MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
UNIVERSITY OF SAAD DAHLEB - BLIDA 1

FACULTY OF SCIENCES

DEPARTMENT OF COMPUTER SCIENCES

Study and deployment of the PacketFence open-source solution to control the Network Access

Report submitted for the fulfillment of the Master degree

Domain: MI

Affiliation: Informatics

Option: Computer systems and networks

By:

AMOKRANE Idir

BRAHIM Badreddine

Jury:

President: Mr. Douga Yassine

Examiner: Mrs. Hayat Daoud

Supervisor (SONATRACH**):**

Mr. Neffah Mohamed

Promoter (USDB**):**

Mr. Ould-Khaoua Mohamed

Academic year: 2022/2023

Abstract

Companies are subject to daily attacks that could result in a number of catastrophes. Companies might protect their computer systems with the support of a solid security plan. Although the field of security is vast, we are particularly interested in using the posture strategy to control access to their computer network and compliance control of the machine that connects to it. We know that in some institutions, the number of users who frequently request the network is very important, making the need for a solution even more pressing.

We have suggested a PacketFence solution that offers a network approach for secure access. The implemented solution effectively manages network access, assigns VLANs dynamically and roles to access that comply with predefined rules, and permits both employees and visitors to bring their own devices.

Key words : PacketFence, Network Access Control, Protection, Open-source, Bring your own device.

الملخص

تتعرض الشركات لهجمات يومية يمكن أن تؤدي إلى عدد من الكوارث. يمكن للشركات حماية أنظمة تكنولوجيا المعلومات الخاصة بها من خلال خطة أمنية قوية. على الرغم من أن مجال الأمان واسع ، إلا أننا مهتمون بشكل خاص باستخدام استراتيجية الموقف للتحكم في الوصول إلى شبكة الكمبيوتر الخاصة بهم والتحكم في الامتثال للجهاز الذي يتصل بها. نحن نعلم أنه في بعض المؤسسات ، يكون عدد المستخدمين الذين يطلبون الشبكة بشكل متكرر أمرًا مهمًا للغاية ، مما يجعل الحاجة إلى حل أكثر إلحاحًا.

اقترحنا حل PacketFence الذي يوفر منهجًا شبكيًا للوصول الآمن. يدير الحل الذي تم تنفيذه الوصول إلى الشبكة بكفاءة ، ويقوم بشكل ديناميكي بتعيين شبكات محلية ويعين أدوار الوصول وفقًا لقواعد محددة مسبقًا ويسمح للموظفين والزوار بإحضار أجهزتهم الخاصة.

الكلمات الدالة: PacketFence ، التحكم في الوصول إلى الشبكة ، حماية ، المصدر المفتوح ، أحضر جهازك الخاص

Résumé

Les entreprises sont soumises à des attaques quotidiennes qui peuvent entraîner un certain nombre de catastrophes. Les entreprises peuvent protéger leurs systèmes informatiques en s'appuyant sur un plan de sécurité solide. Bien que le domaine de la sécurité soit vaste, nous sommes particulièrement intéressés par l'utilisation de la stratégie de posture pour contrôler l'accès à leur réseau informatique et le contrôle de conformité de la machine qui s'y connecte. Nous savons que dans certaines institutions, le nombre d'utilisateurs qui sollicitent fréquemment le réseau est très important, ce qui rend le besoin d'une solution encore plus pressant.

Nous avons proposé une solution PacketFence qui offre une approche réseau pour un accès sécurisé. La solution mise en œuvre gère efficacement l'accès au réseau, attribue des VLANs de manière dynamique et des rôles d'accès conformes à des règles prédéfinies et permet aux employés et aux visiteurs d'apporter leurs propres appareils.

Mots clés : PacketFence, Contrôle d'accès au réseau, Protection, Open-source, Apportez votre propre appareil.

Acknowledgements

First of all, we would like to thank Allah the Almighty and merciful who gave us the strength and the patience to accomplish this modest work.

Secondly, we would like to warmly thank our parents and siblings for the support they gave us, our project supervisor Mr. Neffah Mohamed, for the opportunity he gave us to work in a good environment and our promoter Pr. Ould-Khaoua Mohamed for the trust placed in us and for accepting to direct this work. Our sincere thanks to the members of the jury for the interest in our work by carefully examining it. We would like to express our sincere thanks to all the teachers who have taught us and who by their skills have supported us to succeed in our studies.

Finally, we would also like to thank all the people who have participated directly or indirectly in the realization of this work.

Content

List of abbreviations

Abbreviation	Definition
AAA	Authentication, authorization, accounting
ACL	Access control list
AD	Active directory
AR	Access requester
AV	Anti-virus
BYOD	Bring your own device
CN	Common name
CSV	Comma separated values
CVE	Common vulnerabilities and exposures
DB	Data base
DC	Domain component
DN	Distinguished name
EAP	Extensible authentication protocol
IDS	Intrusion detection system
IPS	Intrusion prevention system
ISE	Identity services engine
LDAP	Lightweight directory access protocol
MAB	MAC authentication bypass
NAC	Network access control
NAS	Network access server
OU	Organizational unit
OVF	Open virtualization format
PAE	Port access entity
PDP	Policy decision point
PEP	Policy enforcement point
PF	PacketFence
RADIUS	Remote authentication dial-in user service
SNMP	Simple network management protocol
SSH	Secure socket shell
UAC	Unified access control
VDI	Virtual desktop infrastructure

List of figures

List of tables

General Introduction

Recent years have seen a rise in the importance of laptops in people's daily lives. Customers are incorporating the use of applications into their everyday routines as a result of the quick development in device sales. These robust gadgets feature user-friendly interfaces, are pre-loaded, and have access to millions of apps, not just for leisure but also for work [1].

Thanks to improved connection, applications are being developed to handle tasks that were previously only possible in the office while traveling or at home. Due to the need for security departments to modify their security systems to accommodate mobile devices, this phenomena has led to changes in the organizational structure of businesses. To incorporate these tools into their daily work processes, people are bringing them to work [1].

Businesses must adapt their access control, authentication, availability, and identity management systems because **Bring Your Own Device (BYOD)** may have a significant impact on how they manage their networks, laptops, and even their staff.

This report is about a solution for a problem that the Sonatrach Headquarters building is facing in the idea that everyone should be able to bring their personal devices and use them in the office for more productivity [2]. But we know that this idea can cause major security problems on a network.

The goal of this work is to investigate the significance of network access control, which can be found as a result of businesses having networks that are increasingly distributed, with offices and business centers dispersed across various geographic locations (branches), all of which require network access. The requirement to access data from any device and location without compromising the security and confidentiality of the information, along with the complex interconnectivity environment, increased the importance of the data held by businesses and organizations. Companies need innovative solutions to address the additional risks and hazards that these situations entail. Initiatives and technologies that fall under the umbrella of network access control are developed to address this demand. Due to the frequent neglect of security-related factors, end users typically do not consider security when using a communications system or network. Users may occasionally view security negatively because they perceive it to be inconvenient and interfere with their ability to do a specific task.

However, security is essential when dealing with computer-based tasks since it is the only measure that can ensure that they are completed with a number of guarantees that are assumed in the physical world. In order to specify how to secure network nodes before they access the network, a concept known as "Network Access Control" and a set of protocols are established. Before giving access to the network, NAC provides control mechanisms that enable validation of previously set rules or policies. Allows the back office and the end user's computer equipment to work together with the network infrastructure, such as routers, switches, and firewalls, to guarantee that the information system is working properly before granting access to the network. As the name suggests, network access control regulates access to the network

through pre- and post-admission regulations. Free software can be set up to establish this kind of policy and can be used to provide Access Control.

Study and deployment of the PacketFence open-source NAC solution in an isolated network especially made for this project powered by the Digital Innovation Center in Sonatrach's Headquarters.

- Make a background overview presenting a general study on the Network Access Control solutions and technologies.
- Make a needs analysis to identify functional and non-functional needs and determine the security policies to be applied to secure the network environment to meet these needs.
- Implement a case study, by creating installation, configuration and test environments for the application.

Organization of the report

The remaining sections of the report are divided into three chapters and conclusion :

- **Chapter I:** presents the background of the fundamental notions of Computer Security and Access Controls, the presentation of Access Control solutions available and then choosing the appropriate NAC solution.
- **Chapter II:** is dedicated to the design and deployment of our open-source Access Control solution.
- **Chapter III:** reserved for the functional tests of the solution carried out during this end-of-study project.
- **Conclusion and Future Works:** general summary about the project and the future works.

CHAPTER I: Background

1. Introduction

In this chapter, there will be initiation to the fundamental notions of computer security and Access Controls, the presentation of some NAC solutions available on the market and then choosing the appropriate one.

2. Computer security

There are several needs and requirements in the domain of computers and information systems based on applications. The researcher must look into earlier thoughts or references in his particular circumstance because all study has a goal known as a solution. Considering all factors related to network security, including authentication, authorization, accessibility, confidentiality, integrity, and the security of tools, services, and data [3].

2.1. Computer security fundamentals

The level of a network's security is the assurance that every computer is operating at its peak efficiency and that the people who use the machines only have access to the privileges that have been granted to them [3].

Computer security must guarantee the:

- **Availability:** It is in charge of making sure that its goals are achieved since a system needs to be built to be sufficiently resistant to intrusions and interference to ensure that it operates correctly and is always accessible to users who want to use its services.
- **Integrity:** It is responsible for ensuring that a message or file hasn't been altered since it was created or while it's being transmitted over a computer network.
- **Confidentiality:** It is the property that stops information from being disclosed to unapproved people or systems. Ensure that only those with the proper authorisation have access to information.

2.2. Physical Security

The physical protection of computer hardware and software is covered under physical security. The companies would need to install the hardware and software supporting the connection, together with the interconnection points, in a safe place that is guarded from theft, interference, and harm. We also need to make sure there are environmental safeguards in place to guard against dangers like fire, water, and extreme heat and humidity. Placing computer workstations in safe locations as well to guard against physical theft, loss, damage, and other unwanted access is required too [4].

2.3. Logical Security

Logical Access Controls are tools for identifying users with access to system resources as well as the kinds of transactions and operations they are allowed to perform. To define the privileges of authorized people, including the permissions, the kinds of transactions and functions that are allowed, we use Access Control Lists (ACLs) and access rules (e.g., read, write, execute, delete, create, and search). ACLs are frequently used to setup hardware and software, or they may be delivered to routers and other devices after being administered offline. Setting up access rules is needed to give authorized workers the right access privileges based on their positions or duties [4].

2.4. Access Controls

The Operating System, Application Systems, Databases, a Particular Security Package, or Any Other Utility can all apply these rules. They are a crucial aid in maintaining the integrity of the information (by limiting the number of users and processes allowed access) and in protecting confidential information from unauthorized access, as well as the network operating system, application system, and other software from unauthorized use or modification. It is also practical to take into account additional logical security factors, such as those pertaining to the process used to assess whether an access permit (requested by a user) corresponds to a specific resource [5].

2.4.1. Network Access Control (NAC)

A method to computer security known as Network Access Control (NAC) aims to integrate user or system authentication, endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), and network security enforcement [6].

Network Access Control (NAC) aims to incorporate endpoint security technologies. It includes network security enforcement, user or system authentication, host intrusion prevention, and vulnerability assessment. The end-stations of employees and visitors that do not have anti-virus software installed, patches, or host intrusion prevention systems are one of the most serious risks to companies' networks [7].

The concept's overall goals can be seen as [8]:

- Network connection Authorization, Authentication, and Accounting (AAA).
- Traffic encryption using the 802.1X protocol.
- Compliance checking based on data such as device vulnerabilities.
    - NAC solutions have the ability to prevent clients from connecting to the network if their antivirus software is absent or they need to upgrade their operating system, which lowers the chance of malware spreading to other connected units.
- Easy implementation of policies.

- The administrator can create policies using a NAC solutions, and it will assign these policies to the desired switch or router.

- Identity and access management.
  - Authenticated users are intended to be used in NAC environments rather than IP addresses, which are often used in IP networks to limit or give access.

2.4.2. Types of Network Access Control

There are various types of Network Access Control, which are described below:

- **Hardware-Based NAC:** Whether "Inline" or "Out-of-Band", this solution typically calls for a device that must be deployed in practically any space where NAC is required. Some of these devices function between the Network Access layer and the network switches, while others have replaced the access switches [9].

- **NAC based on Software Agents:** The following stage involves installing small programs called "Agents" on all of the systems that the NAC needs to govern. These agents are resident on computers and other electronic devices. The findings of the device's scans and monitoring are often sent to a centralized server via these agents. In order to comply with security regulations, systems that do not fulfill the standards will not be granted network access authorization, and they frequently receive some sort of remedial step [9].

- **NAC without Software Agents:** Another variation is agentless NAC, which uses on-demand software components. In this configuration, it is intended that a temporary agent, typically an ActiveX control, regularly scans the client for security flaws or violations of the security policy. The scan results are transmitted to the main policy server, where if the system doesn't comply with the standards, an action is taken as needed. The agent is downloaded once the procedure is finished [9].

- **Dynamic NAC:** It also goes by the name of "NAS Peer-to-Peer" because it is a choice that doesn't require any network-level modifications or software installations on every computer. Agents are installed in secure systems and occasionally become required [9].

2.4.3. Network Access Control Concepts

- **Pre-admission and Post-admission:** Policy-based support prior to gaining access to the prevailing design network in NAC. A host must first pass a pre-admission evaluation before being given complete access to the network. After access has been allowed, a host can be periodically examined to make sure it is not becoming a threat due to post-admission evaluation [10].

- **Agent versus Agentless:** The authentication and security evaluation processes in NAC technology can be performed directly by a software agent installed on the endpoint device or indirectly by evaluating the answers of the endpoint device by an external network-based scanning engine [11].

- **Out-of-Band versus Inline:** The placement of the decision-making and enforcement mechanisms inside the network can also affect how NAC is set up. In the case of out-of-band solutions (**Figure I-2)**, a policy server that is not directly involved in network traffic is often used. As an alternative, Inline NAC (**Figure I-1)** systems integrate enforcement and decision-making at a single location that is part of the regular traffic flow [12].

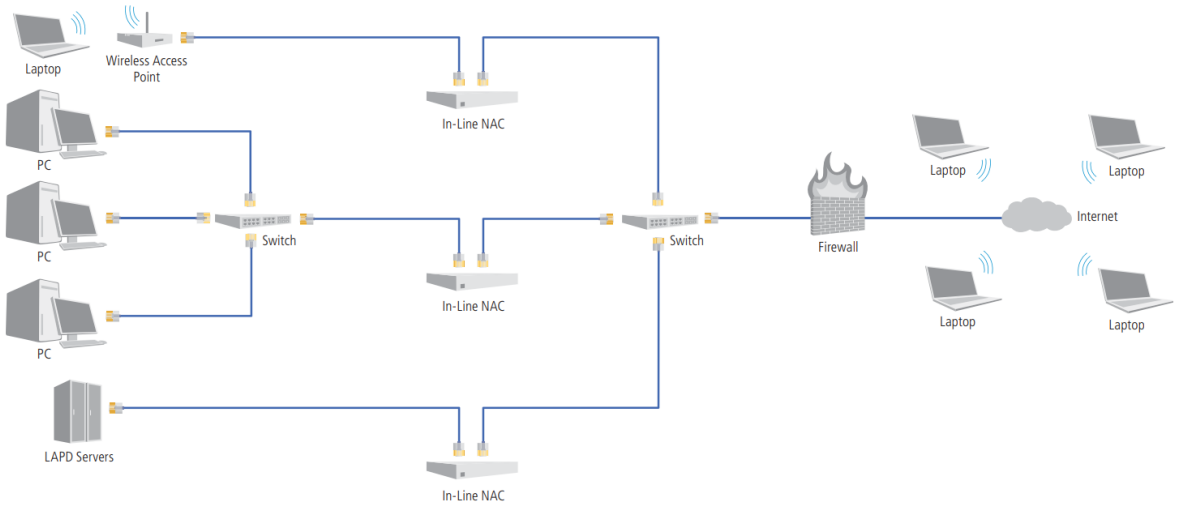

Figure I-1: *Inline NAC Solution*

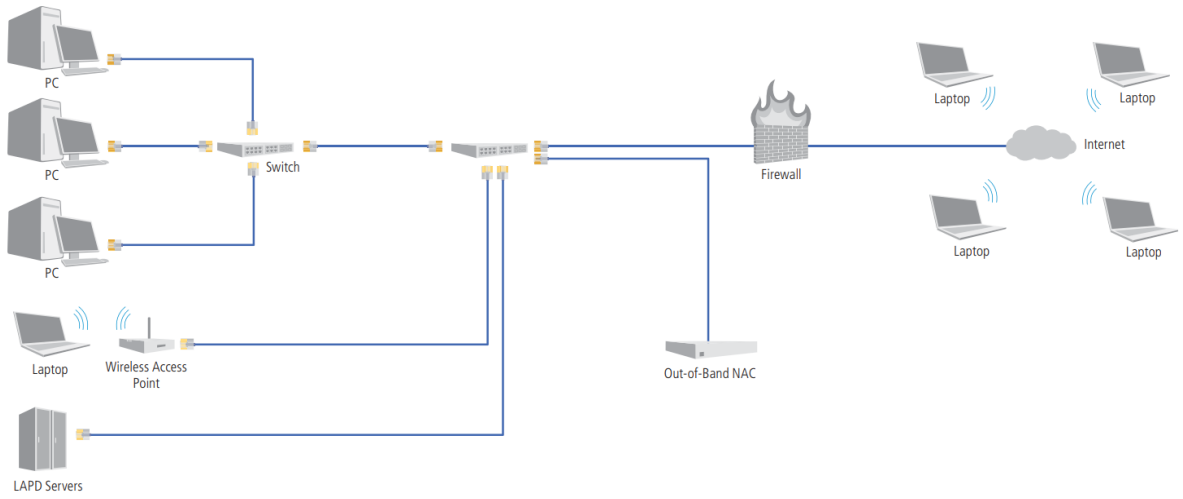

Figure I-2: *Out-of-Band NAC Solution*

- **Remediation, quarantine and captive portals**

The idea behind the deployment of NAC solutions by network operators is that some genuine customers will experience network access denial (if users never had out-of-date patch levels, NAC would be unnecessary). As a result, NAC solutions call for a way to fix the end-user issues that prevent access [6].

There are two typical methods of remediation:

- **Quarantine:** A restricted IP network known as a quarantine network gives users routed access to just specific hosts and Apps. When a NAC product finds that an end-user is out-of-date, the switch port is assigned to a VLAN that is only routed to patch and update servers and not to the rest of the network [6].
- **Captive Portals:** A captive portal blocks HTTP traffic to websites and directs visitors to a website application that offers guidance and tools for updating their PC. No network usage other than the captive gateway is allowed until their computer clears an automatic examination. Paid wireless access operates in a manner akin to this at public access points [6].

2.5. Network Access Control Protocols

2.5.1. IEEE 802.1X Protocol

802.1X is an IEEE standard that provides port-based Network Access Control. It is part of the IEEE 802 (802.1) protocol group. It provides authentication to devices connected to an Ethernet port. This standard can be used for wired or even wireless networks through Wi-Fi access points, 802.1X is a feature available on various network switches.

802.1X actors are shown in the figure (**Figure I-3)**:

- **The Supplicant:** Is the system to authenticate (the client).
- **The Port Access Entity (PAE):** Is the access point to the network.
- **The Authenticator System:** Is the authenticator system. It controls the resources available through EAP [13].

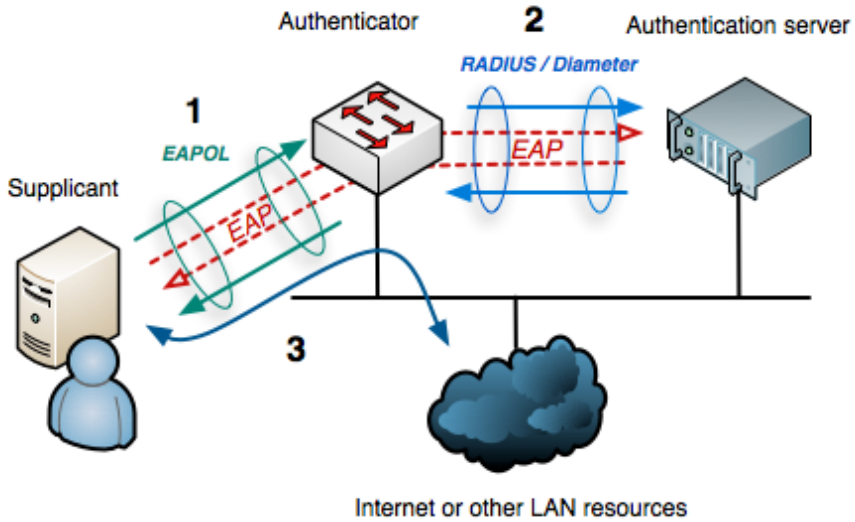

Figure I-3: Diagram showing how 802.1X authentication works [13]

2.5.2. Radius Protocol

The RADIUS protocol (Remote Authentication Dial-In User Service) is an AAA (Authentication Authorization Accounting) type protocol used to centralize the authentication

and authorization of remote access. It is essentially based on a server (RADIUS), connected to an identification database (LDAP for example) and a RADIUS client, called NAS (Network Access Server), acting as an intermediary between the end user and the server. Exchanges between the RADIUS client and the RADIUS server are encrypted and authenticated with the support of a shared secret [14].

There are four different packet types for authentication:

- **Access-Request :** containing user data (login/password, etc.) sent by the access controller.
- **Access-Accept :** if authentication is successful, a message is sent by the server.
- **Access-Reject :** sent by the server when the connection needs to be closed or when the authentication process fails.
- **Access-Challenge :** sent by the server to ask for more details, and therefore, a new Access-Request packet.

The figure below (**Figure I-4**) shows the radius protocol operations flow:

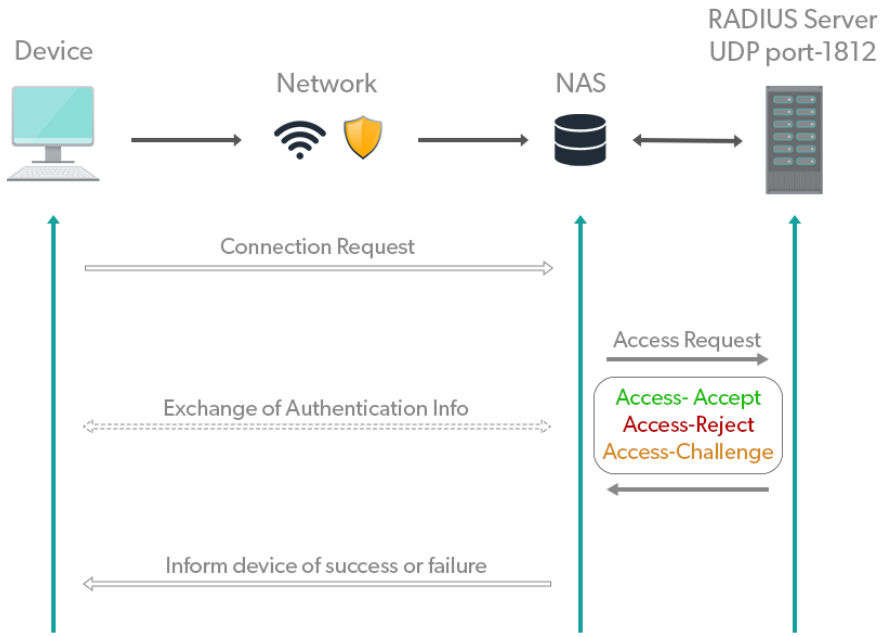

Figure I-4: *Diagram of the RADIUS protocol operations flow [15]*

Radius authentication procedure [16]:

1. The remote user provides the RADIUS client with the login, password, and MAC address necessary for authentication.

2. The "Access-Request" packet is sent by the RADIUS client to the RADIUS server. All user data, including client ID, password, and port number, is contained there. The MD5 hash function will be used to hash the password if one is present.

3. The RADIUS server receives the request, validates the secret it shares with the RADIUS client to ensure the packet's integrity, and then confirms the user's identity by extracting and comparing the data from an AD directory. The RADIUS server has two options: it can either request a new access request or more details.

4. following the challenge, the RADIUS client generates an Access-Request containing the authentication information requested.

5. The request is then verified or denied by the RADIUS server, which then sends a "Access-Accept" or "Access-Reject" packet. A list of authorized services, such as VLAN, may be included in this packet.

2.5.3. EAP Protocol

The EAP protocol (Extensible Authentication Protocol) ensures remote Internet connections and allows the identification of users in the network. It allows the use of several authentication choices, among which are [17]:

- **EAP-MD5:** Authentication with a password.
- **EAP-TLS:** Authentication with an electronic certificate.
- **EAP-TTLS:** Authentication with any authentication method, within a TLS tunnel.
- **EAP-PEAP:** Authentication with any EAP authentication method, within a TLS tunnel.

Basic package types:

- **EAP Request:** Sent by the access controller to the client.
- **EAP Response:** Response from the client to the gatekeeper.
- **EAP Success:** Packet sent to the client at the end of authentication if it is successful.
- **EAP Failure:** Packet sent to the client at the end of authentication if it is failed.

2.6. General Architecture of NAC

All NAC products have three fundamental parts: The Access Requester (also known as the AR), the Policy Decision Point (PDP), and the Policy Enforcement Point (or PEP) [18].

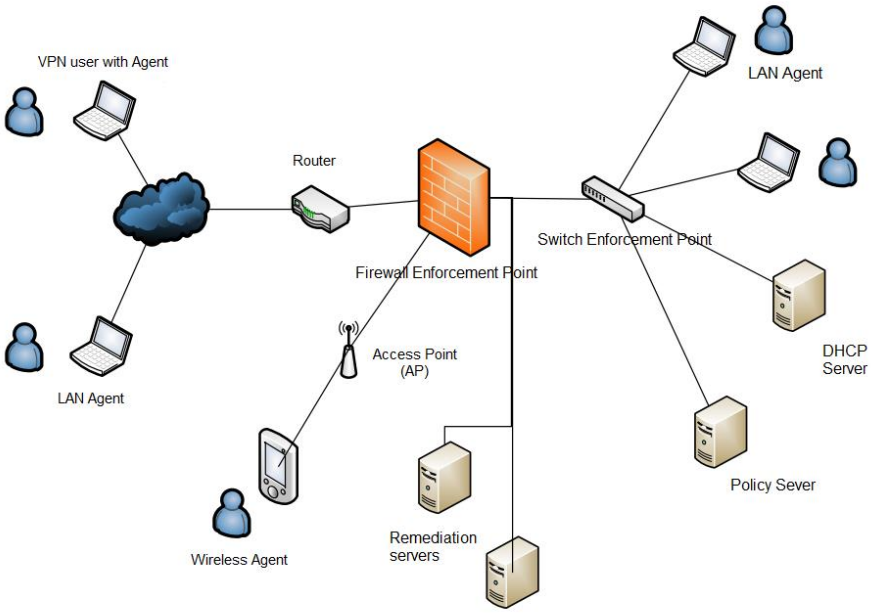

Figure I-5: *General Architecture of NAC [19]*

A high-level NAC architecture is depicted in the previous figure (**Figure I-5**), in which end users can access corporate resources through WLAN, VPN, and LAN[19]. Depending on the vendor's implementation, specific PDP and PEP operations may be located on a single server or dispersed across several servers, but in general, the AR requests access, the PDP assigns a policy, and the PEP upholds the policy.

The AR, which can be any managed device by the NAC system, such as workstations, servers, printers, cameras, and other IP-enabled devices, is the node that is making the attempt to access the network. A different system may examine the host instead of the AR performing its own host assessment. The PDP receives the AR's evaluation in any situation.

The PDP is the mastermind behind everything. The PDP decides what access should be provided based on the AR's posture and a company's specified policy. The NAC product management system may frequently serve as the PDP. In order to assess the state of the host, the PDP frequently uses back-end systems like antivirus, patch management, or a user directory. For instance, an AV manager would inform the PDP if the host's AV software and signature versions were up to date [18].

3. Overview of Network Access Control (NAC) solutions

In this part, we will study some free and commercial network access control (NAC) solutions that exist on the market in order to be able to choose an appropriate solution for our project.

3.1. Commercial access control solutions

3.1.1. Cisco Identity Services Engine (ISE)

Cisco Identity Services Engine (ISE) is a network security policy management platform that provides centralized visibility and control over network access, advanced threat protection, and

integration with third-party security solutions. It is an important tool for organizations to improve their network security posture and protect against advanced threats [20].

Here are a few of its most important and distinguishing features:

• Integrated AAA services that support a variety of identity services, including Active Directory, LDAP, RADIUS, RSA, OTP, and others.

• Integrated BYOD, mobility, and lifecycle management guests with centralized policy management and feature-based access control

• Device health validation and profiling services.

3.1.2. FortiNAC

Fortinet's Network Access Control solution, FortiNACTM, adds visibility, control, and automated reaction for everything that connects to the network to the Security Fabric. In addition to extending management to outside devices and orchestrating automatic responses to a variety of networking events, FortiNAC offers defense against IoT threats [21].

3.1.3. Juniper Unified Access Control (UAC)

Juniper Unified Access Control (UAC) is a network access control solution that provides granular access control and enforcement for enterprise networks. UAC uses a combination of user, device, and location-based policies to enforce access control and deliver consistent security across all network access points, including wired and wireless networks.

UAC provides dynamic policy management and integration with multiple authentication methods, such as Active Directory, LDAP, and RADIUS. It also includes advanced threat detection and mitigation capabilities, such as policy-based quarantine and network access control for IoT devices.

UAC can be deployed as an on-premises solution or as a cloud service, providing organizations with flexibility and scalability. Overall, Juniper UAC is an important tool for organizations looking to secure their network infrastructure and protect against advanced threats [22].

3.2. Open Source Access Control solutions

3.2.1. PacketFence

PacketFence is a Network Access Control (NAC) solution that is reliable, open-source, and free. This robust program is made to protect networks of various sizes, from compact setups to huge and varied infrastructures. Organizations may take use of PacketFence extensive feature set while ensuring the secure protection of their networks. Let's look at some of its notable attributes and abilities [24]:

- Captive-Portal for Registration and Remediation.
- Centralized wired and wireless management.
- 802.1X support.
- Layer-2 isolation of problematic devices.

- Integration with the Snort IDS.
- Integration with the Nessus vulnerability scanner.

3.2.2. OpenNAC

Secure LAN/WAN access is provided by OpenNAC, an open-source Network Access Control. It enables the use of adaptable access policies that are based on rules. It supports a variety of network hardware from Extreme Networks, Cisco, Alcatel, and 3Com as well as clients running Windows, Mac, Linux, and other operating systems.

It is built upon tested open-source building blocks like FreeRadius, iTop, Icinga, and our own creation. It is very flexible and extensible, making it simple to incorporate new features. It is adaptable enough to be integrated with existing systems for asset management, network intrusion detection, and authentication. OpenNAC offers value-added services like network configuration and discovery, backup of network device configurations, and network monitoring in addition to its core Network Access Control functionality [23].

3.2.3. FreeNAC

FreeNAC is a dynamic VLAN management and LAN access control GPL open-source solution. FreeNAC offers simple Virtual LAN assignment, LAN access control (for all types of network devices like servers, workstations, printers, IP-phones, webcams, etc.), real-time inventory of network endpoints, VLAN management, and patch cable documentation. In "VMPS mode," end devices are identified either by MAC addresses or by Certificate & MAC-Address (in "802.1X mode"). FreeRadius is included for 802.1X and OpenVMPS is included for VMPS modes on the communications layer [25].

4. Choosing a network access control solution

In this part we will choose a NAC solution which is the objective of our project based on its operation and the market solutions presented above.

4.1. Comparative study of commercial and Open Source NAC solutions

What differentiates open-source and paid solutions is the supported hardware, the main features, the documentation, the community dedicated to each solution, the ergonomic web interface. To choose a Network Access Control solution, we have to select different architectures, methods and tools. Since the NAC solutions available (free or commercial) are diversified, the choice depends on the criteria presented in the table below:

Table I-1: Comparison between commercial and open-source NAC solutions

Functionalities	Open Source solutions			Commercial solutions		
	OpenNAC	PacketFence	FreeNAC	Cisco ISE	FortiNAC	Juniper UAC
Virtual machine support	✓	✓		✓	✓	
Wired and Wireless Network	✓	✓	✓	✓	✓	✓
Community Support	✓	✓	✓	✓	✓	
Bandwidth Management		✓			✓	✓
Network vendor support	✓	✓	✓		✓	✓
NAC Agent		✓		✓	✓	✓
Device Discovery	✓	✓	✓	✓	✓	✓
Integration with Active Directory	✓	✓	✓	✓	✓	
Reporting Function	✓	✓	✓	✓	✓	✓

4.2. The chosen Access Control solution

The previous table makes a classification of commercial and open-source NAC solutions on the market. The Cisco ISE solution is the leading market leader in NAC solutions. Although it has several advantages, there are a lot of disadvantages such as:

- The cost being very high
- Only Cisco equipment is supported while an open architecture is required in our case for its support for multi-vendor environments.

We note following an in-depth study of free and professional Access Control solutions, several advantages, namely the availability of the source code and the possibility of studying it and modifying it according to our needs and thus distributing it free of charge. In addition, there are several users and developers who offer assistance by sharing documentations and participating in forums, subsequently participating in the improvement of open-source software.

After opting for an open-source solution, the main differences between open-source solutions come from all the supported hardware, the basic functionalities, the possible actions, the documentation, the community specific to each solution, as well as the ergonomics of the Web interface, the granularity of the information obtained, and general security.

The free and open-source Network Access Control (NAC) solution called PacketFence is objectively the best of the commercial and free solutions. It is supported by a company in the event of requests for the development of specific and commercial functionalities. Also, virtualization offers PacketFence deployments by small businesses resource optimization, scalability, cost savings, simplified management, testing capabilities, and increased availability. .In addition, each feature developed for enterprises is in turn subject to the open-source version. The capacities are modular and can be combined. It is capable or comes with a captive portal for registration and remediation, centralized wired and wireless management, powerful BYOD management options, 802.1X support, bandwidth management, layer 2 isolation of problematic devices, integration with Snort/Suricata (IDS/IPS), Nessus/OpenVAS vulnerability scanners, integration with Active Directory, and NAP (Network Access Protection) clients for Health Check (SoH).

Any network, no matter how big or little, may be securely protected using PacketFence. Here are the most suitable network types that PacketFence could run in banks, colleges and universities, engineering companies, convention and exhibition centers, hospitals and medical centers, hotels, manufacturing, school boards, telecommunications companies.

5. Network Access Control tools

Network Access Control systems and tools are diverse, we will have to work with some of the tools compatible with the PacketFence solution and that meet the needs of the company.

5.1. Some of PacketFence components

Here, we'll go over a few of the components that PacketFence uses to carry out its functions. Although PacketFence also supports the integration of some commercial solutions, the majority of available options are open-source.

the figure below presents a summary of PacketFence main components and features :

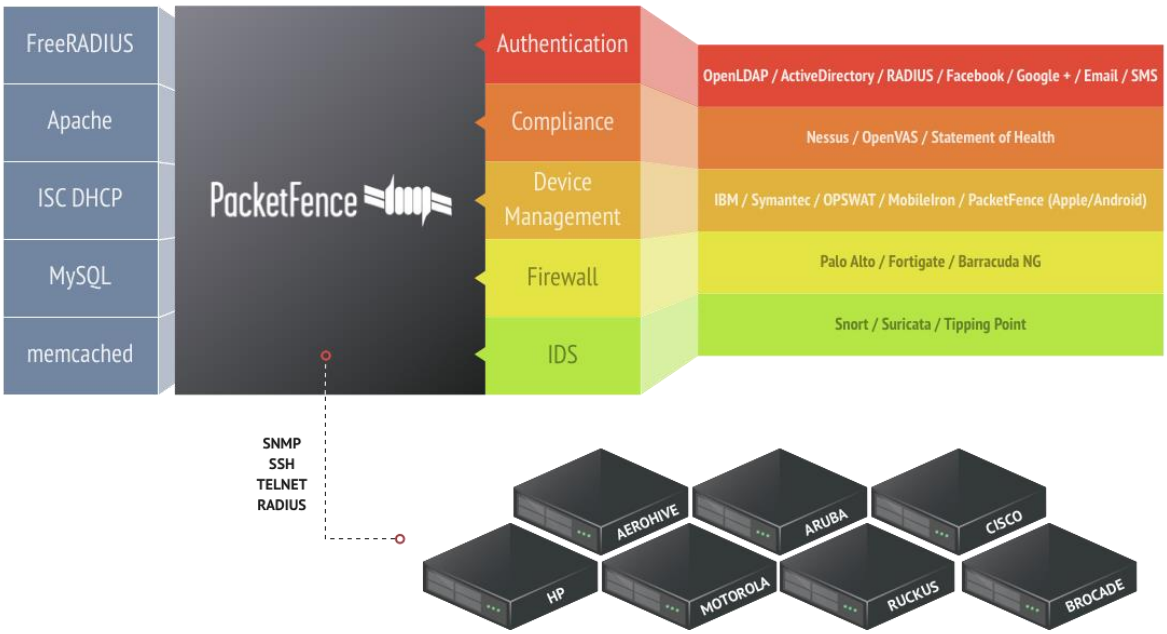

Figure I-6: *PacketFence Components Architecture [24]*

5.1.1. FreeRADIUS protocol

An open-source server called FreeRADIUS is one of the most versatile and feature-rich enterprise radius servers currently on the market, it provides an alternative to other radius servers. Internet Service Providers use FreeRADIUS, among other things, to authenticate their clients and send them an IP configuration. It is thought to be the world's busiest server [26].

5.1.2. Snort Intrusion Prevention System

Throughout the globe, Snort is the leading open-source Intrusion Prevention System (IPS). To identify malicious network activity, Snort IPS employs a set of rules. It then searches for packets that fit those criteria and warns users when it finds them [27]. Since Snort needs a constant internet connection and that our network is isolated from the internet due to security reasons. We won’t be able to add Snort in our PacketFence solution.

5.1.3. Nessus

In terms of vulnerability scanning, Nessus is the market leader. It has the ability to spot vulnerabilities, minimize risk, and guarantee that virtual, mobile, and cloud environments are functioning properly.

It offers malware detection, vulnerability analysis, update management, and sensitive data exploration. It is available in two versions: one for individuals costs $1500 annually, and the other costs $5,000 annually for businesses [28].

The following features are available:

- Scanning without requiring the installation of an agent on the target device; grouping vulnerabilities according to CVE (Critical, High, Medium, Low, Info).
- Flexible results formats (XML, PDF, HTML, CSV).

- Sending results by email.
- And sharing results (requires a corporate version).

5.1.4. OpenVAS (Open Vulnerability Assessment System)

It combines a number of services and tools to provide a very powerful vulnerability scanner. Additionally, OpenVAS can be used to manage these vulnerabilities effectively. The scanner gets the tests to detect vulnerabilities from a feed called "vulnerability tests" (VTs), which contains more than 150,000 vulnerability tests and has a long history and daily updates. All OpenVAS products are GNU GPL-licensed [29], [30].

6. Conclusion

In this chapter, we explored Network Access Control (NAC) strategies in the context of computer security. We studied the basic notions of computer security and Access Control, such as Network Access Controls and physical and logical security measures, were first defined. We looked into the concepts, protocols, and overall architecture of NAC, among other things.

Following that, we reviewed both commercials and open-source NAC solutions, highlighting some notable examples within each. We talked about both commercial and free solutions, which are FortiNAC, Juniper Unified Access Control (UAC), Cisco Identity Services Engine (ISE), PacketFence, FreeNac and OpenNAC.

We carried out a comparison study between open-source and commercial NAC solutions, revealing details about their features, to assist in decision-making. After eliminating some options, we ended up deciding on the Access Control system that best met our needs.

The FreeRADIUS protocol, the Snort intrusion prevention system, Nessus, and OpenVAS (Open Vulnerability Assessment System) were also examined as important Network Access Control tools, as were other PacketFence components.

We have acquired a thorough understanding of the subject by carefully examining the most important components of computer security, NAC solutions, and some pertinent tools. When deciding how to implement secure Access Controls in our network infrastructure, we can use this knowledge to make well-informed choices.

The implementation process will be covered in more detail in the following chapter, along with instructions on how to successfully deploy and set up the NAC solution we have selected.

CHAPTER II: Design and Implementation of the NAC Solution

1. Introduction

After completing the theoretical concepts, we move on to the implementation of our solution, which represents our main task. In this chapter, we will start by specifying the needs and focus on the practical part. The realization of a solution that ensures Access Control of hosts connected to the network.

2. Specification of requirements

This phase represents the "functional" and "non-functional" aspects of the solution.

2.1. Functional requirements

- **Authentication management :** Using Radius authentication server to reinforce user authentication management.
- **Access management:** Controlling access by assigning VLANs dynamically based on role.
- **Supervision :**
  - Viewing the history of Network Access.
  - Checking blocked machines and view the various access phases for any given machine.
- **Administration :**
  - Adjusting the system's configuration by adding new services or protocols.
  - Adding accounts for users.

2.2. Non-functional requirements

- **Flexibility :** You can integrate PacketFence into your environment without having to make any significant changes because it can authenticate your users using a variety of protocols and standards.
- **Virtualization :** ProxMox Virtual Environment will be used to implement our solution in virtual mode.

3. Deployment steps

Here (**Figure II-1**) are the major steps of our solution's deployment and we'll go over each stage individually.

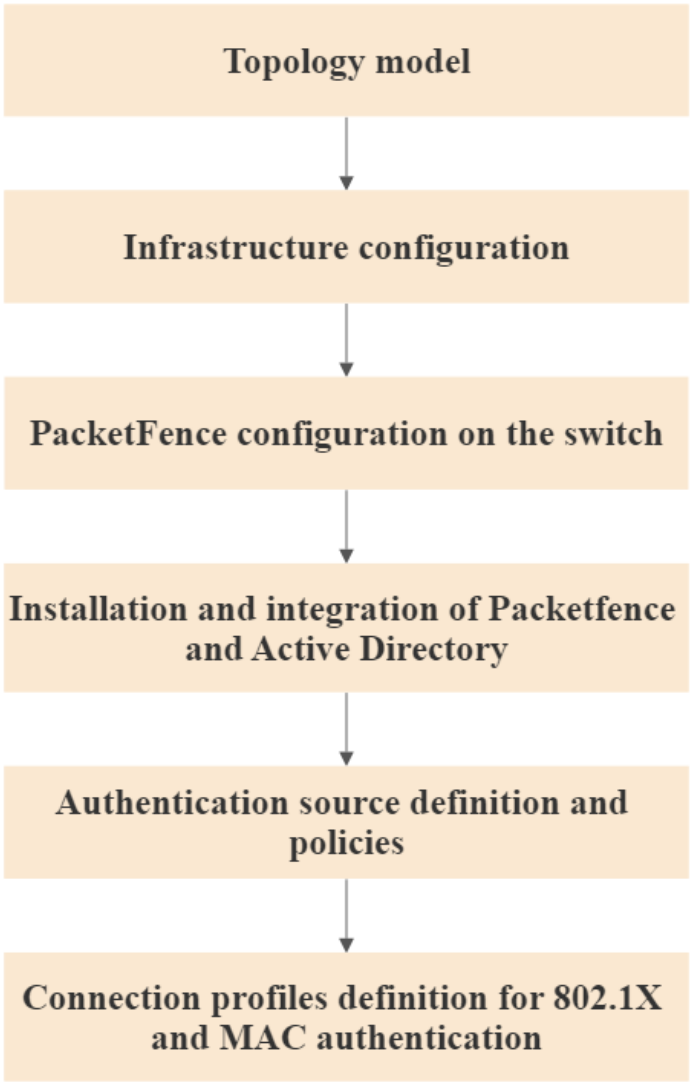

Figure II-1: *Deployment flowchart*

4. Topology model

Our solution is to implement PacketFence on our new server that uses ProxMox as a Virtual Machines Manager which will be related to a Huawei S5735 switch and will control every new attempt to access the network through Ethernet knowing that Sonatrach already has Wireless Network Access Control through a portal. Our managing computer will be connected to the PacketFence Virtual Machine and many other machines through the switch so that we can be able to impose the NAC security solution to every one of them.

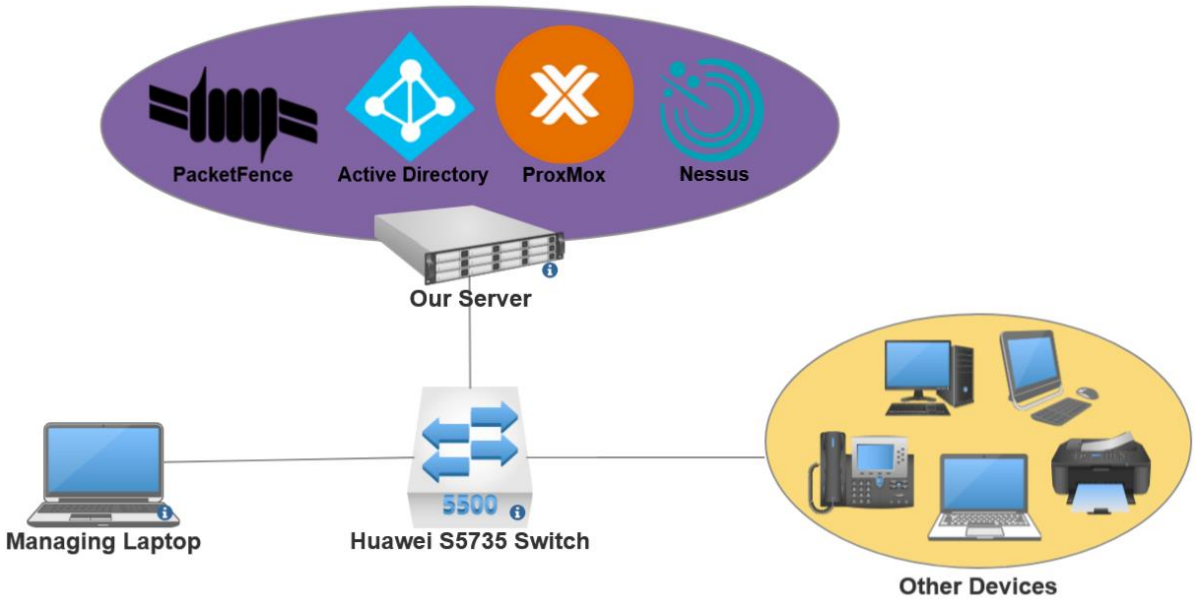

***Figure II-2**: Implementation network architecture*

First of all, in order to implement our solution, we need to create our test environment (**Figure II-2**). We will have to bring:

- Multiple machines (Server with VDIs, Laptops, IP Phones, Printers… etc).
- A switch to link the machines (Huawei S5735).
- PacketFence on our server (With FreeRADIUS).
- An SSH client on our managing computer (PuTTy).
- DHCP server (On the Switch).
- Microsoft Active Directory Server (Also DNS Server).

4.1. Information about our network

- ➢ Switch IP Address : 192.168.10.2
- ➢ DHCP Server : 192.168.10.2
- ➢ Active Directory Server : 192.168.10.136
- ➢ DNS Server : 192.168.10.136
- ➢ PacketFence Server : 192.168.10.183
- ➢ RADIUS Server : 192.168.10.183

5. Implementation of the solution

5.1. Infrastructure configuration

5.1.1. Initial switch settings

First of all, we will have to configure our switch so that it can manage our network easily. The first thing we did is to be connected to it through its console port and use the PuTTy terminal emulation software to log in. The first thing that is asked is to enter the default username and password for the switch, we enter *admin* as a username and *admin@huawei.com* as a password. Then, we are asked to set our own username and password. So, we did, then confirmed by clicking on "y". That's it, now we will be able to access the switch with our new username and password. Just after doing that, we will be able to give a new name to our switch. We used the following commands (**Figure II-3**) :

```
<Huawei> system-view
[Huawei] sysname switchnac
[switchnac] quit
<switchnac> save
```

Figure II-3: *Renaming the Switch*

5.1.2. Interfaces and VLANs configuration

After going through the basic configuration, we will now have to create our VLANs, their related interfaces and a Trunk interface that can go through all of them and which will be assigned to our PacketFence Server so that we can manage everything through it.

First of all, let's create our main VLANs. We will need to create two of them, number 10 for the management that will be assigned as a default one for the trunk port and number 20 for the data that will be assigned to the GE0/0/5 interface, as the following figure shows it (**Figure II-4**) :

```
<switchnac>system-view
[switchnac]vlan batch 10 20
[switchnac]interface GigabitEthernet0/0/1
[switchnac-GigabitEthernet0/0/1]port link-type trunk
[switchnac-GigabitEthernet0/0/1]port trunk pvid vlan 10
[switchnac-GigabitEthernet0/0/1]quit
[switchnac]interface GigabitEthernet0/0/5
[switchnac-GigabitEthernet0/0/5]port link-type access
[switchnac-GigabitEthernet0/0/5]port default vlan 20
[switchnac-GigabitEthernet0/0/5]quit
```

Figure II-4: *Configuring the VLANs*

5.1.3. DHCP and SSH configuration

We have our VLANs configured. But now, we will need to assign IP addresses to our interfaces according to the VLAN they are in. So, we will need to configure the DHCP protocol so that it can dynamically assign IP addresses to every interface (**Figure II-5**).

To do so, we will choose a segment of IP addresses for every VLAN (for example 192.168.10.0 /24 for the management VLAN, 192.168.20.0 /24 for the data VLAN…)

```
[switchnac]dhcp enable
[switchnac]interface vlanif 10
[switchnac-Vlanif10]ip address 192.168.10.2 24
[switchnac]interface vlanif 20
[switchnac-Vlanif20]ip address 192.168.20.1 24
[switchnac]ip pool 10
[switchnac-ip-pool-10]gateway-list 192.168.10.2
[switchnac-ip-pool-10]network 192.168.10.0 mask 24
[switchnac-ip-pool-10]lease day 200
[switchnac-ip-pool-10]quit
[switchnac]ip pool 20
[switchnac-ip-pool-20]gateway-list 192.168.20.1
[switchnac-ip-pool-20]network 192.168.20.0 mask 24
[switchnac-ip-pool-20]lease day 200
[switchnac-ip-pool-20]quit
[switchnac]interface vlanif 10
[switchnac-Vlanif10]dhcp select global
[switchnac]interface vlanif 20
[switchnac-Vlanif20]dhcp select global
```

Figure II-5: *Assigning IP addresses to the VLANs*

To test if it works, we will need to try pinging from one device to another (**Figure II-6**).

```
C:\Users\tassili>ping 192.168.10.183

Pinging 192.168.10.183 with 32 bytes of data:
Reply from 192.168.10.183: bytes=32 time<1ms TTL=64
Reply from 192.168.10.183: bytes=32 time<1ms TTL=64
Reply from 192.168.10.183: bytes=32 time<1ms TTL=64
Reply from 192.168.10.183: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.10.183:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\tassili>
```

Figure II-6: *Testing ping*

Now, we will need to get rid of the console cable and find a way to communicate remotely with our switch through a simple Ethernet cable. There are multiple ways like Telnet but we choose SSH because it is the most secure way to access the switch.

The figure below shows the configuration for SSH login (**Figure II-7**):

```
<switchnac> system-view
[switchnac] user-interface maximum-vty 5
[switchnac] user-interface vty 0 4
[switchnac-hi-vty0-4] idle-timeout 0
[switchnac-ui-vty0-4] authentication-mode aaa
[switchnac-ui-vty0-4] protocol inbound all
[switchnac-ui-vty0-4] commit
[switchnac-ui-vty0-4] quit
[switchnac] interface GigabitEthernet0/0/1
[switchnac-GigabitEthernet0/0/1] ip address 192.168.10.2 24
[switchnac-GigabitEthernet0/0/1] commit
[switchnac-GigabitEthernet0/0/1] quit

[switchnac] aaa
[switchnac-aaa] local
[switchnac-aaa] undo local-user policy security-enhance
[switchnac-aaa] commit
[switchnac-aaa] local-user admin password irreversible-cipher S0natrach123
[switchnac-aaa] local-user admin service-type telnet ssh
[switchnac-aaa] local-user admin level 3
[switchnac-aaa] local-user admin user-group manage-ug
[switchnac-aaa] commit
[switchnac-aaa] quit

[switchnac] ssh user admin
[switchnac] ssh user admin authentication-type password
[switchnac] ssh user admin service-type all
[switchnac] ssh authorization-type default aaa
[switchnac] commit
[switchnac] stelnet server enable
[switchnac] snetconf server enbale
[switchnac] commit
[switchnac] quit
<switchnac> save
```

Figure II-7: *Configuring SSH*

Now that SSH is configured, a user should be created for it (**Figure II-8**):

```
<switchnac> system-view
[switchnac] ssh user admin
[switchnac] ssh user admin authentication-type password
[switchnac] local-user admin service-type ssh
[switchnac] local-user admin privilege level 15
[switchnac] quit
<switchnac> save
```

Figure II-8: *Configuring SSH user*

Now, we can use SSH to access our switch remotely using an Ethernet Cable and a terminal emulator software (PuTTy in our case) (**Figure II-9**).

```
192.168.10.2 - PuTTY
login as: admin
Keyboard-interactive authentication prompts from server:
| User Authentication
| Password:
End of keyboard-interactive prompts from server

Info: The max number of VTY users is 10, and the number
      of current VTY users on line is 1.
      The current login time is 2023-04-12 02:32:20+00:00.
Info: Lastest accessed IP: 192.168.10.16  Time: 2023-04-12 01:41:32  Failed: 0

Info: Smart-upgrade is currently disabled. Enable Smart-upgrade to get recommended version information.
<switchnac>
```

Figure II-9: *Testing SSH through PuTTy*

5.2. PacketFence configuration on the switch

5.2.1. RADIUS server configuration

In order for the switch to communicate with PacketFence as a RADIUS source server, it must be assigned the PF address with a key. This last one is mentioned when adding the switch to the list of network devices at the PacketFence level.

The provided commands configure RADIUS-based authentication, authorization, and accounting on the switch (**Figure II-10**). Initially, the "undo authentication unified-mode" command disables the unified authentication mode. Subsequently, a RADIUS server template named "PacketFence" is created with a shared key defined as "s0natrach123". The IP address and port numbers of the RADIUS server are specified for authentication and accounting purposes. Additionally, the "radius-server retransmit" command sets the number of retransmission attempts for RADIUS messages. The "radius-server authorization" command configures the RADIUS server for authorization.

```
<switchnac>system-view
Enter system view, return user view with Ctrl+Z.
[switchnac]radius-server template packetfence
[switchnac-radius-packetfence]radius-server shared-key cipher s0natrach123
[switchnac-radius-packetfence]radius-server authentication 192.168.10.183 1812
[switchnac-radius-packetfence]radius-server accounting 192.168.10.183 1813
[switchnac-radius-packetfence]radius-server retransmit 2
[switchnac-radius-packetfence]radius-server authorization 192.168.10.183 shared-key cipher s0natrach123
[switchnac]
```

Figure II-10: *Enabling radius server at the switch level*

5.2.2. Activation of AAA and dot1x functions

The commands provided configure the switch's authentication and accounting settings (**Figure II-11**). The commands "authentication-scheme" and "accounting-scheme" define the "pf-auth" and "pf-acct" schemes to be used for authentication and accounting, respectively. RADIUS should be used for authentication and accounting, based on the "authentication-mode" and "accounting-mode" commands.

The "domain" commands create the "PF" domain and relate it to the earlier mentioned accounting, and authentication schemes. The RADIUS server to be used, "PacketFence" is specified by the "radius-server" command.

Finally, the "mac-authen" command enables MAC authentication while the "dot1x enable" command activates 802.1X authentication.

```
[switchnac]aaa
[switchnac-aaa]authentication-scheme pf-auth
[switchnac-aaa-authen-pf-auth]authentication-mode radius
[switchnac-aaa-authen-pf-auth]accounting-scheme pf-acct
[switchnac-aaa-accounting-pf-acct]accounting-mode radius
[switchnac-aaa-accounting-pf-acct]
[switchnac-aaa-accounting-pf-acct]domain pf
Info: The domain pf is for common users. The domain default_admin is for administrators. To modify the para
[switchnac-aaa-domain-pf]authentication-scheme pf-auth
[switchnac-aaa-domain-pf]accounting-scheme pf-acct
[switchnac-aaa-domain-pf]service-scheme pf-cli
[switchnac-aaa-domain-pf]radius-server packetfence
[switchnac-aaa-domain-pf]quit
[switchnac-aaa]quit
[switchnac]
[switchnac]domain pf
Info: Set the default domain success.
[switchnac]dot1x enable
Info: Disable the dot1x handshake function if the Windows operation system is used.
[switchnac]mac-authen
[switchnac]dot1x timer reauthenticate-period 10800
[switchnac]mac-authen timer reauthenticate-period 10800
[switchnac]dot1x dhcp-trigger
[switchnac]
```

Figure II-11: *Enabling AAA and 802.1X at the switch level*

5.2.3. SNMP configuration

The Simple Network Management Protocol settings on the switch are configured using the SNMP commands provided (**Figure II-12**). SNMP is a widespread network management protocol that makes it easier to manage and monitor network devices, using a set of commands and messages sent back and forth between SNMP managers (network management systems) and SNMP agents (network devices). These commands and messages make it possible to find and change device information and configuration settings.

The commands create a local engine ID, which is represented by the value '800007DB0304F9389D2360'. It distinguishes the switch's SNMP agent from other network devices. Configure community strings for read and write access, and set up the SNMP agent. The community strings are secured by encryption. Additionally, the commands state that SNMP version 2c should be used for this protocol's system information version. Overall, these commands enable the switch's SNMP functionality and create a secure connection for network device monitoring and management.

```
[switchnac]snmp-agent
[switchnac]snmp-agent local-engineid 800007DB0304F9389D2360
Warning: All SNMP users will be reset. Continue? [Y/N]:y
[switchnac]snmp-agent community read cipher s0natrach123
[switchnac]snmp-agent community write cipher s0natrach123
[switchnac]snmp-agent sys-info version v2c
Warning: SNMPv1/SNMPv2c is not secure, and it is recommended to use SNMPv3.
[switchnac]
```

Figure II-12: *Configuring SNMP*

5.2.4. ACL configuration

An important setting for the NAC is to create an Access-Control List that filters network traffic to restrict access to a network resource. In our case, the acl's goal is to block any IP traffic from the data VLAN (20) to access the management VLAN (10). And of course, any device out of the known network cannot send IP traffic to either VLANs.

An ACL with the switch's ID 3000 is configured using the commands given. The destination IP range 192.168.10.0/24 is not allowed to receive IP traffic from the source IP range 192.168.20.0/24, according to Rule 5. Regardless of the source IP or the destination IP, IP traffic is allowed under Rule 10. On interface GigabitEthernet0/0/22, the ACL is subsequently used as an outgoing traffic filter (**Figure II-13**).

```
[switchnac]acl number 3000
[switchnac-acl-adv-3000]rule 5 deny ip source 192.168.20.0 0.0.0.255 destination 192.168.10.0 0.0.0.255
[switchnac-acl-adv-3000]rule 10 permit ip source any destination any
[switchnac-acl-adv-3000]quit
[switchnac]interface gigabitEthernet0/0/22
[switchnac-gigabitEthernet0/0/22]taffic-filter outbound acl 3000
[switchnac-gigabitEthernet0/0/22]quit
[switchnac]
```

Figure II-13: *Configuring the ACL*

5.2.5. Configuring the switch ports for 802.1X, MAB and VoIP

To configure the switch port, we first enable the switch ports for hybrid mode, then enable 802.1X and MAB authentication in the interface range [7-46] and the 47th and 48th ports will be configured as VoIP ports.

The endpoint requester must send a periodic EAP over LAN (EAPoL-Start) message in the switchport to speed up the authentication. If a device cannot authenticate using the 802.1X protocol due to the nature and waiting time assigned to the 802.1X protocol, it can try to authenticate using the MAB protocol. If its MAC address is in the PacketFence internal database, it is then allowed to access the network (**Figure II-14**).

```
#
interface GigabitEthernet0/0/46
 port link-type hybrid
 dot1x mac-bypass
 dot1x max-user 1
 dot1x reauthenticate
 dot1x authentication-method eap
#
interface GigabitEthernet0/0/47
 port link-type hybrid
 voice-vlan 100 enable
 port hybrid tagged vlan 100
 mac-authen
#
```

Figure II-14: *Configuring MAC Authentication, 802.1X and Voice Port*

5.3. Installation and integration of PacketFence and Active Directory

The most interesting thing about our project is that it is based on open-source software. An open-source software works basically with every hardware and every operating system. PacketFence can be installed on different Operating Systems like Windows or some Linux distributions. For our case, we have chosen to install its OVF image based on the Debian distribution directly on our server so that we don’t need any OS to launch it and to optimize its performance. To install it, we used the PacketFence Installation Guide and followed every step.

❖ **Minimum Hardware Requirements**

- Intel or AMD CPU 3 GHz, 4 CPU Cores
- 16 GB of RAM
- 200 GB of disk space (RAID-1 recommended)
- 1 network card (2 recommended)

5.3.1. PacketFence Initial Setup

Once the system has been started and the server is linked to the switch through the trunk port, we will use a laptop to access the server through its IP address and enter the PacketFence configuration, where we will specify the mode of operation, network interfaces, administration passwords, and services to run. MariaDB, httpd (Apache Services) and FreeRADIUS are installed by default from the repository.

PacketFence includes a web-based interface that enables step-by-step the settings of NAC. The configuration procedure is composed of several steps.

- **Step 1 : Choosing the enforcement mechanism**

In this step, we are asked to select an enforcement mechanism (**Figure II-15**), we can choose either the Inline mode (all the traffic needs to pass through PacketFence), the VLAN mode (PacketFence is Out-of-Band) or both.

In our case, we will use the VLAN enforcement mode since it is the preferred way of deploying PacketFence and since we will only apply the solution to devices manageable with 802.1X and MAB support (Mac-authentication Bypass).

The decision taken at this phase will have an impact on the following steps, where we will set up the various networks.

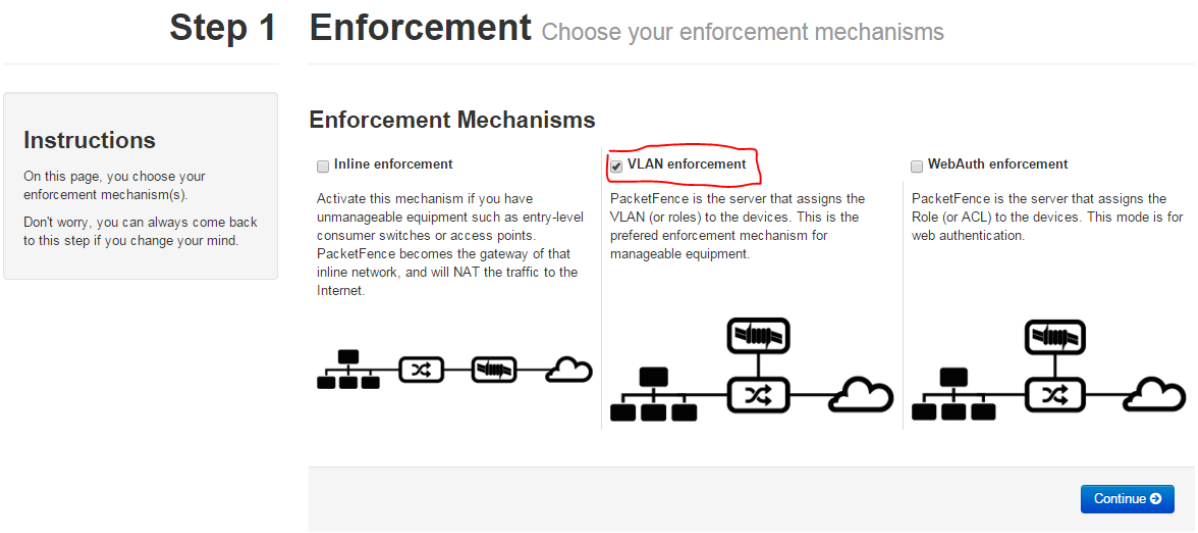

Figure II-15: *Choosing the enforcement mechanism*

- **Step 2 : Interfaces configurations**

Specification of the network addresses and system interfaces where the DHCP server will provide its service for the devices that are trying to access the network. We'll apply the configuration that is specified in the figure below (**Figure II-16**).

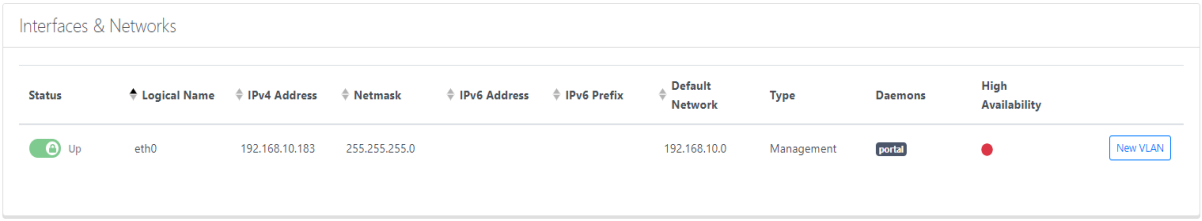

Figure II-16: *Configuring Ethernet interfaces*

- **Step 3 : Configuring the Database-server (On PacketFence)**

To enable PacketFence and establish connections, we will define the scheme for the database and a user. Additionally to a domain and Hostname which will identify the server, and create the administrative user to access the PacketFence Administration Web Interface (**Figure II-17**).

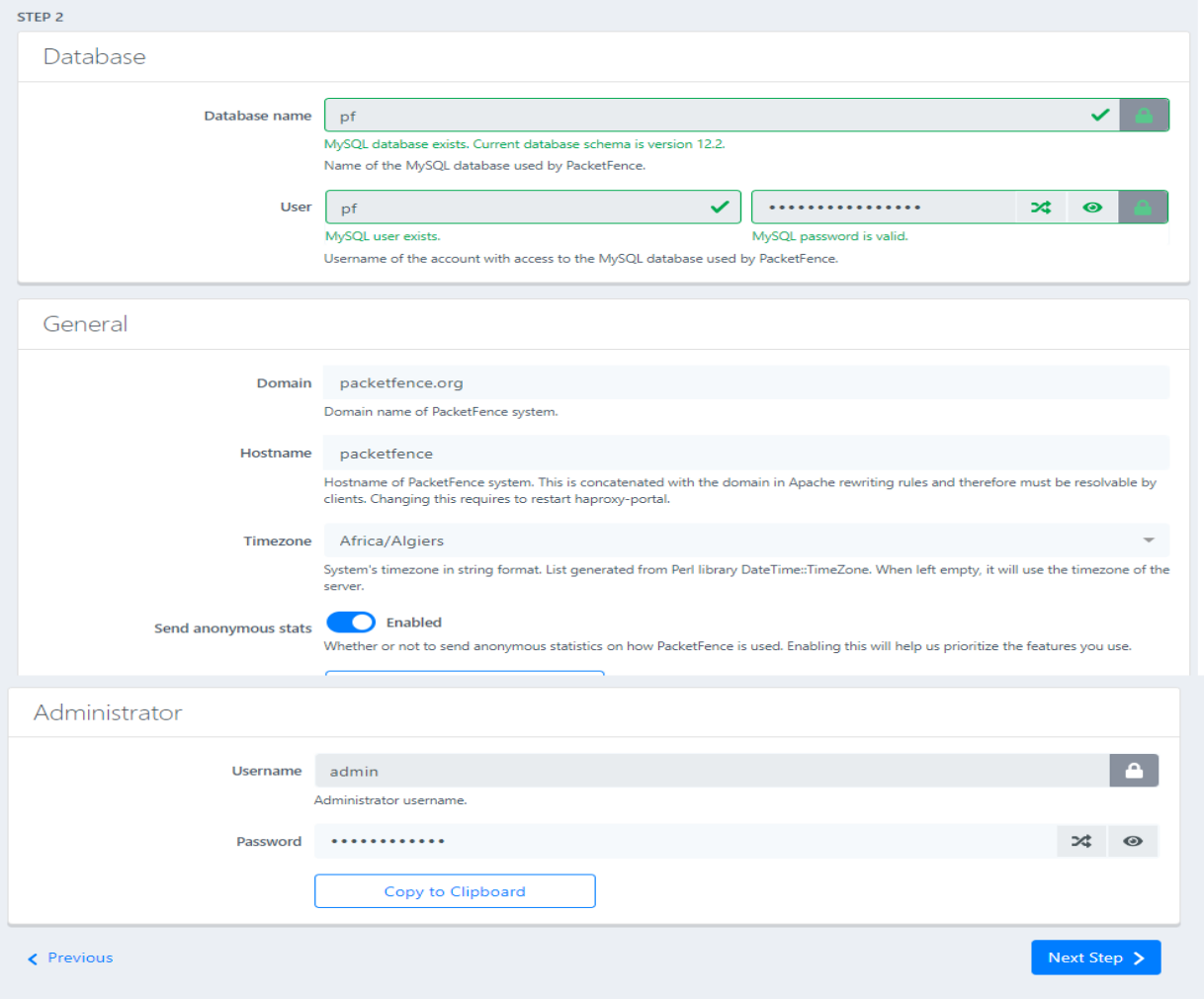

Figure II-17: *Configuring the Database and administrator of the database*

- **Step 4 : NAC Configuration**

In this last step, all services will begin, and we will gain access to the management interface through *https://192.168.10.183:1443*.

5.3.2. Installation of the domain controller (Active Directory)

Active Directory is a Microsoft server service for storing, managing and securing user accounts. The main objective of Active Directory is to provide centralized identification and authentication services to a network of computers using the windows system. To install AD we will used Windows server 2012 in a Virtual Machine, after adding the role Active Directory-Directory services (AD DS).

Our Active Directory server configuration is shown in the following table:

Table II-1: *AD server configuration*

Server name	DC
IP address	**192.168.10.136**
Network mask	**255.255.255.0**
Domain name	**ad.lab**

The next step in getting ready for using AD to authenticate with PacketFence is to create an organizational unit (OU) called "Groups" in Active Directory, which is used for storing LDAP objects (users, groups, computers, printers, and other OUs) to be used for employee, guest, and intern authentication. After that, we added the users (**Figure II-18**).

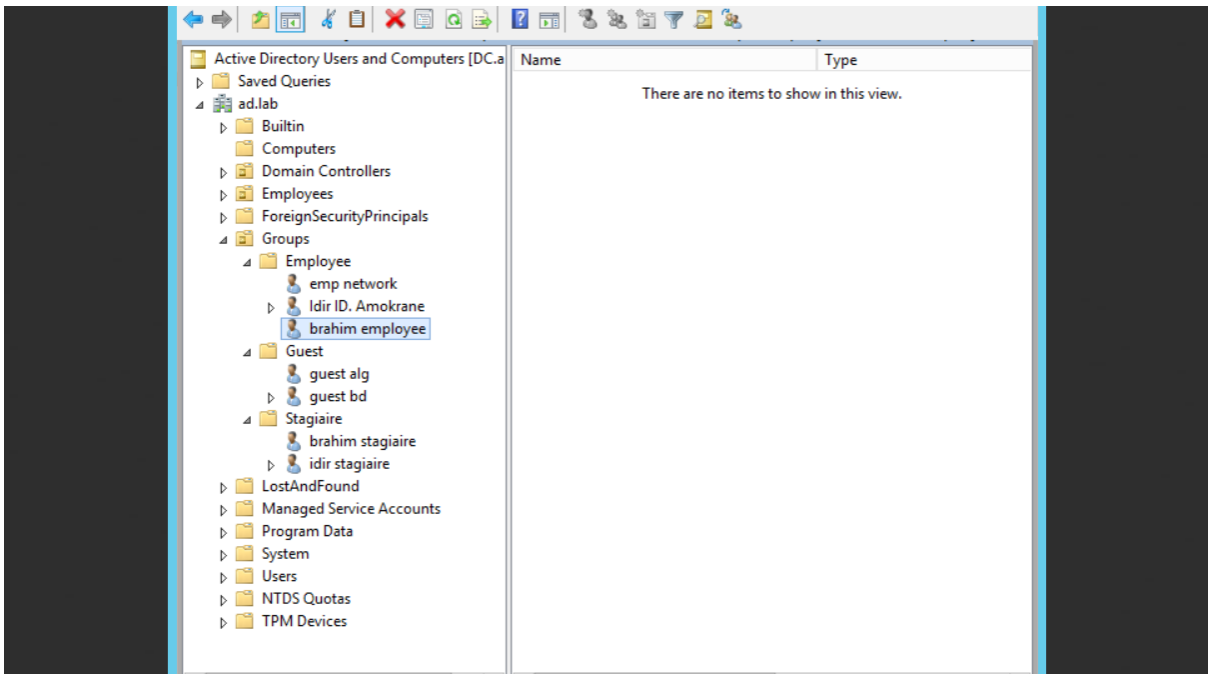

Figure II-18: *Creation of an Organizational unit "Groups"*

5.3.3. PacketFence and AD integration

Before we can use Active Directory to control authentication to PacketFence for users, we need to join PacketFence to the domain. To do this, it is necessary to :

➢ Add AD Domain name and AD server host to PacketFence (**Figure II-19**).

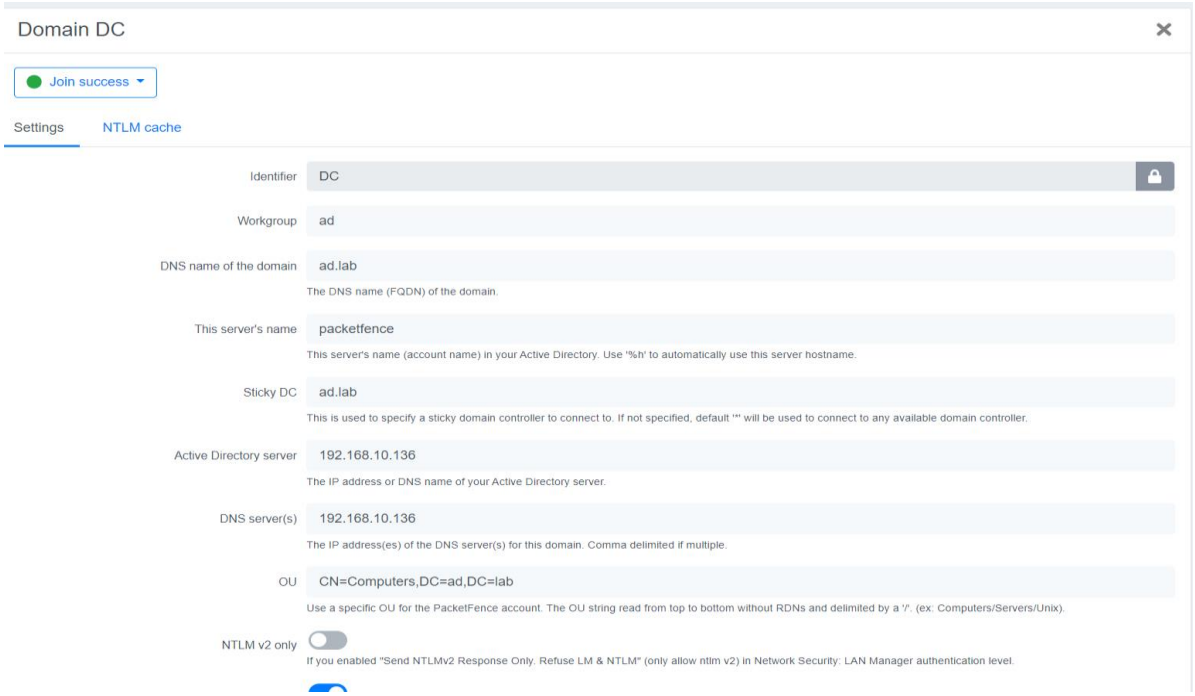

Figure II-19: *Joining PacketFence to AD domain*

➢ Add a domain administrator account to PacketFence. Once it has joined AD, we get the following result (**Figure II-20**):

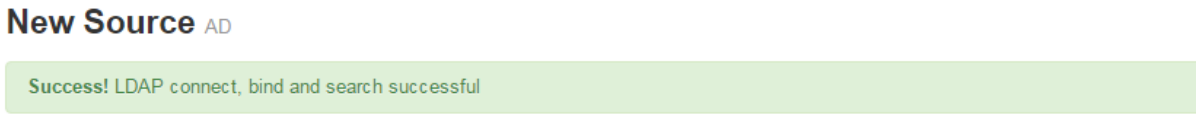

Figure II-20: *Result of Joining PacketFence to Active Directory*

The last step is to add our created domain to "REALMS" where you define how PacketFence should direct authentication depending on the username (**Figure II-21**).

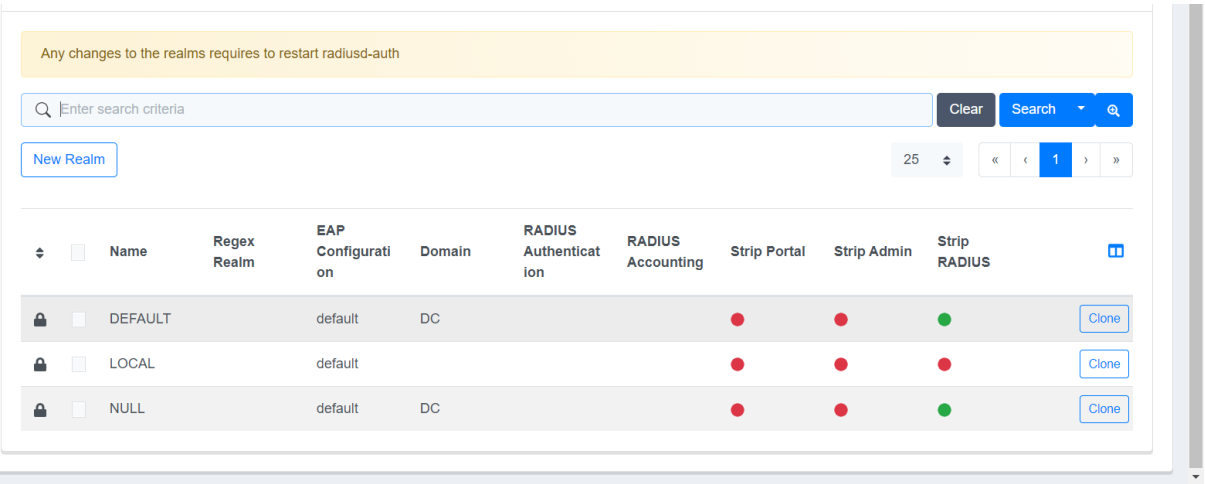

Figure II-21: *Adding created domain to Realms*

5.3.4. Configuring network devices

All the information related to network devices is stored in */usr/local/pf/conf/switches.conf*.

The network device is going to be configured to work together with PacketFence. Within the configuration menu, we can locate the Network Devices subgroup, Switches option (***Configuration > Switches > NEW SWITCH > default***): We proceed to enter the configuration required for the equipment (switch) that will enter in production.

➢ Add switch with it's IP address: 192.168.10.2 (**Figure II-22)**.

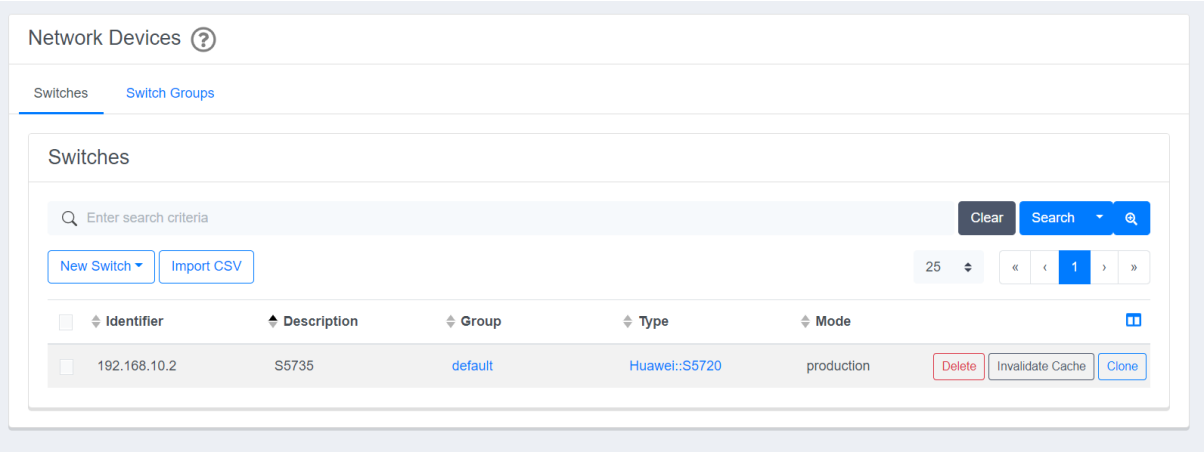

Figure II-22: *Adding Huawei S5735 switch to network devices*

➢ Choose type as Huawei S5720(S5735) and mode as production (**Figure II-23**).

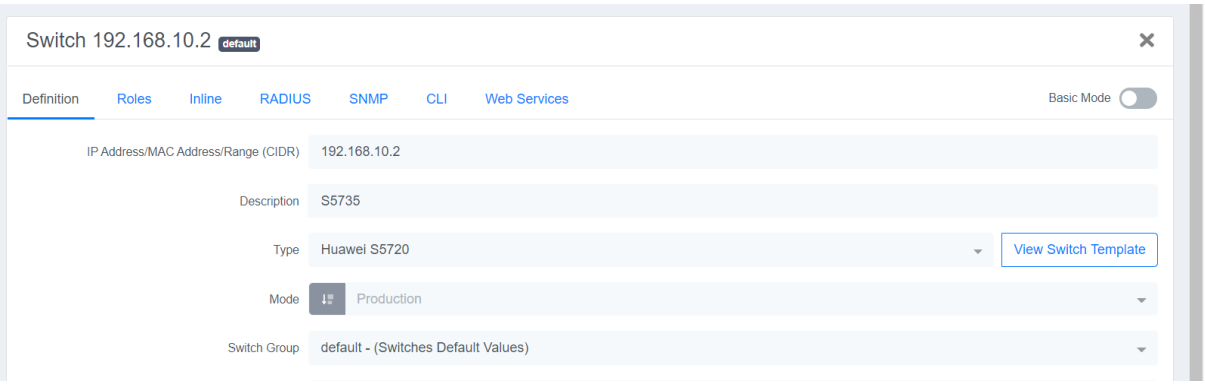

Figure II-23: *Switch Definition*

➢ In the Roles tab (**Figure II-24**), define the roles and the corresponding VLANs. For example, the unregistered device must not belong to any specific VLAN (2 by default) but the registered ones with the correct user credentials will be switched to data VLAN 20 (employee, stagiaire and guest should all be in the data VLAN).

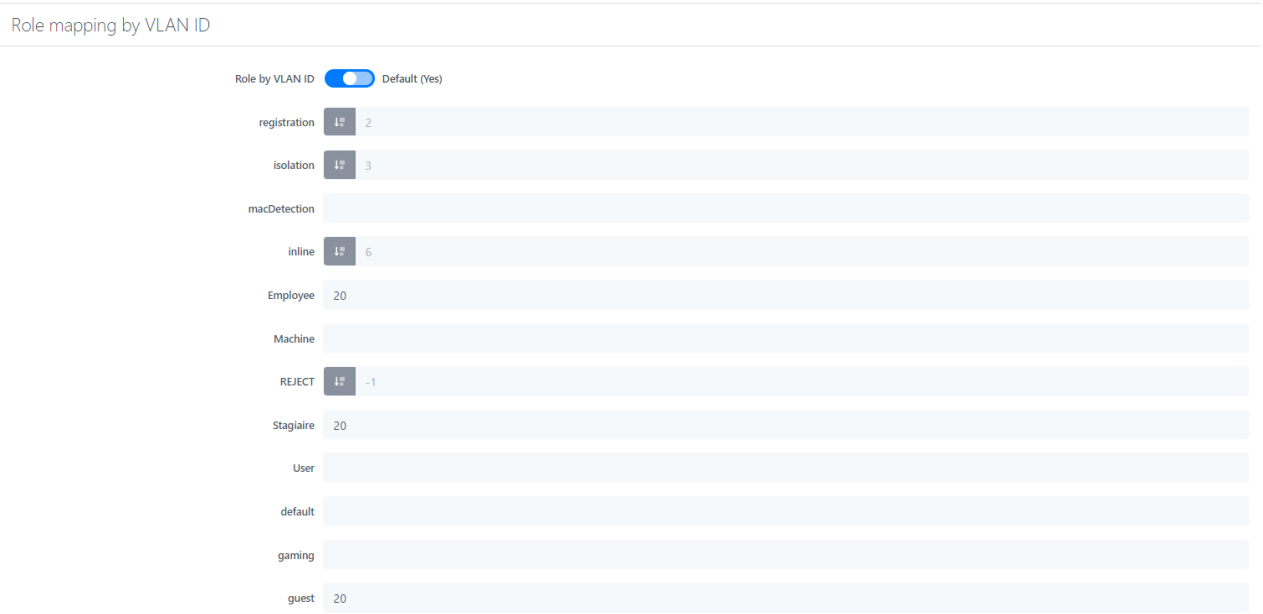

Figure II-24: *Vlans necessary for the operation*

➢ In the RADIUS tab (**Figure II-25**), Enter the same secret key as shared-key on the switch when configuring the 802.1X protocol on the S5735 switch and the “use CoA box” should be checked with the “CoA port” “3799”.

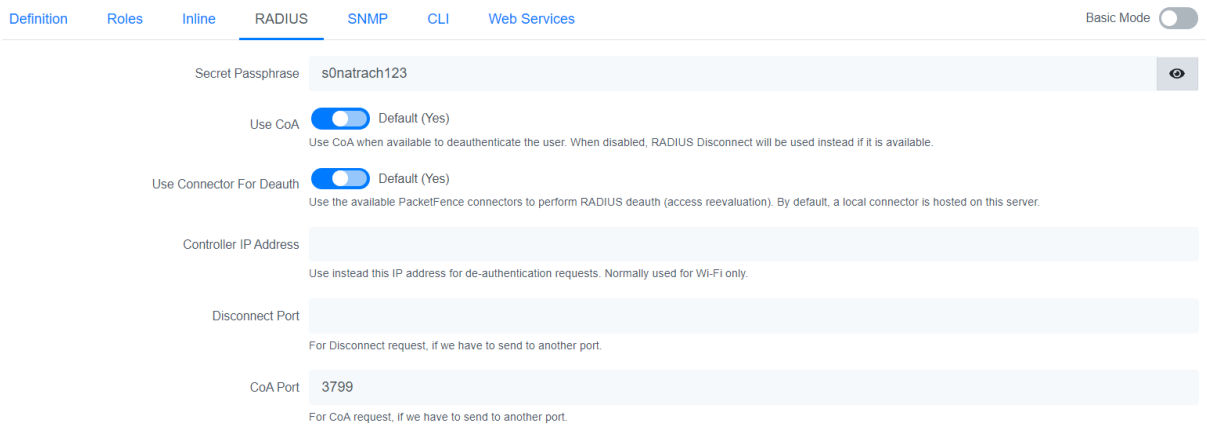

Figure II-25: *Radius passphrase configuration*

➢ At the end, provide the same community write and read configured on the switch in the SNMP tab (**Figure II-26**).

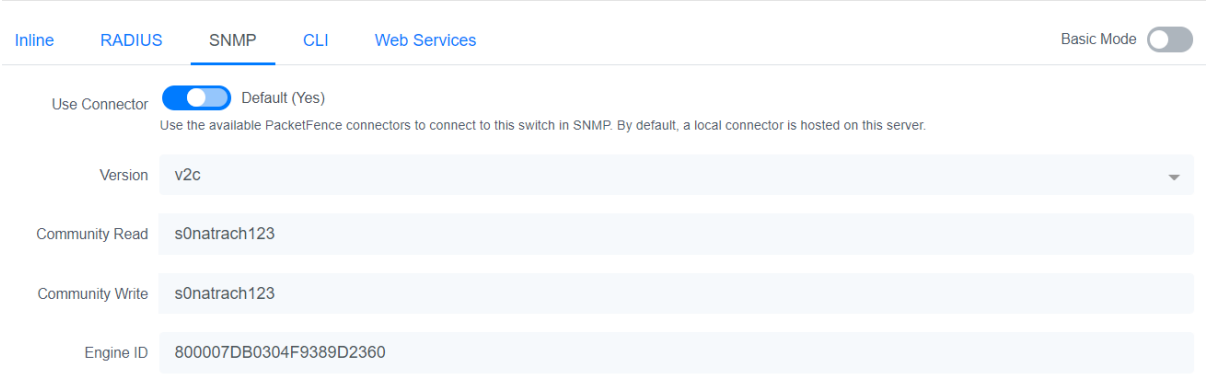

Figure II-26: *SNMP communication configuration*

5.4. Authentication source definition and policies

In this part, we add the Microsoft Active Directory domain controller to PacketFence as an authentication provider (**Figure II-27**). To do this, we must create a new internal source AD, and specify the appropriate Network Access rules under (***Configuration → Policies and Access Control → Authentication Sources***) and all the required fields:

➢ **Name:** DC (The same as our AD server name)

➢ **Description:** DC rules

➢ **Host:** 192.168.10.136 (the IP address of the AD domain) / 389 is the default port that AD and LDAP use

➢ **Base DN:** DC=ad, DC=lab (the full path to our users accounts. In our case, we specified the highest branches of the tree)

➢ **Scope:** Subtree

➢ **Username attribute:** sAMAccountName (The name of the field that PacketFence will use to authenticate users.).

- **Bind DN:** CN=Administrator, CN=Users, DC=ad, DC=lab (The full AD path of a user with domain admin rights)
- **Password:** Sdfg1234+ (The password for the account that we used with Bind DN)

Below is a sample of the configuration screens:

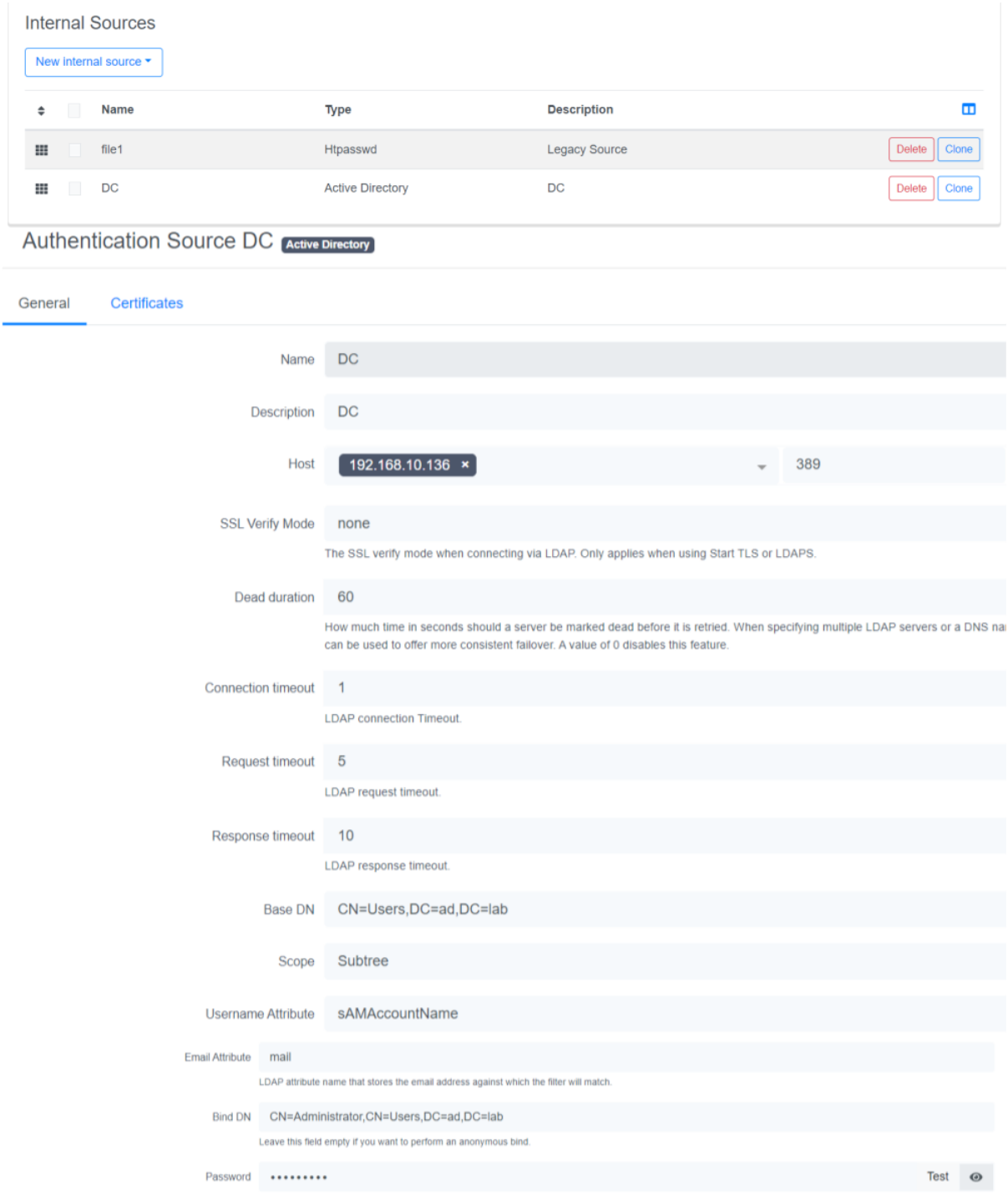

Figure II-27: *The new internal authentication source*

After we filled the fields with the required information, we should now add rules to grant users by assigning roles for each type of users and access duration to the network.

We created 3 rules (**Figure II-28**), (**Figure II-29**), (**Figure II-30**). They are expressed as If condition X, then Y. Where there are multiple possible X conditions and Y actions. For authentication rules, actions *must* set a role, an access duration (in hours), or an expiration date (a future date).

We may need to carefully consider the sequence because we may obviously set many rules and they are evaluated in order, from top to bottom (just like with firewalls!).

- **Employees rule:**

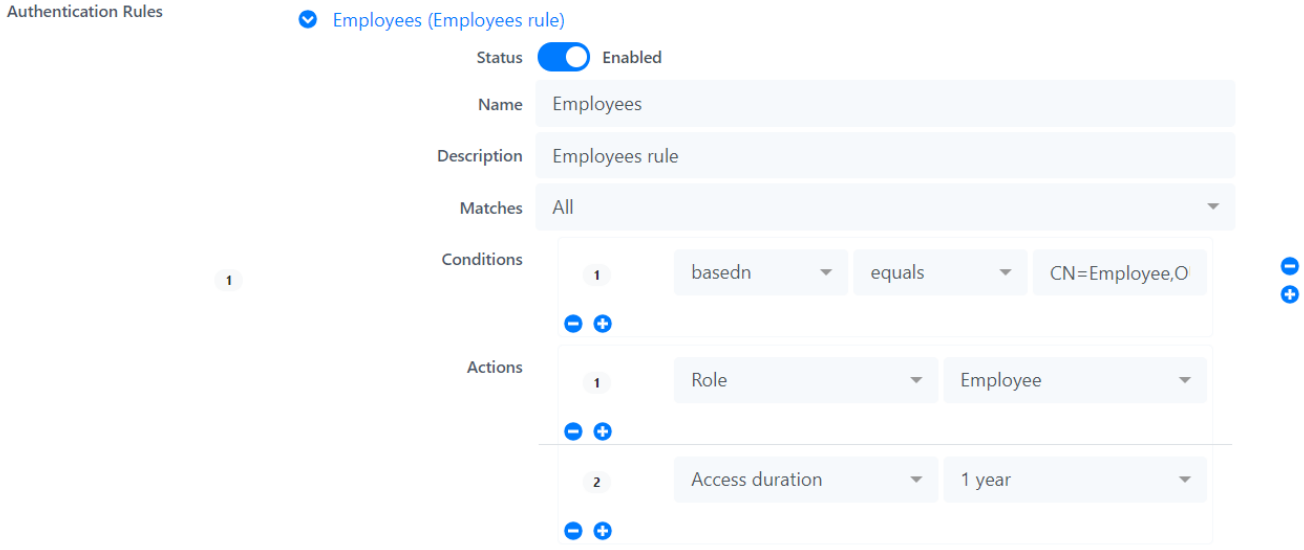

Figure II-28: *Employees authentication rule*

➢ For this rule, we specified as a condition that the user must belong to "CN=Employee,OU=Groups,DC=ad,DC=lab" who was created in section **5.3.2**.

➢ Based on that, it then applies the user role of Employee and sets access duration to 1 year.

- **Interns rule:**

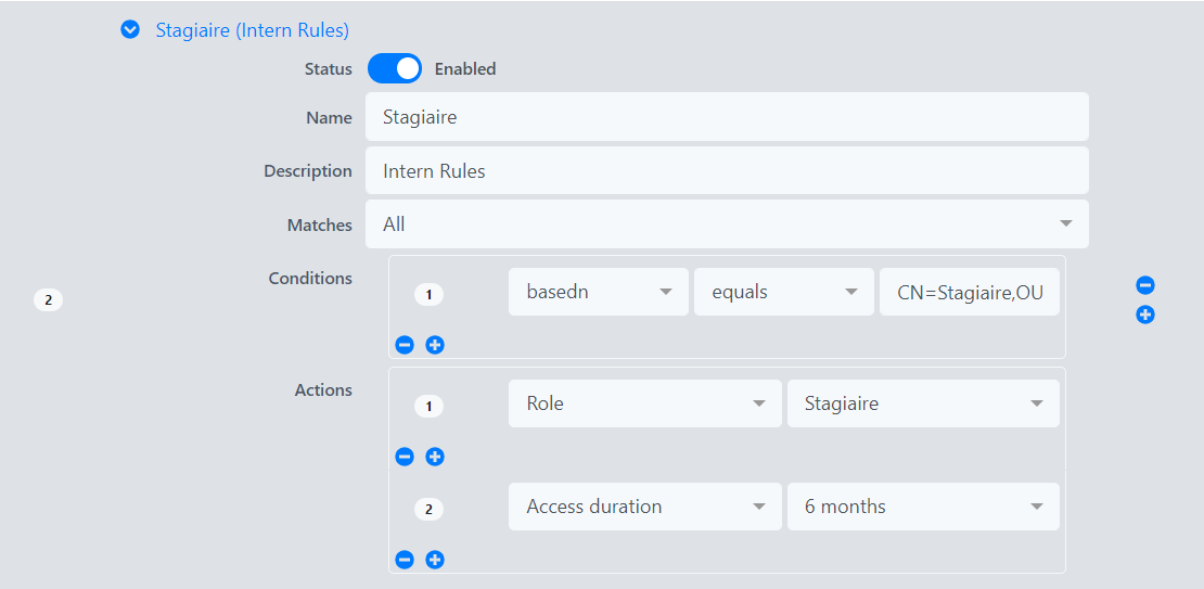

Figure II-29: *Interns authentication rule*

- ➢ For this rule, we specified as a condition that the user must belong to "CN=Stagiaire,OU=Groups,DC=ad,DC=lab".
- ➢ Based on that, it then applies the user role of Stagiaire and sets access duration to 6 months.

- **Guests rule:**

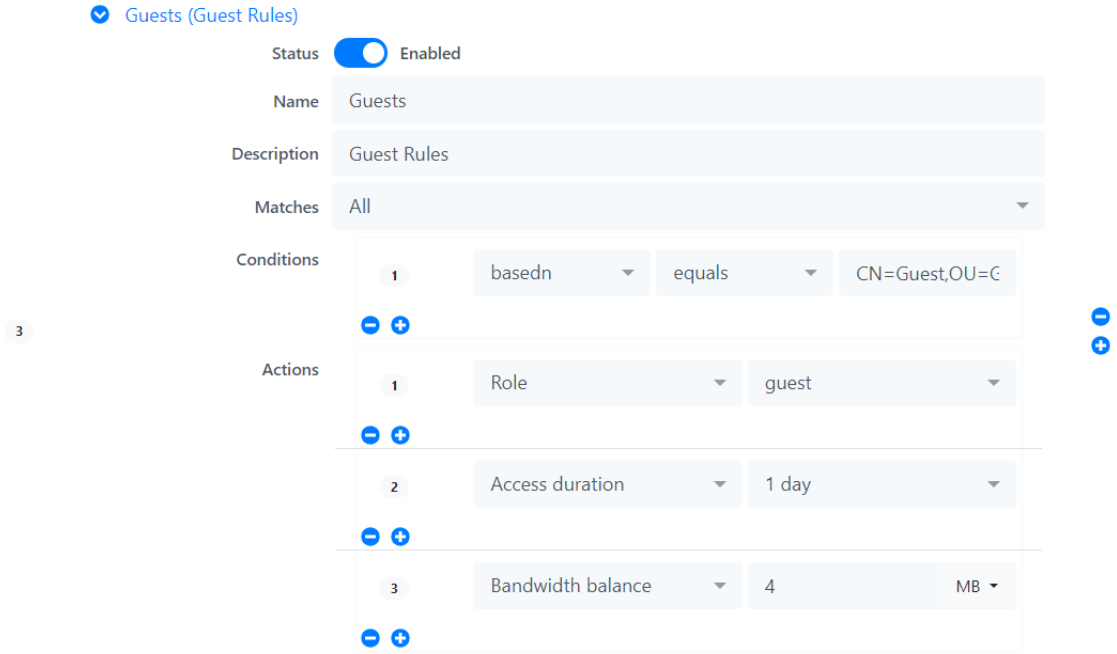

Figure II-30: *Guests authentication rule*

- ➢ For this rule, we specified as a condition that the user must belong to "CN=Guest,OU=Groups,DC=ad,DC=lab".
- ➢ Based on that, it then applies the user role of Guest and sets access duration to 1 day and the bandwidth balance to 4MB.

To evaluate the created rules, we run the ***./pftest authentication*** script in a shell (**Figure II-31**), as we make changes with test user cases.

```
root@packetfence:/bin# pftest authentication stagiairealg Sdfg1234+ DC
Testing authentication for "stagiairealg"

Authenticating against 'DC' in context 'admin'
  Authentication SUCCEEDED against DC (Authentication successful.)
  Matched against DC for 'authentication' rule Stagiaire
    set_role : Stagiaire
    set_access_duration : 1h
  Did not match against DC for 'administration' rules

Authenticating against 'DC' in context 'portal'
  Authentication SUCCEEDED against DC (Authentication successful.)
  Matched against DC for 'authentication' rule Stagiaire
    set_role : Stagiaire
    set_access_duration : 1h
  Did not match against DC for 'administration' rules

root@packetfence:/bin#
```

Figure II-31: *Authentication against AD*

5.5. Connection profiles definition for 802.1X and MAC authentication

The connection profiles in PacketFence allow us to authenticate a number of types of connection sessions using various standard authentication protocols, including PAP (Password Authentication Protocol), CHAP (Challenge-Handshake Authentication Protocol), PEAP (Protected Extensible Authentication Protocol) and EAP (Extensible Authentication Protocol).

PacketFence specifies the authorized protocol available for the network devices on which the user attempts to authenticate and specifies the identity sources from which the user's authentication is validated. Rule-based connection profiles consist of attribute-based filters that determine the authorized protocols and the identity source to be used for processing requests.

- **802.1X profiles :**

  This connection profile in (**Figure II-32**) is to use the 802.1X protocol, and it authenticates user accounts using the Active directory as authentication source for users credentials.

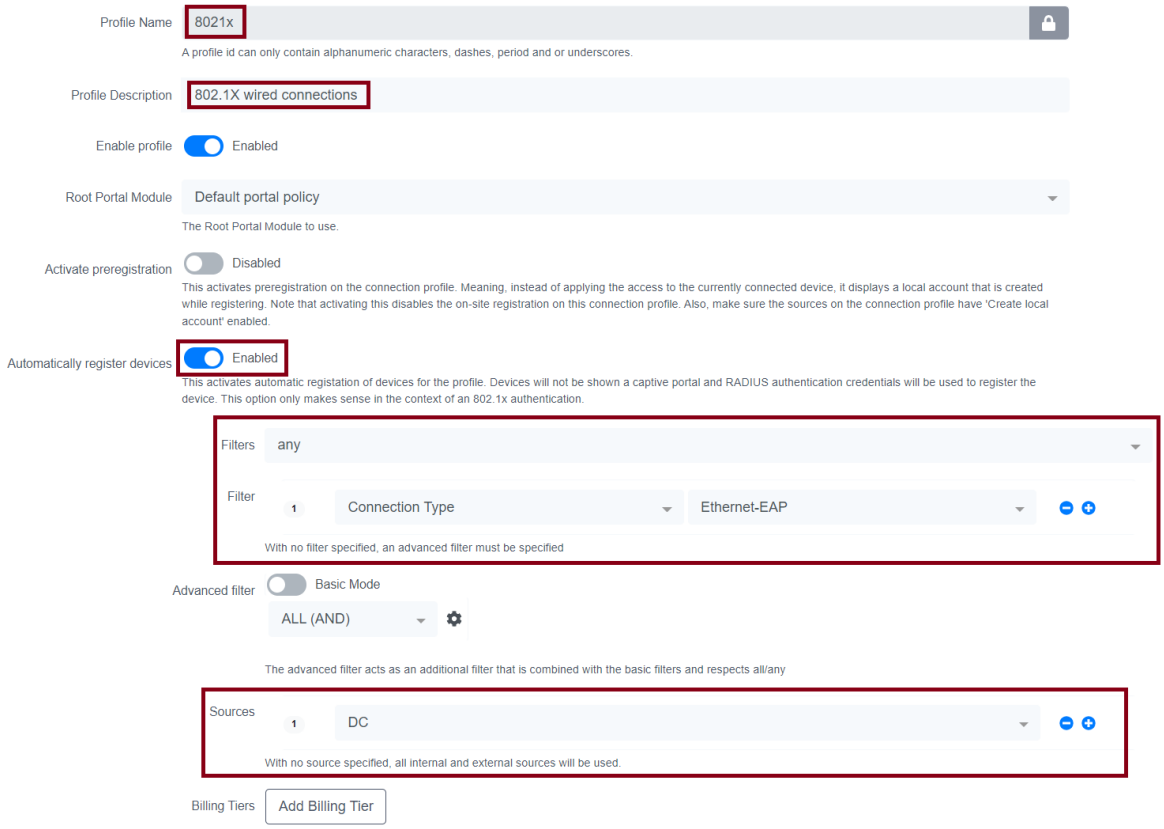

Figure II-32: *802.1X connection profile*

Note: When a client connects through Ethernet-EAP, it signifies that 802.1X credentials are being used.

6. Developing the Python Application for the Tests

Before going to the testing phase, we coded a python app (**Figure II-33**) that will help us in our NAC solution testing process, and also in every future project in the network and security fields. This app is called “Your Network Friend” and has multiple features which are:

- Display your IP, MAC address and Operating System automatically.
- Ping a specific IP address to check its availability.
- Perform a DNS or reverse DNS lookup to retrieve the domain name associated with an IP address or the opposite.
- Scan ports on a specific IP address to check for open ones (Vulnerabilities).
- Sniff network traffic to capture and analyze packets.
- Push network device configurations to configure network devices remotely.

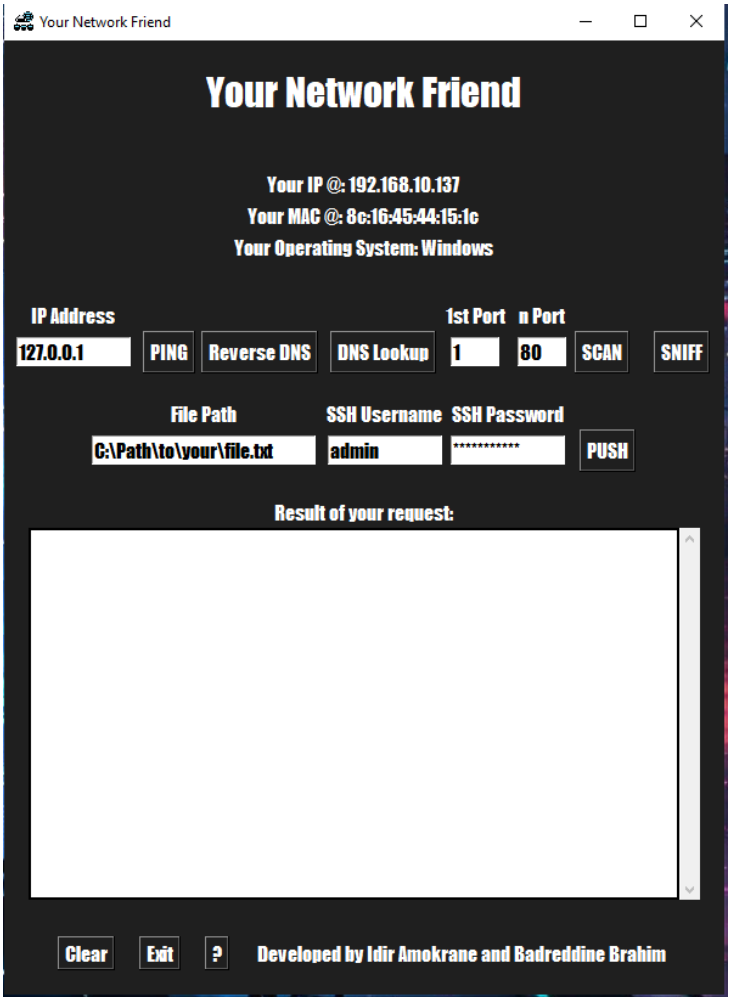

Figure II-33: *Your Network Friend Application GUI*

7. Conclusion

In this chapter, we created a practical architecture for implementing the PacketFence solution in a wired network. We successfully completed the implementation process despite difficulties with unfamiliar technology and little knowledge. We talked about the integration and configuration needs for a secure access control system.

We defined deployment phases and network topology for success. The infrastructure configuration included setting up the basic switch with interfaces, VLANs, DHCP, and SSH settings. After that, we set up PacketFence on the switch, activating RADIUS, AAA, dot1x, and SNMP. Additionally, we connected PacketFence to the Active Directory domain controller.

For network access control, we specified authentication sources and policies, as well as connection profiles for MAC and 802.1X authentication. In addition, we created a desktop program to automate device configuration and optimize network activities.

The above steps let us effectively integrate PacketFence into our network and set up a reliable Access Control system.

We will concentrate on ongoing management and monitoring of the NAC solution in the following chapter to ensure its continued efficacy and security in our network environment.

CHAPTER III: Testing phase

1. Introduction

Once the solution has been implemented, we proceed to the test phase in order to ensure the proper functioning of the equipment and configuration. Verification consists of trying to connect to wired networks, with two scenarios: once as an employee and once as an intern.

2. Flow chart for the operations of PacketFence

In the following (**Figure III.1**) we can see PacketFence operation for the test phase

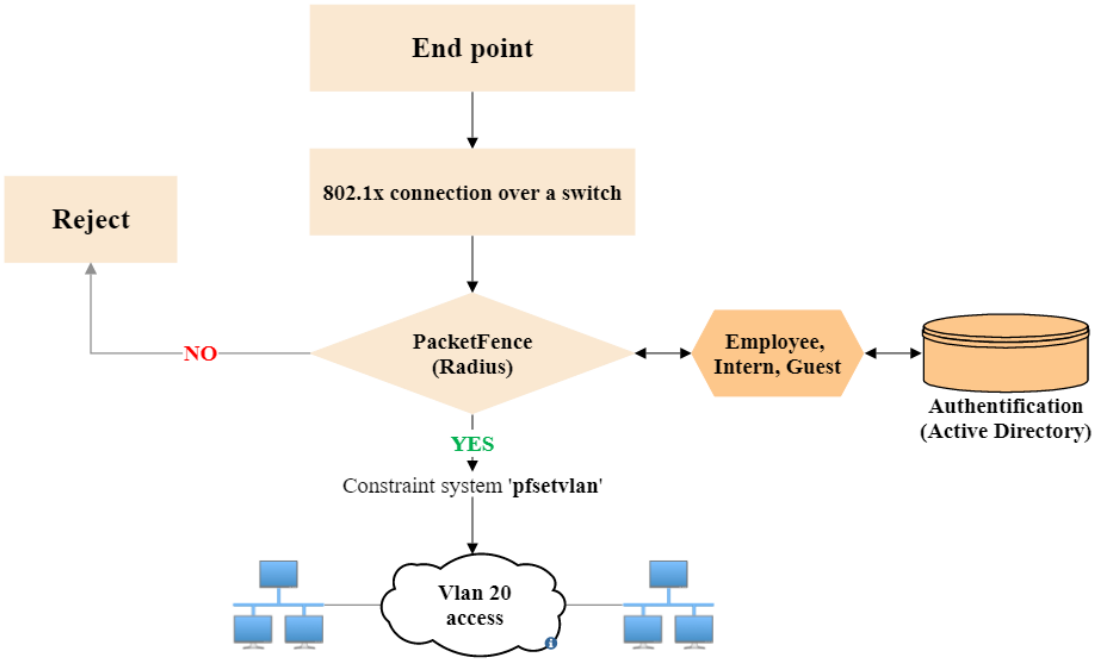

Figure III-1: *Organizational chart of the functioning of PacketFence*

3. Domain user testing

The first test to be performed will allow us to ensure that the authentication to the domain for a user of the wired network is working properly. The first thing we did was to enable 802.1X authentication on the Ethernet network cards because by default it is disabled on a Windows system. We started the "*Wired AutoConfig*" service, responsible for performing IEEE 802.1X authentication on Ethernet interfaces. After launching "*services.msc*" and clicking on the corresponding service, the following window (**Figure III-2**) appears to start the service:

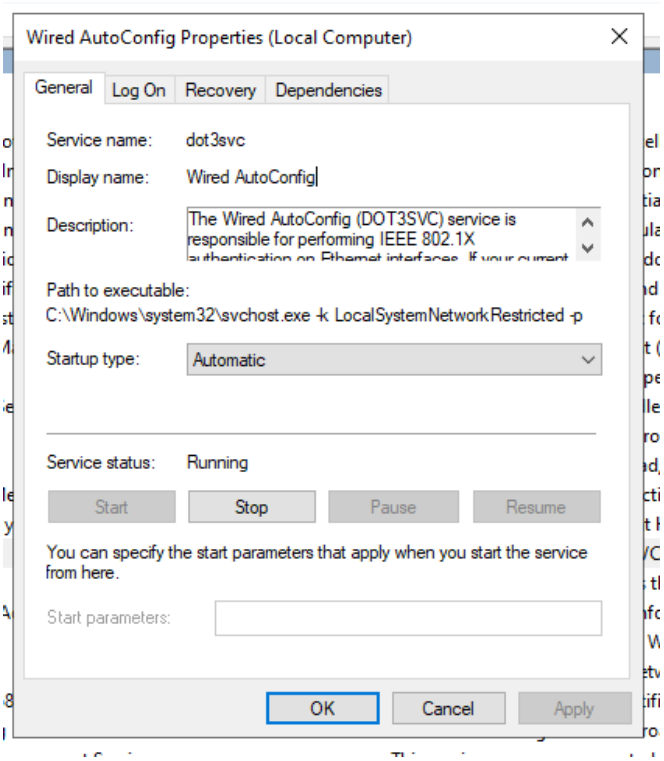

Figure III-2: *Enabling wired autoConfig service*

After that we need to enable 802.1X authentication on the Ethernet interface, as shown in the figure below (**Figure III-3**):

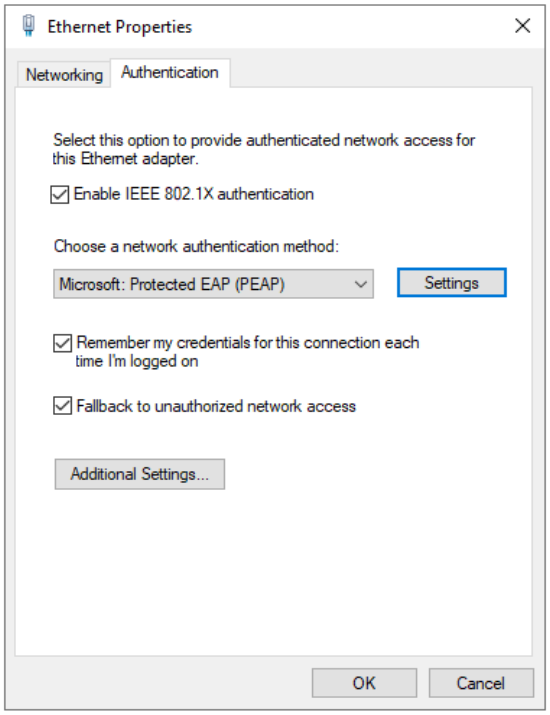

Figure III-3: *Enabling 802.1X on Ethernet card*

In the authentication method (**Figure III-4**), we make sure "Secured password (EAP-MSCHAPv2)" is selected in the EAP protocol settings and that "Validate server certificate" is not checked. Following that, click Configure and make sure the box next to "Automatically use

my Windows logon name and password (and domain, if any)" is not checked. Then validate these operations (click on ok).

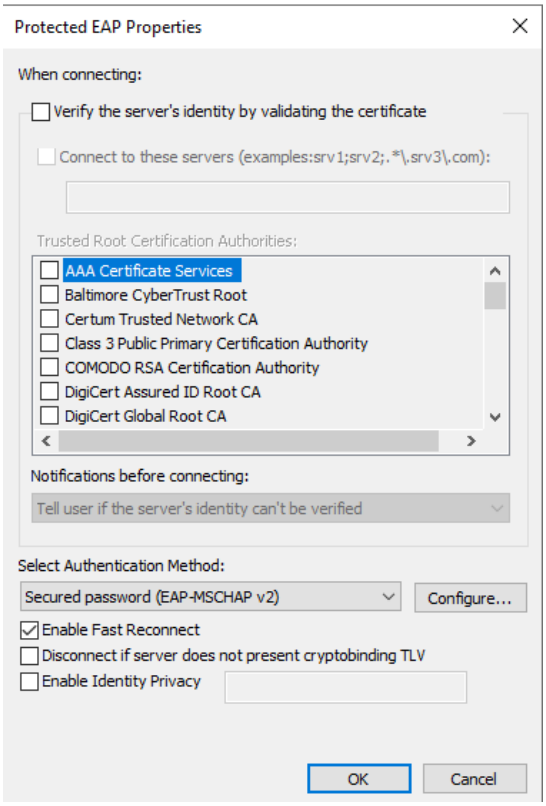

Figure III-4: *EAP settings*

As soon as the cable is connected to the Ethernet interface of the machine, the authentication window appears (**Figure III-5**):

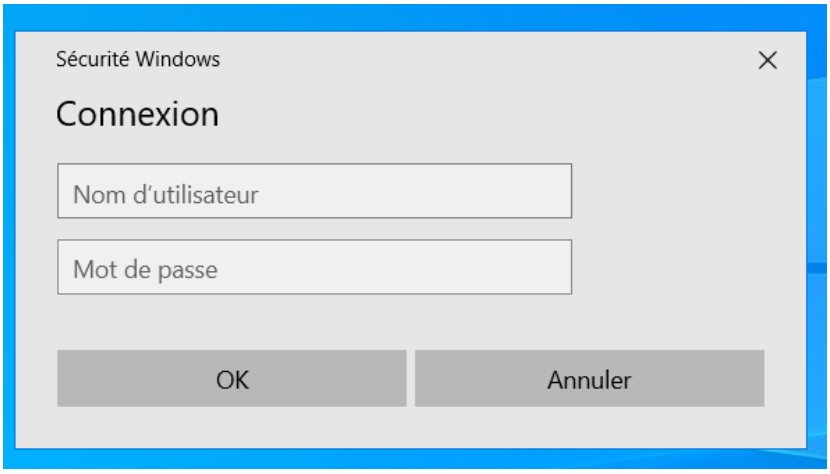

Figure III-5: *Authentication window*

in *'PacketFence audit logs'*, the connection profile "802.1X" is applied to the employee and intern with the authorization status 'Accept' for correct credentials (**Figure III-6**):

Created At	Auth Status	Server IP	MAC Address	Node Status	User Name	NAS IP Address	SSID
05/23/2023 11:35 AM	Accept	192.168.10.183	8c:16:45:44:15:1c	Registered	brahimemp	192.168.10.2	
05/23/2023 11:35 AM	Accept	192.168.10.183	8c:16:45:44:15:1c	Registered	8c164544151c	192.168.10.2	
05/23/2023 11:32 AM	Reject	192.168.10.183	8c:16:45:44:15:1c	Unregistered	brahimemp	192.168.10.2	
05/23/2023 11:32 AM	Reject	192.168.10.183	8c:16:45:44:15:1c	Unregistered	brahimemp	192.168.10.2	
05/23/2023 11:31 AM	Accept	192.168.10.183	8c:16:45:44:15:1c	Registered	empnet	192.168.10.2	
05/23/2023 11:31 AM	Disconnect-ACK		8c:16:45:44:15:1c	Unregistered		192.168.10.2	
05/23/2023 11:30 AM	Accept	192.168.10.183	8c:16:45:44:15:1c	Registered	empnet	192.168.10.2	
05/23/2023 11:08 AM	Accept	192.168.10.183	8c:ec:4b:10:25:e0	Registered	idirstg	192.168.10.2	
05/23/2023 11:06 AM	Accept	192.168.10.183	8c:ec:4b:10:25:e0	Registered	idirstg	192.168.10.2	
05/23/2023 11:05 AM	Accept	192.168.10.183	8c:ec:4b:10:25:e0	Registered	idirstg	192.168.10.2	

Figure III-6: *Authentication on the PacketFence side*

Note: in case the user attempts to enter incorrect credentials, the status "Rejected" appears.

As we can see in the figure below (**Figure III.7**) the full Authentication RADIUS reply. These attributes explain the authentication and authorization procedures of the PacketFence NAC system for the user "idirstg". The answer indicates that the authentication was successful, as indicated by the HTTP status code 200, and the user is granted access to VLAN 20.

RADIUS Reply

```
EAP-Message = 0x03710004
Message-Authenticator = 0x00000000000000000000000000000000
User-Name = "idirstg"
REST-HTTP-Status-Code = 200
Tunnel-Private-Group-Id = "20"
Tunnel-Type = VLAN
Tunnel-Medium-Type = IEEE-802
```

Figure III-7: *Authentication radius reply*

After the authentication process, the new node has access to the local network (VLAN 20) with the default network 192.168.20.0/24 and will be added to PacketFence's local node database with a registered status and user role based on the credentials entered, as shown in the figure below (**Figure III-8**):

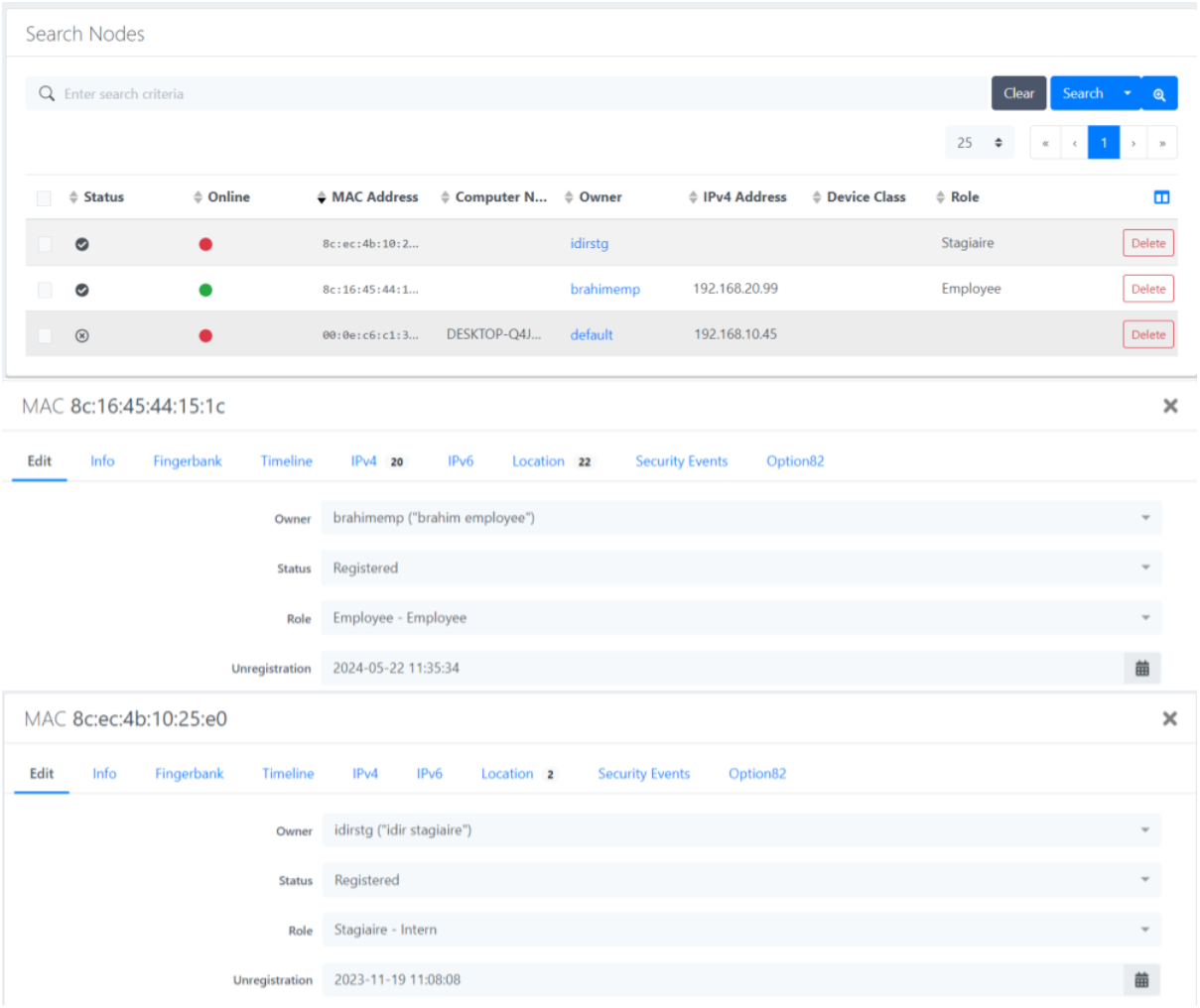

Figure III-8: *Registered nodes*

As we can see (**Figure III-9**), registered users have their own devices where we can see all proper information such as status, role, unregistration date and other information in info , location tabs (connection type/port, last seen...) with the possibility of revoking the access by restarting the switch port.

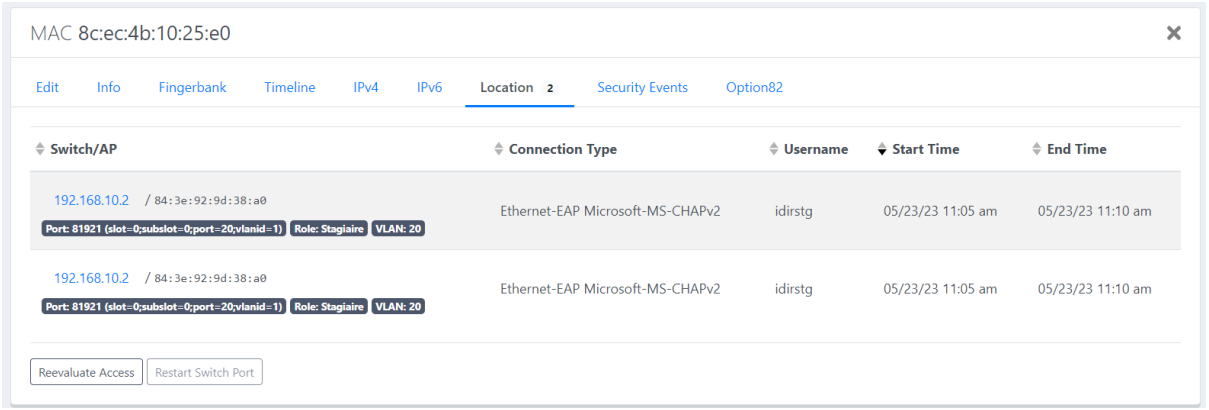

Figure III-9: *Node location in local network*

Below (**Figure III-10**) is a simple representation of our radial network with all it's nodes:

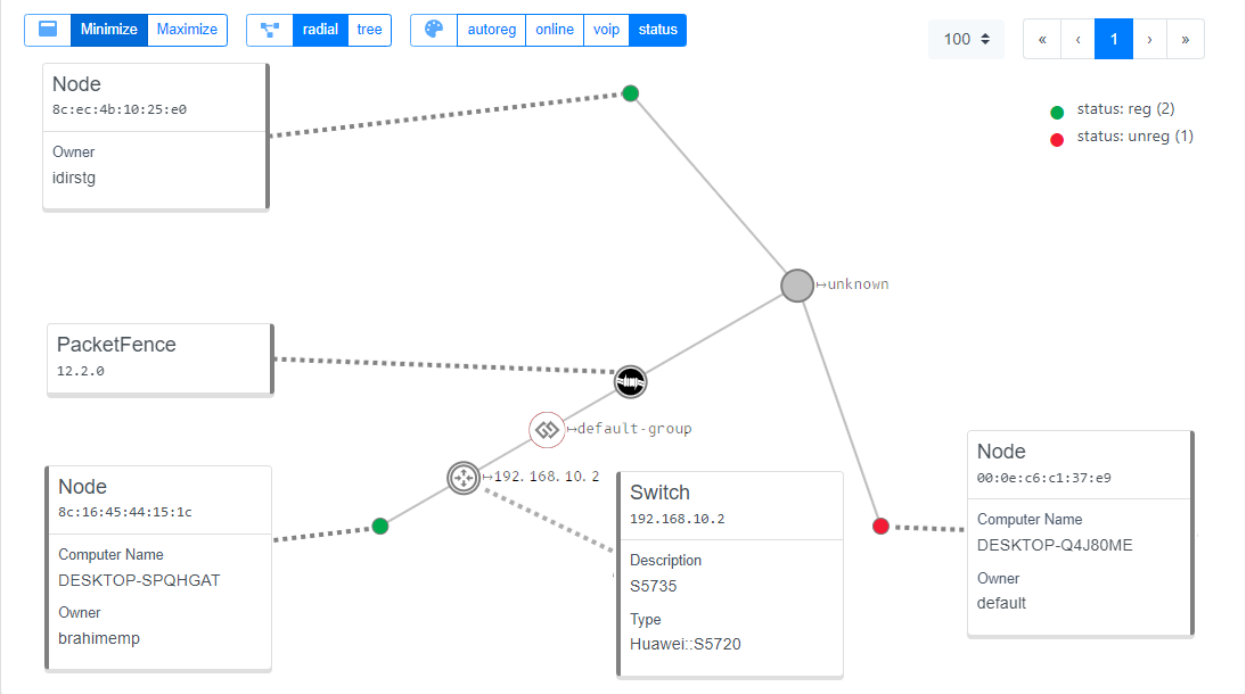

Figure III-10: *Radial model for detected nodes*

4. Testing with "Your Network Friend" Application

Our new application will help us in our testing phase to gain some time instead of using different software (Cmd, Wireshark, Nmap, PuTTy…) to do different commands.

4.1. Pinging from different VLANs

The first thing to do if we want to know if two VLANs are communicating is to perform a ping, and that is what we are going to do here (**Figure III-11**), the picture on the left shows a failed ping due to our ACL that doesn't allow traffic from VLAN 20 to 10, and the second shows a successful ping from a device to another one in the same VLAN.

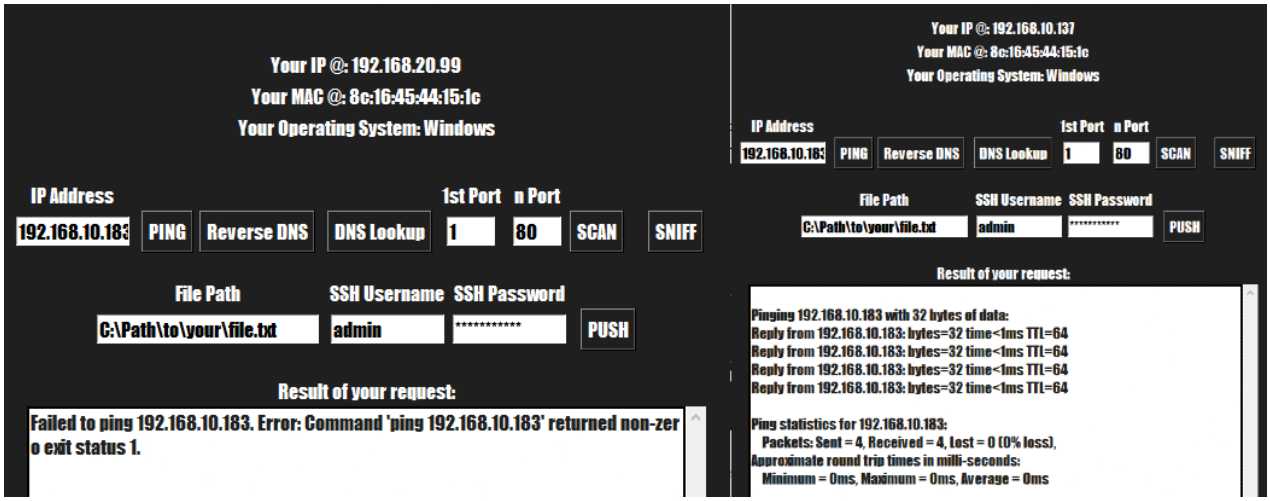

Figure III-11: *Pinging operations in different cases*

4.2. Scanning the open and closed ports on a specific IP address

This feature scans the open ports on an IP address that you enter and in a specific range, it also displays your internet download and upload speed (the speed failed because our main network is isolated) (**Figure III-12**).

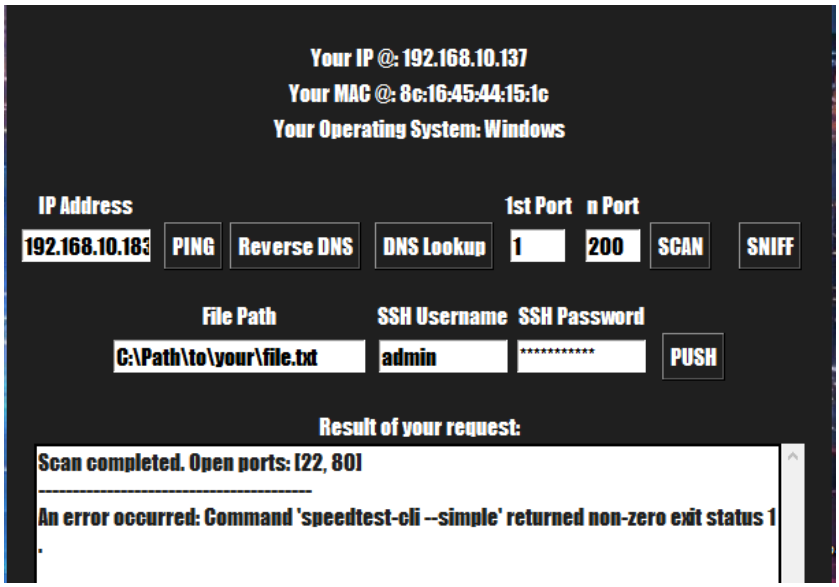

Figure III-12: Scanning for open ports

4.3. Sniffing the network to find some information

This feature sniffs the packets on your network and displays the information about the IP addresses and the ports (we used it here on a different network connected to the internet just to see the results because our main network is isolated) (**Figure III-13**).

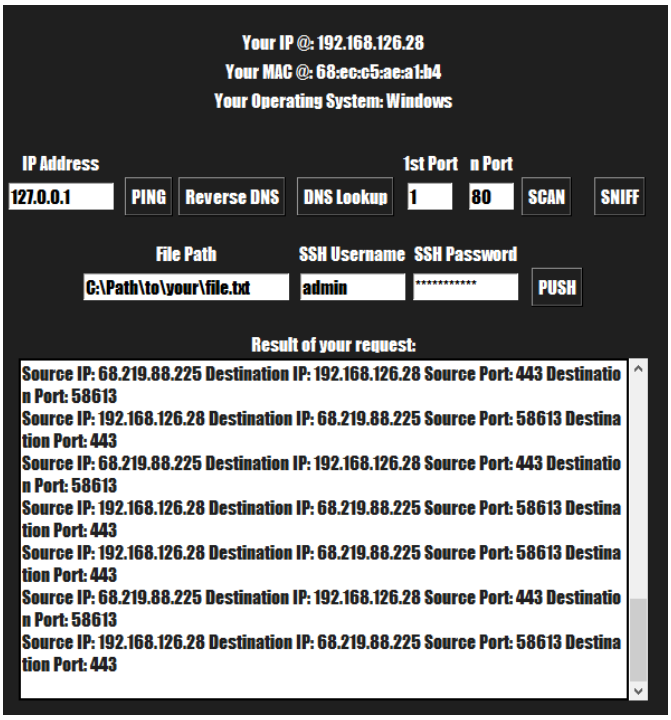

Figure III-13: Sniffing network traffic

4.4. Pushing a configuration into the switch

This feature pushes directly any configuration into our S5735 switch remotely, we just have to enter the .txt file (that contains any commands) path, IP address and SSH credentials and click on 'PUSH' (**Figure III-14**).

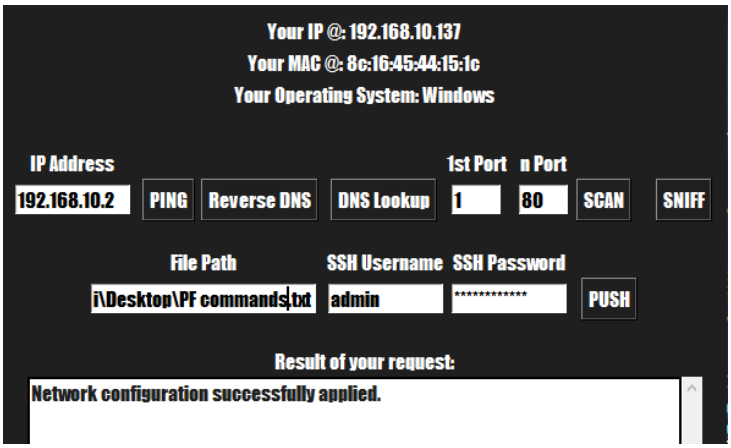

Figure III-14: *Pushing PacketFence configuration*

4.5. DNS lookup and reverse DNS lookup

These two features help you find the hostname of an IP address or the IP address of a hostname (**Figure III-15**).

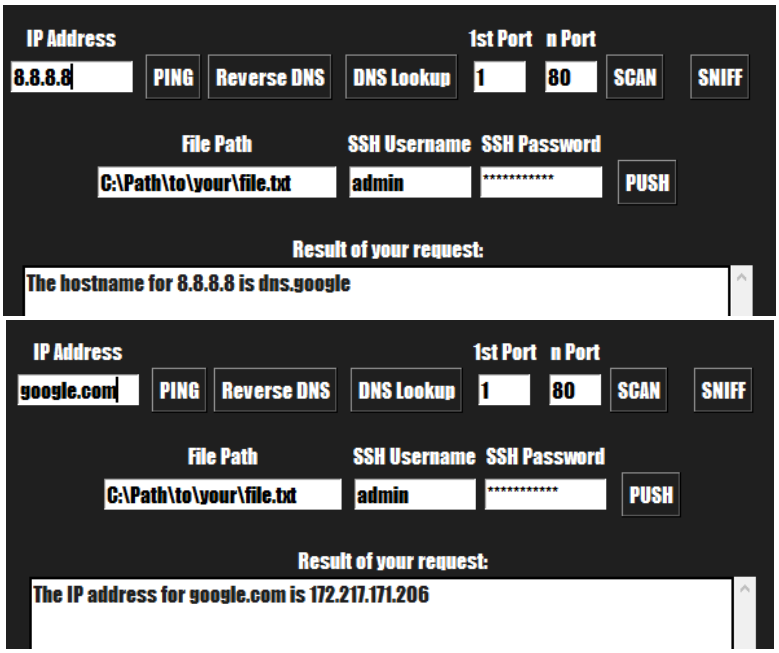

Figure III-15: *DNS and reverse DNS lookup*

5. Conclusion

In this chapter, we pushed our network's PacketFence Network Access Control (NAC) system through a series of tests. To help people understanding PacketFence functionality, we offered a clear flow chart that demonstrated the system's operating flow and decision-making procedures.

Then, we concentrated on analyzing MAC and 802.1X authentication methods while testing domain user authentication. We evaluated PacketFence capability to accurately apply access control policies through simulations of real-world situations and user interactions.

We created the "Your Network Friend" desktop program for testing purposes, which considerably benefited us in comprehending Python coding and network management tools.

Our in-depth testing confirmed PacketFence efficiency in identifying and authenticating domain users, enforcing access control policies, and keeping thorough audit logs. The reliability of the NAC solution was ensured by immediate resolution of any issues found.

In conclusion, PacketFence feasibility in our network environment was verified by our careful testing, which confirmed its successful implementation and functionality.

Conclusion and Future Works

As part of this project for the Sonatrach company, and based on a concern for security and the need to protect critical and vital resources on a permanent basis, we implemented a wired Network Access Control solution which ensures that only authorized persons have access to the network. This solution is even more necessary when you consider that, in some establishments, the number of users who frequently request access to the network is very high.

After an in-depth analysis of the company's needs, we were able to carry out a comparative study of various possible solutions, which led us to adopt the PacketFence solution and validate it in a test environment. We deployed the PacketFence solution, which reacts, in real time, to any attempt to connect to the network by reference to the security policies predefined in the PacketFence platform.

The user is asked to authenticate himself by presenting his user account and associated password if he belongs to the domain, and obtains Internet access. The verification of customer machine conformity status validation was not required on the part of the company due to the complexity of the network architecture so that they could offer us an antivirus server.

Regardless of all the difficulties encountered, we were able to achieve our goal of implementing the solution in the cable network. Our future plans include :

- To implement the solution in the wireless network in order to benefit more from the solution.

- Check the status of the operating system updates and the existence of certain security applications to ensure compliance.

References

[1] D. Kang, J. Oh, and C. Im, “A Study on Abnormal Behavior Detection in BYOD Environment,” vol. 7, no. 12, 2013.

[2] H. Nunoo-Mensah, E. K. Akowuah, and K. O. Boateng, “A Review of Opensource Network Access Control (NAC) Tools for Enterprise Educational Networks,” *Int. J. Comput. Appl.*, vol. 106.

[3] M. L. Mourad and M. M. Aziza, “Implémentation du protocole d’authentification 802.1x avec le serveur RADIUS dans les réseaux informatiques.”.

[4] T. Grance, J. Hash, S. Peck, J. Smith, and K. Korow-Diks, “Security guide for interconnecting information technology systems,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-47, 2002. doi: 10.6028/NIST.SP.800-47.

[5] J. Y. B. Carracedo, “IMPLEMENTATION OF BYOD-TYPE POLICIES UNDER A NAC-BASED APPROACH IN FREE SOFTWARE FOR THE MANAGEMENT OF SECURITY IN NETWORKS DATA,” 2015.

[6] “Network Access Control,” *Wikipedia*. Feb. 07, 2023. Accessed: Feb. 08, 2023. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Network_Access_Control&oldid=1137953892

[7] M. S. Inamdar and A. Tekeoglu, “Security Analysis of Open Source Network Access Control in Virtual Networks,” in *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, Krakow: IEEE, May 2018, pp. 475–480. doi: 10.1109/WAINA.2018.00131.

[8] E. Engfors and J. Markstedt, “Luleå University of Technology Department of Systems and Space Engineering May 28, 2017”.

[9] DRosolen, “How to choose the best Network Access Control solution (NAC),” *Silicon*, Apr. 13, 2009. https://www.silicon.es/como-elegir-la-mejor-solucion-de-control-de-acceso-a-la-red-nac-751 (accessed Feb. 08, 2023).

[10] “Tutorial: Network Access Control (NAC): Page 4 of 11.” https://www.networkcomputing.com/careers-and-certifications/tutorial-network-access-control-nac/page/0/3 (accessed Feb. 08, 2023).

[11] E. Chan, “Network Access Control”.

[12] “What Is Network Access Control? Explaining NAC Solutions.” https://www.varonis.com/blog/network-access-control-nac (accessed Feb. 08, 2023).

[13] “IEEE 802.1X,” *Wikipedia*. Dec. 30, 2022. Accessed: Feb. 09, 2023. [Online]. Available: https://en.wikipedia.org/w/index.php?title=IEEE_802.1X&oldid=1130430396

[14] “RADIUS,” *Wikipedia*. Jan. 19, 2023. Accessed: Feb. 27, 2023. [Online]. Available: https://en.wikipedia.org/w/index.php?title=RADIUS&oldid=1134635324

[15] B. Lee, “RADIUS Protocol Explained,” *JumpCloud*, May 24, 2022. https://jumpcloud.com/blog/what-is-the-radius-protocol (accessed Jun. 01, 2023).

[16] “How RADIUS Server Authentication Works.” https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/authentication/radius_how_works_c.html (accessed Jun. 05, 2023).

[17] “Exposé : 802.1x.” http://igm.univ-mlv.fr/~dr/XPOSE2008/802.1x/EAP.html (accessed Feb. 27,

2023).

[18] "Tutorial: Network Access Control (NAC): Page 2 of 11." https://www.networkcomputing.com/careers-and-certifications/tutorial-network-access-control-nac/page/0/1 (accessed Feb. 08, 2023).

[19] H. N. Security, "Network Access Control (NAC)," *Help Net Security*, Nov. 26, 2007. https://www.helpnetsecurity.com/2007/11/26/network-access-control-nac/ (accessed Feb. 08, 2023).

[20] "ise-solution-overview." Accessed: Feb. 25, 2023. [Online]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/ise-solution-overview.pdf?ccid=cc001033&dtid=odicdc000016&oid=aagsc026000

[21] "fortinac." Accessed: Feb. 25, 2023. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf

[22] "UNIFIED ACCESS CONTROL." Accessed: Feb. 25, 2023. [Online]. Available: https://www.juniper.net/assets/us/en/local/pdf/brochures/1500051-en.pdf

[23] "openNAC site - Solution." http://www.opennac.org/opennac/en/solution.html (accessed Jun. 01, 2023).

[24] "PacketFence | Open Source NAC." https://www.packetfence.org/ (accessed Feb. 25, 2023).

[25] "The FreeNAC Open Source Project on Open Hub." https://www.openhub.net/p/8572 (accessed Feb. 25, 2023).

[26] "FreeRADIUS," *Wikipédia*. Aug. 27, 2019. Accessed: Mar. 01, 2023. [Online]. Available: https://fr.wikipedia.org/w/index.php?title=FreeRADIUS&oldid=162155981

[27] "Snort - Network Intrusion Detection & Prevention System." https://www.snort.org/ (accessed Mar. 01, 2023).

[28] "Tenable® - The Cyber Exposure Management Company," *Tenable®*. https://www.tenable.com/node (accessed May 30, 2023).

[29] "Background," *Greenbone Community Documentation*. http://greenbone.github.io/docs/latest/background.html (accessed May 30, 2023).

[30] "OpenVAS - Open Vulnerability Assessment Scanner." https://www.openvas.org/ (accessed May 30, 2023).

Appendix 1: Host Organization

1. Presentation of the host organization

1.1. Sonatrach

The national oil firm of Algeria is called Sonatrach. With 154 subsidiaries, it is the largest business in Africa today and is frequently referred to as the continent's first "major" oil corporation. It was founded in 1963. Sonatrach ranked as the seventh-largest gas firm in the world in 2021. It had 1,530 billion Algerian dinars in gross sales and 175 billion in net income in 2002. The company generated 30% of Algeria's gross national product with its 120,000 or so employees. 206 million Tons of Oil Equivalent (ToE) were produced annually, with 24 million ToE, or 11.7% of the total, going to the Algerian domestic market.

The company's export sales climbed by 75% in 2021, bringing the year's total revenues up to US$35 billion from US$20 billion. The results can be explained by the "return of global economic activity in 2021," according to vice president Rachid Zerdani. 95 million ToE worth of exports resulted from an increase in production to 185 million ToE. More than 53,000 people worked at Sonatrach, while more than 150,000 people were engaged in its subsidiaries.

1.2. Legal status

On February 11, 1998 by presidential decree n°98-48: SONATRACH was transformed

from a public economic enterprise (EPE) into a joint-stock company (SPA).

1.3. Subsidiaries

Enac, Sipex, Enageo, Ensp, Hyproc SC, Tassili Airlines, Naftal, ENTP, Enip, Enafor, ENGTP.

1.4. Missions and objectives

Since Sonatrach's founding, she has been in charge of its missions and objectives. Some of them are:

1.4.1. Missions

The SONATRACH's essential missions are as follows, under the direction of a general director:

-The creation, maintenance, and exploitation of energy networks across the national frontier. the transformation of export-oriented markets and goods.

- The commercial tool's adaptation to the needs of the energy market for a better understanding of its workings and improved commercial performance.

-The setting up, managing, and maintaining complexes for the production, transportation, and conditioning of hydrocarbons.

-The creation of contemporary management approaches through ongoing training.

-The study, promotion, exploitation, processing, and refinement of hydrocarbons.

-Liquefaction of natural gas, treatment, and hydrocarbon recovery.

-The growth of any joint venture between Algerian businesses and foreign businesses both inside and outside of Algeria.

-The country's medium- and long-term hydrocarbon supplies.

-The investigation, support, and valorization of any other energy source or form.

-the growth of any activity, regardless of method, that has a connection to the hydrocarbon sector. Additionally, any activity that might spark interest in Sonatrach as well as any general activity of any kind that might be directly related to its corporate objectives.

1.4.2. Objectives

-Buying and keeping any portfolio of shares. Equity stakes and other movable assets in any active company, whether it was founded in Algeria or elsewhere

– The ongoing mastering of its foundational vocations.

-The development of its managerial and technological capabilities.

-The creation, administration, and management of hydrocarbon transport, storage, and loading.

1.5. Presentation of the organizational chart of the reception structure

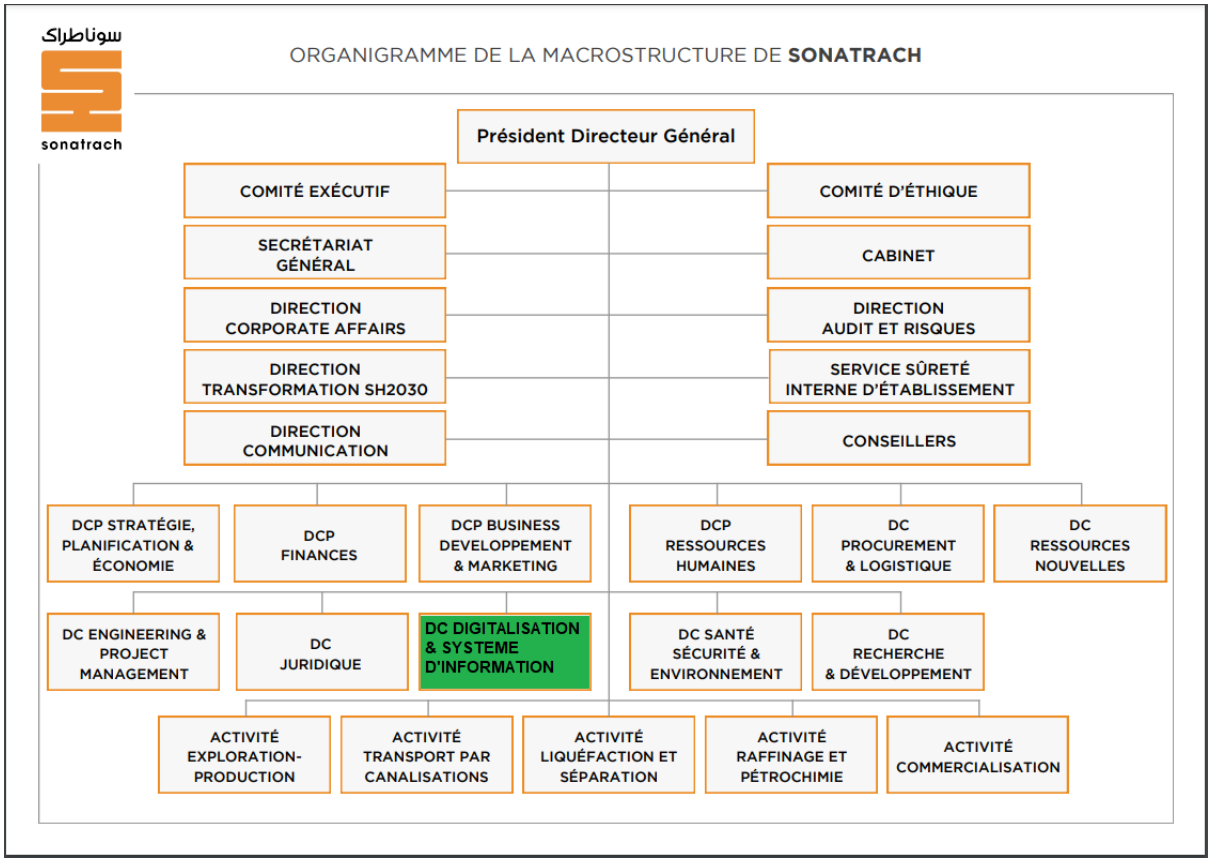

Figure 1-1: *Sonatrach flowchart diagram*

1.6. Department of Reception Presentation (DC-DSI):

DC-DSI: The Central Directorate of Digitalization & Information System:

The Central Directorate-CIO (DC-CIO) is the main processing directorate of the company SONATRACH in computer science, it constitutes:

The preferred tool of the general directorate in terms of IT. The treatment center from the central directions.

The service provider who indicates the operational structures.

The (DC-DSI) does not exercise direct supervision over the company's structures in matters IT, she is the company's interlocutor for all relations in these matters with external organizations. Its organization is based on the following activities :

The fundamental distribution between the activity of realization of computer products and those of their use.

The grouping into homogeneous entities of basic activities that can integrate into sets consistent.

The provision of operational autonomy to internal structures allowing them to search for profitability.

The minimization of the dependence of internal structures by the use of equipment and adequate software The continuous promotion of computer science by the provision of users Of adapted skills and means.

The possibility of taking over the management of the IT equipment of the structures which would be entrusted to him.