UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

"DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO DE RED PRIVADA VIRTUAL EN CAPA 3 UTILIZANDO CISCO IOS PARA LA UNIVERSIDAD NACIONAL DEL ALTIPLANO"

TESIS

PRESENTADO POR:

ARTURO IVAN ATENCIO MENDOZA

EVER JHONATAN MAMANI FIGUEROA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PUNO – PERÚ

2017

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

DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO DE RED PRIVADA VIRTUAL EN CAPA 3 UTILIZANDO CISCO IOS PARA LA UNIVERSIDAD NACIONAL DEL ALTIPLANO

TESIS PRESENTADA POR:

ARTURO IVAN ATENCIO MENDOZA

EVER JHONATAN MAMANI FIGUEROA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

FECHA DE SUSTENTACIÓN: 03-08-2017

APROBADO POR EL JURADO REVISOR CONFORMADO POR:

PRESIDENTE:
Dr. JOSE EMMANUEL CRUZ DE LA CRUZ

PRIMER MIEMBRO:
M.Sc. PEDRO BEJAR MUÑOZ

SEGUNDO MIEMBRO:
M.Sc. EDWIN WILBER CHAMBI MAMANI

DIRECTOR / ASESOR:
Dr. EUDES RIGOBERTO APAZA ESTAÑO

Área : Telecomunicaciones

Tema : Telecomunicaciones y Redes de Datos

Puno – Perú

2017

DEDICATORIA

La presente tesis va dedicada a mi Madre, ya que habiéndome criado sola logró hacer de mí un hombre de bien, además que, con su apoyo y tolerancia durante todo este tiempo, me dio las fuerzas necesarias para continuar en este difícil camino que es la vida. A mi padre y hermana por enseñarme a superar las tribulaciones del día a día.

Arturo Ivan Atencio Mendoza

Dedico este trabajo a las personas que siempre me han apoyado en todo momento y que no dudo lo seguirán haciendo por siempre, a las personas que siempre han estado conmigo. Con todo mi amor:

A MI MADRE

Maria Figueroa Anco

A MI HERMANO

Hector Mamani Figueroa

La familia que tanto amo.

Ever Jhonatan

AGRADECIMIENTO

Doy gracias a mi padre, mi madre y a mi hermana porque sin ellos no hubiera sido posible este objetivo, al Ing. José Cruz por ser mi mentor durante toda mi etapa universitaria y a todas las personas que me demostraron su cariño y soporte durante este periodo tan importante para mí.

Arturo Ivan Atencio Mendoza

AGRADECIMIENTO

Tengo mucho que agradecer a tantas personas que no quisiera omitir a nadie. Por eso, de antemano agradezco a todas las que han contribuido a la formación de mi persona como hijo, hermano, amigo, estudiante, alumno, compañero y, por consecuencia, como profesional.

Agradezco a DIOS por acompañarme siempre en todo lo que hago y permitirme llegar a este dichoso momento.

A mi Madre por darme la vida, el amor y el aliento que necesito para seguir adelante.

A Hector y Randy porque juntos crecimos, peleamos, sufrimos, lloramos, pero sobre todo reímos y compartimos grandes momentos de felicidad. Los quiero hermanos. Muchas gracias por todo.

A mis tíos Celestino, Leandra, Ovidio, Mauro, Mauricia, Percy, Carolina, Erasmo porque siempre fueron los que me llenaban de palabras de aliento y motivación.

A mis abuelitos Vicentina y Froilan porque son el vivo ejemplo de sacrificio, lucha y trabajo constantes para que los hijos crezcan con valores y ganas de superación.

A todos mis docentes, gracias por contribuir a mi preparación profesional. De manera especial a quienes considero mis amigos y buenos profesionales; José Cruz, Ferdinand Pineda, Christian Romero, Luis Baca y Eudes Apaza por la gran amistad y los consejos que me brindaron, sin ningún otro título más que el de mis amigos, muchas gracias.

A mis amigos de Ingeniería Electrónica, de la cual me siento muy orgulloso de ser parte porque juntos emprendimos nuevos retos, logramos importantes logros en beneficio de nuestra carrera. Por la gran amistad que formamos a lo largo de nuestra vida universitaria.

A mi amigo Arturo Atencio por haberme permitido ser parte de este importante proyecto. Gracias por tu dedicación, esfuerzo y gran aporte.

A todos ustedes: mil gracias.

Los quiere y aprecia.

Ever Jhonatan

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INDICE DE ANEXOS

ÍNDICE DE ACRÓNIMOS

C

CA
: (Certificate Authorities) autoridad de certificación, certificadora o certificante es una entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública., *30*, *31*, *74*

CISCO IOS
: Sistema Operativo de Cisco, *2*, *13*, *14*, *15*, *16*, *19*, *59*, *68*, *77*, *117*

D

DH
: Diffie Hellfman, *38*, *40*, *45*, *46*, *50*, *53*, *54*, *55*

DSL
: (Encapsulating Security Payload) La Carga de Seguridad Encapsulada proporciona autenticación, integridad y confidencialidad, que protegen contra la manipulación de los datos y, sobre todo, proporcionar protección de contenido del mensaje., *23*, *28*

E

ESP
: (Encapsulating Security Payload) La Carga de Seguridad Encapsulada proporciona autenticación, integridad y confidencialidad, que protegen contra la manipulación de los datos y, sobre todo, proporcionar protección de contenido del mensaje., *37*, *38*, *46*, *47*, *48*

F

Firewall
: Corta fuegos es un dispositivo de seguridad de red que controla el tráfico de red entrante y saliente y decide si permitir o bloquear el tráfico específico basado en un conjunto definido de normas de seguridad. Firewall puede ser hardware, software o ambos., *97*, *98*

G

GRE
: Generic Routing Encapsulation, *22*, *23*, *25*, *26*, *74*

I

IETF
: (Internet Engineering Task Force) El Grupo de Trabajo de Ingeniería de Internet es una gran comunidad internacional abierta de diseñadores de red, operadores, vendedores e investigadores interesados en la evolución de la arquitectura de Internet y el buen funcionamiento de Internet., *36*, *37*

IKE, *38*, *39*, *44*, *46*, *47*, *50*, *51*, *52*, *53*, *54*, *64*, *65*, *66*, *67*, *87*, *89*, *94*, *98*, *117*

IP
: Internet Protocol, *22*, *26*, *27*, *30*, *31*, *32*, *37*, *48*, *56*, *57*, *58*, *65*, *67*, *74*, *75*, *79*, *80*, *82*, *83*, *84*, *85*, *89*, *95*, *101*, *103*, *107*, *138*

IPsec
: (Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado., *13*, *14*, *23*, *25*, *31*, *32*, *34*, *35*, *37*, *38*, *39*, *40*, *41*, *43*, *44*, *46*, *47*, *48*, *49*, *50*, *51*, *54*, *55*, *63*, *64*, *65*, *66*, *67*, *80*, *87*, *89*, *90*, *91*, *92*, *96*, *100*, *105*, *106*, *107*, *108*, *110*, *111*, *114*, *115*, *117*, *118*

ISAKMP
: Es un protocolo criptográfico que constituye la base del protocolo de intercambio de claves IKE., *50*, *51*, *54*, *64*, *66*, *87*, *88*, *110*, *114*, *117*

L

LAN
: (Local Area Network) Red de área local, es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios)., *13*, *14*, *16*, *19*, *20*, *21*, *61*, *63*, *68*, *90*, *100*, *117*, *119*

M

MD5
: Es un algoritmo de reducción criptográfico de 128-bits desarrollado por la Universidad de MIT el cual hoy día se utiliza con frecuencia como herramienta para validar si un archivo que se obtuvo de una fuente remota fue descargado correctamente., *34*, *38*, *39*, *43*, *45*, *99*

MPLS
: (Multiprotocol Label Switching) es un estándar IP de conmutación de paquetes del IETF, que trata de proporcionar algunas de las características de las redes orientadas a

RESUMEN

En la actualidad, la Universidad Nacional del Altiplano cuenta con un sistema de intercambio de información primordial para el trabajo de dicha institución. Mediante esta red se intercambian los datos de exámenes de admisión, ingresantes a esta casa superior de estudios, datos de los estudiantes, tales como notas, datos de los docentes, entre otros. Es así, que siendo esta red el eje principal para el trabajo de la Universidad Nacional del Altiplano, se encuentra expuesta a ataques cibernéticos y a riesgos de perdida de información que se envía entre las diferentes oficinas. Siendo la finalidad proteger esta información y sobre todo evitar la vulnerabilidad de estos datos una vez subidos a la Internet, es que se ha realizado el diseño y posterior implementación de un prototipo de Red Privada Virtual en la capa de Red, utilizando protocolos de enrutamiento óptimos para el tipo de información que se requiera enviar y protocolos de encriptación para el cifrado de estos datos, acoplándolos a CISCO IOS. Para lograr que la utilización de éste prototipo sea factible en la institución, se realizaron diferentes diseños que permitan la implementación real de la red privada virtual; además los resultados obtenidos en la pruebas del prototipo mostraron que nuestra red transmite los datos de un punto a otro encriptándolos y encapsulándolos con el conjunto de protocolos IPsec que trabaja en la capa 3 o capa de red configurada con Cisco IOS. Los resultados fueron obtenidos con los programas Packet Tracer y Wireshark siendo estos satisfactorios. De esta manera se comprobó que nuestro prototipo de Red Privada Virtual brinda la autenticación, integridad y confidencialidad a los paquetes transmitidos entre la Oficina de Tecnología e Informática y las coordinaciones académicas de la institución, teniendo como resultado una Red segura y confiable protegida en LAN y WAN con un rendimiento mínimo de 89.29% de los 56 datos transmitidos a partir de las pruebas realizadas, y fue implementada dentro del Laboratorio Cisco de la Universidad Nacional del Altiplano demostrando que esta red puede ser aplicada en equipos reales a todas las oficinas de la institución.

Palabras Clave: VPN, Capa de Red, CISCO IOS, IPsec.

ABSTRACT

At present, the National University of the Altiplano has a system of exchange of information primordial for the work of said institution. Through this network, the data of admission exams, entries to this superior study house, student data, such as notes, data of teachers, among others, are exchanged. Thus, since this network is the main axis for the work of the National University of the Altiplano, it is exposed to cyber-attacks and risks of loss of information sent between the different offices. Being the purpose to protect this information and especially avoid the vulnerability of this data once uploaded to the Internet, it has been made the design and subsequent implementation of a prototype of Virtual Private Network in the Network layer, using optimal routing protocols for the type of information required to be sent and encryption protocols for the encryption of these data, coupled to CISCO IOS. To make the use of this prototype feasible in the institution, different designs were made that allow the real implementation of the virtual private network; in addition the results obtained in the prototype tests showed that our network transmits the data from one point to another by encrypting them and encapsulating them with the set of IPsec protocols that works in layer 3 or network layer configured with Cisco IOS. The results were obtained with the programs Packet Tracer and Wireshark being these satisfactory. In this way, our prototype Virtual Private Network provides authentication, integrity and confidentiality to the packets transmitted between the Office of Technology and IT and the academic coordinations of the institution, resulting in a secure and reliable Network protected in LAN and WAN with a minimum yield of 89.29% of the 56 data transmitted from the tests carried out, also was implemented in the Cisco Laboratory of the National University of the Altiplano demonstrating that this network can be applied in real equipment to all the offices of the institution.

Keywords: VPN, network layer, CISCO IOS, IPsec.

CAPITULO I

INTRODUCCIÓN

La presente tesis denominada “Diseño e Implementación de un prototipo de Red Privada Virtual en Capa 3 utilizando CISCO IOS para la Universidad Nacional del Altiplano.”, está desarrollada para brindar una solución factible a la seguridad y protección en la transmisión de datos sensibles que se envían a través de las diferentes Oficinas de la Universidad Nacional del Altiplano.

Hoy en día con el avance exponencial de la tecnología de sistemas de información en las instituciones, las redes se vuelven más vulnerables ya que no cuentan con protocolos de seguridad o la seguridad implementada es básica. Además de ello, otro problema que se puede apreciar es la falta de interés por solucionar este tema, ya sea por desconocimiento o por falta de personal calificado para realizar estas labores. Actualmente son muy pocas las empresas que identifican este problema como grave y deciden implementar protocolos de seguridad en su red.

El trabajo de investigación realizado está dividido en las siguientes secciones:

En la primera sección citamos las referencias teóricas así como los antecedentes que sustentan nuestro trabajo y la hipótesis que se plantea para nuestra investigación.

En la segunda sección describimos los materiales experimentales utilizados para la investigación así como el procedimiento experimental para el diseño e implementación de nuestra VPN.

En la tercera sección se presentan los resultados obtenidos a partir de nuestras experiencias al desarrollar la tesis, mostrando las diferentes etapas de los resultados así como su análisis e interpretación de los mismos.

Por último se muestran las conclusiones a las que se llegó en nuestra investigación, las recomendaciones que sugerimos los tesistas, las referencias utilizadas en el proceso de elaboración de la tesis y los anexos que corresponden.

La presente investigación tuvo como objetivo principal el realizar un diseño y posterior implementación de un prototipo de Red Privada Virtual que permita asegurar y encriptar la información compartida entre las oficinas pertenecientes a la Universidad Nacional del Altiplano.

De la misma forma se definieron como objetivos específicos, diseñar el prototipo de la Red Privada Virtual para operar y controlar el tráfico en LAN y WAN e implementar la Red Privada Virtual en el Laboratorio de Cisco de la Universidad Nacional del Altiplano.

1.1. PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN.

1.1.1. Descripción del Problema

La Universidad Nacional del Altiplano, se ha convertido en una de primeras universidades en consolidar la acreditación de sus carreras profesionales y su posterior licenciamiento institucional, es así que toda la información sensible de ésta institución está migrando a ambientes que involucran el uso de equipos de cómputo, servidores y

redes de datos, y para proteger dicha información se deben considerar los múltiples ataques que sufren; por tal motivo es necesario implementar un sistema de seguridad virtual para enfrentar las amenazas y vulnerabilidades tales como: el robo de información, modificación de datos, denegaciones de servicio, suplantaciones de datos, uso de equipos de cómputo para actividades maliciosas, entre muchos otros.

Según el análisis de 115 000 dispositivos en Internet, descubrió que el 92% de ellos ejecutaba software con vulnerabilidades conocidas. (Cisco, 2016)

Por lo tanto para proteger el intercambio de estos datos y garantizar la seguridad de la información sensible, cumpliendo con las políticas de la seguridad de la información utilizando protocolos adecuados, principalmente es necesario el ‘’**Diseño e Implementación de un prototipo de Red Privada Virtual en Capa 3 utilizando CISCO IOS para la Universidad Nacional del Altiplano**’’.

Además, de acuerdo a las necesidades de nuestra institución, se requiere el **“Diseño del prototipo de la Red Privada Virtual para operar y controlar el tráfico en LAN y WAN”** y la **“Implementación de la Red Privada Virtual en el Laboratorio de Cisco de la Universidad Nacional del Altiplano”**.

1.1.2. Justificación de la Investigación

1.1.2.1. Social

Una Red Privada Virtual dentro de la Universidad Nacional del Altiplano, permite brindar mayor seguridad en la recepción y transmisión de datos sensibles entre las diferentes oficinas de esta casa superior de estudios logrando una mejor confiabilidad por parte de los trabajadores así como una protección del Sistema Universitario de la Institución.

1.1.2.2. Técnica

Con este prototipo de red privada virtual se puede aprovechar las tecnologías que implementen seguridad, ya que estas tecnologías son utilizadas en la mayoría de dispositivos empleados en redes de internet.

1.1.2.3. Económica

La implementación de este prototipo es factible ya que los equipos utilizados en este diseño son similares a los equipos utilizados en la Oficina de Tecnología Informática (OTI) encargada de la administración de la red informática de la Universidad Nacional del Altiplano.

1.2. ANTECEDENTES DE LA INVESTIGACIÓN

En la actualidad se han expuesto diferentes proyectos sobre redes privadas virtuales, sin embargo la mayoría de estos son a nivel nacional e internacional, no habiendo encontrado precedentes sobre un estudio de VPNs a nivel local, por lo que esta investigación espera lograr una base confiable para futuros estudios.

A pesar de ello, la base de esta tesis cuenta con antecedentes solidos que facilitaron la mejor comprensión sobre diferentes temas en específico, los cuales serán nombrados a continuación.

1.2.1. Locales

Las telecomunicaciones son el medio imprescindible para la Universidad Nacional del Altiplano, por lo tanto, es una necesidad contar con servicios de telecomunicaciones más eficientes. De esta manera, el fin de este proyecto es diseñar una red de telecomunicaciones de Banda Ancha con tecnología Multipath TCP enfocada en el

desarrollo tecnológico que permita llevar a esta institución mejores servicios. Para lograr esto, se realizó un estudio del estado actual de los servicios de telecomunicaciones de la Institución, es así que se pudo realizar dicho estudio y proyectar la demanda de los servicios, realizando el diseño eficiente de una red de banda ancha utilizando Multipath TCP, para satisfacer dichas exigencias. (Alvarez Quispe, 2014)

1.2.2. Internacionales

Los desarrollos en Tecnologías de la Información y las Comunicaciones, han generado una convergencia de redes de infraestructura y servicios de valor agregado. En este estudio se presentan falencias en la administración y el mantenimiento de la central telefónica, donde el objetivo es enfatizar el uso de herramientas de seguridad habituales en las redes de datos. Mediante el estudio realizado al problema de la institución se logró realizar llamadas sin ningún tipo de restricciones, concluyendo que la situación descrita corresponde a un compromiso entre la necesidad de brindar acceso remoto al sistema telefónico de la institución y la facilidad de uso de dicho acceso. (Cutuli, Catania, & García Garino, 2012)

La seguridad es primordial en el correcto funcionamiento de las redes de datos; se plantea entonces una necesidad de identificar vulnerabilidades en estas redes, teniendo como objetivo determinar los tipos de ataques a las capas del modelo OSI y las formas de mitigarlos. Es así que el estudio recomienda comenzar por la configuración de los equipos Routers, ya que estos se pueden convertir en la primera línea de defensa contra los ataques informáticos. Por lo tanto se concluye que es importante tener en cuenta los aspectos mencionados en el estudio sobre los tipos de ataques, vulnerabilidades y forma de mitigación, para tener una visión más clara del impacto en las redes de las organizaciones. (Mejía Londoño, Ramírez Galvis, & Rivera Cradona, 2012)

1.3. IMPORTANCIA Y UTILIDAD DEL ESTUDIO

1.3.1. Impactos Esperados

i. Impactos en Ciencia y Tecnología

Se diseña una red con equipos de última generación y gamma alta, preparados para las exigencias de nuevas tecnologías. Además de ello la red es fortalecida con una programación protegida y encriptada, que resguarda la información y la defiende de ataque informáticos.

ii. Impactos económicos

La implementación de éste proyecto, conlleva a reducir gastos en la compra de equipos y software complementarios, ya que los equipos usados forman parte de la Red de la Universidad; además, con la protección implementada dentro de la programación de la Red, se podrá proteger los datos sensibles de la Institución, conservando así, la información necesaria y primordial para la Universidad sin necesidad de añadir gastos externos para dicho fin.

iii. Impactos sociales

Este proyecto brindará una mayor seguridad y confidencialidad a la información contenida dentro de la Red donde se implemente este diseño. Así también, se brinda protección a los datos que hoy en día son principales para la buena marcha de la institución.

iv. Impactos ambientales

El impacto ambiental será nulo. Debido a que los equipos Cisco donde se implementará el prototipo, tienen un impacto ambiental nulo en las zonas geográficas donde son instalados.

1.4. OBJETIVOS DE LA INVESTIGACIÓN

1.4.1. Objetivo general

Diseñar e implementar un prototipo de una Red Privada Virtual en Capa 3 utilizando CISCO IOS para las Oficinas de la Universidad Nacional del Altiplano.

1.4.2. Objetivos específicos

a) Diseñar el prototipo de la Red Privada Virtual para operar y controlar el tráfico en LAN y WAN.
b) Implementar la Red Privada Virtual en el Laboratorio de Cisco de la Universidad Nacional del Altiplano.

CAPITULO II

REVISIÓN DE LITERATURA

2.1. MARCO TEÓRICO

2.1.1. Red Privada Virtual

Hoy en día las soluciones, como los métodos de encriptación diferentes y PKI, hacen posibles que las empresas puedan ampliar sus redes de forma segura a través de Internet. Una forma en que las empresas amplíen sus redes es a través de las redes privadas virtuales (VPN). (Barker, Morris, Wallace, & Watkins, 2013)

2.1.2. Redes de Transmisión de Datos LAN y WAN

Para entender mejor el concepto y el contenido de una VPN, es necesario comprender las redes de transmisión de datos fundamentales, es por ello que a continuación se conceptualizará este tema para un mayor entendimiento de la investigación.

2.1.2.1. Red de Área Local (LAN)

Una red de área local, red local o LAN (del inglés local area network) es la interconexión de varias Computadoras y Periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, o con Repetidores podría llegar a la distancia de un campo

de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar Datos y Aplicaciones. En definitiva, permite una conexión entre dos o más equipos. El término red local incluye tanto el Hardware como el Software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información. (Anónimo, Red de Área Local (LAN), 2013)

Se usan para conectar computadoras personales o estaciones de trabajo, con objeto de compartir recursos e intercambiar información.

Están restringidas en tamaño, lo cual significa que el tiempo de transmisión, en el peor de los casos, se conoce, lo que permite cierto tipo de diseños (deterministas) que de otro modo podrían resultar ineficientes.

Características:

- Simplifica la administración de la red.
- Suelen emplear tecnología de difusión mediante un cable sencillo al que están conectadas todas las máquinas.
- Operan a velocidades entre 10 y 100 Mbps.
- Tienen bajo retardo y experimentan pocos errores. (Reina Toranzo & Ruiz Rivas, 2011)

2.1.2.2. Red de área amplia (WAN)

WAN (Wide Área Network) al igual que las redes LAN, estas redes permiten compartir dispositivos y tener un acceso rápido y eficaz, la que la diferencia de las demás es que proporciona un medio de transmisión a larga distancia de datos, voz, imágenes, videos,

sobre grandes áreas geográficas que pueden llegar a extenderse hacia un país, un continente o el mundo entero, es la unión de dos o más redes LAN.

Características:

- Operan dentro de un área geográfica extensa.
- Permite el acceso a través de interfaces seriales que operan a velocidades más bajas.
- Suministra velocidad parcial y continua.
- Conecta dispositivos separados por grandes distancias, incluso a nivel mundial. (Anónimo, Redes de Área Amplia (WAN), 2009)

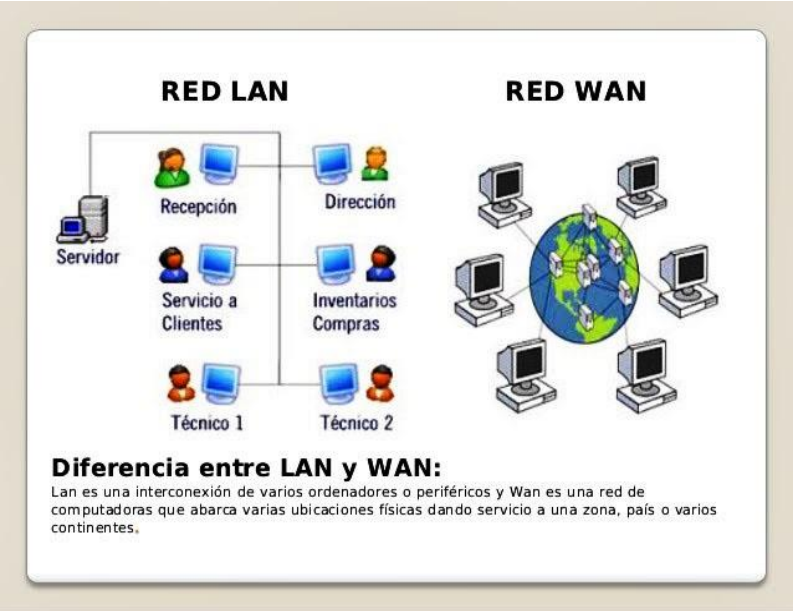


Figura 1: Diferencia entre LAN y WAN

Fuente: WIKI REDES FIMAZ12 (2012), Diferencia entre LAN y WAN (Ilustración), recuperado de https://sites.google.com/site/wikiredesfimaz12/tipo-de-redes-1 (FIMAZ12, 2012)

2.1.3. Concepto de VPN

Una VPN es una red privada que crea un túnel a través de una red pública, generalmente Internet. En lugar de usar una conexión física dedicada, una VPN utiliza conexiones

virtuales enrutadas a través de la Internet de la organización al local remoto. Las primeras VPN eran estrictamente túneles IP que no incluían autenticación o cifrado de datos. Por ejemplo, Generic Routing Encapsulation (GRE) es un protocolo de túnel desarrollado por Cisco que puede encapsular una amplia variedad de tipos de paquetes de protocolo de la capa de red dentro de los túneles IP. Esto crea una conexión virtual punto de a punto en los routers Cisco sobre los puntos remotos a través de una interconexión de redes IP. Otros ejemplos de redes VPN que no incluyen automáticamente medidas de seguridad son las redes Frame Relay, PVCs ATM, y Multiprotocol Label Switching (MPLS).

Una VPN es un entorno de comunicaciones en las que el acceso está estrictamente controlada para permitir conexiones de pares dentro de una comunidad de interés definida. La confidencialidad se logra mediante la encriptación del tráfico dentro de la VPN. Hoy en día, una implementación segura de VPN con cifrado es lo que generalmente se conoce con el concepto de red privada virtual. (Barker, Morris, Wallace, & Watkins, 2013)

Los métodos tradicionales de acceso remoto y creación de WAN privadas resultan ser bastante costosos y puesto que las redes públicas resultan ser mucho más económicas que las privadas, se buscaron maneras de poder establecer una red privada dentro de una red pública. El resultado fue el surgimiento de las Redes Privadas Virtuales (VPN) las cuales han ofrecido ventajas muy amplias a las corporaciones siendo la principal de ellas la reducción de costos de instalación y mantenimiento de forma muy significativa. Se puede definir a una VPN de la siguiente manera:

> *"Una Red Privada Virtual (VPN, Virtual Private Network) es una red privada que utiliza la infraestructura de una red pública para poder transmitir información."*

Una VPN combina dos conceptos: redes virtuales y redes privadas. En una red virtual, los enlaces de la red son lógicos y no físicos. La topología de esta red es independiente de la topología física de la infraestructura utilizada para soportarla. (Gonzales Morales, 2006)

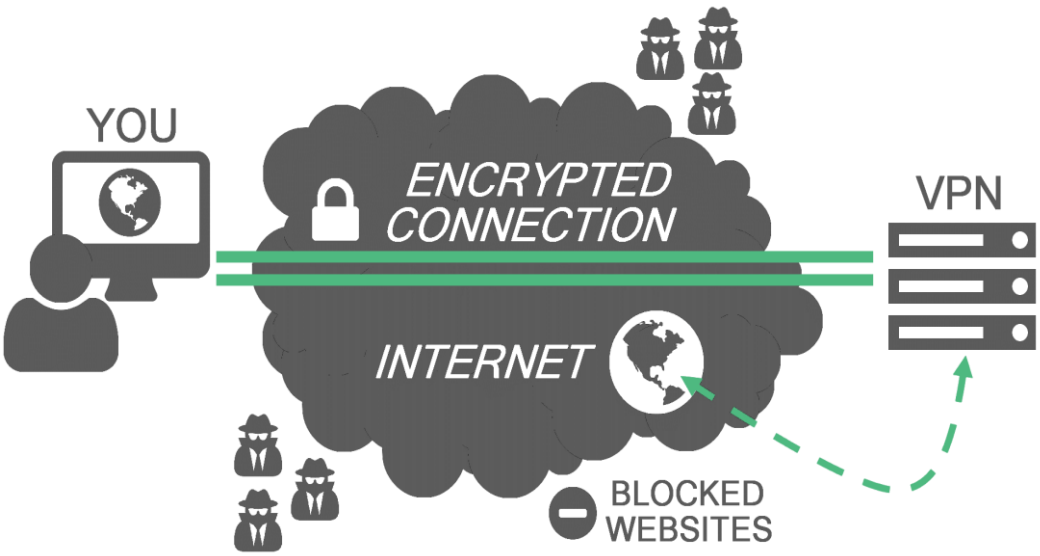


Figura 2: Red Privada Virtual

Fuente: Desconocido (2016), What is VPN (Figura), recuperado de http://www.mywebmymail.com/?q=content/what-vpn (Anónimo, What is VPN, 2016)

En un modo más simple, una VPN conecta dos puntos finales en una red pública para formar una conexión lógica. Las conexiones lógicas se pueden realizar sobre la Capa 2 o Capa 3 del modelo OSI. Las tecnologías de VPN pueden ser clasificados en general, sobre estos modelos de conexión lógica, como VPNs de Capa 2 o VPN de Capa 3. El establecimiento de la conexión entre los sitios ya sea usando VPN de capa 2 o VPN de Capa 3 es la misma. Un encabezado de envió se añade en la parte delantera de la carga útil para conseguir llegar al sitio de destino.

Los ejemplos más comunes de VPN de nivel 3 son GRE, MPLS e IPsec. VPNs de capa 3 puede ser conexiones punto a punto como GRE e IPsec, o se puede establecer

conexiones de cualquier-a-cualquier sitios conectándose a cualquier lugar utilizando MPLS.

2.1.4. Beneficios de las VPN

- Ahorro de costes.- Las VPNs permiten a las organizaciones el ahorro de costo de manera efectiva, la tercera parte de transporte de Internet para conectar oficinas remotas y los usuarios remotos a la Web corporativa principal. Las VPNs eliminan los costosos enlaces WAN dedicados. Además, con la llegada de tecnologías de banda ancha, como DSL, las organizaciones pueden utilizar VPN para reducir sus costes al mismo tiempo aumentar la conectividad de ancho de banda de conexión remota.
- Seguridad.- Las VPN proporcionar el más alto nivel de seguridad mediante el cifrado avanzado y protocolos de autenticación que protegen los datos contra accesos no autorizados.
- Escalabilidad.- Las VPNs permiten a las empresas utilizar la infraestructura de Internet que está dentro de los proveedores de servicios Internet (ISP) y los dispositivos. Esto hace que sea fácil de agregar nuevos usuarios, de modo que las empresas pueden añadir capacidad sin necesidad de añadir infraestructuras importantes.
- Compatibilidad con la tecnología de banda ancha.- Las VPN permite a los trabajadores móviles, tele trabajadores y las personas que quieran ampliar su jornada de trabajo para aprovechar la alta velocidad y la conectividad de banda ancha para tener acceso a sus redes corporativas, proporcionando a los trabajadores una significativa flexibilidad y eficiencia. Las Conexiones de alta

velocidad de banda ancha proporcionan una solución rentable para la conexión de oficinas remotas. (Barker, Morris, Wallace, & Watkins, 2013)

2.1.5. Ventajas y desventajas de una VPN

2.1.5.1. Ventajas

Como tecnología de acceso avanzada ofrece múltiples posibilidades. Las opciones para la conectividad se adaptan a los requisitos de cada empresa. Los beneficios de las VPN son conocidos y además útiles para pequeñas y grandes empresas.

Las VPN tradicionales son fáciles de implementar tanto del lado del ISP como por el del cliente. El proveedor no participa en los procesos de enrutamiento.

Las VPN peer to peer proporcionan una solución óptima en los procesos de enrutamiento empleando topologías de malla completa proporcionando redundancias entre todos los sitios, sin necesidad de implementar cambios desde el punto de vista del cliente.

Agregar sitios nuevos es tan simple como el agregado de nuevos routers e interconectarlos a un nuevo bucle local. La configuración no requiere múltiples circuitos para proporcionar capacidades de malla completa.

2.1.5.2. Desventajas

El coste y las tareas administrativas asociadas en grandes empresas con las topologías de malla completa pueden ser enormes. Para reducir el número de circuitos virtuales requeridos se deben sacrificar posibles rutas redundantes.

Las VPN tradicionales también tienen problemas de sobrecarga cuando se utiliza IPsec o GRE. Los principales beneficios de las VPN peer to peer pueden ser también su principal desventaja, como por ejemplo en la participación del enrutamiento del cliente.

La información de enrutamiento de las distintas redes es redistribuida entre el CE y el PE. Deben aplicarse filtros de enrutamiento en las interfaces de los routers para proteger ambas partes de flujos de rutas no deseadas. El cliente debe confiar en la capacidad del ISP para configurar y mantener la infraestructura de enrutamiento. (Ariganello & Barrientos Sevilla, 2010)

2.1.6. Componentes de una VPN

Los componentes básicos de una VPN aparecen en la figura y son:

- Servidor VPN
- Túnel
- Conexión VPN
- Red pública de tránsito
- Cliente VPN

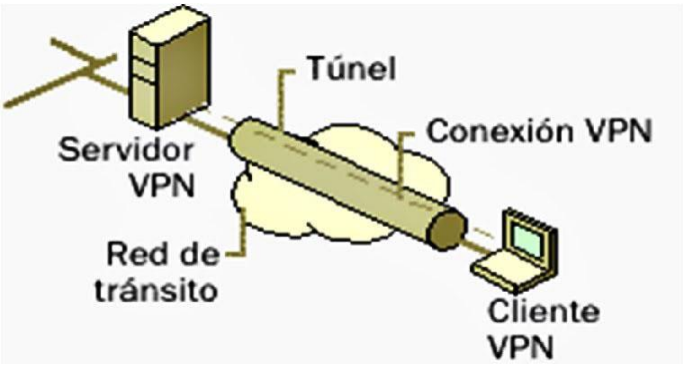


Figura 3: Componentes de una VPN

Fuente: Sambero Brayner (2010), Componentes de una conexión VPN (Figura), recuperado de http://braynerlinares.blogspot.pe/2010/09/redes-vpn.html (Sambero, 2010)

2.1.7. Topologías VPNs

Hay dos tipos básicos de redes VPN:

2.1.7.1. De sitio a sitio

Una VPN sitio a sitio se crea cuando los dispositivos de conexión en ambos lados de la conexión VPN son conscientes de la configuración de la VPN. La "VPN permanece estática, y los Host internos no tienen conocimiento de que existe una VPN. Frame Relay, ATM, GRE y VPN MPLS son ejemplos de VPNs sitio a sitio.

En una VPN sitio a sitio, los Host envían y reciben tráfico TCP/IP normal a través de un Gateway VPN, lo que puede ser un router, firewall, Concentrador VPN de Cisco, o Cisco ASA 5500 Series Adaptive Security Appliance. El Gateway VPN se encarga de encapsular y encriptar el tráfico de salida de un sitio específico y enviarlo a través de un túnel VPN sobre Internet a otro Gateway VPN en el lugar de destino. Tras la recepción, el Gateway VPN destino retira las cabeceras, descifra el contenido, y reenvía el paquete hacia el host de destino dentro de su red privada.

En base a los problemas comerciales que resuelven, las VPN de sitio a sitio pueden subdividirse a su vez en VPN intranet y VPN extranet.

VPN intranet. Las VPN intranet se utilizan para la comunicación interna de una compañía, como aparece en la figura 4. Enlazan una oficina central con todas sus sucursales. Se disfrutan de las mismas normas que en cualquier red privada. Un enrutador realiza una conexión VPN de sitio a sitio que conecta dos partes de una red privada. El servidor VPN proporciona una conexión enrutada a la red a la que está conectado el servidor VPN.

VPN extranet. Estas VPN enlazan clientes, proveedores, socios o comunidades de interés con una intranet corporativa, como se muestra en la figura 4. Se puede implementar una VPN extranet mediante acuerdo entre miembros de distintas organizaciones. Las empresas disfrutan de las mismas normas que las de una red privada. Sin embargo, las amenazas a la seguridad en una extranet son mayores que en una intranet, por lo que una VPN extranet debe ser cuidadosamente diseñada con muchas pólizas de control de acceso y acuerdos de seguridad entre los miembros de la extranet.

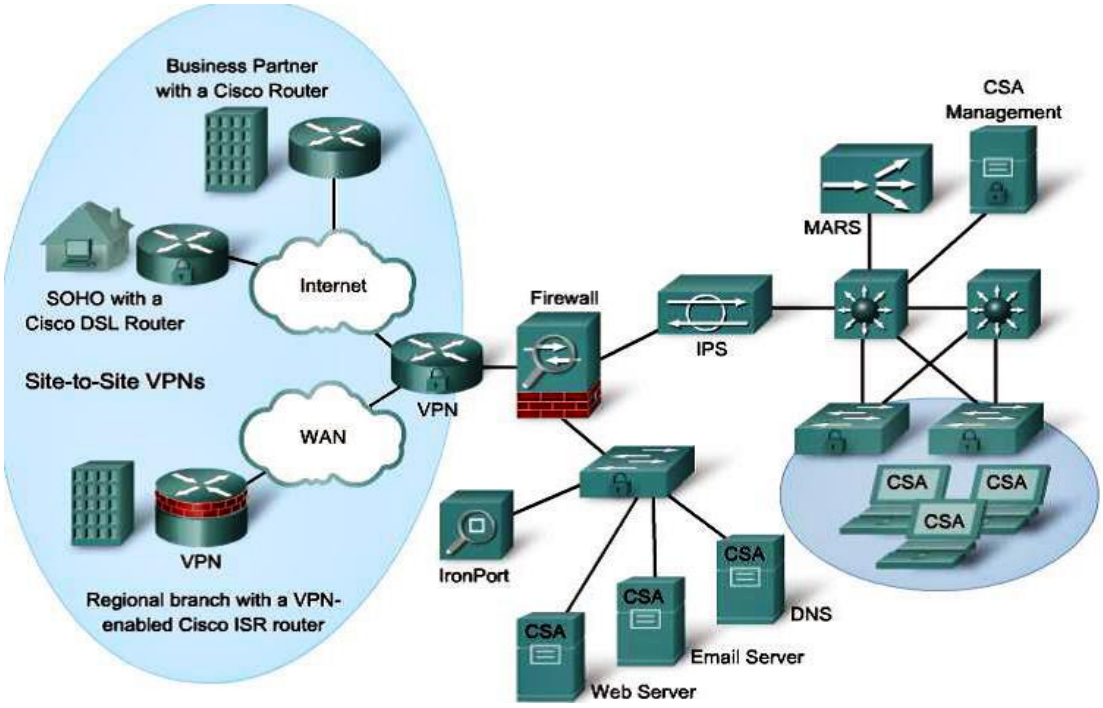


Figura 4: VPN Sitio a Sitio (Site-to-Site)

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), VPN Site-To-Site (Ilustración), recuperado de CCNA Security 640 – 554 Official Cert Guide (Barker, Morris, Wallace, & Watkins, 2013)

2.1.7.2. De acceso remoto

Una VPN de acceso remoto se crea cuando la información no es creada estáticamente, sino que permite cambiar dinámicamente la información y puede ser activado y desactivado. Considere la posibilidad de un teletrabajador que necesita VPN de acceso a

los datos corporativos a través de la Internet. El teletrabajador no tiene necesariamente que configurar la conexión VPN a cada momento. La PC del teletrabajador es responsable de establecer la conexión VPN. La información necesaria para establecer la conexión VPN, tales como la dirección IP de los teletrabajadores y los cambios de forma dinámica dependiendo de la ubicación de cada teletrabajador.

VPN de acceso remoto son una evolución de las redes de conmutación de circuitos, como lo era el servicio telefónico antiguo (POTS) o RDSI. Las VPN de acceso remoto puede apoyar las necesidades de los teletrabajadores, los usuarios móviles, y de los consumidores de extranet para el tráfico de negocios. Las VPN de acceso remoto tienen una arquitectura cliente / servidor en el que un cliente VPN (Host remoto) requiere un acceso seguro a la red de la empresa a través de un dispositivo de servidor de VPN en el borde de la red.

De acuerdo a la tecnología utilizada para establecer la conexión, las VPN de acceso remoto se puede dividir en VPN dial-up y VPN directas:

- VPN dial-up. En esta VPN, el usuario realiza una llamada local al ISP utilizando un módem. Aunque se trata de una conexión lenta es todavía muy común. El uso de este tipo de VPN se da más entre los usuarios móviles, ya que no en todos los lugares a donde se viaja se pueden tener disponibles conexiones de alta velocidad.
- VPN directa. En esta VPN, se utilizan las tecnologías de conexión a Internet de alta velocidad, tales como DSL y módem de cable las cuales ya ofrecen muchos ISP. Este tipo de VPN se puede encontrar principalmente entre los teletrabajadores. Actualmente se pueden obtener conexiones a Internet desde el hogar utilizando estas tecnologías.

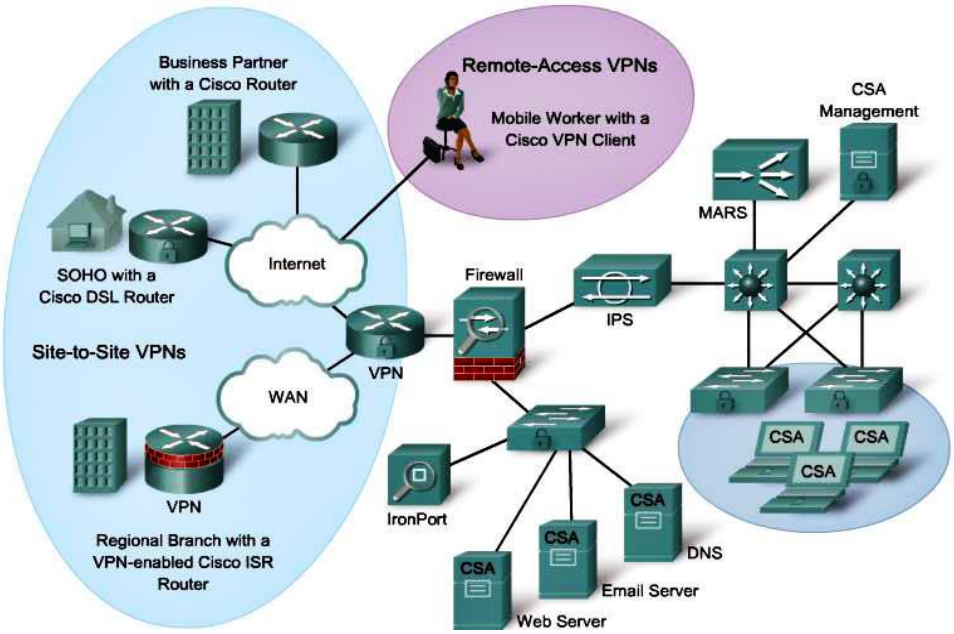


Figura 5: VPN de acceso remoto.

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), VPN remote access (Ilustración), recuperado de CCNA Security 640 – 554 Official Cert Guide (Barker, Morris, Wallace, & Watkins, 2013)

En un acceso remoto VPN, cada Host tiene típicamente un software de cliente VPN de Cisco. Cada vez que el Host intenta enviar tráfico destinado a la VPN, el software Cisco VPN Client encapsula y cifra el tráfico antes de enviarlo por Internet a la puerta de enlace VPN en el borde de la red de destino. Tras la recepción, la puerta de enlace VPN se comporta como lo hace para de una VPN sitio a sitio. (Gonzales Morales, 2006)

Figura 6: Ventana de software VPN Client

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), VPN client window (Imagen), recuperado de CCNA Security 640 – 554 Official Cert Guide (Barker, Morris, Wallace, & Watkins, 2013)

2.1.8. Requerimientos de una VPN

Una VPN debe de contar con ciertos requerimientos que permitan que valga la pena el uso de esta tecnología. Sin estos requerimientos, las VPN no podrán ofrecer la calidad necesaria que requieren las organizaciones para un desempeño óptimo. Una solución VPN debe ofrecer los siguientes requerimientos:

I. Autenticación de usuarios

II. Control de acceso

III. Administración de direcciones

IV. Cifrado de datos

V. Administración de claves

VI. Soporte a protocolos múltiples

VII. Ancho de banda

I. Autenticación de usuarios

La autenticación es uno de los requerimientos más importantes en una VPN. Cada entidad participante en una VPN debe de identificarse a sí misma ante otros y viceversa. La autenticación es el proceso que permite a los diversos integrantes de la VPN verificar las identidades de todos.

Existen muchos mecanismos de autenticación pero el más popular de todos ellos es la Infraestructura de Claves Públicas (PKI, Public Key Infraestructure), el cual es un sistema basado en la autenticación por medio de certificados. Cada integrante de una VPN se

autentica intercambiando los certificados de cada uno, los cuales están garantizados por una autoridad de certificación (CA, Certification Authority) en la que todos confían.

II. Control de acceso

El control de acceso en una red está definido como el conjunto de pólizas y técnicas que rigen el acceso a los recursos privados de una red por parte de usuarios autorizados. Una vez que un usuario ha sido autenticado, se debe definir a qué recursos de la red puede tener acceso dicho usuario. Los diferentes tipos de VPN, ya sea de firewalls, sistemas operativos, etc; son responsables de gestionar el estado de la conexión del usuario.

La VPN debe administrar el inicio de una sesión, permitir el acceso a ciertos recursos, continuar una sesión, impedir el acceso de recursos y terminar una sesión.

III. Administración de direcciones

Un servidor VPN debe de asignar una dirección IP al cliente VPN y asegurarse de que dicha dirección permanezca privada. Está claro que IP no es un protocolo seguro y se puede ver esto en la inseguridad de Internet. Las direcciones deben ser protegidas con fuertes mecanismos de seguridad, esto es, deben usarse técnicas que permitan la ocultación de la dirección privada dentro de una red pública.

La tecnología más utilizada para ocultar la información es el tunneling. El tunneling es una técnica que encapsula los datos (incluyendo la dirección destino privada) dentro de otro conjunto de datos. Así, el contenido de los paquetes encapsulados se vuelve invisible para una red pública insegura como Internet.

IV. Cifrado de datos

Cifrar o encriptar los datos es una tarea esencial de una VPN. Aunque se puedan encapsular los datos dentro de un túnel, estos todavía pueden ser leídos si no se implementan fuertes mecanismos de cifrado de la información. El cifrado es un conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas. El texto sin cifrar se le denomina texto nativo, mientras que el texto cifrado se le denomina texto cifrado. Antes de enviar la información, el servidor VPN cifra la información convirtiéndolo en texto cifrado. El receptor de la información descifra la información y la convierte en texto nativo.

V. Administración de claves

En una VPN, es importante la administración de claves. Para asegurar la integridad de una clave pública, ésta es publicada junto con un certificado. Un certificado es una estructura de datos firmada digitalmente por una organización conocida como autoridad de certificación (CA) en la cual todos confían. Una CA firma su certificado con su clave privada. Un usuario que utiliza la clave pública de la CA podrá comprobar que el certificado le pertenece a dicha CA y por lo tanto, la clave pública es válida y confiable.

VI. Soporte a protocolos múltiples

Para que una solución VPN sea viable, es necesario también que ésta pueda ofrecer soporte a múltiples protocolos. Esto incluye el soporte a protocolos de red que no sean IP como pueden ser AppleTalk, IPX y NetBEUI. PPTP soporta varios protocolos de red. IPsec sólo puede ser utilizado en redes basadas en IP, pero siempre es posible encapsular los protocolos no compatibles dentro de un paquete IP, de modo que puedan ser transportados.

VII. Ancho de banda

El ancho de banda es también un requerimiento importante en una VPN. En el mundo de las redes existe un concepto que define la forma de administrar el ancho de banda con el fin de que el tráfico de una red fluya de forma eficiente. Dicho concepto es la Calidad de Servicio (QoS, Quality of Service). La QoS es una característica muy importante de una VPN. Una solución VPN no estará completa si no proporciona formas para el control y administración del ancho de banda. (Gonzales Morales, 2006)

2.1.9. Tunneling

El tunneling es un método utilizado para encapsular paquetes (conocidos como datos de usuario) dentro de otros paquetes los cuales son enviados utilizando la tecnología de la red por la que viaja. Esto ofrece grandes ventajas, ya que permite el transporte de protocolos con diferente esquema de direccionamiento y que por lo tanto no son compatibles con una red que utiliza otros protocolos de direccionamiento dentro de paquetes que sí reconoce la red. En resumen, el tunneling es un proceso que consta de los siguientes pasos:

- Encapsulación
- Transmisión
- Desencapsulación

2.1.9.1. Tunneling y VPN

Cuando el uso de túneles se combina con el cifrado de los datos, puede utilizarse para proporcionar servicios de VPN. Las VPN utilizan el tunneling para poder ofrecer mecanismos seguros de transporte de datos. Dentro del contexto de las VPN, el tunneling involucra tres tareas principales:

- Encapsulación
- Protección de direcciones privadas
- Integridad de los datos y confidencialidad de éstos

Para que el proceso del tunneling pueda ser llevado a cabo, existen diversos protocolos llamados protocolos de túnel los cuales se encargan de encapsular y desencapsular los datos que viajan dentro de una red privada virtual.

Tres protocolos de túnel son los más usados para la creación de una VPN:

- Protocolo de Túnel punto a punto (PPTP)
- Protocolo de Túnel de Capa 2 (L2TP)
- Protocolo de Seguridad IP

Los protocolos PPTP y L2TP se enfocan principalmente a las VPN de acceso remoto, mientras que IPsec se enfoca mayormente en las soluciones VPN de sitio a sitio. (Gonzales Morales, 2006)

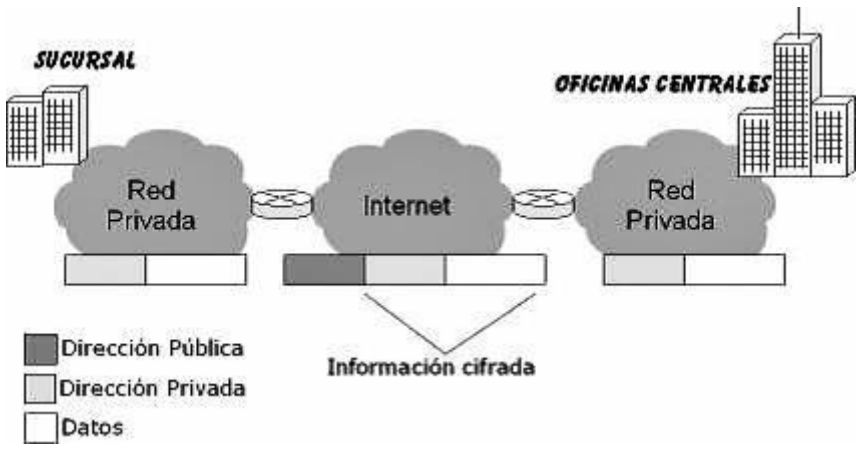


Figura 7: Tunneling de una VPN

Fuente: Gonzales Alexandro (2006), Tunneling en una VPN (Figura), recuperado de Redes Privadas Virtuales (Monografía) (Gonzales Morales, 2006)

2.1.10. Seguridad de los datos

Todas las tecnologías de seguridad en las redes se basan en técnicas criptográficas. Para dar seguridad a los datos, tres aspectos deben de proporcionar estas técnicas.

- Confidencialidad
- Integridad
- Autenticación.

Por confidencialidad se entiende como el hecho de ocultar los datos de usuarios no autorizados. Por integridad se refiere al hecho de asegurar que los datos no sean modificados mientras son transmitidos y la autenticación se refiere al hecho de poder comprobar que los datos provienen del lugar del que se supone deben venir. (Gonzales Morales, 2006)

2.1.10.1. Funciones de dispersión (hash) unidireccionales

Las funciones de dispersión unidireccionales (one-way hash function) son muy utilizadas para la autenticación de datos, para la creación de firmas digitales y también son muy utilizadas por las tecnologías de autenticación de usuarios.

Existen tres formas para autenticar un mensaje. La primera es utilizando cifrado simétrico. Si se supone que sólo el emisor y el receptor comparten la clave, se asegura la autenticación. El resumen del mensaje se puede cifrar usando cifrado de clave pública. Esto proporciona una firma digital, así como la autenticación de los mensajes y no requiere distribuir las claves a las partes que se comuniquen. La tercer forma es utilizando una función de dispersión. Las funciones de dispersión operan sobre un mensaje de longitud variable y produce un resumen del mensaje de longitud fija (hash signature). Estas funciones crean una huella digital electrónica única para un mensaje dado.

Las funciones de dispersión más importantes son **MD5 y SHA-1.**

Resumen de Mensaje versión 5 (MD5, Message Digest version 5). Es un algoritmo de dispersión que autentica los datos de los paquetes. Tuvo versiones anteriores llamadas MD2 y MD4. Este algoritmo toma un mensaje de longitud variable y produce un resumen del mensaje (hash) de 128 bits. MD5 es muy utilizado por IPsec para la autenticación de datos.

2.1.10.2. Algoritmo de Dispersión Segura versión 1 (SHA-1, Security Hash Algorithm).

Es un algoritmo de dispersión el cual fue publicado como estándar en 1993. En 1995 se publicó una versión revisada conocida como SHA-1. Este algoritmo toma como entrada un mensaje con una longitud máxima de 264 bits y produce un resumen del mensaje (hash) de 160 bits. La entrada se procesa en bloques de 512 bits. IPsec y los certificados utilizan ampliamente SHA-1 para la autenticación y las firmas digitales. (Gonzales Morales, 2006)

El cifrado de clave pública puede operar en conjunción con las funciones de dispersión unidireccionales para poder crear una firma digital.

El proceso de creación de una firma digital y la verificación de su autenticidad usando estas técnicas criptográficas se muestra en la figura:

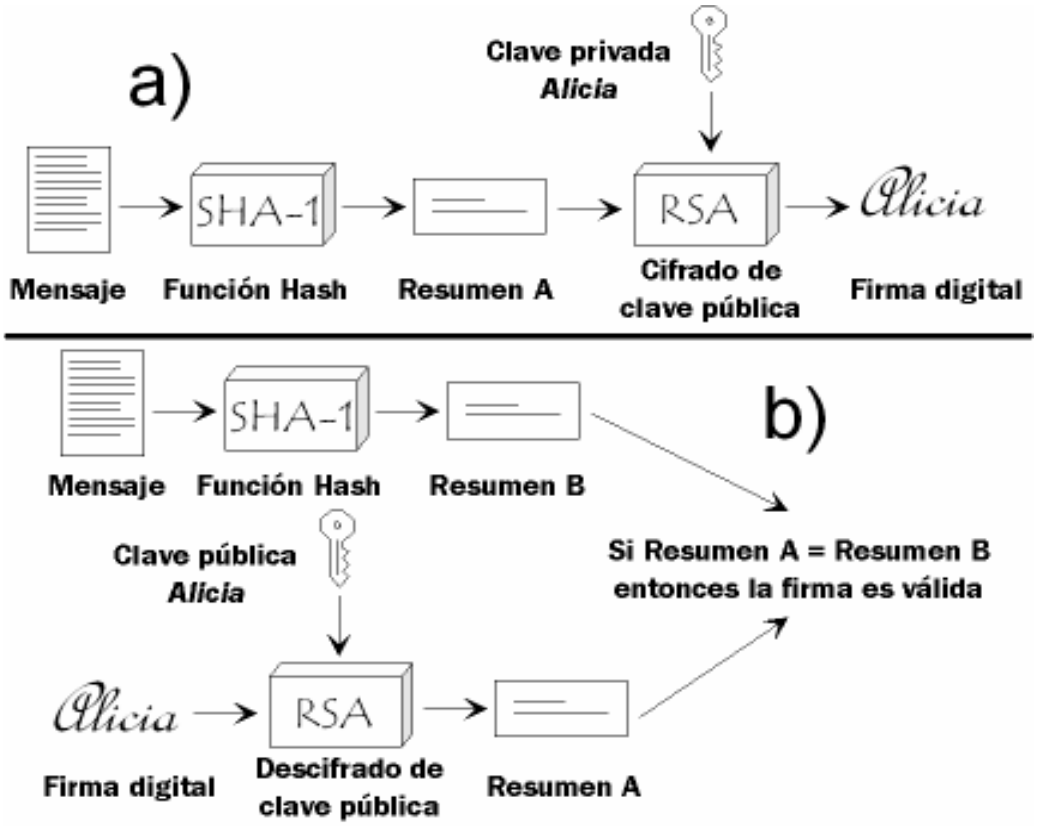


Figura 8: Proceso de creación de cifrado

Fuente: Gonzales Alexandro (2006), Modelo de cifrado de clave pública (Ilustración), recuperado de Redes Privadas Virtuales (Monografía) (Gonzales Morales, 2006)

2.1.11. Tecnologías de las VPN

2.1.11.1. Protocolo de Túnel Punto a Punto (PPTP)

El Protocolo de Túnel Punto a Punto (PPTP, Point-to-Point Tunneling Protocol) es un protocolo de red creado por Microsoft, Ascend Communications y US Robotics el cual permite la realización de transferencias seguras desde clientes remotos a servidores emplazados en redes privadas, empleando para ello tanto líneas telefónicas conmutadas como Internet.

En el escenario típico de PPTP, el cliente establecerá una conexión dial-up con el servidor de acceso a red (NAS) del proveedor del servicio, empleando para ello el protocolo PPP.

Una vez conectado, el cliente establecerá una segunda conexión con el servidor PPTP el cual estará situado en la red privada. Dicho servidor será utilizado como intermediario de la conexión, recibiendo los datos del cliente externo y transmitiéndolos al correspondiente destino en la red privada.

Una desventaja que tiene PPTP es que no posee un único estándar para la encriptación y la autenticación, ya que PPTP se ocupa únicamente de crear un túnel. Además, PPTP es el protocolo VPN menos seguro. L2TP e IPsec ofrecen mejores alternativas para garantizar la seguridad en una VPN. (Gonzales Morales, 2006)

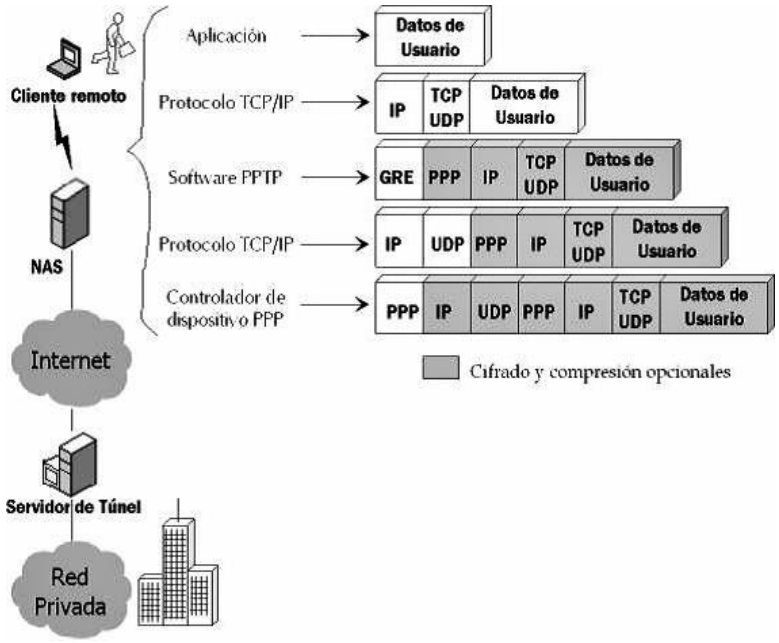


Figura 9: Protocolos de túnel Punto a Punto

Fuente: Gonzales Alexandro (2006), Construcción de un paquete PPTP (Ilustración), recuperado de Redes Privadas Virtuales (Monografía) (Gonzales Morales, 2006)

2.1.11.2. Protocolo de Túnel de Capa 2 (L2TP)

El Protocolo de Túnel de Capa 2 (L2TP, Layer 2 Tunneling Protocol) es un protocolo estándar diseñado para transmitir datos y conectar de forma segura redes a través de Internet.

L2TP es un protocolo estándar aprobado por el IETF (Internet Engineering Task Force), en oposición al protocolo propietario de Microsoft PPTP. Es soportado prácticamente por la totalidad de firmas del mercado de la comunicación de datos, incluyendo Microsoft y Cisco.

L2TP se diseñó específicamente para conexiones de acceso remoto, así como para conexiones sitio a sitio. Mediante la utilización del protocolo PPP, L2TP gana compatibilidad multiprotocolo para protocolos como IPX y AppleTalk. (Gonzales Morales, 2006)

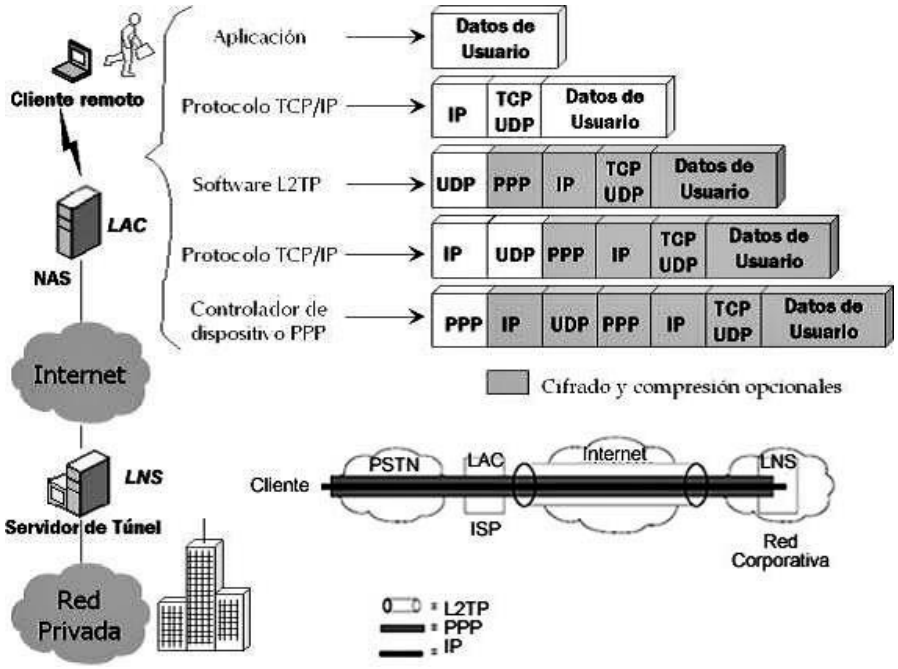


Figura 10: Protocolos de Túnel en capa 2

Fuente: Gonzales Alexandro (2006), Construcción de un paquete L2PT (Ilustración), recuperado de Redes Privadas Virtuales (Monografía) (Gonzales Morales, 2006)

2.1.12. Seguridad IP (IPsec)

IPsec es un estándar IETF (RFC 2401-2412) que define como una VPN se puede configurar utilizando el protocolo de direccionamiento IP. IPsec no está obligado a

ningún tipo de: cifrado específico, autenticación, algoritmos de seguridad, o tecnología Clave. IPsec es un marco de estándares abiertos que especifica normas para las comunicaciones seguras. IPsec se basa en algoritmos existentes para implementar la encriptación, autenticación e intercambio de claves.

IPsec funciona en la capa de red, protegiendo y autenticando los paquetes IP entre los dispositivos IPsec que participan (compañeros).

La Estructura IPsec consta de cinco bloques:

- El primero representa el protocolo IPsec. Las opciones incluyen ESP o AH.
- La segunda representa el tipo de confidencialidad a cabo utilizando un algoritmo de cifrado como DES, 3DES, AES, o SEAL. La elección depende del nivel de seguridad requerido.
- El tercero representa la integridad que puede ser implementada utilizando MD5 o SHA.
- La cuarta representa cómo se establece la clave secreta compartida. Los dos métodos son precompartida o firma digital utilizando RSA.
- El último grupo representa el algoritmo de DH. Hay cuatro distintos algoritmos de intercambio de clave DH para poder elegir entre ellos estan DH Grupo 1 (DH1), DH Grupo 2 (DH2), DH Grupo 5 (DH5), y DH Grupo 7 (DH7). El tipo de grupo seleccionado depende de las necesidades específicas. (Barker, Morris, Wallace, & Watkins, 2013)

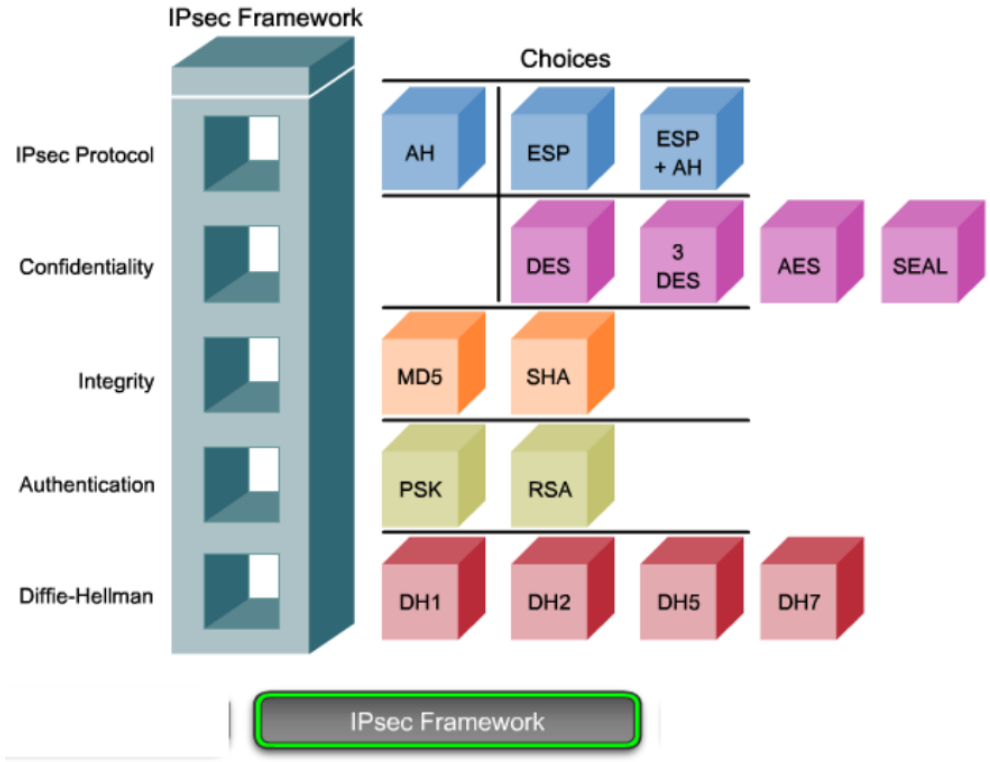


Figura 11: Protocolos de IPsec

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), IPsec protocols (Ilustración), recuperado de CCNA Security 640 – 554 Official Cert Guide (Barker, Morris, Wallace, & Watkins, 2013)

IPsec se basa en protocolos primarios que ayudan a implementar su arquitectura global, como IKE, ESP y AH, es importante comprender que estos protocolos están basados en estándares abiertos, IPsec los utiliza para autenticación, encriptación, generación de llaves y establecimiento de asociaciones de seguridad. IPsec es utilizado para proteger el flujo de los datos a través de una VPN, pero una VPN no necesariamente tiene que requerir que estos contenidos estén protegidos. Una VPN puede ser simplemente un túnel o un enlace entre dos puntos finales, por lo tanto la cabecera o etiqueta es identificada como tal pero el contenido interno está disponible para cualquiera que lo quiera inspeccionar entre dichos extremos finales. Entonces una VPN IPsec puede ser considerada segura y protegida mientras que otro tipo de VPN no comparte este tipo de características. (Ariganello & Barrientos Sevilla, 2010)

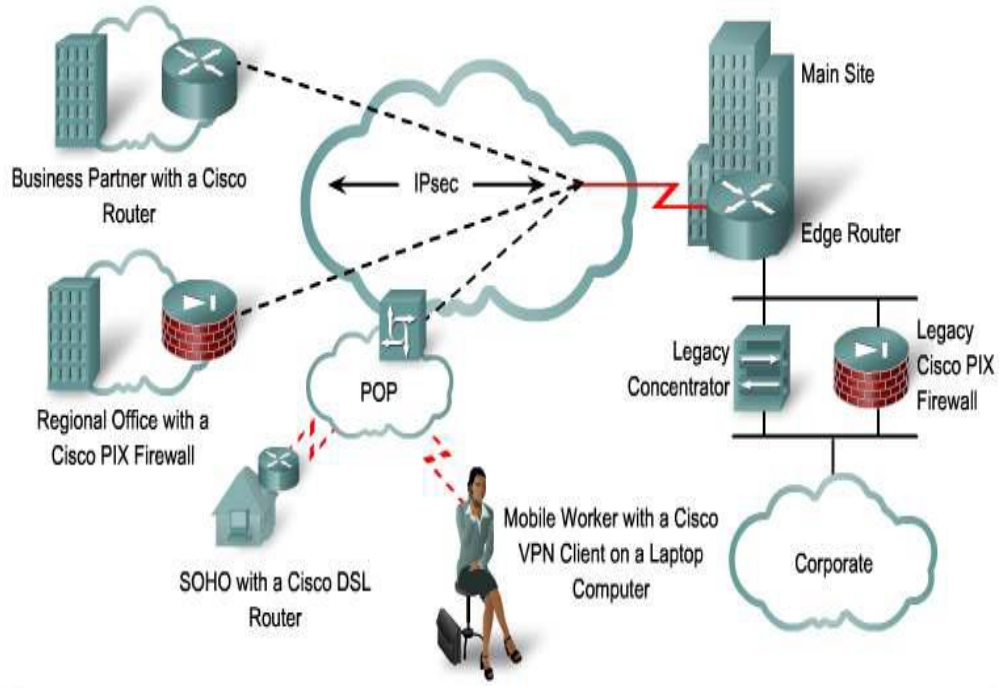


Figura 12: Forma de trabajo de IPsec

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), IPsec Work (Ilustración), recuperado de CCNA Security 640 – 554 Official Cert Guide (Barker, Morris, Wallace, & Watkins, 2013)

2.1.13. Características de IPsec

Las características de IPsec consisten en lo siguiente:

a) Confidencialidad.- IPsec garantiza la confidencialidad mediante el uso de cifrado.

b) Integridad.- IPsec garantiza que los datos llegan sin cambios en el destino utilizando un algoritmo de hash como MD5 o SHA.

c) Autenticación.- IPsec utiliza Internet Key Exchange (IKE) para autenticar de forma independiente usuarios y dispositivos que pueden llevar a cabo la comunicación. IKE utiliza varios tipos de autenticación, incluyendo nombre de usuario y contraseña, contraseña de un solo tiempo, biometría, claves precompartidas (PSKs), y certificados digitales.

d) Intercambio seguro de claves.- IPsec utiliza el algoritmo de DH para proporcionar un método de intercambio de claves públicas de dos compañeros para establecer una clave secreta compartida. (Ariganello & Barrientos Sevilla, 2010)

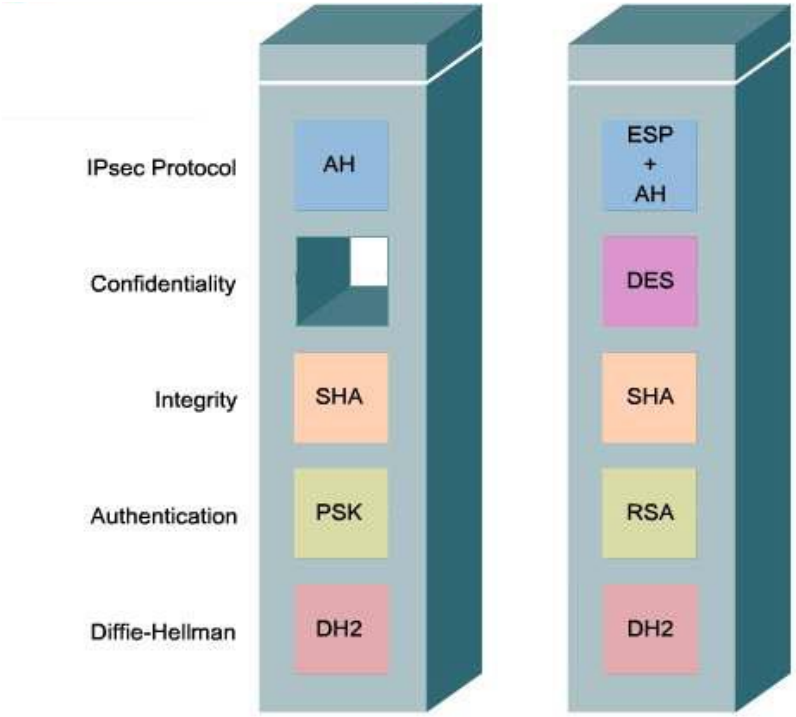


Figura 13: Implementación de IPsec

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), IPsec impleentation (Figura), recuperado de CCNA Security 640 – 554 Official Cert Guide (Barker, Morris, Wallace, & Watkins, 2013)

a) Confidencialidad

La confidencialidad se logra mediante la encriptación del tráfico mientras viaja a través de la VPN. El grado de seguridad depende de la longitud de la clave del algoritmo de cifrado. Si alguien intenta hackear la clave a través de un ataque de fuerza bruta, el número de posibilidades para intentar es una función que dependerá de longitud de la clave. El tiempo para procesar todas las posibilidades está en función de la potencia de los ordenadores del dispositivo de ataque. Cuanto más corta sea la clave, más fácil es romper. Una clave de 64 bits puede tomar aproximadamente un año para romper con un equipo

relativamente sofisticado. Una clave de 128 bits con la misma máquina puede tener más o menos 10^{19} años para descifrar.

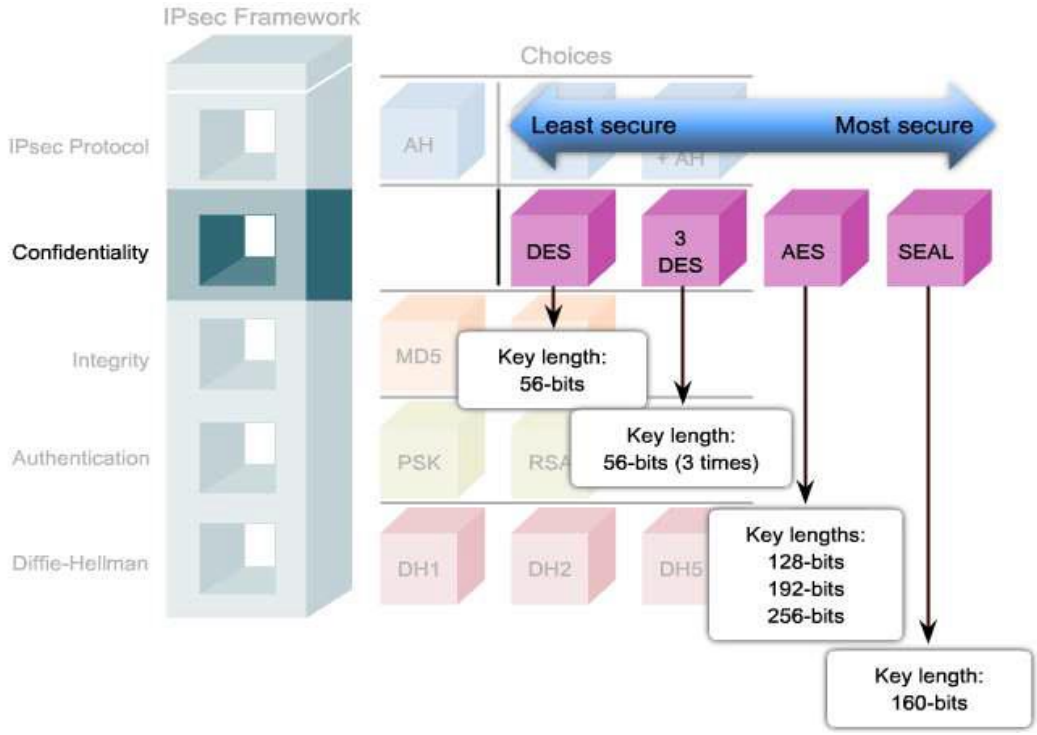


Figura 14: Protocolos de confidencialidad en IPsec

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), IPsec confidentiality (Ilustración), recuperado de CCNA Security 640 – 554 Official Cert Guide (Barker, Morris, Wallace, & Watkins, 2013)

b) Integridad

La próxima función fundamental de la VPN es la integridad de datos. Suponga que un cheque de $ 100 es escrito para Sonia de Jeremy. El cheque es luego enviado por correo a Sonia, pero es interceptado por un atacante. El atacante cambia el nombre y la cantidad en el cheque e intenta cobrarlo. Dependiendo de la calidad de la falsificación del cheque alterado, el atacante podría tener éxito.

Esta situación se aplica a las VPN porque los datos se transportan a través del Internet. Potencialmente, estos datos podrían ser interceptados y modificados. Un método para

proveer datos íntegros es necesario para garantizar que el contenido no haya sido alterado. Un algoritmo de integridad de datos puede ofrecer esta garantía.

Códigos de autenticación de mensajes hash (HMAC) es un algoritmo de integridad de datos que garantiza la integridad del mensaje mediante un valor hash. En el dispositivo local, el mensaje y una clave secreta compartida se procesan a través de un algoritmo de hash, lo que produce un valor hash. Este valor se añade al mensaje y el mensaje se envía a través de la red. En el dispositivo remoto, el valor de hash se vuelve a calcular y se compara con el valor hash enviado. Si el hash del transmisor coincide con el hash recibido, se verifica la integridad del mensaje. Pero, si no coinciden, el mensaje fue alterado y este se invalida.

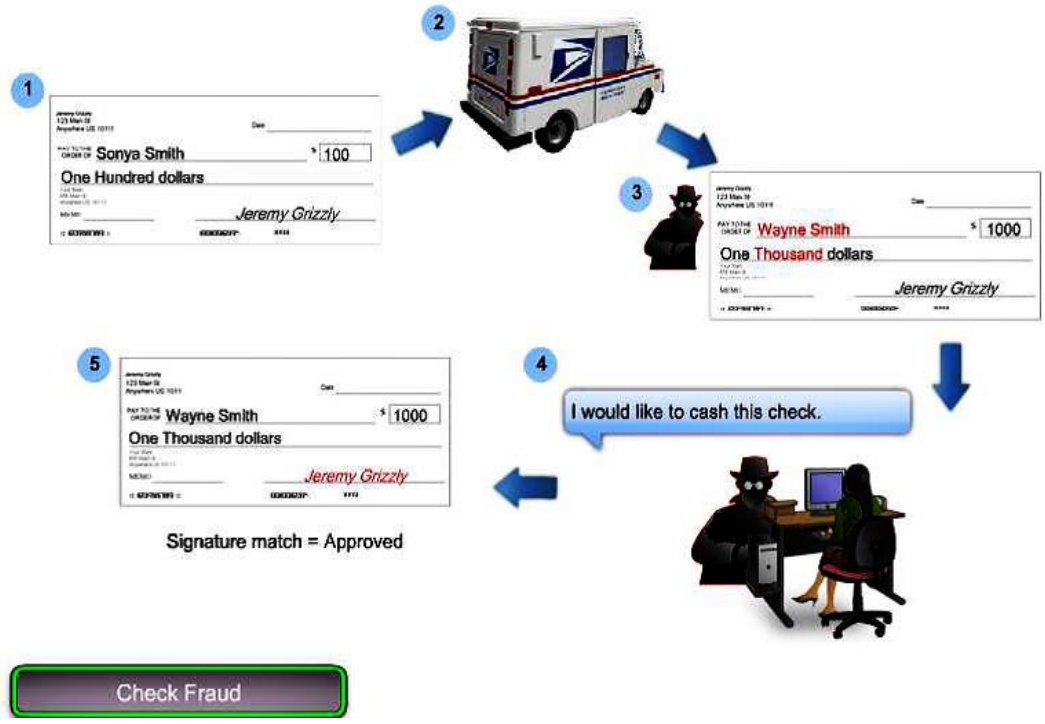


Figura 15: Comprobación de Fraude

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), Check Fraud (Ilustración), recuperado de CCNA Security 640 – 554 Official Cert Guide (Barker, Morris, Wallace, & Watkins, 2013)

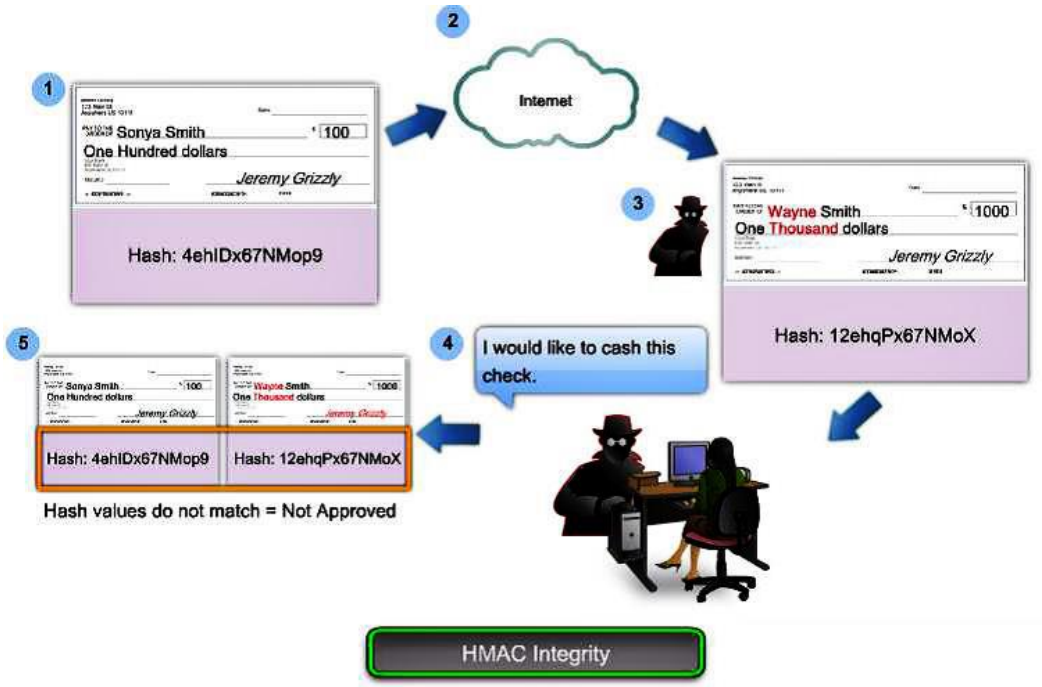


Figura 16: Integridad HMAC

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), HMAC Integrity (Ilustración), recuperado de CCNA Security 640 – 554 Official Cert Guide (Barker, Morris, Wallace, & Watkins, 2013)

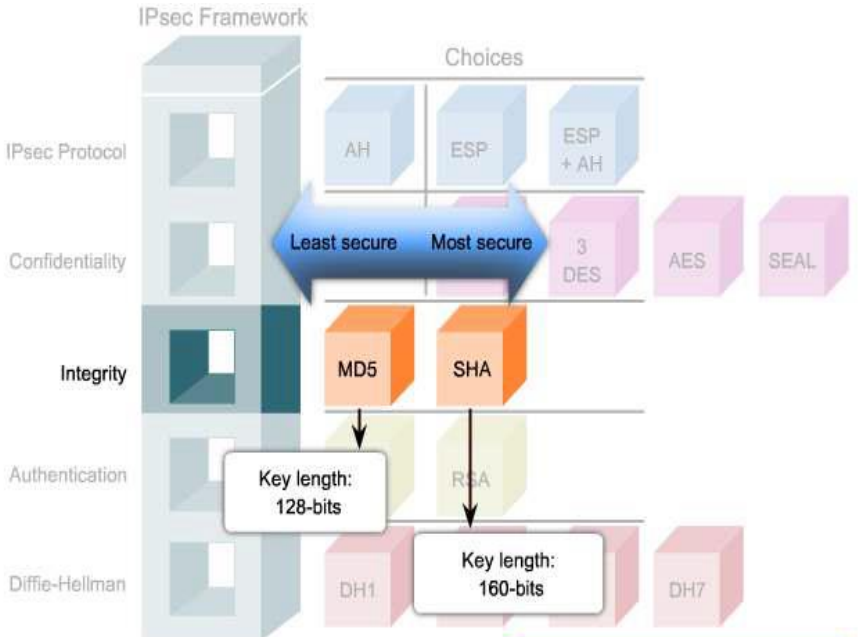


Figura 17: MD5 y SHA

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), MD5 and SHA (Ilustración), recuperado de CCNA Security 640 – 554 Official Cert Guide (Barker, Morris, Wallace, & Watkins, 2013)

c) Autenticación

Cuando se lleva a cabo negocios a larga distancia, es necesario conocer (autenticación) a la persona en el otro extremo del teléfono, correo electrónico o fax. Lo mismo es cierto de las redes VPN. El dispositivo en el otro extremo del túnel VPN debe ser autenticado antes para considerar la ruta de comunicación segura.

Hay dos métodos principales para la configuración de autenticación de los pares.

- Claves Precompartidas (PSKs) - Un valor de la clave secreta pre-compartida es ingresado en cada par de forma manual y se utiliza para autenticar a los pares. En cada extremo, la PSK se combina con otra información que forma la clave de autenticación. Cada par debe autenticar su par opuesto antes de que el túnel se considere seguro. Las Claves pre-compartidas son fáciles de configurar manualmente, pero no son muy escalables, porque cada IPsec debe estar previamente configurado con la clave compartida en cada otra pareja con el cual esta quiera comunicarse.
- Firmas RSA - El intercambio de certificados digitales autentica los pares. El dispositivo local deriva un hash y lo cifra con su clave privada. El hash cifrado se adjunta al mensaje y se envía al extremo remoto y actúa como una firma. En el extremo remoto, el hash cifrado se descifra utilizando la clave pública del local final. Si el hash descifrado encaja, la firma es auténtica. Cada par debe autenticar su par opuesto antes de que el túnel sea considera seguro.

Una tercera vía para llevar a cabo la autenticación es a través de cifrado RSA-nonces. Un nonce es un número aleatorio que se genera por los pares. RSA-nonces utilizar cifrado RSA para cifrar el valor nonce y otros valores. Este método requiere que la clave pública de los dos pares estén presente en otro par antes de que el tercero y cuarto mensajes de

un intercambio IKE se puede lograr. Por esta razón, las claves públicas se deben copiar manualmente a cada pareja, como parte del proceso de configuración. Este método es el menos utilizado de los métodos de autenticación.

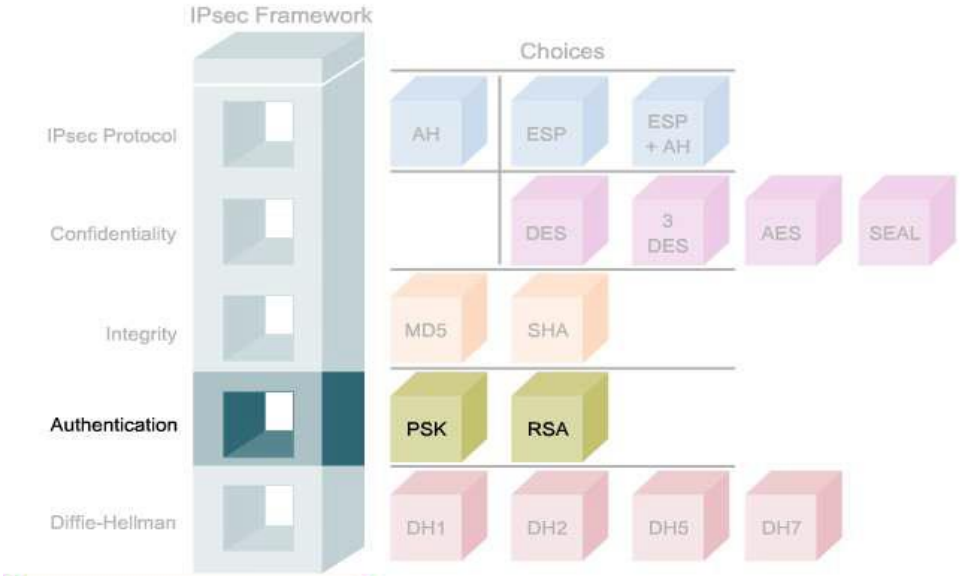


Figura 18: Autenticación en IPsec

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), Authentication (Ilustración), recuperado de CCNA Security 640 – 554 Official Cert Guide (Barker, Morris, Wallace, & Watkins, 2013)

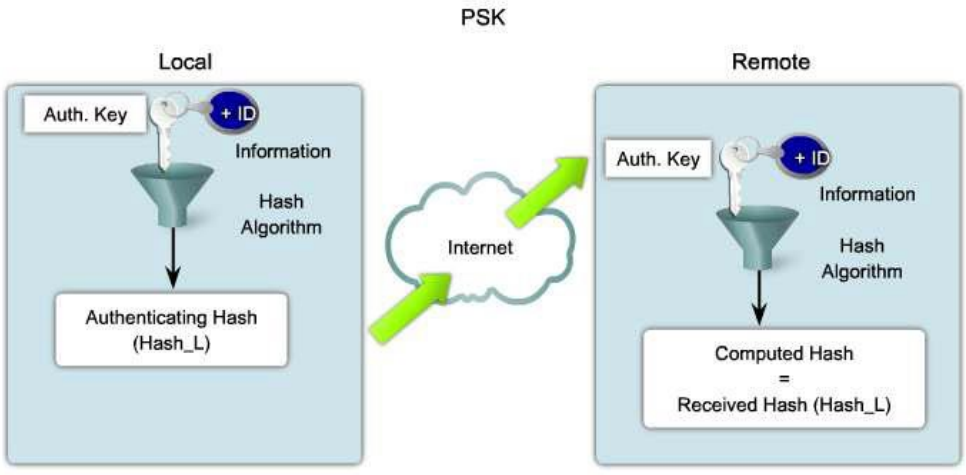


Figura 19: PSK

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), PSK (Ilustración), recuperado de CCNA Security 640 – 554 Official Cert Guide (Barker, Morris, Wallace, & Watkins, 2013)

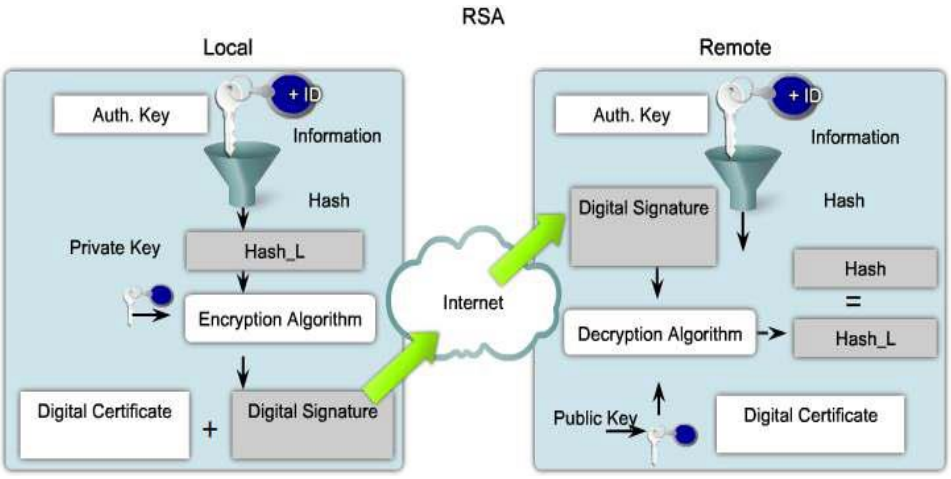


Figura 20: RSA

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), RSA (Ilustración), recuperado de CCNA Security 640 – 554 Official Cert Guide (Barker, Morris, Wallace, & Watkins, 2013)

d) Intercambio seguro de claves

Algoritmos de cifrado como DES, 3DES y AES, así como los algoritmos hash MD5 y SHA-1 exigen una clave compartida secreta simétrica, para realizar el cifrado y descifrado.

¿Cómo los dispositivos obtienen la clave secreta compartida para el cifrado y descifrado?

El Diffie-Hellman (DH) es un acuerdo de clave pública método de intercambio de claves que proporciona un camino para las dos parejas establezcan una clave secreta compartida que sólo ellos conocen, aunque estén comunicados por un canal inseguro.

Variaciones del algoritmo de intercambio de claves DH son conocidos como grupos de DH. Hay cuatro grupos DH: 1, 2, 5, y 7.

- Grupos DH 1, 2, y 5 soporta exponenciación en un primer módulo con un tamaño de clave de 768 bits, 1024 bits, y 1536 bits, respectivamente.

- Cisco clientes 3000 soporta DH grupos 1, 2, y 5.
- Encriptación DES y 3DES son soportados en los grupos DH 1 y 2.
- Encriptación AES es soportada en los grupos DH 2 y 5.

El cliente Certicom movianVPN es soportado en el grupo 7.

- El Grupo 7 es compatible con la criptografía de curva elíptica (ECC), que reduce el tiempo necesario para generar las claves.

Durante la configuración del túnel, los pares VPNs negocian con el grupo DH que usan. (Barker, Morris, Wallace, & Watkins, 2013)

2.1.14. Protocolos de IPsec

Los tres protocolos principales utilizados por IPsec son los siguientes:

a) IKE (Internet Key Exchange)
b) ESP (Encapsulating Security Payload)
c) AH (Authentication Header)

Juntos estos tres protocolos ayudan a implementar su arquitectura global y ofrecen las características mencionadas anteriormente. Cada VPN IPsec utiliza una combinación de estos protocolos para proporcionar las características requeridas por la VPN.

a) IKE

IKE (Internet Key Exchange) ofrece un marco para el intercambio de la negociación de seguridad y llaves de autenticación. Existe una variedad de opciones entre dos extremos IPsec. La negociación segura de estos parámetros utilizada para establecer la VPN IPsec se lleva a cabo por IKE.

IKE también intercambia llaves utilizadas para los algoritmos de encriptación simétrica dentro de VPN IPsec. Comparados con otros algoritmos de encriptación los algoritmos simétricos tienden a ser más eficientes y fáciles de implementar por hardware. La utilización de tales algoritmos requierén un material de llaves apropiados, IKE proporciona los mecanismos de intercambio de dichas llaves.

b) ESP

ESP (Encapsulating Security Payload) proporciona el marco para la confidencialidad de los datos, integridad de los datos autenticación del origen de los datos y opcionalmente características como Anti-replay.

ESP es el único protocolo de IPsec que proporciona encriptación de los datos pero también puede proporcionar todas las otras características de IPsec. Debido a esto último ESP es mayoritariamente utilizado en VPN IPsec hoy en día. Los siguientes procesos de encriptación están disponibles en ESP:

• DES (Data Encryption Standard) es un método de autenticación muy antiguo que está bastante extendido.

• 3DES (Triple Data Encryption Standard) es un bloque encriptado que utiliza tres veces DES.

• AES (Advanced Encryption Standard) es uno de los algoritmos de llaves simétricas más populares actualmente.

Anti-replay es típicamente usado en ESP, pero también es soportado en AH.

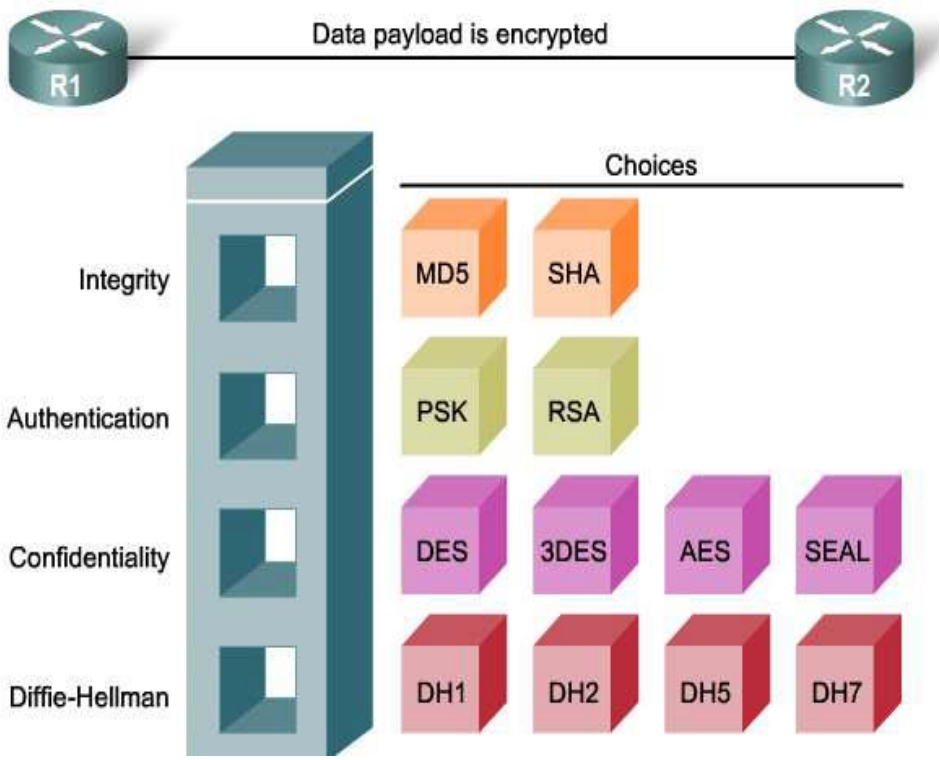


Figura 21: Opciones de Protocolos que trabajan con IKE

Fuente: Ariganello Ernesto y Barrientos Enrique (2010), Protocolos en IKE (Ilustración), recuperado de REDES CISCO CCNP a Fondo. Guía de Estudio para Profesionales. (Ariganello & Barrientos Sevilla, 2010)

c) AH

AH (Authentication Header) proporciona el marco para la integridad de los datos, autenticación del origen de los datos y características opcionales como antireplay. Confidencialidad de los datos no es proporcionada por AH.

AH se asegura que los datos no han sido modificados o interferidos pero no esconde estos datos cuando están transitando. La utilización de AH de manera solitaria ha caído en desuso en favor de ESP

Ambos, AH y ESP utilizan HMAC (Hash-based Message Authentication Code) como chequeo para la autenticación e integridad. (Ariganello & Barrientos Sevilla, 2010)

2.1.15. Modos de IPsec

ESP y AH pueden aplicarse a los paquetes IP en dos modos diferentes, modo de transporte y modo túnel.

2.1.15.1. Modo de transporte

En el modo de transporte, la seguridad se proporciona sólo para la capa de transporte del modelo OSI y superiores. El Modo de transporte protege la carga útil del paquete, pero deja la dirección IP original en texto plano.

La dirección IP original se utiliza para dirigir el paquete a través de Internet.

2.1.15.2. El modo de túnel

El modo de túnel proporciona seguridad para el paquete IP completo original. El paquete IP original es encriptada y luego es encapsulado en otro paquete IP. Esto se conoce Encriptación IP en IP.

La dirección IP en el paquete IP saliente se utiliza para enrutar el paquete a través de Internet.

El modo de túnel ESP se utiliza en IPsec de acceso remoto. Una oficina en casa que no tenga un router para realizar la encapsulación IPsec y el cifrado. En este caso, un cliente de IPsec es ejecutado en la PC y este realiza la encapsulacion y encriptación IPsec IP en IP. En la oficina corporativa, el router desencapsula y descifra el paquete. (Barker, Morris, Wallace, & Watkins, 2013)

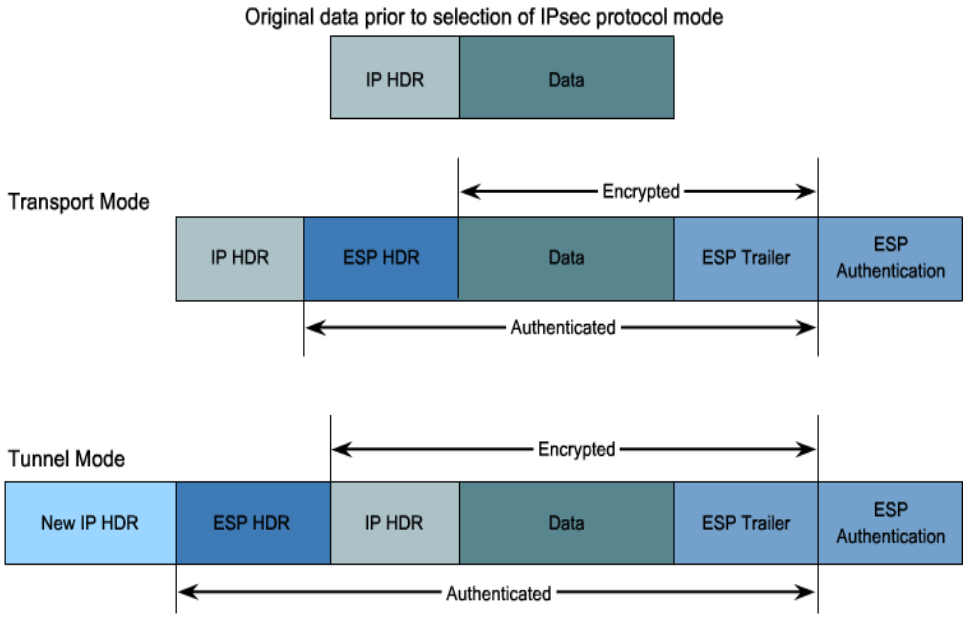


Figura 22: Modo Túnel vs. Modo de Transporte.

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), Transport vs. Tunnel Mode (Ilustración), recuperado de CCNA Security 640 – 554 Official Cert Guide (Barker, Morris, Wallace, & Watkins, 2013)

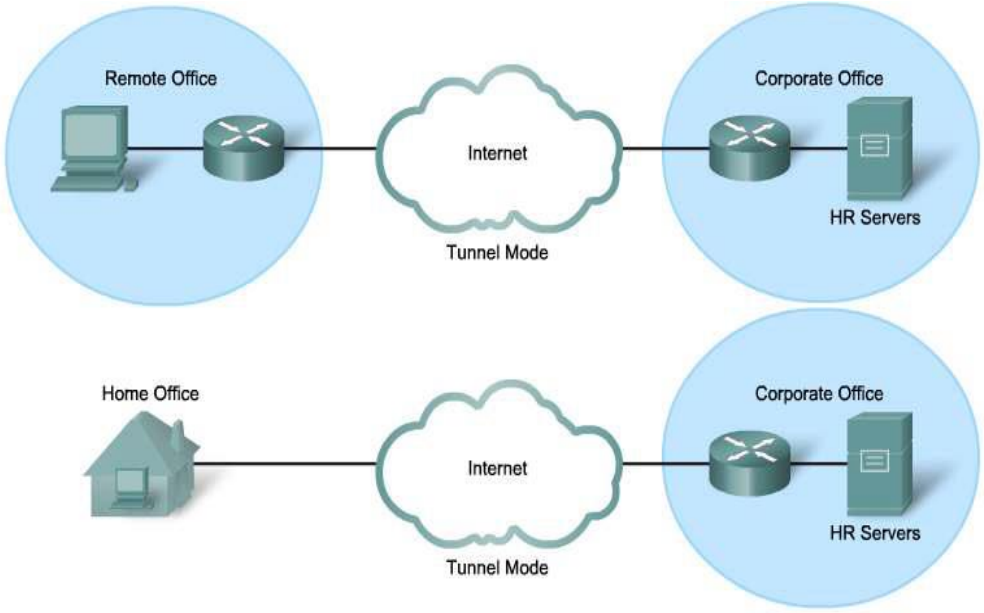


Figura 23: Modo Túnel ilustrado.

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), Tunnel Mode (Ilustración), recuperado de CCNA Security 640 – 554 Official Cert Guide (Barker, Morris, Wallace, & Watkins, 2013)

2.1.16. Intercambio de Claves en Internet

La solución VPN IPsec negocia los parámetros de intercambio de claves, se establece una clave compartida, autentica el par, y negocia los parámetros de codificación. Los parámetros de negociación entre dos dispositivos se conocen como una asociación de seguridad (SA).

2.1.16.1. Asociaciones de Seguridad

Un SA es un componente básico de IPsec. Las asociaciones de seguridad se mantienen dentro de una base de datos SA (SADB), que es establecido por cada dispositivo. Una VPN tiene entradas SA definiendo los parámetros de encriptación IPsec, así como entradas SA para definir los parámetros de intercambio de claves.

Todos los sistemas criptográficos, incluyendo el cifrado Caesar, cifrado Vigenere, Máquina Enigma, o los modernos algoritmos de cifrado, deben negociar cuestiones clave de gestión. Diffie-Hellman (DH) se utiliza para crear una clave secreta compartida. Sin embargo, IPsec utiliza el Internet Key Exchange (IKE) para establecer el proceso de intercambio de claves.

En lugar de transmitir las claves directamente a través de una red, calcula las claves IKE compartida basada en el intercambio de una serie de paquetes de datos. Esto inhabilita que un tercero pueda descifrar las claves, incluso si el tercero logra capturar todos los datos intercambiados que se utiliza para calcular las claves.

IKE es definido en el RFC 2409. Es un protocolo híbrido, que combina la Asociación de Seguridad de Internet y Key Management Protocol (ISAKMP) con los métodos de intercambio de claves Oakley y SKEME. ISAKMP define el formato del mensaje, la mecánica de un protocolo para el intercambio de claves, y el proceso de negociación para

crear una SA de IPsec. ISAKMP no define cómo se gestionan las claves o como se comparen entre los dos pares de IPsec. Oakley y SKEME tienen cinco grupos principales definidos. De estos grupos, los routers Cisco de soportan el Grupo 1 (768-bit), Grupo 2 (clave de 1024 bits), y (1536 Grupo 5-bit).

IKE combina estos protocolos para crear conexiones seguras entre dispositivos de IPsec. Establece SA que sean mutuamente aceptables para cada par. Cada par debe tener idéntico ISAKMP y los parámetros de IPsec para establecer una VPN operativa y segura. Tenga en cuenta que los términos de ISAKMP e IKE son comúnmente utilizados por la industria para referirse a IKE. (Barker, Morris, Wallace, & Watkins, 2013)

2.1.16.2. ¿Cómo funciona IKE?

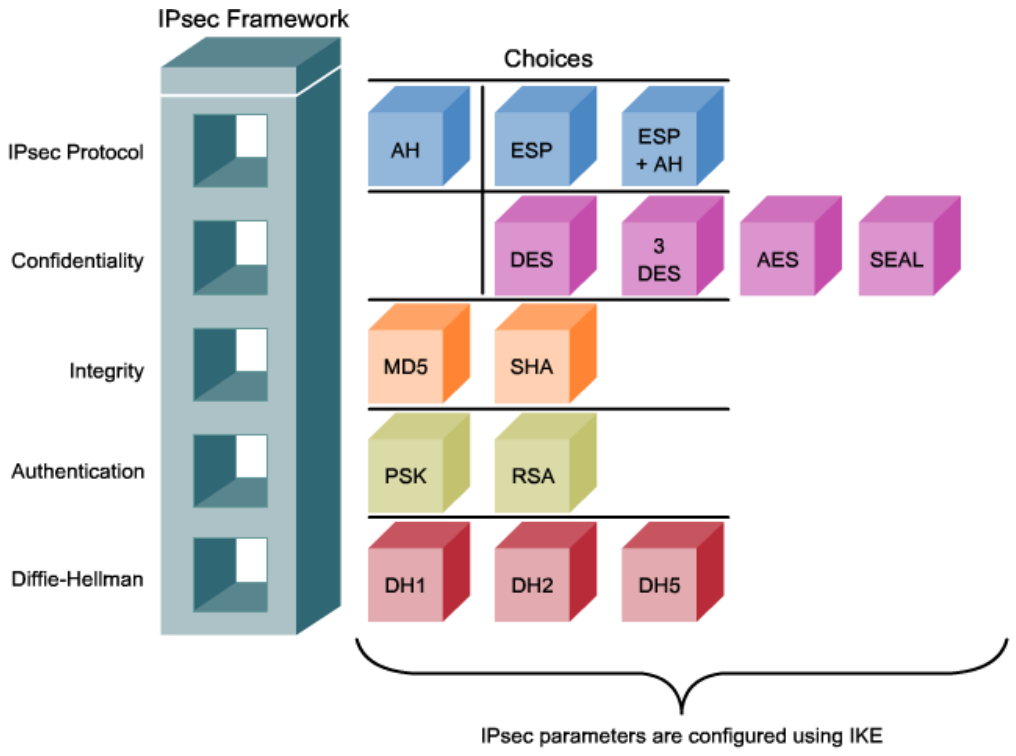


Figura 24: Parámetros IPsec utilizando IKE.

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), IPsec parameters (Figura), recuperado de CCNA Security 640 – 554 Official Cert Guide (Barker, Morris, Wallace, & Watkins, 2013)

Para establecer un canal de comunicación seguro entre dos pares, el protocolo IKE se ejecuta en dos fases:

- Fase 1 - Dos pares de IPsec realizan la negociación inicial de SAs. El propósito básico de la Fase 1 es establecer la política de negociación IKE, autenticar los pares, y establecer un canal seguro entre los pares.

  Puede ser implementado en el modo principal (antes del contacto inicial) o de modo agresivo (después de iniciar el contacto).

- Fase 2 – Las SAs son negociados por el proceso ISAKMP IKE en beneficio de IPsec. Esto Puede ser negociado en modo rápido.

En la Fase 1, en los sets de transformación, se determinan los métodos de hash, y otros parámetros.

Una sesión de IKE comienza con un router (el iniciador) enviando una serie de propuestas a otro router (el respondedor).

La propuesta enviada por el iniciador, define cual protocolos de autenticación y de cifrado son aceptables y cuánto tiempo debería ser impuesto para permanecer las claves activas con “perfect forward secrecy” (PFS).

PFS tiene la condición principal que las claves usadas para proteger los datos no son usadas para obtener cualquier otra clave.

PFS garantiza que si una clave es descubierta, las anteriores y siguientes claves se mantienen seguras. (Barker, Morris, Wallace, & Watkins, 2013)

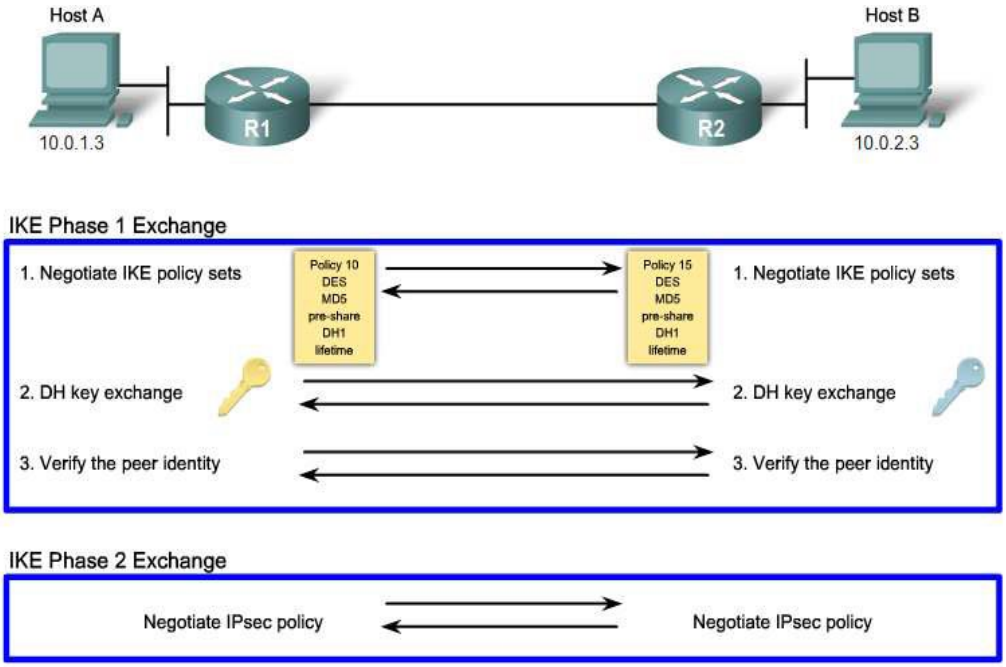


Figura 25: Fases en el intercambio de información con IKE.

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), IKE Phases (Ilustración), recuperado de CCNA Security 640 – 554 Official Cert Guide. (Barker, Morris, Wallace, & Watkins, 2013)

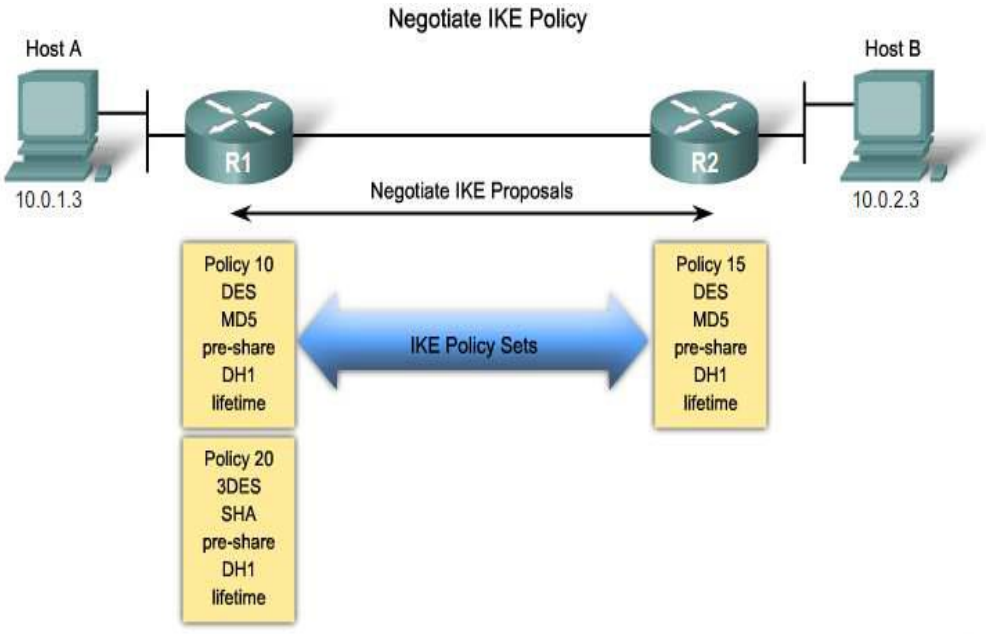


Figura 26: Negociación de la política IKE

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), First Exchange (Ilustración), recuperado de CCNA Security 640 – 554 Official Cert Guide. (Barker, Morris, Wallace, & Watkins, 2013)

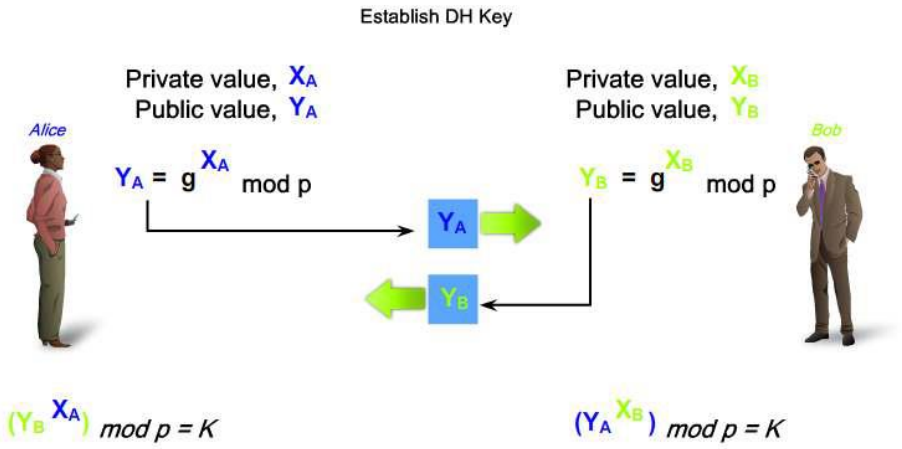


Figura 27: Establecimiento de llave DH.

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), Second Exchange (Ilustración), recuperado de CCNA Security 640 – 554 Official Cert Guide. (Barker, Morris, Wallace, & Watkins, 2013)

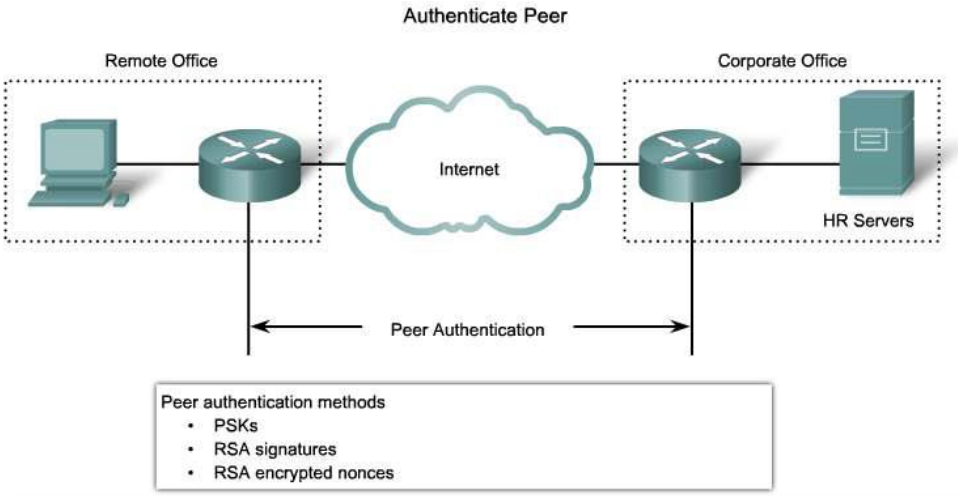


Figura 28: Autenticación de pares.

Fuente: Barker Keith, Morris Scott, Wallace Kevin y Watkins Michael (2013), Third Exchange (Ilustración), recuperado de CCNA Security 640 – 554 Official Cert Guide. (Barker, Morris, Wallace, & Watkins, 2013)

2.1.16.2.1. Modos IKE

- **MODO MAIN O PRINCIPAL**

Los 3 intercambios de la Fase 1 de IKE se denominan modo principal. La meta del modo principal es una vía de comunicación segura para el posterior intercambio entre los pares.

Consiste en el intercambio de seis mensajes entre los peers, que pueden simplificarse en estos tres intercambios mencionados anteriormente.

- **MODO AGRESIVO**

La Fase 1 IKE también puede resultar en modo agresivo. El Modo agresivo es más rápido que el modo principal porque hay pocos intercambios. El Modo agresivo comprime las fases de la negociación SA de IKE en un intercambio con tres paquetes. El modo principal requiere de tres intercambios con seis paquetes.

Los Paquetes en el modo agresivo son:

- Primer paquete.- El iniciador necesita todo los paquetes para la negociación SA en el primer mensaje, incluyendo su clave DH pública.
- Segundo paquete.- El receptor responde con los parámetros aceptables, la información de autenticación, y su clave DH pública.
- Tercer paquete.- El iniciador envía una confirmación de que ha recibido esa información.

La negociación de modo agresivo es más rápido, el ID del iniciador y el respondedor se comunican en texto plano.

Después de que se estableció el SA de IKE, La 2 fase de negociación comienza.

El objetivo de la Fase 2 de IKE es de negociar los parámetros de seguridad de IPsec que se utilizarán para la seguridad del túnel IPsec. La Fase 2 de IKE se conoce como modo rápido y sólo puede ocurrir después de IKE ha establecido el túnel seguro en la Fase 1. Los SAs se negocian por el proceso IKE de ISAKMP en representación de IPsec, el cual necesita encriptar las claves para la operación. El Modo Rapido Negocias las SAs en la

fase 2 de IKE. En esta fase, los SAS que utiliza IPsec son unidireccionales, por lo tanto, un intercambio de claves por separado se requiere para cada flujo de datos.

La Fase 2 de IKE realiza las siguientes funciones:

- Negociar los parámetros de seguridad de IPsec, IPsec transform sets
- Establece IPsec.
- Periódicamente renegocia los SAs IPsec para garantizar la seguridad
- Opcionalmente realiza un intercambio DH adicional

El Modo rápido también renegocia una nueva SA IPsec cuando la vida IPsec SA expira. Básicamente, el modo rápido se actualiza el keying material que crea la clave secreta compartida, basada en el keying material que se deriva del intercambio de DH en la Fase 1. (Ariganello & Barrientos Sevilla, 2010)

2.1.17. ¿Cómo un Administrador de Red evita que los Datos en una VPN sean espiados?

El cifrado de los datos es una forma de protegerlo. El cifrado de datos se consigue mediante la implementación de dispositivos de cifrado en cada sitio. El Internet es el la red más grande de conmutación de paquetes de red pública, por lo tanto, una VPN con IPsec implementada a través de Internet puede proporcionar importantes ahorros a una empresa en comparación con una VPN de líneas alquiladas.

Los servicios de IPsec permiten la autenticación, integridad, control de acceso y confidencialidad. Con IPsec, la información intercambiada entre sitios remotos pueden ser encriptadas y verificados. Ambas, acceso remoto y VPNs sitio a sitio puede ser desplegado usando IPsec. (Barker, Morris, Wallace, & Watkins, 2013)

2.1.18. Modelo OSI

El modelo OSI (Open System Interconnection) es el comienzo de cualquier estudio de redes. Es un modelo idealizado de 7 capas o niveles que representa la subdivisión de tareas teórica que se recomienda tener en cuenta para el estudio o diseño de un sistema.

Esto no significa que todas las redes cumplan o deban cumplir exactamente con este modelo pero se recomienda siempre tener en cuenta el modelo OSI como referencia, ya que conocimiento del mismo posibilita la correcta comprensión de cualquier red e inclusive facilita el poder realizar la comparación entre sistemas diferentes.

A cada capa se le asigna una función específica y las mismas se apilan desde la inferior a la superior de forma que cada una depende de la inmediata inferior para su funcionamiento.

Cada capa dialoga con la capa de arriba, y con su par en el otro equipo accesando la capa de abajo, este diálogo se le llama protocolo: conjunto de reglas que gobiernan el intercambio de datos entre entidades de un mismo nivel.

La unidad de información que intercambian las entidades de cada capa se le denomina PDU (Protocol Data Unit), cada capa o nivel tiene una misión distinta y no se preocupa de lo que debe hacer otro nivel. (Valencia Miranda, 2011)

Inicialmente, el modelo OSI fue diseñado por la ISO para proporcionar un marco sobre el cual crear una suite de protocolos de sistemas abiertos. La visión era que este conjunto de protocolos se utilizara para desarrollar una red internacional que no dependiera de sistemas exclusivos.

El modelo OSI proporciona una amplia lista de funciones y servicios que se pueden presentar en cada capa. También describe la interacción de cada capa con las capas directamente por encima y por debajo de él. Si bien el contenido de este curso está estructurado en torno al modelo de referencia OSI, el análisis se centra en los protocolos identificados en el modelo de protocolo TCP/IP. (Cisco, 2015)

Las 7 capas son las siguientes:

1. Física.- Los protocolos de capa física describen los medios mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar conexiones físicas para la transmisión de bits hacia un dispositivo de red y desde él.
2. Enlace de Datos.- Los protocolos de capa de enlace de datos describen los métodos para intercambiar tramas de datos entre dispositivos en un medio común.
3. Red.- La capa de red proporciona servicios para intercambiar los datos individuales en la red entre dispositivos finales identificados.
4. Transporte.- La capa de transporte define los servicios para segmentar, transferir y rearmar los datos para las comunicaciones individuales entre dispositivos finales.
5. Sesión.- La capa de sesión proporciona servicios a la capa de presentación para organizar su diálogo y administrar el intercambio de datos.
6. Presentación.- La capa de presentación proporciona una representación común de los datos transferidos entre los servicios de la capa de aplicación.
7. Aplicación.- La capa de aplicación proporciona los medios para la conectividad de extremo a extremo entre individuos de la red humana mediante redes de datos. (Cisco, 2015)

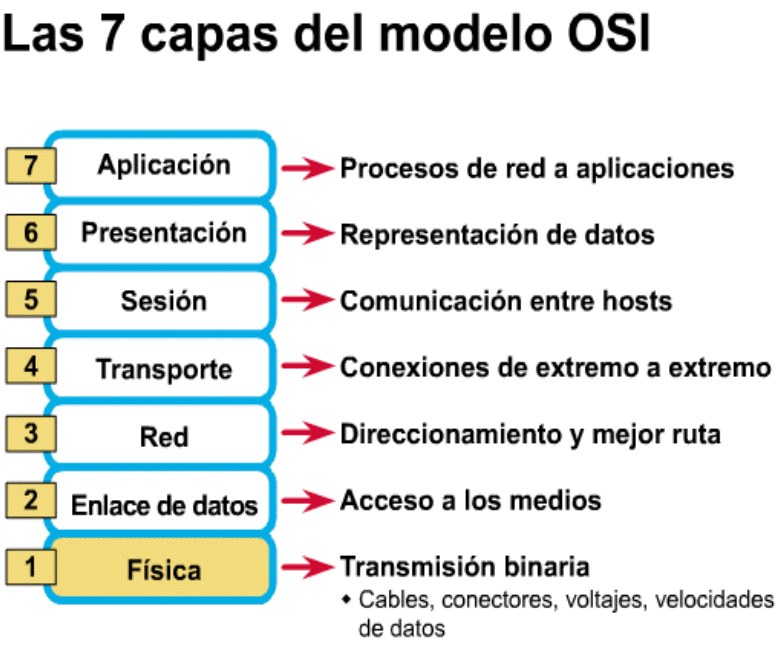


Figura 29: Capas del Modelo OSI.

Fuente: Marín Hector (2015), Las capas del Modelo OSI (Ilustración), recuperado de https://www.goconqr.com/p/4174862-diapositivas-de-el-modelo-osi-slide_sets (Marín Alarcón, 2015)

2.1.19. Capa de Red del Modelo OSI

La capa de red (capa 3 OSI) define el enrutamiento y el envío de paquetes entre redes. Su función es transferir datos desde el host que origina los datos hacia el host que los usa, a través de varias redes separadas si fuera necesario.

"La capa de red del modelo OSI proporciona el enrutamiento de mensajes y determina si el destino de estos es la capa 4 (Transporte) o la capa 2 (Enlace de Datos)".

Esta capa provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados. Para realizar este transporte de extremo a extremo la Capa de red utiliza cuatro procesos básicos:

- ✓ Direccionamiento
- ✓ Encapsulamiento

- ✓ Enrutamiento
- ✓ Desencapsulamiento

Durante la encapsulación en el host origen, un paquete IP se construye en la Capa de red para transportar el PDU de la Capa 4.

Gracias a esto, el paquete puede llevar una PDU a través de muchas redes y muchos routers. Para ello, las decisiones de envío están basadas en la información del encabezado del paquete IP.

- **Nociones importantes que debemos conocer sobre Capa de red**

Ningún paquete puede ser enviado sin una ruta.

Los routers y otros dispositivos de networking, almacenan estas rutas en las tablas de enrutamiento, y las usan para determinar dónde enviar los datos.

Los routers en su tabla de enrutamiento tienen tres características principales:

- Red de destino
- Próximo salto
- Métrica

Un router toma una decisión de reenvío para cada paquete que llega a la interfaz del gateway. Este proceso de reenvío es denominado enrutamiento.

El enrutamiento se hace paquete por paquete y salto por salto.

El router hará una de tres cosas con el paquete:

- Enviarlo al router del próximo salto

- Enviarlo al host de destino
- Descartarlo

Enrutamiento Dinámico:

Entre los protocolos de enrutamiento comunes se incluyen:

- Protocolo de información de enrutamiento (RIP),
- Protocolo de enrutamiento de gateway interior mejorado EIGRP
- Open Shortest Path First OSPF

En este punto es también muy importante conocer el concepto de Gateway (Puerta de Enlace), o Gateway por defecto.

El Gateway es la vía de salida de nuestra red. Por ejemplo, si un paquete va destinado desde un pc en la red A hacia otra red distinta, el paquete primero se enviará a la gateway de la red A. Normalmente el gateway será el router conectado directamente a esa red local. (Anónimo, Capa de Red | Capa 3 OSI, 2012)

2.1.20. CISCO IOS

La naturaleza abierta de Internet hace que seguridad de su Red sea vital para las empresas. Dado que las empresas mueven cada vez más sus funciones de negocio a la red pública, necesitan tomar precauciones para asegurarse de que los datos no puedan ser comprometidos y no sean accesibles a cualquier persona que no esté autorizada para verlo. El acceso no autorizado a la red por un hacker externo o un empleado descontento puede causar daños o la destrucción de los datos de propiedad, afecta negativamente a la productividad de la empresa, e impiden la capacidad de competir. El Instituto de Seguridad Informática informó que en un día promedio, el 41,1% de encuestados fueron

atendidos con al menos un incidente de seguridad. El acceso no autorizado a la red puede también dañar las relaciones con clientes y socios de negocios, que podría cuestionar la capacidad de una empresa para proteger su información confidencial. Los individuos y las corporaciones pueden beneficiarse de la implementación elástica de los servicios en la nube, disponible en todo momento desde cualquier dispositivo, pero estos cambios dramáticos en la industria de servicios empresariales agravan los riesgos en materia de protección de datos y las entidades de utilizarlo (individuos, empresas, gobiernos, etc.). Políticas de seguridad y arquitecturas requieren principios sólidos y un enfoque de ciclo de vida, incluyendo si los datos están en la granja de servidores, móviles en la computadora portátil del empleado, o almacenados en la nube. (Paquet, 2013)

2.1.20.1. DEFINICIÓN DE CISCO IOS

Cisco IOS (originalmente Internetwork Operating System) es el software utilizado en la gran mayoría de routers y switches de Cisco Systems (algunos conmutadores obsoletos ejecutaban CatOS). IOS es un paquete de funciones de enrutamiento, conmutamiento, trabajo de internet y telecomunicaciones que se integra estrechamente con un sistema operativo multitarea.

La interfaz de línea de comandos de IOS (IOS CLI) proporciona un conjunto fijo de comandos de múltiples palabras. El conjunto disponible se determina mediante el "modo" y el nivel de privilegios del usuario actual. El modo "Global configuration" proporciona comandos para cambiar la configuración del sistema y el modo "interface configuration" a su vez, proporciona comandos para cambiar la configuración de una interfaz específica. A todos los comandos se les asigna un nivel de privilegios, de 0 a 15, y pueden ser accedidos por usuarios con los privilegios necesarios. A través de la CLI, se pueden definir los comandos disponibles para cada nivel de privilegio.

- **Arranque del IOS**

Al arrancar un dispositivo de Cisco este realiza un Bootstrap (comprobación de hardware).

Después intentará cargar una imagen IOS desde la memoria Flash o desde un servidor TFTP. En el caso de no hallarla ejecutará una versión reducida de la IOS ubicada en la ROM.

Tras el arranque del sistema localizará la configuración del mismo, generalmente en texto simple. Puede estar ubicada en la memoria NVRAM o en un servidor de TFTP. En el caso de no encontrarla iniciará un asistente de instalación (modo Setup).

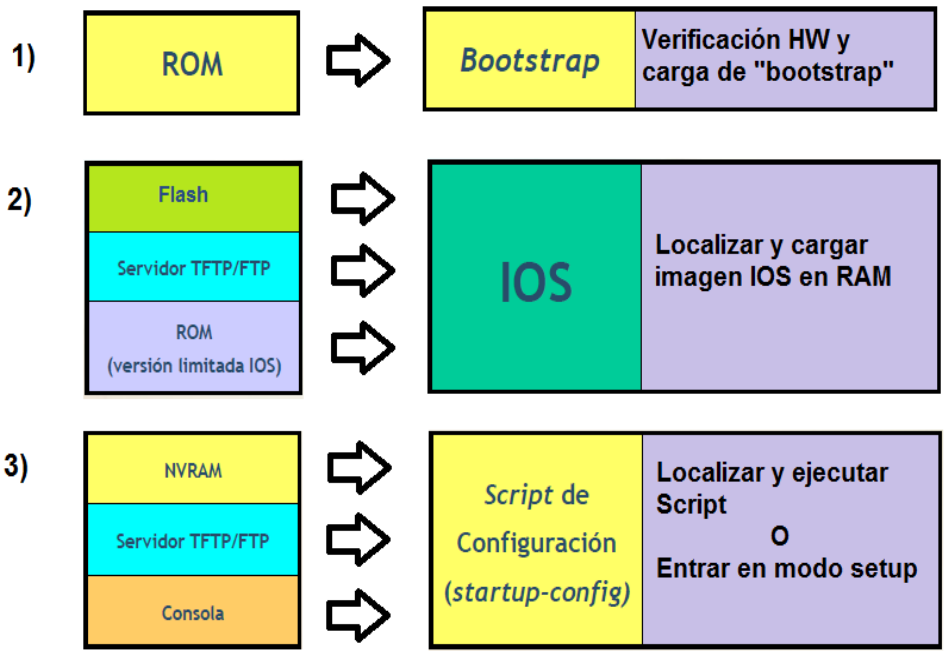


Figura 30: Secuencia de Arranque Cisco IOS.

Fuente: Aka. Daligar (2012), Secuencia de Arranque equipos Cisco (Ilustración), recuperado de https://commons.wikimedia.org/wiki/File:Arranque_Ios.png (Daligar, 2012)

- **Sistema de Archivos**

IOS File System (IFS) puede acceder y almacenar distintos tipos de datos en:

- Bootflash
- Flash. Se usa para almacenar imágenes completas del software cisco IOS. Guarda copia del sistema operativo.
- Flh ASI
- Nvram. Es uno de los componentes de configuración interna de un router. Se usa para almacenar un archivo de configuración de respaldo/inicio
- RCP
- Slo
- Slot1
- System
- TFTP

- **Modos de configuración**

Modo USER EXEC: Modo sin privilegios en el que no podemos modificar ni leer la configuración del equipo. Básicamente, solo podemos utilizar: show, ping, telnet, traceroute. (Wikipedia, 2016)

2.1.21. CISCO CONFIGURING PROFESSIONAL

Cisco Configuring Professional (CCP), es una herramienta de gestión de dispositivos basada en GUI para los routers de acceso de Cisco, específicamente routers de servicios integrados (ISR) y los routers de servicios integrados de segunda generación (ISR G2).

Esta herramienta simplifica enrutamiento, firewall, IPS, VPN, comunicaciones unificadas, WAN y LAN configuración a través de asistentes basadas en GUI.

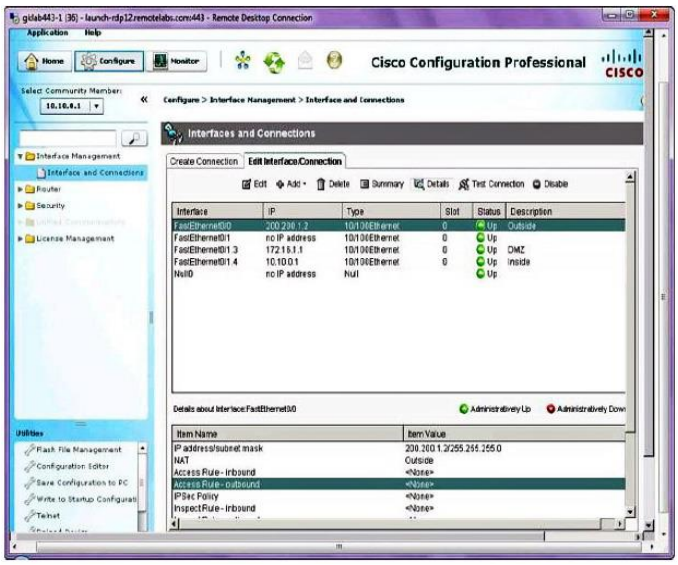


Figura 31: Ventana Principal de Cisco Configuring Professional.

Fuente: Paquet Catherine (2013), CCP window (Figura), recuperado de Implementing Cisco IOS Network Security (IINS) Foundation Learning Guide. (Paquet, 2013)

CCP es una herramienta valiosa para mejorar la productividad para los administradores de red, siendo utilizado para el despliegue de routers con mayor confianza y facilidad. Ofrece un bloqueo del router con un solo clic y una innovadora capacidad de auditoría de seguridad de voz además de comprobar y recomendar cambios en la configuración del router. CCP También supervisa el estado del router y soluciona problemas de WAN y problemas de conectividad en una VPN. La interfaz gráfica de usuario incluye opciones para configurar los módulos del motor Cisco Servicios-Ready (SRE), lo que facilita la integración basada en la funcionalidad del hardware y la centralización de su configuración en el mismo lugar en el que el router alojado está configurado. CCP es gratuito, y se puede descargar desde http://www.cisco.com/go/ciscocp.

Al basarse en configuraciones de mejores prácticas que han sido aprobados por el Centro de asistencia técnica de Cisco (TAC), los administradores de red pueden aprovechar de CCP, para lograr lo siguiente:

- Reducir el coste total de propiedad (TCO) de los routers de Cisco
- Reducir los errores humanos
- Simplificar la configuración inicial en las implementaciones de voz
- Ayudar a que exista una interrelación adecuada entre los usuarios, los planes de marcación, y la configuración de correo de voz

CCP ofrece asistentes inteligentes y soporte de configuración avanzada para lo siguiente:

- Interfaces LAN y WAN
- Network Address Translation (NAT)
- Política firewall de aplicaciones
- IPS, IPsec y SSL VPN
- Calidad de servicio (QoS)
- Control de admisión de red de Cisco (NAC) características de la políticas.

CCP permite a los administradores organizar y gestionar fácilmente varios enrutadores en un solo sitio. (Paquet, 2013)

2.1.22. CONFIGURACIÓN SITIO A SITIO SEGÚN LABORATORIO CCNA SECURITY

Para el desarrollo de la presente tesis, se tomó referencia la topología del laboratorio CCNA Security, indicado a continuación en la Figura 32.

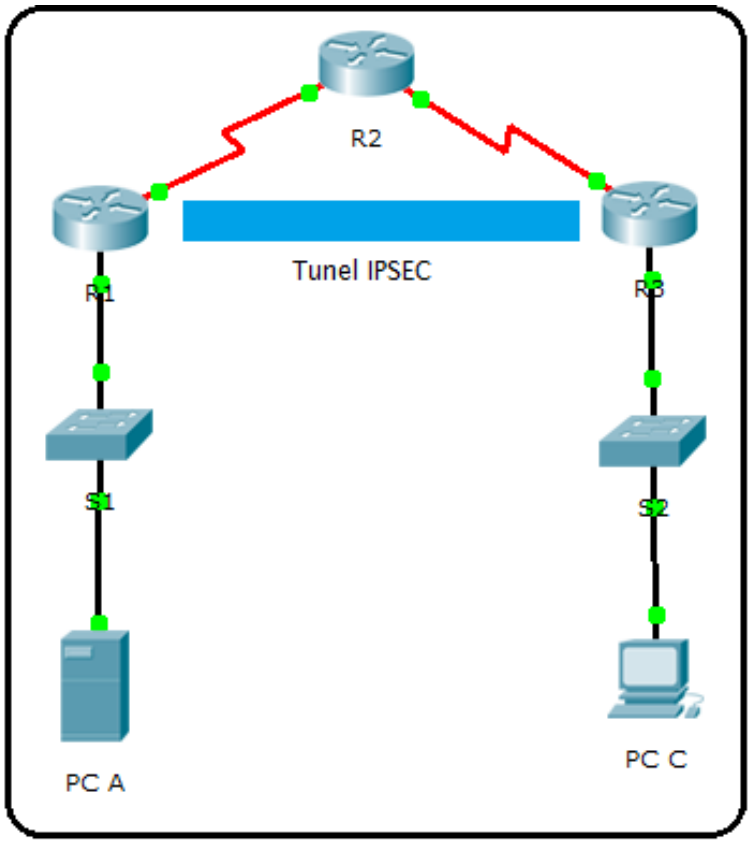


Figura 32: Topología ideal Laboratorio de CCNA Security

Fuente: CCNA Security (2017), Topologia ideal Laboratorio de CCNA Security (Figura), Laboratorio - Configuring a Site-to-Site VPN Using Cisco IOS and CCP. (Cisco Networking Academy, 2017)

Una VPN es un canal de comunicación que se utiliza para formar una conexión lógica entre dos extremos de una red pública. La VPN no necesariamente incluye el cifrado o la autenticación. La VPN IPsec se basa en el protocolo IKE para establecer comunicaciones seguras.

La negociación IPsec en la VPN contiene varios pasos.

1. Un túnel IPsec se inicia cuando el host A envía tráfico "interesante" al host B. El tráfico se considera de interés cuando este viaja entre pares IPsec y cumple con los criterios que se define en la lista de control de acceso (ACL) criptográficas.

2. La Fase 1 IKE comienza. El par IPsec negocia el establecimiento de las políticas de seguridad IKE (SA). Cuando los pares se autentican, un túnel seguro es creado usando Internet Security Association and Key Management Protocol (ISAKMP).

3. La Fase 2 IKE comienza. Los pares de IPsec utilizan el túnel seguro autenticado para negociar la asociación de seguridad (SA) IPsec. La negociación de la política común determina cómo se establece el túnel IPsec.

4. El túnel IPsec se crea y se transfieren datos entre el par IPsec basado en los parámetros de IPsec que se configuran en los IPsec transform sets.

5. El túnel IPsec termina cuando la SA IPsec se suprimen o cuando expira su vida útil.

Existen tareas básicas que necesitan ser desarrolladas para configurar una VPN site-to-site con IPsec.

Tarea 1. Asegurarse de que las ACL configuradas en la interfaz son compatibles con la configuración de IPsec. Generalmente estas son restricciones en la interfaz en que el tráfico VPN se utiliza, por ejemplo, bloquear todo el tráfico que no es IPsec o IKE.

Tarea 2. Crear una directiva de ISAKMP para determinar los parámetros de ISAKMP que se utilizarán para establecer el túnel.

Tarea 3. Definir el IPsec transform set. El transform set define los parámetros que usa el túnel IPsec. El conjunto puede incluir los algoritmos de encriptación y de integridad.

Tarea 4. Crear una crypto ACL. La crypto ACL define cual tráfico se envía a través del túnel IPsec protegido por el proceso de IPsec.

Tarea 5. Crear y Aplicar Crypto Map. El Grupo Crypto Map previamente configurado los parámetros y definir los dispositivos pares IPsec. El Crypto Map es aplicado a la interfaz de salida de la VPN.

Para implementar la VPN utilizaremos como referencia el laboratorio “Configuring a Site-to-Site VPN Using Cisco IOS and CCP” del curso CISCO Security” (Cisco Networking Academy, 2017)

Por lo que seguiremos las siguientes etapas:

a) Primera Etapa: Configuración de Routers y Switchs.

Como primer paso se diseñara y configurará la topología de la red además de los equipos a utilizar, así como el direccionamiento IP de las interfaces, el enrutamiento dinámico, el acceso al equipo y las contraseñas. Así mismo se realizará el direccionamiento IP correspondiente:

a.1.) Configuración de comandos en cada Router

Al realizar la configuración inicial, se renombra cada router y se asigna las direcciones IP en cada interfaz de los routers para facilitar su reconocimiento, de la misma manera se configura las direcciones IP en cada PC.

a.2.) Configuración de Enrutamiento Dinámico

Al terminar de configurar las direcciones IP, se procede con el enrutamiento dinámico en los routers; en este caso se utilizó el protocolo OSPF para realizar dicho enrutamiento.

a.3.) Configuración de PCs y prueba de conectividad de Red

Se asignarán direcciones IP a las host y se comprobará su conectividad utilizando el comando Ping.

b) Segunda Etapa: Configuración site-to-site utilizando Cisco IOS CLI

Esta parte se enfoca en la configuración del túnel IPsec VPN entre los routers.

b.1.) Configuración de ajustes IPsec de la VPN

Se procede a la habilitación de la política IKE entre los routers.

Para permitir la negociación en la Fase 1 de IKE, se crea una directiva ISAKMP y se configura una asociación de pares involucrados con esa directiva ISAKMP. Una directiva ISAKMP define los algoritmos de autenticación y cifrado y la función hash utilizada para enviar tráfico de control entre los dos puntos finales de la VPN. Cuando la asociación de seguridad (SA) ISAKMP haya sido aceptada por los pares IKE, significa que se ha completado la Fase 1 de IKE. Los parámetros de la Fase 2 de IKE se configurarán más adelante.

b.2.) Configuración de los parámetros ISAKMP en Routers

Resumiendo conceptos para la aplicación de los protocolos reconocemos que: La elección de un algoritmo de cifrado determina la confidencialidad del canal de control entre los extremos. Para el control de la integridad se tiene el algoritmo hash y para la autenticación existe Diffie-Hellman.

b.3.) Asignación de Clave Precompartida (PSK)

Aquí se configuran claves en cada router para la autenticación.

b.4.) Configuración del set de transformaciones IPsec

El set de transformaciones IPsec es otro parámetro de configuración de cifrado que los routers negocian para formar una asociación de seguridad. Especifica los algoritmos criptográficos y las funciones (transformaciones) que utilizará nuestro router en los

paquetes de datos reales enviados a través del túnel IPsec. Estos algoritmos incluyen los servicios de cifrado, encapsulación, autenticación e integridad de datos que IPsec puede aplicar.

b.5.) Definición de tráfico importante

El enviar todo los datos generados por los host de la red encriptado causará que el router consuma muchos recursos en el proceso de encriptación y no atienda otros procesos tales como el enrutamiento, entre otros. Por ello es necesario limitar los host y/o las aplicaciones cuyos datos van a ser encriptados. Para ello utilizaremos las acces-list, las cuales pueden ser nombradas o numeradas. Mencionaremos que todas las listas de acceso tienen al final una sentencia implícita.

b.6.) Creación y aplicación de un mapa de encriptación para la VPN

En este punto se realiza una triple asociación: tráfico, configuraciones IKE o IPSec y por último interfaces. Para la creación de Crypto Map, utilizamos el comando "**crypto map name-sequence- num type"** en modo de configuración global para ingresar al modo de configuración del Crypto Map.

Luego, se emite el comando "**match address acces-list"** donde se especifica qué lista de acceso define el tráfico a encriptar.

Ahora, es necesario establecer un par IP o un nombre de host, en nuestro caso el par se define en la interfaz de punto de llegada remota en RCAD de la VPN.

Después, se codifica el set de transformaciones que se va a utilizar con el par anteriormente mencionado, utilizando el comando "**set transform-set –ta"**" donde se establece el tipo perfecto de reenvío secreto utilizando el comando "**set pfs tipo**" además

se modifica el tiempo de vida de la asociación de seguridad IPsec predeterminada con el comando "**set security-association lifetime seconds –seconds**".

b.7.) Comprobación de configuración de IPsec y Crypto Maps

Las configuraciones realizadas se comprobarán con el comando "**show crypto IPsec transform-set**" y el comando "**show crypto map**"

c) Tercera Etapa: Configuración de la VPN con Cisco Configuring Professional

En las anteriores etapas se desarrolló la metodología para implementar la VPN íntegramente con la configuración en Cisco IOS CLI. Existe otro modo de configuración de VPN que es el utilizar el Software Cisco Configuring Professional o CCP, que básicamente brinda una interfaz gráfica a las configuraciones aplicadas en Cisco IOS CLI.

Además de ello, lo que motivó a trabajar con este software es la posibilidad que tiene de administrar varias VPN a la vez desde una misma aplicación, permitiendo así que el desarrollo de la VPN en la UNA – Puno en un futuro sea integro en todas sus oficinas.

c.1.) Configuración de la VPN con IPsec en los Routers utilizando CCP

Luego de asegurar que existe conectividad, se establece los parámetros de seguridad en la interfaz gráfica del software CCP para los routers utilizados en la topología.

2.2. HIPÓTESIS DE LA INVESTIGACIÓN

2.2.1. Hipótesis General

Es posible diseñar e implementar el prototipo de una Red Privada Virtual en Capa 3 utilizando CISCO IOS que permita asegurar y encriptar la información compartida entre las oficinas de la Universidad Nacional del Altiplano.

2.2.2. Hipótesis Específicas

a) El diseño del prototipo de la Red Privada Virtual opera y controla el tráfico en LAN y WAN.

b) Se puede implementar la Red Privada Virtual en el Laboratorio de Cisco de la Universidad Nacional del Altiplano.

CAPITULO III

MATERIALES Y MÉTODOS

3.1. DISEÑO METODOLÓGICO DE LA INVESTIGACIÓN

3.1.1. Tipo y Diseño de Investigación

La investigación de este proyecto es de tipo aplicativo; ya que consiste en el empleo práctico del conocimiento de las Redes que deben utilizarse en las instituciones para proteger diferentes tipos de información: protocolos de enrutamiento y el diseño de redes de routers con la finalidad de mejorar y resolver el problema concreto de la seguridad en transmisión de datos en las redes actuales. La investigación aplicativa busca la generación de conocimiento con aplicación directa a los problemas de la sociedad o el sector productivo. Esta se basa fundamentalmente en los hallazgos tecnológicos de la investigación básica, ocupándose del proceso de enlace entre la teoría y el producto. (Lozada, 2014)

3.1.1.1. Nivel de Investigación

La presente investigación es exploratoria, correlacional y descriptiva.

Es exploratoria, porque se examina un tema o problema de investigación poco estudiado, como es el caso de la aplicación de una Red Privada Virtual en capa 3 para la Universidad

Nacional del Altiplano. (Hernández Sampieri, Fernández-Collado, & Baptista Lucio, 2006, págs. 100-101)

Es correlacional por que tiene como propósito medir el grado de relación entre las variables de las hipótesis planteadas. (Hernández Sampieri, Fernández-Collado, & Baptista Lucio, 2006, pág. 105)

Así como también es descriptiva, porque no se da la manipulación de variables, estas se observan y se describen tal como se presentan en la realidad, su metodología es fundamentalmente descriptiva, aunque puede valerse de algunos elementos cuantitativos y cualitativos. (Hernández Sampieri, Fernández-Collado, & Baptista Lucio, 2006, pág. 102)

3.1.1.2. Diseño de la Investigación

La Investigación es de tipo experimental, porque es un tipo de investigación que utiliza la lógica y los principios encontrados en las ciencias y que serán implementados en una red real mediante un prototipo. La esencia de esta concepción de experimento es que requiere la manipulación intencional de una acción para analizar sus posibles resultados.

Los experimentos pueden ser llevados a cabo en el laboratorio o en la vida real. Aquí se involucran un número relativamente pequeño de personas o equipos y abordan una pregunta bastante enfocada. Los experimentos son más efectivos para la investigación explicativa y frecuentemente están limitados a temas en los cuales se puede manipular la situación en la cual las personas se hallan. (Hernández Sampieri, Fernández-Collado, & Baptista Lucio, 2006, págs. 159-160)

3.2. POBLACIÓN Y MUESTRA DE INVESTIGACIÓN

Al tratarse de una investigación para la Universidad Nacional del Altiplano, se debe identificar las oficinas que hacen uso frecuente del Sistema Universitario así como el tipo de información que éstas intercambian.

Según el Reglamento de Organización y Funciones 2016 (Universidad Nacional del Altiplano, 2016) de ésta casa superior de estudios en el artículo 195, los apéndices 'c', 'd' y 'k' nos indican que:

"Son funciones de la Oficina de Tecnología Informática y Telecomunicaciones:

- Evaluar, proponer, diseñar y desarrollar sistemas de información de acuerdo a las necesidades institucionales.
- Organizar y poner en funcionamiento los sistemas automatizados de procesamiento de información y de manejo administrativo en las dependencias académicas y administrativas de la Universidad.
- Velar por la seguridad de la información automatizada de la institución."

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

"La Coordinación Académica es la encargada de planificar, organizar, ejecutar, controlar y evaluar la información de la actividad académica, estructura curricular, registro y archivo académico de la Facultad."

De todo lo señalado se concluye que, al identificar las necesidades específicas que pretende solucionar esta investigación y, reconociendo las oficinas con prioridad para resolver dichas necesidades, se establece que nuestra población es:

La Oficina de Tecnología Informática y Telecomunicaciones.

Las 19 Coordinaciones Académicas correspondientes a cada facultad.

3.2.1. Muestra de la Investigación

Debido a que el propósito de ésta investigación es asegurar datos informáticos, el prototipo debe contener los materiales y equipos involucrados en la investigación, ya que en ellos será implementada la VPN.

A sabiendas que los equipos necesarios son routers, switches y computadoras, se define que el prototipo será realizado en el laboratorio de Cisco, por su factibilidad en la realización de pruebas para la VPN.

Es así que se concluye que, al no ser prioritario ni necesario, nuestra investigación no cuenta con una muestra definida.

3.3. UBICACIÓN DE LA POBLACIÓN

Universidad Nacional del Altiplano;

Escuela Profesional de Ingeniería Electrónica;

Laboratorio de Cisco.

Dirección: Av. Floral Nº 1153, Puno.

Coordenadas: Latitud: -15.824957 | Longitud: -70.015483

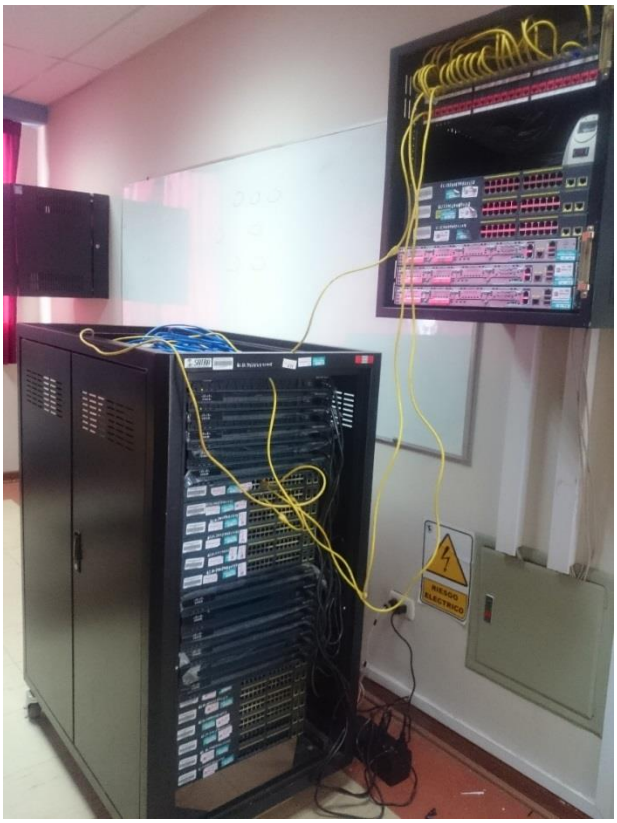


Figura 33: Laboratorio de Cisco UNA - Puno.

Elaboración: Propia.

3.4. MATERIAL EXPERIMENTAL

3.4.1. Hardware

- Computadoras de Escritorio

Cantidad : 02

Procesador : Intel® Core™ i5-2430AM, CPU @ 2.40 GHz

Memoria Instalada (RAM) : 4.00 GB

Tipo de Sistema : Sistema Operativo de 64 bits, Windows 7 Ultimate Service Pack 1

- Servidor: DELL Power Edge R620 (Puma Quispe & Cutipa Nina, 2015)

Cantidad	: 01
Procesador	: Intel® Xeon® E5-2640, 2.50GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95W, DDR3-1333MHz
Memoria RAM	: 768 GB RDIMM, 1600 MHz, Low Volt, Single Rank, x4 Data Width
Ranuras de memoria	: 24
Tipo de memoria interna	: DDR3
Disco Duro	: 146GB, SAS 6Gbps, 2.5in, 15K RPM Hard Drive (Hot-Plug)
Red	: - 1 GbE BASE-T de cuatro puertos Broadcom - 1 GbE BASE-T de cuatro puertos Intel - 1 GbE BASE-T de dos puertos Intel + dos 1 GbE
Fuente de alimentación	: Fuente de alimentación redundante de 750 vatios, de conexión en marcha y eficiencia Titanium
Sistema Operativo	: Linux

- Router Cisco 2901 (HiperLink Technologies, 2016)

Cantidad : 03

Características:

- Puertos Ethernet 10/100/1000 integrados
- Ranuras mejoradas de alta velocidad para interfaces deWAN
- 2 Ranuras para el procesador de señales digitales (DSP)
- 1 Módulo de servicio para los servicios de aplicaciones
- Energía totalmente integrado de distribución de los módulos de soporte 802.3af Power over Ethernet (PoE) y Cisco PoE mejorada

Tipo de Producto Router : Factor de forma Externo - modular - 1U

Peso : 6,1 kg

Dimensión : 43.9 cm x 43.8 cm x 4.5 cm

DRAM Memoria : 512 MB (instalados) / 2 GB (máx.)

Memoria Flash : 256 MB (instalados) / 8 GB (máx.)

Protocolo de direccionamiento: OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, enrutamiento IPv4 estático, enrutamiento IPv6 estático

Protocolo de gestión remota : SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, SSH

Protocolo de interconexión de datos: Ethernet, Fast Ethernet, Gigabit Ethernet

Protocolo de gestión remota : NMP, RMON. Características del Cisco IOS IP Base, soporte de MPLS, soporte para Syslog, soporte IPv6, Queue Server (CBWFQ), Detección ponderado Class-Based Fair Weighted Random Early (WRED)

Cumplimiento de normas : IEEE 802.1Q, IEEE 802.3af, IEEE 802.3ah, IEEE 802.1ah, IEEE 802.1ag

Alimentación : CA 120/230 V (50/60 Hz)

- Switch Cisco 2960 (Intercompras, 2015)

Cantidad : 02

Tecnología de cableado ethernet de cobre: 100BASE-T, 10BASE-T

Cantidad de puertos Fast Ethernet (cobre): 24

Cantidad de puertos SFP : 02

Puertos tipo básico de conmutación RJ-45 Ethernet: Fast Ethernet (10/100)

Cantidad de puertos básicos de conmutación RJ-45 Ethernet: 24

Peso : 3.6kg

Dimensión : 45cm x 4.4cm x 24.2cm

Memoria interna : 64 MB

Memoria Flash : 32 MB

Protocolos de gestión : SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP

Bidireccional completo (Full duplex): Si

Número de VLANs soportadas: 255

Algoritmos de seguridad soportados: 802.1x RADIUS, SSH-2

Adicionalmente a los equipos anteriormente mencionados, se utilizaron los materiales contenidos en la Tabla N° 1.

Material	Cantidad	Descripción
Laptops	02	Procesador: Intel® Core™ i5-2430AM, CPU @ 2.40 GHz Memoria Instalada (RAM): 4.00 GB Tipo de Sistema: Sistema Operativo de 64 bits, Windows 7 Ultimate Service Pack 1
Cables UTP Categoría 5	06	- Para conexiones y aplicaciones IP. - Conductor de cobre sólido de 0.51 mm. - Diámetro exterior 5 mm. - Desempeño probado hasta 200 Mhz. - Impedancia: 100 Ω. Aplicaciones - 1.2 Gbps ATM.
Cable Serial DCE	02	Un dispositivo que suministra los servicios de temporización a otro dispositivo. Habitualmente, este dispositivo se encuentra en el extremo del enlace que proporciona el acceso.

Continúa…

Cable Serial DTE	02	Un dispositivo que recibe los servicios de temporización desde otro dispositivo y se ajusta en consecuencia. Habitualmente, este dispositivo se encuentra en el extremo del enlace del cliente o del usuario.
Convertidor Serial/USB	02	- Admite interfaz serial RS-232 - Admite hasta una transferencia de datos de 500kbps - Compatible con Windows 7 / Vista / XP / 2000 / ME / 98SE / Mac OS 10.1~10.6 - Se instala como un puerto COM de Windows estándar, señales de control de módem Full RS-232 , señales de datos RS-232; TxD, RxD, RTS, CTS, DSR, DTR, DCD, RI, GND
Conector RJ-45	12	- Desempeño superior a 150 Mhz. - Código de color T 568 A y B. - Los conectores RJ-45 K5e, cumplen con las normas ISO/IEC 11801, EIA/TIA 568 B, EN 50173, UL y NMX-I-NYCE-248-2005. - Frecuencia 100 MHz

Tabla N° 1: Materiales adicionales a utilizar en la investigación.

Elaboración: Propia.

3.4.2. Software

- Sistema Operativo de 64bits Windows 7 Ultimate Service Pack 1
- Sistema Operativo Linux: Ubuntu Server 14.04.1 LTS
- CISCO IOS CLI (Preinstalado en los equipos CISCO)
- Software de simulación Packet Tracer v7.0
- Software de simulación GNS 3 v1.5.3

- Cisco Configuring Professional v2.5
- Cisco VPN Client v5.0.07
- Software para configuración de consola HyperTerminal
- Virtual Box v5.0.36
- Software Wireshark v2.2.5
- Microsoft Office 2010

3.4.3. Recursos y Materiales para la Investigación

- Horas de Internet (500 aprox.)
- Textos CCNA Security
- Papers IEEE
- Otros Textos referidos a la investigación

3.4.4. Presupuesto

En la Tabla N° 02 se especifica el costo de los materiales experimentales por unidad, además del costo total para la implementación de la VPN.

Descripción	Unidad de medida	Costo Unitario (S/.)	Cantidad	Costo total (S/.)
Router Cisco 2901	Unidad	5300.00	3	15900.00
Switch Cisco 2960	Unidad	3100.00	2	6200.00
Computadora	Unidad	4000.00	2	8000.00
Laptop	Unidad	3000.00	1	3000.00

Continúa…

Cable UTP Categoría 5	Metro	3.00	24	72.00
Cable Serial DCE	Unidad	40.00	2	80.00
Cable Serial DTE	Unidad	40.00	2	80.00
Convertidor Serial/ USB	Unidad	25.00	2	50.00
Conector RJ-45	Unidad	1.00	12	12.00
Texto CCNA Security	Unidad	255.00	1	255.00
Texto CCNA Security	Unidad	135.00	1	135.00
Papers IEEE	Unidad	44.00	2	88.00
Imprevistos (10%)	-	-	-	3387.20
Total				37259.20

Tabla N° 2: Presupuesto para la realización de la Investigación.

Elaboración: Propia

3.5. TÉCNICAS E INSTRUMENTOS PARA RECOLECTAR INFORMACIÓN

3.5.1. Técnicas

La técnica utilizada en ésta investigación fue:

La observación: Es una técnica de recopilación de datos semi-primaria por la cual el investigador actúa sobre los hechos a veces con la ayuda de algunos instrumentos. (Puma Quispe & Cutipa Nina, 2015)

3.5.2. Instrumentos

El instrumento a utilizar es:

Guía de observación de campo: Pasos que adopta el investigador a fin de hacer una buena estrategia para observar los hechos. (Puma Quispe & Cutipa Nina, 2015)

3.6. PROCEDIMIENTO DEL EXPERIMENTO

Como se mencionó en el marco teórico se utilizaron los siguientes pasos y comandos para implementar la red privada virtual:

3.6.1. Configuración inicial en Routers y demás equipos utilizados para implementación de la VPN.

En esta parte diseñamos y configuramos la topología de nuestra VPN, implementado en base a una a una topología ideal, además se realizan las configuraciones básicas, así como las direcciones IP para cada una de las interfaces, el tipo enrutamiento y las contraseñas de seguridad para acceder a los routers; este procedimiento será simulado en el Software Packet Tracer para su implementación en el laboratorio de Cisco de la UNA Puno.

Al reconocer que la información sensible está focalizada en las coordinaciones académicas de las diferentes facultades de la UNA, es que se toma en cuenta realizar un diseño que interconecte las mismas con el servidor central de la OTI y con el administrador de la red integrada de ésta institución. Identificando los factores involucrados es que se diseña el prototipo de la VPN con la siguiente topología:

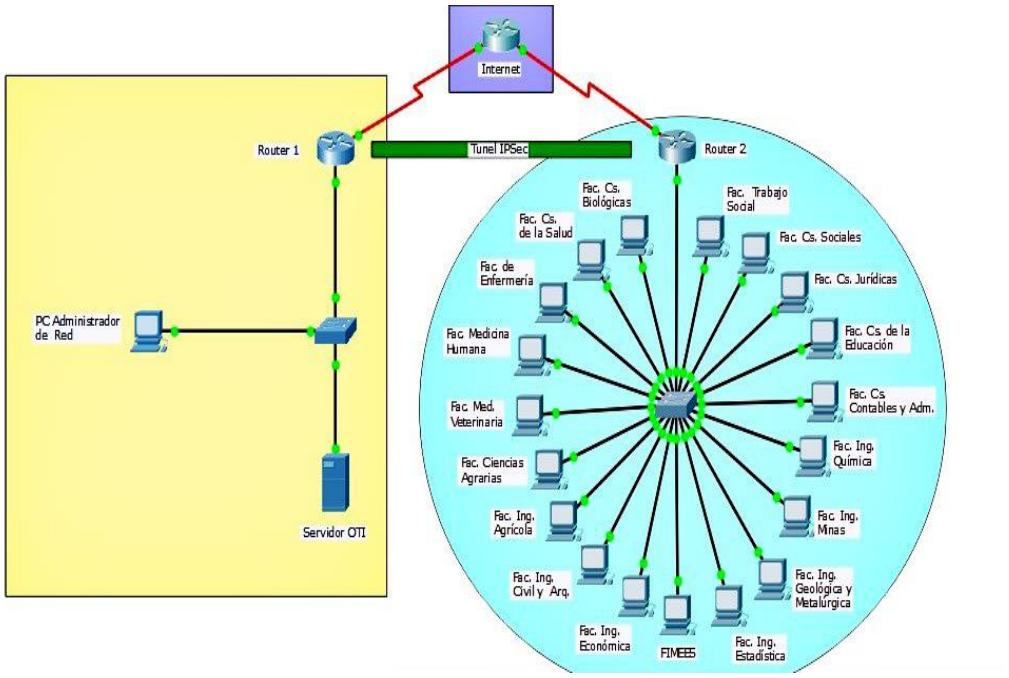


Figura 34: Topología ideal de VPN en la UNA – Puno en Software Packet Tracer 7.0.

Elaboración: Propia.

En la imagen se puede observar que la interconexión se da entre el router 1 (a partir de ahora ROTI) y el router 2 (a partir de ahora RCAD); siendo el router que los conecta la simulación de Internet, por lo tanto se define dónde debe darse la configuración del túnel IPsec. Además de ello, se asigna al router 1 la red de la OTI y al router 2 la red de las coordinaciones académicas de las 19 facultades de ésta institución. En la Tabla N° 3 se detalla el direccionamiento IP real de nuestra VPN.

Dispositivo	**Interfaz**	**Dirección IP**	**Máscara**	**Gateway**	**Puerto Switch**
ROTI	Gig0/1	172.30.8.1	255.255.252.0	N/A	S1 Fa0/1

Continúa…

	S0/0/0 (DCE)	10.5.5.1	255.255.255.240	N/A	N/A
RNET	S0/0/0	10.5.5.2	255.255.255.240	N/A	N/A
	S0/0/1 (DCE)	10.10.10.2	255.255.255.240	N/A	N/A
RCAD	Gig0/1	172.30.28.1	255.255.252.0	N/A	S3 Fa0/1
	S0/0/1	10.10.10.1	255.255.255.240	N/A	N/A
PC Administrador de Red	NIC	172.30.8.20	255.255.252.0	172.30.8.1	S1 Fa0/24
Servidor OTI	NIC	172.30.8.30	255.255.252.0	172.30.8.1	S1 Fa0/2
PC FIMEES	NIC	172.30.28.30	255.255.252.0	172.30.28.1	S3 Fa0/2
PC Fac. Ciencias Biológicas	NIC	172.30.28.31	255.255.252.0	172.30.28.1	S3 Fa0/3

Continúa…

PC Fac. Ciencias de la Salud	NIC	172.30.28.32	255.255.252.0	172.30.28.1	S3 Fa0/4
PC Fac. de Enfermería	NIC	172.30.28.33	255.255.252.0	172.30.28.1	S3 Fa0/5
PC Fac. Medicina Humana	NIC	172.30.28.34	255.255.252.0	172.30.28.1	S3 Fa0/6
PC Fac. Medicina Veterinaria y Zootecnia	NIC	172.30.28.35	255.255.252.0	172.30.28.1	S3 Fa0/7
PC Fac. Ciencias Agrarias	NIC	172.30.28.36	255.255.252.0	172.30.28.1	S3 Fa0/8
PC Fac. Ing. Agrícola	NIC	172.30.28.37	255.255.252.0	172.30.28.1	S3 Fa0/9
PC Fac. Ing. Civil y Arquitectura	NIC	172.30.28.38	255.255.252.0	172.30.28.1	S3 Fa0/10

Continúa…

PC Fac. Ing. Económica	NIC	172.30.28.39	255.255.252.0	172.30.28.1	S3 Fa0/11
PC Fac. Ing. Estadística	NIC	172.30.28.40	255.255.252.0	172.30.28.1	S3 Fa0/12
PC Fac. Ing. Geológica y Metalúrgica	NIC	172.30.28.41	255.255.252.0	172.30.28.1	S3 Fa0/13
PC Fac. Ing. Minas	NIC	172.30.28.42	255.255.252.0	172.30.28.1	S3 Fa0/14
PC Fac. Ing. Química	NIC	172.30.28.43	255.255.252.0	172.30.28.1	S3 Fa0/15
PC Fac. Cs. Contables y Administrativas	NIC	172.30.28.44	255.255.252.0	172.30.28.1	S3 Fa0/16
PC Fac. Cs. de la Educación	NIC	172.30.28.45	255.255.252.0	172.30.28.1	S3 Fa0/17
PC Fac. Cs. Jurídicas y Políticas	NIC	172.30.28.46	255.255.252.0	172.30.28.1	S3 Fa0/18

Continúa…

PC Fac. Cs. Sociales	NIC	172.30.28.47	255.255.252.0	172.30.28.1	S3 Fa0/19
PC Fac. Trabajo Social	NIC	172.30.28.48	255.255.252.0	172.30.28.1	S3 Fa0/20

Tabla N° 3: Tabla de Direccionamiento IP Real en base a modelo CISCO.

Elaboración: Propia.

Ahora, para fines de entendimiento se tiene que diseñar una topología simplificada que permita visualizar el prototipo claramente, además de colaborar con la implementación práctica del mismo. De ésta manera se diseña la siguiente topología:

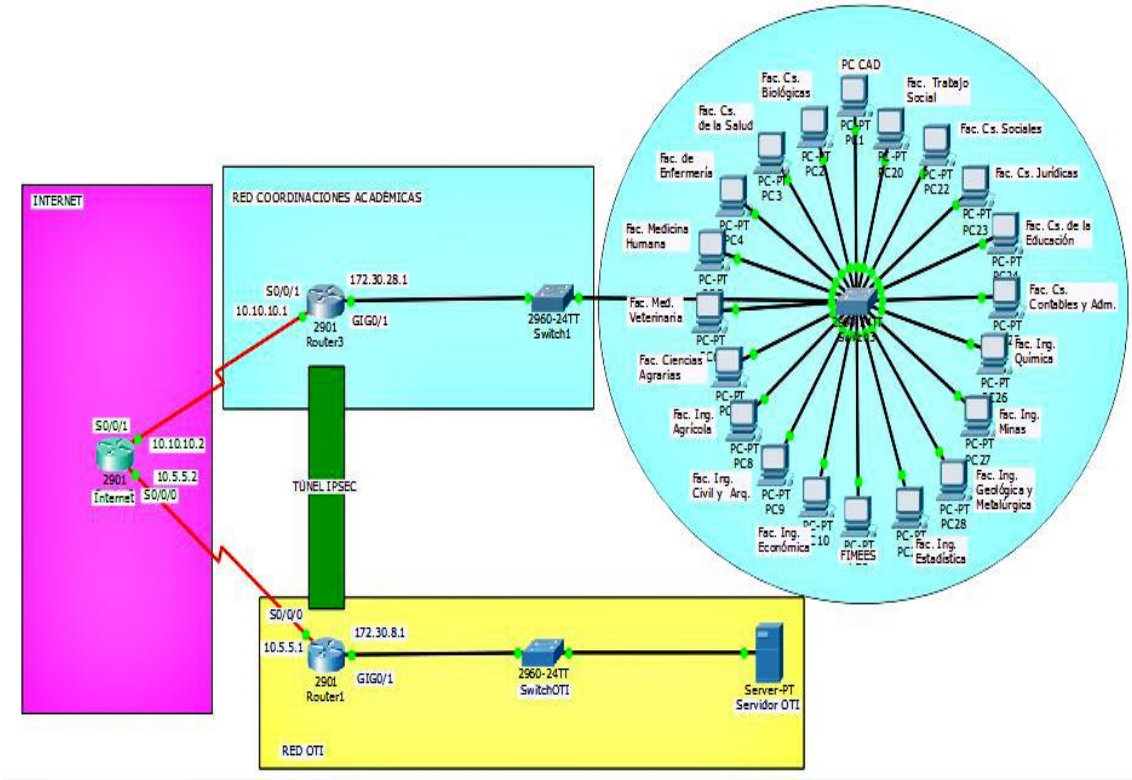


Figura 35: Topología a usar para prototipo de VPN en Software Packet Tracer 7.0.

Elaboración: Propia.

En la imagen se observa el diseño completo de la topología del prototipo de la VPN con sus conexiones, así como lo rangos de las direcciones IP con las que trabajaran y las nomenclaturas con las que se reconocerá cada dispositivo. Esta topología será utilizada tanto en la simulación como en la implementación de la VPN.

3.6.2. Direccionamiento IP mediante comandos en los enrutadores.

Para configurar las direcciones IP se realizó una tabla de direccionamiento; esta tabla facilitará la guía en la configuración de las interfaces, el enrutamiento dinámico, así como en las configuraciones posteriores de la VPN, tanto en las ACLs como en el crypto MAP y demás. La tabla de direccionamiento está diseñada de la siguiente manera:

Dispositivo	Interfaz	Dirección IP	Máscara	Gateway	Puerto Switch
ROTI	GIG0/1	172.30.8.1	255.255.252.0	N/A	S1 Fa0/1
	S0/0/0 (DCE)	10.5.5.1	255.255.255.240	N/A	N/A
RNET	S0/0/0	10.5.5.2	255.255.255.240	N/A	N/A
	S0/0/1 (DCE)	10.10.10.2	255.255.255.240	N/A	N/A
RCAD	GIG0/1	172.30.28.1	255.255.252.0	N/A	S3 Fa0/1
	S0/0/1	10.10.10.1	255.255.255.240	N/A	N/A

Continúa…

SERVIDOR OTI	NIC	172.30.8.30	255.255.252.0	172.30.8.1	S1 Fa0/2
PC-CAD	NIC	172.30.28.30	255.255.252.0	172.30.28.1	S3 Fa0/2

Tabla N° 4: Tabla de Direccionamiento IP de Prototipo en base a modelo CISCO.

Elaboración: Propia.

3.6.3. Tipo de enrutamiento

En este caso el enrutamiento es dinámico, donde la programación implementada fue:

a. En ROTI:

ROTI(config)# router ospf 101

ROTI(config-router)# network 172.30.8.0 0.0.3.255 area 0

ROTI(config-router)# network 10.5.5.0 0.0.0.15 area 0

b. En RNET:

RNET(config)# router ospf 101

RNET(config-router)# network 10.5.5.0 0.0.0.15 area 0

RNET(config-router)# network 10.10.10.0 0.0.0.15 area 0

c. En RCAD:

RCAD(config)# router ospf 101

RCAD(config-router)# network 172.30.28.0 0.0.3.255 area 0

RCAD(config-router)# network 10.10.10.0 0.0.0.15 area 0

3.6.4. Direccionamiento IP de PCs y análisis de conectividad de subredes

El procedimiento en el 'Servidor OTI' como en la 'PC-CAD' es el mismo, se configura una dirección IP estática, una máscara de subred y una puerta de enlace predeterminada, como se muestra en la Tabla de Direccionamiento.

Luego, para verificar la conectividad de la red, se procede con emitir el comando 'ping' entre los 02 puntos como se muestra en las siguientes imágenes.

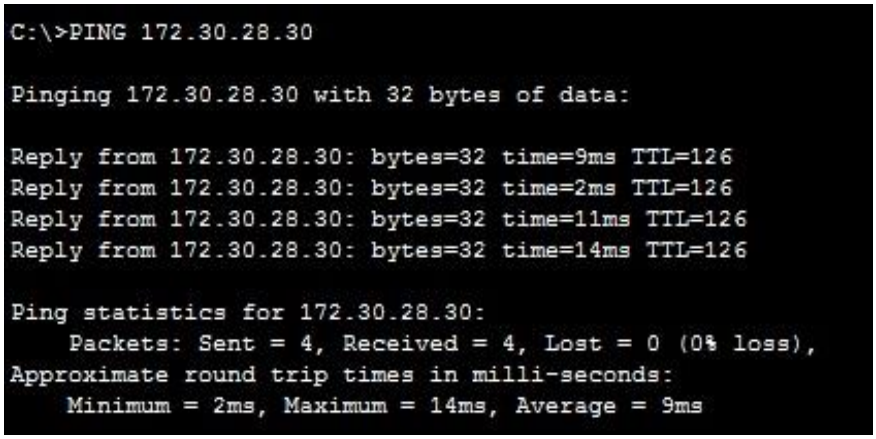


Figura 36: Ping 'Servidor OTI' a 'PC-CAD' (Captura de pantalla).

Elaboración: Propia.

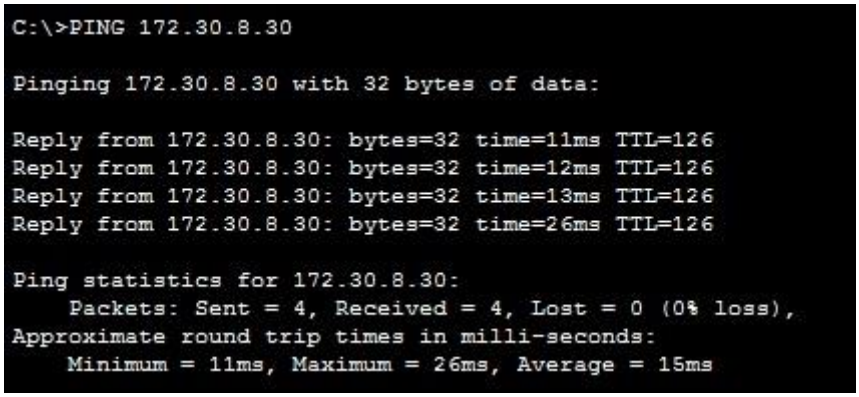


Figura 37: Ping 'PC-CAD' a 'Servidor OTI' (Captura de pantalla).

Elaboración: Propia.

De esta manera se comprueba que existe conectividad entre ambos puntos por consiguiente, queda demostrado que el protocolo de enrutamiento OSPF está configurado y funciona correctamente.

Adicionalmente, se configuró el comando '**security passwords min-length**' para establecer una longitud mínima de caracteres en las contraseñas que se coloquen para asegurar la red; tanto en la simulación como en la implementación la cantidad mínima que se configuró fue de 10 caracteres.

Con fines prácticos, se asignó la contraseña '*vpnosicapa3con*' para la línea de consola y 'vpnosicapa3vty' para la línea vty. Además se introdujo el comando '**service password-encryption**' para encriptar las contraseñas anteriormente colocadas

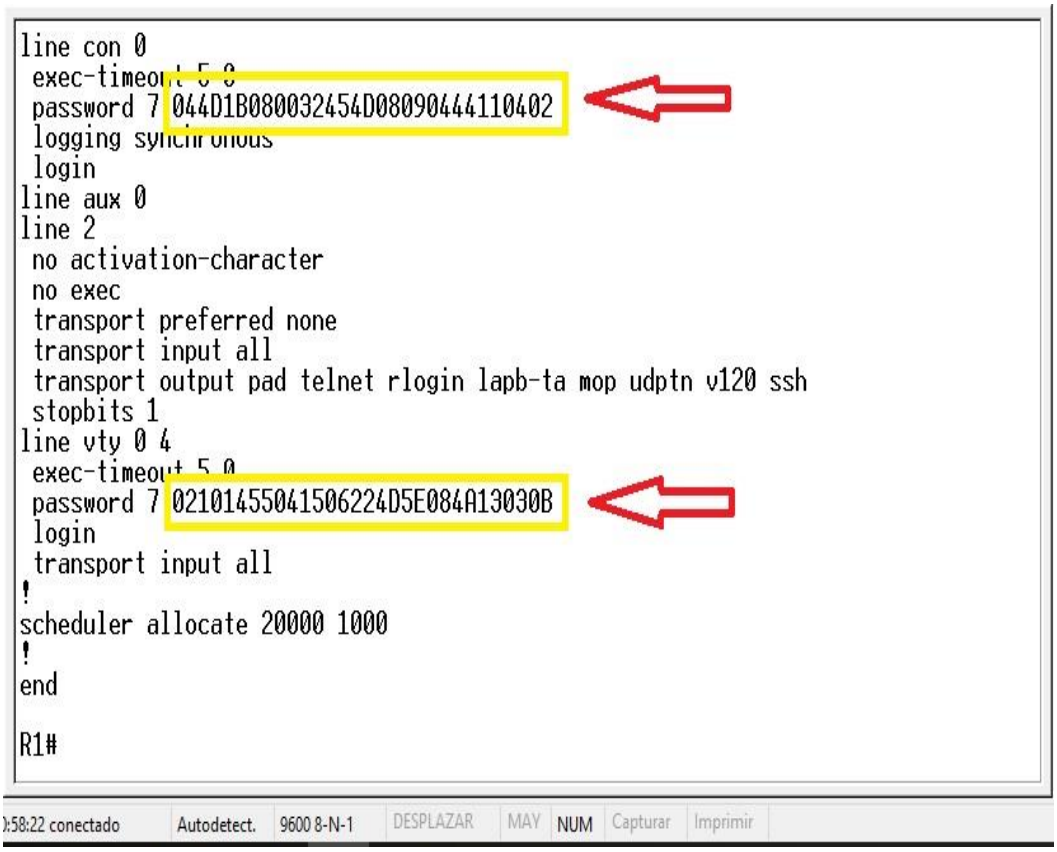


Figura 38: Contraseñas encriptadas con comando 'service password-encription' (Captura de pantalla).

Elaboración: Propia.

3.6.5. Habilitación y verificación de políticas de seguridad en la VPN site-to-site utilizando la interface de comandos de Cisco IOS:

Habiendo verificado en la primera parte la conexión entre las PCs, procedimos con la habilitación de la política IKE en ROTI y RCAD, necesaria para toda la configuración IPsec.

Verificamos que IKE está habilitada:

ROTI(config)# crypto isakmp enable

RCAD(config)# crypto isakmp enable

En nuestra experiencia, tanto en la simulación como en la implementación, se tuvo dificultades para activar IKE en los routers, debido a que si bien se sabe que dichos routers si soportan la política de seguridad, estas políticas no vienen activadas por defecto; en consecuencia se tuvo que emitir el comando de configuración que las activara y así poder continuar con el desarrollo de la investigación.

El comando que se utilizó en los routers fue el siguiente:

ROTI(config)# license boot module c2900 technology-package securityk9

RCAD(config)# license boot module c2900 technology-package securityk9

En la siguiente imagen se muestra una captura real del error así como la aplicación del comando de activación de las políticas de seguridad.

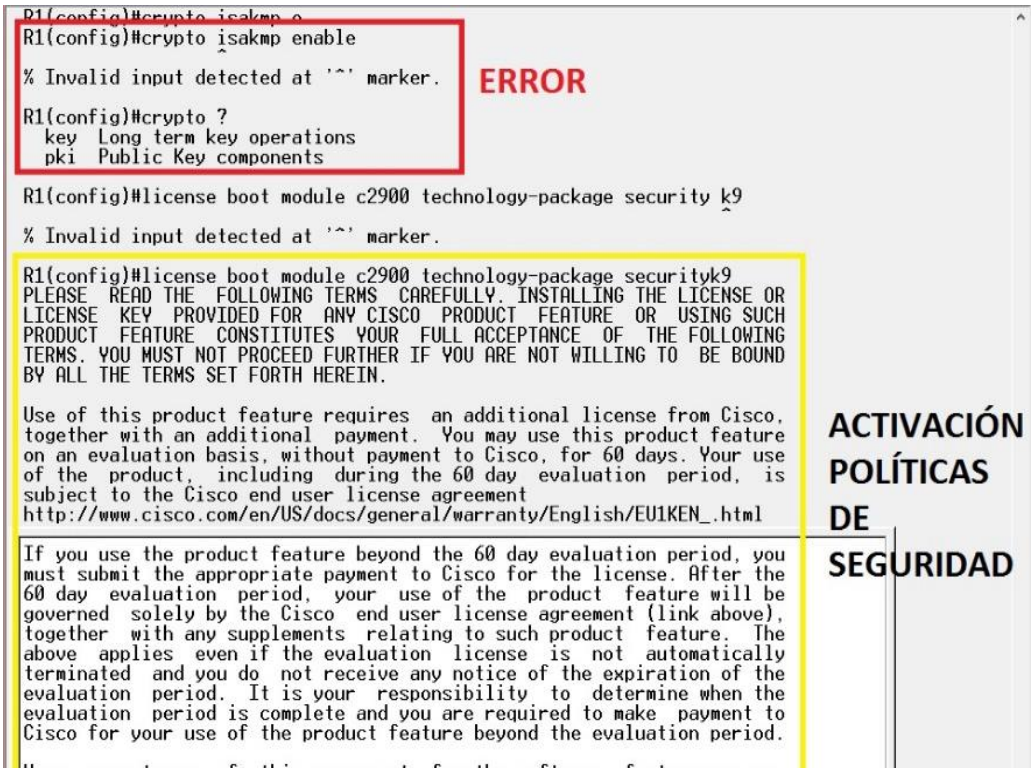


Figura 39: Activación de protocolo ISAKMP (Captura de pantalla).

Elaboración: Propia.

Para realizar este procedimiento se emite el comando:

ROTI(config)# crypto isakmp policy 10

3.6.6. Agrupación de parámetros ISAKMP utilizados en ROTI y RCAD

Entonces, los protocolos utilizados para la configuración de ISAKMP se definieron de la siguiente manera: Configuramos una directiva ISAKMP con una prioridad de 10, Se utilizó la clave precompartida (psk) como tipo de autenticación, aes 256 para el algoritmo de cifrado, ‘sha’ como el algoritmo hash y el intercambio de claves del grupo 5 de Diffie-Hellman. Además se dio a la directiva una vida útil de 3600 segundos (una hora). Todo esto aplicado a los routers ROTI y RCAD.

ROTI(config)# crypto isakmp policy 10

ROTI(config-isakmp)# authentication pre-share

ROTI(config-isakmp)# encryption aes 256

ROTI(config-isakmp)# hash sha

ROTI(config-isakmp)# group 5

ROTI(config-isakmp)# lifetime 3600

ROTI(config-isakmp)# end

RCAD(config)# crypto isakmp policy 10

RCAD(config-isakmp)# authentication pre-share

RCAD(config-isakmp)# encryption aes 256

RCAD(config-isakmp)# hash sha

RCAD(config-isakmp)# group 5

RCAD(config-isakmp)# lifetime 3600

RCAD(config-isakmp)# end

Para verificar IKE se emite el comando "**show crypto isakmp policy**" en los routers anteriormente mencionados, este comando nos muestra si la configuración fue emitida correctamente, en la imagen siguiente se puede apreciar la captura real de la emisión del comando con la configuración realizada.

```
R1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys
).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               3600 seconds, no volume limit
```

Figura 40: Verificación de política IKE (Captura de pantalla).

Elaboración: Propia.

3.6.7. Asociación de Clave Precompartida (PSK)

Identificamos entonces que las direcciones IP deben ser en ROTI 10.5.5.1 por la interfaz S0/0/0 y en RCAD 10.10.10.1 por la interfaz S0/0/1. Estas son las direcciones que se utilizan para enviar el tráfico normal entre ROTI y RCAD.

Para fines prácticos se configuró la clave pre-compartida como ‘vpnuna123’ en los router ROTI y RCAD. Las redes de producción o empresariales deben utilizar una clave mucho más compleja. De los comandos que se muestran a continuación, el primero apunta a la dirección IP remota de RCAD en su interfaz S0/0/1 y el segundo apunta a la dirección IP remota de ROTI en su interfaz S0/0/0.

ROTI(config)# crypto isakmp key vpnuna123 address 10.10.10.1

RCAD(config)# crypto isakmp key vpnuna123 address 10.5.5.1

3.6.8. Determinación de tiempo de vida útil de SA para el set de transformaciones IPsec

Se emitieron los comandos:

ROTI(config)# crypto IPsec transform-set 50 esp-aes 256 esp-sha-hmac

ROTI(cfg-crypto-trans)# exit

RCAD(config)# crypto IPsec transform-set 50 esp-aes 256 esp-sha-hmac

RCAD(cfg-crypto-trans)# exit

También se cambió los tiempos de vida de la asociación de seguridad (SA) IPsec donde su valor predeterminado es de 3600 segundos. En ROTI y RCAD, se estableció el tiempo de vida de la SA de IPsec en 30 minutos o 1800 segundos

3.6.9. Identificación del tráfico de interés de la VPN

En nuestra investigación, el tráfico que se desea encriptar es el tráfico que va de la LAN Ethernet de ROTI a la LAN Ethernet de RCAD y viceversa. Estas listas de acceso se utilizan como salida en las interfaces del punto de llegada de la VPN y deben reflejarse entre sí. Es así que se configuraron las ACLs de tráfico de interés en IPsec de la VPN en ROTI y RCAD de la siguiente manera:

ROTI(config)# access-list 101 permit ip 172.30.8.0 0.0.3.255 172.30.28.0 0.0.3.255

RCAD(config)# access-list 101 permit ip 172.30.28.0 0.0.3.255 172.30.8.0 0.0.3.255

3.6.10. Programación de Mapa de encriptación aplicando el tráfico de interés identificado

Para la programación del Crypto Map realizamos:

ROTI(config)# crypto map CMAP 10 IPsec-isakmp

ROTI(config-crypto-map)# match address 101

ROTI(config-crypto-map)# set peer 10.10.10.1

ROTI(config-crypto-map)# set pfs group5

ROTI(config-crypto-map)# set transform-set 50

ROTI(config-crypto-map)# set security-association lifetime seconds 900

ROTI(config-crypto-map)# exit

Al crear el Crypto Map reflejado en RCAD, solo queda aplicar el mismo a las interfaces ya que las SAs no serán establecidas hasta que el Crypto Map sea activado en el tráfico de interés. Para ello será activado en las interfaces s0/0/0 de ROTI y s0/0/1 de RCAD.

3.6.11. Comprobación de la programación de IPsec y el mapa criptográfico

Utilizando el comando: "**show crypto IPsec transform-set"** desglosa la configuración de IPsec en forma de sets de transformación.

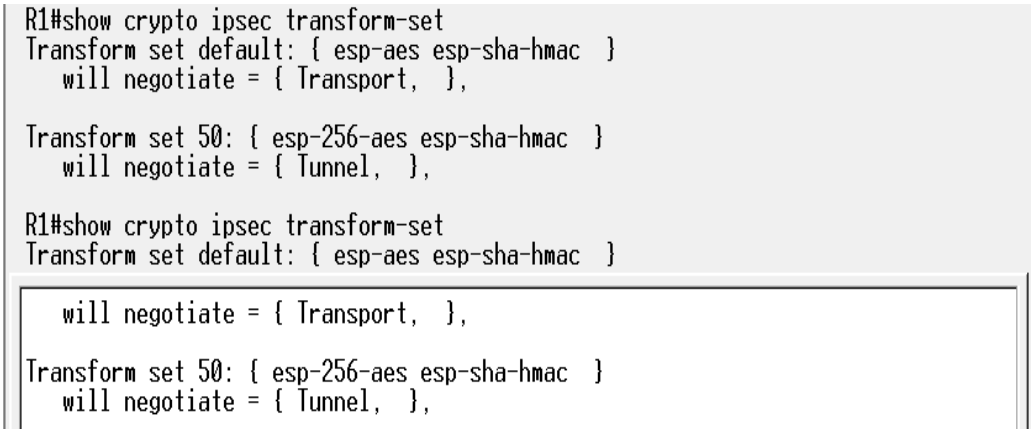


Figura 41: Muestra de configuración IPsec programada en router (Captura de pantalla).

Elaboración: Propia.

Luego, el comando '**show crypto map**' muestra los Crypto Map aplicados en los routers.

```
ROTI#show crypto map
Crypto Map CMAP 10 ipsec-isakmp
        Peer = 10.10.10.1
        Extended IP access list 101
            access-list 101 permit ip 172.30.8.0 0.0.3.255
172.30.28.0 0.0.3.255
        Current peer: 10.10.10.1
        Security association lifetime: 4608000 kilobytes/900
seconds
        PFS (Y/N): Y
        Transform sets={
                50,
        }
        Interfaces using crypto map CMAP:
                Serial0/0/0
```

Figura 42: Muestra de crypto Map creado en router (Captura de pantalla).

Elaboración: Propia.

3.6.12. Configuración de la VPN con Cisco Configuring Professional

Se siguieron los siguientes pasos para la implementación con interfaz virtual:

3.6.12.1. Programación de la VPN con IPsec en ROTI utilizando CCP

Para fines de prueba se colocó ‘adminOTI’ como nombre de usuario y ‘unap123456’ como contraseña de la siguiente manera:

ROTI(config)# username adminOTI privilege 15 secret cisco123456

RCAD(config)# username adminOTI privilege 15 secret cisco123456

Luego de esto se habilitó el acceso HTTP en los routers con los siguientes comandos:

ROTI(config)#ip http secure-server

RCAD(config)#ip http secure-server

Por último se configuró la autenticación de la base de datos local de sesiones web para admitir la conectividad a CCP.

ROTI(config)# ip http authentication local

RCAD(config)# ip http authentication local

De esta manera se procede a abrir el software CCP para configurar la VPN con IPsec en ROTI.

Ejecutamos la aplicación CCP y empezamos a llenar los campos requeridos. Aquí mostramos algunas capturas de pantalla del proceso realizado.

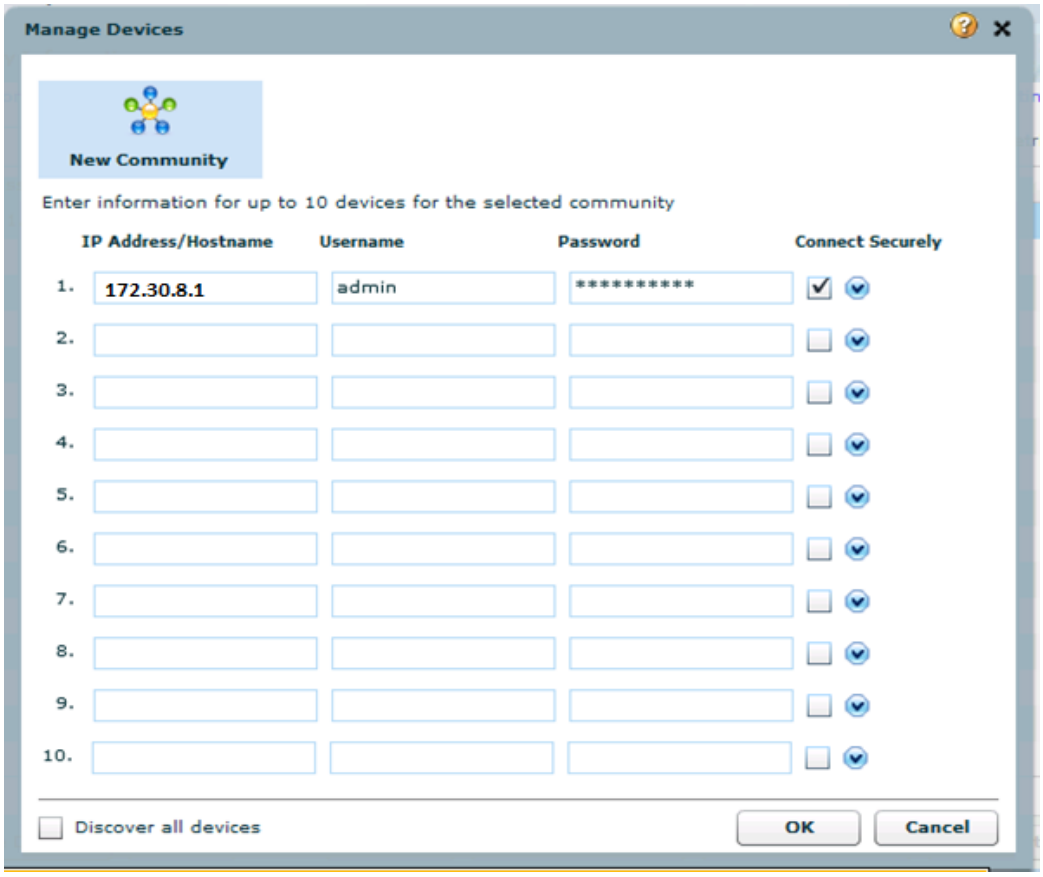


Figura 43: Ventana de administración de los dispositivos – CCP (Captura de pantalla).

Elaboración: Propia.

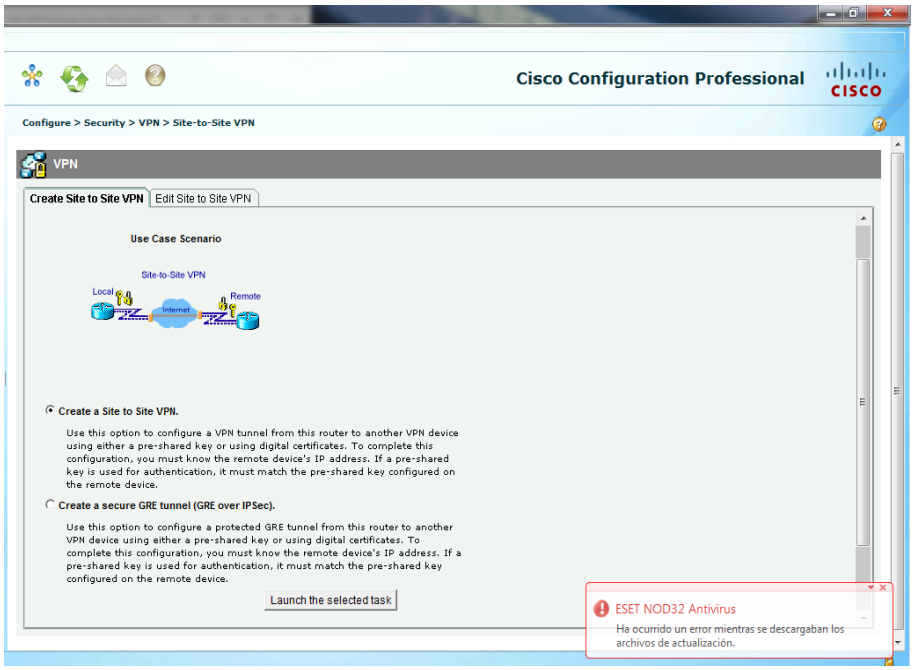


Figura 44: CCP sitio a sitio con VPN Wizard (Captura de pantalla).

Elaboración: Propia.

Fijamos las encriptaciones:

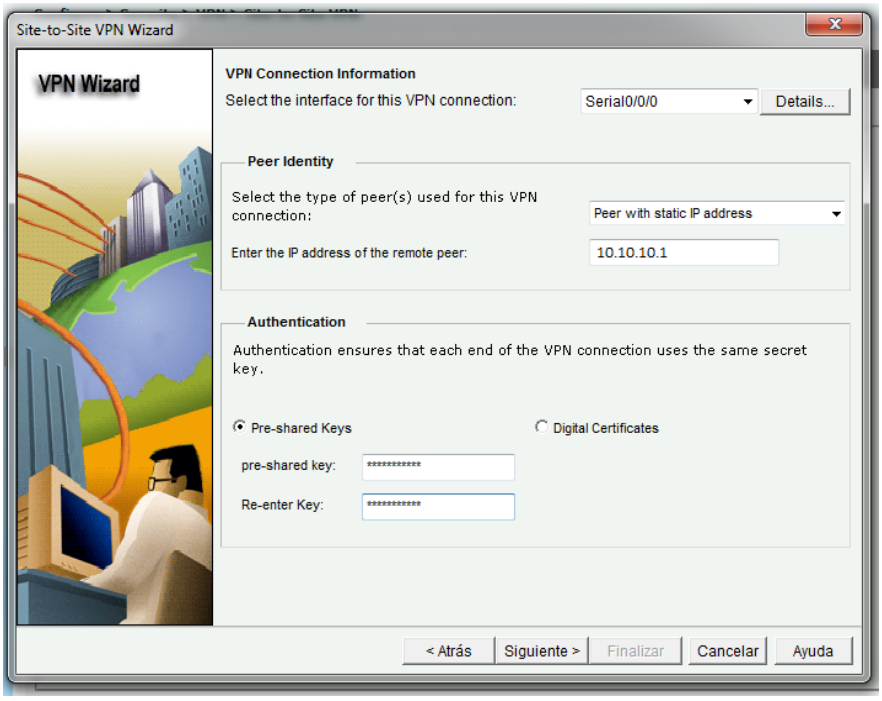


Figura 45: CCP VPN Información sobre la conexión (Captura de pantalla).

Elaboración: Propia.

Configuramos las políticas IKE:

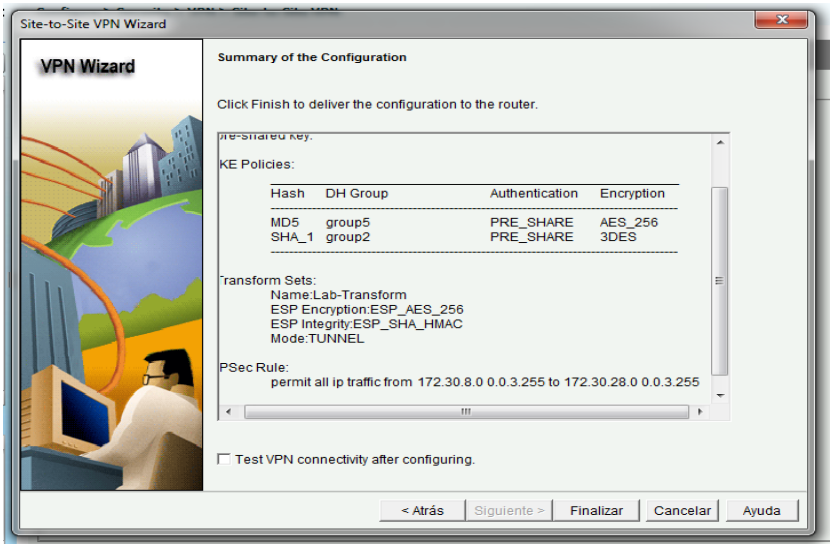


Figura 46: CCP Agrupación de configuraciones (Captura de pantalla).

Elaboración: Propia.

Al dar click en 'Finish' emergerá una ventana, daremos click en 'Deliver' y cuando termine de cargar presionaremos 'OK', de esta forma ROTI quedará configurado.

3.6.12.2. Programación de interfaces espejo para RCAD

Configuramos RCAD con ayuda de las siguientes interfaces:

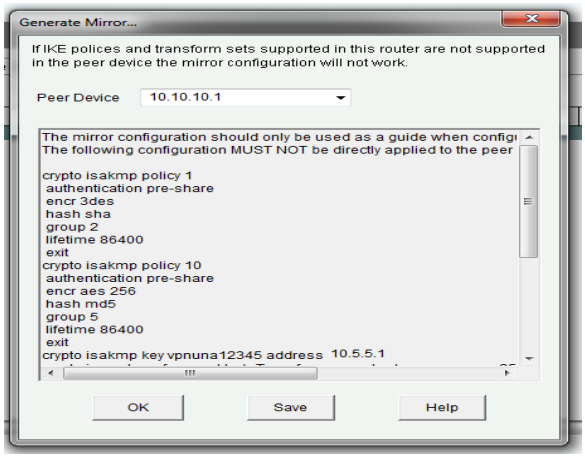


Figura 47: CCP VPN configuración de espejo (Captura de pantalla).

Elaboración: Propia.

Copiaremos esta configuración en un documento de texto y la guardaremos para pegarla en el Cisco IOS CLI del RCAD. Una vez copiada la configuración, aplicaremos el Crypto Map a la interfaz S0/0/1 de RCAD con el siguiente comando:

RCAD(config)# interface S0/0/1

RCAD(config-if)# crypto map SDM_CMAP_1

3.6.12.3. Verificación de la VPN utilizando CCP en ROTI

Para realizar la prueba de la VPN se debe acceder a: Security > VPN > Site-to-Site VPN, luego abrir la pestaña 'Edit Site-to-Site VPN' y dar click en 'Test Tunnel'.

Cuando la ventana llamada 'VPN TroubleShootting' emerja presionaremos Start.

En este procedimiento aparecerá una ventana de Aviso indicando que CCP habilitará las depuraciones del router y generará cierto tráfico en el túnel, haremos clic en YES para continuar.

En la siguiente ventana de 'VPN TroubleShootting', la dirección IP de la interfaz G0/1 de ROTI en la red de origen se muestra de forma predeterminada (172.30.8.1).

Introducimos la dirección IP de la interfaz G0/1 de RCAD en el campo de red de destino (172.30.28.1) y daremos click en 'Continue' para comenzar el proceso.

Como se aprecia en la siguiente imagen la conexión del túnel está activada, por lo tanto se concluye que nuestra VPN está en funcionamiento.

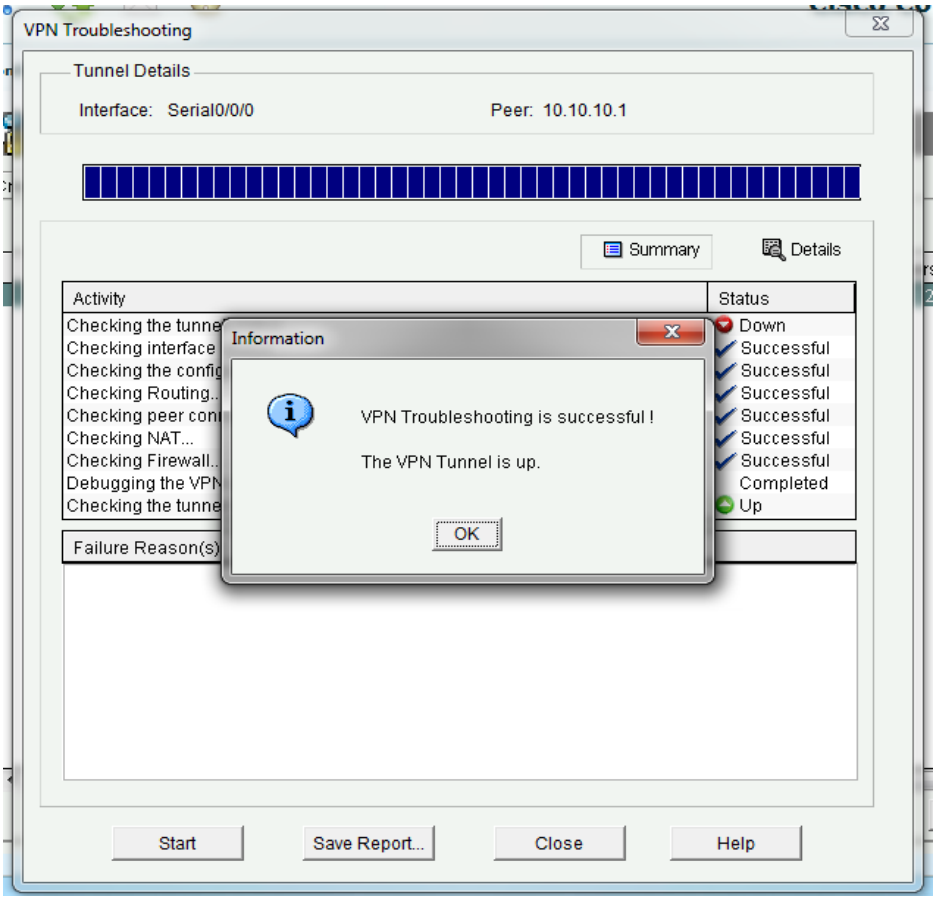


Figura 48: CCP Verificación de funcionamiento de VPN (Captura de pantalla).

Elaboración: Propia.

3.6.13. Programación de un servidor y un usuario VPN con acceso remoto.

Como última parte de la investigación, los tesistas propusimos la configuración de un cliente VPN con acceso remoto, esto simplemente como un experimento adicional para capturar los paquetes encriptados y encapsulados directamente y así poder analizarlos con el software WIRESHARK.

La topología que se utilizará será la misma; con una pequeña variación en los puntos de llegada del túnel IPsec.

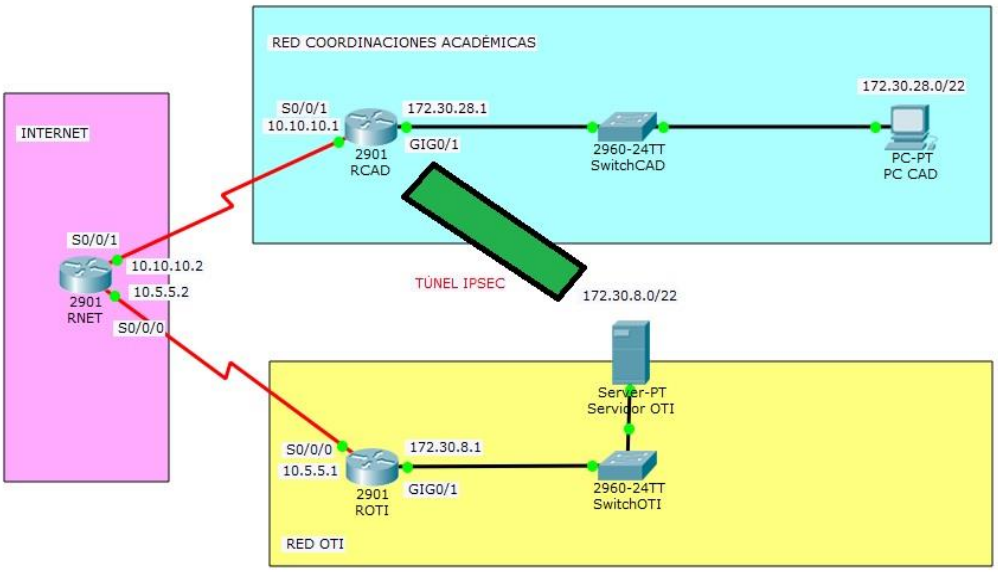


Figura 49: Topología de VPN con acceso remoto con software Packet Tracer 7.0.

Elaboración: Propia.

Esta variación se hace para conectar directamente el servidor como punto de llegada y que los paquetes de datos transmitidos lleguen encriptados hasta el punto final, sin embargo no tiene un efecto significativo en la configuración general de la VPN.

La configuración básica es la misma sin embargo en este caso se hace un enrutamiento estático para apreciar mejor la transmisión de los paquetes de un punto a otro. Para hacer el enrutamiento estático se emitió los siguientes comandos:

ROTI(config)# ip route 0.0.0.0 0.0.0.0 10.5.5.2

ROTI(config)# ip route 0.0.0.0 0.0.0.0 10.10.10.2

En el router RCAD el enrutamiento se configuró de la siguiente manera:

RCAD(config)# ip route 172.30.8.0 255.255.252.0 10.5.5.1

RCAD(config)# ip route 172.30.28.0 255.255.252.0 10.10.10.1

De igual manera se comprueba la conectividad entre los puntos, se activa la seguridad HTTP y se crea una cuenta para poder acceder a CCP y configurar la VPN. En este caso la configuración se realizó en RCAD y se usó ‘adminOTI’ como nombre de usuario y ‘admin01vpn’ como contraseña.

Al acceder a la ventana principal de CCP nos vamos a Configure > Security > Firewall > Firewall para configurar el Firewall de nuestra red, esta configuración se hace debido a la configuración de un acceso remoto.

Una vez abierta la ventana seccionamos la opción ‘Basic Firewall’, y luego damos click en ‘Launch the select task’ para continuar con ‘Siguiente’.

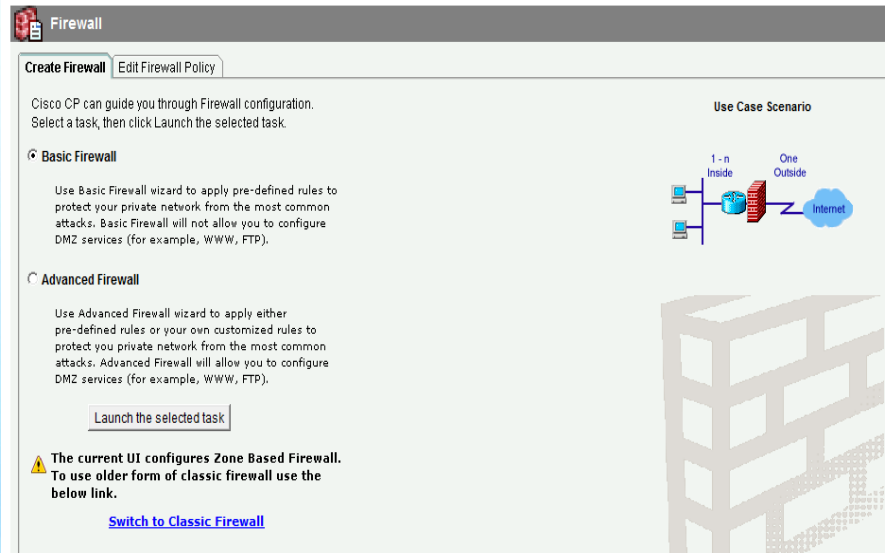


Figura 50: CCP Firewall (Captura de pantalla).

Elaboración: Propia.

Al emerger la pestaña ‘Basic Firewall Interface Configuration’ seleccionaremos ‘Inside (Trusted)’ para la interfaz GigabitEthernet0/1 y ‘Outside (Untrusted)’ para la interfaz Serial0/0/1. En la siguiente ventana seleccionamos ‘Low Segurity’ para el nivel de Seguridad; luego daremos click en ‘Siguiente’ y después en ‘Finish’.

Para enviar los comandos al router daremos click en 'Deliver > OK > OK' y nuestro firewall quedará configurado.

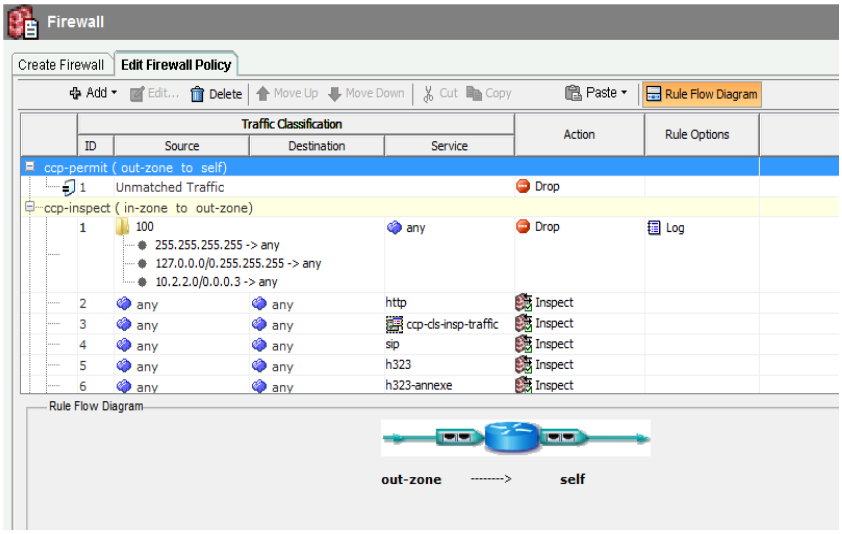


Figura 51: CCP Firewall configurado (Captura de pantalla).

Elaboración: Propia.

Para verificar la funcionalidad de nuestro firewall, se emitió el comando ping a la interfaz S0/0/1 siendo este exitoso; sin embargo al realizar la operación contraria, es decir realizar el ping desde RCAD a la PC-CAD, este no fue exitoso debido a que el ping fue iniciado desde el exterior y fue bloqueado.

3.6.13.1. Aplicación de CCP VPN Wizard para programar el servidor Easy VPN

En el menú de CCP damos click en Configure > Security > VPN > Easy VPN Server, al abrirse la ventana presionaremos 'Launch Easy VPN Server Wizard', nos pide la activación de autenticación y autorización la cual activaremos dando click en OK > Deliver.

Ya estando en la ventana de 'Interface and Authentication' seleccionamos la interfaz en donde termina la conexión del cliente, en este caso seleccionamos la opción 'Unnumbered to' y la interfaz S0/0/1. En el siguiente campo se selecciona la opción 'Pre-shared keys' para el tipo de autenticación y damos click en 'Siguiente'.

En la siguiente ventana 'IKE proposals' damos click en 'Siguiente' para aceptar la directiva IKE por defecto. En la ventana 'Transform Sets' se procede de la misma manera para aceptar los sets de transformación por defecto.

La siguiente ventana configura la autenticación de usuarios de nuestra VPN. Para asegurar la red, debemos permitir el acceso solo a los usuarios con credenciales configuradas en el router, es así que activaremos 'Enable User Authentication' y marcaremos la opción 'Local Only' para que lo anteriormente mencionado se refleje en el acceso remoto a nuestra VPN.

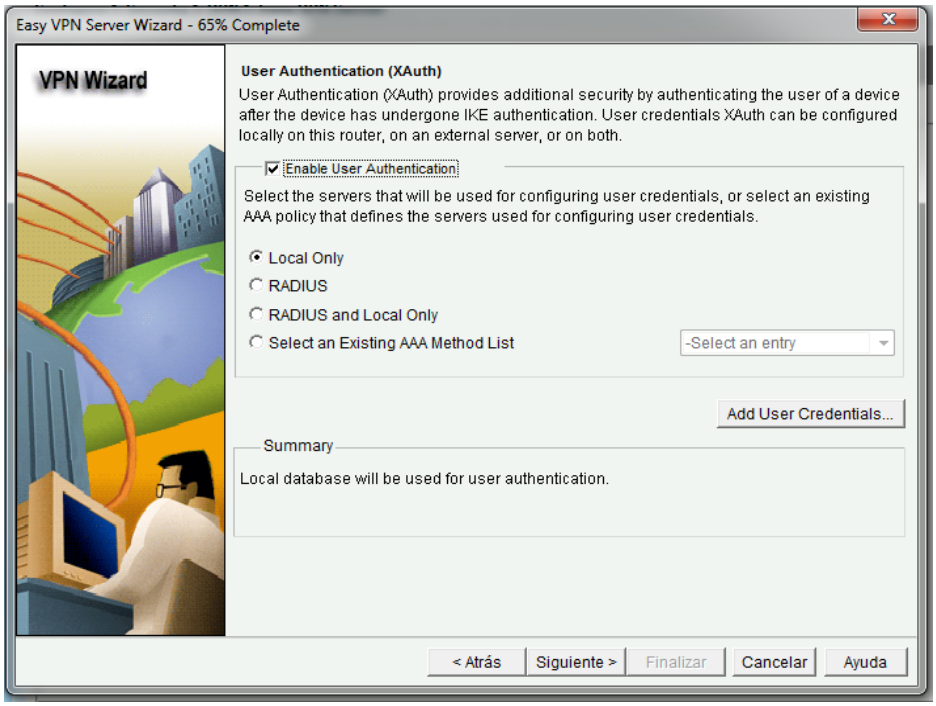


Figura 52: CCP - Configuración de Autenticación de Usuarios (Captura de pantalla).

Elaboración: Propia.

Luego al presionar la pestaña ‘Add User Credentials’ introduciremos la cuenta de prueba para nuestro acceso remoto. Se utilizará ‘VPNuser1’ como nombre de usuario y ‘VPNuser1pass’ como contraseña activando la opción ‘Encrypt password using the MD5 hash algorithm’.

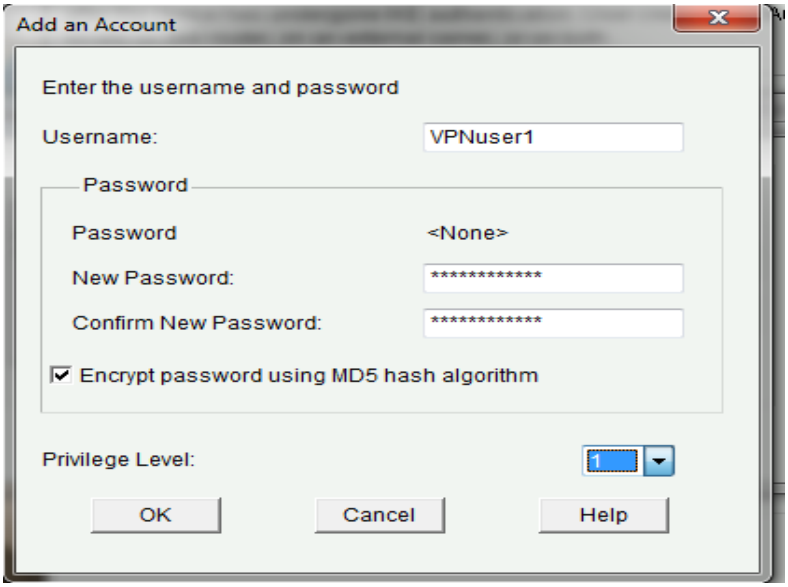


Figura 53: CCP - Usuario VPN agregado (Captura de pantalla).

Elaboración: Propia.

En la ventana ‘Group Authorization and User Group Policies’ debemos crear al menos una directiva de grupo para el servidor VPN. Por consiguiente daremos click en ‘Add’, a continuación en la ventana emergente colocaremos el nombre ‘VPN-Access’ para el grupo y la psk será ‘vpnuna123’; dejaremos activado el check box denominado ‘Pool Information’ y colocaremos como dirección de inicio 172.30.28.100 y como dirección final 172.30.28.150 con una máscara /22. Las máximas conexiones permitidas serán 50, una vez definidos todos los parámetros daremos click en OK.

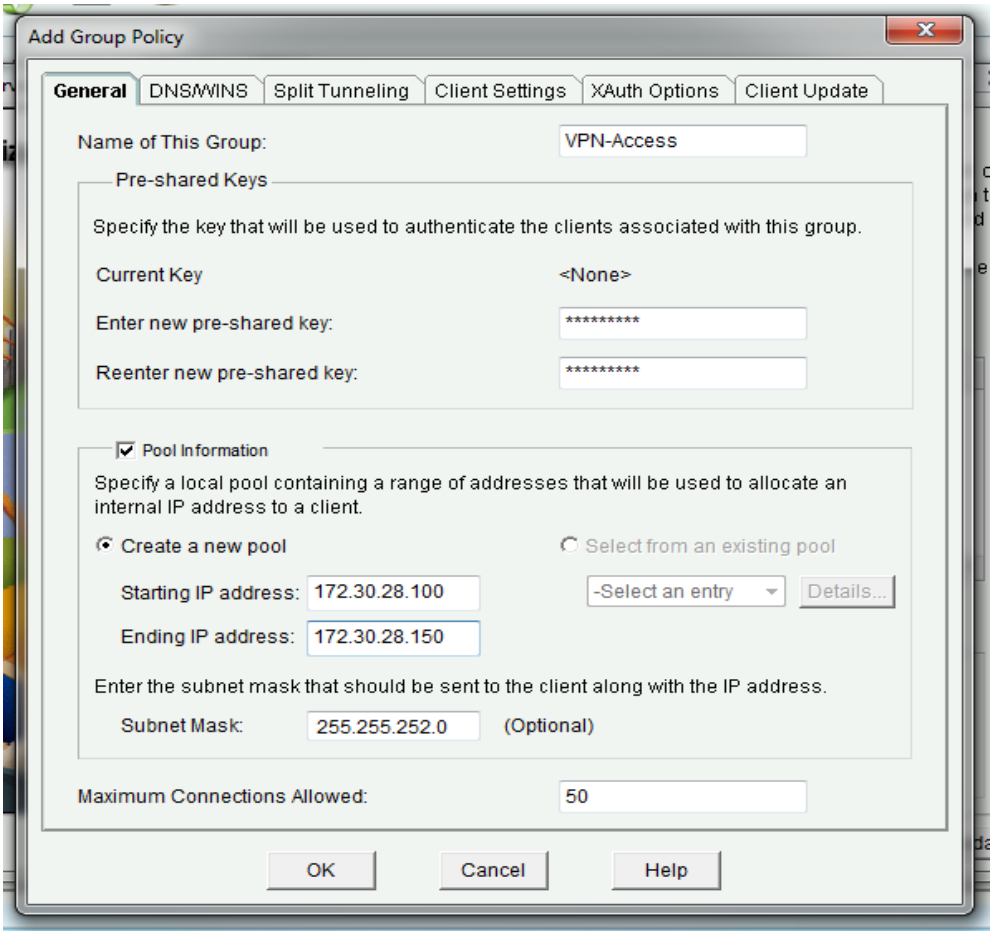


Figura 54: CCP - Autorización de grupos (Captura de pantalla).

Elaboración: Propia.

Al regresar a la ventana de Autorización de Grupos, damos clic en la casilla de verificación 'Configure Idle Timer' e ingresamos una hora (1). Esta configuración sirve para desconectar usuarios inactivos si no hay actividad durante una hora y permite que otros se conecten. Luego damos click en 'Siguiente' para continuar.

Al aparecer la ventana 'Passthrough Configuration', nos aseguramos de que la casilla 'Modify' esté marcada. Esta opción permite a CCP modificar el firewall en S0/0/1 para permitir que el tráfico IPsec VPN alcance la LAN interna. Hacemos click en Aceptar.

Revisamos el resumen de la configuración para entregar los comandos al router.

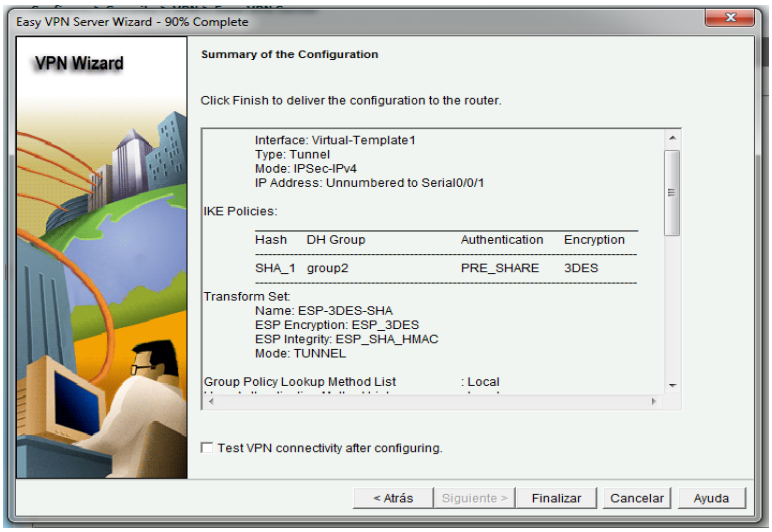


Figura 55: CCP - Resumen de la Configuración (Captura de pantalla).

Elaboración: Propia.

Daremos click en 'Finalizar' y luego en 'Deliver' para enviar la configuración al router; una vez hecho esto verificamos el funcionamiento del servidor VPN.

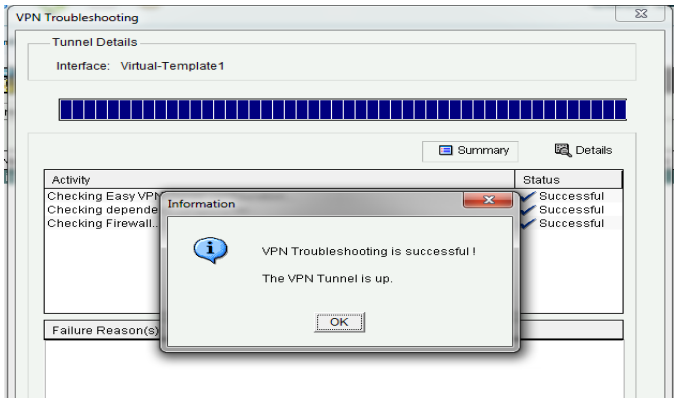


Figura 56: Verificación de operatividad de la VPN (Captura de pantalla).

Elaboración: Propia.

3.6.13.2. Aplicación de VPN Client para testeo de Acceso Remoto a la VPN

Una vez configurado el 'Servidor OTI', abrimos el programa VPN Client, seleccionamos la pestaña 'Connection Entries' y dimos click en 'New'. Introducimos la siguiente información para definir una nueva conexión de entrada:

- Connection Entry: VPN-RCAD
- Description: Conexión a red interna de router RCAD
- Host: 10.10.10.1 (dirección IP de la interfaz S0/0/1 en RCAD)
- Group Authentication Name: VPN-Access
- Password: vpnuna123 (PSK)
- Confirm Password: vpnuna123

Una vez terminada la configuración daremos click en ‘Save’.

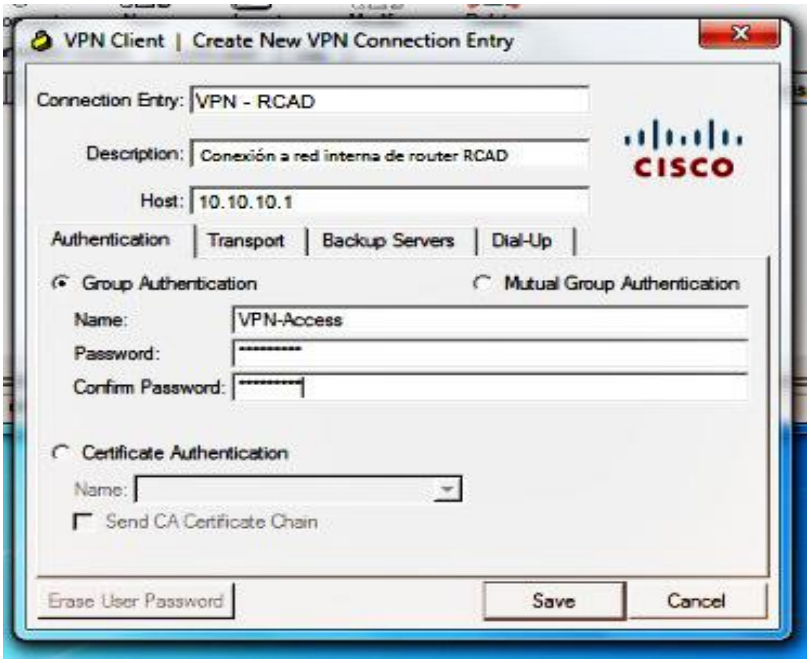


Figura 57: VPN Client - Configuración de nueva conexión (Captura de pantalla).

Elaboración: Propia.

Ahora, seleccionaremos la conexión que apareció en la ventana principal del software y daremos click en ‘Connect’, emergerá una ventana en donde tendremos que colocar la cuenta creada anteriormente con el usuario ‘VPNuser1’ y la contraseña ‘VPNuser1pass’.

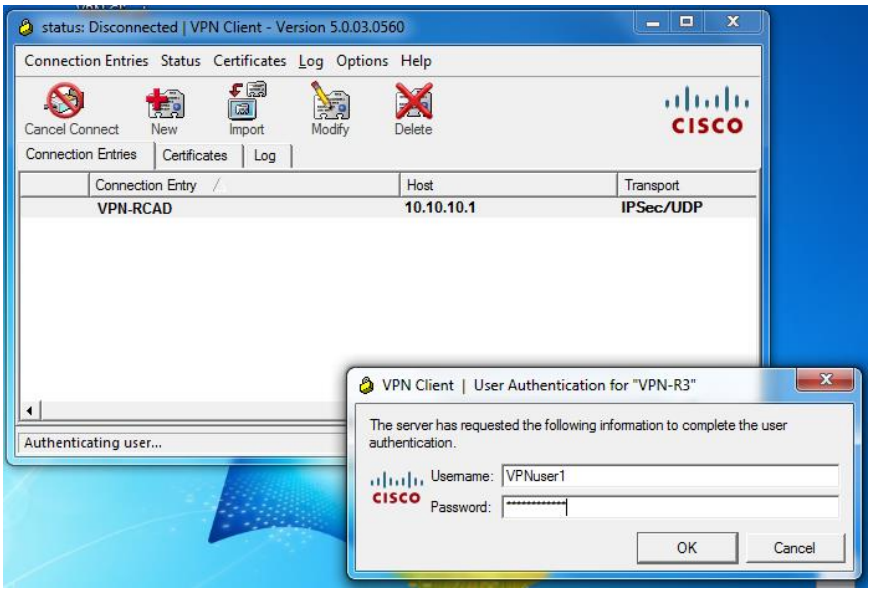


Figura 58: VPN Client - Identificación de cuenta VPN (Captura de pantalla).

Elaboración: Propia.

Al acceder correctamente a la VPN, se activará un icono en la barra de tareas con el símbolo de un candado; este indica la conexión y el acceso remoto a la VPN.

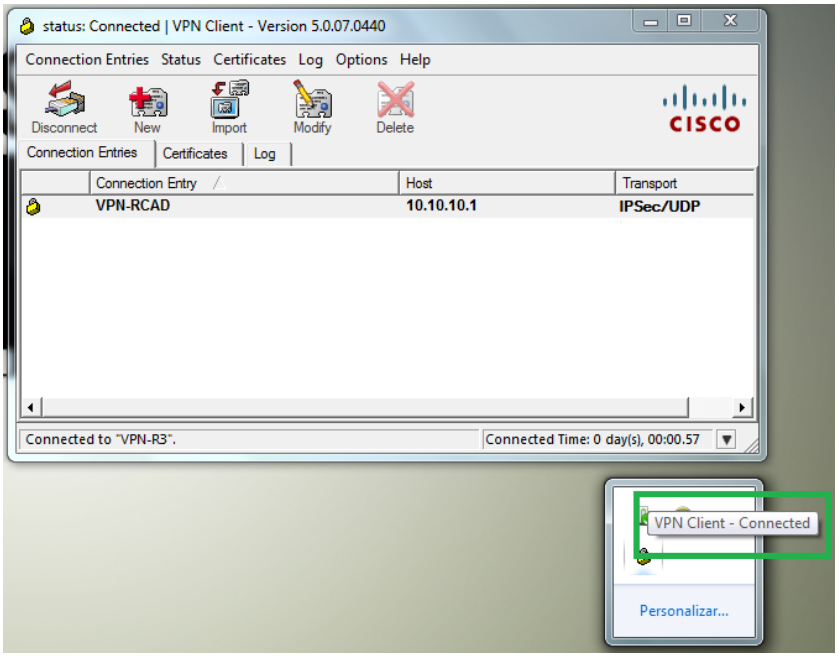


Figura 59: VPN Client - Cliente conectado satisfactoriamente (Captura de pantalla).

Elaboración: Propia.

Para finalizar se comprueba en el análisis de estadísticas de VPN Client que el cliente se conecta por una dirección IP virtual y como último paso se realiza la verificación de conectividad realizando el ping al punto de RCAD.

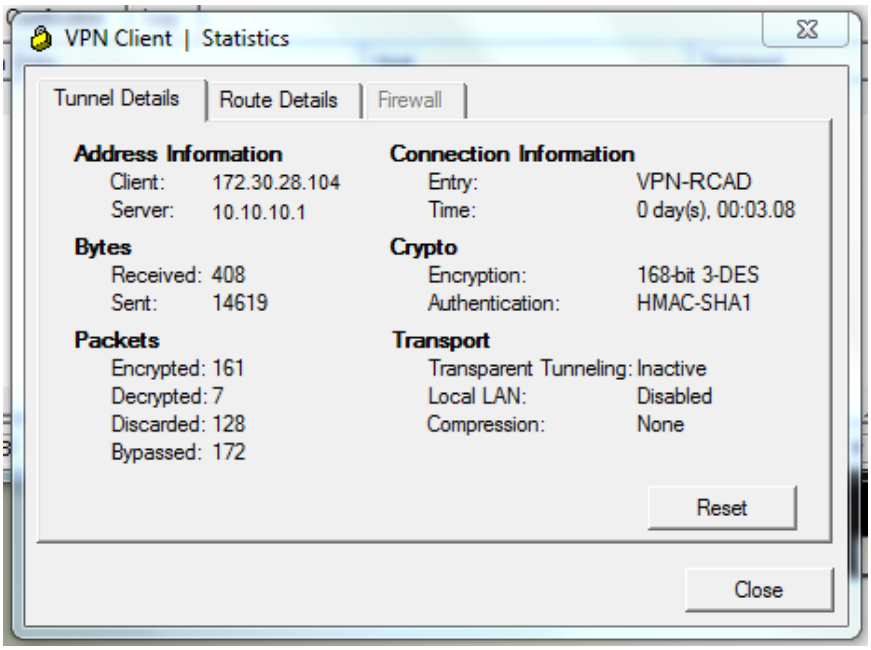


Figura 60: Estadísticas de VPN Client (Captura de pantalla).

Elaboración: Propia.

3.7. PLAN DE TRATAMIENTO DE LOS DATOS

Los datos obtenidos para analizar la configuración y el trabajo de la VPN, se conseguirán a partir de softwares específicos para examinar datos y/o protocolos, así como de la utilización de comandos de programación que permitan visualizar resultados específicos.

Para la recolección de datos principales se siguieron los siguientes pasos:

a) Captura del envío de paquetes entre 02 computadoras a través de la red sin VPN con el software WIRESHARK.
b) Configuración de la VPN utilizando los protocolos determinados correctamente.

c) Emisión del comando ‘show’ para verificar que la programación en los routers es correcta.

d) Captura del envío de paquetes entre las 02 computadoras a través de la red con VPN configurada utilizando el software WIRESHARK.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1. PRUEBA DE CONEXIÓN ENTRE LOS PUNTOS DE LLEGADA DE LA VPN.

Para realizar una prueba simple de conexión entre los dos terminales del túnel IPsec de nuestra VPN, se emitió el comando ‘ping’ y el comando ‘tracert’ desde el ‘SERVIDOR OTI’ a la PC-CAD (de nuestra topología) y viceversa en dos etapas. La primera etapa se efectuó sin la configuración de la VPN y la segunda etapa es desarrollada con la configuración completa de la misma. En la primera etapa con el comando ‘ping’ se comprueba que existe la conexión de los dos puntos debido al enrutamiento dinámico que fue configurado como se muestra en la siguiente imagen.

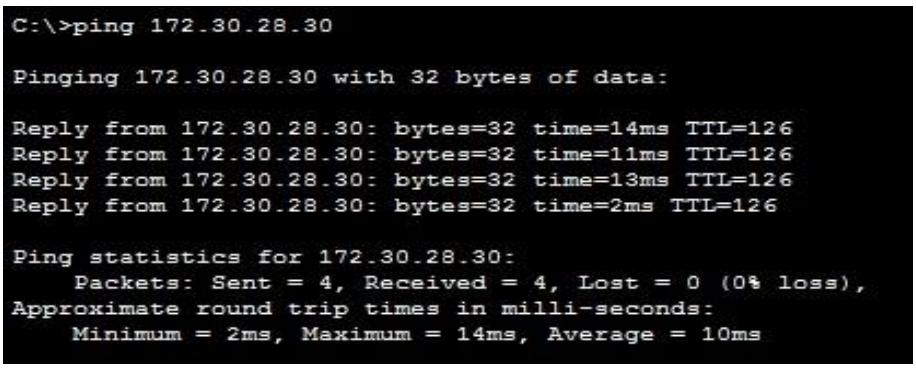


Figura 61: Ping SERVIDOR OTI a PC-CAD sin VPN (Captura de pantalla).

Elaboración: Propia.

Luego con el comando ‘tracert’ se aprecia el camino que llevan los paquetes para llegar a su destino, en este caso observamos que nuestro paquete llegó en 4 saltos hasta el destino.

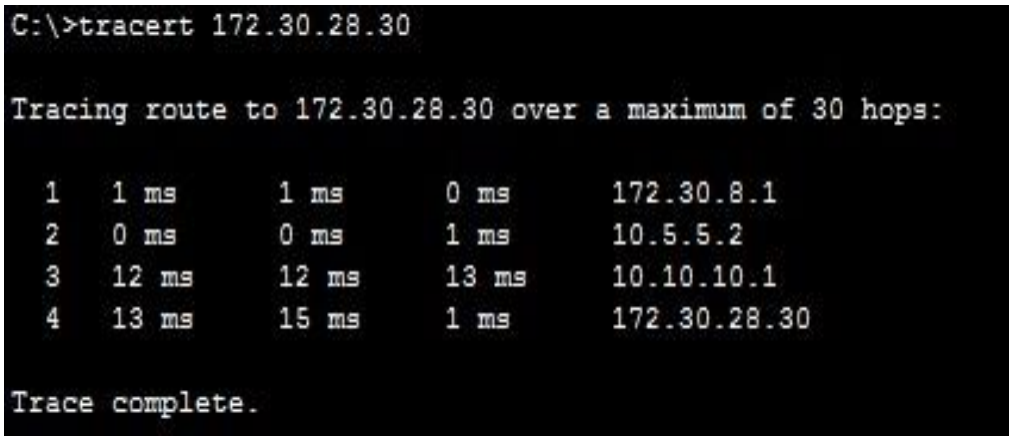


Figura 62: Tracert SERVIDOR OTI a PC-CAD sin VPN (Captura de pantalla).

Elaboración: Propia.

En la segunda etapa también se comprueba la conexión entre los dos puntos con el comando ‘ping’ siendo esta satisfactoria.

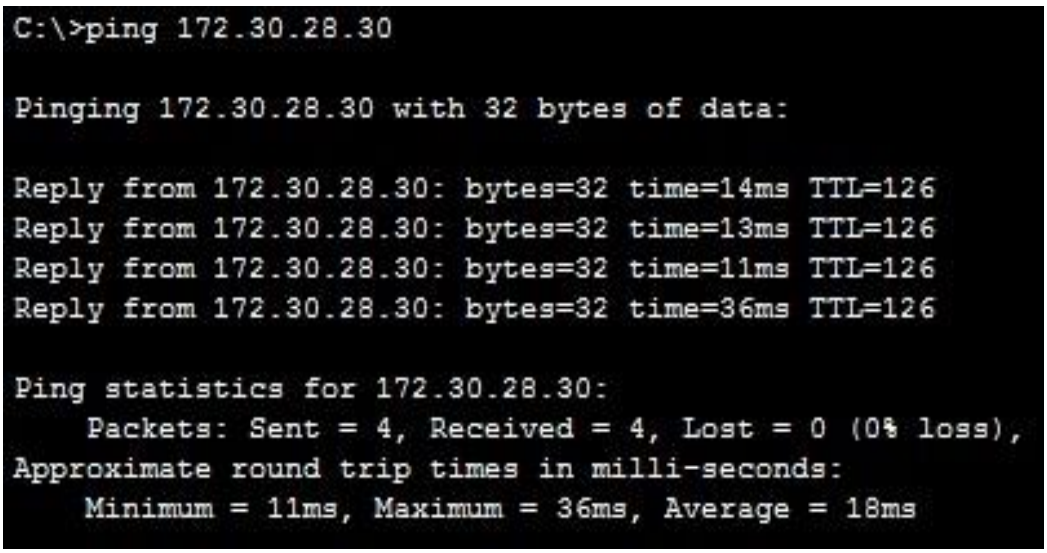


Figura 63: Ping SERVIDOR OTI a PC-CAD con VPN (Captura de pantalla).

Elaboración: Propia.

Sin embargo al emitir el comando ‘tracert’ podemos notar que la cantidad de saltos que utilizaron los paquetes para llegar a su destino se redujo, esto debido a la configuración del túnel IPsec.

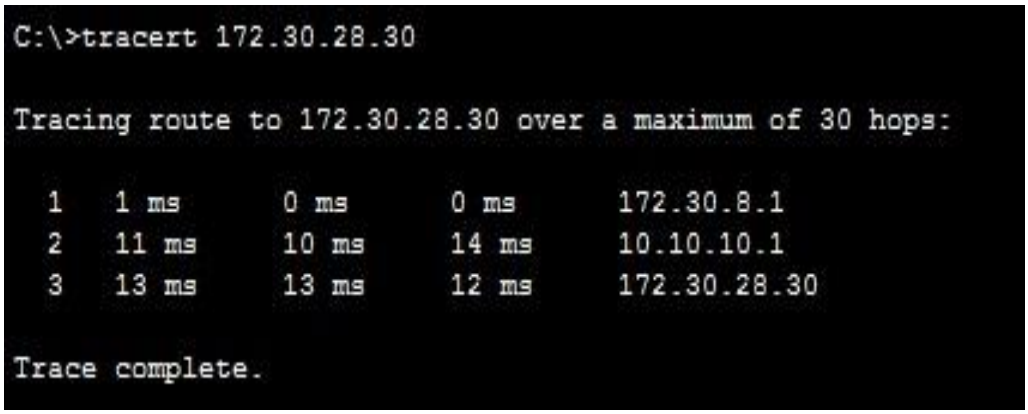


Figura 64: Tracert de SERVIDOR OTI a PC-CAD con VPN (Captura de pantalla).

Elaboración: Propia.

Analizando los resultados obtenidos se interpreta que la conexión entre los puntos existe y nuestro túnel IPsec de la VPN trabaja correctamente.

4.2. VERIFICACIÓN DE OPERATIVIDAD DE LA VPN CON IPSEC.

Al realizar la configuración de la VPN con Cisco IOS CLI, también podemos verificar si esta VPN funciona o no; solo es necesario la emisión de algunos comandos que nos permitan realizar el análisis de dicha VPN.

Lo primero que debemos hacer es intercambiar paquetes de datos entre ROTI y RCAD, para ello se utilizó un ping extendido desde ROTI hacia la dirección IP 172.30.28.1 de la interfaz G0/1 de RCAD. El ping extendido permite controlar la dirección de origen de los paquetes.

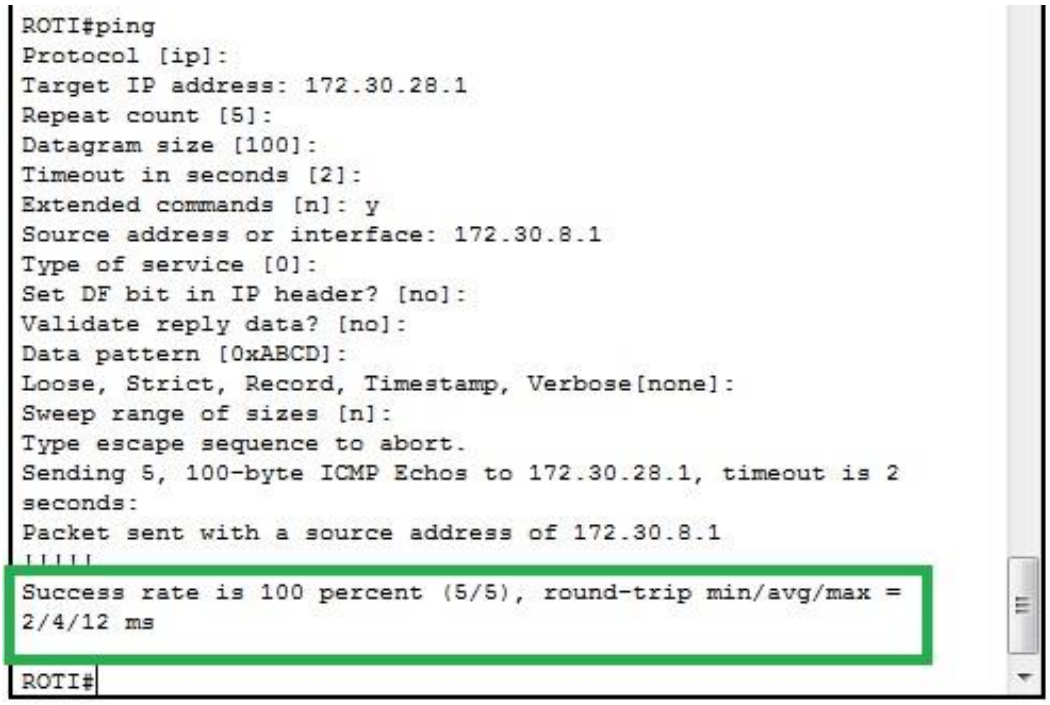


Figura 65: Ping Extendido (Captura de pantalla).

Elaboración: Propia.

Al comprobar que la conexión fue exitosa se procede con la emisión del comando '**show crypto isakmp sa**'

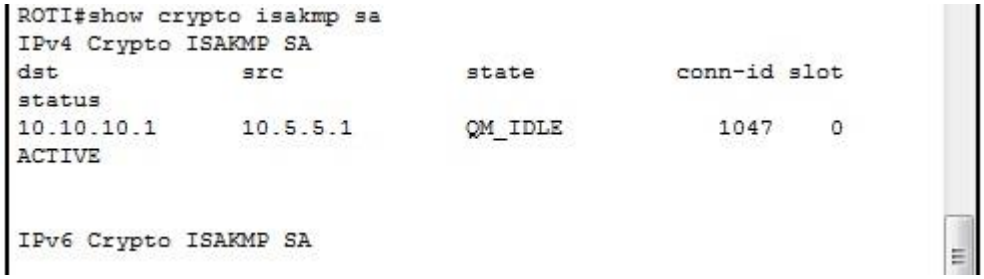


Figura 66: Muestra de SAs activadas (Captura de pantalla).

Elaboración: Propia.

Al reconocer que la fuente de los datos era 172.30.8.1 (ROTI), y el destino era 172.30.28.1 (RCAD). La VPN reconoce este tráfico como un tráfico de interés basado en la definición de la ACL 101. Así que se establece una SA y los paquetes viajan a través del túnel como tráfico encriptado.

Por último emitimos el comando '**show crypto IPsec sa**' donde se puede observar cuantos paquetes de datos fueron transmitidos durante la conexión al realizar el ping extendido, para analizar su contenido. En la imagen que se muestra como ejemplo a continuación se observa que son 12 los paquetes intercambiados entre ROTI y RCAD, encapsulados y encriptados satisfactoriamente con los protocolos configurados en la parte anterior.

Figura 67: Muestra de paquetes transmitidos entre ROTI y RCAD detallado (Captura de pantalla).

Elaboración: Propia.

Es así que con el análisis dado, cualquier tráfico iniciado desde ROTI con una dirección de origen en la red 172.30.8.0/22 y una dirección de destino en la red 172.30.28.0/22 formara una SA y por consiguiente establecerá túneles en su interconexión. En ROTI, el tráfico de interés es cualquier tráfico con una dirección de origen en la red 172.30.28.0/22 y una dirección de destino en la red 172.30.8.0/22. Esto incluye FTP, HTTP, Telnet y otros.

Este proceso se realiza también para verificar la conexión VPN configurada con CCP; el análisis y la interpretación conllevan al mismo fin.

4.3. CAPTURA DE PAQUETES ENCRIPTADOS POR LA VPN

Como mencionamos anteriormente, para realizar la captura de un paquete de datos encriptado fue necesario implementar un servidor y un cliente VPN (3.6.4); es así que se trabajó con el servidor Apache de Ubuntu para realizar las pruebas y con una PC para el cliente VPN.

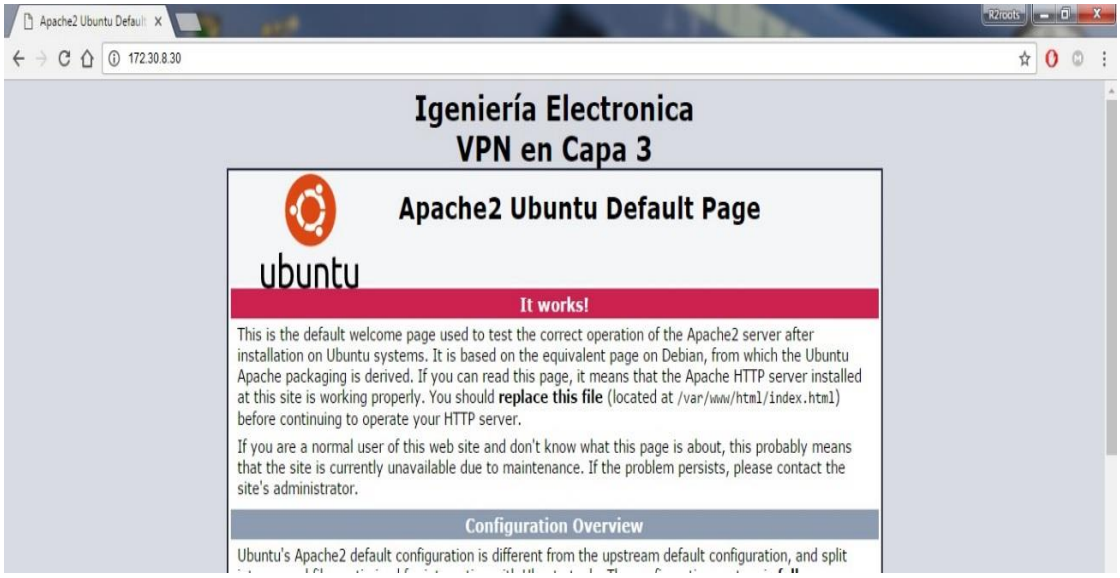
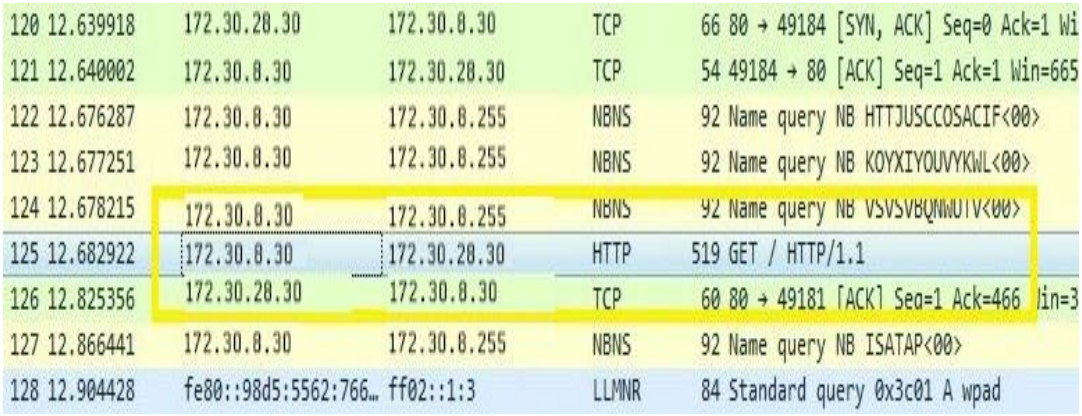


Figura 68: Captura de pantalla Servidor Activo.

Elaboración: Propia.

Para realizar la prueba establecimos la conexión entre los dos puntos con el comando ‘ping’, al mismo tiempo que capturábamos los paquetes con el software Wireshark. De la misma manera que se hizo en el punto (4.1.), se trabajó con dos etapas: Captura de datos sin VPN y captura de datos con VPN.

En la captura de paquetes de la red sin VPN, se observa que los paquetes HTTP son los que intercambian la información en la red.



120 12.639918	172.30.28.30	172.30.8.30	TCP	66 80 → 49184 [SYN, ACK] Seq=0 Ack=1 Wi
121 12.640002	172.30.8.30	172.30.28.30	TCP	54 49184 → 80 [ACK] Seq=1 Ack=1 Win=665
122 12.676287	172.30.8.30	172.30.8.255	NBNS	92 Name query NB HTTJUSCCOSACIF<00>
123 12.677251	172.30.8.30	172.30.8.255	NBNS	92 Name query NB KOYXIYOUVYKWL<00>
124 12.678215	172.30.8.30	172.30.8.255	NBNS	92 Name query NB VSVSVBQNWUIV<00>
125 12.682922	172.30.8.30	172.30.28.30	HTTP	519 GET / HTTP/1.1
126 12.825356	172.30.28.30	172.30.8.30	TCP	60 80 → 49181 [ACK] Seq=1 Ack=466 Win=3
127 12.866441	172.30.8.30	172.30.8.255	NBNS	92 Name query NB ISATAP<00>
128 12.904428	fe80::98d5:5562:766…	ff02::1:3	LLMNR	84 Standard query 0x3c01 A wpad

Figura 69: Wireshark - Captura de paquetes sin VPN (Captura de pantalla).

Elaboración: Propia.

Al desglosar este paquete para seguir su contenido, observamos que los datos del servidor son mostrados sin ninguna encriptación o tipo de seguridad; claramente debido a que la red se encuentra sin la VPN.

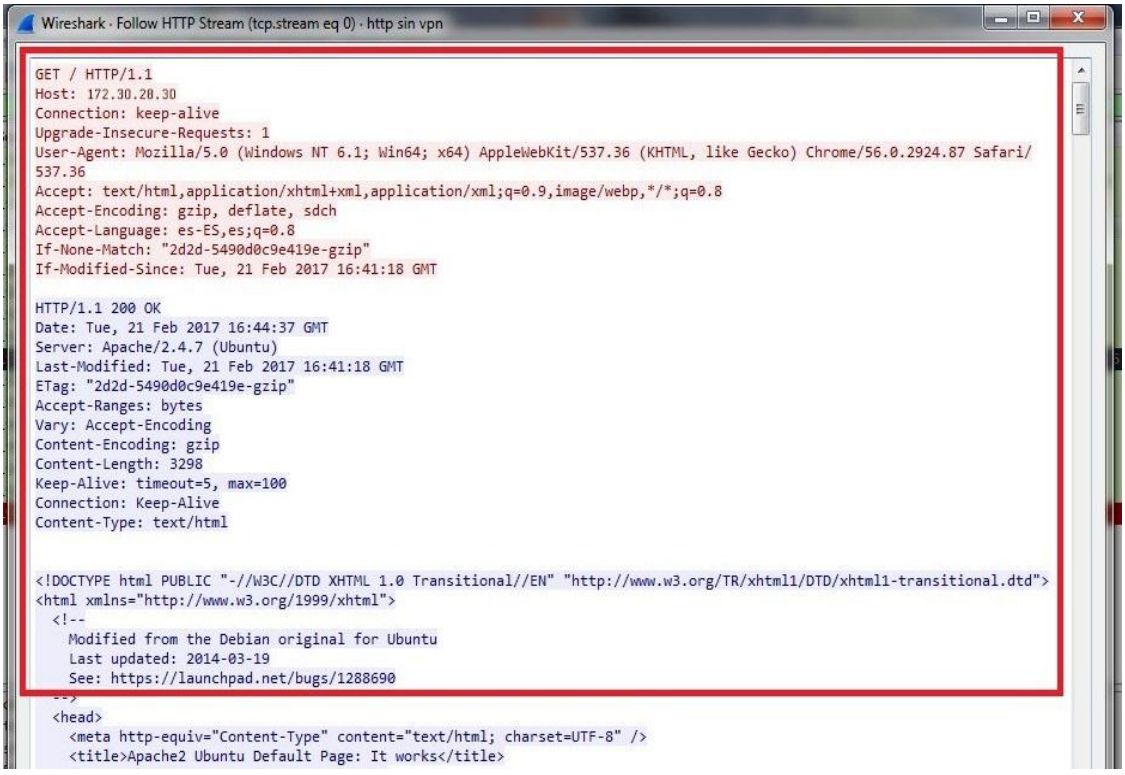
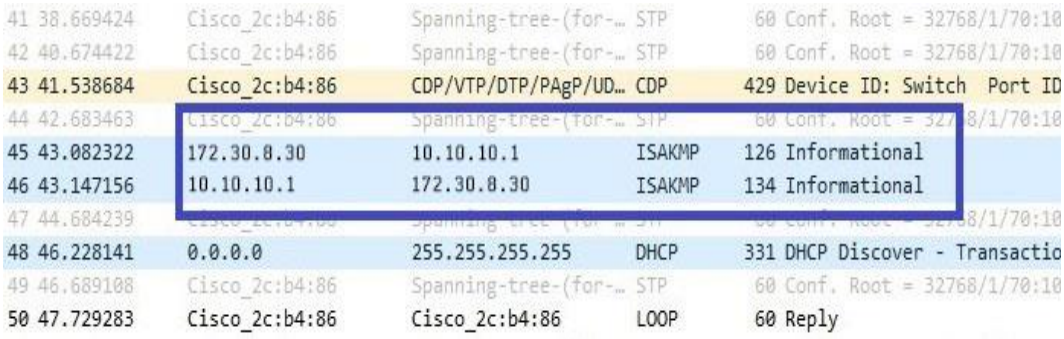


Figura 70: Wireshark - Datos del servidor desencriptados (Captura de pantalla).

Elaboración: Propia.

Ahora, al implementar la VPN en los equipos, establecemos una nueva conexión entre los puntos para realizar una nueva captura con el programa Wireshark; esta vez con el túnel IPsec habilitado y la VPN funcionando, podemos apreciar que los paquetes HTTP han desaparecido y en su lugar solo se muestran paquetes ISAKMP.



41	38.669424	Cisco_2c:b4:86	Spanning-tree-(for-…	STP	60 Conf. Root = 32768/1/70:10
42	40.674422	Cisco_2c:b4:86	Spanning-tree-(for-…	STP	60 Conf. Root = 32768/1/70:10
43	41.538684	Cisco_2c:b4:86	CDP/VTP/DTP/PAgP/UD…	CDP	429 Device ID: Switch Port ID
44	42.683463	Cisco_2c:b4:86	Spanning-tree-(for-…	STP	60 Conf. Root = 32768/1/70:10
45	43.082322	172.30.8.30	10.10.10.1	ISAKMP	126 Informational
46	43.147156	10.10.10.1	172.30.8.30	ISAKMP	134 Informational
47	44.684239	Cisco_2c:b4:86	Spanning-tree-(for-…	STP	60 Conf. Root = 32768/1/70:10
48	46.228141	0.0.0.0	255.255.255.255	DHCP	331 DHCP Discover - Transactio
49	46.689108	Cisco_2c:b4:86	Spanning-tree-(for-…	STP	60 Conf. Root = 32768/1/70:10
50	47.729283	Cisco_2c:b4:86	Cisco_2c:b4:86	LOOP	60 Reply

Figura 71: Wireshark - Captura de paquetes con VPN (Captura de pantalla).

Elaboración: Propia.

A partir de esta captura ya se puede interpretar como un resultado fehaciente que nuestra VPN es funcional, a pesar de ello se decide abrir el paquete para comprobar que información contiene, dándonos el resultado que se muestra en la siguiente imagen.

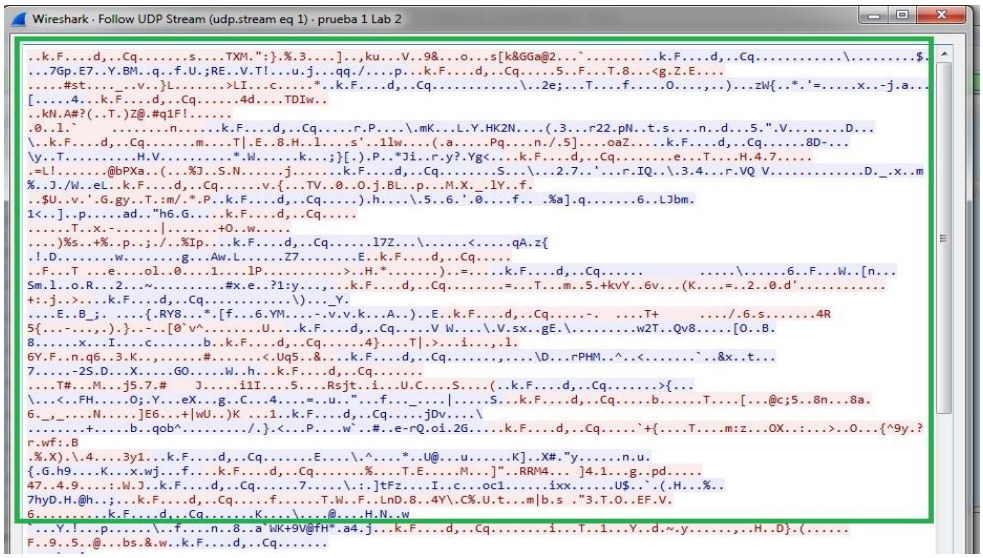


Figura 72: Wireshark - Datos del Servidor encriptados (Captura de pantalla).

Elaboración: Propia.

Como se puede observar, la encriptación es exitosa y los datos que viajan por el túnel IPsec de nuestra VPN son protegidos durante la transmisión de los mismos.

Entonces, con el análisis de los resultados arrojados por los diferentes softwares y aplicación de comandos, es que se comprueba que nuestra VPN logra una conexión óptima además de encriptar todo el tráfico que fluya por ella.

4.4. TRATAMIENTO Y ANÁLISIS DE DATOS.

4.4.1. Tratamiento de Datos.

Para realizar el análisis de seguridad de nuestra VPN se realizaron dos pruebas:

- Prueba de conexión.
- Prueba de encriptación.

Las pruebas se efectuaron en la topología utilizada en el punto (3.6.4.) ya que esta topología permite acceder directamente a los datos transmitidos a través de la VPN. Para ambas pruebas se realizó la emisión del comando ping 7 veces desde el 'SERVIDOR OTI' a la PC-CAD que sería la PC de cualquier coordinación académica de la institución. Sin embargo en la prueba de encriptación se recogieron los datos a partir del software Wireshark que permitan capturar los paquetes transmitidos entre los dos puntos de transmisión de nuestra red. Se toma la cantidad de 7 pruebas solo como muestra. Es así que se toman en las variables los siguientes datos:

- Ping: Se realiza 7 emisiones del comando en la red.
- Paquetes enviados por ping: En la prueba se muestra que cada ping envía 4 paquetes entonces:

  7 pings x 4 paquetes cada ping = 28 paquetes enviados a través de la red.

- Datos capturados en Wireshark: por cada paquete enviado el software Wireshark captura 2 datos, el primer envío desde 'SERVIDOR OTI' a PC-CAD y el segundo desde PC-CAD a 'SERVIDOR OTI', es decir su respuesta, por lo tanto:

  28 Paquetes x 02 datos cada paquete = 56 datos capturados en Wireshark

Todo lo anteriormente mencionado se resume de la siguiente manera:

	Ping	**Paquetes enviados**	**Datos Capturados**
Cantidad por prueba	01	04	08
Cantidad total de pruebas	07	28	56

Tabla N° 5: Variables y cantidad de pruebas.

Elaboración: Propia.

Interpretación: La cantidad de paquetes y datos capturados para la prueba de conexión y encriptación de nuestra VPN son establecidos en esta tabla como base para el análisis posterior de los resultados.

4.4.2. Análisis de datos

- Prueba de Conexión

Como se mencionó anteriormente para realizar la prueba de conexión se utilizó la emisión del comando 'ping' en la lista de comandos cmd.

C:\> ping 172.30.28.30

Al emitir el comando se verifica que la primera prueba del ping no establece una conexión con su par en el envío de los 02 primeros paquetes, y se muestra que existe una pérdida del 50%. La figura 73 detalla los errores capturados directamente de nuestra red.

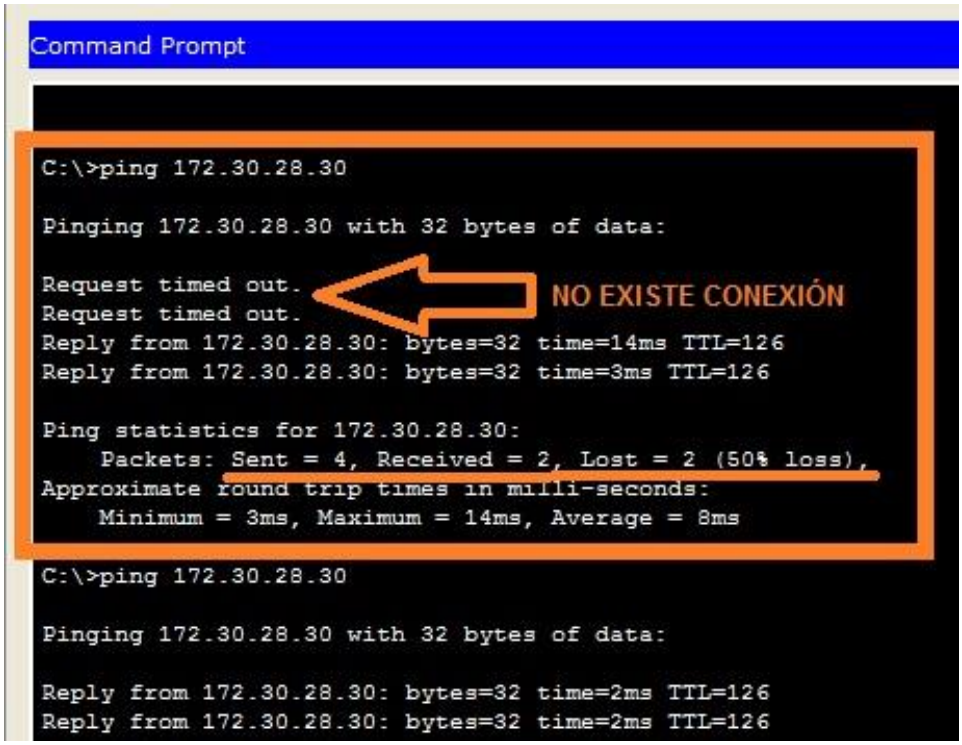


Figura 73: Prueba de conexión con emisión del comando 'PING' (Captura de pantalla).

Elaboración: Propia.

En las siguientes pruebas como se puede apreciar en la misma captura, la conexión se establece de manera continua sin apreciar ningún otro error. Entonces de acuerdo a este dato se establece la Tabla N° 6 de prueba de conexión en la Red.

Variable	**Cantidad de Pruebas**	**Porcentaje de Conexión**
Ping	07	100%
Paquetes Enviados	28	100%
Paquetes Recibidos	26	92.86%

Continúa…

Paquetes no Recibidos	02	07.14%

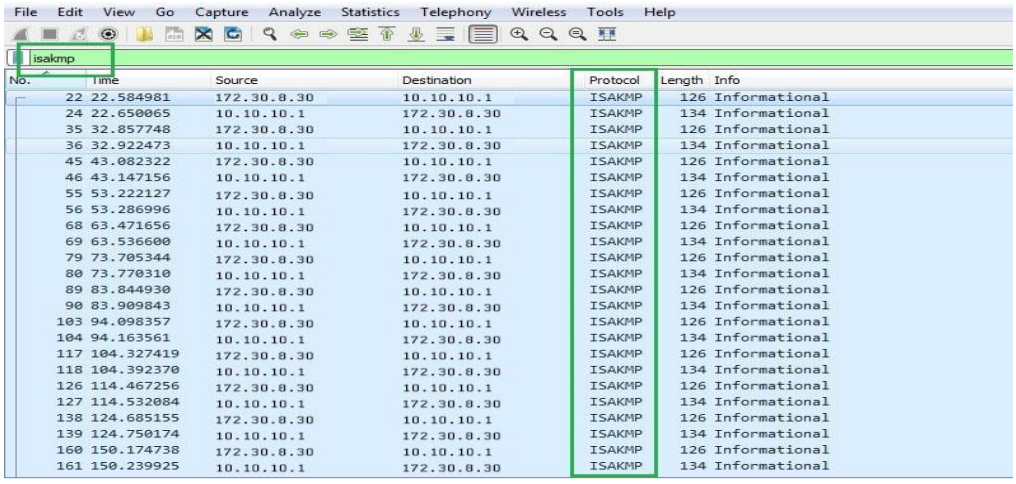
Tabla N° 6: Prueba de Conexión.

Elaboración: Propia.

Interpretación: De acuerdo a las pruebas realizadas se establece que existe un porcentaje de conexión en la VPN del 92.86%, con una pérdida de paquetes del 07.14%, estos resultados reflejan que no hay intercambio de paquetes en la primera conexión de los puntos del túnel IPsec debido al establecimiento del mismo entre los puntos asignados; sin embargo las siguientes pruebas arrojan que la conexión en la red es fluida sin errores ni pérdida de información.

- Prueba de Encriptación

Para la prueba de encriptación, se realizó la captura de datos con el software Wireshark encontrando 50 datos encriptados con el protocolo ISAKMP.



No.	Time	Source	Destination	Protocol	Length	Info
22	22.584981	172.30.8.30	10.10.10.1	ISAKMP	126	Informational
24	22.650065	10.10.10.1	172.30.8.30	ISAKMP	134	Informational
35	32.857748	172.30.8.30	10.10.10.1	ISAKMP	126	Informational
36	32.922473	10.10.10.1	172.30.8.30	ISAKMP	134	Informational
45	43.082322	172.30.8.30	10.10.10.1	ISAKMP	126	Informational
46	43.147156	10.10.10.1	172.30.8.30	ISAKMP	134	Informational
55	53.222127	172.30.8.30	10.10.10.1	ISAKMP	126	Informational
56	53.286996	10.10.10.1	172.30.8.30	ISAKMP	134	Informational
68	63.471656	172.30.8.30	10.10.10.1	ISAKMP	126	Informational
69	63.536600	10.10.10.1	172.30.8.30	ISAKMP	134	Informational
79	73.705344	172.30.8.30	10.10.10.1	ISAKMP	126	Informational
80	73.770310	10.10.10.1	172.30.8.30	ISAKMP	134	Informational
89	83.844930	172.30.8.30	10.10.10.1	ISAKMP	126	Informational
90	83.909843	10.10.10.1	172.30.8.30	ISAKMP	134	Informational
103	94.098357	172.30.8.30	10.10.10.1	ISAKMP	126	Informational
104	94.163561	10.10.10.1	172.30.8.30	ISAKMP	134	Informational
117	104.327419	172.30.8.30	10.10.10.1	ISAKMP	126	Informational
118	104.392370	10.10.10.1	172.30.8.30	ISAKMP	134	Informational
126	114.467256	172.30.8.30	10.10.10.1	ISAKMP	126	Informational
127	114.532084	10.10.10.1	172.30.8.30	ISAKMP	134	Informational
138	124.685155	172.30.8.30	10.10.10.1	ISAKMP	126	Informational
139	124.750174	10.10.10.1	172.30.8.30	ISAKMP	134	Informational
160	150.174738	172.30.8.30	10.10.10.1	ISAKMP	126	Informational
161	150.239925	10.10.10.1	172.30.8.30	ISAKMP	134	Informational

Figura 74: Prueba de encriptación con software Wireshark (Captura de pantalla).

Elaboración: Propia.

De acuerdo a este resultado se realiza la Tabla N° 7 de prueba de encriptación de datos.

Variable	Cantidad de Pruebas	Porcentaje de Conexión
Ping	07	100%
Datos Enviados	56	100%
Datos Capturados	50	89.29%
Datos no encontrados	06	10.71%

Tabla N° 7: Prueba de encriptación de datos.

Elaboración: Propia.

Interpretación: Con la información obtenida se establece que el 89.29% de los datos capturados han sido encriptados por la VPN, sin embargo el 10.71% de estos datos no fueron encontrados en la captura, esto significa que la información que fluye por nuestra VPN solo será transmitida y llegará a su destino si el túnel IPsec está operativo, si aún no se establece el túnel simplemente la información no es enviada para evitar la filtración de la misma.

Como observación se identifica que en la prueba de encriptación, si los datos son convertidos en paquetes, existen 3 paquetes no encontrados a diferencia de la prueba de conexión donde solo fueron 2. Este paquete extra perdido se interpreta como un paquete de prueba que realiza la VPN para verificar la conexión segura entre los dos puntos de transmisión.

Con todos los datos obtenidos se resume que nuestra VPN, a partir de las pruebas (prueba de conexión 92.86% y prueba de encriptación 89.29%), tiene un **rendimiento mínimo de 89.29%.**

4.5. USO DE LOS RESULTADOS Y CONTRIBUCIONES DE LA INVESTIGACIÓN

Al lograr los satisfactoriamente resultados deseados, se reconoce que el prototipo de esta Red Privada Virtual podrá ser aplicado en todas las oficinas de la Universidad Nacional del Altiplano que transmitan información entre sí; además, esta VPN también podrá ser aplicada de manera óptima en otras instituciones del mismo rubro.

Por último, el diseño e implementación de esta Red contribuye en la seguridad y adaptación dentro de la Institución, pues los paquetes van encriptados, siendo su configuración transparente al usuario.

CONCLUSIONES

PRIMERO: Se logró diseñar e implementar el prototipo de una Red Privada Virtual en Capa 3 utilizando CISCO IOS que asegura y encripta la información compartida entre la Oficina de Tecnología e Informática y las coordinaciones académicas de las 19 facultades de la Universidad Nacional del Altiplano. Esta red está diseñada bajo la utilización del túnel IPsec punto a punto que trabaja bajo la política ISAKMP de IKE brindando confidencialidad, integridad y autenticación a la red, estableciendo así un tráfico de datos seguros en las oficinas de la institución que operen bajo la VPN.

SEGUNDO: El diseño del prototipo de la Red Privada Virtual opera y controla el tráfico en LAN y WAN satisfactoriamente, ya que al realizar las pruebas en la red local se constató que nuestra VPN aseguraba los datos transmitidos y al ver el mismo resultado con un servidor y un cliente VPN se concluye que esta red también asegura el tráfico en WAN.

TERCERO: La Red Privada Virtual logró ser implementada en el Laboratorio de Cisco de la Universidad Nacional del Altiplano, con un rendimiento mínimo de 89.29% de los 56 datos transmitidos de acuerdo a las pruebas realizadas.

RECOMENDACIONES

PRIMERO: La red privada virtual al trabajar con túnel IPsec está siendo configurada en la capa de Red, esto tiene un beneficio significativo ya que los datos son asegurados desde la capa 4 a la capa 7 durante el tráfico de la información, sin embargo, el siguiente paso para mejorar nuestra VPN es configurarla en La capa de Enlace de Datos, es decir la capa 2, esto conlleva a otro análisis del tráfico de datos y a muchas variaciones en el uso de protocolos más sofisticados y poco utilizados, a pesar de ello una VPN en capa 2 con base en esta investigación dará un nivel de seguridad más elevado al que ya se logró.

SEGUNDO: Al trabajar con protocolos de seguridad debemos tener presente con que equipos vamos a trabajar, en nuestro caso cuando configuramos la VPN en un router Cisco 2901 tuvimos que habilitar los protocolos de seguridad para que puedan ser ejecutados en el router; esto no necesariamente sucederá en todos los routers ya que depende mucho de la imagen que tengan instalada en su memoria flash. En la práctica nos encontraremos con diferentes modelos de routers y diferentes imágenes pre-instaladas en ellos, para una óptima configuración de la VPN es fundamental analizar las imágenes y los datasheets de los routers para verificar el soporte de los protocolos de seguridad.

TERCERO: Se debe tener en cuenta para una implementación real de la VPN el cableado estructurado dentro de la institución, en nuestro proyecto el cableado ya está definido dentro de la Universidad Nacional del Altiplano por lo tanto no es primordial una investigación para desarrollarlo; aun así, si este prototipo llegase a ser implementado en otra institución debe considerarse como primer paso para dicha implementación el estudio de un cableado estructurado acorde a sus necesidades.

REFERENCIAS BIBLIOGRÁFICAS

- Alvarez Quispe, J. J. (2014). *Diseño de una Red de Banda Ancha, usando tecnología Multipath TCP, para la Universidad Nacional del Altiplano.* Universidad Nacional del Altiplano, Puno, Perú. Puno: Repositorio Institucional UNA - PUNO.
- Anónimo. (17 de Agosto de 2009). *Redes de Área Amplia (WAN)*. Recuperado el 14 de Febrero de 2017, de http://redesdedatosinfo.galeon.com/enlaces2128630.html
- Anónimo. (26 de Enero de 2012). *El Taller del Bit*. Recuperado el 13 de Abril de 2017, de http://eltallerdelbit.com/capa-de-red-capa-3-osi
- Anónimo. (23 de Junio de 2013). *EcuRed. Conocimiento con todos y para todos.* Recuperado el 12 de Febrero de 2017, de https://www.ecured.cu/Red_de_%C3%A1rea_local_(LAN)
- Anónimo. (2016). *MyWebMyMail.com*. Recuperado el 22 de Febrero de 2017, de http://www.mywebmymail.com/?q=content/what-vpn
- Ariganello, E., & Barrientos Sevilla, E. (2010). *REDES CISCO CCNP a Fondo. Guía de Estudio para Profesionales.* (G. E. AlfaOmega, Ed.) México D. F., México: AlfaOmega Ra-Ma.
- Barker, K., Morris, S., Wallace, K., & Watkins, M. (2013). *CCNA Security 640-554 Official Cert Guide.* Indianápolis, Indianápolis, Estados Unidos: Cisco Press.
- Cisco. (2016). *Informe anual de seguridad de Cisco.* California: Cisco Systems.
- Cisco Networking Academy. (2017). *CCNA Security. Laboratorio - Configuring a Remote Access VPN Server and Client.* California: Cisco Public.

- Cisco Networking Academy. (2017). *CCNA Security. Laboratorio - Configuring a Site-to-Site VPN Using Cisco IOS and CCP*. California: Cisco Public.
- Cisco, N. A. (08 de Enero de 2015). *Netacad.* Recuperado el 15 de Abril de 2017, de https://1329709.netacad.com/courses/271576
- Cutuli, R., Catania, C., & García Garino, C. (2012). *Problemas y herramientas en la seguridad de redes de transmisión de datos universitarias. Elcaso de la Universidad de Cuyo.* Trabajo de Investigación, Universidad Nacional de Cuyo, Mendoza, Argentina, Mendoza.
- Daligar. (30 de Junio de 2012). *Wikipedia*. Recuperado el 18 de Marzo de 2017, de https://commons.wikimedia.org/wiki/File:Arranque_Ios.png
- FIMAZ12. (2012). *WIKI REDES FIMAZ12*. Recuperado el 22 de Febrero de 2017, de https://sites.google.com/site/wikiredesfimaz12/tipo-de-redes-1
- Gonzales Morales, A. (2006). *Redes Privadas Virtuales.* Universidad Autónoma del Estado de Hidalgo, Hidalgo. Pachuca: Instituto de Ciencias Básicas e Ingeniería.
- Hernández Sampieri, R., Fernández-Collado, C., & Baptista Lucio, P. (2006). *Metodología de la Investigación* (Cuarta ed.). (R. Del Bosque Alayón, Ed.) México D. F., México: McGraw - Hill Interamericana.
- HiperLink Technologies. (30 de Abril de 2016). *DS3 Comunicaciones*. Recuperado el 06 de Febrero de 2017, de http://ds3comunicaciones.com/cisco/CISCO2901.html

- Intercompras. (23 de Noviembre de 2015). *Intercompras. Su compra por Internet.* Obtenido de https://intercompras.com/p/switch-cisco-catalyst-puertos-puertos-sfp-combo-lan-base-35193

- Lozada, J. (2014). Investigación Aplicada: Definición, Propiedad Intelectual e Industria. *CIENCIAMÉRICA*, 34-39.

- Marín Alarcón, H. (2015). *GoConqr*. Recuperado el 12 de Marzo de 2017, de https://www.goconqr.com/p/4174862-diapositivas-de-el-modelo-osi-slide_sets

- Mejía Londoño, C. A., Ramírez Galvis, N. J., & Rivera Cradona, J. S. (2012). *Vulnerabilidad, tipos de ataques y formas de mitigarlos en las Capas de modelo OSI en las Redes de Datos de las Organizaciones.* Universidad Tecnológica de Pereira, Risaralda, Colombia. Pereira: Repositorio de Tesis - UTP.

- Paquet, C. (2013). *Implementing Cisco IOS Network Security (IINS) Foundation Learning Guide.* (Segunda ed.). Indianápolis, Indiana, Estados Unidos: Cisco Press.

- Puma Quispe, F. F., & Cutipa Nina, B. L. (2015). *DISEÑO E IMPLEMENTACIÓN DE UN ALGORITMO BASADO EN LA COLONIA DE HORMIGAS PARA EL ENRUTAMIENTO EN UNA RED IPV6 EN LA UNIVERSIDAD NACIONAL DEL ALTIPLANO.* Puno: Universidad Nacional del Altiplano.

- Reina Toranzo, F., & Ruiz Rivas, J. A. (2011). *Redes de Área Local.* Guayaquil: Desconocido.

- Sambero, B. (12 de Septiembre de 2010). *Computacion II Humboldt*. Recuperado el 24 de Febrero de 2017, de http://braynerlinares.blogspot.pe/2010/09/redes-vpn.html
- Universidad Nacional del Altiplano. (Enero de 2016). Reglamento de Organización y Funciones 2016. *Reglamento de Organización y Funciones 2016*, 172. Puno, Puno, Puno: Universidad Nacional del Altiplano.
- Valencia Miranda, Á. (2011). *Introducción a la Ingeniería de Telecomunicaciones.* Lima, Lima, Perú: Vicerrectorado de Investigación -UTP.

ANEXOS

ANEXO A: CONFIGURACIÓN DE VPN EN R1

```
ROTI#show running-config
Building configuration...

Current configuration : 1682 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname ROTI
!
!
!
enable secret 5 $1$mERr$zE/zQmilyJGa9yXjKUFhi.
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2901/K9 sn FTX1524SJGX
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
lifetime 3600
!
crypto isakmp key vpnuna123 address 10.10.10.1
!
!
crypto ipsec security-association lifetime seconds 1800
!
crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
!
```

Continúa…

```
crypto map CMAP 10 ipsec-isakmp
set peer 10.10.10.1
set pfs group5
set security-association lifetime seconds 900
set transform-set 50
match address 101
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
ip address 172.30.8.1 255.255.252.0
duplex auto
speed auto
!
interface Serial0/0/0
ip address 10.5.5.1 255.255.255.240
clock rate 64000
crypto map CMAP
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 101
log-adjacency-changes
network 172.30.8.0 0.0.3.255 area 0
network 10.5.5.0 0.0.0.15 area 0
```

Continúa…

```
!
ip classless
!
ip flow-export version 9
!
!
access-list 101 permit ip 172.30.8.0 0.0.3.255 172.30.28.0 0.0.3.255
!
!
!
!
!
line con 0
exec-timeout 5 0
password 7 08375C40060A0C14131B0D5729242A
logging synchronous
login
!
line aux 0
!
line vty 0 4
exec-timeout 5 0
password 7 08375C40060A0C14131B0D573C3F3D
login
!
!
!
end
```

En base a programación Cisco (Cisco Networking Academy, 2017)

Elaboración: Propia

ANEXO B: CONFIGURACIÓN DE VPN EN R3

```
RCAD#show running-config
Building configuration...

Current configuration : 1666 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname RCAD
!
!
!
enable secret 5 $1$mERr$zE/zQmilyJGa9yXjKUFhi.
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2901/K9 sn FTX15246EM5
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
lifetime 3600
!
crypto isakmp key vpnuna123 address 10.5.5.1
!
!
crypto ipsec security-association lifetime seconds 1800
!
crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
!
crypto map CMAP 10 ipsec-isakmp
```

Continúa…

```
set peer 10.5.5.1
set pfs group5
set security-association lifetime seconds 900
set transform-set 50
match address 101
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
ip address 172.30.28.1 255.255.252.0
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/0/1
ip address 10.10.10.1 255.255.255.240
crypto map CMAP
!
interface Vlan1
no ip address
shutdown
!
router ospf 101
log-adjacency-changes
network 172.30.28.0 0.0.3.255 area 0
network 10.10.10.0 0.0.0.15 area 0
!
ip classless
```

Continúa…

```
!
ip flow-export version 9
!
!
access-list 101 permit ip 172.30.28.0 0.0.3.255 172.30.8.0 0.0.3.255
!
!
!
!
!
line con 0
exec-timeout 5 0
password 7 08375C40060A0C14131B0D5729242A
logging synchronous
login
!
line aux 0
!
line vty 0 4
exec-timeout 5 0
password 7 08375C40060A0C14131B0D573C3F3D
login
!
!
!
End
```

En base a programación Cisco (Cisco Networking Academy, 2017)

Elaboración: Propia

ANEXO C: LISTA DE COMANDOS

##R1##

```
enable
conf t
hostname ROTI
enable secret vpnosicapa3
no ip domain-lookup
interface G0/1
ip address 172.30.8.1 255.255.252.0
no shutdown
exit
interface s0/0/0
ip address 10.5.5.1 255.255.255.240
clock rate 64000
no shutdown
exit
router ospf 101
network 172.30.8.0 0.0.3.255 area 0
network 10.5.5.0 0.0.0.15 area 0
exit
security passwords min-length 10
line console 0
password vpnosicapa3con
exec-timeout 5 0
login
logging synchronous
exit
line vty 0 4
password vpnosicapa3vty
exec-timeout 5 0
login
exit
service password-encryption
license boot module c2900 technology-package securityk9
yes
exit
write
reload
===
enable
conf t
crypto isakmp enable
crypto isakmp policy 10
authentication pre-share
encryption aes 256
hash sha
```

Continúa…

```
group 5
lifetime 3600
end
conf t
crypto isakmp key vpnuna123 address 10.10.10.1
crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
exit
crypto ipsec security-association lifetime seconds 1800
access-list 101 permit ip 172.30.8.0 0.0.3.255 172.30.28.0 0.0.3.255
crypto map CMAP 10 ipsec-isakmp
match address 101
set peer 10.10.10.1
set pfs group5
set transform-set 50
set security-association lifetime seconds 900
exit
interface s0/0/0
crypto map CMAP
end
```

##R2##

```
enable
conf t
hostname RNET
enable secret vpnosicapa3
no ip domain-lookup
interface S0/0/0
ip address 10.5.5.2 255.255.255.240
no shutdown
exit
interface s0/0/1
ip address 10.10.10.2 255.255.255.240
clock rate 64000
no shutdown
exit
router ospf 101
network 10.5.5.0 0.0.0.15 area 0
network 10.10.10.0 0.0.0.15 area 0
exit
security passwords min-length 10
line console 0
password vpnosicapa3con
exec-timeout 5 0
login
logging synchronous
```

Continúa…

exit
line vty 0 4
password vpnosicapa3vty
exec-timeout 5 0
login
exit
service password-encryption
license boot module c2900 technology-package securityk9
yes
exit
write
reload

##R3##

enable
conf t
hostname RCAD
enable secret vpnosicapa3
no ip domain-lookup
interface G0/1
ip address 172.30.28.1 255.255.252.0
no shutdown
exit
interface s0/0/1
ip address 10.10.10.1 255.255.255.240
no shutdown
exit
router ospf 101
network 172.30.28.0 0.0.3.255 area 0
network 10.10.10.0 0.0.0.15 area 0
exit
security passwords min-length 10
line console 0
password vpnosicapa3con
exec-timeout 5 0
login
logging synchronous
exit
line vty 0 4
password vpnosicapa3vty
exec-timeout 5 0
login
exit
service password-encryption
license boot module c2900 technology-package securityk9
yes
exit
write

Continúa…

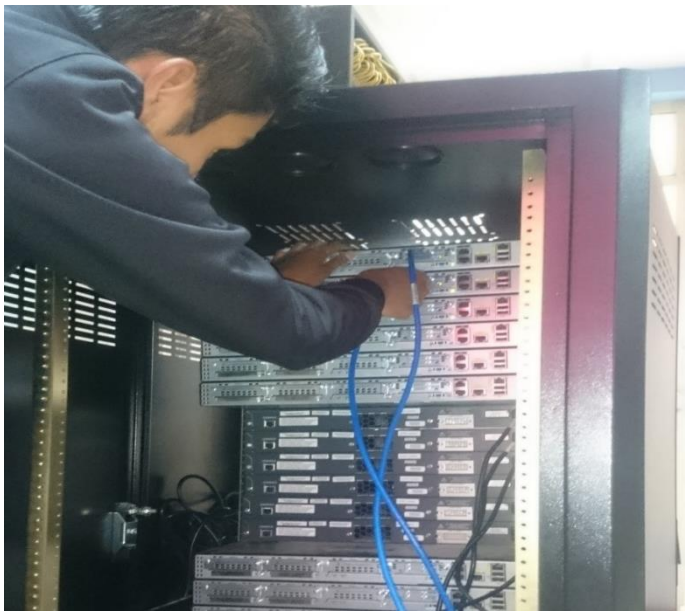
```
reload
===
enable
conf t
crypto isakmp enable
crypto isakmp policy 10
authentication pre-share
encryption aes 256
hash sha
group 5
lifetime 3600
end
conf t
crypto isakmp key vpnuna123 address 10.5.5.1
crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
exit
crypto ipsec security-association lifetime seconds 1800
access-list 101 permit ip 172.30.28.0 0.0.3.255 172.30.8.0 0.0.3.255
crypto map CMAP 10 ipsec-isakmp
match address 101
set peer 10.5.5.1
set pfs group5
set transform-set 50
set security-association lifetime seconds 900
exit
interface s0/0/1
crypto map CMAP
end
```

En base a programación Cisco (Cisco Networking Academy, 2017)

Elaboración: Propia

ANEXO D: FOTOS

Implementación de Topología



Elaboración: Propia

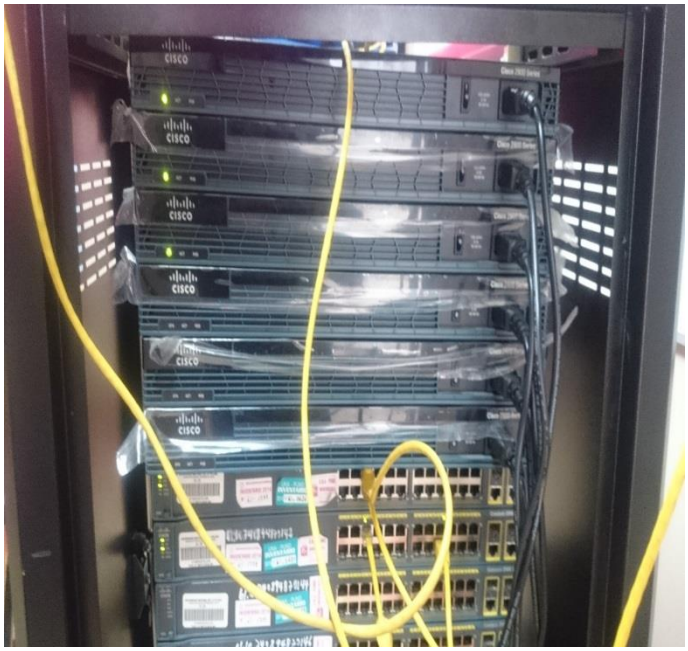
Conexión de Routers

Elaboración: Propia

Prueba de cables UTP para conexión de topología.

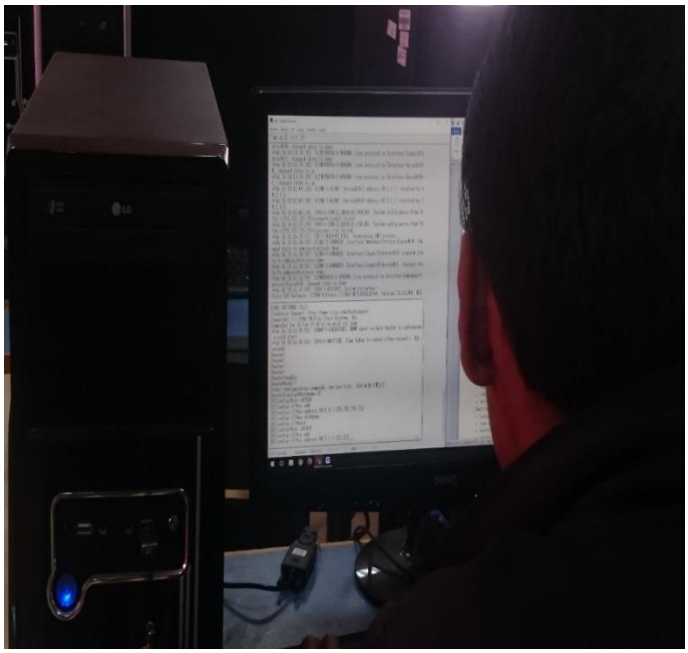
Elaboración: Propia

Topología implementada



Elaboración: Propia

Configuración de Equipos

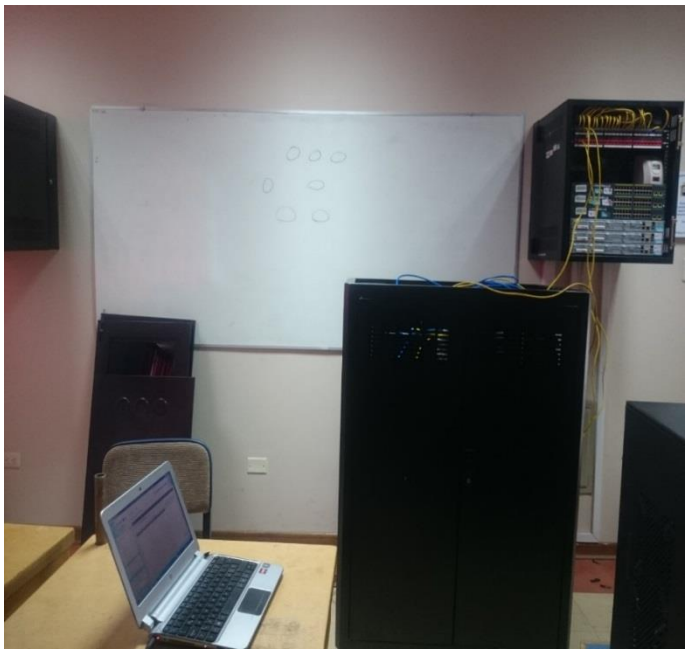


Elaboración: Propia

Configuración de Direccionamiento IP

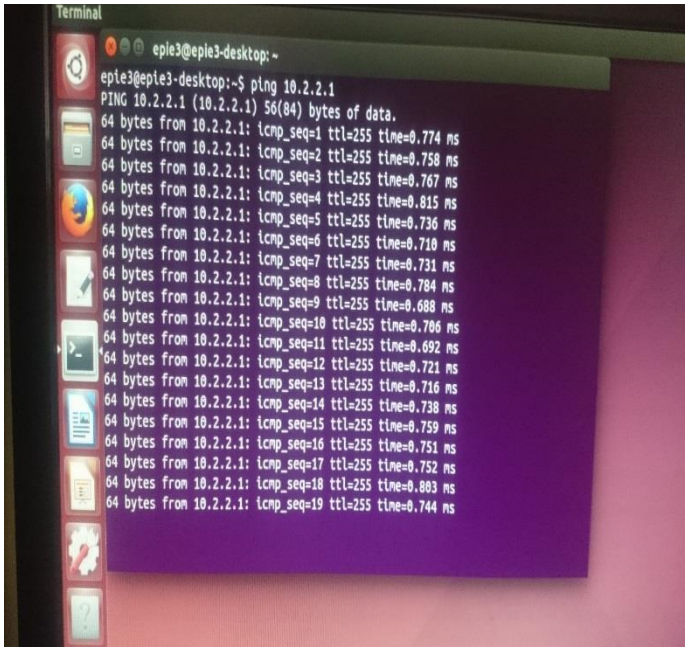
Elaboración: Propia

Prueba de prototipo en el Laboratorio de Cisco



Elaboración: Propia

Prueba de conexión a Servidor



Elaboración: Propia

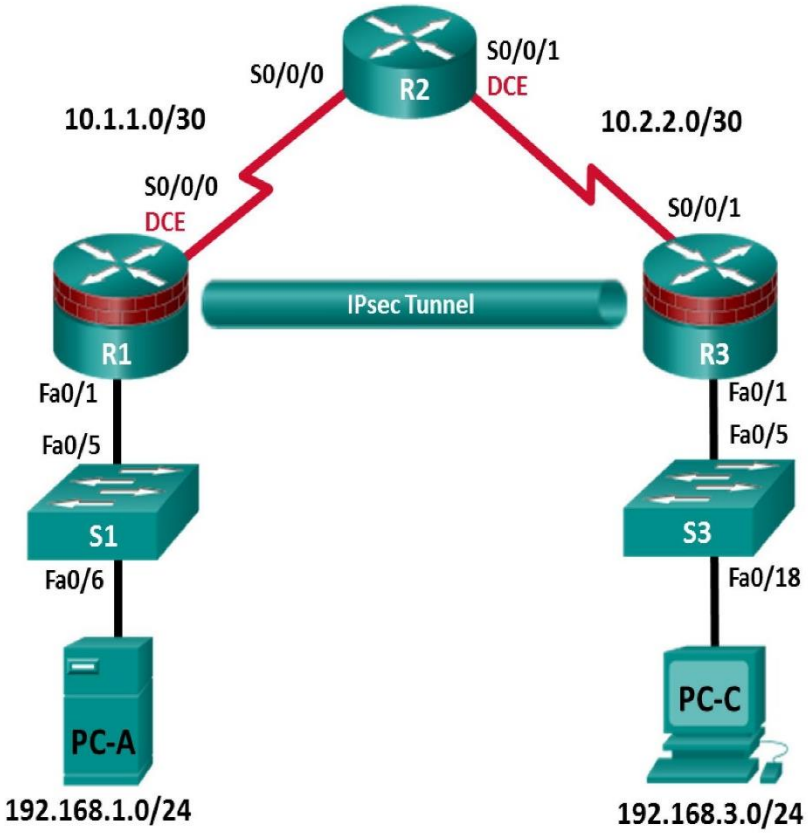
ANEXO E: LABORATORIO DE CISCO UTILIZADO COMO BASE Y FUNDAMENTO

Cisco Networking Academy® Mind Wide Open™

CCNA Security

Lab - Configuring a Site-to-Site VPN Using Cisco IOS and CCP

Topology



Note: ISR G2 devices use GigabitEthernet interfaces instead of FastEthernet Interfaces.

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A	S1 Fa0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	Fa0/1	192.168.3.1	255.255.255.0	N/A	S3 Fa0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 Fa0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 Fa0/18

Objectives

Part 1: Configure Basic Device Settings

- Configure hostnames, interface IP addresses, and access passwords.
- Configure the OSPF dynamic routing protocol.

Part 2: Configure a Site-to-Site VPN Using Cisco IOS

- Configure IPsec VPN settings on R1 and R3.
- Verify site-to-site IPsec VPN configuration.
- Test IPsec VPN operation.

Part 3: Configure a Site-to-Site VPN Using CCP

- Configure IPsec VPN settings on R1.
- Create a mirror configuration for R3.
- Apply the mirror configuration to R3.
- Verify the configuration.
- Test the VPN configuration using CCP.

Background / Scenario

VPNs can provide a secure method of transmitting data over a public network, such as the Internet. VPN connections can help reduce the costs associated with leased lines. Site-to-Site VPNs typically provide a secure (IPsec or other) tunnel between a branch office and a central office. Another common implementation that uses VPN technology is remote access to a corporate office from a telecommuter location, such as a small office or home office.

In this lab, you will build and configure a multi-router network, and then use Cisco IOS and CCP to configure a site-to-site IPsec VPN and then test it. The IPsec VPN tunnel is from router R1 to router R3 via R2. R2 acts as a pass-through and has no knowledge of the VPN. IPsec provides secure transmission of sensitive information over unprotected networks, such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers), such as Cisco routers.

The router commands and output in this lab are from a Cisco 1841 router using Cisco IOS software, release 15.1(4)M8 (Advanced IP Services image). Other routers and Cisco IOS versions can be used. See the Router

Interface Summary Table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the model of the router, the commands available and output produced may vary from what is shown in this lab.

Note: Make sure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 3 Routers (Cisco 1841 with Cisco IOS Release 15.1(4)M8 Advanced IP Services image or comparable)
- 2 Switches (Cisco 2960 or comparable)
- 2 PCs (Windows Vista or Windows 7 with CCP 2.5, latest Java version, Internet Explorer, and Flash Player)
- Serial and Ethernet cables as shown in the topology
- Console cables to configure Cisco networking devices

CCP Notes:

- If the PC on which CCP is installed is running Windows Vista or Windows 7, it may be necessary to right-click the **CCP** icon or menu item, and select **Run as administrator**.
- To run CCP, it may be necessary to temporarily disable antivirus programs and O/S firewalls. Make sure that all pop-up blockers are turned off in the browser.

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, dynamic routing, device access, and passwords.

Note: All tasks should be performed on R1, R2, and R3. The procedure for R1 is shown here as an example.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each router.

a. Configure hostnames, as shown in the topology.

b. Configure the interface IP addresses, as shown in the IP Addressing Table.

c. Configure a clock rate of **64000** for the serial router interfaces with a DCE serial cable attached.

Step 3: Disable DNS lookup.

To prevent the router from attempting to translate incorrectly entered commands, disable DNS lookup.

Step 4: Configure the OSPF routing protocol on R1, R2, and R3.

a. On R1, use the following commands:

```
R1(config)# router ospf 101
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

b. On R2, use the following commands:

```
R2(config)# router ospf 101
R2(config-router)# network 10.1.1.0 0.0.0.3 area 0
R2(config-router)# network 10.2.2.0 0.0.0.3 area 0
```

c. On R3, use the following commands:

```
R3(config)# router ospf 101
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
R3(config-router)# network 10.2.2.0 0.0.0.3 area 0
```

Step 5: Configure PC host IP settings.

a. Configure a static IP address, subnet mask, and default gateway for PC-A, as shown in the IP Addressing Table.

b. Configure a static IP address, subnet mask, and default gateway for PC-C, as shown in the IP Addressing Table.

Step 6: Verify basic network connectivity.

a. Ping from R1 to the R3 Fa0/1 interface at IP address **192.168.3.1**.

If the pings are unsuccessful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.

If the pings are unsuccessful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C, you have demonstrated that the OSPF routing protocol is configured and functioning correctly. If you cannot ping, but the device interfaces are up and IP addresses are correct, use the **show run** and **show ip route** commands to help identify routing protocol-related problems.

Step 7: Configure a minimum password length.

Note: Passwords in this lab are set to a minimum of 10 characters, but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

Use the **security passwords** command to set a minimum password length of **10** characters.

```
R1(config)# security passwords min-length 10
```

Step 8: Configure the basic console and vty lines.

a. Configure **ciscoconpass** as the console password and enable login for R1. For additional security, the **exec-timeout** command causes the line to log out after **5** minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

b. Configure **ciscovtypass** as the vty line password and enable login on R1. For additional security, the **exec-timeout** command causes the line to log out after **5** minutes of inactivity.

c. Repeat these configurations on both R2 and R3.

Step 9: Encrypt clear text passwords.

a. Use the **service password-encryption** command to encrypt the console, aux, and vty passwords.

```
R1(config)# service password-encryption
```

b. Issue the **show run** command. Can you read the console, aux, and vty passwords? Explain.

_____

_____

c. Repeat this configuration on both R2 and R3.

Step 10: Save the basic running configuration for all three routers.

Save the running configuration to the startup configuration from the privileged EXEC mode prompt on R1, R2, and R3.

```
R1# copy running-config startup-config
```

Step 11: Save the configuration on R1 and R3 for later restoration.

Save the R1 and R3 running configurations as text files so the configurations can be used later, in Part 3 of this lab, to restore the routers to configure the VPN with CCP.

Part 2: Configure a Site-to-Site VPN with Cisco IOS

In Part 2 of this lab, you will configure an IPsec VPN tunnel between R1 and R3 that passes through R2. You will configure R1 and R3 using the Cisco IOS CLI. You then review and test the resulting configuration.

Task 1: Configure IPsec VPN Settings on R1 and R3.

Step 1: Verify connectivity from the R1 LAN to the R3 LAN.

In this task, you will verify that with no tunnel in place, the PC-A on the R1 LAN can ping the PC-C on R3 LAN.

From PC-A, ping the PC-C IP address of **192.168.3.3**.

```
PC-A:\> ping 192.168.3.3
```

If the pings are unsuccessful, troubleshoot the basic device configurations before continuing.

Step 2: Enable IKE policies on R1 and R3.

IPsec is an open framework that allows the exchange of security protocols as new technologies, such as encryption algorithms, are developed.

There are two central configuration elements to the implementation of an IPsec VPN:

- Implement Internet Key Exchange (IKE) parameters
- Implement IPsec parameters

a. Verify that IKE is supported and enabled.

IKE Phase 1 defines the key exchange method used to pass and validate IKE policies between peers. In IKE Phase 2, the peers exchange and match IPsec policies for the authentication and encryption of data traffic.

IKE must be enabled for IPsec to function. IKE is enabled, by default, on IOS images with cryptographic feature sets. If it is disabled, you can enable it with the **crypto isakmp enable** command. Use this command to verify that the router IOS supports IKE and that it is enabled.

```
R1(config)# crypto isakmp enable
```

```
R3(config)# crypto isakmp enable
```

Note: If you cannot execute this command on the router, you must upgrade the IOS image that includes the Cisco cryptographic services.

b. Establish an Internet Security Association and Key Management Protocol (ISAKMP) policy and view the available options.

To allow IKE Phase 1 negotiation, you must create an ISAKMP policy and configure a peer association involving that ISAKMP policy. An ISAKMP policy defines the authentication and encryption algorithms and

hash function used to send control traffic between the two VPN endpoints. When an ISAKMP security association has been accepted by the IKE peers, IKE Phase 1 has been completed. IKE Phase 2 parameters will be configured later.

Issue the **crypto isakmp policy number** global configuration mode command on R1 for policy 10.

```
R1(config)# crypto isakmp policy 10
```

c. View the various IKE parameters available using Cisco IOS help by typing a question mark (**?**).

```
R1(config-isakmp)# ?
ISAKMP commands:
  authentication  Set authentication method for protection suite
  default         Set a command to its defaults
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
```

Step 3: Configure ISAKMP policy parameters on R1 and R3.

Your choice of an encryption algorithm determines how confidential the control channel between the endpoints is. The hash algorithm controls data integrity, ensuring that the data received from a peer has not been tampered with in transit. The authentication type ensures that the packet was, indeed, sent and signed by the remote peer. The Diffie-Hellman group is used to create a secret key shared by the peers that has not been sent across the network.

a. Configure an ISAKMP policy with a priority of **10**. Use **pre-shared key** as the authentication type,.**aes 256** for the encryption algorithm, **sha** as the hash algorithm, and Diffie-Hellman group **5** key exchange. Give the policy a lifetime of **3600** seconds (one hour).

Note: Older versions of Cisco IOS do not support AES 256 encryption and SHA as a hash algorithm. Substitute whatever encryption and hashing algorithm your router supports. Ensure that the same changes are made on the other VPN endpoint to be in sync.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# hash sha
R1(config-isakmp)# group 5
R1(config-isakmp)# lifetime 3600
R1(config-isakmp)# end
```

b. Configure the same policy on R3.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# hash sha
R3(config-isakmp)# group 5
R3(config-isakmp)# lifetime 3600
R3(config-isakmp)# end
```

c. Verify the IKE policy with the **show crypto isakmp policy** command.

```
R1# show crypto isakmp policy
Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               3600 seconds, no volume limit
```

Step 4: Configure pre-shared keys.

Because pre-shared keys are used as the authentication method in the IKE policy, a key must be configured on each router that points to the other VPN endpoint. These keys must match for authentication to be successful. The global configuration mode **crypto isakmp key key-string address address** command is used to enter a pre-shared key. Use the IP address of the remote peer, the remote interface that the peer would use to route traffic to the local router.

Which IP addresses should you use to configure the IKE peers, given the topology diagram and IP addressing table?

_____

_____

_____

a. Each IP address that is used to configure the IKE peers is also referred to as the IP address of the remote VPN endpoint. Configure the pre-shared key of **cisco123** on router R1. Production networks should use a complex key. This command points to the remote peer R3 S0/0/1 IP address.

```
R1(config)# crypto isakmp key cisco123 address 10.2.2.1
```

b. Configure the pre-shared key of **cisco123** on router R3. The command for R3 points to the R1 S0/0/0 IP address.

```
R3(config)# crypto isakmp key cisco123 address 10.1.1.1
```

Step 5: Configure the IPsec transform set and life times.

a. The IPsec transform set is another crypto configuration parameter that routers negotiate to form a security association. To create an IPsec transform set, use the **crypto ipsec transform-set tag** command. Use **?** to see which parameters are available.

```
R1(config)# crypto ipsec transform-set 50 ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  comp-lzs      IP Compression using the LZS compression algorithm
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-null      ESP transform w/o cipher
  esp-seal      ESP transform using SEAL cipher (160 bits)
  esp-sha-hmac  ESP transform using HMAC-SHA auth
```

b. On R1 and R3, create a transform set with tag **50** and use an Encapsulating Security Protocol (ESP) transform with an AES 256 cipher with ESP and the SHA hash function. The transform sets must match.

```
R1(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
```

```
R1(cfg-crypto-trans)# exit

R3(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R3(cfg-crypto-trans)# exit
```

What is the function of the IPsec transform set?

_____

_____

_____

_____

c. You can also change the IPsec security association life times from the default of 3600 seconds. On R1 and R3, set the IPsec security association life time to 30 minutes, or **1800** seconds.

```
R1(config)# crypto ipsec security-association lifetime seconds 1800

R3(config)# crypto ipsec security-association lifetime seconds 1800
```

Step 6: Define interesting traffic.

To make use of the IPsec encryption with the VPN, it is necessary to define extended access lists to tell the router which traffic to encrypt. A packet that is permitted by an access list used for defining IPsec traffic is encrypted if the IPsec session is configured correctly. A packet that is denied by one of these access lists is not dropped, but sent unencrypted. Also, like any other access list, there is an implicit deny at the end, which, in this case, means the default action is to not encrypt traffic. If there is no IPsec security association correctly configured, no traffic is encrypted, and traffic is forwarded as unencrypted.

In this scenario, the traffic you want to encrypt is traffic going from R1's Ethernet LAN to R3's Ethernet LAN, or vice versa. These access lists are used outbound on the VPN endpoint interfaces and must mirror each other.

a. Configure the IPsec VPN interesting traffic ACL on R1.

```
R1(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
```

b. Configure the IPsec VPN interesting traffic ACL on R3.

```
R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255
```

Does IPsec evaluate whether the access lists are mirrored as a requirement to negotiate its security association?

_____

_____

_____

Step 7: Create and apply a crypto map.

A crypto map associates traffic that matches an access list to a peer and various IKE and IPsec settings. After the crypto map is created, it can be applied to one or more interfaces. The interfaces that it is applied to should be the ones facing the IPsec peer.

To create a crypto map, use **crypto map name sequence-num type** command in global configuration mode to enter crypto map configuration mode for that sequence number. Multiple crypto map statements can belong to the same crypto map and are evaluated in ascending numerical order. Enter crypto map

configuration mode on R1. Use a type of ipsec-isakmp, which means IKE is used to establish IPsec security associations.

a. Create the crypto map on R1, name it **CMAP**, and use **10** as the sequence number. A message displays after the command is issued.

```
R1(config)# crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
```

b. Use the **match address access-list** command to specify which access list defines which traffic to encrypt.

```
R1(config-crypto-map)# match address 101
```

c. To view the list of possible **set** commands that you can do in a crypto map, use the help function.

```
R1(config-crypto-map)# set ?
  identity              Identity restriction.
  ip                    Interface Internet Protocol config commands
  isakmp-profile        Specify isakmp Profile
  nat                   Set NAT translation
  peer                  Allowed Encryption/Decryption peer.
  pfs                   Specify pfs settings
  reverse-route         Reverse Route Injection.
  security-association  Security association parameters
  transform-set         Specify list of transform sets in priority order
```

d. Setting a peer IP or hostname is required. Set it to R3's remote VPN endpoint interface using the following command.

```
R1(config-crypto-map)# set peer 10.2.2.1
```

e. Hard code the transform set to be used with this peer, using the **set transform-set tag** command. Set the perfect forwarding secrecy type using the **set pfs type** command, and also modify the default IPsec security association life time with the **set security-association lifetime seconds seconds** command.

```
R1(config-crypto-map)# set pfs group5
R1(config-crypto-map)# set transform-set 50
R1(config-crypto-map)# set security-association lifetime seconds 900
R1(config-crypto-map)# exit
```

f. Create a mirrored matching crypto map on R3.

```
R3(config)# crypto map CMAP 10 ipsec-isakmp
R3(config-crypto-map)# match address 101
R3(config-crypto-map)# set peer 10.1.1.1
R3(config-crypto-map)# set pfs group5
R3(config-crypto-map)# set transform-set 50
R3(config-crypto-map)# set security-association lifetime seconds 900
R3(config-crypto-map)# exit
```

g. The last step is applying the crypto map to interfaces.

Note: The security associations (SAs) are not established until the crypto map has been activated by interesting traffic. The router generates a notification that crypto is now on.

Apply the crypto maps to the appropriate interfaces on R1 and R3.

```
R1(config)# interface S0/0/0
```

```
R1(config-if)# crypto map CMAP
*Jan 28 04:09:09.150: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config)# end

R3(config)# interface S0/0/1
R3(config-if)# crypto map CMAP
*Jan 28 04:10:54.138: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config)# end
```

Task 2: Verify the Site-to-Site IPsec VPN Configuration.

Step 1: Verify the IPsec configuration on R1 and R3.

a. Previously, you used the **show crypto isakmp policy** command to display the configured ISAKMP policies on the router. Similarly, the **show crypto ipsec transform-set** command displays the configured IPsec policies in the form of the transform sets.

```
R1# show crypto ipsec transform-set
Transform set 50: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },

R3# show crypto ipsec transform-set
Transform set 50: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

b. Use the **show crypto map** command to display the crypto maps that will be applied to the router.

```
R1# show crypto map
Crypto Map "CMAP" 10 ipsec-isakmp
        Peer = 10.2.2.1
        Extended IP access list 101
            access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
        Current peer: 10.2.2.1
        Security association lifetime: 4608000 kilobytes/900 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): Y
        DH group:  group5
        Transform sets={
                50:  { esp-256-aes esp-sha-hmac  } ,
```

```
        }
        Interfaces using crypto map CMAP:
                Serial0/0/0

R3# show crypto map
Crypto Map "CMAP" 10 ipsec-isakmp
        Peer = 10.1.1.1
        Extended IP access list 101
            access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
        Current peer: 10.1.1.1
        Security association lifetime: 4608000 kilobytes/900 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): Y
        DH group:  group5
        Transform sets={
                50:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map CMAP:
                Serial0/0/1
```

Note: The output of these **show** commands does not change if interesting traffic goes across the connection. You test various types of traffic in the next task.

Task 3: Verify the IPsec VPN Operation.

Step 1: Display isakmp security associations.

The **show crypto isakmp sa** command reveals that no IKE SAs exist yet. When interesting traffic is sent, this command output changes.

```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

IPv6 Crypto ISAKMP SA
```

Step 2: Display IPsec security associations.

The **show crypto ipsec sa** command shows the unused SA between R1 and R3.

Note: The number of packets sent across and the lack of any security associations listed toward the bottom of the output. The output for R1 is shown here.

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: CMAP, local addr 10.1.1.1

   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): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
```

```
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

 local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.2.2.1
 path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
 current outbound spi: 0x0(0)
 PFS (Y/N): N, DH group: none

 inbound esp sas:

 inbound ah sas:

 inbound pcp sas:

 outbound esp sas:

 outbound ah sas:

 outbound pcp sas:
```

Why have no SAs been negotiated?

_____

_____

_____

Step 3: Generate some uninteresting test traffic and observe the results.

a. Ping from R1 to the R3 S0/0/1 interface IP address **10.2.2.1**. These pings should be successful.

b. Issue the **show crypto isakmp sa** command.

c. Ping from R1 to the R3 Fa01 interface IP address **192.168.3.1**. These pings should be successful.

d. Issue the **show crypto isakmp sa** command again. Was an SA created for these pings? Explain.

_____

_____

_____

e. Issue the **debug ip ospf hello** command. You should see OSPF hello packets passing between R1 and R3.

```
R1# debug ip ospf hello
OSPF hello events debugging is on
R1#
*Apr  7 18:04:46.467: OSPF: Send hello to 224.0.0.5 area 0 on FastEthernet0/1 from
192.168.1.1
*Apr  7 18:04:50.055: OSPF: Send hello to 224.0.0.5 area 0 on Serial0/0/0 from
10.1.1.1
*Apr  7 18:04:52.463: OSPF: Rcv hello from 10.2.2.2 area 0 from Serial0/0/0 10.1.1.2
```

```
*Apr  7 18:04:52.463: OSPF: End of hello processing
*Apr  7 18:04:55.675: OSPF: Send hello to 224.0.0.5 area 0 on FastEthernet0/1 from
192.168.1.1
*Apr  7 18:04:59.387: OSPF: Send hello to 224.0.0.5 area 0 on Serial0/0/0 from
10.1.1.1
*Apr  7 18:05:02.431: OSPF: Rcv hello from 10.2.2.2 area 0 from Serial0/0/0 10.1.1.2
*Apr  7 18:05:02.431: OSPF: End of hello processing
```

f. Turn off debugging with the **no debug ip ospf hello** or **undebug all** command.

g. Re-issue the **show crypto isakmp sa** command. Was an SA created between R1 and R3? Explain.

_____

_____

_____

Step 4: Generate some interesting test traffic and observe the results.

a. Use an extended ping from R1 to the R3 Fa01 interface IP address **192.168.3.1**. Extended ping allows you to control the source address of the packets. Respond as shown in the following example. Press **Enter** to accept the defaults, except where a specific response is indicated.

```
R1# ping
Protocol [ip]:
Target IP address: 192.168.3.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.1.1
..!!!
Success rate is 100 percent (3/5), round-trip min/avg/max = 92/92/92 ms
```

b. Re-issue the **show crypto isakmp sa** command.

```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.2.2.1        10.1.1.1        QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

Why was an SA created between R1 and R3 this time?

_____

_____

_____

What are the endpoints of the IPsec VPN tunnel?

_____

_____

_____

c. Ping from PC-A to PC-C. If the pings were successful, issue the **show crypto ipsec sa** command. How many packets have been transformed between R1 and R3?

_____

_____

_____

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: CMAP, local addr 10.1.1.1

   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): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 2, #recv errors 0

     local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.2.2.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0xC1DD058(203280472)

     inbound esp sas:
      spi: 0xDF57120F(3747025423)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2005, flow_id: FPGA:5, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4485195/877)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:
```

```
inbound pcp sas:

outbound esp sas:
 spi: 0xC1DD058(203280472)
   transform: esp-256-aes esp-sha-hmac ,
   in use settings ={Tunnel, }
   conn id: 2006, flow_id: FPGA:6, crypto map: CMAP
   sa timing: remaining key lifetime (k/sec): (4485195/877)
   IV size: 16 bytes
   replay detection support: Y
   Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

d. The previous example used pings to generate interesting traffic. What other types of traffic would result in an SA forming and tunnel establishment?

_____

_____

_____

_____

_____

Part 3: Configure a Site-to-Site IPsec VPN with CCP

In Part 3, configure an IPsec VPN tunnel between R1 and R3 that passes through R2. Task 1 will restore the router to the basic settings using your saved configurations. In Task 2, configure R1 using Cisco CCP. In Task 3, mirror those settings to R3 using CCP utilities. Finally, review and test the resulting configuration.

Task 1: Restore Router R1 and R3 to the Basic Settings.

To avoid confusion as to what was entered in Part 2, start by restoring R1 and R3 to the basic configuration as described in Part 1 of this lab.

Step 1: Restore the basic configuration.

a. Connect to the R1 console using the **ciscoconpass** password.

b. Enter privileged EXEC mode.

c. Reload the router and enter **no** when prompted to save the configuration.

```
R1# reload

System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]
```

d. Connect to the R1 console using the **ciscoconpass** password.

e. Enter privileged EXEC mode.

f. Repeat on R3.

Step 2: Verify connectivity.

Test connectivity by pinging from host PC-A to PC-C. If the pings are unsuccessful, troubleshoot the router and PC configurations before continuing.

Task 2: Configure IPsec VPN Settings on R1 Using CCP.

Step 1: Configure a username and password pair and enable HTTP router access.

a. From the CLI, configure a username **admin** and password **cisco12345** to use with CCP on R1 and R3.

```
R1(config)# username admin privilege 15 secret cisco12345

R3(config)# username admin privilege 15 secret cisco12345
```

b. Enable the secure HTTP server on R1 and R3.

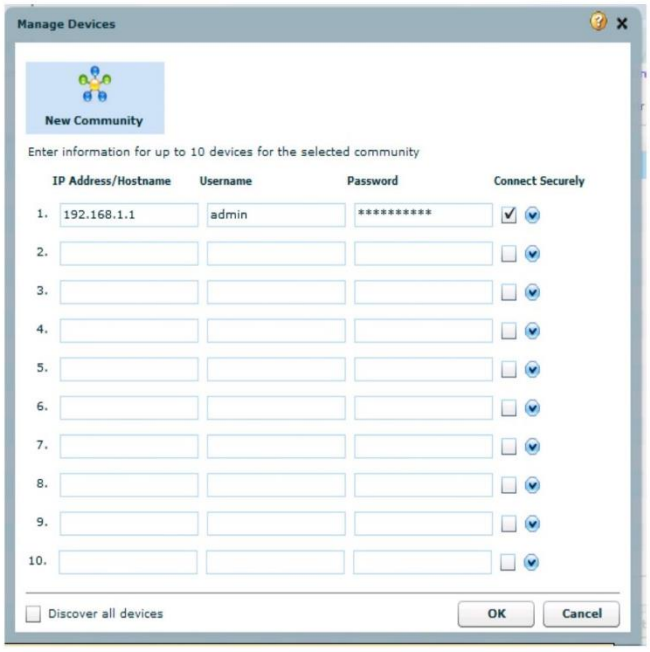
```
R1(config)#ip http secure-server

R3(config)#ip http secure-server
```

c. Configure local database authentication of web sessions to support CCP connectivity.

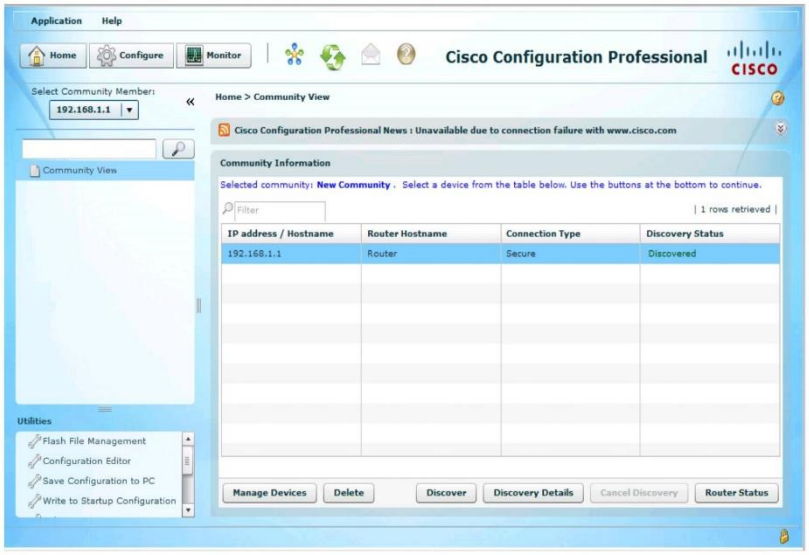
```
R1(config)# ip http authentication local

R3(config)# ip http authentication local
```

Step 2: Access CCP and discover R1.

a. Run the CCP application on PC-A. In the Select/Manage Community window, in the Hostname/Address field, enter the R1 IP address **192.168.1.1**, in the Username field, enter **admin**, and in the Password field, **cisco12345**. Click the **Connect Securely** check box, and then click **OK**.



b. At the CCP Dashboard, click **Discover** to discover and connect to R1. If the discovery process fails, click **Discover Details** to determine the problem and resolve the issue.



Step 3: Start the CCP VPN wizard to configure R1.

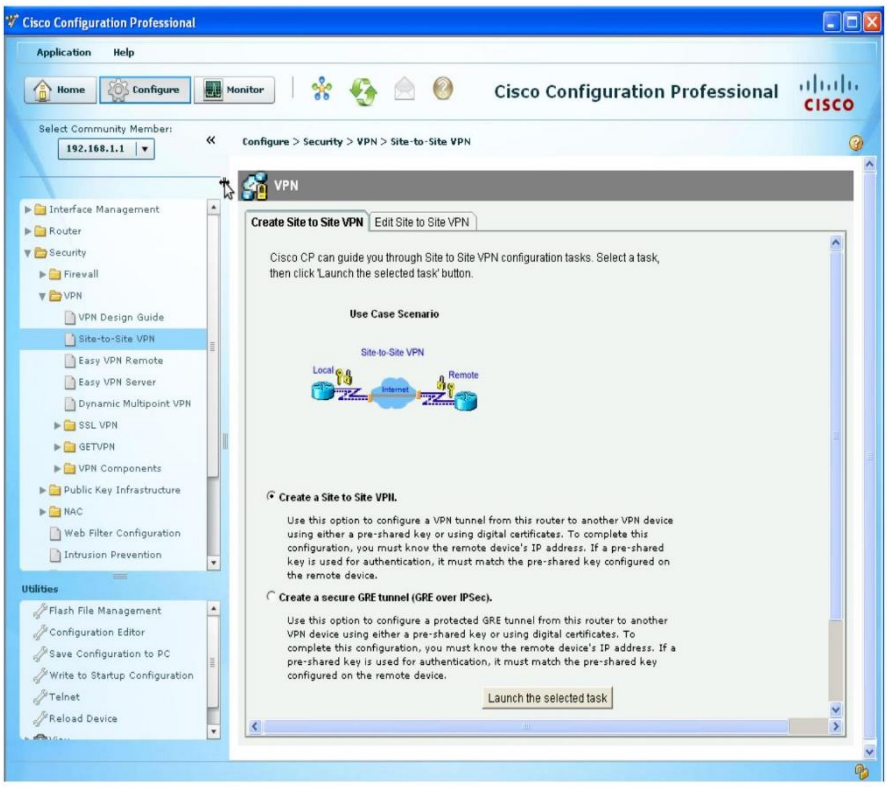
a. On the CCP menu bar, click **Configure**, and click **Security** > **VPN** > **Site-to-Site VPN**. Read through the description of this option.

What must you know to complete the configuration?

_____

_____

_____



b. Click **Launch the selected task** to begin the CCP Site-to-Site VPN wizard.

c. On the initial Site-to-Site VPN Wizard window, the **Quick Setup** option is selected by default. Click **View Defaults** to see what settings this option uses. What type of encryption does the default transform set use?

_____

d. In the initial Site-to-Site VPN wizard window, choose the **Step by Step wizard**, and then click **Next**. Why would you use this option over the Quick setup option?

_____

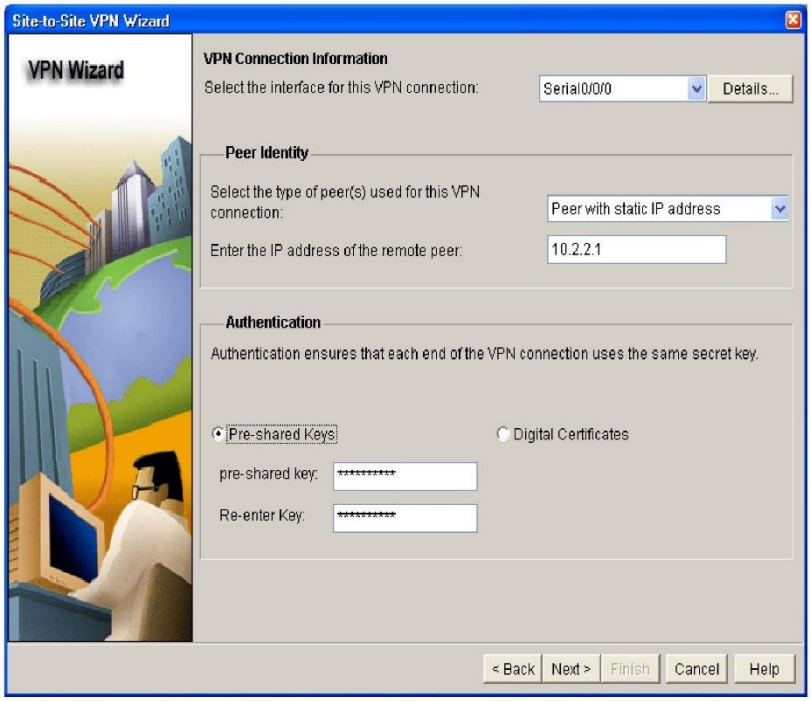
_____

Step 4: Configure basic VPN connection information settings.

a. In the VPN Connection Information window, select the interface for the connection, which should be R1 **Serial0/0/0**.

b. In the Peer Identity section, select **Peer with static IP address**, and enter the IP address of remote peer R3 S0/0/1 (**10.2.2.1**).

c. In the Authentication section, click **Pre-shared Keys**, and enter the pre-shared VPN key **cisco12345**. Re-enter the key for confirmation. This key authenticates the initial exchange to establish the Security Association between devices. When finished, your screen should look similar to the following. When you have entered these settings correctly, click **Next**.



Step 5: Configure IKE policy parameters.

IKE policies are used while setting up the control channel between the two VPN endpoints for key exchange. This is also referred to as the IKE SA. In contrast, the IPsec policy is used during IKE Phase II to negotiate an IPsec SA to pass target data traffic.

a. In the IKE Proposals window, a default policy proposal is displayed. You can use this one or create a new one. What function does this IKE proposal serve?

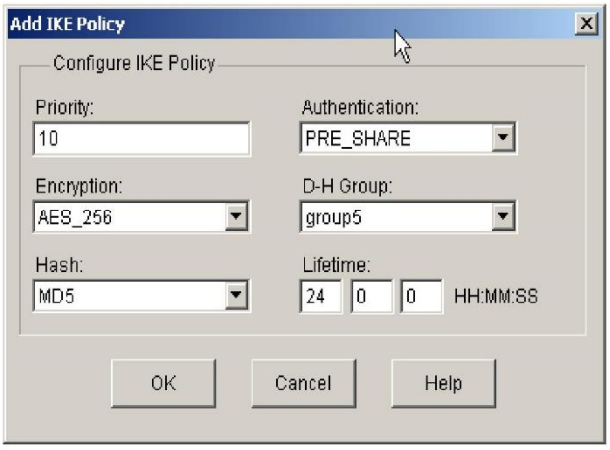
_____

_____

_____

b. Click **Add** to create a new IKE policy.

c. Set up the security policy as shown in the Add IKE Policy dialog box. These settings are matched later on R3. When finished, click **OK** to add the policy, and click **Next**.



d. For assistance in answering the following questions, click **Help**. What is the function of the encryption algorithm in the IKE policy?

What is the purpose of the hash function?

What function does the authentication method serve?

How is the Diffie-Hellman group in the IKE policy used?

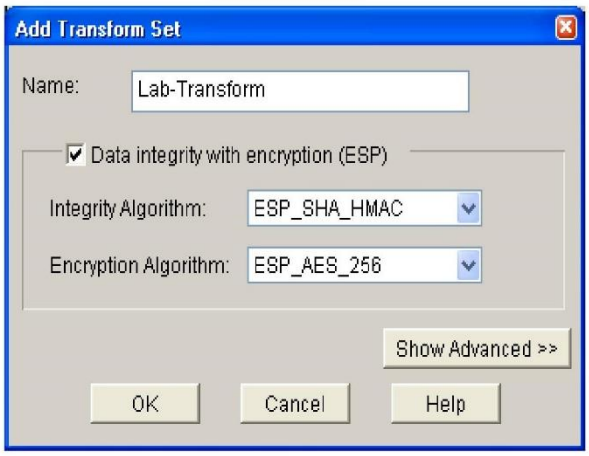
What event happens at the end of the IKE policy's lifetime?

Step 6: Configure a transform set.

The transform set is the IPsec policy used to encrypt, hash, and authenticate packets that pass through the tunnel. The transform set is the IKE Phase 2 policy.

a. A CCP default transform set is displayed. Click **Add** to create a new transform set.

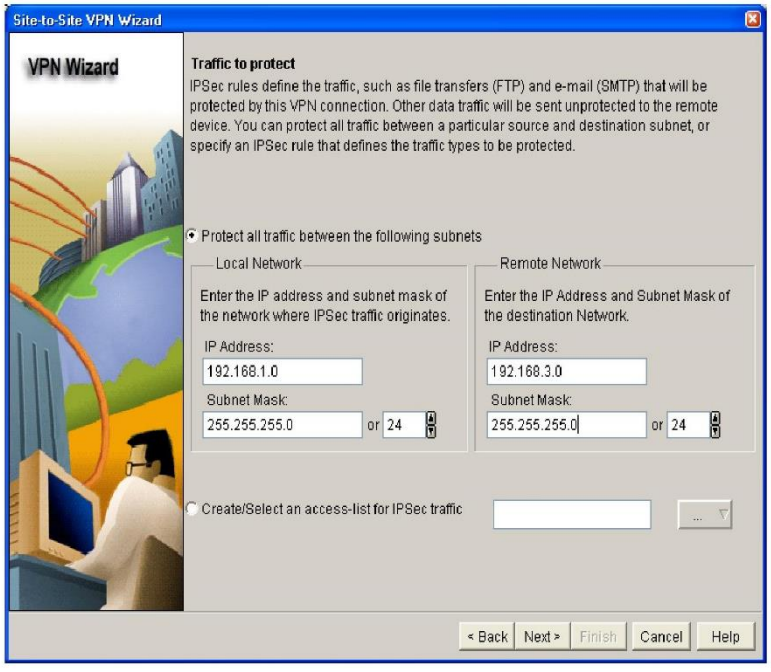
b. Set up the transform set, as shown in the Add Transform Set dialog box. These settings are matched later on R3. When finished, click **OK** to add the transform set, and click **Next**.



Step 7: Define interesting traffic.

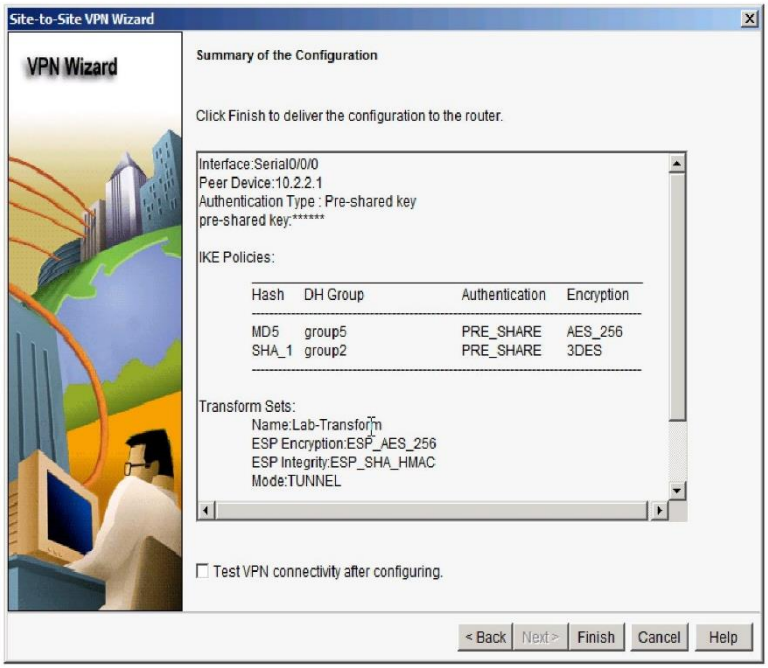
You must define interesting traffic to be protected through the VPN tunnel. Interesting traffic is defined through an access list applied to the router. By entering the source and destination subnets that you would like to protect through the VPN tunnel, CCP generates the appropriate simple access list for you.

In the Traffic to protect window, enter the information as shown below. These are the opposite of the settings configured on R3 later in the lab. When finished, click **Next**.



Step 8: Review the summary configuration and deliver commands to the router.

a. Review the Summary of the Configuration window. It should look similar to the one below. Do not click the **Test VPN connectivity after configuring** check box. This is done after configuring R3. Click **Finish** to continue.



b. In the Deliver Configuration to router window, click **Deliver**. After the commands have been delivered, click **OK**. How many commands were delivered?

_____

Task 3: Create a Mirror Configuration for R3.

Step 1: Use CCP on R1 to generate a mirror configuration for R3.

a. On R1, on the CCP menu bar, click **Configure**, and then click **Security** > **VPN** > **Site-to-Site VPN**. Select the **Edit Site to Site VPN** tab. You should see the VPN configuration listed that you just created on R1. What is the description of the VPN?

_____

b. What is the status of the VPN and why?

_____

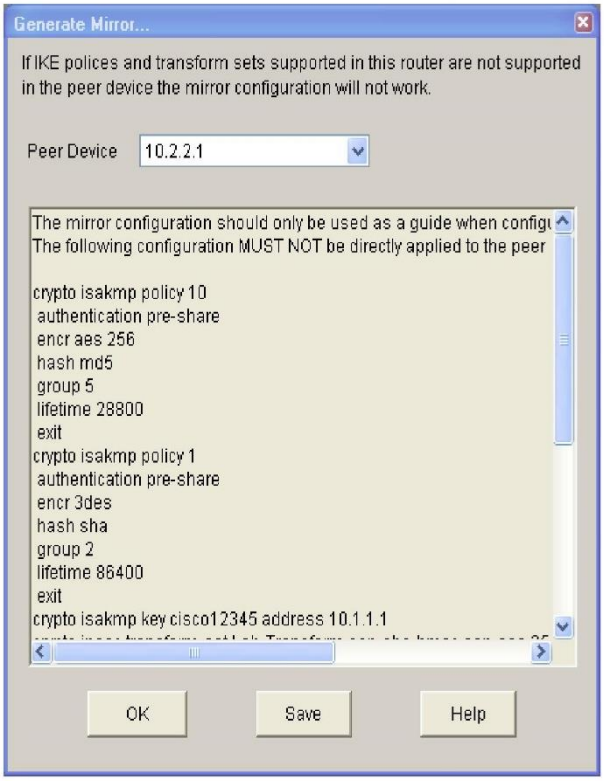
_____

_____

_____

_____

c. Select the VPN policy you just configured on R1 and click **Generate Mirror**. The Generate Mirror window displays the commands necessary to configure R3 as a VPN peer. Scroll through the window to see all the commands generated.



The text at the top of the window states that the configuration generated should only be used as a guide for setting up a site-to-site VPN. What commands are missing to allow this crypto policy to function on R3?

_____

_____

Hint: Look at the description entry following the **crypto map SDM_CMAP_1** command.

Step 2: Save the configuration commands for R3.

a. Click **Save** to create a text file for use in the next task.

b. Save the commands to the desktop or other location and name it **VPN-Mirror-Cfg-for-R3.txt**.

Note: You can also copy the commands directly from the Generate Mirror window.

c. (Optional) Edit the file to remove the explanation text at the beginning and the description entry following the **crypto map SDM_CMAP_1** command.

Task 4: Apply the Mirror Configuration to R3 and Verify the Configuration.

Step 1: Access the R3 CLI and copy the mirror commands.

Note: You can also use CCP on R3 to create the appropriate VPN configuration, but copying and pasting the mirror commands generated from R1 is easier.

NETLAB+ Note: If you are using NETLAB+, Telnet into R3 (**10.2.2.1**) from PC-A to paste the commands generated for R3 using CCP. Use the **terminal monitor** command to view messages during Telnet session.

a. On R3, enter privileged EXEC mode and then global configuration mode.

b. Copy the commands from the text file into the R3 CLI.

Step 2: Apply the crypto map to the R3 S0/0/1 interface.

```
R3(config)# interface S0/0/1
R3(config-if)# crypto map SDM_CMAP_1
*Jan 30 13:00:38.184: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Step 3: Verify the VPN configuration on R3 using Cisco IOS.

a. Display the running configuration beginning with the first line that contains the string "0/0/1" to verify that the crypto map is applied to S0/0/1.

```
R3# show run | begin 0/0/1
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 crypto map SDM_CMAP_1
```

b. On R3, use the **show crypto isakmp policy** command to show the configured ISAKMP policies on the router.

Note: The default CCP policy is also present.

```
R3# show crypto isakmp policy
Global IKE policy
Protection suite of priority 1
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit

Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
```

c. In the above output, how many ISAKMP policies are there?

_____

_____

_____

d. Issue the **show crypto ipsec transform-set** command to display the configured IPsec policies in the form of the transform sets.

```
R3# show crypto ipsec transform-set
Transform set Lab-Transform: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },
```

```
Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

e. Use the **show crypto map** command to display the crypto maps that will be applied to the router.

```
R3# show crypto map
Crypto Map "SDM_CMAP_1" 1 ipsec-isakmp
        Description: Apply the crypto map on the peer router's interface having IP
address 10.2.2.1 that connects to this router.
        Peer = 10.1.1.1
        Extended IP access list SDM_1
            access-list SDM_1 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
        Current peer: 10.1.1.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                Lab-Transform:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map SDM_CMAP_1:
                Serial0/0/1
```

In the above output, the ISAKMP policy being used by the crypto map is the CCP default policy with sequence number priority 1, indicated by the number 1 in the first output line: `Crypto Map "SDM_CMAP_1" 1 ipsec-isakmp`. Why is it not using the one you created in the CCP session — the one shown with priority 10 in Step 3b above?

_____

_____

_____

f. (Optional) In Part 3 Task 2 Step 5, ISAKMP policy 10 was configured on R1, in addition to the default ISAKMP policy 1. Both policies were included in the VPN policy that was generated in Part 3, Task 3. You can force the routers to use the more stringent policy that you created by changing the crypto map references in the R1 and R3 router configurations. In this example, the default ISAKMP policy 1 was removed from both routers.

```
R1(config)# interface S0/0/0
R1(config-if)# no crypto map SDM_CMAP_1
R1(config-if)# exit
*Jan 30 17:01:46.099: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
R1(config)# no crypto map SDM_CMAP_1 1
R1(config)# crypto map SDM_CMAP_1 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)# description Tunnel to 10.2.2.1
R1(config-crypto-map)# set peer 10.2.2.1
R1(config-crypto-map)# set transform-set Lab-Transform
R1(config-crypto-map)# match address 100
R1(config-crypto-map)# exit
R1(config)#interface S0/0/0
R1(config-if)# crypto map SDM_CMAP_1
R1(config-if)#
```

```
*Jan 30 17:03:16.603: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

R3(config)# interface S0/0/1
R3(config-if)# no crypto map SDM_CMAP_1
R3(config-if)# exit
R3(config)# no crypto map SDM_CMAP_1 1
R3(config)# crypto map SDM_CMAP_1 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)# description Tunnel to 10.1.1.1
R3(config-crypto-map)# set peer 10.1.1.1
R3(config-crypto-map)# set transform-set Lab-Transform
R3(config-crypto-map)# match address SDM_1
R3(config-crypto-map)# exit
R3(config)# interface S0/0/1
R3(config-if)# crypto map SDM_CMAP_1
R3(config-if)#
*Jan 30 22:18:28.487: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Task 5: Test the VPN Configuration Using CCP on R1.

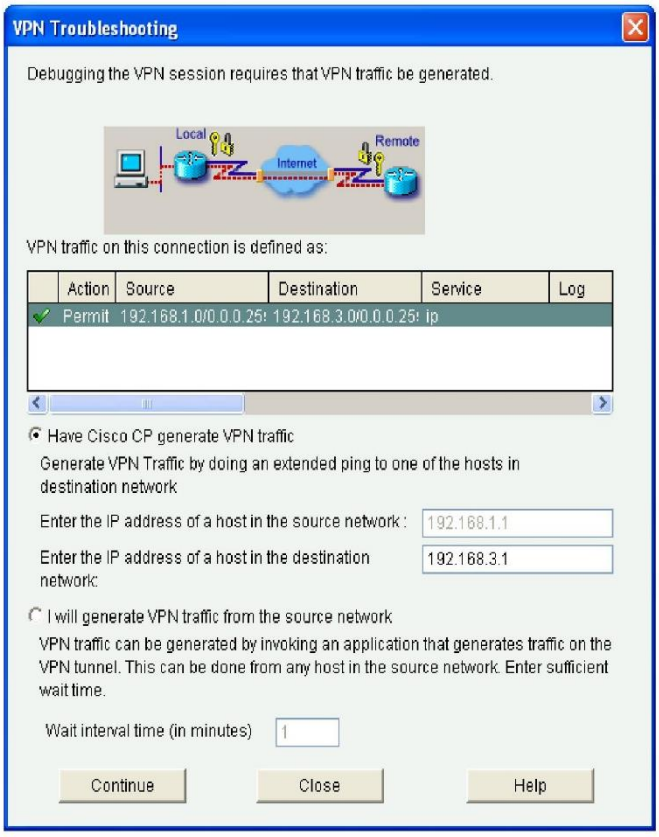
a. On PC-A, use CCP to test the IPsec VPN tunnel between the two routers. Click **Security** > **VPN** > **Site-to-Site VPN**, and then select the **Edit Site-to-Site VPN** tab.

b. On the Edit Site to Site VPN tab, select the VPN and click **Test Tunnel**.

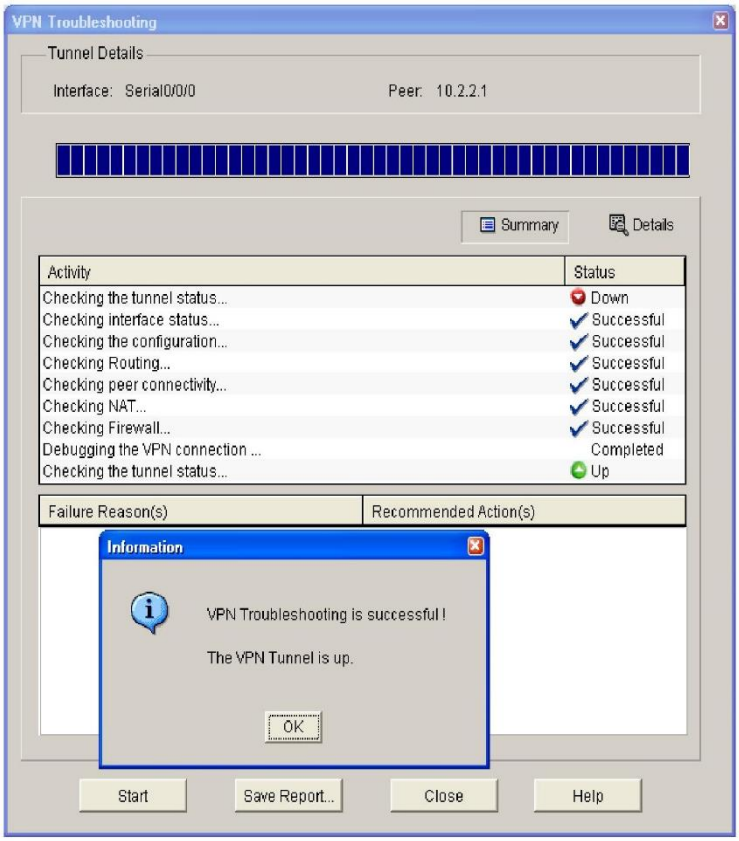
c. When the VPN Troubleshooting window displays, click **Start** to enable CCP to troubleshoot the tunnel.

d. When the CCP Warning window displays indicating that CCP will enable router debugs and generate some tunnel traffic, click **Yes** to continue.

e. In the next VPN Troubleshooting window, the IP address of the R1 Fa0/1 interface in the source network is displayed by default (192.168.1.1). Enter the IP address of the R3 Fa0/1 interface in the destination network field (**192.168.3.1**), and click **Continue** to begin the debugging process.



f. If the debug is successful and the tunnel is up, you should see the screen below. If the testing fails, CCP displays failure reasons and recommended actions. Click **OK** to remove the window.



g. You can save the report if desired; otherwise, click **Close**.

Note: To reset the tunnel and test again, click **Clear Connection** in the Edit Suite-to-Site VPN window. This can also be accomplished at the CLI using the **clear crypto session** command.

h. Issue the **show run interface s0/0/1** command to verify that the crypto map is applied to S0/0/1.

```
R3# show run interface s0/0/1
Building configuration...

Current configuration : 89 bytes
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 crypto map SDM_CMAP_1
end
```

i. Issue the **show crypto isakmp sa** command on R3 to view the security association created.

```
R3# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.2.2.1        10.1.1.1        QM_IDLE           1001    0 ACTIVE

IPv6 Crypto ISAKMP SA
```

j. Issue the **show crypto ipsec sa** command. How many packets have been transformed between R1 and R3?

_____

```
R3# show crypto ipsec sa

interface: Serial0/0/1
    Crypto map tag: SDM_CMAP_1, local addr 10.2.2.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 10.1.1.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 116, #pkts encrypt: 116, #pkts digest: 116
    #pkts decaps: 116, #pkts decrypt: 116, #pkts verify: 116
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.2.2.1, remote crypto endpt.: 10.1.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1
     current outbound spi: 0x207AAD8A(544910730)

     inbound esp sas:
      spi: 0xAF102CAE(2937072814)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2007, flow_id: FPGA:7, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4558294/3037)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x207AAD8A(544910730)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:8, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4558294/3037)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE
```

```
outbound ah sas:

outbound pcp sas:
```

Reflection

1. Would traffic on the Fast Ethernet link between PC-A and the R1 Fa0/0 interface be encrypted by the site-to-site IPsec VPN tunnel? Explain.

_____

_____

_____

_____

_____

2. Compared to using the CCP VPN wizard GUI, what are some factors to consider when configuring site-to-site IPsec VPNs using the manual CLI?

_____

_____

_____

_____

_____

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.