République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira de Béjaia

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

Mise en place d'une solution PAM (la gestion des accès privilégie) au sein de « groupe IFRI »

Réalisé par :

ATMAOUI Idir

DAHMANI Cylia

Devant le jury:

Présidente : M^{me} HOUHA Amel

Examinateur : M^{r} SAADI Mustapha

Promoteur : M^{r} TOUAZI Djoudi

Promotion: 2020/2021

Remerciement

Tout d'abord, nous remercions Dieu, notre créateur de nous avoir donné la force, la volonté et le courage afin d'accomplir ce modeste travail.

Et nous adressons nos vifs remerciements et notre gratitude Â :
Nos familles, surtout nos parents qui nous ont épaulés, soutenus et suivis tout au long de ce projet.

Nous tenons à adresser nos plus profonds et sincères remerciements à notre encadreur ***Dr TOUAZI Djoudi****, pour nous avoir encadrés et guidés tout au long de ce projet, pour tous ses conseils et ses encouragements, pour sa disponibilité et sa compréhension.*

Non sincères remercîments vont à ***Mr HAROUG Aimad*** *et* ***Mr HIDOUS Abdelhakim*** *nos encadreurs de l'entreprise IFRI, pour leur encadrement avec Patience. Leur encouragement et leurs remarques pertinentes nous ont permis de mieux structurer ce travail. Nous les remercions aussi de nous avoir fait profiter de leurs expériences, leurs orientations et leurs conseils nous ont énormément aidés.*

Aussi à tous les enseignants et employés du département Informatique à qui on doit notre avancement.

Nous tenons aussi à remercier également tous les membres de jury pour avoir accepté d'évaluer notre travail.

Enfin, nous remercions tous ceux qui nous ont soutenu et aidé dans la réalisation de ce mémoire de près ou de loin

Dédicaces

À ma mère

Affable, honorable, aimable : Tu représentes pour moi le
Symbole de la bonté par excellence, la source de tendresse et
L'exemple du dévouement. Tu n'as pas cessé de m'encourager
Ta prière et ta bénédiction m'ont été d'un grand secours
Pour mener à bien mes études.
Aucune dédicace ne saurait être assez éloquente pour
Exprimer ce que tu mérites pour tous les sacrifices que tu n'as
Cessé de consentir depuis ma naissance.
Tu as fait plus qu'une mère puisse faire pour que ses
Enfants suivent le bon chemin dans leur vie et leurs études.
Je te dédie ce travail en témoignage de mon profond
Amour. Puisse Dieu, le tout puissant, te préserver et
T'accorder santé, longue vie et bonheur.

À mon Père

Rien au monde ne vaut tes efforts fournis jour et
Nuit pour mon éducation et mon bien être.
Ce travail est le fruit de tes sacrifices.

Aucune dédicace ne saurait exprimer l'amour,
L'estime, et le respect que j'ai toujours eu
Pour toi.

Toi qui es pour moi un exemple

A ma sœur, mes frères et ma belle-sœur et à mon amour « Yasmine N ».

A toute la famille ATMAOUI & BOUGHERRIOU.

Ils vont trouver ici l'expression de mes sentiments de respect et de reconnaissance pour le soutien qu'ils n'ont cessé de me porter.

A tous mes professeurs :

Leur générosité et leur soutien m'oblige de leurs témoigner mon profond respect et ma loyale considération.

A mes chères ami(e)s :

Adel M, Adel L, Amine B, Azdine B, Azdine T, Aris T, Djamal B, Fouad A, Farouk K, Gaya C, Lyes Ait, Mimoun M, Meziane A, Nabil Ait, Nassim A, Oussama M, Sofiane B, Sarah C, Yasmine M.

Je ne peux trouver les mots justes et sincères pour vous exprimer mon affection et mes pensées, vous êtes pour moi des frères, sœurs et des amis sur qui je peux compter.

En témoignage de l'amitié qui nous uni et des souvenirs de tous les moments que nous avons passés ensemble, je vous dédie ce travail et je vous souhaite une vie pleine de santé et de bonheur.

Idir A

Table des matières

Chapitre III: Conception

Chapitre IV: Réalisation

Table des figures

Liste des tableaux

Glossaire

CERT *Computer Emergency Readiness ou Response Team*

Un centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations, mais dont les informations sont généralement accessibles à tous.

DNS *Domain Name Système*

Service disponible dans un environnement TCP/IP permettant de résoudre des noms dutype www.eni.fr en adresse IP. s'est le service d'annuaire « machines» d'internet.

DMZ *DeMilitarized Zone*

Correspond en informatique à un sous-réseau encadré de pare-feu, situé généralement entre le réseau local et l'Internet. Cet emplacement héberge les serveurs qui seront accessibles depuis l'Internet en passant le pare-feu externe généralement au travers d'un mécanisme de translation d'adresses ou de port.

FTP *File Transfer Protocol*

Est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP.

HTTP *Hyper Text Transfer Protocol*

Protocole de transfert de fichiers permettant d'acheminer tous types d'informations.

ICA *Independent Computing Architecture*

Utilisé par les serveurs Citrix Présentation Server. Ces serveurs permettent la mise en place d'une architecture client léger / serveur. Toutes les applications sont gérées par le serveur, le client ne se charge que des entrées/sorties.

IPS *intrusion prevention system*

Une forme de sécurité de réseau qui sert à détecter et prévenir les menaces identifiées.

LAN *Local Area Network*

Réseau à l'étendue géographique limitée.

PAM *Privileged Access Management*

Pare-feu avec solution de gestion des accès privilégie

PET *Polyéthylène Téréphtalate*

Un plastique pétrosourcé : les monomères utilisés, l'éthylène glycol et l'acide téréphtalique, sont issus de la transformation du pétrole.

RDP Remote Desktop Protocol

C'est un protocole, ou une norme technique, permettant d'utiliser un ordinateur de bureau à distance.

RSSI *Responsables de la Sécurité du Système d'Information*

SARL *Statut de la société à Responsabilité Limitée*

Comme son nom l'indique, la Sarl est une société qui se caractérise par la responsabilité limitée des associés : leur perte potentielle se limite au montant de leurs apports respectifs. Il s'agit de la forme de société la plus répandue en France.

SSH *Secure Shell*

est à la fois un programme informatique et un protocole de communication sécurisé.

TCP/IP *Transmission Control Protocol/ Internet Protocol*

Familles de protocoles mondialement connue, indépendante de la couche Physiqueutilisée.

VNC *Virtual Network Computing*

Un système de visualisation et de contrôle de l'environnement de bureau d'un ordinateur distant.

VPN *Virtual Private Network*

Connexion privée (c'est –à-dire protégée, dont le contenu des échanges est chiffré) engénéral sur un réseau public (tel qu'Internet).

Introduction générale

De nos jours, l'une des préoccupations de toute entreprise réside dans le développement et l'implémentation d'une méthode de protection de leurs systèmes d'informations ou de données. Beaucoup d'entreprises économiques à vocation productives détenant des informations précieuses doivent impérativement assurer leur sécurité. Un bon nombre d'informations sont stockées dans des systèmes informatiques, il est de plus en plus nécessaire de les protéger du point de vue intégrité, confidentialité et disponibilité. La protection de ces informations contre une utilisation non autorisée est donc devenue un problème majeur. Ce qui impose un contrôle d'accès rigoureux et fiable aux données.

Notre objectif consiste à donner aux utilisateurs internes et aux clients le droit de manipuler ou de consulter des ressources locales de l'entreprise dans un cadre organisé et réglementaire. Il est nécessaire et vital d'installer un système de contrôle d'accès avec un accès privilégié au système d'information et des contraintes comme la traçabilité, la durée de session et le temps pour accéder au serveur etc...

Dans le cadre de notre stage, nous sommes appelés à faire la mise en place d'une solution de Gestion d'accès privilégiés PAM (Privileged Access Management) à l'aide d'une application Wallix Bastion qui est recommandée. La solution PAM attendue doit créer une véritable sécurisation du système de l'entreprise qui va permettre de valider complètement l'identité des personnes accédant à notre système, en le laissant effectuer des tâches d'autorisation et d'authentification de compte qui restent toujours séparées de notre environnement existant.

Ce mémoire sera subdivisé en quatre chapitres :

Dans le premier sera consacré à présenter l'environnement de notre travail dont l'organisme d'accueil qui est l'entreprise GROUP IFRI où nous avons effectué notre stage.

Dans le deuxième chapitre, nous nous intéressons à la description des généralités sur la sécurité des réseaux informatiques.

Le troisième chapitre présente une vue générale sur les concepts fondamentaux des PAM, le déploiement de la solution Wallix Bastion, l'architecture qui est en cours d'installation par la direction des systèmes d'information et celle que nous proposons.

Enfin, le dernier chapitre présente la réalisation de notre travail qui consiste à la description des étapes suivies pour l'installation et la configuration de Windows server et Wallix Bastion ainsi que les étapes à suivre pour l'utilisation de ces derniers.

Chapitre I

Présentation de l'organisme d'accueil

Introduction

Ce chapitre est consacré pour la présentation de l'organisme d'accueil qui nous a accueillis dans le cadre de notre stage de fin de cycle. Nous allons faire une mise en œuvre d'une solution PAM pour sécuriser le système d'information de l'entreprise en utilisant la gestion des accès privilégiés (Privilèges Access management), au sein du **GROUPE IFRI**.

I. Présentation de l'organisme d'accueil

La Groupe IFRI est une société à caractère industriel, elle est spécialisée dans la production des eaux minérales et des boissons diverses, Elle contribueau développement du secteur agroalimentaire à l'échelle nationale.

I.1. Création et évolution du Groupe IFRI

Cette société est créée par les fonds propres de M. IBRAHIM Laid en 1986, elle était « LIMONADERIE IBRAHIM » spécialisée dans la production de boissons gazeuses en emballage en verre[1].

Depuis la date de création, l'organisation a capitalisé une expérience dans le domaine des boissons. Ce n'est que dix ans plus tard, en 1996, que l'entreprise hérite unstatut juridique de SNC (Société Non Collectif) puis le statut de la SARL (Société à Responsabilité Limitée) composée de plusieurs associés [2].

À cette dernière date, la marque « IFRI » est connue et exploitée dans le monde industriel. Ce fut le point de départ de la première unité de fabrication d'eau minérale naturelle en Algérie sous un emballage en bouteilles en polyéthylène téréphtalate (PET). Plus de vingt (20) millions de bouteilles ont été commercialisées sur l'ensemble du territoire national dans la même année. Ce chiffre atteint 48 millions d'unités en1999, puis 252 millions de litres en 2004. La production franchira le cap des 541378351 millions de litres dans toutes les gammes des produits IFRI en 2012 [3].

[1] : Document de l'entreprise Ifri
[2] : Document de l'entreprise Ifri : "Forme juridique"
[3] : Document de l'entreprise Ifri : "Service commercial"

I.2. Répartition géographique

Le Groupe IFRI est répartie sur deux sites qui sont[4] :

I.2.1. Site IGHZER AMOKRANE

L'activité principale et la direction du Groupe IFRI sont situées, dans la commune d'IGHZER – AMOKRANE, Daïra IFRI OUZELLAGUEN dans la wilaya de Bejaia au nord de l'Algérie. Elle est implantée à l'entrée-Est de la vallée de la Soummam dans la zone « AHRIK IGHZER AMOKRANE », en contre bas du massif montagneux de Djurdjura qui constitue son réservoir naturel d'eau.

I.2.2. Site Zone activité TAHARACHT AKBOU

L'activité secondaire de production de JUS IFRUIT est implantée à la Zone TAHA- RACHT AKBOU sur un site de 20 HA destiné à recevoir les projets d'extension dans la gamme soda, jus etc.

I.3. Activités et filières du GROUPE IFRI

La société travaille 24/24 heures avec des lignes de production automatisées et équipées des systèmes de contrôle de qualité de dernière génération dans toutes les unités et étapes de la production. Grâce aux options technologiques qui ont prévalu lors du choix des équipements de production et de contrôle, IFRI accroît sans cesse ses capacités. Elle veille au respect des normes d'hygiènes, de sécurité et environnementales et de qualité les plus strictes afin de diversifier sa gamme de production.

Le groupe IFRI a diversifié ses filières, il est composé de quatre (4) sociétés[5] :

- ✓ IFRI : qui a pour mission de produire une gamme diversifiée de boissons (eau minérale naturelle, eau minérale gazéifiée, les sodas, les boissons fruitées, les boissons fruitées au lait) ;
- ✓ GENERAL PLAST : créée en 1999, l'entreprise GP (Général PLAST) c'est spécialisé dans la fabrication de la préforme en PET (Polyéthylène Téréphtalate) et bouchon en PEHD (Polyéthylène Haute Densité) ;

[4] : Document de l'entreprise Ifri

[5] : Document de l'entreprise Ifri

- ✓ BEJAIA LOGISQTIQUE : fondée en 2008, la SARL BEJAIA LOGISTIQUE (BL) est la référence Algérienne dans le domaine du transport routier, son activité est étendue dans le transport public de marchandises, location d'engins et matériels pour bâtiments, travaux publics et manutention, location de véhicules avec ou sans chauffeur et dans le transport des produits pétroliers ;
- ✓ HUILERIE OUZELLAGUEN : lancée en 2008 avec la création de la filiale oléicole dénommée SARL Huileries Ouzellaguen. Spécialisée dans la transformation (trituration) d'olives et mise en bouteille d'huile d'olive extra vierge, le produit est commercialisé sous le nom de Numidi

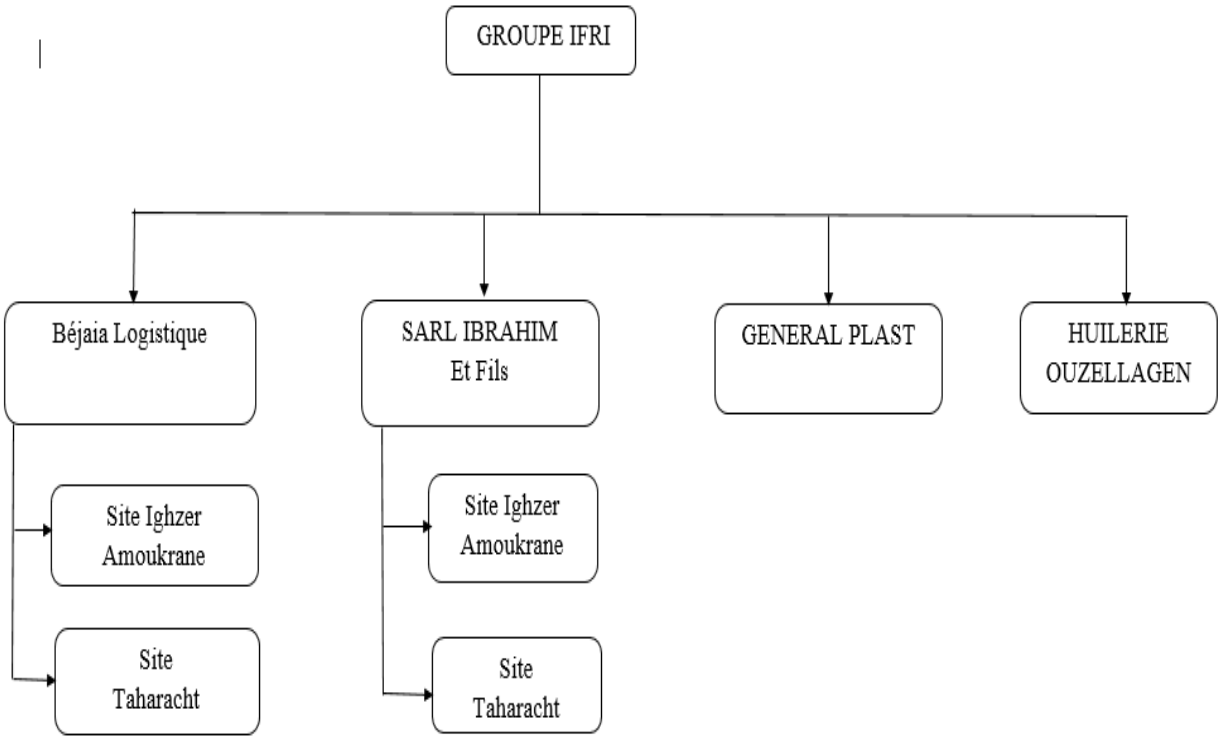

Figure I-1: Organigramme d'activités et filières du GROUPE IFRI.

I.4. Organisation de GROUPE IFRI

La structure organisationnelle des différentes fonctions informatiques de l'entreprise est présentée par la **figure 1.2** :

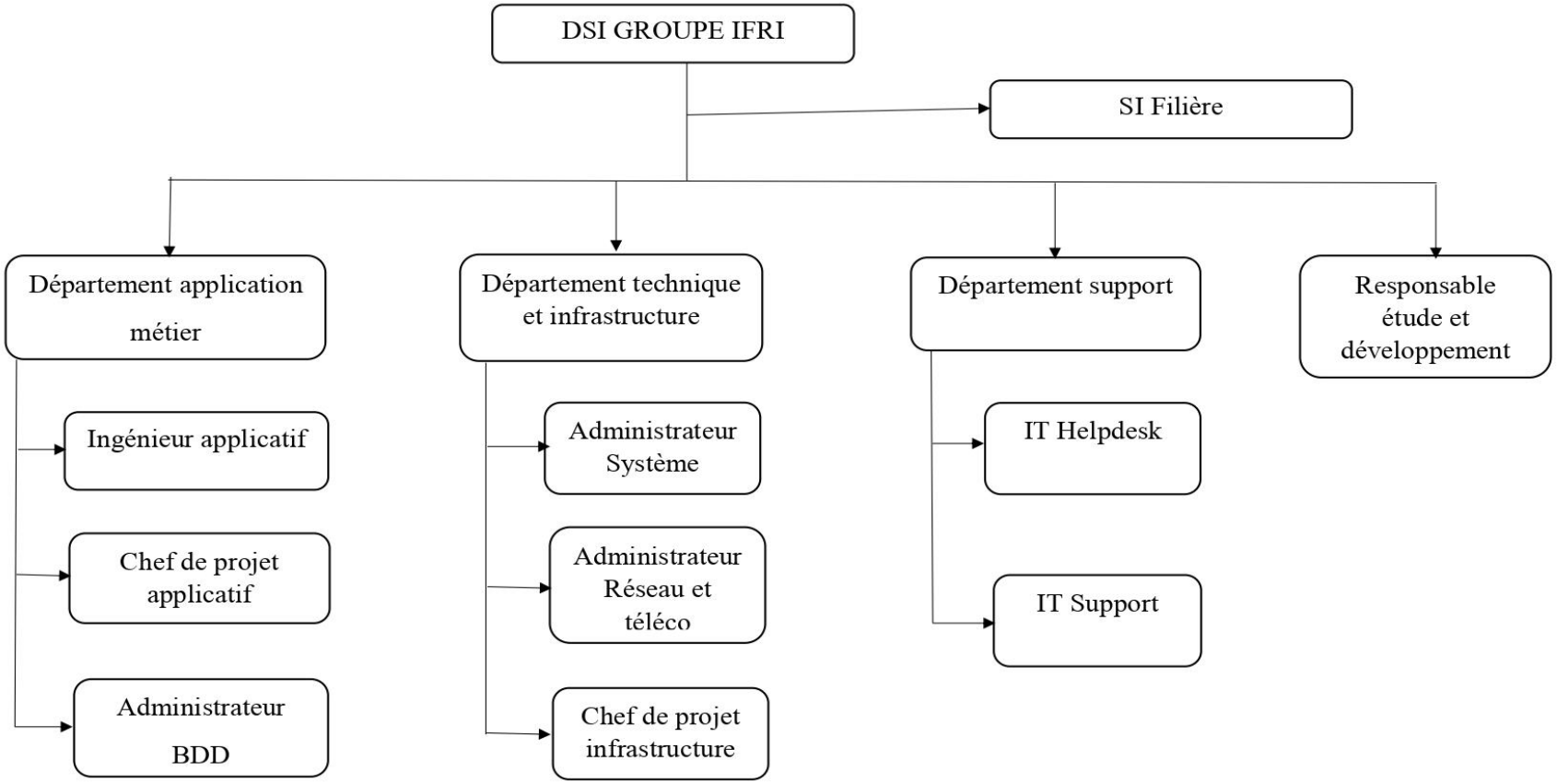

FIGURE I.2 : Organigramme de service informatique du GROUPE IFRI.

I.5. Présence du GROUPE IFRI

Le GROUPE IFRI est présente à l'échelle nationale et internationale.

I.5.1. GROUPE IFRI à l'échelle nationale

Dans un esprit de proximité du consommateur, le produit IFRI figure sur tout le territoire national. La société touche les 58 wilayas, ayant couvert les besoins du marché local. Elle commence à satisfaire le marché algérien avec 500 millions de bouteilles par an (emballage PET et Verre).

I.5.2. GROUPE IFRI à l'échelle internationale

L'établissement IFRI se lance dans la conquête du marché mondial, grâce à la stratégie du groupe en matière de développement des exportations par sa gamme élargie de boissons. Aujourd'hui, le GROUPE IFRI exporte ses produits vers des pays

- ✓ Européens : la France (principalement), l'Espagne, l'Italie, l'Allemagne, et la Belgique, . . .
- ✓ Nord-africaine : l'Algérie, le Soudan, le Mali
- ✓ Asie : Émirats, ….
- ✓ USA

I.6. Architecture du réseau informatique du GROUPE IFRI

Le réseau de groupe est reparti sur quatre sites reliés par la fibre optique, il est constitué de plusieurs équipements, des Switch, des routeurs, des firewalls, pour la plupart des marques hétérogène (hp, alcatel, cisco, dlink, ….).

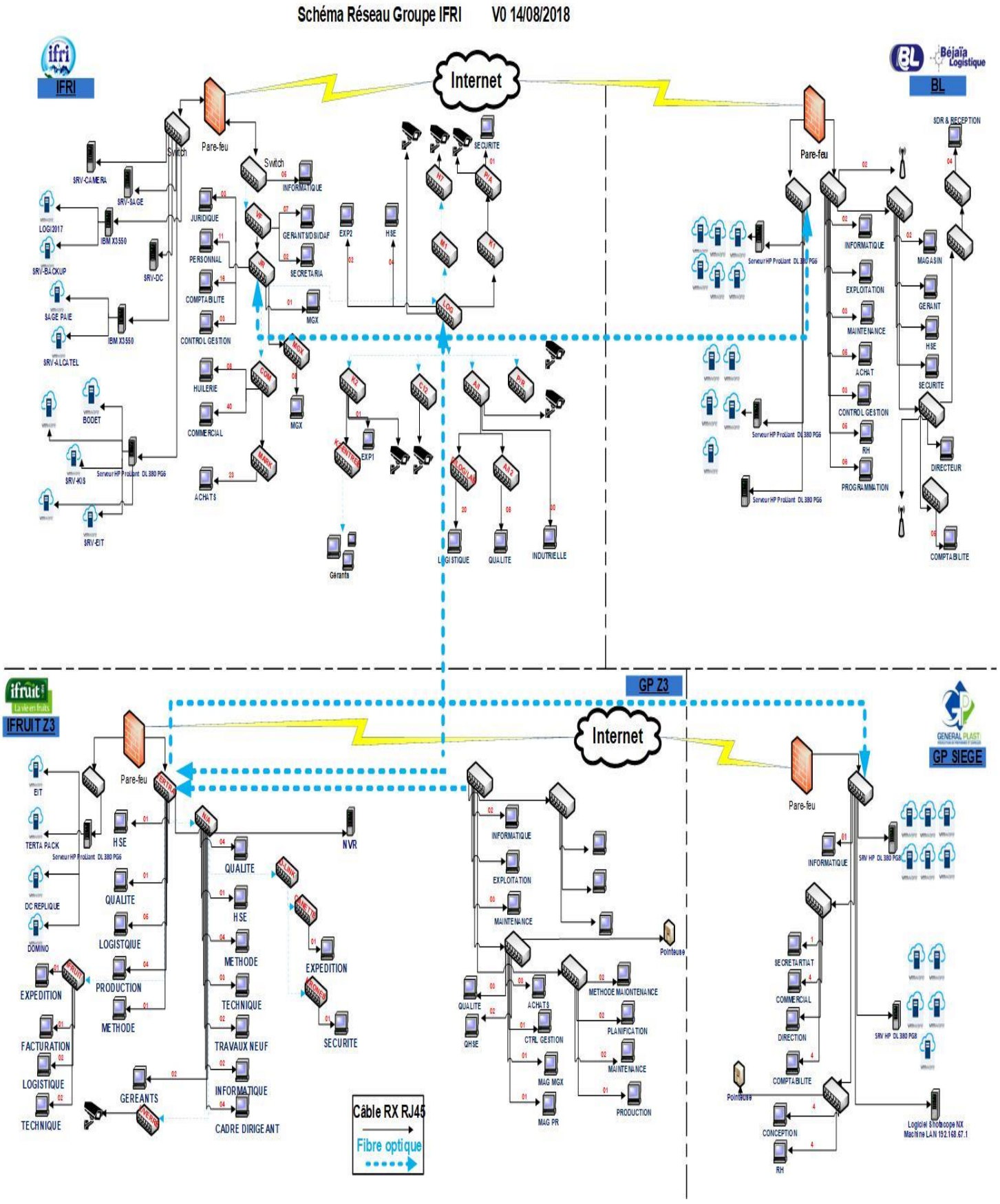

Figure I-3: Architecture actuel du réseau informatique du GROUPE IFRI.

I.7.Critique sur l'architecture actuel du groupe IFRI

- Le réseau est plat, absence d'hiérarchisation
- Absence de segmentation
- Le passage d'un site à une autre, passe par le réseau public. Ce qui compromet la sécurité des données et qui alourdit leur transmission.
- L'accès à Internet doit avoir une seule entrée une seule et sortie pour le réseau
- Le groupe IFRI doit refléter une architecture d'un seul réseau locale réparti sur plusieurs sites. Vers Internet il n'y aura qu'un seule point d'entrée / sortie. Tous les sites seront reliés au site principal (siège d'entreprise). Pour assurer la sécurité d'échange permanent de donnés entre les sites, il est souhaitable d'ajouter entre chaque deux sites (autre que le siège) une liaison entre eux.
- Absence d'un PAM qui permet de gérer les accès privilégiés

I.8. Problème posé dans cette période particulière

Suite au confinement, l'intégration du télétravail au profit usages obligent les entreprises à repenser leur approche de la cyber sécurité. Le poste de travail du collaborateur se trouve désormais de plus en plus souvent en dehors de l'entreprise. C'est d'ailleurs une nécessité pour assurer la continuité de l'activité en cas de crise, comme la pandémie que nous vivons encore actuellement. Le télétravail est en passe de devenir un standard pour les organisations. Ce nouveau paradigme implique des ouvertures de droits souvent dévolus à des « happy few » (administrateurs en astreinte sur l'infrastructure ou des applications, des prestataires de services). La multiplication des droits dévolus augmente la surface d'attaque en s'affranchissant des contraintes et des règles de sécurité périmétriques mises en place, le concept de protection dans l'entreprise.

Conclusion

La présentation de l'entreprise et l'étude de l'existant est une étape nécessaire pour analyser les problèmes auxquels le GROUPE IFRI fait face (Authentification, Traçabilité).

Dans le chapitre suivant, nous allons présenter les déférentes généralités sur la sécurité informatique, et donner les problématiques rencontrées et les objectifs au sein du Groupe.

Chapitre II

Généralités sur la sécurité des réseaux

Introduction

Un grand nombre d'entreprises, sont critiquables du point de vue de la sécurité qui leur en déployée.

La sécurité des réseaux devient alors une problématique essentielle tant pour les individus que pour les entreprises. Il est donc important de définir une politique de sécurité pour ces réseaux et de veiller à son respect. Néanmoins les mécanismes de sécurité préventifs mis en place ne sont pas incontournables. Il est nécessaire de mettre en œuvre des outils permettant de détecter toute violation de la politique de sécurité, c'est-à-dire toute intrusion.

Tout au long de ce chapitre, nous présenterons les principales menaces pesant sur la sécurité des réseaux ainsi que les problématiques et les objectifs.

II.1. Sécurité des réseaux

II.1.1. Définition

La sécurité d'un réseau est un ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir sa sécurité. En général, la sécurité d'un réseau englobe celle du système informatique sur lequel elle s'appuie.

II.1.2. Évaluation de la sécurité d'un réseau

La notion de sécurité fait référence à la propriété d'un système, d'un service ou d'une entité. Elle s'exprime le plus souvent par les objectifs de sécurité suivants[6] :

- La disponibilité (D) ;
- L'intégrité (I) ;
- La confidentialité (C) ;
- La traçabilité

Ces objectifs peuvent être compris comme étant des critères de base auxquels s'ajoutent des fonctions de sécurité qui contribuent à confirmer d'une part la véracité, l'authenticité d'une action, entité ou ressource (notion d'authentification) et, d'autre part, l'existence d'une action (notion de non-répudiation d'une transaction, voire d'imputabilité (figure II.1).

La réalisation des fonctions de sécurité, telles que celles de gestion des identités, du contrôle d'accès, de détection d'intrusion par exemple, contribuent, via des mécanismes de sécurité comme le chiffrement par exemple, à satisfaire les exigences de sécurité exprimées en termes de disponibilité,

[6] Elie MABO, La sécurité des systèmes informatiques (Théorie), université paris 8, support de cours, novembre 2010.

d'intégrité, de confidentialité. Elles concourent à la protection des contenus et des infrastructures numériques. Celle-ci sont supportées par des solutions techniques. À savoir l'intégration du système à sécuriser, par rapport au cycle de vie de ce dernier, par des approches complémentaires d'ingénierie et de gestion de la sécurité informatique.

II.1.2.1. Disponibilité

La disponibilité d'une ressource est relative à la période de temps pendant laquelle le service offert est opérationnel. Le volume potentiel de travail susceptible d'être pris en charge, durant la période de disponibilité d'un service, détermine la capacité d'une ressource à être utilisée (serveur ou réseau par exemple).

Il ne suffit pas qu'une ressource soit disponible, elle doit pouvoir être utilisée avec des temps de réponse acceptables. Sa disponibilité est indissociable de sa capacité à être accessible par l'ensemble des ayants droit (notion d'accessibilité).

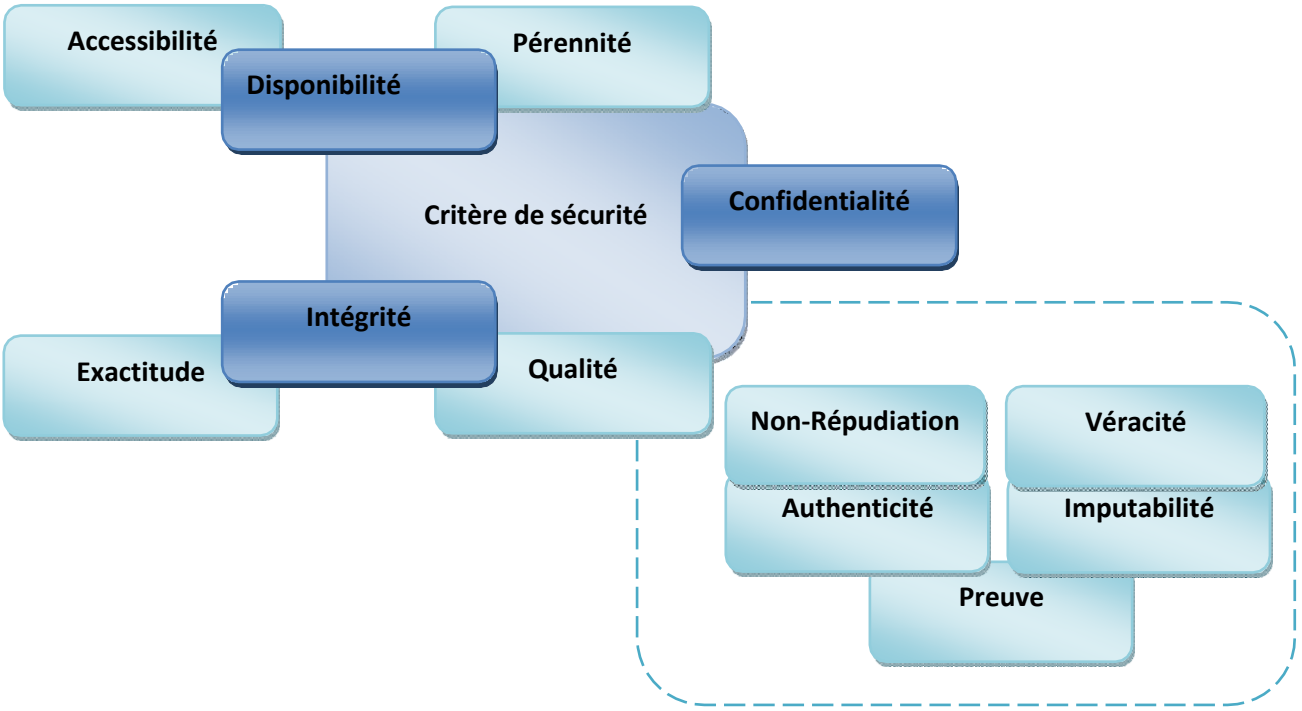

Figure II. 1: Critère de sécurité.

II.1.2.2. Intégrité

Obtenir l'assurance que le trafic qu'un utilisateur reçoit n'a pas été modifié après son envoi par un intermédiaire qui intercepte la communication et la modifie pour ses besoins propres.

II.1.2.3. Confidentialité

Obtenir l'assurance que le trafic d'un utilisateur n'est pas examiné par des tiers. En deux mots,

être sûr que personne ne lit votre courrier ou n'écoute votre communication en général c'est-à-dire il consiste à s'assurer que seuls les personnes autorisées aient accès aux ressources échangées.

II.2.2.4. Identification et authentification

Identifier l'auteur présumé d'un tableau signé est une chose, s'assurer que le tableau est authentique en est une autre. Il en est de même en informatique où des procédures d'identification et d'authentification peuvent être mises en œuvre pour contribuer à réaliser des procédures de contrôle d'accès et des mesures de sécurité.

L'authentification doit permettre de vérifier l'identité d'une entité afin de s'assurer entre autres, de l'authenticité de celle-ci. Pour cela, l'entité devra prouver son identité, le plus souvent en donnant une information spécifique qu'elle est censée être seule à détenir.

Tous les mécanismes de contrôle d'accès logique aux ressources informatiques nécessitent de gérer l'identification, l'authentification des entités et la gestion des droits et permissions associées aux personnes (figure II.2). Cela exclut l'usage anonyme des ressources. C'est également sur la base de l'identification des personnes et des accès aux ressources que s'établissent des fonctions de facturation et de surveillance.

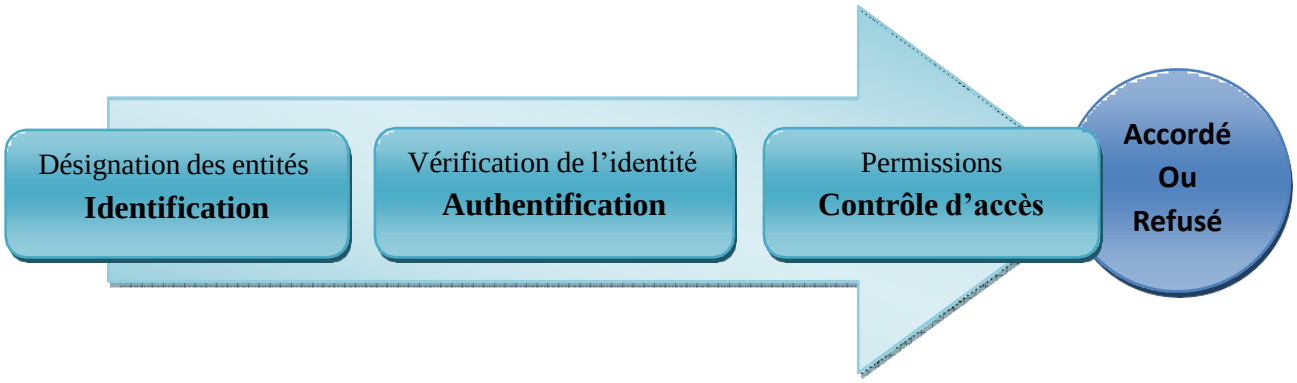

Figure II. 2: Identification et authentification

II.1.2.5. Traçabilité

Ensemble des mécanismes permettant de retrouver les opérations réalisées sur les ressources de l'entreprise. Cela suppose que tout événement applicatif soit archivé pour investigation ultérieure.

II.1.3. Architecture de sécurité

L'architecture de sécurité reflète l'ensemble des dimensions organisationnelle, juridique, humain et technologique de la sécurité informatique à prendre en considération pour une appréhension complète de la sécurité d'une organisation (figureII.3). Définir une architecture globale de la sécurité permet de visualiser la dimension générale et la nature transversale de la sécurité informatique d'une entreprise.il faut identifier ses diverses facettes et composantes afin de pouvoir les développer de façon cohérente, complémentaire et harmonieuse. Cela facilite l'intégration de mesures, de procédures et d'outils de sécurité.

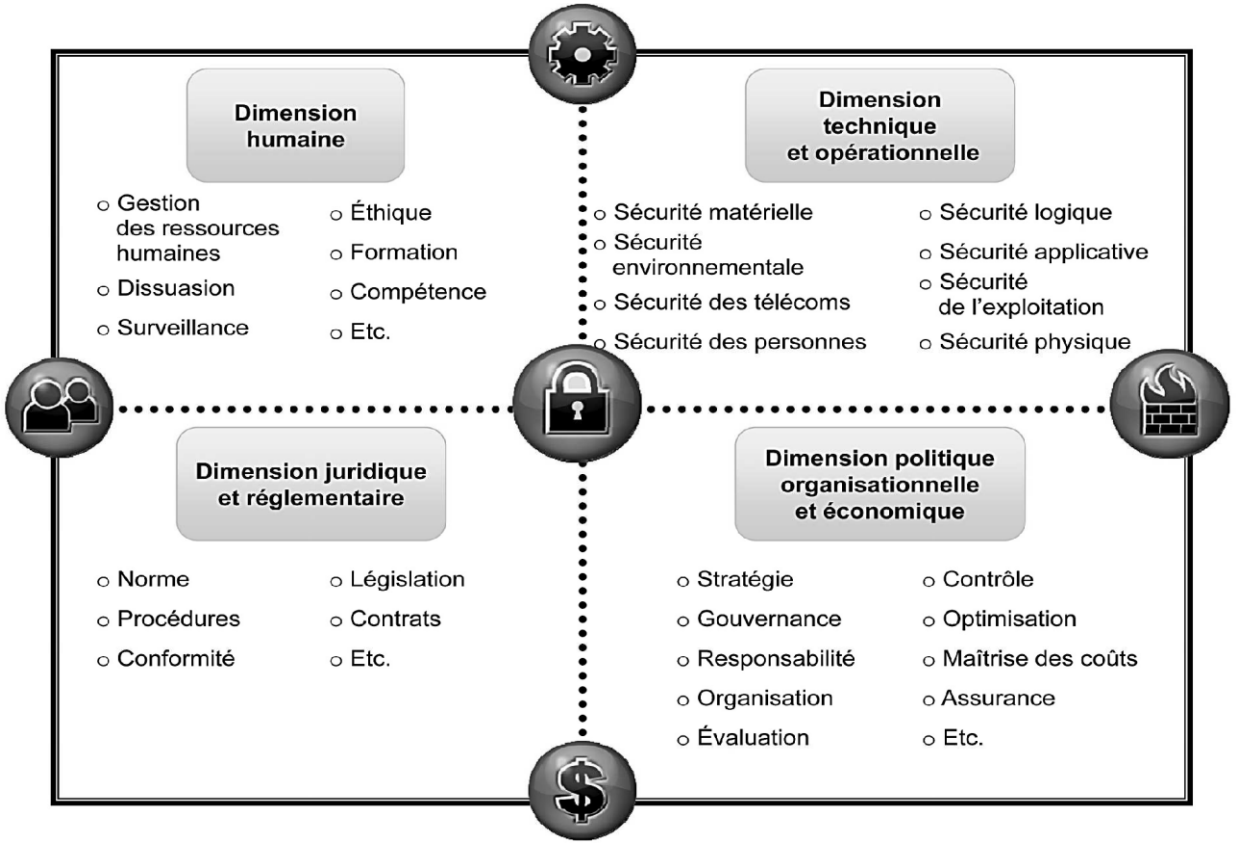

Figure II. 3: Les différentes dimensions d'une architecture de sécurité

Une démarche d'assurance des actifs, de gestion des risques, comme le respect des procédures, la formation, le comportement éthique des utilisateurs ou la conformité réglementaire sont autant de points à identifier dans un cadre d'architecture de sécurité. Ainsi, les critères de la sécurité pourront être réalisés judicieusement par le biais de mesures et de procédures complémentaires.

II.1.4. Les enjeux de la sécurité

II.1.4.1. Enjeux économiques

Les organismes ou entreprises à but lucratif ont presque toujours la même finalité : réaliser des bénéfices sur l'ensemble de leurs activités. Cette réalisation est rendue possible grâce à son

système d'information considéré comme moteur de développement de l'entreprise, d'où la nécessité de garantir la sécurité de ce dernier. La concurrence fait que des entreprises investissent de plus en plus dans la sécurisation de leurs systèmes d'information et dans la qualité de service fournit aux clients.

II.1.4.2. Enjeux politiques

La plupart des entreprises ou organisations se réfèrent aux documents officiels de sécurité élaborés et recommandés par l'État. Ces documents contiennent généralement des directives qui doivent être appliquées par toute structure engagée dans un processus de sécurisation du réseau. Dans le cadre du chiffrement des données par exemple, chaque État définit des cadres et mesures d'utilisation des algorithmes de chiffrement et les recommande aux entreprises exerçant sur son territoire. Le non-respect de ces mesures et recommandations peut avoir des conséquences graves sur l'entreprise. A ce niveau, l'enjeu est plus politique parce que chaque État souhaite être capable de décrypter toutes les informations circulant dans son espace.

II.1.4.3. Enjeux juridiques

Dans un réseau, on retrouve de l'information multiforme (numérique, papier, etc.). Le traitement de celle-ci doit se faire dans un cadre bien défini et dans le strict respect des lois en vigueur. En matière de juridiction, le non-respect des lois et exigences relatives à la manipulation des informations dans un système d'information peut avoir des conséquences graves sur l'entreprise.

II.1.5. Les vulnérabilités

Tous les systèmes informatiques sont vulnérables. Peu importe le niveau de vulnérabilité de ceux-ci. Une vulnérabilité est une faille ou une faiblesse pouvant être exploitée par une personne mal intentionnée pour nuire.

Les vulnérabilités des systèmes peuvent être classées en catégorie (humaines, technologiques, organisationnelles, mise en œuvre).

II.1.5.1. Vulnérabilités humaines

L'être humain de par sa nature est vulnérable. La plupart des vulnérabilités humaines proviennent des erreurs (négligence, manque de compétences, surexploitation, etc.), car ne dit-on pas souvent que l'erreur est humaine? Un système information étant composé des humains, il convient d'assurer leur sécurité si l'on veut garantir un maximum de sécurité dans le système information.

II.1.5.2. Vulnérabilités technologiques

Avec la progression exponentielle des outils informatiques, les vulnérabilités technologiques sont découvertes tous les jours. Ces vulnérabilités sont à la base dues à une négligence humaine lors de la conception et la réalisation. Pour être informé régulièrement des vulnérabilités technologiques découvertes, il suffit de s'inscrire sur une liste ou des listes de diffusion mises en place par les CERT (Computer Emergency Readiness ou Response Team).

II.1.5.3. Vulnérabilités organisationnelles

Les vulnérabilités d'ordre organisationnel sont dues à l'absence des documents cadres et formels, des procédures (de travail, de validation) suffisamment détaillées pour faire face aux problèmes de sécurité du système. Quand bien même ces documents et procédures existent, leur vérification et mises à jour ne sont pas toujours bien assurées[7].

II.1.6. Les menaces

On peut également classer les menaces en deux catégories selon qu'elles n'échangent rien (menaces passives) ou qu'elles perturbent effectivement le réseau (menaces actives).

II.1.6.1. Les menaces passives

Consistent essentiellement à copier ou à écouter l'information sur le réseau. Elles nuisent à la confidentialité des données. Dans ce cas, celui qui prélève une copie n'altère pas l'information elle-même.

[7] Elie MABO, La sécurité des systèmes informatiques (Théorie), université paris 8, support de cours, novembre 2010.

II.1.6.2. Les menaces actives

Sont de nature à modifier l'état du réseau.

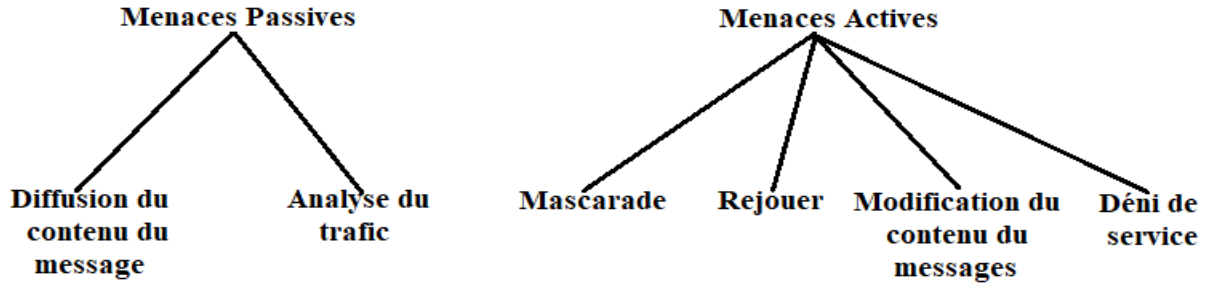

Figure II. 4: Les menaces actives et passives

II.1.7. Les risques

Les risques se mesurent en fonction de deux critères principaux : la vulnérabilité et la sensibilité.

La vulnérabilité désigne le degré d'exposition à des dangers. Un des points de vulnérabilité d'un réseau est un point facile à approcher. Un élément de ce réseau peut être très vulnérable tout en présentant un niveau de sensibilité très faible : le poste de travail de l'administrateur du réseau, par exemple, dans la mesure où celui-ci peut se connecter au système d'administration en tout point du réseau.

La sensibilité désigne le caractère stratégique d'un composant du réseau. Celui-ci peut être très sensible, vu son caractère stratégique mais quasi invulnérable, grâce à toutes les mesures de protection qui ont été prises pour le prémunir contre la plupart des risques.

II.1.8. Les protocoles de sécurité

II.1.8.1. Protocole SSL

Le protocole SSL (Secure Socket Layer) permet de sécuriser tout protocole applicatif s'appuyant sur TCP/IP. (HTTP, FTP, etc.).

Le protocole SSL permet non seulement de fournir les services d'authentification du serveur, mais également les services de confidentialité et de d'intégrité.

Le principe d'une authentification du serveur avec SSL est le suivant :

1- Le navigateur du client fait une demande de transaction sécurise au serveur.

2- 2- Suite à la requête du client, le serveur envoie son certificat au client.

3- Serveur fournir une liste des algorithmes cryptographiques qui peuvent être utilisés pour la transaction entre client/serveur.

4- Le client choisi l'algorithme

5- Le serveur envoie son certificat avec une clé cryptographique correspondante au client
6- Le navigateur vérifie que le certificat délivré est valide
7- Si la vérification est correcte alors le navigateur du client envoie au serveur une clé secrète chiffre à l'aide de la clé publique du serveur qui sera donc le seul capable de déchiffre puis d'utilise cette clé secrète.

II.1.8.2. Protocole SSH

Le protocole SSH (Secure Shell) est un protocole permettant à un client d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée les données circulant entre le client et le serveur sont chiffrées. Ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client qui peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

II.1.8.3. Le protocole RDP

Le protocole RDP (Remote Desktop Protocol) est un protocole, ou une norme technique, permettant d'utiliser un ordinateur de bureau à distance. Les logiciels de bureau à distance peuvent utiliser plusieurs protocoles différents, notamment RDP, ICA (Independent Computing Architecture) et VNC (Virtual Network Computing), mais RDP est le protocole le plus couramment utilisé. Le protocole RDP a été initialement publié par Microsoft. Il est disponible pour la plupart des systèmes d'exploitation Windows, mais il peut également être utilisé avec les systèmes d'exploitation Mac[8].

II.2. Mise en place d'une politique de sécurité

II.2.1 De la stratégie à la politique de sécurité

Une politique de sécurité permet l'expression et la concrétisation d'une stratégie sécuritaire. La politique de sécurité est un outil indispensable à la gouvernance de la sécurité et à la réalisation du plan stratégique de sécurité (figure II.5).

Une politique de sécurité exprime la volonté managériale de protéger les valeurs informationnelles et les ressources technologiques de l'organisation. Elle spécifie les moyens (ressource, procédure, outils…) qui répondent de façon complète et cohérente aux objectifs stratégiques de sécurité.

[8] https://www.cloudflare.com/fr-fr/learning/access-management/rdp-security-risks/

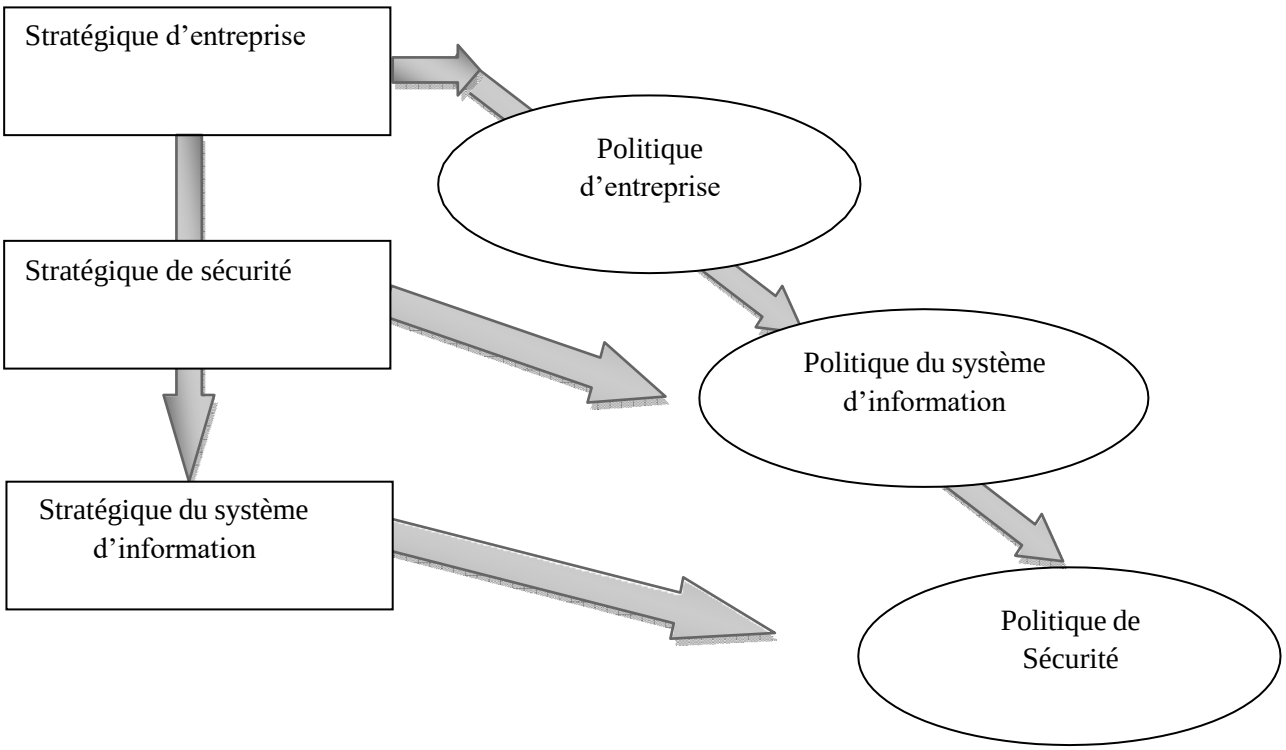

Figure II. 5: Stratégie et politique de sécurité.

La politique de sécurité fait le lien entre la stratégie de sécurité et l'entreprise et la réalisation opérationnelle de la sécurité.

La gestion des risques constitue le point de départ de l'analyse des besoins sécuritaires qui permet la définition de la politique de sécurité. (Figure II.6)

La politique de sécurité permet de transcrire le travail effectué pour comprendre les risques et leurs impacts, en des mesures concrètes de sécurité. Sa spécification facilite le choix et la mise en œuvre des mesures de sécurité. Elle donne de la cohérence à la gestion et contribue à adopter vis-à-vis des risques, une attitude proactive et réactive. Une bonne définition et une réalisation pertinente d'une politique de sécurité autorisant une certaine maitrise des risques informatiques, tout en réduisant leur probabilité d'apparition. Toutefois, il ne faut pas perdre de vue que même un bon gestionnaire de la sécurité, tout en anticipant et prévenant certains accidents volontaires ou non, n'est pas devin. Ne pouvant anticiper toutes les nouvelles menaces, mais sachant qu'elles exploitent les vulnérabilités et les failles des systèmes en place, le gestionnaire s'emploiera à réduire les vulnérabilités de l'environnement à protéger afin de minimiser la probabilité de réalisation de menace. Aucune politique de sécurité, nul service de sécurité, aussi perfectionné soit-il, ne tient si l'intégrité des personnes se trouve mise en cause. En effet, le maillon faible de la sécurité est toujours humain[9].

[9] Solange GHERNAOUTI, Sécurité informatique et réseaux, Ed. Dunod, 4e édition, 2013.

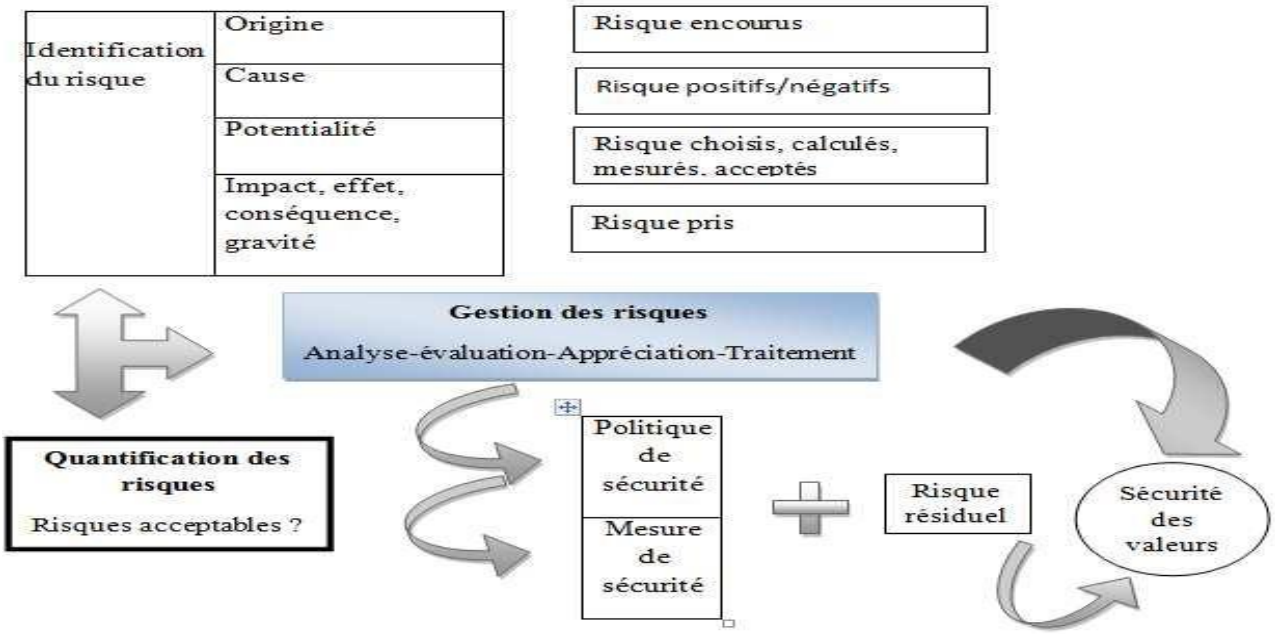

Figure II. 6: De l'analyse des risques à la politique de sécurité.

II.2.2 Propriétés d'une politique de sécurité

Une politique de sécurité résulte d'une analyse des risques est définie pour répondre aux exigences de sécurité, dans un contexte donné. Elle se traduira par la réalisation de mesures, fonction, procédures, service, comme par exemple[10] :

- Des règles de classification de l'information, d'utilisation des ressources ;
- Des outils : contrôle d'accès, chiffrement des donnée, authentification, système pare- feu ou de détection d'incidents, de surveillance et d'enregistrement, journalisation, traçabilité
- Des contrats de services : clauses de responsabilité, devoirs et obligation ;
- Des plans gestion de crise, de secours, de continuité et de reprise ;
- Des plans d'action de poursuite en justice ;
- Des mesures d'assurance, de gestion de la performance ; La définition de la politique de sécurité doit être :
- Simple et compréhensible ;
- Aisément réalisable ;
- De maintenance facile ;
- Véritable et contrôlable ;
- Adoptable par un personnel préalablement sensibilisé, voir formé.

[10] Solange GHERNAOUTI, Sécurité informatique et réseaux, Ed. Dunod, 4e édition, 2013.

Une politique de sécurité ne doit pas être statique mais périodiquement évaluée, optimisée et adaptée à la dynamique du contexte dans lequel elle s'inscrit. Elle doit être évolutive et suivre les modifications du contexte (risques, systèmes, environnement, personnes, règlementation). Ainsi, une politique de sécurité doit prendre en compte les droit d'accès par exemple, les autorisations peuvent varier. Pour ce qui concerne les droits d'accès par exemple, les autorisations peuvent être délivrées pour les jours ouvrés, entre 7 heures et 20 heures, mais exclusivement sur demande pour la nuit ou les week-ends ou encore en fonction de certains événements. Elle doit être adaptable et personnalisable selon des profils des utilisateurs concernés, les flux ou la localisation des acteurs en jeu par exemple.

II.2.3. Stratégies de sécurité

Ils consistent à d´éployer des moyens et des dispositifs visant à sécuriser le système d'information ainsi que de faire appliquer les règles définies dans une politique de sécurité. En voici les principaux dispositifs permettant de s´sécuriser un réseau contre les attaques [11].

II.2.3.1. Pare-feu

De nos jours, toutes les entreprises possédant un réseau local possèdent aussi un accès à Internet, afin d'accéder aux informations disponibles sur le web, et de pouvoir communiquer avec l'extérieur. Cette ouverture vers l'extérieur est indispensable et dangereuse en même temps.

Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer son réseau local, et y accomplir des actions douteuses, parfois gratuites, de destruction, vol d'informations confidentielles. Les mobiles sont nombreux et dangereux et pour parer à ces attaques, une architecture sécurisée est nécessaire. Pour cela, le cœur d'une telle architecture est basée sur un pare-feu.

C'est un ensemble de différents composants matériels (physique) et logiciels (logique) qui contrôlent le trafic intérieur/extérieur selon une politique de sécurité. Un système pare-feu fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines aux réseaux, il s'agit ainsi d'une passerelle filtrante. Il permet d'une part de bloquer des attaques ou connexions suspectes d'accéder au réseau interne. D'un autre côté, un firewall sert dans de nombreux cas également à éviter la fuite non contrôlée d'informations vers l'extérieur. Il propose un véritable contrôle sur le trafic réseau de l'entreprise, Il permet donc d'analyser, de sécuriser et de gérer le trafic réseau.

[11] Drdoigne.J, Réseau informatique, notions fondamentales, Edition ENI, France, Janvier 2013.

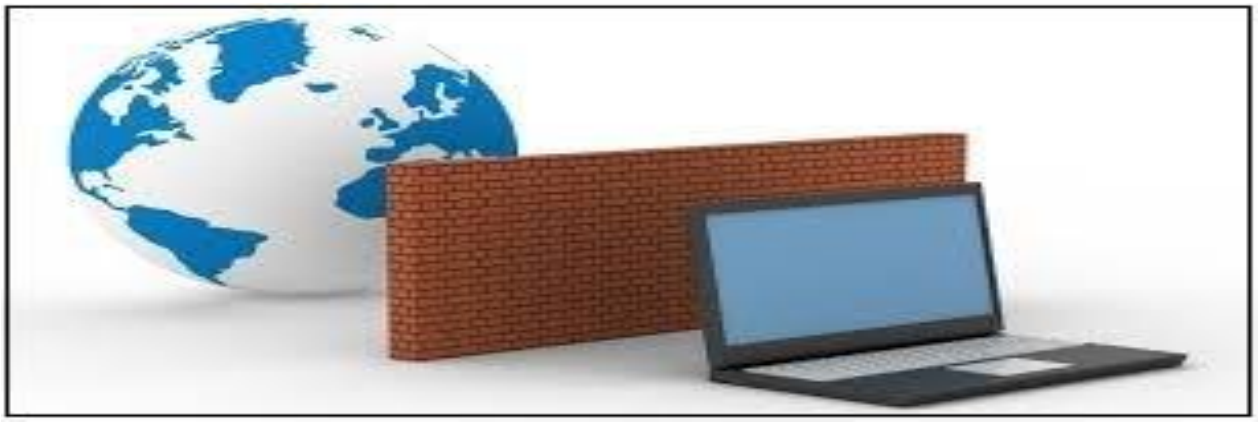

Figure II.7 : pare-feu (firewall).

II.2.3.2. Le proxy

Un serveur proxy (traduction en français de proxy server, appelé aussi serveur mandataire) est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local (utilisant parfois des protocoles autres que le protocole TCP/IP).

La plupart de temps le serveur proxy est utilisé pour le Web, il s'agit alors d'un protocole http. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP. Etc.). Le principe de fonctionnement basique d'un serveur proxy est assez simple ; il s'agit d'un serveur « mandaté » par une application pour effectuer une enquête sur internet à sa place. Ainsi, lorsqu'un utilisateur se connecte à internet à l'aide d'une application client configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente, cherche à joindre et lui transmettre la requête. Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente[12].

II.2.3.3. Zone démilitarisée

L'interconnexion entre le réseau public Internet et le LAN utilise très souvent une zone publique tampon, hébergée dans l'entreprise. Ce cas est nommé zone démilitarisé ou DeMilitarized Zone (DMZ). Elle héberge différents serveurs accessibles depuis l'Internet, tels que :

- Serveur proxy.
- Serveur web hébergeant le site de l'entreprise.
- Relais de messagerie, chargé de réaliser un tri des messages…

[12] Drdoigne.J, Réseau informatique, notions fondamentales, Edition ENI, France, Janvier 2013.

II.2.3.4. Authentification

L'authentification est la vérification d'informations relatives à une personne ou à un processus informatique. L'authentification complète le processus d'identification dans le sens ou l'authentification permet de prouver une identité déclarée. Dans un serveur, un processus d'authentification valide l'identité et après authentification donne l'accès aux données, application, bases de données, fichiers ou sites Internet…etc.

Les techniques d'authentification les plus répondu sont les Mots de passe et les Certificats numérique à clés publique.

II.2.3.5. Mots de passe

C'est le moyen le plus simple et le plus classique de s'assurer que seules les personnes autorisées peuvent accéder aux différents services d'un réseau et de protéger certaines zones du réseau par un mot de passe.

II.2.3.6 IPS

Un système de prévention d'intrusion (ou IPS, Intrusion Prévention System) est un outil similaire aux IDS, sauf que ce système peut prendre des mesures afin de diminuer les risques d'impact d'une attaque. C'est un IDS actif, il détecte un balayage automatisé, l'IPS peut bloquer les ports automatiquement.

II.2.3.7 VPN

Dans les réseaux informatiques, le réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est une technique permettant aux postes distants de communiquer de manière sûre, tout en empruntant des infrastructures publiques (internet). Un VPN repose sur un protocole, appelé protocole de tunnelisation, c'est-à-dire un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie.

II.3. Motivation

Pour maintenir un système sécurisé, les responsables de la sécurité doivent effectuer les évaluations et mettre en œuvre les contrôles recommandés dans la norme. Un domaine de contrôle, cependant, est fondamental pour le succès de pratiquement tous les autres aspects de la norme. C'est le contrôle d'accès, en particulier le contrôle sur des accès à privilèges.

La sécurisation de l'accès privilégié poursuit deux objectifs simples :

1. Limiter à certaines voies autorisées (de façon stricte) la possibilité d'effectuer des actions privilégiées.
2. Protéger et superviser attentivement ces voies.

II.4. Problématique

Dans l'entreprises, tel que le GROUPE IFRI, l'échange des informations devient une nécessité absolue. Malgré la complexité de gestion des accès privilégiés de systèmes de l'administration réseaux, les besoins se multiplient pour élargir les tâches administratives de chaque entreprise quel que soit sa taille. Cependant la gestion des accès privilégiés des utilisateurs est l'une des tâches absolument essentielles dévolue aux administrateurs pour assurer la sécurité des systèmes, d'authentifier des utilisateurs, donner des droits d'accès, En effet, les ressources de l'entreprise tendent de plus en plus à une centralisation des informations.

L'administrateur réseau gère les postes de travail et les serveurs de l'entreprise, pour mettre en place les moyens et les procédures en garantissant la sécurité les performances et la disponibilité des systèmes. SARL IFRI

La problématique générale de notre travail portera sur :

- La sécurisation des Accès privilèges sur le système des employés ainsi que les comptes des clients,
- L'autorisation des accès aux utilisateur et les administrateurs, su la surveillance des audites.

II.5. Objectif

L'objectif principal est de sécuriser le système d'information en supprimant les accès non autorisés sur les ressources sensibles. Cette protection s'appuie sur deux axes principaux :

- La gestion de l'injection et du cycle de vie des mots de passes utilisés dans les ressources administrées et les applications d'administration,
- La traçabilité de toutes les actions réalisées lors de la connexion des utilisateurs ayant un pouvoir de nuisance sur le système d'information, sous forme d'audit ou de traces vidéo.

A l'issu de ce travail, nous serons en mesure de sécuriser et de contrôler les accès au système afin de centraliser la gestion des utilisateurs au sein de l'entreprise sous Windows.

Conclusion

Nous avons essayé à travers ce chapitre d'apporter de la lumière sur les généralités de la sécurité informatique, sa classification. Ainsi, nous avons cité quelques équipements qui peuvent être mis en place pour réaliser cette sécurisation. Enfin, nous avons parlé sur les motivations, les problématiques et les objectifs.

Dans le chapitre suivant, nous allons présenter les déférents outils utilisés et l'architecture proposée. Après, on passera au fonctionnalités des PAM, puis nous allons faire une comparaison des solutions proposées. On finit avec une brève description de la solution déployée et sa mise en place sur l'architecteur proposée.

Chapitre III

Conception

Introduction

Dans ce chapitre nous allons apporter notre solution en tenant compte de l'existant, en améliorant l'architecture existante et en ramenant de la nouveauté du point de vue sécuritaire fiabilité et performance.

III.1. Architecture en cours de réalisation par le staff du groupe 'IFRI GROUP'

Le directeur des systèmes d'informations du groupe IFRI, a mis en œuvre une nouvelle architecture d'une taille importante composée de 4 sites. Elle est constituée de plusieurs équipements, des commutateurs, des pare-feu… de marque Cisco.

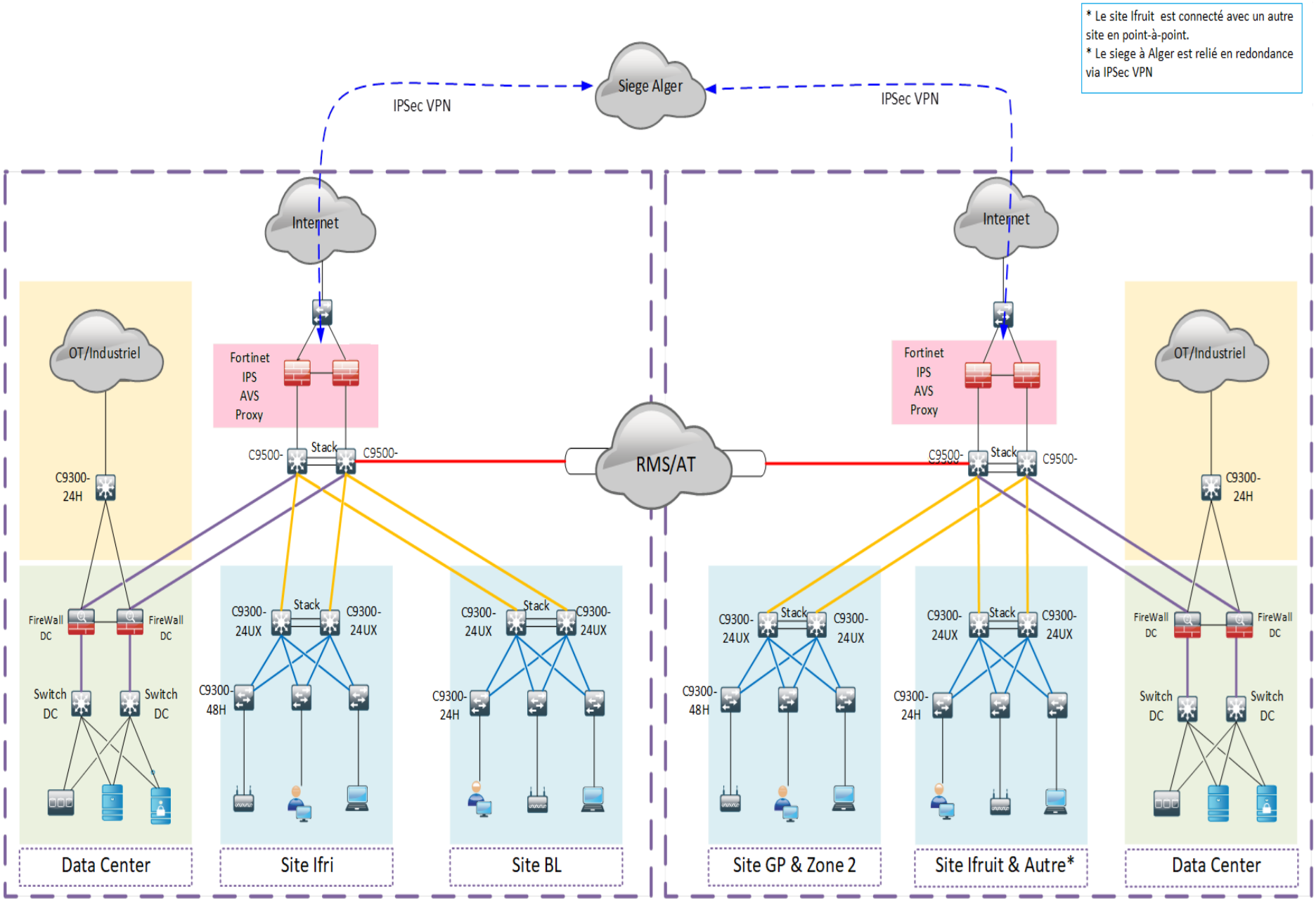

Figure III.1 : Architecture en cours de réalisation

III.2. Critique de l'architecture

A vouloir trop sécuriser l'architecture du système, on a encombré le système avec des équipements supplémentaires (duplication de l'activité des transactions). La facture d'achat et de contrat de maintenance devint trop importante pour l'entreprise. Par contre il est important de penser à la protection des données par une sauvegarde automatique périodique et sécurisé.

III.3. Architecture proposée

Nous proposons une architecture simplifiée, juste le nécessaire, facile à maintenir et à gérer, efficace, optimale, prend en charge toute l'activité de sécurité envisagée et indispensable.

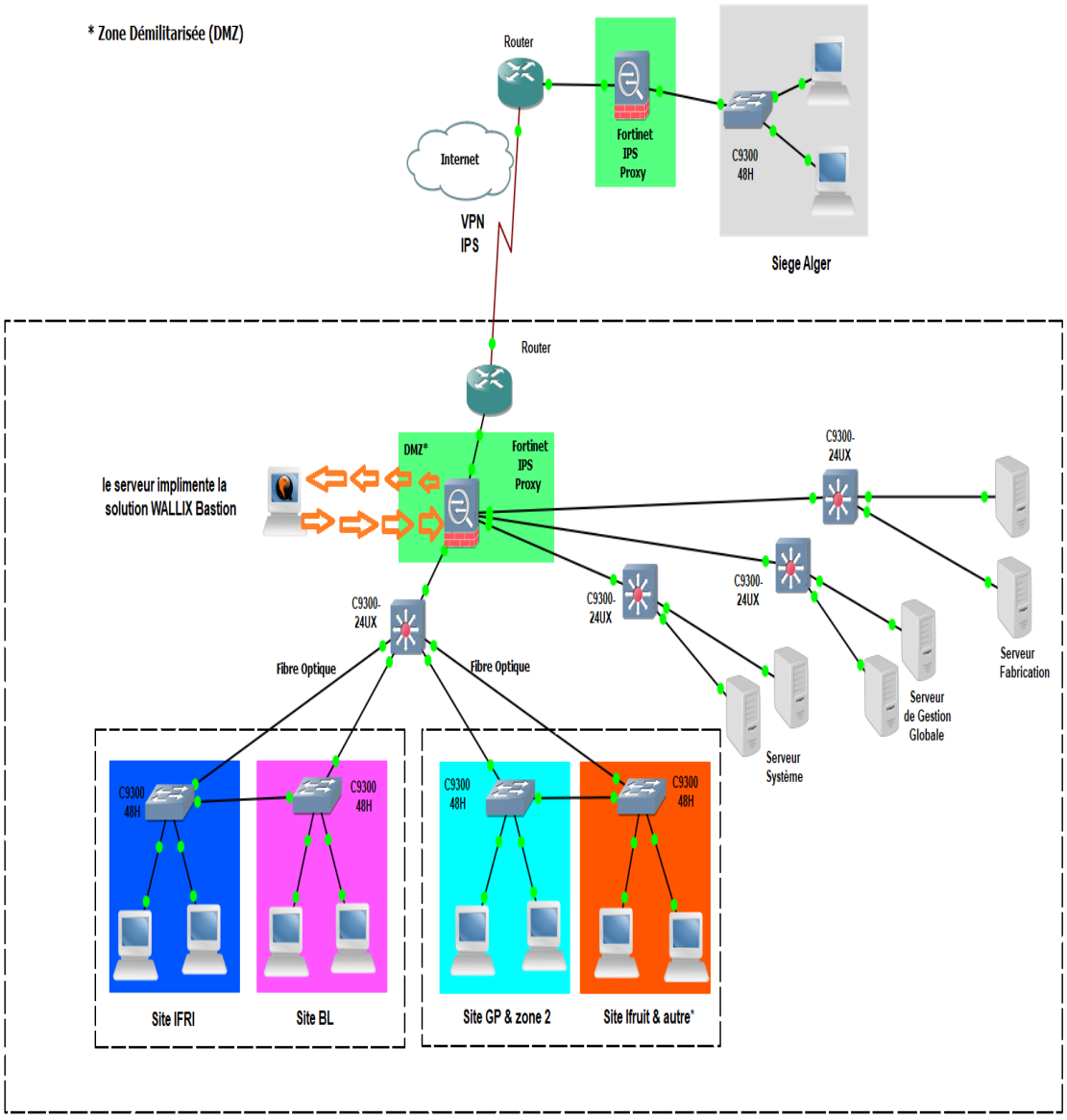

Figure III. 2 : Architecture proposée

III.4. Les concepts fondamentaux des PAM[13] :

III.4.1. Définition de PAM

La gestion des accès privilégiés (PAM) est une solution basée sur la sécurité qui permet de garantir la sécurité de toutes vos données en empêchant les abus d'accès non autorisés. Cela implique l'utilisation d'une gamme d'outils qui vous permettent de garder le contrôle des actions critiques de votre intranet ou de votre infrastructure.

En termes pratiques, cela est principalement accompli en distinguant les individus en question par leurs mots de passe. Chaque individu est suivi et contrôlé par rapport aux actions qu'il a entreprises. Ce qui implique de prendre les informations d'identification des administrateurs, des utilisateurs expérimentés ou des comptes autrement `` privilégiés " et de les stocker dans un référentiel sécurisé. Une fois ceux-ci réalisés, ces utilisateurs doivent passer par votre système PAM pour accéder à ces informations d'identification - ajoutant une couche supplémentaire de sécurité à vos protocoles de mot de passe et aidant à agir comme rempart contre l'ingénierie sociale ou d'autres méthodes d'intrusion.

De plus, une fois que l'utilisateur a accédé à ses informations d'identification via PAM, le système exige que les actions entreprises par ce dernier soient à nouveau « enregistrées » pour que le système se met à jour. Cela fournit un suivi point par point pour aider à déterminer où les problèmes sont survenus et assurer une responsabilité maximale lorsque cela compte le plus.

PAM vous permet de valider complètement l'identité des personnes accédant à votre système, en le laissant effectuer des tâches d'autorisation et d'authentification de compte qui restent toujours séparées de votre environnement existant.

Ces outils sont utilisés par le biais de technologies cloud, permettant à vos utilisateurs d'accéder et de superviser l'utilisation du système de n'importe où dans le monde - créant un coffre-fort numérique auquel seuls les bonnes autorisations peuvent accéder, garantissant un contrôle maximal sans sacrifier l'efficacité interne.

[13] https://www.10duke.com/privileged-access-management/

Figure III. 3 : Gestion des accès privilégie

III.4.2. L'utilité de PAM

La fonctionnalité PAM est essentielle pour les entreprises ayant un grand nombre d'employés ou celles qui ont des rôles complexes au sein d'une organisation. PAM convient parfaitement aux organisations internationales qui permettre à leurs clients et à leurs personnels d'accéder à partir de différents endroits, aux informations, aux entreprises qui détiennent des informations sécurisées ou sensibles, ou aux entreprises existantes qui cherchent à mettre à niveau leur infrastructure ou à améliorer leurs meilleures pratiques.

Les solutions PAM sont déployées par des administrateurs systèmes ou des utilisateurs expérimentés désignés. Ce qui permet d'augmenter d'un degré de contrôle souvent négligé par de nombreuses entreprises.

En bref, PAM est mieux déployé dans les entreprises qui ont besoin de savoir quels utilisateurs ont déployé une activité particulière sur leur système et des informations clés sur la façon dont elle a été utilisée.

III.4.3. L'avantage de PAM

Les principaux avantages de la gestion des accès privilégiés comprennent:

Efficacité: de nombreux systèmes PAM sont caractérisés par plusieurs paramètres qui définissent l'état de son fonctionnement. En qu'elle que sorte en peut définir deux états de son activité :

- ✓ Un système d’accès et de contrôle rapide. Cela rationalise massivement ce qui est souvent un processus physique ardu et non sécurisé qui crée des frictions et des risques pour l'utilisateur et l'administrateur.
- ✓ Un accès un peu long qui permet un contrôle maximal.

Sécurité: PAM est avant tout un système de sécurité qui fournit une couche supplémentaire de sécurité aux comptes. Le déploiement d'un coffre-fort dédié aux mots de passe garantit une couche de contrôle indispensable sur vos administrateurs clés et leur approche de la politique de mot de passe. Ce qui permet également de voir qui accède à quelles informations et à quel moment.

Convivialité: l'utilisation d'une solution PAM réduit considérablement le travail d'administration des comptes pour les administrateurs ou les gestionnaires de comptes, contribuant ainsi à éliminer les erreurs humaines, tout en permettant une sécurité accrue. Cela s'étend aux utilisateurs finaux qui peuvent accéder rapidement au système sans mettre le réseau en danger.

III.4.4. Implémentation de PAM

La gestion des accès privilégiés peut être déployée dans le cadre de l’infrastructure sous la forme d'une suite d'outils dédiée, permettant de personnaliser les protocoles d'accès selon les besoins. En fonction des besoins uniques, le processus de mise en œuvre peut impliquer l'installation et la configuration de l'un des éléments suivants:

- Identification multifactorielle de l'administrateur
- Audit de bout en bout et journaux d’accès
- Outils de provisionnement automatisés et personnalisés pour accorder un accès ad hoc
- Un coffre-fort dédié aux mots de passe pour permettre un stockage sécurisé
- Gestionnaire d'accès détaillé pour permettre un suivi détaillé
- Autres fonctionnalités sur mesure telles que le suivi de session, l'émission de tickets, le contrôle d'accès aux applications et la journalisation du temps pour permettre la capture de données et un contrôle accru sur les droits des utilisateurs

Une fois déployés, les points ci-dessus peuvent être ajustés selon les besoins. On peut créer une gamme d'options de flux de travail permettons une flexibilité maximale et une capacité de répondre à la croissance ou aux exigences légales de cette gamme.

En plus des problèmes de sécurité, PAM permet de créer un détail d’authentification fournissant un aperçu complet de qui a tenté d'accéder au système, comment et quand ? Cela peut aider à fournir des renseignements en direct sur les interactions. Mais permet également

de contrôler les privilèges internes et l'accès des clients. Cela permet d'étendre les fonctionnalités du système aux clients et organismes externes. Aussi, il garantit un contrôle total sur les niveaux d'accès tout en empêchant les erreurs humaines et la création des problèmes au système par les utilisateurs externes.

Cela permet un certain nombre d'avantages, notamment:

Isolation des privilèges: les utilisateurs doivent demander des privilèges pour leurs comptes. Ce qui donne un niveau de contrôle supplémentaire à l'accès. Ces derniers doivent ensuite être approuvées par les administrateurs. Ce qui limite l'accès aux tâches et informations sensibles.

Application du protocole: les solutions PAM peuvent aider à agir comme des barrières douces contre les violations de la pratique. Les comptes doivent passer par des flux de travaux définis et faciles à naviguer. Cela permet d'encourager les meilleures pratiques sans sacrifier la convivialité.

Capture de données: toute demande de privilèges ajoute de nouvelles informations au système, détaillant qui l'a demandée, quand elle a été autorisée, par qui et le suivi des actions clés après coup? Cela peut aider à promouvoir les meilleures pratiques et à garantir que toutes les enquêtes de suivi ont été très efficaces.

Flexibilité élevée: les flux de travail PAM sont hautement personnalisables et peuvent être aussi légers ou aussi sécurisés que nécessaire. Ils permettent un degré élevé de contrôle sur le processus ou bien la capacité de mettre en œuvre des flux de travaux sur mesure selon les besoins.

III.5. Les déférents types des solutions de PAM

- Wallix Bastion
- Priv X
- Okta

III.3.1. Tableaux de comparaison des solutions étudiées

Solution	Wallix Bastion	Okta	Priv X
Description	Solution modulaire de sécurité des comptes privilégiés qui automatise la surveillance des sessions privilégiées, les clés SSH et la gestion des mots de passe.	Okta est le principal fournisseur d'identité pour l'entreprise. Okta Identity Cloud connecte et protège beaucoup d'employés des plus grandes entreprises du monde. Il relie également de manière sécurisée les entreprises à leurs partenaires, fournisseurs et clients. Avec des intégrations approfondies dans plus de 5 000 applications, Okta Identity Cloud permet un accès simple et sécurisé depuis n'importe quel appareil. Des milliers de clients, parmi lesquels Experian, 20th Century Fox, LinkedIn et Adobe, font confiance à Okta pour travailler plus rapidement, booster leurs revenus et maintenir la sécurité.	PrivX se démarque des outils traditionnels de gestion des accès privilégiés (PAM) en offrant une solution allégée et rentable. Par rapport aux solutions PAM, PrivX vous aide à : réduire les coûts liés à la gestion du cycle de vie des mots de passe et des coffres-forts en accordant aux utilisateurs une authentification à court terme uniquement quand ils en ont besoin. PrivX économise sur le temps exécution des tâches de déploiement et de maintenance en évitant d'utiliser des agents sur les postes de travail et les hôtes des clients
Deployment	• Cloud, SaaS, web • Windows • Linux	• Cloud, SaaS, web • Android (mobile) • iPhone (mobile) • iPad (mobile)	• Windows • Mac • Linux • Cloud, SaaS, web
Fonctionalities	❖ API ❖ Authentification multifacteur ❖ Authentification unique ❖ Gestion de la	❖ API ❖ Authentification multifacteur ❖ Authentification unique ❖ Gestion de la conformité ❖ Gestion des audits	❖ API ❖ Authentification multifacteur ❖ Authentification unique ❖ Gestion de l'accès à distance

	conformité ❖ Gestion des audits ❖ Gestion des informations d'identification ❖ Gestion des mots de passe ❖ Gestion des strategies ❖ Gestion des utilisateurs ❖ Portail libre-service	❖ Gestion des informations d'identification ❖ Gestion des mots de passe ❖ Gestion des strategies ❖ Notifications en temps réel	❖ Gestion des informations d'identification ❖ Gestion des mots de passe ❖ Gestion des strategies ❖ Suivi de l'activité des utilisateurs ❖ Suivi des activités ❖ Surveillance en temps réel ❖ Synchronisation de données ❖ Séparation des privilèges ❖ Tableau de bord d'activités
Ressources d'aide	➢ Chat ➢ Service client/e-mail ➢ Support Formation téléphonique	➢ Service client/e-mail ➢ Base de connaissances ➢ FAQ/forums ➢ Support téléphonique ➢ Chat	➢ Service client/e-mail ➢ Base de connaissances ➢ Service de support 24/7 (réponse directe) ➢ FAQ/forums ➢ Support téléphonique ➢ Chat
Formation	✓ Formation présentielle ✓ En ligne en direct	✓ Formation présentielle ✓ En ligne en direct ✓ Webinaires ✓ Documentation ✓ Vidéos	✓ Formation présentielle ✓ Documentation

Tableau III. 1: Les différents solutions de PAM

III.6. Choix de solution

En premier lieu, nous avons fait des recherches sur chacune de ces solutions. Nous constatons que Wallix Bastion est classé premier dans la gestion des accès privilégiés. Toutes les études de comparaison qui sont faites à présent ont donné cette solution comme étant la meilleure.

III.7. Présentation de la solution WALLIX Bastion

III.7.1. Présentation de l'éditeur de WALLIX Bastion

WALLIX est un acteur français reconnu depuis 2013 par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) pour son expertise dans la gestion des accès à privilèges.

WALLIX propose aux entreprises une solution permettant de gérer les risques informatiques liés aux comptes à privilèges en sécurisant leurs accès, leurs mots de passe et en assurant la traçabilité de leurs utilisateurs internes et externes (prestataires). Elle contribue à la mise en conformité des entreprises avec les réglementations de leur secteur d'activité (secteur sensible, santé, finance & assurance) ou de leur métier (fournisseur de services informatiques, hébergeurs de cloud et de données)[14].

III.7.2. Définition de WALLIX Bastion

Wallix Bastion est une panoplie de solutions PAM (Privileged Access Management) simples et efficaces dont l'objectif principale est la traçabilité des accès serveurs. En d'autres termes, les solutions WAB (Wallix Admin Bastion) permettent aux RSI (Réseaux des Systèmes Informatiques), ingénieurs ou administrateurs de sécurité, de savoir, en temps réel ou en différé, qui fait quoi, quand, où et comment?

La solution Wallix Bastion, permet aux entreprises d'immenses possibilités, notamment la traçabilité, le contrôle d'accès aux serveurs, la journalisation des connexions, la surveillance en temps réel, l'analyse du flux SSH, les statistiques et rapports d'activité, et pleins d'autres options.

La solution **WALLIX** fournit également un enregistrement vidéo de la session, de sorte qu'il est possible de visualiser précisément ce que l'utilisateur à privilèges a fait au cours de la

[14] https://www.certilience.fr/2019/06/simplifier-la-gestion-des-comptes-a-privilege-le-bastion-wallix/

session. Si quelque chose de dommageable s'est produit, le responsable sécurité en connaîtra tout de suite tous les détails[15].

Figure III.4 : Wallix logo

III.7.3. Fonctions de sécurité de Wallix Bastion

Les fonctions de sécurité évaluées du Wallix Bastion sont[16] :

- ✓ Les communications sécurisées entre le domaine « utilisateurs » et le domaine « ressources ».
- ✓ L'authentification et le contrôle des accès aux ressources,
- ✓ L'authentification et le contrôle d'accès à l'interface web,
- ✓ L'authentification unique des utilisateurs,
- ✓ La traçabilité des connexions aux ressources,
- ✓ La traçabilité des actions effectuées sur l'interface web,
- ✓ Le stockage sécurisé, le durcissement du Bastion.

III.7.4. Solution de WALLIX Bastion

WALLIX nous propose trois briques permettant de répondre à différents besoins[17] :

III.7.4.1. Session Manager

Grâce au module Session Manager, les sessions utilisateurs font l'objet d'une traçabilité sous forme d'enregistrements qui peuvent être contrôlés en temps réel ou à posteriori. Bastion enregistre la session graphique, capturant tous ce qui est écrit au clavier par les applications utilisées. Il est ainsi possible de savoir qui s'est connecté, quand, à quel compte cible, pendant

[15] https://www.alphorm.com/tutoriel/formation-en-ligne-wallix-bastion-le-guide-du-debutant/tuto-video-se-connecter-en-rdp
[16] Rapport de certification ANSSI-CSPN-2019/15
[17] https://www.certilience.fr/2019/06/simplifier-la-gestion-des-comptes-a-privilege-le-bastion-wallix/

combien de temps ? on peut aussi visionner l'enregistrement de la session pour analyser son contenu. Les alertes se font en temps réel et n'importe quel incident qui pourrait avoir lieu peut être recherché rapidement à des fins d'audit.

Les entreprises peuvent ainsi définir le niveau de sécurité des accès, garantir l'intégrité de leurs fichiers informatiques et prouver que leurs règles d'utilisation sont conformes aux normes et réglementations en vigueur dans leur secteur d'activité. Les utilisateurs se connectent à un compte unique qui leur donne accès à l'ensemble des données dont ils ont besoin, optimisant ainsi leur productivité. Par ailleurs, les utilisateurs, qui accèdent régulièrement à des données sensibles, tels que les directeurs informatiques, les RSSI (Responsables de la Sécurité du Système d'Information), les directeurs de sûreté ou les directeurs des risques ont, grâce à cette solution, une garantie de leur activité vis-à-vis de leurs employeurs, de leurs entreprises ou de leurs clients.

Cela rend possible :

- La centralisation des accès au système d'information de l'entreprise ;
- L'identification des utilisateurs de comptes à privilèges et de comptes partagés ;
- La surveillance en temps réel et l'enregistrement du déroulement des interventions des personnes qui utilisent les accès privilégiés au système d'information ;
- La traçabilité et l'alerte en temps réel sur une utilisation non conforme du système ;
- L'audit à posteriori des enregistrements des sessions des utilisateurs de comptes à privilèges.

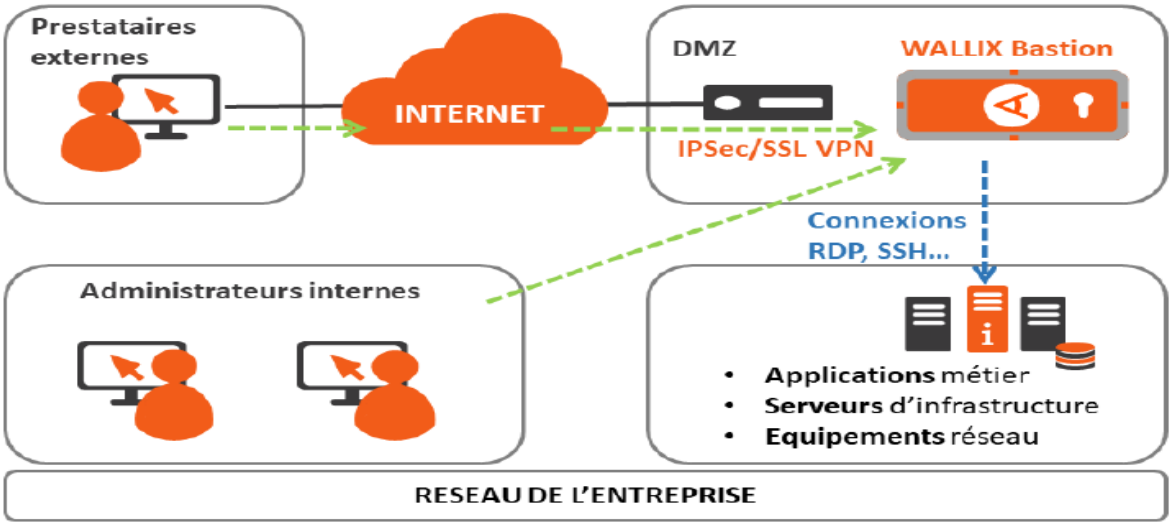

Figure III.5 : Exemple d'une architecture réseau d'entreprise

III.7.4.2. Password Manager (gestion centralisée des mots de passe)

La ‘brique’ Password Manager permet aux équipes informatiques de gérer de manière centralisée le stockage et l’utilisation des mots de passe et des clés (SSH où RDP) par les utilisateurs du Système d’Information.

Contrairement à un coffre-fort de type Keepass, il est possible de partager uniquement les identifiants souhaités avec les personnes habilitées.

Ce module permet également de gérer la rotation automatique des mots de passe sur les ressources cibles.

III.7.4.3. Access Manager (accès aux ressources depuis un navigateur web)

La ‘brique’ Access Manager ajoute une possibilité de connexion depuis un navigateur aux cibles auxquelles des utilisateurs sont autorisés à se connecter. Ces accès aux ressources cibles sont toujours effectués à travers le Bastion. Mais les connexions sont initiées grâce aux clients HTML5 (sans extension supplémentaire dans le navigateur) de l’Access Manager.

Access Manager autorise également les utilisateurs possédant les droits adaptés à afficher les mots de passe des cibles dans le navigateur ou/et de les copier dans le presse-papier.

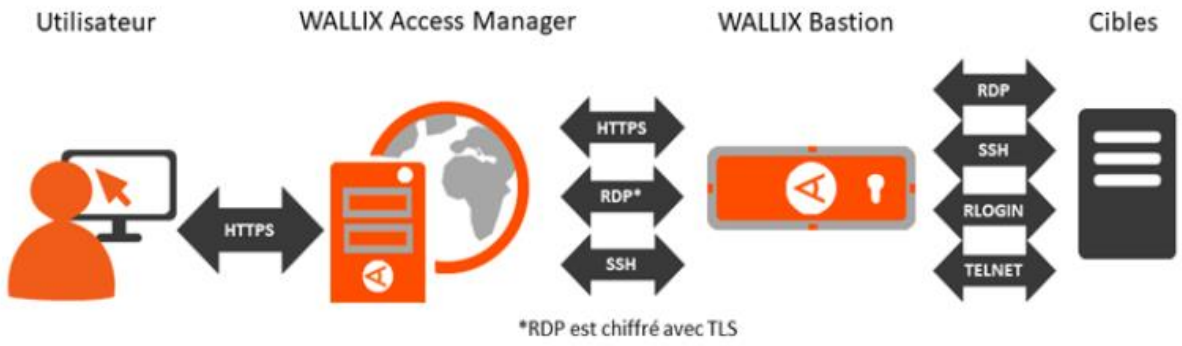

Figure III.6 : La gestion centralisée des mots de passe

III.7.4.4. Positionnement des trois briques dans l’infrastructure

Les briques principales Session Manager et Password Manager sont installées sur la même machine afin de partager le coffre-fort à mots de passe. Voici ci-dessous le schéma de l’infrastructure en fonction de la présence ou non de la brique Access Manager.

✓ **Sans la brique Access Manager**

Dans le cas d'un environnement sans Access Manager, cette machine ne doit jamais être exposée directement sur Internet. Pour cela, il est nécessaire de mettre à disposition un VPN aux prestataires ou administrateurs externes, qui autorisera ensuite la connexion au bastion par SSH ou RDP.

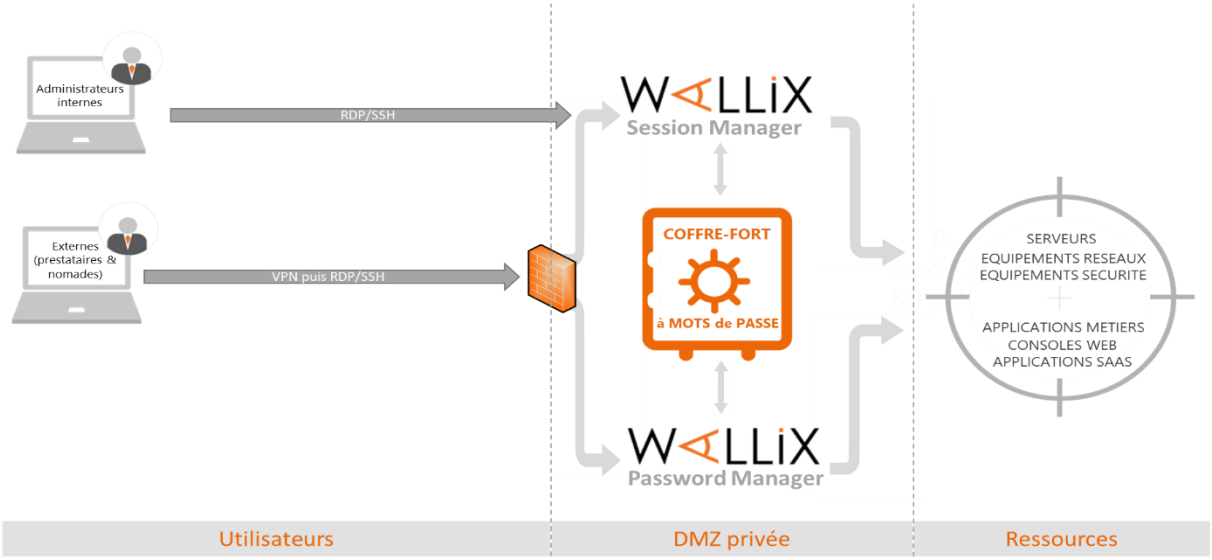

Figure III.7 : Le schéma du coffre-fort wallix sans l'accès manager

✓ **Avec la brique Access Manager**

Dans le cas où la brique Access Manager est déployée, les prestataires ou administrateurs externes auront toujours la possibilité de se connecter en SSH/RDP au Session Manager par l'intermédiaire d'un VPN.

En complément, les utilisateurs externes pourront également se connecter au Session Manager par l'intermédiaire de l'Access Manager directement depuis un navigateur. La brique Access Manager devra être installée sur une seconde machine.

Exemples d'utilisation :

- Lorsqu'il est impossible de fournir une connexion VPN à un prestataire ou administrateur nomade
- Lorsqu'un utilisateur doit se connecter aux ressources depuis un équipement ne disposant pas de VPN (nouveau PC) ou ne permettant pas la connexion en RDP/SSH

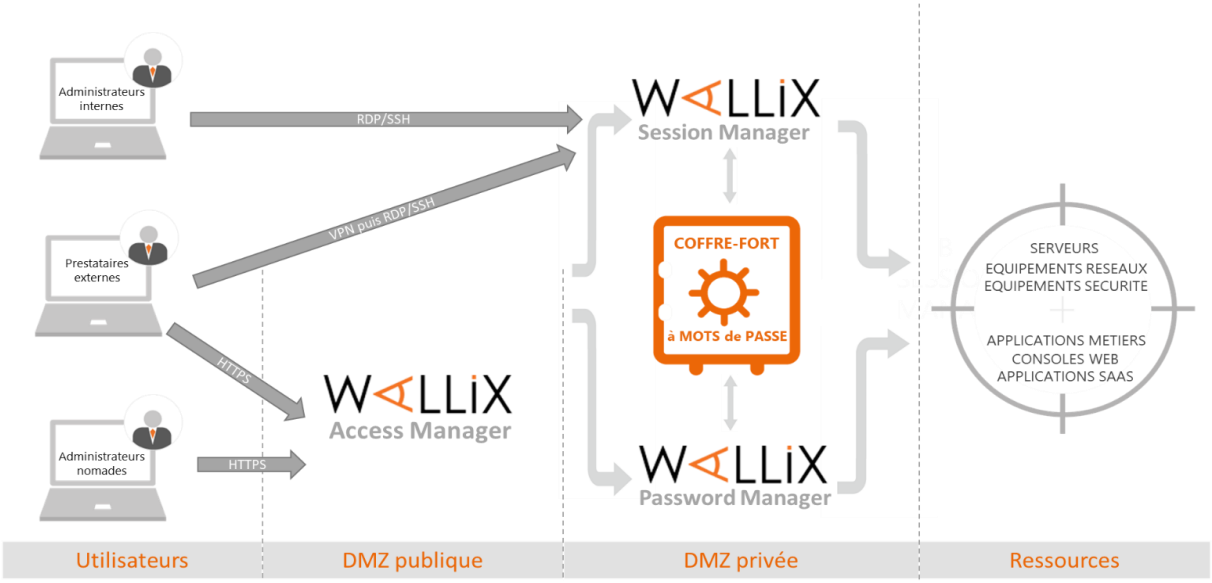

Figure III.8 : Le schéma du coffre-fort wallix avec l'accès manager

Conclusion

Dans ce chapitre, nous avons présenté la nouvelle architecture de groupe IFRI en cours de réalisation et la solution à déployer (Wallix Bastion). Nous avons cité les concepts fondamentaux des PAM (Priviliged Access Management) qui sont particulièrement nécessaires pour la suite de notre travail.

Nous traiterons dans ce qui suit, la configuration de Wallix Bastion et ces déférents services.

Chapitre IV

Réalisation

Introduction

Afin de démontrer l'efficacité de notre solution wallix qui est implémentée sur le firewall de « data center », nous allons exécuter une démonstration qui décrira les différentes étapes de la démarche suivie pour l'application du contrôle d'accès (PAM). Ainsi, nous avons détaillé, dans ce chapitre, toutes les étapes d'installation et de configuration de la solution et ses différents services.

Dans le cadre de notre travail, nous avons fait appel au logiciel VMware Workstation qui permet de simuler plusieurs machines.

IV.1. Installation et configuration de Windows server 2012

En premier lieu, nous avons introduit les différentes étapes à suivre pour installer et configurer Windows server. À la fin de cette installation, nous avons installé les différents services offerts par ce dernier.

IV.1.1. Windows server 2012

Nous avons installé Windows Server 2012 qui est nécessaire si l'on souhaite créer un compte utilisateur afin d'utiliser un accès privilégié à distance en SSH ou RDP.

- **Installation Windows server 2012**

1. Nous avons installé la base classique, puis avons booté sur l'image ISO d'installation de WindowsServer 2012.

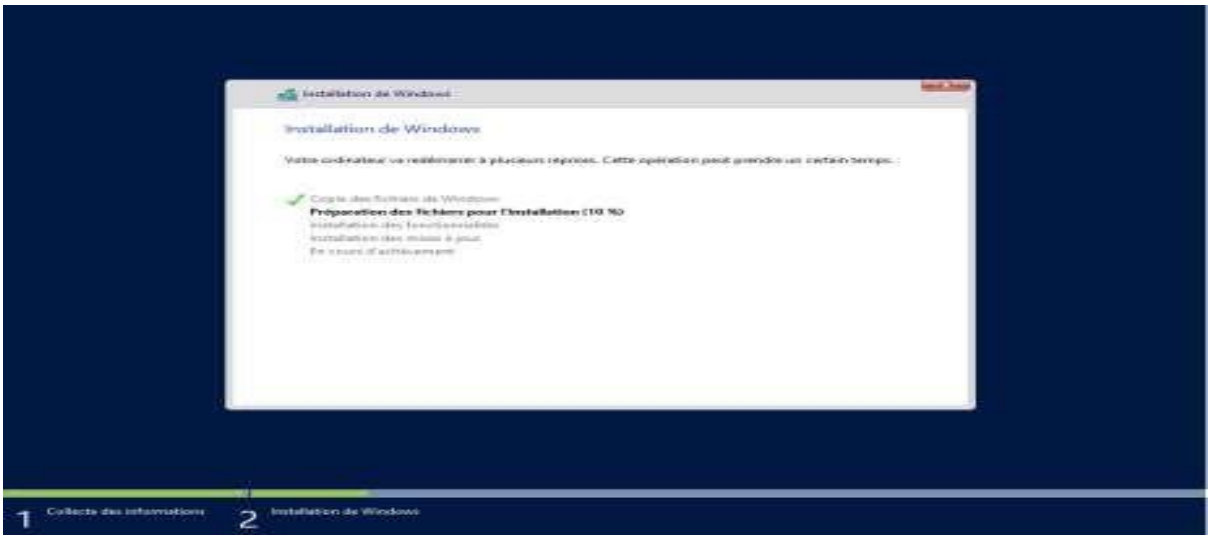

Figure IV-1 : Installation en cours.

2. Après cela, le système redémarre automatiquement et nous demande de paramétrer la date et l'heure, ainsi qu'un mot de passe pour le compte Administrateur. Ce mot de passe doit répondre à la stratégie de complexité des mots de passe définies par défaut dans les éditions serveurs de Windows. A la fin on clique sur "**Terminer**" pour confirmer et continuer.

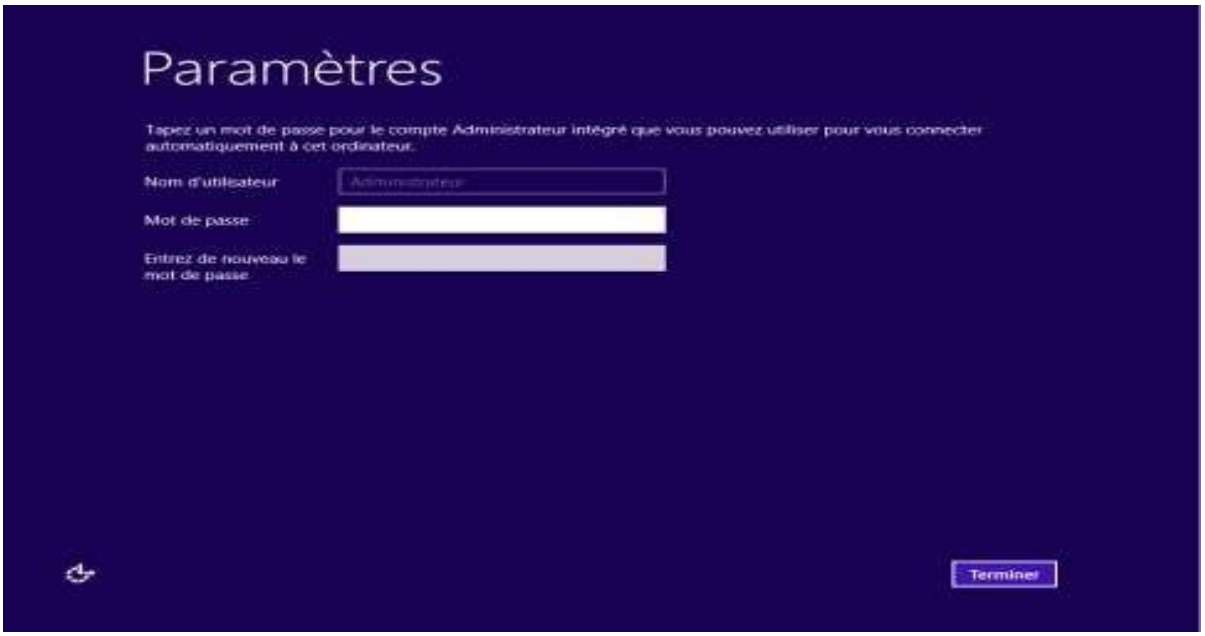

Figure IV-2: Définition d'un mot de passe pour le compte Administrateur.

3. Ouvrir la session Administrateur en appuyant sur "**Ctrl+Alt+Suppr**".

Figure IV-3 : Session administrateur.

Installation terminée

- **Configuration de Windows Server 2012**

Une fois l'installation terminée, nous procédons à la configuration de l'ensemble des paramètres généraux de Windows Server 2012 à l'aide de la page d'accueil du gestionnaire de serveur.

Notons que le gestionnaire de serveur de Windows server 2012 est automatiquement chargé lors de l'ouverture de la session.

a. Configuration des paramètres TCP/IP

Nous accédons au **centre de réseau et partage**, ensuite aux propriétés de notre connexion réseau. Par default, celle-ci est nommée **connexion au réseau local** on clique sur **Ethernet**, puis sur « **propriétés ».** Cette denier nous permet d'accéder aux propriétés du protocole TCP/IP pour attribué les initialisations.

Dans notre cas, nous avons choisi les adresses IP (IPv4) suivantes :

- Adresse IP : 172.16.102.107
- Masque de sous réseau : 255.255.252.0
- Passerelle par défaut : 172.16.102.254
- Serveur DNS préféré : 172.16.102.5
- Serveur DNS auxiliaire : 172.16.102.14

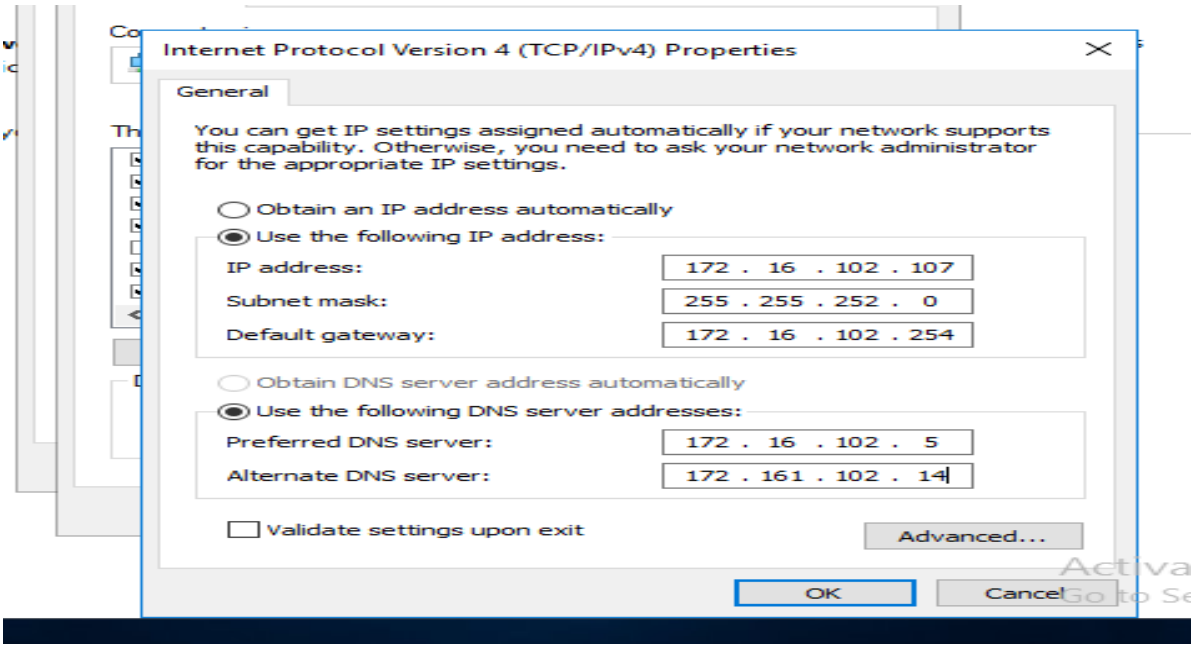

Figure IV-4 : Configuration du protocole TCP/IP.

b. Vérification de la configuration TCP/IP

Nous utilisons l'invite de commande sur lequel on introduit la commande **IP config/all**, et nous aurons comme résultat ce qui est affiché sur la figure si dessous (**Figure IV-5).**

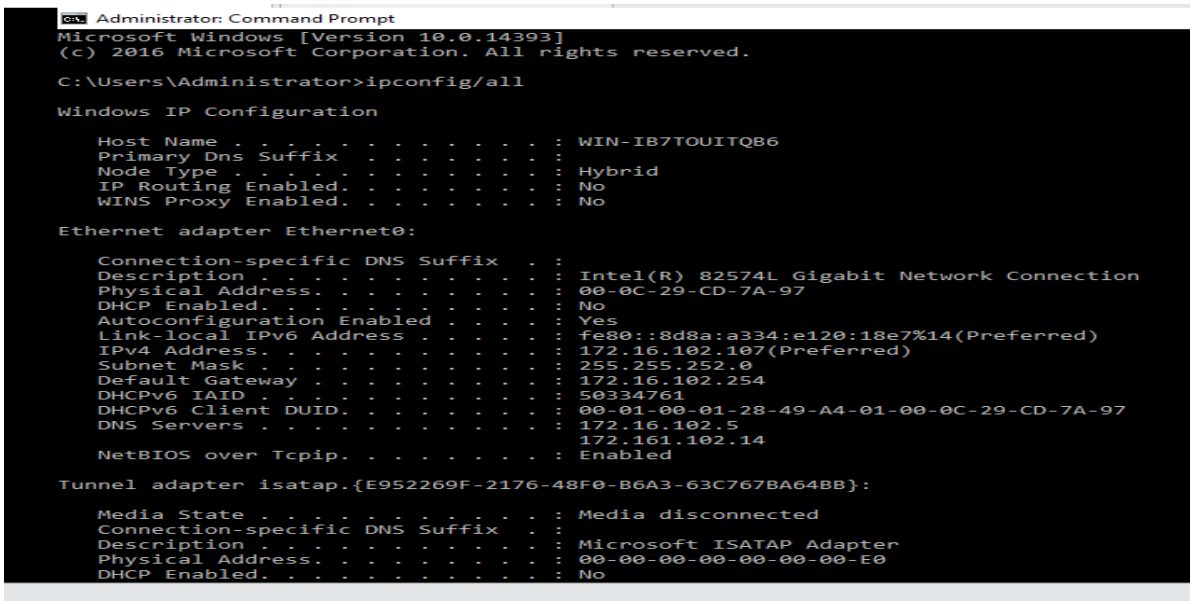

Figure IV-5 : Vérification de protocole TCP/IP.

c. Test de connectivité

Dans cette partie, nous testons notre adresse TCP/IP en tapant la commande **Ping172.16.102.107**

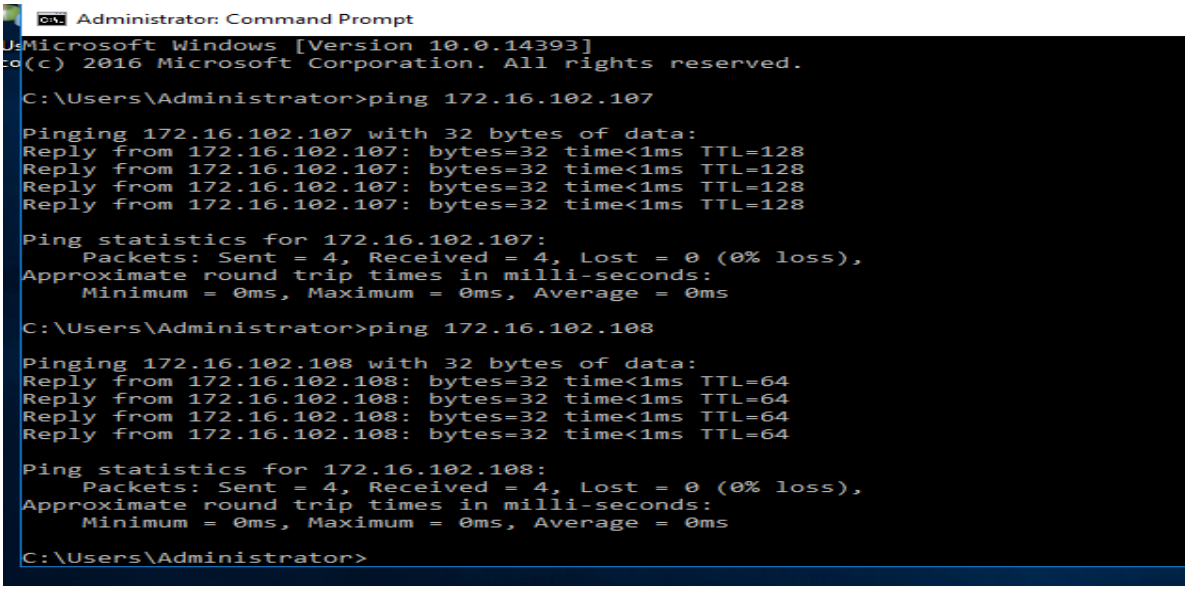

Figure IV-6 : Test de connectivité

IV.1.2. Création d'un compte local utilisateur

a. Nous procédons à la création d'un compte local utilisateur (ifri), qui va lui permettre d'accéder au serveur avec usage de la solution wallix.

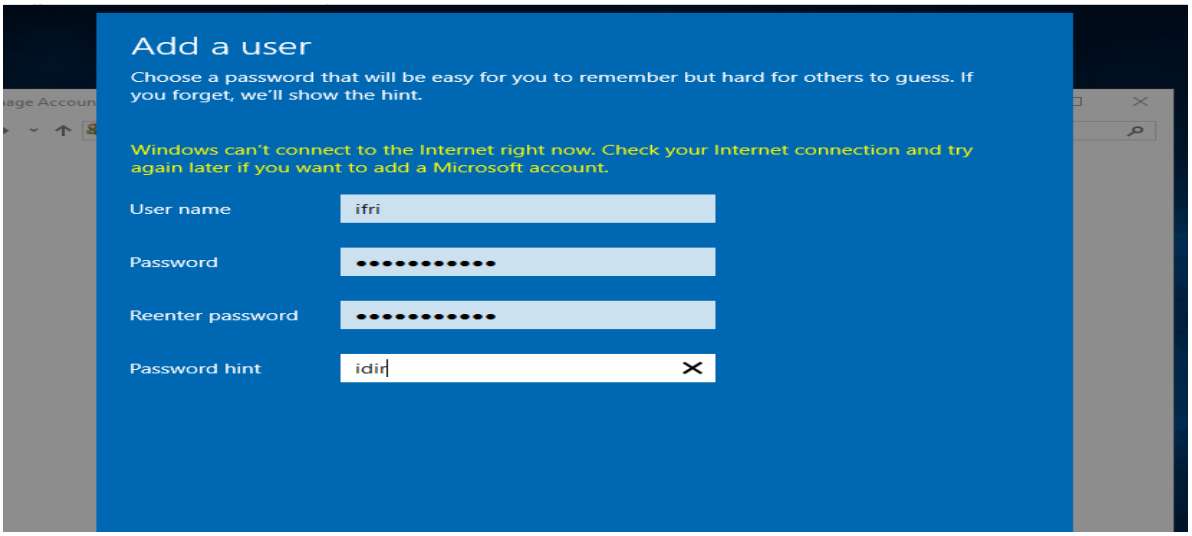

Figure IV-7 : Création du compte utilisateur

b. Compte créés

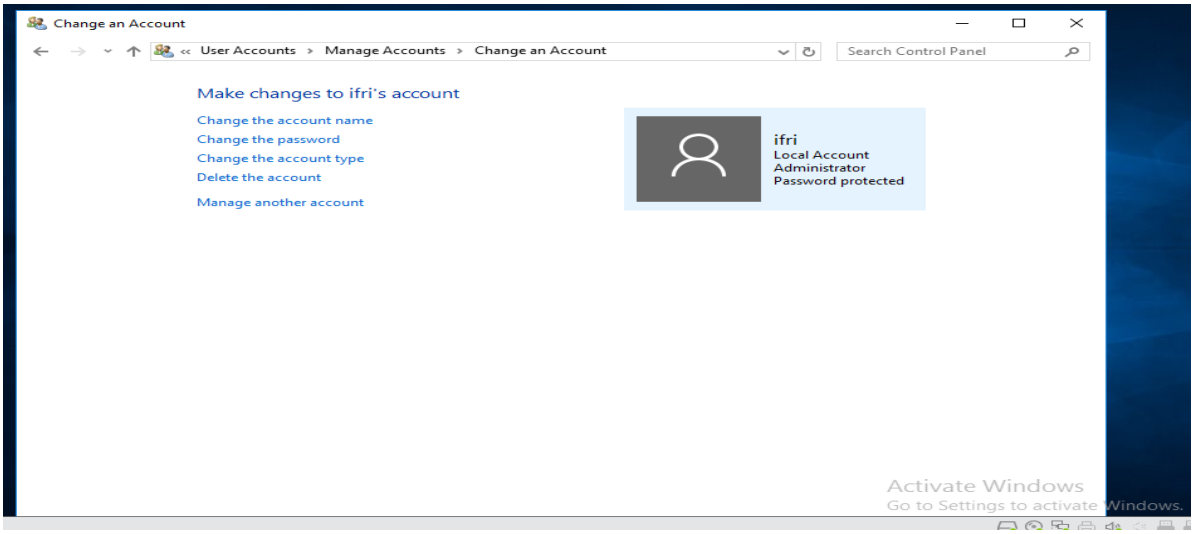

Figure IV-8 : Compte local utilisateur crées « ifri »

IV.2. Installation et configuration de wallix bastion

Après avoir suivi la vidéo de démonstration d'installation et de fonctionnement de wallix bastion, nous allons procéder à son installation réelle :

a. Dans la **Figure IV-9** nous commençons par le lancement de la démo de wallix bastion avec la VMware Workstation.

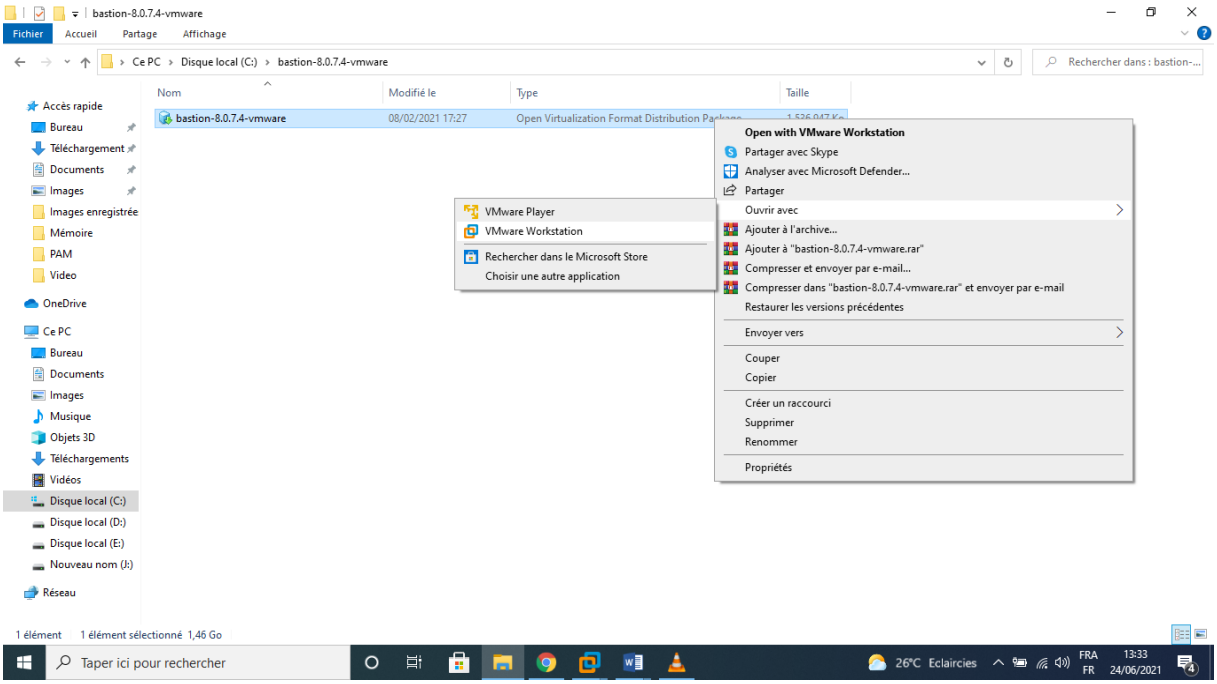

Figure IV-9 : Lancement de Wallix bastion avec la VMware Workstation

b. Une fois VMware lancé, nous devons d'abord augmenter l'espace du disque de la VMware comme l'indique la **Figure IV-10.**

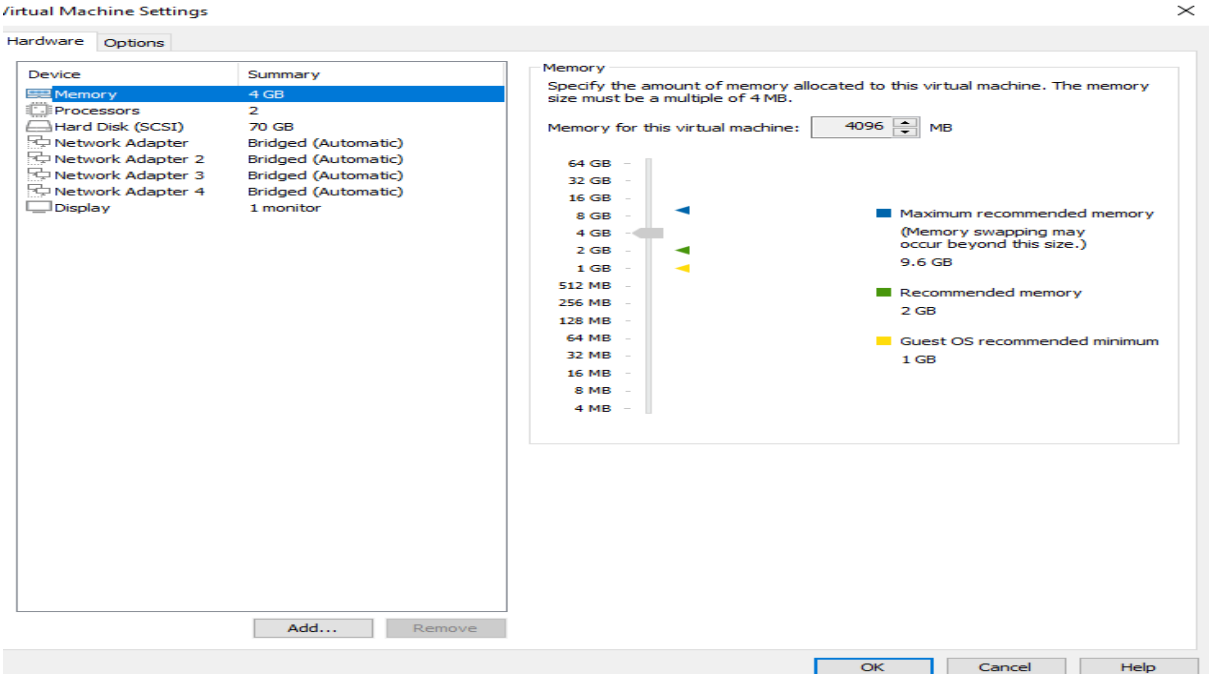

Figure IV-10 : Augmenter l'espace disque

c. Ensuite, nous démarrons le Wallix bastion pour que l'installation se lance.

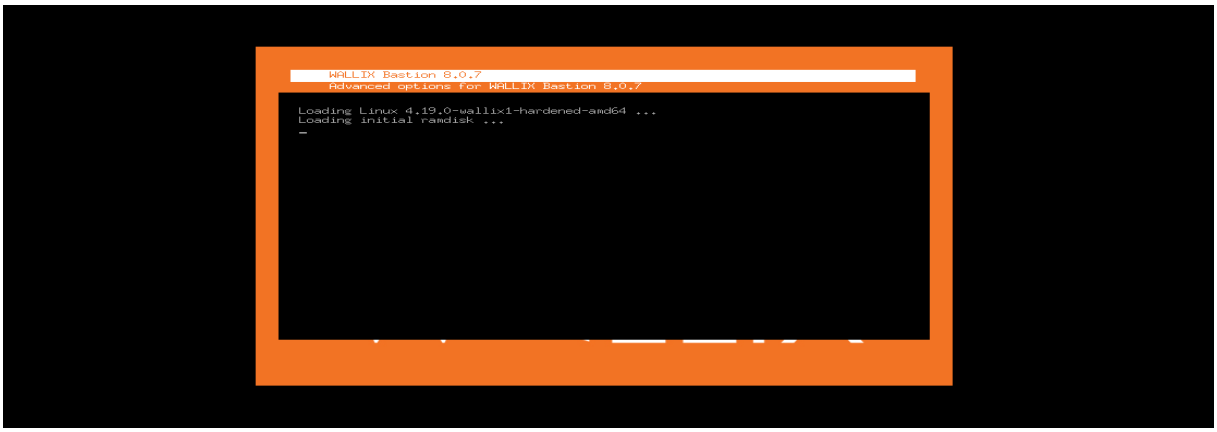

Figure IV-11 : Chargement de l'installation

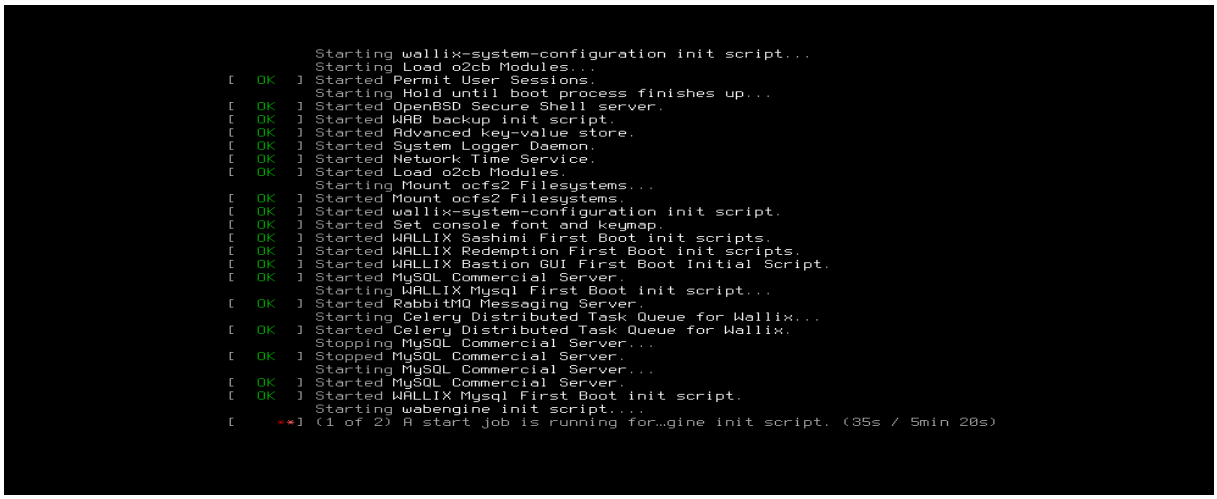

Figure IV-12 : Téléchargement Wallix Bastion en cour

d. Une fois le téléchargement terminé, cela vas nous ouvrir l'accès au lancement de la configuration de wallix comme l'indique les Figures qui suit :

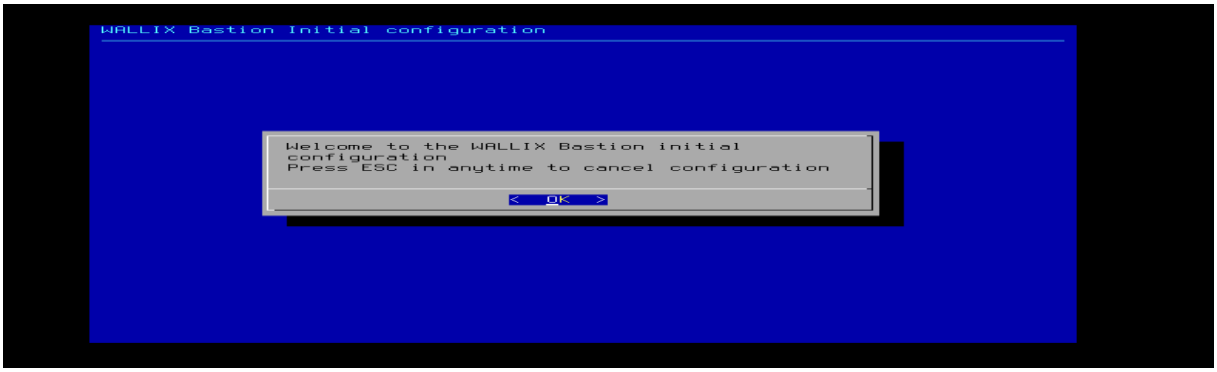

Figure IV-13 : Configuration des paramètres de Wallix Bastion

e. En premier lieu, nous allons choisir la langue à utiliser pour procéder à la configuration.

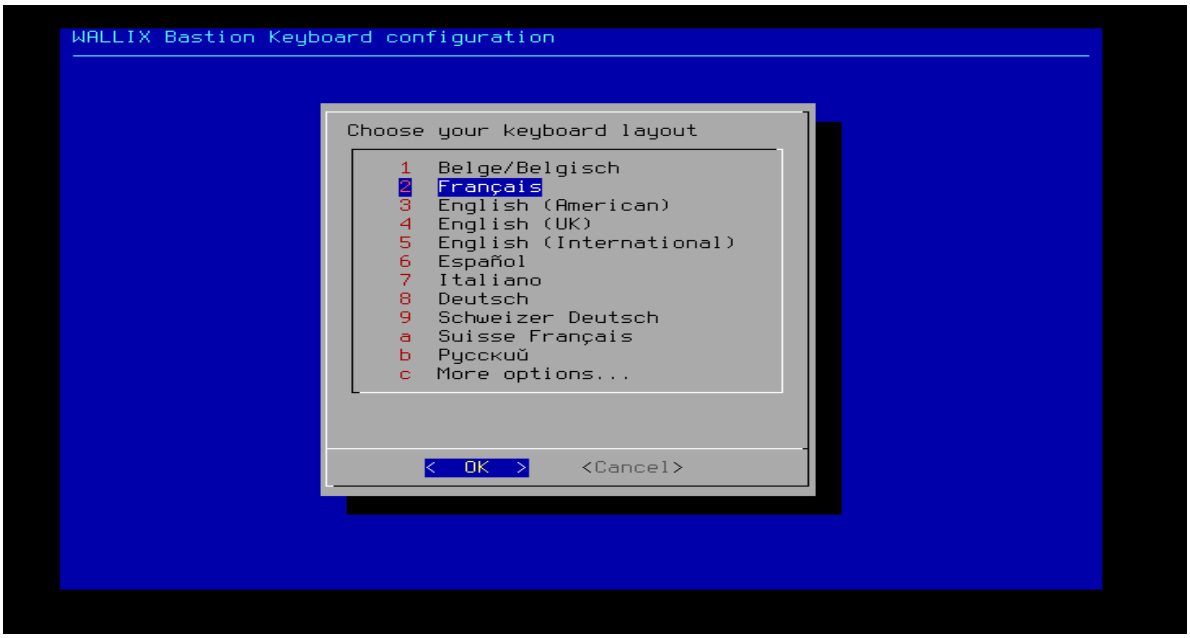

Figure IV-14 : Le choix de la langue

f. Puis, Nous saisissons le mot de passe de wabadmin qui nous a été fourni par la société wallix bastion comme l'indique la **Figure IV-15.**

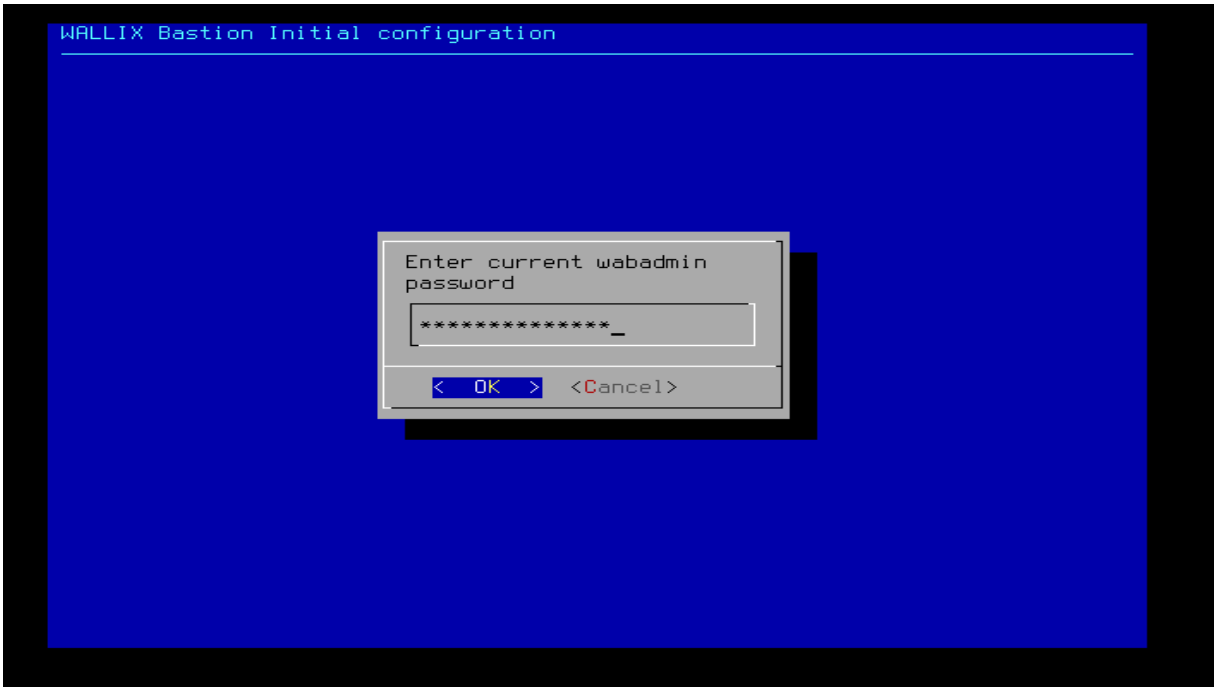

Figure IV-15 : Saisir le mode passe

g. De plus pour sécuriser notre session de wabadmin, nous procédons à un changement du mot de passe wabadmin.

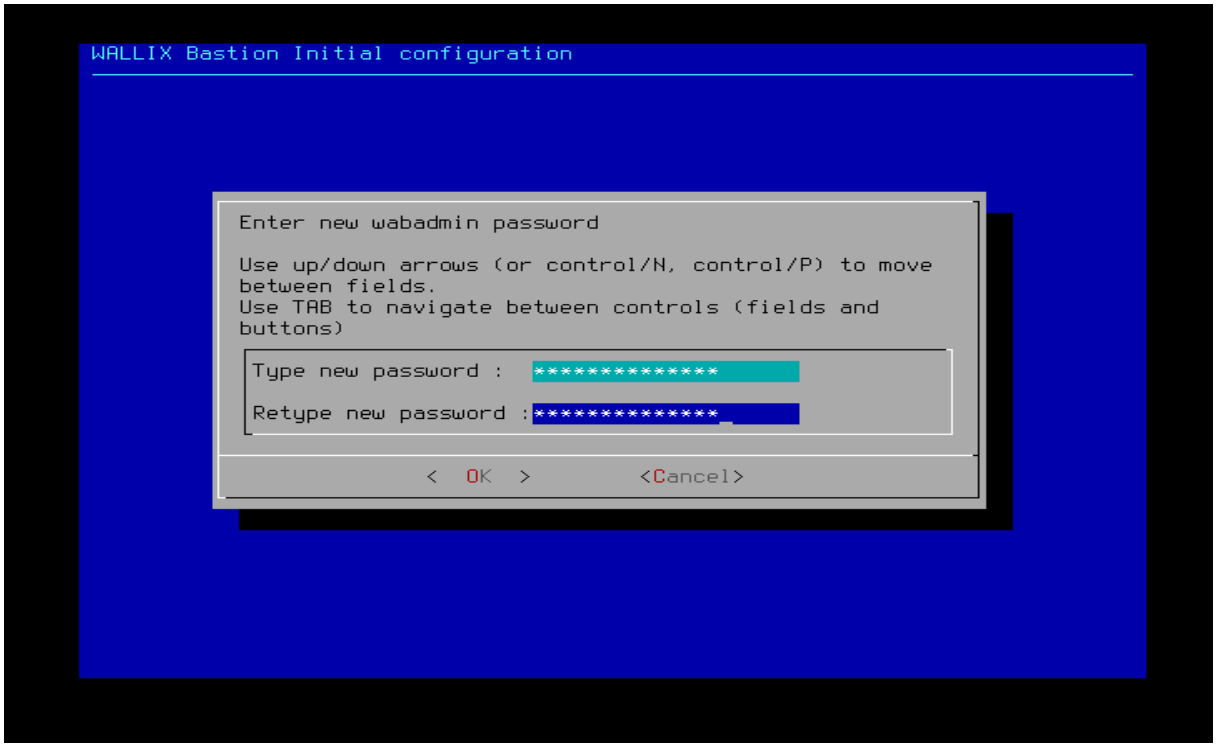

Figure IV-16 : Changement du mot de passe wabadmin

h. En second lieu, nous lançons la configuration du réseau wallix bastion en appuyant sur « **yes »,** comme l'indique la figure ci-dessous.

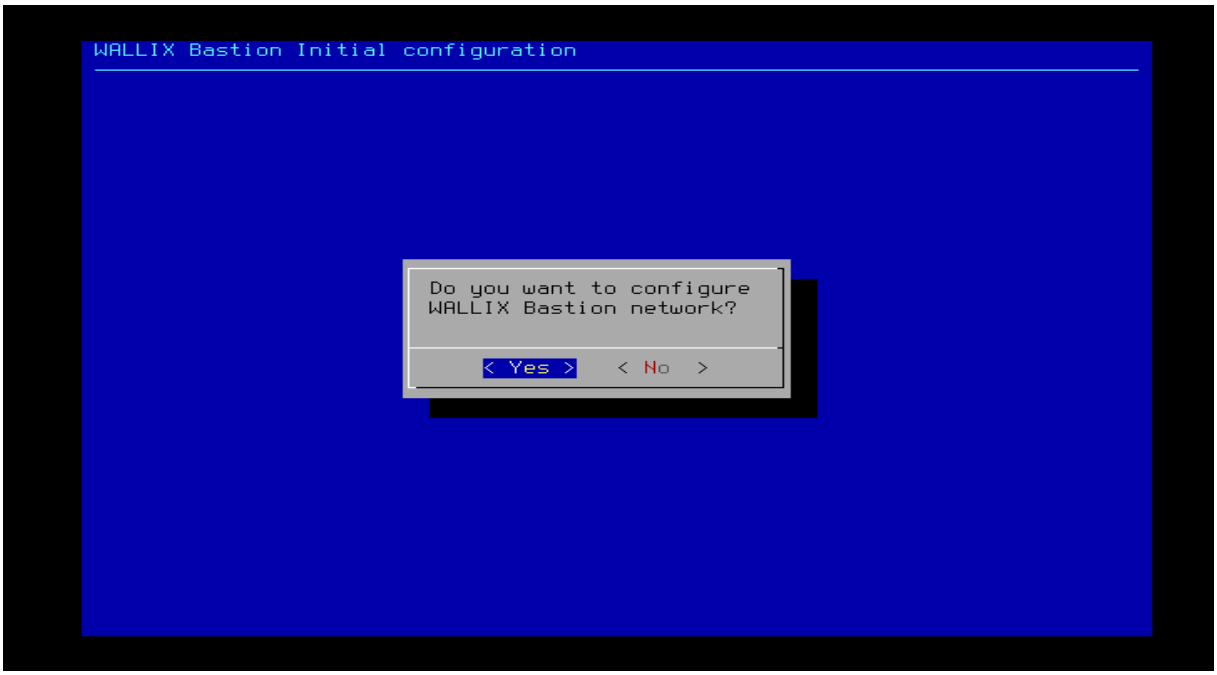

Figure IV-17 : Configuration de réseau Wallix Bastion

i. Dans cette page, nous accédons au paramètre de configuration de Wallix Bastion, en procédant à la configuration de l'adresse IP de réseau, en cliquant sur **Eth0** comme indiquer dans la **figure IV-18**.

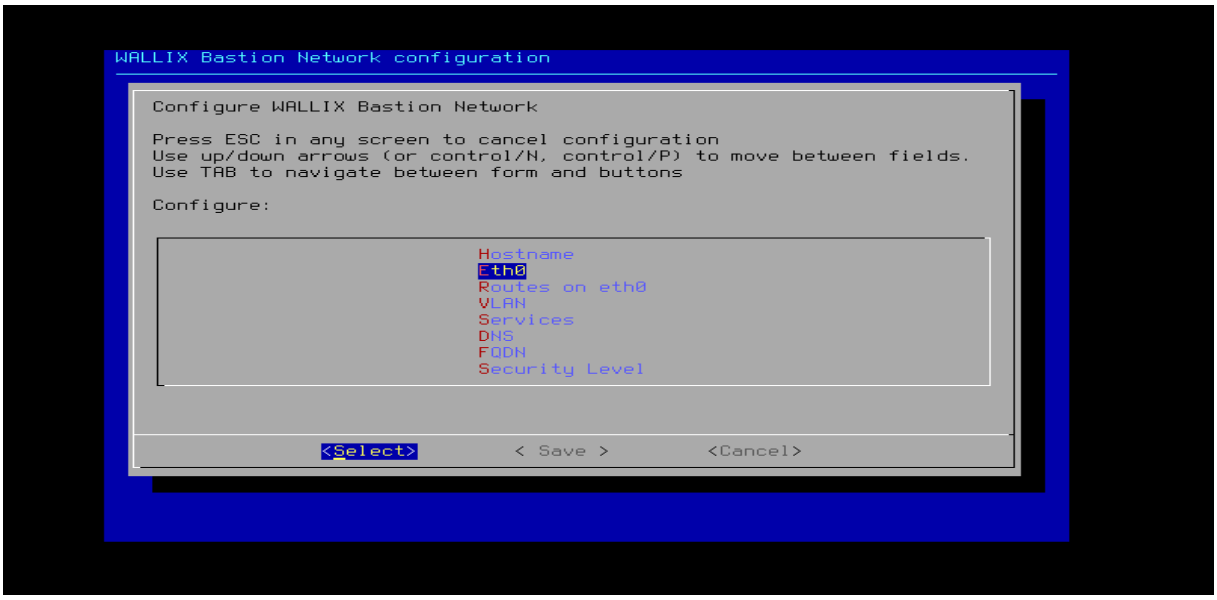

Figure IV-18 : Configuration de l'adresse de réseau

j. On clique sur Eth**0.** Cela nous mène à l'interface ci-dessous pour choisir notre propre configuration en mode **Ethernet** en cliquant sur **NO**.

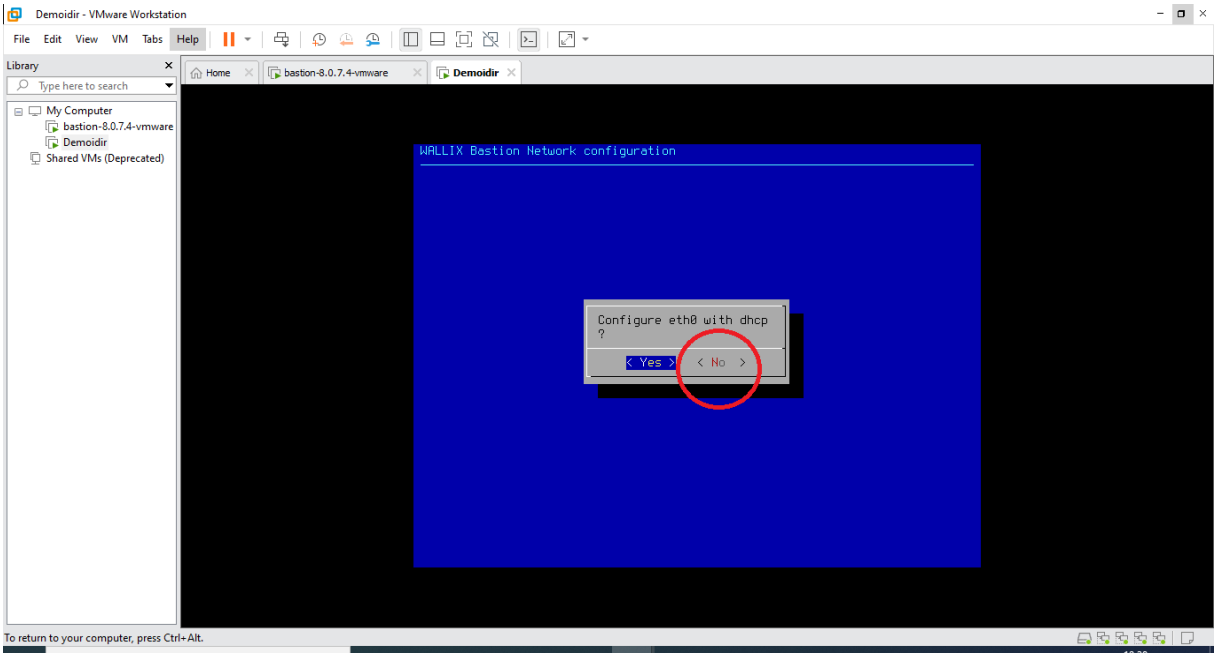

Figure IV-19 : Le choix « No » (configuration de notre choix)

k. En cliquant sur **NO,** nous pouvons modifier l'adresse IP qui communique avec nos serveurs, avec laquelle on communiquera avec notre serveur bastion. OK nous permet de retourner vers la **figure IV-18** pour faire la sauvegarde.

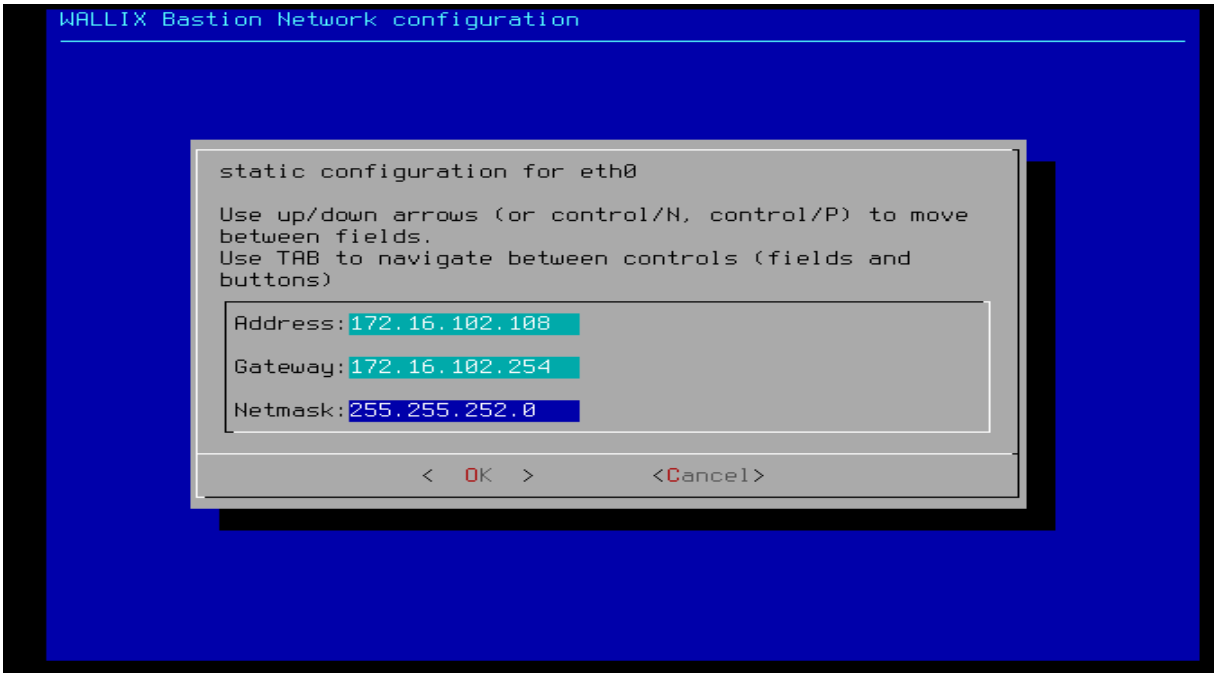

Figure IV-20 : Introduire notre adresse réseau

l. Dans la **figure IV-21** il y a lieu de noter l'adresse IP configurée une fois l'installation terminée et parce que la configuration de système se fait à travers une interface web.

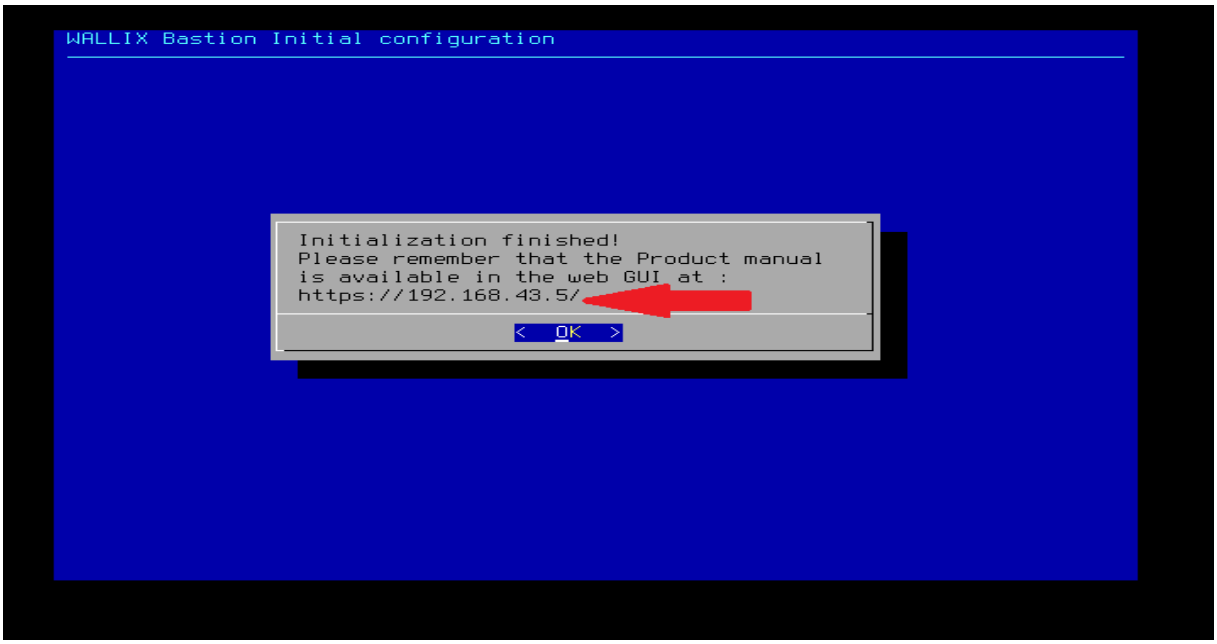

Figure IV-21 : Génération de l'adresse IP

Fin de l'installation.

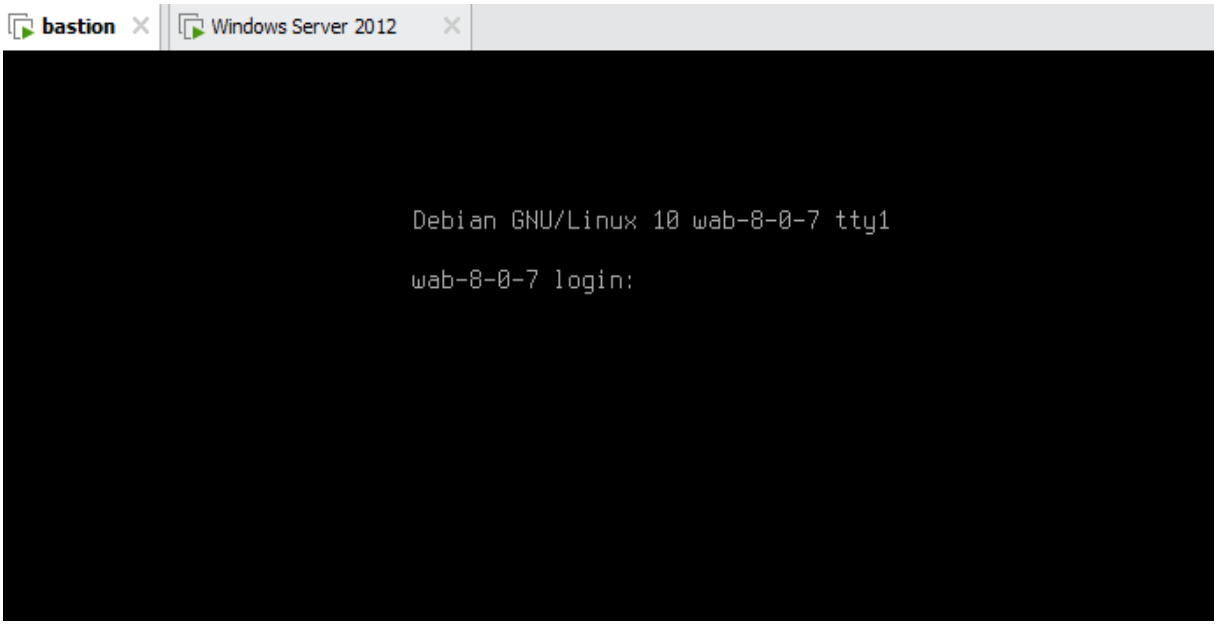

Figure IV-22 : Fin de l'installation

IV.2.1. Connexion sur la plateforme Wallix Bastion avec Web

a. Nous introduisons notre adresse IP sur le web, puis cliquons sur le cercle 2 comme l'indique la figure suivant :

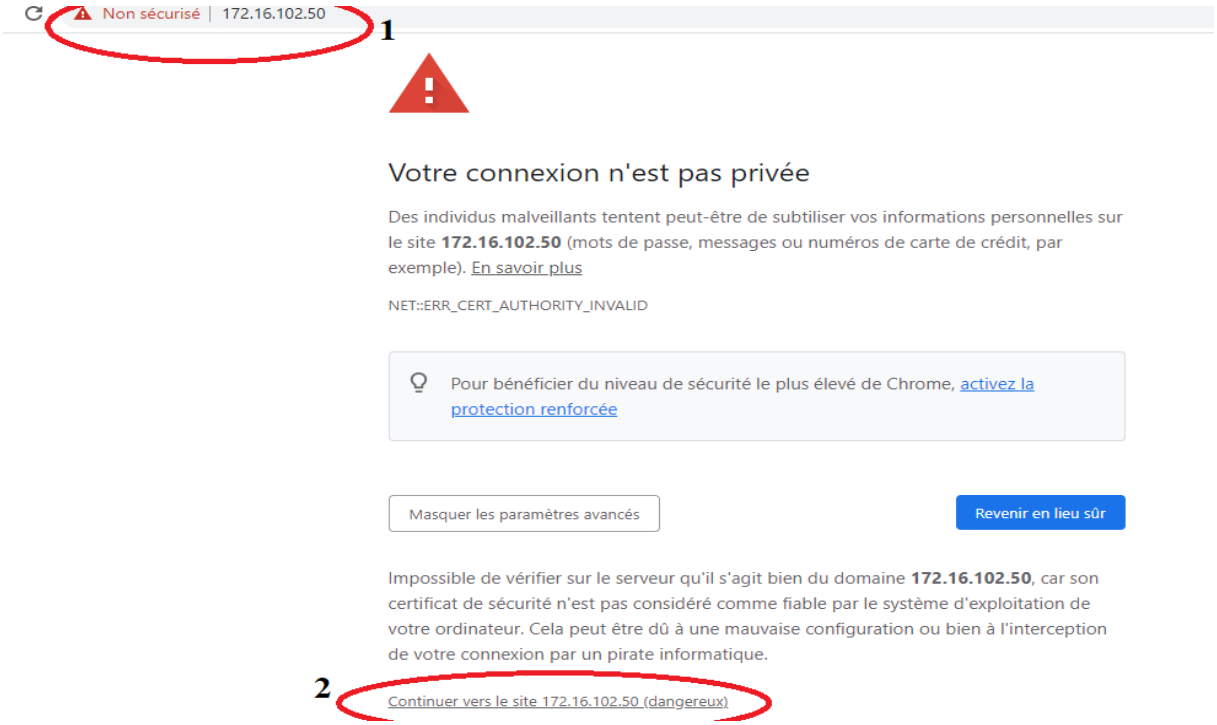

Figure IV-23 : Interface web

b. La connexion vers Wallix Bastion se fait une fois le nom de l'utilisateur et son mot de passe qui nous a été fourni par le guide de l'installation sont introduits.

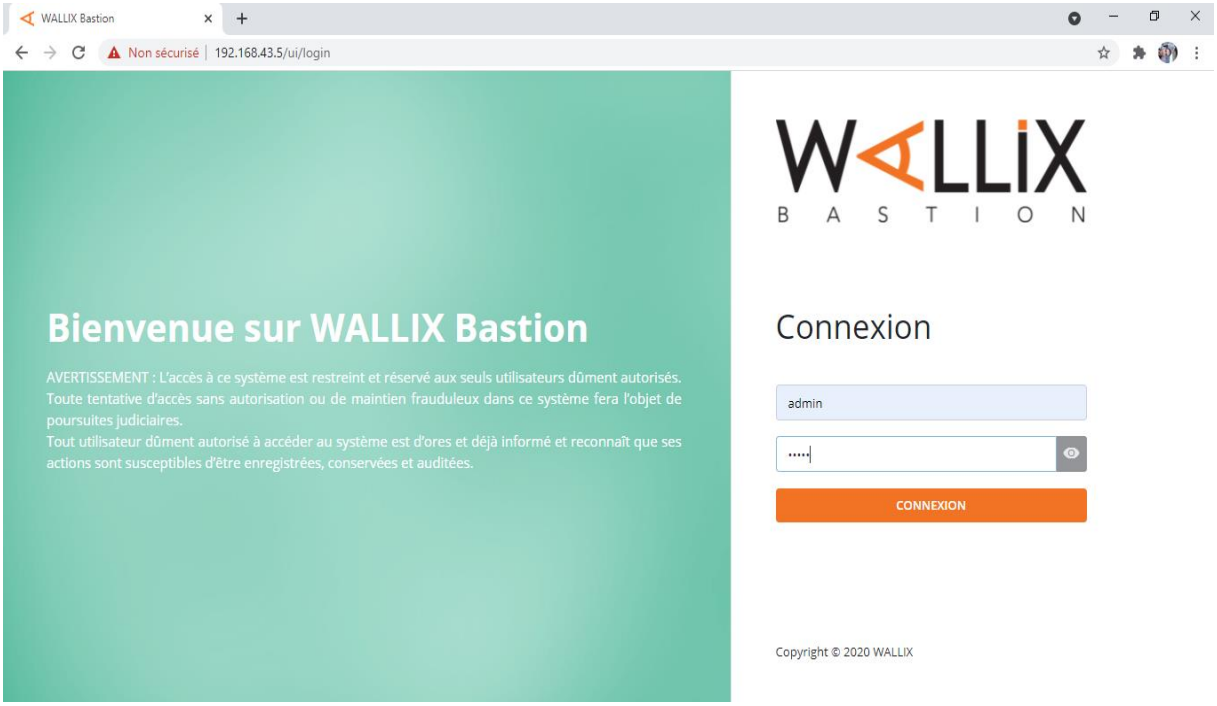

Figure IV-24 : Essai de l'interface de connexion de Wallix Bastion

c. Une fois l'étape précédente est effectuée, il va nous demander de ré-sécuriser notre système par un autre mot de passe.

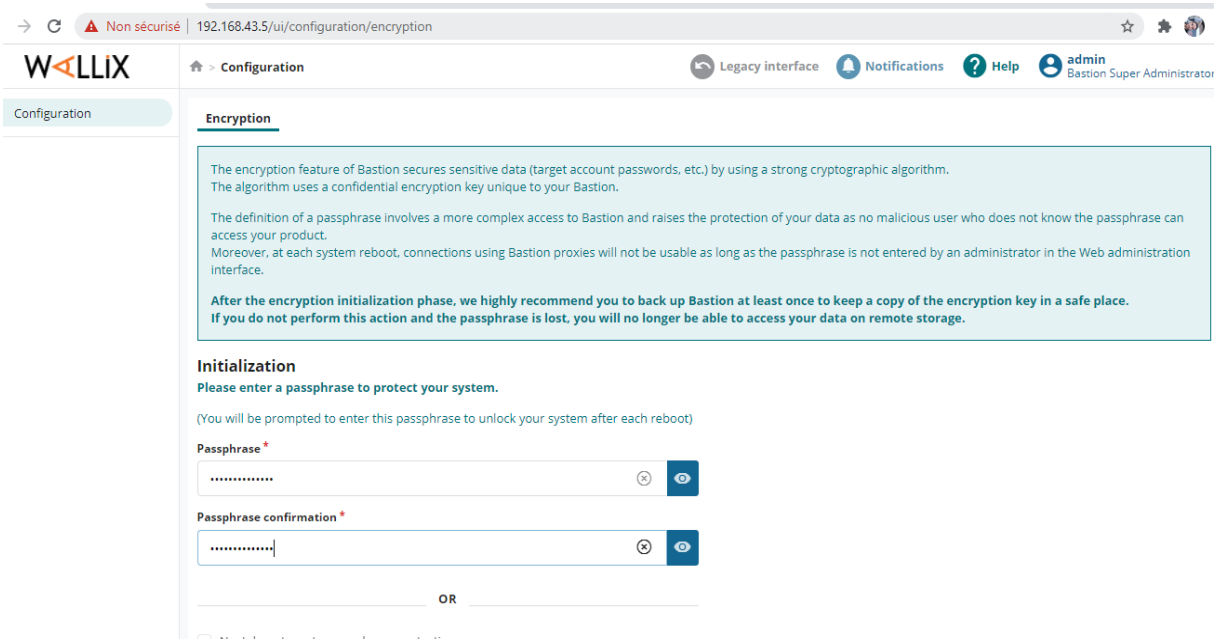

Figure IV-25 : Sécurisation du système

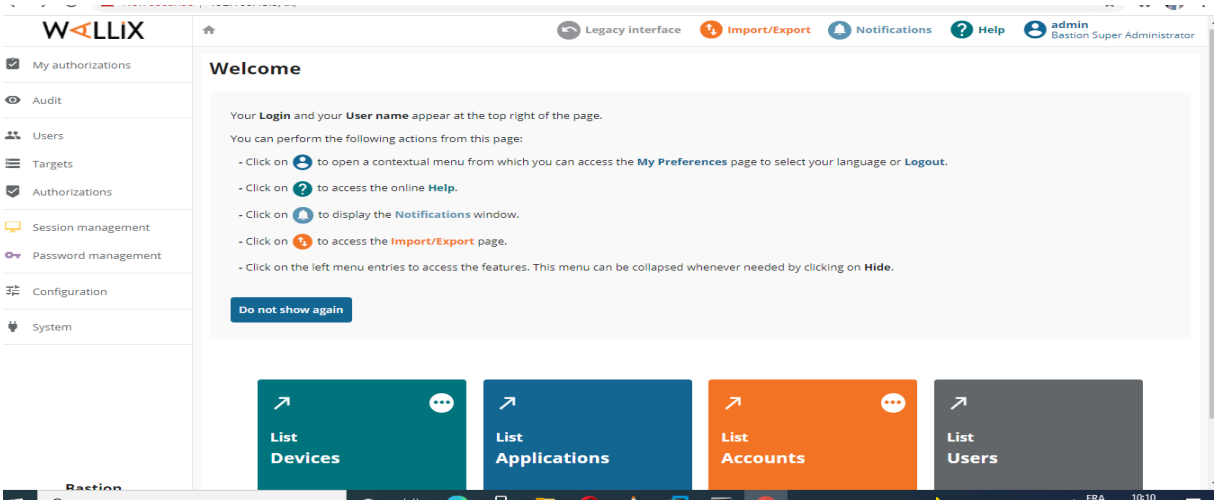

Figure IV-26 : Interface d'accueil de Wallix Bastion

IV.2.2. Configuration de système de wallix bastion

Pour la configuration de système de Wallix Bation, nous procéderons comme suite:

IV.2.2.1. Création d'un compte utilisateur pour lui donner l'accès privilégié vers des systèmes cibles

a. Accéder sur « **Users** » comme indiqué sur la **figure IV-27**.

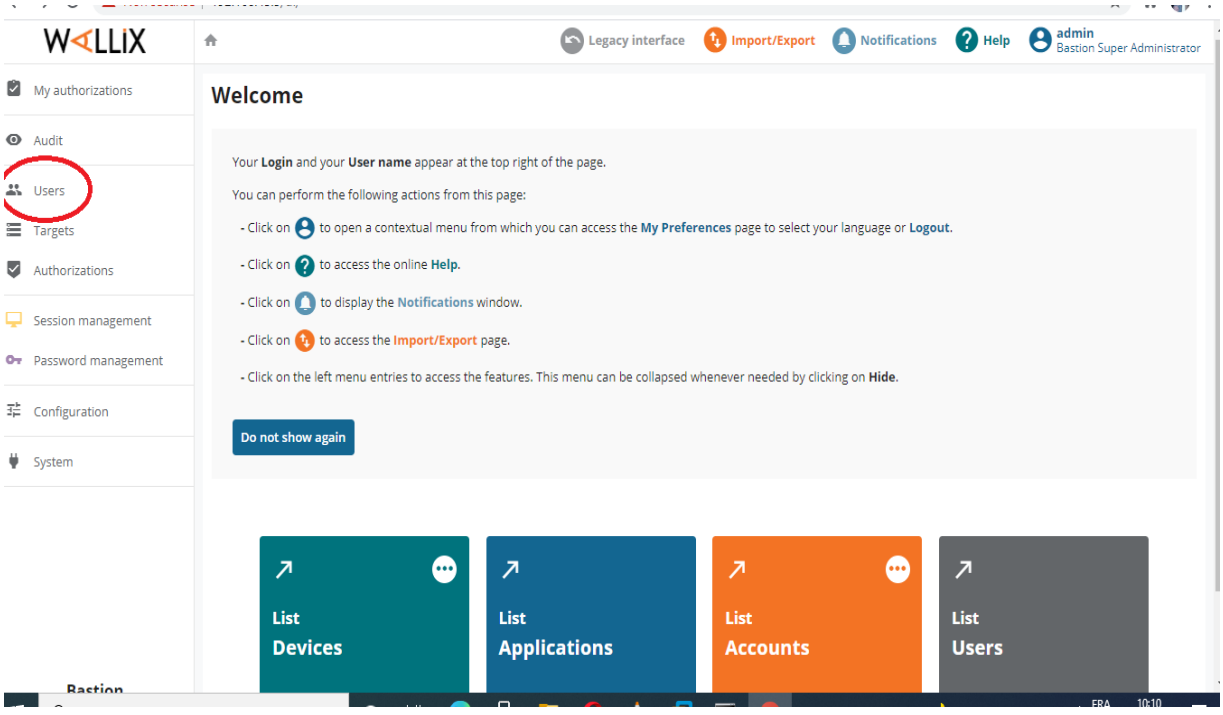

Figure IV-27 : Accéder sur « Users »

b. On clique sur ‘**Add a user’** pour ajouter un utilisateur

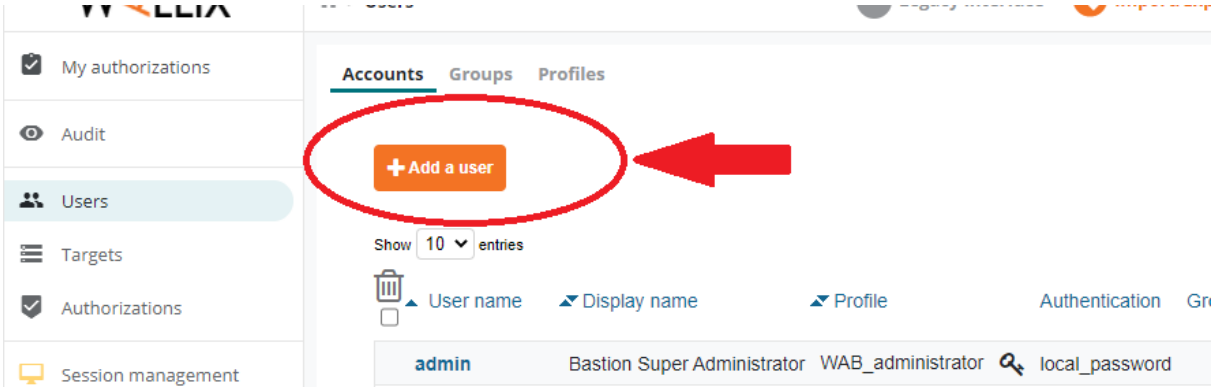

Figure IV-28 : Appui sur ‘Add a user’

c. Remplir les champs indiqués sur la figure qui suit

d. Introduire le mot de de passe utilisateur.

e. Appuyer sur ‘Apply’.

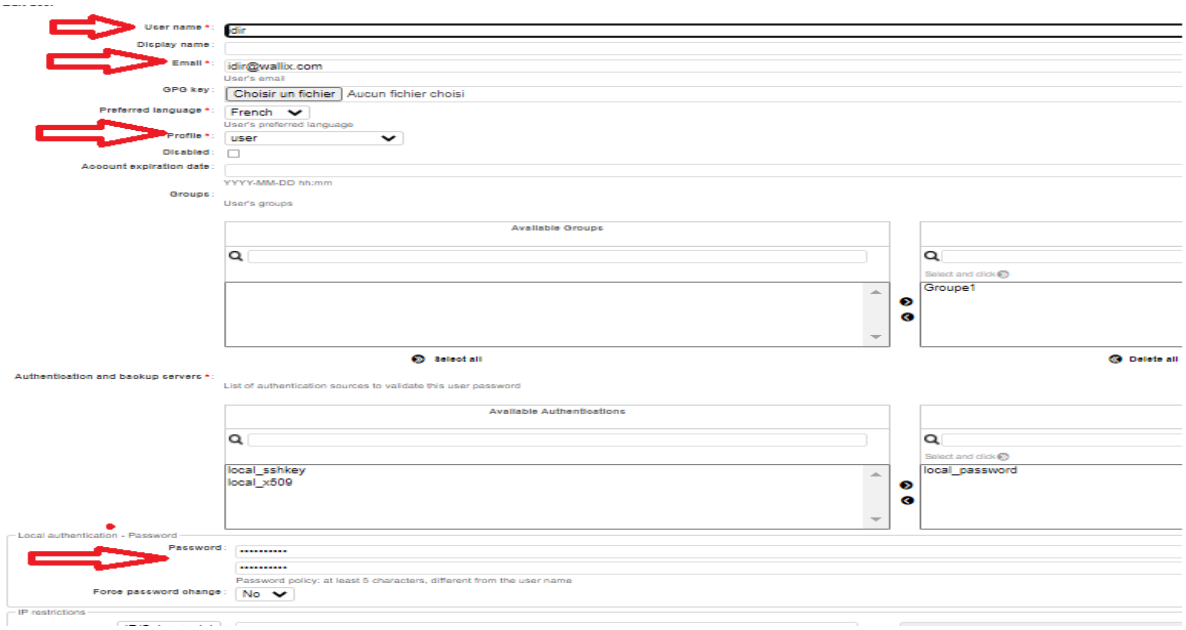

Figure IV-29 : Saisir les valeurs des champs

IV.2.2.2. Création d'un groupe d'utilisateurs ayant les mêmes privilèges et accès en commun (même droits d'accès)

a. Dans '**Users**' on sélectionne toujours '**Groups**'. Pour créer un nouveau groupe, on appuie sur '**Add a group**'.

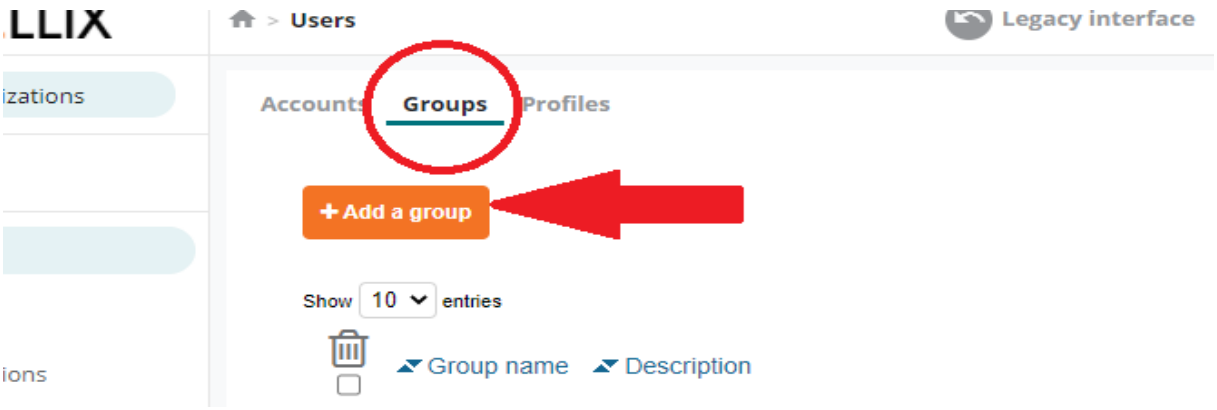

Figure IV-30 : Création d'un nouveau groupe d'utilisateurs

b. On remplit les champs comme indiqué sur la figure :

- La règle **rm\s+. *** sert à tuer l'interface RDP quand le mot de passe qui est introduit est incorrecte
- **RDP** (protocole) nous donne le privilège d'accéder à notre serveur cible (accès distant).

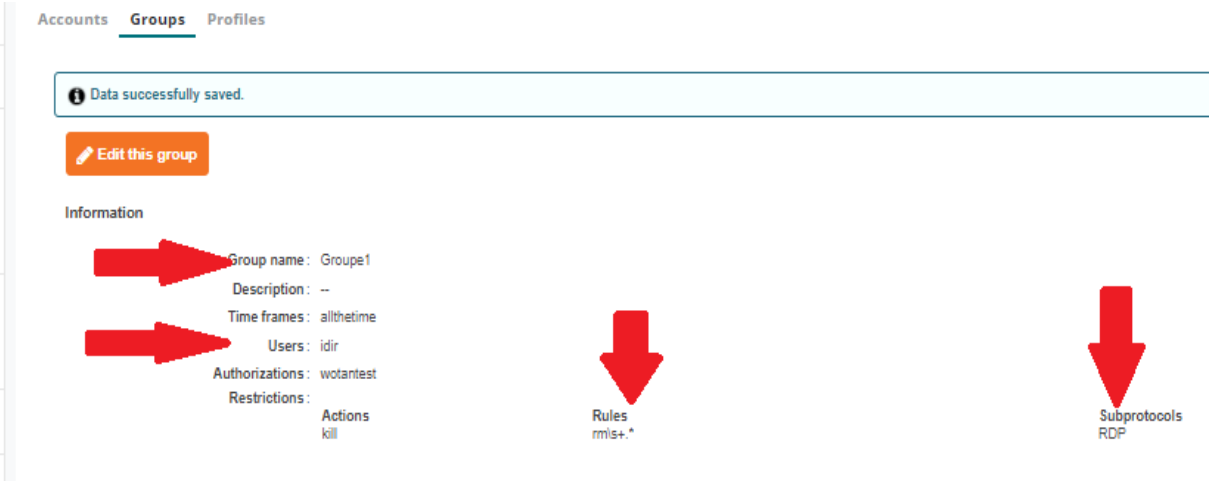

Figure IV-31 : Groupe d'utilisateur créé

Une fois le groupe est créé, on va déclarer les machines d'accès associées.

IV.2.2.3. Création des machines cibles (associées)

a. Cliquer sur '**Device'** pour remplir les champs du menu correspondant

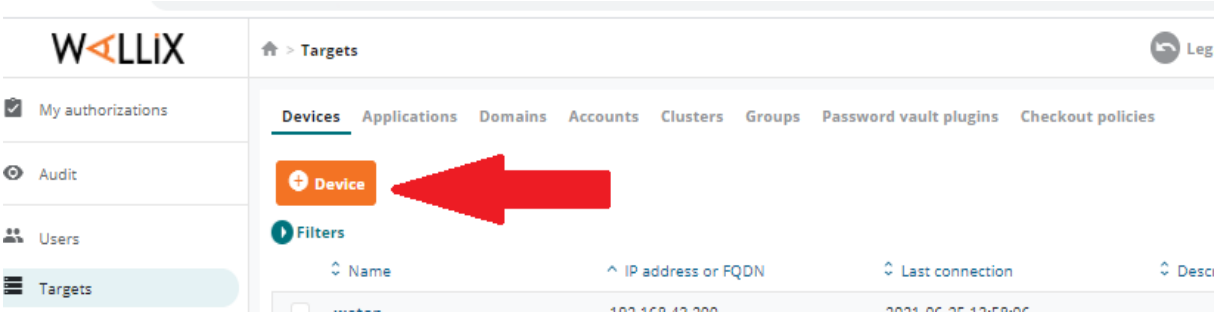

Figure IV-32 : Création d'une machine cible

b. On remplit les champs avec les cordonnées de la machine cible concernée par les accès

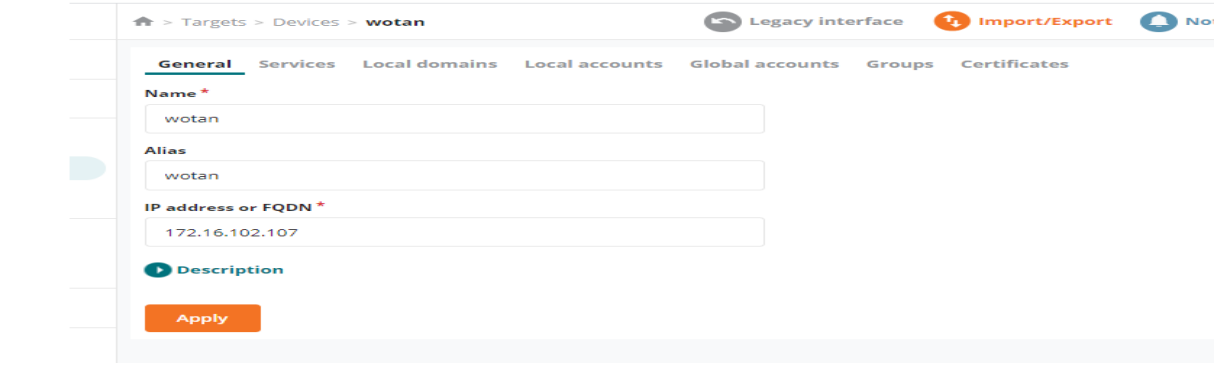

Figure IV-33 : Déclaration de la machine cible

c. Indiquer le protocole RDP pour l'accès sur le service

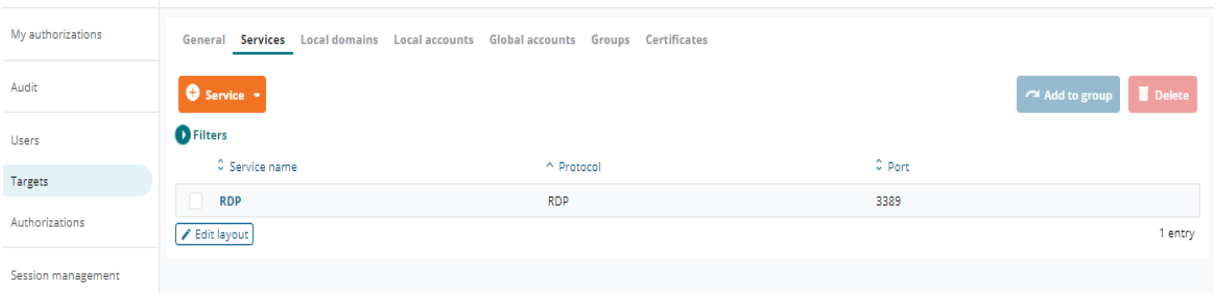

Figure IV-34 : Ajout du protocole d'accès

d. On déclare les comptes qui ont été créés dans cette machine avec le protocole RDP, en indiquant son mot de passe, puis on confirme.

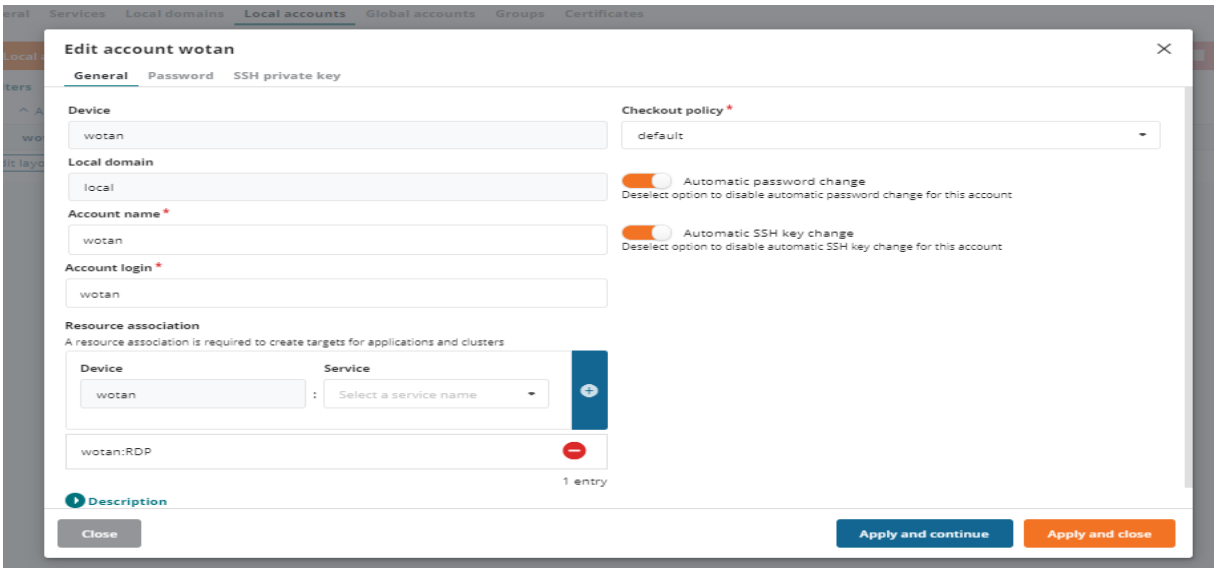

Figure IV-35 : Déclaration des comptes d'accès à la machine cible

IV.2.2.4. Création d'un groupe de machines liées aux droits d'accès déjà créés

a. On accède au groupe ('Groups') puis on appuie sur ajouter un groupe ('+Group') .

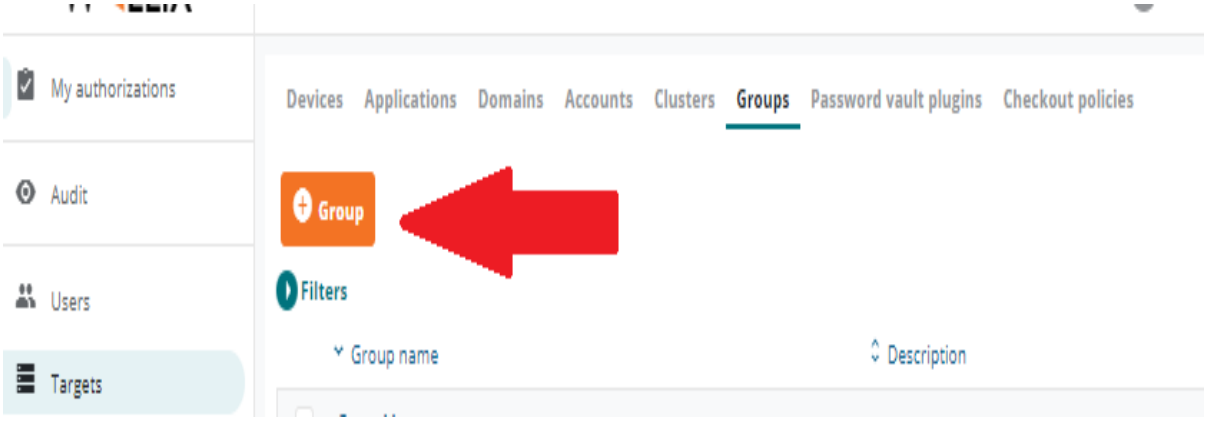

Figure IV-36 : Ajout d'un groupe de machines

b. On crée un groupe qu'on a nommé '**GroupLinux**'

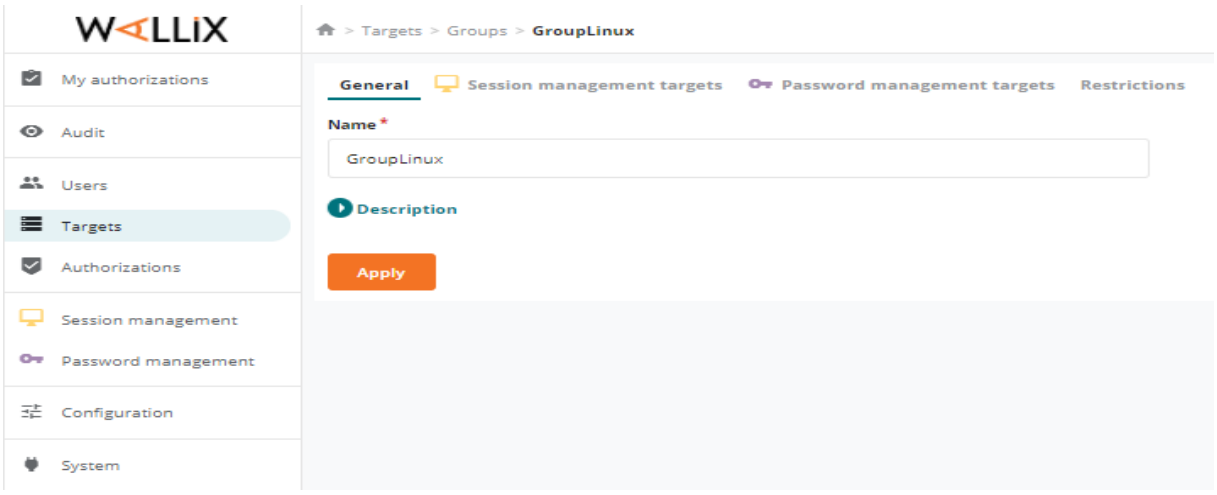

Figure IV-37 : Groupe de machines créées

c. Après, on déclare les utilisateurs accédant à notre machine cible

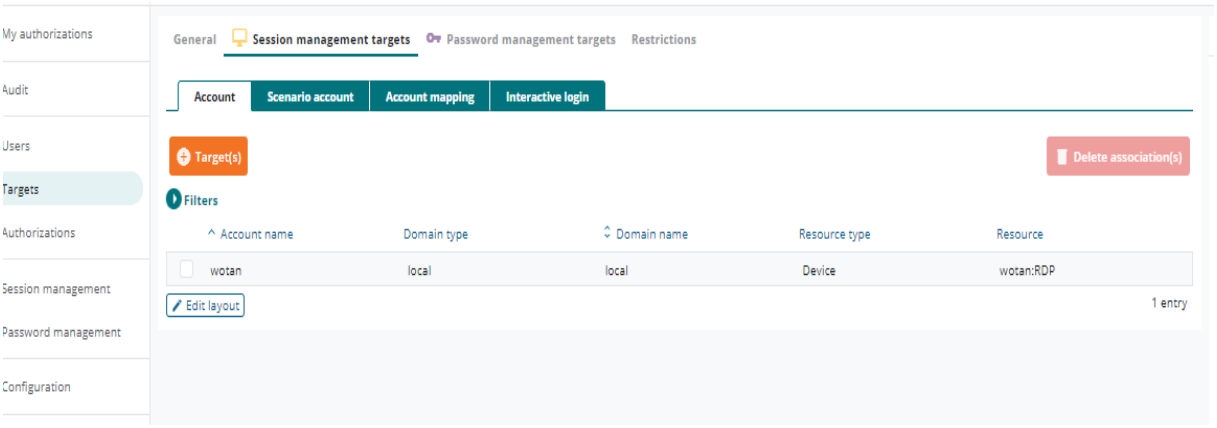

Figure IV-38 : Déclaration des utilisateurs accédant à la machine cible

d. On déclare le mot de passe d'accès à notre machine cible en appuyant sur « password management targets » puis sur ajouter.

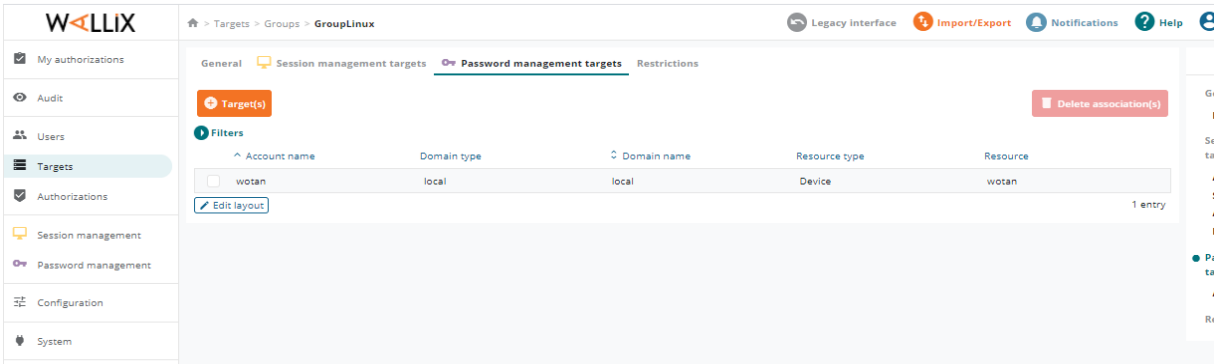

Figure IV-39 : Déclaration du mot de passe

e. Dans restrictions, on ajoute une règle propre qui va nous permettre d'accéder à la machine cible avec le protocole RDP.

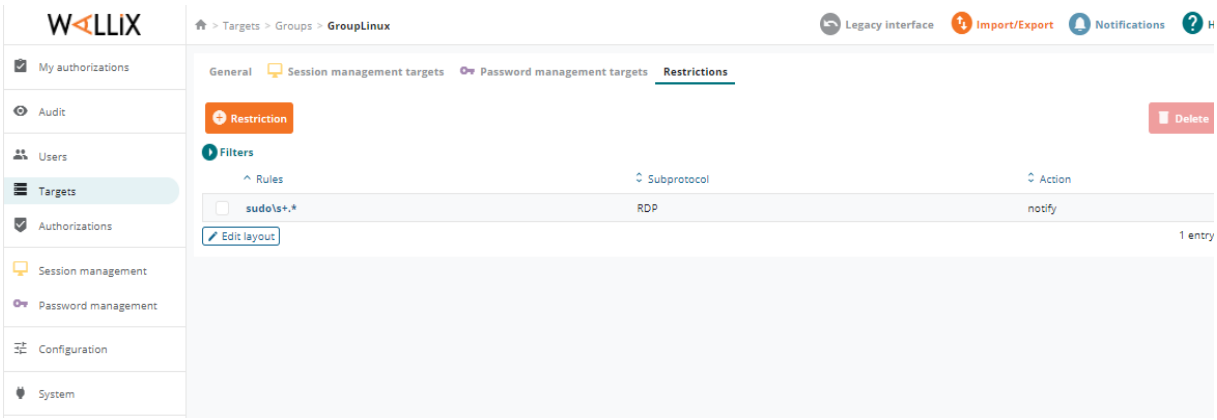

Figure IV-40 : Ajout d'une règle propre

IV.2.2.5. Création des autorisations

a. On clique sur autorisations pour la création

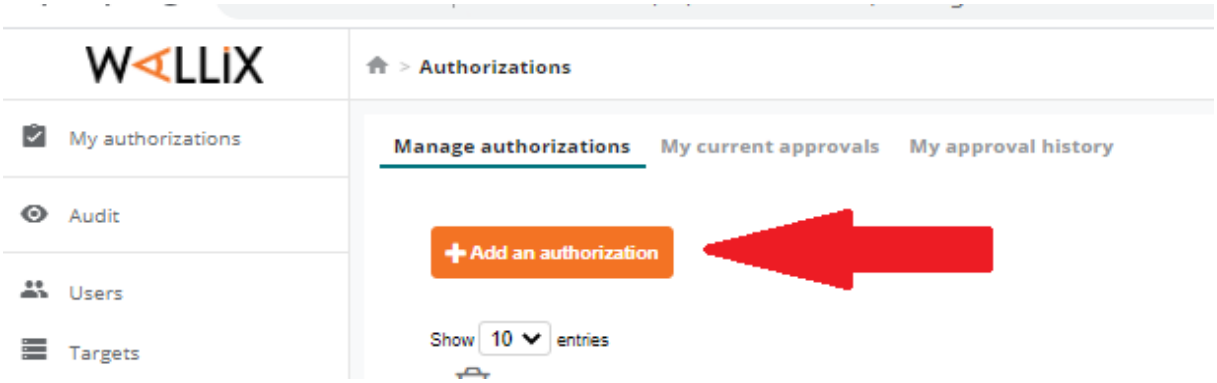

Figure IV-41 : Ajout d'une autorisation

b. Dans ce qui suit, on associe le groupe d'utilisateurs avec le groupe de machines, en sélectionnant tout ce que peut accéder le protocole RDP.

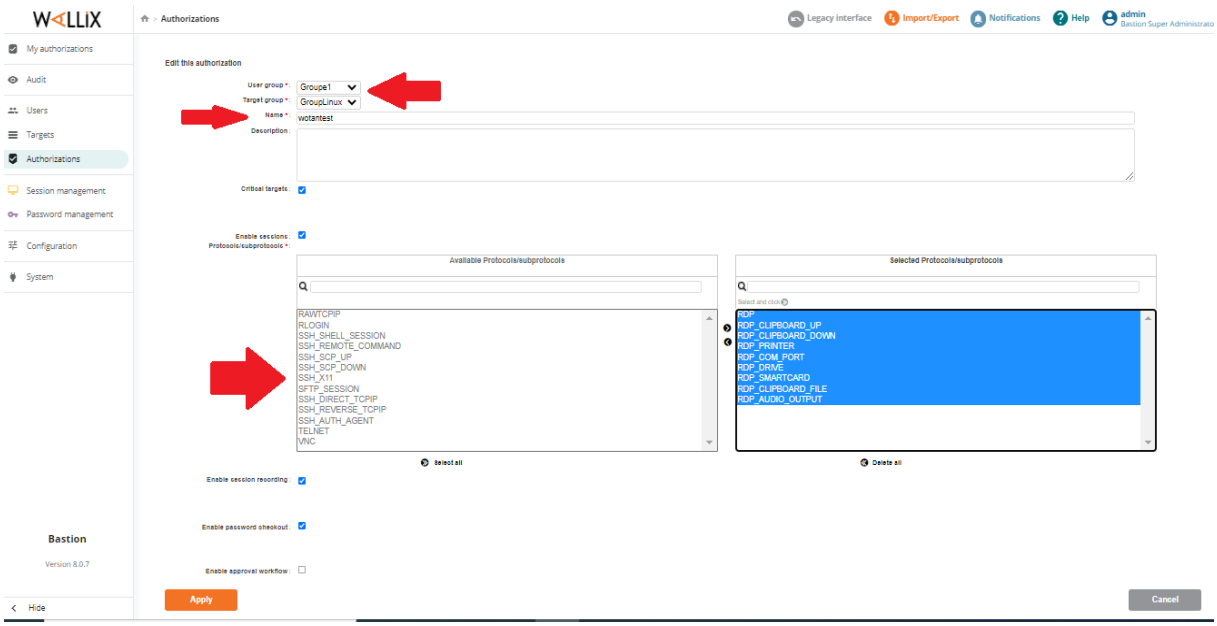

Figure IV-42 : Création d'une autorisation

c. On clique sur '**Apply**', pour signifier la fin de la configuration.

IV.2.2.6. Connexion vers la machine cible via un RDP

a. Une fois la configuration terminée, On se déconnecte de l'interface de l'administration. Puis, nous allons nous connecter avec l'utilisateur que nous avons créé.

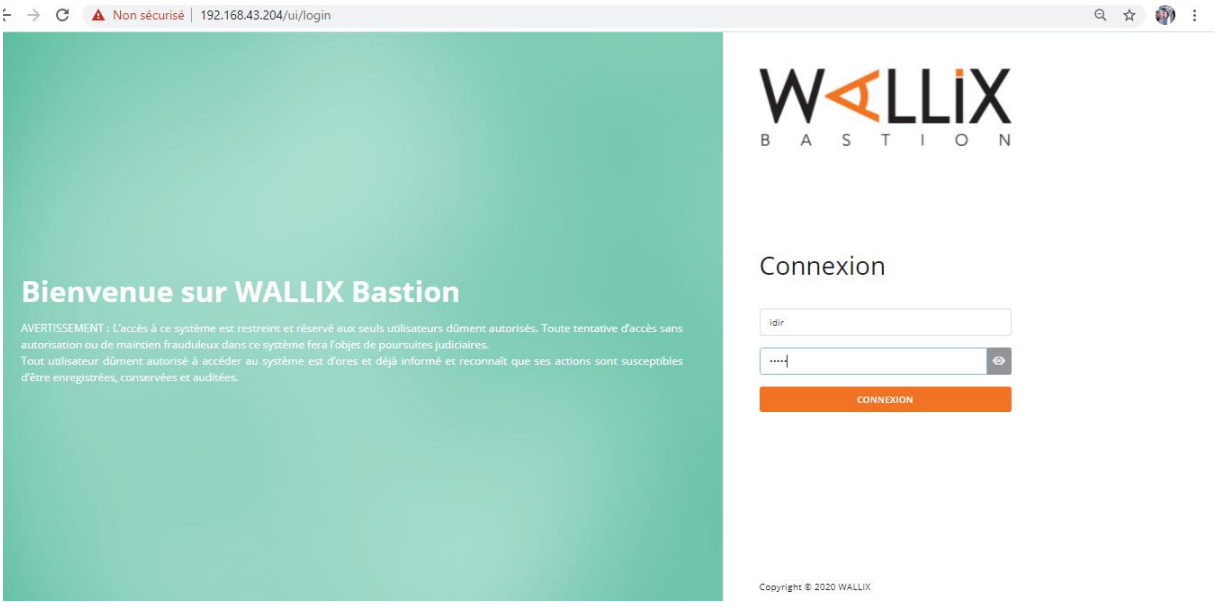

Figure IV-43 : Connexion avec l'utilisateur créé

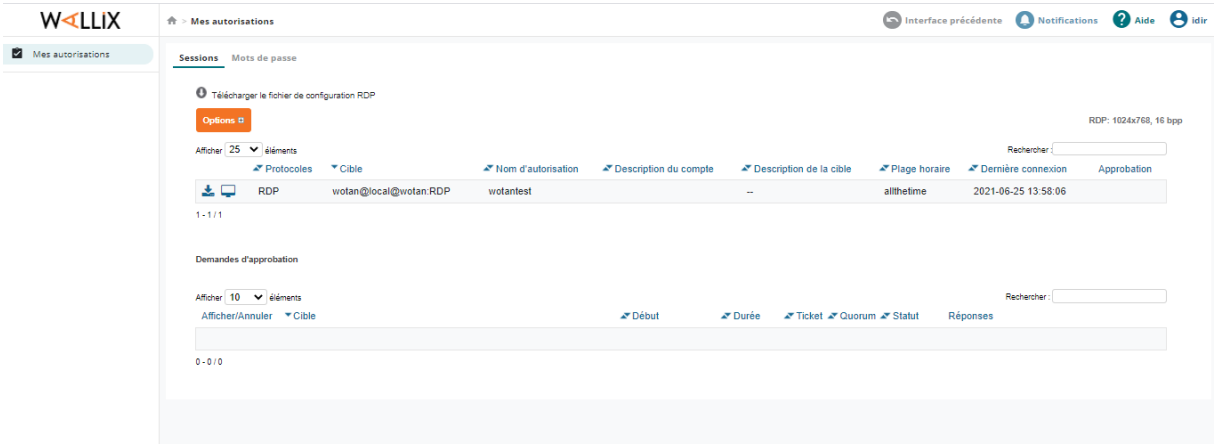

Figure IV-44 : Interface d'accueil utilisateur

b. On perçoit qu'il donne la possibilité à l'utilisateur de télécharger un **RDP**

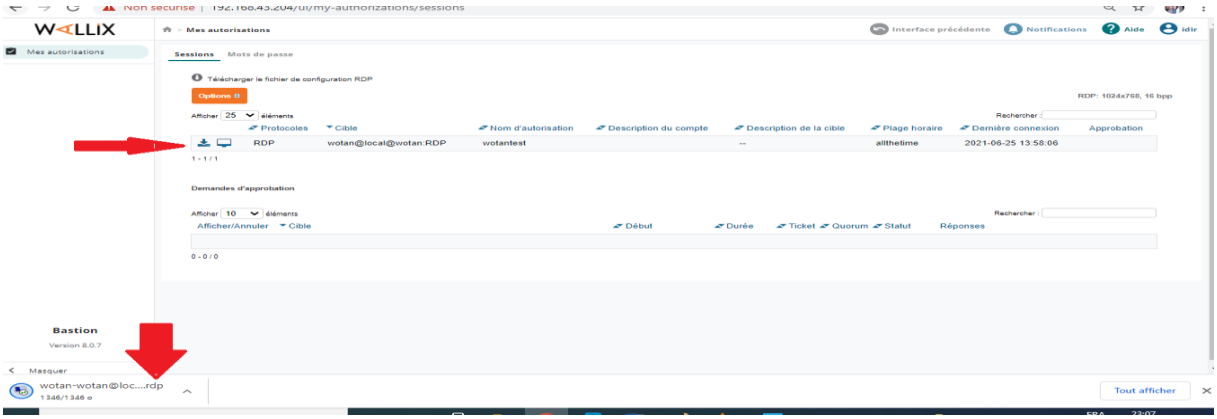

Figure IV-45 : Téléchargement du RDP

c. On clique sur connexion pour continuer

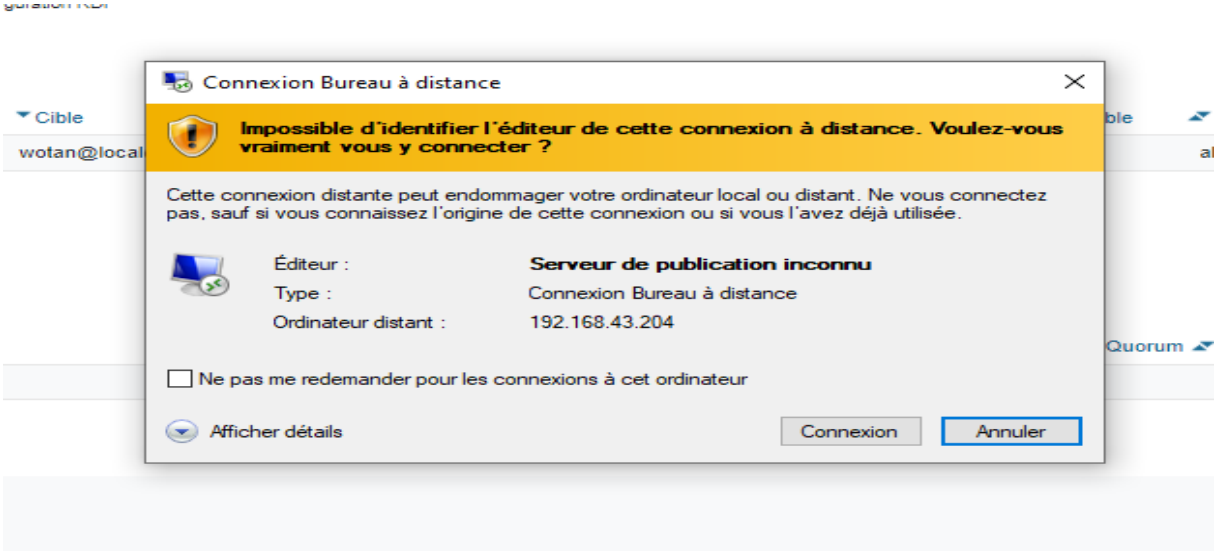

Figure IV-46 : Connexion

d. On introduit le nom de la machine cible plus notre mode passe d'accès.

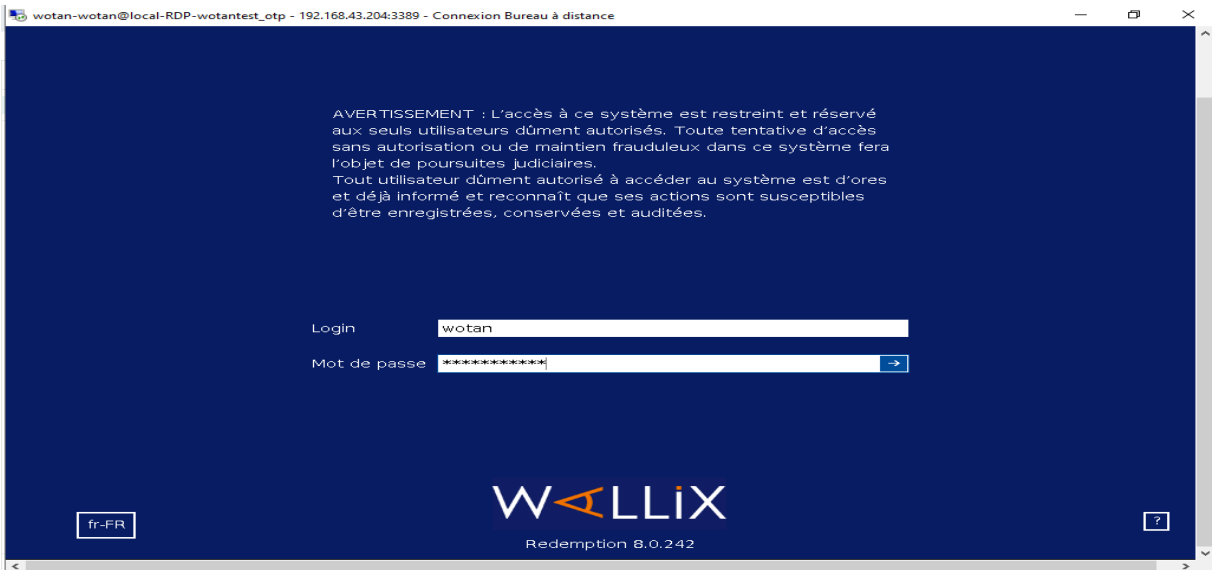

Figure IV-47 : Connexion au serveur

e. On accède à notre serveur cible via le RDP

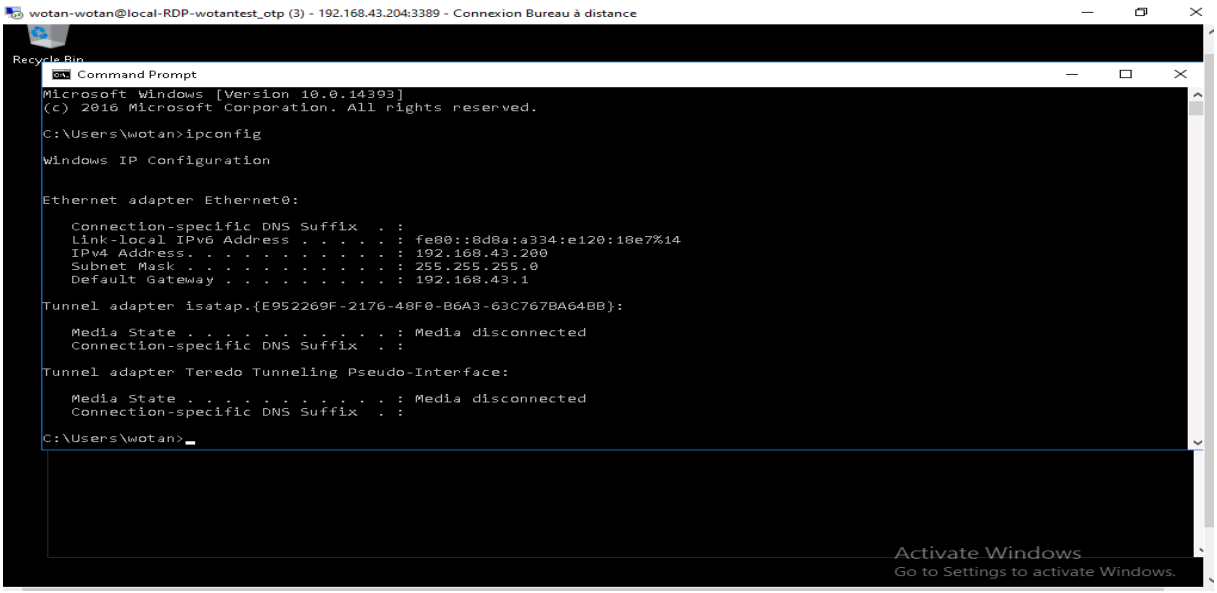

Figure IV-48 : Connexion au serveur cible réussie

IV.2.2.7. Visualisation et enregistrement des vidéos sous wallix bastion

Pour avoir l'accès sur la visualisation, nous nous déconnectons du compte utilisateur et reconnectons sur le compte administrateur.

a. En premier lieu, sur la page **Audit,** puis sur la page **Historique des Sessions,** on aura accès en bas comme indiqué sur la **figure IV-49** :

- Icône indiquant les vidéos enregistrées
- L'adresse IP de la machine cible
- Le protocole d'accès,
- La date et l'heure et la durée de l'enregistrement

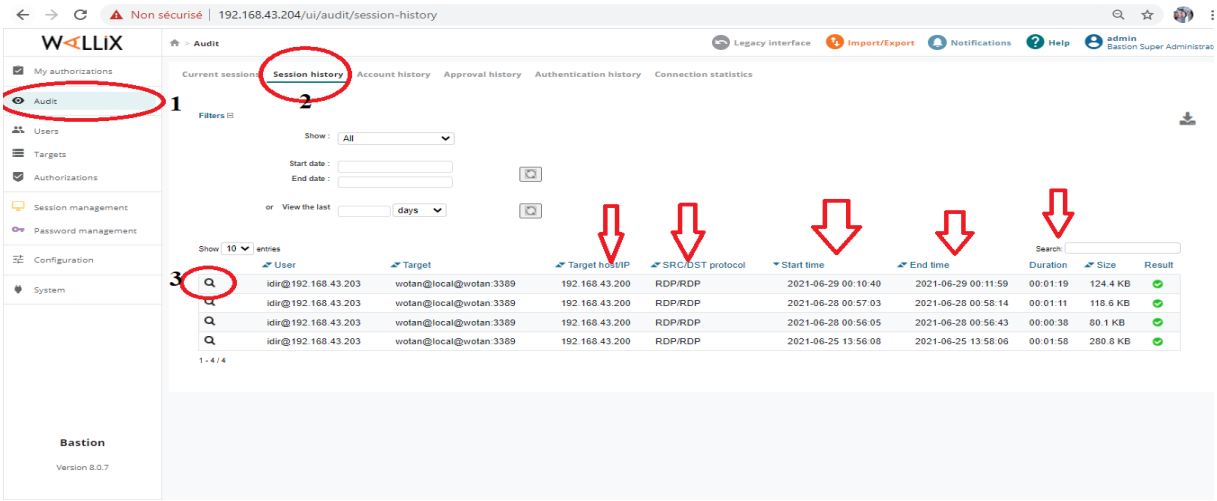

Figure IV-49 : Visualisation de la vidéo

b. On clique sur l'icône, puis la vidéo va se lancer à se générer comme indiquée sur la **figure IV-50**.

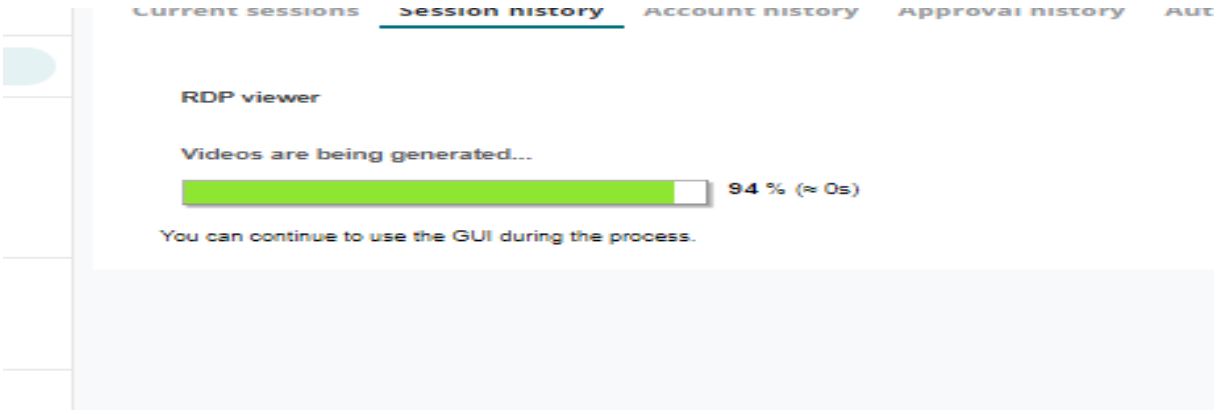

Figure IV-50 : Génération de la vidéo

c. Une fois le vidéo est générée, on procéde à la visualisation du contenue de la vidéo. En bas, On aura la vidéo qui se compose de plusieurs images comme indiqué sur les figures (IV-51 & IV-52) :

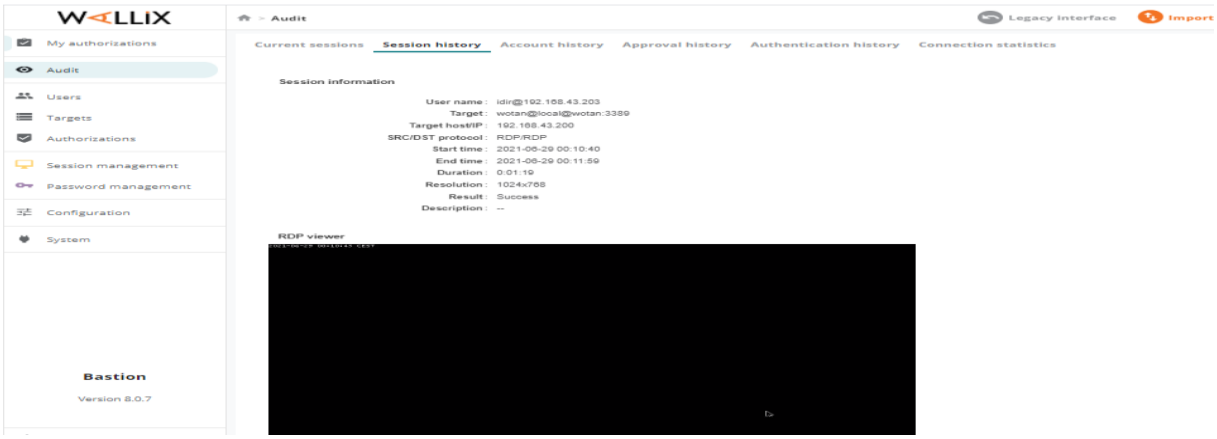

Figure IV-51 : Contenue de la vidéo

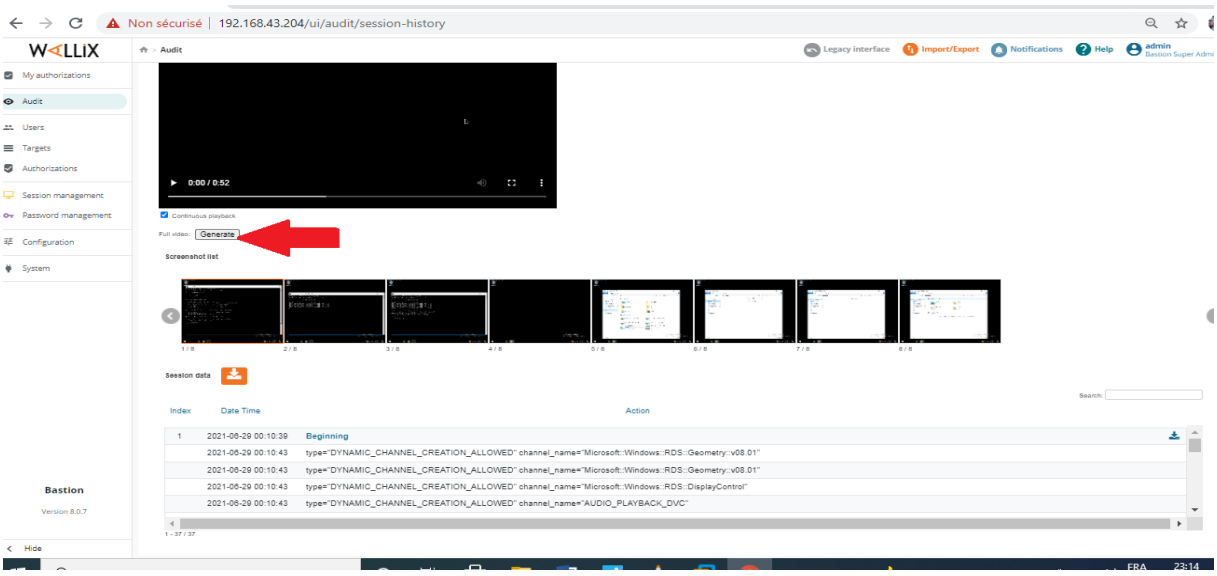

Figure IV-52 : Génération de la vidéo

d. Enfin, on clique sur ‘**generate’** pour que se réalise l’assemblage de la vidéo puis sur **‘Session data’** pour son téléchargement comme indiqué sur la **figure IV-53** :

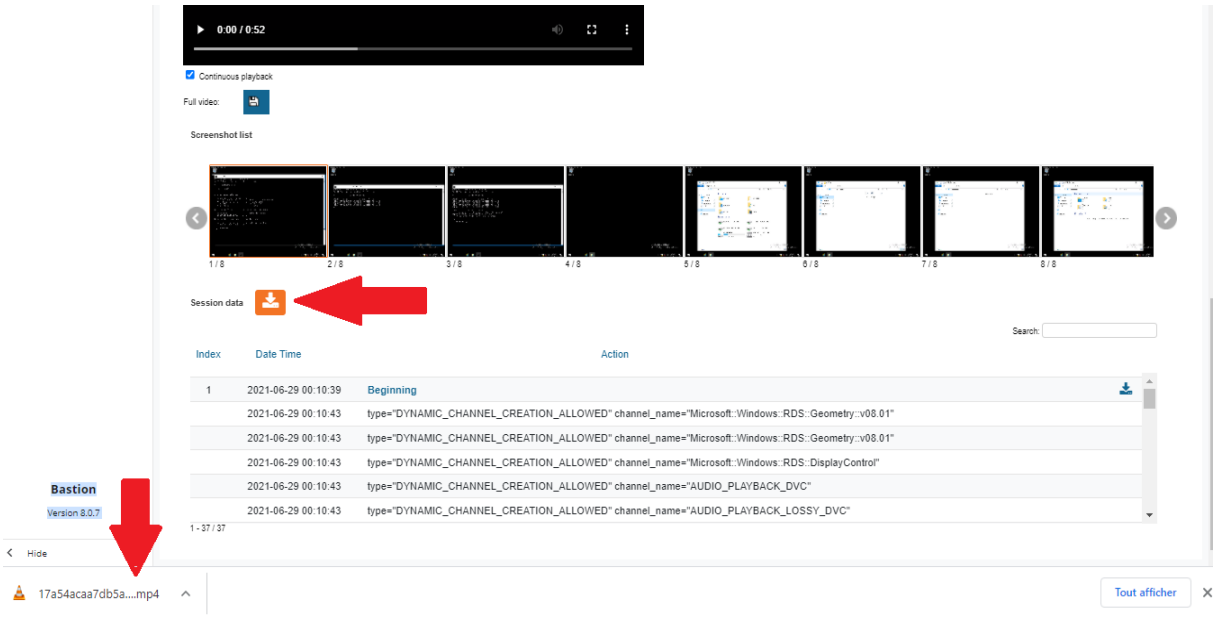

Figure IV-53 : Vidéo téléchargée

Conclusion

Dans ce chapitre, nous avons décrit brièvement les étapes d’installation et de configuration du système Windows Server 2012. Nous avons montré les étapes d’installation et de configuration de système de Wallix Bastion ainsi que la visualisation des vidéos générées.

Cette étape élucide la stratégie de sécurisation des accès utilisateurs aux serveurs de l’entreprise du ‘GROUP IFRI’ par la méthode de gestion d’accès distants privilégiés dite **PAM** avec la solution Wallix Bastion.

Conclusion générale et perspectives

Nous avons effectué notre stage pratique au sein de l'entreprise du groupe IFRI qui nous a très bien accueillis. Nous nous sommes imprégnés des activités du monde professionnel et de l'entreprise. Nous avons implémenté une solution de gestion des accès privilégiés (PAM) comme prévu dans notre objectif du départ, et ce à l'aide d'une application Wallix Bastion, basée sur la traçabilité, le contrôle d'accès, la surveillance en temps réel.

Pour cela, nous avons créé une machine virtuelle dans laquelle a été installé et configuré le système Windows Serveur 2012 et la solution Wallix Bastion. Et afin de vérifier l'efficacité de cette solution, nous avons créé des utilisateurs et configuré le système en attribuant des accès avec le protocole RDP au serveur(s) cible(s).

Nous avons montré aussi que l'application Wallix Bastion s'annonce comme une technique quasi incontournable pour le contrôle d'accès parce que, non seulement elle enregistre la traçabilité des accès aux serveurs et des transactions produites mais elle donne la possibilité d'enregistrer des vidéos d'une manière efficace sur l'état des machines des infrastructures informatiques. Toutefois, pour une sécurité optimale, le PAM doit être associé à d'autres outils de sécurisation existants dans un pare-feu d'un réseau.

Durant notre stage, nous avons acquis de nouvelles connaissances techniques sur la technologie PAM et les tests effectués ont prouvés la réussite de notre solution.

Perspectives :

A présent nous avons assuré un contrôle d'accès aux données mais ces dernières, pour ne pas être perdues, doivent être sauvegardées périodiquement (fin de journée, fin de semaine, fin de mois, fin d'année) et archivées dans un lieu sûr. L'objectif est de créer une sauvegarde automatique programmée en ligne vers un lieu protégé (contre le vol, le feu,…).

Résumé

Ce mémoire traite la sécurité du réseau de GROUPE IFRI avec l'outil PAM (la gestion des accès privilégie). Nous avons présenté PAM, ses composants et son utilisation. Puis, nous avons étudié la technologie WALLIX BASTION sur laquelle repose l'exécution de PAM. Enfin, la solution réalisée et implémentée.

Mots-clefs: PAM, WALLIX BASTION, VMware Workstation, Windows server 2012,.

Abstract

This thesis deals with the security of GROUPE IFRI's network with the PAM tool (privileged access management). We presented PAM, its components and its use. Then we looked at the WALLIX BASTION technology on which the PAM execution is based. Finally, the solution produced and implemented.

Keywords: PAM, WALLIX BASTION, VMware Workstation, Windows server 2012.