PRÉSENTATION GÉNÉRALE DE LA SOLUTION

Aruba ESP et la sécurité Zero Trust

La sécurité en périphérie

Les défis en matière de sécurité du réseau ont grandement évolué ces dernières années, puisque les utilisateurs se sont peu à peu décentralisés et que les attaques sont devenues plus sophistiquées et persistantes. Les approches traditionnelles de la sécurité axée sur le périmètre du réseau sont désormais inefficaces en tant que stratégies de sécurité distinctes. La sécurité des réseaux modernes doit s'adapter à des utilisateurs et des appareils qui évoluent sans cesse, ainsi qu'à des menaces beaucoup plus présentes qui ciblent des zones autrefois « fiables » de l'infrastructure réseau.

La solution Zero Trust a émergé comme modèle efficace pour mieux répondre aux exigences de sécurité changeantes dans l'entreprise moderne en supposant que tous les utilisateurs, appareils, serveurs et segments réseau sont par nature fragiles et potentiellement hostiles. Aruba ESP et la sécurité Zero Trust améliorent la position globale en matière de sécurité du réseau en appliquant un ensemble plus rigoureux de meilleures pratiques et contrôles de sécurité à des ressources réseau autrefois considérées comme fiables.

ARUBA ESP : PRINCIPES CLÉS DU ZERO TRUST

Le Zero Trust varie énormément en fonction du domaine de sécurité envisagé. Bien que les contrôles au niveau de l'application soient un axe principal du Zero Trust, une stratégie complète doit également englober la sécurité du réseau et le nombre croissant d'appareils connectés, y compris l'environnement de télétravail. Aruba ESP et la sécurité Zero Trust incluent une visibilité complète, une micro-segmentation et des contrôles avec des accès restreints, et une surveillance et une application en continu. Les solutions de VPN traditionnelles sont également plus efficaces lorsque les contrôles appliqués aux réseaux de campus et de filiales sont identiques à ceux destinés au télétravail ou aux salariés à distance.

À l'ère de l'IoT, les principes de base d'une bonne sécurité du réseau sont souvent difficiles à mettre en œuvre. Si possible, tous les appareils et utilisateurs doivent être identifiés et correctement authentifiés avant d'avoir accès au réseau. Outre l'authentification, les utilisateurs et les appareils doivent disposer

d'un accès aussi limité que possible pour effectuer leurs activités critiques une fois qu'ils sont sur le réseau. Cela signifie contrôler quel utilisateur ou appareil a accès à quelle ressource réseau ou application. Pour terminer, toutes les communications entre les utilisateurs finaux et les applications doivent être chiffrées.

À LA RECHERCHE D'UNE VISIBILITÉ GLOBALE

Avec l'adoption croissante de l'IoT, la visibilité totale de tous les appareils et utilisateurs sur le réseau est devenue une tâche complexe. Sans visibilité, les contrôles de sécurité critiques qui soutiennent le modèle Zero Trust sont difficiles à appliquer. L'automatisation, le machine learning basé sur l'IA et la possibilité d'identifier rapidement les types d'appareils sont essentiels.

Aruba ClearPass Device Insight utilise une combinaison de techniques de profilage et de découverte passives et actives pour détecter le spectre complet des appareils connectés ou tentant de se connecter au réseau. Cela inclut les appareils basés sur l'utilisateur tels que les ordinateurs portables et tablettes. La solution est cependant différente des outils traditionnels dans sa capacité à identifier l'éventail varié des objets connectés qui sont de plus en plus omniprésents sur les réseaux actuels.

RESTRICTION DES ACCÈS ET MICRO-SEGMENTATION

Une fois la visibilité en place, l'application des meilleures pratiques de Zero Trust associée à la « restriction des accès » et à la micro-segmentation sont des étapes clés. Cela signifie utiliser la meilleure méthode d'identification possible pour chaque terminal sur le réseau (c'est-à-dire une authentification 802.1x et multi-facteurs complète pour les appareils des utilisateurs) et appliquer la politique de contrôle des accès qui autorise uniquement l'accès à des ressources absolument nécessaires pour cet appareil ou utilisateur.

Aruba ClearPass Policy Manager permet la création de politiques d'accès basé sur les rôles qui permettent aux équipes informatique et sécurité de mettre en œuvre ces meilleures pratiques en utilisant un rôle unique et les privilèges d'accès associés appliqués partout sur l'infrastructure de réseau filaire ou sans fil, dans les filiales ou sur les campus. Une fois profilés, les appareils sont automatiquement associés à une politique de contrôle des accès et segmentés vis-à-vis des autres appareils via les capacités de segmentation dynamique d'Aruba. Le pare-feu d'application de la politique (PEF) d'Aruba, un pare-feu applicatif complet intégré dans l'infrastructure réseau d'Aruba, se charge de la mise en application. L'infrastructure Aruba utilise également les protocoles de chiffrement les plus sécurisés tels que la norme WPA3 sur les connexions réseau sans fil.

ClearPass Policy Manager intègre également des solutions d'authentification variées permettant d'utiliser l'authentification multi-facteurs et la capacité à forcer la réauthentification à des points clés du réseau. À travers l'écosystème ClearPass, les clients peuvent facilement intégrer d'autres solutions pour respecter les exigences Zero Trust liées aux informations contextuelles et d'autres données télémétriques de sécurité.

Cela signifie que ClearPass peut s'intégrer dans diverses solutions telles que les outils Endpoint Security pour prendre des décisions de contrôle des accès intelligentes en fonction de la position de l'appareil. Les politiques de contrôle des accès peuvent également être modifiées en fonction du type d'appareil utilisé, du lieu de connexion de l'utilisateur et d'un critère basé sur le contexte.

SURVEILLANCE ET APPLICATION EN CONTINU

Outre le contrôle des accès basé sur des rôles pour appliquer la segmentation granulaire, la surveillance continue des utilisateurs et des appareils sur le réseau fait également partie des meilleures pratiques Zero Trust. Cela permet de traiter les risques associés aux menaces internes, aux maliciels avancés ou aux menaces persistantes qui ont contourné les limites du périmètre traditionnel.

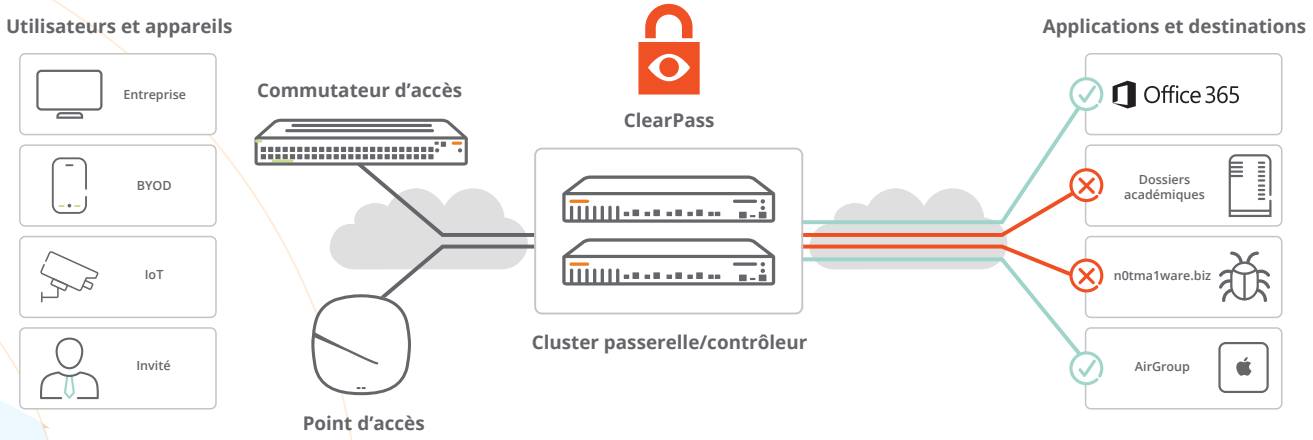

Illustration 1 : Aruba ClearPass attribue automatiquement des stratégies de contrôle d'accès basées sur des rôles, appliquées à l'aide de la segmentation dynamique

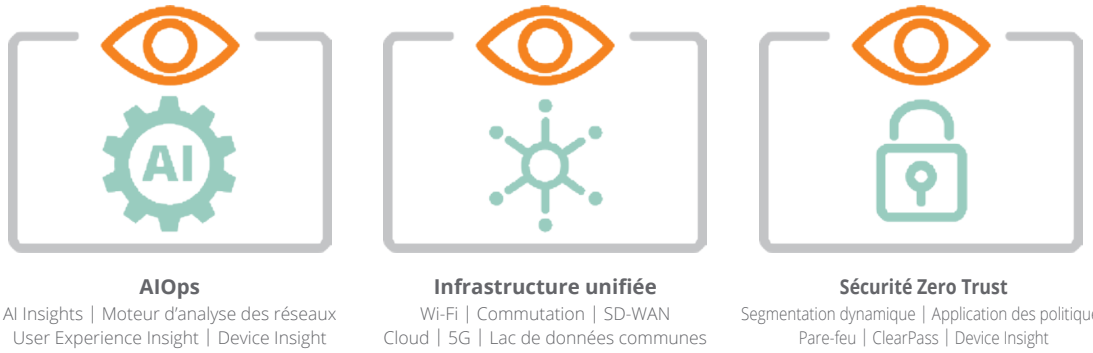

Illustration 2 : la sécurité Zero Trust est un pilier essentiel d'Aruba ESP

Défense contre les menaces avec l'IDS/IPS

Les capacités de défense contre les menaces d'Aruba protègent contre diverses menaces, notamment le hameçonnage, le déni de service (DoS) et les attaques croissantes par ransomware. Les passerelles SD-WAN Aruba 9000 effectuent une détection et une prévention des intrusions basée sur les identités (IDS/IPS), en collaborant avec Aruba Central, ClearPass Policy Manager et le pare-feu d'application des politiques. Les fonctions IDS/IPS basées sur des identités effectuent une inspection du trafic basée sur des signatures et des modèles, à la fois sur le trafic LAN (horizontal) de la succursale et sur le trafic SD-WAN (vertical) qui traversent la passerelle afin de garantir une sécurité réseau intégrée en succursale. Un tableau de bord de sécurité avancé dans Aruba Central fournit aux équipes informatiques une visibilité sur tout le réseau, des métriques de menaces multi-dimensions, des données d'évaluation des menaces, ainsi qu'une corrélation et une gestion des incidents. Les événements de menaces sont envoyés aux systèmes SIEM et à ClearPass pour correction.

360 Security Exchange

Avec plus de 150 intégrations constituées des meilleures solutions de sécurité incluant les ensembles d'outils Security Operations and Response (SOAR), ClearPass Policy Manager est capable d'appliquer dynamiquement les accès en fonction de la télémétrie des menaces en temps réel en provenance de multiples sources. Il est possible de créer des politiques pour prendre des décisions de contrôle des accès en temps réel basées sur les alertes des Next-Gen Firewalls (NGFW), des outils Security Information and Event Management (SIEM) et d'autres sources. Les actions ClearPass sont entièrement configurables avec par exemple l'accès limité (Internet uniquement) ou la suppression d'un appareil du réseau pour correction.

ARUBA ESP (EDGE SERVICES PLATFORM)

Pour aider nos clients à exploiter les opportunités en périphérie, nous avons développé Aruba ESP, la première plateforme pilotée par l'IA du secteur conçue pour unifier, automatiser et sécuriser en périphérie. La sécurité Zero Trust est un composant clé d'Aruba ESP, et une fois associé à AIOps et à une infrastructure unifiée, elle permet aux entreprises de réduire les coûts, de simplifier les opérations et de se protéger.

SYNTHÈSE

Aujourd'hui, l'environnement de réseau et le paysage des menaces nécessitent une autre approche. La sécurité du réseau axée sur le périmètre autrefois utilisée n'a pas été conçue pour le personnel itinérant et les objets connectés émergents modernes. Aruba ESP et la sécurité Zero Trust fournissent un éventail complet de capacités, notamment la visibilité, le contrôle et l'application, pour répondre aux exigences d'une infrastructure réseau pilotée par l'IoT et décentralisée.

aruba
a Hewlett Packard Enterprise company

SO_ZeroTrustSecurity_051120 a00097694fre