



## Solution d'accès invité Aruba

Un accès invité est souvent la première application mise en œuvre lorsqu'une entreprise déploie un réseau local sans fil. L'accès invité met en évidence la coopération d'une entreprise avec ses partenaires et ses visiteurs, et renvoie une image positive de cette entreprise. Un bon système d'accès invité assure avant tout un accès hautes performances fiable à Internet, qui permet à un invité de se connecter sans avoir à surmonter d'innombrables difficultés pour reconfigurer son PC. Grâce à la connectivité mobile et aux services de continuité des applications proposés par Aruba, les invités sont assurés de bénéficier de performances optimales.

Un réseau d'accès invité doit séparer et isoler le trafic interne et le trafic des invités en vue de sécuriser de manière hermétique les serveurs et les réseaux locaux d'une entreprise. Comme l'accès invité est assuré sur la même infrastructure de réseau local et de réseau local sans fil qui prend en charge le trafic interne, il s'agit d'un défi considérable qui est directement relevé par la sécurité mobile proposée par Aruba.

## Utilisation de l'accès invité

Lorsque les invités, les fournisseurs et les travailleurs temporaires bénéficient d'un accès instantané à des informations commerciales d'actualité, leur productivité s'en trouve largement optimisée. En leur proposant un accès sécurisé à Internet, ces utilisateurs peuvent revenir à leur réseau d'entreprise ou personnel via un réseau privé virtuel pour utiliser leur messagerie et d'autres ressources qui ne sont pas stockées sur leur ordinateur portable ni sur leur périphérique mobile.

### **PROTECTION DE L'INTRANET :**

Une solution d'accès invité sécurisée doit faire en sorte que les invités puissent directement se connecter à Internet mais sans jamais pouvoir accéder aux ressources du réseau interne, et ce malgré le fait que le trafic des invités soit pris en charge sur l'infrastructure de réseau local et de réseau local sans fil de l'entreprise parallèlement au trafic informatique de cette entreprise. Les anciennes architectures utilisent un réseau local virtuel dédié pour assurer cette protection. L'administration d'un réseau local virtuel reste toutefois contraignante et la moindre erreur de configuration risque de provoquer des failles de sécurité exploitables par un intrus en vue d'utiliser un réseau d'accès invité pour s'attaquer aux ressources et aux

serveurs de l'entreprise. Aruba met en œuvre la sécurité basée sur l'identité pour identifier, catégoriser et maîtriser le trafic des invités quelle que soit leur itinérance sur le réseau local sans fil, le tout sans aucune configuration du réseau local virtuel.

Les portails captifs constituent désormais un mode d'accès à Internet bien établi, que ce soit dans les hôtels, les centres de conférences ou les zones d'accès à Internet sans fil Wi-Fi. Lorsqu'un invité ouvre pour la première fois son navigateur Web, le flux est intercepté et une page d'authentification s'affiche. Ce portail captif, dont la présentation est adaptable à celle de l'entreprise, peut inviter à saisir une adresse électronique et un mot de passe et/ou à parcourir les modalités d'utilisation.

### **AFFECTATION DES INFORMATIONS D'IDENTIFICATION AVEC FACILITÉ ET FLEXIBILITÉ:**

Certaines entreprises ont pris le parti de proposer un libre accès à Internet à toute personne souhaitant y accéder. Cette pratique se fait toutefois de plus en plus rare en raison des risques encourus par ces entreprises d'être tenues pour responsables du mauvais usage de leur réseau. Par exemple, si l'attaque d'une cible sur Internet

## Avantages:

- **Séparation du trafic:** impossibilité pour les invités d'accéder à l'Intranet de l'entreprise grâce au pare-feu dynamique certifié ICASA
- **Fonctionnalité intégrée:** possibilité d'ajouter l'accès invité à tout réseau existant orienté utilisateurs Aruba
- **Contrôle flexible:** libre accès pour tous grâce à des mots de passe individuels uniques
- **Prêt à l'accueil:** intégration à des systèmes tiers pour la vérification par cartes de crédit

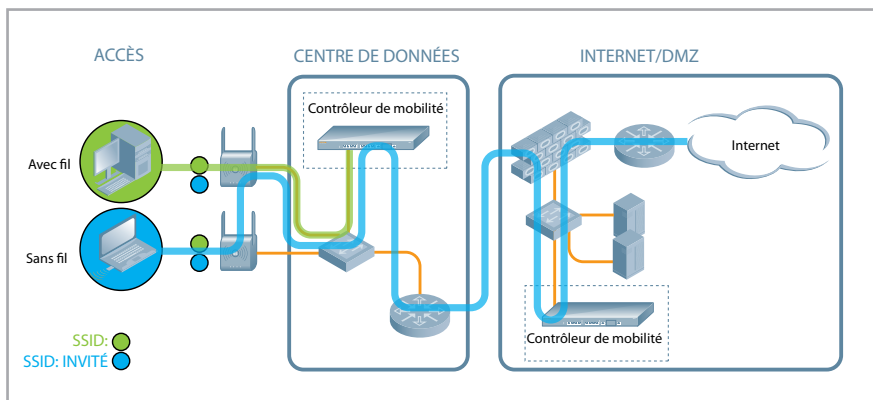
provient du réseau d'une entreprise et que celle-ci n'a pas pris les mesures qui s'imposent pour protéger son réseau, sa responsabilité peut alors être engagée. L'accès invité fait l'objet d'un meilleur contrôle en émettant des mots de passe individuels limités dans le temps, mais cela peut s'avérer contraignant en l'absence de systèmes de prise en charge. La meilleure méthode consiste à remettre à chaque invité une fiche préimprimée ou imprimée à la demande indiquant leur mot de passe unique au moment où il s'enregistre à la réception de l'entreprise. Cela limite les inconvénients tout en optimisant la sécurité.

#### COÛTS D'ADMINISTRATION RÉDUITS:

Les applications informatiques devraient fonctionner sans que les utilisateurs n'aient à solliciter fréquemment le support technique ni à appeler souvent le centre d'assistance. Dans le cadre de l'accès invité, cela signifie que le réceptionniste doit être en mesure d'ajouter facilement des comptes invités et de rapidement émettre des informations d'identification. L'invité doit pouvoir se connecter en ayant à reconfigurer au minimum son PC et le service à Internet doit être fluide et rapide.

**DONNEES D'AUDIT ET D'USAGE:** Les services d'accès invité doivent, eux aussi, proposer des historiques indiquant qui a utilisé le réseau, à quel moment et de quelle manière.

## Mode d'accès invité proposé par Aruba



La solution d'accès invité Aruba est composée de trois éléments essentiels: des points d'accès légers, des contrôleurs de mobilité centraux et des modules logiciels de protection pour les contrôleurs de mobilité. Un système de gestion de la mobilité est également disponible en option pour les réseaux de plus grande envergure. Les points d'accès assurent une connectivité sans fil sécurisée aux périphériques et se connectent sur des systèmes de réseaux locaux/étendus existants de manière à prendre en charge l'ensemble du trafic du réseau local sans fil vers un contrôleur de mobilité installé dans le centre de données via un tunnel GRE ou un tunnel IPsec. La configuration, la gestion, les services de continuité des applications et la sécurité sont centralisés sur le contrôleur de mobilité. L'accès invité est une fonctionnalité propre à tous les réseaux centrés sur l'utilisateur Aruba.

**ACCÈS INVITÉ SUR UN RÉSEAU LOCAL SANS FIL EXISTANT:** Un réseau centré sur l'utilisateur Aruba déployé à des fins professionnelles disposera de points d'accès placés de manière à

assurer une couverture Wi-Fi. Lors de l'ajout d'un accès invité, il peut s'avérer souhaitable de couvrir de nouvelles zones d'un site avec des points d'accès supplémentaires. Dans des installations à plus grande échelle, un contrôleur de mobilité peut être ajouté au niveau de la DMZ du pare-feu de l'entreprise. Le trafic des invités fait entièrement l'objet d'une prise en charge chiffrée, des points d'accès vers un contrôleur de mobilité via des tunnels GRE et vers la DMZ via un autre tunnel crypté, afin d'assurer une connexion sécurisée au pare-feu et à Internet. Les contrôleurs de sécurité Aruba proposent un pare-feu dynamique certifié ICASA qui leur permet de remplir cette fonction exigeante.

**PORTAIL CAPTIF:** L'accès des périphériques clients au réseau est bloqué tant qu'un navigateur Web n'a pas été ouvert et que les informations d'identification et d'authentification n'ont pas été entrées. Le protocole normalisé SSL est utilisé pour sécuriser l'échange des informations d'identification et d'authentification. Le système peut demander un nom et un mot de passe valables ou il peut être configuré

de manière à ne collecter que des adresses électroniques non validées. Les pages du portail captif peuvent être personnalisées à l'image de l'entreprise (logo, informations générales, règles de bonne usage et autre texte). L'intégration d'applications tierces permet l'accès par carte bancaire et propose des systèmes de facturation.

#### **SÉPARATION DU TRAFIC DES INVITÉS:**

Un module logiciel installé sur le contrôleur de mobilité permet de séparer le trafic des invités de l'ensemble du trafic de l'entreprise. Différentes stratégies de sécurité peuvent être appliquées aux fournisseurs sans leur accorder tous les privilèges d'accès au réseau de l'entreprise. Seule la sécurité basée sur l'identité proposée par Aruba présente cet avantage. Le pare-feu

d'application de stratégies assure un contrôle très précis des utilisateurs en appliquant des stratégies à des individus ou à des groupes d'utilisateurs.

#### **ACCÈS BASÉ SUR DES RÔLES:**

Comme l'accès invité est proposé via une page Web, un réceptionniste peut facilement et rapidement ajouter un compte invité personnel pour un visiteur et émettre un mot de passe unique pouvant faire l'objet d'un suivi à l'attention de l'invité. Les comptes peuvent également être préparés à l'avance et attribués aux invités au moment de leur enregistrement. Un « mot de passe invité » peut par ailleurs être publié pour l'ensemble des utilisateurs invités.

### Avantages présentés par la solution d'accès invité Aruba

- Permet de restreindre l'accès au réseau aux invités autorisés.
- Empêche les utilisateurs invités d'accéder au réseau interne, en contrôlant l'accès à Internet en fonction de l'heure, de l'emplacement, du contrat pour la bande passante, etc.
- Propose un système simple pour l'émission d'informations d'identification pour l'accès invité pouvant être utilisé par des employés et des réceptionnistes sans intervention du personnel informatique.
- Gère les données d'imputabilité et d'audit d'usage indiquant qui utilise le réseau, à quel moment et de quelle manière.
- Contrôle l'accès invité sur les réseaux avec et sans fil.
- Assure l'accès invité sans reconfiguration de leur ordinateur et sans besoin de l'assistance du personnel du service informatique.
- S'intègre entièrement au contrôleur de mobilité Aruba.



[WWW.ARUBANETWORKS.COM](http://WWW.ARUBANETWORKS.COM)

1322 Crossman Avenue. Sunnyvale, CA 94089 , États-Unis | Tel. +1 408.227.4500 | Fax.

+1 408.227.4550