



HPE Aruba Networking EdgeConnect Microbranch

Principales caractéristiques

- **Wi-Fi géré dans le cloud** : N'importe lequel de nos points d'accès Wi-Fi 5 ou ultérieur peut être utilisé pour fournir une connectivité fiable et hautement performante afin d'offrir la même expérience utilisateur et la même sécurité, qu'un employé se trouve chez lui ou au bureau.
- **Routes et tunnels automatisés** : Automatise la façon dont le trafic doit être acheminé vers les points de terminaison en fonction de règles pour des applications, des sites web ou des types d'utilisateurs spécifiques afin d'améliorer la performance et la sécurité.
- **Orchestration automatisée des routes et des tunnels** : Les points d'accès peuvent orchestrer les tunnels IPsec à la demande et rediriger le trafic si nécessaire pour optimiser la performance du réseau.
- **SASE et Zero Trust** : Applique un routage fondé sur une politique pour orchestrer les tunnels et diriger certains trafics d'utilisateurs distants pour l'inspection de la sécurité du cloud afin d'étendre les architectures SASE et Zero Trust au bureau à domicile. Optez pour le SASE unifié de HPE Aruba Networking ou tirez parti des intégrations avec une grande variété de fournisseurs de sécurité du cloud.
- **Résolution des incidents de l'intégrité du WAN** : Des vues de tableau de bord fournissent des mises à jour en temps quasi réel sur la disponibilité, l'utilisation et le débit du WAN, avec une exploration de la performance des FAI et des VPN afin d'accélérer la résolution des problèmes.
- **Accès aux ressources du bureau** : Les employés peuvent brancher des téléphones VoIP ou des imprimantes filaires directement sur l'AP et accéder en toute sécurité aux ressources du campus à l'aide des SSID de l'entreprise.

Passer au travail à distance

Désormais, les équipes informatiques sont chargées d'assurer une expérience sécurisée et fiable à une main-d'œuvre hautement distribuée qui accède aux datacenters et aux applications dans le cloud par le biais de connexions haut débit et cellulaires qui échappent au contrôle et à la visibilité de l'équipe informatique. Ce qu'il faut, c'est un moyen plus simple pour le service informatique de fournir une connectivité à l'échelle de l'entreprise aux employés qui travaillent à distance en étendant le WAN du campus au bureau à domicile et aux petits bureaux ou emplacements ad hoc.

Présentation d'EdgeConnect Microbranch

S'appuyant sur la technologie de point d'accès à distance de HPE Aruba Networking, la solution HPE Aruba Networking EdgeConnect Microbranch ajoute des fonctionnalités SD-WAN et SASE avancées en vue de fournir une solution à l'échelle de l'entreprise gérée dans le cloud pour le bureau à domicile ou les petites entreprises dans le cadre d'un environnement de travail hybride.

Le service informatique peut déployer à distance et gérer de manière centralisée une connectivité réseau sécurisée pour des centaines, voire des milliers de télétravailleurs ou d'employés de petits bureaux, afin de leur offrir une expérience similaire à celle du bureau en utilisant HPE Aruba Networking Central et n'importe lequel de nos points d'accès.

Les travailleurs à distance peuvent connecter des clients sans fil (ordinateurs portables, smartphones, tablettes) ainsi que des clients filaires, tels que des téléphones VoIP, et accéder à des applications stratégiques de manière fiable et sécurisée. En guise de sauvegarde, le point d'accès utilise des connexions cellulaires via un dongle LTE inséré dans le port USB ou, dans certains AP, un module enfichable pour la redondance de la liaison montante et la continuité de l'activité. Le service informatique bénéficie d'une approche unifiée qui permet au personnel de configurer, de dépanner et d'optimiser les performances du réseau sur site, dans les succursales et dans les environnements de travail distants. L'orchestration intelligente du routage et des tunnels basée sur des règles permet d'optimiser l'efficacité opérationnelle et les performances du réseau.

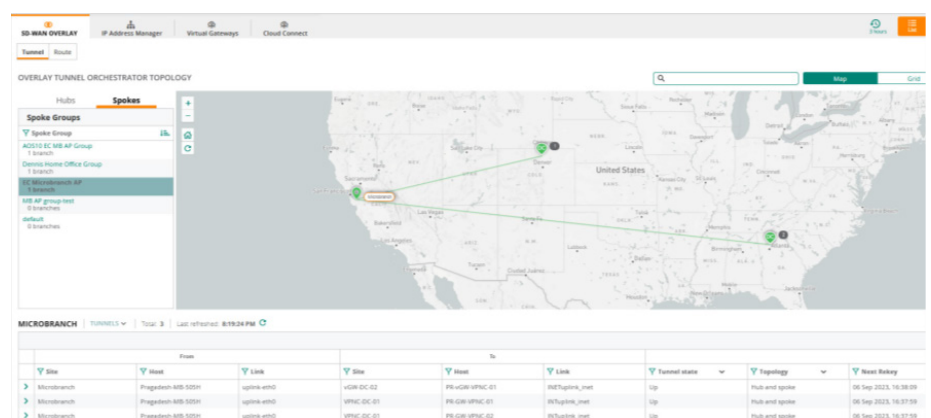


Figure 1. Carte de l'orchestration des tunnels de superposition dans HPE Aruba Networking Central

Architecture du travail à distance

Grâce à des tunnels VPN IPsec, nos points d'accès sont entièrement capables de fournir

une connectivité sans fil (et filaire) sécurisée entre les succursales distantes ou les télétravailleurs et les ressources de l'entreprise. Les tunnels et les routes entre le point d'accès et le datacenter sont automatiquement créés sans intervention de l'utilisateur via Central à l'aide de l'orchestration des tunnels et de celle des routes. Il n'est pas nécessaire de configurer manuellement le tunnel ou de calculer un itinéraire pour optimiser la performance.

Dans l'architecture Microbranch, le point d'accès peut créer un tunnel VPN sur Internet vers un cluster de concentrateur VPN (VPNC) déployé dans un datacenter sur site ou basé sur le cloud ou bien dans un cloud public – ou encore utiliser un accès Internet direct pour un acheminement direct vers une application SaaS. Le point d'accès fournit également une fonctionnalité SD-WAN avancée, auparavant disponible sur les passerelles, pour offrir une fiabilité élevée aux travailleurs à distance. La mise en œuvre est rationalisée puisque la connectivité Wi-Fi et les fonctionnalités SD-WAN sont combinées dans un seul système d'exploitation et exécutées sur l'AP géré dans le cloud sans avoir besoin de matériel ou d'appliances supplémentaires sur site.

La fonctionnalité Microbranch offre une flexibilité avec la prise en charge des modes de déploiement de couche 2, de couche 3 et mixtes. Pour les déploiements de couche 2, le serveur DHCP s'exécute dans le datacenter où se trouve le concentrateur VPN (VPNC). Dans les déploiements de couche 3, le point d'accès lui-même fait office de serveur DHCP pour les clients.

Aucune passerelle ou surcharge associée n'est requise, accélérant ainsi le déploiement et rationalisant les opérations en mode de couche 2, couche 3 ou mixte.

Central assure la gestion et l'orchestration de la solution Microbranch. En tant que console de gestion et d'orchestration, cette solution fournit un point de contrôle unique pour superviser tous les aspects des LAN, WAN et VPN filaires et sans fil de campus, de filiale et de bureaux distants.

Les fonctionnalités d'analyse pilotée par l'IA, d'orchestration et d'automatisation de bout en bout et de sécurité avancée sont intégrées dans la solution de manière native. Des mises à niveau en temps réel, des rapports fiables et une assistance par chat en direct sont aussi fournis pour optimiser les activités de maintenance quotidiennes. Construit sur une architecture de microservices cloud native, Central répond aux exigences de l'entreprise en termes d'adaptation et de résilience.

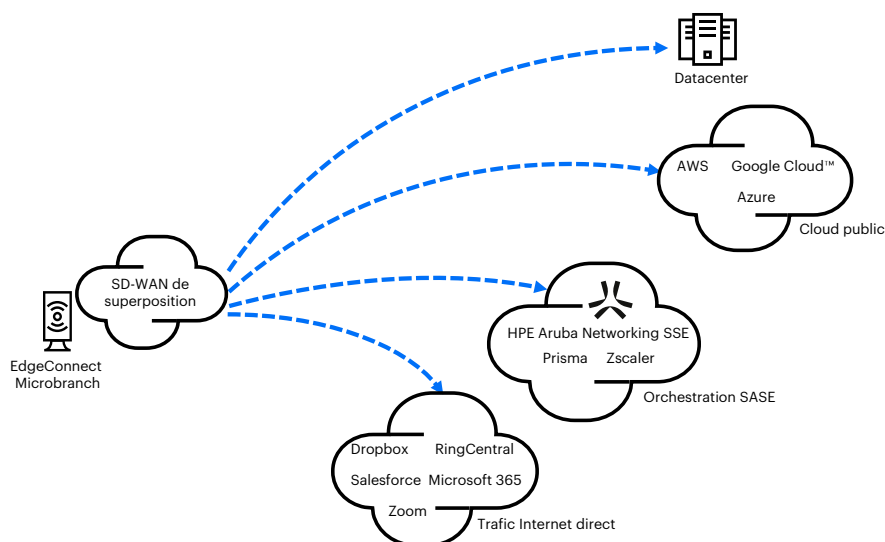


Figure 2. La solution Microbranch prend en charge le mode tunnel divisé et le routage fondé sur une politique SD-WAN pour une sécurité accrue et une expérience utilisateur améliorée.

Routage fondé sur une politique SD-WAN

Traditionnellement, tout le trafic utilisateur est transmis au datacenter pour des vérifications de règles. Ce processus entraîne d'énormes flux de trafic et, avec un nombre toujours croissant d'employés travaillant à distance, l'impact sur l'expérience utilisateur et la productivité des équipes n'est pas négligeable.

L'orchestration fondée sur une politique applique des règles cohérentes au trafic des utilisateurs distants pour renforcer la sécurité et améliorer l'expérience utilisateur. Dans un déploiement Microbranch, le trafic est transféré via le réseau superposé ou vers Internet à l'aide d'un routage basé sur la destination ou peut être transféré à l'aide d'un routage intelligent fondé sur une politique afin de créer des règles qui utilisent toutes les liaisons disponibles.

Grâce au routage fondé sur des politiques, les points d'accès peuvent implémenter de manière cohérente des règles automatisées telles que celles répertoriées ci-dessous pour garantir :

- Le trafic des utilisateurs distants vers l'entreprise est acheminé vers le datacenter via un tunnel VPN IPsec sécurisé.
- Le trafic des utilisateurs distants, tel que le trafic web général, est directement envoyé à l'inspection de la sécurité du cloud via un tunnel orchestré.
- Le trafic des utilisateurs distants vers les applications SaaS de confiance de l'entreprise peut être directement dirigé vers le fournisseur SaaS via Internet afin de minimiser la latence pour les vidéoconférences et autres applications stratégiques.

Les entreprises peuvent également spécifier des règles précises basées sur des applications spécifiques et des sites web de destination (ou catégories web) pour déterminer la manière dont le trafic doit être traité. Étant donné que les politiques sont définies de manière centralisée, elles peuvent être appliquées de manière cohérente. Les utilisateurs bénéficient de performances améliorées puisque des politiques peuvent être implémentées pour optimiser le routage et éviter les retards ou les renvois inutiles du trafic.

L'orchestration des tunnels supprime les problèmes de complexité et d'évolutivité associés à la configuration des tunnels IPsec entre les points d'accès d'un site distant et la passerelle de tête de réseau et peut fonctionner en mode centralisé, distribué ou local pour une plus grande flexibilité.

Sécurité Edge to Cloud Zero Trust et SASE

La solution Microbranch étend le cadre Zero Trust et SASE au domicile/petit bureau dans des environnements de travail hybrides en utilisant un routage fondé sur des politiques pour orchestrer les tunnels et diriger certains trafics d'utilisateurs distants vers une solution SSE (Security Service Edge) telle que HPE Aruba Networking SSE, ou d'autres solutions SSE tierces.

Les politiques d'inspection de sécurité du cloud peuvent être configurées directement via Central pour rationaliser les opérations. Une fois configurées, les fonctionnalités Microbranch canalisent automatiquement le trafic vers la solution SSE via IPsec vers le meilleur POP disponible, permettant ainsi au service informatique de prendre en charge un grand nombre de sites de travail distants sans déployer d'appliances ou d'agents de point de terminaison supplémentaires.

De plus, pour le trafic destiné au datacenter, HPE Aruba Networking ClearPass applique des politiques cohérentes et des contrôles de sécurité granulaires au niveau de l'application, de l'utilisateur, de l'appareil ou de l'emplacement sur les réseaux sans fil, filaires et VPN. D'autres serveurs NAC peuvent également être exploités. Le service informatique bénéficie d'une visibilité détaillée de tous les appareils connectés à l'entreprise, d'un contrôle accru grâce à une authentification ou une autorisation simplifiée et automatisée des appareils, ainsi que d'une analyse et d'une réponse aux incidents plus rapides et meilleures.

En combinant les fonctionnalités avancées des solutions Microbranch avec les services de sécurité Zero Trust fournis dans le cloud d'un SSE, les organisations distribuées peuvent créer une architecture SASE flexible pour garantir un accès stable et sécurisé aux applications métier tout en faisant converger les fonctions réseau et sécurité.

Visibilité complète de l'état du WAN

Pour mieux dépanner et optimiser les performances, la solution Microbranch offre une visibilité sur l'état du WAN et du VPN du point d'accès, y compris les mesures de perte de paquets, de latence et de gigue (Figure 3). Grâce à ces informations, le service informatique peut rapidement évaluer l'état général et déterminer si le problème vient du FAI ou d'ailleurs. De plus, le service informatique peut également surveiller l'utilisation et le débit du trafic à différents intervalles de temps. Avec d'autres solutions, la visibilité informatique sur le WAN est souvent limitée à l'état du concentrateur VPN. Ainsi, lorsque les travailleurs à distance signalent des problèmes, les opérateurs ne sont pas en mesure d'évaluer pleinement la situation.

Déploiement et gestion centralisés

Étant donné que les points d'accès sont gérés par Central natif pour le cloud, le service informatique peut configurer, surveiller et dépanner de manière centralisée à l'aide d'une vue unifiée dans des environnements de campus, de filiales et de travailleurs à distance tout en unifiant la gestion du réseau sur les réseaux filaires, sans fil et SD-WAN. Central fournit des fonctionnalités riches, notamment le provisionnement sans intervention, le clustering automatique et les pools d'adresses IP centralisés. Les services d'orchestration pour les tunnels et les routes automatisent la création de tunnels et l'optimisation des routes. Ils éliminent aussi les processus de configuration manuelle.

Prérequis du produit

HPE Aruba Networking Central pour la gestion et l'orchestration basées sur le cloud Points d'accès Aruba séries 3xx, 5xx ou 6xx exécutant des passerelles ArubaOS 10.x série 7xxx/9xxx ou une passerelle virtuelle dans le datacenter pour agir en tant que concentrateurs VPN

Points essentiels à retenir

La solution Microbranch aide le service informatique à garantir un accès sécurisé et fiable pour les équipes distantes. Il étend le WAN aux travailleurs à distance, en leur offrant une expérience similaire au bureau et en ouvrant de nouveaux cas d'utilisation d'applications pour le travail à distance.

Grâce à la gestion de réseau cloud et au provisionnement sans intervention, le service informatique peut gérer plus facilement les environnements hautement distribués, résoudre les incidents affectant les travailleurs à distance et étendre le cadre SASE pour appliquer des politiques cohérentes sur les campus, les filiales et les environnements de travail à distance.

En savoir plus

Découvrez notre solution de travail à domicile qui exploite HPE Aruba Networking Central et les points d'accès.



Figure 3. Le service informatique bénéficie d'une visibilité et d'une analyse approfondies de l'état du WAN.

Spécifications techniques – Points d'accès Microbranch

	Série 3xx	Série 50x	Série 51x	Série 53x/55x	Série 6xx
Clients maximum	256	256	512	1 024	1 024
Nombre maximal de VLAN	4 094	4 094	4 094	4 094	4 094
Baux DHCP maximum	2 048	2 048	2 048	2 048	2 048
Entrées ARP	4 096	4 096	4 096	4 096	4 096
Tableau MAC	16 384	16 384	16 384	16 384	16 384
Nombre de rôles	32	32	32	32	32
Nombre d'ACL max par rôle	512	512	512	512	512
Nombre d'ACL	2 048	2 048	2 048	2 048	2 048
Active firewall sessions	32 767	32 767	32 767	32 767	32 767

Spécifications techniques – Passerelle Headend

Désignation	Valeur
AP Microbranch max dans un seul compte	20 000
AP Microbranch max dans un seul compte	5 000
AP Microbranch max dans un seul cluster (2 nœuds)	8 000
Microbranch max dans un seul groupe Central	1 000
VPNC max dans un datacenter Microbranch	Cluster 4 nœuds
Microbranch max vers Zscaler	200
Allocations IPMS	100 000

Spécifications techniques – Plateforme

Plateforme	Tunnels de superposition SD-WAN max	Routes max	Débit crypto	Sessions pare-feu	Tableau ARP	Limite d'utilisateurs (noeud L2)
9 240 – base	8 192	32 000	20 Gbit/s	4 millions	64 000	64 000
7 280	8 192	32 000	50 Gbits/s	2 millions	32 768	32 000
7240XM	6 144	32 000	30 Gbits/s	2 millions	32 768	32 000
7 220	4 096	16 000	21 Gbits/s	2 millions	24 576	24 000
7 210	1 024	8 000	8 Gbit/s	2 millions	16 384	16 000
vGW-4G	8 192	32 000	4 Gbit/s	6 millions	-	S/O
vGW-2G	4 096	32 000	2 Gbit/s	256 000	-	S/O
vGW-500M	1 600	2 048	500 Mbit/s	64 000	-	S/O
7 030	512	4 000	2,6 Gbits/s	65 000 (128 000 sur 1.0.6.3+)	4 096	4 000
7 010/7 024	256	4 000	2,6 Gbits/s	64 000	2 048	2 000
9 004/9 012	512	12 000	3 Gbits/s	64 000 (128 000 de 2.3+ quand IDPS est désactivé)	2 048	2 000

[Visiter HPE.com](#)

[Live Chat](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. Les informations figurant dans le présent document sont susceptibles d'être modifiées sans préavis. Les seules garanties relatives aux produits et services Hewlett Packard Enterprise sont stipulées dans les déclarations de garantie expresses accompagnant ces produits et services. Aucune information du présent document ne saurait être considérée comme constituant une garantie supplémentaire. Hewlett Packard Enterprise décline toute responsabilité quant aux éventuelles erreurs ou omissions techniques ou rédactionnelles qui pourraient être constatées dans le présent document.

Google Cloud est une marque déposée de Google LLC. Azure et Microsoft sont des marques commerciales ou des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. Toutes les marques tierces sont détenues par leurs propriétaires respectifs.

a00119570FRE, Rév. 2

HEWLETT PACKARD ENTERPRISE

hpe.com

