UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN
RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

TEMA:

ANÁLISIS DE LOS TIPOS DE VPN PARA LA TRANSMISIÓN SEGURA DE DATOS SENSIBLES EN INTERNET

AUTOR:

LEONARDO ESNEIDER IPARREÑO SANTAMARIA

DIRECTOR:

JUAN DIEGO JARA SALTOS

CUENCA – ECUADOR
2025

Autor:

Leonardo Esneider Iparreño Santamaria
Ingeniero en Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
liparreno@est.ups.edu.ec

Dirigido por:

Juan Diego Jara Saltos
Magister en Telemática.
Máster en Métodos Matemáticos y Simulación Numérica.
jjaras@ups.edu.ec

LEONARDO ESNEIDER IPARREÑO SANTAMARIA
Análisis de los tipos de VPN para la transmisión segura de datos sensibles en internet

DEDICATORIA

A **Dios**, por ser mi guía y fortaleza en todo momento, brindándome la luz necesaria para alcanzar este importante logro.

A mis **padres**, quienes con amor, sacrificio y sabios consejos me han apoyado incondicionalmente. Este triunfo es también suyo, fruto de sus enseñanzas y ejemplo de vida.

A mi **familia**, por su constante apoyo, paciencia y fe en mí, especialmente en los momentos más desafiantes. Gracias por ser mi refugio y mi mayor motivación para seguir adelante.

A los ingenieros, Ana Santamaria (Madre), Lindthon Iparreño Z. (Padre). y Lindhton Iparreño S. (Hermano) por su comprensión, aliento y amor incondicional. Su presencia en mi vida ha sido un pilar fundamental para superar cada obstáculo y alcanzar esta meta.

Dedico este trabajo a todos aquellos que sueñan en grande y trabajan arduamente para alcanzar sus metas, con la esperanza de que este logro sea una inspiración para nunca rendirse.

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a **Dios**, por darme la fortaleza y la claridad necesarias para concluir este proyecto.

A mis **padres y familia**, por su apoyo incondicional, amor y fe en mí a lo largo de este camino. Su confianza y sacrificios han sido la base de mi esfuerzo y dedicación.

A mi **asesor de tesis**, Ingeniero Juan Jara, por su guía, paciencia y orientación durante todo este proceso. Su experiencia y compromiso fueron clave para la realización de este trabajo.

A la **universidad Politécnica Salesiana**, por brindarme las herramientas y el espacio para desarrollar mi potencial, y a los **profesores**, por compartir su conocimiento y motivarme a dar siempre lo mejor de mí.

A mis **compañeros y amigos**, por los momentos compartidos, el apoyo mutuo y las experiencias vividas que enriquecieron mi formación.

Finalmente, agradezco a todas aquellas personas que de alguna manera contribuyeron al desarrollo de este proyecto, directa o indirectamente. A todos ustedes, mi más profundo reconocimiento y gratitud.

Ing. Leonardo Iparreño

Tabla de Contenido

Índice de Tablas

Índice de imágenes

Análisis de los tipos de VPN para la transmisión segura de datos sensibles en Internet

Autor(es):

LEONARDO ESNEIDER IPARREÑO SANTAMARIA

Resumen

Según el Estudio de Uso, Adopción y Compras de Consumidores de VPN de security.org, el 85% de los usuarios de Internet mayores de 18 años saben lo que es una VPN. Esto implica un incremento del 13% en comparación con el año 2020.

ARPANET es responsable del desarrollo del Protocolo de Control de Transferencia/Protocolo Internet (TCP/IP) El protocolo TCP/IP posibilitó la conexión de dispositivos y redes locales a través de una red compartida. Esto introdujo un riesgo de ciberseguridad, ya que una persona ajena podía utilizar la red para acceder a los dispositivos de su interior.

Este proyecto de titulación se propone realizar un análisis integral de los diversos tipos de Redes Privadas Virtuales (VPN) con el objetivo de evaluar su eficacia en la transmisión segura de datos sensibles en el entorno de Internet. La investigación se enfocará en la aplicación práctica de diferentes tipos de VPN, desde las implementaciones de capa 3 hasta soluciones más especializadas. A través de este análisis, se buscará identificar las características clave de cada tipo de VPN y su idoneidad para proteger la privacidad y la integridad de datos sensibles.

El proyecto también incluirá un componente de desarrollo, donde se explorarán posibles mejoras o adaptaciones de las VPN existentes para abordar desafíos específicos relacionados con la seguridad de la transmisión de datos en entornos en constante evolución. Se espera que los resultados de esta investigación y desarrollo proporcionen a las organizaciones y usuarios una guía práctica para seleccionar e implementar soluciones de VPN que se ajusten de manera óptima a sus necesidades de seguridad en la era digital.

Palabras clave:

VPN, TCP/IP, IpSec, Túnel GRE

Abstract

According to security.org's VPN Consumer Usage, Adoption and Purchase Study, 85% of Internet users over the age of eighteen know what a VPN is. This represents an increase of 13% compared to 2020.

ARPANET prompted the creation of the Transfer Control Protocol/Internet Protocol (TCP/IP). TCP/IP allowed devices and local networks to connect over a shared network. This introduced a cybersecurity risk since an outsider could use the network to access the devices inside.

This degree project aims to carry out a comprehensive analysis of the several types of Virtual Private Networks (VPN) with the aim of evaluating their effectiveness in the secure transmission of sensitive data in the Internet environment. The research will focus on the practical application of different types of VPNs, from layer 3 implementations to more specialized solutions. Through this analysis, we will seek to identify the key characteristics of each type of VPN and their suitability to protect the privacy and integrity of sensitive data.

The project will also include a development component, where potential improvements or adaptations to existing VPNs will be explored to address specific challenges related to the security of data transmission in constantly evolving environments. The results of this research and development are expected to provide organizations and users with practical guidance in selecting and implementing VPN solutions that optimally fit their security needs in the digital age.

Keywords:
VPN, TCP/IP, IPSec, Tunnel GRE

1. Introducción

La creciente dependencia de las organizaciones y usuarios individuales en la transmisión de datos sensibles a través de Internet ha destacado la importancia de salvaguardar la privacidad y la seguridad de la información. En este contexto, las Redes Privadas Virtuales (VPN) han surgido como una herramienta fundamental para garantizar la confidencialidad y la integridad de la comunicación en línea. Este artículo se adentrará en el fascinante mundo de las VPN, centrándose en el análisis detallado de los diferentes tipos de VPN disponibles para la transmisión segura de datos sensibles. Desde las VPN de capa 3 que operan a nivel de red hasta otros enfoques especializados, exploraremos cómo estas tecnologías contribuyen a la protección de la información crítica en un entorno cada vez más digital y conectado. Sumérjase con nosotros en esta exploración para comprender mejor cómo elegir la VPN adecuada puede ser crucial para salvaguardar la confidencialidad de los datos en el vasto paisaje de Internet.

Una red Wi-Fi es una red de telecomunicaciones que utiliza el estándar IEEE 802.11 para conectar dispositivos en ella. Estos dispositivos se comunican entre sí mediante señales de radiofrecuencia que pueden oscilar entre 2,4 GHz o 5 GHz. También cumplen con los protocolos definidos en el estándar IEEE 802.11 para garantizar la comunicación entre todos los dispositivos de la red.

La seguridad de la red Wi-Fi se refiere a todos los mecanismos utilizados para proteger los datos compartidos en la red y respetar los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. Es importante recordar que en el modelo OSI, cuando existe un medio no guiado como las ondas de RF, las redes Wi-Fi utilizan ondas de RF en la capa física para transmitir datos diferentes del medio controlado. Los objetos que emiten señales pueden oírse e incluso interpretarse si no se toman las medidas de seguridad adecuadas.

Muchos incidentes de seguridad suelen producirse en habitaciones donde se comparten redes Wi-Fi gratuitas. Los atacantes se aprovechan de la ignorancia de la víctima y de cualquier brecha en la red para obtener información privada y así beneficiarse a expensas de la víctima. Para solucionar este problema, se realizaron muchos parches y actualizaciones para hacer más seguras las redes Wi-Fi, como el estándar Wired Equivalent Privacy (WEP), pero al final no proporcionó suficiente protección a los usuarios y tuvo que ser abandonado. Los estándares WPA (Wi-Fi Protected Access), como WEP, ahora están obsoletos, pero en su momento brindaron protección y confianza a los usuarios y sentaron las bases para estándares más sofisticados, con menos vulnerabilidades y más efectivos. (Hadi, 2022)

Dado el rápido desarrollo de la tecnología, incluidas las comunicaciones inalámbricas y las redes Wi-Fi en particular, el usuario promedio a menudo desconoce todos los avances actuales y no comprende las vulnerabilidades y los riesgos asociados con el acceso a esta tecnología. Las organizaciones encargadas de hacer cumplir la ley están a la vanguardia de estos problemas y trabajan todos los días para mitigar este grave problema, pero, de todos modos, el nivel de seguridad dependerá de la conciencia de los usuarios sobre los riesgos que los rodean. Por ello, este documento resume las principales vulnerabilidades a las que se enfrentan los usuarios al conectarse a redes Wi-Fi y las simula en un entorno controlado para crear guías de soporte para que todos los interesados puedan avanzar y estar preparados con confianza. Traduce todo tipo de ataques a la red Wi-Fi. redes.

La investigación se realizó de manera documentada y experimental, basándose en casos reportados y documentados, así como en documentos oficiales del IEEE sobre el desarrollo del estándar 802.11. Primero, se proporciona una breve descripción de la tecnología y su evolución, seguido de una definición de los estándares de seguridad establecidos, actuales y obsoletos, y luego una definición de las principales vulnerabilidades de las redes Wi-Fi. Estas técnicas se utilizaron y se siguen utilizando para la explotación, las vulnerabilidades se siguen reproduciendo en laboratorios controlados y, finalmente, se implementan mecanismos de

seguridad para evitar ser víctimas de estas vulnerabilidades y se recomienda a los usuarios que se protejan contra cualquier ataque.

El desarrollo y la evolución de los protocolos de seguridad y cifrado, como IPsec, SSL/TLS, PPTP (motivos históricos o para contrastarlo con alternativas modernas) y L2TP, impulsaron el crecimiento de diferentes tipos de VPN que ofrecían soluciones para diferentes necesidades y requisitos de seguridad. Cada tipo de VPN se diseñó para abordar escenarios específicos, como el acceso remoto seguro, la interconexión de redes geográficamente dispersas y la protección de aplicaciones web.

A medida que aumentaba la conciencia sobre la importancia de la seguridad de los datos y las amenazas cibernéticas se volvían más sofisticadas, la adopción de VPN se hizo más generalizada tanto en el ámbito empresarial como en el uso personal. Las VPN se convirtieron en una herramienta esencial para proteger la información confidencial, salvaguardar la privacidad de los usuarios y garantizar la seguridad en la comunicación en línea.

A lo largo del tiempo, el análisis de los tipos de VPN ha ido evolucionando para evaluar y comparar las ventajas y desventajas de cada enfoque. Los avances tecnológicos han permitido una mayor eficiencia y seguridad en la transmisión de datos sensibles a través de VPN, y la investigación y el desarrollo continúan para abordar nuevos desafíos que surgen en el ámbito de la ciberseguridad.

no de los problemas científicos relacionados con el análisis de los tipos de VPN para la transmisión segura de datos sensibles en Internet es la evaluación de la efectividad y seguridad de los diferentes protocolos y tecnologías utilizadas en las VPN. Esto implica identificar las causas y efectos de posibles vulnerabilidades o debilidades en los distintos tipos de VPN y cómo estas pueden afectar la seguridad de la transmisión de datos.

2. Determinación del Problema

El aumento exponencial de la digitalización ha llevado a una dependencia crítica de la transmisión de datos sensibles a través de Internet en entornos empresariales y personales. A pesar de los beneficios asociados con esta práctica, la seguridad de dicha transmisión se ve amenazada por diversos riesgos, destacando la necesidad de una evaluación integral de los diferentes tipos de Redes Privadas Virtuales (VPN) disponibles.

La transmisión segura de datos sensibles en Internet se enfrenta a desafíos significativos debido a la diversidad de tipos de VPN disponibles, lo que plantea la pregunta esencial: ¿Cuál es la efectividad y seguridad de cada tipo de VPN en la protección de datos sensibles durante su transmisión?

La falta de claridad sobre la elección óptima de una VPN para la transmisión segura de datos sensibles puede resultar en vulnerabilidades, intercepciones no autorizadas y compromisos de la confidencialidad. Este problema no solo afecta a usuarios individuales, sino que también representa un riesgo significativo para la seguridad de datos críticos en entornos corporativo.

La realización de un análisis profundo de los tipos de VPN y su aplicación en la transmisión de datos sensibles es esencial para proporcionar orientación práctica a usuarios y organizaciones. Este proyecto de titulación busca abordar esta problemática mediante la investigación aplicada y el desarrollo de recomendaciones fundamentadas para la elección de VPN que mejor se adapten a las necesidades de seguridad en la transmisión de datos sensibles en Internet.

2.1 Antecedentes.

En la década de 1990, el concepto de VPN comenzó a tomar forma con la introducción de túneles de encriptación que permitían a los usuarios conectarse de forma segura a redes privadas a través de Internet. Esto marcó un hito significativo en la seguridad de las comunicaciones en línea.

El desarrollo y la evolución de los protocolos de seguridad y cifrado, como IPsec, SSL/TLS, PPTP y L2TP, impulsaron el crecimiento de diferentes tipos de VPN que ofrecían soluciones para diferentes necesidades y requisitos de seguridad. Cada tipo de VPN se diseñó para abordar escenarios específicos, como el acceso remoto seguro, la interconexión de redes geográficamente dispersas y la protección de aplicaciones web.

A medida que aumentaba la conciencia sobre la importancia de la seguridad de los datos y las amenazas cibernéticas se volvían más sofisticadas, la adopción de VPN se hizo más generalizada tanto en el ámbito empresarial como en el uso personal. Las VPN se convirtieron en una herramienta esencial para proteger la información confidencial, salvaguardar la privacidad de los usuarios y garantizar la seguridad en la comunicación en línea.

A lo largo del tiempo, el análisis de los tipos de VPN ha ido evolucionando para evaluar y comparar las ventajas y desventajas de cada enfoque. Los avances tecnológicos han permitido una mayor eficiencia y seguridad en la transmisión de datos sensibles a través de VPN, y la investigación y el desarrollo continúan para abordar nuevos desafíos que surgen en el ámbito de la ciberseguridad no de los problemas científicos relacionados con el análisis de los tipos de VPN para la transmisión segura de datos sensibles en Internet es la evaluación de la efectividad y seguridad de los diferentes protocolos y tecnologías utilizadas en las VPN. Esto implica identificar las causas y efectos de posibles vulnerabilidades o debilidades en los distintos tipos de VPN y cómo estas pueden afectar la seguridad de la transmisión de datos.

2.2 Formulación del Problema

La incorrecta configuración o implementación de un protocolo VPN podría conducir a vulnerabilidades de seguridad. Esto puede incluir la elección de algoritmos de cifrado débiles, el uso de contraseñas inseguras o la falta de autenticación adecuada. Así también los errores de programación en el software cliente o servidor utilizado para establecer la VPN pueden generar una problemática, generando vulnerabilidades que podrían ser explotadas por atacantes para acceder a datos sensibles.

La implementación de algunos protocolos VPN mal seleccionados pueden generar fallas de diseño que podrían exponer datos sensibles a ataques. Por ejemplo, algunos protocolos pueden tener problemas de escalabilidad o no proporcionar suficiente protección contra ciertos tipos de ataques, generando adicionalmente problemas de interoperabilidad en entornos donde se utilizan diferentes soluciones de VPN, los cual podría resultar en problemas de interoperabilidad que afecten la seguridad de la transmisión de datos dentro de una red empresarial

2.3 Justificación del problema

La justificación del análisis de los tipos de VPN para la transmisión segura de datos sensibles en Internet es crucial debido a los siguientes motivos:

2.3.1 Protección de datos sensibles:

En la era digital actual, las organizaciones y los individuos manejan y transmiten una gran cantidad de datos sensibles y confidenciales. El análisis de los tipos de VPN ayuda a identificar las opciones más seguras y adecuadas para proteger estos datos durante su transmisión a través de redes públicas como Internet.

2.3.2 Aumento de amenazas cibernéticas:

La ciberdelincuencia y las amenazas a la seguridad informática están en constante evolución y se han vuelto más sofisticadas. Un análisis exhaustivo de las tecnologías de VPN garantiza que las soluciones implementadas estén a la altura de los desafíos actuales y puedan resistir ataques cibernéticos.

2.3.3 Necesidad de movilidad y acceso remoto:

Con la creciente tendencia hacia el trabajo remoto y la movilidad, se requiere que los empleados accedan a recursos internos desde ubicaciones externas de manera segura. Un análisis de los tipos de VPN proporciona las opciones más adecuadas para garantizar la conexión segura y el acceso a datos sensibles desde cualquier ubicación.

2.3.4 Cumplimiento normativo y regulaciones:

Muchos sectores, como la salud, las finanzas y el gobierno, están sujetos a regulaciones estrictas sobre la protección de datos y la privacidad. Un análisis detallado de los tipos de VPN permite a las organizaciones cumplir con los requisitos normativos y salvaguardar la información confidencial de sus clientes y usuarios.

2.3.5 Selección de tecnologías adecuadas:

Existen diversos protocolos y tecnologías de VPN, cada uno con sus propias ventajas y desventajas. Un análisis detallado ayuda a seleccionar la opción más adecuada para las necesidades específicas de la organización, considerando factores como el tamaño de la red, la cantidad de usuarios, el tipo de datos que se transmiten y los recursos disponibles.

2.3.6 Confianza en la comunicación en línea:

Los usuarios deben poder confiar en que su comunicación en línea es segura y privada. El análisis de VPN ayuda a identificar las soluciones que garantizan la integridad y la confidencialidad de los datos, lo que aumenta la confianza tanto de los empleados como de los clientes en el uso de servicios y aplicaciones en línea.

2.3.7 Prevención de filtraciones de datos:

Las filtraciones de datos pueden tener consecuencias devastadoras para las organizaciones, incluida la pérdida de confianza del público y daños a la reputación. Un análisis de VPN ayuda a evitar filtraciones mediante la elección de soluciones de seguridad robustas y la implementación adecuada de políticas de acceso.

2.3.8 Horizontes tecnológicos:

En el contexto de un mundo cada vez más conectado digitalmente, la investigación sobre los tipos de VPN para la transmisión segura de datos sensibles en Internet es altamente pertinente. La tecnología de las VPN evoluciona constantemente, y es crucial analizar y comprender los distintos enfoques para garantizar la seguridad y la privacidad de la información en un entorno tecnológico en constante cambio.

2.3.9 Horizontes sociales:

La seguridad de los datos es una preocupación creciente para individuos y organizaciones. La investigación en este campo ayuda a proteger la privacidad de las personas y fomenta la

confianza en las interacciones en línea. Además, el acceso seguro a datos sensibles desde ubicaciones remotas facilita la movilidad laboral y mejora la productividad, lo que tiene un impacto positivo en la sociedad.

2.3.10 Horizontes legales:

La investigación sobre VPN para la transmisión segura de datos se alinea con las regulaciones y leyes de protección de datos en todo el mundo. Cumplir con los requisitos legales es esencial para evitar posibles sanciones y proteger los derechos de privacidad de los usuarios y clientes.

2.3.11 Horizontes ambientales:

Aunque no está directamente relacionada con el medio ambiente, la investigación en este tema puede contribuir indirectamente a la sostenibilidad al facilitar el trabajo remoto y reducir la necesidad de desplazamientos físicos, lo que disminuye la huella de carbono asociada a los viajes y el transporte.

3. Objetivos

3.1 Objetivo General

Analizar y evaluar las tecnologías y protocolos existentes para la habilitación de redes privadas virtuales, que permiten realizar transmisión de datos de forma segura a través de redes públicas, brindando protección y privacidad durante la comunicación.

El objetivo busca proporcionar una visión integral de las ventajas y desventajas de cada tipo de VPN, considerando factores como la seguridad, el rendimiento, la escalabilidad y la interoperabilidad, para que las organizaciones y los usuarios puedan tomar decisiones informadas al implementar soluciones de VPN que resuelvan eficazmente la problemática de la transmisión segura de datos en un entorno en línea cada vez más complejo y amenazante.

3.2 Objetivos específicos

Investigar las diferentes tecnologías de VPN, realizando una comparación de los diversos tipos disponibles.

Evaluar cada tipo de VPN en cuanto a mecanismos de seguridad, cifrado y autenticación utilizados.

Identificar posibles vulnerabilidades y riesgos de seguridad en cada tipo de VPN, resaltando las amenazas potenciales y recomendando medidas de mitigación. Recomendar la mejor opción de habilitación de VPNs, según las necesidades y recursos de cada organización.

Evaluar las características de seguridad de cada tipo de VPN, incluyendo aspectos como la encriptación, la autenticación de usuarios y dispositivos, la gestión de claves y la protección contra amenazas cibernéticas.

4. Marco Teórico referencial

De acuerdo con el panorama actual del presente trabajo de titulación, es esencial comprender el contexto teórico en el que se enmarca cualquier estudio. Este marco teórico referencial proporciona una base sólida para abordar el análisis de los tipos de VPN en el contexto de la transmisión segura de datos sensibles en Internet. La revisión de estos conceptos y principios guiará la investigación aplicada y el desarrollo de recomendaciones prácticas en el proyecto de titulación.

Una empresa con empleados en múltiples ubicaciones puede beneficiarse de IKEv2 debido a su capacidad para reconectar sesiones interrumpidas.

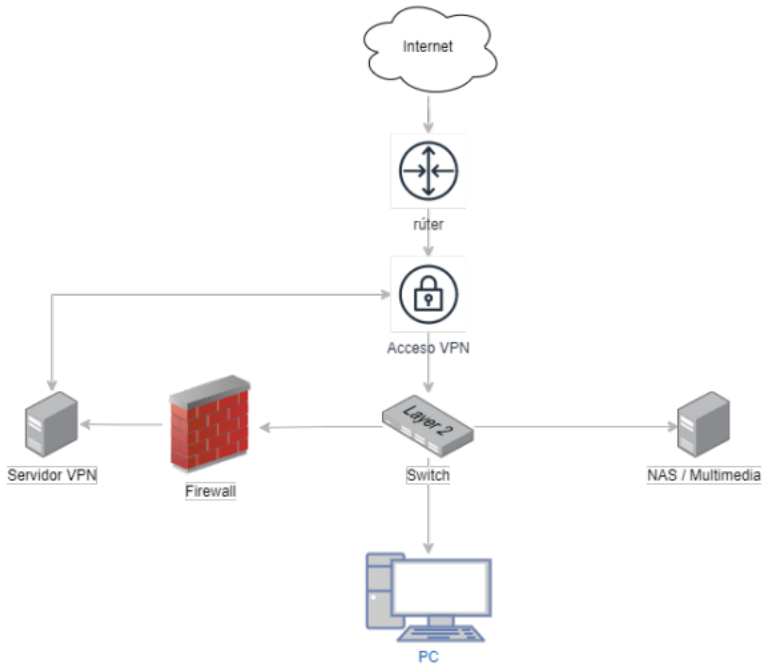


Imagen 1-2 Tecnologías aplicadas para la conexión

Fuente: Creación propia

4.1 Amenaza de seguridad de red

Las amenazas de seguridad de red son potenciales riesgos o vulnerabilidades que pueden comprometer la integridad, confidencialidad o disponibilidad de los datos, sistemas o servicios en una red informática. Estas amenazas pueden provenir tanto de fuentes externas como internas y pueden variar en su naturaleza y alcance.

- Malware
- Ataques de denegación de servicio (DDoS)
- Phishing
- Ingeniería social
- Vulnerabilidades de software
- Ataques de intermediarios (Man-in-the-Middle)
- Ataques de fuerza bruta
- Escuchas ilegítimas (Eavesdropping)
- Ataques de inyección

La gestión eficaz de las amenazas de seguridad de red implica la implementación de medidas de seguridad adecuadas, como firewalls, sistemas de detección de intrusiones, cifrado de datos, políticas de acceso y autenticación sólidas, así como la educación y concienciación de los usuarios para prevenir la ingeniería social y otras formas de ataques.

4.1.1 Dispositivos de seguridad de red

La creciente interconexión de sistemas informáticos y el aumento de amenazas cibernéticas han generado una demanda creciente de dispositivos de seguridad de red eficaces. Estos dispositivos desempeñan un papel crucial en la protección de la integridad, confidencialidad y disponibilidad de los datos en redes informáticas. Este estudio se centra en analizar diversos dispositivos de seguridad de red, incluyendo firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS),

sistemas de prevención de pérdida de datos (DLP), VPNs (Virtual Private Networks), y otros.

El objetivo principal es evaluar la efectividad y la idoneidad de estos dispositivos en la mitigación de diferentes tipos de amenazas cibernéticas. Para lograr esto, se llevará a cabo una revisión exhaustiva de la literatura para comprender las características, funcionalidades y capacidades de cada tipo de dispositivo de seguridad de red. Además, se realizarán pruebas de laboratorio y simulaciones para evaluar su desempeño en escenarios de amenazas simuladas.

Los dispositivos de seguridad de red son herramientas diseñadas para proteger las redes informáticas contra amenazas cibernéticas. Aquí tienes una descripción de algunos de los dispositivos más comunes utilizados para este fin:

Firewall: Un firewall es una barrera de seguridad que controla y filtra el tráfico de red según un conjunto de reglas predefinidas

Routers con funciones de seguridad integradas: Algunos routers vienen con características de seguridad integradas, como filtrado de paquetes, listas de control de acceso (ACL) y servicios VPN, que ayudan a proteger la red contra intrusiones.

Sistemas de detección y prevención de intrusiones (IDS/IPS): Estos sistemas monitorean el tráfico de red en busca de actividades sospechosas o maliciosas.

Sistemas de prevención de pérdida de datos (DLP): Estos dispositivos ayudan a proteger la confidencialidad de la información al monitorear, detectar y prevenir la transmisión no autorizada de datos sensibles fuera de la red corporativa.

VPN (Red Privada Virtual): Una VPN establece una conexión segura y cifrada entre dispositivos remotos y la red corporativa a través de Internet.

Sistema de prevención de intrusos en la red (NIPS): Similar a un IPS, un NIPS se enfoca específicamente en la detección y prevención de intrusiones en una red. Puede monitorear el tráfico en tiempo real y aplicar políticas de seguridad para proteger contra amenazas.

Gateway de seguridad web: Estos dispositivos protegen contra amenazas web al filtrar el tráfico HTTP y HTTPS en busca de malware, phishing y otros ataques basados en la web.

Controladores de acceso a la red (NAC): Un NAC asegura que solo los dispositivos autorizados y cumplidores de políticas puedan acceder a la red, ayudando a prevenir el acceso no autorizado y la propagación de amenazas.

Servidores proxy: Un servidor proxy actúa como intermediario entre los dispositivos de la red y el Internet, filtrando y reenviando el tráfico según políticas de seguridad establecidas.

4.2 Política de seguridad de la red

Una política de seguridad de red es un conjunto de autorizaciones para monitorear, administrar y hacer cumplir la seguridad en toda la infraestructura de red de su organización. Destaca en detalle los controles de acceso de seguridad a la red, los protocolos a seguir y los procedimientos implementados para que la red permanezca protegida de cualquier actividad que pueda comprometer la seguridad. Una política de ciberseguridad es un documento integral que cubre muchos aspectos diferentes de la ciberseguridad de una organización. Estas políticas suelen ser desarrolladas y revisadas por la administración o los servicios subcontratados. Las políticas de ciberseguridad incluyen los siguientes tipos de detalles:

- Una guía para la compra de nuevos equipos o tecnología.
- Las reglas por seguir al acceder o modificar la red.
- Pasos o procedimientos por seguir cuando se produce una brecha de seguridad.
- El proceso de aplicar control de acceso a dispositivos de red.
- Definir privilegios de usuario y acceso de usuario a procesos o servicios autorizados que puedan estar ejecutándose en la red.

4.2.1 Creación de una política de seguridad de la red

Una guía para la compra de nuevos equipos o tecnología. Las reglas por seguir al acceder o modificar la red. Pasos o procedimientos por seguir cuando se produce una brecha de seguridad. El proceso de aplicar control de acceso a dispositivos de red. Definir privilegios de usuario y acceso de usuario a procesos o servicios autorizados que puedan estar ejecutándose en la red.

Podemos contemplar los siguientes ítems:

- Evaluar los riesgos y vulnerabilidades de seguridad existentes.
- Implementar controles de seguridad.
- Definir funciones y responsabilidades
- Resumir las prácticas de respuesta a incidentes
- Crear un proceso de revisión y auditoría

4.3 Sistemas de Criptografía

En el contexto de una VPN (red privada virtual), los sistemas criptográficos juegan un papel esencial para garantizar la confidencialidad y seguridad de las comunicaciones entre dispositivos remotos y la red corporativa. Aquí hay un resumen del papel del cifrado en una VPN.

Confidencialidad de los Datos: Uno de los objetivos principales de una VPN es garantizar la seguridad de los datos transferidos entre dispositivos remotos y la red corporativa. Los sistemas de cifrado utilizados en las VPN cifran los datos durante la transmisión, lo que significa que sólo los destinatarios autorizados pueden descifrar y acceder a la información. Esto garantiza que incluso si se interceptan datos, sólo aquellos con la clave de cifrado adecuada puedan leerlos.

Algoritmos Criptográficos Robustos: En una VPN, se utilizan algoritmos de cifrados sólidos y ampliamente aceptados para garantizar una conexión segura. Algunos de estos algoritmos incluyen AES (Estándar de cifrado avanzado) para cifrado simétrico y RSA (Rivest-Shamir-Adleman) o ECDSA (Algoritmo de firma digital de curva

elíptica) para cifrado asimétrico. Estos algoritmos han sido evaluados exhaustivamente por expertos en seguridad y se consideran altamente seguros contra ataques de criptoanálisis.

Protección contra Intermediarios Maliciosos: Los sistemas criptográficos en las VPN protegen contra ataques de intermediarios (Man-in-the-Middle) al garantizar la autenticidad de los extremos de la conexión. Los protocolos de autenticación, como el intercambio de claves IKE (Internet Key Exchange) en IPSec, aseguran que los dispositivos remotos estén comunicándose con la red corporativa de manera legítima y no con un atacante que se haga pasar por el servidor VPN.

Integridad de los Datos: Además de garantizar la confidencialidad, los sistemas criptográficos en las VPN también protegen la integridad de los datos transmitidos. Se utilizan funciones hash criptográficas para generar valores hash únicos de los datos, que se envían junto con los datos cifrados. El receptor puede verificar estos valores hash para asegurarse de que los datos no hayan sido modificados durante la transmisión.

Gestión Segura de Claves: La gestión adecuada de las claves criptográficas es esencial para la seguridad de una VPN. Los sistemas criptográficos implementan protocolos seguros para el intercambio y la gestión de claves, como el protocolo Diffie-Hellman para el intercambio de claves simétricas o el uso de infraestructuras de clave pública (PKI) para la gestión de claves asimétricas. Esto garantiza que las claves sean generadas, distribuidas y almacenadas de manera segura para evitar su compromiso.

4.3.1 Servicios Criptográficos

La privacidad y la seguridad son dos de las características que más valoran los usuarios de Internet. Por tanto, el mercado ofrece servicios que brindan protección adicional. Una VPN puede ser una opción para una navegación por Internet más segura.

Mercados online define como “una red privada virtual que crea conexiones entre dispositivos en Internet”. Las VPN se utilizan para transmitir datos de forma anónima a través de redes públicas. Se sabe que ocultan las direcciones IP de los usuarios de Internet, además de cifrar datos; De esta forma, nadie podrá acceder a información personal sin permiso.

Una VPN utiliza cifrado para proteger su conexión a Internet del acceso no autorizado. También puede actuar como un mecanismo de cierre para finalizar programas preseleccionados en caso de actividad sospechosa en Internet. Esto reduce la posibilidad de que los datos se vean comprometidos.

Otra función que ofrece esta herramienta es mantener privado su historial de búsqueda en Internet, ya que los ISP y los navegadores, por ejemplo, pueden rastrear estos datos para sus propios fines de marketing. Asimismo, el uso de una VPN sirve para acceder a contenidos de todo el mundo, como servicios de streaming. "

"Su conexión VPN le permitirá cambiar su dirección IP desde su país y acceder a sus programas favoritos si se encuentra fuera de ese país".

Cifrado de Datos: El principal servicio de cifrado de una VPN es el cifrado de datos. Este servicio utiliza un algoritmo de cifrado para convertir texto sin formato en texto cifrado antes de enviarlo a través de la red. Esto asegura que incluso si los datos están bloqueados, solo podrá leer para personas con bloqueos de descifrados apropiados.

Autenticación de los Extremos de la Conexión: Otro servicio importante es la autenticación de los puntos finales de conexión VPN. Esto garantiza que los dispositivos que participan en la conexión VPN sean como dicen ser. Los protocolos de autenticación, como Internet Key Exchange (IKE) en IPSec, se utilizan para verificar la identidad de los puntos finales conectados y evitar ataques de intermediario.

Integridad de los Datos: El código VPN también protege la seguridad de los datos transferidos. Las funciones de división de código se utilizan para crear valores de datos únicos, que se envían a datos cifrados. El destinatario puede verificar estos hashes para asegurarse de que los datos no se hayan modificado durante la transmisión.

Gestión de Claves: Administrar las claves de cifrado adecuadas es esencial para la seguridad de la VPN. Los servicios criptográficos implementan protocolos seguros para el intercambio y la gestión de claves, como el protocolo Diffie-Hellman para el intercambio de claves simétrico, o el uso de infraestructura de clave pública (PKI) para gestionar bloqueos asimétricos. Esto garantiza que las claves se generen, distribuyan y almacenen de forma segura para evitar la exposición.

4.4 Autenticación e Integridad de datos básica

Autenticación:

La autenticación es el proceso de verificar la identidad de un usuario o sistema para confirmar su identidad antes de permitirle acceder a un recurso o servicio. Existen varios métodos de autenticación, que pueden incluir los siguientes:

Autenticación basada en conocimiento: Este método requiere que el usuario proporcione información secreta, como una contraseña, PIN o respuesta a una pregunta de seguridad. Es el método de autenticación más comúnmente utilizado en sistemas informáticos.

Autenticación basada en algo que tienes: Este método implica el uso de un dispositivo físico, como una tarjeta inteligente, una llave USB o un token de autenticación, que el usuario debe poseer para demostrar su identidad.

Autenticación basada en algo que eres: Este método utiliza características biométricas únicas del usuario, como huellas dactilares, reconocimiento facial, iris o voz, para verificar su identidad.

Integridad de Datos:

La integridad de los datos se refiere a la exactitud y confiabilidad de los datos almacenados o transmitidos. Es importante asegurarse de que los datos no se modifiquen, alteren o destruyan de manera no autorizada. Hay algunas formas de garantizar la seguridad de los datos**:**

Funciones hash criptográficas: Estas funciones producen un valor único y fijo de longitud fija, conocido como hash, a partir de los datos de entrada. Cualquier cambio en los datos producirá un hash diferente. Al comparar el hash calculado con un hash conocido, se puede verificar la integridad de los datos.

Firmas digitales: Las firmas digitales utilizan criptografía de clave pública para proporcionar autenticación e integridad de los datos. El emisor de un mensaje o archivo firma digitalmente el contenido utilizando su clave privada. El receptor puede verificar la firma utilizando la clave pública del emisor para asegurarse de que el contenido no haya sido alterado y provenga de la entidad esperada.

Checksums: Los checksums son valores numéricos que se calculan a partir de los datos y se utilizan para verificar su integridad. Se añaden al final de los datos y se recalculan al recibirlos para confirmar que no han sido modificados durante la transmisión.

la autenticación y la integridad de datos son dos aspectos clave de la seguridad de la información. La autenticación verifica la identidad de los usuarios o sistemas antes de otorgarles acceso, mientras que la integridad de datos garantiza que los

datos no sean modificados o alterados de manera no autorizada. Ambos son fundamentales para proteger la confidencialidad, integridad y disponibilidad de la información en entornos digitales.

La imagen 2.3 representa el triángulo de la seguridad de la información, que incluye los tres pilares fundamentales para proteger la información de una organización o sistema: Confidencialidad, Integridad y Disponibilidad. Aquí está el desglose de cada concepto:

Imagen 2-3 Integridad de datos básica

Fuente: (Seguridad de la Información, 2022)

4.5 Confidencialidad

La confidencialidad es esencial para que los servicios de redes privadas virtuales (VPN) garanticen la confidencialidad de la información transmitida a través de la red. El cifrado juega un papel clave para garantizar esta confidencialidad.

E La confidencialidad es esencial para que los servicios de redes privadas virtuales (VPN) garanticen la confidencialidad de la información transmitida a través de la red. El cifrado juega un papel clave para garantizar esta confidencialidad.

Cuando se conecta a un servicio VPN, todas las comunicaciones entre su dispositivo y el servidor VPN están cifradas. Esto significa que si alguien intercepta sus datos mientras viajan por Internet, no podrá leerlos sin la clave de descifrado correcta.

Los servicios VPN utilizan varios protocolos de cifrado, incluidos OpenVPN, IPSec y L2TP/IPSec. Estos protocolos utilizan algoritmos criptográficos robustos para proteger la confidencialidad de los datos.

Además del cifrado de datos, es importante considerar las políticas de registro de su proveedor de VPN. Algunos proveedores mantienen registros de su actividad, lo que puede comprometer su privacidad. Por lo tanto, es importante elegir un proveedor de VPN que tenga una política estricta de no registros o que limite la cantidad de datos registrados.

En otras palabras, la confidencialidad del servicio VPN se logra mediante el cifrado de datos utilizando algoritmos criptográficos sólidos y una política de no registros del lado del proveedor. Esto protege sus comunicaciones y garantiza su privacidad mientras usa una VPN.

La imagen 3.3 ilustra el funcionamiento básico de una VPN (Red Privada Virtual) y su papel en la protección de la privacidad y seguridad en internet.

Imagen 3-3 Protección de una VPN en Internet

Fuente: (https://www.redeszone.net/noticias/seguridad/que-protege-vpn-internet,2024)

4.6 Llave publica para Criptografía

La imagen 4.3 representa el funcionamiento del **cifrado asimétrico**, un método clave en la criptografía moderna. Este proceso utiliza un par de llaves: una llave pública para cifrar el mensaje y una llave privada para descifrarlo.

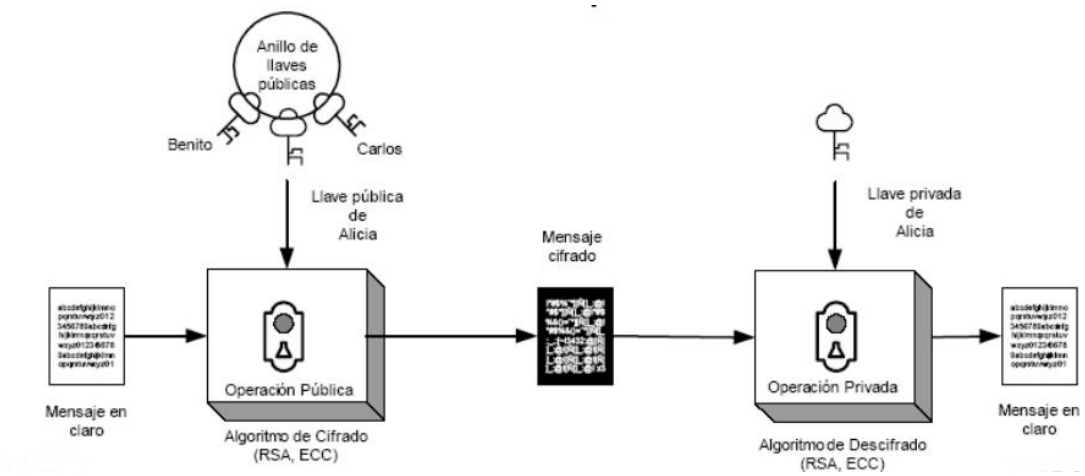


Imagen 4-3 Llave publica

Fuente: (http://ri.uaemex.mx/bitstream/handle/20.500.11799/32727/secme-35753.pdf?sequence=1, 2021)

El uso de criptografía de clave pública o asimétrica se ha adoptado en la criptografía moderna. La criptografía simétrica utiliza la misma clave para cifrar y decodificar datos, pero esta forma de criptografía utiliza una clave diferente. En criptografía asimétrica se utilizan dos claves, una está relacionada con la otra.

La seguridad del sistema se basa en operaciones matemáticas complejas que son fáciles de realizar en una dirección, pero muy difíciles en la otra. El problema de factorización de números grandes en RSA es un ejemplo. No es factible que un atacante deduzca la clave privada correspondiente incluso si la clave pública está disponible públicamente.

La criptografía de clave pública se utiliza en una amplia gama de aplicaciones, desde la seguridad en las comunicaciones por Internet hasta la firma digital de documentos. Ha sido fundamental garantizar la confidencialidad, integridad y autenticidad de los datos en el mundo digital actual.

4.6.1 Ventajas y desventajas de Cifradores asimétricos o criptografía de llave pública

- **Ventajas destacadas:** Seguridad mejorada, autenticación sólida y capacidad para manejar claves de forma segura.
- **Desventajas principales:** Complejidad técnica, rendimiento más bajo y dependencias de la tecnología actual, como los algoritmos resistentes a la computación cuántica.

La tabla 1. enumera las ventajas y desventajas de la criptografía de llave pública (cifrado asimétrico) para evaluar su utilidad en diferentes contextos. Aquí está una explicación detallada de cada aspecto:

Aspecto	Ventajas	Desventajas
Seguridad	No es necesario compartir tu contraseña secreta, lo que disminuye la posibilidad de que sea interceptada.	Puedes ser fácilmente atacado por hackers si tus contraseñas son cortas o tus sistemas de seguridad ya no son efectivos.
Autenticación	Te ayuda a comprobar quién está enviando algo usando firmas digitales.	Necesita una estructura compleja para manejar claves y certificados.
Intercambio de claves	Facilita el intercambio seguro de claves para la criptografía simétrica.	Más lento en comparación con la criptografía simétrica.
Confidencialidad y verificación	Solo el destinatario con la clave privada puede desencriptar los mensajes.	Llaves mucho más grandes, por lo que se necesita más espacio y potencia de la computadora.
Versatilidad	Usado en aplicaciones diversas como cifrado, firmas digitales y autenticación.	No es adecuado para cifrar grandes volúmenes de datos debido a su bajo rendimiento.
Integración con PKI	Compatible con infraestructuras de clave pública, mejorando la gestión de identidad en redes.	Escalabilidad limitada en grandes organizaciones por la complejidad de gestionar múltiples claves públicas.
Impacto de nuevos avances	Resistente a muchos tipos de ataques tradicionales si se configura correctamente.	En riesgo de ser afectado por la computación cuántica, lo que podría poner en peligro su seguridad más adelante.

Tabla 1. Ventajas y desventajas de Cifradores asimétricos

Fuente: ((s/f). Cloudfront.net., 2021)

La encriptación asimétrica es muy importante para mantener segura la comunicación digital hoy en día. A pesar de que tiene sus problemas con el rendimiento y la complejidad, sus ventajas en escalabilidad, confidencialidad y compatibilidad con tecnologías avanzadas la convierten en una parte muy importante de la seguridad informática. Pero es importante analizar bien cómo se va a llevar a cabo, teniendo en cuenta lo que el sistema necesita y los recursos que tenemos disponibles.

4.7 Diffie-Hellman Key Exchange

Intercambiar llaves Diffie Hellman en un protocolo de intercambio seguro de llaves criptográficas sobre un canal público (inseguro) sin haber tenido contacto previo. La llave puede usarse para cifrar subsecuentes. El esquema fue publicado por Whitfield Diffie y Martin Hellman en 1976.

El sistema se basa en la idea de que dos personas pueden crear una llave compartida juntas sin que un intruso que esté escuchando las comunicaciones pueda obtenerla.

La imagen 5.3 representa una analogía visual del **Intercambio de Claves de Diffie-Hellman**, un protocolo criptográfico utilizado para establecer una clave secreta compartida entre dos partes (Alice y Bob) sin necesidad de que estas compartan directamente dicha clave.

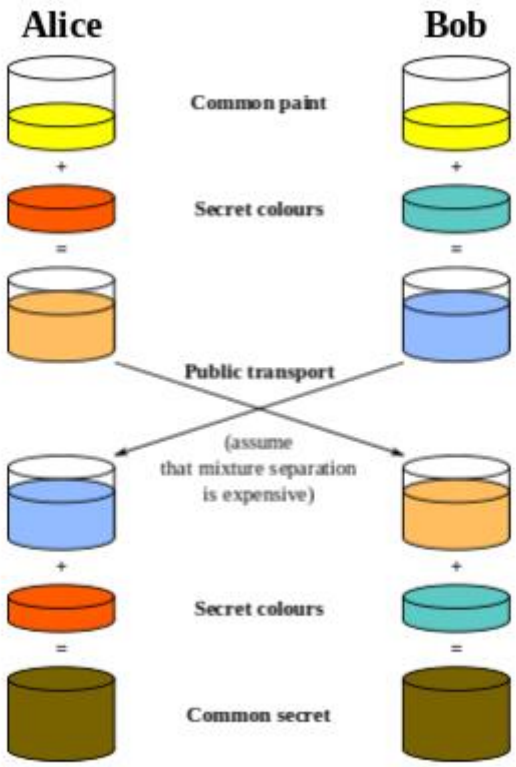


Imagen 5-3 Algoritmo Diffie-Hellman.

Fuente: (https://learnerbits.com/basic-cryptographic-primitives-unit-2/, 2022)

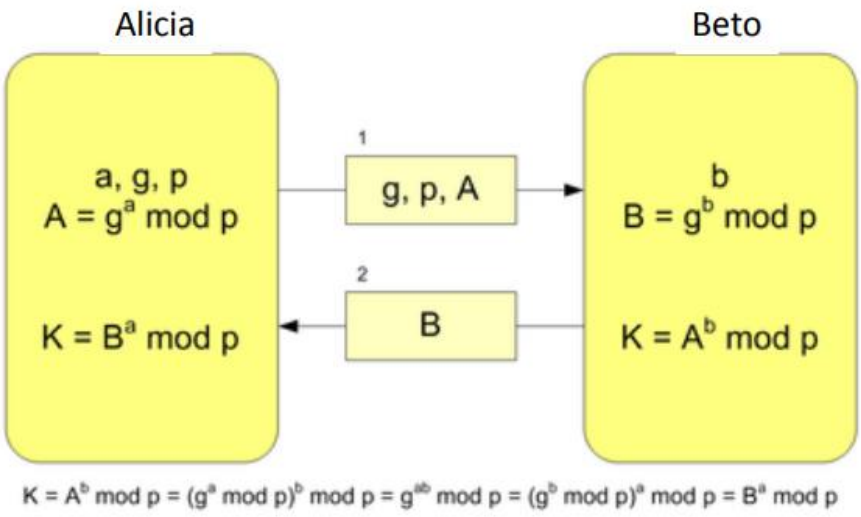


Imagen 6-3- Ejemplo de algoritmo Diffje-Hellman.

Fuente: (https://www.gaussianos.com/criptografia-cifrado-de-clave-publica-i/, 2023)

Alicia y Beto acuerdan usar un número primo p = 23 y un generador g = 5 (el cual es una raíz primitiva módulo 23).

• Alicia selecciona un entero secreto a = 6, y envía a Beto A = g
a mod p
– A = 5
6 mod 23 = 8

• Beto selecciona un entero secreto b = 15, y envía a Alicia B = g
b mod p
– B = 5
15 mod 23 = 19

• Alicia procesa s = B
a mod p
– s = 196 mod 23 = 2

• Beto procesa s = A
b mod p
– s = 8
15 mod 23 = 2

• Alicia y Beto ahora comparten un secreto (el número 2).

4.8 Redes Privadas Virtuales VPN

Las Redes Privadas Virtuales (VPN) son una tecnología importante para la seguridad de la comunicación en línea. Permiten a los usuarios conectarse de manera segura a recursos privados a través de una red pública, como Internet, y acceder a ellos de forma remota. Este acceso seguro es crucial para empresas, organizaciones y usuarios individuales que buscan proteger la confidencialidad y la integridad de sus datos mientras se comunican a través de redes no seguras.

4.8.1 Funcionamiento de las VPN

Las VPN funcionan mediante el establecimiento de un túnel seguro entre el dispositivo del usuario y el servidor VPN. Este túnel cifrado protege los datos que se transmiten a través de él, evitando que terceros intercepten o manipulen la información. Las VPN utilizan diferentes protocolos y técnicas de cifrado para garantizar la seguridad de la comunicación, como IPsec, SSL/TLS, OpenVPN, entre otros.

4.8.2 Tipos de VPN

Existen varios tipos de VPN, cada uno con sus propias características y casos de uso específicos:

- **VPN de acceso remoto:** Permiten a los usuarios individuales conectarse de forma segura a una red privada desde ubicaciones remotas, como sus hogares o lugares de trabajo remotos.
- **VPN de sitio a sitio:** Conectan redes completas entre sí, permitiendo la comunicación segura entre diferentes sucursales o ubicaciones de una empresa.
- **VPN de cliente a servidor:** En este tipo de VPN, los clientes individuales se conectan a un servidor VPN centralizado para acceder a recursos privados de la red.

4.8.3 Operación de IPSec VPN

IPSec (Protocolo de seguridad de Internet) es un conjunto de protocolos de seguridad utilizados para garantizar la seguridad de las comunicaciones a través de una red IP. Una VPN (Red Privada Virtual) utiliza IPSec para crear un túnel seguro a través de una red pública, como Internet, permitiendo que dos redes privadas se conecten de forma segura a través de una red no segura.

4.8.4 Componentes de IPSec

Autenticación: IPSec puede autenticar las partes que se comunican entre sí utilizando métodos como precompartir claves, certificados digitales o autenticación basada en Kerberos.

Integridad de datos: Se garantiza mediante el uso de funciones de hash, que aseguran que los datos no han sido alterados durante la transmisión.

Confidencialidad: Se logra mediante el cifrado de los datos utilizando algoritmos como AES o 3DES, lo que garantiza que solo las partes autorizadas puedan acceder a la información.

Negociación de parámetros de seguridad: PSec, ampliamente adoptado en redes corporativas, utiliza IKE para negociar parámetros dinámicos en escenarios multiusuario, entre los dispositivos que establecen la conexión VPN.

Mitigación: Mantener los protocolos actualizados, aplicar parches de seguridad y utilizar las versiones más seguras de los protocolos de cifrado.

La imagen 7.3 representa la implementación de una **VPN Site-to-Site** con un esquema de redundancia que utiliza túneles primarios y secundarios para conectar dos redes locales (LAN) a través de internet.

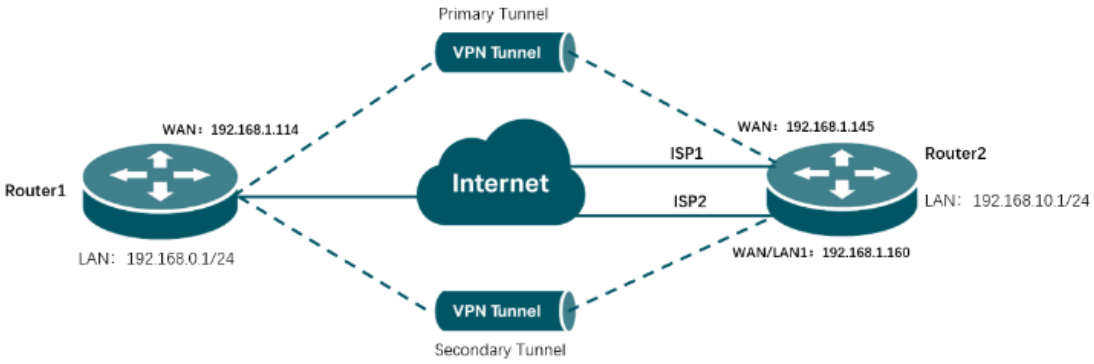


Imagen 7-3 Conexión IPsec VPN.

Fuente: (https://www.tp-link.com/pt/support/faq/3575/, 2020)

4.8.5 Modos de Operación de IPSec:

a. Túnel:

En el conducto, todo el lío IP primero, incluyendo su encabezado, es encapsulado en un moderno lío IP con un moderno encabezado IP. Este túnel se utiliza típicamente para dirigir el trayecto entre repetición redes, como una unión entre repetición Gateway ora entre un host y un Gateway.

- **Cifrado de todo el lío IP:** Tanto el encabezado como la tributo instrumento del lío IP canción cifrados.
- **Integridad de los datos:** Se añade un encabezado de autenticación (AH) ora un encabezado de resolución (ESP) para asegurar la moralidad del lío completo.
- **Encapsulación del lío primero:** El lío IP primero se encapsula en el interior de un moderno lío IP con un moderno encabezado IP. Esto oculta las direcciones IP originales y otros detalles del encabezado IP primero.

El túnel conducto es exacto para concertar conexiones seguras entre redes, como conexiones de bloqueo a bloqueo en una VPN.

b. **Transporte:**

En el modo de transporte, IpSec protege sólo la carga útil de un paquete IP, dejando intacto el encabezado del datagrama IP original. Este modo se utiliza normalmente para proteger las comunicaciones entre dos hosts finales.

Cifrado de carga útil: solo se cifran los datos dentro del paquete IP.

Integridad de datos: se agrega un encabezado de autenticación (AH) o un encabezado de seguridad (ESP) para garantizar la integridad de la carga útil.

Encabezado IP original no cifrado: el encabezado original del datagrama IP no está cifrado. Esto significa que la dirección IP original y otros campos en el encabezado IP permanecen visibles. El modo de transporte es adecuado para el tráfico entre hosts finales dentro de la misma red privada.

4.9 túnel GRE sobre IPSEC

Encapsular paquetes dentro de otros paquetes se denomina "tunelización". Los túneles GRE generalmente se configuran entre dos enrutadores, y cada enrutador actúa como un punto final para el túnel. Los enrutadores están configurados para enviar y recibir paquetes GRE directamente entre sí. El enrutador entre estos dos enrutadores no abre los paquetes encapsulados. Estos sólo se refieren a las cabeceras que rodean el paquete encapsulado para poder transportarlo.

Para entender por qué se llama "tunelización", podemos cambiar un poco la analogía. Si un automóvil necesita ir del punto A en un lado de una montaña al punto B en el otro lado, la forma más eficiente es simplemente cruzar la montaña. Sin embargo, los coches normales no pueden atravesar directamente una roca sólida. Por lo tanto, el coche tiene que rodear la montaña para llegar del punto A al punto B.

Pero imagina que se construyera un túnel para cruzar una montaña. Hoy en día, los coches pueden ir directamente del punto A al punto B. Esto es mucho más rápido y no es posible sin túneles.

Luego, el punto A como un dispositivo conectado a la red, el punto B como otro dispositivo conectado a la red, la red entre los dos dispositivos en las montañas y el paquete de datos que debe enviarse desde el punto A al punto en el automóvil. Imaginemos. B. Imaginemos que esta red no admite el tipo de paquetes de datos que los dispositivos en los puntos A y B necesitan intercambiar. Al igual que un coche que intenta cruzar una montaña, los paquetes de datos no pueden pasar y tienen que recorrer una ruta mucho más larga a través de redes adicionales.

Sin embargo, GRE crea un "túnel" virtual a través de la red "montaña" para pasar paquetes de datos. Así como los túneles crean caminos para los automóviles, GRE (y otros protocolos de túneles) crean caminos para paquetes de datos a través de redes incompatible

4.9.1 Beneficios de un túnel GRE sobre Ipsec

Proporciona un túnel seguro a través de una red no segura, como Internet.

- **Seguridad robusta:** Proporciona autenticación, integridad y confidencialidad de los datos al autenticar paquetes y cifrar su contenido.

Permite encapsular cualquier tipo de tráfico IP dentro de un túnel.

- **Encapsulación de cualquier tipo de tráfico IP:** Proporciona autenticación, integridad y confidencialidad de los datos al autenticar paquetes y cifrar su contenido. GRE le permite encapsular cualquier protocolo de red en paquetes IP, lo que le permite transportar muchos tipos diferentes de tráfico a través de una VPN.

Funciona bien con sistemas que no son compatibles con IPsec, ya que el tráfico encapsulado parece tráfico IP normal.

- **Conexión con sistemas no compatibles con Ipsec:** Los túneles GRE sobre IPsec pueden funcionar incluso en sistemas que no admiten IPsec porque el tráfico encapsulado parece tráfico IP normal.
- **Encabezados GRE:** Contienen información de enrutamiento que permite que los paquetes atraviesen múltiples redes.
- **Implementación en redes de gran escala:** Los túneles GRE sobre IPsec son escalables y se pueden implementar de manera eficiente en redes grandes, como redes corporativas multinacionales.

4.9.2 Protocolo Internet Key Exchange

El Protocolo de intercambio de claves de Internet (IKE) automatiza la administración de claves IPsec. IKE reemplaza la asignación y renovación manual de claves en redes IPv4. IKE permite a los administradores gestionar redes más seguras.

Los administradores del sistema utilizan IPsec para configurar redes IPv4 seguras. El demon in.iked proporciona omisión de claves, autenticación y protección de autenticación en el momento del arranque. Los administradores establecen parámetros en archivos de configuración. No es necesario actualizar las claves manualmente después de configurar los parámetros.

4.9.3 Funcionamiento de IKE

El protocolo IKE (Intercambio de Claves de Internet) es una parte muy importante del sistema de seguridad del Protocolo de Internet (IPsec). La función es crear y controlar relaciones de seguridad llamadas Asociaciones de Seguridad (SA). Este protocolo permite negociar claves criptográficas, autenticar a las partes involucradas y establecer parámetros de seguridad para proteger las comunicaciones.

4.9.4 Compatibilidad de IKE con equipos propietarios y no propietarios

La tabla 2 representa la implementación de una **VPN Site-to-Site** con un esquema de redundancia que utiliza túneles primarios y secundarios para conectar dos redes locales (LAN) a través de internet.

Criterio	Equipos Propietarios	Equipos No Propietarios
Definición	Dispositivos de fabricantes específicos que suelen usar software cerrado o licenciado.	Dispositivos o software de código abierto o libre, como Linux, FreeBSD, etc.
Protocolos soportados	Totalmente compatible con IKE (IKEv1 e IKEv2).	Totalmente compatible con IKE (IKEv1 e IKEv2).
Interoperabilidad	Alta, pero puede depender de extensiones propietarias o configuraciones específicas.	Alta, siempre que se cumplan los estándares de IPsec y configuraciones compatibles.

Criterio	Equipos Propietarios	Equipos No Propietarios
Ejemplos de implementación	Cisco, Fortinet, Juniper, Palo Alto Networks.	strongSwan, OpenSwan, Libreswan, soluciones basadas en Linux o FreeBSD.
Flexibilidad	Limitada por las configuraciones y herramientas proporcionadas por el fabricante.	Alta, con personalización completa en la configuración y elección de herramientas.
Gestión de claves	Basada en herramientas propietarias, puede incluir soporte automatizado o simplificado.	Basada en estándares abiertos, con mayor control manual de la configuración.
Costo	Elevado debido a licencias y equipos especializados.	Bajo o nulo, ya que las herramientas suelen ser de código abierto o gratuitas.
Dependencia de software	Uso de firmware o software propietarios, con actualizaciones controladas por el fabricante.	Uso de software libre con actualizaciones frecuentes de la comunidad de desarrolladores.
Escalabilidad	Escalable, pero puede requerir hardware específico del mismo fabricante.	Muy escalable y adaptable a hardware diverso.
Soporte técnico	Garantizado por el fabricante (generalmente bajo contrato).	Ofrecido por la comunidad o empresas especializadas en soluciones de código abierto.

Tabla 2 Tabla comparativa: Compatibilidad de IKE con Equipos Propietarios y No Propietarios

Tanto en equipos propietarios como no propietarios, el protocolo IKE es completamente compatible gracias a su base en estándares abiertos. Sin embargo, la elección entre estos depende de las necesidades del usuario, presupuesto, nivel de personalización requerido y el entorno de implementación.

4.9.5 Negociación de la seguridad

IKE negocia los parámetros de seguridad, como algoritmos de cifrado, algoritmos de integridad y métodos de autenticación, entre dos dispositivos IPsec que desean comunicarse

La negociación de seguridad en Internet Key Exchange (IKE) es un proceso crítico que permite que dos dispositivos IPsec establezcan una conexión segura y acuerden los parámetros de seguridad necesarios para proteger el tráfico de datos.

a) Inicio de la negociación:

La negociación de seguridad en IKE comienza cuando dos dispositivos IPsec quieren establecer una conexión segura entre sí.

b) Selección de algoritmos y parámetros

Cada dispositivo propone una serie de algoritmos y parámetros de seguridad compatibles que puede utilizar para proteger la comunicación. Esto incluye:

- Algoritmos de cifrado (AES, 3DES, etc.).
- Algoritmos de integridad (HMAC-SHA256, HMAC-SHA1, etc.).
- Métodos de autenticación (precompartidos, certificados digitales, etc.).
- Parámetros de intercambio de claves (tamaño de clave, grupo Diffie-Hellman, etc.).

c) Intercambio de propuestas:

El intercambio de propuestas en IKE (Internet Key Exchange) es el proceso mediante el cual dos dispositivos IPsec negocian y acuerdan los parámetros de seguridad necesarios para establecer una conexión segura. el intercambio de propuestas en IKE es un paso crítico que permite a dos dispositivos IPsec acordar los parámetros de seguridad necesarios para establecer una conexión segura. Este proceso

garantiza una comunicación segura y confiable entre los dispositivos en una red IPsec. Este intercambio ocurre durante la Fase 1 de IKE y consta de varios pasos.

4.9.6 Propuesta de seguridad

Cada dispositivo envía al otro una o varias propuestas de seguridad que especifican los algoritmos y parámetros que está dispuesto a utilizar para proteger la comunicación.

Las propuestas incluyen:

Una propuesta de seguridad en IKE incluye los siguientes elementos clave:

a. **Algoritmo de cifrado (Encryption Algorithm)**
   - Especifica el método para cifrar los datos durante la comunicación.
   - Ejemplos: AES (Advanced Encryption Standard), 3DES, ChaCha20.
   - **Recomendación moderna**: AES con claves de 256 bits.

b. **Algoritmo de integridad (Integrity Algorithm)**
   - Asegura que los datos no han sido modificados durante la transmisión.
   - Ejemplos: HMAC-SHA2 (SHA-256, SHA-384, SHA-512).
   - **Recomendación moderna**: HMAC con SHA-256 o superior.

c. **Algoritmo de intercambio de claves (Key Exchange Algorithm)**
   - Utilizado para establecer claves compartidas de manera segura.
   - Ejemplos: Diffie-Hellman (DH) en diferentes grupos (Grupo 14, Grupo 19).
   - **Recomendación moderna**: Grupos Diffie-Hellman basados en curvas elípticas (ECDH) como el Grupo 19 o 20.

d. **Método de autenticación (Authentication Method)**
   - Define cómo se autenticarán las partes involucradas.
   - Opciones:
     - Clave precompartida (*Pre-Shared Key*, PSK).
     - Certificados digitales (PKI).
     - Autenticación Extensible (EAP) para entornos como VPNs.

e. **Tiempo de vida (Lifetime)**

- Define cuánto tiempo es válida la asociación de seguridad antes de que sea renegociada.
- Se mide en segundos o kilobytes transmitidos.
- Ejemplo típico: 3600 segundos (1 hora).

f. Versión de IKE

- Indica si se utilizará IKEv1 o IKEv2.
- **Recomendación moderna**: Usar IKEv2 por sus ventajas en seguridad y eficiencia.

g. Ejemplo de Propuesta de Seguridad de IKE

La tabla 3 presenta los parámetros comunes utilizados en la configuración de IKE (Internet Key Exchange) en el contexto de VPNs.

Parámetro	Valor Ejemplo
Versión de IKE	IKEv2
Algoritmo de cifrado	AES-256
Algoritmo de integridad	HMAC-SHA2-256
Algoritmo de intercambio de claves	Diffie-Hellman Grupo 19 (ECDH)
Método de autenticación	Certificados digitales
Tiempo de vida	3600 segundos

Tabla 3 Ejemplo de propuesta de Seguridad IKE

4.9.7 Intercambio de propuestas

El intercambio de propuestas de IKE es una parte crucial del proceso de negociación en el protocolo Internet Key Exchange (IKE). Durante este intercambio, las partes participantes (el iniciador y el receptor) acuerdan los parámetros de seguridad que se usarán para proteger las comunicaciones. Este proceso es diferente en IKEv1 e IKEv2, aunque ambos comparten conceptos básicos.

La tabla 4 describe los pasos clave en el proceso de negociación de un túnel VPN utilizando el protocolo IKE (Internet Key Exchange). Este proceso es fundamental para establecer una conexión segura entre dos puntos, como en una VPN Site-to-Site o Cliente-Servidor. A continuación, se explica cada paso:

Paso	Descripción	Responsable
1. Envío de propuesta inicial	El iniciador envía una o más propuestas de seguridad, que incluyen parámetros como algoritmos de cifrado, integridad, intercambio de claves y autenticación.	Iniciador
2. Evaluación de propuestas	El receptor revisa las propuestas recibidas y las compara con su propia configuración para buscar una combinación compatible.	Receptor
3. Selección de la propuesta	Si el receptor encuentra una propuesta compatible, selecciona los parámetros acordados y responde al iniciador con la propuesta aceptada.	Receptor
4. Confirmación del acuerdo	El iniciador y el receptor confirman los parámetros seleccionados y establecen un acuerdo mutuo para los algoritmos y configuraciones a utilizar.	Ambos
5. Inicio del intercambio de claves	Una vez acordados los parámetros, ambas partes realizan el intercambio de claves (usualmente con Diffie-Hellman) para generar material de claves compartidas.	Ambos
6. Autenticación mutua	Ambas partes se autentican usando el método acordado (clave precompartida, certificados digitales o EAP).	Ambos

Tabla 4 Intercambio de propuestas IKE

Los dispositivos intercambian sus propuestas de seguridad a través de mensajes IKE.

Cada mensaje IKE contiene una o varias propuestas de seguridad, dependiendo de la configuración de los dispositivos.

En la relevancia del Proceso la confidencialidad se asegura que los datos intercambiados estén protegidos durante todo el proceso. La integridad le garantiza que los parámetros seleccionados no hayan sido alterados durante la negociación. La autenticidad Confirma que ambas partes son quienes dicen ser, evitando ataques de suplantación.

En las aplicaciones práctica se utilizan VPNs corporativas para interconectar oficinas de manera segura como VPNs corporativas para interconectar oficinas de manera segura, VPNs personales para proteger la privacidad del usuario al navegar por internet en las redes que requieren alta seguridad, como banca en línea y comunicaciones gubernamentales.

4.9.8 Autenticación de identidades

La autenticación de identidades en IKE es el proceso mediante el cual las partes involucradas (el iniciador y el receptor) verifican su identidad mutuamente antes de establecer una asociación de seguridad (Security Association, SA). Este paso es esencial para garantizar que las partes sean quienes dicen ser y para prevenir ataques como la suplantación de identidad o la interceptación maliciosa.

4.10 Proceso de Autenticación en IKE

a. Identificación de las partes

Ambas partes intercambian identificadores, que pueden ser direcciones IP, nombres de dominio, o identificadores personalizados.

Ejemplo: El iniciador puede presentarse como 10.1.1.1 y el receptor como vpn.company.com.

b. Demostración de identidad

Cada parte demuestra su identidad usando el método acordado:

Para PSK: Envían un hash derivado de la clave precompartida.

Para certificados: Presentan su certificado digital.

Para EAP: Realizan el intercambio según el protocolo EAP configurado.

c. Validación de autenticación

Las identidades se validan:

Con PSK, verificando el hash recibido.

Con certificados, verificando que el certificado sea válido y emitido por una CA confiable.

Con EAP, completando el flujo de autenticación definido (e.g., EAP-TLS).

d. Confirmación del proceso

La tabla 5 compara las características principales de las versiones **IKEv1** y **IKEv2** del protocolo Internet Key Exchange, que es clave en la negociación y establecimiento de túneles VPN seguros.

Si ambas partes validan correctamente la identidad del otro, el proceso de autenticación se considera exitoso.

En caso de error (e.g., PSK incorrecta, certificado no válido), la negociación falla.

Aspecto	IKEv1	IKEv2
Métodos soportados	PSK, Certificados	PSK, Certificados, EAP
Eficiencia	Más mensajes de intercambio	Proceso más simplificado
Escenarios avanzados	Limitado	Mejor soporte para autenticación remota
Flexibilidad	Menor	Más opciones, especialmente con EAP

Tabla 5 Autenticación en IKEv1 vs. IKEv2

Ventaja de IKEv2 sobre IKEv1: Supera a IKEv1 en eficiencia, flexibilidad y soporte para escenarios avanzados, haciéndolo más adecuado para las necesidades modernas de redes seguras. En el uso en la práctica IKEv1 Sigue siendo utilizado en sistemas más antiguos o cuando la compatibilidad con dispositivos más viejos es una prioridad, mientras IKEv2 es el estándar preferido para nuevas

implementaciones de VPN debido a su mejor desempeño, seguridad y compatibilidad con tecnologías modernas.

4.11 Establecimiento de asociaciones de seguridad (SA)

Finalmente, se establecen las asociaciones de seguridad (SA) que definirán cómo se protegerá el tráfico de datos IPsec.

Estas SA incluyen información sobre los parámetros de seguridad acordados, las claves de sesión compartidas y las direcciones IP de origen y destino.

a) Selección de propuestas:

Cada dispositivo selecciona las recomendaciones de seguridad que mejor se adaptan a sus políticas y preferencias de seguridad. Si los dispositivos no pueden ponerse de acuerdo sobre los parámetros de seguridad, la negociación falla y no se puede establecer la conexión.

b) Autenticación de identidades:

Después de acordar los parámetros de seguridad, los dispositivos autentican sus identidades mutuas para garantizar que solo los dispositivos autorizados puedan establecer la conexión segura.

Se utilizan métodos de autenticación fuertes, como certificados digitales o precompartidos (PSK), para realizar esta autenticación.

c) Generación de claves de sesión:

La generación de claves de sesión en IKE (Internet Key Exchange) es un paso crucial que ocurre una vez que se han acordado los parámetros de seguridad y se ha completado la autenticación de identidades entre dos dispositivos IPsec.

La generación de claves de sesión en IKE es un proceso crítico que permite a dos dispositivos IPsec establecer una conexión segura y proteger el tráfico de datos utilizando claves de sesión compartidas derivadas mediante el intercambio de

claves Diffie-Hellman. Este proceso garantiza una comunicación segura y confiable entre los dispositivos en una red Ipsec

4.12 Intercambio de claves Diffie-Hellman

La tabla 6 describe el proceso de **intercambio de claves Diffie-Hellman (DH)** en el protocolo IKE, detallando las fases principales, su descripción y los mensajes correspondientes utilizados durante la negociación. Este proceso es crucial para establecer una clave secreta compartida entre dos partes de manera segura.

Fase	Descripción	Mensajes IKE
Intercambio de parámetros DH	El iniciador envía su valor público DH (g^a mod p), y el receptor hace lo mismo con su valor público DH (g^b mod p).	**Mensaje 1** y **Mensaje 2** (IKEv1 o IKEv2)
Cálculo de la clave compartida	Ambas partes calculan la clave secreta compartida a partir de los valores públicos recibidos de la otra parte.	Después de recibir los valores públicos DH.
Confirmación de la clave compartida	Una vez que ambas partes calculan la clave secreta, la comunicación se cifra utilizando esta clave para proteger el resto del proceso de autenticación.	Mensaje de autenticación y establecimiento de SA.

Tabla 6 Proceso de Intercambio de Claves Diffie-Hellman en IKE

Este proceso es utilizado con VPNs son para establecer túneles seguros entre dispositivos como los protocolos de seguridad como IPSec, TLS, y SSH. Cualquier sistema que requiera establecer claves dinámicas sin un canal seguro previo.

IKE utiliza el intercambio de claves Diffie-Hellman para generar claves de sesión compartidas que se utilizarán para proteger el tráfico de datos IPsec.

Durante este cambio:

- Cada dispositivo genera su propio par de claves pública/privada Diffie-Hellman.
- Cada dispositivo envía su clave pública Diffie-Hellman al otro dispositivo.

- Cada dispositivo utiliza la clave pública del otro dispositivo junto con su propia clave privada para generar una clave de sesión compartida.

La tabla 7 presenta las ventajas y desventajas del uso del Intercambio de Claves Diffie-Hellman (DH), que es un método ampliamente utilizado para establecer claves compartidas en comunicaciones seguras. Aquí está la explicación detallada:

Ventaja	Desventaja
Establece una clave secreta sin necesidad de transmitirla.	Requiere de más recursos computacionales, especialmente con grupos grandes.
Alta seguridad, incluso en canales inseguros.	Sensible a ataques de intermediarios si no se autentican correctamente las identidades.
Flexible, compatible con diferentes tamaños de clave y métodos de autenticación.	Vulnerable si se utilizan grupos de Diffie-Hellman pequeños o débiles.

Tabla 7 Ventajas y Desventajas de Diffie-Hellman en IKE

4.12.1 Autenticación de pares

a) Inicio de la negociación

El proceso de autenticación comienza cuando dos dispositivos IPsec desean establecer una conexión segura entre sí.

b) Intercambio de mensajes IKE:

El dispositivo inicia un intercambio de mensajes IKE para negociar parámetros de seguridad y establecer una conexión segura.

c) Propuesta de métodos de autenticación:

Durante el proceso de negociación, la organización ofrece métodos de validación que pueden incluir:

- Autenticación de precompartida (Pre-Shared Key, PSK).
- Autenticación mediante certificados digitales (RSA, DSA, etc.).

d) **Selección del método de autenticación:**

Los dispositivos acuerdan un método de autenticación que sea compatible entre ellos.

e) **Autenticación de identidades:**

- **Autenticación de precompartida (PSK):**

  Si se utiliza autenticación previamente compartida, el dispositivo debe conocer la clave compartida previamente negociada. Cada dispositivo envía su identidad junto con un código hash basado en la clave previamente compartida. El otro dispositivo utiliza su copia de la clave previamente compartida para verificar el valor hash.

- **Autenticación mediante certificados digitales:**

  Si se utiliza autenticación mediante certificados digitales, cada dispositivo presenta su certificado digital durante la negociación.

  El otro dispositivo verifica la autenticidad del certificado utilizando una autoridad de certificación (CA) confiable.

f) **Verificación de identidades:**

Cada dispositivo verifica la identidad del otro dispositivo utilizando el método de autenticación acordado. Esto garantiza que solo los dispositivos autorizados puedan establecer la conexión segura.

g) **Generación de claves de sesión:**

Una vez que se ha completado la autenticación de pares, IKE genera claves de sesión compartidas que se utilizarán para proteger el tráfico de datos IPsec.

h) Establecimiento de asociaciones de seguridad (SA):

Finalmente, se establecen las asociaciones de seguridad (SA) que definirán cómo se protegerá el tráfico de datos IPsec.

Estas SA incluyen información sobre los parámetros de seguridad acordados, las claves de sesión compartidas y las direcciones IP de origen y destino.

4.12.2 Modos de operación

IKE puede funcionar en dos modos:

- Modo principal: En este modo, se negocian todos los parámetros de seguridad y se autentican las identidades de los pares en un intercambio de tres mensajes.
- Modo rápido (agresivo): En este modo, se reduce el número de mensajes intercambiados para establecer la conexión, lo que lo hace más rápido que el modo principal.

La tabla 8 compara los modos de operación del protocolo IKE (Internet Key Exchange), que son configuraciones utilizadas para establecer túneles VPN. A continuación, se explica cada modo de operación y sus características.

Modo de Operación	Descripción	Características	Ventajas	Desventajas
Modo Main (Principal)	El modo más seguro, donde la autenticación y el intercambio de claves ocurren en múltiples pasos, proporcionando más privacidad. El proceso de negociación involucra tres fases.	- Usa tres intercambios de mensajes. - Más seguro porque los valores de las claves no se revelan completamente.	- Alta seguridad. - Menos riesgo de ataques de intermediarios (Man-in-the-Middle). - Protege mejor la privacidad.	- Requiere más tiempo y recursos debido al número de intercambios de mensajes. - Más lento que el modo agresivo.

Modo de Operación	Descripción	Características	Ventajas	Desventajas
Modo Aggressive (Agresivo)	Un modo más rápido que realiza la negociación en solo tres mensajes, pero con menor privacidad. A pesar de ser rápido, la autenticación y los intercambios de claves son más expuestos.	- Usa solo tres intercambios de mensajes. - La información de las claves es más fácilmente accesible a los atacantes en comparación con el modo principal.	- Rápido y eficiente en términos de tiempo. - Menos recursos requeridos. - Utilizado cuando se requiere una conexión rápida.	- Menor seguridad debido a la exposición de las identidades en los intercambios iniciales. - Más susceptible a ataques Man-in-the-Middle.
Modo de Intercambio de Claves (IKEv2)	Mejorado en IKEv2, con una negociación más eficiente y flexible, utilizando solo dos intercambios de mensajes. Compatible con mecanismos de autenticación avanzados como EAP.	- Menos mensajes y más eficiente que IKEv1. - Soporta más métodos de autenticación (PSK, certificados, EAP).	- Mejor eficiencia y menor latencia. - Mejor gestión de errores y recuperación. - Más flexible con autenticación y configuraciones.	- Requiere que ambas partes soporten IKEv2. - Mayor complejidad en la configuración.

Tabla 8 Modo Main (Principal) y Modo Aggressive (Agresivo).

Versiones:

- IKEv1: Es la versión original del protocolo IKE. Utiliza dos fases para establecer conexiones seguras.
- IKEv2: Es la versión más reciente y mejorada del protocolo IKE. Ofrece una mejor eficiencia, capacidad de recuperación y soporte para la movilidad de dispositivos.

La tabla compara los modos de operación del protocolo IKE (Internet Key Exchange) y destaca sus recomendaciones de uso, eficiencia y nivel de seguridad. A continuación, se explica cada fila en detalle:

Modo de Operación	Recomendado para	Eficiencia	Seguridad
Modo Principal	Entornos donde la seguridad es una prioridad alta.	Bajo (más mensajes, más tiempo).	Alta, con protección adicional de las identidades.
Modo Agresivo	Conexiones rápidas donde la latencia es importante.	Alta (menos mensajes).	Menor (posible exposición a ataques Man-in-the-Middle).
Modo IKEv2	Redes modernas que requieren eficiencia y flexibilidad.	Alta (menos mensajes, más eficiente).	Alta (con mejores mecanismos de autenticación y recuperación).

Tabla 9 Resumen de los Modos de Operación

.

4.12.3 Resumen del proceso con un ejemplo

a) Definición de los parámetros de seguridad:

En la imagen 8.3 se definen los parámetros de seguridad, como algoritmos de cifrado, algoritmos de integridad y métodos de autenticación.

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
crypto isakmp key mySharedKey address 203.0.113.1
```

Imagen 8-3 configuración de ISAKMP

Este es un fragmento de configuración de ISAKMP (Internet Security Association and Key Management Protocol), que se utiliza para configurar una política de seguridad para establecer un túnel IPsec, utilizando AES para el cifrado, autenticación basada

en clave precompartida y un grupo Diffie-Hellman 2 para el intercambio de claves. La clave precompartida es mySharedKey y la dirección IP del peer es 203.0.113.1

b) Configuración de las CryptoMaps

Se configura una CryptoMap como se observa en la imagen 9.3 que define cómo se aplicarán los parámetros de seguridad a los paquetes que pasan a través del dispositivo. Definición de las ACL (Listas de Control de Acceso):

```
crypto ipsec transform-set myTransformSet esp-aes esp-sha-hmac
crypto map myCryptoMap 10 ipsec-isakmp
 set peer 203.0.113.1
 set transform-set myTransformSet
 match address 100
```

Imagen 9-3 configuración relacionada con IPsec

En esta imagen 10.3 se muestra una configuración relacionada con IPsec. Se crea un transform-set llamado myTransformSet que utiliza ESP con AES para cifrado y SHA-HMAC para la integridad de los datos. Luego, se configura un crypto map llamado myCryptoMap con ID 10 para establecer una relación de seguridad con un peer en la dirección IP 203.0.113.1. Además, se asigna el transform-set myTransformSet a la política de seguridad y se define un filtro de tráfico mediante la lista de acceso 100

c) Asignación de la CryptoMap a la interfaz:

```
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Imagen 10-3 Access Control List (ACL)

Este comando configura una lista de acceso extendida numerada (ACL 100) que permite cualquier tráfico IP desde la red 192.168.1.0/24 hacia la red 192.168.2.0/24.

d) Negociación de seguridad IKE (Internet Key Exchange):

La imagen 11.3 muestra un fragmento de configuración en un router o dispositivo de red, donde se asigna un mapa criptográfico (crypto map) a una interfaz específica. Esto es común en configuraciones de VPN basadas en IPsec en equipos de red.

La CryptoMap se asigna a la interfaz a través de la cual se enviará el tráfico protegido.

```
interface FastEthernet0/0
 crypto map myCryptoMap
```

Imagen 11-3 habilita la configuración de IPsec VPN utilizando el mapa criptográfico llamado

El comando crypto map myCryptoMap en la interfaz FastEthernet0/0 activa la funcionalidad IPsec VPN sobre esta interfaz para cifrar y proteger el tráfico.

e) Establecimiento de las asociaciones de seguridad (SA):

En la imagen 12.3 se visualiza cuando se envía tráfico desde la red local 192.168.1.0/24 a la red remota 192.168.2.0/24, los dispositivos de red negocian los parámetros de seguridad utilizando IKE.

```
R1(config)# crypto isakmp key mySharedKey address 203.0.113.1
```

Imagen 12-3 comando que define una clave precompartida

Este comando configura una clave precompartida para la autenticación en una VPN IPsec. La clave se utiliza durante la Fase 1 de ISAKMP/IKE para autenticar y establecer confianza entre los dos dispositivos (routers, firewalls, etc.) que forman el túnel.

f) Transmisión segura de datos:

En la imagen 13.3 revisamos el comando y salida mostrados corresponden a la verificación de las Asociaciones de Seguridad (Security Associations, SAs) en el contexto de una conexión VPN configurada con IPsec e IKE. Este comando es esencial para diagnosticar y comprobar el estado de las negociaciones ISAKMP (Internet Security Association and Key Management Protocol).

IKE establece las asociaciones de seguridad (SA) entre los dispositivos de red para proteger el tráfico que pasa entre las dos redes locales.

```
R1#show crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst             src             state          conn-id    status
203.0.113.1     192.0.2.1       QM_IDLE          1001      ACTIVE
```

Imagen 13-3 Salida de un comando ejecutado en un dispositivo de red

Esta salida indica que existe una conexión ISAKMP activa entre dos dispositivos (203.0.113.1 y 192.0.2.1) y que se encuentra en estado QM_IDLE, lo que significa que el intercambio de claves y la negociación del túnel VPN han sido exitosos.

g) **Transmisión segura de datos:**

En la imagen 14.3 revisamos el comando show crypto ipsec sa muestra información sobre las Asociaciones de Seguridad IPsec (IPsec SAs) activas en un dispositivo de red. Estas SAs se utilizan para cifrar y descifrar datos en túneles VPN. Aquí se explica cada parte de la salida mostrada:

Los datos entre las dos redes locales se transmiten de manera segura a través de Internet, protegidos por IPsec y las políticas de seguridad definidas en la Cryptomap

```
R1#show crypto ipsec sa

interface: FastEthernet0/0
   Crypto map tag: myCryptoMap, local addr. 192.0.2.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
  current_peer 203.0.113.1 port 500
    PERMIT, flags={origin_is_acl,}

    #pkts encaps: 203, #pkts encrypt: 203, #pkts digest: 203
    #pkts decaps: 203, #pkts decrypt: 203, #pkts verify: 203
```

Imagen 14-3 verificar el estado de las asociaciones de seguridad IPsec

Esta salida confirma que el túnel IPsec está funcionando correctamente. Los contadores de paquetes indican tráfico bidireccional con cifrado y descifrado exitosos entre los rangos de red local (192.168.1.0/24) y remota (192.168.2.0/24). El túnel está asociado con el par remoto 203.0.113.1.

Se definen los parámetros de seguridad, se crea una CryptoMap y se asigna a la interfaz de salida.

Se negocian los parámetros de seguridad IKE y se establecen las asociaciones de seguridad (SA) entre los dispositivos.

El tráfico entre las dos redes locales se transmite de manera segura a través de Internet, protegido por IPsec y las políticas de seguridad definidas en la CryptoMap.

4.13 Multipoint Generic Routing Encapsulation (mGRE):

4.13.1 Definición:

mGRE es una técnica que permite crear túneles GRE entre múltiples puntos en una red. Permite que múltiples túneles GRE se creen entre los mismos puntos, lo que proporciona una forma eficiente de conectar múltiples sitios remotos.

4.13.2 Características:

Permite que un solo túnel GRE transporte tráfico entre múltiples sitios.

Reduce la sobrecarga de la red al evitar la necesidad de crear un túnel GRE separado para cada par de sitios.

4.13.3 Beneficios:

Escalabilidad: Permite conectar múltiples sitios remotos de manera eficiente.

Eficiencia: Reduce la sobrecarga de la red al compartir un solo túnel GRE entre múltiples sitios.

4.13.4 Uso:

Se utiliza en redes donde múltiples sitios necesitan comunicarse entre sí de manera eficiente, como en redes de sucursales de empresas.

4.14 Dynamic Multipoint VPN (DMVPN):

4.14.1 Definición:

DMVPN es una tecnología de VPN que utiliza mGRE, IPsec y NHRP (Next Hop Resolution Protocol) para crear conexiones VPN dinámicas entre múltiples sitios remotos sin la necesidad de configurar túneles VPN punto a punto.

4.14.2 Componentes:

mGRE: Permite la creación de túneles GRE entre múltiples puntos.

NHRP: Proporciona la resolución dinámica de la próxima dirección de salto, lo que permite a los dispositivos encontrar rutas a través de la red VPN.

IPsec: Proporciona seguridad al cifrar y autenticar el tráfico de la VPN.

4.14.3 Características:

Permite la creación dinámica de túneles VPN entre sitios remotos.

Optimiza el uso de ancho de banda al establecer túneles VPN solo cuando sea necesario.

4.14.4 Beneficios:

Escalabilidad: Permite que una red VPN crezca fácilmente agregando nuevos sitios remotos.

Flexibilidad: Los túneles VPN se establecen dinámicamente según sea necesario, lo que optimiza el uso de recursos de red.

4.14.5 Uso:

Se utiliza en redes empresariales para conectar múltiples sucursales de manera eficiente y segura sobre Internet.

5. Materiales y metodología

Requerimientos Previos

Antes de iniciar la práctica, es necesario tener los siguientes elementos instalados y configurados:

1. **GNS3** (última versión).
2. **Wireshark** para capturar y analizar tráfico de red.
3. **Imágenes de routers compatibles con VPN** (pueden ser Cisco, VyOS o Virtualbox con Ubuntu).
4. **Clientes y servidores** que puedan ejecutar clientes VPN (pueden ser máquinas virtuales o nodos simulados en GNS3).
5. **Herramientas de prueba de red**, como **iPerf** o **Ping** para medir el rendimiento.

5.1 VPN IPsec (Internet Protocol Security)

IPsec es uno de los protocolos más seguros y ampliamente utilizados para redes corporativas. Funciona a nivel de capa de red (capa 3 del modelo OSI) y asegura el tráfico de IP a través de cifrado, autenticación y verificación de la integridad de los datos.

La imagen 15.4 muestra cómo se encapsulan los datos en una comunicación protegida mediante **IPsec (Internet Protocol Security)**, que opera a nivel de red para garantizar la seguridad de los paquetes IP. En esta representación, se destacan las capas del modelo de red implicadas en el proceso de encapsulación y el rol que desempeña cada una.

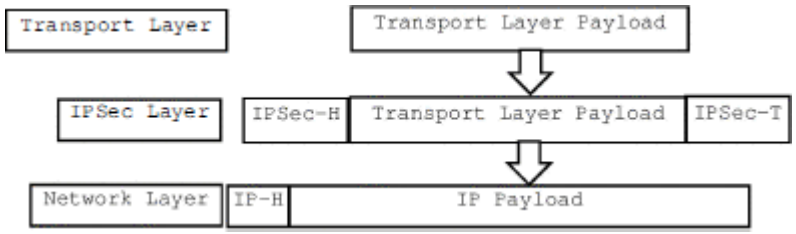


Imagen 15-4 Protocolo de seguridad IPsec

***Fuente**: Application Specific Tunneling Protocol Selection for Virtual Private Networks*

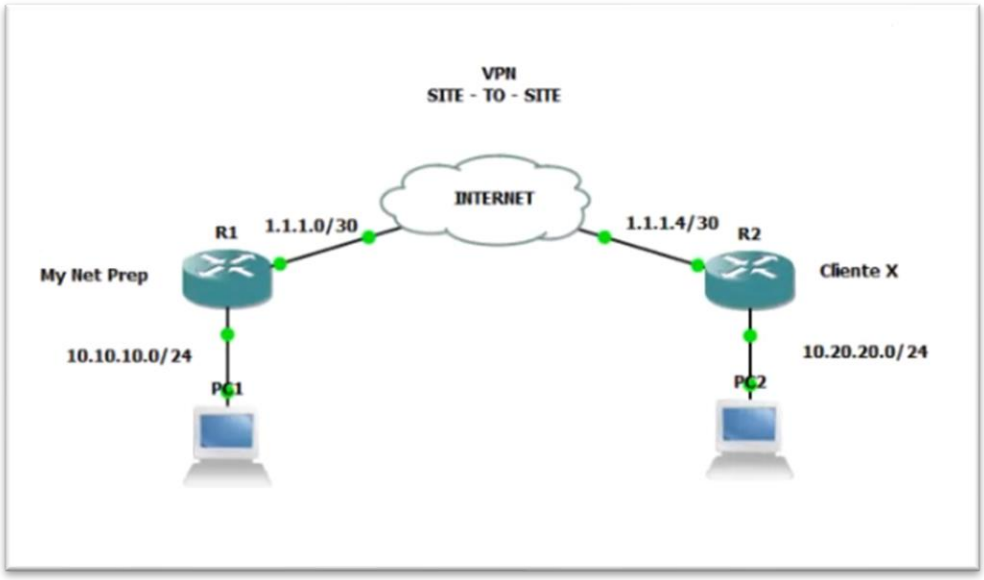
El diagrama refleja cómo IPsec agrega capas de seguridad a los paquetes IP en las comunicaciones de red. Cada capa desempeña un papel en la encapsulación, cifrado y autenticación del tráfico, garantizando que los datos transmitidos sean seguros y confiables. Este enfoque lo hace ideal para proteger comunicaciones en VPNs y otras redes seguras.

5.1.1 Utilidad de herramientas

- **GNS3**: Para simular los dispositivos de red y las conexiones.
- **Wireshark**: Para capturar y analizar el tráfico que fluye a través del túnel VPN IPsec.
- **Ping e Iperf**: Para probar la conectividad y el rendimiento del túnel VPN.

5.2 VPN IPsec (Internet Protocol Security) Site to site

La imagen 16.4 representa la arquitectura de una VPN Site-to-Site, un método utilizado para conectar dos redes locales ubicadas en diferentes lugares geográficos a través de internet. A continuación, se explican los elementos y el funcionamiento de esta configuración:



La topología de red para la simulación en GNS3 consta de:

- Router Sucursal 1: Conectado a la LAN de la sucursal 1.
- Router Sucursal 2: Conectado a la LAN de la sucursal 2.
- Internet Simulado: Un enlace WAN entre los routers de las sucursales para representar la conexión a través de Internet.
- LAN 1 y LAN 2: Redes internas de cada sucursal, donde los dispositivos de ambas LAN podrán comunicarse de forma segura mediante la VPN IPsec Site-to-Site.

Imagen 16-4 topología de Red en GNS3

La imagen17.4 muestra una serie de comandos configurados en un router (R1) en el modo CLI (Command Line Interface). Estos comandos configuran una interfaz de red en el router.

Imagen 17- 4 Configuración de IP. ROUTER 1

R1(config)#interface fastEthernet 0/0
R1(config-if)#ip add
R1(config-if)#ip address 1.1.1.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#c

Esta configuración es parte de la activación y preparación de una interfaz FastEthernet 0/0. El administrador asigna una dirección IP válida para una subred /30, típica en escenarios de conexión punto a punto (por ejemplo, entre routers). La interfaz se habilita con el comando no shutdown.

La imagen 18.4 Demuestra que el router está configurado correctamente para utilizar la interfaz FastEthernet 0/0 con la dirección IP 1.1.1.1/30. Esta configuración básica es común en enlaces WAN o conexiones entre dispositivos de red. El administrador podría necesitar realizar configuraciones adicionales, como agregar un Gateway o configurar rutas estáticas o dinámicas para que el tráfico fluya correctamente.

Imagen 18- 4 Dirección privada

R1(config)#
R1(config)#interface fa
R1(config)#interface fastEthernet 0/1
R1(config-if)#ip address 10.10.10.1 255.255.255.0
R1(config-if)# No shutdown

El administrador está configurando la interfaz FastEthernet 0/1 con la dirección IP 10.10.10.1/24. Sin embargo, la interfaz no estará activa hasta que se ejecute el comando no shutdown, lo que significa que no enviará ni recibirá tráfico.

Para completar esta configuración, el administrador debe ejecutar el comando como se observa en la imagen 18.4 no shutdown para habilitar la interfaz. Esto es un paso obligatorio si se espera que la interfaz funcione correctamente en una red operativa. Además, se podrían agregar rutas u otras configuraciones adicionales según los requisitos del entorno de red.

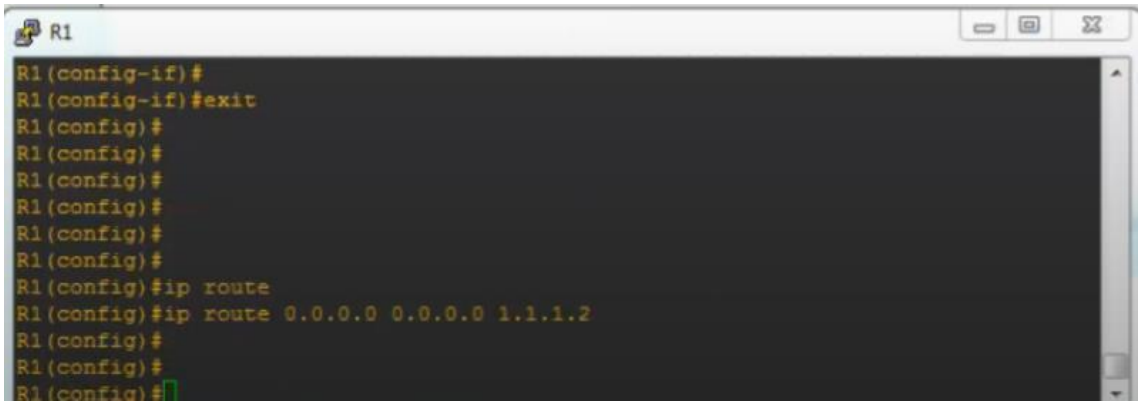


Imagen 18-4 Insertar ruta por defecto

```
R1(config-if)#exit
R1(config)#
R1(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.2
R1(config)#
```

La configuración indica que todo el tráfico destinado a redes no específicas será enviado al siguiente salto 1.1.1.2. Esto se conoce como **ruta por defecto** y es esencial en redes pequeñas o routers que actúan como bordes conectados a Internet.

En la imagen 20.4 se observa que el router ahora tiene configurada una ruta por defecto para enrutar tráfico hacia el siguiente salto 1.1.1.2. Es importante asegurarse de que 1.1.1.2 sea accesible y esté configurado correctamente para manejar el tráfico. Si hay problemas de conectividad, se deberá verificar la conexión física, las interfaces, y las rutas en el siguiente salto.

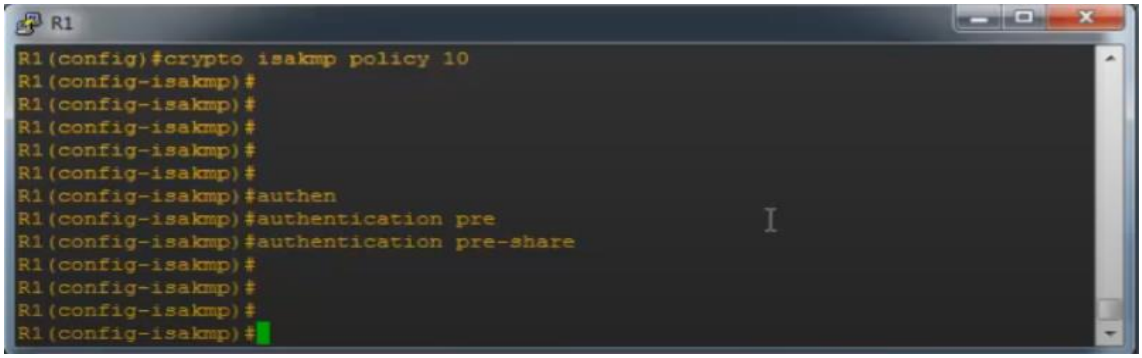


Imagen 20-4 Creación de llaves compartidas

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#
R1(config-isakmp)#authen
R1(config-isakmp)#authentication pre
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#
```

a) **Comando para crear una política ISAKMP**:
   - **crypto isakmp policy 10**:
     - Crea una política ISAKMP con un número de prioridad de 10.
     - ISAKMP (Internet Security Association and Key Management Protocol) se utiliza para negociar parámetros de seguridad durante la fase 1 del establecimiento de un túnel IPsec.

b) **Configuración del método de autenticación**:
   - **authentication pre**:
     - Intenta escribir el comando para configurar el método de autenticación, pero no está completo.
   - **authentication pre-share**:
     - Especifica que el método de autenticación será mediante una clave precompartida (Pre-Shared Key). Este es uno de los métodos más comunes para establecer túneles IPsec debido a su simplicidad.

c) **Prioridad de la política (10)**:

El número 10 representa la prioridad de esta política ISAKMP. Los números más bajos tienen mayor prioridad, y esta política será evaluada antes que otras con números de prioridad más altos.

d) **Autenticación pre-share**:

- Este método utiliza una clave precompartida que debe configurarse en ambos extremos del túnel. Es más sencillo de implementar que otros métodos, como RSA, pero menos seguro para implementaciones de gran escala o sensibles.

El router ahora tiene configurada una política ISAKMP con el método de autenticación Pre-Shared Key (PSK). Sin embargo, para completar esta configuración, el administrador necesitará:

- Configurar la clave precompartida con el comando crypto isakmp key.
- Configurar otros parámetros importantes, como el algoritmo de cifrado, el algoritmo de hash y el grupo Diffie-Hellman.

Este es un paso inicial para establecer un túnel IPsec exitoso.

La imagen 21.4 muestra una terminal de configuración de un router, específicamente en el contexto de la configuración de un protocolo de seguridad para redes privadas virtuales (VPN) utilizando **ISAKMP (Internet Security Association and Key Management Protocol)**. Este protocolo se usa para negociar, establecer, modificar y eliminar asociaciones de seguridad (SA) en una VPN.

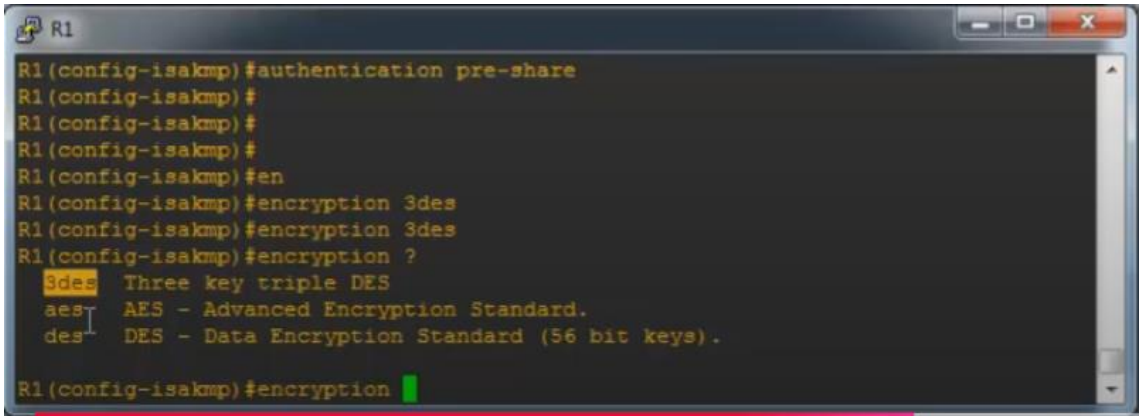


Imagen 21-4 Uso de algoritmo de encriptación

```
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#
```

```
R1(config-isakmp)#en
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#encryption ?
  3des     Three key triple DES
  aes      AES - Advanced Encryption Standard
  des      DES - Data Encryption Standard (56 bit keys).

R1(config-isakmp)#encryption
```

La configuración muestra el proceso de selección del algoritmo de cifrado dentro de una política ISAKMP. En este caso, se está considerando el uso de 3DES como algoritmo de cifrado, aunque el administrador podría optar por AES, ya que es más seguro y eficiente.

El algoritmo de cifrado como se ve en La imagen 22.4 es un elemento crucial en la configuración de políticas ISAKMP para asegurar la confidencialidad de los datos durante las negociaciones de IPsec. Es recomendable utilizar AES en lugar de 3DES o DES, dado que es el estándar actual en seguridad. El administrador deberá completar esta configuración y definir otros parámetros necesarios para la política ISAKMP

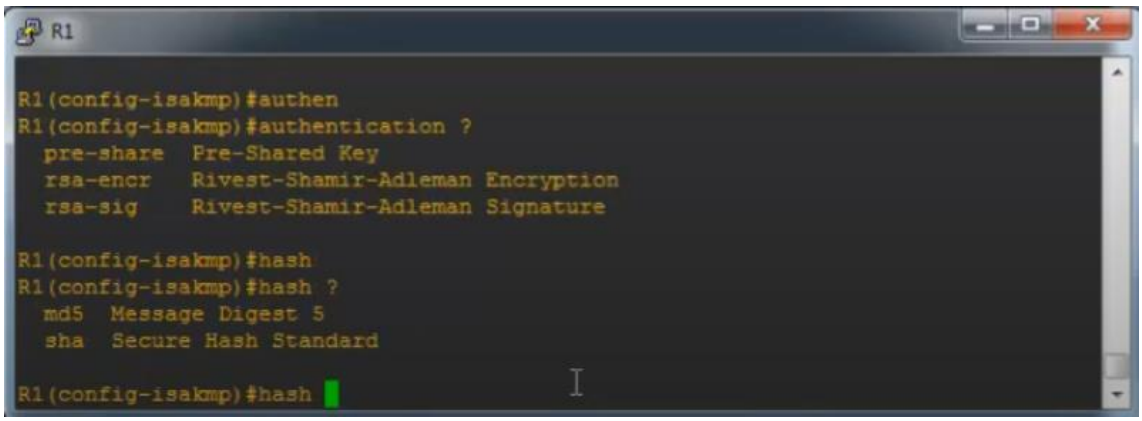


Imagen 22-4 Configuración de los parámetros de autenticación

```
R1(config-isakmp)#authen
R1(config-isakmp)#authentication ?
  pre-share      Pre-Shared Key
  rsa-encr       Rivest-Shamir-Adleman Encryption
  rsa-sig        Rivest-Shamir-Adleman Signature
```

```
R1(config-isakmp)#hash
R1(config-isakmp)#hash ?
  md5          Message Digest 5
  sha          Secure Hash Standard

R1(config-isakmp)#hash
```

El administrador está configurando parámetros clave dentro de una política ISAKMP:

- Está considerando usar **Pre-Shared Key (PSK)** como método de autenticación.
- Tiene la opción de elegir entre los algoritmos de hash MD5 y SHA, siendo **SHA** la opción más segura y preferida en redes modernas.

- Es recomendable elegir **SHA** como algoritmo de hash por su mayor seguridad en comparación con MD5.
- La autenticación mediante **Pre-Shared Key** es adecuada para configuraciones simples o de pequeña escala, pero para mayor seguridad en entornos más grandes, sería mejor considerar opciones como RSA.

La configuración debe completarse definiendo el algoritmo de hash y, si es necesario, otros parámetros adicionales para que la política ISAKMP esté completamente operativa.

La imagen 23.4 muestra una continuación de la configuración del protocolo **ISAKMP** en un router, específicamente seleccionando el algoritmo de hash para garantizar la integridad de los datos y preparándose para configurar otros parámetros relacionados con la seguridad.

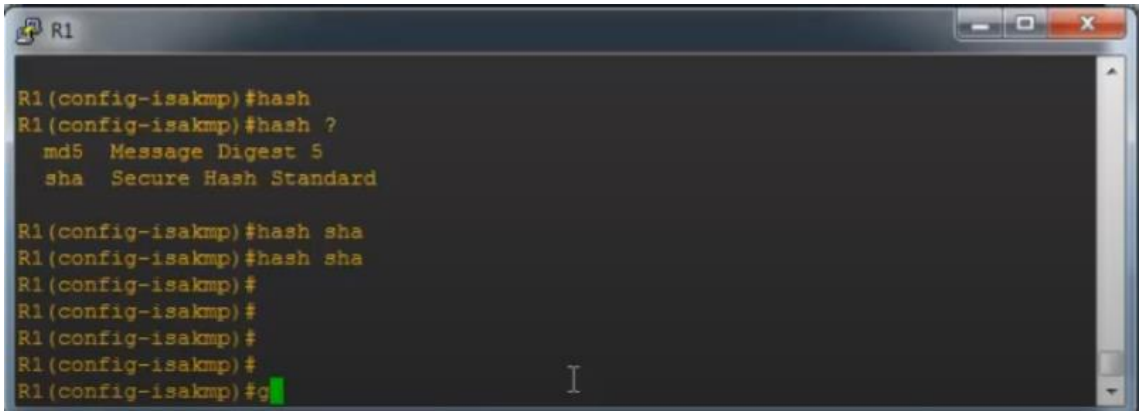


Imagen 23-4 Confidencialidad de datos

```
R1(config-isakmp)#hash
R1(config-isakmp)#hash ?
  md5           Message Digest 5
  sha           Secure Hash Standard

R1(config-isakmp)#hash sha
R1(config-isakmp)#hash sha
R1(config-isakmp)#
R1(config-isakmp)#g
```

La configuración está estableciendo el algoritmo de hash **SHA** en la política ISAKMP actual, lo que es una buena práctica para garantizar la integridad y seguridad en las comunicaciones. La selección de SHA indica que el administrador está siguiendo estándares modernos de seguridad.

SHA es la mejor elección para el algoritmo de hash en esta configuración debido a su robustez frente a vulnerabilidades y para completar la política ISAKMP, el administrador deberá:

- Configurar el grupo Diffie-Hellman con el comando group.
- Asegurarse de incluir otros parámetros necesarios, como cifrado, autenticación, y tiempo de vida de la política.

La configuración está en progreso y debería completarse para garantizar la funcionalidad del túnel IPsec.

La imagen 24.4 muestra la configuración de un grupo de Diffie-Hellman dentro del modo de configuración de ISAKMP en un router. Este paso es esencial en la negociación de claves seguras para una conexión VPN, ya que Diffie-Hellman (DH) permite a las partes intercambiar claves de forma segura incluso en una red insegura.

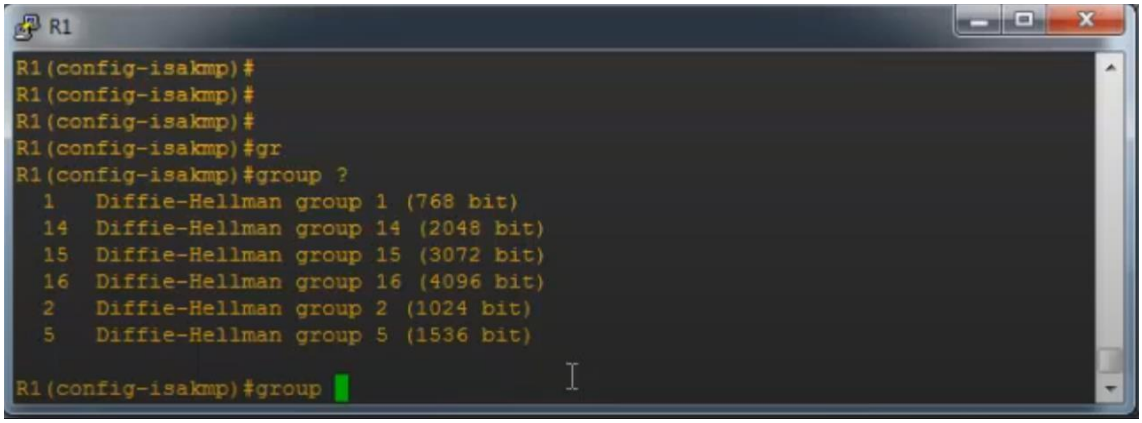


Imagen 24-4 Generación de claves compartidas

R1(config-isakmp)#gr
R1(config-isakmp)#group ?
1 Diffie-Hellman group 1 (768 bit)
14 Diffie-Hellman group 14 (2048 bit)
15 Diffie-Hellman group 15 (3072 bit)
16 Diffie-Hellman group 16 (4096 bit)
2 Diffie-Hellman group 2 (1024 bit)
5 Diffie-Hellman group 5 (1536 bit)

R1(config-isakmp)#group

El administrador está configurando el grupo Diffie-Hellman dentro de la política ISAKMP. Este grupo define la longitud de la clave y el nivel de seguridad en el intercambio de claves durante la fase 1.

Recomendación: Seleccionar grupo 14 (2048 bits), ya que ofrece un balance adecuado entre seguridad y rendimiento. Para configuraciones que requieren máxima seguridad, se podrían utilizar los grupos 15 o 16, aunque esto podría impactar en el rendimiento debido al mayor uso de recursos.

Es importante completar este paso como se revisa en la imagen 25.4 y revisar la política ISAKMP en su totalidad para garantizar la correcta implementación de un túnel IPsec seguro.

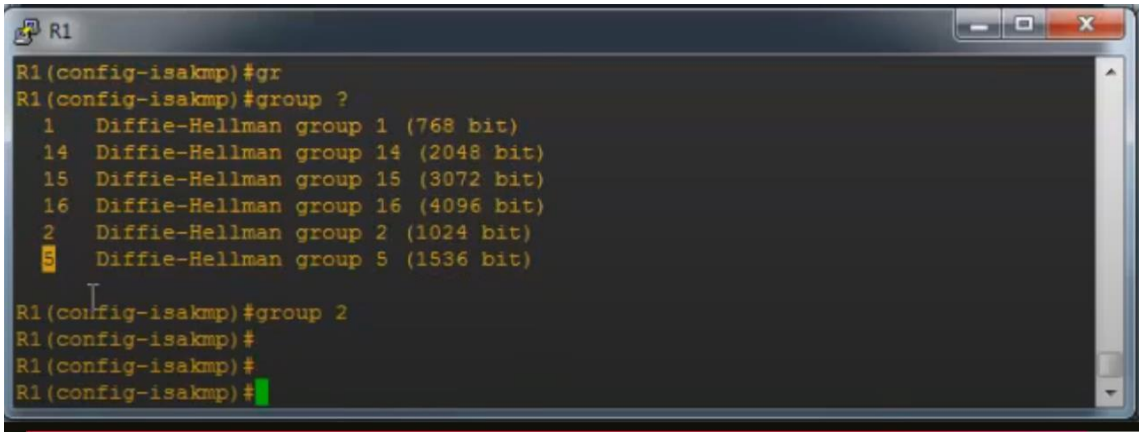


Imagen 25-4 Obtención de Diffie-Hellman grupo 2 site to site

```
R1(config-isakmp)#gr
R1(config-isakmp)#group ?
  1   Diffie-Hellman group 1 (768 bit)
  14  Diffie-Hellman group 14 (2048 bit)
  15  Diffie-Hellman group 15 (3072 bit)
  16  Diffie-Hellman group 16 (4096 bit)
  2   Diffie-Hellman group 2 (1024 bit)
  5   Diffie-Hellman group 5 (1536 bit)

R1(config-isakmp)#group 2
R1(config-isakmp)#
```

La configuración establece el uso del **grupo Diffie-Hellman 2** en la política ISAKMP. Aunque funcional, este grupo no es la opción más segura según los estándares modernos, ya que los grupos con claves más largas (como 14, 15 o 16) son más robustos frente a ataques.

Una recomendación es mejor utilizar **grupo 14 (2048 bits)** o superior para garantizar un nivel de seguridad adecuado, especialmente en redes expuestas a internet. El **grupo 2** puede ser adecuado en entornos más controlados o donde el hardware tiene limitaciones, pero no es lo ideal para redes modernas.

Es importante completar la configuración con otros parámetros necesarios para que la política ISAKMP esté completamente operativa.

La imagen 26.4 muestra la configuración de un conjunto de transformaciones (transform-set) en **IPSec** dentro de un router. Este conjunto de transformaciones define cómo se cifrarán, autenticarán y/o comprimirá el tráfico en un túnel VPN.

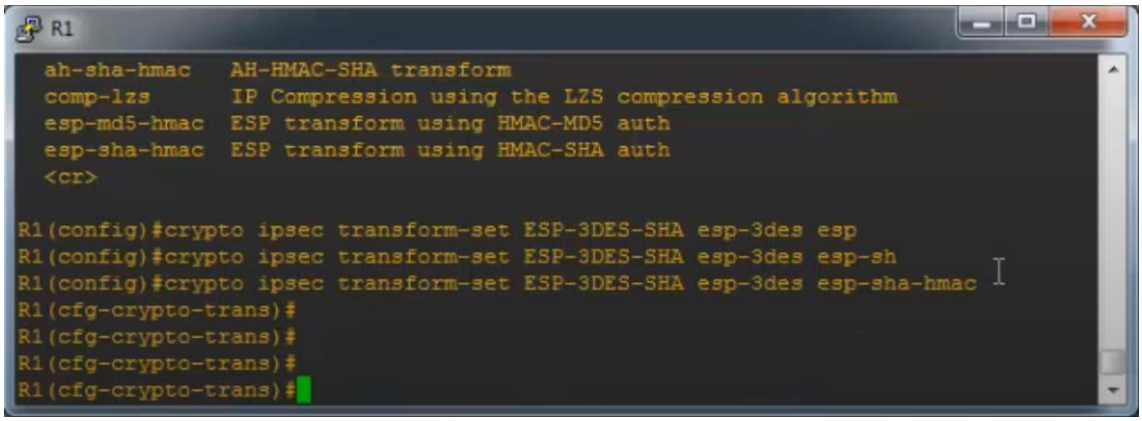


Imagen 26-4 Obtención de Diffie-Hellman grupo 2 site to site

ah-sha-hmac AH-HMAC-SHA transform
comp-lzs IP Compression using the LZS compression algorithm
esp-md5-hmac ESP transform using HMAC-MD5 auth
esp-sha-hmac ESP transform using HMAC-SHA auth
<cr>

R1(config)#crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
R1(cfg-crypto-trans)#

El transform-set ESP-3DES-SHA se configura para utilizar:

- ESP como protocolo.
- 3DES para cifrado.
- HMAC-SHA para autenticación.

Esto significa que el tráfico entre los puntos del túnel IPsec estará cifrado y autenticado utilizando estos algoritmos.

La configuración es funcional y utiliza 3DES y HMAC-SHA, que son algoritmos robustos. Sin embargo, en redes modernas, se recomienda usar AES para cifrado debido a su mayor seguridad y eficiencia.

El transform-set debe ser aplicado en un mapa de cifrado (crypto map) para que se active en el túnel IPsec.

Es recomendable que el administrador revise la compatibilidad con el dispositivo remoto para garantizar que ambos extremos soporten los mismos algoritmos configurados.

La imagen 27.4 muestra la configuración básica de una interfaz en un router identificado como R2. Se realizan configuraciones de red esenciales para habilitar la interfaz y asignarle una dirección IP.

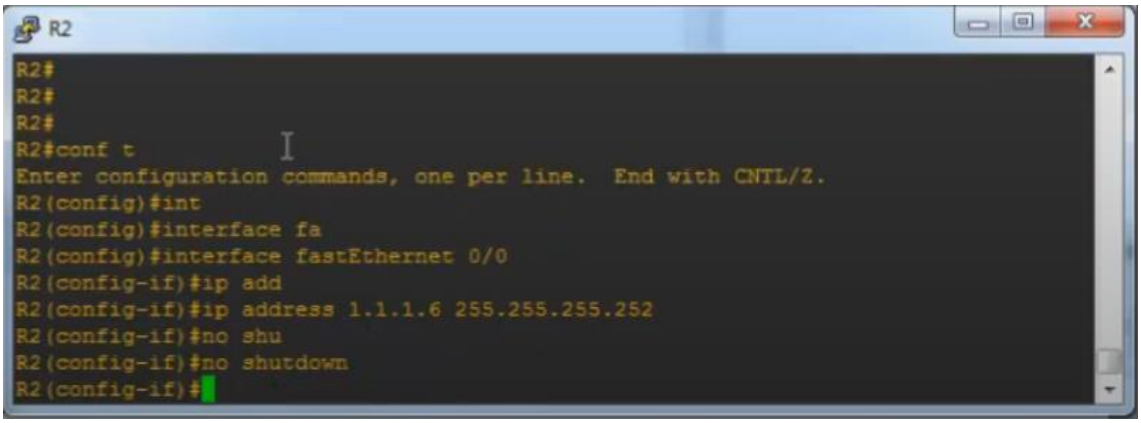


Imagen 27-4 Configuración de ROUTER 2

```
R2#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface fastEthernet 0/0
R2(config-if)#ip add
R2(config-if)#ip address 1.1.1.6 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#
```

El router R2 tiene configurada la interfaz FastEthernet 0/0 con la dirección IP 1.1.1.6/30. Esto sugiere que este dispositivo forma parte de un enlace punto a punto con otro router (probablemente R1), que debería tener la dirección IP 1.1.1.5/30 para completar la conexión.

La configuración está completa para la interfaz FastEthernet 0/0. Para garantizar que el enlace sea funcional, el administrador deberá coincidir en configurar el router remoto (probablemente R1) con una dirección IP dentro de la misma subred.

Se Verifica conectividad utilizando herramientas como ping, luego se Configura rutas estáticas o un protocolo de enrutamiento dinámico, si es necesario, para que el tráfico fluya correctamente entre redes.

Esta configuración es típica en escenarios donde se establecen enlaces punto a punto entre routers en una topología básica.

La imagen 28.4 muestra la configuración básica de una interfaz en un router identificado como **R2**. Se realizan configuraciones de red esenciales para habilitar la interfaz y asignarle una dirección IP.

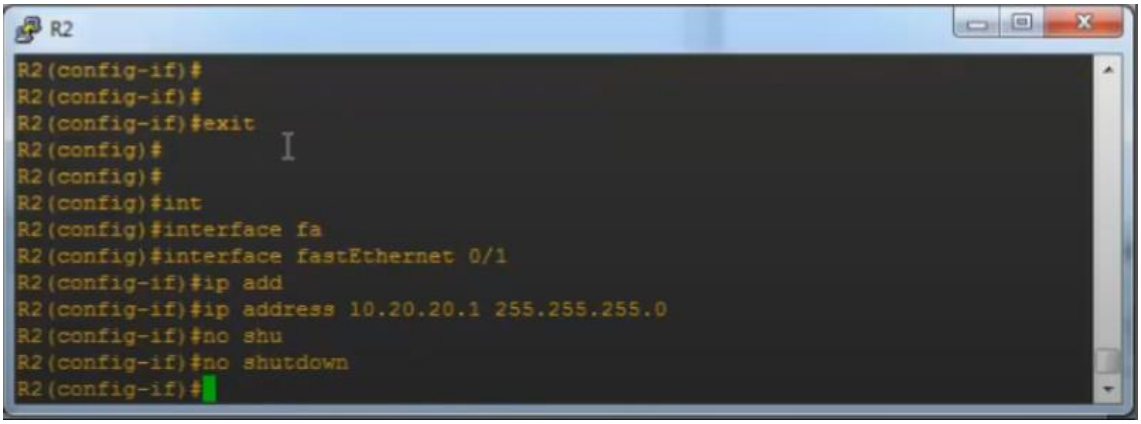


Imagen 28-4 Dirección privada ROUTER 2

```
R2(config)#interface fastEthernet 0/1
R2(config-if)#ip address 10.20.20.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
```

El administrador configura la interfaz FastEthernet 0/1 con una dirección IP de la subred **10.20.20.0/24**. Esto sugiere que esta interfaz está conectada a una red local (LAN), mientras que la otra interfaz configurada previamente (FastEthernet 0/0) probablemente esté conectada a un enlace punto a punto.

La configuración está completa para la interfaz FastEthernet 0/1. Para que esta configuración sea funcional se necesita:

- Asegurarse de que otros dispositivos en la red LAN estén configurados dentro del rango de la subred **10.20.20.0/24**.

- Verificar conectividad local con herramientas como ping.
- Configurar rutas o protocolos de enrutamiento si esta red necesita conectarse con otras redes, como la configurada en FastEthernet 0/0.

Esta configuración es típica de un router que conecta una red local (LAN) con una red externa o un enlace punto a punto.

La imagen 29.4 muestra la configuración de una política de **ISAKMP** en un router identificado como **R2**. ISAKMP es una parte clave del proceso de configuración de una VPN basada en IPSec, y esta política define cómo los dos extremos de la VPN negocian y establecen un canal seguro (fase 1 de IPSec).

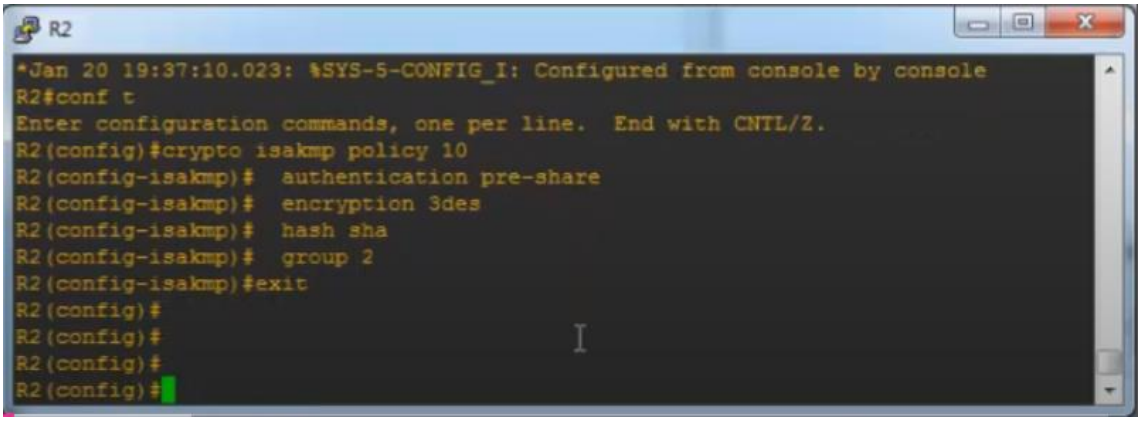


Imagen 29-4 Realizar la configuración del ROUTER 1 en el ROUTER 2

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#crypto isakmp policy 10
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# encryption 3des
R2(config-isakmp)# hash sha
R2(config-isakmp)# group 2
R2(config-isakmp)#exit
R2(config)#
```

La configuración establece una política ISAKMP en el router **R2** con los siguientes parámetros:

- **Autenticación**: Pre-Shared Key (PSK).
- **Cifrado**: 3DES.
- **Hash**: SHA.

- **Grupo Diffie-Hellman**: Grupo 2.

Esta configuración es válida y funcional, pero hay elementos que podrían mejorarse para cumplir con estándares de seguridad más modernos.

Conclusión:

- **Mejoras recomendadas**:
    1. Utilizar **AES** en lugar de 3DES para el cifrado, ya que AES es más seguro y eficiente.
    2. Cambiar a **Diffie-Hellman grupo 14** (2048 bits) o superior para mayor seguridad en el intercambio de claves.
- **Siguiente paso**: Configurar la clave precompartida utilizando el comando crypto isakmp key y asociar esta política a un mapa de cifrado (crypto map) para que sea aplicada al tráfico IPsec.

Esta configuración es adecuada para redes pequeñas o controladas, pero puede necesitar ajustes para entornos más exigentes en términos de seguridad como se observa en la imagen 30.4.

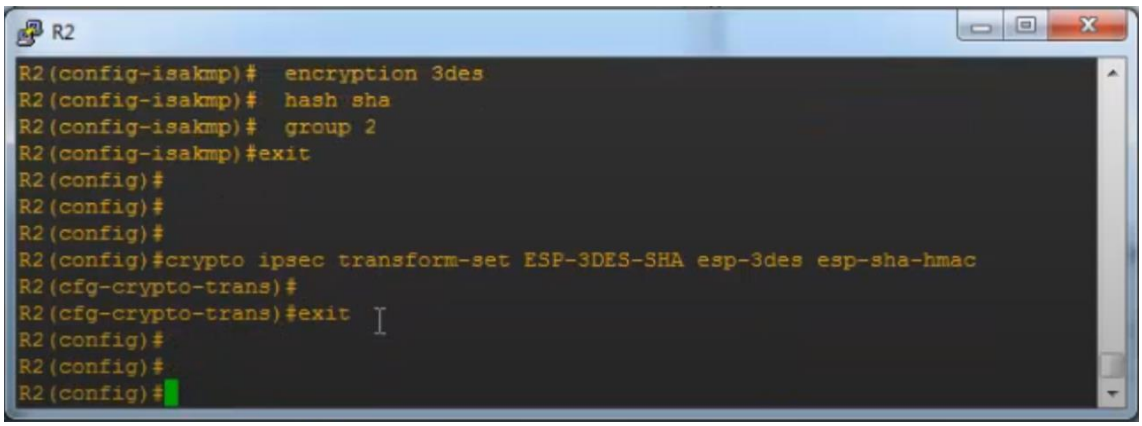


Imagen 30-4 Relacionar con el GRUPO 2 como en el ROUTER 1

R2(config-isakmp)# encryption 3des
R2(config-isakmp)# hash sha
R2(config-isakmp)# group 2
R2(config-isakmp)# exit
R2(config)#
R2(config)#crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac

```
R2(cfg-crypto-trans)#exit
R2(config)#
```

El router R2 ahora tiene configurada una política ISAKMP y un transform-set IPsec con los siguientes parámetros:

- Cifrado: 3DES.
- Integridad: SHA.
- Intercambio de claves: Grupo Diffie-Hellman 2.
- Transform-set: Define cómo se cifrarán y autenticarán los datos en el túnel IPsec utilizando ESP con 3DES y HMAC-SHA.

- Configurar una clave compartida entre ambos routers para autenticar la conexión IPsec.

Conclusión:

- **La configuración es funcional**, pero podría mejorarse:
    1. Cambiar **3DES** por **AES** para un cifrado más seguro y eficiente.
    2. Usar un grupo Diffie-Hellman más fuerte, como el **grupo 14 (2048 bits)**, para una mayor seguridad.
- **Próximos pasos**:
    - Asociar este transform-set y la política ISAKMP a un mapa de cifrado (crypto map).
    - Configurar las claves precompartidas (crypto isakmp key) y definir los peers remotos.

Esta configuración es típica para establecer un túnel IPsec básico y proporciona seguridad razonable en redes controladas.

La imagen 31.4 muestra la configuración de una clave precompartida (pre-shared key) en un router identificado como **R1**. Este es un paso clave para establecer una conexión segura entre dos routers en una VPN IPSec.

Imagen 31-4 Configuración de llave Precompartida

```
R1(config)#
R1(config)#crypto isakmp key cisco add
R1(config)#crypto isakmp key cisco address 1.1.1.6
R1(config)#
```

Este comando configura una clave precompartida (PSK) para la autenticación ISAKMP entre el router R1 y un peer con la dirección IP 1.1.1.6 (probablemente el router R2). Esto es parte del proceso de establecer un túnel VPN IPsec, ya que asegura que ambos extremos utilicen la misma clave para autenticación durante la fase 1 de ISAKMP.

Conclusión:

La configuración de la clave precompartida está correcta. Los próximos pasos incluyen:

- **Verificación en el peer remoto (R2)**:
    - El router **R2** también debe tener configurada la misma clave (cisco) con la dirección IP de **R1** (probablemente 1.1.1.5).

- **Configuración de un mapa de cifrado (crypto map)** en ambos routers, vinculando la política ISAKMP, el transform-set y la configuración del peer.
- **Prueba de conectividad**:
    - Realizar pruebas como ping entre las direcciones IP para asegurarse de que los dispositivos puedan comunicarse.

Esta configuración es esencial para completar el establecimiento del túnel IPsec.

Tenemos en la siguiente imagen 32.4 muestra la configuración de una lista de control de acceso extendida (ACL) en un router identificado como R1. Estas ACL se utilizan para definir el tráfico que se permitirá o denegará en diferentes contextos, como una VPN IPSec.

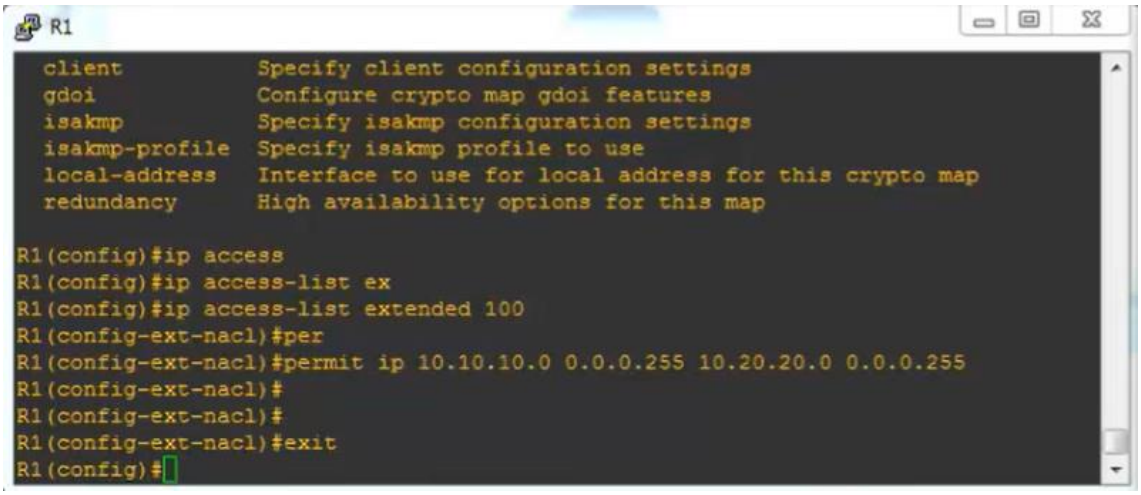


Imagen 32-4 Trafico que se va a permitir por la VPN

```
R1(config)#ip access
R1(config)#ip access-list extended 100
R1(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
R1(config-ext-nacl)#
R1(config-ext-nacl)#exit
R1(config)#
```

La ACL extendida 100 permite el tráfico entre las redes **10.10.10.0/24** y **10.20.20.0/24**. Este paso es crucial para definir qué tráfico debe protegerse por el túnel IPsec.

Conclusión:

- **Uso de la ACL**: La ACL configurada será asociada a un **crypto map** para especificar qué tráfico será cifrado por el túnel IPsec.
- **Próximos pasos**:
    - Configurar el **crypto map** y vincular esta ACL.
    - Verificar que las subredes especificadas en la ACL sean las correctas según la topología de red.
    - Probar la conectividad entre las dos redes una vez configurado el túnel.

Esta configuración es correcta y sigue el estándar para preparar el tráfico que será protegido por el túnel IPsec.

La imagen 33.4 muestra la configuración de un crypto map en el router identificado como R1. Un crypto map es una colección de configuraciones que determinan cómo se aplicarán las políticas IPSec a las conexiones. Este paso es crucial para vincular los parámetros configurados anteriormente, como las listas de acceso (ACL), y activar la protección del tráfico en un túnel VPN.

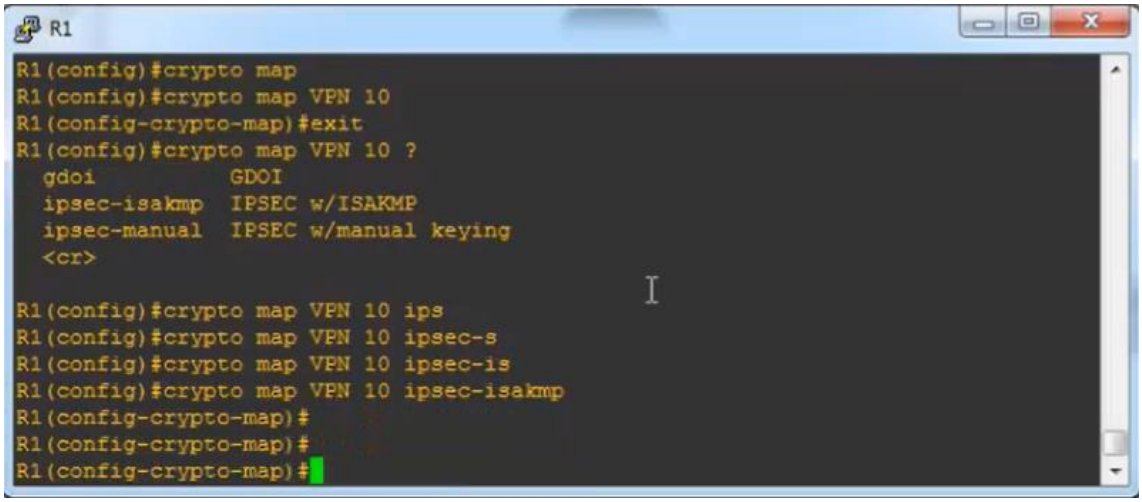


Imagen 33-4 Configuramos el CRYPTO MAP

```
R1(config)#crypto map VPN 10
R1(config-crypto-map)#exit
R1(config)#crypto map VPN 10 ?
  gdoi         GDOI
  ipsec-isakmp IPSEC w/ISAKMP
  ipsec-manual IPSEC w/manual keying
<cr>

R1(config)#crypto map VPN 10 ipsec-isakmp
```

R1(config-crypto-map)#

La configuración está definiendo un mapa de cifrado llamado VPN que utilizará IPsec con ISAKMP. Este mapa de cifrado es una pieza clave para completar la configuración de un túnel VPN IPsec, ya que vincula:

- Las políticas ISAKMP.
- El transform-set configurado.
- La ACL que define qué tráfico debe cifrarse.

Conclusión:

- **Próximos pasos**:
    - Asignar el transform-set previamente configurado (ESP-3DES-SHA) al mapa de cifrado.
    - Vincular la ACL (100) al mapa de cifrado para especificar el tráfico protegido.
    - Aplicar el mapa de cifrado a una interfaz del router con el comando crypto map VPN en la configuración de la interfaz.

La configuración actual es correcta y sigue las prácticas estándar para establecer un túnel IPsec. Es importante completar la asociación de transform-set y ACL, y verificar conectividad con el peer remoto.

La imagen 31.4 muestra la configuración final de un crypto map en un router identificado como R1, vinculando varios elementos previamente configurados. Este paso completa la preparación de una VPN IPSec.

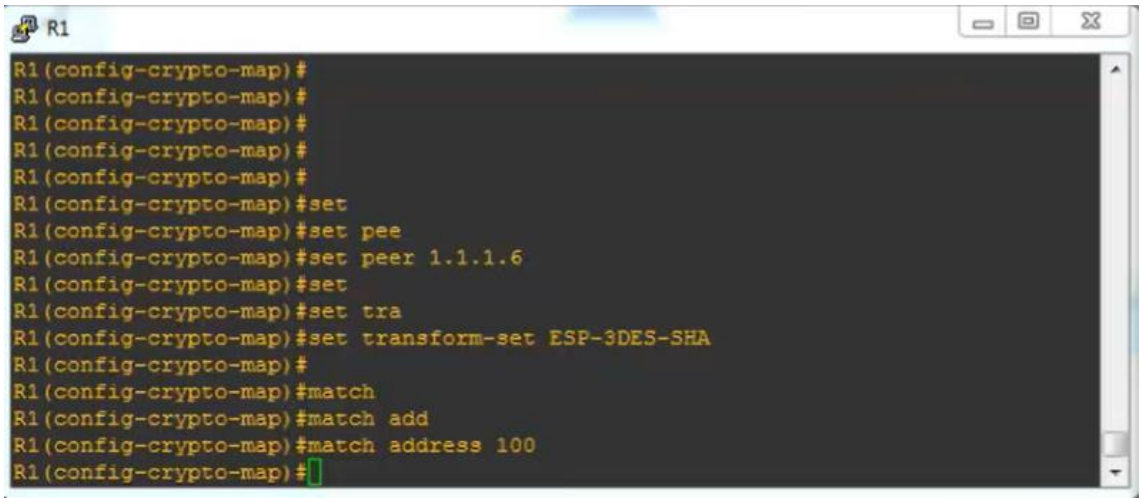


Imagen 31-4 Asignación de dominio de dirección

```
R1(config-crypto-map)#set peer 1.1.1.6
R1(config-crypto-map)#set transform-set ESP-3DES-SHA
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#
```

El mapa de cifrado (VPN 10) está completamente configurado para:

- Usar el peer remoto con dirección IP 1.1.1.6.
- Aplicar el transform-set ESP-3DES-SHA para cifrado y autenticación.
- Proteger el tráfico definido en la ACL 100.

Este mapa de cifrado define todas las reglas necesarias para establecer y gestionar el túnel IPsec entre el router R1 y su peer remoto.

Aplicar el mapa de cifrado a la interfaz saliente del router con el comando crypto map VPN en el modo de configuración de la interfaz correspondiente.

Asegurarse de que el peer remoto (probablemente R2) tenga configuraciones similares y compatibles (clave precompartida, transform-set, ACL, etc.).

- Probar el túnel con comandos como ping y show crypto isakmp sa para verificar que el túnel IPsec esté activo y funcional.

La configuración es correcta y completa en esta etapa, siguiendo estándares para establecer un túnel VPN IPsec seguro.

La imagen 32.4 muestra el paso final para habilitar una configuración VPN en un router identificado como **R1**. Se activan los protocolos y se asocia el **crypto map** a una interfaz de red, lo cual permite que el tráfico cumpla con las políticas IPSec configuradas.

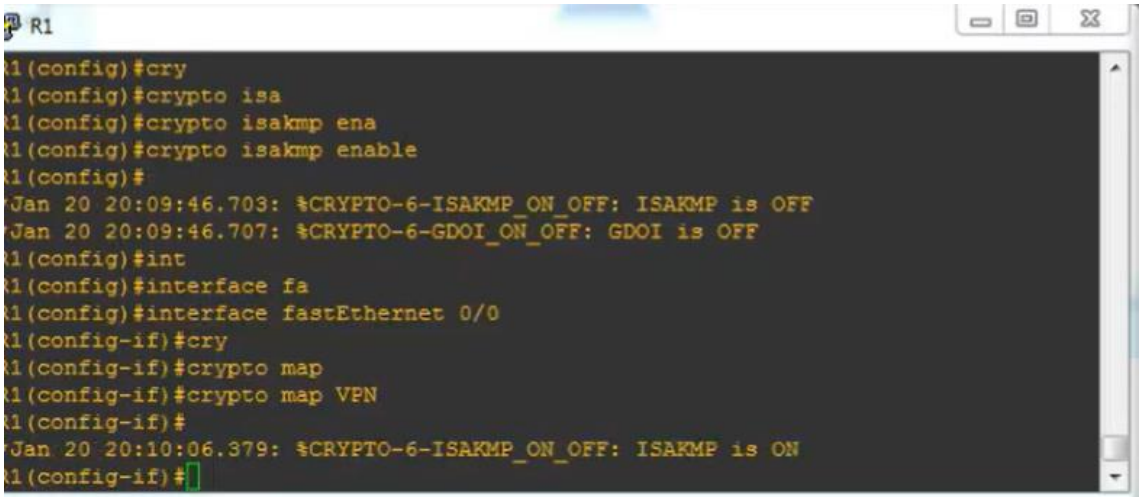


Imagen 32-4 Configuración del túnel VPN

```
R1(config)#crypto isa
R1(config)#crypto isakmp enable
R1(config)#
*Jan 20 20:09:46.703: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Jan 20 20:09:46.707: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
R1(config)#int
R1(config)#interface fastEthernet 0/0
R1(config-if)#crypto map VPN
*Jan 20 20:10:06.379: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
```

Con esta configuración, el router R1 está listo para establecer un túnel IPsec con un peer remoto, ya que:

- ISAKMP está habilitado.

- El mapa de cifrado está correctamente aplicado a la interfaz FastEthernet 0/0.
- Las reglas para cifrar y autenticar el tráfico han sido definidas.

    - Verificar que el peer remoto (por ejemplo, **R2**) tenga configuraciones compatibles.
    - Realizar pruebas de conectividad (ping) entre las redes protegidas.
    - Verificar el estado del túnel utilizando comandos como show crypto isakmp sa y show crypto ipsec sa.

Configuración completada correctamente: Esta es la última etapa en la configuración de un túnel VPN IPsec estándar. El túnel debería establecerse automáticamente cuando haya tráfico que coincida con la ACL definida.

La imagen 33.4 muestra la configuración de una lista de control de acceso extendida (ACL) en un router identificado como R2, que es complementaria a la configuración realizada en el router R1. Esta ACL define el tráfico permitido para ser protegido por IPSec dentro de la VPN.

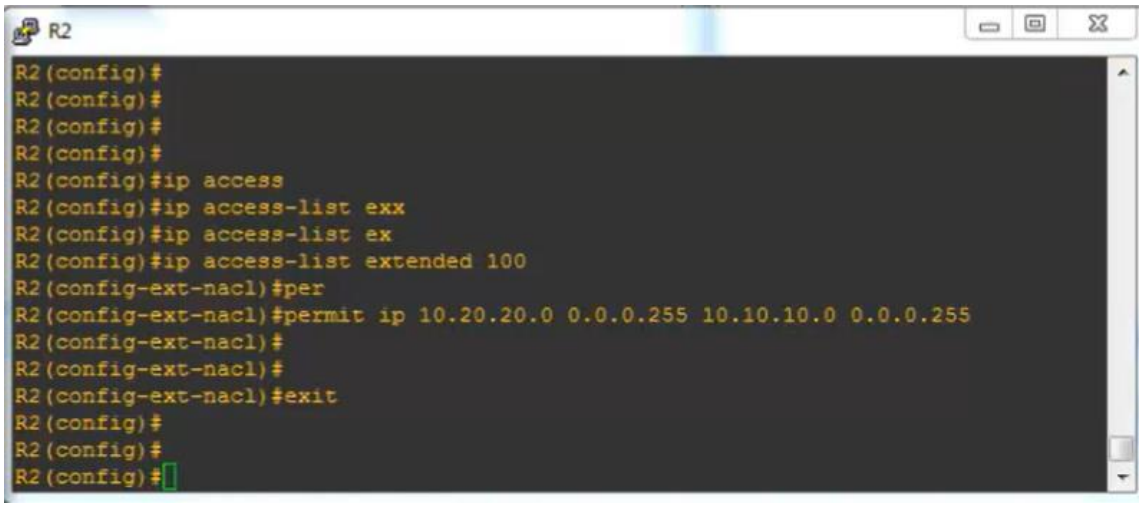


Imagen 33-4 Trafico que se va a permitir por la VPN en ROUTER 2

```
R2(config)#ip access-list extended 100
R2(config-ext-nacl)#permit ip 10.20.20.0 0.0.0.255 10.10.10.0 0.0.0.255
R2(config-ext-nacl)#
R2(config-ext-nacl)#exit
R2(config)#
```

Esta ACL en el router R2 permite el tráfico IP entre la red 10.20.20.0/24 (red local de R2) y la red 10.10.10.0/24 (red local de R1). Este paso es crucial para definir el tráfico que será protegido por el túnel IPsec entre los dos routers.

Esta configuración debe ser consistente con la ACL configurada en el router R1, pero invertida, ya que las direcciones de origen y destino cambian según la perspectiva de cada router.

Esta configuración forma parte de la preparación del tráfico que será cifrado en el túnel IPsec. La implementación es correcta y sigue los estándares para VPNs IPsec.

La imagen 34.4 muestra la activación de ISAKMP y la asociación de un crypto map a una interfaz en el router R2, completando así los pasos necesarios para configurar una VPN IPSec en este router.

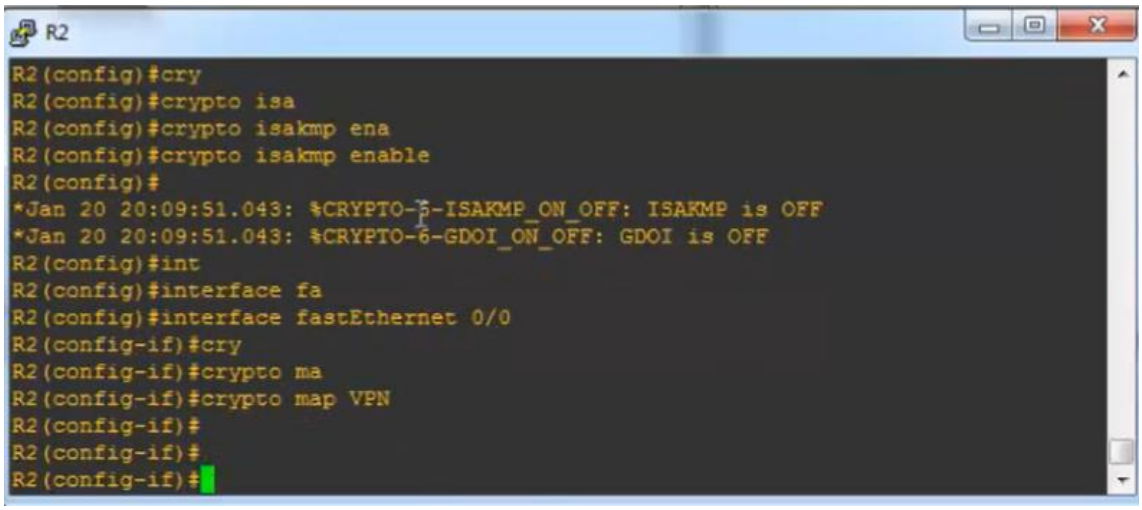


Imagen 34-4 Copiar la configuración del ROUTER 1 en ROUTER 2

```
R2(config)#crypto isakmp enable
R2(config)#
*Jan 20 20:09:51.043: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Jan 20 20:09:51.043: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
R2(config)#interface fastEthernet 0/0
R2(config-if)#crypto map VPN
R2(config-if)#
```

El router R2 ahora está configurado para utilizar ISAKMP e IPsec en la interfaz FastEthernet 0/0. La asociación del mapa de cifrado VPN asegura que el tráfico definido en la ACL correspondiente sea protegido por el túnel IPsec.

5.3 Ejecución y Análisis de la Simulación VPN IPsec (Internet Protocol Security) Site to site

Después de configurar la VPN IPsec Site-to-Site, se pueden realizar pruebas para verificar el funcionamiento y analizar el rendimiento de la conexión VPN.

En la verificación del Túnel Ipsec cada router, se ejecutan comandos como show crypto isakmp sa para verificar que el túnel IPsec se haya establecido correctamente. Esto confirma que ambos routers han autenticado exitosamente el intercambio de claves y han configurado el túnel seguro. La prueba de Conectividad se usa comandos como ping entre dispositivos en la LAN 1 y la LAN 2 para verificar la conectividad a través del túnel VPN.

Para esta prueba se debe Confirmar que las redes protegidas por la VPN pueden comunicarse de forma segura y verificar que el tráfico cifrado y autenticado esté siendo procesado correctamente a través del túnel IPSec como se ve en la imagen 35.4.

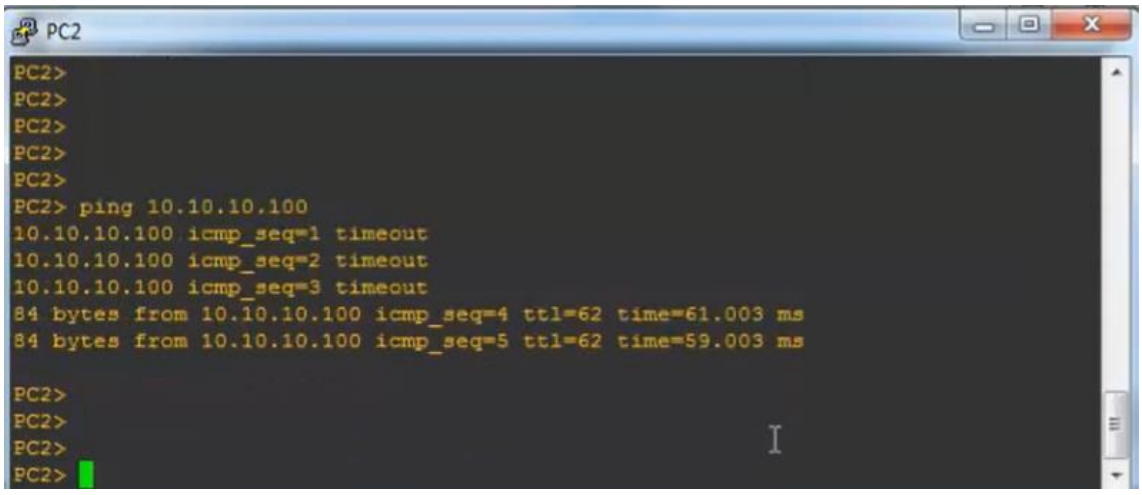


Imagen 35-4 Validación de conexión

El túnel IPsec está funcionando correctamente, y la conectividad entre las redes protegidas está verificada.

Como recomendaciones podemos Monitorear el túnel utilizando comandos como show crypto isakmp sa y show crypto ipsec sa como se ve en la imagen 36.4 para verificar que las fases de negociación y cifrado se mantengan estables.

Esta prueba confirma que la configuración IPsec es funcional y el tráfico entre las redes protegidas está siendo cifrado y transmitido exitosamente.

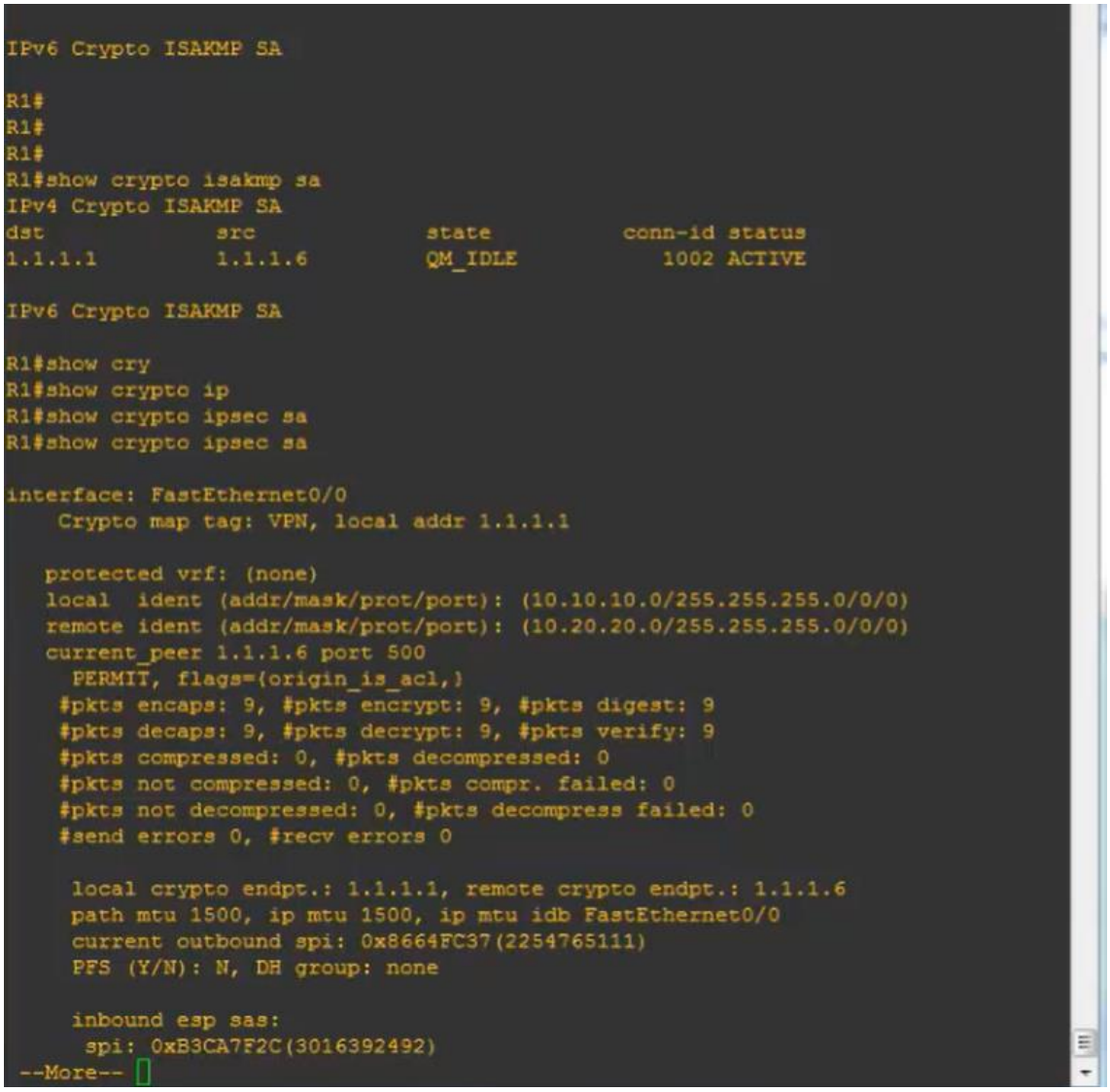


Imagen 36-4 Prueba de configuración satisfecha

En el estado del túnel, en el túnel IPsec está operativo y en estado ACTIVE, con tráfico cifrado y autenticado entre las redes protegidas.

Las Recomendaciones para las redes protegidas activan el Perfect Forward Secrecy (PFS) para mayor seguridad configurando un grupo Diffie-Hellman en la fase 2 o Se Monitorea periódicamente el estado del túnel con estos comandos para asegurar que no haya errores ni interrupciones.

SA activa tanto para tráfico entrante como saliente como se visualiza en la imagen 37.4, las asociaciones están activas, lo que indica que la VPN está funcionando correctamente.

En el tiempo restante la vida útil de las claves es suficiente para continuar la comunicación. La renegociación se realizará automáticamente antes de que expire. Uso de ESP proporciona tanto cifrado como autenticación, asegurando la confidencialidad e integridad del tráfico.

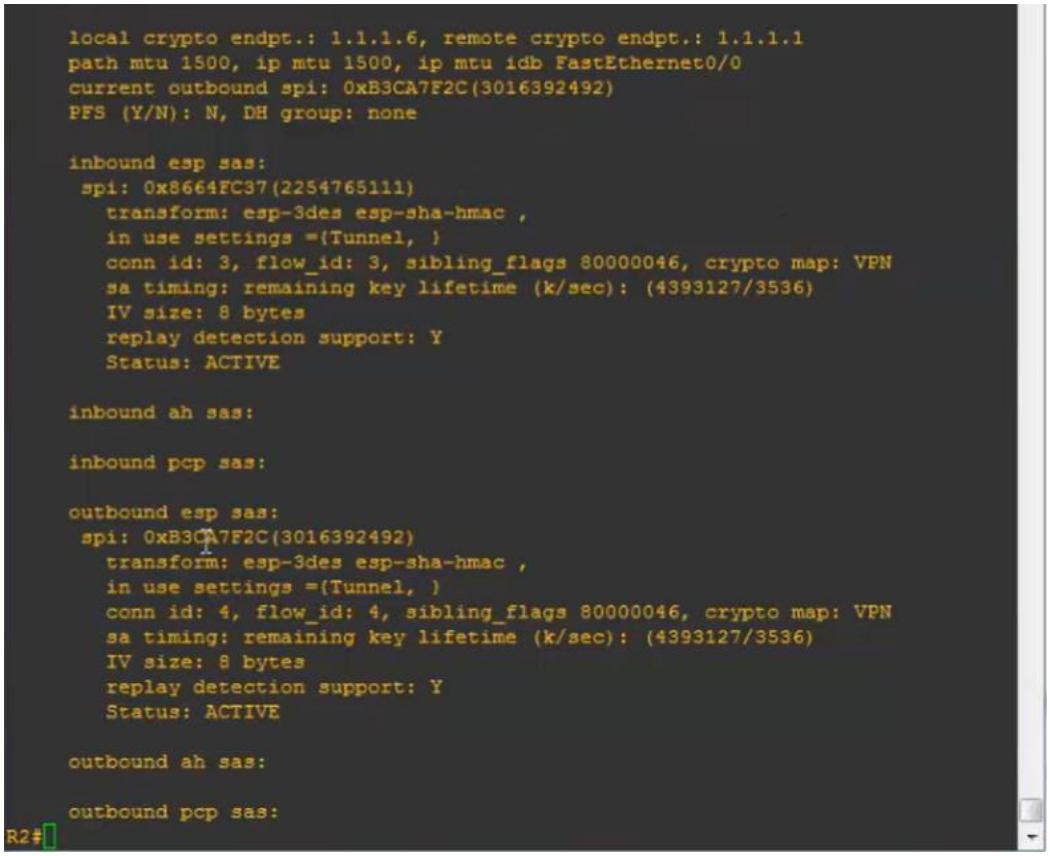


Imagen 37-4 VPN funcionamiento correcto

La latencia y Ancho de Banda Usan herramientas como Iperf, se mide el rendimiento de la conexión VPN en términos de latencia y ancho de banda. Debido a la sobrecarga del cifrado, se puede esperar un pequeño incremento en la latencia y una reducción en el ancho de banda disponible, aunque esto varía según los algoritmos utilizados. A comparación con Conexiones Sin VPN: Comparar el rendimiento entre la conexión con y sin VPN permite evaluar el impacto del cifrado en el rendimiento general.

5.3.1 Pruebas de rendimiento

La simulación de una VPN IPsec Site-to-Site en GNS3 permite observar de primera mano la capacidad de IPsec para proporcionar una conexión segura entre redes remotas. Las conclusiones clave incluyen:

- Conexión Segura: La VPN IPsec proporciona una conexión segura mediante cifrado y autenticación, protegiendo los datos de las redes conectadas.
- Compromiso de Rendimiento: Aunque el cifrado introduce una sobrecarga, el impacto en la velocidad es mínimo en comparación con los beneficios de seguridad.
- Simulación en GNS3: Configurar y analizar una VPN Site-to-Site en GNS3 es una práctica útil que permite comprender mejor los mecanismos de IPsec y evaluar cómo afectan el rendimiento y la seguridad de la red.

Recomendaciones para Implementaciones Reales

- Elección del Algoritmo de Cifrado: Seleccionar algoritmos de cifrado y autenticación equilibrados para mantener la seguridad sin comprometer excesivamente el rendimiento.
- Infraestructura PKI para Claves: En entornos con varias sucursales, usar una infraestructura de claves públicas puede simplificar la gestión de certificados.
- Optimización del Rendimiento: Monitorizar la latencia y el uso del ancho de banda para asegurar un buen balance entre rendimiento y seguridad.

Este análisis de la VPN IPsec Site-to-Site en GNS3 ofrece una visión práctica y técnica para comprender cómo se pueden implementar y optimizar las VPNs en redes empresariales.

5.4 Explicación de las Pruebas:

- **Realizamos la prueba Local (ping 192.168.1.1)**:
    - **Destino**: Dirección IP de la puerta de enlace local configurada en el dispositivo, probablemente la dirección de la interfaz del router de la red LAN.
    - **Resultados**:
        - Todas las solicitudes de ping fueron exitosas (**0% loss**).
        - Los tiempos de respuesta (<1ms) son extremadamente bajos, lo cual es normal para pruebas dentro de una red local.
        - El TTL (**255**) indica que el paquete no recorrió muchos saltos, confirmando que el destino está muy cerca (en la misma red).
- **Prueba Remota (ping 209.165.200.229)**:
    - **Destino**: Dirección IP del siguiente salto configurado como la puerta de enlace hacia internet o una red externa.
    - **Resultados**:
        - Todas las solicitudes de ping fueron exitosas.
        - Los tiempos de respuesta son más altos (**16ms a 19ms**) pero aceptables, indicando que la comunicación con la red remota es funcional.
        - El TTL (**254**) sugiere que el destino está relativamente cerca, con solo uno o dos saltos desde la red local.

La imagen 45.4 muestra una ventana de Command Prompt en Windows donde se están ejecutando comandos ping para verificar la conectividad de red. Los resultados reflejan que las conexiones locales y externas funcionan correctamente.

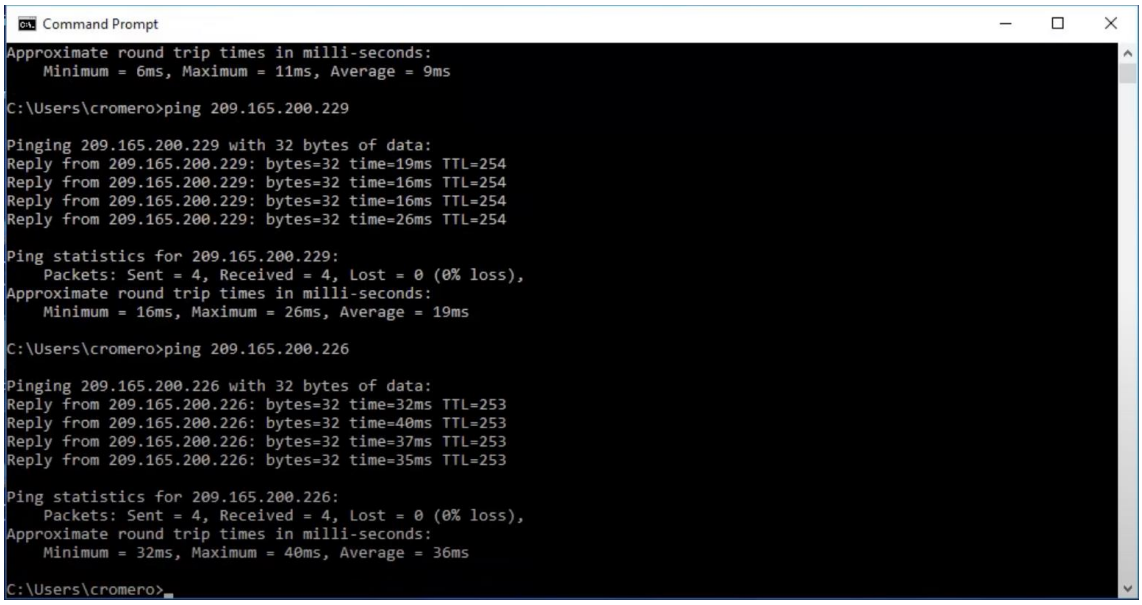


Imagen 45-4 Configuración de Cisco ASAv9 parte 2

Realizamos las siguientes pruebas:

1. **Primera Prueba (ping 209.165.200.229):**
    - Destino: Se realiza una prueba hacia la dirección IP 209.165.200.229, que podría ser la puerta de enlace configurada o un dispositivo conectado a la red WAN.
    - Resultados:
        - Todas las solicitudes fueron exitosas (0% loss).
        - Los tiempos de respuesta oscilan entre 16ms y 19ms, lo cual es razonable para una red WAN cercana.
        - TTL=254: Indica que el paquete viajó un solo salto antes de llegar al destino.
2. **Segunda Prueba (ping 209.165.200.226):**
    - Destino: Se realiza una prueba hacia la dirección IP 209.165.200.226, que podría pertenecer a otro dispositivo en la red WAN o en una red externa.
    - Resultados:

- Todas las solicitudes fueron exitosas (0% loss).
- Los tiempos de respuesta son más altos (32ms a 40ms) en comparación con el primer destino, lo cual puede deberse a una mayor distancia o mayor tráfico en la red.
- TTL=253: Indica que el paquete viajó dos saltos antes de alcanzar el destino.

- **Red Local y WAN Operativa**:
  - La red local y la configuración de rutas están funcionando correctamente, permitiendo conectividad con diferentes direcciones remotas.
- **Recomendaciones**:
  a. **Pruebas Adicionales**:
     i. Probar conectividad con un dominio público (por ejemplo, ping google.com) para verificar la resolución DNS y conectividad a internet.
  b. **Monitoreo del Tráfico**:
     i. Utilizar herramientas en el router, como show ip route y show ip nat translations, para monitorear las rutas activas y las traducciones NAT.

El resultado confirma que el dispositivo tiene acceso funcional a los destinos remotos configurados, lo cual es un indicador de que la red está configurada correctamente.

La imagen 46.4 muestra una sesión de consola en un dispositivo Cisco ASA (Adaptive Security Appliance) utilizando **TightVNC Viewer** para interactuar con el sistema. Este tipo de entorno es común para configurar dispositivos de red mediante comandos en modo CLI (Command Line Interface).

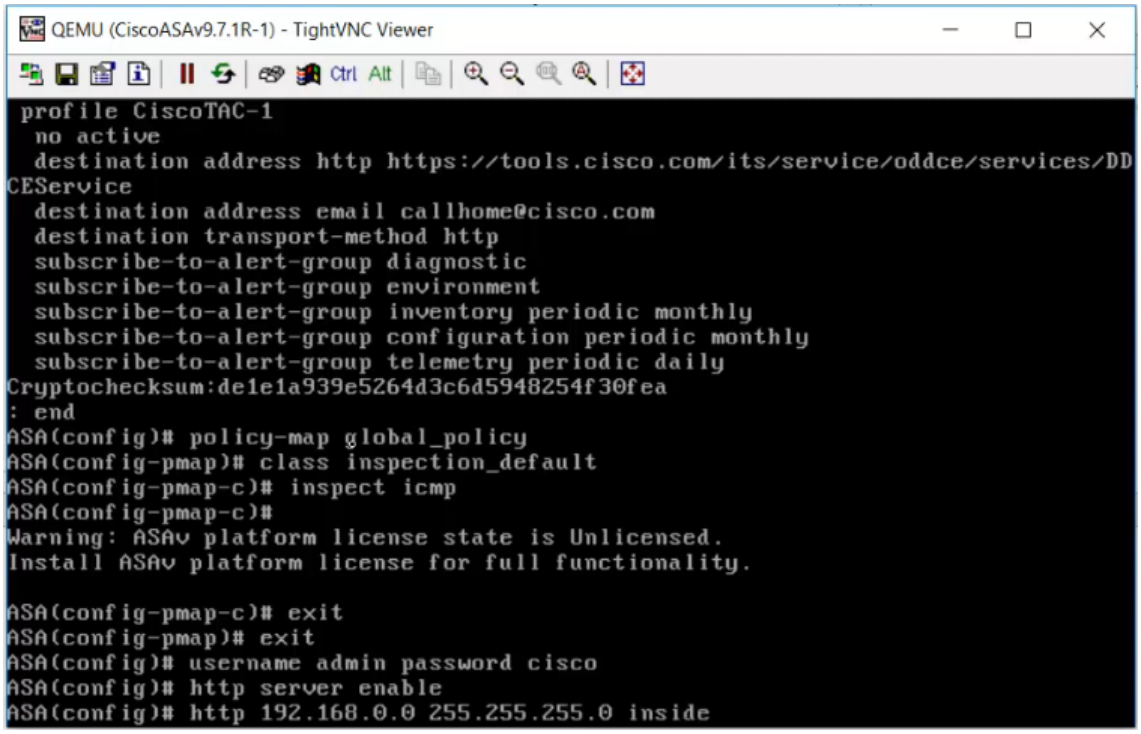


Imagen 46-4 Configuración de Cisco ASAv9 Inside

Explicación:

1. **Configuraciones de Cisco Smart Call Home**:
    - **profile CiscoTAC-1**:
        - Configura un perfil de "Call Home" para enviar alertas y diagnósticos a Cisco.
        - **Destinos**:
            - **https://tools.cisco.com**: Dirección para alertas HTTP.
            - **callhome@cisco.com**: Dirección de correo electrónico para alertas por email.
        - **Grupos de alertas suscritos**:

        - Alertas relacionadas con diagnóstico, ambiente, inventario, configuración y telemetría.

2. **Política Global y Clase de Inspección**:
    - **policy-map global_policy**:
        - Configura una política global para inspección de tráfico.
    - **class inspection_default**:
        - Especifica que se aplica la clase de inspección por defecto.
    - **inspect icmp**:
        - Habilita la inspección de tráfico ICMP (ping), permitiendo su paso a través del firewall.
3. **Estado de Licencia**:
    - El dispositivo muestra un mensaje indicando que no tiene licencia activa. Esto limita algunas funcionalidades del ASA, pero la mayoría de las configuraciones básicas deberían funcionar.
4. **Configuraciones de Administración y HTTP**:
    - **username admin password cisco**:
        - Crea un usuario llamado admin con la contraseña cisco para autenticación en la administración.
    - **http server enable**:
        - Habilita el servidor HTTP del ASA para permitir administración a través de una interfaz web.
    - **http 192.168.0.0 255.255.255.0 inside**:
        - Permite el acceso HTTP desde la red local **192.168.0.0/24** a la interfaz inside del ASA.

Conclusión:

- **La configuración es básica pero funcional**:
    - El ASA está configurado para inspeccionar tráfico ICMP, permitir administración HTTP y enviar alertas a Cisco.
- **Recomendaciones**:

1. **Licencia**:

- Adquirir e instalar una licencia para habilitar la funcionalidad completa del ASA.

2. **Seguridad**:
   - Cambiar la contraseña predeterminada del usuario admin por una más segura.
3. **Acceso HTTP**:
   - Considerar el uso de HTTPS en lugar de HTTP para una administración más segura.

Esta configuración es un punto de partida básico y funcional para la administración y operación del Cisco ASA.

5.4 Acceso Remoto SSL VPN usando ASAv ASDM

Visualizamos en la imagen 38.4 un diagrama de red que conecta dos sitios a través de una red pública (Internet). Aquí se utilizan routers y dispositivos específicos, como un firewall Cisco ASA, para establecer comunicación entre las subredes locales de las dos ubicaciones.

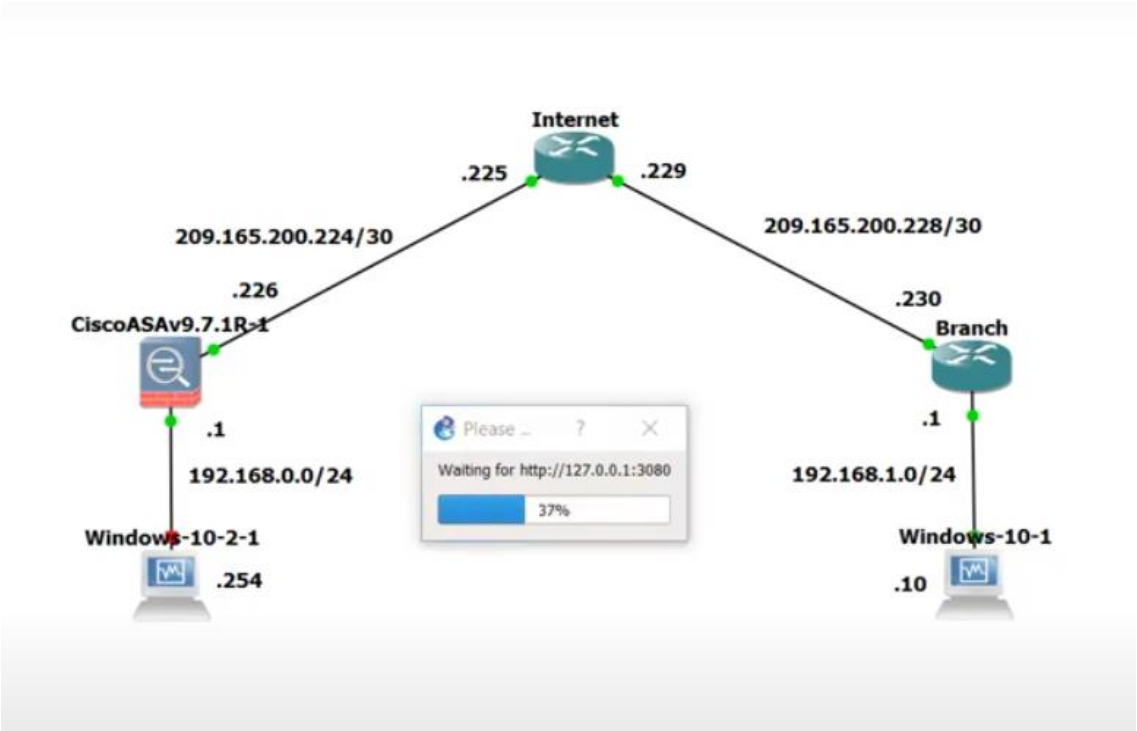


Imagen 38-4 Configuración de ROUTER

Se configura una VPN Site-to-Site para establecer un túnel VPN entre el Cisco ASA y el router Branch para proteger el tráfico entre las redes 192.168.0.0/24 y 192.168.1.0/24. Esto implica configurar políticas ISAKMP/IPSec en ambos extremos y configurar listas de acceso para identificar el tráfico protegido para Asegurarse de que las IP públicas (209.165.200.226 y 209.165.200.230) sean alcanzables.

En la configuración inicial se configura las interfaces y el direccionamiento básico en el ASAv. Usualmente, se necesita una interfaz “inside” para la red interna y otra “outside” para la conexión a Internet. Las direcciones IP: Asigna IPs a las interfaces "outside" con IP pública y "inside" con una red privada y así damos acceso al ASDM: Una vez configurado, el ASDM se acceder y configurar el dispositivo de manera gráfica.

Para las Configuración de Interfaces tenemos:

- Asignar direcciones IP a las interfaces de los routers que conectan a las redes LAN (LAN A y LAN B).
- Configurar las interfaces que conectan a la simulación de Internet (enlace WAN) con direcciones públicas.

La imagen 39.4 muestra configuraciones realizadas en el router Branch, incluyendo la activación de interfaces y el establecimiento de una ruta estática. Esto forma parte de la configuración de red necesaria para habilitar la comunicación y posiblemente un túnel VPN con otro dispositivo, como el Cisco ASA en el sitio principal.

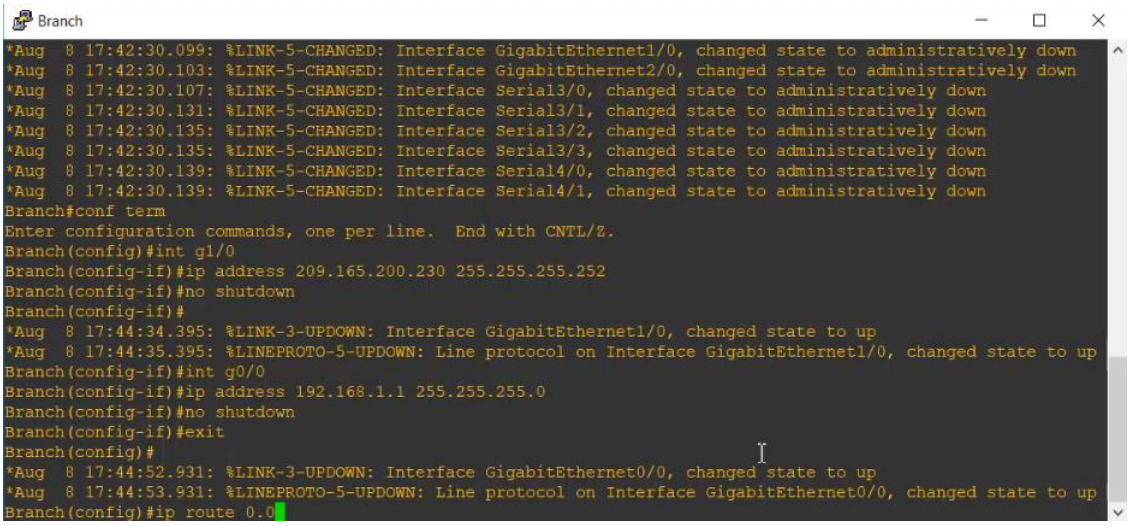


Imagen 39-4 Configuración del terminal

El router en la sucursal (Branch) está configurado para:

- Conectar una red local (LAN) en **192.168.1.0/24** utilizando la interfaz GigabitEthernet0/0.
- Establecer un enlace WAN punto a punto en **209.165.200.228/30** utilizando la interfaz GigabitEthernet1/0.
- Redirigir todo el tráfico desconocido hacia el siguiente salto **209.165.200.229**, configurando así una conexión con la red principal o internet.

- La configuración es adecuada para un entorno típico de sucursal, donde el router actúa como Gateway para la red local y establece una conexión WAN con una red remota.

En las Recomendaciones tenemos:

  - Probar conectividad utilizando comandos como ping hacia el siguiente salto y hacia redes remotas.
  - Asegurarse de que el dispositivo remoto en 209.165.200.229 esté configurado para recibir y reenviar tráfico de esta sucursal.
  - Monitorear las interfaces con comandos como show ip interface brief para confirmar su estado operativo.

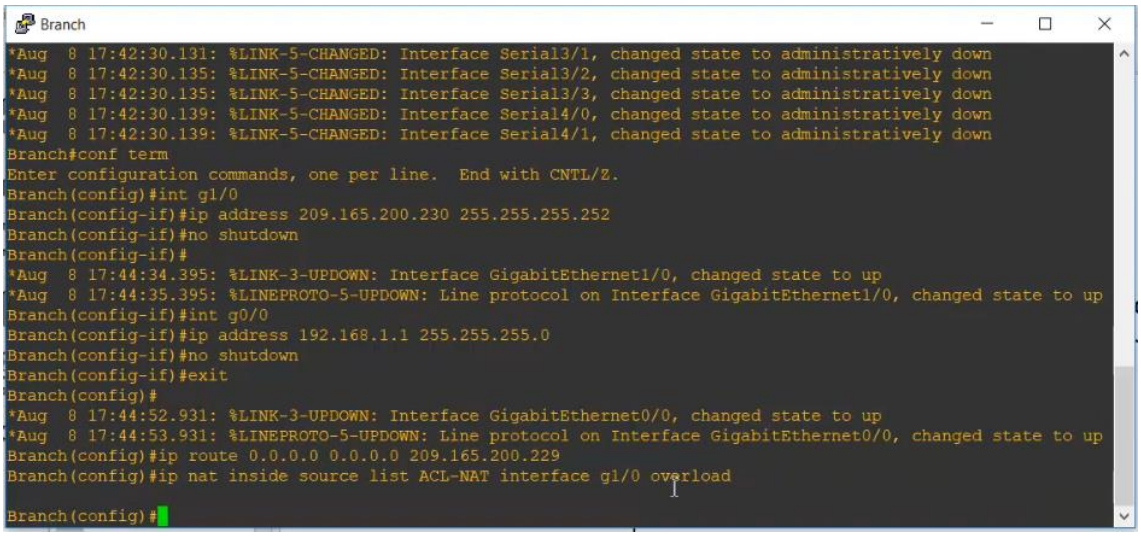


Imagen 40-4 Configuración de interfaz de salida

El router está configurado para:

- Conectar la red interna **192.168.1.0/24** (LAN) con una red remota o internet a través de la interfaz WAN **GigabitEthernet1/0**.
- Redirigir el tráfico no conocido hacia el siguiente salto configurado con la ruta por defecto.
- Usar NAT con sobrecarga para permitir que múltiples dispositivos en la LAN compartan la dirección IP pública **209.165.200.230**.

- **La configuración es funcional** y lista para operar en un entorno donde se requiera conectividad LAN a WAN con NAT.
- **Tenemos las siguientes recomendaciones para la configuración**:
    - Configurar y verificar la lista de acceso ACL-NAT para asegurarse de que incluye el tráfico interno necesario.
    - Probar conectividad hacia la WAN y realizar pruebas de traducción NAT utilizando comandos como show ip nat translations.
    - Monitorear las interfaces con show ip interface brief para confirmar su estado operativo.

Esta configuración cumple con los estándares para un router de sucursal conectado a internet o a una red corporativa.

La imagen 41.4 muestra configuraciones realizadas en el router Branch, incluyendo la activación de interfaces y el establecimiento de una ruta estática. Esto forma parte de la configuración de red necesaria para habilitar la comunicación y posiblemente un túnel VPN con otro dispositivo, como el Cisco ASA en el sitio principal.

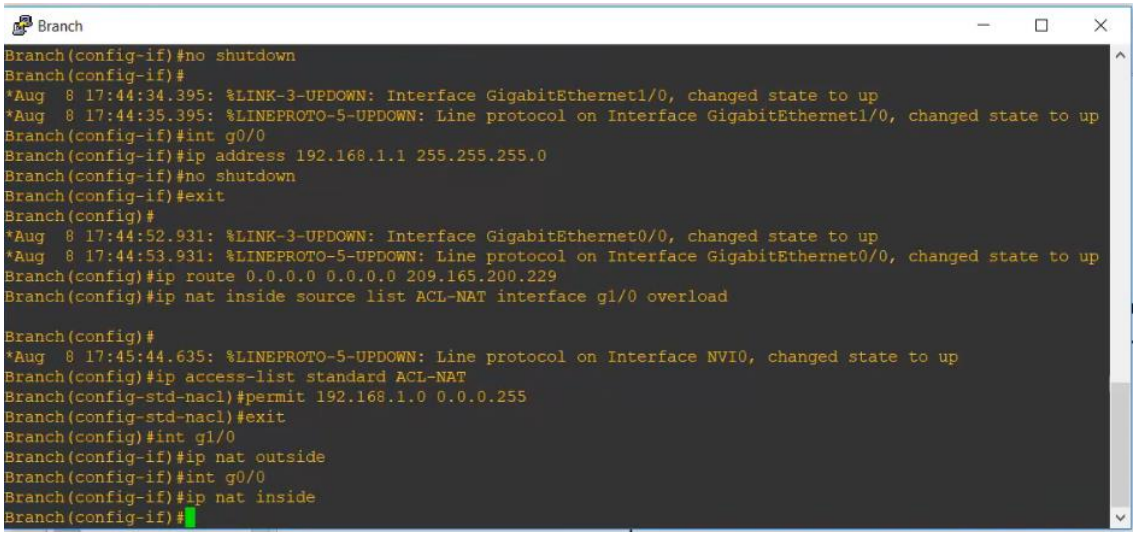


Imagen 41-4 Configuración inside and outside

Tenemos los siguientes puntos importantes para la configuración

- Habilitar WebVPN: En ASDM, activa la opción de WebVPN en la interfaz “outside” para habilitar las conexiones SSL.
- Creación de grupos VPN: Define un grupo de VPN para los usuarios remotos, asignando los parámetros necesarios (como la dirección del túnel, encriptación y autenticación).
- Configuración de DHCP o Pool de direcciones: Establece un pool de direcciones IP para los usuarios remotos que se conectarán a través de la VPN. Esto asegura que cada usuario obtenga una IP en la red interna.
- Asignación de políticas de acceso: Configura las políticas de acceso (ACLs) que especifican a qué recursos internos pueden acceder los usuarios remotos.
- Uso de un cliente VPN: En el host remoto, usa un navegador o cliente compatible con SSL VPN (Cisco AnyConnect, por ejemplo) para conectarse a la dirección pública de la interfaz “outside”.

- Acceso seguro: Verifica que el cliente pueda conectarse y autenticar a través del SSL VPN. Una vez conectado, el cliente debería obtener una IP dentro del rango configurado en el pool.
- Pruebas de conectividad: Realiza pruebas de conectividad (ping, acceso a recursos) hacia la red interna para verificar que la VPN esté funcionando correctamente.

La imagen 42.4 muestra la configuración de la dirección IP manual en un sistema operativo Windows 10, específicamente en las propiedades de la red Ethernet dentro de la configuración de IPv4 (Internet Protocol Version 4).

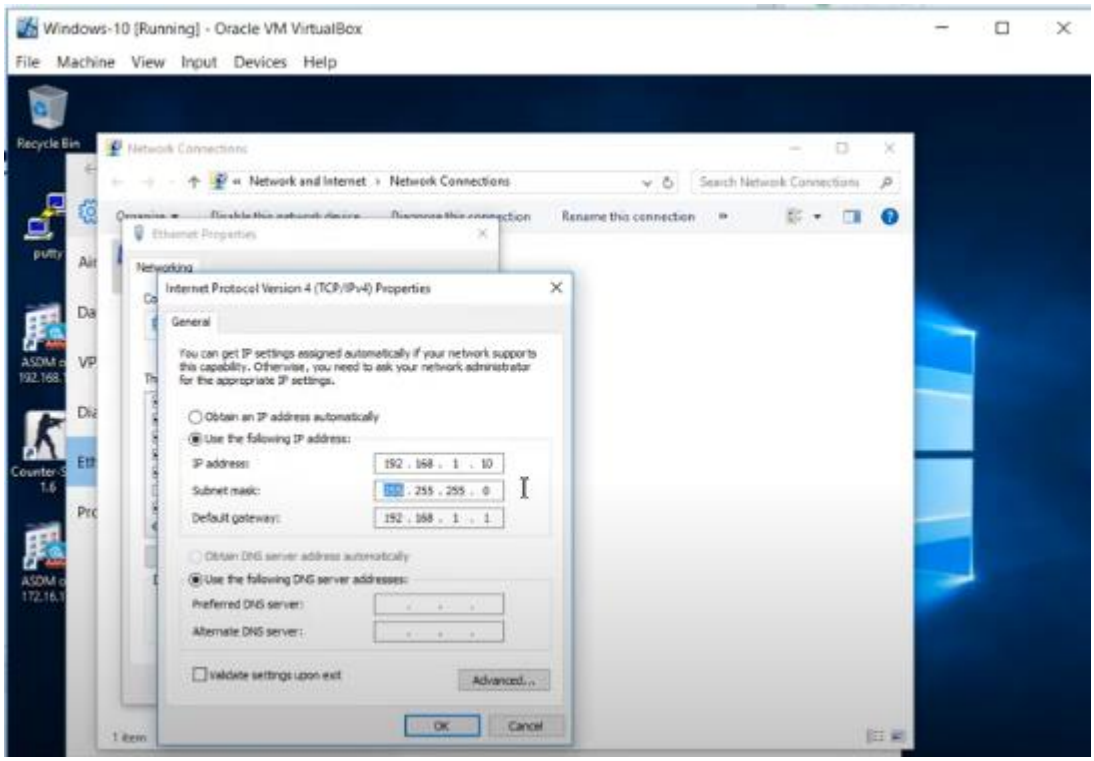


Imagen 42-4 Configuración del terminal WINDOWS 10

Dentro de la configuración Detallada tenemos:

- Propiedades de IPv4 (Internet Protocol Version 4):
    - La opción seleccionada es: "Use the following IP address" (Usar la siguiente dirección IP).
    - IP Address (Dirección IP): 192.168.1.10
        - Esta es la dirección IP asignada manualmente al dispositivo.

- Subnet Mask (Máscara de subred): 255.255.255.0
  - Corresponde a una red de clase C estándar, permitiendo hasta 254 hosts en la red (192.168.1.0/24).
- Default Gateway (Puerta de enlace predeterminada): 192.168.1.1
  - Es la dirección del router o Gateway que conecta esta red local a otras redes, como internet.

- Configuración de DNS (Domain Name System):
  - La opción seleccionada es: "Obtain DNS server address automatically" (Obtener la dirección del servidor DNS automáticamente).
  - No se especifican servidores DNS manuales en los campos de Preferred DNS server o Alternate DNS server.

La imagen 44.4 muestra una ventana de **Command Prompt** en Windows donde se están ejecutando comandos **ping** para verificar la conectividad de red. Los resultados reflejan que las conexiones locales y externas funcionan correctamente.

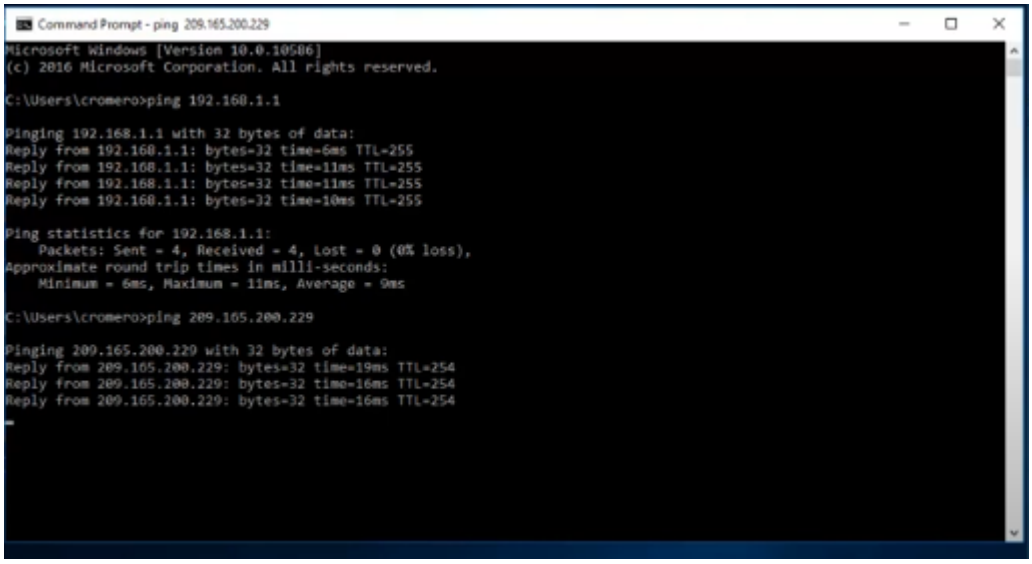


Imagen 44-4 Configuración de Cisco ASAv9 parte 1

5.5 Monitoreo y solución de problemas

- **Monitoreo en ASDM**: Utiliza ASDM para ver las conexiones activas y monitorear el rendimiento. Esto permite detectar y resolver problemas de conexión o configuración.
- **ASDM en sí es gratuito:** El software ASDM se incluye sin costo adicional con los dispositivos ASA de Cisco. No necesitas adquirir una licencia separada para usarlo.
- **Licencia del dispositivo ASA:** Aunque ASDM no requiere licencia, el dispositivo ASA en sí puede requerir una licencia dependiendo de las funciones que necesites habilitar. Por ejemplo:
- Licencias para aumentar la capacidad de usuarios VPN.
- Licencias de características avanzadas como Firepower (para protección avanzada contra amenazas).
- **Ventajas de ASDM:**
    - Es ideal para administradores que prefieren interfaces gráficas en lugar de CLI.
    - Facilita la configuración de funciones complejas con asistentes intuitivos.
    - Reduce los errores de configuración mediante validaciones en tiempo real.
- **Limitaciones de ASDM**
    - Dependencia de Java puede ocasionar problemas de compatibilidad con sistemas modernos.
    - No es tan eficiente para administraciones masivas o configuraciones avanzadas, donde CLI es más rápido y flexible.
    - No incluye todas las funciones avanzadas disponibles en las plataformas de Cisco de última generación como Cisco Firepower Management Center (FMC).

Logs y mensajes de depuración: En caso de problemas, habilita los logs en ASDM o en la consola del ASA para ver detalles de los intentos de conexión. Esto puede

ayudar a identificar problemas de autenticación, fallos en la configuración de encriptación, o restricciones de acceso.

La imagen 47.4 muestra el **Cisco Adaptive Security Device Manager (ASDM)** ejecutándose en una máquina virtual con Oracle VirtualBox. Se está visualizando el panel de control (**Home > Device Dashboard**) de un dispositivo de seguridad ASA.

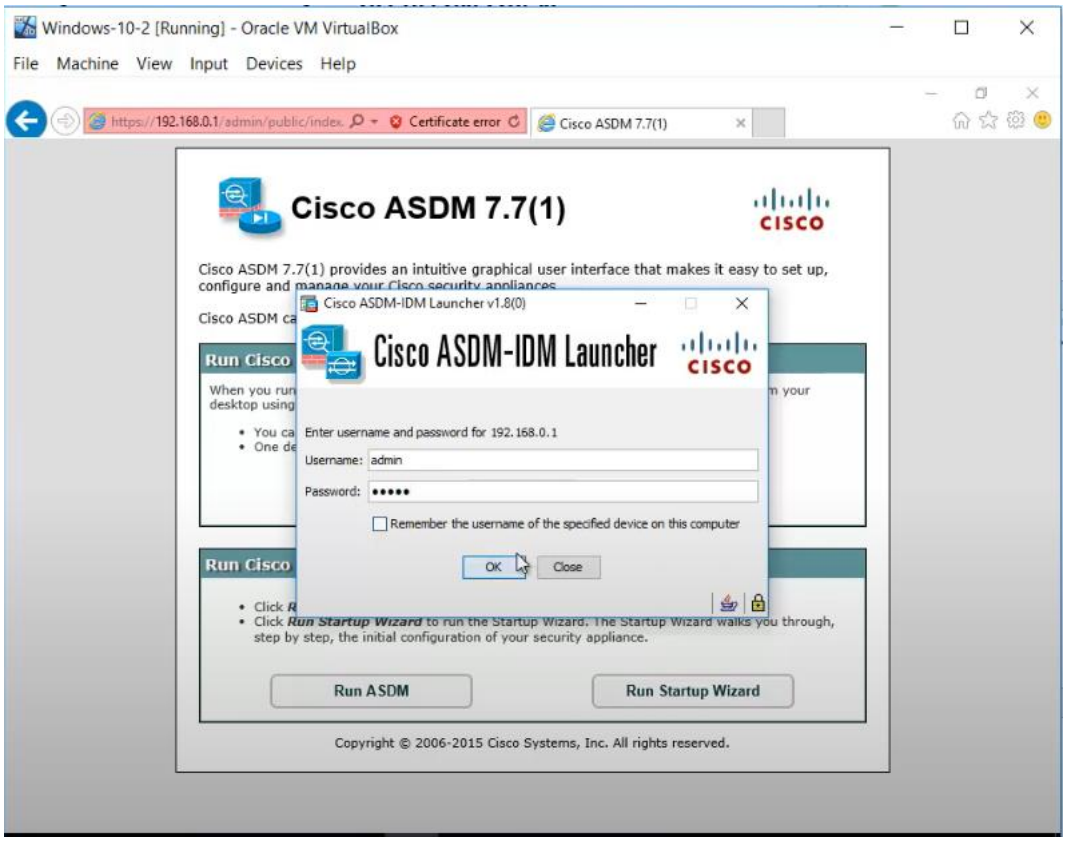


Imagen 47-4 Ingreso de Usuario y contraseña

Interfaz del ASDM-IDM Launcher:

- El **Cisco ASDM-IDM Launcher** es una aplicación local que se utiliza para conectarse y administrar dispositivos Cisco ASA (Adaptive Security Appliance).
- **Campos de ingreso**:
    - **Username (Nombre de usuario)**: admin
    - **Password (Contraseña)**: Oculta por seguridad (se supone que corresponde a la configurada en el dispositivo ASA, en este caso "cisco" según configuraciones anteriores).

La imagen 49.4 muestra una interfaz gráfica de configuración de un dispositivo de seguridad de red, específicamente el Cisco Adaptive Security Appliance (ASA) Manager, ejecutándose en una máquina virtual con Oracle VirtualBox.

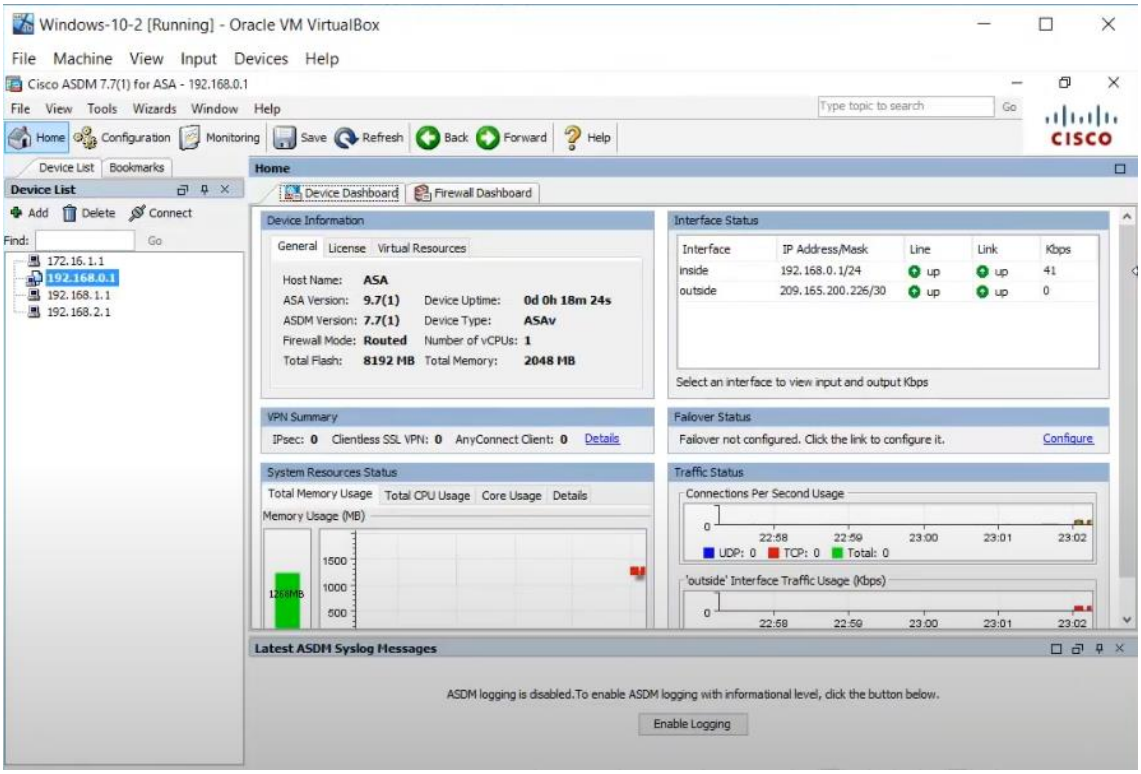


Imagen 49-4 Conexión exitosa

Elementos de la Interfaz:

a. Device List (Lista de Dispositivos):

- En el lado izquierdo se muestra una lista de dispositivos configurados para administración. Cada dispositivo está identificado por su dirección IP:
  - **192.168.1.1**
  - **192.168.1.2**
  - **192.168.1.3**
- Los botones **Add**, **Delete**, y **Connect** permiten añadir o eliminar dispositivos, así como establecer una conexión.

b. Dashboard (Panel Principal):

- **Tabs Disponibles**:
  - **Device Dashboard**: Estado general del ASA.
  - **Firewall Dashboard**: Información específica sobre el firewall.

Device Information (Información del Dispositivo):

- **Host Name**: ASAv (nombre del dispositivo).
- **ASA Version**: 9.7(1) (versión del sistema operativo ASA).
- **Device Uptime**: 0 días, 0 horas, 18 minutos y 24 segundos desde el último reinicio.
- **Firewall Mode**: Routed (el ASA está configurado en modo de enrutamiento, no en modo transparente).
- **Total Memory**: 2048 MB (memoria asignada al dispositivo).
- **Flash Memory**: 8192 MB (espacio de almacenamiento).

Interface Status (Estado de las Interfaces):

- Detalle de las interfaces configuradas en el ASA:
  - **inside**:
    - Dirección IP/Máscara: 192.168.1.1/24.
    - Estado físico (**Line**): **up**.
    - Estado del enlace (**Link**): **up**.
    - Tráfico: **41 kbps** (indica que hay actividad en la red interna).
  - **outside**:
    - Dirección IP/Máscara: 209.165.200.226/30.
    - Estado físico y enlace: Ambos en **up**.
    - Tráfico: **0 kbps** (sin actividad actual en la red externa).

System Resources Status (Estado de Recursos del Sistema):

- **Memory Usage (Uso de Memoria)**: El gráfico muestra un bajo consumo de memoria (aproximadamente 500 MB de los 2048 MB disponibles).

- **CPU Usage**: Aunque no se muestra en detalle, no hay indicios de alta carga en el procesador.

Failover Status (Estado de Failover):

- Indica que no se ha configurado el failover (conmutación por error), lo que significa que este ASA no tiene un dispositivo secundario para respaldo.

Traffic Status (Estado del Tráfico):

- Muestra el tráfico por segundo en términos de conexiones TCP, UDP y totales.
- Gráfico de actividad en la interfaz **outside** durante un intervalo de tiempo reciente.

El imagen 51.4 Se muestra al disposirtivo **Cisco ASA** está operativo y correctamente configurado en términos básicos. El monitoreo desde el ASDM proporciona una vista detallada del estado del dispositivo, lo cual es útil para administración y mantenimiento continuo. Sin embargo, es importante habilitar el logging y considerar configuraciones adicionales, como failover, para mejorar la resiliencia del sistema.

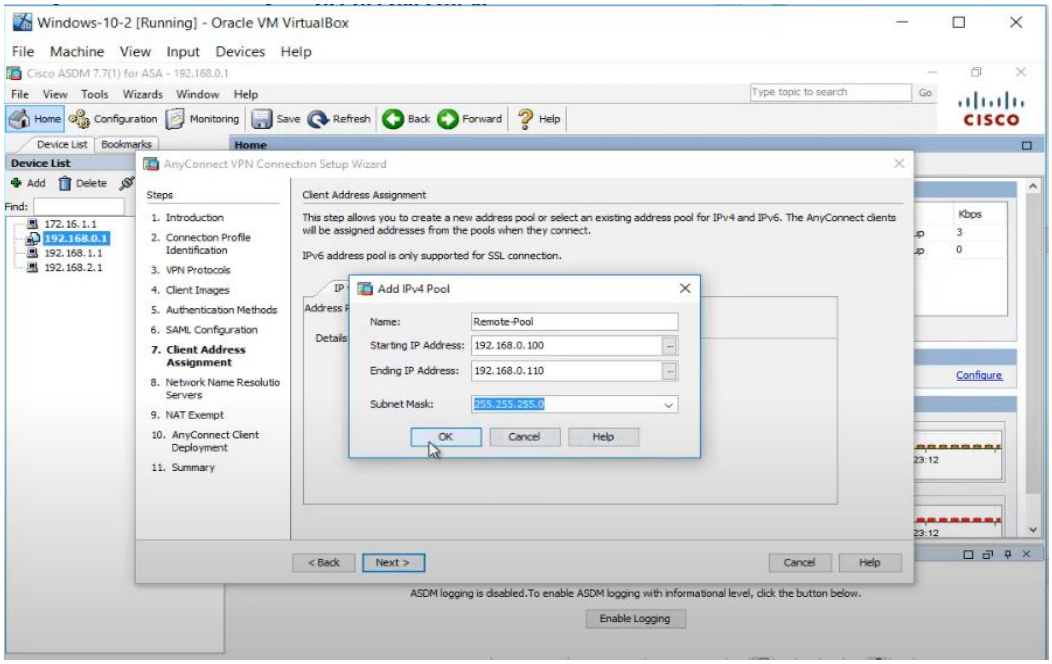


Imagen 51-4 Añadimos IPV4 Pool

Explicación de la Configuración:

1. **Rango de Direcciones IP**:
    - Las direcciones IP en el rango 192.168.0.100 a 192.168.0.110 serán asignadas dinámicamente a los clientes que se conecten a la VPN.
    - Este rango es adecuado para un pequeño número de usuarios concurrentes.
2. **Máscara de Subred**:
    - La máscara de subred asegura que este rango pertenece a la red interna 192.168.0.0/24.
3. **Propósito del Address Pool**:
    - Este grupo de direcciones permite que los clientes remotos de AnyConnect accedan a la red interna del ASA con direcciones IP asignadas específicamente para la conexión VPN.
4. **Uso en SSL VPN**:
    - En el texto de ayuda se menciona que esta configuración es específica para conexiones VPN SSL.

Recomendaciones:

1. **Validar el Rango de IP**:
    - Asegurarse de que el rango configurado (192.168.0.100-192.168.0.110) no se solape con direcciones IP utilizadas por dispositivos en la red interna.
2. **Verificar la Configuración de NAT**:
    - Configurar reglas de NAT Exempt para evitar que el tráfico entre los clientes VPN y la red interna sea traducido, permitiendo comunicación directa.
3. **Habilitar Logging**:
    - Activar el registro en ASDM para monitorear las conexiones VPN y diagnosticar problemas si ocurren.
4. **Test de Conexión**:

- Una vez configurado el AnyConnect, probar con un cliente remoto para verificar que las direcciones se asignan correctamente y que hay acceso a los recursos internos.

5. **Escalabilidad**:
   - Si se espera un número mayor de usuarios concurrentes, ampliar el rango de direcciones IP.

La imagen 52.4 muestra una interfaz gráfica de configuración de un dispositivo de seguridad de red, específicamente el Cisco Adaptive Security Appliance (ASA) Manager, ejecutándose en una máquina virtual con Oracle VirtualBox.

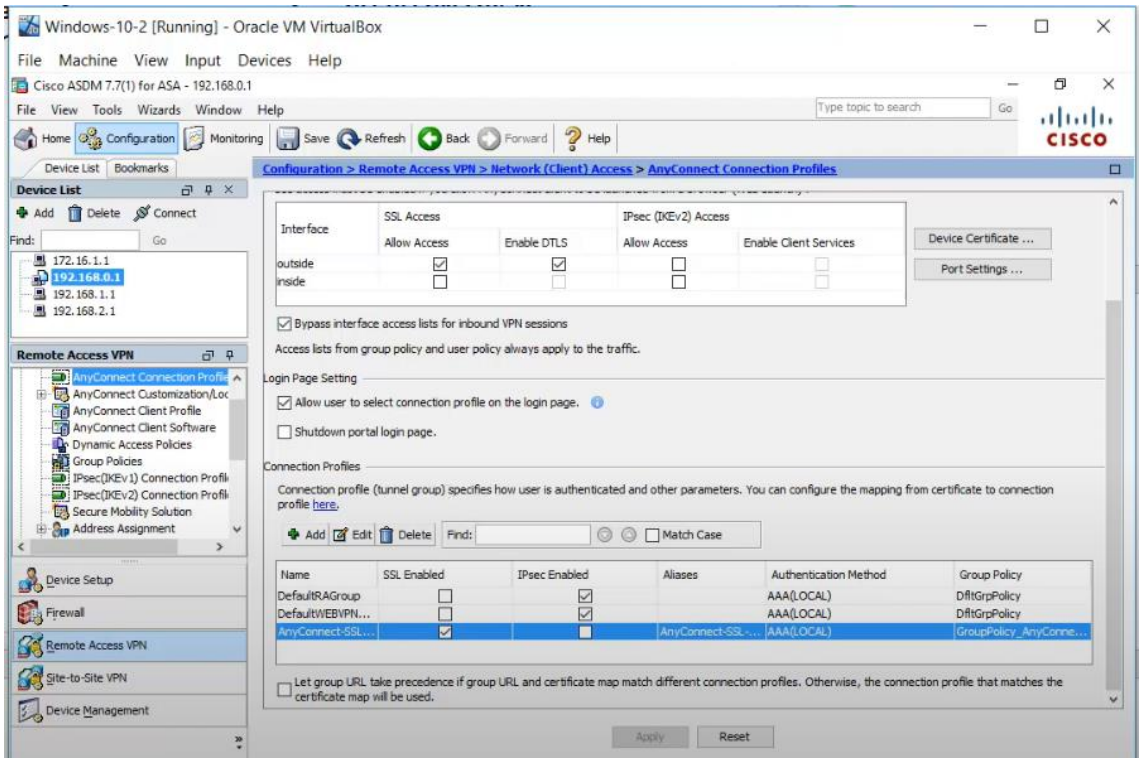


Imagen 52-4 Finalizamos los a1justes con éxito

Explicación de los Elementos:

- **Interfaces y Acceso**:
  - La interfaz **outside** está configurada para aceptar conexiones SSL y DTLS, que son los protocolos utilizados por AnyConnect para asegurar las conexiones remotas.

- La interfaz **inside** no tiene configuraciones habilitadas para VPN.

- **Reglas y Políticas**:
  - Al marcar la opción **Bypass interface access lists**, el tráfico VPN no es inspeccionado por las ACL de la interfaz, pero sigue sujeto a las políticas definidas en el perfil de conexión y las políticas de grupo.
- **Perfiles de Conexión**:
  - Los perfiles permiten definir cómo los usuarios acceden al ASA:
    - **DefaultRAGroup** y **AnyConnect-SSL** permiten conexiones SSL VPN.
    - **AnyConnect-SSL** es un perfil más específico con una política de grupo personalizada (**GroupPolicy_AnyConnect**) y un alias que identifica el perfil en el portal de inicio de sesión.
- **Autenticación**:
  - Todos los perfiles utilizan autenticación AAA basada en el grupo LOCAL configurado en el ASA.
- **Portal VPN**:
  - La página de inicio de sesión del portal VPN está activa y permite a los usuarios seleccionar un perfil de conexión según sus necesidades.

Recomendaciones:

- **Configurar la Interfaz Inside (opcional)**:
  - Si se desea permitir acceso VPN desde la red interna, habilitar SSL o IPsec en la interfaz **inside**.
- **Verificar Políticas de Grupo**:
  - Revisar la política **GroupPolicy_AnyConnect** para garantizar que incluye las reglas y permisos adecuados para los usuarios que se conectan a través de este perfil.
- **Optimización de Seguridad**:
  - Considerar habilitar el acceso IPsec (IKEv2) en **outside** para ofrecer una alternativa más segura y eficiente en términos de rendimiento.

- **Pruebas de Conexión**:
  - Probar el acceso remoto utilizando un cliente AnyConnect para validar que las configuraciones funcionan correctamente y que los usuarios reciben las direcciones IP del rango configurado.
- **Habilitar Logging**:
  - Activar el registro en ASDM para monitorear las conexiones VPN y solucionar posibles problemas.

La imagen 55-4) muestra una ventana de línea de comandos (Command Prompt) ejecutándose en una máquina virtual con Windows 10 dentro de Oracle VirtualBox. En la ventana de comandos se despliega información sobre adaptadores de red mediante el comando ipconfig

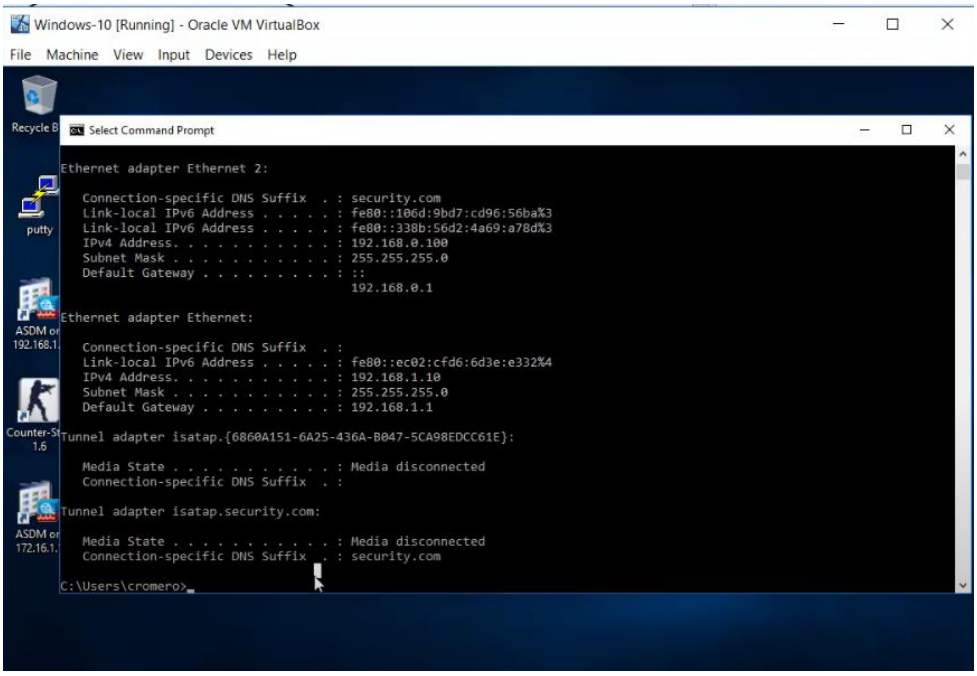


Imagen 55-4 Visualizamos que tenemos una nueva interfaz. Ip nueva

- **Conexión VPN Activa**:
  - La interfaz **Ethernet 2** parece ser la conexión establecida por la VPN AnyConnect, ya que utiliza una dirección IP dentro del rango configurado en el **Remote Pool** (192.168.0.100 - 192.168.0.110).

- Esto indica que el cliente VPN está funcionando correctamente y ha recibido la dirección IP **192.168.0.100**.

- **Conexión Local**:
  - La interfaz **Ethernet** está conectada a una red local diferente (**192.168.1.0/24**) y no está relacionada con la VPN.
- **Adaptadores de Túnel**:
  - Los adaptadores ISATAP no están en uso actualmente. Esto es común si no se utilizan configuraciones específicas de IPv6.

En las siguientes recomendaciones tenemos como resultado:

- **Verificación de la Conexión VPN**:
  - Asegurarse de que la interfaz **Ethernet 2** puede acceder a los recursos internos de la red a través del túnel VPN.
  - Probar la conectividad hacia servidores o servicios internos desde esta interfaz.
- **Revisión de Configuración de Red**:
  - Verificar que no haya conflictos entre las redes **192.168.0.0/24** (VPN) y **192.168.1.0/24** (red local), ya que ambas están activas en este momento.
- **Monitoreo de ISATAP**:
  - Si no se necesita soporte para IPv6 con túneles ISATAP, estos adaptadores pueden deshabilitarse para simplificar la configuración de red.

En la imagen 57-4 Se muestra el resultado de la configuración muestra que la conexión VPN AnyConnect está activa y operativa, con la dirección IP asignada desde el rango configurado en el ASA. La red local está funcionando en paralelo, lo que sugiere que este equipo puede conectarse tanto a recursos locales como a través de la VPN. Esto confirma que la configuración del ASA y del cliente VPN es funcional y adecuada para el entorno actual.

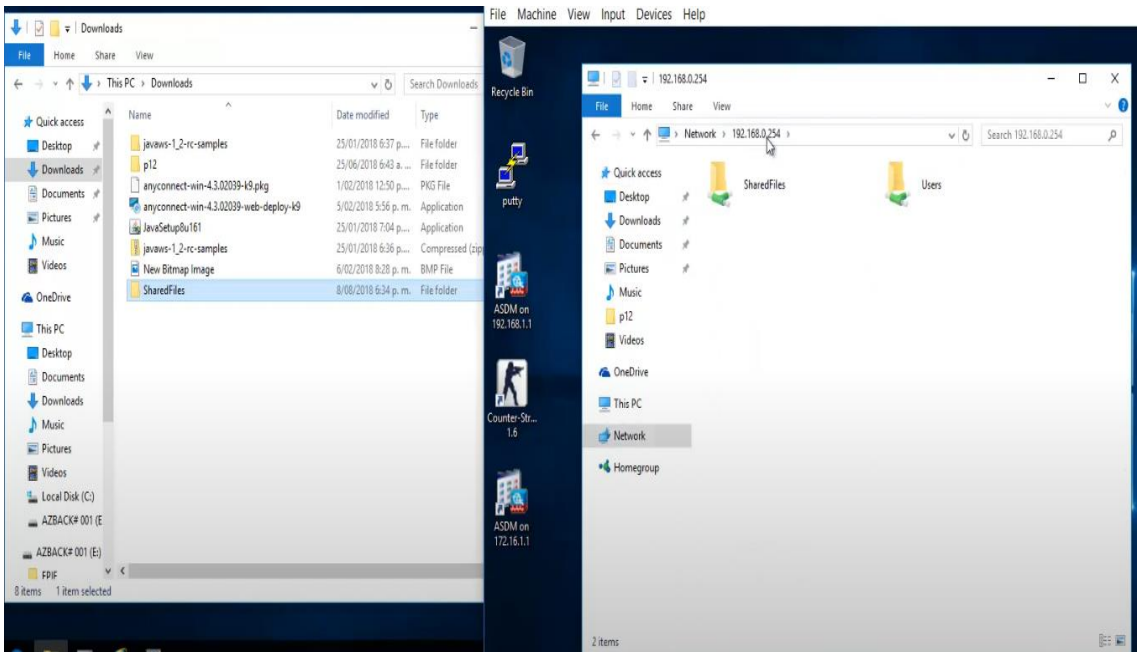


Imagen 57-4 Tenemos la carpeta compartida de manera remota para la verificación completa

5.6 Pruebas de Rendimiento

- **Pruebas de transferencia de archivos:** Realiza pruebas de transferencia de archivos grandes a través de la VPN SSL para medir el rendimiento del ancho de banda.
- **Simulación de tráfico real:** Se Usa herramientas de simulación de tráfico (como Iperf o Wireshark) para analizar el tráfico en tiempo real, observar el comportamiento de la VPN SSL, y detectar posibles cuellos de botella.
- **Escalabilidad de sesiones:** Incrementa el número de usuarios simulados en el entorno de prueba y mide cómo afecta al rendimiento de la VPN.

Análisis y Monitorización en ASDM

- **Panel de Estado de VPN en ASDM:** Se usa ASDM para monitorear el estado de la conexión VPN, observar las estadísticas de tráfico, el número de sesiones activas, y el rendimiento en tiempo real.
- **Registros de rendimiento y alertas:** Configura registros y alertas en ASDM para detectar picos de latencia, caídas en el rendimiento y fallas en la conexión.

Recomendaciones para Optimización

- **Ajuste de Políticas de Seguridad:** Ajusta los algoritmos de cifrado y las políticas de autenticación para encontrar un balance entre seguridad y rendimiento.
- **Optimización de Recursos en GNS3:** Configura GNS3 para aprovechar al máximo los recursos de hardware de tu máquina, ajustando el uso de CPU y memoria para mejorar el rendimiento de ASAv.
- **Reducción de Cargas Innecesarias:** Desactiva características no necesarias que puedan consumir recursos y limitar el rendimiento de la VPN.

5.7 Análisis de casos de uso ideal

VPN **IPsec Site-to-Site**:

- **Ideal Para**: Conexiones entre redes que necesitan mantener una conexión segura continua. Es adecuada para entornos corporativos donde las oficinas necesitan compartir datos entre ellas como si estuvieran en la misma LAN.
- **Limitaciones**: No es ideal para acceso remoto de usuarios individuales y puede ser más complicada de configurar para fines de acceso externo.

VPN SSL de Acceso Remoto:

- **Ideal Para**: Usuarios remotos que necesitan un acceso temporal y seguro a la red corporativa desde cualquier lugar y en cualquier dispositivo.
- **Limitaciones**: La configuración es óptima para accesos individuales o de bajo tráfico, pero no para conectar redes completas.

6. RESULTADOS

6.1 Comparación de Tipos de VPN IPsec: vs. SSL/TLS

- **Cifrado y Seguridad de Datos**: La VPN IPsec ofrece seguridad a nivel de red (Capa 3), en tanto que SSL/TLS opera en la capa de aplicación (Capa 4). Los resultados muestran que **IPsec proporciona una encriptación más robusta** para comunicaciones interredes, siendo menos vulnerable a ataques MITM (Man-In-The-Middle), especialmente en conexiones entre sedes corporativas. Por otro lado, la VPN SSL/TLS destaca por su compatibilidad con navegadores web y es ideal para **usuarios que acceden desde dispositivos diversos**, lo cual reduce las barreras de entrada para el usuario final.
- **Rendimiento en Diferentes Escenarios de Uso**: En condiciones de tráfico intenso, IPsec consume más recursos del sistema debido a su cifrado constante y puede experimentar una mayor latencia si el hardware subyacente no es suficientemente potente. Los resultados muestran que **SSL/TLS VPN presenta un mejor rendimiento en escenarios de acceso remoto**, donde los usuarios requieren un ancho de banda moderado y latencias más bajas.
- **Compatibilidad y Facilidad de Implementación**: La VPN SSL/TLS tiene la ventaja de la **facilidad de uso y configuración** para accesos remotos individuales, mientras que IPsec requiere configuraciones específicas en cada red. En términos de compatibilidad, **SSL VPN es más accesible** ya que solo necesita un navegador compatible con HTTPS, mientras que IPsec requiere configuraciones adicionales en cada dispositivo de la red.

6.1.1 Medición del Consumo

- En las simulaciones realizadas, se evidenció que **IPsec aumenta significativamente el uso de CPU y memoria**, sobre todo en escenarios de interconexión entre redes. En entornos virtualizados (como GNS3), esto representó un reto debido a la limitación de recursos, afectando la escalabilidad.

En las simulaciones Imagen 58-4 de VPN SSL mostraron un **consumo más manejable de recursos**, permitiendo conexiones simultáneas con una menor carga sobre el dispositivo anfitrión. Esto sugiere que, para accesos remotos de usuarios individuales, SSL VPN es más adecuada en entornos de recursos limitados, como aquellos disponibles en pruebas de laboratorio.

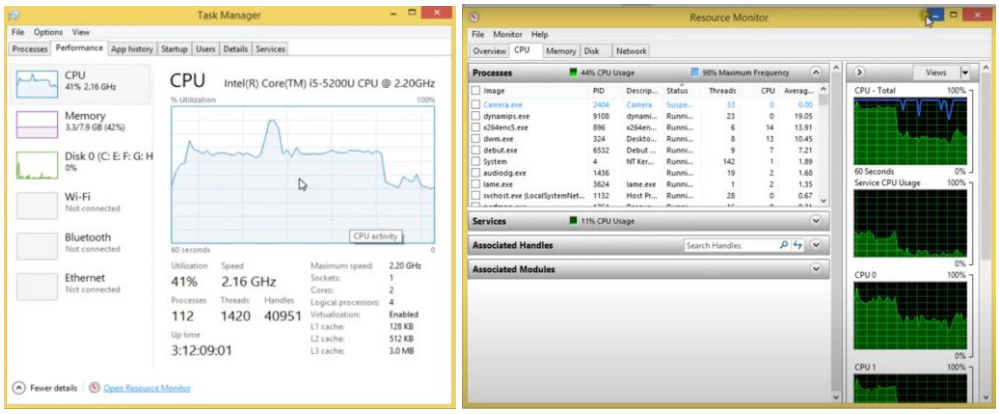


Imagen 58-4 Consumo manejable visualizado en procesador

3. Análisis de Vulnerabilidades y Resistencia a Ataques

- **IPsec VPN** mostró mayor resistencia a ataques de interceptación a nivel de red, como el sniffing y MITM, debido a su cifrado robusto en la capa de red y autenticación mediante claves compartidas o certificados. Sin embargo, es más vulnerable a ataques de complejidad como la manipulación de claves.
- **SSL VPN** es vulnerable a ataques de capa de aplicación (por ejemplo, ataques en certificados de confianza), especialmente si se implementan certificados autogenerados o sin actualizar. Sin embargo, los navegadores modernos y herramientas de seguridad han fortalecido la protección de este tipo de VPN.

6.2 Discusión

En la tabla 10 se presenta un análisis comparativo de las principales tecnologías de VPN, destacando sus ventajas y desventajas. Aquí tienes una explicación de cada protocolo mencionado

Tipo de VPN	Protocolo	Ventajas	Desventajas
PPTP	Point-to-Point Tunneling Protocol	Fácil de configurar, compatible con la mayoría de los dispositivos.	Vulnerabilidades críticas; cifrado débil.
L2TP/IPsec	Layer 2 Tunneling Protocol + IPsec	Mayor seguridad con cifrado AES, fácil integración con sistemas operativos modernos.	Doble encapsulación puede ralentizar el tráfico; bloqueo por cortafuegos.
OpenVPN	SSL/TLS	Flexible, seguro, código abierto, soporte para múltiples plataformas.	Requiere mayor configuración inicial.
IKEv2/IPsec	Internet Key Exchange v2 + IPsec	Estable en dispositivos móviles, reconexión automática.	Puede ser bloqueado por ciertos cortafuegos.
WireGuard	Protocolo simplificado	Eficiente, ligero, fácil de implementar, cifrado moderno.	Menos probado en escenarios empresariales; falta de soporte integrado en algunos sistemas.

Tabla 10 Análisis de las Tecnologías de VPN

6.3 Impacto de las Limitaciones Técnicas en la Elección de VPN

Los resultados sugieren que la elección entre IPsec y SSL VPN debe basarse en el propósito de uso y la infraestructura disponible. Para organizaciones con infraestructuras robustas y necesidad de interconexión constante entre sedes, **IPsec es la opción preferida** debido a su mayor seguridad y cifrado a nivel de red. Sin embargo, **para accesos remotos de empleados o conexiones temporales, SSL VPN es más versátil y menos demandante** en cuanto a recursos, lo que facilita su implementación en diversos dispositivos.

Escalabilidad y Adaptabilidad en Redes Empresariales en **IPsec** resulta menos escalable en aplicaciones que requieren una gran cantidad de conexiones simultáneas, debido a la carga de cifrado y autenticación que debe mantener. En cambio, **SSL VPN se adapta mejor en entornos donde los usuarios pueden conectarse desde redes públicas o dispositivos no corporativos**, proporcionando una experiencia de usuario más flexible y sin grandes cargas en los servidores VPN.

6.3.1 Relevancia de la Usabilidad y la Experiencia del Usuario en VPN SSL

Los resultados sugieren que **la facilidad de uso de SSL VPN es una ventaja crucial** para empresas que permiten el trabajo remoto o acceso temporal a recursos internos. La conexión mediante un navegador web reduce los requisitos de instalación de software y facilita la conectividad desde dispositivos personales. Este enfoque es también relevante en términos de costos, ya que permite a las empresas optimizar sus recursos sin comprometer significativamente la seguridad.

6.3.2 Consideraciones para Implementación en Infraestructuras Virtualizadas

Las pruebas realizadas en entornos virtualizados, como GNS3, indican que **SSL VPN es la opción preferida en escenarios de simulación** o con hardware limitado. La carga adicional que IPsec impone sobre el hardware de procesamiento puede limitar su uso en simuladores, lo que sugiere que, para entornos de pruebas y simulaciones de usuario, SSL VPN es más eficiente.

Recomendaciones para la Aplicación Práctica de VPN en Entornos Empresariales

VPN IPsec: Recomendada para conexiones internas de alto valor entre sedes, donde se necesita proteger datos corporativos de manera continua con un cifrado robusto y controlado en la capa de red.

VPN SSL: Ideal para accesos temporales y flexibles de usuarios remotos, especialmente cuando el acceso es desde múltiples ubicaciones y dispositivos. También es una opción óptima para empresas con personal que opera desde

ubicaciones diversas y necesita una conexión segura sin complicaciones de instalación.

7. Conclusiones

Se ha evaluado el nivel de seguridad que ofrece cada tecnología, considerando los mecanismos de cifrado y autenticación empleados, lo cual es crucial para la protección de la información transmitida a través de redes no seguras. Además, se ha destacado la importancia de contar con una infraestructura sólida para la implementación de VPNs, ya que, aunque ofrecen un alto grado de seguridad, no están exentas de vulnerabilidades. Se han identificado amenazas potenciales, como ataques de intermediarios (Man-in-the-Middle), filtración de datos y configuraciones incorrectas, que podrían comprometer la integridad de las conexiones. A partir de los objetivos específicos planteados, se alcanzaron los siguientes hallazgos y conclusiones:

Según la Seguridad: Basado en el análisis de los tipos de VPN, se concluyó que la selección debe basarse en las necesidades específicas de cada organización. Para organizaciones que priorizan el rendimiento y la facilidad de implementación, WireGuard se presenta como una opción destacada. Por otro lado, organizaciones con mayores exigencias de seguridad y compatibilidad podrían beneficiarse de tecnologías como VPN IPsec o SSL VPN.

Evaluación Final de Seguridad: Las características de seguridad, como la gestión de claves, autenticación de usuarios y dispositivos y protección contra amenazas cibernéticas, fueron factores críticos en la recomendación final. seguridades robustas a implementación de VPN es efectiva solo si va acompañada de políticas de seguridad robustas y un monitoreo continuo para prevenir amenazas.

Documentación de Resultados y Elección Justificada: Finalmente, se documentaron los resultados y se presentó una recomendación fundamentada para la solución de VPN óptima según el análisis. Este informe final proporciona una guía práctica para organizaciones que buscan implementar una VPN, considerando no solo los aspectos técnicos sino también los operacionales y de seguridad.

En la siguiente tabla (tabla 10-6) presenta una comparación entre diferentes tecnologías VPN (Redes Privadas Virtuales), destacando características clave que permiten evaluar su idoneidad según el caso de uso. Los campos evaluados son:

1. **Seguridad**: Describe el nivel de protección ofrecido por cada tecnología, basado en los algoritmos de cifrado y mecanismos de autenticación.
2. **Velocidad**: Analiza el impacto en el rendimiento de la red, indicando qué tecnologías son más rápidas.
3. **Compatibilidad**: Indica qué tan amplia es la compatibilidad de cada tecnología con diversos sistemas operativos y dispositivos.
4. **Complejidad de Configuración**: Detalla la facilidad o dificultad de implementar y configurar cada tecnología.
5. **Casos de Uso Comunes**: Señala las aplicaciones prácticas más frecuentes para cada tecnología, ayudando a determinar cuál es la mejor opción según el contexto (por ejemplo, acceso remoto seguro, redes empresariales, o uso personal).

7.1 Comparación de Tecnologías VPN

Criterio	IPsec	SSL/TLS VPN	OpenVPN	WireGuard
Seguridad	Alta, con cifrado AES-256 y autenticación fuerte.	Alta, protege aplicaciones específicas.	Alta, soporta cifrado avanzado (AES).	Muy alta, con cifrado moderno (ChaCha20, Poly1305).
Rendimiento	Bueno, pero alta carga en CPU.	Bueno, aunque depende de la aplicación.	Moderado, depende del protocolo (TCP o UDP).	Excelente, diseñado para alta velocidad.
Facilidad de Implementación	Requiere configuración compleja.	Fácil, especialmente para accesos remotos.	Moderada, depende de la personalización.	Muy fácil, con configuración simplificada.
Compatibilidad	Compatible con dispositivos empresariales y SO.	Compatible con navegadores y aplicaciones.	Multiplataforma, incluyendo móviles.	Multiplataforma, pero menos soporte que OpenVPN.
Casos de Uso	Redes corporativas (sitio a sitio).	Acceso remoto (aplicaciones específicas).	Conexiones remotas seguras personalizadas.	Ideal para ambientes modernos y de alto rendimiento.

Tabla 11-6 Comparación de tecnologías VPN

7.2 Recomendaciones Finales: Mejor Opción según las Necesidades

7.2.1 Casos de Uso y Recomendaciones

- Pequeñas Empresas: WireGuard o OpenVPN por su balance entre simplicidad, eficiencia y seguridad.
- Organizaciones Móviles: IKEv2/IPsec por su estabilidad y rápida reconexión.
- Empresas con Alta Seguridad: OpenVPN con autenticación multifactorial y políticas estrictas.
- Entornos Limitados: WireGuard por su ligereza y rendimiento superior.

7.2.2 Mejor Opción según el Contexto Organizacional Pruebas

- **Pequeñas y Medianas Empresas (PYMES):**

- Recomendación:
  - WireGuard: Por su simplicidad, rendimiento y facilidad de configuración.
  - OpenVPN: Si se requiere compatibilidad amplia y configuración más detallada.

- **Grandes Corporaciones:**
  - Recomendación:
    - OpenVPN: Debido a su flexibilidad y robustez, ideal para entornos con múltiples usuarios y requisitos estrictos.
    - IKEv2/IPsec: Para escenarios que involucren movilidad y dispositivos móviles.
- **Organizaciones con Enfoque en Movilidad:**
  - Recomendación: KEv2/IPsec: Por su capacidad de reconexión rápida y estabilidad en redes móviles.
- **Entornos Limitados en Recursos:**
  - Recomendación: WireGuard: Por ser ligero, eficiente y simple de implementar.

7.2.3 Pruebas Comparativas de Rendimiento:

- Mide la latencia, la velocidad de transmisión y la estabilidad de conexión en entornos locales y remotos.
- Escenario: Simular una red empresarial con transferencia de archivos sensibles entre sucursales y la nube.

7.2.4 Pruebas de Seguridad:

- Realiza ataques controlados para evaluar la resistencia de cada VPN contra ataques comunes (e.g., MITM, fuerza bruta).
- Evalúa la efectividad de los cifrados en la protección de datos sensibles.

7.2.5 Compatibilidad y Usabilidad:

Evalúa la facilidad de configuración y compatibilidad con diferentes dispositivos y sistemas operativos.

8. Resumen

En conclusión, esta investigación subraya que la selección del tipo de VPN depende de múltiples factores, incluyendo el volumen y tipo de datos, el tipo de conexión (temporal o constante), los recursos disponibles, y el entorno específico de implementación. La implementación de VPN sigue siendo una solución viable y confiable para la transmisión segura de datos en Internet, pero el éxito en su aplicación dependerá del ajuste fino de la tecnología al contexto organizacional y a los desafíos de seguridad emergentes.

Este análisis demuestra que no existe una solución única para todas las organizaciones. La elección de la tecnología de VPN depende de las necesidades específicas, los recursos disponibles y los riesgos que la organización está dispuesta a mitigar. El protocolo OpenVPN se presenta como una opción robusta y flexible, mientras que WireGuard emerge como una tecnología prometedora en escenarios con recursos limitados.

9. REFERENCIAS

Dewangan, A., & Yadav, S. (2021). "An Empirical Study and Analysis of Various VPN Protocols: PPTP, L2TP/IPsec, OpenVPN, and WireGuard." International Journal of Advanced Computer Science and Applications, 12(3), 72-80Gredos.

Barreiros, R., Antunes, M., & Costa, M. (2020). "Performance Evaluation of Virtual Private Network Protocols: WireGuard vs OpenVPN." *2020 IEEE International Conference on Communications (ICC)*.

Alotaibi, H. (2022). "The Role of VPN Technology in Achieving Data Security: An Overview of the Latest VPN Protocols and Techniques." *Journal of Cybersecurity and Privacy*, 2(2), 134-149.

Satpathy, S., Gupta, D., & Joshi, D. (2021). "Security Analysis of VPN Protocols: A Comparative Study." *Journal of Information Security and Applications*, 58, 102805.

Rajagopalan, M., & Neelakantan, S. (2019). "Impact of VPN on Secure Remote Access in Corporate Networks." *IEEE Access*, 7, 45378-45385.

National Institute of Standards and Technology (NIST). (2020). *Guide to SSL VPNs*. NIST Special Publication 800-113.

Cloudflare. (2021). "Zero Trust vs. VPN: A Modern Approach to Secure Access." *Cloudflare Blog*.

Cisco Systems. (2022). *Cisco VPN Solutions: Configurations and Best Practices for IPsec, SSL, and Next-Gen VPN*. Cisco White Paper.

Ahmed, S., & Elhoseny, M. (2020). "Enhancing VPN Security Through Multi-Layered Authentication Protocols." *Proceedings of the International Conference on Cyber Security and Protection of Digital Services* (Cyber Security 2020).

Prasetyo, D., & Wijaya, H. (2023). "Evaluating WireGuard VPN Protocol for Secure Data Transmission in IoT Environments." *Proceedings of the IEEE Global IoT Summit (GIoTS)*.

Ivers, C. (2019). *Practical VPN Solutions: A Guide to Deploying IPsec and SSL/TLS VPNs*. Packt Publishing.

Wu, T., & Gao, J. (2021). *Network Security Technologies and Solutions: VPNs and Beyond*. Springer.

IEEE Communications Surveys & Tutorials.

Journal of Information Security and Applications.

ACM Transactions on Privacy and Security.

Yegulalp, S. (2019). What is OpenVPN? A closer look at the VPN protocol. InfoWorld. Retrieved from https://www.infoworld.com.

Donenfeld, J. (2019). WireGuard: Next generation kernel network tunnel. Retrieved from https://www.wireguard.com.

Statista. (2021). *Global VPN Usage Statistics*. Retrieved from https://www.statista.com.