de l'Edge au cloud.

La segmentation dynamique Zero Trust d'Aruba aide les entreprises à identifier les menaces par appareil, rôle et application tout en se conformant aux normes industrielles telles que PCI, HIPAA et SOX.

En combinant la plateforme SD-WAN avancée à une sécurité cloud utilisant une technologie ZTNA basée sur les politiques, vous vous assurez que le WAN, les utilisateurs, les appareils et les applications de l'entreprise sont sécurisés en permanence.



WAN et sécurité de pointe, sans compromis !

Relevant les défis associés à la sécurité et au coût, les services de sécurité hébergés dans le cloud et à orchestration centralisée continuent de connaître un taux d'adoption élevé. Les services de sécurité à gestion centralisée cloud fournissent une protection à tous les utilisateurs, appuyée par des politiques et des mises en application de politiques cohérentes sur des centaines ou même des milliers de sites, sans nécessiter de déploiements complexes ou de gestion d'appliances de sécurité physiques.

Les solutions SD-WAN avancées telles que la plateforme SD-WAN Edge d'Aruba EdgeConnect permettent aux entreprises de séparer intelligemment le trafic cloud à destination locale du trafic destiné aux succursales sur Internet. En outre, elles prennent en charge la micro-segmentation et une mise en application granulaire des politiques, ce qui permet aux entreprises de sécuriser leur WAN, de se conformer aux normes de l'industrie et de neutraliser les menaces.

L'orchestration automatisée d'un service de sécurité cloud de pointe avec la plateforme SD-WAN Edge d'Aruba EdgeConnect fournit une solution SASE puissante qui ne compromet pas les fonctionnalités réseau ou les capacités de sécurité.

SASE protège l'entreprise contre les menaces et fournit des performances d'applications et une expérience utilisateur de la plus grande qualité tout en maîtrisant les coûts.

Cette alliance entre SD-WAN et la sécurité cloud offre les avantages suivants :

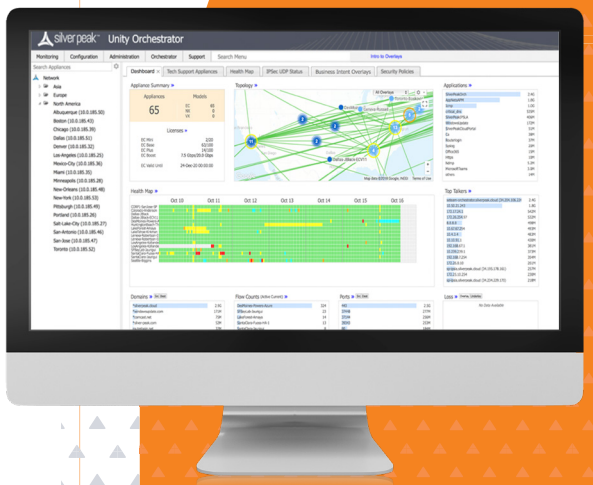
- Meilleure agilité opérationnelle et politiques IT simplifiées avec une architecture SASE qui offre tous les avantages du cloud
- Intégration rationalisée et simplifiée des fonctions de sécurité cloud-native avec des capacités SD-WAN optimisées
- Liberté de choisir la meilleure sécurité réseau et les meilleures capacités SD-WAN
- Pas de dépendance à un seul fournisseur
- Pas besoin de déployer des pare-feu coûteux et complexes dans chaque succursale
- Possibilité d'adopter des innovations en matière de sécurité à l'avenir

Automatisation de la sécurité basée dans le cloud avec SD-WAN

Les entreprises sont à la recherche de nouvelles manières d'intégrer et gérer leurs applications sur leur WAN et leur infrastructure de sécurité. L'un des meilleurs moyens de simplifier l'orchestration des services de sécurité cloud dans les succursales est d'utiliser l'automatisation de la plateforme SD-WAN d'Aruba EdgeConnect.

EdgeConnect utilise les interfaces API et l'orchestration de service de tiers pour s'intégrer à des fournisseurs de sécurité cloud de pointe, notamment ZScaler, Check Point, NetSkope et Palo Alto Prisma Access. Aruba Orchestrator valide les identifiants de sécurité cloud pour la connexion, puis automatise ou orchestre le processus de connexion des succursales de la structure SD-WAN aux PoP (points de présence) de mise en application de la sécurité cloud primaires et secondaires (facultatifs).

La configuration des politiques de sécurité consiste en une simple opération glisser-déposer depuis l'interface utilisateur d'Aruba Orchestrator, et permet aux organisations de préciser une série de politiques de sécurité à appliquer à toutes les succursales d'un seul coup.



Flexibilité et liberté de choix

Les entreprises doivent rester capables d'adopter rapidement et à moindre coût de nouvelles solutions de sécurité leur permettant de faire face aux évolutions constantes des menaces informatiques. Elles doivent évaluer les plateformes qui offrent la possibilité d'intégrer les meilleures solutions de sécurité et solutions réseau. Elles peuvent ainsi éviter d'être dépendantes d'un seul fournisseur de solutions ou d'avoir à se contenter de fonctionnalités et capacités de base.

La plateforme SD-WAN d'Aruba EdgeConnect est un élément essentiel de l'architecture SASE, et permet d'intégrer une plateforme SD-WAN de pointe à une variété de services de sécurité cloud de qualité. Aruba EdgeConnect prend en charge les fonctions de sécurité de base nécessaires aux succursales et complète la sécurité basée dans le cloud, garantissant un service d'accès sécurisé et fluide à travers toute l'entreprise.

Pour plus d'informations, veuillez consulter www.arubanetworks.com/sdwan

eBook_Aruba-Edge-to-Cloud-Security_DC_062321 a00114994enw

aruba
a Hewlett Packard Enterprise company