UNIVERSITÉ DE YAOUNDÉ I
*****
ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE
****
DÉPARTEMENT DE GÉNIE INFORMATIQUE

UNIVERSITY OF YAOUNDE I
*****
NATIONAL ADVANCED SCHOOL OF ENGINEERING
****
DEPARTMENT OF COMPUTER ENGINEERING

RAPPORT DE STAGE PRÉ-INGÉNIEUR

THÈME :

Mise en Oeuvre du NAC pour la Sécurisation d'un Réseau Local

Cas de la DGSN

Élaboré Par

BENGONO CHANEL DYLANE (4E ANNÉE CIA)

Sous la supervision du :

COMMISSAIRE DE POLICE WALWAL ANGOUAKAYE

1ER NOVEMBRE 2022

REMERCIEMENTS

Mes remerciements vont à l'endroit de Monsieur Martin MBARGA NGUELE, Délégué Générale à la Sûreté Nationale qui malgré la sensibilité du secteur d'activité a marqué son accord pour que je puisse effectuer ce stage au sein de l'institution dont il est à la charge.

Au Sous-directeur de la Gestion Informatique, le Commissaire Divisionnaire EVINA ZANGA Hermann.

Aux Ingénieurs-Commissaires de Police Walwal Angoakaye, et WAKEU KOUAM Jerry Aloys pour leur accueil, leur encadrement, leurs multiples conseils, lesquels ont été des plus importants.

À l'ensemble des personnels de la SDGI pour leur intérêt quant à mon sujet de stage et leurs nombreux encouragements tout au long de ce stage, nous pensons à messieurs BELINGA Jean Marie, Mbwoge Bwene Bruno, Sosthène ETABA.

Au Directeur de l'ENSPY et au Chef du Département de Génie Informatique qui travaillent sans cesse pour que nous soyons dans les meilleures conditions d'apprentissage.

À ma famille et surtout à mon père Monsieur NDONGO MELONO Emmanuel Vartant et à ma mère Mme MENDOMO ASSE Solange Dorelle pour leur soutien indéfectible depuis des années et sans qui tout ceci n'aurait été possible

À tous les membres du Core Groupe Emmry (ECG) pour leur soutien moral et financier ainsi qu'à toute la 1ère promotion de la spécialité Cyber Sécurité et Intelligence Artificielle de l'ENSPY.

Nous réitérons nos remerciements à toutes les personnes qui de près ou de loin ont contribué à la rédaction de ce rapport de stage.

ABRÉVIATIONS

Acronymes	Significations
ACL	Access Control List
BYOD	Bring Your Own Device
CIA	Cyber sécurité et Intelligence Artificielle
DFGIL	Direction des Finances, de la Gestion Informatique et Logistique
DGSN	Délégation Générale à la Sûreté Nationale
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
EAP	Extensible Authentication Protocol
ENSPY	École Nationale Supérieure Polytechnique de Yaoundé
HTTP	Hyper Text Transfer Protocol
IPSEC	In Computing, Internet Protocol Security
MAC	Medium Access Control
NAC	Network Access Control
NAP	Network Access Protection
NPS	Network Policy Server
RADIUS	Remote Authentication Dial-In User Service
SDGI	Sous-Direction de la Gestion Informatique et Logistique
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

ABSTRACT

Emerging technologies come with vulnerabilities that can pose a challenge for IT security experts. Moreover, the adoption of Bring Your Own Device (BYOD) policies has increased the security concerns of organizations. Network access control solutions play a crucial role in handling enterprise networks with multiple devices. They can protect the entire network, including physical infrastructure and cloud-based systems. Limited network access enables IT teams to protect the network from unauthorized access. The overall objective of this project is to present an in-depth understanding of the concept of network access control, its essential mechanisms, as well as the configuration and deployment of the open-source NAC PacketFence in INLINE mode in order to secure the local network of the General delegation for National Security.).

Keywords : NAC, INLINE, PACKETFENCE, VLAN ,NETWORK PARTITIONING

RÉSUMÉ

Les technologies émergentes s'accompagnent de vulnérabilités qui peuvent constituer un défi pour les experts en sécurité informatique. En outre, l'adoption de politiques de type "Bring Your Own Device" (BYOD) a accru les préoccupations des organisations en matière de sécurité. Les solutions de contrôle d'accès au réseau jouent un rôle crucial dans la gestion des réseaux d'entreprise comportant de multiples dispositifs. Elles peuvent protéger l'ensemble du réseau, y compris l'infrastructure physique et les systèmes basés sur le cloud. Le NAC permet aux équipes informatiques de protéger le réseau contre les accès non autorisés. L'objectif global de ce projet est de présenter une compréhension approfondie du concept de contrôle d'accès au réseau, de ses mécanismes essentiels ainsi que la configuration et le déploiement du NAC open-source PacketFence en mode INLINE afin de sécuriser le réseau local de la Délégation Générale à la Sûreté Nationale.).

Mots-clés : NAC, INLINE, PACKETFENCE, VLAN ,CLOISONEMENT RESEAU

TABLE DES MATIÈRES

LISTE DES TABLEAUX

TABLE **Page No**

TABLE DES FIGURES

FIGURE **Page No**

INTRODUCTION GÉNÉRALE

Dans les réseaux d'entreprise, le concept d'apporter ses propres appareils (BYOD) au travail et de permettre aux noeuds invités de se connecter au réseau est souvent encouragé. La nécessité de contrôler l'accès au réseau est donc essentielle, car la visibilité des noeuds connectés au réseau est primordiale pour déterminer les menaces potentielles.

Contexte

Dans le cadre de notre formation à L'ENSPY qui exige un stage pré-ingénieur en 4e année j'ai eu le privilège de recevoir l'accord du Délégué Général à la Sûreté Nationale m'autorisant à effectuer ce stage dans l'institution dont il est à la charge en réponse à ma demande. Dans cette correspondance, il m'invite à prendre attache avec le Directeur des Finances, de la Gestion Informatique et Logistique et le Sous-directeur de la Gestion Informatique dont l'une des missions principales est d'assurer la disponibilité, l'intégrité et la confidentialité des données du système d'information de la DGSN.Ce rapport présente une mise en place d'une solution de sécurité et de conformité réseau qui traitera des aspects de manque de sécurité. Cela se traduit par l'établissement d'un mécanisme d'authentification automatique, lors de la connexion d'un équipement au réseau via un câble physique ou le réseau sans fil. Ceci est valable pour un utilisateur permanent ; alors que pour un utilisateur temporaire(visiteur), l'authentification s'effectue via le portail Web. Une fois authentifié, le client (poste de travail) subira quelques tests destinés à s'assurer de sa conformité vis-à-vis de la stratégie de sécurité prédéfinie. Après avoir effectué ces tests et si le client présente des vulnérabilités qui nécessitent l'installation ou la mise à jour d'un composant, il aura un accès restreint lui offrant les mises à jour nécessaires pour établir les remèdes appropriés et atteindre ainsi un état conforme et sain. Aussi, le présent rapport décrit la mise en place de cette solution. Ce rapport est composé de quatre chapitres :

• Le premier chapitre est consacré à une présentation du contexte du projet illustrant notre travail.
• Le deuxième chapitre est un état de l'art présentant une étude générale sur les technologies des solutions de contrôle d'accès et une étude technique sur la solution
choisie.
• Le troisième chapitre traitera de la Mise en OEuvre du NAC pour la DGSN.

• Le quatrième chapitre sera réservé aux Résultats obtenues, Perspectives et Recommandations

CHAPITRE 1

PRÉSENTATION DE LA DGSN

Au cours de ce chapitre, nous exposons le contexte général du projet. Aussi, nous présentons, en premier lieu, l'institution d'accueil, Ensuite, nous dégageons la problématique liée à notre projet pour aboutir aux objectifs fixés par l'institution

Contents

1.1 Historique, Organisation et Emplacement

1.1.1 Historique et Organisation

Après un Arrêté du Haut-Commissaire du Cameroun, les premiers Services de Police de notre pays ont vu le jour en 1925, avec la création du Commissariat de Douala. Par la suite, le Haut-Commissariat de la République Française a signé le 1er Juin 1946, un Arrêté « portant réorganisation de la Sûreté Nationale dans les territoires du Cameroun ». Le 31 Août de la même année, un autre Arrêté « portant transformation du Corps de la Police indigène, en Corps de Gardiens de la Paix et de la Sécurité Publique » est signé. Ce dernier texte constitue l'acte de naissance de notre Police en uniforme. C'est en 1947 que survient la création de la Direction de la Sûreté, couplée avec l'organisation d'un service spécialisé. Il convient de préciser qu'avant 1959, la Police Camerounaise était divisée en deux principales entités, celle du Cameroun Occidental dénommée « West Cameroon Police Force », avec pour quartier général Buea et celle du Cameroun Oriental basée à Yaoundé. La « West Cameroon Police Force » était calquée sur le modèle Britannique. C'est avec la nomination de Jean Marie EVINA EDJO'O comme Directeur de la Sécurité que les deux Polices vont fusionner, ceci bien avant le Référendum du 11 Février 1961. C'est ainsi que de 1959 à 1969, on connaîtra une période transitoire au cours de laquelle les polices des deux États fédérés étaient dirigées par le Premier Ministre ou le Ministre de l'Intérieur. Le 03 Mai 1969, un Décret Présidentiel portant création de la Délégation Générale à la Sûreté Nationale réorganisera les forces de Police avec comme premier Chef de Corps Paul PONDI.Toutefois, il faut relever qu'il existe à cette période, une Police en tenue chargée du Maintien de l'Ordre et, celle en civil oeuvrant en matière de Police Judiciaire et de Renseignements. Ces deux branches vont fusionner en 1979. De 1984 à 1989 et de 1991 à 1996, la Délégation Générale à la Sûreté Nationale sera transformée en Secrétariat d'Etat à la Sécurité Intérieure dirigé respectivement par Messieurs Denis EKANI et Jean FOCHIVE. C'est le Décret n°96/034 du 1er Mars 1996 portant « création de la Délégation Générale à la Sûreté Nationale » et signé du Président de la République, Son Excellence Paul BIYA, qui lui confère sa dernière appellation. Depuis le 30 août 2010, elle a à sa tête, Martin MBARGA NGUELE qui, il faut le mentionner, est à son deuxième passage comme Délégué Général à la Sûreté Nationale après celui du 22 août 1983 au 04 août 1984.

Période	Nom et prénoms	Fonction
2011-	Martin MBARGA NGUELE	Délégué Général à la Sureté Nationale (DGSN)
2009-2011	Emmanuel EDOU	DGSN
2004-2009	Edgar Alain MEBE NGO'O	DGSN
2000-2004	Pierre MINLO MEDJO	DGSN
1997-2000	Luc René BELL	DGSN
1996-1997	Luc LOE	DGSN
1991-1996	Jean FOCHIVE	Secrétaire d'État à la Sécurité Intérieure (SESI)
1990-1991	François Roger NANG	DGSN
1989-1990	Gilbert ANDZE TSOUNGUI	DGSN
1985-1989	Denis EKANI	SESI
1983-1984	Martin MBARGA NGUELE	DGSN
1976-1983	Samuel NGBWA	DGSN
1972-1976	Samuel ENAM MBA	DGSN
1969-1972	Paul PONDI	Délégué Général à la Sureté Nationale (DGSN)
1962-1969	Paul PONDI	Directeur de la Sureté nationale
1960-	Jean Marie EVINA EDJO'O	Directeur de la Sureté nationale

Table 1.1 – Délégués successifs

Période	Nom et prénoms
2015-	Dominique BAYA
2006-2015	Victor NDOKI
x-1998 - x	Victor MBIDA

Table 1.2 – Les SG successifs

Extrême-Nord	Nord	Adamaoua	Nord-Ouest	Sud-Ouest
Ouest	Littoral	sud	Centre	Est

Table 1.3 – Délégations régionales

Dénomination	Date début	Date fin
École Nationale Supérieure de Police de Yaoundé	1979	-
Centre d'instruction et d'application de la Police Nationale de Mutengené	1960	-

Table 1.4 – Formation

Dénomination	Date de Création
Équipes spéciales d'Intervention rapide (ESIR)	2004
Bureau central Interpol pour le Cameroun	1961
Groupement Spécial d'Opération (GSO)	1989
Compagnie de Sécurisation des Diplomates (CSD)	2007
Compagnie de sécurisation des établissements scolaires et universitaires	2015
Opération Dragon Noir	•
Postes de police mobiles	•
Centre National de Production des Titres Identitaires (CNPTI)	2016
Centre National de Commandement de la Vidéosurveillance	2019

TABLE 1.5 – Organes spéciaux

Dénomination	Date
Projet de sécurisation de la nationalité camerounaise	1994

TABLE 1.6 – Projets, Plans, Commissions

FIGURE 1.1. Le Centre National de Commandement de la vidéo surveillance inaugurée en 2019

1.1.2 Emplacement

La DGSN est situé à Nlongkak, Rue Onambele Nkou (place de la province), Yaoundé au Cameroun.

E-mail : agenceuniversitaireinnovation@gmail.com

BP : 1623 Yaoundé - Cameroun ;

Site web : https :// www.dgsn.cm

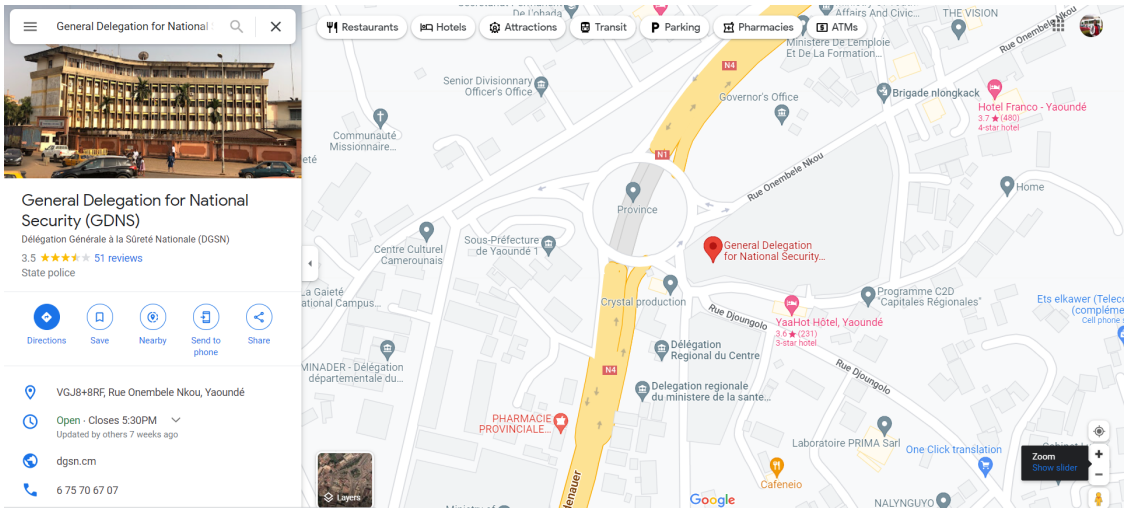

FIGURE 1.2. Localisation DGSN sur Google Map

1.2 Organigramme

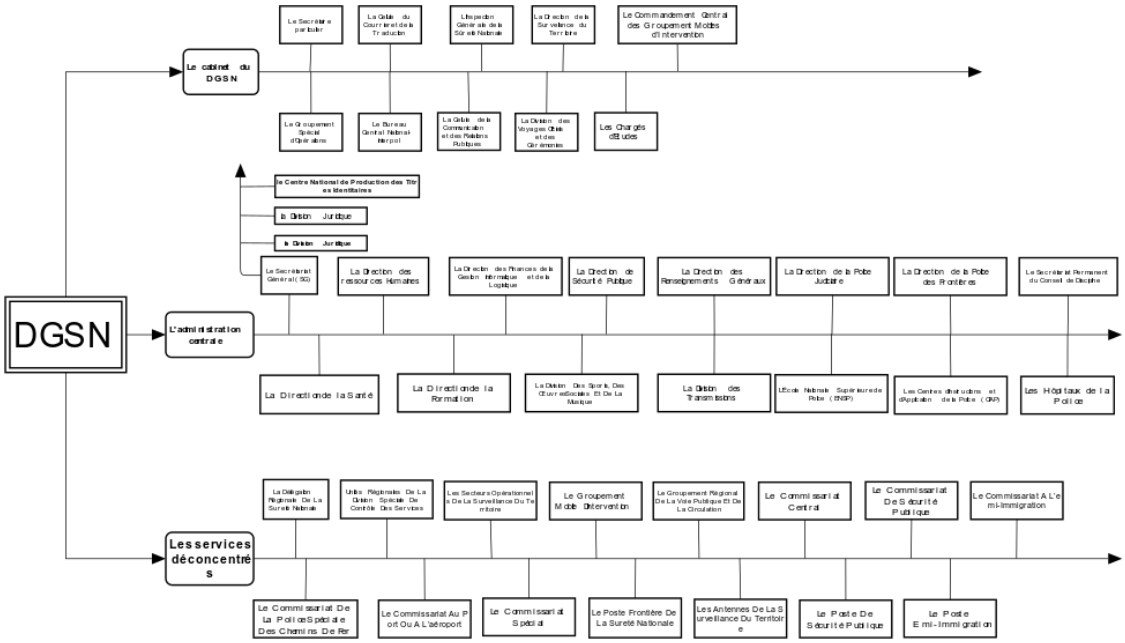

FIGURE 1.3. Organigramme DGSN

1.3 Les Missions de la DGSN

Sous l'autorité du Président de la République, Chef Suprême des Forces de Police, la Sûreté Nationale se définit comme un Corps de Commandement et d'Administration. Elle est composée d'unités territoriales (Postes et Commissariats de Sécurité Publique, Commissariats Centraux) qui sont des forces de première catégorie et des unités spécialisées telles que le Commandement Central des Groupements Mobiles d'Intervention (CCGMI), le Groupement Spécial d'Opérations (GSO) et les Groupements Mobiles d'Intervention (GMI) qui constituent des forces de deuxième catégorie. Elle assure des missions spécifiques, déclinées dans l'article 3 du Décret n°2012/540 du 19 Novembre 2012 portant organisation de la Délégation Générale à la Sûreté Nationale de la manière suivante :

- La Sûreté Nationale a pour mission fondamentale d'assurer le respect et la protection des institutions, des libertés publiques, des personnes et des biens ;
- Elle assure le respect de l'exécution des lois et règlements ;
- Elle concourt à l'exercice de la Police administrative et de la Police judiciaire ;
- Elle concourt en outre à la Défense Nationale.

L'article 4 de ce même Décret dispose que la Sûreté Nationale est chargée :

- De la sécurité intérieure et extérieure de l'État ;
- De la recherche, de la constatation des infractions aux lois pénales et de la conduite de leurs auteurs devant les juridictions répressives ;
- Du maintien de l'ordre et de la paix publics, de la protection, de la sécurité et de la salubrité publiques, plus particulièrement dans les agglomérations urbaines ;
- De la lutte contre la criminalité nationale, internationale et transnationale ;
- De la recherche du renseignement ;
- Des missions d'information, de sécurité, de protection et d'intervention comportant des contacts avec les populations, dans le cadre de la Défense Nationale ;
- De la sécurisation de la nationalité camerounaise ;

1.4 Environnement De Stage

Nous avons effectué notre stage au sein de la Sous-direction de la Gestion Informatique. Selon les articles 65,66,67 et 68 du décret N° 2012/540 portant organisation de la DGSN ; Placée sous l'autorité d'un Sous-Directeur, la Sous-Direction de la Gestion Informatique est

chargée :

- De la conception des programmes, des logiciels et des progiciels ;
- De l'exploitation et de la gestion le cas échéant, des données informatiques de la Sûreté Nationale ;
- Du suivi de l'exploitation rationnelle des installations informatiques de la Sûreté Nationale ;
- Du suivi des applications sectorielles informatiques des services de la Sûreté Nationale ;
- De la participation à l'examen des soumissions relatives aux appels d'offres de marchés ayant pour objet l'acquisition de matériels informatiques pour le compte de la Sûreté Nationale ;
- Des études informatiques de toutes natures ;
- De la formation des personnels à l'outil informatique ;
- Du suivi de l'évolution des techniques dans le domaine informatique ;
- De la documentation et des archives ;
- De l'entretien et de la maintenance des équipements informatiques.

La Sous-Direction de la Gestion Informatique comprend :

- Un Service des Études et des Projets ;
- Un Service de la gestion et de la Coordination ;
- Un Service de l'Exploitation et de l'Entretien des Équipements ;

1.5 Problématique

Dans le cadre de ce stage j'ai été affecté à La DFGIL plus précisément à la SDGI, avec les membres de l'équipe, nous effectuons des tâches de maintenance préventives ainsi que de collectes de données sur les différents équipements du parc informatique (adresses mac, service, n° de porte, nombre de prises réseaux et autres spécificités technique) dans les différentes directions, sous directions et organes spécialisés de la DGSN dans la ville de Yaoundé.
Suite à ses différentes descentes dans les différents démembrements nous avons relevé un certain nombre d'inconvénients à savoir :

- Plusieurs employés ont accès au réseau interne avec leur appareils personnels (ordinateurs et téléphone portable).

- Des ordinateurs de bureau dont la mauvaise configuration présente certains vulnérabilités.
- L'accès est permis à tous les sites internet quel que soit l'internaute.
- Pas de scan des terminaux avant l'accès au réseau.

1.6 Solution Proposée

Afin de réussir la mise en place d'une solution de sécurité intelligente au réseau local DGSN respectant les exigences matérielles et logicielles de l'institution et les besoins réels de l'utilisateur.Il faut assurer les objectifs suivants :

- N'autoriser que les machines répertoriées lors des descentes à se connecter au réseau.
- Refuser l'accès des utilisateurs au réseau sans authentification.
- Gérer la bande passante en fonction de priorité et des besoins.
- Administrer et suivre quotidiennement le journal des alertes.
- Contrôler l'accès aux ressources du réseau afin d'empêcher toute attaque,

Cette solution doit permettre d'atteindre ces objectifs par la mise en place d'une topologie réseau en utilisant le NAC open source **PacketFence**, l'intégration et la configuration des outils assurant la sécurité et le développement d'une interface d'authentification.

CHAPITRE 2

LES TECHNOLOGIES NAC

Le contrôle d'accès au réseau ou NAC est un terme qui décrit diverses technologies développées pour contrôler/restreindre l'accès au réseau par les systèmes d'extrémité en fonction de leur « état de santé ». L'idée de base est que les systèmes d'extrémité dangereux ou vulnérables (« en mauvaise santé ») ne doivent pas communiquer sur le réseau de l'entreprise dans la mesure où ils pourraient introduire un risque de sécurité pour les processus et les services critiques. Une solution NAC empêchera un système d'extrémité en mauvaise santé d'accéder normalement au réseau jusqu'à ce que la santé de ce système soit déterminée. Nous allons initier ce chapitre par la présentation des notions fondamentales du contrôle d'accès, la présentation des solutions de contrôle d'accès qui existent sur le marché puis choisir la solution NAC adéquate.

Contents

2.1 LES PRINCIPES DU NAC

Le NAC (Network Access Control) n'est pas une technique ou une architecture, le NAC est plus Proche d'un concept, d'une solution. Il est censé répondre à la mise en oeuvre de certaines parties de la politique de sécurité concernant l'accès au réseau local (filaire, sans-fil ou VPN), dont principalement :

— l'identification et l'authentification des utilisateurs ;
— l'évaluation du niveau de sécurité des systèmes se connectant ;
— la gestion des « invités » ;
— le contrôle de l'activité ;
— et parfois la détection d'intrusion.

2.2 LES COMPOSANTS D'UNE ARCHITECTURE NAC

2.2.1 Le système d'extrémité (Endpoints)

Il s'agit de l'élément de base qui est constitué par la machine physique qui souhaite accéder à des ressources C'est à partir de ce composant (poste de travail, imprimante, téléphone, etc.) que les informations relatives à l'authentification et à la conformité doivent être récupérées, aussi bien à la demande de connexion que de manière régulière durant la connexion.

2.2.1.1 Identification et authentification

Afin de connaître l'identité d'une entité (personne, ordinateur . . .) et, dans certains cas, valider l'authenticité de cette identification, plusieurs méthodes sont disponibles.

Utilisation de l'adresse MAC Ici, seule l'adresse MAC du système d'extrémité est utilisée pour l'identification. C'est un moyen facile à mettre en oeuvre, par exemple avec l'utilisation des requêtes DHCP. Il nécessite néanmoins la mise en place d'une base renseignée de toutes les adresses MAC autorisées à se connecter sur le réseau. Cette technique ne protège pas de l'usurpation d'identité, en forgeant son adresse MAC un utilisateur pourrait se faire passer pour une imprimante. Des techniques de prise d'empreinte du système d'exploitation

peuvent limiter ce problème en associant et en vérifiant ces informations liées aux adresses MAC de la base.

Portail Web L'authentification à l'aide d'une page Web sécurisée (https), tels les portails captifs, a l'avantage d'être accessible à tous les utilisateurs possédant un navigateur Web. En revanche, cette solution n'est pas envisageable pour les autres systèmes d'extrémité, les imprimantes par exemple.

802.1X Le standard 802.1X (Port Based Network Access Control) est un mécanisme d'authentification utilisé au moment de l'accès au réseau. Basé sur EAP, son principe repose sur des échanges sécurisés entre le « supplicant » (l'utilisateur et sa machine), l'« authenticator » (le point d'accès sans-fil, le commutateur, ...) et l' « authentication server » (un serveur RADIUS par exemple). Si l'identité de l'utilisateur (ou de la machine) est validée, le commutateur ouvrira l'accès au réseau (le VLAN de l'utilisateur peut être transmis par le serveur d'authentification).

2.2.1.2 Conformité

Le but est de récupérer des informations sur l'état du système d'extrémité. Deux possibilités sont envisageables, avec un agent embarqué sur le poste utilisateur ou sans agent. Avec la solution à base d'agents, il faudra prendre en compte le temps d'exécution, la charge CPU, le niveau de sécurité des échanges agent/serveur et la méthode de déploiement de ces agents. Sans agent, le temps d'exécution peut être long (scanner de vulnérabilités), ce qui peut contraindre à évaluer la conformité après la connexion.

2.2.2 Le système d'évaluation (Policy Decision Point)

Cet élément de l'infrastructure est crucial pour la politique de sécurité de l'établissement. À partir des informations recueillies sur le système d'extrémité, des informations sur la méthode d'accès (réseau filaire, sans-fil, VPN), mais aussi à l'aide d'informations sur le lieu où le moment de la demande d'accès, le système d'évaluation va décider d'un contexte de connexion en accord avec la politique de sécurité. Un exemple simple de système d'évaluation serait l'utilisation des adresses MAC des systèmes d'extrémité pour déterminer leur VLAN d'appartenance, le choix de la mise en quarantaine serait fait si l'adresse MAC est inconnue. La complexité du système d'évaluation dépendra de la quantité d'informations obtenue sur les systèmes d'extrémité et de la complexité de la politique d'accès à mettre en place.

2.2.3 Le système de contrainte (Enforcement)

2.2.3.1 Rôle du système de contrainte

C'est l'ensemble des éléments de l'infrastructure réseau permettant de détecter la demande d'accès au réseau et d'appliquer les décisions du système d'évaluation. Dans le cas d'un NAC basé sur un matériel dédié (dit « Appliance ») positionné en coupure sur le réseau, c'est généralement lui qui gérera la connexion du système d'extrémité dans son ensemble et mettra en oeuvre la politique décidée par le système d'évaluation. Si le système NAC n'est pas positionné en coupure (« outofband »), le système de contrainte doit s'appuyer sur l'infrastructure existante. Les actions classiques mises en oeuvre par le système de contrainte sont les suivantes :

— positionner le système d'extrémité dans un VLAN particulier.
— mettre en place des contrôles d'accès aux niveaux 2,3 ou 4 sur les équipements de bordure (commutateurs d'extrémité) ou plus près du coeur du réseau (routeurs, pare-feu, proxy).
— gérer la qualité de service, la bande passante

2.2.3.2 Différents systèmes de contrainte

Systèmes	Avantages	Difficultés	Risques
Serveur Dédiée positionnée en coupure qui capture l'ensemble des Paquets	Facilité de déploiement, gestion centralisée	Cela peut créer un SPOF (Single Point Of Failure), adaptation à la montée en charge difficile	Les systèmes d'extrémité ont déjà un accès au réseau (ils se voient entre eux)
Protocole 802.1X	Isolation au plus près de la demande d'accès	Capacité des matériels existants, il faut un client sur le système d'extrémité, choisir la méthode d'authentification (EAPMD5, EAPTLS...)	Dépendant de l'authentification utilisée (ex : EAPMD5 est à éviter)
VMPS (VLAN Management Policy Server)	La simplicité	Maintenance de la base de connaissance (adresses MAC/VLAN), gestion impossible de plusieurs adresses MAC par port, commutateurs Cisco seulement et en cours d'abandon par le constructeur	Usurpation d'adresse MAC
DHCP pour envoyer le bon profil IP (adresse, routeur, masque) au système d'extrémité	La simplicité	Aucune	Le système d'extrémité doit jouer le jeu (ne pas utiliser d'adresse IP fixe)
Trap SNMP (« link up » et « link down ») émis par les matériels réseau, permettant de détecter la connexion physique d'un système d'extrémité	Adaptable à une grande partie des matériels réseau. Difficulté	La complexité liée à la configuration des agents SNMP	Risque de déni de service avec des instabilités de liens, usurpation d'adresse MAC, les traps utilisent le protocole UDP ce qui n'assure pas la délivrance de l'information, besoin de maintenir un état de l'ensemble des ports

TABLE 2.1 – Différents systèmes de contrainte

2.2.4 Le système de mise en conformité

Dans le cas où le système d'extrémité n'a pas été jugé compatible avec la politique d'accès (manque de correctifs de sécurité, pas d'antivirus, échec de l'authentification, etc.) il est nécessaire de prévoir un contexte réseau où le système pourra se mettre en conformité (mise à jour système, possibilité de télécharger un antivirus, une base de signature à jour, demande de compte d'accès). Cette action de mise en conformité est parfois appelée « **remédiation** ».

La technique la plus communément employée est l'utilisation d'un VLAN spécifique redirigeant le trafic vers un portail captif Web qui doit guider l'utilisateur dans sa mise en conformité. Quelques difficultés apparaissent alors :

— Gérer les matériels sans navigateur Web (imprimante) ;
— Habituer l'utilisateur à ouvrir son navigateur en cas de soucis, même s'il ne souhaitait qu'utiliser son client de messagerie par exemple ;
— Personnaliser la page Web en fonction du problème spécifique ; En plus de ces difficultés, un problème de sécurité est généré en positionnant dans le même réseau des machines potentiellement fragiles. Premièrement, il y a un risque de contamination mutuelle, deuxièmement, ce réseau peut être utilisé par un attaquant pour trouver des machines vulnérables.

2.2.5 Contrôle des activités

Après avoir subi l'ensemble des contrôles et avoir été positionné dans le contexte désiré, un système peut avoir un comportement ne répondant pas à la politique de sécurité. En observant par exemple la bande passante monopolisée par un utilisateur, il peut être utile d'utiliser les techniques de mise en conformité pour isoler et informer l'utilisateur du non-respect de la charte qu'il a acceptée. La mise en place de système de détection d'intrusions (IDS), comportemental ou par signatures, peut aussi permettre de décider de la mise à l'écart d'un système d'extrémité de manière dynamique. Dans ce cas, la réactivité de l'infrastructure à se protéger est bonne mais le risque d'erreur est aussi important, de plus les risques de dénis de service ne sont pas négligeables.

2.3 ÉTUDE COMPARATIVE DES SOLUTIONS DISPONIBLES

Plusieurs solutions NAC sont disponibles. Elles peuvent être classifiées sous deux principales catégories : commerciales et libres.

2.3.1 Les Solutions Commerciales

2.3.1.1 Microsoft : Network Access Protection (NAP)

Les déploiements de la technologie NAP exigent des serveurs dotés de Windows Server 2008 ou 2012 et plus . De plus, cela suppose que des ordinateurs clients, exécutant Windows XP, Windows Vista, Windows 7 ou Windows 8, soient disponibles. Le serveur central chargé de l'analyse de détermination de l'intégrité pour la technologie NAP est un ordinateur doté de Windows Server 2008 ou 2012 et d'un serveur NPS (Network Policy Server). NPS est l'implémentation Windows du serveur et proxy RADIUS (Remote Authentication Dial-In User Service). Le NPS remplace le service d'authentification Internet (IAS ou Internet Authentication Service) dans le système d'exploitation Windows Server 2003. Les périphériques d'accès et les serveurs NAP assument la fonction de clients RADIUS pour un serveur RADIUS NPS. NPS effectue une tentative d'authentification et d'autorisation d'une connexion réseau puis, en fonction des stratégies de contrôle d'intégrité, détermine la conformité de l'intégrité des ordinateurs et la manière de restreindre l'accès réseau d'un ordinateur non conforme.

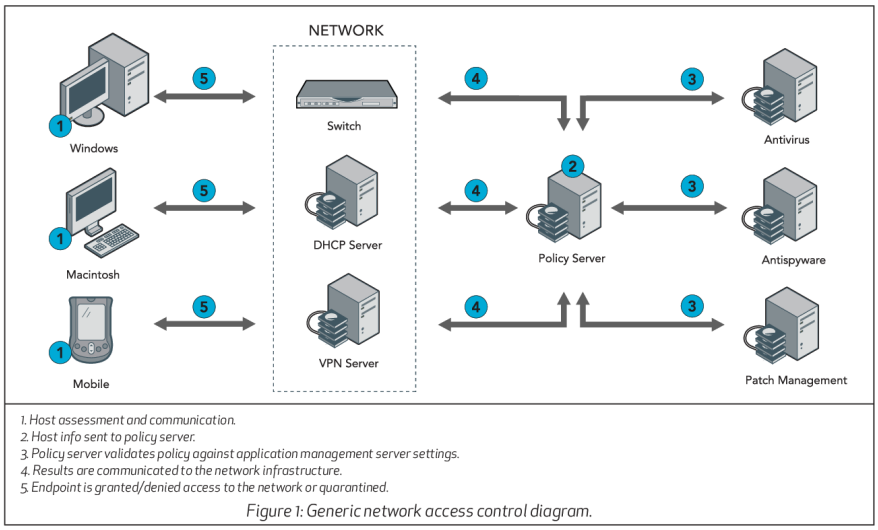

FIGURE 2.1. Architecture d'une solution Microsoft NAP

2.3.1.2 Solution Juniper

La solution Juniper ou Unified Access Control (UAC) s'appuie sur les normes de l'industrie, notamment 802.1X, RADIUS, IPsec et IF-MAP de TNC, lesquelles permettent l'intégration de la solution UAC à n'importe quel équipement de sécurité et réseau tiers. Elle combine l'identité des utilisateurs, le statut de sécurité des dispositifs et les informations sur l'emplacement dans le réseau pour créer une stratégie de contrôle des accès, unique pour chaque utilisateur (qui fait quoi et quand ?). La solution peut être activée en couche 2 à l'aide du protocole 802.1X, ou en couche 3 via un déploiement de réseaux superposés. UAC peut également être mis en oeuvre dans un mode mixte qui utilise le protocole 802.1X pour contrôler les admissions sur le réseau et la couche 3 pour contrôler les accès aux ressources.La figure suivante présente un exemple d'architecture pour une solution UAC :

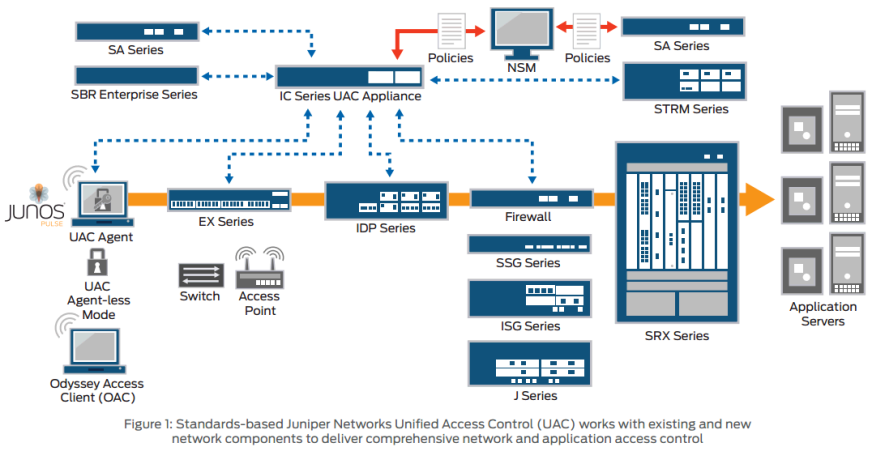

FIGURE 2.2. Architecture de la solution Juniper UAC

2.3.1.3 Solution Cisco : CNAC

La solution NAC proposée par Cisco est constituée de différents composants. Le « NAC Manager » est une interface Web permettant de créer les politiques de sécurité et de gérer les connexions en cours. Les différents profils utilisateurs associés aux vérifications de conformité, ainsi que les actions de remédiation, sont configurés sur ce serveur. Le NAC Manager communique et gère le NAC Server. Le « **NAC Server** » est un serveur qui va accorder ou non l'accès au réseau en fonction des informations recueillies sur les systèmes d'extrémité. C'est sur ce serveur que sont situés les profils de sécurité, les actions de remédiation etc... Ce serveur peut fonctionner en coupure ou « out of band » au niveau 2 ou 3.

— Le « **NAC Agent** » est un agent léger installé sur les postes, chargé de collecter

des informations sur le poste et de les transmettre à l'ACS (serveur Radius Cisco) au moment de la demande de connexion. Des composants additionnels sont aussi proposés.

— Le « **NAC Profiler** » est chargé d'évaluer les systèmes d'extrémité spécifiques comme les téléphones IP, les imprimantes, etc. Ce module permet aussi de localiser physiquement les matériels connectés et d'appliquer des profils en fonction d'informations récupérées.

— Le « NAC Guest Server » permet d'offrir et de gérer les accès pour les visiteurs.

— Le « **Secure Access Control System** » (ACS) est un serveur jouant le rôle de serveur Radius ou Tacacs qui va accorder ou non l'accès au réseau aux utilisateurs. C'est lui qui communique avec les équipements réseaux sur lesquels les connexions sont faites en jouant le rôle d' « authenticator » lors de connexion 802.1X.

Le concept développé par Cisco est l'utilisation de l'ensemble des composants du réseau (commutateurs, routeurs, pare-feu, détecteurs d'intrusions...) pour collecter des informations ou pour appliquer la politique de sécurité décidée.

2.3.2 Les Solutions Libres

2.3.2.1 FreeNAC

La solution FreeNAC effectue l'authentification via deux modes :

- Mode VMPS : les machines du réseau sont identifiées par leur adresse MAC. Les utilisateurs ne sont pas authentifiés dans ce mode.
- Mode 802.1x : les machines du réseau peuvent être authentifiées par certificat et les utilisateurs d'un domaine Windows par leur compte.

L'attribution d'un VLAN est basée sur l'adresse MAC d'une machine. En mode VMPS, l'authentification et l'attribution ont lieu en une seule étape. En mode 802.1x, l'authentification des utilisateurs (dans le domaine Windows), ou celle des machines (par certificat), se déroule en premier, et ce n'est que par la suite que l'adresse MAC est utilisée pour l'attribution du VLAN. (FreeNAC).

2.3.2.2 OpenNAC

OpenNAC est un contrôle d'accès réseau open source pour les environnements d'entreprise LAN/WAN. Active l'authentification, l'autorisation et l'audit basés sur des règles l'accès au réseau. Prend en charge différents fournisseurs de réseau tels que Cisco, Alcatel, 3Com ou Extreme Networks, et différents clients tels que les PC, Mac et périphériques Windows

ou Linux comme les smartphones et les tablettes. Basé sur des composants open source et un auto développement, il s'appuie sur les standards de la comme FreeRadius, 802.1x, AD, LDAP, ... Il est très extensible, de nouvelles fonctionnalités peuvent être intégrées grâce à son architecture de plugin. Facilement intégrable avec les systèmes existants. Enfin et surtout, il fournit des services à valeur ajoutée tels que la gestion de la configuration, le réseau, les configurations de sauvegarde, la découverte réseau et surveillance du réseau.

Fonctionnalités avancées

- Authentification basée sur la norme 802.1x pour les appareils compatibles Prise en charge de l'authentification basée sur LDAP ou DA (Active Directory).
- Prise en charge de la détection des périphériques malveillants à l'aide de traps 802.1x ou SNMP Configuration de masse pour les appareils en ligne à l'aide du module onNetConf
- Mass Backups pour les appareils en ligne utilisant le module onNetBackup.
- Détection du système d'exploitation, antivirus, pare-feu et mises à jour du système Opérateur pour mettre en place une politique d'accès.

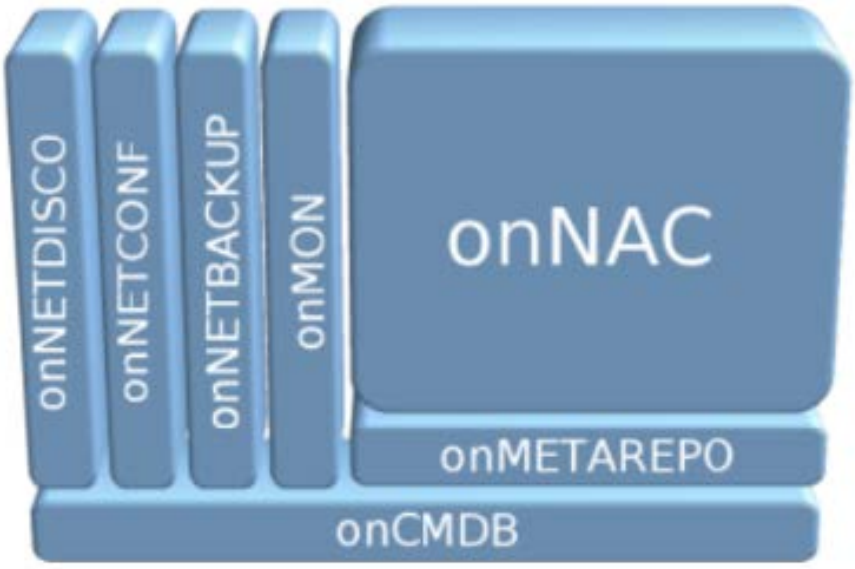

FIGURE 2.3. Architecture générale openNAC

2.3.3 Solution Choisie Pour la Sécurité

2.3.3.1 PacketFence

PacketFence est une solution de contrôle d'accès au réseau (NAC) entièrement prise en charge, fiable et open source. Avec un ensemble impressionnant de fonctionnalités qui comprend un portail captif pour la journalisation et la correction, la gestion centralisée Filaire et sans fil, prise en charge 802.1X, isolation de couche 2 pour les appareils problématiques,intégration avec Snort IDS et scanner de vulnérabilité Nessus ; PacketFence peut être utilisé pour protéger efficacement les réseaux, des réseaux petits à très grands réseaux hétérogènes.

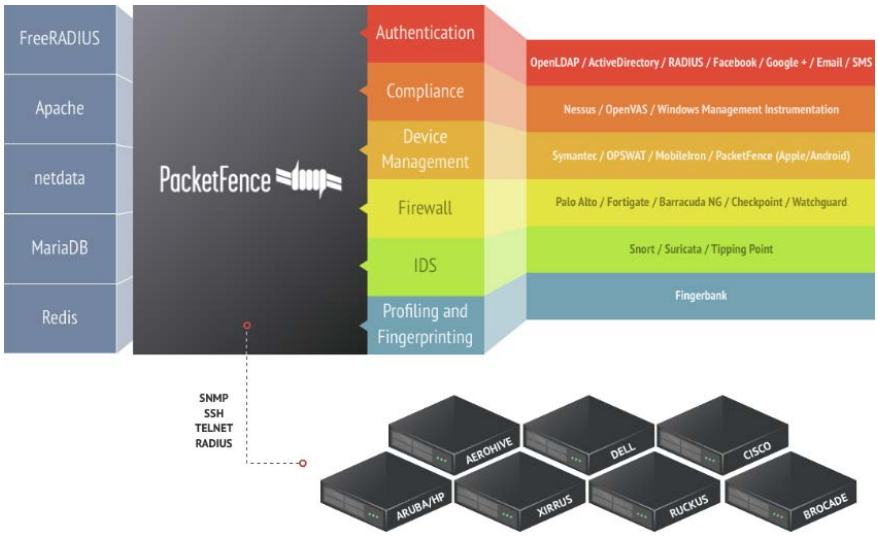

FIGURE 2.4. Architecture des composantes PacketFence

Fonctionnalités avancées

- **Gestion flexible du VLAN** et contrôle d'accès basé sur les rôles : La solution est basée sur le concept d'isolation du réseau à l'aide d'affectations VLAN. Pour ce faire, il n'est pas nécessaire de modifier la topologie du réseau existant, la seule chose qui sera nécessaire pour le faire est de créer deux nouveaux VLAN, un pour L'enregistrement et un pour l'isolement. En outre, il prend également en charge la méthode par rôles de différents fabricants. Le VLAN et les rôles peuvent être attribués de différentes manières :
  — Par commutateur (par défaut pour VLAN)
  — Par catégorie de client (par défaut pour les rôles)
  — Par client

— Utiliser n'importe quelle décision arbitraire (si des extensions Perl sont utilisées)
De plus, la méthode By Switch peut être combinée avec les autres. Par exemple, avec une configuration PacketFence par défaut, les imprimantes ou les PC (s'ils sont classés correctement) peuvent se voir attribuer un VLAN ou un rôle en fonction de l'équipement auquel ils sont connectés. Cela implique que des VLAN de type « par bâtiment » ou « par appareil » peuvent être facilement réalisés.

- **Accès invité - BYOD** : PacketFence offre la prise en charge d'un rôle ou d'un VLAN spécial pour les invités. Si un VLAN invité est activé, le réseau doit être configuré de manière à ce que ledit VLAN invité ne puisse avoir accès qu'à Internet, au VLAN d'enregistrement et au Portail Captif pour savoir comment s'enregistrer pour y avoir accès ou comment cela fonctionne. Il existe différentes méthodes pour l'inscription des invités (si nécessaire) :
  — Enregistrement manuel des invités.
  — Mot de passe du jour.
  — Auto-inscription (avec ou sans informations d'identification).
  — Parrainage d'accès invité (un employé répondant à un invité).
  — Accès invité via e-mail de confirmation.
  — Accès invité via confirmation mobile (via SMS).
  — Accès invité via l'authentification Facebook/Google/GitHub
  — Empreintes digitales DHCP :vous pouvez bloquer les appareils en fonction votre empreinte DHCP.Pratiquement chaque système d'exploitation a une empreinte DHCP unique, vous pouvez donc bloquer l'accès réseau à différents appareils en fonction de cette empreinte.
  — Adresses MAC : vous pouvez spécifier certains modèles d'adresses MAC auxquelles vous ne souhaitez pas accorder l'accès. De cette façon, nous pouvons vous empêcher d'accéder au réseau, par exemple, un fabricant spécifique.
- **Inscription automatique** :
  — Par périphérique réseau
  — Par empreinte DHCP
  — Par fabricant dans l'adresse MAC

  Prise en charge de PKI et EAP-TLS : PacketFence prend en charge EAP-TLS pour l'authentification basée sur des certificats et fournit également une petite solution PKI qui peut être utilisée pour générer un certificat TLS pour chaque appareil ou utilisateur. En outre, il s'intègre également à la solution PKI de

Microsoft. PacketFence utilisera le protocole d'échange de certificat simple (SCEP) pour communiquer avec le service d'inscription de périphérique réseau (NDES) de Microsoft afin de créer le certificat approprié lors d'un processus d'intégration de périphérique final.

— Comptabilisation de la bande passante
— Intégration Microsoft Active Directory
— Déploiement progressif
— Extensible et personnalisable

- **Authentification flexible** : PacketFence peut authentifier les utilisateurs à l'aide de divers protocoles/normes. Cela permet à PacketFence d'être intégré au réseau sans que les utilisateurs finaux aient besoin de mémoriser un autre compte et mot de passe. Les sources d'authentification prises en charge sont les suivantes :

LDAP	RADIUS	Fichier utilisateur local	OAuth2
Microsoft Active Directory	CiscoACS	Format Apache htpasswd	Facebook
OpenLDAP	FreeRadius, Radiator		Google
			GitHub
			LinkedIn
			Microsoft Live

- **Basé sur les normes** PacketFence est conçu pour utiliser des normes ouvertes et éviter la dépendance vis-à-vis des fournisseurs. Parmi ces normes figurent :
  — 802.1X
  — Protocole de gestion de réseau SNMP
  — RADIUS
  — Netflow / PIFIX
  — Itinérance du FAI sans fil (WISPR)

  Compte tenu des informations obtenues via les pages Web officielles de chacun des outils, vous pouvez vérifier comment, sur le site Web de PacketFence, vous pouvez trouver beaucoup plus d'informations sur votre produit, ainsi qu'une explication de chacune des caractéristiques qu'il comprend, tandis que dans la page Web de openNAC, nous ne pouvons trouver qu'une liste des fonctionnalités qu'il inclut et des informations sur les avantages du produit en général, et un bref résumé sur Chacun des modules qui le composent. Cette première impression fait pencher la balance vers faveur de PacketFence, sans même entrer dans les détails pour le moment. **Voici les différences concernant les fonctionnalités les plus utiles pour ce projet de chacun de ces outils illustrés au moyen d'un tableau**.

Caractéristiques	PacketFence	OpenNAC
Déploiement hybride (hors bande + en ligne)	OUI	NON
Prise en charge 802.1X	OUI	OUI
Enregistrement de l'appareil	OUI	NON
Détection d'activités anormales dans le réseau	OUI	NON
Correction via le portail captif	OUI	NON
Contrôle d'accès basé sur les rôles	OUI	NON
Accès invité (BYOD)	OUI	OUI
Prise en charge de PKI et EAP-TLS	OUI	NON
Basé sur des normes	OUI	OUI
Détection et surveillance du réseau	OUI	OUI
Prise en charge basée sur LDAP ou AD	OUI	OUI
Politiques d'accès personnalisables	OUI	OUI
Configuration de masse pour appareil en ligne	OUI	OUI

TABLE 2.2 – Tableau de comparaison des fonctionnalités entre PacketFence et OpenNAC

CHAPITRE 3

MISE EN OEUVRE DU NAC POUR LA DGSN

Contents

3.1 POINTS D'APPLICATION

Un aspect important du contrôle d'accès au réseau qui doit être pris en compte par toute entité souhaitant utiliser une solution NAC est le chemin sur lequel le NAC doit être effectué. En général, le contrôle d'accès est déployé selon deux types de méthodes dans l'infrastructure du réseau, à savoir le NAC basé sur les ports et le NAC basé sur les passerelles..

3.1.1 NAC basé sur les ports

Cette voie de déploiement NAC est fondamentalement construite autour de l'élément de sécurité du port sur un commutateur réseau 802.lX. Le NAC basé sur le port est intégré autour de l'idée de renforcer la sécurité intégrale du port du commutateur par l'utilisation de la norme 802.lX. 802.lX est une norme de sécurité IEEE utilisée pour l'authentification sur un réseau local câblé ou sans fil par l'utilisation de paquets EAP (Extensible Authentication Protocol). Les hôtes s'authentifient à l'aide d'un attribut EAP avant que l'accès à la liaison de données de couche 2 ne soit fourni au réseau particulier (Cygnia.co.uk, 2 juillet 2009). Une solution conçue autour d'un déploiement basé sur le port mettra en quarantaine les périphériques ou les machines jugés non conformes ou qui ne répondent pas aux exigences d'une politique spécifique à la périphérie du réseau. Le point d'application du NAC basé sur le port est donc placé sur le commutateur ou le point d'accès sans fil. La zone dans laquelle les invités non conformes sont placés se trouve dans un VLAN ou un port d'isolation dédié.

3.1.1.1 Problèmes liés au NAC basé sur les ports

Parmi les problèmes relatifs au déploiement basé sur les ports, on trouve des facteurs tels que le déploiement réel de cette méthode. Le déploiement basé sur les ports peut être un processus très complexe et peut être très difficile à mettre en oeuvre, en particulier sur les réseaux à grande échelle. Cela est dû aux complications liées aux exigences des commutateurs, à l'intégration des composants dans l'infrastructure du réseau et aux compatibilités des dispositifs (les commutateurs prennent-ils en charge la norme 802.lx, etc.). Des difficultés peuvent également survenir lors de la segmentation du réseau en VLANs nécessaires à la prise en charge de la norme 802. lx. La configuration des serveurs RADIUS, des interfaces et la détermination des normes NAC qui seront appropriées à l'infrastructure sont également des éléments clés qui peuvent être difficiles à résoudre. De nombreuses compétences sont nécessaires pour gérer un déploiement 802.lx du contrôle d'accès au réseau sur une infrastructure réseau.

3.1.2 NAC basé sur une passerelle

Le déploiement NAC basé sur les passerelles fonctionne différemment du déploiement basé sur les ports. Le déploiement basé sur le port effectue sa mise en application dans la couche 2 (liaison de données) tandis que le déploiement de passerelle effectue sa mise en application dans la couche 3 au niveau du réseau. Il effectue des restrictions par rapport aux adresses IP des dispositifs. Le déploiement par passerelle ne nécessite pas l'utilisation

de l'EAP et utilise plutôt les capacités d'un agent pour s'authentifier par le biais de l'identification de l'utilisateur ou de la machine. L'agent est également utilisé pour effectuer des contrôles de santé et de qualité générale sur les appareils qui ont été identifiés. Le point d'application du déploiement d'une passerelle se fait par l'intermédiaire de pare-feu, ce qui rend la zone de quarantaine à la périphérie du réseau ou à la passerelle par défaut. Le déploiement basé sur une passerelle est une méthode de contrôle d'accès au réseau qui évite la complexité du déploiement basé sur les ports 802.lx, tout en exerçant un degré respectable de sécurité au sein d'une architecture de réseau.

3.1.3 Lequel est le plus adapté pour notre projet

Le choix du type de déploiement le plus avantageux pour une organisation dépend entièrement des objectifs de l'entreprise et de ce qu'elle souhaite obtenir du contrôle d'accès au réseau. Le déploiement basé sur la passerelle peut être considéré comme plus adapté si une organisation a pour objectif d'effectuer des contrôles de santé et de fournir un mécanisme permettant de garantir la conformité aux politiques des périphériques d'extrémité au sein du réseau. Si l'objectif principal de l'organisation est de garantir une sécurité stricte autour des appareils qui se branchent sur le réseau, les solutions 802.lx basés sur les ports sont mieux adaptées. En effet, le déploiement basé sur les ports empêche les machines non autorisées d'avoir accès lorsqu'elles sont connectées à l'infrastructure du réseau via un commutateur ou un point d'accès. Dans notre cas, nous allons utiliser le NAC basé sur les ports.

3.2 IMPLEMENTATION DE LA SOLUTION NAC

Cette section du projet traite de la mise en OEuvre du contrôle d'accès au réseau sous la forme d'un environnement de laboratoire. L'objectif principal est de tester et de transmettre certaines des caractéristiques du contrôle d'accès au réseau par l'utilisation d'une solution NAC. La mise en oeuvre passe par l'installation, la configuration et les tests essentiels d'une solution NAC.

3.2.1 Environnement du travail

Dans cette section on introduira l'environnement matériel et logiciel utilisé pour la réalisation de ce projet.

3.2.1.1 Environnement matériel et logiciel

Processeur	Intel(R) Core (TM) i7-7700HQ CPU @ 2.80GHz 2.81 GHz
RAM	16 Go
Type du système	Système d'exploitation 64bits
Edition Windows	Windows 11 Professionnel

TABLE 3.1 – les caractéristiques du PC utilisé pour la démonstration

Nom de l'outil	La version
PacketFence	PacketFence-ZEN-v11.2.0
VMware-Workstation	VMware-workstation-full-16.1.1
GNS3	GNS3-2.2.33.1-all-in-one-regular
GNS3 VM	GNS3 VM -2.2.33.1
Routeur Cisco VIOS	viosl2 adventerprisek9 m vmdkSSA 1524 0 55 E
Switch Cisco VIOS	i86bi linux adventerprisek9 ms 155 2 T bin
PC1 WINDOW 10	Windows 10 x64 vmdk
PC2 WINDOW 7	Windows 7 x64 vmdk

TABLE 3.2 – liste des outils utilisés pour la démonstration

3.2.2 PacketFence

PacketFence est la solution utilisée pour démontrer et exercer le domaine du NAC dans un environnement de laboratoire. Il est basé sur Debian 11(la version d'installation iso et su r CentOS (pour la version ZEN), c'est une application de contrôle d'accès au réseau gratuite et à code source ouvert, créée comme un mécanisme d'authentification des utilisateurs via les politiques d'identification d'un réseau, d'examen de l'état des dispositifs en termes de qualité et de présentation d'une application d'auto-remédiation. PacketFence est basé sur la méthode de déploiement 802.lx basés sur les ports en ce qui concerne le contrôle d'accès au réseau et se targue d'une quantité impressionnante de fonctionnalités en ce qui concerne les méthodes et les politiques de sécurité. La solution principale offre des fonctions telles que Snort IDS et des analyses via le scanner de vulnérabilité Nessus.

3.2.2.1 PacketFence ZEN

L'intégration de l'application PacketFence dans une architecture réseau peut s'avérer une tâche complexe, dont la mise en oeuvre complète dans un environnement réseau peut parfois prendre des mois. PacketFence ZEN (Zero Effort NAC) est une Appliance VMWare, basée sur Linux, qui constitue une version compacte de la solution. Bien qu'elle ne possède pas toutes les fonctionnalités de la version complète, elle constitue un moyen efficace de tester et d'exercer certains attributs NAC. Il fournit une version allégée et précompilée

de PacketFence construite autour d'un système d'exploitation CentOS. PacketFence ZEN offre une méthode de test du NAC sous la forme d'un processus d'enregistrement. Cette fonctionnalité de ZEN permet d'exercer une fonctionnalité clé du contrôle d'accès au réseau sous la forme d'une authentification d'un utilisateur en fonction de son "enregistrement" pour accéder au réseau.

3.2.3 Les étapes de déploiement

En ce qui concerne le type d'application de PacketFence. La méthode en-ligne (une Appliance bloquante au niveau applicatif) a été choisie plutôt que la méthode Out-of-band (utilise l'infrastructure existante : blocage des commutateurs) raison de la facilité de gestion du projet et de la perspective de ce qui était considéré comme plus approprié pour le déploiement. Des tests avec la méthode d'application hors bande VLAN ont été tentés mais n'ont pas donné de résultats concrets en raison du manque de temps et des complications liées au type de commutateur pris en charge. Une fois que le commutateur Cisco 2960 a été configuré avec les VLAN nécessaires (enregistrement, gestion, isolation, invité, authentification MAC), le serveur PacketFence n'a pas pu récupérer les interfaces configurées dans lesquelles elles étaient placées. C'est un aspect du projet qu'il serait bénéfique de revoir si cela était possible. Comme l'application du VLAN est une fonctionnalité efficace de PacketFence, d'une manière qui décompose vraiment en détail la méthode de déploiement 802.lx basés sur le port.

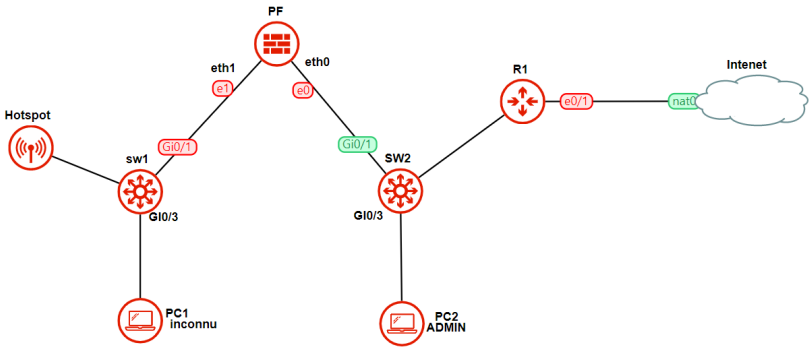

FIGURE 3.1. Architecture de déploiement sous GNS 3

3.2.3.1 Préparation de l'infrastructure

Création des machines Virtuelles Via Workstation, on a importé la machine virtuelle PacketFence Zen téléchargé depuis le site officiel (Packetfence, 2022), une machine virtuelle Windows 7 pour administrer PacketFence et une autre Windows 10 qui permettra de tester le système de contrainte. Pour que PacketFence ZEN fonctionne correctement, une mémoire dédiée de 8 Go est nécessaire pour garantir une exécution efficace de la solution. Une fois l'Appliance démarrée dans la machine virtuelle, les informations d'identification "root" et "p@ck3tf3nc3" comme nom d'utilisateur et mot de passe sont nécessaires pour se connecter à l'interface.

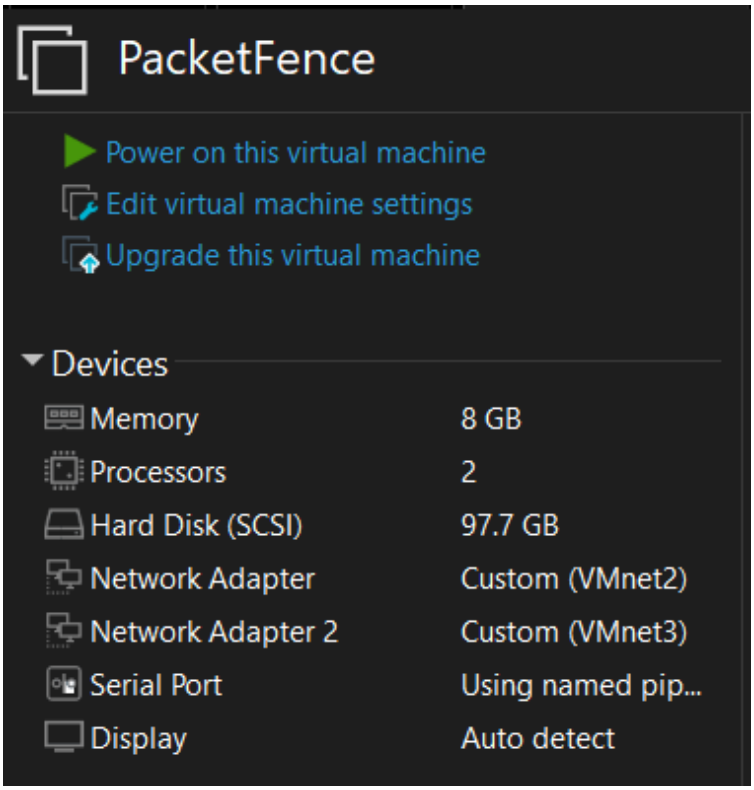

FIGURE 3.2. Configuration VMWare pour Packetfence

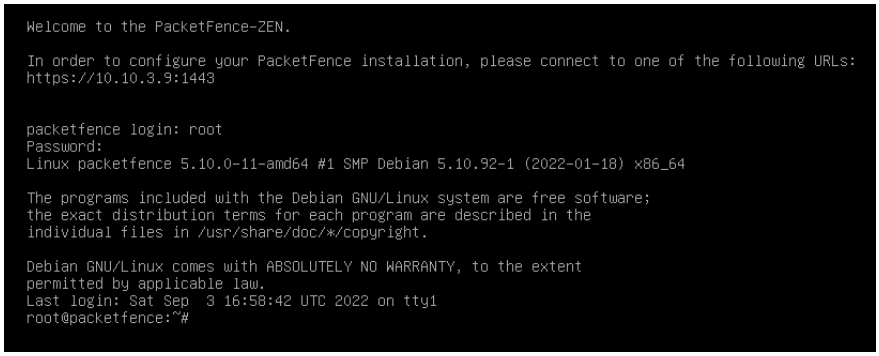

FIGURE 3.3. lancement et connexion sur packetfence

La connexion entre PacketFence et les Switch 1 et 2 • On a configuré les cartes réseaux virtuelles ; @IP et mode (Host Only)

• On braché Packetfence et le switch 1 à travers la carte VMnet3(eth1) en mode Host only, ensuite nous avons branché Packetfence au switch 2 à travers la carte VMnet 2 (eth0) en mode Host only également. Ensuite, on a assigné l'adressage des interfaces du NAC en saisissant la commande :

#nano /etc/network/interfaces

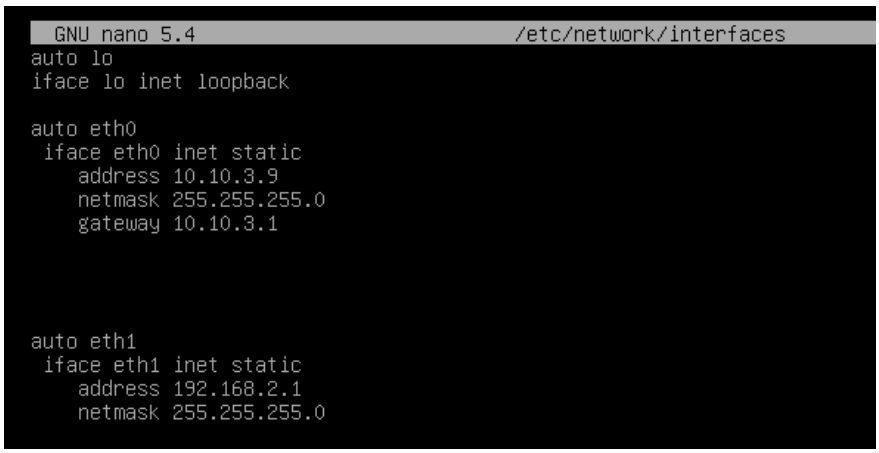

FIGURE 3.4. Adressage des interfaces de Packetfence

Configurations des switches

Switch 1 Ici nous n'avons fait aucune modification sur le switch

Switch 2 Ici, nous avons configuré le routage des paquets et crée le vlan 3 pour le management de packetfence, ensuite nous l'avons assigné à interface GigabitEthernet0/1 qui est relié à packetfence en mode trunk. Nous avons aussi fait passer l'interface GigabitEthernet0/3 au vlan3 car elle sera raccordée avec le pc admin (Windows 7) pour l'administration. On met le switch en mode config en saisissant la commande « configure terminal » ensuite on passe aux commandes suivantes :

```
hostname SW2
ip routing
ip route 0.0.0.0 0.0.0.0 10.11.11.1
int g0/0
no switchport
ip address 10.11.11.2 255.255.255.248
exit
router eigrp 1
network 10.11.11.0
network 10.10.3.0
exit
no ip domain-lookup
ip name-server 8.8.8.8
vlan 3
name Management
exit
interface vlan 3
description vlan Management
ip add 10.10.3.1 255.255.255.0
no shutdown
exit
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 3
switchport mode trunk
spanning-tree portfast
exit
```

```
SW2#show ip interface br
SW2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/2     unassigned      YES unset  down                  down
GigabitEthernet0/3     unassigned      YES unset  up                    up
GigabitEthernet0/0     10.11.11.2      YES NVRAM  up                    up
GigabitEthernet1/0     unassigned      YES unset  down                  down
GigabitEthernet1/1     unassigned      YES unset  down                  down
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  down                  down
GigabitEthernet2/0     unassigned      YES unset  down                  down
GigabitEthernet2/1     unassigned      YES unset  down                  down
GigabitEthernet2/2     unassigned      YES unset  down                  down
GigabitEthernet2/3     unassigned      YES unset  down                  down
GigabitEthernet3/0     unassigned      YES unset  down                  down
GigabitEthernet3/1     unassigned      YES unset  down                  down
GigabitEthernet3/2     unassigned      YES unset  down                  down
GigabitEthernet3/3     unassigned      YES unset  down                  down
Vlan3                  10.10.3.1       YES NVRAM  up                    up
SW2#
```

FIGURE 3.5. configuration du switch 2

On passe en mode config ensuite nous saisissons les commandes suivantes :

```
hostname R1
interface G0/1
ip address dhcp
ip nat outside
no shutdown
exit
ip route 0.0.0.0 0.0.0.0 192.18.18.1
ip name-server 8.8.8.8
int G0/0
ip address 10.11.11.1 255.255.255.248
ip nat inside
no shutdown
exit
router eigrp 1
network 10.11.11.0
network 10.10.3.0
network 10.10.55.0
ex
access-list 1 permit 10.11.11.0 0.0.0.7
access-list 3 permit 10.10.3.0 0.0.0.255
```

```
ip nat inside source list 1 int G0/1 overload
ip nat inside source list 3 int G0/1 overload
```

```
R1#show ip interface br
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                10.11.11.1      YES NVRAM  up                    up
Ethernet0/1                192.168.119.129 YES DHCP   up                    up
Ethernet0/2                unassigned      YES NVRAM  administratively down down
Ethernet0/3                unassigned      YES NVRAM  administratively down down
Ethernet1/0                unassigned      YES NVRAM  administratively down down
Ethernet1/1                unassigned      YES NVRAM  administratively down down
Ethernet1/2                unassigned      YES NVRAM  administratively down down
Ethernet1/3                unassigned      YES NVRAM  administratively down down
Serial2/0                  unassigned      YES NVRAM  administratively down down
Serial2/1                  unassigned      YES NVRAM  administratively down down
Serial2/2                  unassigned      YES NVRAM  administratively down down
Serial2/3                  unassigned      YES NVRAM  administratively down down
Serial3/0                  unassigned      YES NVRAM  administratively down down
Serial3/1                  unassigned      YES NVRAM  administratively down down
Serial3/2                  unassigned      YES NVRAM  administratively down down
Serial3/3                  unassigned      YES NVRAM  administratively down down
NVI0                       10.11.11.1      YES unset  up                    up
```

FIGURE 3.6. Configuration du router R1

3.2.3.2 Configuration de l'infrastructure

Paramétrage de base Pour configurer PacketFence, on a accédé à son interface graphique Web via la machine Windows 7 en saisissant l'adresse IP définit statiquement plus haut dans la barre d'adresse : https ://10.10.3.9 :1443/ Passons maintenant à la configuration de base de notre système y compris le nom de domaine, adresse ipv4 masque de sous réseaux, interface de management.

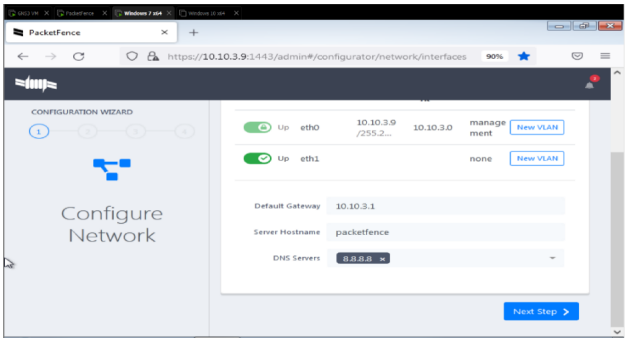

FIGURE 3.7. Interface web de configuration packetfence

Compte administrateur et base de données

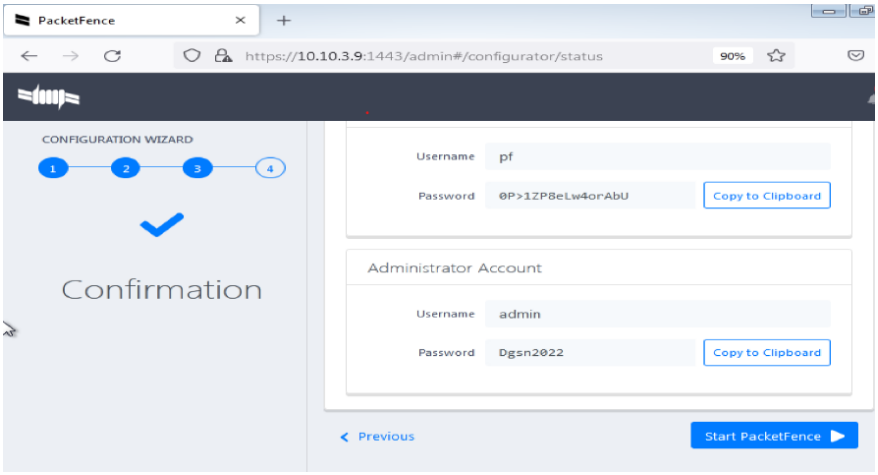

FIGURE 3.8. configuration de la base de données packetfence

Une fois que les configurations générales sont définies efficacement pour l'environnement PacketFence et que le compte administrateur a été créé, les configurations générales nécessaires à la démonstration devraient être achevées. En cliquant sur continuer, vous accéderez à la page des services PacketFence où une liste des principales fonctions des applications sera présentée, ainsi que leur statut actuel (démarré ou arrêté). En cliquant sur le bouton "démarrer les services PacketFence", vous lancerez les services de démarrage spécifiques fournis par PacketFence ZEN, dans ce cas, le serveur devrait être opérationnel. Si tout est configuré de manière appropriée PacketFence générera un message confirmant le succès du processus et invitant l'utilisateur à se rediriger vers l'interface d'administration.

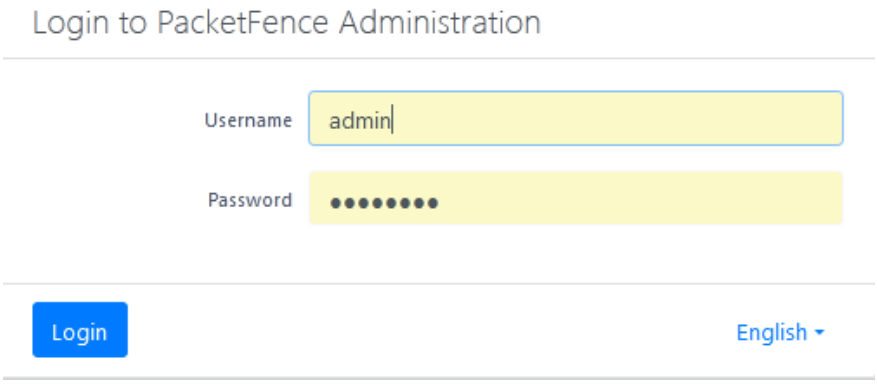

FIGURE 3.9. page de connexion packetfense

3.2.3.3 Ajout d'une interface Inline

PacketFence peut être configuré dès le départ à l'aide du configurateur PacketFence pour la mise en contrainte. Dans cet exemple, nous allons continuer à développer notre déploiement initial en ajoutant une nouvelle interface en ligne pour notre installation PacketFence. La première étape consiste à ajouter une carte d'interface réseau (NIC) dédiée à notre installation actuelle de PacketFence. Dans notre exemple, notre nouvelle carte réseau sera nommée Eth1. L'interface Web de PacketFence listera toutes les interfaces réseau actuellement installées sur le système. Une adresse IP et un masque de réseau seront visibles si l'interface réseau est configurée (soit par DHCP soit déjà configurée manuellement). Vous pouvez peux modifiez ceux-ci, créez/supprimez des VLAN sur des interfaces physiques et activez/désactivez des interfaces. Noter que ces modifications entrent en vigueur immédiatement. La persistance sera écrite uniquement pour activer interfaces. Ce qui signifie que si vous modifiez votre adresse IP de gestion, pour poursuivre le configurateur, vous devrez vous rendre sur cette nouvelle adresse IP que vous venez de définir. En tout temps, vous devrez définir une interface de gestion. Cela signifie que les types d'interface requis pour l'application en ligne sont : • Management • Inline Layer 2

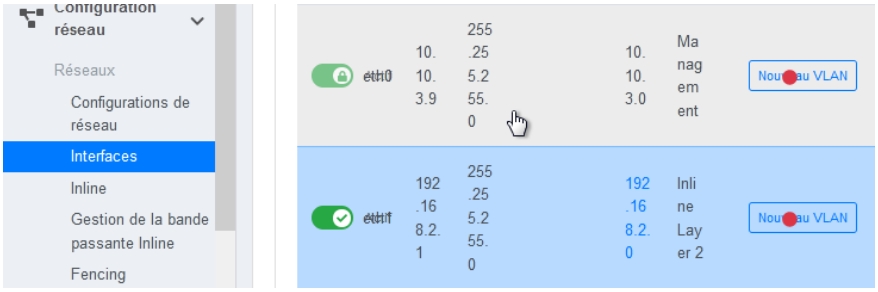

FIGURE 3.10. Interface nécessaire pour le déploiement En ligne

Notons que PacketFence fournira ces services sur son interface en ligne :
• PacketFence fournit son propre service DHCP. Il se chargera de la distribution des adresses IP dans notre Réseau en ligne. PacketFence ne fournira pas de services DHCP sur le réseau de gestion -c'est la responsabilité de votre propre infrastructure.
• PacketFence fournit son propre service DNS. Cependant, pour le mode en ligne, vous aurez également besoin pour donner accès au serveur DNS de votre infrastructure.
Dans 'Configuration→ Configuration réseau →Interfaces', cliquez sur le nom logique Eth0. Fournissez les informations suivantes : IP Address : 192.168.2.1 Netmask : 255.255.255.0 Type : Inline Layer 2 Additional listening daemon(s) : portal DNS Servers : 10.10.3.1,8.8.8.8,192.168.2.1

Enfin, depuis Status →Services, redémarrez le portail haproxy, pfdhcp, iptables, pfdhcplistener, services pfdn.

3.2.3.4 Ajout d'un profile de connexion Inline

La prochaine chose à faire est d'ajouter un nouveau profil de connexion - pour les appareils provenant du réseau en ligne. Nous voulons montrer aux utilisateurs le portail captif avec nos sources d'authentification Null.
Depuis 'Configuration→ Politiques et contrôle d'accès→ Profils de connexion', cliquez sur 'Ajouter un profil'. Fournissez les informations suivantes : - Nom du profil : inline - Filtres : Si nécessaire Réseau 192.168.2.0/24 - Sources : null-source Cliquez ensuite sur "Enregistrer".

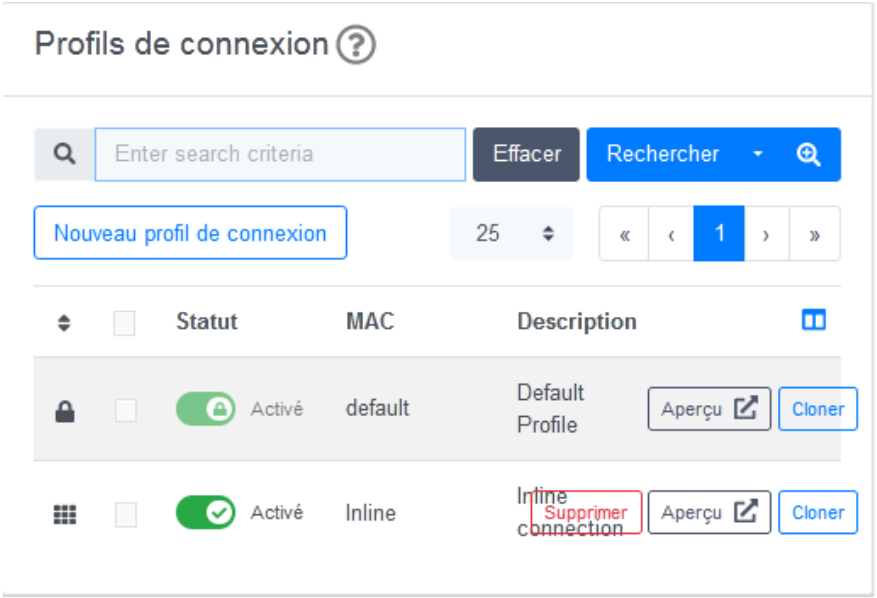

FIGURE 3.11. Ajout d'un profil de connexion

3.2.4 Test de la configuration Inline

Nous pouvons maintenant tester le processus d'enregistrement. Pour ce faire : - connectons un appareil non enregistré (PC1) au commutateur1 (voir figure 3.1) - vérification que PacketFence fournit une adresse IP à l'appareil. Regardez dans le fichier journal suivant : /usr/local/pf/logs/packetfence.log ou vérifiez sur l'ordinateur que vous obtenez une IP dans le Dans la bonne plage de sous-réseau Depuis l'ordinateur - ouvrir un navigateur Web - essayez de nous connecter à un site HTTP (pas HTTPS, par exemple http ://www.packetfence.org) - S'assurer que, quel que soit le site auquel vous voulez vous connecter, vous n'avez accès qu'à

la page d'enregistrement. -Enregistrez l'ordinateur en utilisant la source d'authentification Null.

FIGURE 3.12. portail captif test de connexion avec un appareil non enregistré

Une fois qu'un ordinateur a été enregistré : - assurez-vous que PacketFence modifie les règles du pare-feu (ipset -L) de manière à ce que l'utilisateur soit autorisé à travers. Regardez dans le fichier journal de PacketFence : /usr/local/pf/logs/packetfence.log - à partir de l'interface d'administration web, allez sous Noeuds et assurez-vous que vous voyez l'ordinateur comme étant comme "Enregistré". - l'ordinateur a accès au réseau et à l'Internet

FIGURE 3.13. Activation de l'accès réseau par Packetfence

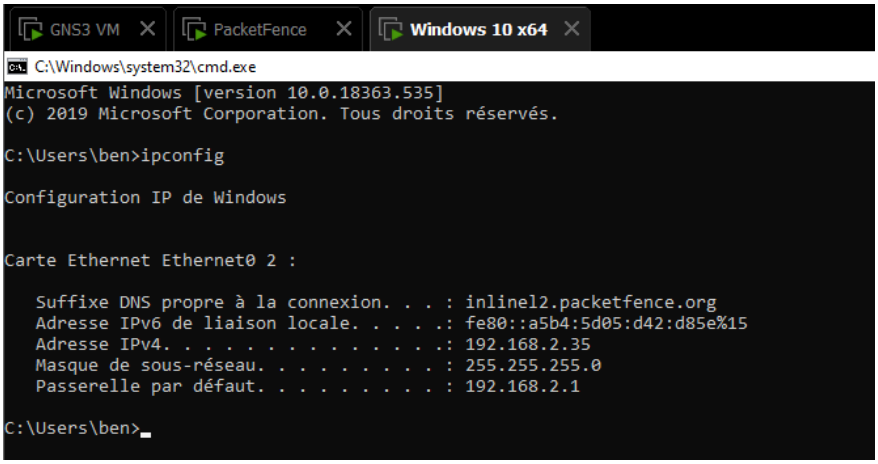

FIGURE 3.14. Adresse attribuée au pc1 après enregistrement

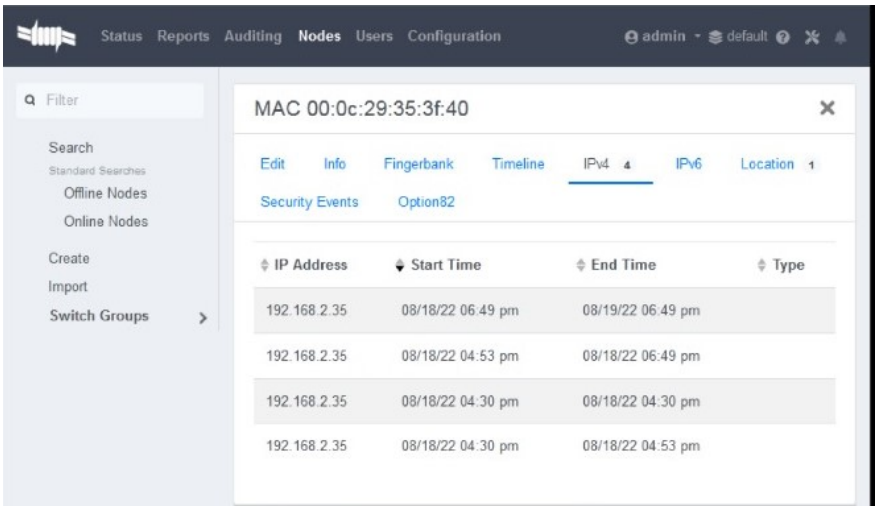

FIGURE 3.15. Detection d'adresse MAC

3.2.5 Gestion du trafic

Il est possible d'activer la Gestion de la bande passante en fonction du rôle de l'appareil. Pour l'activer, vous devez : Aller dans 'Configuration → Configuration du réseau → Gestion de la bande passante inline' et sélectionner le Rôle pour lequel vous souhaitez définir une limite. Définissez une limite de vitesse d'upload et de download et enregistrez. Ensuite redémarrez le service tc pour appliquer les nouvelles règles.

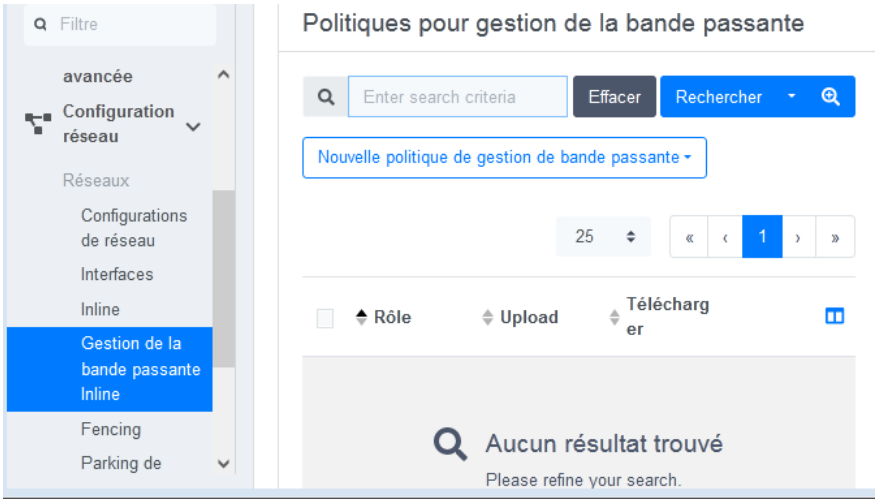

FIGURE 3.16. Gestion de la bande passante pour le profile Inline

CHAPITRE 4

RÉSULTATS OBTENUS

Contents

4.1 Phase 1

La phase 1 de la mise en oeuvre a permis de développer les bases nécessaires au déploiement initial de la solution NAC. Elle a permis de jeter les bases de l'architecture réseau utilisée pour la démonstration et d'acquérir des connaissances sur le téléchargement et la configuration initiale de la machine virtuelle et de l'Appliance PacketFence. Ainsi que les méthodes alternatives possibles par lesquelles la démonstration pourrait être exercée.

4.2 Phase 2

La phase 2 de la mise en oeuvre était basée sur les configurations essentielles nécessaires pour que le serveur PacketFence soit opérationnel. Elle fournit un aperçu des commandes

initiales nécessaires pour le système d'exploitation CentOS ainsi qu'un guide sur la façon dont l'environnement PacketFence a été établi.

4.3 Phase 3

La phase 3 de la mise en oeuvre était plus particulièrement basée sur la surveillance de l'environnement PacketFence et sur la fourniture d'un aperçu et d'une évaluation de la solution à travers l'aspect administratif de l'environnement. Le test et l'évaluation de la fonction d'enregistrement de la solution ont également été effectués, ainsi que la création et le suivi des dispositifs connectés au réseau.

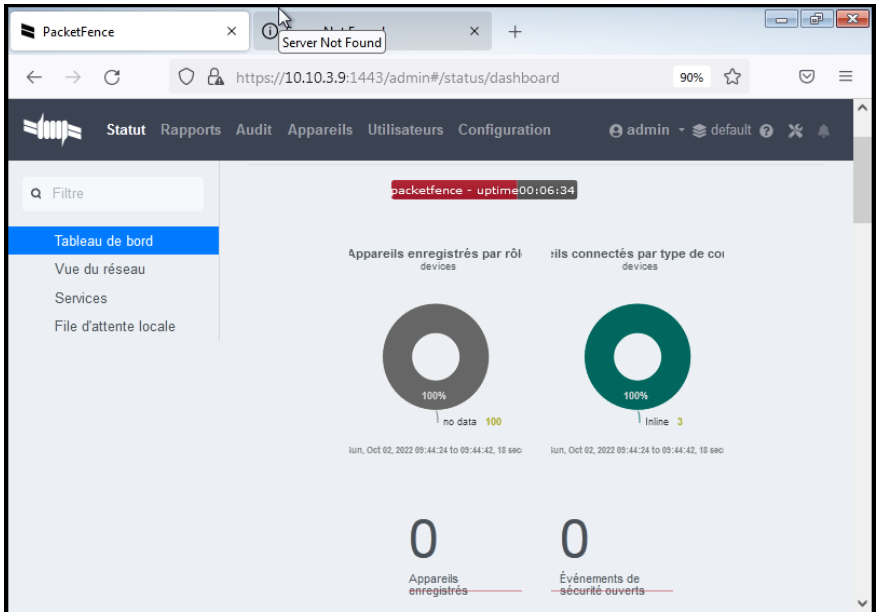

FIGURE 4.1. Tableau de bord packetfence

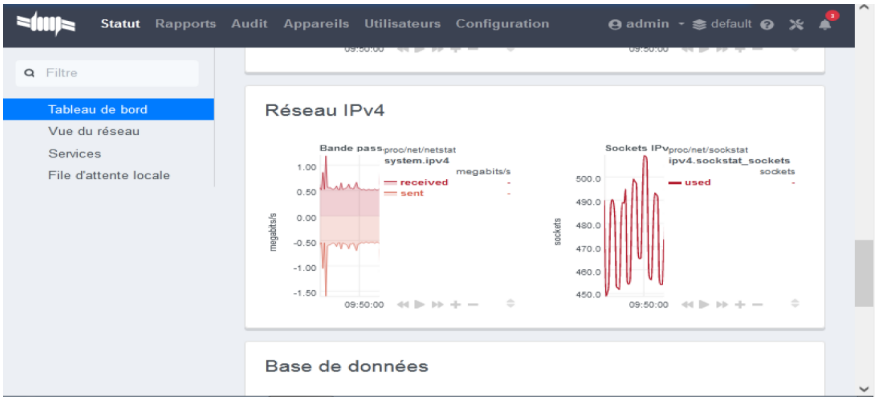

FIGURE 4.2. Diagramme Réseau

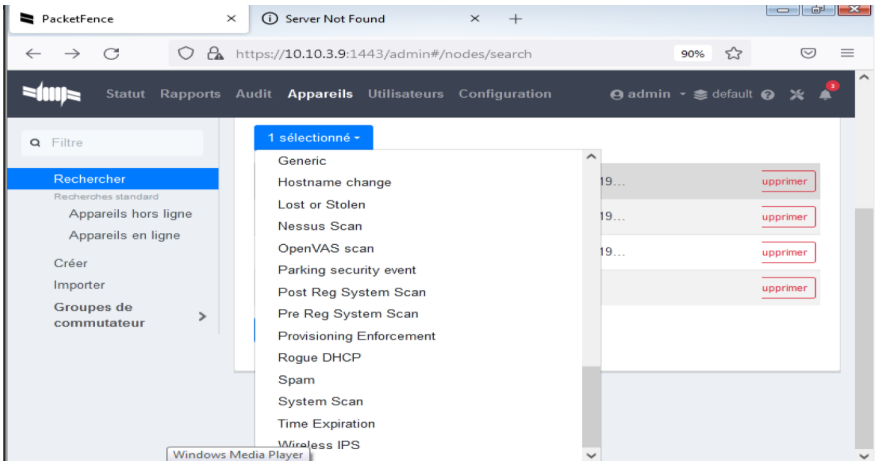

FIGURE 4.3. Quelqiues opérations possibles sur les appareils enregistrés

4.4 Les Limites

PacketFence ZEN était l'application utilisée pour démontrer le contrôle d'accès au réseau.. Les limites concernant la mise en oeuvre du NAC dans un environnement de laboratoire tournent autour de la méthode par laquelle la solution de PacketFence a été déployée. Le type d'application en ligne de PacketFence ZEN limite la démonstration à l'enregistrement et au l'enregistrement et le désenregistrement d'un dispositif dans le réseau. qui, à leur tour, bloqueraient le trafic de cet appareil vers le réseau, mais sans possibilité pour l'appareil de le réprimander. La remédiation à un réseau alternatif était également une limitation, car l'application en ligne ne prend pas nécessairement en charge cette fonctionnalité. Ceci est dû à l'absence d'un VLAN alternatif pour rediriger le dispositif qui a failli se mettre

en conformité. La solution PacketFence est une application difficile à mettre en oeuvre sur n'importe quel réseau. Avec des délais de production qui prennent généralement des mois pour l'intégration. Limitation en ce qui concerne l'exercice et la configuration de certaines des autres fonctionnalités NAC de PacketFence, telles que les analyses de performance et la remédiation en cas de violation telles que les analyses de performance et les mesures correctives en cas de violation.

4.5 Recommandation

Les recommandations pour ce projet s'appliquent notamment à la manière dont la démonstration a été configurée. L'application du VLAN comme méthode initiale d'application serait l'élément principal à prendre en considération pour l'exercice futur de la solution . Ceci est dû au fait que ce type d'application est une meilleure méthode pour tester la solution.La mise en oeuvre du VLAN permettrait d'examiner plus de fonctionnalités en raison du fait que plus de ports seraient disponibles pour démontrer des aspects tels que la remédiation, la détection MAC, l'isolation, la quarantaine, etc. En ce qui concerne le matériel, un commutateur administrable Cisco devrait être envisagé, car il permettrait un meilleur contrôle des états spécifiques des appareils ainsi que des trappes SNMP et une sécurité .renforcée des ports.

CONCLUSION GÉNÉRALE

Le stage que j'ai effectué à la Délégation Générale à la Sûreté nationale m'a donné la possibilité d'être en contact direct avec le monde du travail et découvrir les outils de contrôle d'accès au réseau. En réalité ce stage m'a donné une occasion favorable de faire les premiers pas dans le domaine professionnel après la formation à l'école car il m'a permit de transformer et de voir la différence entre la théorie et la pratique.

Il a donné une grande opportunité, d'une part il m'a permis de tester mes compétences et de démontrer mon savoir-faire et d'autre part il m'a donné la possibilité de gagner en expérience en travaillant auprès des ingénieurs de la structure qui étaient toujours là pour me soutenir et m'apprendre de nouvelles notions.

Le but de notre Travail était la mise en oeuvre d'une solution de contrôle d'accès réseau au sein du réseau local DGSN, pour cela nous avons mené une étude sur les technologies NAC existantes et nous avons choisie Packetfence comme solution , ensuite nous l'avons installé et configuré pour qu'il puisse enregistrer les appareils se connectant au réseau.

BIBLIOGRAPHIE

1. Boivent, F. (2009).
   ⇒Étude du contrôle d'accès au réseau (NAC) pour l'Université de Rennes1. Rennes.
2. Caballero, J. M. (2019).
   ⇒ Control de acceso sobre red cableada. Universidad del Pais Vasco.
3. Ryan, C. (2015).
   ⇒ Network Access Control as Network Security solution. lnstitute of Technology Tallaght Dublin, Dublin.
4. `https://www.packetfence.org/about.html#/overview`
   ⇒ Périphériques réseau pris en charge, Fonctionnalités avancées, Présentation
5. `https://www.juniper.net/documentation/en_US/learn-about/LA_802.1X_NAC.pdf`
   ⇒ Learn About 802.1X Network Access Control (NAC)
6. `https://opennac.org/opennac/en/solution.html`
   ⇒ Présentation et Fonctionnalité OpenNac.