



Réseau orienté utilisateurs d'Aruba pour le secteur public

Quelle est votre vision ? Offrir un accès sans fil conforme à la norme FIPS 140-2 à vos utilisateurs ? Renforcer la productivité des utilisateurs grâce à un accès sans fil, du bureau à la salle de réunion, des centres de contact à la brigade d'intervention ?

Aruba a mis au point une nouvelle approche révolutionnaire pour vous aider à atteindre votre objectif. Les réseaux centrés sur l'utilisateur d'Aruba intègrent des réseaux locaux sans fil adaptatifs, une sécurité basée sur l'identité et des services de continuité des applications ; tout cela au sein d'un système cohésif à hautes performances destiné aux campus d'entreprises, aux immeubles de bureaux, aux succursales, aux espaces extérieurs et aux télétravailleurs. Il en résulte un réseau centralisé rassemblant les applications professionnelles sur le réseau local, le réseau étendu et Internet. Les utilisateurs sont donc plus productifs et la sécurité n'est pas compromise. A la différence des autres solutions, les réseaux orientés utilisateurs d'Aruba exploitent les réseaux existants afin de préserver l'investissement initial et d'éviter toute modification susceptible d'en perturber le fonctionnement.

Fonctionnalités propres à Aruba

SÉCURITÉ INTÉGRÉE POUR LE RESPECT DES NORMES

Le réseau centré sur l'utilisateur d'Aruba constitue une solution mobile sécurisée pour le personnel administratif. La plate-forme Aruba est certifiée conforme aux critères suivants :

- Chiffrement FIPS 140-2 de niveau 2
- Respect des normes 802.11i
- Respect de la directive DOD 8100.2
- Sécurité de bout en bout sur un canal assuré
- Détection et prévention des intrusions
- Certification « Common Criteria »
- Identification 802.1x (dont Common Access Card)
- Certification JITC

SÉCURITÉ BASÉE SUR L'IDENTITÉ – CONTRÔLE D'ACCÈS PAR NIVEAU D'HABILITATION

En entreprise, les applications mobiles exigent que le réseau puisse suivre l'utilisateur dans ses déplacements. Les méthodes de contrôle d'accès traditionnelles reposent sur le point d'entrée, ce qui est contraire à l'essence même de la mobilité. Le contrôle d'accès mobile nécessite des

informations sur l'utilisateur lors de la définition des stratégies : son rôle au sein de l'organisation, son habilitation de sécurité, le type de périphérique utilisé, sa position, l'heure et même son comportement en ligne. Les différents groupes d'employés, sous-traitants et invités en provenance d'autres sous-organisations devront disposer de niveaux d'accès distincts, voire de méthodes d'identification propres (ex. : 802.1x, VPN ou portail captif). Enfin, il faut atteindre tous ces objectifs sans compliquer davantage le réseau. Ils doivent facilement s'intégrer aux structures en place telles que RADIUS, LDAP ou Active Directory.

Les contrôleurs de mobilité et les points d'accès d'Aruba sont déployés de manière stratégique afin d'atteindre ces objectifs. A la différence des autres systèmes qui associent les stratégies à des SSID/VLAN spécifiques en vue de sécuriser et segmenter un réseau, Aruba met en œuvre un pare-feu dynamique certifié ICASA permettant la définition de profils distincts et leur application à chaque utilisateur, niveau d'habilitation et périphérique. Le pare-feu permet également la constitution de listes noires reprenant les clients qui ne respectent pas les règles. Il pourra ainsi mettre fin à une session et interdire tout accès au réseau si nécessaire. Les réseaux orientés utilisateurs

Avantages :

- **Sécurité basée sur l'identité :** les systèmes de sécurité suivent les utilisateurs au fil de leurs déplacements sur les réseaux LAN, WAN ou Internet
- **Gestion centralisée :** configuration, surveillance et dépannage aisés grâce au contrôle centralisé
- **Compatibilité avec les applications :** système optimisé pour la prise en charge sans fil des données, de la voix et de la vidéo sur un réseau convergent
- **Réseau flexible et évolutif :** le déploiement au-dessus de l'architecture existante évite le remaniement complet des réseaux et leurs mises à niveau
- **A l'épreuve du temps :** logiciels permettant une mise à niveau vers les technologies 802.11n, le contrôle d'accès au réseau, le maillage Mesh et la convergence fixe/mobile

d'Aruba viennent compléter les réseaux existants et s'intègrent aux structures de répertoires en place.

GESTION CENTRALISÉE ET DÉPANNAGE

Le déploiement et la gestion d'un réseau de type entreprise peuvent s'avérer fastidieux si ces opérations ne sont pas correctement réalisées. La gestion centralisée du réseau et des stratégies proposée par Aruba est conçue pour permettre un déploiement et un contrôle aisés. Grâce à la gestion centralisée d'Aruba, les données de configuration sont diffusées automatiquement et en toute sécurité sur le réseau, via les points d'accès et les contrôleurs, à distance ou localement. Une seule interface est prévue pour la mise en œuvre et la protection des stratégies sous-jacentes garantissant l'intégrité, la sécurité et le fonctionnement du réseau dans son intégralité. La fonction de contrôle centralisé prend également en compte les profils de performances utilisés par les points d'accès d'Aruba en vue d'en optimiser leur fonctionnement et assurer la prise en charge des applications stratégiques.

Aruba permet la capture des paquets à distance de sorte que les responsables informatiques puissent effectuer un dépannage sur les sites situés à l'autre bout de la ville comme à l'autre bout du pays. De plus, Aruba offre un affichage dynamique intégral de l'environnement RF de chaque bâtiment, base ou site sur le réseau. L'administrateur réseau peut effectuer toutes les opérations de maintenance et les mises à niveau à partir d'un seul et même lieu. Il sera par ailleurs averti en cas d'intrusion ou d'événement de sécurité dès leur apparition.

COMPATIBILITÉ AVEC LES APPLICATIONS

Les services voix et vidéo sur IP sont de plus en plus fréquents dans les entreprises grâce à l'introduction des téléphones mobiles équipés de la technologie Wi-Fi et à l'engouement pour les communications multimédias. Pour proposer des services vocaux par exemple, le réseau doit permettre l'installation d'un système de qualité de service sans fil et câblé. Il doit garantir la sécurité des appels vocaux et ajuster

les modèles de trafic afin d'assurer une voix de qualité. La solution Aruba est parfaitement compatible avec la voix puisqu'elle exploite un pare-feu applicatif afin d'en sécuriser le flux et lui accorder la priorité le cas échéant. Étant donné que la qualité de service et la sécurité demeurent centralisées, le suivi des utilisateurs vocaux au fil de leurs déplacements sur le réseau est aisé. La priorité est accordée au trafic vocal grâce aux balises de qualité de service 802.1p et DSCP. Le système détecte automatiquement les protocoles vocaux les plus répandus (SIP, SVC et SCCP) et accorde la priorité au trafic vocal. Une priorisation supplémentaire peut être effectuée grâce au système Call Admission Control (contrôle d'admission d'appels voix, CAC). Le système CAC définit une limite pour les appels vocaux par point d'accès. En présence d'un nombre d'appels supérieur, ceux-ci sont automatiquement transférés vers les points d'accès voisins afin d'assurer une qualité optimale de la voix.

ÉVOLUTIF ET À L'ÉPREUVE DU TEMPS

Le réseau WLAN doit répondre aux exigences actuelles de l'entreprise, mais il doit aussi permettre son évolution et autoriser l'ajout de périphériques et d'applications mobiles. Le nombre d'utilisateurs et de périphériques, le chargement instantané des applications pendant les heures de pointe et la mobilité des utilisateurs sur les réseaux LAN, WAN ou sur Internet constituent les principaux écueils d'un tel système. Aruba Networks innove et propose une solution permettant d'automatiser la configuration RF, de décharger les serveurs AAA et de faire évoluer les VLAN afin de faire face à une utilisation évolutive. De plus, Aruba propose des plates-formes puissantes, évolutives et dédiées offrant un débit tel qu'il permet d'exploiter réellement les applications existantes, l'infrastructure informatique et les clients standard en place. Conçus pour répondre aux exigences des clients d'aujourd'hui et de demain, la plupart des produits Aruba exploitent une structure logicielle modulaire et évolutive pouvant être améliorée au fil du temps selon la mise à disposition de nouvelles fonctions.

Solution Aruba Networks pour le secteur public

La solution Aruba se compose de quelques éléments essentiels (les points d'accès légers, les contrôleurs de mobilité centraux et leurs modules logiciels), auxquels viennent s'ajouter certains composants facultatifs comme un système d'analyse de gestion et des dispositifs de prévention des menaces. Les points d'accès assurent une connectivité sans fil sécurisée aux périphériques et se connectent sur

des systèmes de réseaux LAN/WAN existants de manière à prendre en charge l'ensemble du trafic du réseau local sans fil (via un tunnel GRE ou IPsec) vers un contrôleur de mobilité installé dans le centre de données. La configuration, la gestion, la continuité de service des applications et la sécurité sont centralisées sur le contrôleur de mobilité. Grâce aux modules de sécurité pour les contrôleurs de mobilité, Aruba apporte la

FICHE MÉTIER

Solution pour le secteur public

sécurité nécessaire et garantit le respect des normes.

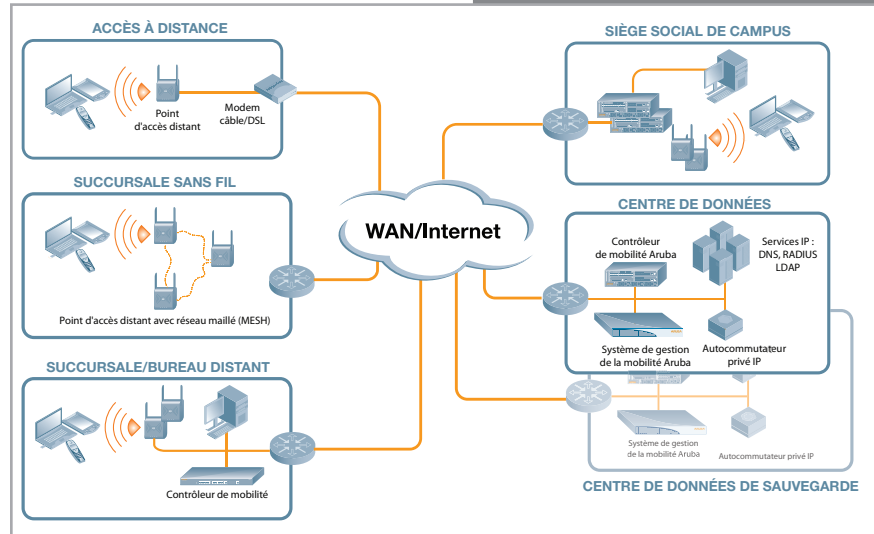
Vous trouverez ci-dessous la présentation d'un réseau sans fil destiné aux entreprises dotées de services informatiques centralisés :

Centre de données : au moins un contrôleur de mobilité est installé dans le centre de données. Il peut être utilisé comme point de configuration et de gestion pour tout le réseau. Ces contrôleurs peuvent également servir de terminaisons pour les points d'accès permettant la liaison sans fil au sein du siège central et les points d'accès distants exploités par les télétravailleurs et les bureaux ad hoc de taille modeste. Le contrôleur principal prend en charge jusqu'à 500 contrôleurs distants. Il peut également prendre le relais d'un contrôleur installé sur un site distant en cas de panne. Dans le cas des déploiements de plus grande envergure, plusieurs contrôleurs principaux peuvent se répartir la gestion des contrôleurs locaux et des points d'accès sur les sites distants. Le système de gestion de la mobilité (Airwave) peut être utilisé comme interface de gestion et de configuration.

Moyennes et grandes entreprises : un contrôleur de mobilité Aruba (contrôleur local) différent est installé selon le nombre de points d'accès requis sur chaque site. Tous les modèles Aruba exploitent le même logiciel et disposent des mêmes fonctions. Seul le nombre de points d'accès pris en charge varie (de 4 à 512 points d'accès). Chaque contrôleur local obtient sa configuration du contrôleur principal. La continuité de service des applications et les niveaux de sécurité sont assurés au niveau de l'utilisateur par le contrôleur local. Différents profils sont affectés en fonction de stratégies de groupes définies dans le système d'identification. Il est également possible de rediriger les invités vers la zone démilitarisée. Les contrôleurs locaux offrent également un système de protection sans fil contre les intrusions. Le cas échéant, l'activation des services d'identification et/ou des requêtes d'accès direct au centre de données est possible. Chaque contrôleur local calibre automatiquement la couverture RF afin d'optimiser les performances et d'éviter les trous de couverture. De plus, pour permettre une couverture sans fil dans les zones où le câblage s'avérerait trop difficile ou trop coûteux, les points d'accès Aruba peuvent assurer la liaison par Wi-Fi grâce au réseau maillé d'entreprise sécurisé (MESH).

Utilisateurs distants et petits bureaux : des points d'accès distants autonomes (Remote AP) constituent une solution efficace pour assurer une liaison

sécurisée et une gestion centralisée des sites ne nécessitant qu'un ou deux points d'accès. Ces derniers peuvent être directement connectés par Ethernet à un réseau Internet public/privé ou au réseau LAN. Les points d'accès distants détectent automatiquement le contrôleur principal. Ils établissent un tunnel VPN



sécurisé vers le centre de données et élargissent la liaison sans fil à l'utilisateur. Le trafic des applications peut être acheminé vers le centre de données ou localement.

SÉCURITÉ DE BOUT EN BOUT

Aruba Networks permet un chiffrement programmable pour une transition aisée vers les systèmes AES-CCM/802.11i et AES-CBC à 256 bits, aussi bien pour les périphériques câblés que sans fil, sans recours à la mise à niveau du matériel. Associé à un système de défense en profondeur, ce dispositif offre une protection intégrée à plusieurs niveaux pour les transmissions sans fil ou par câble, pour le réseau et l'utilisateur.

Aruba est allé encore plus loin en matière d'innovation, en équipant son logiciel FIPS d'un déléstage EAP. Grâce au déléstage EAP, les opérations d'identification et de gestion de clé ont lieu dans un périmètre chiffré sécurisé, défini par le contrôleur de mobilité. Les données ne sont pas transmises en clair ou à l'aide d'algorithmes faibles depuis le contrôleur de mobilité vers le serveur RADIUS externe.

Aruba renforce également les serveurs RADIUS EAP grâce à une fonction RADIUS-sur-IPsec recommandée par le document RFC 3579. Il s'agit donc de la première solution FIPS intégrale pour un déploiement au-dessus d'une structure existante.



WWW.ARUBANETWORKS.COM

1322 Crossman Avenue, Sunnyvale, CA 94089 | Tél. +1 408.227.4500 | Fax. +1 408.227.4550