aruba
a Hewlett Packard Enterprise company

PRÉSENTATION GÉNÉRALE DE LA SOLUTION

ARUBA CLEARPASS POLICY MANAGER

Visibilité et sécurité des accès en mode filaire et sans fil

Vous souvenez-vous du temps où le département IT était le gardien de l'environnement et imposait à la fois des politiques très strictes et un écosystème ultra-protégé ? Aujourd'hui, ce mode de fonctionnement n'a plus lieu d'être. Aujourd'hui, les terminaux de l'entreprise et les terminaux personnels des utilisateurs sont connectés aussi bien à l'intérieur qu'à l'extérieur du périmètre de sécurité.

Les ordinateurs portables, les smartphones, les tablettes et les objets IoT sont en train d'envahir le lieu de travail. La première étape pour sécuriser vos données ? Identifier les personnes connectées au réseau ! La mise en application automatisée de politiques de sécurité adaptées garantit que seuls les utilisateurs et les terminaux autorisés sont connectés. En outre, une protection en temps réel contre les menaces est nécessaire pour sécuriser l'environnement et pour respecter les exigences de conformité et d'audit interne/externe.

Autre inconvénient : l'utilisation d'objets IoT et de dans les réseaux câblés et sans fil est en train de mobiliser l'attention du département IT. La plupart des entreprises ont déjà sécurisé leurs réseaux sans fil et leurs terminaux mobiles, mais elles ont tendance à négliger les ports câblés qui se nichent dans les salles de conférence, les téléphones en mode VoIP et les locaux des imprimantes. Et dans la mesure où les objets IoT ne sont pas toujours dotés d'attributs de sécurité et où ils doivent accéder au réseau de l'entreprise à travers des ressources à administration externe, les connexions par câble présentent de nouveaux risques.

Tout en s'efforçant de garder le contrôle global, le département IT doit s'équiper d'outils permettant de programmer rapidement l'infrastructure sous-jacent et de contrôler les accès au réseau de tous les objets IoT et de tous les mobiles – connus ou inconnus. Pour être performante, une solution de sécurité des accès doit assurer de nombreuses fonctionnalités : profilage, mise en application des politiques, gestion de l'accès des invités, intégration des terminaux en mode BYOD, etc. Ce type de solution offre par ailleurs 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.

LA MOBILITÉ ET L'IT SONT EN TRAIN DE CHANGER NOTRE PERCEPTION DES SOLUTIONS NAC

Le domaine de supervision du département IT dépasse désormais les quatre murs de l'entreprise, et l'objectif des entreprises consiste à proposer une connectivité en tous lieux et 24x7 sans jamais compromettre la sécurité. Comment le département IT peut-il maintenir une visibilité suffisante et un contrôle efficace sans impacter les activités de l'entreprise et l'expérience des utilisateurs ? Il suffit d'appliquer un plan en trois étapes.

1. **Identifier** les terminaux utilisés, leur nombre, leurs points de connexion et leurs systèmes d'exploitation – c'est le point de départ. En générant des informations en continu sur les changements et sur les terminaux qui se connectent et se déconnectent vous disposerez de la visibilité requise sur la durée.
2. **Appliquer** des politiques précises qui définissent les règles d'accès des terminaux, quels que soient l'utilisateur, le type de terminal ou le point d'accès – cette étape assure l'expérience utilisateur attendue. Les entreprises doivent s'adapter à l'évolution incessante des terminaux et de leurs usages, y compris smartphones, caméras de surveillance, etc.
3. **Protéger les ressources** en appliquant des contrôles de politiques dynamiques et en luttant contre les menaces en temps réel s'appliquant également aux systèmes tiers. C'est la dernière pièce du puzzle. Être préparé pour un événement réseau inhabituel à trois heures du matin exige une approche unifiée capable de bloquer certains flux de trafic et de modifier l'état de connexion d'un terminal.

Les entreprises doivent se préparer aussi bien pour les défis existants et pour les situations inattendues. Il n'est pas réaliste de compter sur le département IT ou sur le service d'assistance pour intervenir manuellement chaque fois qu'un utilisateur décide de travailler à distance ou d'acheter un nouveau smartphone. Les solutions NAC ne sont plus limitées à l'évaluation des terminaux connus avant leur accès au réseau.

VISIBILITÉ ET ADMINISTRATION CENTRALISÉES

Les politiques ClearPass et le protocole AAA (Authentication, Authorization, Accounting) assurent le profilage des terminaux, avec interface d'administration Web, reporting complet et alertes en temps réel. Les données contextuelles collectées dans ce contexte sont exploitées pour garantir que les utilisateurs et les terminaux bénéficient des privilèges d'accès appropriés – quelles que soient la méthode d'accès utilisée et la propriété du terminal.

Un moteur de profilage intégré collecte des données en temps réel (catégories de terminal, fournisseurs, versions d'OS, etc.). Il n'est plus nécessaire de « deviner » le nombre de terminaux connectés aux réseaux câblés et sans fil. La visibilité granulaire permet de disposer des données nécessaires pour les audits et pour déterminer les zones présentant des risques en matière de performances ou de sécurité.

LA PUISSANCE DE CLEARPASS EXCHANGE

L'appliance virtuelle autonome ClearPass Universal Profiler propose la même visibilité de profilage que la version complète. Elle s'adresse aux entreprises qui ne sont pas prêtes pour la mise en application d'un ensemble complet de politiques ou pour les sites distants dans lesquels la version complète de ClearPass ne peut pas être déployée immédiatement.

En appliquant des modèles, le département IT peut définir des politiques filaires/sans fil qui tiennent compte de nombreux paramètres dont rôles des utilisateurs, types de terminaux, données d'administration des mobiles (MDM/EMM), statut des certificats, points de connexion, jours de la semaine, etc. Les politiques peuvent imposer des règles pour différentes catégories d'utilisateurs (employés, étudiants, médecins, invités, dirigeants, etc.) et pour les différents types de terminaux que ces utilisateurs décident d'apporter dans l'entreprise.

ClearPass OnConnect est une fonctionnalité qui permet de verrouiller les ports câblés qui appliquent des politiques différentes du protocole AAA. Aucune configuration n'est nécessaire au niveau des terminaux : il suffit de déclarer dans le commutateur une instruction globale (en ligne de commande). Les protocoles standard AAA et 802.1X sont également supportés pour les réseaux câblés et sans fil.

Ces différentes qualités permettent d'appliquer des politiques homogènes et une protection de bout en bout que les autres solutions en silos (AAA, NAC) ne peuvent pas assurer. La capacité de ClearPass d'utiliser plusieurs gisements d'identité dans un seul service de politiques (par exemple, Microsoft Active Directory, annuaires au standard LDAP, bases de données SQL compatibles ODBC, serveurs de jetons/tokens et bases de données internes) est l'un des avantages de ce produit Aruba par rapport aux solutions legacy.

PROVISIONNEMENT DES TERMINAUX SANS INTERVENTION DU DÉPARTEMENT IT

L'administration des terminaux personnels (BYOD) risque d'exercer une pression supplémentaire sur le département IT ou/et sur le service d'assistance et de faire apparaître des problèmes de sécurité.

Avec ClearPass Onboard, les utilisateurs peuvent configurer leurs terminaux en toute indépendance avant de les utiliser dans des réseaux sécurisés. Des certificats adaptés à chaque type de terminal évitent aux utilisateurs la saisie répétée de leurs informations d'identification tout au long de la journée (un avantage incontestable !). L'utilisation de certificats propose un mécanisme de sécurité supplémentaire.

L'équipe IT définit les principaux paramètres : qui peut intégrer des terminaux, les types de terminaux autorisés, le nombre de terminaux par personne. Une autorité de certification intégrée permet au département IT d'intégrer immédiatement les terminaux personnels (indicateur PKI interne), et aucune autre ressource IT n'est nécessaire.

Accès simple et rapide pour les invités

Le BYOD ne se limite pas aux terminaux des employés : il doit également prendre en compte les visiteurs dont le terminal doit accéder au réseau – avec ou sans fil. Le département IT doit disposer d'un modèle très simple qui « pousse » le terminal sur un portail dédié, qui automatise le provisionnement des informations d'identification et qui applique des mécanismes de sécurité pour cloisonner le trafic de l'entreprise.

La fonctionnalité ClearPass Guest permet à différents acteurs (employés, réceptionnistes, animateurs d'événements et autres membres du personnel non IT) de créer des comptes d'accès réseau temporaires pour tous leurs invités du jour. La mise en cache des adresses MAC facilite également les activités des invités : ils peuvent se connecter facilement tout au long de la journée sans avoir à entrer leurs informations d'identification à plusieurs reprises sur le portail des invités.

Par ailleurs, une fonctionnalité d'auto-enregistrement évite l'intervention des employés et permet aux invités de générer leurs propres informations d'identification. Les informations d'identification sont livrées aux invités sous forme de badges imprimés ou par SMS/mail. Les informations d'identification peuvent être stockées dans ClearPass pendant une période définie, ou configurées pour expirer automatiquement au-delà d'un certain nombre d'heures ou de jours.

Accès en fonction de l'état des terminaux

Pendant le processus d'autorisation, il pourra être nécessaire d'évaluer l'état de certains terminaux pour s'assurer qu'ils respectent les politiques internes en matière d'anti-virus, d'anti-spyware et de pare-feu. Cette automatisation motive les utilisateurs à exécuter une analyse antivirus avant de se connecter au réseau de l'entreprise.

ClearPass OnGuard dispose de fonctionnalités qui vérifient l'état de santé des terminaux en fonction des données échangées, ce qui permet d'éliminer les vulnérabilités de la plupart des types et des versions des systèmes d'exploitation. Face à des clients persistants ou éphémères, ClearPass peut identifier les terminaux conformes dans les infrastructures filaires, sans fil et VPN.

Exemples de contrôles d'état qui apportent une sécurité complémentaire :

- Administrer les applications, les services et les clés de registre en mode P2P.
- Déterminer si les périphériques de stockage USB ou les instances de machines virtuelles sont autorisés.
- Gérer l'utilisation des interfaces réseau reliées par des bridges et du cryptage des disques.

Exploiter au mieux les solutions tierces.

ClearPass Exchange facilite l'automatisation de la lutte contre les menaces de sécurité ou l'amélioration des services qui utilisent des solutions tierces les plus répandues (pare-feu, MDM/EMM, MFA, enregistrement des visiteurs et outils SIEM). En s'appuyant sur les données contextuelles intégrées dans ClearPass, les entreprises peuvent générer les niveaux requis de visibilité et de sécurité dans les domaines suivants : types de terminaux, accès au réseau, analyse des flux de trafic, protection contre les menaces.

Les workflows automatisés et les décisions reposent sur une API REST écrite en langage de base, sur les messages syslog et sur le référentiel intégré ClearPass Extensions. Tout en simplifiant la tâche du département IT, cette solution sécurise les activités de l'entreprise sans jamais faire appel à des langages de script complexes ou à des opérations fastidieuses de configuration manuelle. Et pour une intégration plus rapide, les Extensions permettent aux partenaires d'uploader une extension spécialisée pour livraison en temps réel de nouveaux services à des clients communs.

Avec ClearPass Exchange, les réseaux peuvent exécuter automatiquement les actions suivantes :

- Les données MDM/EMM permettent de déterminer si tel ou tel terminal est autorisé à se connecter à un réseau (par exemple, terminal débridé/jailbreak).
- Les pare-feu complètent la protection des politiques en tenant compte des utilisateurs, des groupes et des attributs de chaque terminal, et ils aident ClearPass à corriger les terminaux dont le comportement n'est pas conforme aux politiques.
- Les outils SIEM peuvent être configurés de manière à stocker les données d'authentification des différents terminaux connectés.
- Un utilisateur peut être invité à utiliser une authentification multifacteur pour démontrer que c'est bien lui qui se connecte aux réseaux et aux ressources.

Certains événements réseau peuvent également amener les pare-feu, les outils SIEM et d'autres outils à demander à ClearPass d'appliquer certaines actions à un terminal en mode bidirectionnel. Par exemple, si l'authentification d'accès réseau d'un utilisateur échoue à plusieurs reprises, ClearPass peut envoyer une notification directement sur son terminal ou mettre celui-ci en liste noire pour l'empêcher d'accéder au réseau.

Accéder en tous lieux et en mode sécurisé aux applications de l'entreprise

Pendant la journée de travail, l'accès aux applications de l'entreprise doit être facile et rapide. ClearPass supporte le mode de connexion persistant (SSO) à travers la fonctionnalité ClearPass Auto Sign-On. Par contraste avec le mécanisme SSO standard, qui oblige à se connecter une première fois aux applications requises, la fonctionnalité Auto Sign-On s'appuie sur une connexion réseau unique qui permet aux utilisateurs d'accéder à l'ensemble des applis mobiles de l'entreprise (les utilisateurs doivent uniquement disposer de leur connexion réseau standard ou d'un certificat valide sur leur terminal).

Lorsque la connexion SSO est utilisée, ClearPass peut également être utilisé comme gestionnaire d'identités (IdP) ou comme prestataire de services (SP).

Services Bonjour, DLNA et UPnP

Les équipements qui supportent DLNA/UPnP ou Apple AirPlay/AirPrint (projecteurs, téléviseurs, imprimantes, etc.) peuvent être partagés par les utilisateurs dans l'ensemble de votre infrastructure Aruba Wi-Fi. ClearPass facilite la recherche et le partage de ces équipements.

Par exemple, un enseignant qui prévoit de projeter une présentation à partir d'une tablette est limité à l'écran présent dans sa salle de classe ; il ne peut pas être informé des équipements présents dans d'autres bâtiments de l'université. Toutefois, il peut utiliser le portail dédié pour désigner les personnes autorisées à utiliser son écran ou empêcher les étudiants de l'utiliser.

Autre exemple – Dans un hôpital, les médecins peuvent projeter les images numériques PACS disponibles dans leur iPad sur un grand écran n'importe où dans l'hôpital et améliorer ainsi la collaboration vis-à-vis de certains patients.

SOCLE ADAPTATIF DE SÉCURITÉ ET DE SERVICES

Les tendances actuelles qui visent à proposer une expérience transparente pour les utilisateurs mobiles et à permettre l'adoption rapide des technologies IoT font apparaître une multitude de défis pour le département IT. Pour sécuriser les accès aux réseaux filaires et sans fil en tous lieux et 24x7, le département IT doit planifier es actions, définir un socle efficace et disposer d'outils performants.

ClearPass apporte une solution intégrée et cohérente à ces différents aspects en proposant les fonctionnalités suivantes : identification des terminaux, supervision des politiques, automatisation des workflows et protection automatisée contre les menaces. En exécutant la capture et la corrélation de données contextuelles en temps réel, ClearPass permet de définir des politiques applicables à tous les environnements – au bureau, à l'université, au stade…

Des améliorations récentes ont été apportées à ClearPass pour relever également les nouveaux défis de sécurité réseau : adoption des objets IoT, authentification plus performante des terminaux mobiles et de leurs applis et visibilité plus complète sur les incidents de sécurité. Le fonctionnalités de protection automatisée contre les menaces et de services intelligents garantissent que chaque terminal se voit affecter des privilèges d'accès réseau spécifiques, exigeant rarement l'intervention du département IT.

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 SO_ClearPass_111016