aruba
a Hewlett Packard Enterprise company

SOLUTION BRIEF

CONTRÔLE D'ACCÈS RÉSEAU SÉCURISÉ CLEARPASS CERTIFIÉ CRITÈRES COMMUNS

INTRODUCTION

Les cyberattaques sont de plus en plus intelligentes, ciblées et néfastes. Avec l'augmentation rapide de la surface présentée aux attaques, de par l'avènement des appareils mobiles, BYOD, cloud et des objets connectés, la probabilité de réussite des attaques continue de croître. Qu'il s'agisse d'une agence gouvernementale protégeant des infrastructures vitales ou d'un prestataire de santé en charge des données personnelles de patients, aucune organisation n'est à l'abri du stress causé par la lutte contre ces attaques.

Alors que les agences gouvernementales ont pris les choses en main en définissant les critères et processus de certification des produits, les équipes de sécurité doivent être en mesure de savoir si les produits qu'ils déploient pour la protection de leurs services se conforment à un ensemble validé de normes de sécurité.

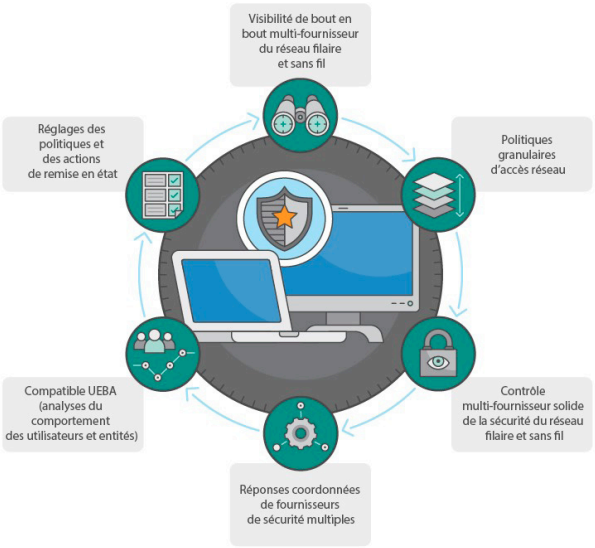
Depuis 1999, des Etats du monde entier ont collaboré à un programme de test et de validation de Critères Communs sur une norme ISO. Ce programme évalue les produits de technologie de l'information et s'assure qu'ils offrent des performances répondant à des normes exigeantes et cohérentes, contribuant ainsi de manière significative à la confiance portée à la sécurité de ces produits. A ce jour, 28 pays participent au consortium Critères Communs par le biais d'initiatives telles que le NIAP aux Etats-Unis, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France et l'Australian Signals Directorate. La certification Critères Communs fait par conséquent partie de la liste des conditions requises pour répondre aux appels d'offres de nombreux Etats.

Aruba est très au fait de la certification Critère Communs sur l'ensemble de ses gammes de produits, et notamment les points d'accès sans fil, les contrôleurs et les logiciels de connexion à distance (VPN). En tant qu'élément clef du cadre de solutions de sécurité de pointe 360 Secure Fabric d'Aruba, ClearPass Policy Manager a reçu les certifications FIPS et Critères Communs.

PRÉSENTATION GÉNÉRALE DE CLEARPASS

La gamme ClearPass de produits de contrôle sécurisé de l'accès réseau offre un profilage, une authentification et une autorisation uniformes, exhaustifs et précis des utilisateurs, systèmes et périphériques cherchant à accéder aux ressources informatiques. ClearPass est conçu pour faire face aux défis de sécurité clefs liés à une organisation sans limites informatiques, et notamment :

- **Visibilité totale.** Lorsque l'accès réseau peut être accordé quasiment n'importe où et n'importe quand, pour n'importe quel périphérique, le premier défi consiste à savoir ce qui se trouve sur le réseau. ClearPass offre de grandes capacités de découverte et de profilage pour permettre non seulement à l'équipe de sécurité, mais également à tout le personnel informatique de voir les personnes et les appareils connectés. Cette connaissance est particulièrement importante lorsque des appareils type objets connectés se connectent au réseau.
- **Contrôle proactif.** Avec ClearPass Policy Manager, chaque utilisateur, système et périphérique sur le réseau reçoit un accès limité aux seules ressources que son rôle nécessite. ClearPass authentifie chaque entité et lui attribue des privilèges d'accès en fonction des stratégies qui ajustent les permissions sur la base du lieu de connexion, de l'appareil utilisé, de l'heure, du type d'utilisateur et d'autres facteurs.
- **Réponse en boucle fermée.** ClearPass doit être considéré comme le gardien du réseau. Le moteur de stratégies qui permet l'accès réseau peut également servir à la réponse à une cyberattaque. Lorsqu'une alerte est émise par l'écosystème de sécurité (pare-feu, sandboxes, détection des terminaux et réponse, SIEM, UEBA, etc.), ClearPass peut prendre toute une gamme de mesures basées sur les stratégies, comme une réauthentification, une limitation de la bande passante, une quarantaine ou un blocage.



Légende : Aruba ClearPass offre une approche en boucle fermée pour le contrôle de l'accès réseau et la réponse.

L'AVANTAGE CLEARPASS

- **Une sécurité assurée grâce à une certification Critères Communs en profondeur.** ClearPass est certifié Critères Communs pour le profil de protection collaborative de périphérique réseau (NDcPP), englobant tous les aspects du contrôle d'accès, et notamment le chiffrement, la sécurité physique, la validation de certificats et le traitement et le traitement SSL. De plus, le serveur d'authentification ClearPass a également reçu une certification Critères Communs supplémentaire qui valide ses capacités d'Authentification, Autorisation et Responsabilité (AAA) par rapport au protocole client/serveur RADIUS aux normes de l'industrie. Ce niveau de certification permet à ClearPass de fonctionner sur les réseaux classifiés et de remplir des fonctions de degré de confidentialité similaire dans le secteur privé.
- **Intégration ouverte et fluide.** Contrairement à d'autres solutions de contrôle d'accès qui nécessitent un engagement vis-à-vis de l'infrastructure d'un fournisseur unique, ClearPass est optimisé pour fonctionner sur n'importe quel réseau. De plus, ClearPass s'intègre avec plus de 120 solutions informatiques généralistes et de sécurité pour leur permettre de tirer parti des profils et des contextes de périphérique générés par ClearPass. Les équipes de sécurité utilisent également ClearPass pour prendre des mesures en réponse à une cyberattaque, de façon manuelle ou automatisée.
- **Un réseau, un point de vue, une stratégie.** La capacité de ClearPass à contrôler l'accès aux ressources informatiques est non seulement indépendante du fournisseur de l'équipement, mais également du type d'accès : filaire, sans fil ou à distance. Les entreprises et organismes conçoivent et mettent en place une stratégie par utilisateur ou par périphérique, et ClearPass applique cette stratégie de manière fluide sur l'ensemble de la topologie du réseau. Cela permet des économies de temps et d'argent qui peuvent être réaffectés à d'autres projets informatiques et de sécurité.
- **Réseaux optimisés.** ClearPass présente un avantage en termes de retour sur investissement qui est qu'il s'agit d'une mise en place de l'accès aux ports et de leur utilisation. Au lieu de désigner des ports pour des cas d'utilisation spécifiques (pour la connexion d'imprimantes, de serveurs, etc.), les entreprises et organismes peuvent utiliser une stratégie de « ports incolores », où chaque port peut permettre la connexion de n'importe quel périphérique, pendant que ClearPass met en œuvre les contrôles d'accès réseau basés sur des rôles appropriés. Cela simplifie l'installation et la configuration des commutateurs et optimise l'utilisation des ports.
- **Accès blindé : vérifier, puis accorder sa confiance.** Certaines solutions de contrôle d'accès permettent à tout utilisateur ou périphérique d'accéder au réseau, puis prennent des mesures si un problème survient. Cette approche de « contrôle d'accès réseau détendu » facilite les cyberattaques ultra-rapides où le logiciel malveillant ne nécessite qu'une seconde pour s'introduire sur le réseau et lancer une attaque prolongée et très néfaste. ClearPass emploie une approche où aucun utilisateur ou périphérique ne peut accéder au réseau sans authentification positive et l'autorisation stratégique appropriée. Quand tout se joue à la seconde près, le contrôle d'accès doit démarrer à T-zéro.
- **Interception des attaques.** L'axiome dit « on ne peut protéger ce que l'on ne voit pas. » L'un des avantages de la découverte et du profilage de ClearPass est une visibilité totale. Mais dans un monde où chaque seconde compte en termes de réponse aux attaques, il est également impossible de répondre à ce que l'on ne voit pas. En utilisant ClearPass pour établir des réponses prédéfinies aux signaux de cyberattaques émanant de l'écosystème de sécurité, les équipes de sécurité peuvent interrompe les attaques avant qu'elles causent des dommages, tout en continuant leur investigation pour déterminer la portée de la faille de sécurité.

RÉSUMÉ

La certification Critères Communs est un processus exigeant qui impose d'avoir une protection de sécurité qui fasse partie intégrante de l'architecture et de la mise en œuvre du produit. Fut un temps, les Critères Communs n'étaient exigés que par les agences gouvernementales, en raison de la grande valeur des équipements et des informations qu'elles devaient protéger. De nos jours, toute entreprise ou organisation doit faire face à des risques similaires, avec des conséquences comparables en cas de réussite d'une cyberattaque. Pour une solution répondant à un besoin aussi crucial que le contrôle d'accès réseau, la certification Critères Communs est essentielle. Avec ses certifications Critères Communs améliorées, ClearPass offre non seulement une base sécurisée, mais également un élément crucial pour prendre en charge l'ensemble de la stratégie de sécurité informatique.

aruba
a Hewlett Packard Enterprise company

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com