Université Libre de Bruxelles

Rapport d'analyse - Groupe 8

INFO-F309

Noëmie Muller, Anthony Kerckhof, Bruno Sylin, Julien Baudru

November 16, 2020

1 Problématique

1.1 Rappel de la problématique

L'aéroport de Zaventem s'inquiète de la sécurité du réseau WiFi et souhaiterait connaître en temps réel la liste de tous les appareils connectés au réseau ainsi que le type d'actions effectuées et l'adresse exacte de ces appareils. En cas d'utilisation suspecte du réseau, il est également demandé de pouvoir en déconnecter et bloquer n'importe quel appareil sans délai.

1.2 Précisions sur la problématique

1.2.1 Une utilisation suspecte

Par utilisation suspecte du réseau Wifi par un utilisateur, nous entendons tout comportement contraire aux lois en vigueur dans le pays. Par comportement suspect, nous entendons également, une utilisation du réseau anormalement élevée par rapport à la moyenne.

1.2.2 Bloquer un utilisateur

Par bloquer un utilisateur nous entendons, interdire définitivement l'accès au réseau WiFi pour cet utilisateur.

1.2.3 Déconnecté un utilisateur

Par déconnecter un utilisateur nous entendons, interdire pour une durée limitée l'accès au réseau WiFi pour cet utilisateur.

2 Description de la solution

Le type de solution que nous proposons pour cette problématique est appelé un **NAC** (Network Access Controler) ou contrôleur d'accès réseau en français. Un NAC permettra à l'administrateur de mettre en oeuvre une politique de contrôle des appareils et de l'accès des utilisateurs au réseau de l'aéroport. Dans le cas particulier du contrôle d'un réseau WiFi, la solution fera partie de la famille des **WNAC** (Wireless Network Acces Controler), c'est à dire un contrôleur d'accès réseau sans-fil en français, à noter que la plupart des solutions **NAC** propose également un contrôle du réseau sans-fil. Ce type de solution permet d'observer en temps réel les appareils connectés sur le réseau et ainsi améliorer le contrôle et la sécurité de celui-ci.

3 Comparaison des différentes solutions

3.1 Sélection

Parmi les différentes solutions disponibles sur le marché, nous avons retenu les quatre offres suivantes :

1. **Aruba Networks** Aruba Newtorks est une filiale de Hewlett Packard Enterprise (HPE) et fournit des solutions de réseau local sans fil pour des organisations de toute taille.
2. **Cisco ISE** Cisco est une entreprise informatique spécialisée dans le matériel réseau et les serveurs.
3. **PacketFence** PacketFence est un logiciel libre de contrôle d'accès au réseau permettant la sécurisation de réseau de petites entreprises jusqu'à de très larges infrastructures.
4. **openNAC** openNAC est un contrôleur d'accès réseau open-source dédié aux environnements d'entreprise LAN/WAN.

3.2 Critères de comparaison

Afin de choisir au mieux une solution adaptée à l'aéroport de Zaventem, nous avons comparé les quatre logiciels cités plus haut selon les critères suivants :

3.2.1 Licence

On retrouve parmi les solutions deux alternatives ayant une licence open-source et deux solutions ayant une licence propriétaires. Les solutions PacketFence et openNAC sont open-source, ce qui signifie que ces logiciel peuvent être redistribués de manière libre, et que les utilisateurs ont accès à leur code source et ont la possibilité de créer des programmes dérivés de ceux-ci. De plus, la majorité des logiciels open-source sont gratuits.
Les deux autres solutions, Aruba Networks et Cisco ISE sont des logiciels avec des licences propriétaires. Si nous perdons avec ce type de produit l'avantage d'avoir libre accès au code source, nous sommes de fait à l'abri de développeurs mal intentionnés ou négligeants en terme de sécurité. De plus, l'utilisation de logiciels propriétaires sont souvent plus accessibles, la conception étant moins tournée vers un public de développeurs aguerris que dans le cadre d'un logiciel open-source.

3.2.2 Budget

Comme annoncé au point précédent, les deux solutions open-source PacketFence et openNAC sont gratuites. Pour les deux solutions propriétaire, les prix varie en fonction du nombre d'appareil connectés au réseau à contrôler. Ainsi, on estime ce nombre en fonction de la fréquentation maximum de l'aéroport de Zaventem en un jour. Pendant la période des vacances d'été où le transit à l'aéroport est le plus important, le nombre de passagers environnait en 2019 les 5,3 millions de passagers[1], ce qui nous fait une moyenne par jour de 85.000 passagers. En prenant en compte les pics d'affluence, le nombre maximal de personnes connectées au réseau WiFi en une journée pourrait avoisiner les 100.000 personnes. (Le record d'affluence en une journée pour l'aéroport de Zaventem était 94.928 voyageurs en 2018[2].)

Pour ce nombre d'appareil, la solution Aruba ClearPass est accessible pour un montant de 712.069€ pour un abonnement d'un an au service, 1.780.173€ pour un abonnement de 3 ans et 2.225.217€ pour un abonnement de 5 ans[3], et la solution Cisco ISE demande de débourser 2.300.000$ (1.946.846,50€) pour un abonnement de 3 ans et 2.875.000$ (2.433.558€) pour une offre de 5 ans . [4]

Notons que la plupart du temps, une offre inférieure est suffisante. Si on tolère que pendant les grandes affluences, le service ne puisse pas gérer tout le monde et que des passagers se retrouveraient sans accès WiFI, les offres à 50.000 ou 10.000 points de terminaison sont acceptables (moyennement une gestion très active du renouvellement de ces points de terminaisons afin qu'ils ne restent pas attribués à des passagers dont l'utilisation n'est pas continue). Les prix descendent alors pour Aruba à 281.000 € pour l'offre de 10.000 points de 5 ans et 1.112.608 € pour l'offre de 50.000 endpoints de 5 ans. L'offre de Cisco est de la même échelle de prix : 325.000 $ (274.516 €) pour une offre de 10.000 points de terminaison pendant 5 ans et 1.553.000 $ (1.311.764 €) pour une offre de 50.000 points de terminaisons pendant 5 ans

3.2.3 Etendue du service

Aruba Networks est particulièrement adaptée aux environnements avec un grand volume de connexions puisqu'il offre plus de 10 millions [5] d'authentification par jour.
Cisco ISE prend en charge jusqu'à 500 000 [5] sessions simultanées et 1.5 million de points d'extrémité par déploiement.
Pour OpenNAC et PacketFence, il n'existe pas de chiffre de comparaison en terme d'étendue des services. OpenNAC stipule cependant que son service peut être adapté aux entreprises de taille S, M et L [6]. Mais puisque ces 2 solutions sont open-source, il est toujours possible de revoir le code afin d'améliorer les capacités. Ces offres ne sont donc limitées en capacité de charge simultanée que par le matériel de l'aéroport.

3.2.4 Réseau hétérogène

Pour ce critère, nous cherchons à savoir si les différentes solutions sont capables de contrôler des réseaux dits *hétérogènes*. Un réseau hétérogène est un réseau alliant réseau filaire (ex. Ethernet : le réseau administratif) et réseau sans-fil (ex. WiFi : disponible pour tous). Parmi notre sélection, les quatre solutions proposent une gestion de réseau hétérogène.

3.2.5 Distribution

Par distribution nous entendons le système sur lequel les différents programmes proposés sont capables de fonctionner. Les solutions propriétaires de CISCO et ArubaNetworks sont toutes les deux disponibles pour Mac, Windows, Android et Linux. [7]. OpenNAC fonctionne quant à lui également sur Windows, Linux et Mac à l'inverse de PacketFence qui n'est disponible que pour les appareils de la famille Linux.

3.2.6 Sécurité

Aruba et Cisco figurent sur la liste des 4 services de NAC approuvés par le Département américain de la défense [8]. Cette liste reprend les produits ayant obtenu la certification d'Interopérabilité (IO) et de Cybersécurité, nécessaire à tout produit désirant faire affaire avec le gouvernement fédéral américain [9]. Mais les 4 solutions utilisent le standard IEEE 802.1X, qui un standard mondial pour la sécurité des réseaux informatiques. Tout appareil ne respectant pas ce standard n'aura pas accès au réseau ce qui assure une première sécurité forte.

3.2.7 Gestion de la bande passante

PacketFence surveille la quantité de bande passante consommée par le réseau et peut écarter ou adapter l'accès au réseau des appareils trop gourmands. Il fournit également un rapport d'utilisation de la bande passante. Cisco ISE et Aruba Network permettent tous les deux une paramétrisation de la bande maximale autorisée par appareil utilisateur connecté au service. OpenNAC quant à lui ne fournit pas d'outil de gestion de la bande passante [10].

3.2.8 Documentation

Un dernier point essentiel concernant le choix de la solution est la présence d'une documentation claire et précise pour cette dernière. Cette documentation permettra à l'administrateur réseau de mener à bien la maintenance du service. Si la documentation de PacketFence fournit un support suffisant concernant l'administration, la configuration et les guides d'installation, OpenNAC dispose en revanche d'une documentation assez pauvre en explications et nécessitant des connaissances avancées en la matière.
Pour les 2 solutions propriétaires, une large documentation est aussi disponible (avec une préférence pour la documentation de Cisco ISE qui est plus complète et plus simple d'utilisation), mais ces solutions se distinguent des premières par l'accès à un support dédié disponible en complément à la documentation pour les administrateurs réseaux afin qu'ils puissent poser leurs questions techniques directement à la source.
Il est également intéressant de noter que les outils open-source sont généralement entourés d'une communauté de développeurs assez importante. Les logiciels OpenNAC et PacketFance sont accompagnés respectivement d'un forum en ligne et d'une mailing list particulièrement actifs qui fournissent un support non négligeable.

3.3 Récapitulatif

Critères	**Aruba**	**Cisco ISE**	**OpenNAC**	**PacketFence**
Licence	Propriétaire	Propriétaire	Open-source	Open-source
Prix	1.800.800€ / 3 ans	2.300.000€ / 3 ans	Gratuit	Gratuit
Étendu du service	10 millions / jour	500.000 sessions simultanées	Seule limite matérielle	Seule limite matérielle
Réseau hétérogène	Oui	Oui	Oui	Oui
Distribution	Toutes	Toutes	Toutes sauf Android	Linux
Sécurité	approuvé FIP & IEEE 802.1x	approuvé FIP & IEEE 802.1x	IEEE 802.1x	IEEE 802.1x
Bande passante	Oui	Oui	Non	Oui
Documentation	Oui	Oui	Peu claire	Oui

4 Solution retenue

Après comparaison, notre équipe a retenu la solution **PacketFence** distribuée par la société *Inverse Inc.*. Nous nous sommes orienté vers cette solution car elle est open-source, et donc gratuite, ce qui permettra à l'aéroport de minimiser le coût de la mise en place d'un tel service. De plus, cette solution est distribuée sur le système d'exploitation Linux, largement utilisé pour la plupart des serveur, évitant des coûts annexes dû l'installation d'un serveur utilisant un autre système d'exploitation. Par ailleurs, cette solution permet le contrôle d'un réseau hétérogène ce qui correspond parfaitement à la demande de l'aéroport visant à contrôler les utilisateurs connectés aux réseaux WiFi. **PacketFence** propose également des outils assez poussés de gestion de la bande passante, ce qui permettra à terme de détecter d'éventuelles utilisations anormales du réseau. Finalement, cette solution dispose d'une documentation détaillée et d'un support de la communauté à travers une mailing très active, ce qui sera un avantage non négligeable lors de la mise en place du NAC par notre équipe.

5 Travaux à prévoir

PacketFence n'étant distribué que sur Linux, il faudra s'assurer que l'aéroport dispose de serveurs tournant sur le bon système d'exploitation.

Par ailleurs, il faudra également prévoir l'ajout de logiciels tels qu'un gestionnaire de base de données, un pare-feu et un serveur web pour assurer une bonne gestion du serveur. Au niveau du hardware du serveur, il est demandé d'avoir au moins les spécifications suivantes:

- Un processeur AMD ou Intel de 2 coeurs minimum à au moins 3Ghz dédié à PacketFence
- 12 GB de RAM (16 GB recommandé) disponible pour PacketFences
- 100 GB d'espace disque (RAID-1 recommandé)
- 1 carte réseau (2 recommandé)
- par ailleurs, nous recommandons d'avoir un LVM (logical volume management)

Il faudra également prévoir l'installation de points d'accès sans-fil compatibles avec le logiciel **PacketFence** [11].

5.1 Phases et planning

La mise en place de ce service se déroulera en deux phases :

Phase 1 - Installation + configuration: Cette phase d'une durée de 2 semaines permettra à notre équipe d'installer et de configurer correctement PacketFence et tous les logiciels nécessaires pour la bonne mise en oeuvre du service demandé.

Phase 1 - Test : Cette phase d'une durée de 2 semaines permettra à notre équipe de tester l'installation et le bon fonctionnement du service proposé sur une région restreinte de l'aéroport.

Phase 2 - Mise en service : Durant cette phase, si la phase de test s'est avérée concluante, nous prévoyons d'étendre l'installation du service à l'ensemble de l'aéroport. La durée de celle-ci dépendra du nombre de points d'accès qui devront éventuellement être modifiés. Elle pourrait durer jusqu'à 2 semaines également.

References

[1] Brussels Airport. Brussels airport a accueilli plus de 5,3 millions de passagers pendant les deux mois d'été, dont plus de 2,6 millions en août. https://www.brusselsairport.be/pressroom/brussels-airport-a-accueilli-plus-de-53-millions-de-passagers-pendant-les-deux-mois-dete-dont-plus-de-26-millions-en-aout/, 2019.

[2] La Libre. Record d'affluence historique à brussels airport en juillet. https://www.lalibre.be/economie/entreprises-startup/record-d-affluence-historique-a-brussels-airport-en-juillet-5b69a7e555324d3f13cde1d4, 2018.

[3] Aruba. Liste de prix hpe réseau janvier 2018. https://www.hpe.com/content/dam/hpe/download/pdf/Liste_de_prix_hpe_r%C3%A9seau_janvier_2018.pdf, 2018.

[4] CISCO. Cisco global price list - 2020. https://ciscogpl.com/cisco+ise.html, 2020.

[5] Drew Robb. 9 top network access control (nac) solutions. https://www.esecurityplanet.com/products/top-network-access-control-solutions.html, 2019.

[6] OpenNAC. Opennac overview. https://community.spiceworks.com/products/56996-opennac, 2014.

[7] Drew Robb. Cisco identity services engine: Nac product overview and insight. https://www.esecurityplanet.com/products/cisco-identity-services-engine.html, 2017.

[8] Approved Products Certification Office (APCO). Dodin approved products list. https://aplits.disa.mil/processAPList.action.

[9] Ashley Neu. 8 product certifications you need to sell to the federal government customer. https://sanctumfederal.com/product-certifications-to-do-business-with-federal-government/, 2020.

[10] Kwame Osei Boateng Henry Nunoo-Mensah, Emmanuel KofiAkowuah. A review of opensource network access control (nac) tools for enterprise educational networks. https://www.researchgate.net/publication/277012927_A_Review_of_Opensource_Network_Access_Control_NAC_Tools_for_Enterprise_Educational_Networks, 2014.

[11] PacketFence. Network devices configuration guide. https://packetfence.org/doc/PacketFence_Network_Devices_Configuration_Guide.html#_wireless_controllers_and_access_point_configurat 2020.

[12] Drew Robb. Hpe aruba clearpass: Nac product overview and insight. https://www.esecurityplanet.com/products/hpe-aruba-clearpass.html, 2017.

[13] Jon Green. Effective network access control in a wireless world. https://www.arubanetworks.com/pdf/technology/TB_TNAC.pdf, 2009.

[14] What is 802.1x network access control (nac)? https://www.juniper.net/us/en/products-services/what-is/802-1x-network-access-control/, 2020.