



UNIVERSIDAD NACIONAL DEL ALTIPLANO
FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA,
ELECTRÓNICA Y SISTEMAS
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA



**“DISEÑO E IMPLEMENTACIÓN DE UNA RED PRIVADA
VIRTUAL USANDO IPSEC PARA ADMINISTRAR
REMOTAMENTE LA RED INSTITUCIONAL DE LA
UNIVERSIDAD NACIONAL DEL ALTIPLANO”**

TESIS

PRESENTADA POR:

HUGO DARÍO AQUINO ARCATA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PUNO – PERÚ

2023



NOMBRE DEL TRABAJO

DISEÑO E IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL USANDO IPSEC PARA ADMINISTRAR REMOTAMENTE LA RED INSTITUCIONAL DE LA UNIVERSIDAD NACIONAL DEL ALTIPLANO

AUTOR

HUGO DARÍO AQUINO ARCATA

RECuento DE PALABRAS

17768 Words

RECuento DE CARACTERES

97251 Characters

RECuento DE PÁGINAS

111 Pages

TAMAÑO DEL ARCHIVO

12.3MB

FECHA DE ENTREGA

Sep 11, 2023 11:00 PM GMT-5

FECHA DEL INFORME

Sep 11, 2023 11:02 PM GMT-5

● **19% de similitud general**

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base

- 18% Base de datos de Internet
- Base de datos de Crossref
- 12% Base de datos de trabajos entregados
- 3% Base de datos de publicaciones
- Base de datos de contenido publicado de Crossref


Christian Augusto Romero Goyzaeta
INGENIERO ELECTRÓNICO
CIP. 133009
ASESOR


Karlos Alexander Ceantuta Chirapo
ING. ELECTRONICO
CIP. 94113
Subdirector (e)
Investigación E.P.I.E.

Resumen



DEDICATORIA

A pesar de haber requerido mucho trabajo y atención, terminar mi tesis no hubiera sido posible sin la ayuda desinteresada de todos los que viajaron conmigo a lo largo del riguroso camino de este esfuerzo. En momentos de angustia y desesperación, varios de ellos me brindaron un firme apoyo. Primero que nada, quiero agradecer a Dios por estar conmigo en todo momento, por sostener mi corazón e iluminar mis pensamientos. También aprecio a las personas con las que entré en contacto durante mi período de estudio, ya que me ayudaron y me hicieron compañía. A mi madre, quien ha sido el apoyo más importante en mi vida y quien constantemente demuestra su amor y apoyo inquebrantable, a pesar de nuestros diferentes puntos de vista. Siento la presencia continua de mi padre a pesar de nuestra separación física, y estoy seguro de que este momento le resultará tan significativo como lo es para mí. Quiero expresar mi más sincero agradecimiento a mi asesor de tesis, cuyo conocimiento y experiencia me permitieron terminar mis estudios.



AGRADECIMIENTOS

Quiero extender mi profundo agradecimiento a todos los que ayudaron con esta investigación y a quienes me apoyaron durante momentos difíciles, alegres y trágicos. Este mensaje está destinado a todos ustedes.

Quiero expresar mi más sincero agradecimiento a mis padres por su amor, compasión y apoyo inquebrantables. Sobre todo, quiero expresar mi gratitud por su tolerancia hacia mí. Mi agradecimiento por todas las veces que usted me ha apoyado en todas las decisiones de mi vida (buenas, terribles e incluso tontas) no se puede expresar adecuadamente con palabras. Te agradezco que me dejes desarrollarme como persona y me dejes ser quien soy.

Quiero expresar mi gratitud a todos mis amigos, tanto a aquellos con quienes he pasado tiempo fuera del aula. Agradezco sinceramente a todos mis compañeros de escuela, que se han convertido en amigos para toda la vida y que serán mis futuros compañeros, por su aliento y alegres celebraciones.

Por supuesto, también tengo que mencionar a las autoridades y a mi querida universidad. Te agradezco que me permitas terminar esta etapa de mi vida. Su perseverancia, dirección y consejo fueron cruciales en la creación de este estudio. Estoy muy agradecido por la oportunidad que me brindaron.



INDICE GENERAL

DEDICATORIA

AGRADECIMIENTOS

INDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ACRÓNIMOS

RESUMEN 14

ABSTRACT..... 15

CAPÍTULO I

INTRODUCCIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA 16

1.2. PLANTEAMIENTO DEL PROBLEMA 18

1.3. HIPÓTESIS DE LA INVESTIGACIÓN 18

1.3.1. Hipótesis General 18

1.3.2. Hipótesis Específicas 18

1.4. OBJETIVOS DE LA INVESTIGACIÓN 18

1.4.1. Objetivo General..... 18

1.4.2. Objetivos Específicos 19

CAPÍTULO II

REVISIÓN DE LITERATURA

2.1. ANTECEDENTES DE LA INVESTIGACIÓN 20

2.2. FUNDAMENTOS DE LAS REDES PRIVADAS VIRTUALES 25

2.2.1. Redes De Computadoras 25

2.2.1.1. Definición 25

2.2.1.2. Clasificación 26

2.2.1.3. Topología..... 27

2.2.1.4. Componentes 31

2.2.2. Modelo OSI 32



2.2.2.1.	Definición	32
2.2.2.2.	Tipos de Servicio	33
2.2.2.3.	Capas del Modelo OSI.....	33
2.2.2.4.	Transmisión de Datos en el Modelo OSI.....	36
2.2.3.	Acceso Remoto y Conexiones WAN	36
2.2.3.1.	Internet, Intranets y Extranet	36
2.2.3.2.	Acceso Remoto	37
2.3.	VIRTUAL PRIVATE NETWORK (VPN)	38
2.3.1.	Definición de una Red Privada Virtual (VPN).....	38
2.3.2.	Tipos de VPN	40
2.3.3.	Arquitecturas Vpn	42
2.3.4.	De Sitio a Sitio.....	42
2.3.4.1.	De Acceso Remoto	43
2.3.4.2.	Tunneling	45
2.3.4.3.	VPN Over LAN	46
2.3.5.	Seguridad en una VPN	47
2.4.	VPN DE ACCESO REMOTO	48
2.5.	SEGURIDAD IP (IPSec).....	48
2.5.1.	Definición de IPSec	48
2.5.1.1.	Protocolos de IPSec	49
2.5.1.2.	Encabezado de Autenticación (AH)	49
2.5.1.3.	Carga de Seguridad Encapsulada (ESP).....	50
2.5.1.4.	Intercambio de Claves En Internet (IKE)	51
2.5.1.5.	Asociaciones de Seguridad (SA)	53
2.5.1.6.	Administración de Claves En IPSec	54
2.5.1.7.	Funcionamiento de IPSec	54
CAPITULO III		
MATERIALES Y METODOS		
3.1.	MATERIALES	56
3.1.1.	Hardware	56



3.1.2. Software.....	56
3.2. TIPO Y DISEÑO DE LA INVESTIGACIÓN	56
3.2.1. Tipo de Investigación	56
3.2.2. Diseño de la Investigación.....	57
3.2.3. Nivel de la Investigación	57
3.3. POBLACIÓN Y MUESTRA DE LA INVESTIGACIÓN.....	57
3.3.1. Población	57
3.3.2. Muestra	59
3.4. UBICACIÓN Y DESCRIPCIÓN.....	59
3.4.1. Ubicación.....	59
CAPÍTULO IV	
RESULTADOS Y DISCUSIÓN	
4.1. DESCRIPCIÓN DE LA INVESTIGACIÓN	60
4.1.1. Procedimiento de Diseño del Prototipo.....	60
4.1.1.1. Topología.....	60
4.1.1.2. Configuración de Dispositivos.....	61
4.2. DISCUSIÓN.....	105
V. CONCLUSIONES	107
VI. RECOMENDACIONES.....	108
VII. REFERENCIAS BIBLIOGRÁFICAS.....	109

Área: Telecomunicaciones

Línea: Redes y computadoras

FECHA DE SUSTENTACIÓN: 19 de setiembre de 2023



ÍNDICE DE FIGURAS

Figura 1: Funcionamiento tunneling.	39
Figura 2: VPN sitio a sitio.	43
Figura 3: VPN de acceso remoto.	45
Figura 4: VPN over LAN.	47
Figura 5: Funcionamiento del protocolo IKE.	52
Figura 6: Topología de red del escenario.	60
Figura 7: Configuración de direccionamiento en R1.	61
Figura 8: Configuración de direccionamiento en R2.	62
Figura 9: Configuración de direccionamiento en R3.	63
Figura 10: Configuración de direccionamiento en el cliente.	63
Figura 11: Verificación de configuración en el cliente.	64
Figura 12: Verificación de configuración desde cliente a R3.	64
Figura 13: Configuración en la computadora de registro y archivo académico.	65
Figura 14: Prueba de conectividad fallida.	65
Figura 15: Verificación de configuraciones en la computadora de archivo y registro académico.	66
Figura 16: Desactivar el cortafuegos en la computadora de archivo y registro académico	66
Figura 17: Desactivar el cortafuegos en la computadora cliente.	67
Figura 18: Conectividad desde el cliente hacia archivo y registro académico.	67
Figura 19: Conectividad desde archivo y registro académico hacia el cliente.	68
Figura 20: Configuraciones básicas en R1.	68
Figura 21: Preparación de R3 para su uso con CCP.	69



Figura 22: Configuración de usuario y autenticación HTTP.....	69
Figura 23: Instalación de CCP.....	69
Figura 24: Requisitos para uso de CCP.....	70
Figura 25: Sitio de descarga de Java.	70
Figura 26: Progreso de instalación de Java.	71
Figura 27: Java en el Panel de Control.....	71
Figura 28: Agregando una excepción en Java.....	72
Figura 29: Agregar el sitio que usa CCP en la computadora local.....	72
Figura 30: Inicio De CCP.....	73
Figura 31: Mensaje de advertencia para el uso de la aplicación.	73
Figura 32: Mensaje de mejoras para los productos de Cisco.	74
Figura 33: Acceso a R3 usando CCP.	75
Figura 34: Descubrimiento de R3.....	76
Figura 35: Firewall en R3 usando CCP.....	76
Figura 36: Configuración de interfaces en el Cortafuegos.....	77
Figura 37: Configuración del nivel de seguridad.	78
Figura 38: Configuraciones en el Cortafuegos.....	78
Figura 39: Comandos enviados para configurar ZBF.	79
Figura 40: Prueba de conectividad hacia Internet.	79
Figura 41: Prueba de ping desde el exterior hacia la red interna.....	80
Figura 42: Inicio de configuración de Easy VPN Server.	80
Figura 43: Consulta para activar AAA en el servidor.	81
Figura 44: Comandos enviados a R3 para configurar AAA.....	81
Figura 45: Indicaciones de Easy VPN Server.	82



Figura 46: Configuración de interfaz en el servidor VPN (R3).	82
Figura 47: Algoritmos para implementar el servidor VPN.	83
Figura 48: Configuración de Transform Set.....	84
Figura 49: Configuración de AAA para ISAKMP.	84
Figura 50: Configuración del servidor AAA para usuarios.....	85
Figura 51: Configuración de un nuevo usuario.	86
Figura 52: Configuración de autorización y políticas de grupo.	86
Figura 53: Configuración del grupo de políticas.	87
Figura 54: Configuración del tiempo de espera para clientes.	88
Figura 55: Protocolo de Control de Túnel de Cisco.	88
Figura 56: Modificación del cortafuegos para la VPN.....	89
Figura 57: Resumen de configuraciones del servidor VPN.	90
Figura 58: Comandos de configuración del servidor VPN.	90
Figura 59: Botón de prueba del servidor VPN.	91
Figura 60: Prueba del servidor VPN exitosa.	92
Figura 61: Instalación de Cisco Systems VPN Client.	92
Figura 62: Ejecución de Cisco Systems VPN Client.....	93
Figura 63: Configuración del servidor (Host) y grupo de autenticación en el cliente. .	94
Figura 64: Usuario y contraseña del cliente VPN.	94
Figura 65: Antes y después de configurar el cliente VPN.....	95
Figura 66: Prueba de ping después de configurar el cliente VPN.....	96
Figura 67: Estadísticas del cliente VPN.	97
Figura 68: Interfaz virtual levantada para la VPN en el servidor R3.	97
Figura 69: Prueba de conectividad continua.	98



Figura 70: Captura de paquetes en la máquina ubicada en la LAN de R3.....	98
Figura 71: Directorio con un archivo que será compartido en la red.	99
Figura 72: Propiedades de directorio para compartirlo en la red.	99
Figura 73: Activación del folder compartido.	100
Figura 74: Acceso al recurso compartido desde el cliente.	100
Figura 75: Carpetas compartidas en la máquina de destino.	101
Figura 76: Transferencia del archivo hacia el cliente externo.....	101
Figura 77: Captura de la transferencia de un archivo con Wireshark.	102
Figura 78: Captura de ICMP.	103
Figura 79: Captura de TCP.....	104
Figura 80: Captura de SMB2.....	105



ÍNDICE DE TABLAS

Tabla 1: Estructura de un encabezado AH.	50
Tabla 2: Estructura de un paquete ESP.....	51
Tabla 3: Tabla de direccionamiento	61



ÍNDICE DE ACRÓNIMOS

- VPN:** Virtual Private Network
- IPSEC:** Internet Protocol security
- IP:** Internet Protocol
- OSI:** Open Systems Interconnection
- LAN:** Local Area Network
- SSL:** Secure Sockets Layer
- L2VPN:** Layer 2 Virtual Private Networks
- MPLS :** Conmutación de Etiquetas Multiprotocolo
- ACID:** Atomicity, Consistency, Isolation and Durability
- CSMA/CD:** Carrier Sense Multiple Access/Collision Detection
- BLE:** Bluetooth Low Energy
- CPU:** Central Processing Unit
- ENIAC:** Electronic Numerical Integrator and Computer
- ETL:** Extract, Transform and Load
- GSM:** Global System for Mobile Communications
- IA:** Inteligencia Artificial
- IDE:** Integrated Development Environment
- IoT:** Internet of Things
- M2M:** Machine to Machine
- MCU:** Multipoint Control Unit
- MIT:** Massachusetts Institute of Technology
- OLAP :** On-Line Analytical Processing
- RAM:** Random Access Memory
- SDCC:** Secure Direct Client-to-Client
- ROM:** Read-Only Memory
- CPU:** Central Processing Unit
- WAN:** Wide Area Network



RESUMEN

La administración de la red en la Universidad Nacional del Altiplano se realiza internamente desde la red de área local. Se propone diseñar una red privada virtual utilizando IPSec para permitir la administración remota sin comprometer la seguridad. El objetivo es proporcionar a los administradores de red acceso remoto seguro a la red como si estuvieran en el mismo lugar físico. Esto se logra mediante un router que actúa como servidor, brindando acceso a los administradores desde dispositivos finales, creando así una red privada virtual segura que abarca Internet, considerado inseguro. La red debe ser segura, fiable y privada, y se implementa con software y hardware, principalmente software que utiliza IPsec y otros protocolos de seguridad IP necesarios. Se ha diseñado e implementado con éxito esta red privada virtual, pasando pruebas de conectividad y gestión satisfactorias. Se realizan capturas de paquetes con Wireshark para demostrar la seguridad de IPsec, que incluye integridad de datos, cifrado, autenticación y disponibilidad. Además, se ha considerado la escalabilidad de la red. Se han implementado servicios de red para administrar y configurar dispositivos y servidores en el centro de datos de la Universidad. Esto permite a un administrador externo y remoto operar virtualmente dentro de la red institucional. La implementación se llevó a cabo en una simulación de Internet y la red institucional, utilizando el sistema operativo Cisco IOS en GNS3 para emular varios dispositivos que conforman la red privada y la red pública.

Palabras Clave: Red privada virtual (vpn), acceso remoto, seguridad IP (IPsec), confiabilidad, privacidad.



ABSTRACT

Network administration at the Universidad Nacional del Altiplano is done internally from the local area network. It is proposed to design a virtual private network using IPSec to allow remote administration without compromising security. The goal is to provide network administrators with secure remote access to the network as if they were in the same physical location. This is achieved by a router that acts as a server, providing access to administrators from end devices, thus creating a secure virtual private network that spans the Internet, considered insecure. The network must be secure, reliable, and private, and is implemented with software and hardware, primarily software that uses IPsec and other necessary IP security protocols. This virtual private network has been successfully designed and implemented, passing satisfactory connectivity and management tests. Wireshark packet captures are performed to demonstrate IPsec security, including data integrity, encryption, authentication, and availability. In addition, the scalability of the network has been considered. Network services have been implemented to manage and configure devices and servers in the University's data center. This allows a remote, external administrator to operate virtually within the institutional network. The implementation was carried out in a simulation of the Internet and the institutional network, using the Cisco IOS operating system on GNS3 to emulate various devices that make up the private network and the public network.

Keywords: Virtual private network (VPN), remote access, security IP (IPsec), reliability, privacy.



CAPÍTULO I

INTRODUCCIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA

Se plantea como estrategia para mejorar la gestión de la red de la Universidad Nacional del Altiplano Puno la creación y aplicación de una red privada virtual (VPN) utilizando IPSec. El objetivo principal de esta implementación es facilitar una administración eficaz de la red universitaria a distancia.

La adopción de una VPN basada en IPSec tiene varias ventajas, incluida la capacidad de establecer conexiones cifradas y seguras a través de redes públicas, como Internet. Esto facilita la administración remota de la red universitaria sin comprometer la seguridad de los datos que se transmiten.

El uso de IPSec asegura la integridad, autenticación y confidencialidad de la información intercambiada entre los nodos de la red. Esta solución proporciona un entorno seguro para la administración remota, evitando posibles vulnerabilidades y ataques externos.

La implementación de esta solución estratégica permitirá a la Universidad Nacional del Altiplano Puno aprovechar las ventajas de la red privada virtual, como flexibilidad, escalabilidad y eficiencia en la administración de la red. Además, garantizará la protección de datos sensibles y dará más confianza en la gestión de la red universitaria.

Una red privada virtual usando IPSec nos permitirá conectar usuarios remotos a la LAN del administrador de la red de la universidad, a través de la infraestructura pública (Internet) de forma segura, ya que los datos deberán transmitirse a través de un canal



encriptado. Conectarse a través de Internet tendrá un coste económico de despliegue muy bajo y la conexión podrá establecerse desde cualquier punto geográfico del planeta.

La investigación se desarrolló en la Universidad Nacional del Altiplano, en el Laboratorio de Cómputo de Telecomunicaciones de la Escuela de Ingeniería Electrónica Profesional.

El trabajo de las personas que utilizan la tecnología como herramienta de apoyo en el día a día ya no se limita a un puesto fijo en la oficina corporativa. Con el desarrollo de la tecnología y la necesidad de que las empresas brinden sus servicios las 24 horas del día a través de Internet, muchos factores conducen a la necesidad de transferir datos privados corporativos de manera segura a través de Internet. . A medida que evoluciona la seguridad de la información, también lo hacen los ciberdelincuentes, que buscan constantemente nuevas formas de interceptar datos privados para una variedad de propósitos. Es posible que los sistemas de información no sean completamente seguros, pero el uso de una VPN para establecer el acceso remoto reduce en gran medida la posibilidad de que dichos datos sean interceptados.

En comparación con otras alternativas como SSL, IPSec ofrece una ventaja significativa. A nivel de red, IPSec se puede implementar sin afectar la funcionalidad de las aplicaciones existentes en la red. Una vez que se establece una conexión mediante IPSec, se pueden transferir varios tipos de datos, como correo electrónico, transferencias de archivos y telefonía IP, sin necesidad de instalar herramientas de aplicación adicionales.

IPSec es ampliamente reconocido como el método más seguro para conectarse a redes privadas virtuales en Internet. Este estándar ofrece una autenticación confiable y encriptación de paquetes IP en la capa de red del modelo Open System Connectivity



(OSI). Además de su seguridad, IPSec destaca por su excelente interoperabilidad entre diferentes fabricantes de redes, lo que lo convierte en la solución más rentable para conexiones VPN.

1.2. PLANTEAMIENTO DEL PROBLEMA

Actualmente la administración de la red de la Universidad Nacional del Altiplano se viene desarrollando de forma interna, es decir, desde la red de área local, lo que se propone es diseñar una red privada usando IPSec para una administración remota sin perder la seguridad de la red universitaria.

1.3. HIPÓTESIS DE LA INVESTIGACIÓN

1.3.1. Hipótesis General

El diseño e implementación de una red privada virtual usando IPSec permitirá administrar remotamente la red institucional de la Universidad Nacional del Altiplano.

1.3.2. Hipótesis Específicas

- El establecimiento de los servicios de red de acceso permitirá la administración y configuración de dispositivos de red y servidores dentro de la infraestructura de tecnologías de la información de la Universidad Nacional del Altiplano.
- La implementación de la red privada virtual usando IPSec permitirá el acceso a la red institucional a través de Internet.

1.4. OBJETIVOS DE LA INVESTIGACIÓN

1.4.1. Objetivo General

Diseñar e implementar una red privada virtual usando IPSec para administrar remotamente la red institucional de la Universidad Nacional del Altiplano.



1.4.2. Objetivos Específicos

- Establecer los servicios de red de acceso para la administración y configuración de dispositivos de red y servidores dentro de la infraestructura de tecnologías de la información de la Universidad Nacional del Altiplano.
- Implementar la red privada virtual usando IPSec sobre Internet y la red institucional.



CAPÍTULO II

REVISIÓN DE LITERATURA

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

La tecnología VPLS (Virtual Private LAN Service) basado en Ethernet es un mecanismo transparente, protocolo independiente, L2VPN (Layer 2 Virtual Private Networks) multipunto para interconectar redes remotas sobre IP (Protocolo de Internet) o MPLS (Conmutación de Etiquetas Multiprotocolo) basadas en redes de proveedores. Las redes VPLS ahora se están volviendo atractivas en muchas aplicaciones empresariales, como los servicios de videoconferencia (VCI), voz sobre IP (VoIP) y videoconferencia debido a su operación simple, independiente del protocolo y rentable. Sin embargo, estas nuevas aplicaciones VPLS exigen requisitos adicionales, como seguridad elevada, escalabilidad mejorada, uso óptimo de los recursos de red y una mayor reducción de los costos operativos. Por lo tanto, la motivación de esta tesis es desarrollar arquitecturas VPLS seguras y escalables para futuras redes de comunicación. En primer lugar, se propone una arquitectura de VPLS plana escalable segura basada en un Protocolo de identidad de host (HIP). Contiene un mecanismo de seguridad basado en clave de sesión y un mecanismo de transmisión eficiente que aumenta la capacidad de ampliación y la escalabilidad del plano de seguridad de las redes VPLS. En segundo lugar, se propone una arquitectura segura jerárquica VPLS para lograr la escalabilidad del plano de control. Un nuevo mecanismo de reenvío de tramas seguras basado en etiquetas cifradas está diseñado para transportar tramas L2 a través de una red VPLS jerárquica. En tercer lugar, un nuevo protocolo distribuido de árbol de expansión (DSTP) está diseñado para mantener una red Ethernet sin bucles a través de una red VPLS. Con DSTP se propone ejecutar una instancia modificada de STP (Spinning Tree Protocol) en cada segmento remoto de la red VPLS. Además, se usan dos Mecanismos de Identificación de



Redundancia (RIM) denominados RIM asociados al cliente (CARIM) y RIM asociados al proveedor (PARIM) para mitigar el impacto de los bucles invisibles en la red de proveedores. Por último, un VPLS (Soft VPLS) la arquitectura está diseñada para superar las limitaciones de administración de túneles en arquitecturas VPLS seguras heredadas. Además, se proponen tres nuevos mecanismos que nos permita mejorar el funcionamiento con respecto a las funciones de gestión de túneles heredadas: Un mecanismo dinámico de establecimiento de túneles, un mecanismo de reanudación de túneles y un rápido mecanismo de transmisión. La arquitectura propuesta utiliza un controlador centralizado para dirigir el establecimiento del túnel VPLS basado en el comportamiento de la red en tiempo real. Por lo tanto, los resultados de la tesis ayudarán a un diseño y desarrollo de sistemas más seguro, escalable y eficiente de las redes VPLS. Además, contribuirá a mejorar la eficiencia en el uso de los recursos de la red y a reducir aún más los costos operativos de las redes VPLS en el futuro (Biga et al., 2020).

En primer lugar, se abordan los principios fundamentales de la topología de una red estable, ya sea esta de naturaleza corporativa o no. A continuación, se presentan y explican brevemente las vulnerabilidades de red y las tecnologías de seguridad actuales. Estas tecnologías son estándar y, aunque la red se basa en equipos de Cisco Systems, se busca que todos los aspectos del diseño sean lo más generales posible, independientemente de la plataforma específica. Es precisamente en el diseño de seguridad de la red donde se busca cumplir los seis requisitos mencionados anteriormente, utilizando tecnologías como Secure Shell, túneles L2TP y encriptación IPsec. Por último, la implementación se traducirá en scripts de configuración de los equipos de telecomunicaciones apropiados para las tareas requeridas, teniendo en cuenta también consideraciones de costos y siempre manteniendo presente el equilibrio entre seguridad y costo (Cobos Briones, 2021).



un concepto de IPsec utilizando planes de datos programables P4 en redes definidas por software (SDN). El prototipo funciona con ESP en modo túnel y admite varios conjuntos de cifrado. Los conmutadores P4 compatibles están configurados para funcionar como puntos finales del túnel IPsec. Además, ofrecemos un agente de cliente para configurar extremos de túneles en hosts Linux para admitir escenarios de aplicaciones de host a host y de sitio a sitio, que son la base de las redes privadas virtuales (VPN). Mientras que las VPN tradicionales requieren protocolos de intercambio de claves complejos como IKE para configurar y renovar los puntos finales del túnel, P4 IPsec se beneficia de un controlador SDN para realizar estas tareas. Uno de los objetivos de este trabajo experimental es investigar qué tan bien se puede implementar P4 IPsec en los conmutadores P4 existentes. Presentamos un prototipo para el conmutador de software BMv2 P4, evaluamos su rendimiento y publicamos su código fuente en GitHub. Explicamos por qué no pudimos proporcionar una implementación útil con la placa Net FPGA SUME. Para el conmutador basado en Tofino Edgecore Wedge 100BF 32X, presentamos dos implementaciones prototipo para hacer frente a una unidad criptográfica faltante. Como otra contribución de este documento, brindamos antecedentes tecnológicos de P4 e IPsec y brindamos una revisión exhaustiva de las aplicaciones de seguridad en P4, IPsec en SDN e implementaciones del plano de datos de IPsec. Según nuestro conocimiento, P4 IPsec es la primera implementación de IPsec para SDN basado en P4 (Castro Serantes, 2021).

Un método completo para validar y evaluar los protocolos de seguridad IPsec en un entorno de servidor Windows se ha desarrollado. El enfoque creado incluye la implementación de reglas de conexión segura con IPsec, que protegen la información transmitida entre los clientes y los servidores, esto que permite una conexión segura y confiable. El objetivo fundamental es establecer una sólida seguridad para evitar el robo



de datos confidenciales que están bajo la gestión del laboratorio de Ecu Ciencia. Para lograr este objetivo, se emplea la conexión TCP, que envuelve la información en el protocolo ESP, asegurando su encapsulamiento seguro. Además, se lleva a cabo un intercambio dinámico de contraseñas utilizando KerberosV5, asegurando la autenticidad de las partes involucradas en la comunicación. Ya se ha creado un método integral para validar y evaluar los protocolos de seguridad IPSec en un entorno de servidor Windows. El método se basa en una exhaustiva recopilación de diversas fuentes primarias que respaldan su base científica y técnica. Estas fuentes abarcan libros, artículos científicos, tesis y la página web de Microsoft. Para respaldar el diseño e implementación de este enfoque de validación y evaluación, se han utilizado dos metodologías: la metodología Top Down y una metodología específica de validación y evaluación. Se realizaron pruebas exhaustivas utilizando IPSec, utilizando un laboratorio de pruebas para simular los equipos físicos disponibles. Se empleó el marco de trabajo sugerido para realizar un análisis minucioso del protocolo IPSec (Rubio, 2021).

La importancia de las redes de comunicaciones en la tecnología de la información se debe a que permiten el intercambio de información entre una variedad de sistemas informáticos, desde computadoras personales hasta cajeros automáticos y computadoras integradas en vehículos. Los protocolos de comunicación regulan estos intercambios de información y evalúan la mejor manera de transmitir la información entre diferentes entidades. Sin embargo, en muchos casos, los intercambios requieren servicios de seguridad como confidencialidad, autenticación y no repudio, que no se contemplan en los protocolos iniciales desarrollados durante la expansión de las redes de comunicación. Para abordar esta falta de seguridad, se han creado protocolos y arquitecturas de seguridad que brindan los servicios de seguridad que necesitan los diferentes protocolos de comunicación. La arquitectura de seguridad IPsec se ha popularizado porque se integra



perfectamente con los protocolos de red de próxima generación, esto que facilita la transparencia de la arquitectura para las aplicaciones y los usuarios y facilita la migración fuera de problemas. Sin embargo, la implementación de estos protocolos y arquitecturas de seguridad ha planteado nuevos desafíos, como la dificultad para que las implementaciones se comuniquen entre sí y la mayor vulnerabilidad a los ataques de denegación de servicio. En este estudio se presenta una metodología integral para evaluar el grado de cumplimiento de la implementación de un protocolo o arquitectura de seguridad con los estándares y el rendimiento esperados, con el objetivo de abordar estos problemas. El propósito principal es minimizar dichos problemas y garantizar un funcionamiento óptimo del sistema. Esta técnica se centra específicamente en la arquitectura de seguridad IPsec y demuestra su utilidad práctica. Se exponen los resultados de la evaluación de múltiples implementaciones de IPsec como parte de este estudio (Duran Pamplona, 2020).

Se sugiere que una empresa comercial utilice una VPN (Red Privada Virtual) basada en el protocolo IPSec como opción tecnológica segura y económica para conectar de forma segura las diferentes sucursales de la empresa, en lugar de utilizar líneas dedicadas costosas. En primer lugar, se realizará un examen del desarrollo de Internet, la diversidad de enlaces de área amplia (WAN) privados y la disponibilidad de proveedores de servicios de Internet en nuestro país. Además, se proporcionará una descripción detallada del protocolo de seguridad IPSec y las Redes Privadas Virtuales (VPN). Este análisis evaluará la situación actual de la empresa comercial y presentará varios escenarios para la implementación de una VPN. El objetivo fundamental de implementar un prototipo de VPN es demostrar que esta tecnología es viable para la empresa y que el uso de IPSec permite establecer comunicaciones seguras a través de Internet. De esta



manera, se busca demostrar que la VPN es una buena opción para proteger las comunicaciones de la empresa (López Manjarres, 2019).

La comunicación de datos vulnerables a las escuchas telefónicas se facilita mediante el uso de una red de intranet. Para solucionar esto, utilice una red virtual privada. Las VPN L2TP e IPsec ofrecen niveles diferentes de seguridad, especialmente en términos de seguridad. Este estudio analizó el funcionamiento de las redes VPN L2TP e IPsec en servidores SMB, enrutadores Mikrotik y servidores Ubuntu para su configuración VPN. En este estudio, se diseñó una VPN L2TP e IPsec configurando el enrutador Mikrotik RB 450G y configurando el servidor SMB utilizando la GUI del servidor Ubuntu 18.04. Para la evaluación de la seguridad, Utilice técnicas de piratería para recopilar datos de inicio de sesión de servidores VPN y servidores SMB, así como técnicas de rastreo para recopilar datos de inicio de sesión de servidores SMB. utilizando los parámetros de retraso, rendimiento y pérdida de paquetes para el análisis de rendimiento. El programa para verificar Wireshark se puede usar en la interfaz GUI para capturar todos los paquetes de datos. El objetivo de la investigación es desarrollar una tecnología VPN basada en L2TP e IPsec para que se pueda evaluar el desempeño después de implementar una VPN basada en L2TP e IPsec. Como resultado, una VPN puede conectarse a HO a HO and HO a HO o desde una conexión pública en una conexión local. El servidor Ubuntu que se utiliza también funciona correctamente (Rivera Morla, 2022).

2.2. FUNDAMENTOS DE LAS REDES PRIVADAS VIRTUALES

2.2.1. Redes de Computadoras

2.2.1.1. Definición

El concepto clave que se utiliza para describir la interconexión de dos o más computadoras a través de un dispositivo especializado, lo que les permite compartir



recursos entre sí. Esta conexión entre computadoras se puede establecer mediante distintos medios, como cables de cobre, también los rayos infrarrojos, consecutivamente también la fibra óptica entre otros.

El propósito principal de la creación de las redes fue facilitar la conexión y poder intercambiar información y recursos para entornos de tipo local, además de proporcionar una forma sencilla de conectar ubicaciones físicamente separadas. Con el paso del tiempo, este avance en las comunicaciones ha llevado a integrar herramientas nuevas lo que permiten una colaboración entre computadoras de diferentes fabricantes. Como resultado, las computadoras interconectadas muestran ventajas, ya que evitan una necesidad para transferir información manualmente mediante dispositivos de almacenamiento portátiles. Gracias a las redes, el intercambio de información no se limita únicamente al ámbito local, sino que también se realiza a larga distancia y a nivel global de manera instantánea. Este avance hace posible la transformación para la acción de comunicarnos y compartir datos, permitiéndonos una mayor eficiencia y rapidez en el intercambio de información en diferentes escalas geográficas (Vinicio, 2021).

2.2.1.2. Clasificación

Las redes informáticas se pueden clasificar según la capacidad a nivel físico para encontrar sus componentes. Estas clasificaciones incluyen redes domésticas, redes corporativas, redes de campus, redes nacionales e incluso redes globales. Cada uno de ellos se describe brevemente a continuación:

- Para la red local que también es denominado como LAN, es una red privada ubicada en un área local, como una oficina, apartamento o edificio. Con respecto a la velocidad de este tipo de tecnologías es de 10 Mbps a 10 Gbps.
- Red de Área del Campus (CAN):



- Estas son LAN ubicadas en edificios en un área fija y conectadas para formar una sola red. El enlace de alta velocidad permite la comunicación.
- Red Metropolitana (MAN):
- Las LAN están conectadas por medio de enlaces que contienen una velocidad máxima el cual tiene infraestructuras con redundancia en la conectividad para evitar un descarte entre un punto y otro, como también es ofrecido por la empresa que brinda el servicio.
- Para el tipo en base a la conectividad en áreas amplias, también conocida como WAN, el cual refiere a una red que realiza una conexión entre muchas redes de tipo locales. Las tasas de transferencia son altas y son de su propiedad. Existe una opción adicional llamada acceso de banda ancha, que incluye servicios como ADSL y módems de cable. Operan en grandes áreas geográficas y brindan servicios remotos de tiempo completo.
- Red de área de almacenamiento (SAN): A pesar de su nombre, esta aplicación está enfocada a negocios que almacenan grandes cantidades de datos.
- Para las redes de tipo personal de tipo inalámbricas como es la WPAN es un tipo de red independiente. Debe permitir conexiones inalámbricas entre ordenadores, teléfonos móviles y otros dispositivos, así como un amplio rango de velocidades de transmisión (Vacas Andrade, 2019).

2.2.1.3. Topología

Para la topología que conectara diseños lógicos o físicos de como un dispositivo y también nodo para una red que se conectan a través de los medios. La forma en que se establece interconexión para un nodo en la red que se ve afectada por la topología de la red. Mientras que algunas topologías son más complejas en términos de configuración y estructura, otras permiten conexiones simples entre nodos.



Tener conocimiento sobre qué topología utilizar en diferentes situaciones es fundamental, ya que una elección inapropiada puede resultar en un mal funcionamiento de la red.

Para una red puede clasificarse en dos categorías: física y también de tipo lógica. Con respecto al aspecto físico este se define como el diseño de forma física en el tipo de red que se constituye, abarcando aspectos como la ubicación y la instalación del equipo. Por otro lado, la topología lógica se centra en la configuración virtual de la red.

Es esencial comprender ambas terminologías para garantizar una implementación adecuada de la red y evitar problemas de rendimiento o fallos en la comunicación (Berrio Rufino, 2021).

Topologías Físicas: existen fundamentalmente cuatro tipos principales, de los cuales se derivan diversas combinaciones. Estas son:

- La topología de bus se distingue por la presencia de un cable central a través del cual se pueden conectar de forma física y por lo tanto los dispositivos tendrán que estar interconectados a una sola única red. Este cable o canal permite la propagación de señales en ambas direcciones, esto cual permite que todos los dispositivos reciban las señales de los demás dispositivos. Esta característica puede resultar ventajosa cuando se requiere que todos los dispositivos tengan acceso a la misma información. Sin embargo, también puede ser una desventaja debido al tráfico en la red, ya que existe la posibilidad de colisiones que pueden afectar su rendimiento.
- La topología en anillo se distingue por conectar todos los dispositivos de la red, como computadoras, impresoras, escáneres, etc., secuencialmente, formando un anillo cerrado. Esta configuración solo conecta cada dispositivo o nodo con los



dos dispositivos o nodos adyacentes. Cada nodo o dispositivo debe transferir la señal al nodo adyacente en la secuencia establecida para que la señal pueda circular por el anillo. De esta manera, la señal recorre el anillo pasando de un dispositivo a otro hasta llegar a su destino. Esta topología ofrece un enfoque ordenado y estructurado para la comunicación en la red, pero requiere un funcionamiento adecuado de todos los dispositivos y poder contener una integridad de una señal para un anillo (Andrés Roig, 2017).

- La topología en anillo se caracteriza por una interconexión secuencial para todos los equipos en una red, como computadoras, impresoras y escáneres, formando un anillo cerrado. En esta configuración, cada dispositivo o nodo está conectado únicamente con los dos dispositivos o nodos adyacentes. Para que la señal pueda circular a lo largo del anillo, cada dispositivo o nodo debe transferirla al siguiente nodo en la secuencia establecida. De esta manera, la señal viaja por el anillo, pasando de un dispositivo a otro hasta llegar a su destino. La topología en anillo proporciona una estructura ordenada y organizada para la comunicación en la red, pero requiere un correcto funcionamiento de todos los dispositivos para mantener la integridad de la señal a lo largo del anillo.
- En la topología en Malla, todos los dispositivos, o al menos algunos de ellos, están interconectados entre sí para lograr redundancia y tolerancia a fallos. En caso de que un enlace falle, la información puede ser redirigida a través de otro enlace disponible. Esta configuración de topología es comúnmente utilizada en redes WAN para garantizar una mayor fiabilidad y disponibilidad del sistema.
- La topología híbrida es el resultado de combinar diferentes tipos de topologías de red, lo que le otorga su nombre. Se utiliza esta configuración cuando la infraestructura de red se vuelve compleja o cuando aumenta la cantidad de



equipos, esto refiere que la topología híbrida que pueda satisfacer estas necesidades particulares (Bonastre Pina, 2019).

- En la topología con medio compartido, todos los dispositivos de la red tienen la capacidad de acceder al mismo medio de comunicación en cualquier momento. Esta característica puede ser tanto una ventaja como una desventaja. La fundamental desventaja del compartir el médium de comunicación es que en dos o más nodos transmiten al mismo momento, pueden ocurrir colisiones. Esto resulta en la pérdida de paquetes y la necesidad de retransmitirlos hasta que no se produzcan colisiones adicionales. La topología de medio compartido es eficiente en redes pequeñas; pero cuando los nodos tienen aumento en su cantidad de implementación aumentara y también proporcionalmente una posibilidad de posibles colisiones. (Vacas Andrade, 2019).
- Las topologías lógicas basadas en tokens se distinguen por usar un testigo o estafeta, también conocido como token, para proporcionar acceso al médium físico de comunicación. Solo el nodo que tiene el token en ese momento puede transmitir o recibir información porque este token circula vía la red en un orden lógico. A diferencia de las topologías basadas en medio compartido, en las topologías basadas en token todos los nodos no pueden transmitir simultáneamente, ya que se requiere poseer el token para llevar a cabo la acción. El mayor inconveniente de este enfoque es la latencia, que es el tiempo que tarda un token en dar la vuelta completa para poder propagarse en un nodo en particular. Pero la ventaja de este método es que no hay colisiones. Las topologías físicas en forma de anillo más adecuadas para las redes basadas en tokens (Gladys Patricia, Alexis Eduardo, Cristhian Salomón, & Eduardo Enrique, 2019).



2.2.1.4. Componentes

Una red de computadoras está compuesta por diversos equipos que desempeñan funciones fundamentales para asegurar su correcto funcionamiento. Estos dispositivos son esenciales dentro del marco del modelo de referencia OSI, ya que son capaces de controlar y regular el flujo de información:

- El concentrador (Hub) es un dispositivo que ha quedado en desuso, aunque aún se utiliza en muchas instalaciones como un medio de conexión entre redes locales. El hub, alimentado por energía eléctrica, se encarga de transmitir los datos de un puerto a todos los puertos conectados en el mismo segmento de red, excepto el puerto desde el cual se enviaron los datos.
- La introducción del hub tuvo un impacto significativo en la arquitectura de las redes. Este dispositivo concentrador conectó directamente cada computadora de la red, reemplazando la topología física del bus lineal tradicional (Brunson, 2015).
- El creciente tráfico de datos ha generado dificultades en la comunicación entre los equipos de las redes. Para realizar la solución a un problema, se hace el desarrollo dispositivos llamados conmutadores.
- Los conmutadores, como dispositivos de capa de enlace de datos del modelo OSI, emplean la dirección MAC presente en la trama Ethernet para su funcionamiento. Estos dispositivos almacenan en memoria las conexiones entre sus puertos y las direcciones MAC de los dispositivos conectados en dicho extremo opuesto para un cable. Los puertos del conmutador pueden tener asociadas una o más direcciones MAC, dependiendo del dispositivo conectado.
- El enrutador es un dispositivo de red que se distingue del resto porque puede conectar redes internas y externas.



- Los enrutadores, al igual que las computadoras personales, dependen de un sistema operativo para ejecutar aplicaciones de software y generar archivos de configuración esenciales para su funcionamiento. Estos archivos de configuración contienen instrucciones precisas para controlar y gestionar el flujo de tráfico tanto de entrada como de salida a través de las interfaces del enrutador. Además, incluyen información detallada sobre los protocolos de enrutamiento utilizados en la LAN, como IP, IPX, así como los protocolos de enrutamiento RIP, EIGRP, OSPF y BGP utilizados para conectarse con otros enrutadores. Los protocolos de enrutamiento permiten que los enrutadores se comuniquen entre sí, intercambiando información sobre sus redes y seleccionando la mejor ruta para enviar los datos, lo que posibilita la conectividad de extremo a extremo (Berrio Rufino, 2021).

2.2.2. Modelo OSI

2.2.2.1. Definición

Con el fin de asegurar la integración de equipos provenientes de diferentes proveedores en la red y evitar situaciones confusas, el modelo de referencia Interconexión del sistema abierto, estandarizado por la Organización Internacional de Normalización (ISO), ha sido desarrollado. Este modelo define una estructura por niveles o capas. Su propósito principal radica en simplificar la interconexión de sistemas provenientes de diversas fuentes, posibilitando el intercambio fluido de información sin restricciones impuestas por los protocolos propietarios utilizados por cada fabricante.

El modelo Open Systems InterConnection (OSI) no se enfoca en definir un modelo de red o topología específico. No tiene que especificar o definir los protocolos de comunicación porque funcionan WITHOUT el modelo. En cambio, lo que hace el modelo



OSI es establecer la funcionalidad de los protocolos con el objetivo de lograr un estándar común (Liyakkathali, Furtado, Sugumar, & Mathur, 2022).

2.2.2.2. Tipos de Servicio

El modelo OSI establece dos tipos básicos de servicios para las telecomunicaciones:

- Comunicación orientada a la conexión: Se requiere establecer una conexión a través de un circuito para intercambiar información. Un ejemplo de este tipo de comunicación es un teléfono, ya sea móvil o fijo, donde se establece una conexión antes de poder intercambiar mensajes.
- Comunicación fuera de línea:
- No es necesario configurar un circuito de antemano para enviar o recibir información. Los mensajes se envían con una dirección de destino y deben llegar lo más rápido posible, pero no necesariamente en orden. Un ejemplo común de esto es enviar un correo electrónico (Iturralde Piedra & Serrano Vázquez, 2020).

2.2.2.3. Capas del Modelo OSI

Dicho modelo comprende 7 niveles o capas de abstracción, cada uno con su propia función, trabajando de forma independiente pero cooperativa para lograr un objetivo final. Esta estructura en capas permite la interoperabilidad de diferentes protocolos al centralizar funciones específicas en cada nivel operativo. Cada capa se puede cambiar sin afectar a las otras capas porque funcionan de forma independiente.

Para iniciar la transferencia de información, la máquina emisora envía los datos desde la capa superior hasta la capa física para su transmisión. En la máquina receptora, los datos llegan a la capa física y atraviesan las diferentes capas hasta llegar a la capa superior más alta en ese sistema (Andrés Roig, 2017).



Capa física: La capa física se encarga de determinar las características del medio de transmisión, como los cables utilizados, su longitud, la tasa de baudios y la necesidad de repetidores para regenerar la señal en intervalos específicos. También define cómo se representarán los valores lógicos de 0 y 1 mediante voltajes o niveles de voltaje.

La capa de enlace de datos tiene la responsabilidad de facilitar la comunicación entre los componentes físicos de una red. Su función principal implica administrar la dirección física de los datos, controlar el acceso a los medios de transmisión y, de manera especial, detectar errores durante la transmisión. Además, esta capa se encarga de construir tramas de bits que contienen información y otros elementos esenciales para controlar la transmisión, asegurando la precisión y evitando la presencia de errores (Berrio Rufino, 2021).

Por lo general, esta capa se divide en dos subcapas conocidas como Control Lógico de Enlace (LLC, por sus siglas en inglés) y Control de Acceso al Medio (MAC, por sus siglas en inglés). La subcapa LLC se encarga de establecer y finalizar conexiones, así como de transferir datos. Por otro lado, la subcapa MAC tiene la responsabilidad de controlar los enlaces, realizar la fragmentación de tramas, detectar y corregir errores, y gestionar el direccionamiento.

La capa de red tiene la responsabilidad de definir y gestionar el enrutamiento entre las redes interconectadas. Su función principal es facilitar la transmisión de datos desde el emisor al receptor, realizando la conmutación y el enrutamiento necesarios para que el mensaje llegue correctamente. Para llevar a cabo esta tarea, la capa de red debe tener conocimiento de la topología de la red en la que opera. El Protocolo de Internet (IP) es el protocolo encargado de esta función.



La capa de transporte es responsable de asegurar el transporte de los datos contenidos en los paquetes desde su origen hasta su destino, sin importar el tipo de red utilizada en niveles inferiores. En esta capa, la unidad de información, conocida como "Protocol Data Unit" (PDU), se llama "datagrama" cuando se utiliza el Protocolo de Datagramas de Usuario (UDP) para una transmisión sin conexión, o "segmento" cuando se utiliza el Protocolo de Control de Transmisión (TCP) para una transmisión orientada a la conexión (Gladys Patricia, Alexis Eduardo, Cristhian Salomón, & Eduardo Enrique, 2019).

Clase de sesión: De este nivel pasamos al nivel orientado a la aplicación. En la capa de sesión, se controla y mantiene el enlace entre las máquinas que intercambian información. Su objetivo principal es garantizar que, una vez que se establece una conexión, permanezca activa hasta que se complete la transferencia.

Clase de presentación: Esta capa es la encargada de representar la información transmitida. La función principal de esta capa es garantizar la legibilidad de los datos recibidos por el usuario, sin importar los protocolos distintos utilizados tanto en el transmisor como en el receptor. La capa de presentación es responsable de traducir una cadena de caracteres a un formato comprensible.

La capa de aplicación, ubicada en el último nivel del modelo OSI, permite a los usuarios interactuar y ejecutar comandos en sus propias aplicaciones. Un ejemplo de esto es la inclusión de un botón para enviar correos electrónicos o un programa diseñado para la transferencia de archivos a través de FTP. Además, esta capa facilita la comunicación entre las capas inferiores, lo que garantiza una transferencia de información eficiente y el correcto funcionamiento de las aplicaciones.



2.2.2.4. Transmisión de Datos en el Modelo OSI

Ahora veamos cómo funcionan las capas del modelo OSI en la transmisión de datos:

- La capa de aplicación del usuario recibe las notificaciones.
- El mensaje, ubicado en la capa de aplicación, se le agrega un encabezado ICI para formar la PDU de la capa de aplicación, la cual se convierte en una IDU y se transfiere a la capa siguiente.
- En este punto, el mensaje se encuentra en la capa de presentación, donde se le asigna un encabezado propio y se transfiere a la capa siguiente.
- A continuación, el mensaje se ubica en la capa de sesión y se repite el proceso descrito anteriormente. Finalmente, se envía a la capa física.
- En la capa física, el paquete es direccionado correctamente hacia el receptor.
- Una vez que el mensaje alcanza el destinatario, cada capa elimina el encabezado añadido por su capa correspondiente para transmitir el mensaje.
- El mensaje ahora llega a la capa de aplicación en el destino, donde se envía al usuario en un formato que puede comprender (González Inostroza, 2021).

2.2.3. Acceso Remoto y Conexiones WAN

2.2.3.1. Internet, Intranets y Extranet

Internet es un sistema a nivel mundial que interconecta diversas redes informáticas, posibilitando la comunicación y el intercambio de información, como archivos, correos electrónicos y grupos de noticias. Gracias a Internet, las redes informáticas pueden establecer conexiones entre sí y ampliar las posibilidades de actividades, facilitando una mayor colaboración y acceso a recursos para todos los



sistemas que participan en él (Franklin Jhimmy, Kirenia, María Magdalena, & José Efraín, 2021).

Intranet es una red interna utilizada por empresas que se fundamenta en la tecnología y los protocolos/servicios de Internet. Proporciona a los usuarios una manera eficiente y ágil de administrar la información. No es necesario tener conexión a Internet para configurar una intranet. Las intranets son una herramienta valiosa para las empresas que buscan cambiar su estructura de trabajo descentralizada y centralizada a una distribuida y flexible. Una de las principales ventajas de una intranet es la reducción de costos y tiempo en comparación con los métodos tradicionales de creación de documentos en papel. Una ventaja adicional es la utilización de navegadores web, que son programas que posibilitan la navegación y búsqueda de archivos en la World Wide Web. Estos navegadores suelen ser de acceso gratuito, como Netscape Navigator e Internet Explorer de Microsoft. Por otro lado, una extranet se refiere a una extensión de una red interna que permite el acceso a información específica por parte de personas u organizaciones externas, siempre sujeto a autenticación y control de acceso.

2.2.3.2. Acceso Remoto

El acceso remoto se refiere a la capacidad de conectarse a una red desde una ubicación externa. Esta funcionalidad ha adquirido una gran relevancia en el campo de las redes, especialmente para las empresas que requieren que sus empleados accedan a la red privada de la compañía durante viajes de negocios u otras ubicaciones remotas (Quishpe Iza, 2021).

Con el avance de las relaciones comerciales internacionales y el incremento de la movilidad laboral, el acceso remoto se ha vuelto cada vez más esencial. Esta demanda ha impulsado el surgimiento de las redes privadas virtuales (VPN, por sus siglas en inglés).



Los usuarios necesitan conexiones que les permitan acceder a sus negocios desde cualquier ubicación en el mundo.

Es necesaria una preparación cuidadosa al implementar un sistema de acceso remoto en una red. Para que el acceso remoto se implemente con éxito, es fundamental determinar qué usuarios lo necesitarán y qué tecnología emplearán. Si una empresa quiere implementar acceso remoto, es fundamental evaluar los usuarios que tiene y determinar si están en la oficina, son móviles o ambos. El siguiente paso es determinar los deseos únicos de estos usuarios y encontrar formas eficientes de satisfacerlos. Entre estos requisitos podrían estar

2.3. VIRTUAL PRIVATE NETWORK (VPN)

2.3.1. Definición de Una Red Privada Virtual (VPN)

Una VPN (red privada virtual) es una red de datos privada que conecta usuarios o segmentos de red a una red central de forma segura mediante una infraestructura de telecomunicaciones. Esta tecnología utiliza un protocolo de túnel para garantizar el secreto de la comunicación (Cueva Osorio & Falla Mejía, 2020).

Las Redes Privadas Virtuales (VPN) utilizan un protocolo llamado Protocolo de Tunelización para cifrar los datos transmitidos y crear una conexión segura similar a una conexión punto a punto privada. El concepto de "túnel" implica que los datos están encriptados desde el momento en que ingresan a la VPN hasta que salen de ella. Esto asegura que cualquier persona sin acceso al túnel no pueda entender los datos que pasan por el túnel. El paquete original no puede enrutarse a sí mismo a través del túnel porque tiene un espacio de direcciones diferente, por lo que se agrega un encabezado adicional. Este encabezado adicional proporciona información de enrutamiento en la red de reenvío.

Para lograr una conexión privada entre los dos extremos del túnel, los datos se cifran en la parte superior del túnel para garantizar la confidencialidad. Cuando el paquete llega al otro extremo del túnel, se descifra y se envía al usuario final.

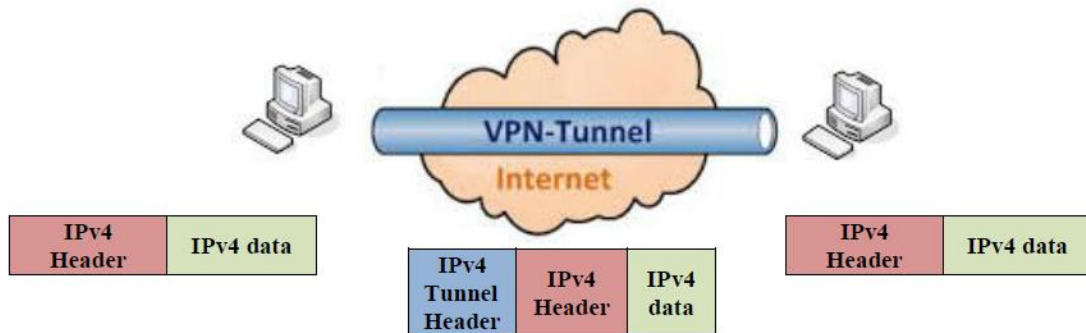


Figura 1: Funcionamiento tunneling.

Fuente: (Andrés Roig, 2017)

Los tres atributos de cada túnel son:

- **Codificar:** Se agrega información adicional a los datos originales para crear túneles y permitir la transmisión de información. Este procedimiento asegura la confidencialidad de los datos, ya que solamente el remitente y el receptor poseen las claves necesarias para cifrar y descifrar la información. De esta manera, cualquier persona que intercepte los datos no podrá acceder al contenido de la información transmitida.
- **Embalar:** Se añade una capa adicional de protección a los datos durante su transmisión, asegurando que solamente el emisor y el receptor posean la clave necesaria para encriptar y desencriptar la información. Esto garantiza la confidencialidad y evita que terceros puedan acceder al contenido de la información interceptada.
- **Exactitud:** Este proceso se divide en autenticación de usuario y validación de datos. Según la configuración, es posible que solo se requiera la autenticación del



usuario o la autenticación mutua. La autenticación de datos implica el uso de un hash encriptado con una contraseña conocida solo por el remitente y el receptor. Esto asegura la integridad de los datos y garantiza que no se modifique durante la transmisión (Andrés Roig, 2017).

2.3.2. Tipos de VPN

Hay varias formas de establecer una VPN en una empresa. Cada fabricante o proveedor de servicios tiene una solución VPN distinta, por lo que cada empresa debe considerar cuidadosamente cuál se adapta mejor a sus propios requisitos. Existen varios tipos de VPN, que incluyen:

Un firewall VPN, generalmente denominado VPN, es una tecnología que crea reglas para regular el acceso entre dos o más redes. Sirve como un filtro que vigila todas las comunicaciones entre las redes y decide si permite o deniega el acceso en función del contenido de esas comunicaciones (Castro Serantes, 2021).

Los cortafuegos se utilizan con frecuencia para proporcionar servicios VPN. Muchos de los productos de firewall de los líderes del mercado Cisco Systems, Nortel Networks y 3Com tienen funcionalidad VPN. Al tener un único punto de control de seguridad, esto tiene la ventaja de simplificar la arquitectura de la red.

Sin embargo, es importante tener en cuenta que tener una VPN en el firewall puede complicar el dispositivo, por lo que se debe tener cuidado al configurar una VPN para evitar que intrusos no autorizados accedan a la red.

Otra opción es utilizar un enrutador o dispositivo conocido como concentrador VPN, que también es ofrecido por empresas como Cisco y otros proveedores. Estas herramientas están diseñadas para implementar VPN tanto en entornos locales como remotos. Estas tecnologías ofrecen las soluciones de VPN más relevantes, así como



métodos de autenticación y encriptación para asegurar la protección de los datos mientras se encuentran en tránsito (Rivera Morla, 2022)

OSVPN: Los servicios VPN ya están incluidos en sistemas operativos como Microsoft Windows, Novell Netware y varias variantes de Linux como Red Hat y Debian. Dado que un único sistema operativo puede proporcionar una variedad de servicios, como un servidor web, nombres de dominio, acceso remoto y VPN, esta opción tiene la ventaja de ser económicamente eficaz. Esta opción también mejora los procedimientos de autenticación y seguridad del sistema operativo. Es importante recordar que este método puede tener fallos de seguridad relacionados con el sistema operativo. La mayoría de la gente usa estas VPN para acceso remoto.

HERRAMIENTA VPN: Este tipo de VPN menos popular requiere la instalación de una segunda aplicación que mejore la capacidad de VPN del sistema operativo. Esta VPN no está integrada en el sistema operativo, a diferencia de otra que sí lo está. Esta forma de VPN tiene la ventaja de ofrecer un mayor nivel de seguridad en comparación con las VPN integradas en los sistemas operativos. Estas VPN, sin embargo, son más lentas que las VPN de hardware y no pueden acomodar a una gran cantidad de usuarios. También pueden tener fallos de seguridad en los sistemas que los ejecutan cuando se utilizan a través de Internet.

PROVEEDOR DE SERVICIO VPN: Un proveedor de servicios ofrece este tipo de VPN, en la que un cliente se conecta a la red del proveedor mediante un enrutador u otro equipo multipropósito. Se utiliza una línea de transmisión, como X.25, Frame Relay, un conmutador ATM o un enrutador IP, para vincular el dispositivo de uso general al equipo del proveedor de servicios. Un "circuito virtual" es el enlace que el proveedor de servicios establece para el cliente (Andrés Roig, 2017).

2.3.3. Arquitecturas Vpn

Existen básicamente cuatro arquitecturas de redes de tipo VPN:

2.3.4. De Sitio a Sitio

Cuando los dispositivos en ambos extremos de la conexión están configurados para usarla, se puede formar una conexión VPN de sitio a sitio. Las partes internas no son conscientes de la presencia de esta VPN, que siempre está cifrada. Frame Relay, ATM, VPN y otros tipos de conexiones son algunos ejemplos de VPN de sitio a sitio.

Las computadoras comúnmente envían y reciben tráfico TCP/IP a través de una puerta de enlace VPN cuando usan una conexión VPN de sitio a sitio. Un enrutador, un firewall, un concentrador Cisco VPN o un dispositivo de seguridad adaptable son algunos ejemplos de esta puerta de enlace. Para transportar el tráfico a través de un túnel VPN a una ubicación de destino VPN especificada diferente, la puerta de enlace tiene la capacidad de recopilar y cifrar datos que llegan desde un sitio determinado. Se eliminan los encabezados, se eliminan los datos pertinentes y el paquete se enruta a las computadoras en el sitio adecuado una vez que el tráfico llega a la puerta de enlace VPN de destino (Naik, Shang, Shen, & Jenkins, 2019).

Las VPN de sitios web se pueden clasificar en dos categorías según los objetivos comerciales que abordan: VPN para intranets y VPN para periféricos. Una VPN de intranet se utiliza para la comunicación dentro de la empresa, como se muestra en la Figura 1.4. Conecta la sede central y sus sucursales, y está sujeta a reglas similares a cualquier otra red. Un enrutador establece una red VPN que conecta las dos partes de la red privada. Un servidor VPN proporciona una conexión directa a la red a la que está conectado.

Por otro lado, una VPN externa conecta a un cliente, proveedor, amigo o comunidad de interés a la red interna de la empresa, como se muestra en la Figura 2.4. La VPN de red externa puede ser utilizada mediante acuerdos entre diferentes miembros de organizaciones. Para las empresas, se aplican las mismas reglas que para las redes privadas. Sin embargo, existen más amenazas de seguridad en la red externa que en la red interna, por lo que las VPN fuera de la red deben estar bien diseñadas, con políticas de seguridad, acuerdos de acceso y privacidad establecidos entre los participantes fuera de línea (Castro Serantes, 2021).

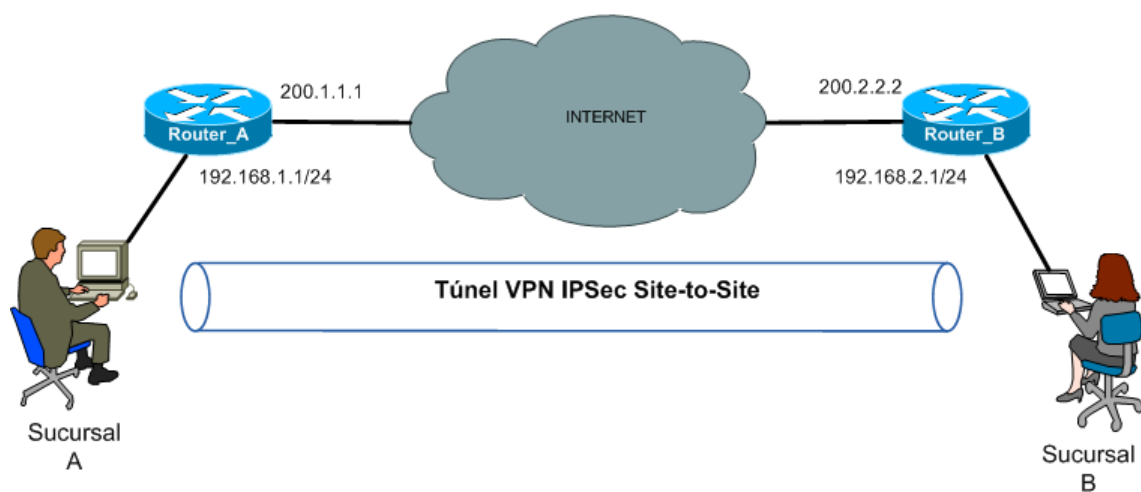


Figura 2: VPN sitio a sitio.

Fuente: (Bonastre Pina, 2019)

2.3.4.1. De Acceso Remoto

Una VPN de acceso remoto se configura de manera que la información no se encuentre cifrada, pero permite cambios dinámicos en los datos y se puede activar y desactivar según sea necesario. Tomemos en cuenta el escenario de un empleado remoto que necesita acceder a los datos de la empresa a través de Internet utilizando una VPN. En este caso, los usuarios remotos no tienen que configurar manualmente una conexión VPN cada vez que necesitan utilizarla. La responsabilidad de establecer la conexión VPN recae en la computadora del usuario remoto. La información necesaria para establecer



dicha conexión, como la dirección IP del usuario remoto, varía dinámicamente dependiendo de la ubicación del mismo (Rojas Celis, Hoyos Rodríguez, & Castro Reyes, 2020).

- La información corporativa está accesible en línea. Un usuario remoto no requiere configurar una conexión VPN cada vez que accede, ya que es su computadora la encargada de establecerla. La información necesaria para establecer la conexión VPN, como la dirección IP del usuario remoto, varía dinámicamente según su ubicación.
- Dependiendo de la computadora utilizada para configurar la conexión, la "VPN de acceso telefónico" se puede dividir en VPN de "acceso telefónico" y VPN directa.
- VPN modificada: En este tipo de VPN, el usuario llama a un proveedor de servicios de Internet (ISP) mediante un módem. Aunque esta conexión puede retrasarse, sigue siendo normal. Es utilizado principalmente por usuarios móviles que no siempre tienen acceso a Internet de alta velocidad en todas las áreas de sus vidas.
- VPN directa: Este tipo de VPN utiliza tecnología de conexión a Internet de alta velocidad, como DSL y módem por cable, que ofrecen muchos proveedores de servicios de Internet. Estas VPN son muy utilizadas por los teletrabajadores ya que ahora es posible conectarse a Internet desde casa gracias a esta tecnología (Castro Serantes, 2021).

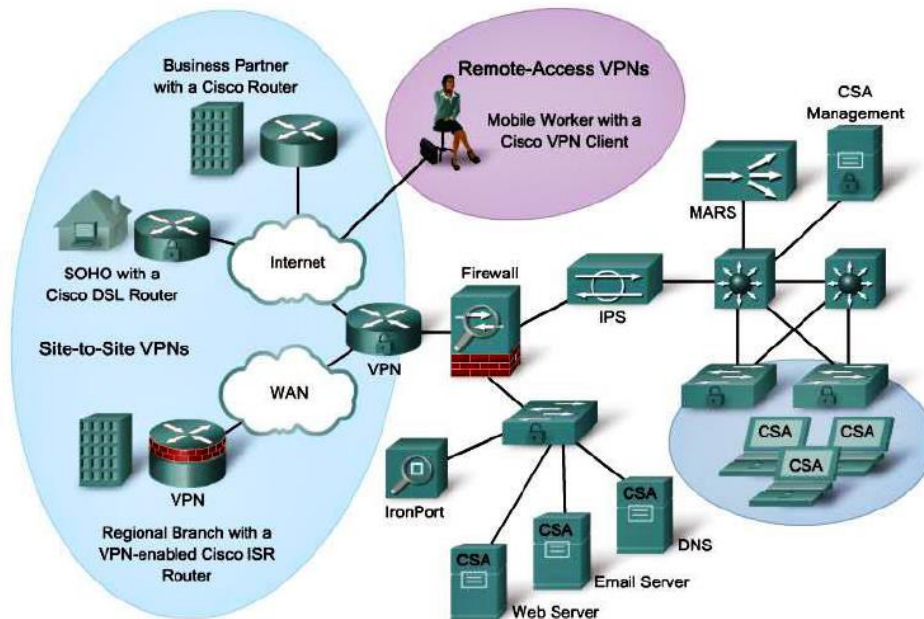


Figura 3: VPN de acceso remoto.

Fuente: (Bonastre Pina, 2019)

Cada servidor en un entorno VPN remoto normalmente viene con el software cliente VPN de Cisco. Antes de que el tráfico se entregue a través de Internet a la puerta de enlace VPN en el borde de la red cuando el servidor intenta enviarlo a través de la VPN, el software cliente VPN de Cisco lo recopila y lo protege. Cuando la puerta de enlace VPN acepta este tráfico, se establece una VPN de sitio a sitio.

2.3.4.2. Tunneling

La tunelización consiste en incrustar un protocolo de red dentro de otro, creando un túnel a través de una red informática. Este túnel permite transferir datos de un extremo a otro sin revelar la información almacenada entre ellos. Los paquetes de datos se enrutan a través de un nodo intermedio que no ve el contenido de los paquetes. Los terminales y protocolos de comunicación utilizados determinan el canal (Galarza Mena & Jaya Condorcana, 2020).



Las técnicas de tunelización se utilizan para diferentes propósitos, dependiendo del problema a resolver. Uno de los ejemplos más populares es el reenvío de tráfico en el contexto de IP móvil. En estos casos, si el nodo móvil está fuera de su red, necesita un agente técnico para realizar ciertas tareas en su nombre, incluida la recopilación y retransmisión del tráfico entrante. La tunelización se utiliza para esto porque debe preservar la estructura y el contenido originales de los paquetes (por ejemplo, direcciones IP de origen y destino, puertos, etc.). Todo esto se hace de forma remota (Rubio, 2021).

2.3.4.3. VPN Over LAN

Esta opción de VPN, aunque no es muy popular, es muy efectiva para uso empresarial. En lugar de utilizar Internet, se utiliza la red de área local (LAN) de una empresa como medio de comunicación. Su principal función es aislar sitios y servicios de la red interna, lo que la convierte en una opción útil para mejorar la seguridad de las redes inalámbricas.

Un ejemplo clásico de su uso es cuando tienes un servidor con información sensible, como un pago, detrás de un dispositivo VPN. Esta herramienta proporciona capacidades adicionales de encriptación y autenticación, lo que garantiza que solo el personal de recursos humanos autorizado tenga acceso a la información.

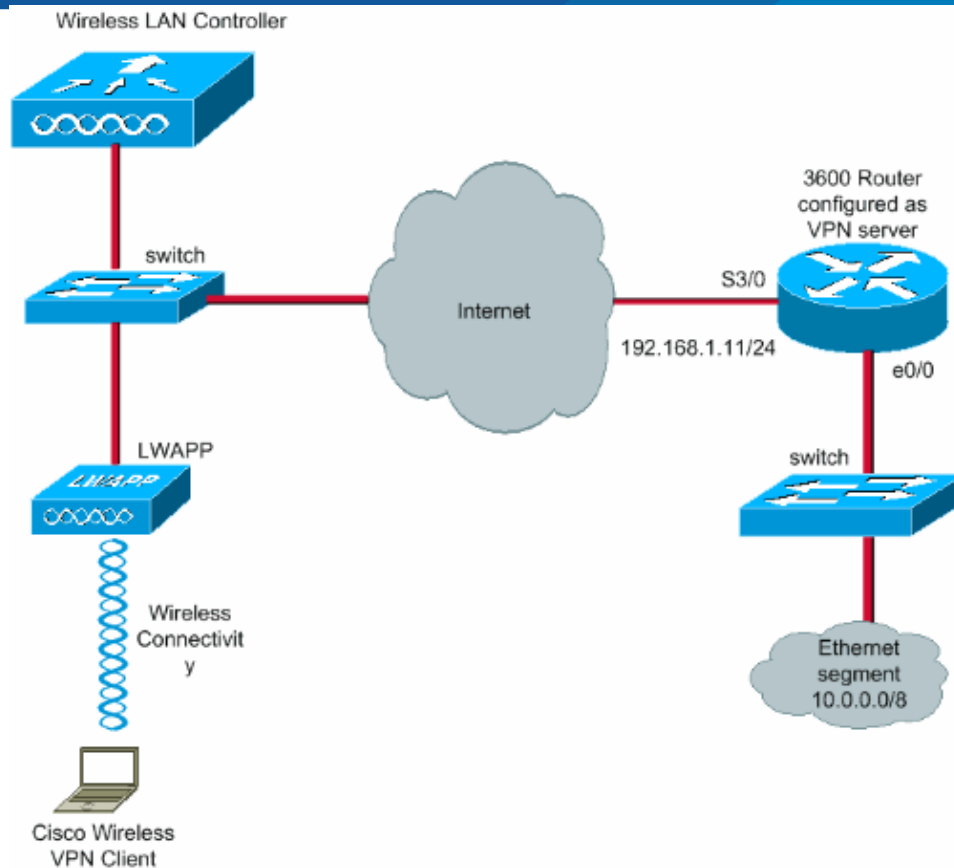


Figura 4: VPN over LAN.

Fuente: (Berrio Rufino, 2021)

Un ejemplo adicional es conectarse a una red Wi-Fi utilizando un túnel privado IPsec o SSL. Estas medidas no solo emplean métodos de autenticación convencionales, como direcciones WEP, WPA y MAC, sino que también agregan capas de seguridad a los túneles VPN establecidos en la LAN interna o externa. Esto incrementa la seguridad y asegura una conexión Wi-Fi segura (Biga, Dufour, Serra, & Peliza, 2020).

2.3.5. Seguridad En Una VPN

Mantener la autenticidad, la integridad y la privacidad durante todo el proceso de comunicación es crucial para la seguridad al utilizar una VPN. La integridad se relaciona con garantizar que los datos no se modifiquen durante el envío, mientras que la privacidad se refiere a proteger la información de usuarios no autorizados. Para identificar la fuente



de los datos y garantizar que se originan en el lugar designado, la autenticación es esencial. Al utilizar una VPN, estos factores son cruciales para garantizar la seguridad.

2.4. VPN DE ACCESO REMOTO

Una VPN es un servicio que proporciona acceso remoto a la red interna y los recursos comerciales de una organización. Estas aplicaciones incluyen correo electrónico, servidores de archivos y aplicaciones de software como CRM, ERP u otras aplicaciones departamentales. Al brindar acceso seguro a Internet, una VPN permite la movilidad de los trabajadores y la conexión de ubicaciones dispersas. A través de un canal encriptado, VPN crea una conexión segura a Internet, lo que nos permite acceder a los servicios y documentos de nuestra empresa desde cualquier lugar (Andrés Roig, 2017).

2.5. SEGURIDAD IP (IPSec)

2.5.1. Definición de IPSec

IPSec es un protocolo de capa 3 desarrollado por el IETF (Grupo de trabajo de ingeniería de Internet) que le permite enviar datos cifrados. Está diseñado para mejorar la seguridad del protocolo IP para confidencialidad, control de acceso, integridad, privacidad y autenticación de datos y fuentes de datos. Las especificaciones de IPSec se definen en los RFC 2401 a 2412 y se actualizan en los RFC 4301 a 4309 (Ardila Castillo, 2019).

IPSec permite la comunicación segura a través de LAN privadas o públicas, WAN e incluso Internet. Ejemplos de su uso son:

Establecer una comunicación interna entre los distintos departamentos de una empresa a través de Internet puede lograrse mediante la creación de una red privada. Esta opción, utilizando Internet o una WAN pública, disminuye la dependencia de una red



privada adicional y conlleva beneficios tanto en términos de reducción de costos como de una mayor eficiencia administrativa.

Acceso remoto seguro a través de Internet: Los usuarios finales cuyos sistemas tienen protocolos de seguridad IP pueden llamar a sus proveedores de servicios de Internet (ISP) y acceder a Internet de forma segura. Esto reduce el costo del transporte y el costo de los empleados que necesitan acceder a Internet cuando no están en la oficina (Paramo Melo, 2020).

Con IPSec, puede establecer una conexión de red interna y externa segura con socios y empleados, proporcionando autenticación, seguridad e intercambio seguro de claves. Asimismo, IPSec ayuda a mejorar la seguridad en el comercio electrónico, incluso el comercio electrónico y las aplicaciones en línea que ya cuentan con protocolos de seguridad internos, porque la implementación de IPSec proporciona un nivel adicional de seguridad.

2.5.1.1. Protocolos de IPSec

A diferencia de la mayoría de los sistemas de seguridad, IPSec opera a nivel de red en lugar de hacerlo a nivel de aplicación. Esto le permite bloquear todos los paquetes IP. Este proceso se lleva a cabo de dos formas distintas y especiales.

2.5.1.2. Encabezado de Autenticación (AH)

El sujeto de autenticación es responsable de garantizar la integridad y autenticidad de los datos que se transmiten. Para ello, cada paquete utiliza el esquema de firma digital HMAC. Esta función garantiza que la red y sus datos estén protegidos contra interferencias de terceros. El contenido del paquete de datos que contiene el encabezado de autenticación no se puede alterar sin detección. Este encabezado se encuentra entre el encabezado IP y la carga útil del paquete y se puede enviar a través de TCP o UDP.

Tabla 1: Estructura de un encabezado AH.

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Next header	Payload length	RESERVED	
Security parameters index (SPI)			
Sequence number			
Hash Message Authentication Code (variable)			

Fuente: (Vinicio, 2021)

Dentro del protocolo AH, el remitente accede a la función hash del mensaje que pretende enviar y la copia en el campo de datos de autenticación en el encabezado AH. Luego, el mensaje se envía a través de Internet. Cuando el mensaje llega al destinatario, este procede a ingresar la misma función hash y la compara con la recibida previamente, bajo la premisa de que todos los involucrados comparten una clave secreta común. Si las señales digitales HMAC son idénticas, se puede concluir que el datagrama no ha sido modificado. La detección de cualquier otro evento sugiere que la información ha sido alterada durante la transmisión.

2.5.1.3. Carga de Seguridad Encapsulada (ESP)

Una capa de seguridad incrustada se encarga de bloquear la información dentro del paquete, evitando que pueda ser leída. Mientras que el encabezado AH protege contra la manipulación del paquete, ESP cifra la carga útil del paquete completo mediante el bloqueo de transporte y sello. Para lograr estas características de seguridad, el intercambio de claves públicas se realiza mediante un algoritmo de cifrado asimétrico (Montaleza Paucar & Jativa Reyes, 2022).

El ESP es responsable de codificar y convertir los datos en un nuevo datagrama IP. Aunque tiene algunas similitudes con el tema AH, la estructura de ESP es más

compleja debido a las diferentes funciones que ofrece. En Internet, los datos se transfieren a través de gráficos de datos TCP, UDP o IP. Si se usa ESP en modo túnel, todos los paquetes IP internos estarán protegidos.

Tabla 2: Estructura de un paquete ESP.

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Security parameters index (SPI)			
Sequence number			
Payload data (variable)			
Padding (0-255 bytes)			
		Pad Length	Next Header
Authentication Data (variable)			

Fuente: (Liyakkathali y otros, 2022)

Para mejorar la seguridad, puede cifrar el gráfico de datos y cifrar completamente el campo de datos. Los algoritmos de clave simétrica como AES en versiones de 128 y 256 bits se utilizan junto con métodos de encriptación como AES:

Radio Canadá, AES:

BFC y AES:

OF B. El cifrado se realiza en bloques y se pueden agregar múltiples bloques a un mensaje, creando un espacio de búfer. La remitente cifra el mensaje original con una clave y lo coloca en un nuevo gráfico de datos de IP protegido por el encabezado ESP. Si se acepta el mensaje, se cerrará y se guardará.

2.5.1.4. Intercambio de Claves en Internet (IKE)

El protocolo IKE se usa para generar y administrar las claves necesarias para establecer una conexión segura usando los protocolos IPsec AH y ESP. Todos los

participantes de IPSec deben usar el mismo método de encriptación y autenticación para mantener la conexión. Esto se puede hacer manualmente en ambos lados o mediante negociaciones independientes utilizando el protocolo IKE.

Es importante señalar que IKE no se limita a IPSec, sino que también se utiliza en algoritmos de enrutamiento como OSPF o RIP para establecer conexiones. IKE es un protocolo híbrido que combina otros protocolos ISAKMP, un protocolo que define la comunicación y la sintaxis en los mensajes IKE, y Oakley, que define el concepto de intercambio seguro de claves entre dos partes anónimas (Lema Balladares, 2021).

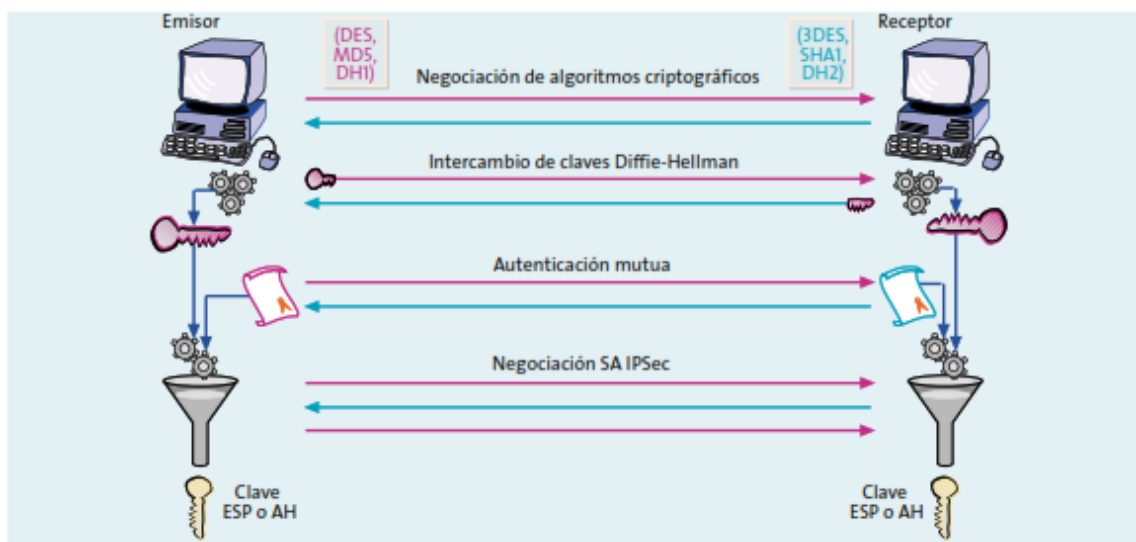


Figura 5: Funcionamiento del protocolo IKE.

Fuente: (Vinicio, 2021)

Para establecer una conexión privada y confiable con IKE, se realiza un protocolo de enlace bidireccional:

- El propósito principal de IKE es establecer una ruta segura y confiable entre dos nodos. Esto se logra utilizando HMAC y un algoritmo de cifrado simétrico derivado de clave. Sin embargo, esto por sí solo no garantiza la identificación de los nodos. Por lo tanto, se realiza un paso de verificación adicional.
- Existen diferentes tipos de autenticación en IKE, pero la más común es la información secreta compartida y el uso de certificados digitales. Conocer un



secreto compartido implica que ambos nodos conozcan una secuencia secreta única y usen funciones hash para demostrar que tienen la clave sin revelarla. Sin embargo, la gestión de varios secretos puede resultar complicada en escenarios de varios nodos, por lo que se recomienda la autenticación con certificado digital X509v3. Esto le permite distribuir de forma segura la clave pública de cada nodo y probar su identidad siendo propietario de la clave privada.

- En la segunda fase de IKE, se negocian parámetros de seguridad específicos relacionados con un protocolo en particular, como AH o ESP. El nodo de envío proporciona todas las opciones de seguridad configuradas en su política, mientras que el nodo de recepción acepta la primera opción que coincida con su configuración de seguridad definida. Ambos nodos conocen el tráfico que intercambiará esta conexión.

2.5.1.5. Asociaciones de Seguridad (SA)

Cuando un paquete AH o ESP llega a una interfaz, la interfaz no sabe qué parámetros de configuración usar. Un servidor puede tener varias conversaciones al mismo tiempo, cada una con su propio conjunto de claves y algoritmos. Por lo tanto, el gerente debe asumir la responsabilidad de este proceso.

Los grupos de seguridad definen las funciones de seguridad utilizadas para la comunicación entre servidores. Una asociación de seguridad (SA) protege los datos en una dirección determinada, lo que significa que se necesita una SA independiente para proteger el tráfico en cada dirección. Estas SA se almacenan en una base de datos denominada Base de datos de asociaciones de seguridad (SADB). La interfaz del sistema utiliza sockets para permitir que aplicaciones específicas accedan a esta base de datos (Vinicio, 2021).



2.5.1.6. Administración de Claves En IPSec

IPSec sería inútil sin las capacidades de autenticación y cifrado. Las organizaciones de seguridad requieren documentos de autenticación y cifrado, y la gestión de estos documentos se denomina gestión de claves. IKE maneja estos problemas automáticamente y usted puede manejar las claves manualmente.

La forma más fácil de establecer una política de privacidad es hacerlo manualmente. El equipo desarrolla estrategias y las distribuye a otros miembros. Todos los involucrados en las comunicaciones seguras utilizan estas pautas como Unidades de política de seguridad (SPD). Sin embargo, la sencillez de este tipo de uso también puede resultar peligrosa. Si las políticas de privacidad se transmiten a través de ubicaciones intermedias, pueden estar expuestas a personas no autorizadas durante el tránsito. En particiones grandes con muchos dispositivos que usan una clave pre compartida, esta condición puede comprometer la seguridad de la nueva clave y hacer que la transferencia falle (Aparicio-Izurieta, 2022).

2.5.1.7. Funcionamiento de IPSec

IPSec es una tecnología VPN que permite transferir datos confidenciales a través de redes públicas. Ofrece muchas funciones de seguridad diferentes, como protección de integridad, integridad y protección de juegos.

A diferencia de la mayoría de los protocolos de seguridad que operan en la capa de aplicación, IPSec opera en la capa de red. Esto significa que puede definir un paquete IP de dos maneras: A Encabezado de autenticación (AH) y protección de carga útil de encapsulación (ESP).



Una de las ventajas de IPSec es su adaptabilidad a diferentes algoritmos criptográficos, incluidos los que puedan aparecer en el futuro. Además, admite varios algoritmos criptográficos que se utilizan en la actualidad.

Para garantizar la transmisión segura de información en Internet utilizando el protocolo IPSec, debe instalar un software en cada dispositivo que utilice o conectar el protocolo al enrutador conectado a la red. Esto garantiza la seguridad de todos los datos enviados y recibidos (Aparicio-Izurieta, 2022).



CAPITULO III

MATERIALES Y METODOS

3.1. MATERIALES

3.1.1. Hardware

- Computadora para trabajos de programación.
- Tipo de procesamiento: Intel Core i5-2430 3.40GHz
- Capacidad de memoria RAM: 4.00GB.
- Adaptador red (Internet).
- OS: Windows 11 con 64 bits.
- Servidor: DELL Power Edge R620 (Puma Quispe & Cutipa Nina, 2015)

3.1.2. Software

- OS Windows 10 64 bits.
- GNS3

3.2. TIPO Y DISEÑO DE LA INVESTIGACIÓN

3.2.1. Tipo de Investigación

La investigación en el presente proyecto es de tipo aplicativo, puesto que consiste en la puesta en práctica acerca de las redes que las instituciones deberían utilizar para salvaguardar información sensible con la finalidad de mejorar y resolver específicamente problemas referidos a la seguridad en transmisión de datos en la actualidad (Carrasco Díaz, 2019).



3.2.2. Diseño de la Investigación

La investigación en cuestión pertenece al enfoque experimental, ya que se basa en los principios lógicos y científicos que posteriormente se implementarán en un caso real utilizando un modelo prototipo. Este tipo de investigación implica la manipulación intencionada de una acción para observar sus efectos y analizar los resultados.

El desarrollo del experimento puede llevarse a cabo tanto en un laboratorio como en un entorno real, aunque el número de personas y equipos involucrados suele ser relativamente pequeño. Los experimentos son especialmente útiles para investigaciones explicativas y suelen estar limitados a situaciones en las que es posible manipular las variables en las que se encuentran las personas (Hernández Sampieri & Mendoza, 2020).

3.2.3. Nivel de la Investigación

Dado que aborda un tema de estudio con pocos o ningún trasfondo, la investigación que se ofrece es exploratoria. De la misma manera, es correlacional porque su objetivo es medir qué tan estrechamente están relacionadas las variables en las hipótesis planteadas. Por otro lado, es descriptivo ya que las variables no se modifican; en cambio, sólo se anotan y se presentan exactamente como lo hacen en la realidad. La metodología puede en algún momento tomar más referencia en ciertos elementos cualitativos y cuantitativos.

3.3. POBLACIÓN Y MUESTRA DE LA INVESTIGACIÓN

3.3.1. Población

Dado que este estudio se realizó en la Universidad Nacional del Altiplano, es importante observar las oficinas que frecuentemente acceden a la red universitaria y el tipo de información que intercambian.



De acuerdo con el artículo 195 de los artículos “c”, “d” y “k” del Ordenamiento de Organización y Funciones 2016 (Universidad Nacional del Altiplano, 2016) de esta cámara de educación superior:

“Son funciones del Departamento de Tecnologías de la Información y las Telecomunicaciones las siguientes:

- Analizar, recomendar, diseñar y desarrollar sistemas de información basados en las necesidades organizacionales.
- Diseñar e implementar un sistema de información automatizado y administrativo en los departamentos académicos y administrativos de la Universidad.
- Garantizar la seguridad de la información del sitio automatizado”.

Además, en el mismo reglamento anteriormente mencionado, en el artículo 299, señala que:

“La comunicación educativa se encarga de planificar, organizar, ejecutar, gestionar y evaluar la información sobre las actividades educativas, los métodos de enseñanza, el registro y los archivos educativos”.

De todo lo dicho, se puede concluir que al tomar en cuenta las necesidades específicas que este estudio pretende atender, y al tomar en cuenta las organizaciones que están a la vanguardia en la atención de estas necesidades, se puede observar que nuestra gente:

- Departamento de Tecnologías de la Información y las Comunicaciones.
- 19 coordinadores académicos de cada departamento.



3.3.2. Muestra

Dado que el propósito de este estudio es proteger la seguridad de los datos informáticos, el modelo debe contar con las herramientas y equipos involucrados en el estudio, como lo serán VPN.

Sabiendo que el equipo necesario son enrutadores, conmutadores y computadoras, se decidió que se creará un modelo en el laboratorio de Cisco para la capacidad de probar VPN.

Por tanto, se concluye que, al no ser el primero ni necesario, nuestro estudio no tiene un modelo definido.

3.4. UBICACIÓN Y DESCRIPCIÓN

3.4.1. Ubicación

- Universidad Nacional del Altiplano.
- Escuela Profesional de Ingeniería Electrónica;
- Laboratorio de Cisco.
- Dirección: Av. Floral N° 1153, Puno.
- Latitud: :15.824957
- Longitud: :70.015483

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. DESCRIPCIÓN DE LA INVESTIGACIÓN

4.1.1. Procedimiento de Diseño Del Prototipo

4.1.1.1. Topología

El escenario muestra dos redes LAN mostradas en color celeste y amarillo, estas dos redes acceden a Internet a través de un proveedor de servicios de Internet (ISP) simulado por R2. El objetivo es permitir el acceso remoto de la computadora ubicada en la red del recuadro celeste (un cliente externo que solicita servicios) hacia la red del recuadro amarillo (sistema de registro y archivo académico), para esto R3 será el servidor VPN y la computadora en el recuadro celeste el cliente.

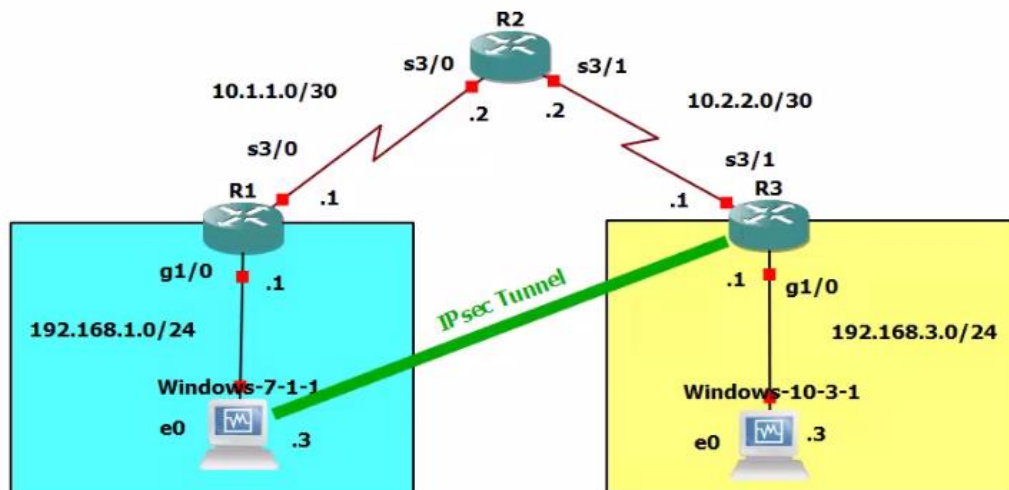


Figura 6: Topología de red del escenario.

Elaboración Propia.

La seguridad está determinada por un túnel IPsec, el túnel permitirá que el cliente pueda ingresar a la red LAN del servidor.

Tabla 3: Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de Subred	Puerta de Enlace
R1	G1/0	192.168.1.1	255.255.255.0	N/A
	S3/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S3/0	10.1.1.2	255.255.255.252	N/A
	S3/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G1/0	192.168.3.1	255.255.255.0	N/A
	S3/1	10.2.2.1	255.255.255.252	N/A
Winds:7	NIC	192.168.1.3	255.255.255.0	192.168.1.1
Winds:10	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Elaboración Propia.

La tabla de direccionamiento muestra las configuraciones que deben realizarse en los dispositivos, para esto se usa la línea de comandos para configurar el direccionamiento en R1, note que se crea una ruta estática por defecto usando la IP del siguiente salto para llegar hacia otras redes.

4.1.1.2. Configuración de Dispositivos

La configuración de los dispositivos se realiza de la siguiente forma.

```
R1#conf term
Enter configuration commands, one per line. End with
CNTL/Z.
R1config)#int g1/0
R1config:if)#ip address 192.168.1.1 255.255.255.0
R1config:if)#no shutdown
R1config:if)#int g1/0
*May 26 15:00:31.831: %LINK:3:UPDOWN: Interface
GigabitEthernet1/0, changed state to up
*May 26 15:00:32.831: %LINEPROTO:5:UPDOWN: Line protocol on
Interface GigabitEthernet1/0, changed state to up
R1config:if)#int s3/0
R1config:if)#ip address 10.1.1.1 255.255.255.252
R1config:if)#no shutdown
R1config:if)#
*May 26 15:00:51.239: %LINK:3:UPDOWN: Interface Serial3/0,
```

Figura 7: Configuración de direccionamiento en R1.

Elaboración Propia.

De la misma forma se usa la línea de comandos para configurar el direccionamiento en R2, note se crean dos rutas estáticas usando la IP del siguiente salto para llegar hacia las redes LAN ubicadas en ambos extremos, LAN de R1 y LAN de R3.

```
R2#conf term
Enter configuration commands, one per line.  End with
CNTL/Z.
R2(config)#int s3&0

% Invalid input detected at '^' marker.

R2(config)#int s3/0
R2(config:if)#ip address 10.1.1.2 255.255.255.252
R2(config:if)#no shutdown
R2(config:if)#
*May 26 15:07:04.443: %LINK:3:UPDOWN: Interface Serial3/0,
changed state to up
*May 26 15:07:05.443: %LINEPROTO:5:UPDOWN: Line protocol on
Interface Serial3/0, changed state to up
R2(config:if)#int s3/1
R2(config:if)#ip address 10.2.2.2 255.255 .255.252
R2(config:if)#clock rate 8064000
R2(config:if)#no shutdown
R2(config:if)#
*May 26 15:07:29.107: %LINK:3:UPDOWN: Interface Serial3/1,
changed state to up
*May 26 15:07:30.107: %LINEPROTO:5:UPDOWN: Line protocol on
Interface Serial3/1, changed state to up
R2(config:if)#
*May 26 15:07:54.015: %LINEPROTO:5:UPDOWN: Line protocol on
Interface Serial3/1, changed state to down
R2(config:if)#exit
R2(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.1
R2(config)#ip route 192.168.3.0 255.255.255.0 10.2.2.1
```

Figura 8: Configuración de direccionamiento en R2.

Elaboración Propia.

También se usa la línea de comandos para configurar el direccionamiento en R3, note que también se crea una ruta estática por defecto usando la IP del siguiente salto para llegar hacia otras redes.

```
R3#conf term

Enter configuration commands, one per line.  End with
CNTL/Z.

R3(config)#int s3/1

R3(config:if)#ip address 10.2.2.1 255.255.255.252

R3(config:if)#no shutdown

R3(config:if)#

*May 26 15:10:20.083: %LINK:3:UPDOWN: Interface
Serial3/1, changed state to up

R3(config:if)#

*May 26 15:10:21.087: %LINEPROTO:5:UPDOWN: Line protocol
on Interface Serial3/1, changed state to up

R3(config:if)#int g1/0
```

Figura 9: Configuración de direccionamiento en R3.

Elaboración Propia.

Se procede a configurar el direccionamiento en la computadora ubicada en el recuadro celeste, el cliente. No es necesario configurar el DNS porque la funcionalidad del túnel no necesita ese servicio.

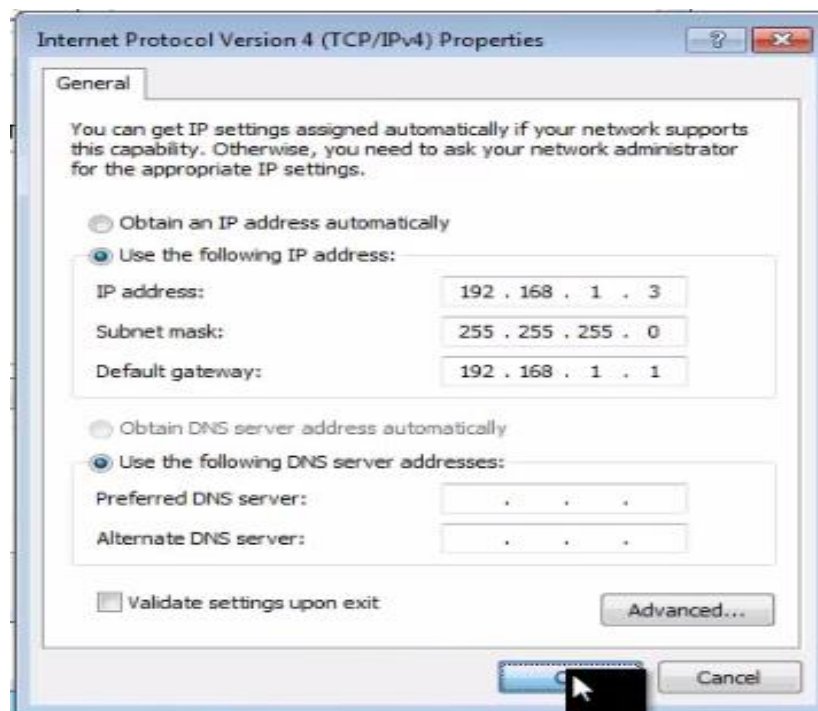
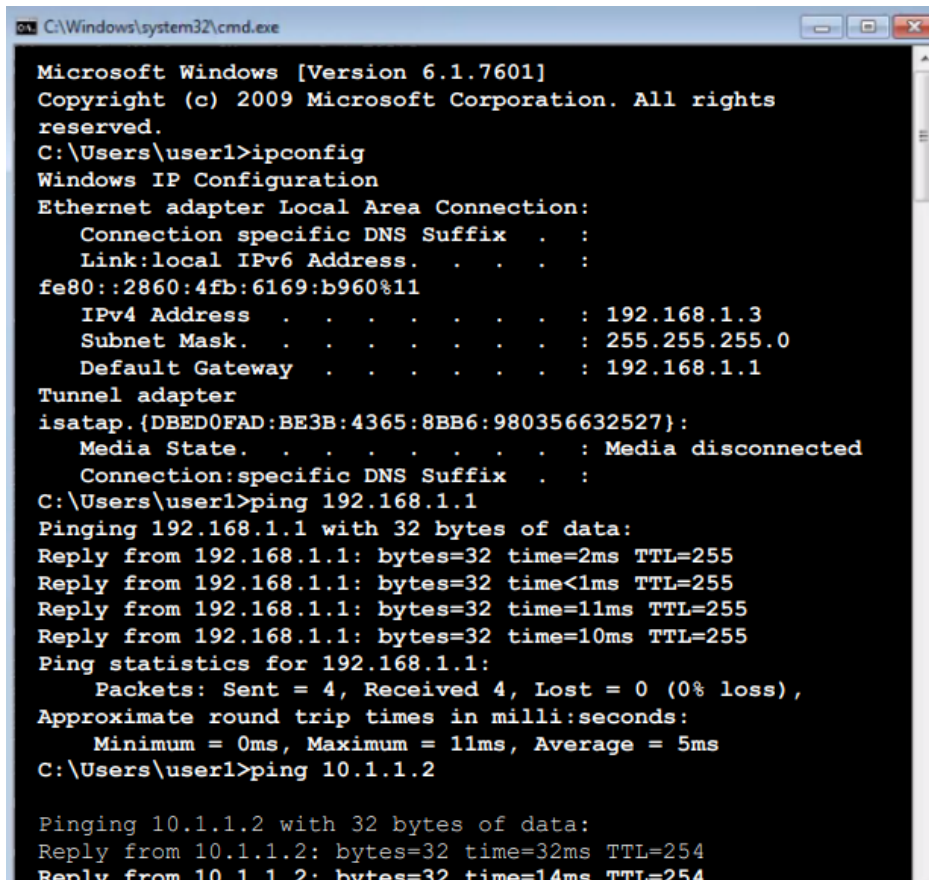


Figura 10: Configuración de direccionamiento en el cliente.

Elaboración Propia.

A continuación, se realiza la verificación de las configuraciones y se hace una prueba de conectividad desde la computadora cliente hacia R1 y R2.

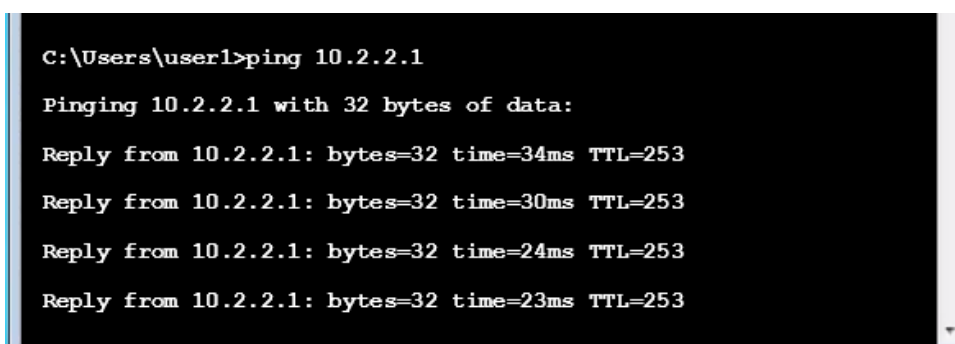


```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\user1>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
    Connection specific DNS Suffix . . . :
    Link-local IPv6 Address . . . . . : fe80::2860:4fb:6169:b960%11
    IPv4 Address . . . . . : 192.168.1.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
Tunnel adapter
isatap.{DBED0FAD:BE3B:4365:8BB6:980356632527}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . :
C:\Users\user1>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=11ms TTL=255
Reply from 192.168.1.1: bytes=32 time=10ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received 4, Lost = 0 (0% loss),
    Approximate round trip times in milli:seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 5ms
C:\Users\user1>ping 10.1.1.2
Pinging 10.1.1.2 with 32 bytes of data:
Reply from 10.1.1.2: bytes=32 time=32ms TTL=254
Reply from 10.1.1.2: bytes=32 time=14ms TTL=254
```

Figura 11: Verificación de configuración en el cliente.

Elaboración Propia.

También se realiza la verificación desde el cliente hacia R3.



```
C:\Users\user1>ping 10.2.2.1
Pinging 10.2.2.1 with 32 bytes of data:
Reply from 10.2.2.1: bytes=32 time=34ms TTL=253
Reply from 10.2.2.1: bytes=32 time=30ms TTL=253
Reply from 10.2.2.1: bytes=32 time=24ms TTL=253
Reply from 10.2.2.1: bytes=32 time=23ms TTL=253
```

Figura 12: Verificación de configuración desde cliente a R3.

Elaboración Propia.

Se procede a configurar el direccionamiento en la computadora ubicada en la LAN de R3, esto ubicado en el sistema de registro y archivo académico.

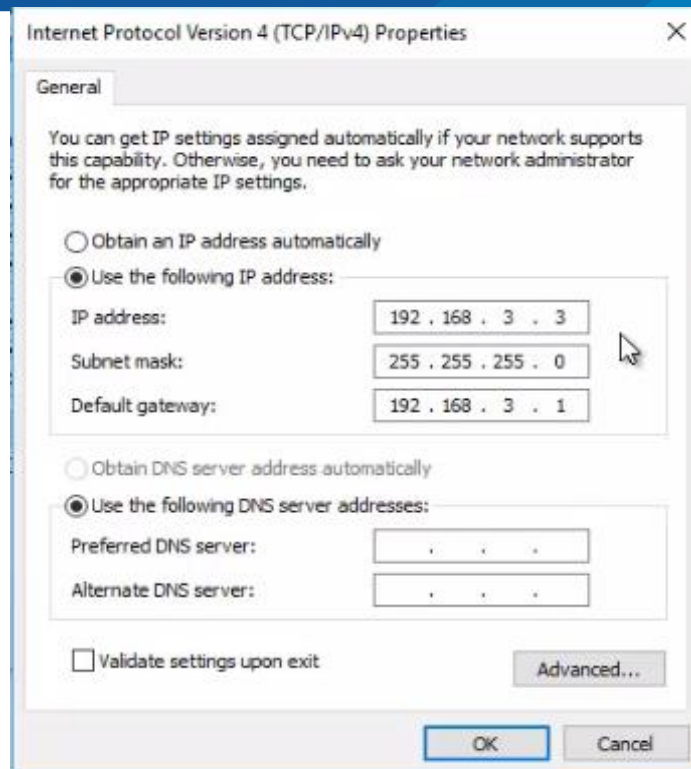


Figura 13: Configuración en la computadora de registro y archivo académico.

Elaboración Propia.

Se trata de hacer una prueba de ping desde el cliente hacia la computadora de registro y archivo académico, esta prueba falla.

```
C:\Users\user1>ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 14: Prueba de conectividad fallida.

Elaboración Propia.

Se verifican las configuraciones en la computadora ubicada en archivo y registro académico, y se determina que está bien configurada y tiene conectividad con su puerta de enlace.

```
C:\Windows\system32\cmd.exe

C:\Users\user1>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection:specific DNS Suffix . . . :
    Link-local IPv6 Address . . . . . : fe80::d435:47d:f213:1fa7%7
    IPv4 Address . . . . . : 192.168.3.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.3.1

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected

    Connection:specific DNS Suffix . . . :

Tunnel adapter
isatap. {96D1FCE7:3B31:417F:8300:7E666A8EDB1B}:

    Media State . . . . . : Media disconnected

    Connection:specific DNS Suffix . . . :

C:\Users\user1>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:
```

Figura 15: Verificación de configuraciones en la computadora de archivo y registro académico.

Elaboración Propia

Para lograr el uso de la herramienta ping entre computadoras basadas en Windows, es necesario desactivar los cortafuegos (firewall) en ambas máquinas.

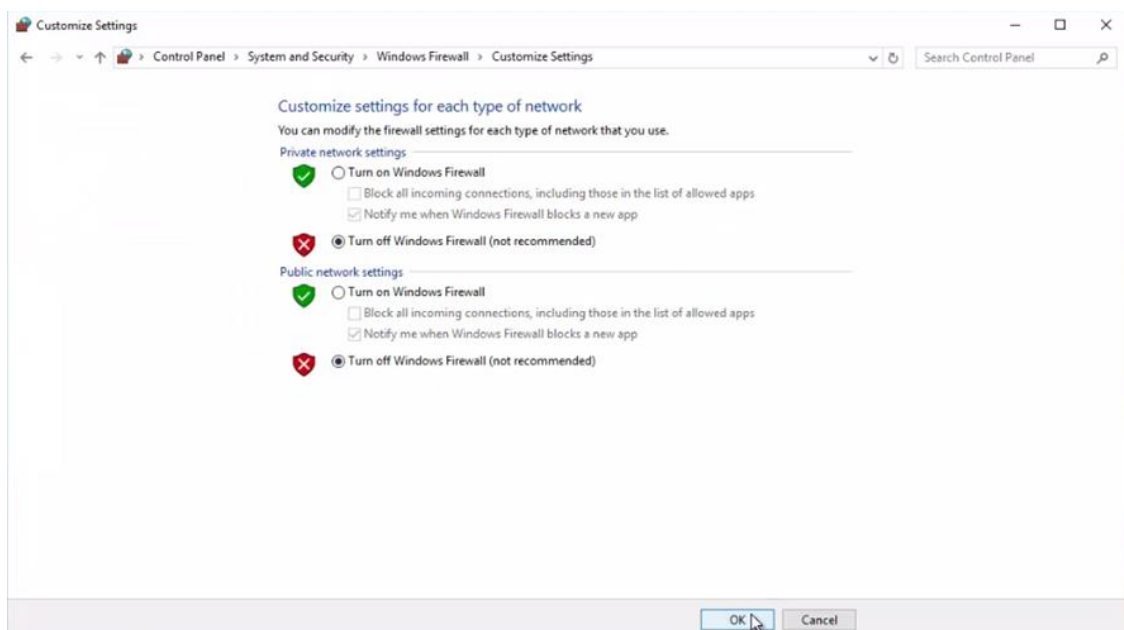


Figura 16: Desactivar el cortafuegos en la computadora de archivo y registro académico.

Elaboración Propia.

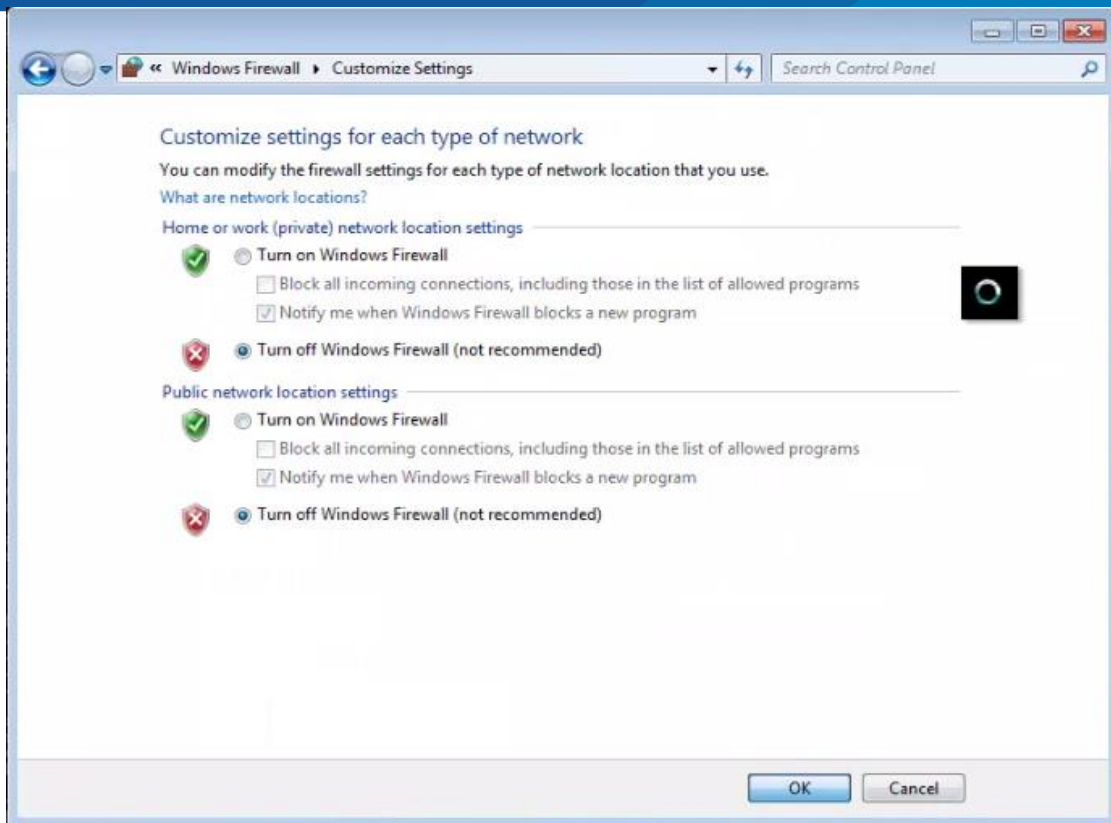


Figura 17: Desactivar el cortafuegos en la computadora cliente.

Elaboración Propia.

Luego se procede a repetir la prueba de conectividad y se puede tener éxito en la prueba de conectividad desde el cliente hacia la computadora destino.

```
C:\Users\user1>ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=55ms TTL=125
Reply from 192.168.3.3: bytes=32 time=39ms TTL=125
Reply from 192.168.3.3: bytes=32 time=43ms TTL=125
Reply from 192.168.3.3: bytes=32 time=37ms TTL=125
Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli:seconds:
        Minimum 37ms, Maximum = 55ms, Average = 43ms
```

Figura 18: Conectividad desde el cliente hacia archivo y registro académico

Elaboración Propia.

También se tiene éxito en la prueba de conectividad desde archivo y registro académico hacia el cliente.

```
C:\Users\user1>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=53ms TTL=125
Reply from 192.168.1.3: bytes=32 time=48ms TTL=125
Reply from 192.168.1.3: bytes=32 time=47ms TTL=125
Reply from 192.168.1.3: bytes=32 time=45ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli:seconds:
        Minimum = 45ms, Maximum = 53ms, Average = 48ms
```

Figura 19: Conectividad desde archivo y registro académico hacia el cliente.

Elaboración Propia.

En R1, R2 y R3 se deben realizar las configuraciones básicas como determinar la longitud mínima de las contraseñas, establecer la contraseña “enable”, configurar la contraseña de consola y líneas terminales virtuales, al mismo tiempo que se configura el tiempo de espera en dichas líneas. Al final se usa el servicio de cifrado de contraseñas. Se muestra como ejemplo las configuraciones en R1.

```
R1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#security passwords min:length 10
R1(config)#enable secret cisco12345
R1(config)#line console 0
R1(config:line) #password ciscoconpass
R1(config:line)#exec:timeout 5 0
R1(config:line)#login
R1(config:line) #logging synchronous
R1(config:line) #line vty 0 4
R1(config:line) #password ciscovtypass
R1(config:line)#exec:timeout 5 0
R1(config:line)#login
R1(config:line)#service password:encryption
```

Figura 20: Configuraciones básicas en R1.

Elaboración Propia.

Es necesario configurar R3 para que sea el servidor VPN, pero antes debemos de prepararlo con configuraciones para que se permita el uso de Cisco Configuration Professional (CCP). Se configura un mensaje de advertencia por cuestiones más legales

que funcionales, se activa el servidor HTTP seguro (HTTPS) y el servidor HTTP también debe ser activado en caso de que haya problemas de acceso usando HTTPS.

```
R3(config)#$ prohibited and prosecuted to the full extent of the law$
R3(config)#ip http secure:server
% Generating 1024 bit RSA keys, keys will be non:exportable...[OK]

R3(config)#
*May 26 15:24:47.743: %SSH:5:ENABLED: SSH 1.99 has been enabled
R3(config)#
*May 26 15:24:47.827: %PKI:4:NOAUTOSAVE: Configuration was modified.
Issue "write memory" to save new certificate
R3(config)#
R3(config)#ip http server
```

Figura 21: Preparación de R3 para su uso con CCP.

Elaboración Propia.

Es necesario crear un usuario con contraseña y con el máximo nivel de privilegios (15). Luego se configura HTTP para que realice la autenticación con la base de datos local de usuarios.

```
R3(config)#username admin01 privilege 15 password admin01pass
R3(config)#ip http authentication local
```

Figura 22: Configuración de usuario y autenticación HTTP.

Elaboración Propia.

El paso posterior es instalar Cisco Configuration Professional (CCP).

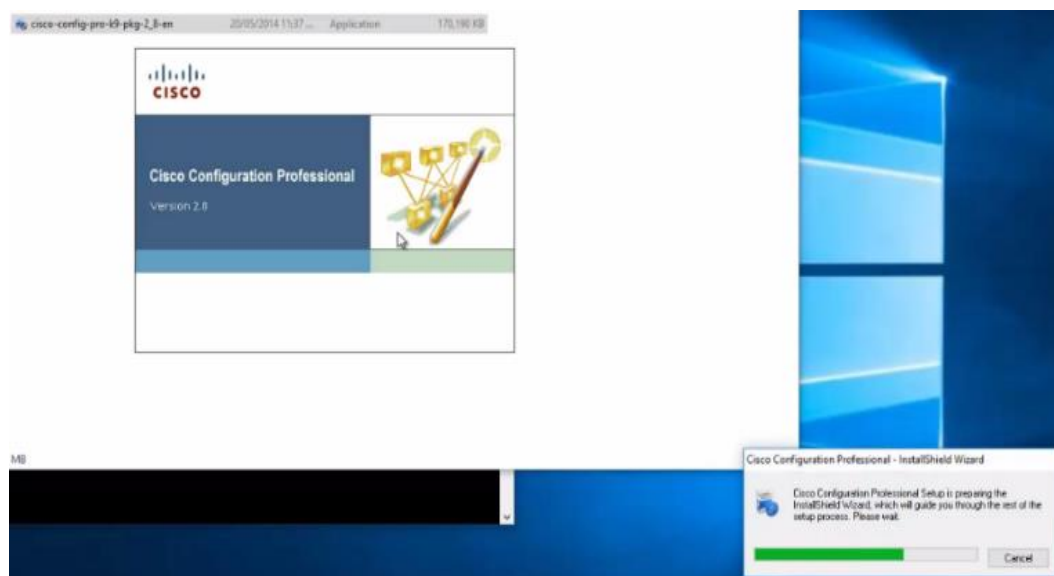


Figura 23: Instalación de CCP.

Elaboración Propia.

Al final de la instalación se muestra si se cumplen los requisitos para que CCP pueda funcionar, en este caso se requiere instalar Java.

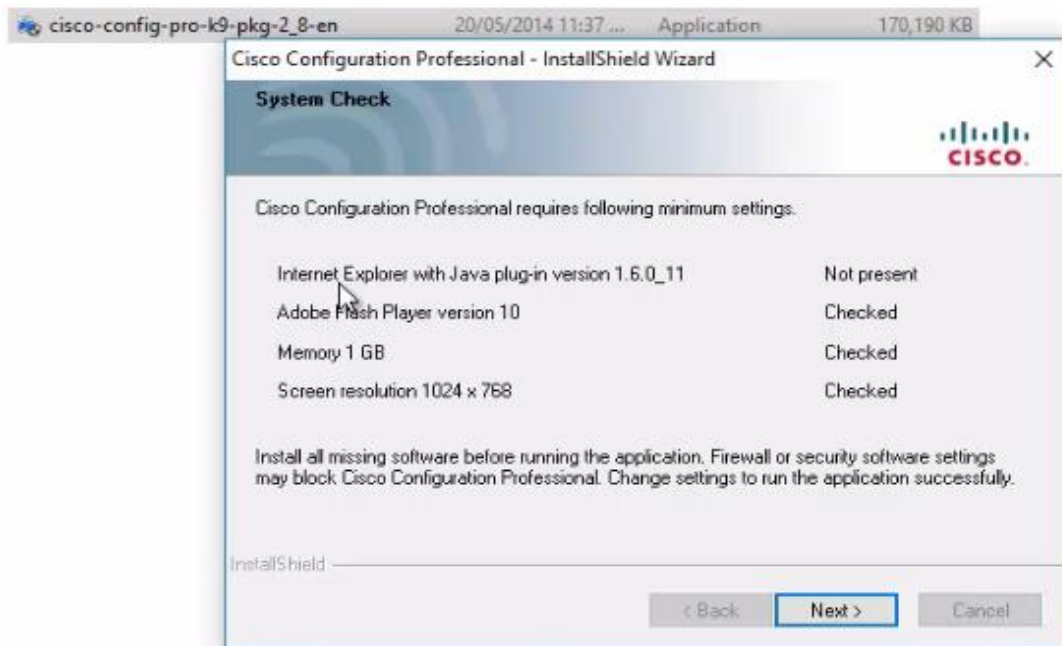


Figura 24: Requisitos para uso de CCP.

Elaboración Propia.

Luego usando Internet se descarga e instala Java desde el sitio java.com.



Figura 25: Sitio de descarga de Java.

Elaboración Propia.



Figura 26: Progreso de instalación de Java.

Elaboración Propia.

Una vez instalado Java es importante configurarlo ingresando al Panel de Control de Windows y buscando las configuraciones de Java (32:bit).

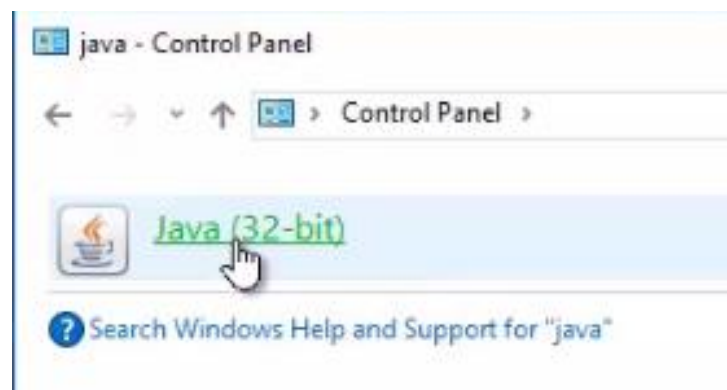


Figura 27: Java en el Panel de Control.

Elaboración Propia.

En la pestaña Security ingresar a Editar Lista de Sitios (Edit Site List) en donde se configurará una excepción, es decir un sitio que será confiable para el administrador, aunque no cumpla con los requerimientos de seguridad completos.

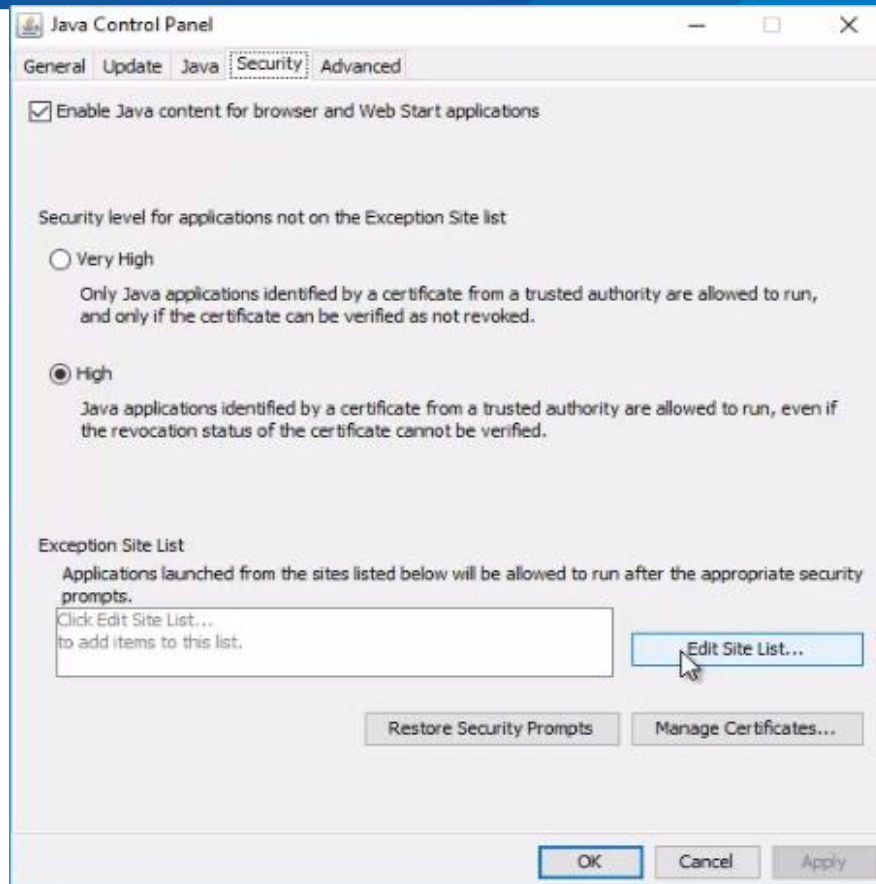


Figura 28: Agregando una excepción en Java.

Elaboración Propia.

Es necesario agregar el sitio `http://127.0.0.1:8600` que usa CCP.

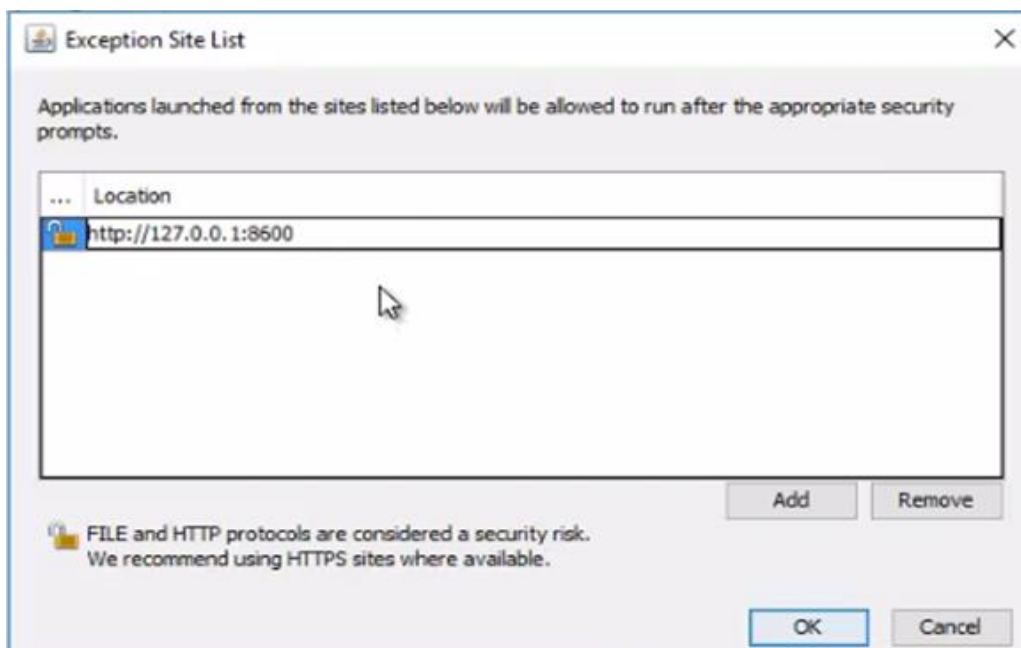


Figura 29: Agregar el sitio que usa CCP en la computadora local.

Elaboración Propia.

El siguiente paso es ejecutar como administrador CCP.

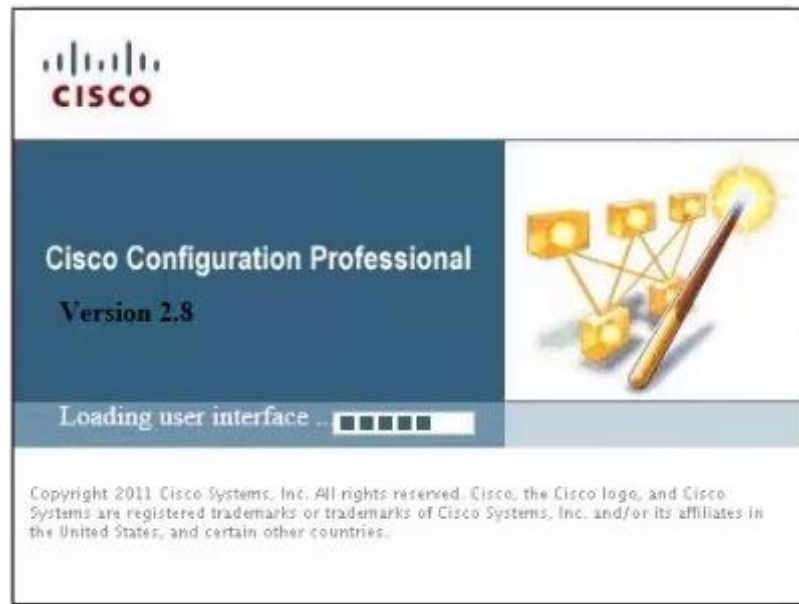


Figura 30: Inicio De CCP.

Elaboración Propia.

Se mostrará una advertencia para confirmar si deseamos correr la aplicación, la respuesta debe ser afirmativa.

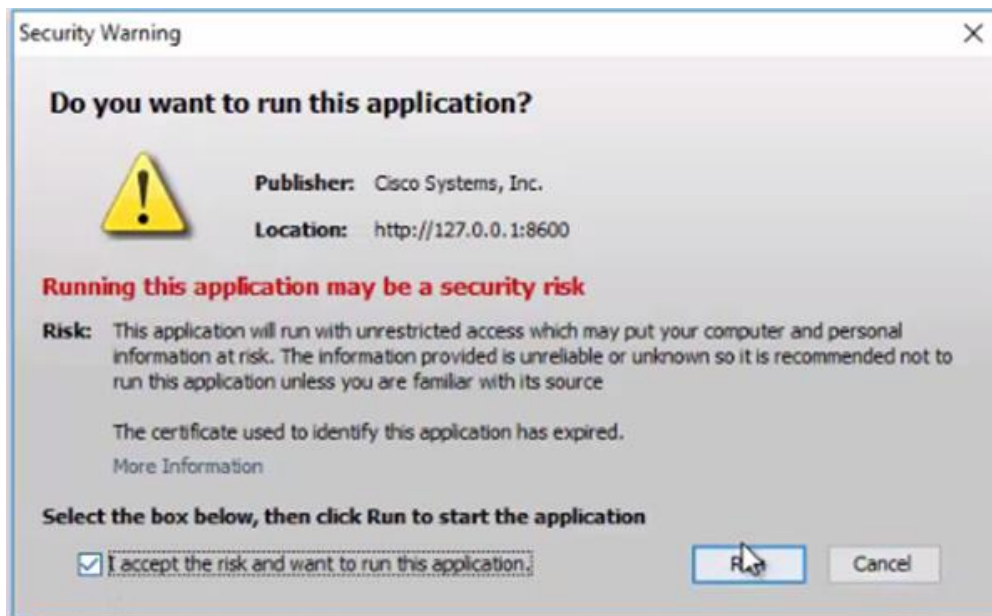


Figura 31: Mensaje de advertencia para el uso de la aplicación.

Elaboración Propia.

Se mostrará un mensaje para mejorar los productos de Cisco, a lo que debemos responder negativamente porque no es parte del estudio.



Figura 32: Mensaje de mejoras para los productos de Cisco.

Elaboración Propia.

Luego emergerá la ventana de comunidad, donde se ingresa la dirección de R3, el nombre de usuario configurado en R3 previamente, admin01 y su respectiva contraseña, admin01pass. Para evitar problemas de seguridad y de certificados, solamente se usará HTTP en el puerto 80, esto no está recomendado porque no es un método seguro, pero como la configuración se realizará sólo una vez, estará permitido. Posteriores configuraciones del túnel IPsec si deberán ser estrictamente seguros.

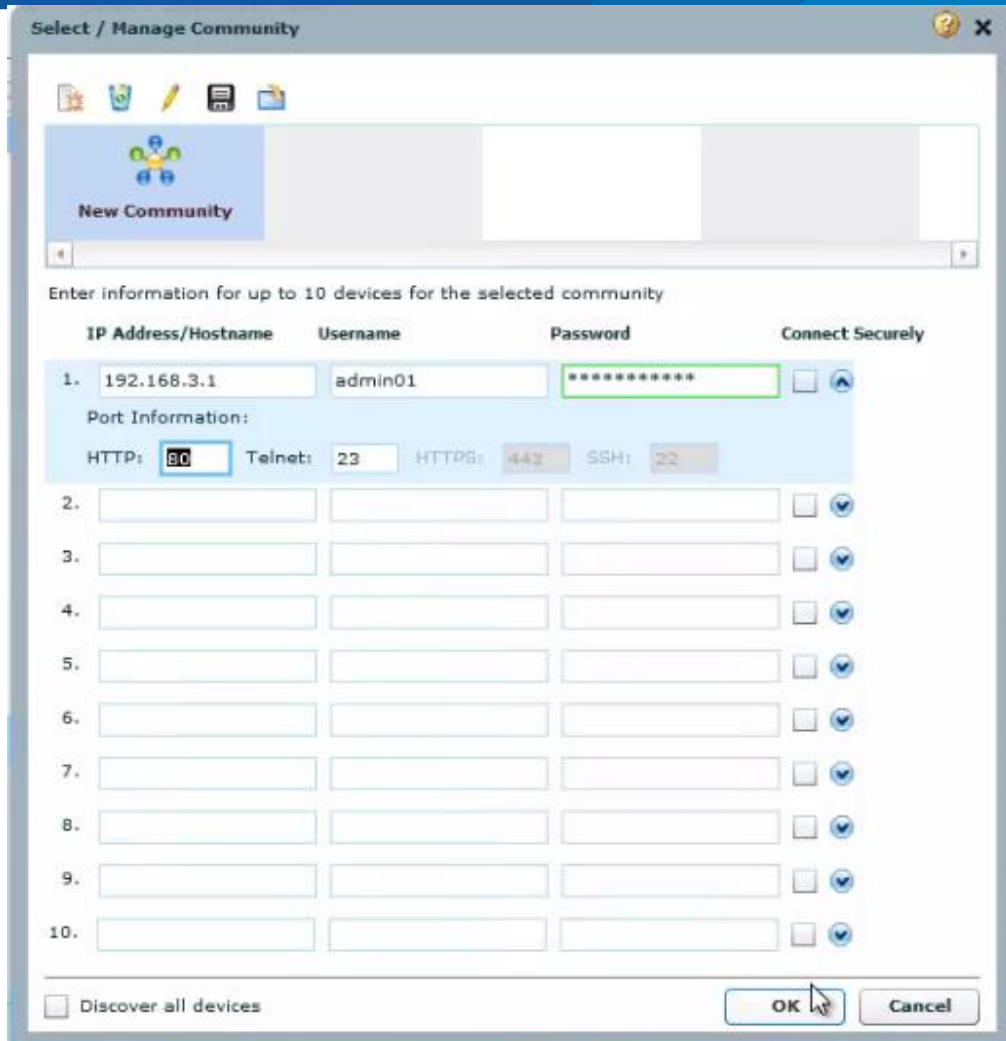


Figura 33: Acceso a R3 usando CCP.

Elaboración Propia.

Para configurar R3 se debe hacer click en Descubrir (Discover).

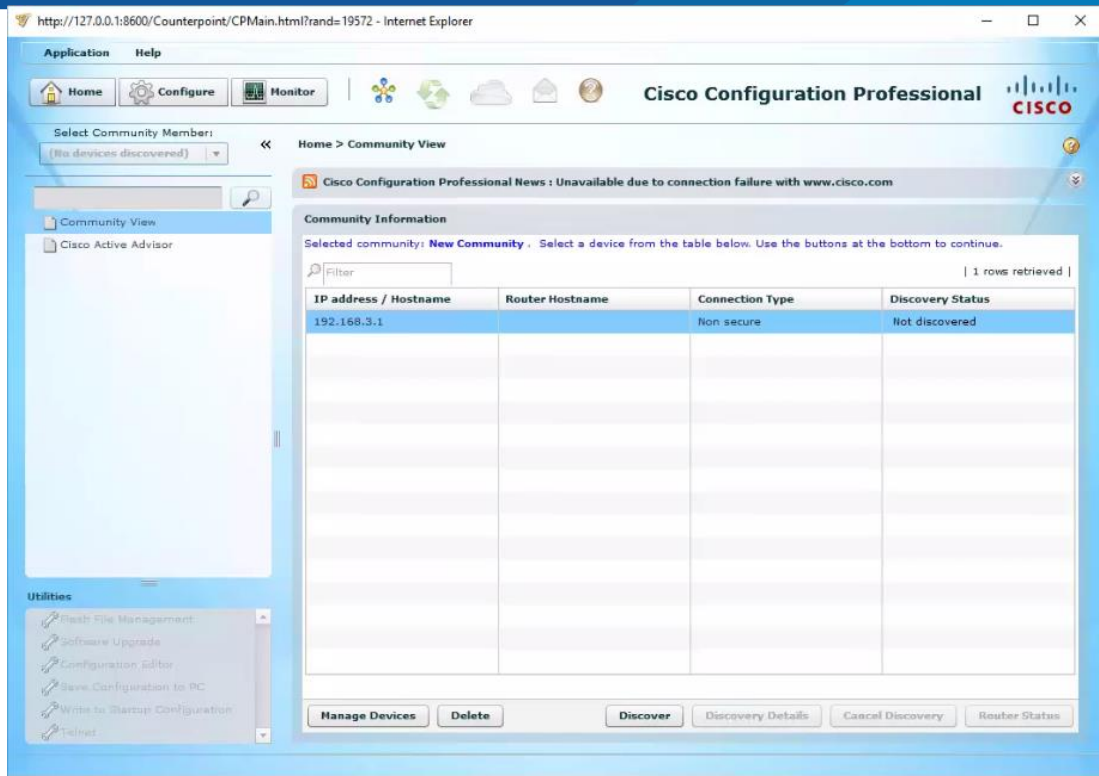


Figura 34: Descubrimiento de R3.

Elaboración Propia.

Luego hacer click en Configurar (Configure) y acceder a la sección Security > Firewall > Firewall. Es necesario elegir el Cortafuegos Básico (Basic Firewall) y hacer click en Launch the selected task.

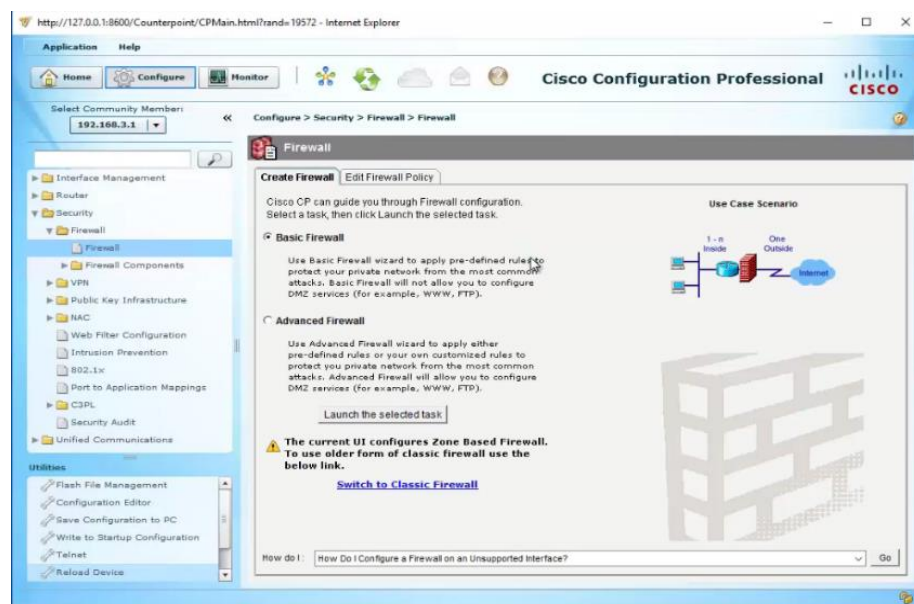


Figura 35: Firewall en R3 usando CCP.

Elaboración Propia.

En la ventana emergente elegir la interfaz G1/0 como confiable interna y la interfaz S3/1 como no confiable externa.

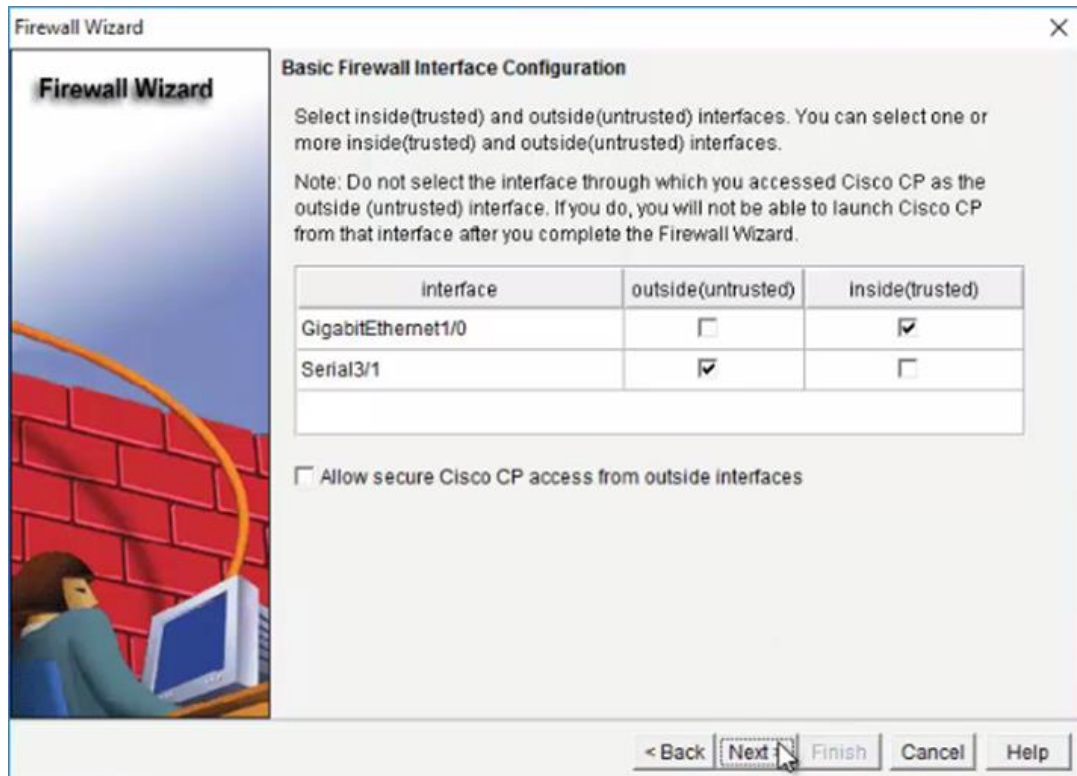


Figura 36: Configuración de interfaces en el Cortafuegos.

Elaboración Propia.

Luego de hacer click en siguiente se configura la seguridad baja para el cortafuegos y pasar al siguiente formulario.

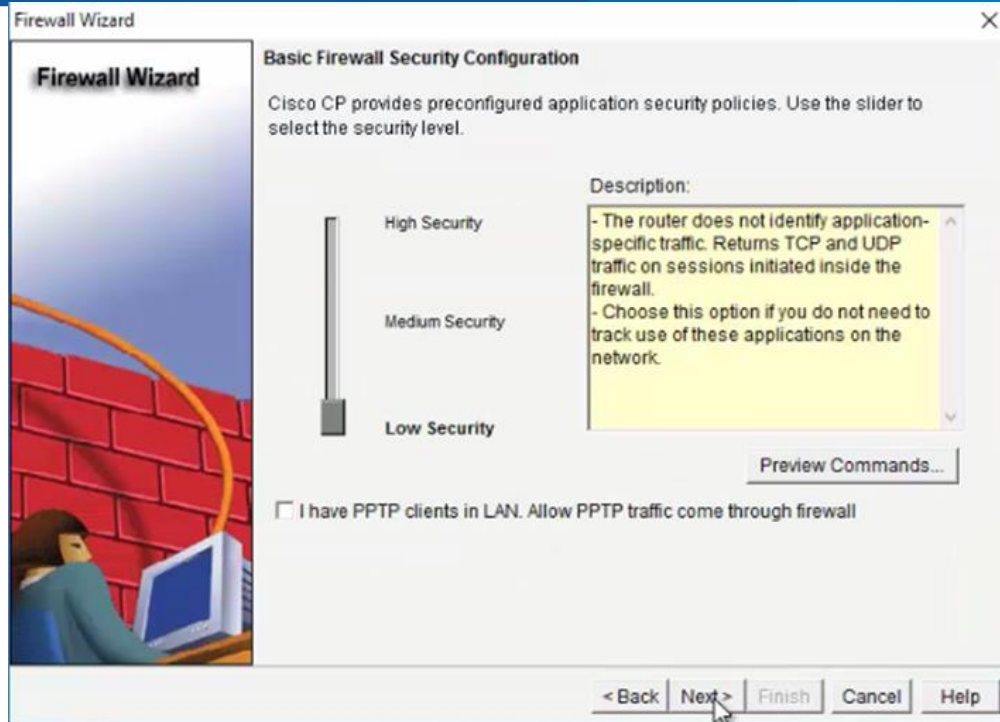


Figura 37: Configuración del nivel de seguridad.

Elaboración Propia.

Seguidamente hay que verificar las configuraciones que se realizarán en el cortafuegos basado en zona (ZBF).

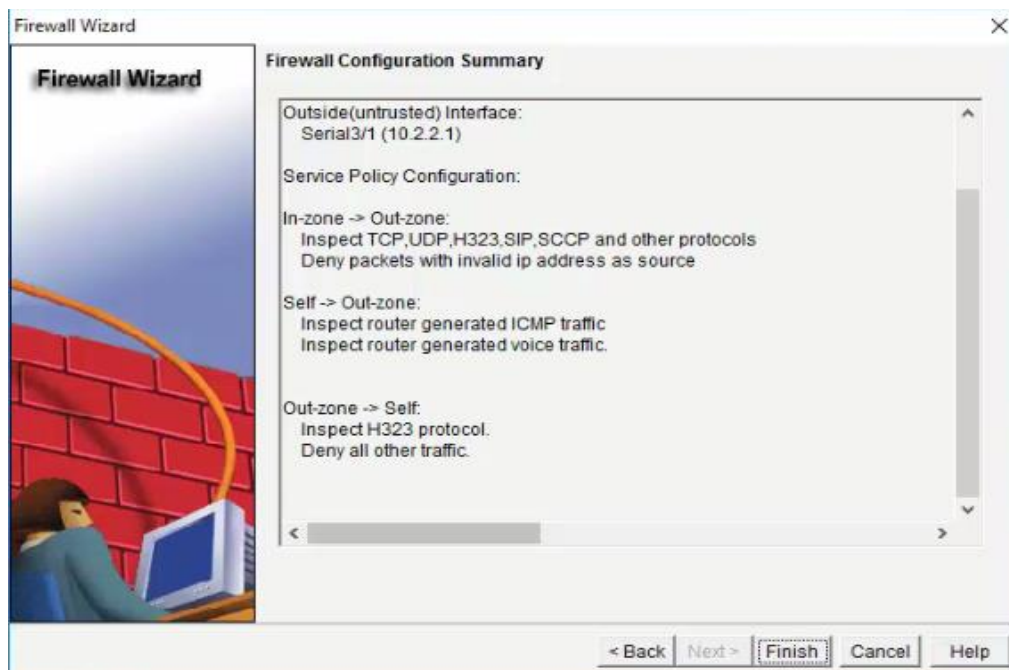


Figura 38: Configuraciones en el Cortafuegos.

Elaboración Propia.

Luego enviar los comandos de configuración hacia el dispositivo haciendo click en Deliver. CCP responderá que el envío fue exitoso y mostrará el número de comandos enviados.

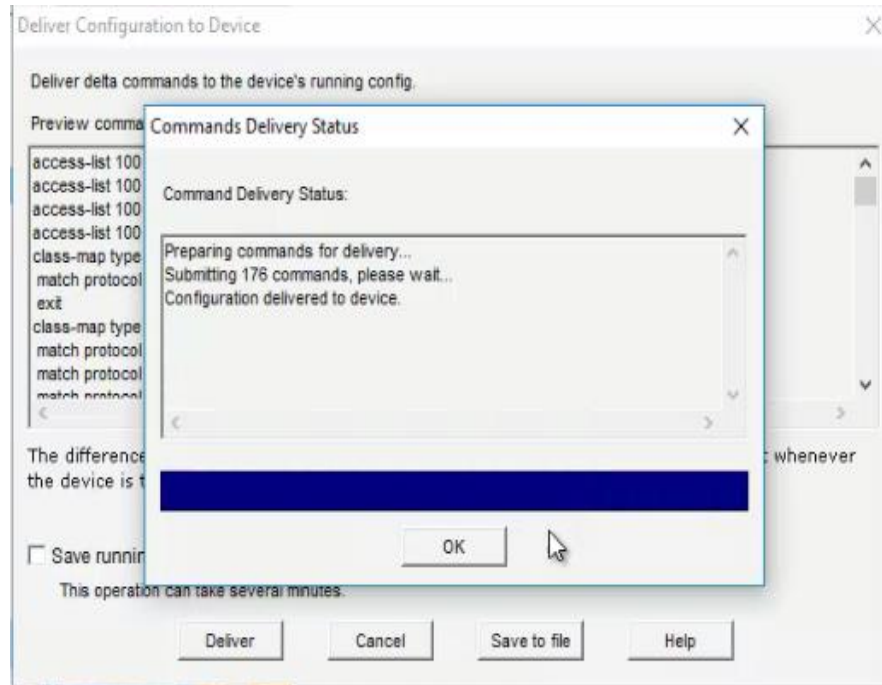


Figura 39: Comandos enviados para configurar ZBF.

Elaboración Propia.

Luego de configurar el cortafuegos basado en zona (ZBF), se hace una prueba de conectividad desde la red interna (archivo y registro académico) hacia R2 (Internet). El resultado es exitoso.

```
C:\Users\user1>ping 10.2.2.2

Pinging 10.2.2.2 with 32 bytes of data:
Reply from 10.2.2.2: bytes=32 time=25ms TTL=254
Reply from 10.2.2.2: bytes=32 time=26ms TTL=254
Reply from 10.2.2.2: bytes=32 time=19ms TTL=254
Reply from 10.2.2.2: bytes=32 time=18ms TTL=254

Ping statistics for 10.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli:seconds:
        Minimum = 18ms, Maximum = 26ms, Average = 22ms
```

Figura 40: Prueba de conectividad hacia Internet.

Elaboración Propia.

Cuando se realiza la prueba desde el exterior (el cliente) hacia la red interna (archivo y registro académico), la prueba fallará porque el cortafuegos basado en zona bloquea el acceso

```
C:\Users\user1>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 41: Prueba de ping desde el exterior hacia la red interna.

Elaboración Propia.

En esta nueva sección configurará el servidor VPN en R3 usando CCP, es necesario acceder a la sección Security > VPN > Easy VPN Server, ingresar al botón Launch Easy VPN Wizard, que permitirá la configuración del servidor.

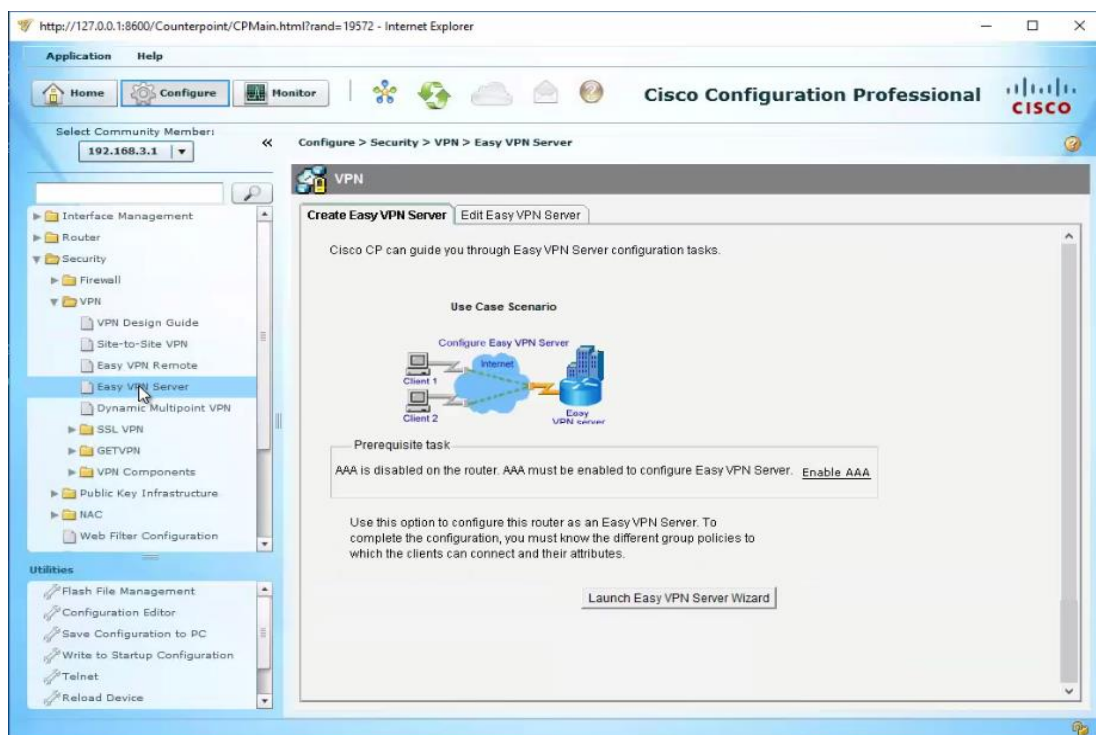


Figura 42: Inicio de configuración de Easy VPN Server.

Elaboración Propia.

CCP preguntará si desea activar AAA en el servidor (R3), la respuesta es afirmativa.

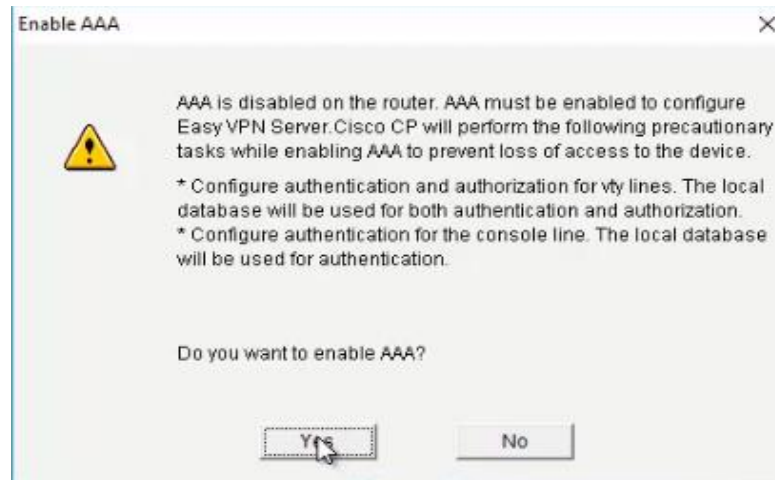


Figura 43: Consulta para activar AAA en el servidor.

Elaboración Propia.

Luego se envían los comandos hacia R3 como se hizo anteriormente.

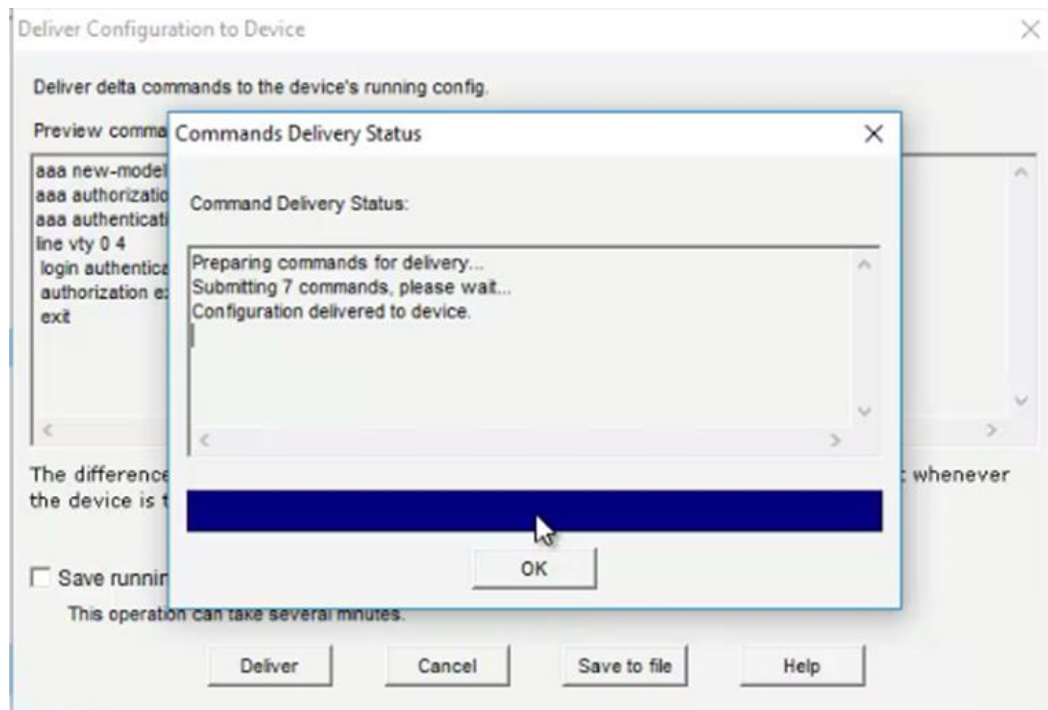


Figura 44: Comandos enviados a R3 para configurar AAA.

Elaboración Propia.

A continuación, se muestran las indicaciones de Easy VPN Server para configurar una VPN.



Figura 45: Indicaciones de Easy VPN Server.

Elaboración Propia.

Como paso siguiente se debe elegir la interfaz S3/1 sin número (unnumbered), que es la interfaz de salida en R3 (servidor VPN). También seleccionar el uso de llave pre:compartida (Pre:Shared Keys).

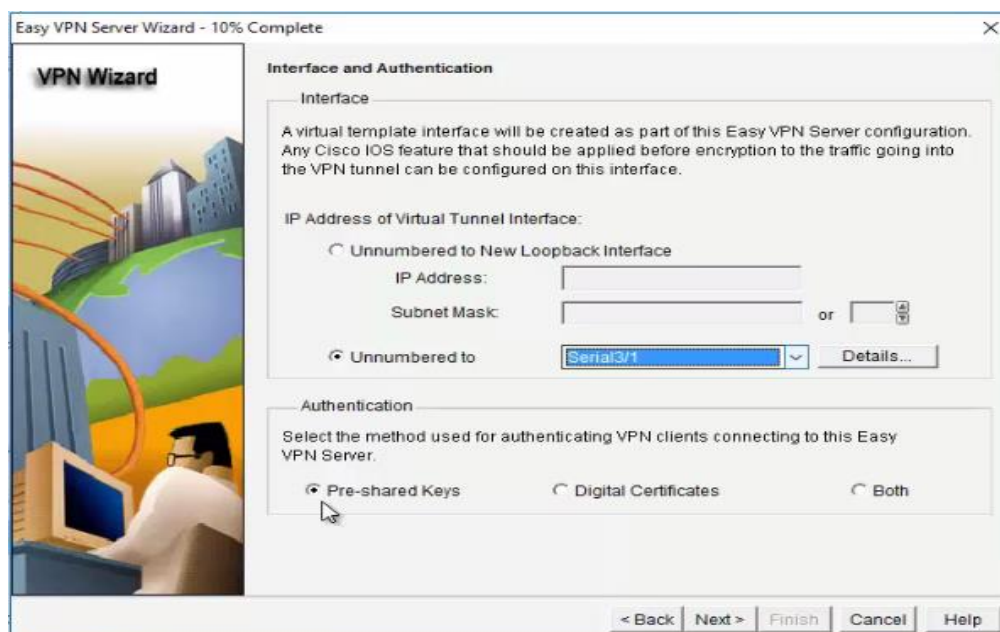


Figura 46: Configuración de interfaz en el servidor VPN (R3).

Elaboración Propia.

En la configuración siguiente se muestra el algoritmo de cifrado por defecto para la autenticación, y es 3DES, el algoritmo HASH por defecto es SHA_1 y será usado para la autenticación. El método para el intercambio de la llave es el Grupo 2 de Diffie Hellman.

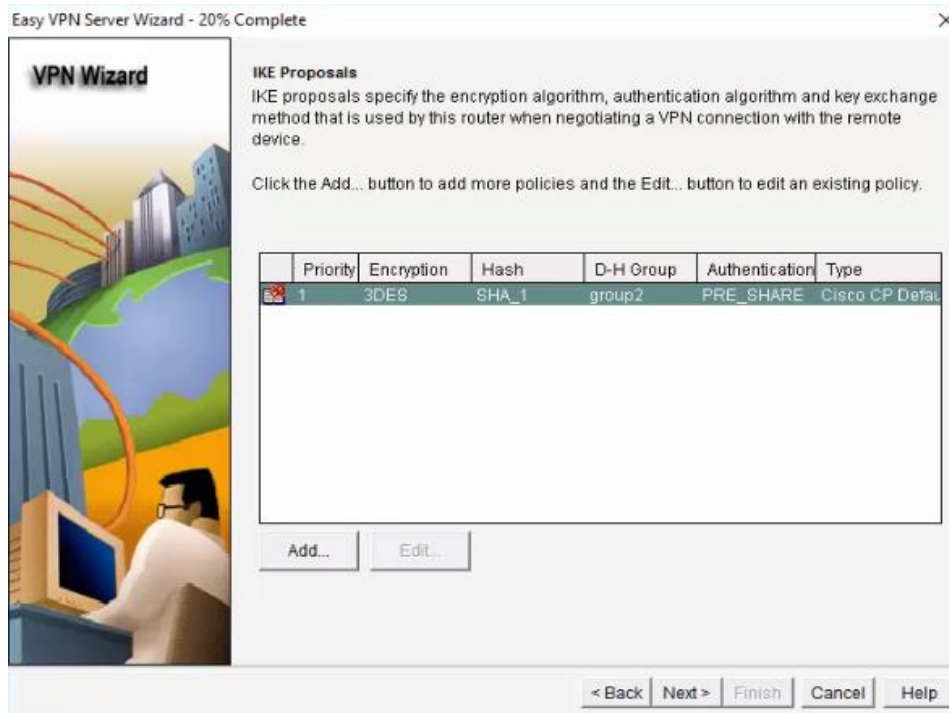


Figura 47: Algoritmos para implementar el servidor VPN.

Fuente: Elaboración Propia.

El algoritmo usado para proteger los datos dentro del túnel VPN con cifrado y autenticación se llama Transform Set. Por defecto se usa 3Des para el cifrado y SHA_HMAC para la integridad.

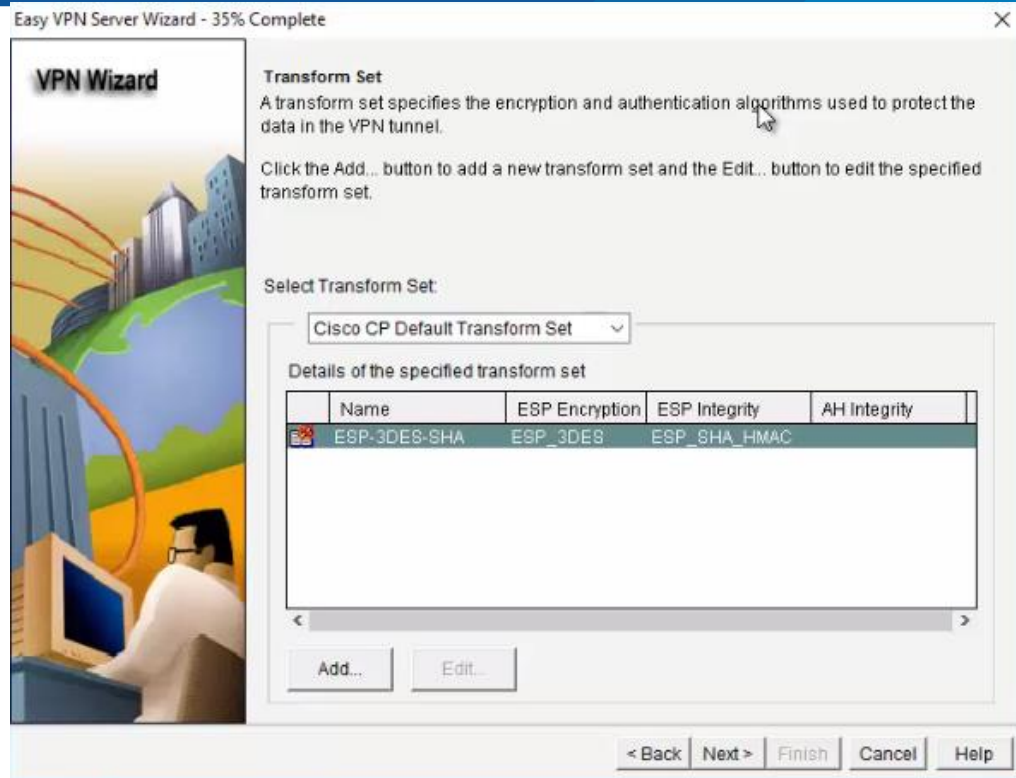


Figura 48: Configuración de Transform Set.

Elaboración Propia.

La configuración del grupo ISAKMP es un grupo de clientes VPN que comparten la misma autenticación e información. Se puede usar un servidor externo, un servidor local o ambos. Seleccionamos un servidor AAA local.

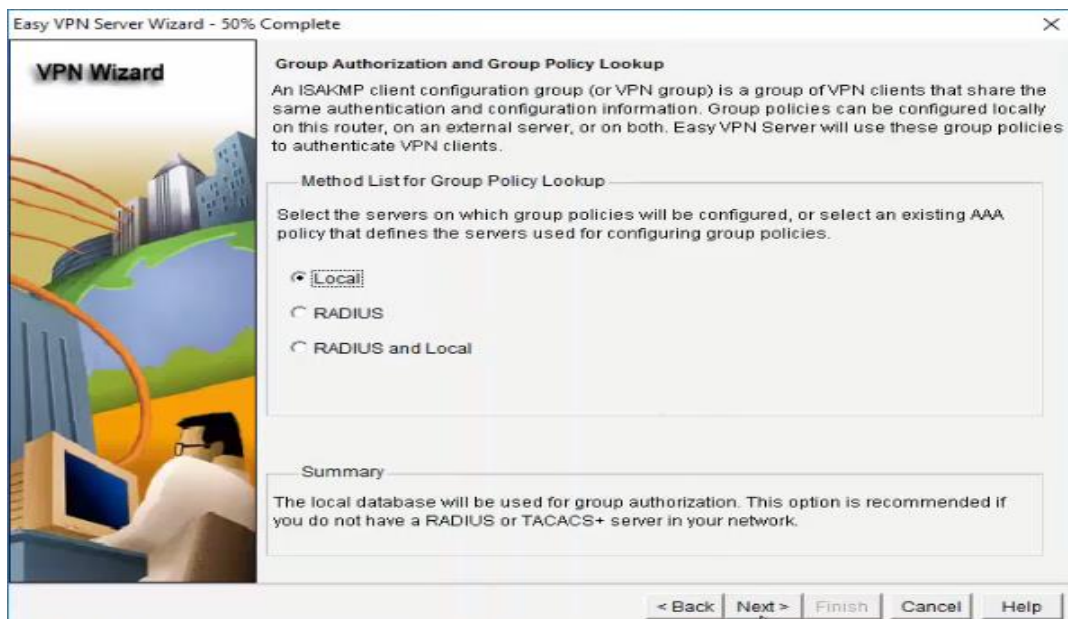


Figura 49: Configuración de AAA para ISAKMP.

Elaboración Propia.

La autenticación de usuario provee seguridad adicional, también se puede elegir alguna de las opciones, preferimos la opción del servidor AAA local.



Figura 50: Configuración del servidor AAA para usuarios.

Elaboración Propia.

Se puede ingresar al botón Agregar Credenciales de Usuario (Add User Credentials), en la ventana emergente ingresar el nombre de usuario, la contraseña, confirmar la contraseña y si se usa un método MD5 para el cifrado. Adicionalmente se puede configurar el nivel de privilegios de usuario.

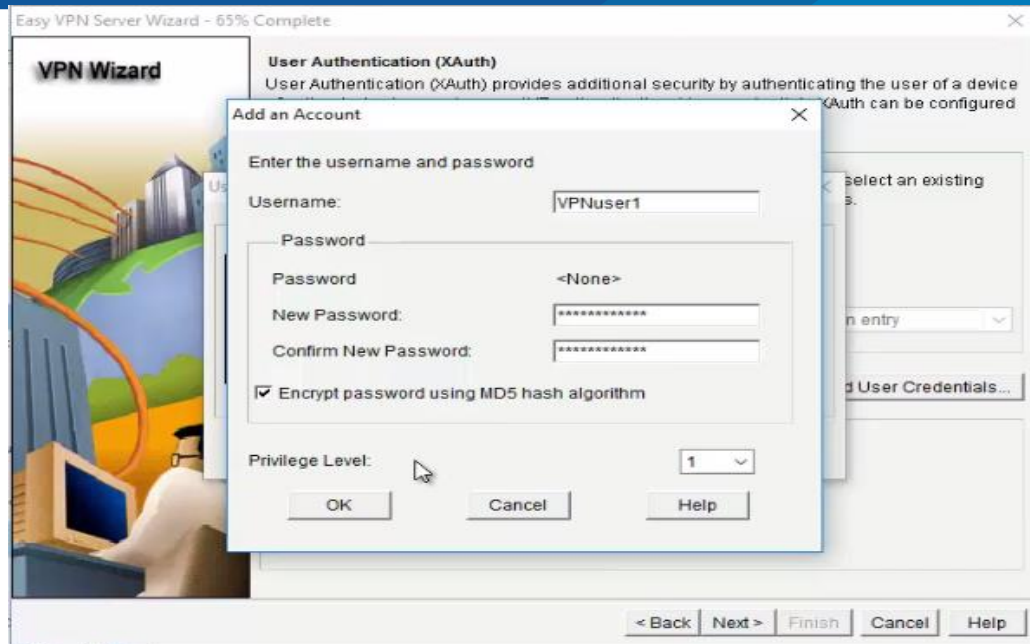


Figura 51: Configuración de un nuevo usuario.

Elaboración Propia.

Para configurar la autorización del grupo y las políticas del grupo de usuarios se establecen atributos y es necesario ingresar al botón Agregar (Add) para su configuración.



Figura 52: Configuración de autorización y políticas de grupo.

Elaboración Propia.

Se configura el nombre del grupo, una contraseña, especificar el pozo de direcciones que serán arrendadas por el servidor hacia los clientes, no es más que un rango de direcciones que corresponden a la red local de R3 (archivo y registro académico).

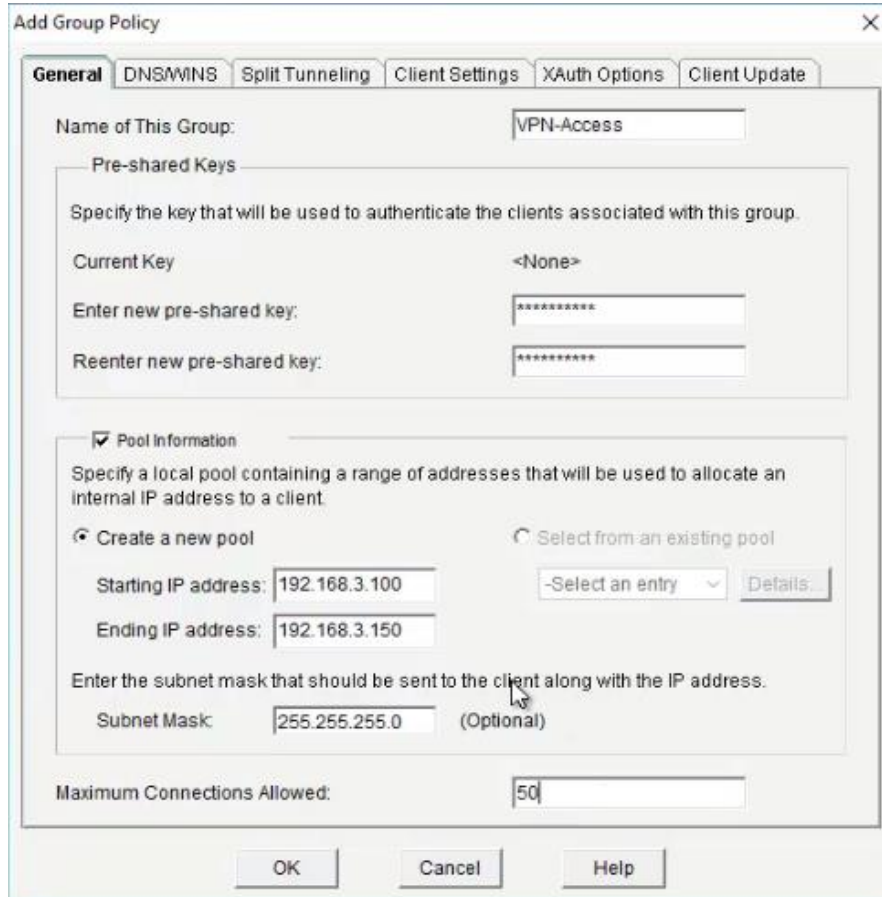


Figura 53: Configuración del grupo de políticas.

Elaboración Propia.

El siguiente paso configurará el tiempo de espera para los clientes que no realicen actividad. Se establece una hora, por ejemplo.



Figura 54: Configuración del tiempo de espera para clientes.

Elaboración Propia.

Para el Protocolo de Control de Túnel de Cisco es preferible no activarlo.



Figura 55: Protocolo de Control de Túnel de Cisco.

Elaboración Propia.

Es necesario modificar la configuración del cortafuegos previamente creado y agregar una entrada con una lista de control de acceso apropiada o política de seguridad que permita que desde la zona exterior (out:zone) se pueda acceder a la red local de R3.

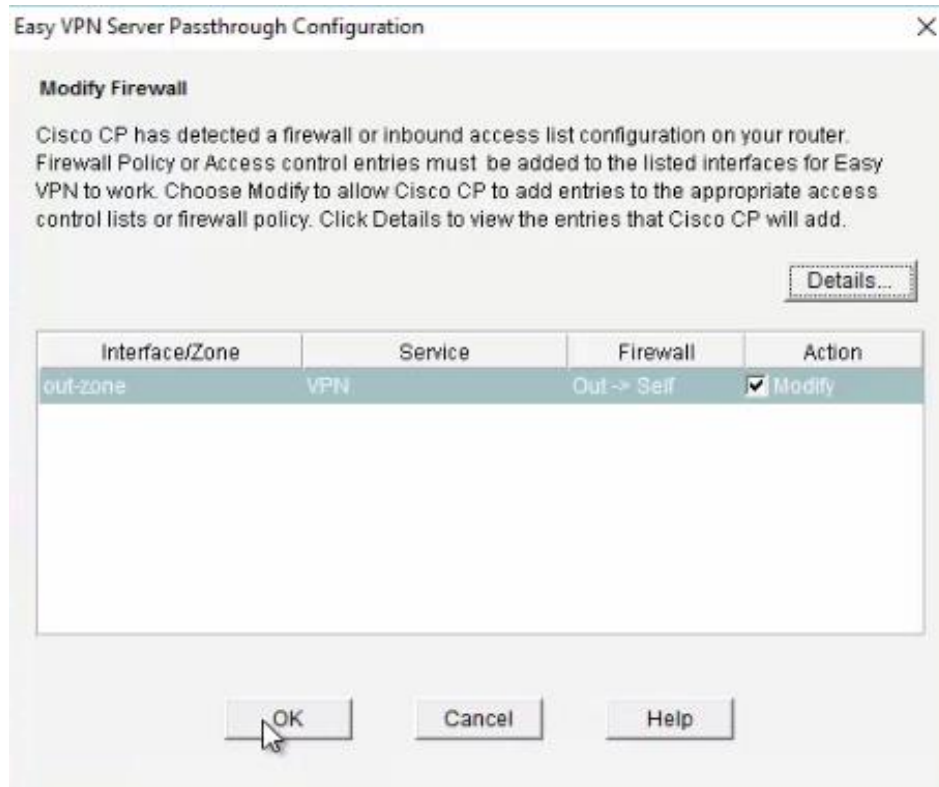


Figura 56: Modificación del cortafuegos para la VPN.

Elaboración Propia.

Finalmente se revisan las configuraciones que se aplicarán en el dispositivo. Aún no probar la conectividad de la VPN después de configurar (Test VPN connectivity after configuring).

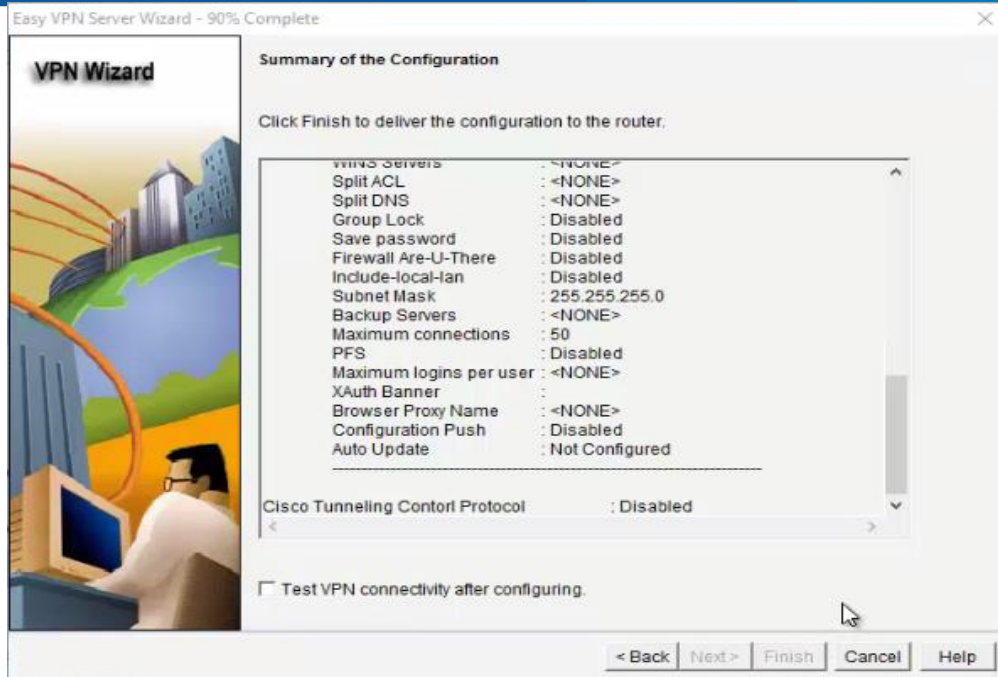


Figura 57: Resumen de configuraciones del servidor VPN.

Elaboración Propia.

Como se hizo en pasos anteriores, enviar los comandos al dispositivo R3.

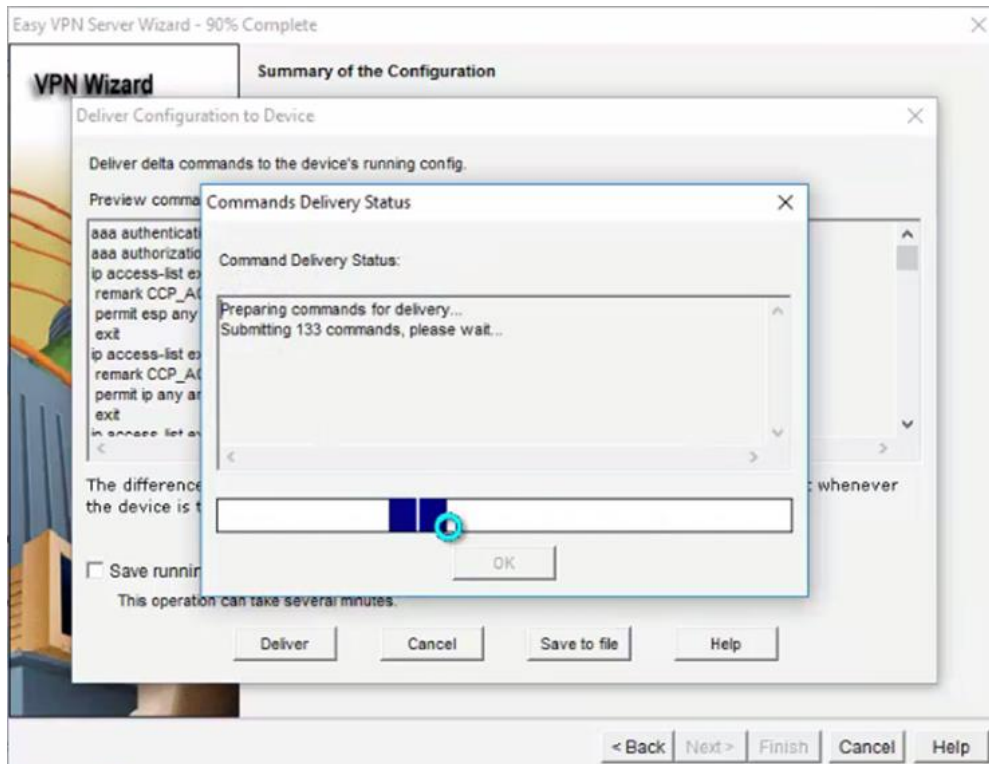


Figura 58: Comandos de configuración del servidor VPN.

Elaboración Propia.

Para hacer la prueba del servidor VPN se hace click en probar el servidor VPN (Test VPN Server).

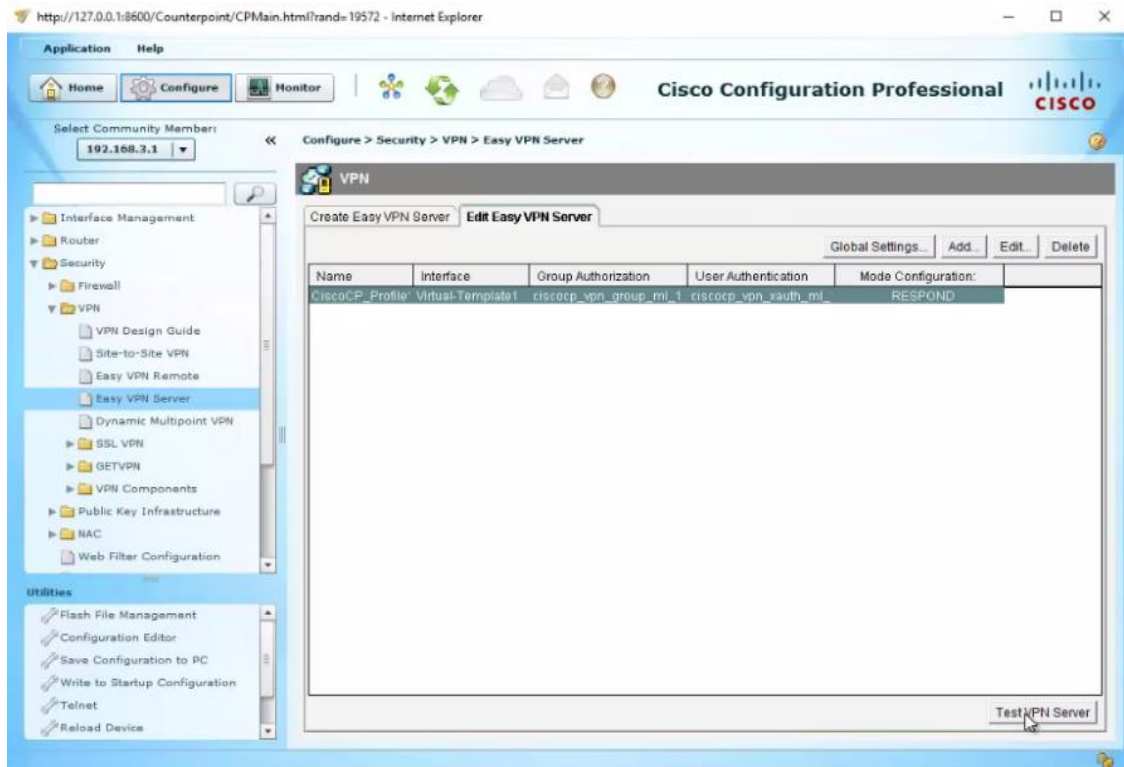


Figura 59: Botón de prueba del servidor VPN.

Elaboración Propia.

La prueba es exitosa porque indica que el servidor está levantado (VPN Tunnel is up).

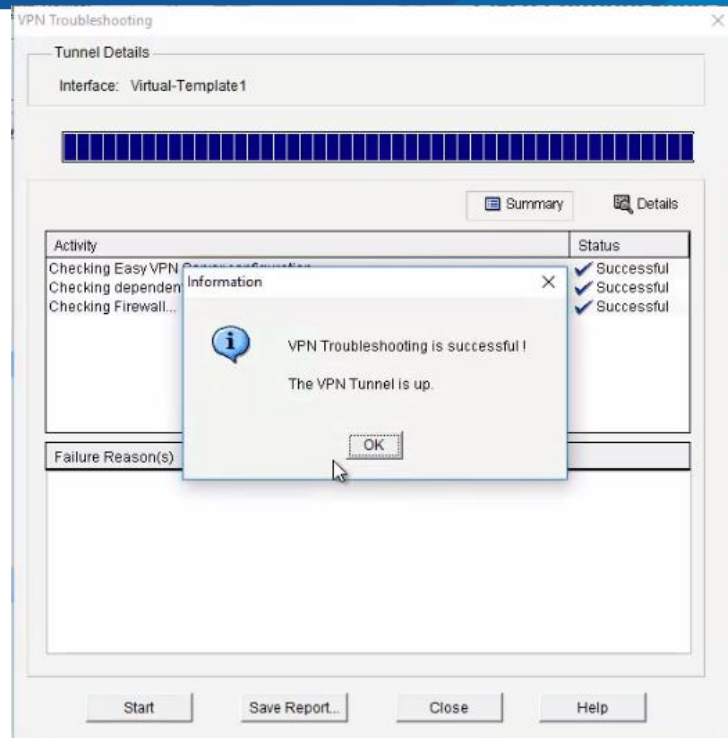


Figura 60: Prueba del servidor VPN exitosa.

Elaboración Propia.

El paso siguiente se debe realizar en la máquina cliente ubicada en una zona exterior a archivo y registro académico (zona amarilla). Aquí se instala el software Cisco Systems VPN Client 5.0, que actúa como cliente VPN.



Figura 61: Instalación de Cisco Systems VPN Client.

Elaboración Propia.

Una vez instalado el software es necesario configurar una nueva conexión (New).

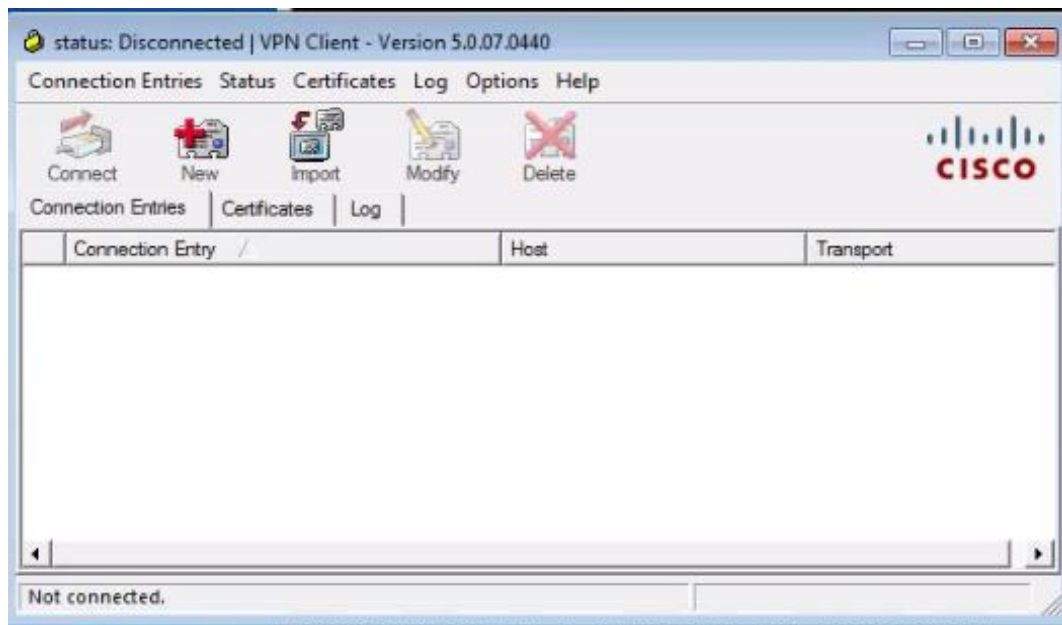


Figura 62: Ejecución de Cisco Systems VPN Client.

Elaboración Propia.

En la ventana emergente elegir un nombre y descripción cualquier para la entrada, luego ingresar la dirección IP del servidor (Host), que es la dirección IP de la interfaz S3/1 en R1, luego en el grupo de autenticación ingresar el nombre VPN:Access como se configuró en el servidor, es necesario tener cuidado por ser sensible a mayúsculas y minúsculas; seguidamente ingresar la contraseña y guardas (Save).



Figura 63: Configuración del servidor (Host) y grupo de autenticación en el cliente.

Elaboración Propia.

Aparece otra ventana emergente donde se debe ingresar el usuario y contraseña, también tener cuidado porque es sensible a mayúsculas y minúsculas. Se trata del usuario que se agregó previamente al momento de configurar el servidor VPN.

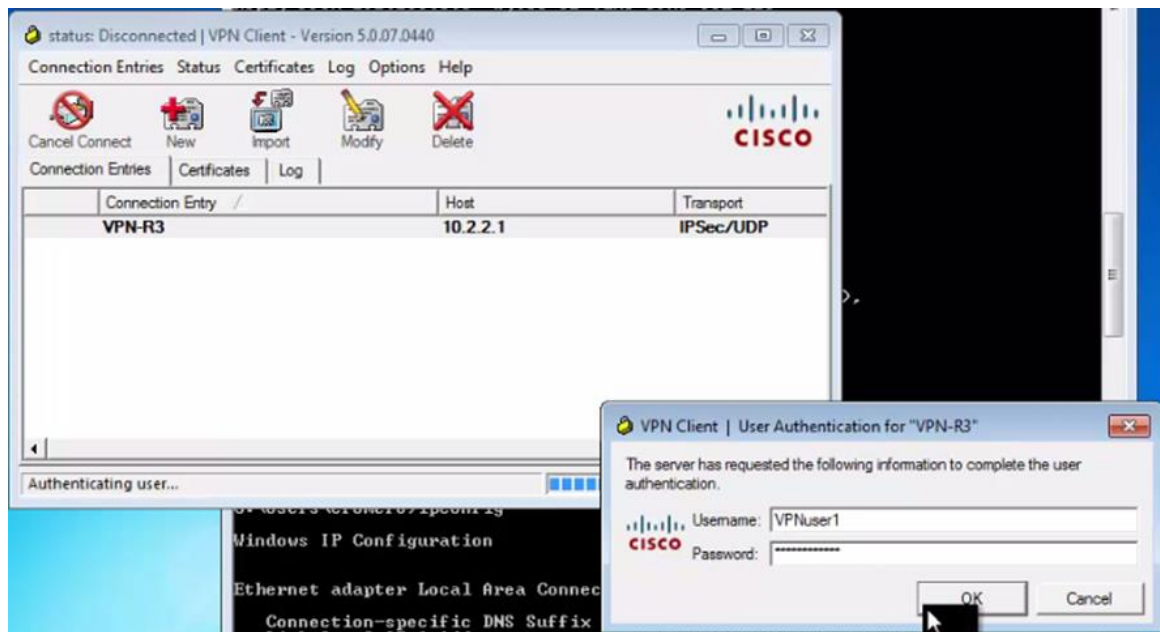
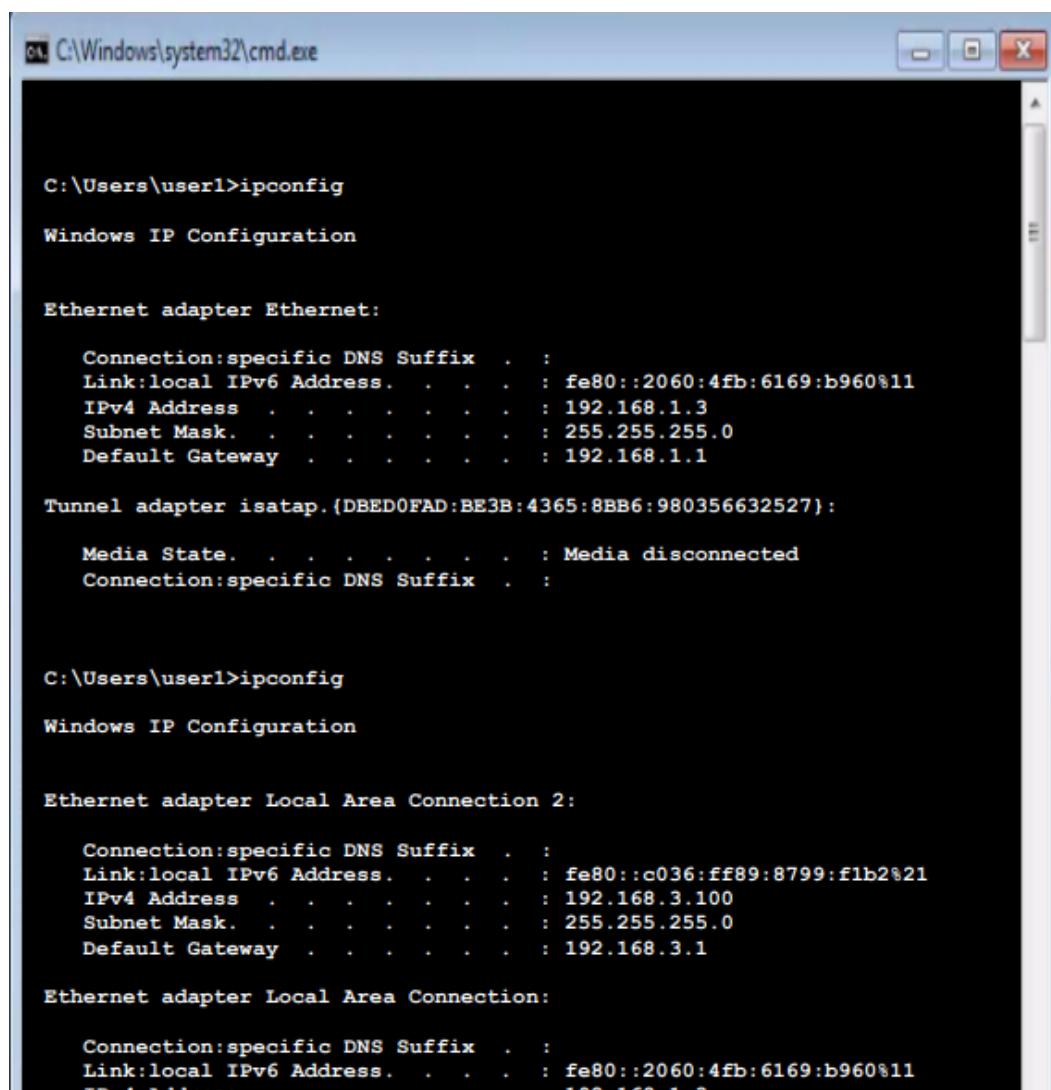


Figura 64: Usuario y contraseña del cliente VPN.

Elaboración Propia.

En el cliente se verifica que hay una nueva conexión de área local (Local Area connection 2, y tiene la dirección IP 192.168.3.100, la primera del pozo de direcciones configurado en el servidor, esta dirección IP corresponde a la LAN de R3, la zona de archivo y registro académico. La primera conexión aún existe y se hace la comparativa del antes y después de la configuración del cliente VPN, antes solo había una conexión y ahora existen dos.



```
C:\Windows\system32\cmd.exe

C:\Users\user1>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection:specific DNS Suffix . . . :
    Link:local IPv6 Address. . . . . : fe80::2060:4fb:6169:b960%11
    IPv4 Address . . . . . : 192.168.1.3
    Subnet Mask. . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter isatap.{DBED0FAD:BE3B:4365:8BB6:980356632527}:

    Media State. . . . . : Media disconnected
    Connection:specific DNS Suffix . . . :

C:\Users\user1>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection:specific DNS Suffix . . . :
    Link:local IPv6 Address. . . . . : fe80::c036:ff89:8799:f1b2%21
    IPv4 Address . . . . . : 192.168.3.100
    Subnet Mask. . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.3.1

Ethernet adapter Local Area Connection:

    Connection:specific DNS Suffix . . . :
    Link:local IPv6 Address. . . . . : fe80::2060:4fb:6169:b960%11
    IPv4 Address . . . . . : 192.168.1.3
```

Figura 65: Antes y después de configurar el cliente VPN.

Elaboración Propia.

La prueba de conectividad es exitosa desde el cliente VPN hacia la computadora ubicada en la LAN de R3 (archivo y registro académico).

```
C:\Users\user1>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=112ms TTL=127
Reply from 192.168.3.3: bytes=32 time=102ms TTL=127
Reply from 192.168.3.3: bytes=32 time=121ms TTL=127
Reply from 192.168.3.3: bytes=32 time=94ms TTL=127

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli:seconds:
        Minimum = 94ms, Maximum = 121ms, Average = 107ms
```

Figura 66: Prueba de ping después de configurar el cliente VPN.

Elaboración Propia.

A continuación, se muestran las estadísticas del cliente VPN, que usa una dirección IP 192.168.3.100, se conecta con el servidor VPN en 10.2.2.1, se muestra los bytes recibidos y enviados, los métodos de cifrado y autenticación, los paquetes cifrados y descifrados; y otras características. Los paquetes cifrados (Encrypted) son los que pasan por el túnel IPsec, aquí se demuestra cómo el túnel creado entre el cliente y el servidor VPN (R3) está cifrado.

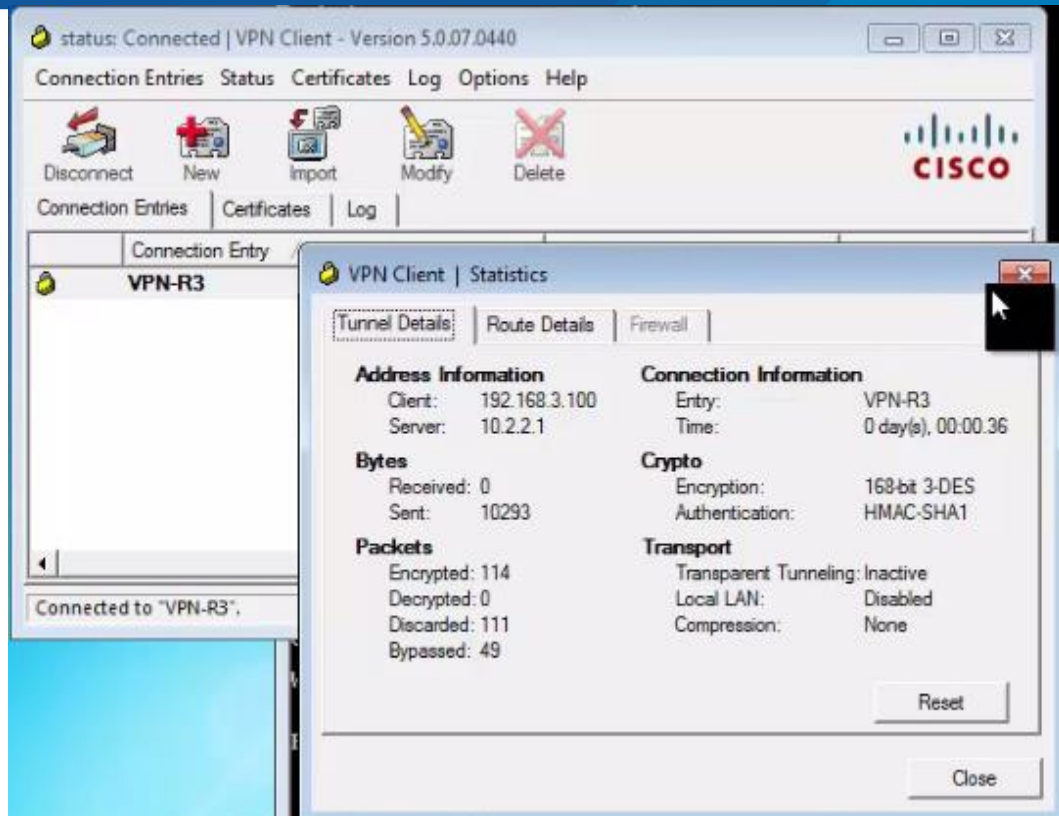


Figura 67: Estadísticas del cliente VPN.

Elaboración Propia.

En la consola de R3 se muestra que la interfaz denominada Virtual: Access2 se levanta (up). Esto no es un comando ingresado en la consola del router R3, simplemente es un registro que notifica el cambio de estado de la interfaz.

```
R3 (config) #
*May 26 16:34:30.639: %LINEPROTO:5:UPDOWN: Line protocol on
Interface Virtual:Access2, changed state to down
R3 (config) #
*May 26 16:34:40.571: %LINEPROTO:5:UPDOWN: Line protocol on
Interface Virtual:Access2, changed state to up
R3 (config) #
```

Figura 68: Interfaz virtual levantada para la VPN en el servidor R3.

Elaboración Propia.

Para un análisis de captura paquetes se realiza una prueba de conectividad desde el cliente hacia la computadora ubicada en la LAN de R3, se usa la opción -t para que sea continua.

```
C:\Users\user1>ping 192.168.3.3 :t

Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=38ms TTL=127
Reply from 192.168.3.3: bytes=32 time=34ms TTL=127
Reply from 192.168.3.3: bytes=32 time=33ms TTL=127
Reply from 192.168.3.3: bytes=32 time=43ms TTL=127
Reply from 192.168.3.3: bytes=32 time=43ms TTL=127
```

Figura 69: Prueba de conectividad continua.

Elaboración Propia.

En la computadora de destino, es decir la que está ubicada en el archivo y registro académico, se usa la herramienta Wireshark que captura los paquetes en su interfaz de red.

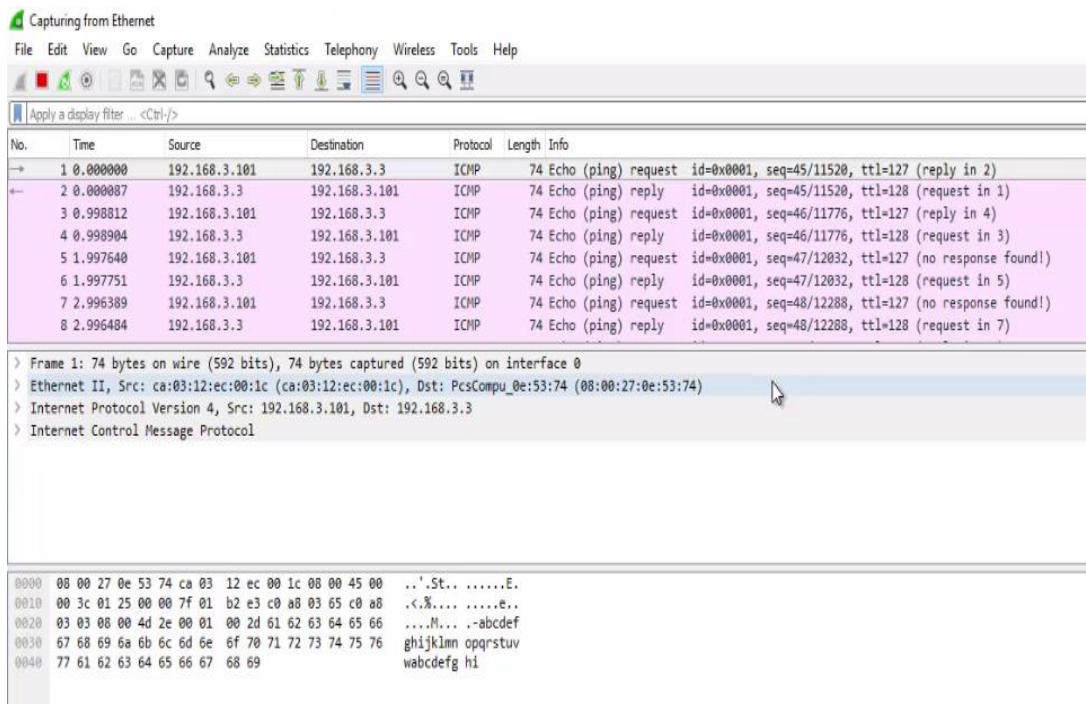


Figura 70: Captura de paquetes en la máquina ubicada en la LAN de R3.

Elaboración Propia.

Para realizar el análisis de un servicio se procede a compartir una carpeta en la red y de esta forma hacer la transferencia de un archivo. Se creó el directorio o carpeta Shared dentro Downloads, allí se crea un archivo.

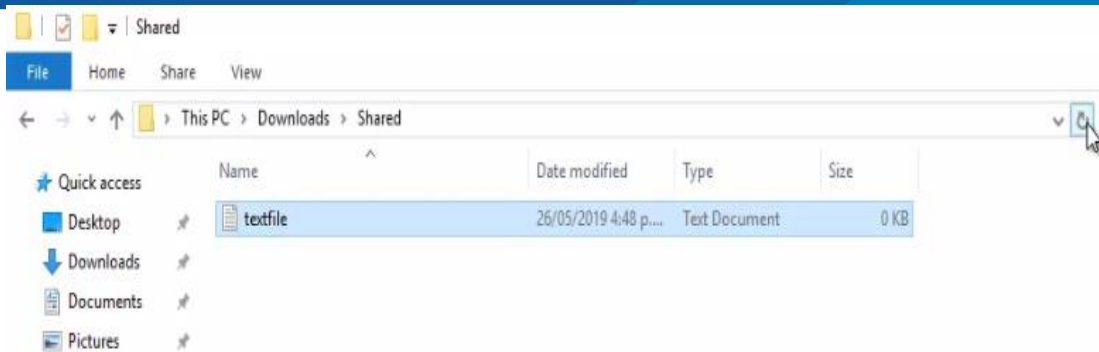


Figura 71: Directorio con un archivo que será compartido en la red.

Elaboración Propia.

Luego en propiedades se comparte el recurso en la red. Dentro de la pestaña Sharing se comparte el recurso con la opción Share.

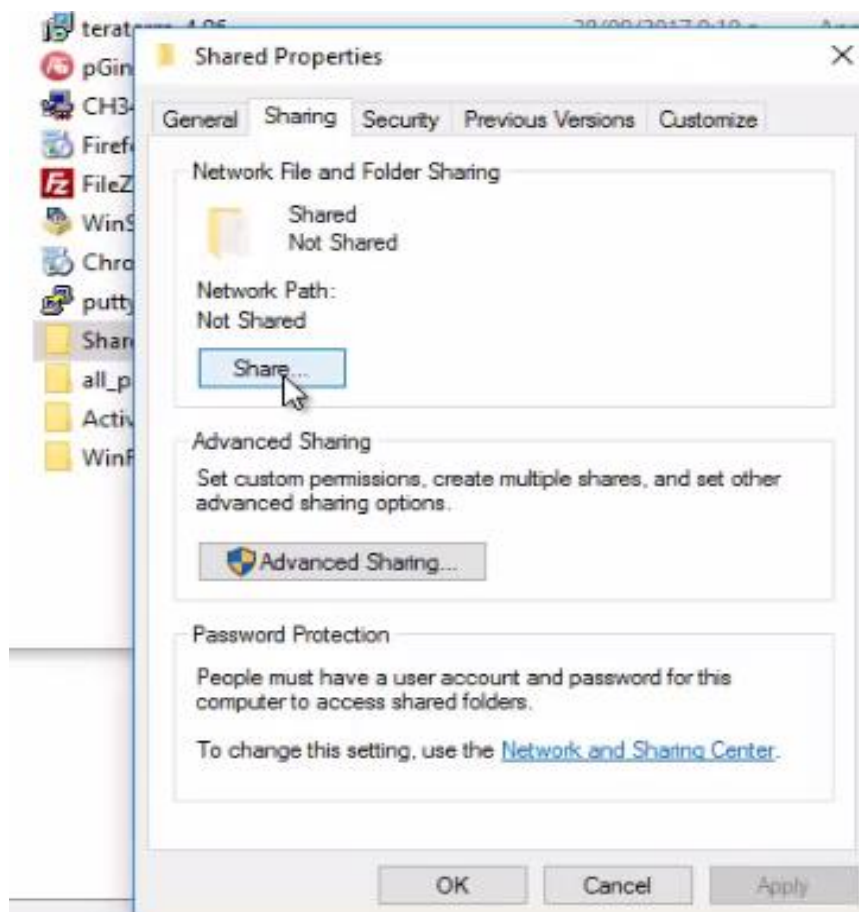


Figura 72: Propiedades de directorio para compartirlo en la red.

Fuente: Elaboración Propia.

En las opciones se pueden elegir los usuarios o el grupo de usuarios con quienes se compartirá el recurso. Luego para compartir de forma avanzada (Advanced Sharing), ingresa a la sección correspondiente.

Es necesario activar el checkbox para compartir el folder (Share this folder) y aceptar (OK).

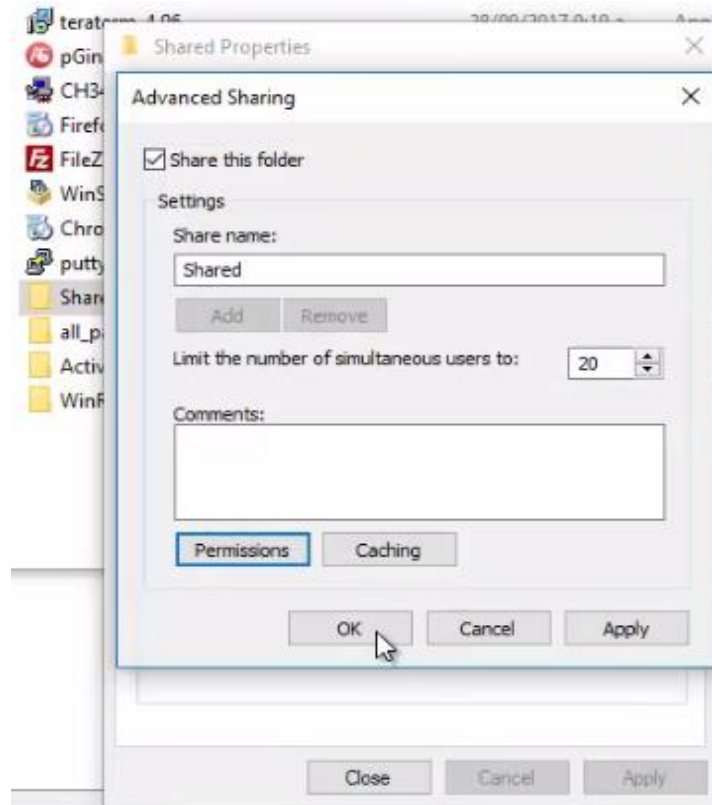


Figura 73: Activación del folder compartido.

Elaboración Propia.

Desde el cliente se ingresa al recurso ingresando la dirección de la computadora de destino ubicada en la red de archivo y registro académico. La dirección es [\\192.168.3.3](http://192.168.3.3).



Figura 74: Acceso al recurso compartido desde el cliente.

Elaboración Propia.

Se ingresa a la carpeta compartida Shared.

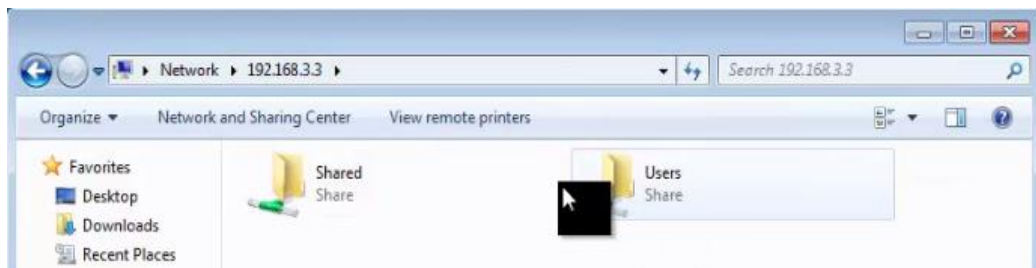


Figura 75: Carpetas compartidas en la máquina de destino.

Elaboración Propia.

Luego se procede a copiar y pegar el archivo compartido dentro de la carpeta, esta transferencia se realiza desde la computadora ubicada en archivo y registro académico, hacia el cliente externo.

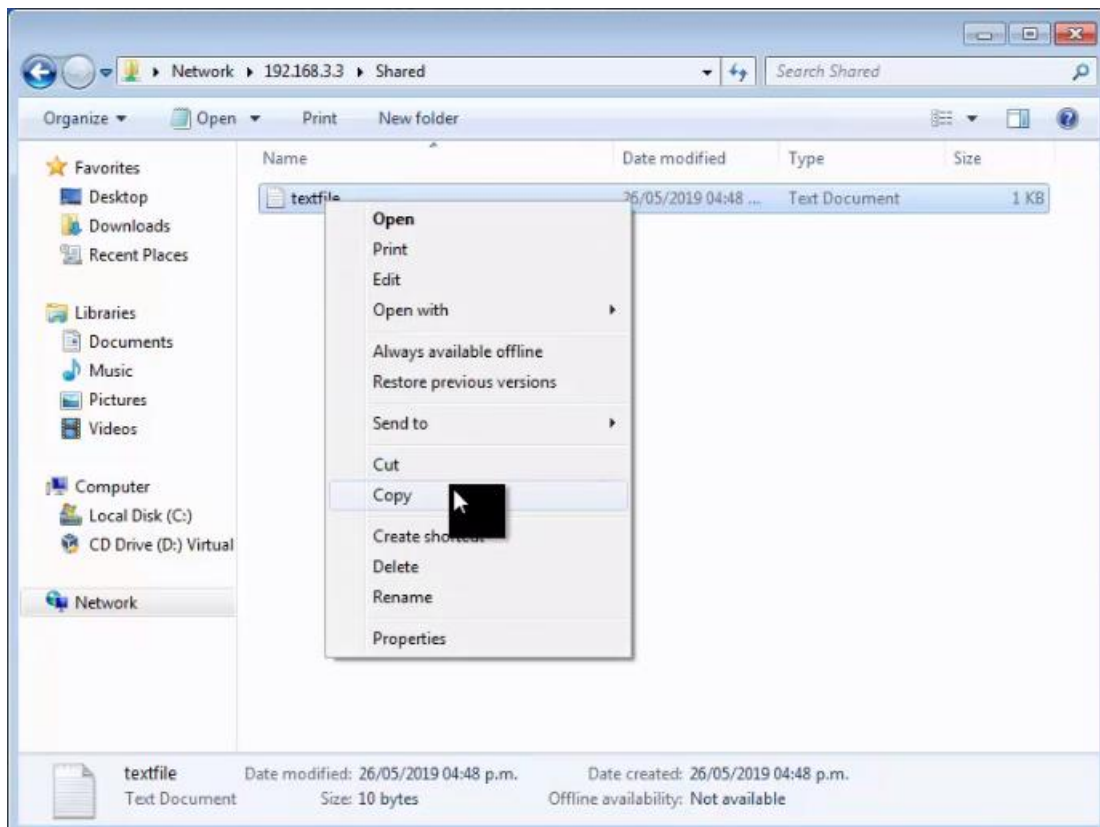


Figura 76: Transferencia del archivo hacia el cliente externo.

Elaboración Propia.

Todo este proceso es capturado por la herramienta Wireshark para su posterior análisis. En la captura de Wireshark se pueden observar protocolos como ICMP, TCP y SMB2. ICMP es el protocolo que produce el ping continuo desde el cliente al destino,

este protocolo funciona en la capa 3 del modelo OSI; TCP es el protocolo de la capa 4 del modelo OSI que permite que los segmentos lleguen al destino de la mejor forma; y SMB2 es el protocolo que se usa para compartir archivos en un entorno de Windows. Note la dirección IP de un cliente 192.168.3.101 y la de destino ubicada en la LAN de R3 (red interna), 192.168.3.3.

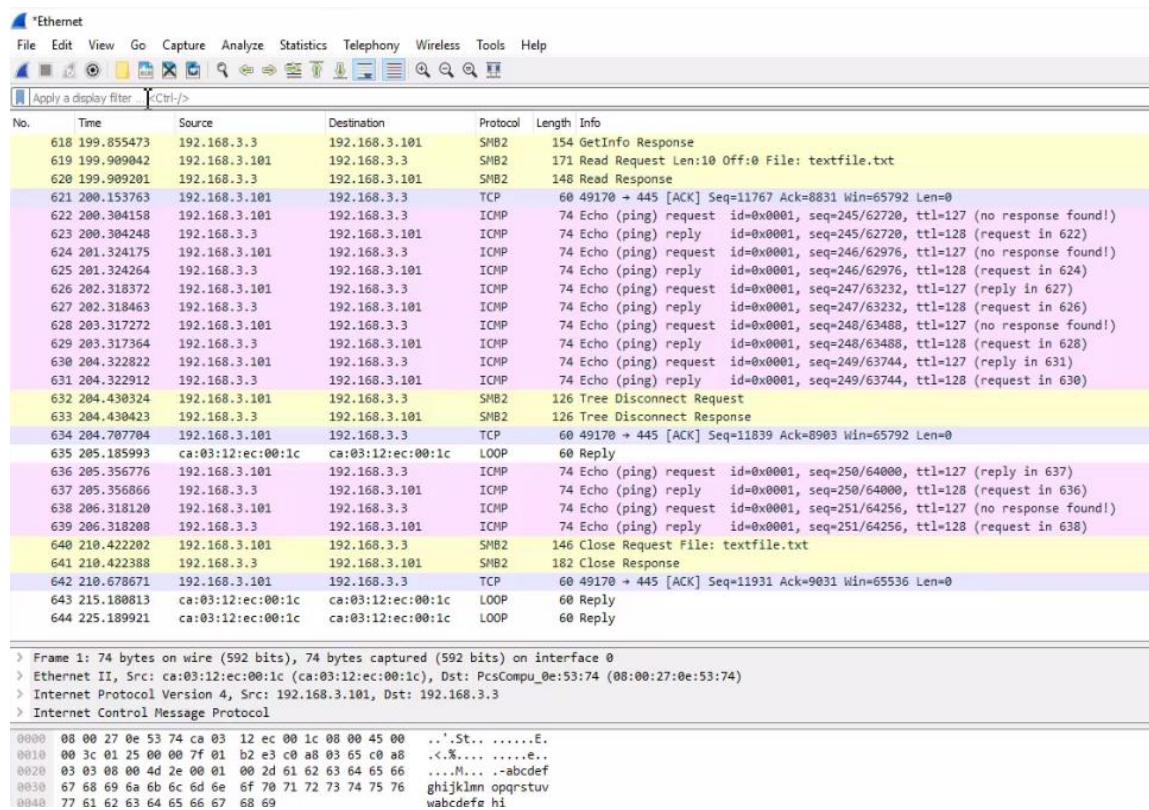


Figura 77: Captura de la transferencia de un archivo con Wireshark.

Elaboración Propia.

La captura 394 muestra ICMP (Internet Control Message Protocol), en capas inferiores se observa la trama Ethernet II con las direcciones MAC de origen y destino, en este caso la dirección MAC de origen es la del cliente y la MAC de destino es de la puerta de enlace (R1). También se observan las direcciones IP de origen (192.168.3.101) y destino (192.168.3.3). Al final en capas superiores se muestra un ICMP tipo 8 (type) que corresponde a una solicitud de tipo eco (ping).



No.	Time	Source	Destination	Protocol	Length	Info
392	170.211428	192.168.3.101	192.168.3.3	ICMP	74	Echo (ping) request id=0x0001,
393	170.211524	192.168.3.3	192.168.3.101	ICMP	74	Echo (ping) reply id=0x0001,
394	171.210331	192.168.3.101	192.168.3.3	ICMP	74	Echo (ping) request id=0x0001,
395	171.210423	192.168.3.3	192.168.3.101	ICMP	74	Echo (ping) reply id=0x0001,
396	172.230522	192.168.3.101	192.168.3.3	ICMP	74	Echo (ping) request id=0x0001,

- > Frame 394: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
- ✓ Ethernet II, Src: ca:03:12:ec:00:1c (ca:03:12:ec:00:1c), Dst: PcsCompu_0e:53:74 (08:00:27:0e:53:74)
 - > Destination: PcsCompu_0e:53:74 (08:00:27:0e:53:74)
 - > Source: ca:03:12:ec:00:1c (ca:03:12:ec:00:1c)
 - Type: IPv4 (0x0800)
- ✓ Internet Protocol Version 4, Src: 192.168.3.101, Dst: 192.168.3.3
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 60
 - Identification: 0x0229 (553)
 - > Flags: 0x0000
 - Time to live: 127
 - Protocol: ICMP (1)
 - Header checksum: 0xb1df [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 192.168.3.101
 - Destination: 192.168.3.3
- ✓ Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0x4c83 [correct]
 - [Checksum Status: Good]
 - Identifier (BE): 1 (0x0001)
 - Identifier (LE): 256 (0x0100)
 - Sequence number (BE): 216 (0x00d8)
 - Sequence number (LE): 55296 (0xd800)
 - [\[Response frame: 395\]](#)
- ✓ Data (32 bytes)
 - Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
 - [Length: 32]

Figura 78: Captura de ICMP.

Elaboración Propia.

Los detalles del Protocolo de Internet versión 4 se muestran en la captura número 402, junto con la dirección de origen del cliente (192.168.3.101), el destino equivalente (192.168.3.3) y otra información. El puerto del cliente (origen) aparece en el Protocolo de control de transmisión como 49166, un puerto dinámico, mientras que el puerto de destino aparece como 445, un puerto conocido que corresponde al servicio SMB. También puede ver el tamaño de la ventana y el número de secuencia.



No.	Time	Source	Destination	Protocol	Length	Info
401	173.454931	192.168.3.3	192.168.3.101	TCP	66	445 → 49166 [SYN, ACK] Seq=0 Ack=1
402	173.508478	192.168.3.101	192.168.3.3	TCP	60	49166 → 445 [ACK] Seq=1 Ack=1 Win=0
403	173.519235	192.168.3.101	192.168.3.3	SMB	213	Negotiate Protocol Request
404	173.526010	192.168.3.3	192.168.3.101	SMB2	463	Negotiate Protocol Response
405	173.572940	192.168.3.101	192.168.3.3	SMB2	162	Negotiate Protocol Request

```

> Frame 402: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: ca:03:12:ec:00:1c (ca:03:12:ec:00:1c), Dst: PcsCompu_0e:53:74 (08:00:27:0e:53:74)
v Internet Protocol Version 4, Src: 192.168.3.101, Dst: 192.168.3.3
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x022d (557)
  > Flags: 0x4000, Don't fragment
    Time to live: 127
    Protocol: TCP (6)
    Header checksum: 0x71ea [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.3.101
    Destination: 192.168.3.3
v Transmission Control Protocol, Src Port: 49166, Dst Port: 445, Seq: 1, Ack: 1, Len: 0
  Source Port: 49166
  Destination Port: 445
  [Stream index: 2]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window size value: 260
    [Calculated window size: 66560]
    [Window size scaling factor: 256]
    Checksum: 0x0a7e [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]

```

Figura 79: Captura de TCP.

Elaboración Propia.

La captura número 620 muestra el servicio de sesión de NetBIOS y el protocolo SMB2 (Server Message Block Protocol Version 2), se muestran algunos detalles como la cabecera (header), la respuesta (Read Response) y los datos (Data) en la capa superior, este campo de datos es el más importante y está mostrado en notación hexadecimal, sin embargo, su representación en ASCII muestra el contenido del archivo “clear text”. Esto es esperado porque entre el cliente y la computadora de destino existe ahora una conexión VPN de acceso remoto, lo que permite que el cliente ingrese de forma virtual a la LAN donde se ubica la computadora de destino, y por eso de forma virtual están en la misma LAN y la transferencia de archivos se realiza con esa naturaleza. El cifrado de datos está establecido entre el cliente VPN y el servidor VPN (R3), donde se configuró un túnel

usando IPsec, pero una vez que el cliente hace uso del túnel, actúa como si estuviera en la misma LAN que el destino.

No.	Time	Source	Destination	Protocol	Length	Info
619	199.909042	192.168.3.101	192.168.3.3	SMB2	171	Read Request Len:10 Off:0
620	199.909201	192.168.3.3	192.168.3.101	SMB2	148	Read Response
621	200.153763	192.168.3.101	192.168.3.3	TCP	60	49170 → 445 [ACK] Seq=1176
622	200.304158	192.168.3.101	192.168.3.3	ICMP	74	Echo (ping) request id=0

> Transmission Control Protocol, Src Port: 445, Dst Port: 49170, Seq: 8737, Ack: 11767, Len: 94
✓ NetBIOS Session Service
Message Type: Session message (0x00)
Length: 90
✓ SMB2 (Server Message Block Protocol version 2)
✓ SMB2 Header
Server Component: SMB2
Header Length: 64
Credit Charge: 1
NT Status: STATUS_SUCCESS (0x00000000)
Command: Read (8)
Credits granted: 1
> Flags: 0x00000001, Response
Chain Offset: 0x00000000
Message ID: Unknown (53)
Process ID: 0x0000feff
> Tree Id: 0x00000005 \\192.168.3.3\Shared
> Session Id: 0x000064000000001d Acct:cromero Domain:WIN7-VIRTBOX-1 Host:WIN7-VIRTBOX-1
Signature: 00000000000000000000000000000000
[Response to: 619]
[Time from request: 0.000159000 seconds]
✓ Read Response (0x08)
> StructureSize: 0x0011
Data Offset: 0x0050
Read Length: 10
Read Remaining: 0
Reserved: 00000000
✓ Data (10 bytes)
Data: 636c6561722074657874
[Length: 10]

0040	01 00 00 00 00 00 08 00	01 00 01 00 00 00 00 00
0050	00 00 35 00 00 00 00 00	00 00 ff fe 00 00 05 00	..5.....
0060	00 00 1d 00 00 00 64 00	00 00 00 00 00 00 00 00d.....
0070	00 00 00 00 00 00 00 00	00 00 11 00 50 00 0a 00P...
0080	00 00 00 00 00 00 00 00	00 00 63 6c 65 61 72 20clear
0090	74 65 78 74		text

Figura 80: Captura de SMB2.

Elaboración Propia.

4.2. DISCUSIÓN

Los datos proporcionados ofrecen una mirada intrigante a cómo se utilizan las redes privadas virtuales (VPN) y las tecnologías IPsec en diversas situaciones y aplicaciones. A partir de los antecedentes y conclusiones proporcionados en una sección previa en esta investigación, se pueden destacar varios puntos clave: Seguridad y Escalabilidad en Redes VPLS: Uno de los temas recurrentes en los antecedentes es la



importancia de garantizar la seguridad y escalabilidad en las redes VPLS. Se mencionan enfoques como el uso de Protocolo de identidad de host (HIP), etiquetas cifradas y protocolos de árbol de expansión (DSTP) para abordar estos desafíos. Estos enfoques son esenciales en un entorno empresarial donde la confiabilidad y la seguridad son fundamentales. Implementación de IPSec en SDN y P4: Un campo de estudio importante es la aplicación de IPSec en la programación P4 y redes definidas por software (SDN). Se proporciona un método más adaptable y dinámico para crear VPN implementando IPSec en conmutadores P4 y administrándolo mediante controladores SDN. Esto puede simplificar la seguridad y la administración de la red. Evaluación de protocolos de seguridad Se enfatiza lo crucial que es evaluar y confirmar cómo se utilizan los protocolos de seguridad como IPSec. Esto es esencial para garantizar que los protocolos cumplan con los criterios de seguridad y rendimiento requeridos. Es una buena idea utilizar los métodos sugeridos para evaluar el cumplimiento y el rendimiento de IPSec. Conexiones VPN utilizadas para empresas: el uso de VPN basadas en IPSec se sugiere como una solución segura y asequible para conectar sucursales de empresas en muchos de sus predecesores. Esta es una opción sensata que puede ahorrar gastos a las empresas manteniendo la seguridad de las comunicaciones. Simulaciones y pruebas: Se enfatiza el valor de las pruebas y simulaciones en la instalación y evaluación de soluciones de red. Es más sencillo comprender el rendimiento y la seguridad de las soluciones sugeridas cuando se utilizan herramientas como Wireshark y simuladores de red (como GNS3).



V. CONCLUSIONES

La red institucional de la Universidad Nacional del Altiplano ha sido diseñada e implementada exitosamente como una red privada virtual utilizando IPSec, se realizaron las pruebas de conectividad y las pruebas de gestión son satisfactorias; también se hicieron capturas de paquetes con Wireshark para mostrar la seguridad que provee IPSec, entre las cuales incluye la integridad de datos, cifrado de datos (encriptación), autenticidad y disponibilidad. También a esto se ha considerado para el diseño, la escalabilidad de la red.

En el centro de datos de la infraestructura de tecnologías de la información de la Universidad Nacional del Altiplano se han desarrollado servicios de red para la gestión y configuración de dispositivos y servidores de red. Esto ha hecho posible que un administrador externo y remoto funcione virtualmente dentro de la red institucional a través de una red privada virtual.

Se implementó una red privada virtual usando IPSec sobre una simulación y emulación de Internet y la red institucional, la emulación se logró ejecutando el sistema operativo real de Cisco denominado IOS (Internetwork Operating System) en GNS3. De esta forma varios IOS fueron emulados en GNS3 para establecer la red con los distintos dispositivos que conformarían una red privada, la red institucional, y una red pública, Internet.



VI. RECOMENDACIONES

Es posible diseñar e implementar otros tipos de redes privadas virtuales mencionadas en el marco teórico, las pruebas de conectividad y las pruebas de gestión también se podrían emular y simular en GNS3 y otros emuladores como EVE-NG o VIRL PE; es posible hacer capturas de paquetes con Wireshark u otro sniffer. De esta forma también se podría mostrar la seguridad, que incluye la integridad, el cifrado, autenticidad y disponibilidad.

Conforme ha ido avanzando la investigación, ha quedado claro que no existe ningún dispositivo de este nivel para ataques informáticos, por lo que es posible añadir un firewall ASA (Adaptive Security Appliance) para garantizar la prevención y actuación ante ataques a la red interna del institucional. red.

Se pueden utilizar sistemas operativos basados en UNIX como GNU/Linux y FreeBSD para construir una red privada virtual. La metodología de diseño, pruebas y resultados puede diferir de la metodología de esta investigación, pero el proceso de diseño, pruebas y resultados es el mismo.



VII. REFERENCIAS BIBLIOGRÁFICAS

- Andrés Roig, A. (2017). DISEÑO DE REDES PRIVADAS VIRTUALES CON ROUTERS CISCO. Valencia, España: Universidad Politecnica de Valencia .
- Aparicio-Izurieta, V. V. (2022). Segurança IP segura na Internet (IPSEC). Universidad Técnica Luis Vargas Torres de Esmeraldas, Ecuador.: <https://doi.org/10.51798/sijis.v3i1.278>.
- Ardila Castillo, N. (2019). Seguridad en las VPN'S. Especialización en Seguridad Informática [736]: <http://repository.unipiloto.edu.co/handle/20.500.12277/6435>.
- Atencio Mendoza, A., & Mamani Figueroa , E. (Agosto de 2017). DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO DE RED PRIVADA VIRTUAL EN CAPA 3 UTILIZANDO CISCO IOS PARA LA UNIVERSIDAD NACIONAL DEL ALTIPLANO". Puno, Puno, Perú: Universidad Nacional del Altiplano.
- Berrio Rufino, K. (2021). Diseño físico y lógico de la infraestructura de red para mejorar los servicios de comunicación en la Municipalidad Distrital de Amarilis, Huánuco – 2019. San Salvador, El Salvador, Centroamérica: Repositorio Institucional UNHEVAL. doi:<https://hdl.handle.net/20.500.13080/6253>
- Biga, D. R., Dufour, F. J., Serra, A., & Peliza, C. (2020). VPNs (Virtual Private Networks). Repositorio Digital UNLaM. doi:<http://repositoriocyt.unlam.edu.ar/handle/123456789/430>
- Bonastre Pina, A. M. (2019). Diseño e implementación de una red inalámbrica de sensores para la detección precoz de incendios forestales. United States: Universitat Politècnica de València. doi:<https://riunet.upv.es/handle/10251/128022>
- Carrasco Díaz, S. (2019). Metodología de la Investigación Científica. Pautas metodológicas para diseñar y elaborar el proyecto de investigación. Lima: Editorial San Marcos.



- Castro Serantes, B. (2021). Estudio e implementación de tecnologías overlay en redes definidas por software SDN. Universitat Oberta de Catalunya (UOC). doi:<http://hdl.handle.net/10609/147211>
- Cobos Briones, Y. A. (2021). Diseño e Implementación de una Red Virtual basada en Docker en un ambiente de redes definidas por Software (SDN). Utilizando ZeroTier y Raspberry Pi. Repositorio Institucional de la Universidad Politécnica Salesiana. doi:<http://dspace.ups.edu.ec/handle/123456789/21982>
- Cueva Osorio, J. D., & Falla Mejía, E. J. (2020). Propuesta de implementación de una red privada virtual de acceso remoto (VPN) para el servicio y acceso de los trabajadores a distancia de Mi Banco – Banco de la microempresa S.A. Universidad Nacional Pedro Ruiz Gallo: <https://hdl.handle.net/20.500.12893/10184>.
- Duran Pamplona, J. (2020). Principales características, modos de perpetración y vulneración de la seguridad informática a través de la modalidad carding. Universidad Nacional Abierta y a Distancia UNAD. doi:<https://repository.unad.edu.co/handle/10596/34366>
- Franklin Jhimmy, T. A., Kirenia, M. Z., María Magdalena, T. Z., & José Efraín, Á. C. (2021). Impacto del intranet y extranet en el desarrollo empresarial. Universidad de la Rioja: <https://dialnet.unirioja.es/servlet/articulo?codigo=8590642>.
- Galarza Mena, R. A., & Jaya Condorcana, C. M. (2020). Migración de datos de IPV4 a IPV6 a través del metodo de tunnel de broker en la empresa G&S Ingenieros. CÍA LTDA. Ecuador: Latacunga: Universidad Técnica de Cotopaxi (UTC):. <http://repositorio.utc.edu.ec/handle/27000/8619>.
- Gladys Patricia, G. A., Alexis Eduardo, V. A., Cristhian Salomón, G. A., & Eduardo Enrique, G. S. (2019). Las Tecnologías de la Información y la Comunicación en la educación universitaria. España: Editorial Saberes del Conocimiento. doi:[https://doi.org/10.26820/reciamuc/3.\(3\).julio.2019.409-422](https://doi.org/10.26820/reciamuc/3.(3).julio.2019.409-422)
- González Inostroza, C. M. (2021). Plataforma de análisis de calidad de servicio en redes WiFi. Universidad de Chile: <https://repositorio.uchile.cl/handle/2250/180525>.
- Iturralde Piedra, D. E., & Serrano Vazquez, L. M. (2020). Guía de buenas prácticas de seguridad en redes para la configuración de dispositivos de capa 2 y 3 del modelo



- OSI y validación en una red de prueba. Universidad del Azuay:
<http://dspace.uazuay.edu.ec/handle/datos/9779>.
- Iza Ninasunta, M. M., & Vera Zambrano, C. S. (2020). Implementación de la Red Privada Virtual VPN en la Universidad Técnica de Cotopaxi – Extensión La Maná. Universidad Técnica de Cotopaxi (UTC):
<http://repositorio.utc.edu.ec/handle/27000/6889>.
- Lema Balladares, Á. M. (2021). Diseño y emulación de una red de datos para integración de intranet y Voip para la dirección distrital de educación de Santo Domingo de los Tsáchilas en la zona urbana. Pontificia Universidad del Ecuador:
<http://repositorio.puce.edu.ec/handle/22000/18888>.
- Liyakkathali, S., Furtado, F., Sugumar, G., & Mathur, A. (2022). A Mechanism to Assess the Effectiveness Anomaly Detectors in Industrial Control Systems. Singapore University of Technology and Design, Singapore.
- López Manjarres, J. F. (2019). Configuración e implementación del Zentyal server 6.0 como una Virtual Private Network (VPN). Universidad Nacional Abierta y a Distancia UNAD. doi:<https://repository.unad.edu.co/handle/10596/31954>
- Montaleza Paucar, P. A., & Jativa Reyes, A. P. (2022). Diseño de la transición del protocolo Ipv4 hacia Ipv6 en la empresa grupo Játiva con base en consideraciones de seguridad en implementación de Ipv6. Universidad Técnica de Cotopaxi (UTC): <http://repositorio.utc.edu.ec/handle/27000/9174>.
- Naik, N., Shang, C., Shen, Q., & Jenkins, P. (2019). D-FRI-CiscoFirewall: Dynamic Fuzzy Rule Interpolation for Cisco ASA Firewall. New Orleans, LA, USA: 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE).
- Paramo Melo, R. A. (2020). Protocolo de seguridad orientado a IPv6 - IPsec. Universidad Nacional Abierta y a Distancia UNAD :
<https://repository.unad.edu.co/handle/10596/38529>.
- Quishpe Iza, L. M. (2021). Estudio para la implementación de una red privada virtual(VPN) utilizando herramientas de software libre. Caso de estudio “Comisión Fulbright del Ecuador”. Universidad Católica del Ecuador:
<http://repositorio.puce.edu.ec/handle/22000/18899>.



- Rivera Morla, L. A. (2022). Red Privada Remota Montada En Raspberry Pi Para La Gestión Segura De Los Recursos Informáticos Entre Las Oficinas De Builderecuador Cia.Ltda. Repositorio Digital Universidad Ecotec. doi:<https://repositorio.ecotec.edu.ec/handle/123456789/497>
- Rojas Celis, J. D., Hoyos Rodríguez, R. D., & Castro Reyes, N. A. (2020). Propuesta de diseño de una VPN de acceso remoto con túneles GRE para permitir plan de continuidad tic para las Mipymes del sector económico terciario, en empresas dedicadas al comercio de equipos partes y piezas electrónicas en Bogotá D.C. Universidad Cooperativa de Colombia: <https://repository.ucc.edu.co/bitstreams/594cbb84-6d9c-422f-9b8a-5059cf7cd10a/download>.
- Rubio, J. (2021). 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. Ecuador: Latacunga: Universidad Técnica de Cotopaxi: UTC. doi:<http://repositorio.utc.edu.ec/handle/27000/7770>
- Hernández Sampieri, R., & Mendoza, C. (2020). METODOLOGÍA INVESTIGACIÓN LAS RUTAS CUANTITATIVA, CUALITATIVA Y MIXTA 6TA EDICIÓN. McGraw-Hill Interamericana de España.
- Vacas Andrade, C. A. (2019). Diseño e implementación de un agente de administración, configuración y monitoreo para dispositivos de red Cisco. Banfield - Lomas de Zamora: Quito: Universidad de las Américas, 2019. doi:<http://dspace.udla.edu.ec/handle/33000/11555>
- Vinicio, M. G. (Mayo de 2021). Análisis de los parámetros de diseño para una red de datos con aplicaciones para. Pachuca, Hidalgo, Mexico: UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL). doi: <http://repositorio.uisrael.edu.ec/bitstream/47000/2843/1/UISRAEL-EC-MASTER-TELECOMUNICACIONES%20-378.242-2021-005.pdf>



DECLARACIÓN JURADA DE AUTENTICIDAD DE TESIS

Por el presente documento, Yo Hugo Darío AQUINO ARCATA,
identificado con DNI 47359177 en mi condición de egresado de:

Escuela Profesional, Programa de Segunda Especialidad, Programa de Maestría o Doctorado
INGENIERIA ELECTRONICA

informo que he elaborado el/la Tesis o Trabajo de Investigación denominada:

“DISEÑO E IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL USANDO IPSEC PARA ADMINISTRAR REMOTAMENTE LA RED INSTITUCIONAL DE LA UNIVERSIDAD NACIONAL DEL ALTIPLANO”

Es un tema original.

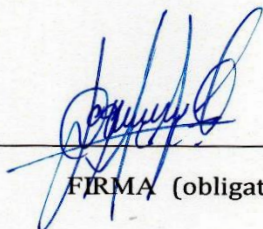
Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como tuyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

En caso de incumplimiento de esta declaración, me someto a las disposiciones legales vigentes y a las sanciones correspondientes de igual forma me someto a las sanciones establecidas en las Directivas y otras normas internas, así como las que me alcancen del Código Civil y Normas Legales conexas por el incumplimiento del presente compromiso

Puno, 12 De Setiembre del 2023


FIRMA (obligatoria)



Huella



AUTORIZACIÓN PARA EL DEPÓSITO DE TESIS O TRABAJO DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL

Por el presente documento, Yo Hugo Darío AQUINO ARCATA,
identificado con DNI 47359177 en mi condición de egresado de:

Escuela Profesional, Programa de Segunda Especialidad, Programa de Maestría o Doctorado

INGENIERIA ELECTRONICA

informo que he elaborado el/la Tesis o Trabajo de Investigación denominada:

“DISEÑO E IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL USANDO IPSEC PARA ADMINISTRAR REMOTAMENTE LA RED INSTITUCIONAL DE LA UNIVERSIDAD NACIONAL DEL ALTIPLANO”

para la obtención de Grado, Título Profesional o Segunda Especialidad.

Por medio del presente documento, afirmo y garantizo ser el legítimo, único y exclusivo titular de todos los derechos de propiedad intelectual sobre los documentos arriba mencionados, las obras, los contenidos, los productos y/o las creaciones en general (en adelante, los “Contenidos”) que serán incluidos en el repositorio institucional de la Universidad Nacional del Altiplano de Puno.

También, doy seguridad de que los contenidos entregados se encuentran libres de toda contraseña, restricción o medida tecnológica de protección, con la finalidad de permitir que se puedan leer, descargar, reproducir, distribuir, imprimir, buscar y enlazar los textos completos, sin limitación alguna.

Autorizo a la Universidad Nacional del Altiplano de Puno a publicar los Contenidos en el Repositorio Institucional y, en consecuencia, en el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, sobre la base de lo establecido en la Ley N° 30035, sus normas reglamentarias, modificatorias, sustitutorias y conexas, y de acuerdo con las políticas de acceso abierto que la Universidad aplique en relación con sus Repositorios Institucionales. Autorizo expresamente toda consulta y uso de los Contenidos, por parte de cualquier persona, por el tiempo de duración de los derechos patrimoniales de autor y derechos conexos, a título gratuito y a nivel mundial.

En consecuencia, la Universidad tendrá la posibilidad de divulgar y difundir los Contenidos, de manera total o parcial, sin limitación alguna y sin derecho a pago de contraprestación, remuneración ni regalía alguna a favor mío; en los medios, canales y plataformas que la Universidad y/o el Estado de la República del Perú determinen, a nivel mundial, sin restricción geográfica alguna y de manera indefinida, pudiendo crear y/o extraer los metadatos sobre los Contenidos, e incluir los Contenidos en los índices y buscadores que estimen necesarios para promover su difusión.

Autorizo que los Contenidos sean puestos a disposición del público a través de la siguiente licencia: Creative

Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional. Para ver una copia de esta licencia, visita: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

En señal de conformidad, suscribo el presente documento.

Puno, 12 De Setiembre del 2023

FIRMA (obligatoria)



Huella