

White Paper |



## **Virtual Branch Networking (VBN) 2.0 et l'émergence de succursales basées sur Internet**

**Juillet 2010**

**ARUBA**<sup>®</sup>  
**ARUBA**  
networks

---

## Table of Contents

<i>Virtual Branch Networking (VBN) 2.0 et l'émergence de succursales basées sur Internet</i>	
<i>Le défi.....</i>	<i>2</i>
<i>Aruba Networks® présente sa solution Virtual Branch Networking (VBN) 2.0 basée sur Internet ...</i>	<i>3</i>
<i>L'architecture VBN 2.0 et ses composants.....</i>	<i>3</i>
Le point d'accès distant .....	4
Le contrôleur de mobilité .....	5
La plate-forme de gestion AirWave.....	6
Service de sécurité du contenu (CSS) .....	7
<i>Présentation de la solution VBN 2.0 .....</i>	<i>8</i>
Mise en réseau d'accès distant avec la solution VBN 2.0.....	8
Modes de réacheminement et de fonctionnement.....	8
Options de chiffrement locales et centralisées .....	9
Fonctionnalité WLAN pour accès distant.....	9
Des performances multimédias garanties avec la qualité de service (QoS) .....	10
La sécurité dans un réseau VBN 2.0.....	10
Pérennité des sites distants.....	11
Évolutivité .....	11
<i>Conclusion.....</i>	<i>12</i>

---

## Le défi

Au cours des dix dernières années, les méthodes de travail ont considérablement évolué et ce changement a eu une incidence majeure sur les entreprises d'informatique.

Le premier élément ayant contribué à changer la donne est la mobilité. Grâce à elle, l'utilisateur final est désormais libre de travailler n'importe où et n'importe quand, améliorant ainsi la productivité. En 2009, les ventes d'ordinateurs portables ont, pour la première fois dans l'histoire de l'informatique, dépassé celle des ordinateurs de bureau.

Les travailleurs ont commencé à se disperser. Avec l'incursion dans de nouveaux marchés géographiques, de multiples succursales ont vu le jour, tandis que des myriades de bureaux à domicile et de télétravailleurs ont fait leur apparition. Les entreprises d'informatique qui fournissent leurs services à ces sites distants ont très vite compris qu'une succursale ne comptant qu'un seul employé présentait les mêmes besoins qu'un bureau de 100 personnes.

Dans le même temps, les serveurs informatiques ont été rassemblés en un nombre réduit de centres de données, tandis que les applications ont été externalisées, donnant ainsi naissance aux concepts de virtualisation et de cloud computing (informatique via Internet). Les applications, qui semblent exécutées en local pour les utilisateurs, sont en réalité distribuées sur Internet via des centres de données dispersés dans le monde entier. En outre, les travailleurs avaient besoin d'un accès sécurisé et fiable à ces applications, qu'ils se trouvent au siège, dans des succursales, à leur domicile ou en déplacement.

La dernière évolution significative est la mise à disposition de connexions à large bande rapides, fiables et économiques. Aujourd'hui, il suffit de quelques jours, voire de quelques heures, pour obtenir une connexion DSL, câblée ou 3G. La disponibilité étendue de la technologie à large bande a permis de relier, de manière rentable, un nombre croissant de succursales, de télétravailleurs, de points de vente et d'agents à domicile aux ressources informatiques d'une entreprise.

Malheureusement, le déploiement d'un équipement informatique identique dans de petites succursales et des bureaux à domicile n'est pas aussi avantageux que dans une structure de 100 personnes. En outre, la gestion de cet équipement informatique (routeurs, commutateurs, réseaux locaux sans fil, serveurs locaux et appareils d'optimisation des réseaux WAN) dans toutes les succursales augmente considérablement les frais d'exploitation. Par conséquent, la protection contre les menaces et d'autres services réseau sont souvent sacrifiés dans les petites structures.

Pour tenter de répondre à ce problème, certains fournisseurs réseau ont créé des solutions de type *succursale prête à l'emploi*, qui rassemblent de nombreuses fonctions dans un seul et même produit. Bien que ces solutions constituent une alternative plus économique à l'utilisation de nombreux appareils autonomes, leur coût reste prohibitif pour la plupart des petites succursales. Par ailleurs, les entreprises d'informatique doivent créer, gérer et assurer la maintenance de configurations distinctes sur chaque site.

Les petites succursales ont besoin d'une architecture entièrement nouvelle pour bénéficier d'un service informatique fiable et de grande qualité. Elles requièrent un périphérique compact, simple à utiliser et économique, faisant l'objet d'une gestion centralisée à partir d'un centre de données. Les services réseau de calcul intensif, tels que la sécurité du contenu, sont désormais fournis sur Internet.

## Aruba Networks® présente sa solution Virtual Branch Networking (VBN) 2.0 basée sur Internet

La solution VBN 2.0 d'Aruba Networks® offre un véritable réseau d'entreprise aux petites structures. Elle permet de réduire les coûts d'investissement jusqu'à 60 %, ainsi que les frais d'exploitation jusqu'à 75 %, par rapport aux routeurs traditionnellement utilisés dans les succursales. Grâce à la migration des services réseau et de sécurité sur Internet, la solution VBN 2.0 remplace les routeurs coûteux par un périphérique simple à utiliser, compact et économique, faisant l'objet d'une gestion centralisée : celui-ci est connu sous le nom de « point d'accès distant ».

La configuration et la gestion des services réseau d'entreprise (notamment les stratégies d'accès utilisateur, les SSID, ainsi que la surveillance et la visibilité de l'administration et du réseau) sont centralisées à partir du centre de données de l'entreprise. Les économies réalisées ne s'arrêtent pas là : il est possible d'utiliser dans les succursales des connexions à large bande au lieu de connexions WAN privées, plus coûteuses.

L'architecture VBN 2.0 englobe à la fois un accès câblé et un accès distant sans fil. Elle peut s'adapter à toutes les structures, des grandes succursales aux télétravailleurs, en passant par les travailleurs itinérants. Elle s'intègre également en toute transparence à une administration centralisée, afin de réduire les frais d'exploitation. Grâce à la solution VBN 2.0, les services de sécurité du contenu sont désormais disponibles sur Internet. Aucun investissement ni aucun équipement sur site n'est nécessaire pour la prise en charge de ces services. Enfin, la solution VBN 2.0 garantit un service de grande qualité aux employés des succursales, ainsi qu'un accès sécurisé aux ressources disponibles au siège de l'entreprise.

### L'architecture VBN 2.0 et ses composants

L'architecture VBN 2.0 inclut trois composants. Tout d'abord, les contrôleurs de mobilité situés dans le centre de données de l'entreprise virtualisent et contrôlent le réseau distant, rassemblant ainsi les fonctionnalités de la succursale dans un emplacement centralisé où les applications sont hébergées.

Ensuite, les points d'accès distants étendent les réseaux de la succursale à partir du centre de données de l'entreprise à l'aide de tunnels VPN. Grâce à la fonction de déploiement automatique, les utilisateurs peuvent installer eux-mêmes les points d'accès distants en toute simplicité sur le site de la succursale, sans recourir à une assistance informatique. Une fois connectés, les points d'accès distants offrent une connexion locale câblée ou sans fil, et localisent l'application de la sécurité et des stratégies liées au trafic.



**Illustration 1. La solution VBN 2.0 et les succursales basées sur Internet.**

Enfin, la plate-forme AirWave unifie la gestion de l'ensemble des utilisateurs et des sites d'accès distants. Le système de gestion comprend des fonctions de contrôle de la configuration, de surveillance et de dépannage. Dans la mesure où le système VBN est basé sur l'identité et repose sur des stratégies, les comptes, les informations d'identification et les rôles sont dérivés des répertoires d'entreprise existants et n'exigent aucune configuration supplémentaire.

Les fonctions réseau étant centralisées et virtualisées, un des principaux avantages de l'architecture VBN réside dans le fait que les points d'accès distants sont des périphériques prêts à l'emploi simples et économiques, permettant un déploiement automatique dans les succursales. Malgré son extrême simplicité, cette solution offre des fonctionnalités et une sécurité répondant aux attentes des professionnels.

Les succursales basées sur Internet virtualisent les configurations de port, de réseau local virtuel, de routeur, de pare-feu, de VPN et de qualité de service (QoS) en un ensemble de stratégies basées sur l'identité. Celles-ci sont définies de façon centralisée, puis étendues à la demande à des périphériques au fur et à mesure que les utilisateurs rejoignent le réseau. Les services utilisant de nombreuses ressources, tels que la sécurité du contenu et la voix, sont placés sur Internet, ce qui permet de réaliser des économies d'échelle et de réduire les coûts. Dans la mesure où ces services ne dépendent plus des périphériques, la durée de vie du matériel s'en trouve prolongée. La mise à niveau des services est réalisée dans le centre de données et sur Internet, et non sur chaque périphérique

L'intégration d'un certain nombre de fonctions au contrôleur de mobilité est essentielle pour obtenir des performances satisfaisantes à un moindre coût. Grâce à l'intégration des fonctionnalités d'authentification, de chiffrement, de pare-feu et de qualité de service (QoS) dans un seul et même périphérique, l'administrateur réseau dispose d'un point de contrôle unique pour les tâches de configuration, de maintenance et de dépannage. Cette organisation permet de réduire les coûts d'investissement initiaux et les frais d'exploitation permanents. Elle offre également une solution qui ne nécessite aucune intervention supplémentaire de l'utilisateur, si ce n'est la spécification des informations d'identification standard. À domicile ou sur un campus, les procédures d'accès au réseau sont identiques.

### Le point d'accès distant



**Illustration 2. Des points d'accès distants simples à utiliser, compacts et économiques, adaptés aux succursales de toutes tailles.**

Côté réseau, le point d'accès distant ressemble à un *client VPN prêt à l'emploi*. Sa fonction de déploiement automatique unique ne nécessite aucune assistance informatique. Il se branche à une connexion réseau de la succursale, obtient automatiquement une adresse et crée un tunnel IPSec vers le contrôleur de mobilité du centre de données. Les points d'accès distants sont parfaitement évolutifs. Ils offrent une solution économique tant aux bureaux à domicile qu'aux succursales de plusieurs utilisateurs.

Côté LAN, le point d'accès distant fournit des options de connectivité câblée ou sans fil à l'utilisateur. Le point d'accès distant intégré offre une sécurité, une gestion et un contrôle de qualité professionnelle à l'aide des technologies utilisées pour les déploiements de réseau local sans fil sur campus. Par ailleurs, il fournit des services

complets de sécurité et de protection contre les intrusions sans fil (WIPS) permettant de contrôler les points d'accès malveillants et les clients mal configurés.

Un pare-feu d'application des stratégies (PEF) est également intégré au point d'accès distant. Il s'agit d'un pare-feu dynamique côté client faisant office de moteur de réacheminement d'accès. Il contrôle la connectivité et la hiérarchisation en fonction des utilisateurs et des stratégies (et non des ports et des sous-réseaux), afin de simplifier la diffusion des services et la mise en place de stratégies de sécurité. Les stratégies appliquées par le pare-feu d'application des stratégies (PEF) du point d'accès distant sont configurées à partir du contrôleur de mobilité central, selon les modèles du réseau.



**Illustration 3. Aruba RAP Functional Diagram**

Il est possible de configurer les points d'accès distants de manière à ce qu'ils déchargent le trafic lié à Internet directement en local, sans passer par le centre de données de l'entreprise. Grâce à la solution VBN 2.0, en plus d'inclure des services basés sur Internet, les points d'accès distants acheminent le trafic lié à Internet vers un service de sécurité du contenu sur le Web.

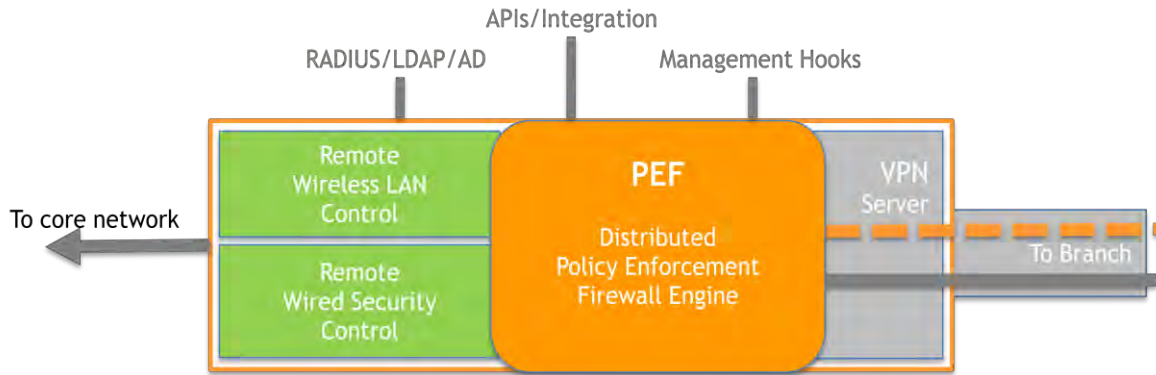
### Le contrôleur de mobilité



**Illustration 4. Le contrôleur Aruba 6000 prend en charge jusqu'à 8 192 points d'accès distants.**

Le contrôleur de mobilité comprend un concentrateur VPN entièrement intégré qui peut servir de terminaison pour les points d'accès distants et qui permet de les gérer. Il inclut également un système de contrôle WLAN complet et centralisé. Cela permet un accès sans fil sécurisé et une analyse du système de détection des intrusions sans fil (WIDS) avancés sur des sites distants, tout en bénéficiant d'un contrôle et d'une visibilité centralisés et en temps réel, semblables à ceux dont vous disposez avec une solution sur campus locale.

Chaque pare-feu d'application des stratégies (PEF) du contrôleur de mobilité fonctionne à la fois comme un point centralisé de définition de stratégie et un point de sécurité secondaire du trafic entrant dans le centre de données depuis des sites distants.



**Illustration 5. Aruba VBN Controller Functional Diagram**

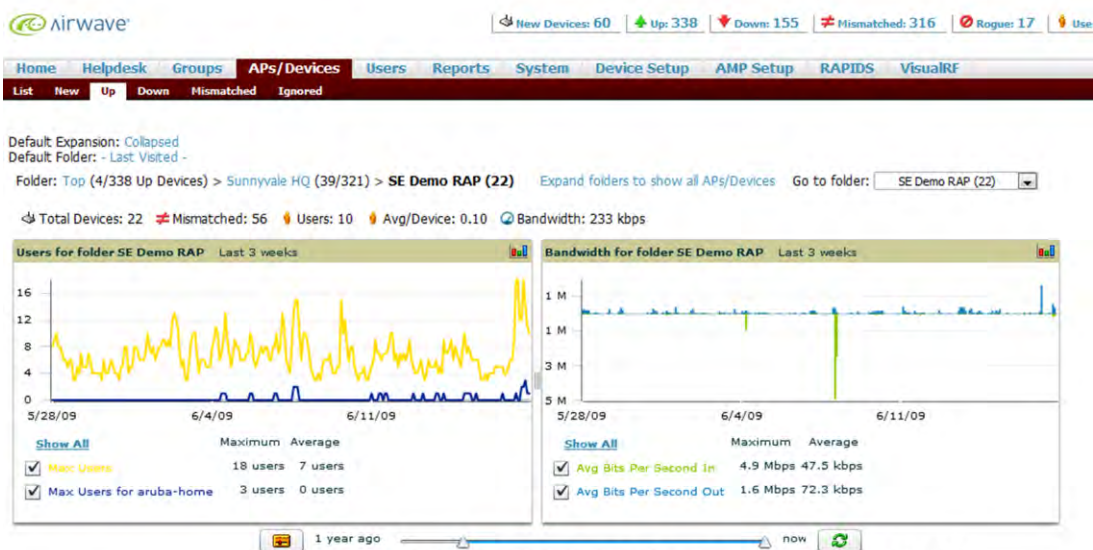
Enfin, ces systèmes disposent d'API et de points d'entrée d'intégration permettant une liaison avec l'infrastructure de clés publiques (PKI) existante, les systèmes de gestion et les autres systèmes de sécurité, tels que RADIUS pour l'application de stratégies d'accès 802.1X.

Les contrôleurs de mobilité sont évolutifs et peuvent assurer la prise en charge de plusieurs milliers de points d'accès et de périphériques distants. Ainsi, plusieurs contrôleurs de mobilité peuvent être reliés à un réseau, pour garantir une répartition optimale du trafic, et gérés de manière centralisée au moyen de stratégies uniformes, afin d'améliorer l'efficacité opérationnelle.

### La plate-forme de gestion AirWave

La plate-forme de gestion AirWave (qui fait partie de l'AirWave 7™ Wireless Management Suite) constitue un panneau unique destiné à la gestion de tous les accès distants au réseau d'entreprise distribué. Elle permet de gérer les utilisateurs et facilite leur configuration via un modèle d'une seule page.

Une fois les configurations terminées, AirWave permet de suivre les utilisateurs chaque fois qu'ils accèdent au réseau et fournit des informations essentielles concernant la génération de rapports, l'audit et le dépannage. Les différentes vues utilisateur offrent des outils de dépannage utiles tant au centre d'assistance qu'aux ingénieurs de support.



**Illustration 6. AirWave RAP Monitoring (partial screen)**

En plus d'assurer la gestion des utilisateurs, la plate-forme AirWave permet de gérer l'infrastructure distante dans son intégralité. Elle est compatible avec les équipements câblés et sans fil de plusieurs fournisseurs, ce qui permet d'unifier la gestion des points d'accès et des commutateurs hérités, ainsi que de l'équipement VBN.

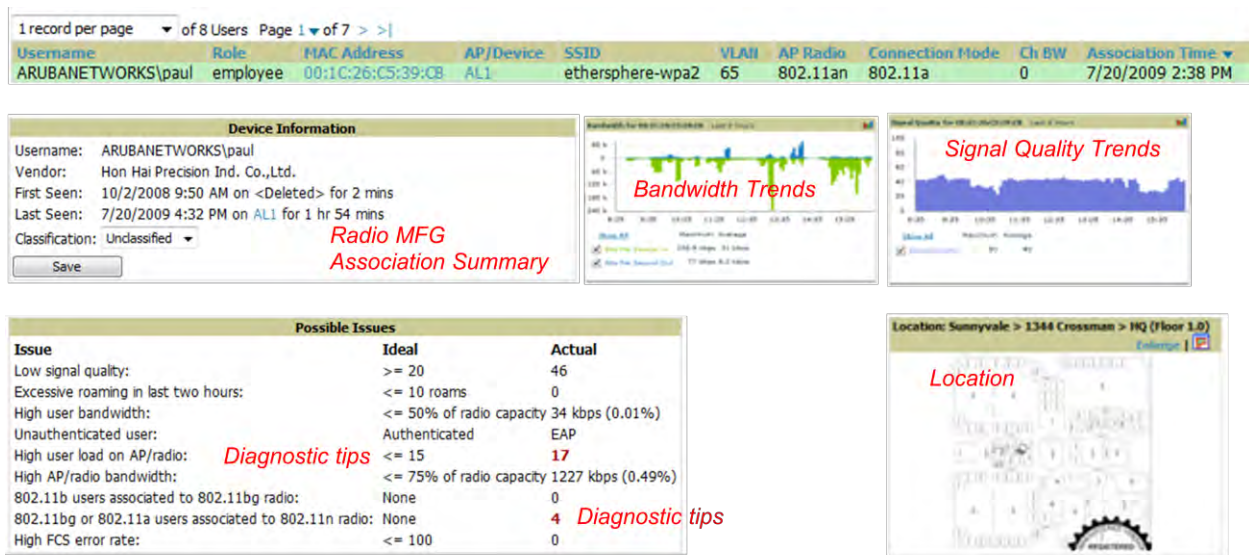


Illustration 7. AirWave User Monitoring (partial screen)

### Service de sécurité du contenu (CSS)

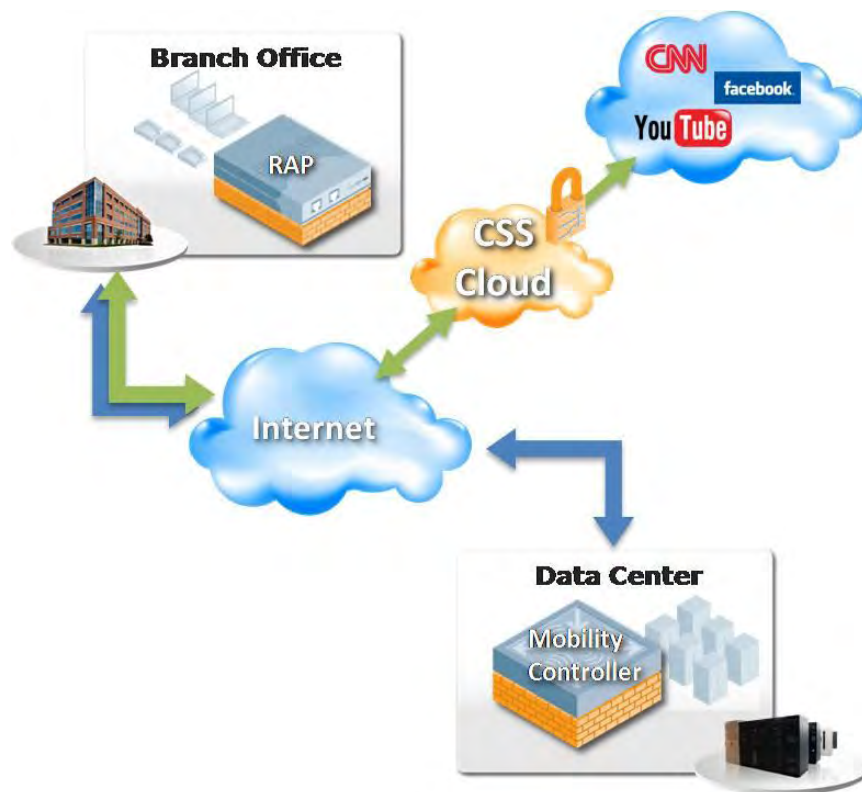
La plupart des succursales et des télétravailleurs disposent aujourd'hui d'un accès rapide à un tunnel Internet via la mise en réseau de tunnels séparés. Grâce à la séparation des tunnels, les utilisateurs peuvent se servir à la fois d'un client VPN pour accéder en toute sécurité aux ressources réseau de l'entreprise et d'une connexion directe à Internet pour une navigation classique. Cette séparation permet d'optimiser les performances tout en déchargeant le canal de communication WAN de l'entreprise.

Bien que des pare-feu soient déployés pour chaque tunnel dans l'architecture VBN 2.0 afin d'empêcher les fuites de trafic du Web vers l'entreprise, les connexions à Internet (notamment la navigation Web et les services de messagerie hébergés sur Internet) risquent d'exposer l'ordinateur d'un employé à des logiciels malveillants, des chevaux de Troie et des virus.

Les utilisateurs sur campus disposent généralement d'une protection assurée par les services de filtrage du contenu de l'entreprise, mais le coût prohibitif de ces services empêche leur déploiement en local au sein des petites succursales. Un appareil de filtrage du contenu doit donc être installé sur site ou l'ensemble du trafic doit être redirigé vers le centre de données de l'entreprise afin d'y être filtré, ce qui annule les avantages de l'accès par tunnels séparés.

Le service de sécurité du contenu (CSS) basé sur Internet d'Aruba, qui est une autre fonction essentielle de la solution VBN 2.0, résout ce problème auquel doivent faire face les succursales en proposant une sécurité du contenu haut débit et à faible latence, dotée de fonctions centralisées de gestion et de génération de rapports.

Tirant parti des centres de données du monde entier, le service CSS assure une protection complète qui comprend le filtrage avancé d'URL, le contrôle de pair-à-pair, un antivirus, un logiciel anti-virus, la détection de réseaux fantômes et la prévention contre la perte des données (DLP). Des journaux Web haut débit inclus dans le service CSS offrent par ailleurs une méthode flexible et puissante pour visualiser les tendances de l'activité Internet dans son ensemble et par utilisateur.



*Illustration 9. Le service de sécurité du contenu (CSS) de la solution VBN 2.0.*

## Présentation de la solution VBN 2.0

### Mise en réseau d'accès distant avec la solution VBN 2.0

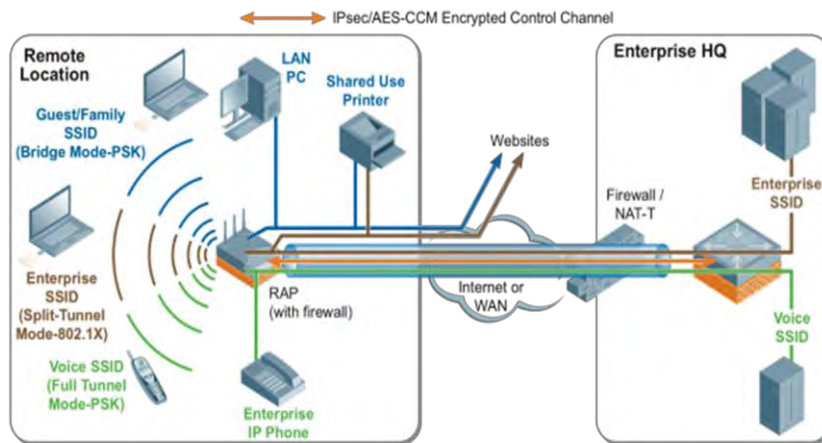
Le point d'accès distant est conçu pour être envoyé aux sites distants dans son emballage d'origine afin d'y être installé par des employés sans formation technique. Grâce à sa fonction de déploiement automatique, aucune intervention du service informatique n'est nécessaire sur le site distant. Le processus d'installation est simplifié à l'extrême : l'utilisateur doit connecter le point d'accès distant à un routeur WAN ou Internet au sein de la succursale ou à son domicile ; il doit ensuite brancher son ordinateur au port Ethernet du point d'accès distant et, enfin, connecter le câble d'alimentation.

L'utilisateur est ensuite invité à saisir l'adresse Internet du contrôleur de mobilité de l'entreprise. Une fois cette opération terminée, le point d'accès distant détecte automatiquement le contrôleur de mobilité, puis il authentifie et configure un tunnel IPSec pour le trafic de contrôle. Aucune intervention supplémentaire n'est nécessaire sur le site distant. Toutes les informations de configuration sont téléchargées via le site central.

### Modes de réacheminement et de fonctionnement : un trafic centralisé, des ponts locaux et des tunnels séparés

Le trafic SSID par tunnel sur un point d'accès distant est destiné au centre de données de l'entreprise. Il est chiffré de bout en bout à l'aide de l'algorithme AES et relié au point d'accès distant via l'encapsulation IPSec.

Il arrive toutefois que les travailleurs des succursales et des bureaux à domicile disposent d'un certain nombre de serveurs, d'imprimantes et d'autres périphériques locaux qu'ils souhaitent mettre en réseau via le point d'accès distant. Au lieu de relier ce trafic au centre de données et de renvoyer le trajet de liaison, ce qui entraîne des retards et consomme de la bande passante WAN, la solution VBN 2.0 permet le pontage de ce trafic en local.



**Illustration 10. VBN Forwarding and Operating Modes**

La séparation des tunnels est gérée directement au niveau du point d'accès distant, afin de décharger le centre de données de l'entreprise et d'améliorer les performances. Comme indiqué précédemment, la séparation des tunnels peut parfois exposer l'ordinateur de l'utilisateur à des logiciels malveillants, des chevaux de Troie et des virus. Pour prévenir une telle situation, le point d'accès distant inclut un pare-feu dynamique et peut envoyer le trafic lié à Internet au service de sécurité du contenu basé sur Internet, en vue d'une inspection détaillée des paquets.

### Options de chiffrement locales et centralisées

La solution VBN 2.0 emploie l'algorithme AES de technologie militaire utilisé dans le protocole WPA2 d'entreprise. Il s'agit d'un algorithme cryptographique complexe qui nécessite un traitement important mais qui constitue à ce jour la norme de sécurité la plus stricte pour les connexions Wi-Fi. La solution VBN 2.0 intègre l'algorithme AES au niveau du matériel, afin de diminuer la charge appliquée au processeur principal du point d'accès distant.

Dans la mesure où du matériel compatible avec l'algorithme AES est utilisé dans les périphériques les plus courants et que cet algorithme constitue la protection la plus élevée à ce jour, il est tout à fait judicieux de l'employer comme méthode de chiffrement pour les données transitant entre les clients distants et le centre de données de l'entreprise. Dans l'architecture VBN 2.0, toutes les données utilisateur sont chiffrées de bout en bout avec l'algorithme AES à l'aide de clés individuelles. Un en-tête GRE est ajouté afin de simplifier la mise en place de tunnels vers les contrôleurs de mobilité sur Internet ou sur les réseaux étendus d'entreprise. Le trafic de contrôle du point d'accès distant dispose de son propre tunnel IPsec qui est sécurisé de manière indépendante.

Cette configuration constitue la solution optimale en cas de trafic lié à un centre de données. L'architecture VBN 2.0 prend toutefois en charge d'autres options flexibles d'acheminement réseau, afin d'offrir une solution appropriée lorsque le trafic n'est pas destiné à un centre de données. Dans ce cas, l'algorithme AES est également employé par radio, mais le déchiffrement est effectué au niveau du point d'accès distant et non au niveau du contrôleur de mobilité central.

### Fonctionnalité WLAN pour accès distant

La technologie Wi-Fi introduit des scénarios de mise en réseau particuliers, incompatibles avec des infrastructures câblées. Par exemple, les trames transmises par radio peuvent comporter des erreurs dues à des interférences de radiofréquences (RF) et aux fluctuations de l'intensité du signal. Pour remédier à cette situation, le système de gestion évolutive de l'environnement réseau (Adaptive Radio Management ou ARM) d'Aruba fournit des outils permettant de visualiser et d'optimiser la couverture RF de façon automatique. Dans les succursales ou sur campus, ARM choisit automatiquement les paramètres de radiofréquences optimaux pour le point d'accès distant, surveille en continu les ondes à la recherche d'éventuels signes d'interférence et change de canal si nécessaire. Les clients Wi-Fi sont généralement configurés avec une liste de SSID acceptables. Ils activent, à intervalles réguliers, le système radio Wi-Fi et vérifient ces SSID. Lorsque vous configurez des périphériques client qui seront utilisés dans des environnements VBN 2.0, pensez à placer le SSID d'entreprise au début de la liste. Il s'agit du

---

même SSID que celui utilisé sur le campus. En règle générale, l'authentification au moyen de ce SSID est gérée via une méthode de connexion, comme une connexion Windows, et elle tire parti de l'authentification 802.1X ainsi que des serveurs RADIUS de l'entreprise.

Côté réseau, les points d'accès distants offrent les mêmes services et sont configurés avec les mêmes profils que les points d'accès du campus. Le SSID permet d'étendre le réseau de l'entreprise aux succursales ou bureaux à domicile, où qu'ils se situent dans le monde.

Quant à l'utilisateur, il n'a besoin de se connecter qu'une seule fois grâce à l'utilisation d'un SSID d'entreprise unique pour l'accès distant et sur le campus. Aucune autre information n'est nécessaire, aucune modification des méthodes de travail n'est utile et la sécurité est entièrement transparente, ce qui réduit les coûts informatiques et les appels au centre d'assistance. En outre, le service de dépannage centralisé permet de diminuer les frais d'exploitation de la solution VBN 2.0.

### **Des performances multimédias garanties avec la qualité de service (QoS)**

Les solutions de voix sur le réseau local sans fil et de convergence fixe/mobile étant de plus en plus courantes, la qualité de service (QoS) est désormais essentielle pour assurer le contrôle des flux de trafic multimédia générés et destinés aux succursales ou aux bureaux à domicile.

Le point d'accès distant et le contrôleur de mobilité sont capables d'identifier et de hiérarchiser correctement le trafic multimédia, et ce même lorsque les balises de priorité de celui-ci sont endommagées lorsqu'il provient d'Internet ou d'un périphérique client. Cette reconstitution des balises est possible grâce à l'utilisation de règles de pare-feu qui identifient les flux et réappliquent les balises appropriées.

La qualité de service (QoS) par radio est concernée par le protocole WMM (Wireless Multimedia), actuellement disponible sur tous les périphériques Wi-Fi. Le protocole WMM garantit que le trafic multimédia est transmis dans les délais, même si le réseau est surchargé de données. Il spécifie des mises en correspondance de codes d'accès aux services différenciés (DSCP) et de balises de type de service IP (IP TOS), afin de maintenir la priorité de bout en bout.

Dans la mesure où les téléphones intelligents et autres périphériques convergents génèrent de la voix et des données sur une connexion unique, il n'est plus possible de séparer chaque type de trafic à l'aide de divers SSID et réseaux locaux virtuels sous-jacents. La solution VBN 2.0 ne nécessite aucune configuration de ce type.

D'autres dispositions liées à la qualité de service (QoS) et prises en charge par la solution VBN 2.0 incluent le contrôle d'admission d'appel (CAC), qui garantit que le nombre d'appels voix et vidéo autorisés ne dépasse pas la capacité du réseau ou de la liaison. La solution VBN 2.0 prend également en charge un gestionnaire de bande passante flexible et basé sur des stratégies, qui offre un contrôle précis du trafic dans les réseaux multi-applications et utilisateurs variés et lors des périodes de congestion du réseau.

### **La sécurité dans un réseau VBN 2.0**

En plus des fonctions complètes de détection et de prévention des menaces offertes par le service CSS basé sur Internet d'Aruba (à savoir, le filtrage avancé d'URL, le contrôle de pair-à-pair, un antivirus, un logiciel anti-virus, la détection des réseaux fantômes et la prévention contre la perte des données), la solution VBN 2.0 propose de nombreuses autres options de sécurité. Grâce à la solution VBN 2.0, le point d'accès distant d'une succursale constitue désormais une extension sécurisée du réseau de l'entreprise. Le contrôle de la configuration, ainsi que la configuration de l'accès utilisateur et du pare-feu, sont effectués par le service informatique à partir du centre de données de l'entreprise. On obtient ainsi une solution de mobilité sécurisée et entièrement intégrée permettant un contrôle complet du service rendu à l'utilisateur.

Puisque la solution VBN 2.0 étend les services du centre de données de l'entreprise vers les succursales au moyen de la même architecture que celle utilisée pour les réseaux locaux sans fil sur campus, elle tire parti des méthodes d'authentification et de chiffrement déjà employées par les clients Wi-Fi. Lorsque le point d'accès distant entre en fonctionnement, les périphériques client de l'entreprise voient les mêmes balises et invites que celles utilisées sur

---

campus. L'expérience utilisateur est ainsi cohérente dans toute l'entreprise : les procédures de connexion, l'authentification via 802.1X et le chiffrement AES sont homogènes.

Dans le même temps, la solution VBN 2.0 surveille en continu les environnements sans fil à la recherche d'éventuelles tentatives d'intrusion. La technologie sans fil représente un défi sécuritaire à part entière car les signaux se propagent au-delà de la zone d'émission immédiate, ce qui rend possible une éventuelle surveillance et une potentielle intrusion sans accès physique aux locaux.

En analysant les ondes, les points d'accès distants peuvent reconnaître les attaques les plus courantes et prendre les mesures nécessaires contre leurs auteurs. Les attaques « man in the middle » et l'usurpation de point d'accès sont détectées et maîtrisées. Des informations supplémentaires sont mises à la disposition des administrateurs via l'intégration aux systèmes de détection et de protection contre les intrusions sans fil (WIDS et WIPS) traditionnels, et des alertes peuvent être générées lors du lancement des contre-mesures.

### **Pérennité des sites distants**

L'échec de la connexion WAN ou Internet locale est la cause la plus fréquente des pannes dans les succursales. Une seule interruption peut suffire à isoler une succursale et à bloquer la diffusion de services essentiels. Une des solutions traditionnellement adoptées est de fournir une connexion Internet redondante. Cette opération entraîne néanmoins une augmentation des coûts et il est toujours possible qu'une panne concerne les deux trajets à la fois. Il est généralement très difficile d'avoir accès à des liaisons véritablement différentes sur la plupart des sites.

Il est en revanche assez rare qu'une panne survienne en même temps au niveau d'une connexion câblée et d'une connexion par téléphone. C'est pourquoi la solution VBN 2.0 utilise le réseau de téléphonie mobile comme trajet de liaison alternatif. Un port USB installé sur le point d'accès distant permet à l'utilisateur de sélectionner le réseau GSM de son choix, en insérant un modem de données approprié. L'utilisation de connexions par téléphone constitue une alternative de qualité et économique, car ces connexions sont la plupart du temps en mode de secours. De nombreux utilisateurs de la solution VBN 2.0 emploient déjà le réseau de téléphonie mobile comme seule connexion de liaison sur un point d'accès distant. Tous obtiennent des résultats satisfaisants.

Les succursales de plus grande envergure peuvent également présenter des modèles de trafic internes importants. Dans le cas d'une panne sur le réseau WAN, un point d'accès distant configuré en mode pont permet d'assurer la continuité de la connectivité. En outre, si une panne survient au niveau du centre de données, le point d'accès distant continue à offrir un tunnel séparé lié à Internet, même si le trafic de l'entreprise est bloqué.

### **Évolutivité**

Les technologies actuelles impliquées dans la conception des réseaux d'accès distant empêchent l'application d'une architecture unique et homogène. En effet, les travailleurs itinérants et les télétravailleurs utilisent généralement des logiciels client VPN, tandis que les employés des succursales utilisent plutôt des dispositifs de type *client VPN prêt à l'emploi* de divers fournisseurs qui exigent des systèmes de gestion et de configuration différents. En outre, pour répondre aux demandes spécifiques, telles que la mise en place de la technologie Wi-Fi et la sécurité du contenu, des équipements supplémentaires sont souvent nécessaires, ce qui contribue à augmenter les coûts, ainsi que la complexité de la configuration et de la prise en charge.

Les difficultés s'accroissent au fur et à mesure que les succursales s'agrandissent. Les succursales de grande envergure ont besoin d'une redondance plus importante ; elles requièrent d'autres liaisons d'accès pour une meilleure pérennité et elles comprennent à la fois plus d'employés et de services. Il arrive un moment où la conception du réseau doit à nouveau être modifiée pour inclure tout un ensemble d'équipements répliquant le site du campus à plus petite échelle.

La solution VBN 2.0 permet une progression fluide (depuis les travailleurs itinérants jusqu'aux succursales les plus importantes) car elle utilise une seule et même architecture, un équipement de centre de données homogène, ainsi qu'une plate-forme unique de gestion et de configuration. Les travailleurs itinérants peuvent ainsi disposer d'un agent d'accès à l'intranet virtuel (Virtual Intranet Access ou VIA) Aruba s'ils ont besoin d'un accès à partir des réseaux Wi-Fi publics. Le point d'accès distant RAP-2 est idéal pour les télétravailleurs requérant d'un accès Wi-Fi sécurisé de base. Le point d'accès distant RAP-5 est quant à lui parfaitement adapté aux cadres travaillant à

---

domicile, aux succursales de petite taille et à celles de plus grande envergure disposant de clients câblés, tels que des imprimantes ou des téléphones de bureau.

Au fur et à mesure que les succursales s'agrandissent et que les employés demandent des services supplémentaires, tels que des imprimantes ou des serveurs locaux, il est primordial de fournir un niveau de pérennité plus élevé. Dans ce scénario, les contrôleurs de succursale de la gamme 600 d'Aruba offrent une résilience et une redondance excellentes, ainsi qu'une capacité améliorée. Dans le cas d'une panne de réseau WAN, ils assurent les services de façon autonome et, en situation normale, ils fonctionnent comme des auxiliaires du contrôleur de mobilité du centre de données. Les contrôleurs de succursale de la gamme 600 d'Aruba sont configurés à l'aide des mêmes interfaces et selon les mêmes principes architecturaux que les autres équipements VBN 2.0.

## Conclusion

La mise en réseau des succursales consistait au départ en un simple modèle de réplication, transposant l'ensemble de l'équipement réseau du siège de l'entreprise à plus petite échelle. Chaque succursale était, en quelque sorte, une version miniature du siège de l'entreprise. Cette situation nécessitait néanmoins un grand nombre de dispositifs complexes et plusieurs systèmes de gestion, sans compter que l'équipement des succursales devait subir de fréquents changements pour suivre l'évolution des exigences de mise en réseau.

La quantité de matériel nécessaire a été réduite lorsque les solutions de type *succursale prête à l'emploi* ont vu le jour, associant un routeur, un commutateur, un réseau privé virtuel, un pare-feu, la voix et d'autres services de sécurité dans un seul et même dispositif. Ces solutions ont ainsi permis de réduire l'empreinte et les erreurs de câblage mais, en interne, ces dispositifs représentaient toujours des systèmes indépendants, configurés et gérés séparément.

L'architecture VBN 2.0 d'Aruba *régule* le coût de la mise en réseau dans les petites succursales et les bureaux à domicile : grâce à elle, vous n'avez plus besoin d'aucun dispositif au coût prohibitif. À la place, les succursales peuvent accéder en toute sécurité à des services de qualité professionnelle ; il leur suffit de relier un point d'accès distant à une connexion à large bande. Grâce à cette fonction de déploiement automatique, aucune intervention du service informatique n'est nécessaire. Cette solution innovante permet, par conséquent, une réduction significative de l'empreinte matérielle, une diminution des frais d'exploitation et une évolutivité sans précédent, sans pour autant compromettre la sécurité.

La solution VBN 2.0 migre les services de calcul intensif, tels que la sécurité du contenu, sur Internet. Les économies d'échelle ainsi réalisées permettent de réduire les coûts. Dans la mesure où ces services ne sont plus reliés à des périphériques, mais à un centre de données basé sur Internet, les performances et les économies sont visibles sur une plus longue période. La mise à niveau des services est réalisée sur Internet et non sur chaque périphérique.

L'architecture VBN 2.0 basée sur Internet virtualise les configurations de port, de réseau local virtuel, de routeur, de pare-feu et de VPN en un ensemble de stratégies basées sur l'identité. Celles-ci sont définies de façon centralisée, puis étendues à la demande à des périphériques distants au fur et à mesure que les utilisateurs rejoignent le réseau. Un système de gestion unique et centralisé assure le contrôle de tous les utilisateurs, des stratégies et de la configuration des équipements.

---

## À propos d'Aruba Networks, Inc.

Les gens sont mobiles. Les réseaux doivent suivre. Aruba fournit des réseaux sécurisés aux utilisateurs, qu'ils soient sur site ou itinérants, en associant plusieurs solutions primées :

- Les réseaux Wi-Fi 802.11n adaptatifs sont optimisés pour garantir aux utilisateurs un accès à toutes les informations essentielles à leur mission, en toutes circonstances. Adapter les réseaux locaux câblés coûteux en les remplaçant par des réseaux Wi-Fi 802.11n haut débit permet de réduire à la fois les coûts d'investissement et les frais d'exploitation ;
- La sécurité basée sur l'identité associe des stratégies d'accès aux utilisateurs et applique ces stratégies lors de chaque accès à un réseau ;
- La mise en réseau distant des succursales, des télétravailleurs fixes et des bâtiments satellites assure un accès distant continu aux applications ;
- La gestion de réseau multi-fournisseur offre un point de contrôle unique ; elle permet de contrôler les réseaux hérités et les nouveaux réseaux sans fil d'Aruba et de ses concurrents.

Le coût, l'aspect pratique et les avantages en matière de sécurité de nos solutions mobiles sécurisées révolutionnent littéralement la façon de travailler, ainsi que le lieu de travail. Cotée au NASDAQ et à l'indice Russell 2000®, la société Aruba est implantée à Sunnyvale, en Californie (États-Unis), et opère sur le continent américain, en Europe, au Moyen-Orient et dans la région Asie-Pacifique. Pour en savoir plus, rendez vous sur le site <http://www.arubanetworks.com>. Pour connaître les actualités en temps réel, suivez Aruba sur [Twitter](#), [Facebook](#) ou le [blog Green Island](#).

© 2010 Aruba Networks, Inc. *AirWave*®, *Aruba Networks*®, *Aruba Mobility Management System*®, *Bluescanner*, *For Wireless That Works*®, *Mobile Edge Architecture*, *People Move. Networks Must Follow.*, *The All-Wireless Workplace Is Now Open For Business*, *RFprotect*, *Green Island* et *The Mobile Edge Company*® sont des marques déposées d'Aruba Networks, Inc. Tous droits réservés. Les autres marques appartiennent à leurs détenteurs respectifs.



1344 Crossman Ave. Sunnyvale, CA 94089-1113  
Tel. 408.227.4500 | Fax. 408.227.4550 | [info@arubanetworks.com](mailto:info@arubanetworks.com)  
<http://www.arubanetworks.com>