

## Le BYOD facile avec Mancala Networks

**De plus en plus d'employés choisissent d'utiliser des équipements mobiles personnels sur leur lieu de travail. Face à cette tendance au "Bring Your Own Device" (BYOD), comment les entreprises, institutions et fournisseurs de services d'infogérance peuvent continuer d'assurer efficacement la sécurité et la conformité réglementaire des réseaux informatiques ? Le défi est de taille, sachant que le nombre et le type d'appareils nomades est en constante augmentation; rien qu'Apple a vendu plus d'un million d'iPhones 4S le jour de sa sortie !**

Selon Gartner, 75% des entreprises ont mis en place des règles encadrant l'utilisation des équipements privés dans le cadre du travail. Certaines d'entre elles, dans une vaine tentative de contourner la problématique du BYOD, vont jusqu'à les interdire purement et simplement dans leur charte informatique. Cette méthode échoue quasi-systématiquement car elle ne s'accompagne pas de la mise en place d'outils efficaces, qui permettraient une application concrète de ces règles sur le réseau lui-même, en temps réel.

Lors d'audits, les entreprises sont alors régulièrement étonnées d'apprendre qu'il existe au moins 30% d'appareils "en trop" connectés à leur réseau par rapport à ce qui est documenté; cet écart provenant bien évidemment très majoritairement de l'utilisation des smartphones et autres équipements BYOD.

La plupart des organisations IT utilisent le mode WPA2-Enterprise pour protéger leur réseau sans fil. Bien que cette configuration soit sécurisée, il ne faut pas bien longtemps aux employés pour découvrir que les données d'authentification de leur PC d'entreprise peuvent également servir à connecter leur équipements personnels iOS ou Android sur ce même réseau. Ce comportement – bien que particulièrement utile pour les employés – complique sérieusement la tâche de l'IT, puisque ces appareils peuvent présenter des failles de sécurité qui n'existent pas sur leur PC d'entreprise, à la configuration contrôlée, voire verrouillée.

Les questions clés à se poser sont les suivantes :

- comment faire la distinction entre le PC d'entreprise de David Jones et le smartphone personnel de M. Jones ?
- Comment appliquer une politique de sécurité à un équipement qui n'est pas directement sous contrôle de l'IT ?
- Comment automatiser les processus de contrôle et d'admission sur le réseau afin de ne pas surcharger inutilement les équipes de support IT ?

Le Network Controller de Mancala fournit les outils nécessaires pour prendre le contrôle des déploiements BYOD. Il permet d'effectuer la transition depuis une politique de sécurité figée (sur une charte informatique) vers une politique appliquée dynamiquement, en temps réel, sur l'ensemble d'un réseau.

- Un système d'inventaire et de profilage en temps réel identifie précisément chaque type d'équipement, facilitant ainsi son contrôle et sa gestion.
- Un portail captif intégré permet d'automatiser la configuration d'un équipement avant son admission sur le réseau. Il est possible d'effectuer l'authentification d'un appareil en parallèle de celle de son utilisateur, et ainsi de distinguer "David Jones sur son PC d'entreprise" de "M. Jones sur son smartphone personnel".

## ■ Les défis du BYOD

Le BYOD offre une grande variété de défis pour les organisations IT. Parmi ceux-ci nous pouvons en citer trois d'importance majeure.

### **L'identification des équipements et des utilisateurs**

De nombreux utilisateurs sont capables de se passer des services de l'IT pour introduire un appareil non enregistré sur le réseau. Celui-ci sera alors difficilement détectable; tout au plus, il sera enregistré que "M. Jones est connecté". Difficile alors de savoir si "M. Jones" utilise son smartphone personnel ou son PC d'entreprise.

### **La sécurisation des équipements mobiles**

La sécurisation d'un appareil personnel diffère sensiblement de celle d'un PC d'entreprise. De manière générale, les identifiants de connexion sont conservés en mémoire des dispositifs mobiles personnels, de sorte que lorsque le réseau sans fil de l'entreprise est détecté, l'appareil s'y connecte "automatiquement". En conséquence de quoi il n'y a aucune garantie que ce soit réellement M. Jones qui se serve "la tablette de M. Jones", ni qu'un dispositif égaré ou volé, déjà configuré pour accéder au réseau, ne puisse être utilisé par une personne malintentionnée pour accéder à des données sensibles.

### **La planification de capacité**

Les équipements BYOD utilisent des ressources telles que des adresses IP et de la bande passante. Une meilleure connaissance du nombre et du type d'appareils pouvant potentiellement se connecter au réseau d'entreprise est indispensable pour permettre d'assurer efficacement la planification de capacité ainsi que la priorisation du trafic.

Certaines entreprises tentent de contourner les problèmes en imposant aux équipements BYOD de se connecter sur leur réseau dit "visiteurs", qui est séparé du réseau principal et généralement limité à un accès Internet basique. Si, comme leur nom l'indique, ces réseaux visiteurs sont parfaits pour des personnes externes à l'entreprise, les employés utilisant leurs équipements personnels pour des raisons professionnelles valides sont rapidement surchargés de contraintes additionnelles de configuration, comme par exemple la nécessité d'utiliser un VPN pour accéder aux ressources internes de l'entreprise. En fait, il est généralement préférable de permettre aux appareils BYOD d'accéder directement au réseau d'entreprise, puisque, sans la possibilité d'effectuer en temps réel un contrôle contextuel strict du réseau, il est impossible d'imposer concrètement l'utilisation du réseau visiteurs à l'ensemble des équipements mobiles personnels.

## ■ Contrôle contextuel et identification des équipements

L'élément clé d'une solution BYOD consiste en la possibilité de mettre en place un contrôle contextuel du réseau. C'est-à-dire d'une part à identifier le type, la fonction et l'utilisateur de chaque équipement qui se connecte au réseau : est-ce un Iphone ? Une imprimante ? Un PC Windows ? Est-il authentifié ? Est-ce un appareil professionnel ou personnel ? Et d'autre part, en se basant sur la réponse à ces questions en temps réel, à appliquer dynamiquement des règles de contrôle et d'utilisation des ressources du réseau.

Le Network Controller de Mancala apporte une réponse aux défis du BYOD en ajoutant aux mécanismes d'authentification standard une couche de contrôle basée sur l'identité de chaque équipement : type, usage, utilisateur.

La technologie de profilage intégrée au Network Controller lui permet de reconnaître les signatures uniques d'appareils mobiles lorsqu'ils s'authentifient et dialoguent suivant les protocoles réseaux les plus courants : RADIUS, DHCP, DNS, ARP, etc. Les appareils sont automatiquement classés par type : PC, routeur, PDA, imprimante, caméra IP, capteur, etc. L'ensemble des informations rassemblées permet au Network Controller de déterminer que c'est "M. Jones qui utilise sa tablette personnelle" plutôt que "M. Jones qui utilise son PC d'entreprise" et d'appliquer des politiques de sécurité appropriées, en temps réel.

Cette capacité d'inventaire en temps réel permet aux administrateurs IT de voir à chaque instant l'intégralité des équipements connectés au réseau, qu'ils soient professionnels ou personnels, tout en identifiant le type d'appareil et son propriétaire.

Une fois qu'un dispositif est identifié et classifié, le Network Controller propose une grande variété d'options de contrôle d'accès et d'utilisation du réseau. En tirant parti de ces différentes options, l'administrateur réseau peut ainsi limiter l'accès aux ressources sensibles de l'entreprise. Pour revenir à notre exemple, David Jones serait ainsi en mesure d'accéder à ses email, ressources RH et financières depuis son PC d'entreprise qu'il n'aurait accès qu'aux emails depuis sa tablette et son smartphone personnels.

## ■ Admission des nouveaux équipements

Afin de prévenir l'explosion des coûts de support informatique, les entreprises doivent adopter une approche contrôlée du provisionnement des accès au réseau par les équipements BYOD de leurs employés. L'architecture flexible du Network Controller permet de gérer de multiples scénarios. Nous nous concentrerons ici sur l'exemple le plus courant.

Un nouvel équipement personnel se connecte au réseau d'entreprise. Détecté comme "inconnu", il est automatiquement placé sur un réseau de quarantaine temporaire, dans l'attente de son admission sur le réseau principal. Son utilisateur est redirigé vers un portail web captif dédié au provisionnement des nouveaux équipements. Il entre alors ses données d'authentification, qui sont validées par l'infrastructure existante (typiquement Active Directory ou LDAP). En parallèle, le Network Controller détermine le profil de l'appareil, qu'il classifie par exemple comme un smartphone personnel inconnu, utilisant iOS. À ce stade, l'utilisateur se verra présenter les instructions requises pour mettre son équipement en conformité avec la politique de sécurité de l'entreprise. Une fois cette opération effectuée, des droits d'accès au réseau adaptés lui seront

accordés. Un système de règles de sécurité contextuelles garantira que cet appareil se comportera de manière cohérente avec sa fonction.

## ■ Conclusion

La plupart des DSI doivent maintenant faire face à la pression irrésistible du BYOD sur l'ensemble du réseau de leur entreprise. Il y a un an seulement, les analystes et les consultants recommandaient l'utilisation d'une plateforme unique, débattant des mérites relatifs d'iOS vs Android vs Blackberry. Aujourd'hui, tous reconnaissent que la bataille de l'uniformisation est perdue et que des solutions doivent être trouvées pour rendre l'infrastructure du réseau plus ouverte, tout en maintenant sécurité et contrôle.

Le Network Controller de Mancala permet aux entreprises, institutions et fournisseurs de services d'infogérance de maîtriser l'évolution des infrastructures réseau, rendue incontournable par l'explosion du nombre et du type d'équipements connectés ainsi que par la mobilité accrue des utilisateurs.

---

### Solution de gestion et de sécurisation en temps réel des réseaux informatiques

Basé sur une technologie brevetée et primée, le Network Controller agit de manière innovante sur les flux de contrôle du réseau.

Le Network Controller s'installe dans le réseau, en complément des routeurs, commutateurs, et pare-feux et interface les services réseaux fondamentaux : DNS, DHCP, RADIUS, SIP. Facilement intégrable aux infrastructures et solutions existantes, il détecte en temps réel les équipements et utilisateurs connectés, analyse leur comportement, et agit automatiquement pour maintenir une sécurité optimale. Il apporte des capacités de visibilité et de contrôle inégalées.

Le Network Controller est disponible sous forme d'une gamme d'éditions logicielles adaptées aux différents besoins des entreprises, des intégrateurs, des hébergeurs et des fournisseurs de services d'infogérance (« Services Providers »). En option, chaque édition est aussi disponible préchargée sur un serveur physique (« appliance »).