aruba
a Hewlett Packard Enterprise company

PRÉSENTATION POUR DIRIGEANTS D'ENTREPRISE

IDENTIFIER, CONNCTER ET PROTÉGER LES MOBILES ET LES OBJETS IOT EN PÉRIPHÉRIE

INTRODUCTION

Le nombre d'objets IoT connectés aux réseaux d'entreprise fait apparaître de nombreux défis pour le personnel IT, qui doit trouver un équilibre entre les avantages des bâtiments intelligents et les risques posés par l'intégration d'un nombre considérable de terminaux inconnus dans leur environnement sans toujours avoir à disposition les outils appropriés pour identifier, profiler et authentifier ces différents terminaux en mode automatique, puis leur appliquer les politiques appropriées.

Les produits annoncés récemment par Aruba s'attaquent à ces défis à travers une approche en quatre étapes de la connectivité des objets IoT en périphérie : Identifier les équipements présents dans le réseau – Connecter les terminaux mobiles et les objets IoT à des commutateurs intelligents – Protéger le réseau à travers une administration performante des politiques – Innover en faisant appel à notre écosystème de partenaires de manière à assurer la sécurité de bout en bout.

LES DÉFIS DE L'ILOT

L'explosion des terminaux mobiles et l'adoption croissante de bâtiments intelligents (« immotique ») font apparaître des défis considérables pour le département IT et pour les dirigeants de l'entreprise.

Manque de visibilité – Savez-vous vraiment quels équipements sont présents dans votre réseau ?

La sécurité commence par l'identification des équipements présents dans le réseau : smartphones non gérés, terminaux inconnus, objets IoT, etc. En effet, ceux-ci augmentent la surface d'attaque et menacent la sécurité de l'entreprise. La capacité de voir tous les équipements présents dans un réseau permet au département IT de mieux comprendre comment celui-ci est utilisé. Le département IT doit être en mesure d'identifier et de profiler chaque terminal qui se connecte au réseau, quel que soit le point de connexion utilisé. Cet objectif devient de plus en plus difficile avec la prolifération des objets IoT filaires/sans fil qui se connectent aux réseaux. Tous les terminaux et objets doivent être profilés et évalués au moment de leur connexion et classés dans une catégorie, l'accès au réseau leur étant automatiquement accordé ou refusé en fonction de leur type, de leur statut de propriété ou de leur système d'exploitation.

Les connexions filaires, la nouvvelle préoccupation

Pour les entreprises commerciales et industrielles, la proportion d'objets IoT filaires peut varier entre 35 % et plus de 50 % (en fonction de leur marché vertical) : détecteurs de mouvement, matériel médical, contrôleurs de processus en atelier, etc. Dans le passé, les discussions relatives aux solutions de contrôle des accès au réseau (NAC) se limitaient généralement aux méthodes permettant de sécuriser un réseau sans fil, parce que c'est ainsi que la plupart des terminaux se connectaient. Les connexions sécurisées, limitées à une session, étaient devenues une exigence, dans la mesure où les captures de transmissions sans fil et les utilisateurs inconnus pouvaient accéder au réseau dès qu'ils étaient à portée d'un point d'accès et d'un identifiant SSID non sécurisés.

Cette priorité données à la sécurisation des réseaux sans fil impliquait que la protection des réseaux filaires était délaissée : leurs commutateurs étant installés derrière des protections solides, ils ne semblaient pas présenter les mêmes vulnérabilités que les réseaux sans fil. Malheureusement, avec la croissance des réseaux filaires, la qualité des commutateurs s'est détériorée, laissant de nombreux ports ouverts et accessibles à tous. Les ports présents dans les salles de réunion et dans les locaux des imprimantes sont des exemples classiques de sécurité aléatoire. Les objets IoT étant de plus en plus souvent connectés en filaire, il devient nécessaire d'accorder le même niveau d'attention à la sécurisation des infrastructures filaires.

Les infrastructures filaires traditionnelles n'ont pas été optimisées pour l'IoT.

Dans les anciens environnements de commutation, les employés n'étaient pas mobiles et l'ilot était... sans objet ! Les ressources étaient protégées derrière un pare-feu, et le département IT devait simplement s'assurer de la protection du périmètre. Avec l'irruption massive des objets IoT, il devient nécessaire de déployer des infrastructures filaires aussi intelligentes que le sans fil. Autrement dit, les commutateurs du 21e siècle doivent disposer de mécanismes de sécurité et de gestion intelligente du réseau pour permettre aux objets IoT de se connecter en toute sécurité et en toute transparence.

La protection du réseau exige des workflows automatisés

Face à des dizaines ou des milliers de mobiles et d'objets IoT inconnus qui se connectent au réseau d'entreprise au quotidien, il est impossible de définir et d'appliquer manuellement des politiques capables de tenir compte de tous les types de terminaux/ Il est donc nécessaire d'automatiser le processus d bout en bout afin de réduire les risques sans surcharger le département IT. Par ailleurs, les terminaux statiques (non mobiles) et l'infrastructure elle-même doivent également être profilés et contrôlés pour détecter tout changement suspect. Si le comportement d'un terminal semble suspect, il doit être automatiquement mis en quarantaine jusqu'à ce que la menace ait été évaluée.

Devancer les pirates, une initiative coûteuse

Les piratages massifs de données sont désormais monnaie courante. Pour les entreprises, les investissements en sécurité sont coûteux et chronophages, et il est pratiquement impossible de garder un temps d'avance sur les pirates à travers la seule innovation. L'écosystème de partenaires Aruba permet de demander à des spécialistes en sécurité ultra-compétents de définir une solution de sécurité de bout en bout.

PROPOSITION ARUBA POUR UNE CONNECTIVITÉ SÉCURISÉE DES OBJETS IOT À LA PÉRIPHÉRIE

1. Identifier et profiler les terminaux et les objets IoT inconnus dans les réseaux filaires/sans fil hétérogènes

La sécurité d'un réseau commence par la découverte des équipements présents dans celui-ci. Les entreprises doivent donc disposer d'une solution leur permettant d'identifier et de profiler tous les types d'équipement. La famille de produits Aruba ClearPass offre un avantage unique par rapport à la concurrence : un profilage en temps réel et sans agents, sous forme d'appliance physique autonome ou de solution logicielle complète assurant la mise en application de politiques.

Ces deux solutions permettent d'identifier en continu les terminaux et les équipements présents dans les réseaux filaires/sans fil (supportant ou non le protocole AAA) et via des adresses IP dynamiques ou statiques.
Les graphiques des tableaux de bord permettent de déterminer le nombre total de terminaux et leur répartition par catégorie, famille et type de terminal.

Notre nouveau produit Aruba ClearPass Universal Profiler se présente sous la forme d'une appliance virtuelle autonome qui peut être déployées et active en quelques minutes. Elle s'adresse aux entreprises qui ne sont pas prêtes pour une solution NAC complète, ou pour les sites distants ou sous-équipés dans lesquels aucune solution NAC n'a été déployée. Universal Profiler est une solution simple et peu coûteuse pour identifier et profiler les équipements présents dans un réseau.

Aruba ClearPass Policy Manager se présente sous la forme d'une appliance physique ou virtuelle qui assure les services suivants : profilage complet, mise en application des politiques filaire/sans fil dans les réseaux AAA et non AAA, supervision de l'accès des invités, intégration des terminaux en mode BYOD, évaluation des terminaux, reporting complet et solution tierce de sécurité et d'optimisation de l'expérience utilisateur.

2. Connexion des objets IoT avec intelligence automatisée

L'adoption croissante des bâtiments intelligents (« immotique ») oblige les entreprises à déployer une infrastructure filaire plus intelligente.
Les améliorations apportées au commutateur ArubaOS-Switch ont été conçues pour permettre de disposer d'une périphérie intelligente et optimisée pour l'accueil des mobile et des objets IoT. Ces améliorations permettent de définir un accès unifié en fonction des rôles dans les réseaux filaires/sans fil, avec la capacité d'identifier et d'assigner des rôles aux objets IoT connectés afin de prioriser les applications critiques et de sécuriser les réseaux.

Les commutateurs Aruba Layer 3 sont également capables de tunnéliser le trafic filaire en fonction des utilisateurs et des ports et de le diriger vers un contrôleur de mobilité (Mobility Controller) qui assure les fonctionnalités suivantes : mise en application des politiques, livraison de services avancés, cryptage du trafic visant à sécuriser le LAN. Pour faire face à la croissance rapide des objets IoT et des terminaux connectés dans les entreprises multisite, nous proposons une solution peu coûteuse : le commutateur Aruba 2540, qui supporte le provisionnement automatisé (« zero touch ») et, en option, une solution d'administration en cloud qui permet la simplification et la réduction des coûts de déploiement et d'administration des réseaux.

3. Protéger les réseaux avec des politiques intelligentes

Dès que vous maîtrisez la visibilité des terminaux en réseau, vous devez vous préoccuper de la mise en application automatique des politiques.
Aruba ClearPass Policy Manager vous aide dans ces deux tâches : identifier les équipements présents dans le réseau et mise en application des politiques et des workflows automatisés dans les infrastructures filaires/sans fil hétérogènes. Avec les solutions ClearPass, vous êtes prêt pour vos opérations réseau : profilage, mise en application des politiques, gestion de l'accès des invités, intégration des mobiles en mode BYOD, etc. Par ailleurs, ces solutions offrent de nombreux avantages, dont réduire la charge de travail du département IT, garantir une protection plus efficace contre les menaces et améliorer l'expérience globale des utilisateurs. Pour répondre aux nouveaux besoins de sécurisation des infrastructures filaires, la fonctionnalité OnConnect utilise les protocoles existants des commutateurs pour assurer le blocage des ports filaires présents dans des emplacements vulnérables tels que les salles de réunion, les téléphones en mode VoIP et les locaux des imprimantes.

4. Accélérer l'innovation pour améliorer la sécurité à la périphérie

L'écosystème technologique d'Aruba propose des solutions de sécurité performantes qui s'intègrent avec ClearPass Exchange pour assurer la sécurité de bout en bout et de la périphérie au cœur. Quelques partenariats récents en matière de sécurité des objets IoT :

- La solution Niara analyse les tendances de trafic associées à différents types de terminaux pour identifier les comportements suspects, puis demande à ClearPass de supprimer du réseau le ou les terminaux incriminés.
- La solution Attivo permet au département IT de créer des objet IoT de type « faux virtuel » pour réagir face aux pirates qui utilisent des faux terminaux pour attaquer un réseau. Dès que le périphérique virtuel adopte un comportement suspect, la solution Attivo demande à ClearPass de supprimer du réseau le ou les terminaux incriminés.

CONCLUSION

L'intégration et l'administration des objets IoT devient essentielle au succès des entreprises qui décident d'intégrer ces solution dans leurs opérations. Les entreprises ont besoin d'une stratégie qui remplit deux objectifs : assurer la connexion en toute sécurité des mobiles et des objets IoT à la périphérie pour profiter de la valeur et des efficacité associées aux bâtiments intelligents et assurer la sécurité des réseaux et des ressources de l'entreprise. En ce qui concerne la connectivité des objets IoT, l'approche Aruba en quatre étapes répond aux défis actuels : identifier les équipements présents dans les réseaux, connecter les terminaux à travers des solutions filaires/sans fil intelligentes, protéger les réseaux par administration automatisée des politiques et faire appel à notre écosystème de partenaires pour renforcer la sécurité de bout en bout et anticiper les risques potentiels.

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089 (USA)
(+1 844) 473 27 82 | TÉL. : 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com EB_MobileIoTEdge_111616