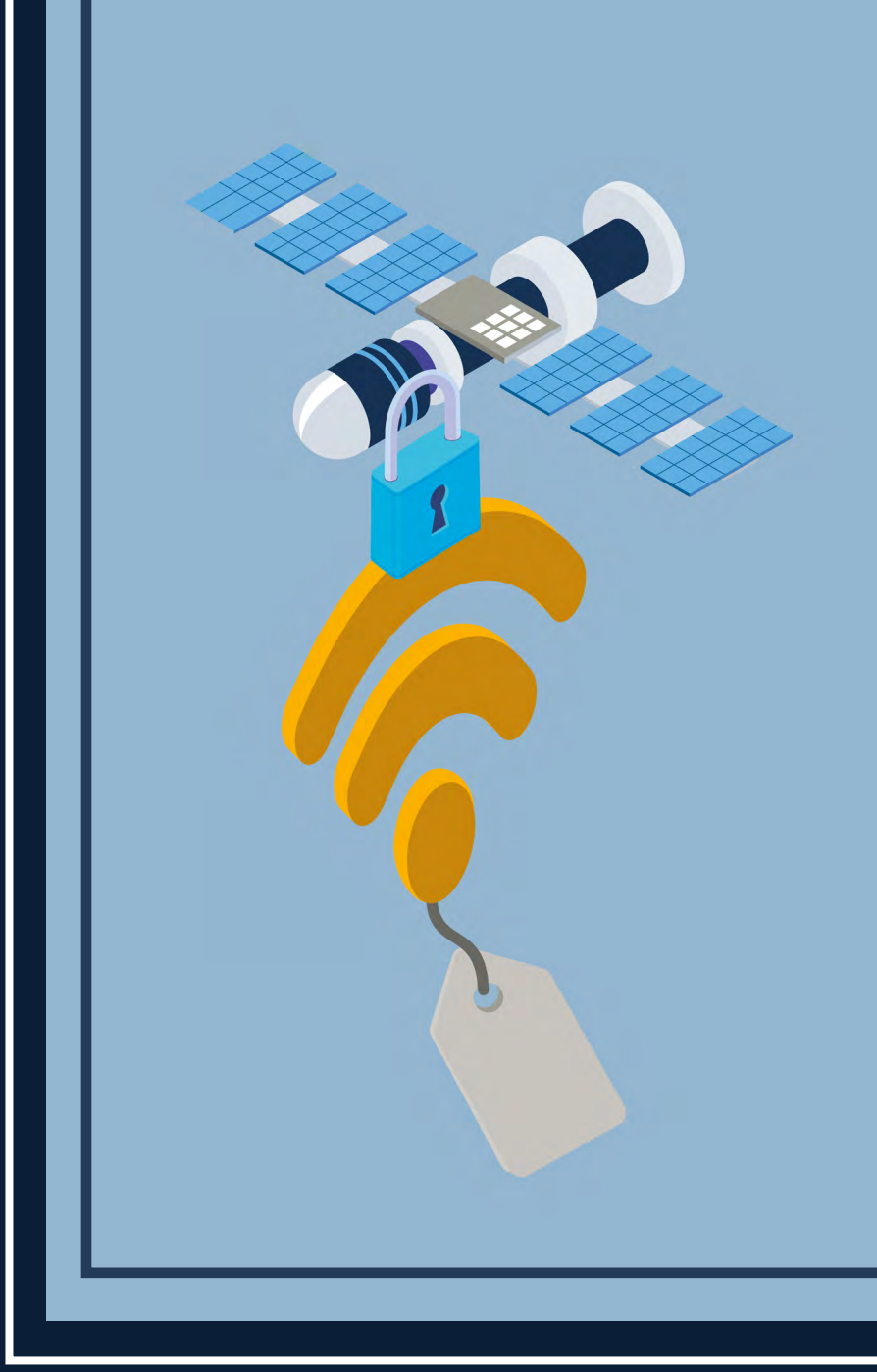
CCN-CERT

BP/11



Security recommendations in corporate Wi-Fi networks

GOOD PRACTICE REPORT

JULY **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Edit

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 CRIPTOLOGICO NACIONAL, c=ES
2021.08.16 11:26:35 +02'00'

Centro Criptológico Nacional, 2021

Date of edition: July 2021

Index

1. About CCN-CERT, National Governmental Cert

The CCN-CERT is the Computer Security Incident Response Team of the National Cryptologic Centre, CCN, attached to the National Intelligence Centre, CNI. This service was created in 2006 as the **Spanish National Governmental** CERT and its functions are set out in Law 11/2002 regulating the CNI, RD 421/2004 regulating the CCN and in RD 3/2010, of 8 January, regulating the National Security Framework (ENS), modified by RD 951/2015 of 23 October.

Its mission, therefore, is to contribute to the improvement of Spanish cybersecurity, by being the national alert and response centre that cooperates and helps to respond quickly and efficiently to cyber-attacks and to actively confront cyber-threats, including the coordination at state public level of the different Incident Response Capabilities or Cybersecurity Operations Centres.

Its ultimate aim is to make cyberspace more secure and reliable, preserving classified information (as stated in art. 4. F of Law 11/2002) and sensitive information, defending Spain's Technological Heritage, training expert personnel, applying security policies and procedures and using and developing the most appropriate technologies for this purpose.

In accordance with these regulations and Law 40/2015 on the the Public Sector Legal System, the CCN-CERT is responsible for the management of cyber-incidents affecting any public body or company. In the case of critical public sector operators, cyber-incidents will be managed by the CCN-CERT in coordination with the CNPIC.

2. Introduction to Wi-Fi wireless networks

A wireless network can be broadly defined as a network of devices capable of communicating with each other via electromagnetic waves and without the need for wires (wireless).

Wireless networks can be classified into personal wireless networks (WPANs), such as those based on infrared or Bluetooth, wireless local area networks (WLANs), such as IEEE 802.11 or HomeRF, and wireless metropolitan or wide area networks (WMAN or WWAN): networks of different generations such as 2G/3G/4G/5G and technology standards such as CDMA and GSM, GPRS, UMTS, WiMAx (IEEE 802.16) or LTE.

There are many types of wireless networks that differ in their characteristics such as their technology, communication standard, architecture, etc. This guide focuses exclusively on WLAN or Wi-Fi networks. These wireless networks are based on the IEEE 802.11 standard and the products are certified by the Wi-Fi Alliance to ensure interoperability.

The main components of a Wi-Fi wireless network are::

- **Client devices.** These are the user devices that request connection to the wireless network for user data transfer (laptops, smartphones, Smart TVs, etc.).
- **Access** Points (APs). These are devices that are part of the wireless infrastructure and are responsible for connecting client devices to each other or to the organization's wired network infrastructure.

A wireless network can be broadly defined as a network of devices capable of communicating with each other via electromagnetic waves and without the need for wires (wireless)

There are three common topologies when talking about wireless Wi-Fi networks: ad-hoc, infrastructure and mesh.

1. In the **ad-hoc topology**, each node is part of a network in which all members have the same role and are free to associate with any node..

2. In the **infrastructure topology** there is a central node (AP), which serves as a link for all clients. This node will typically serve to route traffic to a conventional network or to other networks by converting frames in 802.11 format to the native format of the distribution system (typically 802.3 Ethernet). In order to establish communication, all nodes must be within the coverage area of the AP or its repeaters and be aware of the network parameters.

3. The **mesh topology** mixes the two previous ones (mesh). In this topology, a device acts as an AP and in turn creates a point-to-point network, where any client can connect and communicate with a device that is not in its coverage range, as the connectivity expands as a mesh.

The IEEE 802.11 standard defines the use of the two lower levels of the OSI architecture or model (physical layer and data link layer), specifying their rules of operation in a WLAN network. The physical layer has evolved through the publication of extensions and modifications to the 802.11 standard. Each evolution of the physical layer is named after the working group in charge of the evolution, for example 11b, 11a, 11g, 11n, 11ac, 11ax, 11be, etc. To simplify the identification of technological evolutions, the Wi-Fi Alliance assigns correlative numerical identifiers for each physical layer, with "Wi-Fi 4" being equivalent to 802.11n, "Wi-Fi 5" to 802.11ac, "Wi-Fi 6" to 802.11ax and, as yet unconfirmed, "Wi-Fi 7" to 802.11be.

Regarding security mechanisms, the protocol that was implemented in the original IEEE 802.11 standard is called WEP (Wired Equivalent Privacy). This protocol has been declared insecure due to multiple vulnerabilities detected and is therefore considered unsuitable for wireless networks requiring a minimum of security. Following the vulnerabilities of WEP, IEEE 802.11i was developed as an amendment to the original 802.11 standard with more robust security mechanisms to counter the problems of WEP.

The protocol that was implemented in the original IEEE 802.11 standard, called WEP, has been declared insecure due to multiple vulnerabilities detected

While the final version of IEEE 802.11i was being ratified, and in order to overcome some of the security problems of WEP without the need to replace the wireless hardware, a security protocol was developed that implemented a subset of the 802.11i specifications (pre-RSN and TKIP). This protocol was approved by the Wi-Fi Alliance as **WPA** (Wi-Fi Protected Access).

Subsequently, once 802.11i was ratified, the Wi-Fi Alliance introduced **WPA2** (Wi-Fi Protected Access 2) which already certified full support for the IEEE 802.11i standard (RSN and AES). WPA2 is not compatible, in most cases, with wireless hardware initially designed for WEP, as this hardware does not support the computational burden of the encryption operations of the AES algorithm, which is the primary cryptographic algorithm of WPA2.

Today, most Wi-Fi hardware supports WPA2. WPA (pre-RSN and TKIP) has been declared insecure and, like WEP, should not be used in corporate networks.

WPA and WPA2 have two modes of implementation:

- **Personal (PSK)**, access via a single key pre-shared with all customers.
- **Enterprise (802.1X)**, 802.1X access with dedicated credentials for each client.

Primarily, the two implementations differ in the authentication and key distribution mechanisms. Personal uses the PSK (Pre-shared Keys) mechanism while Enterprise uses the 802.1X authentication mechanism, with the use of an Authentication Server (AS), typically RADIUS protocol.

As far as possible all Wi-Fi networks should use Enterprise mode with 802.1X and the use of PSK would be justified only when clients do not have 802.1X support.

It the use of a network with PSK is required, it is recommended to use non-standard mechanisms offered by some manufacturers that allow assigning a different pre-shared key for each client device differentiated by its MAC address.

During 2017 and 2018 critical attacks on the *4-way handshake* of WPA2 (KRACK Attacks) were published. This led to the announcement by the Wi-Fi Alliance of the **WPA3** protocol specification (WPA3-v2.0 published on 20/12/2019).

The WPA3 protocol has two main objectives. The first objective is to certify in Wi-Fi products the correct implementation of the proposed countermeasures against the so-called KRACK Attacks. The second objective is to update existing mechanisms to increase the level of security and to prevent known attack techniques.

As far as possible all Wi-Fi networks should use Enterprise mode with 802.1X

The main features of WPA3 and its modes of operation are:

- **WPA3-Personal-SAE**
  - WPA3-Personal-***Only*** Mode
    - Mandatory use of 802.11w *Management Frame Protection* (MFP)
    - **Mandatory use of *Simultaneous Authentication of Equals*** (SAE)
  - WPA3-Personal-***Transition*** Mode
    - *MFP-802.11w* optional for a WPA2-Personal client
    - PSK for WPA2-Personal and SAE for WPA3-Personal clients
- **WPA3-Enterprise-802.1X**
  - WPA3-Enterprise-***Only*** Mode
    - Mandatory use of MFP-802.11w
  - WPA3-Enterprise-T***ransition*** Mode
    - Optional use of MFP-802.11w for WPA2-Enterprise clients
  - WPA3-Enterprise-192-bit Mode*t*
    - Mandatory use of MFP-802.11w
    - 256-bit AES-GCM encryption of user traffic
    - Restricted encryption *cipher suites* on the EAP channel:
      - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        - ECDHE and ECDSA using elliptic curve P-384
      - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        - ECDHE using elliptic curve P-384
        - RSA >= 3072 bits
      - TLS_DHE_RSA_WITH_AES_256_GCM_SHA3844
        - DHE and RSA >= 3072 bits

New vulnerabilities and attacks have been published on WPA3 that force us to rethink whether it is necessary to make modifications to the protocol (Dragonblood affecting Dragonfly of SAE and EAP-pwd). Vulnerabilities have also been published that affect client chips and access points, allowing buffered frames to be decrypted when sent with TK=0 after disassociation (Kr00K vulnerability published in February 2020).

Wireless technologies are constantly changing and evolving. It is very important that administrators keep up to date and apply the necessary countermeasures to published vulnerabilities and threats. It is also important to be aware of the evolutions of the standard and to consider them when a technology innovation is needed.

3. Risks and threats in Wi-Fi networks

Wireless networks are exposed to most of the same risks as wired networks, plus those introduced by Wi-Fi technology.

To control these risks, organizations that require the use of such networks must adopt safeguards to minimize the likelihood of impact on both existing and newly deployed infrastructures.

Moreover, as with any technology, it is essential to continuously monitor new vulnerabilities that may appear in the future and affect the organization.

Whenever possible, it is recommended to use wired access and disable wireless interfaces.

Whenever possible, it is recommended to use wired access and disable wireless interfaces

The following are the main threats affecting wireless networks:

- Due to an unknown vulnerability, the computer could be compromised by having the wireless interface enabled without the need for physical contact by the attacker.
- Access may be gained through wireless connections to other non-wireless environments that are connected to them.
- Information that is transmitted wirelessly can be intercepted even from kilometres away, with no possibility of detecting this capture.
- Denial of Service (DoS) attacks against such infrastructures (signal jammers, malicious packets, etc.) can easily occur.
- Traffic can be injected into wireless networks over long distances (even kilometres).
- Using unencrypted networks or knowing the infrastructure, rogue APs can be deployed by spoofing to obtain information (e.g. spoofing the Radius server to steal corporate username/password credentials if EAP-TLS certificates are not used).
- Access to wireless network can lead to execute "Man in the Middle" attacks.
- Connection information can be obtained by accessing a legitimate computer and performing a forensic analysis of the same.
- Access to networks can be gained by using the connected networks of third parties that do not maintain an adequate security policy.
- Insider attacks can be carried out by deploying unauthorised wireless networks.
- Information about the owning entity and client devices can be disclosed in open data that can be easily captured (SSID and MAC addresses).

Access to wireless network can lead to execute "Man in the Middle" attacks

4. Corporate Wi-Fi networks

The Wi-FI service of a corporation is mainly composed of two structural blocks:

- User devices acting as an end client.
- The physical architecture of access and complementary services.

This guide covers access to the Wi-Fi service for both corporate devices and users. It assumes that the devices have been certified and configured to support 802.1X-based access control using the EAP-TLS method. Through an initial deployment, the devices have been configured and provisioned with a client certificate to identify device and user.

Wi-Fi service administrators shall configure and use the different existing mechanisms and solutions to secure the basic pillars of network access control:

- Authenticate users and devices.
- Authorise by applying the policies according to the user/device role.
- Continuously check the health and performance of the device.
- Secure communications through encryption layers (Wi-Fi and VPN).
- Record the actions carried out for analysis and monitoring (*Accounting*).

Wi-Fi service administrators shall configure and use the different existing mechanisms and solutions to secure the basic pillars of network access control

4.1 Wi-Fi service architecture

In the following sections we will analyse the main features with respect to the definition of logical architecture, physical architecture and network segregation.

To define both the physical and logical architecture of a corporate Wi-Fi network, it is difficult to generalise recommendations, since its design is not only affected by the needs and characteristics of the corporation itself, but also by the manufacturer's product chosen as the Wi-Fi service solution.

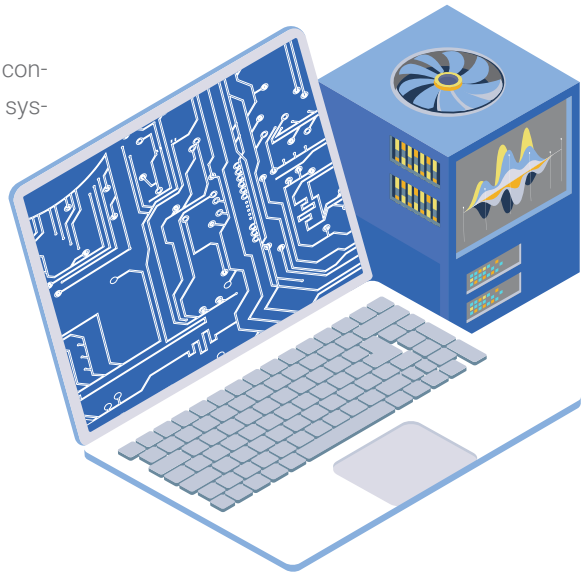
4.1.1 Logical and physical architecture

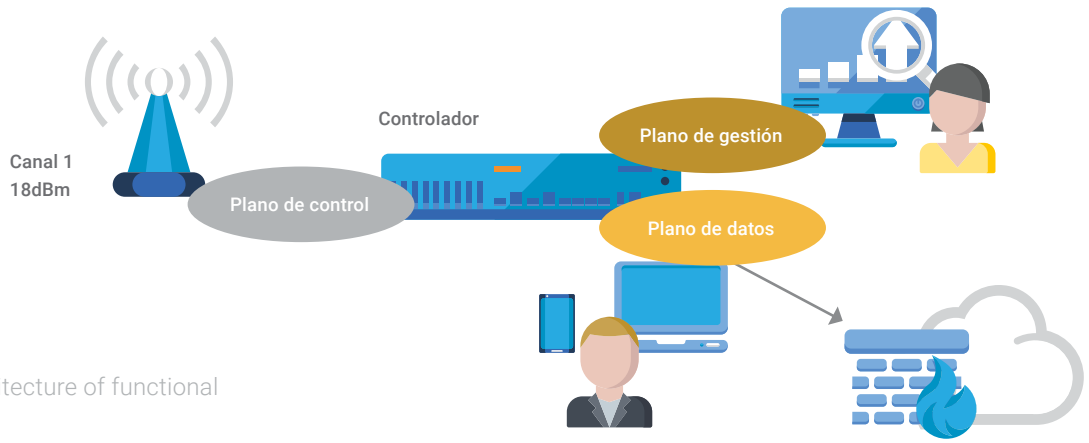
When talking about the logical architecture of a corporate Wi-Fi network, three functional levels (*planes or layers*) can be defined as shown in **Figure 1**:

1. **Data plane** (*Data or Forwarding Plane*): In charge of moving user data packets in different directions: user-network, network-user and user-user.

2. **Control Plane**: Where the different protocols, processes and functions of the Wi-Fi service reside: packet routing, loop protection, automatic channel and power allocation, etc.

3. **Management Plane**: The one that allows the administrator to configure and monitor the Wi-Fi service: GUI-Web, CLI-SSH, SNMP, syslog, etc.





[Figure 1]
Logical architecture of functional planes

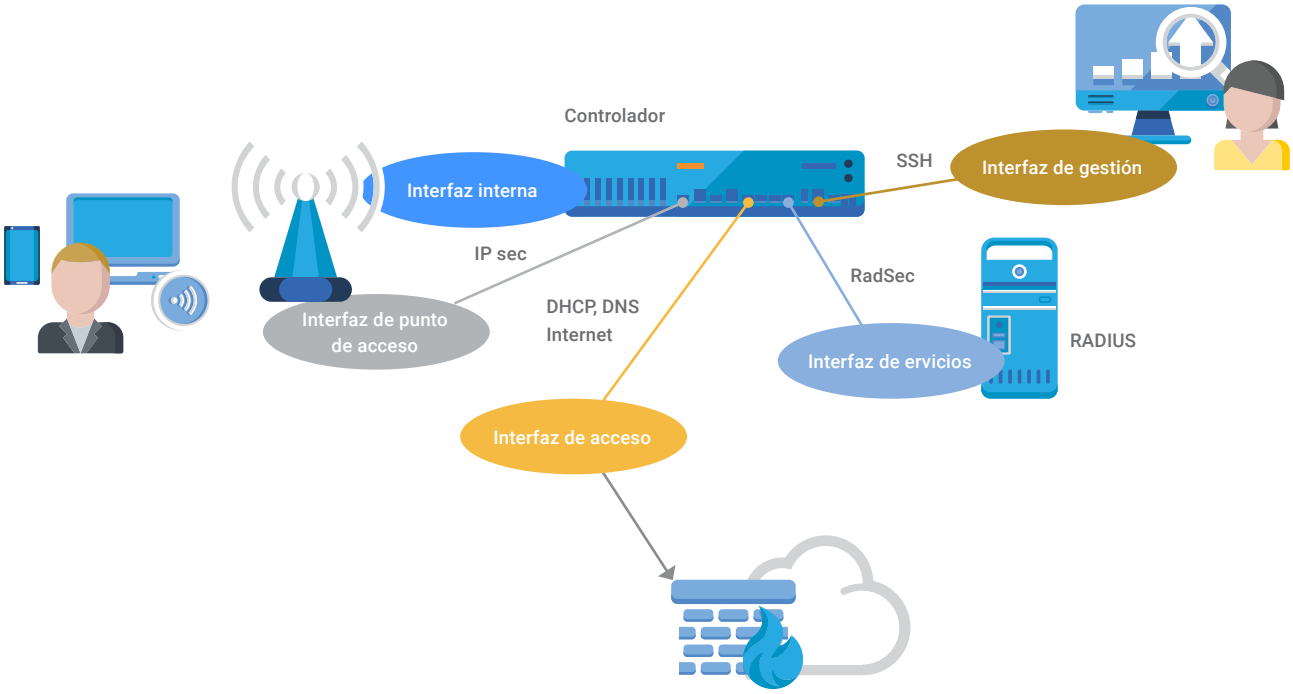
To secure a Wi-Fi network, it is important to know where each of the logical planes is located and how the different elements that form part of the service communicate. Each product and manufacturer's solution has its own architecture definition and it is the administrator's task to know its own characteristics in order to configure it correctly.

For example, we can find fully centralised solutions based on a controller and so-called lightweight access points. The access points establish an IPsec tunnel against the controller and the controller is in charge of managing all the tasks defined in the data, control and management plane.

Figure 2 depicts how the controller can have dedicated physical interfaces for management traffic (GUI-Web, CLI-SSH, SNMP, syslog, etc.) and have separate physical interfaces for the data plane by segregating user traffic into different VLANs.

The controller could act as a layer 2 device by switching Wi-Fi user traffic to the access network or it could take on layer 3 tasks by routing traffic between the different user networks. In both cases it could perform Firewall functions or even perform application identification, URL filtering and categorisation, IDS/IPS analysis, malware analysis, etc.

To secure a Wi-Fi network, it is important to know where each of the logical planes is located and how the different elements that form part of the service communicate



[Figure 2]
Architecture of physical interfaces

The controller also takes on other control plane tasks such as the orchestration of channel and power allocation. Depending on the vendor solution, certain control plane tasks may be delegated to a server or cloud service outside the controller.

There are controller-based solutions that decentralise some logical plane. For example, an administrator may decide to hand over the data plane to the access point without the need to concentrate traffic at the controller. In this case, user traffic will be dumped to the antenna interface itself, segregating into different user VLANs and maintaining the IPsec tunnel to the controller to keep the management and control plane centralised.

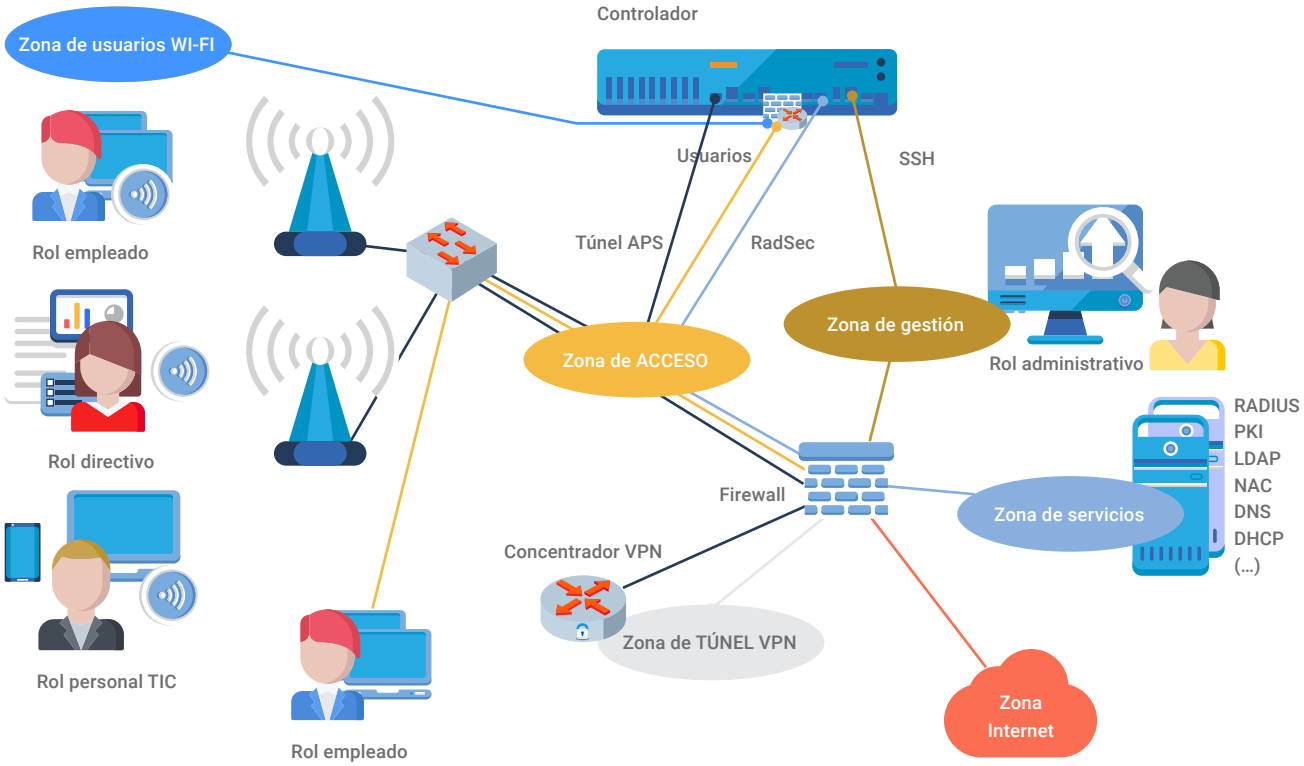
We can also find fully decentralised solutions commonly referred to as controller-less. The data plane is assigned to each access point and the control plane can be of the mesh type in which all access points interact as equals or of the master type in which one access point assumes the role of administrator of the control plane. The management plane can also be assumed by a master access point or can be centralised virtually in a cloud service.

4.1.2 Segregation of zones, networks and roles

For a correct grouping and isolation of the different devices that make up a corporate Wi-Fi network, it is recommended to maximise segregation. It would be ideal to apply a zero trust model that applies security policies to all communication that takes place between any elements of the network, whether they are clients or servers.

To simplify the example, it is proposed to create zones, virtual networks (VLANs) and roles in the logical architecture depicted in **Figure 3.**

- **Access area:** set of networks configured in the access switches:
  - **Network for access points:** network dedicated to communication between access points and controller which establish an IPsec tunnel.
  - **User network:** creation of different VLANs per department, physical availability, security level or user role/profile.
  - **Network for service access:** network dedicated to service access such as RADIUS requests from the controller.
- **VPN tunnel zone:** When a user establishes a VPN tunnel with the corporate tunnel concentrator, an end-to-end protected trusted network is defined. It is beyond the scope of this guide to recommend which networks shall be accessed through the tunnel as this will vary depending on corporate interests and policies.
- **Internet access zone:** it will provide the corporate network with access to the Internet through a firewall that protects all communications between zones.
- **Management area:** it will be used to carry out the administration and configuration tasks of all the systems connected to it.
- **Service area:** where the corporate servers are located. It is recommended to carry out micro-segmentation and to secure any communication that takes place between the different elements, both clients and servers.
- **Controller user networks:** these are networks that shall only be defined in the access point controller for the purpose of securing communications with the access network.



[Figure 3]
Segregation of zones, networks and roles

If it is decided that the controller will act as a level 3 equipment (performing routing tasks) two zones can be defined in the controller for the users: Wi-Fi user network zone and corporate access network zone.

Once the authentication of the user device is completed, within the controller, the concept of authorisation role is applied for each session. The role affects user traffic and session exchanges with the corporate access network.

The application of a role can force a change of user network by assigning a new VLAN or it could be indicated not to change the VLAN, so as not to affect the IP configuration of the client, but to modify the network filtering rules.

The following roles can be defined:

- **Validation role:**

  to be applied to the client that has successfully completed the 802.1X authentication process (phase 2 of the security model to be discussed later). The client will remain in this role while it is being analysed for compliance with the device health status requirements and other authorisation attributes. Only accesses that are strictly necessary to obtain IP configuration and receive or make connections against the NAC agent solution services will be allowed.

- **Quarantine role:**

  it will be applied to those clients that do not comply with the security requirements. This may be due to a negative report from the NAC agent regarding the status of the device or due to indication of some other authorisation attribute. If remediation is possible, the role policy shall allow access to the necessary resources to fix the problem.

- **Healthy state role:**

  it will be applied to those clients that meet the established security requirements. This role will allow clients to create a VPN tunnel (phase 4 of the security model to be discussed below). Establishing the VPN tunnel will give access to the tunnel network where an IP address server will be available to provide a new IP address through which encapsulated traffic is transmitted and received.

- **Healthy status role with profile:**

  different policies may need to be applied depending on the user profile, in which case a specific role could be created for each profile (e.g. employees, managers, technical staff, students, teachers, etc.).

5. Security model

This section will show the four-phase security model to be configured and implemented in a secure corporate Wi-Fi network. The model applies to corporate devices and corporate users.

It is recommended to use a single **802.1X-Enterprise** corporate SSID using **EAP-TLS** as authentication method with server and client certificates. Once the client is authenticated and authorised, the wireless channel will be encrypted with **AES**. Then, a continuous analysis of the health status of the device will be performed with a **NAC agent** and/or the behaviour of the device will be monitored using ***fingerprinting*** techniques. The result of the health status analysis will modify the authorisation level if necessary. Finally, to ensure end-to-end encryption, an **encrypted VPN tunnel** will be established.

- **Phase 0:**
  Configuration of the corporate service and deployment of clients.
- **Phase 1:**
  Association and authentication through MAC address.
- **Phase 2:**
  802.1X authentication and authorisation with EAP-TLS.
- **Phase 3:**
  Network access and continuous health check of the device.
- **Phase 4:**
  Establishment of an encrypted VPN tunnel.

> **The model applies to corporate devices and corporate users**

5.1 Phase 0: configuration and deployment

Before starting the access phases, the Wi-Fi service solution must be configured by the administrator and the configuration of the client devices must be deployed in order to access the Wi-Fi service.

5.1.1 Enterprise mode configuration

The WPA3-v2.0 specification gives the option to configure different WPA3-Enterprise modes. **Figure 4** represents the decision making of the WPA3-Enterprise mode to be configured: Only, Transition or 192-bit. The modes will be conditioned to the features supported by the different elements of the Wi-Fi solution:

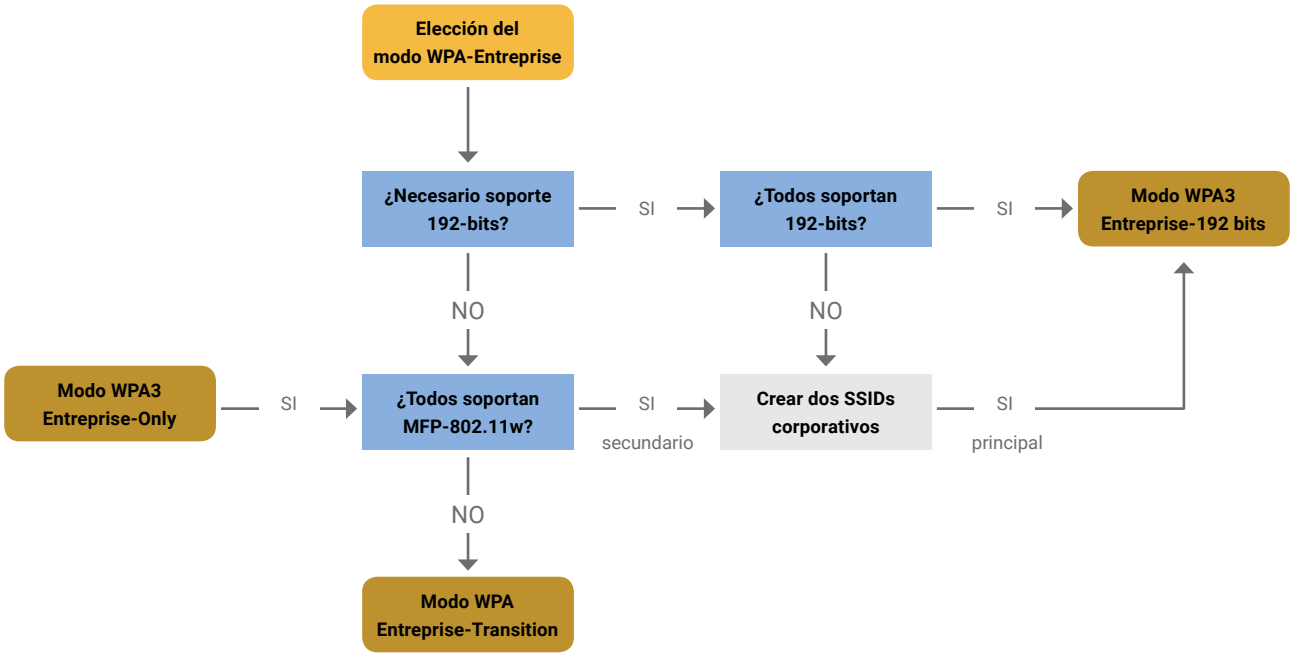
- **MFP-802.11w:** on client devices and access points.
- **Robust cipher suites:** on client supplicant and authentication server.
- **AES-256-GCM encryption:** on client devices and access points..

Where possible, it is recommended to use a single SSID to give access to the corporate Wi-Fi network (e.g. "corp_1X"). At the time of writing these recommendations, the highest level of security is provided by WPA3-Enterprise-192-bit mode (MFP-802.11w mandatory, strong cipher suites and AES-256-GCM traffic encryption).

If all devices and elements of the Wi-Fi infrastructure support WPA3-Enterprise-192-bit mode, it is recommended to use it in the corporate SSID.

However, as WPA3 is a very recent specification, it is possible that not all devices support 192-bit mode. If client support is partial, it will be necessary to define a second corporate SSID to give access to unsupported devices (e.g. "corp_1X_2") in order to maintain the highest level of 192-bit security on the main SSID.

If all devices and elements of the Wi-Fi infrastructure support WPA3-Enterprise-192-bit mode, it is recommended to use it in the corporate SSID



[Figure 4]
Choice of WPA3-Enterprise Mode

For SSIDs where 192-bit mode is not configured, it is recommended to at least optionally enable all features that are a requirement for 192-bit mode: use of the robust cipher suites, AES-256-GCM encryption and MFP-802.11w.

When all devices support WPA3-Enterprise but only some support 192-bit, the first SSID could be configured in WPA3-Enterprise-192-bit mode and the second SSID in WPA3-Enterprise-Only mode, making the use of MFP-802.11w mandatory.

In the event that WPA2-Enterprise devices that do not support MFP-802.11w need to be serviced, the second SSID shall be configured in WPA3-Enterprise-Transition mode making the use of MFP-802.11w optional for WPA2-Enterprise devices.

In case it is chosen not to configure 192-bit mode, a single corporate SSID in WPA3-Enterprise-Only mode could be configured, if all devices support MFP-802.11w, or WPA3-Enterprise-Transition mode if some device does not support MFP-802.11w.

It may be the case that the Wi-Fi infrastructure does not support WPA3 and the only alternative is to configure an SSID with WPA2-Enterprise in which case it is recommended to allow the maximum supported security levels at least optionally: MFP-802.11w, AES-256-GCM encryption and support by strong cipher suites in the authentication server.

It is recommended to define a migration plan for all devices that do not support WPA3-Enterprise in order to enhance security mechanisms and to implement countermeasures for published vulnerabilities..

5.1.2 Wi-Fi service configuration

We will assume that the Wi-Fi infrastructure will use a primary corporate SSID in WPA3-Enterprise-192-bit mode called "corp_1X" and a second SSID in WPA3-Enterprise-Transition mode called "corp_1X_2" to serve devices that do not support all 192-bit security mode requirements.

Access points will advertise the two services and the devices will be configured indicating, among other parameters, their corresponding SSID. All 192-bit mode security mechanisms shall be optionally offered on the SSID in WPA3-Enterprise-Transition mode.

For authentication, an EAP channel shall be established between the supplicant client and the authentication server over 802.1X and RADIUS protocols (user-controller section and controller-server section respectively). The RADIUS communication between controller and authentication server shall be protected by the RadSec protocol (based on TLS). The EAP channel shall encapsulate the EAP-TLS method to perform certificate-based authentication.

In order to use the **EAP-TLS method**, a PKI infrastructure is required to generate and manage client and server certificates. Complementary services such as databases to store authorisation attributes (an LDAP, an active directory or any other database) will also be necessary.

A digital certificate will be generated for the authentication server signed by a CA that clients trust and the hostname of the server from the certificate will be verified.

The authentication server will trust the CA signing the client certificates and it will verify the revocation status (e.g. with OCSP: *Online Certificate Status Protocol*).

5.1.3 Deployment of client configuration

Clients will have a digital certificate that is signed by a CA trusted by the authentication server. It is recommended that the client certificate includes attributes that identify both the user and his device.

The authentication server will use certain attributes of the certificate during the authorisation process to decide which role or policy to apply to the authenticated session (e.g. CN, SAN or email).

A preferably automated client device configuration protocol or mechanism shall be defined.

It is important that the client cannot modify the configuration parameters as he/she could disable basic checks that would allow access to a spoofed Wi-Fi service (e.g. by disabling the verification of the hostname and CA-root that signs the authentication server certificate).

The WPA3-v2.0 specification provides for the possibility to disable the option that allows the client to add a trust exception to the authentication server certificate when the validation of the authentication server certificate fails (TOD: T*rust Override Disable, UOSC: User Override of Server Certificate*). For clients that have been configured in deployment it is recommended to indicate the TOD-STRICT OID: "1.3.6.1.4.1.1.40808.1.3.1" in the authentication server certificate to avoid interaction and exceptions in case of validation failure.

An example of the parameters to be configured in the clients:

[Figure 5] Deployment and configuration of the client

	Client WPA3-Enterprise-192-bits	Client WPA3-Enterprise-Transition
Corporate SSID	“corp_1X”	“corp_1X_2”
MFP-802.11w	Mandatory	Optional
Encryption	AES-256-GCM	AES-128-CCMP Optional: AES-256-GCM
Credentials	Client Private Key and Client Certificate (signed by CA-root-client)	
Radius server data to be verified mandatory	CA-root-server certificate hostname (e.g. "radius.corp.es")	

5.2 Phase 1: MAC authentication and association

Once the Wi-Fi service has been configured and the clients have been deployed, the Wi-Fi service access phases begin.

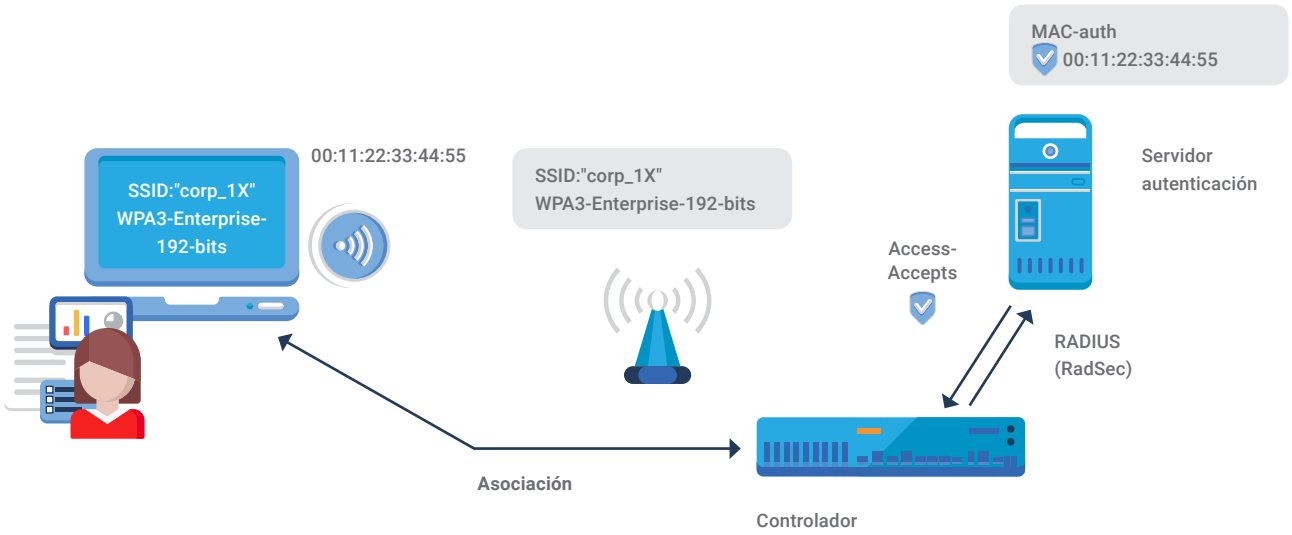
In the first phase, the customer does not have any mechanism to have confidence in the infrastructure offering the Wi-Fi service. The only information that is validated is the SSID name of the beacon announcements. When a service announcement is received, the association is initiated.

The client could use non-standardised mechanisms for the detection of malicious services such as geolocation consistency, fingerprinting of the features advertised in beacons and BSSID addresses of access points. All data in the beacon frame, including SSID and MAC addresses, are easily spoofable and should never be used as the sole authentication system.

During the association, depicted in **Figure 6**, it is recommended that the corporate infrastructure performs a first authentication based on the MAC address of the wireless client, although we know that this is an attribute that can be easily spoofed.

Regarding MAC authentication, two types of policies can be combined: whitelist-based or blacklist-based policies. A whitelist can contain all MAC addresses of the corporate clients configured during deployment. A blacklist can contain all MAC addresses considered as malicious.

Once the Wi-Fi service has been configured and the clients have been deployed, the Wi-Fi service access phases begin



[Figure 6]
MAC association and authentication

As an example, all MAC addresses on a whitelist could be given access to phase 2 (802.1X), while association to any unknown or blacklisted MAC addresses will be blocked.

As another example, one could omit the whitelist and allow by default any MAC address that is not included in a blacklist.

MAC address-based authentication allows us to block and protect access to the authentication server. For example, when detecting a DoS attempt against 802.1X we could blacklist all participating MAC addresses and block them permanently or for a defined period of time as a containment mechanism.

5.3 Phase 2: 802.1X authentication and authorisation with EAP-TLS

If the client successfully passes MAC association and authentication, the infrastructure will prompt the client to use the 802.1X protocol to establish an EAP communication with the authentication server **(step 1 and 2** in **Figure 7)**. The method to be used in the EAP channel is EAP-TLS.

The authentication server, after checking the client's identity identifier, will send its certificate **(step 3)** so that the client can verify the hostname and decide whether it trusts the CA signing the certificate **(step 4)**, according to the configuration made during the deployment of the clients.

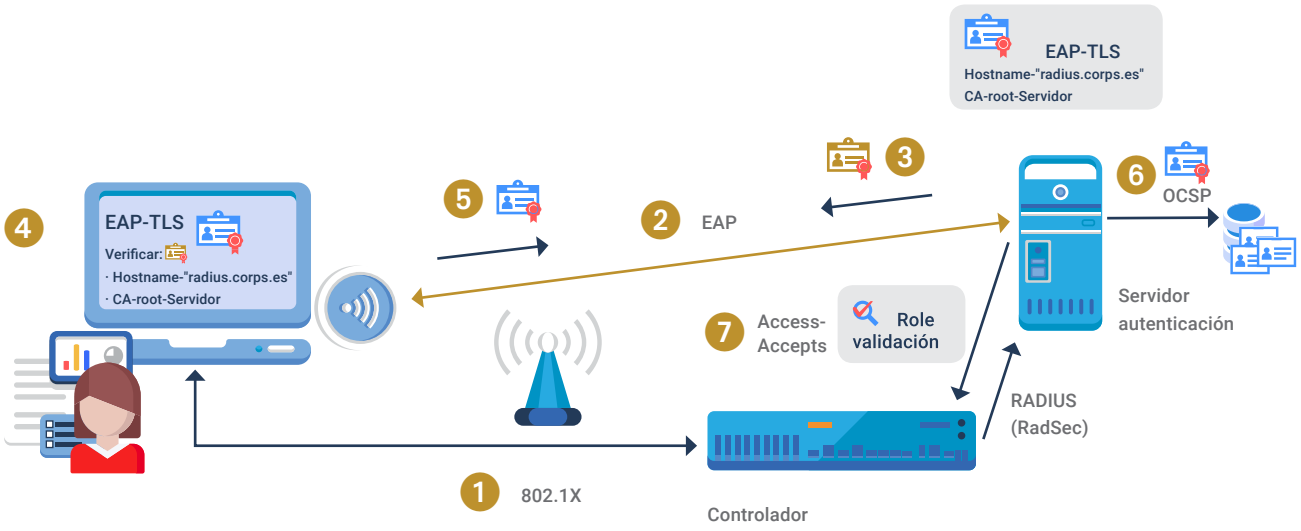
If everything is correct, the client will send its certificate to the authentication server **(step 5)**. The server will check the attributes of the client's certificate and verify its validity using the resources of the trusted CA that signs the client's certificate, e.g. OCSP **(step 6)**.

If the server concludes that the authentication is successful it shall proceed with the authorisation of the client device.

For authorisation, the server will collect a number of attributes from different sources and together with the data obtained through the authentication process it will determine the resulting role to be applied to the client device session.

Authorisation attributes can be static such as the user's personal data, or dynamic such as device health status reports, physical location, network behaviour applying pattern-based signatures, etc.

If the client successfully passes MAC association and authentication, the infrastructure will prompt the client to use the 802.1X protocol to establish an EAP communication with the authentication server



[Figure 7]
Authentication via EAP-TLS

The resulting role may contain settings such as VLAN, firewall filters to apply, bandwidth control, or any other parameters that the network infrastructure allows to be applied. If the server determines that it does not have enough data to decide on the health of the device, it may apply a "validation role" to provide the minimum services necessary to receive a device health status report **(step 7)**.

At the end of the authentication and authorisation process:

- The customer will be able to calculate the PMK (Pairwise Master Key).
- The authentication server shall use the RADIUS channel to send to the controller or access point all necessary attributes for authorisation and PMK calculation.

A *4-way-handshake* is then performed between the access point and the client to verify mutual trust, deriving from the PMK the encryption keys for the traffic on the wireless section (PTK and GTK).

As long as the client device remains associated to the Wi-Fi service, the EAP channel shall remain active to perform re-authentications with the server and regenerate the cryptographic keys according to the defined intervals.

5.4 Phase 3: network access and device health status

Once the authentication is done, the authorisation attributes have been applied and the 4-way handshake has been completed, the client has access to the data network **(step 1** in **Figure 8)**. The authorisation attributes will define the access policy and the allowed services **(step 2)**.

Once the authentication is done, the authorisation attributes have been applied and the 4-way handshake has been completed, the client has access to the data network

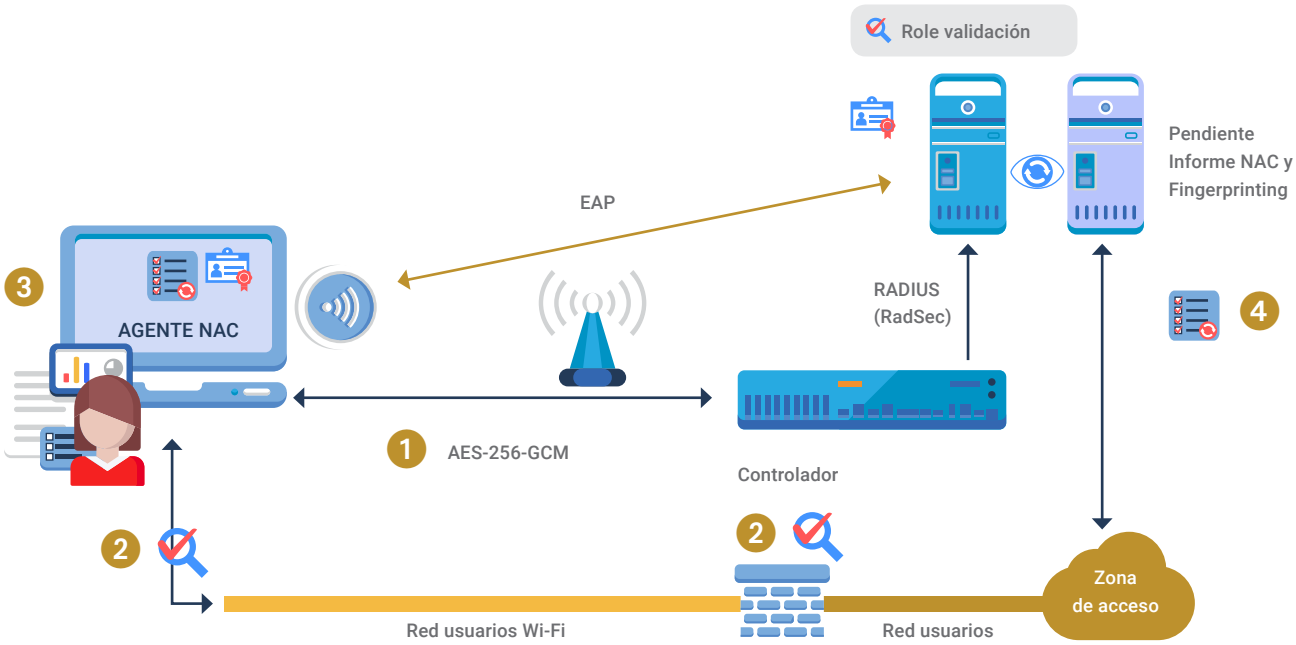
The first basic service offered to the customer is DHCP which will allow the customer to configure the IP interface (IP address, subnet mask, default route, DNS server and other corporate parameters). The use of DHCP by the customer will be mandatory avoiding manual configurations. To simplify the registration and auditing processes the IP allocation will be static per device by linking each IP address to a MAC address.

To simplify the management of security policies, the use of user names, groups or roles is recommended as an alternative to the use of IP addresses. It is recommended to record the mapping between IP address and user name to allow their reference in policies and access logs.

All direct communications between clients shall be blocked to prevent the spread of infections. If direct communication between clients is necessary, alternatives to provide the same service or to enable proxy solutions should be explored.

All network communications will be scanned and protected by security equipment (firewall, IDS/IPS, URL-filtering, malware scanning, netflow, etc.).

Network analysis tools allow the generation of dynamic attributes to be used in the authorisation process to determine the role of the user. Fingerprinting or profiling can be done by analysing DHCP requests, the user-agent of http requests, applications identified by the firewall, netflow session patterns, etc.



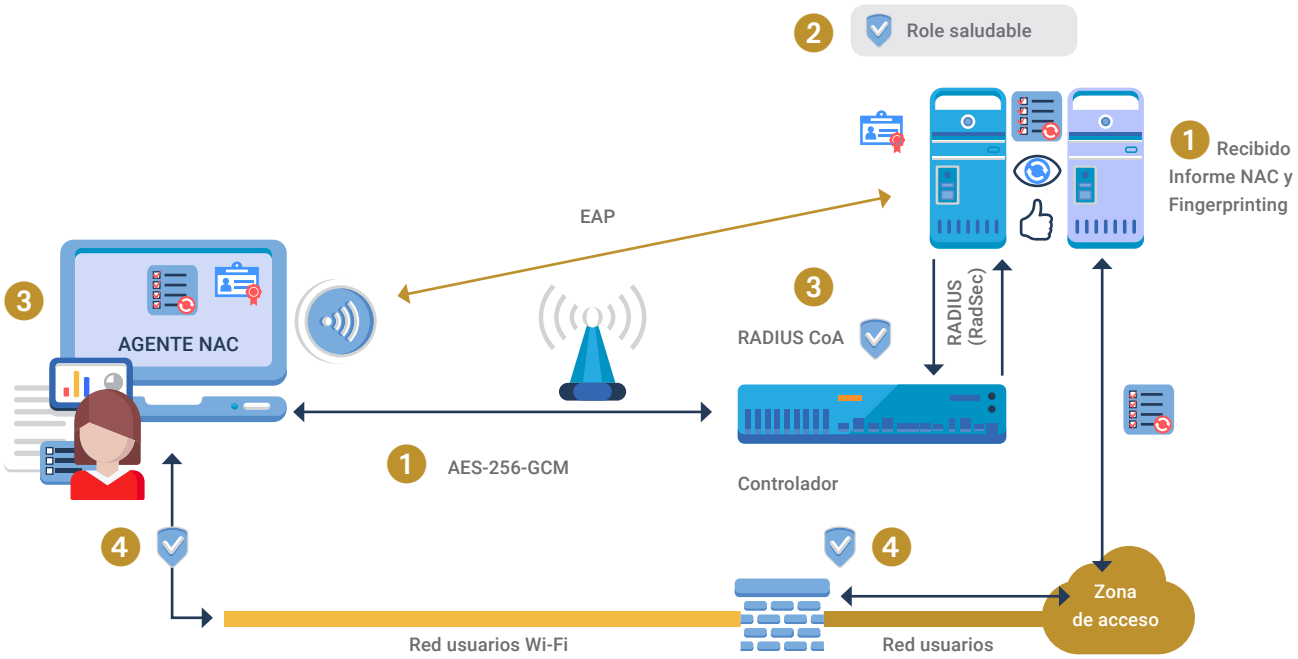
[Figura 8]
Checking the device status through the NAC Agent

For better analysis and profiling, it is recommended to use a programme, agent or system (NAC agent) installed on the computer of the user who is going to access the network to verify that the terminal to be accessed has minimum security requirements **(step 3)**.

These recommended minimum requirements are::

- The client computer's operating system is up to date with versions no older than two months (or as determined by the organisation's security policy).
- The equipment has a protection system such as an anti-virus or EDR solution installed and running, with updates no older than two months (or as determined by risk analysis).

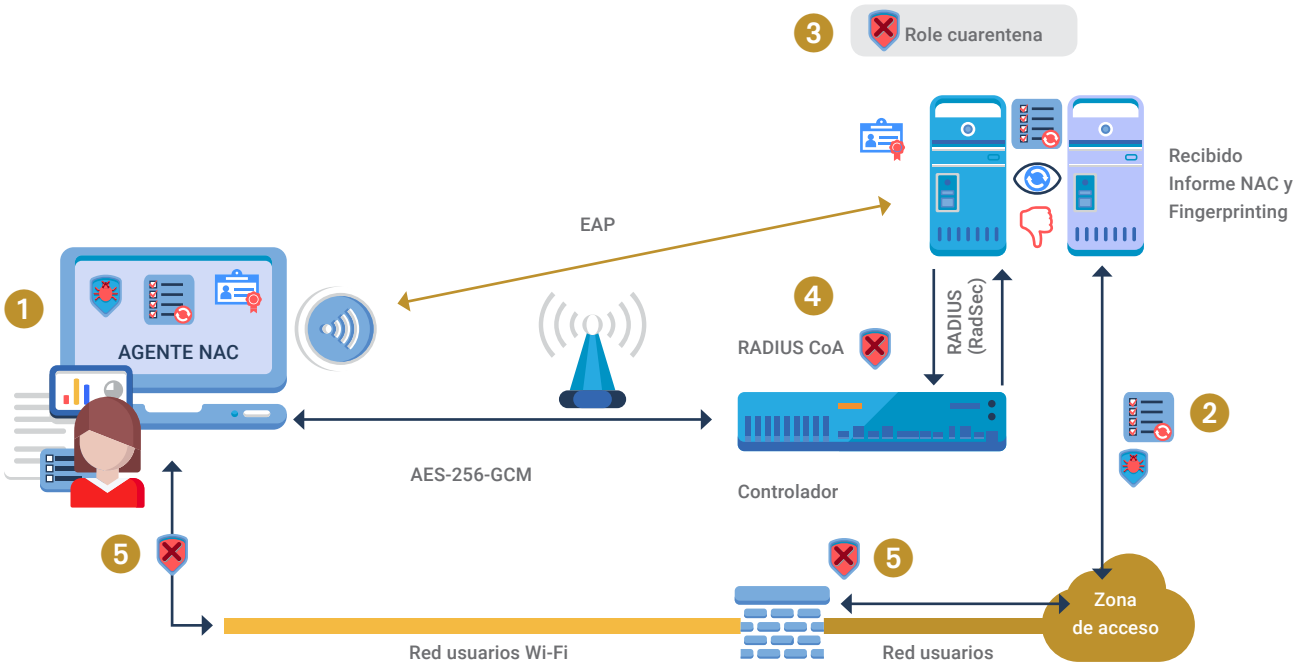
The NAC agent will send the status of the device to a NAC server to verify the health of the connected equipment **(step 4)**. This agent will run periodically (recommended every 30 seconds), allowing to know if the status of the device has changed so that different network access policies can be defined and applied depending on the fulfilment of the network access requirements.



[Figure 9]
Device with healthy state

The NAC agent status reports and scan attributes shall be made available to the authentication server to enable it to decide on the role to be applied to a device session.

Initially after authentication, the authentication server can apply the **"validation role"** until the health status report is received. If the report is healthy, via a Radius CoA, it will switch to **"healthy status role"** **(Figure 9)**.



[Figure 10]
Device in quarantine state

If, on the other hand, the report indicates that it does not comply with the security requirements, it will switch to **"quarantine role"**, restricting access to the minimum services required to solve the problems detected **(Figure 10)**.

It is also possible to modify the authorisation status of clients who have been deemed healthy to quarantine if a change of status is detected.

For example, a change in the *fingerprinting* of the device type or operating system when analysing the user-agent or DHCP, a suspicious traffic pattern or use of an unauthorised application when analysing netflow or firewall application identification, accessing a malicious URL, downloading malware, etc.

5.5 Phase 4: setting up the encrypted VPN tunnel

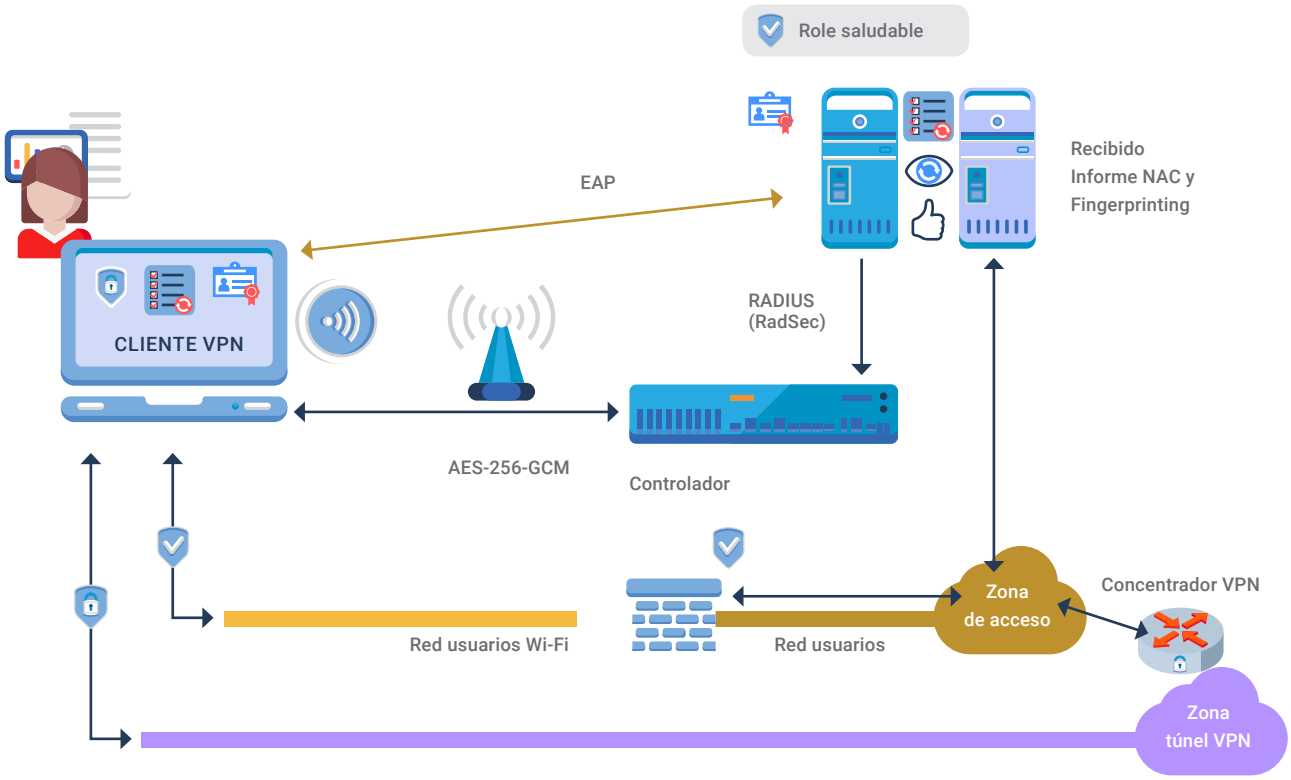
Wireless encryption will be complemented by the establishment of an encrypted VPN tunnel to the corporate VPN concentrator. This extends encryption from the client to a corporate trust zone, with information in transit being protected through strong encryption and authentication mechanisms.

It is recommended to consult the specific guidelines regarding VPN tunnelling solutions to determine the solution that meets the needs of the corporation. In general, the maximum level of security supported by the product and VPN clients should be used.

The following cryptographic suites can be taken as a reference:

[Figure 11] Recommended cryptographic algorithms

ALGORITHM MEDIUM HIGH	MEDIUM	HIGH
Advanced Encryption Standard (AES)	128 bits	256 bits
Digital Signature Elliptic Curve Digital Signature Algorithm (ECDSA)	256 bit curve	384 bit curve
Key exchange Elliptic Curve Diffie-Hellman (ECDH)	256 bit curve	384 bit curve
Hashing Secure Hash Algorithm (SHA)	SHA-256	SHA-384



[Figure 12]
Setting up the VPN tunnel

Depending on the solution implemented and its integration with the Wi-Fi solution, the process of association, authentication, status verification and VPN tunnel establishment may be performed with a single agent or application.

On the other hand, we can find non-integrated solutions in which there is a supplicant responsible for the association and authentication, a NAC agent for status reporting and finally a VPN client who establishes the encrypted tunnel.

Whatever the solution, the VPN tunnel should be established as soon as possible after gaining access to the network in order to secure all communications. But it would be understandable to disallow the VPN tunnel to be established until the device obtains the healthy state role.

Once the tunnel is up and running, the client will have two different connections, the "Wi-Fi User Network" connection and the "VPN Tunnel Network" connection. The latter will be the default interface for all client traffic.

The "Wi-Fi User Network" with AES-GCM-256 encryption from the client to the delivery point od the controller's data plane will carry the encrypted encapsulation of the "VPN Tunnel Network". On leaving the controller the "VPN Tunnel Network" will be encapsulated and will traverse any existing infrastructure to reach the VPN concentrator which provides an authenticated and encrypted channel from the customer device to the VPN concentrator itself.

Despite the double encryption of the "Wi-FI user network" and "VPN tunnel network", secure sessions will be established at the application level with protocols that encrypt the channel from the client to the application server (e.g. https and TLS). And over this application channel, the information sent shall be protected so that it is accessible only by authorised users or recipients (e.g. by encrypting e-mails or files with the authorised recipient's public key, either PGP or certificate).

The different layers of encryption protect communications against vulnerabilities such as Kr00k because if an attacker manages to decrypt Wi-Fi frames, all he will be able to see is encrypted frames through the VPN tunnel.

Despite the double encryption of the "Wi-FI user network" and "VPN tunnel network", secure sessions will be established at the application level with protocols that encrypt the channel from the client to the application server

6. Security recommendations

This section contains a series of security recommendations that should be considered when deploying the network. Some of these recommendations have already been mentioned in previous sections.

For further information on the information described here, please consult the guides listed in the reference section.

6.1 Initial considerations

- Conduct **risk analysis and risk management** before starting network deployment, including the availability of systems and services, the integrity of data and transactions, the level of confidentiality, the authenticity of data exchanged and the traceability of these exchanges on the equipment to be used, the connections to be established between them and who will operate them and how they will be operated.

- **Consider wired access.** A wired access has always less exposure to threats. Compromise of the device when the wireless interface is enabled by the exploitation of some unknown vulnerability cannot be ruled out with the aggravation of succeeding without physical contact and from a long distance.

- **Analyse the equipment to be purchased.** Check the capacity to support the required protocols and the release of updates by the manufacturer. Apply redundancy on those systems that in case of failure, error or attack would disturb the normal operation of the service. Make an inventory of devices and review it periodically.

- **Ensure physical access** to the organisation's premises, especially to areas where equipment is deployed.

- **Conduct an analysis of the radiation range** of the access points (this analysis should be included in regular security reviews). Define the location of access points and try to keep them away from the outside perimeter of the organisation.

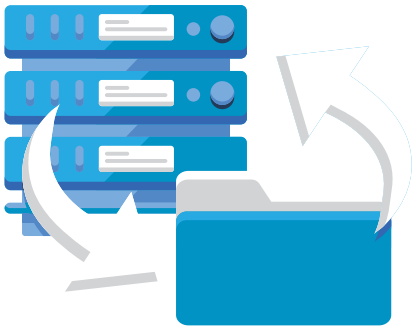
- Develop a set of **security policies** defining who has physical access to the network equipment, who has administration access, and what procedures should be executed in case of intrusion. This policy should also specify the methods to be used to recover the normal operation of the devices in case of failures, errors, intrusions, etc. Periodic compliance checks of security policies should be carried out.

- To prevent malicious access to the wired network of the access points, authenticate and authorise the wired access of the access points using **802.1X with EAP-TLS** on the access switches.

- **Educate** users on the use of this technology and the risks associated with its use.

6.2 Updates and backups

- Keep your **equipment updated** to the latest version. Download updates through the manufacturers' official providers as long as such a service is offered via a secure communication protocol.
- Make **backups** periodically, and store them on computers other than those being backed up.
- Establish mechanisms that define **procedures for** information **retrieval**, as well as mechanisms for testing its correct functioning prior to its implementation.
- Transfer files via the local file upload option (local file) or **SCP.** Disable the use of FTP and TFTP.



6.3 Methods and conditions of access

- Create a **dedicated management network** that only carries management and administration traffic.
- Use **secure computers as access methods** such as access via command line interface (CLI), web interface (Web GUI) or SSH (port 22 TCP) with access lists. Always request user credentials to access computers, whatever method is used.

- Establish secure procedures that allow to **control the establishment and change of access credentials** (either user-password or certificate).
- Generate **user-password credentials and certificates individually** and in accordance with the relevant password policy as this facilitates the user traceability process. Use secure channels to transfer information between devices such as certificates, agents, software, etc. Install Wi-Fi authentication certificates in such a way that they are not exportable or erasable.
- Block unwanted access to systems, either through **firewalls** or by setting up access restrictions on the equipment itself.
- Configure the **three security mechanisms** of the model defined above for connecting client users via Wi-Fi (802.1X, NAC agent and encrypted VPN tunnel).
- Use Wi-Fi access via **IEEE 802.1X** protocol **with EAP-TLS method**. Disable the option to use TLSv1.0 and TLSv1.1.
- Configure the **NAC agent** to check the health status of the device every 30 seconds.
- Use **IKEv2** for IPsec tunnelling.
- Use **centralised authentication systems** such as RADIUS servers and protect communication channels with secure protocols such as RadSec.

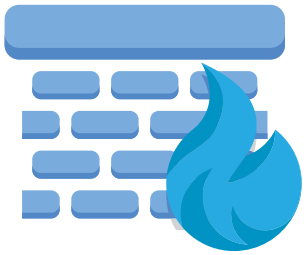
6.4 Configuration of services in the equipment

- Remove all the **information that is configured by default** for those services that you are going to use.
- If possible, use a **DHCP server** outside the Access Point Controller. In addition, it is recommended to configure fixed IP address allocation for each client and that an IP address is not obtained until the user is authenticated.
- Have all devices synchronised in time via **NTP** and enable authentication.
- Use external **SNMP and *syslog*** type servers to collect specific data about the equipment and transactions occurring on the network. Use **SNMPv3** as it includes security improvements of authentication and encrypted data sending with regard to SNMPv1 and SNMPv2.
- Enable only **secure protocols** on the access point controller.
- Prevent denial of service attacks through the establishment of **broadcast and multicast** controls.
- Prohibit or disable all configurations that use **IPv6** if you are not going to use it in your network.
- Enable **FIPS** mode if available.
- Use **access lists** to configure the enabled services for each client machine or device.
- Enable the **Wireless** Intrusion Detection System **(Wireless IDS)** of the Wi-Fi controller if available.

Disable all configurations that use IPv6 if you are not going to use it in your network

6.5 User policies and firewall rules

- Establish **user roles** that allow hierarchical access (with different permissions) to the defined services.
- Limit traffic between users connected to the network: prohibition of peer-to-peer communication through the prevention of **traffic between users**, limitation of port access, etc.
- Establish access lists **(ACLs)** of IP addresses valid only for Wi-Fi clients.
- **Limit the ports** that shall be open on network equipment to the services they are using and preferably require identification and **filtering of applications** regardless of the protocol port used.
- Include mechanisms to prevent or mitigate both ***ARP Spoofing*** and ***IP Spoofing in order to*** avoid Man-In-The-Middle and IP address cloning/spoofing attacks.
- Establish defence control through the configuration of a set of rules of the controller **firewall**.



6.6 Events and system monitoring

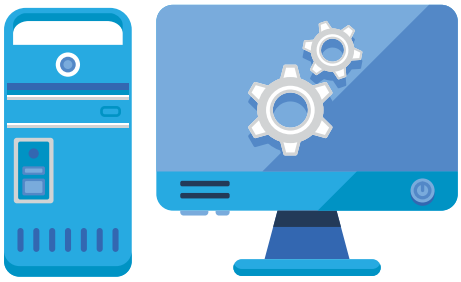
An important point to take into account is the collection of events and the monitoring of system resources to detect possible anomalies that could affect the service.

Some examples of indicators to monitor are CPU, RAM memory, available storage space, active processes, traffic through physical interfaces, established sessions, number of associated and authenticated users, response time of services such as Radius, DHCP and DNS, authentication and association records, equipment temperature, etc.

Resources can be monitored via SNMPv3 or proprietary protocols of the manufacturer's solution. Nowadays it is common to be able to consult the equipment status using web queries via API-REST. It is also common to use mechanisms such as syslog to export system events to a central console.

It is highly recommended to have a SIEM type tool with correlation capabilities over the monitored data and collected system events. It is even possible to perform analysis based on device and user behaviour (UEBA).

In addition to monitoring and correlation, all metrics and events are necessary to carry out a forensic investigation in the event of an incident. It is important to define a policy for the storage and historical processing of events in order to be able to access the data if required in the event of a security incident.



6.7 Other recommendations

- Conduct a **regular vulnerability scan** and consider other configurations that will improve the security of your network.
- **Monitor network traffic** and perform periodic searches for anomalies.
- Implement Intrusion Detection Systems **(IDS)** for the detection of possible anomalies that generate alarms.

7. Basic security decalogue

This Decalogue of good practices aims to lay the foundations for security measures to be taken into account when installing a Wi-Fi network in a corporate environment.

1. **Consider eliminating any wireless access while prioritising wired access. Perform the associated risk analysis and management prior to the implementation of the Wi-Fi network. Analyse the equipment to be purchased, planning the necessary radio coverage and defining the security policy to be applied.**
2. **Conduct an inventory of devices by periodically reviewing the inventory and potential vulnerabilities. Keep all equipment up-to-date, backups and recovery procedures tested.**
3. **Create a dedicated management network, carrying only management and administration traffic, using secure protocols.**
4. **Generate certificates with user and device data. Create different user roles for better security policy enforcement.**
5. **Use centralised authentication systems such as RADIUS servers using secure channels such as RadSec.**
6. **Make a DHCP assignment of fixed IP address for each client/device in each of the different networks.**
7. **Configure the clients to use 802.1X-EAP-TLS, NAC agent and encrypted VPN tunnel as recommended.**
8. **Limit physical and logical access to computers according to the defined roles and disable the service when not in use.**
9. **Implement Intrusion Detection Systems (IDS) for the detection of possible anomalies that generate alarms.**
10. **Monitor network traffic and perform a periodic search for anomalies.**

8. References

CCN-STIC-406 Security in wireless networks:	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 Secure configuration of Aruba network equipment for Wi-Fi environments:	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 Security in wireless networks in the 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 VPN security in the framework of the 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
WPA3-v2.0 Specification published on 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