UNIVERSIDAD TÉCNICA DE COTOPAXI

DIRECCIÓN DE POSGRADO

MAESTRÍA EN SISTEMAS DE LA INFORMACIÓN

MODALIDAD: PROPUESTA METODOLÓGICA Y TECNOLÓGICA AVANZADA

Título:

Marco de trabajo para validación y evaluación de la implementación de protocolos de seguridad IPsec en el proyecto EcuCiencia en la Universidad Técnica de Cotopaxi.

Trabajo de titulación previo a la obtención del título de Magíster en Sistemas de Información

Autor:
Robinson Damián Malliquinga Guzmán
Tutor:
Mgs. Jorge Bladimir Rubio Peñaherrera

LATACUNGA – ECUADOR

2021

APROBACIÓN DE TUTOR

En mi calidad de Tutor del trabajo de Titulación “Marco de trabajo para validación y evaluación de la implementación de protocolos de seguridad IPsec en el proyecto EcuCiencia en la Universidad Técnica de Cotopaxi.” presentado por Malliquinga Guzmán Robinson Damián, para optar por el Título de Magister en Sistemas de Información.

CERTIFICO

Que dicho trabajo de investigación ha sido revisado en todas sus partes y se considera que reúne los requisitos y méritos suficientes pare ser sometido a la presentación para la valoración por parte del tribunal de lectores que se designe y su exposición y respectiva defensa.

Latacunga, febrero, 12, 2021

……..

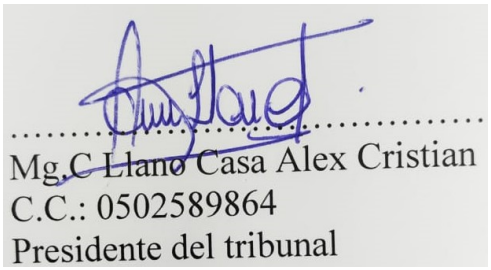
M.Sc Jorge Bladimir Rubio Peñaherrera

C.C.: 0502222292

APROBACIÓN TRIBUNAL

El trabajo de Titulación: Marco de trabajo para validación y evaluación de implementación de protocolos de seguridad IPsec en el proyecto EcuCiencia en la Universidad Técnica de Cotopaxi, ha sido revisado, aprobado y autorizado su impresión y empastado, previo a la obtención del título de Magíster en Sistemas de Información; el presente trabajo reúne los requisitos de fondo y forma para que el estudiante pueda presentarse a la exposición y defensa.

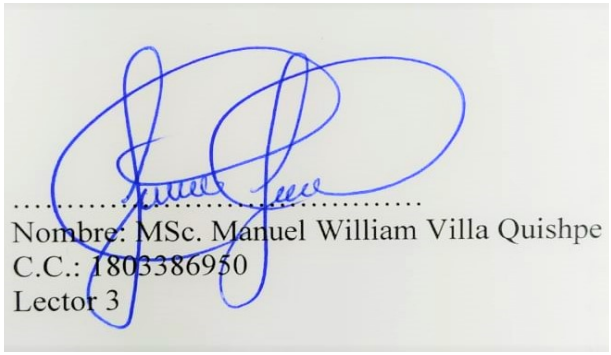
Latacunga, febrero, 12, 2021



……
Mg.C Llano Casa Alex Cristian
C.C.: 0502589864
Presidente del tribunal

Firmado electrónicamente por:
GUSTAVO
RODRIGUEZ
BARCENAS

……
Nombre: PhD. Gustavo Rodríguez Bárcenas
C.C.: 1757001357
Lector 2



……
Nombre: MSc. Manuel William Villa Quishpe
C.C.: 1803386950
Lector 3

DEDICATORIA

A mis padres por guiarme por el buen camino, los cuales me han inculcado la humildad, paciencia y la sabiduría para poder salir adelante con fuerza y perseverancia para no desmayar en los problemas que se presentan y se presentaran ensenándome que no puedo desfallecer por más difícil que se torne a su vez brindándome un apoyo incondicional en todas mis decisiones.

A mi novia, la cual me ha brindado un gran apoyo, consejos y a su vez una gran paciencia, sabiéndome escuchar y darme sus palabras de aliento para poder salir adelante y seguir esforzándome más a cada paso que daba no solo en mis estudios si no también en mi vida.

Damián

AGRADECIMIENTO

Agradezco a Dios, quien me ha llenado de bendiciones en todo este tiempo pues con su infinito amor me ha dado muchas oportunidades para salir a delante y poder escalar un peldaño más en mi meta profesional.

A mis padres Fernando y María, expreso mis más sinceros agradecimientos, pues gracias al cariño y a todo su esfuerzo e infinita paciencia demostrada en estos años he logrado ver la perseverancia y constancia que me han infundado un profundo respeto por lo cual estoy muy orgulloso.

A mi novia Alicia por siempre darme el empuje para salir a delante, dándome palabras de aliento y llenándome de ideas que puedo usar en cada paso que doy no solo estudiantil si no también laboral.

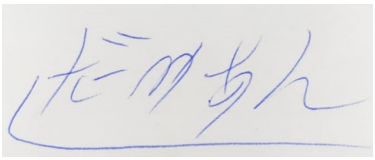
También agradezco a la Universidad Técnica de Cotopaxi y de manera especial a mi tutor de tesis el M.Sc Jorge Bladimir Rubio Peñaherrera por la paciencia, apoyo y colaboración .

Robinson Damián Malliquinga Guzmán

RESPONSABILIDAD DE AUTORÍA

Yo, Robinson Damián Malliquinga Guzmán, con CI: 0503786931, soy el autor de proyecto con el siguiente tema: Marco de trabajo para validación y evaluación de la implementación de protocolos de seguridad IPsec en el proyecto EcuCiencia en la Universidad Técnica de Cotopaxi y asumo la autoría de los contenidos y los resultados obtenidos en el presente trabajo de titulación.

Latacunga, febrero, 12, 2021



……..

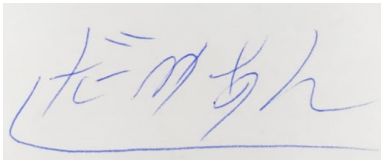
Robinson Damián Malliquinga Guzmán

C.C.: 0503786931

RENUNCIA DE DERECHOS

Yo, Robinson Damián Malliquinga Guzmán, con CI: 0503786931, autor de proyecto con el siguiente tema: Marco de trabajo para validación y evaluación de la implementación de protocolos de seguridad IPsec en el proyecto EcuCiencia en la Universidad Técnica de Cotopaxi renuncio a los derechos de autoría intelectual total y/o parcial del presente trabajo de titulación a la Universidad Técnica de Cotopaxi.

Latacunga, febrero, 12, 2021



……..

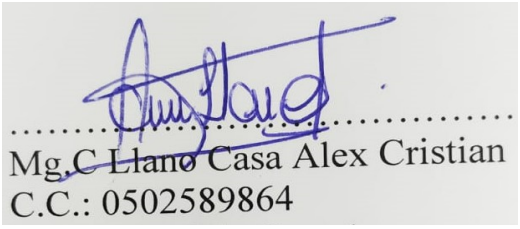
Robinson Damián Malliquinga Guzmán

C.C.: 0503786931

AVAL DEL PRESIDENTE

Yo MSc. Alex Llano, declara que el presente trabajo de titulación: Marco de trabajo para validación y evaluación de la implementación de protocolos de seguridad IPsec en el proyecto EcuCiencia en la Universidad Técnica de Cotopaxi, contiene las correcciones a las observaciones realizadas por los lectores en sesión científica del tribunal.

Latacunga, febrero, 12, 2021



UNIVERSIDAD TÉCNICA DE COTOPAXI

DIRECCIÓN DE POSTGRADO

MAESTRÍA EN SISTEMAS DE INFORMACIÓN

Título: Marco de trabajo para validación y evaluación de la implementación de protocolos de seguridad IPsec en el proyecto EcuCiencia en la Universidad Técnica de Cotopaxi.

Autor: Robinson Damian Malliquinga Guzman

Tutor: Mgs. Jorge Bladimir Rubio Peñaherrera

RESUMEN

En el presente proyecto se realiza un marco de trabajo para la validación y la evaluación de protocolos de seguridad IPSec todo esto dentro de un servidor Windows en el cual se implementa reglas de conexión segura con IPSec en las cuales proveen una conectividad que protege la información entre cliente – servidor, con esto se pretende proporcionar una seguridad para evitar robo de información que maneja el laboratorio de EcuCiencia utilizando la conexión TCP, en la cual se encapsula la información mediante ESP y un intercambio dinámico de contraseñas mediante KerberosV5. La fundamentación científico técnica es recopilada de varias fuentes primarias de información entre las cuales destacan: artículos científicos, tesis, libros, página oficial de Microsoft. Por lo cual se adaptan dos metodologías las cuales son: Metodología Top Down y la metodología para la validación y evaluación, por lo cual para evaluar dicho marco de trabajo se procede a la realización de un laboratorio de pruebas en el cual se simulará los equipos físicos que se dispone en dicho laboratorio en el cual se realiza las pruebas necesarias para la utilización de IPSec y mediante la utilización del marco de trabajo se realiza un análisis del protocolo IPSec.

PALABRAS CLAVE:

TCP, UDP, IPSec, ESP, IKE, Encriptación

UNIVERSIDAD TÉCNICA DE COTOPAXI

DIRECCIÓN DE POSTGRADO

MAESTRÍA EN SISTEMAS DE INFORMACIÓN

Title: Framework for validation and evaluation of the implementation of IPsec security protocols in the EcuCiencia project at the Technical University of Cotopaxi

Author: Robinson Damian Malliquinga Guzman

Tutor: Mgs. Jorge Bladimir Rubio Peñaherrera

ABSTRACT

In this project a framework for the validation and evaluation of IPSec security protocols is carried out within a Windows server in which secure connection rules are implemented with IPSec which provide a connectivity that protects the information between client - server, this is intended to provide security to prevent theft of information handled by the EcuCiencia laboratory using the TCP connection, in which the information is encapsulated by ESP and a dynamic exchange of passwords using KerberosV5. The scientific-technical foundation is compiled from several primary sources of information, among them: scientific articles, theses, books, Microsoft's official web page. For which two methodologies are adapted which are: Methodology Top Down and the methodology for validation and evaluation, for which to evaluate this framework we proceed to the realization of a test laboratory in which the physical equipment that is available in this laboratory will be simulated in which the necessary tests for the use of IPSec are performed and through the use of the framework an analysis of the IPSec protocol is performed.

KEYWORDS:

TCP, UDP, IPSec, ESP, IKE, Encryption

Bolívar Maximiliano Cevallos Galarza con cédula de identidad número: 0910821669 Licenciado en Ciencias de la Educación mención Inglés con número de registro de la SENESCYT: 1020-15-1372475; **CERTIFICO** haber revisado y aprobado la traducción al idioma inglés del resumen del trabajo de investigación con el título: Marco de trabajo para validación y evaluación de la implementación de protocolos de seguridad IPsec en el proyecto EcuCiencia en la Universidad Técnica de Cotopaxi de: Robinson Damian Malliquinga Guzman, aspirante a magister en Sistemas de Información

Latacunga, Julio 01, 2021

Bolívar Maximiliano Cevallos Galarza
ID 0910821669

MARCO PAUL BELTRAN SEMBLANTES

CENTRO DE IDIOMAS

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

El presente documento es realizado en base a la línea de investigación de Tecnologías de la Información y Comunicación, a su vez se trabaja simultáneamente con la sub línea de investigación la cual comprende al Diseño, implementación y configuración de redes y seguridad computacional, aplicando normas y estándares internacionales. Mediante la realización de un marco de trabajo para la validación y evaluación del protocolo de seguridad se adapta dos tipos de metodologías las cuales satisfacen y otorgan componentes necesarios para la implementación de una red segura, pues con esto se realiza un análisis en base a pruebas de validación entregando una simulación de implementación satisfactoria con respecto a la seguridad que ofrece un protocolo de comunicación segura.

En los últimos años se ha visto como las redes de comunicaciones han pasado a ser parte de nuestra vida cotidiana. Por lo tanto, a medida que pasa el tiempo, las redes de ordenadores han dejado de ser un medio de comunicación para un segmento especifico de la población, por lo cual estas pasan a ser utilizadas por parte de los ciudadanos y empresas, utilizándose para actividades que varían desde la compra electrónica, el control logístico en puertos y aeropuertos internacionales hasta las redes de laboratorios estudiantiles. Este incremento en el uso de las redes de comunicaciones ha tenido múltiples consecuencias, pudiendo destacar entre ellas el aumento de la información que fluye dentro de las mismas. En muchos casos nos encontramos con que esta información requiere mayor protección en su tránsito por las diferentes redes, ya sea mediante servicios de confidencialidad, de autodetección, encriptación, encapsulamiento, etc.… a su vez, el aumento en el uso de las redes de comunicaciones ha llevado aparejado un incremento en el tipo de dispositivos que crecen en dichas redes: desde supercomputadoras y ordenadores pertenecientes a múltiples empresas hasta teléfonos móviles, agendas personales e incluso consolas, llegando al extremo en que el termino de “redes de computadores” ha sido desplazado por el de “redes de comunicaciones”.

En problema que se ha detectado dentro del laboratorio de EcuCiencia de la Universidad Técnica de Cotopaxi es que no disponen de un protocolo de comunicación segura, ni reglas de seguridad adecuadas para la protección de los datos que se manejan dentro de dicho laboratorio, por lo cual en términos de seguridad de la información la red interna actual dentro de dicho laboratorio no cumple con las características de comunicación segura básica, lo cual genera problemas en la seguridad de la información.

Para la formulación del problema se realiza una pregunta la cual se plantea lo siguiente: ¿Cómo elegir un protocolo de seguridad para proporcionar una mejora de la integridad de los datos para el proyecto de EcuCiencia de la Universidad Técnica de Cotopaxi?

Para lo cual el Objetivo General que se formula es: Definir un marco de trabajo a partir de un prototipo para generar datos óptimos en la implementación de protocolos de seguridad.

Para alcanzar al cumplimiento del objetivo antes mencionado se propone la especificación de los objetivos específicos los cuales son: Recopilar información bibliográfica mediante publicaciones científicas y medios digitales de fuentes confiables, para poder desarrollar un mejor conocimiento sobre el cómo seleccionar el protocolo adecuado.

Realizar un análisis las especificaciones de los protocolos de seguridad para identificar los aspectos críticos a la hora de establecer el consentimiento o la no aplicación con respecto a lo descrito en el estándar para su implementación en EcuCiencia.

Implementar en base a los resultados de las pruebas realizadas en conformidad a un estándar en el cual se muestre las capacidades y limitaciones de interoperabilidad de la implementación del protocolo de seguridad en base a las diferentes opciones.

Para dicho cumplimiento de los objetivos específicos es necesario detallar las tareas a realizar de cada uno de ellos para lo cual se detallan en la siguiente tabla:

Tabla 1. Tabla de tareas

Objetivos Específicos	**Actividades**
Recopilar información bibliográfica mediante publicaciones científicas y medios digitales de fuentes confiables, para poder desarrollar un mejor conocimiento sobre el cómo seleccionar el protocolo adecuado.	Realizar la búsqueda de información bibliográfica de primera mano en las cuales se pueda verificar la información.
Realizar un análisis las especificaciones de los protocolos de seguridad para identificar los aspectos críticos a la hora de establecer el consentimiento o la no aplicación con respecto a lo descrito en el estándar para su implementación en EcuCiencia.	Realización de pruebas para la conformidad con el estándar. Verificar las capacidades en interoperabilidad. Verificar las limitaciones en interoperabilidad.
Implementar en base a los resultados de las pruebas realizadas en conformidad a un estándar en el cual se muestre las capacidades y limitaciones de interoperabilidad de la implementación del protocolo de seguridad en base a las diferentes opciones.	Pruebas de rendimiento de los protocolos de seguridad. Análisis de los datos arrojados por las pruebas de los protocolos.

Elaborado por: El investigador

Para que el proceso sea investigativo se ha realizado acorde a etapas de los aspectos críticos del proyecto, las cuales se detalla en la siguiente tabla:

Tabla 2. Etapas de los aspectos críticos del proceso investigativo.

Etapa	Descripción
Recolección de información base, aspectos antecedentes, estado del arte.	Análisis y revisión del material bibliográfico relacionado a aspectos de seguridad de la información mediante protocolos de seguridad IPSec y el entendimiento de la teoría para el proceso de la investigación.

Entendimiento de la metodología Top Down y la metodología para la evaluación y validación.	Entender el proceso que sigue dichas metodologías para la realización de un marco de trabajo que cubra las necesidades de la implementación.
Adaptación de las metodologías a un marco de trabajo.	Adaptación de las etapas más importantes de cada metodología para poder utilizar un marco de trabajo ágil para la implementación de un protocolo IPSec.
Realización de las pruebas.	Realizar pruebas de rendimiento para saber si dicho protocolo asegura la información en la comunicación.
Análisis y conclusiones en base a las pruebas sobre el protocolo IPSec.	Realización del análisis sobre la protección que otorga el protocolo IPSec.

Elaborado por: El investigador

Debido al rápido progreso de la tecnología las áreas de seguridad de la información están convergiendo rápidamente y las diferencias entre juntar, transportar, almacenar y procesar información desaparecen con rapidez. Por lo cual en base a una investigación y análisis de desempeño de las tecnologías Ipsec se quiere desarrollar un marco de trabajo en el que nos permita realizar una implementación en base a las pruebas realizadas para así tener una visión más puntual sobre el antes de la protección y después de la implementación del protocolo al momento de desarrollar un proyecto de redes de datos y telecomunicaciones.

Actualmente se maneja el transporte de IPv4 inseguro, refiriéndonos a la palabra inseguro como susceptible de ser copiado y en Ipsec se maneja transporte Ipv4 seguro sobre una plataforma insegura; el desempeño de los servicios depende de las tecnologías de red de acceso que ofrecen los proveedores a nivel WAN, la integridad y la privacidad del tráfico Ipv4 que pasa por las infraestructura, redes y equipos externos están siempre ligadas a los convenios y acuerdos de confidencialidad que ofrecen los proveedores de servicio de internet.

Sin embargo, la manera en que la información siga siendo vulnerable en cuanto a la privacidad se debe a que no existe ningún tipo de encriptación en el transporte de la información, teniéndose teóricamente un hueco en la seguridad.

Para el presente proyecto es determinar un marco de trabajo el cual permita una implementación confiable mediante Ipsec, para lo cual se busca obtener una arquitectura personal que permita generar una alta calidad en la seguridad que responda a todas las necesidades de los usuarios.

Finalmente, el propósito de esta investigación es implementar un protocolo de seguridad al proyecto de EcuCiencia que se encuentra en la Universidad Técnica de Cotopaxi proveyendo de una arquitectura más segura que se adapte en gran medida a las necesidades de dicho proyecto y así brindar un apoyo al mejoramiento en la protección de la información.

Para complementar es necesario especificar el marco de trabajo el cual está basado en adaptar dos metodologías siendo la primera la Metodología Top – down para el diseño de redes conjuntamente con la Metodología de validación y evaluación, estas metodologías son usadas para la gestión del proceso de la implementación del protocolo IPSec, todos estos aspectos se verificaran y validaran utilizando el diseño experimental lo cual permitirá garantizar la propuesta y la implementación adecuada para la protección de la comunicación entre la red.

CAPÍTULO I

FUNDAMENTACIÓN TEÓRICA

Antecedentes

Como antecedentes para la realización de este proyecto, se ha revisado el trabajo realizado por "Brito Ayala Juan Carlos" en su trabajo de titulación con el tema de: "Estudio Comparativo Entre Ipsec Y Mpls Para Redes Privadas Virtuales (Vpn) [1]", en la cual se realiza un marco comparativo para el análisis del desempeño que tienen las redes con la utilización de Ipsec y MPLS, a su vez revisando y comparando las ventajas y desventajas de cada uno respectivamente.

A su vez se revisa el proyecto realizado por "Juan Sebastián Romero Chafla" en su trabajo de titulación con el tema de: "Análisis comparativo del rendimiento del tráfico en redes MPLS con túneles IPSec en entornos IPv6". En dicho proyecto se busca definir datos comparativos en los cuales se muestra el rendimiento con un protocolo IPv6 implementando tuéneles Ipsec. A su vez dicho proyecto se enfoca en la simulación de redes con el fin de obtener resultados para la realización de un análisis comparativo.

Conjuntamente para este proyecto se adapta la metodología Top – Down para el diseño de la red simultáneamente con la adaptación de la "Metodología para la validación y evaluación remota de implementaciones de protocolos de seguridad. Aplicación a la arquitectura IPSec" propuesta por Antonio Izquierdo Manzanares. Las dos metodologías son adaptadas para la realizar un marco de trabajo el cual permita probar el rendimiento de la red y la protección de datos que esta ofrece a la misma.

Fundamentación epistemológica

EcuCiencia

"Creado para potenciar comunidades colectivas de conocimientos e informar sobre el Proyecto para el establecimiento de una Red de Estudios Cienciométricos en las Universidades de la Zona 3 del Ecuador." [2]

“Dar a conocer la producción científica de estas universidades y visualizar los investigadores que aportan de una manera u otra a la ciencia en el Ecuador es uno de los propósitos del proyecto.” [2]

Modos de transporte de datos

Para tener un amplio conocimiento sobre los modos de transporte de la información en las redes de datos se adquiere conocimientos sobre el modelo OSI, pues a partir de este modelo se basan todos los sistemas de telecomunicaciones y sus respectivas redes de datos.

Modelo OSI

“A finales de la década de los setenta, la organización nacional para la normalización ISO inicio a desarrollar un modelo para la conexión en red, a este modelo se le denomino Modelo de referencia de interconexión de sistemas abiertos, bautizado con el nombre de Open Systems Interconnection Reference Model, por sus siglas en ingles OSI. Este modelo ofrece un marco de trabajo conceptual desde 1984 [3]”.

“OSI es un modelo basado en niveles para el diseño de sistemas de red. Este modelo además permite la interconexión de sistemas abiertos, o lo que es lo mismo, permite que dos sistemas diferentes se puedan comunicar independientemente de su arquitectura. [4]”

“El modelo OSI (Open System interconnections) fue propuesto por la ISO, en el mercado existía muchas arquitecturas de protocolos, unas abiertas y otras propietarias, pero todas diferentes. La torre OSI pretendía ser un modelo básico de referencia, un marco para el desarrollo de estándares que permiten la interoperabilidad completa. [5]”.

Entendida la definición del modelo OSI, se presenta las siete capas o niveles que existen dentro de dicho modelo los cuales son detallados a continuación.

Capa 1 – Capa física

“Transmite una cadena de bits no estructurados sobre un medio físico. Define las características físicas del sistema cableado, abarca también los métodos de red disponibles, incluyendo Token Ring, Ethernet y ArcNet. [5]”.

Esta primera capa es la que se encarga de la transmisión de información a través del medio físico del emisor- receptor, ya que en dicha capa debe ser posible él envió de datos a través de un canal de comunicación como lo son cable UTP, fibra óptica e incluso aire y a su vez que puedan llegar a su destino de manera correcta.

Capa 2 – Capa de enlace de datos

"Proporciona un servicio similar al nivel físico, mejorando las características de fiabilidad de la transmisión. Añade bits adicionales a los que forman el mensaje para poder detectar errores de transmisión en el mismo y poder pedir su retransmisión. [5]".

La transmisión de los datos se lleva a cabo en la primera capa la cual es el nivel físico, por lo tanto, en dicho nivel no puede proporcionar ningún mecanismo para asegurar que los datos que son enviados desde el emisor lleguen sin ningún tipo de error al receptor, por lo cual la capa de enlace de datos se encarga de proporcionar que la transmisión de la información sea fiable.

Capa 3 – Capa de red

"Controla el funcionamiento de la subred, decidiendo qué ruta de acceso física deben tomar los datos basándose en las condiciones de red, la prioridad de servicio y otros factores. [5]"

Esta capa es encargada de todas las funciones necesarias para que la información sea encaminada correctamente en caso de que el emisor y el receptor estén en redes diferentes.

Capa 4 – Capa de transporte

"El nivel de transporte garantiza que los mensajes se entregan sin errores, en secuencia y sin pérdidas o duplicaciones. Libera a los protocolos de nivel superior de cualquier problema con la transferencia de datos entre ellos y sus colegas. La función principal de este nivel consiste en asegurar la calidad de transmisión entre los terminales que utilizan la red, lo que implica recuperar errores, ordenar correctamente la información, ajustar la velocidad de transmisión de la información (control de flujo de datos), etc. [5]"

Esta capa se encarga de entregar de manera completa y sin errores la información o datos que circulen dentro de la red hasta el destino esperado, esto realizado conjuntamente con las capas anteriores.

Capa 5 – Capa de sesión

El nivel de sesión permite organizar el intercambio de datos entre procesos estableciendo una sesión entre cada uno de los procesos que se ejecutan en diferentes estaciones, ya que esta capa asume que dos puntos extremos disponen de la misma categoría, esto ayuda a la comunicación entre cliente – servidor.

Capa 6 – Capa de presentación

"El nivel de presentación da formato a los datos que deberán presentarse al nivel de aplicación. Se puede ver como el traductor de la red. Este nivel puede traducir datos de un formato utilizado por el nivel de aplicación en un formato común en la estación emisora, y después convertir el formato común a un formato que se sabe que la capa de aplicación en la estación receptora. [5]"

Esta capa se encarga de encerrar las capas inferiores en el formato de los datos para el nivel de aplicación, ya que en este nivel tiene que ver con la semántica de la información que puede ser intercambiada entre un emisor – receptor.

Capa 7 – Capa de aplicación

La capa de aplicación actúa como una ventana para que los usuarios y los procesos de aplicaciones tengan acceso a servicios de red, en otras palabras, se interactúa netamente con la red pues esta es la capa más alta del modelo OSI.

Paquetes de arquitectura TCP/IP

"El término genérico "TCP/IP" usualmente significa cualquier cosa y todo con referencia a los protocolos específicos TCP e IP. Pueden incluir otros protocolos, aplicaciones e incluso los medios de red. [6]" Se redactan los siguientes ejemplos de protocolos: UDP, ARP e ICMP, las aplicaciones que trabajan con estos protocolos son los siguientes: TELNET, FTP y RPC.

"Se trata de un conjunto de protocolos, aunque los más conocidos sean TCP (nivel de transporte) e IP (nivel de red). Las aplicaciones que corren sobre TCP/IP no

tienen que conocer las características físicas de la red en la que se encuentran; con esto, se evita el tener que modificarlas o reconstruirlas para cada tipo de red. [5]"

Por cada capa del modelo OSI, existen las unidades de datos del protocolo llamadas PDU, las cuales son utilizadas para el intercambio de la información entre las diferentes capas. Por lo cual se presentan a continuación:

PDU de capa 1 – Bit

"El PDU correspondiente a la capa 1 es el bit, representación digital de 1 o 0 binario, consiste en una secuencia de bits de preámbulo, una cabecera y de un PDU de capa superior conocido como PDU de capa 2 llamados trama. [1]"

PDU de capa 2 – Trama

"El PDU correspondiente a la capa 2 es la trama, al igual que en la capa 1 consta de una cabecera o header seguida de un PDU de capa 3 llamado paquete y un valor de secuencia de corrección de errores o checksum. [1]"

PDU de capa 3 – Paquete

"El PDU correspondiente a la capa 3 es el paquete, al igual que en las anteriores capas consta de una cabecera o header seguida de un PDU de capa 4 llamado segmento. [1]"

PDU de capa 4 – Segmento

"El PDU correspondiente a la capa 4 es el segmento, al igual que en las capas anteriores consta de una cabecera o header seguida de un PDU de capa superior. Como se puede observar en la figura 1 desde la capa 1 hasta la capa 7 existe la misma operación o funcionalidad de cabecera de capa seguida del PDU de capa superior. [1]"

Protocolos de la familia TCP/IP

Un protocolo es un procedimiento estándar el cual permite la comunicación entre procesos por lo general entre una red de equipos, por lo cual dispone de un conjunto de reglas las cuales son respetadas para el envío y la recepción de datos a través de la red.

"En ocasiones se le denomina conjunto de protocolos TCP/IP, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de

Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia. Existen tantos protocolos en este conjunto que llegan a ser más de 100 diferentes, entre ellos se destacan los siguientes: [1]"

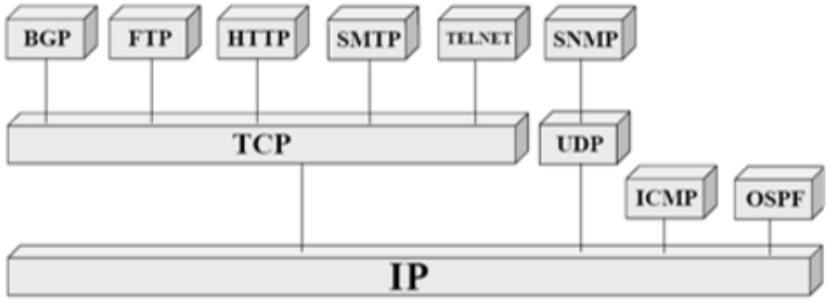


Gráfico 1 Protocolos de la familia TCP/IP
Elaborado por: CARLOS BRITO AYALA JUAN

TCP Protocolo de control de transmisión

La capa que esta sobre la capa de interredes en el modelo TCP/IP se llama usualmente capa de transporte. Esta capa está diseñada para permitir que las entidades en los nodos de origen y destino lleven a cabo una conversación, lo mismo que en la capa de transporte OSI. Aquí se definieron dos protocolos de extremo a extremo. El primero, TCP (Protocolo de Control de la Transmisión) es un protocolo confiable orientado a la conexión originada en una maquina la cual entregue sin errores en cualquier otra máquina de la red interna.

UDP Protocolo de datagramas de usuario

Este protocolo es de nivel de transporte el cual está basando en el intercambio de datagramas, pues este permite en envío de datagramas a través de la red sin que se haya establecido una conexión.

"El protocolo UDP se limita a recoger el mensaje y enviar el paquete por la red sin necesidad de establecer una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Para garantizar la llegada, el protocolo exige a la máquina de destino del paquete que envíe un mensaje. Si dicho mensaje no llega pasado un tiempo establecido, la máquina de

destino envía el mensaje de nuevo. Esto puede originar la duplicación y/o desordenación de los datagramas a su destino. [7]”

Máxima transferencia de datos

“La tasa de transferencia es la medida real del ancho de banda en un momento determinado, en una ruta específica al transmitirse un conjunto especifico de datos; por lo general, la tasa de transferencia es mucho menor que el ancho de banda máximo que el medio de trasmisión soporta. [8]”

“Cuando hablamos de máxima transferencia de datos para redes existen muchos parámetros o variables a considerar, pues existen limitaciones a nivel de hardware y protocolos que dificultan el poder obtener una fórmula para obtener este resultado. [1]”

La tasa de transferencia es determinada por diferentes factores entre los cuales se pueden destacar: Dispositivos dentro de la red, topología de la red, cantidad de usuarios dentro de la red y los tipos de datos que son transferidos.

Retardo en la transmisión

La latencia en la transmisión de datos es la suma de los retardos temporales que se producen durante la transmisión de información dentro de la red, esta latencia o retardo puede darse por diversos factores entre los cuales se detallan los más relevantes: Mal estado de los medios de transmisión, tamaño de los archivos y la cantidad de equipos que existen entre el emisor y el receptor.

Unidad máxima de transferencia de datos MTU

La unidad máxima de transferencia es un término de redes, expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse desde un computador usando un protocolo de comunicación.

La unidad de transferencia máxima de una unidad de datos transferidos en el momento de una ruta de transferencia conectada entre los dos sistemas finales e incluyendo las redes y el dispositivo de transferencia. “Ejemplos de distintos protocolos usados en internet: [1]”

- Ethernet: 1518bytes
- PPPoE:1492 bytes

- ATM (AAL5): 8190 bytes

“Para el caso de IP, el máximo valor de la MTU es 65.536 bytes. Sin embargo, ése es un valor máximo teórico, pues, en la práctica, la entidad IP determinará el máximo tamaño de los datagramas IP en función de la tecnología de red por la que vaya a ser enviado el datagrama. Por defecto, el tamaño de datagrama IP mínimo es de 576 bytes (512bytes de datos + 64 de cabeceras). Sólo pueden enviarse datagramas más grandes si se tiene conocimiento fehaciente de que la red destinataria del datagrama puede aceptar ese tamaño. En la práctica, dado que la mayoría de máquinas están conectadas a redes Ethernet o derivados, el tamaño de datagrama que se envía es con frecuencia de 1500 bytes. [1]”

Tamaño máximo de segmento MSS

“El MSS tiene gran importancia en las conexiones en bajo IP, particularmente en aplicaciones TCP. Cuando se usa el protocolo TCP para efectuar una conexión, los ordenadores que se conectan deben acordar y establecer el tamaño de la MTU que ambos puedan aceptar. El valor típico de MTU en una red puede ser, por ejemplo, 576 ó 1500 bytes. Tanto la cabecera IP como la cabecera TCP tienen una longitud variable de al menos 20 bytes. En cualquier caso, el MSS es igual a la diferencia MTU - cabecera TCP - cabecera IP. [1]”

Rendimiento (Throughput)

“En particular, el dispositivo electrónico de transmisión puede monitorear la comunicación con uno o más dispositivos electrónicos receptores, y puede calcular una métrica de rendimiento en función de la comunicación monitoreada. [9]”

“El rendimiento se define como, la relación de los datos totales que llegan a un receptor del remitente. El tiempo que toma el receptor para recibir el último mensaje se denomina rendimiento. El rendimiento, se expresa como bytes o bits por segundo (bps). Algunos factores afectan el rendimiento, tales como, si hay muchos cambios topológicos en la red, comunicaciones poico fiables entre nodos, ancho de banda limitado disponible y energía limitada. [10]”

Multi-Protocol Label Switching (MPLS)

"MPLS es una tecnología que combina diversas funciones de enrutamiento de capa 3 con las funciones de envió de capa 2, al estar ligado con protocolos que cumplen funciones específicas dentro del ámbito de red se lo llama multiprotocolo, adicionalmente esta brinda la posibilidad de interactuar con varias tecnologías de transporte de información, sea este a nivel de enlace o físico y con aplicaciones que están sobre el nivel de red. [11]"

MPLS es un método de "forwardear" paquetes a través de una red usando información contenida en etiquetas añadidas en los paquetes IP, se puede considerar un estándar IP de conmutación de paquetes del IETF RFC 3031, que trata de proporcionar algunas de las características de las redes orientadas a conexión a las redes no orientadas a conexión. MPLS soporta múltiples aplicaciones incluyendo: unicast y multicast routing, VPN, ingeniería de tráfico, Qos, etc. [1]

Componentes y características de MPLS

"En diferentes entornos las redes MPLS especifican múltiples mecanismos para manejar el tráfico de la información, por ejemplo flujos entre diferentes hardware de equipos físicos, flujos entre diferentes tecnologías e incluso flujo de información entre diferentes aplicaciones lo cual permite que se pueda proveer medios independientes y autónomos para poder manejar direcciones IP, en las etiquetas de longitud fija lo cual permite que cuando se utilice una técnica de ruteo esta pueda mantener la conmutación del paquete gracias a la facilidad de interactuar con diferentes interfaces con protocolos de ruteo. [11]"

Etiquetas MPLS

"Una etiqueta es un identificador de 32 bits que señala una FEC (Forward Equivalence Class) determinada. Generalmente la etiqueta es asignada en función de la capa de red, pero a diferencia de IP, la cual da la dirección del host propietario de los datos del paquete IP; la información que contiene la etiqueta pertenece únicamente al LSR emisor y al LSR receptor para tener una conexión al siguiente salto. [12]"

"Las etiquetas MPLS, se encuentran encapsuladas dentro de una cabecera de 32 bits que contiene información necesaria para que un router o nodo logre identificar y

enrutar el paquete hacia su destino, con lo cual se logra diferenciar un paquete hacia su destino, con lo cual se logra diferenciar un paquete en cada uno de los nodos entre diferentes FEC y determinar así el siguiente salto entre las redes MPLS. [11]"

"Las etiquetas son campos de la cabecera MPLS de longitud corta y fija (20 bits), que se añaden a los paquetes, con el fin de que estos tengan un determinado tratamiento y encaminamiento en los LSR y en los ruteadores LER que van atravesando hasta llegar a su destino. En cada uno de los equipos de comunicaciones de la red MPLS, se puede realizar los procesos de adición, de extracción o de modificación de las etiquetas de los paquetes. [1]"

Forwarding Equivalence Class (FEC)

El FEC es un identificador que permite agrupar a los paquetes, para que estos reciban un mismo tratamiento dentro de la red MPLS y puedan ser transmitidos del mismo modo.

"Una clase de envío equivalente, representa a un grupo de paquetes que comparten requerimientos comunes para el transporte de los mismos, es decir que todos los paquetes que están incluidos en este grupo contienen la misma ruta de envío hacia su destino. [12]"

"Un FEC es un conjunto de paquetes que entran en la red MPLS por la misma interfaz, reciben la misma etiqueta y por tanto circulan por un mismo trayecto. Normalmente se trata de datagramas que pertenecen a un mismo flujo. Una FEC puede agrupar varios flujos, pero un mismo flujo no puede pertenecer a más de una FEC al mismo tiempo. [12]"

"Los LSR de entrada se encargan de asociar un paquete a una FEC y se basan en muchos de los casos en la dirección de destino, el no ser así estos se basan en el origen, puertos e incluso en protocolos de servicio, es decir que cada nodo LSR construye una tabla para especificar un paquete que debe de ser enviado, esta se denomina Base de información de etiquetas LIB. [11]"

IPsec Internet Protocol Security

"IPSec está compuesto de un conjunto de estándares con los cuales dan al IP funciones de seguridad basadas en criptografía, proporciona confidencialidad, integridad y autenticidad de datagramas IP. [13]"

"Ipsec está diseñado para proporcionar seguridad inter-operable, de alta calidad, basada en criptografía, tanto para IPv4 como para IPv6. [14]"

IPsec es un protocolo que está sobre la capa del protocolo de Internet (IP). Este permite a dos o más equipos comunicarse asegurando la información que se maneja entre los mismos. La "pila de red" IPsec incluye soporte para las dos familias de protocolos, IPv4.

"IPsec (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado. [15]"

"IPsec emplea dos protocolos diferentes - AH y ESP - para asegurar la autenticación, integridad y confidencialidad de la comunicación. Puede proteger el datagrama IP completo o sólo los protocolos de capas superiores. [15]"

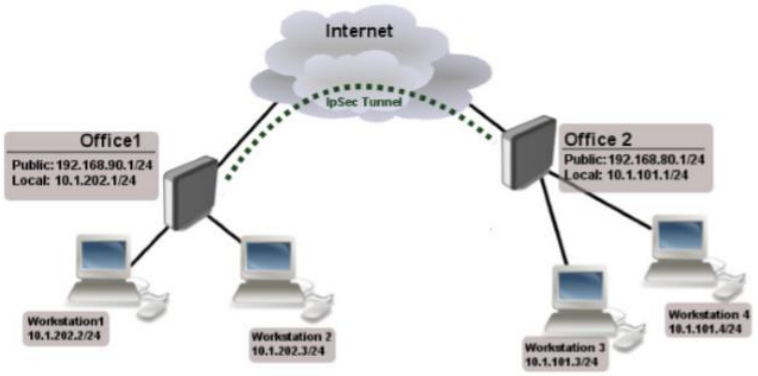


Gráfico 2 Seguridad del protocolo de internet IPsec

Elaborado por: Müller, Ing. Luis

El objetivo principal de IPSec es brindar seguridad de extremo a extremo de los equipos, lo que significa que los únicos hosts que tienen que conocer la protección de IPSec son el emisor y el receptor. "Cada equipo controla la seguridad por sí

mismo en su extremo, bajo la hipótesis de que el medio por el que se establece la comunicación no es seguro. [15]”

Estos modos se denominan respectivamente, túnel el datagrama IP se encapsula completamente dentro el protocolo IPsec. En modo transporte IPsec sólo maneja la carga del datagrama IP, insertándose la cabecera IPsec entre la cabecera IP y la cabecera del protocolo de capas superiores.

Características de Ipsec

Dentro de IPsec puede utilizar diversos protocolos y herramientas que dotan de seguridad a el tráfico de la red asegurando que la información llegue a su destino de una manera íntegra y sin ningún tipo de error. Entre las cuales se puede destacar lo siguiente:

“Encriptación: es un proceso por el cual convertimos una información perfectamente entendible en algo totalmente incomprensible. Como es lógico este proceso es reversible. Para llevarlo a cabo se necesita de algoritmos de encriptación. [16]”

“Integridad: la integridad de la información enviada es uno de los aspectos que se puede tratar con Ipsec. Comprobando la integridad de la información podemos asegurarnos de que no ha sido modificada por nadie en el trayecto a su destino. [16]”

“Autenticación: cuando existe una comunicación entre dos entidades es importante tener por seguro que el otro extremo es quien dice ser y no ser un farsante. [16]”

“Claves basadas en criptografía. Las claves cifradas, que se comparten entre los sistemas que se comunican, crean una suma de comprobación digital para cada paquete IP. Cualquier modificación del paquete altera la suma de comprobación, mostrando al destinatario que el paquete ha sido cambiado en su tránsito. Se utiliza material de claves diferente para cada segmento del esquema de protección global y se puede generar nuevo material de claves con la frecuencia especificada en la directiva de IPSec. [15]”

“Administración automática de claves. Las claves largas y el cambio dinámico de claves durante las comunicaciones ya establecidas protegen contra los ataques.

IPSec usa el protocolo Asociación de seguridad en Internet y administración de claves (ISAKMP, Internet Security Association and Key Management Protocol) para intercambiar y administrar dinámicamente claves cifradas entre los equipos que se comunican. [15]"

IPSec existe en el nivel de red, la cual proporciona seguridad automática a todos los equipos que estén dentro de una misma red y autentificados en la misma.

"Autenticación mutua. IPSec permite el intercambio y la comprobación de identidades sin exponer la información a la interpretación de un atacante. La comprobación mutua (autenticación) se utiliza para establecer la confianza entre los sistemas que se comunican. Sólo los sistemas de confianza se pueden comunicar entre sí. Los usuarios no tienen que estar en el mismo dominio para comunicar con la protección de IPSec. Pueden estar en cualquier dominio de confianza de la empresa. La comunicación se cifra, lo que dificulta la identificación e interpretación de la información. [15]"

Carga de Seguridad Encapsulada (ESP)

Protocolo Carga de seguridad de encapsulación (ESP, Encapsulating Security Payload). ESP proporciona privacidad a los datos mediante el cifrado de los paquetes IP.

"El protocolo ESP puede proporcionar cifrado sin autenticación. Esto no tiene mucho sentido en una aplicación. Protege la aplicación contra intrusos pasivos. [17]"

Este protocolo tiene como objetivo principal proporcionar confidencialidad, para lo cual se especifica en el modo de cifrar los datos que se desean enviar y como este contenido incluye un datagrama IP. A su vez este protocolo puede ser utilizado conjuntamente con el protocolo AH.

"El protocolo ESP puede asegurar la integridad del paquete empleando una HMAC y la confidencialidad empleando cifrado. La cabecera ESP se genera y añade al paquete tras cifrarlo y calcular su HMAC. La cabecera ESP consta de dos partes. [1]"

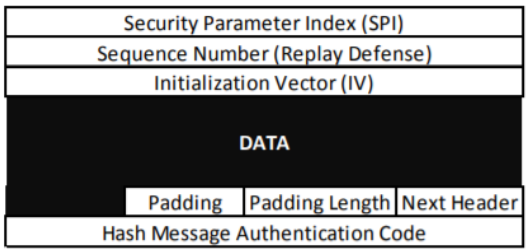


Gráfico 3 Carga de seguridad encapsulada

Elaborado por: BRITO AYALA JUAN CARLOS

Protocolo de Intercambio de Internet IKE

"Este protocolo hibrido cuyo propósito es negociar y proveer autenticación de claves para las asociaciones de seguridad de una manera protegida por lo tanto este no es un protocolo que viene incluido en IPSec, si no que ayuda al manejo de claves. [18]"

El protocolo IKE resuelve el problema más importante del establecimiento de comunicaciones seguras: la autenticación de los participantes y el intercambio de claves simétricas. El protocolo IKE emplea el puerto 500 UDP para su comunicación.

Este protocolo establece un vínculo de cifrado mediante el cual la conexión de 2 nodos, es en este proceso donde se negocial las asociaciones de seguridad con IPSec emplea algoritmos de cifrado y encriptación en ambos extremos de la conexión de la seguridad Ipsec (emisor-receptor) y emplea proceso con las asociaciones de seguridad de ISAMP, establece, negocia y autentica.

Debilidades del protocolo IKE

La debilidad más prominente que se puede mencionar con respecto a dicho protocolo es la compatibilidad con las plataformas limitadas por lo cual dicho protocolo no dispone de implementación mediante código abierto, lo cual hace que sea fácil de bloquear el puerto 500 UDP que este protocolo maneja.

Protocolo de cabecera de autenticación AH

"AH proporciona integridad sin conexión, autenticación de datos y protección de reproducción opcional, pero, a diferencia de ESP, no proporciona confidencialidad. En consecuencia, tiene un encabezado mucho más simple que ESP. [19]"

La cabecera de autenticación es empleada para brindar integridad orientada a no conexión y la autenticación en el origen de datos a las partes de la cabecera IP, por lo cual para brindar seguridad al paquete se emplea adicionalmente algoritmos de encriptación, con el propósito de que la información al ser transportada desde el emisor hacia el receptor no sea modificada a esto se le llama también integridad de la información, para lo cual el protocolo AH emplea el algoritmo HMAC.

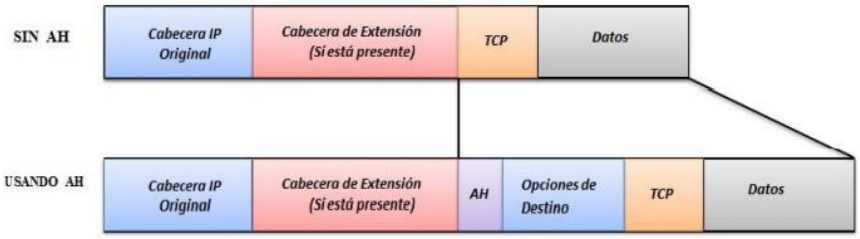


Gráfico 4 Localización de la cabecera de autenticación en modo transporte

Elaborado por: Jorge Enrique Lopez Logacho

Algoritmos de Encriptación

"Con las herramientas descritas anteriormente, es posible construir un sistema muy complicado y muy extensible para la seguridad de la red. IPSec es un ejemplo. IPSec utiliza cifrados. [20]"

"Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se está usando. Sólo si el atacante obtuviera la clave, le serviría conocer el algoritmo. [1]"

"El algoritmo de cifrado DES (Data Encryption Estándar) usa una clave de 56 bits, lo que significa que hay 2 elevado a 56 claves posibles (72.057.594.037.927.936 claves). Esto representa un número muy alto de claves, pero un ordenador genérico puede comprobar el conjunto posible de claves en cuestión de días. [1]"

"AES o también conocido como algoritmo Rijndael fue elegido por el NIST (National Institute of Standards and Technology), para ser el estándar en los próximos 20 años , fue elegido después de pasar un periodo de análisis durante aproximadamente 3 años, Rijndael fue elegido como la mejor opción dentro de 15 candidatos, sus principales características fueron su fácil diseño, su versatilidad en ser implementado en diferentes dispositivos, así como ser inmune a los ataques

conocidos hasta la fecha, soportar bloques de datos de 128 bits y claves de 128, 192, y 256 bits. La idea básica general es tener un estándar que mejore el "performance" de 3DES y sea resistente a los ataques conocidos. [1]"

Vulnerabilidades de IPSEC

En la actualidad no existe un protocolo el cual sea cien por ciento seguro, por lo tanto, el protocolo IpSec no es una excepción, ya que dentro del mismo existe varias vulnerabilidades entre la más relevante y que no se ha podido eliminar definitivamente es el factor humano al momento de configurar dicho protocolo ya que si este protocolo es configurado de manera incorrecta el mismo no se podrá aprovechar al máximo las ventajas de dicho protocolo.

Otra de las debilidades latentes que se ha pasado por alto, pero se encuentra prácticamente mitigada, aunque sigue presente es la utilización de algoritmos descontinuados como lo es el algoritmo "DES", para lo cual para evitar esta debilidad el sistema operativo de Windows muestra un mensaje de confirmación de utilización en caso de utilizar dicho algoritmo y sugiere el nuevo algoritmo el cual es 3DES.

Topologías de IPSEC

La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad (SA) como base para construir funciones de seguridad en IP. Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros (tales como las claves) que se está usando para cifrar y autenticar un flujo particular en una dirección. Por lo tanto, en el tráfico normal bidireccional los flujos son asegurados por un par de asociaciones de seguridad. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) le corresponde al administrador de IPsec.

VPN IPsec Punto a Punto

En el siguiente gráfico se puede apreciar: "La forma más básica de VPN IPsec se representa como una arquitectura dedicada de un circuito punto a punto uniendo dos extremos. [1]"

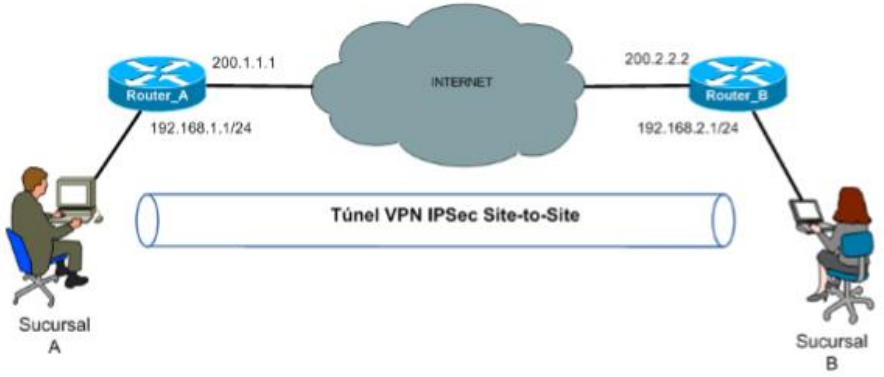


Gráfico 5 VPN Ipsec Punto a Punto

Elaborado por: Chaupis Guardia

Análisis de performance y monitoreo de redes

"El análisis y monitoreo generalmente llamado gestión de red se refiere a obtener valores continuos en el tiempo de las variables significativas del sistema, consiste en monitorizar y controlar los recursos de red con el fin de verificar su funcionamiento y evitar degradación en el mismo. [1]"

Monitoreo de Ancho de Banda

"El monitoreo de ancho de banda sirve para la medición del ancho de banda de conexiones de red y equipos (routers, switches, etc.), encontrar cuellos de botella y errores de conectividad para evitarlos en el futuro. Generalmente la gestión y monitoreo de equipos en redes IP son realizados utilizando SNMP. [1]"

Analizadores de Protocolos

"Un analizador de protocolos o sniffer es una herramienta que sirve para desarrollar y depurar protocolos y aplicaciones de red. Permite al ordenador capturar diversas tramas de red para analizarlas, ya sea en tiempo real o después de haberlas capturado. [1]"

"Los analizadores de protocolos se usan en diversas arquitecturas de red, tales como Redes LAN (10/100/1000 Ethernet; Token Ring; FDDI (Fibra óptica)), Redes Wireless LAN, Redes Gigabit, Redes WAN. Entre los usos principales de los analizadores de protocolos. [1]"

Wireshark

Wireshark es el analizador de protocolos de red más utilizado y ampliamente utilizado en el mundo. Le permite ver lo que sucede en su red a nivel microscópico y es el estándar de facto (y a menudo de jure) en muchas empresas comerciales y sin fines de lucro, agencias gubernamentales e instituciones educativas. El desarrollo de Wireshark prospera gracias a las contribuciones voluntarias de expertos en redes de todo el mundo y es la continuación de un proyecto iniciado por Gerald Combs en 1998. [21]

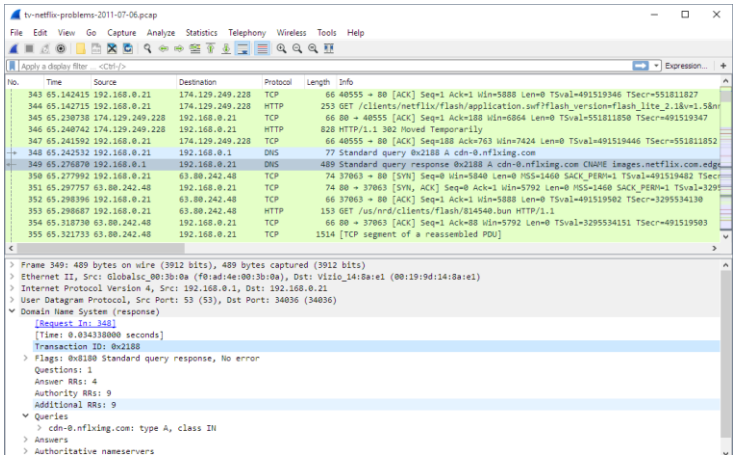


Gráfico 6 Wireshark
Elaborado por: wireshark.org

Medidor de Performance IPERF

La herramienta IPERF es una herramienta o aplicación cliente servidor para medición o pruebas de performance de redes, su interfaz es gráfica y consiste en un generador de flujos TCP y será la aplicación que utilizaremos para las pruebas sobre las maquetas a implementar en este proyecto.

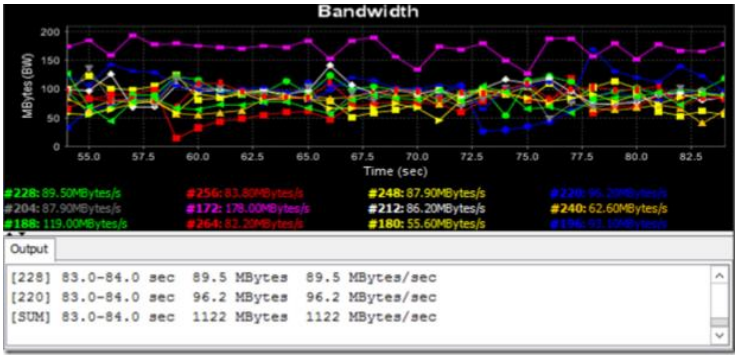


Gráfico 7 iperf
Elaborado por: wifisafe.com

Fundamentación del estado del arte

Dentro de un historial actualizado de investigaciones realizadas dentro de este campo se menciona dos trabajos los cuales son los más relevantes dentro del área. Se destaca el tema investigativo por parte de "Elén Marcela Gallegos Altamirano e Ismael Alexander Román González**"** en su tema: "Análisis de mecanismos de seguridad en un ISP de nivel 3 y propuesta de implementación de IPSec en un entorno IPV6".

A su vez se revisa el investigador: "Brito Ayala Juan Carlos" con su tema: "Estudio comparativo entre Ipsec y MPLS para redes privadas y virtuales (VPN)". Como resultado de esta investigación se puede apreciar diferentes tipos de pruebas para la comprobación del desempeño que tienen IPSec en entornos controlados.

Como resultado de las mismas se puede apreciar que las pruebas correspondientes a IPSec "se vuelve inestable al no poder manejar un flujo de más ancho de banda con paquetes pequeños. [1]"

Estos trabajos investigativos han dado como resultado una mejora sustancial con lo que respecta a la protección de la información, pero a su vez se mencionan los investigadores "Elén Marcela Gallegos Altamirano e Ismael Alexander Román González**"** que al momento de aplicar IPSec los paquetes son encapsulados dos veces por lo cual incrementan su tamaño y esto ocasiona que se tenga que procesar un tamaño de archivo de mayor tamaño lo que causa una degradación en la red.

Conclusiones Capítulo I:

- Se concluye que al momento de realizar la búsqueda bibliográfica se encuentran estudios realizados sobre los protocolos de seguridad en los cuales se puede apreciar el uso del protocolo IPSec para la comunicación segura y la protección de la información.
- Existen diferentes maneras de asegurar la información gracias a IPSec por lo cual se utiliza el conocimiento adquirido en esta búsqueda bibliográfica para la puesta en marcha del proyecto.
- Se han realizado trabajos que tienen como base el protocolo IPSec para establecer la comunicación segura en las cuales destaca el uso conjunto del protocolo ESP y el IKE para el intercambio de claves de manera rápida y la encapsulación, por lo cual se puede concluir que el uso del protocolo IPSec es sumamente importante para establecer una conexión segura y la protección de la información entre cliente – servidor.

CAPÍTULO II

Metodología

Análisis

El presente proyecto está enfocado en la simulación de una red de computadoras con el fin de obtener un resultado previo el cual será utilizado para cumplir con el objetivo principal y cumpliendo a cabalidad con los objetivos específicos definidos, así como la naturaleza de la investigación a través de un método experimental-analítico y sistemático conjuntamente apoyado con investigación documental.

Método experimental

Dado que el proyecto va más allá de la descripción conceptualizada o el establecimiento de relaciones entre los conceptos basados en análisis, es decir que está dirigido a responder las casusas en la problemática del entorno de la utilización del protocolo IPSec, pues se centra en el análisis mediante la simulación de una red de computadoras con dicho protocolo de seguridad.

Método analítico

En la naturaleza de la investigación corresponde un análisis comparativo previo a la recopilación de datos que permitirá conocer los resultados claves que condescenderá y contribuirá con investigaciones futuras e incluso con implementaciones de futuros proyectos. El método analítico en cuestión permitirá cubrir varias ventajas las cuales se detallan a continuación:

- Revisión del estado actual de la red en el laboratorio de EcuCiencia de la Universidad Técnica de Cotopaxi con el objetivo de levantar información referente al proyecto técnico, es decir dispositivos y componentes que conforman la red a nivel físico y lógico.
- Definir los instrumentos mediante los cuales se realizará la simulación del presente proyecto, es decir todo lo referente a las herramientas de software, software de simulación o hardware.

- Se verificará los datos extraídos mediante el software de wireshark de los paquetes transmitidos dentro de la red antes mencionada con el fin de realizar su análisis correspondiente.

Investigación descriptiva

Un estudio descriptivo mediante el cual se recolecta la información sin cambiar su entorno, es decir sin manipulación del mismo, normalmente es el mejor método de recolección de información que demuestra relaciones entre variables y describe el mundo tal cual es.

Tomando en cuenta el punto de partida de los objetivos antes planteados, se puede apoyar en esta técnica para la recolección de datos mediante una entrevista a los encargados del proyecto EcuCiencia la cual será tomada como una muestra de la población de la Universidad Técnica de Cotopaxi.

Variable cuantitativa

Es aquella que puede ser ordenada con respecto a magnitud. Se refieren siempre a atributos de objetos o cosas que incorporan la magnitud como una característica esencial. Pueden responder a preguntas del tipo ¿cuánto? –por ejemplo, número de hijos, edad, número de ensayos en un experimento-. Las variables cuantitativas pueden ser a su vez continuas y discretas.

Población

Para esta investigación se ha tomado como muestra poblacional de trabajo al proyecto EcuCiencia que se encuentra dentro de la Universidad Técnica de Cotopaxi, en la cual se observara el estado actual de la seguridad dentro del proyecto.

Métodos específicos de la investigación

Método de observación

La ciencia comienza con la observación, que puede ser considerada como el método más antiguo y moderno de recogida de datos. Esta afirmación, aparentemente contradictoria, se justifica por la gran evolución que ha experimentado el método observacional en los últimos años. Ahora bien, la observación sin más, no puede

ser considerada como método científico. Por ello resulta conveniente distinguir entre la observación ordinaria y la observación científica.

El principal objetivo de la observación es la comprobación del fenómeno que se tiene frente a la vista, con la preocupación de evitar y precaver los errores de la observación que podrían alterar la percepción de un fenómeno o la correcta expresión del mismo. En tal sentido, el observador se distingue del testigo ordinario, ya que este último no intenta llegar al diagnóstico, además son muchos los sucesos que le pasan desapercibidos.

Por lo cual se ha considerado el método de la observación científica pues esta cuenta con varias ventajas las cuales cabe recalcar las más importantes pues esta hace posible la intención de información tal como se presenta (ocurre). Además de conocer las formas de conducta que son consideradas en algunos casos sin importancia por los sujetos observados y que pueden ser percibidas por lo tanto este método permitirá realizar una hipótesis más acertada a partir de los datos observados y recopilados, a su vez nos ayudara al análisis de los bienes materiales que se encuentran en el proyecto EcuCiencia.

Método hipotético-deductivo

Se ha considerado este método ya que permitirá saber si la afirmación hipotética se ha realizado es verdadera o falsa al momento la implementación del proyecto.

Instrumentos

Entrevista

Ha sido considerada como la opción más favorable el diseño de una entrevista en la cual ayudara a reunir información relevante pues esta esta emitida por los profesionales involucrados en dicho proyecto, así como la seguridad que manejan dentro del proyecto EcuCiencia.

Diseño cuasi experimental

Los diseños cuasiexperimentales identifican un grupo de comparación lo más parecido posible al grupo de tratamiento en cuanto a las características del estudio de base (previas a la intervención). El grupo de comparación capta los resultados que se habrían obtenido si el programa o la política no se hubieran aplicado (es

decir, el contra fáctico). Por consiguiente, se puede establecer si el programa o la política han causado alguna diferencia entre los resultados del grupo de tratamiento y los del grupo de comparación. [22]

Los diseños experimentales son aquellos métodos o procedimientos utilizados clásicamente en la psicología experimental, para determinar el efecto de una o más variables independientes en dos o más grupos de sujetos. Se refiere a la forma y manera del procedimiento de comprobar un resultado y refutar otro u otros posibles.

Metodología Top-Down Network Design

"La metodología Top-Down propuesta por Cisco Press & Priscilla Oppenheimer se basa en las necesidades de análisis de requerimientos y diseño arquitectónico de las redes de comunicación, que debe realizarse antes de la selección de determinados componentes específicos para construir la red física. Un proceso Top-Down describe las múltiples faces por las que una red atraviesa utilizado el llamado cilo de vida de redes PDIOO (Planificación – diseño – implementación – operación - optimización). [23]"

La infraestructura de la red de datos en el proyecto EcuCiencia no dispone de seguridades adecuadas u óptimas para su desempeño adecuado, por lo cual se planea implementar una red de datos segura y confiable contando con un dimensionamiento de la red basado en una metodología formal y la implementación de políticas de gestión de red.

Dentro de presente trabajo se planea adaptar la metodología Top-Down Network Design propuesta, la misma que se centra en las necesidades de requerimientos de diseño arquitectónico de redes de comunicación por lo cual se plantea 4 fases las cuales son:

- Análisis de negocios objetivos y limitaciones: "en esta fase se identifica los objetivos y restricciones del negocio, y los objetivos y restricciones técnicos. [23]"
- Diseño lógico: "En esta fase se diseñará la topología de red, el modelo de direccionamiento y nombramiento, y se seleccionará los protocolos de brindging, swintching y routing para los dispositivos de interconexión. El

diseño lógico también incluye la seguridad y la administración de la red. [23]"

- Diseño físico: "Esta fase implica en seleccionar las tecnologías y dispositivos específicos que darán satisfacción a los requerimientos técnicos de acuerdo al diseño lógico propuesto (LAN/WAN). [23]"
- Plan de implementación: "Cada sistema es diferente; la selección de métodos y herramientas de prueba correctos, requiere creatividad, ingeniosidad y un completo entendimiento del sistema a ser evaluado. [23]"

Como segunda metodología se realiza la adaptación de la Metodología para la validación y evaluación remota de implementaciones de protocolos de seguridad propuesta por Antonio Izquierdo Manzanares.

Metodología de validación y evaluación

La metodología se divide de forma que inicialmente se presenta las definiciones de términos que utilizaran en la metodología, y un análisis acerca de la conformidad y rendimiento.

Para lo cual se realiza una simulación en un laboratorio controlado en el cual se realiza la simulación de los equipos con los que se cuenta en el laboratorio de EcuCiencia lo más acercada dentro a la realidad, se presenta la metodología de validación y evaluación, la misma que será adaptada a el proyecto, la cual divide de forma que inicialmente se presentan las definiciones de términos que se utilizaran en la metodología y un análisis de la conformidad y el rendimiento.

Conformidad y rendimiento

Para la implementación de un protocolo de seguridad es conforme a la especificación de dicho protocolo o arquitectura, para lo cual los requisitos de conformidad pueden ser **obligatorios** ya que cuyo cumplimiento se reduce a los casos en los cuales las implementaciones pueden ser totalmente opcionales o voluntarias.

En cuanto al rendimiento que ofrece la implementación de un protocolo de seguridad, los parámetros que se evalúan pueden dependientes del tráfico de red o independientes del tráfico de red. Aquellos parámetros que dependen del tráfico de

la red modifican los resultados que serán utilizados para la evaluación correspondiente. También se ven afectadas por el tráfico que se esté dando dentro de la misma red.

Por lo tanto, las fases que se toman en cuenta para la implementación del protocolo de seguridad son las siguientes entre las cuales se dispone de una tarea específica:

Fase 1 tareas preliminares

En esta fase inicial de las pruebas se determinará cuáles son las implementaciones a validar y revaluar y a su vez los recursos que serán necesarios para completar la tarea.

Determinar el tipo de análisis

Para determinar el tipo de análisis realizado se debe de llevar a cabo tres tipos de análisis entre los cuales son la validación de la conformidad, la evaluación de rendimiento y la validación de la conformidad y evaluación del rendimiento.

En este caso en análisis que será de utilidad en este proyecto es:

Evaluación de rendimiento: al llevar el análisis este se someterá a pruebas de rendimiento que proporcionen información acerca de la capacidad de protección de la información, pues los análisis serán a partir de un conjunto de pruebas de comportamiento.

Identificación de los recursos necesarios

Los recursos necesarios en este punto son las herramientas necesarias para la verificación del estado en la red por lo cual se lo realiza con la utilización de software de verificación de trafico de red.

Fase 2 Documentación preliminar

En esta parte de la documentación debe de ser clara y concisa para que cualquier persona pueda adquirir sin problemas el conocimiento sobre las pruebas realizadas para la implementación.

En este punto se procede a la realización de un entorno controlado lo más cercano a las características que disponen los equipos en el laboratorio de EcuCiencia, para

lo cual se documentara los aspectos generales del protocolo de seguridad y el rendimiento del mismo.

Fase 3 Análisis del estándar

En esta fase se realizará el estudio del estándar que permita ampliar los conocimientos adquiridos en la fase anterior.

Fase 4 Validación de la conformidad

Para definir un conjunto de pruebas que permitan el análisis es necesario identificar aquellas capacidades que aparecen recogidas en el estándar.

Identificación de los mecanismos criptográficas

Dado que existen diferentes mecanismos criptográficos, es necesario identificar cuáles son las que mejor se adaptan al estándar, teniendo en cuenta la evolución de los estándares en base a los protocolos.

Identificación de las características obligatorias

Dentro de las especificaciones de los protocolos de seguridad se incluye un mínimo conjunto de funcionalidades las cuales deben de ser incluidas en cualquier implementación de dicho protocolo. Este mínimo de funcionalidades debe ser identificado para poder incluir la validación por parte de las pruebas.

Diseño de pruebas

Una vez se disponga de la información suficiente acerca de los aspectos del estándar que se va a validar, se procederá a definir el conjunto de las pruebas que servirá para evaluar la capacidad y el comportamiento.

La definición de cada prueba constara con la siguiente información:

- Objetivos: el objetivo de cada una de las pruebas.
- Obligatoriedad: si es obligatoria la implementación de dicho protocolo.
- Medios de prueba: configuración del sistema de pruebas.
- Resultado previsto: descripción del éxito y del fallo.
- Configuraciones validas: variaciones de los parámetros en caso de ser necesario.

Fase 5 Evaluación del rendimiento

Rendimiento de los mecanismos criptográficas

El rendimiento de dichos mecanismos es muy variable entre los sistemas, por lo cual es necesario identificar los aspectos correspondientes al rendimiento que es necesario para la evaluación.

Identificación de los parámetros dependientes del trafico

Detallar los parámetros de rendimiento que sean dependientes del tráfico de red o las características concretas del tráfico que se utiliza para llevar a cabo la evaluación.

Identificación de parámetros independientes del trafico

Se identificará los aspectos del rendimiento de la red y las características del tráfico de red estos datos no afectan directamente los resultados finales de las pruebas anteriores.

Diseño de las pruebas

Una vez que se disponga de la información necesaria se realizara la evaluación del rendimiento, entre las cuales contara con la siguiente información:

- Objetivos: aspectos que se pretende evaluar.
- Medios de prueba: configuración del sistema de pruebas.
- Configuraciones validas: variaciones de los parámetros en caso de ser necesario.

Fase 6 Definiciones de perfiles de trafico

Los perfiles de tráfico serán definidos en el momento de llevarse a cabo la validación y la evaluación, en la cual se recogen las características del tráfico que se utiliza para llevar a cabo los análisis del rendimiento.

Los perfiles de tráfico deben contener la siguiente información:

- Protocolo: cual es el protocolo o los protocolos utilizados en él envió de datos.
- Tamaño de los paquetes.
- Sentido: Punto a punto o bidireccional.

- Medición: equipo o software que lleva a cabo la medición de parámetros.
- Retardo: Retardo artificial incluido en la red.

Fase 7 Tareas finales

Para finalizar el proceso se lleva a cabo la recopilación del material generado en las fases anteriores, tanto lo referente al protocolo de seguridad como a las pruebas que deben de aplicarse.

Correlación de variables

La correlación es una estadística que expresa hasta qué punto dos variables están relacionadas linealmente, el coeficiente de correlación es la medida especifica que cuantifica la intensidad de la relación lineal entre dos variables en un análisis de correlación.

La correlación nos permite medir el signo y magnitud de la tendencia entre dos variables, la magnitud nos indica la fuerza de la relación y esta toma un valor entre -1 a 1 por lo tanto mientras más cercano sea el valor de los extremos a los valores antes mencionados más fuertes o débiles serán las tendencias de las variables.

Se puede mencionar que, si la correlación tiene un valor de 1 o -1 se considera que la correlación es perfecta, caso contrario si la correlación vale 0 se menciona que las variables no están correlacionadas.

En el Anexo 12 se puede apreciar la correlación de las variables sin ninguna protección, a su vez conjuntamente con la aplicación del protocolo seguro IpSec. Cabe recalcar que una vez aplicado el protocolo seguro se aprecia un resultado favorable en el cual se confirma que el nivel de seguridad de incrementa.

Conclusiones Capítulo II:

- Se concluye los instrumentos seleccionados para la realización y adaptación de esta metodología son los adecuados pues permiten tener un seguimiento continuo al proyecto.
- Al momento de realizar la definición de las metodologías a utilizar se puede seleccionar que partes de las mismas se adaptaran a este proyecto por lo cual se puede establecer un marco de trabajo adecuado el cual satisfaga las necesidades de dicho proyecto.
- Se concluye que las dos metodologías que son tomadas como referencia para la realización del marco de trabajo pueden ser adaptadas de manera correcta al proyecto pues disponen de varias fases las cuales pueden ser variables.

CAPÍTULO III

APLICACIÓN Y/O VALIDACIÓN DE LA PROPUESTA

Análisis de la situación actual

Para realizar el análisis en el cual se encuentra el laboratorio de EcuCiencia se procede a una revisión del estado actual de la arquitectura de la red tanto física como lógica, por lo tanto, se puede apreciar de primera mano que dicho laboratorio cuenta con: un servidor, seis equipos clientes, un router y un switch, esto es traducido en una red simple de tipo estrella con comunicación cliente – servidor. A su vez es mencionado por parte del encargado del laboratorio que no cuentan con protocolos de seguridad para la protección de la información entre los equipos.

Mediante esta información obtenida se procede a la verificación de los componentes que disponen dentro del laboratorio y más a delante proceder con el análisis correspondiente de los mismos los cuales se detallan a continuación.

- Servidor
- Computadores de escritorio
- Switch

Conjuntamente se procede a realizar un diagrama lógico y físico mediante la herramienta packet tracer, en el grafico 10 se muestra como está organizado el laboratorio de EcuCiencia.

Por lo tanto, el laboratorio cuenta con un cableado estructurado en el cual están interconectados varios equipos mediante un switch al servidor principal con una conexión directa de punto a punto.

Para la realización de dicho proyecto por cuestiones de la actual pandemia que está ocurriendo en el Ecuador se procede a realizar un pequeño laboratorio de pruebas en el cual se mantendrá un ambiente controlado dentro de un espacio virtual en el cual se cuenta con las condiciones ideales para simular una red segura y que esta ayude a la recolección de datos y elaboración de las pruebas necesarias.

Este proyecto será realizado en un laboratorio pequeño el cual está conformado por un equipo portátil físico y tres equipos virtuales los cuales contaran con las características mínimas para que el funcionamiento de los equipos al mismo tiempo no de ningún tipo de **lag** al momento de realizar la recogida de datos pertinente.

Marco de trabajo para la validación y evaluación de implementación de protocolos de seguridad IPSec.

Fase 1 Analizar requerimientos

1. Analizar red existente

   Para el análisis de la red pertinente se realiza la entrevista oportuna a la persona encargada del laboratorio de EcuCiencia, por lo cual la información que es brindada es de primera mano, por lo tanto, se menciona que dispone de una arquitectura de red local básica. Sin ningún tipo de seguridades extras.

   Por consiguiente, se implementa el laboratorio de pruebas en la cual se realizará las simulaciones y pruebas para tener los datos los datos necesarios.

2. Analizar tráfico existente

   Flujo de trafico de transmisión de un computador a nivel LAN

   Tabla 3. Flujo de trafico de transmisión de un computador a nivel LAN

Impresora	Transmite	127Kbps
Mensajería	Transmite	148Kbps
Total	Transmite	275Kbps

   Elaborado por: El investigador

   Flujo tráfico de un computador a nivel WAN

   Tabla 4. Flujo tráfico de un computador a nivel WAN

Correo Institucional	Transmite	1024Kbps
Correo Email	Transmite	1024Kbps
Total	Transmite	2048Kbps

   Elaborado por: El investigador

   En adelante se detalla el ancho de banda con el cual se realiza los cálculos necesarios para lo cual se utiliza el programa **SPEEDTEST,** pues este nos

ayuda a calcular de manera precisa el ancho de banda que está dentro de la computadora base.

A su vez se verificará cual es el ancho de banda de las 3 computadoras virtuales que se está manejando en dicho equipo.

Actualmente se realiza la prueba a la operadora con la cual se tiene contratado internet el cual es NETLIFE el cual nos ofrece una velocidad de 40mb(30-38mb) mediante fibra para la conectividad. la velocidad de subida y bajada se puede apreciar en la siguiente tabla.

Tabla 5. Velocidad del internet

Velocidad de subida	Velocidad de descarga
38000 kbps	38000 kbps
38 mb	38 mb

Elaborado por: El investigador

Por lo tanto, para saber cuál es la capacidad de transmisión de cada equipo se procede a dividir los kbps por los equipos existentes.

Transmisión = 38000/3

Transmisión = 12000 kbps

3. Análisis del rendimiento ancho de banda

   El ancho de banda con el que se está trabajando en estos momentos para la implementación de un protocolo de seguridad a un nivel de laboratorio es sumamente importante y es suministrado una velocidad variante entre 30mbs y 38mbs esta velocidad es de suma importancia pues al momento de configurar un protocolo de seguridad este no debe afectar al ancho de banda que se maneja dentro del laboratorio.

Fase 2 Desarrollar diseño lógico

1. Diseñar topología de red

   El diseño lógico de la red es realizado en base a las limitaciones del laboratorio de pruebas que se maneja de manera personal por lo cual se plantea el siguiente diseño el cual puede ser utilizado como referencia del laboratorio de EcuCiencia.

Diseño lógico de EcuCiencia

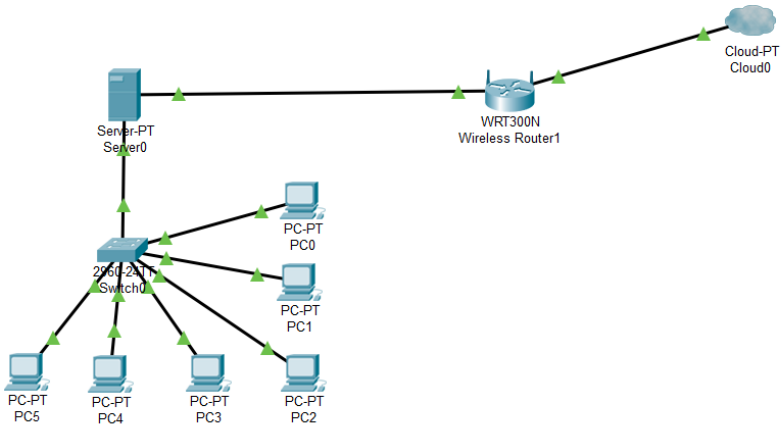


Gráfico 8 Diseño lógico de EcuCiencia

Elaborado por: El investigador

Diseño lógico del laboratorio de pruebas

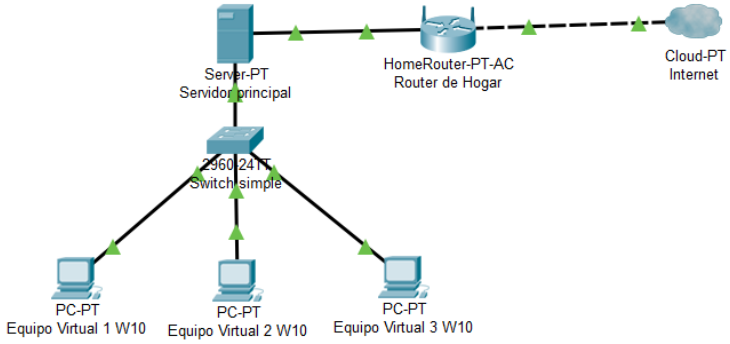


Gráfico 9 Diseño lógico del laboratorio de pruebas

Elaborado por: El investigador

2. Diseñar modelos de direccionamiento

   El modelo de direccionamiento que se va a utilizar dentro de esta red es el modelo de direccionamiento a través de IP, ya que se plantea la reutilización del diseño lógico de la red a su vez que gracias a este direccionamiento los paquetes pueden ser enviados y recibidos de una manera más eficiente, a su vez de localizar un equipo que se encuentre dentro de esta red de una manera más sencilla.

3. Seleccionar protocolos

   El protocolo a utilizar es IpSec, en modo transporte al cual se realizará las pruebas necesarias para saber si es un protocolo seguro, y a su vez verificar si este aporta una mejora en la seguridad del laboratorio de pruebas.

   Para la selección del protocolo se plantea el siguiente cuadro comparativo en el cual se detallan las ventajas y desventajas de utilizar cada protocolo.

Tabla 6. Tabla comparativa de protocolos

	Detalles							
Protocolos	Compatibilidad Windows	Compatibilidad con plataformas antiguas	Seguro	Rápido	Fácil configuración	Requiere programas de terceros	Soporte	Requiere Actualización
IPSec	✓	X	✓	✓	✓	X	✓	x
PPTP	✓	✓	X	✓	✓	X	X	X
SSTP	✓	✓	-	✓	✓	X	X	X
OpenVPN	✓	X	✓	✓	X	✓	-	✓

Elaborado por: El investigador

4. Análisis de los protocolos

   Una vez listado los protocolos y puesto las ventajas y desventajas de cada uno de los protocolos seguros se procede a la utilización del protocolo seguro de IPSec puesto que este dispone de una compatibilidad con las distribuciones de Windows a partir de Windows 8.1.

   IPSec es ampliamente más recomendable para su uso en servidores ya que este dispone de una compatibilidad nativa con el mismo, a su vez que es rápido y seguro en él envió de paquetes conjuntamente con una fácil configuración. Todo esto con un soporte por parte de Microsoft.

   El protocolo OpenVPN es otro protocolo seguro el cual tiene una amplia compatibilidad con Windows y a su vez es rápido y seguro, pero en este caso dicho protocolo necesita actualizaciones y requiere programas de terceros los cuales coloca un soporte limitado correspondiente a fallas o errores inesperados al momento de la implementación del mismo. Por lo cual dicho protocolo se deja de lado para su utilización.

5. Seleccionar mecanismos criptográficos

   El mecanismo criptográfico en este caso se realizará las pruebas necesarias para la comprobación de la seguridad por lo cual se realiza la utilización de los siguientes:

AH: Cabecera de autentificación, la cual se inserta entre la cabecera IP estándar y los datos que son transportados puede ser un mensaje TCP, UDP o ICMP, se lo puede utilizar de diferentes maneras, en modo transporte y modo túnel.

ESP: Este protocolo tiene como objetivo principal el proporcionar confidencialidad, pues especifica el modo de cifrar los datos que se van a enviar.

IKE: Este protocolo establece un vínculo de cifrado mediante el cual la concesión autentica 2 nodos, en este proceso es en donde se negocian las asociaciones de seguridad con IPSec, ya que se emplean algoritmos de cifrado y encriptación en ambos extremos de la conexión (emisor - receptor).

Tabla 7 Tabla comparativa

	Cabezera protegida	Integridad	Encriptacion	Autenticacion	Intercambio de claves Automatico	Mejoras
AH	✓	✓	X	✓	X	X
ESP	X	✓	✓	✓	X	X
IKE	X	✓	✓	✓	✓	X
IKEv2	✓	✓	✓	✓	✓	✓

Elaborador por: El investigador

Fase 3 Desarrollar diseño físico

1. Arquitectura física actual de la red

   La arquitectura de la red actual que se maneja dentro del laboratorio de EcuCiencia se puede verificar en el gráfico 10:

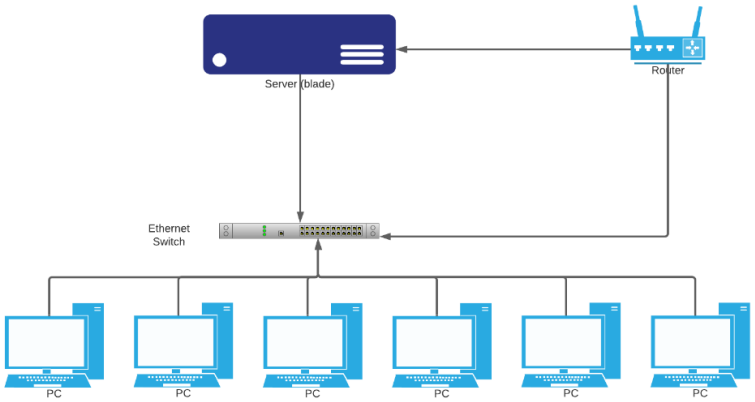


Gráfico 10 Diseño físico de EcuCiencia

Elaborado por: El investigador

Una vez presentada la estructura actual en el laboratorio de EcuCiencia se presenta en el gráfico 11, el diseño físico del laboratorio de pruebas que se está manejando al momento de realizar las pruebas para recabar información.

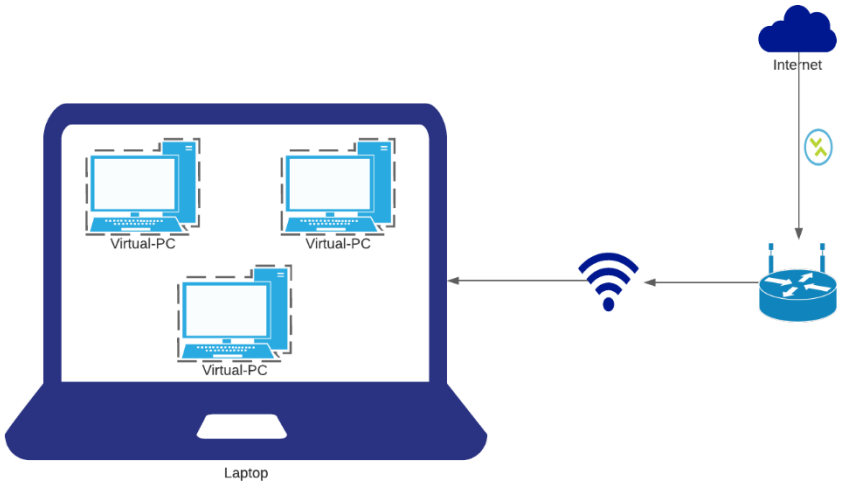


Gráfico 11 Diseño físico de pruebas

Elaborado por: El investigador

Como se puede apreciar en la imagen el laboratorio contiene máquinas virtuales las cuales funcionan al mismo tiempo simulando el tráfico de red que se está realizando en ese momento. Por lo tanto, una máquina virtual es la que contiene el servidor con el SO Windows server 2016 y las siguientes máquinas virtuales contienen SO Windows 10 pro.

2. Seleccionar tecnologías y dispositivos

   Para realizar las simulaciones se ha seleccionado los siguientes equipos y conjuntamente su descripción de cada uno de ellos.

   Laptop i7: El computador seleccionado es un I7 de 8va generación el cual dispone de 16GB de memoria RAM y 1TB en disco duro lo cual ayuda a soportar la carga de las máquinas virtuales y sus configuraciones respectivas.

   Router Huawei eg8m8145v5g06: El router es proporcionado por parte de la empresa Netlife con la cual se dispone de un contrato de internet para la utilización en este laboratorio de trabajo personal.

Virtual Box: Como herramienta de trabajo se selecciona el programa virtual box para la creación de las máquinas virtuales y su correspondiente configuración. Se selecciona este programa pues consume menos recursos que otras herramientas como los es Vmware.

Packet Tracer: se utiliza la versión actualizada para el diseño lógico de las redes y a su vez la simulación parcial de como funcionaria la red de tenerla físicamente.

Windows server 2016: Se selecciona esta versión de SO, pues es la versión más estable de los Windows server y contiene nuevos paquetes de seguridad y es más compatible con IpSec de manera nativa.

Windows 10: La selección de este SO, es en base a la utilización en el laboratorio de EcuCiencia por lo cual se coloca la misma versión y se los carga con programas básicos para el uso el uso de las mismas.

Fase 4 Ejecución

En esta fase se procede a configuración de los servicios base que deben de tener el servidor y de los equipos para la realización de las pruebas en las cuales se procede a la verificación de la seguridad de otorgan los protocolos de seguridad.

1. Configuración del servidor

   En este punto para la realización de la implementación se ha seleccionado el servidor Windows server 2016 para lo cual se realiza la configuración necesaria del SO, este SO ha sido seleccionado por la compatibilidad con el protocolo IpSec de manera nativa en la cual se puede configurar de manera más ágil y eficiente dicho protocolo.

   1.1. Instalación del servidor

   Dentro de la instalación del servidor se utiliza los requerimientos mínimos por defecto que recomienda el SO de Windows server 2016, por lo cual se detallan los requisitos mínimos que se utilizaran en la siguiente tabla con información oficial por parte de Microsoft.

Tabla 8. Requerimientos mínimos Windows server

Windows server 2016	
Detalle	Requisitos Mínimos
Procesador	Procesador de 64 bits, 1,4GHz
Memoria RAM	2GB en memoria RAM
Almacenamiento (Disco duro)	32GB en Disco Duro
Red	Adaptador de red capas de un rendimiento de al menos gigabit.

Elaborado por: El investigador

Por lo tanto, se realiza la creación de una máquina virtual la cual dispone las características mínimas para su funcionamiento correcto, a su vez asignando una segunda tarjeta de red la cual servirá para la interconexión con los demás equipos, por lo cual se puede apreciar en la siguiente imagen la configuración asignada.

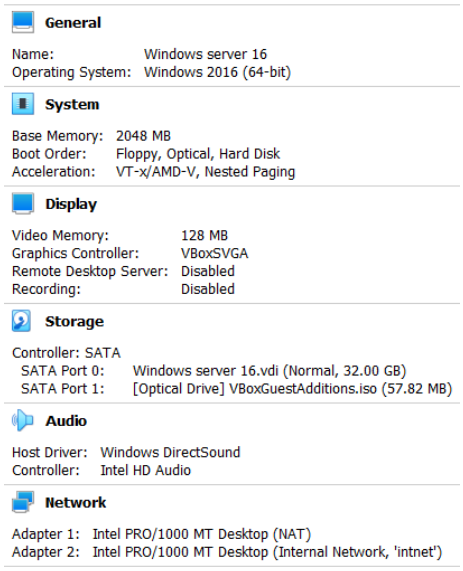


Gráfico 12 Requisitos básicos de la máquina virtual

Elaborado por: El investigador

Para la instalación del equipo se puede apreciar en **Anexos** el manual de la instalación que se utilizó para la Windows server 2016.

1.2. Tares Post Installation de Windows server 2016

Conjuntamente se realiza las tareas post instalación que debe de tener el servidor antes de implantar el protocolo de IpSec, para lo cual se detalla

dichas tareas después de la instalación de Windows server 2016, los cuales se pueden apreciar en el **Anexo 3**.

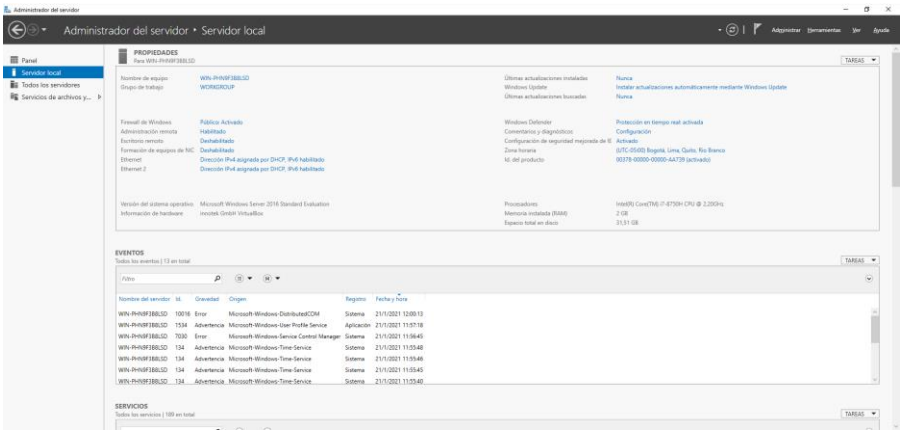


Gráfico 13 tareas post instalación Windows server 2016

Elaborado por: El investigador

Partiendo la configuración del servidor se debe de cambiar de manera inicial el nombre del servidor en este caso se colocará el nombre de sv-seguridad para que sea identificado con dicho nombre, por consiguiente, para verificar las tareas que se han realizado se lo puede apreciar el Anexo. A su vez se presenta una imagen en la cual se encuentra realizadas las tareas post instalación.

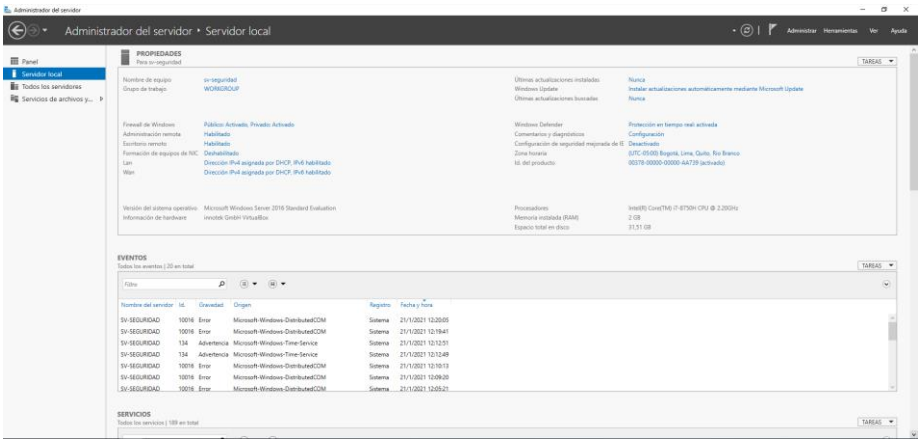


Gráfico 14 Cambio de nombre al servidor

Elaborado por: El investigador

2. Como esta armada la red

   La red actual está estructurada de manera virtual, por lo cual se conecta el servidor Windows server 2016 con 3 equipos virtuales que cuentan con Windows 10, a su vez se menciona que para la conectividad de los equipos virtuales se utiliza una topología de tipo estrella.

A continuación, en el gráfico 15 se muestra de manera gráfica como está estructurada la red de manera virtual.

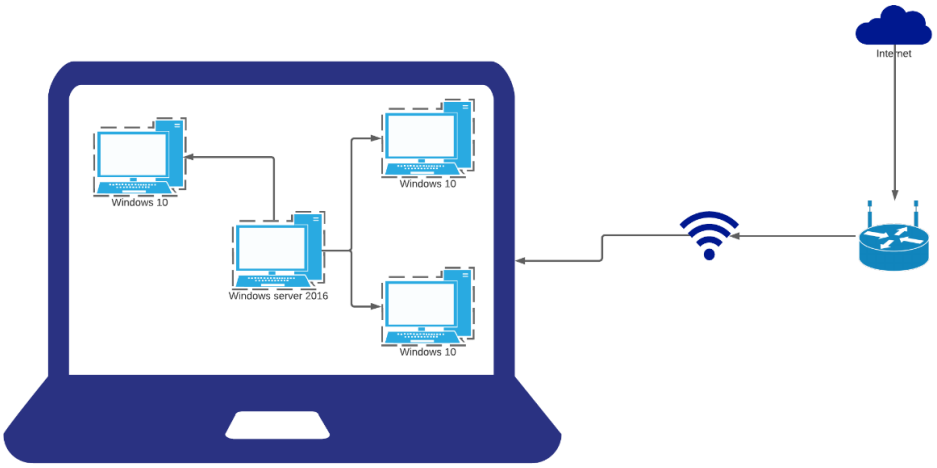


Gráfico 15 Red virtual estructurada

Elaborado por: El investigador

3. Configuración de los servicios base dentro del servidor

   Los servicios configurados dentro del servidor son los siguientes:

   - Active directory
   - DHCP
   - Servicio de enrutamiento
   - Grupos y usuarios

4. Configuración del protocolo dentro del servidor

   Una vez configurado los servicios anteriores se procede a la instalación y configuración de IPSec dentro del servidor, por lo tanto, se procede a la correspondiente instalación principal del servicio.

5. Configuración del cliente

   Siguiendo con las configuraciones en este punto se realiza la configuración de los computadores clientes colocándolos con sus respectivas configuraciones básicas, por tal razón se realiza lo siguiente:

   5.1. Instalación del equipo cliente

   Para la instalación de dicho equipo se realiza la configuración con las características básicas las cuales necesita dicho SO para funcionar, por lo tanto, se detalla en la siguiente tabla los requerimientos básicos que se necesita su funcionamiento.

Tabla 9. Requisitos mínimos de Windows 10

Windows 10	
Detalle	Requisitos Mínimos
Procesador	Procesador a 1 GHz o más rápido
Memoria RAM	1 GB para 32 bits o 2 GB para 64 bits
Almacenamiento (Disco duro)	16 GB para un SO de 32 bits o 32 GB para un SO de 64 bits

Elaborado por: El investigador

Una vez identificados los requerimientos mínimos para su funcionamiento se procede a instalar el equipo cliente de manera virtual, para lo cual para ver el tipo de instalación con la cual se trabajó en la parte de anexos se encuentra el manual de la instalación del SO. En la siguiente imagen se puede apreciar la configuración que se utilizó para la creación de las máquinas virtuales.

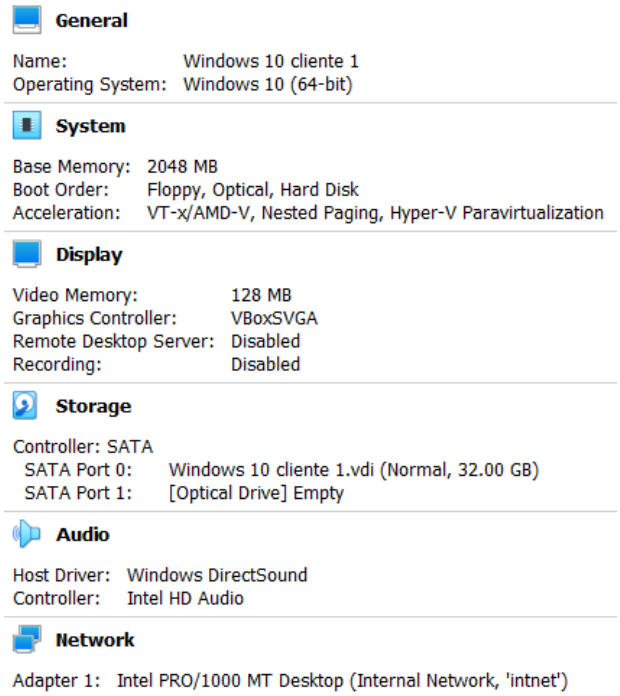


Gráfico 16 Requisitos de la máquina virtual Windows 10

Elaborado por: El investigador

5.2. Instalación de programas y configuración del equipo

Para la realización de las pruebas se instala dentro del cliente programas básicos entre los cuales están Office y programas pre instalados en el mismo Windows, a su vez se verifica que se disponga de conectividad cliente – servidor para la comunicación entre ambos.

5.3. Configuración del protocolo en el cliente

6. Detallar paso a paso el proceso de montaje de infraestructura

La manera en la que está montada la infraestructura es de manera virtual por lo cual se realiza la configuración del servidor de la siguiente manera:

1. En la creación de la máquina virtual el cual lleva el SO de Windows server 2016 se habilitará dos tarjetas de red en las cuales una actuará como la WAN la cual provee de internet y la segunda será colocada de manera LAN para proporcionar la red y conexión entre los diferentes equipos.
2. Una vez seleccionado habilitadas las tarjetas virtuales se procede a la configuración de la red LAN la cual se dará el nombre de "intnet", esta será utilizada para la conexión entre los equipos virtuales.
3. En el siguiente paso se realiza la configuración de la red por parte del cliente en la cual se asegura que el equipo esté dentro de la red LAN, en la cual se pueda tener conectividad mediante internet y conectividad al servidor.
4. Para los siguientes equipos se debe realizar el punto número 3.

Fase 5 Probar

1. Análisis del diseño de red

1.1. Levantamiento de la información

Antes de realizar las pruebas necesarias del protocolo seguro se debe de levantar la información sobre el rendimiento de la red en la cual se está trabajando para saber qué tan estable es dicha red, cabe recalcar que esta prueba de rendimiento se realizara dentro del laboratorio de pruebas.

- Ping continuo a la IP del servidor
- Ping desde el servidor al cliente
- Acceso a internet

- Verificación de los equipos en la red

2. Plan de pruebas

Se realiza un plan de pruebas en las cuales se detallan las más importantes para conocer qué tan seguro es el protocolo seleccionado.

2.1.Diseño de pruebas

En esta etapa se realiza el diseño del formato en el cual se realizarán las pruebas colocando la descripción de la prueba, el objetivo de la prueba, los datos que deben de registrarse, la duración estimada de la misma, los resultados obtenidos y observaciones en caso de ser necesarias. Para lo cual se realiza un formato en el cual se detallarán los resultados de las pruebas efectuadas.

En la siguiente tabla se puede apreciar el formato el cual se va a manejar para la realización de las pruebas.

Tabla 10. Formato de pruebas

Descripción		Prueba: #
Objetivo		
Registro de datos		
Duración estimada		
Resultados		
Observaciones		

Elaborado por: El investigador

Por lo cual se detallan las siguientes pruebas que serán puestas en marcha para probar desde la conectividad hasta la seguridad por lo cual se presentan las siguientes pruebas.

Pruebas de conectividad

- Prueba de conectividad básica.
- Prueba de comunicación con los equipos clientes.
- Prueba de comunicación con el servidor.

Pruebas de Inicialización del servicio IPSec

- Puesta en marcha del servicio de IPSec.
- Verificación del estado del servicio IPSec.

Pruebas de conectividad entre equipos con el servicio IPSec activo

- Verificación mediante ping continuo el tiempo de demora de inicialización del servicio en el cliente.
- Comunicación mediante ping entre cliente – servidor con el servicio activo.
- Tiempo de respuesta con el servicio activo.
- Tiempo de respuesta con el servicio activo con ping continuo entre cliente - servidor

Pruebas de comprobación de la seguridad

En este punto se realiza las pruebas de seguridad mediante el protocolo para lo cual se realiza un formato diferente el cual se puede apreciar en loa siguiente tabla en el cual se califica con **"✓"** en caso de ser positivo, una **"X"** en caso de ser negativo y un **"–"** en caso de tener falencias.

Tabla 11. Formato de prueba de comprobación de seguridad

Descripción						Prueba:#
Objetivo						
Registro de datos						
Calificadores						
	Comunicación	Paquetes enviados con éxito	Paquetes erróneos	Encriptación	Encapsulamiento	Protocolo seguro
Ping al servidor						
Archivo de texto plano						
Varios archivos de texto plano						
Documento PDF						
Documentos PDF						
Imagen						
Imágenes						
Navegación						
Observaciones						

Elaborado por: El investigador

3. Realizar las pruebas (Análisis de las pruebas)

   La evidencia de realización de las pruebas se puede verificar en el **Anexo 12**, en las cuales se aprecia los parámetros calificadores.

   Prueba #01

   Esta prueba tiene como finalidad la comunicación entre los equipos clientes y el servidor, por lo cual la conectividad entre los mismos es satisfactoria ya

que estos tienen comunicación mediante ping continuo, por lo tanto, la comunicación entre equipos y el servidor es exitosa.

Prueba #02

Esta prueba es realizada para probar la conectividad que se dispone entre equipos clientes para el intercambio de información por lo cual se utiliza un ping continuo entre los equipos para la verificación de la comunicación por lo cual existe una comunicación correcta entre los diferentes equipos.

Prueba #03

Al momento de realizar esta prueba se puede apreciar que los equipos y usuarios están creadas mediante active directory, a su vez estas reglas se encuentran activadas dentro del servidor.

Prueba #04

Al momento de realizar la prueba se verifica que todos los clientes estén dentro del mismo dominio del servidor y que exista una conectividad entre los mismos, por ende, se detecta un error el cual no existe una comunicación entre los equipos mediante red, por esta razón se realiza la configuración de los equipos para las opciones de red en las cuales está la comunicación entre los equipos atados a un dominio.

Prueba #05

Al momento de realizar la prueba de comunicación con el protocolo IPSec se pudo apreciar mediante la utilización de wireshark que la seguridad ya se incrementó con respecto a la comunicación entre los diferentes equipos por ende se puede verificar que el protocolo seguro no se interpone en la comunicación de cliente – servidor.

Prueba #06

Al momento de realizar la prueba se puede apreciar que al momento de realizar un ping continuo desde el cliente al servidor este se conecta sin ningún tipo de problemas, de la misma manera al momento de enviar un archivo de texto plano, PDF e incluso imágenes por lo cual la comunicación "Cliente – Servidor" es correcta, pero a su vez mediante la utilización del programa wireshark se puede apreciar que la comunicación se produce a través del protocolo TCP para la comunicación mediante la red y este no

proporciona ningún tipo de seguridad para la encriptación de datos y él envió de archivos.

Cabe recalcar que se realiza la prueba de navegación y se puede apreciar de similar manera que la comunicación no dispone de ningún tipo de seguridad interna.

Prueba #07

Al momento de realizar la prueba se puede verificar que el nivel de seguridad mediante el protocolo TCP con IPSec ha incrementado notablemente con respecto a la comunicación entre equipos, a su vez se encuentra algunas falencias al momento de enviar diferentes tipos de archivos al servidor y a su vez la navegación.

En dicha prueba la seguridad en la comunicación entre equipos se encuentra en un nivel seguro básico puesto que se está aplicando un protocolo especifico.

Prueba #08

En esta prueba se utiliza dos reglas que involucran a los protocolos TCP y ICMP con IPSec para la comunicación entre los equipos, por lo cual la seguridad se ha incrementado estableciendo una comunicación segura la cual encripta y encapsula los mensajes enviados mediante el protocolo ESP a través de la red, a su vez se puede apreciar que existen algunas falencias en él envió de archivos pues estos aun no son encriptados, por ende, se procede a la siguiente prueba.

Como resultado de la misma se puede apreciar que la navegación segura mediante internet se ha establecido al encriptar la información que se está buscando.

Prueba #09

Una vez realizada la prueba se puede apreciar que los archivos enviados se encuentran con una encriptación y un nivel de comunicación seguro para la transmisión de archivos y a su vez la navegación por internet, se puede apreciar fallas en la comunicación segura en base a la navegación, pero este caso estos datos se generan en base a un error en el internet los cuales podrían afectar a la comunicación segura.

4. Rendimiento de los mecanismos

Para la ver el rendimiento de los mecanismos se realiza las siguientes pruebas para comprobar su funcionamiento partiendo desde la velocidad con la cual se trabaja en los equipos. Para lo cual se puede apreciar en las siguientes imágenes la velocidad que se maneja en el servidor y los clientes. Mediante la herramienta web SpeedTest se obtienen los siguientes resultados los cuales son:

Gráfico 17 ancho de banda del servidor
Elaborado por: El investigador

Gráfico 18 ancho de banda del equipo 1
Elaborado por: El investigador

Gráfico 19 ancho de banda del equipo 2
Elaborado por: El investigador

Gráfico 20 ancho de banda del equipo 3
Elaborado por: El investigador

Siguiendo con la verificación del rendimiento de los mecanismos se utilizará la herramienta ipref para realizar un envió de datos a través de la red mediante el protocolo TCP y UDP para los datagramas correspondientes. Por lo cual se realiza el envio de ping mediante dicha herramienta para ver si los paquetes enviados llegan de manera correcta.

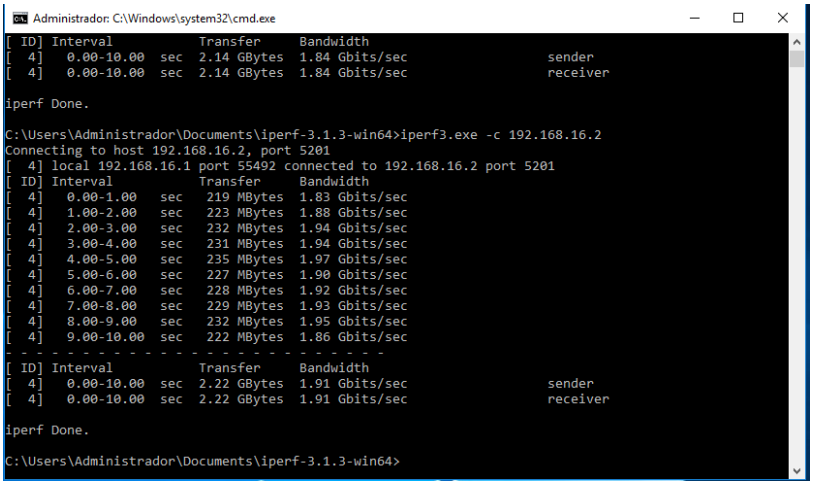


Gráfico 21 Envió de ping controlado protocolo TCP
Elaborado por: El investigador

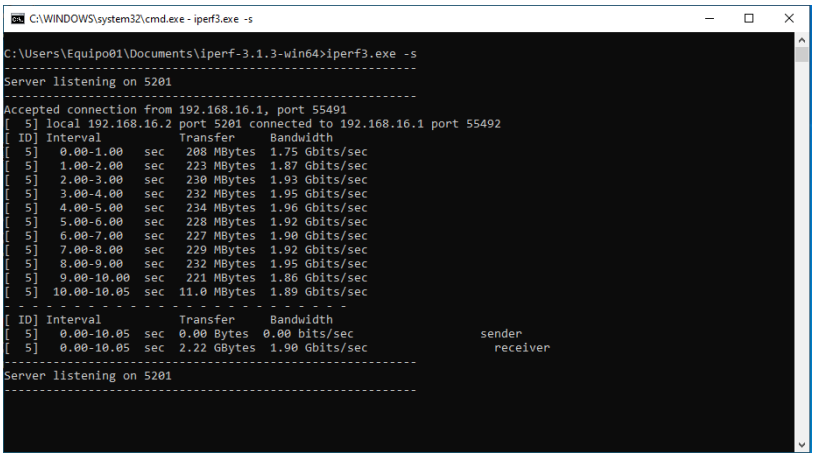


Gráfico 22 Recepción de información
Elaborado por: El investigador

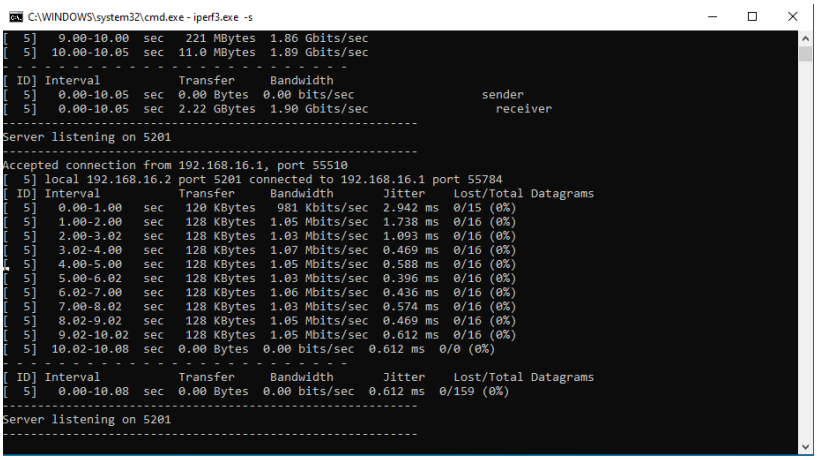


Gráfico 23 Recepción de información Protocolo UDP
Elaborado por: El investigador

Para la confirmación de la utilización de los protocolos se realiza un ping continuo al servidor desde el cliente para saber si los protocolos de

seguridad están funcionando de manera correcta para la comunicación segura entre de los equipos.

Por lo tanto, en la siguiente imagen se puede apreciar una captura de datos mediante el programa de wireshark sobre si los protocolos seguros están funcionando mediante la comunicación de dos equipos.

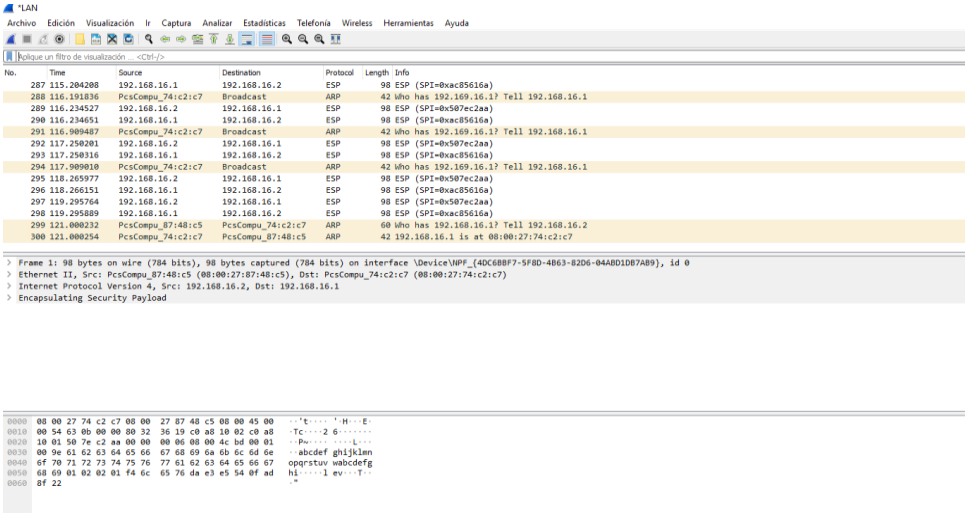


Gráfico 24 Captura de datos en ping continuo mediante wireshark
Elaborado por: El investigador

Mediante el uso de las herramientas se pudo verificar que el rendimiento de la red y los componentes funcionan de manera correcta salvo al momento de ver el ancho de banda ya que en ese aspecto el ancho de banda tiene una variación pues las medidas que son realizadas ninguna dispone de un ancho de banda estable.

5. Correcciones o modificaciones para optimizar la red

   En este punto se analiza el estado en el cual se encuentra la red en la cual se está trabajando y las configuraciones de la misma respectivamente por lo cual las pruebas anteriormente realizadas se necesita mejorar la seguridad con respecto a las reglas de seguridad.

   Por lo cual las pruebas anteriores brindan la información necesaria para mejorar la seguridad en la comunicación entre equipos, a su vez se realiza la optimización de la red entregando reglas las cuales ayudan a la integridad de la información.

Fase 6 Tareas finales

1. Documentación de las fases anteriores

   Para la finalización se procede a la recopilación de la documentación realizada en los pasos anteriores dando como resultado un informe final sobre los resultados obtenidos de dicha implementación.

Resultado del diseño experimental

Como resultado de la observación se puedo verificar que dentro del laboratorio de EcuCiencia se manejan un servidor principal y seis equipos clientes los cuales son utilizados para realizar módulos de programación para dicho laboratorio, a su vez también son utilizados para el envío de archivos de texto plano, imágenes, PDF e incluso videos. Gracias a estos datos obtenidos por la observación se puede realizar un laboratorio pequeño de pruebas en el cual se simulará el servidor y tres máquinas clientes las cuales tendrán una comunicación entre ellas.

Conjuntamente mediante la observación se puede verificar que la topología de la red con la cual se trabaja dentro del laboratorio de EcuCiencia es una topología de red tipo estrella, la cual se adapta a las necesidades de dicho laboratorio.

La investigación bibliográfica aporto con una vasta información acerca de cómo realizar la implementación del protocolo de IPSec y como es su funcionamiento y a su vez las herramientas idóneas para la comprobación de la red.

Como resultado de la adaptación de dos metodologías se ha realizado un marco de trabajo mediante el cual se puede disponer de una herramienta más flexible la cual permite documentar las partes más importantes de la implementación de una red para la comunicación segura a su vez de entregar pruebas las cuales permiten realizar un análisis sobre la seguridad que entrega el protocolo seguro IpSec.

Partiendo de las pruebas sin un protocolo de seguridad se verifica que la información que se maneja dentro del servidor y los clientes está abierto a cualquier sniffer, el cual puede aprovechar la información o robársela en casos extremos. Por lo tanto, se revisa el envío de archivos y se puede apreciar que mediante un captador de datos se encuentra el destino y el origen al cual se está enviando los archivos.

Para una mejor apreciación en la siguiente imagen se puede apreciar el nivel de seguridad que dispone una comunicación seguridades.

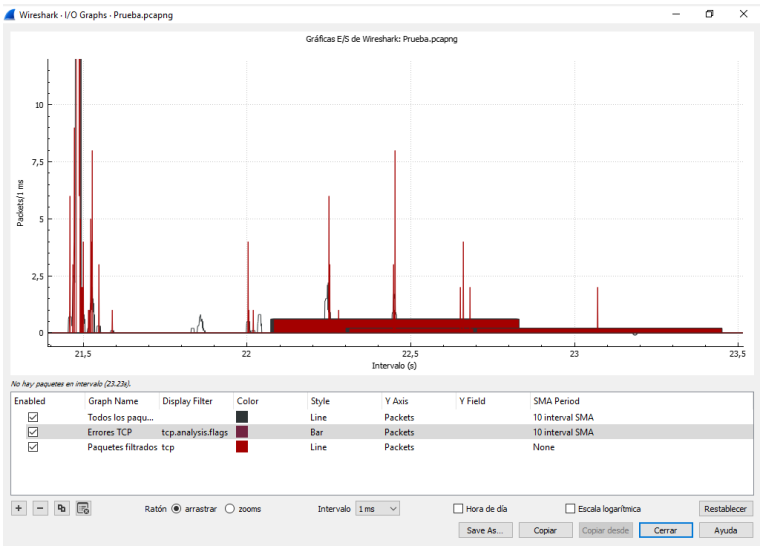


Gráfico 25 Comunicación TCP sin protocolo seguro

Elaborado por: El investigador

Al momento de realizar una comunicación constante hacia un el servidor por medio de una conexión que no contiene ningún tipo de seguridad, se puede constatar que el error en los envíos de paquetes se hace evidente por lo cual existen más deficiencias al momento de enviarlos de manera emisor – receptor.

Por lo tanto, con la utilización del protocolo IPSec se puede apreciar que la información se encuentra más segura al momento de comunicarse entre equipos que se encuentran dentro de una red LAN. El protocolo IPSec es un protocolo de comunicación segura en la cual se protege la información privada ya sea de ataques externos o como se los puede conocer “El hombre del medio”, gracias a este protocolo se puede asegurar la información con la que se está trabajando dentro del laboratorio de EcuCiencia, pero a su vez el protocolo IPSec esta desactualizado puesto que en la actualidad dicho protocolo es más seguro con la utilización del protocolo IPV6.

Para la comprobación del protocolo seguro se muestra en los siguientes gráficos el nivel de protección que se adquiere una vez aplicado el protocolo seguro.

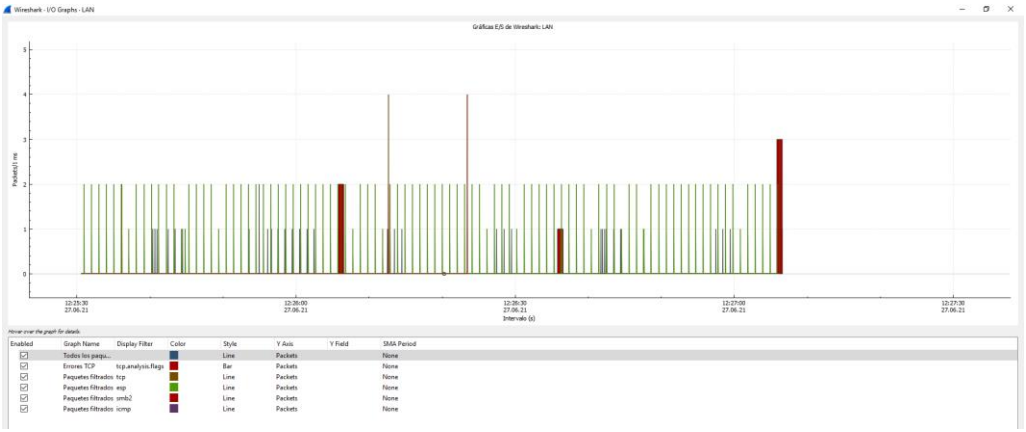


Gráfico 26 Comunicación TCP con protocolo IpSec

Elaborado por: el investigador

Como se puede apreciar al momento de colocar el protocolo seguro IpSec se puede constatar que este ayuda a mitigar los errores en gran medida, dando como resultado un menor número de paquetes enviados por milisegundos (ms) pero de una manera más firme y con más estabilidad y seguridad en el encapsulamiento de los paquetes enviados.

Discusión de la aplicación y/o validación de la propuesta

Con los resultados recopilados al momento de realizar la simulación en el laboratorio de pruebas se puede apreciar que el nivel de seguridad incrementa significativamente, como diferencia principal se menciona que este proyecto es enfocado en la comunicación segura para la protección de la información que se está manejando dentro de una sub red LAN la cual dispone de acceso a internet pero no dispone de ningún protocolo de seguridad por lo cual se compra las diferencias más importantes entre disponer de un servidor sin ningún tipo de protección de la información a un servidor con un protocolo de seguridad el cual ayuda a la integridad de la información.

Esto es realizado para que dentro de la red no exista el termino de “El hombre del medio”, el cual hace referencia a que puede existir un sniffer el cual puede apoderarse de la información o perjudicar dicha información por lo cual se puede apreciar que gracias a la implementación de un protocolo de seguridad esta incrementa un nivel de seguridad como lo es la encriptación de la información para

que esta pueda llegar de un extremo a otro sin el sospecha de que el archivo sea corrompido o dañado.

Como diferencias principales se puede mencionar que para la implementación de un protocolo seguro como lo es IPSec, lo realizan en base a un modo de túnel VPN el cual sirve ayuda a proteger la información desde dos tipos de red, caso contrario el cual se realiza dentro de este proyecto pues está enfocado netamente en un modo de transporte el cual es el más utilizado dentro de las subredes como en este caso se realiza en un laboratorio de pruebas para asegurar que la información que se obtenga optima.

Como fortaleza del proyecto se puede recalcar la realización de un marco de trabajo el cual adapta dos tipos de metodologías satisfacen las necesidades de implementación a su vez las mismas entregan documentación relevante sobre la implementación de una red segura para la protección de los datos.

Mediante la utilización de dicho marco de trabajo se puede apreciar que la seguridad de la información dentro de un servidor se incrementa sustancialmente pues el protocolo IPSec funciona dentro de la capa tres del modelo OSI el cual se encarga del transporte seguro de los datos.

Gracias a esto se puede mencionar que gracias a la implementación del protocolo IPSec se ha incrementado la seguridad de los datos otorgándole integridad a los datos, encapsulamiento de la información y encriptación para que solo el emisor y receptor pueda interpretar dichos mensajes recibidos.

Conclusiones del III Capítulo

- Luego de finalizar el proyecto se puede concluir que se ha cumplido con los objetivos planteados al inicio del proyecto, ya que se ha diseñado un marco de trabajo para la implementación de una alternativa en la comunicación segura entre equipos.
- Se concluye que el protocolo IPSec se encarga de brindar un nivel de seguridad necesaria para la protección de la información dentro de una red LAN ya sea en una empresa o en un laboratorio, pues IPSec al ser un

estándar reconocido ampliamente es utilizado por diversos equipos cuanta con un amplio soporte.

Conclusiones generales

- Se concluye que al momento de realizar el análisis de los protocolos de comunicación segura se ha identificado que es necesario la aplicación de los mismos ya que al momento de establecer un protocolo seguro, la seguridad e integridad de la información es más robusta.
- Se concluye que mediante la simulación efectuada se puede brindar un nivel más alto de seguridad dentro del laboratorio de IPSec, pues gracias a dicho protocolo la información transmitida dentro de la red dispone de características más seguras las cuales ayudan a la integridad de los datos por lo tanto la implementación es satisfactoria a nivel de red LAN.
- Se concluye que la información obtenida en la simulación sobre la implantación del protocolo IPSec ofrece seguridad más robusta ya sea a una red o a un solo computador dependiendo de la implementación que se realice, pues se puede proporcionar seguridad de extremo a extremo en modo túnel o en modo transporte para una red la cual está conectada a un router.

Recomendaciones

- Se recomienda que el laboratorio de EcuCiencia migre a una red en la cual se establezca el protocolo IPv6 pues con esto se puede aprovechar de mejor manera los recursos y las bondades que ofrece el protocolo seguro IPSec.
- Se recomienda que se debe cuantificar el ancho de banda de los accesos a internet ya que la navegación incluye las descargas y videos los cuales viajan a través de los datos y estos a su vez incrementan el tráfico de la red por lo cual se debe administrar el ancho de banda de mejor manera.
- Se recomienda que no solo se debe de utilizar IPSec para la seguridad dentro de una red se debe complementar con túneles VPN, pues estos proporcionan una mejor seguridad, pero algunas veces no es suficiente por lo cual hay que complementarlo con políticas internas de seguridad.

- Se recomienda tener mejor conocimiento sobre las distintas tecnologías para en realizar la implementación mediante el uso de equipos Cisco las cuales ofrecen una mejor tecnología sobre IPSec.
- Se recomienda motivar a la Universidad la implementación del protocolo IPV6, en la cual se puede desarrollar nuevas redes y servicios para asi poder ofrecer una mejor seguridad ofertada por IPSec.
- Se recomienda la inclusión de acceso a ciertas páginas de internet pues estas consumen un ancho de banda, por lo cual se debe de crear exclusiones para no generar tráfico en exceso.

Bibliografía

[1] B. A. J. CARLOS, «http://repositorio.espe.edu.ec/,» 22 Febrero 2015. [En línea]. Available: http://repositorio.espe.edu.ec/handle/21000/12532. [Último acceso: 10 Marzo 2020].

[2] U. T. d. Cotopaxi, «EcuCiencia,» PH.D Gustavo Rodriguez Barcenas, 2018. [En línea]. Available: http://ecuciencia.utc.edu.ec/. [Último acceso: 10 Febrero 2021].

[3] J. E. V. H. CARLOS MARIO CASTAÑO CASTAÑEDA, «https://core.ac.uk/,» 2016. [En línea]. Available: https://core.ac.uk/download/pdf/71399425.pdf. [Último acceso: 10 03 2020].

[4] J. C. M. Perez, Sistemas Informaticos y Redes Locales, Madrid: RA-MA, 2014.

[5] L. D. Chaupis Guardia, «http://repositorio.une.edu.pe,» 03 Octubre 2018. [En línea]. Available: http://repositorio.une.edu.pe/handle/UNE/3585. [Último acceso: 03 Marzo 2020].

[6] O. Byron, «Visualizador de tráfico de red de comunicación basadas en la Arquitectura TCP/IP,» *Revista Universidad y Sociedad*, vol. 11, nº 2, pp. 193-202, 2019.

[7] S. A. S. Puebla, «https://repositorio.unican.es/,» 05 Septiembre 2018. [En línea]. Available: https://repositorio.unican.es/xmlui/bitstream/handle/10902/14509/410031.pdf?sequence=1&isAllowed=y. [Último acceso: 10 Marzo 2020].

[8] P. A. BONILLA FERNÁNDEZ, «http://repositorio.espe.edu.ec/,» 28 Octubre 2016. [En línea]. Available: http://repositorio.espe.edu.ec/bitstream/21000/11237/1/T-ESPE-049435.pdf. [Último acceso: 10 Marzo 2020].

[9] W. S. Kish, «Remedial Action Based on Monitored Wireless Throughput». US Patente US 20170171052A1 , 15 Julio 2017.

[10] C. M. F. Vinicio, «repositorio.ucsg.edu.ec,» 02 Junio 2017. [En línea]. Available: http://repositorio.ucsg.edu.ec/bitstream/3317/8343/1/T-UCSG-POS-MTEL-67.pdf. [Último acceso: 10 Marzo 2020].

[11] J. S. R. Chafla, «https://dspace.ups.edu.ec/,» 29 Noviembre 2016. [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/13048/1/UPS%20-%20ST002280.pdf. [Último acceso: 10 Marzo 2020].

[12] C. I. A. Maria, «http://dspace.ucuenca.edu.ec/,» 04 Abril 2016. [En línea]. Available:

http://dspace.ucuenca.edu.ec/bitstream/123456789/24191/3/tesis.pdf. [Último acceso: 10 Marzo 2020].

[13] E. F. L. MONTES, «http://biblioteca.usac.edu.gt,» Octubre 2005. [En línea]. Available: http://biblioteca.usac.edu.gt/tesis/08/08_0261_CS.pdf. [Último acceso: 6 Febrero 2020].

[14] I. H. A. Francisconi, IPsec en Ambientes, Primera ed., H. A. Francisconi, Ed., Villa Nueva, Villa Nueva: Carril Gody Cruz 2801, 2005, p. 2.

[15] I. L. Müller, «http://www.laminfo.com/,» 2011. [En línea]. Available: http://www.laminfo.com/blog/archivos/__5_unidad_V_IP_sec.pdf. [Último acceso: 10 Marzo 2020].

[16] G. Marques, IPsec y Redes Privadas Virtuales, Primera ed., Estados Unidos, Madrid: RA-MA, 2016.

[17] J. S. Tiller, A Technical Guide to IPSec Virtual Private Networks, US: CRC, 2001, p. 313.

[18] J. E. L. Logacho, «dspace.ups.edu.ec,» Noviembre 2013. [En línea]. Available: https://dspace.ups.edu.ec/handle/123456789/5372. [Último acceso: 6 Febrero 2021].

[19] V. B. S. W. Mohd Khalid, IPSec VPN Design, Indianapolis, Estados Unidos de America: Cisco Press, 2005, pp. 19-21.

[20] N. D. D. Harkins, IPSec: The New Security Standard for the Internet, Intranets, and Virtual private networks, Estados Unidos de America: Mary Sudul, 2002, p. 19.

[21] wireshark.org, «https://www.wireshark.org,» Gerald Combs , 2020. [En línea]. Available: https://www.wireshark.org/index.html#aboutWS. [Último acceso: 10 Marzo 2020].

[22] H. W. y. S. Sabarwal, «pdfs.semanticscholar.org,» 2014. [En línea]. Available: https://pdfs.semanticscholar.org/c90d/07751b1f51cf3fea8fdca6b50ef2b592b626.pdf. [Último acceso: 12 Marzo 2020].

[23] B. M. A. O. D. L. CRUZ, «http://repositorio.uladech.edu.pe/,» 28 Marzo 2018. [En línea]. Available: http://repositorio.uladech.edu.pe/handle/123456789/2283. [Último acceso: 6 Febrero 2021].

Anexos

Anexo 1

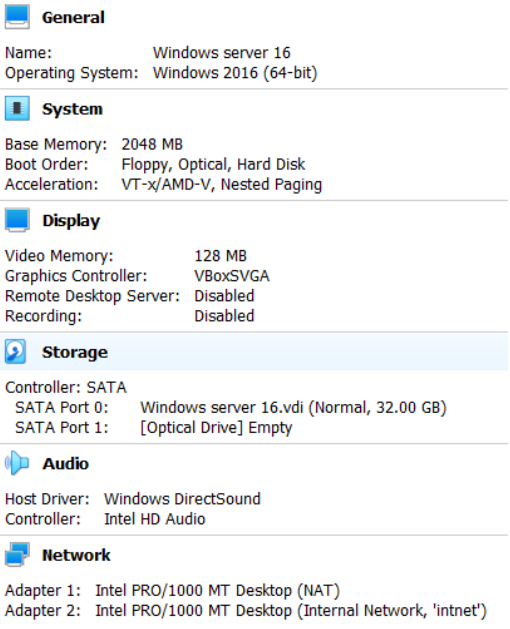
Instalación de Windows server 2016

Para la instalación de Windows server 2016 se otorga de las características básicas que este necesita para su funcionamiento correcto las cuales son:

Windows server 2016
Requisitos Mínimos
Procesador de 64 bits, 1,4GHz
2GB en memoria RAM
32GB en Disco Duro
Adaptador de red capas de un rendimiento de al menos gigabit.

Una vez detallado los requerimientos mínimos de funcionamiento se procede a la preparación de la máquina virtual con dichos requerimientos.

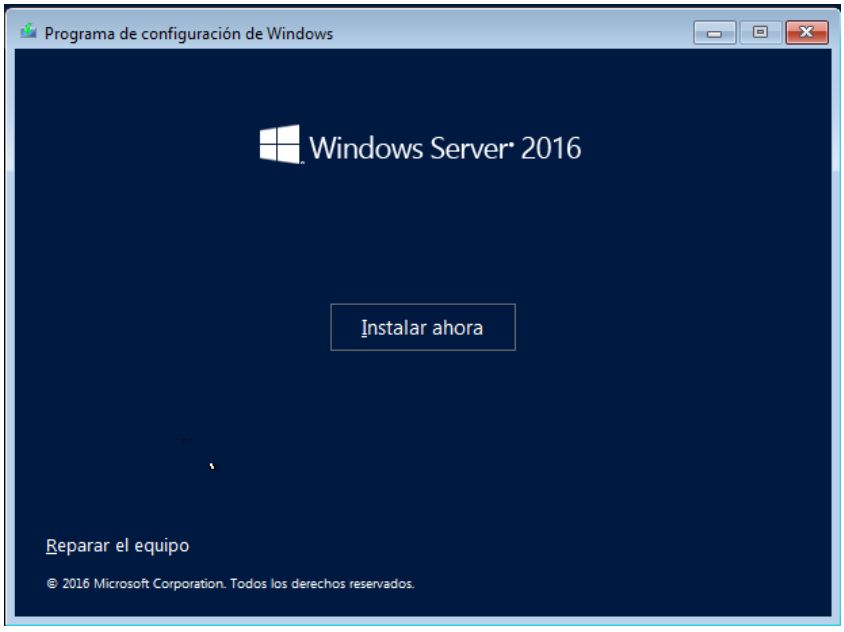
A su vez se coloca una doble tarjeta de red pues en este caso se utilizará la primera tarjeta para que provea de internet y la segunda será la encargada de distribuir los servicios del protocolo seguro y el acceso a internet, esta segunda tarjeta estará dentro de una red interna la cual esta nombrada como **"intnet"**. Por lo cual se puede apreciar en la siguiente imagen las configuraciones realizadas.



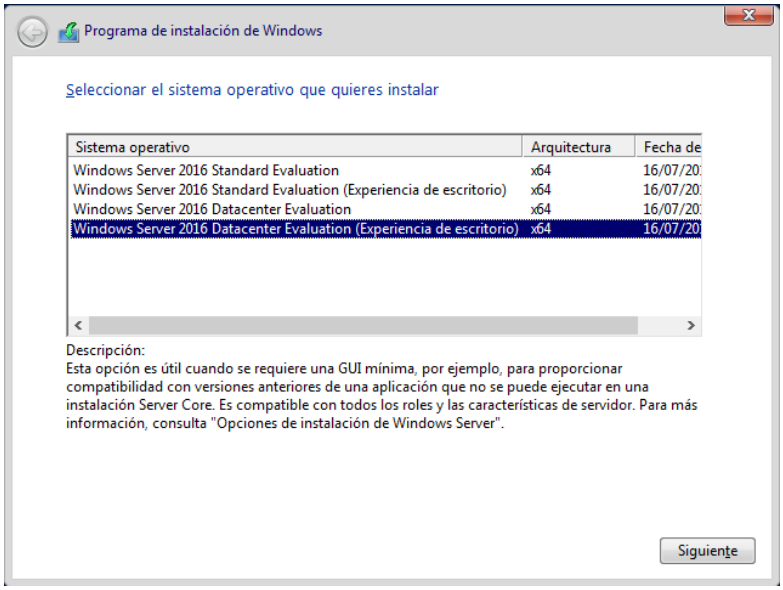
Una vez realizada la configuración dentro de la máquina virtual se realiza la instalación del sistema operativo siguiendo los siguientes pasos:

1. Primero se debe seleccionar la configuración de la fecha, idioma y la distribución del teclado que se maneja, en este caso se selecciona el idioma español, la fecha y hora del ecuador y como distribución del teclado se colocara teclado de Estados Unidos ya que el teclado que se maneja en este caso es uno estadounidense. Seleccionar “Siguiente”

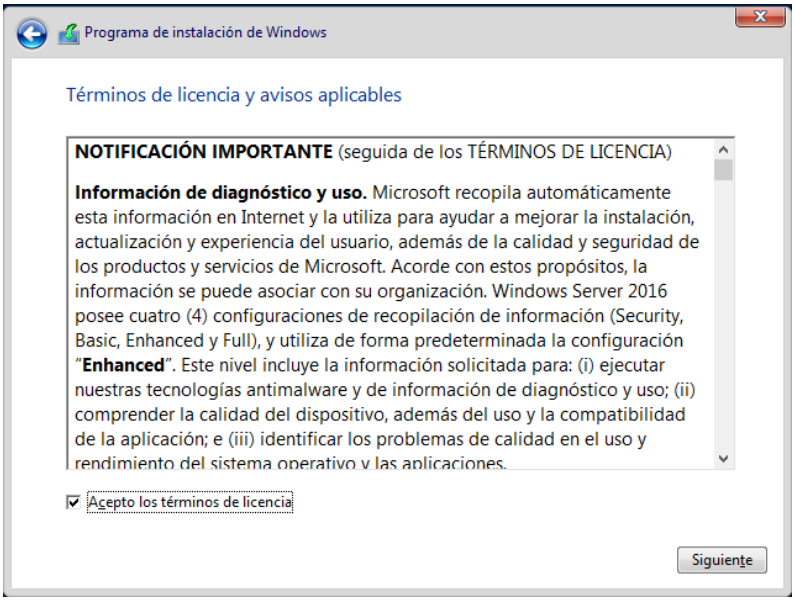
2. Siguiendo el paso anterior se selecciona “Instalar” la cual nos enviar al siguiente paso.



3. En el siguiente paso nos permite seleccionar la distribución de Windows server que se desea instalar en este caso se seleccionara la versión **“Windows server 2016 Datacenter”** con experiencia de escritorio” la cual nos entrega el entorno grafico para trabajar de una manera más dinámica. Una vez seleccionada la distribución se debe dar clic en **“Siguiente”**

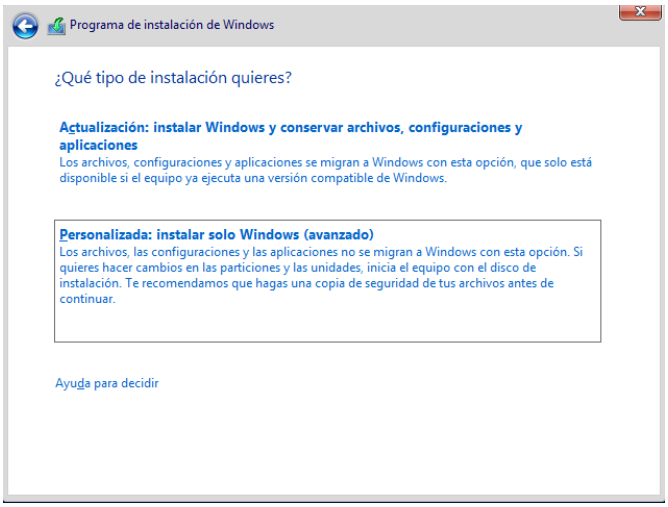


4. Como siguiente paso se debe de aceptar los términos y condiciones del uso del sistema operativo de Windows. Y seleccionar “Siguiente”

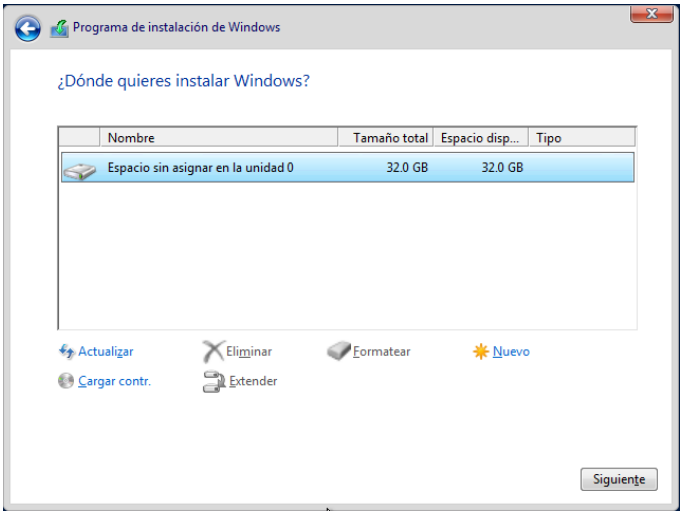


5. Una vez seleccionado siguiente nos aparece el tipo de instalación entre las cuales esta mediante actualización y personalizada, en la cual se

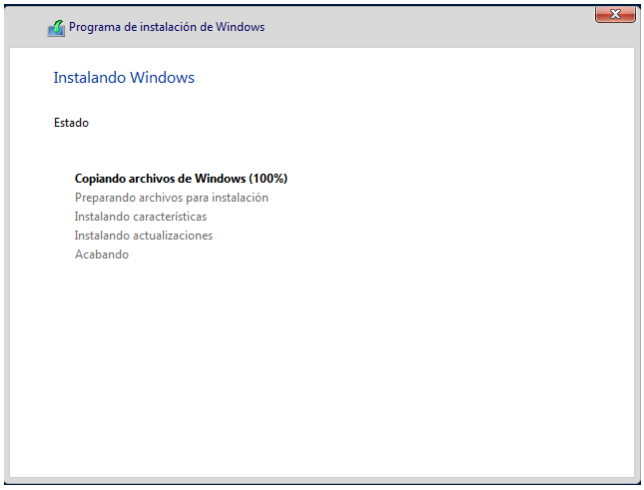
seleccionará la instalación **personalizada.** Y se proseguirá automáticamente en el momento de seleccionar el tipo de instalación.



6. Al momento de realizar la instalación se debe de seleccionar el disco en el cual se va a realizar la instalación en este caso al ser una máquina virtual se selecciona el disco duro en cual ira nuestro sistema operativo y cuál es la capacidad del mismo. Seleccionar siguiente para proseguir con el proceso de instalación.

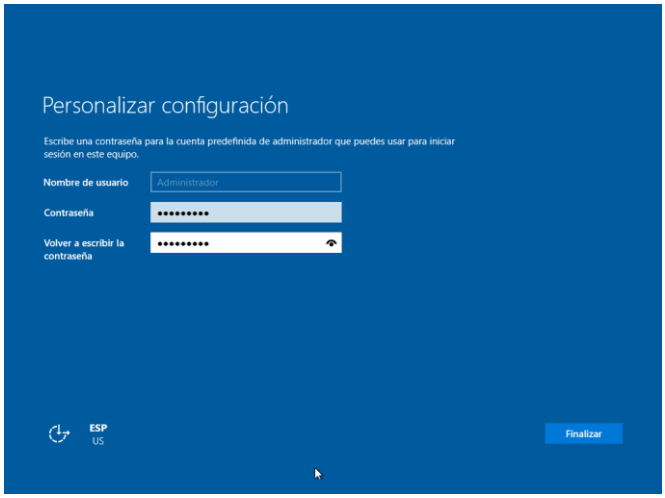


7. Una vez terminado el paso anterior se procede a esperar que finalice la instalación por lo cual se despliega la siguiente pantalla.



En esta pantalla se puede apreciar el progreso de cada uno de los procedimientos de instalación una vez terminada la instalación el servidor se reiniciará de manera automática para la configuración final la cual es del usuario administrador.

8. Al momento de haber culminado el reinicio del sistema operativo se debe de crear por defecto el usuario administrador dotándole de una contraseña segura para el acceso al mismo. Por lo cual se establece una combinación de letras en mayúsculas y números para dicho proceso de autenticación.



9. Como paso final se dará clic en finalizar para culminar con la instalación, una vez finalizado aparecerá la siguiente pantalla.

En la cual se debe de utilizar la unión de teclas que nos pide por defecto para ingresar al sistema operativo. Por lo cual una vez adentro dispondremos de la siguiente interfaz y se dará por terminada la instalación.

Anexo 2

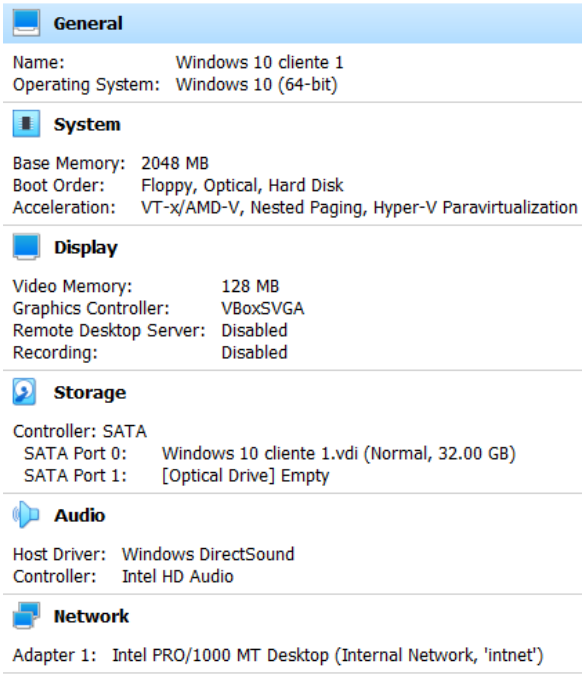
Instalación de Windows 10

En este caso para la instalación de Windows 10 se procede a la utilización de los requerimientos mínimos de instalación los cuales son:

Windows 10
Requisitos Mínimos
Procesador a 1 GHz o más rápido
1 GB para 32 bits o 2 GB para 64 bits

16 GB para un SO de 32 bits o 32 GB para un SO de 64 bits

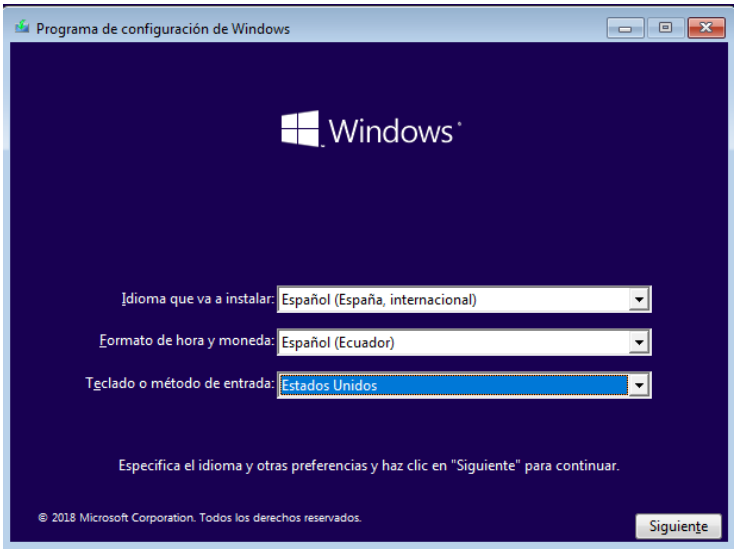
Con estos requerimientos se procede a la preparación de la máquina virtual la cual contendrá dichos requisitos. Lo cual se puede apreciar en la siguiente imagen.



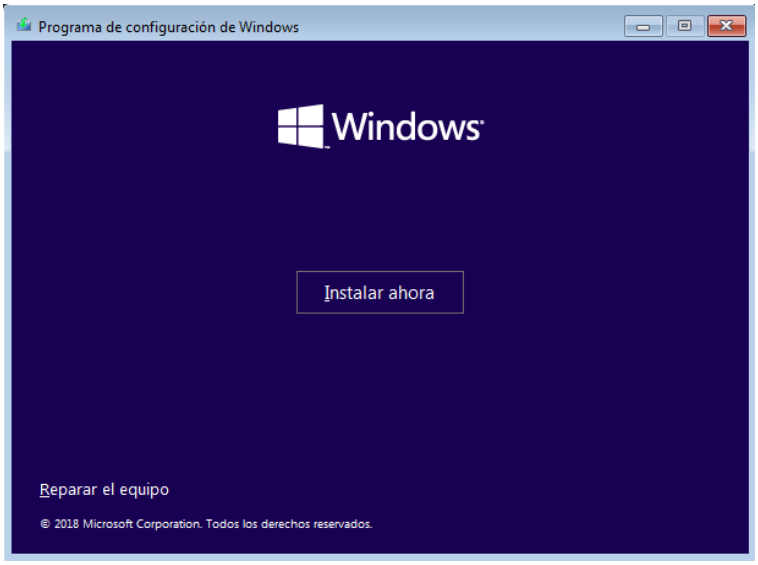
Este equipo contara con la red interna la cual es **“intnet”** la cual está relacionada con el servidor.

Para continuar con la instalación se debe realizar los siguientes pasos para su correcta instalación:

1. Para la instalación aparecerá una pantalla como en el caso de la instalación de Windows server 2016 en la cual se deberá seleccionar el idioma, el formato de la fecha y hora y la distribución del teclado, por lo cual se selecciona el idioma español, el horario de Ecuador y la distribución de este teclado como se lo menciono en el anexo anterior se dispone de un teclado en inglés. Estos cambios pueden verificarse en la siguiente imagen.

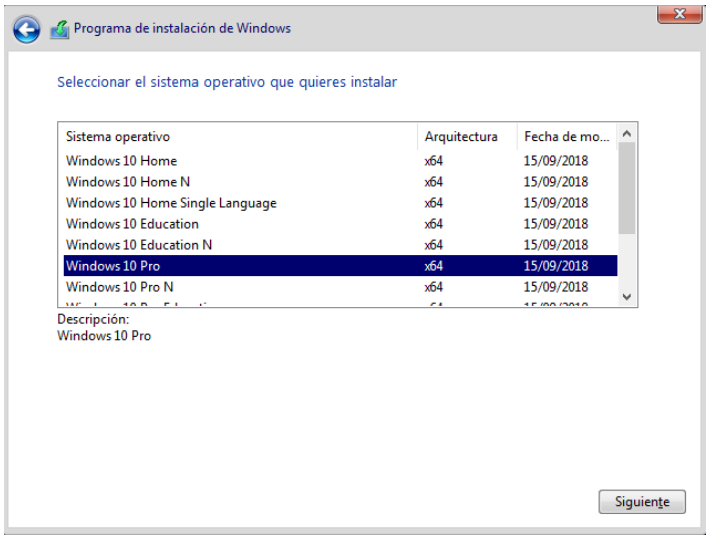


2. Cuando se despliega la siguiente ventana se debe de colocar “Instalar ahora” para seguir con el procedimiento de instalación del sistema operativo.

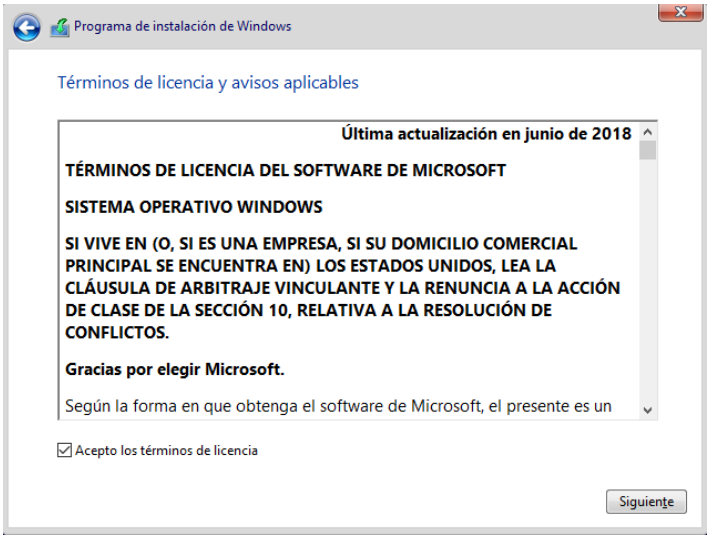


3. Una vez seleccionado “Instalar ahora” se despliega una ventana en la cual se debe colocar la clave de la distribución de Windows en caso de ser necesario en este caso se selecciona la opción “No tengo la clave de este producto” para proseguir con la instalación, más a delante se puede colocar una licencia en caso de ser necesario.

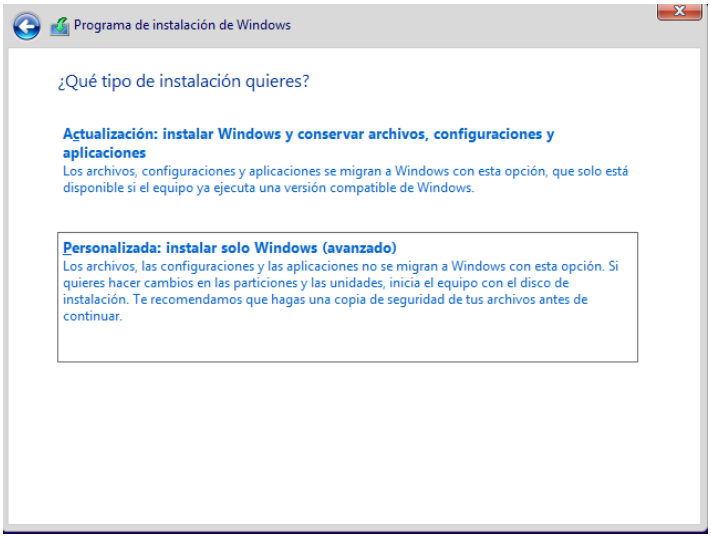
4. Después de haber realizado el paso anterior aparecerá una ventana en la cual se debe seleccionar la distribución del sistema operativo, por lo cual en este caso se selecciona Windows 10 pro en su versión de 64bits. Una vez seleccionado el tipo de distribución se dará clic en siguiente.



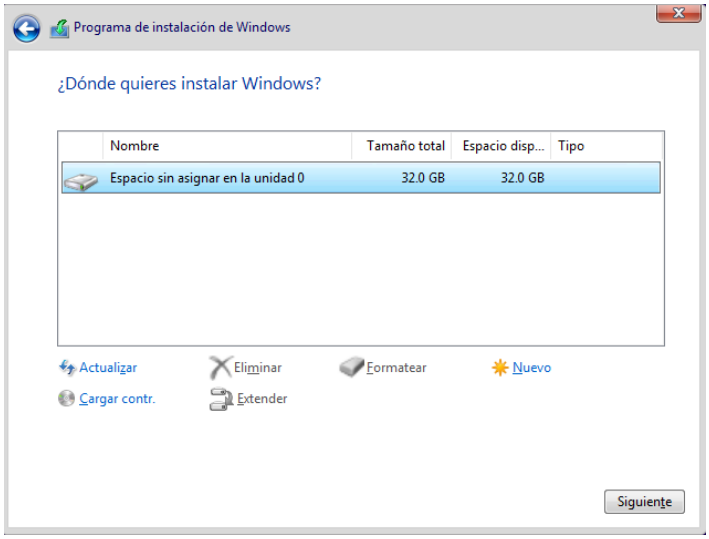
5. Como en el caso anterior se debe de aceptar los términos y condiciones de uso del sistema operativo, ya que en caso de no aceptarlos la instalación no podrá continuar. Se debe de dar clic en “Siguiente”.



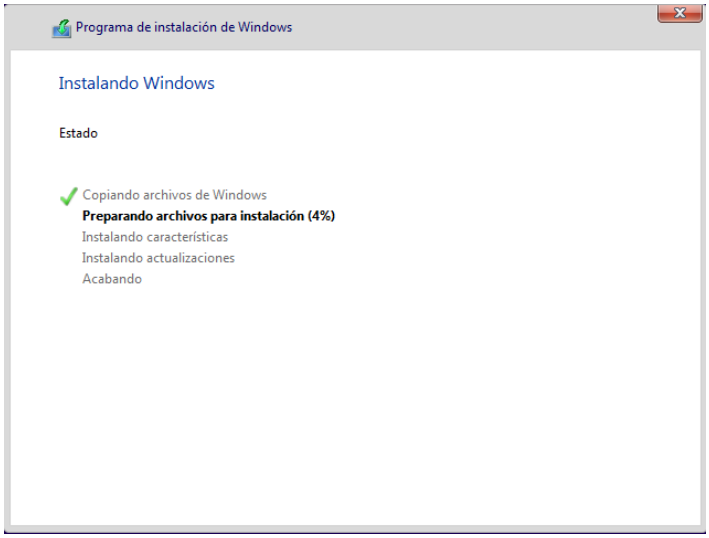
6. A su vez como nos muestra dos tipos de instalación la primera por medio de actualización y la segunda personalizada, por lo cual se selecciona “Personalizada” y dar clic en “Siguiente”.



7. Una vez seleccionada el tipo de instalación se debe seleccionar el disco en el cual se instalará el sistema operativo por lo cual en este caso se selecciona el disco duro que se está manejando y se da clic en “Siguiente” para proseguir con la instalación.

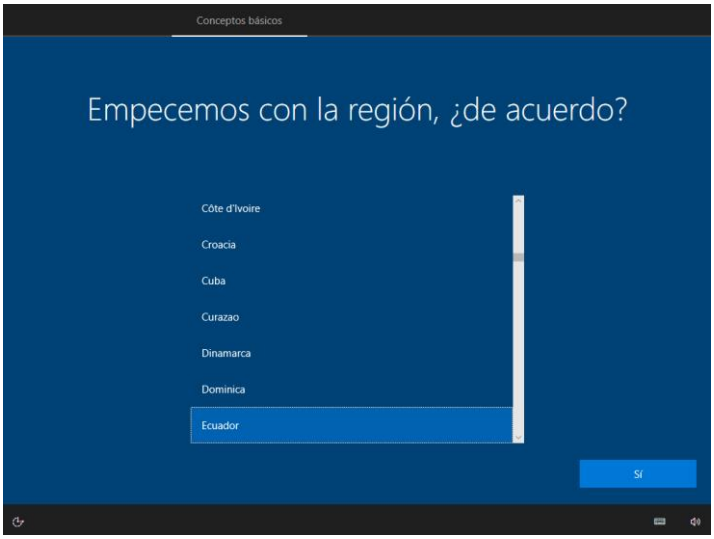


8. Una vez inicializada la instalación se despliega una pantalla en la cual aparece el proceso de instalación automático del sistema, en este punto el equipo se reiniciará varias veces hasta culminar todos los procesos.

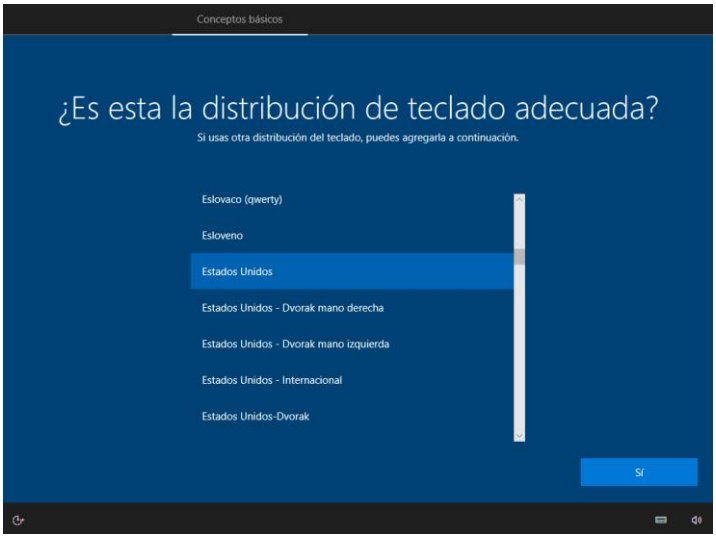


9. Una vez finalizado los procesos nos aparecerá las configuraciones finales en las cuales se configura de la siguiente manera.

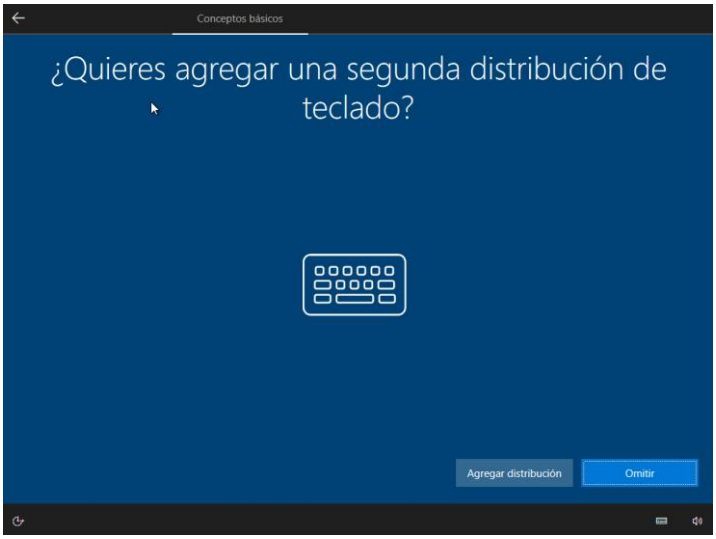
   9.1. Al momento de que aparezca la siguiente ventana se debe seleccionar el país en este caso se selecciona Ecuador. Una vez seleccionado el país se debe dar clic en “Si”.



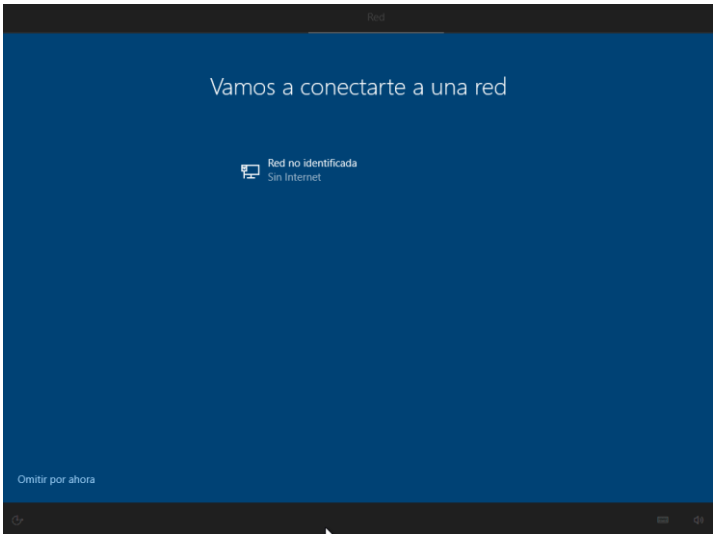
9.2.En la siguiente ventana aparecerá la configuración del teclado en este caso se seleccionará “Estados Unidos”, ya que el teclado con el cual se está trabajando es norteamericano.



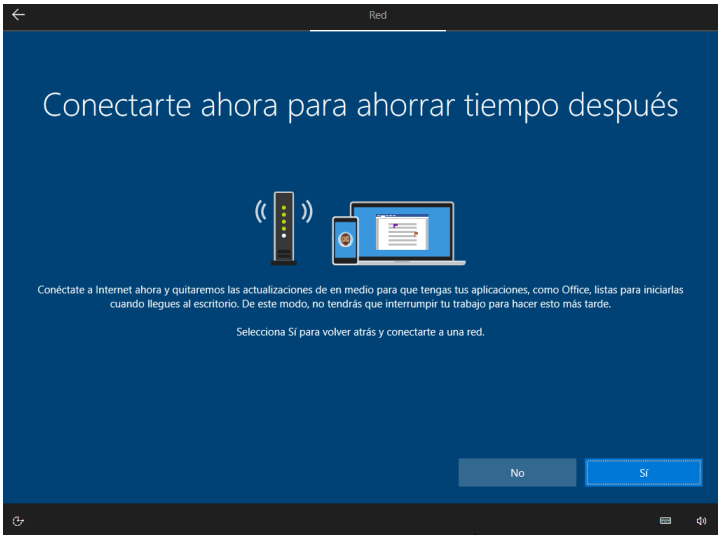
9.3.En la siguiente ventana Windows pregunta si la distribución de teclado esta correcta caso contrario se puede agregar una nueva distribución, pero en este caso ya se tiene seleccionado el tipo de teclado por lo cual se da clic en siguiente.



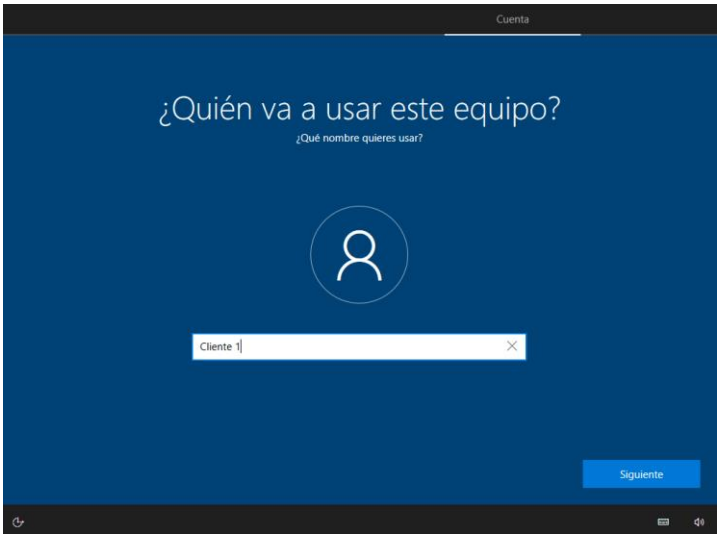
9.4. En la siguiente ventana en caso de disponer de una tarjeta wifi o una red mediante cable esta aparecerá para seleccionar dicha red en este caso se selecciona “Omitir por ahora”.



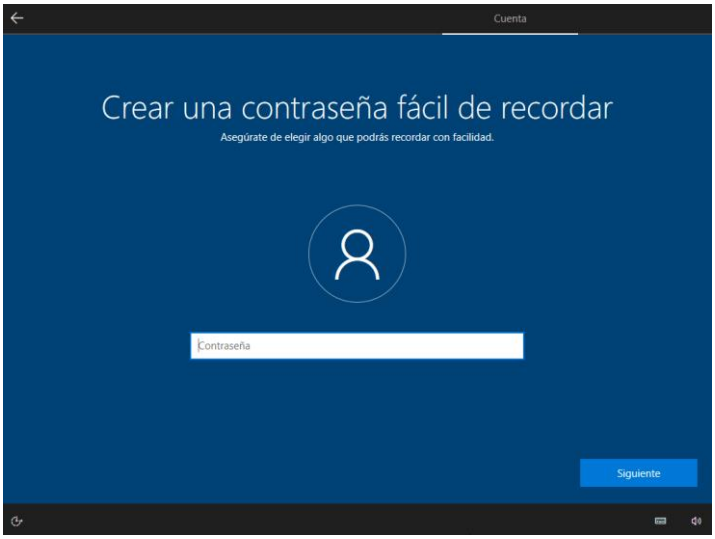
9.5. En la siguiente ventana se selecciona la opción de no pues el equipo virtual no está conectado al momento a ninguna red.



9.6. En la siguiente ventana se realiza el paso **"9.4."** y **"9.5.",** pues por defecto una vez reiniciado el equipo pide una nueva confirmación para el acceso a una red, por lo cual se procede con los pasos anteriormente mencionados y automáticamente se despliega la siguiente ventana en la cual se detalla un usuario y se debe dar clic en siguiente.



9.7. En la siguiente ventana nos pedirá una contraseña, pero en ese espacio en este caso será dejado en blanco y se debe dar clic en siguiente.



9.8.Como paso final se seleccionar el tipo de configuración que va a tener dicha maquina en este caso serán desactivadas todas las opciones. Una vez deshabilitada todas las opciones se seleccionará la opción aceptar.

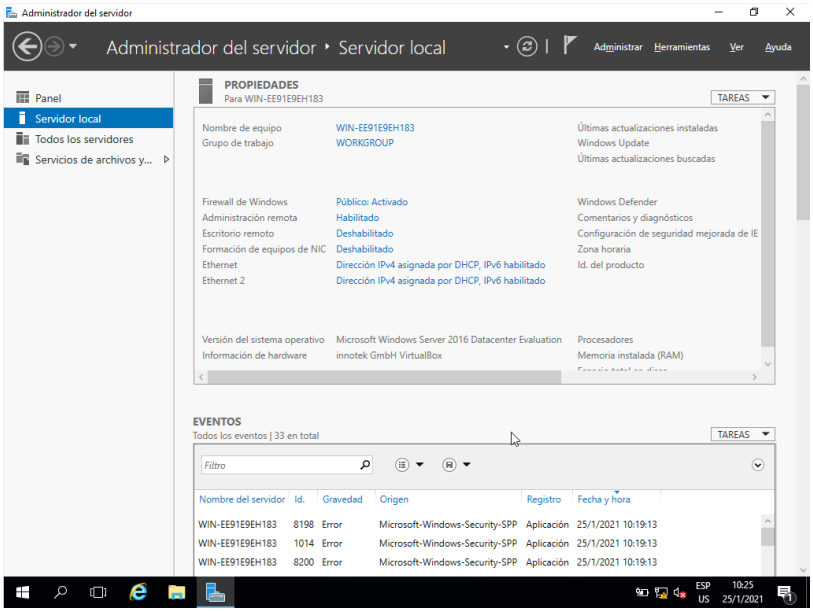
9.9. Como paso final solo se debe de esperar a que la pantalla desplegada finalice y se tendrá una interfaz limpia como la que se puede apreciar a continuación.

Anexo 3

Tareas post instalación del servidor

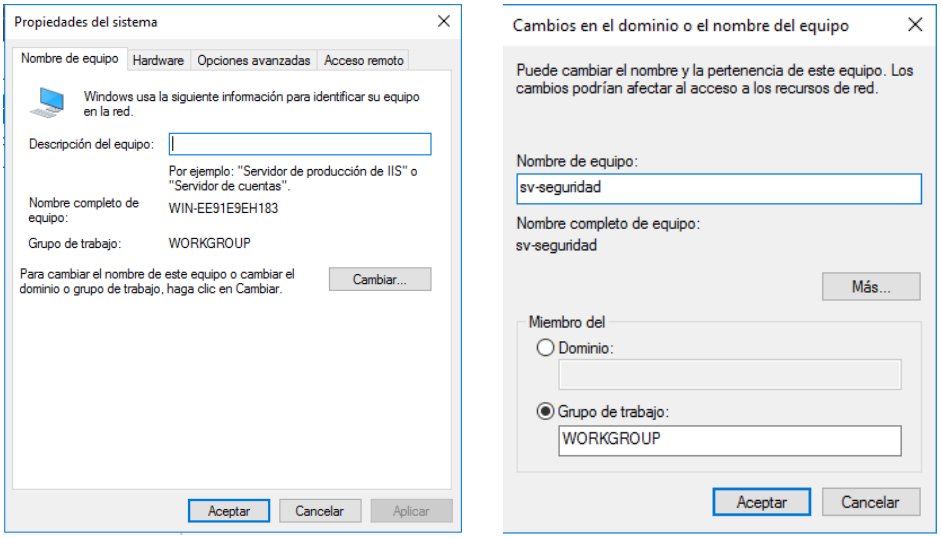
En esta parte se realiza las tareas post instalación de Windows server 2016, esto se debe realizar después de cualquier instalación de servidor Windows.

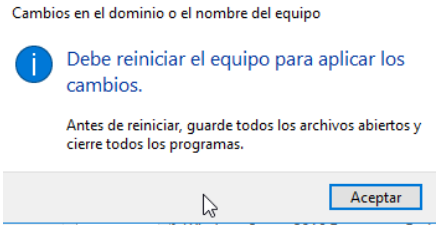
1. Dentro del panel de administración de tareas se selecciona la opción “Configurar este servidor local” la cual desplegara la siguiente ventana.



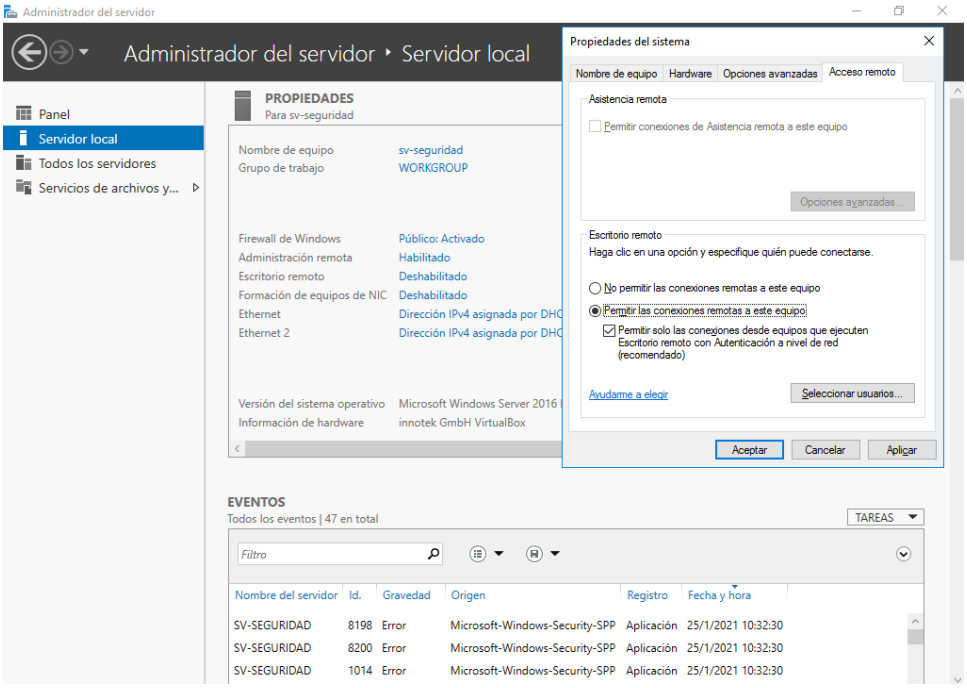
En esta ventana se debe de realizar los siguientes cambios entre los cuales se debe cambiar el nombre del servidor la cual en este caso se re nombrara a “sv-seguridad” por lo cual se da clic en las letras azules las cuales están en mayúsculas con las iniciales WIN, una vez seleccionado aparecerá la

siguiente ventana en la cual se selecciona “Cambiar” y se desplegará otra ventana en la cual cambiaremos el nombre que estaba por el antes mencionado. Una vez cambiado se selecciona la opción de aceptar y el equipo pedirá que para que los cambios sean efectuados se debe de realizar un reinicio por lo tanto se debe aceptar la ventana emergente.

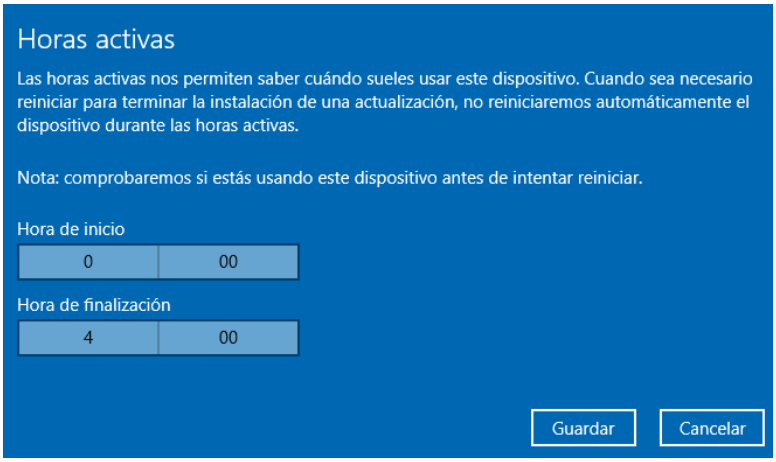




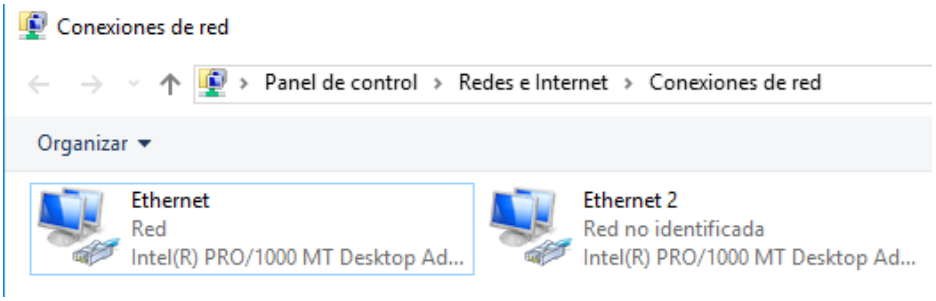
2. Como paso siguiente se debe realizar la habilitacion del escritorio remoto puesto que esta viene desabilitada por defecto, en este caso se sigue la misma logica que el paso anterior por lo cual se debe de dar clic en las letras azules y se desplegara una ventana en la cual se seleccionara la opcion “Permitir las conecciones remotas a este equipo”, una vez terminado el proceso se procede a dar clic en “Aceptar”.



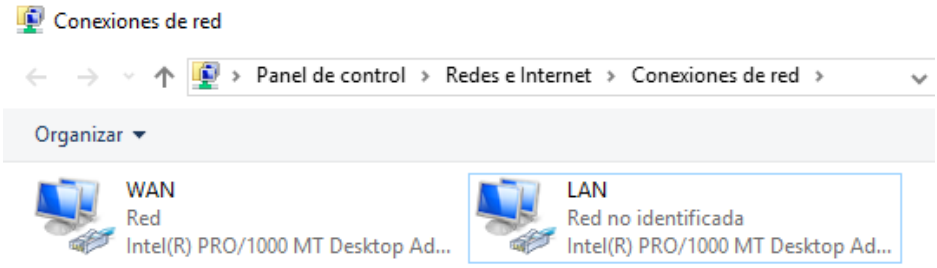
3. El siguiente paso es cambiar la manera en la que se realizan las actualizaciones por lo tanto se procede a cambiar la hora de actualizacion y la fechas de actualizacion a su vez que tipo de actualizaciones se desea tener. Esta configuracion se puede apreciar en las siguientes imágenes.



4. Como siguiente paso se procede a la identificación de las tarjetas de red las cuales una será la que proporcione internet y la segunda la cual está atada a la red interna.



En este caso la primera tarjeta será la cual nos está suministrando internet y la segunda es la cual nos entregara la red LAN. Por lo cual se cambia los nombres de las mismas para poder identificarlas de mejor manera.

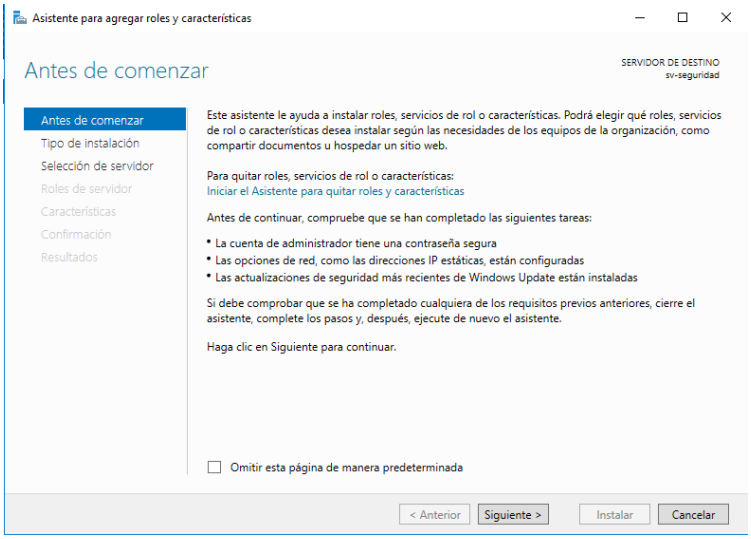


Anexo 4

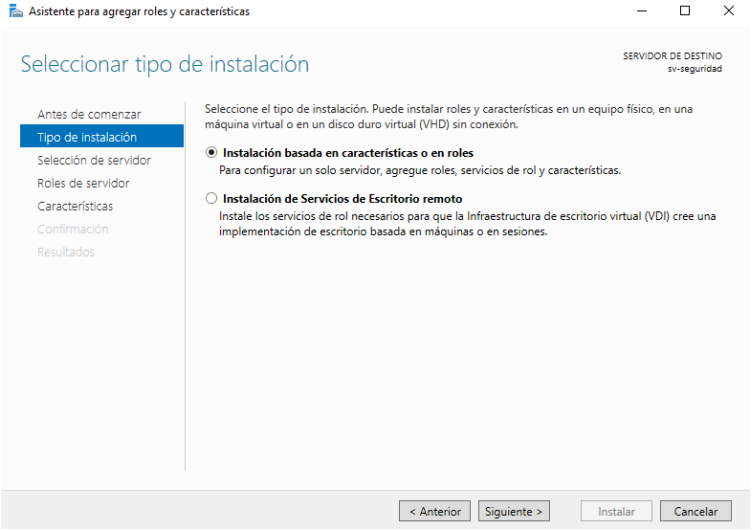
Instalación de servicios en Windows server 2016

Instalación de Active Directory (Directorio Activo)

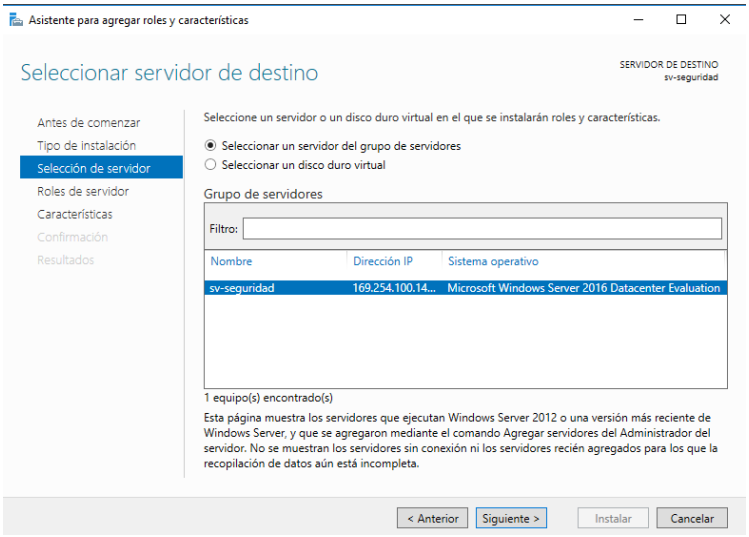
1. Para la instalación de AD se debe de abrir la ventana de administrador del servidor en el cual se selecciona la opción de “Agregar roles y características”, la cual desplegara la siguiente ventana.



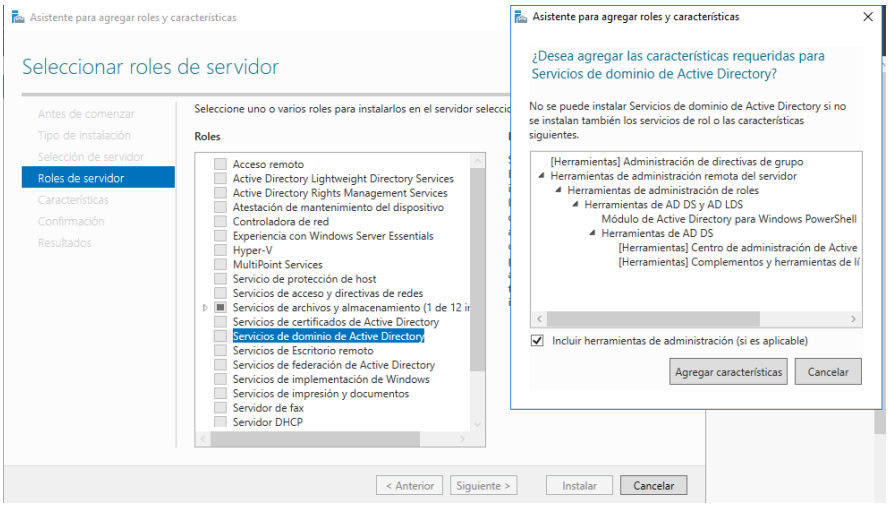
2. Dentro de esta ventana se selecciona la opción de siguiente lo cual enviara a la otra ventana en la cual aparece dos opciones las cuales son: “Instalación basada en características o roles” e “Instalación de servicios de escritorio remoto” por lo cual se selecciona la primera opción y se da clic en “siguiente”.



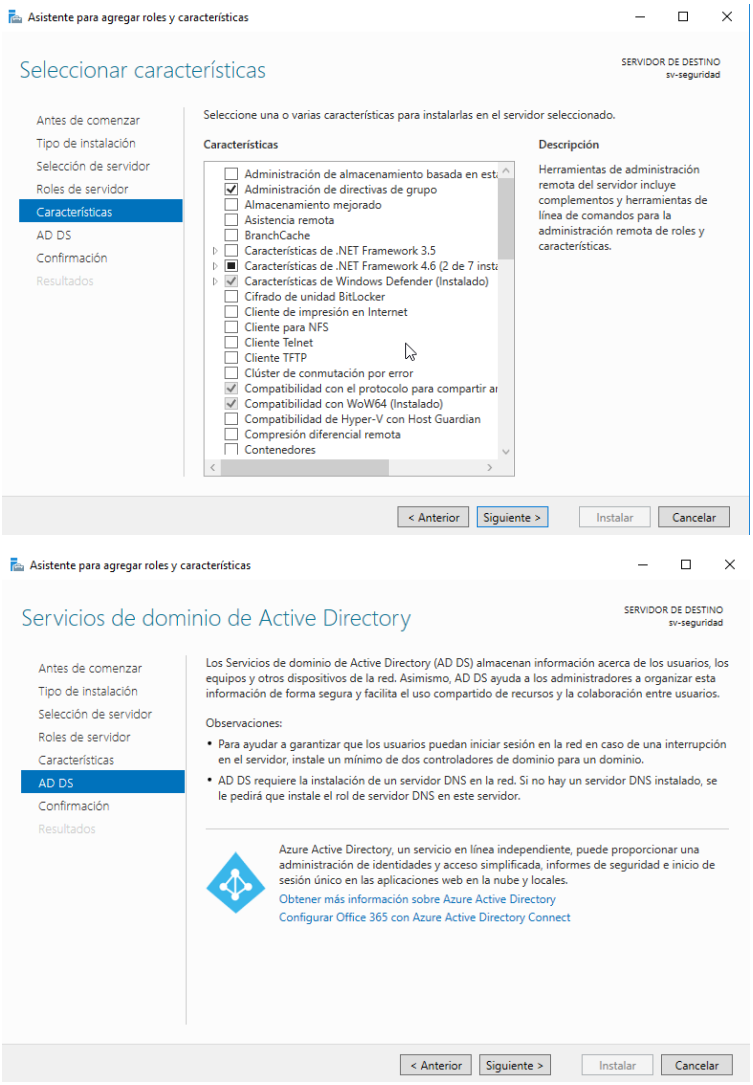
3. Como paso siguiente se debe escoger el servidor en el que se desea instalar el servicio por lo cual se selecciona el servidor actual y se coloca siguiente.



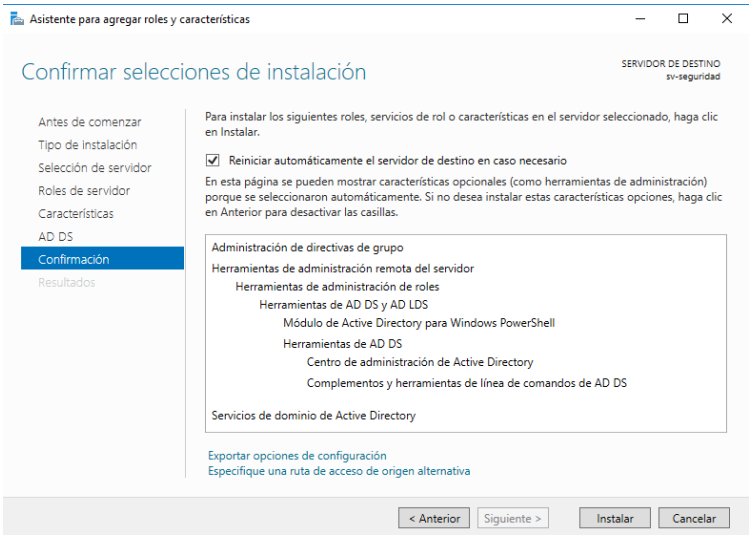
4. Una vez realizado la selección del servidor se desplegar una ventana en la cual aparecen todos los roles y características que se desea instalar por lo cual se selecciona la opción que dice “Servicios de dominio de active directory”, una vez seleccionado aparecerá una ventana emergente la cual detalla los servicios que van a ser instalados lo cual se debe dar clic en la opción “Agregar características”.



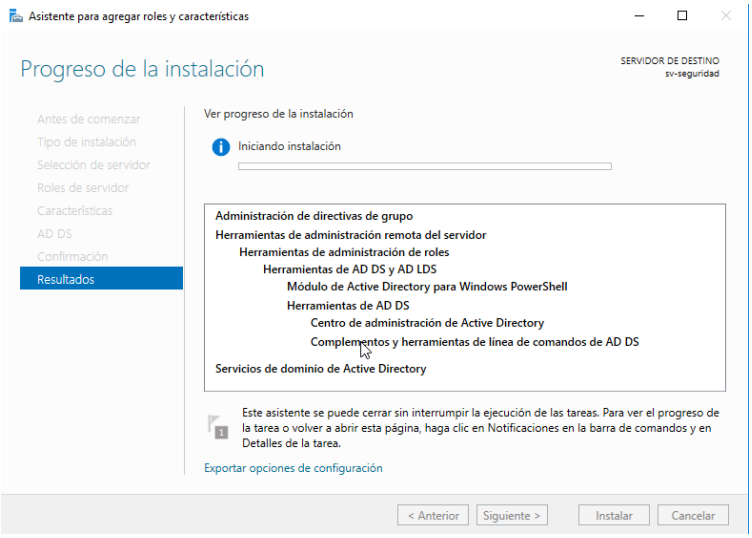
5. El proceso siguiente va ser una ventana en la cual muestra las características que van a ser instaladas. Se selecciona siguiente a las dos ventanas que se muestran a continuación.



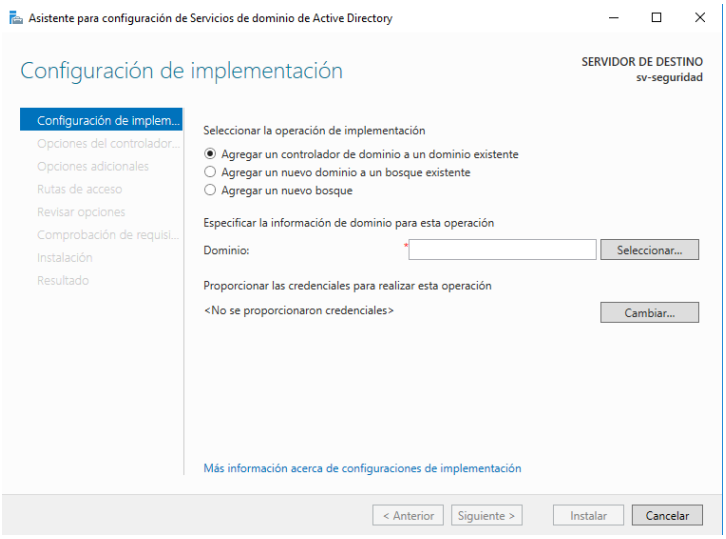
6. Para finalizar el proceso de instalación en la ventana siguiente se debe colocar “Reiniciar automáticamente de destino en caso necesario” y colocar en siguiente por lo cual este proceso de instalación se tardará varios minutos dependiendo de la velocidad del disco duro.



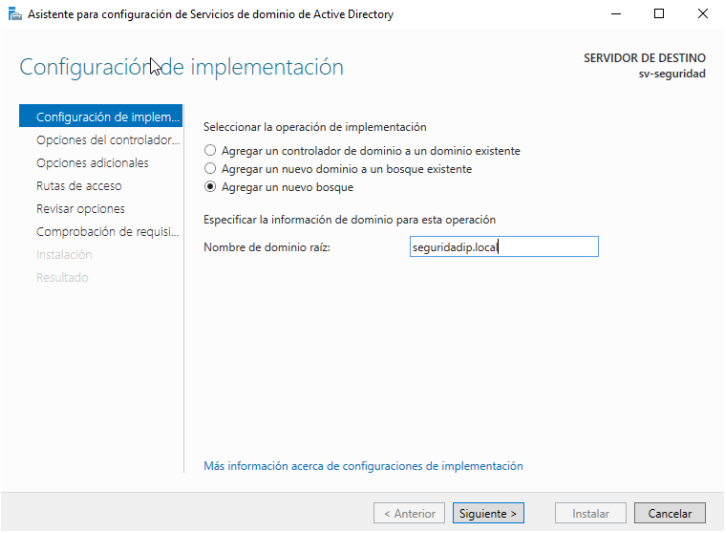
7. Una vez terminado la verificación de todo lo que se va a instalar se colocara “Instalar” y el proceso empezara.



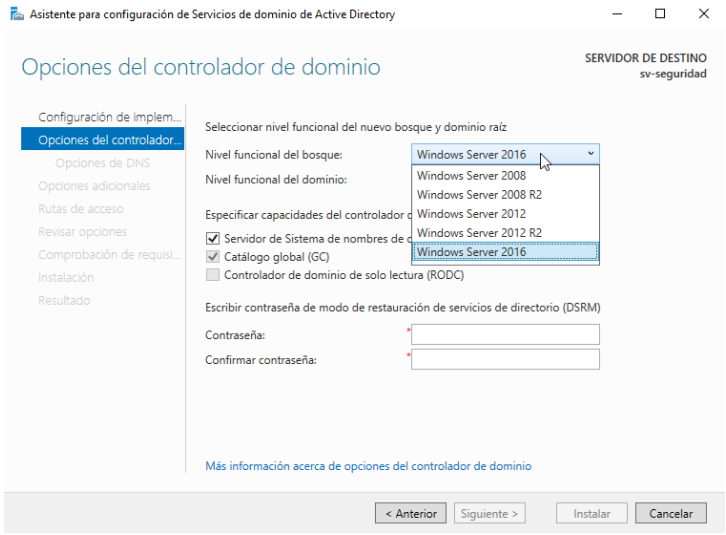
8. Una vez finalizado el proceso de instalación se debe realizar seleccionar la opción que dice “Promover este servidor a controlador de dominio” en el cual aparecerá la siguiente ventana.



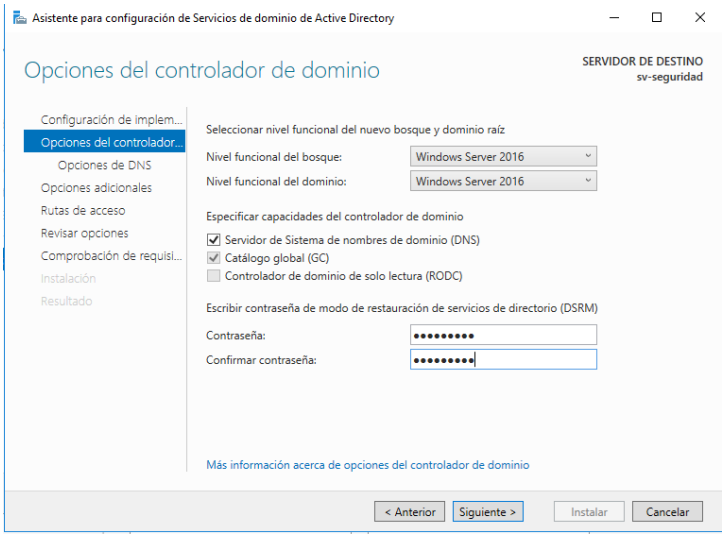
8.1. En este caso se procede a que este servidor sea un controlador de dominio por lo cual se selecciona “Agregar un nuevo bosque” en el cual se detallara el nombre de “seguridadip.local”. Dar clic en siguiente.



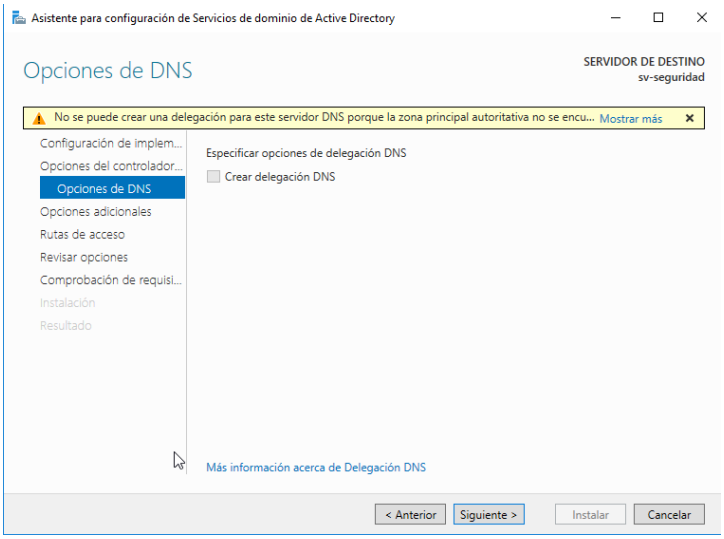
8.2. En la siguiente ventana se puede apreciar el nivel de funcionamiento de este servicio en este caso se selecciona Windows server 2016, pero a su vez puede ser compatible con Windows server 2012R2.



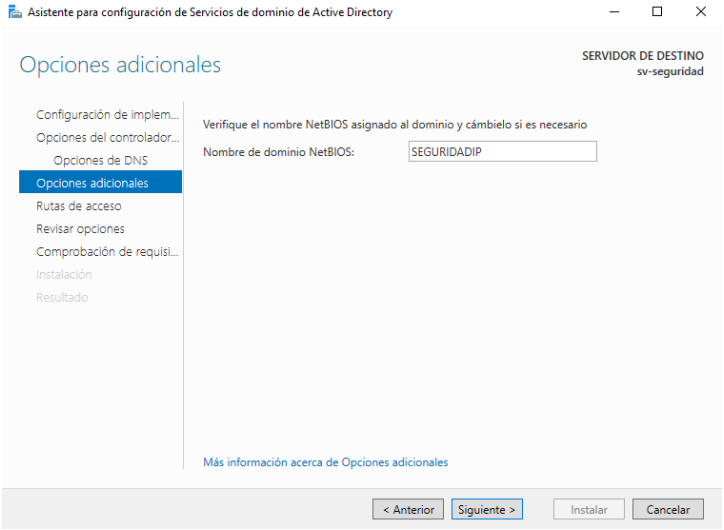
8.3. Dentro de esta ventana se realiza la configuración de la contraseña que va a tener por lo cual se establece una contraseña segura comprendida de números y letras. Dar clic en siguiente para proseguir con el proceso.



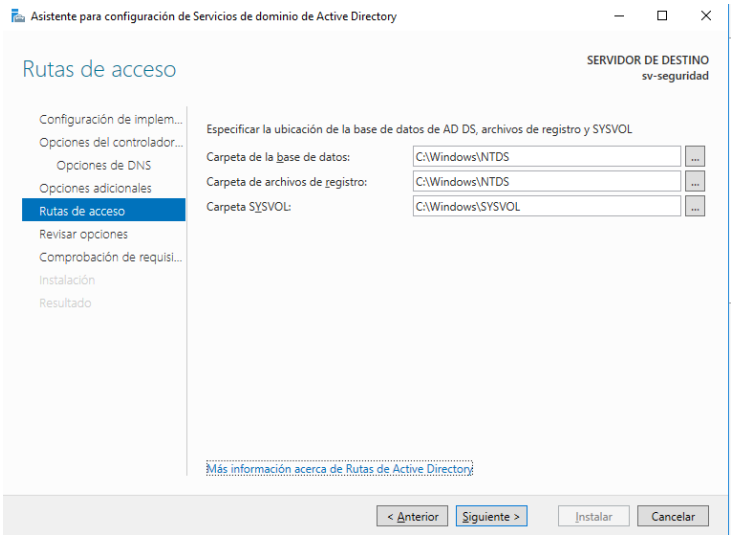
8.4. En la siguiente ventana daremos clic en siguiente para poder realizar una configuración después en caso de ser necesaria.



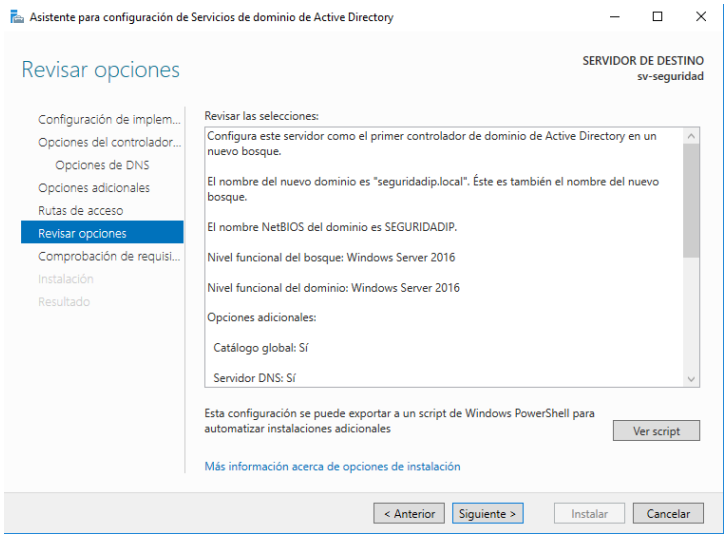
8.5. En el siguiente proceso nos deberá dar el nombre de dominio que hemos colocado al momento de colocar el nuevo árbol. Dar clic en siguiente para proseguir con la configuración.



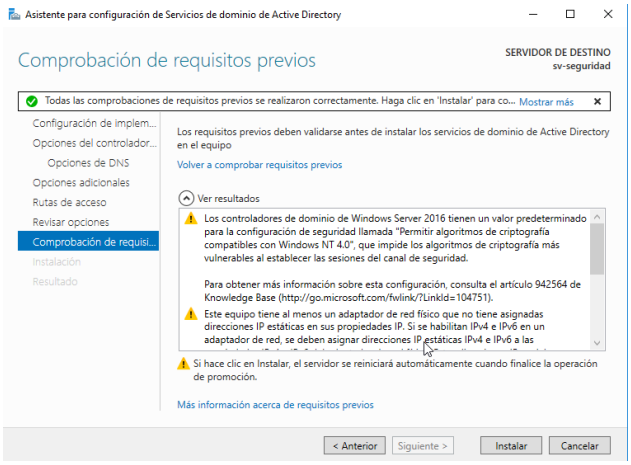
8.6. En las ventanas siguientes nos aparecerá las direcciones en las cuales se especifica las bases de datos del AD y la carpeta de archivos de registro por lo cual se dejará por defecto en este aspecto. En este caso se deja por defecto esta situación al ser un laboratorio de pruebas por lo general en un servidor de producción se deben cambiar la ubicación de las carpetas.

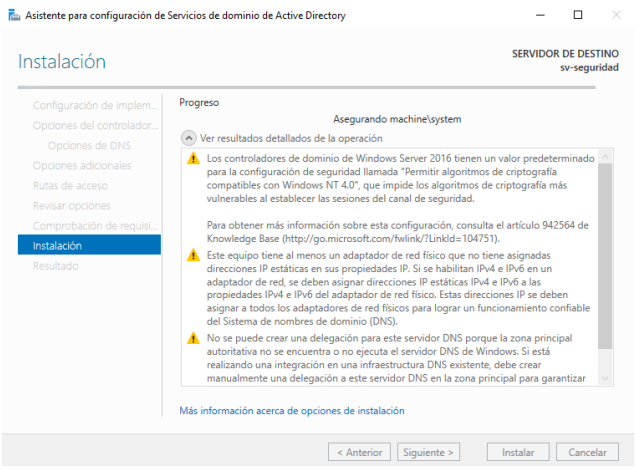


8.7. Para finalizar la instalación nos mostrara una ventana en la cual aparece un resumen de lo que se ha realizado. Dar clic en siguiente para continuar con la implementación.

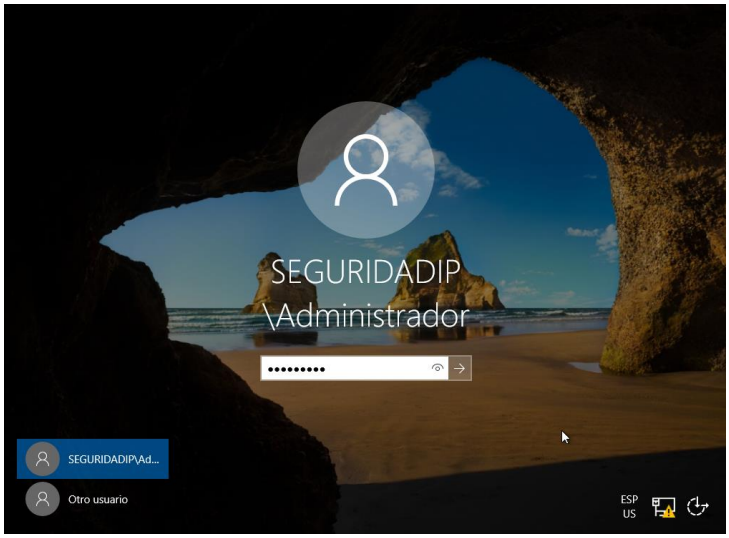


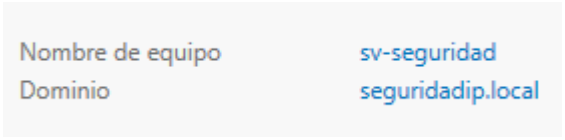
8.8. Aparecerá una ventana en la cual nos muestra lo que se va a instalar dentro del servidor por lo cual se da clic en instalar para seguir con la instalación y finalizar el proceso.

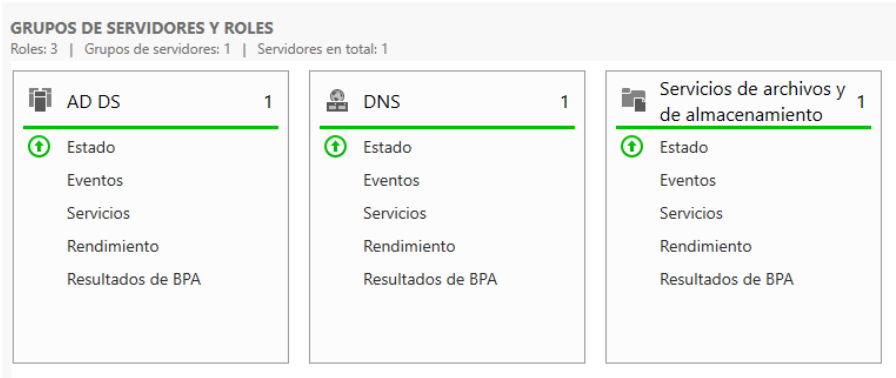




9. Una vez finalizado los procesos anteriores el servidor se reinicia y se procede a la comprobación del servicio AD instalación dentro del panel principal de administración del servidor, a su vez se puede apreciar al momento de iniciar la pantalla principal de Windows server el nombre de dominio.



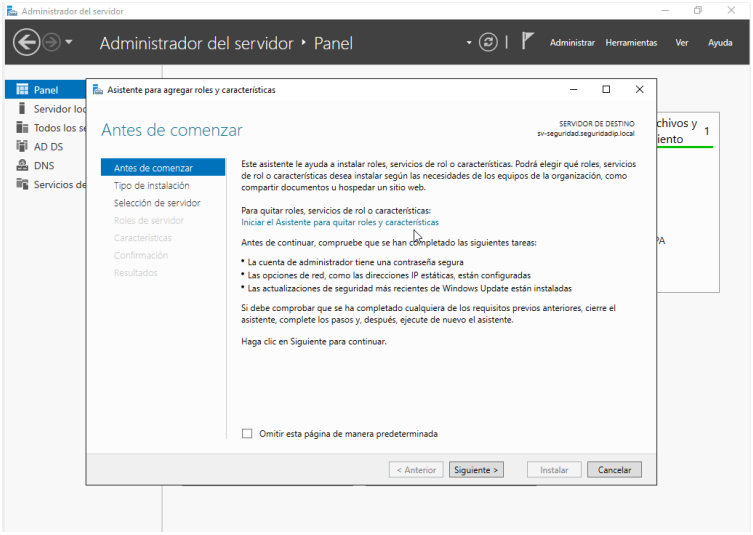




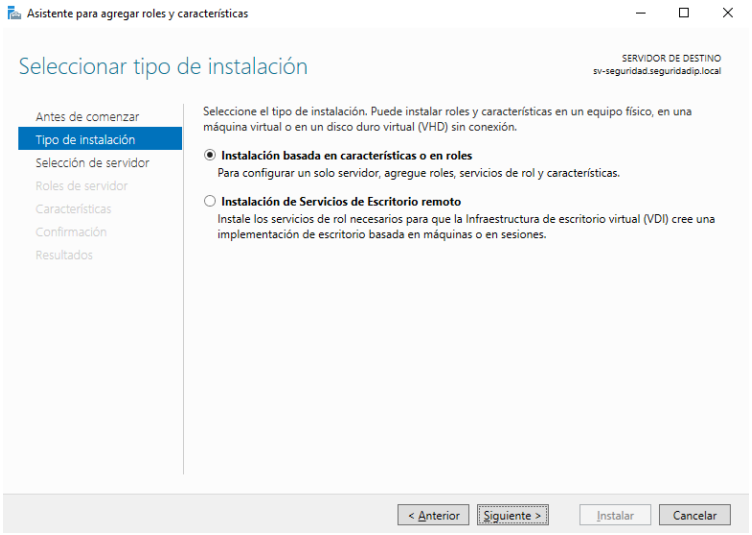
Anexo 5

Procedimiento para la Instalación de DHCP

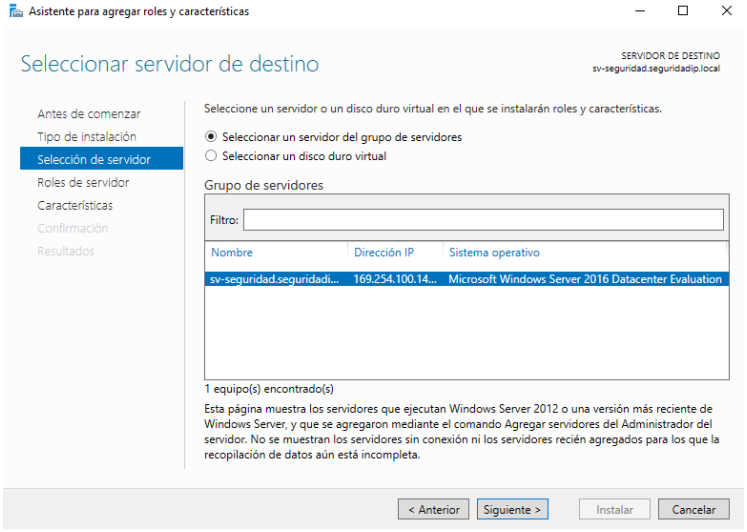
1. Para la instalación de DHPC se debe ingresar a la ventana de administración del servidor y agregar roles y características en la cual aparecerá la siguiente ventana la cual se pudo apreciar en el **Anexo 4,** a su vez se realiza procesos similares.



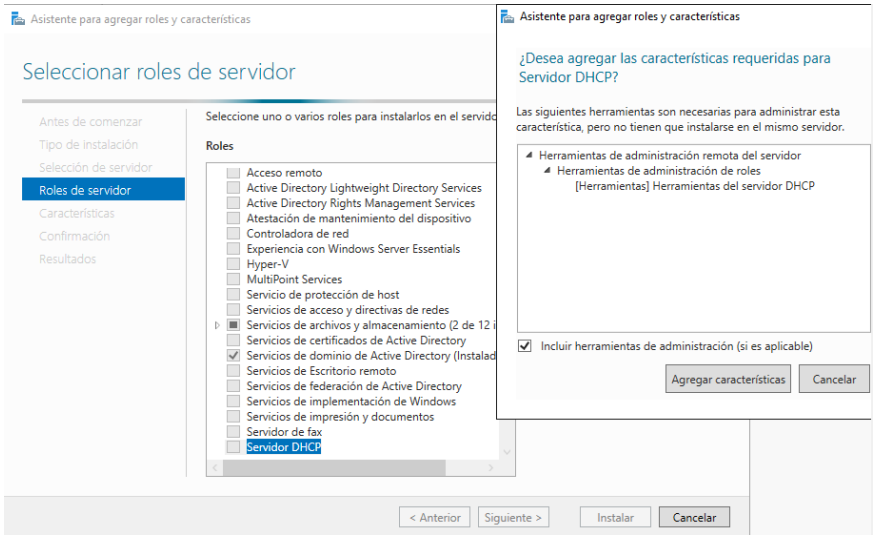
2. Se coloca instalación de basada en características o en roles y dar clic en siguiente.



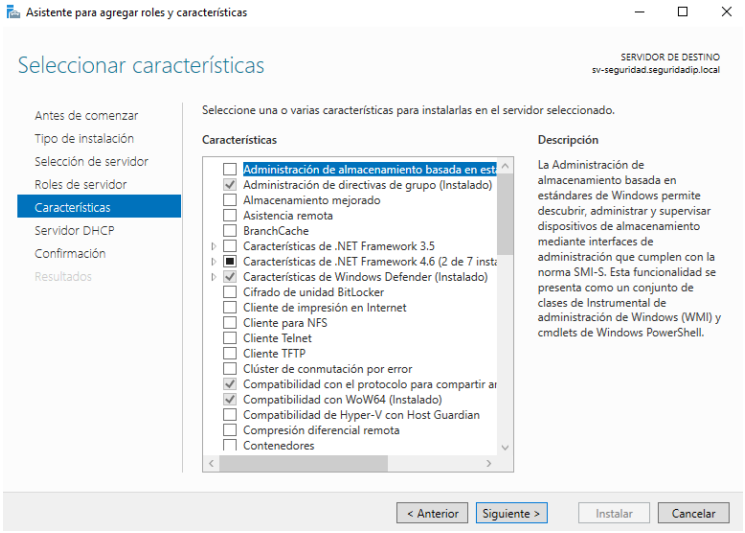
3. Siguiendo con los pasos necesarios se selecciona el servidor en el cual se instala dicho servicio por lo cual se selecciona el servidor, se procede a dar clic en siguiente.



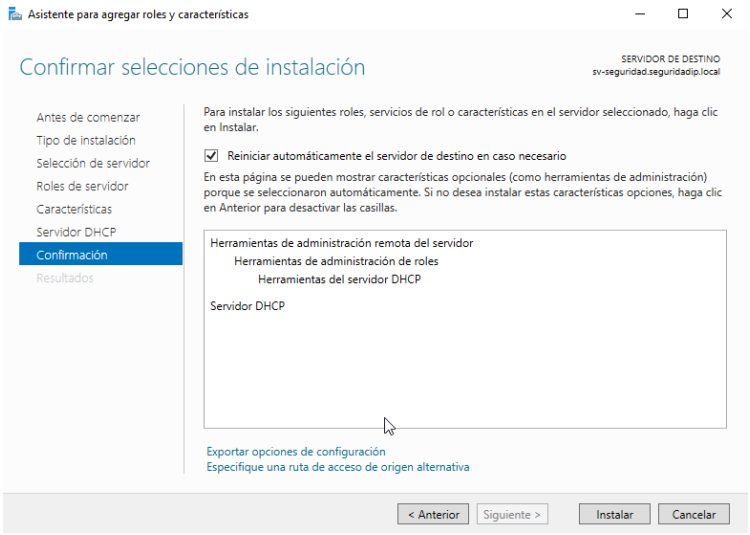
4. Una vez seleccionado se realiza la instalación de servidor DHCP y conjuntamente aparecerá una ventana emergente la cual indican las características dentro de este servicio. Por lo cual se selecciona “Agregar características” y dar clic en siguiente.



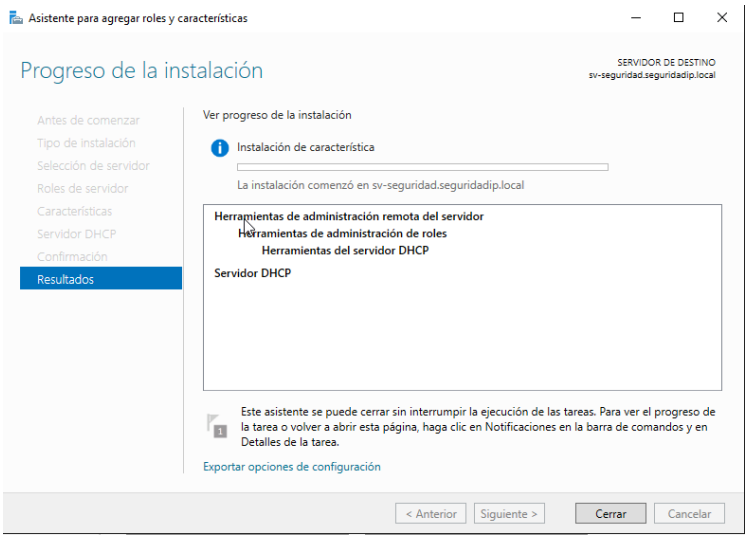
5. En la siguiente ventana se coloca siguiente para proseguir con el proceso de instalación.



6. Una vez seleccionado las características del servidor por lo cual se debe seleccionar la opción de “Reiniciar automáticamente el servidor de destino en caso necesario” y seleccionar la opción instalar.

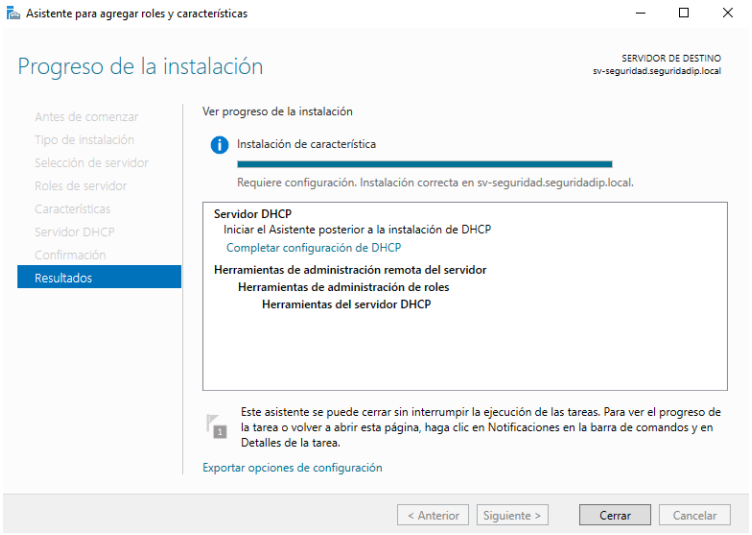


Una vez el proceso inicie la ventana el proceso de instalación.

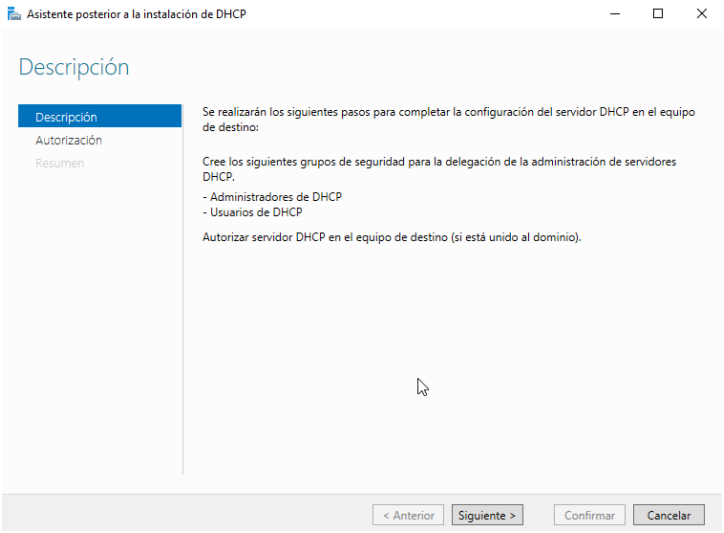


7. Para completar la instalación del servidor se da clic sobre la opción “Completar configuración de DHCP”

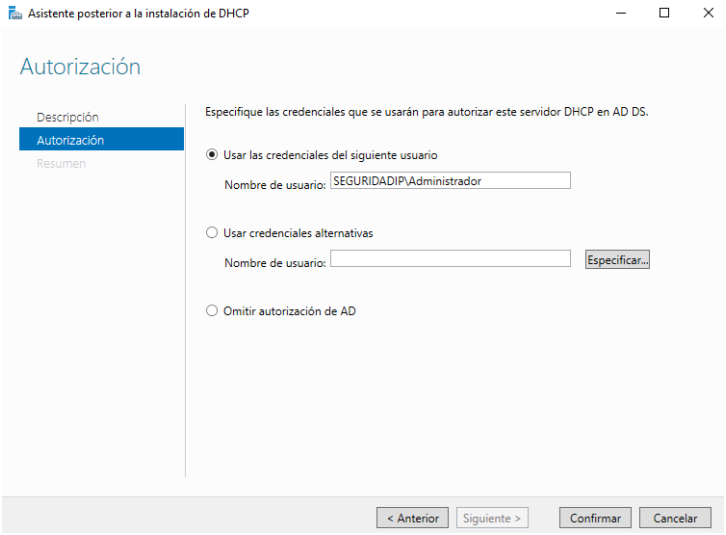
   7.1. En este proceso se prosigue con la siguiente ventana la cual aparecerá lo siguiente.



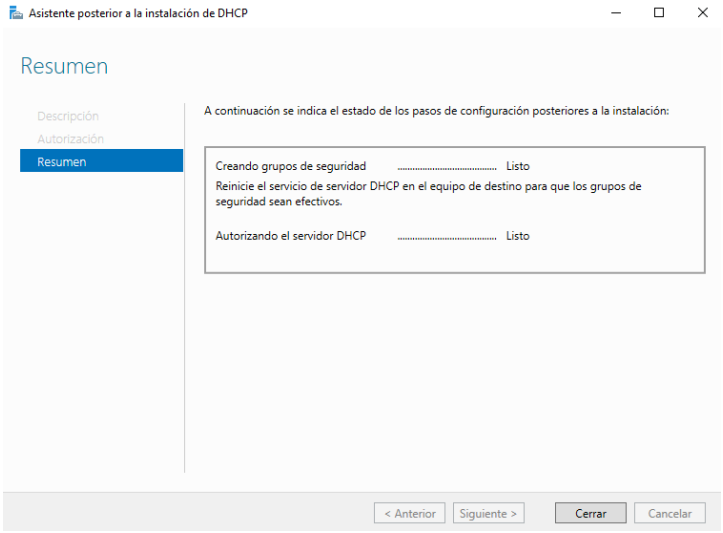
7.2. En la siguiente ventana que se despliega en la cual se debe dar clic en siguiente.



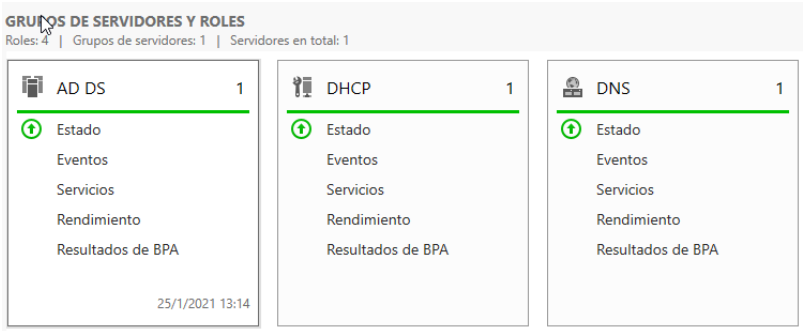
7.3.En la siguiente imagen se en donde se muestran las credenciales las cuales se utilizará, por lo cual se da clic en confirmar.



7.4. La siguiente ventana aparecerá en la cual muestra el estado del servicio DHCP, por lo cual se debe dar clic en cerrar.



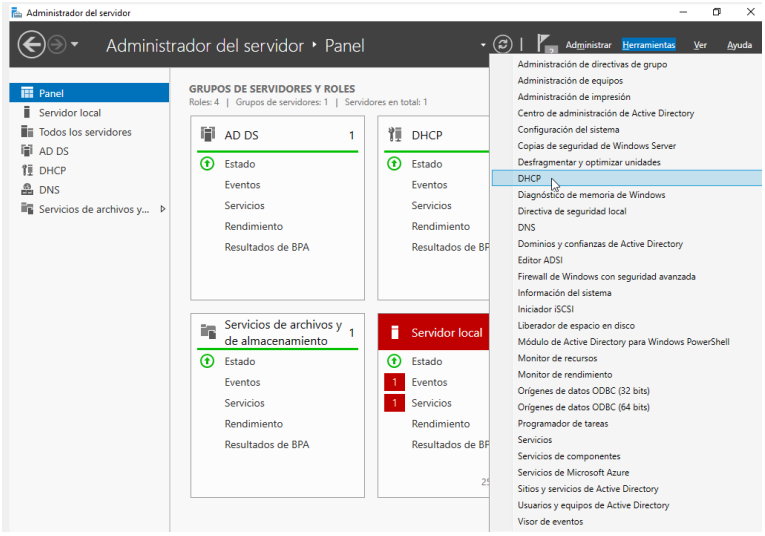
8. Una vez finalizado el proceso el servicio aparece dentro de panel central el cual se muestra el estado activo del mismo en el cual está en verde por lo cual está funcionando correctamente.



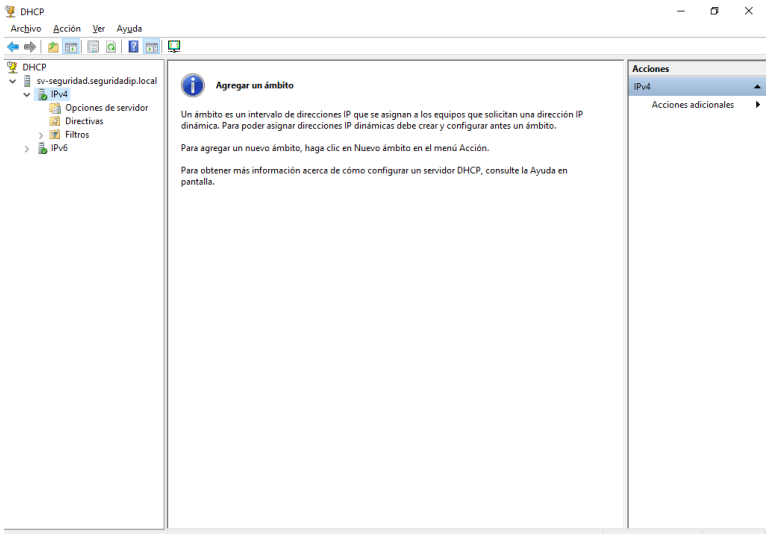
Anexo 6

Configuración de DHCP

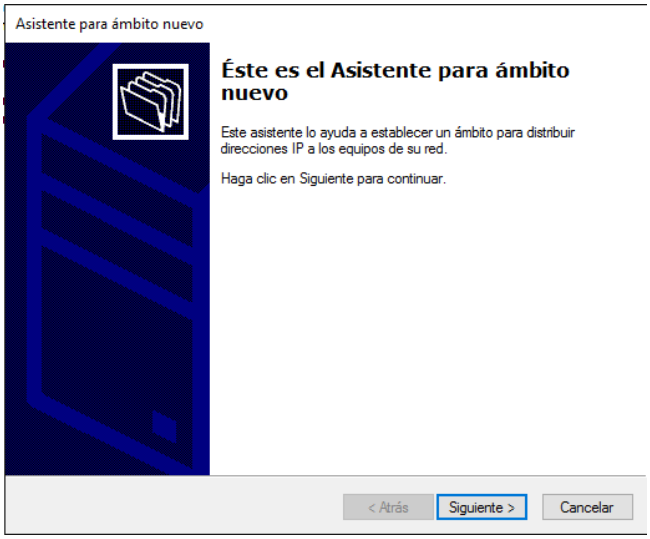
1. Dentro del administrador del servidor se selecciona la opción de herramientas en al cual se dará clic sobre la opción de DHCP para su configuración.



2. La ventana emergente que acaba de aparecer es el entorno de configuración del servicio DHCP, en la cual se creara un nuevo ámbito en IPV4.



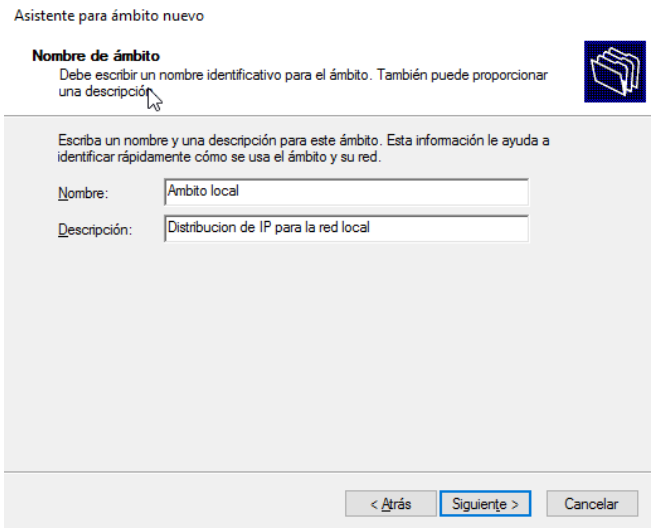
3. Al momento de realizar clic derecho sobre IPv4 aparecerá las opciones necesarias para lo cual se selecciona la opción de “Nuevo Ámbito” en la cual aparecerá una ventana en la cual se debe dar clic en siguiente para continuar con el proceso de configuración.



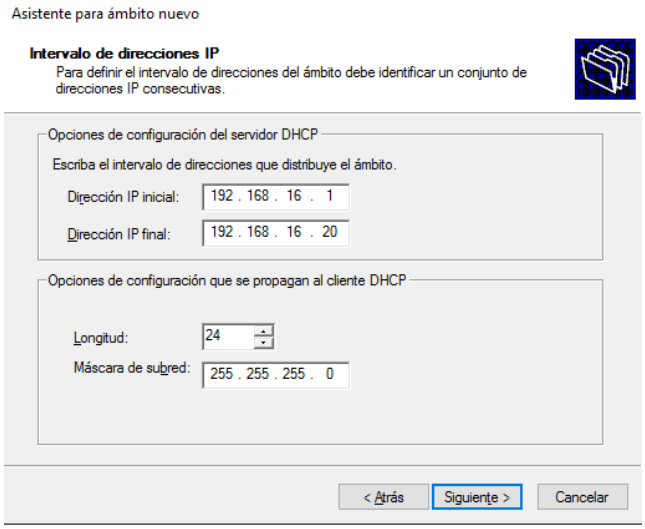
4. Siguiendo con la configuración nos solicita que coloquemos un nombre en el ámbito y una pequeña descripción para lo cual se colocara lo siguiente:

   Nombre: Ámbito local

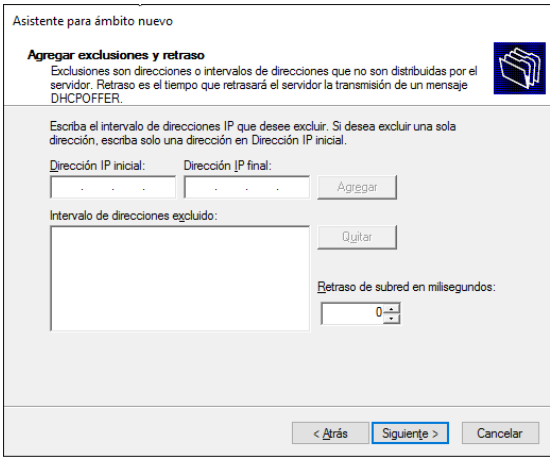
   Descripción: Distribución de IP para la red local

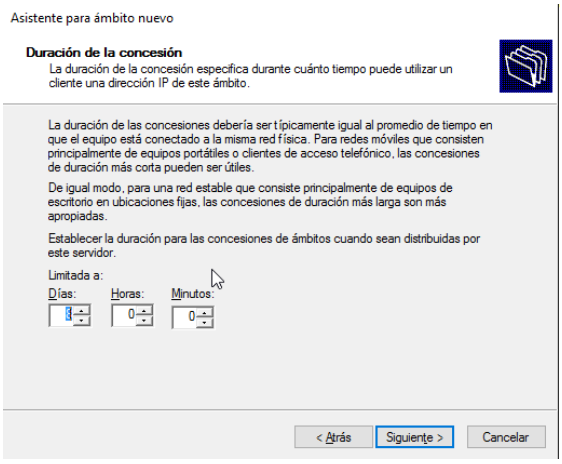


5. Una vez realizado la descripción y la colocación del nombre se procede a realizar la configuración de del intervalo de las Ip que serán asignadas dentro de la red local, para lo cual se establece un rango inicial desde 192.168.16.1 y la final 192.168.16.12, conjuntamente con una longitud de 24 y una máscara de subred la cual es 255.255.255.0. Se procede a colocar siguiente para continuar con la configuración.

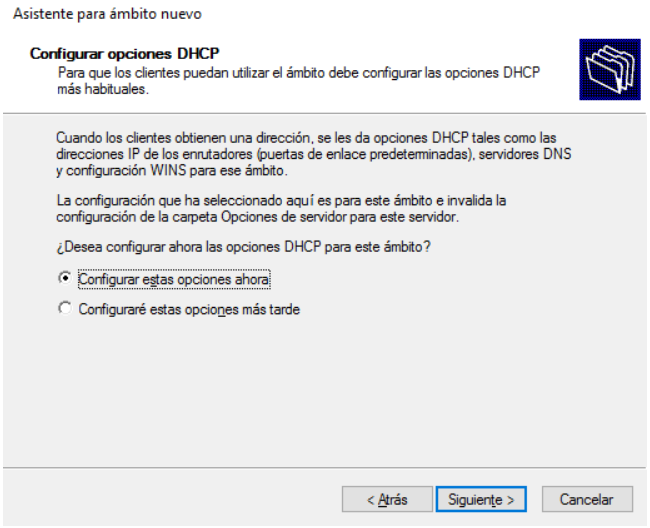


6. Las siguientes ventanas se realizará la configuración por defecto.

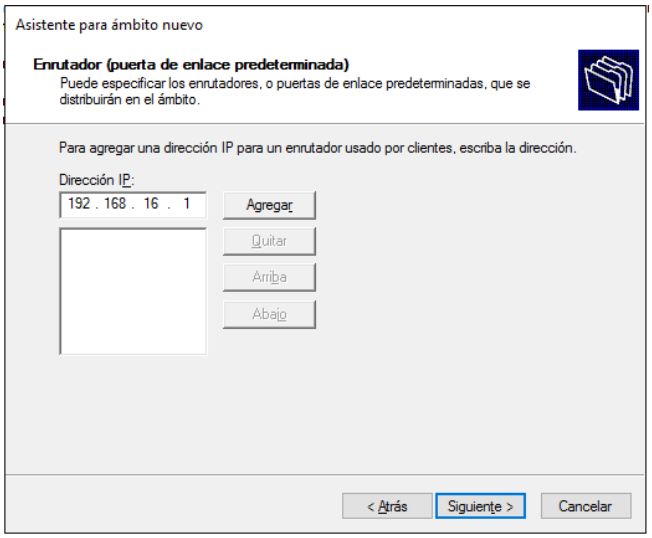




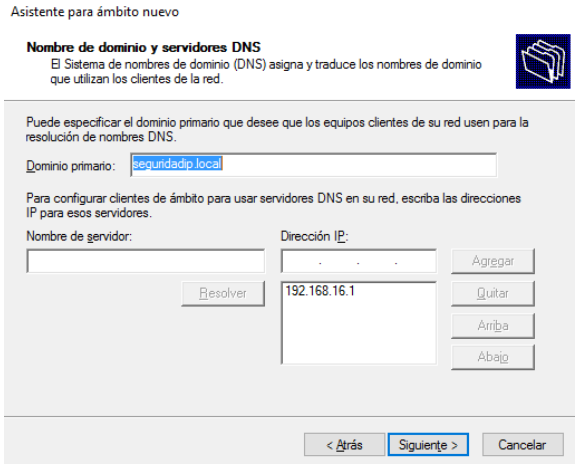
7. Ahora se procede a la configuración de las opciones de DHCP para lo cual dentro una ventana nos menciona si se desea configurar ahora o más tarde, por lo cual se seleccionará configurar ahora.



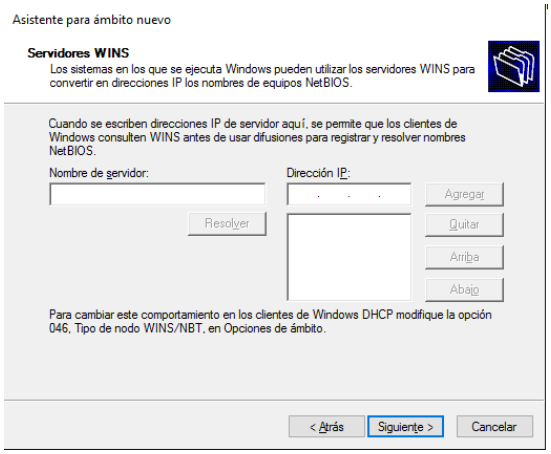
8. En este punto se colocará la dirección IP la cual servirá para el enrutamiento el cual aún no está configurado, pero se lo realizará más adelante, pero por el momento se configura de la siguiente manera. Por lo cual se selecciona la opción Agregar y siguiente.



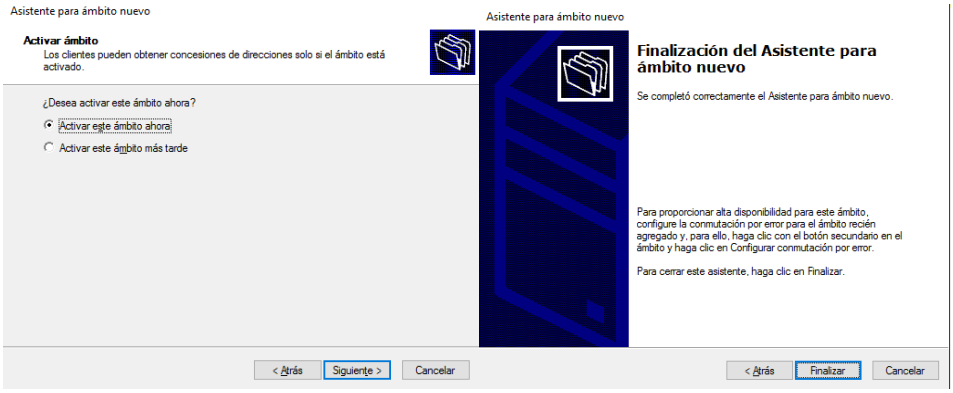
9. En la siguiente ventana se puede apreciar el nombre del servidor de DNS y la IP en la que esta se encuentra en este caso se da en el botón agregar y siguiente.



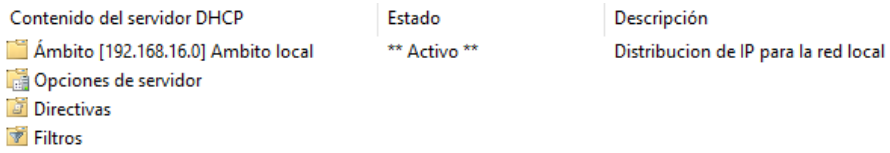
10. En la siguiente ventana lo que se debe realizar es dar clic en siguiente pues esa configuración se quedara por defecto.



11. Para finalizar Windows nos pregunta si se desea activar el ámbito ahora y por lo cual se selecciona la opción activar ámbito ahora y dar siguiente y finalizar para acabar con la configuración del servicio DHCP.



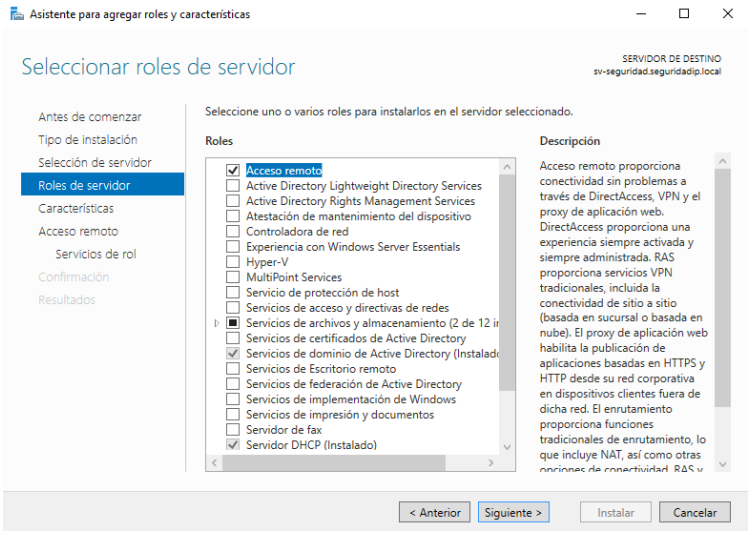
12. Una vez finalizado el proceso se debe de verificar cual es el estado del servicio y confirmar si esta **“Activado”.**



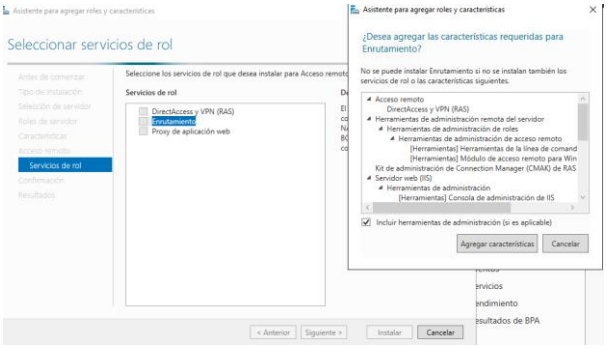
Anexo 7

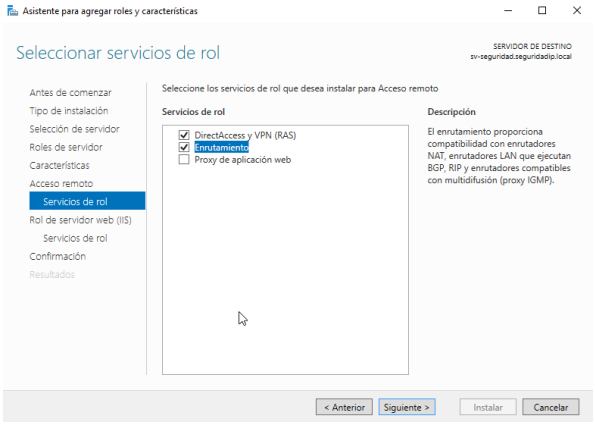
Instalación del servicio de enrutamiento

1. Para la instalación de este servicio se realiza de la misma manera que los anteriores anexos, por lo cual se dirige de manera directa a escoger el Rol llamado **“Acceso remoto”.**

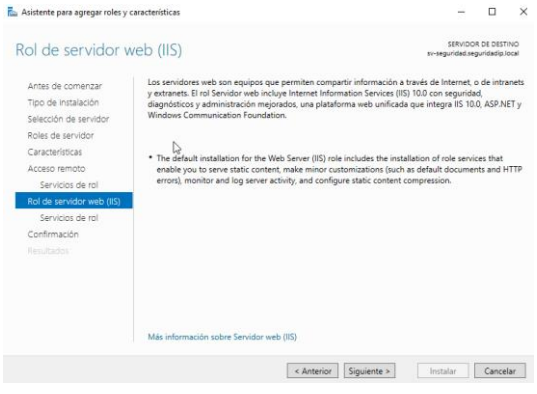


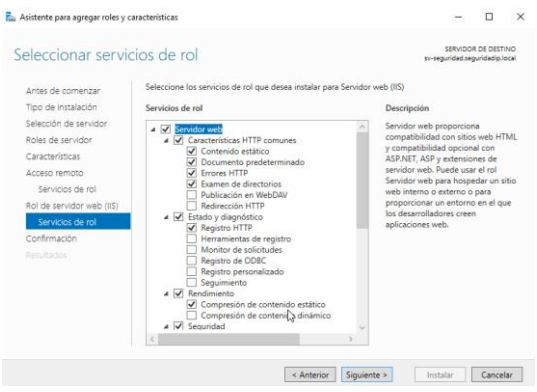
2. Por lo cual se selecciona de manera directa los servicios de rol en el cual se selecciona la opción de enrutamiento y agregar las características por necesarias que ofrece el asistente en este caso este enrutamiento sirve para para proveer de internet a los demás equipos a través del servidor.



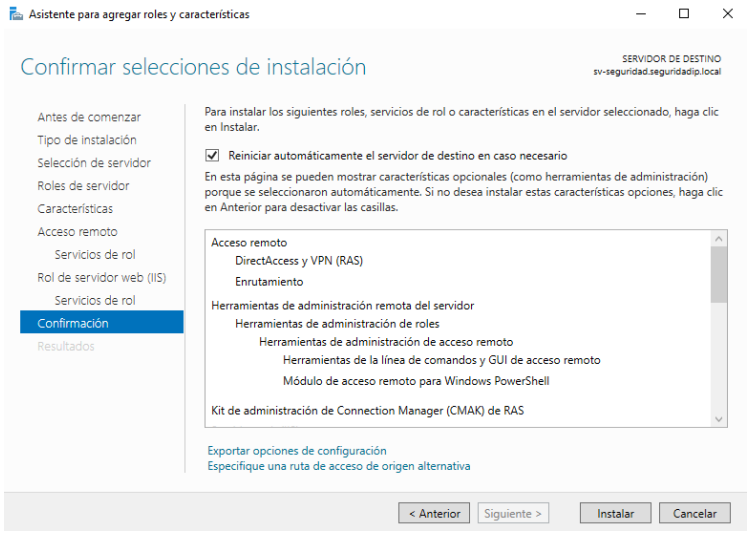


3. Las siguientes opciones las dejaremos por defecto para la configuración que se realizara más adelante por lo tanto las siguientes ventanas deben de ser dado clic en siguiente.

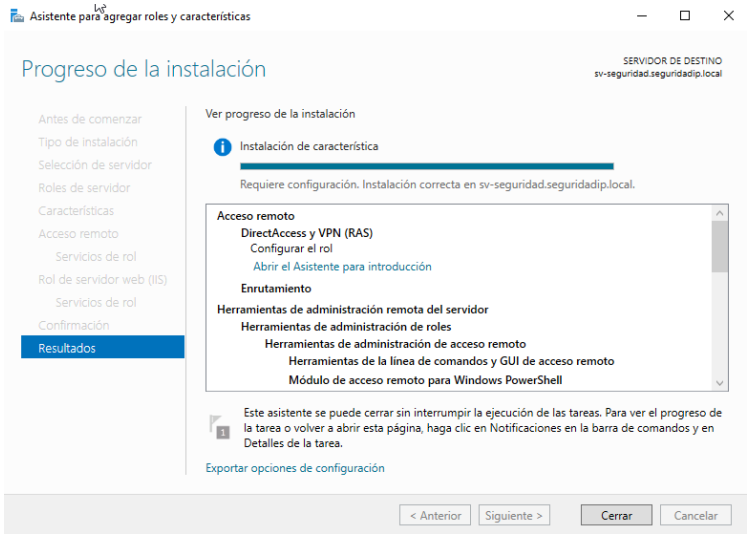




4. En la siguiente imagen se selecciona la opción de reiniciar el servidor automáticamente y luego dar clic en instalar.



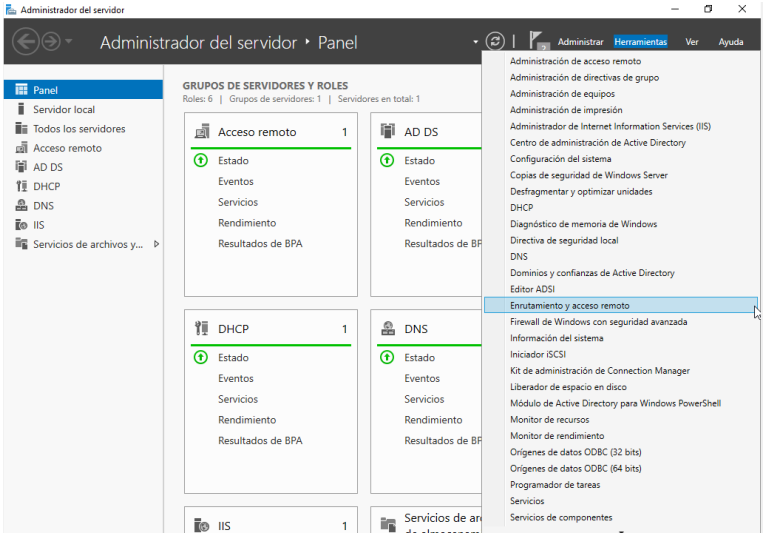
5. Una vez aparece la siguiente imagen hay que colocar la opción de cerrar.



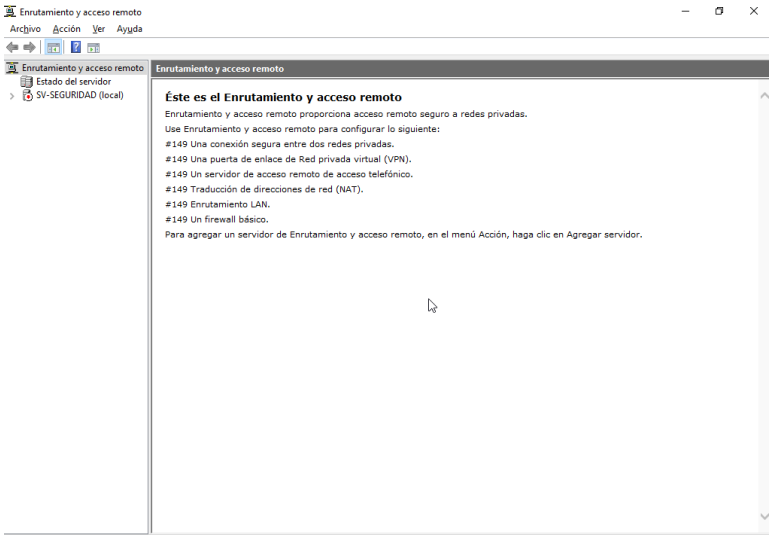
Anexo 8

Configuración de enrutamiento y acceso remoto

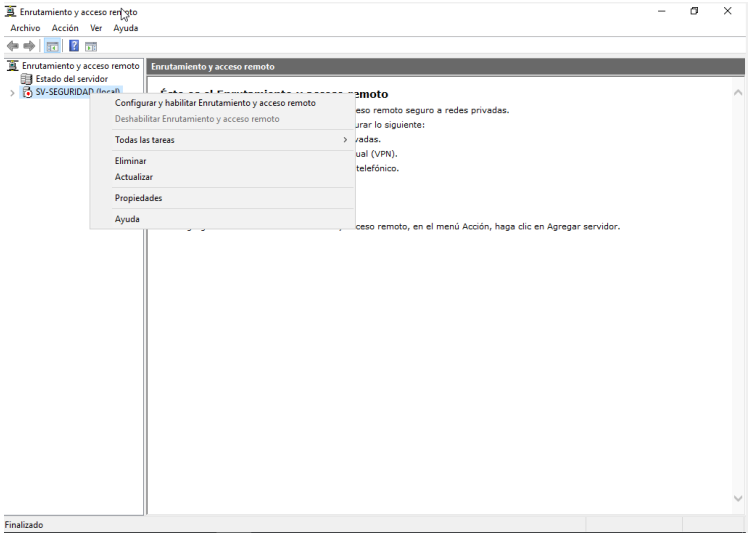
1. Para la configuración del enrutamiento se debe abrir la ventana de administración del servidor en el cual se debe seleccionar la opción herramientas y buscar la opción que dice “Enrutamiento y acceso remoto”.



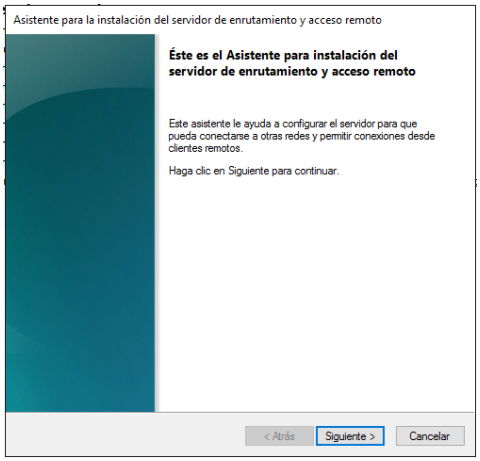
2. Una vez aparezca la siguiente imagen debe de aparecer en la parte izquierda con una flecha roja la cual significa que está instalado mas no configurado.



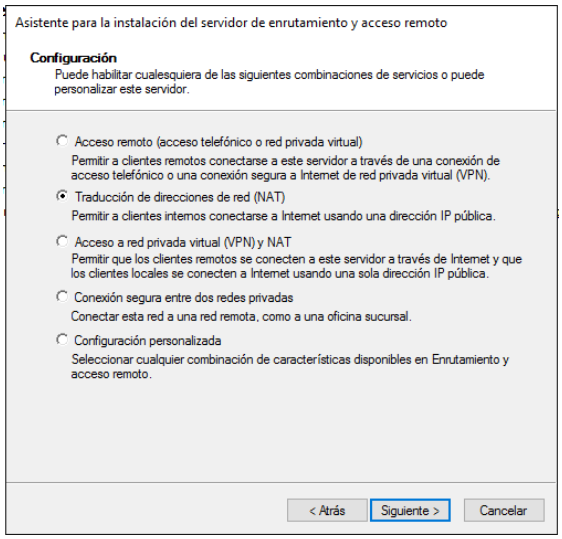
3. Por lo tanto, se debe dar clic derecho sobre el nombre del servidor y seleccionar “Configurar y habilitar Enrutamiento y acceso remoto”.



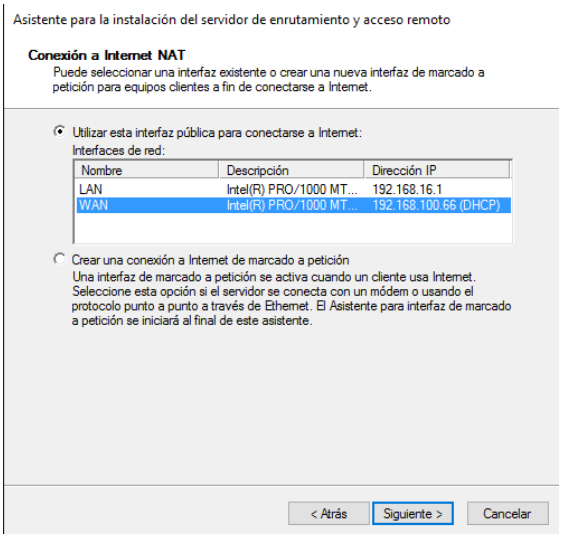
4. En la siguiente imagen el paso a seguir es dar siguiente.



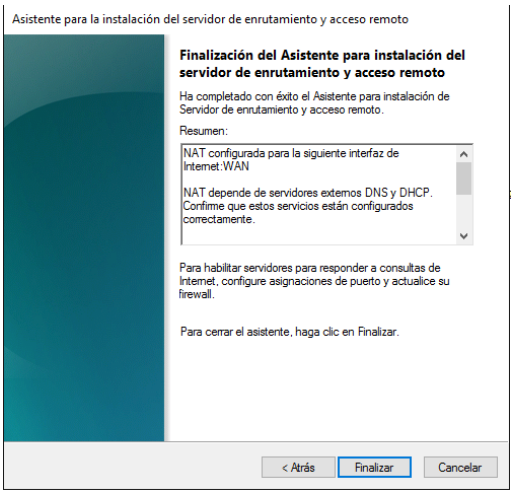
5. En la siguiente imagen lo que hay que seleccionar es “Traducción de direcciones de Red NAT”, para que los equipos conectados a la red tengan acceso a internet.

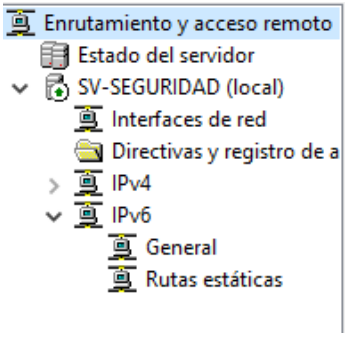


6. Una vez seleccionada la opción se debe seleccionar la tarjeta de red que está proveyendo de internet en este caso es WAN y siguiente.



7. Una vez finalizados los procesos solo hay que colocar finalizar. Por lo cual aparece la siguiente imagen la cual ya esta subida.





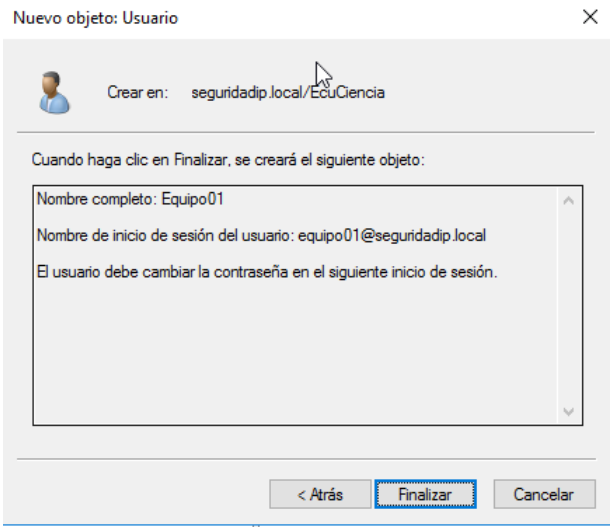
Anexo 9

Configuración de usuarios en una unidad administrativa

1. Para la configuración correspondiente primero se debe crear una unidad administrativa dentro del servidor en el cual se realiza la creación de usuarios y las contraseñas correspondientes para así poder unirlos a un dominio.
2. Por lo cual nos dirigimos a usuarios y equipos de Active directory para la creación de una nueva directiva, en la cual se da clic derecho sobre el

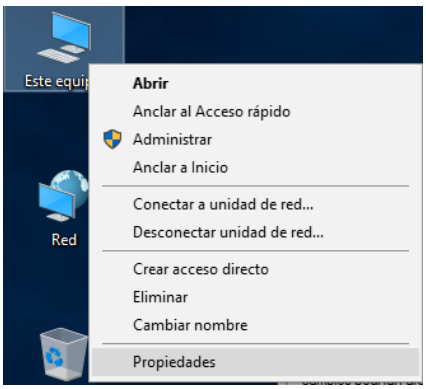
nombre de dominio y se selecciona la opción de nueva unidad organizativa.

3. Una vez creado la unidad organizativa debemos de realizar la creación del primer usuario en este caso el nombre será “equipo01” y la contraseña estará definida mediante las características de contraseñas seguras las cuales son mezcla de letras y números.
4. Una vez creado tendremos los siguientes datos y al usuario creado por lo cual hay que colocar estos datos dentro del cliente.



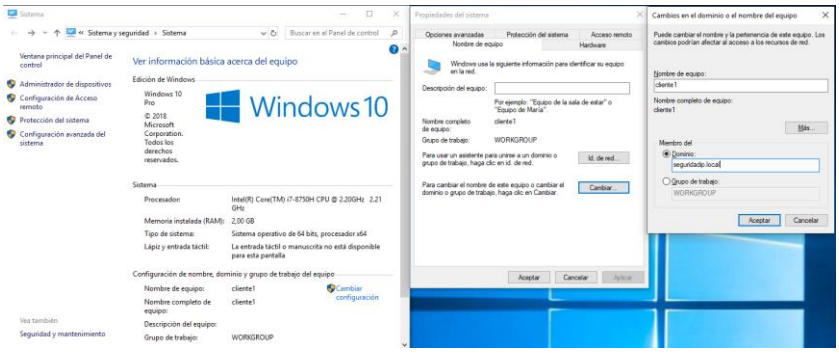
5. En este paso se debe anexar al cliente dentro de nuestro dominio por lo cual dentro del equipo cliente se debe realizar la siguiente configuración:

   5.1. Dar clic derecho sobre el equipo y seleccionar propiedades.

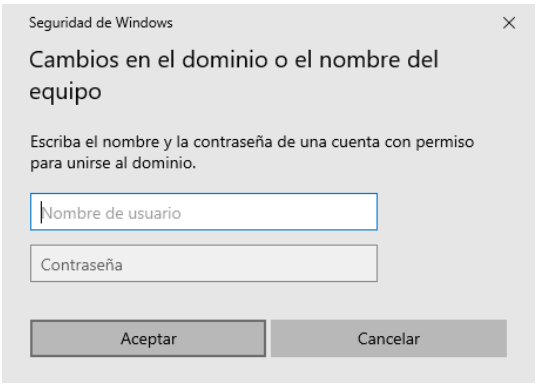


   5.2. Una vez seleccionada la opción de propiedades se despliega una ventana la cual muestra las características del equipo por lo cual se debe ingresar a nuestro dominio mediante la selección de la opción

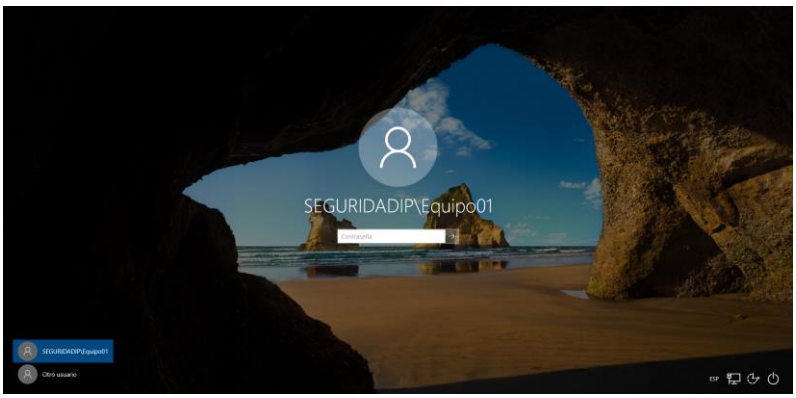
“Cambiar”, se despliega una nueva ventana en la cual se puede colocar el nombre del dominio y dando clic en aceptar.

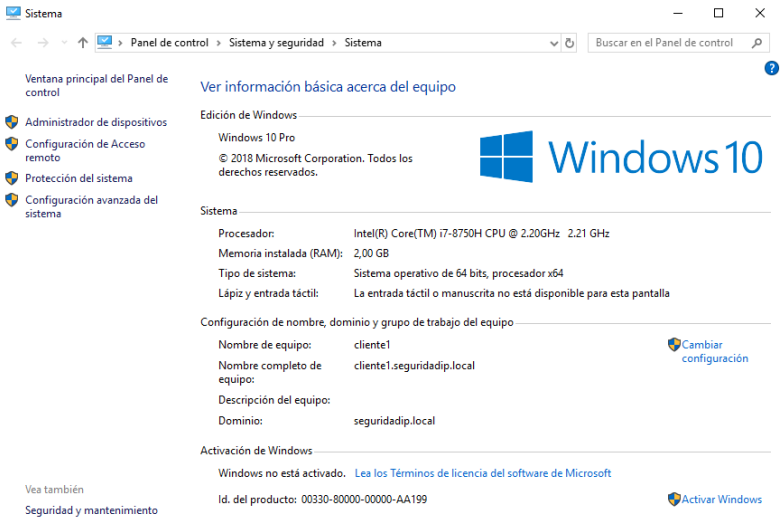


5.3. Una vez realizado este proceso el sistema requerirá las credenciales respectivas tales como el usuario y la contraseña, las cuales han sido creadas para dicho usuario por lo cual se digitan las credenciales necesarias para el ingreso.



5.4. Una vez realizado dicho paso el equipo será reiniciado automáticamente, por lo cual una vez haya terminado dicho proceso aparecerá el nombre del dominio y el usuario el cual esta creado dentro del mismo. Por lo tanto, para ingresar se debe colocar las credenciales respectivas.

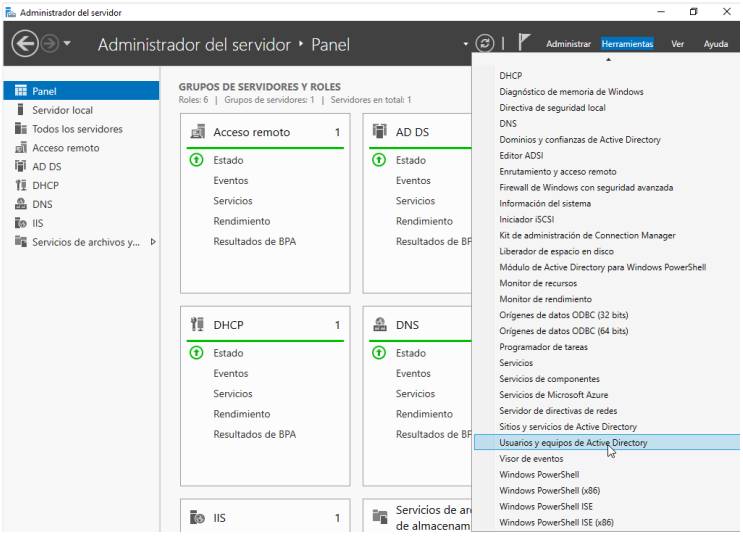




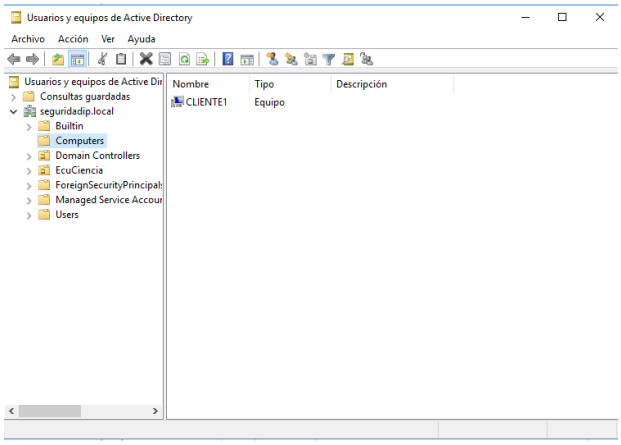
Anexo 10

Configuración de IPSec

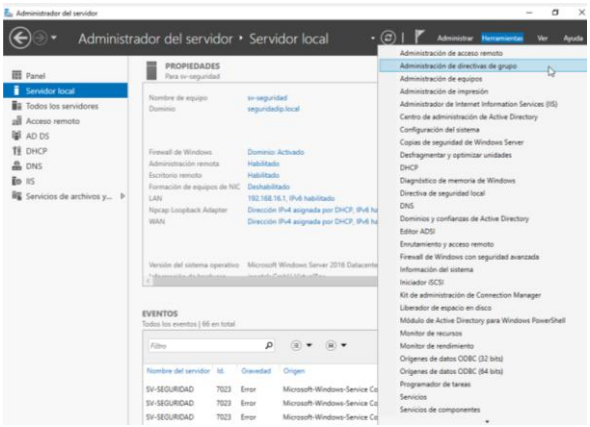
1. Dentro de administración del servidor debemos dirigirnos a la opción de usuarios y equipos de active directory para realizar la configuración necesaria mediante directiva de grupo.



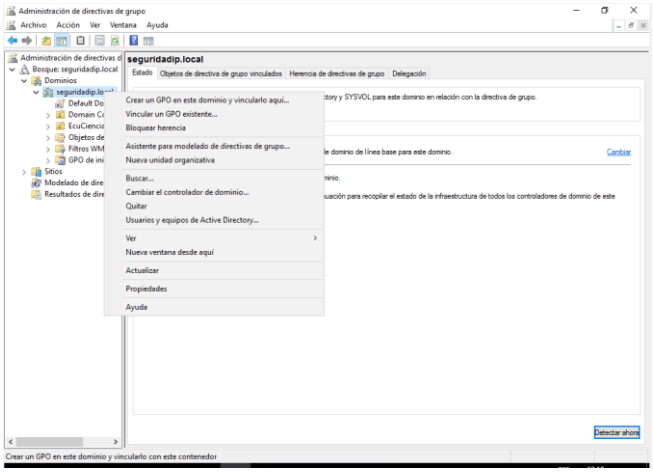
2. Una vez dentro del mismo debemos de verificar que los equipos se encuentren en la carpeta de Computers por lo cual vemos que se encuentra vacío por lo cual se procederá a la colocación de los equipos.



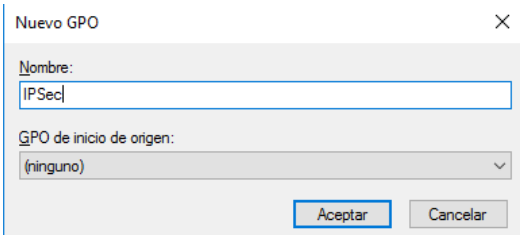
3. Una vez verificado si se encuentra algún equipo se procede abrir la opción de administración de directivas de grupo para la creación de una nueva directiva.



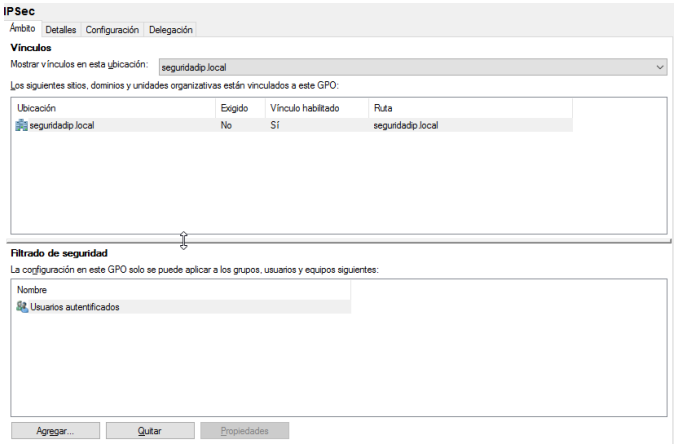
4. Una vez dentro de dicha ventana se procede a la creación de una nueva directiva.



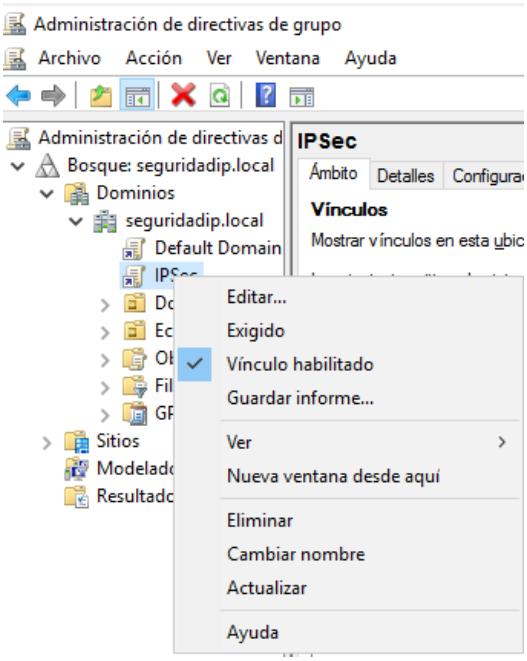
Por lo cual aparece una nueva ventana emergente en la cual nos pide el nombre en este caso colocaremos el nombre de IPSec. Y dar clic en aceptar para proseguir con los pasos necesarios.

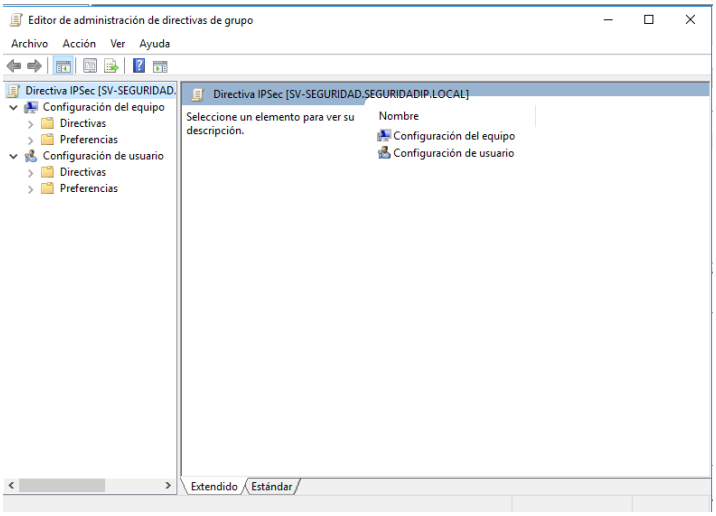


5. Una vez se tenga la siguiente imagen se procede a la edición de la misma.



6. Para editar dicha directiva se debe dar clic derecho sobre la directiva creada y una vez se realice este paso se desplegará una nueva ventana.



7. 

8. Una vez aparezca esta nueva ventana se creará la regla para habilitar IPSec en este tipo de conexiones.

   Para dicha configuración se debe seguir los siguientes pasos:

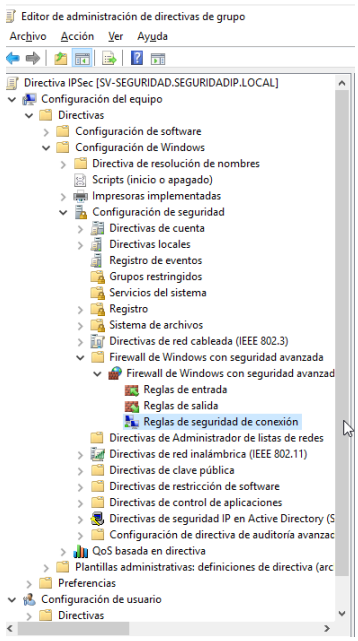
   8.1. Dar clic en configuración de equipo

   8.2.Buscar la opción de directivas y dar clic sobre la configuración de Windows.

   8.3.Dar clic en configuración de seguridad

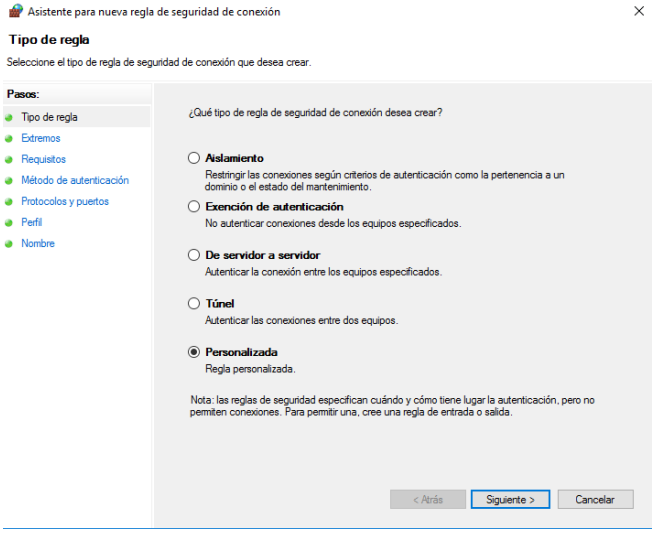
   8.4.Dar clic en firewall de Windows con seguridad avanzada.

   8.5.Seleccionar reglas de seguridad de conexión.

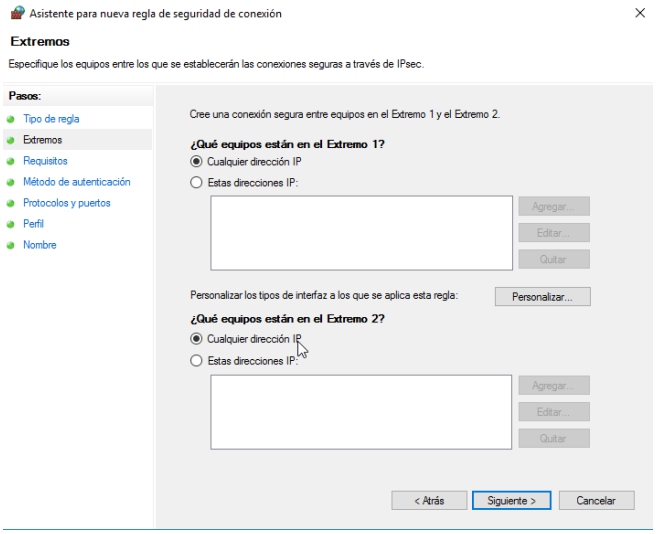


9. En este caso una vez en las reglas se seguridad se procede a realizar la configuración de una nueva regla. Una vez se dé clic en nueva regla

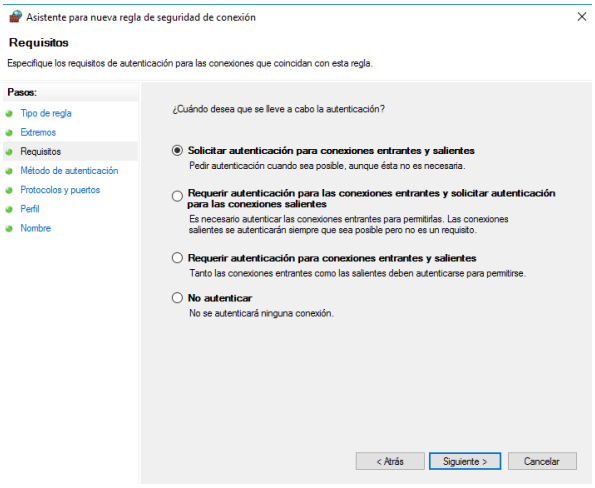
aparecerá la siguiente ventana en la cual se debe seleccionar la opción de personalizada. Dar clic en siguiente para proseguir con el proceso de configuración.



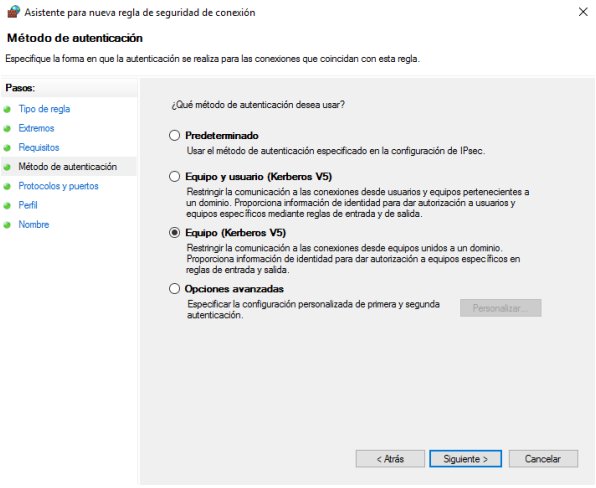
10. En la siguiente ventana realizará una pregunta acerca de las IP de destino que se dispone en las cuales se colocara por defecto a cualquier IP para la realización de las pruebas iniciales.



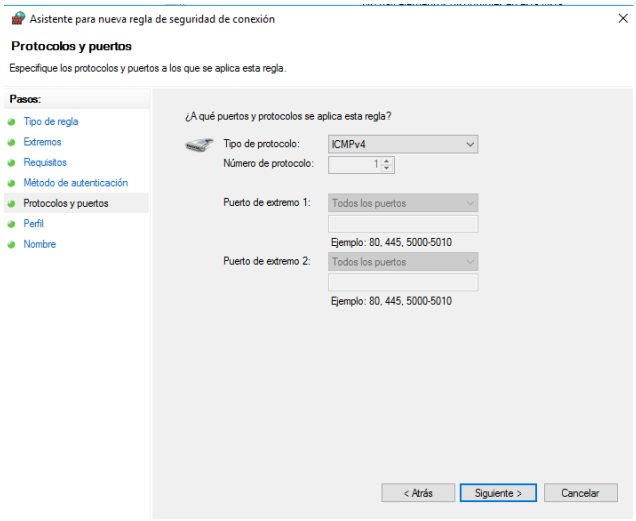
11. En la siguiente ventana nos ofrecerá diferentes opciones entre las cuales se selecciona la opción de requerir autenticación para las conexiones entrantes.



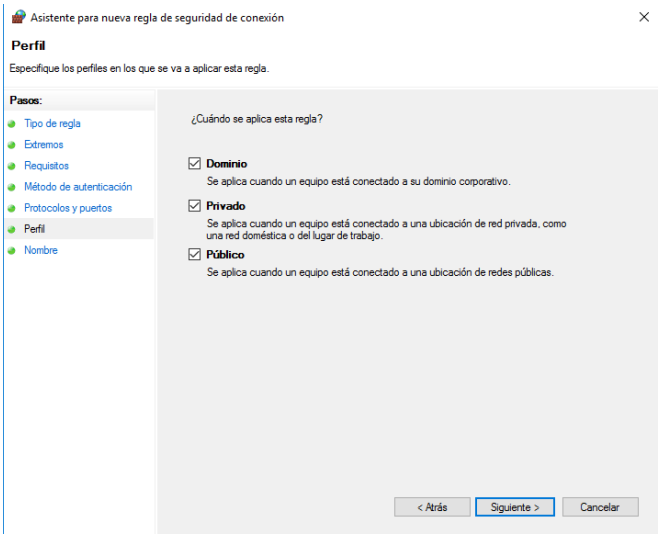
12. Una vez seleccionado el tipo de autentificación que se desea nos pregunta nuevamente en la cual utilizaremos solo para los equipos.



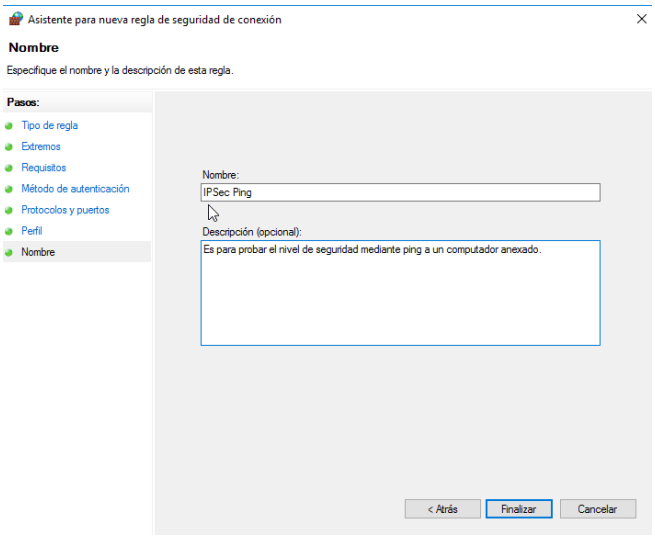
13. Se procede a configurar el protocolo el cual se utiliza en este caso que es el ICMPv4, dar siguiente para continuar con el proceso.

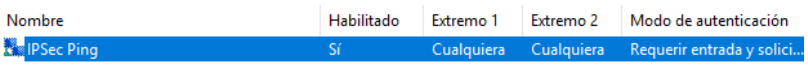


14. Para finalizar aparecerá una ventana en donde nos pregunta a quien se aplica esta regla y por defecto se dejará por defecto todo seleccionado.



15. Como finalización pedirá un nombre y una descripción en la cual se colocará por defecto que se realizará ping mediante IPSec para comprobar el nivel de seguridad. Y se debe dar clic en finalizar para culminar con el procedimiento.



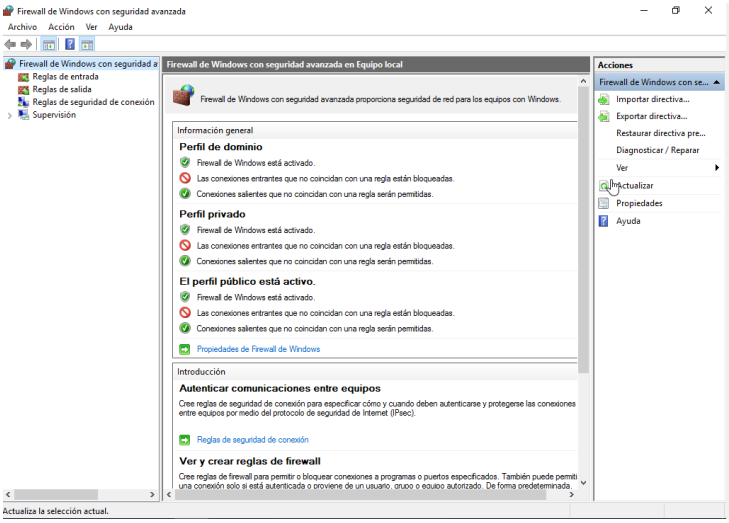


Anexo 11

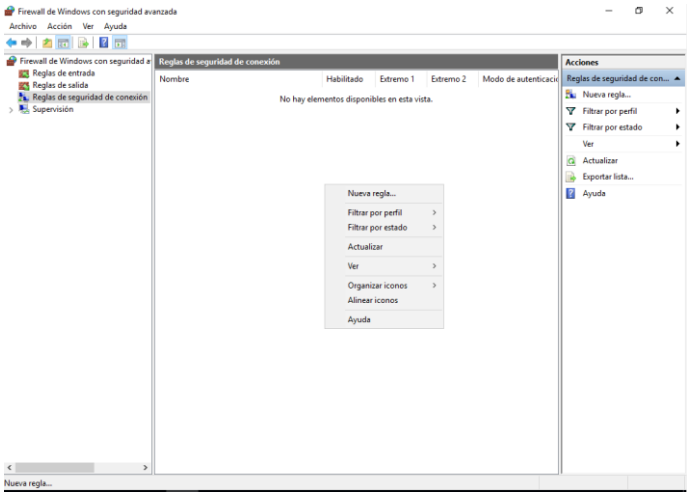
Creación de las reglas de IPSec

1. Para la creación de las reglas de IpSec se debe acceder al firewall de Windows con seguridad avanzada, una vez dentro se debe ubicar la

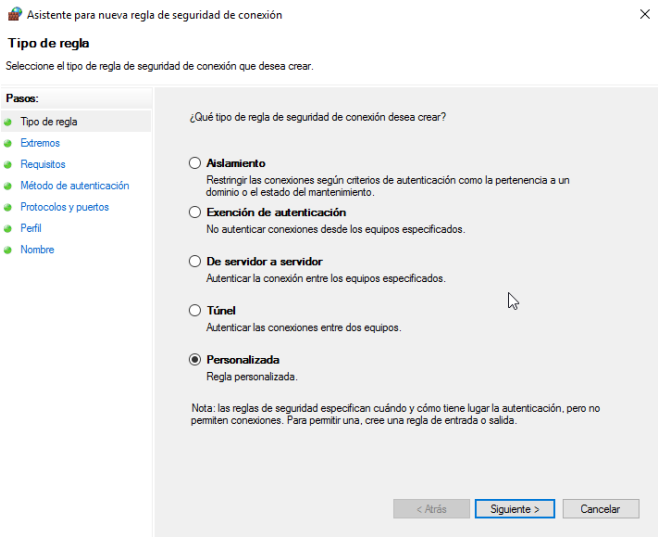
opción de reglas de seguridad de conexión en las cuales colocaremos las reglas que se necesitan para la IpSec.



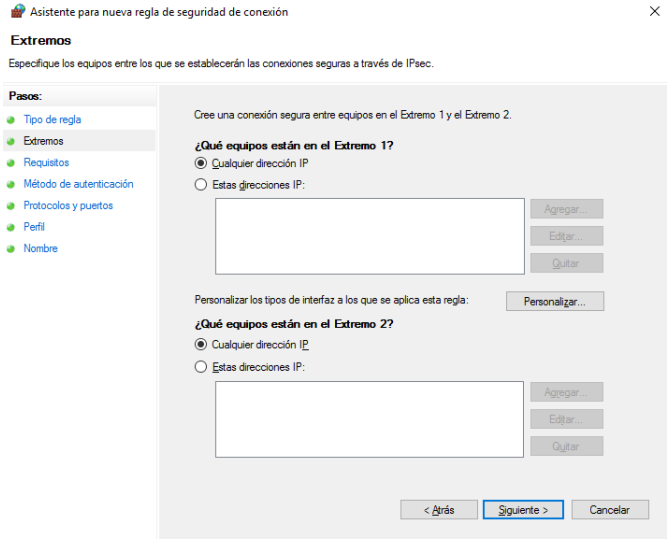
2. Dentro de “reglas de seguridad de conexión”, se procede a crear las reglas necesarias para IpSec de la siguiente manera.
   Clic derecho en la pantalla en blanco y nueva regla.



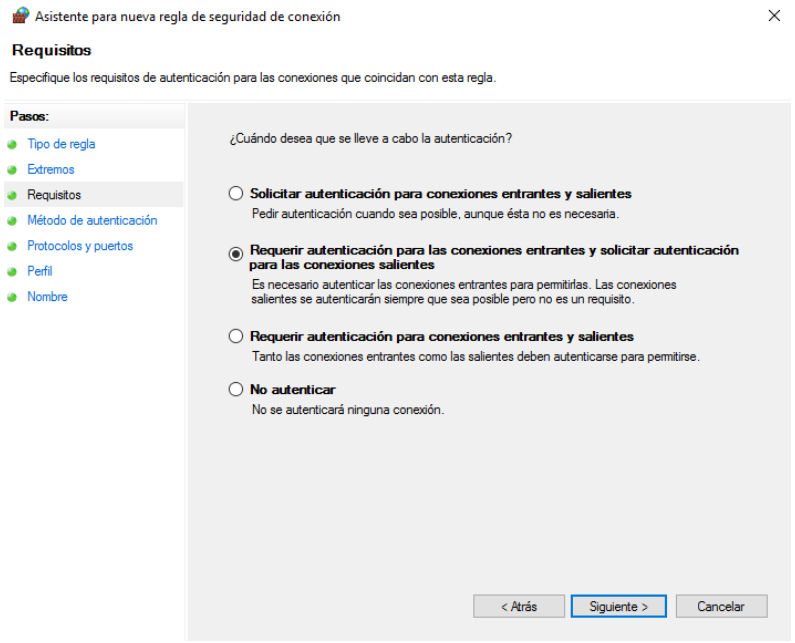
3. Dentro de la siguiente pantalla aparecerá la siguiente ventana en la cual se debe seleccionar la creación de una nueva regla personalizada y dar clic en siguiente.



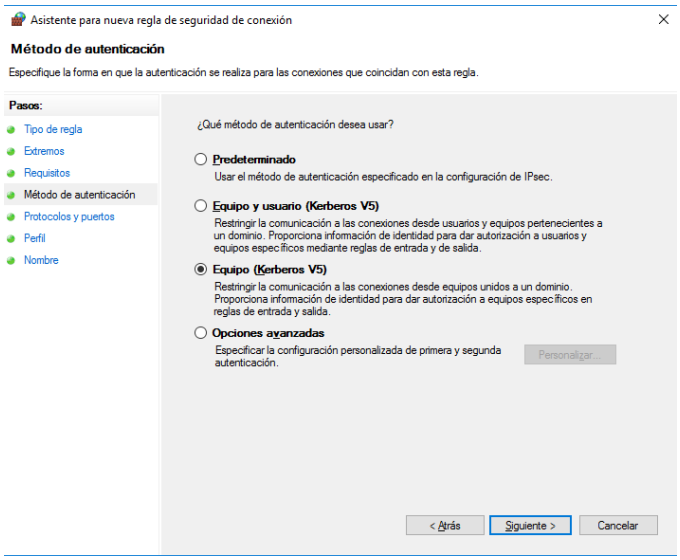
4. En la siguiente ventana, se selecciona la opción de cualquier dirección IP en los dos extremos, esto ayudara a que dentro de la red tengan una protección de extremo a extremo.



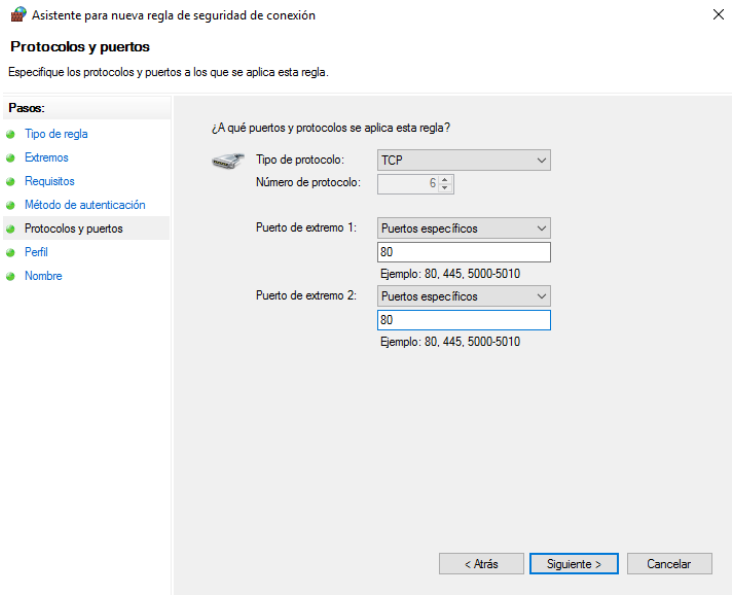
5. En la siguiente ventana se procede a seleccionar el requerimiento de autenticación para las conexiones de entrada y las conexiones de salida, dar clic en siguiente para proceder con el siguiente procedimiento.



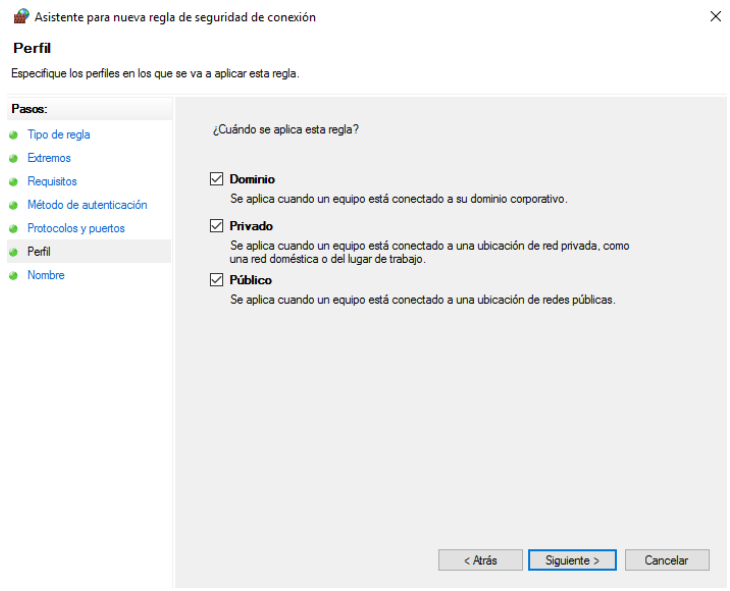
6. En la siguiente ventana se procede a seleccionar un tipo de autenticación en la cual se selecciona Kerveros v5 la cual ayudara con el intercambio de claves automáticas. Dar clic en siguiente para continuar con el siguiente paso.



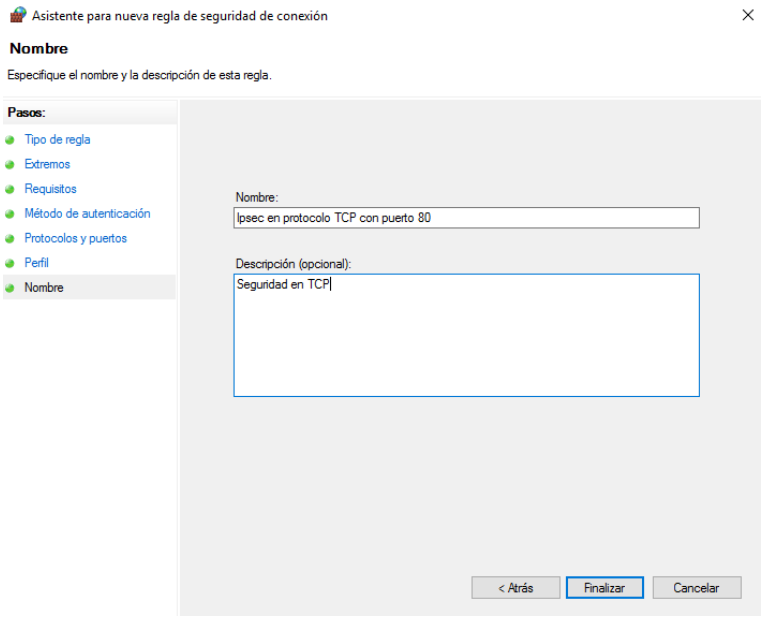
7. En la siguiente ventana se procede a la configuración del protocolo que será protegido a través de dicha regla en este caso se selecciona el protocolo TCP, con la configuración del puerto 80. Dar clic en siguiente para continuar con la configuración de la regla.



8. En la siguiente ventana se la deja por defecto con las características ya seleccionadas, dar clic en siguiente para seguir con el último paso de la configuración.



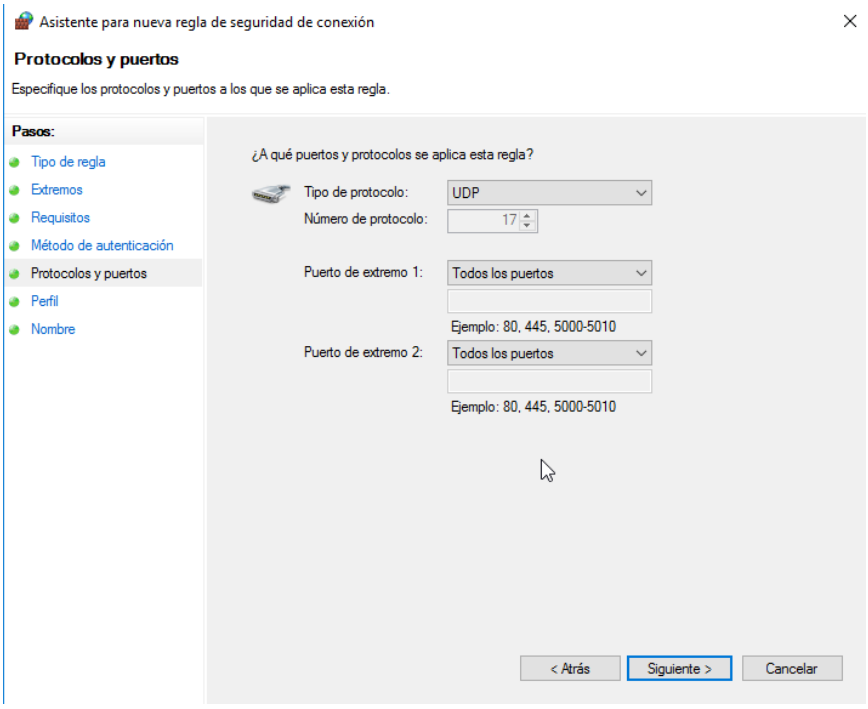
9. Se colocará un nombre y una descripción de la misma para en este caso finalizar con la configuración de la regla, se recomienda colocar nombres clave que tengan que ver con la configuración IpSec.



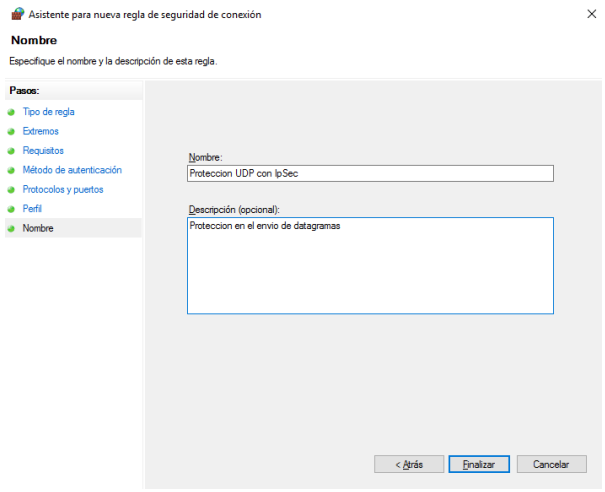
En este momento se creó la primera regla de IpSec para continuar con las reglas se procede a realizar los mismos procedimientos, salvo que al momento de seleccionar el protocolo se cambiara.

La siguiente regla está a continuación.

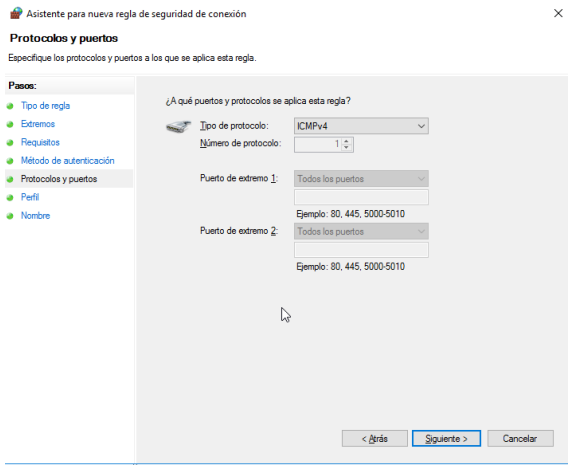
10. Para la siguiente regla se selecciona el protocolo UDP para el envío de datagramas mediante IP.



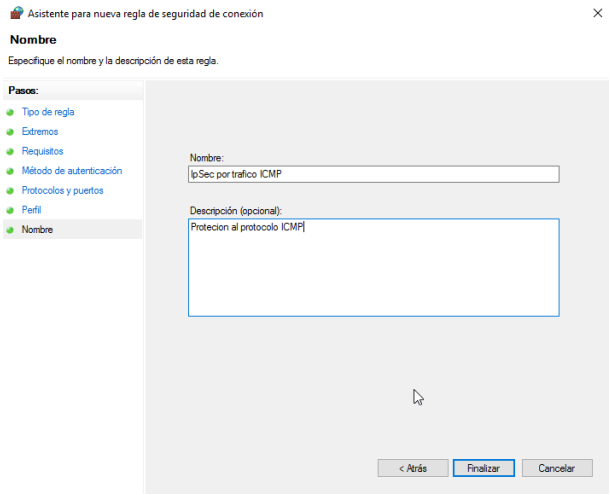
11. Conjuntamente como los pasos anteriores se otorga de un nombre y una descripción a la misma. La cual será “Protección UDP con IpSec”



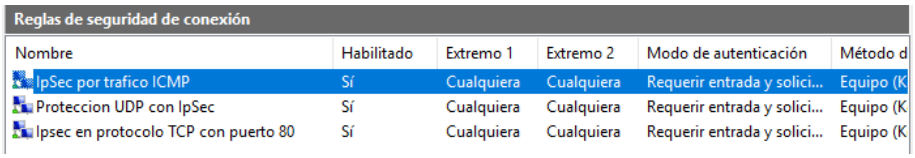
12. Para la siguiente regla se selecciona el protocolo ICMPv4, este protocolo es encargado de los mensajes de internet. En este caso una vez seleccionado se deja por defecto los puertos.



13. En este caso como en los pasos anteriores se otorga de un nombre y una descripción la cual es “IpSec por tráfico ICMP”



14. Una vez finalizadas las reglas se puede apreciar que se encuentran dentro de reglas de seguridad de conexión.



Reglas de seguridad de conexión

Nombre	Habilitado	Extremo 1	Extremo 2	Modo de autenticación	Método d
IpSec por trafico ICMP	Sí	Cualquiera	Cualquiera	Requerir entrada y solici...	Equipo (K
Proteccion UDP con IpSec	Sí	Cualquiera	Cualquiera	Requerir entrada y solici...	Equipo (K
Ipsec en protocolo TCP con puerto 80	Sí	Cualquiera	Cualquiera	Requerir entrada y solici...	Equipo (K

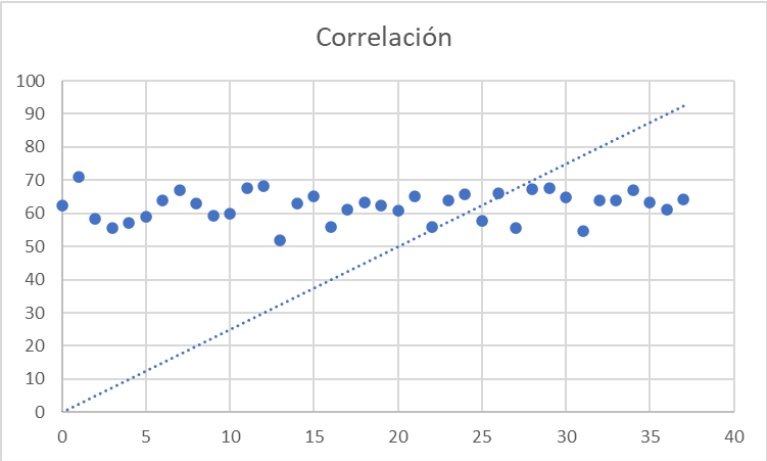
Anexo 12

En el siguiente anexo se procede a la verificación de la correlación de variables sin ningún tipo de seguridad y después de la aplicación protocolo seguro IpSec, cabe recalcar que los datos obtenidos son por parte de un ping controlado en base a segundos y paquetes enviados sin el protocolo seguro.

Tabla de datos para la verificación de la correlación

Tiempo Segun	Tamaño MB	Tiempo Segun	Tamaño MB	Tiempo Segun	Tamaño MB	Tiempo Segun	Tamaño MB
0	62.4	11	67.5	22	56	33	63.8
1	71.1	12	68.2	23	63.8	34	66.9
2	58.3	13	52	24	65.7	35	63.3
3	55.6	14	63	25	57.6	36	61
4	57.2	15	65.1	26	66.1	37	64.3
5	59.1	16	56	27	55.6		
6	64	17	61.1	28	67.2		
7	67	18	63.3	29	67.7		
8	63	19	62.4	30	64.9		
9	59.4	20	60.7	31	54.7		
10	59.9	21	65	32	63.8		

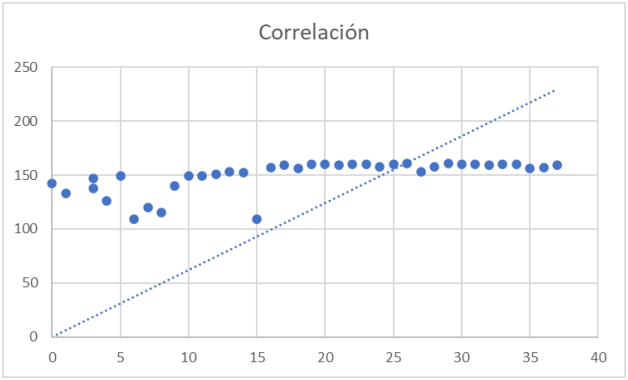
Gráfico en el cual se puede apreciar la correlación que tiene como un resultado de 0.115676531 en la cual se puede apreciar que no existe una correlación importante.



En la siguiente tabla se puede apreciar los datos para la realización de la correlación una vez aplicado el protocolo seguro IpSec.

Tiempo Segun	Tamaño MB	Tiempo Segun	Tamaño MB	Tiempo Segun	Tamaño MB	Tiempo Segun	Tamaño MB
0	142	11	149	22	160	33	160
1	133	12	151	23	160	34	160
3	138	13	153	24	158	35	156
3	147	14	152	25	160	36	157
4	126	15	109	26	161	37	159
5	149	16	157	27	153		
6	109	17	159	28	158		
7	120	18	156	29	161		
8	115	19	160	30	160		
9	140	20	160	31	160		
10	149	21	159	32	159		

El siguiente grafico muestra, la correlación la cual da un resultado de 0.651791878, el cual menciona que es una correlación media – grande en la cual se aprecia un cambio sustancial.



Anexo 13

Pruebas de IPSec

Descripción	Prueba de conectividad entre servidor y equipo01, equipo02 y equipo03	Prueba: #01
Objetivo	Verificar el estado de conexión de los equipos con el servidor.	
Registro de datos	Ping 192.168.100.66 -t (desde el equipo01 al Servidor) Ping 192.168.16.1 -t (desde el equipo01 al Servidor) Ping seguridadip.local -t (desde el equipo01 al Dominio) Ping 192.168.100.66 -t (desde el equipo02 al Servidor) Ping 192.168.16.1 -t (desde el equipo02 al Servidor) Ping seguridadip.local -t (desde el equipo02 al Dominio) Ping 192.168.100.66 -t (desde el equipo03 al Servidor) Ping 192.168.16.1 -t (desde el equipo03 al Servidor) Ping seguridadip.local -t (desde el equipo03 al Dominio)	
Duración estimada	La duración estimada será alrededor de 1 minuto por ping realizado.	
Resultados	Conectividad estable Paquetes enviados correctamente Paquetes entregados correctamente Ningún paquete perdido	
Observaciones	Se realiza la prueba de conectividad básica en la cual al momento de realizar un ping al servidor este tiene una conectividad exitosa por lo cual se considera esta prueba satisfactoria.	

Descripción	Prueba de conectividad entre equipos01, equipo02, equipo03	Prueba: #02
Objetivo	Verificar el estado de la conexión de las máquinas virtuales clientes a través de un ping entre ellos.	
Registro de datos	Ping 192.168.16.1 -t desde el equipo02 Ping 192.168.16.2 -t desde el equipo03 Ping 192.168.16.3 -t desde el equipo01	
Duración estimada	La duración estimada será alrededor de 30 segundos a 1 minuto por ping realizado.	
Resultados	Conectividad estable Paquetes enviados correctamente Paquetes entregados correctamente Ningún paquete perdido	
Observaciones	Se realiza la prueba de conexión entre los equipos que están en esta red interna de equipos virtuales dando como resultado una conectividad exitosa por lo cual se considera esta prueba satisfactoria.	

Descripción	Validación de las reglas mediante active directory	Prueba: #03
Objetivo	Verificar si las reglas están funcionando dentro de la red interna con los equipos en funcionamiento.	
Registro de datos	Verificación de los equipos mediante active directory Verificación de las reglas en active directory	
Duración estimada	3 minutos	
Resultados	Verificar que los equipos consten dentro de active Verificar que la creación de las reglas esté correcta	
Observaciones	Las reglas se encuentran ingresadas para esta prueba y los equipos se encuentran dentro de la directiva por lo cual esta prueba se da por satisfactoria.	

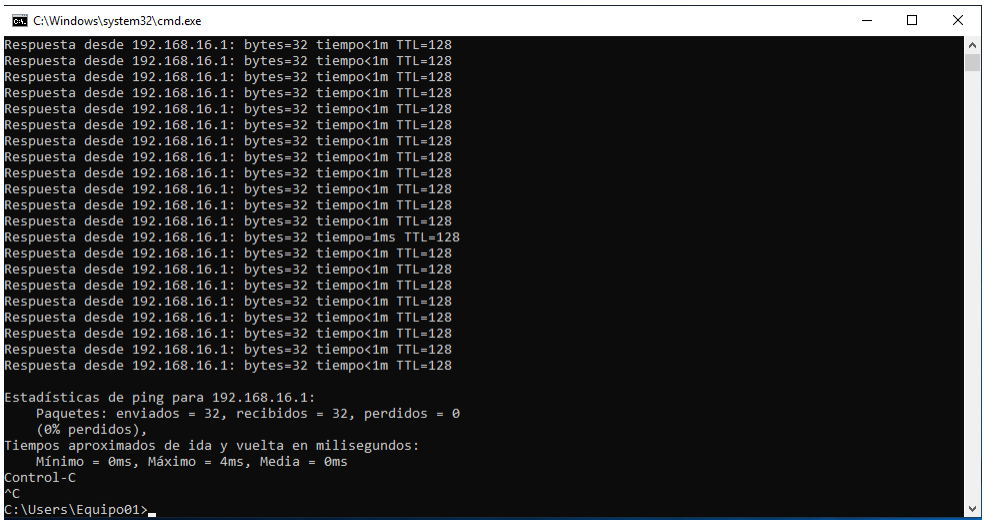
Descripción	Validación de que los equipos clientes se encuentren dentro del dominio.	Prueba: #04
Objetivo	Verificar que los equipos clientes estén dentro del dominio del servidor para la realización de las pruebas.	
Registro de datos	Ingreso a las propiedades de los equipos Verificación del dominio Ingresar al dominio	
Duración estimada	15 min	
Resultados	Equipos unidos a un dominio Cada equipo dispone de sus permisos de autenticación	
Observaciones	Se aprecia que los 3 equipos están dentro del dominio, pero no existe una conectividad entre el servidor y el cliente. Por lo cual se revisan las configuraciones en las cuales se aprecia que no está configurado las opciones de red para la identificación de los equipos dentro de la misma. Por lo cual se considera una prueba satisfactoria.	

Descripción	Verificación de conectividad a través de IPSec entre servidor y equipo01, equipo02, equipo03	Prueba: #05
Objetivo	Verificar cual es el estado de la información al momento de enviar un ping controlado al servidor desde los clientes.	
Registro de datos	Ping 192.168.100.66 -t (desde el equipo01 al Servidor) Ping 192.168.16.1 -t (desde el equipo01 al Servidor) Ping seguridadip.local -t (desde el equipo01 al Dominio) Ping 192.168.100.66 -t (desde el equipo02 al Servidor) Ping 192.168.16.1 -t (desde el equipo02 al Servidor) Ping seguridadip.local -t (desde el equipo02 al Dominio) Ping 192.168.100.66 -t (desde el equipo03 al Servidor) Ping 192.168.16.1 -t (desde el equipo03 al Servidor) Ping seguridadip.local -t (desde el equipo03 al Dominio) Capturadora de datos wireshark	
Duración estimada	30 segundos a 1 minuto por ping realizado	
Resultados	Encriptación de la información al momento de realizar el ping. Incremento en el número de bits al momento de realizar el ping.	
Observaciones	Al momento de realizar el ping mediante IPSec se puede apreciar mediante la capturadora de datos de wireshark que la información esta encriptada correctamente y el número de bits se incrementaron de 36 a 96 por la encriptación. Por lo cual la prueba realizada tiene calificación de satisfactoria.	

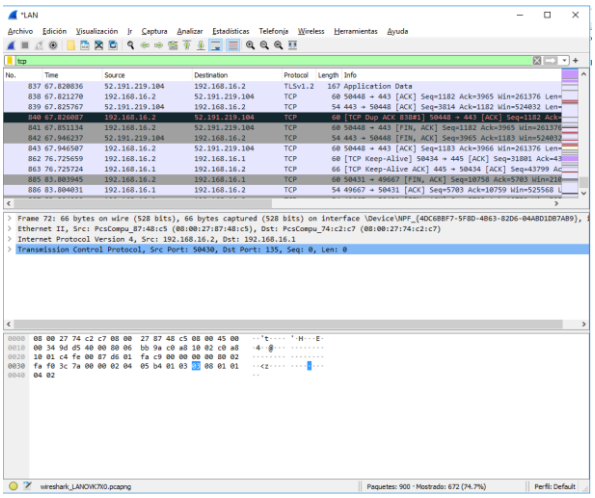
Descripción	Verificación de la seguridad sin ningún tipo de protocolo seguro ni encapsulamiento.					Prueba: # 06
Objetivo	Revisar el nivel de seguridad que dispone la conexión cliente servidor.					
Registro de datos	Ping al servidor “seguridadip.local” desde el equipo01 Envió de archivos de texto plano (1-n) al mismo tiempo. Envió de Documentos DPF (1-n) al mismo tiempo. Envió de imágenes (1-n) al mismo tiempo.					
Calificadores						
	Comunicación	Paquetes enviados con éxito	Paquetes erróneos	Encriptación	Encapsulamiento	Protocolo seguro
Ping al servidor	✓	✓	X	X	X	X
Archivo de texto plano	✓	✓	X	X	X	X
Varios archivos de texto plano	✓	✓	X	X	X	X
Documento PDF	✓	✓	X	X	X	X
Documentos PDF	✓	✓	X	X	X	X
Imagen	✓	✓	X	X	X	X
Imágenes	✓	✓	X	X	X	X
Navegación	✓	✓	X	X	X	X
Observaciones	La prueba realizada muestra que existe conectividad de cliente-servidor y a su vez se puede realizar el envío de archivos sin ningún tipo de problema, pero al momento de verificar el tipo de seguridad mediante el programa de wireshark se puede apreciar que en esta prueba no existe ningún tipo de seguridad que ayude a la seguridad de la información. Por ende, esta prueba tiene la calificación de satisfactoria para pasar a la siguiente prueba.					

Evidencias

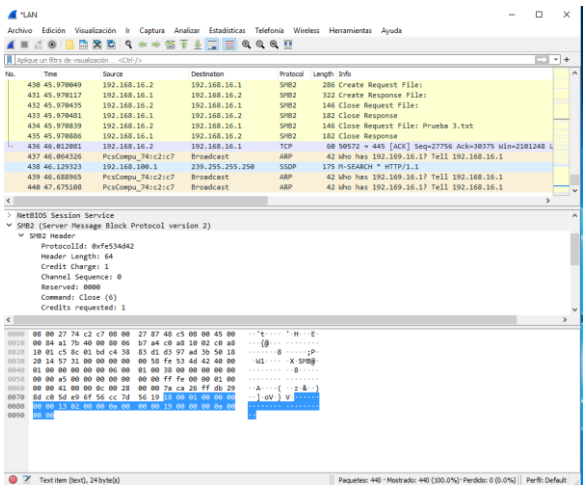
Ping continuo al servidor



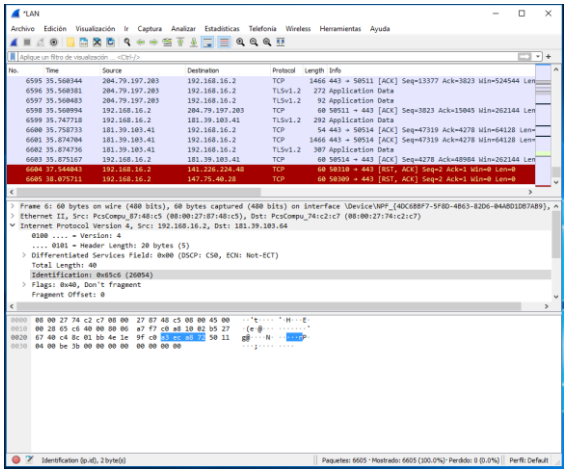
Trafico de la red mediante el programa wireshark



Envió de archivos de texto plano, DPF e imágenes.



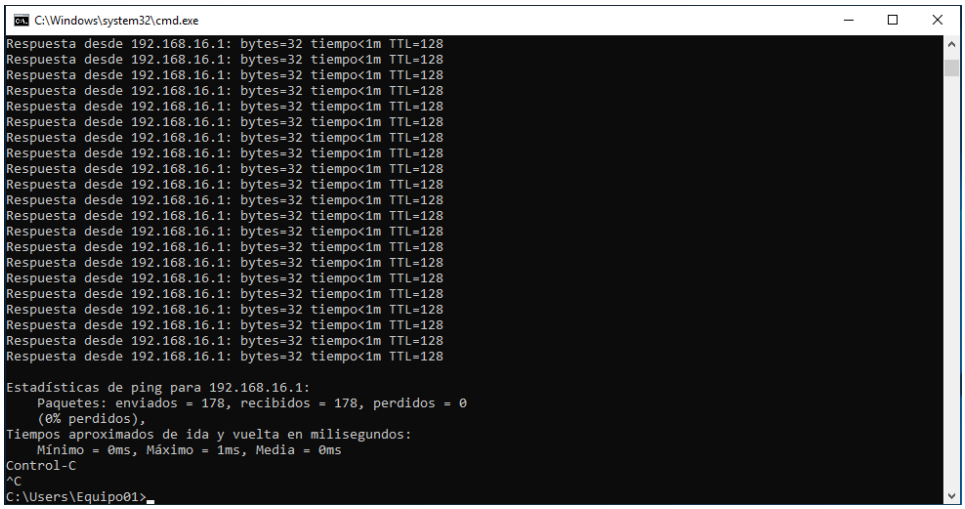
Datos capturados mediante navegación sin protocolo de seguridad



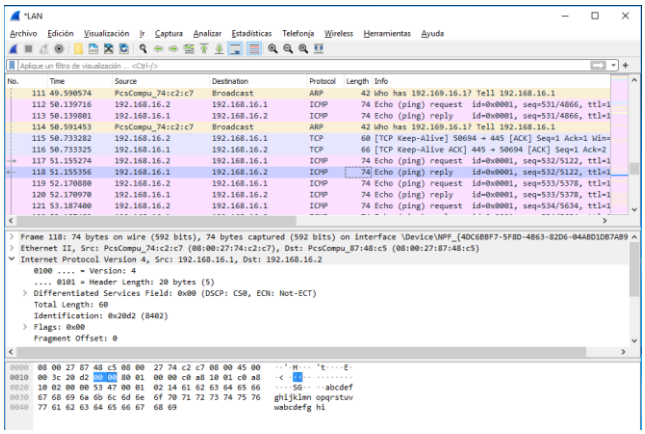
Descripción	Verificación de la encriptación de seguridad mediante el protocolo TCP con IPSec					Prueba: # 07
Objetivo	Verificar el funcionamiento del protocolo de seguridad TCP con IPSec para					
Registro de datos	Ping al servidor “seguridadip.local” desde el equipo01					
	Envió de archivos de texto plano (1-n) al mismo tiempo.					
	Envió de Documentos DPF (1-n) al mismo tiempo.					
	Envió de imágenes (1-n) al mismo tiempo.					
Calificadores						
	Comunicación	Paquetes enviados con éxito	Paquetes erróneos	Encriptación	Encapsulamiento	Protocolo seguro
Ping al servidor	✓	✓	X	✓	✓	✓
Archivo de texto plano	✓	✓	X	-	X	-
Varios archivos de texto plano	✓	✓	X	-	X	-
Documento PDF	✓	✓	X	-	X	-
Documentos PDF	✓	✓	X	-	X	-
Imagen	✓	✓	X	-	X	-
Imágenes	✓	✓	X	-	X	-
Navegación	✓	✓	-	-	-	-
Observaciones	Esta prueba dispone del protocolo seguro IPSec en el cual se muestra que al momento de realizar el ping este asegura la comunicación mediante el protocolo TCP. Pero al momento de realizar el envío de un archivo de texto plano, PDF e imágenes, este tiene falencias al momento de proteger el archivo enviado. Pero a su vez se puede apreciar que el nivel de seguridad se incrementó conforme a la prueba anterior realizada.					
	Por ende, esta prueba es considerada satisfactoria pues satisface las necesidades de comunicación entre equipos. Se considera satisfactoria para pasar a la siguiente prueba.					

Evidencias

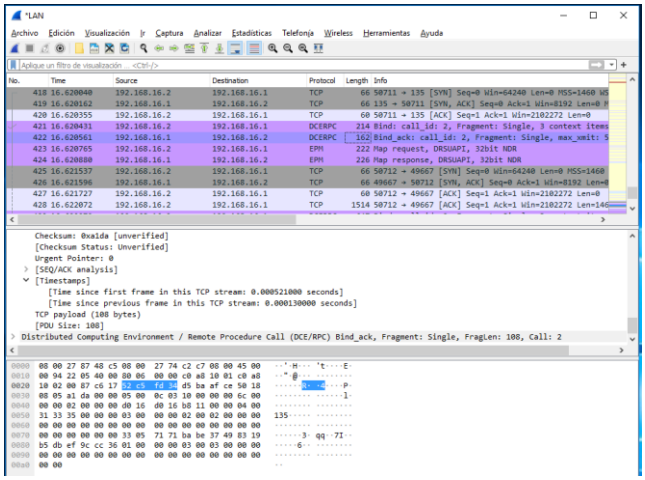
Ping continuo al servidor



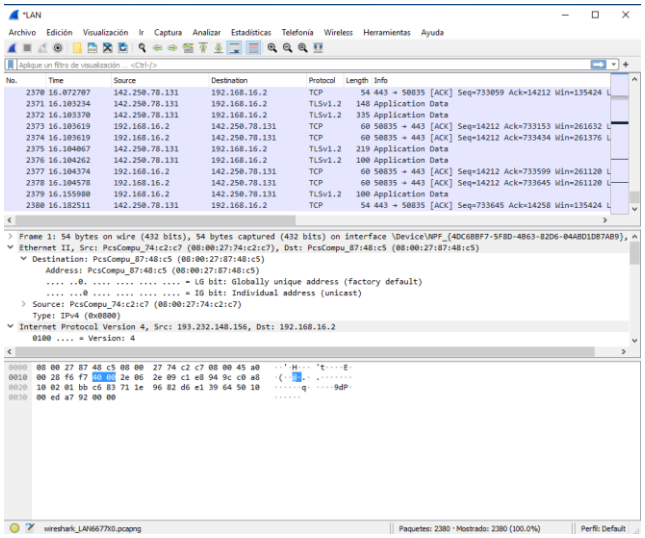
Verificación de datos mediante wireshark



Verificación del envío de datos mediante wireshark



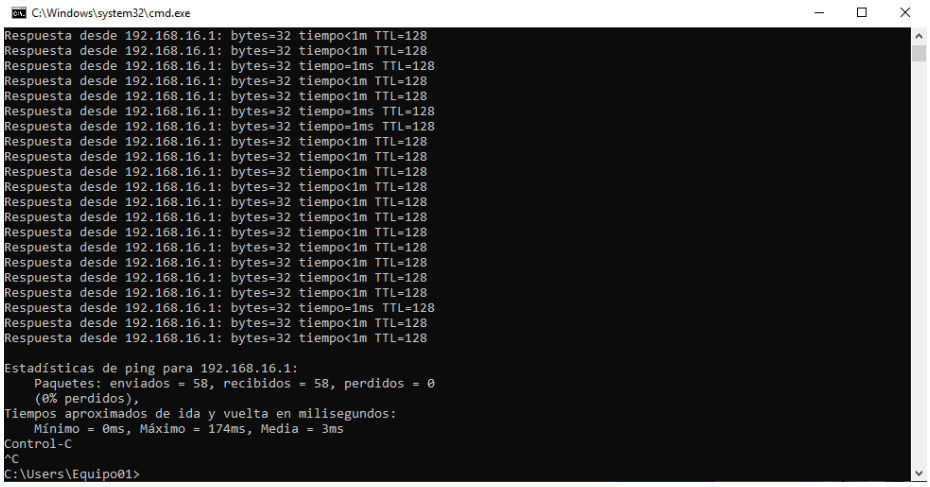
Verificación de la navegación mediante wireshark



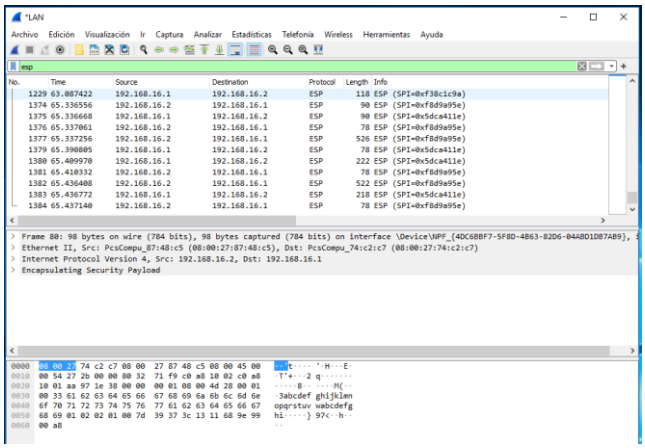
Descripción	Verificación de la encriptación de seguridad dos reglas de conexión segura aplicando el protocolo TCP e ICMP con IPSec				Prueba: # 08
Objetivo	Verificar si el nivel de seguridad incrementa al momento de realizar las				
Registro de datos	Ping al servidor “seguridadip.local” desde el equipo01				
	Envió de archivos de texto plano (1-n) al mismo tiempo.				
	Envió de Documentos DPF (1-n) al mismo tiempo.				
	Envió de imágenes (1-n) al mismo tiempo.				
Calificadores					
	Comunicación	Paquetes enviados con éxito	Paquetes erróneos	Encriptación	Encapsulamiento	Protocolo seguro
Ping al servidor	✓	✓	X	✓	✓	✓
Archivo de texto plano	✓	✓	X	-	-	-
Varios archivos de texto plano	✓	✓	X	-	-	-
Documento PDF	✓	✓	X	-	-	-
Documentos PDF	✓	✓	X	-	-	-
Imagen	✓	✓	X	-	-	-
Imágenes	✓	✓	X	-	-	-
Navegación	✓	✓	X	✓	-	-
Observaciones	Esta prueba fue realizada en base a dos reglas para la conexión segura la primera en base a TCP e ICMP las cuales sirven para establecer una comunicación segura entre los equipos a su vez dentro de la navegación se puede ver que la encriptación ya se encuentra activa para la navegación segura.					
	Por lo cual esta prueba da satisfactoria en la comunicación segura por lo tanto se procede con la siguiente prueba.					

Evidencias

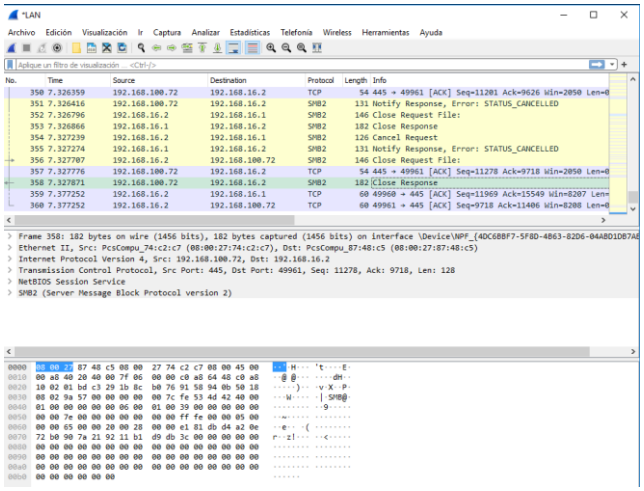
Ping continuo al servidor



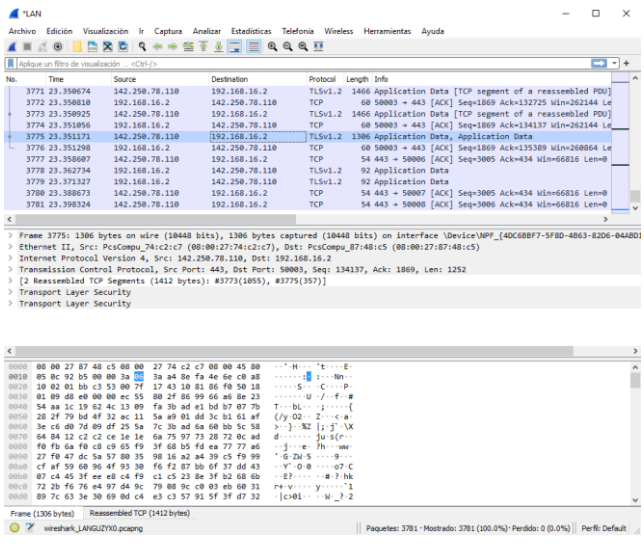
Verificación de datos mediante wireshark



Verificación de envío de archivos mediante wireshark



Verificación de navegación mediante wireshark



Descripción	Verificación de la seguridad utilizando 3 reglas de conexión segura las cuales establecen una conectividad segura incluyendo					Prueba: # 09
Objetivo	Verificar el nivel de encriptación y seguridad de la información que se está					
Registro de datos	Envió de archivos de texto plano (1-n) al mismo tiempo. Envió de Documentos DPF (1-n) al mismo tiempo. Envió de imágenes (1-n) al mismo tiempo.					
Calificadores						
	Comunicación	Paquetes enviados con éxito	Paquetes erróneos	Encriptación	Protocolo seguro	Comunicación segura
Archivo de texto plano	✓	✓	X	✓	✓	✓
Varios archivos de texto plano	✓	✓	X	✓	✓	✓
Documento PDF	✓	✓	X	✓	✓	✓
Documentos PDF	✓	✓	X	✓	✓	✓
Imagen	✓	✓	X	✓	✓	✓
Imágenes	✓	✓	X	✓	✓	✓
Navegación	✓	✓	-	✓	✓	-
Observaciones	Durante esta prueba se puede apreciar que a la comunicación entre los equipos y el servidor es mucho mas segura pues al momento de verificar el flujo TCP se puede verificar que la información se encuentra encriptada de puto a punto, a su vez con respecto a la navegación se vuelve más segura, pero existen algunas caídas en la comunicación TCP, las cuales pueden ser en base al internet o intermitencias en la misma.					

Evidencias

Verificación de paso de archivos mediante wireshark

Verificación de navegación mediante wireshark