Universidad de Cienfuegos “Carlos Rafael Rodríguez”

Facultad de Ingeniería

Carrera de Ingeniería Informática

Título:

“Propuesta de Arquitectura para el Control de Acceso a la red WLAN de la UCF”.

Trabajo de diploma para optar por el título de Ingeniería en Informática

Autor:

José Arturo García Torres

Tutor:

Ing. Alex González Paz

Cienfuegos, Cuba

2014-2015

Declaración de Autoría.

Declaro que yo, José Arturo García Torres soy el único autor de este trabajo y autorizo a la Facultad de Ingenierías de la Universidad de Cienfuegos y al Centro de Estudios de Ingeniería y Sistemas para que hagan el uso que estimen pertinente con este trabajo.

Para que así conste firmo la presente a los _____ días del mes de _____ del _____.

_____

José Arturo García Torres

_____

Ing. Alex González Paz

Pensamiento

Dedicatoria

A mi familia

Resumen

Actualmente, la Universidad de Cienfuegos (UCF), ofrece el servicio de acceso a intranet e Internet, no sólo mediante una infraestructura de red cableada, sino también de forma inalámbrica. Sin embargo, el control para el acceso a dicho recurso y los registros que se tienen sobre su uso, no son los deseados para tareas de administración de red. La seguridad en el uso de las redes es un elemento básico, esta juega un rol determinante en el caso de las redes inalámbricas locales (WLAN), debido a que el medio de transmisión en estas es el aire, por lo que los mecanismos de autenticación y cifrado son indispensables para garantizar la autenticidad y la confidencialidad de la información que se transmite en ellas. En el presente trabajo se propone una arquitectura para el control de acceso de la red inalámbrica local de la UCF, la implementación de un servidor RADIUS (Remote Authentication Dial-In User Service) capaz de permitir conectividad a una amplia gama de dispositivos que soporten el estándar IEEE 802.11n y a la vez que sea capaz de garantizar un nivel de seguridad adecuado, siempre en dependencia del tipo de usuario y dispositivo que se conecte. La arquitectura comprende varios métodos de control de acceso como los propios utilizados en las redes WLAN, WPA y WPA2. Para la implementación de esta arquitectura se propone una variante que utiliza software libre.

Palabras claves:

Arquitectura, WLAN, Servidor RADIUS, Software Libre

Abstract

Currently, the University of Cienfuegos (UCF), offers the service of access to intranet and Internet, not only through a wired network infrastructure, but also wirelessly. However, controlling for access to this resource and records held about its use are not desired for network management tasks. The safe use of networks is a staple, this plays a more decisive role in the case of wireless local area networks (WLAN), because the means of transmission in these is the air, so that the mechanisms Authentication and encryption are essential to ensure the authenticity and confidentiality of the information transmitted on them. In this paper an architecture for access control of the local wireless network UCF, implementing a server Remote Authentication Dial-In User Service (RADIUS) capable of allowing connectivity to a wide range of devices that support the proposed IEEE 802.11n while capable of ensuring an adequate level of safety, always depending on the type of user and device connected. The architecture comprises various methods of access control as own used in WLAN, WPA and WPA2 networks. To implement this architecture uses a variant proposed free software.

Keywords:

Architecture, Wireless Network, RADIUS Server, Free Software

Índice de contenido

Índice de tablas

Índice de figuras

Introducción

Una de las innovaciones en redes de datos que actualmente está teniendo auge en todo el mundo, son las tecnologías de redes inalámbricas, principalmente las Wireless Local Area Network (WLAN) que aunque no aportan mejora de ancho de banda como la Fibra Óptica, sí lo son por el medio de transmisión que utilizan, que es el aire, característica que le proporciona una serie de ventajas sobre las redes cableadas en diversas situaciones como: fácil acceso, la flexibilidad, rapidez de despliegue, costos de instalación, movilidad, entre otras.

Pero junto a las ventajas que genera la transmisión aérea, las WLAN crean un problema grave, el de la seguridad. No se debe pasar por alto las múltiples vulnerabilidades de estas redes, por lo que la seguridad será siempre uno de los puntos importantes a considerar cuando se implementa una WLAN.

En la actualidad, la seguridad de las redes de empresas e instituciones juega un rol fundamental, sobre todo en las WLAN, su medio de propagación da la oportunidad para que un intruso acceda a la red sin tener autorización, o para interceptar la comunicación comprometiendo información sensible; por lo que los mecanismos de autenticación y cifrado son imprescindibles para garantizar la autenticidad y confidencialidad de la información que se transmite en ellas. Estas redes se han convertido en un elemento clave para el aumento de la productividad de las instituciones.[1]
Controlar quién accede a un recurso y la forma cómo se usa, son necesidades evidentes hoy en día para cualquier institución, no sólo por la importancia de la información que circula en la red, sino para velar por la prestación de un buen servicio de Internet e intranet.

En la mayoría de los escenarios, las redes WLAN se interconectan con otras tecnologías de redes, dando como resultado sistemas heterogéneos de gran complejidad. En un contexto como el anterior es conveniente poder utilizar los mecanismos de seguridad, tales como los mecanismos de autenticación y cifrado, de forma integrada. Esta integración permite a los usuarios acceder a este tipo de redes con comodidad y garantizar un nivel adecuado de seguridad. El despliegue de redes inalámbricas locales en aquellas instituciones que ya posean redes cableadas no tiene un impacto significativo

sobre la infraestructura de seguridad, puesto que los mecanismos de seguridad de las WLAN se pueden integrar sin problemas a los mecanismos propios de las redes Local Area Network (LAN).[2]

Los mecanismos de seguridad que se pueden aplicar en las redes WLAN son diversos y estos actúan en las diferentes capas del modelo Open System Interconection (OSI). Desde que surgieron estas redes se desarrollaron mecanismos específicamente para garantizar la seguridad de estas: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WAP), Institute of Electrical and Electronics Engineers (IEEE), 802.11i y WPA versión 2 (WPA2), aunque se pueden utilizar mecanismos como las Virtual Point Network (VPN) que se aplican a otros tipos de redes.[3]

Los Access Point (AP) sin la configuración correcta y adecuada no solo pueden dar problemas de conexión, sino también vulnerabilidades en la red, lo que permite que agentes externos ingresen a esta, logrando ver, modificar e incluso eliminar archivos. Por este motivo, es importante no descuidar la seguridad de los datos corporativos. Frecuentemente se invierte en alarmas, seguros, vigilancia, pero se escatima en gastos a la hora de proteger los datos.[4] Las Tecnologías de la Información y la Comunicación (TIC) se han convertido, desde su llegada a los escenarios nacionales, en un elemento indispensable para establecer las líneas de desarrollo de la sociedad cubana. Pero al igual que en otras esferas también ha sido afectada por la aplicación de las injustas medidas, donde se incluyen las restricciones impuestas al acceso en Cuba a Internet.[5]

Las leyes estadounidenses prohíben exportar o reexportar a determinados países, entre los que figura Cuba, productos de Software de empresas norteamericanas. Por este motivo, Cuba se ve obligada también a comprar las licencias de Software, sus actualizaciones y la transferencia de tecnología a través de terceros países, haciendo costoso y difícil el trabajo. Además muchas de las aplicaciones y herramientas importantes todavía están basadas en Software Propietario.[6]

Cuba potencia desde el 2005 la migración al Software Libre en aras de alcanzar la soberanía tecnológica y la seguridad del país. Existen múltiples herramientas de Software Libre para la seguridad de redes, imprescindibles a tener en cuenta en las redes cubanas. Al utilizarlas se atiende a la necesidad del país de migrar a dichas tecnologías y proteger la información de las empresas cubanas.[7]

En Cuba desde hace algunos años se ha ido insertando progresivamente el uso de la tecnología inalámbrica basada en los estándares de la IEEE 802.11, teniendo en cuenta las facilidades de su instalación en industrias, centros de trabajos, tiendas recaudadoras de divisa, bancos y universidades.[5]

La Universidad de Cienfuegos (UCF) ha sido partícipe de este desarrollo. Esta cuenta con un total de 14 AP disponibles, lo cual no es una alta cantidad con respecto a las dimensiones de la institución. Esta situación se une a la actual carencia de antenas para estos dispositivos. Por lo anteriormente planteado se decide seguir el criterio de priorizar las áreas de docencia y densidad de usuarios (número de usuarios por edificación) a la hora de identificar las zonas de cobertura. Se priorizan la biblioteca universitaria, los docentes, el rectorado, el comedor, la cafetería, el hotel universitario (“Hotelito”), y los albergues del personal extranjero [8]. La UCF cuenta con un gran número de usuarios (personas vinculadas a la universidad y visitantes autorizados), los cuales tienen acceso a las aplicaciones web disponibles en el centro; por lo que el uso seguro de la red es de vital importancia. Para ello, en años anteriores, se ha trabajado en este tema, con el fin de brindar servicios de seguridad en la red WLAN.

En la UCF, se logró implementar una arquitectura de control de acceso que tiene como principal medida el Control de Acceso al Medio (MAC), la asignación de Internet Protocol (IP) y la asignación de nombre de usuario y contraseña a cada uno de los usuarios. Sin embargo aunque el filtrado por MAC es un método extendido por todo el mundo por su facilidad de configuración; se basa en realizar dicho control mediante la comprobación de la dirección MAC de nivel 2 o nivel de trama. Este sistema de autenticación tiene varios problemas. El primero es que cada vez que un usuario es adicionado o eliminado y los usuarios no son fijos o hay usuarios itinerantes, hay que dar de alta y de baja direcciones con la siguiente carga de gestión y el consiguiente peligro de dejar alguna entrada a la lista “olvidada”, estas modificaciones se realizan de forma manual lo que requiere de tiempo y acceso a diferentes sistemas, complicando la administración del servicio y afectando la prontitud en la respuesta a los usuarios finales que tienen que moverse hasta el nodo central para realizar su solicitud, por lo que la carga administrativa de la WLAN aumenta. Otra de las atenuantes es lo fácil que resulta cambiar la dirección MAC de un dispositivo, lo que hace sencillo sustituirla por una válida, y por tanto, que

este método de autenticación resulte vulnerable. El método de ataque consiste en capturar y analizar el tráfico que pasa por la WLAN y guardar direcciones MAC válidas, para que en el momento que alguna de ellas quede libre, sustituir ésta por la dirección MAC del dispositivo cliente. Analizando esta situación se deduce que este método de autenticación resulta ineficiente. A lo cual se suma el aumento significativo de la cantidad de usuarios con dispositivos móviles que soportan el estándar Wi-Fi, pero que no pueden conectarse debido a que sus equipos no soportan WPA/WPA2.

Por todo lo anterior era necesario cambiar la arquitectura de control de acceso por una que no fuera dependiente de la configuración de los puntos de acceso, a su vez la nueva arquitectura debía basarse en la utilización de Software Libre, debido a las múltiples ventajas que este nos ofrece y permitir la conectividad Wi-Fi a todos aquellos equipos que soporten el protocolo IEEE 802.11n.

Ante esta situación se logra identificar como ***problema de investigación*** a resolver la no existencia de un apropiado control de acceso a la red WLAN de la UCF.

Por lo que se plantea como ***idea a defender*** la utilización de una arquitectura para el control de acceso a la red WLAN de la UCF mediante la utilización de software libre permitirá, mejorar el control de acceso a la red.

Por lo antes descrito se define como ***objeto de estudio***: Redes WLAN

Como ***campo de acción*** se tiene: el Control de Acceso de los usuarios a las Redes WLAN.

Con el fin de suplir dichas necesidades en la red inalámbrica de la universidad, se define como ***objetivo general***:

Proponer una arquitectura para el control de acceso a la red WLAN de la UCF mediante la utilización de herramientas de Software Libre.

De este objetivo se derivan los siguientes ***objetivos específicos***:

I. Seleccionar los mecanismos para el control de acceso a la red WLAN de la UCF.
II. Diseñar la arquitectura para el control de acceso de la red WLAN de la UCF empleando herramientas de Software Libre.
III. Evaluar la arquitectura propuesta a partir de pruebas de laboratorio.

Para lograr esta investigación se desarrollarán las siguientes ***tareas***:

- El estudio del estado del arte relacionado con los mecanismos de control de acceso a la red WLAN.
- Análisis de las herramientas basadas en software libre existentes que permiten el control de acceso a las redes WLAN.
- Selección de las herramientas basadas en software libre que permiten la conexión segura de dispositivos inalámbricos a la red WLAN de la UCF.
- Diseño de los escenarios de prueba para la validación de la arquitectura propuesta.

El ***aporte práctico*** de este trabajo radica en que la Universidad de Cienfuegos contará con el diseño de una arquitectura para el control de acceso a la red WLAN de la UCF basado en herramientas de software libre.

El informe se estructuró en: introducción, tres capítulos, conclusiones, recomendaciones, referencias bibliográficas y anexos.

Para ello en el ***capítulo 1*** se hace un estudio de los estándares y tendencias actuales así como las tecnologías comunes para la implementación de mecanismos de control de acceso a redes locales inalámbricas.

En el ***capítulo 2*** se propone una arquitectura para el control de acceso a la red inalámbrica local de la UCF.

Por último en el ***capítulo 3*** se dedica a la implementación de la arquitectura propuesta, se evalúa y valida la misma mediante pruebas de laboratorio.

Capítulo 1: Redes Inalámbricas.

1.1 Introducción al Capítulo

Para dar inicio a los temas relacionados con las redes WLAN es fundamental conocer los principios generales en los que se basan, su funcionamiento, familiarizarse con los términos que se manejan, conocer sus componentes físicos, su relación e integración con las redes tradicionales.

Los principios básicos asociados a la tecnología inalámbrica se pueden encontrar en los documentos y patentes del ingeniero eléctrico Nikola Tesla; así como en su exposición sobre la historia de la tecnología inalámbrica y la radio.

Actualmente las redes inalámbricas de área local están teniendo un gran crecimiento en cuanto a su desarrollo y aceptación. El propósito principal de éstas es dar acceso y conectividad a las tradicionales redes cableadas como lo son las LAN (Local Area Network), WAN (Wide Area Network), MAN (Metropolitan Area Network).

Existen redes inalámbricas WLAN, estas más que una sustitución de las LAN convencionales, son una extensión de las mismas que permiten el intercambio de información entre los distintos medios, donde la naturaleza de la conexión sin cable es transparente al cliente.[9]

Se podría considerar que el objetivo fundamental de las redes WLAN es el de proporcionar las facilidades no disponibles en los sistemas cableados y formar una red total donde coexistan los dos tipos de sistemas. Las redes inalámbricas son una alternativa para hacer llegar una red tradicional a lugares donde el cableado no lo permite. En general las WLAN se utilizan como complemento de las redes fijas.[2]

1.2 Relación de las WLAN y las tecnologías de redes LAN tradicionales.

El organismo regulador IEEE (Institute of Electronics and Electrical Engineer) publicó el estándar 802.11 (802 hace referencia al grupo de documentos que describen las características de las LAN) dedicado a redes LAN ***inalámbricas.*** Este estándar es una serie de especificaciones para el establecimiento de tecnologías de redes de área local

y redes de área metropolitanas basadas en el modelo OSI (*Open Systems Interconnection*), norma que fue ratificada en 1990.[9]

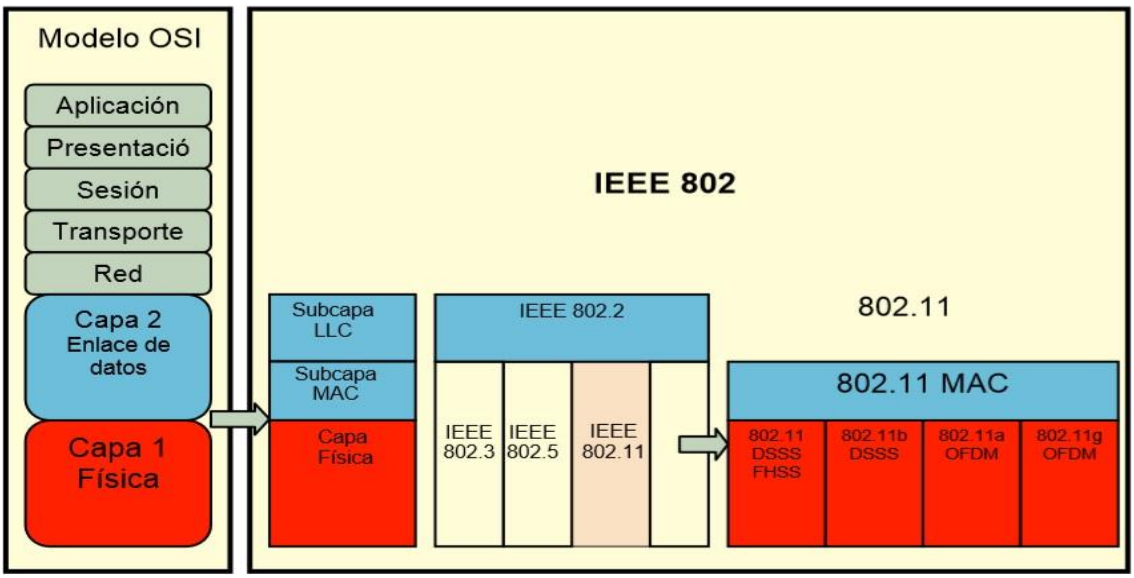

Figura 1. Comparación del estándar 802.11 con respecto al modelo OSI.

El modelo OSI describe la forma de cómo la información en una computadora es transferida a una aplicación en otro equipo. Organiza el proceso de comunicación en siete capas independientes (Física, Enlace, Red, Transporte, Sesión, Presentación y Aplicación), (ver la figura 1). La mayoría de las redes públicas y privadas de comunicaciones utilizan el modelo OSI como modelo de referencia.[1]

Las tecnologías de redes LAN IEEE 802 definen únicamente los temas relacionados con las dos primeras capas del modelo OSI:[9]

- ***Capa de Enlace.***

La IEEE 802 divide a la capa de enlace en dos subcapas: la subcapa LLC (Logical Link Control) y la subcapa MAC (Medium Access Control). Como se observa en la figura 1, la subcapa LLC es definida por el estándar 802.2 y es común a toda la familia de redes 802, tanto para las redes tradicionales (cableadas) como para las WLAN (802.11) el trabajo de esta subcapa es ocultar las diferencias entre las variantes 802 con la finalidad de que sean imperceptibles para la capa de red, en cambio para el subnivel MAC cambia ya que define las técnicas de acceso, es decir, cómo cada terminal puede hacer uso del medio de comunicación común.

- ***Capa Física.***

El objetivo principal de esta capa es transmitir bits por un canal de comunicación, en el caso de las WLAN, el canal de comunicación es el espectro radioeléctrico y la capa física define las técnicas de transmisión y modulación de la señal.

1.3 Estándares más importantes de la familia 802.11.

En 1997 la IEEE integró un nuevo miembro a la familia 802: el 802.11, que se ocupa de definir las especificaciones para las redes inalámbricas de área local WLAN; para ello utiliza tecnología de radiofrecuencia que están normadas bajo el estándar 802.11 de la IEEE y se encuentran situadas entre las tecnologías inalámbricas de mediano alcance (ver la figura 2).[3]

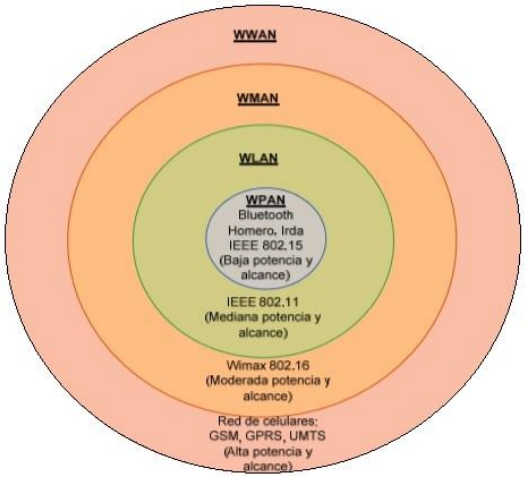

Figura 2. Estándares de redes inalámbricas.[1]

Las especificaciones base del estándar 802.11 definen una capa MAC y dos capas físicas basadas en el uso de radiofrecuencia en la banda de 2.4 GHz. Ambas se diferencian en el método de transmisión de radio utilizado. Una emplea el sistema FHSS (Frequency Hopping Spread Spectrum) y la otra, el sistema DSSS (Direct Sequence Spread Spectrum), después surgió la técnica de transmisión OFDM (Orthogonal Frequency Division Multiplexing).[10]

Los dos estándares 802.11 originales tenían las desventajas de operar a velocidades bajas (1 y 2 Mbps), además los equipos tenían costos altos. Posteriormente surgieron nuevas capas físicas que mejoraron la velocidad de transmisión y empezaron a salir los primeros productos aceptados por el mercado. Poco después dicho estándar fue ampliado, a través de extensiones al estándar original, incluyendo el 802.11a y el

802.11b. A continuación se mencionan algunos de los diferentes estándares para redes WLAN:[11]

- **IEEE 802.11:** estándar de WLAN original. Soporta de 1 Mbps a 2 Mbps.
- **IEEE 802.11a:** aprobado en 1999. Opera en la banda de 5 GHz y utiliza 52 OFDM (Orthogonal Frequency-Division Multiplexing) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. Tiene 12 canales sin solapa, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede inter-operar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.
- **IEEE 802.11b:** velocidad máxima de transmisión de 11 Mbps y utiliza el mismo método de acceso definido en el estándar original CSMA/CA. El estándar funciona en la banda de 2,4 GHz. En la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5,9 Mbits sobre TCP (Protocolo de Control de Transmisión) y 7,1 Mbit/s sobre UDP.
- **IEEE 802.11e:** aprobado en 2005, permite inter-operar entre entornos públicos, de negocios y usuarios residenciales. Puede considerarse como uno de los primeros estándares inalámbricos que permite trabajar en entornos domésticos y empresariales con garantías de Calidad de Servicio (QoS).[12]
- **IEEE 802.11f:** es una recomendación para proveedores de puntos de acceso que permiten que los productos sean compatibles. Utiliza el protocolo IAPP (Inter Access Point Protocol) que le permite a un usuario itinerante cambiarse claramente de un AP a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red.
- **IEEE 802.11g:** surgió en el año 2003 y es la evolución de 802.11b. Utiliza la banda de 2,4 Ghz pero opera a una velocidad teórica máxima de 54 Mbit/s. Es compatible con el estándar b y utiliza las mismas frecuencias.
- **IEEE 802.11i:** está dirigido a batir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Íntegra–Seguras– Temporales), y AES (Estándar de Cifrado Avanzado). Se implementa en WPA2.

En junio de 2007 el IEEE publicó una nueva versión del estándar 802.11 en el que se incorporan las modificaciones aprobadas desde la versión de 1999. Además de las 802.11a, 11b, 11e, 11g y 11i mencionadas anteriormente, 802.11 del 2007 incluye las siguientes: **802.11d** (2001) sobre operación de **802.11a/b** en diferentes dominios regulatorios, **802.11h** (2003) sobre mecanismos de selección de canal de radio y control de potencia y **802.11j** (2004) sobre operación de 4,9 y 5 GHz.[13]

El documento **802.11f** sobre prácticas recomendadas, que se había publicado en 2003 fue retirado por el IEEE en febrero de 2006. Tras la aparición de IEEE 802.11-2007, el IEEE continuó el desarrollo de las siguientes nuevas enmiendas:[10]

- **IEEE 802.11k:** aprobado en el 2008. Utiliza los equipos de red y los terminales Wi-Fi para hacer un uso eficiente de los recursos de radio, facilita la selección de un nuevo AP con lo que ayuda a reducir el tiempo necesario para el cambio, complementando a los procedimientos de 802.11r.

- **IEEE 802.11n:** fue ratificado el 11 de septiembre de 2009. Ofrece una velocidad de transferencia hasta 600 Mbps, trabajando en las frecuencias de 2,4 GHz y 5 GHZ. Este estándar incorpora un ancho de banda de los canales de 40MHz, la tecnología MIMO, incluyendo mejoras a nivel físico y MAC. Todas las versiones de 802.11xx, aportan la ventaja de ser compatibles entre sí, de forma que el usuario no necesitará nada más que su adaptador wifi integrado para poder conectarse a la red. Sin duda esta es la principal ventaja que diferencia a Wi-Fi de otras tecnologías propietarias, como LTE (Long Term Evolution), UMTS (Sistema universal de telecomunicaciones móviles) y Wimax (Interoperability for Microwave Access).
- **IEEE 802.11r:** aprobado en el 2008. Tiene como objetivo minimizar el tiempo que tarda un terminal móvil en cambiar de un punto de acceso (AP) a otro según se desplaza para obtener mejor cobertura.
- **IEEE 802.11s:** especifica procedimientos para redes Wi-Fi malladas en las que la información puede dar varios saltos a través de enlaces de radio entre equipos Wi-Fi hasta llegar a su destino.
- **IEEE 802.11u:** cambios en 802.11 para facilitar el interfuncionamiento con redes externas.

- **IEEE 802.11v:** se encarga de gestionar las redes y los dispositivos Wi-Fi.
- **IEEE 802.11w:** extensión de 802.11i para proteger las tramas de gestión.
- **IEEE 802.11y:** operación en la banda de 3650-3700 MHz en EE.UU.
- **IEEE 802.11z:** extensiones del mecanismo DLS (Direct Link Setup) de 802.11e.
- **IEEE 802.11aa:** transporte de audio y vídeo en modo streaming.
- **IEEE 802.11ac:** caudal alto en bandas por debajo de 6 GHz.
- **IEEE 802.11ad:** caudal alto en la banda de 60 GHz (57-66 GHz).
- **IEEE 802.11.2:** a diferencia de las anteriores, este documento no es una enmienda, sino que define una práctica recomendada para la evaluación de prestaciones de 802.11 en diversos escenarios.

1.4 Estructuras y elementos de la red.

Las WLAN se integran en una red IP de forma similar a las LAN cableadas. Es común, que el mismo equipo que implementa las funciones de punto de acceso Wi-Fi (AP), integre también un enrutador IP con interfaces Ethernet e incluso el módem ADSL.[9]

En el caso de una WLAN que cubra un área amplia, por ejemplo una universidad, será necesario desplegar varios AP en lugares adecuados de la zona a cubrir. La conexión entre los AP y la red IP de la entidad de que se trate se puede hacer con cableado Ethernet.[1]

Existen diferentes arquitecturas de red para interconectar WLAN con redes móviles. Mediante esta interconexión los usuarios pueden acceder a los servicios de su red móvil también desde terminales WLAN. Además si el usuario dispone de un terminal dual puede utilizarlo para acceder directamente a la red móvil o a través de la WLAN dependiendo de las coberturas disponibles, tipo de servicio.[14]

- ***Adaptadores de Red Inalámbricos***

Estas son las interfaces que conectarán los equipos de los usuarios (PC, Notebooks, etc.) a la estructura de la red. Estos elementos tienen distintos modelos según la forma en que se conecten al equipo del usuario. Hay tres dispositivos internos para conectarse a los buses PCMCIA (Personal Computer Memory Card International Association), PCI (Peripheral Component Interconnect), CompactFlash (dispositivo de almacenamiento de datos) y uno externo para conectarlo al conector USB del equipo del usuario.

- ***Punto de Acceso Inalámbrico***

Este dispositivo permite a los equipos que poseen Adaptadores de Red Inalámbricos conectarse entre sí. Además permite comunicarse con otros Puntos de Acceso de modo de ampliar la cobertura de la LAN. Esta última función se asocia a una funcionalidad como Bridge. Además de conectar equipos de usuarios se pueden conectar switches o routers pertenecientes a la infraestructura de red de cableado de cobre o fibra preexistente.

- ***Punto de Acceso de Red Inalámbrico con funciones de Router.***

Cuando es necesario unir una LAN con otra LAN, es recomendable utilizar este dispositivo que será el encargado de interpretar las direcciones de origen y destino de las comunicaciones internas o externas y encaminarlas convenientemente.

- ***Antenas***

Si bien cada uno de los dispositivos WLAN anteriores poseen un dispositivo irradiante básico que le permite comunicarse con otros dispositivos cercanos, es posible que las distancias entre los usuarios sea tal, que se deba utilizar antenas con características especiales. Normalmente el tipo de antena a utilizar se elige según la topología de los puntos a unir. Por ejemplo para una topología punto a punto se utiliza una antena direccional que concentre la potencia en un determinado sentido; para una topología Punto-Multipunto se utiliza una Antena Omnidireccional en el centro geográfico de la red y antenas direccionales apuntando al centro en los puntos circundantes.

- ***Amplificadores***

Cuando con la potencia irradiada por las antenas no alcanza para cubrir adecuadamente la dispersión de usuarios de la red, es necesario agregar amplificadores para la señal de transmisión.

1.5 Mecanismos de seguridad en redes WLAN.

Al igual que son numerosos los ataques a redes WLAN existentes, también lo son los mecanismos de seguridad que se pueden aplicar para proteger los mismos, éstos actúan en las diferentes capas del modelo OSI. Es importante resaltar que los mecanismos de

seguridad para redes WLAN están evolucionando continuamente para adaptarse a las necesidades de seguridad de los usuarios.

1.5.1 Mecanismos de seguridad del nivel de enlace IEEE 802.11

Desde la aparición de las redes WLAN los mecanismos del nivel de enlace desarrollados específicamente para garantizar su seguridad han sido: WEP, WPA, IEEE 802.11i y WPA2. Existen otros dos protocolos de seguridad del nivel de enlace, que son aplicables también en otros tipos de redes (por ejemplo Ethernet) además de las redes WLAN. Estos son PPTP y L2TP .[3]

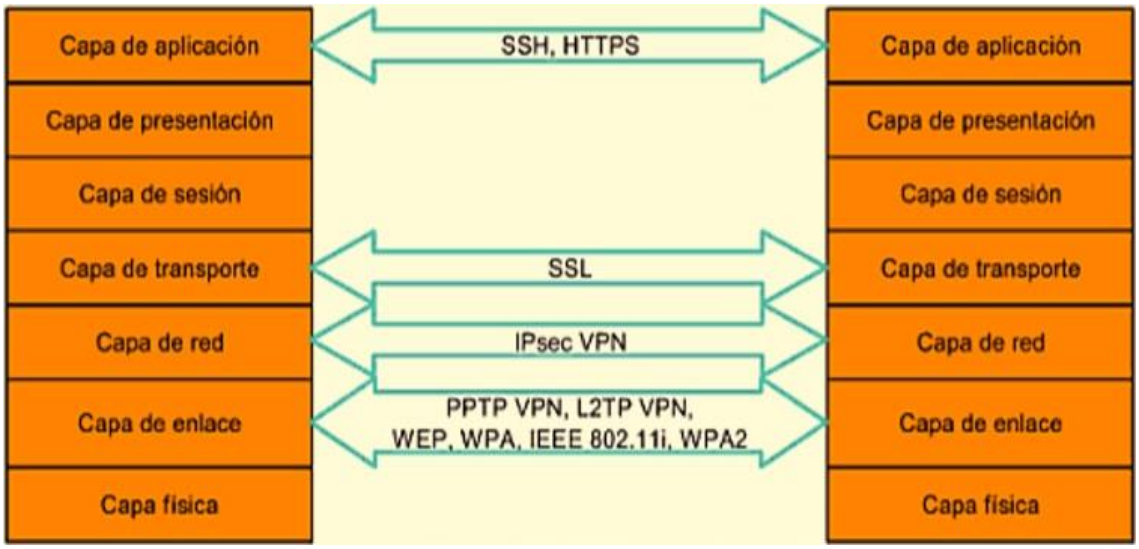

Figura 3. Mecanismos de seguridad existentes en las diferentes capas del modelo OSI.[1]

IEEE 802.11 es un estándar de la IEEE que define los protocolos de comunicaciones en las capas Física y Enlace del modelo de referencia OSI para Redes Inalámbricas de Área Local; 802.11 fue la versión original publicada en 1997, pero se han realizado mejoras en la velocidad de transmisión y actualmente se tienen las siguientes variantes: 802.11b, 802.11a, 802.11g y 802.11n.[11]

1.5.1.1 Protocolo WEP (Wired Equivalent Privacy).

El protocolo WEP no fue creado por expertos en seguridad o criptografía, así que pronto se demostró que era vulnerable ante los problemas RC4 descritos por David Wagner cuatro años antes. En 2001, Scott Fluhrer, Itsik Mantin y Adi Shamir publicaron su famoso artículo sobre WEP, mostrando dos vulnerabilidades en el algoritmo de encriptación: debilidades de no-variación y ataques IV (Vector de Inicialización).

Los fallos de seguridad de WEP pueden resumirse en:

- Debilidades del algoritmo RC4 dentro del protocolo WEP debido a la construcción de la clave.
- Los IVs son demasiado cortos (24 bits – hacen falta menos de 5000 paquetes para tener un 50% de posibilidades de dar con la clave) y se permite la reutilización de IV (no hay protección contra la repetición de mensajes).
- No existe una comprobación de integridad apropiada (se utiliza CRC32 para la detección de errores y no es criptográficamente seguro por su linealidad).
- No existe un método integrado de actualización de las claves.
- Airodump: herramienta de sniffing utilizada para descubrir las redes que tienen activado WEP.[15]
- Aireplay: herramienta de inyección para incrementar el tráfico.[15]
- Aircrack: crackeador de claves WEP que utiliza los IVs únicos recogidos.[15]

WEP es el mecanismo de seguridad más básico de todos los existentes. Solo dispone de un solo mecanismo de autenticación: la propia clave WEP. Debido a la ampliamente demostrada inseguridad de WEP[16] surgieron los estándares IEEE 802.11i, WPA y WPA2 que mejoran la autenticación y el cifrado en una WLAN.[3][17]

1.5.1.2 Protocolo WPA (Acceso Protegido Wi-Fi)

Dada la magnitud de alarma que causó en los usuarios de equipos Wi-Fi la vulnerabilidad ante cualquier usuario malintencionado por el rompimiento de WEP, exigen una solución rápida y que no conllevara a cambiar sus equipos, es decir que fuera compatible con el hardware que ya poseían. WPA opera a nivel de MAC y está basado en el borrador del estándar IEEE 802.11i.[18]

WPA es un subconjunto de las especificaciones de 802.11i (se basó en el Draft 3 de 802.11i.). El estándar IEEE 802.11i introdujo varios cambios fundamentales, como la separación de la autenticación de usuario de la integridad y privacidad de los mensajes, proporcionando una arquitectura robusta y escalable, que sirve igualmente para las redes locales domésticas como para los grandes entornos de red corporativos. La nueva arquitectura para las redes Wireless se llama RSN (Robust Security Network) y utiliza autenticación 802.1X, distribución de claves robustas, nuevos mecanismos de integridad

y privacidad. Además de tener una arquitectura compleja, RSN proporciona soluciones seguras y escalables para la comunicación inalámbrica. Una RSN sólo aceptará máquinas con capacidades RSN, pero IEEE 802.11i también define una red transicional de seguridad, TSN (Transitional Security Network), una arquitectura en la que pueden participar sistemas RSN y WEP, permitiendo a los usuarios actualizar su equipo en el futuro. Si el proceso de autenticación o asociación entre estaciones utiliza 4-Way handshake, la asociación recibe el nombre de RSNA (Robust Security Network Association).[18]

WPA incrementa el tamaño de las claves y el número en uso e introduce un nuevo mensaje de control de integridad seguro. Concretamente WPA contempla:[3]

- **IEEE 802.1X** como estándar de control de acceso. Maneja dos opciones para su implantación: el modo "**personal**" que considera el uso de una clave compartida como método de autenticación para evitar el tener que instalar un servidor RADIUS, y el modo "**enterprise**" basado en el uso de un RADIUS como servidor de autenticación.
- **TKIP** como esquema de encriptación con claves de 128 bits y vector de inicialización de 48 bits, además de contemplar un sistema para la asignación dinámica de claves y rotación de las mismas. Cara al control de integridad incorpora el algoritmo MIC.

1.5.1.3 Acceso Protegido Estándar IEEE 802.11i o WPA2 (Wi-Fi Protected Access 2)

El estándar 802.11i fue adoptado y recibió el nombre comercial WPA2 por parte de la Alliance Wi-Fi. WPA2 fue diseñado para resolver las necesidades de muchas organizaciones, buscando una tecnología interoperable y certificada basada en el estándar completo de IEEE 802.11i. WPA2 es compatible con WPA, por lo que algunos productos WPA pueden ser actualizados a WPA2 por software. Sin embargo en otros casos es necesario un cambio del hardware debido a los altos requerimientos de cómputo del cifrado AES.[19] El estándar IEEE 802.11i introdujo varios cambios fundamentales, como la separación de la autenticación de usuario de la integridad y privacidad de los mensajes, proporcionando una arquitectura robusta y escalable, que

sirve igualmente para las redes locales domésticas como para los grandes entornos de red corporativos.[20]

1.6 Protocolos de red para la autenticación.

La seguridad incluye varios aspectos, todos importantes. Uno de ellos es controlar quiénes acceden a la red (Autenticación), a qué servicios tienen acceso (Autorización) y por qué tiempo hacen uso del mismo (Accounting). En esta dirección, los protocolos de seguridad más usados en todo el mundo para el control de acceso a redes son: RADIUS, TACACS+ y DIAMETER.[21]

1.6.1 RADIUS (Remote Authentication Dial-In User Server)

RADIUS (Remote Authentication Dial-In User Server) desarrollado originalmente por Livingston Enterprise en 1991 y publicado posteriormente en las RFC 2138 y 2139, actualmente está definido en la RFC 2865 (Autenticación y Autorización) y en la 2866 (Contabilización).[21]

Es un protocolo para el control de acceso a la red, implementado en dispositivos como routers, switch y servidores, provee autenticación centralizada, autorización y manejo o contabilización de cuentas (AAA). Es un sistema de seguridad distribuido que garantiza el acceso remoto a redes y servicios de la red contra el acceso no autorizado.[22][23]

RADIUS consta de tres componentes: un protocolo con un formato de trama que utiliza el Protocolo de Datagramas de Usuario (UDP), un servidor y un cliente.[24]

Principales características:

- ***Funciona bajo el modelo cliente-servidor***, pues requieren de un cliente RADIUS, que puede ser un NAS, que interactúe con los servidores RADIUS. Los clientes transmiten a los servidores información del usuario, generalmente sus credenciales como nombre y contraseña. Los servidores se encargan de recibir las solicitudes de conexión de usuarios, autenticar al usuario y brindarle toda la información de configuración necesaria al cliente RADIUS para que pueda ofrecerle al usuario el servicio deseado.
- Los servidores RADIUS soportan varios esquemas de autenticación de usuario como: EAP (Extensible Authentication Protocol), PAP (Password Authentication

Protocol) y CHAP (Challenge Handshake Authentication Protocol) y soportan varios orígenes de información como: una base de datos del sistema (/etc/passwd), o una base de datos interna (del propio servidor RADIUS), mecanismos PAM y otros como Active Directory, LDAP y Kerberos.

- Es un protocolo de la capa de aplicación que utiliza UDP como transporte. Los puertos oficialmente definidos por la IANA (Internet Assigned Numbers Authority) son el 1812 para la autenticación y el 1813 para la contabilización, pero están los puertos 1645 y 1646 no oficiales pero ampliamente usados en implementaciones de servidores y clientes RADIUS.
- Capacidad para el manejo de sesiones, notificando inicio/cierre de conexión, lo que permite que al usuario se le pueda determinar su consumo y facturar en consecuencia; esta constituye una de las características fundamentales de este protocolo.

Cuando un usuario o equipo envía una solicitud a un NAS (Servidor de Acceso a la Red) para obtener acceso a un recurso de red particular, envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere al dispositivo NAS a través de los protocolos de la capa de enlace, por ejemplo PPP quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS solicitando el acceso a la red. El servidor RADIUS comprueba que la información es correcta utilizando algunos de los esquemas de autenticación mencionados anteriormente (esto dependen del propio servidor RADIUS).[25]

El servidor entonces devuelve una de las tres respuestas siguientes:

1. **Acceso aceptado:** el usuario tiene acceso. Una vez que el usuario se ha autenticado, el servidor RADIUS le asigna los recursos de red como dirección IP entre otros parámetros.
2. **Reto de acceso:** se solicita información adicional de usuario como PIN (Número Identificación Personal), una contraseña secundaria o, simplemente se emplean diálogos de autenticación entre el usuario y el Server RADIUS por medio del uso de túneles seguros entre ellos, de manera que las credenciales de acceso están ocultas para el servidor de acceso a la red.

3. **Acceso rechazado:** se le rechaza el acceso al usuario por diferentes razones, entre ellas que la cuenta del usuario esté desactivada o sea desconocida, o al proporcionar una prueba no válida de identificación.

El hecho de que el protocolo RADIUS sea abierto, proporciona ventajas, en cuanto a que puede soportar diferentes esquemas de autenticación, además de estar ampliamente extendido debido a la cantidad de productos que implementan este protocolo.[26]

1.6.2 TACACS+ (Terminal Acces Controller Access Control System)

TACACS+ está basado en el protocolo TACACS (Terminal Acces Controller Access Control System) utilizado para el control de acceso mediante autenticación y autorización, definido desde 1997 por el IETF (Interner Engineering Task Force) en un borrador no publicado draft-grant-tacacs 02.txt.[27]

TACACS+ evoluciona los protocolos anteriores, incluyendo nuevas características de seguridad en sus paquetes; mientras que RADIUS combina la autenticación y autorización en un perfil de usuario, TACACS+ separa estas acciones.[24][27]

TACACS+ es un protocolo propietario de Cisco que funciona bajo el modelo cliente-servidor y emplea el protocolo TCP para el transporte, puerto 49. A diferencia del protocolo RADIUS, este implementa encriptación no sólo en las credenciales sino también en los datos, utilizando también un secreto compartido mediante el algoritmo de encriptación MD5.[24]

Los mensajes que se intercambian entre un cliente y un servidor TACACS+, tienen el formato siguiente:[27]

- **Version** (Versión): 1 octeto para indicar el número de versión
- **Type** (Tipo): 8 bits para indicar un tipo de mensaje dependiendo de la acción: autenticación autorización o contabilización.
- **Seq_no** (Número de secuencia): 1 octeto para indicar el número de secuencia de paquetes de la sesión actual.
- **Flags** (Banderas): 1 octeto para indicar si hay o no datos encriptados después del campo longitud.
- **Session_id** (identificador de sesión): 4 octetos para identificar la sesión en cada paquete de respuesta del servidor.

- **Length** (Longitud): Longitud del paquete.

Debido al crecimiento de Internet y la introducción de nuevas tecnologías de acceso, incluidas las inalámbricas, DSL, Mobile IP y Ethernet, routers y servidores de acceso de red cuya complejidad y densidad demandan nuevas exigencias en los protocolos AAA, como por ejemplo manejar políticas para varios servicios, incapaz de cubrirlas con TACACS+ es que surge DIAMETER.

1.6.3 DIAMETER

Desarrollado en 1998 y definido por la IETF (Grupo de Trabajo de Ingeniería de Internet) desde el 2003 en la RFC 3588 en la que se definen una serie de parámetros mínimos para un protocolo AAA, aunque existen otras RFC que definen parámetros del protocolo sobre IP4, IP6, 3GGP, SIP, QoS. DIAMETER usa los protocolos TCP o SCTP para el transporte por el puerto 3868 y emplea seguridad mediante el uso de TLS o IPSEC.[28]

Este protocolo proporciona autenticación, autorización y contabilidad, para aplicaciones de acceso a la red o de movilidad IP (roaming), también extiende su uso para situaciones de roaming, está diseñado para trabajar localmente como en estado de alerta, sondeo y captura, con la finalidad de ofrecer servicios dinámicos [9]. Una de las principales características de este protocolo es su flexibilidad y extensión mediante la adición de nuevos comandos y atributos, por ejemplo para el uso del EAP, lo que facilita entrega confiable de los pares atributos-valores (AVPs), capacidad de negociación, notificación de errores, posibilidad de expansión al poder agregar nuevos comandos y AVPs y servicios básicos de aplicaciones como por ejemplo manejo de sesiones y contabilidad.[29]

Las AVPs constituyen una parte importante de este protocolo, se usan para enviar información, algunas son empleadas para el funcionamiento propio de DIAMETER y otras para transmitir los datos de las aplicaciones que usan DIAMETER.[24]

Dado que DIAMETER no es un protocolo completo en sí mismo, sino que requiere de extensiones específicas para cada aplicación referentes a la tecnología o arquitectura de acceso a la red; el mismo sólo provee requisitos mínimos para ser protocolo AAA, por tanto para su implementación es necesario garantizar la interoperabilidad, significa que

todos los nodos deben estar preparados para recibir mensajes DIAMETER y evitar el bloqueo, lo que significa que todos los nodos DIAMETER deberían usar SCTP.[30]

Los mensajes DIAMETER están formados por una cabecera DIAMETER y un número variable de pares Atributos-Valores (AVPs), teniendo los paquetes la siguiente estructura:[24][30]

En la **cabecera** AVP se especifican algunos parámetros como: la compatibilidad con RADIUS, si el paquete es un acuse de recibo y contiene códigos de comandos, se especifican números de secuencias para corresponder las solicitudes con las respuestas y se indican próximo envío y próximo recibido.

Los comandos AVP definen o especifican, entre otros parámetros, los comandos DIAMETER usados e indican si el AVP está encriptado usando encriptación hop-by-hop y especifican si se requiere soporte AVP.

El flujo de mensajes con DIAMETER se inicia con la estabilización de la conexión. Después el iniciador envía un mensaje de Solicitud e Intercambio de Capacidades (CER), la otra parte envía un mensaje de respuesta de intercambio de capacidades (CEA), posteriormente puede negociarse si se desea TLS, esto es opcional y la conexión está lista para el intercambio de mensajes de aplicación. Si no han ocurrido intercambios de mensajes por un tiempo, uno de los dos enviará una solicitud de dispositivo “perro guardián” (DWR) y el otro deberá responder con una respuesta al dispositivo “perro guardián” (DWA). La comunicación puede terminarse por cualquiera de las partes enviando una solicitud de desconexión (DPR) y la otra parte debe responder a la solicitud (DPA). Con esto ya queda desconectada la conexión.

DIAMETER es empleado básicamente para aplicaciones IMS (Subsistema de Multimedia IP) en aplicaciones 3GPP y aplicaciones móviles sobre Ipv4.

1.7 Servidores que implementan el protocolo RADIUS.

Tabla 1. Comparativa de diferentes servidores que implementan el protocolo RADIUS.

	Sistema Operativo	Encriptación que soporta	Base de Datos	No
Tekradius	Windows	MD5, PEAP, y TLS	LDAP, SQL, PostgreSQL	Si
EmeraldV5	Windows Linux	PEAP, TTLS y LEAP	LDAP, SQL, PostgreSQL	No
RAD-series	Windows	MD5, TLS, PEAP, TTLS y LEAP	LDAP, SQL, PostgreSQL	No
Odyssey	Windows	MD5, TLS, PEAP, TTLS y LEAP	LDAP, SQL, PostgreSQL	No
Steef Belted Radius 4.0	Windows Sun Solaris	MD5, TLS, PEAP, TTLS y LEAP	LDAP, SQL, PostgreSQL	No
Zeroshell	Windows Linux	EAP-TLS, EAP-TTLS y PEAP	LDAP, SQL, PostgreSQL	Si
FreeRADIUS	Linux, Debian, Ubuntu, Suse, Mandriva, FedoraCore, FreeBSD, MacOS, OpenBSD, Solaris Windows	MD5, TLS, PEAP, TTLS y LEAP	LDAP, OpenLDAP SQL, PostgreSQL	Si
daloRADIUS	Linux, Debian, Ubuntu, Suse, Mandriva	MD5, TLS, PEAP, TTLS	LDAP, OpenLDAP, SQL	Si

La implementación de este servidor se hubiese podido llevar a cabo por otros productos de control de acceso como lo son FreeRADIUS, Zeroshell, daloRADIUS. En el caso de daloRADIUS y Zeroshell, estos implementan y dejan de brindar otras características que no son de interés en este trabajo. Por su parte, FreeRADIUS es un proyecto de OpenSource que brinda tantas funcionalidades como el resto de los servidores analizados. Por lo que en esta dirección se escoge FreeRADIUS como servidor de dominio por ser el que mejor se adecua a las características y necesidades de la entidad.

1.7.1 FreeRADIUS una opción de Software Libre para la seguridad de redes.

Según la Free Software Fundación, el Software Libre respeta la libertad de los usuarios sobre su producto adquirido y, por tanto, una vez obtenido puede ser usado, copiado, estudiado, modificado y redistribuido libremente.[31]

El software libre suele estar disponible gratuitamente, o al precio de costo de la distribución a través de otros medios; sin embargo no es obligatorio que sea así, por lo tanto no hay que asociar software libre a "*software gratuito*" (denominado *freeware*) ya que, conservando su carácter de libre, puede ser distribuido comercialmente "software comercial". Análogamente, el "software gratis" o "gratuito" incluye en ocasiones el código fuente; no obstante, este tipo de software no es libre en el mismo sentido que el software libre, a menos que se garanticen los derechos de modificación y redistribución de dichas versiones modificadas del programa.[32]

El Software Libre cuenta con una gran comunidad de apoyo y soporte, ha ido ganando espacio en la actualidad cubana, impulsado también por ser una tecnología que no se comete delito por tenerlo o usarlo, permitiendo ahorrar recursos en el pago de licencias. El acceso de usuarios móviles no deseados a la red inalámbrica se puede evitar implementando Software Libre que permita autentificar, autorizar y contabilizar los accesos; dicha herramienta que lo permite es FreeRADIUS.

Proyecto iniciado en 1999 por Alan DeKok y Miquel Van Smoorenburg, este software libre y de código abierto es uno de los servidores RADIUS de mayor popularidad en el mundo. Inició como un proyecto de servidor RADIUS que permitiera una mayor colaboración de la comunidad y que pudiera cubrir las necesidades que otros servidores RADIUS no podían.[33]

FreeRADIUS puede ser configurado en una antigua torre de escritorio para servir en cualquier lugar, puede operar tanto en sistemas con recursos limitados atendiendo desde una docena o a unos cientos de usuarios, o puede ser instalado en los servidores apropiados para apoyar a millones de usuarios y peticiones. Actualmente incluye soporte para LDAP, SQL y otras bases de datos, así como EAP, EAP-TTLS y PEAP. Además de incluir soporte para todos los protocolos comunes de autenticación y bases de datos.

Convirtiéndolo en uno de los más completos, versátiles y usados en todo el mundo, gracias a la variedad de módulos que le componen.[34]

Además de implementar diversos elementos relacionados con RADIUS, tales como:[33][34]

- Una biblioteca BSD para clientes, módulos para soporte en apache y un servidor de RADIUS.
- El servidor de FreeRADIUS es modular, para facilitar su extensión, es escalable y soporta prácticamente toda clase de clientes Radius (por ejemplo, ChilliSpot, JRadius, etc.)
- Se puede ejecutar en múltiples sistemas operativos: Linux (Debian, Ubuntu, Suse, Mandriva, FedoraCore, etc.), FreeBSD, MacOS, OpenBSD, Solaris, e incluso MS Windows por medio de cygwin.
- Soporta el uso de proxies y la replicación de servidores.

1.8 Conclusiones Parciales:

Se caracterizan las redes inalámbricas, sus funcionalidades, las ventajas que estas nos brindan, sus principales protocolos y se explican los riesgos a los que están expuestas estas redes, los mecanismos de seguridad que se pueden aplicar para proteger las redes WLAN varían según el nivel de seguridad requerido, el tipo de servicio deseado, el coste de gestión y mantenimiento de las soluciones adoptadas y como estos mecanismos actúan en la ***capa de enlace*** del modelo OSI, siendo WPA, WPA2 e IEEE802.11i los de mayor uso. De todos los mecanismos mencionados WPA, WPA2 e IEEE 802.11i son mecanismos de seguridad propios de redes WLAN.

Se describen las diferentes características de los protocolos de autenticación de usuarios en redes WLAN, cómo la elección de uno u otro depende de las necesidades e interés del negocio, DIAMETER es empleado básicamente para aplicaciones IMS (Subsistema de Multimedia IP) en aplicaciones 3GPP y aplicaciones móviles sobre Ipv4 y se propone la utilización de Software Libre mediante el empleo de herramientas y protocolos para la autenticación de usuarios en redes WLAN.

Para llevar a cabo la arquitectura que se propone en este trabajo se utilizará un Servidor RADIUS y como herramienta para los mecanismos de control de acceso FreeRADIUS.

Capítulo 2: Diseño de arquitectura para el control de acceso a la red WLAN de la UCF.

La utilización de tecnologías de software libre y de código abierto en las redes corporativas es una tendencia que va en aumento en todo el mundo, debido a sus ventajas económicas, pues estas abaratan los costos, al poder contar con las licencias de software (gratis en la mayoría de los casos), y los bajos costos relacionados con la infraestructura dando un mayor grado de flexibilidad.

2.1 Restricciones y necesidades.

La Universidad de Cienfuegos cuenta con un gran número de usuarios (personas vinculadas a la universidad y visitantes autorizados), los cuales tienen acceso a las aplicaciones web disponibles en el centro; por lo que el uso seguro de la red es de vital importancia. Para ello, en años anteriores, se ha trabajado en este tema, con el fin de brindar servicios de seguridad en la red WLAN.

En la UCF, está implementada una arquitectura de control de acceso que tiene como principal medida de control el Control de Acceso al Medio (MAC), la asignación de Internet Protocol (IP) y la asignación de nombre de usuario y contraseña a cada uno de los usuarios. Sin embargo aunque el filtrado por MAC es un método extendido por todo el mundo por su facilidad de configuración; se basa en realizar dicho control mediante la comprobación de la dirección MAC de nivel 2 o nivel de trama. Este sistema de autenticación tiene varios problemas. El primero es que cada vez que un usuario es adicionado o eliminado y los usuarios no son fijos o hay usuarios itinerantes, hay que dar de alta y de baja direcciones con la siguiente carga de gestión y el consiguiente peligro de dejar alguna entrada a la lista ***"olvidada"***, estas modificaciones se realizan de forma manual lo que requiere de tiempo y acceso a diferentes sistemas, complicando la administración del servicio y afectando la prontitud en la respuesta a los usuarios finales que tienen que moverse hasta el nodo central para realizar su solicitud, haciendo que la carga administrativa de la WLAN aumente. Otra de las atenuantes es lo fácil que resulta cambiar la dirección MAC de un dispositivo, lo que hace sencillo sustituirla por una válida, y por tanto, que este método de autenticación resulte vulnerable. El método de ataque consiste en capturar y analizar el tráfico que pasa por la WLAN y guardar direcciones MAC válidas, para en el momento que alguna de ellas quede libre, sustituir ésta por la dirección

MAC del dispositivo cliente. De todo esto se deduce inmediatamente que este método de autenticación resulta claramente ineficiente. A esto último se suma el aumento significativo de la cantidad de usuarios con dispositivos móviles que soportan el estándar Wi-Fi.

Otro de los objetivos que se persiguen con dicha propuesta es que en Cuba desde el 2005 se promueve la migración al Software Libre en aras de alcanzar la soberanía tecnológica y la seguridad del país. Existen múltiples herramientas de Software Libre para la seguridad de redes, imprescindibles a tener en cuenta en las redes cubanas. Al utilizarlas se atiende a la necesidad del país de migrar a dichas tecnologías y proteger la información de las empresas cubanas.

Debido a las restricciones, la política de conexión a la red requiere de diferentes niveles de seguridad en la conexión inalámbrica, en función de los permisos de acceso del perfil de usuario.[35]

El modelo de arquitectura para el acceso inalámbrico universal a una WLAN corporativa requiere de una solución de compromiso entre la seguridad del acceso, la compatibilidad de los dispositivos cliente y la necesidad de brindar diferentes servicios a grupos de usuarios distintos.[9]

A continuación se mencionan algunas de las restricciones y necesidades importantes del acceso Wi-Fi universal:[13]

Compatibilidad del equipamiento: Esta es una restricción importante a la hora de definir la política de seguridad de acceso a la red de los dispositivos inalámbricos. Debido a que el problema de la compatibilidad tiene varias aristas, en este trabajo se asume que se cuenta con AP y con clientes compatibles con el estándar IEEE 802.11n; además se asume que los AP soportan los estándares de seguridad inalámbrica WPA y WPA2.

Compatibilidad de los sistemas operativos: No todos los Sistemas Operativos (S.O) soportan los modelos RSN o TSN, aun cuando el hardware del cliente lo soporte. No obstante en el caso de los S.O de computadoras este problema solo está presente en las versiones antiguas, muchas de ellas ya descontinuadas por sus fabricantes. Se puede afirmar que los S.O actuales de las familias Windows, Linux y Mac OS X tienen soporte tanto para WPA como WPA2. De igual forma pasa con los PDA y Smartphone, donde la mayoría tienen soporte para WPA y WPA2.[35]

Permisos de usuarios y grupos de usuarios: La validación de los usuarios así como los permisos asociados a estos presenta una gran complejidad. Primero se necesita una base de datos de usuarios que contenga la información necesaria para la autenticación, así como la información referente a los permisos tanto de grupo como permisos específicos de usuario. Esta base de datos debe ser compatible con los métodos de acceso seleccionados para la autenticación de los usuarios y con los S.O de los nodos cliente [39]. Además debe definirse un protocolo que permita realizar las tareas AAA necesarias para validar el acceso a los recursos de la red por parte de los usuarios; este protocolo debe actuar de nexo entre los mecanismos de autenticación de los equipos cliente y la base de datos de usuarios en el servidor. También se debe definir cómo se implementarán los permisos de usuario una vez que estos estén autenticados y conectados a la WLAN. Por último se deberá definir la forma en que se generarán los registros de las operaciones que llevan a cabo los usuarios; esto permitirá auditar tanto las operaciones cómo los patrones de tráfico, así como conocer si el comportamiento de la red inalámbrica es el deseado.

Herramientas de administración de usuarios y perfiles: Son necesarias herramientas que faciliten la administración de los permisos de usuarios y perfiles de usuarios, de tal manera que el crecimiento en el número de usuarios y perfiles no se convierta en un problema para los administradores de la red.[35]

2.2 Modelo de arquitectura

El modelo de arquitectura a proponer debe dar solución a las restricciones y necesidades planteadas en el epígrafe anterior. En la figura 1 se muestra el esquema lógico de conexiones (topología) de la arquitectura propuesta. En esta se puede observar que básicamente el acceso inalámbrico a la red corporativa se realiza por dos tipos de usuarios diferentes, esto se debe a que existen dispositivos (Notebooks, Smartphone…) que su hardware no es lo suficiente potente para trabajar con los algoritmos de seguridad propuestos por WAP y WAP2:

1. Usuarios que se conectan desde dispositivos móviles como Laptops, Notebooks, Tablet, PDAs, Smartphone. (**WLAN-1**).

2. Usuarios que se conectan desde estaciones de trabajo fijas situadas en laboratorios, departamentos, etc. (**WLAN-2**).

Debido a que el escenario de conectividad de los usuarios de las estaciones de trabajo fijas es más seguro, las reglas que se aplican son permisivas, considerando la red **WLAN-2** como parte de la red corporativa, aunque siempre tomando las previsiones necesarias (por ejemplo: VLAN independiente). Sin embargo en el caso de los usuarios que se conectan desde dispositivos móviles se aplican reglas restringidas en el firewall que separa la red **WLAN-1** de la red corporativa, de hecho se le considera como una red semipública dada la naturaleza itinerante de sus nodos.[35]

Ambas redes WLAN utilizan el mismo servidor de autenticación (servidor RADIUS) para llevar a cabo las tareas AAA. Sin embargo los métodos de acceso son totalmente diferentes. En el caso de la red **WLAN-1**, la cual brindará servicios de conectividad inalámbrica a la gama de dispositivos compatibles con el estándar IEEE 802.11n, los métodos son varios y van desde el uso de un Portal Cautivo hasta la utilización de tecnologías de VPN, con el objetivo de brindar el servicio de conexión a la WLAN de la UCF a la mayor cantidad y variedad de dispositivos posibles. Por otra parte en el caso de la red **WLAN-2**, la cual provee de conectividad inalámbrica a estaciones de trabajo con interfaces de red compatibles con IEEE 802.11n, el método de control de acceso es WPA2/WPA *Enterprise*, tal y como se implementa.

Como se puede observar en la figura 2, todo el tráfico de la red **WLAN-1** converge en el Servidor de Control de Acceso, realizándose en este punto todos los controles correspondientes a los permisos que poseen los usuarios dentro de su perfil de conectividad [39]. Es importante aclarar que el switch 1 debe soportar la implementación de VLANs para aislar los dominios de colisión de las redes LAN y **WLAN-2**, así como aislar en una VLAN independiente a los servidores de la red corporativa, con el correspondiente filtrado en el firewall del Router.

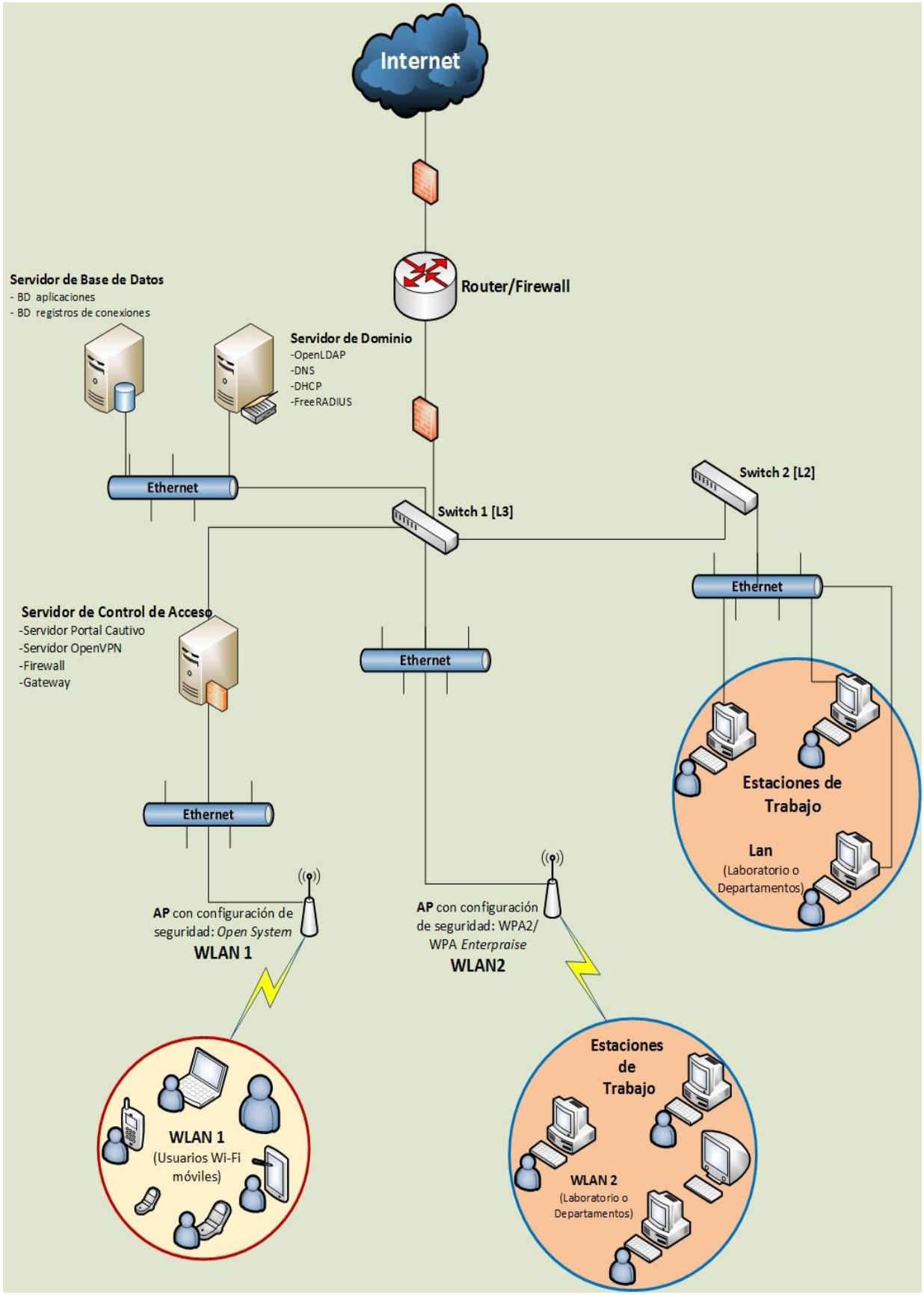

Figura 4. Topología de la arquitectura propuesta.

2.3 Módulos a implementar

En la figura 1 se muestran la implementación de los módulos Servidor de Dominio, Servidor de Bases de Datos y Servidor de Control de Acceso. Básicamente la arquitectura se divide en 4 módulos:

1. Puntos de Acceso Inalámbricos
2. Servidor de Control de Acceso
3. Servidor de Dominio
4. Servidor de Bases de Datos

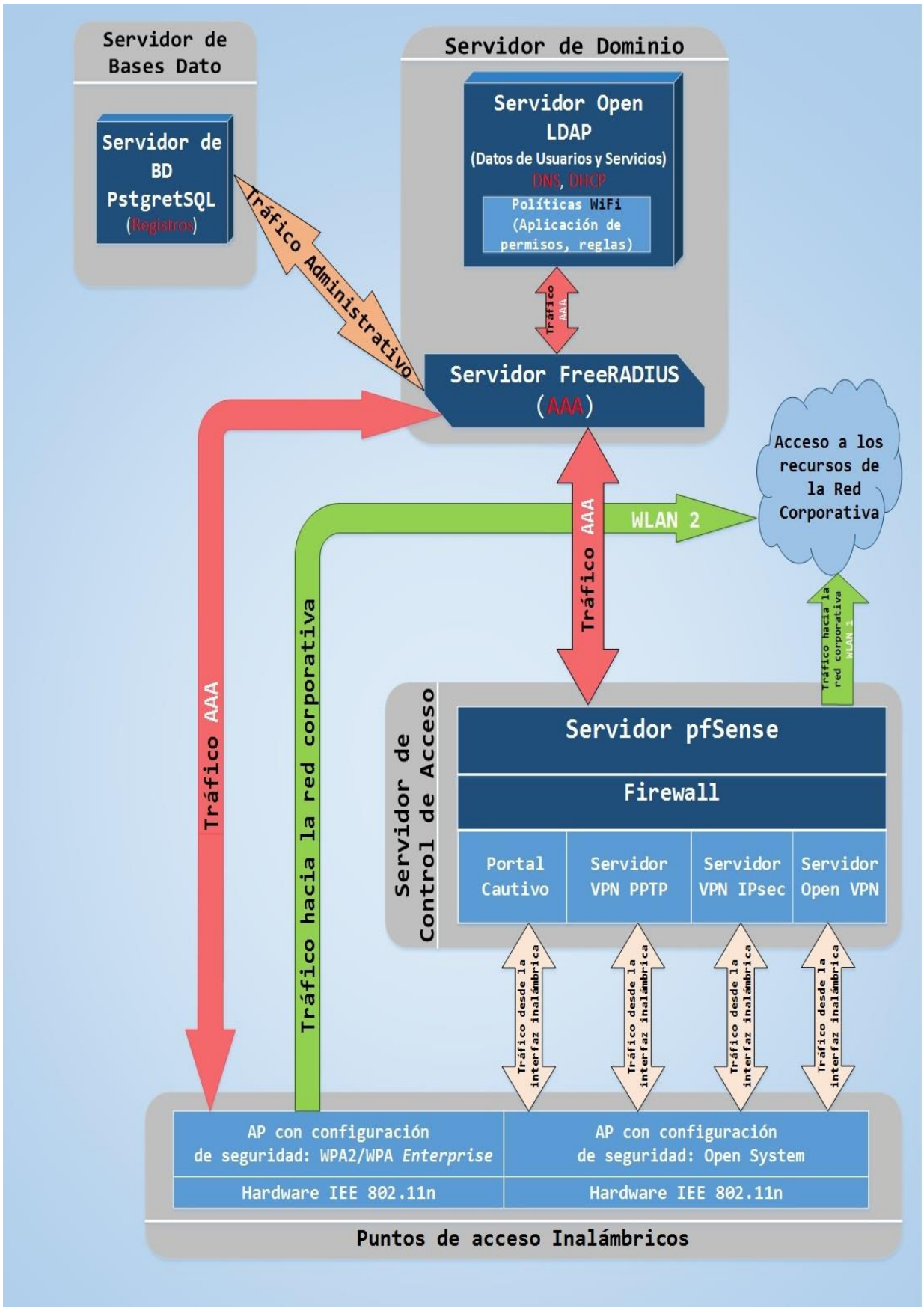

Figura 5. Módulos de la arquitectura que se deben implementar.

2.3.1 Puntos de acceso inalámbricos

Para la implementación de este módulo se necesitan al menos dos AP, uno para brindar servicio de conectividad inalámbrica a la red **WLAN-1** y el otro para la red **WLAN-2**. Debido a que la arquitectura propuesta es escalable pudieran utilizarse tantos AP como fuera necesario, todo está en dependencia de las necesidades de la institución donde se despliegue la misma. Las pruebas para la evaluación de la arquitectura se realizarán con dos AP NETGEAR WNAP320, compatibles con IEEE 802.11 b/g e IEEE802.11n además de soportar WPA/WPA2, clientes DHCP (Dynamic Host Configuration Protocol) y el estándar 802.1Q VLAN (virtual LAN). Estos AP se pueden gestionar tanto a través de SSH como de una interfaz web.[36]

2.3.2 Servidor de Control de Acceso

Este módulo es uno de los de mayor complejidad, está compuesto por cuatro bloques, cada uno con funciones específicas pero interdependientes. Estos bloques son:

- Servidor Portal Cautivo
- Servidor VPN PPTP
- Servidor VPN IPsec
- Firewall/NAT

Tabla 2. Comparativa de diferentes Servidores de Portal Cautivo.

Parámetros	Portal PfSense	Portal M0nowall	Portal Chillispot	Portal Air Marshall
Open Source	Posee todas las características de un Open Source.	No es un Open Source, es un free software que permite su libre uso y distribución pero no su libre modificación.	Posee todas las características de un Open Source.	No es un Open Source, es un free software que permite su libre uso y distribución pero no su libre modificación.
Facilidad de Instalación	Sencilla	Sencilla	Sencilla	Sencilla
Facilidad de Configuración	Sencilla mediante interfaz Web, incluye una larga lista de características que lo hacen atractivo para ser utilizado en ambientes corporativos.	Compleja, la configuración completa del sistema se almacena en un solo archivo de texto XML para mantener la transparencia.	Compleja, se realiza modificando el archivo de configuración en un editor de texto.	Sencilla mediante interfaz Web.
Seguridad	Confiables	Confiables	Confiables	Confiables
Escalabilidad	Cuenta con un gestor de paquetes para ampliar sus funcionalidades. Existen alrededor de setenta módulos disponibles.	Cuenta con un gestor de paquetes para ampliar sus funcionalidades.	No cuenta con un gestor de paquetes disponibles.	No cuenta con un gestor de paquetes disponibles.
Lenguajes que soportan	PHP	PHP	HTML, PHP, JAVASCRIPT	HTML
Interfaz del Administrador	Amigable y fácil de utilizar	Amigable y fácil de utilizar	No existe interfaz	Amigable y fácil de utilizar
Interfaz del Usuario	Amigable y fácil de utilizar	Amigable y fácil de utilizar	Amigable y fácil de utilizar	Amigable y fácil de utilizar

La implementación de este módulo se hubiese podido llevar a cabo por otros productos de control de acceso como lo son PfSense, M0n0wall, Chillispot, Air Marshall. En el caso de M0n0wall, éste implementa los cuatro bloques definidos dentro del Servidor de Control de Acceso y otras características que no son de interés en este trabajo. Por su parte, PfSense es un proyecto de software derivado del proyecto M0n0wall y básicamente brinda las mismas funcionalidades que éste, pero a su vez agrega otras, como un quinto bloque correspondiente al servidor de OpenVPN, que no es soportado por M0n0wall. Por lo que en esta dirección se escoge PfSense como servidor de control de acceso por ser el que mejor se adecua a las características y necesidades de la entidad.

PfSense

El proyecto PfSense se inició en septiembre de 2004 por Chris Buechler y Ullrich Scott como una derivación de M0n0wall. PfSense es una distribución personalizada de FreeBSD adaptado para su uso como Firewall y Router. Se caracteriza por ser de código abierto, puede ser instalado en una gran variedad de ordenadores, e incluye una larga lista de características que lo hace atractivo para ser utilizado en ambientes corporativos, además cuenta con una interfaz web sencilla basa en PHP para su configuración y administración, por lo que tanto no es indispensable contar con conocimientos avanzados sobre la línea de comandos UNIX para su manejo.[37][38]

I) Servidor Portal Cautivo

Un Portal Cautivo es un programa de una red informática que vigila el tráfico HTTP, fuerza a un cliente a ver una página web en especial, que usualmente se utiliza para autenticar al cliente, además de darle la bienvenida a los usuarios e informar de las condiciones del acceso que se ofrecen, una vez autenticado pueden navegar por Internet de forma normal y se redirige hacia una página web (que en este caso se aloja en PfSense). El programa intercepta todo el tráfico HTTP hasta que el usuario se autentifica. El portal se encargará de hacer que esta sesión caduque al cabo de un tiempo. También puede empezar a controlar el ancho de banda usado por cada cliente (permitiendo gestionar la Calidad de Servicio).[39] [40]

II) Servidor VPN PPTP

En los servidores Linux el soporte para PPTP (Point to Point Tunneling Protocol) es provisto por el servicio PoPToP y por módulos del kernel para PPP y MPPE. Es un protocolo de comunicaciones desarrollado por Microsoft, U.S. Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics conocidas colectivamente como PPTP Forum, para implementar VPN. La especificación para PPTP fue publicada por el RFC 2637, aunque no ha sido ratificada como estándar por el IETF. Permite el intercambio seguro de datos de un cliente a un servidor formando una VPN, esta tecnología PPTP encapsula los paquetes ppp en datagramas IP para su transmisión bajo redes basadas en TCP/IP. El punto fuerte del PPTP es su habilidad para proveer en la demanda, soporte multi-protocolo existiendo una infraestructura de área de trabajo, como Internet.[41]

III) Servidor VPN IPsec

IPsec (Internet Protocol Security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado. Los protocolos de IPsec (IP Security) se definieron originalmente en las RFC 1825 y 1829, publicadas en 1995, pero posteriormente fue actualizado en 1998 y 2005 (RFC 4301 y RFC 4309).[42]

PfSense incluye implementaciones de servidores de VPN utilizando a IPsec, pudiéndose crear 2 tipos básicos de VPNs: VPN sitio a sitio y VPN de acceso remoto.[37]

Los protocolos de IPsec actúan en la capa de red, la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan de la capa de transporte (capa 4 del modelo OSI) hacia arriba. Esto hace que IPsec sea flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP, los protocolos de capa de transporte más usados. Una ventaja importante de IPsec frente a SSL y otros métodos que operan en capas superiores, es que para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código.[42]

La utilización de este proporciona una serie de ventajas como lo son:[41][42]

- Integridad, confidencialidad y seguridad de datos.
- Las VPN reducen los costos y son sencillas de usar.
- Facilita la comunicación entre lugares distantes.

IV) Servidor OpenVPN

OpenVPN, es un producto de software creado por James Yonan en el año 2001 y que ha estado mejorando desde entonces. OpenVPN es una solución de conectividad publicada bajo la licencia GPL, de software libre. Ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente, resulta una buena opción en tecnologías Wi-Fi, además de soportar una amplia gama de configuraciones de VPN basadas en SSL/TLS (Secure Sockets Layer/ Transport Layer Security), incluyendo acceso remoto, LAN to LAN VPN, respuesta ante fallos y diferentes técnicas de control de acceso. Es una solución multiplataforma (Linux, Windows, OpenBSD, FreeBSD, NetBSD, Mac OS X y Solaris) que ha simplificado mucho la configuración de las VPN.[43]

OpenVPN implementa redes seguras en la capa 2 o 3 (según el modo que se utilice Tunnel o Bridge) de la pila de protocolos OSI utilizando como extensión el protocolo SSL/TLS, soportando métodos de autenticación del cliente de manera flexible. Otra de las ventajas de utilizar OpenVPN es la compatibilidad que ofrece con la infraestructura de clave pública (PKI) mediante el uso de certificados X.509 y la técnica de intercambio de claves RSA, es compatible con NAT (Network Address Translation), DHCP y con los dispositivos de red virtuales TUN/TAP. OpenVPN no ofrece compatibilidad con estándares tales como IPsec, IKE, PPTP o L2TP.[44]

Debido a todo lo expuesto anteriormente se propone utilizar OpenVPN en la implementación por su facilidad de uso y el alto nivel de seguridad que brindan las VPN implementadas con este software.

V) Firewall/NAT

En esta propuesta de implementación el Servidor de Control de Acceso juega el rol (entre otros) de Gateway de la red inalámbrica **WLAN-1**. En tal efecto actúa como router/firewall y aplica las reglas de conectividad al tráfico de red que pasa a través de él. Estas reglas se aplican a través del módulo de filtrado de PfSense. En el caso específico de las VPN IPsec es necesario la utilización de NAT-T (IPsec no es compatible con NAT por lo que es

necesario encapsular al protocolo ESP dentro de paquetes UDP) para que los clientes de la **WLAN-1** tengan acceso a los recursos de la red corporativa.[37]

VI) SSL/TLS (Secure Sockets Layer/ Transport Layer Security)

Secure Sockets Layer (capa de conexión segura) y su sucesor Transport Layer Security (seguridad de la capa de transporte) son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.[43]

SSL implica una serie de fases básicas como son:[45][43]

- Negociar entre las partes el algoritmo que se usará en la comunicación
- Intercambio de claves públicas y autenticación basada en certificados digitales
- Cifrado del tráfico basado en cifrado simétrico
- Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar.

2.3.3 Servidor de Dominio

Este módulo está compuesto por los servidores OpenLDAP y RADIUS. Además en el Servidor de Dominio se define la política de conectividad de los usuarios inalámbricos y se brindan los servicios de DNS y DHCP.

I) Servidor OpenLDAP

LDAP (Lightweight Directory Access Protocol) es un protocolo de Internet para acceder a servicios de directorio distribuidos que actúan en concordancia con los modelos de datos y servicios X.500 definidos por la ISO.

El proyecto OpenLDAP se inició en 1998 por Kurt Zeilenga. Es un servidor LDAP que se distribuye bajo licencia GNU (OpenSource), que permite que el software se pueda usar de forma gratuita tanto de forma educativa como profesional. Además se dispone del código fuente para poder realizar nuestras propias modificaciones, se puede ejecutar

en múltiples sistemas operativos: Linux (Debian, Ubuntu, Suse, Mandriva, FedoraCore, etc.), FreeBSD, MacOS, OpenBSD, Solaris, e incluso MS Windows por medio de Cygwin. Se caracteriza por:

- Operaciones de lectura rápidas: Debido a la naturaleza de los datos almacenados en los directorios las lecturas son comunes que las escrituras.
- Datos relativamente estáticos: Los datos almacenados en los directorios no suelen actualizarse con mucha frecuencia.
- Entorno distribuido, fácil replicación
- Estructura jerárquica: Los directorios almacenan la información de forma jerárquica de forma nativa.
- Orientadas a objetos: El directorio representa a elementos y a objetos. Los objetos son creados como entradas, que representan a una colección de atributos.
- Esquema Standard: Los directorios utilizan un sistema standard que pueden usar fácilmente diversas aplicaciones.

Figura 6. Elementos que intervienen en la autentificación OpenLDAP.

II) Servidor RADIUS

RADIUS es un protocolo de control de acceso que autentica usuarios a través de un método muy común denominado genéricamente desafío/respuesta. El proceso que lleva a cabo se denomina AAA.[46]

El proceso de AAA se puede sintetizar en las siguientes preguntas que realiza el servidor de acceso al cliente:[47][48]

- ¿Quién eres? (**A**uthentication)
- ¿Qué servicios estoy autorizado a darte? (**A**uthorization)
- ¿Qué hiciste con los servicios mientras los usabas? (**A**ccounting)

III) Política de conectividad Wi-Fi

Este bloque es uno de los pilares del modelo de arquitectura que se propone, el cual tiene como objetivo aplicar políticas de uso de la red inalámbrica a través de la aplicación de perfiles de conectividad a distintos grupos de usuarios.

Se pueden definir tantos perfiles de conectividad como se requiera para implementar las políticas de uso. Para aplicar estas herramientas es necesario definir los diferentes grupos de usuarios, definir las políticas de uso que se desea implementar y modelar los perfiles de conectividad que las reflejan y se deben aplicar a los grupos de usuarios.[35]

2.3.4 Servidor de Bases de Datos

La función de este módulo dentro de la arquitectura propuesta es el almacenamiento de los datos de registros (Accounting) del servidor RADIUS. Se propone el motor de bases de datos PostgreSQL, el cual es un ORDBMS (Object-Relational Database Management System) de software libre, robusto, potente, flexible e interoperable, soporta el estándar SQL [49]. De igual forma se podía haber elegido como motor de bases de datos a MySQL, sin embargo la arquitectura propuesta pretende ser genérica y escalable, por lo que en el caso de redes corporativas con gran cantidad de usuarios inalámbricos el volumen de datos a almacenar puede ser alto. Esto último es una razón para elegir a PostgreSQL por encima de MySQL, debido a que el primero es un motor de bases de datos robusto[35].

También se puede considerar tener el motor de bases de datos junto con el Servidor de Dominio y no en un servidor externo, de esta manera se minimiza la cantidad de equipos que interactúan, lo cual significa una menor cantidad de puntos de fallas.[46] Sin embargo tiene también sus desventajas, dentro de ellas que la arquitectura se haría monolítica y poco escalable, concentrando el procesamiento en un solo punto. Además es algo común que en las redes corporativas exista al menos un Servidor de Bases de Datos, por lo que no tiene sentido recargar al Servidor de Dominio con un servicio que ya es ofrecido por otro servidor dentro de la red corporativa en cuestión.

2.4 Conclusiones parciales

Utilizando herramientas de software libre fue posible construir un prototipo del modelo de infraestructura propuesto. Dicho prototipo, brinda a los administradores de red, un conjunto de herramientas que permiten representar, aplicar y controlar diferentes políticas

de uso de la red inalámbrica. A su vez ofrece a los usuarios múltiples formas de conectarse, a través las mismas credenciales.

El uso de protocolos libres permite que la infraestructura que se utiliza para la implementación, pueda ser usada simultáneamente por otros servicios que requieren de autenticación, disminuyendo el costo total de propiedad de la infraestructura de red al no duplicar servicios de autenticación a la vez que proporciona un nivel adecuado de escalabilidad.

Capítulo 3: Implementación técnica a escala de laboratorio.

En este capítulo se llevarán a cabo las pruebas de laboratorio correspondientes a la propuesta de arquitectura descrita en el capítulo anterior. Para ello se describe la instalación de del Servidor de Dominio, el Servidor de Base de Datos y el Servidor de Control de Acceso.

3.1 Instalación del Servidor de Dominio

Como servidor de dominio se utilizó Windows Server 2008 R2, con el objetivo de simular la situación existente en la entidad, lo más real posible. Además resultó ser idóneo teniendo en cuenta el tiempo disponible para realizar las pruebas.

Windows Server 2008 R2 es un sistema operativo de Windows Server y está diseñado para albergar la próxima generación de redes, aplicaciones y servicios web. Con este sistema operativo se puede desarrollar, entregar y administrar experiencias y aplicaciones de usuario de gran riqueza, ofrecer una infraestructura de red segura y aumentar la eficacia y el valor tecnológico dentro de la organización [50]. En la tabla 10 del Anexo B se detallan los requisitos de hardware para la instalación de Windows Server 2008 R2:

La instalación de este sistema operativo se realiza a través de un asistente bastante amigable, como es común en los sistemas de Microsoft. Una vez que se concluye la instalación de Windows Server 2008 R2 y se garantiza que todos los drivers correspondientes funcionan correctamente se debe proceder a instalar los siguientes roles:

- Active Directory Domain Services

- DNS Server

- DHCP Server

En la figura 7 se puede observar una vista de la herramienta de administración Server Manager, mediante la cual se instalan y configuran los roles. Una vez instalados dichos roles en el servidor de Dominio se cuenta con todos los servicios definidos en la arquitectura propuesta.

Además de estos roles es conveniente para las pruebas que se realizarán la instalación del rol Active Directory Certificate Services pues en determinados casos es necesario un certificado para que los clientes puedan validar al servidor.

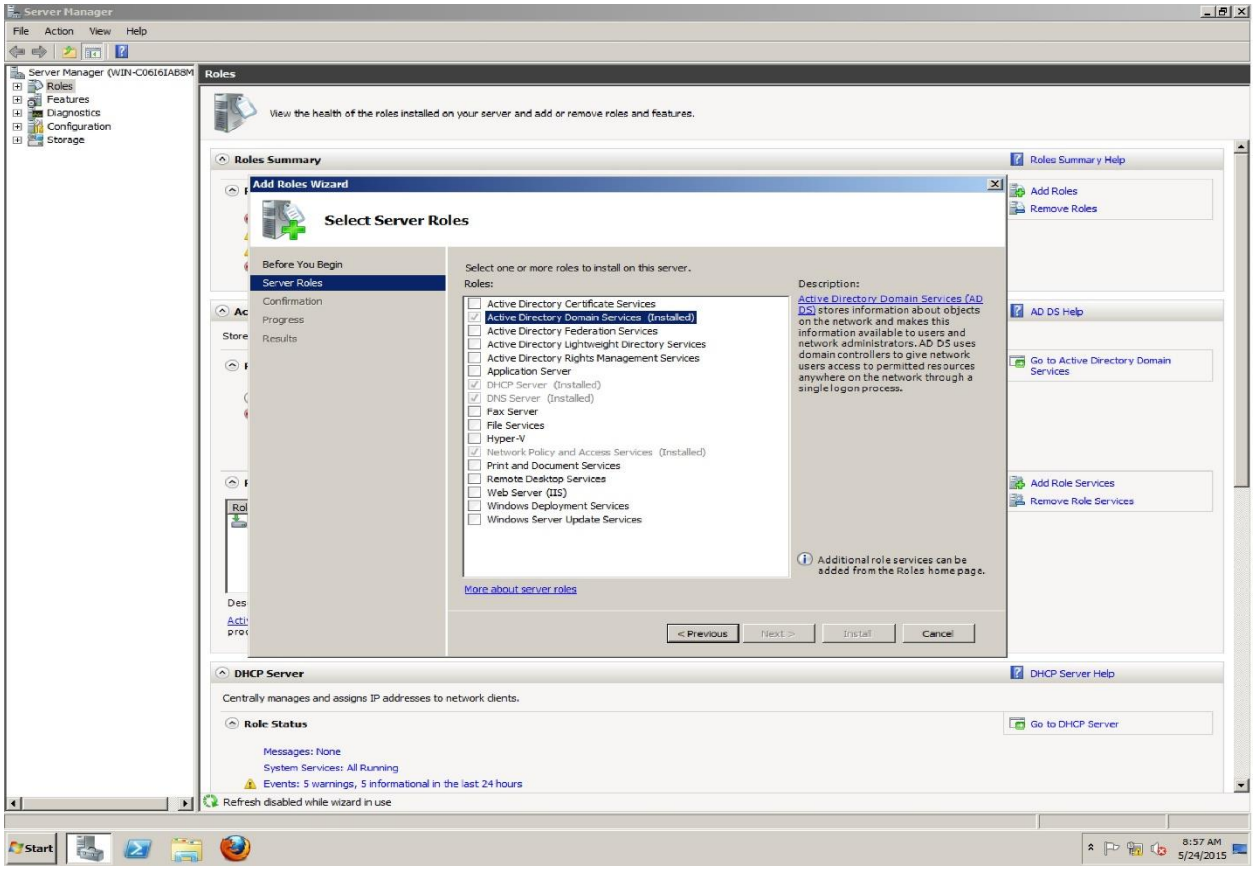

Figura 7. Vista de la herramienta administrativa Server Manager. En este caso se muestra el asistente para la instalación de roles. Nótese que los roles requeridos ya se encuentran instalados.

3.1.1 Instalación del Servidor FreeRADIUS.

FreeRADIUS puede ser configurado en una antigua torre de escritorio para servir en cualquier lugar, puede operar tanto en sistemas con recursos limitados atendiendo desde una docena o a unos cientos de usuarios, o puede ser instalado en los servidores apropiados para apoyar a millones de usuarios y peticiones. Actualmente incluye soporte para LDAP, SQL y otras bases de datos, así como EAP, EAP-TTLS y PEAP. Además de incluir soporte para todos los protocolos comunes de autenticación y bases de datos.[34]

En Ubuntu 12.04 se dispone de la última versión (ver figura 8) de FreeRADIUS de modo que puede ser instalada con facilidad. Se encuentra con una variedad de paquetes (ver

figura 9) que deben ser instalados solo los requeridos según las necesidades que se tengan.

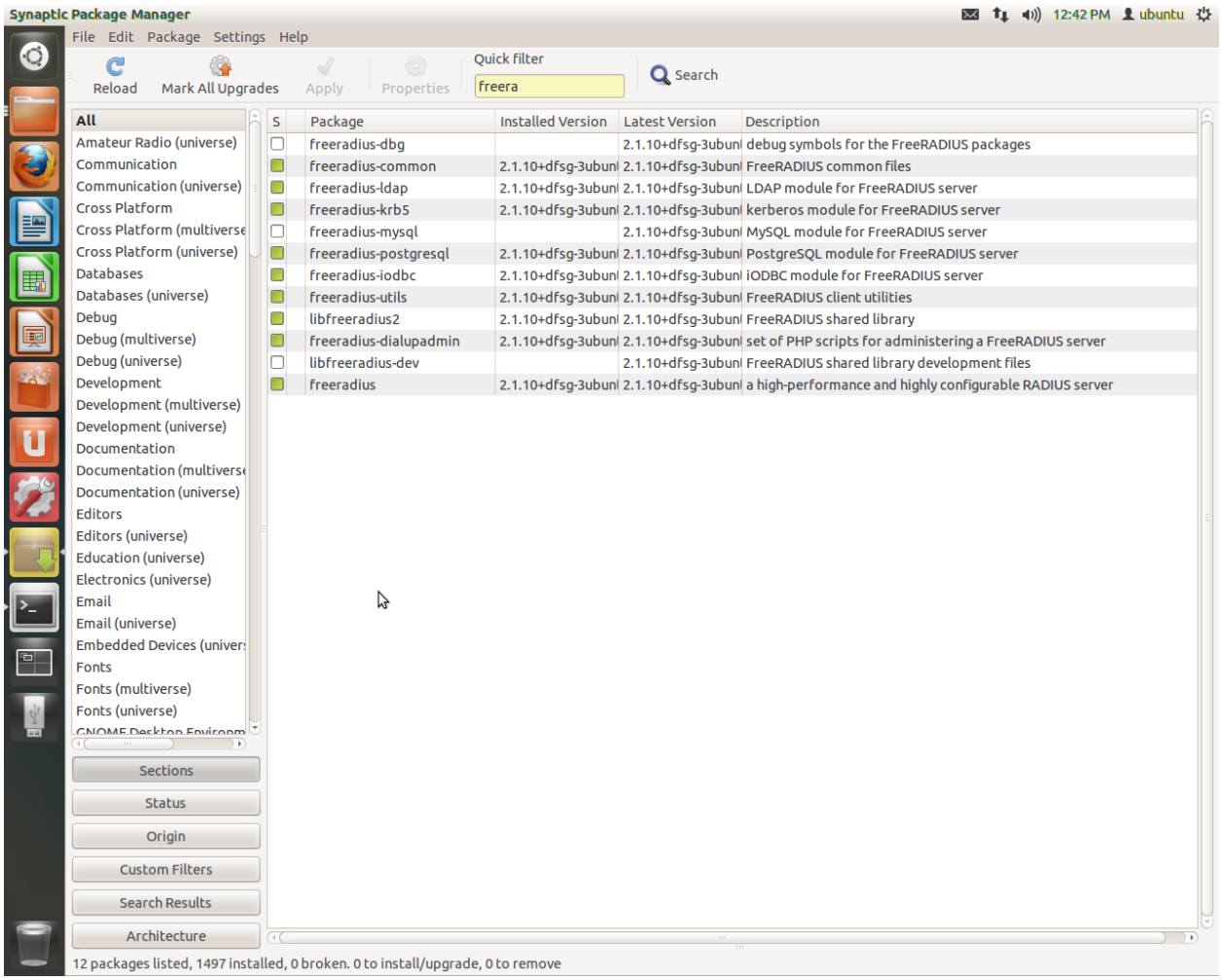

Figura 8. Ambiente gráfico (donde lo marcado en verde son los paquetes seleccionados para llevar a cabo la instalación del Servidor FreeRADIUS)

3.2 Instalación del Servidor de Base de Datos.

En Ubuntu se dispone de paquetes para varias versiones (ver figura 9) de PostgreSQL: desde la 7.4, 8.0, 8.1 y 8.2, 9.1 de modo que se instala la última versión a no ser que se necesite alguna anterior. Los paquetes necesarios para una instalación completa son los de la parte cliente (postgresql-client) y los de la parte servidor (postgresql). En el ordenador que se use como cliente sólo se necesitaran los paquetes del cliente. Es recomendable instalar un cliente gráfico que facilite la interacción con el servidor. En este caso se recomienda usar pgAdmin III.

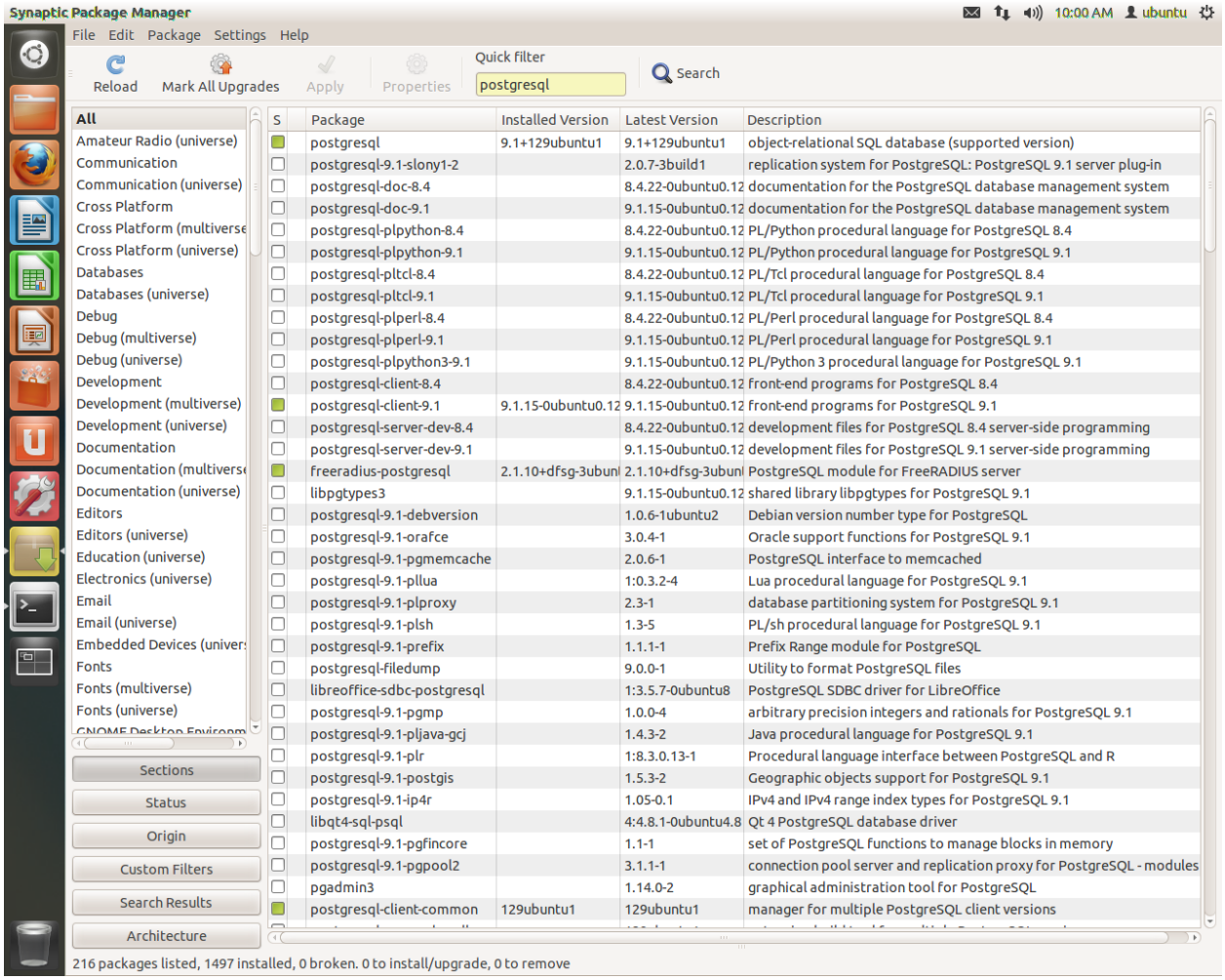

Figura 9. Ambiente gráfico (donde lo marcado en verde son los paquetes seleccionados para llevar a cabo la instalación de PostgreSQL)

3.3 Instalación del Servidor de Control de Acceso

En el caso del Servidor de Control de Acceso, no se llevará a cabo una instalación desde cero sino que se van a utilizar máquinas virtuales (VM) preinstaladas.

Para poder utilizar las VM es necesario un software de virtualización, en este caso las imágenes de las VM disponibles requieren de algún producto de VMware. Para las pruebas de laboratorio que se realizarán se utilizará VMware Workstation, sin embargo en un ambiente de producción donde se pretenda la virtualización de servidores se deben utilizar otros productos de la familia VMware [51]. No obstante, los fabricantes de PfSense, no recomiendan el uso de las VM en ambientes de producción debido a que sus productos son seguros cuando se ejecutan sobre una máquina real [52].

3.3.1Ejecución de la Máquina Virtual de PfSense.

Una vez instalado el software de virtualización, la VM se debe almacenar en una partición del disco duro de la PC en la cual está instalado el SO anfitrión (en este caso Windows Server 2008 R2), sobre el cual se instaló VMware Workstation.

Posteriormente se ejecuta el software de virtualización VMware Workstation, y se carga desde la consola de administración la VM de PfSense y se define el camino donde está almacenada la VM. En la figura 10 se muestran las características de la VM y la opción para la iniciar la ejecución de la misma.

Una vez iniciada la ejecución de la VM el SO invitado (guest) se carga sobre un entorno de hardware virtual. En la figura 10 se puede observar a PfSense (SO invitado) en ejecución sobre un entorno virtual proporcionado por VMware Workstation, que a su vez está ejecutándose sobre Windows Server 2008 R2 (SO anfitrión).

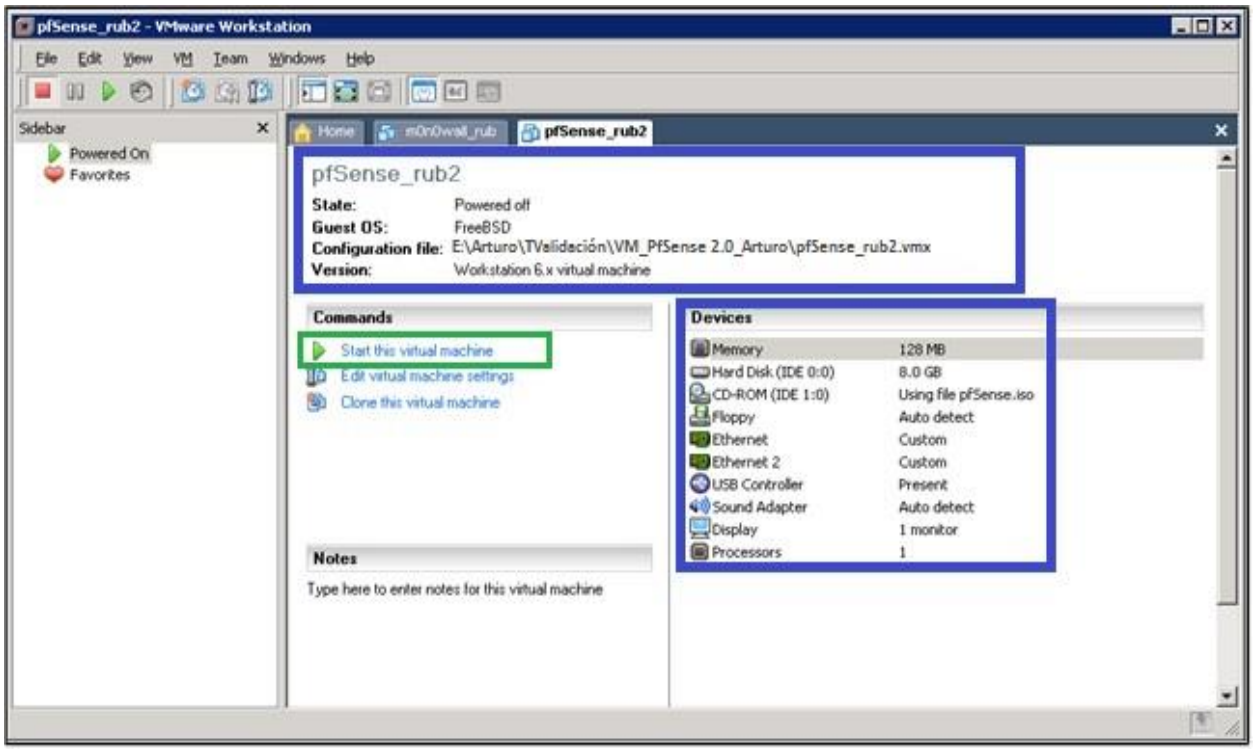

Figura 10. Características de la VM de PfSense y opción para iniciar la ejecución de la VM.

3.4 Implementación de la arquitectura propuesta a escala de laboratorio y configuración de los distintos módulos.

Una vez instalados los servidores de Dominio, Bases de Datos y Control de Acceso se puede proceder a implementar la arquitectura propuesta, en este caso a escala de

laboratorio. Primeramente se deben garantizar las conexiones de modo que se cumpla con la topología de la arquitectura tal y como se define en la figura 4. Posteriormente se deben configurar cada uno de los distintos módulos de la arquitectura para que cumplan con sus respectivas funciones.

3.4.1 Configuración de los Puntos de Acceso.

La configuración de los AP es bien sencilla y se realiza a través de una interfaz web. Dentro de los parámetros a configurar estan:

- Nombre del AP
- Dirección IP del AP
- Nombre de la red inalámbrica (SSID)
- Modo de operación
- Canal/frecuencia
- Razón de Datos
- Parámetros de seguridad-

En la tabla 3 se muestra la configuración de estos parámetros para los dos AP que serán utilizados en la implementación de la arquitectura. En el anexo C se pueden observar las capturas de pantalla correspondientes a la configuración de los distintos parámetros utilizando la interfaz Web de administración de los AP (figuras 28 a la 35).

Tabla 3. Configuración de los parámetros importantes en los Puntos de Acceso.

Parámetros	Red Inalámbrica para clientes Wi-Fi itinerantes	Red Inalámbrica para clientes Wi-Fi fijos situados en Departamentos y Laboratorios
Nombre del AP	AP-1	AP-2
Dirección IP	192.168.0.12	192.168.195.11
SSID	WLAN-1	WLAN-2
Modo de Operación	802.11 n	802.11 n

Canal/frecuencia	Canal 11 (2.462 GHz)	Canal 6 (2.437 GHz)
Razón de Datos	La mejor (best): - 54 Mbps para 802.11 n -	La mejor (best): - 54 Mbps para 802.11 n -
Autenticación de Red	Sistema abierto (Open system)	WPA/WPA2 Enterprise
Cifrado de datos	Ninguna	TKIP/AES
Servidor RADIUS	No	Si

3.4.2 Configuración del Servidor de Dominio.

La configuración del Servidor de Dominio presenta determinada complejidad debido a que hay que configurar varios roles. Dentro de los cuatro roles instalados en este servidor hay dos que son básicos y aunque forman parte de la propuesta no son el foco de atención de este trabajo. Debido a lo anterior a continuación se expone la configuración de los roles: Active Directory Domain Services y Network Policy and Access Services. No obstante en el anexo D se pueden observar las capturas de pantalla correspondientes a la configuración de los roles DHCP (figuras 36) y DNS (figuras 37).

I Definición de usuarios y grupos de usuarios

En el servicio Active Directory Users and Computer del rol Active Directory Domain Services se definen los usuarios y grupos de usuarios y equipos que tendrán acceso al dominio ucf-prueba.edu.cu. Los grupos se crean dentro del contenedor Users, estos se llamarán: WLAN-1_Users, WLAN-2_Users y WLAN-2_Computers respectivamente (ver figura 11).

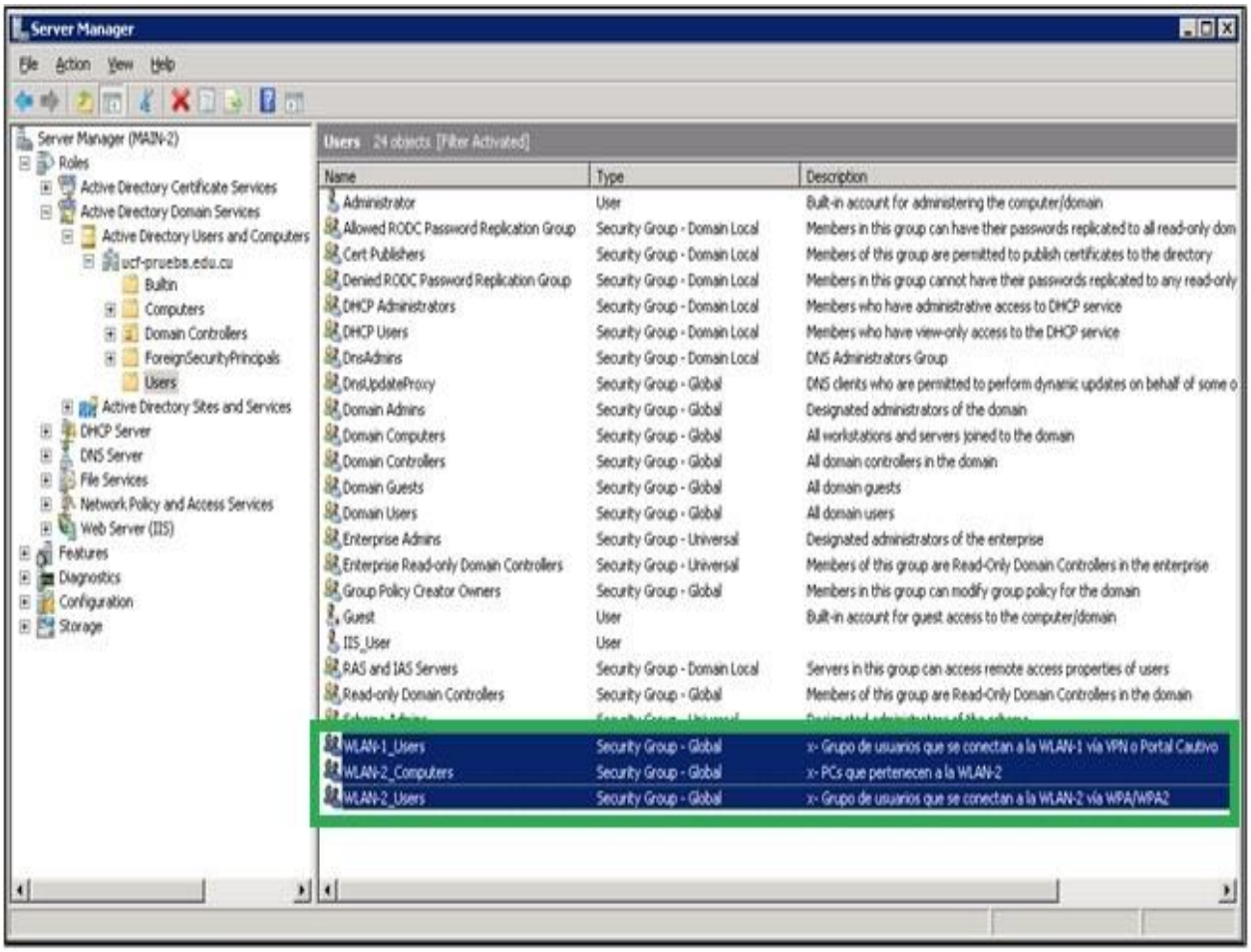

Figura 11. Definición de los grupos de usuarios WLAN-1_Users, WLAN-2_Users y WLAN-2_Computers.

Por último se deben crear tres usuarios: User_1, User_2 y User_3, los dos primeros pertenecerán al grupo WLAN-1_Users y el último a WLAN-2_Users (ver figura 12). Estos usuarios serán los que se utilizarán para probar los distintos métodos de acceso definidos en la arquitectura propuesta. En el caso del grupo WLAN-2_Computers a este pertenecerán todas las PC del dominio que formarán parte de la red WLAN-2.

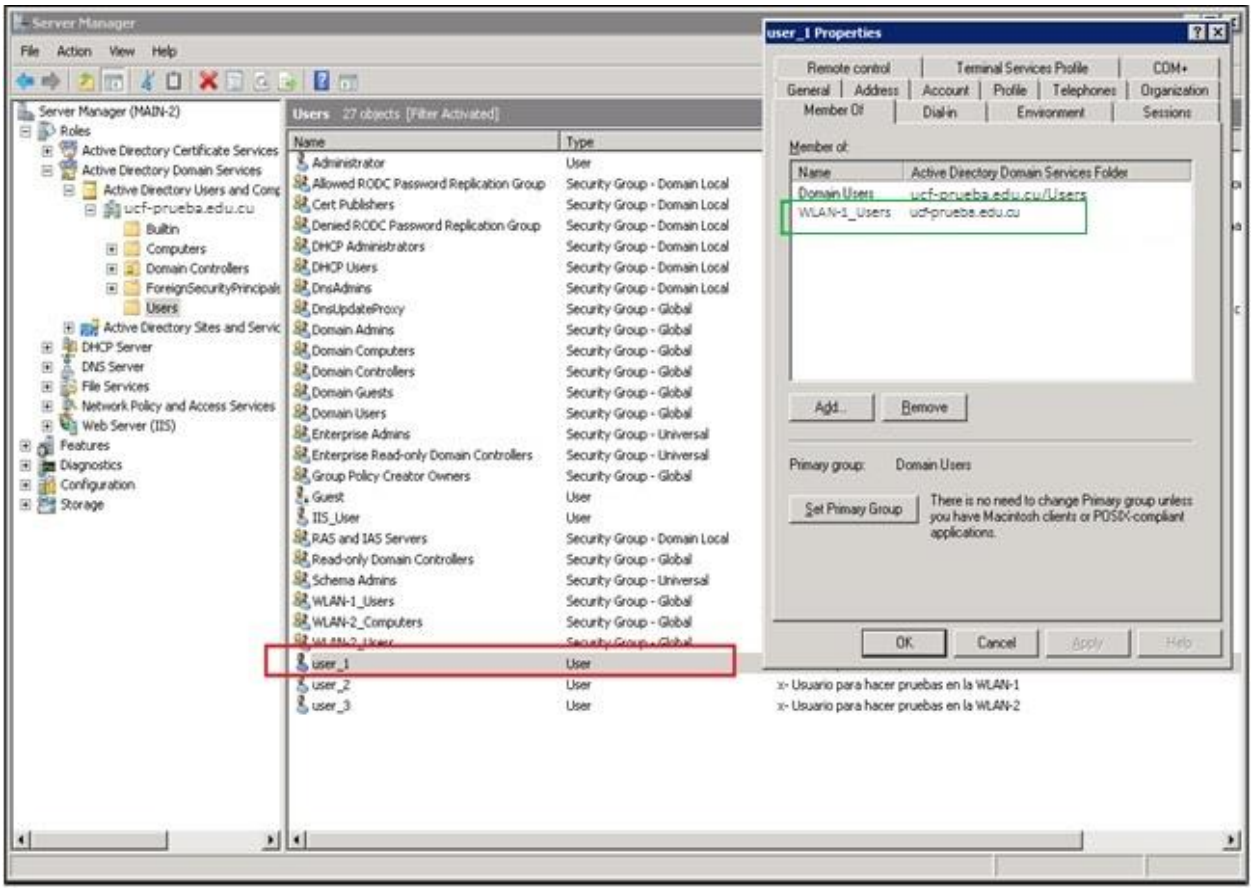

Figura 12. Definición de usuarios. En este caso se declara al usuario User_1miembro del grupo WLAN-1_Users.

II Definición de los usuarios RADIUS.

Los usuarios RADIUS se definen en la sección RADIUS Users del servicio NPS del rol Network Policy and Access Services. Los dos primeros corresponden a los servidores de Control de Acceso de PfSense. El tercer cliente corresponde al AP-2, el cual les brindará servicio a los clientes inalámbricos fijos de la WLAN-2.

III Definición de la política de conectividad

Las políticas de conectividad se definen permitiendo el acceso a la red a todos los equipos clientes, y los requisitos de autenticación y autorización para la conexión. Se puede utilizar NPS para gestionar de forma centralizada el acceso a la red a través de los puntos de acceso inalámbricos, servidores VPN, servidores de llamada bajo demanda (dial-in) y switches con autenticación basada en el protocolo 802.1x [53].

En este caso se definen las políticas correspondientes a los accesos inalámbricos a través de WPA/WPA2, PPTP VPN, OpenVPN, VPN IPsec y Portal Cautivo.

IV Definición del almacén de logs del servidor RADIUS

En el caso del almacenamiento de los logs (data logging) del servidor RADIUS se utilizará, según la arquitectura propuesta en el capítulo 2, un Servidor de Bases Datos PostgreSQL. Esta configuración debe realizarse posteriormente a que se cree la BD Radius_Accounting y se definan los permisos de usuario en el Servidor de Bases de Datos.

3.4.3 Configuración del Servidor de Bases de Datos.

En el Servidor de Bases de Datos se debe crear la BD que almacenará los logs del Servidor RADIUS. Esta va a llevar por nombre *Radius_Accounting* y tendrá acceso con permisos de propietario de la BD (*db_owner*), el usuario *user,* definido dentro del propio gestor de Base de Datos.

3.4.4 Configuración del Servidor de Control de Acceso.

I) Configuración de las interfaces LAN y WAN de PfSense

Antes de proceder a configurar los parámetros generales de PfSense se deben definir las asociaciones entre las redes virtuales (VMnet) y los adaptadores físicos de red (ver figura 12). Después se deben editar las propiedades de las interfaces de red de las VM para definir un puente entre las interfaces y las VMnet definidas anteriormente (ver figura 13 y 14)

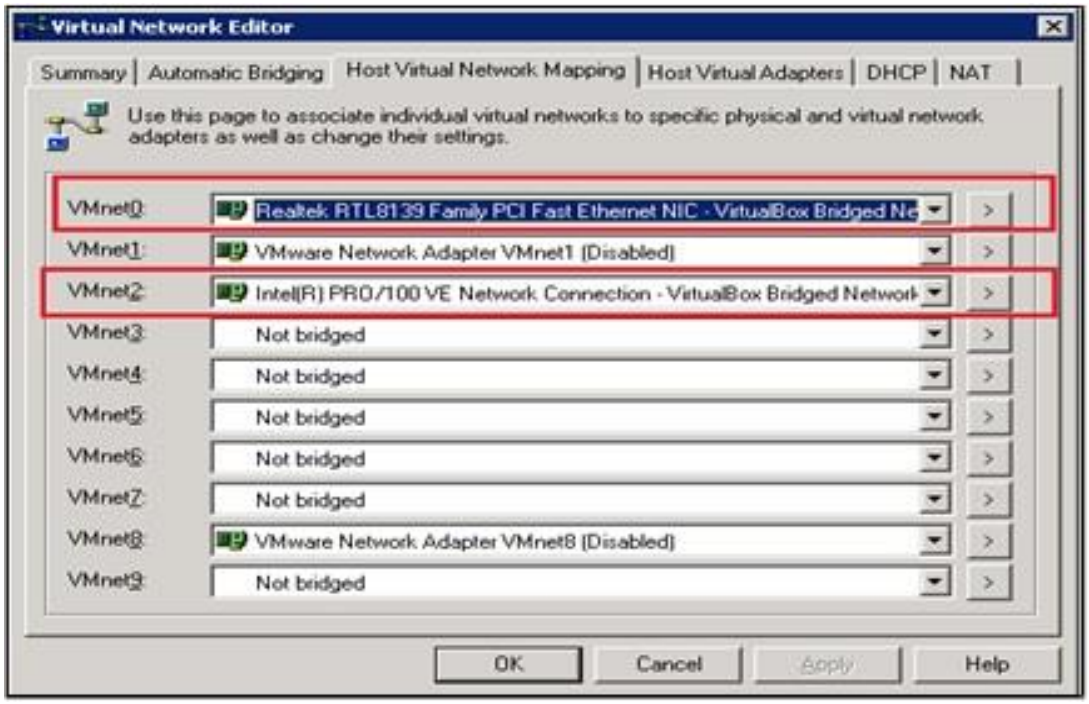

Figura 13. Asociación de las VMnet con los adaptadores físicos de red presentes en la PC donde corren las VM.

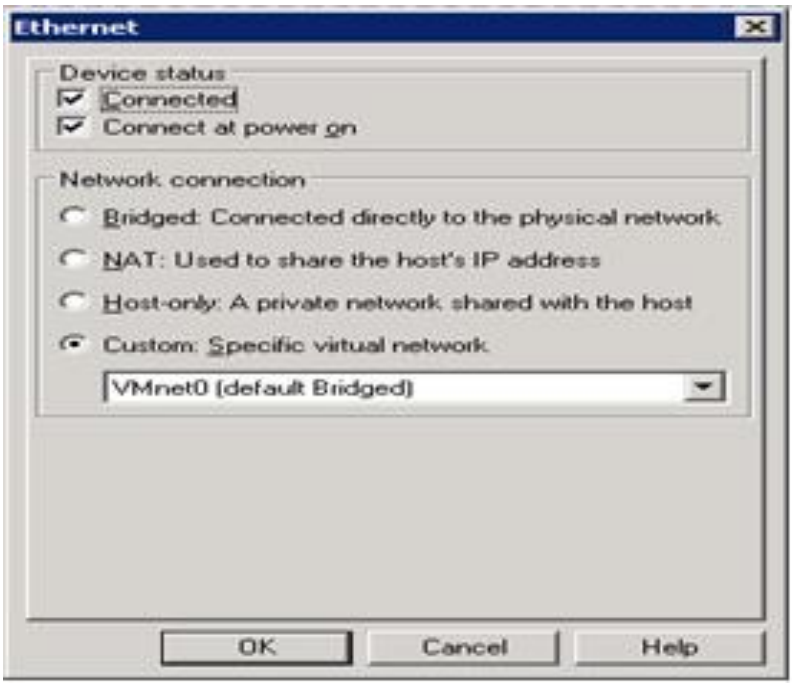

Figura 14. Interfaz Ethernet (LAN) se puentea con la VMnet0.

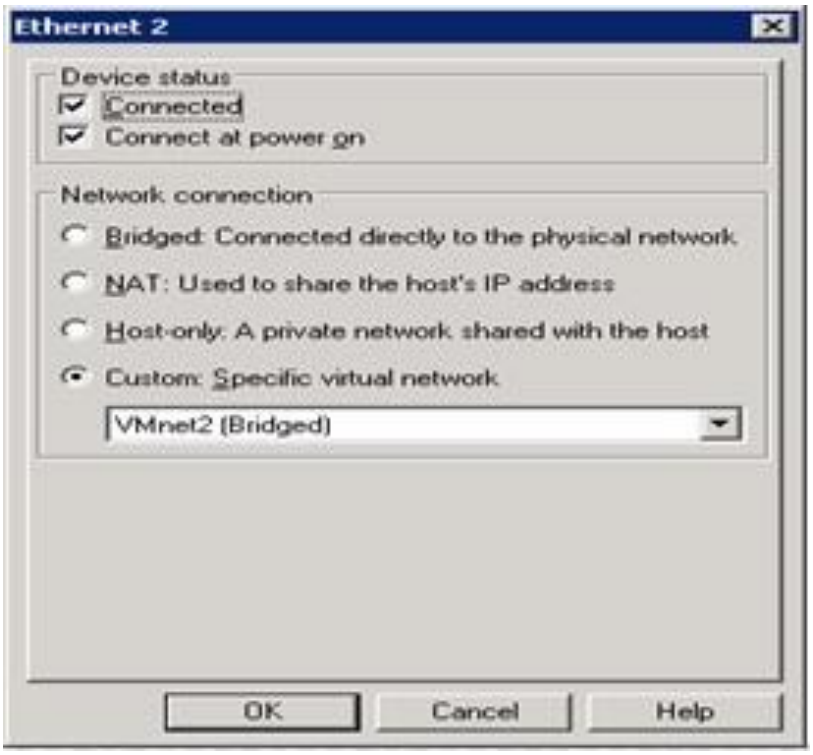

Figura 15. Interfaz Ethernet2 (WAN) se puentea con la VMnet2.

Posteriormente se ejecuta la VM y se le asigna una dirección IP a la interfaz LAN desde la consola. En este caso se asigna la IP 192.168.0.3 en PfSense. Una vez realizado esto ya se puede acceder a la herramienta Web de administración para terminar de configurar los parámetros de las interfaces de red. Se asigna la IP 192.168.195.14 en el caso de PfSense).

II) Configuración de los parámetros generales de PfSense

La configuración de los parámetros se realiza desde la herramienta Web, a la cual se accede de la siguiente forma: http://dirección_IP. Dentro de los parámetros que se definen está el nombre de host, el servidor de DNS, el servidor de tiempo, la autenticación segura vía https (figura 15).

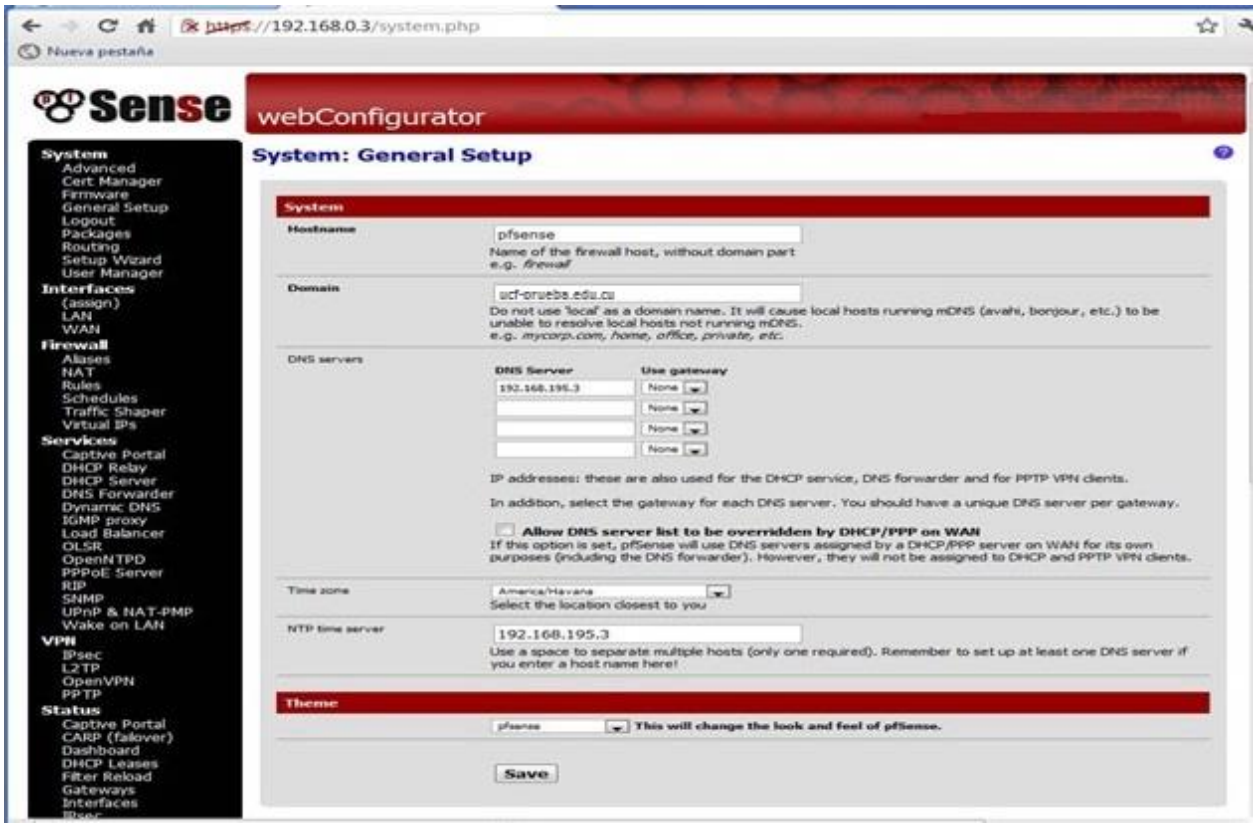

Figura 16. Herramienta Web de administración de PfSense.

III) Configuración del servidor de VPN PPTP

El servidor de VPN PPTP se implementa en PfSense, la configuración es bien similar. En la tabla 4 se pueden observar los parámetros básicos de la configuración de este servidor. En el anexo E se presentan las capturas de pantalla correspondientes a la configuración así como la regla en el Firewall necesaria para que los clientes puedan acceder a los recursos de la red corporativa.

Tabla 4. Configuración de los parámetros del servidor de VPN PPTP.

Parámetros	PfSense
Dirección del Servidor PPTP 192.168.04	192.168.04
Rango de Direcciones remotas	192.168.1.128/26
Uso de Radius	Si
Dirección de Servidor de RADIUS	192.168.195.3

Secreto compartido con el Servidor RADIUS	SecretTest
Fortaleza del Cifrado	128 bits

IV) Configuración del servidor de VPN IPsec

El servidor de VPN IPsec se implementa en PfSense, la configuración es detallada. En la tabla 5 se pueden observar los parámetros básicos de la configuración de este servidor.

Tabla 5. Configuración de los parámetros del servidor VPN IPsec.

Parámetros	PfSense
NAT-T	Activado
Fase 1	
Método de Autenticación	Clave precompartida
Modo de negociación	Agresivo
Algoritmo de cifrado	AES (256 bits)
Algoritmo hash	SHA1
Diffie Hellman key group	2 (1024 bits)
Fase 2	
Protocolo	ESP
Algoritmo de cifrado	3DES, Blowfish, CAST 128, AES
Algoritmo hash	SHA1
PFS key group	2 (1024 bits)

V) Configuración del servidor de OpenVPN

El servidor de OpenVPN se implementa solo en PfSense. En la tabla 6 se pueden observar los parámetros básicos de la configuración de este servidor. En el anexo G se presentan las capturas de pantalla correspondientes a la configuración así como la regla

necesaria en el Firewall. Tabla 6 Configuración de los parámetros del servidor de OpenVPN.

Tabla 6. Configuración de los parámetros del servidor de OpenVPN.

Parámetros	PfSense
Modo Servidor	Acceso Remoto (SSL/TLS + autenticación de usuarios)
Extremo para la autenticación	main-2.ucf-prueba.edu.cu (ver figura 47 del anexo G)
Protocolo	UDP
Modo del dispositivo	Tun
Interfaz	LAN
Puerto Local	1194
Autenticación TLS	Habilitada
Autoridad certificadora	Test_CA (ver figura 48 del anexo G)
Certificado del Servidor	Certificate_Server
Longitud de los parámetros Diffie Hellman	1024 bits
Algoritmo de cifrado	AES-128-CBC (128 bits)
Red para los túneles	192.168.3.0/24

VI) Configuración del Portal Cautivo

El Portal Cautivo se implementa en PfSense. En la tabla 7 se pueden observar los parámetros básicos de la configuración.

Tabla 7. Configuración de los parámetros del Portal Cautivo.

Parámetros	PfSense
Interfaz	LAN
Ventana popup de desconexión	Habilitada
URL de redirección (página a la que se redirige el usuario una vez sea autenticado)	Habilitada (Puede ser cualquier página Ej: www.google.com)
Autenticación	FreeRADIUS
IP del Servidor RADIUS	192.168.195.3
Puerto para la autenticación	1812
Secreto compartido con el Servidor FreeRADIUS	SecretTest
Contabilidad	Habilitada
Puerto para la contabilidad	1813
Servidor http	192.168.0.3
Certificado https	Se copia el certificado x.509 en formato PEM en el cuadro de texto. (por comodidad se utiliza el mismo certificado utilizado por el servidor de OpenVPN)
Llave privada para https	Se copia la llave privada RSA en formato PEM en el cuadro de texto. (por comodidad se utiliza la misma llave utilizada por el servidor de OpenVPN)
Contenido de la Página del Portal	código HTML

Contenido de la Página de Error	código HTML

3.4.5 Pruebas de conectividad de los clientes Wi-Fi.

Las pruebas de conectividad se realizaron utilizando todos los métodos de acceso comprendidos en la arquitectura propuesta. En la tabla 8 se pueden observar las características de los clientes Wi-Fi que se utilizaron en las pruebas, en función del método de acceso empleado. En el anexo I se muestran las capturas de pantalla correspondientes a varias de las pruebas realizadas.

Tabla 8. Características de los clientes Wi-Fi según el método de acceso empleado. Método.

Método de Acceso	Software Cliente	Plataforma	SO
WPA/WPA2	Nativo	Windows	Windows XP SP3 Professional Windows 7 Enterprise
		Linux	Ubuntu 10.04 LTS
VPN PPTP	Nativo	Windows	Windows XP SP3 Professional Windows 7 Enterprise
		Android	Android 1.6
VPN IPSec	Shrew Soft VPN Client	Windows	Windows XP SP3 Professional Windows 7 Enterprise

OpenVPN	OpenVPN Client	Windows	Windows XP SP3 Professional Windows 7 Enterprise
Portal Cautivo	Navegador web estándar	Windows	Windows XP SP3 Professional Windows 7 Enterprise
		Linux	Ubuntu 10.04 LTS
		Android	Android 1.6

3.5 Conclusiones parciales.

Para las pruebas se implementó la arquitectura propuesta a escala de laboratorio. Se instaló y configuró el Servidor de Dominio Windows 2008 R2 y el Servidor de Bases de Datos PostgreSQL. En el caso del Servidor de Control de Acceso se ejecutó PfSense sobre las máquinas virtuales preinstaladas que se ejecutan sobre el software de virtualización VMware Workstation. Las pruebas de conectividad de los clientes Wi-Fi fueron satisfactorias, tanto para el acceso a la WLAN-1 como a la WLAN-2.

Conclusiones

Al culminar este trabajo se puede concluir lo siguiente:

- Se evaluaron los mecanismos de control de acceso a las redes WLAN, desde los específicos de estas redes como WEP, WPA y WPA2 hasta otros de amplia utilización en otro tipos de redes tales como las VPN de acceso remoto de capa 2 y 3 (PPTP, L2TP, IPSEC, OpenVPN), así como mecanismos de capas superiores como SSL/TLS. La aplicación de estos mecanismos varía según el nivel de seguridad requerido, el tipo de servicio deseado y el coste de gestión y mantenimiento de las soluciones.
- Se seleccionaron los mecanismos adecuados para el control de acceso a la Red WLAN de la UCF, teniendo en cuenta que se trató de permitir conectividad a la mayor cantidad de dispositivos, siempre que soporten el estándar Wi-Fi y a su vez garantizar una seguridad adecuada, en dependencia del tipo de usuario y dispositivo que se conectan a la red inalámbrica. En el caso de las estaciones de trabajo con interfaces de red inalámbricas se seleccionó a WPA/WPA2 modo empresarial, utilizando EAP protegido (PEAP) y contraseñas MSCHAPv2. En el caso de los clientes Wi-Fi móviles se seleccionaron los métodos Portal Cautivo y VPN de acceso remoto, tanto de capa 2 como de capa 3.
- Se diseñó una arquitectura para el control de acceso de la red WLAN de la UCF. La misma comprende dos redes WLAN separadas, una primera (WLAN-1) para clientes Wi-Fi móviles tales como Laptops, Notebooks, PDA, Smartphone, Tablet y otra (WLAN-2) para las estaciones de trabajo con interfaces de red inalámbrica IEEE 802.11 n situadas en departamentos, laboratorios. En el caso de la WLAN-1 se propuso un Servidor de Control de Acceso que implemente un Portal Cautivo así como servidores de VPN (PPTP, IPsec y OpenVPN).
- Se evaluó la arquitectura mediante pruebas de laboratorio. Para ello se instaló y configuró un Servidor de Dominio Windows Server 2008 R2 con los roles de Active Directory, DNS, DHCP y se instaló además un Servidor FreeRADIUS. También se instaló y configuró un servidor de Bases de Datos PostgreSQL para almacenar los registros del servidor FreeRADIUS. En el caso del Servidor de Control de Acceso se instaló PfSense, derivado del Sistema Operativo FreeBSD. Por último se configuraron los distintos servicios y funcionalidades, se evaluó la arquitectura a

través de pruebas de conectividad desde clientes de varias plataformas (Windows, Linux y Android) utilizando los métodos de acceso que comprende la arquitectura propuesta.

Recomendaciones

Para trabajos futuros se recomienda:

1. Validar la arquitectura propuesta mediante pruebas de campo.
2. Realizar pruebas con clientes Wi-Fi móviles de otras plataformas (Mac, iPhone, iPad, BlackBerry, Nokia).

Referencias Bibliográficas

[1] Izaskun Pellejero, Amaia Lesta, y Fernando Andreu, «Fundamentos y aplicaciones de seguridad en Redes WLAN». 2006.

[2] J. B. C. Manuel Álvarez Campana, Francisco González Vidal, Raquel Pérez Leal, Isabel Román Martínez, y Enrique Vázquez Gallo, «Tecnologías de Banda Ancha y Convergencia de Redes». Gobierno de España, Ministerio de Industria, Turismo y Comercio. Secretaría de Estado de Telecomunicaciones, 2010.

[3] Guillaume Lehembre, «Seguridad Wi-Fi – WEP, WPA y WPA2», *Rev. Hakin9*, vol. 1/2006, feb. 2015.

[4] Klaus Romanek, Psiber Data GmbH, y Krailling, «Diseño y Planificación Profesional de Redes Inalámbricas», jun-2008.

[5] Rafael A. Hernández Espinosa, «Reflexiones sobre el uso del Software Libre en Cuba. Ventajas - Monografias.com», ago-2014. [En línea]. Disponible en: file:///D:/Tesis%20Redes/23-04-2015(Software%20Libre)/Reflexiones%20sobre%20el%20uso%20del%20Software%20Libre%20en%20Cuba.%20Ventajas%20-%20Monografias.com.htm. [Accedido: 21-may-2015].

[6] Cubadebate, «Promueve Cuba uso de software libre para garantizar soberanía tecnológica | Cubadebate», 21-mar-2013. [En línea]. Disponible en: file:///D:/Tesis%20Redes/23-04-2015(Software%20Libre)/Promueve%20Cuba%20uso%20de%20software%20libre%20para%20garantizar%20soberan%C3%ADa%20tecnol%C3%B3gica%20_%20Cubadebate.htm. [Accedido: 21-may-2015].

[7] Inter Press Service en Cuba, «Cuba y el software libre | Inter Press Service en Cuba», 22-abr-2015. [En línea]. Disponible en: file:///D:/Tesis%20Redes/23-04-2015(Software%20Libre)/Cuba%20y%20el%20software%20libre%20_%20Inter%20Press%20Service%20en%20Cuba.htm. [Accedido: 21-may-2015].

[8] Juan Manuel Castellanos Hernández, Jansel Leyva Bravo, y Yilena Abrahantes Hurtado, «Implementación de una red inalámbrica en la Universidad de Cienfuegos». 31-ene-2014.

[9] Izaskun Pellejer, Amaia Lesta, y Fernando Andreu, «Seguridad en redes WLAN». 2008.

[10] J. B. C. Manuel Álvarez Campana, Francisco González Vidal, Raquel Pérez Leal, Isabel Román Martínez, y Enrique Vázquez Gallo, «Tecnologías de Banda Ancha y Convergencia de Redes». Gobierno de España, Ministerio de Industria, Turismo y Comercio. Secretaría de Estado de Telecomunicaciones, 2010.

[11] Carlos Navarrete Chávez, «Evaluación de la tecnología IEEE802.11n con la plataforma OPNET». Universidad Politécnica de Catalunya, 14-oct-2009.

[12] Stefan Mangold, Sunghyun Choi, y Peter May, «IEEE 802.11e Wireless LAN for Quality of Service».

[13] Rubersy Ramos García, «Arquitectura para el Control de Acceso de la Red inalámbrica local de la Universidad Central "Marta Abreu" de Las Villas», Universidad Central «Marta Abreu» de Las Villas, Santa Clara, 2011.

[14] Cybercom, «Redes LAN Inalámbricas (Wireless LAN)». Perú, 06-mar-2015.

[15] Rodrigo Castro, «Avanzando en la seguridad de las redes WIFI», sep. 2005.

[16] Guillaume Lehembre, «Seguridad Wi-Fi – WEP, WPA y WPA2», *Rev. Hakin9*, vol. 1/2006.

[17] Wi-Fi Alliance®, «WPA™ Deployment Guidelines for Public Access Wi-Fi® Networks». 28-oct-2004.

[18] Wi-Fi Alliance®, «Wi-Fi CERTIFIED™ WPA2® Delivers Advanced Security to Homes, Enterprises and Mobile Devices». sep-2009.

[19] Rodrigo Castro, «Avanzando en la seguridad de las redes WIFI», p. 10, sep. 2005.

[20] Saulo Barajas, «Protocolos de seguridad en redes inalámbricas», Universidad Carlos III de Madrid, 06-mar-2015.

[21] CISCO, «¿Cómo el RADIUS trabaja?», p. 2, 25-dic-2014.

[22] C. Rigney Livingston, «RFC 2866 RADIUS Accounting». Network Working Group, jun-2000.

[23] C. Rigney Livingston, A. Rubens Merit, W. Simpson Daydreamer, y S. Willens Livingston, «RFC 2138 Remote Authentication Dial In User Service(RADIUS)». abr-1997.

[24] Néstor Gabriel Forero Saboya, «Taxonomia-de-los-Servidores-AAA-Radius-Diameter-y-TACACS», p. 9, nov. 2009.

[25] C. Rigney, S. Willens, A. Rubens, y W. Simpson, «RFC 2856 Remote Authentication Dial In User Service (RADIUS)». jun-2000.

[26] Emilio José Mira Alfaro, «RADIUS en Linux y Cisco», p. 10, ago. 2001.

[27] Nuttsy Aurora Lazo García, «DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN Y WLAN CON SISTEMA DE CONTROL DE ACCESO MEDIANTE SERVIDORES AAA». jul-2012.

[28] P. Calhoun, J. Loughney, Nokia, E. Guttman, Sun Microsystems, Inc., G. Zorn, Cisco Systems, Inc., J. Arkko, y Ericsson, «RFC 3588 - Diameter Base Protocol», sep-2003. [En línea]. Disponible en: file:///G:/Download%20Tesis/freeDiameter/RFC%203588%20-%20Diameter%20Base%20Protocol.htm. [Accedido: 21-may-2015].

[29] «RFC 5719 - Updated IANA Considerations for Diameter Command Code Allocations». [En línea]. Disponible en: file:///G:/Download%20Tesis/freeDiameter/RFC%205719%20-%20Updated%20IANA%20Considerations%20for%20Diameter%20Command%20Code%20Allocations.htm. [Accedido: 21-may-2015].

[30] V. Fajardo, Ed., Telcordia Technologies, J. Arkko, Ericsson Research, J. Loughney, Nokia Research Center, G. Zorn, Ed., y Network Zen, «RFC 6733 - Diameter Base Protocol», oct-2012. [En línea]. Disponible en: file:///G:/Biblio/freeDiameter/RFC%206733%20-%20Diameter%20Base%20Protocol.htm. [Accedido: 21-may-2015].

[31] Mariana Atopo y Jesús Jiménez, «Software libre y software propietario». jul-2011.

[32] Beatriz Silverio Espinosa, «Importancia de la Migración a Linux | Revista Tino», 14-nov-2012. [En línea]. Disponible en: file:///D:/Tesis%20Redes/23-04-2015(Software%20Libre)/Importancia%20de%20la%20Migraci%C3%B3n%20a%20Linux%20_%20Revista%20Tino.htm. [Accedido: 21-may-2015].

[33] Dirk van der Wal, *FreeRADIUS Beginner's Guide*. Packt Publishing Ltd. Livery Place 35 Livery Street Birmingham B3 2PB, UK., 2011.

[34] Wenche Backman-Kamila (, Tuukka Vainio, Miika Räisänen, y Thomas Backa, «FreeRADIUS Database Connection», p. 18, ene. 2013.

[35] Vergara, P.F.G., «Arquitectura Unificada para Control de Acceso en Redes Inalámbricas Seguras». 2007.

[36] NETGEAR, «ProSafe Wireless-N Access Point WNAP320». 26-ene-2011.

[37] Guillermo Galvan, «Instalacion de Pfsense», 12-dic-2010.

[38] Aura Cárdenas, Alexander Galvis, Jonattan Ospina, y Roger Perez, «pfsense firewall». [En línea]. Disponible en: file:///D:/Tesis%20Redes/Yasel/pfsense%20firewall.htm. [Accedido: 21-may-2015].

[39] ANA KATERINE MONTESINOS GELVEZ, «INSTALACION Y CONFIGURACION DE SISTEMA PERIMETRAL: “ZEROSHELL”.» 2013.

[40] David Omar Guevara Aulestia, «Autenticación de Redes Inalámbricas usando chillispot.» 2012.

[41] Francisco R. Santonja Rodilla, «Implementación de una Red Privada Virtual en Linux». 2005-2004.

[42] Jovana Palibrk, Ivan Ivanović, y Dušan Pajin, «The Implementation of the AMRES VPN Service». Produced by the AMRES-led working group on Security, mar-2013.

[43] Juan José Tomás Cánovas, «Servicio VPN de acceso remoto basado en SSL mediante OpenVPN». oct-2008.

[44] Cristina Gil Álvaro, «Servidor de túneles para el establecimiento de redes privadas virtuales punto a punto mediante OpenVPN». Proyecto de Sistemas Informáticos Facultad de Informática Universidad Complutense de Madrid, 2011-2010.

[45] Paul Gerard Porter, «Configuring FreeRADIUS for LDAP over SSL Authentication», *Cisco CCNP and CCSP*, 2015. [En línea]. Disponible en: file:///G:/InstalacionFreeradius/Configuring%20FreeRADIUS%20for%20LDAP%20over%20SSL%20Authentication%20_%20Paul%20Gerard%20Porter.htm. [Accedido: 23-may-2015].

[46] GLADIS SOFÍA ASADOVAY LEMA y LILIANA MERCEDES CAIZA ORTIZ, «ANÁLISIS COMPARATIVO DE SERVIDORES DE AUTENTIFICACIÓN RADIUS Y LDAP CON EL USO DE CERTIFICADOS DIGITALES PARA MEJORAR LA SEGURIDAD EN EL CONTROL DE ACCESO A REDES WIFI». 2013.

[47] Alfonso Celestino Martínez, «Implementaciones de seguridad en redes inalámbricas. Caso Práctico: RIU», Universidad Nacional Autónoma de México, 2009.

[48] C. Rigney Livingston, «RFC 2139 RADIUS Accounting». abr-1997.

[49] Daniel Pecos Martínez, «PostGreSQL vs. MySQL», p. 5.

[50] MicrosoftTechnet, «Windows Server 2008 y Windows Server 2008 R2.», 03-oct-2011. [En línea]. Disponible en: http://technet.microsoft.com/es-es/library/dd349801(WS.10).aspx.

[51] VMware, «Productos de VMware». [En línea]. Disponible en: http://vmware.ie/lasp/products/.

[52] BSD_Perimeter_LLC., «Installing pfSense in VMware under Windows.», 2009. [En línea]. Disponible en: http://doc.pfsense.org/index.php/Installing_pfSense_in_VMware_under_Windows.

[53] Microsoft., «Acceso a red y Políticas. Roles y Tecnologías de Windows Server 2008: Servicios de Red y Accesos.», 2011. [En línea]. Disponible en: http://www.microsoft.com/spain/windowsserver2008/roles/apps_ras.mspx.

Bibliografía

[1]Hernández Oliveros Ricardo y Pérez Reyes Oscar Alberto, «802.11 N APLICACIONES DE ÚLTIMA GENERACIÓN». 2008.

[2]Microsoft., «Acceso a red y Políticas. Roles y Tecnologías de Windows Server 2008: Servicios de Red y Accesos.», 2011. [En línea]. Disponible en: http://www.microsoft.com/spain/windowsserver2008/roles/apps_ras.mspx.

[3]Novell, Inc., «Administration Guide Integrating Novell eDirectory with FreeRADIUS». ene-2011.

[4]GLADIS SOFÍA ASADOVAY LEMA y LILIANA MERCEDES CAIZA ORTIZ, «ANÁLISIS COMPARATIVO DE SERVIDORES DE AUTENTIFICACIÓN RADIUS Y LDAP CON EL USO DE CERTIFICADOS DIGITALES PARA MEJORAR LA SEGURIDAD EN EL CONTROL DE ACCESO A REDES WIFI». 2013.

[5]Vergara, P.F.G., «Arquitectura Unificada para Control de Acceso en Redes Inalámbricas Seguras». 2007.

[6]David Omar Guevara Aulestia, «Autenticación de Redes Inalámbricas usando chillispot.» 2012.

[7]Rodrigo Castro, «Avanzando en la seguridad de las redes WIFI», p. 10, sep. 2005.

[8]CISCO, «¿Cómo el RADIUS trabaja?», p. 2, 25-dic-2014.

[9]«Comprendiendo PPTP y VPN». [En línea]. Disponible en: file:///D:/Tesis%20Redes/Nueva%20carpeta/Comprendiendo%20PPTP%20y%20VPN.htm. [Accedido: 21-may-2015].

[10]Joel Barrios Dueñas, «Configuración básica de Freeradius con soporte de LDAP.», 06-mar-2015. [En línea]. Disponible en: http://www.alcancelibre.org/staticpages/index.php/como-freeradius-basico. [Accedido: 06-mar-2015].

[11]Paul Gerard Porter, «Configuring FreeRADIUS for LDAP over SSL Authentication», Cisco CCNP and CCSP, 2015. [En línea]. Disponible en: file:///G:/InstalacionFreeradius/Configuring%20FreeRADIUS%20for%20LDAP%20over

%20SSL%20Authentication%20_%20Paul%20Gerard%20Porter.htm. [Accedido: 23-may-2015].

[12]Inter Press Service en Cuba, «Cuba y el software libre | Inter Press Service en Cuba», 22-abr-2015. [En línea]. Disponible en: file:///D:/Tesis%20Redes/23-04-2015(Software%20Libre)/Cuba%20y%20el%20software%20libre%20_%20Inter%20Press%20Service%20en%20Cuba.htm. [Accedido: 21-may-2015].

[13]Nuttsy Aurora Lazo García, «DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN Y WLAN CON SISTEMA DE CONTROL DE ACCESO MEDIANTE SERVIDORES AAA». jul-2012.

[14]Klaus Romanek, Psiber Data GmbH, y Krailling, «Diseño y Planificación Profesional de Redes Inalámbricas», jun-2008.

[15]«Diseño y Planificación Profesional de Redes Inalámbricas.pdf». .

[16]Luis de Zayas Buigas y Augusto Sao Avilés, «Elementos conceptuales básicos útiles para comprender las redes de telecomunicación», ACIMED v.10 n.6, 2002.

[17]Yurisander Guevara, «El Software Libre llega a los “ta” - Informática - Suplementos - Juventud Rebelde - Diario de la juventud cubana», 22-abr-2015. [En línea]. Disponible en: file:///D:/Tesis%20Redes/23-04-2015(Software%20Libre)/El%20Software%20Libre%20llega%20a%20los%20%C2%ABta%C2%BB%20-%20Inform%C3%A1tica%20-%20Suplementos%20-%20Juventud%20Rebelde%20-%20Diario%20de%20la%20juventud%20cubana.htm. [Accedido: 21-may-2015].

[18]Wi-Fi Alliance, «Enabling the Future of Wi-Fi® Public Access». Wi-Fi Alliance, feb-2005.

[19]Carlos Navarrete Chávez, «Evaluación de la tecnología IEEE802.11n con la plataforma OPNET». Universidad Politécnica de Catalunya, 14-oct-2009.

[20]Dirk van der Wal, FreeRADIUS Beginner’s Guide. Packt Publishing Ltd. Livery Place 35 Livery Street Birmingham B3 2PB, UK., 2011.

[21]Wenche Backman-Kamila (, Tuukka Vainio, Miika Räisänen, y Thomas Backa, «FreeRADIUS Database Connection», p. 18, ene. 2013.

[22]Izaskun Pellejero, Amaia Lesta, y Fernando Andreu, «Fundamentos y aplicaciones de seguridad en Redes WLAN». 2006.

[23]Center for History and New Media, «Guía rápida». [En línea]. Disponible en: http://zotero.org/support/quick_start_guide.

[24]Stefan Mangold, Sunghyun Choi, y Peter May, «IEEE 802.11e Wireless LAN for Quality of Service».

[25]Juan Manuel Castellanos Hernández, Jansel Leyva Bravo, y Yilena Abrahantes Hurtado, «Implementación de una red inalámbrica en la Universidad de Cienfuegos». 31-ene-2014.

[26]Francisco R. Santonja Rodilla, «Implementación de una Red Privada Virtual en Linux». 2005-2004.

[27]A. V. Velásquez, S, Castro, B, y Velandia, A, «Implementación de un servidor de autenticación Radius en un ambiente de pruebas para la red inalámbrica de la UPB – Sede Laureles», Universidad Pontificia Bolivariana. Medellín, Colombia.

[28]Alfonso Celestino Martínez, «Implementaciones de seguridad en redes inalámbricas. Caso Práctico: RIU», Universidad Nacional Autónoma de México, 2009.

[29]Beatriz Silverio Espinosa, «Importancia de la Migración a Linux | Revista Tino», 14-nov-2012. [En línea]. Disponible en: file:///D:/Tesis%20Redes/23-04-2015(Software%20Libre)/Importancia%20de%20la%20Migraci%C3%B3n%20a%20Linux%20_%20Revista%20Tino.htm. [Accedido: 21-may-2015].

[30]Guillermo Galvan, «Instalacion de Pfsense», 12-dic-2010.

[31]ANA KATERINE MONTESINOS GELVEZ, «INSTALACION Y CONFIGURACION DE SISTEMA PERIMETRAL: “ZEROSHELL”.» 2013.

[32]BSD_Perimeter_LLC., «Installing pfSense in VMware under Windows.», 2009. [En línea]. Disponible en: http://doc.pfsense.org/index.php/Installing_pfSense_in_VMware_under_Windows.

[33]Microsoft, «Microsoft Server 2008 R2 Overview.», 21-sep-2011. [En línea]. Disponible en: http://www.microsoft.com/sqlserver/en/us/product-info/overview-capabilities.aspx.

[34]Aura Cárdenas, Alexander Galvis, Jonattan Ospina, y Roger Perez, «pfsense firewall». [En línea]. Disponible en: file:///D:/Tesis%20Redes/Yasel/pfsense%20firewall.htm. [Accedido: 21-may-2015].

[35]Daniel Pecos Martínez, «PostGreSQL vs. MySQL», p. 5.

[36]VMware, «Productos de VMware». [En línea]. Disponible en: http://vmware.ie/lasp/products/.

[37]Cubadebate, «Promueve Cuba uso de software libre para garantizar soberanía tecnológica | Cubadebate», 21-mar-2013. [En línea]. Disponible en: file:///D:/Tesis%20Redes/23-04-2015(Software%20Libre)/Promueve%20Cuba%20uso%20de%20software%20libre%20para%20garantizar%20soberan%C3%ADa%20tecnol%C3%B3gica%20_%20Cubadebate.htm. [Accedido: 21-may-2015].

[38]NETGEAR, «ProSafe Wireless-N Access Point WNAP320». 26-ene-2011.

[39]Saulo Barajas, «Protocolos de seguridad en redes inalámbricas», Universidad Carlos III de Madrid, 06-mar-2015.

[40]Alfonso Miñarro López, «Radius: Mecanismo de seguridad en accesos desde movilidad», Telefónica España, dic-2009.

[41]Cybercom, «Redes LAN Inalámbricas (Wireless LAN)». Perú, 06-mar-2015.

[42]Rafael A. Hernández Espinosa, «Reflexiones sobre el uso del Software Libre en Cuba. Ventajas - Monografias.com», ago-2014. [En línea]. Disponible en: file:///D:/Tesis%20Redes/23-04-2015(Software%20Libre)/Reflexiones%20sobre%20el%20uso%20del%20Software%20Libre%20en%20Cuba.%20Ventajas%20-%20Monografias.com.htm. [Accedido: 21-may-2015].

[43]C. Rigney Livingston, A. Rubens Merit, W. Simpson Daydreamer, y S. Willens Livingston, «RFC 2138 Remote Authentication Dial In User Service(RADIUS)». abr-1997.

[44]C. Rigney Livingston, «RFC 2139 RADIUS Accounting». abr-1997.

[45]B. Aboba y M. Beadles, «RFC 2486 The Network Access Identifier». The Network Working Group, ene-1999.

[46]C. Rigney, S. Willens, A. Rubens, y W. Simpson, «RFC 2856 Remote Authentication Dial In User Service (RADIUS)». jun-2000.

[47]C. Rigney Livingston, «RFC 2866 RADIUS Accounting». Network Working Group, jun-2000.

[48]C. Rigney, W. Willats, y P. Calhoun, «RFC 2869 RADIUS Extensions». jun-2000.

[49]D. Mitto y Nortel Network, «RFC 2882 Network Access Servers Requirements: Extended RADIUS Practices». jul-200d. C.

[50]P. Calhoun, J. Loughney, Nokia, E. Guttman, Sun Microsystems, Inc., G. Zorn, Cisco Systems, Inc., J. Arkko, y Ericsson, «RFC 3588 - Diameter Base Protocol», sep-2003. [En línea]. Disponible en: file:///G:/Download%20Tesis/freeDiameter/RFC%203588%20-%20Diameter%20Base%20Protocol.htm. [Accedido: 21-may-2015].

[51]R. Drom y J.Schnizlein, «RFC 4014 - Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option». feb-200d. C.

[52]«RFC 5719 - Updated IANA Considerations for Diameter Command Code Allocations». [En línea]. Disponible en: file:///G:/Download%20Tesis/freeDiameter/RFC%205719%20-%20Updated%20IANA%20Considerations%20for%20Diameter%20Command%20Code%20Allocations.htm. [Accedido: 21-may-2015].

[53]V. Fajardo, Ed., Telcordia Technologies, J. Arkko, Ericsson Research, J. Loughney, Nokia Research Center, G. Zorn, Ed., y Network Zen, «RFC 6733 - Diameter Base Protocol», oct-2012. [En línea]. Disponible en: file:///G:/Biblio/freeDiameter/RFC%206733%20-%20Diameter%20Base%20Protocol.htm. [Accedido: 21-may-2015].

[54]Say Hood Chiu, «Seguridad en Redes Inalámbricas 802.11», Universidad Central de Venezuela, Fac. Ciencias, ene. 2008.

[55]Izaskun Pellejer, Amaia Lesta, y Fernando Andreu, «Seguridad en redes WLAN». 2008.

[56]Giovanni Zuccardi, y Juan David Gutiérrez, «Seguridad Informática en 802.11». ene-2006.

[57]Guillaume Lehembre, «Seguridad Wi-Fi – WEP, WPA y WPA2», Revista hakin9, vol. 1/2006, feb. 2015.

[58]«Servicio de Directorio con LDAP [4]: OpenLDAP (I)». [En línea]. Disponible en: file:///G:/HOYYYYY/Servicio%20de%20Directorio%20con%20LDAP%20%5B4%5D%20%20OpenLDAP%20(I).htm. [Accedido: 23-may-2015].

[59]Juan José Tomás Cánovas, «Servicio VPN de acceso remoto basado en SSL mediante OpenVPN». oct-2008.

[60]Cristina Gil Álvaro, «Servidor de túneles para el establecimiento de redes privadas virtuales punto a punto mediante OpenVPN». Proyecto de Sistemas Informáticos Facultad de Informática Universidad Complutense de Madrid, 2011-2010.

[61]Mariana Atopo y Jesús Jiménez, «Software libre y software propietario». jul-2011.

[62]Néstor Gabriel Forero Saboya, «Taxonomia-de-los-Servidores-AAA-Radius-Diameter-y-TACACS», p. 9, nov. 2009.

[63]J. B. C. Manuel Álvarez Campana, Francisco González Vidal, Raquel Pérez Leal, Isabel Román Martínez, y Enrique Vázquez Gallo, «Tecnologías de Banda Ancha y Convergencia de Redes». Gobierno de España, Ministerio de Industria, Turismo y Comercio. Secretaría de Estado de Telecomunicaciones, 2010.

[64]Jovana Palibrk, Ivan Ivanović, y Dušan Pajin, «The Implementation of the AMRES VPN Service». Produced by the AMRES-led working group on Security, mar-2013.

[65]Wi-Fi Alliance®, «The State of Wi-Fi®Security». sep-2009.

[66]Wi-Fi Alliance®, «Wi-Fi Certified™ for WMM™-Support for Multimedia Applications with Quality of Service in Wi-Fi® Networks». 01-sep-2004.

[67]Wi-Fi Alliance®, «Wi-Fi CERTIFIED™ WPA2® Delivers Advanced Security to Homes, Enterprises and Mobile Devices». sep-2009.

[68]Wi-Fi Alliance®, «Wi-Fi Certified Wi-Fi Direct™». oct-2010.

[69]MicrosoftTechnet, «Windows Server 2008 y Windows Server 2008 R2.», 03-oct-2011. [En línea]. Disponible en: http://technet.microsoft.com/es-es/library/dd349801(WS.10).aspx.

[70]Wi-Fi Alliance®, «WPA™ Deployment Guidelines for Public Access Wi-Fi® Networks». 28-oct-2004.

Glosario de términos

AAA: Authentication, Authorization and Accounting (Autenticación, Autorización y Contabilidad)

ADSL: Asymmetric Digital Subscriber Line (Línea de abonado digital asimétrica)

AES: Advanced Encryption Standard (Estándar de Cifrado Avanzado)

ATM: Asynchronous Transfer Mode (Modo de Transferencia Asíncrona)

AP: Access Point (Punto de Acceso inalámbrico)

AppleTalk: Conjunto de protocolos de Apple para la conexión de redes. Está en desuso.

BD: Data Base (Base de Datos)

BSS: Basic Service Set (Conjunto de servicios básicos)

CCMP: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (protocolo de encriptación de IEEE 802.11i)

CHAP: Challenge Handshake Authentication Protocol (Protocolo de autenticación por desafío mutuo)

CRC-32: Cyclic Redundancy Check (Comprobación de redundancia cíclica)

DIAMETER: Protocolo de red para la autenticación de los usuarios que se conectan remotamente a Internet.

EAP: Extensible Authentication Protocol (Protocolo de autenticación extensible)

EAP-FAST: EAP- Flexible Authentication via Secure Tunneling (EAP- Autenticación flexible a través de Túnel Seguro)

EAP-TLS: Extensible Authentication Protocol-Transport Level Security (RFC 2716)

ESP: Encapsulated Security Payload (Carga de seguridad encapsulada)

Firewall: Cortafuegos (componente de un sistema o una red que está diseñado para bloquear el acceso no autorizado)

Frame Relay: Técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual, introducida por la ITU-T a partir de la recomendación I.122 de 1988

FreeBSD: Sistema operativo de software libre para computadoras

FTP: File Transfer Protocol (Protocolo de Transferencia de Archivos)

Gateway: Pasarela o puerta de enlace

GPRS: General Packet Radio Service (Servicio General de Paquetes vía Radio)

GRE: Generic Routing Encapsulation (Encapsulación de Enrutamiento Genérico)

GSM: Global System for Mobile Communications (Sistema Global para las comunicaciones Móviles)

Hypervisor: Monitor de máquina virtual

IBSS: Independent basic service set (Conjunto de servicios básicos independientes)

IEEE: Institute of Electrical and Electronics Engineers

IP: Internet protocol (Protocolo de Internet)

IPsec: Internet Protocol security (Protocolo de Internet Seguro)

IPX: Internetwork Packet Exchange

LAN: Local Area Network (Red de Área Local)

LEAP: Localized Encryption and Authentication Protocol

LDAP: Lightweight Directory Access Protocol (Protocolo Ligero de Acceso a Directorios)

L2TP: Layer 2 Tunneling Protocol (Protocolo de Túnel de Capa 2)

NetBEUI: NetBIOS Extended User Interface

MIC: Message Integrity Check (Control de la Integridad del Mensaje)

MPPE: Microsoft Point to Point Encryption (Cifrado punto a punto de Microsoft)

MSCHAP: Microsoft Challenge Handshake Authentication Protocol (Protocolo de autenticación por desafío mutuo de Microsoft)

MSCHAPv2: MSCHAP versión 2

MAC: Media Access control (Control de Acceso al Medio)

One time password: OTP (Contraseña de un solo uso)

ORDBMS: Object Relational Database Management

OU: Organizational Unit (Unidad organizativa)

PAP: Password Authentication Protocol (Protocolo de Autenticación de Clave de acceso)

PHP: PHP Hypertext Pre-processor (Lenguaje de programación web)

PPP: Point to Point Protocol (Protocolo Punto a Punto)

PPTP: Point to Point Tunneling Protocol (Protocolo de Túnel Punto a Punto)

Proxy: Programa o dispositivo que realiza una tarea de acceso a Internet en lugar de otro ordenador.

QoS: Quality of Service (Calidad de Servicio)

RADIUS: Remote Authentication Dial-In User Server (Protocolo de red para la autenticación de los usuarios que se conectan remotamente a Internet)

Router: Enrutador

RSA: Rivest, Shamir y Adleman (Sistema criptográfico de clave pública)

RC4: Rivest Cipher 4

RSN: Robust Security Network (Red de seguridad robusta)

SO: Operating System (Sistema Operativo)

SSH: Secure Shell (Intérprete de órdenes segura)

TI: Tecnologías de la información

TKIP: Temporal Key Integrity Protocol (Protocolo de Integridad de Clave Temporal)

TSN: Transitional Security Network

UAM: Universal Access Method (Método de acceso universal)

UMTS: Universal Mobile Telecommunications System (Sistema de telefonía móvil de tercera generación)

Smartphones: Teléfono inteligente

SSID: Service Set IDentifier (Nombre incluido en todos los paquetes de una red Wi-Fi para identificarlos como parte de esa red)

VM: Virtual machine (Máquina Virtual)

VPN: Virtual Private Network (Red privada virtual)

WEP: Wired Equivalent Privacy (Privacidad Equivalente a Cableado)

Wi-Fi: Wireless Fidelity (Es una marca de la Wi-Fi Alliance)

WLAN: Wireless Local Area Network (Red inalámbrica de Área Local)

WAN: wide area network (Red de área amplia)

MAN: Metropolitan Area Network (Red de Área metropolitana)

WMAN: Wireless Metropolitan Area Network (Red inalámbrica de área metropolitana)

WPA: Wi-Fi Protected Access (Acceso Protegido Wi-Fi)

WPA2: WPA versión 2

WPAN: Wireless Personal Area Network (Red inalámbrica de Área Personal)

WPA-PSK: Wi-Fi Protected Access with Pre-Shared Key (Acceso Protegido Wi-Fi con clave previamente compartida)

WWAN: Wireless Wide Area Network (Red inalámbrica de área extensa)

X.25: Es un estándar de la ITU-T para redes de conmutación de paquetes de área amplia

X11: X Window System (Sistema de ventanas X)

Anexos

Anexo A. Mecanismos de seguridad en WLAN

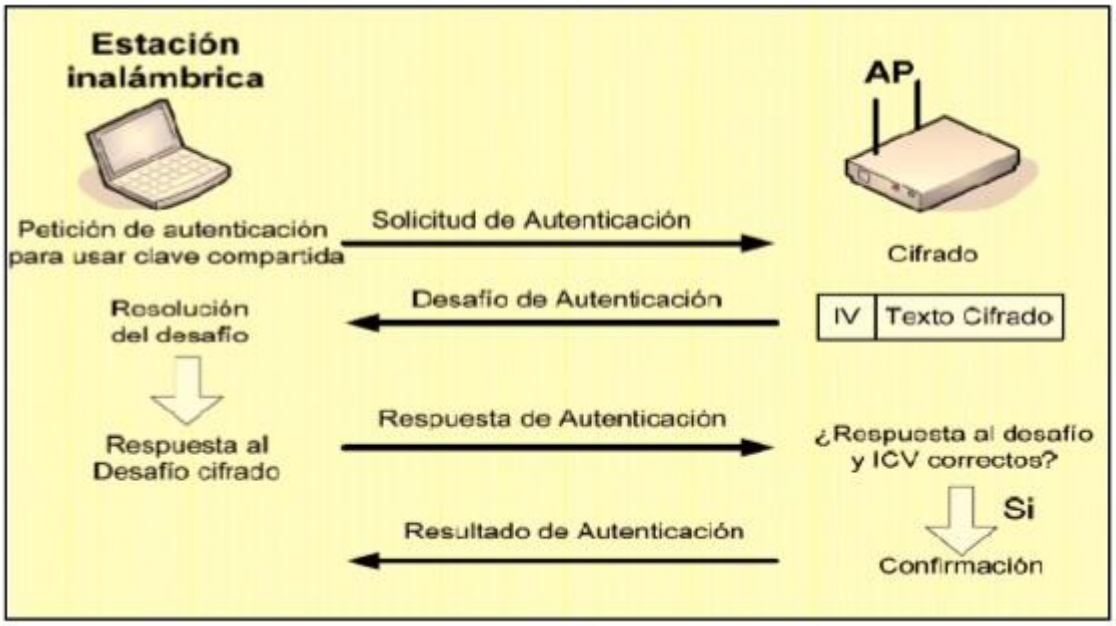

Figura 17 A.1. Proceso de autenticación con clave compartida en una WLAN que emplea WEP.[1]

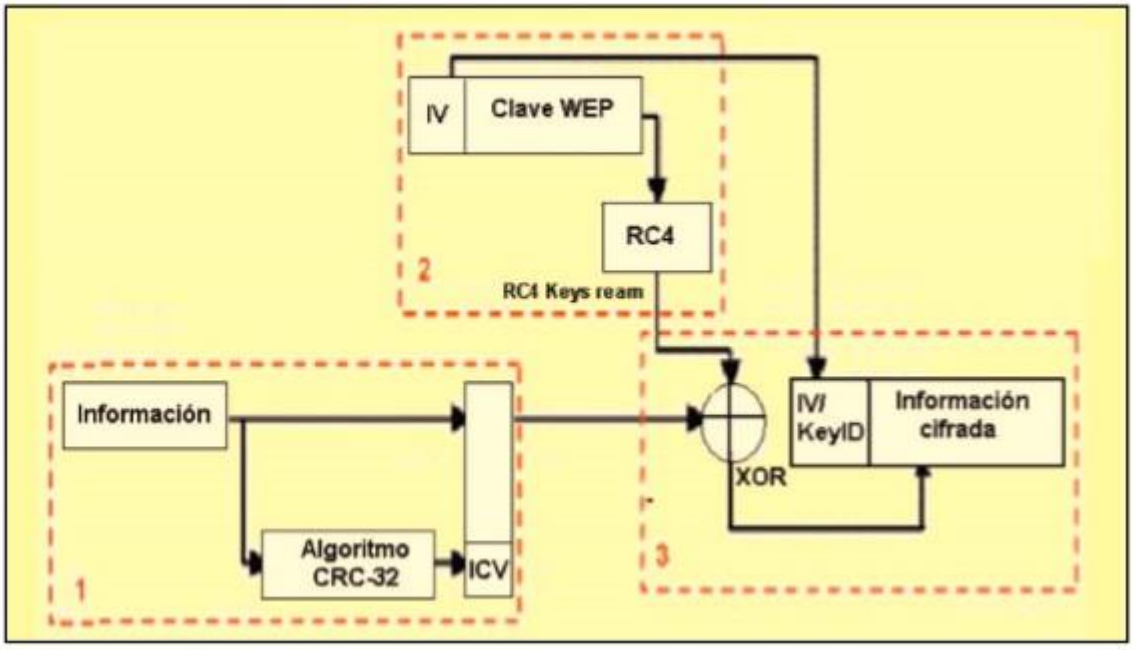

Figura 18. A.2. Proceso de cifrado WEP.[1]

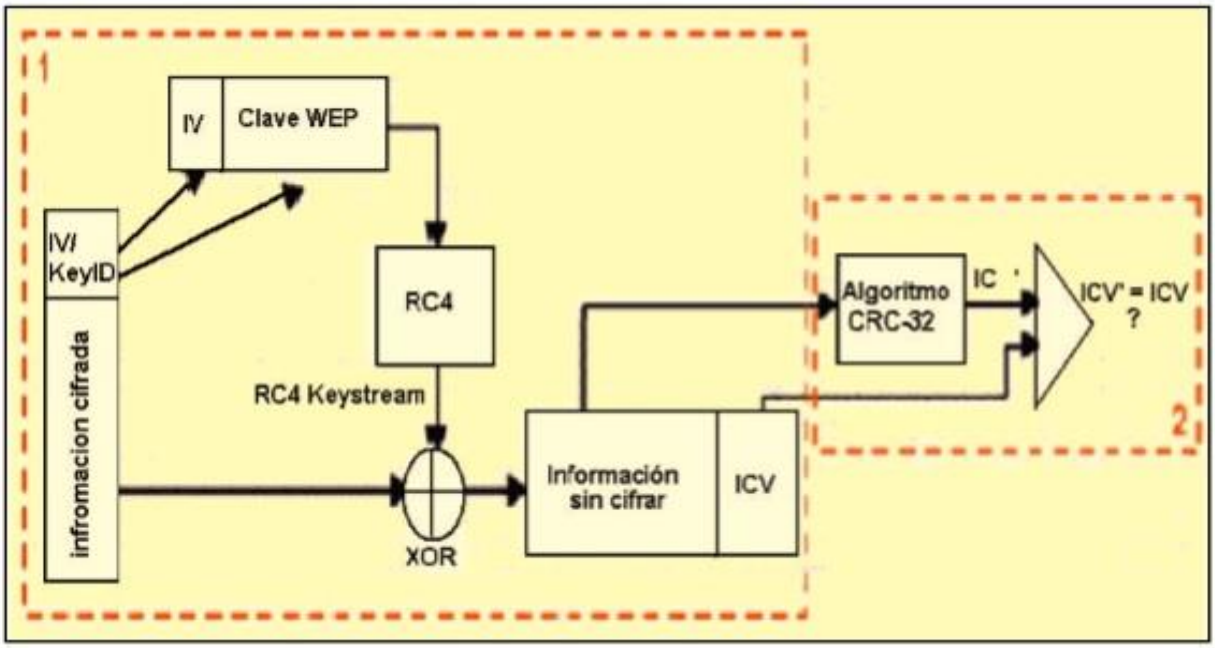

Figura 19. A.3. Proceso de descifrado WEP.[3]

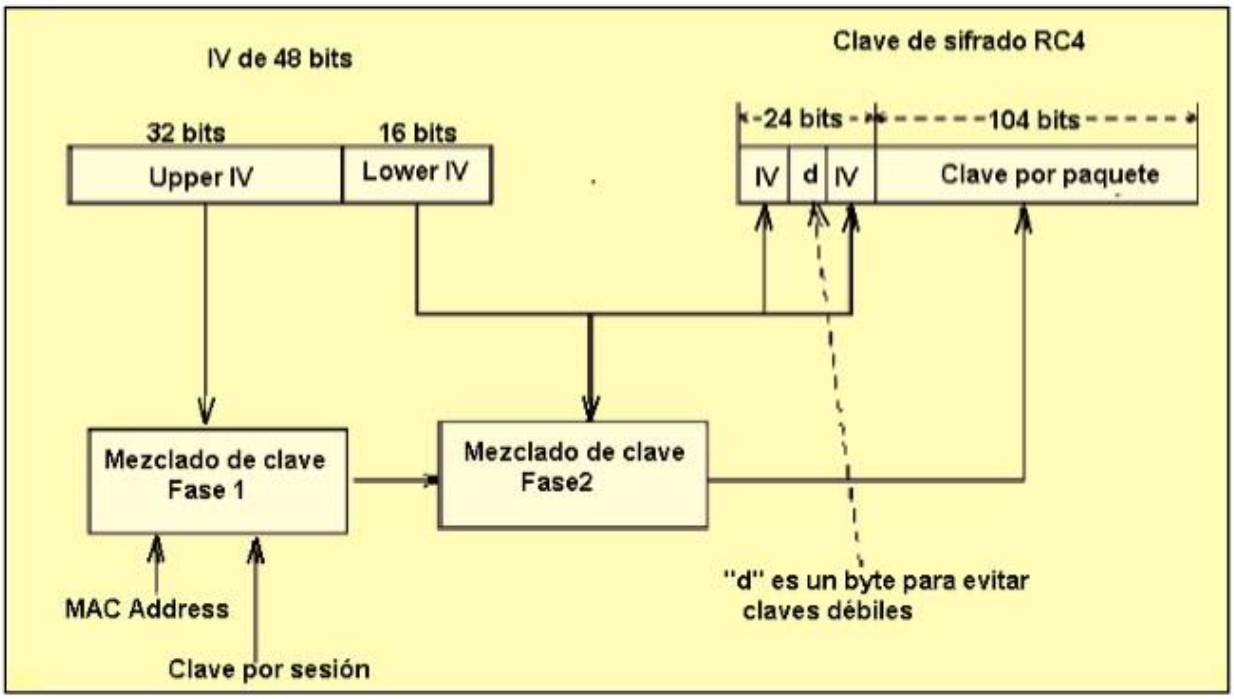

Figura 20. A.4. Generación dinámica de clave por paquete en TKIP.[3]

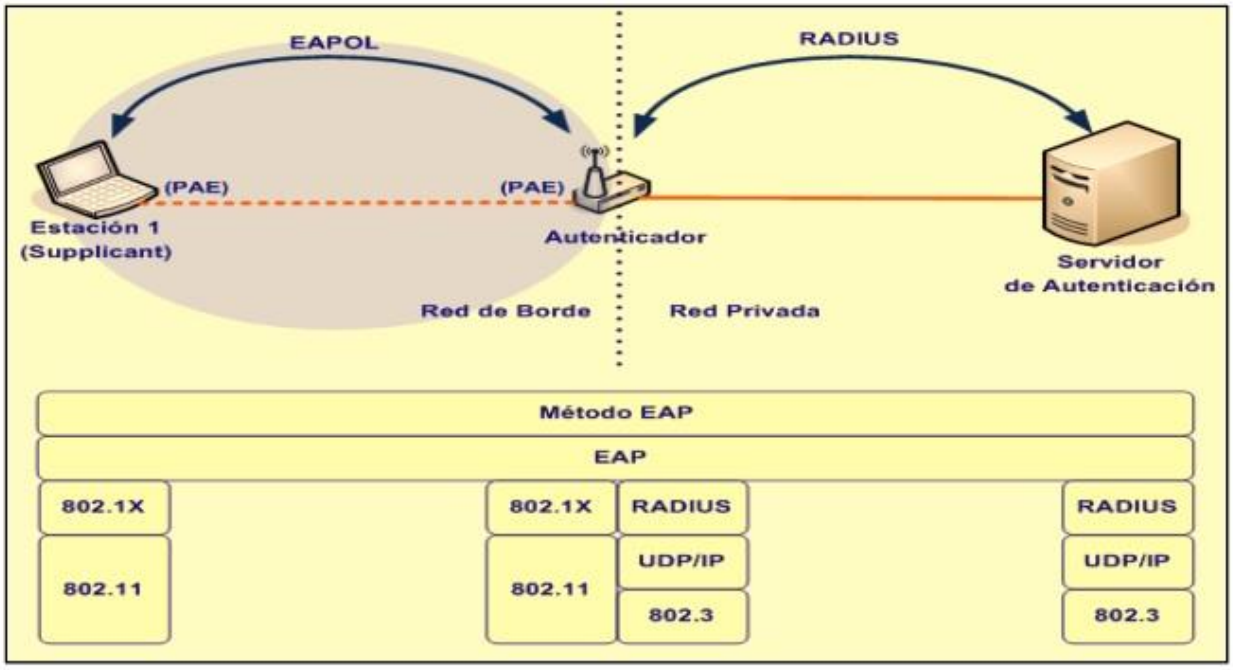

Figura 21. A.5. Autenticación WLAN arquitectura IEEE 802.1x[1]

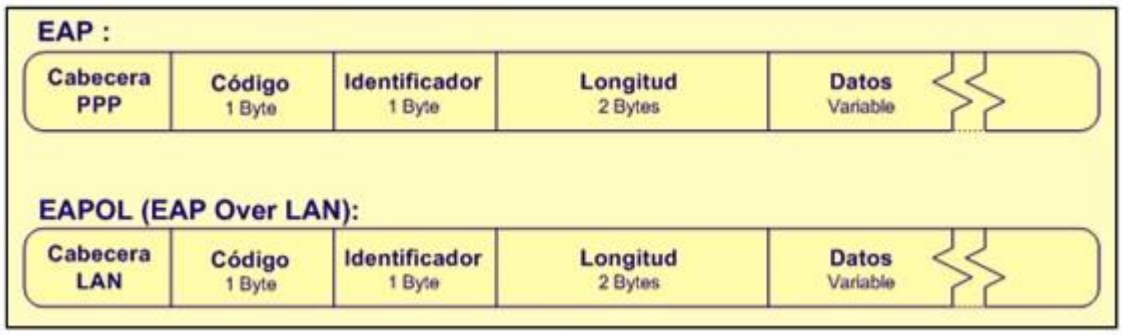

Figura 22. A.6. Formato genérico de los paquetes EAP.[1]

Figura 23. A.7. Formato de Paquetes EAP Solicitud y Respuesta.[1]

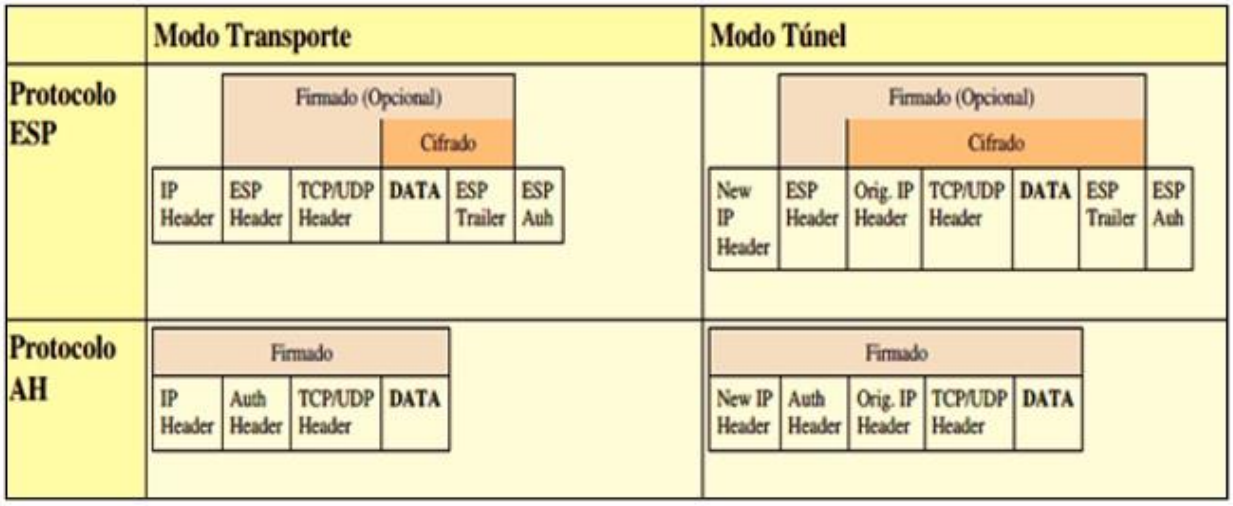

Figura 24. A.8. Protocolos y modos de operación de IPsec.[3]

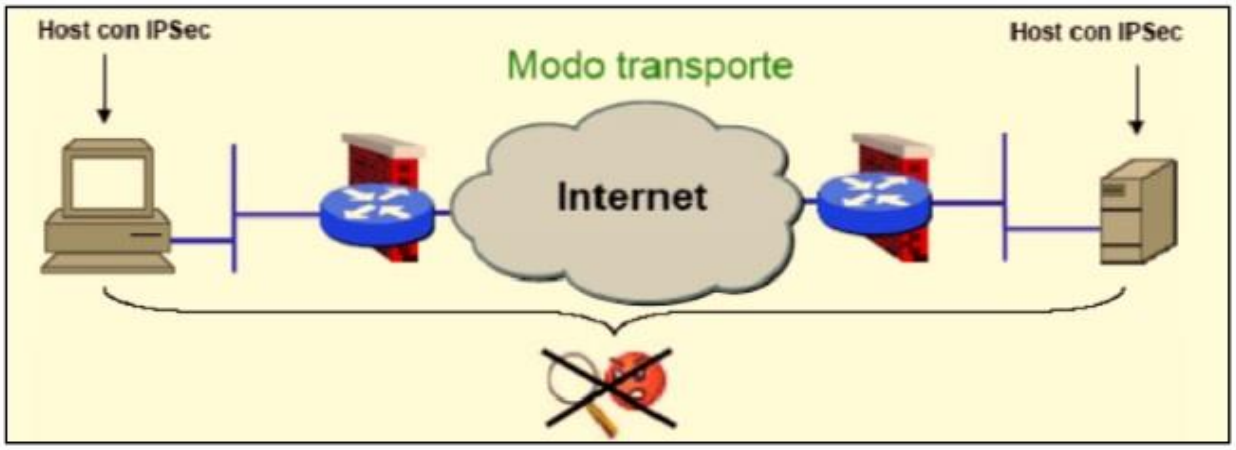

Figura 25. A.9. Modo Transporte en IPsec.[3]

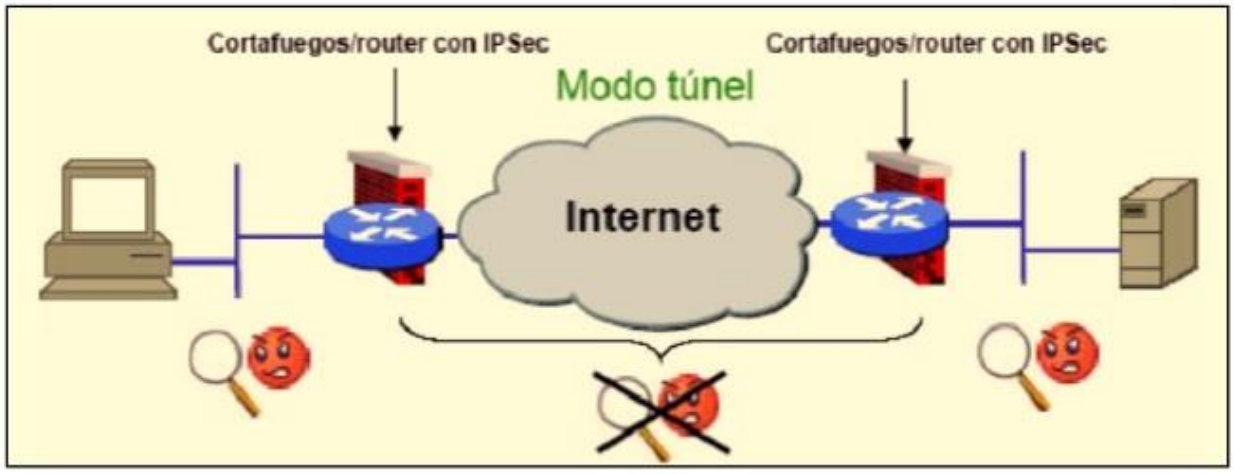

Figura 26. A.10. Modo Túnel en IPsec.[3]

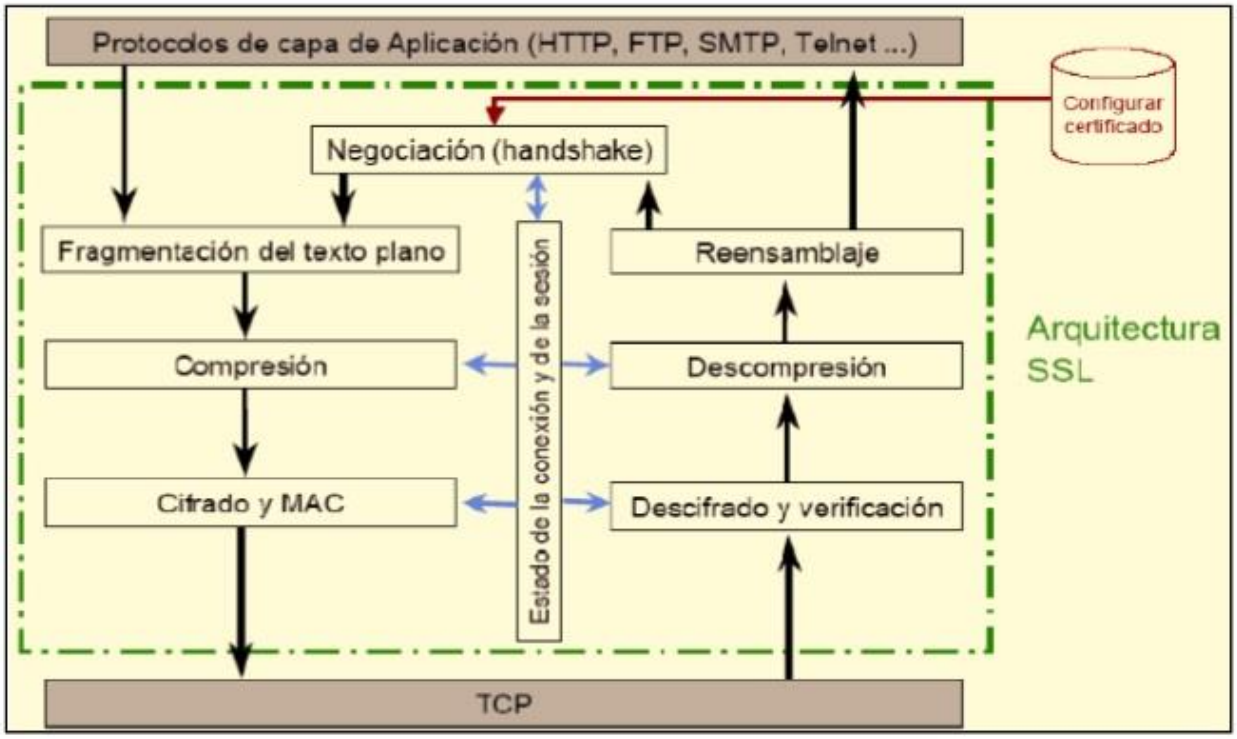

Figura 27. A.11. Arquitectura SSL/ TLS.

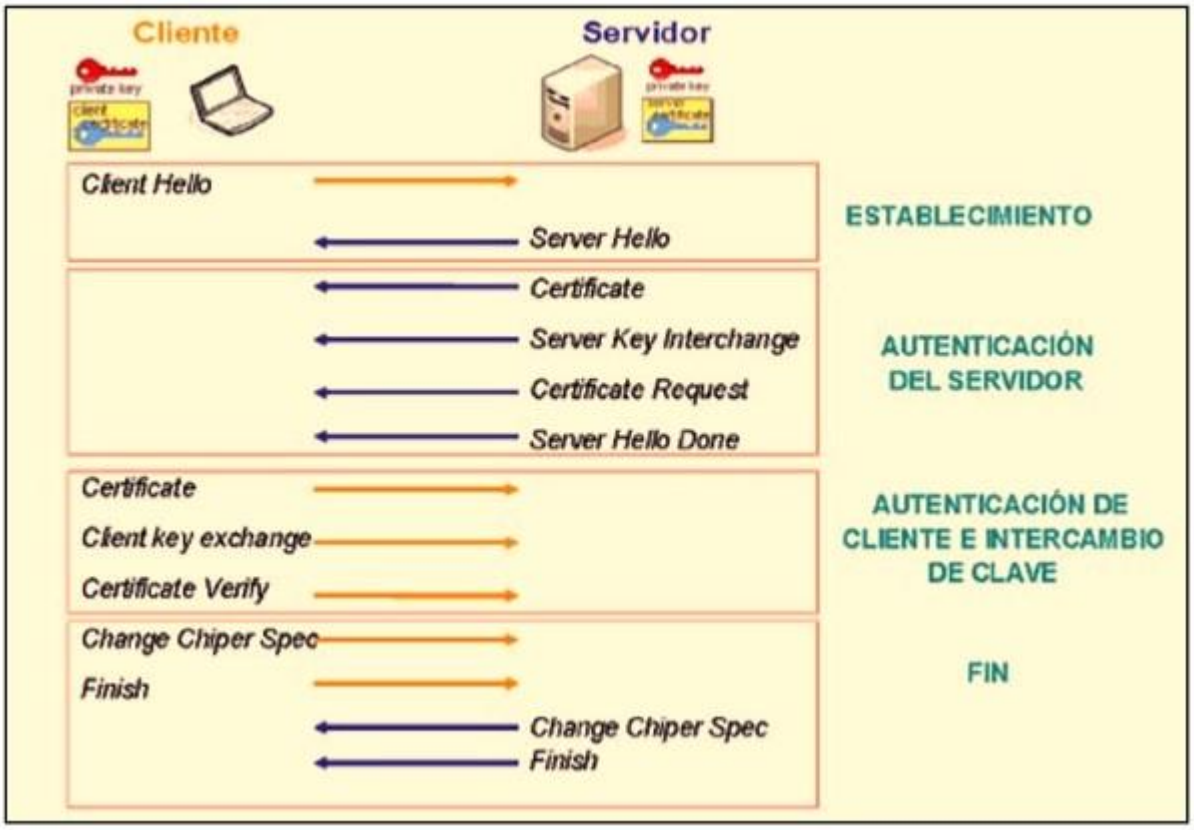

Figura 28. A.12. Intercambio de mensajes para el establecimiento de un canal seguro en SSL.

Anexo B. Requisitos

Tabla 1. Requisitos de hardware para instalar Ubuntu Server 12.04

Componente	Requisitos
Procesador	Mínimo: 1 GHz (procesador x86) o 1.4 GHz (procesador x64)
Memoria	Mínimo: 512 MB RAM Máximo (sistemas de 32 bits): 4 GB (Standard) o 64 GB (Enterprise Datacenter) Máximo (sistemas de 64 bits): 8 GB (Foundation) o 32 GB (Standard) o 2 TB (sistemas basados en Enterprise, Datacenter e Itanium)
Requisitos de espacio en disco	Mínimo (sistemas de 32 bits): 20 GB o más Mínimo (sistemas de 64 bits): 32 GB o más Foundation: 10 GB o más Nota: las computadoras con más de 16 GB de RAM requieren más espacio en disco para paginación, hibernación y volcado de archivos
Pantalla	Súper VGA (800 × 600) o monitor de mayor resolución
Otros	Teclado y mouse o dispositivo compatible

Tabla 2. Requisitos de hardware para instalar Windows Server 2008 R2.

Componente	Requisito
Procesador	Mínimo: 1 GHz (procesador x86) o 1.4 GHz (procesador x64) Nota: se requiere un procesador Intel Itanium 2 para Windows Server 2008 para sistemas basados en Itanium
Memoria	Mínimo: 512 MB RAM Máximo (sistemas de 32 bits): 4 GB (Standard) o 64 GB (EnterpriseDatacenter) Máximo (sistemas de 64 bits): 8 GB (Foundation) o 32 GB (Standard) o 2 TB (sistemas basados en Enterprise, Datacenter e Itanium)
Requisitos de espacio en disco	Mínimo (sistemas de 32 bits): 20 GB o más Mínimo (sistemas de 64 bits): 32 GB o más Foundation: 10 GB o más Nota: las computadoras con más de 16 GB de RAM requieren más espacio en disco para paginación, hibernación y volcado de archivos
Pantalla	Super VGA (800 × 600) o monitor de mayor resolución
Otros	Teclado y mouse

Tabla 3. Requisitos de hardware y software para instalar PostgreSQL.

Componente	Requisitos
Marco de trabajo	El programa de instalación de PostgreSQL instala los siguientes componentes de software requeridos por el producto: .NET Framework 3.5 SP11 SQL Server Native Client Archivos auxiliares para la instalación de SQL Server
Disco duro	Las necesidades de espacio en disco variarán con los componentes de PostgreSQL que instale.
Pantalla	Resolución mínima de 800 x 600 píxeles
Otros dispositivos	Dispositivo señalador: se necesita un mouse Microsoft o dispositivo señalador compatible

Anexo C. Configuración de los Puntos de Acceso

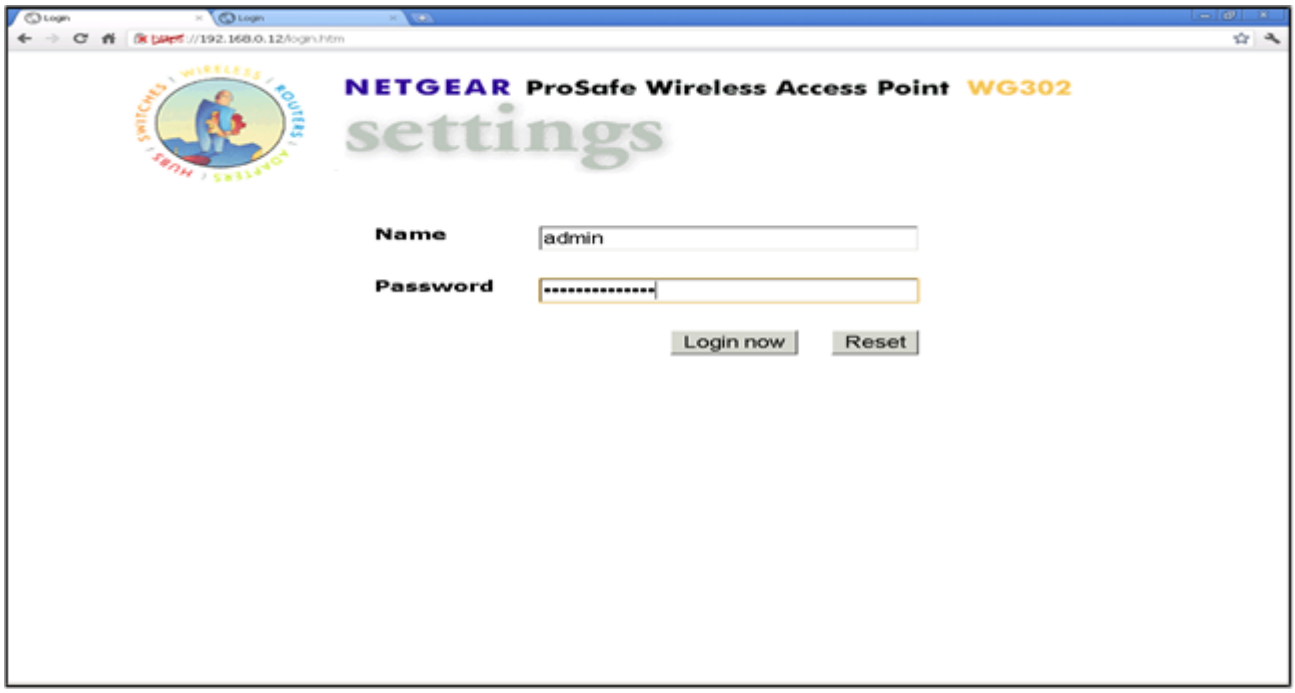

Figura 29. Interfaz Web de administración de los Puntos de Acceso NetGear WG302. En este caso se trata de la página de autenticación del AP-1.

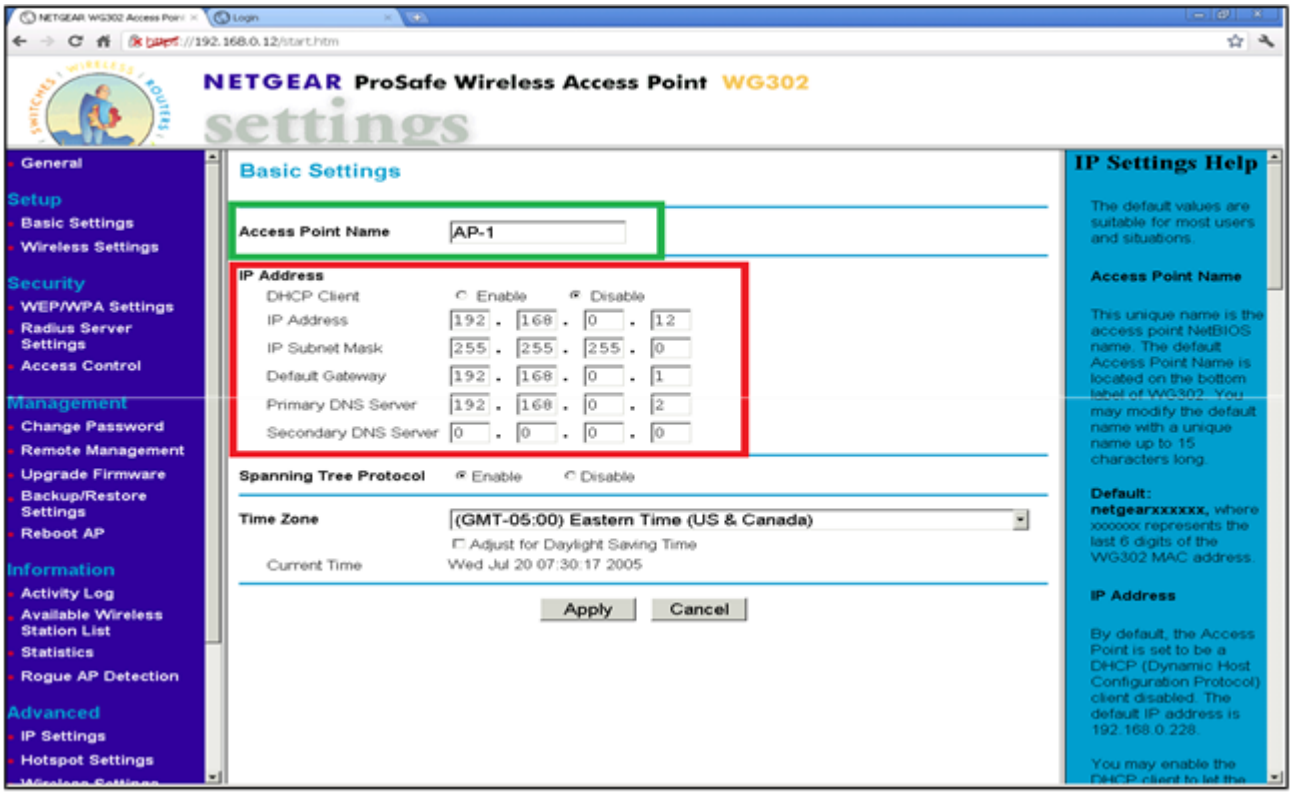

Figura 30. Configuración de los parámetros básicos del AP-1 (nombre del AP, dirección IP).

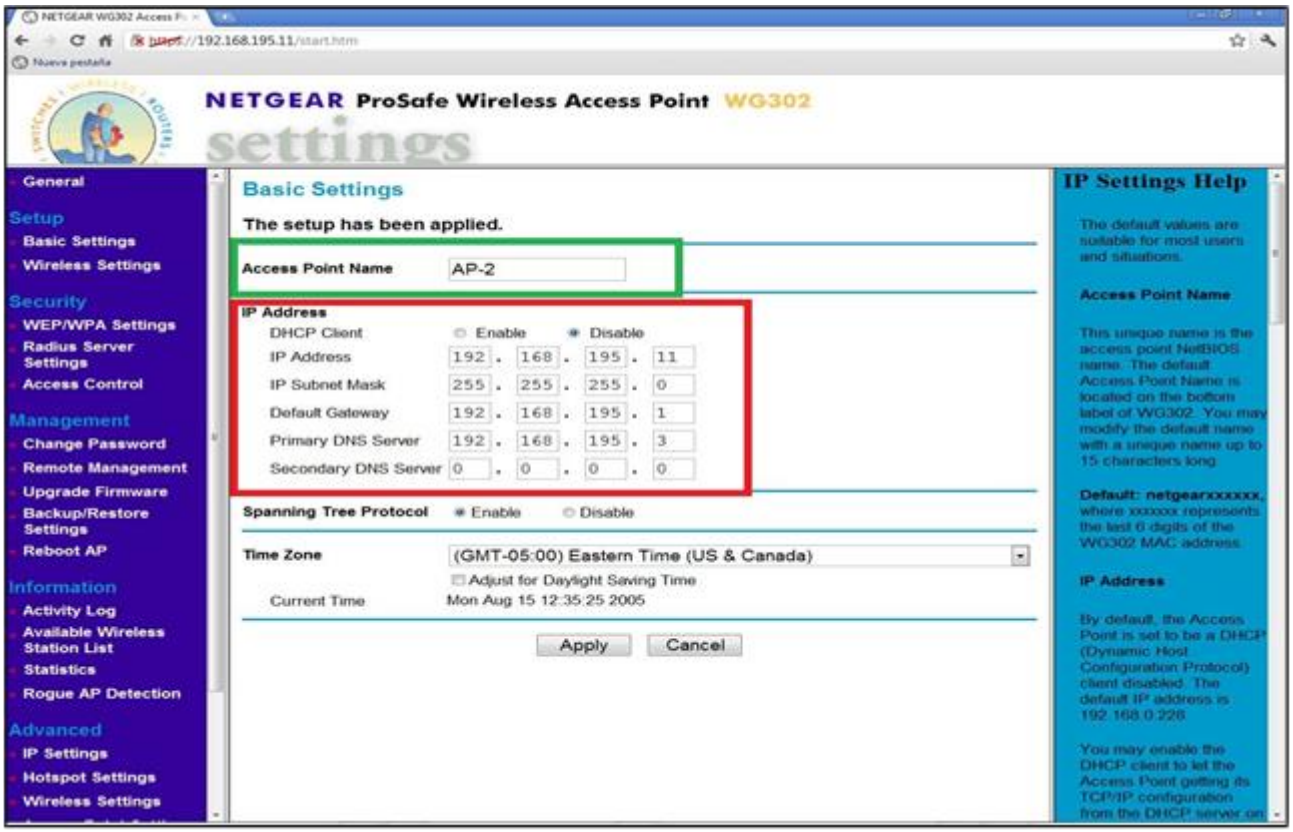

Figura 31. Configuración de los parámetros básicos del AP-2 (nombre del AP, dirección IP).

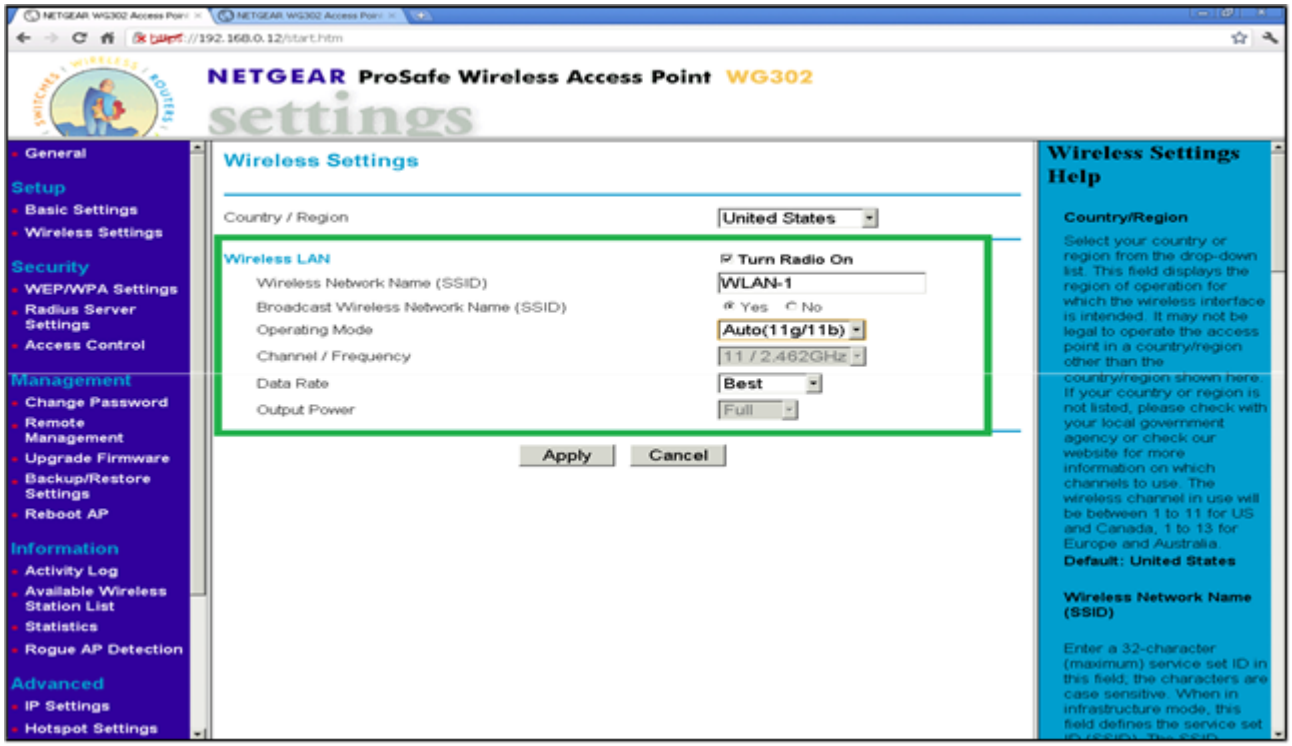

Figura 32. Configuración de los parámetros Wireless del AP-1 (nombre de la red, modo de operación, canal/frecuencia, razón de datos).

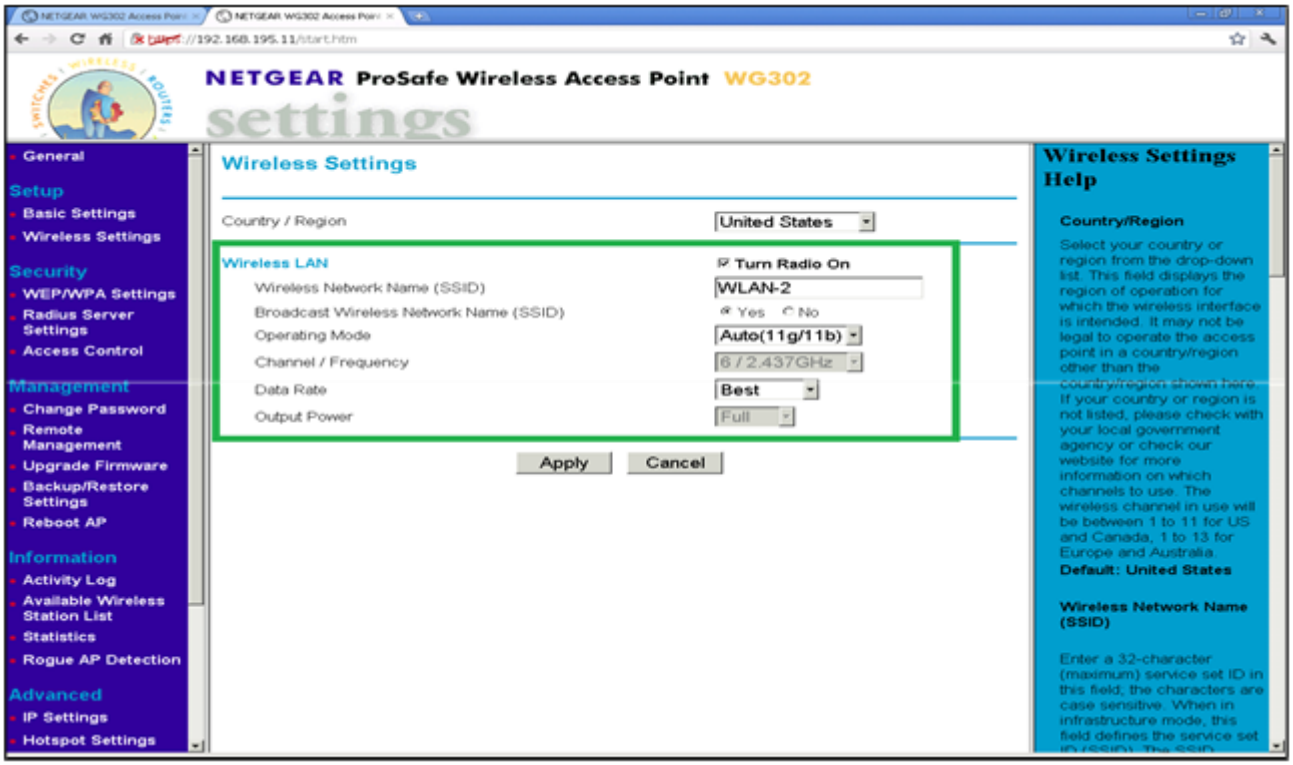

Figura 33. Configuración de los parámetros Wireless del AP-2 (nombre de la red, modo de operación, canal/frecuencia, razón de datos).

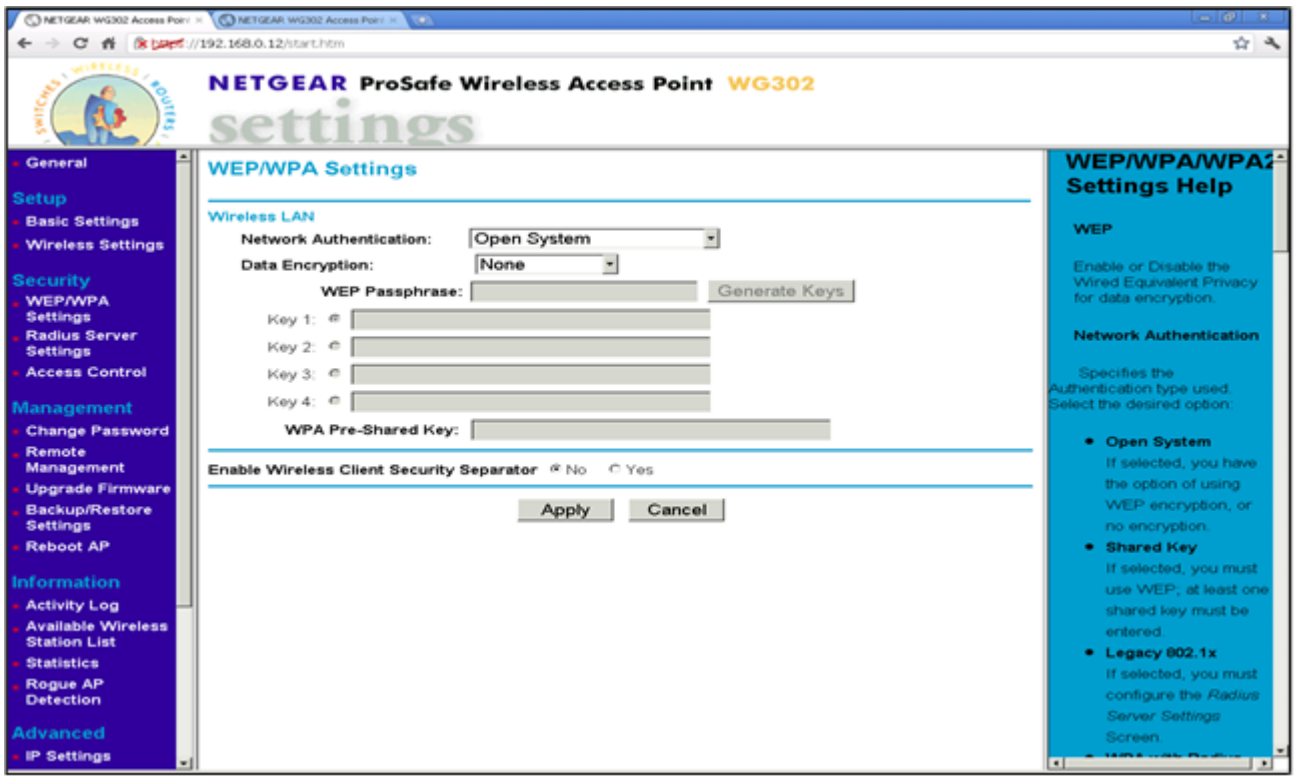

Figura 34. Configuración de los parámetros de seguridad del AP-1 (autenticación de red, cifrado de datos).

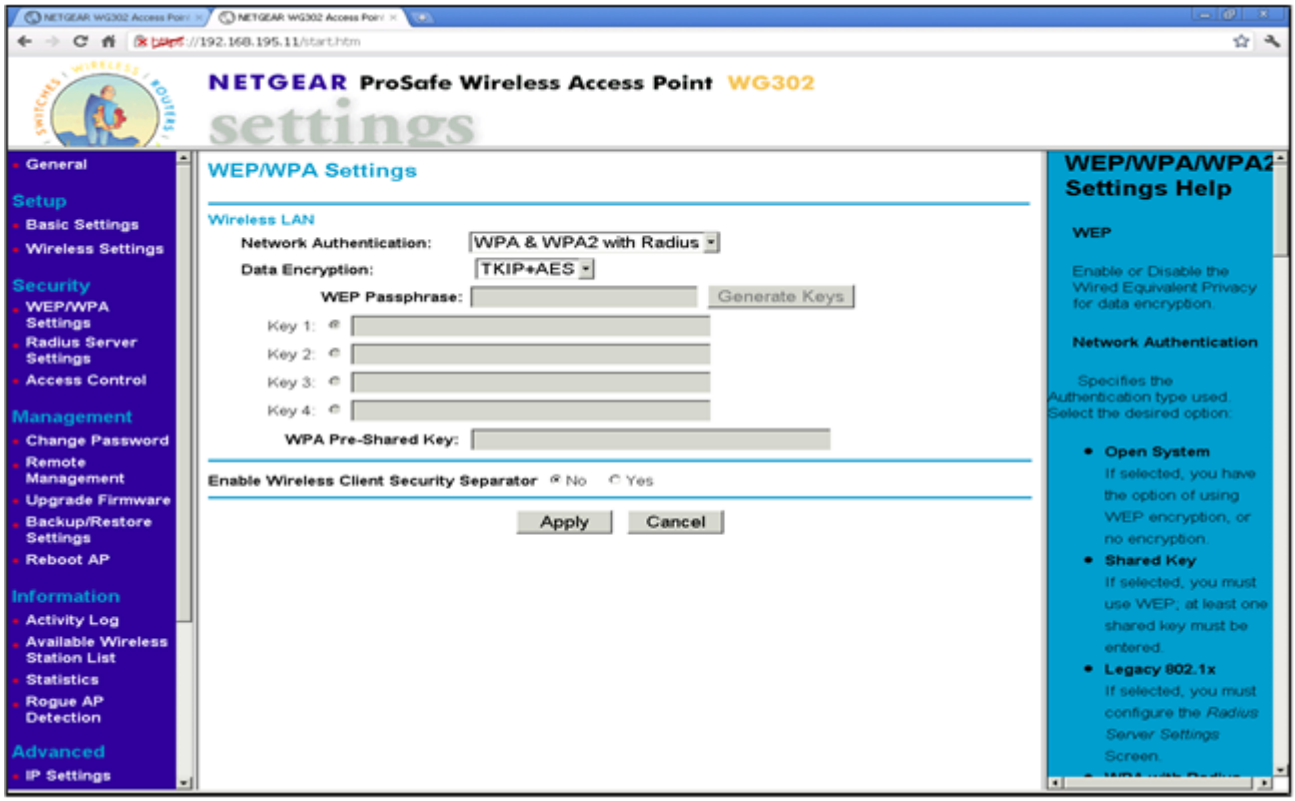

Figura 35. Configuración de los parámetros de seguridad del AP-2 (autenticación de red, cifrado de datos).

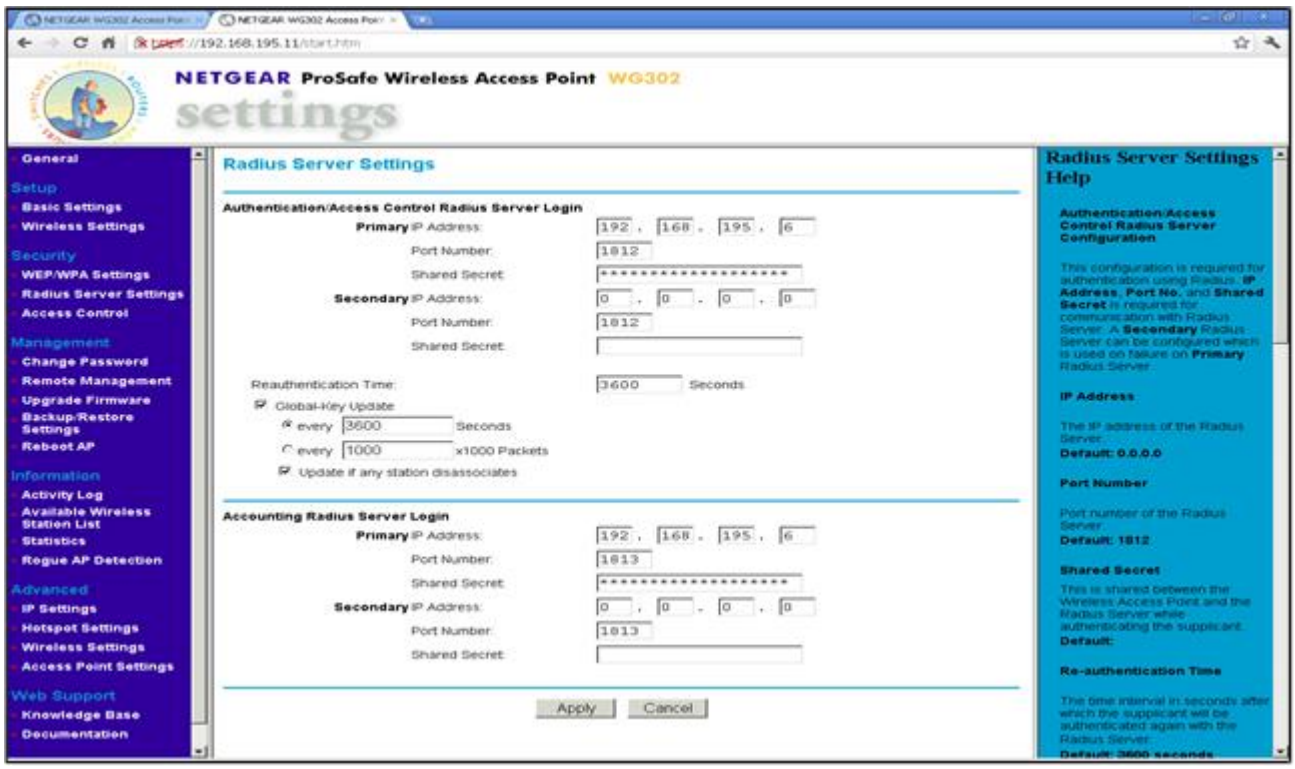

Figura 36. Configuración de los parámetros de seguridad del AP-2 (parámetros correspondientes al servidor RADIUS).

Anexo D. Configuración de los roles DHCP y DNS del Servidor de Dominio.

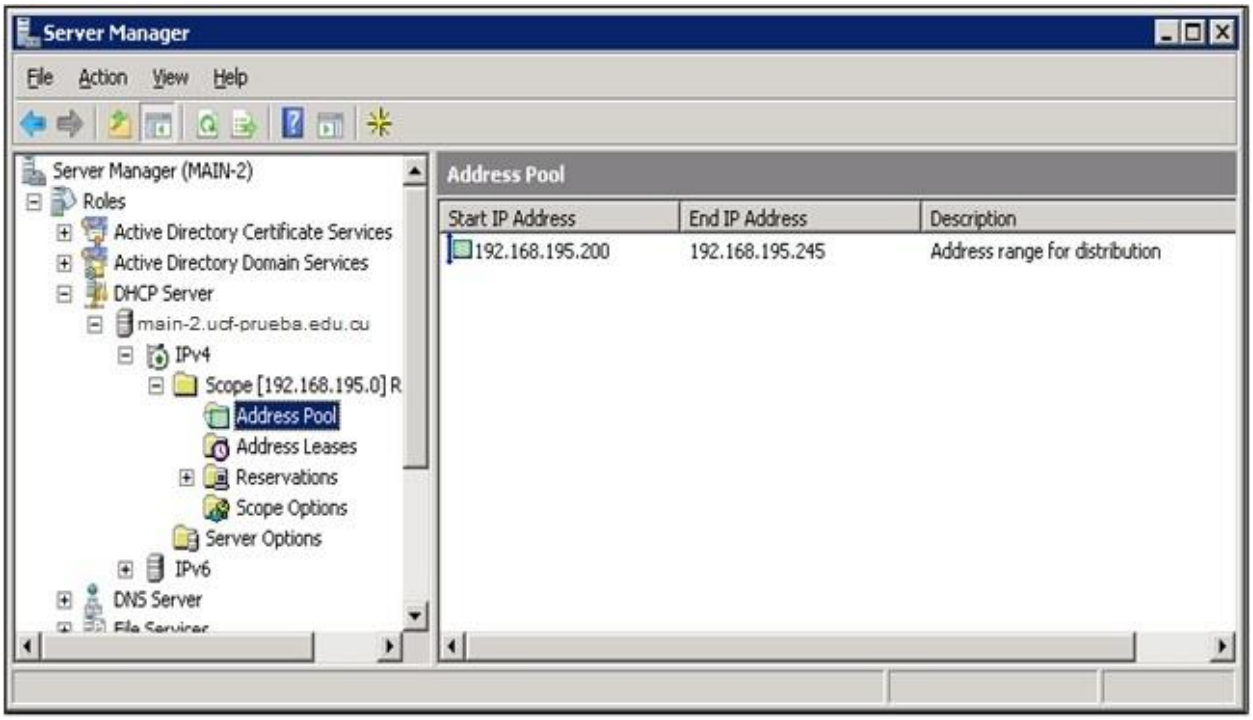

Figura 37. Configuración del rol DHCP. En este caso se define el rango de direcciones IP que pueden ser asignadas a los clientes DHCP.

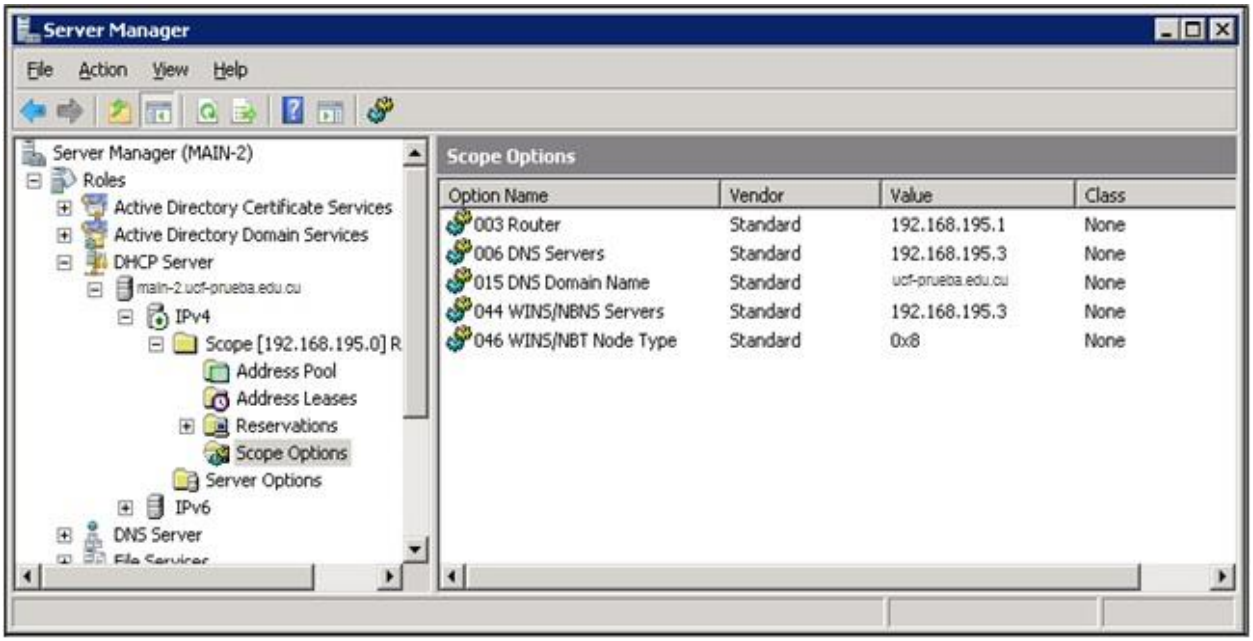

Figura 38. Configuración del rol DHCP. En este caso se definen los parámetros del ámbito (scope): Router, DNS Server, WINS Server y DNS Domain Server, los cuales serán asignados a la configuración de los clientes DHCP.

Anexo E. Configuración del servidor de VPN PPTP

Figura 39. Configuración del servidor VPN PPTP en PfSense.

Figura 40. Regla en el Firewall de PfSense para la VPN PPTP.

Anexo F. Configuración del servidor de VPN IPsec

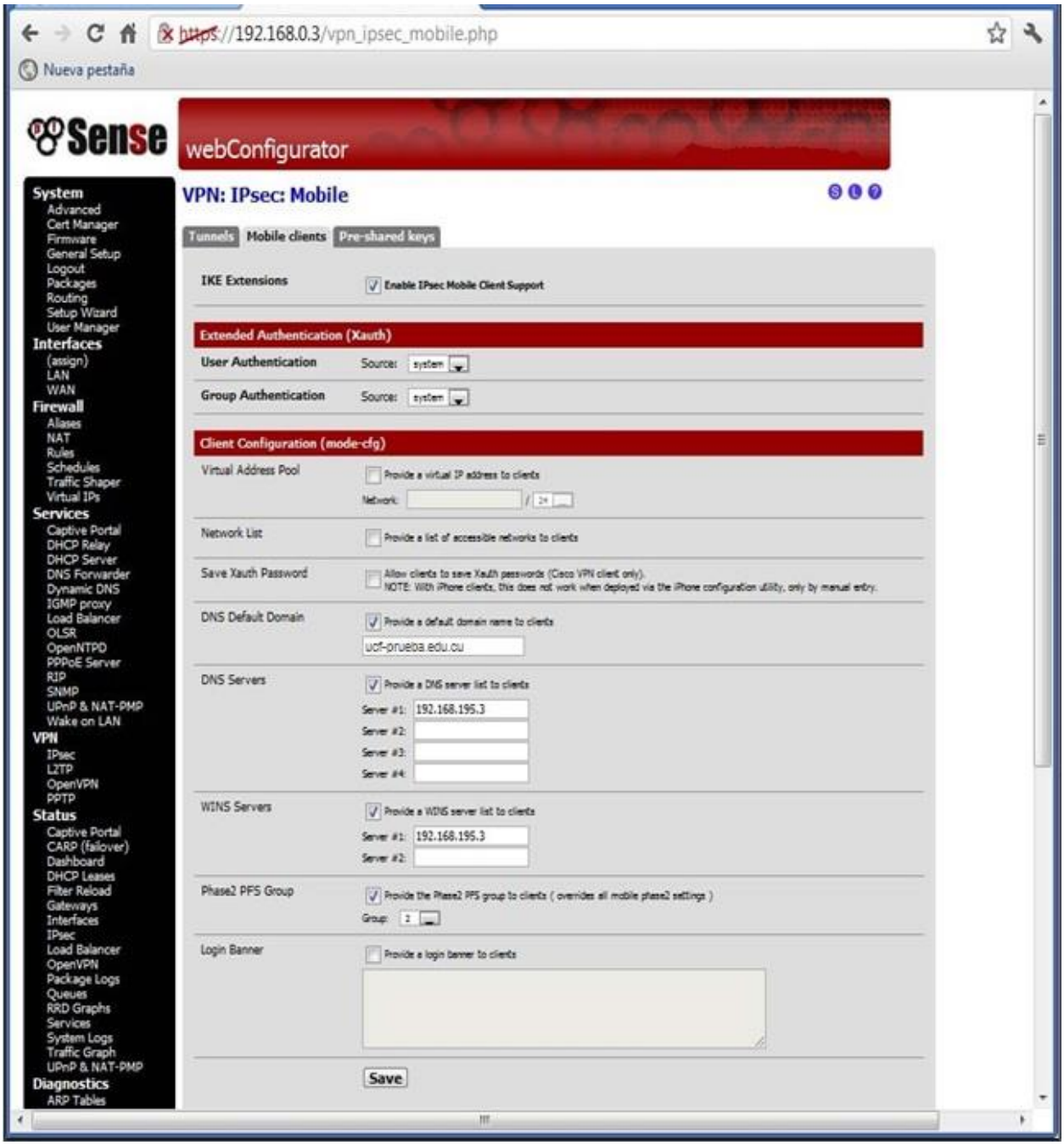

Figura 41. Configuración del servidor VPN IPsec en PfSense (parte 1).

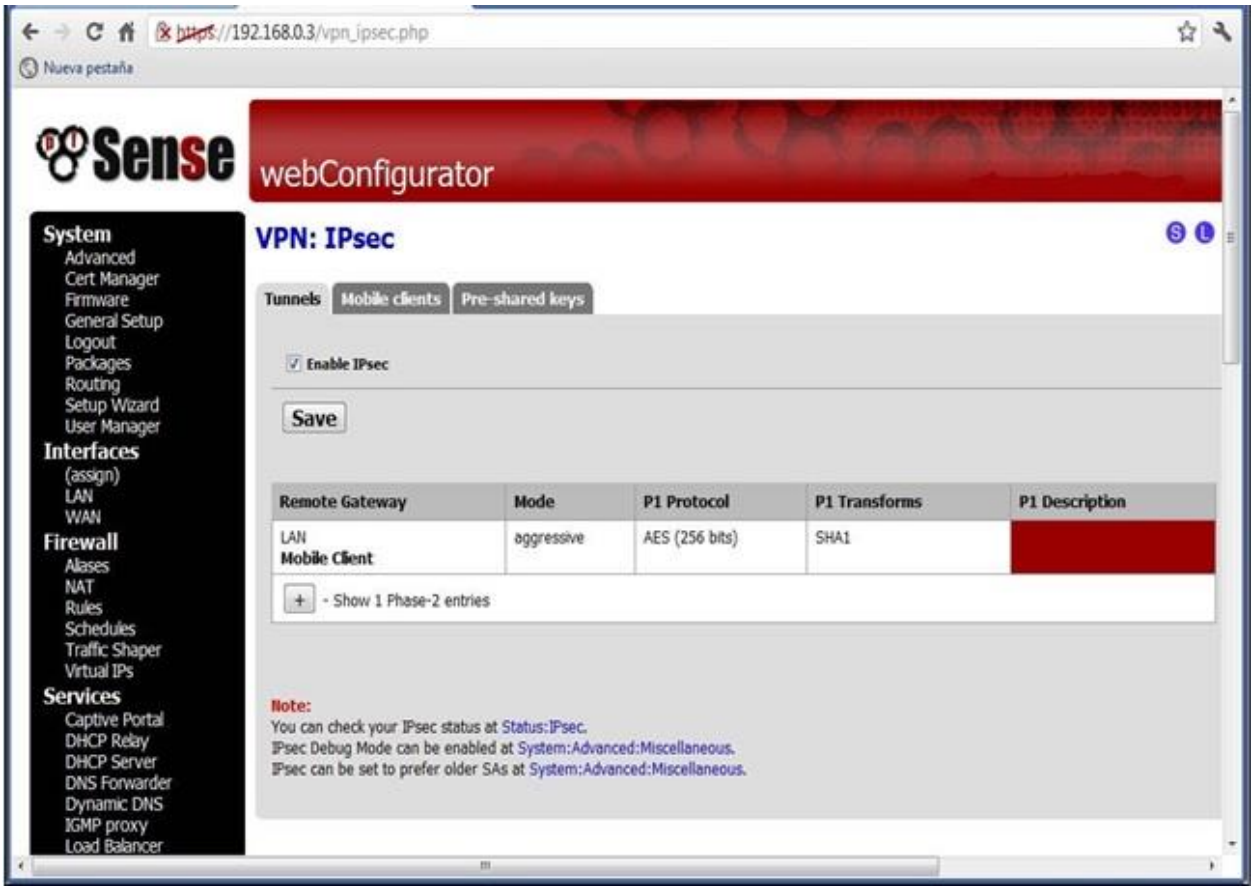

Figura 42. Configuración del servidor VPN IPsec en PfSense (parte 2).

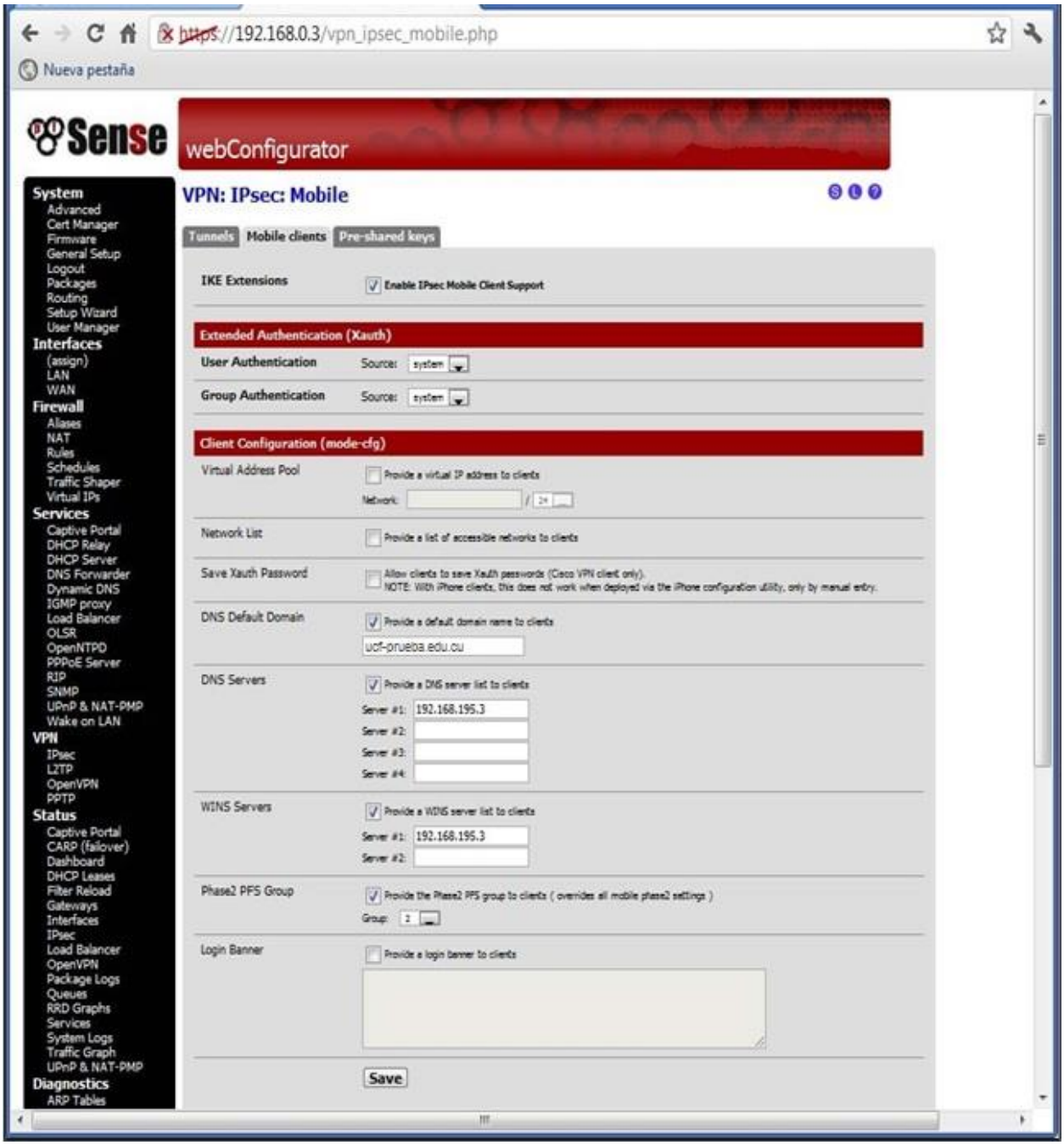

Figura 43. Configuración del servidor VPN IPsec en PfSense (parte 3).

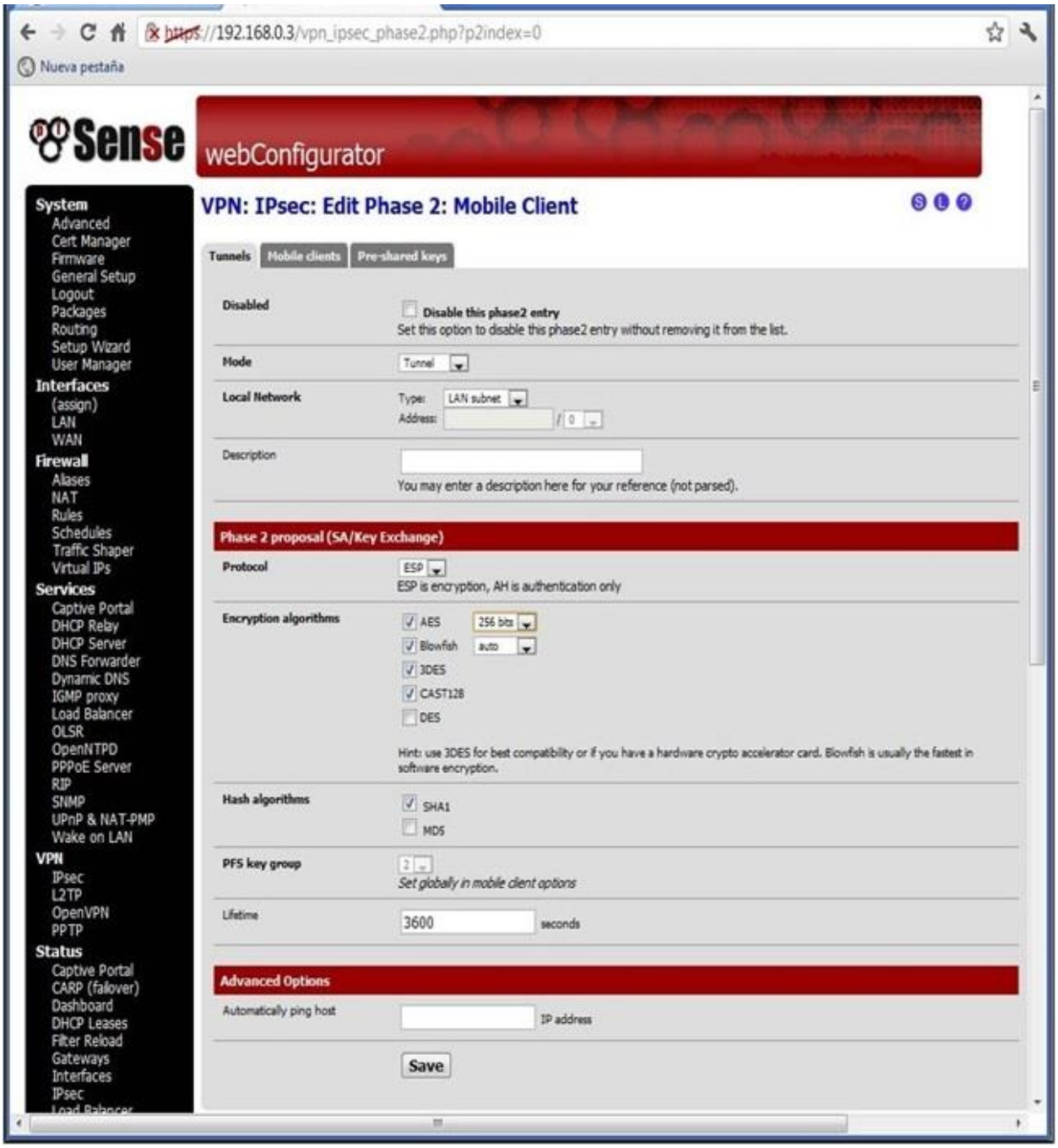

Figura 44. Configuración del servidor VPN IPsec en PfSense (parte 4).

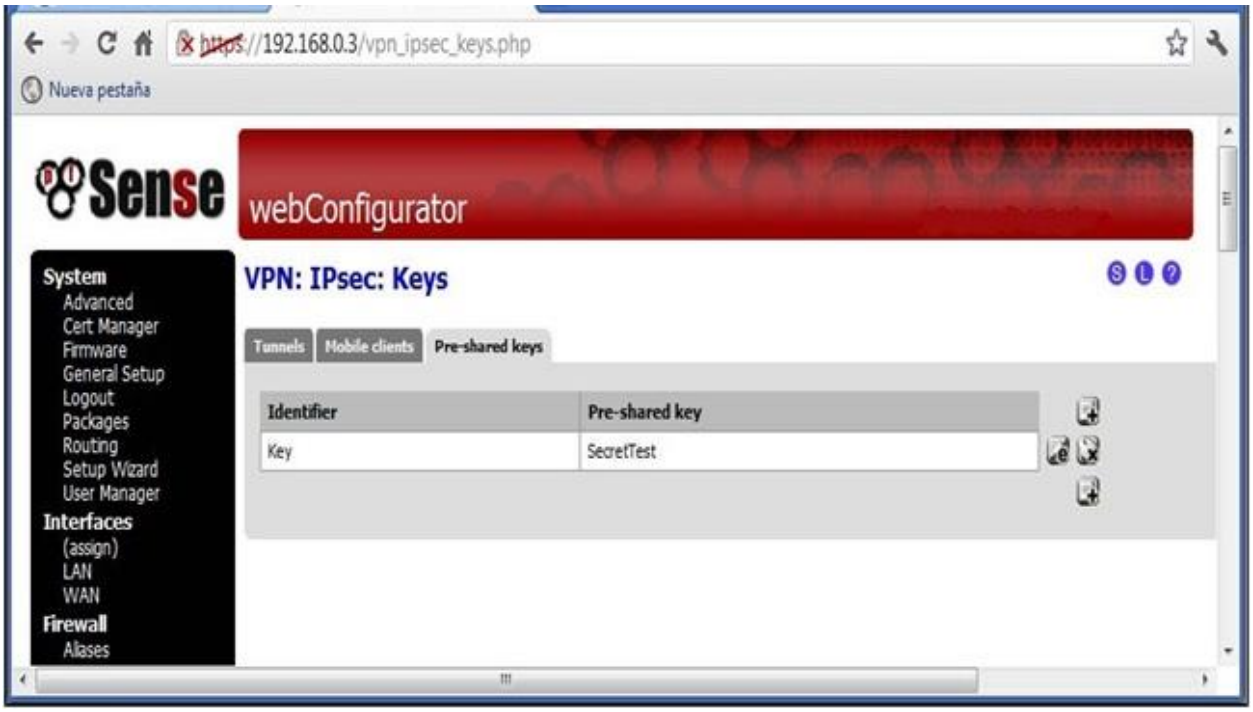

Figura 45. Configuración del servidor VPN IPsec en PfSense (parte 5).

Figura 46. Regla en el Firewall de PfSense para la VPN IPsec (interfaz IPsec).

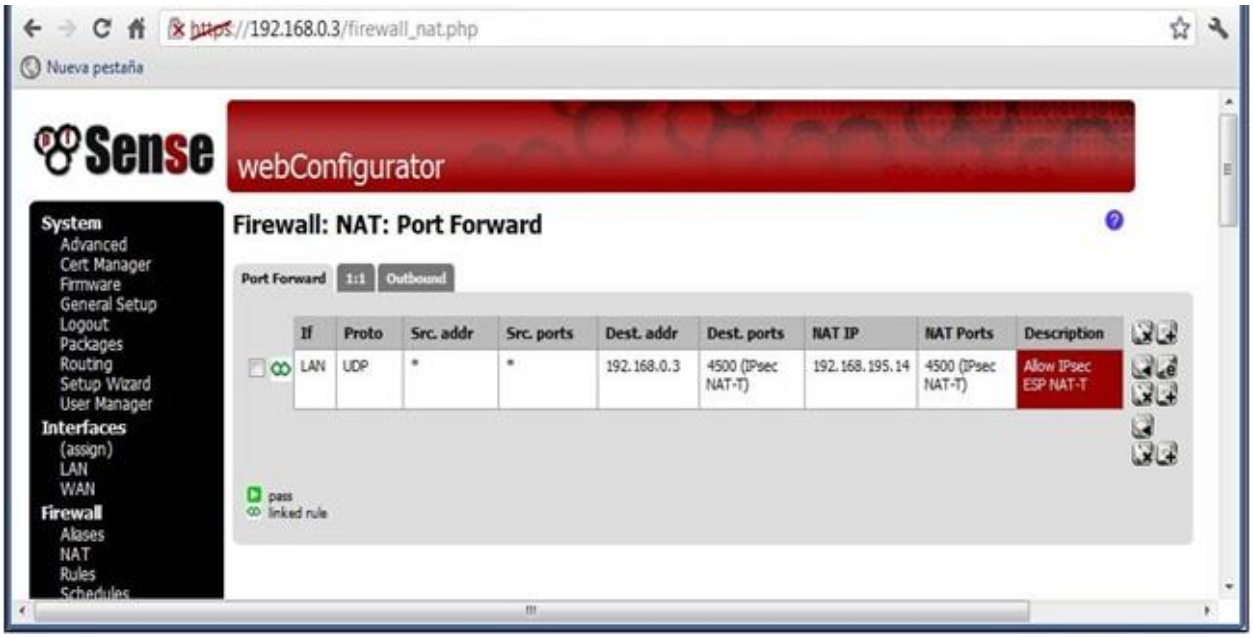

Figura 47. Regla NAT en el Firewall de PfSense para la VPN IPsec.

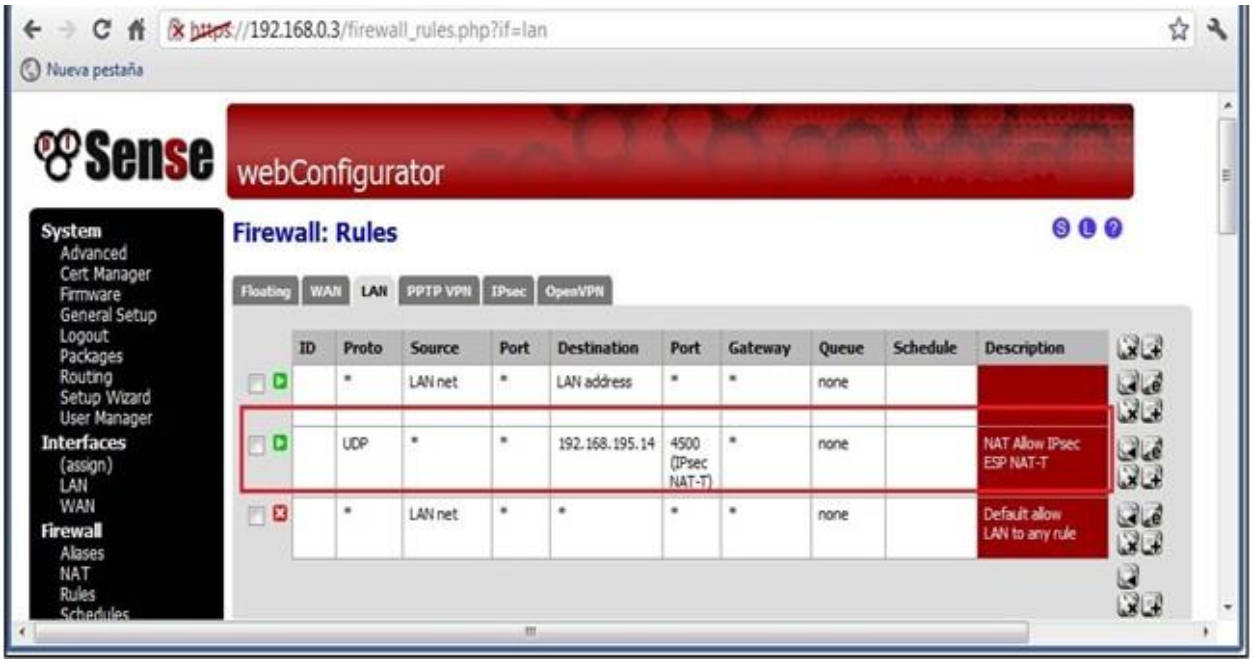

Figura 48. Regla en el Firewall de PfSense para la VPN IPsec (interfaz LAN).

Anexo G. Configuración del servidor de OpenVPN

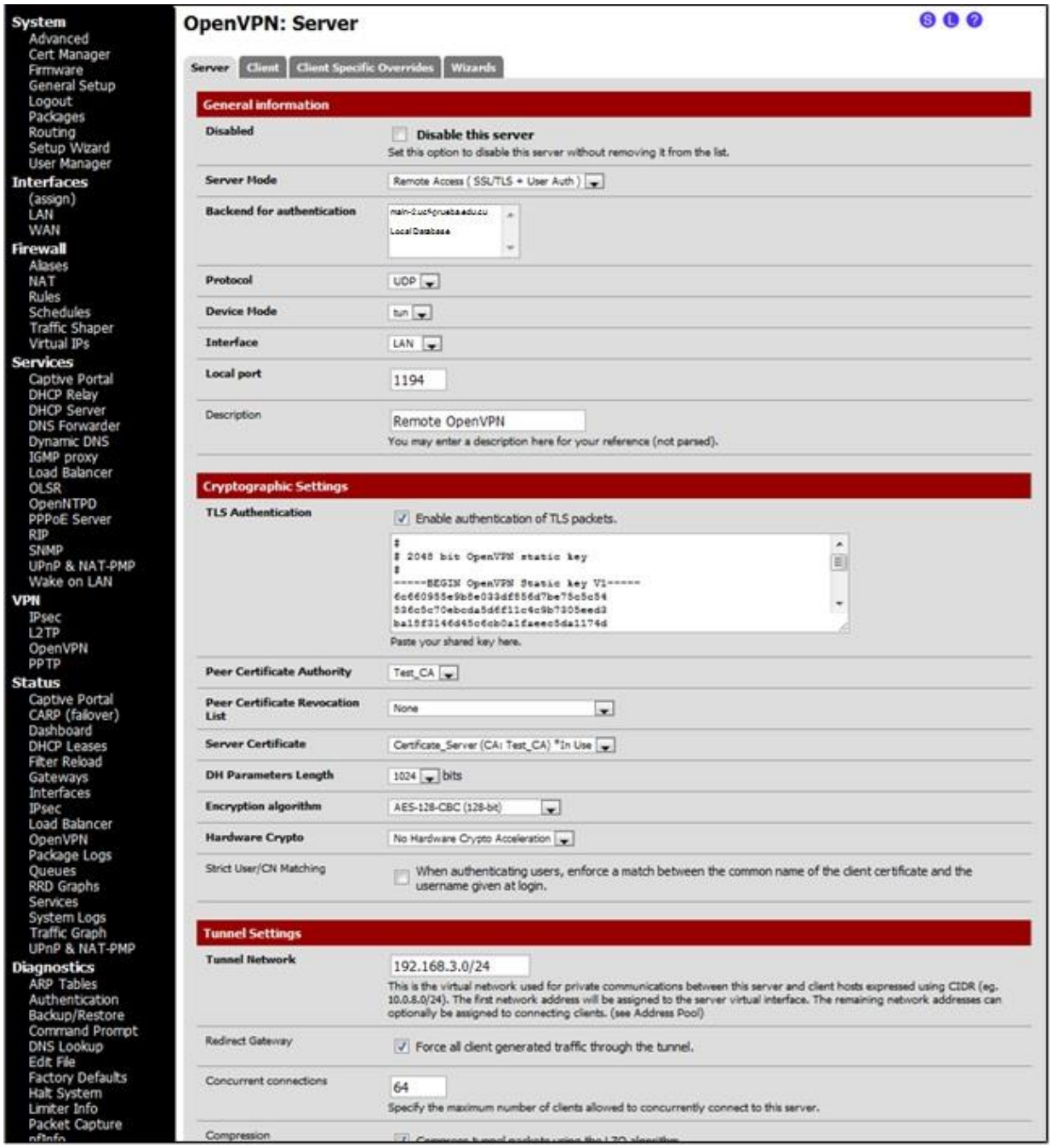

Figura 49. Configuración del servidor de OpenVPN (parte 1).

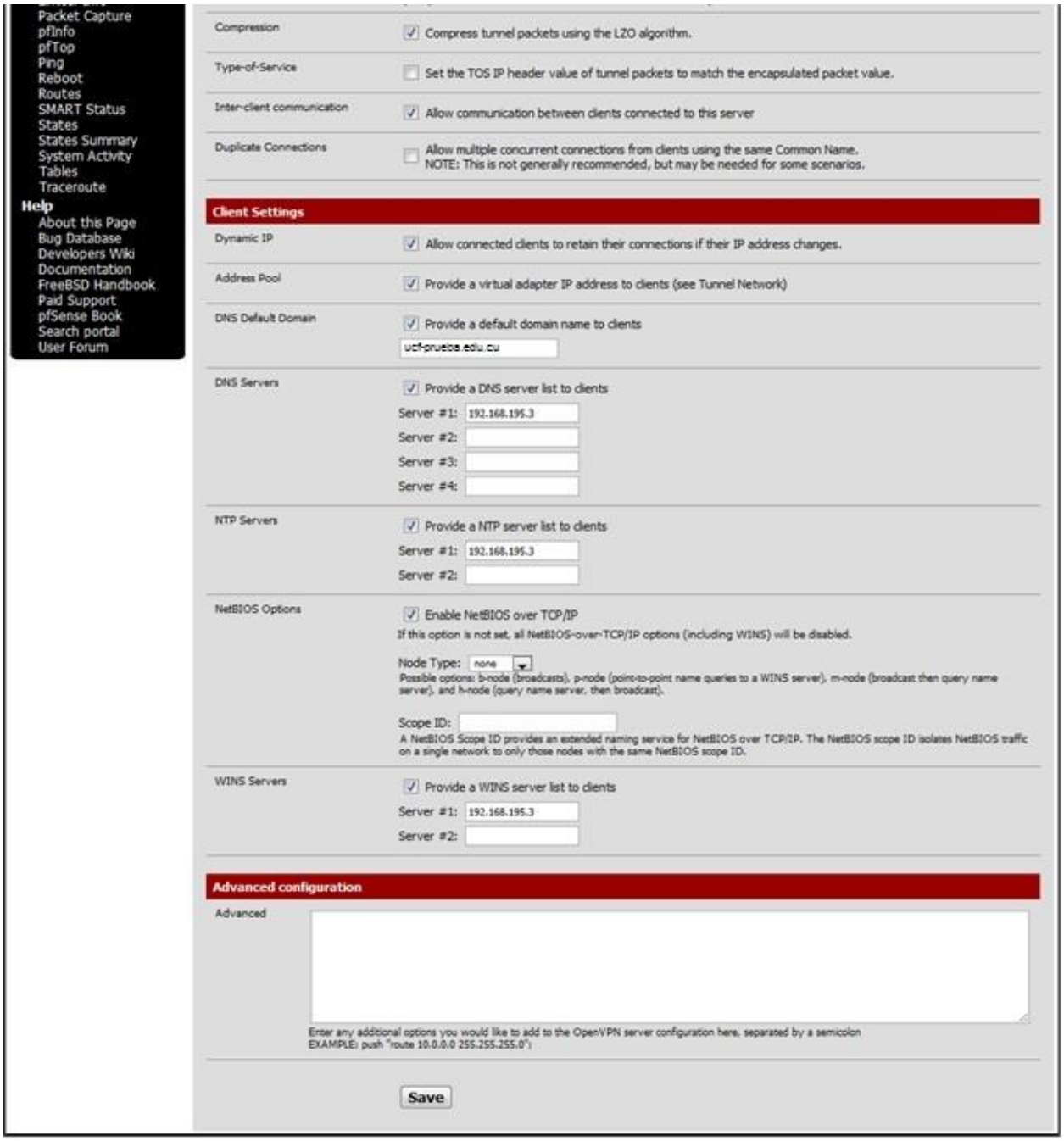

Figura 50. Configuración del servidor de OpenVPN (parte 2).

Figura 51. Regla en el Firewall para la OpenVPN.

Anexo H. Pruebas de conectividad.

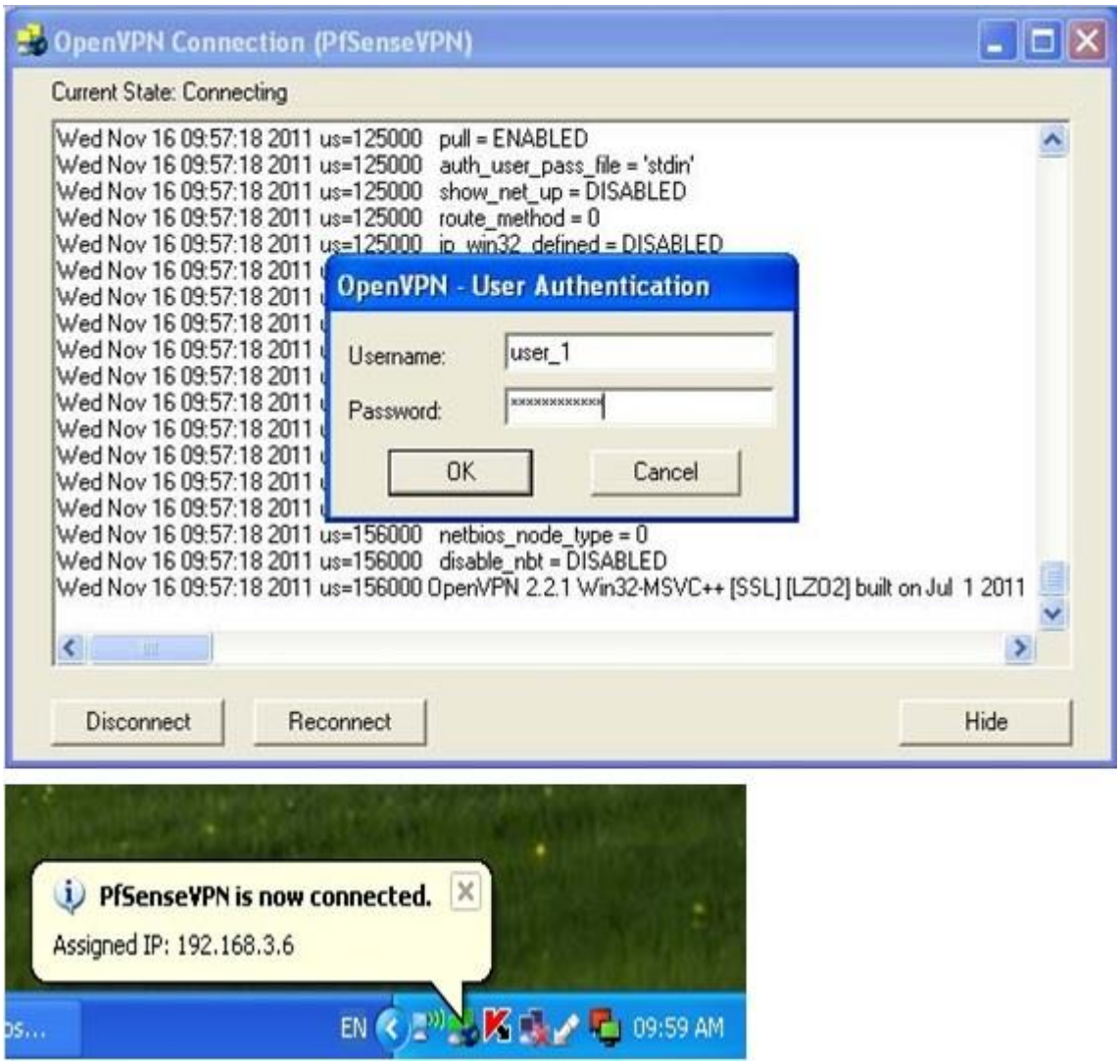

Figura 52. Conexión de un cliente al servidor OpenVPN de PfSense.

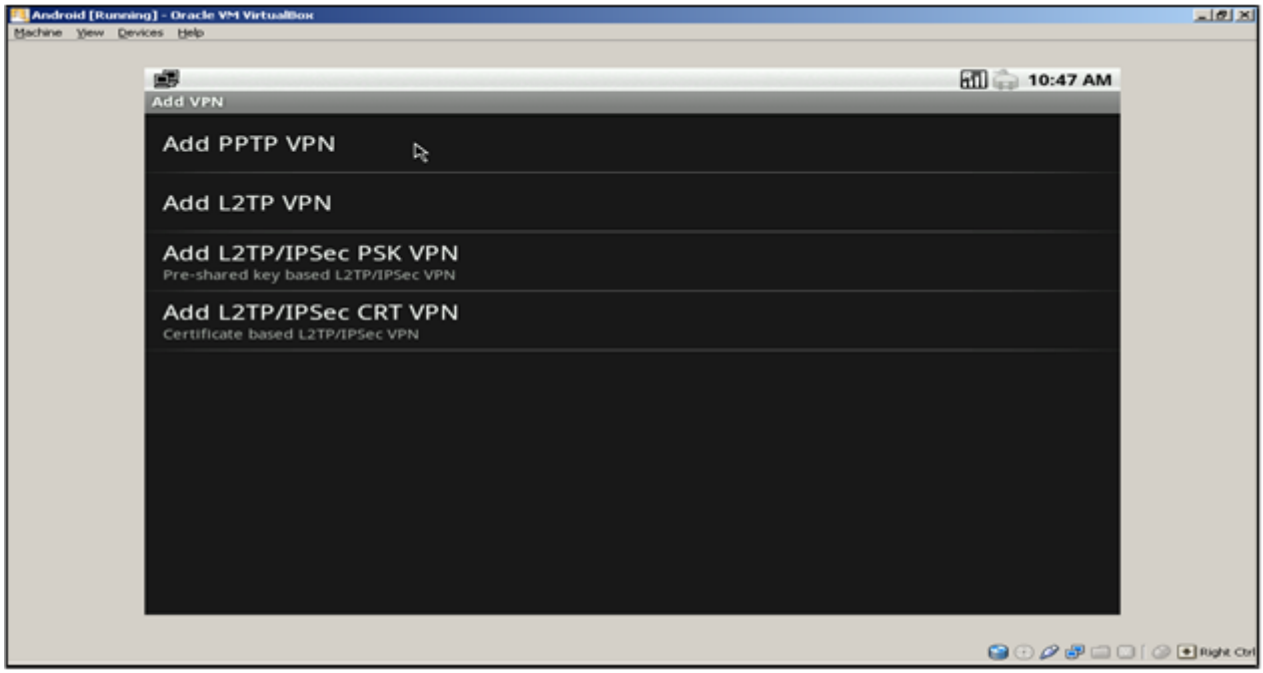

Figura 53. Clientes VPN disponibles en el SO Android 1.6

Figura 54. Ventana de autenticación del cliente VPN del SO Android 1.6 ejecutándose en una VM.