COMMENT TIRER PROFIT DES PROGRAMMES BYOD ?

DES SERVICES RÉSEAU CONÇUS POUR GARANTIR LA SÉCURITÉ, LA MOBILITÉ ET LA LIBERTÉ DE CHOIX DES SALARIÉS

NOTE D'APPLICATION

Alcatel·Lucent Enterprise

RÉSUMÉ

À l'heure où un nombre accru d'entreprises se demandent comment exploiter les programmes Bring Your Own Device (BYOD) afin d'améliorer leur productivité, il est important que les équipes informatiques soient suffisamment flexibles pour développer des solutions personnalisées, adaptées aux besoins des entreprises. Alcatel-Lucent fournit tous les éléments requis pour créer des architectures agiles, capables de tirer efficacement parti des programmes BYOD. Les services BYOD d'Alcatel-Lucent, qui complètent la solution Alcatel-Lucent Converged Campus Network Solution, garantissent aux utilisateurs et aux terminaux autorisés un accès permanent à l'ensemble des ressources dont ils ont besoin. Les utilisateurs bénéficient d'une qualité d'expérience supérieure, quelle que soit l'application utilisée, sur l'ensemble des réseaux fixes et mobiles. Cette solution, qui laisse aux salariés une grande liberté de choix, offre également une connectivité omniprésente, un accès simplifié et des communications permanentes. Elle empêche les salariés non autorisés ou les terminaux non conformes d'accéder aux ressources de l'entreprise et de mettre en danger l'intégrité et la sécurité des informations.

TABLE DES MATIÈRES

BYOD ET COMMUNICATIONS PROFESSIONNELLES

Les entreprises s'intéressent déjà depuis un moment à l'engouement des salariés pour les pratiques BYOD (Bring Your Own Device). Il y a un peu plus d'un an, un rapport publié par Accenture précisait que 45 % des salariés jugeaient leurs terminaux et applications personnels plus utiles que ceux de l'entreprise.[1] 66 % affirmaient ne pas se soucier des politiques informatiques de leur entreprise car utilisant uniquement les technologies nécessaires à la réalisation de leur travail. 23 % disaient utiliser régulièrement leurs terminaux personnels à titre professionnel et 27 % utiliser des applications non propriétaires pour améliorer leur productivité.

À l'époque, ce rapport (comme d'autres) visait à expliquer l'adoption croissante du BYOD, phénomène auquel les entreprises de toutes tailles se trouvaient confrontées. Un an plus tard, le rapport Gartner ajoute que, partout dans le monde, les services informatiques intègrent de plus en plus la tendance BYOD dans l'entreprise. En fait, ce rapport précise que les programmes d'entreprise destinés à tirer profit du BYOD deviennent monnaie courante et que, d'ici 2016, 38 % des entreprises s'attendent à ne plus fournir de terminaux hardware à leurs salariés.

La culture émergente du BYOD et la « consumérisation » des communications professionnelles sont la conséquence directe de la multiplication des petits terminaux mobiles, tels les Netbooks (mini-PC portables), les smartphones et les tablettes. Les utilisateurs se reposent sur ces terminaux dans un nombre accru de situations professionnelles et personnelles. Les applications deviennent chaque jour plus mobiles et les utilisateurs plus connectés (« always on ») à l'échelle de la planète. Dans ce processus, les salariés sont plus souvent connectés à leurs clouds personnels d'applications et de services qu'aux réseaux de l'entreprise et s'attendent à une simplicité d'utilisation identique dans toutes les applications.

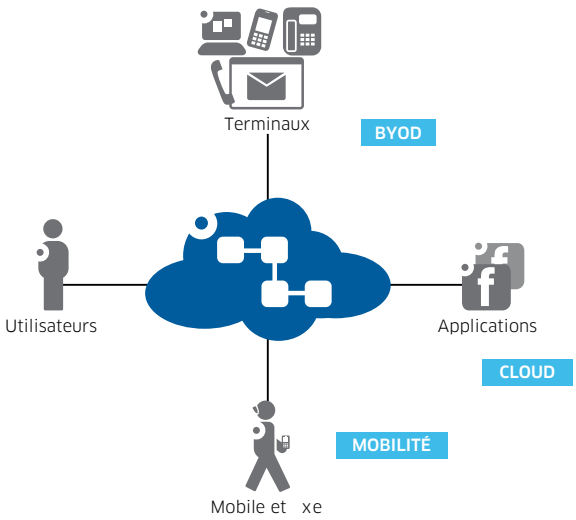
Habitués à pouvoir accéder en permanence à leurs applications personnelles (où qu'ils se trouvent et quel que soit le terminal utilisé), les salariés souhaitent disposer du même type d'accès, transparent et universel, lorsqu'ils se connectent à des applications professionnelles avec leurs terminaux personnels, dans l'entreprise comme à l'extérieur. Ils veulent utiliser leurs terminaux personnels pour poursuivre les communications numériques engagées avec leurs collègues, leurs partenaires et leurs clients, où qu'ils se trouvent et quelle que soit l'application choisie. Et ils veulent pouvoir le faire en utilisant les réseaux fixes ou mobiles de leur choix.

Toutefois, le BYOD présente un réel défi pour les services informatiques des entreprises. Parce que le service informatique de l'entreprise ne contrôle pas les terminaux mobiles et les clouds personnels des salariés, il existe un risque accru d'accès externe non autorisé à des données professionnelles sensibles, et ce chaque fois que de tels terminaux et applications sont utilisés. Les entreprises doivent non seulement trouver le moyen d'adopter le BYOD pour répondre aux besoins de communications de leurs salariés mais elles doivent aussi tirer profit du changement de mode de fonctionnement pour améliorer la productivité des salariés et protéger les réseaux des accès indésirables.

[1] « Consumer IT: The Global Infiltration into the Workforce », Accenture BlogPodium, Mai 2012, www.accenture-blogpodium.nl/site.
[2] « Bring Your Own Device: The Facts and the Future », Gartner, http://www.gartner.com/newsroom/id/2466615.a

Alcatel-Lucent fournit aux entreprises tous les éléments dont elles ont besoin pour créer des architectures, des solutions et des services agiles, qui répondent à l'évolution des besoins de communication des salariés et permettent d'exploiter efficacement les programmes BYOD. Avec une gamme complète d'offres de services, de solutions de communications et de produits fixes et mobiles, Alcatel-Lucent offre aux entreprises un large éventail de ressources, destinées à garantir la mobilité des salariés et la transparence des communications dans les clouds personnels et les réseaux d'entreprise. Alcatel-Lucent fournit en outre des services de communications pour smartphones et tablettes optimisés pour permettre une gestion efficace des communications (Figure 1)

Figure 1. Alcatel-Lucent offre des services de communications optimisés pour permettre une gestion efficace des communications



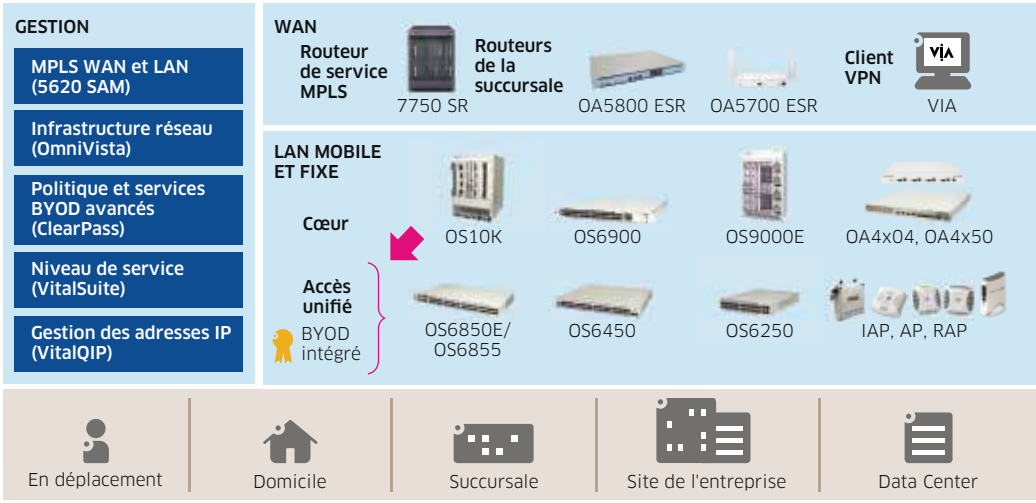
Dans le cadre de cette approche globale, Alcatel-Lucent intègre un outil BYOD dans la solution Converged Campus Network Solution. L'approche Alcatel-Lucent du BYOD est conçue de manière à ce que seuls les utilisateurs autorisés et les terminaux approuvés puissent accéder en permanence aux ressources dont ils ont besoin. Elle garantit à tous les utilisateurs une qualité d'expérience exceptionnelle sur l'ensemble des applications. Cette solution laisse aux salariés la liberté de choix à laquelle ils s'attendent et leur garantit les avantages suivants : connectivité universelle, accès simplifié et communications omniprésentes. Plus important encore, la solution Alcatel-Lucent pour le BYOD empêche les salariés non autorisés ou les terminaux non conformes d'accéder aux ressources de l'entreprise et de mettre en danger l'intégrité et la sécurité des données professionnelles.

CRÉER LE CHOIX DE LA MOBILITÉ, DES APPLICATIONS ET DES TERMINAUX

Alcatel-Lucent Converged Campus Network Solution assure la prise en charge du BYOD, offre une qualité d'expérience utilisateur exceptionnelle et garantit une simplicité d'utilisation comparable à celle de la sphère privée pour l'ensemble des communications professionnelles. Cette solution garantit la très grande qualité de service des communications personnelles et professionnelles de l'utilisateur. En leur offrant le choix et le contrôle des médias et des terminaux disponibles, elle permet aux utilisateurs de communiquer simultanément avec autant de personnes qu'ils le souhaitent, en utilisant les terminaux de leur choix.

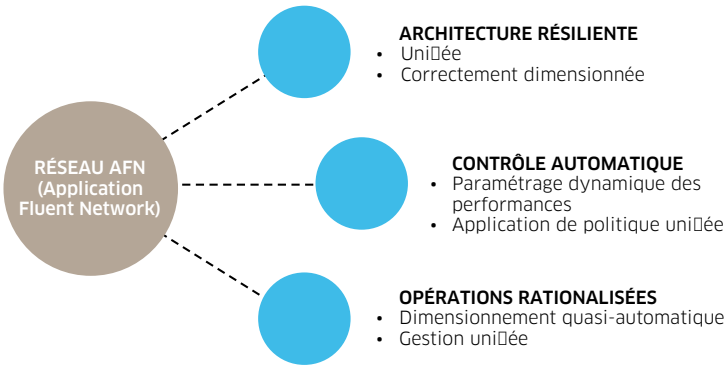
La solution Alcatel-Lucent Converged Campus Network Solution prend en charge le BYOD dans une gamme complète de produits et de solutions intégrés, conçus pour garantir l'« Application Fluency » (Figure 2).

Figure 2. Alcatel-Lucent Converged Campus Network Solution assure la prise en charge du BYOD dans un ensemble de produits et de solutions qui garantissent l'Application Fluency



Un réseau AFN (Application Fluent Network) qui intègre ces éléments est adapté aux nouveaux modèles de fourniture de trafic et d'applications requis pour prendre en charge le BYOD (Figure 3). L'architecture réseau est plus intelligente et plus dynamique. Elle prend en charge l'interconnexion transparente des applications personnelles de chaque utilisateur, leur permettant ainsi de fonctionner sur le réseau de l'entreprise. Le réseau contrôle et identifie la nature du trafic généré par l'utilisateur et donne la priorité au trafic professionnel stratégique. Il gère la fourniture de ce trafic au niveau de qualité requis pour les processus de communication de l'entreprise. Cette solution permet d'optimiser en permanence la productivité de l'utilisateur final.

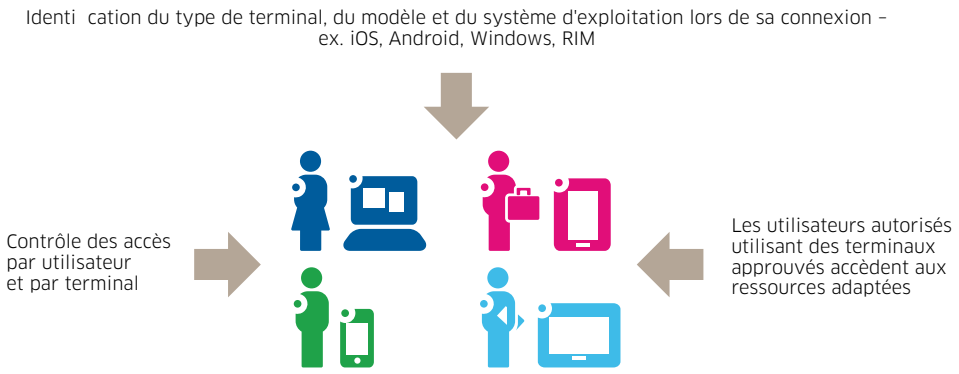
Figure 3. Une réseau AFN Alcatel-Lucent donne la priorité au trafic professionnel par rapport au trafic personnel ou non stratégique



Mode de fonctionnement

La mise en œuvre Alcatel-Lucent du BYOD dans la solution Converged Campus Network Solution repose sur une gestion intelligente des politiques et sur l'identification des terminaux. Grâce à ces fonctionnalités, les utilisateurs disposant de droits adaptés et de terminaux approuvés accèdent aux ressources de communication dont ils ont besoin et bénéficient d'une qualité d'expérience exceptionnelle (Figure 4). Elles permettent également d'empêcher des salariés non autorisés ou des terminaux non conformes d'accéder aux ressources de l'entreprise.

Figure 4. Le BYOD Alcatel-Lucent dans la solution Converged Campus Network Solution repose sur l'identification intelligente des terminaux



Une fois le terminal identifié, des décisions sont prises pour assurer sa gestion et celle des applications de communication utilisées. La gestion est effectuée à l'aide des outils suivants :

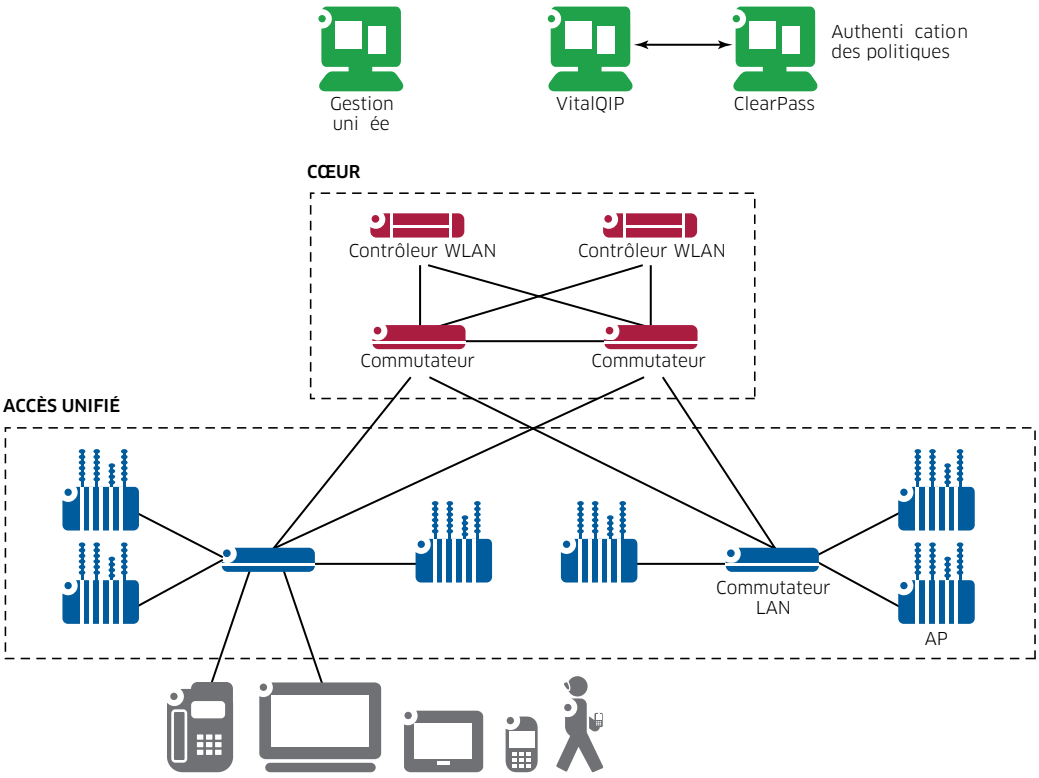
- Un mécanisme performant d'autorisation et de contrôle des accès, qui permet l'authentification de l'utilisateur et du terminal ;
- Un contrôle de l'intégrité, qui permet de détecter tout terminal non approuvé essayant d'accéder au réseau et d'empêcher les applications non autorisées d'utiliser la bande passante du réseau ou d'enfreindre les politiques de l'entreprise. Ce contrôle garantit que les terminaux qui se connectent au réseau ne cachent ni virus ni programme malveillant et qu'ils ne s'apprêtent pas à infecter le réseau ou d'autres terminaux ;
- Un mécanisme de qualité de service (QoS) et de hiérarchisation, qui vérifie que toutes les applications approuvées fonctionnent correctement lorsqu'elles utilisent le réseau, et que tout le trafic est hiérarchisé en fonction du type de communication généré par les applications.

Grâce à ces trois éléments, la gestion Alcatel-Lucent des politiques et l'identification des terminaux BYOD répondent à l'ensemble des besoins de contrôle d'accès et notifient l'infrastructure réseau des droits et de la bande passante accordés à chaque utilisateur en fonction du terminal utilisé. Les terminaux de type imprimantes, appareils photos ou scanners peuvent être ajoutés automatiquement comme terminaux de « liste blanche », sans nécessiter d'intervention informatique. À partir de là, l'infrastructure Converged Campus Network Solution d'Alcatel-Lucent gère les droits du réseau, tout en assurant le contrôle permanent de l'état de santé et de la conformité de chaque terminal. Ce processus est appliqué à l'ensemble des salariés, des sous-traitants et des invités qui se connectent au réseau.

Contrôle des accès

La plateforme Aruba ClearPass™ Policy Manager (CPPM) pilote les capacités d'accès unifié BYOD et la solution Converged Campus Network Solution d'Alcatel-Lucent. Elle fournit aux salariés, aux sous-traitants et aux invités un accès réseau basé sur les utilisateurs et les terminaux dans l'ensemble de l'infrastructure de réseaux VPN, fixes et mobiles.

Figure 5. Une plateforme de gestion des politiques pilote l'accès unifié dans la solution Converged Campus Network Solution d'Alcatel-Lucent



Avec la plateforme CPPM, des politiques d'accès réseau gérées de manière centralisée fournissent toutes les capacités d'authentification nécessaires aux salariés hyper mobiles actuels, quel que soit le type de terminal utilisé ou son propriétaire. Des services automatisés permettent aux utilisateurs d'intégrer leurs terminaux personnels, d'enregistrer des terminaux AirPlay et AirPrint pour le partage de données et de créer des identifiants d'accès invité de manière sécurisée. Le résultat est une solution permanente et évolutive de contrôle des accès réseau, qui dépasse les exigences de protection des terminaux BYOD et des terminaux gérés par les équipes informatiques.

La plateforme CPPM applique de manière centralisée toutes les composantes du BYOD sur la base de droits d'accès réseau détaillés, accordés en fonction des éléments suivants : profil réseau de l'utilisateur, type de terminal, paramètres de gestion, état de santé du terminal, localisation et moment de la connexion. Les éléments intégrés suivants garantissent l'application transparente des politiques dans l'ensemble du réseau : Remote Authentication Dial In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS +), gestion des profils, fonctions d'intégration, contrôles de l'état de santé et des accès invités, capacité d'exploitation de solutions tierces de gestion des terminaux mobiles.

Application Fluency

En gérant l'accès de cette façon, Alcatel-Lucent garantit le principe d'Application Fluency. La création de niveaux de contrôle d'accès différencié permet de répondre aux préoccupations pratiques de divers groupes d'utilisateurs.

Les services opérationnels d'une entreprise peuvent ainsi se voir accorder des droits d'accès à certaines ressources et applications spécifiques. De plus, diverses catégories de terminaux peuvent être définies pour les utilisateurs des différents services. Selon cette approche, une catégorie de terminaux BYOD peut se voir attribuer des droits d'accès différents de ceux dont bénéficient les terminaux de l'entreprise.

Mais l'accès différencié permet également aux équipes informatiques de contrôler le nombre de terminaux qu'un utilisateur apporte dans l'entreprise. Par exemple, les managers ou les équipes de vente peuvent être autorisés à utiliser jusqu'à deux terminaux personnels pour satisfaire leurs exigences en termes d'ultra-mobilité et de permanence des interactions clients. À l'inverse, les salariés basés sur site peuvent se voir limiter à l'utilisation d'un seul terminal personnel car ils sont censés utiliser leur ordinateur professionnel la majeure partie du temps.

Les visiteurs forment également un groupe distinct avec des besoins d'accès spécifiques. Une solution d'accès invité peut être utilisée pour différencier le trafic invité, personnaliser l'expérience de chaque utilisateur et assurer la visibilité de ce type de connexions. La combinaison de différentes solutions d'accès fournit également aux équipes informatiques les données nécessaires pour adapter les exigences de bande passante aux différents groupes d'utilisateurs, aux objectifs de planification et aux audits réseau. Dans un but de simplification, la plateforme CPPM propose également des fonctions de gestion des accès invités. La fonction CPPM Guest™ rationalise les processus de travail et permet aux opérateurs ou aux sponsors, tels les services de réception, les responsables événementiels et le personnel externe aux services informatiques, de créer des comptes temporaires pour accorder des accès Wi-Fi®.

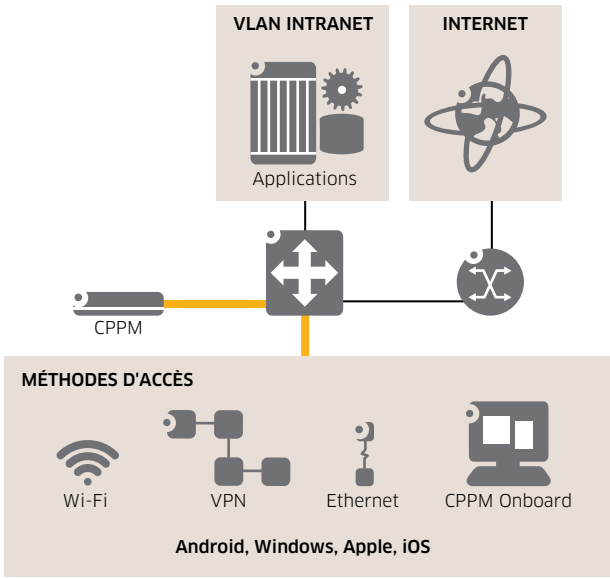
Les invités peuvent également s'auto-enregistrer pour obtenir un accès réseau. Une fois l'enregistrement effectué, la fonction CPPM Guest envoie aux utilisateurs un SMS ou un e-mail comprenant les identifiants de connexion à un compte. Un tel compte peut être configuré pour expirer automatiquement au bout d'un nombre d'heures ou de jours prédéterminé.

Parce qu'elle fonctionne à l'extérieur de la plateforme CPPM, la fonction CPPM Guest est initiée par l'ensemble des fonctions d'authentification, d'autorisation, de comptabilité et d'application des politiques de la plateforme CPPM. Cette dernière évolue de manière transparente dans l'ensemble des réseaux multifournisseurs VPN, fixes et mobiles et assure la prise en charge de différents référentiels d'identité. La fonction CPPM Guest peut donc évoluer pour prendre en charge les besoins des grandes entreprises et des réseaux multisites et gérer des accès sécurisés basés sur le type d'utilisateur pour le compte de centaines de milliers d'utilisateurs simultanés. De plus, grâce à la visibilité complète des accès invités, la fonction CPPM Guest simplifie l'évaluation de l'utilisation réseau, l'identification des exigences de couverture et l'adaptation aux besoins de conformité de l'entreprise et de l'industrie.

Intégration des terminaux

La plateforme CPPM gère également l'intégration des terminaux. La solution peut dimensionner et configurer automatiquement les terminaux mobiles personnels d'un salarié (Windows®, Mac OS® X, iOS®, Android™ version 2.2 et au-delà) et autoriser chaque terminal à se connecter au réseau de manière sécurisée. L'intégration des terminaux est assurée à l'aide de la fonction CPPM Onboard™ (Figure 6).

Figure 6. La plateforme CPPM gère l'intégration des terminaux à l'aide de la fonction Onboard



CPPM Onboard permet aux salariés, aux sous-traitants et aux partenaires de configurer eux-mêmes leurs terminaux mobiles personnels. Le portail d'inscription CPPM détecte automatiquement le système d'exploitation d'un terminal et suggère à l'utilisateur le pack de configuration approprié. Il propose une solution simple pour configurer les paramètres des réseaux VPN, fixes et mobiles, appliquer des identifiants de terminaux uniques et garantir que les utilisateurs se connectent aux réseaux 802.1X de manière sécurisée, avec une implication informatique minimale.

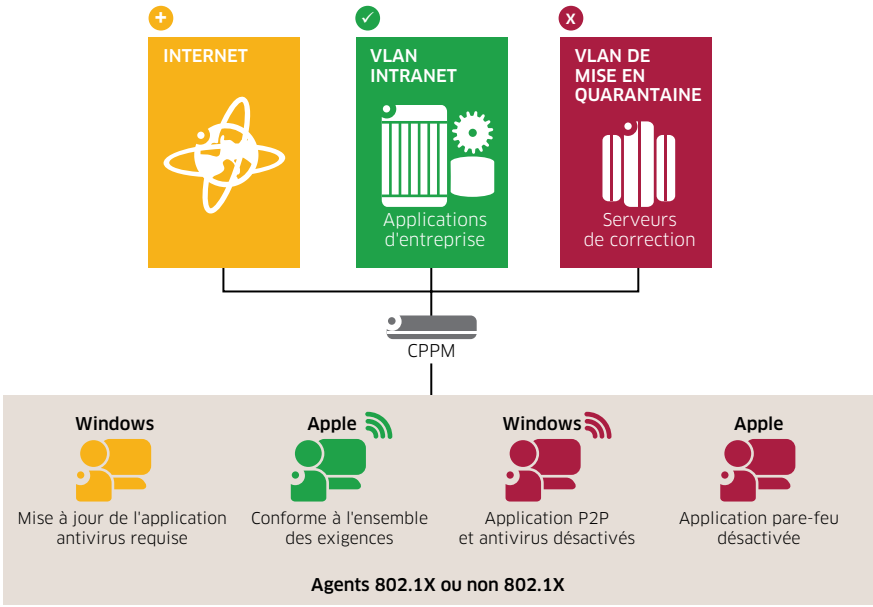
La fonction CPPM Onboard tire parti des capacités d'autorisation de certificats de la plateforme pour publier des identifiants uniques, qui comprennent des données de certificats ainsi que des données relatives aux utilisateurs et aux terminaux. L'allocation d'identifiants de terminaux uniques à l'aide de la fo888nction CPPM Onboard protège les entreprises qui veulent adopter les initiatives BYOD sans introduire d'autorités de certification externes. Des capacités de menu et de recherche permettent de révoquer et de supprimer rapidement les certificats accordés à certains terminaux mobiles lorsqu'un utilisateur quitte l'entreprise ou lorsqu'un terminal mobile est déclaré perdu ou volé.

Cette simplicité d'intégration contribue à la rationalisation des processus des centres de support informatique. Elle permet aux équipes informatiques d'automatiser et de protéger les nombreux processus requis pour réussir la mise en œuvre des initiatives BYOD, tout en améliorant l'expérience utilisateur.

Vérification de l'intégrité

Les contrôles de l'intégrité et de l'état de santé des terminaux sont gérés par la fonction CPPM OnGuard™. Cette dernière garantit une protection adaptée aux entreprise. Elle procède à une vérification avancée de l'intégrité des points de connexion sur les principaux systèmes d'exploitation et garantit ainsi la conformité des terminaux avant connexion. Ces vérifications et contrôles sont réalisés en complément des audits de pare-feux personnels, de logiciels antivirus et anti-espions effectués par les processus standard de contrôle et de protection des accès réseau (NAC/NAP). Parce qu'elle veille à l'entière conformité des terminaux utilisateur, la fonction CPPM OnGuard™ garantit la protection permanente du réseau (Figure 7).

Figure 7. Les contrôles de l'intégrité et de l'état de santé des terminaux sont gérés par la fonction CPPM OnGuard™



Les processus NAC et NAP avancés de la fonction CPPM OnGuard garantissent une protection optimale contre les vulnérabilités. Lorsque l'état de santé d'un terminal ne répond pas aux critères de conformité, l'utilisateur reçoit un message pour l'en informer ainsi que des instructions de mise en conformité, si la correction automatique n'est pas utilisée. Pour une protection accrue, la fonction CPPM OnGuard peut contrôler des données plus précises qu'avec les agents NAP standards. Elle permet également d'évaluer les attributs spécifiques aux produits (produit, moteur, versions des fichiers de données pour les applications antivirus).

Gestion des applications mobiles

La fonction de gestion des applications mobiles (MAM) est assurée par l'application WorkSpace CPPM. Cette fonction permet aux équipes informatiques de protéger, de diffuser et de gérer des applications professionnelles sur des terminaux mobiles personnels. L'application mobile WorkSpace donne la possibilité aux utilisateurs d'intégrer leurs propres terminaux, d'organiser et de gérer leurs applications mobiles et de fournir un accès réseau à leurs invités.

Grâce à l'application WorkSpace, les services informatiques de l'entreprise créent facilement des politiques destinées à contrôler les modes d'utilisation des applications professionnelles et de protection des données. Il est possible de lancer une session VPN automatique lorsque des applications professionnelles spécifiques sont utilisées sur les réseaux publics. Les applications professionnelles peuvent également être verrouillées sur la base de critères de localisation ou de géolocalisation.

Pour les utilisateurs, l'appli mobile WorkSpace offre des capacités de contrôle sans précédent sur l'ensemble des terminaux personnels que l'utilisateur est autorisé à connecter au réseau. Elle renseigne sur l'état de la politique relative aux applications, fournit un accès aux boutiques App Store de l'entreprise et garantit une identification unique aux applications professionnelles. Elle permet également aux utilisateurs de créer et de gérer temporairement des comptes Wi-Fi invités, sans avoir à passer par le service informatique ou le service de réception.

L'appli WorkSpace prend en charge l'un des plus importants écosystèmes d'applications mobiles professionnelles de l'industrie. Le service informatique peut aisément assurer la protection, la distribution et la gestion de plus de 40 applications de productivité de tiers ainsi que celle d'applications développées en interne. Les contrôles détaillés de politiques et les mises à jour automatiques permettent aux équipes informatiques d'appliquer des changements de politique par application sans avoir à redéployer les applications déjà installées sur les terminaux.

À l'aide de WorkSpace, les équipes informatiques peuvent également distribuer et gérer des applications approuvées par l'entreprise à partir d'une boutique App Store interne. Un profil réseau utilisateur est utilisé pour déterminer les applications qui sont installées automatiquement sur le terminal. Le service informatique peut également identifier les applications professionnelles utilisées et procéder à la mise à jour rapide de l'une d'elles sans toucher au terminal de l'utilisateur.

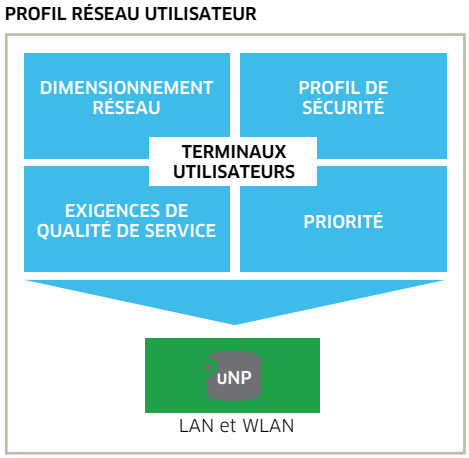
Pour terminer, WorkSpace supprime les problèmes de responsabilité d'entreprise en empêchant les équipes informatiques d'accéder aux données personnelles des utilisateurs. Avec WorkSpace, les équipes informatiques peuvent effacer ou verrouiller les applications et les données de l'entreprise mais n'ont aucune visibilité sur les données privées des utilisateurs.

Contrôle de la qualité de service à l'aide des profils uNP

La gestion de l'ensemble des communications d'un réseau d'entreprise doit permettre de garantir une très grande qualité de service. La combinaison des solutions Alcatel-Lucent Converged Campus Network Solution et CPPM permet aux utilisateurs de bénéficier de communications personnelles et professionnelles de qualité optimale en exploitant les attributs uniques des profils uNP.

Dans la mise en œuvre Alcatel-Lucent du BYOD, toutes les communications réseau sont gérées en contexte à l'aide des informations associées aux différents utilisateurs, applications et terminaux. Il faut pour cela créer des profils réseau utilisateur (uNP) en fonction de chaque combinaison salarié/terminal/application. Le profil uNP est prédéfini pour spécifier les paramètres de sécurité et de qualité de service affectés à un utilisateur dans une situation particulière. Les commutateurs deviennent les points d'application des paramètres de sécurité et de qualité de service. Le profil uNP peut également affecter l'appartenance à un réseau VLAN. (Figure 8).

Figure 8. Lors de la mise en œuvre Alcatel-Lucent du BYOD, les conversations réseau sont gérées en fonction des profils utilisateur réseau (uNP)



À l'aide de ces informations, le réseau peut identifier les utilisateurs et les terminaux et les lier à un profil uNP. Ce processus permet au réseau de comprendre chaque communication et de s'adapter automatiquement à certaines exigences spécifiques. Le réseau peut également détecter automatiquement la localisation d'un utilisateur ou d'un terminal en surveillant le trafic à partir d'un port de routeur spécifique. Il peut alors répondre automatiquement aux besoins de l'utilisateur et du terminal connecté à ce port, y compris fournir les paramètres de sécurité et de qualité de service. Il peut enfin identifier les communications d'un utilisateur et d'un terminal donnés comme devant faire l'objet d'un suivi de qualité de service.

Gestion unifiée des accès et des communications

La gestion unifiée des communications et des accès basée sur les profils uNP est assurée à l'aide de la technologie de virtualisation de réseau et de la topologie de réseau plate et simplifiée qui sont au cœur de la solution Converged Campus Network Solution d'Alcatel-Lucent (Figure 9). Cette architecture est conçue pour améliorer la résilience et optimiser l'utilisation des ressources réseau. Elle comprend tous les éléments nécessaires à la gestion efficace des accès unifiés et au principe d''Application Fluency :

- Capacité à gérer les communications en contexte, à l'aide des profils uNP intégrés dans les commutateurs de la couche d'accès ;
- Commutateurs de couche d'accès configurés pour détecter et contrôler les communications et pour gérer la qualité de service permettant de garantir une expérience utilisateur de qualité optimale ;
- Couche d'orchestration des services, qui permet aux applications et aux terminaux de détecter des services sur le réseau. Elle propose un portail commun de fourniture et de contrôle des services afin de garantir l'interopérabilité (y compris la capacité à partager un cadre d'application des politiques).

Figure 9. Architecture plate et simplifiée de la solution Converged Campus Network Solution d'Alcatel-Lucent

Le cœur de réseau 10 et 40 GigE de l'architecture est géré par les commutateurs LAN OmniSwitch™ 10K et OmniSwitch 6900. Ces commutateurs procèdent à l'analyse et au traitement de différents types de trafic sur la base d'une classification granulaire établie à l'aide des profils uNP. Les entreprises peuvent affecter des priorités en fonction des applications, des utilisateurs ou de la combinaison des deux. L'architecture distribuée traite le trafic en entrée et permet de l'acheminer intelligemment vers d'autres éléments en évitant le goulot d'étranglement central. Elle permet également aux entreprises de faire évoluer leur environnement pour répondre à l'augmentation des besoins, sans compromettre la performance et les capacités de bande passante.

Le réseau convergent comprend une couche d'accès unifiée où une infrastructure de politiques unique, un mode d'authentification commun, une base de données utilisateurs unique et un ensemble unique de variables de localisation s'appliquent à tous les terminaux, mobiles et fixes.

L'accès réseau fixe est fourni par les gammes de commutateurs LAN empilables OmniSwitch 6850E et OmniSwitch 6855 renforcés, OmniSwitch 6450 et OmniSwitch 6250. L'accès mobile est assuré par les points d'accès mobiles, connectés directement pour accéder aux commutateurs de la couche d'accès, et le contrôle est assuré par les solutions LAN mobiles OmniAccess™ 6000/4000. Des technologie IAP (points d'accès instantanés), avec des fonctions de contrôle virtualisées intégrées dans les points d'accès, sont également disponibles.

CONCLUSION

Parce qu'un nombre accru d'entreprises se demandent comment exploiter les programmes Bring Your Own Device (BYOD) pour améliorer la productivité, il est nécessaire que les équipes informatiques soient suffisamment flexibles pour développer des solutions personnalisées, adaptées aux besoins des entreprises.

La mise en œuvre Alcatel-Lucent du BYOD avec la solution Alcatel-Lucent Converged Campus Network Solution offre aux responsables informatiques la flexibilité nécessaire pour adopter immédiatement une stratégie BYOD et l'adapter à l'évolution des exigences. Cette solution est conçue pour gérer l'ensemble des besoins de contrôle d'accès de l'entreprise et pour informer l'infrastructure réseau de l'entreprise des droits et capacités de bande passante autorisés en fonction de l'utilisateur et du terminal. À partir de là, l'infrastructure Alcatel-Lucent gère les droits réseau, tout en assurant le contrôle permanent de l'état de santé et de la conformité de chaque terminal. Ce niveau de contrôle peut être configuré pour tous les salariés, sous-traitants et invités qui accèdent au réseau fixe ou mobile.

L'architecture AFN (Application Fluent Network) avancée, qui est au cœur de la solution Alcatel-Lucent pour le BYOD, est conçue pour communiquer directement avec tous les éléments réseau de l'entreprise, pour collecter les données utilisateur stratégiques et pour fournir des instructions concernant les profils uNP à utiliser en fonction de la combinaison utilisateur/terminal. Le profil réseau peut intégrer de nombreux paramètres (pare-feux, gestion de bande passante, détection des anomalies du trafic, identité VLAN, etc.) afin de garantir la qualité d'expérience utilisateur.

À l'encontre des autres solutions BYOD, la mise en œuvre Alcatel-Lucent du BYOD est parfaitement adaptée aux deux types de terminaux mobiles et fixes qui se connectent au réseau. Elle fournit un ensemble complet de fonctions de correction, de filtrage des applications, de contrôle permanent de la sécurité et de comptes rendus de gestion. Enfin, elle est conçue pour s'adapter aux invités qui se connectent au réseau de nombreuses façons différentes (y compris pour les accès sponsorisés et non sponsorisés) et garantir une gestion, une protection et un accès adaptés.

Cette approche évolutive fonctionne avec une grande diversité de terminaux. Elle procure à l'utilisateur final davantage de liberté, tout en assurant la sérénité des responsables réseau.

SIGLES ET ACRONYMES

AFN	Application Fluent Network
BYOD	Bring Your Own Device
LAN	Local Area Network - Réseau LAN
MAM	Mobile Application Management - Gestion des applications mobiles
NAC	Network Access Control - Contrôle des accès réseau
NAP	Network Access Protection - Protection des accès réseau
QoS	Quality of Service - Qualité de service
RADIUS	Remote Authentication Dial In User Service
TACACS+	Terminal Access Controller Access-Control System Plus
uNP	User Network Profile - Profil uNP
VLAN	Virtual Local Area Network - Réseau VLAN
VPN	Virtual Private Network - Réseau VPN
WLAN	Wireless Local Area Network - Réseau WLAN

Alcatel·Lucent
Enterprise