HPE aruba networking

EBOOK

Sécurité Edge to Cloud : Un nouveau réseau étendu et une nouvelle sécurité de la périphérie

Guide pratique pour l'adoption d'une architecture de service d'accès sécurisé en périphérie (SASE)

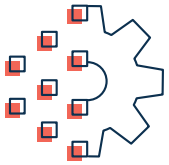
La transformation numérique et le télétravail ont un impact sur le réseau étendu et la sécurité dans un monde orienté vers le cloud

Alors que les organisations doivent relever les défis posés par la pandémie de COVID-19 et la démocratisation du travail flexible (WFA), l'adoption de services hébergés dans le cloud continue de s'accélérer. Cette évolution accentue l'urgence de transformer le datacenter conventionnel et les réseaux MPLS et VPN en un service réseau d'accès sécurisé à la périphérie (SASE) natif pour le cloud, qui permet un provisionnement plus dynamique de services réseau sécurisés tout en protégeant ses données de l'ensemble du réseau WAN.

Les trois questions les plus importantes auxquelles les responsables informatiques doivent répondre pour sécuriser leur réseau étendu sont les suivantes :

- Comment puis-je m'assurer que je sélectionne la bonne architecture SD-WAN pour prendre en charge en toute sécurité les applications de l'entreprise dans un environnement donnant la priorité au cloud ?
- Comment l'environnement permanent et hybride du travail à distance (WFA) va-t-il influer sur les décisions informatiques concernant l'adoption d'une architecture de sécurité dans un cadre SASE ?
- Comment les services informatiques peuvent-ils gérer les défis de sécurité liés à la prolifération des dispositifs IOT, principalement sans agent ?

Examinons comment les prérequis évoluent en matière de réseau et de sécurité dans un monde orienté cloud.



50 %

des personnes interrogées en 2021 déclaraient la mise en place et l'exécution de diverses initiatives de transformation numérique par rapport à 38 % en 2020[1]

45 %

des entreprises ont une stratégie axée sur le cloud[2]

1, 2. Enquête d'ESG sur les intentions de dépenses en technologies informatiques, décembre 2020

Zéro confiance, ZTNA et SASE dans un monde prioritairement axé sur le cloud

Les solutions de sécurité classiques n'ont pas été conçues autour du cloud. Le concept de réacheminement du trafic vers un datacenter centralisé fonctionnait lorsque toutes les applications y résidaient. Cependant, avec l'augmentation du trafic des utilisateurs dans les filiales et la migration des applications vers le cloud, le réacheminement du trafic sur un réseau hérité en étoile nuit à l'expérience utilisateur, augmente les risques de sécurité et coûte cher.

Les solutions de sécurité réseau héritées n'intègrent peut-être pas encore le concept de zéro confiance pour le contrôle et la gestion des accès basés sur les identités et les rôles. Ce concept repose sur le principe qu'aucune action de l'utilisateur ou du logiciel n'est fiable tant qu'il n'est pas authentifié. En d'autres termes, il faut tout authentifier, puis limiter l'accès aux seules applications et données nécessaires en fonction du rôle de l'utilisateur ou de l'appareil. La sécurité zéro confiance exige que tous les utilisateurs, dispositifs et instances d'application prouvent qui ils sont ou ce qu'ils prétendent être et si ils sont autorisés à accéder uniquement aux ressources qu'ils recherchent, qu'ils se trouvent à l'intérieur ou à l'extérieur du périmètre du réseau.

L'accès réseau Zéro confiance (ZTNA) est un ensemble de technologies fonctionnant dans un modèle zéro confiance, où l'accès est accordé uniquement aux personnes qui en ont besoin sur la base d'un accès restrictif, défini par des politiques granulaires. ZTNA offre aux utilisateurs une connectivité transparente et sécurisée aux applications privées sans jamais les placer sur le réseau ni les exposer sur Internet.

Enfin, il y a le SASE, un terme inventé par Gartner. SASE désigne un service d'accès sécurisé en périphérie dans une architecture qui combine des fonctionnalités SD-WAN avancées, avec des fonctions de sécurité du réseau complètes fournies par le cloud, telles que la passerelle Web sécurisée (SWG), l'agent de sécurité des accès au cloud (CASB), le pare-feu as-a-service (FWaaS), ZTNA, etc.

Défis liés à la sécurité du réseau local et du WAN

Dans le monde d'aujourd'hui, où le cloud est roi, les besoins en sécurité des réseaux étendus et locaux sont plus interdépendants que jamais. Pour concrétiser toutes les promesses de la transformation numérique, les entreprises devront transformer à la fois leurs architectures WAN et de sécurité pour prendre en charge des applications d'entreprise hébergées et accessibles depuis n'importe quel endroit et n'importe quel réseau de transport.

Examinons les principaux défis de sécurité et de réseau étendu auxquels sont confrontées les équipes informatiques et de mise en réseau des entreprises :

- Comment puis-je profiter des avantages commerciaux et opérationnels du cloud tout en maintenant des niveaux élevés de sécurité et en réduisant le risque global ?
- Comment garantir une expérience utilisateur cohérente et de qualité pour toutes les applications de l'entreprise hébergées dans le cloud sur le réseau étendu ?
- Comment déployer et appliquer des politiques d'accès au réseau cohérentes pour les employés travaillant dans un environnement hybride (en partie dans le bureau/la filiale ou en télétravail) ?
- Comment puis-je assurer la sécurité et la connectivité WAN d'un si grand nombre de dispositifs, d'utilisateurs et d'applications ?
- Est-ce que choisir une plateforme SD-WAN adaptée peut améliorer l'intégration de la sécurité du réseau étendu et du réseau local ?
- Puis-je obtenir tous les services de sécurité dont j'ai besoin auprès d'un seul fournisseur ?

Intégration des applications SD-WAN et des politiques de sécurité

Dans l'économie mondiale d'aujourd'hui, qui évolue toujours plus vite, les entreprises ont besoin de l'agilité nécessaire pour créer rapidement de nouvelles filiales et ajuster dynamiquement les règles de politique et de sécurité. L'extension du contexte des politiques est également cruciale pour l'automatisation des filiales et constitue une capacité clé que seule une solution SD-WAN avancée, telle que la plateforme SD-WAN Aruba EdgeConnect Enterprise, peut offrir.

Une solution SD-WAN avancée peut également aider les entreprises à éliminer le recours à de multiples appareils en unifiant les fonctions clés de la périphérie du réseau étendu de la filiale, telles que :

- SD-WAN
- Routage
- Pare-feu et segmentation de nouvelle génération
- Gestion unifiée des menaces (UTM)
- Visibilité et contrôle des réseaux et des applications
- Optimisation des réseaux WAN

La consolidation de ces fonctions simplifiera ou allégera la périphérie du réseau étendu de la filiale. La centralisation de la gestion va également améliorer l'efficacité informatique et assurer une qualité de service (QoS) et une application des politiques de sécurité plus cohérentes.

L'orchestration centralisée de SD-WAN Aruba EdgeConnect unifie la configuration et la gestion continue. Elle garantit également que la qualité de service et la sécurité sont appliquées et mises en œuvre de manière cohérente pour les applications (ou les catégories d'applications) indépendamment de la manière dont on y accède ou 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.

Comment SD-WAN rend la sécurité plus cohérente

La mise en œuvre d'une architecture SASE qui combine la sécurité fournie par le cloud avec une solution SD-WAN avancée élimine le coût et la complexité associés à la gestion de plusieurs pare-feu de nouvelle génération sur site. Ce modèle nécessite toujours une fonctionnalité de pare-feu dynamique par zone sur les sites des filiales pour bloquer les menaces entrantes.

La plateforme EdgeConnect offre les services suivants :

- Intelligence et connaissance des applications pour reconnaître et autoriser les applications de la liste d'autorisation à accéder directement aux ressources hébergées dans le cloud
- Intégration automatisée avec les fournisseurs de pointe de Security Service Edge (SSE), depuis la filiale jusqu'au point de présence (PoP) d'application de la sécurité le plus proche

Ses avantages clés incluent :

- Latence réduite
- Performances des applications optimisées
- Qualité d'expérience optimale pour les applications SaaS de confiance

L'intégration d'Aruba Threat Defense à la plateforme SD-WAN Aruba EdgeConnect Enterprise étend les fonctionnalités avancées de détection et de prévention des intrusions (IDS/IPS) au SD-WAN. Les appliances physiques et virtuelles de EdgeConnect s'appuient sur l'infrastructure de réduction des menaces d'Aruba et sur les flux d'évaluation des menaces d'Aruba Central, ce qui permet aux entreprises d'assurer une sécurité latérale entre les serveurs et de sécuriser l'accès local à Internet depuis les filiales. Elles peuvent être déployées de manière centralisée, sur site ou dans le cloud. La journalisation des menaces fournit des analyses du réseau et de la sécurité à Aruba Central et offre des fonctionnalités UTM complètes de la périphérie au cloud (Edge to Cloud).

Zéro confiance : Sécurisation de la périphérie par rôle, contexte et application

Avec l'augmentation du nombre d'appareils mobiles, du personnel à distance, d'applications hébergées dans le cloud et de périphériques de l'Internet des objets (IoT), les entreprises doivent aligner les politiques de mise en réseau et les politiques de sécurité sur les intentions de l'entreprise.

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

Cette nouvelle couche de contexte permet une segmentation fine des types de dispositifs en fonction de leur rôle dans l'organisation, sans la complexité de la gestion de milliers de VLAN. Par exemple, une politique de segmentation fine peut être définie pour empêcher les caméras de sécurité d'accéder au traitement des transactions par carte de crédit ou aux systèmes de gestion du chauffage, de la ventilation et de la climatisation. Elle peut également restreindre les fonctions des caméras de sécurité afin qu'elles puissent communiquer avec la tête de réseau de surveillance ou le dispositif d'enregistrement, mais pas avec les autres caméras. Cela aide le service informatique à gérer la conformité de la sécurité des applications et les audits de sécurité. Elle génère également des journaux de bord des menaces qui peuvent être exportés vers une application tierce de gestion des informations et des événements de sécurité (SIEM).

57 %

des personnes interrogées déclarent que leur entreprise a déployé ou va déployer une solution Zéro confiance[3]

49 %

des personnes interrogées affirment que leur organisation a déployé ou va déployer des architectures SASE[4]

71 %

des personnes interrogées choisiraient un fournisseur de pointe lors du déploiement d'un SD-WAN et d'une sécurité basée sur le cloud pour une architecture SASE[5]

3, 4, 5. Ponemon Institute, The State of SD-WAN, SASE and Zero Trust Security Architectures, avril 2021

Aruba ClearPass : Sécuriser l'internet des objets avec une solution SD-WAN avancée

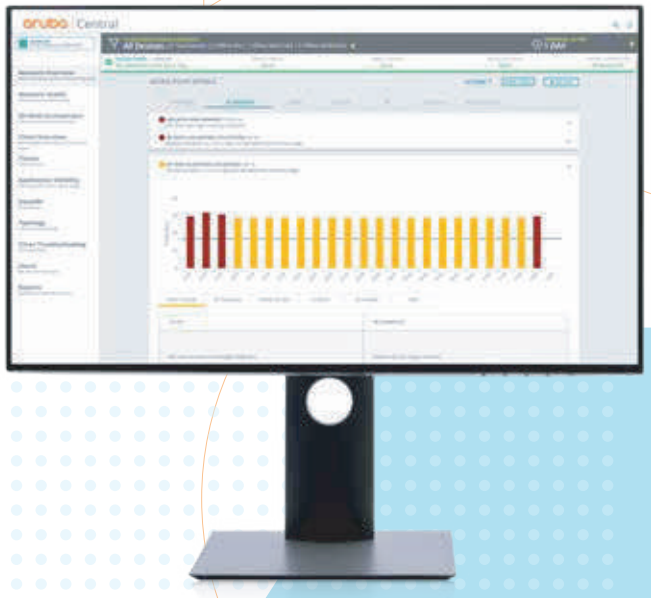
Les téléphones mobiles, les ordinateurs portables ou les tablettes peuvent être sécurisés à l'aide d'agents logiciels ZTNA ; cependant, les agents logiciels de sécurité ne peuvent pas être installés sur les dispositifs IoT, puisqu'ils sont sans agent. Cela pose un problème de sécurité auquel le SASE ne peut répondre directement.

Une plateforme SD-WAN Aruba EdgeConnect peut réduire le risque associé aux atteintes à la sécurité lors du déploiement des dispositifs IoT. La plateforme EdgeConnect identifie et classe le trafic des applications dès le premier paquet, l'intercepte à la périphérie du réseau et peut l'affecter à un segment approprié. Cette segmentation globale sécurise le réseau par rapport aux autres trafics.

L'intégration de ClearPass avec EdgeConnect augmente l'intelligence de l'application avec l'identité de l'utilisateur et de l'appareil et la politique basée sur des rôles, et permet une segmentation encore plus fine. Le contexte supplémentaire basé sur l'identité permet une application cohérente de la politique de sécurité, qui peut être appliquée à l'échelle du réseau, de l'edge au cloud.

La segmentation dynamique zéro confiance d'Aruba permet aux entreprises d'isoler les menaces de sécurité par dispositif, rôle et application, tout en respectant les normes de conformité industrielles telles que PCI, HIPAA et SOX.

La combinaison d'un SD-WAN évolué et d'une sécurité fournie par le cloud à l'aide d'un ZTNA reposant sur les politiques établies garantit que le réseau étendu de l'entreprise, les utilisateurs, les appareils et les applications sont toujours sécurisés.



Réseau étendu et sécurité de pointe, sans compromis !

Pour relever les défis de la sécurité et des coûts, des services de sécurité de pointe, hébergés dans le cloud et orchestrés de manière centralisée, ont vu le jour et continuent d'être rapidement adoptés. Les services de sécurité dans le cloud, gérés de manière centralisée, assurent la protection de tous les utilisateurs, grâce à des politiques cohérentes et à l'application de politiques sur des centaines, voire des milliers de sites, sans la complexité du déploiement ou de la gestion de dispositifs de sécurité physiques.

Grâce aux solutions de la plateforme SD-WAN Aruba EdgeConnect Enterprise, les entreprises peuvent répartir intelligemment le trafic localisé dans le cloud à partir des sites de filiales sur Internet. De plus, ces solutions prennent en charge les fonctionnalités de micro-segmentation et l'application granulaire des politiques, ce qui permet aux entreprises de sécuriser leur réseau étendu, de se conformer aux exigences de conformité et de se défendre contre les atteintes à la sécurité.

Les intégrations automatisées avec les solutions de sécurité basées sur le cloud des fournisseurs de pointe de SSE permettent d'obtenir une architecture SASE puissante sans compromettre les fonctionnalités du réseau ni les capacités de sécurité.

SASE protège l'entreprise contre les menaces et offre des performances d'applications et une expérience utilisateur optimales tout en maîtrisant les coûts.

Les avantages de ce mariage entre SD-WAN et SSE sont les suivants :

- Une plus grande agilité pour l'entreprise et des politiques informatiques simplifiées, grâce à une architecture SASE qui offre tous les avantages du cloud
- Une intégration simplifiée et rationalisée des fonctions de sécurité natives pour le cloud avec des fonctionnalités SD-WAN optimisées
- La liberté de choisir la sécurité du réseau de pointe et les fonctionnalités SD-WAN de pointe
- Éviter le verrouillage d'un seul fournisseur
- Éliminer la nécessité de déployer des pare-feux de nouvelle génération coûteux et complexes dans chaque filiale
- Flexibilité nécessaire pour adopter les futures innovations en matière de sécurité

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

Les entreprises cherchent des moyens plus simples d'intégrer et de gérer leurs applications à travers leur réseau étendu et leur infrastructure de sécurité. L'une des meilleures façons de simplifier l'orchestration des services de sécurité basés sur le cloud sur les sites des filiales est de tirer parti de l'automatisation avec Aruba EdgeConnect SD-WAN.

EdgeConnect utilise des interfaces d'applications (API) et l'orchestration de services tiers pour s'intégrer aux principaux fournisseurs de SSE, notamment Zscaler, Netskope, McAfee et Palo Alto Prisma Access. Aruba WAN Orchestrator valide les informations d'identification de la sécurité du cloud pour la connexion, puis automatise ou orchestre le processus de connexion des filiales dans la matrice SD-WAN aux points de présence primaires et secondaires facultatifs d'application de la sécurité les plus proches.

La configuration des politiques de sécurité se fait par simple glisser-déposer à partir de l'interface utilisateur intuitive d'Aruba WAN Orchestrator, ce qui permet aux entreprises de spécifier un ensemble de politiques de sécurité à appliquer à toutes les filiales en une seule action.

Flexibilité et liberté de choix

Le paysage des menaces ne cessant d'évoluer, les entreprises doivent rester agiles en adoptant de nouvelles solutions de sécurité de manière rapide et rentable. Elles doivent trouver des plateformes qui offrent une liberté de choix pour intégrer des solutions de réseau et de sécurité de pointe. Elles évitent ainsi d'être enfermées dans des solutions à fournisseur unique ou de se contenter de fonctionnalités et de capacités de base.

La plateforme SD-WAN Aruba EdgeConnect est un pilier essentiel d'une architecture SASE de pointe, car elle permet d'intégrer la meilleure plateforme SD-WAN de sa catégorie avec les meilleurs services de sécurité de leur catégorie fournis par le cloud. Aruba EdgeConnect prend en charge les fonctions de sécurité fondamentales requises au niveau de la filiale et complète le SSE pour offrir un service d'accès sécurisé en périphérie transparent dans toute l'entreprise.

Pour plus d'informations, consultez l'adresse suivante :

www.arubanetworks.com/sdwan

SEQUENCE INFORMATIQUE

eBook_Aruba-Edge-to-Cloud-Security_RM_071122 a00114994fre

HPE aruba networking