ColloQUIUM
Editorial - Centro de Formación

Control de acceso a redes inalámbricas por medio de protocolos de autenticación de usuarios

Kriss Ivette Chinchay Quiroz
Violeta Alexandra Peña Fernández
Gilberto Carrión Barco
Denny John Fuentes Adrianzén
Anthony Hans Delgado Chavarri
Rayber Mario Yeckle Arteaga

Control de acceso a redes inalámbricas por medio de protocolos de autenticación de usuarios

Kriss Ivette Chinchay Quiroz
Violeta Alexandra Peña Fernández
Gilberto Carrión Barco
Denny John Fuentes Adrianzén
Anthony Hans Delgado Chavarri
Rayber Mario Yeckle Arteaga

ColloQUIUM
Editorial - Centro de Formación

Kriss Ivette Chinchay Quiroz
Violeta Alexandra Peña Fernández
Gilberto Carrión Barco
Denny John Fuentes Adrianzén
Anthony Hans Delgado Chavarri
Rayber Mario Yeckle Arteaga

Control de acceso a redes inalámbricas
por medio de protocolos de autenticación de usuarios

Editado por Colloquium
ISBN: **978-9942-600-42-4**
Primera edición 2022

La obra fue revisada por pares académicos antes de su proceso editorial, en caso de requerir certificación debe solicitarla a: sbores@colloquium-editorial.com.

Ecuador 2022

Kriss Ivette Chinchay Quiroz
Universidad Nacional Pedro Ruiz Gallo – Lambayeque, Perú
https://orcid.org/0000-0002-8210-0907
kchinchayq@unprg.edu.pe

Ingeniera en Computación e Informática por la Universidad Nacional Pedro Ruiz Gallo. Especialista en redes y seguridad informática para pequeñas y medianas empresas.

Violeta Alexandra Peña Fernández
Universidad Nacional Pedro Ruiz Gallo – Lambayeque, Perú
https://orcid.org/0000-0003-2706-1287
vpenaf@unprg.edu.pe

Ingeniera en Computación e Informática por la Universidad Nacional Pedro Ruiz Gallo. Especialista en redes y seguridad informática para pequeñas y medianas empresas

Gilberto Carrión Barco
Universidad Nacional Pedro Ruiz Gallo – Lambayeque, Perú
https://orcid.org/0000-0002-1104-6229
gcarrion@unprg.edu.pe

Ingeniero en Computación e Informática, Licenciado en Administración Pública, Magister en Docencia Universitaria, Maestro en Gestión Pública, Maestro en Ingeniería de Sistemas, Doctor en Ciencias de la Computación y Sistemas. Docente adscrito al Departamento Académico de Computación y Electrónica de la Universidad Nacional Pedro Ruiz Gallo de Lambayeque - Perú.

Denny John Fuentes Adrianzén
Universidad Nacional Pedro Ruiz Gallo – Lambayeque, Perú
https://orcid.org/0000-0003-4864-1352
dfuentesad@unprg.edu.pe

Ingeniero Informático y de Sistemas, Maestro en Administración con Mención en Gerencia Empresarial, Doctor en Ciencias de la Computación y Sistemas. Además, con Estudios Concluidos en la Maestría en Gestión Pública por EUCIM-USMP. Docente adscrito al Departamento Académico de Computación y Electrónica de la Universidad Nacional Pedro Ruiz Gallo de Lambayeque, Perú.

Anthony Hans Delgado Chavarri
Universidad Tecnológica del Perú – Chiclayo, Perú
https://orcid.org/0000-0003-1755-6833
c22470@utp.edu.pe

Profesional graduado en Ingeniería de Sistemas y Computación, con maestría en Dirección estratégica de Tecnologías de Información. Soy Microsoft Certified Trainer (MTC). Cuento con la Certificación Internacional de Excel Expert. Con amplios conocimientos y aplicación de gestión de servicio de TI con ITIL y también de estándares, normas de gestión de servicio de TI, además, manejo de base de datos, servidores y soporte de TI. Conocimiento de mejora continua en tecnologías de información (DevOps, KanBan, SCRUM, Protección de Datos), ISO 27001 e ISO 9001. Experiencia en asesoría de tesis de TI y Metodologías agiles. Experiencia como Coordinador Académico y Co- Gerente de CAP - IT CIX centro de certificación Internacional Microsoft.

Rayber Mario Yeckle Arteaga
Universidad Privada Señor de Sipán – Chiclayo, Perú
https://orcid.org/0000-0002-7526-0320
rayber.yeckle@untrm.edu.pe

Ingeniero de Sistemas, Maestro en Gestión Pública por la Universidad Privada Cesar Vallejo, Docente contratado en la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas – Perú, adscrito al Departamento Académico de Ingeniería de la Facultad de Ingeniería de Sistemas y Mecánica Eléctrica. y jefe del Área de Informática de la Red de Salud Bagua de Amazonas - Perú

Prólogo

El uso esencial de las redes inalámbricas en la actualidad ha tomado gran protagonismo en nuestro día a día, pues la época de vivencia que afrontamos al atravesar por una pandemia mundial nos ha enseñado a depender del mundo virtual; debido a esto es de gran importancia mantener segura la información que poseemos dado que existe la posibilidad de ser vulnerada por usuarios maliciosos que tratan de apropiarse o darle uso indebido. Por lo tanto la presente investigación tiene como principal objetivo analizar los protocolos de autenticación de usuarios en el control de acceso a datos en redes inalámbricas de área local por medio de la comparación de protocolos de seguridad de red para garantizar la correcta elección del protocolo a implementar, presenta una metodología de tipo aplicada con un alcance descriptivo y un enfoque cualitativo con un diseño narrativo de tópicos, contando como participantes cuatro protocolos de autenticación a comparar: RADIUS, TACACS +, DIAMETER y KERBEROS, siendo divididos los criterios de comparación utilizados en 3 categorías: Características básicas de autenticación, Forma de trabajo del protocolo de autenticación y Funcionalidad AAA. Asimismo, se concluye que la investigación realizada sobre la comparación de protocolos de autenticación de usuarios obtuvo como resultado la elección del protocolo RADIUS, realizando su implementación por medio del servidor FreeRADIUS y LDAP en una máquina virtual; demostrando su viabilidad.

INTRODUCCIÓN

El ritmo acelerado de las redes inalámbricas en la actualidad nos permite considerarlas como el medio de transporte de datos indispensable en organizaciones u hogares, ya que están al alcance de cualquier persona; debido a esto es de gran importancia mantener segura dicha información ya que existe la posibilidad de ser vulnerada por usuarios maliciosos que tratan de apropiarse o darle uso indebido, llegando a exponer la confidencialidad y veracidad de los datos.

Las redes inalámbricas hacen uso de ondas de radio para poder conectar dispositivos y convertir las señales de información en una forma adecuada para que pueda ser transmitida por medio de aire. Estas redes permiten a los dispositivos remotos que se puedan conectar, independientemente de la distancia que se encuentren ubicados. Todo ello sin necesidad de alternativas e instalaciones cableadas, haciendo que el uso de esta tecnología sea sumamente conocido y con una rápida extensión (Salazar, 2016).

Actualmente, las organizaciones hacen todo lo posible para sostener el control y contribuir con resguardar sus redes corporativas y su base de información de las vulnerabilidades cibernéticas, por esta razón se resalta la indispensable seguridad de datos mientras se transporta por la red pública (Carrión-Barco et al., 2021).

Los estragos de la pandemia que estamos afrontando, han demostrado un crecimiento del trabajo remoto, reavivando el interés de los ciberdelincuentes por los ataques de fuerza bruta, los cuales se utilizan usualmente para descifrar algoritmos de cifrado u obtener contraseñas débiles, contraseñas de correo electrónico, credenciales de redes sociales, acceso a Wi-Fi, etcétera; intentando su acceso múltiples veces hasta que logren el objetivo (Fortinet, 2020).

Gutiérrez (2020) expresó que, entre los meses de enero y junio del año 2020, México recibió en totalidad 3 mil 100 millones de intentos de ciberataques entre empresas, instituciones financieras y gubernamentales. Eduardo Zamora, director de Fortinet México consideró que el aumento del trabajo a distancia y la "teleducación" ha reanimado el interés de los hackers por la existencia de una notable cantidad de servidores de protocolo de escritorio remoto mal configurados. Asimismo Prensa Latina (2020) manifestó la cantidad de intentos de ciberataques

a las plataformas digitales de Panamá, siendo 655 millones durante los primeros seis meses del año 2020, revelado en un informe de Threat Intelligence Insider Latin America de Fortinet, detectando también ciberataques conocidos como el phishing y el ransomware, los cuales colocaban el peligro la seguridad de la red, contando con una de las denuncias más recientes por parte del Ministerio de Educación de Panamá, siendo víctima de intento de ciberataque.

Además, esta pandemia ha provocado graves crisis económicas y sanitarias en todo el mundo. Sin embargo, otra consecuencia de COVID-19 es que las organizaciones han acelerado su digitalización e inversión en tecnología. El experto de la multinacional ABB ofrece algunas sugerencias para que puedan disminuir los riesgos de ciberataques que amenacen su seguridad operativa: (1) Desarrollar una copia de seguridad o contar con una política de back-up. (2) Realizar auditorías y monitoreos continuos para descubrir situaciones anormales a tiempo. (3) Crear "listas blancas" para ejecutar programas. (4) Desarrollar estrategias claras de identificación y autenticación de usuarios para el acceso y operaciones para cada usuario. (5) Actualice continuamente los programas de antivirus y los sistemas operativos (Gestión, 2020a).

Los ciberataques están presentes hasta en situaciones electorales, de tal manera señaló Microsoft en el año 2020, al haber descubierto 200 ataques vinculados a grupos de hackers rusos contra personal de campaña y consultores políticos para las elecciones presidenciales de los Estados Unidos. El vicepresidente de seguridad de clientes de Microsoft, Tom Burt, confirmó que este mismo grupo de ciber espías rusos habían intervenido en las elecciones estadounidenses del año 2016. Burt hizo mención que piratas informáticos chinos habían importunado a personas “estrechamente asociadas con las campañas y candidatos presidenciales de Estados Unidos”, además agregó que los piratas informáticos iraníes habían hecho el intento de iniciar sesión en cuentas pertenecientes a funcionarios del mandatario republicano Donald Trump y de miembros de su personal de campaña (Gestión, 2020b).

Siendo una realidad que se viene presentando mundialmente, Prakash & Kumar, (2018) afirman que la seguridad puede considerarse la columna vertebral de cualquier sistema distribuido proporcionada por protocolos de autenticación, siendo necesario que funcione correctamente. En el diseño de protocolos de Internet, la

seguridad se plantea de manera estructurada mediante el análisis de amenazas, lo que requiere una comprensión de alto nivel de la arquitectura de comunicación del protocolo y luego derivando los requisitos de seguridad (Tschofenig et al., 2019).

En el presente año 2021, según el estudio Estado del Riesgo Cibernético en Latinoamérica en Tiempos del COVID-19 el 49% de las empresas peruanas percibió un aumento en los ataques cibernéticos, además se revela por medio de la encuesta que el 21% considera que el phishing es el ataque ciberataque que ha incrementado mientras tanto el 20% sostiene que ha sido el malware. El phishing sucede cuando un farsante al ganarse la confianza de su víctima (que puede ser una persona, empresa o servicio) llega a conseguir que le revelen información o haga clic en un enlace peligroso, lamentablemente solo el 20% aumentó su presupuesto de ciberseguridad durante la pandemia, el 51% en seguridad de acceso remoto y el 44% en seguridad en la nube (Gestión, 2021).

Nuestro país fue víctima de los cibercriminales entre enero y junio del año 2020, ascendiendo a la cifra de 600 millones de intentos de ciberataque. Llegando a posicionarse como el quinto país con más diligencia cibercriminal de 10 países analizados, entre los cuales se encuentran Colombia, Brasil, Argentina, Chile, Panamá entre otros (El Comercio, 2020).

Las amenazas a la red y la privacidad continúan aumentando y expandiéndose. Sin embargo, según la Encuesta Global de Seguridad de la Información, muestran que entre las empresas peruanas que participaron en dicha encuesta, un número considerable del 59% no cuenta con un responsable de seguridad cibernética para reportar al directorio o no tiene nivel de gestión ejecutiva. Aunque la gestión de riesgos y la ciberseguridad son realmente necesarias para prevenir ataques a la red, no son mecanismos de protección completamente seguros. Por ello, en la actualidad es vital brindar protección adicional, que pueda controlar y mitigar los efectos negativos de los delitos informáticos, como enormes pérdidas económicas relacionadas con interrupciones operativas, pérdida o robo de información sensible, juicios por fraude o estafa, o violar la privacidad de los datos personales (Gestión, 2020d).

Chira (2020) manifestó que se ha descubierto el 51.6% de los usuarios de las herramientas informáticas sin seguridad y el 99% considera que nos hace falta

capacitaciones sobre seguridad para evitar los ciberataques en una empresa. Diversas empresas e instituciones presentan esta problemática, como lo menciona Mamani (2019) en la Universidad Nacional del Altiplano, los servidores no cuentan con un monitoreo constante para cada usuario y eso no es garantía de seguridad, ya que, personas ajenas a la universidad podrían interferir en la red Wi-Fi, ocasionando deficiencias.

Asimismo, Gestión (2020c) alude uno de los sectores más atacados, fue el bancario pues se registraron cientos de intentos de quebrantamiento a los sistemas de seguridad. Aunque es cierto la pandemia ha impedido la realización de diversas actividades, existen acciones indispensables que forman parte de la actividad económica del país; y estas son las transacciones financieras, realizándose en un 95% por Internet.

Los investigadores de seguridad de SophosLabs han explicado que las familias de ransomware, van a seguir perfeccionando y modificando sus técnicas y métodos para convertirse más evasivas sin embargo se continuará usando malware básico, determinan que los cibercriminales utilizan herramientas legítimas, por lo tanto, se convierte mucho más peligrosa al estar fuera del radar mientras se mueven por la red hasta estar preparados para lanzar la parte principal del ataque. Se consideró que la tendencia en el 2021 está basada en atacar a empresas pequeñas porque permiten amenazar a sus víctimas con difundir la información o datos privados y lanzar nuevos ataques a servidores de las organizaciones que lograrían alarmar a los empleados que están realizando trabajo remoto y no tienen redes personales protegidas para su conectividad (El Peruano, 2020).

Generalmente, al realizar la implementación de puntos de acceso inalámbrico en la red de una organización de tipo corporativo, se opta por un protocolo y un método de acceso que cumpla con las políticas definidas por dicha organización. Se definen también, en esta elección, las características que deben cumplir los dispositivos de los usuarios, excluyendo a todos los equipos que no cumplen con dichas características (Espinoza, 2018).

Por lo tanto, la presente investigación “Comparación de protocolos de autenticación de usuarios en el control de acceso a redes inalámbricas”, plantea la formulación del problema de la siguiente manera ¿cuáles son los protocolos de autenticación

de usuarios que garanticen el control de acceso a datos en redes inalámbricas de área local?

Presentando como principal objetivo analizar los protocolos de autenticación de usuarios en el control de acceso a datos en redes inalámbricas de área local por medio de la comparación de protocolos de seguridad de red para garantizar la correcta elección del protocolo a implementar y como objetivos específicos (1) Obtener información científica relacionada con los protocolos de autenticación de usuarios por medio de la revisión sistemática de la literatura en base de datos, siguiendo los criterios de búsqueda, (2) Esquematizar la información científica relacionada con los protocolos de autenticación de usuarios a través de la comparación de atributos y características de estos por medio de tablas de análisis, (3) Proponer el método de control de acceso apropiado mediante la implementación del protocolo seleccionado para redes inalámbricas y (4) Corroborar la factibilidad y valor científico de los resultados de la investigación mediante juicio de expertos.

La investigación se justifica de manera social, puesto que promueve la resolución de la vulnerabilidad e inseguridad que día a día vienen presentando las redes inalámbricas; de manera metodológica, porque permite identificar el modo perjudicial que afecta a diversas organizaciones y hogares brindando la posibilidad de ser una guía a utilizar para mejorar su seguridad cibernética; finalmente de manera tecnológica, ya que mediante la comparación de protocolos de autenticación de usuarios a realizar nos va permitir elegir el protocolo óptimo para reducir los ataques y vigilar el control de acceso.

Se aborda la siguiente hipótesis: mediante la comparación de protocolos de autenticación de usuarios y posterior elección de uno de ellos, se podrá garantizar el control de acceso a datos en redes inalámbricas de área local. Aplicando una metodología de tipo aplicada con un alcance descriptivo y un enfoque cualitativo con un diseño narrativo de tópicos. Finalmente siendo dividida en cinco capítulos.

CAPÍTULO I

Como antecedentes internacionales tenemos Pradeep et al. (2019) en su investigación "*Verificación formal de autenticación y confidencialidad para el protocolo de seguridad TACACS + usando Scyther",* manifestaron que para los sistemas de comunicación, la confiabilidad de los protocolos de seguridad es muy importante porque los agentes que se comunican compartirán datos confidenciales en redes públicas que no son de confianza. Pradeep et al. (2019) tuvieron como objetivo verificar formalmente el protocolo de seguridad TACACS+, usando la técnica Model Checking, empleando el verificador de modelos Scyther. Los autores propusieron dos modelos para el protocolo TACACS+, llegando a la conclusión que el modelo 1 no proporcionó los requisitos de propiedad de seguridad de autenticación y confidencialidad; todo lo contrario, al modelo TACACS+ 2, proporcionó con éxito la propiedad de seguridad Confidencialidad y Autenticación. Además, por medio del verificador de modelos Scyther se demostró que es seguro.

Además, Andrade (2019) en su indagación *"Análisis de prestaciones de los protocolos de autenticación remota RADIUS y TACACS+ en Infraestructura de Comunicaciones Corporativas"*, planteó como objetivo analizar los servicios de los protocolos de autenticación remota RADIUS y TACACS+ en la infraestructura de comunicaciones corporativas, la cual presentó inconvenientes con el manejo de sus redes, principalmente en redes WLAN, aspirando al estudio de las características y servicios de los protocolos mencionados también diseñar el ambiente de prueba para validar la prestación de cada protocolo en un ambiente Open Source para finalmente evaluar y constatar su funcionamiento correcto, realizando encuestas a los directivos de diversas entidades públicas de Riobamba. Concluyendo que el tiempo de autenticación Radius es más eficiente que TACACS+ y en cuestión de seguridad TACACS+ es el más adecuado por protocolos de transporte, interoperabilidad. Andrade (2019) recomendó priorizar costos e implementación.

Asimismo, Prakash & Kumar (2018) en su artículo *"Protocolos y técnicas de autenticación: una encuesta"*, mencionaron que el objetivo fue estudiar los métodos

de autenticación más utilizados teniendo en cuenta sus ventajas y desventajas, haciendo uso de la descripción de los protocolos de autenticación que son más usados e implementados en el mundo, concluyendo que en su mayoría cubren el marco EAP usualmente empleado.

Por su parte, Cuzme & Bosmediano (2017) en su investigación *"Administración y gestión de usuarios para acceso a la red inalámbrica de la Facultad de Ingeniería en Ciencias Aplicadas basado en el Protocolo 802.1x",* que tuvo como objetivo incrementar los niveles de seguridad en el intercambio de información dentro de la red inalámbrica de la Facultad de Ingeniería en Ciencias Aplicadas. Consistió en el diseño e implementación de un servidor que proporcione Autenticación, Autorización y Auditoria (AAA) en la red inalámbrica de la Facultad de ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte, utilizando el método EAP-TTLS basados en el protocolo IEEE 802.1x. El estudio tuvo como principal conclusión obtener una gestión centralizada de usuarios a través del servidor implementado, contando con apoyo de una distribución equitativa del recurso a través del método de colas simples (QUEUES), garantizando de esta forma una conexión más sólida, certera y confiable ante posibles ataques informáticos, a su vez despejando la disponibilidad de la red.

Teniendo en cuenta a González et al. (2016) en su estudio investigativo *"Propuesta de protocolos de seguridad para la red inalámbrica local de la Universidad de Cienfuegos",* cuyo objetivo fue comparar los protocolos de seguridad con la selección de los que formarán parte de la propuesta para la red WLAN de la Universidad de Cienfuegos haciendo uso de un análisis comparativo, apoyado en el método de autenticación y la técnica de cifrado. Concluyendo que el estándar WAP2 fue la alternativa más certera para el campus de la universidad mencionada, la cual requiere autenticación y auditoría de los usuarios con sus credenciales. Identificando los requisitos de seguridad que se quieren obtener, de esta manera se puedan emplear los protocolos combinándolos, según las necesidades.

También podemos mencionar a Singh et al. (2016) en su indagación *"Relevamiento y análisis del sistema de autenticación moderno"*, contempló como objetivo analizar diversos protocolos autenticados teniendo en cuenta sus ventajas y desventajas, peligros a la seguridad, vulnerabilidades y su defensa al ataque. Haciendo uso de la encuesta y análisis de algunos protocolos como método, llegando a la conclusión que los protocolos PAP y SPAP son más débiles a los ataques de seguridad en comparación con EAP, Kerberos, CHAP, MS-CHAP, que son competentes y se mantienen firmes ante los ataques de seguridad.

Cristescu et al. (2016) en su artículo *"Implementación de una solución AAA-RADIUS basada en protocolos de autenticación heredados"*, plantearon una solución vinculada con la autenticación, autorización y contabilidad de los usuarios que tienen la intención de ingresar a Internet mediante una red segura, aplicando el protocolo RADIUS el cual fue utilizado para encapsular paquetes de los protocolos de autenticación heredados además de hacer uso para el diseño y la implementación el Programa 8950 AAA, de esta manera concluyeron que este resultado de servidor se puede autenticando usuarios mediante protocolos heredados, realizar escenarios de autenticación, autorización y contabilidad con finalidad educativa y para depurar e identificar cualquier error en el programa 8950 AAA para ciertos escenarios.

Pacyna & Chrabaszcz (2016) en su artículo *"Evaluación del protocolo de reautenticación EAP"*, mencionaron que cuando el host móvil realiza el proceso de conexión a la red inicial en un sistema inalámbrico o celular, una gran parte del retraso en el acceso a la red se debe a la autenticación, autorización y generación de un material de codificación criptográfico. El propósito de su artículo fue evaluar mejoras al Protocolo de Autenticación Extensible (EAP) introducido con el Protocolo de Reautenticación EAP (ERP), que está diseñado para su uso en el sistema de Autenticación, Autorización y Contabilidad (AAA), utilizando una metodología cualitativa. Llegando a la conclusión que las nuevas características del protocolo (especialmente las extensiones del protocolo y el nuevo marco de gestión de

claves) disminuyen la sobrecarga de señalización, descargan el servidor y mejoran la seguridad de los enlaces inalámbricos.

Ghilen et al. (2015) en su artículo "*Integración y análisis de seguridad formal de un esquema de distribución de claves cuánticas dentro del protocolo CHAP*", tuvieron como objetivo la presentación y mejora de la seguridad CHAP mediante una extensión cuántica nueva, la cual conforma la criptografía cuántica y utiliza sus beneficios, para poder estudiar la seguridad del protocolo mencionado se hizo uso de la herramienta PRISM como revisor de modelo obteniendo como conclusión que debería ser obligatorio aumentar el número de fotones transmitidos N demostrando que el enfoque de revisión de modelos mostró que su extensión cuántica CHAP proporciona un acuerdo de claves.

Colombo et al. (2015) en su investigación "*Problemas y desventajas que impiden la implementación nativa de Single Sign On basado en Kerberos en sistemas Linux*", plantearon como objetivo discernir problemas y desventajas que los usuarios deben contender cuando intentan utilizar el mecanismo de inicio de sesión único, haciendo uso en conjunto con el Protocolo Kerberos V5 como medio de autenticación de usuarios en ambiente Linux. Dado lo expuesto a lo largo del escrito, se deduce que al requerir instalaciones o configuraciones en los distintos clientes trae consigo grandes desventajas, una gran desventaja es la complejidad para ejecutar el sistema de manera completa en un periodo importante y de corto tiempo.

Citando a Alonso (2013), en su estudio investigativo "*Análisis comparativo de dos protocolos para control de acceso y administración de equipos de telecomunicaciones*", cuyo objetivo fue realizar una comparación específica entre estos dos protocolos, precisando fundamentalmente sus características de funcionamiento, ventajas, desventajas y aplicaciones para contar con estándares suficientes y poder hacer una recomendación sobre la elección de uno de ellos. La metodología empleada en esta investigación tuvo un alcance descriptivo propositivo, concluyendo que el conjunto de protocolos AAA tiene las

características adecuadas en el esquema de seguridad de la red de comunicaciones actual y tiene la posibilidad de verificación de identidad, autorización y auditoría.

Dentro de los antecedentes nacionales podemos citar a Mamani (2019) en su investigación "*diseño e implementación de un sistema de administración, autenticación y control en el estándar 802.11 en el centro de comunicaciones de la universidad nacional del altiplano*", tuvo como objetivo comunicar a los usuarios de la Universidad Nacional del Altiplano acerca de la gran importancia de mantener seguras las redes inalámbricas, basándose en la susceptibilidad que existe en el entorno profesional, la cual es aprovechada por los ciberdelincuentes. El método de estudio aplicado fue tecnológico ya que desarrolló los efectos producidos por un sistema con protocolos AAA con Radius, a la vez correlacional. Llegando a la conclusión que logró implementar un servidor RADIUS, autenticando a 70 usuarios registrados como operarios del Centro de Comunicaciones logrando la prohibición de acceso a 30 de ellos, que no fueron registrados en dicho servidor, comprobando que cada usuario empleara contraseñas seguras. Mamani (2019) nos recomendó realizar copias de seguridad en los servidores y equipos mediadores como también supervisar pertinentemente la auditoría de red.

Espinoza (2018) en su estudio "*Desarrollo e implementación de un sistema de control de acceso a redes inalámbricas mediante RADIUS*", manifestó que el objetivo de su investigación, fue indagar el desarrollo de un diseño para la implementación de un sistema de seguridad inalámbrica que logrará controlar la acción de los usuarios en el Instituto Geofísico del Perú, considerándose de tipo tecnológica correlacional. Tecnológica porque se planteó desarrollar e implementar los efectos que produce un sistema de seguridad de control de acceso con RADIUS y correlacional porque cuantificó el grado de relación entre las variables. Concluyendo que a lo largo de la investigación se ha señalado diferentes mecanismos de protección y amparo de la información que implica el uso de estándares de seguridad para las aplicaciones que utilicen dispositivos móviles y también RADIUS. Considerando como recomendación del autor, desarrollar un

plan de trabajo, analizando los recursos tecnológicos para que sean capaces de soportar nuevas tecnologías además de comprender la realidad y la perspectiva de los usuarios, para contar con la aceptación de todos los empleados y Alta Dirección, al proponer una mejora.

Teniendo en cuenta a Tafur & Chavez (2018), en su indagación "*análisis de protocolos de protección de redes inalámbricas Wi-fi para la detección de vulnerabilidades frente a posibles ataques que atenten contra la seguridad de la información*", se basaron en la búsqueda de soluciones concernientes a los inconvenientes que existen entorno a la frágil seguridad que es aprovechada por los ciberatacantes, considerando como objetivo principal indagar los protocolos de seguridad de redes inalámbricas, con el fin de reducir las vulnerabilidades a posibles ataques, para salvaguardar la información. En cuanto a su metodología empleada fue comparativa y tecnológica, ya que realizaron una investigación semejante de los mecanismos de seguridad para hallar la tecnología más segura. Concluyendo así que Tafur & Chavez (2018) lograron descubrir su manejo y debilidades por medio del estudio comparativo de las vulnerabilidades. Recomendando tener en cuenta la monitorización de las redes Wi-Fi.

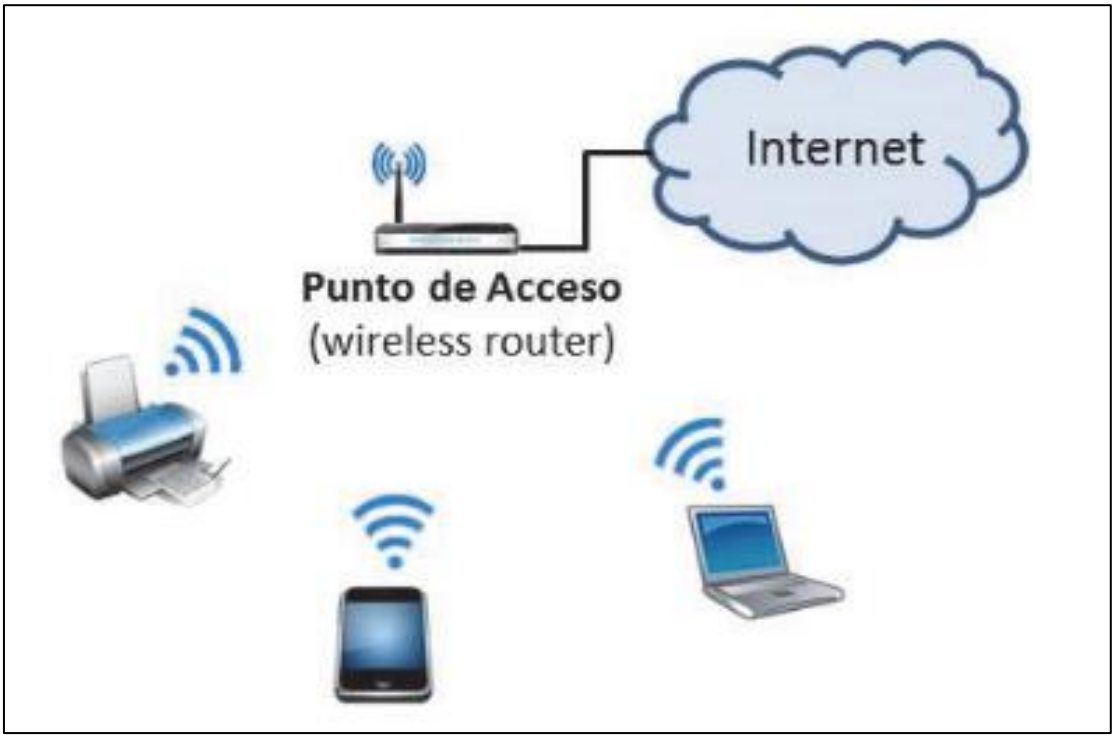
De acuerdo con Bardales (2015) en su investigación "*sistema de gestión de acceso a una red Wi-fi utilizando software libre para mejorar el nivel de seguridad del acceso a la información*", tuvo como objetivo principal la mejora del nivel de seguridad al momento de ingresar información a la Municipalidad Distrital de la Esperanza, logró obtener información aplicando entrevistas y encuestas al personal de la municipalidad; haciendo uso del método de análisis de datos, la Prueba Z de diferencia de medias, destinando la prueba t Student para indicador de nivel de satisfacción junto con la metodología de Jerry FitzGerald se consideró como la opción más acertada para el desarrollo del proyecto. La implementación del sistema admitió el control de los usuarios y perfeccionó la velocidad de entrega de la información en la institución. Llegando a la conclusión que se ha logrado la grande mejora del nivel de seguridad informativa gracias a la implementación del sistema.

Wireless Local Area Network (WLAN)

Como expresa Salazar (2016), las Redes Inalámbricas de Área Local (WLAN) brindan acceso inalámbrico con un rango usual de hasta 100 metros, lo cual facilita a los usuarios la capacidad de moverse dentro de un área de cobertura local y aun así continuar conectado a la red, están constituidas en el estándar IEEE 802.11, el cual cuenta con diferentes estándares para redes inalámbricas de área local, el primer estándar aceptado fue el IEEE 802.11b, que permitía hasta 11 Mbps en la banda frecuencial sin licencia de 2,4 GHz. Su sucesor es el estándar IEEE 802.11g, diseñado con un mayor ancho de banda. Un punto de acceso IEEE 802.11g admitirá clientes 802.11b y 802.11g. De manera similar, las computadoras portátiles con tarjeta IEEE 802.11g podrán acceder a los puntos de acceso 802.11b existentes, así como a los nuevos puntos de acceso 802.11g. La velocidad máxima de transmisión del enlace inalámbrico IEEE 802.11g es de 54 Mbps, pero disminuirá automáticamente cuando la señal de radio sea débil o se detecten interferencias.

Las WLAN, hacen uso de radiofrecuencia para transferir y recibir datos por aire, minimizando así la necesidad de conexiones por cable (Cisco, s. f.-c).

Figura 1: Esquema de una WLAN en hogar



Fuente: Salazar (2016)

Ventajas de las WLAN

García (2013) menciona que es sabido que se necesita una red de comunicación que permita compartir información de manera más sencilla sin realizar movilidad entre equipos. Las redes inalámbricas o WLAN representan las siguientes ventajas:

- La movilidad que brinda este tipo de redes permite conseguir información de cualquier parte de una empresa u organización, en tiempo real, la producción de esta información figura mayor productividad a la empresa y más posibilidades de servicio.
- Una de sus ventajas más importantes, es su fácil instalación, pues no requiere ni necesita algún tipo de cableado.
- De uso es muy flexible, se puede llegar a muchos lugares a comparación de las redes cableadas totalmente limitadas.
- Puede que requiera una inversión inicial de costo sin embargo tiene mayor tiempo de vida y su mantenimiento e implementación es de menor gasto.
- Es escalable, referente a las modificaciones en la topología de la red, se realizan de manera sencilla.

Aspectos importantes en las WLAN

Según García (2013) los aspectos más importantes son:

Cobertura

La distancia a las que pueden llegar las ondas de radiofrecuencia o de infrarrojos va en función del diseño del producto y del camino de propagación, de manera especial en lugares cerrados. Los sistemas de redes inalámbricas, en su mayoría, hacen uso de la radiofrecuencia porque pueden atravesar la mayor parte de los lugares cerrados y toda clase de obstáculos, teniendo una cobertura típica que va de 30m a 100m.

Rendimiento

El rendimiento de una WLAN se somete a una serie de parámetros, algunos de ellos son:

- Número de usuarios
- Del retardo de la red
- Factores de propagación

- Tipo de sistema inalámbrico utilizado

Integridad y fiabilidad

Estas redes siendo testeadas por muchos años, poseen actualmente diseños vigorosos brindando integridad de datos, igualando o superando a una red cableada.

Compatibilidad con las redes existentes

En su mayoría, brindando un estándar de interconexión con redes cableadas (Ethernet o Token Ring), sus nodos son sostenidos por el sistema de la red de la misma manera que cualquier otro nodo de una red LAN.

Simplicidad y facilidad de uso

La naturaleza de las redes inalámbricas, es clara usuario, las aplicaciones trabajan de la misma manera como si se trabajara en una red cableada. Una WLAN incorpora herramientas para orientar problemas asociados a los elementos inalámbricos del sistema, en una red inalámbrica rara vez se requiere su uso.

Seguridad en la comunicación

La seguridad ha sido uno de los principios para diseñar dispositivos inalámbricos. Usualmente dentro de las redes WLAN, se aprovisionan elementos de seguridad haciendo que estas sean mucho más seguras que las redes cableadas en su mayoría.

Escalabilidad

Las redes WLAN tiene un diseño que puede tolerar un amplio número de nodos y/o extensas áreas físicas agregando puntos de acceso para dar energía a la señal o para extender la cobertura.

Alimentación en las plataformas móviles

En los productos WLAN, los fabricantes emplean técnicas para maximizar el uso de la energía del computador y el tiempo de vida de su batería.

Seguridad laboral

La potencia de salida de los sistemas WLAN es muy baja, dado que las señales de radio se atenúan prontamente con la distancia, por lo tanto, estas redes deben cumplir normas precisas de seguridad.

UBUNTU

Según Ubuntu (2021), es una añeja palabra africana que tiene la connotación de "humanidad para los demás". La distribución de Ubuntu simboliza lo superior de la sociedad global que comparte software en el mundo, siendo el escritorio de Ubuntu una de las plataformas de estación de trabajo Linux más utilizada en el mundo.

Linux fue implantado en el 2004, dividido en ediciones comunitarias patentadas sin apoyo ni software libre, por lo tanto, Mark Shuttleworth se agrupó con un equipo de desarrolladores de Debian proponiendo crear un escritorio Linux fácil de usar llamado Ubuntu.

El primer lanzamiento oficial de Ubuntu con versión 4.10 denominado 'Warty Warthog', Ubuntu hoy tiene muchas derivaciones. Existen ediciones especiales para servidores, nubes OpenStack y dispositivos conectados, lo que convierte a Ubuntu en una plataforma exclusiva que se escala desde la electrónica de consumo hasta el escritorio y hasta la nube para la informática empresarial.

Entre sus ventajas: es un software gratuito para todos con los mismos términos, disminuye costos de los servicios profesionales, el lanzamiento de actualizaciones continuas está disponibles gratuitamente para todos los usuarios y se puede obtener soporte, consultoría y mayores herramientas mediante la página oficial de Ubuntu.

LDAP

Según LDAP (2021), Lightweight Directory Access Protocol significando en español Protocolo ligero de acceso a directorios es un mecanismo y protocolo juicioso, manejable y bien soportado fundado en estándares asentados sobre TCP/IP para relacionarse con servidores de directorio incorporado. Usualmente utilizado para la autenticación, el almacenamiento y recuperación de información sobre usuarios, grupos y aplicaciones. Un servidor de directorio LDAP es un depósito de datos que permite utilizarlo en variedad de aplicaciones.

Los puertos TCP estándar para LDAP son 389 para comunicaciones no cifradas y 636 para LDAP a través de un canal cifrado TLS, aunque no es raro que los servidores LDAP escuchen en puertos alternativos por una variedad de razones.

WINDOWS SERVER

Microsoft Windows Server es una serie de sistemas operativos de servidor de nivel empresarial diseñados para compartir servicios entre múltiples usuarios y proporcionar un control de gestión integral sobre las redes empresariales, las aplicaciones y el almacenamiento de datos. Las principales funciones de Windows Server incluyen Active Directory, administración de información del usuario, seguridad y la capacidad de colaborar con otros directorios (SoftTrader, 2021).

Windows Server fue creado para ser uso del servidor, por lo que tiene muchas ventajas para empresas que hacen uso de él; incluso puede reducir el tiempo de configuración de hardware y software. Esta herramienta de Microsoft tiene programación en C ++ y, debido a sus múltiples ventajas, millones de empresas en todo el mundo la utilizan. El sistema es fácil de usar, por lo que puede ser operado por cualquier miembro de la empresa. Además de administrar archivos de forma centralizada, Windows Server también administra archivos. Este tipo de servidor multiusuario puede mejorar los resultados operativos generales. Al mismo tiempo, por su sencilla gestión, se puede manejar de forma fácil y rápida (Anónimo, 2020).

Según De León (2019) Windows Server cuenta con las siguientes versiones:

- Windows 2000
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019

Una de las ventajas de Windows Server es que su aprendizaje es mucho más fácil a diferencia de otros sistemas, es similar a las versiones de escritorio que ya se conocen, aunque la versión de servidor contiene diferentes herramientas y servicios, lo hace de la misma forma, haciendo que el sistema se sienta familiar. Otra de sus ventajas es que cuenta con el respaldo técnico y soporte de una de las

empresas tecnológicas más grandes, los programas de capacitación y certificación que brindan aseguran una capacitación. Por el contrario, como todo sistema también posee ciertas desventajas, empezando por la principal, el no ser gratuito, su licencia posee un costo.

KALI LINUX

Kali Linux es un sistema operativo de código abierto, en versión perfeccionada y mejorada de la distro BackTrack basada en Debian, siendo creada por Offensive Segurity lanzada en el año 2013. El principal objetivo es colocar a disposición una de las mejores herramientas para trabajar la auditoría en internet y tener un gran sistema de seguridad informática ante los peligros que puedan existir asegurando que nuestros equipos informáticos puedan acceder a Internet sin riesgo de sufrir ataque de hackeo (Instituto Superior de Ciberseguridad, 2018).

Entre sus características principales (Kali, 2021):

- Cuenta con más de 600 herramientas de prueba de penetración incluidas, ubicadas en el sitio de Kali Tools.
- Es completamente gratuito y siempre lo será.
- Constante desarrollo del Árbol de Git de código abierto, todo el código fuente que se incluye en Kali Linux está disponible para cualquiera que desee modificar o reconstruir paquetes para satisfacer sus necesidades específicas.
- Compatible con FHS, se adhiere al Estándar de jerarquía del sistema de archivos, permitiendo a los usuarios localizar archivos de soporte, bibliotecas, etc.
- Compatible con dispositivos inalámbricos de amplio alcance, admite tantos dispositivos inalámbricos como sea posible.
- Posee kernel personalizado.
- Es desarrollado en un entorno seguro, haciendo uso de múltiples protocolos seguros.
- Todos los paquetes y repositorios están firmados por GPG.

- Posee soporte multilingüe, se ha logrado que Kali permita a más usuarios operar en su idioma nativo y localizar las herramientas que necesitan para el trabajo.
- Completamente personalizable: entendemos perfectamente que no todos estarán de acuerdo con nuestras decisiones de diseño, por lo que hemos hecho que sea lo más fácil posible para nuestros usuarios más aventureros personalizar Kali Linux a su gusto, hasta el kernel.
- Compatibilidad con ARMEL y ARMHF, pues los sistemas de placa única basados en ARM como Raspberry Pi y BeagleBone Black, entre otros, se están volviendo cada vez más frecuentes y económicos. Kali Linux está disponible en una amplia gama de dispositivos ARM y tiene repositorios ARM integrados con la distribución principal.

WIRESHARK

Considerado como el analizador de protocolos de red más notable y usado del mundo. Da acceso a poder ver lo que sucede en la red a manera microscópica. El desarrollo de Wireshark fue prospero gracias a las contribuciones voluntarias de expertos en redes de todo el mundo además de ser la sucesión de un proyecto iniciado por Gerald Combs en 1998. Entre las funciones principales de Wireshark, se incluye: Wireshark tiene un rico conjunto de funciones que incluye lo siguiente (Wireshark, 2021):

- Inspección a detalle de diversos protocolos, siendo actualizados constantemente.
- Captura en vivo y análisis fuera de línea.
- Es multiplataforma, se puede ejecutar en Windows, Linux, macOS, Solaris, FreeBSD, NetBSD y muchos otros.
- Realiza un análisis integro de VoIP.
- Los análisis en vivo se pueden leer desde Ethernet, IEEE 802.11, PPP / HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI y más.
- Permite descifrar muchos protocolos, incluidos IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP y WPA / WPA2

Figura 2: Interfaz de Página Principal Wireshark

Fuente: (Wireshark, 2021)

Además, Wireshark, intercepta el tráfico y lo modifica a un formato legible a entender, siendo más sencillo identificar el tráfico que está cruzando la red, en frecuencia y la latencia. Sin duda, los profesionales encuentran una gran utilidad en el análisis de identidades IP con esta herramienta, la mayoría de los paquetes son TCP, UPD e ICMP (España, 2018).

ACCESS POINT

Es un dispositivo de red que autoriza a dispositivos con capacidad inalámbrica para poder conectarse a una red cableada. También se puede usar un Access Point o extensiones de malla para ampliar la potencia y alcance de la señal de su red inalámbrica con la finalidad de proporcionar una cobertura inalámbrica completa. Existen diversos tipos de configuraciones más comunes siendo a continuación (Cisco, s. f.-a):

- **Access point de raíz**

Se conecta directamente a una LAN cableada, proporcionando un punto de conexión para usuarios inalámbricos. Si existe más de un access point conectado a la LAN, los usuarios pueden pasar de una zona de las instalaciones a la otra zona sin perder la conexión de red.

- **Access point repetidor**

Puede configurarse como repetidor independiente amplificar el alcance de la infraestructura o aventajar algún obstáculo que bloquea las comunicaciones por radio. El repetidor reenvía el tráfico entre los usuarios inalámbricos y la red cableada.

- **Puentes**

Pueden configurarse access points como puentes de raíz o no de raíz a fin de unir varias redes. Un access point en este rol establecerá un enlace inalámbrico con un puente no de raíz. El tráfico se transmite por el enlace inalámbrico a la red cableada.

- **Puente de grupo de trabajo**

Los access points que están en modo de puente de grupos de trabajo pueden relacionarse a otros access points como clientes y brindar conexiones de red para los dispositivos acoplados a los puertos Ethernet.

- **Unidad central en una red totalmente inalámbrica**

En una red absolutamente inalámbrica, el access point actúa como una unidad de raíz independiente funcionando como un concentrador que enlazar a todas las estaciones juntas. Un access point trabaja como punto central de las comunicaciones, logrando aumentar el alcance de comunicación de los usuarios inalámbricos.

FreeRADIUS

FreeRADIUS es el servidor RADIUS de código abierto más popular y más implementado del mundo. Sirve como base para múltiples ofertas comerciales y proporciona la autenticación, autorización y las necesidades de contabilidad (AAA) de muchas empresas. Entre sus beneficios son sus (Network RADIUS SARL, 2014):

- Características
- Modularidad
- Escalabilidad

Freeradius (2018) mencionan que este servidor se inició en agosto de 1999 por Alan DeKok y Miquel van Smoorenburg. Miquel, desarrollado utilizando un diseño

modular para incentivar una participación comunitaria más activa. Desde entonces, se han lanzado nuevas versiones cada poco mes incluyendo soporte para diversos tipos de autenticación en cualquier otro servidor. El proyecto se ha expandido para incluir una serie de otros productos relacionados con RADIUS, que incluyen:

- freeradius-client Una biblioteca cliente RADIUS con licencia BSD.
- mod_auth_radius Un módulo RADIUS para Apache 1.xy 2.x.
- pam_radius_auth Un módulo de autenticación conectable (PAM) para autenticación y contabilidad RADIUS.

Muchas configuraciones comunes se documentan como sugerencias o ejemplos en los archivos de configuración. Diversos problemas comunes se tratan en los archivos de configuración, junto con las soluciones sugeridas.

Figura 3: Logo de FreeRADIUS

Fuente: (Freeradius, 2018)

AAA

Tschofenig et al. (2019) definen AAA como autenticación, autorización y contabilidad. La autenticación es la comprobación de que un usuario sea válido cuando solicite servicios de red. Este debe presentar una autenticidad y credenciales para poder ser autenticado. La autorización es la decisión de si los servicios solicitados podrán ser brindados al usuario que presentó anteriormente su identidad y sus credenciales. Este estado puede ser modificado en el transcurso de la sesión por motivos de límites de consumo. La contabilidad consiste en hacerle seguimiento al consumo de recursos del usuario para facturación, auditoría, y / o planificación del sistema. Los datos contables típicos recopilados incluyen la identidad del usuario, el servicio proporcionado y cuándo se inició y finalizó el servicio.

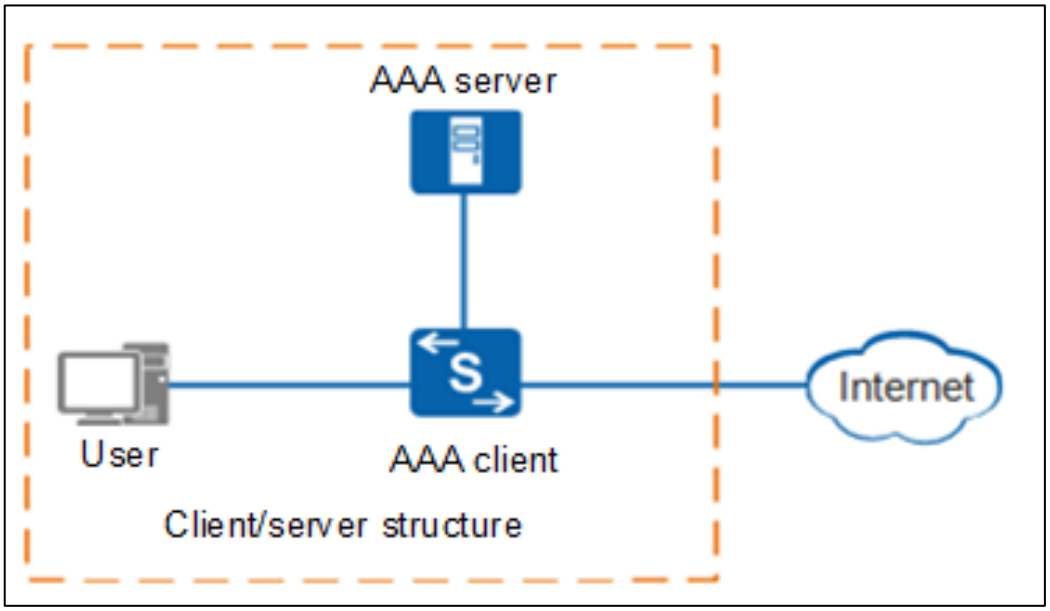
Un Servidor de Acceso a la red (NAS) concede servicios para cada usuario basados en la autenticación y asegura que el servicio concedido sea contabilizado. El NAS se contacta con un servidor AAA separado para verificar las credenciales del usuario y después envía los datos de contabilidad al servidor AAA. Por lo tanto, NAS es un cliente AAA.

Beneficios de AAA

Según Arias & Carrillo (2017), AAA cuenta con los siguientes beneficios:

- Mayor flexibilidad y control de la configuración de acceso.
- Escalable.
- Métodos estandarizados de autenticación.

Figura 4: Arquitectura básica de AAA



Fuente: (Hernández, 2020)

Teniendo en cuenta los siguientes protocolos que serán objeto de comparación para conocer el más competente para controlar el acceso a redes inalámbricas:

RADIUS

El servicio de usuario de acceso telefónico de autenticación remota (RADIUS) es un protocolo de red que se utiliza para autorizar y autenticar a los usuarios que

acceden a redes remotas. Fue desarrollado por Livingston Enterprises, Inc. en 1991 y se convirtió en un estándar del Grupo de Trabajo de Ingeniería de Internet (IETF). Se utilizó por primera vez para conectarse a universidades en Michigan. La National Science Foundation (NSF) otorgó una subvención al proveedor de Internet sin fines de lucro Merit Network, y firmaron un acuerdo para desarrollar un protocolo con Livingston Enterprises, que finalmente se convirtió en RADIUS (Fortinet, s. f.).

Lo utilizan habitualmente proveedores de servicios de Internet (ISP), proveedores de redes móviles y redes corporativas y educativas. Este protocolo suele estar oculto internamente en redes controladas y el usuario final no puede verlo directamente. En otras palabras, se ejecuta entre sistemas confiables en la red (Network Radius, s. f.).

Por otra parte, Zhang et al. (2015) en su artículo sostienen que es un protocolo de Cliente/Servidor que hace uso primordial del conmutador y el servidor de autenticación. Identifica a los usuarios con nombre y contraseña, de los cuales, si son autenticados exitosamente, tienen la autorización de utilizar los recursos admitidos y hará el pago de su servicio de internet según el registro de uso guardado. Por consiguiente, RADIUS abarca 3 funciones principales que son autenticación, autorización y contabilidad.

Una de las características más resaltantes del protocolo RADIUS es su capacidad para procesar sesiones, puede notificar cuando inicio y cuando finaliza una conexión para que los usuarios puedan determinar el uso y la duración de la sesión (Plasencia, 2013).

Según C. Rigney et al. (2000) en el RFC 2865, el cual dejó obsoleto al RFC 2138; manifestaron que las características claves de RADIUS son:

- Modelo cliente / servidor

Un Servidor de Acceso a la Red (NAS) actúa como un cliente RADIUS. El cliente es responsable de llevar la información del usuario al servidor RADIUS designado y luego realizar operaciones en la respuesta devuelta. El servidor RADIUS es responsable de admitir las solicitudes de conexión del usuario, autenticarlo y luego devolver toda la información de configuración necesaria para que el cliente pueda proporcionar servicios a los usuarios.

- Seguridad de la red

Las transacciones entre el cliente y el servidor RADIUS se autentican a través del uso de una clave secreta compartida, que nunca se envía a través de la red. Además, la contraseña del usuario se envía encriptada entre el cliente y el servidor RADIUS, para descartar la posibilidad de que alguien que espíe una red insegura pueda determinar la contraseña del usuario.

- Mecanismos de autenticación flexibles

El servidor RADIUS puede permitir varios métodos para autenticar al usuario. Cuando le concede el nombre de usuario y la contraseña original, otorgados por el usuario, puede admitir PPP PAP o CHAP, inicio de sesión UNIX y otros mecanismos de autenticación.

- Protocolo extensible

Todas las transacciones constan de 3 tuplas de longitud variable “Attribute-Length-Value”. Se pueden agregar nuevos valores de atributo sin cambiar la implementación existente del protocolo.

Funciones principales

Como señala Fortinet (s. f.), RADIUS realiza tres funciones básicas:

- Autenticación: RADIUS autentica dispositivos o usuarios antes de permitirles acceder a la red.
- Autorización: RADIUS autoriza a los dispositivos o usuarios a permitirles utilizar servicios específicos en la red.
- Contabilidad: RADIUS considera la cantidad de recursos utilizados durante la sesión, como paquetes, bytes y tiempo invertido.
-

Campos de un paquete RADIUS

- Code (Código)

El campo *código* es un octeto utilizado para identificar el tipo de paquete RADIUS. Cuando se recibe un paquete con un campo de código no válido, se descarta silenciosamente.

Figura 5: Código RADIUS

1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

Fuente: (C. Rigney et al., 2000)

- Identifier (Identificador)

  El campo *identificador* es un octeto que ayuda a emparejar solicitudes y respuestas. Si el servidor RADIUS tiene la misma dirección IP de origen del cliente y el mismo identificador y puerto UDP de origen en un período corto de tiempo, se pueden detectar solicitudes duplicadas.

- Length (Longitud)

  El campo *longitud* tiene dos octetos, indica la longitud del paquete. La longitud mínima es 20 y la longitud máxima es 4096.

- Authenticator (Autenticador)

  El campo *autenticador* tiene dieciséis octetos. El octeto más importante se envía primero. Este valor se usa para autenticar la respuesta del servidor RADIUS y se usa en el algoritmo de ocultación de contraseñas.

- Attributes (Atributos)

  El campo *atributos* es de longitud variable y contiene una lista de atributos requeridos por el tipo de servicio y cualquier atributo opcional requerido. Los únicos atributos obligatorios con el usuario y la contraseña.

Figura 6: Campos de un paquete RADIUS

1	User-Name	23	Framed-IPX-Network
2	User-Password	24	State
3	CHAP-Password	25	Class
4	NAS-IP-Address	26	Vendor-Specific
5	NAS-Port	27	Session-Timeout
6	Service-Type	28	Idle-Timeout
7	Framed-Protocol	29	Termination-Action
8	Framed-IP-Address	30	Called-Station-Id
9	Framed-IP-Netmask	31	Calling-Station-Id
10	Framed-Routing	32	NAS-Identifier
11	Filter-Id	33	Proxy-State
12	Framed-MTU	34	Login-LAT-Service
13	Framed-Compression	35	Login-LAT-Node
14	Login-IP-Host	36	Login-LAT-Group
15	Login-Service	37	Framed-AppleTalk-Link
16	Login-TCP-Port	38	Framed-AppleTalk-Network
17	(unassigned)	39	Framed-AppleTalk-Zone
18	Reply-Message	40-59	(reserved for accounting)
19	Callback-Number	60	CHAP-Challenge
20	Callback-Id	61	NAS-Port-Type
21	(unassigned)	62	Port-Limit
22	Framed-Route	63	Login-LAT-Port

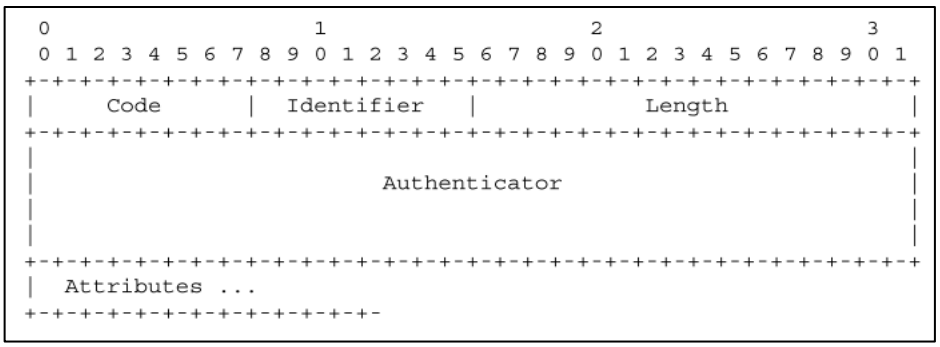
Fuente: (C. Rigney et al., 2000)

Campos de un atributo

- Type (Tipo)

El campo *tipo* tiene un octeto. Un cliente y un servidor RADIUS pueden ignorar atributos con un *tipo* desconocido.

Figura 7: Tipo de atributos



Fuente: (C. Rigney et al., 2000)

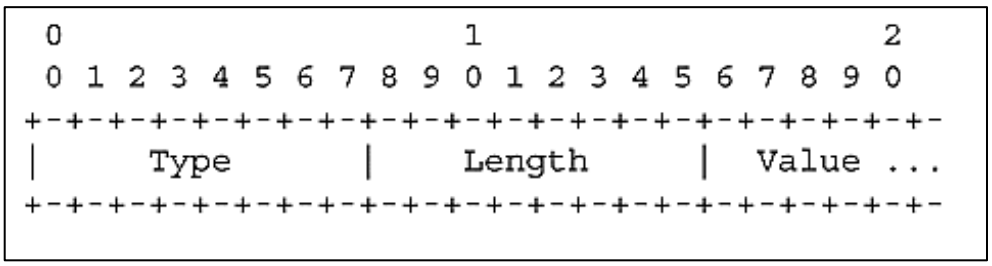
- Length (Longitud)

El campo *longitud* tiene un octeto y señala la longitud de este atributo, incluidos los campos *Tipo, Longitud* y *Valor.* Si se recibe un atributo en la solicitud de acceso, pero la longitud no es válida, se debe enviar una denegación de acceso.

- Value (Valor)

El campo *valor* tiene cero o más octetos y posee información específica del atributo. El formato y la longitud del campo *valor* están definidos por los campos de *Tipo* y *Longitud*.

Figura 8: Campos de un atributo



Fuente: (C. Rigney et al., 2000)

Mensajes más comunes de RADIUS

Los mensajes RADIUS se envían como mensajes de datagramas de usuario UDP. El puerto UDP 1812 se usa para mensajes de autenticación RADIUS, mientras que el puerto 1813 se usa para mensajes de administración de cuentas RADIUS. La carga útil UDP de un paquete RADIUS contiene solo un mensaje RADIUS. (Plasencia, 2013)

Según López (2015), Radius preside de los siguientes mensajes:

- Access-Request (Solicitud de acceso)
  El cliente RADIUS lo envía para solicitar autenticación y autorización para el acceso a la red.

- Access-Accept (Aceptación de acceso)
  El servidor RADIUS lo envía en respuesta al mensaje Access-Request. Este

mensaje informa al cliente de la correspondiente autenticación y autorización, y proporciona los atributos necesarios.

- Access-Reject (Rechazo de acceso)

  El servidor RADIUS lo envía en respuesta al mensaje Access-Request. Este mensaje informa al cliente que su solicitud ha sido rechazada, proporcionando el motivo.

- Access-Challenge (Desafío de acceso)

  El servidor RADIUS lo envía en respuesta al mensaje Access-Request. El mensaje se envía al cliente con un reto al que este tiene que responder.

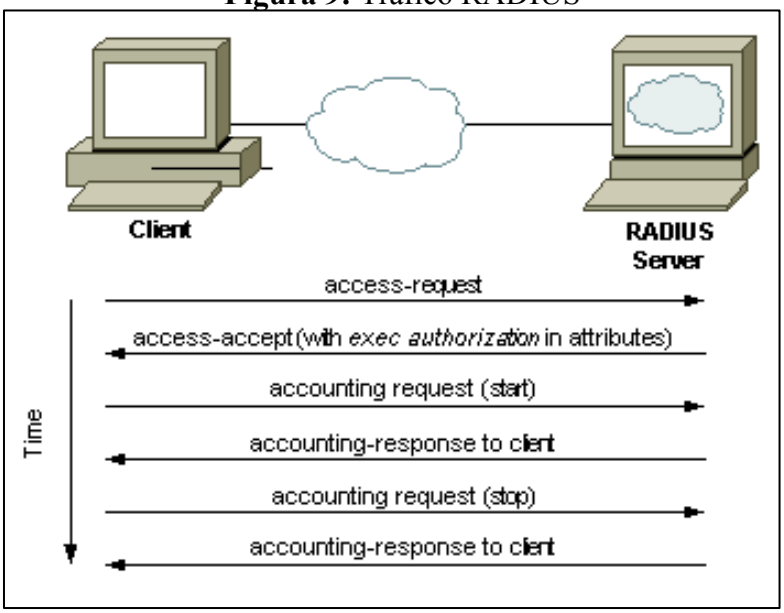
- Accounting-Request (Solicitud de administración de cuentas)

  El cliente RADIUS lo envía para precisar la información de conexión aceptada. Puede ser de tipo start o stop para iniciar o detener el acouting.

- Accounting-Response (Respuesta de administración de cuentas)

  El servidor RADIUS lo envía en respuesta al mensaje Accounting-Request. Este mensaje informa la correcta recepción de la solicitud e inicia el procesamiento de la sesión.

Figura 9: Tráfico RADIUS



Fuente: (Cisco, 2008)

Beneficios:

Según (Network Radius, s. f.) el protocolo cliente/servidor abarca muchas ventajas para los clientes:

- Solución abierta y escalable.
- Amplio soporte de grandes proveedores.
- Fácil de modificar.
- Separa los procesos de seguridad y comunicación.
- Adecuado para la mayoría de los sistemas de seguridad.
- Funciona con cualquier dispositivo cliente que admita el protocolo.
- Implementación de cliente muy simple.

TACACS +

De acuerdo con Ravi et al. (2017), es un protocolo que brinda control de acceso para enrutadores de red, servidores de acceso a la red y otros dispositivos informáticos mediante uno a más servidores centralizados. Concede servicios AAA (autenticación, autorización y rendición de cuentas), haciendo uso de un nombre de usuario junto al mecanismo de autenticación de contraseñas fijas, sin embargo, este mecanismo presenta amenazas a la seguridad resultando más conveniente el uso de contraseñas de "un solo uso". La contabilidad en TACACS + facilita contabilizar los servicios utilizados y auditar los servicios de seguridad.

Dahm et al. (2020) manifiestan que la separación de autenticación, autorización y contabilidad es un elemento primordial del diseño del protocolo TACACS +, pues es un conjunto de tres protocolos; poder separar estos elementos son de utilidad para usarlos en la administración de dispositivos. TACACS + autoriza una longitud y contenido arbitrarios para admitir una autenticación alternativa de mecanismos además utiliza TCP para garantizar la entrega. El protocolo permite al cliente TACACS + pedir multas de control de acceso granulado y autoriza al servidor responder a cada componente de esa solicitud.

Citando a Thorsten et al. (2017) mencionan que TACACS + usa TCP para su transmisión. El puerto 49 del servidor está asignado para el tráfico TACACS +. Una sesión TACACS + es una única secuencia de autenticación, un único intercambio de autorización o un único intercambio contable. La sesión de contabilidad y autorización constará de un par de paquetes (solicitud y respuesta). La sesión de autenticación puede implicar el intercambio de cualquier número de paquetes.

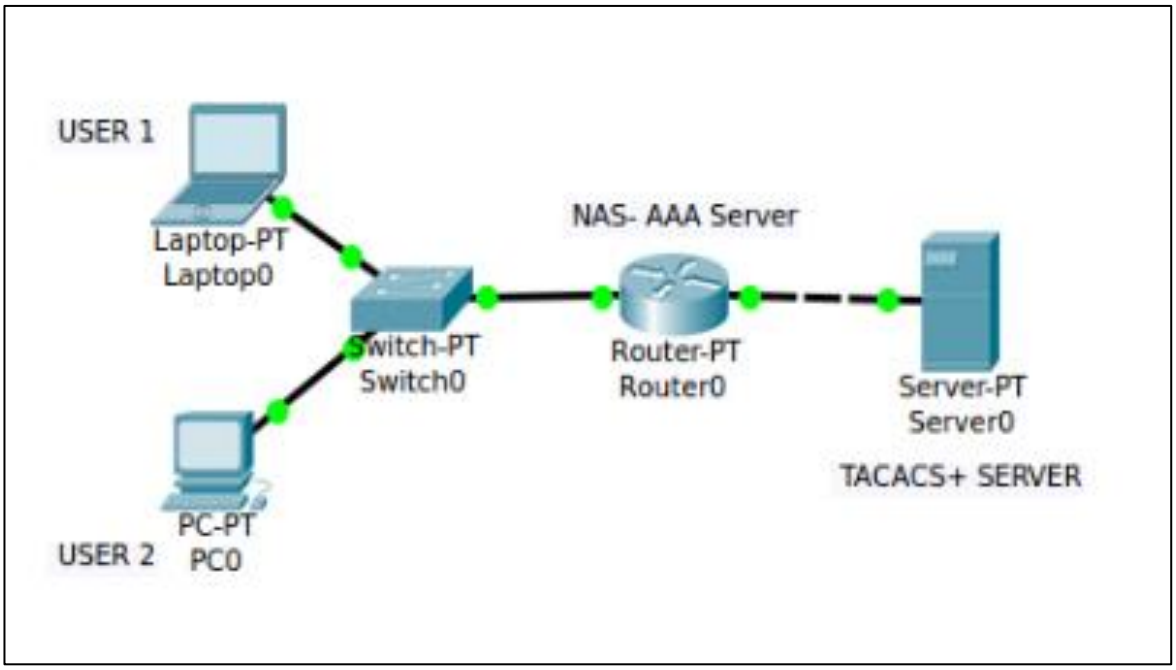
Seguridad General en TACACS+

Dahm et al. (2020) hacen referencia que el protocolo TACACS + no tiene incluido un mecanismo de seguridad que tenga la capacidad de cumplir con los requisitos actuales, se consideran con mejor referencia como "ofuscación" y no "encriptación" pues no brindan integridad. Al suponer que el atacante con acceso al flujo de datos puede para leer y modificar todos los paquetes TACACS + se presentan algunos de los posibles riesgos:

- La información contable puede ser modificada por medio del atacante.
- El atacante puede completar varios campos con compensaciones conocidas para intentar evitar las comprobaciones de autenticación o autorización.
- A pesar de brindar cierta medida de privacidad en el transporte, es vulnerable al menos algunos ataques de texto sin formato conocidos, ataques de texto plano o ataques de fuerza bruta que sacan provecho de la eficiencia del algoritmo MD5.

Siendo algunas de las razones que invitan al usuario, que implementan el protocolo TACACS +, a limitar el acceso a los clientes conocidos y mantener el control de toda la ruta de transmisión ya que los atacantes pueden correr con la suerte de descifrar la clave o romper la ofuscación sin restricciones.

Figura 10: Configuración de red TACACS +

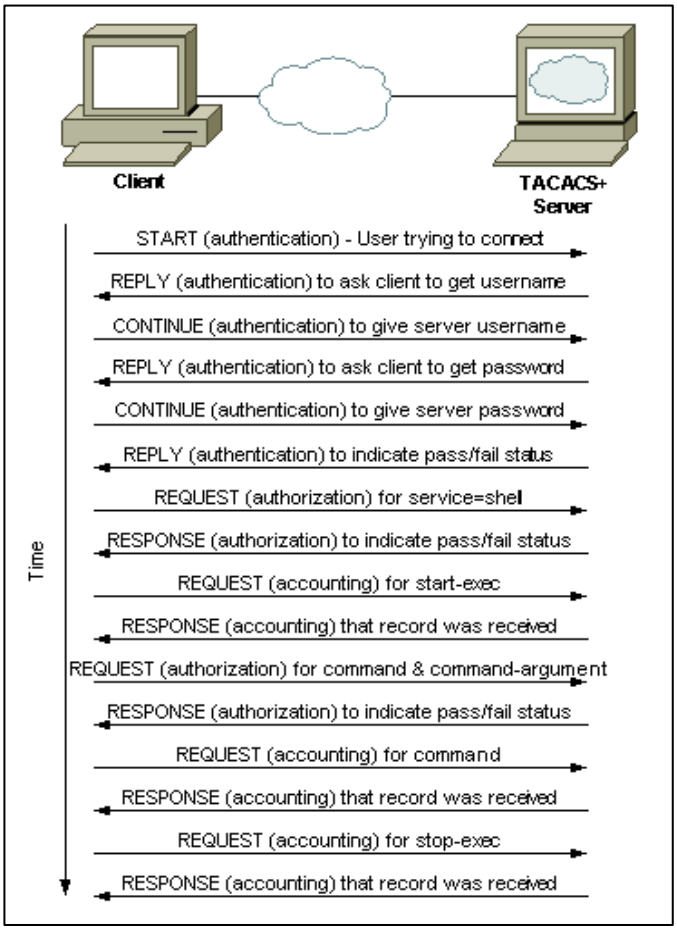


Fuente: (Pradeep et al., 2019)

Paquetes y sesiones TACACS+

Según Cisco (2008), cifra todo el cuerpo del paquete, pero conserva el encabezado estándar TACACS+. Hay un campo en el encabezado en el que indica si el cuerpo está encriptado. Para fines de depuración, es conveniente que el cuerpo del paquete no esté encriptado. Sin embargo, durante el manejo normal, el cuerpo del paquete de datos está del todo encriptado para lograr una comunicación más segura. TACACS+ es una versión propietaria de Cisco del TACACS, por tal razón se soporta solamente con Cisco ACS.

Figura 11: Tráfico TACACS +



Fuente: (Cisco, 2008)

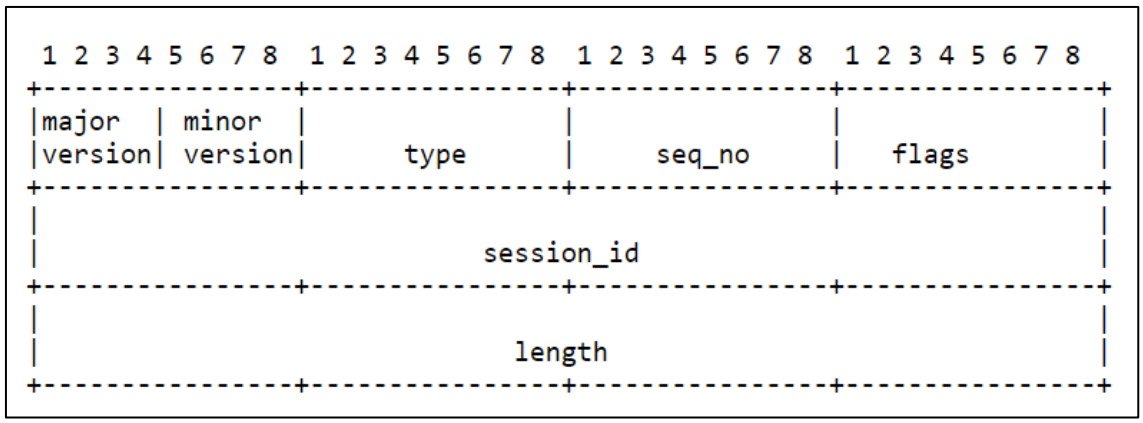
Algunas reglas generales que se aplican a todos los tipos de paquetes TACACS + (Dahm et al., 2020):

- Para indicar que los campos de datos de longitud variable no se utilizan, se coloca cero, los campos mencionados deben ser ignorados.
- Las longitudes de los campos de datos y mensajes en un paquete por su campo de longitud correspondiente se deben detallar.

El encabezado del paquete TACACS +

Todos los paquetes TACACS + comienzan con el siguiente encabezado de 12 bytes, este encabezado describe el resto del paquete.

Figura 12: Paquete TACACS +



Fuente: (Dahm et al., 2020)

El cuerpo del paquete TACACS +

Los tipos de cuerpo de TACACS + se definen en el encabezado del paquete.

Modo de conexión única

Para precisar la admisión del modo de conexión única, el servidor establece este indicador en el primer paquete de respuesta, teniendo la potestad de establecerlo, así el cliente no lo haya establecido, pero también sucede que el cliente ignora el indicador y cerrar la conexión después de que finalice la sesión.

Finalización de sesión

Los paquetes de respuesta detallados para los tipos de paquetes en las secciones de Autenticación, Autorización y Contabilidad, contienen un campo de estado. Los tres tipos de paquetes REPLY definen valores que representan PASS, ERROR y FAIL.

- El servidor argumenta con PASS o FAIL para indicar que el procesamiento de la solicitud se completó y que el cliente puede aplicar el resultado que permite examinar la ejecución de la acción que motivó el envío de la solicitud al servidor.
- El servidor argumenta con ERROR para indicar que no se haya completado el procesamiento de la solicitud.

Al completar una sesión, la conexión TCP debe manejarse según el modo de negociación:

- Si no se negoció el modo de conexión única, se debe cerrar la conexión.

- Si se habilitó el modo de conexión única, se debe dejar abierta la conexión, la cual puede cerrarse después de un lapso de tiempo.
- Si se habilitó el modo de conexión única, pero se produjo un error debido a problemas de conexión, no se debe aceptar otra sesión nueva en la conexión.

Ofuscación de datos

Este mecanismo está basado en una clave secreta, este valor secreto compartido es conocido por el cliente y el servidor. Las llaves secretas deben permanecer a escondidas y el servidor debe permitir la asociación de una única clave con cada cliente.

Cisco (2018) precisa las especificaciones AAA del protocolo TACACS +, siendo las siguientes:

Especificación de la autenticación TACACS +

Al haber identificado y definido una clave asociada de cifrado TACACS +, es adecuado determinar listas de métodos para la autenticación TACACS +, este protocolo opera a través de AAA y emite el comando de autenticación AAA.

Especificación de la autorización TACACS +

La autorización AAA admite establecer parámetros que circunscribe el acceso de un usuario a la red. Esta autorización es posible aplicarse en comandos, conexiones de red y sesiones EXEC.

Especificación de la contabilidad TACACS +

La contabilidad AAA accede a rastrear los servicios a los que los usuarios pueden ingresar junto con la cantidad de recursos de red que consumen. Siendo de mayor facilidad la contabilidad TACACS + a través de AAA, se debe emitir el comando de contabilidad AAA especificando este protocolo como método de contabilidad.

Mejores prácticas de TACACS +

- No se debe confiar en la ofuscación del protocolo TACACS +, se debe usar TACACS + dentro de un ambiente seguro.
- TACACS + además de implementarse en redes que garanticen la privacidad de la comunicación, siendo llevada a cabo en una red separada del resto del tráfico.
- Los proveedores deben proporcionar mecanismos para ayudar al administrador a lograr estas mejores prácticas.

DIAMETER

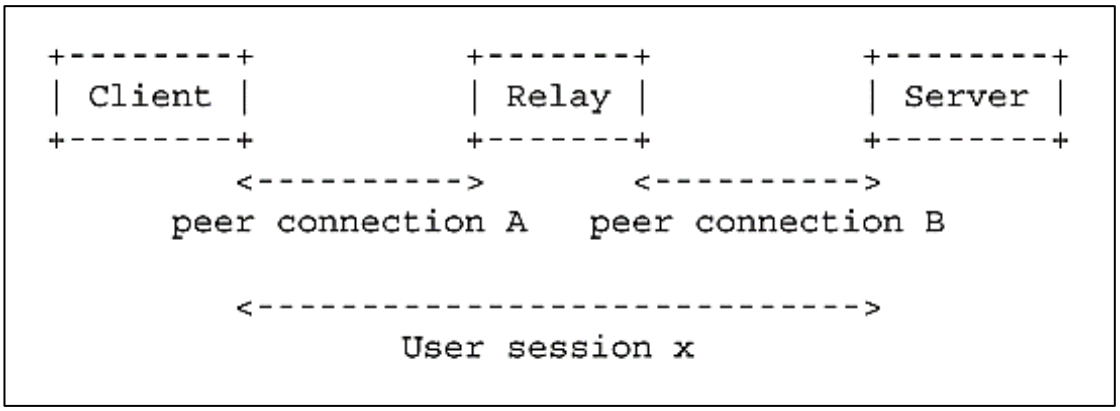
Citando a Fajardo et al. (2012), señalaron que el protocolo Diameter fue diseñado para proporcionar autenticación, autorización y contabilidad (AAA) en aplicaciones que se encuentren en situaciones locales y de itinerancia (como acceso a la red o movilidad IP). El protocolo base de Diameter está definido por RFC6733 ha desfasado a RFC3588 y RFC5719, debiendo contar con compatibilidad para todas las nuevas implementaciones.

El protocolo Diameter se encarga de establecer conexiones con los pares, la negociación de capacidades, cómo enviar y enrutar mensajes a través de los pares y cómo finalmente desconectarse. La comunicación entre pares de Diámetro comienza cuando un par envía un mensaje a otro par de Diameter, está conformado por un encabezado seguido de uno o más pares atributo-valor (AVP). Un AVP incluye un encabezado y es usado para la encapsulación de datos específicos del protocolo.

Conexiones y sesiones DIAMETER

Una conexión se refiere a una conexión a nivel de transporte entre dos pares para enviar y recibir mensajes Diameter. Una sesión es un concepto lógico en la capa de aplicación que hay entre el cliente Diameter y el servidor Diameter. Se identifica mediante el AVP de ID de sesión.

Figura 13: Conexiones y sesiones de DIAMETER



Fuente: (Fajardo et al., 2012)

Formato del encabezado de DIAMETER

- Version (Versión)

El campo *versión* indica la versión del protocolo Diameter, este valor debe ser 1.

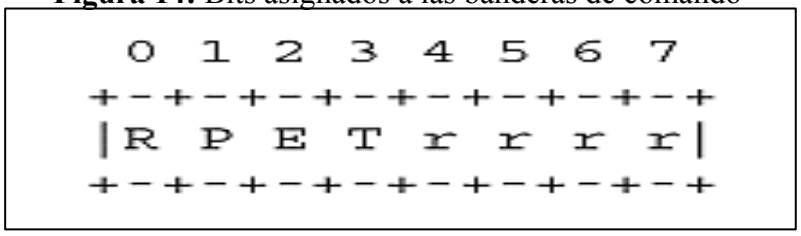
- Length (Longitud del mensaje)

El campo *longitud* tiene tres octetos, indica la longitud del mensaje de Diámetro, incluido el campo de encabezado y el AVP de relleno.

- Flags (Banderas de comando)

  El campo *banderas* tiene ocho bits

Figura 14: Bits asignados a las banderas de comando



Fuente: Fajardo et al. (2012)

- Command code (Código de comando)

  El campo *código de comando* tiene tres octetos para transmitir el comando asociado con el mensaje. A cada par de solicitud / respuesta de comando se le asigna un código de comando, y el subtipo (solicitud o respuesta) se reconoce mediante el bit "R" en el campo de banderas de comando del encabezado de DIAMETER. Cada mensaje de DIAMETER debe incluir un código de comando, que se utiliza para determinar la acción a realizar en un mensaje específico.

Figura 15: Códigos de comandos

Command name	Abbreviation	Code
Abort-Session-Request	ASR	274
Abort-Session-Answer	ASA	274
Accounting-Request	ACR	271
Accounting-Answer	ACA	271
Capabilities-Exchange-Request	CER	257
Capabilities-Exchange-Answer	CEA	257
Device-Watchdog-Request	DWR	280
Device-Watchdog-Answer	DWA	280
Disconnect-Peer-Request	DPR	282
Disconnect-Peer-Answer	DPA	282
Re-Auth-Request	RAR	258
Re-Auth-Answer	RAA	258
Session-Termination-Request	STR	275
Session-Termination-Answer	STA	275

Fuente: (Fajardo et al., 2012)

- Application-ID

  El campo *ID de aplicación* tiene cuatro octetos, que se utilizan para identificar a qué aplicación se aplica el mensaje. La aplicación puede ser una aplicación de autenticación, una aplicación de contabilidad o una aplicación específica del proveedor.

- Hop-by-Hop Identifier (Identificador de salto a salto)

  El *identificador de salto a salto* es un campo entero de 32 bits sin firmar (en orden de bytes de red) que ayuda a hacer coincidir solicitudes y respuestas.

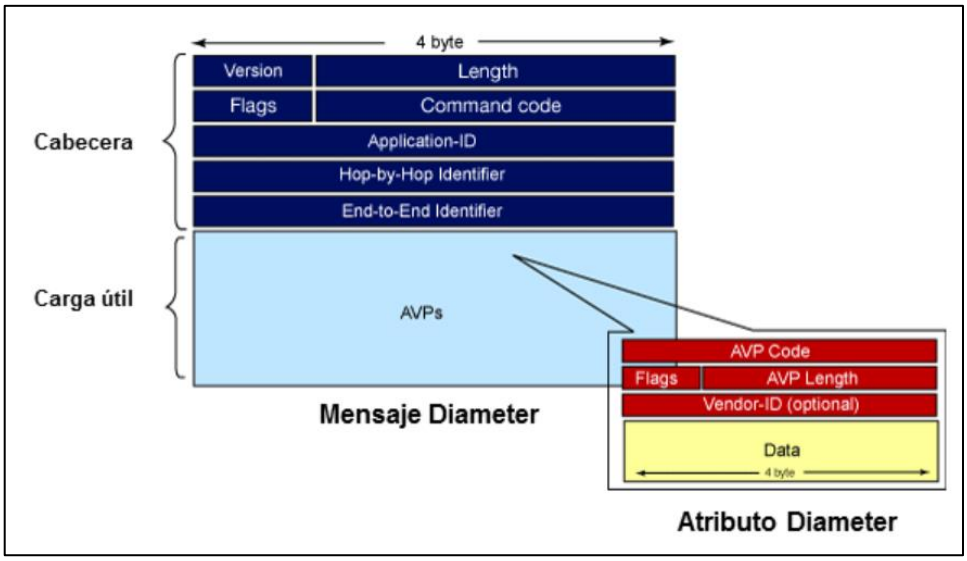
- End-to-End Identifier (Identificador de extremo a extremo)

  El *identificador de extremo a extremo* es un campo entero sin signo de 32 bits (en orden de bytes de red) que se utiliza para detectar mensajes duplicados.

- AVPS (Par Atributo - Valor)

  Los AVP son un método para aislar información relacionada con los mensajes de Diameter.

Figura 16: Formato de la cabecera de los mensajes DIAMETER y de los AVP



Fuente: (Millán, 2017)

Facilidades del protocolo DIAMETER

Fajardo et al. (2012) mencionan que DIAMETER proporciona las siguientes facilidades:

- Capacidad para intercambiar mensajes y entregar AVP.
- Notificación de errores.
- Negociación de capacidades.
- Gestión de sesiones de usuario o contabilidad

Características

- Transportar información de autenticación de usuarios para permitir al servidor de Diameter autenticar al usuario.
- Transportar información de autorización específica del servicio entre el cliente y los servidores, lo que permite al par determinar si concede la solicitud de acceso de un usuario.
- Intercambiar información sobre el uso de recursos, que se puede utilizar con fines contables, planificación de capacidad, etc.
- Enrutar, retransmitir, proxy y redireccionar mensajes de Diameter mediante la jerarquía de servidores.

Mejoras del protocolo DIAMETER

Tschofenig et al. (2019) nos especifican las principales diferencias entre RFC 3588 y RFC 6733:

- SEGURIDAD: RFC 6733 especifica Transport Layer Security (TLS) como la principal manera de resguardar los mensajes de Diameter, especificando a la vez el uso de un puerto conocido. Está obsoleta la seguridad de un extremo a otro que se describe en RFC 3588 puesto que la solución técnica real aún no se ha estandarizado.
- DESCUBRIMIENTO DE NODO DE DIÁMETRO: Un nodo de diámetro reconoce con qué nodo necesita comunicarse mediante configuración manual o un procedimiento de descubrimiento dinámico. RFC 6733 simplificó el procedimiento de descubrimiento dinámico, ya que se reconoció que muchos proveedores habían implementado solamente el mecanismo basado en DNS.
- EXTENSIBILIDAD: La historia presentada en RFC 3588 para extender Diameter no fue clara y producía extensiones incompatibles. RFC 6733 aclaró la extensibilidad del diámetro.
- ACLARACIONES: Las aclaraciones por parte de RFC 6733 son el resultado de muchas discusiones dentro del grupo de trabajo para reconstruir las intenciones originales y combinarlas con implementaciones.

KERBEROS

El protocolo Kerberos fue implementado por el Instituto de Tecnología de Massachusetts (s. f.), el cual manifiesta que es un protocolo de autenticación de red. Su objetivo es proporcionar una autenticación sólida para aplicaciones cliente/servidor, por medio del uso de cifrado de claves. El MIT a la vez manifiesta que este protocolo emplea una sólida tecnología de cifrado para que el usuario pueda demostrar su identidad al servidor a través de una conexión de red insegura (y viceversa). Una vez que el cliente y el servidor utilizan Kerberos para demostrar su identidad, también pueden cifrar todas las comunicaciones para proteger la privacidad e integridad de los datos.

Kerberos brinda un medio para verificar las identidades de, por ejemplo, un usuario de estación de trabajo o un servidor de red en una red sin protección. Kerberos lleva a cabo la autenticación como un tercero de confianza a servicio de autenticación mediante el uso convencional (secreto compartido clave). Existen dos medios básicos mediante los cuales un cliente puede solicitar credenciales a un servidor Kerberos. El primero medio, el cliente envía una solicitud de texto sin cifrar para un ticket para el servidor deseado al Servidor de Autenticación (AS), la respuesta se envía cifrada en la clave secreta del cliente, por lo general, esta solicitud es para un ticket de concesión de tickets (TGT), que luego se puede utilizar con el servidor de concesión de tickets (TGS) y en segundo medio, el cliente envía una solicitud al TGS, haciendo uso del TGT para autenticarse en el TGS, la respuesta está encriptada en la clave de sesión del TGT (Neuman et al., 2005).

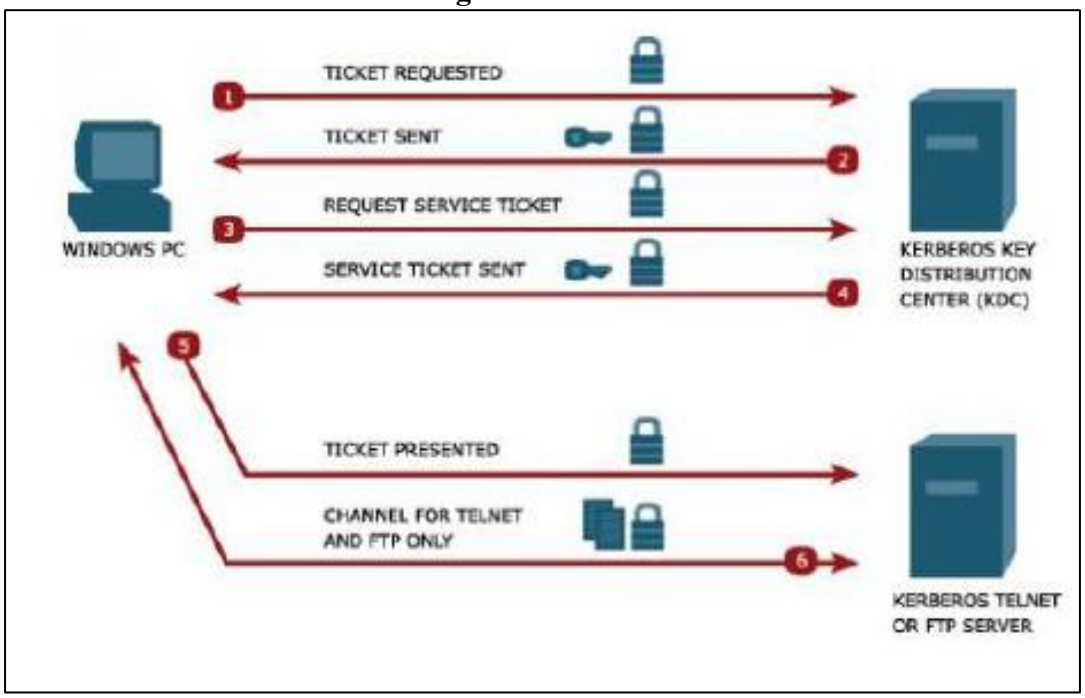
Dayanand et al. (2020) expresaron que Kerberos, es un protocolo de autenticación con la finalidad de garantizar el cuidado de datos en una red no estable, el cual a la vez permite acceder a diversos servicios previstos por medio de Internet solo para clientes autorizados. Este protocolo hace uso de métodos para el cifrado de claves simétricas y un centro de distribución de claves, que tiene la posibilidad de integrarse a redes existentes.

El sistema Kerberos está basado en el concepto de tickets. Un ticket es un conjunto de información electrónica que identifica a un usuario o servicio, además permite reconocer los privilegios que pueda tener para ingresar a la red. Cuando realiza una transacción que se basa en Kerberos, envía una solicitud transparente de un ticket a un Centro de Distribución de claves (KDC). El KDC autoriza a una base de datos para autenticar la identidad y retorna un ticket que brinda permiso para acceder a otro equipo. La manera de usar los tickets es establecida mediante políticas, las cuales son determinadas durante la instalación o administración del servicio Kerberos (ITCA FEPADE, s. f.).

El proceso de autenticación Kerberos procede: un cliente envía una solicitud al servidor de autenticación (AS) de "credenciales" para un servidor determinado. El AS responde con estas credenciales, cifradas en la clave del cliente. Las credenciales residen en un "ticket" para el servidor y una clave de encriptación temporal (también conocida como "clave de sesión"), el cliente transmite el ticket

(contiene la identidad del cliente y una copia de la clave de sesión) al servidor. La clave de sesión (ahora compartida por el cliente y el servidor) se usa para autenticar al cliente y también podría usarse para autenticar el servidor. Es bueno recordar que la gran mayoría de aplicaciones que hacen uso de Kerberos para iniciar una conexión de red basada en flujo (Neuman et al., 2005).

Figura 17: Tráfico Kerberos



Fuente: (ITCA FEPADE, s. f.)

Metodología del protocolo KERBEROS

ITCA FEPADE (s. f.) menciona las entidades en el flujo de Kerberos:

- Cliente: Empieza el contacto con una solicitud de un servicio.
- Servidor: Conforma el recurso al que el usuario desea acceder.
- Servidor de autenticación (AS): Brinda la autenticación a los clientes. El servidor ofrece un ticket llamado TGT (Ticket Awarding Ticket), verificando si el cliente se encuentra autenticado.
- Centro de distribución de claves (KDC): Se dividen en tres partes en el entorno Kerberos: base de datos, servidor de autenticación (AS) y servidor de concesión de tickets (TGS) conformando el Centro de distribución de claves.

- Ticket Granting Server (TGS): Procede como un servicio para la asignación de tickets de servicio.

Usos y solicitudes de banderas de tickets

Neuman et al. (2005) menciona que cada ticket de Kerberos abarca un conjunto de indicadores que se usan para indicar sus atributos. La mayoría de las banderas pueden ser solicitadas por un cliente cuando se obtiene el ticket; se pueden activar y desactivar automáticamente mediante un servidor Kerberos según su necesidad. A continuación, se menciona:

Tickets iniciales, pre autenticados y autenticados por hardware

La bandera INICIAL indica que un ticket se emitió utilizando el protocolo AS, los servidores de aplicaciones que necesiten del conocimiento demostrado de la clave secreta de un cliente, pueden insistir en que esta bandera se establezca en cualquier ticket que acepten de esta manera puedan estar seguros de que la clave del cliente se presentó recientemente al servidor de autenticación.

Los indicadores PRE-AUTHENT y HW-AUTHENT ofrecen información adicional sobre la autenticación inicial, de manera autónoma de si el boleto actual se emitió directamente o se emitió sobre la base de un TGT.

Entradas inválidas

La bandera INVALID indica que un ticket no es válido, los servidores de aplicaciones deben rechazar los tickets que tengan esta bandera establecida, emitiéndose un boleto tardío en el formulario. Estos boletos sin validez deben reconocerse por KDC antes de su uso, presentándolos en una solicitud TGS; El KDC solo validará los boletos después de que haya pasado su hora de inicio. Esta validación es necesaria para que los tickets con fecha posterior (hayan sido robados antes de su hora de inicio) tengan la posibilidad de volverse inválidos permanentemente.

Entradas renovables

El uso de tickets de duración corta y la obtención de nuevos tickets de manera habitual, tendría que requerir que el cliente tenga acceso a largo plazo, lo cual se torna un mayor riesgo, por lo tanto, las entradas renovables se pueden usar para moderar las consecuencias del robo; posee dos tiempos de vencimiento, el primero

se produce con el vencimiento de la instancia actual del boleto y el segundo es el último valor permitido para un tiempo de vencimiento individual.

Entradas tardías

Hay posibilidades que las aplicaciones tengan la necesidad de obtener boletos para su uso mucho más tarde, estos tickets brindan una forma de obtenerlos del KDC en el momento de la presentación del trabajo para dejarlos sin actividad hasta que se activen y validen mediante una solicitud adicional del KDC.

Tickets Proxiable y Proxy

El indicador PROXIABLE, es un ticket que, cuando se establece, le dice al servidor de otorgamiento de tickets que está bien emitir un nuevo ticket (pero no un TGT) con una diferente dirección de red. PROXIABLE se determina si el cliente lo solicita en la autenticación inicial. El indicador PROXY se fija en un ticket por el TGS cuando emite un ticket proxy. Los servidores de aplicaciones pueden marcar esta bandera y pueden requerir autenticación adicional.

Entradas reenviables

Estos tickets tienen una interpretación similar al indicador PROXIABLE, sin considerar que los TGT también pueden emitirse con diferentes direcciones de red; se repone de forma predeterminada, pero se puede restaurar y se establezca configurando la opción FORWARDABLE en la solicitud AS cuando solicitan su TGT inicial.

Comprobación de políticas en tránsito

En Kerberos, el servidor de aplicaciones es en última instancia responsable de aceptar o rechazar la autenticación y debe verificar que solo se confíe en los KDC para autenticar un principal.

Aceptar como delegado

Para algunas aplicaciones, un cliente puede necesitar delegar autoridad a un servidor para actuar en su nombre al contactar otros servicios. Esto requiere que el cliente reenvíe las credenciales a un servidor intermedio. La capacidad de un cliente de obtener un vale de servicio para un servidor no transmite información al cliente sobre si se debe confiar en el servidor para aceptar credenciales delegadas. OK-

AS-DELEGATE proporciona una forma para que un KDC comunique la política de dominio local a un cliente con respecto a si se confía en un servidor intermedio para aceptar tales credenciales.

Otras opciones de KDC

- **Renovable-OK**

La opción RENOVABLE-OK precisa que el cliente aceptará un boleto renovable si no se puede proporcionar un boleto con la vida solicitada, si no habría posibilidad de proporcionarlo, entonces el KDC tiene la posibilidad de emitir un boleto renovable con una renovación igual a la hora de finalización solicitada.

- **ENC-TKT-IN-SKEY**

La opción ENC-TKT-IN-SKEY acepta la autenticación de usuario a usuario al permitir que el KDC emita un ticket de servicio cifrado utilizando la clave de sesión de otro TGT emitido a otro usuario. La opción ENC-TKT-IN-SKEY es únicamente aceptada por el servicio de otorgamiento de boletos, señala que el ticket que se emitirá para el servidor final se cifrará en la clave de sesión del segundo TGT adicional proporcionado con la solicitud.

- **Autenticación de hardware sin contraseña**

La opción OPT-HARDWARE-AUTH muestra que el cliente tiene la intención de hacer uso de alguna forma de autenticación de hardware en vez de o a la vez de la contraseña del cliente u otra clave de cifrado de duración prolongada.

OPT-HARDWARE-AUTH es únicamente aceptado por el servicio de autenticación. Si lo admite y lo permite la política, el KDC devolverá un código de error de KDC_ERR_PREAUTH_REQUIRED e incluirá los METHOD-DATA necesarios para realizar dicha autenticación.

Los criterios de comparación que conforman la siguiente investigación son, según las características básicas de autenticación

- Algoritmo: El algoritmo de autenticación genera un valor de suma de verificación de integridad o síntesis basado en los datos y una clave (Oracle, 2010).

- Tipo de clave: Según Barker (2016) las claves se identifican según su categoría como claves privadas, públicas o simétricas (o sea secretas).

- Tamaño de clave: Es la longitud de una clave en bits que utiliza un algoritmo de encriptación (Barker, 2020).

- Tipo de autenticación: El tipo de autenticación, precisa el tipo de protocolo de seguridad que se emplea para enviar el nombre de usuario y contraseña al servidor para establecer una conexión de red.

- Cifrado: Es la conversión de datos de un formato legible a un formato codificado, el cual solo pueda leerse después de su descodificación con la clave apropiada, la clave puede estar almacenada en un sistema de recepción. Es considerado como el elemento primordial para la seguridad de datos, siendo la forma más sencilla de impedir un robo de información en un sistema informático, además de ser un medio para demostrar la autenticidad de la información verificando que no haya pasado por modificaciones durante la transmisión. Los métodos para codificar y descodificar la información son (Kaspersky, 2018):

  Cifrado de clave simétrica: o llamado como algoritmo de clave secreta, es un método de descodificación de mensajes, el cual debe ser previamente provisto al receptor antes de que el mensaje se pueda descodificar, se hace uso de la misma clave que se utiliza en la codificación y descodificación, lo que resulta más conveniente para los usuarios individuales y los sistemas cerrados.

  Criptografía asimétrica: a diferencia del método previamente mencionado, este método hace uso de dos claves diferentes pero vinculadas entre sí (pública y privada), Ambas claves pueden cifrar un mensaje y la clave opuesta sirve para descodificarlo.

Según la forma de trabajo del protocolo de autenticación:

- Soporte multiprotocolo: También llamado en inglés como Multiprotocol Label Switching o MPLS, creado por la Internet Engineering Task Force; es un estándar para la transmisión de datos (incluyendo voz y servicios transmitidos por IP) bajo distintas etiquetas con la finalidad de unir distintos

tipos de datos ya transmitidos mediante una misma red y de esta manera no generen un problema de velocidad (Optical Networks, 2019).

- Interoperabilidad: Es considerada como la capacidad de un sistema de información para comunicarse y compartir información de manera eficaz, con diversos sistemas de información, por medio de una interconexión libre, mecánica y transparente, sin dejar de hacer uso en ningún momento de la interfaz del sistema propio (Gómez, 2007).
- Protocolo de transporte: Es similar al protocolo de enlace. Maneja el control de errores, el control de flujo, la secuencia de paquetes, etc. Teniendo en cuenta que en el nivel de transporte se necesita una manera para especificar la dirección del destino, es complejo establecer una conexión, es posible almacenar paquetes dentro de la subred y es necesario brindar la dirección cuando una aplicación requiere establecer conexión con otra, a nivel transporte esta dirección se llama TSAP (Transport Service Access Point) (Herramientas Web, s. f.).
- Sistema operativo: Es el software (programa o conjunto de programas) que realiza la gestión de los recursos de la máquina junto a sus indispensables servicios en un sistema informático, el sistema operativo es ejecutado en modo privilegiado (Universidad de Alicante, 2015).

Según su funcionalidad AAA:

- Autenticación: Es la acción de verificar una identidad, de manera que la etiqueta preexistente de un espacio de nombres conocidos, como el originador de un mensaje (autenticación de mensaje) o como el punto final de un canal (autenticación de entidad). (Aboba & Wood, 2003)
- Autorización: Es la acción de precisar si posee un derecho en particular, se puede otorgar una credencial específica. (Aboba & Wood, 2003)
- Contabilidad: Es la acción de recopilar información acerca de la utilidad de recursos con el fin de realizar análisis de tendencias, auditoría, facturación o asignación de costos. (Aboba & Wood, 2003)

CAPÍTULO II

Se realizó la comparación de cuatro protocolos de autenticación de usuarios, por medio de tres categorías conformadas por diversos criterios; dichos criterios fueron elegidos teniendo en cuenta las características básicas, manera de trabajo y funcionalidad de cada protocolo, lo cual permitió de esta manera obtener un análisis eficiente de cada protocolo además de la elección del protocolo más eficiente para su implementación.

La primera tabla comparativa expresa la categoría que hace referencia a las características básicas de autenticación. Estas características fueron tomadas en cuenta según los criterios que consideramos indispensables conocer, los cuales son: algoritmo, tipo de clave, tamaño de clave, tipo de autenticación y cifrado; permitiendo comprender las cualidades que presenta cada protocolo y de acuerdo a esto seleccionar el más idóneo.

La segunda tabla comparativa manifiesta la categoría que alude a la forma de trabajo de cada protocolo de autenticación, siendo los criterios considerados: soporte multiprotocolo, interoperabilidad, protocolo de transporte y sistema operativo. La forma de trabajo es la manera en la cual un protocolo se desempeña al hacer uso de él en un proceso de autenticación, los criterios anteriormente mencionados nos permiten conocer el protocolo de autenticación más viable.

Por último, la tercera tabla comparativa hace referencia a la categoría basada en la funcionalidad AAA, en la cual los criterios son: autenticación, autorización y contabilidad. Esta categoría permite conocer qué protocolos realizan las tres funciones, controlando el acceso de los usuarios autorizados e impidiendo el acceso no autorizado.

Tabla 1: Categoría 1. Características básicas de autenticación

Criterios de comparación	RADIUS	TACACS+	DIAMETER	KERBEROS
Algoritmo	AES / HMAC-SHA1 (Spitzer, 2015)	MD5 (Medway Gash et al., 2020)	HMAC – MD5 (Arias & Carrillo, 2017)	SHA y MDA5 (IBM, 2015)
Tipo de clave	Clave secreta (Cisco, s. f.-b)	Clave secreta (Medway Gash et al., 2020)	Clave secreta (Chaparro & Mejía, 2006)	Clave secreta (Singh et al., 2016)
Tamaño de clave	128 bits (C. Rigney et al., 2000)	504 bits (Cisco, 2019)	128 bits (Fajardo et al., 2012)	256 bits (Ibáñez & López, 2017)
Tipo de autenticación	EAP, PAP, MSCHAP (De Luz, 2021)	Uso de un NAS en el proceso de autenticación (Alonso, 2013)	EAP, PAP, MSCHAP (Castro & Eras, 2017)	Mediante distribución de llaves - KDC (Pérez, 2019)
Cifrado	Cifrado solo de la contraseña (Cisco, 2008)	Cifrado de todo el cuerpo del paquete, sin considerar la cabecera (Thorsten et al., 2017)	Cifrado de todo el cuerpo del paquete (P. González, 2014)	Criptografía robusta (Colombo et al., 2015)

Fuente: Elaboración propia.

Tabla 2: Categoría 2. Forma de trabajo del protocolo de autenticación

Criterios de comparación	RADIUS	TACACS+	DIAMETER	KERBEROS
Soporte multiprotocolo	Ofrece soporte multiprotocolo limitado (Cisco, 2008)	Ofrece soporte multiprotocolo (Cisco, 2008)	Ofrece soporte multiprotocolo (P. González, 2013)	No ofrece soporte multiprotocolo (MIT Kerberos, 2021)
Interoperabilidad	Ampliamente compatible (TechLibrary, 2020)	No se admite ampliamente fuera de Cisco (TechLibrary, 2020)	Entre múltiples dispositivos y proveedores (Hacom, s. f.)	Admite la interoperabilidad (IBM, s. f.)
Rendimiento	Escalabilidad óptima, brinda notificaciones (Dafonte & Pallardó, 2015) Al ser uno de los pioneros está ampliamente desarrollado, el cual proporciona un amplio rendimiento al autenticar a los clientes que intenten conectarse a la red inalámbrica (De Luz, 2021).	Escalabilidad deficiente sin embargo brinda notificaciones (Cisco, 2012). Es importante el cuidado del tráfico puesto que el rendimiento puede verse afectado y reflejado en la experiencia del usuario final (Cisco, 2020).	Escalabilidad óptima, no notifica ninguna conexión (Dafonte & Pallardó, 2015). Sin embargo ofrece un gran control de sesiones de autenticación respaldado por el Proxy que utiliza garantizando una conexión estable a pesar de un amplio tráfico (Trujillo, 2020).	Notifica conexión mediante solida criptografía (MIT Kerberos, 2021) Al generar claves privadas temporales, llamadas claves de sesión, crea mensajes de inicio de sesión, sin embargo, al tener acceso un usuario ajeno al sistema, este queda expuesto (Cisco, 2006).
Protocolo de transporte	UDP (C. Rigney et al., 2000)	TCP (Ravi et al., 2017)	TCP con TLS o IPSEC (P. González, 2014)	UDP / TCP (Dayanand et al., 2020)
Sistema operativo	Windows Linux	Cisco	Windows Linux	Windows Linux

Fuente: Elaboración propia.

Tabla 3: Categoría 3. Funcionalidad AAA

Criterios de comparación	RADIUS	TACACS+	DIAMETER	KERBEROS
Autenticación	Sí	Sí	Sí	Sí
Autorización	Sí	Sí	Sí	No
Contabilidad	Sí	Sí	Sí	Sí

Fuente: Elaboración propia.

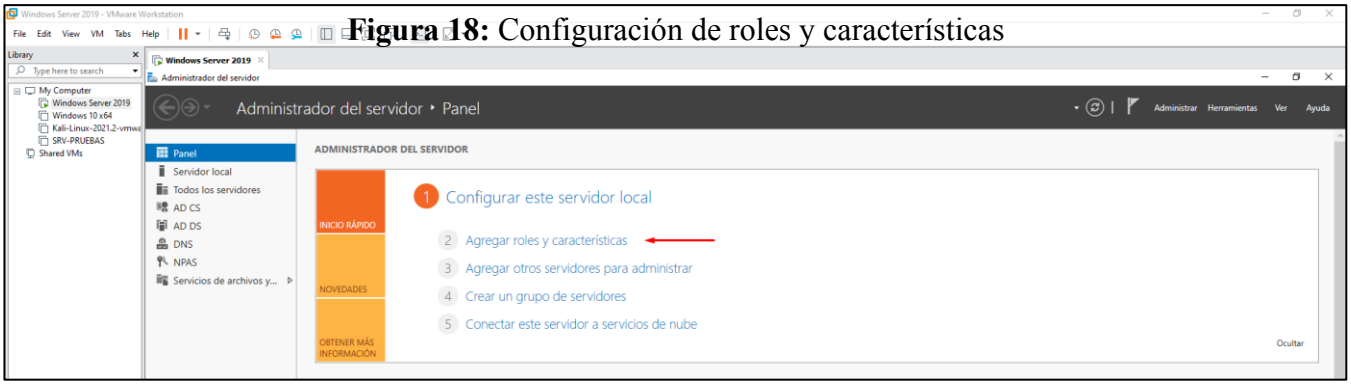
Por consiguiente, al realizar los cuadros comparativos por categorías de los Protocolos de Autenticación seleccionados, se consideró indispensable comprobar dicha información mediante la prueba de rendimiento de cada uno al realizar la conexión al Servidor.

Sin antes mencionar que el protocolo TACACS+ no fue evaluado, ya que se aplica únicamente en enrutadores y conmutadores Cisco, los cuales no se cuentan físicamente ni han sido conceptuados en el desarrollo de esta Tesis.

Para los protocolos RADIUS y KERBEROS, se hizo uso del Windows Server 2019, tal como se visualiza en las pruebas mostradas.

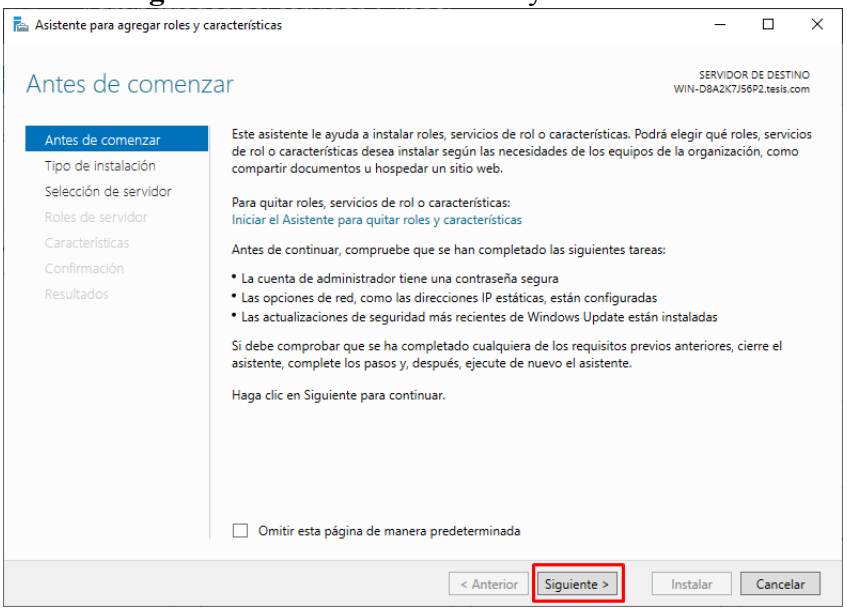
- Se instalaron los roles y características necesarias para poder comprobar la funcionalidad del protocolo RADIUS y KERBEROS.

Figura 18: Configuración de roles y características



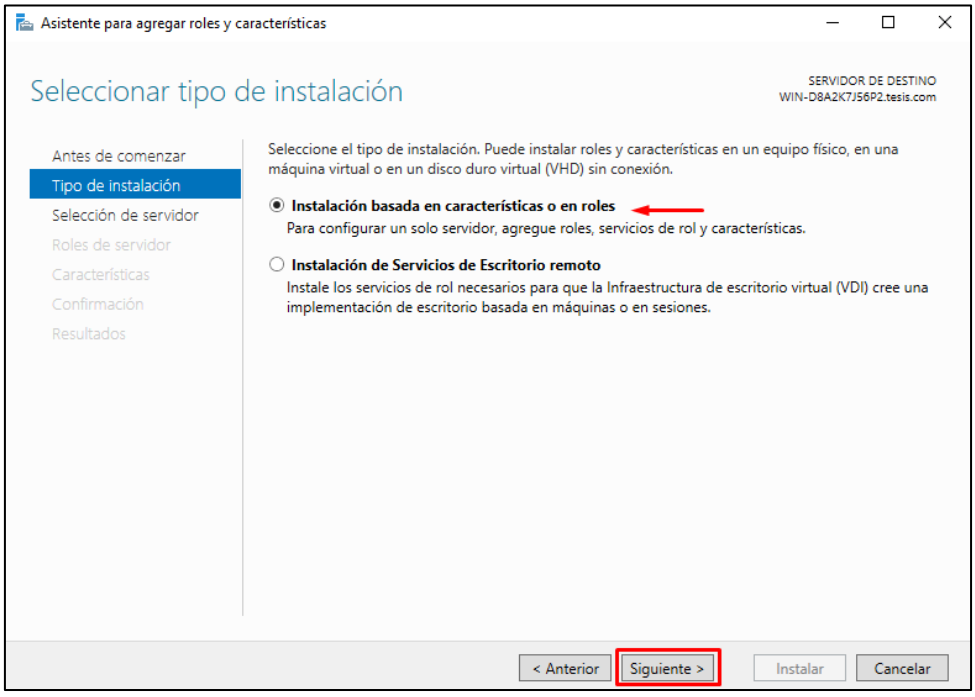
Fuente: Elaboración propia.

Figura 19: Instalación de roles y características



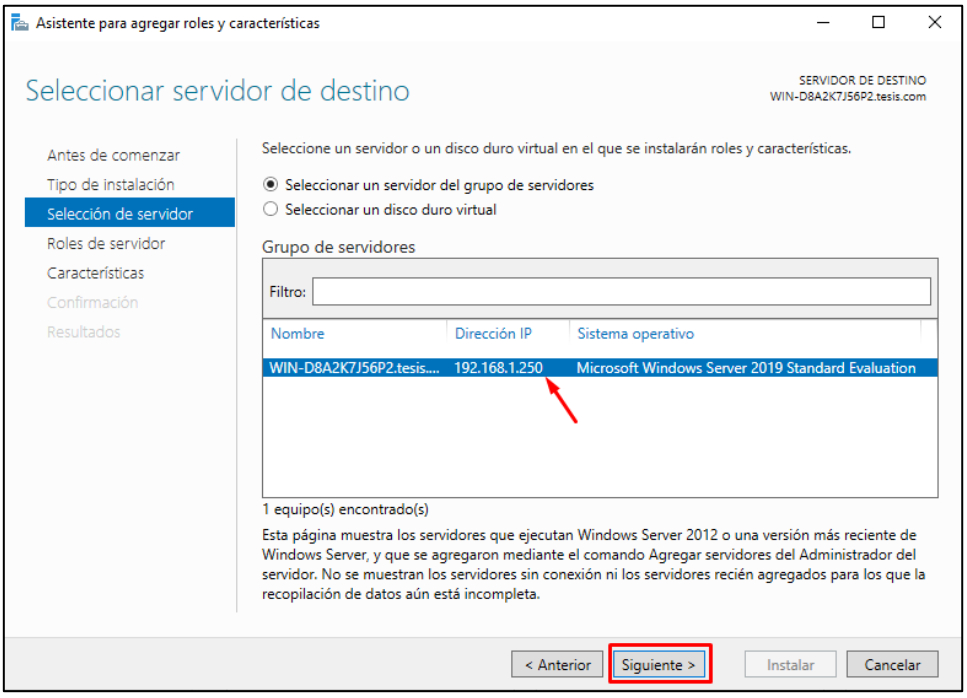
Fuente: Elaboración propia.

Figura 20: Tipo de instalación de roles y características



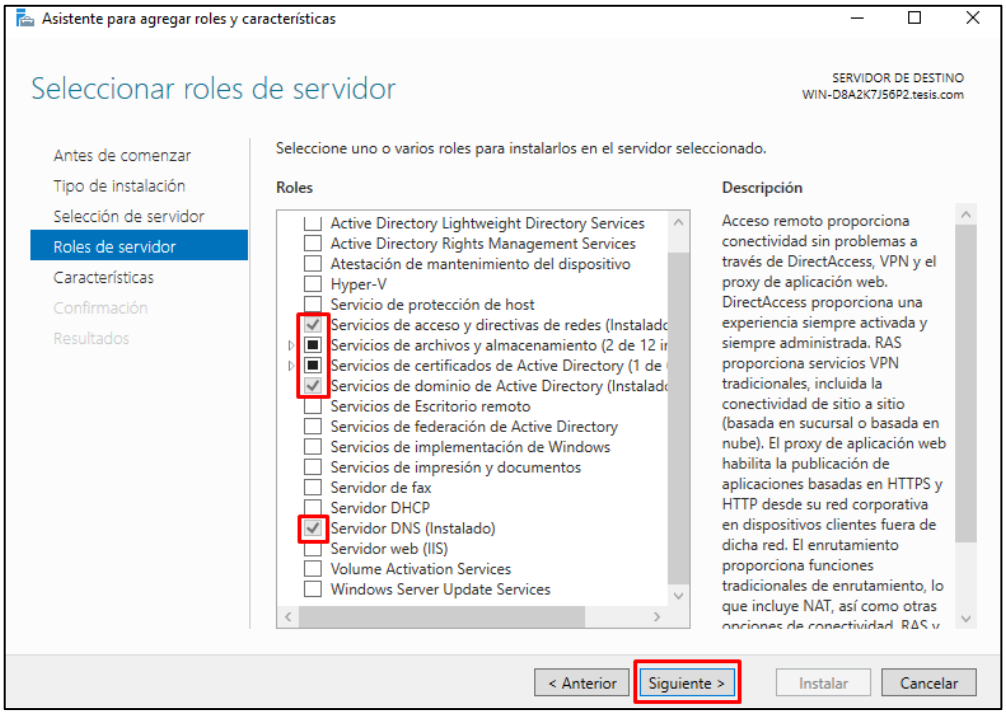
Fuente: Elaboración propia.

Figura 21: Servidor de destino, roles y características



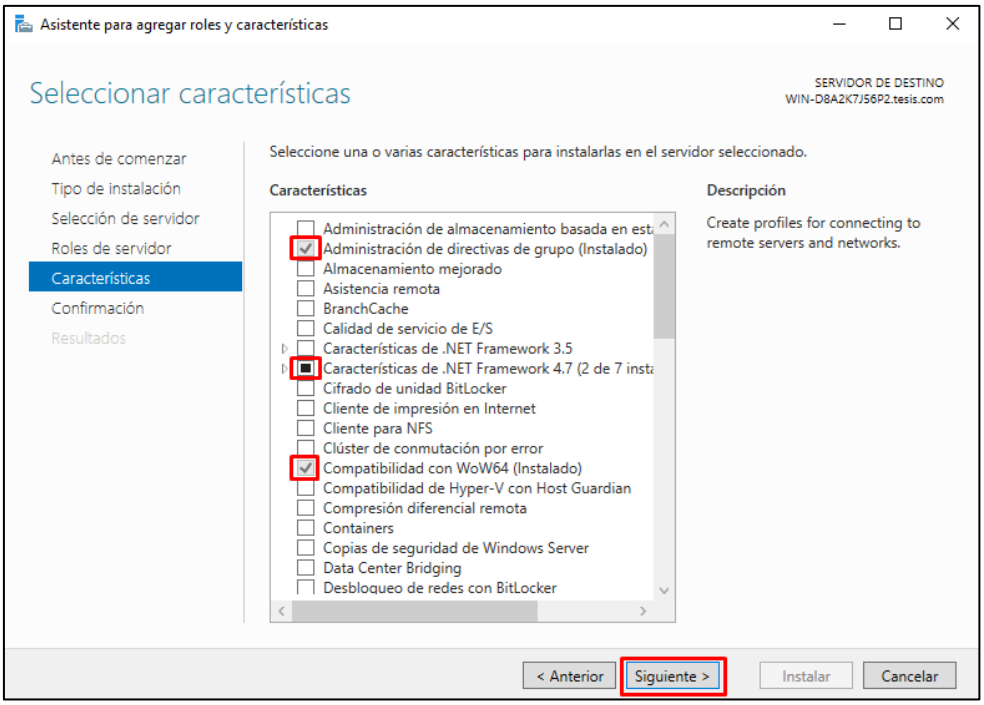
Fuente: Elaboración propia.

Figura 22: Selección roles de servidor



Fuente: Elaboración propia.

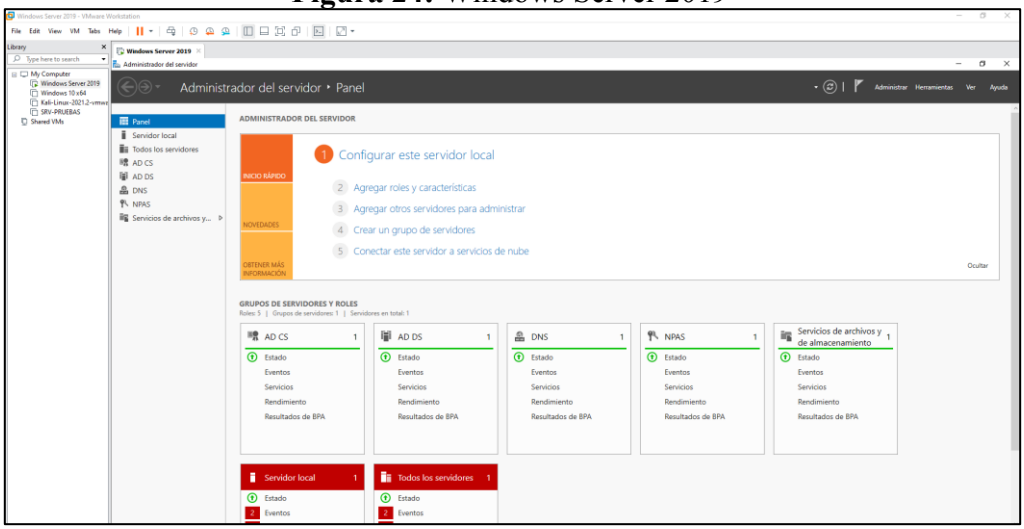
Figura 23: Selección de características



Fuente: Elaboración propia.

- Al finalizar la instalación de los roles y características, se visualiza la Interfaz principal de Windows Server con lo configurado.

Figura 24: Windows Server 2019

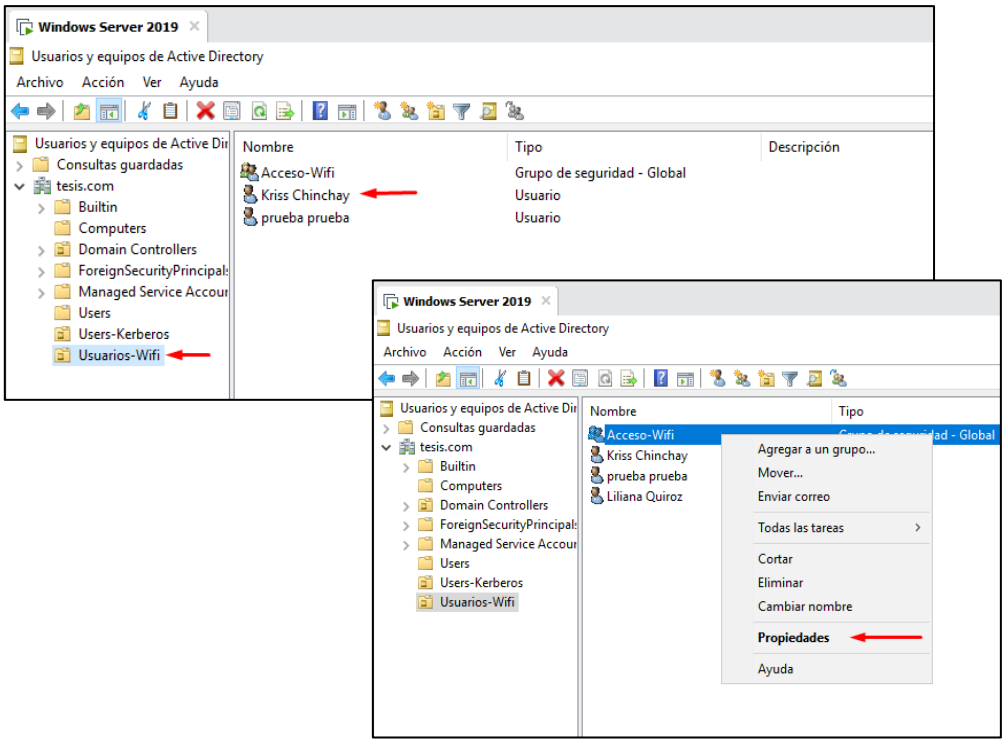


Fuente: Elaboración propia.

- **Para RADIUS**, es necesario ingresar al dominio creado en el momento de la instalación de la máquina virtual, mediante la opción *Herramientas*, "*Usuarios y equipos de Active Directory*", clic en el dominio creado (siendo **tesis.com**), clic en la carpeta *Managed Service Account,* crear la carpeta para crear usuarios (siendo **Usuarios-Wifi**).

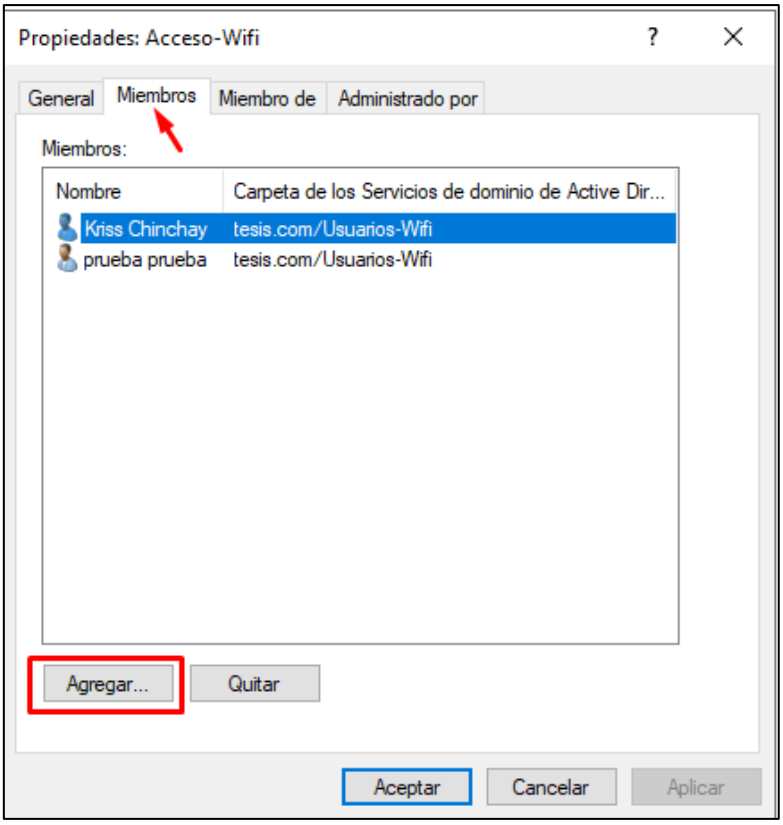
- Se debe agregar los usuarios a ingresar mediante Wifi.

Figura 25: Usuarios y equipos de Active Directory



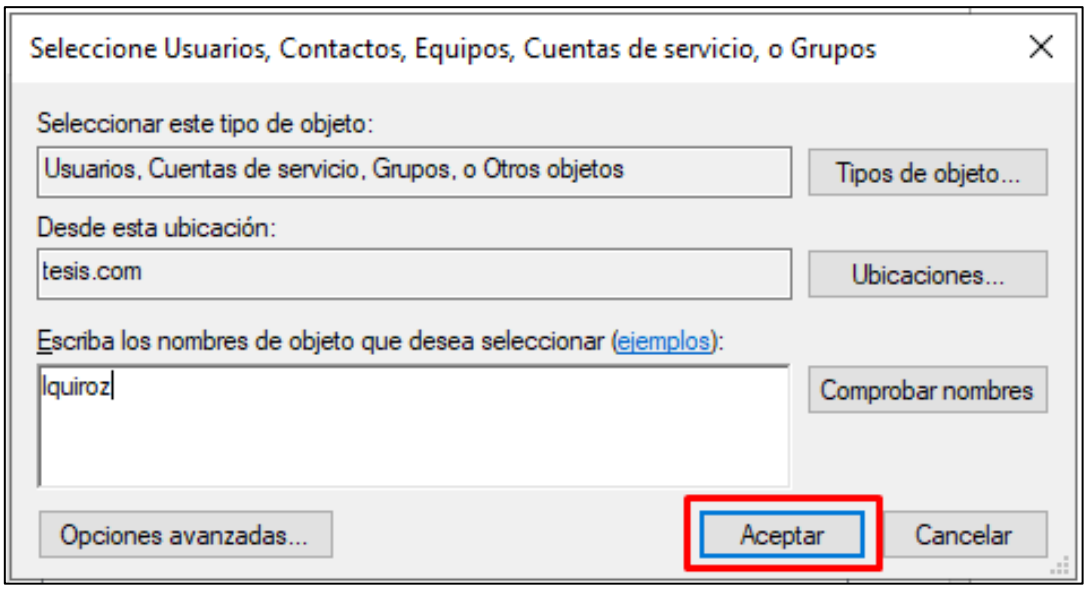
Fuente: Elaboración propia.

Figura 26: Propiedades: Acceso-Wifi



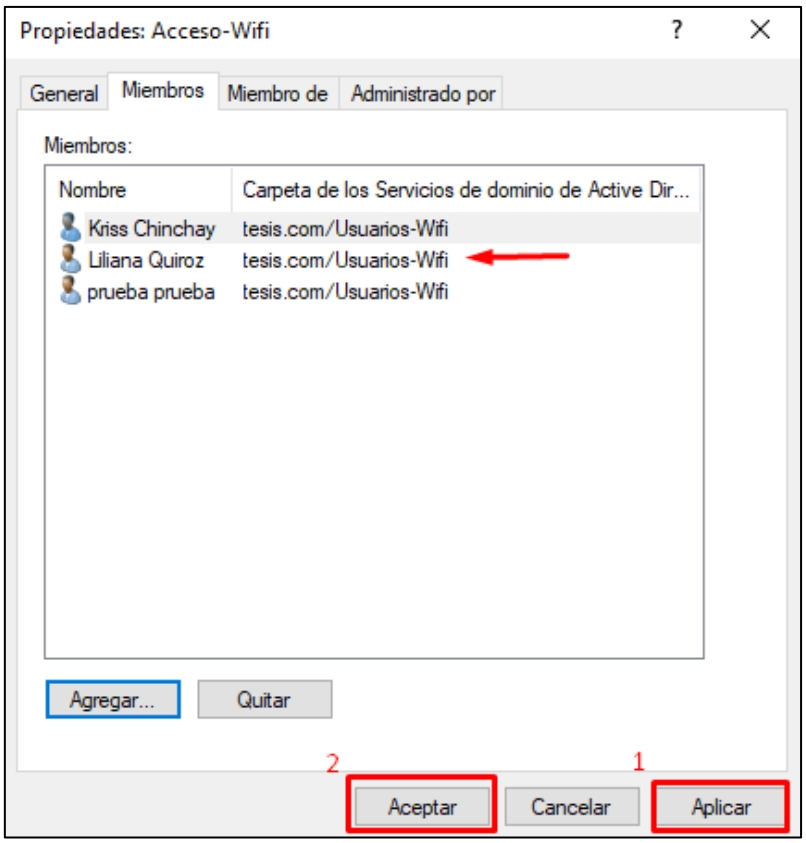
Fuente: Elaboración propia.

Figura 27: Selección de usuarios para agregar



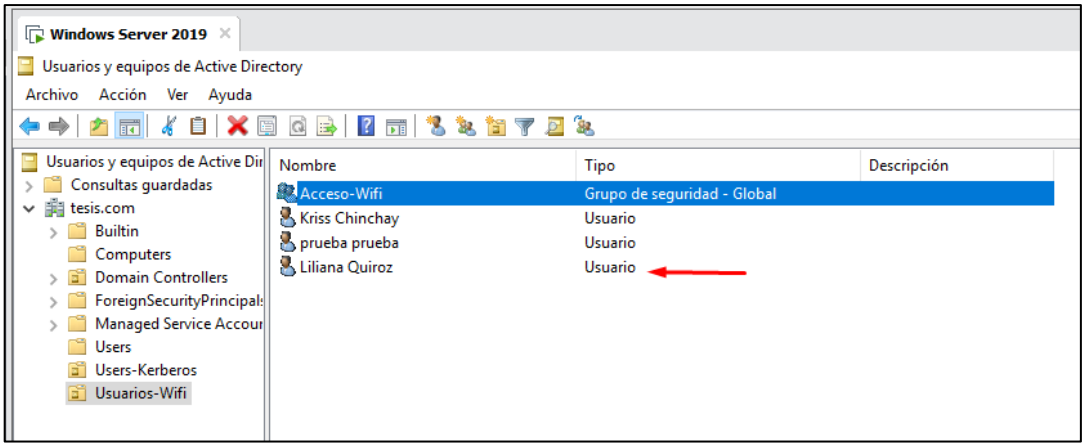
Fuente: Elaboración propia.

Figura 28: Propiedades: Acceso-Wifi, miembros agregados



Fuente: Elaboración propia.

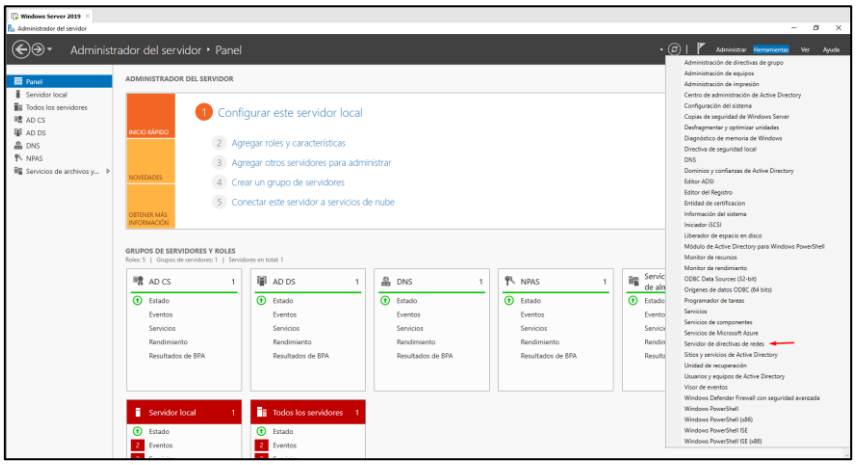
Figura 29: Vista de Miembros, Usuarios-Wifi



Fuente: Elaboración propia.

- Para la configuración de clientes y servidores RADIUS, se dirige a *Herramientas*, opción *"Servidor de directivas de redes"*

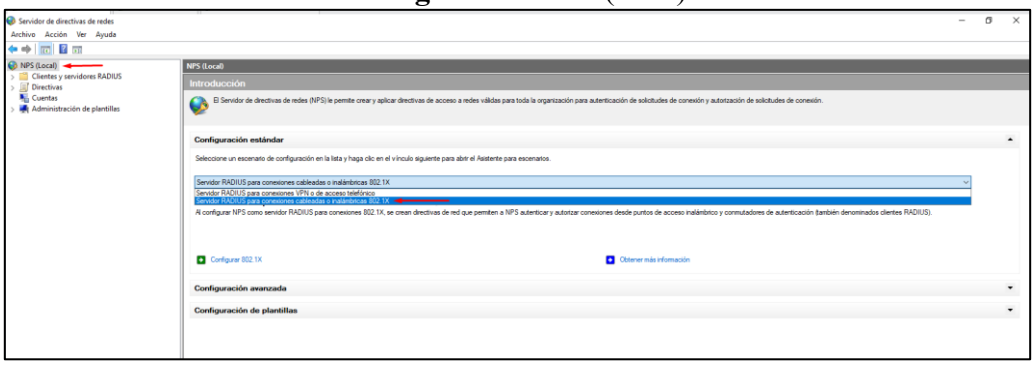
Figura 30: Servidor de directiva de redes"



Fuente: Elaboración propia.

- Continuando, en NPS (local) se selecciona la opción *"Servidor RADIUS para conexiones cableadas o inalámbricas 802.1X"*

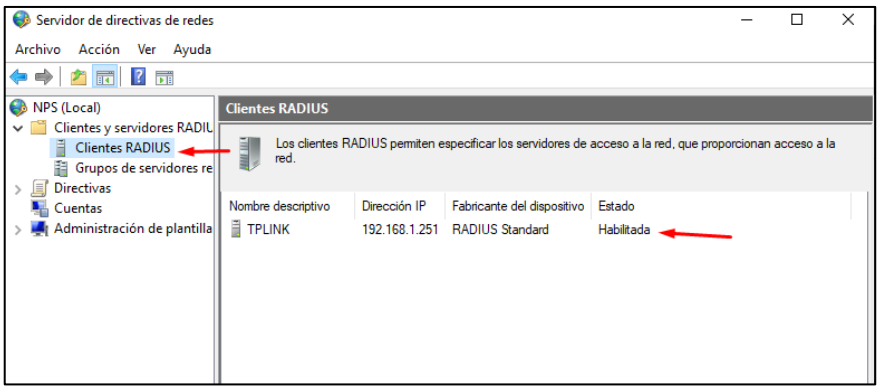
Figura 31: NPS (local)



Fuente: Elaboración propia.

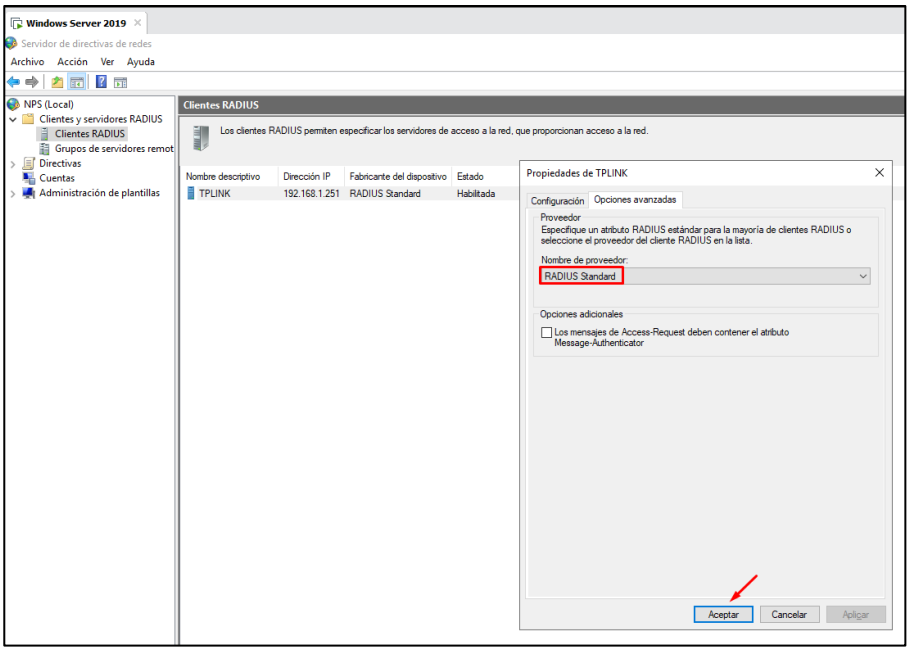
Aún en NPS (local) se configura el Cliente RADIUS el cuál es el Access Point, siendo su dirección *IP: 192.168.1.251*

Figura 32: Cliente RADIUS



Fuente: Elaboración propia.

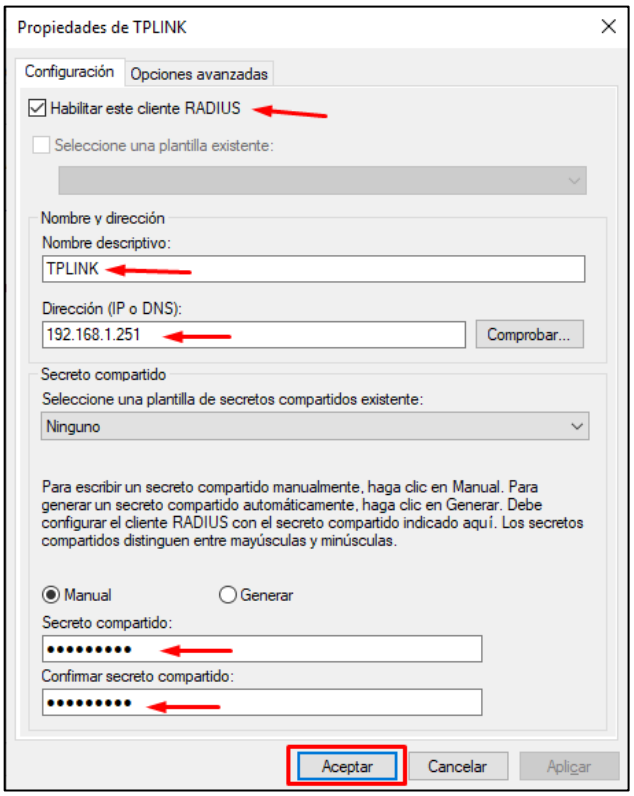
Figura 33: Cliente RADIUS configurado



Fuente: Elaboración propia.

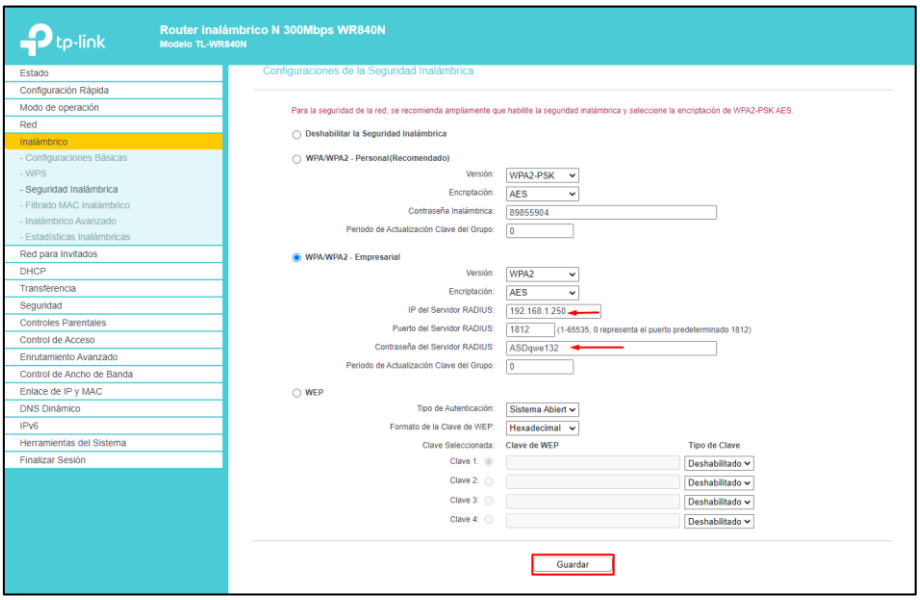
- Con la configuración finalizada, al asistir a las propiedades del Cliente, es fundamental ingresar la misma contraseña tanto en Secreto compartido como en la opción de Contraseña del Servidor RADIUS que se encuentra en la configuración del Access Point.

Figura 34: Configuración del Cliente RADIUS



Fuente: Elaboración propia.

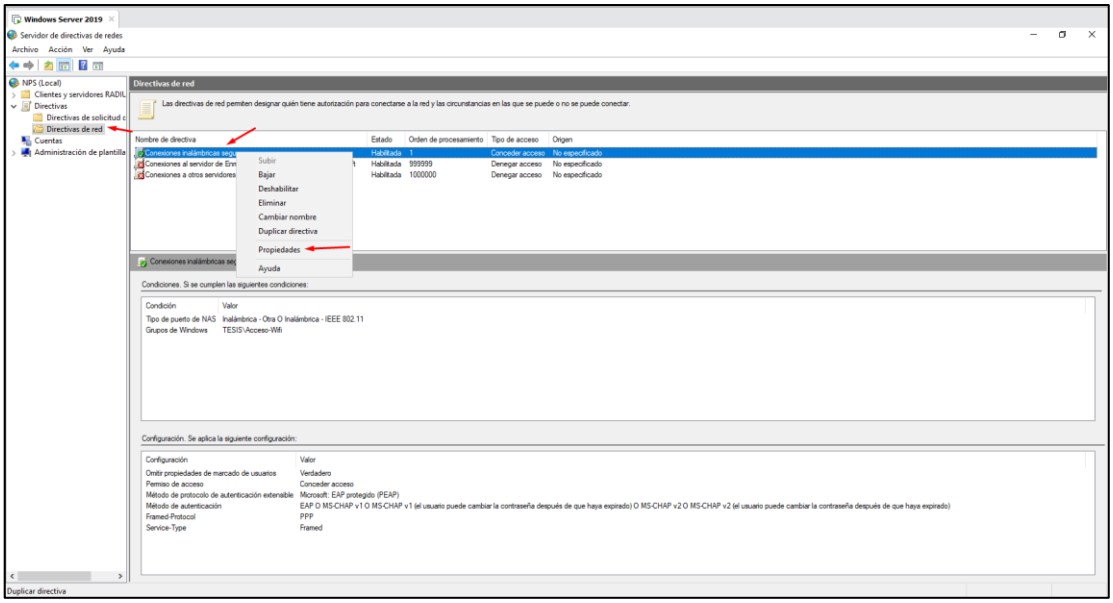
Figura 35: Configuración del Access Point



Fuente: Elaboración propia.

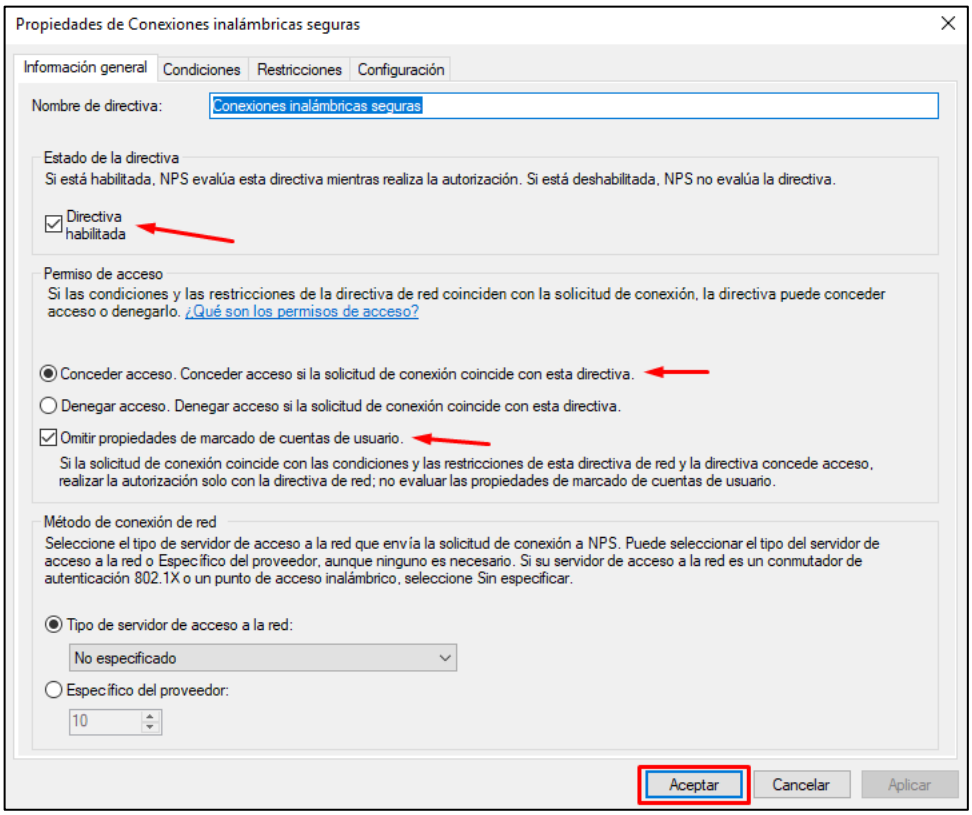
- Al asistir a NPS (local), en la sección de Directivas ingresando a Directivas de Red existe una sección de *"Conexiones inalámbricas seguras"*, la cual en sus propiedades se debe habilitar la directiva y conceder el acceso. Además de asegurar que se encuentre en *condiciones* del grupo Tesis y en restricciones, método de autenticación EAP.

Figura 36: NPS (local)



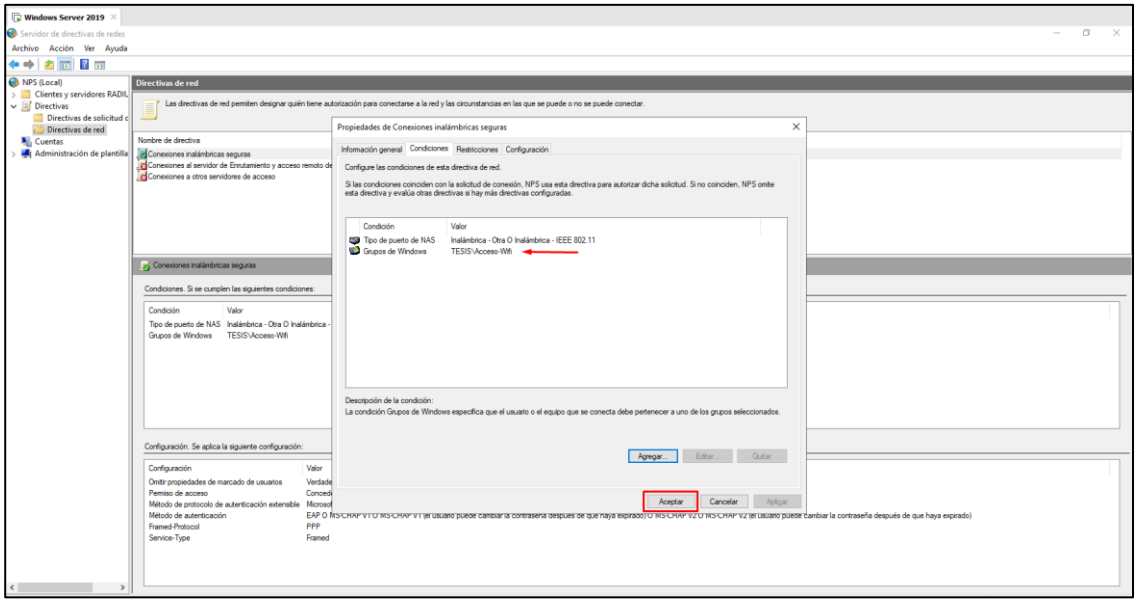
Fuente: Elaboración propia.

Figura 37: Propiedades de Conexiones inalámbricas seguras



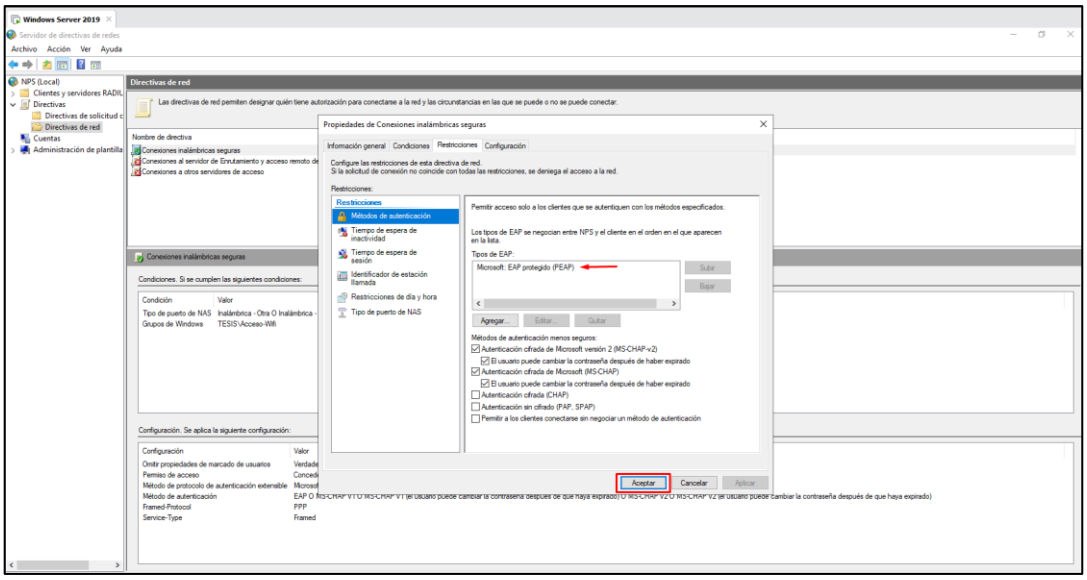
Fuente: Elaboración propia.

Figura 38: Condiciones - Propiedades de Conexiones inalámbricas seguras



Fuente: Elaboración propia.

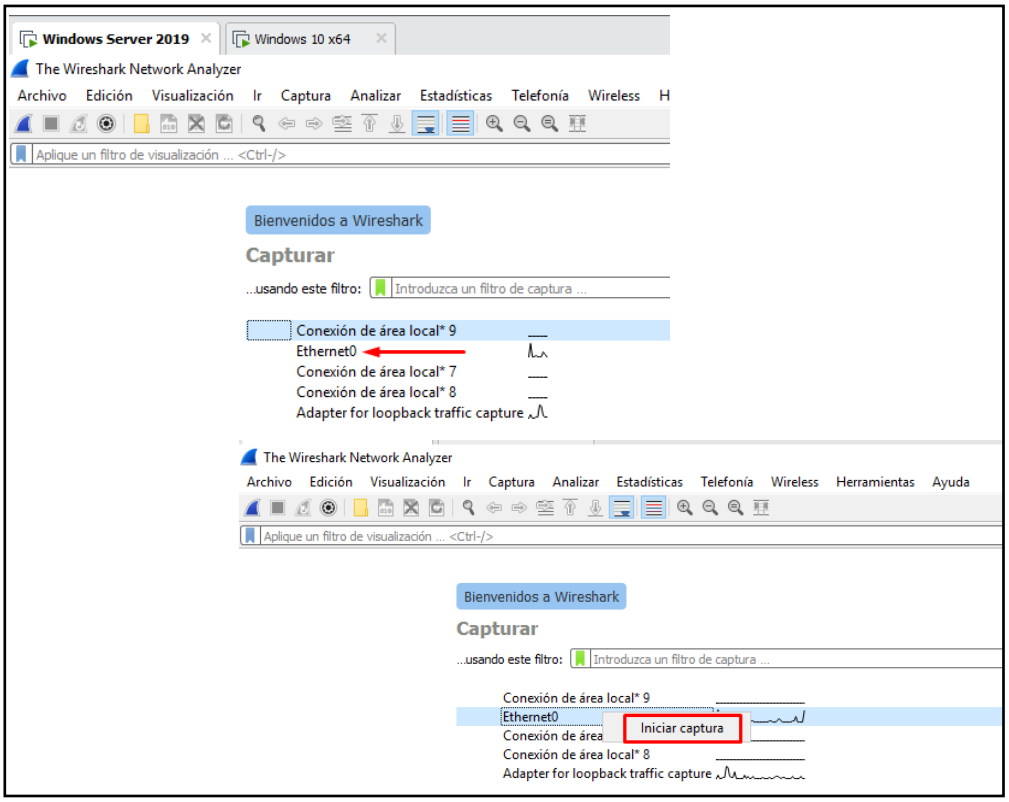
Figura 39: Restricciones - Propiedades de Conexiones inalámbricas seguras



Fuente: Elaboración propia.

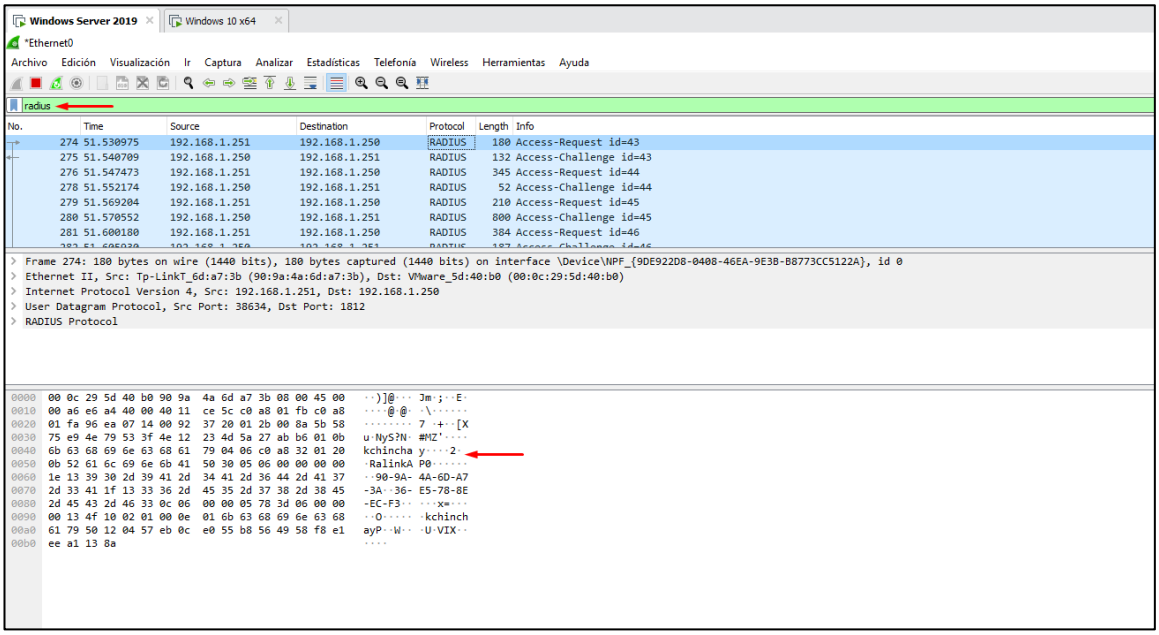
- Para comprobar el Protocolo de Autenticación RADIUS mediante la herramienta Wireshark, al seleccionar *Ethernet0*, clic derecho *Iniciar captura* y digitar *RADIUS* para poder comprobar el tiempo y conexión.

Figura 40: Prueba RADIUS en Wireshark



Fuente: Elaboración propia.

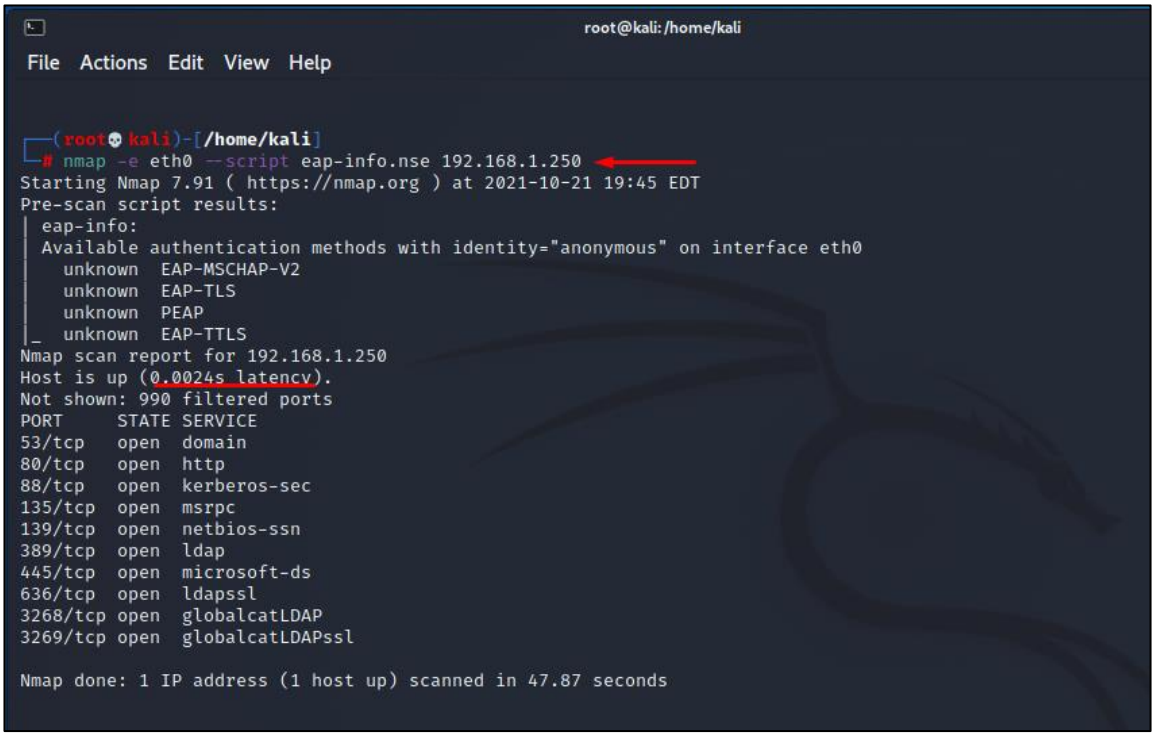
Figura 41: Resultado de prueba RADIUS en Wireshark



Fuente: Elaboración propia.

- A la vez se puede visualizar el tiempo de latencia mediante *Kali Linux* mediante un script predeterminado para poder reconocerlo.

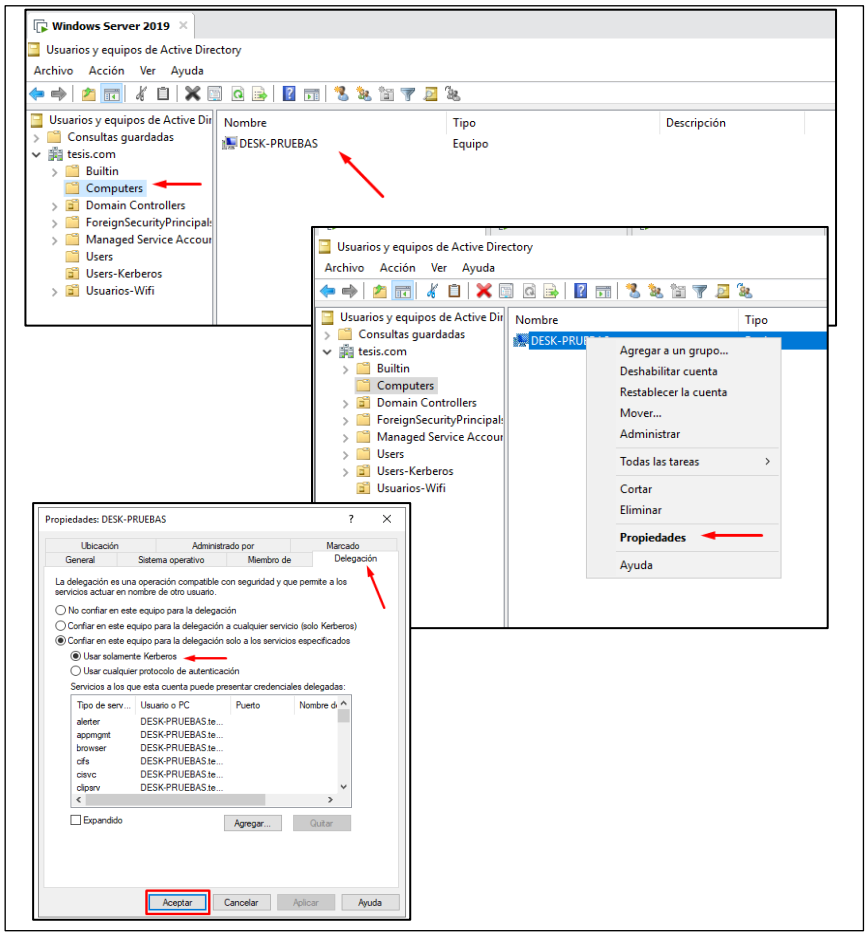
Figura 42: Prueba RADIUS en Kali Linux



Fuente: Elaboración propia.

- **Para KERBEROS**, es necesario ingresar al dominio creado en el momento de la instalación de la máquina virtual, mediante la opción *Herramientas*, "*Usuarios y equipos de Active Directory"*, clic en el dominio creado (siendo **tesis.com**), clic en la carpeta *Computers,* para poder agregar los Clientes que estarán permitidos a ingresar mediante este protocolo, siendo en este caso *DESK-PRUEBAS*; se configura con clic derecho en el nombre e ingresar a la opción: *Propiedades*, asistir a *Delegación* y seleccionar *Usar solamente Kerberos* para finalmente *Aceptar* y guardar la configuración.

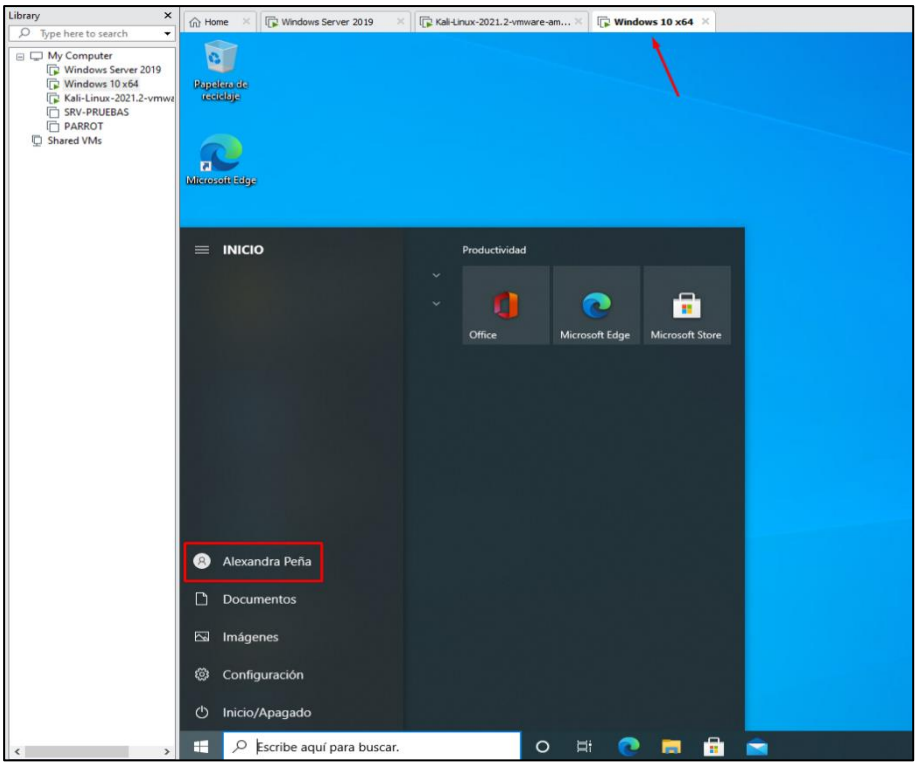
Figura 43: Configuración inicial - Kerberos



Fuente: Elaboración propia.

- Se debe ingresar desde el cliente *DESK-PRUEBAS* para que se pueda probar el rendimiento del protocolo.

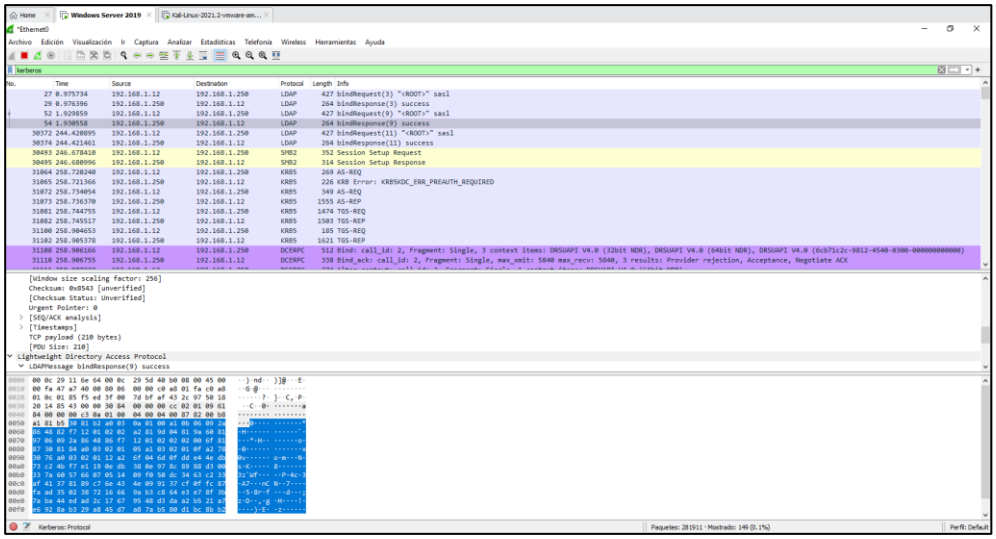
Figura 44: Windows 10 Cliente



Fuente: Elaboración propia.

- Para comprobar el Protocolo de Autenticación KERBEROS como se realizó con el protocolo anterior, se hace uso de la herramienta Wireshark,

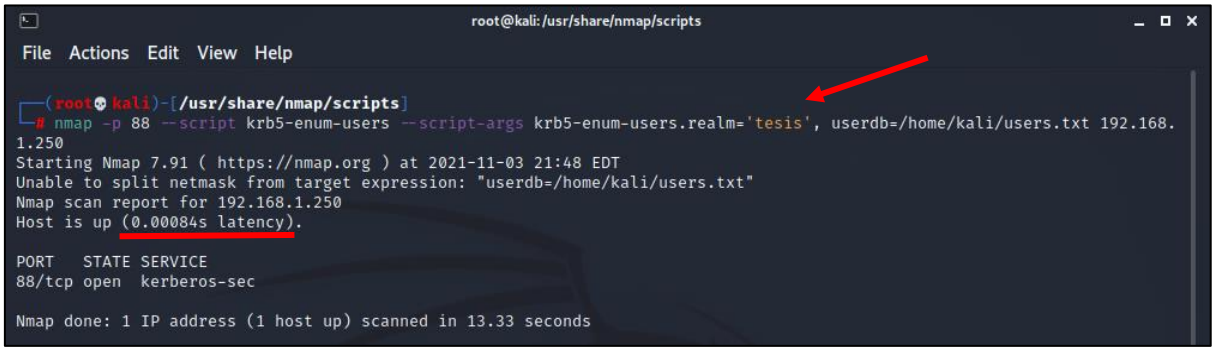
Figura 45: Resultado de prueba KERBEROS en Wireshark



Fuente: Elaboración propia.

- A la vez se puede visualizar el tiempo de latencia mediante *Kali Linux* mediante un script predeterminado para poder reconocerlo.

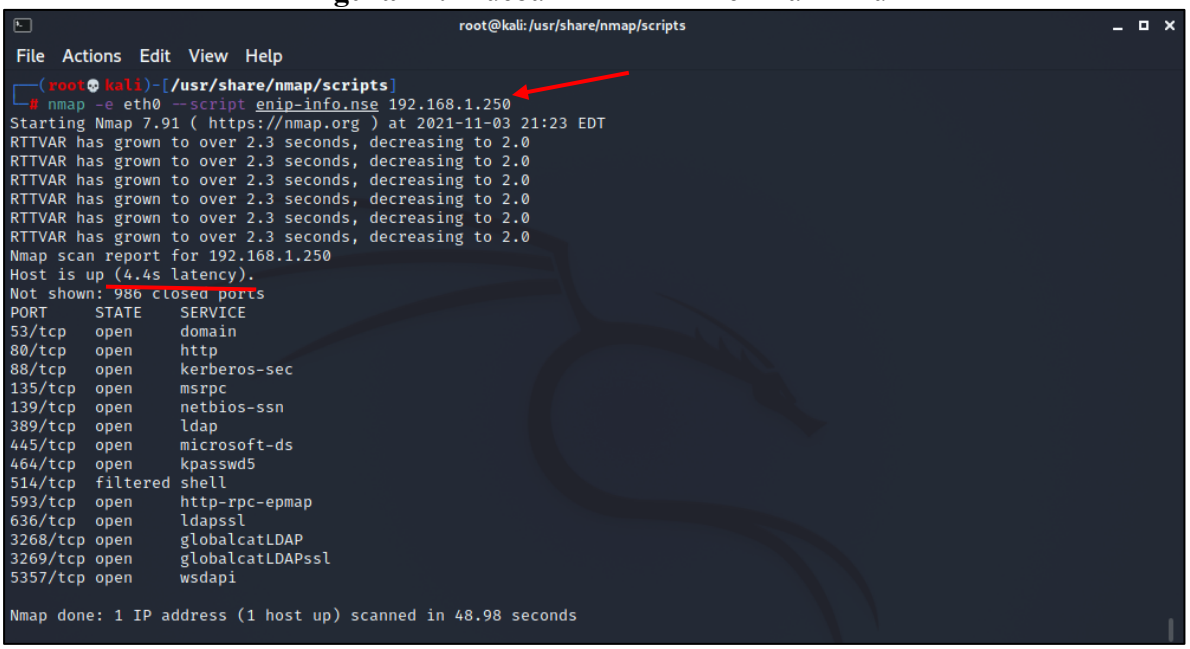
Figura 46: Prueba KERBEROS en Kali Linux



Fuente: Elaboración propia.

- **Para DIAMETER**, se consideró su prueba mediante un Script que están predefinidos en la herramienta *NMAP* en Kali Linux, de esta manera se prueba directamente la latencia del protocolo.

Figura 47: Prueba DIAMETER en Kali Linux



Fuente: Elaboración propia.

De esta manera se concluye refiriendo que, gracias a las pruebas de rendimiento realizadas, se ha podido identificar la fortaleza de cada Protocolo de Autenticación, puesto que cada uno ofrece particularidades que los hace auténticos, sin embargo, se puede considerar por la diversidad de información existente, tiempo de desarrollo y aporte, al Protocolo RADIUS el más acertado a usar a la vez el tiempo

de latencia de cada protocolo demuestra también su rapidez lo cual es un gran motivo a considerar.

1.1. Ponderación y elección del protocolo a implementar

Para la ponderación de los protocolos de autenticación de usuarios, se hizo uso de una escala del 0 al 3 en donde 0 equivale a: no cuenta, 1 equivale a: nivel bajo, 2 equivale a: nivel medio y 3 equivale a: nivel alto. Se tuvo en cuenta ocho criterios en común considerados con mayor relevancia para realizar ponderación y elección entre los cuatro protocolos de autenticación de usuarios, de esta manera implementar el protocolo más competente después del análisis realizado previamente.

Tabla 4: Ponderación de protocolos

Criterios	RADIUS	TACACS+	DIAMETER	KERBEROS
Compatibilidad con diversos proveedores	3	1	3	3
Nivel de seguridad	3	3	3	2
Compatibilidad con software propietario	3	3	3	3
Compatibilidad con software libre	3	0	3	3
Autenticación y autorización	3	3	3	1
Soporte multiprotocolo	2	3	2	0
Protocolo Cliente/Servidor	3	3	0	3
TOTAL	**20**	**16**	**17**	**15**

Fuente: Elaboración propia.

Finalizando la ponderación de los protocolos de autenticación de usuarios, se concluyó que el protocolo a implementar obteniendo un total de **20 puntos**, fue RADIUS. Desglosando cada criterio evaluado, posee un alto nivel de compatibilidad con diversos proveedores ya que es compatible con software propietario y libre, a pesar de poseer un nivel medio de seguridad logra autorizar y autenticar usuarios.

Además, es un protocolo cliente/servidor que ofrece soporte multiprotocolo limitado al transportar datos.

1.2. Implementación del Protocolo de Autenticación en el Servidor FreeRADIUS

Tras la elección de RADIUS como el protocolo de autenticación de usuarios, la implementación desarrollada se basó en montar un servidor FreeRADIUS en una máquina virtual, siendo por elección nuestra, Ubuntu.

FreeRADIUS se caracteriza por proveer un amplio rendimiento, compatibilidad con protocolos de autenticación frecuentemente utilizados, desmesurada seguridad además de ser un software totalmente gratuito y Ubuntu siendo un sistema operativo de código abierto, el cual fue elegido por disponer las mejores herramientas al realizar una auditoría en internet y poseer de un gran sistema de seguridad informática.

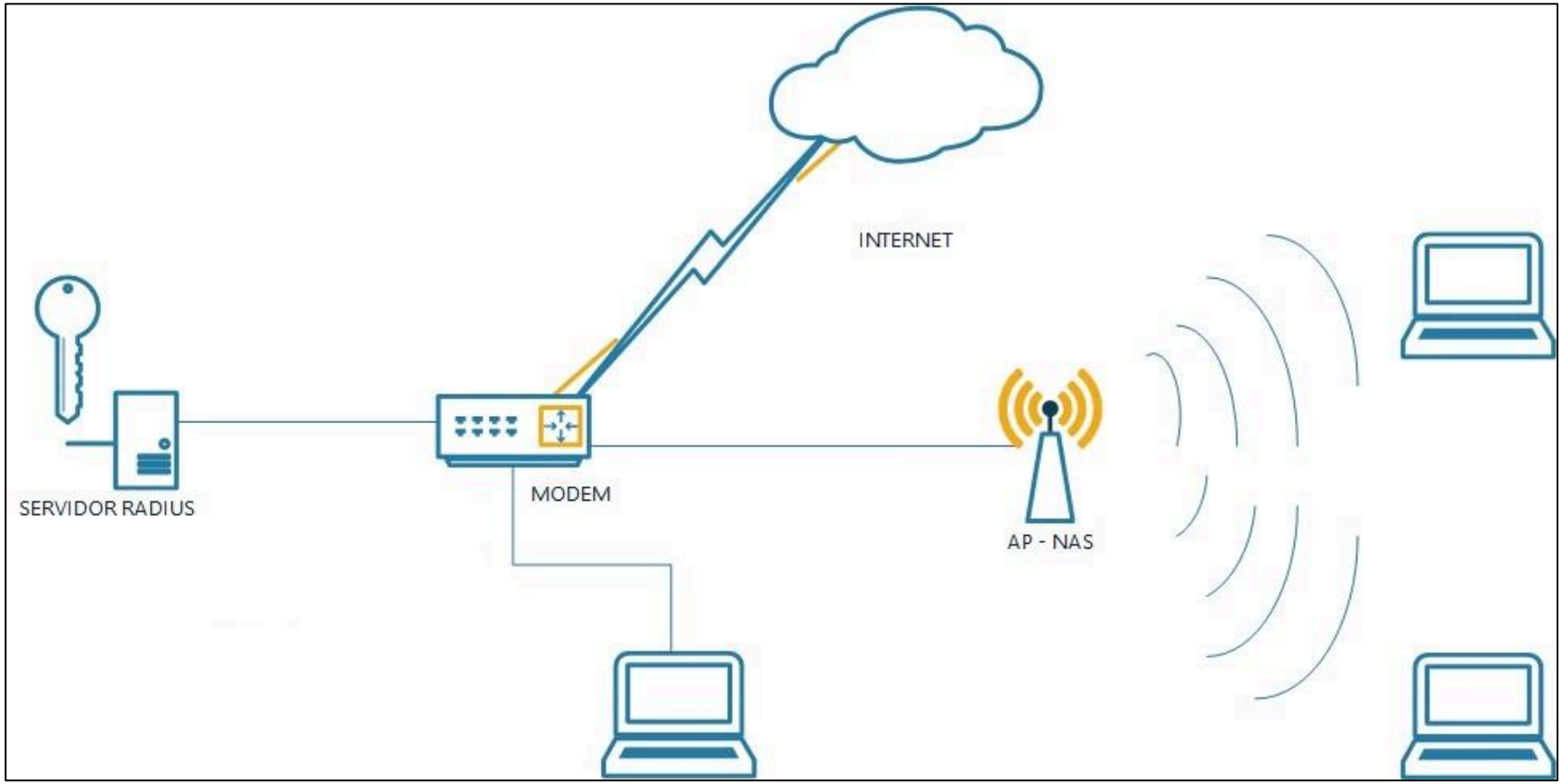
Por lo tanto, al finalizar su exitosa configuración, se realizó la creación de usuarios y un cliente, Access Point, el cual viene a ser el dispositivo al que los usuarios realizaron la conexión.

Access Point es un dispositivo que con ayuda del servidor FreeRADIUS permite la correcta autenticación para que los usuarios que cuenten con dispositivos inalámbricos puedan acceder a la red.

Después de realizar la configuración del Access Point mediante web y conectado con el servidor instalado en la máquina virtual, finalizamos la implementación con la ejecución de pruebas desde diversos dispositivos inalámbricos ingresando de manera correcta y errónea el usuario con su respectiva contraseña, creados durante la configuración del servidor en la máquina virtual.

Fundamentando nuestro siguiente diagrama:

Figura 48: Diagrama de Red



Fuente: Elaboración propia.

Para lograr la implementación, ha sido necesario hacer uso de:

- Máquina Virtual: Virtual Box
- Sistema Operativo: Ubuntu 21.04
- Servidor FreeRadius
- Laptops y celulares (dispositivos a conexión WiFi)
- Access Point

La implementación detallada anteriormente de manera general se dividió en las siguientes etapas:

- ETAPA I: INSTALACIÓN DE SOFTWARE DE VIRTUALIZACIÓN

  Luego de la elección de VirtualBox como el software de virtualización a utilizar, referente a sus características por la ventaja de ser gratuito; se procede a su descarga y su eficaz instalación de su última versión al 2021, VirtualBox 6.1.

- ETAPA II: INSTALACIÓN DEL SISTEMA OPERATIVO UBUNTU

  Al contar con el Virtual Box ya operativo, se crea una máquina virtual en la cual se importó la imagen ISO descargada del sistema operativo Ubuntu 21.04.

- ETAPA III: CONFIGURACIÓN INICIAL DEL SISTEMA OPERATIVO

  Continuar con su configuración para poder iniciar la máquina virtual de manera correcta.

- ETAPA IV: INSTALACIÓN DEL SERVIDOR FREERADIUS Y LDAP

  Con Ubuntu ya operativo, se procede con la instalación del servidor FreeRADIUS y LDAP haciendo uso de los paquetes necesarios.

- ETAPA V: CREACIÓN DE USUARIOS EN EL SERVIDOR LDAP

  Contando con los paquetes FreeRADIUS y LDAP instalados, se hace uso de los respectivos comandos para la creación de usuarios y cliente.

- ETAPA VI: CONEXIÓN DE LOS SERVIDORES CON EL ACCESS POINT

  Para finalizar la correspondiente implementación y configuración de los servidores en la máquina virtual, se configura el Access Point en la página web añadiendo el IP Radius, el cual es el IP de la máquina virtual.

- ETAPA VII: PRUEBAS REALIZADAS

  Para comprobar la efectividad de la implementación, se realizó pruebas en diversos dispositivos inalámbricos.

  Al finalizar la implementación se procedió a la Validación de Expertos, para lo cual se dispuso a tres profesionales un documento de evaluación conformado por: explicación del desarrollo de la Tesis, tablas de categorización para los protocolos a comparar, ponderación y elección del protocolo a implementar, manual de implementación de protocolo RADIUS y las pruebas realizadas; con la finalidad de que sea posible por parte de los profesionales emitir su juicio de pertinencia de la solución del diseño propuesto. Constatando que los tres expertos brindaron su opinión favorable, indicadas mediante la Hoja de Validación de Aporte Práctico; afirmando que si se llega a implementar el diseño propuesto puede resultar beneficioso para cualquier organización.

La investigación realizada sobre la comparación de protocolos de autenticación de usuarios obtuvo como resultado la elección del protocolo RADIUS, demostrado en las pruebas de rendimiento y en la simulación de su

implementación; quedando en evidencia su viabilidad, se desglosan las siguientes conclusiones:

- Según los criterios de búsqueda, mediante la revisión sistemática de los documentos analizados, se logró obtener el conocimiento científico en relación a los protocolos de autenticación de usuarios, el cual fue fundamental para llevar a cabo la presente investigación.

- Mediante las tablas de análisis se logró sintetizar y esquematizar la información científica de atributos y características de los protocolos de autenticación de usuarios, seguidamente luego de su comparación y ponderación, permitieron la correcta selección del protocolo a implementar.

- El método de control de acceso propuesto, tras la selección del protocolo de autenticación RADIUS, gracias a las pruebas de rendimiento y la información sintetizada de cada Protocolo de Autenticación, se sustentó en la implementación del servidor FreeRADIUS y LDAP en una máquina virtual conjuntamente a la conexión a un Router y luego a un Access Point, lo cual deja en evidencia la seguridad que puede llegar a tener una red inalámbrica mediante el uso gratuito de estas herramientas.

- La viabilidad y la calidad científica de la investigación, fue ratificada por tres expertos de amplia y reconocida trayectoria profesional en el departamento de Lambayeque, haciendo notar que la propuesta cumple y demuestra el amplio potencial para poder hacerla realidad.

BIBLIOGRAFÍA

Aboba, B., & Wood, J. (2003). RFC 3539 - Authentication, Authorization and Accounting • AAA, Transport Profile. *Internet Engineering Task Force (IETF)*.

Alonso, I. (2013). Análisis comparativos de dos protocolos para control de acceso y administración de equipos de telecomunicaciones. En *Universidad Católica de Colombia*. http://hdl.handle.net/10983/812

Andrade, G. (2019). Análisis de prestaciones de los protocolos de autenticación remota RADIUS y TACACS+ en Infraestructura de Comunicaciones Corporativas [Escuela Superior Politécnica de Chimborazo]. En *Escuela Superior Politécnica de Chimborazo*. http://dspace.espoch.edu.ec/handle/123456789/10997

Anónimo. (2020). *¿Qué es, para qué Sirve y Cuántas Versiones de Windows Server Existen? | Mira Cómo Se Hace*. 29 de mayo. https://miracomosehace.com/que-es-sirve-cuantas-versiones-windows-server-existen/

Arias, M., & Carrillo, C. (2017). Rediseño del sistema de autenticación de usuarios de una red coorporativa a través de la aplicación de la plataforma tecnológica de autenticación CISCO ISE (Identity Services Engine) para la empresa NET IO Servicios S.A. [Escuela Politécnica Nacional]. En *Escuela Politécnica Nacional*. http://bibdigital.epn.edu.ec/handle/15000/17011

Bardales, M. (2015). Sistema de gestión de acceso a una red wi-fi utilizando software libre para mejorar el nivel de seguridad del acceso a la información. En *Universidad César Vallejo*. https://repositorio.ucv.edu.pe/handle/20.500.12692/11713

Barker, E. (2020). Recommendation for key management: En *National Institute of Standards and Technology (NIST)*. https://doi.org/10.6028/NIST.SP.800-57pt1r5

C. Rigney, S. Willens, Rubens, A., & Simpson, W. (2000, junio). *RFC 2865 - Remote Authentication Dial In User Service (RADIUS)*. Internet Engineering Task Force (IETF). https://tools.ietf.org/html/rfc2865

Carrión-Barco, G., Sánchez-Chero, M.-J., Del Castillo Castro, C. I., Campos Flores, F. W., & Timaná Alvarez, M. (2021). Modelo de seguridad informática para un medio de conexión pública. *Revista de la Universidad del Zulia*, *12*(32), 344-357. https://doi.org/10.46925//rdluz.32.21

Castro, C., & Eras, G. (2017). Análisis de factibilidad para la configuración del protocolo DIAMETER en los servidores de telefonía IP ELASTIX para el cifrado de paquetes de voz y autenticación caso de estudio: empresas que tengan integrada la central de telefonía IP ELASTIX. En *Universidad de Guayaquil*. http://repositorio.ug.edu.ec/handle/redug/23888

Chaparro, R., & Mejía, M. (2006). Análisis de desempeño y evaluación de requerimientos AAA en protocolos de seguridad sobre redes inalámbricas IEEE 802.11. *Ciencia e Ingeniería Neogranadina*, *16*(2), 74-85. https://doi.org/10.18359/rcin.1236

Chira, E. (2020, septiembre 10). La ciberseguridad de las compañías en jaque. *El Peruano*. https://elperuano.pe/noticia-la-ciberseguridad-de-companias-jaque-103474.aspx

Cisco. (s. f.-a). *¿Qué es un access point?* Cisco. Recuperado 2 de abril de 2021, de https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-access-point.html

Cisco. (s. f.-b). *radius-server_key*. Cisco. Recuperado 1 de febrero de 2021, de https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/n5k/commands/radius-server-key.html

Cisco. (s. f.-c). *Wireless Local Area Network (WLAN)*. Cisco. Recuperado 26 de enero de 2021, de https://www.cisco.com/c/en/us/tech/wireless-2f-mobility/wireless-lan-wlan/index.html

Cisco. (2006). *Descripción general de Kerberos: Servicio de autenticación para sistemas de red abierta*. Cisco. https://www.cisco.com/c/es_mx/support/docs/security-vpn/kerberos/16087-1.html

Cisco. (2008). *TACACS+ and RADIUS Comparison - Cisco*. Cisco. https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-

authentication-dial-user-service-radius/13838-10.html#comparing

Cisco. (2012). *Ejemplo de Configuración de TACACS+ en un Punto de Acceso Aironet para la Autenticación de Login con Uso de la GUI*. Cisco. https://www.cisco.com/c/es_mx/support/docs/wireless-mobility/wireless-lan-wlan/70149-tacacs-ap-config.html

Cisco. (2018). TACACS+ Configuration Guide, Cisco IOS Release 15S. En *Cisco*. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_tacacs/configuration/15-s/sec-usr-tacacs-15-s-book/sec-cfg-tacacs.html?dtid=osscdc000283

Cisco. (2019). *Cisco Nexus 5000 Series NX-OS Software Configuration Guide*. Cisco. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/sec_tacacsplus.html#57009

Cisco. (2020). *Guía de Cisco para fortalecer los dispositivos Cisco IOS*. Cisco. https://www.cisco.com/c/es_mx/support/docs/ip/access-lists/13608-21.html

Colombo, M., Valeije, S. N., & Segura, L. (2015). Problemas y desventajas que impiden la implementación nativa de Single Sign On basado en Kerberos en sistemas Linux. *2015 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, 885-889. https://doi.org/10.1109/Chilecon.2015.7404677

Cristescu, G.-C., Croitoru, V., & Sorici, V. (2016). Implementing an AAA-RADIUS solution based on legacy authentication protocols. *2016 12th IEEE International Symposium on Electronics and Telecommunications (ISETC)*, 75-80. https://doi.org/10.1109/ISETC.2016.7781061

Cuzme, F. G., & Bosmediano, C. P. (2017). Administración y gestión de usuarios para acceso a la red inalámbrica de la Facultad de Ingeniería en Ciencias Aplicadas basado en el Protocolo 802.1x. *Universidad Técnica del Norte*, 8. http://repositorio.utn.edu.ec/handle/123456789/7127

Dafonte, P., & Pallardó, C. (2015). RADIUS: Seguridad en Sistemas de Información. En *RADIUS: Seguridad en Sistemas de Información*. https://doi.org/10.29057/xikua.v3i5.1279

Dahm, T., Ota, A., Medway Gash, D. C., Carrel, D., & Grant, L. (2020). RFC 8907 - The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol. *Internet Engineering Task Force (IETF)*. https://www.rfc-editor.org/info/rfc8907

Dayanand, L., Nida, K., Sahana, D., Brahmananda, S., & Madhurya, J. (2020). Kerberos: Security Analysis of Authentication protocol. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(5), 7569-7575. https://doi.org/10.30534/ijatcse/2020/94952020

De León, A. (2019, mayo 22). *Windows Server: ¿Qué es? Características, Ventajas y Desventajas*. HOSTING DIARIO. https://hostingdiario.com/windows-server/

De Luz, S. (2021). *Descubre para qué sirve un servidor RADIUS y su funcionamiento*. Redes Zone. https://www.redeszone.net/tutoriales/servidores/que-es-servidor-radius-funcionamiento/

El Comercio. (2020, agosto 17). Perú fue blanco de más de 613 millones de intentos de ciberataques en el primer trimestre. *El Comercio*. https://elcomercio.pe/economia/peru/ciberataques-peru-fue-blanco-de-mas-de-613-millones-de-intentos-de-ciberataques-en-el-primer-trimestre-ciberdelincuencia-fortinet-covid-19-redes-sociales-wi-fi-ncze-noticia/

El Peruano. (2020). Tendencias de ciberseguridad para el 2021. *El Peruano*. https://elperuano.pe/noticia/109658-tendencias-de-ciberseguridad-para-el-2021

España, C. (2018). *¿Qué es Wireshark? Así funciona la nueva tendencia esencial en seguridad*. CSO España. https://cso.computerworld.es/tendencias/que-es-wireshark-asi-funciona-la-nueva-tendencia-esencial-en-seguridad

Espinoza, E. (2018). Desarrollo e implementación de un sistema de control de acceso a redes inalámbricas mediante RADIUS [Universidad Mayor de San Marcos]. En *Universidad Nacional Mayor de San Marcos*. https://hdl.handle.net/20.500.12672/10018

Fajardo, V., Arkko, J., Loughney, J., & Zorn, G. (2012). RFC 6733 - Diameter Base Protocol. *Internet Engineering Task Force (IETF)*. http://www.rfc-

editor.org/info/rfc6733.

Fortinet. (s. f.). *What Is the RADIUS Protocol?* FORTINET. Recuperado 26 de enero de 2021, de https://www.fortinet.com/resources/cyberglossary/radius-protocol

Fortinet. (2020). *Fortinet | Threat Intelligence Insider LATAM*. Fortinet. https://www.fortinetthreatinsiderlat.com/en/Q2-2020/PE/html/trends#trends_position

Freeradius. (2018). *Sobre nosotros | Documentación Freeradius*. FREERADIUS. https://freeradius.org/about/

García, F. (2013). Sistema de transporte de datos. *Redes Inalámbricas*, 1-54. http://index-of.co.uk/REDES/wlan.pdf

Gestión. (2020a). ¿Cómo evitar un ataque cibernético en un entorno más digitalizado? *Gestión*. https://gestion.pe/tecnologia/como-evitar-un-ataque-cibernetico-en-un-entorno-mas-digitalizado-noticia/

Gestión. (2020b). Microsoft detecta ciberataques de Rusia y China vinculados a campaña electoral en EE.UU. *Gestión*. https://gestion.pe/economia/empresas/microsoft-detecta-ciberataques-de-rusia-y-china-vinculados-a-campana-electoral-en-eeuu-noticia/

Gestión. (2020c, septiembre 16). Hasta junio se registraron más de 600 millones de ciberataques en Perú. *Gestion*. https://gestion.pe/economia/empresas/hasta-junio-se-registraron-mas-de-600-millones-de-ciberataques-en-peru-noticia/

Gestión. (2020d, diciembre 11). Ciberseguridad en el Perú: ¿Qué tan preparados estamos para enfrentar la ciberdelincuencia? *Gestión*. https://gestion.pe/publirreportaje/ciberseguridad-en-el-peru-que-tan-preparados-estamos-para-enfrentar-la-ciberdelincuencia-noticia/

Gestión. (2021). Phishing, el ciberataque que más se incrementó en el país debido a pandemia. *Gestión*. https://gestion.pe/tecnologia/phishing-el-ciberataque-que-mas-se-incremento-en-el-pais-debido-a-pandemia-noticia/

Ghilen, A., Azizi, M., & Bouallegue, R. (2015). Integration and formal security analysis of a quantum key distribution scheme within CHAP protocol. *2015 IEEE/ACS 12th International Conference of Computer Systems and*

Applications (AICCSA), 1-7. https://doi.org/10.1109/AICCSA.2015.7507129

Gómez, L. (2007). Interoperabilidad en los Sistemas de Información Documental (SID): la información debe fluir. *Códice*, *1*. https://core.ac.uk/download/pdf/290487285.pdf

González, A., Beltrán, D., & Fuentes, E. (2016). Propuesta de protocolos de seguridad para la red inalámbrica local de la Universidad de Cienfuegos. *Revista Científica Multidisciplinar de la Universidad de Cienfuegos*, *8*, 8. http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S2218-36202016000400017&lng=es&nrm=iso

González, P. (2013). *Las tecnologías Triple A (Parte II de III)*. Flu Project. https://www.flu-project.com/2013/12/las-tecnologias-triple-parte-ii-de-iii.html

González, P. (2014). *Las tecnologías Triple A (Parte III de III)*. Flu Project. https://www.flu-project.com/2014/01/las-tecnologias-triple-parte-iii-de-iii.html

Gutiérrez, J. (2020, agosto 17). Recibió México más de 3 mil millones de ciberataques: Fortinet. *La Jornada*. https://www.jornada.com.mx/ultimas/economia/2020/08/17/recibio-mexico-mas-de-3-mil-millones-de-ciberataques-fortinet-6354.html

Hacom. (s. f.). *Diameter Interworking Function*. Hacom. Recuperado 6 de febrero de 2021, de https://www.hacom-tech.com/diameter-interworking-function/

Hernández, G. (2020). *Conociendo el concepto de AAA en el ámbito de la seguridad informática.* Comunidad Huawei Enterprise. https://forum.huawei.com/enterprise/es/conociendo-el-concepto-de-aaa-en-el-ámbito-de-la-seguridad-informática/thread/601036-100233

Herramientas Web. (s. f.). *Protocolos de transporte*. Herramientas Web para la enseñanza de protocolos de comunicación. Recuperado 28 de enero de 2021, de https://neo.lcc.uma.es/evirtual/cdd/tutorial/transporte/protrans.html

Ibáñez, J., & López, F. (2017). Autenticación para acceso a datos distribuidos basado en Kerberos. *Universidad Autónoma Metropolitana-Cuajimalpa (UAM-C)*, 10. https://www.researchgate.net/publication/339207167_Autenticacion_para_acc

eso_a_datos_distribuidos_basado_en_Kerberos

IBM. (s. f.). *Soporte del mecanismo de autenticación Kerberos (KRB5) para la seguridad*. IBM. Recuperado 9 de febrero de 2021, de https://www.ibm.com/support/knowledgecenter/es/SS7K4U_9.0.5/com.ibm.websphere.zseries.doc/ae/csec_kerb_auth_explain.html

IBM. (2015). *Cifrado*. IBM. https://www.ibm.com/docs/es/elm/6.0?topic=information-encryption

Instituto de Tecnología de Massachusetts. (s. f.). *Kerberos: el protocolo de autenticación de red*. Instituto de Tecnología de Massachusetts. Recuperado 25 de septiembre de 2020, de https://web.mit.edu/kerberos/#what_is

Instituto Superior de Ciberseguridad. (2018). *Kali Linux ¿Por qué descargar y cómo utilizarlo?* Instituto Superior de Ciberseguridad. https://isciberseguridad.es/kali-linux-descargar-instalar/

ITCA FEPADE. (s. f.). *Kerberos*. ITCA FEPADE. Recuperado 27 de enero de 2021, de https://virtual.itca.edu.sv/Mediadores/cms/u94_kerberos.html

Kali. (2021). *¿Qué es Kali Linux?* Kali. https://www.kali.org/docs/introduction/what-is-kali-linux/

Kaspersky. (2018). *¿Qué es el cifrado de datos?* Kaspersky. https://latam.kaspersky.com/resource-center/definitions/encryption

Kinsinger, F. S. (2009). Beneficence and the professional's moral imperative. *Journal of Chiropractic Humanities*, *16*(1), 44-46. https://doi.org/10.1016/j.echu.2010.02.006

LDAP. (2021). *LDAP*. LDAP. https://ldap.com/learn-about-ldap/

López, A. (2015, febrero 5). *Protocolos AAA y control de acceso a red: Radius*. INCIBE-CERT. https://www.incibe-cert.es/blog/protocolos-aaa-radius

Mamani, L. (2019). Diseño e implementación de un sistema de administración, autenticación y control en el estándar 802.11 en el Centro de Comunicaciones de la Universidad Nacional del Altiplano [Universidad Nacional del Altiplano]. En *Universidad Nacional del Altiplano*.

http://repositorio.unap.edu.pe/handle/UNAP/11860

Medway Gash, D. C., Carrel, D., & Grant, L. (2020). RFC 8907: The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol. *Internet Engineering Task Force (IETF)*. https://www.rfc-editor.org/info/rfc8907

Millán, R. (2017). Qué es DSR (Diameter Signaling Router). *BIT*, 2-4. https://www.ramonmillan.com/documentos/diametersignalingrouter.pdf

MIT Kerberos. (2021). *Kerberos: el protocolo de autenticación de red*. MIT Kerberos. https://web.mit.edu/kerberos/#what_is

Network Radius. (s. f.). *The RADIUS Protocol*. networkradius.com. Recuperado 20 de enero de 2021, de https://networkradius.com/doc/current/introduction/RADIUS.html

Network RADIUS SARL. (2014). Chapter 1 - Introduction. *THE FREERADIUS TECHNICAL GUIDE*.

Neuman, C., Yu, T., Hartman, S., & Raeburn, K. (2005). *RFC 4120: The Kerberos Network Authentication Service V5,* . https://tools.ietf.org/html/rfc4120

Optical Networks. (2019). *¿Qué es la red MPLS y cómo funciona?* Optical Networks. https://www.optical.pe/blog/que-es-una-red-mpls/

Oracle. (2010). *Algoritmos de autenticación y cifrado en IPsec (Guía de administración del sistema: servicios IP)*. Oracle. https://docs.oracle.com/cd/E19957-01/820-2981/ipsec-ov-11/index.html

Pacyna, P., & Chrabaszcz, R. (2016). Evaluation of EAP re-authentication protocol. *2016 17th International Telecommunications Network Strategy and Planning Symposium (Networks)*, 45-49. https://doi.org/10.1109/NETWKS.2016.7751151

Pérez, E. (2019). *Kerberos (I): ¿Cómo funciona Kerberos? - Teoría*. TARLOGIC. https://www.tarlogic.com/es/blog/como-funciona-kerberos/

Plasencia, L. (2013). Servidor AAA para validación y control de acceso de usuarios hacia la infraestructura Networking de un ente del Ministerio de Defensa Nacional. [Universidad Técnica de Norte]. En *Universidad Técnica del Norte*.

http://repositorio.utn.edu.ec/handle/123456789/994

Pradeep, R., Sunitha, N. ., Ravi, V., & Verma, S. (2019). Formal Verification of Authentication and Confidentiality for TACACS+ Security Protocol using Scyther. *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1-6. https://doi.org/10.1109/ICCCNT45670.2019.8944623

Prakash, A., & Kumar, U. (2018). Authentication Protocols and Techniques A Survey. *International Journal of Computer Sciences and Engineering*, *6*(6), 8. https://doi.org/10.26438/ijcse/v6i6.10141020

Prensa Latina. (2020, agosto 23). Más de 600 millones de ciberataques registra Panamá en 2020. *ElPaís.cr*. https://www.elpais.cr/2020/08/23/mas-de-600-millones-de-ciberataques-registra-panama-en-2020/

Raffino, M. (2020, julio). *Autonomía*. Concepto.de. https://concepto.de/autonomia/

Raffino, M. (2021, enero 15). *Justicia*. Concepto.de. https://concepto.de/justicia/

Ravi, V., Sunitha, N. ., Pradeep, R., & Verma, S. (2017). Formal methods to verify authentication in TACACS+ protocol. *2017 2nd International Conference On Emerging Computation and Information Technologies (ICECIT)*, 1-4. https://doi.org/10.1109/ICECIT.2017.8453431

Salazar, J. (2016). Redes Inalámbricas. En *Techpedia*. http://techpedia.fel.cvut.cz/es/single/?objectId=9

Singh, A., Kumar, S., Agarwal, M., & Nandi, S. (2016). Survey and analysis of Modern Authentication system. *2016 International Conference on Accessibility to Digital World (ICADW)*, 51-56. https://doi.org/10.1109/ICADW.2016.7942512

SoftTrader. (2021). *Todo lo que deben saber sobre Windows Server 2016 (+ nuevas funciones)*. SOFTTRADER. https://softtrader.es/blog-microsoft/todo-lo-que-deben-saber-sobre-windows-server-2016-nuevas-funciones/

Spitzer, N. (2015). *¿Son RADIUS y TACACS + alguna vez permitidos en FIPS 140-2 escenarios compatibles?* it-swarm-es. https://www.it-swarm-es.com/es/cisco/son-radius-y-tacacs-alguna-vez-permitidos-en-fips-140-2-

escenarios-compatibles/l958451464/

Tafur, C., & Chavez, J. (2018). Análisis de protocolos de protección de redes inalámbricas Wi-Fi para la detección de vulnerabilidades frente a posibles ataques que atenten contra la seguridad de la información [Universidad Señor de Sipán]. En *Universidad Señor de Sipán*. http://repositorio.uss.edu.pe/handle/uss/5374

TechLibrary. (2020). *Configuración del orden de autenticación de Junos OS para RADIUS, TACACS + y autenticación de contraseña local*. Juniper Networks. https://www.juniper.net/documentation/es/junos/topics/task/configuration/authentication-order-authentication-methods-configuring.html

Thorsten, D., Andrej, O., Douglas, M., Carrel, D., & Lol Grant. (2017). *The TACACS+ Protocol*. Internet Engineering Task Force. https://tools.ietf.org/id/draft-ietf-opsawg-tacacs-07.html

Trujillo, H. (2020). *Fase 1 Protocolos de Control y Señalización*. Scribd. https://es.scribd.com/document/534067672/Fase-1-Protocolos-de-Control-y-Senalizacion

Tschofenig, H., Decugis, S., Mahoney, J., & Korhonen, J. (2019). Diameter. En *Wiley*. Wiley. https://doi.org/10.1002/9781118875889

Ubuntu. (2021). *Ubuntu*. Ubuntu. https://ubuntu.com/about

Universidad de Alicante. (2015). Sistemas Operativos. *Universidad de Alicante*.

Virtualbox.org. (2021). *VirtualBox*. VirtualBox. https://www.virtualbox.org/

Wireshark. (2021). *Wireshark*. https://www.wireshark.org/

Zerón, A. (2019). Beneficencia y no maleficencia. *Revista de la Asociación Dental Mexicana*, *76*(6), 306-307. https://www.medigraphic.com/cgi-bin/new/resumen.cgi?IDARTICULO=90445

Zhang, J., Guo, Y., Chen, Y., & Ma, J. (2015). Research of AAA messages Based on 802.1x authentication. *2015 IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 618-621. https://doi.org/10.1109/IAEAC.2015.7428627

ColloQUIUM
Editorial - Centro de Formación

N: 978-9942-600-42-4