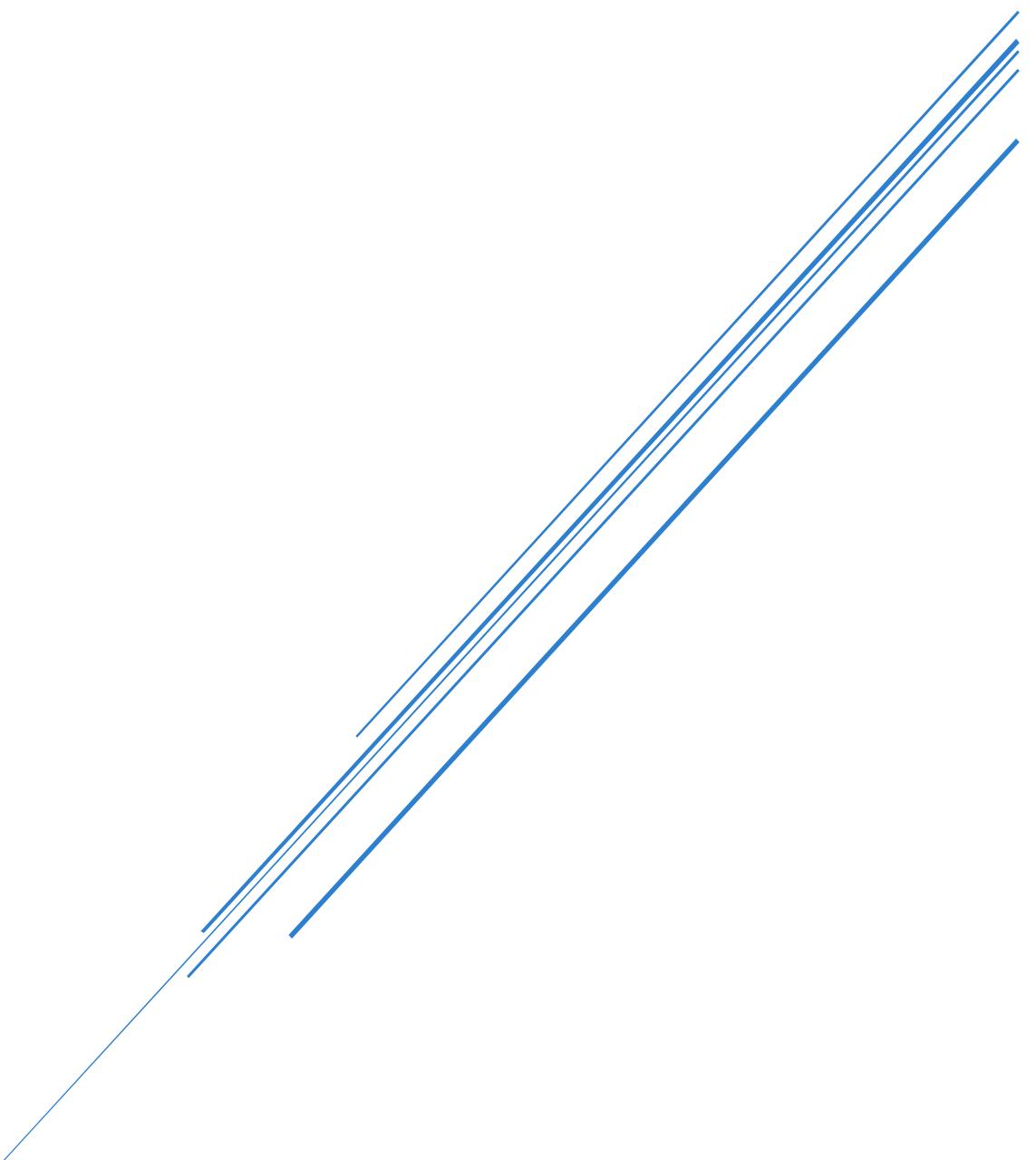


MISE EN PLACE D'UNE SOLUTION WIFI SECURISEE



Assumer
Antoine LETELLIER, Mahdi BOUDIA, Lucas ROMAIN

Sommaire

Introduction	2
1. <i>Inventaire des ressources numériques</i>	<i>2</i>
1.1 Equipement Réseau	2
1.2 Postes de Travail.....	2
1.3 Sécurité Informatique.....	2
2. <i>Planning de travail et répartition des tâches</i>	<i>3</i>
3. <i>Présentation de la norme IEEE802.11.....</i>	<i>4</i>
Qu'est-ce que IEEE 802.11 ?.....	4
Différence entre IEEE 802.11 et Wi-Fi.....	4
Évolution de la norme IEEE 802.11	4
Comparaison des normes :	5
Les différentes vitesses de transmissions :	6
4. <i>Les différents protocoles de sécurité wifi.....</i>	<i>7</i>
Transition de WPA à WPA2 :	7
Adoption de WPA2 dans les réseaux Wi-Fi :	8
Failles de sécurité et limites de WPA2 :	8
Wi-Fi Protected Access 3 (WPA3):.....	8
Nouvelles fonctionnalités de sécurité et améliorations dans WPA3 :	8
Considérations pour la migration et le déploiement de WPA3 :	9
Compatibilité des appareils avec WPA3 :	9
Adoption de WPA3 dans l'industrie :	9
Gestion des failles de sécurité et vulnérabilités dans WPA3 :	9
Avantages et limites du WEP :.....	9
Faiblesses de sécurité dans WEP par rapport aux protocoles plus récents :	10
Considérations pour migrer de WEP vers WPA, WPA2 ou WPA3 :	10
Niveaux de sécurité et normes de cryptage : WEP, WPA, WPA2 et WPA3 :	10
Perspectives des protocoles de sécurité sans fil :	11
Sécurité Wi-Fi : exploration des normes et types de cryptage :	11
Meilleures pratiques :	11
Différences entre les normes de chiffrement WPA, WPA2 et WPA3 :	12
Avantages et inconvénients des différents types de cryptage Wi-Fi :	12
Choisir la bonne norme de cryptage pour les réseaux domestiques et professionnels :	12
Mise en œuvre de protocoles de sécurité Wi-Fi pour une protection améliorée du réseau ;	13
Meilleures pratiques pour sécuriser les réseaux sans fil avec cryptage :	13
5. <i>Procédure d'installation de la borne et configuration de cellules wifi.....</i>	<i>14</i>
1. Configuration des paramètres réseaux pour la borne wifi	15
2. Création d'un point d'accès WI-FI	18
3. Création de VLAN	19
6. <i>Présentation du fonctionnement d'une solution RADIUS et certificats</i>	<i>22</i>
Qu'est-ce qu'une solution RADIUS ?.....	22
Le rôle des certificats dans une solution RADIUS :	23
Configuration d'une solution RADIUS avec certificats :	24
7. <i>Procédure d'installation et de configuration de cette solution sous Windows Serveur.....</i>	<i>25</i>
1. Configuration du service RADIUS	30



Introduction

L'objectif de cet inventaire est de recenser, ainsi que de documenter les ressources numériques présentes sur l'îlot informatique, et ce, afin de faciliter leur gestion, et leur maintenance. Cet îlot est composé de divers équipements réseau, postes de travail et dispositifs de sécurité.

1. Inventaire des ressources numériques

1.1 Équipement Réseau

Nom de l'équipement	Photographie	Modèle	Rôle	État
PointAcces-Cisco		Cisco WAP371	Point d'accès Wi-Fi	OK
Switch-Principal		Cisco 2960 Series	Switch Principal	OK
Routeur-Principal		Cisco 2901 Series	Routeur Principal	OK

1.2 Postes de Travail

Nom de l'équipement	Photographie	Modèle	Rôle	État
PC1		ThinkStation PC	Ordinateur de Test	OK
PC2		ThinkStation PC	Ordinateur de Test	OK

1.3 Sécurité Informatique

Nom de l'équipement	Photographie	Modèle	Rôle	État
Firewall-Netgate		Netgate SG-3100	Firewall Principal	OK



2. Planning de travail et répartition des tâches

Document	Lucas ROMAIN	Antoine LETELLIER	Mahdi BOUDIA	Les Semaines
Procédure RADIUS		X		Semaine 1 à 5
Présentation de la norme IEEE802.11		X	X	Semaine 3
Étude comparative des différents protocoles de sécurité wifi	X		X	Semaine 2
Présentation du fonctionnement d'une solution RADIUS et certificat	X		X	Semaine 1
Procédure de la borne wifi et configuration		X	X	Semaine 1 à 5



3. Présentation de la norme IEEE802.11

Qu'est-ce que IEEE 802.11 ?

IEEE 802.11 est un ensemble de normes définissant les protocoles pour les réseaux locaux sans fil (WLAN). Publiée initialement en 1997 par l'Institut des Ingénieurs Électriciens et Électroniciens (IEEE), cette norme est devenue la base des technologies Wi-Fi modernes. Elle établit les règles de transmission et de réception des données via des ondes radio, permettant une connectivité sans fil fiable et universelle.

Différence entre IEEE 802.11 et Wi-Fi

IEEE 802.11 est une spécification technique, tandis que le terme Wi-Fi est utilisé pour désigner des réseaux locaux sans fil conformes à cette norme.

- **IEEE 802.11** : Encadre les couches physiques et l'accès réseau dans un WLAN.
- **Wi-Fi** : Représente l'application pratique de la norme 802.11, souvent associé à un usage grand public.

Bien que d'autres protocoles pourraient théoriquement être utilisés pour les réseaux locaux sans fil, IEEE 802.11 est devenu le standard de facto, rendant les deux termes pratiquement interchangeables.

Évolution de la norme IEEE 802.11

Depuis sa première publication en 1997, la norme IEEE 802.11 a connu plusieurs évolutions marquantes. La première version, **802.11-1997**, offrait des débits maximums de 1 à 2 Mbps, ce qui, bien que révolutionnaire à l'époque, est aujourd'hui largement dépassé par les normes actuelles.

En 1999, la norme **802.11b** a introduit des débits atteignant 11 Mbps, permettant ainsi une adoption plus large des réseaux sans fil dans les foyers et les petites entreprises.



En 2003, la norme **802.11g** est arrivée, augmentant les débits à 54 Mbps, ce qui a permis une meilleure prise en charge des applications multimédia telles que la vidéo en streaming.

L'année 2009 a marqué un tournant avec l'introduction de **802.11n**, qui a multiplié les flux de données pour atteindre des débits théoriques allant jusqu'à 600 Mbps, offrant ainsi des performances largement améliorées pour les réseaux domestiques et professionnels.

En 2014, la norme **802.11ac** a été lancée, optimisant particulièrement le streaming vidéo et les transferts de données à des débits supérieurs à 1 Gbps, répondant ainsi aux exigences croissantes des utilisateurs.

La norme **802.11ax**, également connue sous le nom de **Wi-Fi 6**, introduite en 2019, a été conçue pour améliorer l'efficacité des réseaux dans des environnements denses, comme les stades ou les immeubles de bureaux, en maximisant la capacité et la gestion des appareils connectés simultanément.

Enfin, la norme **802.11be**, prévue pour 2024, devrait permettre des débits impressionnantes de 45,1 Gbps, répondant aux besoins des applications émergentes telles que la réalité augmentée, la réalité virtuelle et l'Internet des objets (IoT), positionnant ainsi les réseaux sans fil pour les défis technologiques futurs.

Comparaison des normes :

	IEEE 802.11n (Wi-Fi 4)	IEEE 802.11ac (Wi-Fi 5)	IEEE 802.11ax (Wi-Fi 6/6E)
Taux de transfert théorique	300 Mbit/s	867 Mbit/s	1 200 Mbit/s
Taux de transfert maximal	600 Mbit/s	6 936 Mbit/s	9 608 Mbit/s
Portée	Jusqu'à 100 m	Jusqu'à 50 m	Jusqu'à 50 m
Gamme de fréquences	2,4 GHz + 5 GHz	5 GHz	2,4 GHz + 5 GHz + 6 GHz
Unités d'émission et de réception	4 x 4	8 x 8	8 x 8
Antennes	MIMO	MU-MIMO	MU-MIMO
Largeur de canal	Jusqu'à 40 MHz	Jusqu'à 160 MHz	Jusqu'à 160 MHz
Méthode de modulation	64 QAM	256 QAM	1024 QAM



Les différentes vitesses de transmissions :

	IEEE 802.11 (Wi-Fi 1)	IEEE 802.11n (Wi- Fi 4)	IEEE 802.11ac (Wi- Fi 5)	IEEE 802.11ax (Wi-Fi 6/6E)
Fréquence	2,4 GHz	2,4 GHz + 5 GHz	5 GHz	2,4 GHz + 5 GHz + 6 GHz
Flux	1	1, 2, 3, 4	1, 2, 3, 4, 5, 6, 7, 8	1, 2, 3, 4, 5, 6, 7, 8
Pour une largeur de canal de 20 MHz	Jusqu'à 2 Mbit/s	Jusqu'à 300 Mbit/s	-	Jusqu'à 574 Mbit/s
Pour une largeur de canal de 40 MHz	-	Jusqu'à 600 Mbit/s	-	Jusqu'à 1 144 Mbit/s
Pour une largeur de canal de 80 MHz	-	-	Jusqu'à 3 400 Mbit/s	Jusqu'à 4 804 Mbit/s
Pour une largeur de canal de 160 MHz	-	-	Jusqu'à 6 936 Mbit/s	Jusqu'à 9 608 Mbit/s

Notons qu'elles ne sont que “théorique”, les vitesses atteintes dépendent de plusieurs facteur comme les autres réseaux, de grandes distances, des murs et plafonds épais ou d'autres obstacles peuvent ralentir sensiblement la vitesse de transmission. La transmission selon la norme 802.11 utilise un canal partagé qui est utilisé simultanément par plusieurs participants. Cela a également un impact sur la vitesse réelle. Ce qui explique pourquoi les vitesses théoriques ne sont généralement pas atteintes.



4. Les différents protocoles de sécurité wifi

Wi-Fi Protected Access 2 (WPA2) est un protocole de sécurité et un programme de certification développés par la Wi-Fi Alliance pour sécuriser les réseaux informatiques sans fil. En tant que mise à niveau de son prédecesseur, Wi-Fi Protected Access (WPA), WPA2 fournit des mesures de sécurité robustes qui corrigent les vulnérabilités et les lacunes du WPA.

Fonctionnalités de sécurité et normes de cryptage de WPA2 :

WPA2 intègre des fonctionnalités de sécurité avancées et des normes de cryptage conçues pour renforcer la protection des réseaux sans fil. Il repose sur l'Advanced Encryption Standard (AES), un algorithme cryptographique approuvé par les autorités gouvernementales, offrant un niveau de sécurité supérieur et une robustesse accrue par rapport au Temporal Key Integrity Protocol (TKIP) utilisé dans WPA. De plus, WPA2 propose un mode de clé pré-partagée (PSK), appelé WPA2-PSK, qui simplifie la configuration pour les utilisateurs domestiques tout en maintenant un haut niveau de sécurité.

Avantages	Désavantages
Cryptage plus robuste (AES)	Plus de puissance de traitement est nécessaire
Contrôles améliorés de l'intégrité des données	Problèmes de compatibilité avec les anciens appareils
Meilleure protection contre les attaques	Configuration complexe pour les grands réseaux

Transition de WPA à WPA2 :

Passer de WPA à WPA2 nécessite de mettre à jour le firmware ou le logiciel de votre routeur et des appareils connectés afin qu'ils prennent en charge ce standard. Ce processus est souvent simple pour les appareils récents, mais peut poser un problème avec des équipements plus anciens ne prenant pas nativement en charge WPA2. Avant de procéder à la transition, il est essentiel de vérifier que tous les appareils du réseau sont compatibles pour éviter les interruptions de connectivité.



Adoption de WPA2 dans les réseaux Wi-Fi :

L'intégration de WPA2 dans un réseau sans fil exige de configurer correctement les paramètres du routeur et des appareils connectés. Cela inclut la sélection de WPA2 comme mode de sécurité, le choix d'AES comme méthode de chiffrement, et la création d'un mot de passe unique et robuste. Pour une sécurité renforcée, l'activation de WPA2-Enterprise est recommandée, car elle permet une authentification des utilisateurs plus avancée.

Failles de sécurité et limites de WPA2 :

Bien que WPA2 offre des niveaux de sécurité élevés, il n'est pas exempt de vulnérabilités. L'attaque par réinstallation de clé (KRACK) est l'une des failles les plus connues, permettant potentiellement à un attaquant situé à proximité d'intercepter et de manipuler les données sur un réseau protégé par WPA2. Cependant, cette vulnérabilité peut être minimisée grâce à une configuration réseau adéquate et à des mises à jour régulières des logiciels concernés.

Wi-Fi Protected Access 3 (WPA3):

WPA3 est la dernière évolution du protocole de sécurité Wi-Fi, introduite par la Wi-Fi Alliance pour répondre aux besoins croissants des réseaux sans fil modernes. Il propose des améliorations majeures par rapport à WPA2, avec des mesures de sécurité renforcées adaptées aux exigences actuelles.

Nouvelles fonctionnalités de sécurité et améliorations dans WPA3 :

WPA3 se distingue par des avancées majeures en matière de sécurité. Parmi celles-ci, l'authentification simultanée des égaux (SAE) remplace la méthode de clé pré-partagée (PSK) de WPA2, offrant une résistance accrue aux attaques par dictionnaire hors ligne. En outre, WPA3 introduit une suite de sécurité 192 bits, conforme à la suite CNSA (Commercial National Security Algorithm), qui assure une protection avancée pour les réseaux traitant des données hautement sensibles. Ces innovations visent à renforcer la confidentialité et la résilience des connexions sans fil, en rendant les réseaux plus robustes face aux menaces modernes.



Considérations pour la migration et le déploiement de WPA3 :

Passer de WPA2 à WPA3 nécessite une planification soignée. Bien que WPA3 soit rétro compatible avec WPA2, de nombreux appareils existants ne prennent pas en charge ce protocole de manière native. Certaines infrastructures nécessiteront des mises à jour de micrologiciel, tandis que d'autres pourraient exiger un remplacement matériel. L'ampleur et le coût de cette transition dépendent principalement de l'âge et des capacités des équipements réseau actuels.

Compatibilité des appareils avec WPA3 :

La prise en charge de WPA3 varie selon les appareils. Si la plupart des équipements récents sont conçus pour fonctionner avec WPA3, de nombreux appareils plus anciens ne pourront y accéder qu'après des mises à jour de micrologiciel, ou pas du tout. Avant de migrer vers WPA3, il est crucial d'évaluer les capacités de tous les appareils sur le réseau et d'identifier les éventuelles mises à niveau matérielles nécessaires.

Adoption de WPA3 dans l'industrie :

L'adoption de WPA3 se développe rapidement, avec un nombre croissant de fabricants intégrant ce protocole dans leurs produits récents. Toutefois, la transition complète de WPA2 vers WPA3 reste progressive en raison des coûts et des défis techniques liés à la modernisation des infrastructures et des équipements existants.

Gestion des failles de sécurité et vulnérabilités dans WPA3 :

Bien que WPA3 améliore significativement la sécurité, il présente encore des vulnérabilités. Par exemple, des faiblesses ont été identifiées dans la procédure de prise de contact SAE, qui pourraient permettre à des attaquants de récupérer des informations de mot de passe. Ces risques peuvent toutefois être minimisés grâce à une configuration adéquate et à des mises à jour logicielles régulières. La Wi-Fi Alliance continue de surveiller et d'améliorer la sécurité de WPA3 pour atténuer ces vulnérabilités et protéger les réseaux contre les menaces émergentes.

Avantages et limites du WEP :

Le WEP (Wired Equivalent Privacy) était l'un des premiers protocoles conçus pour sécuriser les réseaux sans fil, offrant une protection de base contre les intrusions. Son



principal avantage réside dans sa compatibilité avec une vaste gamme d'appareils plus anciens. Cependant, les limites de WEP sont significatives : son algorithme de chiffrement est vulnérable à diverses cyberattaques, et il ne dispose pas de mécanismes d'échange dynamique de clés, ce qui le rend obsolète par rapport aux standards modernes.

Faiblesses de sécurité dans WEP par rapport aux protocoles plus récents :

En comparaison avec WPA, WPA2, et WPA3, les failles du WEP sont flagrantes. Les protocoles ultérieurs, tels que WPA et WPA2, utilisent des méthodes de cryptage bien plus robustes comme le TKIP (Temporal Key Integrity Protocol) et l'AES (Advanced Encryption Standard). Ces protocoles introduisent également des mécanismes d'échange de clés dynamiques et des processus d'authentification des utilisateurs, offrant une sécurité réseau bien supérieure. WPA3 va encore plus loin en intégrant des améliorations comme l'authentification simultanée des égaux (SAE).

Considérations pour migrer de WEP vers WPA, WPA2 ou WPA3 :

La migration du WEP vers un protocole plus sécurisé nécessite une évaluation approfondie. L'âge et les capacités des appareils réseau sont essentiels : certains équipements plus anciens ne supportent pas les protocoles modernes et peuvent nécessiter des mises à jour du micrologiciel ou des remplacements matériels. En outre, il est important de tenir compte de l'impact des méthodes de cryptage avancées sur les performances du réseau, car elles exigent une puissance de traitement plus élevée. Planifier soigneusement cette transition permettra de renforcer la sécurité tout en minimisant les perturbations.

Niveaux de sécurité et normes de cryptage : WEP, WPA, WPA2 et WPA3 :

Les niveaux de sécurité et les normes de cryptage ont évolué pour répondre aux menaces croissantes sur les réseaux sans fil :

- **WEP (Wired Equivalent Privacy)** : Offrant une sécurité minimale, il utilise un algorithme de chiffrement vulnérable, rendant les réseaux faciles à compromettre.
- **WPA (Wi-Fi Protected Access)** : A introduit le **TKIP (Temporal Key Integrity Protocol)** pour pallier les failles de WEP. Bien qu'une amélioration, il reste moins sécurisé comparé aux normes modernes.



- **WPA2** : A adopté l'**AES (Advanced Encryption Standard)**, un standard de cryptage beaucoup plus robuste, et a remplacé le TKIP pour améliorer la sécurité.
- **WPA3** : Intègre des fonctionnalités avancées comme l'**authentification simultanée des égaux (SAE)**, offrant une protection renforcée contre les attaques par dictionnaire et une meilleure confidentialité sur les réseaux ouverts.

Perspectives des protocoles de sécurité sans fil :

Avec l'évolution constante des réseaux sans fil, les futurs protocoles de sécurité devront anticiper des cybermenaces de plus en plus complexes. Les priorités incluront :

1. **Cryptographie renforcée** : Adoption de méthodes plus avancées, telles que la cryptographie quantique ou post-quantique.
2. **Authentification améliorée** : Développement de processus plus fiables, éventuellement intégrant des biométries ou des identités numériques décentralisées.
3. **Adaptabilité et résilience** : Protocole capable de détecter et de répondre en temps réel aux intrusions et vulnérabilités.

L'accent sera également mis sur la compatibilité avec les appareils connectés dans un monde toujours plus interconnecté.

Sécurité Wi-Fi : exploration des normes et types de cryptage :

La sécurité Wi-Fi repose sur la mise en œuvre de normes adaptées aux besoins des réseaux :

- **Analyse des normes** : WEP, WPA, WPA2 et WPA3 diffèrent par leur approche du chiffrement et de l'authentification.
- **Choix adapté** : WPA2 est aujourd'hui un minimum pour les réseaux privés ; WPA3 est recommandé pour des besoins avancés.
- **Mise en œuvre** : Configurer les paramètres de cryptage, définir des mots de passe robustes, et maintenir des mises à jour régulières.

Meilleures pratiques :

- Utilisez **AES** et privilégiez **WPA3**.
- Désactivez les anciens protocoles comme **WEP** ou **WPA**.



- Surveillez le réseau pour détecter d'éventuelles intrusions.

La sécurité des réseaux Wi-Fi est un processus continu, nécessitant des mises à jour régulières et une adaptation proactive aux nouvelles menaces.

Differences entre les normes de chiffrement WPA, WPA2 et WPA3 :

Fonctionnalités	WPA	WPA2	WPA3
Méthode de chiffrement	TKIP	AES	AES et SAE
Gestion des clés	PSK et EAP	PSK et EAP	PSK, EAP et SAE
Compatibilité	Appareils plus anciens	Appareils modernes	Appareils plus récents
Niveau de sécurité	Modérée	Haute	Très haut

Avantages et inconvénients des différents types de cryptage Wi-Fi :

Type de chiffrement	Avantages	Inconvénients
WPA	Compatible avec les appareils plus anciens, sécurité améliorée via WEP	Moins sécurisé que WPA2 et WPA3, sensible aux attaques
WPA2	Cryptage fort (AES), largement compatible	Nécessite plus de puissance de traitement, problèmes de compatibilité potentiels avec les appareils plus anciens
WPA3	Fonctionnalités de sécurité améliorées, résistantes aux attaques par dictionnaire hors ligne	Nécessite un matériel moderne, pas encore aussi largement adopté

Choisir la bonne norme de cryptage pour les réseaux domestiques et professionnels :

Le choix de la norme de cryptage dépend des besoins spécifiques du réseau :

- **Pour les réseaux domestiques :** WPA2 ou WPA3 sont largement suffisants. WPA2 offre une sécurité solide, tandis que WPA3 ajoute des fonctionnalités avancées telles que l'authentification simultanée des égaux (SAE), idéale pour les réseaux modernes.



- **Pour les réseaux professionnels** : Les entreprises traitant des données sensibles devraient opter pour WPA3, qui offre des protections renforcées adaptées aux environnements exigeants, notamment grâce à son mode WPA3-Enterprise.

Mise en œuvre de protocoles de sécurité Wi-Fi pour une protection améliorée du réseau :

Pour garantir une protection optimale :

1. **Configurer la norme choisie** : Sélectionnez WPA2 ou WPA3 comme protocole de sécurité dans les paramètres du routeur.
2. **Définir un mot de passe robuste** : Utilisez un mot de passe complexe, unique et difficile à deviner.
3. **Mettre à jour régulièrement le micrologiciel** : Les mises à jour corrigent les vulnérabilités et renforcent la sécurité.
4. **Activer des fonctionnalités avancées** : Lorsque possible, activez des options comme le filtrage d'adresses MAC ou le mode réseau invité.

Meilleures pratiques pour sécuriser les réseaux sans fil avec cryptage :

Pour aller au-delà du choix du cryptage, mettez en œuvre ces bonnes pratiques :

- **Utilisez des mots de passe uniques et complexes** : Mélangez majuscules, minuscules, chiffres et symboles.
- **Activez un pare-feu réseau** : Il offre une couche supplémentaire de protection contre les attaques.
- **Désactivez les fonctionnalités inutiles** : Supprimez la gestion à distance du routeur si elle n'est pas indispensable.
- **Surveillez l'activité réseau** : Identifiez les appareils connectés et détectez toute intrusion potentielle.
- **Créez un réseau invité** : Séparez les connexions des visiteurs pour protéger les données critiques dans les environnements professionnels.

En combinant des protocoles de cryptage avancés avec des mesures préventives solides, vous pouvez considérablement renforcer la sécurité de vos réseaux sans fil.



5. Procédure d'installation de la borne et configuration de cellules wifi.

Pour bien configurer votre borne wifi, avec un stylo ou avec un objet fin veuillez appuyer sur le bouton « **RESET** » pendant 10 secondes

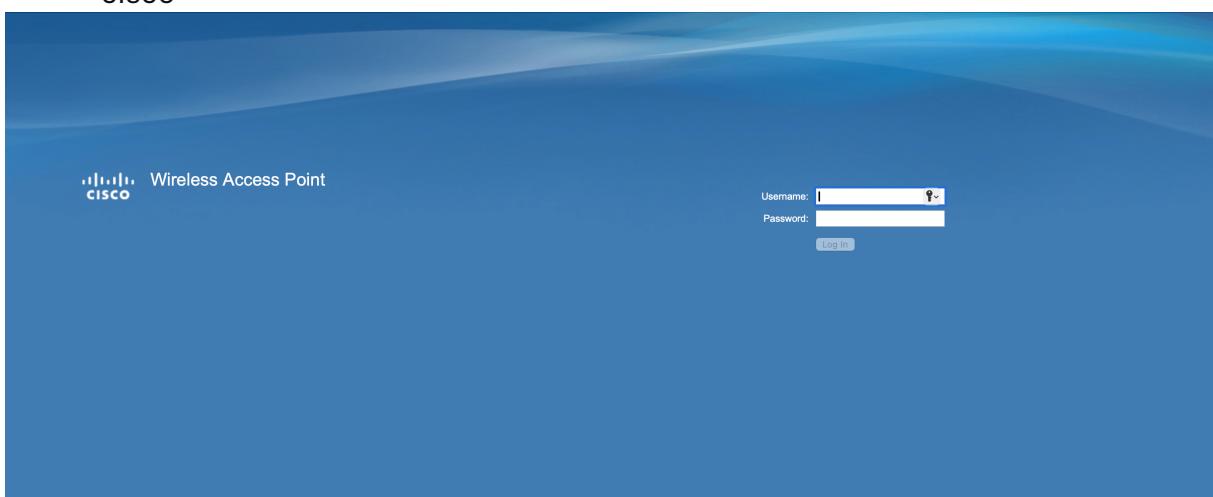


L'accès au point Wi-Fi redémarrera pendant environ une minute avant de se réinitialiser avec sa configuration par défaut.

Ensuite, sur votre serveur Active Directory, ouvrez le gestionnaire DHCP et localisez la plage d'adresses IP correspondant au VLAN pour identifier l'IP attribuée à l'équipement Wi-Fi. Assurez-vous également que le port du switch est configuré en mode accès (Access). Dans cet exemple, l'interface de gestion du point d'accès est accessible via : <https://172.16.0.21>

Les infos de connexions par default sont :

- cisco
- cisco



Une petite fenêtre de configuration rapide va se lancer, veuillez bien « Cancel » pour le faire manuellement.



Puis après veuillez changer le mot de passe afin d'avoir une sécurité robuste pour votre borne wifi.

1. Configuration des paramètres réseaux pour la borne wifi

Veuillez cliquer sur « **LAN** » puis veuillez cliquer sur « **VLAN And IPv4 Address** » pour renseigner votre IP correspondant au schéma de votre infrastructure.



Veuillez renseigner votre management VLAN ID. Pour ma part cela sera le VLAN 100 afin de maintenir l'accès après la modification de la Configuration du matériel réseau.

Veuillez renseigner dans IPv4 Settings en Static IP votre IP.

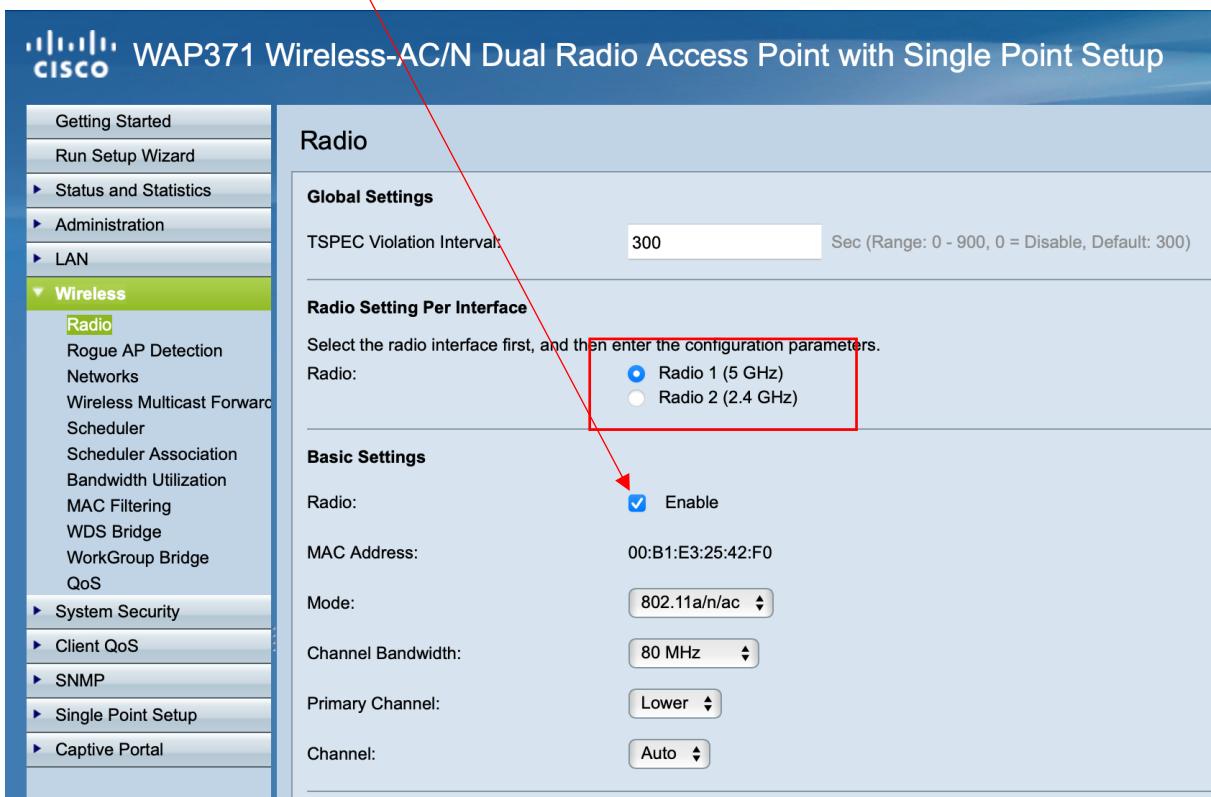
The screenshot shows the Cisco WAP371 configuration interface. The left sidebar has a 'LAN' section selected, which includes 'VLAN and IPv4 Address'. The main area shows 'Global Settings' with MAC Address (00:B1:E3:25:42:F0), Untagged VLAN (Enable), Untagged VLAN ID (1), and Management VLAN ID (100). The 'IPv4 Settings' section is highlighted with a red box. It shows Connection Type (Static IP selected), Static IP Address (172.16.0.10), Subnet Mask (255.255.255.0), Default Gateway (172.16.0.254), and Domain Name Servers (172.16.0.1 and 8.8.8.8). Below this is the 'DHCP Auto Configuration Settings' section, which is currently disabled. The bottom status log indicates 'Auto Configuration stopped: TFTP server and configuration file name not available.' A 'Save' button is at the bottom.



Veuillez cliquer dans « Wireless » puis dans « Radio » pour configurer pour activer les bandes de fréquences wifi 2.4 GHz et 5 GHz.



Veuillez cocher sur « Enable »



2. Création d'un point d'accès WI-FI

Nous allons configurer un point d'accès destiné à garantir une sécurité optimale pour les réseaux sans fil dans un environnement professionnel, en intégrant un serveur RADIUS.

Accédez à l'onglet « **System Security** », puis sélectionnez « **Radius Server** ».

The screenshot shows the device's configuration interface with a sidebar and a main content area.

Navigation Sidebar:

- Getting Started
- Run Setup Wizard
- ▶ Status and Statistics
- ▶ Administration
- ▶ LAN
- ▶ Wireless
- ▼ System Security
- RADIUS Server

The "System Security" and "RADIUS Server" items are highlighted with a red border. The "RADIUS Server" item is also highlighted with a green background.

Main Content Area - RADIUS Server Page:

Server IP Address Type: IPv4 IPv6

Server IP Address-1: 172.16.0.1 (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1 - 64 Characters)

Key-2: (Range: 1 - 64 Characters)

Key-3: (Range: 1 - 64 Characters)

Key-4: (Range: 1 - 64 Characters)

RADIUS Accounting: Enable

Buttons:

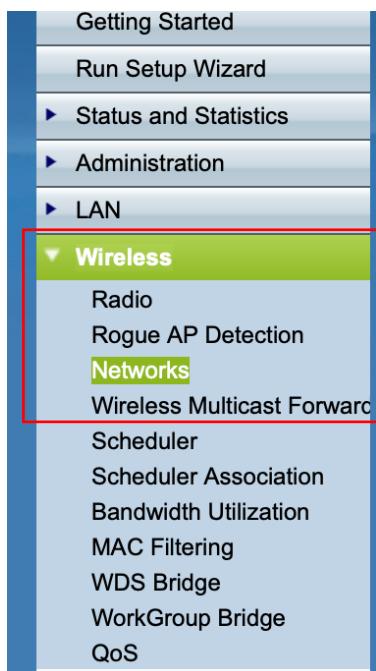
- Save



3. Création de VLAN

Pour configurer les VLANs **Direction**, **Compta** et **Admin**, procédez comme suit :

Accédez à l'onglet « **Wireless** », puis sélectionnez « **Network** ».



Cliquez sur le bouton « **Add** » pour ajouter un nouveau VLAN.

Configurez chaque VLAN en attribuant les noms et paramètres appropriés.

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)									
	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer
	0	<input checked="" type="checkbox"/>	1	ADMIN	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
	1	<input checked="" type="checkbox"/>	10	ALM-Direction	<input checked="" type="checkbox"/>	WPA Enterprise	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
	2	<input checked="" type="checkbox"/>	10	ALM-Business	<input checked="" type="checkbox"/>	WPA Enterprise	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
	3	<input checked="" type="checkbox"/>	30	ALM-Compta	<input checked="" type="checkbox"/>	WPA Enterprise	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
	4	<input checked="" type="checkbox"/>	40	ALM-RH	<input checked="" type="checkbox"/>	WPA Enterprise	Disabled	<input type="checkbox"/>	<input type="checkbox"/>

Add **Edit** **Delete**

Veuillez cocher la case pour configurer votre réseau invité ou dédié au VLAN. Puis cliquer sur « **Édit** »

Virtual Access Points (SSIDs)

	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer
	4	<input checked="" type="checkbox"/>	40	ALM-RH	<input checked="" type="checkbox"/>	WPA Enterprise	Disabled	<input type="checkbox"/>	<input type="checkbox"/>

Show Details

Add **Edit** **Delete**



Mettre le vlan dédié. Pour ma part c'est « **50** ».

A screenshot of a network configuration interface. At the top, there are buttons for 'Add', 'Edit', and 'Delete'. Below that, a table header row shows columns for VLAN ID (set to 5), Priority (set to 50), and other settings. The main body of the table is empty.

Mettre un nom. Pour ma cela va être « **ALM-Formation** »

A screenshot of a network configuration interface. The VLAN ID is set to 50 and the name is 'ALM-Formation'. The status is set to 'Disabled'.

Veuillez Mettre le « **WPA Entreprise** » pour pourvoir mettre un identifiant et un mot de passe d'un utilisateur AD qui correspond au groupe.

A screenshot of a network configuration interface. The VLAN ID is set to 50 and the name is 'ALM-Formation'. The WPA mode dropdown is open, showing options: 'None', 'WPA Personal', and 'WPA Enterprise'. The 'WPA Enterprise' option is highlighted.

Veuillez décocher « **Use global RADIUS server settings** » pour pouvoir configurer manuellement.

Mettre l'IP du serveur RADIUS puis rentrer le mot de passe secret configurer pour RADIUS

Veuillez cocher « **Enable RADIUS Accounting** »

Puis cliquer sur « **Add** »

A screenshot of a detailed RADIUS configuration form. The 'WPA Versions' section includes checkboxes for 'WPA-TKIP', 'WPA2-AES', and 'Enable pre-authentication'. A checkbox for 'Use global RADIUS server settings' is unchecked and highlighted with a red box. The 'Server IP Address Type' section has a radio button selected for 'IPv4'. The 'Server IP Address-1' field contains '172.16.0.1'. The 'Key' section contains four fields labeled 'Key-1' through 'Key-4', each with a placeholder '*****'. A checkbox for 'Enable RADIUS Accounting' is checked. At the bottom left, a red box highlights the 'Add' button.

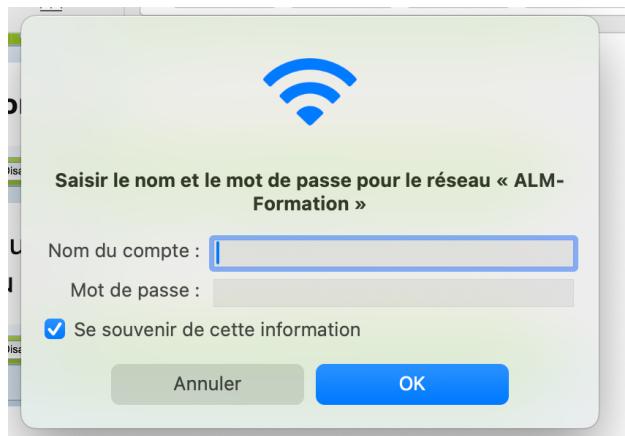


Veuillez mettre vos identifiants de connexion d'un utilisateur AD.

Pour nous nos infos de connexions sont :

User : première lettre du prénom + nom de famille en entier

MDP : mot de passe attribué



6. Présentation du fonctionnement d'une solution RADIUS et certificats

Qu'est-ce qu'une solution RADIUS ?

RADIUS (Remote Authentication Dial-In User Service) est un protocole utilisé pour gérer l'authentification, l'autorisation et la traçabilité des utilisateurs qui se connectent à un réseau, comme le Wi-Fi d'une entreprise.

1. **Authentification** : Vérifie l'identité de l'utilisateur (nom d'utilisateur/mot de passe ou certificat).
2. **Autorisation** : Vérifie si l'utilisateur a le droit d'accéder au réseau ou à un service spécifique.
3. **Traçabilité** : Garde des logs (historique) de qui s'est connecté et quand.

Comment ça marche ?

1. **L'utilisateur se connecte** : Par exemple, à un réseau Wi-Fi protégé.
2. **Le point d'accès (ou contrôleur Wi-Fi)** :
 - Transmet les informations de connexion (nom d'utilisateur/mot de passe ou certificat) au serveur RADIUS.
3. **Le serveur RADIUS** :
 - Vérifie les informations reçues en les comparant à une base de données d'utilisateurs (localement ou sur un Active Directory).
4. **Réponse du serveur RADIUS** :
 - Si les informations sont correctes, il renvoie un "**Accès autorisé**".
 - Sinon, l'accès est refusé.



Le rôle des certificats dans une solution RADIUS :

Les certificats remplacent les noms d'utilisateur et mots de passe pour rendre l'authentification plus sécurisée.

1. Certificat ?

- Un certificat est une sorte de carte d'identité numérique, délivrée par une autorité de certification (CA, Certificate Authority).
- Il contient des informations comme le nom de l'utilisateur ou de l'appareil et est signé pour garantir qu'il est valide.

2. Pourquoi les utiliser avec RADIUS ?

- **Sécurité renforcée** : Les mots de passe peuvent être piratés, mais un certificat est plus difficile à compromettre.
- **Facilité pour l'utilisateur** : Une fois configuré, l'utilisateur n'a pas besoin de saisir de mot de passe.

3. Comment ça fonctionne avec RADIUS ?

- Avant de se connecter, chaque utilisateur ou appareil doit avoir un certificat installé.
- Lorsqu'un utilisateur essaie de se connecter, le serveur RADIUS vérifie si le certificat est :
 - Valide (pas expiré, émis par une autorité de confiance).
 - Associé à un utilisateur autorisé.



Configuration d'une solution RADIUS avec certificats :

1. Serveur RADIUS :

- Par exemple : FreeRADIUS (open source) ou Microsoft NPS (Network Policy Server).
- Connecté à une base de données d'utilisateurs (LDAP, Active Directory, etc.).

2. Autorité de certification (CA) :

- Installe une CA pour générer et signer les certificats (par exemple, Active Directory Certificate Services sous Windows ou OpenSSL pour Linux).

3. Distribution des certificats :

- Chaque utilisateur ou appareil reçoit un certificat signé par la CA.
- Les appareils doivent avoir confiance en cette CA (certificat racine installé).

4. Configuration des points d'accès réseau :

- Les points d'accès Wi-Fi doivent être configurés pour rediriger les connexions vers le serveur RADIUS.

Avantages et limites :

Avantages :

- Sécurité accrue grâce aux certificats.
- Gestion centralisée des accès.
- Compatible avec beaucoup de matériel réseau.

Limites :

- Complexité initiale pour mettre en place (surtout pour les certificats).
- Nécessite une bonne gestion des certificats (renouvellements, révocations).

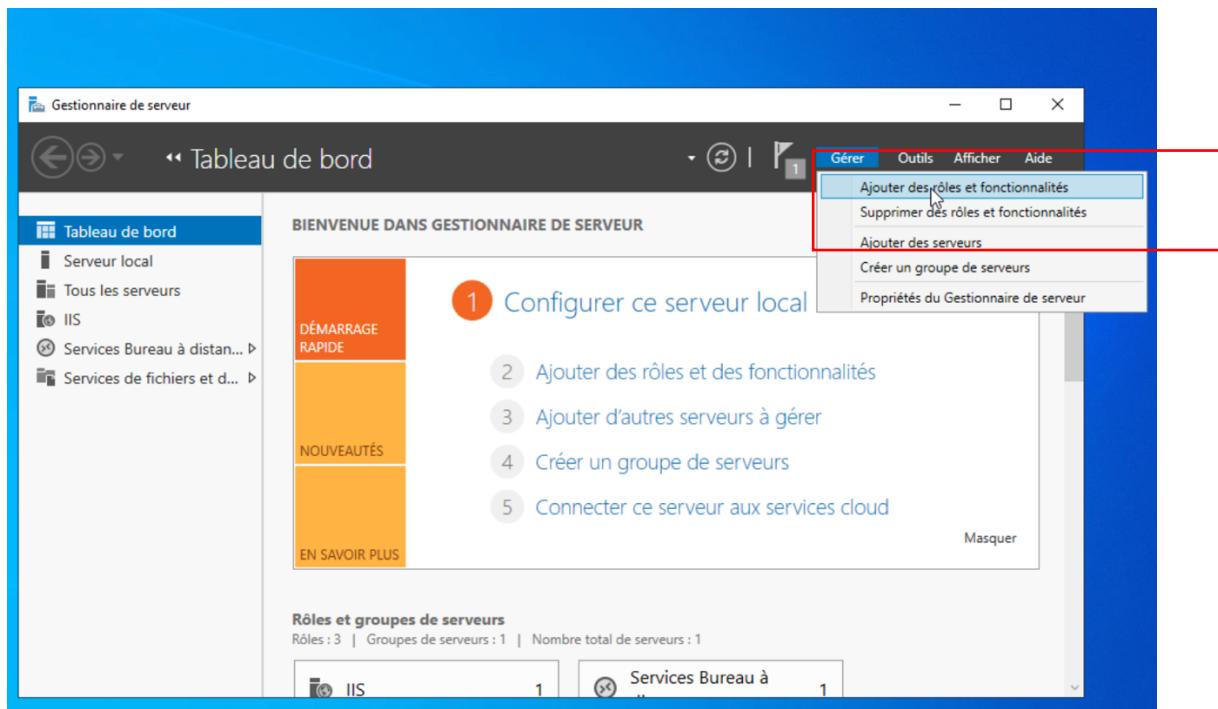


7. Procédure d'installation et de configuration de cette solution sous Windows Serveur

Veuillez ajouter un service NPS.

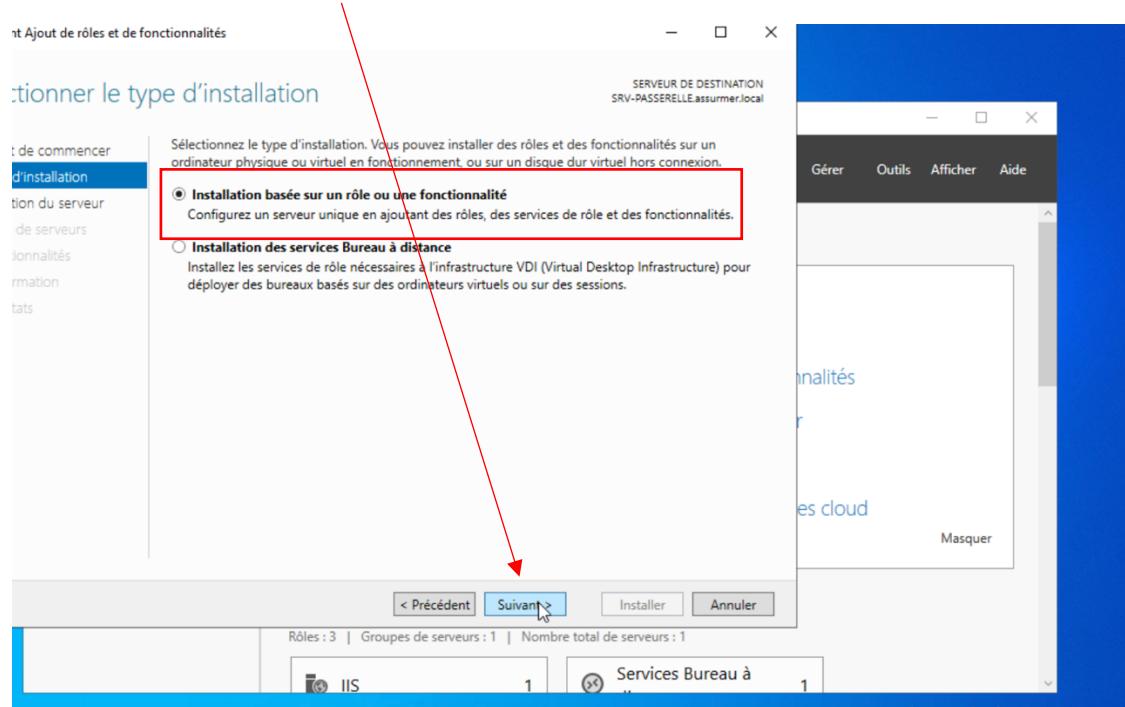
Le service NPS (Network Policy Server) est un rôle Windows qui permet de centraliser l'authentification, l'autorisation et la gestion des stratégies réseau via des protocoles comme RADIUS.

Cliquer sur « Outils » puis sur « Ajouter des rôles et fonctionnalités »



Veuillez cocher « **Installation basée sur un rôle ou une fonctionnalité** »

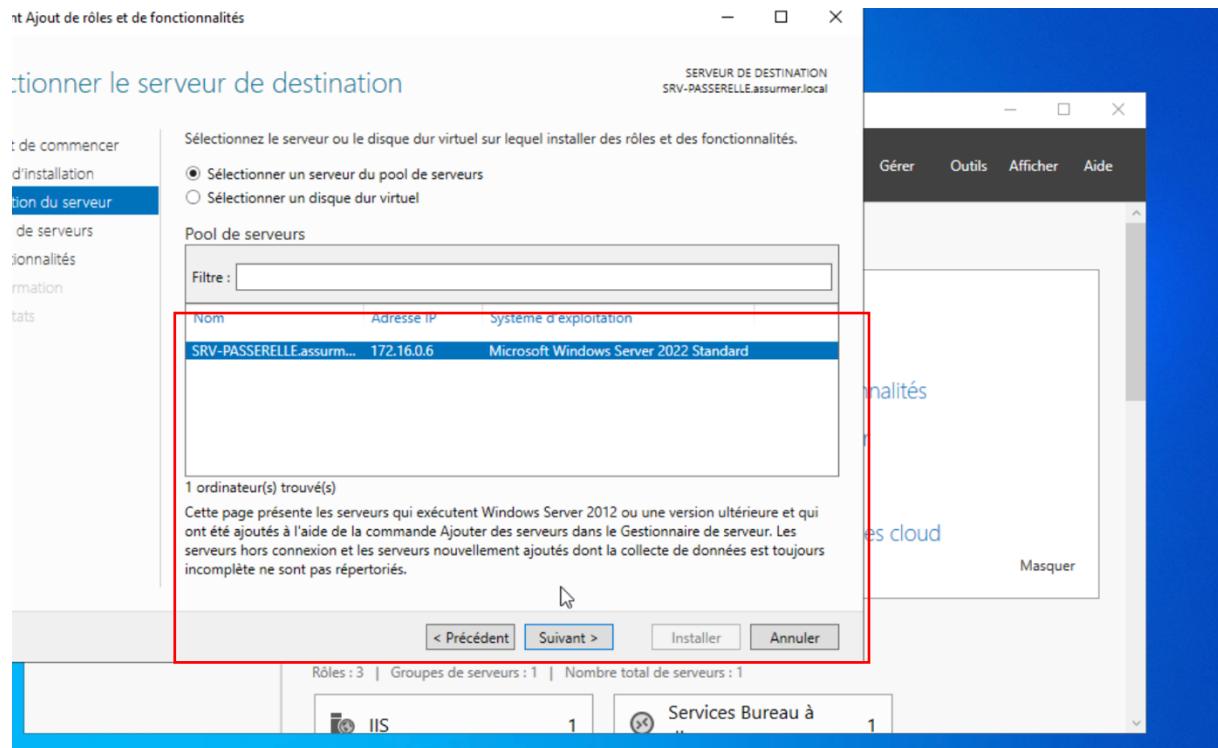
Puis cliquer sur « **Suivant** »



Choisir le serveur où vous voulez l'installer. Pour ma part cela sera L'AD sur 172.16.0.1

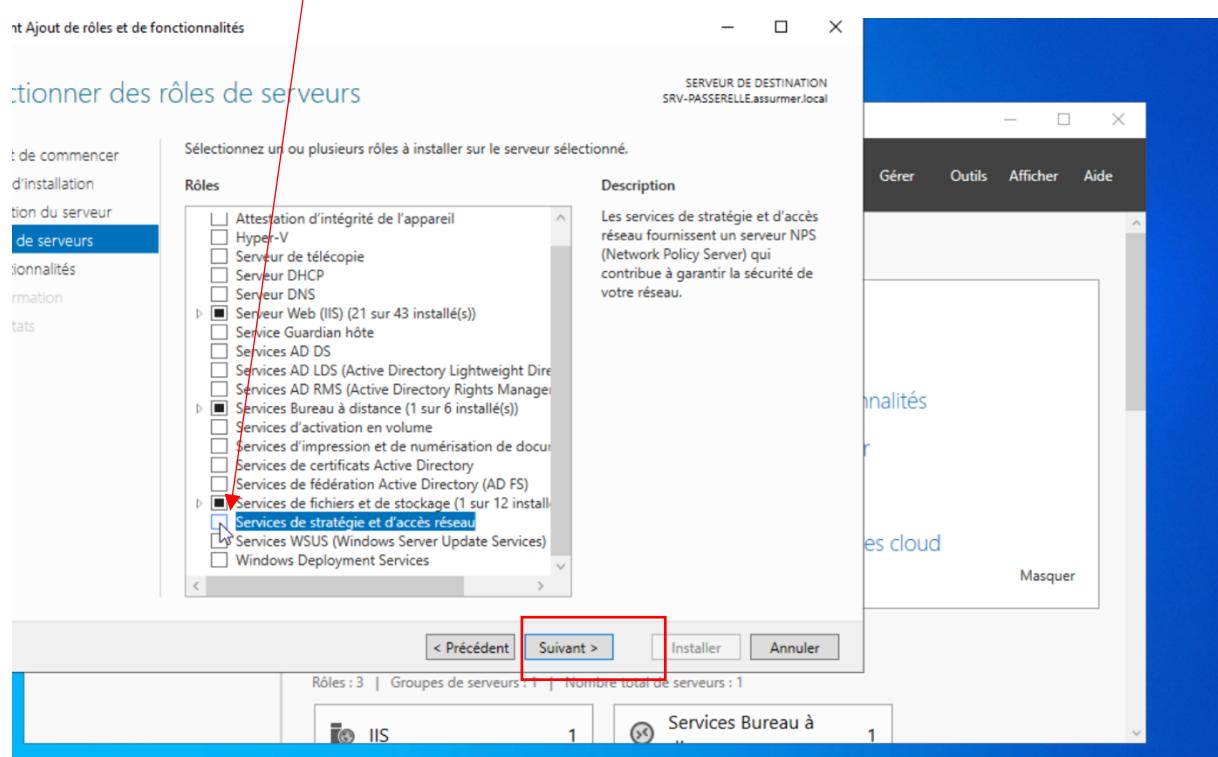
Puis cliquer sur « **Suivant** »





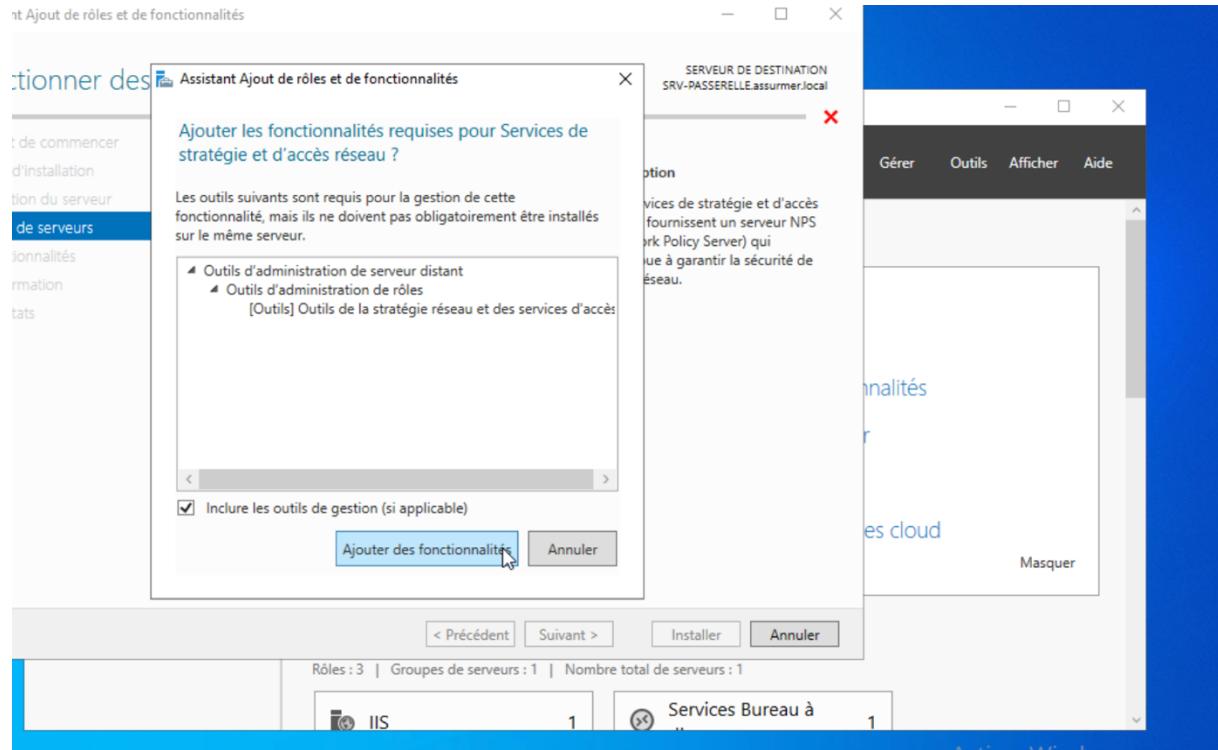
Veuillez cocher le « Services de stratégie et d'accès réseau »

Puis cliquer sur « Suivant »

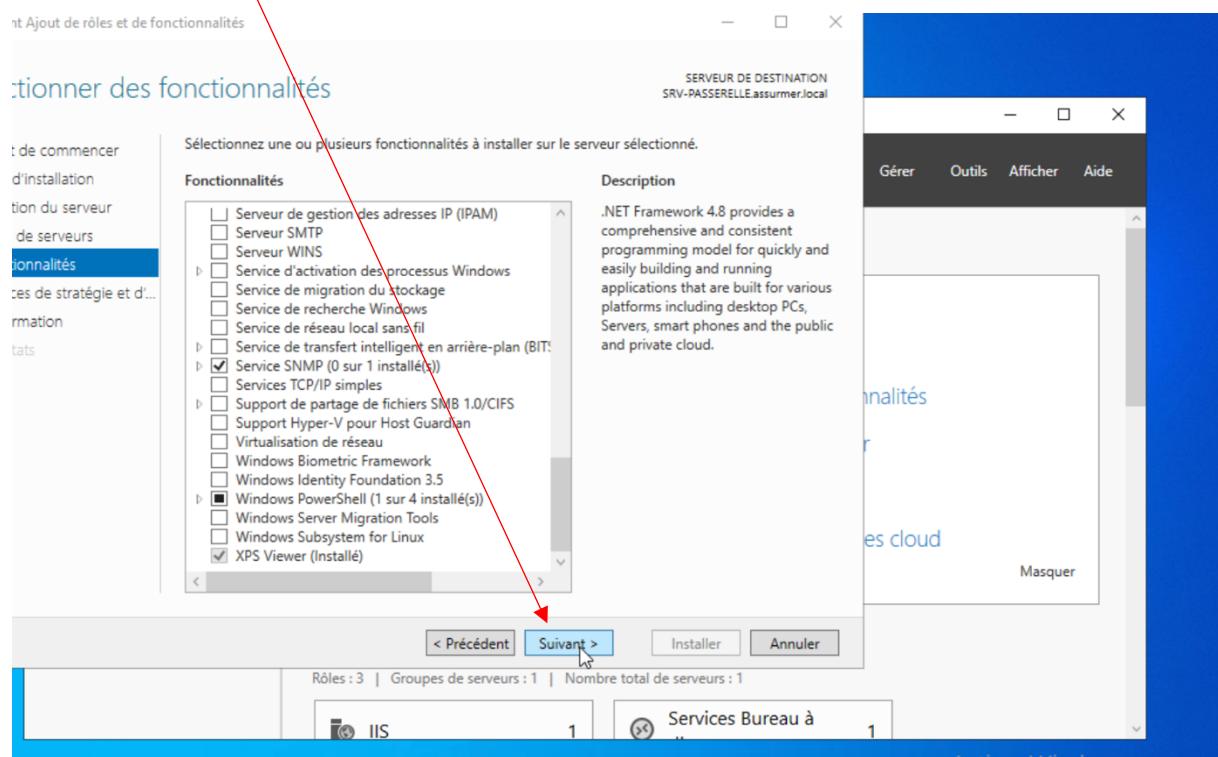


Veuillez cliquer sur « Ajouter des fonctionnalités »



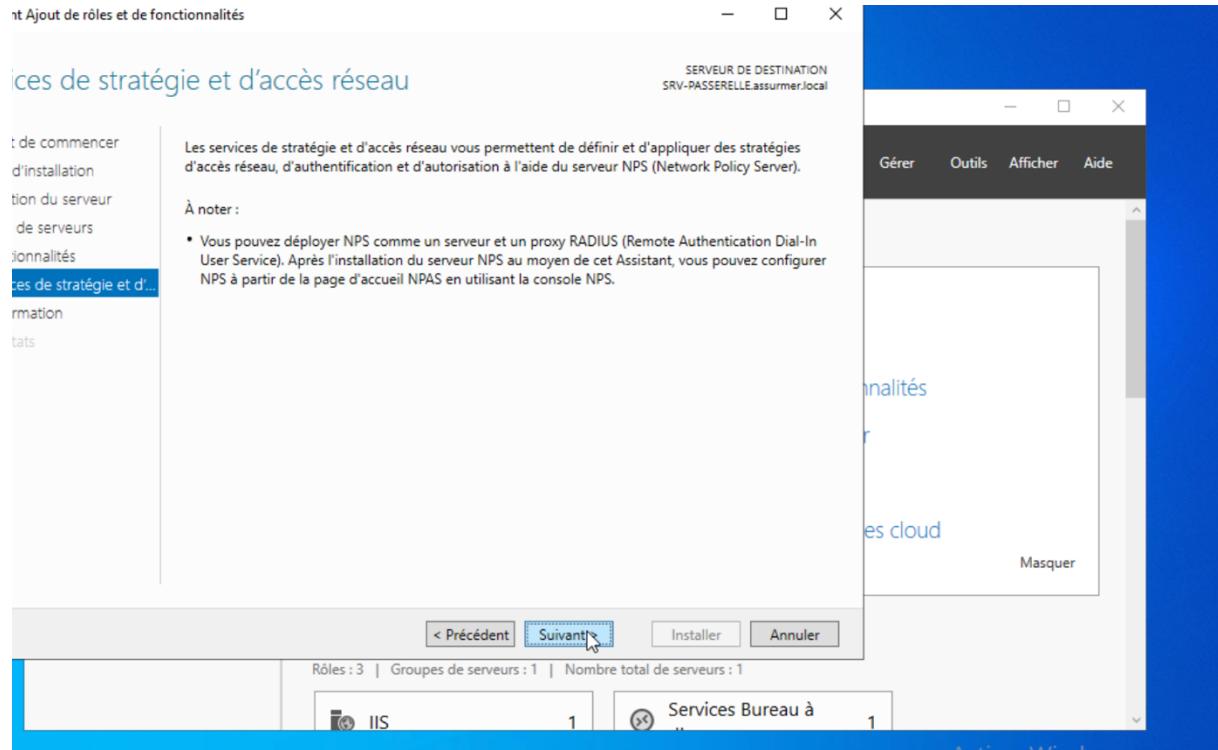


Cliquer sur « Suivant »



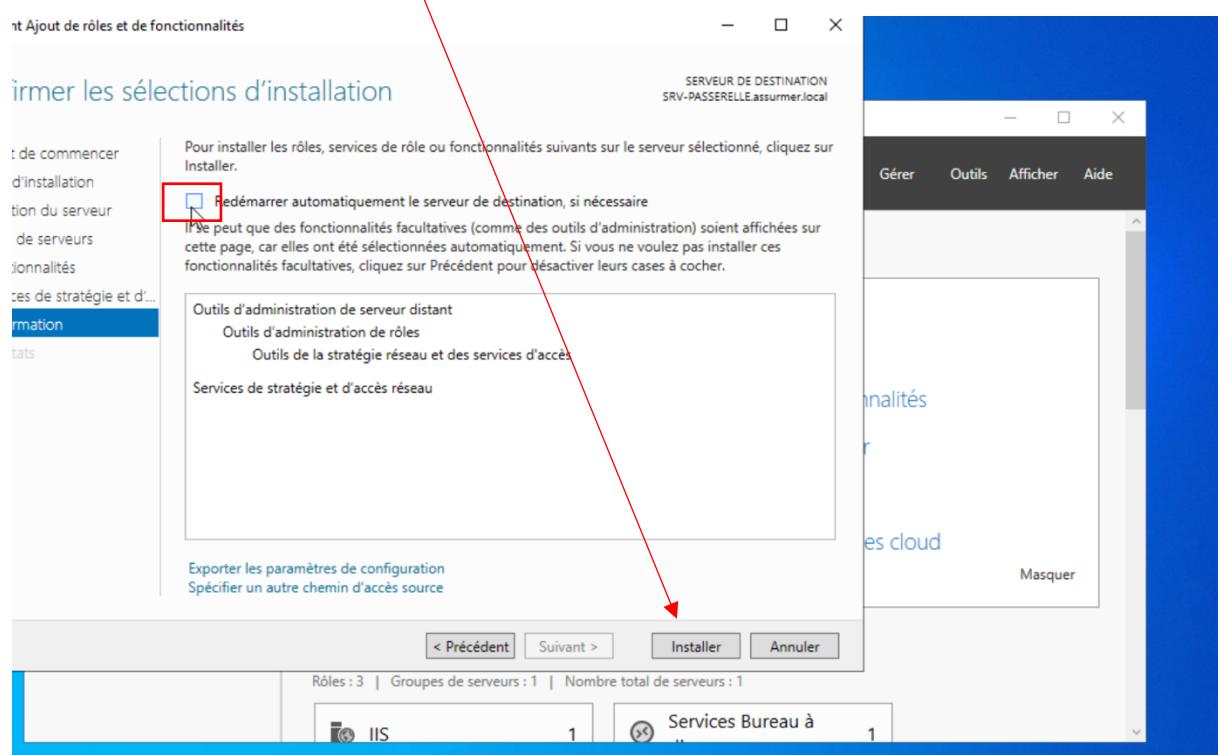
Cliquer sur « Suivant »





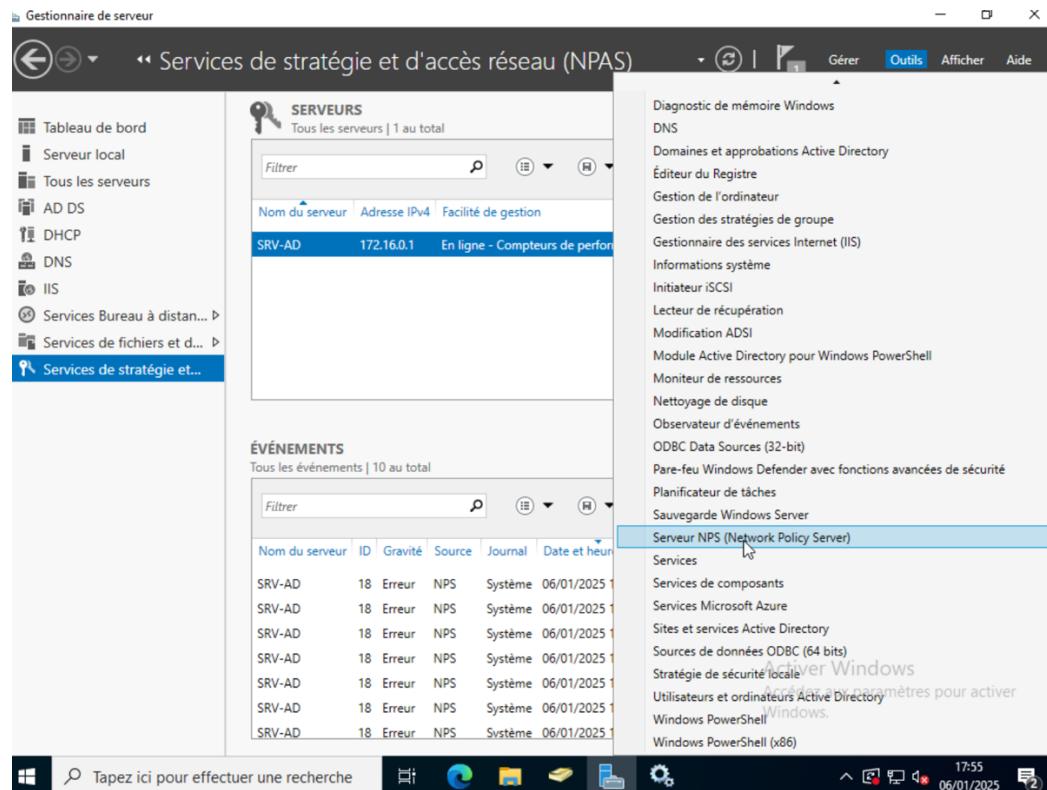
Veuillez cocher la case « **Redémarrer automatiquement le serveur de destination, si nécessaire** »

Puis veuillez cliquer sur « **Installer** »



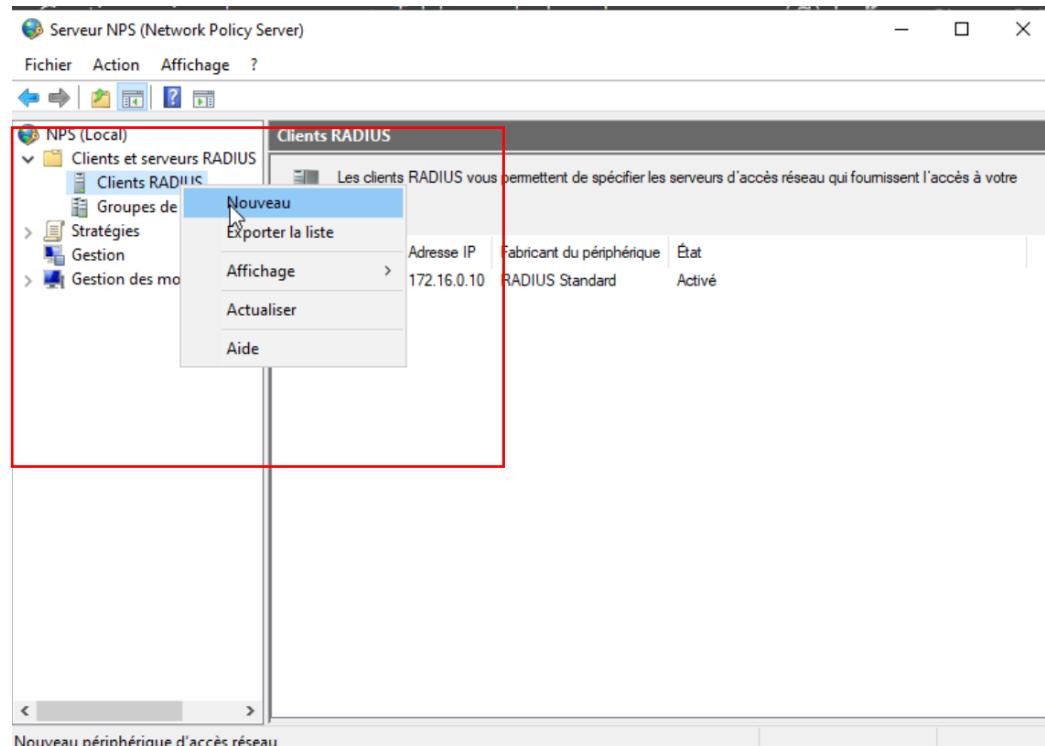
1. Configuration du service RADIUS

Après redémarrage de votre Windows Serveur, veuillez cliquer sur « Outils » puis sur

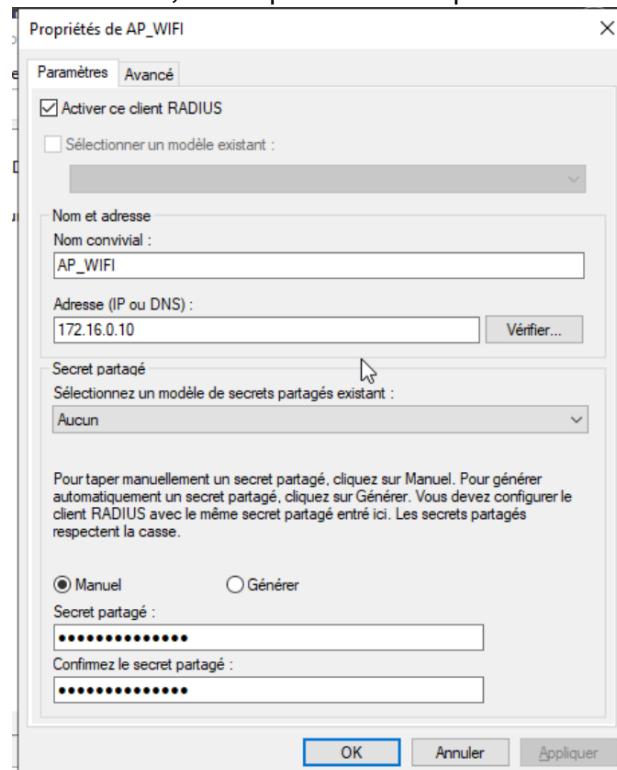


Veuillez Cliquer sur le dossier « **Clients et serveurs RADIUS** » puis sur « **Client RADIUS** »

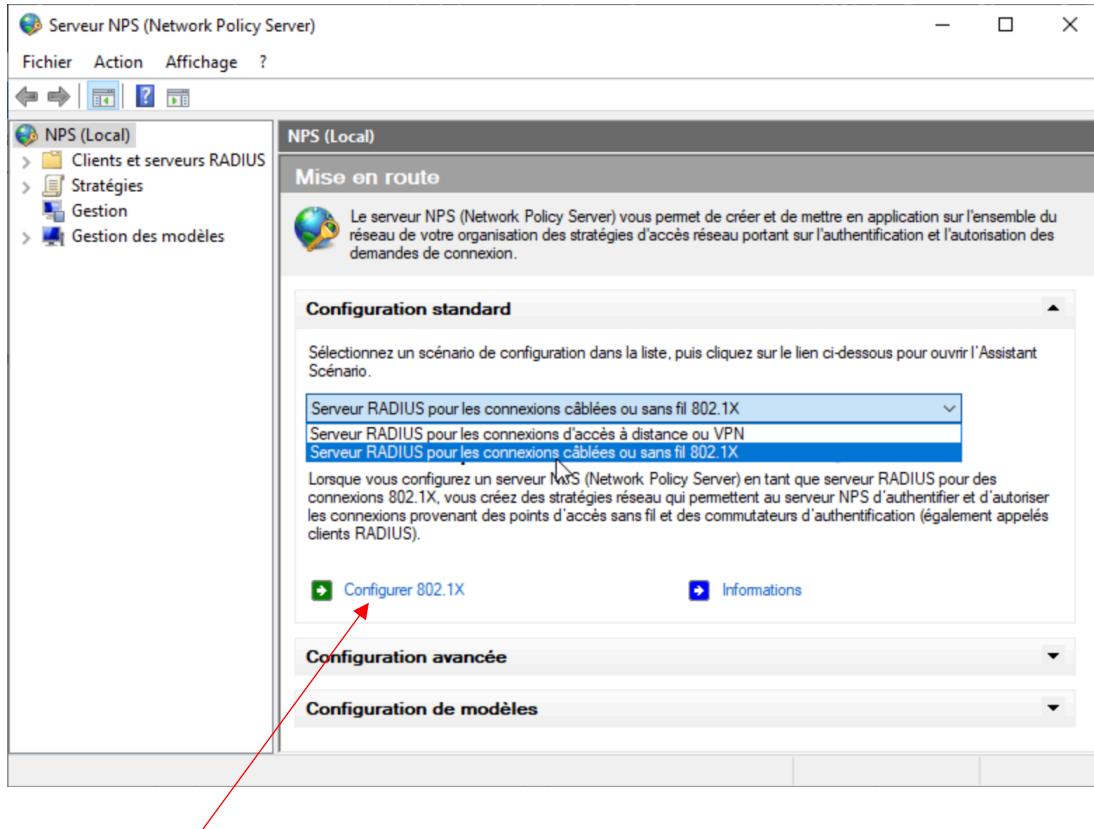
Puis sur « **Nouveau** »



Indiquez les informations suivantes : le nom convivial, l'adresse IP ou DNS de votre borne Wi-Fi, ainsi que le mot de passe du secret partagé

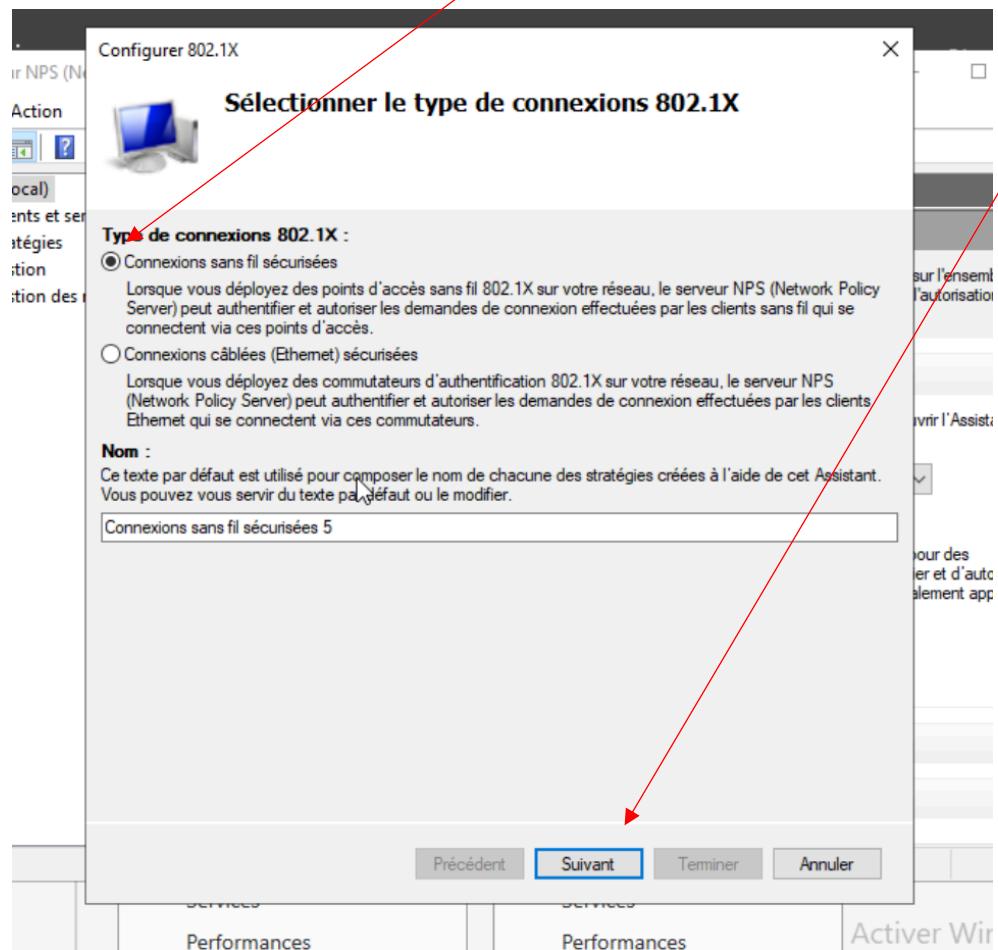


Veuillez cliquer sur « **Serveur RADIUS pour les connexions câblées ou sans fil** »

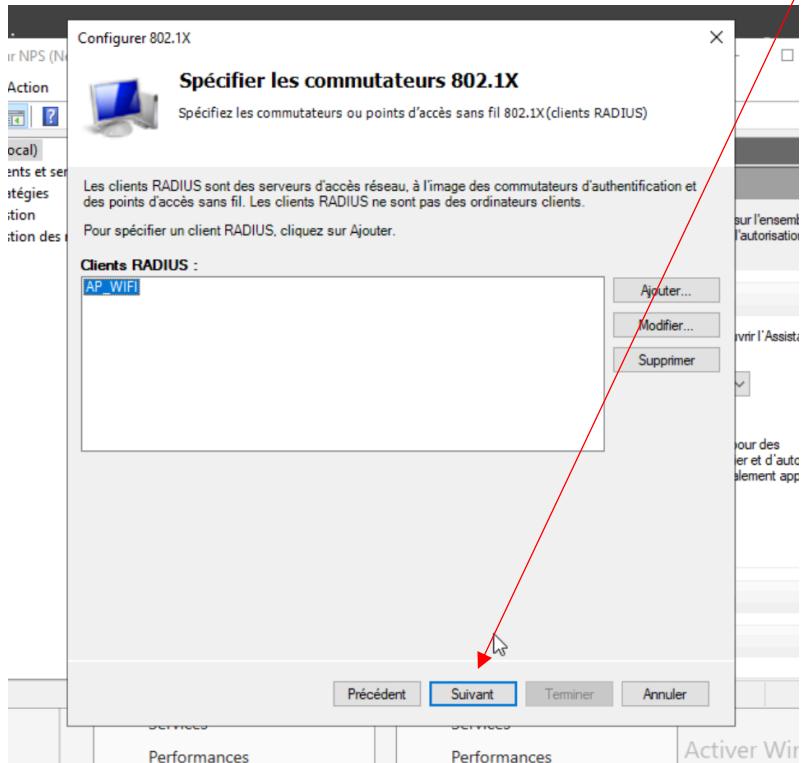


Puis sur « Configurer 802.1X

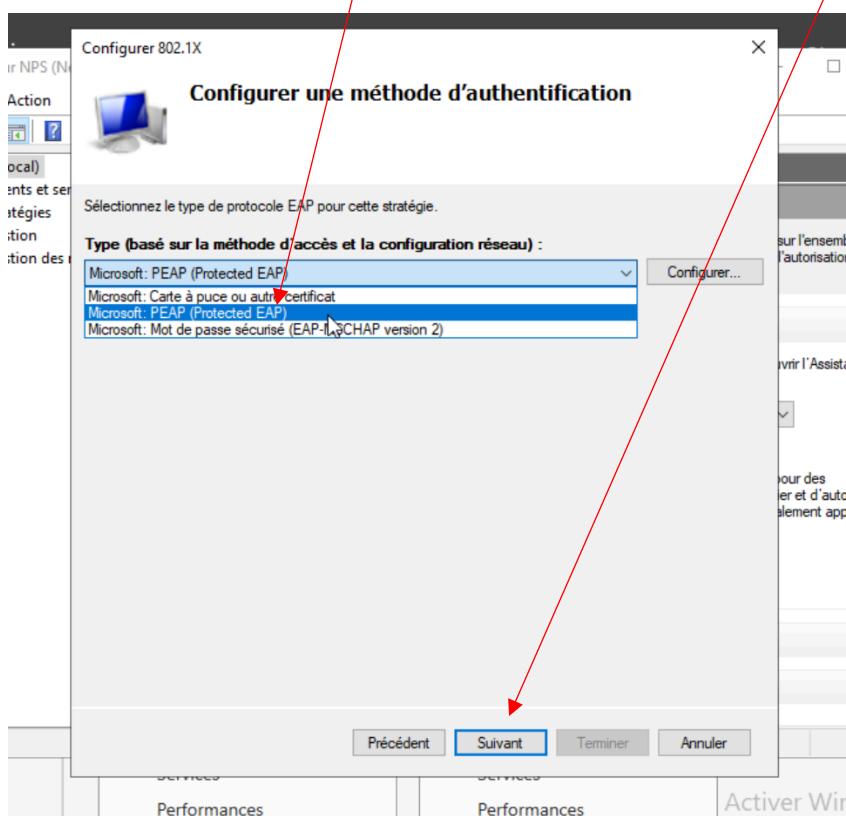
Veuillez cocher la case « Connexions sans fil sécurisées » puis cliquer sur « Suivant »



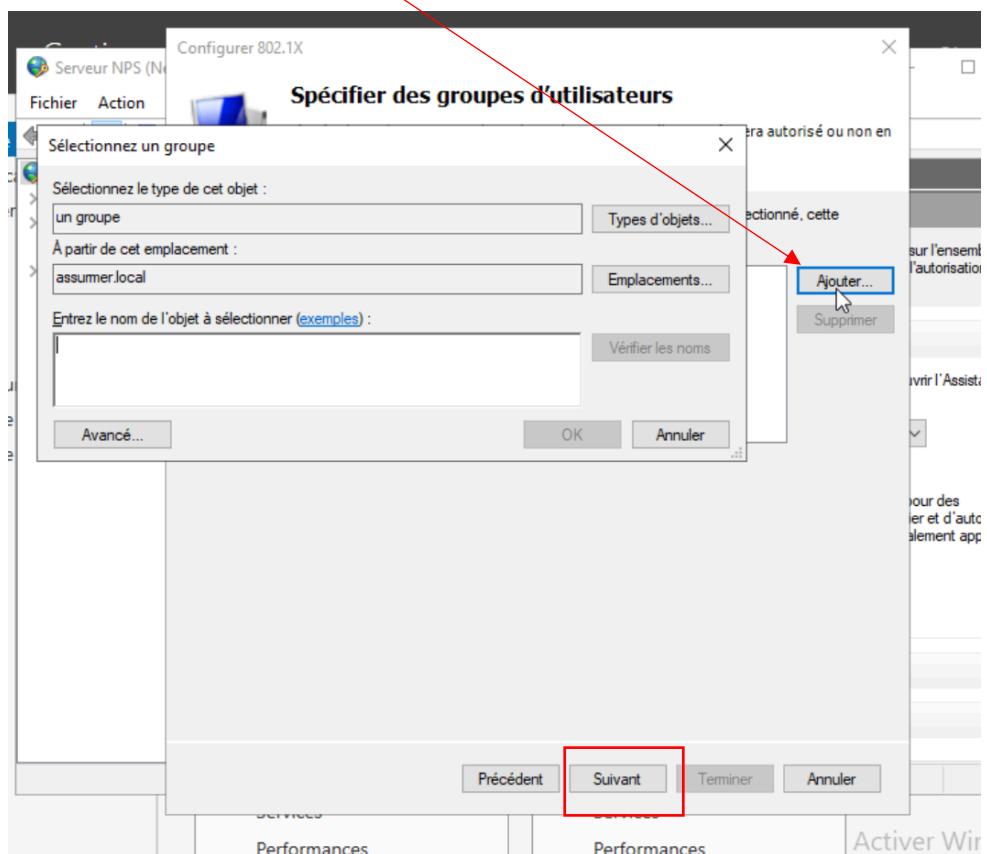
Veuillez mettre votre Client RADIUS. Puis cliquer sur « **Suivant** »



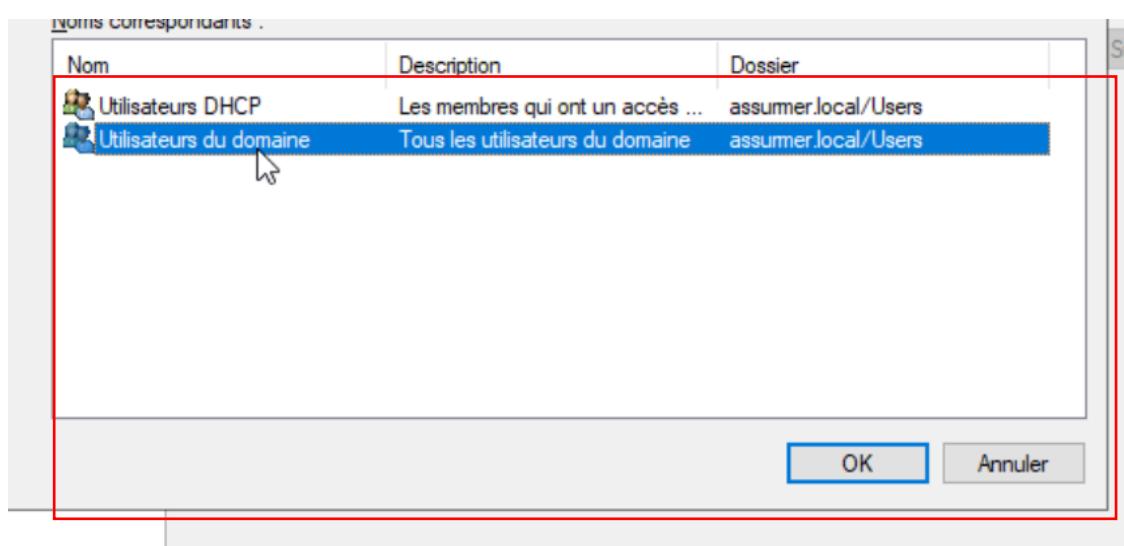
Veuillez cliquer sur « **Microsoft PEAP** » puis cliquer sur « **Suivant** »



Veuillez cliquer sur « Ajouter » puis ajoutez « Utilisateurs du nom de domaine »



Puis cliquer sur « OK » puis cliquer sur « Suivant »



Voici la page qui doit être affiché, puis cliquer « **Suivant** »

Configurer 802.1X

X

Spécifier des groupes d'utilisateurs

L'accès des utilisateurs membres du ou des groupes sélectionnés sera autorisé ou non en fonction du paramètre d'autorisation d'accès de la stratégie réseau.

Pour sélectionner des groupes d'utilisateurs, cliquez sur Ajouter. Si aucun groupe n'est sélectionné, cette stratégie s'applique à tous les utilisateurs.

Groupes

ASSURMER\Utilisateurs du domaine

Ajouter...
Supprimer

Précédent Suivant Terminer Annuler



Veuillez cliquer sur « **Suivant** »

Configurer 802.1X

Configurer les contrôles du trafic

Utilisez des réseaux locaux virtuels (VLAN) et des listes de contrôle d'accès (ACL) pour contrôler le trafic réseau.

Si vos clients RADIUS (commutateurs d'authentification et points d'accès sans fil) prennent en charge l'affectation de contrôles de trafic à l'aide d'attributs de tunnel RADIUS, vous pouvez configurer ces attributs ici. Si vous configurez ces attributs, le serveur NPS invite les clients RADIUS à appliquer ces paramètres pour les demandes de connexion authentifiées et autorisées.

Si vous n'utilisez pas de contrôles du trafic ou si vous souhaitez les configurer ultérieurement, cliquez sur Suivant.

Configuration du contrôle du trafic
Pour configurer les attributs de contrôle du trafic, cliquez sur Configurer.

Configurer...

Précédent **Suivant** Terminer Annuler

Cliquez sur « **Terminer** »

Configurer 802.1X

Fin de la configuration des nouvelles connexions câblées/sans fil sécurisées IEEE 802.1X et des clients RADIUS

Vous avez créé les stratégies suivantes et configuré les clients RADIUS ci-dessous.

- Pour afficher les détails de la configuration dans votre navigateur, cliquez sur Détails de la configuration.
- Pour modifier la configuration, cliquez sur Précédent.
- Pour enregistrer la configuration et fermer cet Assistant, cliquez sur Terminer.

Stratégie de demande de connexion :
Connexions sans fil sécurisées 5

Stratégies réseau :
Connexions sans fil sécurisées 5

[Détails de la configuration](#)

Précédent **Suivant** Terminer Annuler



Cliquez sur « NPS (Local) » puis faites « Démarrer le service NPS »

