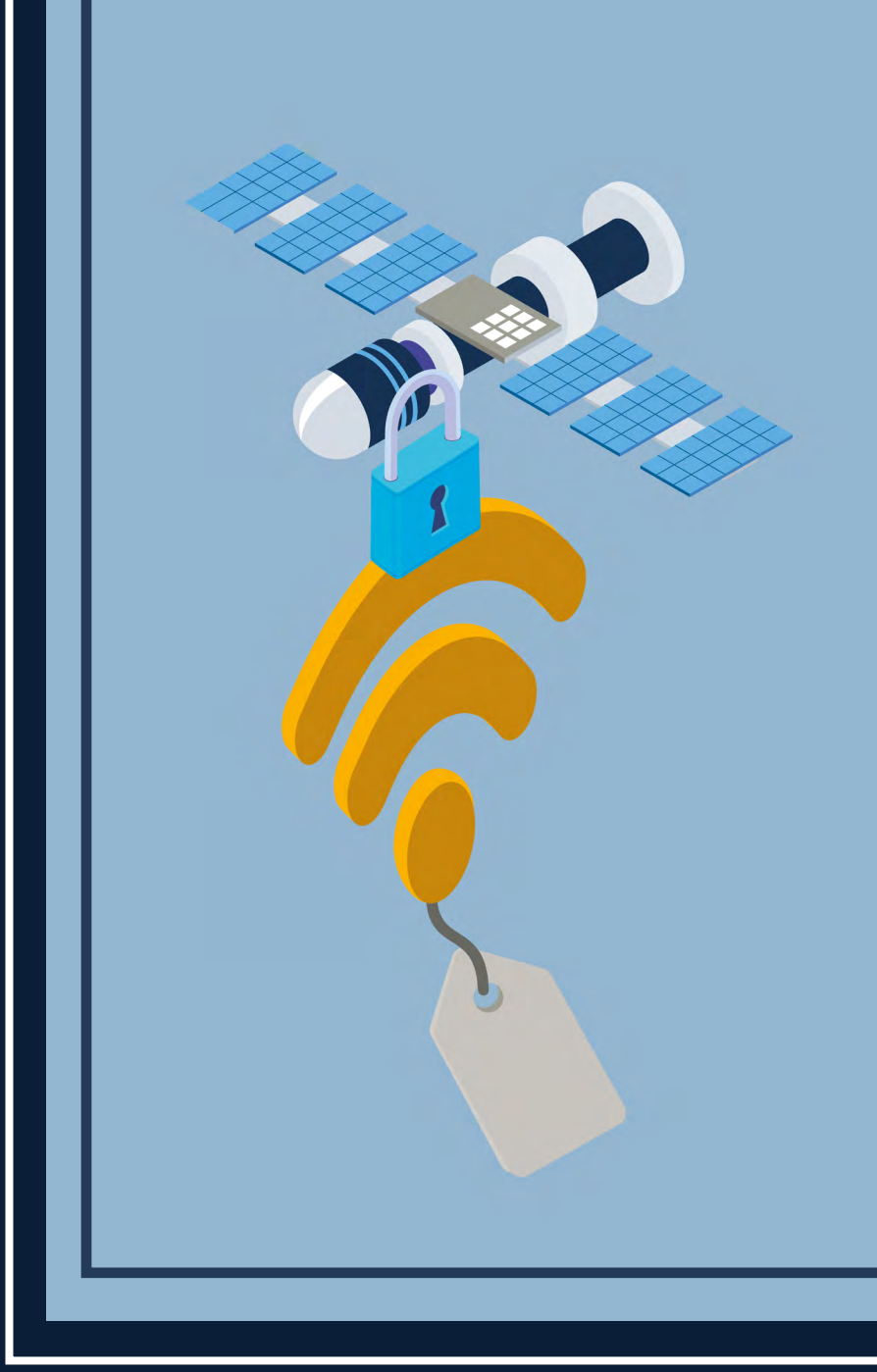
CCN-CERT

BP/11



Recommandations de sécurité dans les réseaux Wi-Fi d'entreprise

RAPPORT DE BONNES PRATIQUES

JUILLET **2021**

ccn-cert centro criptológico nacional
CCN centro criptológico nacional

Ëditér par

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLÓGICO NACIONAL, c=ES
2021.08.16 11:24:33 +02'00'

Centro Criptológico Nacional, 2021

Date d'édition: Juillet 2021

Index

1. À propos du CCN-CERT, certificat gouvernemental national

Le CCN-CERT est la capacité de réponse aux incidents de sécurité informatique du Centre national de cryptologie (CCN) rattaché au Centre national de renseignement (CNI). Ce service a été créé en 2006 en tant que **CERT gouvernemental national espagnol** et ses fonctions sont incluses dans la loi 11/2002 réglementant le CNI, le RD 421/2004 réglementant le CCN et dans le RD 3/2010, du 8 janvier, réglementant le schéma de sécurité nationale (ENS), modifié par le RD 951/2015 du 23 octobre.

Sa mission est de contribuer à l'amélioration de la cybersécurité espagnole, en étant le centre national d'alerte et de réponse qui coopère et aide à répondre rapidement et efficacement aux cyberattaques et à faire face activement aux cybermenaces, y compris la coordination au niveau public de l'État des différentes capacités de réponse aux incidents ou des centres opérationnels de cybersécurité existants.

F de la loi 11/2002) et d'informations sensibles, de défendre le patrimoine technologique de l'Espagne, de former du personnel spécialisé, d'appliquer des politiques et des procédures de sécurité, et d'utiliser et de développer les technologies les plus appropriées à cette fin.

Conformément à ce règlement et à la loi 40/2015 sur le régime juridique du secteur public, le CCN-CERT est responsable de la gestion des cyber-incidents qui affectent tout organisme ou entreprise publique. Dans le cas des opérateurs critiques du secteur public, la gestion des cyberincidents sera assurée par le CCN-CERT en coordination avec le CNPIC.

2. Introduction aux réseaux sans fil Wi-Fi

Un réseau sans fil peut être défini en termes généraux comme un réseau formé par des dispositifs ayant la capacité de communiquer entre eux par le biais d'ondes électromagnétiques et sans nécessiter de câblage (sans fil).

Les réseaux sans fil peuvent être classés en réseaux sans fil personnels (WPAN), tels que ceux basés sur l'infrarouge ou le Bluetooth, en réseaux locaux sans fil (WLAN), tels que IEEE 802.11 ou HomeRF, et en réseaux métropolitains ou étendus sans fil (WMAN ou WWAN) : réseaux de différentes générations, telles que 2G/3G/4G/5G et normes technologiques telles que CDMA et GSM, GPRS, UMTS, WiMAx (IEEE 802.16) ou LTE.

Il existe de nombreux types de réseaux sans fil qui diffèrent par leurs caractéristiques telles que leur technologie, leur norme de communication, leur architecture, etc. Ce guide se concentre exclusivement sur les réseaux WLAN ou Wi-Fi. Ces réseaux sans fil sont basés sur la norme IEEE 802.11 et les produits sont certifiés par la Wi-Fi Alliance pour garantir leur interopérabilité.

Les principaux composants d'un réseau sans fil Wi-Fi sont :

- **Dispositifs clients.** Il s'agit des appareils de l'utilisateur qui demandent une connexion au réseau sans fil pour transférer les données de l'utilisateur (ordinateurs portables, smartphones, Smart TV, etc.).
- **Points d'accès (AP).** Il s'agit de dispositifs qui font partie de l'infrastructure sans fil et qui sont chargés de connecter les dispositifs clients entre eux ou avec l'infrastructure du réseau câblé de l'organisation.

Un réseau sans fil peut être défini en termes généraux comme un réseau formé par des dispositifs ayant la capacité de communiquer entre eux par le biais d'ondes électromagnétiques et sans nécessiter de câblage (sans fil)

Il existe trois topologies courantes lorsqu'on parle de réseaux Wi-Fi sans fil : ad-hoc, infrastructure et maillage.

1. Dans la **topologie ad hoc**, chaque noeud fait partie d'un réseau dans lequel tous les membres ont la même fonction et sont libres de s'associer à n'importe quel noeud.

2. Dans la **topologie d'infrastructure**, il y a un noeud central (AP), qui sert de lien pour tous les clients. Ce noeud sert généralement à acheminer le trafic vers un réseau conventionnel ou vers d'autres réseaux différents, en convertissant les trames au format 802.11 au format natif du système de distribution (généralement 802.3 Ethernet). Pour établir la communication, tous les noeuds doivent se trouver dans la zone de couverture de l'AP ou de ses répéteurs et connaître les paramètres du réseau.

3. La **topologie maillée** mélange les deux précédentes (mesh). Dans cette topologie, un appareil fait office de point d'accès et crée à son tour un réseau point à point, dans lequel n'importe quel client peut se connecter et communiquer avec un appareil qui ne se trouve pas dans sa zone de couverture, puisque la connectivité s'étend comme un maillage.

La norme IEEE 802.11 définit l'utilisation des deux niveaux inférieurs de l'architecture ou modèle OSI (couche physique et couche liaison de données), en précisant leurs règles de fonctionnement dans un réseau WLAN. La couche physique a évolué grâce à la publication d'extensions et de modifications de la norme 802.11. Chaque évolution de la couche physique porte le nom du groupe de travail en charge de l'évolution, par exemple 11b, 11a, 11g, 11n, 11ac, 11ax, 11be, etc. Pour simplifier l'identification des évolutions technologiques, la Wi-Fi Alliance attribue des identifiants numériques corrélatifs à chaque couche physique, "Wi-Fi 4" étant équivalent à 802.11n, "Wi-Fi 5" à 802.11ac, "Wi-Fi 6" à 802.11ax et, non encore confirmé, "Wi-Fi 7" à 802.11be.

En ce qui concerne les mécanismes de sécurité, le protocole qui a été mis en oeuvre dans la norme IEEE 802.11 originale est appelé WEP (Wired Equivalent Privacy). Ce protocole a été déclaré non sécurisé en raison des multiples vulnérabilités détectées et est donc considéré comme inadapté aux réseaux sans fil qui nécessitent un minimum de sécurité. Suite aux vulnérabilités du WEP, l'IEEE 802.11i a été développé comme un amendement à la norme 802.11 originale avec des mécanismes de sécurité plus robustes pour contrecarrer les problèmes du WEP.

Le protocole mis en œuvre dans la norme IEEE 802.11 d'origine, appelé WEP, a été déclaré non sécurisé en raison des multiples vulnérabilités détectées

Alors que la version finale de l'IEEE 802.11i était en cours de ratification, et afin de résoudre certains des problèmes de sécurité du WEP sans avoir à remplacer le matériel sans fil, un protocole de sécurité a été développé qui mettait en oeuvre un sous-ensemble des spécifications 802.11i (pré-RSN et TKIP). Ce protocole a été approuvé par la Wi-Fi Alliance sous le nom de **WPA** (Wi-Fi Protected Access).

Par la suite, une fois la norme 802.11i ratifiée, la Wi-Fi Alliance a introduit le **WPA2** (Wi-Fi Protected Access 2) qui certifiait déjà le support complet de la norme IEEE 802.11i (RSN et AES). Le WPA2 n'est pas compatible, dans la plupart des cas, avec le matériel sans fil initialement conçu pour le WEP, car ce matériel ne supporte pas la charge de calcul des opérations de cryptage de l'algorithme AES, qui est l'algorithme cryptographique principal du WPA2.

À ce jour, la plupart des matériels Wi-Fi prennent en charge le WPA2. Le WPA (pré-RSN et TKIP) a été déclaré non sécurisé et, comme le WEP, ne doit pas être utilisé sur les réseaux d'entreprise.

WPA et WPA2 ont deux modes de mise en oeuvre :

- **Personnel (PSK)**, accès par une clé unique pré-partagée avec tous les clients.
- **Entreprise (802.1X)**, accès 802.1X avec des informations d'identification dédiées pour chaque client.

Les deux implémentations diffèrent principalement au niveau des mécanismes d'authentification et de distribution des clés. Personal utilise le mécanisme PSK (Pre-shared Keys) tandis que Enterprise utilise le mécanisme d'authentification 802.1X, avec l'utilisation d'un serveur d'authentification (AS), généralement le protocole RADIUS.

Dans la mesure du possible, tous les réseaux Wi-Fi devraient utiliser le mode Entreprise avec 802.1X et l'utilisation de PSK ne serait justifiée que lorsque les clients ne disposent pas du support 802.1X.

S'il est nécessaire d'utiliser un réseau avec PSK, il est recommandé d'utiliser les mécanismes non standard proposés par certains fabricants qui permettent d'attribuer une clé pré-partagée différente pour chaque dispositif client se différenciant par son adresse MAC.

Au cours de 2017 et 2018, des attaques critiques sur la poignée de main à 4 voies de WPA2 (attaques KRACK) ont été publiées. Ce fait a déclenché l'annonce par la Wi-Fi Alliance de la spécification du protocole WPA3 (WPA3-v2.0 publié le 20/12/2019).

Le protocole WPA3 a deux objectifs principaux. Le premier objectif est de certifier dans les produits Wi-Fi l'application correcte des contre-mesures proposées contre les attaques dites KRACK. Le deuxième objectif est de mettre à jour les mécanismes existants pour augmenter le niveau de sécurité et éviter les techniques d'attaque connues.

Dans la mesure du possible, tous les réseaux Wi-Fi devraient utiliser le mode Entreprise avec 802.1X

Les principales caractéristiques du WPA3 et ses modes de fonctionnement sont les suivants :

- **WPA3-Personal-SAE**
  - **Mode WPA3-Personal-Only (personnel uniquement)**
    - Utilisation obligatoire de la *protection des trames de gestion* (MFP) 802.11w
    - Utilisation obligatoire de l'*authentification simultanée des égaux* (SAE)
  - **Modo WPA3-Personal-*Transition***
    - *MFP-802.11w* en option pour un client WPA2-Personal
    - PSK pour les clients WPA2-Personal et SAE pour les clients WPA3-Personal.
- **WPA3-Enterprise-802.1X**
  - **Mode WPA3-Enterprise-Only**
    - Utilisation obligatoire du MFP-802.11w
  - **Mode de transition WPA3-Enterprise**
    - Utilisation facultative du MFP-802.11w pour les clients WPA2-Enterprise
  - **Mode WPA3-Enterprise-192 bits**
    - Utilisation obligatoire du MFP-802.11w
    - Cryptage AES-GCM 256 bits du trafic utilisateur
    - *Suites de chiffrement* restreintes sur le canal EAP :
      - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        - ECDHE et ECDSA utilisant la courbe elliptique P-384
      - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        - ECDHE utilisant la courbe elliptique P-384
        - RSA >= 3072 bits
      - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
        - DHE y RSA >= 3072 bits

Sur le WPA3 de nouvelles vulnérabilités et attaques ont été publiées qui obligent à repenser s'il est nécessaire de faire des modifications sur le protocole (Dragonblood qui affecte Dragonfly de SAE et EAP-pwd). Des vulnérabilités ont également été publiées qui affectent les puces clientes et les points d'accès permettant le déchiffrement des trames mises en mémoire tampon lorsqu'elles sont envoyées avec TK=0 après dissociation (vulnérabilité Kr00K publiée en février 2020).

Les technologies sans fil changent et évoluent constamment. Il est très important que les administrateurs se tiennent au courant et appliquent les contre-mesures nécessaires aux vulnérabilités et menaces publiées. Il est également important de connaître les évolutions de la norme et d'en tenir compte lorsqu'un rafraîchissement technologique est nécessaire.

3. Risques et menaces dans les réseaux Wi-Fi

Les réseaux sans fil sont exposés à la plupart des mêmes risques que les réseaux câblés, plus ceux introduits par la technologie Wi-Fi.

Pour maîtriser ces risques, les organisations qui ont besoin d'utiliser de tels réseaux doivent adopter des mesures de protection pour minimiser la probabilité d'un impact sur les infrastructures existantes et nouvellement déployées.

En outre, comme pour toute technologie, il est essentiel de surveiller en permanence les nouvelles vulnérabilités qui pourraient apparaître à l'avenir et affecter l'organisation.

Dans la mesure du possible, il est recommandé d'utiliser un accès filaire et de désactiver les interfaces sans fil.

Dans la mesure du possible, il est recommandé d'utiliser un accès filaire et de désactiver les interfaces sans fil

Voici les principales menaces qui pèsent sur les réseaux sans fil :

- En raison d'une vulnérabilité inconnue, l'ordinateur pourrait être compromis en ayant l'interface sans fil activée sans que l'attaquant ait besoin d'un contact physique.
- L'accès peut être obtenu par des connexions sans fil à d'autres environnements non sans fil qui y sont connectés.
- Les informations transmises sans fil peuvent être interceptées même à des kilomètres de distance, sans qu'il soit possible de détecter cette capture.
- Des attaques par déni de service (DoS) contre ce type d'infrastructure peuvent facilement se produire (brouilleurs de signaux, paquets malveillants, etc.).
- Le trafic peut être injecté dans les réseaux sans fil sur de longues distances (voire des kilomètres).
- En utilisant des réseaux non cryptés ou en connaissant l'infrastructure, il est possible de déployer des points d'accès malveillants en usurpant des informations (par exemple, en usurpant le serveur Radius pour voler les identifiants et les mots de passe de l'entreprise si les certificats EAP-TLS ne sont pas utilisés).
- Une fois l'accès à un réseau sans fil obtenu, des attaques de type "Man in the Middle" peuvent être menées.
- Les informations relatives à la connexion peuvent être obtenues en accédant à un ordinateur légitime et en effectuant une analyse judiciaire de celui-ci.
- L'accès aux réseaux peut être obtenu en utilisant les réseaux connectés de tiers qui ne maintiennent pas une politique de sécurité adéquate.
- Les attaques de l'intérieur peuvent être menées en déployant des réseaux sans fil non autorisés.
- Les informations concernant l'entité propriétaire et les appareils clients peuvent être révélées dans des données ouvertes qui peuvent être facilement capturées (SSID et adresses MAC).

Une fois l'accès à un réseau sans fil obtenu, des attaques de type "Man in the Middle" peuvent être menées

4. Réseaux Wi-Fi d'entreprise

Le service Wi-FI d'une entreprise est principalement composé de deux blocs structurels :

- Les appareils de l'utilisateur agissant comme un client final.
- L'architecture physique de l'accès et des services complémentaires.

Ce guide couvre l'accès au service Wi-Fi pour les appareils et les utilisateurs de l'entreprise. Il suppose que les dispositifs ont été certifiés et configurés pour prendre en charge le contrôle d'accès basé sur la norme 802.1X en utilisant la méthode EAP-TLS. Lors d'un déploiement initial, les appareils ont été configurés et dotés d'un certificat client pour identifier l'appareil et l'utilisateur.

Les administrateurs de services Wi-Fi doivent configurer et utiliser les différents mécanismes et solutions existants pour garantir les piliers de base du contrôle d'accès au réseau :

- Authentifier les utilisateurs et les appareils.
- Autoriser en appliquant les politiques selon le rôle de l'utilisateur/du dispositif.
- Vérifiez en permanence la santé et le comportement de l'appareil.
- Sécuriser les communications en utilisant des couches de cryptage (Wi-Fi et VPN).
- Enregistrer les actions réalisées pour l'analyse et le suivi (*comptabilité*).

Les administrateurs de services Wi-Fi doivent configurer et utiliser les différents mécanismes et solutions existants pour garantir les piliers de base du contrôle d'accès au réseau

4.1 Architecture du service Wi-Fi

Dans les sections suivantes, nous analyserons les principales caractéristiques concernant la définition de l'architecture logique, de l'architecture physique et de la ségrégation des réseaux.

Pour définir l'architecture physique et logique d'un réseau Wi-Fi d'entreprise, il est difficile de généraliser certaines recommandations car sa conception est non seulement affectée par les besoins et les caractéristiques de l'entreprise mais aussi par le produit du fabricant choisi comme solution de service Wi-Fi.

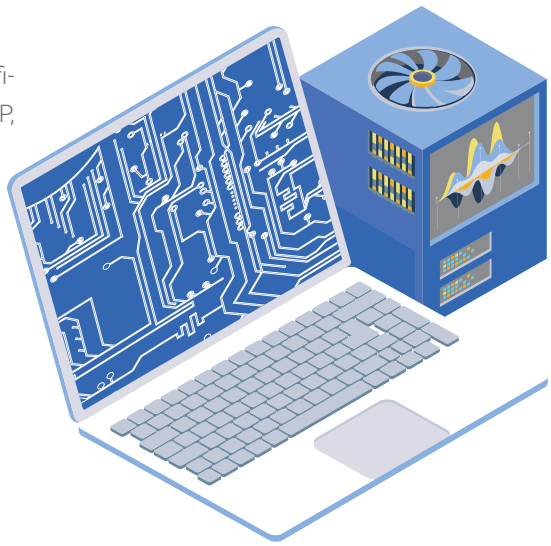
4.1.1 Architecture logique et physique

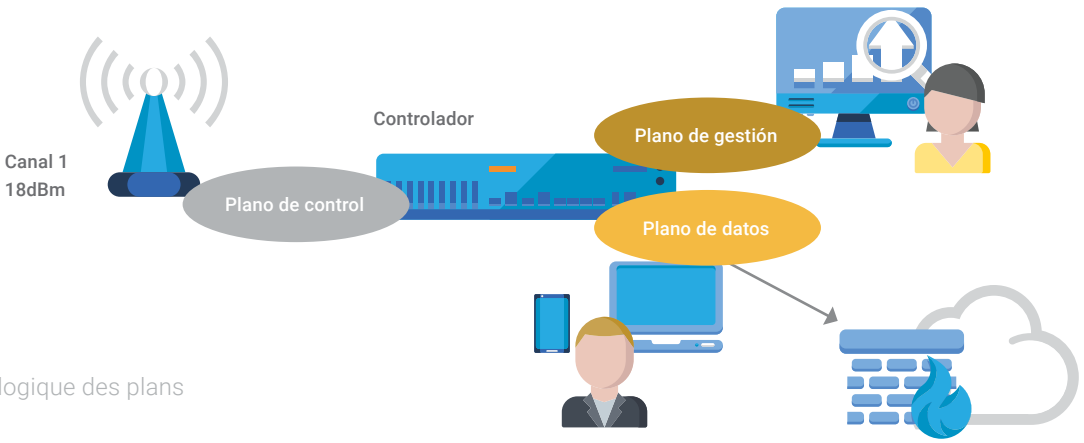
Lorsqu'on parle de l'architecture logique d'un réseau Wi-Fi d'entreprise, on peut définir trois plans fonctionnels (*plans ou couches*) représentés dans la **figure 1** :

1. *Plan de données ou plan de transfert :* chargé de déplacer les paquets de données des utilisateurs dans différentes directions : utilisateur-réseau, réseau-utilisateur et utilisateur-utilisateur.

2. *Plan de contrôle :* où résident les différents protocoles, processus et fonctions du service Wi-Fi : routage des paquets, protection contre les boucles, attribution automatique des canaux et de la puissance, etc.

3. *Management Plane* : Celui qui permet à l'administrateur de configurer et de surveiller le service Wi-Fi : GUI-Web, CLI-SSH, SNMP, syslog, etc.





[Figure 1]
Architecture logique des plans fonctionnels

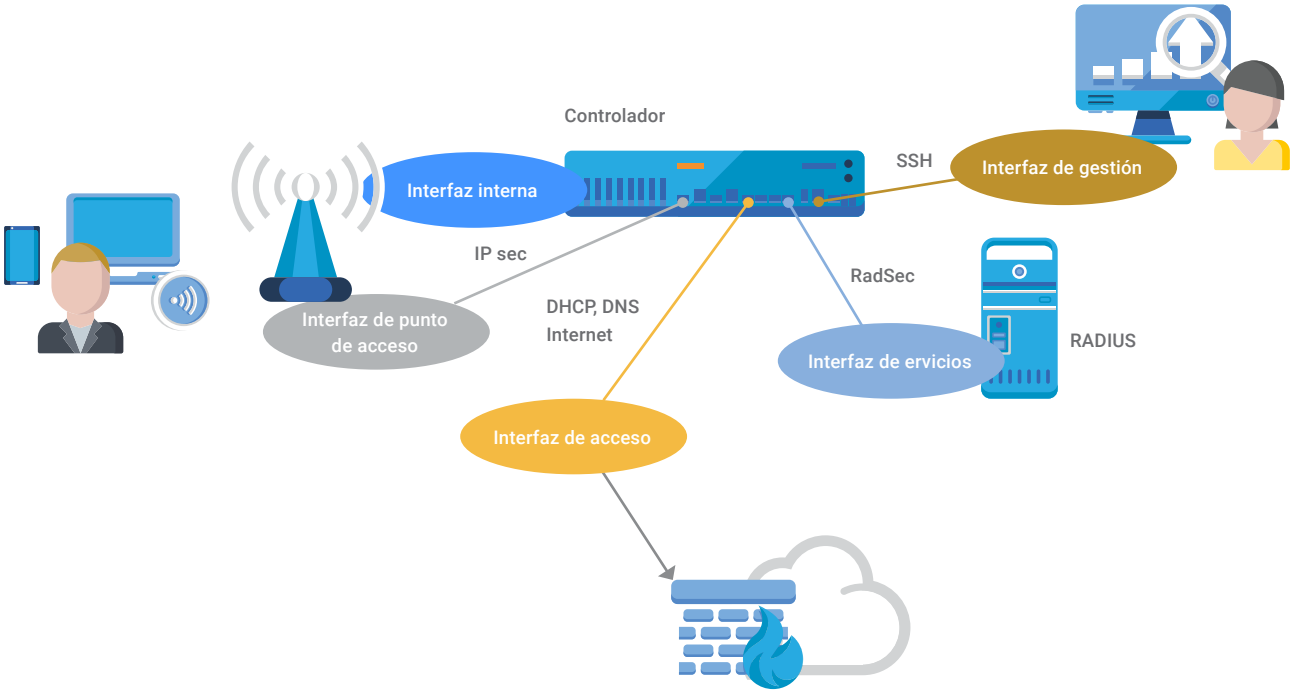
Pour sécuriser un réseau Wi-Fi, il est important de savoir où se trouve chacun des plans logiques et comment les différents éléments qui font partie du service communiquent. Chaque produit et solution du fabricant a sa propre définition de l'architecture et c'est la tâche de l'administrateur de connaître les caractéristiques de chacun d'eux afin d'effectuer une configuration correcte.

Par exemple, nous pouvons trouver des solutions entièrement centralisées basées sur un contrôleur et des points d'accès dits "légers". Les points d'accès établissent un tunnel IPsec vers le contrôleur, qui est chargé de gérer toutes les tâches définies dans le plan de données, de contrôle et de gestion.

La **figure 2** montre comment le contrôleur peut avoir des interfaces physiques dédiées au trafic de gestion (GUI-Web, CLI-SSH, SNMP, syslog, etc.) et avoir d'autres interfaces physiques indépendantes pour le plan de données en séparant le trafic utilisateur dans différents VLAN.

Le contrôleur peut agir en tant que dispositif de couche 2 en commutant le trafic des utilisateurs Wi-Fi vers le réseau d'accès ou il peut assumer des tâches de couche 3 en acheminant le trafic entre les différents réseaux d'utilisateurs. Dans les deux cas, il pourrait remplir des fonctions de pare-feu ou même effectuer l'identification des applications, le filtrage et la catégorisation des URL, l'analyse IDS/IPS, l'analyse des logiciels malveillants, etc.

Pour sécuriser un réseau Wi-Fi, il est important de savoir où se trouve chacun des plans logiques et comment les différents éléments qui font partie du service communiquent



[Figure 2]
Architecture des interfaces physiques

Le contrôleur prend également en charge d'autres tâches du plan de contrôle telles que l'orchestration de l'allocation des canaux et de la puissance. Selon la solution du fournisseur, certaines tâches du plan de contrôle peuvent être déléguées à un serveur ou à un service en nuage extérieur au contrôleur.

Il existe des solutions basées sur les contrôleurs qui décentralisent certains plans logiques. Par exemple, un administrateur peut prendre la décision de céder le plan de données au point d'accès sans avoir à concentrer le trafic sur le contrôleur. Dans ce cas, le trafic utilisateur sera déversé sur l'interface de l'antenne elle-même, en le séparant en différents VLAN utilisateur et en maintenant le tunnel IPsec vers le contrôleur pour conserver la centralisation du plan de gestion et de contrôle.

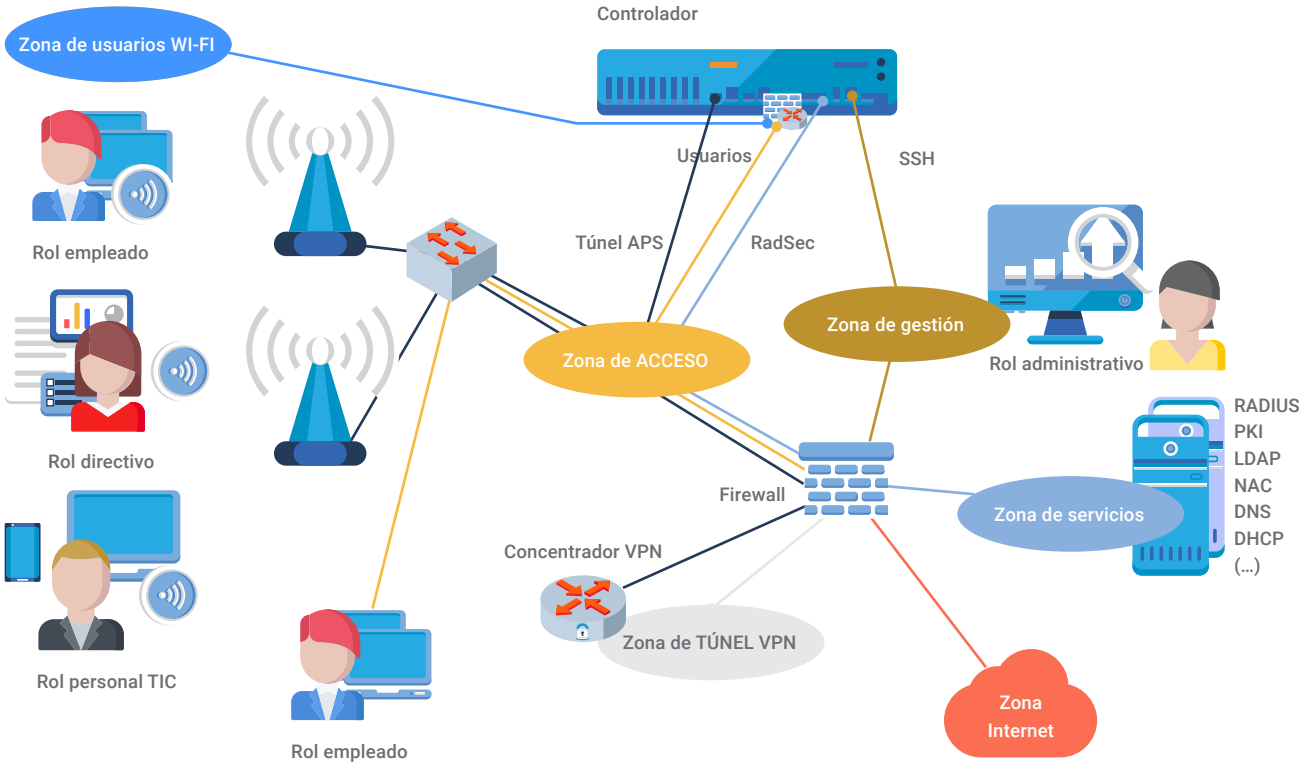
On peut également trouver des solutions totalement décentralisées, communément appelées "sans contrôleur". Le plan de données est attribué à chaque point d'accès et le plan de contrôle peut être de type maillé, dans lequel tous les points d'accès interagissent de manière égale, ou de type maître, dans lequel un point d'accès assume le rôle d'administrateur du plan de contrôle. En ce qui concerne le plan de gestion, il peut également être assumé par un point d'accès maître ou centralisé virtuellement dans un service en nuage.

4.1.2 La ségrégation des zones, des réseaux et des rôles

Pour regrouper et isoler correctement les différents appareils qui composent un réseau Wi-Fi d'entreprise, il est recommandé de maximiser la ségrégation. L'idéal serait d'appliquer un modèle de confiance zéro qui applique des politiques de sécurité à toutes les communications qui ont lieu entre les éléments du réseau, qu'ils soient clients ou serveurs.

Pour simplifier l'exemple, nous proposons la création de zones, de réseaux virtuels (VLAN) et de rôles dans l'architecture logique présentée à la **figure 3**.

- **Zone d'accès** : ensemble de réseaux configurés dans les commutateurs d'accès :
  - **Réseau pour les points d'accès :** réseau dédié à la communication entre les points d'accès et le contrôleur qui établit un tunnel IPsec.
  - **Réseau d'utilisateurs :** créez différents VLAN par département, disponibilité physique, niveau de sécurité ou rôle/profil d'utilisateur.
  - **Réseau pour l'accès aux services :** réseau dédié pour l'accès aux services tels que les requêtes RADIUS du contrôleur.
- **Zone de tunnel VPN :** Lorsqu'un utilisateur établit un tunnel VPN avec le concentrateur de tunnel de l'entreprise, un réseau de confiance protégé de bout en bout est défini. Il n'entre pas dans le cadre de ce guide de recommander les réseaux auxquels on accède par le tunnel, car cela varie en fonction des intérêts et des politiques de l'entreprise.
- **Zone d'accès à Internet :** elle fournira au réseau d'entreprise un accès à Internet par le biais d'un pare-feu qui protège toutes les communications entre les zones.
- **Zone de gestion :** elle sera utilisée pour effectuer les tâches d'administration et de configuration de tous les systèmes qui lui sont connectés.



[Figure 3]
Séparation des zones, des réseaux et des rôles

- **Zone de service :** où sont situés les serveurs de l'entreprise. Il est recommandé de procéder à une micro-segmentation et d'appliquer la sécurité à toute communication qui a lieu entre les différents éléments, clients et serveurs.

- **Réseaux de l'utilisateur du contrôleur :** il s'agit de réseaux qui ne seront définis que sur le contrôleur du point d'accès dans le but de sécuriser les communications avec le réseau d'accès.

Si vous décidez que le contrôleur agira comme un équipement de niveau 3 (effectuant des tâches de routage), vous pouvez définir deux zones sur le contrôleur pour les utilisateurs : la zone de réseau utilisateur Wi-Fi et la zone de réseau d'accès d'entreprise.

Une fois l'authentification du dispositif utilisateur terminée, au sein du contrôleur, le concept de rôle d'autorisation est appliqué pour chaque session. Ce rôle affecte le trafic des utilisateurs et les échanges de sessions avec le réseau d'accès de l'entreprise.

L'application d'un rôle peut forcer un utilisateur à changer de réseau en lui attribuant un nouveau VLAN ou bien elle peut indiquer de ne pas changer de VLAN, afin de ne pas affecter la configuration IP du client, mais de modifier les règles de filtrage du réseau.

Vous pouvez définir les rôles suivants :

- **Rôle de validation :**

  Sera appliqué à un client qui a terminé avec succès le processus d'authentification 802.1X (phase 2 du modèle de sécurité discuté plus loin). Le client restera dans ce rôle pendant qu'il est analysé pour vérifier sa conformité aux exigences relatives à l'état de santé du dispositif et aux autres attributs d'autorisation. Les accès strictement nécessaires pour pouvoir obtenir la configuration IP et recevoir ou établir des connexions contre les services de la solution d'agent NAC seront autorisés.

- **Rôle de quarantaine :**

  Ce rôle sera appliqué aux clients qui ne répondent pas aux exigences de sécurité. Cela peut être dû à un rapport négatif de l'agent NAC concernant le statut du dispositif ou à une autre indication d'attribut d'autorisation. Si la remédiation est possible, la politique de rôle permettra l'accès aux ressources nécessaires pour résoudre le problème.

- **Rôle d'état sain :**

  Sera appliqué aux clients qui répondent aux exigences de sécurité établies. Ce rôle permettra aux clients de créer un tunnel VPN (phase 4 du modèle de sécurité qui sera abordé plus loin). Lorsque le tunnel VPN est établi, on accède au réseau du tunnel où se trouve un serveur d'adresses IP qui fournit une nouvelle adresse IP par laquelle le trafic encapsulé sera transmis et reçu.

- **Rôle de statut sain avec profil :**

  Il se peut que des politiques différentes doivent être appliquées en fonction du profil de l'utilisateur, auquel cas un rôle spécifique pourrait être créé pour chaque profil (par exemple, employés, cadres, personnel technique, étudiants, enseignants, etc.)

5. Modèle de sécurité

ette section présente le modèle de sécurité basé sur quatre phases à configurer et à mettre en oeuvre dans un réseau Wi-Fi d'entreprise sécurisé. Le modèle s'applique aux appareils et aux utilisateurs de l'entreprise.

Il est recommandé d'utiliser un seul SSID d'entreprise **802.1X-Enterprise** qui utilise **EAP-TLS** avec des certificats de serveur et de client comme méthode d'authentification. Une fois le client authentifié et autorisé, le canal sans fil sera crypté avec **AES**. Ensuite, une analyse continue de l'état de santé de l'appareil sera effectuée avec un **agent NAC** et/ou le comportement de l'appareil sera surveillé à l'aide de techniques d'***empreinte digitale***. Le résultat de l'analyse de l'état de santé permettra de modifier le niveau d'autorisation si nécessaire. Enfin, pour assurer le cryptage de bout en bout, un **tunnel VPN crypté** sera établi.

- **Phase 0:**
  Configuration du service d'entreprise et déploiement des clients.
- **Phase 1:**
  Association et authentification par adresse MAC.
- **Phase 2:**
  Authentification et autorisation 802.1X avec EAP-TLS.
- **Phase 3:**
  Accès au réseau et contrôle continu de l'état de santé du dispositif.
- **Phase 4:**
  établissement d'un tunnel VPN crypté.

> **Le modèle s'applique aux appareils et aux utilisateurs de l'entreprise**

5.1 Phase 0 : Configuration et deploiement

Avant de commencer les phases d'accès, il est nécessaire de configurer la solution de service Wi-Fi par l'administrateur et de déployer la configuration des dispositifs clients pour accéder correctement au service Wi-Fi.

5.1.1 Paramètres du mode entreprise

La spécification WPA3-v2.0 offre la possibilité de configurer différents modes WPA3-Enterprise. La **figure 4** représente la prise de décision du mode WPA3-Enterprise à configurer : Only, Transition ou 192 bits. Les modes seront conditionnés aux fonctionnalités supportées par les différents éléments de la solution Wi-Fi :

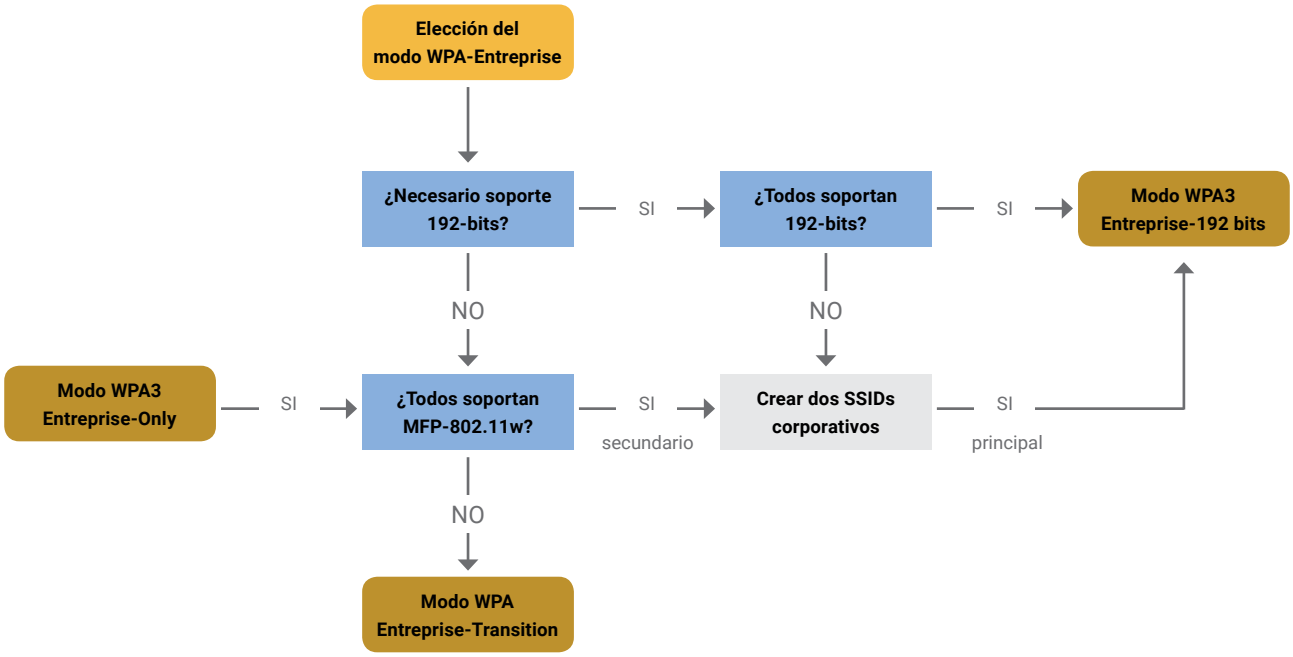
- **MFP-802.11w :** sur les périphériques clients et les points d'accès.
- **Suites de chiffrement robustes :** sur le client supplicant et le serveur d'authentification.
- **Cryptage AES-256-GCM :** sur les dispositifs clients et les points d'accès.

Si possible, il est recommandé d'utiliser un seul SSID pour accéder au réseau Wi-Fi de l'entreprise (par exemple, "corp_1X"). Au moment de la rédaction du présent document, le plus haut niveau de sécurité est assuré par le mode WPA3-Enterprise-192 bits (MFP-802.11w obligatoire, suites de chiffrement fortes et cryptage du trafic AES-256-GCM).

Si tous les appareils et éléments de l'infrastructure Wi-Fi prennent en charge le mode WPA3-Enterprise-192 bits, il est recommandé de l'utiliser dans le SSID de l'entreprise.

Mais comme le WPA3 est une spécification très récente, il est possible que tous les appareils ne prennent pas en charge le mode 192 bits. Si la prise en charge du client est partielle, il sera nécessaire de définir un deuxième SSID d'entreprise pour donner accès aux dispositifs non pris

Si tous les appareils et éléments de l'infrastructure Wi-Fi prennent en charge le mode WPA3-Enterprise-192 bits, il est recommandé de l'utiliser dans le SSID de l'entreprise



[Figure 4]
Choix du mode WPA3-Enterprise

en charge (par exemple, "corp_1X_2") afin de maintenir le plus haut niveau de sécurité 192 bits sur le SSID principal.

Sur les SSID où le mode 192 bits n'est pas configuré, il est recommandé d'activer au moins de manière facultative toutes les fonctions qui sont une exigence du mode 192 bits : utilisation des suites de chiffrement robustes, chiffrement AES-256-GCM et MFP-802.11w.

Lorsque tous les appareils prennent en charge le mode WPA3-Enterprise mais que seuls certains prennent en charge le mode 192 bits, vous pouvez configurer le premier SSID en mode WPA3-Enterprise-192 bits et le second SSID en mode WPA3-Enterprise-Only rendant l'utilisation du MFP-802.11w obligatoire.

Si les appareils WPA2-Enterprise qui ne prennent pas en charge le MFP-802.11w doivent être dépannés, le deuxième SSID doit être configuré en mode WPA3-Enterprise-Transition, rendant le MFP-802.11w facultatif pour les appareils WPA2-Enterprise.

Si vous choisissez de ne pas configurer le mode 192 bits, vous pouvez choisir de configurer un seul SSID d'entreprise en mode WPA3-Enterprise-Only si tous les appareils prennent en charge le MFP-802.11w, ou en mode WPA3-Enterprise-Transition si aucun appareil ne prend en charge le MFP-802.11w.

Il se peut que l'infrastructure Wi-Fi ne prenne pas en charge WPA3 et que la seule alternative soit de configurer un SSID avec WPA2-Enterprise ;

dans ce cas, il est recommandé d'autoriser les niveaux de sécurité maximaux pris en charge au moins en option : MFP-802.11w, cryptage AES-256-GCM et prise en charge de suites de chiffres robustes dans le serveur d'authentification.

Il est recommandé de définir un plan de migration pour tous les appareils qui ne prennent pas en charge WPA3-Enterprise afin de renforcer les mécanismes de sécurité et de mettre en oeuvre des contre-mesures pour les vulnérabilités publiées.

5.1.2 Configuration du service Wi-Fi

Nous supposerons que l'infrastructure Wi-Fi annoncera un SSID d'entreprise primaire en mode WPA3-Enterprise-192 bits nommé "corp_1X" et un second SSID en mode WPA3-Enterprise-Transition nommé "corp_1X_2" pour desservir les appareils qui ne prennent pas en charge toutes les exigences du mode de sécurité 192 bits.

Les points d'accès annonceront les deux services et les appareils seront dotés de la configuration indiquant, entre autres paramètres, le SSID qui leur correspond. Tous les mécanismes de sécurité en mode 192 bits seront proposés en option sur le SSID en mode WPA3-Enterprise-Transition.

Pour effectuer l'authentification, un canal EAP sera établi entre le client suppliant et le serveur d'authentification via les protocoles 802.1X et RADIUS (jambe utilisateur-contrôleur et jambe contrôleur-serveur respectivement). La communication RADIUS entre le contrôleur et le serveur d'authentification sera protégée par le protocole RadSec (basé sur TLS). Le canal EAP encapsulera la méthode EAP-TLS pour effectuer une authentification basée sur un certificat.

Pour utiliser la **méthode EAP-TLS**, il sera nécessaire de disposer d'une infrastructure PKI pour générer et gérer les certificats des clients et des serveurs. Des services complémentaires tels que des bases de données pour stocker les attributs d'autorisation (un LDAP, un annuaire actif ou toute autre base de données) seront également nécessaires.

Un certificat numérique sera généré pour le serveur d'authentification signé par une autorité de certification à laquelle les clients feront confiance et le certificat vérifiera le nom d'hôte du serveur.

Le serveur d'authentification fera confiance à l'autorité de certification qui signe les certificats du client et vérifiera leur statut de révocation (par exemple avec OCSP : *Online Certificate Status Protocol*).

5.1.3 Déploiement de la configuration du client

Les clients disposeront d'un certificat numérique qui sera signé par une autorité de certification approuvée par le serveur d'authentification. Il est recommandé que le certificat du client comprenne des attributs qui identifient à la fois l'utilisateur et son appareil.

Le serveur d'authentification utilisera certains attributs du certificat pendant le processus d'autorisation pour décider du rôle ou de la politique à appliquer à la session authentifiée (par exemple CN, SAN ou email).

Un protocole ou un mécanisme de configuration du dispositif client doit être défini, de préférence de manière automatisée.

Il est important que le client ne puisse pas modifier les paramètres de configuration, car il pourrait désactiver les vérifications de base qui permettraient d'accéder à un service Wi-Fi usurpé (par exemple, en désactivant la vérification du nom d'hôte et de la racine de l'autorité de certification qui signe le certificat du serveur d'authentification).

La spécification WPA3-v2.0 envisage la possibilité de désactiver l'option qui permet au client d'ajouter une exception de confiance au certificat du serveur d'authentification lorsque la validation échoue (TOD : Trust Override Disable, UOSC : User Override of Server Certificate). Pour les clients qui ont été configurés en déploiement, il est recommandé d'indiquer l'OID TOD-STRICT : "1.3.6.1.4.1.1.40808.1.3.1" dans le certificat du serveur d'authentification afin d'éviter toute interaction et exception en cas d'échec de la validation.

Un exemple des paramètres à configurer dans les clients :

[Figure 5] Déploiement et configuration du client

	Client WPA3-Enterprise-192-bits	Client WPA3-Enterprise-Transition
SSID de l'entreprise	“corp_1X”	“corp_1X_2”
MFP-802.11w	Requis	En option
Cryptage	AES-256-GCM	AES-128-CCMP Optionnel :AES-256-GCM
Références	Clé privée du client et certificat du client (signé par CA-root-client)	
Données du serveur Radius à vérifier obligatoirement	Certificat de l'AC-serveur racine nom d'hôte (par exemple : "radius.corp.es")	

5.2 Phase 1 : Association MAC et authentification

Une fois que le service Wi-Fi a été configuré et que les clients ont été déployés, les phases d'accès au service Wi-Fi commencent.

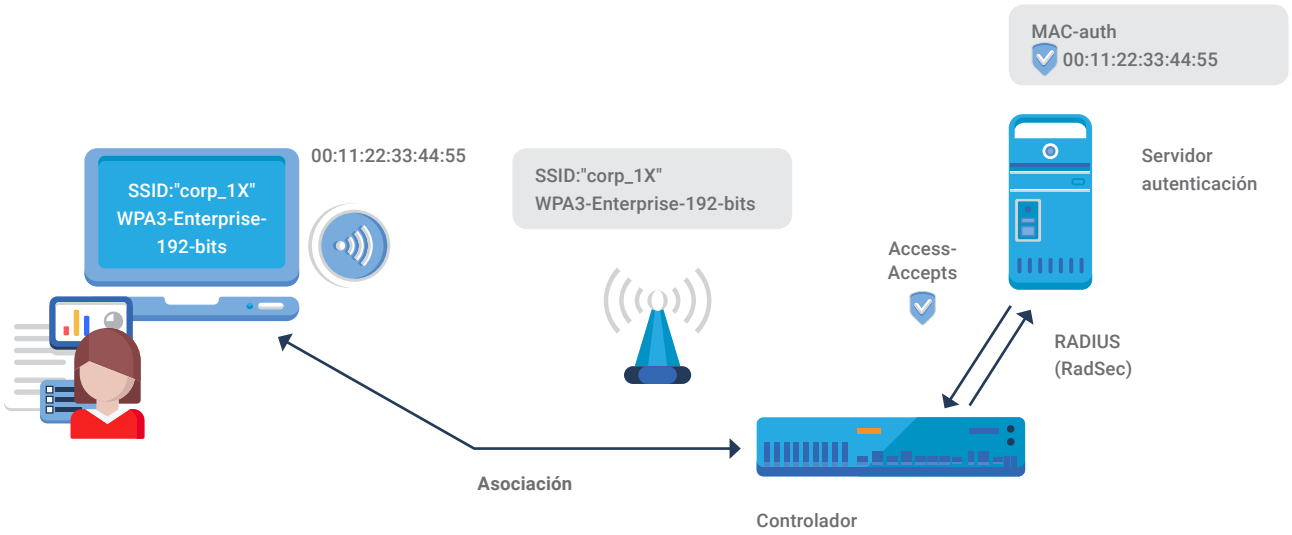
Dans la première phase, le client ne dispose d'aucun mécanisme lui permettant d'avoir confiance dans l'infrastructure offrant le service Wi-Fi. La seule information qui est validée est le nom SSID des annonces de *balises*. Lorsqu'une annonce de service est reçue, l'association est initiée.

Le client pourrait utiliser des mécanismes non standard pour la détection des services malveillants, comme la cohérence de la géolocalisation, l'*empreinte digitale* des fonctions annoncées dans les balises et les adresses BSSID des points d'accès. Toutes les données de la trame de balise, qui comprennent le SSID et les adresses MAC, sont facilement falsifiables et ne doivent jamais être utilisées comme seul système d'authentification.

Pendant l'association, décrite à la **figure 6**, il est recommandé que l'infrastructure de l'entreprise effectue une première authentification basée sur l'adresse MAC du client sans fil, bien que nous sachions qu'il s'agit d'un attribut qui peut être facilement usurpé.

Pour l'authentification MAC, deux types de politiques peuvent être combinés : basée sur une liste blanche ou une liste noire. Une liste blanche peut contenir toutes les adresses MAC des clients d'entreprise configurés lors du déploiement. Une liste noire peut contenir toutes les adresses MAC considérées comme malveillantes.

Une fois que le service Wi-Fi a été configuré et que les clients ont été déployés, les phases d'accès au service Wi-Fi commencent



[Figure 6]
Association et authentification MAC

Pour donner un exemple, vous pouvez donner accès à la phase 2 (802.1X) à toutes les adresses MAC qui figurent sur une liste blanche, en bloquant l'association à toute adresse MAC inconnue ou figurant sur une liste noire.

Autre exemple, vous pouvez omettre la liste blanche et autoriser par défaut toute adresse MAC qui ne figure pas sur une liste noire.

L'authentification basée sur l'adresse MAC nous permet de bloquer et de protéger l'accès au serveur d'authentification. Par exemple, lors de la détection d'une tentative de DoS contre la norme 802.1X, nous pourrions mettre sur liste noire toutes les adresses MAC participantes et les bloquer de manière permanente ou pendant une période de temps définie, comme mécanisme de confinement.

5.3 Phase 2 : Authentification et autorisation 802.1X avec EAP-TLS

Si le client passe avec succès l'association et l'authentification MAC, l'infrastructure invite le client à utiliser le protocole 802.1X pour établir une communication EAP avec le serveur d'authentification (étapes 1 et 2 de la **Figure 7**). La méthode à utiliser sur le canal EAP est EAP-TLS.

Le serveur d'authentification, après avoir vérifié l'identifiant du client, enverra son certificat (étape 3) afin que le client puisse vérifier le nom d'hôte et décider s'il fait confiance à l'autorité de certification qui signe le certificat (étape 4), selon la configuration effectuée lors du déploiement des clients.

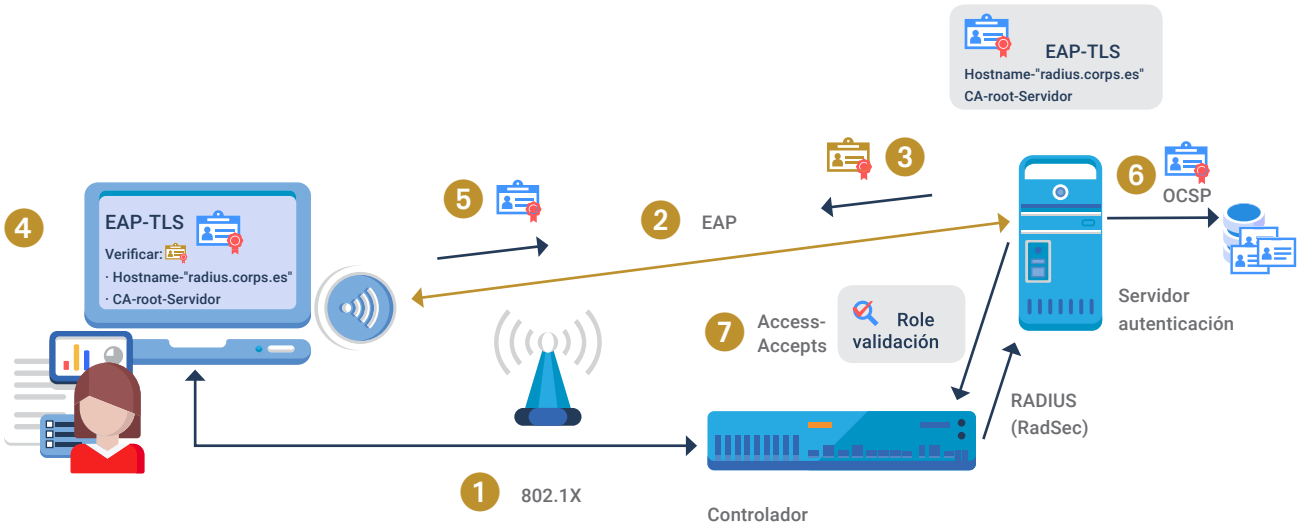
Si tout est correct, le client enverra son certificat au serveur d'authentification (étape 5). Le serveur vérifiera les attributs du certificat du client et demandera sa validité en utilisant les ressources de l'autorité de certification de confiance qui signe le certificat du client, par exemple OCSP (étape 6).

Si le serveur conclut que l'authentification est réussie, il procède à l'autorisation du dispositif client.

Pour l'autorisation, le serveur collectera un certain nombre d'attributs provenant de différentes sources et, avec les données obtenues lors du processus d'authentification, déterminera le rôle résultant à appliquer à la session du dispositif client.

Les attributs d'autorisation peuvent être statiques, comme les données personnelles de l'utilisateur, ou dynamiques, comme les rapports sur l'état de santé du dispositif, la localisation physique, le comportement du réseau par l'application de signatures basées sur des modèles, etc.

Si le client passe avec succès l'association et l'authentification MAC, l'infrastructure invite le client à utiliser le protocole 802.1X pour établir une communication EAP avec le serveur d'authentification



[Figure 7]
Authentification via EAP-TLS

Le rôle résultant peut contenir des paramètres tels que le VLAN, les filtres de pare-feu à appliquer, le contrôle de la bande passante, ou tout autre paramètre que l'infrastructure du réseau permet d'appliquer. Si le serveur détermine qu'il ne dispose pas de suffisamment de données pour se prononcer sur l'état de santé du dispositif, il peut appliquer un "rôle de validation" pour fournir les services minimums nécessaires à la réception d'un rapport sur l'état de santé du dispositif (étape 7).

A la fin du processus d'authentification et d'autorisation :

- Le client peut calculer la PMK (Pairwise Master Key).
- Le serveur d'authentification utilisera le canal RADIUS pour envoyer tous les attributs d'autorisation et de calcul de la PMK nécessaires au contrôleur ou au point d'accès.

Ensuite, la poignée de main à 4 voies est effectuée entre le point d'accès et le client pour vérifier la confiance mutuelle en dérivant de la PMK les clés de chiffrement pour le trafic sans fil (PTK et GTK).

Tant que le dispositif client reste associé au service Wi-Fi, le canal EAP reste actif pour effectuer des réauthentifications avec le serveur et la régénération des clés cryptographiques selon les intervalles définis.

5.4 Phase 3 : L'accès au réseau et l'état de santé de l'appareil

Une fois que l'authentification a été passée, que les attributs d'autorisation ont été appliqués et que la poignée de main quadruple a été achevée, le client a accès au réseau de données (étape 1 de la **figure 8**). Les attributs d'autorisation définiront la politique d'accès et les services autorisés (étape 2).

Une fois que l'authentification a été passée, que les attributs d'autorisation ont été appliqués et que la poignée de main quadruple a été achevée, le client a accès au réseau de données

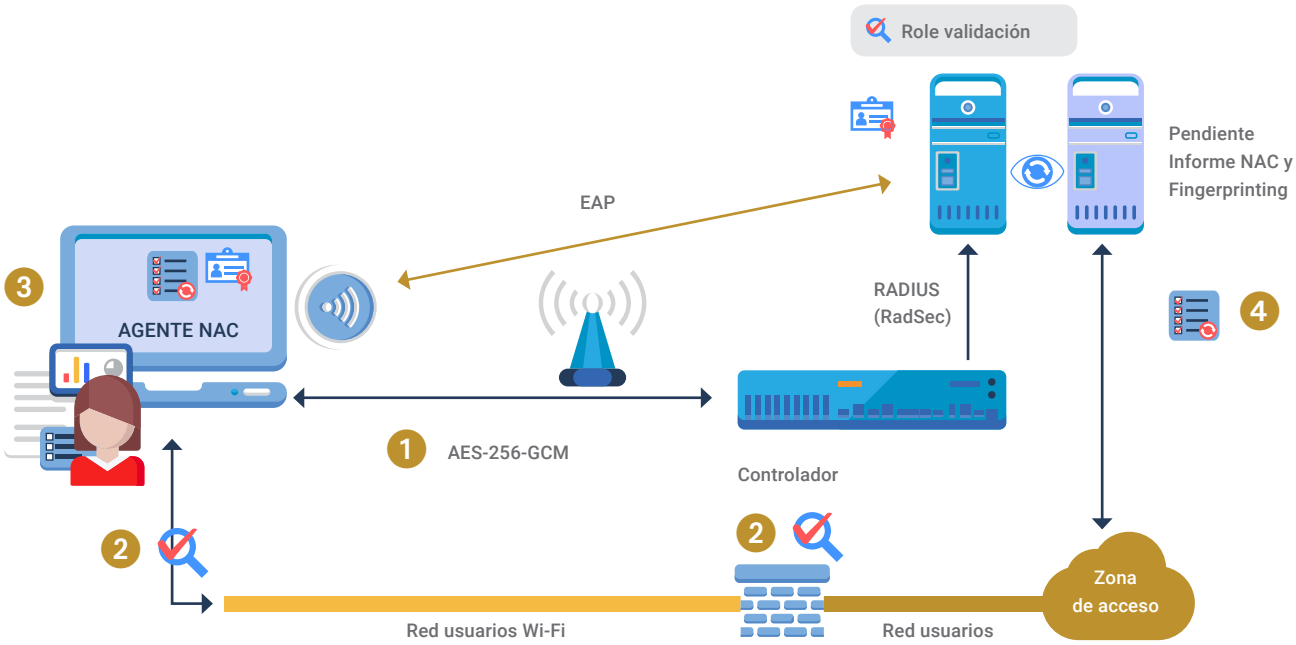
Le premier service de base offert au client est le DHCP qui permettra au client de configurer l'interface IP (adresse IP, masque de sous-réseau, route par défaut, serveur DNS et autres paramètres d'entreprise). L'utilisation du DHCP par le client sera obligatoire pour éviter les configurations manuelles. Pour simplifier les processus d'enregistrement et d'audit, l'attribution des adresses IP sera statique pour chaque appareil, chaque adresse IP étant associée à une adresse MAC.

Pour simplifier la gestion des politiques de sécurité, il est recommandé d'utiliser des noms d'utilisateurs, des groupes ou des rôles plutôt que des adresses IP. Il est recommandé d'enregistrer le mappage entre l'adresse IP et le nom d'utilisateur afin de pouvoir y faire référence dans les politiques et les journaux d'accès.

Toutes les communications directes entre les clients seront bloquées pour éviter la propagation des infections. Si une communication directe entre les clients est nécessaire, il convient d'étudier des alternatives pour offrir le même service ou permettre des solutions de substitution.

Toutes les communications du réseau seront analysées et protégées par des équipements de sécurité (pare-feu, IDS/IPS, filtrage des URL, analyse des logiciels malveillants, netflow, etc.)

Les outils d'analyse de réseau vous permettent de générer des attributs dynamiques qui seront utilisés dans le processus d'autorisation pour déterminer le rôle de l'utilisateur. L'empreinte ou le profilage peut être réalisé en analysant les requêtes DHCP, l'agent utilisateur des requêtes http, les applications identifiées par le pare-feu, les modèles de session netflow, etc.



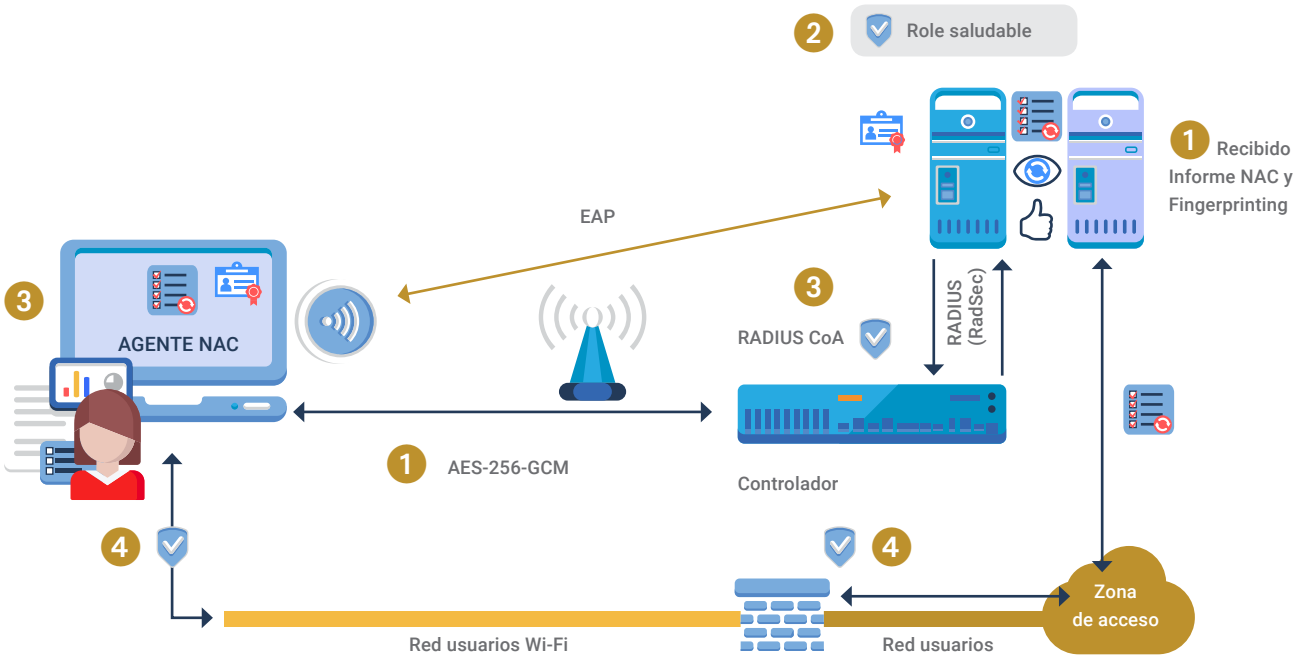
[Figure 8]
Vérification de l'état du dispositif par l'agent NAC

Pour une meilleure analyse et un meilleur profilage, il est recommandé d'utiliser un programme, un agent ou un système (agent NAC) installé sur l'ordinateur de l'utilisateur qui accèdera au réseau pour vérifier que le terminal auquel on accède possède les exigences minimales de sécurité (étape 3).

Ces exigences minimales recommandées sont les suivantes :

- Le système d'exploitation de l'ordinateur client est à jour, avec des versions ne datant pas de plus de deux mois (ou selon la politique de sécurité de l'organisation).
- L'équipement est doté d'un système de protection, tel qu'un antivirus ou une solution EDR, installé et en fonctionnement, avec des mises à jour datant de moins de deux mois (ou selon l'analyse des risques effectuée).

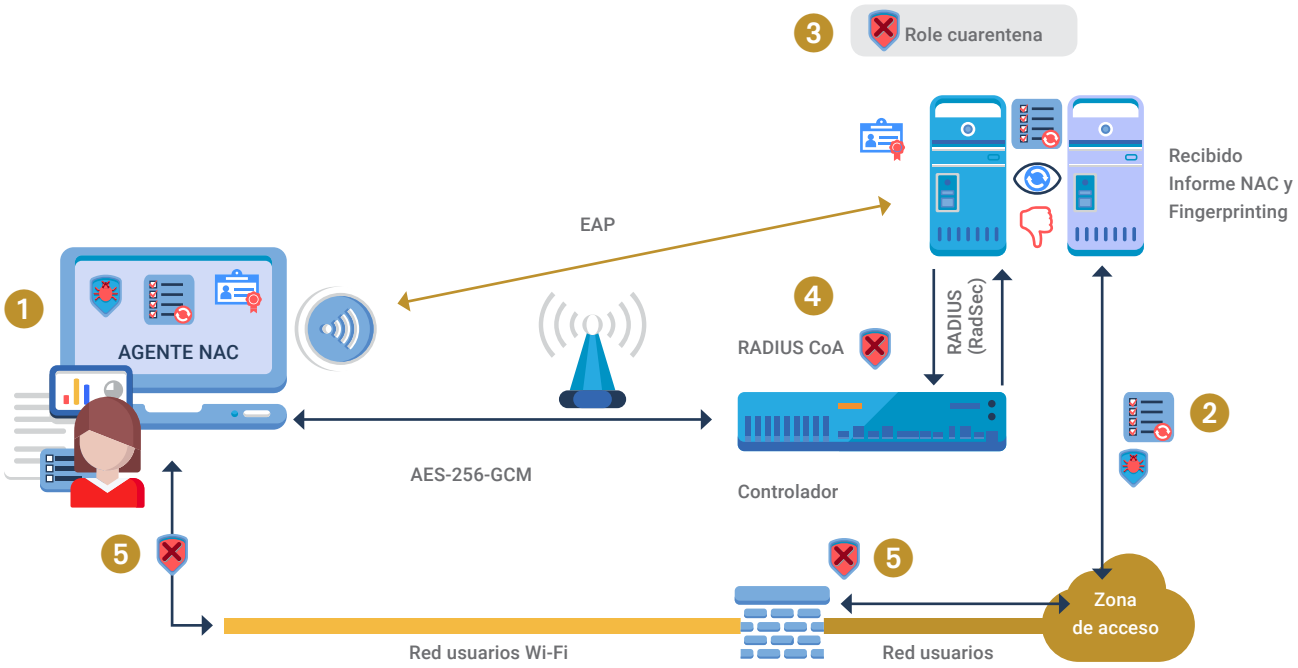
L'agent NAC enverra l'état du périphérique à un serveur NAC pour vérifier la santé du périphérique connecté (étape 4). Cet agent sera exécuté périodiquement (il est recommandé de le faire toutes les 30 secondes), ce qui permet de savoir si l'état du dispositif a changé, de sorte que vous pouvez définir et appliquer différentes politiques d'accès au réseau en fonction de la conformité des exigences d'accès au réseau.



[Figure 9]
Dispositif en état de santé

Les rapports d'état de l'agent NAC et les attributs d'analyse seront mis à la disposition du serveur d'authentification afin qu'il puisse prendre la décision quant au rôle à appliquer à une session de dispositif.

Au départ, après l'authentification, le serveur d'authentification peut appliquer le **"rôle de validation"** jusqu'à ce que le rapport sur l'état de santé soit reçu. Si le rapport est sain, via un CoA Radius, il passera au **"rôle d'état sain"** (Figure 9).



[Figure 10]
Dispositif en état de quarantaine

Si, en revanche, le rapport indique qu'il n'est pas conforme aux exigences de sécurité, il passe au "rôle de quarantaine", limitant l'accès aux seuls services minimums nécessaires pour résoudre les problèmes détectés **(figure 10)**.

Il sera également possible de modifier l'autorisation de mise en quarantaine des clients qui ont été considérés comme sains si un changement de statut est détecté.

Par exemple, une modification du type de dispositif ou de l'*empreinte* du système d'exploitation lors de l'analyse de l'agent utilisateur ou du DHCP, un modèle de trafic suspect ou l'utilisation d'une application non autorisée lors de l'analyse du flux net ou de l'identification de l'application du pare-feu, l'accès à une URL malveillante, le téléchargement d'un logiciel malveillant, etc.

5.5 Phase 4 : Établir le tunnel VPN crypté

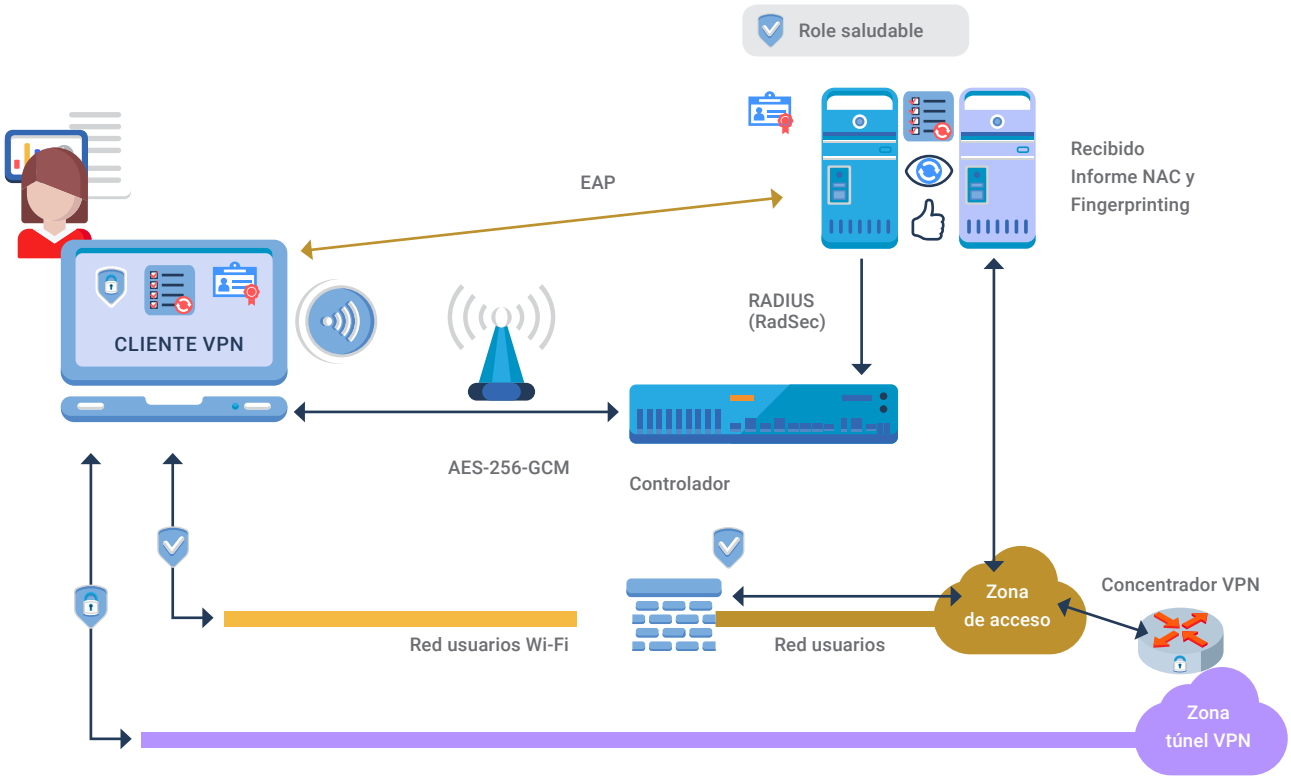
Le cryptage sans fil sera complété par l'établissement d'un tunnel VPN crypté avec le concentrateur VPN de l'entreprise. Cela étend le cryptage du client à une zone de confiance de l'entreprise, les informations en transit étant protégées par des mécanismes de cryptage et d'authentification robustes.

Il est recommandé de consulter les directives spécifiques concernant les solutions de tunneling VPN afin de déterminer la solution qui répond aux besoins de votre entreprise. En général, utilisez le niveau maximal de sécurité pris en charge par le produit et les clients VPN.

Les suites cryptographiques suivantes peuvent être prises comme référence :

[Figure 11] Algorithmes cryptographiques recommandés

ALGORITHME	MEDIO	ALTO
Cryptage Standard avancé (AES)	128 bits	256 bits
Signature numérique Algorithme de signature numérique à courbe elliptique (ECDSA)	256 bit curve	384 bit curve
Échange de clés Diffie-Hellman à courbes elliptiques (ECDH)	256 bit curve	384 bit curve
Hachage Algorithme de hachage sécurisé (SHA)	SHA-256	SHA-384



[Figure 12]
Configuration du tunnel VPN

En fonction de la solution mise en oeuvre et de son intégration avec la solution Wi-Fi, le processus d'association, d'authentification, de vérification du statut et d'établissement du tunnel VPN peut se faire avec un seul agent ou une seule application.

D'autre part, nous pouvons trouver des solutions non intégrées dans lesquelles, d'une part, nous avons le suppliant en charge de l'association et de l'authentification, d'autre part, un agent NAC en charge du rapport d'état et enfin un client VPN en charge de l'établissement du tunnel crypté.

Quelle que soit la solution, le tunnel VPN doit être établi dès que possible, juste après l'accès au réseau, afin de sécuriser toutes les communications. Mais il serait compréhensible de prendre la décision de ne pas autoriser l'établissement du tunnel VPN jusqu'à ce que le dispositif obtienne le rôle d'état sain.

Une fois le tunnel mis en place, le client aura deux connexions différentes, la connexion "Réseau utilisateur Wi-Fi" et la connexion "Réseau tunnel VPN". Cette dernière sera l'interface par défaut pour tout le trafic client.

Le "réseau utilisateur Wi-Fi" avec un chiffrement AES-GCM-256 du client au point de livraison du plan de données du contrôleur transportera l'encapsulation chiffrée du "réseau tunnel VPN". En quittant le contrôleur, le "réseau tunnel VPN" sera encapsulé et passera par toute infrastructure existante jusqu'au concentrateur VPN qui fournit un canal authentifié et crypté du dispositif du client au concentrateur VPN lui-même.

Malgré le double cryptage du "réseau utilisateur Wi-FI" et du "réseau tunnel VPN", des sessions sécurisées seront établies au niveau de l'application avec des protocoles qui cryptent le canal du client au serveur d'application (par exemple https et TLS). Et sur ce canal d'application, les informations envoyées seront protégées de manière à ce que seuls les utilisateurs ou les destinataires autorisés puissent y accéder (par exemple, en chiffrant les courriels ou les fichiers avec la clé publique du destinataire autorisé, soit par PGP ou par certificat).

Les différentes couches de cryptage protègent les communications contre les vulnérabilités telles que le Kr00k, car si un attaquant parvient à décrypter les trames Wi-Fi, il ne pourra voir que les trames cryptées à travers le tunnel VPN.

Malgré le double cryptage du "réseau utilisateur Wi-FI" et du "réseau tunnel VPN", des sessions sécurisées seront établies au niveau de l'application avec des protocoles qui cryptent le canal du client au serveur d'application

6. Recommandations en matière de sécurité

Cette section contient une série de recommandations de sécurité qui doivent être prises en compte lors du déploiement du réseau. Certains d'entre eux ont déjà été indiqués dans les sections précédentes.

Pour de plus amples renseignements sur les informations décrites ici, veuillez consulter les guides indiqués dans la section Références.

6.1 Premières considérations

- Procéder à l'**analyse et à la gestion des risques** avant de commencer le déploiement du réseau, notamment la disponibilité des systèmes et des services, l'intégrité des données et des transactions, le niveau de confidentialité, l'authenticité des données échangées et la traçabilité de ces échanges sur les équipements à utiliser, les connexions à établir entre eux et qui les exploitera et comment ils seront exploités

- **Envisagez un accès filaire.** Un accès filaire sera toujours moins exposé aux menaces. On ne peut exclure la possibilité de compromettre l'appareil en activant l'interface sans fil par l'exploitation d'une vulnérabilité inconnue, avec l'aggravation de la réussite sans contact physique et à longue distance.

- **Analyser l'équipement à acheter.** Vérifiez la capacité à prendre en charge les protocoles requis et la publication des mises à jour par le fabricant. Appliquer la redondance sur les équipements qui, en cas de panne, d'erreur ou d'attaque, ne permettent pas le fonctionnement normal du service. Faites un inventaire des dispositifs et révisez-le périodiquement.

- **Assurer l'accès physique** aux locaux de l'organisation, notamment aux zones où sont déployés les équipements.

- **Effectuez une analyse de la portée des rayonnements** des points d'accès (cette analyse doit être incluse dans l'analyse de sécurité périodique). Définissez l'emplacement des points d'accès et essayez de les éloigner du périmètre extérieur de l'organisation.

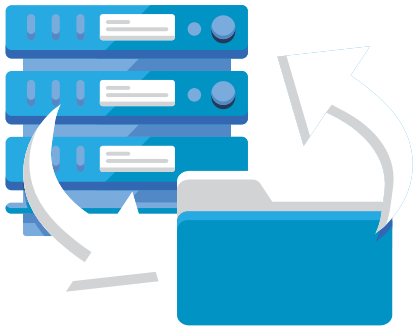
- Développez un ensemble de **politiques de sécurité** qui définissent qui a un accès physique aux équipements du réseau, qui a accès à leur administration, et quelles procédures doivent être exécutées en cas d'intrusion. Cette politique doit également préciser les méthodes à utiliser pour rétablir le fonctionnement normal des dispositifs en cas de défaillance, d'erreur, d'intrusion, etc. Des contrôles de conformité périodiques doivent être effectués pour s'assurer que les politiques de sécurité sont respectées.

- Pour empêcher tout accès malveillant au réseau filaire des points d'accès, authentifiez et autorisez l'accès filaire des points d'accès à l'aide de la norme **802.1X avec EAP-TLS** sur les commutateurs d'accès.

- **Former** les utilisateurs à l'utilisation de cette technologie et aux risques associés à son utilisation.

6.2 Mises à jour et sauvegardes

- Maintenez vos **appareils à jour** avec la dernière version. Téléchargez les mises à jour par l'intermédiaire des fournisseurs officiels des fabricants, pour autant que ce service soit proposé via un protocole de communication sécurisé.
- Faites des **sauvegardes** périodiques, en les stockant sur des ordinateurs autres que ceux qui sont sauvegardés.
- Établir des mécanismes qui définissent les **procédures de recherche** d'informations, ainsi que des mécanismes pour tester son bon fonctionnement avant sa mise en oeuvre.
- Transférer des fichiers via l'option de téléchargement de fichiers locaux (fichier local) ou **SCP**. Désactiver l'utilisation de FTP et TFTP.



6.3 Méthodes et conditions d'accès

- Créez un **réseau de gestion dédié** qui ne transporte que le trafic de gestion et d'administration.
- Utilisez des **méthodes d'accès sécurisé à l'ordinateur**, telles que l'interface de ligne de commande (CLI), l'interface Web (Web GUI) ou l'accès SSH (port 22 TCP) avec des listes d'accès. Demandez toujours les informations d'identification de l'utilisateur pour accéder aux ordinateurs, quelle que soit la méthode utilisée.

- Établir des procédures sécurisées qui permettent de **contrôler l'établissement et la modification des justificatifs d'accès** (mot de passe utilisateur ou certificat).

- Définissez une durée maximale d'inactivité ***(délai de session) après laquelle*** l'ordinateur sera verrouillé et l'utilisateur sera invité à saisir à nouveau ses informations d'identification.

- Générer le **mot de passe de l'utilisateur et les informations d'identification du certificat individuellement** et selon la politique de mot de passe correspondante pour faciliter le processus de traçabilité de l'utilisateur. Utilisez des canaux sécurisés pour transférer des informations entre les dispositifs tels que des certificats, des agents, des logiciels, etc. Installez les certificats d'authentification Wi-Fi de manière à ce qu'ils ne puissent pas être exportés ou supprimés.

- Bloquez tout accès indésirable aux systèmes, soit par des **pare-feu**, soit en configurant des restrictions d'accès sur les ordinateurs eux-mêmes.

- Configurez les **trois mécanismes de sécurité** du modèle défini ci-dessus pour la connexion des clients utilisateurs via Wi-Fi (802.1X, agent NAC et tunnel VPN crypté).

- Utilisez l'accès Wi-Fi via le protocole **IEEE 802.1X avec la méthode EAP-TLS**. Désactiver l'option permettant d'utiliser TLSv1.0 et TLSv1.1.

- Configurez l'**agent NAC pour qu'il** vérifie l'état de santé du périphérique toutes les 30 secondes.

- Utilisez **IKEv2** pour le tunnelage IPsec.

- Utilisez des **systèmes d'authentification centralisés** tels que les serveurs RADIUS et protégez les canaux de communication avec des protocoles sécurisés tels que RadSec

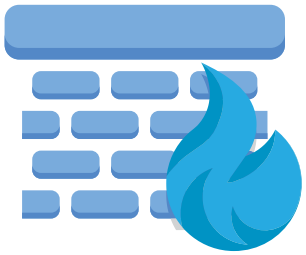
6.4 Configuration des services sur votre ordinateur

- Supprimez toutes les **informations qui sont configurées par défaut** pour les services que vous allez utiliser.
- Si possible, utilisez un **serveur DHCP** extérieur au contrôleur de point d'accès. En outre, il est recommandé de configurer l'attribution d'une adresse IP fixe pour chaque client et de faire en sorte qu'une adresse IP ne soit pas obtenue tant que l'utilisateur n'est pas authentifié.
- Faites en sorte que tous les appareils soient synchronisés dans le temps en utilisant **NTP** et en activant l'authentification.
- Utilisez des serveurs **SNMP et *syslog*** externes pour collecter des données spécifiques sur les ordinateurs et les transactions sur le réseau. Utilisez **SNMPv3** parce qu'il comprend des améliorations de sécurité en matière d'authentification et de livraison de données cryptées par rapport à SNMPv1 et SNMPv2.
- Activez uniquement les **protocoles sécurisés** sur le contrôleur du point d'accès.
- Prévenir les attaques par déni de service en établissant des contrôles de **diffusion et de multidiffusion**.
- Interdisez ou désactivez toutes les configurations qui utilisent **IPv6** si vous ne comptez pas l'utiliser sur votre réseau.
- Activez le mode **FIPS** si disponible.
- Utilisez les **listes d'accès** pour configurer les services activés pour chaque ordinateur ou périphérique client.
- Activez le système de détection d'intrusion **sans fil (Wireless IDS)** du contrôleur Wi-Fi s'il est disponible.

Désactivez toutes les configurations qui utilisent IPv6 si vous ne comptez pas l'utiliser sur votre réseau

6.5 Politiques d'utilisation et règles de pare-feu

- Établir des **rôles d'utilisateur** qui permettent un accès hiérarchique (avec différentes autorisations) aux services définis.
- Limiter le trafic entre les utilisateurs connectés au réseau : interdire la communication de pair à pair en empêchant le **trafic entre les utilisateurs**, limiter l'accès aux ports, etc.
- Configurez des listes d'accès **(ACL)** d'adresses IP valables uniquement pour les clients Wi-Fi.
- **Limitez les ports** qui doivent être ouverts sur les équipements du réseau aux services qu'ils utilisent et effectuez de préférence une identification et un **filtrage des applications** indépendamment du port de protocole utilisé.
- Inclure des mécanismes qui empêchent ou atténuent l'***usurpation ARP*** et l'***usurpation IP*** afin d'éviter les attaques de type *Man-In-The-Middle* et les attaques de clonage/usurpation d'adresses IP.
- Établissez un contrôle de défense en configurant un ensemble de règles de **pare-feu** pour le contrôleur.



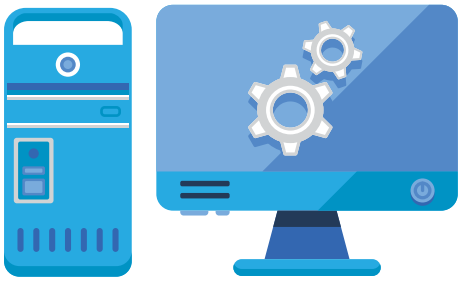
6.6 Événements et surveillance du système

Un point important à prendre en compte est la collecte des événements et la surveillance des ressources du système pour détecter les éventuelles anomalies qui pourraient affecter le service.

Parmi les exemples d'indicateurs à surveiller, citons le processeur, la mémoire RAM, l'espace de stockage disponible, les processus actifs, le trafic à travers les interfaces physiques, les sessions établies, le nombre d'utilisateurs associés et authentifiés, le temps de réponse des services tels que Radius, DHCP et DNS, les enregistrements d'authentification et d'association, la température de l'équipement, etc.

Les ressources peuvent être surveillées à l'aide de SNMPv3 ou de protocoles propriétaires de la solution du fabricant. Aujourd'hui, il est courant de pouvoir consulter l'état des équipements à l'aide de requêtes web via API-REST. Il est également courant d'utiliser des mécanismes tels que le syslog pour exporter les événements du système vers une console centrale.

Il est fortement recommandé de disposer d'un outil de type SIEM ayant des capacités de corrélation sur les données surveillées et les événements système collectés. Vous pouvez même effectuer une analyse basée sur le dispositif et le comportement de l'utilisateur (UEBA).



Outre la surveillance et la corrélation, toutes les mesures et tous les événements sont nécessaires pour mener une enquête médico-légale en cas d'incident. Il est important de définir une politique de stockage et de traitement historique des événements pour pouvoir accéder aux données en cas de besoin lors d'un incident de sécurité.

6.7 D'autres recommandations

- Effectuez **régulièrement des analyses de vulnérabilité** et évaluez d'autres configurations qui améliorent la sécurité de votre réseau.
- **Surveillez le trafic réseau** et effectuez une recherche périodique d'anomalies.
- Mettre en oeuvre des systèmes de détection d'intrusion **(IDS)** pour détecter d'éventuelles anomalies qui génèrent des alarmes..

7. Décalogue de sécurité de base

Ce décalogue de bonnes pratiques vise à poser les bases des mesures de sécurité à prendre en compte lors de l'installation d'un réseau Wi-Fi dans un environnement d'entreprise.

1. **Envisagez d'éliminer tout accès sans fil et de donner la priorité aux accès câblés. Effectuez l'analyse et la gestion des risques associés avant la mise en oeuvre du réseau Wi-Fi. Analyser les équipements nécessaires à acquérir, planifier la couverture radio nécessaire et définir la politique de sécurité applicable.**
2. **Effectuez un inventaire des dispositifs en examinant périodiquement votre inventaire de dispositifs et les vulnérabilités potentielles. Maintenez tous les équipements à jour, les sauvegardes et les procédures de récupération testées.**
3. **Créez un réseau de gestion dédié, ne transportant que le trafic de gestion et d'administration, en utilisant des protocoles sécurisés.**
4. **Générer des certificats avec les données de l'utilisateur et du dispositif. Créez différents rôles d'utilisateur pour une meilleure application de la politique de sécurité.**
5. **Utilisez des systèmes d'authentification centralisés tels que des serveurs RADIUS utilisant des canaux sécurisés tels que RadSec.**
6. **Effectuez une attribution DHCP d'une adresse IP fixe pour chaque client/appareil sur chacun des différents réseaux.**
7. **Configurez les clients pour utiliser 802.1X-EAP-TLS, l'agent NAC et le tunnel VPN crypté comme recommandé.**
8. **Limitez l'accès physique aux ordinateurs ainsi que l'accès logique en fonction des rôles définis et désactivez le service lorsqu'ils ne sont pas utilisés.**
9. **Mettre en oeuvre des systèmes de détection d'intrusion (IDS) pour détecter d'éventuelles anomalies qui génèrent des alarmes.**
10. **Surveillez le trafic réseau et effectuez une recherche périodique d'anomalies.**

8. Références

CCN-STIC-406 Sécurité dans les réseaux sans fil :	http://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/71-ccn-stic-406-seguridad-en-redes-inalambricas/file.html
CCN-STIC-647b Configuration sécurisée des équipements réseau Aruba pour les environnements Wi-Fi :	http://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/600-guias-de-otros-entornos/2701-ccn-stic-647b-configuracion-segura-de-equipos-de-red-aruba-para-entornos-wifi/file.html
CCN-STIC-816 Sécurité des réseaux sans fil dans l'ENS :	http://www.ccn-cert.cni.es/pdf/guias-de-acceso-publico-ccn-stic/2317-ccn-stic-816-seguridad-en-redes-inalambricas-en-el-ens/file.html
CCN-STIC-836 Sécurité VPN dans le cadre de l'ENS :	https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2299-ccn-stic-836-seguridad-en-vpn-en-el-marco-del-ens/file.html
Spécification WPA3-v2.0 publiée le 20/12/2019 :	https://www.wi-fi.org/file/wpa3-specification

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es


cn-cert
centro criptológico nacional
CCN
centro criptológico nacional