UNIVERSIDAD NACIONAL DE SAN MARTÍN - T

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

"SEGURIDAD Y CONTROL DEL ACCESO A LAS REDES INALÁMBRICAS EN LA UNSM-T MEDIANTE SERVIDORES DE AUTENTIFICACIÓN RADIUS CON EL USO DE CERTIFICADOS DIGITALES".

Para optar el Título de:

INGENIERO DE SISTEMAS E INFORMÁTICA

Presentado por el Bachiller

Jhony Fermin Blas Rinza.

Tarapoto -Perú

2017

UNIVERSIDAD NACIONAL DE SAN MARTÍN - T

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

SEGURIDAD Y CONTROL DEL ACCESO A LAS REDES INALÁMBRICAS EN LA UNSM-T MEDIANTE SERVIDORES DE AUTENTIFICACIÓN RADIUS CON EL USO DE CERTIFICADOS DIGITALES.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO DE SISTEMAS E INFORMÁTICA

Presentado por:

Bachiller : Jhony Fermin Blas Rinza

Asesor : Ing. Mg. Miguel Ángel Valles Coral

SUSTENTADO Y APROBADO ANTE EL HONORABLE JURADO:

Presidente : Ing. M.sc. Jorge Damián Valverde Iparraguirre

Secretario : Ing. M.sc. Miguel Angel Rengifo Arias

Miembro : Ing. Alberto Alva Arévalo

DEDICATORIA

A mis padres**: Ludith Rinza Cardenas y Arcadio Blas lopez**, por su apoyo incondicional y aliento en los momentos difíciles a lo largo de la realización de mi carrera Profesional y de mi vida.

A Dios, por ser mi guía en todo momento, y por ponerme en el camino de aquellas personas que han contribuido grandemente en mi carrera, y en formarme como persona.

GRACIAS SEÑOR.

AGRADECIMIENTO

Al Ing. **Miguel Ángel Valles Coral**, por el apoyo esmerado y paciencia en la asesoría del desarrollo de mi proyecto de tesis.

A mis familiares y mis amigos quienes me brindaron su apoyo moral para lograr culminar con éxito este gran proceso que forma parte de mi desarrollo como profesional.

RESUMEN

La presente tesis trata sobre la necesidad de mejorar los niveles de seguridad en el acceso a la red de datos de la Ciudad Universitaria de la UNSM-T a través de la red inalámbrica disponible en la misma.

En el capítulo I, se identifica el problema, sus causas y consecuencias, así como el estado del arte con un marco teórico que entre otras cosas conceptualiza las variables identificadas en la operacionalización de variables con la finalidad de tener el suficiente conocimiento para abordar la problemática identificada.

El capítulo II, nos habla sobre materiales y métodos relacionados con la hipótesis, el ámbito geográfico y el diseño utilizado en la investigación, procedimientos y técnicas, así como instrumentos utilizados durante la ejecución de la investigación.

El capítulo III, muestra los resultados de la investigación, se discuten los mismos y se contrastan con los antecedentes de la investigación identificados y referenciados.
El capítulo IV, finalmente muestra las conclusiones y recomendaciones que como investigador tesista realizo a fin de que se mejore la seguridad en el acceso a las redes inalámbricas de la ciudad universitaria de la Universidad Nacional de San Martín-Tarapoto.

SUMMARY

This thesis addresses the need to improve safety levels in access to the data network of the University City of UNSM-T through the available wireless network in it.
In Chapter I, the problem, its causes and consequences, as well as the state of the art with a theoretical framework that among other things conceptualizes the variables identified in the operationalization of variables in order to have sufficient knowledge to address the problems identified identified.

Chapter II, talks about materials and methods related to the hypothesis, the geographical scope and design used in research, procedures and techniques and instruments used during the execution of the investigation.

Chapter III shows the results of the investigation, they are discussed and contrasted with the background of the research identified and referenced.

Chapter IV finally shows the conclusions and recommendations as tesista research conducted so that security is improved access to wireless networks campus of the National University of San Martin-Tarapoto.

ÍNDICE

NOMENCLATURAS

a) Lista de cuadros.

b) Lista de figuras.

c) Lista de siglas, abreviaturas y símbolos.

- **AP** Access Point, Punto de Acceso
- **AES** Advanced Encryption Standard, es un esquema de cifrado por bloques adoptado como un estándar de cifrado
- **AAA** Autentificación, Autorización y Contabilidad
- **ATA** Advanced Technology Attachment, Tecnología Avanzada de Contacto
- **DNS** Domain Name Service, Servicio de Nombres de Dominio
- **DHCP** Dinamic Host Configuration Protocol
- **EAP** Protocolo de autentificación extensible
- **LDAP** Lightweight Directory Access Protocol, Protocolo Ligero de Acceso a Directorios
- **MD5** Message-Digest Algorithm 5
- **RADIUS** Remote Authentication Dial-In User Service
- **RFI** Request For Information
- **RFC** Request for Comment
- **SSL** Secure Socket Layer, Nivel de Zócalo Seguro
- **SHA** Secure Hash Algorithm

- **SSID** Service Set IDentifier
- **TLS** Transport Layer Security, Seguridad para Nivel de Transporte
- **TKIP** Protocolo de integridad de clave temporal
- **TCP** Transmission Control Protocol, Protocolo de Control de Transmisión
- **Wifi** Wireless Fidelity, Fidelidad Inalámbrica es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica
- **WEP** Wired Equivalent Privacy, Privacidad Equivalente a Cableado, además es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite.
- **WPA** Wi-Fi Protected Access, Acceso Protegido Wi-Fi

INTRODUCCIÓN

El objetivo del presente trabajo es plantear una plataforma de seguridad para el acceso inalámbrico al servicio de internet la UNSM-T., de tal forma que se permita mejorar el control de acceso a las redes inalámbricas a través de la implementación de servidores de acceso inalámbrico basados en protocolos de seguridad avanzados como lo es Radius.

Para ello se plantea la interrogante ¿es posible mejorar la seguridad y el control de acceso a las redes inalámbricas en la UNSM-T mediante servidores de autentificación radius con el uso de certificados digitales?

El problema radica en las deficiencias en cuanto al control de acceso a las redes inalámbricas existentes en la Ciudad Universitaria, ya que son redes sin ningún tipo de seguridad, lo cual la hace muy vulnerable a ataques contra los diferentes recursos existentes como pueden ser servicios, equipos, servidores, etc.

Además de lo mencionado líneas arriba, esta deficiencia en el control de acceso a las redes inalámbricas existentes en la Ciudad Universitaria de la Universidad Nacional de San Martín - Tarapoto, repercute sobre el rendimiento de la red, que si bien no forma parte del presente estudio, la propuesta permitirá mejorar este rendimiento.

Se revisa entonces el estado del arte a fin de evaluar las propuestas teóricas que se pueden utilizar en este sentido, además de antecedentes que sirvan como ejemplo de cómo trabajar la propuesta.

Al final se evalúa el impacto de los servidores de acceso inalámbrico basado en protocolos de seguridad avanzados sobre la mejora de la seguridad y el control de acceso a las redes inalámbricas en la UNSM-T.

CAPÍTULO I

I. EL PROBLEMA

1.1 Antecedentes del problema.

Siendo la Universidad Nacional de San Martín – Tarapoto, la institución de educación superior más importante de la Región San Martín y estando en la obligación de brindar las mejores condiciones para el correcto desarrollo de las actividades académicas, administrativas y de investigación, ha mejorado las condiciones de la infraestructura de comunicación existente.

La mejora ha repercutido en las facilidades de acceso a los servicios de comunicación de la Universidad, a través del cual se utilizan múltiples servicios, principalmente Internet y sus servicios relacionados (búsquedas, correo electrónico, ftp, etc.).

Todos los docentes, administrativos y estudiantes que poseen un equipo con funcionalidades para el acceso a redes inalámbricas, pueden conectarse a la red de la Universidad a través de las redes inalámbricas, lo que ha incrementado la demanda de ancho de banda por el indiscriminado uso del servicio y el deficiente control de la seguridad.

Considerando que el acceso a la red de datos (Internet), se realiza a través de una línea dedicada de 45 megas, las condiciones para un acceso de calidad a Internet desde la red Lan está garantizado, sin embargo la elevada demanda en horas punta afecta esta característica, por lo que es necesario implementar políticas de seguridad más avanzados.

1.2 Definición del problema.

La Universidad Nacional de San Martín –Tarapoto, es una institución universitaria formadora de profesionales competitivos para la sociedad, que genera innovación de conocimientos y fortalece la cultura y los valores, que está en proceso de acreditación.

Durante estos años se ha preocupado por mejorar su infraestructura de comunicaciones, implementando por ejemplo una red de datos en la Ciudad Universitaria que interconecta sus edificios con backbone de fibra óptica, la misma que es única a nivel de la macro región, convirtiéndola en pionera, llevando la

vanguardia de los adelantos tecnológicos permitiendo el desarrollo académico y la investigación.

Gracias a ello, y a una fuerte política académica destinada a brindar facilidades a los estudiantes para el desarrollo de sus clases, que incluye la adquisición de una infraestructura de acceso inalámbrico, se puede brindar a internet a la comunidad universitaria en su conjunto para que realicen sus actividades académicas y administrativas de manera adecuada.

He allí entonces la importancia de la infraestructura de comunicaciones dentro la Ciudad Universitaria, puesto que permite garantizar la continuidad de la operativa diaria. Sin embargo ha de mencionarse que la demanda del servicio de internet supera largamente la oferta (la demanda identificada requiere 95 megas de acceso y sólo se cuenta con 45 megas), por lo que el servicio muchas veces llega a saturarse presentando inconvenientes a los usuarios finales debido principalmente a las deficientes políticas y procedimientos para el control del acceso a la red inalámbrica para hacer uso del internet de la UNSM-

Al revisar en sí las causas del problema, se puede mencionar que la autenticación y autorización para el acceso al servicio no está adecuadamente configurada, impidiendo la posibilidad de controlar los límites de uso en ancho de banda y cuotas de transferencia para un uso más racional del servicio.

Al no tener unas adecuadas políticas de autenticación y autorización, así como también asignación de cuotas de la red, esto perjudica de manera continua las operaciones, haciendo que en muchas veces el servicio de la línea de internet sea un poco deficiente.

Así mismo debido a este problema en el cual se enfoca la investigación, es notable identificar consecuencias como el de la saturación de ancho de banda del servicio de internet, así como también posibles violaciones a la seguridad de la red, de tal forma que se esto repercuta en la calidad de servicio para los usuarios que hacen uso del internet.

1.3 Formulación del problema.

¿Es posible mejorar la seguridad y el control de acceso a las redes inalámbricas en la UNSM-T mediante servidores de autentificación radius con el uso de certificados digitales?

1.4 Justificación e importancia.

De la conveniencia

La presente tesis de investigación servirá para mejorar la seguridad y control del acceso a las redes inalámbricas, de la misma manera nos ayudará a optimizar los recursos de la red y tener un mejor control de uso del ancho de banda.

De la Relevancia Social

Esto a su vez beneficiara a los usuarios que hagan uso del servicio de internet, reduciendo los problemas de saturación del ancho de banda.

De Las Implicancias Prácticas

De la misma manera se podrá tener el control o administración de los usuarios mediante políticas de asignación de cuotas.

Del Valor Teórico

El uso de Certificados Digitales resuelve problemas de seguridad pues este proporciona un sistema más robusto y seguro dentro de la red.

De La Utilidad Metodológica

Finalmente con la implementación del Servidor de autentificación de certificados digitales en las redes inalámbricas se pretende incrementar los niveles de seguridad en el ingreso, al mismo tiempo que se quiere mantener un control más directo sobre los usuarios que se conecten a dicha red.

1.5 Alcance y limitaciones

La trascendencia de la investigación radica en permitir y concienciar a los profesionales de la información, sobre la seguridad y acceso a las redes inalámbricas, el mismo que abarcara la red de datos de la de la Universidad Nacional de San Martín.

II. MARCO TEÓRICO

2.1 Antecedentes de la investigación.

2.1.1 Tesis Internacionales

Según (Mauricio, 2010) en su tesis “Diseño e implementación de arquitectura de conectividad y seguridad AAA en UDNET (authentication, authorization and accounting)” indica que este proyecto consiste en el análisis, diseño e implementación de una arquitectura de conexión y seguridad denominada AAA. Para que AAA funcione necesita configurar un protocolo base, el cual puede ser TACACS+ o RADIUS. TACACS+ es un protocolo patentado por CISCO, por lo cual requiere: que todos los equipos sean CISCO y pagar el precio que exigen para permitir la utilización de este protocolo. RADIUS es de libre uso y no tiene ninguna limitante con respecto al fabricante de los equipos donde se vaya a implementar.

Según (Gomez, 2007), en su tesis Arquitectura Unificada para Control de Acceso en Redes Inalámbricas Seguras, de la Universidad de Mendoza. Dice: La implementación de redes inalámbricas en ámbitos semi públicos constituye uno de los desafíos no resueltos en la actualidad. Al contrario de los ámbitos puramente corporativos, en escenarios de este tipo, los administradores no pueden definir las características de conectividad de los dispositivos inalámbricos que poseen los usuarios. Adicionalmente es muy frecuente la necesidad de diferenciar el tipo de servicios que se brindan de acuerdo a las necesidades de distintos grupos de usuarios. En efecto, en general cada protocolo o método de acceso resuelve una parte del problema, y generalmente de manera excluyente; por lo tanto no permite la integración de soluciones diferentes sobre los mismos equipos en simultáneo.
Estas necesidades plantean la conveniencia de solucionar una problemática que no es cubierta por ninguno de los protocolos inalámbricos existentes en la actualidad.

2.1.2 Tesis Nacionales

Según (Lazo, 2012), en su tesis “DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN Y WLAN CON SISTEMA DE CONTROL DE ACCESO MEDIANTE SERVIDORES AAA”, dice la presente tesis consiste en el diseño e implementación de una red LAN (Local Area Network) y WLAN (Wireless Local Area Network) con sistema de control de acceso AAA (Authentication, Authorization and Accounting). El primer paso fue

implementar una red LAN utilizando el mecanismo Etherchannel y el protocolo de balanceo de carga en la puerta de enlace GLBP (Gateway Load Balancing Protocol) para optimizar el uso de recursos de la red. Luego se implementó el servidor ACS (Access Control Server) que utiliza el protocolo TACACS+ para centralizar el acceso de los administradores de los equipos de la red.

Según (Molina, 2012), en su tesis "Propuesta de segmentación con redes virtuales y priorización del ancho de banda con qos para la mejora del rendimiento y seguridad de la red lan en la empresa editora el comercio planta norte", indica el presente trabajo plantea una propuesta de Segmentación con Redes de Áreas Locales Virtuales (VLAN's) y priorización del Ancho de Banda con Calidad de Servicio (QoS) para la mejora del Rendimiento y Seguridad de la Red de Área Local (LAN) en la Empresa Editora El Comercio – Planta Norte.
La empresa Editora El Comercio – Planta Norte posee una red plana en su diseño lo cual dificulta la administración del tráfico de la Red, debido a la ausencia de estándares de calidad en gestión de tráfico LAN, políticas de seguridad no alineadas a las necesidades de la empresa y desaprovechamiento de la performance de los equipos de comunicación instalados.
Correlación: Coincide en el propósito del uso de ciertos estándares en cuanto a tecnología para interconectar sobre una LAN extendida varios nodos, de tal forma de asegurar la disponibilidad del enlace y mantener una adecuada performance. Aquí tomamos en cuenta la experiencia en la determinación y estimación del ancho de banda ideal en función al tipo de información a transferir o compartir entre los puntos que se interconectan; en base a este ancho de banda y la necesidad de la disponibilidad de la red se selecciona la alternativa entre las diferentes tecnologías existentes. El criterio de priorizar el ancho de banda en función al tipo de información nos da la idea del uso de QoS.

2.1.3 Tesis Locales

Según (Morales, 2013), en su tesis "Mejora de la comunicación a través de una red integral corporativa de información entre los locales descentralizados de la municipalidad provincial de alto amazonas- yurimaguas" tiene como Objetivo General, Mejorar la comunicación entre los locales descentralizados de la

Municipalidad Provincial de Alto Amazonas-Yurimaguas a través de una Red Integral Corporativa de Información que permita una eficiente y oportuna información entre las diversas Gerencias y/o áreas de la entidad para su mejor desempeño hacia la población..

Correlación: Coincide en el propósito del uso de ciertos estándares en cuanto a tecnología para interconectar sobre una LAN extendida que ayude a tener una calidad eficiente y segura en cuanto a administración de usuarios se refiere.

Según (Carrasco, 2013) en su tesis "Optimización del ancho de banda de internet y mejora de la seguridad aplicados a la red de datos en la Universidad Nacional de San Martín" indica: Este proyecto de investigación tiene como objetivo general Incrementar el rendimiento del ancho de banda y la seguridad de la red de datos de la Universidad Nacional de San Martín – Tarapoto.

Correlación: Guarda mucha correlación y coincide con el propósito del uso de ciertos estándares en cuanto Definir las listas de control de acceso que determinen los límites de uso de los servicios relacionados a internet utilizados en la red de datos de la Universidad Nacional de San Martín.

2.2 Definición de términos.

Radius:

Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

DHCP:

Llamada protocolo de configuración dinámica de host, es un protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. Así los clientes de una red IP pueden obtener sus parámetros de configuración automáticamente.

Protocolo AAA:

En seguridad informática, el acrónimo AAA corresponde a un tipo de protocolos que realizan tres funciones: autenticación, autorización y contabilización (en inglés, Authentication, Authorization and Accounting). La expresión protocolo

AAA no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados.

Wlan:

Una red de área local inalámbrica, también conocida como WLAN (del inglés wireless local area network), es un sistema de comunicación inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de éstas. Usan tecnologías de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas.

Carretera de comunicación:

"Carrtera de la comunicacion" fue un término popularizado durante la década de 1990 para referirse a la red de los sistemas de comunicaciones digitales y telecomunicaciones asociadas y orientadas al transporte global de información y conocimiento

TACACS:

Es un protocolo de autenticación remota, propietario de cisco, que se usa para comunicarse con un servidor de autenticación comúnmente usado en redes Unix. TACACS permite a un servidor de acceso remoto comunicarse con un servidor de autenticación para determinar si el usuario tiene acceso a la red.

Backbone de fibra óptica:

La palabra backbone se refiere a las principales conexiones troncales de Internet. Están compuestas de un gran número de routers interconectados comerciales, gubernamentales, universitarios y otros de gran capacidad que llevan los datos a través de países, continentes y océanos del mundo mediante cables de fibra óptica.

Networking:

Es acudir a actividades y eventos con el fin de incrementar su red de contactos profesionales y buscar oportunidades de negocio.

Nodos:

En informática y en telecomunicación, de forma muy general, un nodo es un punto de intersección, conexión o unión de varios elementos que confluyen en el mismo lugar

Topología de red:

La topología de red se define como el mapa físico o lógico de una red para intercambiar datos.

Radio enlaces:

Se denomina radio enlace a cualquier interconexión entre los terminales de telecomunicaciones efectuados por ondas electromagnéticas.

Línea de vista:

La propagación de la línea de visión se refiere a la radiación electromagnética o a la propagación de ondas acústicas.

Tasa de transferencia:

En informática y telecomunicaciones, el término tasa de bits (en inglés: bit rate), a menudo tasa de transferencia, define el número de bits que se transmiten por unidad de tiempo a través de un sistema de transmisión digital o entre dos dispositivos digitales.

Dominio de colisión:

Un dominio de colisión es un segmento físico de una red de computadores donde es posible que las tramas puedan "colisionar" (interferir) con otros. Estas colisiones se dan particularmente en el protocolo de red Ethernet.

Dominio de broadcast:

Un dominio de difusión o broadcast es una red lógica de dispositivos que comparten básicamente la misma subred y la misma puerta de enlace.

Segmento de red:

Segmento de red es un sinónimo de LAN: es un conjunto de equipos (computadoras y periféricos) conectados en red.

VLan:

Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

Paquetes de datos:

Paquete de red o paquete de datos es cada uno de los bloques en que se divide la información para enviar, en el nivel de red

QoS:

QoS o Calidad de Servicio (Quality of Service, en inglés) es el rendimiento promedio de una red de telefonía o de computadoras, particularmente el rendimiento visto por los usuarios de la red. Cuantitativamente mide la calidad de los servicios

que son considerados varios aspectos del servicio de red, tales como tasas de errores, ancho de banda, rendimiento, retraso en la transmisión, disponibilidad, jitter, etc.

WLAN:

Una red de área local inalámbrica, también conocida como WLAN (del inglés wireless local area network), es un sistema de comunicación inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de éstas.

Active Directory:

Active Directory (AD) es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos (principalmente LDAP, DNS, DHCP, Kerberos...).

Intranet:

Una intranet es una red informática que utiliza la tecnología del Protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización.

TCP/IP:

El modelo TCP/IP describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red.

2.3 Bases teóricas

Generalmente para la implementación correcta de este proyecto se requería acumular ciertos conceptos e información que representen una fuente importante de datos de las que se pueda extraer requisitos fundamentales de los procesos de autenticación radius considerando principalmente que los conceptos que vimos en el transcurso de este proyecto fueron documentos relacionados con la implementación de mecanismos de seguridad para el control de acceso en redes inalámbricas.

2.3.1 Autenticación segura, control de acceso y privacidad de datos en redes inalámbricas.

Según (Pellejero, Andreu, & Lesta, 2006). Las empresas valoran cada día más la posibilidad de migrar a redes inalámbricas (WLANs). Los usuarios quieren

cada vez más tener acceso a redes inalámbricas en cualquier momento, en cualquier lugar; los administradores de sistemas (IT Managers) no se pueden resistir a la facilidad y flexibilidad de su instalación, así como beneficiarse de los ahorros más que demostrables a largo plazo que su implementación reporta.

Sin embargo, la seguridad ha sido hasta ahora el reto para los fabricantes de equipamiento inalámbrico más difícil de rebatir, siendo el obstáculo más generalizado a la hora de implementar redes inalámbricas.

La última especificación 802.1x provee un completo roadmap para la implementación de elementos óptimos de seguridad en redes WLAN. No sorprende que un servidor de autenticación juego un rol muy importante en la seguridad en una red WLAN basada en 802.1x. Además, los nuevos métodos de seguridad proveen de una autenticación potente además de técnicas de privacidad de datos para asegurar completamente las redes inalámbricas.

- Define los aspectos específicos que caracterizan la seguridad en redes WLAN, y describe como 802.1x los acomete.
- Describe las reglas de un servidor de autenticación y los métodos de seguridad tales como EAP-TTLS (Extensible Autentication Protocol Tunneled Transport Layer Security) en WLANs securizadas
- Demuestra como los softwares de seguridad WLAN de Funk Software Odyssey y Steel-Belted Radius, ambos basados en 802.1x cubren la Funcionalidad y los requerimientos de prestaciones que debe tener un entorno seguro WLAN.

2.3.2 Beneficios de las redes WLANS

La demanda de acceso a redes WLAN se ha incrementado notablemente en los últimos meses.

Los usuarios demandan de accesos a redes inalámbricas porque les permite acceder a sus redes y a Internet en cualquier parte del lugar de trabajo, sin la necesidad de tener que “engancharse /enchufarse /conectarse”.

A los IT Managers les atrae las redes WLANs porque ellos consideran que son más fáciles de instalar (no hay que tirar cables y traspasar ni suelos ni paredes, ni techos), son redes flexibles (se pueden instalar en lugares donde no es posible hacerlo con redes cableadas, y no es necesario recablear cuando se produce un cambio de un empleado de sitio o de replanteó total de una oficina), y además, en

parte gracias a esta flexibilidad, estas redes son menos caras de mantener en el largo plazo.

Por estas razones, los expertos dan expectativas al mercado WLAN de un crecimiento continuado, incluso en el caso de una recesión de la economía. Cahners estima que la facturación de redes WLAN alcanzará los 4.6 billones de dólares en el año 2005; actualmente las redes WLANs ya tienen una penetración significativa en sectores como Educación, Hospitales, Banca, e Industria; además de que cada vez más se están produciendo bajadas de precios en el equipamiento lo que ayudará a que se adopte esta tecnología en otras industrias. Incluso los propietarios de localizaciones públicas, lo que la industria conoce como hot spots, están entrando en el mercado. Ciber cafés, salas de aeropuertos, librerías, son solo unos pocos ejemplos de localizaciones que están ofertando accesos inalámbricos a sus clientes.

2.3.3 Arquitectura de las redes WLAN y retos en la seguridad.

Como en cualquier cambio de tecnología, la migración de los usuarios a redes WLANs tiene sus objeciones. La inversión inicial en hardware puede ser significativa y según como fastidiosa ya que las empresas tendrán que desplegar varios puntos de acceso, y equipar a cada usuario con tarjetas de redes inalámbricas cuando la mayoría de ellos ya tienen buenas tarjetas de red integradas en las redes cableadas.

Pero a pesar de todo esto, la principal preocupación para migrar a una red WLAN es la seguridad. Los cables físicos se convierten en uno de los primeros obstáculos para los hackers que quieren violar una red. Es poco probable que un extraño que se conecte a una red corporativa pase desapercibido, tanto si la seguridad de la red está puesta en marcha o por la proximidad de los usuarios autenticados en la red que estén cerca del “hacker”.

En una red WLAN, los credenciales y los datos de los usuarios se transmiten en dos sentidos: desde el cliente hacia el punto de acceso inalámbrico (AP) y viceversa en un radio que puede alcanzar los 100 metros o más.

El hecho de que los datos se transmitan vía radio en vez de que se transmitan a través de un cable, introduce retos en la seguridad:

- ¿Cómo se puede prevenir que las credenciales de los usuarios puedan ser interceptadas en el momento de la autenticación?
- Una vez que se ha completado la autenticación, como se puede proteger la privacidad de los datos que se transmiten entre el cliente y los Aps?
- ¿Cómo se puede estar seguro de que solo usuarios autorizados se conecten a la red correcta?

2.3.4 Métodos de seguridad y control de acceso a las redes

2.3.4.1 Autenticación

La mayoría de los protocolos basados en passwords en uso hoy en día dependen de lo complicada que sea la password que utilice el usuario. El Servidor provee de intentos de validación hacia el usuario solicitando una password que el cliente envía al servidor, validando éste la respuesta por parte del usuario contra dicha password que se encuentra en una base de datos. Esta aproximación de carácter general se describe en CHAP, MS- CHAP, MS-CHAP-V2, EAP/MD5-Challenge y en EAP/One Time Password.

El problema de esta aproximación es que si una persona no autorizada observa el proceso de envío y respuesta puede montar lo que se llama un diccionario de ataque, en el cual passwords aleatorias se testean contra las validaciones enviadas por los usuarios hacia los servidores para tratar de averiguar cuáles son las respuestas correctas. Ya que normalmente las password tienen poca entropía, con estos ataques puede ser sencillo descubrir muchas passwords.

Mientras que esta vulnerabilidad ya ha sido bien entendida, no se le da importancia en entornos donde los ataques de personas no autorizadas se pueden producir, aunque sean poco probables. Por ejemplo, en conexiones en redes cableadas a través de software de dialers (dial-up) usando sus proveedores de servicio, los usuarios no le dan importancia de que estas conexiones puedan ser monitorizadas. Los usuarios tienen buena voluntad al confiar sus passwords a los proveedores de servicios, o al menos permitiéndoles a éstos chequear el proceso de envío y respuesta de passwords ya que los proveedores de servicio reenvían estas passwords a sus servidores locales de autenticación usando, por ejemplo, servidores RADIUS, sin que el usuario se preocupe de que los proveedores de servicio puedan montar diccionarios de ataque que puedan usar sobre las credenciales de usuario

que están observando. Lo que sucede es que un usuario típico tiene relación con un único proveedor de servicio, por lo que este grado de confianza es enteramente aceptable.

Sin embargo, con el advenimiento de las redes inalámbricas, esta situación cambia dramáticamente. El legado al que predispone los protocolos de passwords, está sujeto a los usuarios no deseados además de los tipos que aparecen en medio de los ataques (“espías”). Un intruso que ataque una red inalámbrica puede montar un diccionario de ataque contra dichos protocolos de passwords. Además, el espía puede saltarse la autenticación íntegra, apropiarse de la conexión y actuar como si fuera un usuario.

2.3.4.2 Privacidad de los datos

Otro asunto es la seguridad de la conexión de datos entre el cliente y el AP después de la autenticación. Aunque los clientes pueden negociar claves después de dicha autenticación, si las claves no se encriptan relacionándose a la autenticación efectuada anteriormente,, la sesión de transferencia de datos podría estar sujeta a espías. Por lo tanto es incumbencia en el proceso de la autenticación el disponer de claves que se puedan distribuir entre los clientes y los Aps que permitan que la subsiguiente conexión de datos se pueda encriptar.

2.3.4.3 Puntos de acceso no permitidos

El último reto de seguridad surge de la posibilidad que alguien se le ocurriese instalar un punto de acceso no permitido en la red inalámbrica que le permitiese trabajar en la misma. Aunque esta situación es poco probable ya que las técnicas de autenticación mutua lo impiden bastante (donde el cliente inalámbrico autentifica la red a la que está conectado), no se debería de echar en el olvido.

2.3.5 Las primeras implementaciones de las redes WLAN

Las primeras implementaciones (diseñadas inicialmente para uso en el hogar), hacían poco por resolver estos problemas de seguridad. El 802.11b, publicado en 1999, fue la primera especificación IEEE que perfiló las especificaciones y protocolos de las redes inalámbricas con su equivalente en velocidad y seguridad en las redes cableadas. Conocidas mayoritariamente como Wi-Fi (wireless fidelity), 802.11b provee de ratios de transmisión inalámbricos de 11 Mbps.

En las soluciones WLAN 802.11b, la autenticación de los usuarios se producía de una manera muy transparente, vía el direccionamiento único del dispositivo inalámbrico MAC (Media Access Control). Cada AP contiene una base de datos con cada uno de las direcciones MAC de los clientes autorizados. Si la dirección MAC del cliente está presente en la base de datos del AP, al usuario se le permitía el acceso a la red. Esto, por supuesto, deja la dirección MAC del usuario expuesta a cualquiera que "esnife" la red podría ver una dirección MAC válida que se esté transmitiendo. (y, por lo tanto, redefinir su propio dispositivo a esa dirección). Además, si el dispositivo del cliente lo robaban, el "nuevo cliente" disponía de todas las credenciales necesarias para acceder a la red (sin tener que saber un nombre de usuario y una password o ser un invitado a conectarse a dicha red inalámbrica).

Como adición a los problemas de seguridad que este método introduce, tampoco se escala bien. La dirección MAC para cada usuario se debe de almacenar en cada AP de la red inalámbrica, creando un problema de gestión enorme e incrementando además la posibilidad de lagunas en la seguridad debido a descuidos en la administración que esta gestión conlleva.

La privacidad de datos se proveía vía un sub-protocolo que se llamaba wired equivalent privacy, o WEP, que pretendía proveer del mismo nivel de seguridad que en una red cableada. Así, la primera generación de implementación de WEP no proveía dicho nivel de seguridad que se encuentra en las redes cableadas. En realidad, numerosas publicaciones, una de ellas elaborada por AT&T, demostró de manera muy convincente que WEP era fácilmente crackeable, generando muchas dudas sobre la privacidad de cualquier transmisión de datos inalámbricas.

2.3.5.1 El problema con WEP

En WEP, tanto el cliente como el AP tiene la misma clave de encriptación de 40 bits, (un "secreto compartido" entre ambos). Cuando el cliente intenta autenticarse, el AP provee de intentos de validación, que el cliente retorna, encriptado con la clave y un vector de inicialización de 24 bits (IV) que intenta que la clave sea parcialmente aleatoria, usando el algoritmo de encriptación RC4 PRNG. El AP desencripta la validación y, si coincide con la validación inicial, autentifica al cliente.

La principal vulnerabilidad de WEP resulta de la clave de encriptación que es constante, el pequeño vector IV, y de la alta velocidad de la conexión. Teóricamente, a la velocidad máxima de transmisión (11 Mbps), el sistema se verá forzado a reutilizar un vector IV cada 5 horas; en la práctica, y debido a la disponibilidad de velocidades menores como resultado de tener más tráfico, el sistema todavía garantiza el reutilizar cualquier clave de encriptación cada 24 horas. Ya que la clave de encriptación nunca varía, significa que en el plazo máximo de un día, un hacker puede recolectar 2 paquetes encriptado s con la misma clave, con lo que el hacker puede posteriormente trabajar sobre ellos y obtener la clave de encriptación.

2.3.5.2 La solución 802.1X

802.1 .1x es la siguiente generación de las especificaciones y protocolos de las redes inalámbricas que se han escrito para direccionar la seguridad y los escollos de gestión de 802.11b. El protocolo 802.1x provee de subprotocolos y métodos para proteger de manera más eficiente la autenticación y la transmisión de datos incluyendo:

- **Un proceso de autenticación**, (tal como el servidor RADIUS o la autenticación basada en APs), para manejar la autenticación de usuarios, los atributos de conexión, y otras materias relativas a la definición y seguridad de la conexión inalámbrica. Mientras que el protocolo 802.1x no recomienda un procedimiento de autenticación sobre otro, el mercado ha adoptado por mayoría aplastante RADIUS como el proceso de autenticación preferido para las redes inalámbricas por varias razones:
- **Con RADIUS**, la autenticación se basa en el usuario, no en el dispositivo, así por ejemplo, un portátil robado no implicará una brecha en el sistema de seguridad de la compañía.
- **RADIUS** elimina la necesidad de almacenar y gestionar los datos de autenticación en cada AP de la red inalámbrica, haciendo que la seguridad sea considerablemente más sencilla de gestionar y escalar.
- **RADIUS** ya ha sido ampliamente desplegado para otros tipos de autenticación en la Red (básicamente es el sistema de autenticación que utilizan los operadores de Telefonía móvil.
- **Extensible Autentication Protocol (EAP), y EAPoL (EAP over LAN).**

EAPol es el protocolo de transporte que se usa para negociar la conectividad segura del usuario a la red inalámbrica. La seguridad se maneja por los “tipos de autenticación EAP” desarrollado por diferentes vendedores (Funk, Cisco o Microsoft, por ejemplo) que pueden proteger credenciales de datos, la privacidad de los datos, o ambas cosas.

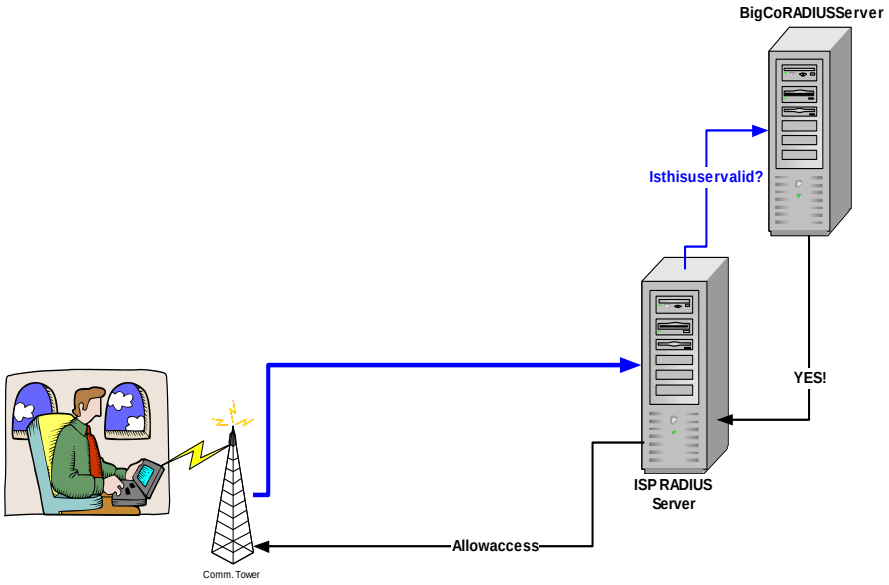


Figura 1. Proceso Autenticación Radius

***Fuente**: Microsoft Corporation, 2001*

2.3.6 Tipos de autenticación EAP

Ya que la seguridad en las redes inalámbricas es absolutamente esencial, y teniendo en cuenta que los tipos de autenticación EAP proveen de las diferentes maneras de conexiones seguras a redes inalámbricas, diferentes empresas están rápidamente desarrollando y añadiendo más tipos de autenticaciones EAP a sus Aps. Algunos de los tipos de autenticación EAP más comunes que se despliegan actualmente son:

- **EAP-TTLS**. Funk Software y Certicom han desarrollado conjuntamente EAP-TTLS (Tunneled Transport Layer Security). EAP-TTLS ofrece los beneficios dobles de la seguridad extrema que da el link inalámbrico, además de ser

muy fácil de definir y gestionar. EAP-TTLS es una extensión de EAP-TLS que provee a la certificación, autenticación mútua del cliente y la red. A diferencia de EAP-TLS, sin embargo, EAP-TTLS solo requiere certificados de la parte del servidor, eliminando la necesidad de configurar cada cliente inalámbrico. Además, soporta el legado de los protocolos de passwords, por lo que podrá desplegarlos contra su sistema de autenticación actual (tales como tokens o Active Directories). Es una autenticación de cliente tunelizada con registros TLS, asegurando que el usuario permanece anónimo de fisgones del link inalámbrico además de la red entera hacia el servidor RADIUS.

- **EAP-TLS (Transport Layer Security).** EAP-TLS- el método de seguridad usado en el cliente 802.1x en Windows XP, provee una seguridad muy potente, pero requiere que cada cliente de la red inalámbrica ejecute una certificación. Es apropiado generalmente para empresas que ya han desplegado una infraestructura PKI. EAP-TLS provee para la certificación, autenticación mutua del cliente y la red. Para obtener la autenticación, dependerá tanto del cliente como del servidor; el usuario se genera dinámicamente con sesiones basadas en claves WEP que se distribuyen para asegurar la conexión. Windows XP incluye un cliente EAP-TLS.
- **EAP-Cisco Wireless.** También llamado LEAP (Lightweight Extensible Authentication Protocol), este tipo de autenticación EAP se utiliza básicamente en los APs de Cisco, incluyendo la serie Aironet. Aunque es fácil de definir y gestionar, LEAP no provee de fuertes credenciales de seguridad en el link inalámbrico, dejando las credenciales de passwords a merced de los ataques de los diccionarios. Encripta la transmisión de datos usando las claves WEP generadas dinámicamente, y soporta autenticación mútua.

EAP-MD-5 Challenge. El primer tipo de autenticación que se ha implementado en el tiempo, esencialmente duplica la protección de passwords CHAP en una red inalámbrica. EAP-MD5 representa un tipo de soporte entre los dispositivos 802.1x. Debido a las vulnerabilidades conocidas de los sistemas de seguridad, un sistema que depende del dispositivo no es recomendable en empresas muy concienciadas en la seguridad.

Es probable que esta lista de tipos de autenticación crecerá y cada vez más y más vendedores de software entrarán en el mercado de la seguridad de las redes inalámbricas, hasta que el mercado elija un estándar. (Por ejemplo, Cisco y Microsoft presentarán soluciones basadas en EAP-PEAP, un protocolo muy sólido de seguridad inalámbrico que ofrece un subconjunto de las funcionalidades de las que dispone EAP-TTLS.

En general, deberá de evaluar el tipo de autenticación EAP que esté considerando desplegar basándose en las siguientes funcionalidades:

- **Provee de la credencial de seguridad**: El intercambio seguro de información entre usuarios durante el proceso de autenticación previene el robo de credenciales y protege al usuario de la privacidad del sitio donde se encuentre.
- **Permite autenticación mútua del cliente y la red**: La autenticación mútua previene de una intrusión en la red por parte de un usuario no autorizado, asegurando que el cliente se conecta a la red correcta.

- **Requiere ud. de encriptación dinámica de claves:** La generación dinámica de claves, que son diferentes para cada usuario y sesión mejora significativamente las transmisiones de datos seguras entre usuarios.
- **Soporta re-keying:** Re keying es la generación de nuevas claves cada ciertos intervalos de tiempo durante la sesión de un cliente en una red inalámbrica. El re-keying hace que sea virtualmente imposible a un fisgón vulnerar y desencriptar una conexión.
- **Es fácil de manejar:** La facilidad de implementación y gestión es un aspecto crítico, particularmente si ud. está desplegando una red inalámbrica para cientos o miles de usuarios. Por ejemplo, EAP-TLS requiere certificación por parte del cliente, que tendrá que tener que configurar de manera separada para cada red inalámbrica, mientras que EAP-TTLS no requiere certificación por parte del cliente.
- **Puede ud. implementarlo de manera sencilla en su red:** La posibilidad de desplegar seguridad inalámbrica de una manera rápida en la infraestructura existente de su red permite disponer de ella de manera inminente, permitiendo a los usuarios conectarse a la red inalámbrica de la manera a las

que ellos estén acostumbrados. Por ejemplo, EAP-TTLS permite autenticación segura a los usuarios de la red inalámbrica contra las bases de datos de autenticación de Windows.

2.3.6.1 Web en entornos 802.1x

802.1x no se define sobre WEP. Esto hace que 802.1x no provisione ni recomiende un método mejorado que asegure la privacidad de los datos; en realidad, las claves WEP todavía forman parte de una manera básica de la mayoría de las encriptaciones de las conexiones inalámbricas.

Sin embargo, la mayoría de los tipos de autenticación explicados anteriormente, incluyendo EAP-TTLS, elimina los problemas introducidos por el uso de claves estáticas WEP. Cuando cualquiera de estos tipos de autenticación EAP están en uso, los portátiles robados o que se han perdido no presentan un problema serio de seguridad. En cambio, a cada usuario se le solicita una nueva clave como parte del proceso de autenticación cada vez que se conecta; además, las claves nuevas también pueden ser regeneradas cada ciertos intervalos (digamos, cada 10 minutos) durante una sesión de un usuario. En la práctica, este rápido re-keying de las claves WEP resuelve los problemas con WEP. Nuevas técnicas de encriptación se introducirán en el futuro que resolverán los problemas con WEPP en la práctica y en la teoría.

En la mayoría de los entornos 802.1x más comunes, los Aps difieren al servidor RADIUS la autenticación de los usuarios soportando uno de los tipos de autenticación EAP explicados anteriormente. El Servidor RADIUS maneja estas funciones, proveyendo de autenticación crucial y capacidades de protección de datos de acuerdo a los requerimientos de autenticación EAP en uso. Aunque algunos detalles pueden variar de un tipo de autenticación EAP a otro, los siguientes pasos proveen un entorno básico de cómo se hace la transacción entre el cliente de la red inalámbrico y el servidor RADIUS y cómo trabaja éste para definir una conexión inalámbrica segura:

1. El Cliente WLAN (llamado el “Suplicante” en los documentos IEEE) trata de acceder a la red. [EAPoL]
2. El AP (el “Autenticador”) responde a las peticiones, y le pedirá al cliente que se identifique. [EAPoL]

3. El Cliente responde con su identidad al AP. [EAPoL]
4. El AP reenviará la petición de Acceso al servidor RADIUS con la identidad del usuario. [RADIUS]
5. El Servidor RADIUS responderá con una validación al AP. La validación indicará el tipo de autenticación EAP requerido por el servidor. [RADIUS]
6. El AP reenviará la validación al cliente [EAPoL]
7. Si el cliente está de acuerdo con el tipo de EAP, la negociación continuará, si no, el cliente no responderá con un NAK (no está de acuerdo), pidiendo y sugiriendo un método alternativo [EAPoL]
8. El AP pasará la respuesta al servidor RADIUS [RADIUS]
9. Si estas credenciales son correctas, el servidor RADIUS acepta al usuario. Si no, se rechaza al usuario. Una aceptación de Acceso o de Rechazo se envía. [RADIUS]
10. Si la autenticación es un éxito, El AP conecta el cliente a la red.

Ya que los servidores RADIUS juegan un rol central en la seguridad WLAN (Actúan como un agente de autenticación entre el cliente y el AP, proveyendo y reforzando cualquiera de las otras medidas de seguridad que se especifique en el tipo de autenticación EAP); las Empresas están analizando como maximizar el retorno de sus inversiones en WLAN por lo que les piden a los servidores RADIUS que:

- Soporte todos los tipos de autenticación EAP
- Soporten equipamientos de múltiples vendedores, en una WLAN sencilla, así la empresa puede hacer crecer su red inalámbrica añadiendo el equipamiento que cubra sus requerimientos (en vez de estar atados a las soluciones que provea un vendedor particular)
- Ofrezca las prestaciones y la capacidad de transacciones para soportar migraciones a gran escala a redes inalámbricas, así como el incremento de transacciones que acompaña a las técnicas adicionales de seguridad tales como la re-autenticación.

2.3.7 Soluciones Funk software para redes Wlans seguras.

Los Servidores RADIUS de Funk Software (Odyssey y Steel-Belted Radius), están diseñados para proveer de seguridad a los accesos a redes inalámbricas. Dependiendo de sus requerimientos, podrá encontrar que una combinación de

Odyssey y Steel-Belted Radius cubren la máxima funcionalidad y una solución muy efectiva en coste.

- **Odyssey Server:** Odyssey Server es un servido RADIUS especialmente diseñado para manejar controles de accesos y seguridad. Está especialmente indicado para pequeñas empresas o redes autónomas en grandes organizaciones donde el acceso a la red se gobierna por nombres de usuario y passwords Windows. Aparte de permitir autenticación segura a los usuarios de la red inalámbrica contra una base de datos Windows, y definir las conexiones seguras, Odyssey Server se puede comunicar Steel-Belted Radius para autentificar a los usuarios de las redes inalámbricas en oficinas remotas o en departamentos distribuidos contra una infraestructura central de seguridad que puede estar basada o no en Windows.
- **Steel-Belted Radius/Enterprise Edition:** Steel-Belted Radius/Enterprise Edition es el servidor RADIUS líder del Mercado de Funk Software, siendo el único capaz de gestionar accesos y la seguridad de usuarios remotos y de redes inalámbricas. Provee el mismo nivel de seguridad en las redes inalámbricas que provee Odyssey, extendiendo esa capacidad también a los usuarios remotos, asegurando que solo los usuarios autorizados se puedan conectar (si éstos están conectado vía VPN, dial o firewall), recibiendo el nivel apropiado de acceso. Además, Steel-Belted Radius le permite autenticar a sus usuarios remotos y sus redes inalámbricas contra una amplia variedad de sistemas de autenticación back-end incluyendo sistemas de tokens y LDAP (Basado en un almacén de nombres y password). Finalmente, Steel- Belted Radius soporta plenamente accounting RADIUS, por lo que podrá de una manera sencilla controlar y tener documentados los accesos remotos de usuarios así como desde las redes inalámbricas.
- **Steel-Belted Radius/Global Enterprise Edition (GEE):** Steel-Belted Radius/Global Enterprise Edition extiende las posibilidades de Steel-Belted Radius/Enterprise Edition para cubrir las necesidades de gestión de seguridad que necesitan empresas de carácter global que manejan miles de usuarios remotos y usuarios de redes inalámbricos a través de múltiples localizaciones.

Además de ofrecer todas las posibilidades del Steel-Belted Radius/Enterprise Edition, Steel-Belted Radius/Global Enterprise Edition permite distribución sofisticada de peticiones de autenticación y accounting (para manejar fácilmente la gestión centralizada de usuarios lejanos, además de integrar sin ataduras los nuevos usuarios que se necesiten, por ejemplo, como resultado de una fusión entre 2 compañías). Además, soporta características avanzadas de fiabilidad si ud. necesitase tiempo de funcionamiento de la red del 99.999%, fácilmente gestionable desde un sistema de monitorización basado en red SNMP.

Cualquiera que sea el servidor RADIUS de Funk Software apropiado para su red, encontrará que cada uno de ellos ofrece:

- **Soporte para EAP y potentes tipos de autenticación EAP:** soportando los nuevos protocolos que puedan aparecer. Odyssey Server y Steel-Belted Radius soporta los tipos de autenticación EAP, EAP-TTLS, EAP-TLS, y EAP-Cisco Wireless (LEAP)
- **Amplio soporte de múltiples vendors:** Odyssey y Steel-Belted Radius reflejan el amplio soporte de múltiples vendors que siempre acompaña a los productos de Funk Software. Odyssey y Steel-Belted Radius soportan todos los Aps compatibles 802.1x, incluyendo Cisco 802.1x clients que ya tenga desplegado en su organización.
- **Soporte de múltiples tipos de autenticación EAP en una red WLAN sencilla.** Odyssey y Steel-Belted Radius permiten diferentes definiciones de usuarios que usen diferentes tipos de autenticación EAP, en la misma WLAN. Esto le proporciona al administrador de la WLAN la flexibilidad de variar el equipamiento basándose en las necesidades de seguridad de cada uno de los usuarios.(y así construir la red inalámbrica en cualquiera de las formas que mejor cubra aspectos de seguridad global, prestaciones y objetivos presupuestarios).

Además, cuando EAP-TTLS está en uso, Odyssey y Steel-Belted Radius proveen de beneficios de gestión muy convincentes, haciendo que sea la forma más sencilla de solución segura 802.1x que se puede desplegar en una empresa.

- **Seguridad insuperable:** Odyssey y Steel-Belted Radius emplea técnicas avanzadas de seguridad, tanto durante el proceso de autenticación del usuario como durante la sesión para prevenir accesos no autorizados a su

red, además de evitar fisgones en la conexión.

EAP –TTLS permite a los usuarios ser autenticados en la red WLAN con sus credenciales de passwords actuales, y, usando una potente criptografía de claves públicas/privadas, para proteger a estas passwords contra fisgones y otros ataques que de repente se puedan producir por el advenimiento de las comunicaciones inalámbricas.

Y, Odyssey y Steel-Belted Radius generan claves dinámicas por sesión para encriptar la conexión inalámbrica y proteger la privacidad de los datos. Odyssey y Steel-Belted Radius se pueden configurar para hacer re- autenticación y así re-key en cualquier intervalo de tiempo; efectuar frecuentes re-keying desbarata los ataques conocidos contra los métodos de encriptación usados en las comunicaciones inalámbricas (WEP).

Despliegue más fácil, ya que no se requiere las certificaciones de los clientes. Odyssey y Steel-Belted Radius le permiten evitar la sustancial carga administrativa cuando se efectúa la operación de autorizar la certificación, revocar, además de gestionar otros tipos de certificados que una solución 802.1x basada en EAP-TLS requiere. En cambio, Odyssey y Steel-Belted Radius provees de una seguridad extremadamente fuerte, permitiéndoles a los usuarios conectarse con sus nombres de usuarios y passwords habituales.

- ✓ Despliegue seguro contra cualquier base de datos de autenticación. Odyssey y Steel-Belted Radius ofrecen diferentes opciones según donde quiera autentificar a sus usuarios de redes inalámbricas.
- ✓ Elija Odyssey si necesita autentificar usuarios de una WLAN contra una base de datos de autenticación de Windows (Windows XP o Windows 2000 Native Domain, Windows NT Domains).
- ✓ Elija Steel-Belted Radius si necesita autentificar usuarios de una WLAN y usuarios remotos contra Windows, así como contra bases de datos basadas en SQL/LDAP, sistemas token tales como RSA Security´s ACE/Server, TACACs+, NIS/NIS+ (si corre sobre Solaris) y una base de datos nativa.

Odyssey también puede traspasar peticiones de autenticación de usuarios a Steel-Belted Radius para autenticaciones contra cualquiera de las bases de datos back-end que Steel-Belted Radius soporta. Esta característica es importante por 2 motivos:

- ✓ **Prestaciones**. La seguridad en redes WLAN es desde el punto de vista de la computación, muy intensiva, puede añadir Odyssey Servers para gestionar la seguridad, mientras que opcionalmente puede pasarle a Steel-Belted Radius el proceso de la autenticación del usuario de la WLAN.
- ✓ **Costo**: Odyssey cuesta menos que Steel-Belted Radius. Por lo que podría desplegar Odyssey Server en redes **WLANs** distribuidas alrededor de su empresa, y tenerlas comunicadas con Steel-Belted Radius en la sede central.
- ✓ **Multiplataforma**: Odyssey Server corre sobre Windows XP/2000 (Server y Professional); Steel-Belted Radius corre sobre XP/2000/NT y Solaris para disponer de compatibilidad en su entorno de red.

2.3.8 Odyssey Client

El componente final de la suite de Funk Software de los productos de seguridad de redes WLANs es Odyssey Client. Odyssey Client corre sobre un dispositivo inalámbrico y permite al usuario conectarse de manera segura a la red.

Soporta potentes métodos de autenticación EAP para obtener la máxima seguridad, incluyendo EAP-TTLS y/o EAP-TLS.

- ➢ **Fácil de desplegar y gestionar:** Odyssey Client provee de un soporte insuperable multi-plataforma y multi-vendor que soporte tarjetas de clientes que soporten 802.1x. También ofrece numerosas herramientas de auto-configuración por lo que podrá racionalizar despliegues de accesos a redes inalámbricas de gran escala además de los obligados niveles de seguridad que las corporaciones exigen.
- ➢ **Protege la confidencialidad de las credenciales de los usuarios:** Odyssey Client protege totalmente la identidad de los usuarios entre el nodo del cliente y la red, para proteger la privacidad de la localización donde se encuentre contra la vigilancia, adquisición indeseada de información de marketing, además de otras intrusiones desde monitorizaciones a fisgones.
- ➢ **Provee compatibilidad multi-plataforma:** Odyssey Client corre sobre Windows XP, 2000, 98 y ME, para garantizar la compatibilidad de su entorno de red.

2.3.9 Radius

Según (Lopez, 2012). RADIUS (Remote Authentication Dial-In User Server) es un protocolo cliente/servidor, donde el cliente es un NAS (Network Access Server) y el servidor es un software ejecutado en un equipo UNIX, LINUX o Windows. Como protocolo de transporte emplea UDP, para establecer comunicación utiliza dos puertos: el 1813 para contabilidad y el 1812 para autenticación y autorización.

2.3.9.1 Cliente RADIUS

Según (Cevallos & Ponton, 2011), también denominado NAS, es un equipo de comunicación, puede ser un access point, un switch, un RAS entre otros, los cuales serán la puerta de ingreso a la red, al cual los usuarios se conectan físicamente por medio de cable, wireless, ADSL o RTB.

Este punto de paso entre el cliente y el servidor será el encargado de derivar las peticiones de acceso a los servidores, y acuerdo a la respuesta recibida del servidor dará permiso o negara acceso al usuario.

Para su correcto funcionamiento el cliente requiere los siguientes datos:

- ✓ Dirección IP o nombre del servidor RADIUS
- ✓ Puerto de autenticación y autorización
- ✓ Puerto de contabilidad, por donde recibe los eventos de conexión
- ✓ Clave de autorización, que codifica la información enviada en la negociación con el servidor.

2.3.9.2 Servidor RADIUS

Según Pontón P. (2013). Software instalado como servicio en el sistema operativo de una computadora, es el encargado de administrar las cuentas de acceso. Recibe la autenticación y luego de realizar la comparación con sus registros envía un mensaje permitiendo o negando el acceso, además ira almacenando los eventos de dichos procesos. Para aceptar las consultas del cliente debe tener un perfil del NAS con la dirección IP del cliente y la clave de autorización.

En la comunicación con el cliente, se intercambian los siguientes mensajes:

- ✓ Access - Request: Solicitud de atención para autenticación
- ✓ Access - Accept: Acepta la autenticación
- ✓ Access - Reject: No acepta la autenticación
- ✓ Accounting - Request: Registra eventos
- ✓ Accounting – Response: Confirmación de evento registrado

En la siguiente figura se muestra la secuencia de intercambio de mensajes:

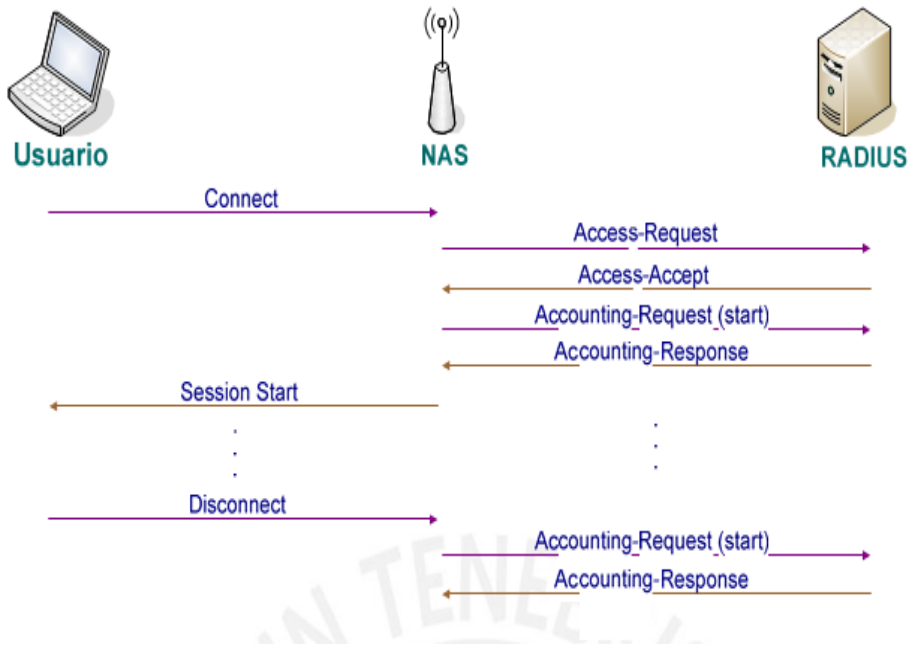


Figura 2. Secuencia de intercambio de mensajes
***Fuente**: "Sistema de Autenticación y Cifrado"*

Dentro de los mensajes se envían atributos que contienen información necesaria para una adecuada comunicación. A continuación se detalla los atributos que son transportados en cada mensaje:

Access – Request

User - Name: Cuenta del usuario

User - Password: Pasword del usuario

Access – Accept

Frame - IP - Address: Dirección IP a entregar

Frame - IP - Netmask: Mascara de la dirección IP a entregar

Accounting – Request

Acct - Status - Type: Estado de conexión

Acct - session Time: Tiempo de sesión

Acct - Terminate - Cause: Causa de desconexión.

En la tabla 1.1 se hace una breve comparación de los principales servidores de autenticación.

Tabla 1. Comparación entre servidores de autenticación

Nombre	S.O.	802.1x	Libre
IAS Windows	Windows	TLS, PEAP Y LEAP	No
Tekradius	Windows	MD5, PEAP y TLS	Sí
EmeraldV5	Windows	PEAP, TTLS y LEAP	No
RAD-series	Windows	MD5, TLS, PEAP, TTLS y	No
Odyssey	Windows	MD5, TLS, PEAP, TTLS y	No
Steef	Windows	MD5, TLS, PEAP, TTLS y	No
Belted	Sun	LEAP	
FreeRadius	Linux	MD5, TLS, PEAP, TTLS y	Sí

Fuente: “Seguridad en WLAN IEEE 802.11”

2.4 Hipótesis

La implementación de servidores de autentificación radius con el uso de certificados digitales mejorará la seguridad y el control de acceso a las redes inalámbricas en la UNSM-T.

2.4.1 Hipótesis alterna

La implementación de servidores de autentificación radius con el uso de certificados digitales SÍ mejorará la seguridad y el control de acceso a las redes inalámbricas en la UNSM-T.

2.4.2 Hipótesis nula

La segmentación de la red y priorización del ancho de banda NO permitirá mejorar el rendimiento y la seguridad de la red de la Universidad Nacional de San Martín – Tarapoto.

2.5 Sistema de variables

2.5.1 Variable independiente.

Implementación de servidores de autentificación radius con el uso de certificados digitales.

2.5.2 Variable dependiente.

Seguridad y el control de acceso a las redes inalámbricas en la UNSM-T.

2.6 Escala de medición

Tabla 2. Escala de medición variables.

Tipo de Variable	Variable	Indicador	Escala de medición	Instrumento Evaluación.
Dependientes	Seguridad y el control de acceso a las redes inalámbricas en la UNSM-T.	Listas de control de acceso.	Unidad	Reporte de la ACL
		Recursos de seguridad integrados	Unidad	Reportes y documentación
		Mecanismos avanzados de protección	Unidad	Reportes y documentación
		Mecanismos de Autenticación.	Unidad	Reportes y documentación
Independientes	Implementación de servidores de autentificación radius con el uso de certificados digitales.	Servidor de autenticación implantado	Unidad	Documentación de la implantación.

Fuente: Elaboración propia

2.7 Objetivos

2.7.1 General

- Plantear una plataforma de seguridad para el acceso inalámbrico al servicio de internet la UNSM-T.

2.7.2 Objetivo Especifico

- Incrementar la seguridad y el control de acceso a las redes inalámbricas en la UNSM-T.
- Implementar servidores de acceso inalámbrico al servicio de internet basado en protocolos de seguridad avanzados (radius).
- Evaluar el impacto de los servidores de acceso inalámbrico basado en protocolos de seguridad avanzados sobre la mejora de la seguridad y el control de acceso a las redes inalámbricas en la UNSM-T.

CAPÍTULO II

III. MATERIALES Y MÉTODOS

3.1 Universo y muestra

Para el desarrollo de la presente investigación, se determina que el universo de la misma son todos los estudiantes que cuentan con un dispositivo que cuenten con conexión inalámbrica y la unidad de análisis es la red de datos de la UNSM-T-FISI, teniendo entonces como universo lo siguiente:

Tipo	Cantidad
Alumnos	339

Fuente: Oficina de Control y Registro Académico y Oficina de Personal.

Determinación del muestreo y el tipo más adecuado.

En función a las características de la población y siendo ésta conformada por tres tipos, el muestro a utilizar será el de muestreo aleatorio.

Cálculo del tamaño de la muestra.

Para realizar el cálculo del tamaño de la muestra se tomará en cuenta que el muestreo a utilizar será aleatorio.

Siendo la fórmula para el cálculo el siguiente:

$$n = \frac{S^2}{\frac{\varepsilon^2}{Z^2} + \frac{S^2}{N}}$$

Dónde:

n = tamaño necesario de la muestra = 2844

N = tamaño de la población.

Z = margen de confiabilidad o número de unidades de desviación estándar en la distribución normal que producirá un nivel deseado de confianza = 1.96
E = error o diferencia máxima entre la media muestra y la media de la población que se está dispuesto a aceptar con un nivel de confianza que se ha definido = 0.05

p = 0.5

q = 0.5

A partir de la fórmula entonces tenemos la distribución de la muestra en la tabla siguiente:

Tipo	Cantidad
Alumnos	24

.

3.2 Ámbito geográfico

El proyecto "**SEGURIDAD Y CONTROL DEL ACCESO A LAS REDES INALÁMBRICAS EN LA UNSM-T MEDIANTE SERVIDORES DE AUTENTIFICACIÓN RADIUS CON EL USO DE CERTIFICADOS DIGITALES**". Se realizará en la Ciudad Universitaria de la Universidad Nacional de San Martín, en el distrito de Morales, provincia y departamento de San Martín, en el pabellón de la Facultad de Ingeniería de Sistemas e Informática.

3.3 Diseño de la investigación

3.3.1 Tipo de investigación

El tipo de la investigación es Aplicada o Tecnológica, ya que la investigación pretende aplicar los conocimientos ya existentes en el área de Tecnología de Información.

3.3.2 Nivel de investigación

La investigación desarrollada en este estudio es de nivel correlacional, fundamentado en el hecho de que se comprobará cómo la variable independiente, Implementación de servidores de autentificación radius con el uso de certificados digitales, influye positivamente en la variable dependiente que es seguridad y el control de acceso a las redes inalámbricas en la UNSM-T.

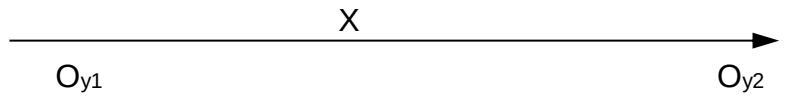
3.3.3 Diseño de investigación

Esta investigación, por sus características es de un Diseño Cuasi experimental, Transversal

El diseño será Cuasi Experimental, puesto que se aplicará la prueba de hipótesis diferencia de medias a la misma muestra, mediante muestras pareadas.

Siendo el diagrama del diseño cuasi experimental.

Figura 3. Diagrama del diseño experimental de la investigación.



Fuente: Elaboración propia

Dónde:

X = Es el experimento o aplicación de la variable independiente

Oy1 = Observación de la variable dependiente antes de la aplicación del experimento.

Oy2 = Observación de la variable dependiente después de la aplicación del experimento.

.

3.4 Procedimientos y técnicas

3.4.1 Procedimientos

Los parámetros para la obtención de la información estadística, serán obtenidos mediante herramientas de medición, como NTOP, IPTRAF, Fortianalyzer, considerando que su puesta en marcha debe realizarse en horarios de altas tasas de transferencias de información, archivos que pesan en promedio de 9 a 30 mbps, cuyos resultados se utilizan para su posterior análisis.

Este procedimiento se utiliza para agrupar datos por medio de la computadora, para tabular, ponderar e interpretar usando una hoja de cálculo en Excel. La información se presenta mediante histogramas.

3.4.2 Técnicas

Las técnicas para la recolección de datos que se utilizan en el estudio son: la observación, reportes de la solución implementada, la encuesta, así como softwares de simulación y medición de indicadores de red. La encuesta se define como un procedimiento que consiste en hacer las mismas preguntas, a una parte de la población, que previamente fue definida y determinada.

El software que se utiliza para la obtención de valores de indicadores de rendimiento de la red lan es NTOP, IPTRAF, así como el Fortianalyzer, que son

software de análisis de tráfico de red y permiten monitorizar en tiempo real, mediante la utilización del protocolo SNMP, los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto.

Lo que hacen estos softwares es monitorizar toda la red en busca de datos para generar estadísticas. Los protocolos que son capaces de monitorizar son: TCP/UDP/ICMP/ARP.

3.5 Instrumentos

3.5.1 Instrumentos de recolección de datos

Se emplearán fuentes bibliográficas como artículos científicos obtenidos en revistas electrónicas y textos especializados sobre el tema. El método de investigación utilizado será el de la Observación, porque se trata de una investigación en la cual se recolectan datos a partir de la observación en campo del cambio de los indicadores luego de la aplicación del experimento.

Por el procesamiento de los datos, se plantea un enfoque cuantitativo toda vez que se trata de medición numérica continua de los valores de los indicadores.

3.5.2 Instrumentos de procesamiento de datos

Una vez concluidas las etapas de recolección y procesamiento de datos se inicia con la determinación de la muestra bajo la técnica del muestreo estratificado.

Así mismo para el análisis de los datos se aplicarán técnicas estadísticas: Tablas de Distribución de Frecuencias, medidas estadísticas (promedio, desviación estándar, coeficiente de variación), prueba de hipótesis con la distribución T-students (diferencia de medias a la misma muestra, mediante muestras pareadas), evaluándose a los indicadores para determinar el cumplimiento de los objetivos planteados de forma que se puedan realizar conclusiones y proporcionar recomendaciones que los investigadores están en capacidad de generar

Este procedimiento se utilizará para agrupar los datos por medio de computadoras, a tabular, ponderar e interpretar los datos usando una hoja de cálculo en Excel, serán presentados la información recopilada por medio de encuestas que

serán transcritas a su posterior análisis, en este caso el indicador estadístico serán presentados como información en forma de cuadros y gráficos.

3.6 Prueba de hipótesis

Recordemos las hipótesis de trabajo:

Hipótesis alterna (H1)

La implementación de servidores de autentificación radius con el uso de certificados digitales SÍ mejorará la seguridad y el control de acceso a las redes inalámbricas en la UNSM-T.

Hipótesis nula (H0)

La segmentación de la red y priorización del ancho de banda NO permitirá mejorar el rendimiento y la seguridad de la red de la Universidad Nacional de San Martín – Tarapoto.

Procedimiento: Se inició con la observación a todos los servicios de red de la UNSM -T, y a continuación se procedieron a hacer pruebas de ataques a los mismos por diferentes modalidades, y a continuación se muestran los resultados encontrados.

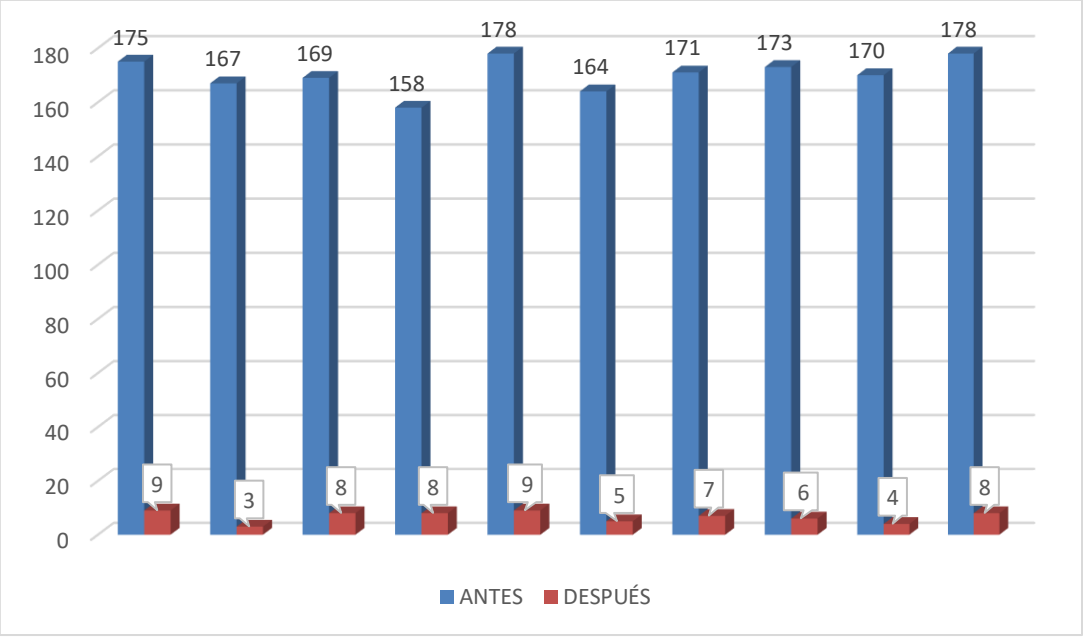
Para efectos de la presente investigación, se toma como dato los resultados de los ataques a la seguridad realizados, a partir de la cual se presenta la siguiente tabla en la que las columnas del ANTES representan datos que se obtuvieron antes de RADIUS y las columnas DESPUÉS son datos obtenidos ya con RADIUS en producción

Tabla 3. Resultados de las pruebas de ataques a la seguridad y control de acceso a las redes inalámbricas de la UNSM-T, ANTES y DESPUÉS de la implementación de servidores de autentificación radius con el uso de certificados digitales

Definición	ANTES		DESPUÉS	
	Intentos	Exitoso	Intentos	Exitosos
Ataque WPA-SPK	180	175	180	9
DNS Tunneling	180	167	180	3
Ataque DOS	180	169	180	8
Man in the middle	180	158	180	8
MAC Cloning	180	178	180	9
FMS	180	164	180	5
Mecanismos de autenticación	180	171	180	7
DDoS	180	173	180	6
Phishing	180	170	180	4
Dribbling blade	180	178	180	8
Promedio		**170.3**		**6.7**
Desviación estándar		**6.25**		**2.11**

Fuente: Elaboración propia.

Figura 4. Comparación de intentos exitosos de ataques a la seguridad Antes y Después de RADIUS



Cálculo de estadígrafos más importantes calculados a partir de los datos obtenidos ANTES de RADIUS.

Estadígrafo	Fórmula	Valor
Promedio:	$\bar{X} = \sum_{i=1}^{N} x_i$	170.3
Mediana:	$Me = x_{i1} + \left(\frac{\left({}^{N_m}/_{2} \right) - N_i - 1}{fi} \right) . (x_{i2} - x_{i1})$	170.5
Desviación estándar:	$S = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \bar{x})^2}{n-1}}$	6.25
Coeficiente de variación	$:C_v = \frac{S}{\bar{X}} * 100\%$	3.67%

Cálculo de estadígrafos más importantes calculados a partir de los datos obtenidos DESPUÉS de RADIUS:

Estadígrafo	Fórmula	Valor
Promedio:	$\bar{X} = \sum_{i=1}^{N} x_i$	6.7
Mediana:	$Me = x_{i1} + \left(\frac{\left({}^{N_m}/_{2} \right) - N_i - 1}{fi} \right) . (x_{i2} - x_{i1})$	7.5
Desviación estándar:	$S = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \bar{x})^2}{n-1}}$	2.11
Coeficiente de variación	$:C_v = \frac{S}{\bar{X}} * 100\%$	31.5%

Tabla 4. Prueba T-student para comparar resultados de la cantidad de ataques a la seguridad exitosos ANTES y DESPUÉS de Radius.

H_0: $\mu_a - \mu_d = 0$: **los ataques exitosos a la seguridad ANTES y DESPUÉS no presenta diferencias significativas.**

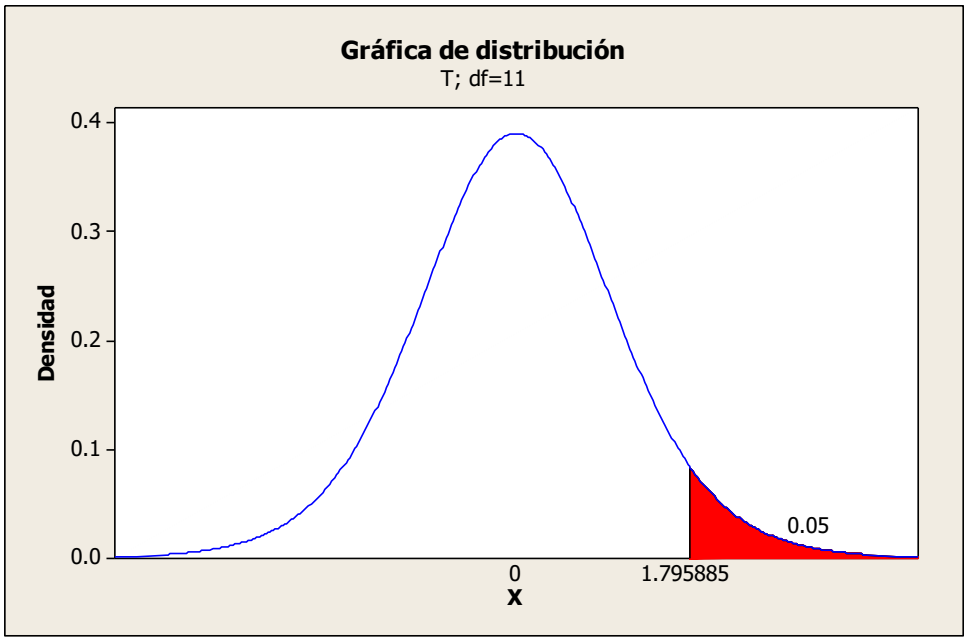
H_1: $\mu_a - \mu_d > 0$: los ataques exitosos a la seguridad ANTES es significativamente mayor DESPUÉS.

En nuestro caso se dispone de dos grupos de observaciones independientes con diferentes varianzas, la distribución de los datos en cada grupo no puede compararse únicamente en términos de su valor medio, para lo cual utilizamos la fórmula conocido como el test de Welch basada en el estadístico:

$$t = \frac{\left(\overline{X_{antes}} - \overline{X_{después}}\right)}{\sqrt{\frac{S^2_{antes}}{N_{antes}} + \frac{S^2_{después}}{N_{después}}}} = \frac{(30.2473 - 21.0962)}{\sqrt{\frac{3.1612^2}{11} + \frac{2.3701^2}{11}}} = 7.681755$$

Medidas Estadísticas	**Prueba "t" datos a-pareados**	**Valor p Significación**
$\overline{X}_{antes} = 170.3$ $\overline{X}_{despues} = 6.7$ $\overline{d} = -163.6$ $S_{antes} = 6.25$ $S_{después} = 2.11$	**$T_{calculada}$= 7.681755** **$T_{tabular}$= 1.795885** **$T_{calculada} > T_{tabular}$**	**P=**0.000000048428067 **< 0.05** Se Rechaza H_0 Porque los ataques exitosos a la seguridad ANTES de RADIUS son mayores que DESPUÉS.

***Figura 5 Gráfica de distribución de los ataques exitosos a la seguridad*.**



Fuente: SPSS.

A continuación se presentan algunos argumentos que confirman el enunciado de la hipótesis.

- Los resultados de esta investigación comprueban las hipótesis propuestas. Entonces se puede afirmar que la implantación RADIUS, sí aporta mejoras en la seguridad.
- Es decir el uso del RADIUS ha mejorado la seguridad y ha permitido que los resultados de la red se mejoren.
- La seguridad en redes tipo inalámbricas, es un factor muy importante debido a la naturaleza del medio de transmisión: el aire.
- Las características de seguridad en la WLAN (Red Local Inalámbrica), se basa especialmente en la protección a la comunicación entre el punto de acceso y los clientes inalámbricos, controlan el ingreso a esta red, y protegen al sistema

de administración de acceso no autorizado

- Sin un sistema de control existente, como lo es la red inalámbrica de la Ciudad Universitaria de la Universidad Nacional de San Martín - Tarapoto, los procedimientos y mecanismos de seguridad eran tan débiles e inexistentes que se puede tener acceso con relativa facilidad hacia la red LAN desde cualquier usuario sin la debida autorización.

- Al implementar el sistema de autenticación, permitió brindar mayor confianza a los usuarios al manejar información estrictamente confidencial.

- Con el sistema de autenticación se logró dar acceso únicamente a los equipos y usuarios autorizados, restringiendo de esta manera el acceso no autorizado, con lo que se evitó ataques a la red y proliferación de virus informáticos.

- El sistema de autenticación y autorización vía web estará basado en un protoloco seguro, lo que permite encriptar los mensajes que se envían en la red entre un servidor y un cliente, garantizando de esta manera la seguridad en la transmisión de la información a través de la web.

CAPÍTULO III

IV. RESULTADOS.

Para la implementación del sistema de autenticación inalámbrica vía web se utiliza una arquitectura de red simple compuesta por un punto de acceso inalámbrico, un cable ethernet para el acceso a la intranet, un servidor de seguridad, y uno o varios clientes con tarjeta de red inalámbrica. La arquitectura se puede ver en la figura

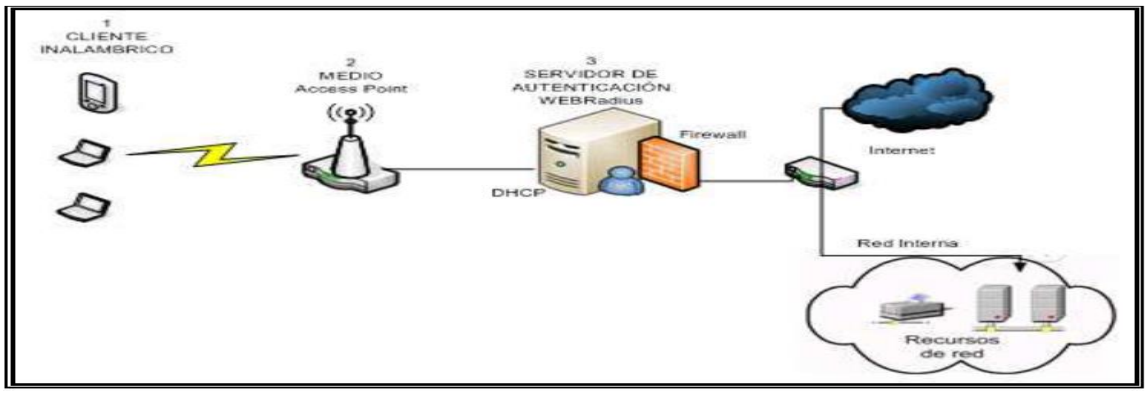


Figura 6. Arquitectura de acceso inalámbrico propuesto.
Fuente: Elaboración propia

El primer elemento de la arquitectura es un cliente inalámbrico que se conecta al punto de acceso a través de una tarjeta de red inalámbrica, el segundo elemento es un punto de acceso que sirve como medio para que el cliente inalámbrico se conecte con el servidor de seguridad y la red ethernet, y el tercer elemento es el servidor de seguridad que contiene los servicios de DHCP para que los clientes obtengan una dirección IP, RADIUS para administrar la autenticación de los clientes y un firewall para autorizar o denegar el acceso a la red ethernet o al Internet.

DISCUSIÓN DE LOS RESULTADOS

- Gracias a la implementación del servidor de autenticación radius con uso de certificados digitales, se ha logrado incrementar la seguridad y el control de acceso a las redes inalámbricas en la red de la Ciudad Universitaria de la Universidad Nacional de San Martín – Tarapoto, ya que la información que se envía entre el cliente y los acces points, ahora está no solamente encriptado con algoritmos como SHA5, sino que además sólo pueden acceder a la red usuarios autenticados contra el servidor de dominio, esto está en relación a lo indicado por Gómez, (2007), quien afirma que la implementación de redes inalámbricas en ámbitos semi públicos constituye uno de los desafíos no resueltos en la actualidad. Al contrario de los ámbitos puramente corporativos, en escenarios de este tipo, los administradores no pueden definir las características de conectividad de los dispositivos inalámbricos que poseen los usuarios.
- Como se muestra en el capítulo de resultados, se ha llegado a implementar el servidor de acceso inalámbrico basado en protocolos de seguridad avanzados (radius), permitiendo mejorar la seguridad y control en el acceso a redes inalámbricas, implementando inclusive un servidor de certificados que emite certificados y que se usa para encriptar la información que se transmite entre el cliente y el acces point.
- La evaluación del impacto de los servidores de acceso inalámbrico basado en protocolos de seguridad avanzados sobre la mejora de la seguridad y el control de acceso a las redes inalámbricas en la UNSM-T, se realizó en la prueba de hipótesis, y se detalla cuál es el impacto logrado, esto está relacionado con lo afirmado por Lazo, (2012) quien afirma que, gracias al servidor RADIUS, un usuario inalámbrico puede autenticarse e ingresar a la red; asimismo, el servidor TACACS+, teniendo como base el nivel de privilegio del usuario, permite a este ingresar o no a los equipos de red para realizar configuraciones en los equipos

CAPÍTULO IV

v. CONCLUSIONES

- La seguridad y control en las redes inalámbricas de la UNSM- T, serán beneficiadas de forma positivamente, ya que al implementarse un servidor radius con certificados digitales se estará minimizando el riesgo de los robos de información y ataques a la red.

- Los protocolos avanzados de seguridad con un servidor radius con certificados digitales nos permitieron encriptar los mensajes que se envían por la red entre un servidor y un cliente, garantizando de esta manera la seguridad en la transmisión de la información a través de la web.

- A partir del desarrollo del sistema de autenticación y autorización RADIUS con certificados digitales, se logró cubrir las falencias de seguridad que se encontraban actualmente en la red inalámbrica de la UNSM-T, obteniendo excelentes resultados después de la investigación.

VI. RECOMENDACIONES

- Dado el nivel de seguridad para el acceso a las redes inalámbricas existente actualmente en la red de datos de la Ciudad Universitaria de la Universidad de San Martín, se recomienda incrementar la seguridad y el control de acceso a las redes inalámbricas en la misma, a fin de salvaguardar la integridad de la información y todos los demás activos intangibles que forman parte de esta red.

- Si bien es cierto existen muchas formas de mejorar la seguridad de para el acceso inalámbrico a la red como pueden ser Filtrado MAC, PSK, etc, se recomienda la implementación ser servidores de acceso inalámbrico al servicio de internet basado en protocolos de seguridad avanzados (radius), puesto que gracias a esta implementación, no sólo se garantiza el acceso mediante la autenticación y autorización, sino además se encripta la información que se transmite entre el cliente y el acces point.

- Finalmente, recomendamos tomar los resultados de la prueba de hipótesis a fin de evaluar el impacto de los servidores de acceso inalámbrico basado en protocolos de seguridad avanzados sobre la mejora de la seguridad y el control de acceso a las redes inalámbricas en la UNSM-T.

VII. REFERENCIAS BIBLIOGRAFICAS

Carrasco, E. (2013). *Optimización del ancho de banda de internet y mejora de la seguridad aplicados a la red de datos en la Universidad Nacional de San Martín.* Tarapoto, Perú: Universidad Peruana Unión.

Cevallos, Y., & Ponton, D. (2011). *Investigación del servidor Radius para la seguridad en redes Lan Inalambricas.* Chimborazo, Ecuador: UNCh.

Gomez, P. (2007). *Arquitectura Unificada para Control de Acceso en Redes Inalámbricas Seguras.* La Plata, Argentina: Universidad de Mendoza.

Lazo, N. (2012). *Diseño e implementación de una Red Lan y WLan con Sistema de Control de Acceso Mediante Servidores AAA.* Lima, Perú: PUCP.

Lopez, J. (2012). *Diseño e implementación de un sistema de gestión de accesos a una red Wi-Fi utilizando software libre.* Lima: PUCP.

Mauricio, M. (2010). *Diseño e implementación de arquitectura de conectividad y seguridad AAA en UDNET (authentication, authorization and accounting).* Bogota, Colombia: Universidad Distrital Facultad Tecnológica.

Molina, J. (2012). *Propuesta de segmentación con redes virtuales y priorización del ancho de banda con qos para la mejora del rendimiento y seguridad de la red lan en la empresa editora el comercio planta norte.* Arequipa, Perú: Universidad Católica Santo Toribio de Mogrovejo.

Morales, A. (2013). *Mejora de la comunicación a través de una red integral corporativa de información entre los locales descentralizados de la municipalidad provincial de alto amazonas- yurimaguas.* Tarapoto, Perú: Universidad Nacional de San Martín.

Pellejero, I., Andreu, F., & Lesta, A. (2006). *Fundamentos y aplicaciones de seguridad en redes WLAN: de la teoría a la práctica.* España: Prentice Hall.

VIII. ANEXOS

A continuación procederemos a instalar y configurar el servidor de Radius usando Windows 2012R2.

8.1. Primero ponemos una IP estática a nuestro servidor

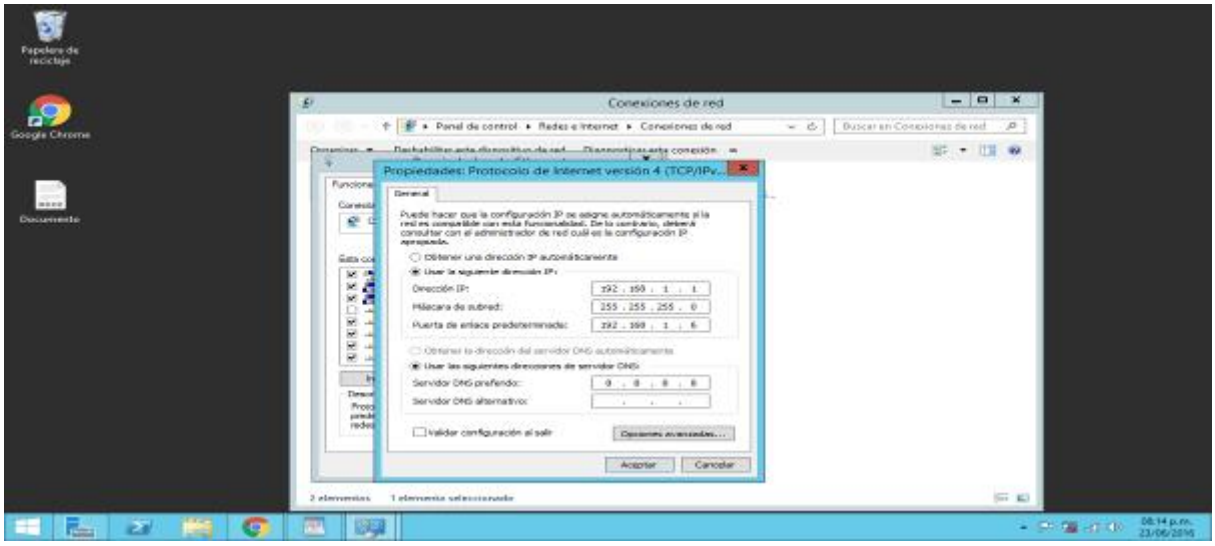


Figura N° 05. Configuración de IPS
Fuente: Elaboración Propia

8.2. Luego instalamos características a utilizar en el servidor.

Figura N° 06. Instalación de Características del servidor
Fuente: Elaboración Propia

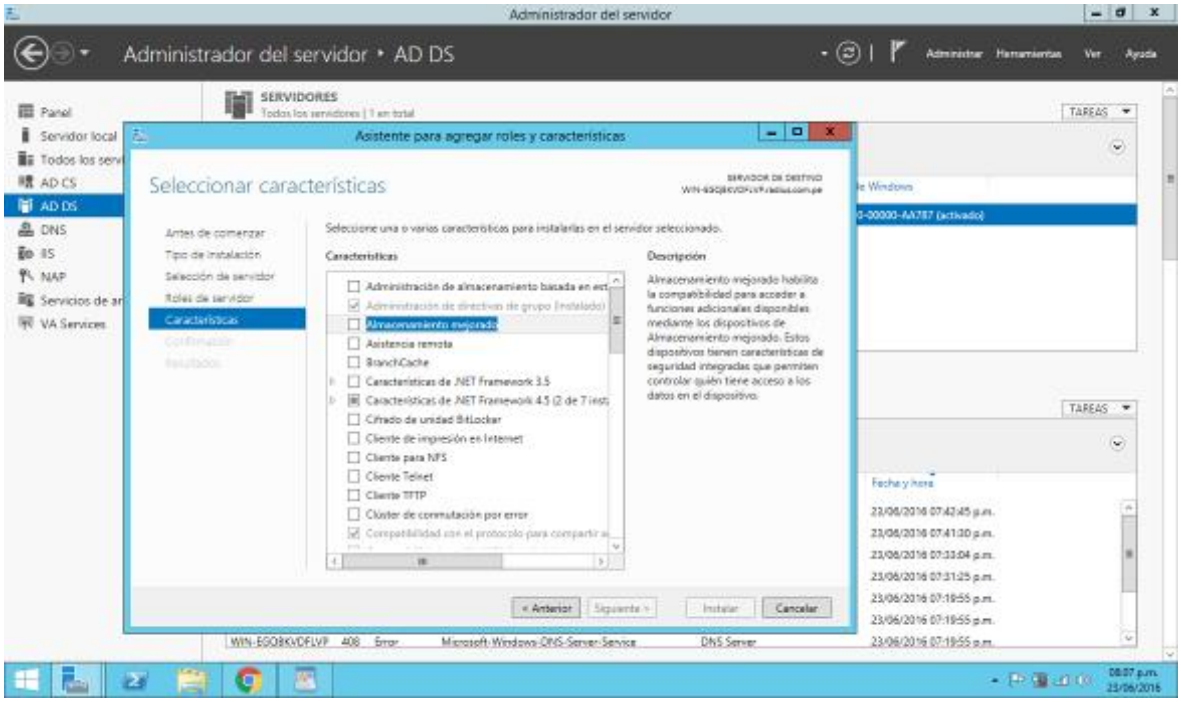


Figura N° 07. Instalación de Características del servidor
Fuente: Elaboración Propia

8.3. Seleccionaremos la opción Autoridad de Certificado, y pulsaremos siguiente

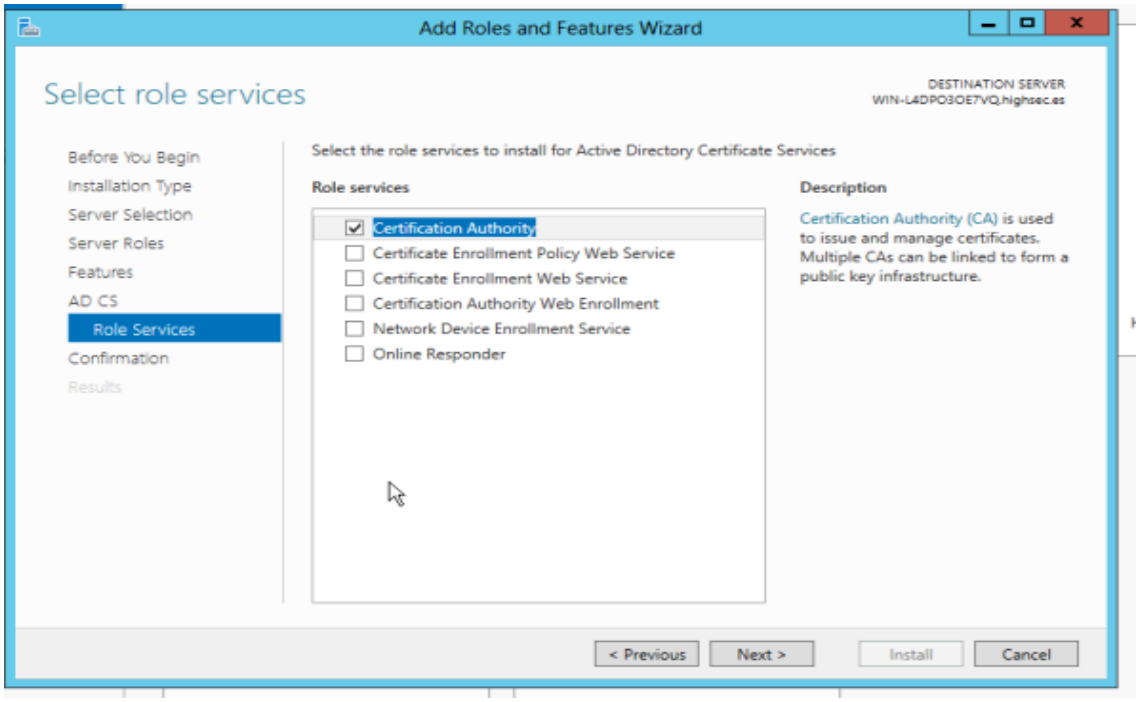


Figura N° 08. Instalación de Autorización de certificados
Fuente: Elaboración Propia

8.4. Una vez instalado configuramos el Active Directory.

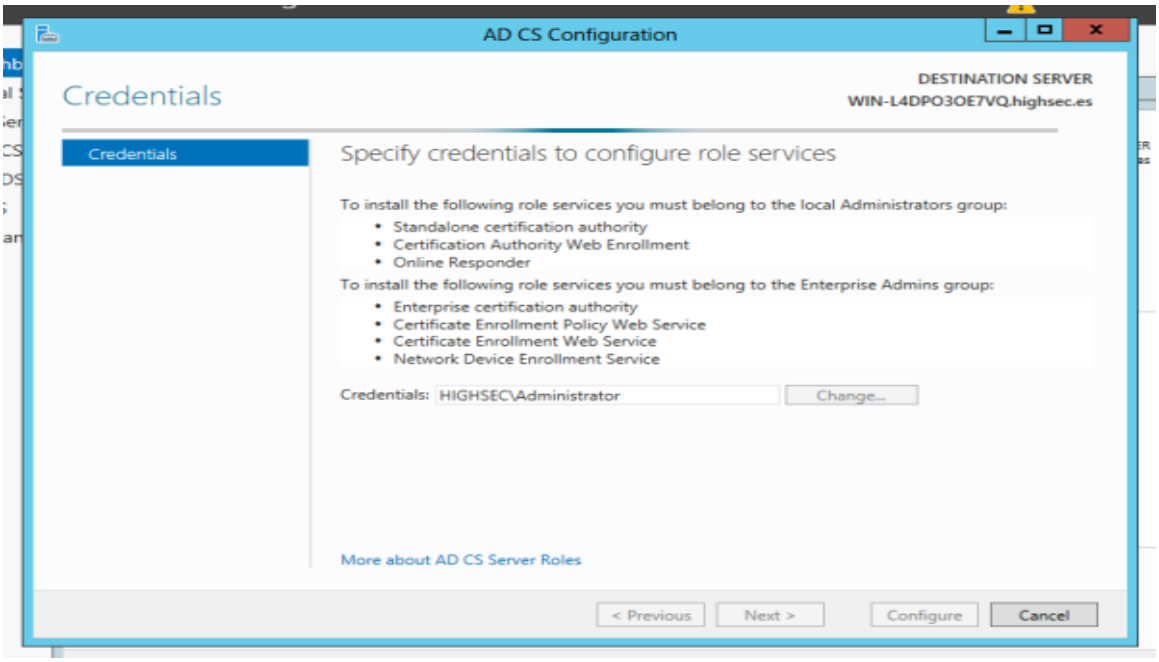


Figura N° 09. Instalación de Active directory
Fuente: Elaboración Propia

8.5. Seleccionaremos el tipo de certificado en este caso será Enterprise CA.

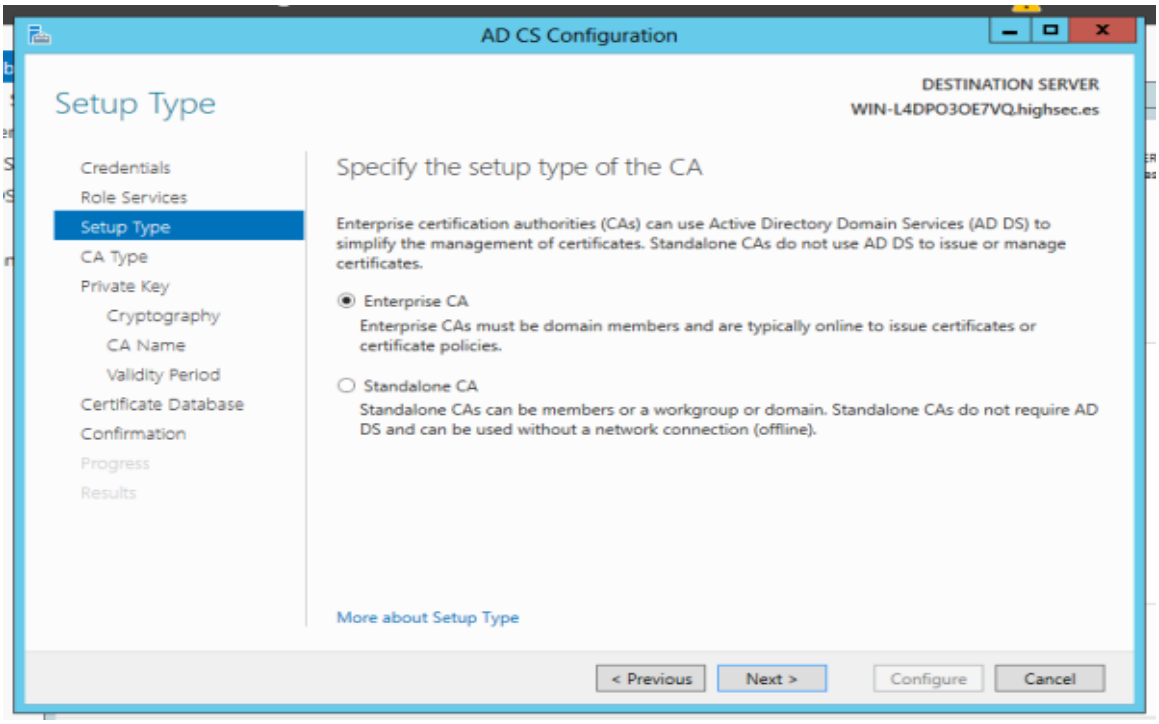


Figura N° 10. Instalación de Tipos de certificados
Fuente: Elaboración Propia

8.6. Seleccionamos las opciones criptográficas. También marcamos la opción "Allow administrator interaction when the private key is..." y le damos en siguiente.

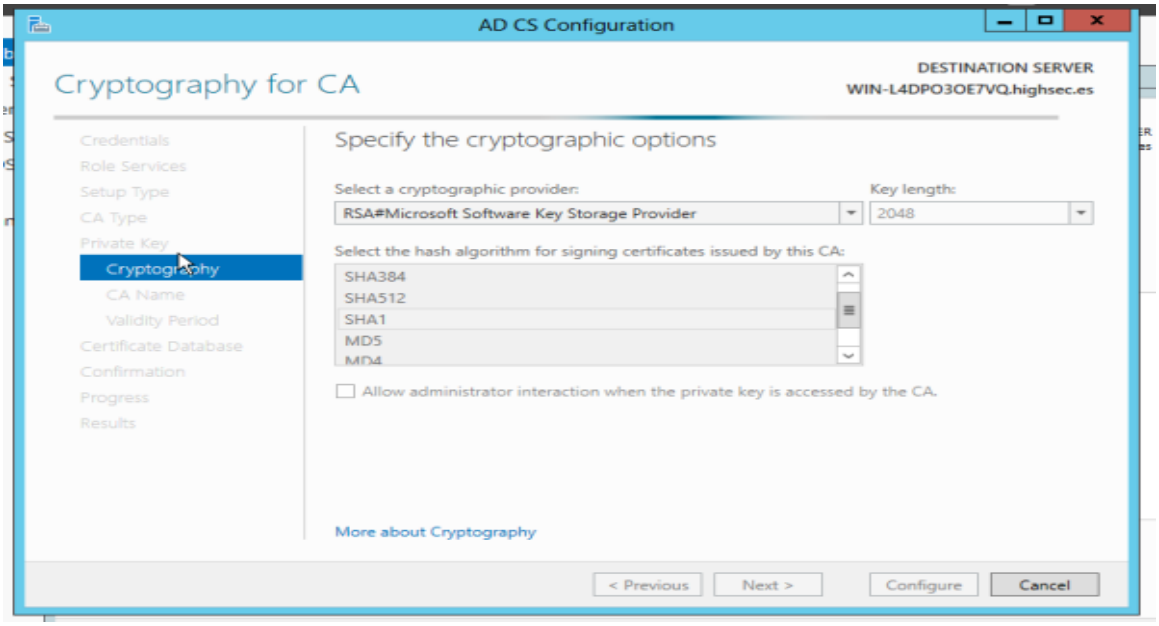


Figura N° 11. Instalación de Tipo de encriptación
Fuente: Elaboración Propia

8.7. Seleccionamos el periodo de validez del certificado.

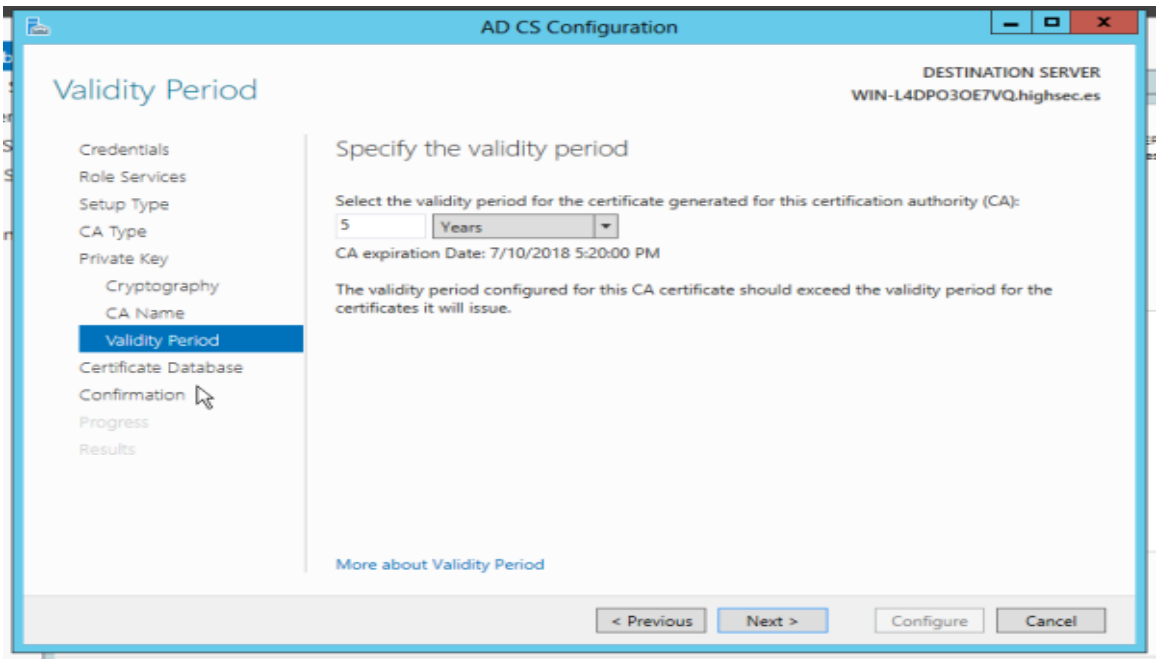


Figura N° 12. Configuración del periodo de validez del certificado digital
Fuente: Elaboración Propia

8.8. Al igual que el wizard de promoción a DC, esta configuración nos permite elegir la localización del certificado y del log.

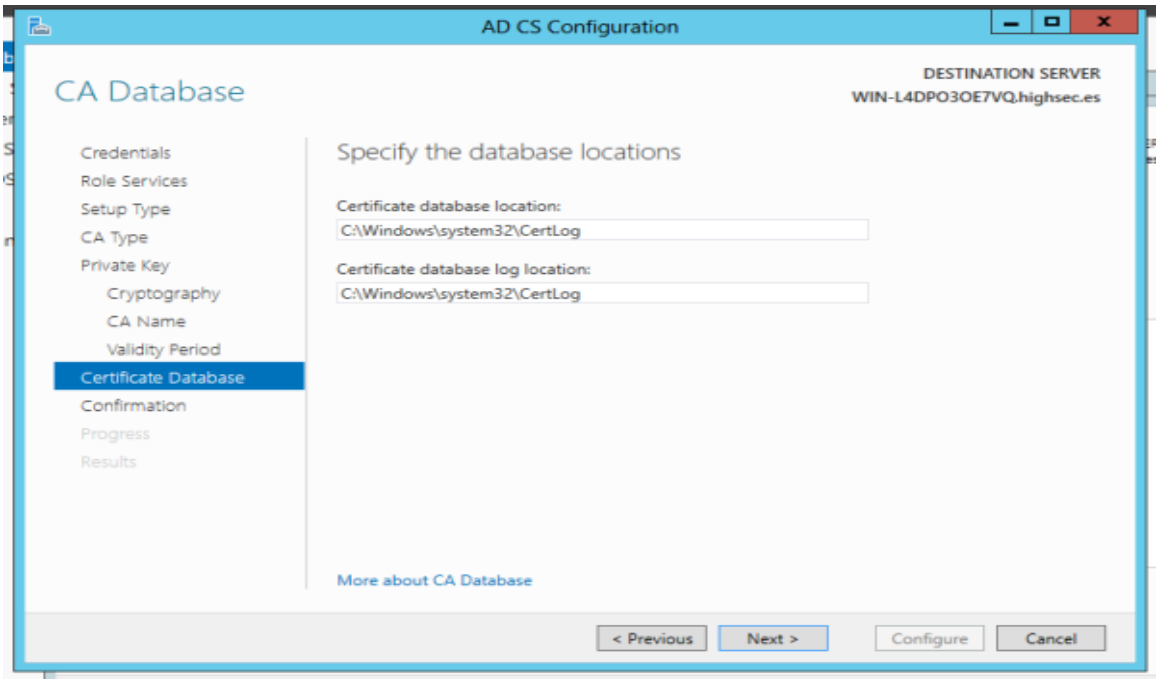


Figura N° 13. Configuración de logs para registro de actividades
Fuente: Elaboración Propia

8.9. Nos dirigiremos al manager del servidor para agregar roles en el servidor y seleccionaremos la opción las políticas de red y servicios de acceso, tal y como se ve en la captura

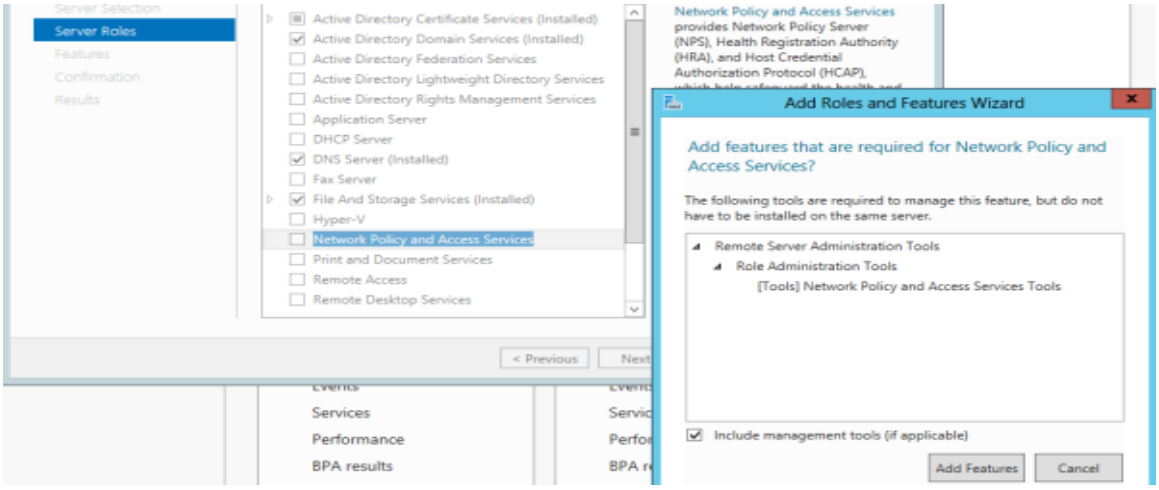


Figura N° 14. Configuración de roles del servidor
Fuente: Elaboración Propia

8.10. Una vez terminada la instalación procedemos a configurar el Access Point. La configuración se realizó en un modem-router-switch ZTE modelo ZXHN H108N. Clic en Wireless

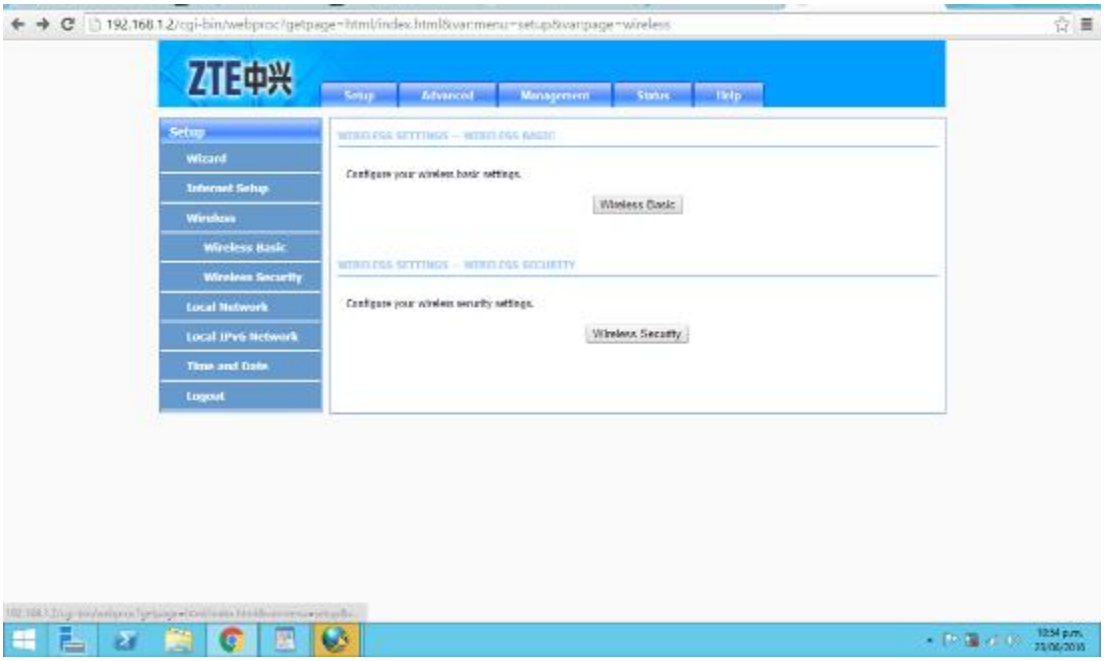


Figura N° 15. Configuración de acces point
Fuente: Elaboración Propia

8.11. Seleccionamos la opción “Servidor RADIUS para conexiones cableadas o inalámbricas 802.1X”

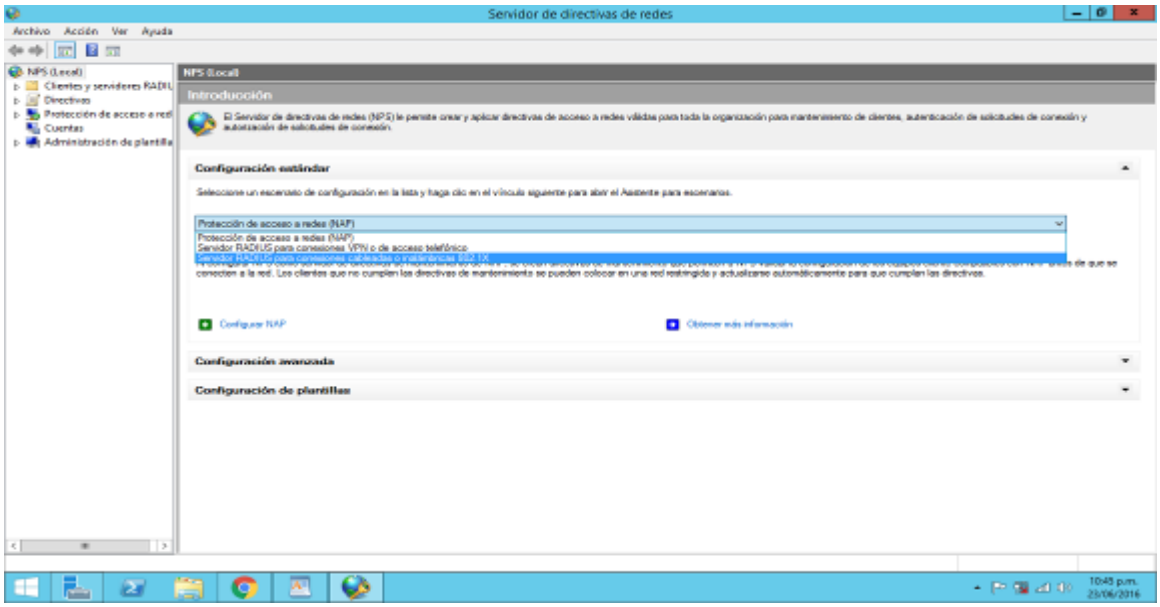


Figura N° 16. Configuración del servidor radius
Fuente: Elaboración Propia

8.12. Colocamos la misma contraseña que se puso en Access Point.

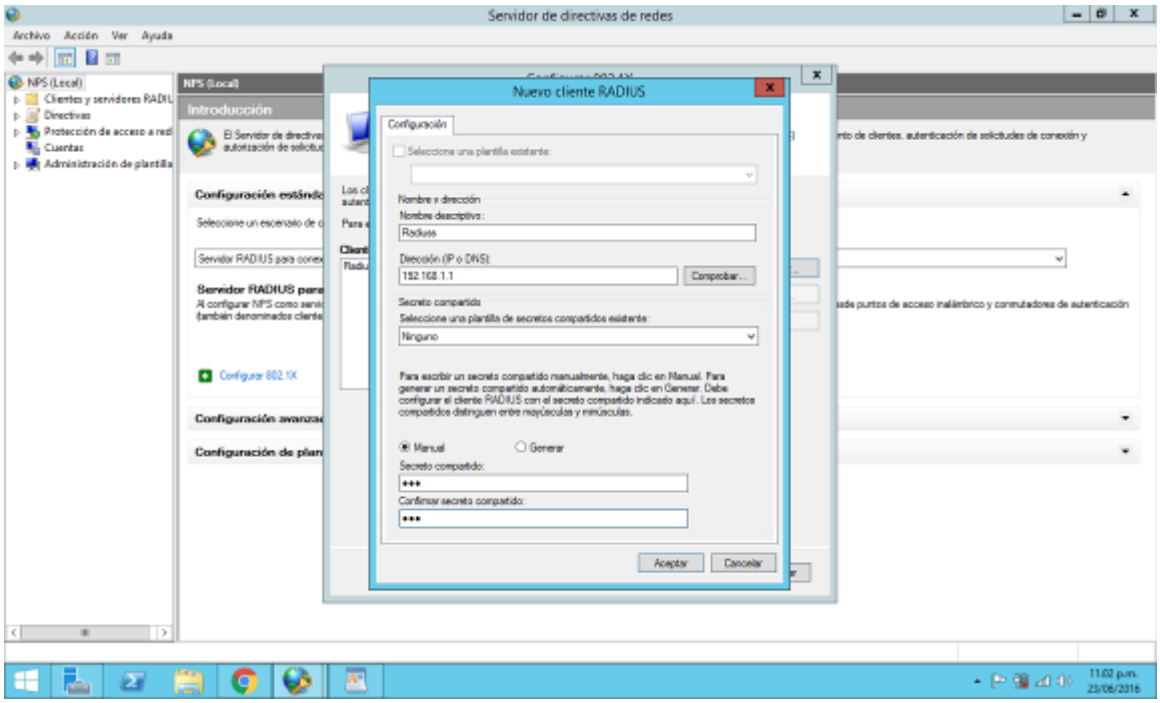


Figura N° 17. Enlace del servidor con access point
Fuente: Elaboración Propia

8.13. Luego le damos en siguiente y seleccionamos “Microsoft: Contraseña segura (EAP-MSCHAP v2)”.

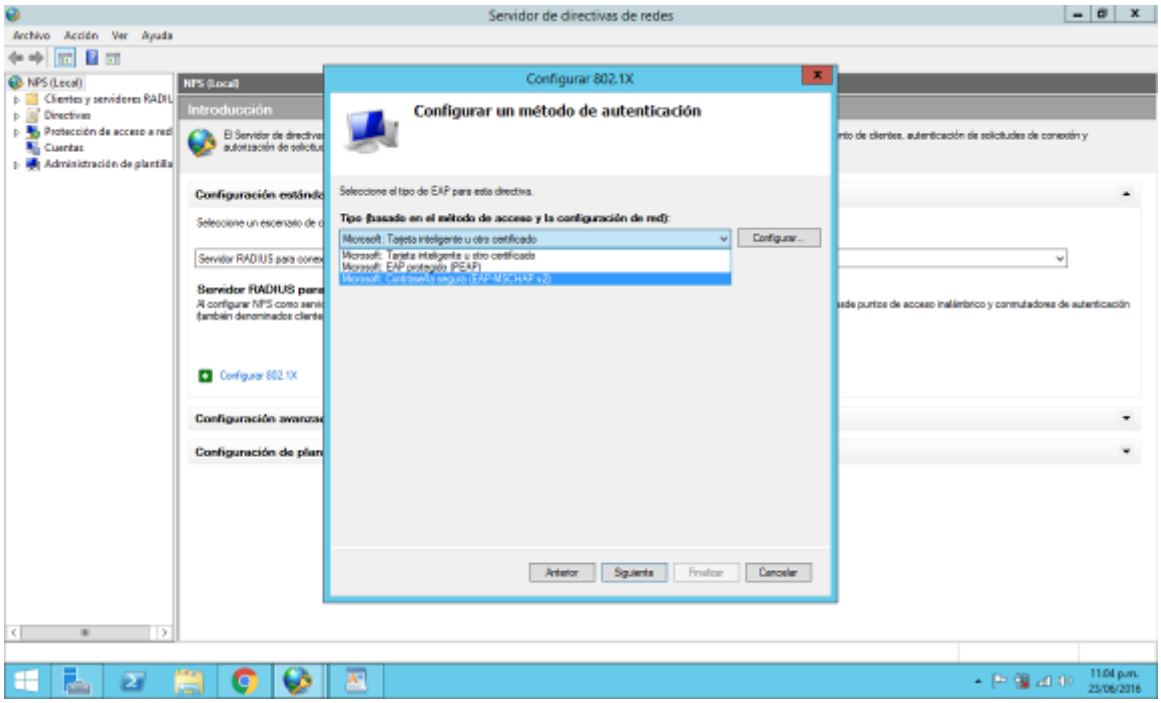


Figura N° 18. Configuración de encriptación de password servidor radius
Fuente: Elaboración Propia

8.14. Agregamos el grupo y damos clic en siguiente

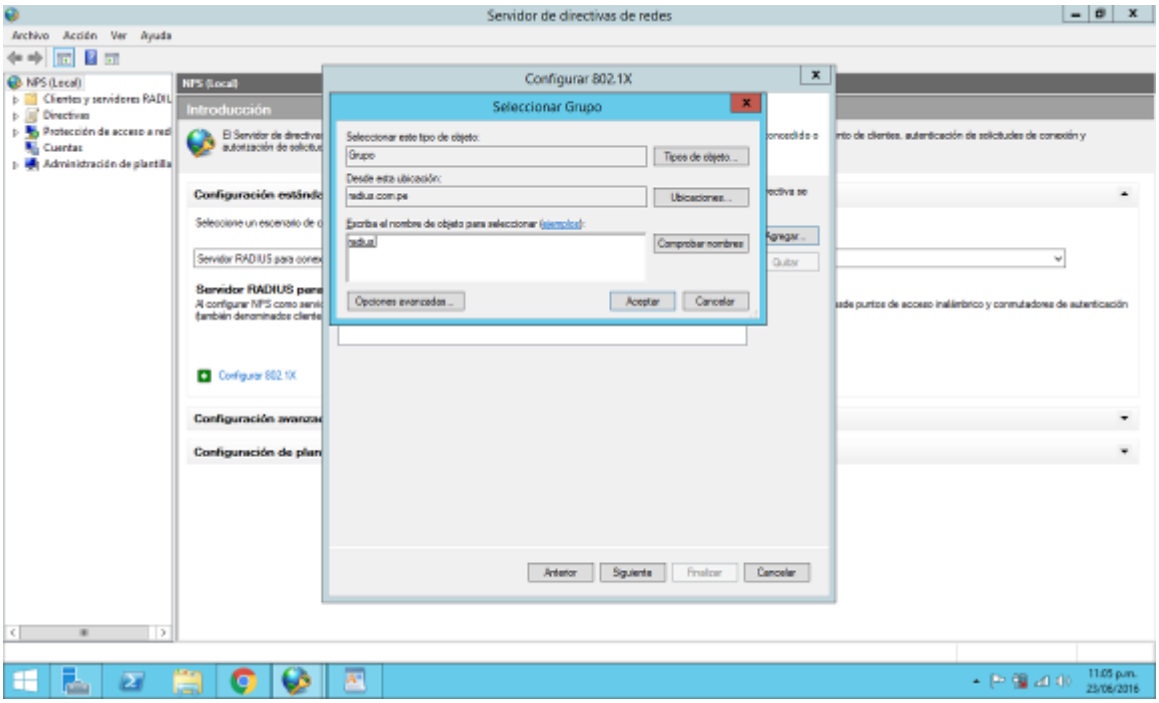


Figura N° 19. Configuración de asignación de grupos a la red
Fuente: Elaboración Propia

8.15. Damos clic en agregar y seleccionamos "Microsoft: Protected EAP (PEAP)" luego damos clic en aplicar y aceptar.

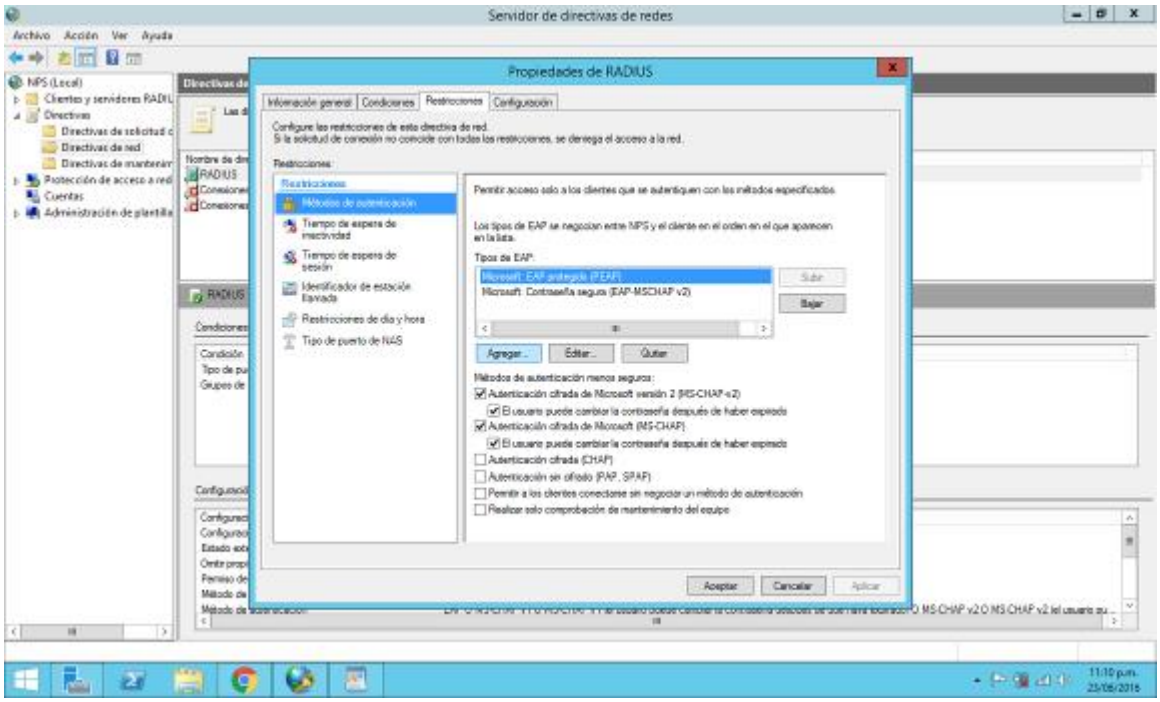


Figura N° 20. Configuración la protección de la red
Fuente: Elaboración Propia

8.16. Comprobamos que la opción "Registrar Servidor en Active Directory" este desactivada.

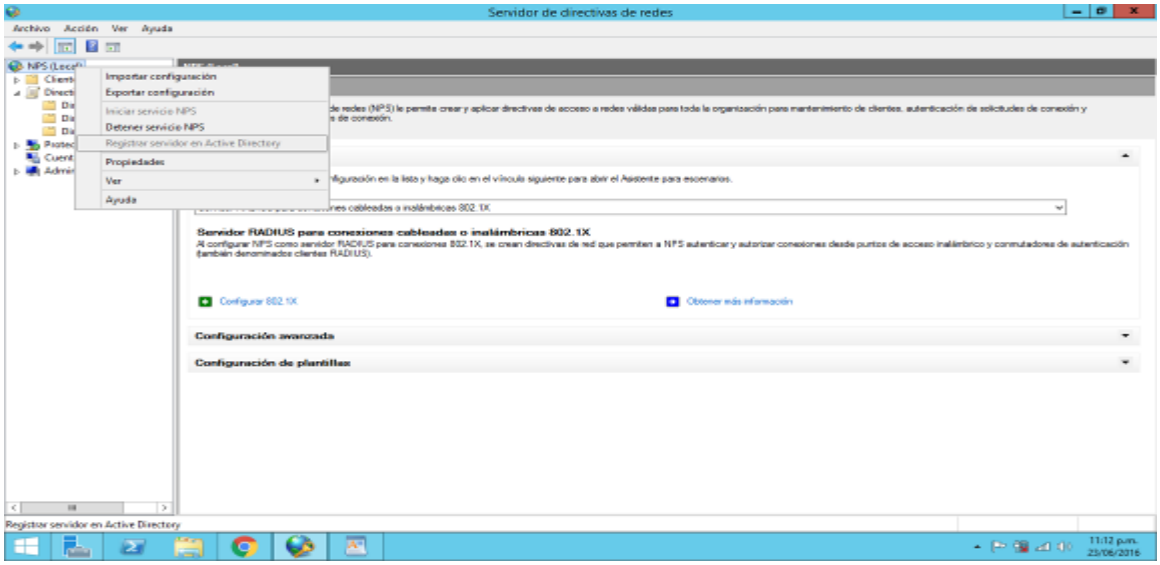


Figura N° 21. Registro del servidor en Active Directory
Fuente: Elaboración Propia

8.17. Ahora comprobamos el nombre de la red en el equipo y nos conectamos a la señal WiFi

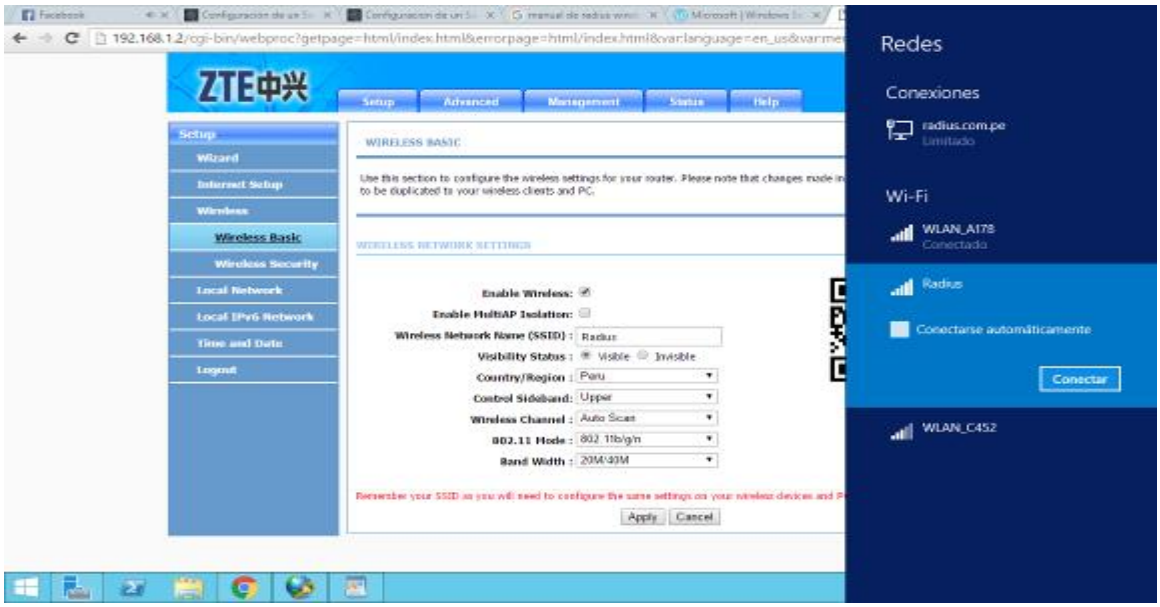


Figura N° 22. Configuración del router
Fuente: Elaboración Propia

8.18. Nos pide las credenciales y procedemos a ingresar con un usuario que creamos anteriormente y su contraseña

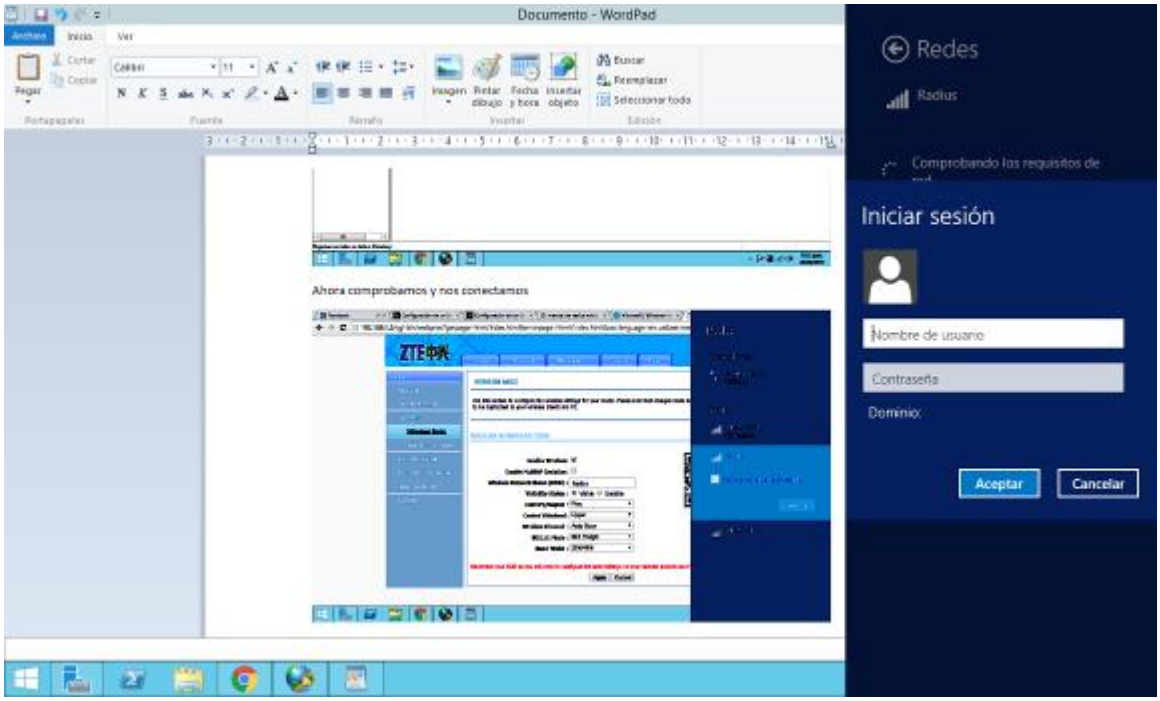


Figura N° 23. Credenciales para el acceso a la red
Fuente: Elaboración Propia

8.19. Finalmente nos conectamos y observamos que esta se realizó con éxito.

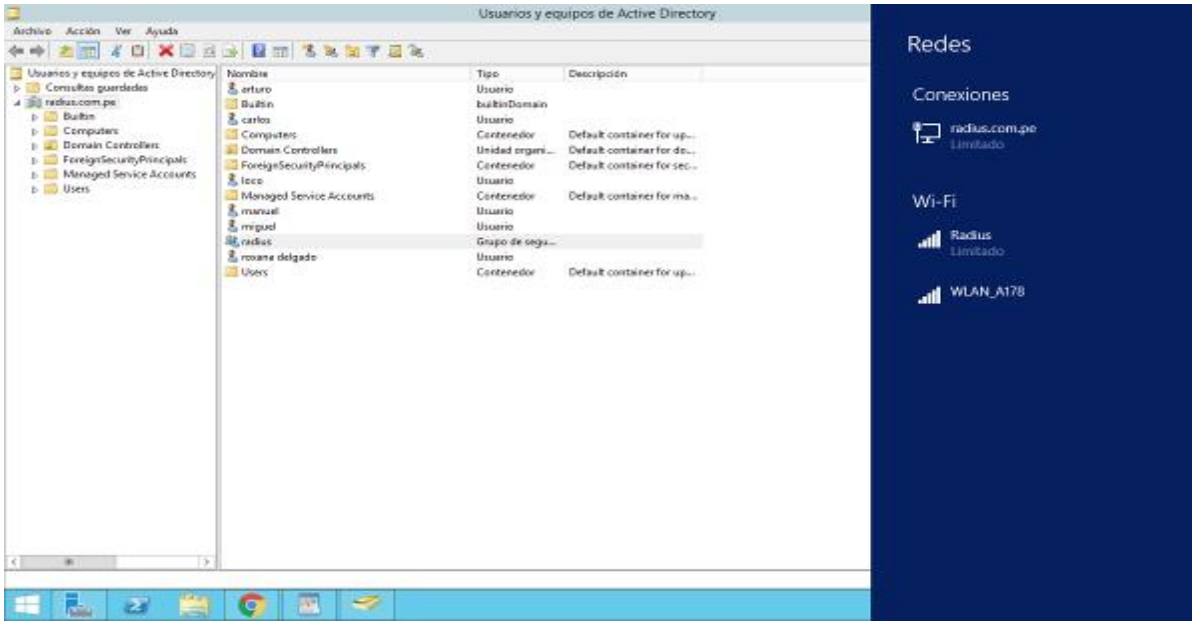


Figura N° 24. Configuración correcta del servidor Radius
Fuente: Elaboración Propia