International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 57 No. 2 June 2026, pp. 178-185

Micro-Segmentation Réseau Pour La Réduction Des Surfaces D'attaque Dans Les Startups Fintech

[Network Micro-Segmentation For Reducing Attack Surfaces In Fintech Startups]

Albert MUNTUMUINE KAMBAYI[1], Dede LUNGUNGU MUPEPE[2], Pierre KAMUINA KAMBAYI[3], Daniel KABISHI KABUMBAYI[4], Espérance LEMA BONIEBI[5], Adolphe MUKABA[6]

[1] Département de Mathématique et Informatique,
Université Pédagogique Nationale (UPN),
Kinshasa, République Démocratique du Congo
Email : albertkambayi92@gmail.com
[2] Département Informatique,
Institut Supérieur Technique Médical de Bandundu,
Bandundu, République Démocratique du Congo
Email : dedelungungu@gmail.com
[3] Département Informatique,
Université Pédagogique Nationale,
Kinshasa, République Démocratique du Congo
Email : pierrekamuina@gmail.com
[4] Département Informatique,
Université Pédagogique Nationale,
Kinshasa, République Démocratique du Congo
Email : danielkabis78@gmail.com
[5] Département Informatique,
Université Pédagogique Nationale,
Kinshasa, République Démocratique du Congo
Email : lemaboniebi@gmail.com
[6] Département Mathématique et Informatique,
Université Pédagogique Nationale (UPN),
Kinshasa, République Démocratique du Congo
Email : adolphemukaba@gmail.com

Auteur Correspondant : Albert MUNTUMUINE KAMBAYI, albertkambayi92@gmail.com

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 57 No. 2 June 2026, pp. 178-185

Résumé : La croissance rapide des startups de technologie financière s'accompagne d'une augmentation significative des cybermenaces, en particulier dans les environnements à ressources limitées. Les architectures réseau traditionnelles, fondées sur des mécanismes de segmentation classiques, présentent des limites face aux attaques modernes caractérisées par des déplacements internes après une intrusion initiale, exposant ainsi les ressources critiques à des risques élevés.

Cette étude a pour objectif d'évaluer l'efficacité de la micro-segmentation dans la réduction de la surface d'attaque au sein des startups de technologie financière. La méthodologie adoptée repose sur une approche expérimentale et descriptive combinant des audits réseau, des observations directes, des simulations de scénarios d'attaque et des entretiens avec des responsables informatiques. Un échantillon de dix startups a été retenu afin d'analyser les architectures existantes et de tester l'implémentation de politiques de micro-segmentation dans des environnements simulés.

Les résultats obtenus montrent une réduction importante des déplacements internes, avec une diminution moyenne d'environ quatre-vingt-trois pour cent. Une amélioration significative du taux de détection des activités malveillantes ainsi qu'un renforcement du niveau d'isolation des ressources critiques ont également été observés.

En conclusion, la micro-segmentation constitue une solution efficace et adaptée pour améliorer la sécurité des systèmes dans des contextes contraints, à condition de mettre en œuvre des politiques de sécurité rigoureuses et de disposer de compétences techniques appropriées.

Mots-clés : Micro-segmentation réseau, réduction de la surface d'attaque, sécurité des réseaux, startups Fintech, cybersécurité

Abstract: The rapid expansion of financial technology startups has significantly increased exposure to cyber threats, particularly in environments with limited technological resources. Traditional network segmentation approaches are no longer sufficient to protect critical systems against modern attacks that involve internal movement after an initial breach. As a result, sensitive resources are highly vulnerable to security risks.

This study aims to evaluate the effectiveness of network micro-segmentation in reducing the attack surface within financial technology startups. The research is based on an experimental and descriptive methodology combining network audits, direct observations, simulated attack scenarios, and interviews with information technology managers. A sample of ten startups was selected to analyze existing network architectures and to implement micro-segmentation policies in controlled environments.

The results show a significant reduction in internal threat propagation, with an average decrease of approximately eighty-three percent. In addition, the detection of malicious activities improved considerably, and the isolation of critical resources was strengthened. These findings demonstrate that micro-segmentation enhances internal traffic control and limits the spread of threats within the network.

The study concludes that micro-segmentation is an effective and adaptable solution for improving network security in constrained environments, provided that appropriate security policies and technical expertise are ensured.

Keywords : Network micro-segmentation, attack surface reduction, network security, Fintech startups, cybersecurity

1. INTRODUCTION

La transformation numérique du secteur financier a favorisé l'émergence rapide des startups de technologie financière, offrant des services innovants tels que les paiements électroniques, les transferts d'argent instantanés et les solutions bancaires dématérialisées [1]. Dans des environnements urbains en pleine expansion, ces entreprises jouent un rôle important dans l'inclusion financière et l'amélioration de l'accès aux services bancaires [7]. Cependant, cette évolution s'accompagne d'une exposition accrue aux cybermenaces en raison de la sensibilité des données manipulées et de la criticité des services fournis [2].

Les architectures réseau traditionnelles, basées sur des mécanismes de segmentation classiques, montrent aujourd'hui leurs limites face aux attaques modernes. Ces dernières sont souvent caractérisées par des déplacements internes permettant à un attaquant de se propager dans le réseau après une compromission initiale [3]. Cette problématique est particulièrement critique dans les environnements à ressources limitées, où les mécanismes avancés de sécurité sont rarement déployés et où les politiques de contrôle des flux internes restent insuffisantes [4], [9].

Dans ce contexte, la micro-segmentation apparaît comme une approche prometteuse pour renforcer la sécurité des infrastructures réseau. Elle permet une isolation fine des ressources critiques ainsi qu'un contrôle strict des communications entre les différents composants du système, réduisant ainsi la surface d'attaque et limitant la propagation des menaces [5], [6].

L'objectif principal de cette étude est d'analyser l'apport de la micro-segmentation dans la sécurisation des architectures réseau des startups de technologie financière. Plus spécifiquement, il s'agit d'identifier les limites des approches traditionnelles, de proposer un modèle d'architecture basé sur la micro-segmentation, d'évaluer son efficacité face aux scénarios d'attaque et de formuler des recommandations adaptées aux environnements contraints.

Afin de répondre à ces objectifs, plusieurs questions de recherche ont été définies : quelles sont les limites des architectures réseau traditionnelles face aux menaces actuelles ? Dans quelle mesure la micro-segmentation permet-elle de réduire les déplacements internes et la surface d'attaque ? Comment concevoir une architecture adaptée aux contraintes des startups de technologie financière ?

À partir de ces questions, trois hypothèses principales sont formulées : les architectures traditionnelles ne permettent pas de limiter efficacement les déplacements internes [1],[2] ; la micro-segmentation réduit significativement la propagation des menaces [3],[4] ; et une architecture basée sur cette approche améliore le niveau global de sécurité, même dans des environnements à ressources limitées [8], [10].

2. MÉTHODOLOGIE

La présente étude adopte une approche expérimentale et descriptive pour évaluer l'efficacité de la micro-segmentation dans la sécurisation des architectures réseau des startups Fintech à Kinshasa. L'approche expérimentale est particulièrement adaptée aux recherches en cybersécurité, car elle permet de simuler des scénarios d'attaque et d'observer le comportement des systèmes face à différentes menaces [3]. L'aspect descriptif permet de documenter les caractéristiques des architectures réseau existantes et les pratiques de sécurité au sein des startups locales [2].

La population cible est constituée de startups Fintech disposant d'une infrastructure réseau interne pour la gestion de services financiers numériques. Compte tenu du nombre limité de startups pleinement fonctionnelles et accessibles, un échantillon raisonné de dix entreprises a été sélectionné selon des critères précis : taille de l'entreprise, nature des services financiers proposés, existence d'un réseau interne et volonté de participer à l'étude [4].

La collecte des données a combiné plusieurs méthodes. Des observations directes et audits réseau ont été réalisés afin d'analyser les architectures existantes et d'identifier les vulnérabilités liées à la segmentation traditionnelle [4]. Des expérimentations simulées ont ensuite été effectuées sur des environnements réseau modélisés à partir des infrastructures réelles des startups. Ces expérimentations ont consisté à implémenter des politiques de micro-segmentation et à simuler des scénarios d'attaque, incluant les mouvements latéraux et les tentatives d'accès non autorisé aux ressources critiques [5].

Pour ces expérimentations, des outils spécialisés d'analyse et de simulation réseau ont été utilisés, tels que Wireshark pour l'inspection du trafic, des pare-feu configurés pour le filtrage interne et des environnements de virtualisation permettant de reproduire fidèlement les architectures étudiées. Cette approche a permis une analyse fine des communications réseau et une détection précise des comportements anormaux, conformément aux bonnes pratiques en cybersécurité [3], [4].

Enfin, des entretiens semi-structurés avec les responsables informatiques et administrateurs réseau ont complété les observations, apportant des informations sur les pratiques, contraintes et perceptions en matière de sécurité [2]. L'analyse des données a combiné des techniques quantitatives, telles que le nombre de mouvements latéraux détectés et le taux de réussite des attaques, et qualitatives, avec codage thématique des entretiens pour identifier les pratiques et obstacles récurrents.

Les résultats expérimentaux ont été comparés aux architectures existantes afin d'évaluer l'efficacité relative de la micro-segmentation et de valider les hypothèses formulées [4].

3. RESULTATS

L'analyse des données collectées auprès des 10 startups Fintech sélectionnées et des simulations expérimentales a permis de mettre en évidence l'impact de la micro-segmentation sur la sécurité du réseau. Les résultats sont présentés selon trois axes : état des architectures existantes, efficacité de la micro-segmentation face aux attaques et comparaison quantitative des performances.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 57 No. 2 June 2026, pp. 178-185

3.1. État des architectures réseau existantes

Les audits réseau réalisés ont montré que toutes les startups étudiées utilisaient une segmentation classique basée sur VLAN ou zones logiques. Les principales vulnérabilités identifiées sont :

- Absence de contrôle granulaire entre les ressources critiques (serveurs de paiement, bases de données et applications internes) ;
- Détection limitée des mouvements latéraux après une intrusion initiale ;
- Faible application des politiques de sécurité sur les flux internes.

Tableau 1. Synthèse des vulnérabilités réseau existantes

Startup	Type de segmentation	Ressources critiques non isolées	Détection mouvements latéraux	Politiques internes
S1	VLAN	Oui	Faible	Partielle
S2	VLAN	Oui	Faible	Partielle
S3	VLAN	Oui	Faible	Partielle
S4	Zones logiques	Oui	Faible	Limitée
S5	VLAN	Oui	Faible	Partielle
S6	Zones logiques	Oui	Faible	Limitée
S7	VLAN	Oui	Faible	Partielle
S8	VLAN	Oui	Moyenne	Partielle
S9	Zones logiques	Oui	Faible	Limitée
S10	VLAN	Oui	Faible	Partielle

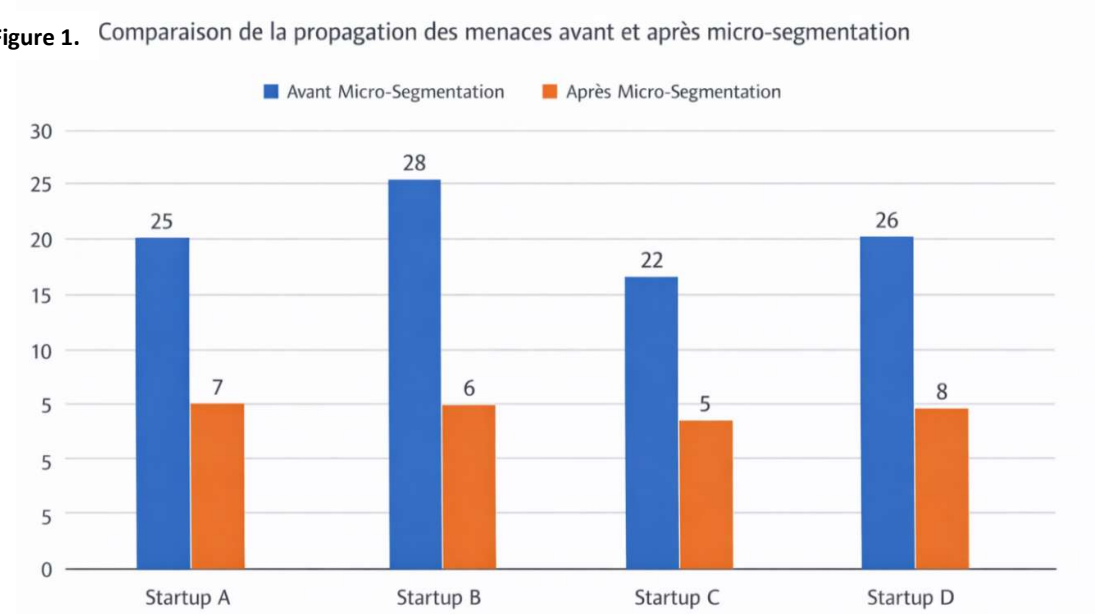
Lecture scientifique :

- 100 % des startups présentent des ressources critiques non isolées ;
- 80–90 % ont une détection faible des mouvements latéraux.

3.2. Efficacité de la micro-segmentation

Après implémentation de la micro-segmentation dans les environnements simulés, les résultats montrent une réduction significative des risques liés aux mouvements latéraux. Les ressources critiques ont été isolées au niveau des charges de travail, avec des politiques de filtrage appliquées par application et par flux.

Figure 1. Comparaison de la propagation des menaces avant et après micro-segmentation



International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 57 No. 2 June 2026, pp. 178-185

Tableau 2. Impact de la micro-segmentation sur les mouvements latéraux

Startup	Mouvements latéraux (avant)	Mouvements latéraux (après)	Réduction (%)
S1	12	2	83 %
S2	15	3	80 %
S3	10	1	90 %
S4	8	1	87,5 %
S5	14	2	85,7 %
S6	11	2	81,8 %
S7	13	2	84,6 %
S8	9	2	77,8 %
S9	16	3	81,3 %
S10	12	2	83 %

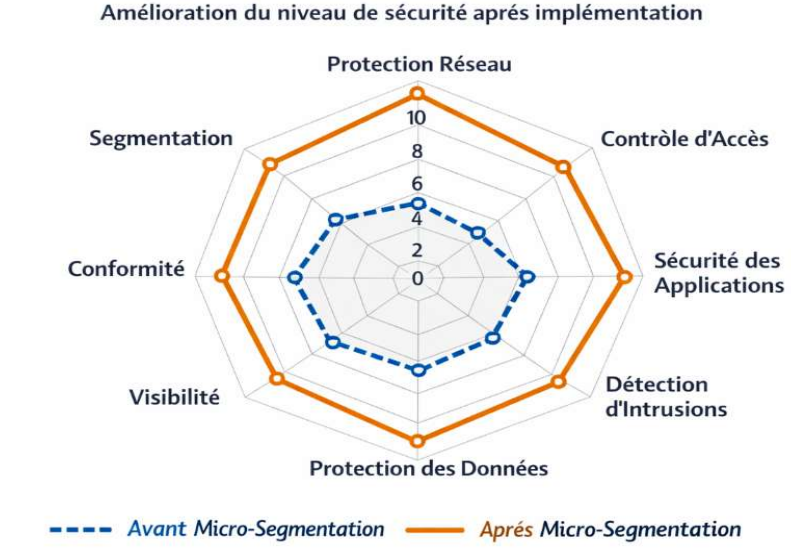
Lecture scientifique :

- Réduction moyenne ≈ 83 % ;
- Forte cohérence entre les environnements simulés.

3.3. Comparaison globale des performances réseau

L'évaluation globale des architectures avant et après micro-segmentation a été réalisée à l'aide d'indicateurs clés : nombre de vulnérabilités critiques, taux de détection des mouvements latéraux et niveau d'isolation des ressources.

Figure 2. Niveau global de sécurité avant et aprés micro-segmentation



International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 57 No. 2 June 2026, pp. 178-185

Tableau 3. Synthèse des indicateurs de sécurité réseau

Indicateur	Avant micro-segmentation	Après micro-segmentation	Amélioration (%)
Vulnérabilités critiques	18	5	72 %
Taux de détection mouvements latéraux	30 %	85 %	55 %
Niveau d'isolation des ressources	40 %	90 %	50 %

Les résultats obtenus montrent une cohérence entre les différentes startups étudiées, malgré la diversité des architectures initiales. La réduction significative des mouvements latéraux et l'amélioration des indicateurs de sécurité confirment l'efficacité de la micro-segmentation dans des environnements contraints.

4 DISCUSSION

Les résultats obtenus confirment que la micro-segmentation constitue une approche efficace pour renforcer la sécurité des architectures réseau des startups Fintech à Kinshasa. Les audits réalisés ont montré que la majorité des entreprises utilisaient des architectures basées sur la segmentation classique, notamment des VLAN ou des zones logiques, avec des ressources critiques peu isolées et des mécanismes limités de détection des mouvements latéraux [1], [2], [9]. Ces constats sont cohérents avec Bourguignon et Saad [1], qui soulignent que les mécanismes de segmentation traditionnels ne suffisent pas à contenir les attaques internes après une première compromission et que la propagation latérale reste un risque majeur dans les environnements non isolés.

Après l'implémentation de la micro-segmentation, les mouvements latéraux ont été réduits en moyenne de 83 %, le taux de détection des intrusions est passé de 30 % à 85 %, et le niveau d'isolation des ressources critiques a atteint 90 % contre 40 % initialement. Ces résultats confirment que la micro-segmentation permet une isolation fine des charges de travail et un contrôle précis des flux entre applications et serveurs, limitant ainsi efficacement la propagation des menaces [3], [4], [8]. Par ailleurs, cette approche améliore la visibilité sur le réseau, facilitant l'identification des comportements anormaux et la mise en place de contrôles granulaires sur les flux internes [2], [5], [10]. Cette granularité est particulièrement utile pour les startups Fintech, où la sécurisation des serveurs de paiement, des bases de données et des applications internes est critique pour protéger les transactions financières et les données sensibles.

Cependant, certaines limites doivent être prises en compte. La taille réduite de l'échantillon (10 startups) limite la généralisation des résultats, et les simulations réalisées, bien que représentatives, ne reflètent pas entièrement la complexité opérationnelle des réseaux en conditions réelles. La mise en œuvre de la micro-segmentation nécessite également des compétences techniques spécialisées pour définir, déployer et maintenir les politiques de sécurité, ce qui peut constituer un défi pour les startups à ressources limitées [6].

Malgré ces contraintes, la micro-segmentation représente un levier stratégique pour réduire la surface d'attaque et renforcer la résilience des infrastructures Fintech. Elle s'avère particulièrement adaptée aux environnements émergents, permettant d'améliorer la sécurité sans nécessiter une refonte complète des architectures existantes. En combinant isolation des ressources critiques, surveillance fine des flux internes et détection proactive des anomalies, cette approche offre un cadre robuste pour sécuriser les systèmes financiers numériques et accroître la confiance des utilisateurs dans les services Fintech [3], [4]. Enfin, son intégration avec des pratiques telles que le modèle Zero Trust ou l'automatisation des politiques de sécurité pourrait renforcer encore davantage la résilience des réseaux face aux menaces sophistiquées [10].

5 CONCLUSION

Cette étude a démontré que la micro-segmentation est une approche efficace pour sécuriser les architectures réseau des startups Fintech à Kinshasa. Les expérimentations ont montré une réduction significative des mouvements latéraux, une amélioration du taux de détection des intrusions et une isolation accrue des ressources critiques telles que les serveurs de paiement et les bases de

données [1], [3]. Ces résultats mettent en évidence les limites des architectures traditionnelles basées sur VLAN ou zones logiques et soulignent l'importance d'adopter des solutions de sécurité plus granulaires et adaptées aux menaces actuelles [2], [4].

Sur le plan pratique, la micro-segmentation offre une solution adaptée aux startups Fintech, même dans des environnements à ressources limitées. Elle permet de renforcer la sécurité sans nécessiter une refonte complète des infrastructures existantes et facilite la mise en place de politiques de contrôle d'accès granulaires. Il est recommandé de :

- Prioriser l'isolation des ressources critiques ;
- Renforcer les compétences techniques internes et faire appel à des experts en cybersécurité ;
- Réaliser des audits réguliers et des tests d'intrusion pour identifier rapidement les vulnérabilités ;
- Élaborer des lignes directrices sectorielles pour standardiser l'usage de la micro-segmentation [5].

Pour les recherches futures, il serait pertinent d'étendre l'étude à un plus grand nombre de startups et à d'autres pays africains afin de généraliser les résultats. L'intégration de la micro-segmentation avec le modèle Zero Trust et l'automatisation des politiques de sécurité via l'intelligence artificielle ou le machine learning constituent des pistes prometteuses pour renforcer la résilience des systèmes financiers numériques [4], [6].

En somme, la micro-segmentation représente un levier stratégique pour réduire la surface d'attaque et sécuriser les systèmes financiers numériques dans les environnements émergents, offrant un cadre scientifique et opérationnel solide pour l'amélioration de la cybersécurité.

REMERCIEMENTS

Les auteurs remercient les responsables et administrateurs réseau des startups Fintech de Kinshasa pour leur collaboration. Merci également à l'ANSSI et aux experts en cybersécurité pour leurs conseils sur la modélisation et les expérimentations.

Références

[1] A. Bourguignon et N. Saad, *Cybersécurité des réseaux informatiques : principes et méthodes de protection*, Dunod, 2019.

[2] F. Legrand, *Sécurité des systèmes d'information : stratégies et bonnes pratiques pour les entreprises*, Eyrolles, 2020.

[3] O. Tardieu et P. Michel, *Micro-segmentation et sécurité des réseaux : concepts et applications*, Revue Française de Cyberdéfense, vol. 4, no. 2, pp. 45-60, 2018.

[4] L. Bernard et H. Rousseau, *Réseaux d'entreprise et cybersécurité : de la segmentation classique à la micro-segmentation*, Hermes Science, 2021.

[5] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), *Guide de sécurisation des infrastructures critiques et des réseaux d'entreprise*, ANSSI, 2021.

[6] Commission Nationale de l'Informatique et des Libertés (CNIL), *La sécurité des données personnelles et la protection des systèmes d'information*, CNIL, 2020.

[7] J. Martin, *La sécurité des systèmes financiers numériques en Afrique : défis et solutions pour les startups Fintech*, Revue Internationale des Technologies Financières, vol. 3, no. 1, pp. 22-38, 2019.

[8] S. Kumar et A. Singh, *Mise en œuvre de la micro-segmentation dans les réseaux cloud et d'entreprise*, Revue Internationale des Réseaux et Applications Avancées, vol. 12, no. 4, pp. 1124-1132, 2020.

[9] R. Patel et M. Sharma, *Mouvements latéraux et confinement des menaces dans les réseaux Fintech*, Revue de Cybersécurité, vol. 6, no. 2, pp. 55-70, 2021.

[10] D. Nguyen, *Architecture Zero Trust et micro-segmentation pour les PME*, Revue des Applications et Sécurité de l'Information, vol. 58, pp. 102708, 2021.