



Diseño e implantación de redes Wi-Fi seguras

Rafael César Baldeón Guillama
Grado de Ingeniería Informática

María Isabel March Hermo

9 de junio de 2019.

Agradecimientos

A mi mujer Isabel, por su apoyo y esfuerzo durante todos estos años. Sin ella sería imposible.

A mi hijo Daniel, al que pienso recompensarle toda su vida por los momentos perdidos.

A mis padres, por su sacrificio para darme unos estudios y enseñarme a luchar.

A mi "Family" (José, Yaya, Rosi, Carla, Carolina, Alejandro), por ayudarme en esta travesía.

A todos los que me valoran y confían en mí.



Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-CompartirIgual [3.0 España de Creative Commons](https://creativecommons.org/licenses/by-nc-sa/3.0/es/)

B) GNU Free Documentation License (GNU FDL)

Copyright © 2019 Rafael César Baldeón Guillama.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.

A copy of the license is included in the section entitled "GNU Free Documentation License".

C) Copyright

© (el autor/a)

Reservados todos los derechos. Está prohibido la reproducción total o parcial de esta obra por cualquier medio o procedimiento, comprendidos la impresión, la reprografía, el microfilme, el tratamiento informático o cualquier otro sistema, así como la distribución de ejemplares mediante alquiler y préstamo, sin la autorización escrita del autor o de los límites que autorice la Ley de Propiedad Intelectual.

FICHA DEL TRABAJO FINAL

Título del trabajo:	Diseño e implantación de redes Wi-Fi seguras.
Nombre del autor:	Rafael César Baldeón Guillama
Nombre del consultor:	María Isabel March Hermo
Fecha de entrega (mm/aaaa):	06/2019
Área del Trabajo Final:	Redes de computadores
Titulación:	<i>Grado de Ingeniería Informática</i>
Resumen del Trabajo (máximo 250 palabras):	
<p>En los últimos años se ha producido un incremento de las redes Wi-Fi debido a su facilidad de instalación, flexibilidad y bajo coste. Estas redes presentan grandes ventajas para su implantación en cualquier entorno y su principal finalidad es proporcionar acceso a Internet. Los servicios e información que ofrece Internet han supuesto un gran avance para nuestra sociedad.</p> <p>Sin embargo, este tipo de redes inalámbricas cuentan con el gran inconveniente de la seguridad. Las redes Wi-Fi que no se están correctamente protegidas son vulnerables, y presentan riesgos y amenazas para los usuarios. Asimismo, Internet no está libre de peligros, ya que cada día aumentan los incidentes de seguridad por una insuficiente protección de estos accesos.</p> <p>Uno de los objetivos de este trabajo es proporcionar una amplia visión de las redes Wi-Fi y de la importancia de su seguridad. Para ello, se explicarán los diferentes ataques y vulnerabilidades de este tipo de redes, y se especificarán los nuevos sistemas (WPA3 y <i>Enhanced Open</i>) que servirán para crear soluciones que aporten robustez a la red.</p> <p>Para la protección de los accesos a Internet, se definirán los diferentes perfiles que pueden configurarse según el nivel de seguridad requerido. Aplicar estas herramientas permitirá disminuir las posibles incidencias y minimizar las amenazas sobre los dispositivos en sus comunicaciones en Internet.</p> <p>Finalmente, se expondrán diversas recomendaciones para reducir los riesgos de seguridad, y a través de casos prácticos, se demostrará la eficacia de estas soluciones y configuraciones para la protección de distintos entornos.</p>	

Abstract (in English, 250 words or less):

In recent years there has been an increase in Wi-Fi networks due to its ease of installation, flexibility and low cost. These networks present great advantages for their implementation in any environment and its main purpose is to provide Internet access. The services and information offered by the Internet have been a great step forward for our society.

However, this type of wireless networks have the great disadvantage of security. Wi-Fi networks that are not properly protected are vulnerable, and present risks and threats to users. Likewise, the Internet is not free of dangers, as security incidents increase every day due to insufficient protection of these accesses.

One of the objectives of this work is to provide a broad view of Wi-Fi networks and the importance of their security. For this, the different attacks and vulnerabilities of this type of networks will be explained, and the new systems (WPA3 and Enhanced Open) will be specified that will serve to create solutions that provide robustness to the network.

For the protection of Internet access, the different profiles that can be configured according to the required level of security will be defined. Applying these tools will reduce possible incidents and minimize threats to the devices in their Internet communications.

Finally, several recommendations will be presented to reduce security risks, and through practical cases, the effectiveness of these solutions and configurations for the protection of different environments will be demonstrated.

Palabras clave (entre 4 y 8):

Wi-Fi, WPA3, seguridad, 802.11, ataques, 802.1X, OWE y Radius.

Índice

1. Introducción.....	1
1.1 Contexto y justificación del Trabajo.....	1
1.2 Objetivos del Trabajo.....	1
1.3 Enfoque y método seguido.....	2
1.4 Planificación del Trabajo.....	2
1.5 Breve resumen de productos obtenidos.....	3
1.6 Breve descripción de los otros capítulos de la memoria.....	4
2. Redes inalámbricas (Wi-Fi).....	5
2.1. Conceptos en redes Wi-Fi.....	5
2.2. Estándares Wi-Fi.....	8
2.3. Topologías sobre redes Wi-Fi.....	10
2.4. Monitorización.....	12
3. Seguridad en redes Wi-Fi.....	13
3.1. Ataques a las redes Wi-Fi.....	13
3.2. Protocolos de seguridad Wi-Fi.....	15
3.2.1. WEP.....	17
3.2.2. WPA/WPA2.....	17
3.2.3. WPS.....	18
3.3. Nueva generación de seguridad Wi-Fi.....	19
3.3.1. WPA3.....	19
3.3.2. Wi-Fi Enhanced Open.....	21
3.3.3. Wi-Fi Easy Connect.....	22
4. Medidas adicionales a la seguridad.....	23
4.1. Protocolo 802.1x.....	23
4.2. NAC (Network Access Control).....	25
4.3. WIDS / WIPS.....	26
5. Perfiles de seguridad.....	26
5.1. Firewall.....	27
5.2. IDS/IPS.....	27
5.3. Antimalware.....	28
5.4. Application Control.....	29
5.5. Web filtering.....	30
5.6. Data Loss Prevention.....	30
5.7. SSL-Inspection.....	31
6. Recomendaciones para la implementación de una red Wi-Fi.....	32
6.1. Dispositivos de interconexión.....	32
6.2. Mecanismos de seguridad.....	34
6.3. Medidas adicionales a la seguridad.....	34
6.4. Perfiles de seguridad.....	35
7. Casos prácticos.....	36
7.1. Entornos domésticos.....	37
7.2. Entornos sitios públicos.....	41
7.3. Entornos corporativos.....	46
7.4. Perfiles de seguridad.....	53
8. Conclusiones.....	58
9. Glosario.....	59

10. Bibliografía	61
11. Anexos	63
Anexo 1	63
Anexo 2	65
Anexo 3	66
Anexo 4	68
Anexo 5	69

Lista de figuras

Ilustración 1: Relación de tareas	2
Ilustración 2: Diagrama de Gantt	3
Ilustración 3: Relación de entregas	3
Ilustración 4: Canales banda 2,4 Ghz	6
Ilustración 5: Canales banda 5 GHz	6
Ilustración 6: Punto de acceso	7
Ilustración 7: Router inalámbrico	7
Ilustración 8: Repetidor inalámbrico	8
Ilustración 9: Extensor inalámbrico	8
Ilustración 10: Nuevos nombre estándares Wi-Fi	9
Ilustración 11: Elementos visuales Wi-Fi	10
Ilustración 12: Topología ad-hoc	10
Ilustración 13: Topología infraestructura	11
Ilustración 14: Configuración ESS	11
Ilustración 15: Configuración Mesh/Mallada	12
Ilustración 16: EasyMesh	12
Ilustración 17: SSL-Inspection	32
Ilustración 18: Proceso conexión cliente	16
Ilustración 19: Proceso autenticación cliente	16
Ilustración 20: WPA3-SAE Handshake	20
Ilustración 21: Logotipo Dragonblood	21
Ilustración 22: OWE Handshake	22
Ilustración 23: EasyConnect	22
Ilustración 24: Conexión EAP (Radius)	24
Ilustración 25: EAP-TTLS	24
Ilustración 26: Acceso HTTPS Router Inalámbrico	33
Ilustración 27: Planificación programa Wi-Fi activa	33
Ilustración 28: Monitorización red Wi-Fi	35
Ilustración 29: Funcionalidades NGF	35
Ilustración 30: Detener servicios NetworkManager	36
Ilustración 31: Configuración WPA3-Personal en Router	37
Ilustración 32: Configuración adicional WPA3-Personal	37
Ilustración 33: Fichero cliente WPA3-Personal	38
Ilustración 34: Comando conexión cliente WPA3-Personal	38
Ilustración 35: Información wpa_cli WPA3-Personal	38
Ilustración 36: Captura tráfico WPA3-Personal	39
Ilustración 37: Wireshark handshake WPA3-Personal	39
Ilustración 38: Wireshark SAE	39
Ilustración 39: Wireshark SAE PMF	40
Ilustración 40: Wireshark Integridad WPA3-Personal	40
Ilustración 41: Configuración OWE en Router	41
Ilustración 42: Configurar planificación Wi-Fi activa OWE	41
Ilustración 43: Fichero cliente OWE	42
Ilustración 44: Comando conexión cliente OWE	42
Ilustración 45: Información wpa_cli OWE	42
Ilustración 46: Captura tráfico OWE	43

Ilustración 47: Wireshark OWE Handshake	43
Ilustración 48: Wireshark OWE PMF	43
Ilustración 49: Wireshark OWE Cliente (Diffie Hellman)	44
Ilustración 50: Wireshark OWE Router (Diffie Hellman)	44
Ilustración 51: Wireshark OWE Integridad	45
Ilustración 52: Wireshark OWE Datos cifrados	45
Ilustración 53: Configuración red WPA3-Enterprise	46
Ilustración 54: Configuración WPA3-Enterprise	47
Ilustración 55: Configuración adicional WPA3-Enterprise	47
Ilustración 56: Configuración FreeRadius smb.conf	48
Ilustración 57: Configuración FreeRadius krb5.conf	48
Ilustración 58: Configuración FreeRadius nsswitch.conf	48
Ilustración 59: Configuración FreeRadius radius.conf	49
Ilustración 60: Configuración FreeRadius mschap	49
Ilustración 61: Configuración CA ca.cnf	49
Ilustración 62: Configuración CA server.cnf	49
Ilustración 63: Alta usuario Directorio activo	50
Ilustración 64: Configuración wpa_supplicant WPA3-Enterprise	50
Ilustración 65: Fichero cliente WPA3-Enterprise	50
Ilustración 66: Wireshark WPA3-Enterprise	51
Ilustración 67: Cifrados soportados tarjeta Wi-Fi	51
Ilustración 68: Fichero cliente WPA2-Enterprise	52
Ilustración 69: wpa_cli WPA2-Enterprise	52
Ilustración 70: Topología Firewall UTM	53
Ilustración 71: Página principal Firewall UTM	53
Ilustración 72: Reglas Firewall	53
Ilustración 73: Activación IPS	54
Ilustración 74: Habilitar proxy HTTP	54
Ilustración 75: Perfiles Web Filtering	54
Ilustración 76: Habilitar Web Filtering	55
Ilustración 77: Políticas de acceso	55
Ilustración 78: Políticas de acceso habilitadas	55
Ilustración 79: Habilitar Proxy HTTPS (SSL Inspection)	56
Ilustración 80: Cliente certificado CA (SSI Inspection)	56
Ilustración 81: Detección virus	56
Ilustración 82: Detección contenido bloqueado	56
Ilustración 83: Registro de accesos	57
Ilustración 84: Registro virus detectado	57

1. Introducción

1.1 Contexto y justificación del Trabajo

En los últimos años se están incrementando las implantaciones de redes Wi-Fi en los hogares y organizaciones. En la mayoría de los casos, estas redes no cuentan con los requerimientos de seguridad necesarios para proteger los sistemas, ordenadores o la información que circula en estas conexiones, por lo que muchas de estas redes están expuestas a ataques desde el exterior que podrían afectar a la privacidad de la información, acceso a infraestructura crítica o se podrían realizar acciones ilícitas a través de estas conexiones a Internet.

Algunas de estas redes se usan en sitios públicos (hoteles, restaurantes, bibliotecas, etc.) como servicios a los usuarios. En particular, este tipo de Wi-Fi públicas se configuran de forma abierta (sin contraseña) o con una contraseña que se publica a estos usuarios. Estas redes son las más peligrosas y expuestas porque no implementan ningún sistema de seguridad y, por ello, los atacantes suelen utilizarlas para lograr sus objetivos.

Asimismo, esta proliferación de dispositivos inalámbricos, tanto en las organizaciones como en los hogares, está siendo aprovechada cada vez más por los piratas informáticos para ejecutar sus ofensivas. Además, en estos equipos Wi-Fi aparecen vulnerabilidades que no suelen ser resueltas por los usuarios, quedando estas redes con “agujeros” de seguridad al descubierto.

Por otro lado, el aumento de los ataques desde Internet, a través de los correos electrónicos o navegación, están provocando las paradas de servicios importantes, la pérdida de información, etc. Los usuarios de muchas de las organizaciones se conectan a Internet con la única protección de un programa antivirus instalado en cada equipo, que por norma general no cubren todos estos nuevos tipos de ataque.

Como solución a todos estos problemas de seguridad, en este trabajo se describirán los diferentes tipos de soluciones, como el uso del nuevo estándar WPA3 en las redes domésticas y las infraestructuras empresariales, y la implantación de distintos perfiles de seguridad en los accesos a Internet. Estos sistemas de seguridad se pueden fusionar para lograr unas comunicaciones seguras, proteger la información y los servicios que se prestan en estos modelos de red.

1.2 Objetivos del Trabajo

Los objetivos que se pretenden conseguir en este proyecto son los siguientes:

- Definir los conceptos de las redes Wi-Fi, y las posibles topologías que se pueden configurar.
- Exponer los distintos mecanismos de seguridad de las redes Wi-Fi, incluyendo las nuevas certificaciones.
- Concienciar de los riesgos y brechas de seguridad de este sistema.
- Conocer las medidas adicionales de seguridad para permitir un mayor nivel de control de acceso.

- Desglosar los diferentes perfiles de seguridad para inspeccionar los accesos a Internet.
- Proporcionar los modelos de configuración de estas redes que minimicen los problemas de seguridad.

1.3 Enfoque y método seguido

El enfoque de este trabajo fin de grado se basó en la búsqueda de una solución óptima de seguridad para entornos de redes Wi-Fi. Las soluciones actuales presentan deficiencias y se investigaron los nuevos sistemas de seguridad para conseguir una mayor fiabilidad en estas comunicaciones.

El método seguido para la realización de este proyecto reside en la división de la memoria en una parte teórica y otra práctica. Cada una de estas partes tiene las siguientes características:

- Parte teórica: se recopila e incorpora toda la información relativa a las redes Wi-Fi, los protocolos de seguridad a implantar, medidas adicionales de seguridad, los ataques y vulnerabilidades de este tipo de redes inalámbricas y los perfiles de seguridad.
- Parte práctica: se configura y documenta los entornos más comunes (doméstico, sitios públicos y corporativos) con un alto nivel de seguridad para este tipo de redes. Además, se incluye en esta parte la implementación de una configuración de acceso a Internet de forma segura, mediante el uso de perfiles de seguridad en equipos cortafuegos.

Para lograr los objetivos, se valora positivamente la implementación y documentación de los casos prácticos, ya que han servido para demostrar y concluir la mayor robustez de las soluciones planteadas.

1.4 Planificación del Trabajo

La planificación del trabajo se divide en varias tareas y fases que se detallan a continuación:

Tareas	Días	Inicio	Fin
Entrega del plan de trabajo	6	25-feb.	3-mar.
1ª FASE: Recopilar información sobre las redes Wifi (Seguridad)	13	4-mar.	17-mar.
Recopilar información sobre redes Wi-Fi	6	4-mar.	10-mar.
Recopilar información sobre protocolos de seguridad en redes Wi-Fi	6	11-mar.	17-mar.
2ª FASE: Recopilar información sobre los perfiles de seguridad en Internet	6	18-mar.	24-mar.
3ª FASE: Selección y adquisición del equipamiento o software necesarios	6	25-mar.	31-mar.
4ª FASE: Realización de la parte teórica de la memoria	31	1-abr.	2-may.
Sección Wi-Fi y seguridad	20	1-abr.	21-abr.
Sección Perfiles de seguridad	10	22-abr.	2-may.
5ª FASE: Realización de la parte práctica de la memoria	23	3-may.	26-may.
Implementación y documentación de la configuración Wi-Fi	14	3-may.	17-may.
Implementación y documentación de la configuración perfiles de seguridad	8	18-may.	26-may.
6ª FASE: Revisión de la memoria	13	27-may.	9-jun.
7ª FASE: Preparación y entrega de la presentación	6	10-jun.	16-jun.
8ª FASE: Preguntas del Tribunal	6	17-jun.	23-jun.

Ilustración 1: Relación de tareas

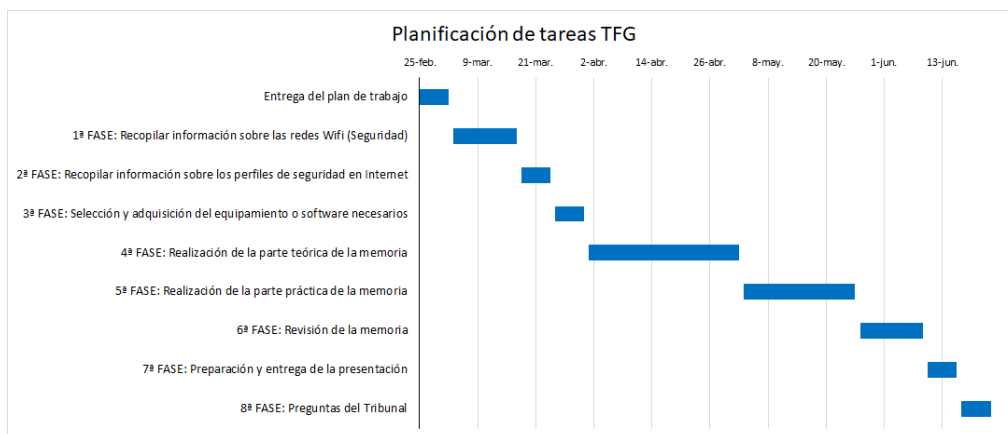


Ilustración 2: Diagrama de Gantt

Asimismo, se han realizado varias entregas, algunas de ellas para comprobar el correcto avance del proyecto, durante el desarrollo del trabajo que se detallan a continuación:

Entregas	Fecha entrega
Plan de trabajo	3-mar.
Primer informe quincenal	16-mar.
Segundo informe quincenal	31-mar.
PEC1	14-abr.
Tercer informe quincenal	27-abr.
Cuarto informe quincenal	12-may.
PEC2	25-jun.
Entrega final	9-jun.
Presentación trabajo	16-jun.
Preguntas Tribunal	23-jun.

Ilustración 3: Relación de entregas

1.5 Breve resumen de productos obtenidos

El producto obtenido es un documento que servirá de referencia para implementar las redes Wi-Fi de forma segura, y configurar una solución de seguridad para proteger a los clientes en los accesos a Internet. Asimismo, se incluyen los distintos problemas de seguridad y vulnerabilidades que presentan las redes inalámbricas, y los diferentes peligros a los que están expuestos los equipos en la navegación en Internet.

Dada la importancia de asegurar y reducir los riesgos en estas redes, se detallan diversos sistemas, protocolos y perfiles de seguridad que provean de un mayor grado de protección en estas redes y clientes.

Con el objetivo de mitigar las posibles brechas de seguridad, se proponen una serie de recomendaciones generales y específicas de configuración según el entorno que se decida implantar. Además, se realizan una serie de casos prácticos con la finalidad de demostrar al lector los beneficios de estas soluciones. Estas pruebas aportan información fundamental para seleccionar los requisitos de seguridad en cualquier escenario.

Finalmente, este trabajo contiene como anexo una serie de manuales que servirán de ayuda a los usuarios para configurar las soluciones propuestas. Todas las guías se han desarrollado de manera que los usuarios pueda llevarlas a la práctica de forma sencilla.

1.6 Breve descripción de los otros capítulos de la memoria

Los capítulos que forman parte de esta memoria son:

Capítulo 2: Descripción de las redes inalámbricas, incluyendo los conceptos, estándares actuales y futuros, y las topologías que se pueden implantar sobre estas redes. Este capítulo es básico para entender la terminología que se desarrolla en los siguientes capítulos.

Capítulo 3: Explicación de los principales ataques a las redes Wi-Fi y los mecanismos de seguridad que existen. Además, se enumeran los protocolos de seguridad, tanto actuales como nuevos, incluyendo sus vulnerabilidades. Este capítulo se exponen los peligros de este tipo de redes inalámbricas, y se utiliza como referente para encontrar las soluciones de seguridad a estos problemas.

Capítulo 4: En esta parte se describen las medidas adicionales de seguridad que aportan un extra de seguridad a las redes Wi-Fi. Una de las medidas que se especifican es el protocolo 802.1x que será utilizada como solución recomendada en los entornos corporativos.

Capítulo 5: En este capítulo se especifican las aplicaciones de seguridad que se pueden configurar en los perfiles de seguridad. Este apartado es necesario para conocer las protecciones a los equipos de los usuarios que se pueden implantar en el acceso a Internet.

Capítulo 6: En este capítulo se enumeran las recomendaciones en las configuraciones de las redes Wi-Fi y en la protección de los accesos a Internet. Este apartado aporta la información fundamental para incrementar el nivel de seguridad de estas redes.

Capítulo 7: Aplicación de los diferentes casos prácticos en los tres entornos (doméstico, sitios públicos y corporativo) más típicos en esta clase de redes inalámbricas. Además, se configura un entorno con perfiles de seguridad sobre un equipo cortafuegos para demostrar la protección sobre los usuarios. En este capítulo se muestran las características de seguridad que proporcionan las recomendaciones y soluciones propuestas.

2. Redes inalámbricas (Wi-Fi)

Una red inalámbrica es un tipo de red que permite la interconexión de dispositivos a través de ondas electromagnéticas, sin utilizar cables o medios alámbricos. El uso de este modelo de red se ha incrementado en estos últimos años debido a la sencillez de instalación y a la flexibilidad que ofrece.

Aunque existen varios tipos de sistemas inalámbricos, este proyecto se basará en la tecnología Wi-Fi. La marca comercial Wi-Fi (Wireless Fidelity) fue creada en el año 1999 por la *Wi-Fi Alliance* (organización que se encarga de certificar los productos que cumplen los estándares 802.11). Aunque en el año 1997 aparece la primera versión del estándar 802.11 con velocidades de 2 Mbps, no es hasta el año 1999 cuando surge la primera versión actualizada de este estándar consiguiendo velocidades de 11 Mbps (802.11b). A partir de este año, la tecnología Wi-Fi se convierte en popular y empiezan a venderse productos con esta denominación.

Las ventajas más importantes, tanto para hogares como para entornos empresariales, que se obtienen con esta tecnología son las siguientes:

- Eliminación del coste del cableado.
- Solventa problemas de conectividad en zonas de difícil acceso mediante cable.
- Solución más económica que los sistemas cableados.
- Rápida implantación y puesta en servicio.
- Facilidad para ampliar la cobertura y cubrir más espacios de trabajo.
- Permite la movilidad de los usuarios.

Debido a estos beneficios, diversas organizaciones optan por este sistema de conexión para su infraestructura de red. Empresas de todos los ámbitos sustituyen sus redes cableadas por sistemas inalámbricos para mejorar la productividad de su personal, ya que estos no dependen de una ubicación fija, sino que pueden trabajar desde en las distintas zonas de los centros de trabajo.

Este tipo de redes cuentan con varias desventajas que principalmente están relacionadas con la seguridad. Algunos de estos inconvenientes se relacionan a continuación:

- Dificultad para limitar la cobertura de la señal inalámbrica.
- Acceso a la señal desde largas distancias.
- Uso de métodos de encriptación desfasados.
- No se controla o monitoriza el acceso a la red inalámbrica

2.1. Conceptos en redes Wi-Fi

Dentro del mundo de las redes Wi-Fi existe una gran variedad de conceptos y neologismos. Cada día aparecen nuevos nombres y denominaciones de los distintos elementos que forman parte de esta tecnología. En la actualidad existe una diversidad de conceptos que se deben conocer para poder entender su funcionamiento.

Estos conceptos se dividen en tres grupos:

- Medios de transmisión

Los medios de transmisión son la vía por la que se transmiten los datos, y en el caso de las redes inalámbricas se encuentra agrupados en los medios de transmisión no guiados. Aunque existen varios tipos de medios de transmisión inalámbricos (Infrarrojo, Bluetooth, etc.), en este apartado se describirá el sistema de conexión por medio de radiofrecuencias.

La radiofrecuencia es un concepto que se aplica a la porción menos energética del espectro electromagnético que se encuentra en el rango de los 3 hercios (Hz) y los 300 Gigahercios (GHz). Esta tecnología es la utilizada por los dispositivos Wi-Fi para las comunicaciones entre los dispositivos. Las bandas utilizadas por este tipo de red son la 2,4 GHz y 5 GHz, y se encuentran dentro de la banda ICM reservadas internacionalmente para fines industriales, científicos y médicos.

En España, la banda de 2,4 GHz cuenta con un ancho total de 100 Megahercios (MHz) que se divide en 13 canales de 22 MHz cada uno. En este caso existen muchos canales superpuestos que se solapan pudiéndose producirse interferencias entre ellos.

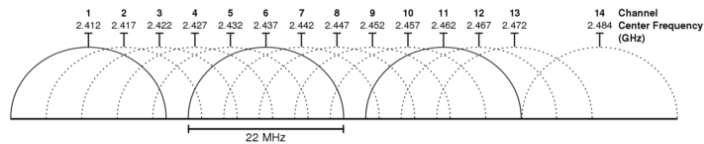


Ilustración 4: Canales banda 2,4 Ghz

Se observa en la imagen que los canales 1, 6 y 11 no se solapan, siendo los canales perfectos para ser utilizados por no competir por ese espacio radioeléctrico.

En el caso de la banda de 5 GHz cuenta con un total de 21 canales de 20 MHz cada uno y se dividen en:

- 5.180 MHz (canal 36) a 5.320 MHz (canal 64)
- 5.500 MHz (canal 100) a 5.700 MHz (canal 140)

En esta banda no se producen solapamiento en los canales que se utilizan, como se puede observar en la siguiente imagen:

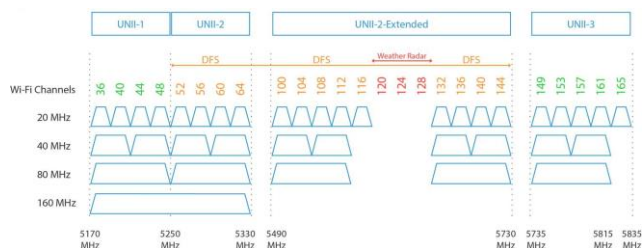


Ilustración 5: Canales banda 5 GHz

Cada una de estas bandas cuentan con sus ventajas y desventajas. En el siguiente cuadro se detallan las diferencias más importantes entre ambas bandas:

	2,4 GHz	5 GHz
Canales	3 canales no superpuestos	21 canales no superpuestos
Interferencias	Muchas interferencias	Menos interferencias
Velocidad Máxima	Menos velocidad	Más velocidad
Ancho de banda	Menor ancho de banda	Mayor ancho de banda
Rango de red	Mayor alcance de red	Menor alcance de red

Por otro lado, hay que indicar que la *Wi-Fi Alliance* ha desarrollado un nuevo estándar denominado WiGig (Wireless Gigabit) que usará la banda de los 60 GHz (entre los 57 y 66 GHz). La conexión WiGig permite la transferencia de datos más rápida al utilizar una banda menos congestionada. El inconveniente de esta banda está en que no puede atravesar muros o paredes, y su máxima cobertura es de 10 metros.

- Equipos de interconexión

Los equipos de interconexión son los elementos que se encargan de comunicar todos los dispositivos en una red Wi-Fi. Entre los equipos más importantes en este grupo se encuentran los siguientes:

- Punto de Acceso: Este dispositivo permite interconectar los dispositivos inalámbricos para formar una red.



Ilustración 6: Punto de acceso

- Router inalámbrico: Es un equipo de red que además de hacer funciones de punto de acceso proporciona un acceso a otra red (principalmente, Internet).

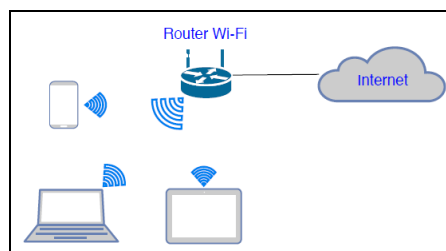


Ilustración 7: Router inalámbrico

- Repetidor inalámbrico: Es un dispositivo que permite ampliar la cobertura de red Wi-Fi. Estos equipos funcionan de manera similar a un punto de acceso, y se conecta a un router o punto de acceso de manera inalámbrica.

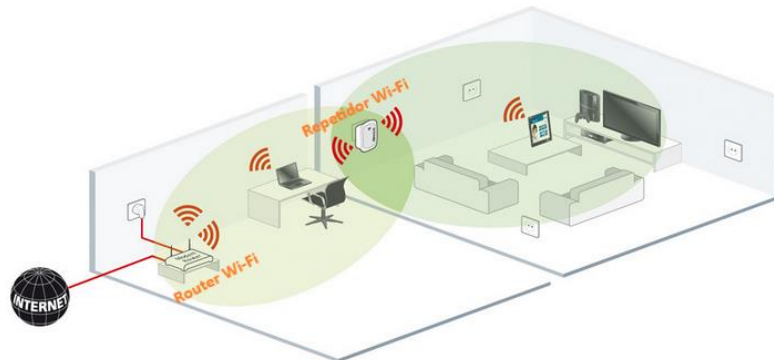


Ilustración 8: Repetidor inalámbrico

- Extensor inalámbrico: Este equipo proporciona una ampliación de cobertura de la red Wi-Fi. Este dispositivo se conecta a un router o punto de acceso a través de un cable.

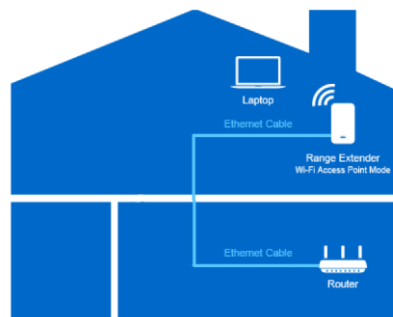


Ilustración 9: Extensor inalámbrico

- Dispositivos finales

Los equipos finales son aquellos que utilizan los usuarios para conectarse a las redes Wi-Fi. En este tipo de dispositivos se engloban los ordenadores, portátiles, *tablets*, *smartphones*, cámaras IP, televisores, etc.. Además, en estos últimos años ha incrementado el número de dispositivos cotidianos (neveras, lavadoras, aspiradoras, etc.), conocidos con el concepto de IoC (Internet de las cosas), que utilizan las redes Wi-Fi para conectarse a Internet.

2.2. Estándares Wi-Fi

Los estándares Wi-Fi llevan evolucionando desde sus primeras versiones, en el año 1997, hasta las nuevas adaptaciones en los últimos años. Las nuevas versiones de estos estándares siempre han buscado el incremento de la velocidad, reducir las latencias y la estabilidad de las conexiones.

Seguidamente, se describirán los principales estándares desde sus comienzos hasta la actualidad:

- IEEE 802.11: Año 1997. Fue el primer estándar que se desarrolló y permitió transmitir a una velocidad de 1 Mbps.
- IEEE 802.11a: Año 1999. Este estándar funciona sobre la banda de 5GHz y la velocidad de transmisión es de 54 Mbps.
- IEEE 802.11b: Año 1999. Esta versión utiliza la banda de 2,4 GHz y consiguió transmitir a 11 Mbps.
- IEEE 802.11g: Año 2003. Este estándar fue el sucesor del 802.11b. Utiliza la banda de 2,4 GHz transmitiendo a velocidades de 54 Mbps.
- IEEE 802.11n: Año 2009. En esta versión se consiguió que los dispositivos se conectaran a las dos frecuencias de 2,4 y 5 GHz, y pueden transmitir a velocidades de 600 Mbps.
- IEEE 802.11ac: Año 2014. En este estándar se pueden utilizar ambas bandas 2,4 y 5 GHz, y se consiguen transmisiones hasta de 1,3 Gbps.
- IEEE 802.11ax: Año 2018-2019. Este estándar trabaja sobre los espectros 2,4 y 5 GHz, utilizando la tecnología MIMO, MU-MIMO y la aplicación de OFDMA con modulación 1024-QAM y pueden alcanzar los 11 Gbps.




En el año 2018, *Wi-Fi Alliance* creó el programa *Generational Wi-Fi* con el objetivo de buscar una nomenclatura más sencilla para los consumidores asignada a las generaciones Wi-Fi. De esta forma, se proporcionan a los usuarios, fabricantes y operadores una descripción más fácil de los productos para permitir reconocer las capacidades de cada dispositivos y conexiones Wi-Fi. Los nuevos nombres de las generaciones son Wi-Fi 4, Wi-Fi 5 y Wi-Fi 6, y cada una de estas denominaciones está relacionada con los estándares de la siguiente:

- 802.11n se corresponde con Wi-Fi 4.
- 802.11ac se corresponde con Wi-Fi 5.
- 802.11ax se corresponde con Wi-Fi 6.



Ilustración 10: Nuevos nombre estándares Wi-Fi

Asimismo, la *Wi-Fi Alliance* presentó unos nuevos elementos visuales de interfaces de usuarios para identificar las generaciones de Wi-Fi. Estos elementos pueden ser usados en los diferentes productos para que sean identificados por los usuarios. Los elementos visuales que están disponibles son:

Generation of network connection	Sample user interface visual
Wi-Fi 6	
Wi-Fi 5	
Wi-Fi 4	

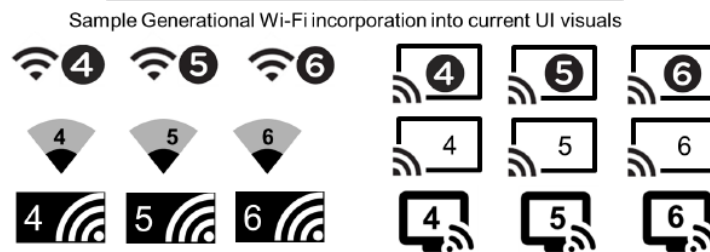


Ilustración 11: Elementos visuales Wi-Fi

2.3. Topologías sobre redes Wi-Fi

Los modos que se definen en el estándar 802.11 son los siguientes:

- **Modo ad-hoc:** Este modelo consiste en la comunicación entre 2 o más dispositivos entre sí con sus adaptadores de red wifi, por lo que no existe un punto de acceso o dispositivo para interconectar estos equipos. Este modo se denomina punto a punto o IBSS (Independent Basic Service Set), y para ser configurado los equipos deben establecer el mismo SSID (Service Set Identifier) y número de canal.

Este modo tiene limitaciones en la cobertura y su rendimiento se reduce cuantos más equipos se conecten a la misma conexión.

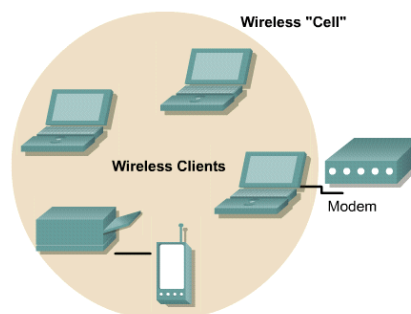


Ilustración 12: Topología ad-hoc

- **Modo infraestructura:** En este modo existe un equipo central, que puede ser un punto de acceso o router inalámbrico, que interconecta a los equipos para formar una red. Los dispositivos se conectan con el elemento central y no entre

ellos. Este modo se denomina BSS (Basic Service Set), y para ser configurado los equipos deben establecer el mismo SSID (Service Set Identifier) y número de canal.

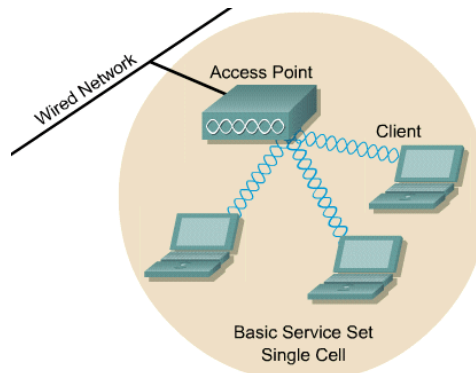


Ilustración 13: Topología infraestructura

Existen otros tipos de topologías que permiten ampliar la disponibilidad de la red y la cobertura de la red. A continuación, se describen las otras configuraciones que se pueden implementar:

- **Extended Service Set (ESS):** En esta topología se unen 2 o más BSS conectados a través de un sistema cableado. Este sistema admite la creación de varias redes inalámbricas de tamaño variable según las necesidades y complejidad. En este modo, los dispositivos se conectan a través del elemento central de la red (punto de acceso), y estos elementos centrales se interconectan entre sí por medio de un sistema cableado.

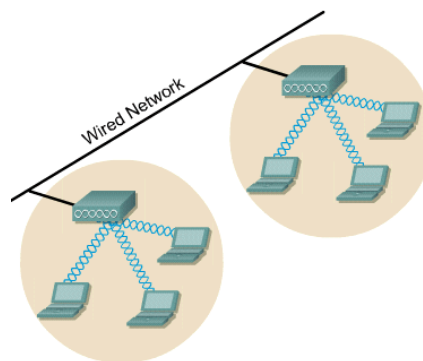


Ilustración 14: Configuración ESS

- **Mallada (Mesh):** En este modelo se mezclan las dos topologías, ad-hoc e infraestructura, para conseguir una arquitectura con mayor cobertura, estabilidad y control. En esta topología existe un elemento central (estación base/router) y los dispositivos satélites (puntos de acceso) que se conectan entre ellos para formar una única red.

Los dispositivos que se conectan a los equipos de esta infraestructura utilizan el mismo SSID y, según el nivel de señal y otros parámetros, se conecta a uno u otro punto de acceso.

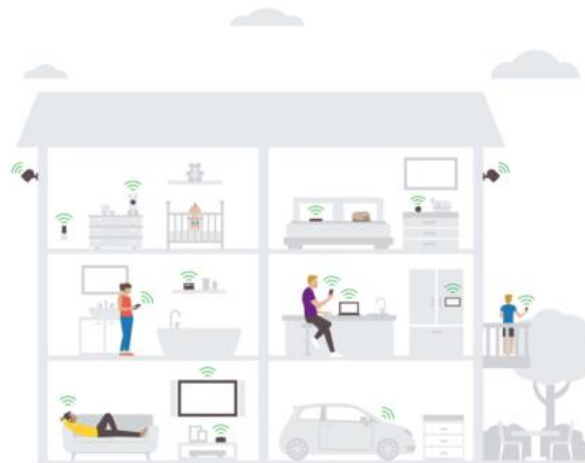


Ilustración 15: Configuración Mesh/Mallada

Desde *Wi-Fi Alliance* se ha creado una certificación para dispositivos que soporten la topología mallada en infraestructuras Wi-Fi denominado *Wi-Fi EasyMesh*. Esta certificación está muy orientada a entornos domésticos, por lo que los productos certificados con este programa son muy fáciles de instalar y usar. Además, una de las características de estos productos certificados es que transforman la estructura de la red según las nuevas necesidades para brindar un conexión estable y rápida.

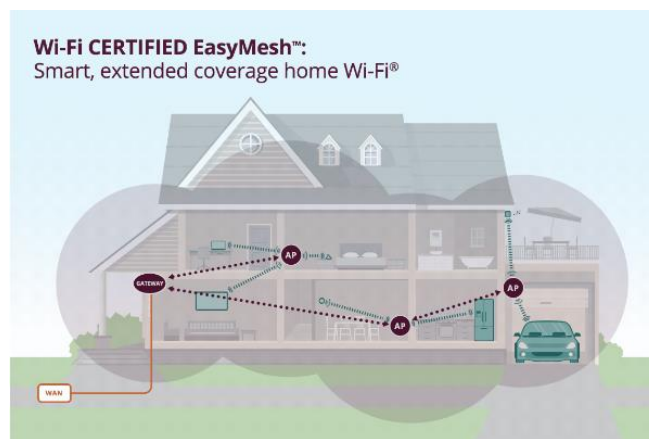


Ilustración 16: EasyMesh

2.4. Monitorización

La monitorización de la red Wi-Fi debe ser una tarea que realizar de forma continua y regular, ya que es necesario disponer de herramientas que informen y alerten de posibles accesos no autorizados a nuestra red. Este tipo de medidas están resueltas en sistemas como el NAC (que se describen en el apartado 4.2), pero para entornos domésticos existen variedad de soluciones que registran las conexiones de los equipos en nuestra red.

Para redes domésticas podemos utilizar herramientas que realizan un escaneo en la red para detectar e inventariar, a través de la dirección IP o dirección MAC, los distintos dispositivos conectados a la red. Después de realizar este escaneo se debe verificar si todos los dispositivos que se encuentran conectados son legítimos. En el caso de que se detecte un equipo desconocido se tiene que realizar las modificaciones necesarias (cambiar contraseña, limitar la cobertura, etc.) en los dispositivos de la red para expulsar al usuario anónimo.

Estas aplicaciones pueden ser vulnerables cuando un atacante modifica y utiliza una dirección MAC (*MAC Spoofing*) o dirección IP (*IP Spoofing*) (ambos conceptos están descritos en el apartado 3.1) de un dispositivo legítimo. En este caso, el equipo pasará desapercibido en nuestra herramienta, ya que lo detectará como equipo confiable.

3. Seguridad en redes Wi-Fi

En este apartado, se describirán los principales ataques a las redes Wi-Fi con la finalidad de exponer una muestra global de los peligros. Además, se detallarán los protocolos y mecanismos de seguridad que se pueden implementar conjuntamente sobre estas redes para eliminar o atenuar estos ataques. Asimismo, en los protocolos de seguridad se especificarán las diferentes vulnerabilidades que sufren cada uno de ellos. En la última parte, se mostrarán los nuevos protocolos de seguridad que desde *Wi-Fi Alliance* se están incorporando al mercado inalámbrico.

3.1. Ataques a las redes Wi-Fi

Antes de describir los diferentes protocolos de seguridad que se pueden aplicar en este tipo de redes, se relacionarán algunas de las más importantes formas de ataques a estas conexiones.

Las redes Wi-Fi cuentan con los mismos problemas de seguridad que las redes cableadas, pero incorporando las vulnerabilidades que presentan las redes inalámbricas. Algunos tipos de ataques están dirigidos a causar daños o incidentes en la red, mientras otros buscan obtener o modificar la información que circula por ella. Se debe tener en cuenta que todos los objetivos pueden estar orientados tanto a organizaciones como a entornos domésticos, por lo que se tiene que preparar la infraestructura para dificultar el ataque y limitar o minimizar el efecto de este.

Según la finalidad del ataque se dividen en:

- Interrupción del servicio: El atacante logra dejar indisponible la red o un servicio determinado.
- Apropiación de la información: El atacante obtiene la información que viaja por la red de manera no autorizada.
- Modificación de los datos: El atacante consigue modificar los datos que circulan en la red.

- Suplantación: El atacante se hace pasar por otro usuario o dispositivo.

Todos estos propósitos tienen su correspondiente clase y técnica de ataque que se basan en vulnerabilidades de los sistemas o en fallos de la configuración. En muchos de los ataques fusionan varios de estas finalidades para conseguir su meta.

En el caso de la apropiación y modificación de la información se puede establecer como uno de los principales objetivos para los atacantes. La información que viaja en la gran parte de las redes inalámbricas es muy sustancial, ya que puede contener datos valiosos para un atacante. Además, si un usuario no autorizado se puede conectar a la infraestructura de una empresa o en un entorno doméstico, y logra acceder a cualquier dispositivo (ordenador, servidor, móvil, etc.), entonces este atacante podrá recopilar gran cantidad de información sensible. Asimismo, cuando el atacante esté conectado podrá recolectar y modificar los datos que pasan por la red.

Para este tipo de objetivos existen varias técnicas de ataque sobre las redes inalámbricas. En algunos de estos métodos no es necesario disponer de la clave de acceso a la red como en los entornos de sistemas abiertos (Redes sin seguridad). Mientras, en otros modelos, el ataque se basa en obtener las contraseña o credenciales para poder conectarse a la red como un usuario legítimo, o las claves de sesión para descifrar la información enviada o suplantar a otro equipo.

Las técnicas de ataque más características en las redes Wi-Fi para son:

- Ataques DoS (Denial of Service) o DDoS (Distributed Denial of Service).

Se produce cuando un usuario no autorizado realiza un ataque a la red para dejarla no disponible. El atacante introduce tráfico en la conexión para producir la desconexión de los usuarios de la red o dejar inoperativo los dispositivos de conexión. También, sobre esta técnica se utilizan inhibidores de señales para interferir los canales e interrumpir la transmisión de la información.

- Man in the middle (MiTM) (Hombre en el medio)

El atacante se incrusta en la comunicación entre dos equipos y puede obtener la información que se envían entre ambos.

- Rogue AP o Fake AP

Esta técnica de ataque consiste en la instalación de un punto de acceso de manera ilegal en ubicaciones, principalmente con mucha afluencia o en organizaciones, para capturar el tráfico de red, y posteriormente utilizar la información obtenida (credenciales, números de tarjeta, etc.) para realizar otros ataques o robar.

En algunas de estas técnicas es necesario suplantar la identidad de un equipo de la red (cliente o dispositivo de interconexión). Para llevar a cabo esta sustitución de identidad se suelen utilizar las siguientes técnicas:

- ARP Spoofing: El atacante envía falsos mensajes ARP al equipo víctima para que asocie la dirección IP de un dispositivo a la dirección MAC del equipo del atacante. Con este método las conexiones que realiza la víctima sobre un dispositivo legítimo se realizarán contra el equipo del atacante.
- MAC Spoofing: En esta técnica el pirata informático modifica la dirección MAC de su sistema operativo para suplantar la dirección MAC de otro equipo. El atacante consigue vulnerar la seguridad de filtrado de direcciones MAC configurada en los dispositivos de interconexión.
- IP Spoofing: La metodología de este ataque se basa en la modificación de la dirección IP del equipo atacante para poder suplantar a un equipo legítimo.

3.2. Protocolos de seguridad Wi-Fi

Antes de comenzar a describir los protocolos de seguridad que se pueden implementar en los dispositivos Wi-Fi, se definirán los distintos mecanismos que se deben cumplir para garantizar y proteger la información que se envía a través de este medio. Estos mecanismos de seguridad son los siguientes:

- Autenticación – Es el mecanismo que verifica al dispositivo en la red. Este proceso se realiza entre el dispositivo cliente y el dispositivo de interconexión (punto de acceso), y existen dos tipos:
 - Autenticación de sistema abierto: En este proceso, el cliente envía una solicitud de autenticación con su ID (MAC del cliente) al punto de acceso, y este último concederá o no el acceso a la red.
 - Autenticación de clave compartida: En este modelo de autenticación se produce un desafío entre el cliente y el punto de acceso. Este método se puede aplicar utilizando uno de los protocolos de seguridad para controlar el acceso a la red.

Tras una correcta autenticación, se realiza el proceso de asociación del cliente en el punto de acceso y el acceso a la red. En este método se reconoce el dispositivo del cliente y se registra en el punto de acceso.

- Privacidad – Este mecanismo consiste en cifrar la información que viaja por la red con el objetivo de que los datos no estén expuestos. En caso de un ataque, la información capturada no sea inteligible por el atacante.

Además de estos dos métodos, se puede incluir un tercer mecanismo denominado integridad, que es el proceso que garantiza que los datos no son modificados durante el envío y recepción de la información entre el cliente y el dispositivo de interconexión.

Se explicará un ejemplo del proceso de unión de un cliente, mediante una autenticación con clave compartida, con el dispositivo de interconexión:

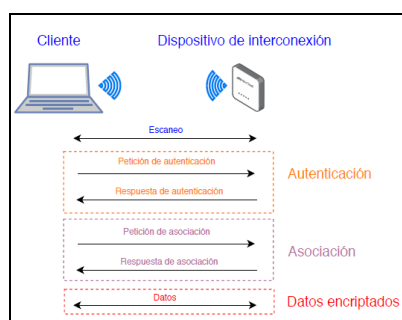


Ilustración 17: Proceso conexión cliente

En este proceso, el cliente realiza un escaneo para encontrar una red accesible para conectarse. El dispositivo de interconexión le envía el SSID (descrito en el apartado 2.3) de la red, entonces el cliente usando la información recibida realiza la petición de autenticación a este dispositivo.

En este proceso el dispositivo envía datos en texto plano como reto, y el cliente responde a este reto con la petición de autenticación con el reto cifrado utilizando la clave compartida. Para finalizar, el dispositivo cifra el reto con la clave compartida y comprueba si es igual al reto encriptado que ha enviado el cliente. En caso de que sean iguales, el dispositivo envía al cliente una respuesta afirmativa de autenticación.

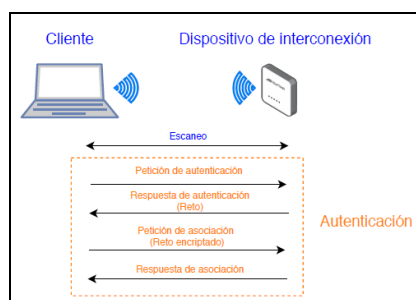


Ilustración 18: Proceso autenticación cliente

Cuando finaliza esta fase de autenticación, el cliente realiza una petición de asociación. Si es aceptada, el dispositivo asigna unos recursos al cliente y le envía un ID de asociación para identificarlo en la red. Finalmente, cuando termina estas dos primeras fases correctamente, el cliente y el dispositivo se produce la transmisión de información de forma cifrada.

A continuación, describiremos los principales protocolos de seguridad, con sus respectivas vulnerabilidades, y las nuevas certificaciones de la *Wi-Fi Alliance*:

- WEP (Apartado 3.2.1)
- WPA/WPA2 (Apartado 3.2.2)
- WPS (Apartado 3.2.3)
- WPA3 (Apartado 3.3.1)
- Wi-Fi *Enhanced Open* (Apartado 3.3.2)
- Wi-Fi *Easy Connect* (Apartado 3.3.3)

3.2.1. WEP

WEP (Wired Equivalent Privacy) es un mecanismo de seguridad que protege las comunicaciones en las redes Wi-Fi. Este algoritmo fue definido en el primer documento del estándar 802.11 en el año 1997 (IEEE 802.11-1997). Con este protocolo se pueden usar los dos métodos de autenticación abierto o clave compartida. Además, emplea el algoritmo de cifrado RC4, sobre el nivel 2 de OSI y con un tamaño de clave de 40 bits, para aportar privacidad y el código de detección de error CRC-32 para proporcionar la integridad.

Además, en la versión *Dynamic WEP* se incluye como sistema de autenticación el uso de los protocolos 802.1x y EAP (Extensible Authentication Protocol).

Vulnerabilidades del protocolo WEP

Desde hace unos años, el protocolo de seguridad WEP presenta brechas de seguridad que permiten descubrir la contraseña de acceso. Tras capturar una gran cantidad de información (vectores de inicialización) de la red se puede obtener la clave WEP. El problema de este protocolo se encuentra en el uso de un algoritmo de cifrado (RC4) débil.

3.2.2. WPA/WPA2

WPA (Wi-Fi Protected Access) es el primero de los nuevos estándares de seguridad tras WEP. Este protocolo fue definido en el estándar 802.11i del año 2004 (IEEE 802.11i-2004) y finalmente incluido en el estándar de 802.11 en el año 2007 (IEEE 802.11i-2007). Este mecanismo de seguridad emplea el protocolo TKIP (Temporal Key Integrity Protocol) para implementar la encriptación y la integridad de la información. TKIP fue adoptado como una solución temporal a las inseguridades que presentaba el sistema WEP. Sin embargo, este nuevo protocolo utiliza el algoritmo de RC4 de WEP para encriptar la información, pero con un tamaño de clave de 128 bits, mientras para la integridad de los datos usa el algoritmo MIC (Michael Integrity Check).

WPA2 (Wi-Fi Protected Access 2) fue introducido en el estándar 802.11 en el año 2004 (IEEE 802.11i-2004). Este nuevo protocolo es la solución de continuidad del protocolo WPA mejorando la encriptación, a través del algoritmo AES (Advanced Encryption Standard), y la integridad con el uso del protocolo CCMP (Counter-Mode / CBC-MAC Protocol). AES es un algoritmo criptográfico simétrico que es más robusto que los anteriores utilizados.

Además, en estos estándares se incluyen nuevos sistemas de autenticación que:

- Permiten autenticar a usuarios individuales mediante el uso de usuario y contraseña sobre un servidor externo.
- Usan una infraestructura formada por el protocolo 802.1x conjuntamente con EAP (Extensible Authentication Protocol)

La *Wi-Fi Alliance* definió dos sistemas de uso para estos protocolos:

- WPA/WPA2-Personal: Se utilizan claves pre compartidas (PSK: *Pre-Shared Keys*)
- WPA/WPA2-Enterprise: Se utilizan servidores de autenticación sobre 802.1x o EAP

Estos nuevos sistemas de autenticación permiten un mayor control de acceso siendo una solución ampliamente usada en organizaciones y empresas.

Vulnerabilidades del protocolo WPA/WPA2

Aunque sean los protocolos con más tiempo en las redes y utilicen algoritmos de cifrados más robusto, estos sistemas tienen vulnerabilidades. En ambas versiones se pueden conseguir la clave de acceso a la red configurados sobre el modo Personal. Las técnicas para obtener estas claves se basan en capturar la información durante el proceso de *4-ways handshake* del protocolo. Con estos datos se realiza el cálculo de la contraseña utilizando un ataque de diccionario. Esta técnica de ataque tiene una alta tasa de acierto cuando se utiliza un diccionario óptimo.

En el año 2017, unos investigadores descubrieron un fallo de seguridad en el protocolo WPA2. La denominación de este ataque es KRACK (Key Reinstallation Attacks) y puede comprometer la información que transita por la red. El funcionamiento de este ataque consiste en conseguir la clave de sesión (no la contraseña precompartida) que se utiliza entre el equipo cliente y el dispositivo de interconexión. Cuando el atacante obtiene esta clave de sesión puede descifrar la información que envía un dispositivo cliente. Incluso, con esta clave se puede descifrar toda la información que se ha recopilado con anterioridad a la obtención de la clave.

3.2.3. WPS

WPS (Wi-Fi Protected Setup) es un sistema que permite, mediante un proceso sencillo, conectar dispositivos a una red Wi-Fi. Los métodos para unir los dispositivos a la red son:

- PBC (Push Botton Configuration): En este modelo, el punto de acceso o enrutador dispone de un botón físico que al ser pulsado permitirá, durante dos minutos, la conexión de los clientes. Este sistema tiene el problema de que tras la pulsación del botón un usuario no conocido o atacante puede conectarse a la red si se encuentra dentro de la zona de cobertura.
- PIN: En las redes que utilicen este procedimiento, únicamente se necesita un código PIN (Personal Identification Number) para conectarse a la red. Este método de conexión es muy fácil de utilizar para integrar en la red dispositivos loC, ya que solo necesita disponer de este código.
- NFC (Near Field Communication): Este modo de configuración permite conectar a la red un dispositivo acercando el dispositivo cliente al punto de acceso. De esta forma, el punto de acceso envía la información de la

configuración al cliente por medio de NFC. Este método es más sólido porque para conectarse a la red se necesita tener acceso físico a los puntos de acceso o enrutadores.

Vulnerabilidades del protocolo WPS

El sistema de WPS sobre PIN es un sistema endeble debido a una mala implementación del protocolo. En la actualidad, existen variedad de herramientas para conseguir el PIN de un punto de acceso, por lo que este sistema es totalmente vulnerable.

3.3. Nueva generación de seguridad Wi-Fi

Después de muchos años usando los protocolos WPA y WPA2, y tras la aparición de la vulnerabilidad sobre estos protocolos que se explota a través de KRACK. La *Wi-Fi Alliance* se encuentra en el proceso de implantación de un nuevo protocolo de seguridad denominado WPA3. Este nuevo sistema aporta un sistema de autenticación más robusto y un incremento de la capacidad de los algoritmos criptográficos. Además, este nuevo estándar permite obtener entornos más simples de configuración y con mayor seguridad.

Además, se expondrán las nuevas certificaciones *Wi-Fi Enhanced Open* y *Wi-Fi Easy Connect* que lograrán mejoras de seguridad en la conexión de los dispositivos a las redes Wi-Fi.

3.3.1. WPA3

Este novedoso protocolo, que es compatible con los dispositivos de WPA2, es actualmente una certificación opcional para los dispositivos Wi-Fi. Dentro de las características de este nuevo sistema de seguridad, hay que indicar que en las redes que implementen este método se añadirán las siguientes mejoras:

- Los últimos métodos de seguridad.
- No se permitirá utilizar protocolos obsoletos.
- Requerirán del uso de *Protected Management Frames* (PMF) para cifrar la información de control o gestión desde el dispositivo de interconexión y el cliente. Con esto se consigue proteger a la red de ataques de deautenticación que fuercen la desconexión de equipos de la red.

Según el propósito y la seguridad que se desee implantar en la red, este protocolo, al igual que WPA2, cuenta con los modos de configuración Personal y Enterprise. En los siguientes apartados describiremos ambos modelos para especificar las nuevas características.

- **WPA3-Personal**

Este protocolo de seguridad ofrece mejor protección a los usuarios, incluso utilizando claves que no cumplen con los requisitos mínimos de seguridad.

Para conseguir este nivel de protección se usa el sistema SAE (Simultaneous Authentication of Equals) que sustituye al WPA2-PSK (descrito en el apartado 3.2.2). Este método de autenticación basado en contraseña se fundamenta en el *DragonFly key exchange* (definido en la RFC 7664). Además, el método SAE aporta las características de PFS (*Perfect Forward Secrecy*), que garantiza que una clave actual no compromete la seguridad de las claves usadas anteriormente, y de protección a ataques de diccionario fuera de línea (offline).

El proceso se inicia con el envío del atributo de la conexión denominado *Robust Security Network Element* (RSNE) que incluye la información de los algoritmos de cifrado y los algoritmos de autenticación soportados por el punto de acceso y el cliente en la conexión.

El funcionamiento del *handshake* de SAE comienza con una contraseña para la autenticación denominada PAKE (Password Authenticated Key Exchange). Tras finalizar este primer *handshake* se obtiene una clave denominada PMK (*Pairwise Master Key*) que se utilizará en el siguiente *4-ways handshake*. Posteriormente, se procede al proceso de asociación entre el cliente y el dispositivo de interconexión.

Cuando finaliza el proceso de asociación, la clave cifrada PMK será usada en el *4-ways handshake* para obtener una clave PTK (*Pairwise Transient Key*) que se utilizará para generar las claves de sesión de la conexión que cifrarán los datos.

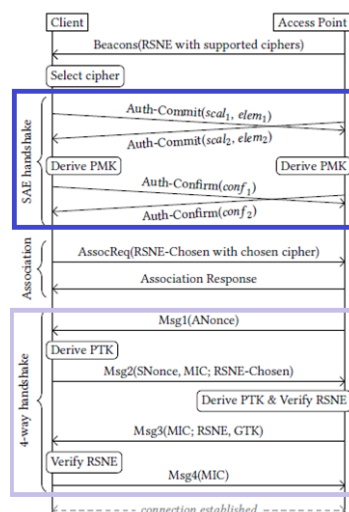


Ilustración 19: WPA3-SAE Handshake

- **WPA3-Enterprise**

Este modelo de seguridad está orientado a organizaciones (empresas, gobiernos, etc.), ya que brinda un mayor nivel de protección a la infraestructura de red. Además, ofrece un modo de configuración opcional con protocolos de seguridad de 192-bit de clave y herramientas criptográficas mejoradas como son:

- **Autenticación:** 256-bit *Galois/Counter Mode Protocol* (GCMP-256)

- **Derivación y confirmación de clave:** 384-bit *Hashed Message Authentication Mode* (HMAC) con *Secure Hash Algorithm* (HMAC-SHA384)
- **Clave de establecimiento y autenticación:** *Elliptic Curve Diffie-Hellman* (ECDH) intercambio y *Elliptic Curve Digital Signature Algorithm* (ECDSA) usando 384-bit.
- **Robusto *Protection Management Frame* (PMF):** 256-bit *Broadcast/Multicast Integrity Protocol Galois Message Authentication Code* (BIP-GMAC-256)

La opción de utilizar 192-bit de clave como modo de seguridad en WPA3-Enterprise garantiza una solución robusta de protección unida con las mejoras de las herramientas criptográficas.

Vulnerabilidades del protocolo WPA3

A principios del mes de abril, los investigadores, que habían descubierto la vulnerabilidad del protocolo WPA2, informaron de las vulnerabilidades que tiene el sistema WPA3. Este ataque al nuevo mecanismo de seguridad para redes Wi-Fi se denomina *DragonBlood*. Uno de los fallos detectados puede hacer que un atacante robe la información de un cliente sin conocer la clave de la red. También, otra de las vulnerabilidades se basa en forzar un *downgrade* del *handshake* para que no use SAE y utilice el de 4-ways, y realizar el mismo ataque que en WPA2.

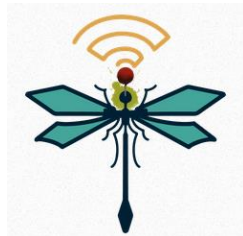


Ilustración 20: Logotipo Dragonblood

Por otro lado, se ha descubierto un ataque de DoS a los puntos de acceso mediante el uso de gran cantidad de *handshake* en WPA3. Incluso, han podido atacar al método EAP-PWD (descrito en el apartado 4.1), sobre RADIUS, que permite conseguir las credenciales del usuario que utiliza para la autenticación.

3.3.2. Wi-Fi Enhanced Open

En la actualidad, existen muchos sitios públicos que ofrecen acceso a Internet a través de redes Wi-Fi abiertas. Este tipo de sistemas presentan un riesgo, ya que los datos que circulan por estas redes son accesibles para cualquier individuo que se encuentre en la zona de cobertura. Además, esta información no está protegida porque no se le aplica ningún sistema de cifrado.

Wi-Fi Alliance ha desarrollado una solución para proteger a los usuarios que se conectan a las redes abiertas. La certificación *Enhanced Open* proporciona protección a los usuarios que se conectan a estas redes, ya que se aplica un cifrado a los datos sobre los usuarios no autenticados. Por medio del protocolo OWE (*Opportunistic*

Wireless Encryption) definido en el RFC 8110, los clientes dispondrán de seguridad en las comunicaciones y los proveedores de estas redes no necesitarán compartir o publicar la contraseña de la red.

En las conexiones sobre OWE, los clientes y los dispositivos de interconexión realizan un intercambio de claves *Diffie-Hellman* durante la asociación. El protocolo *Diffie-Hellman* es un protocolo de establecimiento de claves entre dos clientes que no han tenido contacto previo, mediante un canal inseguro y de forma anónima. La clave obtenida en este primer proceso es utilizada para generar las claves de sesión.

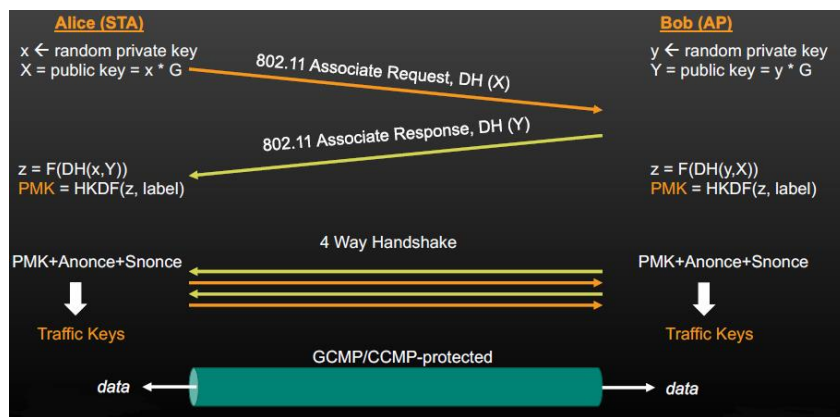


Ilustración 21: OWE Handshake

De esta forma, se consigue que la comunicación esté encriptada y sin que el usuario haya introducido ninguna contraseña. Además, este sistema es compatible con los portales cautivos que se utilizan en algunas de estas redes.

3.3.3. Wi-Fi Easy Connect

La Wi-Fi Alliance ha creado la certificación *Easy Connect* como mecanismo estandarizado para aprovisionar y configurar dispositivos Wi-Fi de una forma sencilla. Este sistema logra reducir la dificultad y mejorar la experiencia del usuario en la asociación de los dispositivos a la red. Los usuarios podrán recibir la configuración de la red mediante el escaneo de un código QR desde su dispositivo. El cliente transmite la información a los dispositivos que desea conectar a la red, y estos se conectan a la red sin utilizar contraseñas o credenciales de acceso.



Ilustración 22: EasyConnect

El sistema *Easy Connect* incorpora un cifrado robusto, por medio de criptografía de clave pública, para asegurar que las redes permanezcan protegidas a medida que se

agregan nuevos equipos. Además, este modelo está orientado a dispositivos loC por la facilidad que se asocian a la red.

4. Medidas adicionales a la seguridad

Después de desarrollar los distintos sistemas de seguridad que se pueden aplicar a las conexiones Wi-Fi, se describirán algunas de las medidas adicionales que se pueden implantar para permitir un mayor control y protección de la red. Hay que indicar estas posibles soluciones están dirigidas a entornos corporativos, ya que el coste de implantación y gestión de estos sistemas es muy elevado.

En este apartado, se describirán las siguientes medidas:

- Protocolo 802.1X
- NAC (*Network Access Control*)
- WIDS/WIPS

4.1. Protocolo 802.1x

802.1x es un protocolo de protección de los puertos de red mediante autenticación. En los entornos Wi-Fi se usa este protocolo en los modelos Enterprise para controlar el acceso a los dispositivos a través de credenciales de acceso o certificados digitales. Los roles que se definen en este sistema son:

- Suplicante: Es el cliente Wi-Fi de la conexión. (Ordenador, móvil, Tablet)
- Autenticador: Es el dispositivo Wi-Fi de interconexión. (Punto de acceso)
- Servidor de autenticación: Es el servidor que dispone de la base de datos con la información de usuarios. (Radius, Microsoft NPS)

Cuando un usuario intenta conectarse a la red, se abre un puerto entre el punto de acceso y el cliente para su validación. El usuario envía los datos de autenticación que son comprobados por el servidor de autenticación. En caso de que las credenciales no sean las correctas, el autenticador cierra el puerto y no permite la conexión del dispositivo a la red.

Para llevar a cabo la autenticación se utiliza el EAP (*Extensible Authentication Protocol*) como protocolo de envío de la información del suplicante al servidor de autenticación.

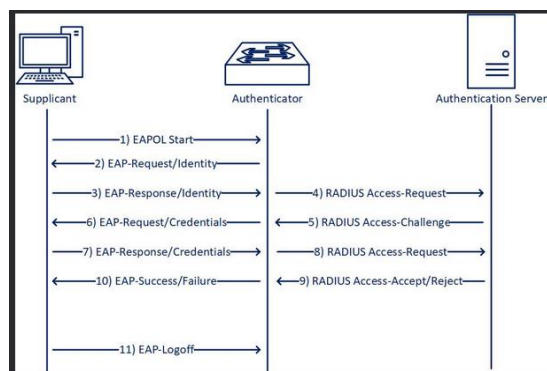


Ilustración 23: Conexión EAP (Radius)

Los métodos que pueden ser utilizados sobre el protocolo EAP son:

- EAP-PEAP (*Protected EAP*): En este método se necesita un certificado en el servidor de autenticación, lo que permite que el cliente verifique el servidor antes de pasar las credenciales por el túnel. Esto facilita la implementación porque los clientes no necesitan certificados, pero es susceptible a ataques MitM (que se describe en el apartado 3.1) si el cliente no es configurado correctamente.
- EAP-TLS: En esta técnica se necesitan certificados en ambos externos (suplicante y servidor de autenticación) siendo una solución más robusta y potente, y resistente a ataques MitM. Dentro de sus ventajas se encuentra la compatibilidad con variedad de dispositivos y con Directorio Activo de Microsoft. Sin embargo, supone más carga de trabajo para la administración, ya que cada dispositivo necesita un certificado válido.
- EAP-TTLS (*Tunneled TLS*): Este método es una extensión del EAP-TLS pero utiliza un canal encriptado para el paso de información al servidor de autenticación. En este sistema se utiliza un servidor intermedio (*proxy*) entre el authenticator y el servidor de autenticación que protege la información desde inicio a fin.

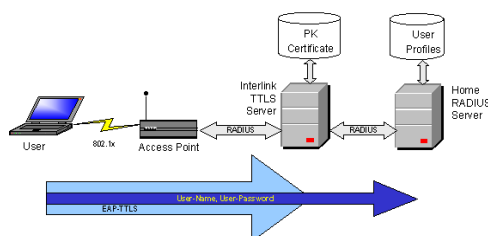


Ilustración 24: EAP-TTLS

- EAP-FAST: Es un método desarrollado originalmente por Cisco y es similar a PEAP pero con mayor complejidad. En la primera fase, el sistema utiliza las PACs (*Protected Access Credentials*) que son claves secretas compartidas que se sirven para autenticarse entre sí (cliente y servidor) y establecer el túnel TLS para la fase dos. En la segunda fase, se produce la autenticación con las credenciales del cliente mediante el envío de esta información a través del túnel TLS. En su implementación no es necesario que el servidor de

autenticación disponga de certificado (aunque es recomendado), pero su complejidad en el diseño compromete su uso.

- EAP-PWD: Es un método que utiliza una contraseña para la autenticación. Este sistema presenta riesgos por ser susceptible a ataques de diccionario.
- EAP-LEAP: Es un método propietario de Cisco que no se sugiere su implementación debido a los problemas de seguridad. El uso de MSCHAP presenta riesgos en el proceso de autenticación.
- EAP-MD5: Este sistema es obsoleto y no se recomienda su uso, ya que es un método inseguro. Uno de sus principales problemas es que no realiza la autenticación del lado servidor.

4.2. NAC (Network Access Control)

NAC es una solución que permite controlar los accesos a la infraestructura de red. Este sistema proporciona una visibilidad completa de la red aportando información importante para la administración y gestión de los dispositivos. Asimismo, esta tecnología proporciona un medio para impedir la conexión de equipos o usuarios no autorizados en la red. Además, esta herramienta monitoriza la red y envía alertas cuando detecta cualquier anomalía en los accesos o tráfico de red que envía un equipo.

Las características más representativas de esta solución son:

- Reconoce a los usuarios, dispositivos y roles en la red.
- Comprueba si los equipos cumplen con las políticas de seguridad (Antivirus, Sistema operativo actualizado, etc.) definidas por la organización. En caso de no cumplir los requisitos, se encarga de aislar el dispositivo de la red.
- Permite el acceso a la red de invitados de forma fácil y segura.
- Elimina las conexiones de equipos no autorizados.
- Audita e informa de los accesos a la red

Además, NAC se puede integrar con soluciones 802.1x para incrementar el nivel de seguridad y confiabilidad de la red. En las implementaciones estándar de los sistemas NAC se suelen incorporar el protocolo 802.1x para realizar el proceso de autenticación en la red.

En la configuración de estos sistemas de forma conjunta se dividen las tareas en:

- NAC: Se encarga de asignar VLAN (Virtual LAN), Direccionamiento IP y aplicar políticas de seguridad. Las VLAN se utilizan para crear redes lógicas en los conmutadores (*switch*), y de esta forma separar o aislar a los dispositivos en redes distintas. Las políticas de seguridad están relacionadas con el tipo de dispositivo o usuario que se conecta.
- 802.1x: Realiza el proceso de autenticación de los usuarios o dispositivos.

4.3. WIDS / WIPS

WIDS (*Wireless Intrusion Detection System*) es un sistema desarrollado para detectar e informar de las intrusiones dentro de las redes Wi-Fi. Mientras que, un WIPS (*Wireless Intrusion Prevention System*) es un sistema o dispositivo que monitoriza la red inalámbrica para localizar incidencias de seguridad y realizar una contramedida de forma automática.

La principal diferencia entre estas tecnologías radica en que la primera detecta y avisa de las intrusiones, y la segunda tras descubrir e informar la incidencia aplica una solución. WIPS es una herramienta más completa, ya que agrega un extra de seguridad a la infraestructura. Las principales categorías que hacen vulnerable una infraestructura de red y que se pueden controlar estos sistemas son:

- Puntos de accesos no autorizados (*Rogue AP*): Son puntos de accesos que se integran dentro del sistema sin la autorización del administrador de la red.
- Puntos de accesos mal configurados: Son dispositivos de interconexión que no cuentan con la configuración de red óptima para garantizar la seguridad.
- Puntos de accesos “Gemelos malignos/*Evil Twin*”: Son puntos de acceso configurados como clones de los puntos de acceso legítimos.

Además, esta solución da una visión completa de la red inalámbrica analizando todo el espectro radioeléctrico y realizando un inventario de equipos y dispositivos para disponer de una seguridad más precisa. En estas herramientas se pueden definir las localizaciones de todos los dispositivos para ayudar conocer la ubicación del lugar donde se están produciendo las incidencias de la red. En algunas configuraciones y productos, se utilizan puntos de accesos dedicados a controlar un espacio de la red con la idea de vigilar zonas específicas más propensas a ataques.

Los sistemas WIPS son necesarios en los entornos empresariales con las capacidades de administración de seguridad y monitorización. Estas soluciones, que pueden encontrarse integradas en la administración de la red, reducen los problemas de seguridad y facilita la gestión de los dispositivos de interconexión, las políticas de seguridad, y simplifica la administración de eventos.

5. Perfiles de seguridad

Desde el comienzo de Internet hasta la actualidad, las amenazas han incrementado de forma exponencial en el ciberespacio. Cada día aparecen nuevos virus, *malware*, *bots*, etcétera, que ponen en riesgos la continuidad de los servicios de una organización o destruyen la información de los usuarios. Para suprimir o minimizar estos peligros se deben implantar sistemas de seguridad que detecten y eliminen estos riesgos.

Como medida de defensa se deben utilizar aplicaciones de seguridad para proteger la infraestructura de red. Estas aplicaciones se pueden agrupar para formar un único

perfil de seguridad. Un perfil de seguridad es un conjunto de acciones que se implementan en la infraestructura de red para proteger el sistema. Estos perfiles se pueden definir según el tipo de información que se desee proteger, el origen del tráfico, el destino del tráfico, etcétera. Además, este tipo de sistemas se pueden adaptar a las necesidades de cada organización.

En este apartado, se describirán una serie de aplicaciones de seguridad orientadas a controlar las conexiones internas y el acceso a Internet.

5.1. Firewall

Un *firewall* o cortafuegos es una aplicación o dispositivo que monitoriza, bloquea o permite las conexiones entre los distintos dispositivos de una red. En la actualidad, los cortafuegos están diseñados para inspeccionar el tráfico de red en las capas 3 (red), 4 (transporte), 5 (sesión), 6 (presentación) y 7 (aplicación) del modelo OSI. Los distintos tipos de *firewall* son:

- Filtrado de paquetes: Es la principal funcionalidad de los cortafuegos y se basa en el control de los accesos a la red por medio de reglas de filtrado utilizando los siguientes atributos:
 - Dirección IP origen o destino
 - Protocolo UDP o TCP
 - Número de puerto origen o destino
 - Contenido de los paquetes
 - Tamaño de los paquetes
- Con estado: Este *firewall* se fundamenta en el cortafuegos de filtrado de paquetes, pero añadiendo la monitorización del estado (inicio, transferencia de información o finalización) de la conexión.
- De aplicación o DPI (*Deep Packet Inspection*): Es un cortafuegos de estado que incorpora inspección del tráfico en la capa de aplicación. Este tipo de *firewall* detecta si sobre un puerto o protocolo estándar se inyecta contenido no deseado o malicioso.

El cortafuegos de aplicación es el más recomendado para cualquier entorno, ya que no solo comprueba el tráfico a nivel de red y transporte, sino que inspecciona el contenido de los paquetes. Este modelo de cortafuegos logra controlar y filtrar el tráfico a nivel de aplicación, por lo que puede comprobar si en la conexión se transmite un virus, una aplicación P2P, aplicaciones del tipo YouTube o Skype, etcétera. Además, el análisis de los paquetes se realiza en tiempo real, lo que evita retrasos en el envío y recepción de los paquetes.

5.2. IDS/IPS

IDS (*Intrusion Detection System*) es un sistema que detecta los accesos no autorizados a los equipos o a la red. Mientras que, IPS (*Intrusion Prevention System*) es una

evolución de IDS que incorpora contramedidas para bloquear los intentos de accesos malintencionados. IDS e IPS suelen utilizar sensores para recolectar el tráfico que se transmite por la red y descubrir las amenazas. Los tres tipos de sensores son:

- Sensores basados en equipo: Este tipo de recolector recibe y analiza los datos del equipo a nivel de sistema operativo. Este tipo de sensor recolecta mucha información, por lo que puede afectar al rendimiento del equipo.
- Sensores basados en red: Este modelo de sensor recopila y analiza la información que se transfiere por la red, por lo tanto, es poco intrusivo. Este sistema de recolección no afecta a los equipos, ya que no cuentan con ninguna aplicación residente en los sistemas.
- Sensores basados en aplicación: Dentro de los sensores basados en equipos, se encuentra este modelo de recolector basado en aplicación. Este tipo de sensor recibe la información de las aplicaciones que están en ejecución en el equipo.

Los sistemas IPS detectan las acciones peligrosas utilizando los siguientes métodos:

- Firmas: Dispone de una base de datos actualizada con las vulnerabilidades conocidas.
- Políticas: Definición de las políticas y acciones a realizar en el sistema.
- Anomalías: Detecta las amenazas basándose en el patrón del funcionamiento normal del tráfico.
- *Honeypot*: Se configura un equipo vulnerable que es interesante para que ser atacado. Desde este equipo se puede obtener información importante del atacante.

Los sistemas IDS solo registran e informan de posibles amenazas o comportamientos extraños en la red. Sin embargo, IPS aporta mayor seguridad y fiabilidad en la infraestructura, ya que implementa acciones de bloqueo para minimizar las amenazas.

Asimismo, un aspecto importante a tener en cuenta sobre esta herramienta es su situación en la infraestructura de red, puesto que una mala ubicación podría afectar al rendimiento del sistema o podría no lograr la seguridad deseada. En la actualidad, estas funcionalidades están incluidas en equipos o aplicaciones cortafuegos, y se suelen aplicar en los accesos a Internet, custodiando la DMZ, y en la capa de distribución de la red para monitorizar el tráfico que se envía desde los clientes.

5.3. Antimalware

Antes de la aparición de Internet existían algunos virus que se introducían en los sistemas a través de los medios de almacenamiento, y su acción no era excesivamente dañina. Tras la aparición de Internet, se ha incrementado la creación de programas maliciosos dada su facilidad de infección y propagación por este medio.

Actualmente, el término *malware* define aquellas aplicaciones que infectan y destruyen un sistema o equipo sin la autorización del usuario.

Existen una gran variedad de programas o aplicaciones maliciosas como son:

- **Virus informático:** Programa informático diseñado para alterar el correcto funcionamiento de un sistema.
- **Gusanos:** Es similar a un virus informático, pero con la propiedad de que no necesita la intervención del usuario para activarse y se propaga automáticamente por la red de ordenadores.
- **Troyano:** Parecido a un virus, aunque su finalidad no es destruir el sistema. Este programa pasa desapercibido para el usuario y abre una puerta trasera con el fin de que otros programas maliciosos acceden al ordenador.
- **Adware:** Este programa tiene la misión de mostrar publicidad de forma continua mientras el usuario navega por Internet.
- **Ransomware:** Este modelo de programa realiza un secuestro de la información del ordenador y solicita un rescate económico al usuario para liberar los datos.
- **Spyware:** Esta aplicación no altera el sistema, sino que recolecta información del sistema o del usuario para enviarla al atacante.

Para reducir estos posibles incidentes, se debe implantar un sistema Antimalware en la conexión a Internet de los usuarios. Estas herramientas Antimalware realizan un análisis estático, en tiempo real, de todo el tráfico que se recibe desde Internet, detectando y bloqueando los programas maliciosos.

Los nuevos productos Antimalware disponen de soluciones *SandBox* que permiten la ejecución de aplicaciones, descarga de archivos desde Internet o navegación por páginas web en un entorno aislado y seguro. Además, *Sandbox* ofrece mejoras en la seguridad mediante la catalogación de archivos sospechosos o detección de ficheros de alto riesgo. Asimismo, algunas de estas utilidades descubren y eliminan las posibles amenazas a través de análisis inteligentes (emulando código, análisis manual, detección de respuesta, etcétera) sobre entornos virtuales separados.

5.4. Application Control

La tecnología *Application Control* detecta y actúa sobre el tráfico de red en función de la aplicación que generó el tráfico. Esta utilidad comprueba, mediante firmas, si el flujo de información se corresponde con cada aplicación y detecta los errores en caso de que una aplicación utilice un puerto o protocolo distinto.

Para las organizaciones es complicado controlar los accesos a las distintas aplicaciones que existen en Internet. En muchas ocasiones, se realizan filtrado de algunos puertos, a través de los cortafuegos, para limitar el acceso a algunas de las aplicaciones. Sin embargo, muchos de los programas utilizan puertos similares (HTTP o HTTPS) para su funcionamiento, por lo que es complicado controlar este tráfico.

Por medio de esta utilidad se puede limitar el uso de aplicaciones específicas o que se encuentren englobadas en un tipo de categoría. Algunos de estas categorías de aplicaciones son:

- Redes sociales (Facebook, Twitter, Instagram)
- P2P (Emule, Bittorrent)
- Juegos (Casas de apuestas, Juegos online)
- Correos electrónicos (Gmail, Outlook)
- Acceso remoto (Teamviewer, Logmein)
- Almacenamiento en la nube (Google Drive, OneDrive)

Con este tipo de herramienta se puede filtrar, monitorizar o bloquear el uso de estas aplicaciones por parte de los usuarios. Las organizaciones pueden definir políticas de seguridad relacionadas con los accesos a las aplicaciones o grupo de aplicaciones categorizadas. Además, se protege a la infraestructura de red de intentos de suplantación de aplicaciones para introducir cualquier tipo de *malware*.

5.5. Web filtering

Web Filtering es una utilidad que permite controlar el contenido que un usuario puede visualizar en Internet. En estos días, es muy importante poder inspeccionar la navegación de los equipos en el ciberespacio, ya que es clave para las organizaciones conseguir una administración y mayor control de las conexiones al exterior. La implantación de un servicio *Web Filtering* es importante por las siguientes razones:

- Empleados que acceden a Internet para asuntos no laborales
- Congestión en el acceso a Internet
- Usuarios con acceso a contenido inapropiado o malicioso
- Acceso a información protegida por derechos de autor

Además, cada día, los ataques desde las páginas web son más sofisticados y dirigidos a diferentes usuarios u organizaciones específicas. Las nuevas formas de ataques, como *Phishing* (método de engaño de los ciberdelincuentes para obtener información de la víctima) o *Pharming* (ataque sobre los sistemas DNS para redirigir a la víctima a los servidores del atacante), obligan a los administradores a implementar sistemas que reduzcan las amenazas y dificulten estos ataques.

5.6. Data Loss Prevention

DLP (*Data Loss Prevention*) o “Fuga de datos” es una herramienta que previene la fuga de datos cuyo origen se encuentra dentro de la organización. Estas aplicaciones están diseñadas con inteligencia artificial para aprender sobre el contenido de los documentos confidenciales y las acciones que realizan los usuarios con estos ficheros. La monitorización de estos recursos por parte de DLP garantiza que no se transmitan

datos confidenciales fuera de la organización. Las causas de las fugas de datos se pueden producir por:

- Usuarios de la organización,
- Acceso de individuos no autorizados,
- *Malware* que se introduce en la red.

El principal propósito de esta utilidad es comprobar y bloquear que no se envíe información a Internet (almacenamiento en la nube, redes sociales, correos electrónicos, etcétera) que incluyan datos confidenciales.

Por otro lado, muchas de las organizaciones deben cumplir normativa como las relacionadas con protección de datos personales (RGDP y LOPD-GDD) o la ley propiedad intelectual (LPI). Algunas de estas herramientas incluyen plantillas para aplicarlas sobre los documentos que se envían al exterior.

5.7. SSL-Inspection

En Internet se ha incrementado el uso de protocolos seguros (HTTPS, POP3S, FTPS, etcétera) en los accesos a los servicios web, ya que este protocolo aplica un cifrado, por medio de una sesión SSL (*Secure Sockets Layer*), en la comunicación que encripta los datos confidenciales en las transmisiones cliente-servidor y servidor-cliente.

Esta funcionalidad es aprovechada por los nuevos programas maliciosos para realizar sus ataques. Uno de los posibles escenarios se produce cuando un usuario descarga y ejecuta un archivo malicioso, esta aplicación abre una sesión HTTPS con el servidor de C&C (Command & Control) y, a través de esta conexión cifrada, se transfiere el *malware* al equipo sin ser detectado.

SSL-Inspection es una solución que descripta las conexiones cifradas para descubrir y bloquear las posibles amenazas. Esta funcionalidad es especialmente utilizada con el protocolo HTTPS, pero también puede ser aplicada a protocolos como FTPS, POP3S, IMAPS y SMTPS.

En las organizaciones ha aumentado la necesidad de implantar *SSL-Inspection* para controlar e interceptar los ataques que se producen por el cifrado de la información. En las configuraciones recomendadas se realiza una inspección completa o profunda de SSL, donde los datos se descifran e inspeccionan para comprobar si está libre de *malware*.

Este procedimiento se basa en la instalación de un dispositivo que hace la función de MitM (*Man in the Middle*) (que se describe en el apartado 3.1) imitando al receptor de la sesión inicial SSL. Posteriormente, el contenido se descifra para una aplicarle la inspección. Una vez que se completa la inspección, el contenido descriptado se vuelve a cifrar y se realiza una nueva sesión de SSL reproduciendo al remitente. Para finalizar, el contenido se vuelve a cifrar y se envía al remitente.

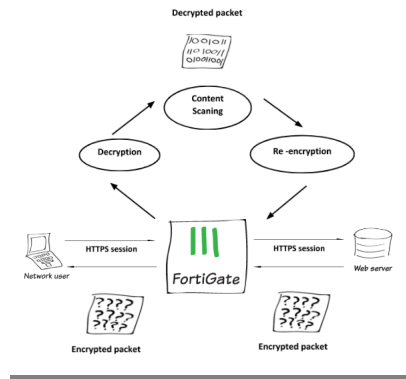


Ilustración 25: SSL-Inspection

Además, se pueden crear listas blancas de dominios o direcciones web para que no se aplique la inspección. Esta característica es necesaria en algunos entornos por motivos de privacidad de la información.

6. Recomendaciones para la implementación de una red Wi-Fi

En este apartado se describirán las principales acciones de seguridad para la implementación de una red Wi-Fi. Inicialmente, se detallarán las recomendaciones de forma general para cualquier infraestructura, y, en el siguiente capítulo, se plantearán las soluciones para cada uno de los entornos domésticos, sitios públicos y organizaciones, ya que son los escenarios más comunes para la configuración de estas redes inalámbricas.

Las recomendaciones generales están orientadas a las acciones a realizar para mejorar la seguridad y minimizar los riesgos de acceso no autorizados a la red. Estas recomendaciones se dividen en los siguientes puntos:

6.1. Dispositivos de interconexión

Los equipos que integran la infraestructura de una red Wi-Fi son los elementos más críticos. A este equipamiento se le debe aplicar medidas de protección para reducir los problemas de seguridad.

Las principales acciones que realizar son:

- Estudio de los dispositivos: Los equipos que formen parte de nuestra infraestructura deben cumplir unas exigencias mínimas de seguridad. Antes de adquirir los dispositivos de interconexión (puntos de acceso, *router*, etc.) se deben analizar y definir nuestras necesidades, y valorar los dispositivos que satisfagan los requisitos de seguridad definidos. Además, estos dispositivos deberán estar certificado por la *Wi-Fi Alliance* para garantizar su seguridad.
- Protocolo de conexión: Muchos dispositivos de interconexión tienen habilitado por defecto el acceso vía HTTP para el acceso al portal de configuración. Este

protocolo envía los datos en texto claro, por lo que se recomienda configurar el acceso por el protocolo HTTPS (TLS 1.2) y SSH (versión 2).



Ilustración 26: Acceso HTTPS Router Inalámbrico

- Claves de acceso: Las claves de acceso que están configuradas por defecto en los dispositivos deben ser sustituidas durante la primera configuración. Los requisitos que deben tener las contraseñas de acceso son los siguientes:
 - Tamaño: Igual o superior a 8 caracteres.
 - Composición: Mayúsculas, minúsculas, números y caracteres especiales.Además, es recomendable modificar esta contraseña cada cierto tiempo (por ejemplo, cada 6 meses).
- Actualización *firmware*: Los fabricantes realizan actualizaciones importantes en los sistemas operativos de estos equipos. Muchas de estas actualizaciones añaden nuevas características, pero también aplican correcciones de errores o parches sobre vulnerabilidades. Por este motivo, es muy importante tener actualizado los dispositivos a las últimas versiones estables.
- Mínima funcionalidad: En la configuración de los dispositivos se debe aplicar el concepto de mínima funcionalidad, es decir, solo tener activado aquellos servicios que se necesitan y desactivar todas las características no se usan.
- Establecer franja horaria (días/horas): En algunos dispositivos se puede limitar las franjas horarias de conexión a la red Wi-Fi. Esta funcionalidad permite activar la red en los periodos que tienen que utilizarse.

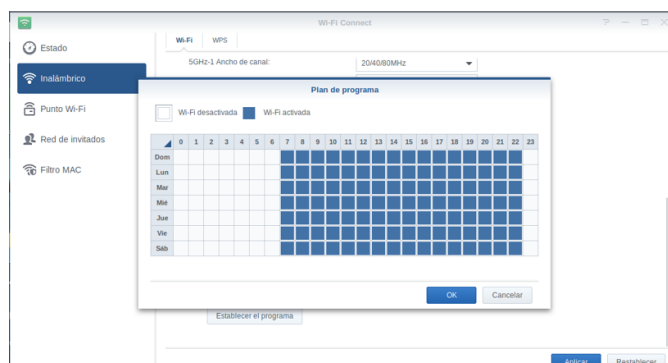


Ilustración 27: Planificación programa Wi-Fi activa

6.2. Mecanismos de seguridad

- WPA3: Como mecanismo de seguridad se recomienda implementar el nuevo protocolo WPA3. Según el modelo de la red se deberá seleccionar el sistema más adecuado, WPA3-Personal para entornos domésticos y sobre infraestructuras empresariales implantar un sistema sobre WPA3-Enterprise. Aunque en entornos WPA3-Personal es más complicado que a través de ataque de diccionarios o fuerza bruta descubrir la contraseña, se recomienda configurar una clave con los mismos requisitos (tamaño y composición) que para el acceso a la gestión de los dispositivos.
- OWE: En sitios públicos (hostelería, bibliotecas, etc.) dejar de utilizar los sistemas abiertos debido a sus problemas de seguridad (tráfico sin cifrar). Es recomendable empezar a utilizar dispositivos certificados en *Wi-Fi Enhanced Open* y configurar el sistema OWE, ya que con este nuevo protocolo se consigue que el tráfico se transmita cifrado protegiendo la información.
- SSID oculto: El SSID que configurado por defecto debe ser modificado, y sustituido por un nuevo SSID oculto. De esta forma, se consigue que los individuos no autorizados no pueden detectar fácilmente el nombre de la red.
- No usar WPS: Debido a las vulnerabilidades de este sistema se recomienda desactivarlo en la primera configuración del dispositivo. En su caso, se plantea el uso de dispositivos certificados en *Wi-Fi Easy Connect*, ya que con este nuevo mecanismo se consigue, de manera sencilla, conectar dispositivos a una red Wi-Fi de forma segura.

6.3. Medidas adicionales a la seguridad

Todas las medidas adicionales que se describieron en este documento son recomendables para ser implementadas en una red inalámbrica. Sin embargo, los dos primeros mecanismos (Protocolo 802.1x y NAC) y los sistemas WIDS/WIPS están más orientados a empresas, ya que los costes de implementación de estas soluciones son muy altos, no solo en lo referente al importe del equipamiento sino a los costes de gestión y mantenimiento de estas infraestructuras.

Por otro lado, la monitorización de la red debe ser llevada a cabo en cualquier entorno. Las redes Wi-Fi tienen que contar con sistemas que monitoricen, controlen y analicen el tráfico de los accesos a la red. Estos controles se pueden realizar de forma proactiva o reactiva, según el nivel de control específico que se necesite. Los controles proactivos se realizan mediante la ejecución de herramientas de monitorización, de forma puntual, para explorar la red y descubrir las posibles amenazas. Mientras que, en los controles reactivos se establecen aquellos eventos y las acciones a realizar (envío de e-mail, SMS, etc.) en los sistemas cuando se detecta cualquier incidente en la red.

En entornos domésticos se recomienda utilizar controles proactivos a través de herramientas (*SoftPerfect WiFi Guard*, *Wireless Network Watcher*, etc.) que se ejecuten de manera regular con el objetivo de detectar intrusos.

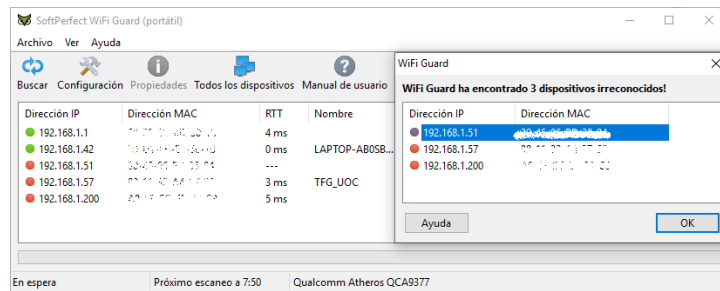


Ilustración 28: Monitorización red Wi-Fi

En entornos empresariales, se aconseja implantar sistemas integrados con las medidas adicionales de seguridad (802.1X, NAC, WIDS/WIPS, etc.) que de manera reactiva avisen e informen de las actividades anómalas o problemas de seguridad.

6.4. Perfiles de seguridad

Este modelo de seguridad está principalmente orientado a las infraestructuras de las organizaciones, ya que en sus redes se conectan un amplio número de dispositivos (portátiles, ordenadores, móviles, etc.) y usuarios con distintos roles. Para aplicar todas las aplicaciones de control descritas en el apartado dedicado a este modelo, se recomienda implantar soluciones *Firewall UTM (Unified Threat Management)* o *NGFW (Next Generation Firewall)*. Con estos tipos de herramientas se consigue ejecutar en un mismo dispositivo (*software* o *hardware*) diferentes aplicaciones de seguridad para controlar y asegurar los accesos a Internet.

Estos modelos aportan la centralización de la configuración de seguridad de la empresa en un único dispositivo. Además, desde estos equipos se puede monitorizar y analizar todo el tráfico de la red hacia Internet. Asimismo, estos cortafuegos mejorados reciben actualizaciones (de forma automática) de los motores y archivos de firmas (*malware*, IDS/IPS, etc.) para lograr mejoras de funcionalidad y seguridad de las aplicaciones.

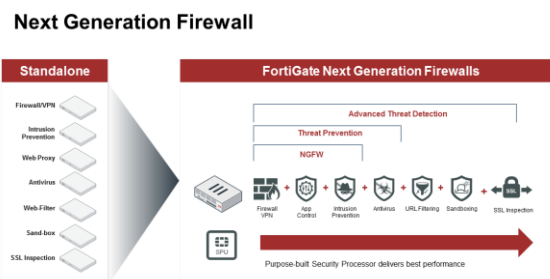


Ilustración 29: Funcionalidades NGF

Se recomienda ubicar este dispositivo, dentro de la topología de red, en la parte más próxima a la conexión a Internet. Además, todo el tráfico que no sea hacia redes internas deberá ser redirigido a este equipo para que sea analizado y se determine si presenta algún tipo de amenaza.

7. Casos prácticos

En esta sección se describirán los casos prácticos realizados en la red laboratorio sobre los entornos más comunes en que se implementan redes inalámbricas. En cada uno de los entornos se detallarán las configuraciones de los dispositivos, la verificación de la seguridad y sus conclusiones. Los entornos que se han implantado en el caso práctico son los siguientes:

- Domésticos
- Sitios públicos
- Corporativos

Para realizar la parte práctica de estas demostraciones se ha creado una red laboratorio formada por los siguientes dispositivos:

- Portátil Lenovo Ideapad 330S
 - Sistema Operativo: Ubuntu Desktop 18.04
 - Tarjeta de red Wifi: Qualcomm Atheros QCA9377
- Portátil Asus F552L
 - Sistema Operativo: Ubuntu Desktop 18.04
 - Tarjeta de red cable: Ralink RTL8111
 - Tarjeta de red wi-fi: Ralink RT3290
- Router Synology MR2000ac
 - Sistema operativo: SRM 1.2-7779 Update 1
 - Equipo certificado por *Wi-Fi Alliance* para WPA3 (Personal y Enterprise) y OWE. (Anexo 1)

Además, se demostrará como un dispositivo UTM, que aplique perfiles de seguridad a la red y a la navegación en Internet, aporta un alto nivel de seguridad en los clientes.

Actualmente, los sistemas WPA3 y OWE no están soportados de forma nativa en los sistemas operativos Linux, Windows, Android o IOS, por lo que para realizar este laboratorio se ha instalado y configurado el componente *wpa_supplicant* (v.2.8) que se encuentra en modo desarrollo (Anexo 2). Este componente es utilizado por las estaciones clientes, principalmente en sistemas operativos Linux, para conectarse a los dispositivos de interconexión (*Authenticator*).

En el cliente Ubuntu se deberá detener y deshabilitar el servicio *NetworkManager* para utilizar el componente *wpa_supplicant*.

```
root@TFG_UOC_2019:~# systemctl stop NetworkManager
root@TFG_UOC_2019:~# systemctl disable NetworkManager
Removed /etc/systemd/system/dbus-org.freedesktop.nm-dispatcher.service.
Removed /etc/systemd/system/multi-user.target.wants/NetworkManager.service.
root@TFG_UOC_2019:~# █
```

Ilustración 30: Detener servicios NetworkManager

Además, con el objetivo de verificar y demostrar el correcto funcionamiento de este nuevo protocolo se ha instalado el conjunto de herramientas *aircrack-ng* y la aplicación

Wireshark. Con estas herramientas se mostrará las principales características de seguridad que aporta el nuevo sistema WPA3 y OWE.

Por otro lado, se ha realizado una actualización del firmware del router Synology MR2200ac, y aplicado un parche de seguridad para mitigar la vulnerabilidad del WPA3 (*Dragonblood*) en este modelo de *router*. (Anexo 3)

7.1. Entornos domésticos

En los entornos domésticos se deberán aplicar las acciones descritas en las recomendaciones generales. Asimismo, en este modelo se aconseja utilizar como mecanismo de seguridad el WPA3-Personal para proteger las conexiones con las nuevas características de seguridad. En los siguientes puntos se especificará el procedimiento para realizar esta configuración en la red laboratorio.

- Configuración del dispositivo de interconexión (Synology MR2200ac)

En este equipo debemos habilitar el nivel de seguridad WPA3-Personal con una clave, y se ocultará el SSID de la red como medida de protección.

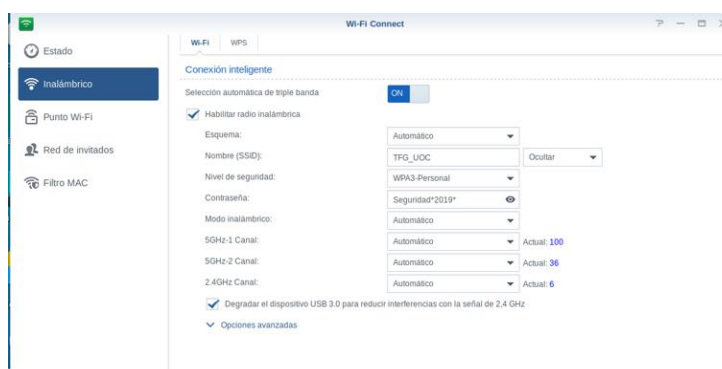


Ilustración 31: Configuración WPA3-Personal en Router

Al seleccionar el nivel de seguridad WPA3-Personal se activa automáticamente la opción de compatibilidad con PMF (*Protected Management Frames*) de forma obligatoria. Además, es conveniente activar el aislamiento de AP, para aislar a los clientes entre sí, y programar una franja horaria para activar la red Wi-Fi.

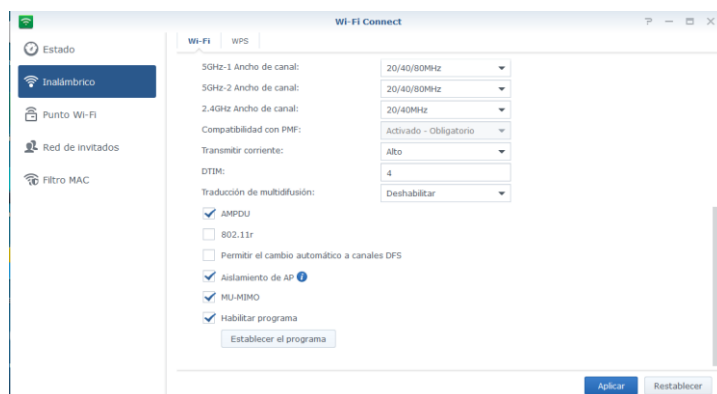


Ilustración 32: Configuración adicional WPA3-Personal

- Configuración del equipo cliente

En el cliente se creará el fichero de configuración (wpa3-TFG_UOC.conf) con los parámetros necesarios que utiliza el *wpa_supplicant* para la conexión. Este fichero se alojará en el directorio `/etc/wpa_supplicant/`

```

root@TFG_UOC_2019:/etc/wpa_supplicant
Update_config=1
ctrl_interface=/run/wpa_supplicant
ctrl_interface_group=adm
network={
    ssid="TFG_UOC"
    psk="Seguridad*2019*"
    scan_ssid=1
    key_mgmt=SAE
    ieee80211w=2
}

```

Ilustración 33: Fichero cliente WPA3-Personal

Las tres primeras líneas del fichero se añaden para que desde la utilidad *wpa_cli* se pueda controlar el componente *wpa_supplicant* y actualizar este fichero de configuración. En la configuración de la red de conexión, se encuentran los parámetros,

- Ssid: Nombre de la red Wi-Fi
- Psk: Clave de la conexión sobre WPA3-Personal
- Scan_ssid: Con valor 1, permite la asociación a dispositivos con ssid ocultos (no broadcast).
- Key_mgmt: Con valor SAE, define el protocolo de seguridad SAE que se utilizará en la autenticación.
- ieee80211w: Con valor 2, activa el uso de PMF de forma obligatoria.

Para la conexión a la red, se ejecutará el siguiente comando,

```

root@TFG_UOC_2019:~# wpa_supplicant -i wlp2s0 -c /etc/wpa_supplicant/wpa3-TFG_UOC.conf &

```

Ilustración 34: Comando conexión cliente WPA3-Personal

Para comprobar la conexión sobre este protocolo, se ejecuta el siguiente comando *wpa_cli*, y se verifica que estamos conectados sobre este protocolo de seguridad.

```

root@TFG_UOC_2019:/etc/wpa_supplicant# wpa_cli -i wlp2s0
wpa_cli v2.8
Copyright (c) 2004-2019, Jouni Malinen <j@wi.fi> and contributors
This software may be distributed under the terms of the BSD license.
See README for more details.

Interactive mode
> status
bssid=00:11:32:a4:e7:57
freq=2437
ssid=TFG_UOC
id=0
mode=station
pairwise_cipher=CCMP
group_cipher=CCMP
key_mgmt=SAE
pmf2
mgmt_group_cipher=BIP
sae_group=19
wpa_state=COMPLETED
ip.address=192.168.1.42
p2p_device_address=30:d1:0b:e1:6e:1b
address=30:d1:0b:e1:6e:1b
uuid=66b077f9-74f0-54c8-930e-773592ab3203

```

Ilustración 35: Información wpa_cli WPA3-Personal

Tras realizar la conexión del cliente al dispositivo de interconexión, se comprobará, con las herramientas *airodump-ng* y *Wireshark*, las nuevas características de seguridad. Se ejecuta el comando *airodump-ng* con los parámetros de la interfaz inalámbrica (canal 6 sobre 2,4 Ghz, dirección MAC del dispositivo de interconexión y nombre del interfaz en modo monitor) y el nombre de los ficheros donde se guardarán las capturas del tráfico,

```
root@cesar-X550LA:/home/cesar/capturas# airodump-ng -c 6 --bssid 00:11:32:a4:e7:57 wlp3s0f0mon -w SAE
```

Ilustración 36: Captura tráfico WPA3-Personal

Tras realizar la captura, se observan las nuevas fases de *handshake* que implementa WPA3-Personal,

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Synology_a4:e7:57	Broadcast	802.11	306	Beacon frame, SN=338, FN=0, Flags=....., BI=100, SSID=Wildcard (Broadcast)
2	4.610818	Synology_a4:e7:57	LiteonTe_e1:6e:1b	802.11	307	Probe Response, SN=212, FN=0, Flags=....., BI=100, SSID=TFG_UOC
3	4.610828	Synology_a4:e7:57	Synology_a4:e7:57	802.11	10	Acknowledgement, Flags=.....
4	9.203276	LiteonTe_e1:6e:1b	Synology_a4:e7:57	802.11	128	Authentication, SN=257, FN=0, Flags=.....
5	9.203780	LiteonTe_e1:6e:1b	LiteonTe_e1:6e:1b	802.11	10	Acknowledgement, Flags=.....
6	9.362498	Synology_a4:e7:57	LiteonTe_e1:6e:1b	802.11	128	Authentication, SN=213, FN=0, Flags=.....
7	9.363018	Synology_a4:e7:57	Synology_a4:e7:57	802.11	10	Acknowledgement, Flags=.....
8	9.395274	LiteonTe_e1:6e:1b	Synology_a4:e7:57	802.11	64	Authentication, SN=258, FN=0, Flags=.....
9	9.395780	LiteonTe_e1:6e:1b	LiteonTe_e1:6e:1b	802.11	10	Acknowledgement, Flags=.....
10	9.397826	Synology_a4:e7:57	LiteonTe_e1:6e:1b	802.11	64	Authentication, SN=214, FN=0, Flags=.....
11	9.397834	Synology_a4:e7:57	Synology_a4:e7:57	802.11	10	Acknowledgement, Flags=.....
12	9.405514	LiteonTe_e1:6e:1b	Synology_a4:e7:57	802.11	161	Association Request, SN=259, FN=0, Flags=....., SSID=TFG_UOC
13	9.405508	LiteonTe_e1:6e:1b	LiteonTe_e1:6e:1b	802.11	10	Acknowledgement, Flags=.....
14	9.410114	Synology_a4:e7:57	LiteonTe_e1:6e:1b	802.11	200	Association Response, SN=215, FN=0, Flags=.....
15	9.410124	Synology_a4:e7:57	Synology_a4:e7:57	802.11	10	Acknowledgement, Flags=.....
16	9.433154	Synology_a4:e7:57	LiteonTe_e1:6e:1b	EAPOL	155	Key (Message 1 of 4)
17	9.433164	Synology_a4:e7:57	Synology_a4:e7:57	802.11	10	Acknowledgement, Flags=.....
18	9.435724	LiteonTe_e1:6e:1b	Synology_a4:e7:57	EAPOL	161	Key (Message 2 of 4)
19	9.436226	LiteonTe_e1:6e:1b	LiteonTe_e1:6e:1b	802.11	10	Acknowledgement, Flags=.....
20	9.449026	Synology_a4:e7:57	LiteonTe_e1:6e:1b	EAPOL	221	Key (Message 3 of 4)
21	9.449034	Synology_a4:e7:57	Synology_a4:e7:57	802.11	10	Acknowledgement, Flags=.....
22	9.452108	LiteonTe_e1:6e:1b	Synology_a4:e7:57	EAPOL	133	Key (Message 4 of 4)
23	9.452100	LiteonTe_e1:6e:1b	LiteonTe_e1:6e:1b	802.11	10	Acknowledgement, Flags=.....

Ilustración 37: Wireshark handshake WPA3-Personal

Además, en la fase SAE-Handshake se puede comprobar el uso del protocolo SAE para la autenticación, cálculo de clave basado en criptografía de curva elíptica (256-bit random ECP group), y los parámetros *scalar* y *element* (descritos en el apartado 3.3.1).

```
> Frame 4: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits)
> IEEE 802.11 Authentication, Flags: .....
v IEEE 802.11 wireless LAN
  v Fixed parameters (104 bytes)
    Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
    SAE Message Type: Commit (1)
    Group Id: 256-bit random ECP group (19)
    Scalar: f0caa6dadcf963a88e417001b71ceb0636f926cb15f2f2f95...
    Finite Field Element: 053e15e40c89479cdb75c629f30d031cae181ecb875919e2...
```

Ilustración 38: Wireshark SAE

En la fase de asociación se puede observar el uso de SAE, del protocolo de cifrado AES CCMP de 128 bits y del protocolo de encriptación BIP-CMAC-128 de 128 bits para PMF.

```

    Tagged parameters (133 bytes)
    > Tag: SSID parameter set: TFG_UOC
    > Tag: Supported Rates 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
    > Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    > Tag: Power Capability Min: 0, Max: 20
    > Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 26
      RSN Version: 1
      > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM) CCMP-128 (128 bits)
      Pairwise Cipher Suite Count: 1
      > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM) CCMP-128 (128 bits)
      Auth Key Management (AKM) Suite Count: 1
      > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) SAE (SHA256) CCMP-128 (128 bits) + SHA256
      > RSN Capabilities: 0x00c0
        .... = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
        .... = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
        .... = RSN PTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STakeySA (0x0)
        .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STakeySA (0x0)
        .... = Management Frame Protection Required: True
        .... = Management Frame Protection Capable: True
        .... = Joint Multi-band RSNA: False
        .... = PeerKey Enabled: False
      PMKID Count: 0
      PMKID List
      > Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
        Group Management Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
        Group Management Cipher Suite type: BIP (128) (6)
      > Tag: HT Capabilities (802.11n D1.10)
      > Tag: Extended Capabilities (8 octets)
      > Tag: RM Enabled Capabilities (5 octets)
      > Tag: Supported Operating Classes
  
```

Ilustración 39: Wireshark SAE PMF

En la fase de 4-way handshake, se observa que el tercer mensaje incluye el Nonce (256 bits) y el envío del parámetro MIC (integridad) de 128 bits para generar la clave sesión,

```

    802.1X Authentication
      Version: 802.1X-2004 (2)
      Type: Key (3)
      Length: 183
      Key Descriptor Type: EAPOL RSN Key (2)
      [Message number: 3]
      > Key Information: 0x13c8
      Key Length: 16
      Replay Counter: 2
      WPA Key Nonce: f6290f329e028a77fbfbbcb24ef013765a6c14f44c6df8aad... Nonce 256 bits
      Key IV: 00000000000000000000000000000000
      WPA Key RSC: 0000000000000000
      WPA Key ID: 0000000000000000
      WPA Key MIC: 9c5aaeda3a28b0e041648264c1d3f752 Integridad 128 bits
      WPA Key Data Length: 08
      WPA Key Data: 766c714668ef0fb742b80f3fb18d4914e4f99c0bf08ad4f1...
  
```

0000	88 02 3a 01 30 d1 6b e1 6e 1b 00 11 32 a4 e7 57	...	0:k: n: 2: W
0010	00 11 32 a4 e7 57 10 00 06 00 aa aa 03 00 00 00	...	2: W:
0020	88 8e 02 03 00 b7 02 13 c8 00 10 00 00 00 00 00
0030	00 00 02 fe 29 0f 32 9e 02 8a 77 bf bb cb 24 ef	...	2: W:
0040	01 37 65 ae c1 4f 44 c0 df 8a ad 85 96 10 67 71	...	7e: 0D:
0050	02 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Ilustración 40: Wireshark Integridad WPA3-Personal

Conclusión

Se concluye que el protocolo WPA3 aporta mayor seguridad que WPA2-Personal, ya que implementa un sistema de *handshake* (SAE) que resuelve la vulnerabilidad de KRACK. Además, utiliza un cifrado de 128 bits que dificulta el descubrimiento de la contraseña, ya sea por ataque de diccionario o por fuerza bruta. Asimismo, la utilización de criptografía de curva elíptica aporta PFS (*Perfect Forward Secrecy*), por lo que un atacante que obtuviera la contraseña, por cualquier medio, no podría descifrar las comunicaciones que hubiera capturado anteriormente, ya que la contraseña no forma parte de la clave de sesión (PTK).

7.2. Entornos sitios públicos

Los sitios públicos (restaurantes, tiendas, centros comerciales, etc.) son lugares donde se publican redes abiertas para los clientes sin ningún tipo de autenticación.

En este tipo de redes se deberán aplicar las acciones descritas en las recomendaciones generales. Asimismo, en este modelo se aconseja utilizar como mecanismo de seguridad el OWE, con un dispositivo certificado *Enhanced-Open*, ya que aporta mayor seguridad que las redes abiertas sin control.

En los siguientes puntos se especificará el procedimiento para realizar esta configuración en la red laboratorio.

- Configuración del dispositivo de interconexión (Synology MR2200ac)

En este equipo existe la posibilidad de activar una red de invitados debemos con nivel de seguridad OWE. Es recomendable que esta red de invitados esté aislada de la red local mediante la desactivación del parámetro “Permitir acceder a mi red local”.

En este caso, no se puede ocultar el SSID de la red, ya que es necesario que el cliente pueda conocerlo. Además, es recomendable fijar un número máximo de conexiones de los clientes.

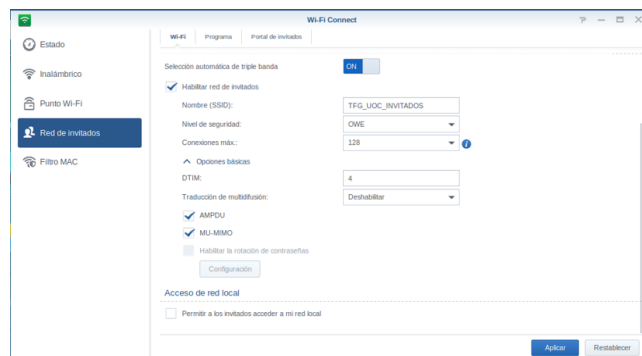


Ilustración 41: Configuración OWE en Router

Además, se puede programar una franja horaria para desactivar la red Wi-Fi en los horarios que no se necesitan.

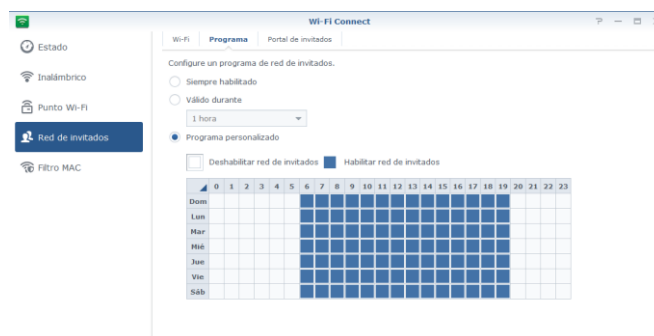
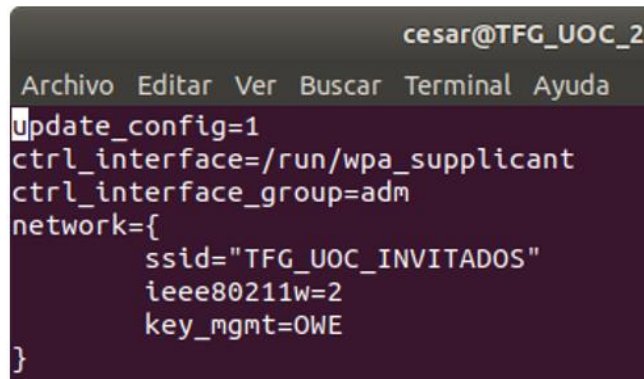


Ilustración 42: Configurar planificación Wi-Fi activa OWE

- Configuración del equipo cliente

El fichero de configuración (OWE-TFG_UOC.conf) con los parámetros necesarios que utiliza el *wpa_supplicant* para la conexión. Este fichero se alojará en el directorio */etc/wpa_supplicant/*



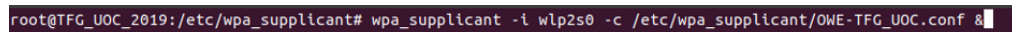
```
cesar@TFG_UOC_2019:~$ cat /etc/wpa_supplicant/OWE-TFG_UOC.conf
Update_config=1
ctrl_interface=/run/wpa_supplicant
ctrl_interface_group=adm
network={
    ssid="TFG_UOC_INVITADOS"
    ieee80211w=2
    key_mgmt=OWE
}
```

Ilustración 43: Fichero cliente OWE

Las tres primeras líneas del fichero se añaden para que desde la utilidad *wpa_cli* se pueda controlar el componente *wpa_supplicant* y actualizar este fichero de configuración. En la configuración de la red de conexión, se encuentran los parámetros,

- Ssid: Nombre de la red Wi-Fi
- Key_mgmt: Con valor OWE, define el protocolo de seguridad OWE que se utilizará en la autenticación.
- ieee80211w: Con valor 2, activa el uso de PMF de forma obligatoria.

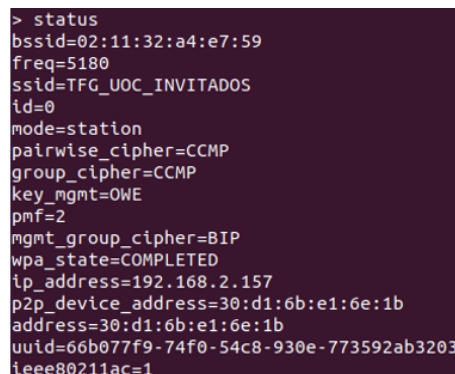
Para la conexión a la red, se ejecutará el siguiente comando,



```
root@TFG_UOC_2019:/etc/wpa_supplicant# wpa_supplicant -i wlp2s0 -c /etc/wpa_supplicant/OWE-TFG_UOC.conf &
```

Ilustración 44: Comando conexión cliente OWE

Para comprobar la conexión sobre este protocolo, se ejecuta el siguiente comando *wpa_cli*, y se verifica que estamos conectados sobre este protocolo de seguridad.



```
> status
bssid=02:11:32:a4:e7:59
freq=5180
ssid=TFG_UOC_INVITADOS
id=0
mode=station
pairwise_cipher=CCMP
group_cipher=CCMP
key_mgmt=OWE
pmf=2
mgmt_group_cipher=BIP
wpa_state=COMPLETED
ip_address=192.168.2.157
p2p_device_address=30:d1:6b:e1:6e:1b
address=30:d1:6b:e1:6e:1b
uuid=66b077f9-74f0-54c8-930e-773592ab3203
ieee80211ac=1
```

Ilustración 45: Información *wpa_cli* OWE

Se ejecuta el comando airodump-ng con los parámetros de la interfaz inalámbrica (canal 6 sobre 2,4 Ghz, dirección MAC del dispositivo de interconexión y nombre de la interfaz en modo monitor) y el nombre de los ficheros donde se guardarán las capturas del tráfico,

```
root@cesar-X550LA:/home/cesar# airodump-ng -c 6 --bssid 00:11:32:a4:e7:57 wlp3s0f0mon -w OWE
```

Ilustración 46: Captura tráfico OWE

Tras realizar la captura, se muestran la negociación que realiza el protocolo OWE,

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Synology_a4:e7:57	Broadcast	802.11	325	Beacon frame, SN=352, FN=0, Flags=....., BI=100, SSID=TFG_UOC_INVITADOS
2	4.074750	Synology_a4:e7:57	LiteonTe_e1:6e:1b	802.11	317	Probe Response, SN=210, FN=0, Flags=....., BI=100, SSID=TFG_UOC_INVITADOS
3	4.074760	Synology_a4:e7:57	Synology_a4:e7:57	802.11	10	Acknowledgement, Flags=.....
4	8.663110	LiteonTe_e1:6e:1b	Synology_a4:e7:57	802.11	30	Authentication, SN=257, FN=0, Flags=.....
5	8.663614	Synology_a4:e7:57	LiteonTe_e1:6e:1b	802.11	10	Acknowledgement, Flags=.....
6	8.667710	Synology_a4:e7:57	LiteonTe_e1:6e:1b	802.11	30	Authentication, SN=219, FN=0, Flags=.....
7	8.668230	Synology_a4:e7:57	Synology_a4:e7:57	802.11	10	Acknowledgement, Flags=.....
8	8.673350	LiteonTe_e1:6e:1b	Synology_a4:e7:57	802.11	208	Association Request, SN=258, FN=0, Flags=....., SSID=TFG_UOC_INVITADOS
9	8.673344	LiteonTe_e1:6e:1b	LiteonTe_e1:6e:1b	802.11	10	Acknowledgement, Flags=.....
10	8.693822	Synology_a4:e7:57	LiteonTe_e1:6e:1b	802.11	259	Association Response, SN=220, FN=0, Flags=.....
11	8.693832	Synology_a4:e7:57	Synology_a4:e7:57	802.11	10	Acknowledgement, Flags=.....
12	8.716862	Synology_a4:e7:57	LiteonTe_e1:6e:1b	EAPOL	133	Key (Message 1 of 4)
13	8.716870	Synology_a4:e7:57	Synology_a4:e7:57	802.11	10	Acknowledgement, Flags=.....
14	8.718918	LiteonTe_e1:6e:1b	Synology_a4:e7:57	EAPOL	161	Key (Message 2 of 4)
15	8.719422	Synology_a4:e7:57	LiteonTe_e1:6e:1b	802.11	10	Acknowledgement, Flags=.....
16	8.732222	Synology_a4:e7:57	LiteonTe_e1:6e:1b	EAPOL	221	Key (Message 3 of 4)
17	8.732742	Synology_a4:e7:57	Synology_a4:e7:57	802.11	10	Acknowledgement, Flags=.....
18	8.734792	LiteonTe_e1:6e:1b	Synology_a4:e7:57	EAPOL	133	Key (Message 4 of 4)
19	8.735296	LiteonTe_e1:6e:1b	LiteonTe_e1:6e:1b	802.11	10	Acknowledgement, Flags=.....

Ilustración 47: Wireshark OWE Handshake

En la fase asociación se puede comprobar el uso del protocolo OWE para la autenticación. Asimismo, se observa la utilización del protocolo de encriptación AES CCMP de 128 bits y el cifrado BIP-CMAC-128 sobre las tramas de gestión (PMF).

```

  Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 26
    RSN Version: 1
    Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM) CCMP-128 (128 bits)
      Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Group Cipher Suite type: AES (CCM) (4)
    Pairwise Cipher Suite Count: 1
    Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM) CCMP-128 (128 bits)
      Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
    Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) Opportunistic Wireless Encryption OWE
      Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) Opportunistic Wireless Encryption
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: Opportunistic Wireless Encryption (18)
    RSN Capabilities: 0x00c0
      .....0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .....0 = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .....00 = RSN PTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STakeySA (0x0)
      .....00 = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STakeySA (0x0)
      .....1 = Management Frame Protection Required: True
      .....1 = Management Frame Protection Capable: True
      .....0 = Joint Multi-band RSNA: False
      .....0 = PeerKey Enabled: False
    PMKID Count: 0
    PMKID List
    Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
      Group Management Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Group Management Cipher Suite type: BIP (128) (6)
  
```

Ilustración 48: Wireshark OWE PMF

En esta fase de asociación, se utiliza el protocolo Diffie-Hellman para el establecimiento de clave. El cliente envía su parámetro clave pública (256 bits) al dispositivo de interconexión donde se encuentra la clave cifrada.

```

> Frame 8: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits)
> IEEE 802.11 Association Request, Flags: .....
  IEEE 802.11 wireless LAN
    Fixed parameters (4 bytes)
      Capabilities Information: 0x1431
      Listen Interval: 0x0005
    Tagged parameters (180 bytes)
      Tag: SSID parameter set: FFG_UOC_INVITADOS
      Tag: Supported Rates 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
      Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
      Tag: Power Capability Min: 0, Max: 20
      Tag: RSN Information
      Tag: HT Capabilities (802.11n D1.10)
      Tag: Extended Capabilities (8 octets)
      Tag: RM Enabled Capabilities (5 octets)
      Tag: Supported Operating Classes
    Ext Tag: OWE Diffie-Hellman Parameter
      Tag Number: Element ID Extension (255)
      Ext Tag Length: 34
      Ext Tag Number: OWE Diffie-Hellman Parameter (32)
      Group: 256-bit random ECP group (19)
      Public Key: 1d4c29995cebfb82ddcdcee5fa57fc4acb1027c36cbec5...
    Tag: Vendor Specific: Microsoft Corp.: WPA/WME: Information Element

0000 00 00 38 01 00 11 32 a4 e7 57 30 d1 6b c1 6e 1b .....2..W0.k:n
0010 00 11 32 a4 e7 57 20 10 31 14 05 00 00 11 54 46 ..2..W..1...TF
0020 47 5f 55 4f 43 5f 49 4e 56 49 54 41 44 4f 53 01 G_UOC_IN_VITADOS-
0030 08 02 04 0b 16 0c 12 18 24 32 04 30 48 00 6c 21 ..... $2:0H`!l
0040 02 00 14 30 1a 01 00 00 0f ac 04 01 00 00 0f ac .....0.....
0050 04 01 00 00 0f ac 12 c0 00 00 00 00 0f ac 0e 2d .....
0060 1a 5f 19 1b ff 00 00 00 00 00 00 00 00 00 00 00 .....o.....
0070 01 00 00 00 00 00 00 00 00 00 7f 03 04 00 00 .....
0080 00 01 00 00 40 4e 05 70 00 00 00 3b 14 51 51 .....@f.p...:QQ
0090 53 54 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 STstuvwx yz{|}~
00a0 01 02 ff 23 20 13 00 1d 4c 29 99 5c be f8 2d dd .....#...L)...
00b0 dc dc ee 5f a5 76 fc 4a cb 10 27 c3 6c be c5 27 .....v.v.j...}...
00c0 59 59 9c 60 2b a2 a3 dd 07 00 50 f2 02 00 01 00 .....v.v.z...}...p.....
Bytes 167-198: Public Key ( wlan_ext_tag_owe_oh_parameter_public_key)

```

Ilustración 49: Wireshark OWE Cliente (Diffie Hellman)

El dispositivo de interconexión contesta a esta solicitud con su parámetro de clave pública (256 bits) al cliente,

```

> Frame 10: 259 bytes on wire (2072 bits), 259 bytes captured (2072 bits)
> IEEE 802.11 Association Response, Flags: .....
  IEEE 802.11 wireless LAN
    Fixed parameters (6 bytes)
    Tagged parameters (229 bytes)
      Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
      Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
      Tag: RM Enabled Capabilities (5 octets)
      Tag: HT Capabilities (802.11n D1.10)
      Tag: HT Information (802.11n D1.10)
      Tag: Overlapping BSS Scan Parameters
      Tag: Extended Capabilities (8 octets)
      Tag: Vendor Specific: Microsoft Corp.: WPA/WME: Parameter Element
      Tag: Vendor Specific: Qualcomm Inc.
      Tag: Vendor Specific: Qualcomm Inc.
      Tag: RSN Information
    Ext Tag: OWE Diffie-Hellman Parameter
      Tag Number: Element ID Extension (255)
      Ext Tag Length: 34
      Ext Tag Number: OWE Diffie-Hellman Parameter (32)
      Group: 256-bit random ECP group (19)
      Public Key: 2de768084d10bc4f3df9e44cf9673bf530740e9c8744cbe...

0000 00 27 a4 00 00 42 43 5e 00 62 32 2f 00 dd 1f 8c .....BC^ b2/....
0010 fd f0 00 00 01 01 00 00 01 00 00 00 00 00 00 .....
0020 ff ff 16 11 32 a4 e7 58 00 11 32 a4 e7 57 dd 08 .....X..2..W...
0030 8c fd f0 01 01 02 01 00 30 14 01 00 00 0f ac 04 .....0.....
0040 01 00 00 0f ac 04 01 00 00 0f ac 12 cc 00 ff 23 .....h..H...0...#
0050 20 13 00 1d 4c 29 99 5c be f8 2d dd .....h..H...0...#
0060 96 73 bf 53 07 40 a9 c8 74 4c be fb e3 02 68 da .....S..g..ll...h..
0070 09 bf 62 .....p.....
Bytes 227-258: Public Key ( wlan_ext_tag_owe_oh_parameter_public_key)

```

Ilustración 50: Wireshark OWE Router (Diffie Hellman)

Tras finalizar satisfactoriamente la asociación del cliente en el dispositivo de interconexión, comienza la creación de la clave de sesión. Para esto se realiza el proceso *4way-handshake* desde el dispositivo de interconexión al cliente para generar dicha clave. En esta captura se puede observar la segunda parte de la negociación, donde el cliente envía al dispositivo el Nonce (256 bits) y el control de integridad MIC (128 bits).

```

> Frame 14: 161 bytes on wire (1288 bits), 161 bytes captured (1288 bits)
> IEEE 802.11 QoS Data, Flags: .....T
> Logical-Link Control
  > 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 123
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 2]
    > Key Information: 0x0100
    Key Length: 0
    Replay Counter: 1
    WPA Key Nonce: 3ca6cb14c53286fc51643788e93d4711e7834b3c077ffe... Nonce
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 054d04ef86ebf122ac3b6fd164f54ed7 Integridad - 128 bits
    WPA Key Data Length: 28
    > WPA Key Data: 301a010000fac040100000fac040100000fac12c000000...
    > Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 26
      RSN Version: 1
      > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
        Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
        Group Cipher Suite type: AES (CCM) (4)
        Pairwise Cipher Suite Count: 1
      > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
        > Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
          Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
          Pairwise Cipher Suite type: AES (CCM) (4)
          Auth Key Management (AKM) Suite Count: 1
          > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) Opportunistic Wireless Encryption
            > RSN Capabilities: 0x00c0
  > Bytes 51-82: WPA Key Nonce (wlan_rsn_eapol_key_desc_nonce)
    0030 00 00 01 3c a6 cb 14 c5 32 86 fc 51 64 37 88 e5 ...c.... 2..qd7..
    0040 3d 47 11 7e 78 34 b3 c0 77 ff ef f2 32 7b 65 c9 ...G~x4...w~+2(e... 256 bits
  > Bytes 51-82: WPA Key Nonce (wlan_rsn_eapol_key_desc_nonce)

```

Ilustración 51: Wireshark OWE Integridad

En la siguiente captura se comprueba como la conexión sobre OWE envía los datos cifrados. La información que se transmite entre el router del operador (Internet) y cliente con OWE, y a la inversa, se encuentra encriptada con la clave de sesión. Además, se observan los parámetros con las direcciones MAC del dispositivo de interconexión y del cliente.

```

> Frame 1429: 1519 bytes on wire (12152 bits), 1519 bytes captured (12152 bits)
> IEEE 802.11 QoS Data, Flags: .p....F.
  Type/Subtype: QoS Data (0x0020)
  > Frame Control Field: 0x8842
    > 000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: liteont_e1:6e:1b (30:d1:6b:e1:6e:1b) Cliente
    Transmitter address: Synology_a4:e7:57 (00:11:32:a4:e7:57) Dispositivo de interconexión
    Destination address: liteont_e1:6e:1b (30:d1:6b:e1:6e:1b) Cliente
    Source address: AskeyCom_0d:30:1d (78:29:ed:0d:30:1d) Router operador (Internet)
    BSS Id: Synology_a4:e7:57 (00:11:32:a4:e7:57)
    STA address: liteont_e1:6e:1b (30:d1:6b:e1:6e:1b)
    ... .. 0000 = Fragment number: 0
    0010 0001 1101 ... = Sequence number: 541
  > QoS Control: 0x0000
  > CCNP parameters
    CCNP Ext. Initialization Vector: 0x000000001128
    Key Index: 0
  > Data (1485 bytes)
    Data: f316bae798d721cd740958a320f958def6dedf391524ed23...
    [Length: 1485]
    0020 00 00 f3 16 ba e7 98 d7 21 cd 74 09 58 a3 20 f9 ...c.... 1.t.X...
    0030 30 0e f6 06 df 39 15 24 e1 23 77 fd 33 74 9e fa ...95~m~3b~
    0040 3e 38 0b 02 4b 9d f9 71 d0 32 2d f9 ee c0 74 e8 ...K~q ~2...t
    0050 45 b9 2b 37 f9 77 2d 7b ab b4 44 ae 9c 30 30 0c ...+~w{ ~D~00
    0060 e9 18 7c 01 a4 58 37 13 16 9f f0 e5 4c a2 65 b5 ...X7...L.e
    0070 cb b5 5b c9 e2 4f 55 ff 98 2f c3 79 7f 6f 83 1d ...00~ /~y~o~
    0080 30 63 e8 48 b1 d0 25 11 2c 8d 37 9c e7 93 44 ce ...H~%~ /~7~D
    0090 44 c5 7a a2 d5 5b 4a 3f f7 0f 74 65 81 8f 2c 5d ...z~[? ~te...
    00a0 5a ad 57 8c 74 8e a2 4d 3d ad 47 04 1a ba d8 2b ...t~H ~G...+
    00b0 88 c1 4f 23 cb e5 82 39 80 5c 5d 42 1e f7 e7 fa ...8~9 ~\|B...
    00c0 50 ff 3a 27 5d ed c2 c3 04 7e f0 95 e1 80 88 fd ...:~)~...~...
    00d0 d1 76 d9 45 23 e7 f8 2d 33 97 4f 18 60 32 4c 4c ...v~#... 3~0~2LL
    00e0 28 50 31 c3 90 ab 4c 4a d4 47 58 20 ba 7e 28 df ...P1~L] ~GX ~(-
    00f0 54 a8 6d 39 d2 87 2f 80 80 14 04 23 72 35 77 47 ...T~m9~/~ /~#~#SwG
    0100 d2 98 d2 20 f2 84 86 f7 6d 91 8c d4 b1 b9 7c 53 ...~... m...~S
    0110 3d 95 82 89 58 de c2 65 40 a5 45 db 69 bd f3 ef ...~X~e @~E~i...
  > Datos cifrados

```

Ilustración 52: Wireshark OWE Datos cifrados

Conclusión

La conclusión de este caso práctico es que el nivel de seguridad OWE debe ser utilizado para entornos de sitios públicos en sustitución de los sistemas abiertos. Esta solución aporta encriptación sobre la información y protege a los usuarios de estos establecimientos de que su información pueda ser accesible.

7.3. Entornos corporativos

La infraestructura de red de estos entornos corporativos es compleja y se deben realizar las acciones necesarias para controlar los accesos a la red. Estas acciones de seguridad se utilizarán para controlar los accesos de una gran cantidad de usuarios y proteger la información que se transmite por la red.

En este modelo se aconseja utilizar como mecanismo de seguridad WPA3-Enterprise, ya que aporta un alto nivel de confidencialidad y mayor control en los accesos. Asimismo, este nuevo protocolo permite, aunque de modo opcional, un tamaño de clave de 192 bits. El modelo con este tamaño de clave (192 bits) es recomendable para entornos que requieran un alto nivel de seguridad. Esta práctica se realizará con el tamaño de clave de 128 bits.

Por otro lado, en este tipo de infraestructuras es recomendable utilizar controladoras Wi-Fi, ya que permite de una forma centralizada gestionar y controlar los distintos puntos de acceso. Además, es conveniente implantar sistemas NAC para controlar los equipos que se conectan a la red.

En la red de laboratorio se mostrará la configuración para una red con nivel de seguridad WPA3-Enterprise. En este caso se utilizará EAP-TTLS (*Tunneled TLS*) sobre MSCHAPv2 para la autenticación de los usuarios. Se ha optado por este modelo, ya que garantiza que la información de autenticación se envíe de forma segura y tiene menos carga de trabajo para la gestión de los clientes. Para implantar este sistema se hace necesario instalar un servidor de autenticación y un servidor para la gestión de usuarios. En la red laboratorio se han configurado los siguientes sistemas:

- Portátil Asus F552L
 - Sistema Operativo: Ubuntu Desktop 18.04
 - VirtualBox 6.0.8
 - Servidor de autenticación
 - Sistema operativo: Ubuntu Server 18.04
 - FreeRADIUS 3.0.19
 - Servidor para la gestión de usuarios.
 - Sistema operativo: Windows Server 2016 Datacenter Evaluation (Licencia para 180 días)

El plano de red de esta configuración es el siguiente:

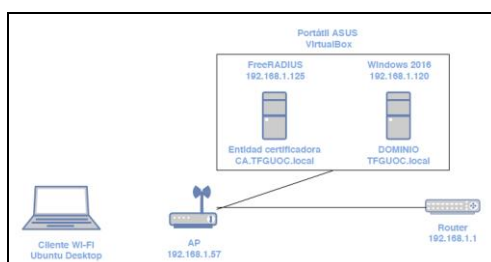


Ilustración 53: Configuración red WPA3-Enterprise

En los siguientes puntos se especificará el procedimiento para realizar esta configuración en la red laboratorio.

- Configuración del dispositivo de interconexión (Synology MR2200ac)

En este equipo se configura el nivel de seguridad WPA3-Enterprise y se oculta el SSID. En el servidor de autenticación se configura la dirección IP del equipo FreeRADIUS (192.168.1.125), y la clave de secreto compartido.

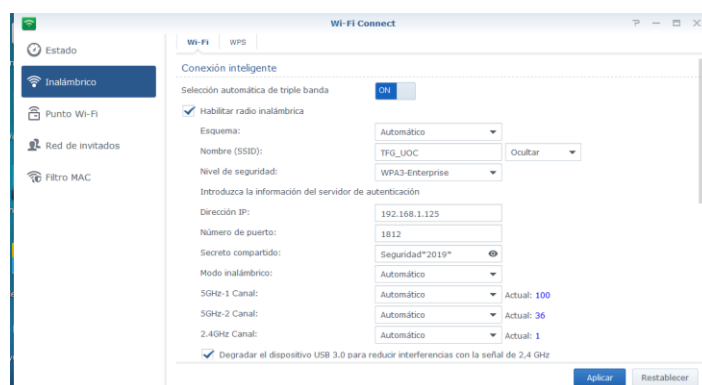


Ilustración 54: Configuración WPA3-Enterprise

Seleccionamos la opción de “Aislamiento de AP” para que los dispositivos inalámbricos no se pueden conectar entre ellos. Asimismo, se observa que la opción de “Compatibilidad con PMF” queda establecida como activada obligatoria. También, se recomienda habilitar una franja horaria para activar la red Wi-Fi en los periodos que se debe utilizar.

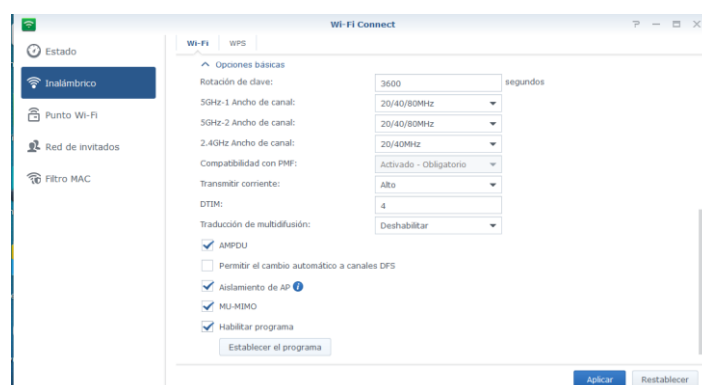


Ilustración 55: Configuración adicional WPA3-Enterprise

- Configuración del servidor autenticación y entidad certificación

Tras la instalación de FreeRADIUS (Anexo 4), se lleva a cabo la configuración de los distintos parámetros para la integración con el Directorio Activo y la configuración de EAP-TTLS (MSCHAPv2). Para ello se debe tener instalado el demonio *Winbind* (conectividad con entornos Windows) y la aplicación *ntlm_auth* (que se utiliza conjuntamente con *winbind* para evaluar las respuestas de NTLM)

Primero, se modifican los ficheros `/etc/samba/smb.conf`, `/etc/krb5.conf` y `/etc/nsswitch.conf` para la integración con Directorio Activo,

`/etc/samba/smb.conf`

```
##### Global Settings #####
[global]
## Browsing/Identification ##
# Change this to the workgroup/NT-domain name your Samba server will part of
workgroup = TFGUOC
password server = 192.168.1.125
realm = TFGUOC.local
security = ads
winbind use default domain = no
load printers = no
printcap name = /dev/null

##### Share Definitions #####
# Un-comment the following (and tweak the other settings below to suit)
# to enable the default home directory shares. This will share each
# user's home directory as \\server\username
[homes]
comment = Home Directories
browseable = no
writable = yes
```

Ilustración 56: Configuración FreeRadius smb.conf

`/etc/krb5.conf`

```
[libdefaults]
    default_realm = TFGUOC.local
    dns_lookup_realm = false
    dns_lookup_kdc = true
[logging]
    default = FILE:/var/log/krb5libs.log
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kmadmin.log
[realms]
    TFGUOC.local = {
        kdc = 192.168.1.120
        admin_server = 192.168.1.120
        default_domain = tfguoc.local
    }
[domain_realm]
    .tfguoc.local = TFGUOC.local
    tfguoc = TFGUOC.local
[kdc]
    profile = /etc/krb5kdc/kdc.conf
[appdefaults]
    pam = {
        debug = false
        ticket_lifetime = 36000
        renew_lifetime = 36000
        forwardable = true
        krb4_convert = false
```

Ilustración 57: Configuración FreeRadius krb5.conf

`/etc/nsswitch.conf`

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the 'glibc-doc-reference' and 'info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         files winbind
group:          files winbind
shadow:        files winbind

protocols:     files winbind
services:      files winbind

netgroup:      files winbind
automount:     files winbind
```

Ilustración 58: Configuración FreeRadius nsswitch.conf

Posteriormente, se realizan los cambios en los ficheros de FreeRADIUS con el objetivo de configurar la conexión entre el dispositivo de interconexión y el servidor, y la configuración de EAP-TTLS (MSCHAPv2). Se modifica el fichero `/usr/local/etc/raddb/radius.conf` para definir los parámetros de seguridad con el dispositivo de interconexión,

```
# You can now specify one secret for a network of clients.
# When a client request comes in, the BEST match is chosen.
# i.e. The entry from the smallest possible network.
client 192.168.1.57
    ipaddr = 192.168.1.57
    secret = Seguridad*2019*
```

Ilustración 59: Configuración FreeRadius radius.conf

Para activar la autenticación sobre el Directorio Activo, se modifica el fichero `/usr/local/etc/raddb/mods-available/mschap`

```
with_ntdomain_hack = yes
ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --username=%{%{Stripped-User-Name}:-%{%{User-Name}:-None}} --challenge=%{%{mschap:Challenge}:-00} --nt-response=%{%{mschap:NT-Response}:-00} --domain=%{%{mschap:NT-Domain}"
```

Ilustración 60: Configuración FreeRadius mschap

Finalmente, se modifica el fichero `/usr/local/etc/raddb/mods-available/eap` para configurar la validación sobre EAP-TTLS. Se modifica de `default_eap_type = md5` a `default_eap_type = peap` (permite el uso de MSCHAPv2).

En lo relacionado con la entidad de certificación, desde el mismo FreeRADIUS se puede crear una entidad de certificación (CA) para la generación de los certificados que se usarán en las negociaciones entre los distintos dispositivos. Para generar esta CA, se deben modificar los siguientes parámetros del fichero ubicado en `/usr/local/etc/raddb/certs/ca.cnf`,

```
[ req ]
prompt                = no
distinguished_name    = certificate_authority
default_bits          = 2048
input_password        = Seguridad*2019*
output_password       = Seguridad*2019*
x509_extensions       = v3_ca

[certificate_authority]
countryName           = ES
stateOrProvinceName  = SC DE TENERIFE
localityName          = TEJINA
organizationName     = UOC
emailAddress          = rbaldeon@uoc.edu
commonName            = ca.tfguoc.local
```

Ilustración 61: Configuración CA ca.cnf

Además, se deben modificar los siguientes parámetros del fichero ubicado en `/usr/local/etc/raddb/certs/server.cnf`,

```
[ req ]
prompt                = no
distinguished_name    = server
default_bits          = 2048
input_password        = Seguridad*2019*
output_password       = Seguridad*2019*

[server]
countryName           = ES
stateOrProvinceName  = SC DE TENERIFE
localityName          = TEJINA
organizationName     = UOC
emailAddress          = rbaldeon@uoc.edu
commonName            = ca.tfguoc.local
```

Ilustración 62: Configuración CA server.cnf

Finalmente, ejecutar el comando `make` para la generación de los certificados CA.

- Configuración del servidor Windows Server 2016

Tras la instalación del servidor Windows Server 2016, se configura el rol de Servicios de dominio de Active Directory para crear un dominio. Finalmente, se crea un usuario, denominado “usuario”, para realizar las pruebas de autenticación.

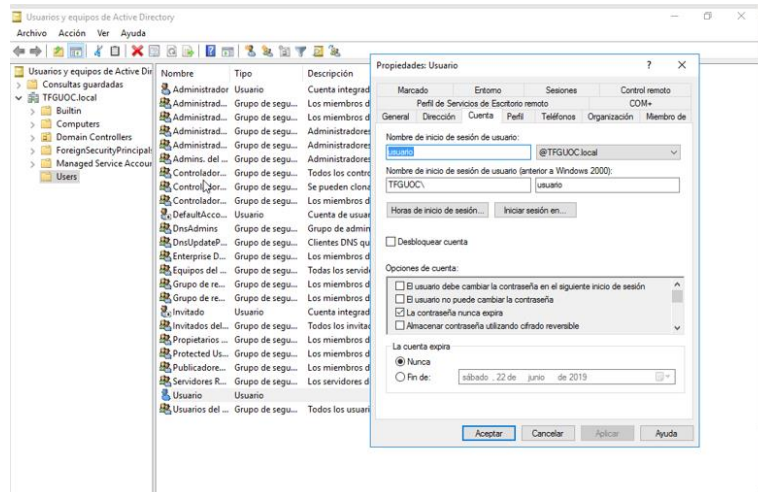


Ilustración 63: Alta usuario Directorio activo

- Configuración del equipo cliente

La aplicación (*wpa_supplicant*), utilizada en las conexiones sobre WPA3, está en modo de desarrollo, por lo que para poder utilizar la opción de WPA3-Enterprise se necesita modificar el fichero de configuración (*.config*) de la aplicación, añadir las líneas relativas a este protocolo y realizar una nueva compilación del *software*.

```
# Enable some testing options code? Not intended for production code.
CONFIG_TESTING_OPTIONS=y
CONFIG_SUITEB=y 128 bits
CONFIG_SUITEB192=y 192 bits
```

Ilustración 64: Configuración wpa_supplicant WPA3-Enterprise

El fichero de configuración (EAP-TFG_UOC.conf) con los parámetros necesarios que utiliza el *wpa_supplicant* para la conexión. Este fichero se alojará en el directorio */etc/wpa_supplicant/*

```
Update_config=1
ctrl_interface=/run/wpa_supplicant
ctrl_interface_group=adm
network={
    ssid="TFG_UOC"
    key_mgmt=WPA-EAP-SUITE-B
    eap=TTLS
    scan_ssid=1
    ieee80211w=2
    group_mgmt=BIP-GMAC-256
    ca_cert="/home/cesar/ca.pem"
    identity="usuario"
    password="Seguridad*2019*"
    phase2="auth=MSCHAPV2"
}
```

Ilustración 65: Fichero cliente WPA3-Enterprise

Las tres primeras líneas del fichero se añaden para que desde la utilidad *wpa_cli* se pueda controlar el componente *wpa_supplicant* y actualizar este fichero de configuración. En la configuración de la red de conexión, se encuentran los parámetros,

- Ssid: Nombre de la red Wi-Fi
- Key_mgmt: Con valor WPA-EAP-SUITE-B, define el protocolo de seguridad sobre WPA3-Enterprise.
- EAP: Se utiliza el protocolo EAP-TTLS
- scan_ssid: Con valor 1, permite la asociación a dispositivos con ssid ocultos (no broadcast).
- leee80211w: Con valor 2, activa el uso de PMF de forma obligatoria.
- Group_mgmt: Cifrado para PMF, en este caso BIP-GMAC-256
- Ca_cert: Ruta del certificado del servidor Radius.
- Identity: El nombre del usuario
- Password: La contraseña del usuario
- Phase2: Se configura la autenticación sobre MSCHAPv2

Hay que indicar que los intentos de conexión sobre este protocolo no fueron satisfactorios debido al nivel de encriptación requerido. Como se puede observar en la siguiente captura de pantalla, el WPA3-Enterprise utiliza el protocolo GMCP-256 como sistema de cifrado,

```
> Tag: Vendor Specific: Qualcomm Inc.
  > Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 26
    RSN Version: 1
    > Group Cipher Suite: 00:0f:ac (Ieee 802.11) GCMP (256)
    Pairwise Cipher Suite Count: 1
    > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) GCMP (256)
    Auth Key Management (AKM) Suite Count: 1
    > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA (SHA384-SuiteB)
    > RSN Capabilities: 0x00cc
    PMKID Count: 0
    PMKID List
    > Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (GMAC-256)
  > Tag: Vendor Specific: Qualcomm Inc.
```

Ilustración 66: Wireshark WPA3-Enterprise

Mientras que la tarjeta de red wi-fi de nuestro equipo no soporta este protocolo (se adjunta captura de pantalla de los protocolos de cifrado que soporta la interfaz de red Qualcomm Atheros QCA9377)

```
Supported Ciphers:
* WEP40 (00-0f-ac:1)
* WEP104 (00-0f-ac:5)
* TKIP (00-0f-ac:2)
* CCMP-128 (00-0f-ac:4)
* CMAC (00-0f-ac:6)
* CMAC-256 (00-0f-ac:13)
* GMAC-128 (00-0f-ac:11)
* GMAC-256 (00-0f-ac:12)
```

Ilustración 67: Cifrados soportados tarjeta Wi-Fi

Por otro lado, hay que indicar que esta configuración está verificada sobre WPA2-Enterprise, utilizando los mismos dispositivos y el siguiente fichero de configuración para el cliente.

```
root@TFG_UOC_2019: /etc/wpa_supplicant x
update_config=1
ctrl_interface=/run/wpa_supplicant
ctrl_interface_group=adm
network={
    ssid="TFG_UOC"
    key_mgmt=WPA-EAP-SHA256
    eap=TTLS
    scan_ssid=1
    pairwise=CCMP
    group=CCMP
    ieee80211w=2
    ca_cert="/home/cesar/ca.pem"
    identity="usuario"
    password="Seguridad*2019*"
    phase2="auth=MSCHAPV2"
}
```

Ilustración 68: Fichero cliente WPA2-Enterprise

Se añade la salida del comando `wpa_cli`, donde se verifica la correcta conexión sobre este protocolo de seguridad.

```
> status
bssid=00:11:32:a4:e7:58
freq=5500
ssid=TFG_UOC
id=0
mode=station
pairwise_cipher=CCMP
group_cipher=CCMP
key_mgmt=WPA2-EAP-SHA256
pmf=2
mgmt_group_cipher=BIP
wpa_state=COMPLETED
ip_address=192.168.1.42
p2p_device_address=30:d1:6b:e1:6e:1b
address=30:d1:6b:e1:6e:1b
Supplicant PAE state=AUTHENTICATED
suppPortStatus=Authorized
EAP state=SUCCESS
selectedMethod=21 (EAP-TTLS)
eap_tls_version=TLSv1.2
EAP_TLS_cipher=ECDHE-RSA-AES256-GCM-SHA384
tls_session_reused=0
EAP-TLSv0 Phase2 method=MSCHAPV2
eap_session_id=15319015c0b58e1d7d48f01775c4ffe04710f9c8c38c4fe6b7cdca3abd90e0084a86196dfdc60d4b
3d3d7cd93e6cec14387cb15e8840a5e3618b98e0282d999bd1
uuid=66b077f9-74f0-54c8-930e-773592ab3203
ieee80211ac=1
>
```

Ilustración 69: `wpa_cli` WPA2-Enterprise

Conclusión

La conclusión a este estudio es que en entornos corporativos se recomienda el uso del nivel de seguridad WPA3-Enterprise. Este protocolo se puede configurar sobre tamaños de clave de 128 bits (SUITEB) o 192 bits (SUITEB192). Asimismo, estos sistemas utilizan unos protocolos de encriptación muy robustos para lograr una infraestructura segura. En caso de implementarlo, se tendría que realizar un estudio de los equipos clientes y los sistemas para garantizar la correcta integración con este protocolo.

En lo relacionado con el servicio de autenticación de los usuarios, se plantea la utilización de EAP-TTLS (MSCHAPv2), ya que es un sistema que requiere poca administración (no necesita la instalación de certificados en los clientes) y logra un alto nivel de seguridad. Además, este método es compatible con los principales sistemas operativos clientes Windows, Linux, Android e IOS.

Por otro lado, una implantación con el protocolo WPA2-Enterprise utilizando PMF, de forma obligatoria, y con un método de autenticación EAP-TTLS (MSCHAPv2) consigue un nivel óptimo de seguridad. Además, esta solución está actualmente aprobada como uno de los sistemas seguros para redes Wi-Fi en organizaciones.

7.4. Perfiles de seguridad

En este caso práctico, se ha utilizado un *Firewall UTM OpenSource* denominado *Endian Firewall 3.3.0 (Community Edition)* para la configuración de los perfiles de seguridad. En esta aplicación gratuita no se podrán aplicar todas las aplicaciones de seguridad descritas en este documento. Este sistema se ha instalado (Anexo 5) en el VirtualBox del portátil Asus.

La topología de este sistema es la siguiente:

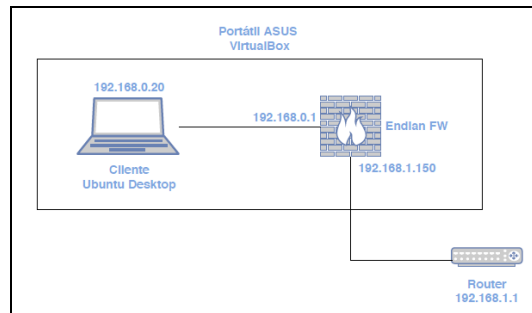


Ilustración 70: Topología Firewall UTM

La pantalla inicial del *Firewall UTM* es la siguiente, en ella podemos observar los distintos menús que presenta.

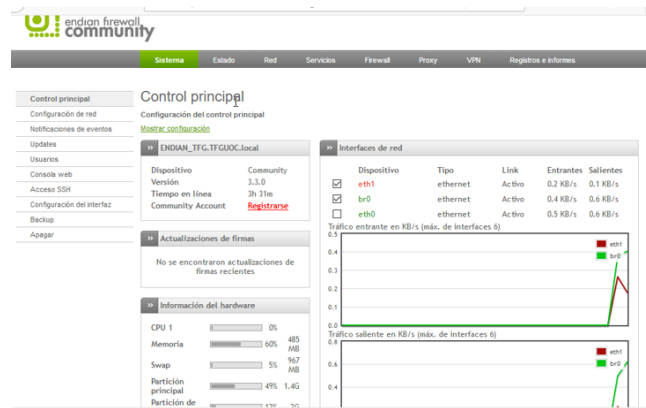


Ilustración 71: Página principal Firewall UTM

En la opción de *Firewall*, se definen las reglas de acceso. En esta configuración se permite desde la red Verde (Interna) hacia la red Roja (Internet) los puertos más comunes para navegar.

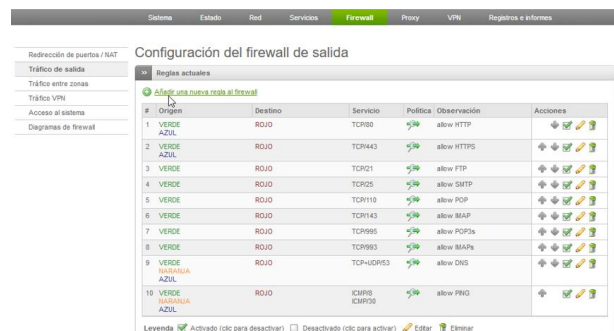


Ilustración 72: Reglas Firewall

En el menú Servicios, se activará el sistema IPS y se definirá la actualización diaria para las reglas de IPS.

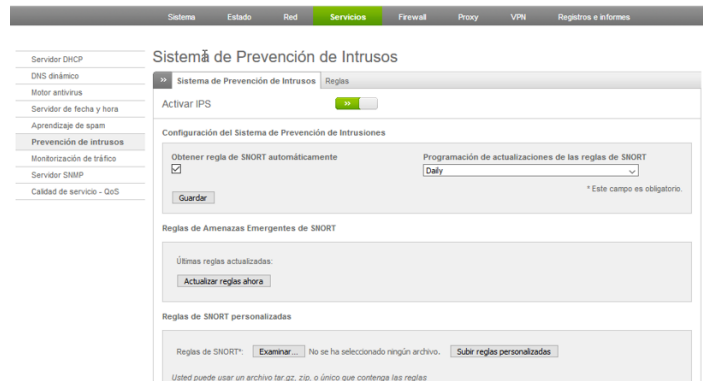


Ilustración 73: Activación IPS

Para el control de la navegación, se habilitará el Proxy HTTP sobre el puerto 8080. Además, en la configuración se configurará en modo transparente. Asimismo, se activará todas las opciones de registro para disponer de la información de la navegación de los usuarios.

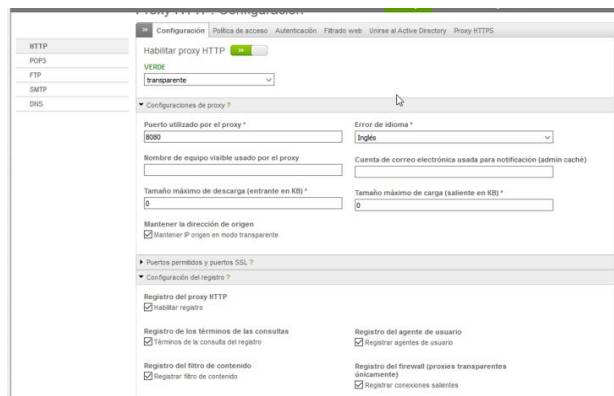


Ilustración 74: Habilitar proxy HTTP

En la siguiente acción, se configura el servicio de Web Filtering con el objetivo de filtrar el acceso a páginas web según su contenido. Para ello, se selecciona Filtrado web, y se añade un nuevo perfil. En este perfil, se marcan en rojo los contenidos que se bloquean los accesos.

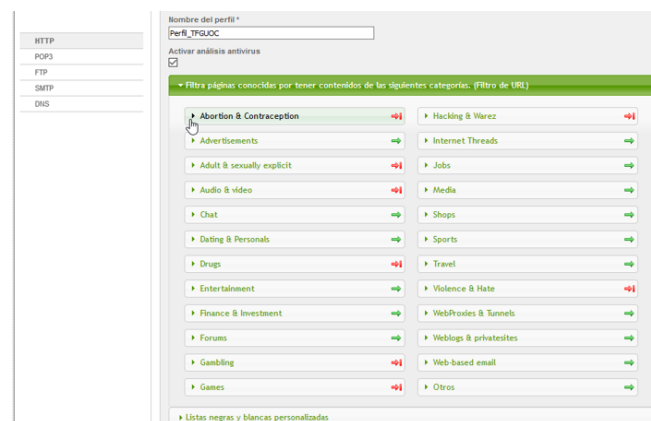


Ilustración 75: Perfiles Web Filtering

Además, en esta opción se puede definir el tiempo para las actualizaciones de las páginas web. En este caso, se configura para que se actualice de forma diaria.

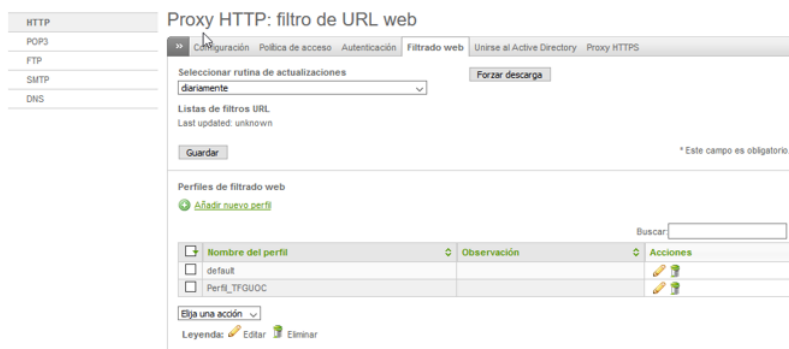


Ilustración 76: Habilitar Web Filtering

Para activar este perfil, se accede al menú de Políticas de acceso y se añade una nueva política de acceso con la siguiente información.

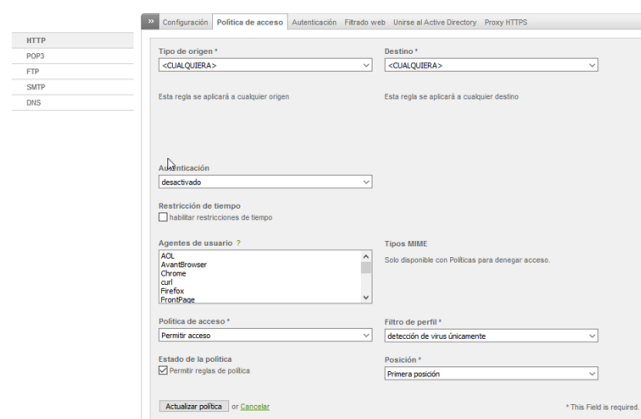


Ilustración 77: Políticas de acceso

La configuración de las políticas finaliza con la creada para filtrado web y otra para la detección de virus (por defecto).

#	Política	Origen	Destino	Grupo de autenticación/usuario	Cuándo	Agente de usuario	Actions
1	filter using 'perfil_tfguoc'	CUALQUIERA	CUALQUIERA	no necesario	Siempre	CUALQUIERA	
2	filtro de virus	CUALQUIERA	CUALQUIERA	no necesario	Siempre	CUALQUIERA	

Ilustración 78: Políticas de acceso habilitadas

Se configurará el SSL-Inspection a través de la opción Proxy HTTPS. En dicha opción, se realizará una descryptación y escaneo del contenido para detectar cualquier contenido malicioso. Tras activar esta opción, se deberá descargar el certificado del Endian (Download) y añadirlo a los certificados de las entidades de confianza de los navegadores de los clientes. Asimismo, se pueden dar de alta dominios donde no se necesita realizar la inspección SSL, como por ejemplo en las entidades bancarias por privacidad.

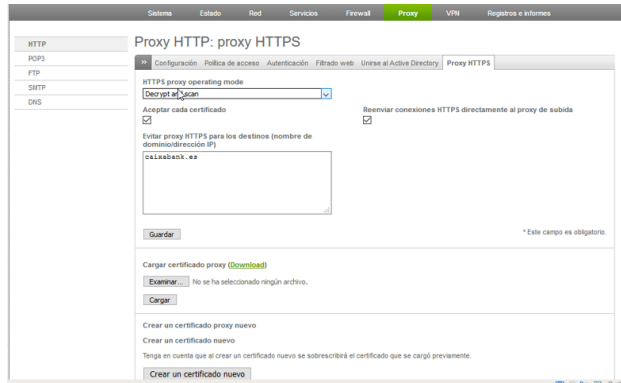


Ilustración 79: Habilitar Proxy HTTPS (SSL Inspection)

Tras finalizar la configuración del Firewall UTM, se procederá a realizar la configuración del certificado en el navegador del cliente.

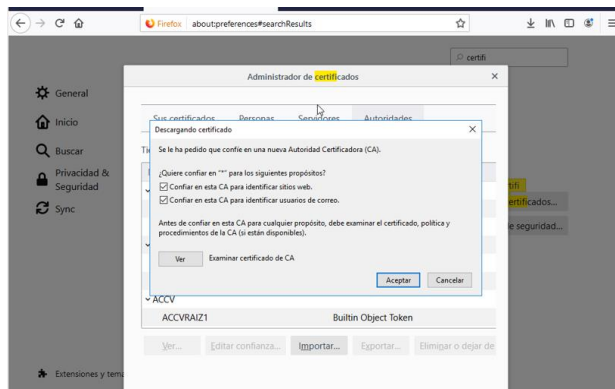


Ilustración 80: Cliente certificado CA (SSL Inspection)

Para verificar el correcto funcionamiento de este sistema, primero se intentará realizar una descarga del virus "eicar" (virus de prueba). En este caso, se deniega el acceso por la detección del virus.



Ilustración 81: Detección virus

En la siguiente demostración, se intentará acceder a la categoría bloqueada Audio & Video. La página web que se pretende acceder es www.youtube.com, y será denegado el acceso por pertenecer a una categoría bloqueada.

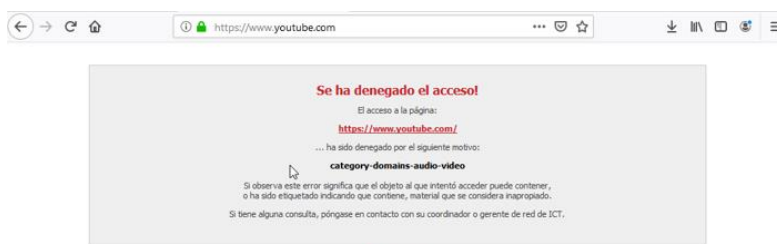


Ilustración 82: Detección contenido bloqueado

Finalmente, se muestra el menú de registro con el objetivo de monitorizar los accesos y los avisos que se producen en la navegación o en los sistemas IPS.

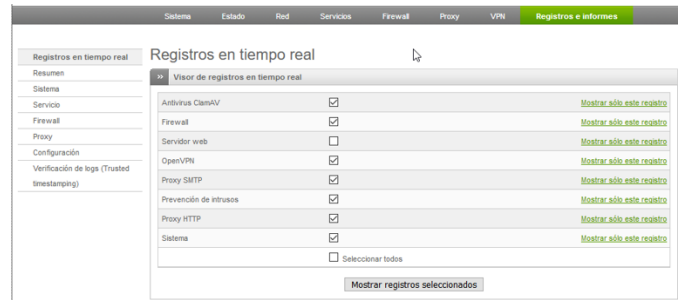


Ilustración 83: Registro de accesos

En estos registros, se puede acceder a la información que se produce durante la navegación. En el caso del antivirus, se puede observar como queda registrado el intento de acceso a la web.

Antiviru...	2019-05-24 18:46:14	clamd (4292) Portable Executable support enabled.
Antiviru...	2019-05-24 18:46:14	clamd (4292) ELF support enabled.
Antiviru...	2019-05-24 18:46:14	clamd (4292) Mail files support enabled.
Antiviru...	2019-05-24 18:46:14	clamd (4292) Mail: RFC1341 handling enabled.
Antiviru...	2019-05-24 18:46:14	clamd (4292) OLE2 support enabled.
Antiviru...	2019-05-24 18:46:14	clamd (4292) PDF support enabled.
Antiviru...	2019-05-24 18:46:14	clamd (4292) SZIP support enabled.
Antiviru...	2019-05-24 18:46:14	clamd (4292) HTML support enabled.
Antiviru...	2019-05-24 18:46:14	clamd (4292) XMLElement support enabled.
Antiviru...	2019-05-24 18:46:14	clamd (4292) HWFP support enabled.
Antiviru...	2019-05-24 18:46:14	clamd (4292) Heuristic: precedence enabled.
Antiviru...	2019-05-24 18:46:14	clamd (4292) Self checking every 600 seconds.
Antiviru...	2019-05-24 18:56:47	clamd (4292) SelfCheck: Database status OK.
Antiviru...	2019-05-24 19:06:47	clamd (4292) SelfCheck: Database status OK.
Antiviru...	2019-05-24 19:14:08	clamd (4292) /var/tmp/CI_TMP_krV03F: Eicar-Test-Signature UNOFFICIAL(44d89812fea8a8f36de02e1278ab-b02f68): FOUND
Antiviru...	2019-05-24 19:17:26	clamd (4292) SelfCheck: Database status OK.
Antiviru...	2019-05-24 19:37:10	clamd (4292) SelfCheck: Database status OK.
Antiviru...	2019-05-24 19:45:31	freshclam (6646) ClamAV update process started at Fri May 24 19:45:31 2019
Antiviru...	2019-05-24 19:45:31	freshclam (6646) Your ClamAV installation is OUTDATED!
Antiviru...	2019-05-24 19:45:31	freshclam (6646) Local version: 0.99.4 Recommended version: 0.101.2
Antiviru...	2019-05-24 19:45:31	freshclam (6646) DON'T PANIC! Read http://www.clamav.net/documents/upgrading-clamav
Antiviru...	2019-05-24 19:46:23	freshclam (6646) Downloading main.cvd [100%]
Antiviru...	2019-05-24 19:47:17	freshclam (6646) Database load killed by signal 9
Antiviru...	2019-05-24 19:47:17	freshclam (6646) Failed to load new database
Antiviru...	2019-05-24 19:47:48	clamd (4292) SelfCheck: Database status OK.

Ilustración 84: Registro virus detectado

Conclusión

Como conclusión a esta herramienta, se indica que los *Firewall UTM* son sistemas muy recomendados para entornos corporativos. Desde un único punto de la red, se puede controlar los accesos a Internet, filtrar el contenido y proteger la infraestructura de la entrada de aplicaciones maliciosas. Además, estos sistemas permiten realizar un registro de los distintos accesos a las páginas web (bloqueadas y permitidas), por lo que se podrían detectar clientes con posibles virus o usuarios que navegan a contenido inapropiado para la organización.

8. Conclusiones

Las conclusiones de este trabajo se focalizan en la implantación de una arquitectura Wi-Fi con seguridad. Según se ha desarrollado este trabajo, no se puede asegurar que las redes inalámbricas sean totalmente seguras. Sin ir más lejos, tras la redacción de los nuevos mecanismos de seguridad (WPA3) se produce la noticia del *DragonBlood* (descrito en el apartado 3.3.1), por lo que las garantías de este nuevo sistema quedan en duda. Sin embargo, los fabricantes informan que la aplicación de los parches correspondientes resuelve estas vulnerabilidades, y que se deben realizar las acciones necesarias para mitigar o reducir los posibles problemas de seguridad de cualquier tipo de red.

En principio se ha conseguido realizar la mayoría de los objetivos marcados y dentro de los plazos previstos. No obstante, hay que indicar que las pruebas en el laboratorio sobre WPA3-Enterprise no se pudieron realizar satisfactoriamente debido a la falta de recursos en el portátil y por ser un sistema que está en fase de certificación de productos por los fabricantes. Aunque, toda la infraestructura que se instaló fue verificada sobre WPA2-Enterprise, que cuenta con características similares en niveles de seguridad.

Las pruebas de laboratorio sobre el sistema *Opensource (Endian)*, para implantar los perfiles de seguridad, han sido bastante útiles. Con esta aplicación gratuita pude demostrar la importancia de contar con unos de estos equipos en la infraestructura de entornos corporativos. Esta herramienta cuenta con las principales aplicaciones de seguridad, y su interfaz de gestión es muy sencilla y cómoda de usar.

La metodología fue íntegramente seguida para conseguir los objetivos definidos en el plan de trabajo. Aunque, se produjo un inconveniente en la realización de la parte documental de los perfiles de seguridad que me obligaron a modificar los plazos previstos. En los siguientes periodos se volvió al itinerario marcado para continuar con el desarrollo del proyecto. En relación a las pruebas de laboratorio de los mecanismos de seguridad, se podría haber ampliado los periodos para poder buscar una solución factible al protocolo WPA3-Enterprise.

Las líneas de trabajo futuras estarían dirigidas en la instalación y configuración de dispositivos donde el protocolo WPA3 se encuentra integrado de forma nativa. También, se plantea como trabajo de futuro la configuración de sistemas NAC y 802.1X en las infraestructuras de las redes inalámbricas. Este tipo de medidas adicionales a la seguridad permiten una mayor robustez de la seguridad, ya que se controla a nivel de puerto del conmutador y se comprueba si el cliente cuenta con los requisitos para conectarse a la red.

9. Glosario

AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
BIP-GMAC	Broadcast/Multicast Integrity Protocol Galois Message Authentication Code
BSS	Basic Service Set
C&C	Command & Control
CA	Certification Authority
CCMP	Counter-Mode / CBC-MAC Protocol
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DoS	Denial of Service
DPI	Deep Packet Inspection
EAP	Extensible Authentication Protocol
EAP-FAST	EAP Flexible Authentication via Secure Tunneling
EAP-LEAP	EAP-Lightweight Extensible Authentication Protocol
EAP-PEAP	EAP-Protected EAP
EAP-PWD	EAP-Password
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ESS	Extended Service Set
FTPS	FTP Secure
GCMP	Galois/Counter Mode Protocol
HMAC	Hashed Message Authentication Mode
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBSS	Independent Basic Service Set
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IMAPS	Internet Message Access Protocol Secure
IoT	Internet de las cosas
IP	Internet Protocol
IPS	Intrusion Prevention System
KRACK	Key Reinstallation Attacks
LOPD-GDD	Ley de Protección de Datos y garantía de los derechos digitales
LPI	Ley de Propiedad Intelectual
MAC	Media Access Control
MIC	Michael Integrity Check
MIMO	Multiple Input Multiple Output
MitM	Man in the Middle
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MU-MIMO	Multiple User-Multiple Input Multiple Output

NAC	Network Access Control
NFC	Near Field Communication
NGFW	Next Generation Firewall
NTLM	New Technology LAN Manager
OFDMA	Orthogonal Frequency-Division Multiple Access
OWE	Opportunistic Wireless Encryption
P2P	Peer-to-Peer
PAKE	Password Authenticated Key Exchange
PBC	Push Botton Configuration
PFS	Perfect <i>Forward Secrecy</i>
PIN	Personal Identification Number
PMF	Protected Management Frames
PMK	Pairwise Master Key
POP3S	Post Office Protocol Secure version 3
PSK	Pre-Shared Keys
PTK	Pairwise Transient Key
QAM	Quadrature Amplitude Modulation
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
RGDP	Reglamento general de protección de datos
RSNE	Robust Security Network Element
SAE	Simultaneous Authentication of Equals
SHA	Secure Hash Algorithm
SMTPS	Simple Mail Transfer Protocol Secure
SSH	Secure SHell
SSID	Service Set IDentifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UTM	Unified Threat Management
VLAN	Virtual Local Area Network
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
Wi-Fi	Wireless Fidelity
WiGig	Wireless Gigabit
WIPS	Wireless Intrusion Prevention System
WPA	Wi-Fi Protect Access
WPS	Wi-Fi Protected Setup

10. Bibliografía

Libros:

- [1] James F. Kurose, Keith W. Ross. **Computer Networking. A Top-Down Approach.** 7ª Edición. Pearson. 2017

Web:


- [2] <https://www.wi-fi.org/> (05/03/2019)
- [3] <https://es.wikipedia.org/wiki/Wifi> (05/03/2019)
- [4] https://es.wikipedia.org/wiki/IEEE_802.11 (05/03/2019)
- [5] <https://es.wikipedia.org/wiki/Radiofrecuencia> (06/03/2019)
- [6] <https://www.teldat.com/blog/es/wpa3-redes-wi-fi-con-seguridad-wpa3-personal-wpa3-enterprise/> (06/03/2019)
- [7] <https://www.teldat.com/blog/es/wpa3-redes-wi-fi-con-seguridad-wpa3-personal-wpa3-enterprise/> (07/03/2019)
- [8] <https://securebox.comodo.com/ssl-sniffing/ssl-inspection/> (15/03/2019)
- [9] https://es.wikipedia.org/wiki/Sistema_de_prevenici%C3%B3n_de_intrusi%C3%B3n_inal%C3%A1brica (15/03/2019)
- [10] https://www.arubanetworks.com/techdocs/Instant_83_WebHelp/Content/Instant_UG/Authentication/802_1X_Authentication.htm (22/03/2019)
- [11] <https://www.endian.com> (27/03/2019)
- [12] <https://www.microsoft.com> (27/03/2019)
- [13] <https://jimswirelessworld.wordpress.com/2018/09/20/aruba-takes-the-lead-with-wpa3/> (17/04/2019)
- [14] <https://papers.mathyvanhoef.com/dragonblood.pdf> (18/04/2019)
- [15] <https://www.intel.es/content/www/es/es/support/articles/000006999/network-and-io/wireless-networking.html> (27/04/2019)
- [16] <https://mikeguy.co.uk/posts/2018/06/understanding-nac-802.1x-and-mab/> (27/04/2019)
- [17] <https://www.watchguard.com/es/wgrd-solutions/security-topics/trusted-wireless-environment> (29/04/2019)

- [18] <https://digitalguardian.com/blog/what-application-control> (03/05/2019)
- [19] <https://www.incibe.es/protege-tu-empresa/blog/dlp-protege-tus-datos-fugas-informacion> (04/05/2019)
- [20] https://es.wikipedia.org/wiki/Software_de_prevenci%C3%B3n_de_p%C3%A9rdida_de_datos (03/05/2019)
- [21] <https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/605938/why-you-should-use-ssl-inspection> (04/05/2019)
- [22] <https://www.fortinet.com/blog/business-and-technology/redefining-next-generation-firewalls.html> (18/05/2019)
- [23] [https://wiki.archlinux.org/index.php/WPA_supplicant_\(Espa%C3%B1ol\)](https://wiki.archlinux.org/index.php/WPA_supplicant_(Espa%C3%B1ol)) (11/05/2019)
- [24] <https://www.draw.io> (26/05/2019)


11. Anexos

Anexo 1

Certificado Wi-Fi Alliance Router Synology MR2200ac



Wi-Fi CERTIFIED™ Interoperability Certificate
This certificate lists the features that have successfully completed Wi-Fi Alliance interoperability testing.
Learn more: www.wi-fi.org/certification/programs



Certification ID: WFA77433**Page 1 of 2**

Date of Last Certification	October 24, 2018
Company	Synology Inc.
Product	Synology Router MR2200ac
Model Number	MR2200ac
Product Identifier(s)	
Category	Routers
Subcategory	Access Point for Home or Small Office (Wireless Router)
Hardware Version	Product: 1.0, Wi-Fi Component: 1.0
Firmware Version	Product: 7025, Wi-Fi Component: 7025
Operating System	Linux, version: 4.4
Frequency Band(s)	2.4 GHz, 5 GHz - Concurrent

Summary of Certifications

CLASSIFICATION	PROGRAM
Connectivity	Wi-Fi CERTIFIED™ a, b, g, n, ac WPA™ – Enterprise, Personal WPA2™ – Enterprise, Personal WPA3™ – Enterprise, Personal Wi-Fi Enhanced Open™
Optimization	WMM®
Access	Wi-Fi Protected Setup™



Security

WPA™ – Enterprise, Personal
 WPA2™ – Enterprise, Personal
 WPA3™ – Enterprise, Personal
 EAP Type(s)
 EAP-TLS
 EAP-TTLS/MSCHAPv2
 PEAPv0/EAP-MSCHAPv2
 PEAPv1/EAP-GTC
 EAP-SIM
 EAP-AKA
 EAP-AKA Prime
 EAP-FAST
 Protected Management Frames
 192-bit Security

Wi-Fi Protected Setup™ (continued)

PIN
 Push-Button (PBC)

Spectrum and Regulatory Features

802.11d

Wi-Fi CERTIFIED™ a

Wi-Fi CERTIFIED™ b

Wi-Fi CERTIFIED™ g

Wi-Fi CERTIFIED™ n

2.4 GHz, 5 GHz - Concurrent
 2 Spatial Streams 2.4 GHz
 2 Spatial Streams 5 GHz
 Short Guard Interval
 TX A-MPDU
 STBC Transmit
 40 MHz operation in 2.4 GHz, with coexistence mechanisms
 40 MHz operation in 5 GHz

Wi-Fi CERTIFIED™ ac

2 Spatial Streams 5 GHz
 Rx MCS 8-9 (256-QAM)
 Tx STBC 2x1
 Rx A-MPDU of A-MSDU
 Tx SU beamformer
 Low Density Parity Check coding
 Tx DL MU-MIMO
 Extended 5 GHz Channel Support

Wi-Fi Enhanced Open™

ECC Group 20

WMM®

Wi-Fi Protected Setup™

2.4 GHz, 5 GHz - Concurrent

Anexo 2

Instalación aplicación wpa_supplicant v2.8

Para la instalación del wpa_supplicant v2.8 se realizarán los siguientes pasos:

1. Descargar la aplicación de la siguiente URL,

wget https://w1.fi/cgiit/hostap/snapshot/hostap_2_8.tar.gz

```
root@cesar-Aspire-A315-53:/home/cesar/Descargas# wget https://w1.fi/cgiit/hostap/snapshot/hostap_2_8.tar.gz
--2019-06-06 19:35:26-- https://w1.fi/cgiit/hostap/snapshot/hostap_2_8.tar.gz
Resolviendo w1.fi (w1.fi)... 212.71.239.96
Conectando con w1.fi (w1.fi)[212.71.239.96]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: no especificado [application/x-gzip]
Guardando como: "hostap_2_8.tar.gz"

hostap_2_8.tar.gz [ <=> ] 4,11M 5,41MB/s en 0,8s
2019-06-06 19:35:28 (5,41 MB/s) - "hostap_2_8.tar.gz" guardado [4310635]
```

2. Descomprimir el fichero con el siguiente comando,

```
tar -xvf hostap_2_8.tar.gz
```

3. Acceder a la carpeta ../hostap_2_8/wpa_supplicant, y crear el fichero .config,

```
cp configure .config
```

4. Editar el fichero .config y modificar los siguientes parámetros.

```
CONFIG_SAE=y
CONFIG_OWE=y
```

5. Instalar las siguientes librerías con el comando *apt-get install <librerías>*

- *pkg-config*
- *libnl-3-dev*
- *git*
- *virtualenv*
- *build-essential*
- *python3-dev*
- *libdbus-glib-1-dev*
- *libgirepository1.0-dev*

6. Compilar el programa mediante el commando,

```
sudo make
```

7. Para finalizar, realizar la instalación

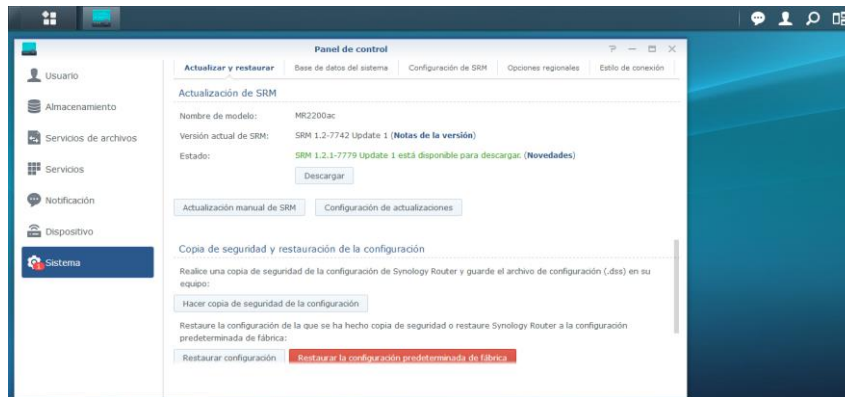
```
sudo make install
```

Anexo 3

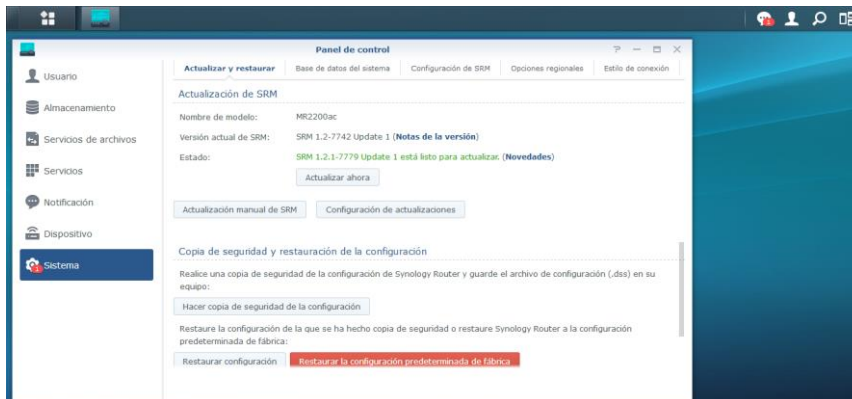
Actualización firmware Router MR220ac

El procedimiento para realizar la actualización de sistema operativo del Router Synology MR2200ac es el siguiente:

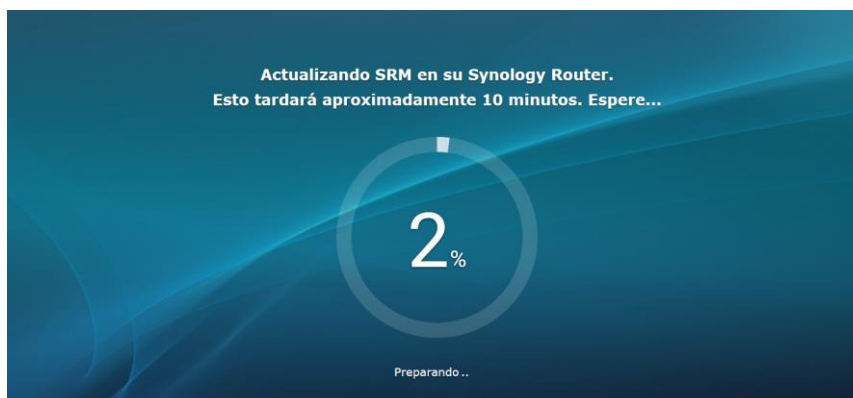
1. Acceder al Panel de Control, y en este menú seleccionar Sistema,



2. Si el equipo está conectado a Internet, informará que tiene una actualización para instalar. Para actualizar el router hacer clic en el botón “Actualizar ahora”,



3. Comenzará el proceso de actualización.

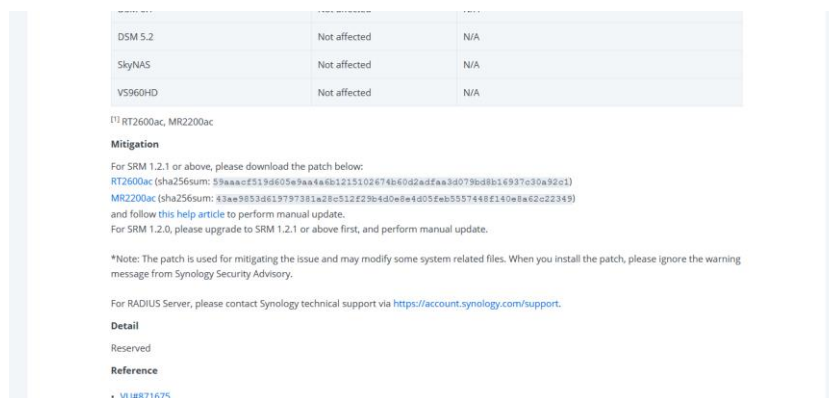


- Tras finalizar la actualización, el equipo está operativo y nos indica que no existen más actualizaciones.

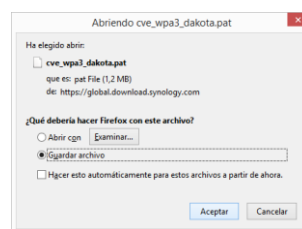


Debido a la vulnerabilidad DragonBlood (descrita en el apartado 3.3.1), el fabricante publicó un parche para mitigar esta incidencia,

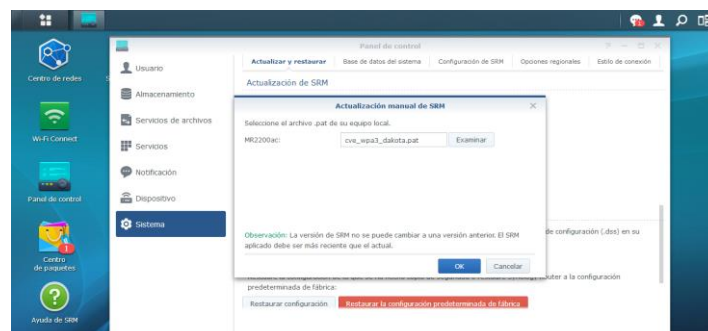
https://www.synology.com/es-es/security/advisory/Synology_SA_19_16



Para instalar dicho parche, se descarga el fichero asociado al router MR2200ac,



Se procedió a ejecutar la actualización manual para mitigar esta vulnerabilidad.



Anexo 4

Instalación FreeRadius v3.0.19

El procedimiento para la instalación del software *FreeRadius* se define a continuación:

1. Descargar el instalador de la siguiente dirección,

<ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-3.0.19.tar.gz>

```
root@radius_tfg:/tmp# wget ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-3.0.19.tar.gz
--2019-05-08 18:13:43-- ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-3.0.19.tar.gz
=> 'freeradius-server-3.0.19.tar.gz'
Resolving ftp.freeradius.org (ftp.freeradius.org)... 62.210.29.29
Connecting to ftp.freeradius.org (ftp.freeradius.org)|62.210.29.29|:21... connected.
Logging in as anonymous ... Logged in!
=> SYST ... done.      => PWD ... done.
=> TYPE I ... done.   => CWD (1) /pub/freeradius ... done.
=> SIZE freeradius-server-3.0.19.tar.gz ... 4886632
=> PASV ... done.     => RETR freeradius-server-3.0.19.tar.gz ... done.
Length: 4886632 (4,7M) (unauthoritative)

freeradius-server-3.0.19 100%[=====] 4,66M 5,40MB/s in 0,9s
2019-05-08 18:13:45 (5,40 MB/s) - 'freeradius-server-3.0.19.tar.gz' saved [4886632]
root@radius_tfg:/tmp#
```

2. Descomprimir el fichero mediante el comando,

```
tar -zxvf freeradius-server-3.0.19.tar.gz
```

3. Acceder a la carpeta */freeradius-server-3.0.19*, y para configurar, compilar e instalar la aplicación se ejecutan los siguientes comandos,

```
./configure
sudo make
sudo make install
```

Para comprobar que se encuentra instalado correctamente, se ejecuta el comando *radiusd -v* para verificar la versión del FreeRadius,

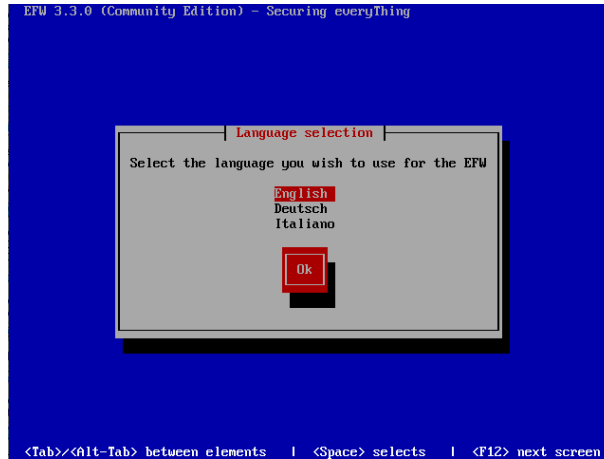
```
cesar@radius_tfg:/etc$ radiusd -v
radiusd: FreeRADIUS Version 3.0.19, for host x86_64-unknown-linux-gnu, built on May  8 2019 at 18:23:00
FreeRADIUS Version 3.0.19
Copyright (C) 1999-2019 The FreeRADIUS server project and contributors
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE
You may redistribute copies of FreeRADIUS under the terms of the GNU General Public License
For more information about these matters, see the file named COPYRIGHT
cesar@radius_tfg:/etc$
```

Anexo 5

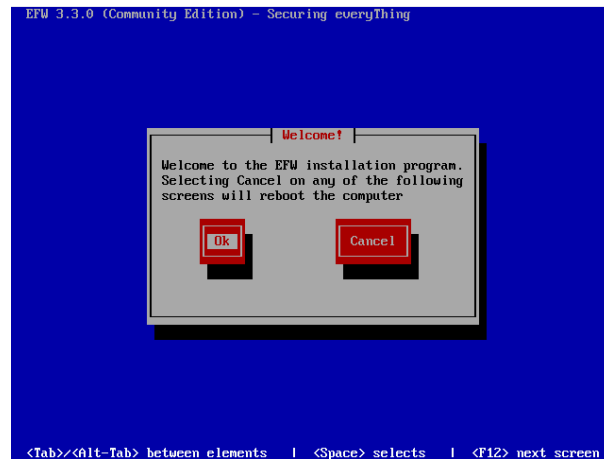
Instalación y configuración Endian v3.3.0

El procedimiento para la instalación del Firewall UTM es el siguiente:

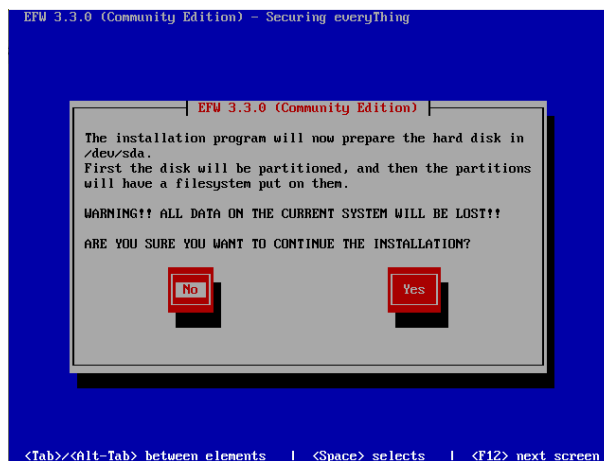
1. Seleccionar el idioma (en este caso, English),



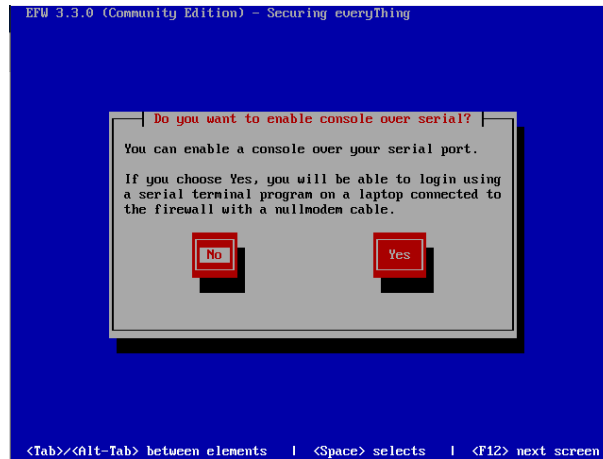
2. Hacer clic en el botón "OK",



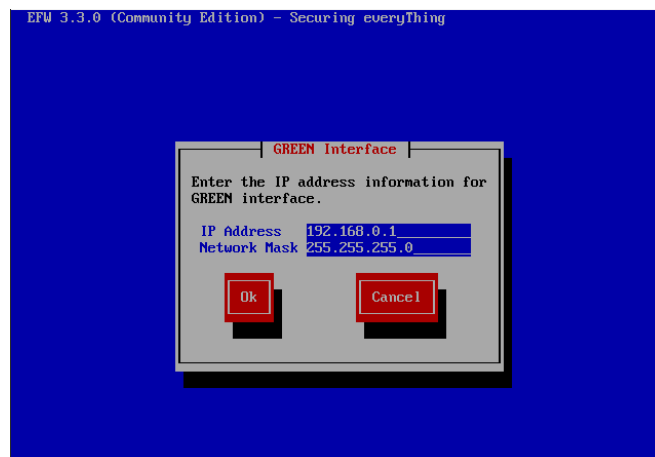
3. Para particionar el disco, hacer clic en el botón "Yes",



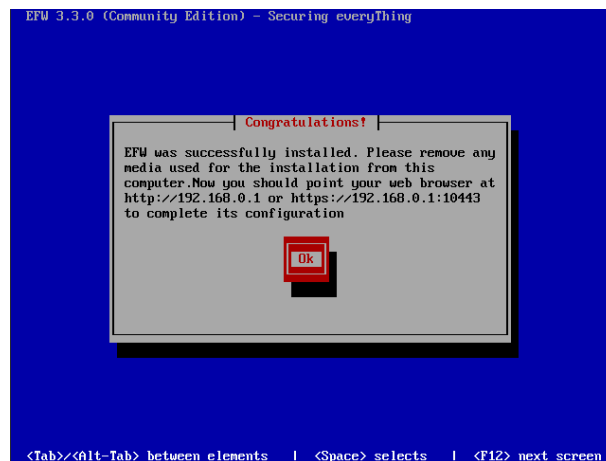
4. Sobre un equipo virtualizado sin puerto serie, seleccionar "No"



5. Asignar dirección IP de gestión,

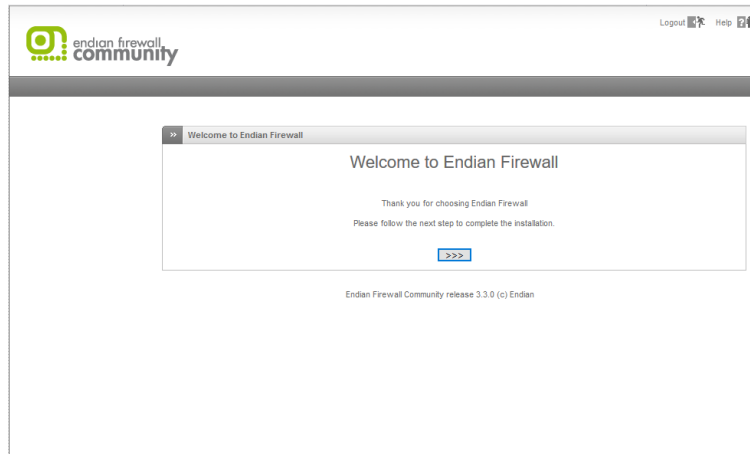


6. Tras finalizar la instalación, el equipo nos informa que para acceder se debe utilizar un navegador e introducir la dirección *https://<dirección IP configurada>:10443*

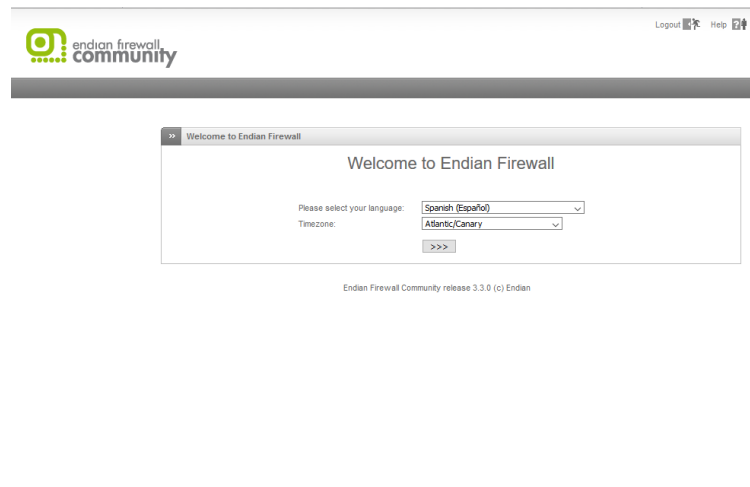


El procedimiento para realizar la configuración del equipo es el siguiente:

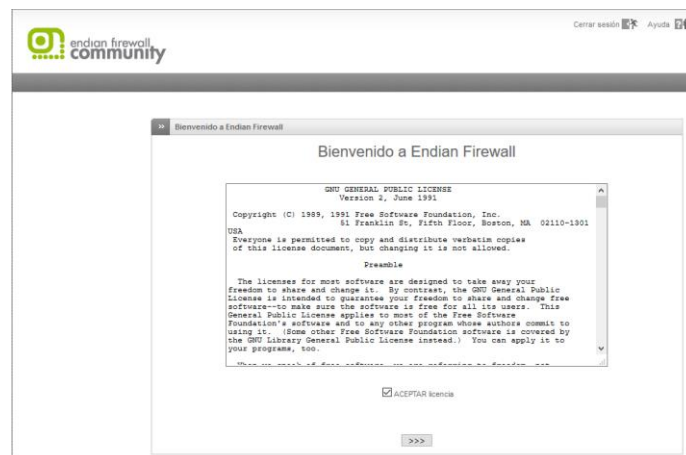
1. Acceder con el navegador a la dirección *https://<dirección IP configurada>:10443*, (en este caso *https://192.168.0.1:10443*)



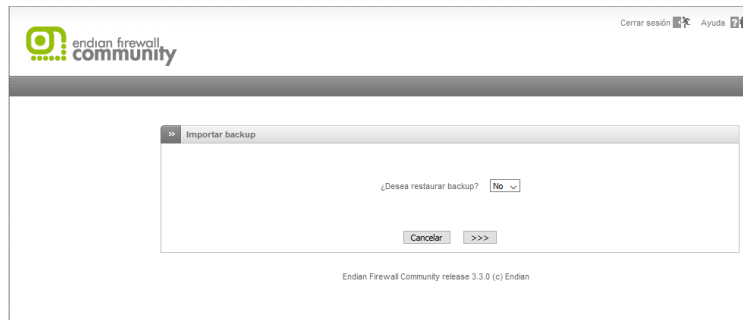
2. Seleccionar el idioma y la zona horaria,



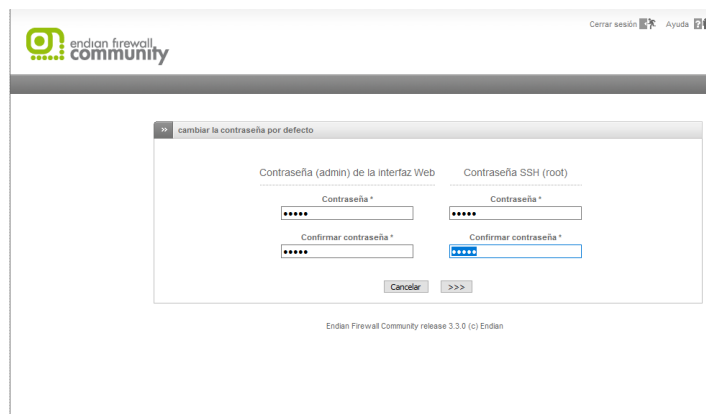
3. Aceptar las condiciones de la licencia,



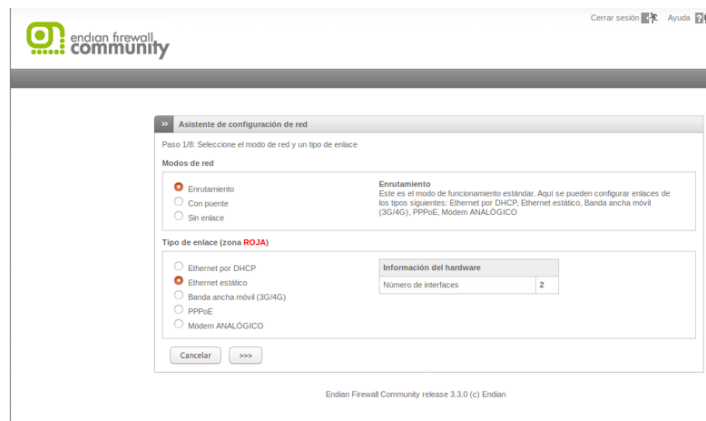
4. Dado que es una nueva instalación y no se dispone de backup, seleccionar “No”,



5. Configurar las contraseñas de admin (para la interfaz web) y para el acceso por SSH,



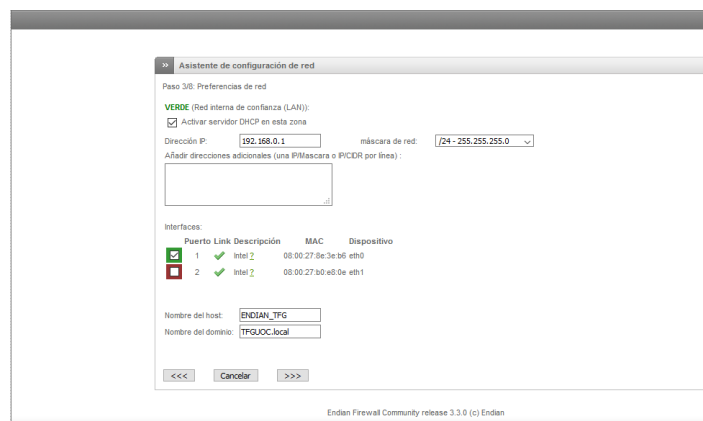
6. Como se va a comportar como un Firewall UTM, seleccionar como modo de red “Enrutamiento” y el tipo de enlace “Ethernet estático”,



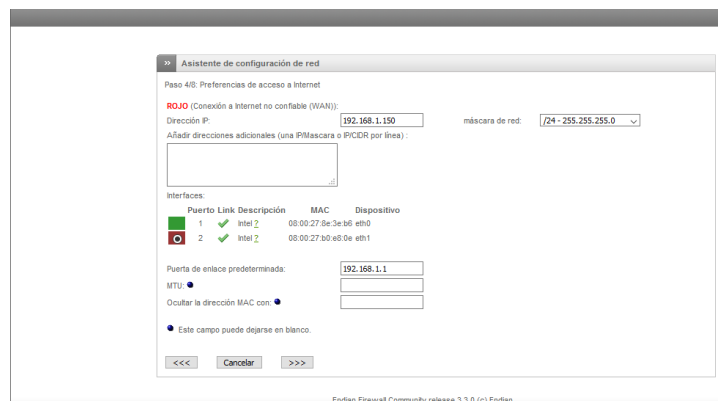
7. En este caso, solo se tienen dos redes (Interna y acceso a Internet), por lo que no se seleccionan más segmentos de red,



8. Se configura la dirección IP del Firewall UTM de la red interna y se activa el servidor DHCP. Además, se añade el nombre del host y el nombre del dominio.



9. Se configura la interfaz con conexión a Internet, y se añade la puerta de enlace (en este caso la dirección IP del router del operador) para el acceso a Internet.



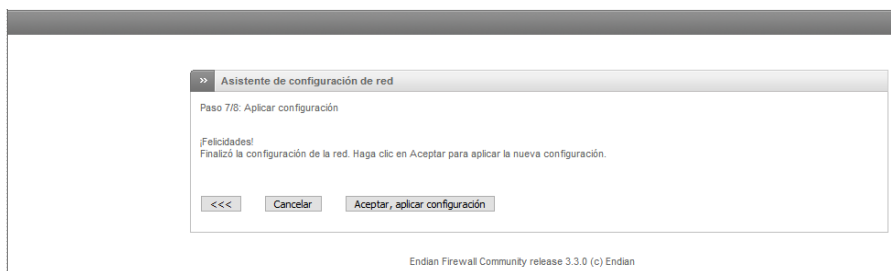
10. Se introducen los servidores DNS (en este caso los servidores DNS que provee el operador).



11. Se añade la dirección de correo electrónico del administrador.



12. Se hace clic en el botón "Aceptar, aplicar configuración" para guardar la configuración realizada.



13. Finalmente, nos indica que ha finalizado con éxito la configuración del equipo.

