

SonicWall assure le VPN pour l'iPad

Les entreprises doivent faire face à la multiplication de leurs employés qui utilisent des appareils Apple iPad et iPhone. Largement plébiscités, ils sont très recherchés même par les professionnels qui n'hésitent pas à transgresser les règles d'usages de l'entreprise, voire à se détourner du matériel fourni par cette dernière, pour disposer de « leur » iPhone... Un phénomène qui ne peut qu'aller en s'accroissant avec les pratiques du « *buy it yourself* » (BIY) ou du « *bring your own device* » (BYOD) qui laissent l'employé acquérir lui-même le matériel sur lequel il souhaite travailler.

l'ipad et l'iPhone sont également un facteur d'innovation, de puissants outils de mobilité qui dépassent la simple téléphonie et sur lesquels de plus en plus d'éditeurs développent des interfaces de consultation ou de saisie. Dans ces conditions, l'entreprise doit prendre en compte ce maillon terminal désormais incontournable de la chaîne qui la relie à ses employés mobiles. Mais elle doit en revanche s'assurer que l'accès aux ressources de son réseau est sécurisé.

La sécurité du VPN SSL unifié

Pour SonicWall, concepteur d'appareils pare-feu (firewall) de nouvelle génération, la reconnaissance des iPad et iPhone et la sécurisation de l'accès doivent être mis en place dès le pare-feu. Une application SonicWall Mobile Connect est à télécharger sur l'App Store. Lorsque qu'un mobile se présente à l'entrée du réseau sécurisé par le pare-feu, celui-ci détecte Mobile Connect, ouvre la connexion VPN SSL et chiffre le trafic. Les données qui transitent en dehors de l'entreprise du ou vers le smartphone ou la tablette sont alors ainsi rendues inexploitablement par les personnes qui chercheraient à les intercepter.

Les administrateurs peuvent également activer les services sécuritaires complémentaires proposés sur les appareils de SonicWall, comme Clean VPN – analyse antivirus, anti-spyware et prévention des intrusions sur les connexions VPN, ce qui permet aux utilisateurs d'iOS de bénéficier du même niveau de protection que s'ils se trouvaient dans le périmètre réseau et avec la garantie que les communications relayées par les appareils ne soient pas infectées – ou Application Intelligence and Control pour déterminer quelles applications iOS doivent disposer en priorité de la bande passante pour assurer la performance de la communication.

Une solution complémentaire

SonicWall Mobile Connect vient compléter Clean Wireless, la solution de chiffrement des données, antivirus, anti-spyware et de prévention des intrusions, et les services de filtrage de contenu pour garantir le respect des règles de conformité au niveau de la passerelle sur les réseaux Wi-Fi, qui couvre les appareils qui se connectent sans fil dans l'entreprise. Avec cette extension, l'entreprise assure à ses utilisateurs une protection étendue aux déplacements ou aux accès au réseau à partir de bornes Internet publiques.

« Les iPad et iPhone sont de loin les appareils les plus privilégiés par les employés qui veulent pouvoir travailler partout et à tout moment, indique **Patrick Sweeney**, vice-président of product management and corporate marketing chez SonicWALL. *Mobile Connect App* permet d'étendre les règles de sécurité aux

personnes se connectant en dehors du périmètre réseau protégé et de répondre ainsi aux exigences strictes en la matière des entreprises, services publics ou établissements scolaires. Cela ne peut que favoriser la productivité. »