UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL SISTEMAS Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

# ANÁLISIS COMPARATIVO DE TÉCNICAS DE CIFRADO UTILIZADAS EN LA CONFIDENCIALIDAD DE LA INFORMACIÓN EN UNA RED PRIVADA VIRTUAL

# TESIS DE GRADO

**PARA OBTENER EL TÍTULO DE:**
**INGENIERO DE SISTEMAS**

**AUTOR**
**Bach. Carlos Alberto Fernández Falen**

**ASESOR**
**Ing. Gilberto Martín Ampuero Pasco**

**LAMBAYEQUE – PERÚ**
**2017**

# PROYECTO DE TESIS:

# "ANÁLISIS COMPARATIVO DE TÉCNICAS DE CIFRADO UTILIZADAS EN LA CONFIDENCIALIDAD DE LA INFORMACIÓN EN UNA RED PRIVADA VIRTUAL"

**Bach. Carlos Alberto Fernández Falen**

**Responsable de Tesis.**

**Ing. Gilberto Martín Ampuero Pasco.**

**Patrocinador.**

.

# PROYECTO DE TESIS:

## "ANÁLISIS COMPARATIVO DE TÉCNICAS DE CIFRADO UTILIZADAS EN LA CONFIDENCIALIDAD DE LA INFORMACIÓN EN UNA RED PRIVADA VIRTUAL"

## MIEMBROS DEL JURADO

_____

**Mg. Ing. Robert Edgard Puican Gutierrez.**
**PRESIDENTE DE JURADO.**

_____

**Ing. César Augusto Guzmán Valle.**
**MIEMBRO DE JURADO.**

_____

**Ing. Roberto Carlos Arteaga Lora**
**MIEMBRO DE JURADO.**

**DEDICATORIA**

A mis queridos Padres: **Franco Fernández**, **Felicita Irene Falen** y a mis hermanos Elizabeth y Segundo Franco. Por su gran amor y apoyo incondicional, por enseñarme a ser responsable y luchar para seguir adelante, y sobretodo porque gracias a ellos he logrado esta meta.

Atte. Carlos Alberto Fernández Falen

## AGRADECIMIENTO

A Dios, por permitirme vivir y seguir el camino correcto, con objetivos claros, luchando por obtener lo que más quiero y por darme la oportunidad de que mi familia se sienta orgullosa de mis triunfos.

Al Ingeniero Martín Ampuero, mi asesor, quien me apoyo en la elaboración de éste proyecto de investigación.

Atte. Carlos Alberto Fernández Falen

# ÍNDICE

Contenido Página

DEDICATORIA…… 04

AGRADECIMIENTO…… 05

ÍNDICE…….. 06

ÍNDICE DE TABLAS…… 09

ÍNDICE DE ILUSTRACIONES…….. 09

ÍNDICE DE ANEXOS……..... 10

RESUMEN…… 11

ABSTRACT…… 12

INTRODUCCIÓN…….. 13

ASPECTO INFORMATIVO…… 15

**CAPITULO I…….** 16

**PLANTEAMIENTO DEL OBJETO DE ESTUDIO……** 17

1.1. Realidad Problemática…… 17

1.2. Formulación del Problema…….. 19

1.3. Objetivos…… 20

1.3.1. Objetivo General…… 20

1.3.2. Objetivos Específicos…….. 20

1.4. Justificación e Importancia…… 20

1.5. Hipótesis…… 20

**CAPITULO II……..** 23

**ANTECEDENTES DE OTRAS INVESTIGACIONES……..** 24

2.1. Estado del arte…….. 25

2.2. Bases teórico científico…… 27

2.2.1. Red Privada Virtual…… 27

2.2.2. Seguridad…… 30

2.2.3. Criptografía…….. 33

2.2.4. Algoritmo Criptográfico…….. 34

2.2.4.1. Algoritmos Criptográficos Simétricos…… 36

2.2.4.2. Algoritmos Criptográficos Asimétricos……. 43

2.2.4.3. Algoritmos Criptográficos Hash…… 45

2.2.5. Protocolo L2TP…… 50

2.2.6. Librerías para algoritimos de encriptación……. 52
2.2.7. Autenticación…….. 53
2.3. Definición de términos básicos…….. 54
2.3.1. Algoritmo…… 54
2.3.2. Ataque informático…… 54
2.3.3. Criptografía…… 55
2.3.4. Delito Informático…….. 55
2.3.5. Encriptación…….. 55
2.3.6. Esteganografía…… 55
2.3.7. Red privada virtual…… 56
2.3.8. Seguridad…… 56
2.3.9. Técnicas de encriptación…….. 56
2.4. Caracteristicas de funcionamiento y aplicaciones de las redes privadas virtuales……. 57
2.4.1. Introducción…… 57
2.5. Funcionamiento y Caracteristicas…….. 59
2.6. Tipos de VPN's y sus aplicaciones……. 62
2.6.1. Arquitectura de conexión VPN……. 62
2.6.1.1. VPN de acceso remoto……. 62
2.6.1.2. VPN punto punto……..... 63
2.6.1.3. VPN interna VLAN…… 64
2.6.2. VPN basadas en internet o intranet……. 64
2.6.2.1. VPN basadas en internet…….. 64
2.6.2.1.1. Acceso remoto a través de internet.... 64
2.6.2.1.2. Acceso de redes a través de internet.. 65
2.6.2.2. VPN basadas en intranet……. 66
2.6.2.2.1. Acceso remoto a través de intranet.... 66
2.6.2.2.2. Acceso de redes a través de intranet.. 67
2.6.2.3. VPNs dinámicas……. 67
2.7. Protocolos usados por las VPNs…….. 68
2.7.1. Protocolo de túnel punto a punto (PPTP)……. 68
2.7.1.1. Encapsulación…… 69
2.7.2. Protocolo de túnel de capa 2…… 70

2.7.2.1. Encapsulación…… 70
2.7.2.1.1. Encapsulación L2TP…… 70
2.7.2.1.2. Encapsulación IPSec…… 70
2.7.3. IPSec…… 71
2.7.3.1. Definición…… 71
2.7.3.2. Arquitectura de seguridad…… 71
2.7.3.3. Estado actual de estándar…… 72
2.7.3.4. Propósito de diseño…….. 73
2.7.3.5. Modos…….. 74
2.7.3.5.1. Modo transporte…… 74
2.7.3.5.2. Modo túnel…… 74
2.7.3.6. Protocolos…….. 74
2.7.3.6.1. Authenticación header (AH)……. 75
2.7.3.6.2. Encapsulating Security Payload (ESP) 76
**CAPITULO III…… 78**
**Marco metodológico…….. 79**
3.1. Tipo y diseño de la investigación…….. 79
3.2. Población y muestra…… 79
3.3. Hipótesis…… 79
3.4. Operacionalización…….. 79
3.5. Métodos, técnicas y herramientas de recolección de datos……. 80
3.6. Procedimiento para la recolección de datos…… 80
3.7. Plan de análisis estadístico de datos…… 81
3.8. Criterios éticos…… 81
3.9. Criterios de rigos científico…….. 81
**CAPITULO IV…… 82**
4.1 Tipos de pruebas…… 83
4.2. Pruebas de rendimiento…… 83
4.2.1. Resultados…… 84
4.3. Pruebas de seguridad…….. 85
4.3.1. Resultados…….. 88
**CAPITULO V…… 93**
5.1. Implementación de VPN utilizando IPSec…….. 94

5.2. Instalación y configuración…….. 94
5.3. Discusión de resultados…….. 99
**CONCLUSIONES……. 101**
**RECOMENDACIONES…… 103**
**BIBLIOGRAFÍA…… 105**
**ANEXOS…… 107**

## INDICE DE TABLAS

Tabla 01: Características variable dependiente……..21
Tabla 02: Variable Dependiente-Rendimiento…….....80
Tabla 03: Rendimiento del sistema en modo túnel…….84
Tabla 04: Rendimiento del sistema en modo transporte……84
Tabla 05: Algoritmos para la transmisión segura de los datos……..96
Tabla 06: Técnicas de encriptación de datos en una red privada virtual……97
Tabla 07: Protocolos – Soluciones…….....98

## INDICE DE ILUSTRACIÓNES

Ilustración 1: Ataques malintencionados generados mediante PDF, Flash y Java.....17
Ilustración 2: Origen de la Criptografía…….....33
Ilustración 3: Clasificación de algoritmos criptográficos…….35
Ilustración 4: Estructura general de Feistel en DES……38
Ilustración 5: Ejemplo de matriz de estado con Nb=5 (160 bits). …….40
Ilustración 6: Ejemplo de clave con $N_k$=4 (128 bits). ……..40
Ilustración 7: AES SubBytes…….....42
Ilustración 8: AES ShiftRows…….....42
Ilustración 9: AES Mixcolumns…….....42
Ilustración 10: AES AddRoundKey…….....43
Ilustración 11: Funcionamiento del L2TP…….....51
Ilustración 12: Diseño de VPN de dos redes privadas a través del Internet. ……57
Ilustración 13: Equivalente lógico de una conexión VPN……...59
Ilustración 14: Túnel en una VPN…….....62
Ilustración 15: Un usuario remoto que establece un túnel con la oficina principal…….63
Ilustración 16: Conexión punto a punto…….....63
Ilustración 17: Acceso remoto a través de Internet…….65
Ilustración 18: Conexión de redes a través de Internet……..65
Ilustración 19: Acceso remoto a través de Intranet…….66

Ilustración 20: Conexión de redes a través de una intranet……...67
Ilustración 21: Encapsulación PPTP para una trama PPP……69
Ilustración 22: Encapsulación L2TP e IPSec para un datagrama PPP……71
Ilustración 23: Esquema físico de conexión…….....86
Ilustración 24: Tráfico SSH capturado sin túnel VPN……..86
Ilustración 25: Tráfico SSH capturado sin túnel VPN……87
Ilustración 26: Tráfico SSH capturado con túnel VPN……87
Ilustración 27: Tráfico SSH capturado con túnel VPN……88
Ilustración 28: Esquema físico de conexión…….....89
Ilustración 29: Tráfico FTP capturado sin túnel VPN…….....90
Ilustración 30: Tráfico FTP capturado sin túnel VPN……..90
Ilustración 31: Tráfico FTP capturado con túnel VPN……91
Ilustración 32: Tráfico FTP capturado con túnel VPN……91
Ilustración 33: Topología de conexión VPN…….....95

**ÍNDICE DE ANEXOS**

Anexo 01:
Configuración de servidor FTP en Linux Centos 6.5……108
Anexo 02:
Instalación y Configuración de Servidor VPN en Linux Centos 6.5……112
Anexo 03:
Instalación y Configuración de Cliente VPN…….....121
Anexo 04:
WIRESHARK…….....126

## RESUMEN

Se realizan pruebas de rendimiento y seguridad, en la primera se analiza el proceso de transferencia de archivos en el modelo cliente/servidor VPN, tomando en cuenta: distintas longitudes de archivos, utilizando formatos de archivos conocidos como pdf, docx, text e imágenes, se mide la carga del CPU, la tasa de transferencia, el tiempo promedio relativo, combinando los protocolos IPsec (AH, SEP) en modo túnel y modo transporte.

Además se realiza un análisis comparativo de los protocolos de seguridad, IPsec, SSH, SSL, utilizando dos escenarios primero utilizando un canal seguro VPN y el segundo sin utilizar el canal VPN. Para su implementación se utilizó el analizador de protocolos Wireshark, programas SSH y SSL.

## ABSTRACT

Performance and security tests are performed, the first one analyzes the process of file transfer in the VPN client / server model, taking into account: different file lengths, using file formats known as pdf, docx, text and images, the CPU load, the transfer rate, the relative average time are measured, combining the IPsec protocols (AH, SEP) in tunnel mode and transport mode.

In addition, a comparative analysis of security protocols, IPsec, SSH, SSL is performed, using two scenarios first using a secure VPN channel and the second without using the VPN channel. For its implementation, the Wireshark protocol analyzer, SSH and SSL programs were used.

# INTRODUCCIÓN

El ser humano se encuentra en la era de la información, y la computadora se ha convertido en el medio favorito para poder comunicarse. Todo tipo de organizaciones ya sea empresas pequeña y grande, universidades, institutos, gobierno, etc., requieren de métodos para poder transmitir información, de forma rápida, eficiente, segura y a un precio razonable. Esto lleva al desarrollo continuo de tecnologías de la información y actualización de las ya existentes con el fin de satisfacer las necesidades de dichas organizaciones en este mundo globalizado.

La seguridad es uno de los aspectos más desafiantes de la Internet y las aplicaciones de red, las cuales están creciendo muy rápido; por lo que la importancia y el valor de los datos intercambiados a través de Internet u otros tipos de medios están aumentando. De ahí la búsqueda de la mejor solución para ofrecer la protección necesaria contra ataques de intrusos a nuestros datos, junto con la prestación de estos servicios en el tiempo es uno de los temas más interesantes en las comunidades relacionadas con la seguridad.

La criptografía es una de las principales categorías de la seguridad informática que convierte la información de su forma normal en un formato ilegible. Las características principales que identifican y diferencian a los algoritmos de encriptación uno de otro son su capacidad para asegurar los datos protegidos contra ataques, su velocidad y eficiencia en hacerlo.

Las Redes Privadas Virtuales (VPN) constituyen una tecnología a la cual se le está dando cada vez mayor importancia puesto que permite la transmisión de información a grandes distancias sin necesidad de implementar una compleja y costosa infraestructura de red. Por lo cual la seguridad de los datos que se

transmiten es fundamental, esto se logra mediante el protocolo de TÚNEL, mecanismo por el cual se encapsula paquetes de protocolos arbitrarios, utilizando además, ciertos mecanismos para preservar la confidencialidad e integridad de los datos enviados.

Hablar de la confidencialidad de la información es garantizar que la información personal será protegida para que no sea divulgada sin consentimiento de la persona. Dicha garantía se lleva a cabo por medio de protocolos que limitan el acceso a ésta información.

En este sentido la criptografía es un pilar fundamental en la seguridad de la información, no solo en los archivos sino también en el medio de transporte, ya que permite ocultar el contenido de un mensaje con la aplicación de diferentes técnicas de encriptación. El presente estudio propone un análisis comparativo de las técnicas de encriptación en una red privada virtual, evaluando la eficiencia de dichas técnicas en el envío de la información a través de una red privada virtual, asegurando la confidencialidad de la información.

# ASPECTO INFORMATIVO

**1.1 Título del proyecto**

Análisis comparativo de técnicas de cifrado utilizadas en la confidencialidad de la información en una Red Privada Virtual

1.2 **Código del proyecto**: IS-2015-007

**1.3 Personal investigador**

1.3.1 Autor:

Fernández Falen, Carlos Alberto

1.3.2 Asesor

Ing. Gilberto Martín Ampuero Pasco
Profesor Asociado a tiempo completo
martinampuero@hotmail.com

**1.4 Escuela Profesional**

Ingeniería de Sistemas

**1.5 Orientación de la investigación**

1.5.1 Área de investigación

Desarrollo de Tecnologías e Innovación.

1.5.2 Línea de investigación

Tecnologías de la información y Comunicación (TIC).

**1.6 Localidad o Institución donde se realizará el proyecto**

Lambayeque

**1.7 Duración estimada**

5 meses

**1.8 Fecha de inicio**

Noviembre del 2016

# CAPITULO I

# PLANTEAMIENTO DEL OBJETO DE ESTUDIO

## 1.1. REALIDAD PROBLEMÁTICA

En la actualidad, las redes afrontan dos vertientes de erosión de la confianza, una es un descenso de la credibilidad de los clientes en la integridad de los productos; la otra, se resume en los numerosos indicios que apuntan a que los sujetos malintencionados están derrotando los mecanismos de confianza. De esta manera, se pone en duda la eficacia de las arquitecturas de autorización, autenticación y garantía de aplicaciones y redes. (Cisco, Informe Anual de Seguridad, 2013)

De todas las amenazas basadas en la Web que minan la seguridad, las vulnerabilidades del lenguaje de programación Java siguen constituyendo el objetivo más explotado por los criminales online, de acuerdo con los datos de Cisco.

Los datos de Sourcefire, que ahora forma parte de Cisco, también muestran que las vulnerabilidades de Java conforman la amplia mayoría (91%) de los indicadores de riesgo (IoC) que supervisa la solución FireAMP de Sourcefire, que está destinada a la protección frente al malware avanzado y a su análisis. (Cisco, Informe Anual de Seguridad, 2014).

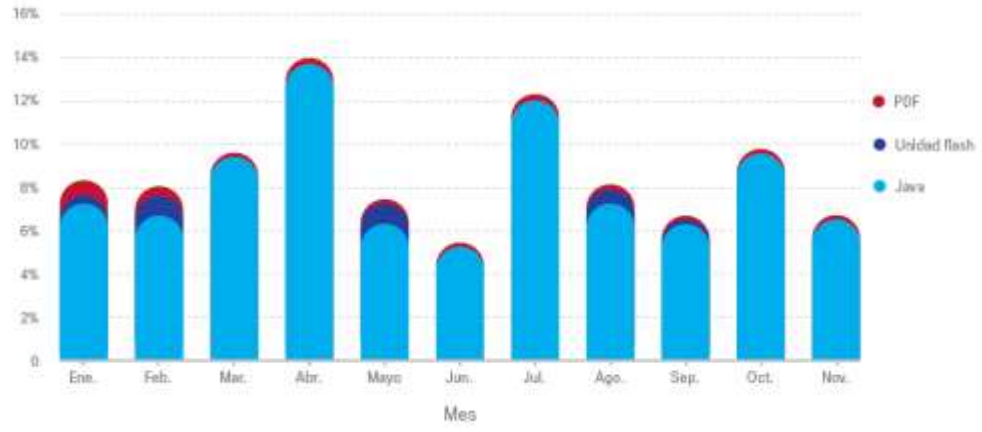



***Ilustración 1*** **- Ataques malintencionados generados mediante PDF, Flash y Java**

**Fuente: Informes de Cisco Cloud Web Security 2014**

En materia de seguridad informática, el 2014 está signado por una creciente preocupación de los usuarios en torno a la pérdida de privacidad en Internet. Además, el informe “Tendencias 2014 en Seguridad Informática” elaborado por los especialistas de ESET Latinoamérica, destaca la evolución del cibercrimen y

la diversificación del malware hacia otro tipo de dispositivos como los aspectos centrales en materia de Seguridad Informática para el próximo año. (Eset, 2013)

Las causas del por qué se da este tipo de problemas es por la masificación del uso de internet, las personas en la actualidad usan el Internet para realizar sus transacciones, no se le presta suficiente atención a la confidencialidad de la información del cliente, y una de las mayores causas es que el atacante encontró la vulnerabilidad del sistema, lo que ha llevado a los hackers a tener que robar nuestra información. Más aun cuando no tenemos un sistema seguro y es vulnerable. (Alonso, 2009)

Es en este contexto que surgen las redes privadas virtuales (VPN), como alternativa de bajo costo a servicios contratados dedicados de red de área amplia para las comunicaciones de datos, tanto para conectar redes distantes como usuarios remotos con la red de la organización, utilizando una infraestructura de comunicación de datos pública y compartida. (Alonso, 2009)

Las tecnologías de redes privadas virtuales han evolucionado para representar no solo una opción económica para las comunicaciones sino también como una solución complementaria para lograr eficiencia, velocidad, seguridad, confiabilidad en otros servicios de red de área amplia. (Alonso, 2009)

Las redes privadas virtuales utilizan una infraestructura compartida y pública para la interconexión, por lo que la seguridad de los datos que se transmiten es fundamental. En el contexto de una VPN esto se resuelve mediante un protocolo de túnel, es decir un mecanismo que es capaz de encapsular paquetes de protocolos arbitrarios, mediante el agregado de encabezados, utilizando además mecanismos para preservar la confidencialidad e integridad de los datos enviados. (Alonso, 2009)

Las redes privadas virtuales proporcionan el mayor nivel posible de seguridad mediante seguridad IP cifrada o IPsec o túneles VPN de Secure Sockets Layer (SSL) y tecnologías de autenticación. Estas tecnologías protegen los datos que pasan por la red privada virtual contra accesos no autorizados. (Padilla, 2014).

## 1.2. FORMULACIÓN DEL PROBLEMA

Las redes privadas virtuales de acceso remoto son el mecanismo ideal para extender o acercar los servicios de red local, en forma completa o parcial, a los usuarios itinerantes y tele trabajadores. Esta circunstancia dista de ser ideal si no se tiene en cuenta, nuevamente, el aspecto seguridad respecto a validar a quién se conecta y de acuerdo a esto, que permisos y autorizaciones posee. Estas precauciones deben reflejar las políticas de seguridad de la información definidas previamente por la organización. (Alonso, 2009)

En la actualidad existe un incremento de las conexiones de banda ancha tanto en puntos de acceso comerciales como en los hogares. Este aumento se observa también en la capacidad de ancho de banda ofrecido. Esta situación beneficia la puesta en práctica de VPN de acceso remoto. Una actividad muy popular es el tele trabajo, que permite desde otra ubicación física contar con los recursos de la información que se poseen en la oficina. (Cisco, Informe Anual de Seguridad, 2014)

En su investigación (Hernández, 2012) estudia la criptografía de curvas elípticas que reduzcan el tiempo de cómputo de la multiplicación escalar.
Desde el punto de vista algorítmico, las curvas elípticas de Koblitz permiten que el cálculo de la multiplicación escalar pueda ser realizado rápidamente mediante la aplicación del endomorfismo de Frobenius, sin requerir el uso de doblados de puntos. Los resultados obtenidos de este trabajo de investigación ponen de manifiesto la aceleración obtenida en la paralelización de la multiplicación escalar, optimizando tanto algorítmicamente como con el uso de tecnologías recientes.

Es por ello que la presente investigación propone evaluar técnicas de encriptación para buscar una solución que balancee seguridad con facilidad de uso en los datos que se trasmiten en una red privada virtual VPN, planteando ***¿Cómo se puede determinar la eficiencia de los métodos de cifrado en un Red Privada Virtual?***

## 1.3. OBJETIVOS

### 1.3.1. OBJETIVO GENERAL

Analizar el funcionamiento de los principales protocolos de cifrado que hacen posible la creación de túneles dentro de una infraestructura pública, llamados accesos VPN y que permiten dar confidencialidad a los datos.

### 1.3.2 OBJETIVOS ESPECÍFICOS

- ✓ Análisis del funcionamiento básico y funcional de redes privadas virtuales (VPN).
- ✓ Analizar algoritmos para la transmisión segura de los datos en una Red Privada Virtual.
- ✓ Analizar las diversas técnicas de encriptación de datos en una red privada virtual.
- ✓ Evaluar la eficiencia de las técnicas criptográficas en la red privada virtual.

## 1.4. JUSTIFICACION E IMPORTANCIA

### 1.4.1 JUSTIFICACION

Con esta investigación se pone a disposición de la comunidad científica y tecnológica conocimientos sobre técnicas de encriptación que brinden confiabilidad a la empresa en el momento de enviar información; lo cual posibilita que se realicen nuevas investigaciones al respecto y así seguir avanzando en esta línea de investigación de manera tal que se pueda conseguir un nivel de confianza y seguridad en el envío de información a través de la VPN; brindando a la sociedad y a las empresas un sistema más seguro y por lo tanto mucha más confianza al momento de realizar sus transacciones. Económicamente tanto las empresas como las personas no se verán afectadas ya que se podrá contar con un sistema mucho más seguro.

## 1.5. HIPÓTESIS

Un análisis comparativo de las diferentes técnicas de cifrado permitirá determinar la eficiencia en la seguridad de una Red Privada Virtual.

## VARIABLES

**Variable Independiente**

Técnicas de encriptación

**Variable Dependiente**

La seguridad de la Red Privada Virtual

**Operacionalización**

**Tabla 01: Características variable dependiente.**

| VARIABLE DEPENDIENTE | DIMENSIONES | INDICADORES | TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS |
|---|---|---|---|
| Seguridad de la Red Privada Virtual | Medidas de rendimiento | Tiempo de procesamiento | Registrar la cantidad de segundos que tarda en encriptar cada algoritmo. |
| | | Costo de procesamiento | Costo de implementación del algoritmo |
| | Medida de Seguridad | Cantidad datos que se puede visualizar | Captura de datos en la VPN |

**Fuente: Creación propia**

## DISEÑO DE CONTRASTACIÓN DE LA HIPÓTESIS

**Validación:** Se validarán los instrumentos de recolección de datos.

**Contrastación:** Se contrastará la hipótesis a través de métodos estadísticos debido al diseño cuasi experimental.

## POBLACIÓN Y MUESTRA

**La población:** Base de datos de ataques a Red Privada Virtual.

**La Muestra:** Ataques de la base de datos dirigidos a redes privadas virtuales

## MATERIALES, TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Para la recolección de datos se utilizarán:

- **Observación**.
- **Técnicas:**

**Registro de observaciones:** Se usan para recopilar los datos de las pruebas del sistema propuesto y evidencia de las técnicas

- **Instrumento:**

  **Ficha de registro de eventos:** Este instrumento se usan para el registro de los eventos de las pruebas de aplicación de las técnicas.

## MÉTODOS Y PROCEDIMIENTOS PARA LA RECOLECCIÓN DE DATOS

El desarrollo de la presente investigación, se ha basado en la utilización de técnicas de Encriptación de datos:

- Recopilación de Datos
- Pre – Procesado.
- Criptografía.
- Resultados.

Se realizará mediante la puesta en ejecución de las técnicas usadas y evaluar el desempeño de cada una de ellas de acuerdo con los indicadores que se ha establecido.

# CAPITULO II

## ANTECEDENTES DE OTRAS INVESTIGACIONES

### *Encriptación RSA de archivos de texto*

Este trabajo de tesis se desarrolla en base a la programación en lenguaje Java para los algoritmos de encriptación RSA, que basa su seguridad en la dificultad de factorizar números primos muy grandes aunque como todo sistema de encriptación de clave pública, el RSA puede estar sujeto a ataques con el fin de obtener el mensaje original o descubrir la clave privada.

(Lomparte, 2005)

### *Seguridad VPN basada en la combinación de L2TP and IpSec*

Esta investigación está desarrollada para proporcionar un método de construcción de red privada virtual segura por la combinación de L2TP y IPSec con el fin de cumplir los requisitos de la transmisión segura de datos y mejorar la tecnología de seguridad VPN. La simulación y análisis demuestran que el método de construcción puede mejorar la seguridad de la transmisión de datos, y los resultados de la simulación de VPN es valioso para los profesionales de seguridad se refieren. (Li & Sun, 2012)

### *Adaptive Data Hiding Based on Visual Cryptography*

En esta investigación (Sciences, 2014) se utilizó un método basado en la criptografía visual y la estenografía con el objetivo de mejorar la seguridad y robustez de los datos. El método minimiza la perceptibilidad de la distorsión introducida en comparación con los métodos de indicador de píxeles. Cuatro parámetros a saber MSE, BPP y la capacidad de incrustación se utilizan como indicadores para la comparación. La criptografía visual con la estenografía proporciona MSE mínimo y máxima PSNR y capacidad de incrustación

moderada. Estos parámetros deciden la imperceptibilidad y robustez de la imagen y proporciona una mejor resistencia contra diversas formas de ataques.

## 2.1. Estado del Arte

***Diseño e integración de algoritmos criptográficos en sistemas empotrados sobre FPGA***

En este trabajo se integran implementaciones hardware de algoritmos criptográficos a la biblioteca OpenSSL la cual es utilizada por aplicaciones sobre el sistema operativo Linux para asegurar redes TCP/IP. Los algoritmos implementados son el AES y las funciones resumen SHA-1 y SHA-256. Estos algoritmos son implementados como coprocesadores del procesador MicroBlaze utilizando interfaces FSL para el intercambio de datos entre ellos. Estos coprocesadores son integrados dentro de la biblioteca OpenSSL considerando la naturaleza multitarea del sistema operativo Linux, por lo que se selecciona un mecanismo de sincronización para controlar el acceso a estos dispositivos. Además son presentados los resultados de velocidad alcanzados por los coprocesadores integrados en la biblioteca utilizando la herramienta speed de la misma. Finalmente es presentado el impacto de estos coprocesadores en la velocidad de transmisión a través de una red privada virtual utilizando la herramienta OpenVPN. (Aldaya, 2013)

***Implementación de la criptografía basada en atributos en un dispositivo móvil***

Esta tesis describe el análisis, el diseño y la implementación de una biblioteca de software eficiente, que compute emparejamientos bilineales de una manera eficaz sobre un dispositivo móvil equipado con un procesador ARM Cortex A9.

Asimismo, se describe el diseño e implementación del protocolo ABE utilizando la biblioteca desarrollada en este trabajo, y se presenta una aplicación demostrativa capaz de cifrar archivos a través del esquema ABE Criptografía Basada en Atributos como mecanismo de control de acceso.

La biblioteca criptográfica desarrollada genera tres funciones principales: el emparejamiento bilineal, la multiplicación escalar de puntos y la proyección de una cadena a un punto

(Ramírez, 2012)

***Análisis y mejora del rendimiento del algoritmo AES para su utilización en teléfonos móviles***

La presente tesis se enmarca dentro del estudio y desarrollo de algoritmos criptográficos para dispositivos móviles, enfocándose en el desarrollo de una mejora en la implementación del algoritmo AES en un dispositivo móvil con arquitectura ARM de 32 bits. Se realizó un análisis de los algoritmos más utilizados con respecto a su desempeño (en tiempo y seguridad) y tras elegir el algoritmo más idóneo (AES) se han aplicado diversas técnicas para mejorar su implementación de manera que se ahorren al máximo los recursos limitados que un dispositivo móvil posee.

Se concluyó que para lograr reducir el tiempo de procesamiento se debe aplicar técnicas específicas, como el Loop unrolling y transposición de matrices, con las que se ha conseguido reducir el tiempo de procesamiento en un aproximado de 50% en la operación de cifrado y un 80% en la operación de descifrado.

(Meza, 2014)

## 2.2. Bases teórico científico

### 2.2.1. Red Privada Virtual

Según (Alonso, 2009) una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

La conexión VPN a través de Internet es técnicamente una unión wide area network (WAN) entre los sitios pero al usuario le parece como si fuera un enlace privado— de allí la designación "virtual private network"

**Características básicas:**

- Autentificación y autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.

- Integridad: de que los datos enviados no han sido alterados. Para ello se utiliza funciones de Hash. Los algoritmos de hash más comunes son los Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA).
- Confidencialidad/Privacidad: Dado que sólo puede ser interpretada por los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard(DES), Triple DES (3DES) y Advanced Encryption Standard (AES).
- No repudio: es decir, un mensaje tiene que ir firmado, y quien lo firma no puede negar que envió el mensaje.
- Control de acceso: Se trata de asegurar que los participantes autenticados tiene acceso únicamente a los datos a los que están autorizados.
- Auditoria y registro de actividades: Se trata de asegurar el correcto funcionamiento y la capacidad de recuperación.
- Calidad del servicio: Se trata de asegurar un buen rendimiento, que no haya una degradación poco aceptable en la velocidad de transmisión.

**Tipos de VPN**

- **VPN de acceso remoto:** Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local

de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

- **VPN punto a punto:** Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales. Es más común es el también llamado tecnología de túnel o tunneling.
- **VPN over LAN:** Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

  Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

Otro ejemplo es la conexión a redes Wi-Fi haciendo uso de túneles cifrados IPSec o SSL que además de pasar por los métodos de autenticación tradicionales (WEP, WPA, direcciones MAC, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN interna o externa.

### 2.2.2. Seguridad

(Lucena Lopez, 2010) El concepto de seguridad en la información es mucho más amplio que la simple protección de los datos a nivel lógico. Para proporcionar una seguridad real hemos de tener en cuenta múltiples factores, tanto internos como externos. En primer lugar habría que caracterizar el sistema que va a albergar la información para poder identificar las amenazas, y en este sentido podríamos hacer la siguiente subdivisión:

- ✓ ***Sistemas aislados.*** Son los que no están conectados a ningún tipo de red. De unos años a esta parte se han convertido en minoría, debido al auge que ha experimentado Internet.
- ✓ ***Sistemas interconectados.*** Hoy por hoy casi cualquier ordenador pertenece a alguna red, enviando y recogiendo información del exterior casi constantemente.

  Esto hace que las redes de ordenadores sean cada día más complejas y supongan un peligro potencial que no puede en ningún caso ser ignorado.

En cuanto a las cuestiones de seguridad que hemos de fijar podríamos clasificarlas de la siguiente forma:

- ***Seguridad física***. Englobaremos dentro de esta categoría a todos los asuntos relacionados con la salvaguarda de los soportes físicos de la información, más que de la información propiamente dicha. En este nivel estarían, entre otras, las medidas contra incendios y sobrecargas eléctricas, la prevención de ataques terroristas, las políticas de copias de respaldo (backups), etc. También se suelen tener en cuenta dentro de este punto aspectos relacionados con la restricción de acceso físico a las computadoras únicamente a personas autorizadas.

- ***Seguridad de la información.*** En este apartado prestaremos atención a la preservación de la información frente a observadores no autorizados. Para ello podemos emplear tanto criptografía simétrica como asimétrica, estando la primera únicamente indicada en sistemas aislados, ya que si la empleáramos en redes, al tener que transmitir la clave por el canal de comunicación, estaríamos asumiendo un riesgo excesivo.

- ***Seguridad del canal de comunicación.*** Los canales de comunicación rara vez se consideran seguros. Debido a que en la mayoría de los casos escapan a nuestro control, ya que pertenecen a terceros, resulta imposible asegurarse totalmente de que no están siendo escuchados o intervenidos.

- ***Problemas de autentificación.*** Debido a los problemas del canal de comunicación, es necesario asegurarse de que la información que recibimos en la computadora viene de quien realmente creemos que viene, y que además no ha sido alterada. Para esto se suele emplear criptografía asimétrica en conjunción con funciones resumen (hash).

- ***Problemas de suplantación.*** En las redes tenemos el problema añadido de que cualquier usuario autorizado puede acceder al sistema desde fuera, por lo que hemos de confiar en sistemas fiables para garantizar que los usuarios no están siendo suplantados por intrusos. Para conseguir esto normalmente se emplean mecanismos basados en contraseñas.

- ***No repudio.*** Cuando se recibe un mensaje no sólo es necesario poder identificar de forma univoca al remitente, sino que éste asuma todas las responsabilidades derivadas de la información que haya podido enviar. En este sentido es fundamental impedir que el emisor pueda repudiar un mensaje, es decir, negar su autoría sobre él.

- ***Anonimato.*** Es, en cierta manera, el concepto opuesto al del no repudio. En determinadas aplicaciones, como puede ser un proceso electoral o la simple denuncia de violaciones de los derechos humanos en entornos dictatoriales, es crucial garantizar el anonimato del ciudadano para poder preservar su intimidad y su libertad. Es una característica realmente difícil de conseguir, y desafortunadamente no

goza de muy buena fama, especialmente en países donde prima la seguridad nacional sobre la libertad y la intimidad de los ciudadanos.

### 2.2.3. Criptografía

(Real Academia, 2010) La palabra criptografía proviene de la unión de los términos griegos (Del gr. κρυπτός, oculto, y -grafía), y su definición es: "Arte de escribir con clave secreta o de un modo enigmático".

Existen dos trabajos fundamentales sobre los que se apoya prácticamente toda la teoría criptográfica actual. Uno de ellos, desarrollado por (Claude, 1948) en sus artículos "A Mathematical Theory of Communication" y "Communication Theory of Secrecy Systems" (1949), sienta las bases de la Teoría de la Información y de la Criptografía moderna. El segundo, publicado por (Diffie & Hellman, 1976), se titulaba "New directions in Cryptography", e introducía el concepto de Criptografía Asimétrica, abriendo enormemente el abanico de aplicación de esta disciplina.

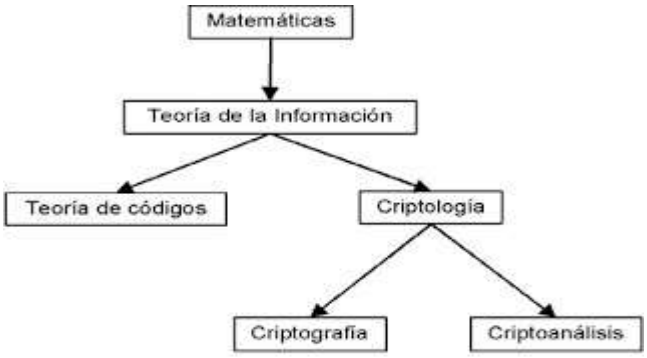



***Ilustración 2* - Origen de la Criptografía**

**Fuente: Según (Claude Elwood Shannon)**

Conviene hacer notar que la palabra Criptografía solo hace referencia al uso de códigos, por lo que no engloba a las técnicas que se usan para romper dichos códigos, conocidas en su conjunto como Criptoanálisis. En cualquier caso ambas disciplinas están íntimamente ligadas; no olvidemos que cuando se diseña un sistema para cifrar información, hay que tener muy presente su posible criptoanálisis, ya que en caso contrario podríamos llevarnos desagradables sorpresas.

### 2.2.4. Algoritmo criptográfico

Es un método matemático que se emplea para cifrar y descifrar un mensaje. Generalmente funciona empleando una o más claves (números o cadenas de caracteres) como parámetros del algoritmo, de modo que sean necesarias para recuperar el mensaje a partir de la versión cifrada.

El mensaje antes de cifrar se denomina texto en claro y una vez cifrado se denomina texto cifrado

**Clasificación de algoritmos criptográficos**

Según (Claude Elwood Shannon) los algoritmos criptográficos pueden ser clásicos o modernos. La criptografía clásica incluye la construcción de máquinas, que mediante mecanismos, comúnmente engranes o rotores, transformaban un mensaje en claro a un mensaje cifrado, como la máquina Enigma usada en la Segunda Guerra Mundial

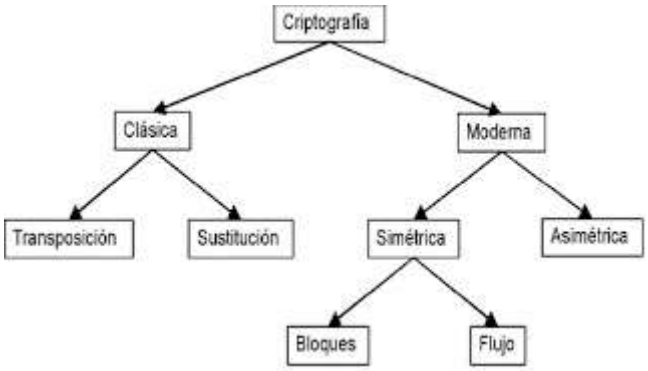



***Ilustración 3* - Clasificación de algoritmos criptográficos**

**Fuente: Según (Claude Elwood Shannon)**

Los algoritmos criptográficos modernos se clasifican en Simétricos y Asimétricos

La **criptografía simétrica**, también llamada criptografía de clave secreta o criptografía de una clave, es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.

La **criptografía asimétrica** también llamada criptografía de clave pública o criptografía de dos claves, es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la confidencialidad del envío del mensaje, nadie salvo el destinatario puede descifrarlo

#### 2.2.4.1. Algoritmos criptográficos simétricos

***Data Encryption Standard (DES)***

Es un algoritmo de cifrado escogido como un estándar FIPS en los Estados Unidos en 1976, y cuyo uso se ha propagado ampliamente por todo el mundo. El algoritmo fue controvertido al principio, con algunos elementos de diseño clasificados, una longitud de clave relativamente corta, y las continuas sospechas sobre la existencia de alguna puerta trasera para la National Security Agency (NSA). Posteriormente DES fue sometido a un intenso análisis académico y motivó el concepto moderno del cifrado por bloques y su criptoanálisis.

Hoy en día, DES se considera inseguro para muchas aplicaciones. Esto se debe principalmente a que el tamaño de clave de 56 bits es corto; las claves de DES se han roto en menos de 24 horas. Existen también resultados analíticos que demuestran debilidades teóricas en su cifrado, aunque son inviables en la práctica. Se cree que el algoritmo es seguro en la práctica en su variante de Triple DES, aunque existan ataques teóricos.

***Funcionamiento del algoritmo:***

La estructura básica del algoritmo aparece representada en la figura 4; hay 16 fases idénticas de proceso, denominadas rondas. También hay una permutación inicial y final denominada PI y PF, que son funciones inversas entre sí (PI "deshace" la acción de PF, y viceversa). PI y PF no son criptográficamente significativas, pero se incluyeron presuntamente para facilitar la carga y descarga de bloques sobre el hardware de mediados de los 70. Antes de las rondas, el bloque es dividido en dos mitades de 32 bits y procesadas alternativamente. Este entrecruzamiento se conoce como esquema Feistel.

La estructura de Feistel asegura que el cifrado y el descifrado sean procesos muy similares — la única diferencia es que las subclaves se aplican en orden inverso cuando desciframos. El resto del algoritmo es idéntico. Esto simplifica enormemente la implementación, en especial sobre hardware, al no haber necesidad de algoritmos distintos para el cifrado y el descifrado.

El símbolo rojo "⊕" representa la operación OR exclusivo (XOR). La función-F mezcla la mitad del bloque con parte de la clave. La salida de la función-F se combina entonces con la otra mitad del bloque, y los bloques son intercambiados antes de la siguiente ronda. Tras la última ronda, las mitades no se intercambian; ésta es una característica de la estructura de Feistel que hace que el cifrado y el descifrado sean procesos parecidos

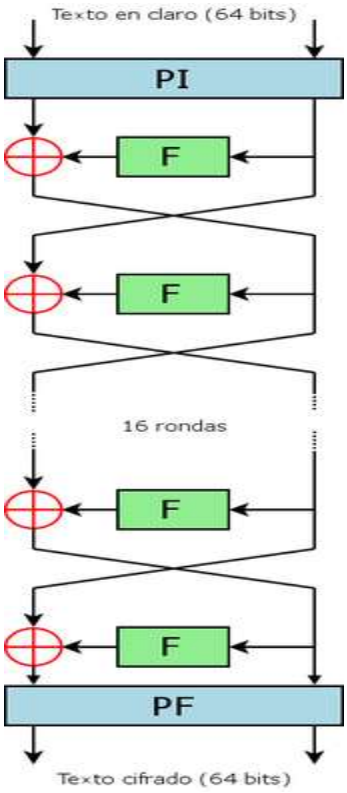



***Ilustración 4* - Estructura general de Feistel en DES**

**Fuente: Según (** (Wikipedia, 2014)

### Cuatro pasos de la función de Feistel

*Expansión* — la mitad del bloque de 32 bits se expande a 48 bits mediante la permutación de expansión, denominada E en el diagrama, duplicando algunos de los bits.

*Mezcla* — el resultado se combina con una subclave utilizando una operación XOR. Dieciséis subclaves — una para cada ronda — se derivan de la clave inicial mediante la generación de subclaves descrita más abajo.

*Sustitución* — tras mezclarlo con la subclave, el bloque es dividido en ocho trozos de 6 bits antes de ser procesados por las S-cajas, o cajas de sustitución. Cada una de las ocho S-cajas reemplaza sus seis bits de entrada con cuatro bits de salida, de acuerdo con una trasformación no

lineal, especificada por una tabla de búsqueda. Las S-cajas constituyen el núcleo de la seguridad de DES — sin ellas, el cifrado sería lineal, y fácil de romper.

*Permutación* — finalmente, las 32 salidas de las S-cajas se reordenan de acuerdo a una permutación fija; la P-caja

Alternando la sustitución de las S-cajas, y la permutación de bits de la P-caja y la expansión-E proporcionan las llamadas "confusión y difusión" respectivamente, un concepto identificado por Claude Shannon en los 40 como una condición necesaria para un cifrado seguro y práctico

**Estándar avanzado de Cifrado (AES)**

En octubre de 2000 el NIST (National Institute for Standards and Technology) anunciaba oficialmente la adopción del algoritmo Rijndael como nuevo Estándar Avanzado de Cifrado (AES) para su empleo en aplicaciones criptográficas no militares, culminando así un proceso de más de tres años, encaminado a proporcionar a la comunidad internacional un nuevo algoritmo de cifrado potente, eficiente, y fácil de implementar.

AES es un sistema de cifrado por bloques, diseñado para manejar longitudes de clave y de bloque variables, ambas comprendidas entre los 128 y los 256 bits. Realiza varias de sus operaciones internas a nivel de byte, interpretando éstos como elementos de un cuerpo de Galois GF ($2^8$). El resto de operaciones se efectúan en términos de registros de 32 bits. Sin embargo, en algunos casos, una secuencia de 32 bits se toma como

un polinomio de grado inferior a 4, cuyos coeficientes son a su vez polinomios en GF($2^8$).

AES, a diferencia de algoritmos como DES, no posee estructura de red de Feistel. En su lugar se ha definido cada ronda como una composición de cuatro funciones invertibles diferentes, formando tres capas, diseñadas para proporcionar resistencia frente a criptoanálisis lineal y diferencial. Cada una de las funciones tiene un propósito preciso:

- **La capa de mezcla lineal.** Funciones desplazar fila y mezclar columnas permite obtener un alto nivel de difusión a lo largo de varias rondas.
- **La capa no lineal.** Función ByteSub consiste en la aplicación paralela de s-cajas con propiedades óptimas de no linealidad.
- **La capa de adición de clave.** Es un simple or-exclusivo entre el estado intermedio y la sub clave correspondiente a cada ronda.

| | | | | |
|---|---|---|---|---|
| $a_{0,0}$ | $a_{0,1}$ | $a_{0,2}$ | $a_{0,3}$ | $a_{0,4}$ |
| $a_{1,0}$ | $a_{1,1}$ | $a_{1,2}$ | $a_{1,3}$ | $a_{1,4}$ |
| $a_{2,0}$ | $a_{2,1}$ | $a_{2,2}$ | $a_{2,3}$ | $a_{2,4}$ |
| $a_{3,0}$ | $a_{3,1}$ | $a_{3,2}$ | $a_{3,3}$ | $a_{3,4}$ |

*Ilustración 5:* Ejemplo de matriz de estado con Nb=5 (160 bits).
**Fuente: Según (** (Wikipedia, 2014)

| | | | |
|---|---|---|---|
| $k_{0,0}$ | $k_{0,1}$ | $k_{0,2}$ | $k_{0,3}$ |
| $k_{1,0}$ | $k_{1,1}$ | $k_{1,2}$ | $k_{1,3}$ |
| $k_{2,0}$ | $k_{2,1}$ | $k_{2,2}$ | $k_{2,3}$ |
| $k_{3,0}$ | $k_{3,1}$ | $k_{3,2}$ | $k_{3,3}$ |

*Ilustración 6:* Ejemplo de clave con $N_k$=4 (128 bits).
**Fuente: Según (** (Wikipedia, 2014)

AES utiliza claves de **128, 192 o 256 bits** de longitud, sobre bloques fijos de 16 bytes, lo que da como resultado bloques cifrados en la salida del mismo tamaño que en la entrada, 16 bytes.

Uno de los puntos destacados del AES es la manera en la que se aplica su clave **K** . En primer lugar, ésta se expande en un subconjunto formado por (**k0,k1,k2,… kn**), a cada una de ellas se le aplica una función round **r**(kn, ), que realiza una operación binaria **XOR** con el mensaje, es decir, el bloque de entrada es cifrado por cada una de las subclaves r( kn )hasta llegar al final.

En cada round, se llevan a cabo diferentes funciones de sustitución y permutación, por lo tanto se cambia el orden y estado inicial de los datos incluidos en el mensaje inicial. Este proceso debe ser reversible, para que el sistema sea capaz de desencriptar el mensaje.

**Funcionamiento técnico del algoritmo**

Expansión de la clave usando el esquema de claves de Rijndael.

- Etapa inicial:

  AddRoundKey

- Rondas:

  SubBytes — en este paso se realiza una sustitución no lineal donde cada byte es reemplazado con otro de acuerdo a una tabla de búsqueda.

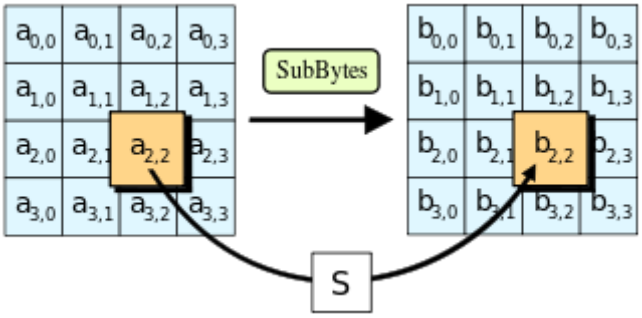



***Ilustración 7* - AES SubBytes**
**Fuente: Según (** (Wikipedia, 2014)

ShiftRows — en este paso se realiza una transposición donde cada fila del «state» es rotada de manera cíclica un número determinado de veces.

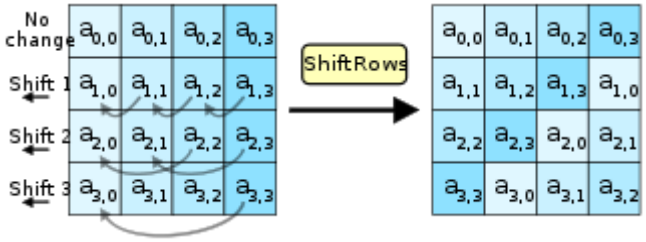



***Ilustración 8* - AES ShiftRows**
**Fuente: Según (** (Wikipedia, 2014)

MixColumns — operación de mezclado que opera en las columnas del «state», combinando los cuatro bytes en cada columna usando una transformación lineal.

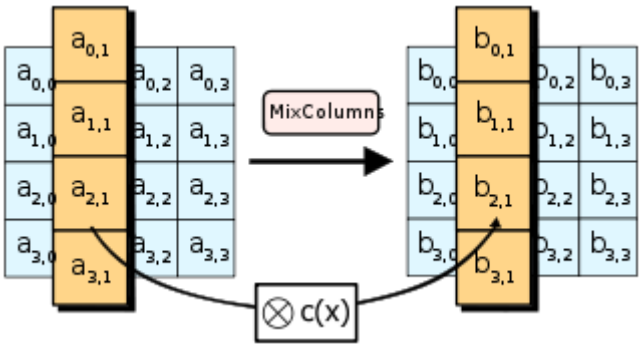



***Ilustración 9* - AES Mixcolumns**
**Fuente: Según (** (Wikipedia, 2014)

AddRoundKey — cada byte del «state» es combinado con la clave «round»; cada clave «round» se deriva de la clave de cifrado usando una iteración de la clave.

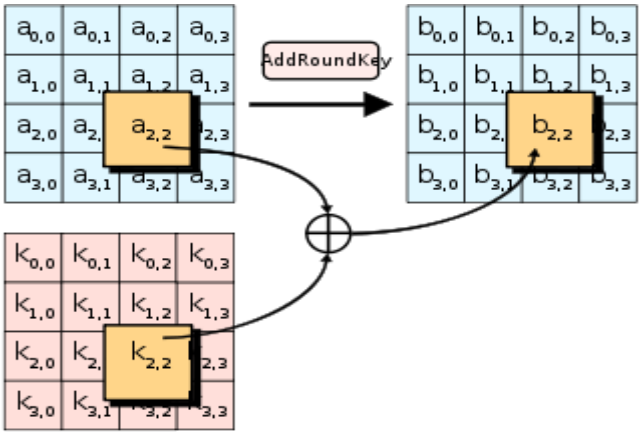



***Ilustración 10* - AES AddRoundKey**
**Fuente: Según (** (Wikipedia, 2014)

- Etapa final:

SubBytes

ShiftRows

AddRoundKey

### 2.2.4.2. Algoritmos criptográficos asimétricos

**RSA**

Desarrollado en 1977 es el primer y más utilizado algoritmo de llave pública y es válido tanto para cifrar como para firmar digitalmente.

La seguridad de este algoritmo radica en el problema de la factorización de números enteros. Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto.

Actualmente estos primos son del orden de $10^{200}$, y se prevé que su tamaño crezca con el aumento de la capacidad de cálculo de los ordenadores.

Como en todo sistema de clave pública, cada usuario posee dos claves de cifrado: una pública y otra privada. Cuando se quiere enviar un mensaje, el emisor busca la clave pública del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, este se ocupa de descifrarlo usando su clave privada.

Se cree que RSA será seguro mientras no se conozcan formas rápidas de descomponer un número grande en producto de primos. La computación cuántica podría proveer de una solución a este problema de factorización.

Funcionamiento técnico del algoritmo

Supongamos que Bob quiere enviar a Alicia un mensaje secreto que solo ella pueda leer. Alicia envía a Bob una caja con una cerradura abierta, de la que solo Alicia tiene la llave. Bob recibe la caja, escribe el mensaje, lo pone en la caja y la cierra con su cerradura (ahora Bob no puede leer el mensaje). Bob envía la caja a Alicia y ella la abre con su llave. En este ejemplo, la caja con la cerradura es la «clave pública» de Alicia, y la llave de la cerradura es su «clave privada».

Técnicamente, Bob envía a Alicia un «mensaje llano» $M$ en forma de un número $m$ menor que otro número $n$, mediante un protocolo reversible conocido como padding scheme («patrón de relleno»). A continuación genera el «mensaje cifrado» $c$ mediante la siguiente operación:

$$c \equiv m^e \pmod{n},$$

Donde $e$ es la clave pública de Alicia.

Ahora Alicia descifra el mensaje en clave $c$ mediante la operación inversa dada por

$$m \equiv c^d \pmod{n},$$

Donde $d$ es la clave privada que solo Alicia conoce

#### 2.2.4.3. Algoritmos criptográficos Hash

**MD5**

Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5 es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

La codificación del MD5 de 128 bits es representada típicamente como un número de 32 dígitos hexadecimal. El siguiente código de 28 bytes ASCII será tratado con MD5 y veremos su correspondiente hash de salida:

MD5 ("Generando un MD5 de un texto") = 5df9f63916ebf8528697b629022993e8

Un pequeño cambio en el texto (cambiar '5' por 'S') produce una salida completamente diferente.

MD5 ("Generando un MDS de un texto") = e14a3ff5b5e67ede599cac94358e1028

**Funcionamiento técnico del algoritmo**

En este documento "palabra" es una entidad de 4 bytes y un byte es una entidad de 8 bits. Una secuencia de bytes puede ser interpretada de manera natural como una secuencia de bits, donde cada grupo consecutivo de ocho bits se interpreta como un byte con el bit más significativo al principio. Similarmente, una secuencia de bytes puede ser interpretada como una secuencia de 32 bits (palabra), donde cada grupo consecutivo de cuatro bytes se interpreta como una palabra en la que el byte menos significativo está al principio.

El símbolo "+" significa suma de palabras.
X <<< s se interpreta por una rotación de bits a la izquierda sobre 'X', 's' posiciones
not(x) se entiende como el complemento de x

El algoritmo md5 empieza suponiendo que tenemos un mensaje de 'b' bits de entrada, y que nos gustaría encontrar su resumen. Aquí 'b' es un valor arbitrario entero no negativo, pero puede ser cero, no tiene por qué ser múltiplo de ocho, y puede ser muy largo. Imaginemos los bits del mensaje escritos así:

m0 m1 ... m{b-1}

Los siguientes cinco pasos son efectuados para calcular el resumen del mensaje.

*Paso 1. Adición de bits*

El mensaje será extendido hasta que su longitud en bits sea congruente con 448, módulo 512. Esto es, si se le resta 448 a la longitud del mensaje tras este paso, se obtiene un múltiplo de 512. Esta extensión se realiza siempre, incluso si la longitud del mensaje es ya congruente con 448, módulo 512.

La extensión se realiza como sigue: un solo bit "1" se añade al mensaje, y después se añaden bits "0" hasta que la longitud en bits del mensaje extendido se haga congruente con 448, módulo 512. En todos los mensajes se añade al menos un bit y como máximo 512.

*Paso 2. Longitud del mensaje*

Un entero de 64 bits que represente la longitud 'b' del mensaje (longitud antes de añadir los bits) se concatena al resultado del paso anterior. En el supuesto no deseado de que 'b' sea mayor que 2^64, entonces sólo los 64 bits de menor peso de 'b' se usarán.

En este punto el mensaje resultante (después de rellenar con los bits y con 'b') se tiene una longitud que es un múltiplo exacto de 512 bits. A su vez, la longitud del mensaje es múltiplo de 16 palabras (32 bits por palabra). Con M[0 ... N-1] denotaremos las palabras del mensaje resultante, donde N es múltiplo de 16.

*Paso 3. Inicializar el búfer MD*

Un búfer de cuatro palabras (A, B, C, D) se usa para calcular el resumen del mensaje. Aquí cada una de las letras A, B, C, D representa un registro de 32 bits. Estos registros se inicializan con los siguientes valores hexadecimales, los bytes de menor peso primero:

palabra A: 01 23 45 67
palabra B: 89 ab cd ef
palabra C: fe dc ba 98
palabra D: 76 54 32 10

*Paso 4. Procesado del mensaje en bloques de 16 palabras*

Primero definimos cuatro funciones auxiliares que toman como entrada tres palabras de 32 bits y su salida es una palabra de 32 bits.

$$F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$$
$$G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$$
$$H(X,Y,Z) = X \oplus Y \oplus Z$$
$$I(X,Y,Z) = Y \oplus (X \vee \neg Z)$$

Los operadores $\oplus, \wedge, \vee, \neg$ son las funciones XOR, AND, OR y NOT respectivamente.

En cada posición de cada bit X actúa como un condicional: si X, entonces Z sino Y. La función Z podría haber sido definida usando + en lugar de v ya que XY y not(x) Z nunca tendrán unos ('1') en la misma posición de bit.

Es interesante resaltar que si los bits de X, Y y Z son independientes y no

sesgados, cada uno de los bits de F(X,Y,Z) será independiente y no sesgado.

Las funciones G, H e I son similares a la función F, ya que actúan "bit a bit en paralelo" para producir sus salidas de los bits de X, Y y Z, en la medida que si cada bit correspondiente de X, Y y Z son independientes y no sesgados, entonces cada bit de G(X,Y,Z), H(X,Y,Z) e I(X,Y,Z) serán independientes y no sesgados. Nótese que la función H es la comparación bit a bit "xor" o función "paridad" de sus entradas.

Este paso usa una tabla de 64 elementos T[1 ... 64] construida con la función Seno. Denotaremos por T[i] el elemento i-ésimo de esta tabla, que será igual a la parte entera del valor absoluto del seno de 'i' 4294967296 veces, donde

Código del MD5:

```
/* Procesar cada bloque de 16 palabras. */
para i = 0 hasta N/16-1 hacer

  /* Copiar el bloque 'i' en X. */
  para j = 0 hasta 15 hacer
    hacer X[j] de M[i*16+j].
  fin para /* del bucle 'j' */

/* Guardar A como AA, B como BB, C como CC, y D como DD. */

/* Ronda 1. */
/* [abcd k s i] denotarán la operación
     a = b + ((a + F(b, c, d) + X[k] + T[i]) <<< s). */
/* Hacer las siguientes 16 operaciones. */
[ABCD  0  7  1] [DABC  1 12  2] [CDAB  2 17  3] [BCDA  3 22  4]
[ABCD  4  7  5] [DABC  5 12  6] [CDAB  6 17  7] [BCDA  7 22  8]
[ABCD  8  7  9] [DABC  9 12 10] [CDAB 10 17 11] [BCDA 11 22 12]
[ABCD 12  7 13] [DABC 13 12 14] [CDAB 14 17 15] [BCDA 15 22 16]

/* Ronda 2. */
/* [abcd k s i] denotarán la operación
    a = b + ((a + G(b, c, d) + X[k] + T[i]) <<< s). */
/* Hacer las siguientes 16 operaciones. */
[ABCD  1  5 17] [DABC  6  9 18] [CDAB 11 14 19] [BCDA  0 20 20]
[ABCD  5  5 21] [DABC 10  9 22] [CDAB 15 14 23] [BCDA  4 20 24]
[ABCD  9  5 25] [DABC 14  9 26] [CDAB  3 14 27] [BCDA  8 20 28]
[ABCD 13  5 29] [DABC  2  9 30] [CDAB  7 14 31] [BCDA 12 20 32]

/* Ronda 3. */
```

```
/* [abcd k s t] denotarán la operación
    a = b + ((a + H(b, c, d) + X[k] + T[i]) <<< s). */
/* Hacer las siguientes 16 operaciones. */
[ABCD  5  4 33] [DABC  8 11 34] [CDAB 11 16 35] [BCDA 14 23 36]
[ABCD  1  4 37] [DABC  4 11 38] [CDAB  7 16 39] [BCDA 10 23 40]
[ABCD 13  4 41] [DABC  0 11 42] [CDAB  3 16 43] [BCDA  6 23 44]
[ABCD  9  4 45] [DABC 12 11 46] [CDAB 15 16 47] [BCDA  2 23 48]

/* Ronda 4. */
/* [abcd k s t] denotarán la operación
    a = b + ((a + I(b, c, d) + X[k] + T[i]) <<< s). */
/* Hacer las siguientes 16 operaciones. */
[ABCD  0  6 49] [DABC  7 10 50] [CDAB 14 15 51] [BCDA  5 21 52]
[ABCD 12  6 53] [DABC  3 10 54] [CDAB 10 15 55] [BCDA  1 21 56]
[ABCD  8  6 57] [DABC 15 10 58] [CDAB  6 15 59] [BCDA 13 21 60]
[ABCD  4  6 61] [DABC 11 10 62] [CDAB  2 15 63] [BCDA  9 21 64]

/* Ahora realizar las siguientes sumas. (Este es el incremento de cada
   uno de los cuatro registros por el valor que tenían antes de que
   este bloque fuera inicializado.) */

   A = A + AA
   B = B + BB
   C = C + CC
   D = D + DD

fin para /* del bucle en 'i' */
```

*Paso 5. Salida*

El resumen del mensaje es la salida producida por A, B, C y D. Esto es, se comienza el byte de menor peso de A y se acaba con el byte de mayor peso de D

### 2.2.5. Protocolo L2TP

El protocolo de Reenvío de Capa Dos, tiene como objetivo proporcionar un mecanismo de tunneling para el transporte de tramas a nivel de enlace de datos del modelo (OSI), es un protocolo de encapsulamiento.

El L2TP es un protocolo estándar diseñado para transmitir datos y conectar de forma segura redes a través de internet.

L2TP se diseñó específicamente para conexiones de acceso remoto, así como para conexiones sitio a sitio. Mediante la utilización del protocolo PPP, L2TP.

**Estructura de L2TP**

- Concentrador de Acceso L2TP
- Servidor de Red L2TP
- Topología L2TP

**Funcionamiento de L2TP**

El túnel y su correspondiente conexión de control deben ser establecidas antes de que se inicien las llamadas entrantes o salientes. Una sesión L2TP debe ser establecida antes de que L2TP comience a entunelar tramas PPP.

La operación del protocolo L2TP se lleva a cabo de la siguiente manera.

1. Se establece la conexión control inicial entre el LAC y el LNS intercambiando los mensajes SCCRQ, SCCRP y SCCCN.
2. Se lleva a cabo la autenticación del túnel utilizando CHAP para ello.
3. Después de que se establece la conexión de control, se crean sesiones individuales cada sesión corresponde a un único flujo de tramas PPP entre el LAC y el LNS. Se intercambian los mensajes

ICRQ, ICRP, ICCN para llamadas entrantes y OCRQ ICRP y OCCN para llamadas salientes.

4. Una vez que se establece el túnel, las tramas PPP del sistema remoto son recibidas por el LAC, encapsuladas en L2TP y enviadas por el túnel apropiado. El LNS recibe el paquete y desencapsula la trama PPP.
5. Se utilizan números de secuencia con el fin de identificar los mensajes para mantener un transporte confiable de éstos.
6. Se emplea el mensaje Hello para mantener activa la conexión.
7. Para finalizar la sesión, o el LAC o el LNS envían un mensaje CDN.
8. Para finalizar la conexión de control, o el LAC o el LNS envían un mensaje Stop CCN.

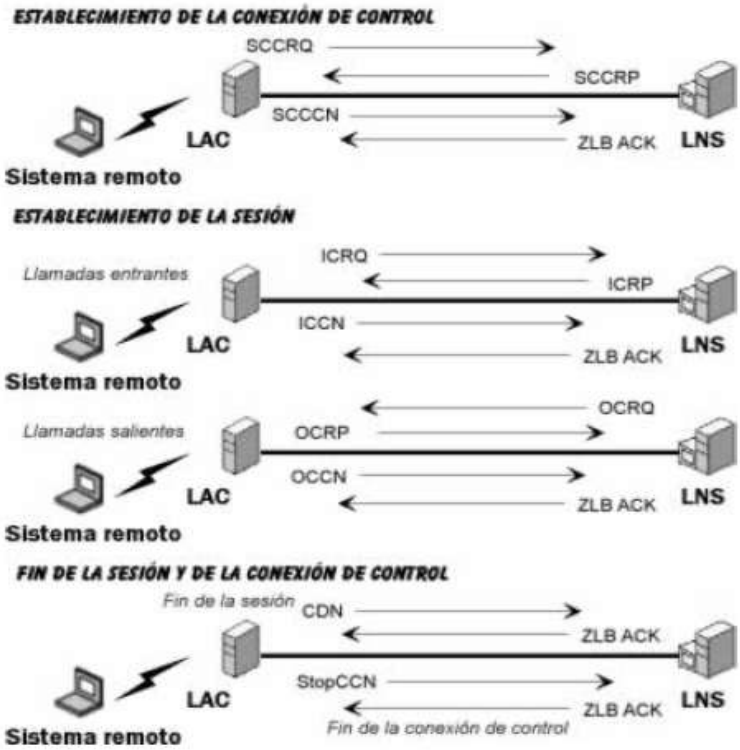



***Ilustración 11*- Funcionamiento del L2TP**

**Fuente: Según (Gonzales Morales, 2008)**

.

### 2.2.6. Librerías para algoritmos de encriptación

Según (Maiorano, 2010) los diferentes entornos de desarrollo poseen una buena variedad de funcionalidades criptográficas incorporadas.

El Java Cryptography Architecture (JCA) es un framework para trabajar con criptografía usando el lenguaje de programación Java. Esto forma parte de la API de seguridad Java, y fue introducido por primera vez en JDK 1.1 en el paquete java.security

Esta JCE (Java Cryptography Extension) se consideró como la implementación concreta de algoritmos criptográficos de acuerdo a los lineamientos definidos por la JCA (incorporada a partir de la JDK 1.4), aunque actualmente las siglas JCA y JCE también se usan de manera general para referir a la arquitectura del framework.

Desde la JDK 1.4 -o J2SE 1.4.2- encontraremos los algoritmos de hashing MD2, MD5, SHA-1, SHA-256, SHA-384 y SHA-512. Se podrá firmar digitalmente mediante el algoritmo DSA, cifrar simétricamente mediante AES, Blowfish, DES, DESede -o TripleDES, o 3DES- y RC2; asimétricamente, a partir de 1.5 -o J2SE 5.0- con RSA.

Considerando el entorno de desarrollo .NET, el soporte de criptografía lo encontramos en las funcionalidades provistas por el namespace System.Security.Cryptography. A partir de esta raíz común encontramos clases que proveen implementaciones de varios algoritmos criptográficos. El modelo criptográfico del framework .NET implementa un patrón extensible de herencia de clases derivadas: existen clases de tipo de

algoritmo, a nivel abstracto; luego, clases de algoritmos, que heredan de una clase de tipo de algoritmo (abstractas también), y bajo estas últimas, las implementaciones concretas de las clases de algoritmos.

Se dispone de MD5 y SHA1 en todas las versiones del framework .NET. La familia SHA-2 (SHA-256, SHA-385, SHA-512) sólo está disponible a partir de la versión 3.5, igual que el algoritmo de cifrado simétrico AES. En todas las versiones en cambio dispondremos de DES, TripleDES y RC2. También se dispone aquí de los algoritmos asimétricos DSA y RSA.

La función de hashing md5() en PHP quizás sea la función criptográfica de un entorno de desarrollo más popularmente utilizada. Estuvo disponible desde la versión 4.0 del lenguaje, y a partir de la versión 4.3 se contaba ya con sha1(). Lamentablemente, no hay mucho más. Para cifrar, firmar, autenticar, etc., en este entorno, serán necesarias librerías o frameworks adicionales.

Aquí encontraremos menos opciones, estas son, los algoritmos de hashing MD5 y SHA-1 únicamente.

### 2.2.7. Autenticación

Como ya se ha dicho, el concepto de autentificación viene asociado a la comprobación del origen e integridad de la información. En general, y debido a los diferentes tipos de situaciones que podemos encontrar en un sistema informático, distinguiremos tres tipos de autentificación:

- Autentificación de mensaje. Queremos garantizar la procedencia de un mensaje conocido, de forma que podamos asegurarnos de que no es una falsificación.

  Este mecanismo se conoce habitualmente como firma digital.
- Autentificación de usuario mediante contraseña. En este caso se trata de garantizar la presencia de un usuario legal en el sistema. El usuario deberá poseer una contraseña secreta que le permita identificarse.
- Autentificación de dispositivo. Se trata de garantizar la presencia frente al sistema de un dispositivo concreto. Este dispositivo puede estar solo o tratarse de una llave electrónica que sustituye a la contraseña para identificar a un usuario.

Nótese que la autentificación de usuario por medio de alguna característica biométrica, como pueden ser las huellas digitales, la retina, el iris, la voz, etc. Puede reducirse a un problema de autentificación de dispositivo, solo que el dispositivo en este caso es el propio usuario

## 2.3. Definición de términos básicos

### *2.3.1. Algoritmo*

Conjunto finito de instrucciones para llevar a cabo una tarea. Constan de pasos finitos, no ambiguos y, de ser posible, eficientes. (Alonso, 2009)

### *2.3.2. Ataque informático*

Un ataque informático es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro

sistema informático (ordenador, red privada, etcétera). (Cisco, Informe Anual de Seguridad, 2014)

### *2.3.3. Criptografía*

Tradicionalmente se ha definido como el ámbito de la criptología que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados. Por tanto, el único objetivo de la criptografía era conseguir la confidencialidad de los mensajes.

### *2.3.4. Delito informático*

Un delito informático es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

### *2.3.5. Encriptación*

La encriptación es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave. Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros, pueden ser contraseñas, número de tarjetas de crédito, conversaciones privadas, entre otros. (Latinoamérica, 2013)

### *2.3.6. Esteganografía*

Está enmarcada en el área de seguridad informática, trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia. Es

decir, se trata de ocultar mensajes dentro de otros objetos y de esta forma establecer un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase inadvertido para observadores que tienen acceso a ese canal. (Eset, 2013)

### *2.3.7. Red privada virtual*

Una red privada virtual, RPV o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos. (Alonso, 2009)

### *2.3.8. Seguridad*

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. (Cisco, Informe Anual de Seguridad, 2014)

### *2.3.9. Técnicas de encriptación*

Tecnología que permite la transmisión segura de información, al codificar los datos transmitidos usando una fórmula matemática que "desmenuza" los datos

## 2.4. CARACTERÍSTICAS DE FUNCIONAMIENTO Y APLICACIONES DE LAS REDES PRIVADAS VIRTUALES

### 2.4.1. INTRODUCCIÓN

Los sistemas de red son desde hace algún tiempo parte de los procesos de muchas empresas, no solo porque estas han comenzado a ofrecer sus servicios a través de Internet sino porque al expandirse físicamente requiere mantener una conectividad permanente con sus sucursales, socios e incluso sus empleados que al no estar físicamente en la organización requieren continuar con los trabajos asignados.

Sin embargo, en una gran cantidad de países el acceso a esta conectividad suele implicar grandes inversiones, en mucho de los casos marcados por la situación geográfica de los extremos que producen la comunicación. Mantener canales exclusivamente dedicados para realizar intercambio de información puede volverse una tarea difícil al momento de garantizar anchos de banda y bajos costos.

En un principio el medio físico o el canal dedicado mas utilizado para la comunicación de las diferentes redes locales eran las líneas telefónicas, con la ventaja de que la disponibilidad es muy alta y que se garantiza la privacidad. El gran inconveniente del uso de las líneas telefónicas es su alto costo, ya que se suele cobrar un pago mensual más una tarifa por el uso, en el que se tienen en cuenta la duración de las llamadas y la distancia hacia donde se hace.


***Ilustración 12*: Diseño de VPN de dos redes privadas a través del Internet.**

**Fuente: eltomason.blogspot.pe**

Una VPN-Virtual Private Network- (Red Privada Virtual) consiste en utilizar un canal de comunicaciones público como es Internet para comunicaciones privadas, de tal forma que no se necesita tener un canal dedicado para la comunicación, es decir una VPN es aquella red privada construida sobre una red pública.

Se le llama virtual, porque esta depende del uso de una conexión virtual, que es una conexión temporal que no tiene una presencia física real. Esta conexión virtual puede hacerse entre dos máquinas, entre una máquina y una red, y, entre dos redes.

Una de las principales razones que ha direccionado el mercado en este sentido son los costos, puesto que resulta mucho más barato interconectar sucursales utilizando una infraestructura pública que desplegar una red físicamente privada.

Hoy en día existen varias formas de garantizar la seguridad de un canal entre dos puntos como un emisor y un receptor, estas pueden ser el uso de Extranets, o protegiendo los servidores propios mediante passwords o incluso utilizar canales dedicados para todas las comunicaciones que requieran un canal seguro. Pero utilizar tecnología VPN tiene muchas ventajas con respecto a las otras soluciones, entre las principales tenemos:

- ***Ahorro en costos de comunicaciones:*** En el caso de usuarios remotos, cuando quieren utilizar los servicios de la compañía no necesitan conectarse directamente a los servidores de la compañía, sino que se conectan directamente por su conexión a Internet. Por otro lado, la compañía puede utilizar sus líneas de conexión a Internet para realizar transmisiones de datos, sin necesidad de contratar líneas privadas adicionales.
- ***Ahorro en costos operacionales:*** Usando VPN para dar acceso a los usuarios, la compañía puede deshacerse de los bancos de módems y de los servidores para acceso remoto, de manera que ya no habrá que administrar esos dispositivos.

- ***Entorno de trabajo independiente de tiempo y lugar a un costo reducido:*** Mediante el uso de una VPN, los trabajadores remotos pueden acceder a los servicios de la compañía desde cualquier lugar y a cualquier hora sin necesidad de realizar llamadas a larga distancia ni utilizando líneas privadas.
- ***Una compañía puede ofrecer servicios a sus socios mediante una VPN:*** Ya que la tecnología VPN permite accesos controlados y proporciona un canal seguro para compartir información de negocios.

## 2.5. FUNCIONAMIENTO Y CARACTERISTICAS

Una VPN es un sistema para simular una red privada sobre una red pública, en la mayoría de los casos la red pública es el Internet, pero también puede ser una red ATM-Asynchronous Transfer Mode- (Modo de Transferencia Asíncrona) o Frame Relay. La idea es que la red pública sea vista desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.

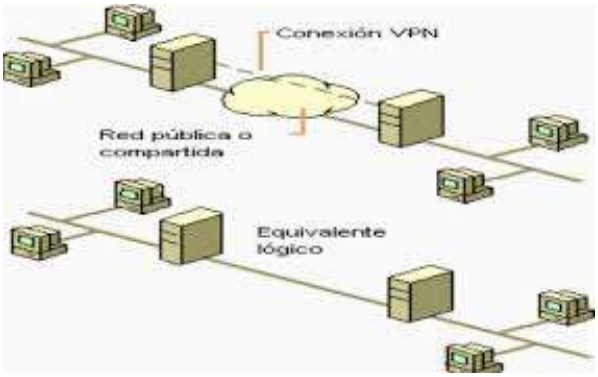



***Ilustración 13:*** **Equivalente lógico de una conexión VPN**

**Fuente:http://romancedeunanota-sersh.blogspot.pe/2010/04/**

Las redes privadas virtuales permiten que la comunicación se realice por un canal seguro. Por canal seguro se entiende que la comunicación cumpla con los siguientes requisitos.

1. **Autentificación:**

   Las técnicas de autenticación son esenciales en las VPNs, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autenticación en VPNs es conceptualmente parecido al logeo en un sistema como nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas de autenticación usados en VPN están basados en un sistema de claves compartidas.

   La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no haya algún tercer participante que se haya entrometido en la conversación. La autenticación también puede ser usada para asegurar la integridad de los datos. Los datos son procesados con un algoritmo de hashing para derivar un valor incluido en el mensaje como checksum.

   Cualquier desviación en el checksum indica que los datos fueron corruptos en la transmisión o interceptados y modificados en el camino.

2. **Encriptación:**

   Todas las VPNs tienen algún tipo de tecnología de encriptación, que esencialmente empaqueta los datos en un paquete seguro. La encriptación es considerada tan esencial como la autenticación, ya que protege los datos transportados para que no puedan ser vistos y entendidos en el viaje de un extremo a otro de la conexión. Existen dos tipos de técnicas de encriptación que se usan en las VPN: encriptación de clave secreta, o privada, y encriptación de clave pública.

   En la **encriptación de clave secreta**, se utiliza una contraseña secreta conocida por todos los participantes que necesitan acceso a la información encriptada. Dicha contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de encriptación posee el problema que, como la contraseña es compartida por todos los participantes y debe mantenerse secreta, al ser revelada, debe ser

cambiada y distribuida a los participantes, con lo cual se puede crear de esta manera algún problema de seguridad.

La **encriptación de clave pública** implica la útilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

En las VPNs, la encriptación debe ser realizada en tiempo real. Por eso, los flujos encriptados a través de una red son encriptados utilizando encriptación de clave secreta con claves que son solamente buenas para sesiones de flujo.

El protocolo más usado para la encriptación dentro de las VPNs es IPSec- Internet Protocol Security- (Seguridad del Protocolo Internet), que consiste en un conjunto de propuestas del IETF- Internet Engineering Task Force-(Fuerza de Tarea de Ingenieros en Internet) que delinean un protocolo IP seguro para IPv4-Protocolo Internet versión 4- y IPv6-Protocolo Internet versión 6-. IPSec provee encriptación a nivel de IP.

**3. Integridad:**

Debe garantizarse la integridad de los datos, esto es, que los datos que le llegan al receptor sean exactamente los que el emisor transmitió por el canal. Para esto se pueden utilizar firmas digitales.

**4. Tunneling**

La forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo túneles virtuales entre dos puntos para los cuales se negocian esquemas de encriptación y autentificación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública. Como se usan redes públicas, usualmente Internet, es necesario prestar debida atención a las

cuestiones de seguridad, que se aborda a través de estos esquemas de encriptación y autentificación y que se describieron anteriormente.

Para crear el túnel es preciso que un protocolo especial encapsule cada paquete origen en uno nuevo que incluya los campos de control necesarios para crear, gestionar y deshacer el túnel, tal como se muestra en la Ilustración 14.

Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan encriptados.

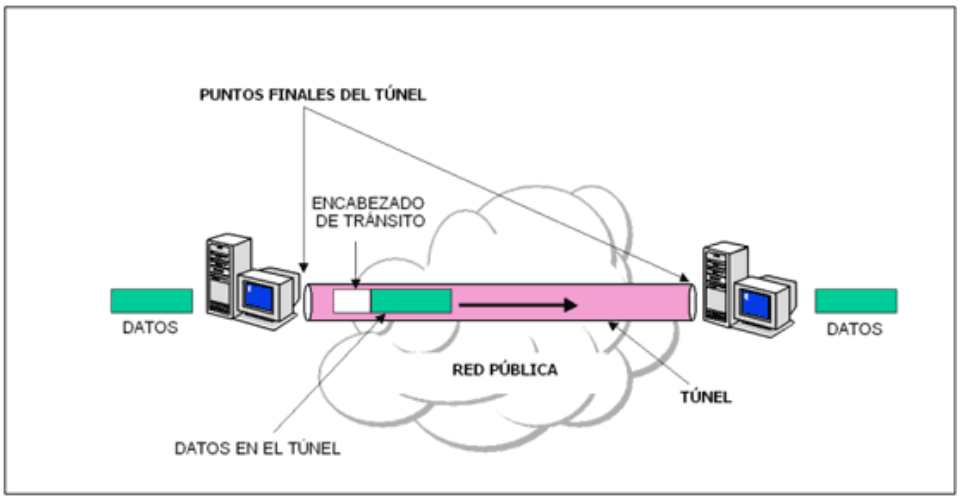



***Ilustración 14:*** **Túnel en una VPN.**

**Fuente: eltomason.blogspot.pe**

## 2.6. TIPOS DE VPN's Y SUS APLICACIONES.

### 2.6.1. ARQUITECTURAS DE CONEXIÓN VPN.

Básicamente existen tres arquitecturas de conexión VPN:

#### 2.6.1.1. VPN de acceso remoto

Esta es la arquitectura de conexión más utilizada actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hotel, aviones, etcétera) utilizando Internet como vínculo de acceso (**Ilustración 15**). El cliente de acceso remoto (cliente VPN), se autentifica al servidor de acceso remoto (el servidor VPN), y para una mutua autentificación, el servidor se autentifica ante el cliente. Una vez autenticados tienen un nivel

de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura 'dial-up' (módems y líneas telefónicas), aunque por razones de contingencia todavía conservan sus viejos módems.

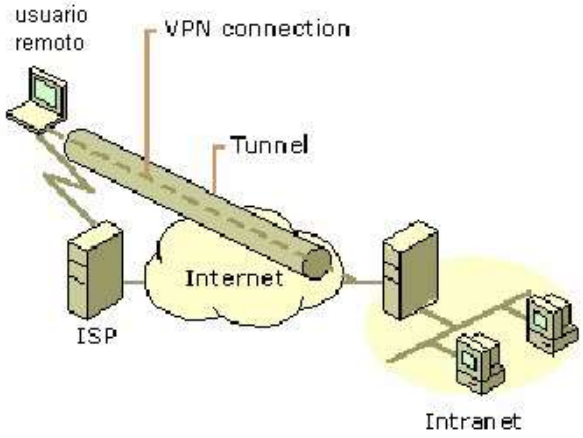



***Ilustración 15:*** **Un usuario remoto que establece un túnel con la oficina principal.**

**Fuente: eltomason.blogspot.pe**

### 2.6.1.2. VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN (Ilustración 16). Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales.


***Ilustración 16:*** **Conexión punto a punto**

**Fuente: eltomason.blogspot.pe**

#### 2.6.1.3. VPN interna VLAN

Esta conexión es la menos difundida pero una de las más poderosas para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma LAN-Local Area Network- (Red de Area Local) de la empresa. Esta conexión es muy útil para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

### 2.6.2. VPN BASADAS EN INTERNET O EN INTRANET

#### 2.6.2.1. VPN basadas en Internet

Si se opta por un conexión de VPN basada en Internet, se tiene la ventaja que disminuyen los costos debido a que se puede ahorran los gastos de llamadas telefónicas de larga distancia y a números 1800, y se aprovecha la gran disponibilidad de Internet.

##### 2.6.2.1.1. Acceso remoto a través de Internet.

Cuando se trata de una Acceso remoto a través de Internet, los usuarios en vez de realizar una costosa llamada de larga distancia o a un número 1-800 para conectarse con un NAS- Network Access Service - (Servidor de Acceso a la Red) de la compañía o externo, puede llamar a un ISP-Proveedor de Servicio de Internet- local. Aprovechando esta conexión física con el ISP local, el cliente de acceso remoto inicia una conexión VPN a través del Internet con el servidor VPN de la organización. Una vez creada la conexión VPN, el cliente de acceso remoto puede tener acceso a los recursos de la intranet privada. (La Ilustración 17 muestra el acceso remoto a través de Internet).

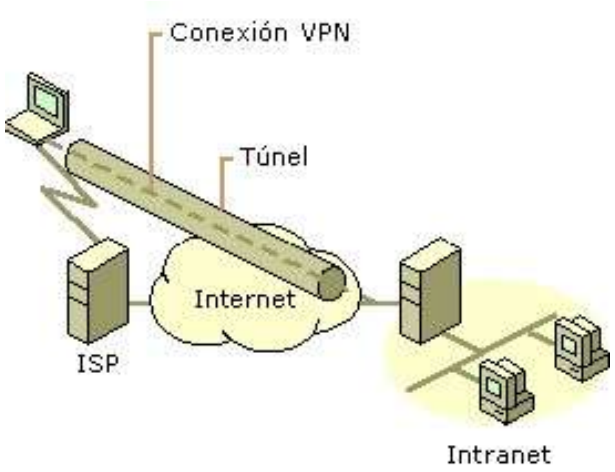



***Ilustración 17:*** **Acceso remoto a través de Internet.**

**Fuente: eltomason.blogspot.pe**

### 2.6.2.1.2. Conexión de redes a través de Internet.

Cuando se realiza una conexión de redes a través de Internet, un enrutador reenvía paquetes a otro enrutador a través de una conexión VPN. Esto se conoce como una conexión VPN de enrutador a enrutador. (La Ilustración 18 muestra la conexión de redes a través de Internet.)

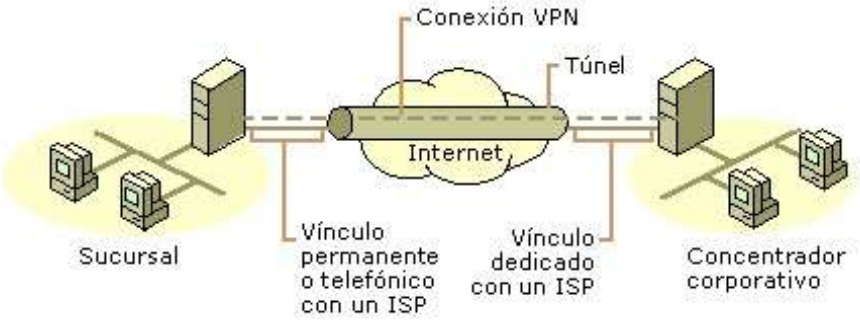



***Ilustración 18:*** **Conexión de redes a través de Internet**

**Fuente: eltomason.blogspot.pe**

#### 2.6.2.2. VPN basadas en Intranet

Si se opta por una conexión de VPN basadas en intranet se tiene la ventaja que se aprovecha la conectividad IP en la intranet de una organización.

##### 2.6.2.2.1. Acceso remoto a través de Intranet.

En las intranets de algunas organizaciones o empresas, los datos de un departamento (por ejemplo, el departamento financiero o de recursos humanos) son tan confidenciales que la red del departamento está físicamente desconectada de la intranet del resto de la organización. Aunque así se protegen los datos del departamento, se crea un problema de acceso a la información por parte de aquellos usuarios que no están físicamente conectados a la red independiente.

Mediante una conexión VPN basada en Intranet, la red del departamento está físicamente conectada a la intranet de la organización pero se mantiene separada gracias a un servidor VPN. El servidor VPN no proporciona una conexión enrutada directa entre la intranet de la organización y la red del departamento. Los usuarios de la intranet de la organización que disponen de los permisos apropiados pueden establecer una conexión VPN de acceso remoto con el servidor VPN y tener acceso a los recursos protegidos de la red confidencial del departamento. Adicionalmente, para mantener la confidencialidad de los datos, se cifran todas las comunicaciones realizadas a través de la conexión VPN. Para aquellos usuarios que no tienen derechos para establecer una conexión VPN, la red del departamento está oculta a la vista.

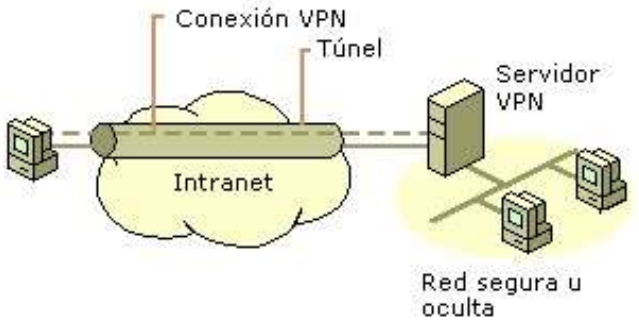



***Ilustración 19:*** **Acceso remoto a través de Intranet**

Fuente: https://i-technet.sec.s-msft.com/dynimg/IC197923.gif

#### 2.6.2.2.2. Conexión de redes a través de Intranet.

Se puede también conectar dos redes a través de una intranet mediante una conexión VPN de enrutador a enrutador. Este tipo de conexión es ideal para las organizaciones que poseen departamentos en diferentes ubicaciones, cuyos datos son confidenciales, pueden utilizar una conexión VPN de enrutador a enrutador para comunicarse entre sí.

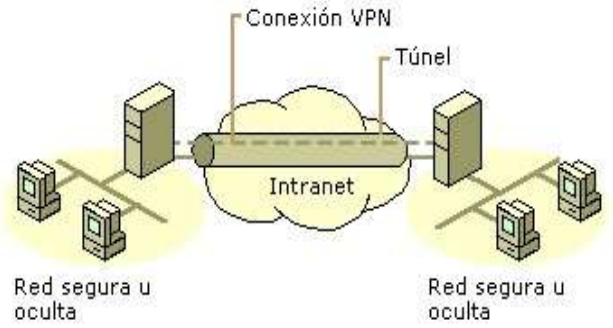



***Ilustración 20:*** **Conexión de redes a través de una intranet.**
**Fuente: https://i-technet.sec.s-msft.com/dynimg/IC197923.gif**

### 2.6.2.3. VPNs DINAMICAS

Como ya conocemos Internet no fue diseñada originalmente para el ámbito de los negocios, por lo que carece de la tecnología necesaria para la seguridad en las transacciones y comunicaciones que se producen en los negocios, por lo tanto cabe la pregunta, ¿Cómo establecer y mantener la confianza para los negocios en el Internet?

La respuesta es que esto se puede conseguir mediante la utilización de VPNs Dinámicas. A diferencia de una VPN tradicional, una VPN Dinámica proporciona, además de un alto nivel de seguridad a ambos extremos, una flexibilidad necesaria para acoplarse dinámicamente a la información que necesitan los distintos grupos de usuarios. Las VPNs Dinámicas pueden ofrecer esta flexibilidad ya que están basadas en una única arquitectura. Además, una VPN Dinámica proporciona más recursos y servicios a una Intranet, para hacer mayor uso de los recursos de la información.

Las principales características que proporcionan las VPN dinámicas son:

- Proporciona una seguridad importante para la empresa.
- Se ajusta dinámicamente a las diferentes clases de usuarios y a sus características.
- Permite la posibilidad de intercambio de información en diversos formatos.
- El ajuste que hace para cada usuario lo consigue gracias a los diferentes navegadores, aplicaciones, sistemas operativos, etc...
- Mantiene la integridad total, independientemente del volumen administrativo, cambios en la tecnología o complejidad del sistema de información corporativo.

## 2.7. PROTOCOLOS USADOS POR LAS VPN's

Existen una gran variedad de protocolos de red para el uso de las VPN que ya han sido implementados, estos protocolos intentan ofrecer la mayor seguridad posible en cuanto a VPN se refiere.

### 2.7.1. PROTOCOLO DE TÚNEL PUNTO A PUNTO (PPTP)

PPTP-Point to Point Tunneling Protocol- (Protocolo de Túnel Punto a Punto) es una especificación de protocolo desarrollada por varias compañías, para proveer entre usuarios de acceso remoto y servidores de red una red privada virtual, normalmente, se asocia PPTP con Microsoft.

La principal ventaja de PPTP radica en su habilidad para soportar protocolos no IP, y su principal problema o desventaja es su fallo a elegir una única encriptación y autentificación estándar que puede dar como efecto que dos productos que acceden con la especificación PPTP pueden llegar a ser completamente incompatibles simplemente porque la encriptación de los datos sea diferente.

Existen dos escenarios comunes para las VPN que utilizan un protocolo de túnel punto a punto:

- El usuario remoto se conecta a un ISP que provee el servicio de PPTP hacia el RAS-Servidor de Acceso Remoto. En este escenario el usuario remoto estable una conexión PPP con el ISP, que luego establece la conexión PPTP con el servidor RAS.
- El usuario remoto se conecta a un ISP que no provee el servicio de PPTP hacia el servidor RAS y, por lo tanto, debe iniciar la conexión PPTP desde su propia máquina cliente. En este escenario, el usuario remoto se conecta al ISP mediante PPP y luego llama al servidor RAS mediante PPTP.

Luego de establecida la conexión PPTP, para cualquiera de los dos casos, el usuario remoto tendrá acceso a la red corporativa como si estuviera conectado directamente a la misma.

#### 2.7.1.1. Encapsulación

Las tramas PPP-Point to Point Protocol- (Protocolo Punto a Punto) (que consisten en un datagrama IP o Appletalk) se empaquetan con un encabezado GRE- Generic Routing Encapsulation (Encapsulación de enrutamiento genérico) y un encabezado IP. En el encabezado IP están las direcciones IP de origen y de destino que corresponden al cliente VPN y al servidor VPN.

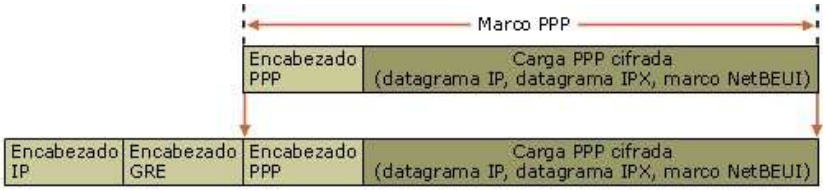



***Ilustración 21:*** **Encapsulación PPTP para una trama PPP.**

**Fuente: https://i-technet.sec.s-msft.com/dynimg/IC197923.gif**

### 2.7.2. PROTOCOLO DE TÚNEL DE CAPA 2 (L2TP)

Uno de los principales competidor de PPTP en soluciones VPN fue L2F- Layer 2 Forwarding-, desarrollado por Cisco. Con el fin de mejorar L2F, se combinaron las mejores características de PPTP y L2F para crear un nuevo estándar llamado L2TP.

L2TP opera en la capa de enlace del modelo OSI - Open System Interconnection Reference Model - (Modelo de Referencia de Sistemas Abiertos de interconexión). L2TP, al igual que PPTP soporta clientes no IP, pero también da problemas al definir una encriptación estándar.

L2TP utiliza la seguridad de protocolos Internet para los servicios de cifrado. La combinación de L2TP e IPSec se conoce como L2TP/IPSec. L2TP/IPSec proporciona los servicios de red privada virtual (VPN) principales de encapsulación y cifrado de datos privados.

#### 2.7.2.1. Encapsulación

La encapsulación de paquetes L2TP/IPSec consta de dos niveles:

##### 2.7.2.1.1. Encapsulación L2TP

Las Tramas PPP (que consiste en un datagrama IP o un datagrama IPX) se empaquetan con un encabezado L2TP y un encabezado UDP-User Datagram Protocol- (Protocolo de Datagrama de Usuario).

##### 2.7.2.1.2. Encapsulación IPSec

El mensaje L2TP resultante se empaqueta a continuación con un encabezado de ESP - Encapsulating Security Payload- (Carga de Seguridad de Encapsulación) de IPSec, y un finalizador de autenticación IPSec que proporciona autenticación e integridad de mensajes y un encabezado IP final.

El encabezado IP contiene las direcciones IP de origen y de destino que corresponden al cliente VPN y al servidor VPN.


***Ilustración 22:*** **Encapsulación L2TP e IPSec para un datagrama PPP.**

**Fuente. https://haciendounavpn.wordpress.com/2014/06/30/estructura-y-protocolos-utilizados-en-las-vpn/**

## 2.7.3. IPsec

### 2.7.3.1. Definición

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

Los protocolos de **IPsec** actúan en la capa de red, la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan de la capa de aplicación (capa 7 del modelo OSI). Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP.

### *2.7.3.2. Arquitectura de seguridad*

**IPsec** está implementado por un conjunto de protocolos criptográficos para asegurar el flujo de paquetes, garantizar la autenticación mutua y establecer parámetros criptográficos.

La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad (SA) como base para construir funciones de seguridad en IP. Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros (tales como las claves) que se está usando para cifrar y autenticar un flujo particular en una

dirección. Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) le corresponde al administrador de IPsec.

Para decidir qué protección se va a proporcionar a un paquete saliente, IPsec utiliza el índice de parámetro de seguridad (SPI), un índice a la base de datos de asociaciones de seguridad (SADB), junto con la dirección de destino de la cabecera del paquete, que juntos identifican de forma única una asociación de seguridad para dicho paquete. Para un paquete entrante se realiza un procedimiento similar; en este caso IPsec toma las claves de verificación y descifrado de la base de datos de asociaciones de seguridad.

En el caso de multicast, se proporciona una asociación de seguridad al grupo, y se duplica para todos los receptores autorizados del grupo. Puede haber más de una asociación de seguridad para un grupo, utilizando diferentes SPIs, y por ello permitiendo múltiples niveles y conjuntos de seguridad dentro de un grupo. De hecho, cada remitente puede tener múltiples asociaciones de seguridad, permitiendo autenticación, ya que un receptor sólo puede saber que alguien que conoce las claves ha enviado los datos. Hay que observar que el estándar pertinente no describe cómo se elige y duplica la asociación a través del grupo; se asume que un interesado responsable habrá hecho la elección.

#### *2.7.3.3. Estado actual del estándar*

IPsec es una parte obligatoria de IPv6, y su uso es opcional con IPv4. Aunque el estándar está diseñado para ser indiferente a las versiones de IP, el despliegue y experiencia hasta 2007 atañe a las implementaciones de IPv4.

Los protocolos de IPsec se definieron originalmente en las RFCs 1825 y 1829, publicadas en 1995. En 1998 estos documentos fueron sustituidos por las RFCs 2401 y 2412, que no son compatibles con la 1825 y 1829, aunque son conceptualmente idénticas. En diciembre de 2005 se produjo la tercera generación de documentos, RFCs 4301 y 4309. Son en gran parte un superconjunto de la 2401 y 2412, pero proporcionan un segundo estándar de

Internet Key Exchange. Esta tercera generación de documentos estandarizó la abreviatura de IPsec como "IP" en mayúsculas y "sec" en minúsculas.

Es raro ver un producto que ofrezca soporte de RFC1825 y 1829. "ESP" se refiere generalmente a 2406, mientras que ESPbis se refiere a 4303.

#### *2.7.3.4. Propósito de diseño*

IPsec fue proyectado para proporcionar seguridad en **modo transporte** (extremo a extremo) del tráfico de paquetes, en el que los ordenadores de los extremos finales realizan el procesado de seguridad, o en **modo túnel** (puerta a puerta) en el que la seguridad del tráfico de paquetes es proporcionada a varias máquinas (incluso a toda la red de área local) por un único nodo.

IPsec puede utilizarse para crear VPNs en los dos modos, y este es su uso principal. Hay que tener en cuenta, sin embargo, que las implicaciones de seguridad son bastante diferentes entre los dos modos de operación.

La seguridad de comunicaciones extremo a extremo a escala Internet se ha desarrollado más lentamente de lo esperado. Parte de la razón a esto es que no ha surgido infraestructura de clave pública universal o universalmente de confianza (DNSSEC fue originalmente previsto para esto); otra parte es que muchos usuarios no comprenden lo suficientemente bien ni sus necesidades ni las opciones disponibles como para promover su inclusión en los productos de los vendedores.

Como el Protocolo de Internet no provee intrínsecamente de ninguna capacidad de seguridad, IPsec se introdujo para proporcionar servicios de seguridad tales como:

1. Cifrar el tráfico (de forma que no pueda ser leído por nadie más que las partes a las que está dirigido)
2. Validación de integridad (asegurar que el tráfico no ha sido modificado a lo largo de su trayecto)
3. Autenticar a los extremos (asegurar que el tráfico proviene de un extremo de confianza)

4. Anti-repetición (proteger contra la repetición de la sesión segura).

#### 2.7.3.5. Modos

Así pues y dependiendo del nivel sobre el que se actúe, podemos establecer dos modos básicos de operación de **IPsec**: **modo transporte** y **modo túnel**.

##### 2.7.3.5.1. Modo transporte

En **modo transporte**, sólo la carga útil (los datos que se transfieren) del paquete IP es cifrada o autenticada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, ya que eso invalidaría el hash. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera (por ejemplo traduciendo los números de puerto TCP y UDP). El **modo transporte** se utiliza para comunicaciones ordenador a ordenador.

Una forma de encapsular mensajes IPsec para atravesar NAT ha sido definido por RFCs que describen el mecanismo de NAT transversal.

##### 2.7.3.5.2. Modo túnel

En el **modo túnel**, todo el paquete IP (datos más cabeceras del mensaje) es cifrado o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El **modo túnel** se utiliza para comunicaciones red a red (túneles seguros entre routers, p.e. para VPNs) o comunicaciones ordenador a red u ordenador a ordenador sobre Internet.

#### 2.7.3.6. Protocolos

**IPsec** consta de tres protocolos que han sido desarrollados para proporcionar seguridad a nivel de paquete, tanto para IPv4 como para IPv6:

- **Authentication Header** (AH) proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados.

- **Encapsulating Security Payload** (ESP) proporciona confidencialidad y la opción -altamente recomendable- de autenticación y protección de integridad.
- **Internet key exchange** (**IKE**) emplea un intercambio secreto de claves de tipo Diffie-Hellman para establecer el secreto compartido de la sesión. Se suelen usar sistemas de Criptografía de clave pública o clave pre-compartida.

Los algoritmos criptográficos definidos para usar con IPsec incluyen HMAC-SHA-1 para protección de integridad, y Triple DES-CBC y AES-CBC para confidencialidad.

#### 2.7.3.6.1. Authentication Header (AH)

AH está dirigido a garantizar integridad, sin conexión y autenticación de los datos de origen de los datagramas IP. Para ello, calcula un Hash Message Authentication Code (HMAC) a través de algún algoritmo hash operando sobre una clave secreta, el contenido del paquete IP y las partes inmutables del datagrama. Este proceso restringe la posibilidad de emplear NAT, que puede ser implementada con NAT transversal. Por otro lado, AH puede proteger opcionalmente contra ataques de repetición utilizando la técnica de ventana deslizante y descartando paquetes viejos. AH protege la carga útil IP y todos los campos de la cabecera de un datagrama IP excepto los campos mutantes, es decir, aquellos que pueden ser alterados en el tránsito. En IPv4, los campos de la cabecera IP mutantes (y por lo tanto no autenticados) incluyen TOS, Flags, Offset de fragmentos, TTL y suma de verificación de la cabecera. AH opera directamente por encima de IP, utilizando el protocolo IP número 51. Una cabecera AH mide 32 bits.

**Diagrama de paquete AH:**

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

**Significado de los campos:**

**Next header**

Identifica el protocolo de los datos transferidos.

**Payload length**

Tamaño del paquete AH.

**RESERVED**

Reservado para uso futuro (hasta entonces todo ceros).

**Security parameters index (SPI)**

Indica los parámetros de seguridad que, en combinación con la dirección IP, identifican la asociación de seguridad implementada con este paquete.

**Sequence number**

Un número siempre creciente, utilizado para evitar ataques de repetición.

**HMAC**

Contiene el valor de verificación de integridad (ICV) necesario para autenticar el paquete; puede contener relleno.

### 2.7.3.6.2. Encapsulating Security Payload (ESP)

El protocolo ESP proporciona autenticidad de origen, integridad y protección de confidencialidad de un paquete. ESP también soporta configuraciones de sólo cifrado y sólo autenticación, pero utilizar cifrado sin autenticación está altamente desaconsejado porque es inseguro. Al contrario que con AH, la cabecera del paquete IP no está protegida por ESP (aunque en ESP en modo túnel, la protección es proporcionada a todo el paquete IP interno, incluyendo la cabecera

interna; la cabecera externa permanece sin proteger). ESP opera directamente sobre IP, utilizando el protocolo IP número 50.

Un diagrama de paquete ESP:

<table>
<tr><th>0 - 7 bit</th><th>8 - 15 bit</th><th>16 - 23 bit</th><th>24 - 31 bit</th></tr>
<tr><td colspan="4">Security parameters index (SPI)</td></tr>
<tr><td colspan="4">Sequence number</td></tr>
<tr><td colspan="4">Payload data (variable)</td></tr>
<tr><td></td><td colspan="2">Padding (0-255 bytes)</td><td></td></tr>
<tr><td></td><td></td><td>Pad Length</td><td>Next Header</td></tr>
<tr><td colspan="4">Authentication Data (variable)</td></tr>
</table>

**Significado de los campos**

**Security parameters index (SPI)**
Identifica los parámetros de seguridad en combinación con la dirección IP.

**Sequence number**
Un número siempre creciente, utilizado para evitar ataques de repetición.

**Payload data**
Los datos a transferir.

**Padding**
Usado por algunos algoritmos criptográficos para rellenar por completo los bloques.

**Pad length**
Tamaño del relleno en bytes.

**Next header**
Identifica el protocolo de los datos transferidos.

**Authentication data**
Contiene los datos utilizados para autenticar el paquete.

# CAPITULO III

# MARCO METODOLOGICO

## 3.1. Tipo y diseño de la investigación

La investigación tiene un diseño de tipo Tecnológico – Cuasi Experimental Aplicada: Porque aplica teorías especializadas con el tema de investigación.

Cuasi Experimental: Porque los datos que componen la muestra no se eligen de forma aleatoria.

## 3.2. Población y muestra

La población: Base de datos de ataques a las Redes Privadas Virtuales, compuesta por siete tipos (husmeadores de Red, Integridad de datos, ataques de contraseña, ataques de denegación de servicios, Ataque de hombre al medio, spoofing, ataques de claves comprometidas)

La Muestra: Ataques dirigidos a redes privadas virtuales, como husmeadores de red e integridad de datos.

## 3.3. Hipótesis

La implementación de técnicas de encriptación incrementará la seguridad de la red privada virtual

## 3.4. Operacionalización

Variable Independiente

Técnicas de encriptación

Variable Dependiente

La seguridad la red privada virtual.

**Tabla 02:** ***Variable Dependiente-Rendimiento***

| VARIABLE DEPENDIENTE | DIMENSIONES | INDICADORES | TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS |
|---|---|---|---|
| Seguridad de datos en una red privada virtual | Medidas de Rendimiento | Efectividad de aciertos en paquetes. | Contar la cantidad de algoritmos utilizados. |
| | | Tiempo de procesamiento. | Registrar la cantidad de segundos que tarda en encriptar cada algoritmo. |
| | | Costo de procesamiento. | Registrar cantidad de consumo de cpu, en el uso del algoritmo. |

**Fuente: Creación propia**

## 3.5. Métodos, técnicas e instrumentos de recolección de datos

**Métodos:**

Para la recolección de datos se utilizarán:

- Observación.

- Técnicas: Registro de observaciones:

  Se usan para recopilar los datos de las pruebas del sistema propuesto y evidencia de las técnicas

- Instrumento: Ficha de registro de eventos: Este instrumento se usan para el registro de los eventos de las pruebas de aplicación de las técnicas.

## 3.6. Procedimiento para la recolección de datos

El desarrollo de la presente investigación, se ha basado en la utilización de técnicas de Encriptación de datos:

- Recopilación de Datos
- Pre – Procesado.

- Criptografía.
- Resultados.

Se realizará mediante la puesta en ejecución de las técnicas usadas y evaluar el desempeño de cada una de ellas de acuerdo con los indicadores que se ha establecido.

## 3.7. Plan de análisis estadísticos de datos

**Tabulación de datos:**

- Uso de tablas estadísticas
- Uso de gráficos estadísticos, como producto del procesamiento de los datos obtenidos de las pruebas realizadas y procesadas.

**Análisis de datos:**

- Interpretación de indicadores de acuerdo con las pruebas que se realizaran.

## 3.8. Criterios éticos

**Objetividad:** El análisis de la situación encontrada se basará en criterios técnicos imparciales.

**Confidencialidad:** Se asegurará que los registros usados para la prueba que son del ámbito privado no sean divulgados al público.

**Veracidad:** La información mostrada será verdadera

## 3.9. Criterios de rigor científico

**Validación:** Se validarán los instrumentos de recolección de datos.

**Contrastación:** Se contrastará la hipótesis a través de métodos estadísticos debido al diseño cuasi experimental.

# CAPITULO IV

## 4.1. TIPOS DE PRUEBAS

Las pruebas realizadas a la implementación de la VPN se basaron en dos tipos:

- Pruebas de Rendimiento
- Pruebas de Seguridad

## 4.2. PRUEBAS DE RENDIMIENTO

Las pruebas de rendimiento se realizaron tomando en cuenta lo siguiente:

- LONGITUD DE ARCHIVO
  - 10KB, 100KB, 1MB, 10MB, 100MB
- MÉTRICA
  - CARGA DE CPU (%)
  - TASA DE TRANSFERENCIA (KBITS/SEG)
  - TIEMPO RELATIVO (SEG.)
- PROTOCOLO:
  - IPSEC
  - AH EN MODO TÚNEL Y MODO TRANSPORTE
  - ESP EN MODO TÚNEL Y MODO TRANSPORTE

Se procedió a realizar la prueba de transferencia de archivos entre el cliente VPN y una estación de la red privada realizando las combinaciones de los protocolos de IPSEC (AH y ESP) solo en modo túnel; la misma transferencia se realizó en modo transporte (este modo fue diseñado para conexiones entre dos estaciones) pero entre el cliente VPN y el servidor VPN, y una transferencia entre los dos extremos sin VPN.

Luego se procedió a medir la carga del CPU del servidor VPN, la tasa de transferencia y el tiempo relativo.

Para medir estos parámetros se utilizó el programa "TOP", programa que nos permite visualizar los procesos que hay en ejecución y cuanta memoria consumen en tiempo real en ambientes Linux.

Los datos promedios obtenidos se muestran a continuación:

**Tabla 03: *Rendimiento del sistema en modo túnel***

| | AH | | ESP | |
|---|---|---|---|---|
| | FTP | FTP/VPN | FTP | FTP/VPN |
| CARGA DE CPU (%) | 15.3 | 20.1 | 15.3 | 24.5 |
| TASA DE TRANSFERENCIA (KB/SEG) | 625 | 513 | 625 | 495 |
| TIEMPO PROMEDIO RELATIVO (SEG.) | 1.51 | 2.09 | 1.51 | 2.21 |

**Fuente: Creación propia.**

**Tabla 04: *Rendimiento del sistema en modo transporte.***

| | AH | | ESP | |
|---|---|---|---|---|
| | FTP | FTP/VPN | FTP | FTP/VPN |
| CARGA DE CPU (%) | 15.3 | 18.5 | 15.3 | 20.7 |
| TASA DE TRANSFERENCIA (KB/SEG) | 625 | 585 | 625 | 562 |
| TIEMPO PROMEDIO RELATIVO (SEG.) | 1.51 | 2.01 | 1.51 | 2.12 |

**Fuente: Creación propia.**

### 4.2.1. Resultados

Como se puede observar en los resultados obtenidos, el protocolo IPSEC produce una tara (overhead) en el procesador, esto se debe a que el uso de los algoritmos de cifrado y autenticación necesitan más recursos para generar números aleatorios, los cuales son necesarios para realizar el cifrado, la tara es un poco mayor utilizando el protocolo ESP en modo túnel, esto debido a que el tamaño del paquete a cifrar es mayor que en el protocolo AH.

También se verifica una caída en la tasa de transferencia de datos, esto debido al tamaño del paquete IP sobre una VPN, el cual es de mayor tamaño en la transmisión con IPSEC que en una transmisión regular, el protocolo AH en modo transporte es más rápido, debido en parte a que no utiliza cifrado, lo que reduce el tamaño del paquete y solo agrega una cabecera extra al paquete IP original dando como resultado una velocidad ligeramente menor que en una transferencia normal.

## 4.3. PRUEBAS DE SEGURIDAD

Existen programas como SSH (para el “login” remoto), el SSL (para las aplicaciones Web) y PGP (para el correo electrónico) que aseguran los datos entre dos aplicaciones y que utilizan los mecanismos de trabajo de capa 7 (capa de aplicación). Estos programas trabajan muy bien, pero están limitados a cifrar únicamente los datos entre los puertos asociados a él.

Para poder mostrar los problemas de seguridad de algunos de estos protocolos de seguridad de aplicación (SSH, SSL) se procedió a utilizar un analizador de protocolos de red (Wireshark) (Anexo 4) para observar el comportamiento del protocolo SSH entre dos computadoras, en una sesión se analizó utilizando un canal seguro con VPN y otra sesión sin utilizar la VPN.

El diagrama de conexión utilizado para estas pruebas es el que se muestra a continuación:

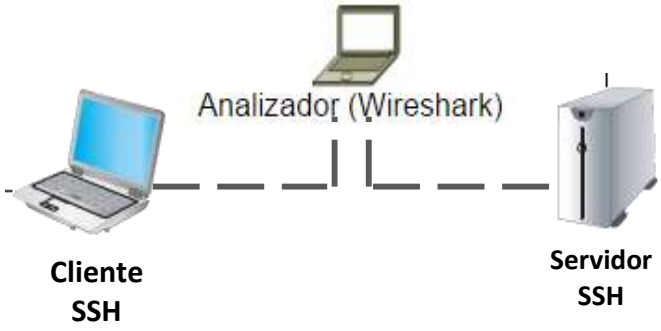



***Ilustración 23:*** **Esquema físico de conexión**

Una muestra del tráfico SSH capturado en la sesión sin túnel VPN se muestra en la **Ilustración 24** e **Ilustración 25**, en él se puede observar que los datos de la capa de aplicación, se encuentran cifrados

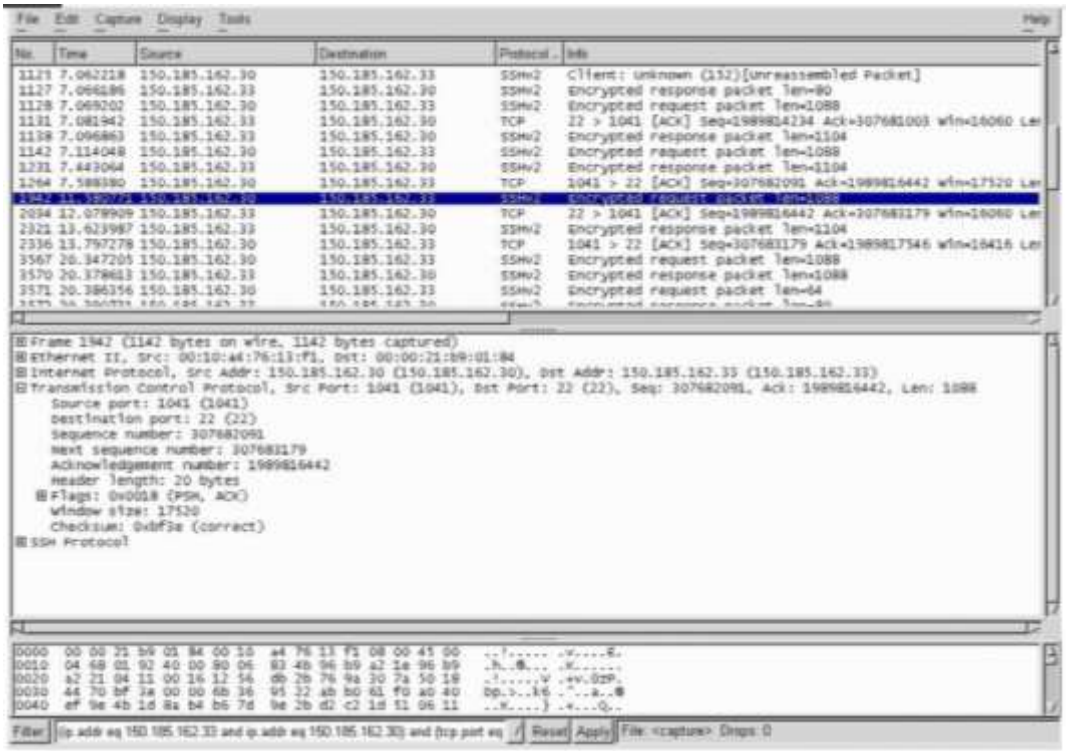


***Ilustración 24:*** **Tráfico SSH capturado sin túnel VPN**

| | | | | | |
|---|---|---|---|---|---|
| 1138 | 7.096863 | 150.185.162.33 | 150.185.162.30 | SSHv2 | Encrypted response packet len=1104 |
| 1142 | 7.114048 | 150.185.162.30 | 150.185.162.33 | SSHv2 | Encrypted request packet len=1088 |
| 1231 | 7.443064 | 150.185.162.33 | 150.185.162.30 | SSHv2 | Encrypted response packet len=1104 |
| 1264 | 7.588380 | 150.185.162.30 | 150.185.162.33 | TCP | 1041 > 22 [ACK] Seq=307682091 Ack=1989816442 Win=17520 Len |
| 1942 | 11.580771 | 150.185.162.30 | 150.185.162.33 | SSHv2 | Encrypted request packet len=1088 |
| 2034 | 12.078909 | 150.185.162.33 | 150.185.162.30 | TCP | 22 > 1041 [ACK] Seq=1989816442 Ack=307683179 Win=16060 Len |
| 2321 | 13.623987 | 150.185.162.33 | 150.185.162.30 | SSHv2 | Encrypted response packet len=1104 |
| 2336 | 13.797278 | 150.185.162.30 | 150.185.162.33 | TCP | 1041 > 22 [ACK] Seq=307683179 Ack=1989817546 Win=16416 Len |
| 3567 | 20.347205 | 150.185.162.30 | 150.185.162.33 | SSHv2 | Encrypted request packet len=1088 |
| 3570 | 20.378613 | 150.185.162.33 | 150.185.162.30 | SSHv2 | Encrypted response packet len=1088 |

***Ilustración 25:*** **Tráfico SSH capturado sin túnel VPN**

Utilizando el mismo esquema de conexión de la figura 4.1 se procedió a realizar una segunda captura de paquetes de datos de una sesión SSH pero a través de un túnel IPSec VPN, estos datos se muestran en la **Ilustración 26** y **27**.

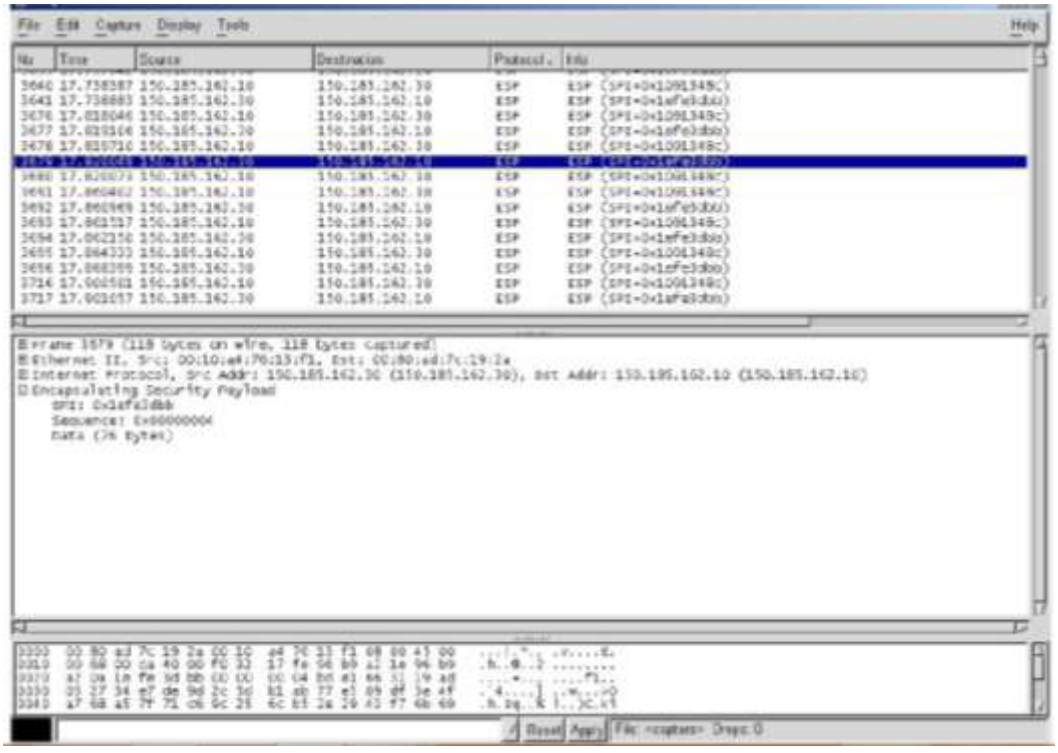


***Ilustración 26:*** **Tráfico SSH capturado con túnel VPN**

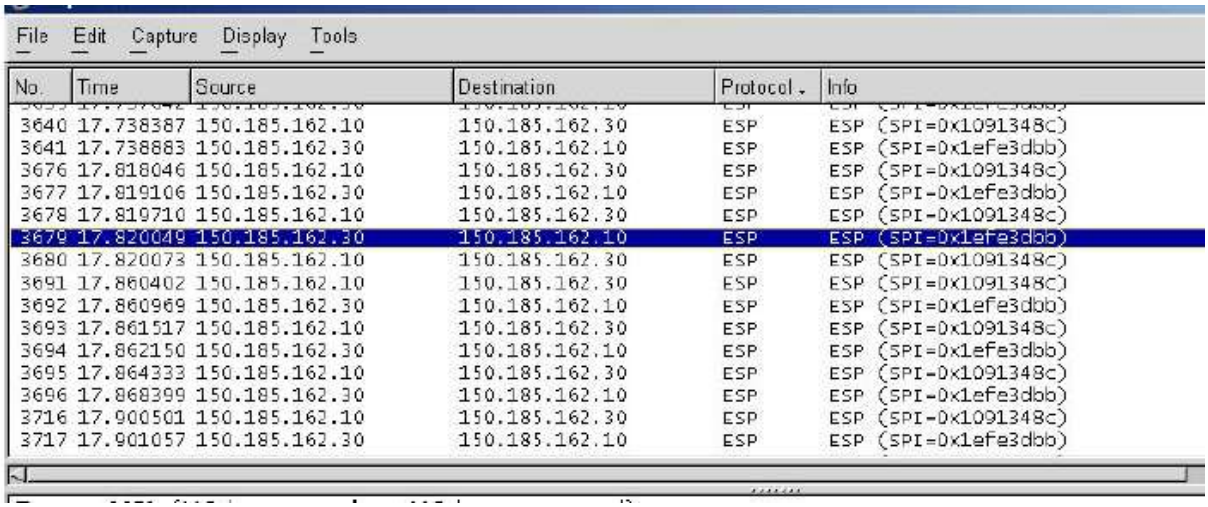



***Ilustración 27:*** **Tráfico SSH capturado con túnel VPN**

### 4.3.1 Resultados

En la sesión de SSH sin túnel VPN se pueden observar los números de los puertos asociados en la conexión, esto permite determinar fácilmente el servicio que se está ejecutando. Se descubre entonces que el servidor SSH escucha y transmite por el puerto TCP 22 y el cliente SSH utiliza el puerto TCP 1041.

Otros protocolos de seguridad como HTTPS y SSL (puerto 443), muestran un comportamiento de tráfico capturado similar, con la excepción de que estos utilizan números de puertos diferentes.

Cuando se utiliza el túnel IPSec solamente podemos ver los paquetes nativos de este protocolo (ESP, AH, IKE), no podemos saber qué aplicación se está ejecutando ni qué servicios hay disponibles. IPSec asegura todos los datos, sin tomar en cuenta la aplicación que se está ejecutando entre los entes involucrados en la transmisión.

Las pruebas de seguridad justifican la utilización de un túnel IPSec, ya que éste difiere de SSH y otros protocolos de cifrado basado en una aplicación, porque IPSec cifra los datos desde la capa 3 (capa de red del modelo OSI) por lo tanto ningún dato de capas superiores es mostrado, reduciendo así las vulnerabilidades de seguridad.

## VERIFICANDO LAS PRUEBAS DE SEGURIDAD CON UN PROTOCOLO NO CIFRADO COMO FTP (PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS)

Para esta prueba procedemos a configurar un servidor FTP en Linux Centos 6.5 **(Anexo 01)**. Para poder mostrar los problemas de seguridad de algunos de estos protocolos de seguridad de aplicación se procedió a utilizar un analizador de protocolos de red (Wireshark) para observar el comportamiento del protocolo FTP entre dos computadoras, en una sesión se analizó utilizando un canal seguro con VPN y otra sesión sin utilizar la VPN.

El diagrama de conexión utilizado para estas pruebas es el que se muestra a continuación:

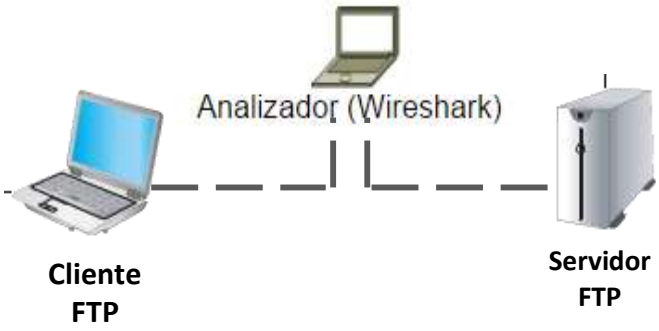



***Ilustración 28*: Esquema físico de conexión**

Una muestra del tráfico FTP capturado en la sesión sin túnel VPN se muestran en la **Ilustración 29 y 30**, en él se puede observar que los datos de la capa de aplicación, se encuentran sin cifrar y se puede visualizar el usuario, contraseña, protocolo y puerto TCP utilizado.

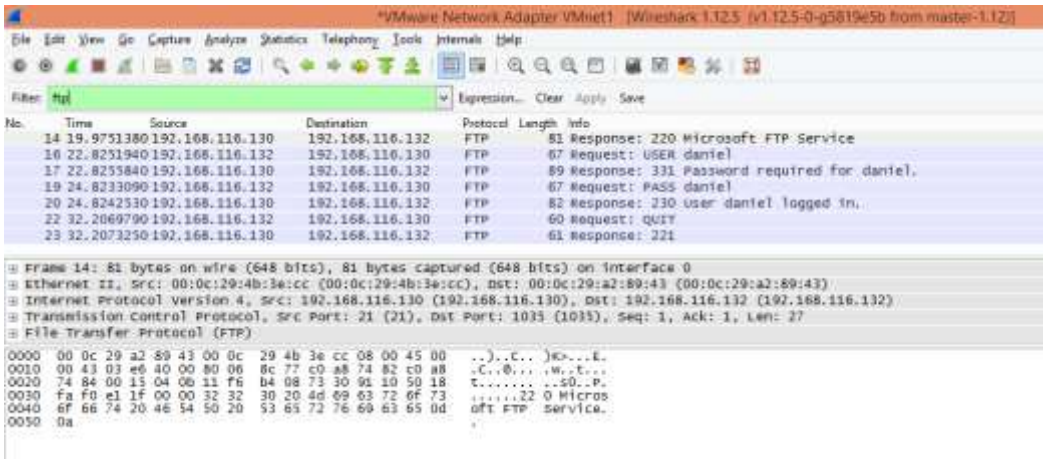



***Ilustración 29:*** **Tráfico FTP capturado sin túnel VPN**

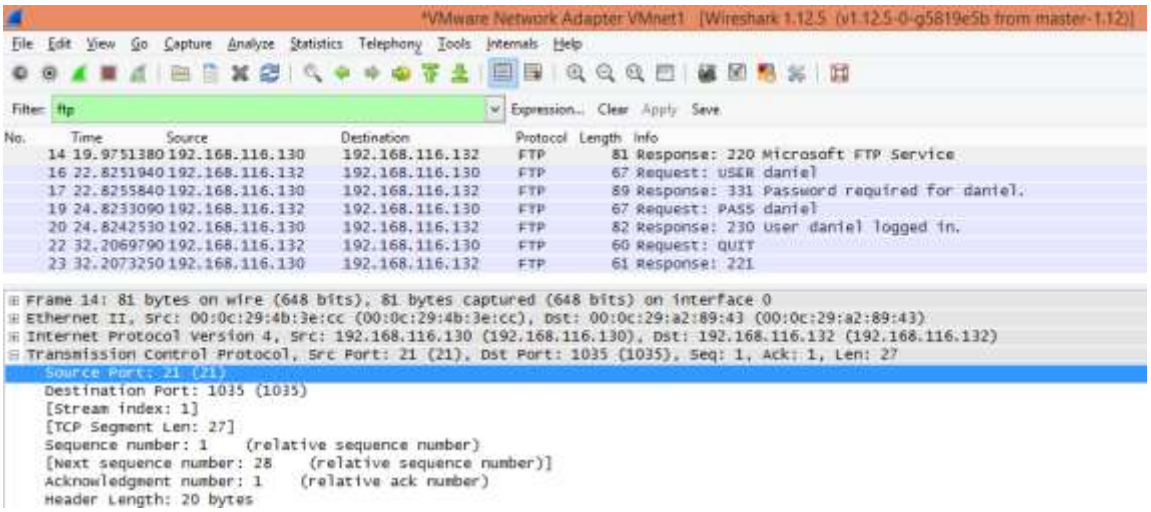



***Ilustración 30:*** **Tráfico FTP capturado sin túnel VPN**

Utilizando el mismo esquema de conexión de la figura 4.4 se procedió a realizar una segunda captura de paquetes de datos de una sesión FTP pero a través de un túnel VPN (Anexo 02 y 03), estos datos se muestran en la **Ilustración 31 y 32**.

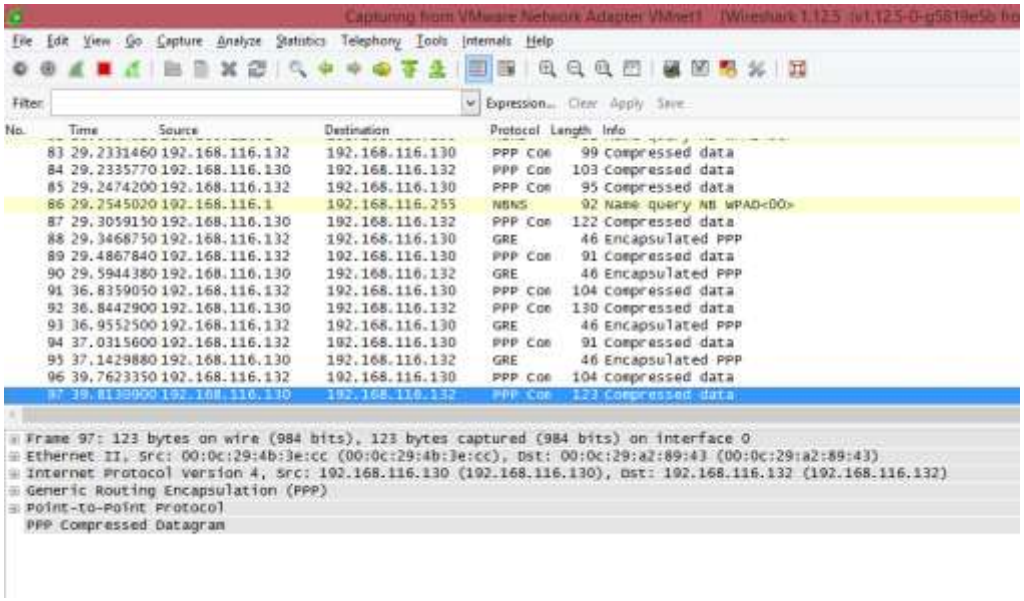



***Ilustración 31:*** **Tráfico FTP capturado con túnel VPN**

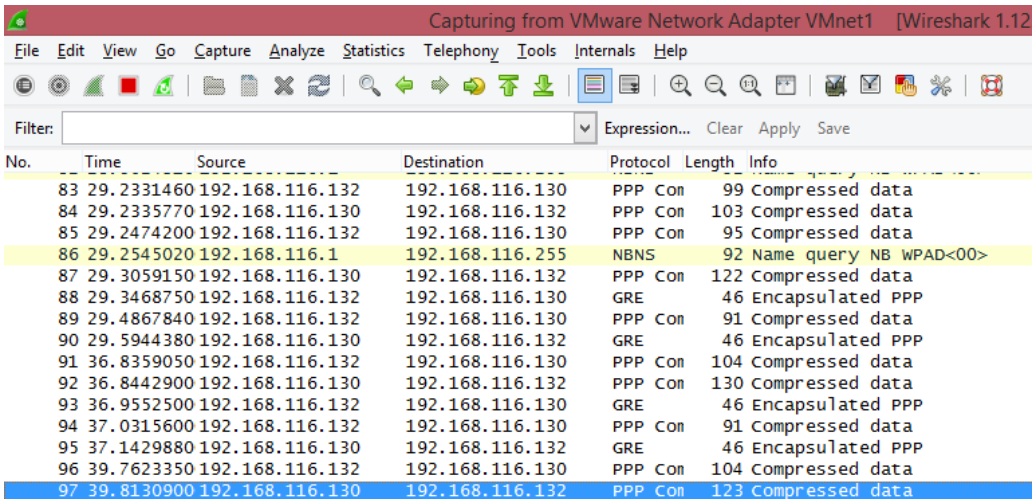



***Ilustración 32:*** **Tráfico FTP capturado con túnel VPN**

## Resultados

En la sesión de FTP sin túnel VPN se pueden observar los números de los puertos asociados en la conexión, esto permite determinar fácilmente el servicio que se está ejecutando. Se descubre entonces que el servidor FTP escucha y transmite por el puerto TCP 21 y el cliente FTP utiliza el puerto TCP 1035.

Cuando se utiliza el túnel IPSec solamente podemos ver los paquetes nativos de este protocolo, no podemos saber qué aplicación se está

ejecutando ni qué servicios hay disponibles. IPSec asegura todos los datos, sin tomar en cuenta la aplicación que se está ejecutando entre los entes involucrados en la transmisión.

Las pruebas de seguridad justifican la utilización de un túnel IPSec, ya que éste difiere de SSL y otros protocolos de cifrado basado en una aplicación, porque IPSec cifra los datos desde la capa 3 (capa de red del modelo OSI) por lo tanto ningún dato de capas superiores es mostrado, reduciendo así las vulnerabilidades de seguridad.

# CAPITULO V

## 5.1. IMPLEMENTACION DE REDES PRIVADAS VIRTUALES UTILIZANDO IPSEC

La metodología para la implementación en la realización de esta investigación, con Redes Privadas Virtuales se basó en:

- Instalación, configuración y pruebas.
- Análisis de un caso práctico; simulación de una oficina central, con el software de virtualización VMWare y un cliente de igual manera virtualizado en VMWare, que podría usar un sistema operativo en Windows o en linux

## 5.2. INSTALACIÓN Y CONFIGURACIÓN

Para la instalación de la red privada virtual se escogió un software de dominio público (GNU) de nombre OPENVPN, que es una implementación de Linux de la VPN.

Se utilizó el sistema operativo Linux Centos 6.5 con una Versión del kernel 2.6.

Es en este caso necesario el uso de certificados digitales para establecer la conexión segura, estos certificados deben de ser confiables, o sea que deben de ser validados (firmados) por una autoridad de certificación que actúa como notario, asegurando que el certificado firmado es del ente (persona, equipo, software, etc.) que dice ser; estos certificados se realizaron utilizando el programa de fuente abierta openSSL. Se generaron 3 certificados, para la Autoridad de Certificación (CA), para el servidor VPN y para el cliente VPN.

Se instaló el cliente VPN bajo Windows 2000 profesional o Linux, y se instaló el certificado generado por la CA.

Una vez completada la instalación y configuración de los equipos se preparó el escenario de conexión que se muestra a continuación (**Ilustración 33**)

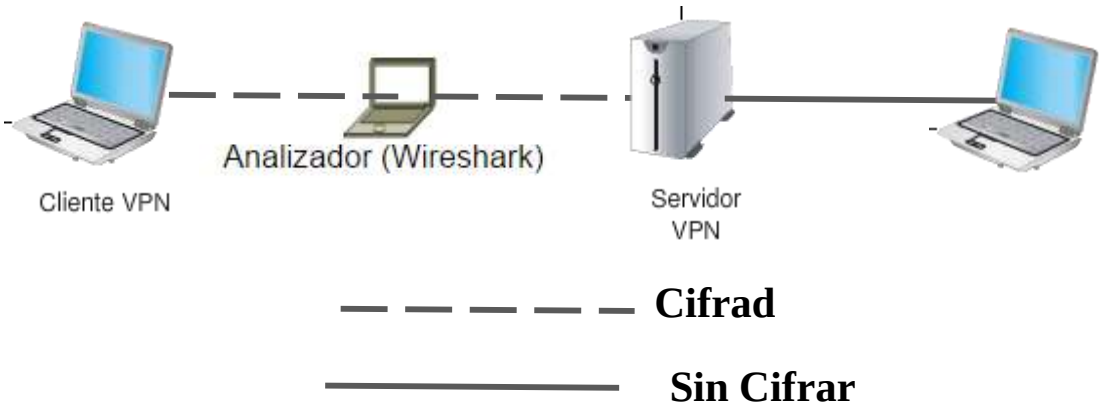



***Ilustración 33:*** **Topología de conexión VPN.**

La mejor elección de una u otra tecnología, depende de los requerimientos de la organización o empresa, así como de la infraestructura de la misma, también se deben tomar en cuenta factores importantes como el rendimiento y el nivel de uso. A partir de las diferencias, ventajas y desventajas de IPSec y SSL citadas anteriormente, se presentan dos tablas que ofrecen criterios importantes a ser tomados en cuenta para inclinarnos por una u otra tecnología:

**Tabla 05: Algoritmos para la transmisión segura de los datos**

| Algoritmo | DES | 3DES | AES | IDEA |
|---|---|---|---|---|
| **Tamaño de la Clave** | 56 bits | 168 bits | 128, 192, 256 bits | 128 bits |
| **Tamaño de bloque** | 64 bits | 64 bits | 128 bits | 64 bits |
| **N° de vueltas** | 16 | 48 | 10, 12, 14 | 8 |
| **Vulnerabilidad** | Dejo de ser utilizado en 1998 Por EE.UU. por haber sido vulnerado | Es 3 veces más seguro que el DES pero a la vez es 3 veces más lento. | No ha sido vulnerado | Es robusto frente al criptoanálisis diferencial y diferencial Imposible los ataques por fuerza bruta |
| **Observaciones** | Creado en 1977 | Publicado en 1999 Está en desuso | Desarrollado en 1997 En el 2003 fue declarado seguro por EE.UU Fue creado para reemplazar al 3DES Es más rápido que el 3DES | Fue desarrollado en 1990 y mejorado en 1992 |
| | | | Seguro y Usado en VPNS con IPSEC | |

**Fuente: Creación propia.**

**Tabla 06:** ***Diversas técnicas de encriptación de datos en una red privada virtual***

| | **SSL/TLS** | **IPsec** |
|---|---|---|
| **Control de accesos** | | |
| Conexiones permanentes | | **X** |
| Conexiones efímeras o puestos móviles | **X** | |
| Ambos Tipos de acceso | **X** | **X** |
| **Usuarios** | | |
| Todos los usuarios son empleados de la compañía | | **X** |
| No todos los usuarios son empleados de la compañía | **X** | |
| No todos los usuarios son empleados de la compañía, además algunos trabajan con sus propios sistemas | **X** | **X** |
| **Software Cliente** | | |
| Todos los usuarios han de tener acceso a todos los recursos de la red | | **X** |
| Deseamos controlar el acceso a determinadas aplicaciones | **X** | |
| Necesitamos niveles variables de control de acceso en las diferentes aplicaciones | **X** | **X** |
| **Confidencialidad y Autenticidad** | | |
| Precisamos de un alto nivel de seguridad en el cifrado y autentificación | | **X** |
| La confidencialidad y la autenticidad no son especialmente críticas en nuestros sistemas | **X** | |
| Precisamos de niveles moderados de confidencialidad e integridad | **X** | |
| **Nivel Técnico de los Usuarios** | | |
| Entre moderado y alto | | **X** |
| Entre moderado y bajo | **X** | |
| **Implantación, flexibilidad y escalabilidad** | | |
| Deseamos una implantación rápida y de facilidad mantenimiento | **X** | |
| Deseamos flexibilidad en las modificaciones futuras | | **X** |
| Ambas consideraciones son importantes | **X** | **X** |

**Fuente: creación propia**

**Tabla 07: *Protocolos – Soluciones***

| SOLUCIONES | SSL | IPSEC | COMENTARIO |
|---|---|---|---|
| **Telecommuter** Ej. Empleados trabajando desde casa | Apropiado | Ideal | IPSec proporciona acceso seguro a todos los recursos y aplicaciones.<br><br>SSL da acceso a aplicaciones sólo SSL |
| **VPN Red-a-Red** Ej. Oficina remota conectada a WAN corporativa | Inapropiado | Ideal | IPSec provee túneles seguros entre localizaciones fijas |
| **Web mail Remoto** Ej. Outlook Web, Lotus iNotes | Ideal | Complejo | SSL permite acceso seguro desde cualquier navegador web. |
| **Seguridad interna de aplicación** Ej. HR Self-service | Ideal | Complejo | SSL proporciona seguridad de la aplicación dentro de la VPN |
| **Portales de aplicación** Ej. iPlanet, aplicaciones web corporativas | Ideal | Complejo | SSL es la elección más simple<br>IPSec es muy complejo |
| **Seguridad VOIP** Ej. Ethernet red–a-red o telecommuter con VoIP | Inapropiado | Ideal | VOIP no puede transportarse en<br>SSL<br>IPSec es la solución para encriptación de VoIP |
| **Seguridad en Wireless LAN** Ej. Proveer seguridad a las WLAN con autenticación y encriptación fuerte | Apropiado | Ideal | IPSec proporciona acceso seguro a todos los recursos de la red.<br><br>SSL requiere 'traducir' aplicaciones a HTTP. |

**Fuente: creación propia**

### 5.3. Discusión de resultados

- Tanto IPSec como SSL son tecnologías confiables y eficaces, que pueden ser usadas para proveer seguridad en comunicaciones altamente sensibles.
- Cada una de estas tecnologías tiene sus ventajas y desventajas, y su mayor rendimiento dependerá del escenario en el que se encuentren operando.
- IPSec es un protocolo muy seguro, basado en estándares y muy adecuado para tráficos totalmente IP. El uso de este protocolo es el más indicado cuando se tienen los siguientes requerimientos:
    - Conexiones permanentes
    - Todos los usuarios son empleados de la compañía
    - Todos los usuarios han de tener acceso a todos los recursos de la red
    - Precisamos de un alto nivel de seguridad en el cifrado y autentificación
    - Deseamos flexibilidad en las modificaciones futuras de la red.
- También podemos concluir que IPSec se considera un protocolo ideal para las siguientes aplicaciones:
    - VPN Acceso remoto.
    - VPN Red-a-Red
    - Seguridad VoIP
    - Seguridad en Wireless LAN
- SSL es un protocolo que ofrece una mayor sencillez a la hora de crear conexiones seguras por Internet. El uso de este protocolo es el más indicado cuando se tienen los siguientes requerimientos:
    - Conexiones efímeras o puestos móviles
    - No todos los usuarios son empleados de la compañía
    - Deseamos controlar el acceso a determinadas aplicaciones

  - La confidencialidad y la autenticidad no son especialmente críticas en nuestros sistemas
  - Deseamos una implantación rápida y de facilidad mantenimiento
- También podemos concluir que SSL se considera un protocolo ideal o apropiado para las siguientes aplicaciones:
  - VPN Acceso remoto.
  - Web mail remoto.
  - Seguridad interna de aplicación
  - Portales de aplicación
  - Seguridad en Wireless LAN
- Finalmente podemos decir que las empresas pueden beneficiarse de usar IPsec y SSL en sus redes privadas virtuales al aplicar cada una de estas tecnologías en las aplicaciones y para los requerimientos apropiados.

# CONCLUSIONES

- Podemos concluir que la implementación de VPN´s, es más segura cuando se utilizan Túneles IPSec , esto por su bajo costo y grandes prestaciones, además del hecho implícito de seguridad que trae el código abierto, por lo que es posible estudiar y modificar el código para adaptarlo a las necesidades del servidor.

- De acuerdo con los resultados que se han obtenido en las pruebas de rendimiento y seguridad se pudo comprobar que en la práctica la implementación de Redes Privadas Virtuales es factible desde muchos puntos de vista (económicos, de seguridad, de confiabilidad, etc) además trae muchos beneficios asociados a la conectividad de usuarios remotos y oficinas distantes, esto a pesar de la sobrecarga introducida por el uso de VPN no afecta de manera significativa en las redes de datos.

- El uso de Túneles aplicada a las Redes Privadas Virtuales (VPN), dan una mejor fiabilidad de seguridad, autenticación y confiabilidad en las transmisiones sobre redes públicas como es el caso de Internet.

# RECOMENDACIONES

- Se recomienda el uso de Redes Privadas Virtuales en conexiones que se realizan sobre la red pública (Internet) entre dependencias de instituciones geográficamente distantes, además de representar un bajo costo por el uso de una red pública en contraste al uso de líneas dedicadas.

- Analizar las posibilidades de uso comercial de implementar Redes Privadas Virtuales (VPN) utilizando código Abierto o Libre.

- Estudiar la Implementación de VPNs en las dependencias de las instituciones que utilizan enlaces inalámbricos, como manera de garantizar la integridad y la confidencialidad en el intercambio de información, previniendo el robo de contraseñas de usuarios y permitir un control en el acceso de todos los clientes inalámbricos.

- Implementar un manual de políticas de seguridad asociadas a la implementación de VPNs, así como un completo entendimiento de criptografía de clave pública y manejo de certificados y firmas digitales.

# BIBLIOGRAFÍA

Aldaya, A. C. (Diciembre de 2013). Diseño e integración de algoritmos criptográficos en sistemas empotrados sobre FPGA. *EAC*, 51.

Alonso, J. A. (2009). *Redes privadas virtuales.* España: RA-MA.

Cisco. (2013). *Informe Anual de Seguridad.* EEUU.

Cisco. (2014). *Informe Anual de Seguridad.* EEUU.

Eset. (2013). *Estudio de seguridad.* EEUU.

Gonzales Morales, A. (2008). *Red Privada Virtual.* Perú.

Hernández, A. F. (Febrero de 2012). Implementación multinúcleo de la multiplicación escalar en curvas de Koblitz. México, México.

Latinoamérica, E. (2013). *Tendencias 2014 en Seguridad Informática.* México.

Li, C., & Sun, C. (2012). *Secure VPN Based on Combination of L2TP and IpSec.* EEUU.

Lomparte, K. R. (2005). Encriptación RSA de archivos de texto. Lima, Lima, Perú.

Lucena Lopez, M. (2010). *Criptografía y Seguridad en Computadoras.* Colombia.

Maiorano, A. (2010). *Criptografía – Técnicas de desarrollo para profesionales.* Segu-info.

Meza, N. P. (2014). Análisis y mejora del rendimiento del algoritmo AES para su utilización en teléfonos móviles. México, México, México.

Padilla, J. L. (2014). *Investigaciones en tecnologías de información informática y computación.* EEUU: Palibrio LLC.

Ramírez, A. H. (Octubre de 2012). Implementación de la criptografía basada en atributos en un dispositivo móvil. México, México, México.

Real Academia. (2010). *Diccionario.*

Sciences, J. o. (2014). *Adaptive Data Hiding Based on Visual Cryptography.* EEUU.

Wikipedia. (10 de Junio de 2014). *Advanced Encryption Standard*. Obtenido de http://es.wikipedia.org/wiki/Advanced_Encryption_Standard

Bellovin, Steven M. (1996). «Problem Areas for the IP Security Protocols». Proceedings of the Sixth Usenix Unix Security Symposium: 1-16.

K.G. Paterson y A. Yau (2006). «Cryptography in theory and practice: The case of encryption in IPsec». Eurocrypt 2006, Lecture Notes in Computer Science Vol. 4004: 12-29.

J.P. Degabriele y K.G. Paterson (2007). «Attacking the IPsec Standards in Encryption-only Configurations». IEEE Symposium on Security and Privacy, IEEE Computer Society: 335-349.

# ANEXOS

# Anexo 01

## CONFIGURACION DE SERVIDOR FTP EN LINUX CENTOS 6.5

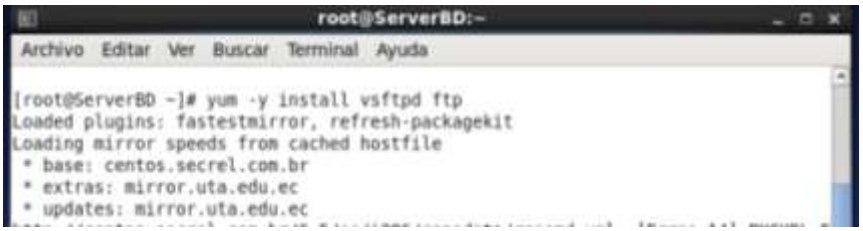
- En este anexo paso a paso se describe cómo instalar y configurar un servidor de protocolo de transferencia de archivos (FTP).
- En el caso del Linux Centos, el servidor debe tener un programa instalado para poder utilizar el servicio FTP; en este caso vamos a usar el servidor VSFTPD. Este es un servidor FTP rápido y seguro para sistemas Unix / Linux.
- Para instalar el servicio FTP, seguimos estos pasos:

**Parámetros para la configuración del servidor:**

- El nombre de mi servidor es serverDB y la dirección IP es 192.168.25.133/24. Estos valores cambiarán según su red.

**Instalación de VSFTPD**

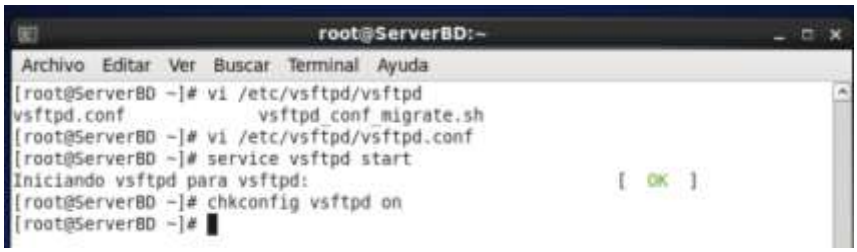
- Todos los comandos deben emitirse con el usuario 'root'. Ejecute el siguiente comando en la terminal para instalar el paquete vsftpd:
- # yum –y install vsftpd ftp




**Configuración de VSFTPD**

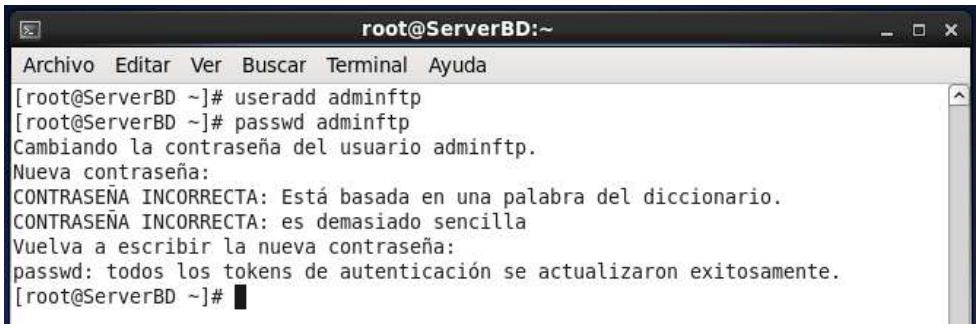
- Se debe editar el archivo de configuración del VSTFPD, el cual se encuentra en la siguiente ruta: /etc/vsftpd/vsftpd.conf.


- Debemos encontrar las siguientes líneas y hacer los cambios como se muestra a continuación:
- [...]
- **## Establecemos este valor en NO ##**
- Esta opción permite ingresar sin necesidad de tener un usuario configurado, la recomendación es dejarla en NO si no queremos que esto suceda.
    - anonymous_enable=NO
- ## Descomentar estas dos líneas ##
    - ascii_upload_enable=YES
    - ascii_download_enable=YES
- ## Eliminamos el comentario – Escribimos el mensaje de bienvenida - Esto es opcional ##
- Esta opción permite poner un mensaje de bienvenida para que cuando iniciamos sesión en el cliente de FTP se muestre el Slogan o Nombre de nuestro sitio o empresa.
    - ftpd_banner= Bienvenidos a Mi Sitio FTP - SIPAN.
- ## Añadir esta línea al final del archivo ##
- Esta opción se habilita para que el servidor FTP, utilice la hora local.
    - use_localtime=YES
- Iniciamos el servicio vsftpd y hacemos que se inicie automáticamente en cada reinicio:

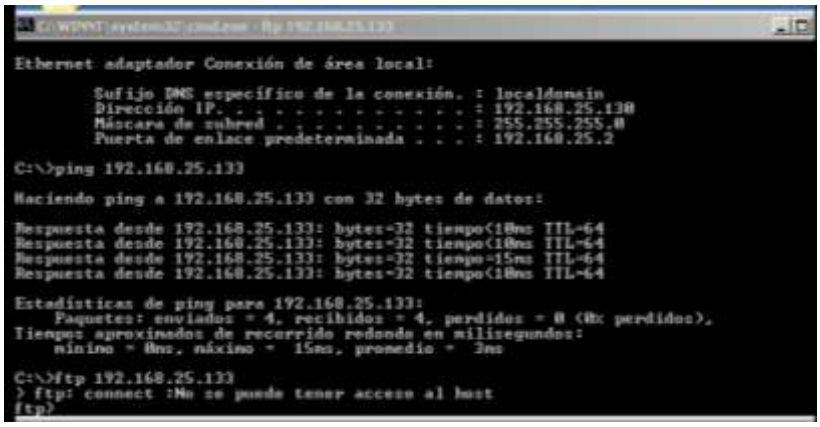



**Crear usuarios FTP**

- Por defecto, al usuario root no se le permite iniciar sesión en el servidor ftp para fines de seguridad. Así que vamos a crear un usuario de prueba llamado "adminftp" con la contraseña "centos":




**Ahora iniciamos una nueva sesión con el servidor FTP** (lo podemos realizar desde cualquier cliente Windows o Linux)**:**




- Limpiamos las reglas del firewall

```
[root@ServerBD ~]# iptables -F
[root@ServerBD ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@ServerBD ~]#
```

- Ahora podremos conectarnos a un servidor FTP sin ningún problema.

```
C:\>ftp 192.168.25.133
Conectado a 192.168.25.133.
220 Bienvenidos a mi sitio FTP - SIPAN.
Usuario (192.168.25.133:(none)): adminftp
331 Please specify the password.
Contraseña:
500 OOPS: cannot change directory:/home/adminftp
Error al iniciar la sesión.
ftp>
```

- Se obtendrá un error como "500 oops: cannot change directory".
- Esto es porque el SELinux restringe al usuario para iniciar sesión en el servidor ftp. Así que vamos a actualizar los valores booleanos de SELinux para el servicio FTP, usamos el siguiente comando:
  - **setenforce 0**

```
setfiles              setsid
[root@ServerBD ~]# setenforce 0
[root@ServerBD ~]#
```

- Ahora iniciamos una nueva sesión con el servidor FTP:

```
C:\>ftp 192.168.25.133
Conectado a 192.168.25.133.
220 Bienvenidos a mi sitio FTP - SIPAN.
Usuario (192.168.25.133:(none)): adminftp
331 Please specify the password.
Contraseña:
230 Login successful.
ftp>
```

# Anexo 02

# INSTALACIÓN Y CONFIGURACIÓN DE SERVIDOR VPN EN LINUX CENTOS 6.5

En este anexo se realizará la instalación de un Servidor VPN en el SO CENTOS 6.5, también se explicará la instalación y configuración de un cliente VPN para su conexión hacia el servidor que hemos creado con anterioridad.

**¿Qué es un Servidor VPN?**

De sus siglas "Virtual Private Network", que a su traducción al español seria "Red Privada Virtual", no es más que una "extensión" ficticia de nuestra red local hacia la red local de destino, permitiendo ser "virtualmente" parte de ella.

**¿Ventajas?**

Existen varias ventajas por el cual podemos encontrar si usamos VPN:

- Son fáciles de montar y no son realmente costosas.
- Mejora la comunicación de los usuarios de la red origen y destino.

**¿Qué es OpenVPN?**

*OpenVPN* es una aplicación de código abierto que implementa una red privada virtual VPN. Puede ser utilizado para crear una conexión segura entre redes de área local distribuidas físicamente.

*OpenVPN Access Server* es una solución software completa de túnel de red seguro mediante VPN, con una interfaz de configuración sencilla mediante web. Posee clientes para Windows, Mac, Linux, Android e iOS.

**OpenVPN Access Server** es compatible con una amplia gama de configuraciones, incluyendo acceso remoto seguro y acceso a redes internas con control de acceso de grano fino.

**Escenario inicial para montar una red VPN con OpenVPN**

Dispondremos de una red local LAN con el direccionamiento 192.168.25.0/24, en la que habrá un servidor y equipos informáticos. Se pretende conseguir que un equipo cliente externo, se pueda comunicar con cualquier equipo de la red interna utilizando las IP's privadas, como si el equipo cliente externo estuviera físicamente conectado a la red interna.

**Prerequisitos para montar una red privada virtual VPN con OpenVPN**

Servidor físico o virtual con sistema operativo Linux CentOS

El servidor que tendrá el rol de *servidor OpenVPN Access Server* debe tener los siguientes requisitos:

- Sistema operativo Linux CentOS 6.5
- *SELinux* desactivado.
- Servicios *iptables* e *ip6tables* deshabilitados.
- El servidor con Linux necesitará conexión a Internet.
- IP Pública estática

Es recomendable, para establecer una VPN con la red privada de nuestra organización o casa, disponer de una IP pública estática. Esta IP nos la proporcionará nuestro proveedor de servicios de Internet. Si no disponemos de IP estática y por el contrario es dinámica, deberemos disponer de algún software que nos envíe la IP pública.

**Instalación y configuración de OpenVPN Access Server en un servidor con Linux CentOS**

Accederemos al servidor con Linux CentOS 6.5, desde la consola del shell de comandos, accediendo con superusuario root, ejecutaremos el siguiente comando:

*rpm -Uvh http://swupdate.openvpn.org/as/openvpn-as-2.0.10-CentOS6.x86_64.rpm*


Una vez instalado *OpenVPN Access Server* con el comando anterior estableceremos la contraseña del usuario administrador.

Por defecto, *OpenVPN Access Server* utiliza autenticación PAM. Esto quiere decir que los usuarios que se configuren en *OpenVPN Access Server* deben existir en el sistema operativo Linux, ya que será este quien valide la contraseña. Inicialmente existe un único usuario llamado *openvpn* que crea el programa de instalación. Es necesario establecerle la contraseña para poder iniciar sesión en la página web de administración de *OpenVPN Access Server*.

Para establecer la contraseña al usuario *openvpn*, en la consola del servidor de Linux, escribiremos el comando:

***passwd openvpn***

Introduciremos la contraseña (centospvn) deseada para el usuario *openvpn*.

```
Client UI: https://192.168.25.133:943/
[root@ServerBD Escritorio]# passwd openvpn
Cambiando la contraseña del usuario openvpn.
Nueva contraseña:
CONTRASEÑA INCORRECTA: Está basada en una palabra del diccionario.
Vuelva a escribir la nueva contraseña:
passwd: todos los tokens de autenticación se actualizaron exitosamente.
[root@ServerBD Escritorio]#
```

Tras la instalación de *OpenVPN Access Server* y el establecimiento de la contraseña para el usuario openvpn estaremos en disposición de iniciar la configuración de *OpenVPN Access Server*, para ello abriremos un navegador web (podemos abrirlo desde cualquier equipo de la red LAN del servidor de OpenVPN) e introduciremos la URL:

*https://192.168.25.133:943/admin*

(192.168.25.133 será la IP del servidor Linux CentOS con OpenVPN)

También se podría utilizar la URL de acceso externo si ya hemos redireccionado los puertos (como indicamos aquí):

*https://{IP pública}:943/admin*

El navegador informará de que el certificado no está validado, aun así podemos continuar. Esto se debe a que el certificado ha sido generado por el propio servidor en el momento de la instalación, pulsando en "Opciones Avanzadas" podremos ver el detalle del mensaje de aviso:


Pulsaremos en "Acceder a 192.168.25.133 (Entiendo los riesgos)":


Iniciamos sesión utilizando el usuario *openvpn* y la contraseña que se le estableció:


La primera vez que se accede a la consola de administración web de OpenVPN Access Server mostrará un formulario de aceptación de la licencia. Lo leeremos y si estamos de acuerdo pulsaremos "Agree" para continuar:

Nos mostrará la página principal de la consola de administración web de *OpenVPN Access Server*:


La configuración básica es bastante simple, accederemos a sección *Server Network Settings*. En esta ventana estableceremos los siguientes valores:

**Hostname or IP Address**: en este campo introduciremos la IP pública del router (que podemos obtener como indicamos aquí). Si disponemos de un dominio registrado que apunta a la IP pública podremos utilizarlo también.

*Interface and IP Address*: marcaremos eth0: 192.168.25.133.

**Protocol**: marcaremos Both (Multi-daemon mode).

El resto de valores los dejaremos por defecto:

**Number of TCP daemon**: 2.

*TCP Port number*: 443.

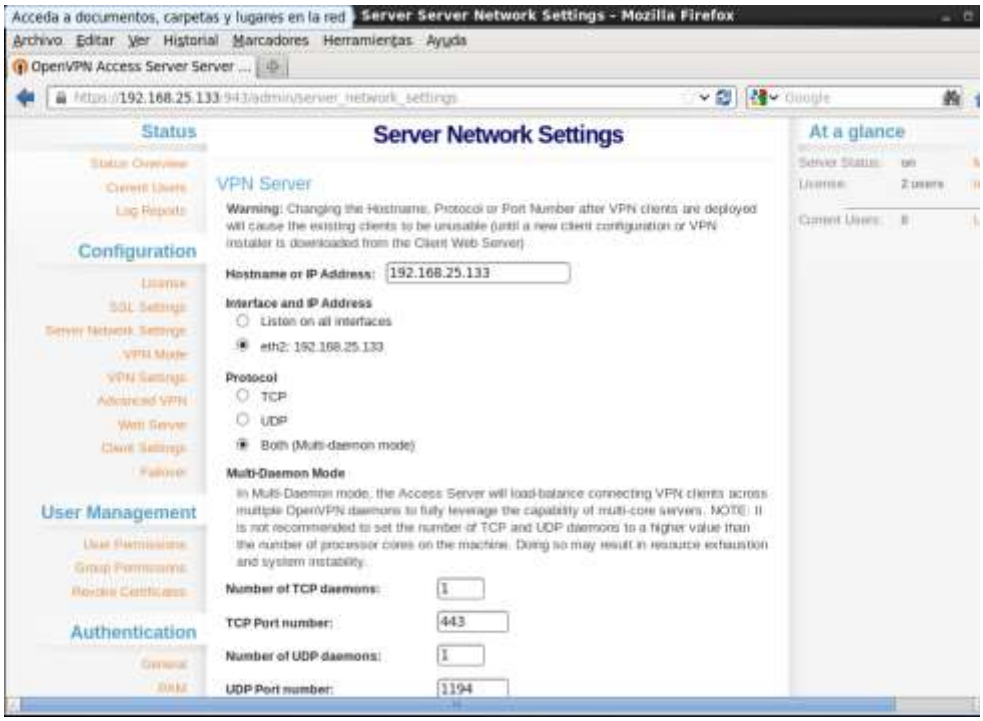
*Number of UDP daemons*: 2.

*UDP Port number*: 1194.

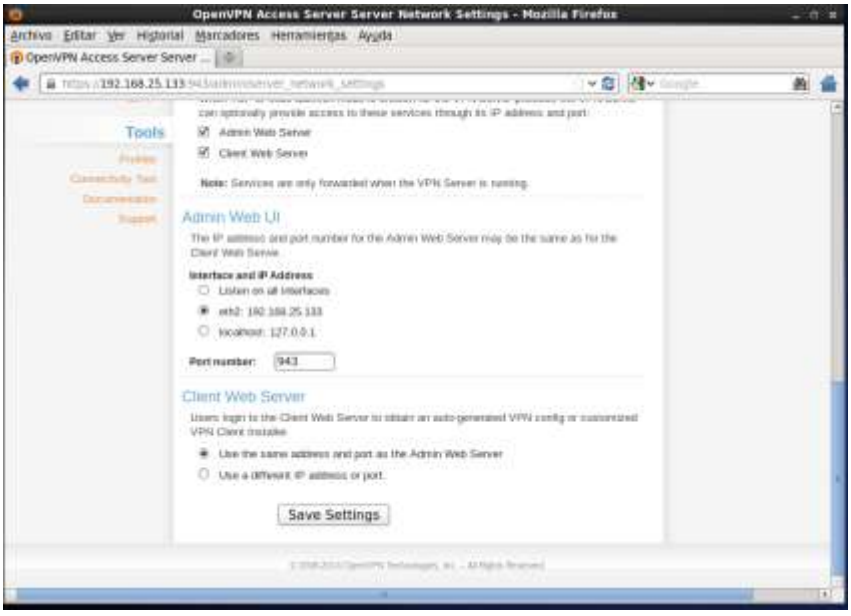
Service Forwarding:

**Admin Web Server**: maraceremos esta opción.

*Client Web Server*: marcaremos esta opción.




A continuación se guardarán los cambios, pulsando en *Save Settings* (al final de la página):




Aplicaremos la configuración pulsando sobre el botón *Update Running Server*:


De esta forma ya tendremos el servidor OpenVPN configurado.

# Anexo 03

# INSTALACIÓN Y CONFIGURACIÓN DE CLIENTE VPN

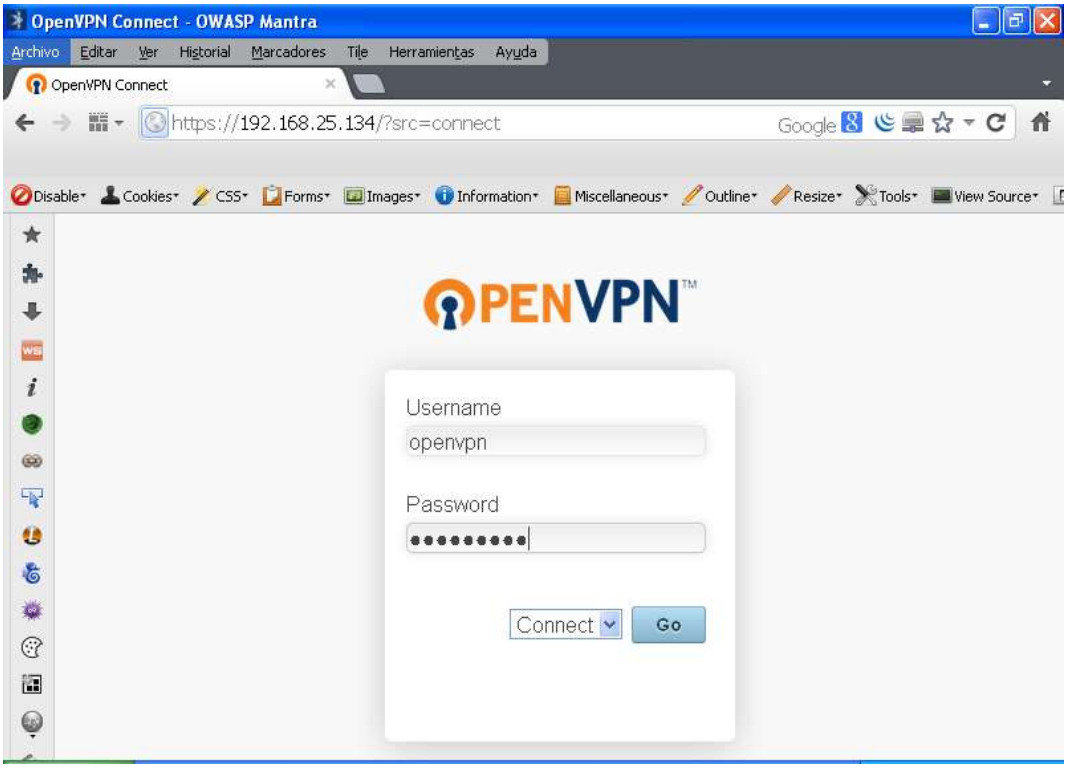
Aquí configuraremos un cliente VPN que nos permitirá la conexión al servidor que anteriormente hemos configurado.

## Configurar el acceso VPN desde un equipo cliente desde fuera de la red, desde Internet

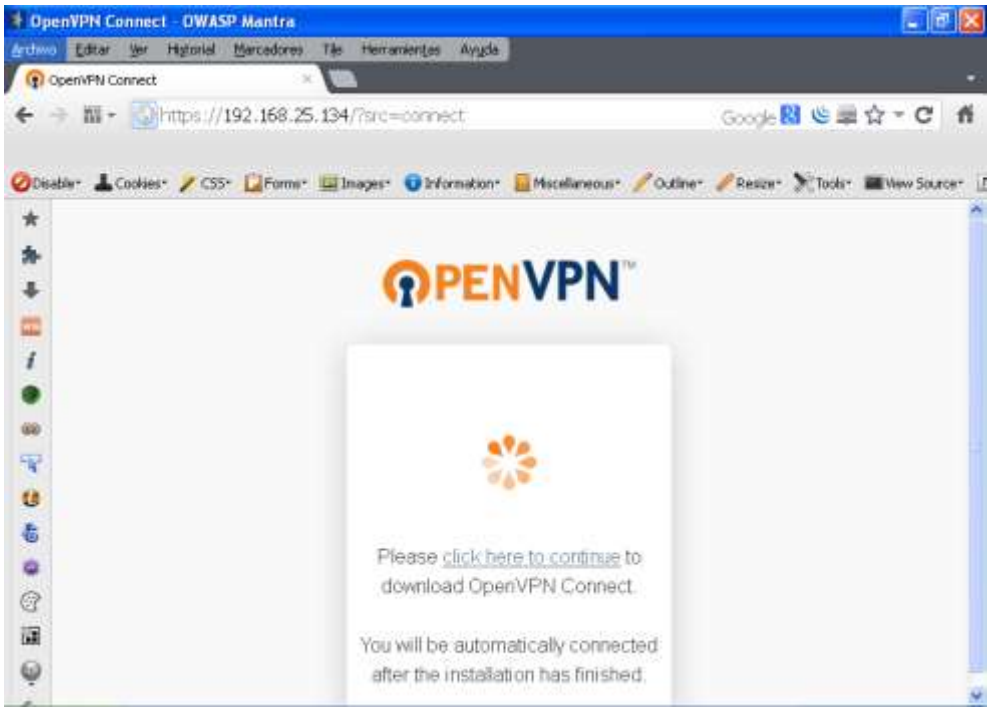
Una vez montado el servidor OpenVPN y configurado ya estaremos en disposición de poder conectarnos desde un equipo externo a través de Internet. Para ello, en el equipo cliente, situado fuera de la red interna LAN, que tenga acceso a Internet, abriremos un navegador y accederemos a la la URL:

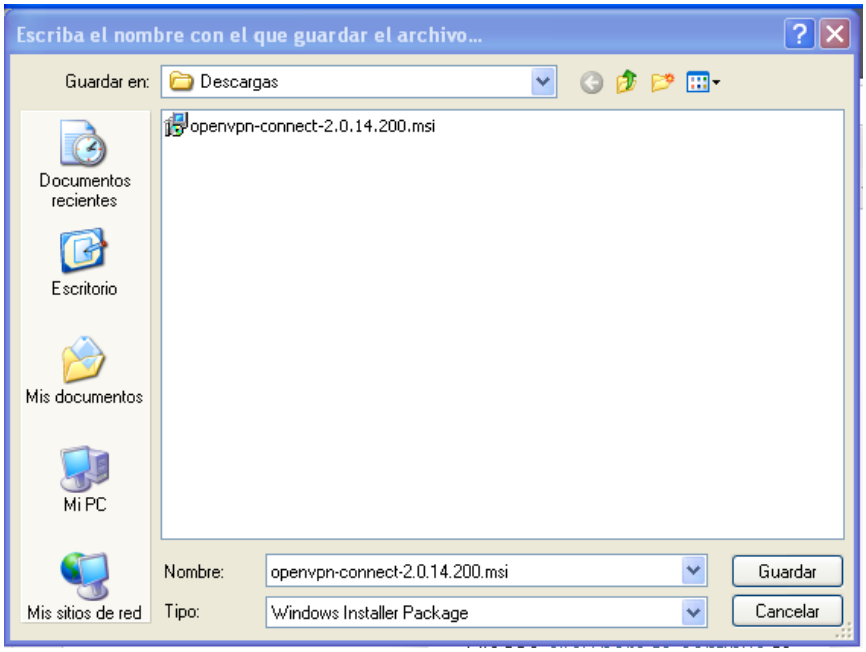
*https://{IP pública del router de la red interna}*

Nos mostrará la ventana de inicio de sesión de OpenVPN, introduciremos usuario y contraseña establecidos en la configuración de OpenVPN:


Pulsaremos en "Click here to continue", de esta forma se iniciará la descarga de la aplicación cliente de OpenVPN. Una vez descargado el fichero*openvpn-connect-xxx.msi* lo ejecutaremos:



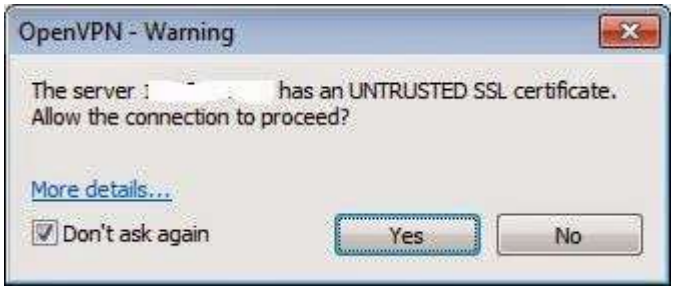




El programa cliente de OpenVPN se instalará directamente creando un acceso directo en el escritorio y en el menú de inicio:

Al terminar la instalación el cliente se autoejecutará. Para conectar al servidor OpenVPN pulsaremos con el botón secundario del ratón sobre el icono del cliente OpenVPN, que se habrá situado en el área de notificación (de color naranja con un aspa en color gris) y seleccionaremos *Connect to {IP pública}*:

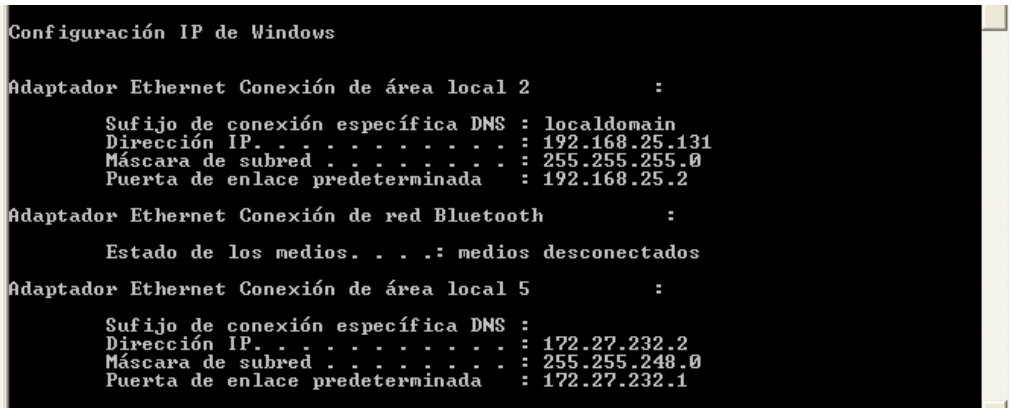
Introduciremos las credenciales de acceso al servidor OpenVPN:


Y por último aceptaremos el aviso sobre que el certificado no está verificado pulsando en "Yes":




Con el texto: *The server xxx has an UNTRUSTED SSL certificate. Allow the connection to proceed?*

A partir de este momento tendremos asignada una IP de la red 127.27.232.0/20 y ya tendremos acceso a cualquier equipo de la red interna 192.168.25.0/24.


Configuración IP de Windows
Adaptador Ethernet Conexión de área local 2 :
Sufijo de conexión específica DNS : localdomain
Dirección IP. . . . . : 192.168.25.131
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada : 192.168.25.2
Adaptador Ethernet Conexión de red Bluetooth :
Estado de los medios. . . .: medios desconectados
Adaptador Ethernet Conexión de área local 5 :
Sufijo de conexión específica DNS :
Dirección IP. . . . . : 172.27.232.2
Máscara de subred . . . . . : 255.255.248.0
Puerta de enlace predeterminada : 172.27.232.1

# Anexo 04

# WIRESHARK

Wireshark, una herramienta de análisis de redes antes conocido como Ethereal, captura los paquetes en tiempo real y los muestra en formato legible por humanos.

Wireshark incluye filtros, código de colores y otras características que le permiten profundizar en el tráfico de red e inspeccionar los paquetes individuales.

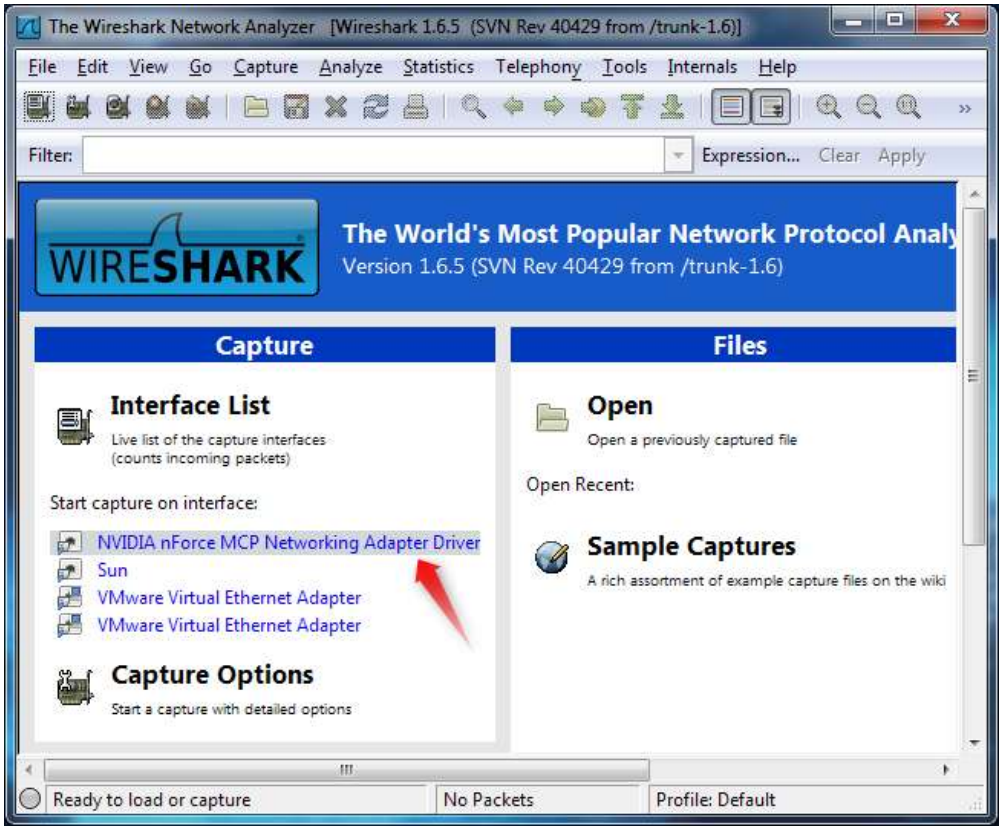
Aquí se mostrara los conceptos básicos de la captura de paquetes, filtrados y control de dichos aparatos. Puede utilizar Wireshark para inspeccionar el tráfico de red de un programa sospechoso, analizar el flujo de tráfico en la red, o solucionar problemas de red.

Puede descargar Wireshark para Windows, Linux o Mac OS X desde http://www.wireshark.org/download.html . Si está utilizando Linux u otro sistema UNIX, es probable que encuentres Wireshark en sus repositorios de paquetes. Por ejemplo, si estás usando Ubuntu, encontrará Wireshark en el Centro de Software de Ubuntu.

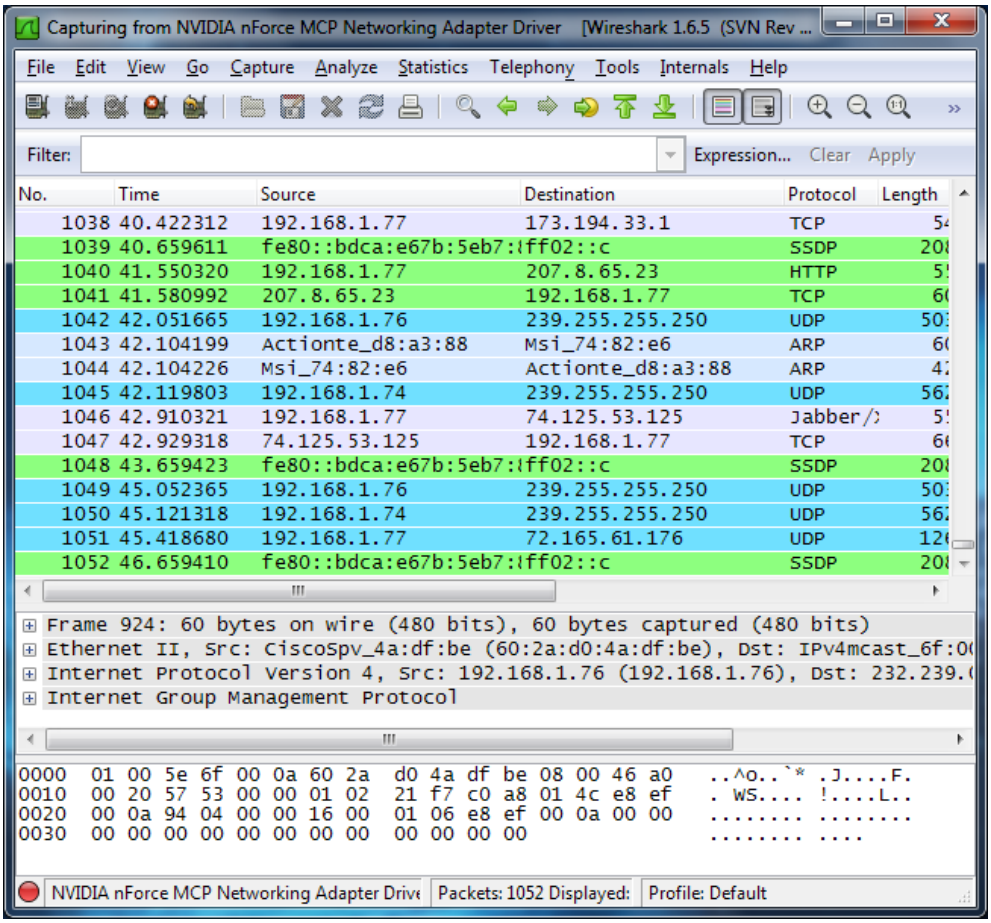
**Captura de paquetes**

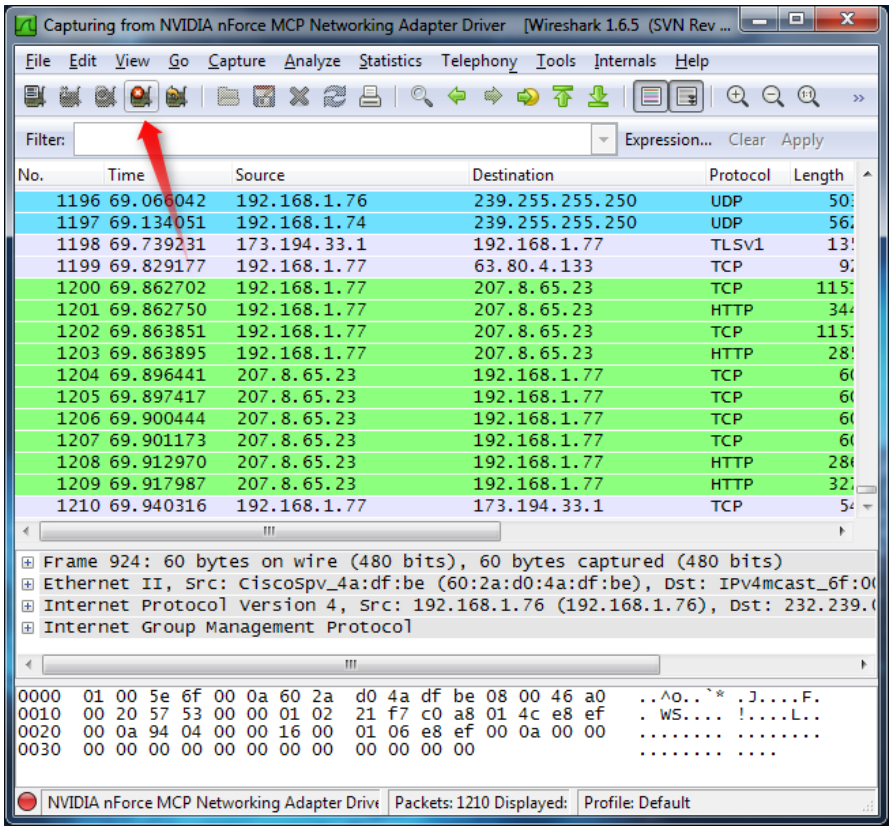
Después de descargar e instalar Wireshark, podemos iniciar y hacer clic en el nombre de una interfaz en la Lista de interfaz para comenzar la captura de

paquetes en esa interfaz. Por ejemplo, si desea capturar el tráfico en la red inalámbrica, haga clic en la interfaz inalámbrica.



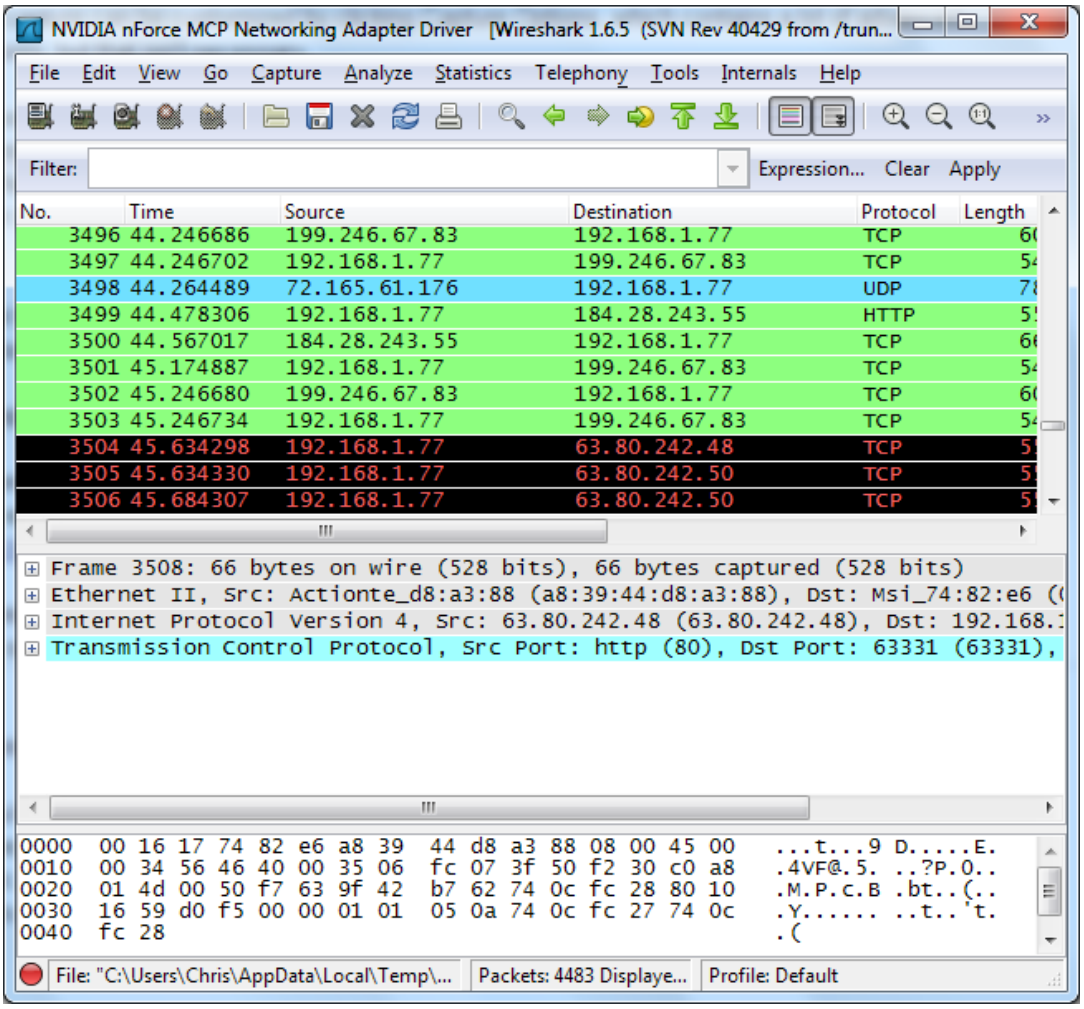

Tan pronto como haga clic en el nombre de la interfaz, verá los paquetes que comienzan a aparecer en tiempo real. Wireshark captura cada paquete enviado desde o hacia su sistema. Si está capturando en una interfaz inalámbrica y tiene el modo promiscuo habilitado en sus opciones de captura, también verá los otros paquetes en la red.


Capturing from NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev ...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Length
1038 40.422312 192.168.1.77 173.194.33.1 TCP
1039 40.659611 fe80::bdca:e67b:5eb7: ff02::c SSDP
1040 41.550320 192.168.1.77 207.8.65.23 HTTP
1041 41.580992 207.8.65.23 192.168.1.77 TCP
1042 42.051665 192.168.1.76 239.255.255.250 UDP
1043 42.104199 Actionte_d8:a3:88 Msi_74:82:e6 ARP
1044 42.104226 Msi_74:82:e6 Actionte_d8:a3:88 ARP
1045 42.119803 192.168.1.74 239.255.255.250 UDP
1046 42.910321 192.168.1.77 74.125.53.125 Jabber/
1047 42.929318 74.125.53.125 192.168.1.77 TCP
1048 43.659423 fe80::bdca:e67b:5eb7: ff02::c SSDP
1049 45.052365 192.168.1.76 239.255.255.250 UDP
1050 45.121318 192.168.1.74 239.255.255.250 UDP
1051 45.418680 192.168.1.77 72.165.61.176 UDP
1052 46.659410 fe80::bdca:e67b:5eb7: ff02::c SSDP
Frame 924: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: CiscoSpv_4a:df:be (60:2a:d0:4a:df:be), Dst: IPv4mcast_6f:0
Internet Protocol Version 4, Src: 192.168.1.76 (192.168.1.76), Dst: 232.239.
Internet Group Management Protocol
0000 01 00 5e 6f 00 0a 60 2a d0 4a df be 08 00 46 a0 ..^o..`* .J....F.
0010 00 20 57 53 00 00 01 02 21 f7 c0 a8 01 4c e8 ef . WS.... !....L..
0020 00 0a 94 04 00 00 16 00 01 06 e8 ef 00 0a 00 00 ........ ........
0030 00 00 00 00 00 00 00 00 00 00 00 00 ........ ....
NVIDIA nForce MCP Networking Adapter Drive
Packets: 1052 Displayed:
Profile: Default


Capturing from NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev ...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Length
1196 69.066042 192.168.1.76 239.255.255.250 UDP
1197 69.134051 192.168.1.74 239.255.255.250 UDP
1198 69.739231 173.194.33.1 192.168.1.77 TLSv1
1199 69.829177 192.168.1.77 63.80.4.133 TCP
1200 69.862702 192.168.1.77 207.8.65.23 TCP
1201 69.862750 192.168.1.77 207.8.65.23 HTTP
1202 69.863851 192.168.1.77 207.8.65.23 TCP
1203 69.863895 192.168.1.77 207.8.65.23 HTTP
1204 69.896441 207.8.65.23 192.168.1.77 TCP
1205 69.897417 207.8.65.23 192.168.1.77 TCP
1206 69.900444 207.8.65.23 192.168.1.77 TCP
1207 69.901173 207.8.65.23 192.168.1.77 TCP
1208 69.912970 207.8.65.23 192.168.1.77 HTTP
1209 69.917987 207.8.65.23 192.168.1.77 HTTP
1210 69.940316 192.168.1.77 173.194.33.1 TCP
Frame 924: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: CiscoSpv_4a:df:be (60:2a:d0:4a:df:be), Dst: IPv4mcast_6f:0
Internet Protocol Version 4, Src: 192.168.1.76 (192.168.1.76), Dst: 232.239.
Internet Group Management Protocol
0000 01 00 5e 6f 00 0a 60 2a d0 4a df be 08 00 46 a0 ..^o..`* .J....F.
0010 00 20 57 53 00 00 01 02 21 f7 c0 a8 01 4c e8 ef . WS.... !....L..
0020 00 0a 94 04 00 00 16 00 01 06 e8 ef 00 0a 00 00 ........ ........
0030 00 00 00 00 00 00 00 00 00 00 00 00 ........ ....
NVIDIA nForce MCP Networking Adapter Drive
Packets: 1210 Displayed:
Profile: Default

### La codificación en color

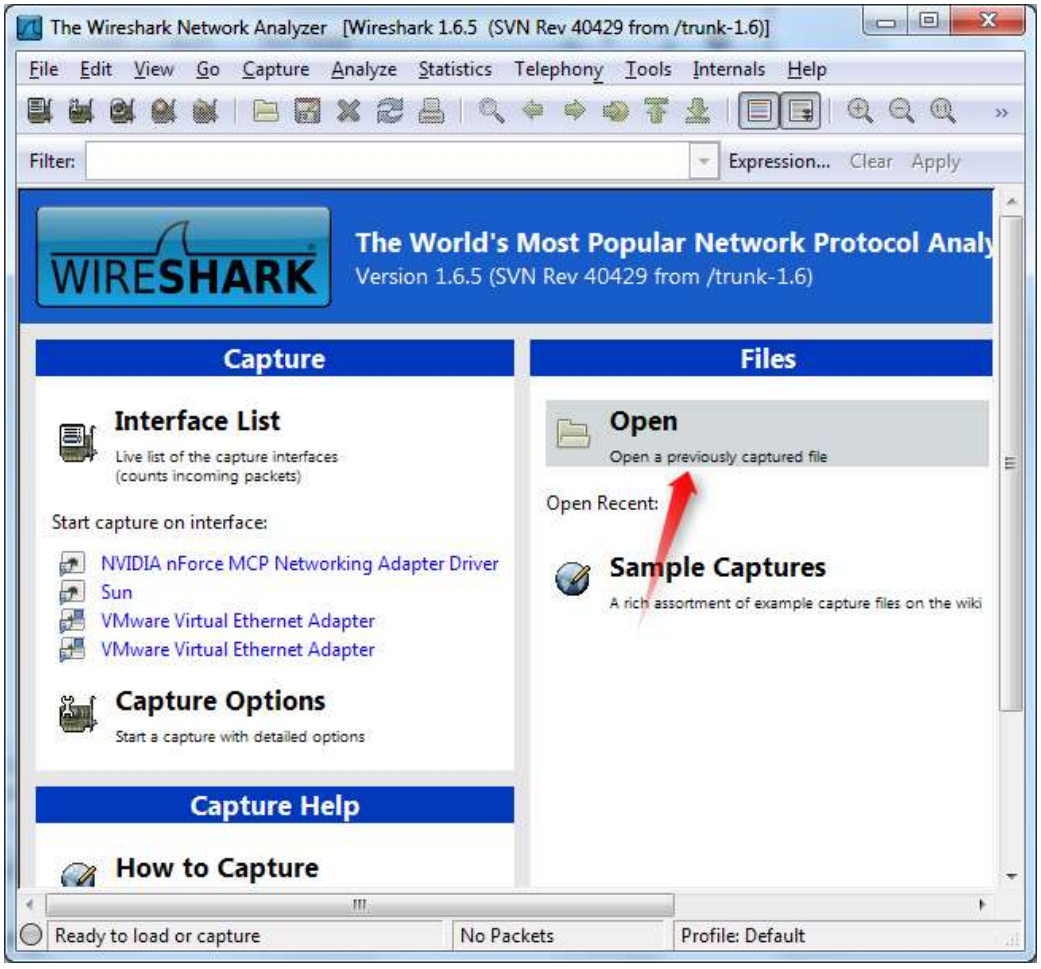
Es probable que vea los paquetes resaltados en verde, azul y negro. Wireshark utiliza colores para ayudarle a identificar los tipos de tráfico de un vistazo. Por defecto, el verde es el tráfico TCP, azul oscuro es el tráfico DNS, azul claro es el tráfico UDP y negro identifica los paquetes TCP con problemas - por ejemplo, podrían haber sido entregadas fuera de orden.




### Captura de ejemplo

Si no hay nada interesante en su propia red a inspeccionar, el wiki de Wireshark contiene una página de archivos de captura de muestra que se puede descargar e inspeccionar.

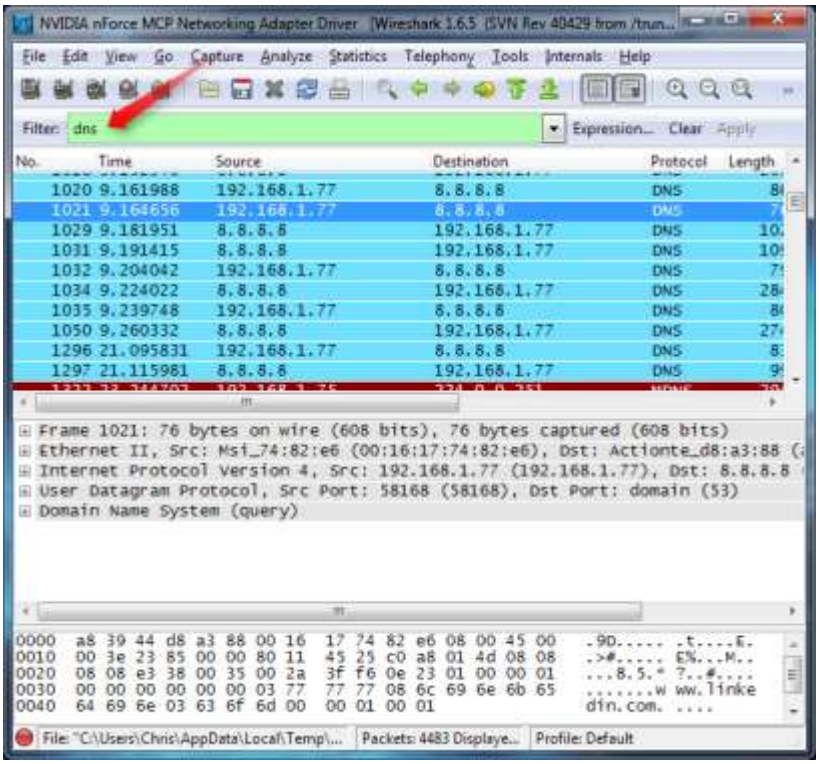
La apertura de un archivo de captura es fácil; simplemente haga clic en Abrir en la pantalla principal y busque el archivo. También puede guardar sus propias capturas de Wireshark y abrirlos más tarde.



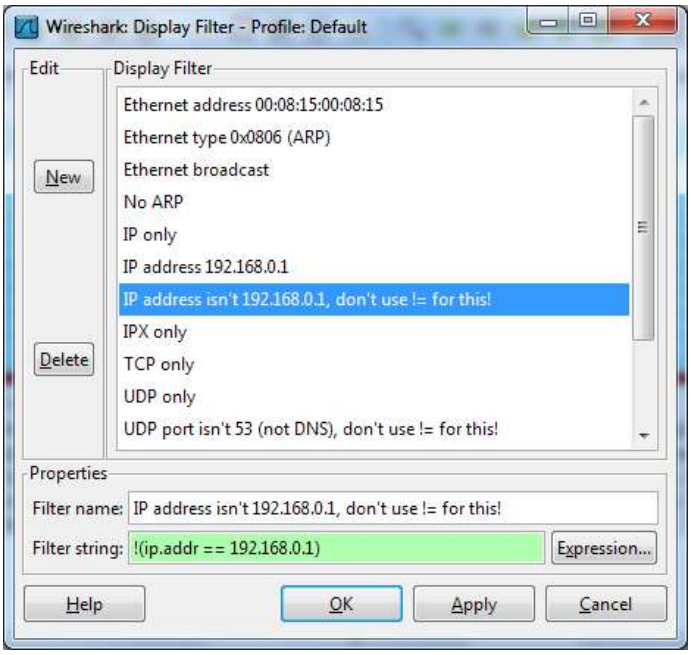

**Filtrado de paquetes**

Si está tratando de inspeccionar algo específico, es probable que tenga una gran cantidad de paquetes para filtrar. Ahí es donde los filtros de Wireshark sirven.

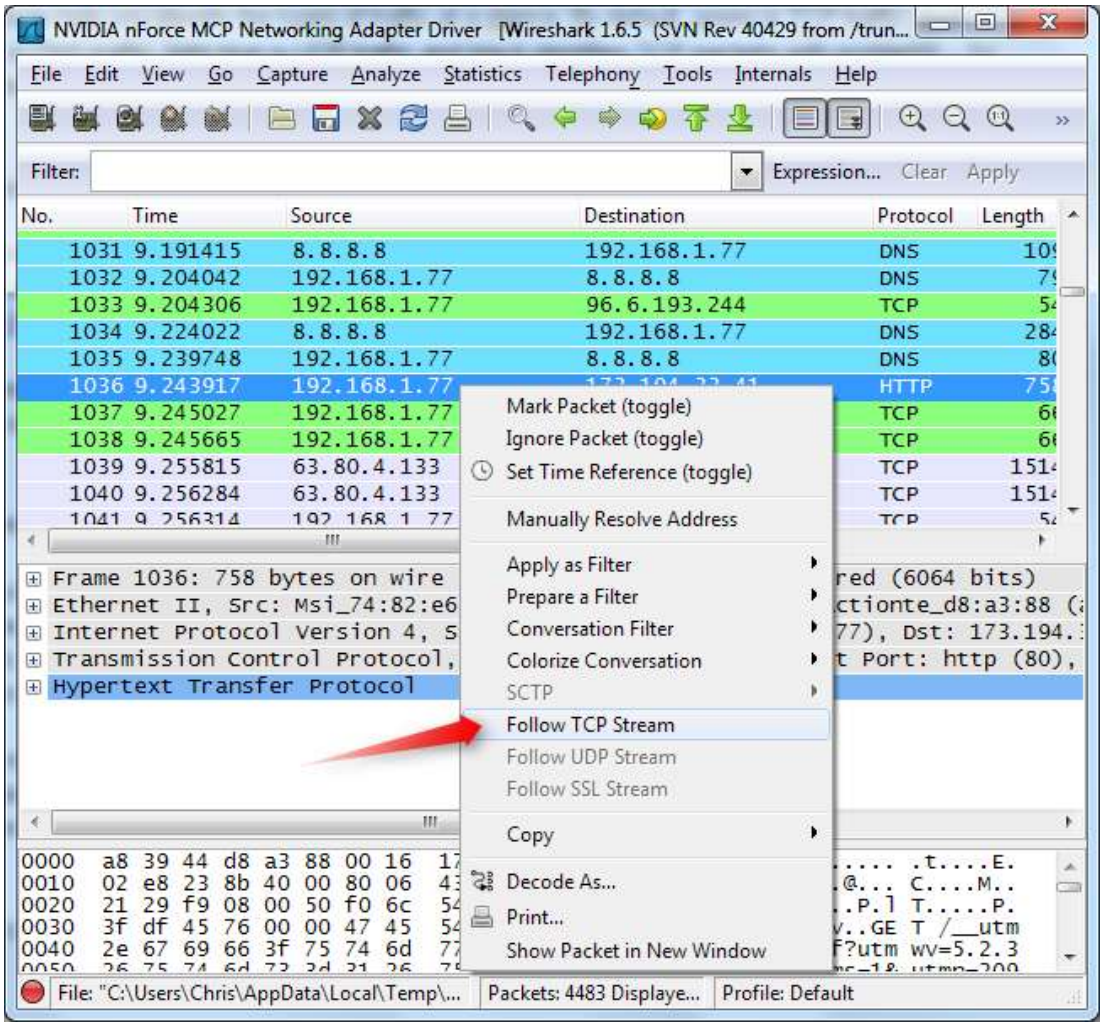
La forma más básica para aplicar un filtro es, escribiendo en la caja del filtro en la parte superior de la ventana y hacer clic en Aplicar (o pulsando Enter). Por ejemplo, escriba "dns" y verás paquetes DNS solamente. Cuando empiezas a escribir, Wireshark le ayudará Autocompletar su filtro.



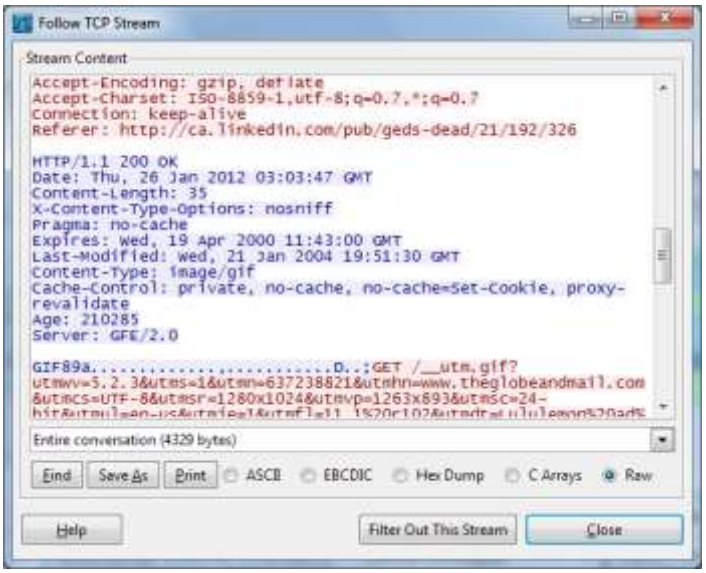

También puede hacer clic en el menú Analizar y seleccione Mostrar Filtros para crear un nuevo filtro.



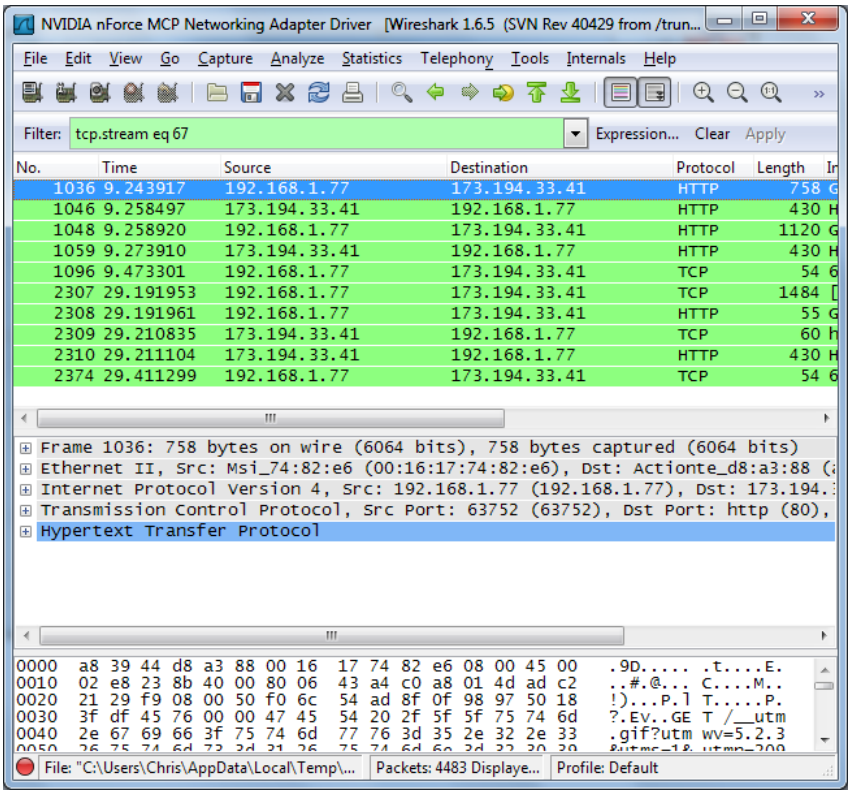

Otra cosa interesante que puede hacer es click derecho en un paquete y seleccione Follow TCP Stream.




Vas a ver la conversación completa entre el cliente y el servidor.

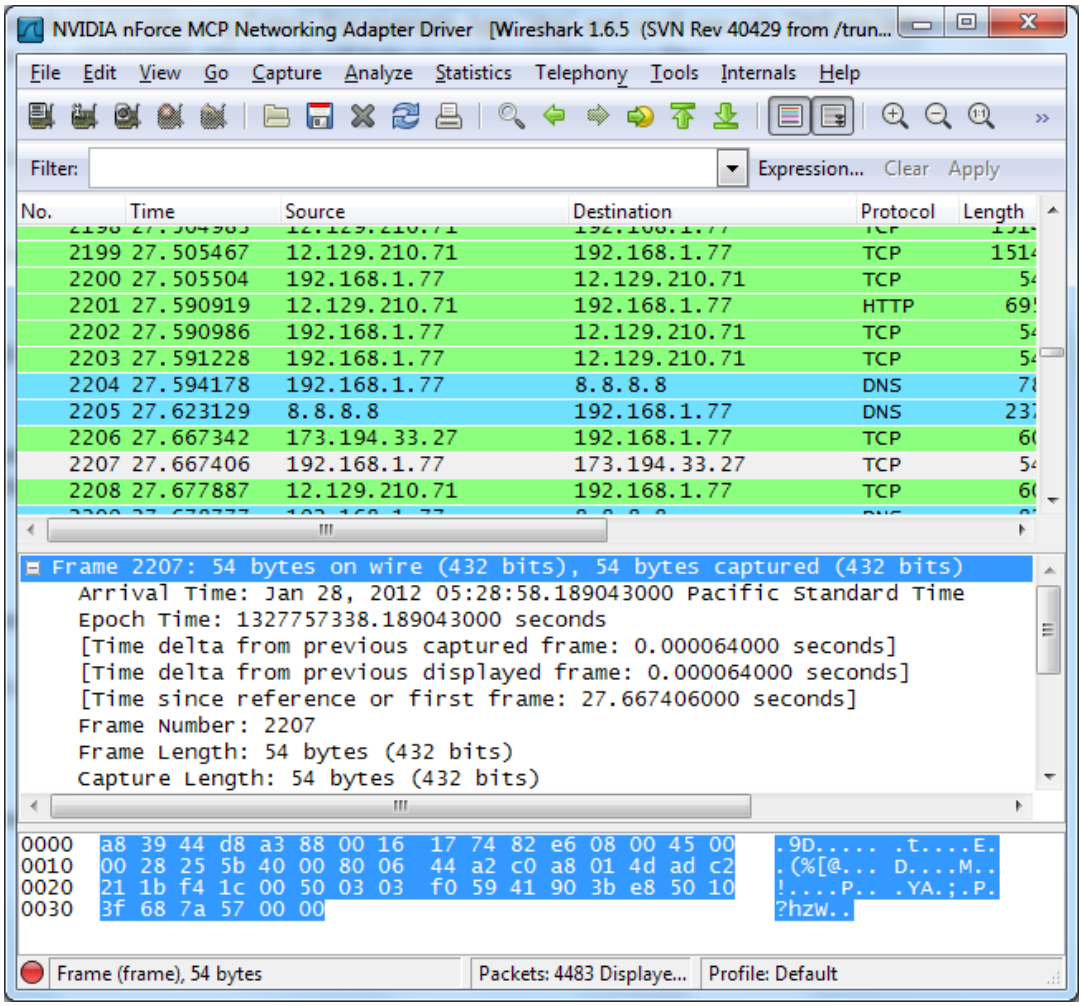



Cerramos la ventana y encontraremos que un filtro se ha aplicado de forma automática y que se muestran los paquetes que componen la conversación.

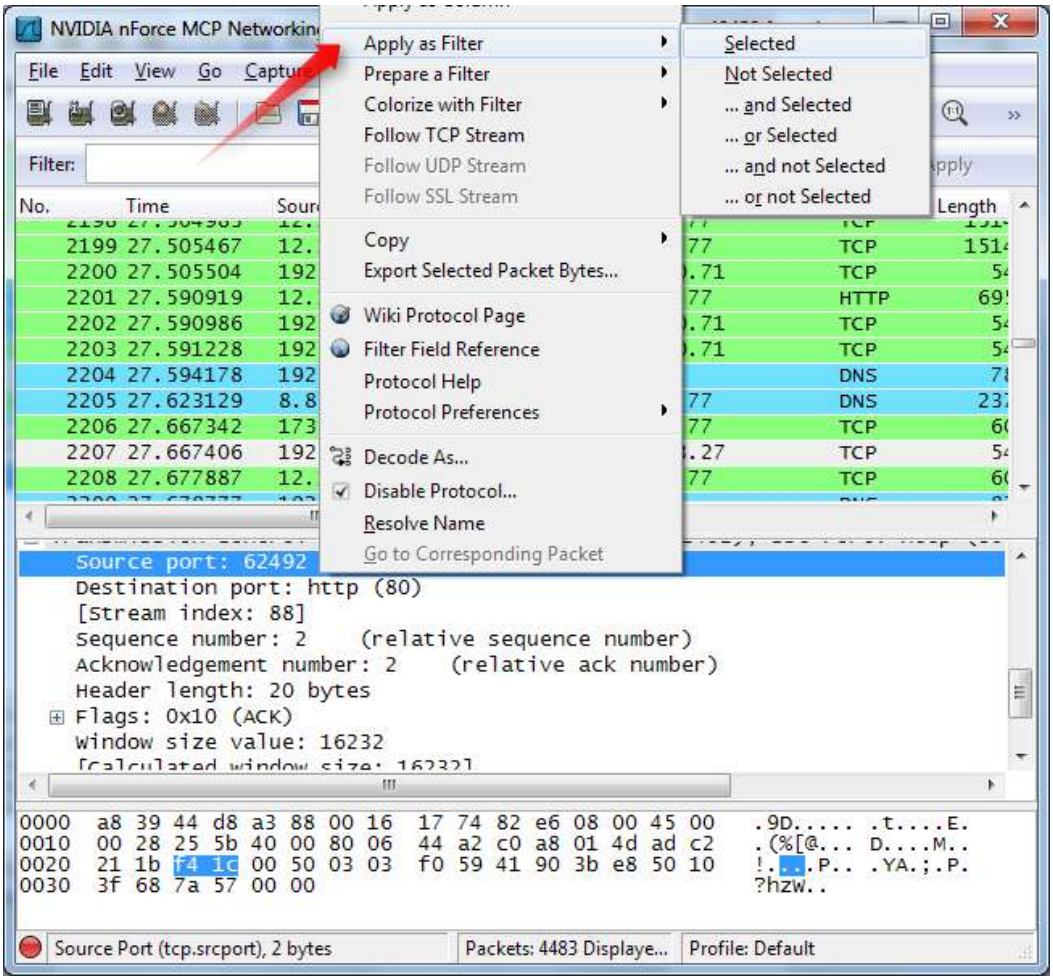



### Inspección de Paquetes

Hacemos click en un paquete para seleccionarlo y se puede visualizar hacia abajo para ver sus detalles.




También podemos crear filtros aquí - simplemente hacer click derecho en uno de los detalles y utilizar el submenú Aplicar como filtro para crear un filtro basado en él.




Wireshark es una herramienta muy potente. Los profesionales lo utilizan para depurar las implementaciones de protocolo de red, examinar los problemas de seguridad e inspeccionar partes internas del protocolo de red.