

CLOUD COMPUTING ET SÉCURITÉ D'INFORMATION

-Master Big Data & Cloud Computing

ENCADRÉ PAR :

Pr. RAFALIA Najat

PRÉSENTÉ PAR :

BOURACHED Douha & BENLAMHAIRA Oumaima

Remerciement

Nous tenons à exprimer notre profonde gratitude envers notre professeur, Mme. RAFALIA Najat, pour son soutien inconditionnel et ses précieux conseils tout au long de notre travail. Sa disponibilité, son expertise et sa bienveillance ont été d'une aide inestimable pour mener à bien notre projet.

Nous souhaitons également remercier chaleureusement tous ceux qui ont apporté leur contribution à ce travail, que ce soit par leur aide technique, leur participation à nos discussions ou tout simplement leur encouragement. Nous sommes reconnaissants envers nos camarades de classe qui ont partagé leurs connaissances et leurs expériences, ainsi que nos amis et nos familles pour leur soutien moral et leur patience pendant cette période exigeante.

Enfin, nous tenons à exprimer notre gratitude envers notre institution et ses membres pour nous avoir donné l'opportunité de réaliser ce projet et pour leur soutien tout au long de notre parcours académique. Nous espérons que ce travail sera utile et contribuera à la poursuite de nos recherches futures.

Table des matières :

Remerciement	1
Table des matières :	2
Table de figures	4
Liste des abréviations	5
Introduction Générale :	6
Chapitre I : Cadre général du projet.....	7
1 Introduction :	7
2 Objectifs de ce rapport :	7
2.1 Méthodologie :	7
3 Importance de la sécurité de l'information dans le cloud computing :	8
4 Conclusion :	8
Chapitre II : Généralités sur le cloud computing.....	9
1 Introduction :	9
2 Cloud Computing :	9
2.1 Définition du cloud computing :	9
2.2 Les cinq caractéristiques du cloud computing	10
2.3 Modèles de déploiement :	11
3 Conclusion :	12
Chapitre III : Une comparaison approfondie des modèles de service cloud.....	13
1 Introduction :	13
2 Les différents modèles de service en nuage :	13
2.1 Définition du terme As-A-Service :	13
2.2 Infrastructure en tant que service (IaaS) :	13
2.2.1 Définition :	13
2.2.2 Avantages & Inconvénients :	14
2.3 Plateforme en tant que service (PaaS) :	14
2.3.1 Définition :	14
2.3.2 Avantages & Inconvénients :	14
2.4 Logiciel en tant que service (SaaS) :	15
2.4.1 Définition :	15

2.4.2	Avantages & Inconvénients :	16
2.5	Différences entre IaaS, PaaS, et SaaS :	16
3	Conclusion :	17
Chapitre IV : Les défis de sécurité des données dans le cloud et les stratégies de protection.....		18
1	Introduction :	18
2	Principaux défis de sécurité liés au cloud :	18
2.1	Le manque de visibilité et de contrôle :	18
2.2	Les problèmes de confidentialité de données :	19
2.3	Le contrôle d'accès des utilisateurs :	19
3	Moyen de sécurisation de cloud :	19
3.1	Pare feu (Firewall) :	19
3.2	Contrôle d'accès aux utilisateurs :	20
3.3	Cryptage de données dans le cloud :	20
4	Conclusion :	21
Chapitre VI : Étude de cas : Mise en place d'un pare-feu dans le Cloud.....		22
1	Introduction :	22
2	Cloud Azure :	22
3	Implémentation :	22
3.1	Création du groupe de ressource :	22
3.2	Création de réseaux virtuelle :	23
3.3	Déployer une machine virtuelle :	25
3.4	Création de pare-feu :	27
3.5	Se connecter à la machine virtuelle à travers le pare-feu :	28
3.5.1	Première règles NATRule :	28
3.6	Table de routage :	30
4	Conclusion :	32
Conclusion Générale :		33
5	Autres Références :	34

Table de figures.

Figure 1 : Modele visual du cloud computing	10
Figure 2:Les caractéristiques du cloud computing.....	10
Figure 3:Les modèles de déploiement du cloud	11
Figure 4:Differences entre IaaS, PaaS, et SaaS :	17
Figure 5:Cloud Firewall.....	20
Figure 6:Cryptage des données dans le cloud.....	21
Figure 7:Configuration de ressource groupe.....	23
Figure 8:Validation et création.....	23
Figure 9:Configuration des réseaux et des sous réseaux	24
Figure 10: Réseau virtuel a été créé.....	24
Figure 11: Configuration de la machine virtuelle	25
Figure 12: Configuration de la machine virtuelle :	26
Figure 13: La machine virtuelle a été créé	26
Figure 14 :Rendre l'adresse IP de la machine virtuelle statique	27
Figure 15 :Configuration du pare-feu.....	27
Figure 16: 2.Configuration du pare-feu.....	28
Figure 17: Déploiement du pare-feu a été effectué	28
Figure 18: Ajout d'une collection de règles.....	29
Figure 19:Connexion à distance	29
Figure 20: Connexion à la machine virtuelle.....	29
Figure 21:Lors de la premier connexion l'utilisateur avait le droit d'accéder à n'importe quel site.....	30
Figure 22: Configuration de la table de routage	30
Figure 23: Création d'une table de routage	31
Figure 24:Résultat après la création de la table de route	31
Figure 25:Résultat après l'ajout d'une règle d'application	32

Liste des abréviations

Abréviation	Signification
NIST	National Institute of Standards and Technology
DMAIC	Define / Measure / Analyze / Improve / Control
IaaS	Infrastructure-as-a-Service
PaaS	Platform-as-a-Service
SaaS	Software-as-a-Service
VM	Virtual Machine

Introduction Générale :

Avec l'augmentation de la quantité de données générées et stockées par les entreprises, le cloud computing est devenu un choix populaire pour le stockage et le traitement de ces données. Cependant, la sécurité de l'information est un défi majeur pour les entreprises qui utilisent le cloud computing. En effet, lorsque les données sont stockées en dehors de l'entreprise, il peut être difficile de contrôler la sécurité des données et de les protéger contre les menaces en ligne.

Ce rapport a pour objectif de fournir une compréhension approfondie de la sécurité de l'information dans le cloud computing. Pour y parvenir, nous aborderons plusieurs aspects clés de la sécurité de l'information dans le cloud computing. Nous commencerons par définir ce qu'est le cloud computing et les différents types de modèles de service en nuage, modèles de déploiements ainsi que les caractéristiques de ce dernier. Nous expliquerons ensuite les défis associés à la sécurité de l'information dans le cloud computing et les conséquences potentielles pour les entreprises en cas de faille de sécurité. Nous discuterons également des stratégies et des technologies de protection des données disponibles pour les entreprises qui utilisent le cloud computing.

Enfin, pour faciliter la compréhension de la théorie, nous inclurons une partie implémentation de ce rapport. Cette section consistera en une démonstration concrète des concepts abordés dans la partie théorique en utilisant des outils et des technologies réels, où nous montrerons comment créer et configurer une machine virtuelle dans le cloud et comment configurer et créer des règles NAT et des règles d'applications dans un firewall pour protéger cette machine virtuelle. Cette démonstration permettra de mieux comprendre comment les entreprises peuvent appliquer les stratégies et technologies de protection des données dans leur environnement de cloud computing.

Ce rapport fournira une base solide pour comprendre les enjeux de la sécurité de l'information dans le cloud computing et comment les entreprises peuvent prendre des mesures pour protéger leurs données en utilisant le cloud.

Mots Clés : Cloud Computing, la sécurité de l'information, modèles de service en nuage, Modèles de déploiement, Machine Virtuelle, Firewall, Règles NAT, Règles d'applications.

Chapitre I : Cadre général du projet

1 Introduction :

Dans ce premier chapitre, nous allons explorer l'importance cruciale de la sécurité de l'information dans le monde du cloud computing. Le cloud computing est de plus en plus populaire en tant que solution pour stocker et traiter les données, mais cette popularité soulève des préoccupations en matière de sécurité de l'information. Nous énoncerons également les objectifs de ce rapport, qui visent à fournir une compréhension approfondie de la sécurité de l'information dans le service en nuage.

2 Objectifs de ce rapport :

L'objectif de ce rapport est de fournir une compréhension approfondie de la sécurité de l'information dans le cloud computing. Nous allons explorer les différents aspects de la sécurité de l'information dans le cloud computing, en examinant les défis, les stratégies et les technologies pour protéger les données, ainsi que les réglementations et les normes de sécurité applicables. Nous allons également décrire en détail le cloud computing, ses caractéristiques, modèles de services et modèles de déploiement dans un chapitre dédié plus tard dans le rapport.

L'objectif est de fournir une compréhension claire et complète des considérations de sécurité à prendre en compte lors de l'utilisation du service en nuage et savoir comment on peut aider les entreprises à adopter les bonnes pratiques pour protéger les données sensibles.

2.1 Méthodologie :

Une analyse critique du projet s'est imposée lors de notre travail. Pour ce faire, nous nous sommes basés sur la méthode DMAIC, méthode adaptable à diverses problématiques permettant la récolte d'informations précises et exhaustives d'une situation et d'en mesurer le niveau de connaissance que l'on possède.

Les 5 étapes de la méthode DMAIC sont les suivantes :

- **Définir** : pour poser le problème en définissant les symptômes.
- **Mesurer** : pour quantifier l'ampleur du problème.
- **Analyser** : pour déterminer les causes du problème.
- **Innover / Améliorer** : pour identifier la ou les solution(s) au problème.
- **Contrôler** : pour vérifier et maintenir l'amélioration dans le temps.

Le processus s'articule ensuite autour de deux phases essentielles :

1. Recherche théorique sur les questions de sécurité du cloud computing.
2. La phase de réalisation consiste à mener une conception applicative.

3 Importance de la sécurité de l'information dans le cloud computing :

La sécurité de l'information est l'une des préoccupations les plus importantes pour les entreprises qui utilisent le cloud computing. Avec la croissance rapide de la technologie cloud, les entreprises stockent de plus en plus de données sensibles sur des serveurs distants, ce qui peut les exposer à de nombreux risques de sécurité. Les menaces peuvent provenir de sources internes ou externes et incluent les attaques en ligne, les erreurs de configuration, les fuites de données et la violation de la confidentialité.

L'importance de la sécurité de l'information dans le cloud computing est encore accentuée par le fait que les entreprises dépendent de plus en plus du cloud pour les activités critiques, telles que la gestion de la chaîne d'approvisionnement, les transactions financières et les communications internes. Une interruption de la sécurité de l'information peut avoir des conséquences graves pour la réputation de l'entreprise et la confiance des clients.

Il est donc crucial que les entreprises prennent des mesures pour protéger les données sensibles dans le cloud computing. Les entreprises doivent évaluer les risques liés à la sécurité de l'information, adopter des stratégies de sécurité efficaces et s'assurer que les fournisseurs de services en nuage prennent des mesures pour protéger les données. Cela peut inclure l'utilisation de technologies de cryptage, de contrôles d'accès et d'authentification, de techniques de gestion des identités et des accès, et de conformité aux réglementations et normes de sécurité pour le cloud computing (Nous examinerons en détail ces sujets dans les chapitres à venir).

En garantissant la sécurité de l'information, les entreprises peuvent profiter des nombreux avantages du cloud computing tout en minimisant les risques pour leur activité.

4 Conclusion :

En résumé, ce premier chapitre présente les objectifs de ce rapport ainsi que la méthodologie adoptée pour la réalisation de ce mini projet. Nous avons également mis en évidence l'importance cruciale de la sécurité de l'information dans le cloud computing. La protection des données sensibles est devenue un enjeu majeur pour les entreprises, qui doivent prendre des mesures pour protéger les informations. Ce rapport vise à fournir une compréhension approfondie de la sécurité de l'information dans le service en nuage, en examinant les différentes stratégies et les technologies disponibles pour garantir la sécurité des données dans le cloud computing.

Chapitre II : Généralités sur le cloud computing

1 Introduction :

Dans ce deuxième chapitre, nous allons examiner le service en nuage en détaillant sa définition, ses caractéristiques et ses modèles de déploiement. Nous allons également discuter des avantages et des défis liés à l'utilisation du cloud computing. Ce chapitre est fondamental pour comprendre les enjeux de la sécurité de l'information dans le cloud computing, qui seront examinés dans les chapitres suivants.

2 Cloud Computing :

2.1 Définition du cloud computing :

« Le cloud computing est un modèle qui permet un accès réseau à la demande et pratique à un pool partagé de ressources informatiques configurables (telles que réseaux, serveurs, stockage, applications et services) qui peuvent être provisionnées rapidement et distribuées avec un minimum de gestion ou d'interaction avec le fournisseur de services. »¹

Le cloud computing est un modèle informatique permettant aux utilisateurs d'accéder à des applications et des services via Internet sans avoir à gérer l'infrastructure sous-jacente. Ce modèle est basé sur l'utilisation de ressources partagées, telles que les serveurs, les bases de données et les applications, qui sont gérées par une entreprise de nuage. Les utilisateurs peuvent accéder à ces ressources en ligne à partir de n'importe où et à tout moment, simplement en utilisant un appareil connecté à Internet.

L'une des caractéristiques clés de ces définitions est le concept de scalabilité, qui permet de s'adapter à la demande, d'être élastique et de ne payer que ce qui est utilisé. Cela offre un avantage considérable par rapport à une infrastructure dédiée à l'entreprise où les serveurs sont souvent largement sous-utilisés.

¹ Maricela-Georgiana Avram (Olaru), Advantages and challenges of adopting cloud computing from an enterprise perspective. The 7th International Conference Interdisciplinarity in Engineering (INTER-ENG 2013).

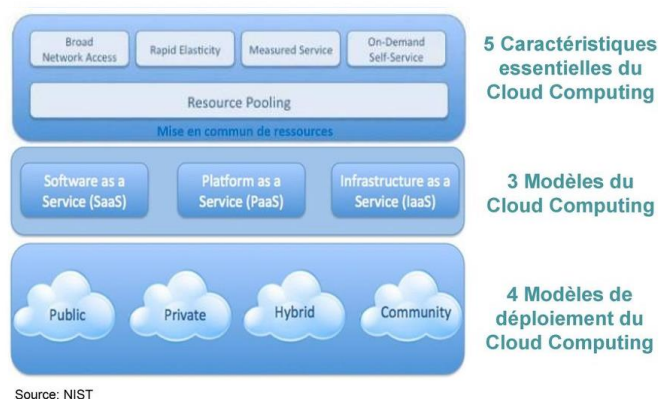


Figure 1 : Model visual du cloud computing

NIST définit le cloud computing en décrivant cinq caractéristiques essentielles, trois modèles de services de cloud computing, et trois modèles de déploiement de cloud computing. Ils sont résumés sous forme visuelle à la figure 1 et expliquées en détail ci-dessous.²

2.2 Les cinq caractéristiques du cloud computing

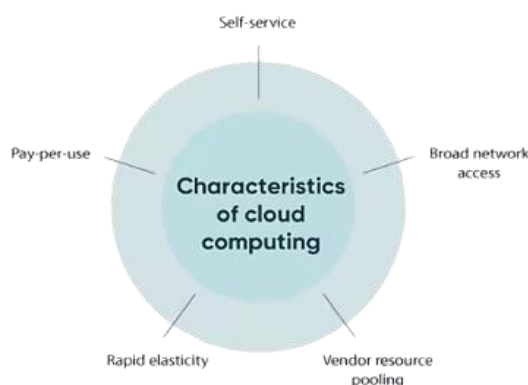


Figure 2: Les caractéristiques du cloud computing

Les services Cloud présentent cinq caractéristiques essentielles qui démontrent leur relation, et leurs différences avec les approches informatiques traditionnelles :

- Accès aux services par l'utilisateur à la demande :

La mise en œuvre des systèmes est entièrement automatisée et c'est l'utilisateur, au moyen d'une console de commande, qui met en place et gère la configuration à distance.

- Paiement à l'utilisation :

Les clients paient uniquement les services informatiques qu'ils utilisent et peuvent surveiller leur utilisation.

- Élasticité rapide :

Le cloud computing est capable d'ajuster rapidement et automatiquement les ressources de traitement, de stockage de données et de bande passante réseau pour satisfaire les exigences des utilisateurs.

² Fa-Chang Cheng, Wen-Hsing Lai." The Impact of Cloud Computing Technology on Legal Infrastructure within Internet Focusing on the Protection of Information Privacy", International Workshop on Information and Electronics Engineering 29 (2012) 241-251.

➤ **Pool de ressources :**

Les fournisseurs de cloud utilisent des ordinateurs partagés pour fournir leurs services. La virtualisation et les mécanismes multi-utilisateurs permettent de séparer les clients et de protéger leurs données contre tout accès non autorisé.

➤ **Accès étendu :**

Les utilisateurs peuvent accéder aux données et aux ressources informatiques à partir de différents appareils. Le cloud est accessible depuis n'importe quel appareil connecté à Internet, y compris les ordinateurs de bureau, les ordinateurs portables, les tablettes et les smartphones.

Le cloud computing a connu une croissance rapide en raison de ses avantages évidents pour les entreprises, tels que la réduction des coûts d'infrastructure et la flexibilité accrue. Cependant, le stockage de données sensibles et critiques sur des serveurs gérés par une entreprise de nuage peut soulever des préoccupations quant à la sécurité de ces informations. C'est pourquoi il est important de comprendre les défis de la sécurité de l'information dans le cloud computing et de mettre en place des mesures de protection appropriées.

2.3 Modèles de déploiement :

Selon la définition donnée précédemment, un nuage se réfère à une infrastructure distante gérée par un prestataire pour offrir des services informatiques. Les différents prestataires peuvent être désignés comme le nuage d'Amazon, de Google, etc. Il existe quatre principaux types de modèles de déploiement pour les nuages : le nuage privé, le nuage communautaire, le nuage public et le nuage hybride.

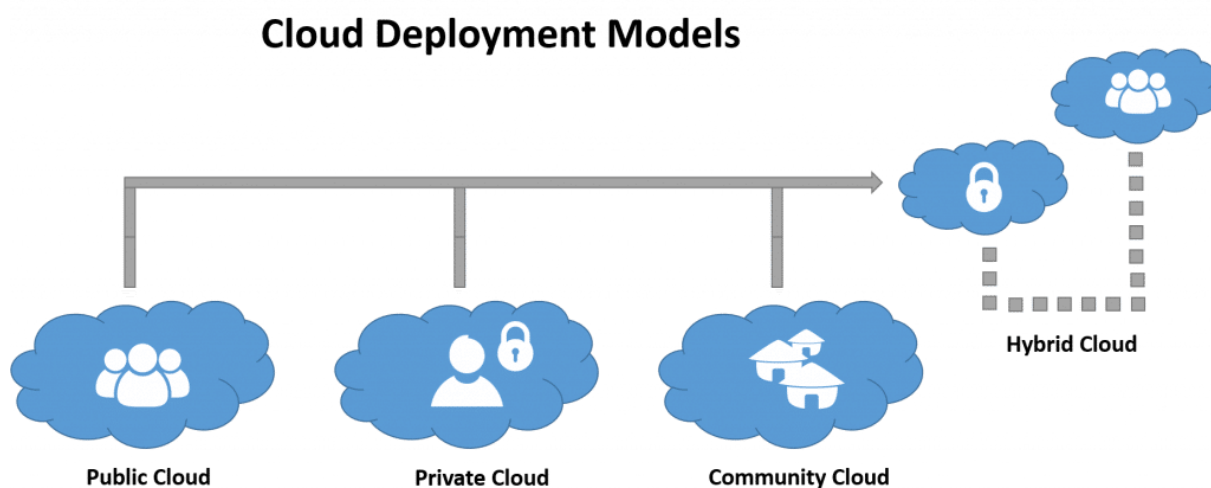


Figure 3: Les modèles de déploiement du cloud

➤ **Nuage public :**

Ce type de nuage est déployé pour le grand public et géré par une entreprise tierce. Les utilisateurs peuvent accéder aux ressources en payant un abonnement ou en utilisant un modèle de paiement à l'utilisation.

➤ **Nuage privé :**

Ce type de nuage est déployé pour un seul client ou une entreprise, et les ressources sont gérées exclusivement pour cette entreprise. Ce modèle est souvent utilisé pour des besoins de sécurité accrus ou pour des restrictions réglementaires.

➤ **Nuage communautaire :**

Configuré pour être utilisé par une communauté d'utilisateurs provenant d'entreprises ayant des intérêts communs. Il peut être détenu et géré par des entreprises d'une communauté, un tiers ou une combinaison des deux.

➤ **Nuage hybride :**

Ce modèle combine des aspects des modèles privé et public. Certaines ressources peuvent être déployées en interne, tandis que d'autres peuvent être accessibles via un nuage public. Ce modèle est souvent utilisé pour des besoins spécifiques, tels que la protection de données sensibles, tout en bénéficiant de la flexibilité et de la commodité d'un nuage public.

3 Conclusion :

En conclusion de ce chapitre, nous avons défini le concept de Cloud Computing, ses caractéristiques et présenté les différents modèles de déploiement disponibles : le nuage privé, le nuage communautaire, le nuage public et le nuage hybride. Chacun de ces modèles offre des avantages et des inconvénients en termes de coût, de flexibilité, de contrôle et de sécurité. Il est important de comprendre les différences entre ces modèles pour choisir celui qui convient le mieux aux besoins en matière de services informatiques.

Chapitre III : Une comparaison approfondie des modèles de service cloud

1 Introduction :

Pour le troisième chapitre, nous allons explorer les différents modèles de services en nuage disponibles. Nous détaillerons les modèles les plus couramment utilisés, leurs caractéristiques et leurs avantages et inconvénients pour aider à choisir le modèle le plus approprié pour une utilisation donnée. Nous discuterons également des différences entre les différents modèles de services en nuage pour une compréhension complète des options disponibles.

2 Les différents modèles de service en nuage :

Trois modèles de services peuvent être offerts sur le Cloud : Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS). Ces trois modèles de service doivent être déployés sur des Infrastructures qui possèdent les cinq caractéristiques essentielles citées plus haut pour être considérées comme du Cloud Computing. Mais avant tout qu'est ce que ce veut dire « As-A-Service » ?

2.1 Définition du terme As-A-Service :

Le terme « aas » ou « as-a-Service » désignent l'externalisation d'un service de cloud computing par un tiers, afin de permettre aux utilisateurs de se concentrer sur des aspects plus importants de leur activité, tels que leur code et la relation avec les clients. Chacun des types de cloud computing permet de réduire la gestion de l'infrastructure sur site. En effet, une infrastructure informatique sur site implique une grande responsabilité pour l'utilisateur et le responsable, qui doivent gérer, mettre à jour et remplacer chaque composant eux-mêmes. Le cloud computing permet de déléguer la gestion d'un ou plusieurs composants de l'infrastructure, ce qui permet de gagner du temps pour se consacrer à d'autres tâches.

2.2 Infrastructure en tant que service (IaaS) :

2.2.1 Définition :

Infrastructure as a Service (IaaS) est un modèle de service de cloud computing qui fournit un accès à distance aux ressources informatiques, telles que les serveurs, le stockage et les réseaux. Avec IaaS, les utilisateurs peuvent louer des ressources à la demande plutôt que de devoir acheter et gérer leur propre matériel et logiciel sur site. Les fournisseurs de services IaaS sont responsables de la maintenance du matériel et de l'infrastructure sous-jacente, ainsi que de la sécurité, de la sauvegarde des données et de la redondance.

Le modèle IaaS est utilisé par les entreprises pour répondre rapidement à des besoins en matière de capacité, de stockage et de traitement des données, sans avoir à investir dans leur propre infrastructure coûteuse. Les utilisateurs peuvent ainsi augmenter ou réduire la capacité en fonction de leurs besoins en temps réel, sans avoir à s'inquiéter des coûts liés à l'achat de nouveaux serveurs ou équipements de stockage.

2.2.2 Avantages & Inconvénients :

Avantages de l'IaaS :

- Flexibilité : l'IaaS permet aux entreprises de disposer de ressources informatiques selon leurs besoins spécifiques, sans avoir à investir dans une infrastructure surdimensionnée qui ne sera pas utilisée pleinement.
- Évolutivité : les ressources peuvent être ajoutées ou supprimées rapidement en fonction des besoins, ce qui permet aux entreprises de s'adapter rapidement à des pics de demande imprévus.
- Sécurité : les fournisseurs d'IaaS ont généralement des niveaux de sécurité élevés et des politiques de sauvegarde des données fiables, ce qui peut aider les entreprises à protéger leurs données contre les menaces externes et internes.
- Coût : l'IaaS permet aux entreprises de réaliser des économies substantielles en évitant les coûts liés à l'achat et à la maintenance d'une infrastructure informatique interne.

Inconvénients de l'IaaS :

- Dépendance à l'égard du fournisseur : en utilisant l'IaaS, les entreprises sont tributaires du fournisseur pour la disponibilité et la qualité des ressources informatiques, ce qui peut entraîner une perte de contrôle sur leur propre infrastructure.
- Risque de sécurité : bien que les fournisseurs d'IaaS aient des politiques de sécurité solides, il y a toujours un risque potentiel de violation de données ou d'attaques par des pirates.
- Personnalisation limitée : l'utilisation de l'IaaS peut limiter la personnalisation des ressources informatiques, ce qui peut être un problème pour les entreprises qui ont des besoins spécifiques ou qui souhaitent exécuter des applications ou des logiciels personnalisés.

Il est important de noter que les avantages et les inconvénients de l'IaaS peuvent varier en fonction des besoins et des exigences de chaque entreprise.

2.3 Plateforme en tant que service (PaaS) :

2.3.1 Définition :

Le Platform as a Service (PaaS) est un modèle de déploiement de cloud computing qui fournit un environnement de développement et de déploiement d'applications en ligne. Avec PaaS, les développeurs peuvent créer, tester et déployer des applications sans avoir à s'occuper de l'infrastructure sous-jacente, ce qui inclut le matériel, le système d'exploitation et les logiciels de base. Les fournisseurs de PaaS proposent un ensemble de services permettant de créer, exécuter et gérer des applications dans le cloud.

2.3.2 Avantages & Inconvénients :

Le modèle de service PaaS présente à la fois des avantages et des inconvénients.

Avantages :

- Rapidité de développement : grâce aux outils fournis par la plateforme, les développeurs peuvent créer rapidement des applications et les déployer facilement.
- Évolutivité : les plates-formes PaaS sont généralement conçues pour être facilement extensibles, ce qui permet aux applications de croître avec les besoins de l'entreprise.
- Maintenance simplifiée : la maintenance de l'infrastructure est prise en charge par le fournisseur de la plateforme, ce qui permet aux développeurs de se concentrer sur le développement de l'application.
- Coûts réduits : le modèle PaaS permet de réduire les coûts de développement et de maintenance de l'infrastructure, ce qui est particulièrement intéressant pour les petites entreprises qui n'ont pas les moyens de se doter d'une infrastructure coûteuse.

Inconvénients :

- Limitations techniques : les plateformes PaaS ont des limites techniques qui peuvent restreindre les fonctionnalités de l'application. Les développeurs peuvent se trouver dans l'incapacité de modifier certains aspects de l'infrastructure, ce qui peut limiter la créativité et l'innovation.
- Dépendance vis-à-vis du fournisseur : les entreprises utilisant des plateformes PaaS sont étroitement liées à leur fournisseur de services. Elles doivent être conscientes de cette dépendance et prendre en compte les risques potentiels en matière de sécurité et de disponibilité.
- Risques de sécurité : les plateformes PaaS sont vulnérables aux cyberattaques, ce qui peut mettre en danger les données de l'entreprise et les applications qu'elle utilise. Les entreprises doivent être vigilantes et s'assurer que le fournisseur de la plateforme prend les mesures nécessaires pour protéger leurs données.

En somme, le modèle PaaS offre de nombreux avantages, notamment en matière de rapidité et de simplicité de développement, mais présente également des risques potentiels liés à la sécurité et à la dépendance vis-à-vis du fournisseur.

2.4 Logiciel en tant que service (SaaS) :

2.4.1 Définition :

Le modèle de service SaaS (Software as a Service) est le plus courant dans le Cloud Computing. Ce modèle consiste à fournir un logiciel ou une application en tant que service via Internet. Le logiciel est installé et exécuté sur les serveurs du fournisseur de services, et les utilisateurs peuvent accéder à l'application à partir de n'importe quel appareil connecté à Internet, via un navigateur web ou une application dédiée.

Le modèle SaaS permet aux utilisateurs de bénéficier de logiciels et d'applications sans avoir à les installer et à les gérer eux-mêmes. Le fournisseur de services est responsable de l'infrastructure, des mises à jour et des correctifs de sécurité, ce qui permet aux utilisateurs de se concentrer sur l'utilisation de l'application plutôt que sur la gestion de l'infrastructure sous-jacente.

2.4.2 Avantages & Inconvénients :

Le modèle SaaS présente plusieurs avantages pour les utilisateurs, notamment :

- **Accessibilité** : les applications SaaS sont accessibles à partir de n'importe quel appareil connecté à Internet, ce qui permet une utilisation facile et flexible.
- **Mises à jour automatiques** : le fournisseur SaaS est responsable de toutes les mises à jour logicielles, ce qui permet aux utilisateurs de bénéficier des dernières fonctionnalités et des améliorations de sécurité sans avoir à les installer manuellement.
- **Coût** : le modèle SaaS est généralement facturé sur une base d'abonnement mensuel ou annuel, ce qui permet une gestion plus facile des coûts. En outre, les utilisateurs n'ont pas besoin d'investir dans des infrastructures coûteuses pour héberger des applications en interne.

Cependant, le modèle SaaS présente également certains inconvénients, notamment :

- **Dépendance au fournisseur** : les utilisateurs sont entièrement dépendants du fournisseur SaaS pour le fonctionnement de leurs applications, ce qui peut entraîner une certaine vulnérabilité en cas de pannes ou de fermeture du service.
- **Personnalisation limitée** : les applications SaaS sont souvent limitées en termes de personnalisation et de fonctionnalités spécifiques en raison de la nature standardisée du service.
- **Sécurité** : les données sont stockées sur les serveurs du fournisseur SaaS, ce qui peut entraîner des préoccupations en matière de sécurité et de confidentialité. Les utilisateurs doivent être conscients de la politique de sécurité de leur fournisseur et prendre des mesures appropriées pour protéger leurs données.

2.5 Différences entre IaaS, PaaS, et SaaS :

Les trois modèles de service cloud computing (IaaS, PaaS, SaaS) se distinguent par le niveau de gestion et de responsabilité qu'ils offrent à l'utilisateur final.

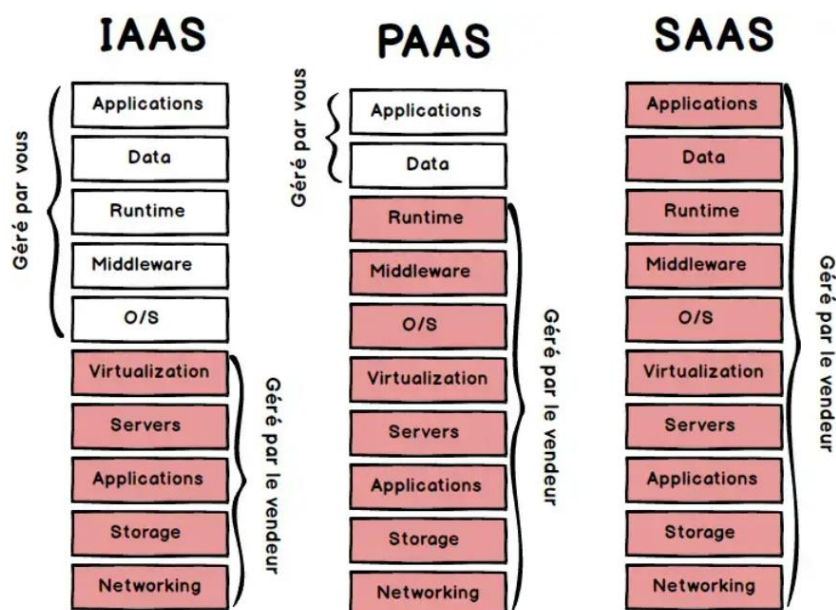


Figure 4: Différences entre IaaS, PaaS, et SaaS :

- IaaS est là pour vous fournir une flexibilité maximale en matière d'hébergement d'applications personnalisées, ainsi qu'un data center pour le stockage de données.
- PaaS est le plus souvent basé sur une plate-forme IaaS afin de réduire les besoins en administration système. Cela vous permet de vous concentrer sur le développement d'applications plutôt que sur la gestion d'infrastructure.
- SaaS offre des solutions prêtes à l'emploi et qui répondent à un besoin commercial particulier (tel qu'un site Web ou un courrier électronique). La plupart des plateformes SaaS modernes sont construites sur des plateformes IaaS ou PaaS.

3 Conclusion :

En conclusion, les modèles de services en nuage offrent des solutions flexibles pour répondre aux besoins des utilisateurs en matière d'hébergement, de gestion et de maintenance de leurs applications et de leurs données. Chaque modèle de service en nuage a ses avantages et ses inconvénients, il est donc important de comprendre les différences entre eux et de choisir celui qui convient le mieux à vos besoins spécifiques. En explorant les trois modèles de services en nuage les plus couramment utilisés, nous avons fourni une base solide pour aider à prendre une décision éclairée lors de la mise en place d'une infrastructure en nuage.

Chapitre IV : Les défis de sécurité des données dans le cloud et les stratégies de protection

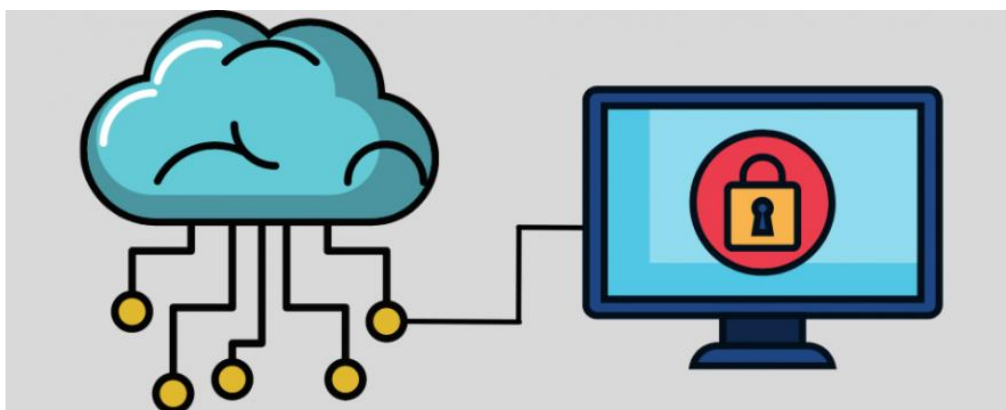
1 Introduction :

Avec tous ses avantages tels que l'évolutivité, la flexibilité, la rentabilité, le cloud computing représentent des économies substantielles pour l'entreprise et une plus grande commodité d'emploi pour ses utilisateurs. Mais les solutions de stockage dans le cloud posent certains défis et risques aux organisations qui le mettent en œuvre. Elles sont notamment la cible de tentatives d'atteinte à la sécurité bien connues.

2 Principaux défis de sécurité liés au cloud :

La sécurité est le facteur le plus souvent cité qui peut rendre une entreprise réticente à l'utilisation du stockage cloud. Une fois qu'un contenu quitte les locaux d'une entreprise, celle-ci n'a plus de contrôle sur la façon dont il est traité et stocké.

Selon statista, 64% des personnes interrogées dans une enquête menée en 2021 ont déclaré que la perte ou la fuite de données est leur plus grand défi avec le cloud computing. De même, 62 % ont déclaré que la confidentialité des données était leur deuxième défi le plus important.



2.1 Le manque de visibilité et de contrôle :

L'un des principaux avantages de l'utilisation des technologies basées sur le cloud est que le client n'a pas à gérer les ressources (par exemple, les serveurs) nécessaires au fonctionnement. Cependant, la délégation de la responsabilité de la gestion de la maintenance quotidienne des logiciels, de la plateforme ou des actifs informatiques peut entraîner une diminution de visibilité et de contrôle sur ces actifs.

Cela peut faire obstacle à l'organisation quand on veut :

- Tester l'efficacité de nos contrôles de sécurité puisqu'il n'y a aucune visibilité sur les outils et les données de la plateforme cloud

- La mise en place de plans de réponse aux incidents puisqu'il n'a pas nécessairement un contrôle total sur les ressources cloud
- Analyser les informations sur vos données, services et utilisateurs ce qui est souvent cruciale pour identifier les modèles d'utilisation incorrects associés à une faille de sécurité.

2.2 Les problèmes de confidentialité de données :

Si un service cloud manque de cybersécurité, l'envoi de données sensibles peut le rendre vulnérable au vol. Même lorsque de solides mesures de cybersécurité sont en place, le transfert de données vers le cloud peut enfreindre les accords de confidentialité entre une entreprise et ses clients. Des amendes, des restrictions commerciales et des atteintes à la réputation peuvent en résulter.

2.3 Le contrôle d'accès des utilisateurs :

Le contrôle d'accès des utilisateurs, qui relève presque toujours de la responsabilité de l'utilisateur, est un défi critique pour la sécurité du cloud, quel que soit le type de service cloud utilisé. Cependant, comme pour les solutions de sécurité sur site, le contrôle de l'accès des utilisateurs dans le cloud peut être difficile, surtout si le service cloud ne dispose pas de paramètres de contrôle très robustes.

3 Moyen de sécurisation de cloud :

Parmi les moyens de sécurité on a :

3.1 Pare feu (Firewall) :

La connexion d'ordinateurs personnels à d'autres systèmes informatiques ou à Internet offre de nombreux avantages, notamment la facilité de collaboration avec d'autres personnes, la mise en commun des ressources et une créativité accrue. Cependant, cela peut se faire au détriment d'une protection complète du réseau et des appareils. Le piratage, l'usurpation d'identité, les logiciels malveillants et la fraude en ligne sont des menaces courantes auxquelles les utilisateurs peuvent être confrontés lorsqu'ils s'exposent en connectant leurs ordinateurs à un réseau ou à Internet.

Une protection proactive est essentielle lors de l'utilisation de tout type de réseau. Les utilisateurs peuvent protéger leur réseau des pires dangers en utilisant un pare-feu.

Un pare-feu est un composant clé de la sécurité dans le cloud. Le pare-feu est un système de sécurité qui permet de surveiller et de contrôler le trafic réseau entrant et sortant d'un système informatique. Dans le contexte du cloud, le pare-feu est un élément essentiel de la sécurité pour protéger les données et les ressources de l'utilisateur dans le cloud.

Le pare-feu dans le cloud peut être configuré pour bloquer le trafic non autorisé et filtrer les données malveillantes provenant d'internet. Il peut également être configuré pour restreindre l'accès aux ressources du cloud à partir d'adresses IP spécifiques, ou pour autoriser l'accès uniquement à partir de certaines plages d'adresses IP.

Les pare-feux dans le cloud sont également capables de détecter et de bloquer les attaques de déni de service distribué (DDoS). Les pare-feux de nouvelle génération utilisent des technologies avancées de détection de menaces pour identifier et bloquer les attaques sophistiquées, telles que les attaques de phishing et les attaques par injection SQL.

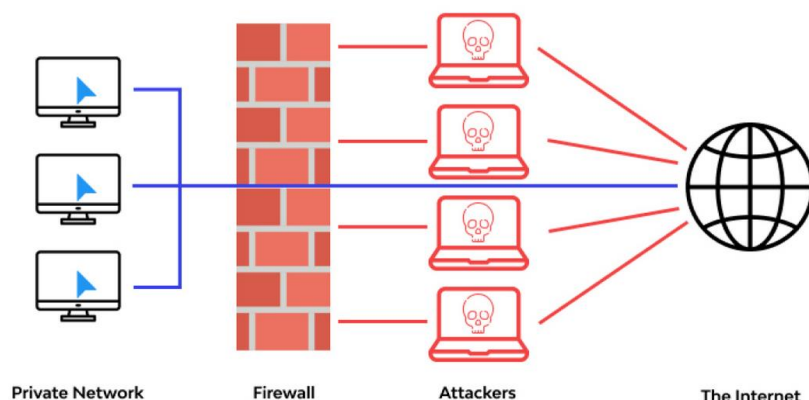


Figure 5:Cloud Firewall

3.2 Contrôle d'accès aux utilisateurs :

Le contrôle d'accès à Internet peut jouer un rôle important dans la sécurité des données d'une organisation. Il permet de limiter l'accès à certains sites Web et de restreindre l'utilisation de certains protocoles et applications qui pourraient présenter un risque pour la sécurité.

Voici quelques exemples d'impacts positifs du contrôle d'accès à Internet sur la sécurité des données :

- Protection contre les logiciels malveillants :

Les sites Web malveillants peuvent contenir des virus, des logiciels espions et d'autres programmes malveillants qui peuvent infecter les ordinateurs des utilisateurs et compromettre la sécurité des données. Le contrôle d'accès à Internet peut aider à bloquer l'accès à ces sites et à réduire le risque d'infection.

- Prévention des fuites de données :

Le contrôle d'accès à Internet peut aider à limiter l'utilisation de certains protocoles et applications qui pourraient être utilisés pour transférer des données sensibles hors du réseau de l'organisation. Par exemple, les employés peuvent être empêchés d'utiliser des services de stockage en nuage ou des services de messagerie instantanée qui ne sont pas approuvés par l'organisation.

- Réduction des risques de phishing :

Le contrôle d'accès à Internet peut aider à bloquer l'accès à des sites Web de phishing, qui sont conçus pour tromper les utilisateurs en leur demandant de fournir des informations sensibles telles que des identifiants et des mots de passe. En limitant l'accès à ces sites, le risque de vol de données par phishing peut être réduit.

3.3 Cryptage de données dans le cloud :

Le cryptage de données dans le cloud fait référence à l'utilisation de techniques de cryptographie pour protéger les données stockées dans le cloud.

Le cryptage de données dans le cloud fait référence à l'utilisation de techniques de cryptographie pour protéger les données stockées dans le cloud. Les services de cloud computing sont de plus en plus populaires pour stocker des données en raison de leur coût relativement faible, de leur accessibilité et de leur évolutivité. Toutefois, la sécurité des données dans le cloud est une préoccupation majeure pour de nombreuses organisations, en particulier lorsqu'il s'agit de données sensibles ou confidentielles.

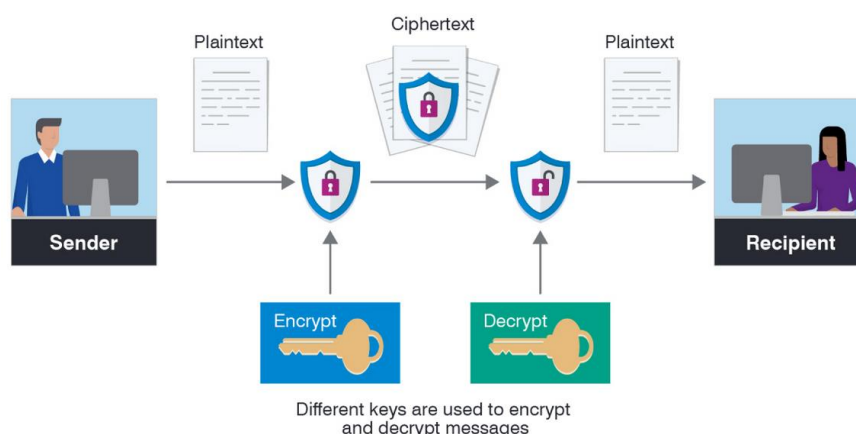


Figure 6: Cryptage des données dans le cloud

Le cryptage de données dans le cloud peut être réalisé de plusieurs manières, notamment :

➤ Cryptage de bout en bout :

Les données sont cryptées avant d'être envoyées dans le cloud et ne sont déchiffrées que lorsque l'utilisateur se connecte au cloud pour récupérer les données. Cette méthode offre un niveau de sécurité élevé, car les données sont chiffrées tout au long de leur transit et de leur stockage dans le cloud.

➤ Cryptage au niveau du serveur :

Les données sont cryptées une fois qu'elles atteignent le serveur de cloud et sont stockées sous forme chiffrée. Cette méthode est moins sécurisée que le cryptage de bout en bout, car les données sont déchiffrées une fois qu'elles atteignent le serveur, ce qui laisse une fenêtre d'opportunité pour les attaquants.

➤ Cryptage de base de données :

Les données sont stockées dans une base de données chiffrée qui est hébergée dans le cloud. Cette méthode offre un niveau élevé de sécurité, car les données sont chiffrées même lorsqu'elles sont stockées dans la base de données.

4 Conclusion :

La protection des données dans le cloud computing est une préoccupation majeure pour les organisations qui adoptent cette technologie.

En utilisant ces stratégies et technologies, les entreprises peuvent aider à sécuriser leurs données sensibles.

Chapitre VI : Étude de cas : Mise en place d'un pare-feu dans le Cloud

1 Introduction :

Bienvenue dans le quatrième chapitre de notre rapport sur le Cloud Computing. Dans ce chapitre, nous allons explorer les différentes étapes que nous avons suivies pour mettre en place notre solution Firewall en utilisant Microsoft Azure comme plateforme Cloud. Le Firewall est une solution de sécurité essentielle pour protéger les systèmes informatiques contre les menaces extérieures. Notre objectif était de créer une solution Firewall efficace et facile à gérer pour assurer la sécurité de notre infrastructure en nuage. Nous allons décrire les différentes étapes que nous avons suivies, en fournissant des explications détaillées et des exemples pratiques pour faciliter la compréhension.

2 Cloud Azure :

Azure est une plateforme de services cloud fournie par Microsoft qui permet aux entreprises de déployer, de gérer et de développer des applications et des services via Internet.

Azure fournit une grande variété de services, notamment des services d'hébergement de machines virtuelles, des bases de données, des services de stockage de fichiers, des services de messagerie, des services de sécurité et de conformité, des services d'analyse et d'intelligence artificielle, ainsi que des outils de développement et de gestion.

Avec Azure, les entreprises peuvent tirer parti de la puissance du cloud pour accélérer l'innovation, améliorer l'agilité des affaires et réduire les coûts d'infrastructure informatique. En outre, Azure offre une grande flexibilité en permettant aux entreprises de choisir les services dont elles ont besoin, ainsi que la capacité de les ajuster et de les mettre à l'échelle en fonction de leurs besoins en temps réel.



3 Implémentation :

3.1 Création du groupe de ressource :

Azure Resource Group est un conteneur logique qui permet aux utilisateurs de gérer et d'organiser les ressources Azure en fonction de leurs besoins. Il s'agit d'un service de gestion de ressources d'Azure qui permet de regrouper les ressources Azure en fonction de leur fonctionnalité, de leur emplacement géographique, de leur cycle de vie, etc.

Microsoft Azure | Search resources, services, and docs (G+)

Home > Resource groups > Create a resource group

Create a resource group

Basics | Tags | Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Project details

Subscription * ⓘ Free Trial

Resource group * ⓘ FW-ResourceGroup

Resource details

Region * ⓘ (US) East US

Figure 7: Configuration de ressource groupe

Tous les services >

Créer un groupe de ressources

✓ Validation réussie.

De base | Étiquettes | Vérifier + créer

De base	
Abonnement	Azure subscription 1
Groupe de ressources	FW-ResourceGroup
Région	East US
Étiquettes	
Aucun	

Figure 8: Validation et creation

3.2 Création de réseaux virtuelle :

Azure Virtual Networks est un service de réseau cloud qui vous permet de créer un réseau privé virtuel (VPN) dans Azure. Le service vous permet de connecter plusieurs machines virtuelles (VM) à un réseau privé sécurisé et isolé, et de contrôler les communications entre ces machines virtuelles.

Tous les services > Réseaux virtuels >

Créer un réseau virtuel

De base **Adresses IP** Sécurité Étiquettes Vérifier + créer

Espace d'adressage du réseau virtuel, spécifié sous la forme d'un ou plusieurs préfixes d'adresse en notation CIDR (par exemple, 192.168.1.0/24).

Espace d'adressage IPv4

10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 adresses)

192.168.0.0/16

☐ Ajouter un espace d'adressage IPv6

Plage d'adresses du sous-réseau en notation CIDR (par exemple, 192.168.1.0/24). Elle doit faire partie de l'espace d'adressage du réseau virtuel.

+ Ajouter un sous-réseau Supprimer le sous-réseau

Nom de sous-réseau	Espace d'adressage de sous-réseau	Passerelle NAT
default	10.0.0.0/24	-

Vérifier + créer < Précédent Suivant : Sécurité > Télécharger un modèle pour automation

Ajouter un sous-ré...

Nom de sous-réseau * AzureFirewallSubnet

Espace d'adressage de sous-réseau * 192.168.1.0/24

192.168.1.0 - 192.168.1.255 (251 + 5 adresses réservées Azure)

PASSERELLE NAT

Simplifiez la connectivité à Internet à l'aide d'une passerelle de traduction d'adresses réseau. Une connectivité sortante est possible sans équilibreur de charge ou adresses IP publiques attachées à vos machines virtuelles. [En savoir plus](#)

Passerelle NAT Aucun

POINTS DE TERMINAISON DE SERVICE

Créez des stratégies de point de terminaison de service pour autoriser le trafic vers des ressources Azure spécifiques à partir de votre réseau virtuel ou des réseaux de destination de...

Ajouter Annuler

Figure 9: Configuration des réseaux et des sous réseaux

Tous les services > Réseaux virtuels >

Créer un réseau virtuel

Validation réussie

De base Adresses IP Sécurité Étiquettes **Vérifier + créer**

De base

Abonnement	Azure subscription 1
Groupe de ressources	FW-ResourceGroup
Nom	FW-VirtualNetwork
Région	East US

Adresses IP

Espace d'adressage	10.0.0.0/16, 192.168.0.0/16
Sous-réseau	default (10.0.0.0/24), AzureFirewallSubnet (192.168.1.0/24), Server1.Subnet2 (192.168.2.0/24)

Étiquettes

Aucun

Créer < Précédent Suivant > Télécharger un modèle pour automation

Figure 10: Réseau virtuel a été créé

3.3 Déployer une machine virtuelle :

Cette partie est réservée pour la création et la configuration de notre machine virtuelle.

Créer une machine virtuelle ...

De base Disques Mise en réseau Administration Monitoring Paramètres avancés Étiquettes Vérifier + créer

Créez une machine virtuelle qui exécute Linux ou Windows. Sélectionnez une image dans la Place de marché Azure ou utilisez une image personnalisée. Renseignez l'onglet De base et sélectionnez Vérifier + créer pour provisionner une machine virtuelle avec des paramètres par défaut, ou passez en revue chaque onglet pour une personnalisation complète. [En savoir plus](#)

Détails du projet

Sélectionnez l'abonnement pour gérer les coûts et les ressources déployées. Utilisez les groupes de ressources comme les dossiers pour organiser et gérer toutes vos ressources.

Abonnement * Azure subscription 1

Groupe de ressources * FW-ResourceGroup [Créer nouveau](#)

Détails de l'instance

Nom de la machine virtuelle * server1

Région * (US) East US

Options de disponibilité Zone de disponibilité

Zone de disponibilité * Zones 1

☒ Vous pouvez désormais sélectionner plusieurs zones. La sélection de plusieurs zones crée une machine virtuelle par zone. [En savoir plus](#)

Type de sécurité Standard

Image * Windows Server 2016 Datacenter - x64 Gen2 [Voir toutes les images](#) | [Configurer la génération de machine virtuelle](#)

Architecture de machine virtuelle ☐ Arm64 ☒ x64

Vérifier + créer < Précédent Suivant : Disques >

Figure 11: Configuration de la machine virtuelle

Tous les services / Machines virtuelles

Créer une machine virtuelle

De base Disques **Mise en réseau** Administration Monitoring Paramètres avancés Étiquettes Vérifier + créer

Définissez la connectivité réseau de votre machine virtuelle en configurant les paramètres de la carte d'interface réseau. Vous pouvez contrôler les ports et la connectivité entrante/sortante avec des règles de groupe de sécurité, ou placer derrière une solution d'équilibrage de charge existante. [En savoir plus](#)

Interface réseau

Quand vous créez une machine virtuelle, une interface réseau est créée pour vous.

Réseau virtuel * [Créer](#)

Sous-réseau * [Gérer la configuration du sous-réseau](#)

Adresse IP publique [Créer](#)

Groupe de sécurité réseau de la carte réseau ☐ Aucun ☒ De base ☐ Paramètres avancés

Ports d'entrée publics * ☒ Aucun ☐ Autoriser les ports sélectionnés

Sélectionner des ports d'entrée

i Tout le trafic en provenance d'Internet sera bloqué par défaut. Vous pouvez changer les règles de port d'entrée dans la page Machine virtuelle > Mise en réseau.

Supprimer la carte réseau lors de la ☐

[Vérifier + créer](#) [< Précédent](#) [Suivant : Administration >](#)

Figure 12: Configuration de la machine virtuelle :

Microsoft Azure Rechercher dans les ressources, services et documents (G)

Tous les services > Machines virtuelles >

Créer une machine virtuelle

Validation réussie

PRODUCT DETAILS

1 X Standard D4s v3
by Microsoft
[Terms of use](#) | [Privacy policy](#)

Subscription credits apply **0,3760 USD/hr**
[Pricing for other VM sizes](#)

TERMS

By clicking "Créer", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above, (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

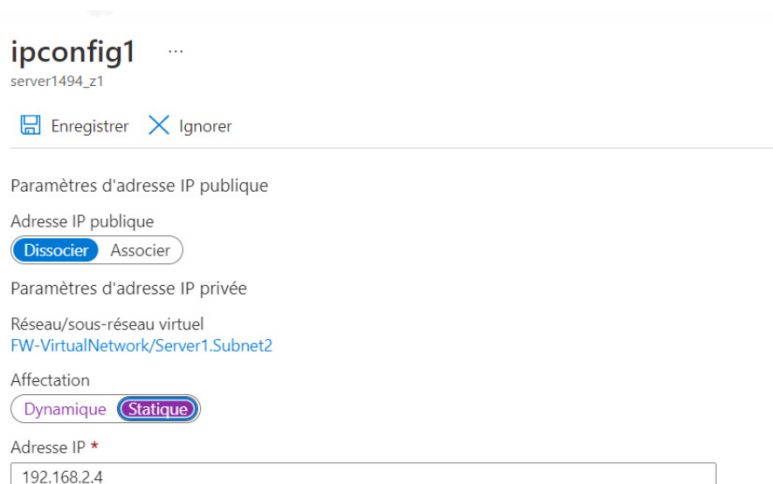
De base

Abonnement	Azure subscription 1
Groupe de ressources	FW-ResourceGroup
Nom de la machine virtuelle	server1
Région	East US
Options de disponibilité	Zone de disponibilité
Zone de disponibilité	1
Type de sécurité	Standard
Image	Windows Server 2016 Datacenter - Génération 2
Architecture de machine virtuelle	x64
Taille	Standard D4s v3 (4 processeurs virtuels, 16 Gio de mémoire)
Nom d'utilisateur	bingo
Ports d'entrée publics	Aucun

[Créer](#) [< Précédent](#) [Suivant >](#) [Télécharger un modèle pour automation](#)

Figure 13: La machine virtuelle a été créé

Pour faciliter la gestion du réseau : Lorsqu'une adresse IP est dynamique, elle peut changer chaque fois que la machine virtuelle est redémarrée ou reconnectée au réseau. Cela peut compliquer la gestion du réseau car il est plus difficile de localiser la machine virtuelle et de la configurer pour communiquer avec d'autres machines sur le réseau. En configurant l'adresse IP de la machine virtuelle en statique, il est plus facile de la gérer car elle aura toujours la même adresse IP.



ipconfig1 ...

server1494_z1

Enregistrer Ignorer

Paramètres d'adresse IP publique

Adresse IP publique

Dissocier Associer

Paramètres d'adresse IP privée

Réseau/sous-réseau virtuel

FW-VirtualNetwork/Server1.Subnet2

Affectation

Dynamique Statique

Adresse IP *

192.168.2.4

Figure 14 :Rendre l'adresse IP de la machine virtuelle statique

3.4 Création de pare-feu :

Azure Firewall est un service de pare-feu managé qui offre une sécurité avancée pour les applications et les réseaux déployés dans Azure. Il permet de protéger les ressources cloud contre les menaces en filtrant le trafic réseau entrant et sortant.



Accueil > Pare-feux >

Créer un pare-feu ...

De base Étiquettes Vérifier + créer

Le Pare-feu Azure est un service de sécurité réseau managé basé sur le cloud qui protège vos ressources Réseau virtuel Azure. Il s'agit d'un pare-feu avec état complet qui est fourni en tant que service et qui combine haute disponibilité et scalabilité illimitée dans le cloud. Vous pouvez créer, appliquer et journaliser des stratégies d'application et réseau sur plusieurs abonnements et réseaux virtuels, de manière centralisée. Le Pare-feu Azure utilise une adresse IP publique statique pour vos ressources de réseau virtuel, ce qui permet aux pare-feu externes d'identifier le trafic issu de votre réseau virtuel. Le service est entièrement intégré à Azure Monitor pour la journalisation et l'analytique. [En savoir plus](#)

Détails du projet

Abonnement *

Azure subscription 1

Groupe de ressources *

FW-ResourceGroup

Créer nouveau

Détails de l'instance

Nom *

Firewall900

Région *

East US

Figure 15 :Configuration du pare-feu

Figure 16: 2. Configuration du pare-feu

Le déploiement du pare-feu a été effectué :

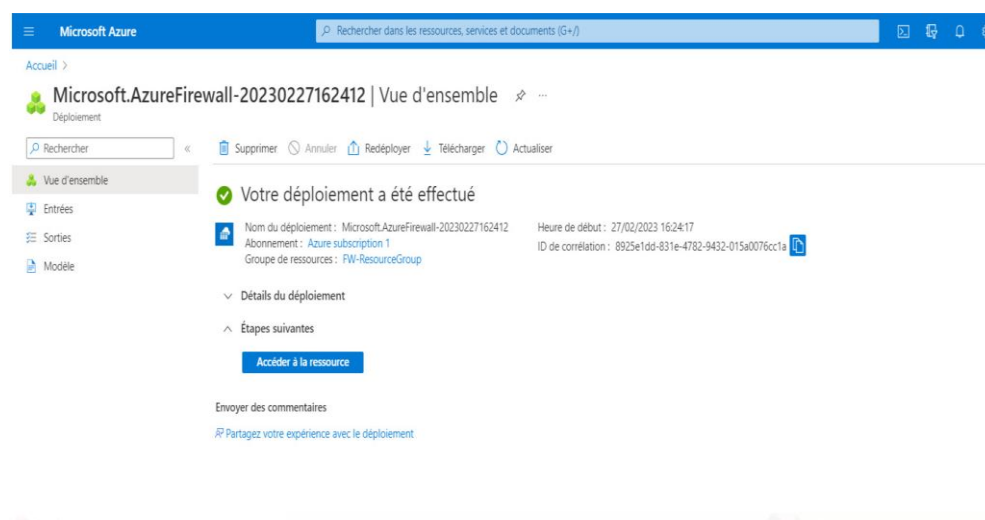


Figure 17: Déploiement du pare-feu a été effectué

3.5 Se connecter à la machine virtuelle à travers le pare-feu :

3.5.1 Première règles NATRule :

Les règles NAT (Network Address Translation) dans Azure Firewall vous permettent de rediriger le trafic provenant d'adresses IP publiques vers des adresses IP privées dans votre réseau virtuel Azure. Cela peut être utile pour permettre à des utilisateurs externes d'accéder à des ressources internes, ou pour permettre à des machines dans votre réseau virtuel d'accéder à Internet.

Ajouter une collection de règles

Nom *

Type de collection de règles *

Priorité *

Action de collection de règles

Groupe de collections de règles *

Règles

Nom *	Type de source	Source	Protocole *	Ports de	Type de destination *	Destination *	Type tr
RDPrule	Adresse IP	*	TCP	3389	Adresse IP	104.211.8.170	Adres
	Adresse IP	*, 192.168.10.1, 192...	0 sélectionné	8080	Adresse IP	192.168.10.1	Adres

Figure 18: Ajout d'une collection de règles

En ajoutant cette règle on peut se connecter à la machine virtuelle à travers le pare-feu.

Connexion Bureau à distance

Connexion Bureau A distance

Ordinateur :

Nom d'utilisateur : bingo

Les informations d'identification enregistrées seront utilisées pour la connexion à cet ordinateur. Vous pouvez les [modifier](#) ou les [supprimer](#).

Figure 19: Connexion à distance

Se connecter à la machine virtuelle depuis la machine locale

Windows Security

Enter your credentials

These credentials will be used to connect to 13.83.57.99.

☐ Remember me

Figure 20: Connexion à la machine virtuelle

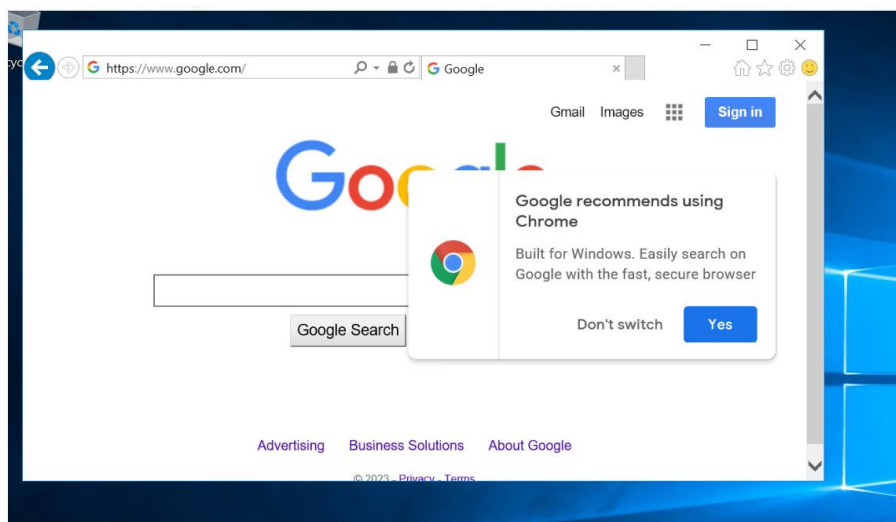


Figure 21: Lors de notre première connexion l'utilisateur avait le droit d'accéder à n'importe quels sites.

3.6 Table de routage :

La table de routage d'un pare-feu Azure (Azure Firewall) est utilisée pour spécifier les règles de routage qui permettent à la solution de filtrer et de contrôler le trafic réseau entrant et sortant dans le réseau virtuel Azure.

La table de routage peut être configurée pour inclure des règles pour diriger le trafic vers des destinations spécifiques, en fonction de divers critères tels que l'adresse IP de la source et de la destination, le port utilisé, le protocole utilisé et d'autres critères.

Ces règles peuvent être utilisées pour rediriger le trafic vers le pare-feu Azure afin qu'il soit filtré et sécurisé avant d'atteindre sa destination finale, ou pour rediriger le trafic vers des appliances virtuelles tierces pour effectuer des tâches spécifiques telles que l'inspection de paquets SSL.

Microsoft Azure

Accueil > Tables d'itinéraires >

Créer Route table

De base Tags Vérifier + créer

Détails du projet

Sélectionnez l'abonnement pour gérer les coûts et les ressources déployées. Utilisez les groupes de ressources comme les dossiers pour organiser et gérer toutes vos ressources.

Abonnement * ⓘ Azure subscription 1

Groupe de ressources * ⓘ FW-ResourceGroup
[Créer nouveau](#)

Détails de l'instance

Région * ⓘ East US

Nom * ⓘ MyRouteTable

Propager des routes de passerelle * ⓘ ☒ Yes ☐ No

Figure 22: Configuration de la table de routage

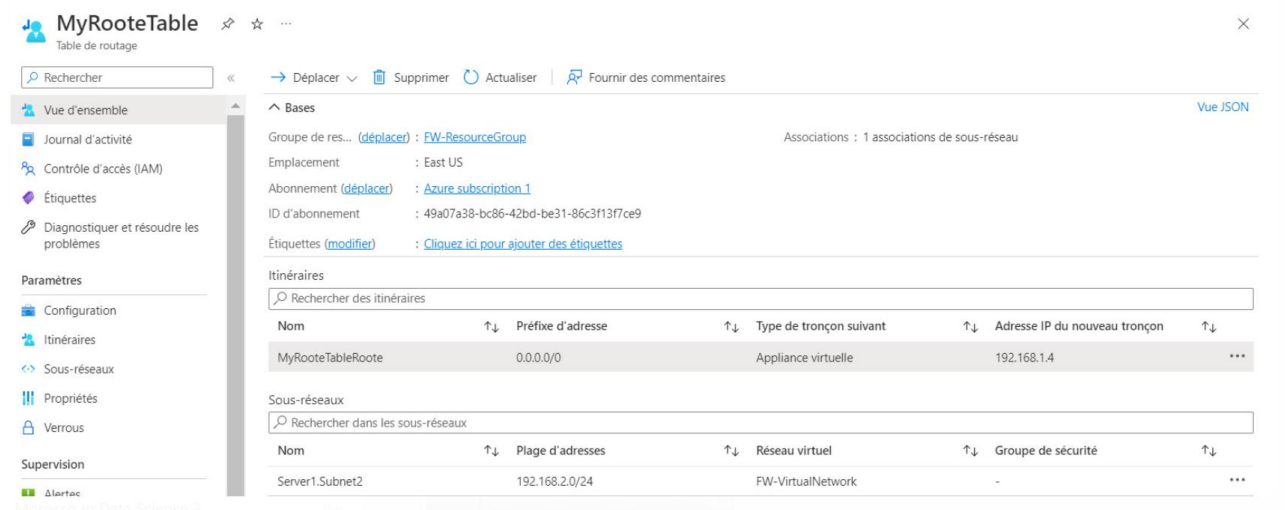


Figure 23: Création d'une table de routage

Création d'une route qui bloque tout trafic entrant et sortant

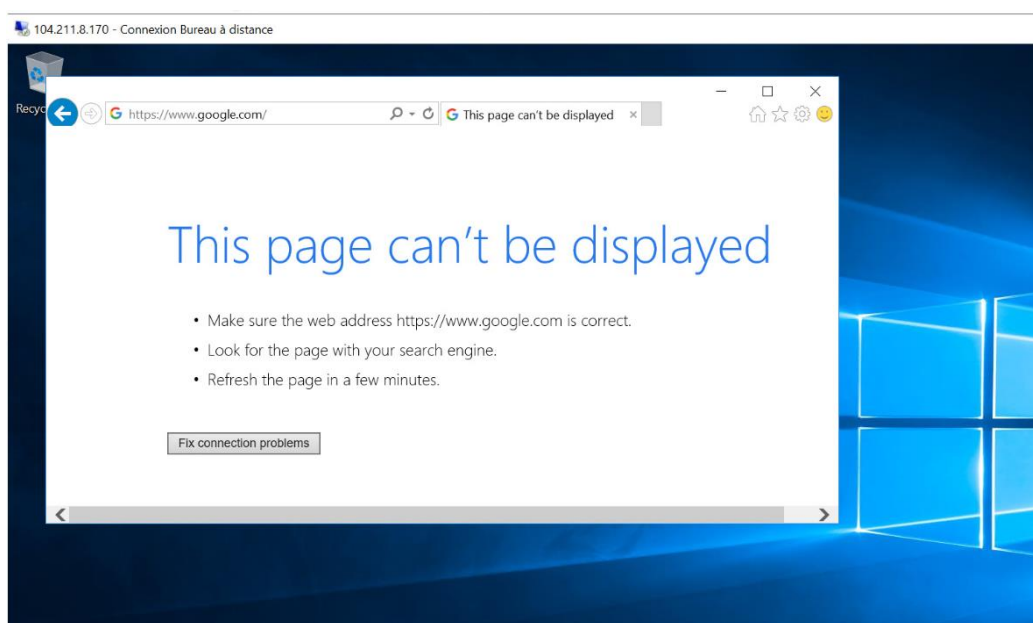
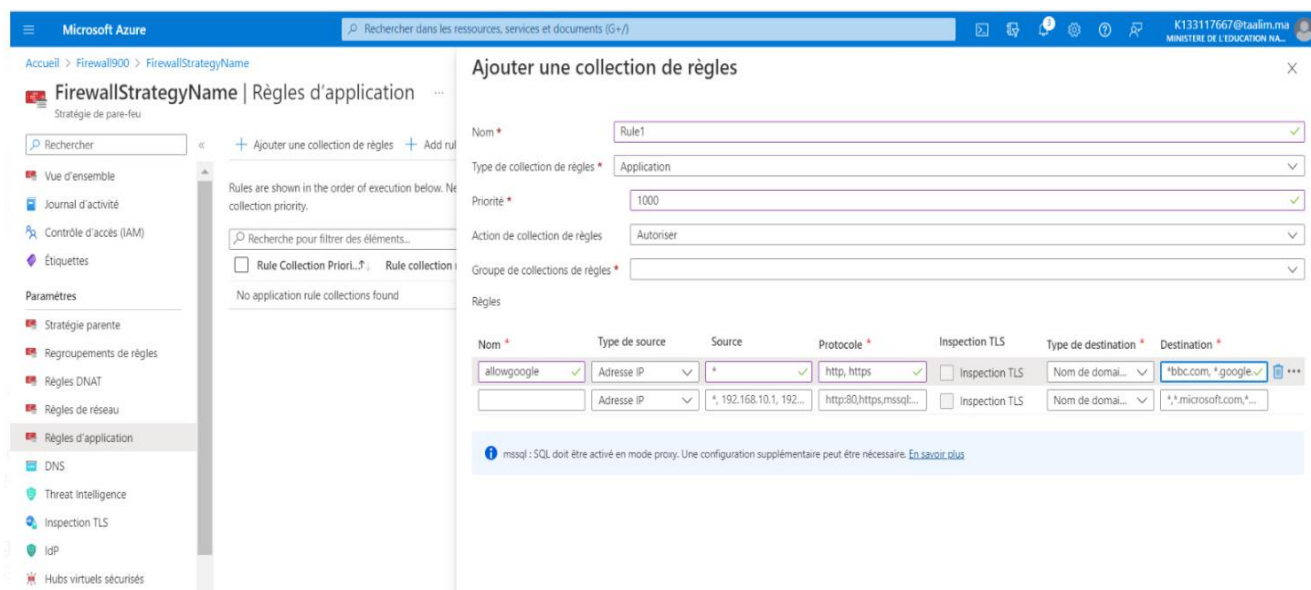


Figure 24: Résultat après la création de la table de route

Après la création du route l'utilisateur ne peut pas accéder à aucun site



On a ajouté une règle d'application pour autoriser l'accès à google

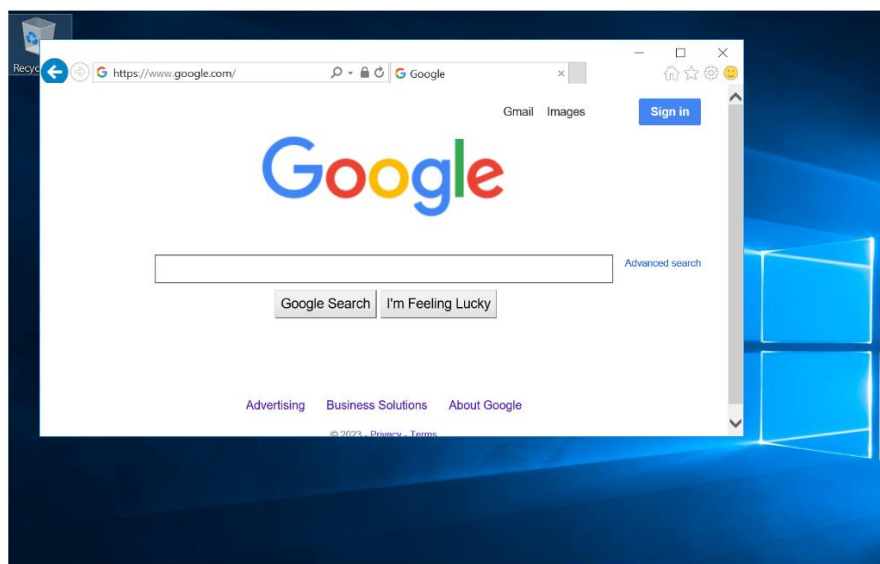


Figure 25: Résultat après l'ajout d'une règle d'application

L'accès a été autorisé. De même pour tous les autres sites on peut autoriser ce qu'on veut et refuser ce qu'on veut.

4 Conclusion :

En effectuant ces étapes, nous avons créé un environnement de cloud computing sécurisé qui protège nos applications et nos données contre les menaces de sécurité. Cependant, la sécurité est un processus continu, nous devons donc surveiller régulièrement notre environnement de cloud computing pour détecter les menaces de sécurité émergentes et mettre en place des mesures de sécurité appropriées pour les contrer.

Conclusion Générale :

La conclusion générale est l'occasion de récapituler les principaux points abordés dans le rapport. Nous avons commencé par définir le Cloud Computing et ses caractéristiques essentielles, avant de nous concentrer sur les différents modèles de déploiement et de services en nuage. Nous avons également présenté les avantages et les inconvénients de chaque modèle, ce qui peut aider les entreprises à choisir la solution la mieux adaptée à leurs besoins.

Ensuite, Nous avons expliqué les défis associés à la sécurité de l'information dans le cloud computing et nous avons discuté également des stratégies et des technologies de protection des données disponibles.

Enfin, nous avons détaillé notre implémentation d'un pare-feu pour améliorer la sécurité des données dans le Cloud Computing. Nous avons expliqué comment cela peut aider à protéger les informations sensibles et à prévenir les violations de données.

En résumé, le Cloud Computing offre de nombreux avantages, mais il est important de comprendre les risques et les mesures de sécurité nécessaires pour protéger les données de l'entreprise.

5 Autres Références :

Jonatha Anselmi, Danilo Ardagna, Mauro Passacantando." Generalized Nash equilibria for SaaS/PaaS Clouds", European Journal of Operational Research 236 (2014) 326–339

Thomas. (2020, February 10). Différence Entre IaaS, SAAS et paas. WayToLearnX.from <https://waytolearnx.com/2019/03/difference-entre-iaas-saas-et-paas.html>

"IaaS, paas, Saas : Quelles sont les différences ?," Red Hat - We make open source technologies for the enterprise. [Online].

Kessler, T. (2017). Sécurité de l'information avec le cloud computing. Bulletin des médecins suisses, 98(45), 1493-1494.

KESSLER, Thomas. Sécurité de l'information avec le cloud computing. Bulletin des médecins suisses, 2017, vol. 98, no 45, p. 1493-1494.

Kessler, Thomas. "Sécurité de l'information avec le cloud computing." Bulletin des médecins suisses 98.45 (2017): 1493-1494.

M. rediriger directement vers: "Qu'est-ce que le cloud computing ?," ServiceNow. [Online]. Available: <https://www.servicenow.com/fr/products/it-operations-management/what-is-cloud-computing.html>.

"Les Défis de Sécurité dans le cloud computing: Problèmes et solutions ..." [Online]. Available:https://www.researchgate.net/publication/260733580_Les_defis_de_securite_dans_le_Cloud_Computing_Problemes_et_solutions_de_la_securite_en_Cloud_Computing.

Futura, "DÉFINITION: Cloud computing - informatique EN NUAGE: Futura Tech," Futura, 08-Apr-2015. [Online]. Available: <https://www.futura-sciences.com/tech/definitions/informatique-cloud-computing-11573/>.

Elmrabti, A. A., Abou El Kalam, A., & Ouahman, A. A. (2012, April). Les défis de sécurité dans le Cloud Computing: Problèmes et solutions de la sécurité en Cloud Computing. In 2012 National Days of Network Security and Systems (pp. 80-85). IEEE.

ELMRABTI, Almokhtar Ait, ABOU EL KALAM, Anas, et OUAHMAN, Abdellah Ait. Les défis de sécurité dans le Cloud Computing: Problèmes et solutions de la sécurité en Cloud Computing. In : 2012 National Days of Network Security and Systems. IEEE, 2012. p. 80-85.