aruba
a Hewlett Packard Enterprise company

PRÉSENTATION GÉNÉRALE DE LA SOLUTION

SEGMENTATION DYNAMIQUE

Accès simple et sécurisé qui unifie les réseaux filaires et sans fil

Le nombre croissant des devices IoT et l'utilisation de services stratégiques de mobilité et cloud sont à l'origine d'innovations numériques sur le lieu de travail, ce qui nous amène à la question suivante : la périphérie du réseau est-elle suffisamment intelligente pour connecter en toute sécurité tous les types d'appareils et d'utilisateurs ? Les réseaux filaires et sans fil existants ont été créés sans tenir compte de la connectivité essentielle pour l'entreprise, de l'accès à l'IoT ou de la sécurité. L'approche actuelle consistant à utiliser des configurations manuelles et statiques pour ces appareils mobiles et ces devices IoT en perpétuelle évolution, situés sur l'ensemble des réseaux de campus et de succursales, implique de nouveaux risques en matière de sécurité et est devenue une tâche fastidieuse dont doivent s'acquitter les équipes informatiques chaque jour.

Pour simplifier et sécuriser le réseau, la segmentation dynamique Aruba unifie la mise en œuvre des politiques sur les réseaux filaires et sans fil, tout en garantissant la sécurité et la séparation du trafic. Cela permet désormais de faire co-exister aisément les opérations commerciales et les réseaux gérés par l'entreprise avec l'IoT et les appareils clients gérés par l'informatique, tout en optimisant l'expérience réseau et les opérations informatiques du cœur à la périphérie.

La segmentation dynamique tire parti de l'intelligence obtenue grâce à la fonction fondamentale d'Aruba en matière de politique basée sur les rôles, des pare-feu utilisateurs, ainsi que d'une vaste visibilité des applications de couche 7 et d'un filtrage intégré du contenu Web.

PRINCIPAUX MOTEURS COMMERCIAUX ET TECHNIQUES

Simplification de l'administration des politiques

L'intégration de l'IoT et des appareils client a généralement nécessité plusieurs points de contact, requérant la configuration manuelle de nouveaux VLAN, ACL ou sous-réseaux à chaque entrée dans le réseau. Des mutations, des ajouts et des changements permanents concernant les vastes réseaux distribués peuvent également être chronophages et sujets à l'erreur. La conception d'un réseau doté d'une solide sécurité tout en réduisant la complexité s'excluent généralement mutuellement.

PRINCIPAUX AVANTAGES

- **Amélioration d'une expérience utilisateur cohérente** – Étendre le rôle de l'utilisateur, l'inspection approfondie des paquets des applications et les fonctionnalités de profilage des appareils des réseaux sans fil aux réseaux filaires
- **Simplification des opérations réseau** – Gagnez du temps et éliminez la prolifération anarchique des réseaux VLAN en réduisant la configuration nécessaire pour les SSID, les ACL, les ports filaires
- **Amélioration de la sécurité et de la visibilité des appareils** – ClearPass et les pare-feu d'application des politiques (PEF) offrent une amélioration de la visibilité et de l'application des politiques

Amélioration de l'expérience utilisateur

Au fur et à mesure que les utilisateurs se déplacent de bureau en bureau ou de site en site, ils s'attendent à la même expérience réseau quel que soit l'endroit ou le mode de connexion, filaire ou sans fil. Et il s'avère difficile de leur demander d'utiliser un réseau privé virtuel (VPN). Toute expérience réseau nécessitant une assistance informatique est considérée comme négative. L'expérience utilisateur - qu'il s'agisse d'un employé, d'un invité, d'un acheteur ou d'un étudiant - influence la réussite d'une organisation. Souvent, la connexion de nouveaux types d'appareils, tels que des smartphones, des imprimantes ou des équipements de vidéoconférence s'effectue à l'insu ou sans l'assistance des équipes informatiques. Les équipes informatiques

La vulnérabilité du réseau s'avère exposée en raison du nombre d'appareils IoT/sans interface connectés aux réseaux d'entreprise qui devraient atteindre plus de 20 milliards d'ici 2020.

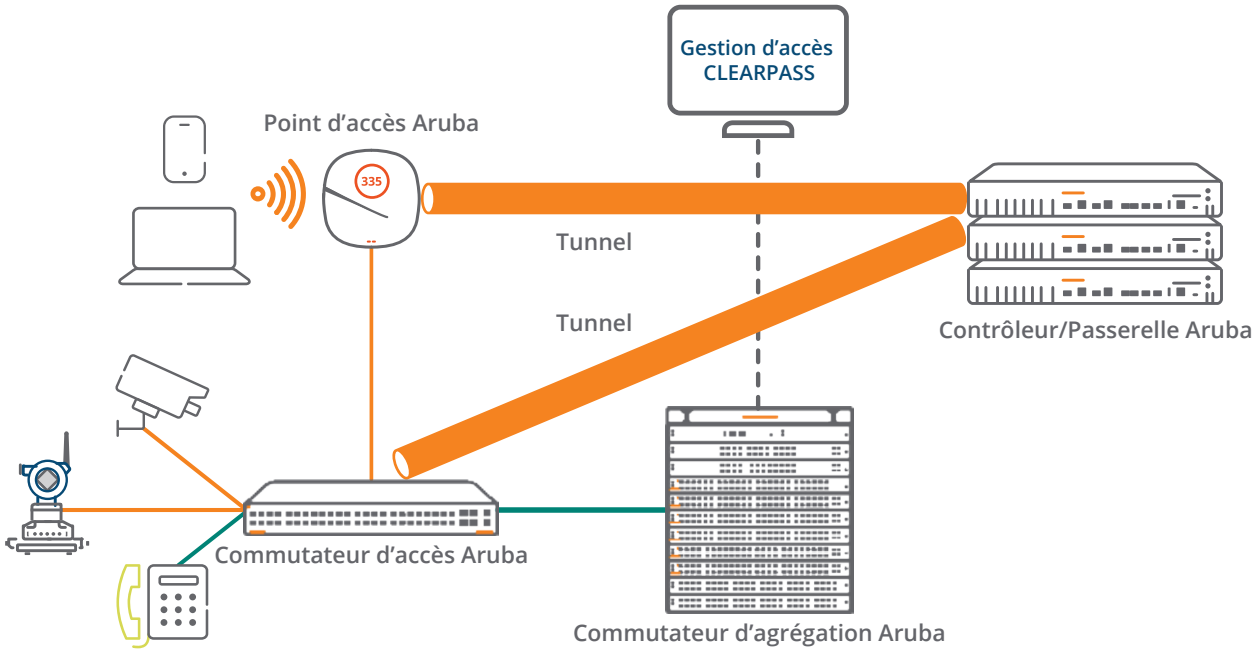
Source : Gartner (janvier 2017)

devraient ensuite assurer une expérience sans faille tout en maintenant la visibilité et la gestion de tous les équipements sur un réseau sécurisé.

Qu'il s'agisse d'un éclairage intelligent, de caméras de sécurité ou de lecteurs de badges, les devices IoT sont rapidement déployés dans tous les réseaux de toutes tailles. Cette nouvelle connectivité réseau apporte de nombreux avantages intéressants, mais elle expose également le réseau à des risques de sécurité. En effet, ces appareils entrent sur les même chemins d'accès que les données stratégiques sensibles, à savoir financières, médicales et commerciales. Ces appareils disposent rarement d'une solide sécurité intégrée et manquent également d'authentification robuste. Les mots de passe sont stockés en texte clair, ils manquent de demandeurs sécurisés, et sont souvent situés physiquement dans des espaces publics non sécurisés, ce qui ouvre la porte à des brèches dans le réseau.

EXTENSION DES INNOVATIONS WLAN À LA COMMUTATION

La segmentation dynamique étend la gestion sécurisée des politiques d'Aruba et les fonctionnalités d'application des



La segmentation dynamique, un élément essentiel de l'Experience Edge

politiques WLAN pour simplifier et sécuriser l'accès au réseau filaire. Une telle fonctionnalité se traduit par la possibilité d'assigner aux appareils clients filaires des politiques basées sur le port ou le rôle de l'utilisateur. Une solution idéale car le nombre des devices IoT devrait atteindre 20 milliards d'ici 2020. Les commutateurs réseau Aruba, désormais couverts par ClearPass pour la gestion des politiques et les contrôleurs de mobilité pour leur application, jouent un rôle clé dans l'unification de l'accès réseau.

Politiques basées sur des rôles

En mettant en œuvre la segmentation dynamique, il est possible de prendre des décisions en matière de politique basée sur des rôles et d'accorder des droits d'accès en fonction du type d'appareil, de l'application utilisée, et même de l'emplacement de l'utilisateur ou de l'appareil. Utilisées à l'origine pour répondre à la sécurité sans fil, les politiques basées sur les rôles segmentaient le trafic réseau par type d'utilisateur (employé, invité ou sous-traitant) tout en simplifiant considérablement la gestion du réseau en supprimant les configurations de réseau complexes et statiques. Cette puissante fonctionnalité a rationalisé les workflows informatiques tels que la gestion des accès et des stratégies BYOD et a amélioré les performances des applications.

En étendant la gestion dynamique des politiques basée sur les rôles dans l'ensemble des points d'accès sans fil et des commutateurs filaires, on obtient une solution fondamentalement simple, sécurisée mais différente, pour gérer et appliquer les politiques de mobilité, d'IoT et du cloud. Les passerelles/contrôleurs de mobilité d'Aruba qui appliquent les définitions des politique ClearPass sont désormais en mesure de comprendre et d'utiliser les rôles de manière dynamique. Cette fonctionnalité élimine la tâche fastidieuse et sujette à l'erreur de gestion des VLAN, ACL et des sous-réseaux complexes et statiques en attribuant des politiques de manière dynamique.

Segmentation de couche 4-7

La deuxième fonctionnalité fondamentale exploitée par les commutateurs Aruba est la segmentation. L'architecture WLAN Aruba maintient le trafic sécurisé et séparé grâce l'utilisation de tunnels entre les points d'accès et un contrôleur ou une passerelle. Cette segmentation basée sur les tunnels fournit une sécurité semblable à l'inspection de pare-feu du trafic à haut risque, grâce à l'utilisation du

La segmentation dynamique simplifie et sécurise les réseaux filaires et sans fil en définissant le contrôleur de mobilité comme un moteur d'application d'une politique unifiée. Le trafic provenant d'un point d'accès ou d'un commutateur est incorporé dans des tunnels GRE pour une inspection par le pare-feu d'exécution dynamique des stratégies (PEF).

pare-feu d'exécution dynamique des stratégies (PEF) d'Aruba. Le PEF assure un contexte granulaire (utilisateur, appareil, application, emplacement), et réduit la nécessité de pare-feu coûteux pour la première ligne d'interrogation et de défense. Avec des politiques contextuelles basées sur les identités, le type d'appareil et l'emplacement, vous pouvez satisfaire les besoins de différents groupes d'utilisateurs avec une configuration réseau unique, les flux de trafic s'adaptant simplement aux rôles assignés.

En utilisant cette architecture de tunneling WLAN, les commutateurs Aruba peuvent désormais fournir une approche de segmentation basée sur les rôles par rapport à l'utilisation traditionnelle, plus manuelle des VLAN locaux. Il s'agit d'une solution idéale pour les devices IoT non fiables ou pour la visibilité des applications, étant donné que les commutateurs Aruba peuvent désormais tunnéliser de manière dynamique le trafic sélectionné vers le contrôleur pour une inspection approfondie des paquets et l'authentification des appareils, tout comme un point d'accès. Par exemple, une caméra de sécurité peut se voir attribuer un rôle avec des droits qui limitent son trafic à un serveur spécifique uniquement, ce qui réduit le risque d'une entrée malveillante dans d'autres sections du réseau.

Cette nouvelle fonctionnalité de segmentation améliore le niveau de sécurité avec le tunneling, qui peut être configuré pour un tunneling basé sur des ports (PBT) avec l'ensemble de l'authentification réalisée sur le contrôleur ou pour un tunneling basé sur les utilisateurs (UBT) avec l'ensemble de l'authentification effectuée sur le commutateur. Cette segmentation fonctionnant comme un overlay, elle peut co-exister avec des implémentations VLAN en utilisant des tunnels sécurisés dans des zones sélectionnées sans remplacement intégral de l'ensemble de l'infrastructure de commutation.

LES INGRÉDIENTS DE LA SOLUTION

Points d'accès sans fil Aruba

Une performance Wi-Fi 802.11ac et 802.11ax Wi-Fi qui répond aux besoins de tous les environnements. L'intelligence IA intégrée et les services de localisation offrent à l'informatique l'automatisation et la visibilité nécessaire pour fournir une expérience optimale, à la fois pour les utilisateurs et les appareils IoT.

Commutateurs réseau Aruba

Créez une base sans fil-filaire intégrée, qui offre une évolutivité, une sécurité et des performances élevées aux réseaux de campus et de succursales. La segmentation dynamique offre aux équipes informatiques un moyen simple et unique d'appliquer des politiques, d'utiliser des services avancés et de segmenter de manière sécurisée le trafic utilisateur et IoT partout dans le réseau via des tunnels. Ceux-ci peuvent être configurés comme des tunnels basés sur des ports (PBT) avec authentification effectuée sur le contrôleur ou des tunnels basés sur des utilisateurs (UBT) avec authentification effectuée au niveau du commutateur Aruba.

Passerelles et contrôleurs de mobilité Aruba

Les contrôleurs ou passerelles, éléments essentiels de la solution, agissent comme un agent d'application de la politique pour le trafic filaire et sans fil. Le contrôleur de mobilité Aruba (exécutant AOS 8.1 ou un version ultérieure) permet aux équipes informatiques de tirer parti de l'application des politiques, des contrats de bande passante et d'autres restrictions de trafic. Dans un environnement de succursale, la passerelle de succursale gérée par Aruba Central joue ce rôle. Le pare-feu d'application de la politique sert de technologie réseau sous-jacente pour prendre en charge ces deux environnements.

Aruba ClearPass Policy Manager avec profilage

Gérez et appliquez de manière centralisée les politiques d'accès au réseau pour le contrôle d'accès sans fil et filaire. Ses principales fonctions sont le profilage des appareils, l'authentification, l'autorisation et l'application des politiques. En utilisant ClearPass, une fois le rôle et les privilèges définis, ils suivent l'utilisateur ou l'appareil dans l'ensemble de l'accès filaire et sans fil. Ainsi, si l'utilisateur bascule sur un appareil inconnu ou s'il se trouve sur un réseau non sécurisé, la politique modifie automatiquement les privilèges d'autorisation. Les rôles utilisateur téléchargeables (DUR) sont configurés sur ClearPass, ce qui élimine la nécessité de définir des rôles ou des politiques sur un commutateur.

RÉCAPITULATIF

Pour mieux gérer la mobilité stratégique pour l'entreprise et l'émergence des exigences en matière de connectivité IoT, la solution innovante de segmentation dynamique d'Aruba simplifie les opérations informatiques et améliore la sécurité, en appliquant de manière dynamique les politiques unifiées et en mettant en œuvre des services avancés dans l'ensemble du réseau. Cela garantit une distribution transparente des politiques d'accès et de sécurité appropriées, leur application automatique et leur mise en œuvre indépendante pour tous les utilisateurs et les appareils filaires et sans fil.

SO_DynamicSegmentation_SK_092419 a00058593fre