République Algérienne Démocratique et Populaire
Ministére de l'Enseignement Supérieur et de la Recherche Scientifique
Université A. Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de Fin de Cycle

En vue de l'obtention du diplôme de Master Professionnel en Informatique

Option :

Administration et Sécurité des Réseaux

Thème

Déploiement d'une passerelle de bureau à distance sécurisée. Cas d'étude : groupe Cevital – Béjaïa

Réalisé par :

M^{lle} MEDJOUDJ Klodia
M^{lle} MAZOUZ Thilelli

Devant le jury composé de :

Présidente :	M^{lle} HOUHA Amel	M.A.A	Université de Béjaïa
Encadrante :	M^{lle} ZAMOUCHE Djamila	M.A.B	Université de Béjaïa
Examinatrice :	Mme CHABANE Sara	M.A.B	Université de Béjaïa
Examinatrice :	M^{lle} BRAHMI Saloua	Doctorante	Université de Béjaïa

Promotion 2022 – 2023

Remerciements

Nous tenons d'abord à remercier Dieu le tout puissant et miséricordieux, qui nous a donné le courage, la volonté et la patience afin d'accomplir ce modeste travail.

Nous tenons à exprimer notre profonde gratitude et nos sincères remerciements à notre encadrante ***Dr. ZAMOUCHE Djamila*** *pour l'honneur qu'elle nous a fait en acceptant de nous encadrer, elle a été le meilleur guide et conseiller, pour sa patience, sa disponibilité et ses encouragements. Ses conseils précieux ont permis une bonne orientation dans la réalisation de ce travail.*

Un grand merci pour ***M. CHALANE Tahar*** *notre maître de stage pour toute l'aide qu'il a pu nous procuré, son accompagnement tout au long de cette expérience professionnelle. Sans oublier de remercier l'ensemble des employés de la direction des Systèmes d'Information de CEVITAL pour les conseils qu'ils ont pu nous accorder au cours de notre stage.*

Nos sincères remerciements aux membres de jury qui nous ont fais l'honneur en acceptant d'évaluer notre travail. Nous leurs présentons toute notre gratitude et nos profonds respects.

Nos plus chaleureux remerciements vont également à à nos parents, nos familles et à tous nos amis pour leurs soutiens morales et financiers et de nous avoir encourager et accompagner durant notre cursus d'étude.

Enfin, nous remercions tous ceux qui ont contribués de près ou deloin à l'élaboration de ce mémoire.

Dédicaces

Avec tous mes sentiments de respect, avec l'expérience de ma reconnaissance, je dédie mon projet de fin d'étude.

À la prunelle de mes yeux ***maman*** *merci pour tout ce que tu as fait pour moi. ton amour inconditionnel, tes sacrifices, tes conseils avisés et surtout ta confiance en moi. Que tu trouves ici le témoignage de ma profonde reconnaissance.*

À mon support qui était toujours à mes côtés pour me soutenir, m'encourager et m'épauler pour que je puisse atteindre mes objectifs, merci ***mon père****, que ce travail traduit ma gratitude et mon affection.*

Vous avez donné le plus beau des cadeaux : une éducation, le meilleur héritage que les parents puissent transmettre à leur enfant. Puisse dieu vous prêter la bonne santé et longue vie afin que je puisse a mon tour vous combler.

À mes chères sœurs ***Chanez****,* ***Nihad*** *et chers frères* ***Hamza****,* ***Adem*** *pour leurs compréhensions et patience.*

À toute ma famille, en particulier mes deux oncles ***Lounis*** *et* ***Achour****, à ma tante* ***Zahra*** *pour leurs aides, conseils et encouragement durant mes années d'étude.*

À ma binôme et chère amie ***Thilelli*** *à qui je souhaite bonne chance pour son avenir.*

A tous mes proches, tous les ami(e)s, tous ceux et celles qui ont cru en moi, merci.

Klodia

Dédicaces

C'est avec une profonde gratitude et en toute sincérité que je dédie ce modeste travail de fin de cycle.

À la personne la plus précieuse de mon cœur, à celle qui m'appris le vrai sens de la vie, à celle qui m'a donné de la tendresse, de la force et de la détermination pour continuer le chemin et affronter les différents obstacles, à la femme qui a souffert sans me laisser souffrir, ma chère adorable ***maman****.*

À l'homme à qui je dois ma réussite et tout mon respect et a été souvent à mes côtés pour me soutenir et m'encourager. À celui qui m'a toujours appris comment réfléchir avant d'agir, qui m'a soutenu tout au long de ma vie scolaire, à celui dont je suis fière de porter son nom, mon cher ***père****.*

Aucune dédicace ne saurait exprimer l'amour et le respect que j'ai toujours eu pour vous. Ce modeste travail est le fruit de votre éducation, que Dieu vous accorde une bonne santé et une vie longue et heureuse.

À mes précieuses sœurs ***Tiziri****,* ***Dehbia*** *,* ***Kahina*** *et mon très cher frère* ***Moussa*** *qui m'ont toujours soutenu et encouragé tout au long de mes études. Que Dieu les protège et leurs offre la chance et le bonheur.*

À mes adorables nièces ***Asma****,* ***Eline****,* ***Amel*** *et mon aimable neveu* ***Billal*** *que dieu les bénisse et les garde.*

À toute ma famille qui m'a doté d'une éducation digne son amour a fait de moi ce que je suis aujourd'hui. Mon grand-père, mes grands-mères, mes oncles, mes tantes, mes cousins et mes cousines. Que Dieu leurs donne une longue et joyeuse vie.

À tous mes ami(e)s avec lesquels j'ai partagé les bons et les mauvais moments qui m'ont toujours encouragé, et à qui je souhaite plus de succès.

À ma chère collègue ***Klodia****, merci pour les bons moments qu'on a partagés ensemble, et à qui je souhaite une vie pleine de santé et de bonheur.*

À toutes les personnes que j'apprécie et que je n'ai pas citées qui m'ont aidé à réaliser mon travail de près ou de loin.

À tous ceux que j'aime.

Thilelli

Table des matières

Table des figures

Liste des abréviations

AH	Authentication Header
ACL	Access Control Lists
API	Application Programming Interface
CPU	Central Processing Unit
CD	Compact Disc
DSI	Direction Des Systèmes D'informations
DMZ	Zone Démilitarisée
DOS	Denial Of Service
DVD	Digital Versatile Disc
DNS	Domain Name System
ENAJUC	Entreprise Nationale Des Jus Et Conserve Alimentaires
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GSA	Grandes Surfaces Alimentaires
GOGETP	Compagnie Générale Des Équipements De Travaux Publics
GPAO	Gestion De La Production Assistée Par Ordinateur
GSM	Global System For Mobile
GRH	Gestion Des Ressources Humaines
GUI	Graphical User Interface
GNOME	GNU Network Object Model Environment
GRUB	Grand Unified Bootloader
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IPS	Intrusion Prevention Systems
IDS	Intrusion Detection System
IP	Internet Protocol
ICMP	Internet Control Message Protocol
IPsec	Internet Protocol Security
IOS	IPhone Operating System
JDBC	Java Database Connectivity
LAN	Local Area Network
MAC	Media Access Control
MACOS	Macintosh Operating System
MYSQL	My Structured Query Language
NAC	Network Access Control
PC	Personal Computer
RDP	Remote Desktop Protocol
SPA	Société Privée Algérienne
SSG	Secure Services Gateway
SSL	Secure Sockets Layer
SSH	Secure Socket Shell

SIEM	Security Information And Event Management
SFTP	Secure File Transfer Protocol
SDK	Software Development Kit
TLS	Transport Layer Security
TELNET	Telecommunication Network
TCP	Transmission Control Protocol
TOMCAT	Total Onboard Material Configuration Audit Tool
TOTP	Time-based One-time Password
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VSAT	Very Small Aperture Terminal
VPN	Virtual Private Network
VPDN	Virtual Private Dialup Network
VNC	Virtual Network Computing
VM	Virtual Machine
WSUS	Windows Server Update Services
2FA	Two-factor Authentication

Introduction générale

De nos jours, le monde connaît une avance considérable dans l'Informatique qui joue un rôle très important dans le développement technologique de nombreuses entreprises grâce aux logiciels qui proposent maintenant des solutions à tous les problèmes. Outre, l'évolution de la *technologie d'accès à distance* permettant de profiter de taux de transfert de plus en plus rapides.

Avec la progression des menaces Informatiques et l'augmentation du nombre de télétravailleurs notamment dans la période de pandémie de *Covid-19*, l'*accès distant sécurisé* est devenu un élément essentiel des environnements informatiques actuels. Pour une utilisation optimale, le modèle nécessite la formation des utilisateurs, des politiques de sécurité renforcées et le développement de meilleures pratiques en matière de sécurité. Le bureau distant est une solution puissante et idéale qui offre une assistance à distance rapide garantissant la sécurité de l'accès, la mobilité des utilisateurs et la mise à disposition des applications à tout moment et à n'importe quel endroit.

Notre contribution consiste à déployer une *passerelle de bureau à distance sécurisée* nommée *Guacamole* permettant d'accéder à des environnements de bureau à l'aide de protocoles de bureau à distance (tels que SSH ou RDP). Cette dernière se compose de plusieurs parties ; serveur guacamole, client guacamole, l'application Web qui implémente une interface Web avec laquelle un utilisateur interagit réellement avec Guacamole et Guacd ou le cœur de Guacamole qui traduit entre les protocoles de bureau à distance et le protocole guacamole. La principale raison d'utiliser Guacamole est un accès constant, mondial et sans entrave à vos ordinateurs.
Pour assurer la sécurité de la passerelle et permettre aux utilisateurs de se connecter à distance en toute sécurité et en garantissant la confidentialité de leurs données, nous avons choisi de mettre en place deux méthodes d'authentification à deux facteurs fortes à savoir TOTP pour générer des codes à usage unique basés sur le temps, et DUO pour nous offrir de plus la réception des notifications push.

Ce mémoire est organisé en cinq chapitres. Dans le premier chapitre intitulé *« Présentation de l'organisme d'accueil »* , nous allons présenter l'organisme d'accueil Cevital ainsi le contexte du projet, la problématique ainsi que les solutions proposées.

Dans le deuxième chapitre intitulé *« Prérequis et méthodologies »*, nous allons introduire les généralités sur la sécurité Informatique et la passerelle de bureau à distance.

Le troisième chapitre *« Installation et configuration de Guacamole »* va porter sur la la phase de réalisation où on va spécifier les outils de développement utilisés et les différentes étapes d'installation et configuration pour la mise en place de la passerelle de bureau à distance «Guacamole» avec l'illustration et l'explication de quelques interfaces de l'application.

Le quatrième chapitre *« Implémentation de l'authentification à deux facteurs dans Guacamole »* consiste à renforcer la sécurité de l'application et obtenir une vérification supplémentaire de l'identité de l'utilisateur.

Le cinquième chapitre nommé *« Mise en service et test »* porte sur l'analyse de la sécurité où nous allons effectuer des tests afin de garantir la fiabilité et la robustesse de la passerelle .

Enfin, une dernière partie constitue une conclusion générale qui résume l'apport essentiel de notre travail.

Chapitre 1

Présentation de l'organisme d'accueil

1.1 Introduction

CEVITAL est la première entreprise privée algérienne à avoir investi dans des secteurs d'activité diversifiée. Elle est considérée le leader du secteur des industries alimentaires en Algérie en couvrant la plupart des besoins nationaux. Elle a traversé d'importantes étapes historiques pour atteindre sa taille et sa notoriété actuelle.

Ce chapitre s'articule autour de deux parties. Dans la première partie nous allons présenter l'entreprise CEVITAL et son organisme ainsi que l'organigramme qui illustre les différentes directions de cette société, notamment la direction des systèmes d'information (DSI) où on a effectué notre stage. La deuxième partie sera consacrée à la définition de contexte de notre projet tout en posant la problématique autour de laquelle tournera ce dernier.

1.2 Société d'accueil CEVITAL

1.2.1 Présentation de CEVITAL

CEVITAL est une Société Par Actions (SPA), créée avec des fonds privés en mai 1998, par l'entrepreneur algérien ISSAD REBRAB. Elle est la première société privée dans l'industrie de raffinage d'huiles brutes sur le marché algérien, constituée de plusieurs unités de production équipées de la dernière technologie et poursuit son développement par divers projets en cours de réalisation[1]. La figure 1.2 illustre les différentes unités "Agro-Industrie".

FIGURE 1.1 – Logo Cevital [1].

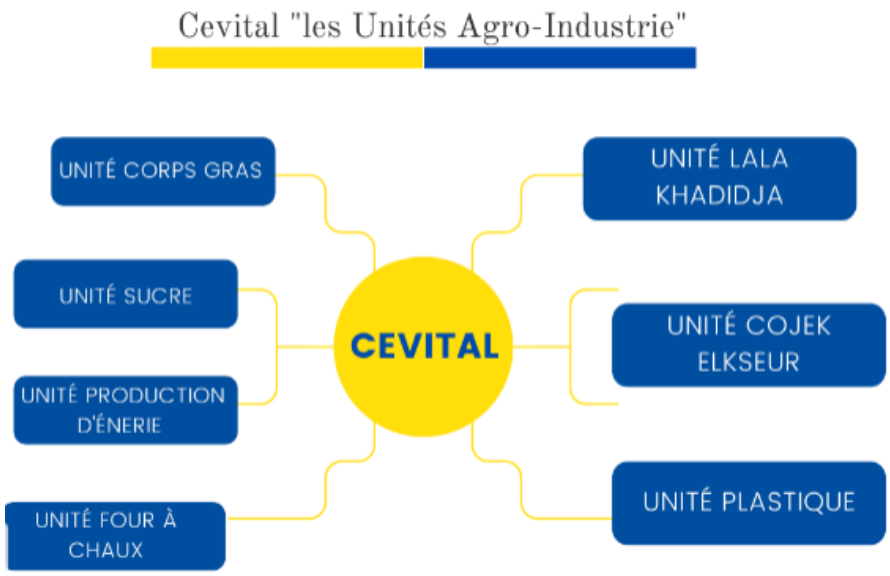

FIGURE 1.2 – Les différentes unités "Agro-Industrie" [2] .

1.2.2 Historique

CEVITAL est une entreprise algérienne, agissant dans les domaines de l'industrie agroalimentaire et de la grande distribution. Elle s'est bâti sur une histoire, un parcours et des valeurs qui ont fait sa réussite et sa renommée.
Pour s'imposer sur le marché, Cevital négocie avec les grandes sociétés commerciales, telles que CARREFOUR et AUCHAIN (en France), ROYAL (en suisse) et autres sociétés spécialisés dans l'import-export en UKRAINE et Russie. Ses produits se vendent aujourd'hui dans plusieurs pays, notamment en Europe, au Maghreb, au Moyen Orient et en Afrique de l'Ouest.
CEVITAL a traversé d'importantes étapes historiques pour atteindre sa taille et sa notoriété actuelle.
Ci-après, quelques dates qui ont marqué l'histoire de CEVITAL [3] :

- 1975 : lancement dans la construction métallique .
- 1986 : création de METAL SIDER (sidérurgie).
- 1991 : création du quotidien d'information liberté.
- 1997 : création d'Hyundai MOTORS ALGERIE : représentant officiel d'Hyundai motor company (Corée du Sud).
- 1998 : création de CEVITAL SPA industries agroalimentaires.
- Février 1999, le debut des travaux de génie civil des raffineries et la mise en service en août 1999.
- 2006 : Acquisition de COJEK, filiale d'ENAJUC : Jus et conserves.
  Création de NUMIDIS-UNO (GSA).
- 2007 : création de MFG (verre plat).
  Création de SAMHA : Assemblage et distribution de produits électroniques et électroménagers de marque SAMSUNG Électroniques en Algérie.
- 2008 : création de MFG Europe : Commercialisation de verre plat en Europe.
  Création de GOGETP : Engins de travaux publics VOLVO.
  Création de NUMILOG : Entreprise spécialisée dans logistique et la gestion de la chaîne logistique.

- 2010 : Démarrage de l'exportation du sucre en Europe.
- 2013 : CEVITAL rachète le Français OXXO, spécialisée dans la menuiserie PVC.
  Investi dans ALAS (Espagne) : Usine d'aluminium ;
- 2014 : CEVITAL reprend les activités françaises du groupe FAGOR-Brandt : électroménager français.
  Investi dans AFFERPI (Italie) : usine de métal ;
- 2014 – aujourd'hui : le groupe CEVITAL a su marquer sa présence sur les trois continents (Afrique, Europe et Amérique latine) avec un volume d'export parmi les plus élevés en Algérie.
  Il réalise un chiffre d'affaires de 4 Milliards de dollars et vise à atteindre 25 Milliards de dollars à l'horizon 2025. Cette évolution est le résultat d'une vision moderne, ambitieuse et stratégiquement cohérente avec l'économie algérienne et internationale.

1.2.3 Situation géographique

Le complexe CEVITAL agro-industrie s'étend sur une superficie de 45000 m^2, c'est le plus grand complexe privé en Algérie. Il se situe au niveau du nouveau quai du port de Bejaia, à $3km$ du sud-ouest de cette ville, à proximité de la route nationale N° 09 et N°26.

Cette situation géographique de l'entreprise lui a été très bénéfique étant donné qu'elle lui confère l'avantage de proximité économique. En effet elle se trouve proche du port et de l'aéroport. Cet emplacement lui permet aussi de posséder un quai privé, la prédisposant à l'accostage de cargo de 40000 à 60000 tonnes [4].

FIGURE 1.3 – Situation géographique de Cevital [3].

1.2.4 La structure organisationnelle de CEVITAL

La figure 1.4 illustre l'organigramme générale du groupe CEVITAL, où chaque direction a pour but d'assurer le bon fonctionnement de chaque partie du groupe [5]. Notre étude porte, au niveau du groupe CEVITAL, sur l'optimisation du partage et du transfert de fichiers, qui dépend de la direction des systèmes d'information.

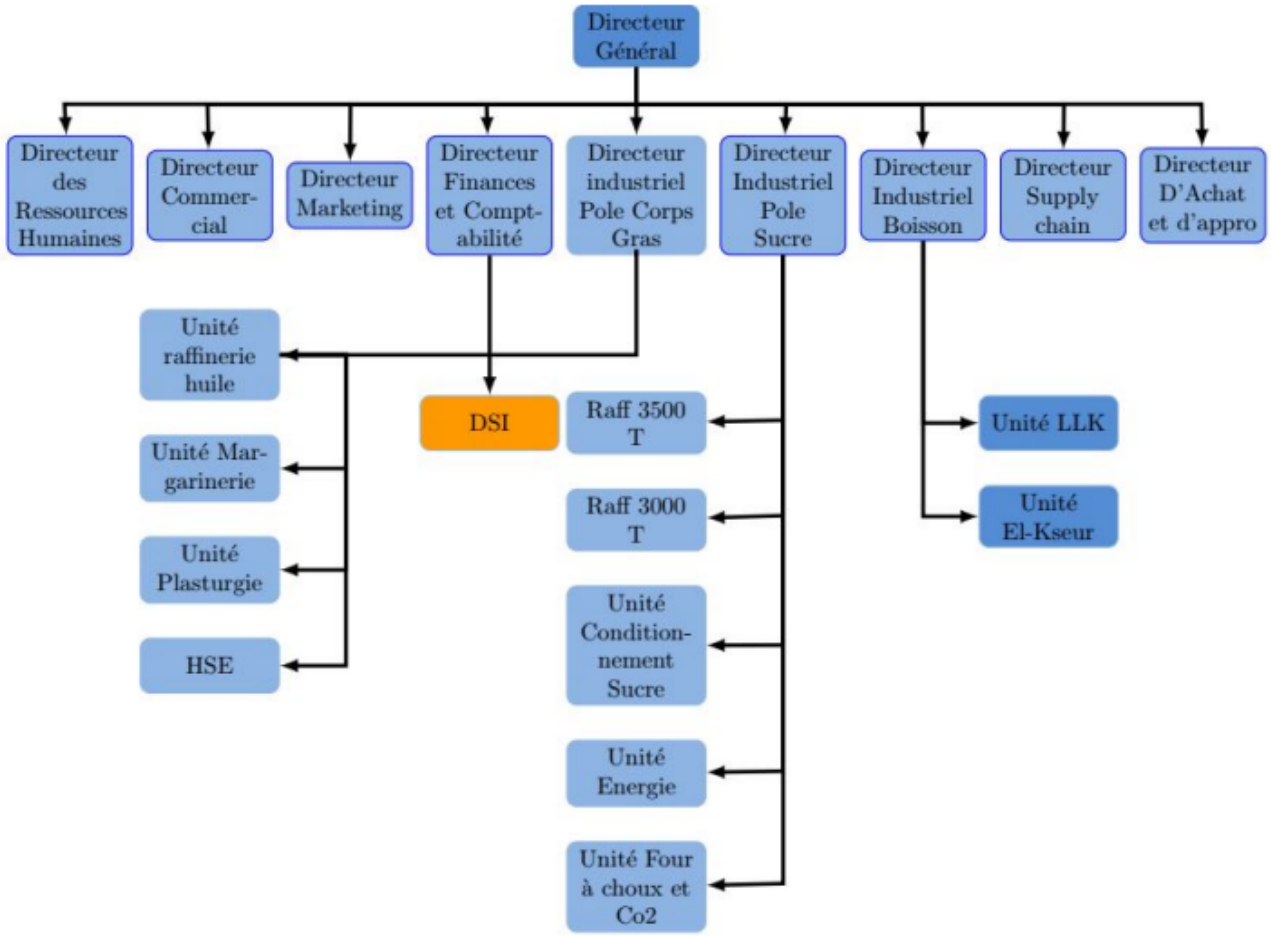

FIGURE 1.4 – Organigramme du groupe cevital [5].

1.2.4.1 Présentation de la Direction des Systèmes d'Informations (DSI)

La Direction des Systèmes d'Informations (DSI) est chargée de

. gérer l'ensemble des systèmes d'informations et de télécommunication de l'entreprise.

. Elle assure la mise en place des moyens technologiques de l'information nécessaires pour supporter et améliorer l'activité, la stratégie et la performance de l'entreprise.

. Elle doit ainsi veiller à la cohérence des moyens informatiques et de communication mise à la disposition des utilisateurs, à leur mise à niveau, à leur maîtrise technique et à leur disponibilité et opérationnalité permanente et en toute sécurité.

. Elle définit également, dans le cadre des plans pluriannuels, les évolutions nécessaires en fonction des objectifs de l'entreprise et des nouvelles technologies.

1.2.4.2 Organigramme de DSI

DSI est un ensemble de département application Métiers, département information technologie, département transformation digitale et département système information. Chaque département a pour objectif d'améliorer le niveau de l'informatique et ces services pour garantir le développement et la progression des services du groupe Cevital [6].
La figure 1.5 illustre L'organigramme de la Direction des Systèmes d'Informations.

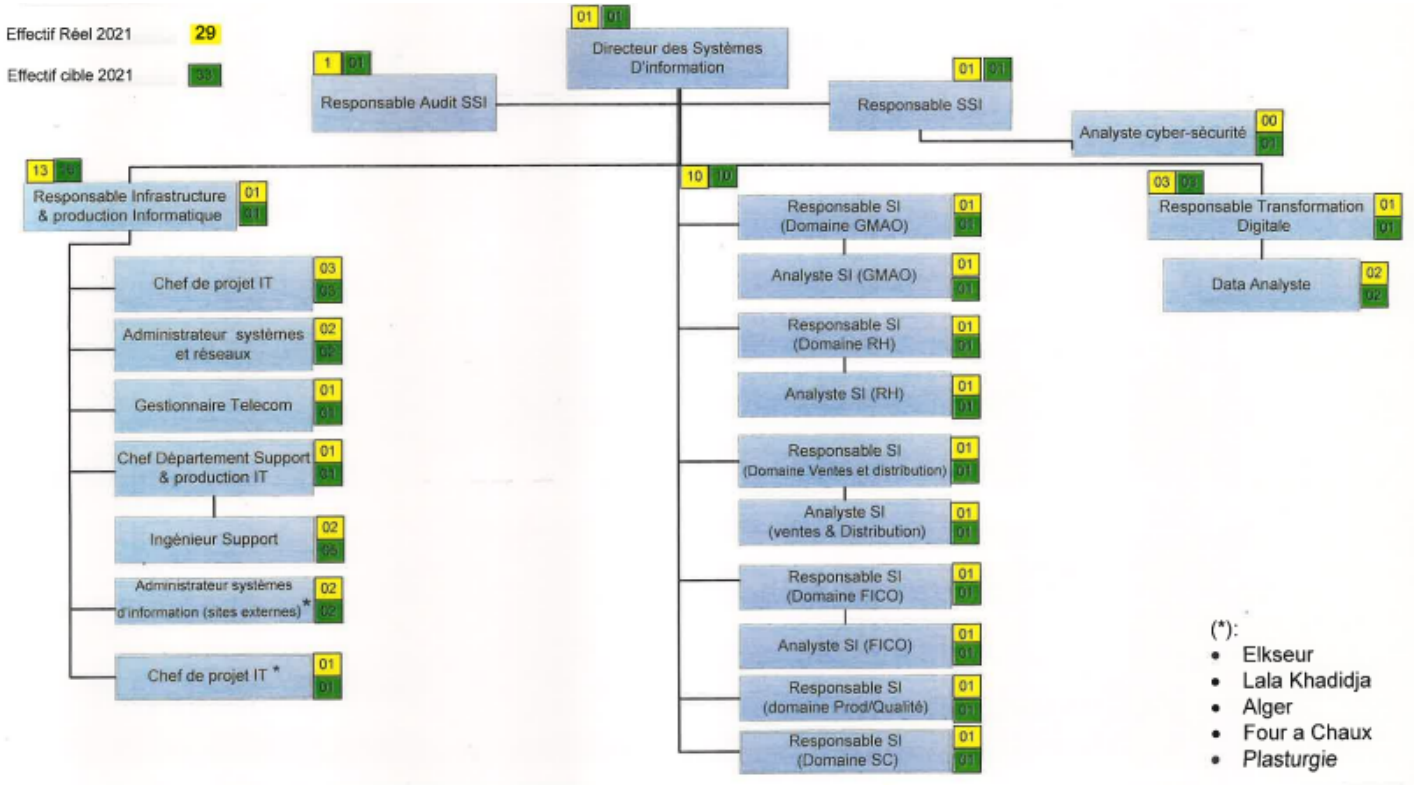

FIGURE 1.5 – Organigramme de la direction système d'information.

1.2.4.3 Utilisation du réseau informatique

Les différents collaborateurs (environ mille utilisateurs du réseau informatique) de CEVITAL utilisent chaque jour les différentes applications et services offerts par le réseau afin d'effectuer nombreuses opérations, comme le partage de ressources (logiciels, bases de données, imprimantes...) entre différents utilisateurs, indépendamment de leur localisation géographique, la communication entre les personnes distantes, garantir la sécurité des données et la recherche d'informations grâce à l'internet. Nous pouvons citer les applications et services suivants [3] :

- Applications de GPAO.
- Le partage de document via un serveur dédié (cloud privé).
- Microsoft Exchange et Azure.
- Service Mail.
- Application comptabilité et gestion des stocks.
- Accès internet pour le collaborateur.

1.2.4.4 Architecture du réseau Informatique de CEVITAL

Cevital dispose d'un réseau Interne assez vaste permettant de relier les différents bâtiments, unités de production et directions du complexe. Nous pouvons le décomposer en plusieurs parties : le backbone du réseau, un pare-feu, un DMZ, une couverture WIFI, un routeur, Switches et un datacenter (où sont placés les serveurs de l'entreprise). Le réseau est composé de plusieurs équipements qui pour la majorité sont de marque Cisco (Switch Catalyst, Routeur) interconnectés entre eux par fibre optique, ou cuivre, ainsi des équipements satellitaires VSAT pour établir la communication entre les différents sites interconnectés [7].

1.2.4.5 La sécurité informatique au niveau de CEVITAL

La politique de sécurité de CEVITAL repose sur deux parties : partie logique et partie physique [8].

— **Sécurité logique :** consiste à protéger le réseau contre les attaques de piratage et l'écoute clandestine. Elle se fait à l'aide de :

1. Pare-feu : Le pare-feu utilisé pour cette partie est un paloalto 3020 connecté à un commutateur de distribution Catalyst 4705R et à la DMZ de l'autre côté. Il est doté de fonctions unifiées de gestion des menaces : antivirus, antispam, système de prévention des intrusions et filtrage des contenus web. Les administrateurs réseau utilisent une politique de sécurité pour contrôler le trafic via ce pare-feu.
2. Serveur Proxy : C'est un serveur Microsoft qui se situe entre le pare-feu et le commutateur principal. Sa mission est de fournir une gestion simplifiée et c'est une passerelle Web sécurisée qui protège les employés lors de leur navigation sur Internet.
3. DMZ :(zone démilitarisée) : Une DMZ est mise en place pour permettre aux clients de se connecter au réseau à partir de sites externes. Il se compose d'un serveur FTP relié au pare-feu. Son rôle est d'identifier ceux qui souhaitent y accéder afin d'en restreindre l'accès en laissant un chemin sécurisé vers la base de données CEVITAL.

— **Sécurité physique :** consiste à :

1. Accès au local des équipements réseau : L'accès local aux équipements de technologie de réseau géré est protégé par un système de contrôle d'accès et accessible uniquement aux :
   — Instalateur, Agent de Maintenance.
   — Administrateur réseau.
   — Les personnes chargées de la sécurité du data center.
2. Détecteur d'incendie : pour éviter les dommages, un système de protection contre les incendies a été mis en place indépendamment de tous les autres systèmes.
3. Régulateurs de température et faux planchers : Le matériel et les composants électriques sont extrêmement sensibles à l'humidité. Pour cette raison, les ingénieurs de CEVITAL ont installé des régulateurs de température pour maintenir la température ambiante et des planchers surélevés pour prévenir les dégâts (inondations, ruptures de canalisations, etc.).
4. Onduleur : pour éviter les coupures de courant inattendues, tous les dispositifs du système d'information CEVITAL sont connectés à un circuit ondulé avec une disponibilité supérieure à 1/4 d'heure pour permettre une extension spécifique au système.

1.3 Critique de l'existant et problématique

Au cours de notre stage pratiqué mené à l'entreprise CEVITAL, une étude approfondie concernant la sécurité Informatique au sein de Cevital a été menée. Cette étude nous a permis de ressortir les problématiques liées à la sécurité Informatique de Cevital et les décisions à prendre pour le choix de la solution et son déploiement.

Dans cette partie, nous exposerons le contexte de notre projet, le problème et les solutions à mettre en œuvre qui s'adapte au fonctionnement de l'entreprise.

1.3.1 Contexte du projet

La sécurité des systèmes d'information est une problématique d'une importance majeure pour les individus ainsi que pour les entreprises. Elle protège l'information d'une multitude de vulnérabilités et menaces afin de garantir la continuité de l'organisme, restreindre les dommages et avoir le degré de protection désiré.

Après avoir vu les faiblesses et les améliorations dans le domaine de la sécurité Informatique, nous allons pouvoir passer à l'étude de l'accès distant sécurisé qui offre de nombreux avantages à une entreprise. Cela en déployant une passerelle de bureau à distance sécurisée**"GUACAMOLE"** qui répond aux problèmes de gestion des connexions à distance à partir d'un emplacement centralisé ainsi protéger les ressources d'une organisation et définir les privilèges d'accès des utilisateurs aux informations, ce qui rend le système plus sécurisé.

Bien que l'accès distant offre de nombreux avantages à l'entreprise, tout accès externe expose considérablement son réseau à des menaces de sécurité potentielles. Donc l'authentification à deux facteurs est devenue indispensable pour tous les réseaux qui prennent en charge l'accès distant.

1.3.2 Problématique

Aujourd'hui, la sécurité est un enjeu majeur pour les entreprises. Les menaces numériques ne cessent pas d'augmenter. Pour les contrer, il est primordial de recourir à des méthodes avancées d'authentification et de gestion d'accès à distance au lieu d'utiliser la gestion manuelle des terminaux.

CEVITAL possède une forte sécurité, mais il est important de noter que la sécurité est un processus continu et en constante évolution, les attaques évoluent constamment et les entreprises doivent continuellement renforcer leur sécurité pour se protéger contre ces menaces.

Au sein de l'entreprise CEVITAL, des projets de virtualisation de serveurs ont été mis en œuvre pour leur permettre de fournir un accès à des serveurs virtuels qui sont hébergés sur un serveur physique depuis n'importe quel endroit ou appareils disposant d'un navigateur web. En proposant ce projet d'amélioration de la sécurité de la passerelle de bureau à distance, nous pouvons aider à renforcer et protéger les données et les ressources de Cevital contre les différentes attaques et les tentatives d'accès non autorisées ainsi offrir des méthodes et des solutions de sécurisation de cette passerelle. De ce fait, quelles technologies pourrions-nous utiliser dans le souci de garantir une bonne sécurisation, une continuité des services et du fonctionnement optimal malgré la défaillance d'un ou plusieur élément matériel ou logiciel ?

1.3.3 Objectifs

Pour assurer le bon fonctionnement de l'accès à distance sécurisé, nous avons opté pour le déploiement une passerelle de bureau à distance open source appelée "Guacamole".

Il serait très utile et pratique d'avoir des solutions technologiques pour rendre le travail en entreprise plus conviviale, plus accessible et plus collaboratif. Ces techniques doivent être capables de :

- L'utilisation des bonnes méthodes de protection des terminaux, de l'authentification à deux facteurs (2FA) et des logiciels de sécurité contribuera largement à faire de l'accès à distance un moyen sûr de connecter deux appareils.
- Unifier les moyens d'accès à des applications développées.
- Faciliter le travail collaboratif.
- simplifier l'utilisation des techniques existants.

- Permettre le partage de ressources entre les services et personnes autorisées.

Donc afin de remédier au problème traité dans la problématique, nous avons choisi de mettre en place trois méthodes de sécurisation , deux basées sur une technologie d'authentification à deux facteurs, l'autre méthode c'est la réception des notifications par émail pour avertir les administrateurs lorsqu'un utilisateur se connecte et déconnecte ce qui permet de détecter toute activité suspecte. ce qui peut augmenter le niveau de sécurité et les capacités de détection.

1.4 Conclusion

CEVITAL se caractérise par des moyens efficaces et outils modernes tels que leurs logiciels, et ainsi d'un bon savoir faire, qui aide à mieux gérer les différentes fonctions de cette entreprise. Sa mission principale est le développement de sa production afin d'assurer la bonne qualité de ses différents produits et de satisfaire ses différents clients par la couverture du marché national.

Dans ce chapitre, nous avons présenté l'organisme d'accueil dans lequel nous avons effectué notre stage. Ensuite, nous avons éclairci notre thème en mettant en avant une problématique bien précise qui détermine les axes autour desquelles tournera notre travail, tout ce qui nous a conduits logiquement à la formulation des solutions quant à ce qui concerne notre thème.
Dans le chapitre suivant nous aborderons les différents aspects liés à la sécurité informatique et l'accès à distance sécurisé .

Chapitre 2

Pré-requis et méthodologies

2.1 Introduction

Dans nos jours, la sécurité informatique et l'accès distant sécurisé présentent un outil très important pour protéger le systéme d'information d'une organisation. Au long de ce chapitre nous allons introduire dans un premier temps des notions de base de la sécurité puis nous décrivons les différentes attaques menacant le système informatique ainsi que les techniques et méthodes de protection. Par la suite nous allons faire une étude sur l'accès distant sécurisé ainsi définir la passerelle de bureau à distance Guacamole, ses avantages et ses limites.

2.2 la sécurité Informatique

2.2.1 Définition

La notion de sécurité informatique couvre l'ensemble des moyens, outils, techniques et méthodes pour garantir que seules les personnes ou autres systèmes autorisés interviennent sur le système et ont accès aux données, sensibles ou non [9].On ce qui nous concerne, le point de départ de notre analyse sera le suivant : *"La sécurité est l'ensemble des mesures permettant d'assurer la protection des biens / valeurs".*

2.2.2 Importance de la sécurité Informatique

La sécurité Informatique est importante pour de nombreuses raisons. Elle permet de garantir la confidentialité des données ainsi de lutter contre les virus et les logiciels malveillants. Ces derniers peuvent en effet endommager les ordinateurs et les réseaux, et faire perdre des données importantes.
La sécurité Informatique est essentielle pour prévenir les attaques et les tentatives d'hameçonnage, le vol d'informations et des données confidentielles sur les différents appareils intelligents et ordinateurs ainsi pour prévenir les failles de sécurité.
Mettre en place une sécurité permet aux entreprises d'éviter les menaces et réaliser un gain énorme grâce à la proximité et à la rapidité de service ainsi la fiabilité et la stabilité qui met la clientèle et les collaborateurs en confiance lorsqu'ils font affaire avec l'entreprise [10].

2.2.3 La sécurité et les entreprises

De manière plus concrète, une entreprise parle de la sécurité pour [11] :

- **Protéger sa réputation :** le monde du piratage Informatique et de l'Internet en particulier fascine le public. C'est pourquoi, tout incident Informatique, qu'il s'agisse de transferts

illicites, de vols de numéros de cartes de crédit, d'espionnage, de fraudes internes, de déni de service ou tout simplement de maquillage de sites est susceptible de faire les gros titres des journaux locaux, nationaux ou mondiaux.

- **Assurer la continuité de ses activités :** aujourd'hui, la majorité des activités d'une organisation, quelle que soit sa taille, repose sur des processus Informatiques. En fonction de l'importance du processus touché et de la durée, une indisponibilité peut conduire à un arrêt d'activité temporaire, au chômage technique ou à la faillite.
- **Protéger ses données stratégiques et ses propriétés intellectuelles :** dans un contexte de concurrence universelle où la course aux marchés est toujours plus intense, où les valeurs se perdent, l'espionnage est un élément stratégique à ne pas négliger que l'on est du côté offensif ou défensif. Et, si les méthodes traditionnelles comme l'infiltration, la visite des locaux de jour comme de nuit, le vol de documents, l'analyses poubelles sont encore plus applicables aujourd'hui qu'elles ne l'étaient hier, la technologie offre de nouvelles perspectives d'évasion ou d'infiltration. Pour n'en citer que quelques-unes : les documents transportés sur les disques durs des portables, les stations de travail équipées de graveurs, le courriel externe, les serveurs et bases de données accessibles de l'extérieur.
- **Protéger les données privées de sa clientèle et de ses employés :** mis à part les obligations légales en la matière, chaque organisation a l'obligation morale de ne pas trahir la confiance que ses clients et employés lui ont accordée en mettant tout en œuvre pour protéger leurs données telles que coordonnées, numéros de cartes de crédit ou de comptes bancaires, données médicales, données juridiques, commandes exécutées, etc.
- **Se prémunir de la fraude :** la fraude, en particulier la fraude interne, est en croissance, et un inhibiteur de cette croissance est la technologie.
- **Satisfaire aux exigences légales :** le passé a prouvé à maintes reprises que les organisations « non sécurisées » représentent un danger pour elles-mêmes mais surtout pour les autres. Les États, les compagnies d'assurances, les compagnies de cartes de crédit l'ont bien compris et établissent pour ce faire une série de législations et de réglementations que les organisations sont priées de respecter si elles souhaitent s'épargner des procès ou pénalités.
- **Éviter des pertes financières :** les pertes financières directes résultent directement d'un crime informatique comme les transferts financiers illicites, les détournements. Quant aux pertes indirectes, elles résultent à court, moyen ou long terme de tous les points abordés plus haut.

2.2.4 Les services de sécurité :

Aujourd'hui dans un monde ultra-informatisé, les entités en communication peuvent se trouver à de grandes distances grâce notamment à Internet. Les réseaux utilisés pour connecter ces entités offrent des qualités de service variables en matière de rapidité, fiabilité et de confidentialité. En effet, les échanges d'information sont de plus en plus nombreux et importants, et la sécurité de ces échanges a pris une importance particulière [12].

Les principaux Services de Sécurité sont, à savoir [11] :

2.2.4.1 Confidentialité

Assure que l'information soit protégée contre toute divulgation accidentelle ou malveillante aux parties non autorisées.

2.2.4.2 Intégrité

Assure que l'information et les systèmes soient protégés contre toute modification ou destruction accidentelle ou malveillante.

2.2.4.3 Disponibilité

Assure que l'information et les systèmes soient accessibles et utilisables par les parties autorisées aux moments où elles en ont besoin.

En plus de ses caractéristiques de base, nous trouvons également les services suivants :

2.2.4.4 Authentification

Assure l'identification d'un individu, d'une entité mais également l'origine de l'information ou encore d'une opération effectuée sur celle-ci.

2.2.4.5 Autorisation

Assure le contrôle du type d'activités ou d'informations qu'une personne ou entité est autorisée à effectuer ou accéder.

2.2.4.6 Non-répudiation

Assure le fait qu'une personne ou entité ne puisse nier avoir effectué une activité. Dans le domaine du courriel, la non-répudiation est utilisée pour garantir que le destinataire ne pourra nier avoir reçu l'information, et assurer que l'expéditeur de l'information ne peut nier avoir envoyé l'information.

2.2.4.7 Journalisation

Assure que tout accès à un système, tout accès à une information ainsi que toute opération exercée sur ceux-ci soit journalisée (répertoriée).

2.3 L'importance de sécuriser les réseaux

Le moyen le plus efficace d'assurer la sécurité d'un système Informatique est de déterminer la nature des problèmes de sécurité et de prendre les mesures qui s'imposent.

2.3.1 Menaces

2.3.1.1 Définition

De manière générale, une menace peut se définir comme étant l'action ou l'événement pouvant porter préjudice à ce que l'on désire protéger. Dans le domaine Informatique, la menace peut se traduire comme étant l'action ou l'événement dont le déclenchement pourrait porter atteinte à l'une, voire à plusieurs, des caractéristiques critiques de l'information et des systèmes qui la traitent et la maintiennent, à savoir, la confidentialité, l'intégrité et la disponibilité.

Les effets des différentes menaces varient considérablement suivant les conséquences affectant l'entreprise, certaines affectent la confidentialité ou l'intégrité des données, d'autres agissent sur la disponibilité des systèmes.

2.3.1.2 les types de menaces

Les menaces les plus courantes peuvent être résumées de la façon suivante [13] :

- **Erreurs et omissions :** ce sont des menaces importantes pour l'intégrité des données et des Systèmes. Ces erreurs ont souvent une origine *humaine*. En effet, même les programmes les plus sophistiqués ne peuvent pas tout détecter. N'importe quelle personne intervenant sur le système d'information (utilisateur, administrateur système, développeur...) contribue directement ou indirectement à ces dangers mettant en péril la sécurité des systèmes. Souvent l'erreur concerne une menace (erreur d'entrée de données, erreur déprogrammation...) ou encore crée elle-même la vulnérabilité.
- **Les fraudes et vols :**peuvent être commis par l'intérieur ou l'extérieur de l'entreprise. Par expérience, il s'avère, la plupart du temps, que la menace vient de l'intérieur (des utilisateurs ayant des accès privilégiés aux systèmes). En effet, par défaut, ce sont les utilisateurs familiers de l'entreprise qui sont dans la meilleure position pour commettre des forfaits.
- **Sabotage causé par des employés :**ce sont les personnels les plus familiarisés avec les systèmes et les applications. Ils peuvent donner à perpétrer des dommages, sabotages. Ce qui implique la nécessité de gérer et de contrôler de façon rigoureuse les comptes des utilisateurs, surtout de ceux qui ont des accès privilégiés aux systèmes ;
- **Les Hackers :**le terme *hacker* ou encore *cracker* fait référence à la personne qui s'introduit dans les systèmes d'informations sans autorisation pour, dans le pire des cas, provoquer des dégradations dans les données ou les applications. Ses actions peuvent s'effectuer à partir de l'intérieur (dans le cas où il a pu obtenir un accès sur le réseau) ou de l'extérieur de l'entreprise. Toutefois, il n'est pas toujours facile de détecter sa présence sur les systèmes ni de connaître ce qu'il a provoqué comme dégâts.

2.3.2 Les vulnérabilités

2.3.2.1 Définition

Ce sont les failles de sécurité dans un ou plusieurs systèmes. Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non.
Une faille de sécurité ou vulnérabilité, désigne en informatique toute faiblesse d'un système se traduisant par une incapacité partielle de celui-ci à faire face aux attaques ou aux intrusions informatiques. Elle permet à une personne potentiellement malveillante d'altérer le fonctionnement normal du système ou encore d'accéder à des données non autorisées.

2.3.2.2 Type de vulnérabilité

Pour le domaine de la sécurité informatique, Il existe trois familles de vulnérabilités [13] :

- **Vulnérabilités liées aux domaines physiques**

- Manque de redondance et de ressource au niveau équipement.
- Accès aux salles informatiques non sécurisé.
- Absence ou mauvaise stratégie de sauvegarde des données.

- **Vulnérabilités liées aux domaines organisationnels**

- Manque de ressources humaines et de personnels qualifiés, communications.
- Absence de contrôles périodiques, documents de procédures adaptés à l'entreprise.

- Moyens adaptés aux risques encourus.
- Trop grande complexité fonctionnelle.

- **Vulnérabilités liées aux domaines technologiques**

- Failles nombreuses dans les services et applicatifs Web et les bases de données.
- Pas de mises à jour des systèmes d'exploitation et des correctifs.
- Pas de contrôle suffisant sur les logiciels malveillants.
- Récurrence des failles et absence de supervision des évènements.
- Réseaux complexes, non protégés.
- Mauvaise utilisation de la messagerie.

2.3.3 Les risques dans un système informatique

2.3.3.1 Définition formelle des risques

Selon Nichan Margossian, le risque peut être défini comme l'éventualité d'un événement futur, susceptible de causer généralement un dommage, une altération. C'est donc la probabilité de l'existence d'une situation dangereuse pouvant conduire à un événement grave, par exemple un accident ou une maladie. Dans le mot risque, il y a toujours la notion de probabilité, plus celle-ci est grande, plus le risque est important et plus l'événement dangereux pourrait être imminent et grave [14].

Prenons un autre exemple tiré de la vie courante. En conduisant trop vite sur une route de montagne, on risque d'occasionner une sortie de route, qui entraînerait des dégâts matériels ou humains plus ou moins importants. L'événement craint serait la sortie de route, résultat d'une vitesse excessive. Ces deux points forment un scénario, c'est-à-dire une suite de causes nécessaires à la survenue de l'accident. La probabilité d'occurrence sera fonction de la vitesse de la conduite, de l'état de la route ou des conditions météorologiques, de la circulation, etc. La cible sera la voiture et les personnes à bord, ainsi que tout élément extérieur impliqué dans l'accident (mobilier, passants, etc.). Enfin, l'impact sera le résultat des dégâts occasionnés, pouvant être légers (quelques éraflures sur la carrosserie) à majeurs (le décès ou l'hospitalisation d'une personne).

Il est ainsi possible de représenter le risque par ces quatre facteurs (voir la figure 2.1) : la cause ou le scénario, la probabilité d'occurrence, la cible, et l'impact [15].

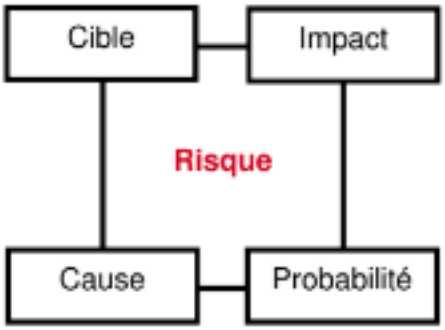

FIGURE 2.1 – Risque [15].

2.3.4 Les attaques

2.3.4.1 Définition

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.
Une **«attaque »** est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du systèmes et généralement préjudiciables.

2.3.4.2 Les motivation des attaques

- obtenir un accès au système.
- voler des informations.
- récupérer des données bancaires.
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.)
- troubler le bon fonctionnement d'un service.

2.3.4.3 Les techniques d'attaques

Dans cette section, nous nous pencherons sur les différents types d'attaques [16].

1. **Les attaques directes :** le hacker attaque directement sa victime à partir de son ordinateur. Voir La figure 2.2.

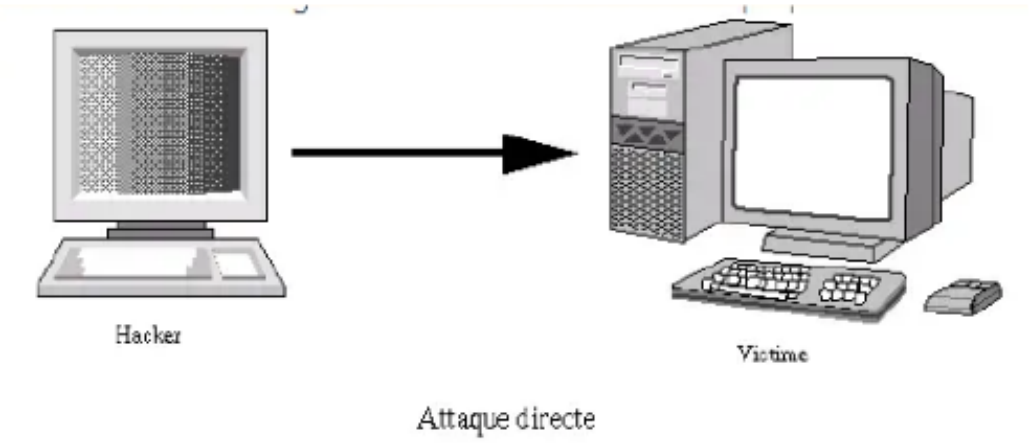

FIGURE 2.2 – Attaque directe [16].

2. **Les attaques indirectes par rebond :** Cette attaque est hautement appréciée par les pirates. En effet, le rebond a deux avantages :
   — Masquer l'identité (l'adresse IP) du hacker.
   — Éventuellement, utiliser les ressources del'ordinateur intermédiaire car il est plus puissant (CPU, bande passante...) pour attaquer. Voir la figure 2.3

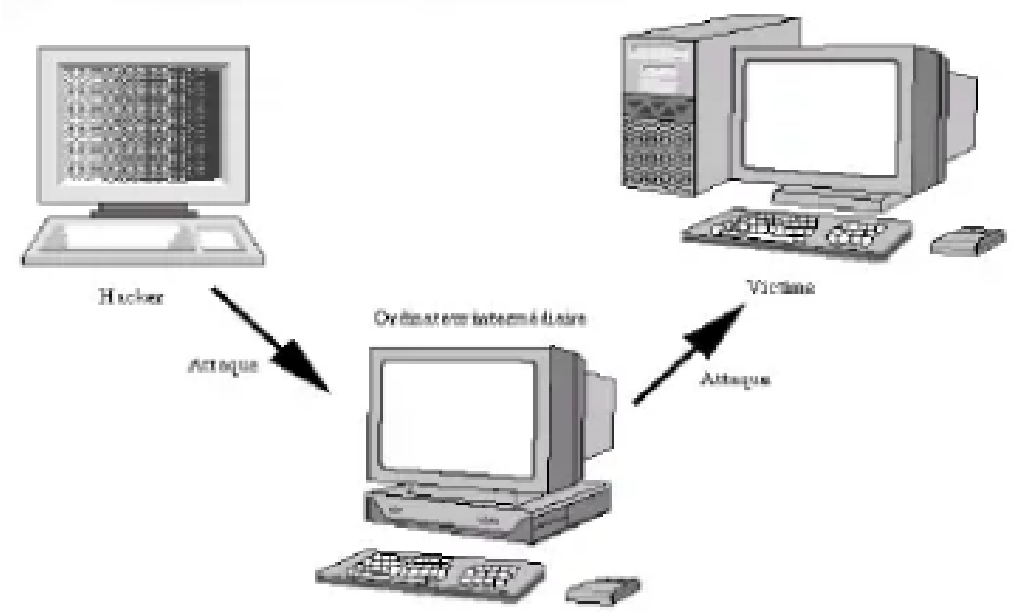

FIGURE 2.3 – Les attaque indirectes par rebond [16].

3. **Les attaques indirectes par réponse :** Au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. C'est cette réponse à la requête qui va être envoyée à l'ordinateur victime (voir la figure 2.4).

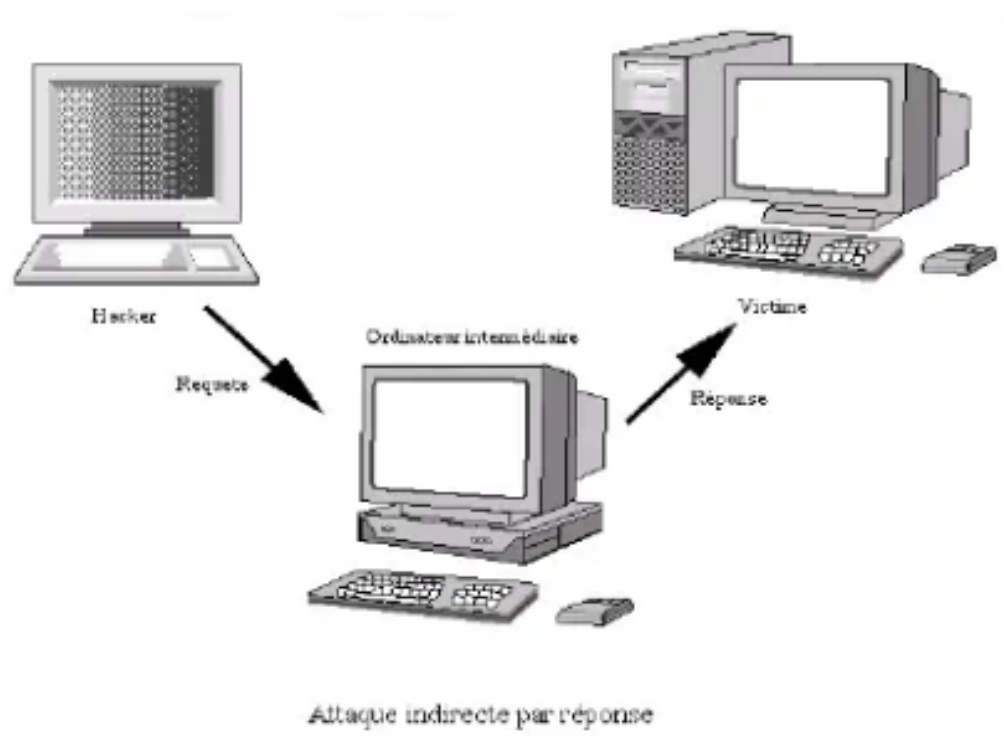

FIGURE 2.4 – Les attaques indirectes par réponse [16].

2.3.4.4 Types d'attaques et comment se protéger

Les différents types d'attaques possibles peuvent se résumer comme suit [16] :

— **Denial of Service :** Une attaque par déni de service est une attaque qui a pour but de mettre hors-jeu le système qui est visé. Ainsi, la victime se voit dans l'incapacité d'accéder à son réseau. Ce type d'attaque peut aussi bien être utilisé contre un serveur d'entreprise qu'un particulier relié à internet.
Comment s'en protéger ? Être à jour dans les correctifs logiciels (Patch).

— **Sniffing :** le reniflage (Sniffing) est une technique qui consiste à analyser le trafic réseau. Lorsque deux ordinateurs communiquent entre eux, il y a un échange d'informations (trafic). Mais, il est toujours possible qu'une personne malveillante récupère ce trafic. Elle peut alors l'analyser et y trouver des informations sensibles.
Comment s'en protéger ?
Utiliser de préférence un switch (commutateur) plutôt qu'un hub, Utiliser des protocoles chiffrés pour les informations sensibles comme les mots de passe, Utiliser un détecteur de sniffer.

— **Balayage des ports :** le scanning consiste à balayer tous les ports sur une machine en utilisant un outil appelé scanner. Le scanner envoie des paquets sur plusieurs ports de la machine. En fonction de leurs réactions, le scanner va en déduire si les ports sont ouverts.
Comment s'en protéger ? Scanner sa machine pour connaître les ports ouverts surveiller les ports ouverts avec un firewall et fermer ceux qui ne sont pas utiles Utiliser un IDS (détecteur d'intrusion) ou mieux un IPS (prévention d'intrusion).

— **Le Pishing :** le social engineering est l'art de manipuler les personnes. Il s'agit ainsi d'une technique permettant d'obtenir des informations d'une personne, qu'elle ne devrait pas donner en temps normal, en lui donnant des bonnes raisons de le faire.

— **Attaque par force brute :** le crackage des mots de passe consiste à deviner le mot de passe de la victime.
Comment s'en protéger ?
Choisir un mot de passe robuste.
Changer régulièrement de mot de passe pour éviter que ce dernier ne soit trouvé par un tel outil.

— **L'usurpation d'adresse IP (IP Spoofing) :** est une technique consistant à remplacer l'adresse IP de l'expéditeur IP par l'adresse IP d'une autre machine ;
Comment s'en protéger ?
On ne peut pas empêcher quelqu'un d'usurper une identité. En revanche, il faut à tout prix être sûr de l'identité de la machine avec laquelle on dialogue.
Utiliser des protocoles sécurisés comme ssh qui empêche le spoofing.

— **Man in the Middle :** Man in the Middle signifie l'homme du milieu. Cette attaque a pour but de s'insérer entre deux ordinateurs qui communiquent. Soient deux ordinateurs A et B voulant dialoguer. Maintenant, si un pirate décide de se faire passer pour l'ordinateur A auprès de B et de B auprès d'A, ainsi, toute communication vers A ou B passera par le pirate, l'homme au milieu.

— **- Le Smurf :** ce procédé est décomposé en deux étapes : La première est de récupérer l'adresse IP de la cible par spoofing, la seconde est d'envoyer un flux maximal de paquets ICMP ECHO(ping) aux adresses de Broadcast. Chaque ping comportant l'adresse spoofée de l'ordinateur cible. Si le routeur permet cela, il va transmettre le broadcast à tous lesordinateurs du réseau, qui vont répondre à l'ordinateur cible. La ciblerecevra donc un maximum de réponses au ping, saturant totalement sa bande passante.
Comment s'en protéger ? Configurer le firewall pour filtrer les paquets ICMP écho ou les limiter à un pourcentage de la bande passante. Configurer le routeur pour désactiver le broadcast.

2.3.4.5 Conséquences pour les entreprises

Les impacts d'une cyberattaque se situent à de multiples niveaux. Et les entreprises qui en sont victimes ne parviennent pas toujours à préserver leur activité. Les failles de sécurité mettent en péril les entreprises qui n'ont pas pris les devants :

- **des finances mises à mal :** extorsion de fonds, rançons, baisse de chiffre d'affaires et du cours en bourse.
- **une image de marque et une confiance dégradées :** vis-à-vis des clients, des actionnaires, des partenaires, des collaborateurs ou de l'opinion publique.
- **une organisation déstabilisée :** impossibilité de poursuivre l'exploitation suite au piratage d'un système d'informations ou d'un réseau d'énergie.
- **des informations confidentielles livrées à la concurrence ou revendues :** données, secrets de fabrication, procédés scientifiques ou industriels.

Selon une étude HTTPCS/Celsy, 60% des entreprises qui sont victimes d'une cyberattaque ne réussissent pas à maintenir leur activité.

2.4 Mécanismes de la défense

Un mécanisme de sécurité, est un ensemble de stratégies conçu pour détecter, prévenir et lutter contre une attaque de sécurité [16]. Avec l'évolution des systèmes et des réseaux, il existe une panoplie de mécanismes de sécurité servant à protéger les systèmes ainsi que les services qu'ils offrent. Nous abordons dans ce qui suit, les principaux mécanismes utilisés :

2.4.1 Audit de sécurité

L'audit de sécurité d'un réseau offre une image complète du réseau sous forme d'un rapport détaillé qui donne un aperçu instantané et en temps réel du statut du réseau. Une analyse peut être faite sur le résultat du balayage en utilisant des filtres dans les rapports, ce qui permet de sécuriser le réseau de manière proactive, par exemple, en fermant les ports ouverts, en supprimant les comptes utilisateurs qui ne sont plus utilisés ou en désactivant les points d'accès sans fil. En termes de sécurité, il permet d'identifier des points de vulnérabilité du réseau, cependant, il ne permet pas de détecter les attaques qu'a déjà subie le réseau ou que subira dans le futur.

2.4.2 Journalisation

La journalisation consiste à enregistrer les activités et les connexions de chaque acteur utilisant un réseau. En effet, les journaux d'évènements (logs) constituent une brique technique indispensable à la gestion de la sécurité des réseaux et plus généralement des systèmes. En effet, les journaux sont une source d'information riche permettant de constater si des attaques ont eu lieu, de les analyser et potentiellement de faire en sorte qu'elles ne se reproduisent pas.

Dans ce cas, les évènements constituant les journaux sont consultés et analysés en temps réel. Les journaux peuvent également être employés a posteriori pour retrouver les traces d'un incident de sécurité, l'analyse des journaux d'un ensemble de composants (postes de travail, équipements réseaux, serveurs, etc.) peut alors permettre de comprendre le cheminement d'une attaque et d'évaluer son impact

2.4.3 Antivirus

Un antivirus est un logiciel permettant de protéger une machine contre les programmes/logiciels néfastes ou les fichiers potentiellement exécutables. De nos jours, les antivirus sont aussi des anti-malwares c'est-à-dire ils protègent aussi les machines contre tous les autres types de malwares à savoir les vers et les chevaux de Troie. Il consiste à chercher les codes malveillants dans les logiciels infectés. Cependant, un antivirus ne protège pas le réseau contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime accédant à une ressource alors qu'il n'est pas autorisé à le faire.

2.4.4 Systèmes de détection d'intrusion

Un système de détection d'intrusions (ou IDS) est un appareil ou une application qui alerte l'administrateur en cas de faille ou de violation de règles de sécurité dans un réseau, permettant ainsi de prévenir les risques d'intrusion. Ce système consiste à surveiller et analyser les activités d'un réseau en repérant celles qui sont anormales ou suspectes, cependant, il ne permet pas de détecter les accès incorrects mais autorisés par un utilisateur légitime. Par ailleurs, certaines mauvaises détections peuvent arriver tels que les taux de faux positifs et les taux de faux négatifs.

2.4.5 Pare-feu

Un pare-feu (ou Firewall en anglais) est un système logiciel ou matériel installé sur une machine ou un routeur, permettant de contrôler les communications qui traversent un réseau donné. Ce mécanisme permet de protéger un réseau privé de certaines intrusions provenant d'un réseau externe (par exemple internet), telles que les communications sortantes déclenchées par un malware installé. Par ailleurs, il a pour fonction de faire respecter la politique de sécurité du réseau, qui définit quelles sont les communications autorisées ou interdites.

Concrètement, il s'agit d'une passerelle qui consiste à filtrer les paquets entrants et sortants en se basant sur une interface pour le réseau à protéger, et une autre pour le réseau externe (souvent c'est internet)

2.4.6 Contrôle d'accès

Le mécanisme du contrôle d'accès au réseau (NAC 2) permet de renforcer sa sécurité en limitant les ressources réseau accessible aux terminaux selon une stratégie de sécurité définie. En effet, il permet de vérifier les droits d'accès aux données d'un utilisateur, toutefois, il n'empêche pas l'exploitation d'une vulnérabilité par un assaillant. Le NAC convient particulièrement aux grands organismes et entreprises qui exercent un contrôle strict sur leur réseau. Les solutions existantes possibles pour gérer les accès autorisés sont l'utilisation des VPN ou des tunnels.

2.4.7 Authentification réseau

L'authentification réseau permet d'authentifier une machine quand elle essaie de se connecter sur le réseau et savoir avec précision si elle est déjà connectée en lui donnant les autorisations nécessaires pour l'usage du réseau. L'authentification réseau est nécessaire au bon fonctionnement des autres mécanismes de défense, et elle est indépendante des autres méthodes d'authentifications vers les systèmes d'exploitation ou les applications.

Il existe deux catégories de protocoles qui peuvent être utilisées pour l'authentification réseau, il y a d'une part, les protocoles propriétaires comme VMPS de Cisco Authentification

qui est seulement valable sur une adresse MAC et réseau filaire. et d'autre part, il y a les protocoles ouverts comme RADIUS et 802.1x authentification sur adresse MAC [17].

2.4.8 Bourrage de trafic

Le bourrage de trafic est destiné à protéger un réseau contre les attaques passives qui consistent à capturer et à analyser le trafic circulant dans le réseau. Ce mécanisme consiste à injecter des messages inutiles pour faire échouer les tentatives d'analyse du trafic. Cette pratique permet d'améliorer la confidentialité des données, notamment au niveau du volume du trafic.

2.4.9 Chiffrement des données

Le chiffrement consiste à transformer un message en clair en un message incompréhensible, en utilisant généralement un algorithme basé sur des clés. Essentiellement, deux techniques de cryptographie sont utilisées :

(1) Le chiffrement symétrique qui consiste à utiliser la même clé dite secrète pour chiffrer et déchiffrer un message, tandis que

(2) le chiffrement asymétrique qui se base sur une paire de clés, c'est-à-dire une clé publique pour le chiffrement du message, et une clé privée pour le déchiffrer, sachant que seul le destinataire du message qui possède la clé privée lui permettant de déchiffrer le message.

2.4.10 Signature numérique

La signature numérique est un mécanisme permettant de garantir l'intégrité et la non-répudiation d'un message ou d'un document électronique. Analogiquement a la signature manuscrite d'un document papier, la signature numérique permet d'authentifier un document ou un contrat électronique.

2.4.11 Protection physique

La protection physique d'un réseau consiste à rendre inaccessibles tous ses équipements, pour fournir une protection totale, mais qui peut être excessive, car le réseau n'aura aucun accès de l'extérieur. Par exemple, le fait d'isoler complètement le réseau d'un organisme sensible tel qu'une centrale nucléaire, toutefois, cette solution peut paraître trop radicale dans le cas des entreprises.

2.4.12 Protocoles de Sécurité

2.4.12.1 SSL/TLS

Ils sont tous les deux des protocoles situés entre le niveau transport et Application.
SSL et TLS se comportent en effet comme une couche intermédiaire supplémentaire, car ils sont indépendants du protocole utilisé au niveau application. Cela signifie donc qu'il peut aussi bien être employé pour sécuriser une transaction web, l'envoi ou la réception d'email, etc. SSL et TLS sont donc transparents pour l'utilisateur et ne nécessitent pas l'emploi de protocoles de niveau Application spécifiques [18].

2.4.12.2 IP Sec

IPsec est un protocole qui regroupe une suite de sous protocoles utilisant des algorithmes et des services cryptographiques permettant le transport de données sécurisées sur un réseau

IP. présente le gros avantage de permettre la gestion des dispositifs de sécurité sans aucune modification sur les ordinateurs des utilisateurs. IPsec fournit deux types de service de sécurité : Authentication Header **(AH)**, qui permet essentiellement l'authentification de l'expéditeur des données, et Encapsulating Security Payload **(ESP)**, qui prend en charge à la fois l'authentification de l'expéditeur et le chiffrement des données [22].

2.4.12.3 HTTPs

- **HTTPS connexions chiffrées**
  Est une extension de HTTP. Le « S » à la fin est l'initiale du mot « Secure » (sécurisé) et il fonctionne grâce au protocole TLS (Transport layer Security), le successeur du protocole SSL (Secure Sockets Layer), la technique de sécurité standard pour établir une connexion chiffrée entre un serveur web et un navigateur. Sans la présence de HTTPS, toutes les données que vous entrez sur un site seront envoyées en format de texte brute et seront, par conséquent, vulnérables aux interceptions et à l'espionnage. C'est pour cette raison que vous devriez toujours vérifier qu'un site utilise bien HTTPS avant d'y entrer quelques données que ce soit [23].

2.4.12.4 Protocoles FTPS versus SFTP

Afin de protéger les transferts de fichiers de ces menaces, des protocoles sécurisés ont été développés. Actuellement, deux de ces protocoles sécurisés sont largement utilisés : FTPS et SFTP.
La différence entre les deux protocoles est le fait que FTPS est basé sur le tunnel SSL/TLS (permet de sécuriser les connexions FTP en utilisant des certificats SSL, tout en authentifiant l'utilisateur), alors que SFTP tire sa sécurité de SSH (est un protocole qui permet de transférer et gérer des fichiers au-dessus d'une connexion sécurisée SSH à travers son port 22, en prenant en charge les fonctionnalités d'authentification de SSH) [24].

2.4.13 Protocoles de bureau à distance

2.4.13.1 RDP

une norme technique, permettant d'utiliser un ordinateur de bureau à distance. L'un des avantages est qu'il ne nécessite pas de VPN. Il conserve également les données stockées en toute sécurité sur le bureau de l'utilisateur, au lieu de les stocker sur des serveurs cloud ou sur les appareils personnels non sécurisés de l'utilisateur. En outre, le RDP permet aux entreprises disposant d'une infrastructure informatique sur site de permettre à leurs employés de travailler à domicile [19].

2.4.13.2 TELNET/SSH

- **TELNET**
  Est un protocole client-serveur basé sur l'échange de données via des connexions TCP. Le protocole permet le contrôle d'ordinateurs à distance grâce à des entrées et sorties textuelles [20].
- **SSH**
  Est un protocole d'administration à distance qui permet aux utilisateurs de contrôler et de modifier leurs serveurs distants sur Internet. Le service a été créé en tant que remplacement sécurisé pour le Telnet non chiffré, et utilise des techniques cryptographiques pour s'assurer que toutes les communications vers et depuis le serveur distant se produisent de

manière chiffrée. Il fournit un mécanisme pour authentifier un utilisateur distant, transférer les entrées du client vers l'hôte et relayer la sortie vers le client [21].

2.5 Étude sur l'accès à distance dans le domaine informatique

L'accès à distance a évolué conjointement avec les avancées technologiques, permettant de profiter de taux de transfert de plus en plus rapide, d'ailleurs de nos jours, nous pouvons trouver toute une série de solutions d'accès à distance avec différents degrés de sécurité.

Au moment où l'accès à distance a été introduit, il a annoncé l'arrivée d'une nouvelle forme d'organisation du travail : le télétravail. Grâce à l'accès distant nous pouvons accéder à des documents qui ne sont pas physiquement accessibles, il est même parfois possible de prendre carrément le contrôle de l'ordinateur distant et permettre aux techniciens de dépanner des systèmes informatiques sans se rendre sur place, etc [25].

2.5.1 Définition de l'accès a distance

L'accès à distance est une méthode qui permet aux utilisateurs d'accéder à un appareil ou à un réseau et de se connecter à des services, des applications ou des données informatiques depuis n'importe quel endroit. Cette connexion permet aux utilisateurs d'accéder à un réseau ou à un ordinateur à distance via l'internet, une connexion réseau ou d'autres moyens [26].

2.5.2 Définition de l'accès a distance sécurisé

L'accès distant sécurisé est une combinaison de processus ou de solutions de sécurité conçue pour bloquer l'accès non autorisé aux ressources numériques d'une entreprise et empêcher la perte de données sensibles. Il peut englober, entre autres, un certain nombre de méthodologies telles que le VPN, l'authentification multifacteur et la protection des terminaux [27].

2.5.3 Fonctionnement de l'accès a distance sécurisé

Chaque solution d'accès à distance est différente, mais en général, toutes fonctionnent de manière similaire [27].

- **Protéger les terminaux de tous les utilisateurs distants :**
  La sécurisation des terminaux dans un data Center est beaucoup plus facile par rapport à celle des terminaux des utilisateurs distants qui utilisent fréquemment plusieurs appareils. Un logiciel antivirus doit être installé sur tous les terminaux : PC, Mac, du type Linux, iOS ou Android. Les politiques de sécurité doivent exiger que tous les employés maintiennent le niveau de protection en vigueur s'ils doivent accéder aux ressources de l'entreprise.
- **Empêcher l'accès à distance d'augmenter la surface d'attaque :**
  La mise en place de l'accès distant peut présenter des risques pour l'entreprise. Plus précisément, les attaques de rançongiciel analysent souvent les serveurs RDP (Remote Desktop Protocol) et accèdent à partir de n'importe quel port disponible. De même, il faut éviter d'ouvrir les ports d'accès à distance à moins que les pare-feu ne soient configurés pour répondre uniquement aux adresses IP connues des administrateurs système.
- **Adopter l'authentification multifacteur :**
  L'authentification à deux facteurs (2FA) exige que les utilisateurs fournissent des moyens d'identification qui peuvent être générés par un terminal ou à partir d'une application pour

smartphone tel que DUO, Google Authenticator, FreeOTP afin d'accéder aux ressources de l'entreprise.

- **Utiliser des réseaux privés virtuels (VPN) :**
  De nombreux utilisateurs distants voudront se connecter à partir d'un réseau Wi-Fi non sécurisé ou utiliser d'autres connexions réseau non fiables. Le VPN peut éliminer ce risque, mais le logiciel de terminal VPN doit également être mis à jour pour éviter les vulnérabilités pouvant résulter d'anciennes versions du client logiciel.
- **Normaliser les journaux et assurer le suivi des informations de sécurité :**
  Les outils de gestion des informations et des événements de sécurité (SIEM) existants qui enregistrent le trafic des terminaux clients peuvent soudainement considérer les utilisateurs connectant à partir de leurs adresses IP personnelles comme une anomalie ; par conséquent, des ajustements peuvent donc être nécessaires à la fois au niveau de l'outil SIEM et des fonctionnalités de géolocalisation ou de géoblocage dans les pare-feu pour permettre aux collaborateurs de se connecter à partir de n'importe quel endroit.
- **Former les utilisateurs et les sous-traitants :**
  Avec l'apparition de nouvelles cyber menaces et attaques d'hameçonnage qui prétendent être liés au virus. Dans le cadre de leurs formations à la sécurité et à la conformité, il convient de rappeler à tous les collaborateurs et autres personnes accédant aux ressources de l'entreprise de ne pas cliquer sur les e-mails non sollicités ou sur les liens qu'ils contiennent.
- **Mettre à jour les politiques pour le personnel distant :**
  Il faut bien vérifier que les politiques d'utilisation acceptables couvrent les actifs informatiques personnels des collaborateurs (ordinateurs, ordinateurs portables, tablettes et smartphones, y compris la mise à jour des logiciels antivirus et VPN qui peuvent être installés sur les appareils leurs appartenant.

2.5.4 Utilisation de l'accès distance

Les entreprises peuvent utiliser l'accès à distance pour accomplir de nombreuses tâches [28] :

- **Visionneuse de bureau en direct :** pour les techniciens du service d'assistance technique, il est crucial de voir ce que l'utilisateur voit sur l'ordinateur distant pour accélérer la résolution des problèmes.
- **Utilitaire de transfert de fichiers :** Copier des fichiers sur l'ordinateur distant et transférer des fichiers depuis l'appareil distant.
- **Automatisation des accès et des processus :** un logiciel d'accès à distance incluant l'automatisation des processus permet de rédiger des scripts de tâches répétitives et de réparer en masse une série d'ordinateurs distants.
- **Contrôle des privilèges d'accès :** établir des droits d'accès aux appareils pris en charge sans qu'un utilisateur sur le site distant n'accorde une autorisation à chaque fois.
- **Sécurité de la connexion :** la sécurité de la session est essentielle pour éviter le piratage par des individus malveillants, car la plupart des connexions à distance s'effectuent à travers des canaux publics sur internet.
- **Journalisation de session :** captures d'écran et fonctionnalités associées. Toutes les actions effectuées sur l'ordinateur distant doivent être enregistrées. Il s'agit d'une mesure de sécurité importante pour se prémunir contre les actions malveillantes et montrer aux utilisateurs l'ensemble des tâches qui ont été réalisé sur le terminal distant.

- La possibilité de pouvoir accéder à plusieurs terminaux et ouvrir plusieurs sessions sur le même terminal.
- Disposer d'un canal de communication intégré permettant au technicien de communiquer avec l'utilisateur final. Il peut s'agir d'un système de chat textuel ou d'un canal de communication vocale ;
- Accès depuis des appareils mobiles afin de maintenir les charges de travail.
- Acheminer le trafic réseau entre les sous-réseaux d'un réseau local (LAN).

2.5.5 Passerelle de bureau à distance

Avec l'apparition incessante de nouvelles menaces et vulnérabilités, il est peut-être difficile d'accéder et de contrôler en toute sécurité tous les terminaux de notre entreprise, mais les solutions d'accès à distance sécurisé simplifient et fluidifient ce processus. Ces dernières consistent en des outils et des logiciels utilisés pour permettre l'accès aux ordinateurs et aux appareils à n'importe quel lieu.

2.5.5.1 Guacamole

Guacamole est une passerelle de bureau à distance open source et sans client qui permet d'accéder à des ordinateurs distants à partir de différents systèmes d'exploitation via un navigateur Web à l'aide de divers protocoles de bureau à distance tels que RDP, SSH, VNC.

L'application web *Guacamole* est apparue pour la première fois en 2011, elle est souvent utilisé avec le serveur web Apache, où Apache agit en tant que serveur proxy pour Guacamole. Avec guacamole, il est possible de gérer plusieurs utilisateurs et connexions, de les regrouper dans des groupes, de configurer des contraintes d'accès (horaire, nombre de connexion, ...) et d'enregistrer les sessions en vidéo.

2.5.5.2 Avantages d'utiliser du guacamole

Parmi les différents avantages de Guacamole, on peut citer [29] :

- Pas d'installation nécessaire sur les postes clients.
- Virtualisation des postes de travail .
- Sauvegarde de la machine virtuelle via des snapshots.
- Données sécurisées et accessibles à tout moment.
- Maintenance simplifiée.
- Sensibilisation aux problèmes de sécurité (Il prend en charge des protocoles de chiffrement tels que SSL/TLS et inclut l'authentification à 2FA).
- Gestion centralisée des connexions à distance.
- Accès à distance simplifié (accès aux équipements distant via un navigateur web).

2.5.5.3 Limites et éventuelles contraintes de guacamole

- **Performance :** La performance de guacamole dépend de plusieurs facteurs, notamment la puissance du serveur Guacamole, la bande passante réseau disponible et la charge du serveur distant. Si la bande passante réseau est limitée, cela peut entraîner des délais et des ralentissements dans l'affichage des sessions à distance.
- **Prise en charge des protocoles :** Guacamole prend en charge plusieurs protocoles de bureau à distance mais il peut ne pas prendre en charge certains protocoles propriétaires ou spécialisés, ce qui limite son utilisation dans certains environnements spécifiques.

- **Dépendance à un navigateur web :** Guacamole repose entièrement sur les navigateurs web pour fournir l'interface utilisateur et l'accès à distance. Par conséquent, certaines fonctionnalités avancées, telles que l'accélération matérielle, peuvent être limitées dans un environnement de navigateur.

2.6 Splashtop vs Apache Guacamole

Dans ce qui suit nous allons effectuer une analyse comparative entre Splashtop et Apache Guacamole.

1 **Accès à distance et capacités de soutien à distance :** Splashtop est une solution offrant un accès à distance aux ordinateurs, et une assistance à distance aux équipes informatiques par contre Apache guacamole est adapté uniquement à l'accès à distance aux ordinateurs.

2 **Performance :** Splashtop est utilisé pour le Streaming audio et vidéo haute performance avec faible latence, pour les ordinateurs Windows et Mac mais avec Guacamole Les utilisateurs sont confrontés à des connexions distantes retardées vers les Mac.

3 **Sécurité** Ensemble robuste de fonctions de sécurité et conformité

4 **Programmation de l'accès à distance** Les administrateurs informatiques peuvent programmer des horaires spécifiques et gérer les autorisations d'accès des étudiants aux ordinateurs des laboratoires via une console d'administration centralisée, ce qui leur permet de contrôler étroitement l'accès et l'utilisation mais Guacamole n'a pas de fonction de programmation.

5 **Architecture** Dans Splashtop le streamer est installé sur les ordinateurs et les utilisateurs à distance à l'aide de l'application Splashtop Business depuis n'importe quel appareil Par contre Guacamole s'agit d'une passerelle de bureau à distance sans client prenant en charge les protocoles standard tels que VNC, RDP et SSH.

6 **Dossiers en cours de session** Avec les deux solutions les utilisateurs peuvent transférer des fichiers, enregistrer une session, imprimer à distance, et bien plus encore pendant une session à distance.

7 **Soutien à la demande** Les équipes informatiques peuvent se connecter à distance à n'importe quel appareil et résoudre les problèmes techniques, sans aucune installation préalable

2.7 conclusion

Dans ce chapitre, nous avons présenter des concepts liés à la sécurité informatique. Nous avons aussi exposé les diverses menaces, vulnérabilités et attaques ainsi que les mécanismes de défense. Puis, nous avons opté pour la définition de l'accès à distance et de son importance fondamentale en entreprise.

Dans le chapitre suivant, nous passerons en revue l'approche et les outils de développement utilisés pour la réalisation de Guacamole et discuterons de certaines interfaces d'application.

Chapitre 3

Installation et configuration de la passerelle

3.1 Introduction

Dans ce chapitre, nous nous intéressons à la description de la phase de la réalisation. Nous commençons par la spécification des différents environnements de développement, matériels et logiciels. Nous présentons par la suite les différentes étapes d'installation et configuration des outils utilisés pour la mise en place de la passerelle de bureau à distance . Nous terminons par quelques interfaces, captures et explications de fonctionnement de l'application.

3.2 Matériel utilisé

Pour pouvoir implémenter et configurer l'architecture souhaitée dont la nécessité de mettre en place une gestion facile et efficace, nous avons travaillé avec un Pc de marque HP avec une RAM de 4 Go. Dans le but d'assurer la compatibilité des environnements, nous avons choisi de travailler avec le système d'exploitation Windows 10.

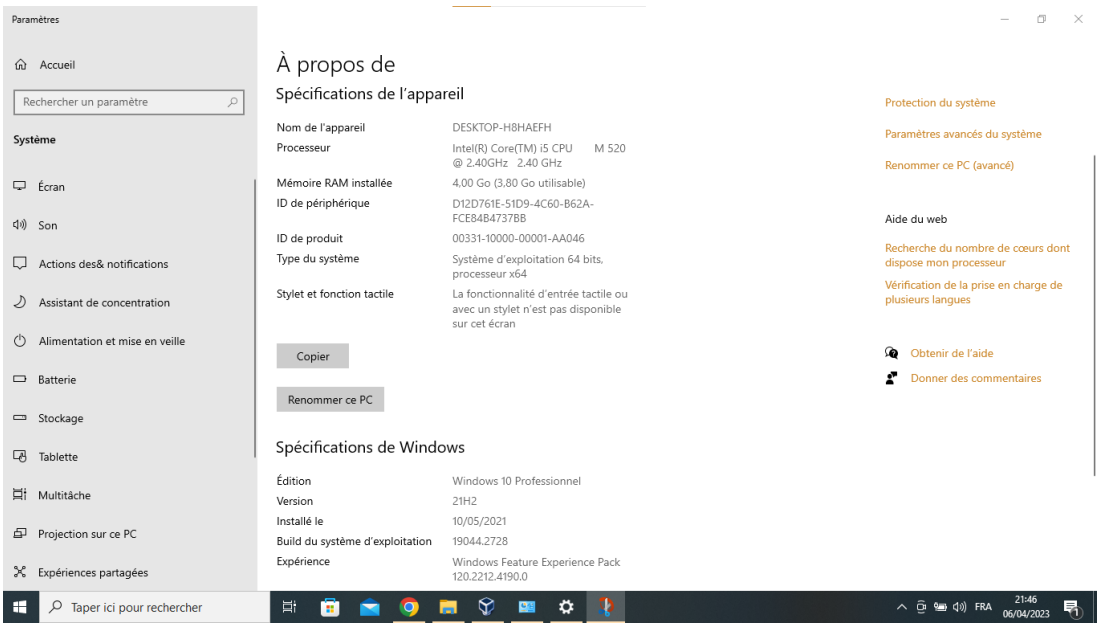

FIGURE 3.1 – Matériel utilisé.

3.3 Présentation des outils utilisés

Présentation de notre démarche : Nous avons travaillé dans un environnement virtuel sur l'app VirtuelBox pour créer des machines virtuelles, nous avons tout d'abord configuré les interfaces réseau de chaque machine pour qu'elles soient connectées au même réseau local et tester la connectivité entre eux. Puis nous avons déployé avec succès la passerelle guacamole sur DEBIAN 11 et configuré l'accès à distance entre les différentes machines virtuelles sur notre réseau local.

3.3.1 Présentation de la machine virtuelle

Dans ce qui suit nous allons présenter les deux outils essentiels qui permettent une bonne contribution pour la réalisation de notre projet.

3.3.1.1 Oracle VM VirtualBox 7.0.4

Oracle VM Virtualbox est un logiciel de virtualisation multiplate-forme. Il permet aux utilisateurs d'étendre leur ordinateur existant pour exécuter plusieurs systèmes d'exploitation, y compris Microsoft Windows, Mac OS X, Linux et Oracle Solaris en même temps.

Conçu pour les professionnels de l'Informatique et les développeurs, Oracle VM Virtualbox est idéal pour tester, développer, démontrer et déployer des solutions sur plusieurs plates-formes à partir d'une seule machine [30].

3.3.1.2 Téléchargement d'Oracle VM Virtualbox 7.0.4

On pourrait toutefois télécharger une version d'évaluation de Virtualbox via la façon suivante : [31]

1. Se rendre sur le lien suivant : https ://www.virtualbox.org/wiki/Downloads
2. Choisir la version du produit à télécharger puis via un menu on clique sur le système d'exploitation qui convient avec notre machine, le téléchargement se lance automatiquement.

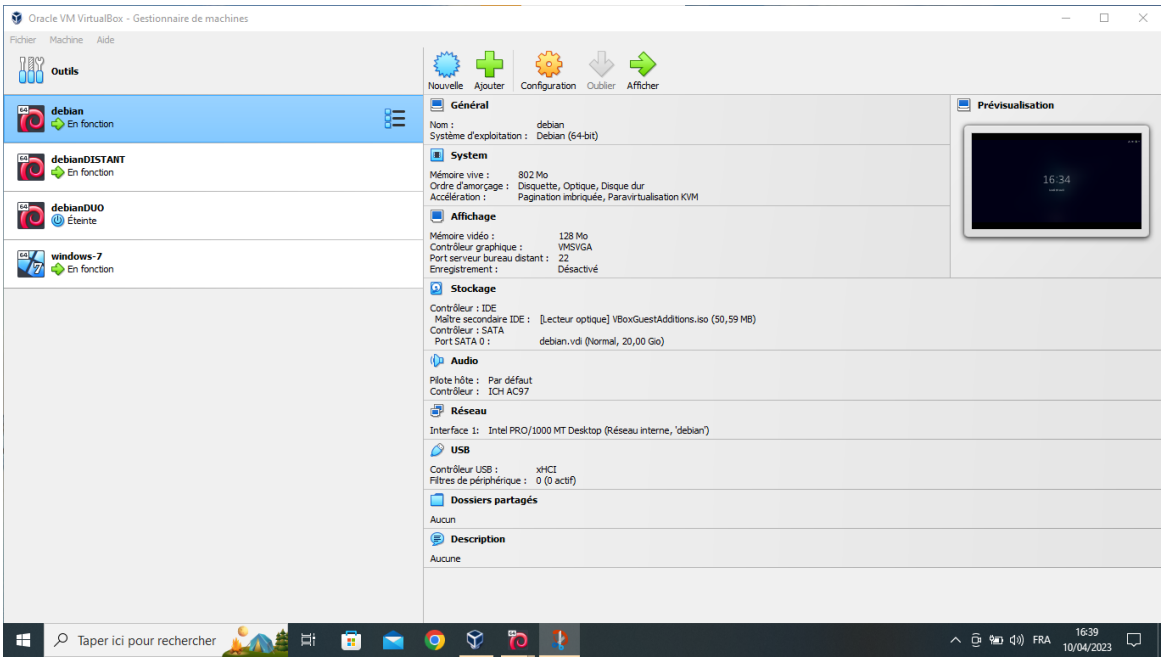

FIGURE 3.2 – Oracle VM VirtualBox 7.0.4.

3.3.2 LINUX DEBIAN

3.3.2.1 Pourquoi choisir Debian ?

Nous avons choisi la distribution Debian pour plusieurs raisons :

- Ses qualités techniques : Debian est réputé pour sa stabilité, pour son très bon système de gestion des dépendances entre les différents composants (ce qui rend l'installation et le retrait des programmes très facile) et pour sa rapidité à réparer les failles de sécurité [32].
- Il intègre des outils et des capacités de projet GNU et est fourni avec des milliers d'applications logicielles pour une installation et une exécution faciles [33].

3.3.2.2 Présentation de Linux Debian

Debian est appelée la mère des distributions Linux, Construit sur le noyau Linux, Debian GNU/Linux est un système d'exploitation (OS) open source et gratuit basé sur une interface utilisateur graphique (GUI).

3.3.2.3 Téléchargement de Linux Debian 11

Pour le système d'exploitation 64 bits, On pourrait cependant télécharger DEBIAN via la façon suivante :

- Se rendre sur le site officiel de debian https ://www.debian.org/.
- Après l'affichage on cliquera sur le bouton "télécharger" puis "Obtenir debian".
- Il nous mènera vers une autre page pour télécharger une image ISO d'installation.
- On va choisir "image d'installation complète" puis on clique sur le lien "Télécharger les Image des CD ou DVD par HTTP".
- On va choisir des images du DVD (4,4 Go chacune), un clic sur "Amd64".
- Enfin on cliquera sur le lien "debian-11.6.0-amd64-DVD-1.iso".

3.3.2.4 Installation de Linux Debian sur VirtuelBox

Pour ce faire, on doit suivre les étapes suivantes :

- On démarre VirtualBox et cliquer sur l'icône "Nouvelle".
- On entre un nom pour la machine virtuelle ("Debian" par exemple), puis on importe l'image ISO d'installation de GNU Debian/Linux et on clique sur "suivant".
- Définir la taille de la mémoire pour la machine virtuelle : 1024 Mo au minimum et clique sur "suivant".
- Pour la partie du stockage, un disque virtuel va être créé par défaut (20G disponible) en cliquant sur "create a virtuel hard disk now", puis "suivant".
- On peut affiner quelques paramètres dans la VM en effectuant un clic droit sur la VM puis cliquer sur “Configuration”.
- On clique ensuite sur “Démarrer” pour lancer la VM.
- L'installateur de Debian est lancé. On choisit “Graphical install”.
- L'installation est ensuite classique : Choisir la langue, la loclisation, clavier préféré.
- On commence maintenant la configuration du réseau, on débute par définir un nom d'hôte pour le système, l'ajout du nom de domaine auquel appartient cet hôte, on peut le laisser vide s'il ne fait partie d'aucun domaine ou s'il peut être configuré ultérieurement.

- Choisir un mot de passe pour l'utilisateur root. Ensuite saisir un nom d'un utilisateur, son nom de compte puis son mot de passe.
- Le programme d'installation va maintenant nous guider à travers le partitionnement des disques. Dans cette section on choisit la méthode de partionnement, dans notre cas c'est "utiliser le disque entier" puis sélectionner le disque à partitionner.
- Choisir tous les fichiers dans une partition, ce qui est recommandé pour les nouveaux utilisateurs.
- Choisir Oui pour écrir les modifications sur les disques, et on démarre l'installation du système de base.
- Si on a des médias supplémentaires, nous pouvons les ajouter ou simplement ignorer en sélectionnant l'option "non".
- Ensuite, configurer le gestionnaire de paquets : On choisit d'abord l'emplacement du miroir à proximité de notre réseau.
- On sélectionne un miroir d'archives Debian dans la liste : "Deb.debian.org".
- On ajoute les informations du protocole de communication HTTP, si nécessaire pour accéder à Internet ou laissez-les vides.
- Participer à l'enquête sur l'utilisation du package ou choisir aucune option.
- On peut maintenant sélectionner une collection prédéfinie de logiciels tels que l'environnement de bureau, le serveur Web, le serveur SSH. Nous continuons avec les paramètres par défaut, c'est-à-dire avec le bureau GNOME.
- Choisir Oui pour installer le chargeur de démarrage GRUB sur notre lecteur principal.
- Choisir le périphérique pour l'installation du chargeur de démarrage.
- Enfin, l'écran de fin d'installation s'affiche, on clique sur le bouton Continuer pour redémarrer.
- Après le redémarrage, il s'affiche l'écran de connexion Debian 11, on clique sur le compte d'utilisateur, puis donnez le mot de passe.

3.4 l'architecture de la passerelle Guacamole

Dans ce qui suit, nous allons voir comment l'application Guacamole est implémentée. Guacamole n'est pas une application Web autonome et se compose de plusieurs parties. Cette dernière est en fait destinée à être simple et minimale, la majorité du travail de fond étant effectué par des composants de niveau inférieur [34]. Dans son fonctionnement, Guacamole possède plusieurs couches applicatives résumant tout cela par un petit diagramme illustré dans la figure 3.3.

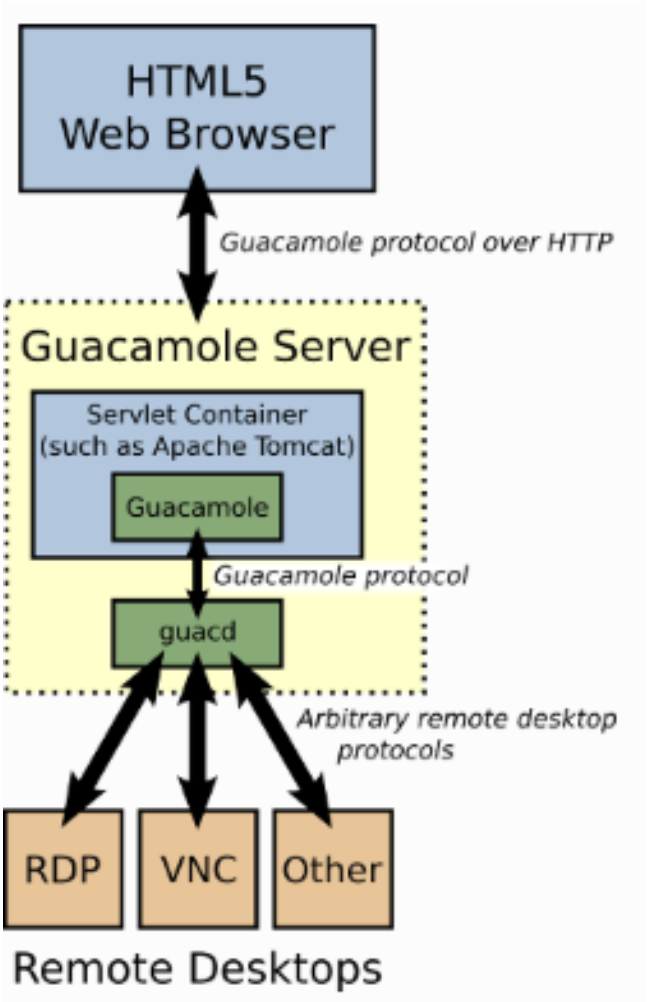

FIGURE 3.3 – Diagramme des couches applicatives de Guacamole [34].

3.4.1 Server guacamole

Fournit tous les composants côtés serveur et natifs requis par Guacamole pour se connecter à des ordinateurs de bureau distants. Il fournit aussi le proxy Guacd et les bibliothèques associées [35].

3.4.2 Client Guacamole

Il s'agit d'une application Web HTML 5 et d'un client qui nous permet de se connecter à nos serveurs/ordinateurs de bureau distants. Ceci est soutenu par le serveur Tomcat [35].

3.4.3 Le protocole Guacamole

L'application Web ne comprend aucun protocole de bureau à distance. En fait, elle comprend que le protocole Guacamole, qui est un protocole de rendu d'affichage à distance et de transport d'événements.

L'ajout de la prise en charge d'un protocole de bureau à distance particulier (comme RDP) à Guacamole implique donc l'écriture d'une couche intermédiaire (Guacd) qui *traduit* entre le protocole de bureau à distance et le protocole Guacamole. Cette implémentation particulière s'affiche sur un affichage distant plutôt que sur un affichage local [34].

3.4.4 Guacd

Le cœur de Guacamole qui charge dynamiquement la prise en charge des protocoles de bureau à distance et les connecte aux bureaux à distance en fonction des instructions reçues de l'application Web. Guacd est un processus démon qui est installé avec Guacamole et s'exécute en arrière-plan, implémente juste le protocole Guacamole pour déterminer quel support de protocole doit être chargé et quels arguments doivent lui être transmis [34].

3.4.5 L'application web

La partie de Guacamole avec laquelle un utilisateur interagit réellement est l'application Web. Elle s'appuie sur Guacd et n'implémente rien de plus qu'une interface Web et une couche d'authentification élégante [34].

*** Déploiement classique :**

Les utilisateurs se connectent à un serveur Guacamole avec leur navigateur Web. Le client Guacamole, écrit en Javascript, est servi aux utilisateurs par un serveur Web au sein du serveur Guacamole. Une fois chargé, ce client se reconnecte au serveur via HTTP en utilisant le protocole Guacamole.

L'application Web déployée sur le serveur Guacamole lit le protocole Guacamole et le transmet à Guacd, le proxy Guacamole natif. Ce proxy interprète en fait le contenu du protocole Guacamole, se connectant à n'importe quel nombre de serveurs de bureau à distance au nom de l'utilisateur [34].

3.5 Installation et configuration de apache Guacamole

Nous avons fais cette installation sur un serveur Debian 11.

3.5.1 Installation de Guacamole-Server

On commence par l'installation des dépendances requises [36].

3.5.1.1 Installation des prérequis

La première chose à faire est de mettre à jour Debian

```
root@debian:~# sudo apt-get update
```

```
root@debian:~# sudo apt-get upgrade
```

Puis, on passe à l'installation de "make" car on l'aura besoin pour compiler Guacamole

```
root@debian:~# sudo apt install make -y
```

Ensuite installer les prérequis suivants

```
root@debian:~# sudo apt install gcc g++ libcairo2-dev libjpeg62-turbo-dev libpng
-dev libtool-bin libossp-uuid-dev libavcodec-dev libavformat-dev libavutil-dev l
ibswscale-dev freerdp2-dev libpango1.0-dev libssh2-1-dev libvncserver-dev libtel
net-dev libssl-dev libvorbis-dev libwebp-dev libpango1.0-dev libwebsockets-dev l
ibpulse-dev -y
```

3.5.1.2 Installation de Guacamole-Server

On commence l'installation du premier composant essentiel [42]. La dernière version disponible est la 1.5.0 (lors de la réalisation de notre mémoire).

On télécharge l'archive sur le serveur

```
root@debian:~# wget https://downloads.apache.org/guacamole/1.5.0/source/guacamol
e-server-1.5.0.tar.gz
```

On décompresse l'archive

```
root@debian:~# tar xvf guacamole-server-1.5.0.tar.gz
```

On accède au dossier qui vient d'être décompressé

```
root@debian:~# cd guacamole-server-1.5.0/
```

On vérifie que toutes les dépendances nécessaires sont installées sur le serveur à l'aide de configure, et là on va avoir que des yes, la preuve que l'installation de ces dernières est réussie

```
root@debian:~/guacamole-server-1.5.0# sudo ./configure --with-init-dir=/etc/init
.d
```

Maintenant on va compiler puis installer "Guacamole-Server"

```
root@debian:~/guacamole-server-1.5.0# sudo make
```

On passe à l'installation

```
root@debian:~/guacamole-server-1.5.0#  sudo make install
```

On crée les différents liens avec les librairies

```
root@debian:~/guacamole-server-1.5.0# sudo ldconfig
```

On active le service de Guacamole

```
root@debian:~/guacamole-server-1.5.0# sudo systemctl enable guacd
```

Puis on démarre le service

```
root@debian:~/guacamole-server-1.5.0# sudo systemctl start guacd
```

Enfin on vérifie bien que le service est actif

```
root@debian:~/guacamole-server-1.5.0# systemctl status guacd
● guacd.service - LSB: Guacamole proxy daemon
     Loaded: loaded (/etc/init.d/guacd; generated)
     Active: active (running) since Sat 2023-04-08 18:28:14 CEST; 9min ago
       Docs: man:systemd-sysv-generator(8)
      Tasks: 1 (limit: 850)
     Memory: 10.5M
        CPU: 48ms
     CGroup: /system.slice/guacd.service
             └─25437 /usr/local/sbin/guacd -p /var/run/guacd.pid
```

3.5.2 Installation de Guacamole-Client

Ici, on va installer le client qui nous fournit l'interface HTML5 et pour cela, on a besoin d'installer **Tomcat** [36].

```
root@debian:~# sudo apt install tomcat9 tomcat9-admin tomcat9-common tomcat9-use
r -y
```

Vérifions que le serveur Tomcat fonctionne

```
● tomcat9.service - Apache Tomcat 9 Web Application Server
     Loaded: loaded (/lib/systemd/system/tomcat9.service; enabled; vendor prese>
     Active: active (running) since Sat 2023-04-08 18:43:39 CEST; 9min ago
       Docs: https://tomcat.apache.org/tomcat-9.0-doc/index.html
    Process: 27451 ExecStartPre=/usr/libexec/tomcat9/tomcat-update-policy.sh (c>
   Main PID: 27455 (java)
      Tasks: 29 (limit: 850)
     Memory: 99.1M
        CPU: 15.735s
     CGroup: /system.slice/tomcat9.service
             └─27455 /usr/lib/jvm/default-java/bin/java -Djava.util.logging.con>
```

Maintenant on va télécharger le client et le stocker dans un dossier qu'on va créer

```
root@debian:~# sudo wget https://downloads.apache.org/guacamole/1.5.0/binary/gua
camole-1.5.0.war -O /etc/guacamole/guacamole.war
```

Maintenant, on va devoir créer un lien symbolique vers Tomcat9 WebApps pour activer l'utilisation du client

```
root@debian:~# sudo ln -s /etc/guacamole/guacamole.war /var/lib/tomcat9/webapps/
```

Enfin, pour que l'application soit totalement déployée, on va redémarrer les services

```
root@debian:~# sudo systemctl restart tomcat9
root@debian:~# sudo systemctl restart guacd
```

Maintenant on a accès à la page d'authentification de Guacamole en se rendant sur la page IP_SERVER :8080/guacamole ou sur localhost :8080/guacamole.

FIGURE 3.4 – Authentification Guacamole.

3.5.3 Configuration Guacamole-Server/Client

3.5.3.1 Configuration du serveur

On a installé tous les principaux services, il faut maintenant les configurer et faire en sorte qu'ils fonctionnent tous ensemble [36].

On crée les dossiers extensions et lib dans le dossier /etc/guacamole

```
root@debian:~# sudo mkdir /etc/guacamole/{extensions,lib}
```

On rajoute la variable d'environnement de Guacamole

```
root@debian:~# sudo echo "GUACAMOLE_HOME=/etc/guacamole"  /etc/default/tomcat9
GUACAMOLE_HOME=/etc/guacamole /etc/default/tomcat9
```

On va installer un gestionnaire de base de données SQL, car c'est par lui qu'on gérera l'authentification des utilisateurs. Nous pouvons installer MySQL ou MariaDB

```
root@debian:~# sudo apt install mariadb-server mariadb-client
```

On va se connecter au serveur de base de données

```
root@debian:~# sudo mysql
```

Il faudra exécuter la requête ci-dessous

```
MariaDB [(none)]> CREATE DATABASE guacamole_db;
Query OK, 1 row affected (0,164 sec)

MariaDB [(none)]> CREATE USER 'guacamole_user'@'localhost' IDENTIFIED BY 'P@$sW0
rd';
Query OK, 0 rows affected (0,237 sec)

MariaDB [(none)]> GRANT SELECT,INSERT,UPDATE,DELETE ON guacamole_db.* TO 'guacam
ole_user'@'localhost';
Query OK, 0 rows affected (0,122 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,038 sec)

MariaDB [(none)]> quit;
Bye
root@debian:~#
```

Télécharger l'extension mysql pour Guacamole

```
root@debian:~# wget https://dlcdn.apache.org/guacamole/1.5.0/binary/guacamole-au
th-jdbc-1.5.0.tar.gz
```

Décompresser l'archive

```
root@debian:~# tar vfx guacamole-auth-jdbc-1.4.0.tar.gz
```

Ajouter les tables nécessaires dans la base de données créée

```
root@debian:~# cat guacamole-auth-jdbc-1.5.0/mysql/schema/*.sql | sudo mysql gua
camole_db
```

Installation de l'extension

```
root@debian:~# sudo cp guacamole-auth-jdbc-1.5.0/mysql/guacamole-auth-jdbc-mysql
-1.5.0.jar /etc/guacamole/extensions/
```

Télécharger le driver JDBC

```
root@debian:~# wget https://dev.mysql.com/get/Downloads/Connector-J/mysql-connec
tor-java-8.0.28.tar.gz
```

Décompresser l'archive

```
root@debian:~# tar xvzf mysql-connector-java-8.0.28.tar.gz
```

Installer le driver pour Guacamole.

```
root@debian:~# sudo cp mysql-connector-java-8.0.28/mysql-connector-java-8.0.28.j
ar /etc/guacamole/lib/
```

3.5.3.2 Configuration du client

On passe désormais à la configuration du client pour utiliser la base de données [36]. Tout d'abord, on crée le fichier de configuration

```
root@debian:~# sudo nano /etc/guacamole/guacamole.properties
```

Ici, on va ajouter la configuration en l'adaptant à notre environnement mysql

```
  GNU nano 5.4          /etc/guacamole/guacamole.properties *
# Hostname et port du serveur Guacamole
guacd-hostname: 127.0.0.1
guacd-port: 4822

# MySQL properties
mysql-hostname: localhost
mysql-port: 3306
mysql-database: guacamole_db
mysql-username: guacamole_user
mysql-password: P@$sW0rd
```

La configuration est enfin terminée, on va maintenant lier le dossier de configuration à Tomcat

```
root@debian:~# sudo ln -s /etc/guacamole /usr/share/tomcat9/.guacamole
```

On redémarre les services

```
root@debian:~# sudo systemctl restart tomcat9
root@debian:~# sudo systemctl restart guacd
```

L'installation et la configuration de base sont terminées, dans ce qui suit nous allons voir comment utiliser Guacamole.

3.6 Accéder à Guacamole dans un navigateur

Apache Guacamole devrait maintenant être accessible via un navigateur Web.

- On ouvre un navigateur Web sur notre machine DEBIAN
- On accède à l'URL : [ip] :8080/guacamole, en remplaçant [ip] par l'adresse IP de notre serveur. Cela affichera l'invite d'authentification.
- On entre *"guacadmin"* comme nom d'utilisateur et *"guacadmin"* comme mot de passe. On clique ensuite sur "Connexion".

3.7 Utiliser guacamole

Guacamole permet d'accéder à la plupart des fonctionnalités d'un ordinateur de bureau à partir de votre navigateur Web. Dans ce qui suit nous allons voir comment utiliser Guacamole et le personnaliser.

Une fois connecté avec succès, une page qui s'affiche, c'est l'écran d'accueil de Guacamole où toutes les connexions disponibles sont répertoriées, ainsi que des vignettes de toutes les connexions récemment utilisées ou actives. La figure 3.5 illustre l'écran d'accueil de guacamole :

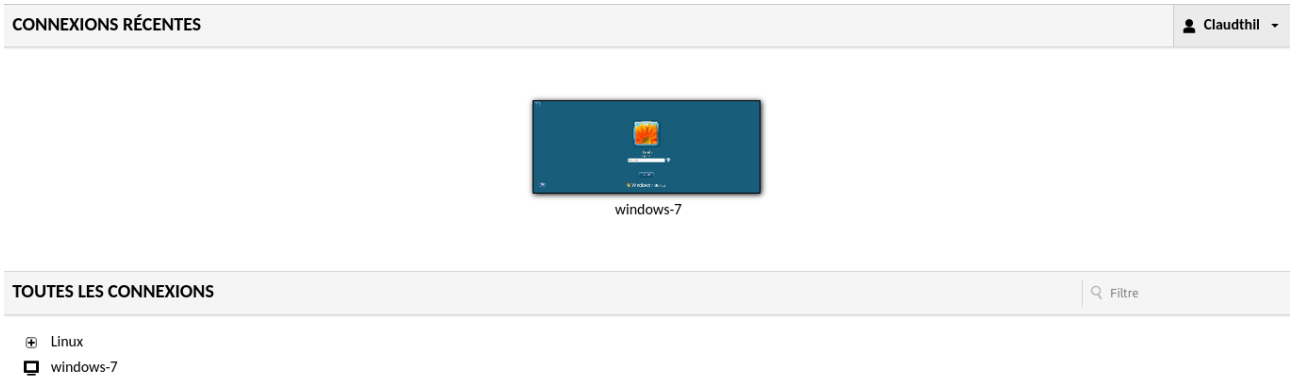

FIGURE 3.5 – Interface d'accueil de Guacamole.

L'écran Guacamole contient un menu dans le coin supérieur droit appelé *«menu utilisateur»*. Ce menu affiche le nom d'utilisateur et contient plusieurs options qui dépendent du niveau d'accès de l'utilisateur :

- **Acceuil**
  Revient à l'écran d'accueil, si l'utilisateur n'y est pas déjà.
- **Paramètres**
  Navigue vers l'interface des paramètres, qui permet d'accéder aux préférences de l'utilisateur telles que la langue d'affichage. Si l'utilisateur a accès aux fonctions d'administration, celles-ci se trouvent également dans l'interface des paramètres.
- **Se déconnecter**
  Se déconnecter complètement de Guacamole, en fermant toutes les connexions en cours et mettant fin à la session Guacamole.

3.7.1 Créer un compte administrateur

La première chose à faire est de créer un nouvel utilisateur administrateur afin de supprimer la compte "guacadmin" créé par défaut. On accède au menu, on sélectionne Paramètres et on clique sur "Utilisateurs" puis sur "Nouvel Utilisateur".

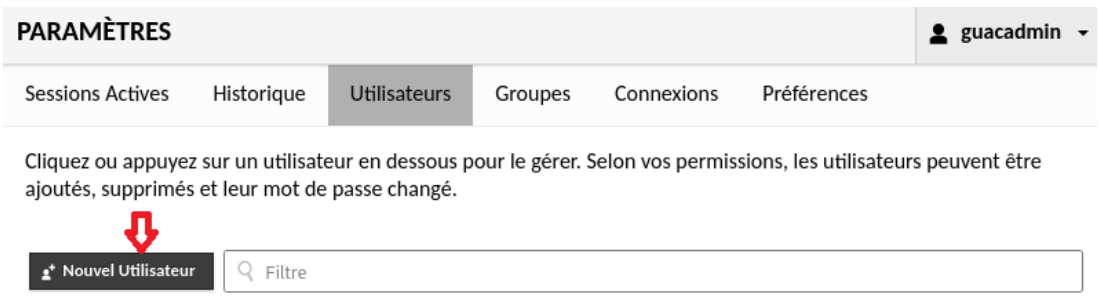

FIGURE 3.6 – Création d'un nouvel utilisateur.

Une interface qui apparaît où on pourra renseigner ses informations personnelles, ses permissions, les restrictions du compte, etc.

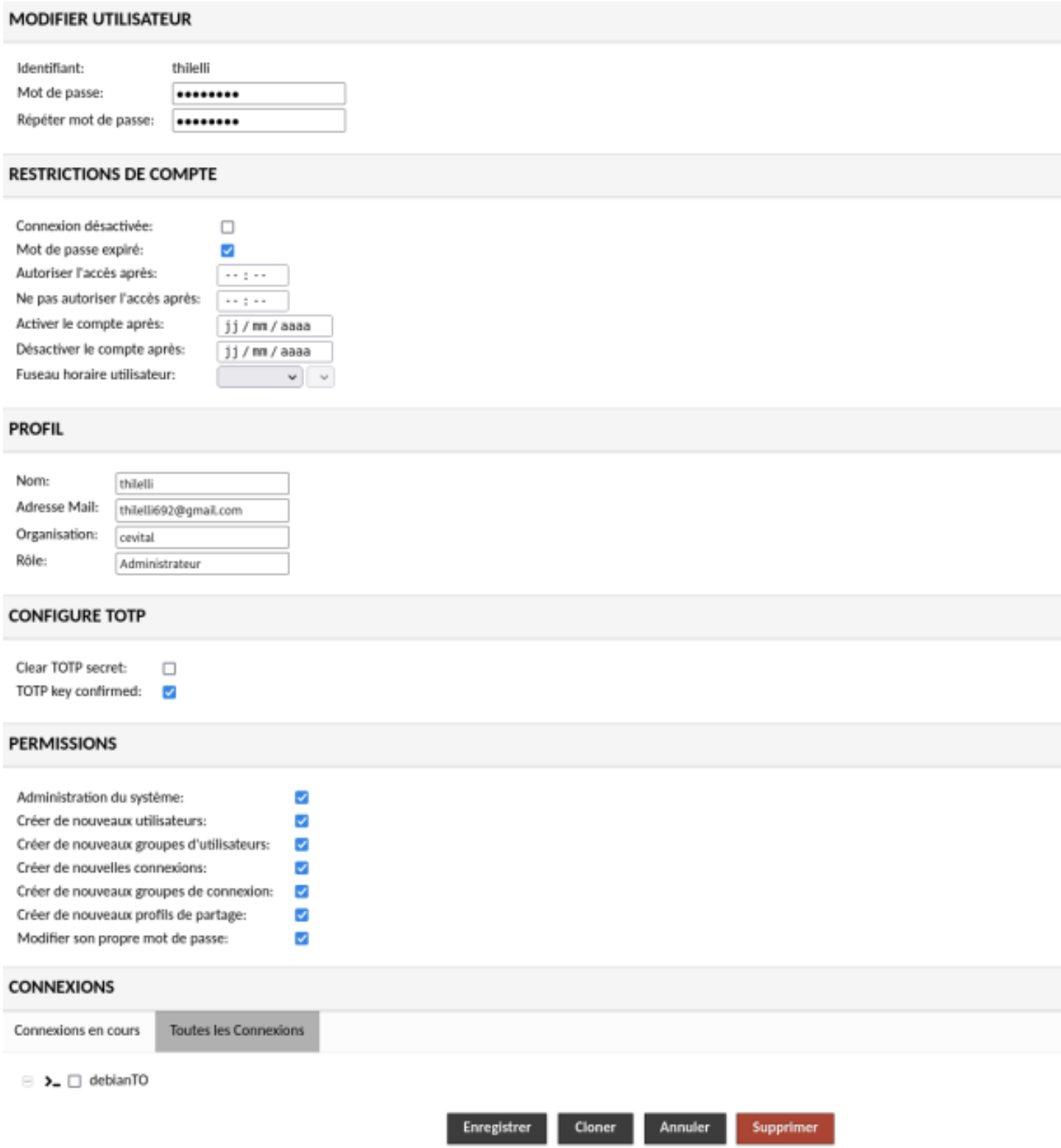

FIGURE 3.7 – Informations concernant le nouvel utilisateur.

Il ne reste qu'à connecter avec ce compte et supprimer celui de "guacadmin".

3.7.2 Créer un compte utilisateur

Pour créer un compte utilisateur, il suffit de suivre la même procédure vue précédemment, la seule chose qui change est sur les permissions ou on ne laisse que la possibilité à l'utilisateur de changer son mot de passe.

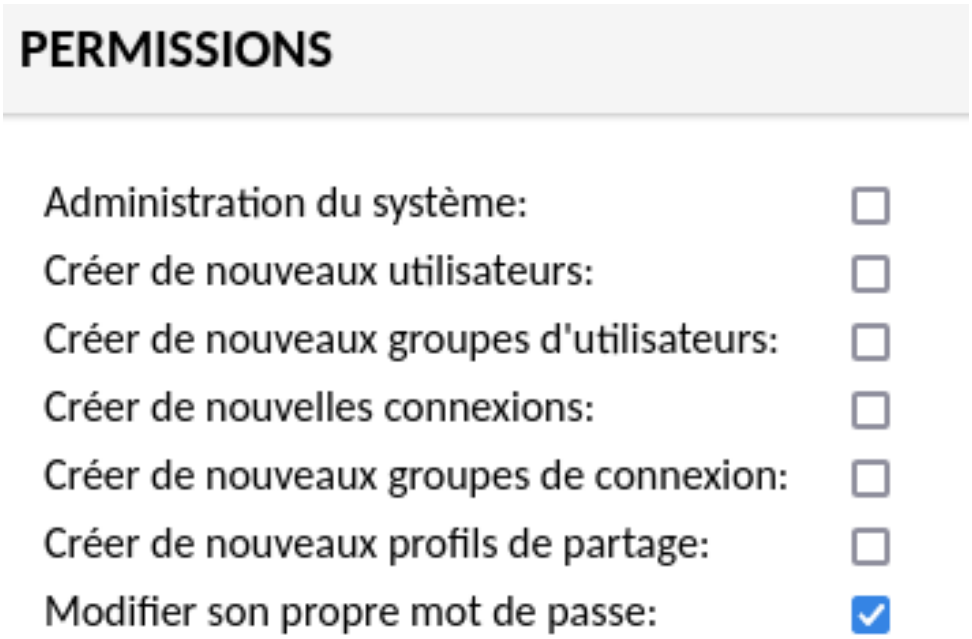

FIGURE 3.8 – Permissions des utilisateurs.

3.7.3 Créer un groupe utilisateur

Les groupes utilisateurs vont permettre de regrouper les comptes utilisateurs dans un groupe afin de pouvoir leurs données les accès plus facilement, à la place de gérer utilisateur par utilisateur.

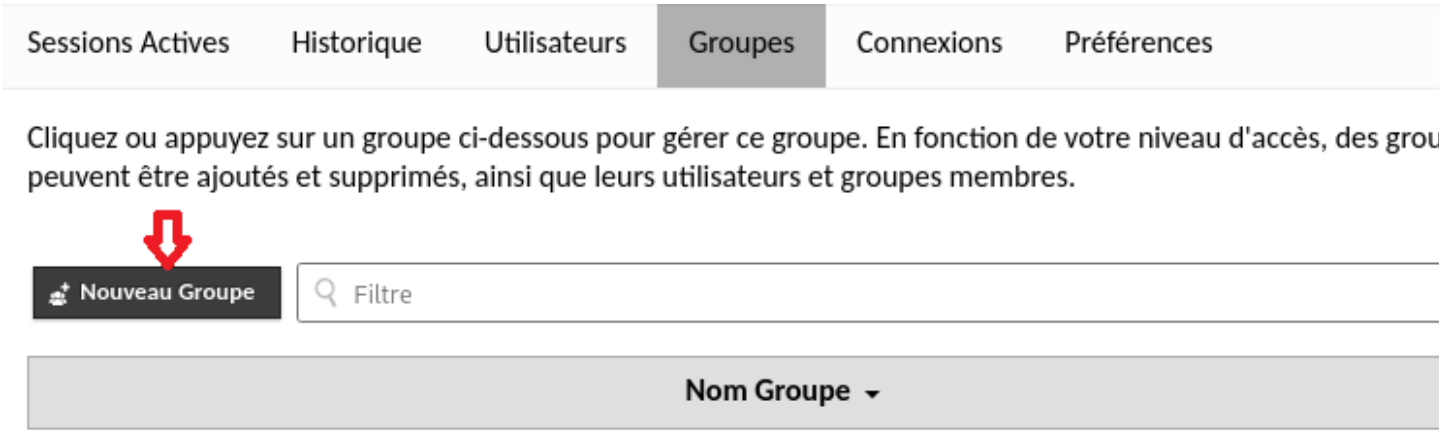

FIGURE 3.9 – création d'un nouveau groupe.

Ici, on pourra choisir le nom du groupe, les membres, les permission, cocher les groupes de connexion liés au groupe, etc. Puis cliquer sur "Enregistrer".

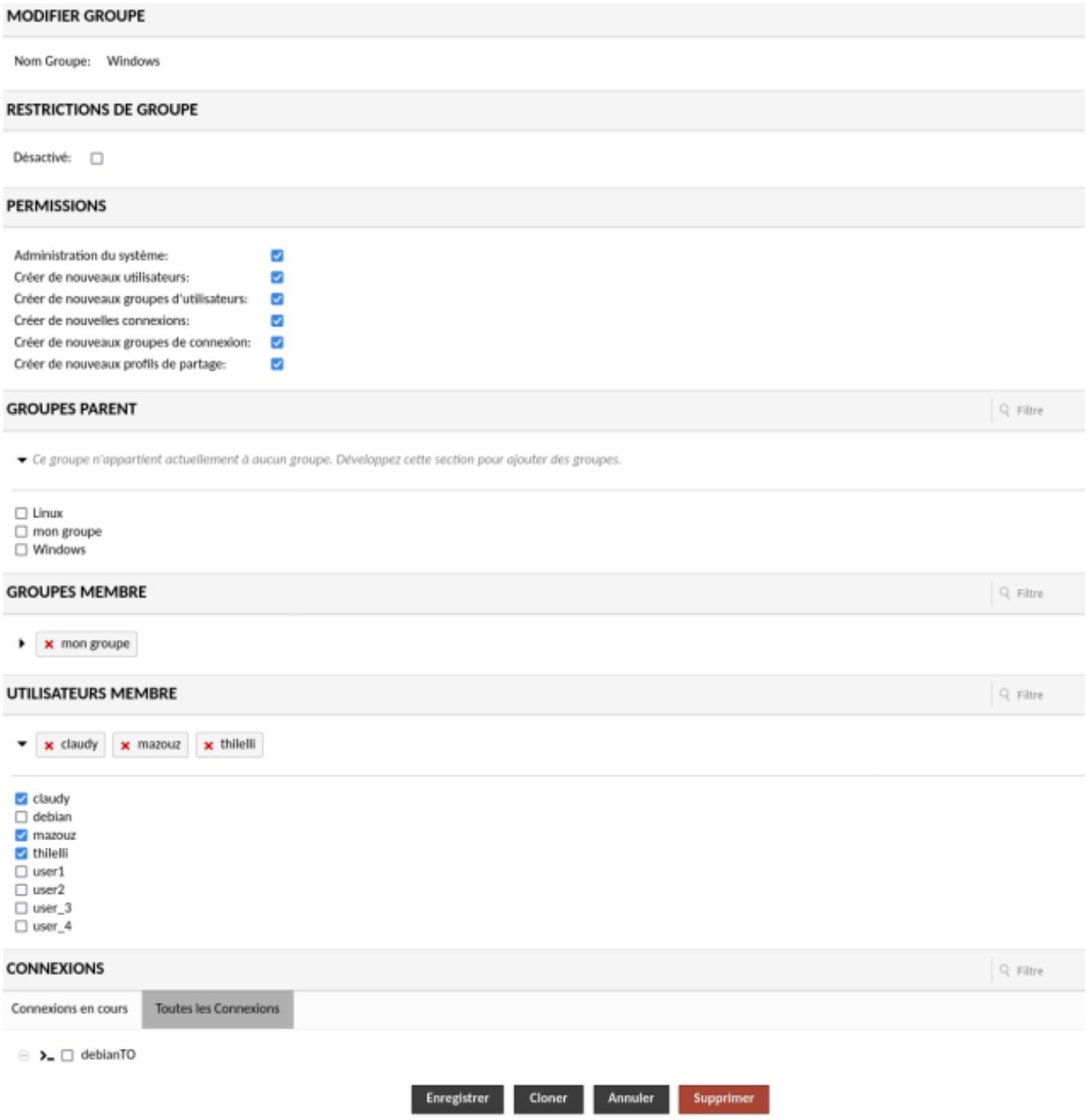

FIGURE 3.10 – Informations concernant le groupe créé.

3.7.4 Créer un groupe de connexions

Dans connexions on clique sur "Nouveau groupe"

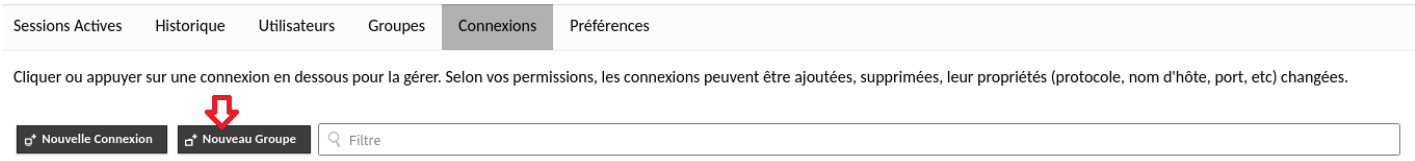

FIGURE 3.11 – Création d'un groupe de connexions.

puis remplir les champs de l'interface

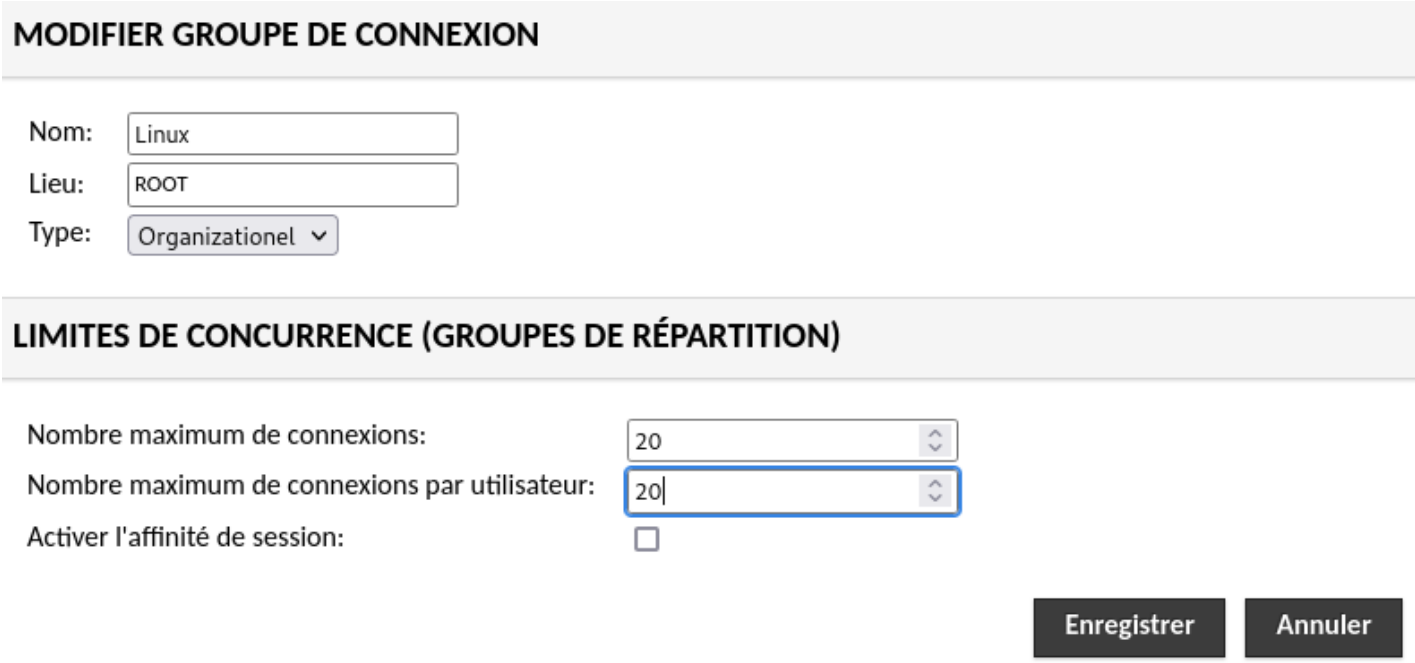

FIGURE 3.12 – Informations concernant le nouvel groupe de connexions.

Le groupe est créé et visible dans la liste des connexions, si on le déplie, on voit que l'on peut ajouter des connexions et des sous-groupes de connexions.

FIGURE 3.13 – Un groupe de connexions "Linux".

3.7.5 Ajouter une nouvelle connexion.

* Retenir

  Avant toute chose, pour gérer l'accès à distance entre les machines virtuelles on a besoin :

  - Mettre les machines dans un réseau local. Pour cela on accéde à la configuration des machines qu'on veut mettre dans un réseau local sur Oracle VM VirtualBox, puis dans la section réseau on change le mode d'accès réseau en "réseau interne" ;
  - Changer les @ IP dynamiques en @ IP statique sans oublier la passerelle par défaut.

Pour ajouter une connexion, on a deux possibilités :

- cliquer sur le bouton "Nouvelle Connexion" ;
- Cliquer sur "Nouvelle Connexion" qui se trouve au niveau des groupes de connexions.

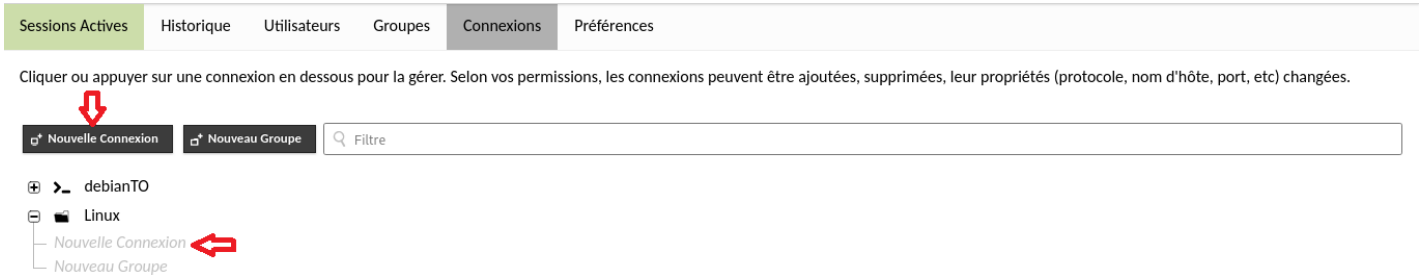

FIGURE 3.14 – Création d'une nouvelle connexion.

Pour créer une nouvelle connexion, on doit indiquer le protocole qu'on veut utiliser. On a : [37]

- **Protocole VNC :** Le protocole VNC est le plus simple et le premier protocole prit en charge par Guacamole. Bien qu'ils ne soient généralement pas aussi rapides que RDP, de nombreux serveurs VNC sont adéquats, et VNC sur Guacamole a tendance à être plus rapide que VNC seul en raison de la diminution de l'utilisation de la bande passante.
- **Protocole RDP :** Le protocole RDP est plus compliqué que VNC, il était le deuxième protocole officiellement prit en charge par Guacamole. RDP est plus rapide que VNC en raison de l'utilisation de la mise en cache, dont Guacamole profite.
- **Protocole SSH :** Contrairement à VNC ou RDP, SSH est un protocole texte. Son implémentation dans Guacamole est une combinaison d'un émulateur de terminal et d'un client SSH, car le protocole SSH n'est pas intrinsèquement graphique. Le support SSH de Guacamole émule un terminal côté serveur, et dessine l'écran de ce terminal à distance sur le client.
- **Protocole Telnet :**
  Telnet est un protocole texte et offre des fonctionnalités similaires à SSH. Par nature, il n'est pas crypté et ne prend pas en charge le transfert de fichiers.
- **Protocole Kubernetes :** Kubernetes fournit une API pour se connecter à la console d'un conteneur sur le réseau. Comme avec SSH et telnet, le support Kubernetes de Guacamole émule un terminal côté serveur qui s'affiche sur l'écran du client Guacamole.

Dans notre projet, on va s'intéresser aux deux protocoles RDP et SSH.

* **Configurer une connexion RDP**

  Dans un premier temps, on va activer l'option bureau à distance pour la machine **Windows 7**, et comme on est dans un réseau local, le port par défaut est le **3389**.
  Si nous connectons à distance à cette machine, il faut changer le port par défaut et faire la règle de redirection du port sur le routeur. Pour configurer "une connexion RDP", il existe plusieurs options à mentionner. On va se concentrer sur les principales.

- On commence par nommer la connexion et sélectionner le protocole RDP

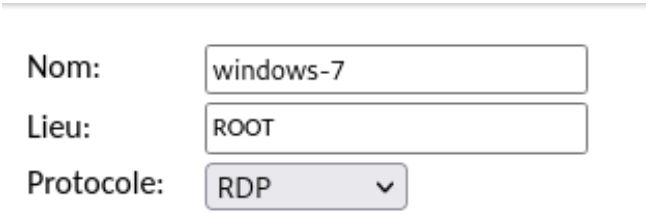

FIGURE 3.15 – Nom de la connexion et du protocole associè

- On peut définir le nombre de connexions simultanées maximum dans "Limites de concurrences".

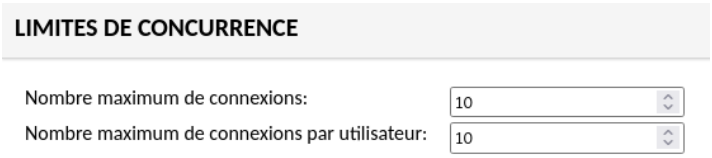

FIGURE 3.16 – Nombre de connexions simultanées

- On va maintenant s'intéresser à la partie "PARAMETRES", là on voit qu'on peut configurer tous les paramètres du client RDP (Passerelle RDS, Redirection des périphériques, Performances...).
- Dans la section"Réseau", on va indiquer le nom ou l'adresse IP de l'hôte ainsi que le port (3389) pour RDP.
- Dans la partie "Authentification", on va indiquer directement le compte à utiliser pour se connecter. On va saisir le nom de l'utilisateur et le mot de passe, on sélectionne le mode de sécurité (Négociation automatique, NLA, Chiffrement RDP, Chiffrement TLS, Hyper-V/VMConnect) et on coche la case Ignorer le certificat du serveur car les VM Windows Compute Engine sont provisionnées avec un certificat auto-signé pour les services de bureau à distance. Nous devons donc indiquer à Guacamole d'ignorer les problèmes de validation du certificat.

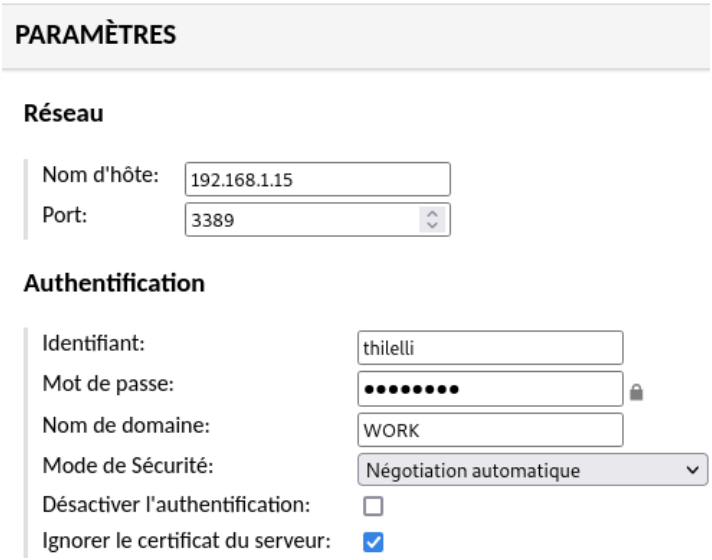

FIGURE 3.17 – Les paramètres d'authentification et du réseau de la connexion RDP.

- On peut configurer les redirections de périphériques.
- On peut activer ou désactiver les options de performance en fonction de notre connexion.
- Un autre élément de configuration qui est l'enregistrement de la session dans la section "Enregistrement écran".
  On va indiquer l'emplacement où ils seront stockés "/var/guacamole/"(par exemple), mais il faudra au préalable avoir créé le dossier sur le serveur pour que cela fonctionne et ensuite indiquer le nom de l'enregistrement.
- Enfin enregistrer la connexion

* Utilisation de la connexion RDP

Pour tester la connexion RDP, on clique sur "Accueil" puis sur le nom de la connexion.
Nous voilà maintenant connecté. La figure 3.18 illustre l'interface d'accueil de la machine Windows 7 :

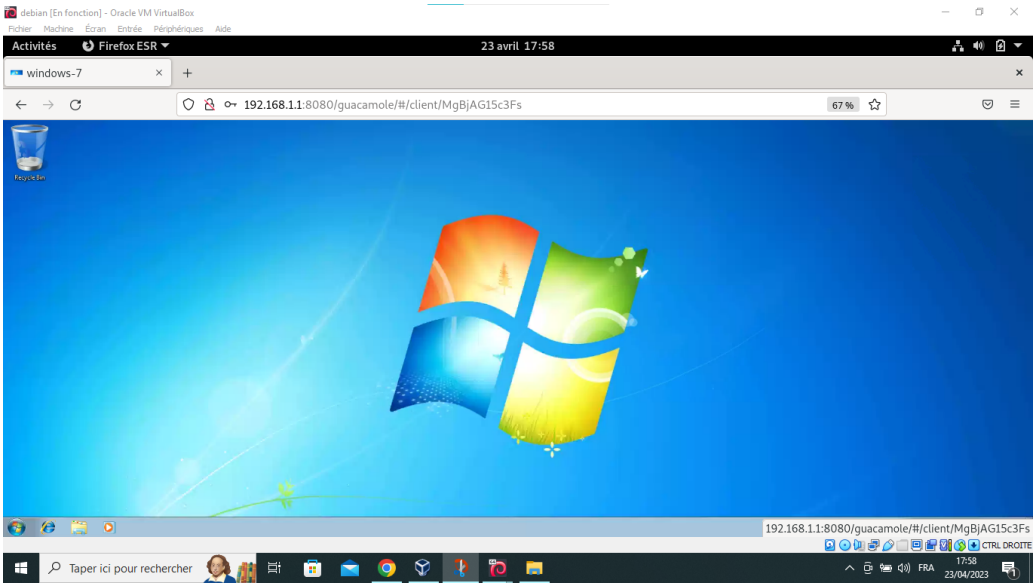

FIGURE 3.18 – l'écran d'accueil de Windows 7.

* Configurer une connexion SSH

La première chose à faire est d'activer l'option bureau à distance pour la machine Linux (dans notre cas c'est Debian 11), et comme on est dans un réseau local, le port par défaut est le 22.

- D'abord, on nomme la machine et on sélectionne le protocole SSH

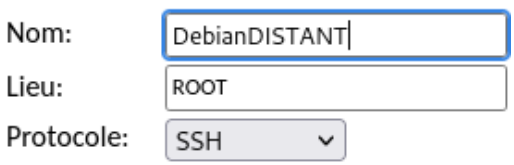

FIGURE 3.19 – Nom de la connexion et le protocole associé.

- Dans la section "Réseau", on indique l'adresse d'hôte (ou son nom DNS) et le port SSH (22), puis des informations sur l'environnement utilisateur.

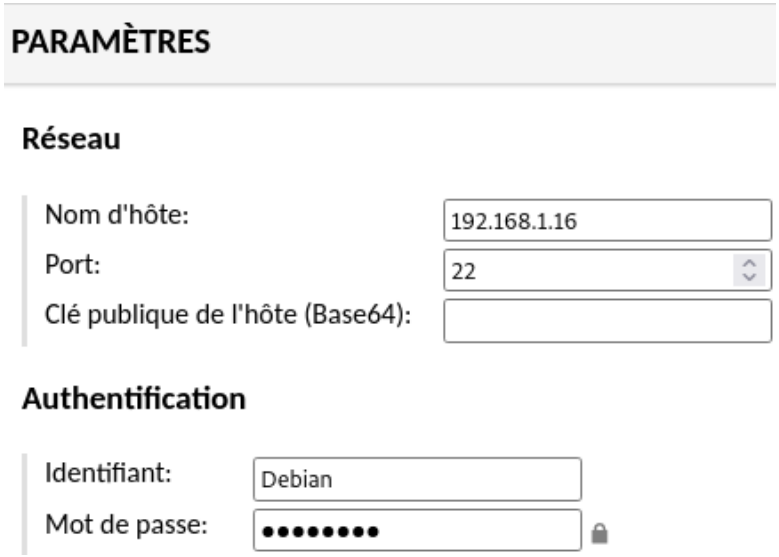

FIGURE 3.20 – Informations d'authentification et du réseau de la connexion SSH.

- On active le SFTP afin de pouvoir échanger des fichiers avec les machines distantes.

FIGURE 3.21 – Activation de SFTP.

- On peut également configurer d'autres paramètres comme les paramètres d'affichage et l'enregistrement d'écran.
- Enfin enregistrer la connexion.

*** Utilisation de la connexion SSH**

Dans l'écran d'accueil de guacamole on clique sur le nom de la connexion

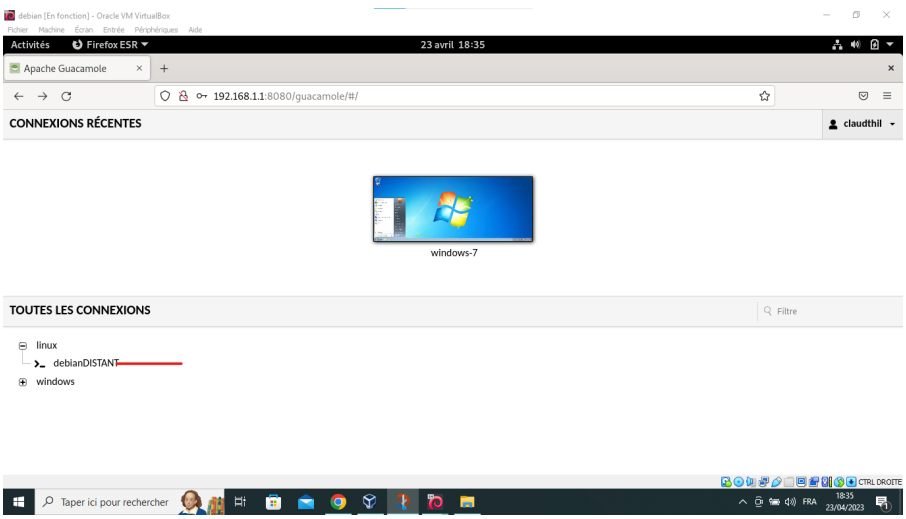

FIGURE 3.22 – Ecran d'accueil de Guacamole qui illustre toutes les connexions.

Là on se retrouve avec le terminal de notre serveur sur le navigateur de Guacamole.

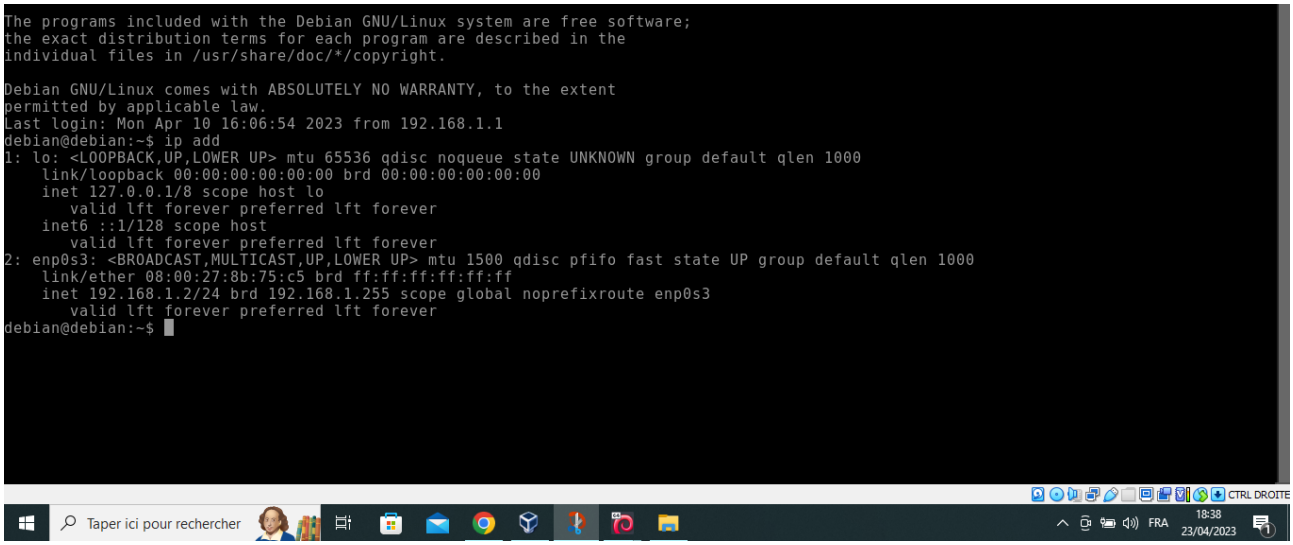

FIGURE 3.23 – Authentification réussie.

3.7.6 Affecter les connexions aux groupes

Cette opération est obligatoire afin que les utilisateurs puissent avoir accès aux connexions. Dans la gestion des groupes utilisateurs on clique sur le groupe à éditer. Tout en bas de la page dans la section "Connexion", on choisit lesquels on désire affecter et on clique sur enregistrer.

3.8 Suivre les sessions

Il est possible de suivre les sessions en cours depuis l'administration en allant sur le menu Sessions Actives. Depuis cette vue, on peut voir les connexions en cours avec la possibilité de fermer une session et de suivre en direct et d'interagir en cliquant sur le nom de la connexion.

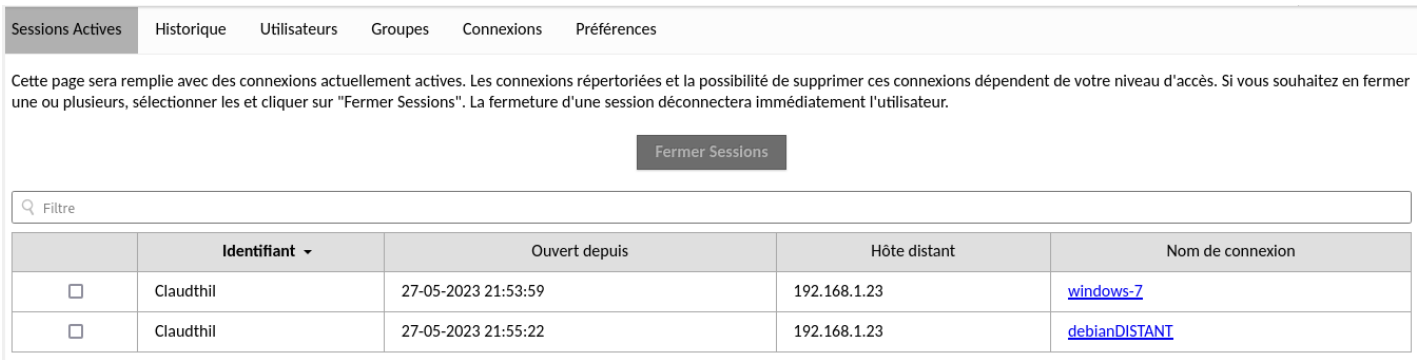

FIGURE 3.24 – Sessions active.

3.9 Historique des sessions

L'historique des sessions est disponible à différents emplacements :

- Dans le menu Historique

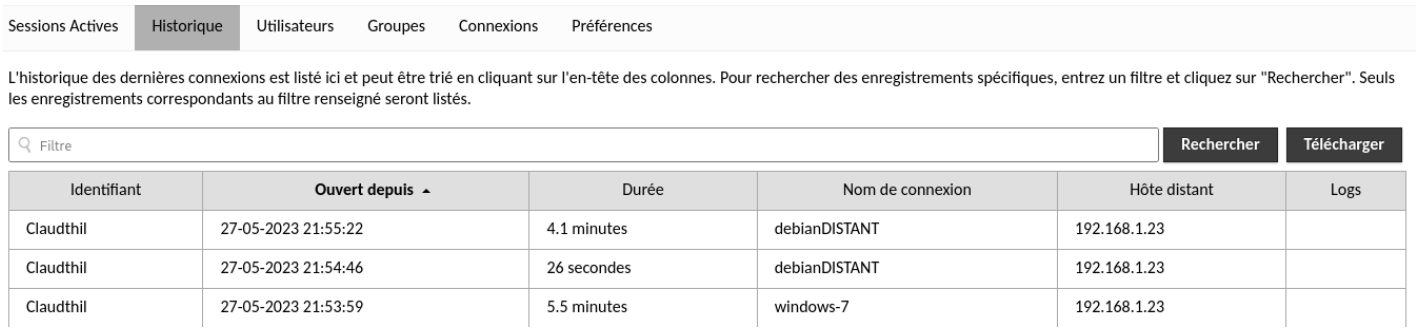

FIGURE 3.25 – Historique des sessions.

- Dans l'édition d'une connexion

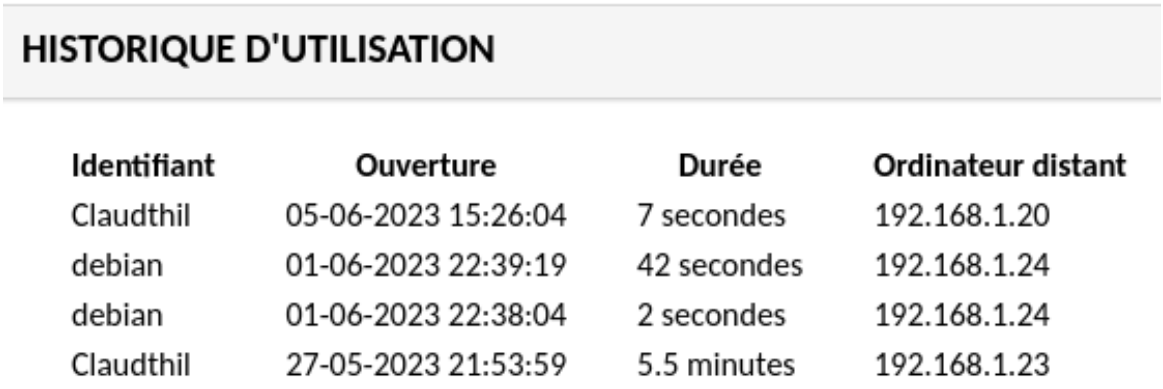

FIGURE 3.26 – Historique d'utilisation des sessions.

3.10 Conclusion

Dans ce chapitre nous avons présenté les différentes étapes d'installation et de configuration qui nous a aidés à déployer la passerelle Guacamole. Enfin, nous avons vu comment utiliser cette dernière afin de prouver l'accès à distance.

Le chapitre suivant nous renseigne comment réussir la configuration, après installation de guacamole, des méthodes de sécurisation à savoir "TOTP" et "DUO" afin de mieux sécuriser la passerelle d'accès à distance.

Chapitre 4

Implémentation de l'authentification à deux facteurs

4.1 Introduction

Pour déterminer l'implémentation de la solution, il est essentiel de disposer d'informations précises sur les problèmes de sécurité qui sont rencontrés par GUACAMOLE, où chacun ayant son contexte propre et ses solutions. Sécuriser un environnement Informatique revient à considérer chacun de ces cas. Ces problèmes peuvent être logiciels, matériels ou carrément du piratage.

Nous diviserons donc ce chapitre en deux parties. La première partie est dédiée à la mise en place de l'authentification à deux facteurs TOTP et la seconde partie est dédiée à l'implémentation de l'authentification à deux facteurs DUO.

4.2 L'authentification à deux facteurs

Un facteur d'authentification est une catégorie d'informations d'identification utilisée pour la vérification d'une identité. Il permet d'ajouter un niveau de sécurité supplémentaire. Si un compte est compromis, l'utilisateur malveillant ne pourra pas accéder aux machines distantes.

L'authentification à deux facteurs utilise par ailleurs des codes secrets à usage unique et des notifications soumis à une contrainte de temps pour empêcher l'usurpation d'identité.

4.2.1 l'authentification TOTP

Cette méthode utilise un mot de passe unique basé sur le temps, ce deuxième facteur d'authentification peut-être fourni par les applications "Google Authenticator", "FreeOTP", "Duo Mobile", "Microsoft Authenticator". Il en existe d'autres.

4.2.1.1 Conditions préalables

Le processus d'inscription utilisé par le support TOTP de Guacamole doit pouvoir stocker une clé générée automatiquement dans le compte de l'utilisateur, certaines exigences doivent être satisfaites pour que TOTP fonctionne comme prévu :

- Une autre extension doit être installée pour prendre en charge le stockage de données arbitraires à partir d'autres extensions.
- Il est recommandé que l'authentification par rapport à une base de données soit entièrement configurée avant de configurer TOTP.

4.2.1.2 Installer l'extension d'authentification Guacamole TOTP

Guacamole ne s'installe pas avec l'extension d'authentification TOTP par défaut. Ainsi, pour configurer l'authentification à deux facteurs TOTP sur Apache Guacamole, nous devons télécharger et installer l'extension [38].

À partir de la page des versions, nous allons téléchargées l'authentification TOTP qui corresponds à la version de notre serveur Guacamole installé.

```
root@debian:~# wget https://dlcdn.apache.org/guacamole/1.5.0/binary/guacamole-au
th-totp-1.5.0.tar.gz
```

Nous allons extraire l'extension et déplacer-la vers GUACAMOLE-HOME/extensions, qui est dans notre configuration etc/guacamole/extensions/.

```
root@debian:~# tar -zxf guacamole-auth-totp-1.5.0.tar.gz guacamole-auth-totp-1.5
.0/guacamole-auth-totp-1.5.0.jar
```

```
root@debian:~# mv guacamole-auth-totp-1.5.0/guacamole-auth-totp-1.5.0.jar /etc/g
uacamole/extensions/
```

4.2.1.3 Configurer l'authentification à deux facteurs TOTP sur Apache Guacamole

TOTP fonctionne par défaut. Certaines des configurations utilisées avec TOTP incluent [38].

- **totp-issuer :** définit le nom lisible par l'homme de l'entité délivrant les comptes d'utilisateurs. S'il n'est pas spécifié, "Apache Guacamole" sera utilisé par défaut.
- **totp-digits :** nombre de chiffres à inclure dans chaque code TOTP généré. Les valeurs légales sont 6, 7 ou 8. Par défaut, des codes à 6 chiffres sont générés.
- **totp-period :** la durée pendant laquelle chaque code généré doit rester valide, en secondes. Par défaut, chaque code reste valide pendant 30 secondes.
- **totp-mode :** L'algorithme de hachage qui doit être utilisé pour générer les codes TOTP. Les valeurs légales sont "sha1", "sha256" et "sha512". Par défaut, "sha1" est utilisé.

Nous allons mettre à jour les valeurs dans le fichier de configuration guacamole.properties.

```
 GNU nano 5.4          /etc/guacamole/guacamole.proprties
totp-issuer: 8
totp-digits: 6
totp-period: 30
totp-mode: “sha256”
```

4.2.1.4 Fonctionnement de TOTP avec GUACAMOLE

Lorsqu'un utilisateur tente de se connecter à Guacamole, les autres méthodes d'authentification installées seront interrogées en premier :

FIGURE 4.1 – Première authentification simple de guacamole après l'ajout de 2FA TOTP

Ce n'est qu'après que l'authentification a réussi avec l'une de ces méthodes que Guacamole invite l'utilisateur à vérifier davantage son identité avec un code d'authentification :

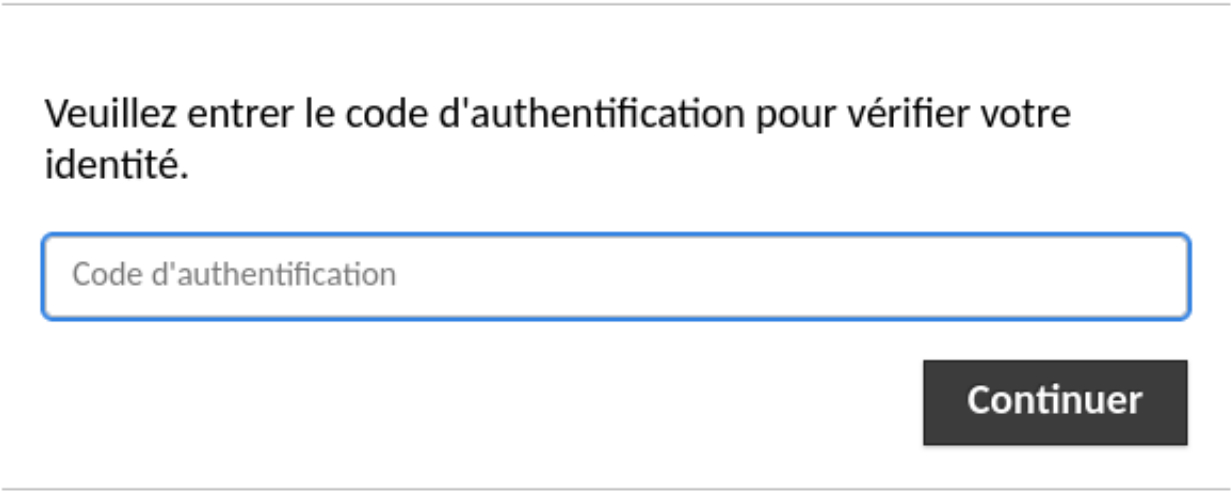

FIGURE 4.2 – Le code d'authentification après une inscription initiale réussite.

Si la tentative d'authentification initiale et la vérification à l'aide de TOTP réussissent, l'utilisateur sera autorisé à entrer. Si l'un ou l'autre des mécanismes échoue, l'accès à Guacamole est refusé.

4.2.1.5 Vérification de l'authentification à deux facteurs TOTP sur Apache Guacamole

Redémarrons notre serveur : [38]

```
root@debian:~# systemctl restart tomcat9
```

Maintenant nous allons connecter à l'interface Web de Guacamole en tant qu'utilisateur. Une fois la connexion réussie, nous serons accueillie par une telle interface.

FIGURE 4.3 – Vérification réussie de 2FA TOTP sur apache guacamole.

4.2.1.6 Inscription à guacamole TOTP Authentification

Pour terminer le processus d'inscription, nous avons scanné le code-barres avec l'application d'authentification à deux facteurs sur notre téléphone, nous avons utilisé FreeOTP. Une fois que nous avons scanné le code-barres, on entre le code d'authentification à 6 chiffres et on clique sur "Continuer" pour se connecter au tableau de bord Guacamole [38].

Lors de la reconnexion, nous sommes toujours invité à saisir le code.

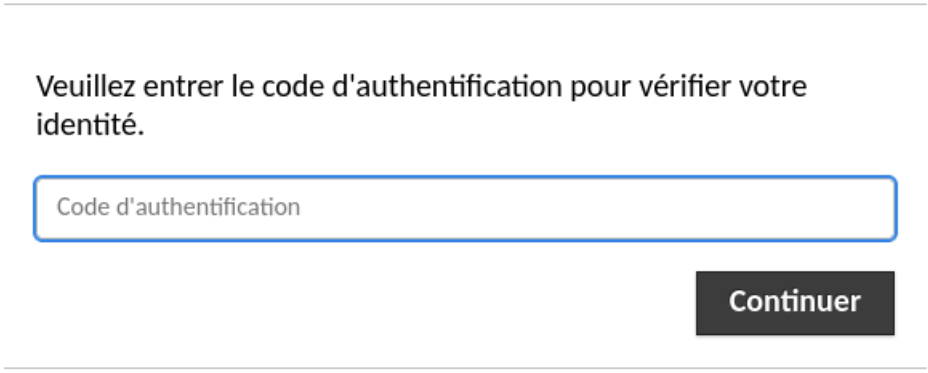

FIGURE 4.4 – Saisir le code après l'inscription a guacamole avec 2FA TOTP.

En tant qu'administrateur, nous pouvons réinitialiser le secret TOTP de l'utilisateur ainsi que confirmer ou désactiver la connexion TOTP.

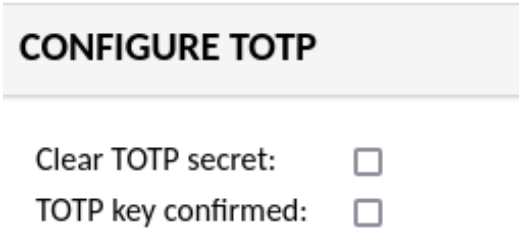

FIGURE 4.5 – Informations sur la configuration TOTP.

4.2.2 L'authentification DUO

Guacamole prend en charge Duo en tant que deuxième facteur d'authentification, superposé à toute autre extension d'authentification . L'extension d'authentification Duo permet aux utilisateurs d'être en outre vérifiés par rapport au service Duo avant que le processus d'authentification ne soit autorisé à réussir. Elle permet aussi d'offrir une possibilité de recevoir des notifications push pour connecter à guacamole.

4.2.2.1 Installer l'authentification Duo

L'extension d'authentification Duo est disponible séparément de l'extension principale guacamole.war.

Pour configurer l'authentification Duo sur Apache Guacamole, nous devons télécharger et installer l'extension qui correspond à la version de notre serveur Guacamole installé.

À partir de la page des versions : http ://guacamole.apache.org/releases/. Nous allons télécharger l'extension d'authentification Duo

```
root@debian:~# wget https://dlcdn.apache.org/guacamole/1.5.0/binary/guacamole-auth-duo-1.5.0.tar.gz
```

Nous allons Extraire l'extension

```
root@debian:~# tar -xvzf guacamole-auth-duo-1.5.0.tar.gz
```

Puis copier guacamole-auth-duo-1.5.1.jar dans etc/guacamole/extensions/.

```
root@debian:~/guacamole-auth-duo-1.5.0# cp guacamole-auth-duo-1.5.0.jar /etc/gua
camole/extensions/
```

4.2.2.2 Ajouter Guacamole au Duo

Tout d'abord, on doit créer un compte Duo gratuit, sur le lien : https ://duo.com/

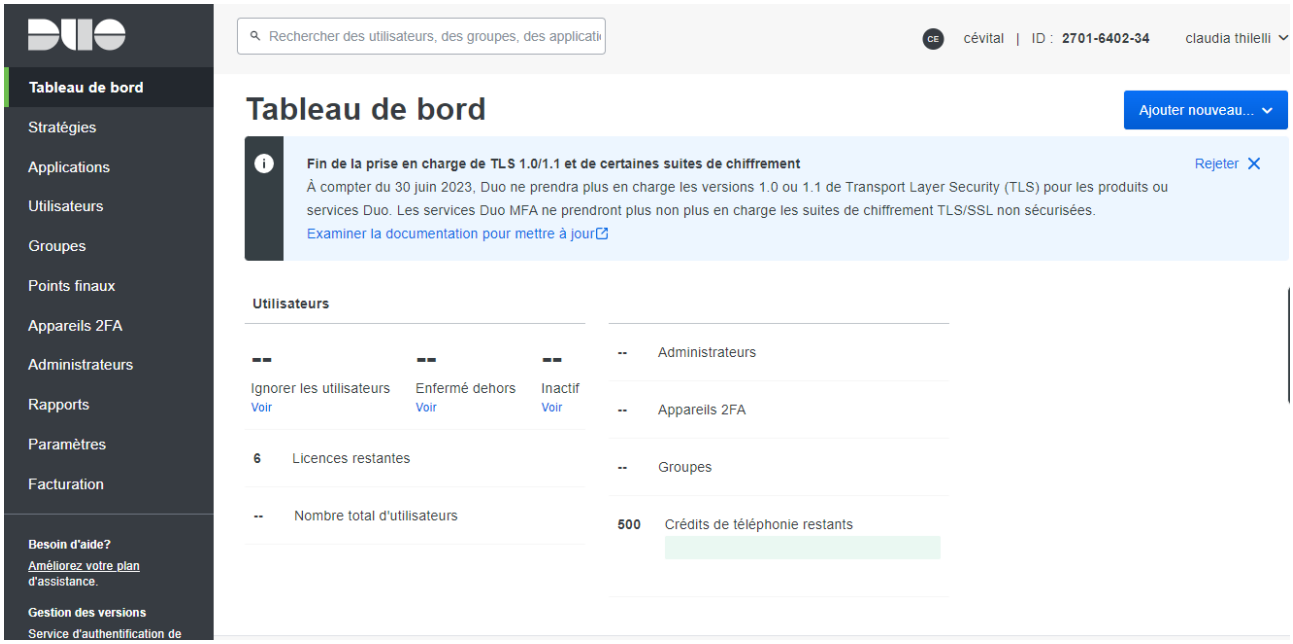

FIGURE 4.6 – Interface du compte Duo.

L'extension Duo de Guacamole utilise l'API d'authentification générique de Duo qu'ils appellent le "SDK Web". Pour utiliser Guacamole avec Duo, on doit l'ajouter en tant que nouvelle application "Web SDK" depuis l'onglet "Applications" du panneau d'administration de notre compte Duo , puis cliquer sur Protéger une application et choisir Web SDK.

FIGURE 4.7 – Application "Web SDK".

On défile vers le bas, dans les paramètres de Web SDK, on renomme l'application en quelque chose de plus représentatif que "Web SDK". Ce nom d'application est celui qui sera présenté aux utilisateurs lorsqu'ils seront invités par Duo à s'authentifier davantage

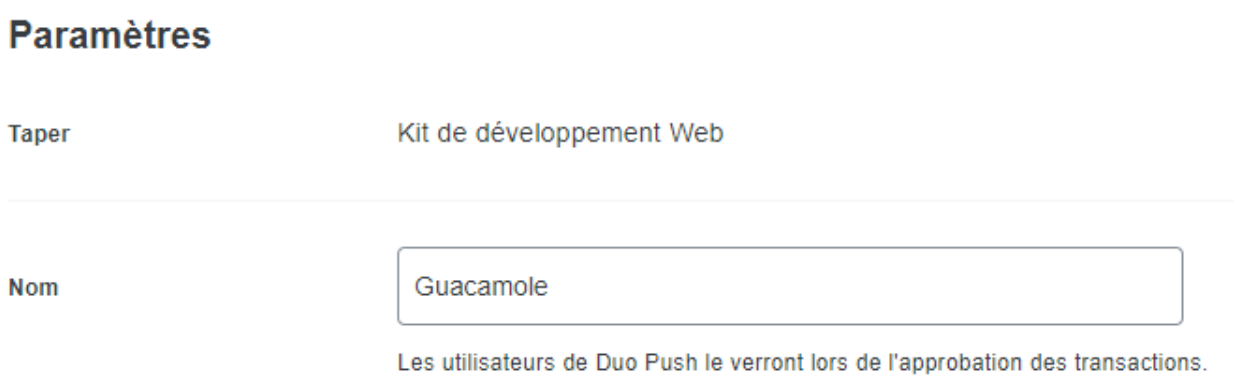

FIGURE 4.8 – Rennomage de l'application "Web SDK" à "Guacamole".

Afin de configurer Guacamole, nous avons besoin de trois informations qui sont répertoriées dans la section "Détails" de l'application : la clé d'intégration, la clé secrète et le nom d'hôte de l'API. On note ces éléments et on enregistre l'application nouvellement configurée.

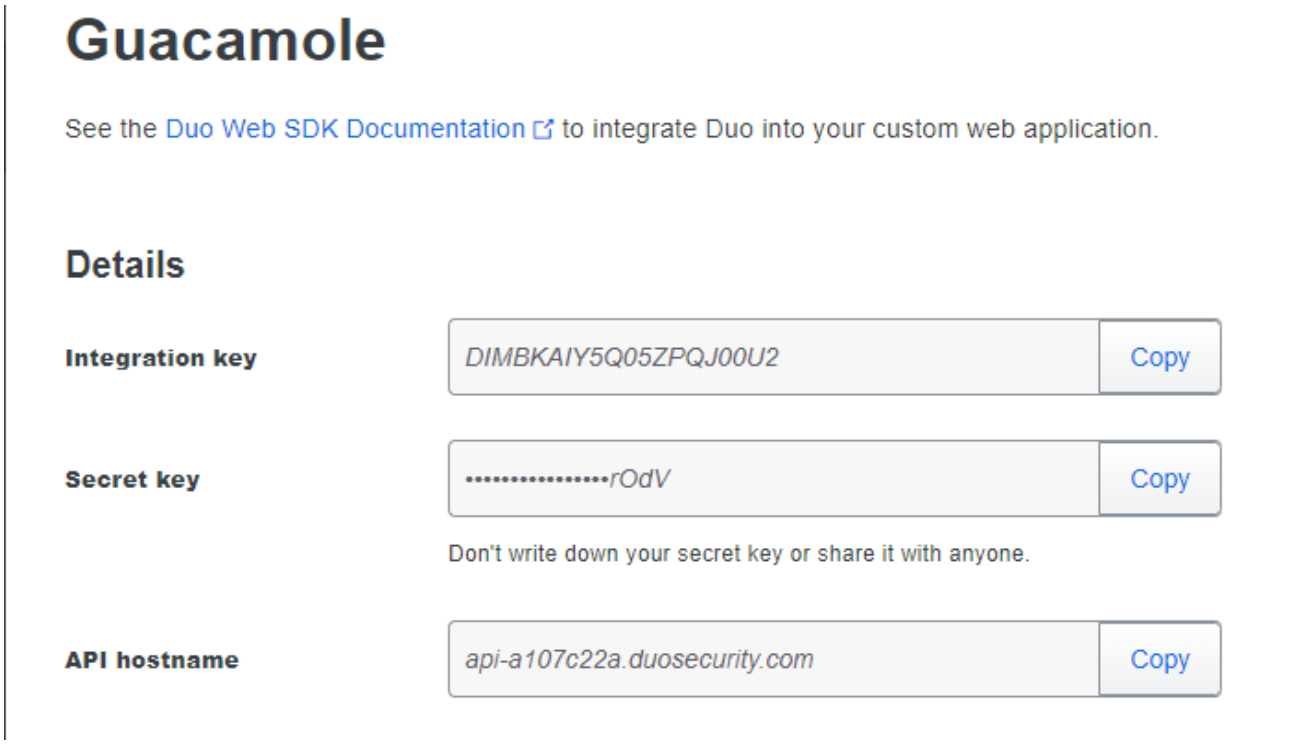

FIGURE 4.9 – Informations utilisées pour configurer Guacamole avec Duo.

4.2.2.3 Configurer Guacamole pour Duo

Les informations de configuration spécifiques à l'application récupérées à partir de Duo doivent être ajoutées dans guacamole.properties pour décrire comment Guacamole doit se connecter au service Duo : [39]

- **duo-api-hostname**
  Le nom d'hôte du point de terminaison de l'API Duo à utiliser pour vérifier les identités des utilisateurs. Elle est généralement sous la forme api-XXXXXXXX.duosecurity.com, où "XXXXXXXX" est une valeur alphanumérique arbitraire attribuée par Duo.
- **duo-integration-key**

La clé d'intégration fournie pour Guacamole par Duo. Elle est obligatoire et doit contenir EXACTEMENT 20 caractères.

- **duo-clé-secrète**
  La clé secrète fournie pour Guacamole par Duo. Elle est sensible et agit comme mot de passe de Duo pour l'application configurée. Cette valeur est obligatoire et doit contenir EXACTEMENT 40 caractères.
  Le dernier élément nécessaire à la configuration est "la clé d'application".
- **duo-application-key**
  Une clé arbitraire et aléatoire qu'on génére manuellement pour Guacamole. Cette valeur est obligatoire, doit être gardée secrète et comporter AU MOINS 40 caractères.
  Elle est requise par l'API d'authentification de Duo et destinée à être unique à chaque déploiement d'une application utilisant son API.

La clé d'application peut être générée avec la commande

```
root@debian:~# dd if=/dev/random count=1 | sha256sum
395556d58e030a016ee25097876dcfc30b45cad4e417783b608e955f7d13e090  -
```

Maintenant, les fichiers guacamole.properties doivent être mis à jour. On saisit le nom d'hôte de l'API, la clé d'intégration, la clé secrète et la clé d'application comme ci-dessous

```
#duo config
duo-api-hostname: api-a107c22a.duosecurity.com
duo-integration-key: DIMBKAIY5Q05ZPQJ00U2
duo-secret-key: bFAIBydbhGr12XHzDUBtNHh3DwTtH4K1sDMErOdV
duo-application-key: 395556d58e030a016ee25097876dcfc30b45cad4e417783b608e955f7d13e090
```

Enfin, il faut redémarrer les services tomcat9 et guacd pour lire les modifications de guacamole.properties et synchroniser l'heure du serveur.

4.2.2.4 Fonctionnement de DUO avec guacamole

Pour utiliser l'extension d'authentification Duo, un autre mécanisme d'authentification devra également être configuré. Lorsqu'un utilisateur tente de se connecter à Guacamole, les autres méthodes d'authentification installées seront interrogées en premier :
Nous avons implémenté cette solution 2FA DUO sur une autre machine virtuelle Debian.

FIGURE 4.10 – Première authentification simple de guacamole après l'ajout de 2FA DUO.

Ce n'est qu'une fois l'authentification réussie avec l'une de ces méthodes que Guacamole contactera Duo pour obtenir une vérification supplémentaire de l'identité de l'utilisateur.

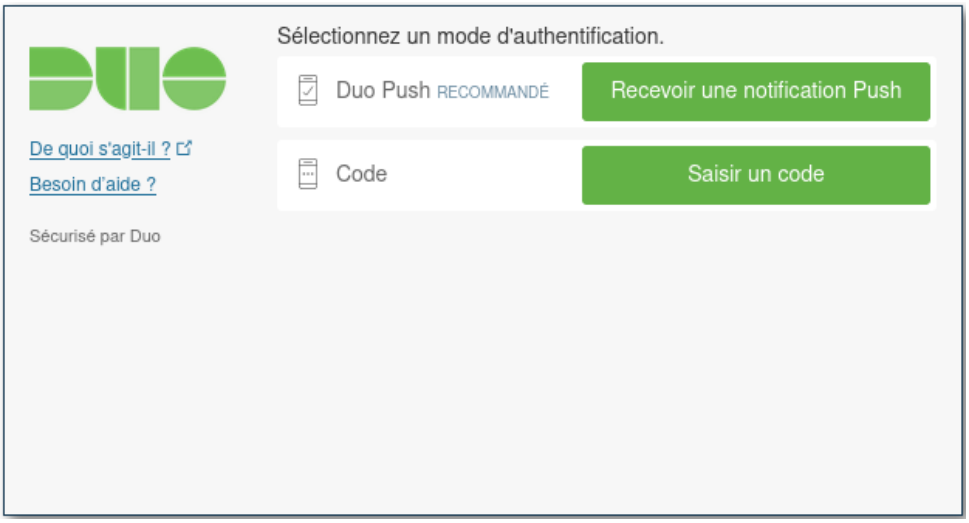

FIGURE 4.11 – Le choix d'authentification de 2FA DUO.

Si la tentative d'authentification initiale et la vérification via Duo réussissent, l'utilisateur sera autorisé à entrer. Si l'un ou l'autre des mécanismes échoue, l'accès à Guacamole est refusé.

4.2.2.5 Vérification de l'authentification à deux facteurs DUO sur Apache Guacamole

- Nous allons connecter à l'interface Web de Guacamole en tant qu'utilisateur. Une fois l'authentification initiale réussie, nous serons accueillis par une telle interface qui permet le démarrage de la configuration

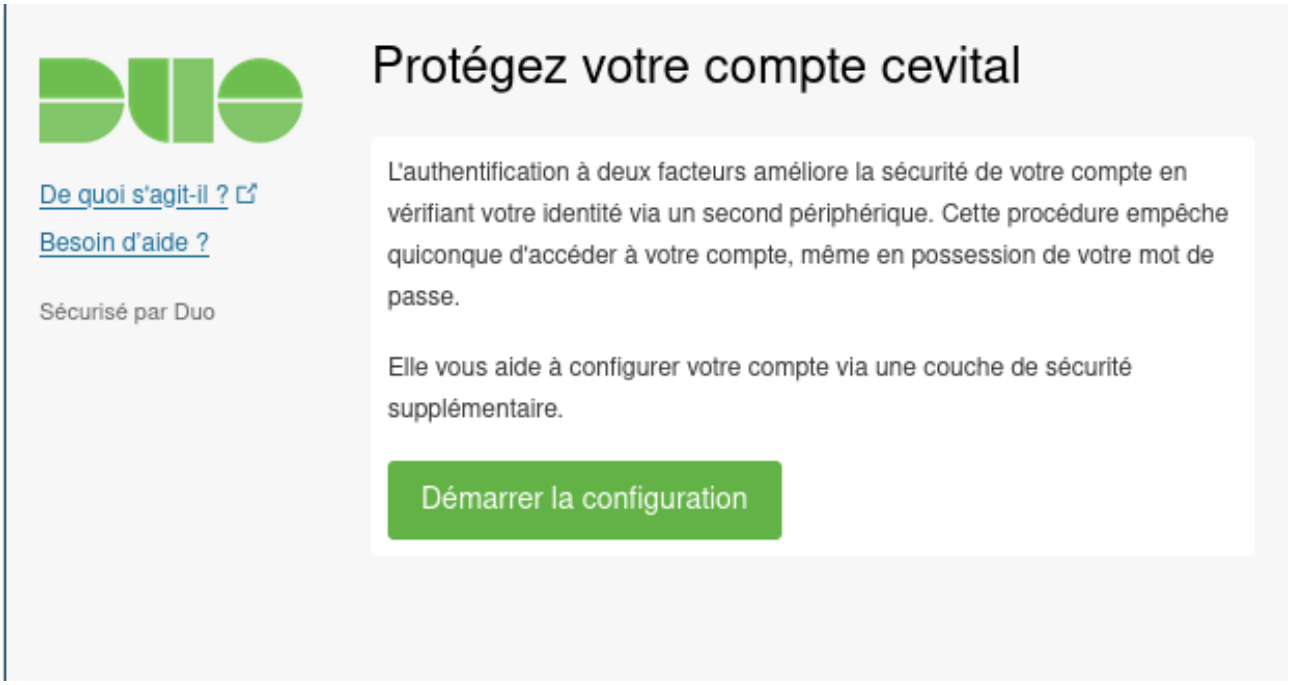

FIGURE 4.12 – Démarrage de la configuration de 2FA duo.

- Aprés avoir cliqué sur Démarrer la configuration, on va choisir le type de périphérique qu'on veut utiliser (Mobile, Tablette, Clé de sécurité) ainsi choisir le système qui convient avec nos périphériques(IOS ou Android)
- Dans cette interface il nous demande D'installer l'application Duo Mobile pour Android . une fois installée on clique sur "Lapplication Duo Mobile est installée"

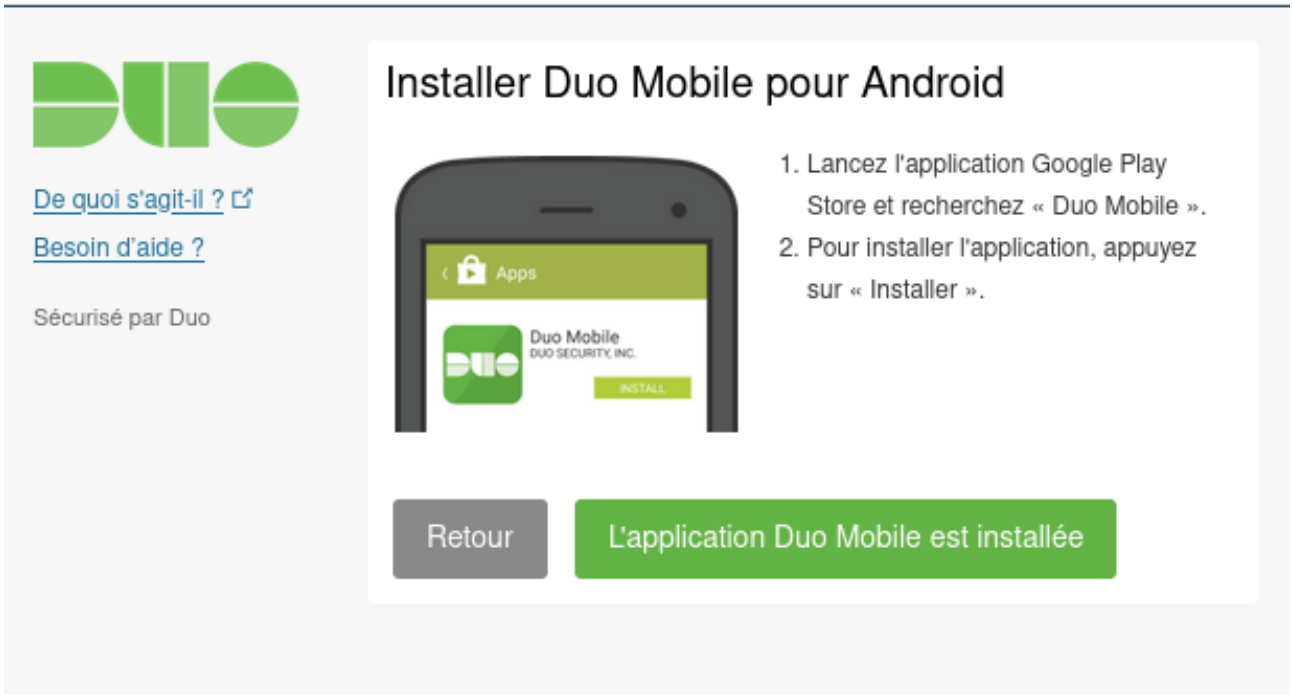

FIGURE 4.13 – Installation de l'application duo mobile pour android.

- On ouvre Duo Mobile sur notre Android puis on scanne le code QR affiché dans l'interface

FIGURE 4.14 – Scanner le QR pour 2FA DUO.

- Cette interface permet à l'utilisateur de choisir un mode d'authentification .

FIGURE 4.15 – Chousir la méthode d'authentification après une inscription réussite de 2FA DUO.

- Si on choisit Duo Push, on va recevoir une notification dans l'application Duo Mobile sur notre android

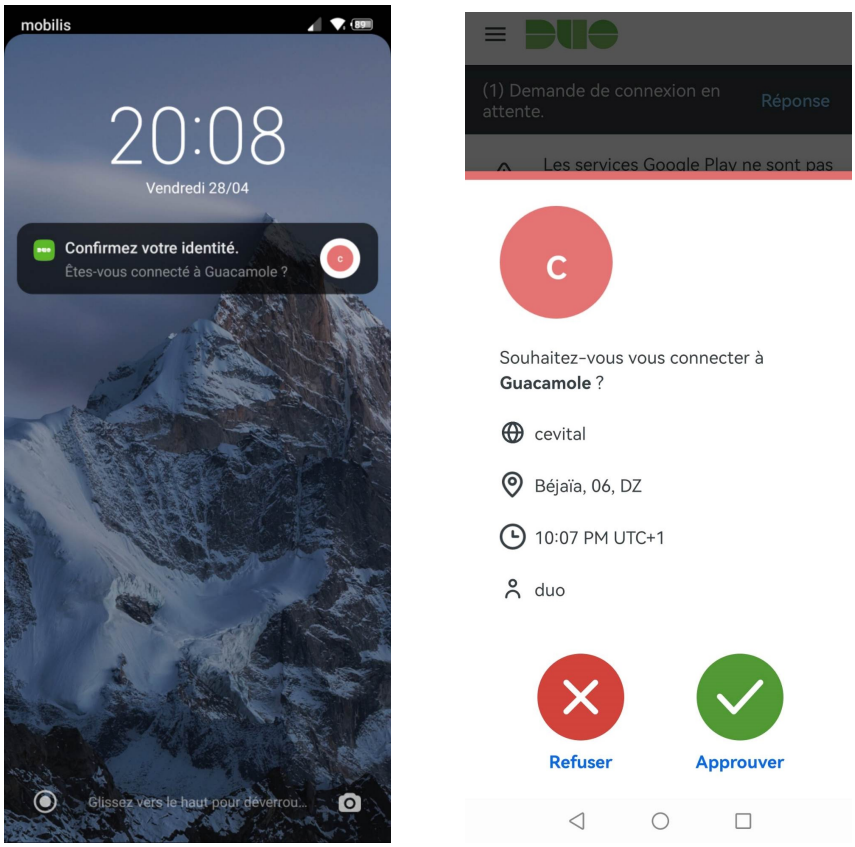

FIGURE 4.16 – La réception d'une notification à l'app DUO Mobile avec le choix d'authentification 'DUO PUSH'.

4.3 Conclusion

Au cours de ce chapitre, nous avons implémenté la solution de sécurité, que nous avons proposé pour la passerelle d'accès à distance guacamole. Nous avons présenté des outils importants puis nous avons donné toutes les étapes de configuration nécessaires de ces outils.

Dans le prochain chapitre nous allons montrer également des tests permettant la confirmation de la bonne implémentation et configuration de la sécurisation effectuée.

Chapitre 5

Mise en service et test

5.1 Introduction

Dans ce dernier chapitre, nous allons voir des cas pratiques concernant le déploiement et la sécurisation de la passerelle d'accès à distance par les 2 méthodes utilisées. Nous allons effectuer quelques tests que nous avons réalisés en lançant quelques attaques par des utilisateurs non légitimes et voir comment cette application faire face à ces dernières.

5.2 Interfaces de l'application

Dans ce qui suit, nous allons présenter quelques interfaces de l'application "Guacamole".

5.2.1 La liste des utilisateurs

En cliquant sur "Utilisateurs" dans la liste des sections de paramètres, on va accéder à l'écran de gestion des utilisateurs. Ici, on peut ajouter de nouveaux utilisateurs, modifier les propriétés et les privilèges des utilisateurs existants et afficher les heures auxquelles chaque utilisateur s'est connecté pour la dernière fois. Si on a un grand nombre d'utilisateurs, on peut également saisir des termes de recherche dans le champ "Filtre" pour filtrer la liste des utilisateurs par nom d'utilisateu [40].

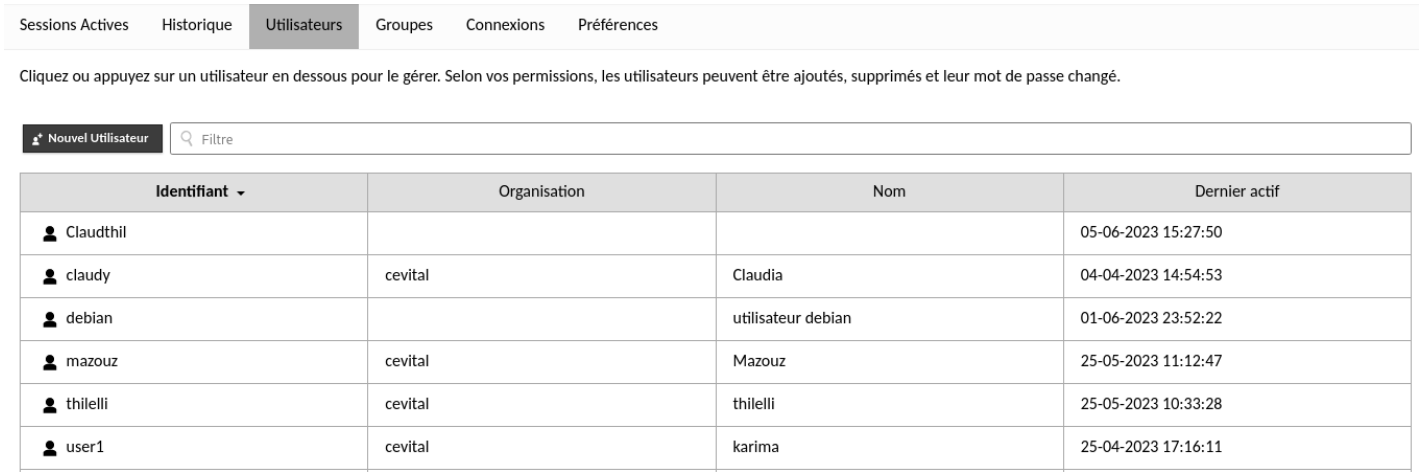

FIGURE 5.1 – Liste utilisateurs.

5.2.2 La liste des groupes utilisateurs

En cliquant sur "Groupes" dans la liste des sections de paramètres, on va accéder à l'écran de gestion des groupes d'utilisateurs. Ici, on va ajouter de nouveaux groupes et modifier les propriétés et les privilèges des groupes existants. Si on a un grand nombre de groupes d'utilisateurs, on peut également entrer des termes de recherche dans le champ « Filtre » pour filtrer la liste des groupes par nom [40].

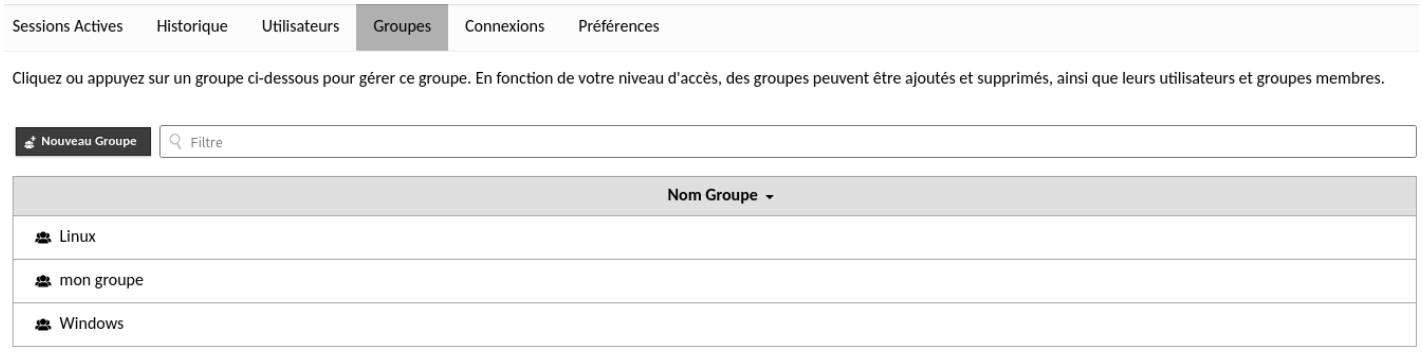

FIGURE 5.2 – List des groupes utilisateurs.

5.2.3 La liste des connexions et groupes de connexions

En cliquant sur "Connexions" dans la liste des sections de paramètres, on va accéder à l'écran de gestion des connexions. L'écran de gestion des connexions permet aux administrateurs de créer et de modifier des connexions, des profils de partage et des groupes de connexion. Si on dispose d'un grand nombre de connexions, on peut également entrer des termes de recherche dans le champ "Filtre" pour filtrer la liste des connexions par nom ou protocole [40].

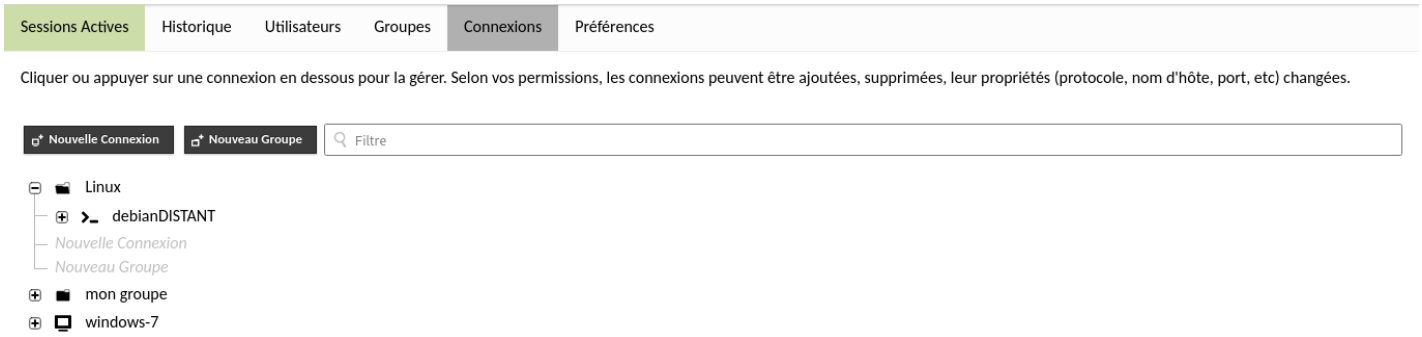

FIGURE 5.3 – Liste des connexions et groupes de connexions.

5.3 Test

Cette activité consiste à tester les résultats de l'implémentation pour s'assurer de la robustesse de notre passerelle du bureau à distance Guacamole et lutter contre les différentes attaques informatiques avec ses méthodes de sécurité puissantes.

5.3.1 Interface d'authentification

On va commencer par présenter l'interface de connexion des admins et des utilisateurs. Pour tester, nous avons rempli les champs spécifiques pour le loginet le mot de passe, après la validation, l'authentification est réussie.

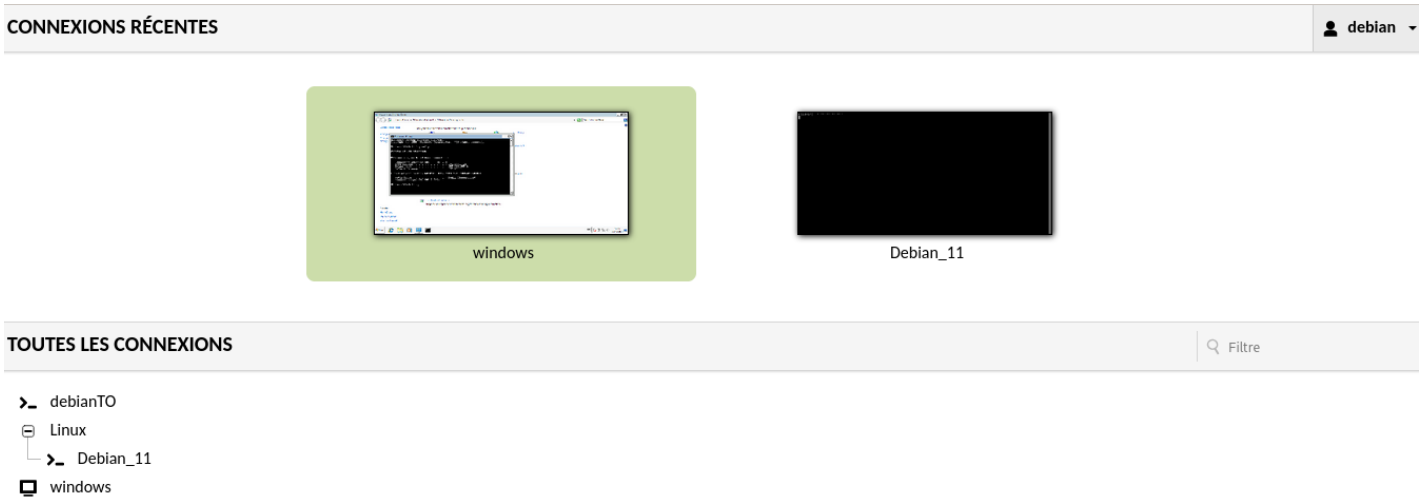

FIGURE 5.4 – Authentification admin.

5.3.2 Accès rejeté pour un individu intrus

Si un utilisateur non légitime tente d'accéder avec le même nom d'utilisateur mais avec un mot de passe différent, l'accès est rejeté.

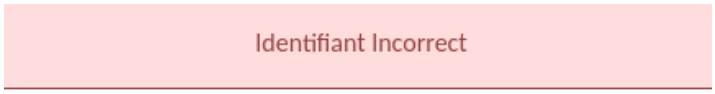

FIGURE 5.5 – accès rejeté.

5.3.3 Désactiver le compte d'un utilisateur

Si l'admin a remarqué une action non voulue d'un utilisateur, il peut désactiver son compte après une telle date ou ne pas lui autoriser l'accès après un moment donné suite à une action non habituée.
Cette fonctionnalité est utilisée aussi pour désactiver les comptes utilisateurs qui ne sont plus utilisés.

FIGURE 5.6 – desactiver un compte utilisateur.

Maintenant, on passe pour tester le degré de sécurité de l'application Guacamole en implémentant les deux méthodes d'authentification à deux facteurs (2FA) : la méthode TOTP et DUO.

5.3.4 Authentification avec la méthode 2FA TOTP

Cette méthode permet de vérifier l'identité de l'utilisateur en envoyant un code de six chiffres à l'application d'authentification à 2FA sur le téléphone de l'utilisateur légitime.

Si un utilisateur malveillant essaie d'accéder à la passerelle de bureau à distance en connaissant les identifiants d'un utilisateur légitime ; l'accès est refusé avec TOTP car la vérification du code est échouée.
le code de validation sera recu par le propriétaire du compte, ce qui implique que quelqu'un d'autre a essayé d'accéder à son compte donc il est dans l'obligation de changer son mot de passe.

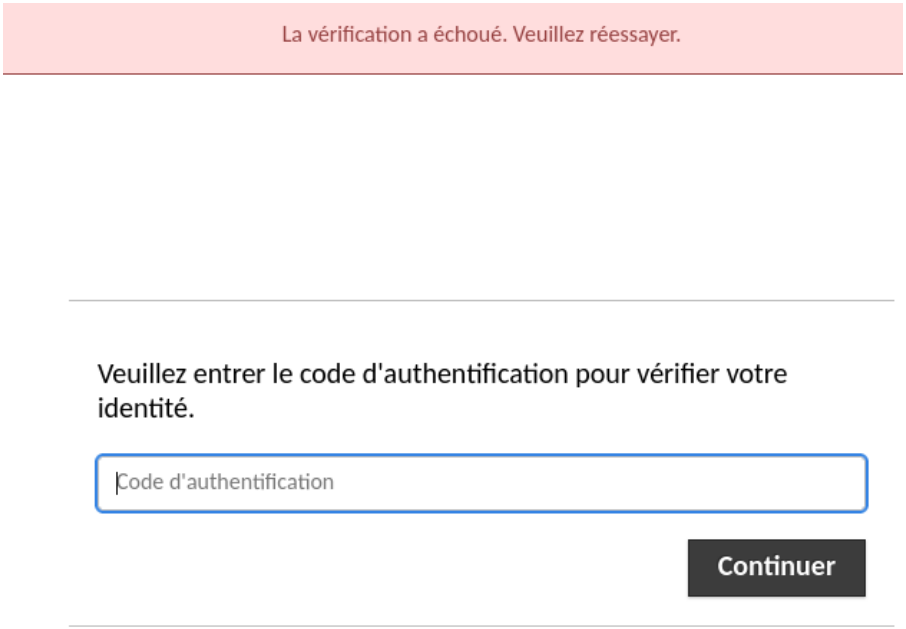

FIGURE 5.7 – Vérification du code est échouée.

5.3.5 Authentification avec la méthode 2FA DUO

Cette méthode utilise deux modes d'authentification pour vérifier l'identité de l'utilisateur : envoyer un code de six chiffres ou recevoir une notification Push sur l'application Duo Mobile installée sur le téléphone de l'utilisateur légitime.

Si un attaquant essaie d'accéder à guacamole avec les identifiants de cet utilisateur légitime ; l'accès est refusé car :

- La vérification du code est échouée :

FIGURE 5.8 – Vérification du code est échouée.

- S'il choisit de rececvoir une notification push :
  Il va attendre une durée du temps puis la connexion sera interrompue, car la notification Push va etre recue par la proprietaire du compte sur l'application Duo mobile installée sur son téléphone, ce qui implique que quelqu'un d'autre a essayé d'accéder à son compte donc il doit changer son mot de passe.

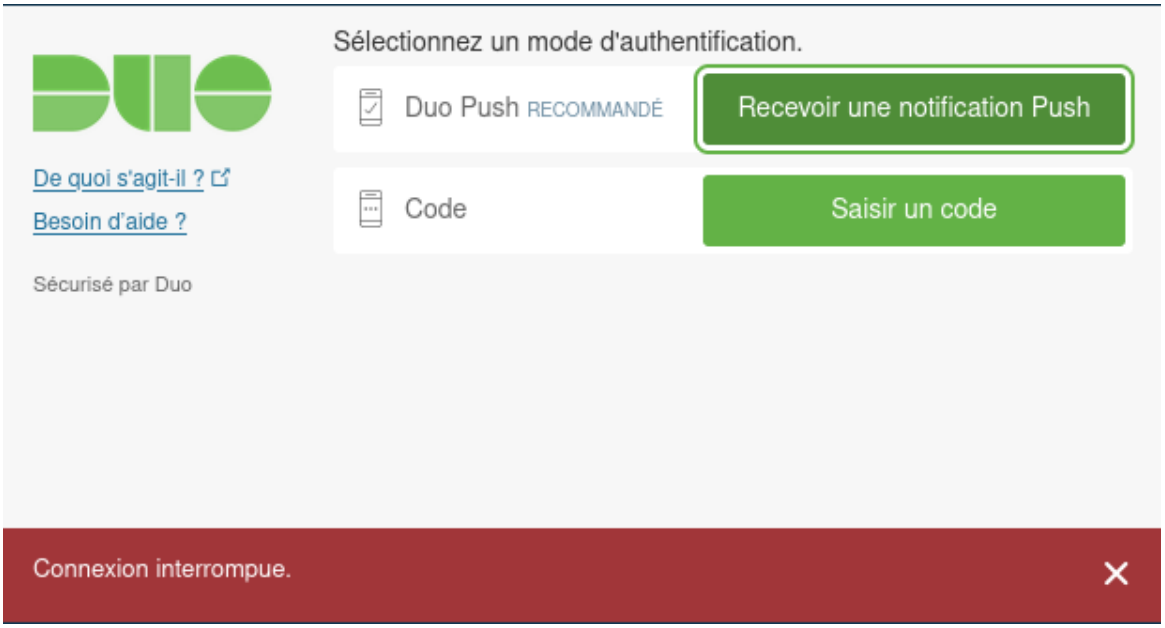

FIGURE 5.9 – Connexion interrompue.

5.4 Conclusion

Ce dernier chapitre décrit la phase de mise en service et tests, où nous avons présenté quelques interfaces de notre application. Aussi, nous avons éffectué des tests afin de garantir sa fiabilité et robustesse contre les différentes attaques.

Conclusion générale

Ce travail nous a permis d'acquérir une expérience professionnelle intéressante. Nous avons amélioré nos connaissances et compétences en terme de configuration dans un environnement virtuel, qu'est VirtuelBox. De plus nous avons perfectionné nos connaissances dans le domaine de la *sécurité d'accès à distance* dans une entreprise grâce à l'implémentation d'une *passerelle de bureau à distance*, qui est *Guacamole*.

Ce document est divisé en 5 chapitres, **le premier** qui est intitulé *"Présentation de l'organisme d'accueil"* comprend deux parties, la première a porté sur l'étude de l'établissement d'accueil, sur la direction des systèmes d'informations DSI, qui nous a permis de prendre connaissance des différentes failles de sécurité Informatique du CEVITAL, et la deuxième a porté sur le contexte de notre projet, problématique et les solutions proposés.

Le second chapitre s'est axé sur le volet théorique, il a porté sur les différents aspects de sécurité informatique afin de mettre en évidence la nécessité de mettre en place des mécanismes de défense contre les attaques. Ainsi une étude globale sur l'accès à distance sécurisée avec l'explication du principe de Guacamole, ses différents avantages et limites.

L'aspect pratique a fait l'objet du troisiéme chapitre, qui comporte à son tour trois parties, dont la première a porté sur la spécification des différents environnements de développement, matériels et logiciels, la deuxiéme a porté sur les différentes étapes d'installation et configuration pour la mise en place de la passerelle de bureau à distance GUACAMOLE et enfin, la troisième a porté sur l'utilisation de cette dernière.

La réalisation des solutions proposées est faite dans le quatrième chapitre, qui nous a permis de connaitre les différents concepts d'authentification à deux facteurs liés aux *TOTP et DUO*, ainsi que les notions et principes de fonctionnement. Il nous a abouti à des amélioration de sécurité dont en premier lieu, *2FA TOTP* pour générer des codes de connexion temporaires à usage unique, puis à l'implémentation de *2FA DUO* pour offrir également la possibilité de recevoir des notifications push pour connecter à guacamole.

Le résultat des tests de notre solution est présenter dans le dernier chapitre, où nous avons présentation des cas pratiques concernant le déploiement et la sécurisation de la passerelle d'accès à distance.

Ce travail nous a permis d'avoir une visibilité concrète sur un domaine très important, qui est la sécurité Informatique et l'accès à distance. Il est clair que le stage au sein de l'entreprise CEVITAL de Béjaïa a été très bénéfique quant à l'application de nos connaissances scientifiques et jumelage de la théorie et la pratique.

Perspectives :

Comme perspective de notre travail :

- Nous proposons de renforcer la sécurité en ajoutant des foncionalités supplimentaires tel que la gestion des identités et des accès en utilisant d'autres méthodes d'authentification comme la biometrie.
- Ajouter un autre mode de sécurité pour l'authentification DUO qui est les appelles téléphoniques.
- La mises à jour quotidienne de l'application pour se prévenir contre des nouvelles attaques.

Bibliographie

[1] Cevital,2016. Disponible sur : http ://www.cevital.com/[consulté le 07/05/2023].

[2] KHIREDDINE, Rahim, 2023. Cevital presentation[en ligne]. Disponible sur : https ://prezi.com/p/jcsq6mgwo_xj/cevital-presentation/[consulté le 14/04/2023].

[3] KEMACHA, Habiba, ALOUACHE, Lynda, 2021. La Haute Disponibilité des Réseaux (HSRP). Mémoire de Master. Informatique. Bejaia : Université Abderrahmane Mira.

[4] Ferchouli, Sylia, Gherabi, Salima, 2021. Le rôle des relations publiques 2.0 dans l'amélioration de l'e-réputation de l'entreprise. Mémoire de Master. Communication et Relations Publiques. Bejaia : Université Abderrahmane Mira.

[5] BOUKOUCHA, Ilhem, CHALOUR, Yasmina, 2021. Mise en Place d'une Plateforme de Transfert de Fichiers Sécurisé. Mémoire de Master. Informatique. Bejaia : Université Abderrahmane Mira.

[6] AGGOUN, Sarra, BELKACEM, Sabrina, 2013. Mise en oeuvre d'une solution de sécurité basé sur les IDS Cas d'étude : entreprise Cevital. Mémoire de Master. Informatique. Bejaia : Université Abderrahmane Mira.

[7] AZEROUK, Nassim, BENMOUHOUB, Djamel, 2019. Urbanisation des systèmes d'informations et étude de migration vers des solutions cloud (Infrastructure Openstack). Mémoire de Master. Informatique. Bejaia : Université Abderrahmane Mira.

[8] Smahi, Imene, Tabta, Hanane, 2021. Mise en place d'un IDS en utilisant SNORT Cas d'´etude : CEVITAL. Mémoire de Master. Informatique. Bejaia : Université Abderrahmane Mira.

[9] Alain Fernandez, 16 mars 2023. Comment sécuriser le Système d'Information ? [en ligne]. Disponible sur : https ://www.piloter.org/systeme-information/securite informatique.htm[consulté le 15/05/2023].

[10] bakeli. Pourquoi la sécurité informatique est-elle importante ?[en ligne]. Disponible sur : https ://www.bakeli.tech/pourquoi-la-securite-informatique-est-importante/[consulté le 04/06/2023].

[11] GODART, Didier, 2002. Sécurité Informatique Risques,Stratégies et Solutions. Deuxiéme Edition. Belgique : L.Venanzi, 471 p. ISBN 2-930287-21-7.

[12] BOUKHAROU, Radja, 2019. Sécurité des réseaux. Support de cours. Réseaux et Systèmes Distribués. Constantine : Université Abdelhamid Mehri - Constantine 2.

[13] CARPENTIER, Jean-Francois, 2009. La sécurité informatique dans la petite entreprise :Etat de l'art et bonnes pratiques. France : Edition ENI, 276 p. DataPro. ISBN 978-2-7460-4820-1.

[14] NICHAN, Margossian, 2011. Risques professionnels, 2eme édition. Paris : Dunod, 496 p. Technique et ingénierie - Environnement et sécurité. 978-2-10-055795-0 .

[15] QUINTON, Eric, 2017. La sécurisation d'une application web : Risque, chiffrement et traitement des vulnérabilité avec php. Great Britain : ISTE Editions Ltd, 209 p.

[16] SCRIBD, May 06, 2020. La Sécurité informatique[en ligne]. Disponible sur : https :fr.scribd.com /presentation/460243552/Securite-Informatique[consulté le 19/05/2023].

[17] Authentification. Qu'est ce que l'authentification réseau ?[en ligne]. Disponible sur : https ://www.authentification.eu/quest-ce-que-lauthentification-reseau/[consulté le 14/05/2023].

[18] FrameIP.com. Protocole ssl et tls[en ligne]. Disponible sur : https ://www.frameip.com/ssl-tls/[consulté le 22/05/2023].

[19] CLOUDFLARE. Qu'est-ce que le protocole RDP (Remote Desktop Protocol) ?[en ligne]. Disponible sur : https ://www.cloudflare.com/fr-fr/learning/access-management/what-is-the-remote-desktop-protocol/[Consulté le 23/05/2023].

[20] Digital Guide IONOS. Telnet : qu'est-ce que c'est et comment l'activer ?[en ligne]. Disponible sur : https ://www.ionos.fr/digitalguide/serveur/outils/telnet/[consulté le 23/05/2023].

[21] Fatima Z, Mar 24, 2023. SSH : Comprendre et Mieux Utiliser ce Protocole[en ligne]. Disponible sur : https ://www.hostinger.fr/tutoriels/ssh-linux[consulté le 23/05/2023].

[22] La Rédaction TechTarget, février 2016. Ipsec[en ligne]. Disponible sur :https ://www.lemagit.fr /definition/IPsec[consulté le 22/05/2023].

[23] GlobalSign. Quelle est la différence entre HTTP et HTTPS ?[en ligne]. Disponible sur : https ://www.globalsign.com/fr/blog/la-difference-entre-http-et-https[consulté le 23/05/2023].

[24] John Carl Villanueva, December 11, 2022. Ssl vs ssh - a not-so-technical comparison[en ligne]. Disponible sur : https ://www.jscape.com/blog/ssl-vs-ssh-simplified[consulté le 22/05/2023].

[25] Poncelet, Nicolas, 2006. Accès à distance : fonctionnement, sécurité et implémentation. THÈSE. SCIENCES INFORMATIQUES. Namur Institut d'Informatique.

[26] NinjaOne.Qu'est-ce qu'un logiciel d'accès à distance ? Guide 2023 de l'accès à distance [en ligne]. Disponible sur : https ://www.ninjaone.com/fr/blog/guide-2023-logiciels-d-acces-a-distance/url [consulté le 21/05/2023].

[27] Vmware. l'accès distant sécurisé[en ligne]. Disponible sur : https ://www.vmware.com/fr /topics/glossary/content/secure-remote-access.html [consulté le 21/05/2023].

[28] Atera. QU'EST- CE QU'UN LOGICIEL D'ACCÈS À DISTANCE ?[en ligne]. Disponible sur :https ://www.atera.com/fr/en-quoi-consiste-un-[consulté le 21/05/2023].

[29] SEKENS. APACHE GUACAMOLE – VDI[en ligne]. Disponible sur : https ://www.sekens.fr /hebergement-et-cloud/apache-guacamole-vdi/[consulté le 18/05/2023].

[30] ORACLE, June, 2021. Oracle VM VirtualBox Overview.

[31] Virtualbox. Télécharger virtual box[en ligne]. Disponible sur : https ://www.virtualbox.org /wiki/Downloads[consulté le 03/03/2023].

[32] Alexis de Lattre, 2002. Formation Debian GNU/Linux.

[33] techopedia, 5 September, 2018. Debian GNU/Linux[en ligne] . Disponible sur : https ://www.techopedia.com/definition/18746/debian-gnulinux[consulté le 04/03/2023].

[34] Apache Guacamole. Implementation and architecture[en ligne]. Disponible sur : https : //guacamole.apache.org/doc/gug/guacamole-architecture.html[consulté le 24/04/2023].

[35] Rdr-it. Guacamole : gérer les accès à votre environnement informatique [en ligne]. Disponible sur : https ://rdr-it.com/guacamole-gerer-acces-environnement-informatique/[consulté le 27/04/2023].

[36] Boris Tougma, Jul 3, 2022. Guacamole : Serveur de connexion à distance[en ligne]. Disponible sur : https ://boris-cyber.hashnode.dev/guacamole-serveur-de-connexion-a-distance[consulté le 26/04/2023].

[37] Apache guacamole. Chapitre 5. Configuration de Guacamole[en ligne]. Disponible sur : https ://guacamole.apache.org/doc/1.1.0/gug/configuring-guacamole.html[consulté le 18/05/2023].

[38] Kifarunix, April 9, 2022. Configure TOTP Two-Factor Authentication on Apache Guacamole[en ligne]. Disponible sur : https ://kifarunix.com/configure-totp-two-factor-authentication-on-apache-guacamole/[consulté le 30/04/2023].

[39] ApacheGaucamole. Duo two-factor authentication[en ligne]. Disponible sur : https : //guacamole.apache.org/doc/gug/duo-auth.html[consulté le 27/04/2023].

[40] ApacheGuacmole. Administration[en ligne]. Disponible sur :https ://guacamole.apache.org /doc/gug/administration.html[consulté le 26/05/2023].

Résumé

L'Informatique a atteint une prodigieuse évolution technologique dans différents domaines qui a conduit de plus en plus à l'évolution du mode et des méthodes de travail. Les technologies peuvent rendre les taches plus souples. En effet, elles permettent aux utilisateurs d'accéder à distance à des ressources informatiques telles que des fichiers et les applications , ce qui considérablement améliore la productivité et la flexibilité. L'objectif de ce mémoire est de répondre au problème de sécurité de l'accès distant. Pour atteindre cet objectif, nous avons déployé une passerelle de bureau à distance sécurisée *« Guacamole »* qui peut être utile pour travailler à distance et accéder aux bureaux et applications depuis n'importe quel endroit. Deux méthodes de sécurisation à savoir, l'authentification à deux facteurs *TOTP*, et *DUO* sont déployées afin de renforcer la sécurité de l'accès distant et permettre aux administrateurs de surveiller les utilisateurs lors de leurs connexion, ce qui permet de détecter toute activité suspecte. Nous avons effectué une série de tests pour assurer que la passerelle fonctionne correctement et que les utilisateurs peuvent se connecter en toute sécurité. Les résultats des tests montrent que la passerelle est efficace et sécurisée.

Mots-clés : Sécurité informatique, Accès distant sécurisé, Passerelle de bureau à distance, Guacamole, Authentification à deux facteurs, TOTP, DUO.

Abstract

Computing has reached a prodigious technological evolution in different fields which has led more and more to the evolution of the mode and methods of work. Technologies can make stains softer. Indeed, they allow users to access distance to computer resources such as files and applications, which consi-dramatically improves productivity and flexibility. The purpose of this dissertation is to answer remote access security issue. To achieve this goal, we deployed a *« Guacamole»* secure remote desktop gateway that can be useful for working remotely and access desktops and applications from anywhere. This project carries also on the deployment of the two security methods : two-factor authentication *TOTP*, and *DUO* in order to strengthen the security of remote access and allow administrators to monitor users during their connection, which makes it possible to detect any activity suspicious. It also explores the pros and cons of Guacamole versus to other remote desktop solutions. Finally, this work encompasses the different aspects of computer security and secure remote access to ensure the robustness of a system information against the various computer attacks by using security methods powerful laughter.Also includes performing tests to ensure the gateway is working properly and users can connect securely. Test results show that the gateway is efficient and secure.

Keywords : Computer Security, Secure Remote Access, Remote Desktop Gateway, Guacamole, Two-Factor Authentication, TOTP, DUO.