ELABORACIÓN DE UNA PROPUESTA DE IMPLEMENTACIÓN DE UN MODELO DE TRANSFERENCIA DE DATOS CON ADECUADOS NIVELES DE SERVICIO

JOSÉ MAURICIO JAIMES TAVERA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICO MECANICAS
ESCUELA DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2012

ELABORACIÓN DE UNA PROPUESTA DE IMPLEMENTACIÓN DE UN MODELO DE TRANSFERENCIA DE DATOS CON ADECUADOS NIVELES DE SERVICIO

JOSÈ MAURICIO JAIMES TAVERA

Monografía presentada como requisito para optar el titulo de Especialista en Telecomunicaciones

Director:
Ing. ANDRÉS AUGUSTO JACOME LOBO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICO MECANICAS
ESCUELA DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2012

Quiero dedicarle este nuevo triunfo en mi vida, inicialmente a Dios por darme la oportunidad de existir, por su gran amor asía mí al brindarme los medios necesarios para continuar mi formación. Pero sobre todo, por haberme heredado el tesoro más valioso que pudo darme como hijo "Mi madre. Que sin limitar esfuerzo alguno sacrificó gran parte de su vida para educarme. Por todo el amor y comprensión que desde niño me ha brindado, por ayudarme cada día a cruzar con firmeza el camino de la superación, por que con su apoyo y aliento hoy he logrado uno de mis más grandes anhelos. Por guiar mí camino y estar a mi lado en los momentos más difíciles.

A mi hermana y sobrinos por el apoyo incondicional, la alegría y la fortaleza necesaria para seguir adelante.

AGRADECIMIENTOS

El autor expresa sus agradecimientos a:

La empresa Sistemas y Computadores S.A. quienes me brindaron el tiempo para retomar mis estudios de Especialización y llevarlos a cabo exitosamente.
Director de tesis Andrés Augusto Jácome Lobo, por su valiosa asesoría, por todos los conocimientos que compartió conmigo y por dedicar parte de su valioso tiempo para que el proyecto hoy fuera un éxito.
Docentes de la Especialización, por sus aportes en la formación de profesionales especialistas orgullo de la institución.

.

CONTENIDO

LISTA DE FIGURAS

GLOSARIO

ASCII: American Standard Code for Information Interchange - Código Estándar Estadounidense para el Intercambio de Información, E un código de caracteres basado en el alfabeto latino.

CANAL DEDICADO: es una solución de acceso de alta velocidad a través de un canal confiable y seguro de uso propio.

CLIENTE / SERVIDOR: es un modelo de aplicación distribuida en el que las tareas se reparten entre los proveedores de recursos o servicios, llamados servidores, y los demandantes, llamados clientes.

CRIPTOGRAFÍA: es la ciencia de usar las matemáticas para encriptar y desencriptar datos.

FUNCIÓN HASH: es una función computable mediante un algoritmo donde las entradas son un conjunto de elementos que pueden ser cadenas, y las convierte en un rango de salida finito.

LAN: (L*ocal Area Network*) o una red de área local es la interconexión de computadores y periféricos. Su extensión está limitada físicamente a un edificio, con repetidores aplicado en la interconexión de estaciones de trabajo en oficinas, fábricas, etc.

MAN: *Metropolitan Area Network o u*na red de área metropolitana es una red de alta velocidad que da cobertura en un área geográfica extensa que proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado .

MD5. Message Digest algorithm 5 - Algoritmo de Resumen de Mensaje 5.

PROTOCOLO DE RED: es una regla o estándar que controla o permite la comunicación de computadores a través de una red. Estos protocolos pueden ser implementados por hardware, software, o una combinación de ambos.

PUERTO: es una interfaz para comunicarse con un programa a través de la red suele estar numerado para poder identificar la aplicación que lo usa. Esta asignación de puertos permite a una máquina establecer simultáneamente diversas conexiones con máquinas distintas, ya que todos los paquetes que se reciben tienen la misma dirección, pero van dirigidos a puertos diferentes.

SFTP. SSH File Transfer Protocol o *Secure File Transfer Protocol*) es un protocolo del nivel de aplicación que proporciona la funcionalidad necesaria para la transferencia y manipulación de archivos sobre un flujo de datos fiable. Se utiliza comúnmente con SSH para proporcionar la seguridad a los datos, aunque permite ser usado con otros protocolos de seguridad.

SSH. Secure SHell - Protocolo de Acceso Seguro a Máquinas Remotas.

SSL. Secure Socket Layer - Seguridad de la Capa de Transporte.

TCP: *Transmission Control Protocol* o *Protocolo de Control de Transmisión*. Se usa para la crear conexiones entre computadores para enviar datos. Este protocolo garantiza que los datos son entregados a su destino sin errores y en el orden que fueron enviados; a su vez proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma maquina gracias a los puertos.

TUNNELING: Consiste en encapsular un protocolo de red sobre otro protocolo de

red encapsulador creando un túnel dentro de una red de computadores. De esta manera se encaminan los paquetes de datos que van encriptados de forma que los datos son ilegibles para los extraños.

RESUMEN

TITULO: ELABORACIÓN DE UNA PROPUESTA DE IMPLEMENTACIÓN DE UN MODELO DE TRANSFERENCIA DE DATOS CON ADECUADOS NIVELES DE SERVICIO[*]

AUTOR: JOSÈ MAURICIO JAIMES TAVERA[**]

PALABRAS CLAVES: FTP, FTPS, VPN, Firewall, vulnerabilidades, calidad del servicio, transmisión de archivos.

En la actualidad, las organizaciones están orientadas a redes con infraestructuras grandes y complejas y surge la necesidad de compartir información confidencial, para ello, se hace indispensable tener un medio ágil, rápido y seguro para la transferencia de datos entre diferentes puntos de la organización ubicadas en otras ciudades, debido a que dichos datos generalmente son de gran tamaño, con información sensible para las organizaciones, la cual, puede ser empleada para realizar análisis estadísticos, diseñar estrategias de mercadeo, toma decisiones gerenciales, o realizar procesamiento de la información financiera. Por lo tanto, deben tratarse de manera segura garantizando la confidencialidad, integridad y disponibilidad de los mismos. Estos archivos que contienen grandes volúmenes de registros representan un espacio de almacenamiento mayor haciendo difícil su envío a los lugares solicitados, donde las herramientas disponibles actualmente como el correo electrónico no cuentan con la capacidad suficiente y los niveles de seguridad requeridos por las organizaciones.

Un protocolo empleado para esa tarea es el FTP el cual deberá estar acompañado de mecanismos de control de acceso y preferiblemente acompañado de medidas de cifrado (utilizar FTPS), lo cual mitigará los riesgos asociados a la seguridad de los datos. Otro factor que se debería optimizar son las conexiones a Bases de Datos, con el objetivo de que éstas no se vean interrumpidas a la hora de realizar el procesamiento de la información y así no entorpecer los procesos posteriores lo cual implicaría entre otras, inconsistencias en la información. Se observa que cada vez se hace más necesario utilizar un esquema donde la velocidad y las conexiones seguras son la clave del éxito.

[*] Monografía.

[**] Facultad de Ingeniería Físicomecánicas. Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones. Director. Andrés Augusto Jácome Lobo

ABSTRACT

TITLE: DEVELOPMENT OF A PROPOSAL OF IMPLEMENTATION OF A DATA TRANSFER MODEL WITH APPROPRIATE LEVEL OF SERVICE[*]

AUTHOR: JOSE MAURICIO JAIMES TAVERA[**]

KEYWORDS: FTP, FTPS, SFTP, VPN, Firewall, vulnerabilities, quality of service, file transfer.

Nowadays, organizations are network oriented with large and complex infrastructure and therefore arises a need to share confidential information, for it is indispensable to have an agile, fast and secure data transfer between different parts of the organization located in other cities, because these data are usually large, with sensitive information for organizations, which can be used for statistical analysis, design marketing strategies, making management decisions or execute processing of financial information. Therefore it must be treated safely ensuring the confidentiality, integrity and availability of data. These files containing large volumes of records represent a larger storage space making it difficult to send the requested locations, where currently available tools such as email does not have plenty capacity and the safety levels required by organizations.

A protocol used for this task is the FTP which must be accompanied by mechanisms of access control and preferably accompanied by measures of encryption (using FTPS), which would mitigate the risks associated to data security. Another factor that should be optimized are the connections to Data Bases, in order that they are not interrupted when performing the processing of information so as not to obstruct with subsequent processes which could involve among others, inconsistencies in the information. It is observed that is becoming more necessary to use a scheme where speed and secure connections are the key to success.

[*] Monography

[**] Faculty of Physic-Mechanical Engineering, School of Electrical, Electronic and Telecommunications Engineering. Director. Andrés Augusto Jácome Lobo

INTRODUCCIÓN

El continuo crecimiento de las redes informáticas a nivel mundial incluyendo el empresarial, donde se comparten recursos, que abarca desde notificaciones, documentos, normas, manuales hasta complejas transacciones privadas, estando expuesto a que la información sea alterada por atacantes externos o internos, buscando obtener beneficios propios, y que las medidas adoptadas no sean suficientes para garantizar la integridad, confiabilidad y confidencialidad del recurso compartido, causando contratiempos en la presentación de la información e incurriendo en sobrecostos.

El FTP es un protocolo de red estándar que se utiliza para transferir archivos desde un host a otro host a través de una red basada en TCP, como el Internet. FTP se basa en una arquitectura cliente-servidor y utiliza el control por separado y conexiones de datos entre el cliente y el servidor.

Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor, o apropiarse de los archivos transferidos.

Para solucionar este problema son de gran utilidad el paquete SSH, SSH File Transfer Protocol (también conocido como SFTP o Secure File Transfer Protocol) es un protocolo del nivel de aplicación que proporciona la funcionalidad necesaria para la transferencia y manipulación de archivos sobre un flujo de datos fiable. Se utiliza comúnmente con SSH para proporcionar la seguridad a los datos, aunque permite ser usado con otros protocolos de seguridad que permiten transferir

archivos pero cifrando todo el tráfico. Por lo tanto, se hace indispensable elaborar una propuesta que cumpla los requisitos de seguridad.

Este modelo fue elaborado con la intención de facilitar a las organizaciones que deseen una guía básica del modelo de transmisión de datos seguro a seguir cumpliendo con las expectativas de seguridad.

Este trabajo permite aplicar los conocimientos adquiridos en el proceso de aprendizaje durante la Especialización de Telecomunicaciones de la Universidad Industrial de Santander.

1. MARCO TEÓRICO

1.1 MÉTODOS DE TRANSMISIÓN DE ARCHIVOS

Existen muchas formas de que un usuario copie datos de un computador a otro. A continuación se menciona algunos de estos métodos.

Lo primero es tener ubicado los archivos que deseo copiar, deberá decidir el mejor método para transferirlos a otro computador y que cumpla con las necesidades de seguridad.

- Disquetes. Si sólo tiene unos pocos archivos para copiar, el copiarlos a un disquete y transferirlos a otra computadora es definitivamente una de las soluciones más fáciles. Sin embargo, si necesita copiar grandes cantidades de datos de una computadora a otra, deberá intentar una solución alternativa.

- CDs y DVDs. Graban información en CD y DVDs, si el computador desde la que desea copiar archivos posee una unidad que graba CDs/DVDs, puede copiar los mismos en un CD/DVD grabable (o regrabable) para moverlos a otra PC. Este método permite almacenar unos 650 MB para el caso de un CD, y más de 4,7 GB en el caso de los DVDs.

- USB. Con la creciente popularidad de los puertos y dispositivos USB, los usuarios pueden transferir archivos de un computador a otro si poseen unidades USB externas como discos duros USB, pueden fácilmente copiar información al disco duro USB y luego conectar esa unidad al otro computador para transferir los datos. Esta solución permite al usuario hacer rápidos backups o copias de seguridad de los archivos, así como también tener la posibilidad de transferir rápidamente y de manera fácil información.

- Recursos compartidos a través de una red de computadores: En una red Trabajo en Grupo podemos compartir, o hacemos disponibles a través de la red, cualquier directorio o impresora que deseemos de forma que puedan ser accedidos por otros usuarios. En redes con configuraciones de cliente/servidor, utilizaremos cuentas para establecer quién puede acceder a qué archivos, directorios e impresoras.

1.2 PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Estos métodos permiten compartir archivos desde el más sencillo e inseguro hasta el más robusto y complejo, el inconveniente es que no todos los métodos pueden garantizar que la información no sea alterada, accedida, divulgada o eliminada sin autorización. Existen tres requisitos principales de seguridad en tecnologías de acceso remoto:

- CONFIDENCIALIDAD. Consiste en proteger la información contra la lectura de terceros no autorizada y se logra por medio de la encripción.

- INTEGRIDAD. Es de suma importancia proteger la información contra la modificación o eliminación sin el debido permiso del dueño o responsable. Incluyendo respaldos de información, documentación, registros contables del sistema, tráfico en la red, también comprende tipo de modificaciones causadas por error de hardware y/o software, causadas de forma intencional o accidental.

- AUTENTICACION. Es el principio que permite garantizar que el usuario sea realmente quien dice ser. Para ello, se deben implementar un mecanismo para verificar quien esta enviando la información.

A continuación se mencionan otros conceptos de apoyo recomendados para una transferencia de archivos segura.

- NO REPUDIO. Cuando ni origen ni el destino en un mensaje deberían poder negar la transmisión. Es decir, quien envía el mensaje puede probara que en efecto el mensaje fue enviada y el destino que lo recibió.

- DISPONIBILIDAD. (recursos y de la información). No tiene sentido si la información se encuentra intacta pero los usuarios no pueden acceder a ella. por lo tanto, se deben proteger los servicios de cómputo y la información para que estén disponibles a los usuarios autorizados.

- CONTROL DE ACCESO. Consiste en el control de quien y como utiliza los recursos que ofrece el sistema mediante políticas, incluyendo pre-admisión, chequeo de políticas de seguridad en el usuario final y controles post-admisión a los que pueden acceder.

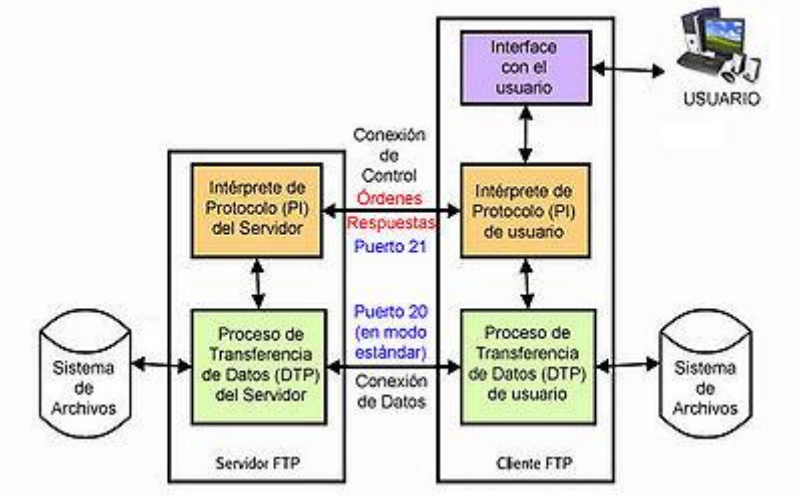
- AUDITABILIDAD. Consiste en tener los mecanismos necesario para poder monitorear el sistema, quien lo hace y cuando lo hace.

Todos estos principios y servicios de seguridad se deben tener en cuenta en el momento de elaborar una propuesta que permite la transferencia de archivos segura.

1.3 FTP

File Transfer Protocol o Protocolo de Transferencia de Archivos es un protocolo de red para la transferencia de archivos entre sistemas interconectados, basado en la arquitectura cliente servidor. Donde un equipo cliente se puede conectar a un servidor FTP para descargar o enviarle archivos, sin importar el sistema operativo de cada equipo. *Referencia el RFC 959.*

Figura 1. Modelo FTP



El servicio FTP se utiliza normalmente en los puertos de red 20 y 21. Un problema que se presenta con el uso del FTP es que se diseño para ofrecer máxima velocidad de conexión, sin tener en cuenta la seguridad debido a que todo intercambio de información incluyendo el login y password del usuario se realiza en texto plano sin ningún tipo de cifrado, donde un atacante que logre capturar el trafico en la red podrá acceder a la información transferida.

1.3.1 Cliente FTP. Es un programa que se instala en el equipo del usuario y que utiliza el protocolo FTP para conectarse a un servidor FTP con el fin de transferir o descargar archivos.

Para su uso, se requiere conocer el nombre del archivo, el origen y el destino donde se desea transferir o descargar el archivo.

1.3.2 Servidor FTP. Es un programa que se ejecuta en un servidor que generalmente se encuentra conectado a internet inclusive a tipos de redes LAN, MAN entre otras. El cual permite el intercambio de datos.

El uso más común de los Servidores FTP es para alojamiento de páginas Web, copias de seguridad. Para ello, existen protocolos para que los datos se transmitan cifrados como el SFTP**.**

1.3.3 Modos de Conexión al servidor FTP. El protocolo FTP permite dos modos de conexión por parte del cliente que son:

- Modo Activo: También conocido como Estándar o PORT, por enviar comandos tipo PORT al servidor por el canal de control al establecer la conexión. En este modo el servidor FTP crea el canal de datos en su puerto 20, en cambio al lado del cliente el canal de datos se asocia a un puerto aleatorio mayor al 1024. Para ello, el cliente envía un comando PORT al servidor por el canal de control notificando el puerto. Para que el servidor a su vez abra la conexión de datos por el puerto dado para la transferencia de archivos.

- Modo Pasivo. Cuando el cliente envía un comando PASV sobre el canal de control, el servidor FTP le indica por el canal de control el puerto al que debe conectarse el cliente y debe ser mayor a 1023. Entonces el cliente inicia la conexión desde el puerto siguiente al puerto de control hacia el puerto del servidor FTP dado.

Es importante tener claro que antes de cada nueva transferencia tanto en el modo Activo o Pasivo, el cliente debe enviar otra vez un comando de control (PORT o PASV, de acuerdo al modo de conexión), y el servidor recibirá esa conexión de datos en un nuevo puerto aleatorio en modo pasivo o por el puerto 20 en modo activo.

1.3.4 Tipos de Transferencia de Archivos FTP. Existen dos tipos para transferir archivos a lo largo de la red:

- Tipo ASCII. Ideal para archivos que contenga caracteres imprimibles como paginas HTML, pero no las imágenes que contengan.
- Tipo BINARIO. Ideal cuando se trata de archivos comprimidos, ejecutable, imágenes, música.

El uso inadecuado del tipo de transferencia podría ocasionar perdida del archivo.

1.4 PROTOCOLO SSH

SSH (Secure Shell) es un estándar de facto por ser ampliamente empleado que permite al usuario registrarse en un sistema remoto sobre una red. Igualmente asegura las conexiones sobre Internet encriptando toda la información confidencial, incluso las contraseñas, archivos binarios y comandos de configuración. *Referencia RFC 2196.*

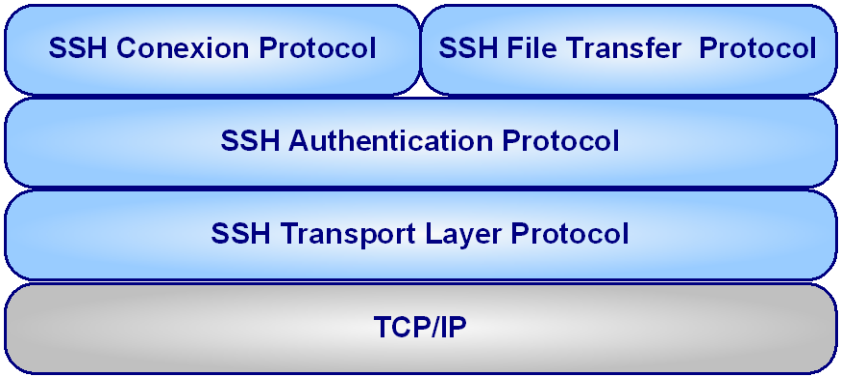
El protocolo SSH se desarrollo con el fin de dar solución a los dos problemas más agudos en Internet: logins seguros en terminales remotos y transferencia segura de archivos. Adicionalmente SSH puede hacer túneles para sesiones arbitrarias de TCP sobre una simple y segura conexión SSH; esta característica hace que sea posible asegurar las comunicaciones de otras aplicaciones sin necesidad de modificarlas, de esta forma los usuarios pueden continuar utilizando aplicaciones como el correo electrónico y las sesiones X11 en una forma segura.

SSH está siendo estandarizado por el SecSh Working Group del IETF (Internet Engineering Task Force). SSH es un estándar abierto y bien documentado, y las implementaciones de diferentes vendedores se han sido probadas extensivamente para garantizar su interoperabilidad.

El protocolo SSH consta de tres componentes plenamente identificables:

- El protocolo de la capa de transporte
- El protocolo de autentificación
- El protocolo de conexión.

Figura 2: Componentes del Protocolo SSH



1.4.1 Protocolo de la Capa de Transporte. La capa de transporte de SSH es un protocolo de transporte seguro a bajo nivel. Su misión es de proporcionar un canal confidencial sobre una red insegura basándose en una encripción fuerte, realiza autenticación criptográfica del servidor, realiza el intercambio de claves y proporciona protección de integridad. Además genera un identificador único de sesión que será usado por los protocolos de nivel superior.

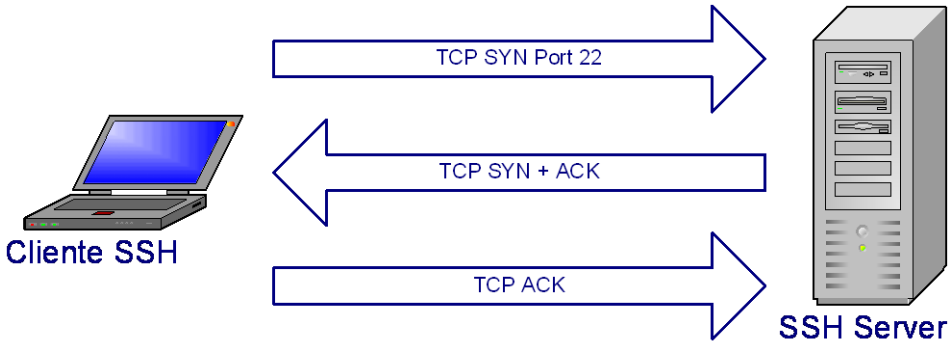
Este protocolo ha sido diseñado para ser simple y flexible, para permitir la negociación de parámetros y para minimizar el número de viajes de ida y vuelta entre el cliente y el servidor. Aquí se negocian los métodos para intercambio de claves, los algoritmos de clave pública y las funciones Hash que se usaran para garantizar la integridad de la información. En la mayoría de los casos sólo 2 viajes ida y vuelta son necesarios para hacer el intercambio de claves, la autenticación del servidor, el requerimiento del servicio y la notificación de la aceptación del servicio. En el peor de los casos serán necesarias 3 viajes ida y vuelta.

Algunas personas pueden preocuparse por el incremento en el tamaño de los paquetes debido a las nuevas cabeceras, la carga, y el MAC (Message Authentication Code). El tamaño mínimo de un paquete es del orden de 28 bytes (dependiendo de los algoritmos negociados). Este incremento se hace despreciable cuando se trata de paquetes grandes, en cambio en paquetes de 1-byte (Sesiones tipo telnet) el incremento es realmente significativo. Sin embargo, si se tienen en cuenta las cabeceras TCP/IP, y las cabeceras de Ethernet el incremento real es menor al 10%.

Adicionalmente, el protocolo de la capa de transporte de SSH permite comprimir los datos antes de realizar la encripción, siempre y cuando esta se haya negociado en el inicio de la sesión.

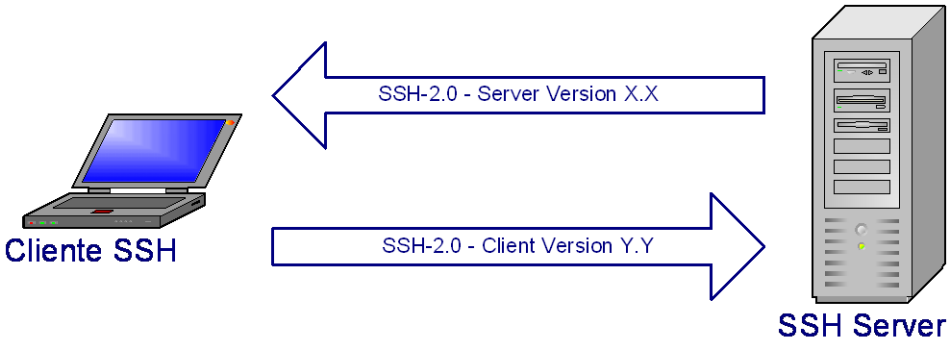
- **Descripción de la conexión.** El cliente inicia el proceso solicitando una conexión TCP/IP por el puerto 22, el cual ha sido oficialmente asignado por la IANA para uso del protocolo SSH. El servidor acepta la solicitud y establece la conexión.

Figura 3. Solicitud de conexión TCP/IP



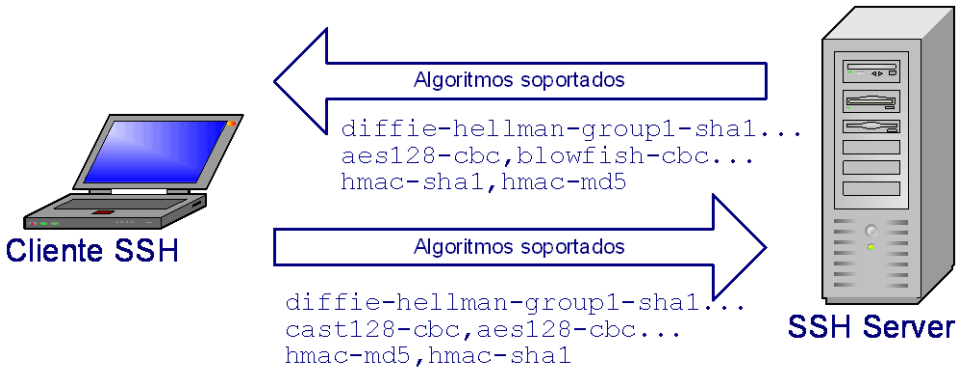
Una vez establecida la conexión TCP/IP, tanto el servidor como el cliente se envían la versión del protocolo que están utilizando y la versión del software.

Figura 4. Versión del Protocolo y software



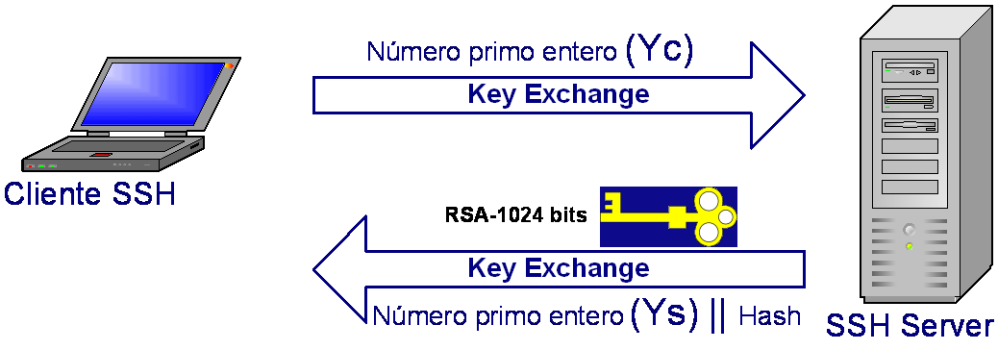
Conocidas las versiones de los protocolos y del software, el servidor inicia la negociación de los algoritmos con el cliente. En este momento tanto el cliente como el servidor se comunican mutuamente informándose de los algoritmos soportados y específicamente del sus algoritmos preferidos en cada una de las categorías.

Figura 5. Negociación de algoritmos soportados



Ya establecidos los algoritmos con los cuales se llevará a cabo la comunicación el servidor procede a autenticarse criptográficamente con el cliente. Para ello, utilizan el protocolo acordado anteriormente (Diffie Hellman) y comparten dos elementos globales: un número primo seguro q y a un generador del subconjunto Zq, tal que a<q.

Figura 6. Proceso de autenticación con el cliente.



El cliente selecciona un Xc<q y calcula Yc = aXc mod q, y envía este valor al servidor. El servidor hace lo mismo y selecciona un Xs<q y calcula Ys=aXs mod q. Adicionalmente, el servidor calcula la clave secreta K = YcXs mod q, y el identificador de sesión, el cual es equivalente al Hash de los siguientes elementos concatenados: versiones del cliente y el servidor, la clave publica o certificados del servidor, Yc, Ys y K. El servidor envía al cliente Ys, su clave pública y el identificador de sesión (Hash).

El cliente por toma el valor Ys y calcula la clave secreta K = YsXc mod q, y calcula el identificador de sesión (Hash) de la misma forma que lo hizo el servidor. Si el identificador de sesión es igual al calculado por el servidor, esté será autenticado por el cliente. Este identificador de sesión se usará como la clave secreta para cualquiera que sea el algoritmo de encripción que se negocio anteriormente. A partir de este momento la conexión estará cifrada y el servidor quedará a la espera de una solicitud de servicio.

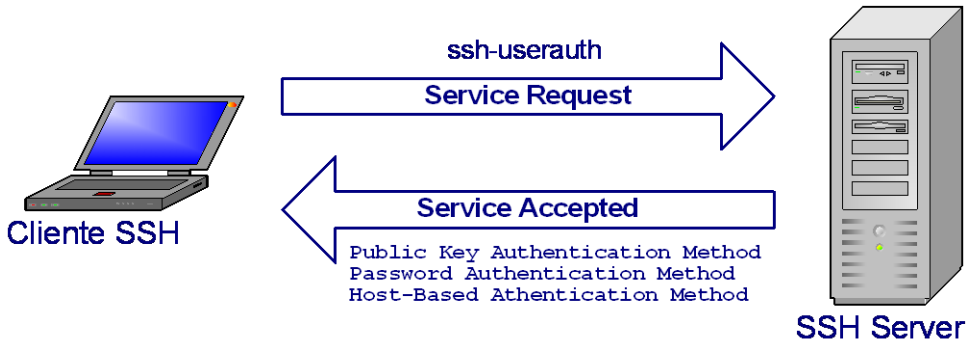
1.4.2 Protocolo de Autenticación. El protocolo de autenticación ofrece mecanismos que pueden usarse para autenticar al usuario cliente en el servidor. Los mecanismos individuales especificados en protocolo de autenticación usan el identificador de sesión proporcionado por el protocolo de transporte y depende de

la seguridad y la integridad garantizada por la capa de transporte de SSH.

El protocolo de autenticación posee un timeout, después del cual la conexión debe desconectarse si no ha sido posible autenticar el host cliente. Además se cuenta con un contador el cual lleva el número de intentos errados de autenticación; cuando este número excede el límite el servidor debe desconectarse.

- Descripción del proceso de autenticación. El cliente inicia el proceso haciendo la petición del servicio al servidor. Si el servidor rechaza la petición, enviará un mensaje de desconexión, de lo contrario, enviará un mensaje de servicio aceptado. Una vez iniciado el servicio, este tendrá acceso al identificador de sesión generado por la capa de transporte. Iniciado el servicio, el servidor controla la autentificación del cliente, diciéndole a este que métodos pueden ser usados para continuar el intercambio en cualquier momento. El cliente tiene la libertad de intentar con cualquiera de los métodos sin importar el orden en que el servidor se los haya presentado.

Figura 7. Proceso de Autenticación



- Principales métodos de autenticación soportados. Según el protocolo SSH, el único método que es indispensable es la autenticación por medio de claves públicas (Public Key). Métodos adicionales como lo son la autentificación basada en el host, o autenticación por password son opcionales y dependen de la

distribución.

- Public Key: La tenencia de una clave pública sirve como autentificación. El método trabaja enviando una firma creada con la clave pública del usuario. El servidor por su parte se encarga de validar tanto la clave como la firma, si ambas son validas la solicitud del cliente será aceptada. Las claves públicas son almacenadas de forma cifrada en el host cliente, y deben usar una clave antes de que la firma sea generada, de lo contrario la operación de firmado requerirá de procesamiento adicional.

- Password: En el caso en que la autentificación del usuario utilice el método de password, el servidor debe confrontar el password con las entradas existentes en una base de datos. Aún cuando los passwords se ingresen en texto claro, el paquete entero es cifrado por la capa de transporte. Si el usuario requiere cambiar su password debido a que este ha expirado el servidor no permitirá la autenticación del usuario. Además, si el password no cumple con los requerimientos de las políticas de seguridad establecidas en el servidor, este podrá solicitar al usuario que cambie su clave. Desde el punto de vista de la internacionalización, el proceso de autenticación por password funciona independientemente del software y el sistema operativo del cliente.

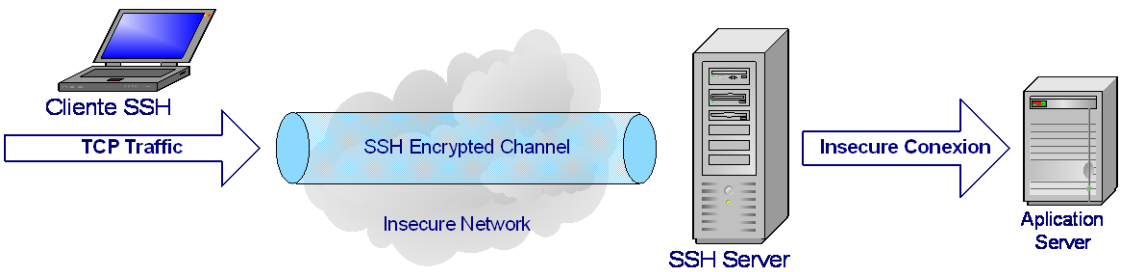
- Host-Based: En algunos casos se pude realizar el proceso de autentificación basándose en el host desde el cual el usuario está comunicándose, y con el nombre de la máquina (hostname). Sin embargo, este tipo de autenticación no proporciona mayor seguridad. Cuando se usa este método el cliente envía al servidor una firma creada con la clave privada del cliente, la cual será comprobada por el servidor con la clave pública del cliente. Una vez se ha establecido la identidad del host cliente el servidor realiza la autenticación basada en los nombres de usuario en el servidor y en el cliente, tal como lo haría en UNIX *rhost* o *hosts.equiv.*

1.4.3 Protocolo de Conexión. El protocolo de conexión describe un mecanismo para multiplexar diferentes streams de datos sobre un canal de transporte confidencial y autenticado. Igualmente, especifica canales para acceder un shell interactivo, crea túneles para varios protocolos externos a través del canal seguro (Incluso para conexiones TCP/IP arbitrarias), y permite acceder subsistemas seguros en el servidor.

- Tunneling: Tal vez la característica más interesante es la capacidad de crear túneles a través de un canal cifrado para conexiones TCP/IP. De esta forma es posible realizar conexiones seguras a servidores de aplicaciones sin poner en riesgo la información transmitida a través de una red insegura. Aplicaciones como los protocolos FTP, SMTP, POP3, IMAP, DNS, y otros pueden ser accedidos remotamente gracias a que el protocolo SSH permite realizar un reenvío de puertos.

Para el reenvío de puertos, el cliente solicita al servidor SSH una conexión segura mediante el protocolo de la capa de transporte de SSH, autentica el usuario ante el servidor y solicita el servicio de TCP port forwarding. Una vez establecido el canal seguro, el cliente le indica al servidor SSH la dirección IP del servidor de aplicaciones y el puerto hacia el cual quiere ser redireccionado. El servidor SSH establece la conexión con el servidor de aplicaciones y actúa de forma transparente con el cliente.

Figura 8. Conexión del Servidor SSH con el Servidor de aplicaciones



- Secure File Transfer Protocol (SFTP): Este protocolo proporciona transferencia de archivos segura. El SFTP asume que las capas inferiores cumplen con su tarea de proporcionar un canal seguro, que el servidor ha autenticado satisfactoriamente el cliente y que la identidad del cliente está disponible para el protocolo.

En general, este protocolo sigue un modelo simple de solicitud-respuesta. Cada solicitud y cada respuesta contienen un número de secuencia y múltiples solicitudes pueden estar en cola de espera simultáneamente. Relativamente existe una gran cantidad de mensajes de solicitud diferentes, y sólo un pequeño número de respuestas posibles. Cada solicitud puede tener uno o más mensajes de respuesta.

- Secure Copy (SCP): Es un medio de transferencia segura de archivos informáticos entre un host local y otro remoto o entre dos hosts remotos, usando el protocolo Secure Shell (SSH).

El protocolo SCP es básicamente idéntico al protocolo rcp de BSD. A diferencia de rcp, los datos son cifrados durante su transferencia, para evitar que potenciales packet sniffers extraigan información útil de los paquetes de datos. Sin embargo, el protocolo mismo no provee autenticación y seguridad; sino que espera que el protocolo subyacente, SSH, lo asegure.

El modo SCP o Simple Communication Protocol, es un protocolo simple que deja al servidor y al cliente tener múltiples conversaciones sobre una TCP normal. Este protocolo esta diseñado para ser simple de implementar.

El servicio principal de este protocolo es el control del dialogo entre el servidor y el cliente, administrando sus conversaciones y agilizadas en un alto porcentaje, este protocolo le permite a cualquiera de los dos establecer una sesión virtual sobre la normal.

1.5 FTPS

También conocido como FTP Secure o FTP-SSL es una extensión del FTP que agrega soporte para los protocolos criptográficos TLS y SSL. *Referencia RFC 2246.*

Con este método la transferencia de archivos se cifra, agregando seguridad a la misma. El cifrado puede ser a nivel de datos, a nivel de comandos o ambos.

Si el canal de comandos no se cifra, se dice que el protocolo está usando un canal de comandos en claro (CCC). Si el canal de datos no está cifrado, se dice que el protocolo usa un canal de datos en claro (CDC).

1.5.1 Protocolo TLS. (Transport Layer Security - Seguridad de la Capa de Transporte) es el sucesor del SSL (Secure Sockets Layer – Capa de conexión Segura). Estos protocolos permiten proporcionar comunicaciones seguras en Internet, usando un modelo de autenticación y privacidad de la información entre dos puntos de la red sobre Internet mediante el uso de la criptografía.

El protocolo SSL fue diseñado de manera modular extensible, con soporte para compatibilidad hacia delante y hacia atrás y negociación entre las partes (peer-to-peer).

Normalmente el servidor es el único que es autenticado, garantizando así su identidad, pero el cliente se mantiene sin autenticar, para que la autenticación sea mutua se requiere una infraestructura de claves públicas (o PKI) para los clientes.

Estos protocolos permiten prevenir ataques de escuchas (eavesdropping), evitar la falsificación de la identidad del remitente y mantener la integridad del mensaje en una aplicación cliente-servidor.

El protocolo SSL/TSL se basa en tres fases básicas:

- Fase de Negociación de Algoritmos: Entre el cliente y el servidor negocian que algoritmos criptográficos se emplearan para autenticarse y cifrar la información.

- Fase de intercambio de Claves: El cliente y el Servidor se autentican mediante el uso de certificados digitales e intercambian las claves para el cifrado, según la negociación anterior.

- Fase de Establecimiento del Túnel de Encripción: El cliente y el servidor inician el tráfico de información cifrada y establece el túnel seguro.

El protocolo SSL/TLS para la comunicación entre el cliente y el servidor se basa en el intercambio de mensajes. En cada uno de los mensajes existe un campo (content_type) en el cual se especifica el protocolo de nivel superior que se esta usando. Estos mensajes puede ser comprimidos, cifrados y empaquetados con un código de autentificación del mensaje llamado (MAC).

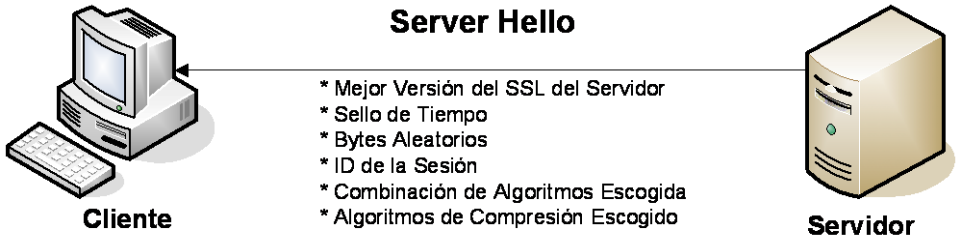
Al momento de iniciar la conexión, el nivel de registro encapsula otro protocolo, el protocolo handshake, que tiene el content_type 22 donde se envía diferentes mensajes.

- Descripción de la conexión. El cliente inicia la comunicación enviando un mensaje "Client Hello" dónde especifica una lista de conjunto de cifrados, métodos de compresión y la versión del protocolo SSL más alta permitida. Además envía una serie de bytes aleatorios (Challenge de Cliente o Reto) para uso posterior y puede enviar el identificador de la sesión.

Figura 9. Mensaje Client Hello

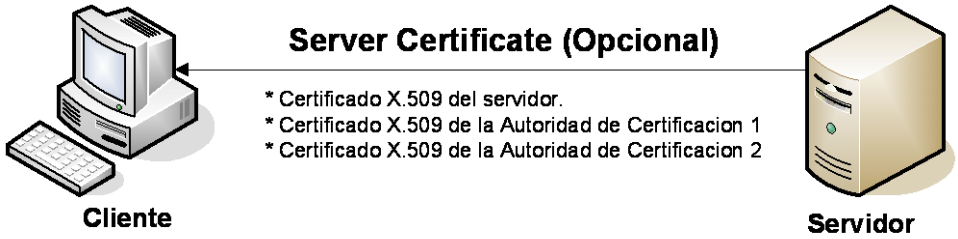
El servidor recibe la solicitud y responde con un mensaje “Server Hello”, indicando los parámetros elegidos por el servidor de acuerdo a las opciones ofrecidas por el cliente.

Figura 10. Mensaje Server Hello



Cuando los parámetros de conexión ya están seleccionados, el cliente y servidor intercambian certificados (de acuerdo a las claves públicas de cifrado seleccionadas). Estos certificados son actualmente X.509, pero hay también un borrador especificando el uso de certificados basados en OpenPGP.

Figura 11. Mensaje Server Certificate



Si la conexión tiene que ser mutuamente certificada el servidor pide un certificado al cliente y éste se la enviaría.

El cliente verifica la autenticidad del servidor.

Figura 12. Mensaje Client Certificate

Cliente y servidor negocian una clave secreta común (master secret), que puede derivarse de un intercambio Diffie-Hellman, o utilizando la clave privada de cada uno para cifrar una clave pública que servirá para cifrar a la vez la clave secreta. El resto de claves son derivadas a partir de este master secret y los valores aleatorios generados en el cliente y el servidor, que son pasados a través una función pseudo-aleatoria.

Figura 13. Mensaje Server Key.

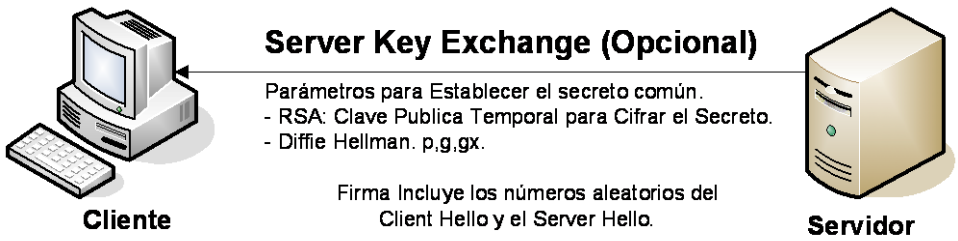


Figura 14. Mensaje Client key Exchange

Cliente y servidor aplican los parámetros negociados.

El uso más común es:

- AUTH TLS o FTPS Explicito, Método preferido de acuerdo al RFC que define FTP sobre TLS. El cliente se conecta al puerto 21 del servidor y comienza una sesión FTP sin cifrar de manera tradicional, pero pide que la seguridad TLS sea usada y realiza la negociación apropiada antes de enviar cualquier dato sensible.

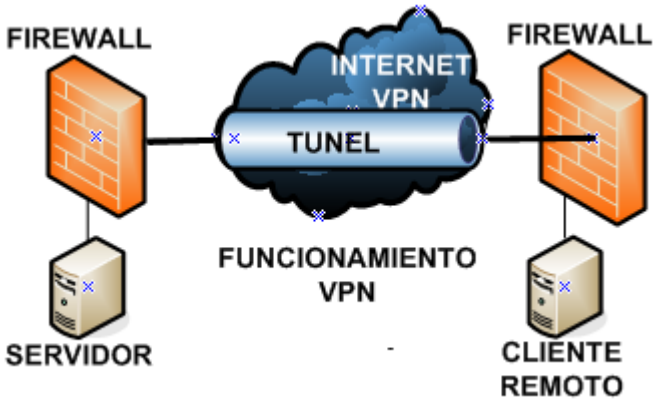
- AUTH como está definido en RFC 2228.

- FTPS Implícito Método antiguo, pero todavía ampliamente implementado en el cual el cliente se conecta a un puerto distinto (como por ejemplo 990), y se realiza una negociación SSL antes de que se envíe cualquier comando FTP.

1.6 VPN

Las siglas en Ingles de Virtual Private Network o “Red Privada Virtual” es una tecnología que permite la extensión de la red local sobre una red pública o no controlada como es el Internet. Ver Figura 15.

Figura 15. Conexión VPN



Su uso se basa en la posibilidad de conectar de forma remota dos o más puntos de cómputo de manera segura utilizando para su conexión el Internet.

1.6.1 Características VPN. Los requerimientos básicos que debe tener una VPN al momento de implementar son:

- Identidad de los Usuarios. Consiste en verificar y restringir el acceso a la VPN a usuarios que no estén autorizados y proporcionar registros estadísticos de los usuarios que accedieron, cuando y a que información.

- Administración de direcciones. Consiste en establecer una dirección del cliente en la red privada y debe asegurarse que las direcciones privadas se conserven.

- Codificación de datos. Los datos a transmitir a través de la red pública (Internet), deben ser previamente encriptados para que no puedan ser leídos por usuarios no autorizados de la red. Esta tarea se realiza con algoritmos de cifrado como 3DES o AES que sólo pueden ser leídos por el emisor y receptor. Y para que lo datos no se han alterados se utiliza funciones de Hash como son los MD5 y el SHA.

- Administración de claves. La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

1.6.2 Tipos de VPN. Básicamente existen tres arquitecturas de conexión VPN:

- VPN Gateway to Gateway. Consiste en interconectar dos sedes de trabajo utilizando Internet como vínculo de acceso para compartir todos sus recursos. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local. El trafico que viaja a través de la red insegura va encriptado entre los dos gateways ofreciendo confidencialidad. Un atacante podría cumplir su objetivo siempre y cuando se encuentre dentro del dominio de alguna de las dos redes.

- VPN Gateway a Host. Consiste cuando todos los usuarios de una red requieren acceso seguro a un host o un servidor de la otra red. Un ejemplo es cuando los usuarios de una sede requiere acceso a un servidor de base de datos que se encuentra en la sede principal para ello el gateway de una sede se autentica con el host de la otra.

- VPN Host to Host. Consiste en conectar oficinas remotas con la sede principal de la Empresa. El servidor VPN, que posee un vínculo a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sede se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Ofreciendo confidencialidad, integridad y autenticación.

Esto ha permitido eliminar los costosos vínculos punto a punto tradicionales realizados mediante conexiones de cable físicas entre los nodos, sobre todo en las comunicaciones internacionales.

1.7 CIFRADO DE DATOS

En un Sistema de Comunicación de Datos, es vital asegurar que la Información viaje segura, manteniendo, su confidencialidad durante su almacenamiento y/o transmisión a través de los recursos informáticos.

Es por eso que existe un proceso de cifrado en el cual los datos a proteger son traducidos a algo que aparentemente es aleatorio y que no tiene significado alguno, es decir, los datos encriptados o cifrados. Pero también existe otro proceso conocido como descifrado en el cual los datos son convertidos nuevamente por medio de un método a su estado original.

La ciencia encargada de usar las matemáticas para encriptar y desencriptar datos que posteriormente puede ser almacenada en un medio inseguro o transferido a través de la red como el Internet y aun así permanecer secreta se conoce como la criptografía.

1.7.1 Métodos de Encripción. Para poder Encriptar un dato, se pueden utilizar dos procesos matemáticos diferentes los simétricos y los asimétricos.

- Algoritmos Simétricos**.** Utilizan una clave (un número, palabra, frase, o contraseña) con la cual se encripta y desencripta el documento. Todo documento encriptado con una clave, deberá descifrarse, en el proceso inverso, con la misma clave. Es importante destacar que la clave debería viajar con los datos, lo que hace arriesgada la operación, imposible de utilizar en ambientes donde interactúan varios interlocutores.

- Algoritmos Asimétricos (RSA). Requieren dos Claves, una Privada (única y personal, solo conocida por su creador) y la otra llamada Pública, ambas relacionadas por una fórmula matemática compleja imposible de reproducir.

El concepto de criptografía de clave pública surgió con el fin de solucionar la distribución de claves secretas de los sistemas tradicionales, mediante un canal inseguro. Mientras que la clave Privada deberá ser guardada.
Cuando se requiera verificar la autenticidad de un documento enviado por una persona se utiliza la Clave Publica para verificar el origen del mensaje porque el utilizó su Clave Privada para encriptar el mensaje.

- Firma Digital. Surgió como una oferta tecnológica para acercar la operatoria social usual de la firma ológrafa (manuscrita) al marco de lo que se ha dado en llamar el ciberespacio o el trabajo en redes.
Es la transformación de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posee el mensaje original y la clave pública del firmante, pueda establecer de forma segura, que dicha transformación se efectuó utilizando la clave privada correspondiente a la pública del firmante, y si el mensaje es el original o fue modificado.

1.7.2 Otros Métodos y técnicas de Encripción. A continuación se mencionara algunos:

- RSA. Algoritmo válido tanto para Encriptar como para firmar digitalmente. Su seguridad parte del problema de la factorización de números enteros donde 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.

- Blowfish. Algoritmo realiza un cifrado simple en 16 ciclos, con un tamaño de bloque de 64 bytes para un total de 448 bits.

- Triple DES. Algoritmo de 168 bits pero con seguridad efectiva de 112 bits fue desarrollado por el gobierno de EEUU seguro, pero lento. Consiste en encriptar

con el algoritmo DES tres veces con tres llaves diferentes.

- AES. *Advanced Encryption Standard.* Uno de los algoritmos más utilizados en criptografía simétrica, al convertirse en estándar en el año 2002. Utiliza un esquema de cifrado por bloques de 128 bits y claves de 128, 192 o 256 bits. Este algoritmo es rápido tanto por software como por hardware, fácil de implementar y no requiere alto consumo de memoria para el proceso.

2. ANÁLISIS DEL MÉTODO

La necesidad de transferir archivos de gran volumen de un sitio a otro de manera oportuna rápida y segura. El caso de estudio que se va analizar para dar una propuesta que cumpla con los requisitos de seguridad se da para una infraestructura donde el uso de las VPN's para la comunicación de los sitios remotos ubicados en varios puntos geográficos con la sede principal, en este momento surge una nueva necesidad de garantizar la transferencia de archivos de forma segura y constante utilizando un FTP Seguro y se hace indispensable estudiar que mecanismos se deben adoptar para lograr este objetivo.

En primera instancia se mencionan algunas ventajas y recomendaciones sobre el uso del protocolo FTPS:

✓ Al estar basado en el protocolo FTP se pueden acceder a los archivos independientemente del sistema operativo que utilice.

✓ Con este método la transferencia de archivos permite realizar cifrado a nivel datos, a nivel comandos o ambos la cual permite que el usuario y password requeridos no puedan ser detectados por captura de tráfico en la red.

✓ Usar el modo Pasivo debido a que el modo Activo tiene un grave problema de seguridad, porque la máquina cliente debe estar dispuesta a aceptar cualquier conexión de entrada en un puerto superior al 1024, esto tiene incidencia si tenemos el equipo conectado a una red insegura como Internet. De hecho, los cortafuegos que se instalen en el equipo para evitar ataques seguramente rechazarán esas conexiones aleatorias.

En segunda instancia es recomendable utilizar un método de acceso desde puntos

remotos, para ello se presentan las siguientes alternativas, siendo aconsejable el uso de VPN en vez de canales dedicados por el costo que este implica.

✓ El canal dedicado. Seria necesario adquirir el servicio o tender un cable ya sea de cobre o fibra óptica de un punto a otro, esta opción a nivel de costos no es rentable porque al querer enlazar la sede principal con una sucursal que se encuentra a varios Kilómetros de distancia el costo sería mensual por kilómetro mas el mantenimiento si fuese necesario sin importar el uso.

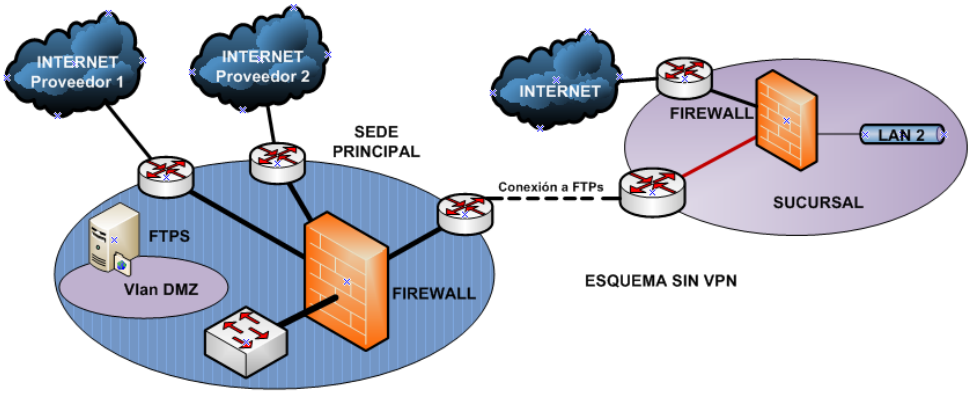
✓ VPN: Los costos son bajos al usar el Internet como medio de conexión adquirido por un proveedor local, además de tener la posibilidad de que mis datos viajen encriptados y seguros, con una buena calidad y velocidad.

Para que la información no sea alterada se utilizara el algoritmo Hash cual permite garantizar que el archivo no fue modificado.

Para garantizar el la transferencia de archivos con adecuados niveles de servicios es necesario realizar un análisis de lo que se requiere para dicho fin, para ello, se van analizar tres escenarios.

- Escenario 1. Transmisión mediante Internet sin VPN.

Figura 16. Transmisión mediante Internet sin VPN.



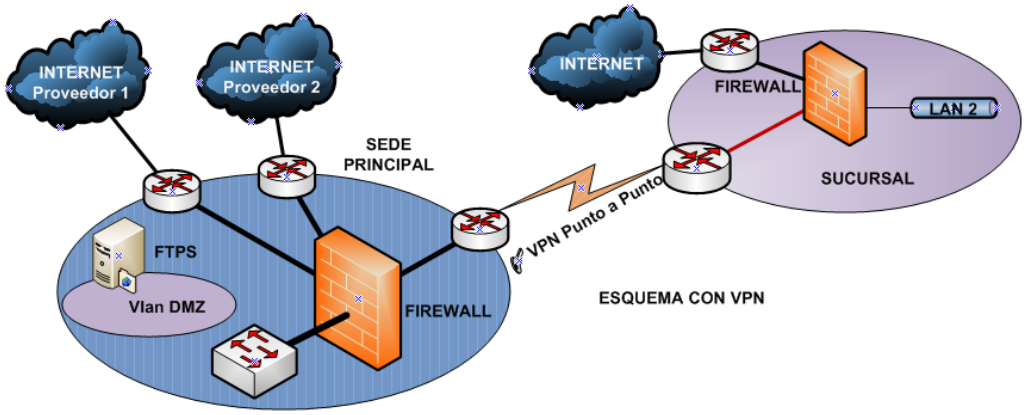
Desventajas de Transmisión sin VPN.

✓ Se requiere publicar el FTPS, lo cual podría facilitar el acceso a personas no autorizadas o generar denegaciones de servicio.

✓ Para poder acceder desde un punto remoto se recomienda tomar medidas de control adicionales como matricular en el Firewall corporativo las direcciones IP autorizadas para acceder al servidor FTPs. Lo anterior no permite el acceso desde sitios como hoteles o aeropuertos al no contar con una dirección IP fija.

- Escenario 2. Transmisión mediante Internet con VPN.

Figura 17. Transmisión mediante Internet con VPN.



Las ventajas del uso de VPN en el esquema de transmisión son:

✓ Permitir conectar redes físicamente separadas sin necesidad de usar una red dedicada, sino mediante el uso de Internet donde la movilidad y facilidad de conexión es evidente.

✓ Ofrece garantía de que los datos no han sido modificados mediante el uso de funciones criptográficas de validación de integridad (hash) y ofrece

confidencialidad de los datos al garantizar que solo puedan ser interpretados por el emisor y receptor gracias al uso de algoritmos de cifrado 3DES, AES permitiendo la transferencia de datos más segura.

✓ Al utilizar algoritmos de compresión permite optimizar el tráfico del cliente.

Algunas Desventajas del uso de VPN son:

✓ Incrementa la latencia de la transmisión y el ancho de banda requerido para la operación de la solución.

✓ Si la seguridad de alguno de los nodos de la VPN fuera vulnerada, esto afectaría la seguridad de todos los componentes de la VPN.

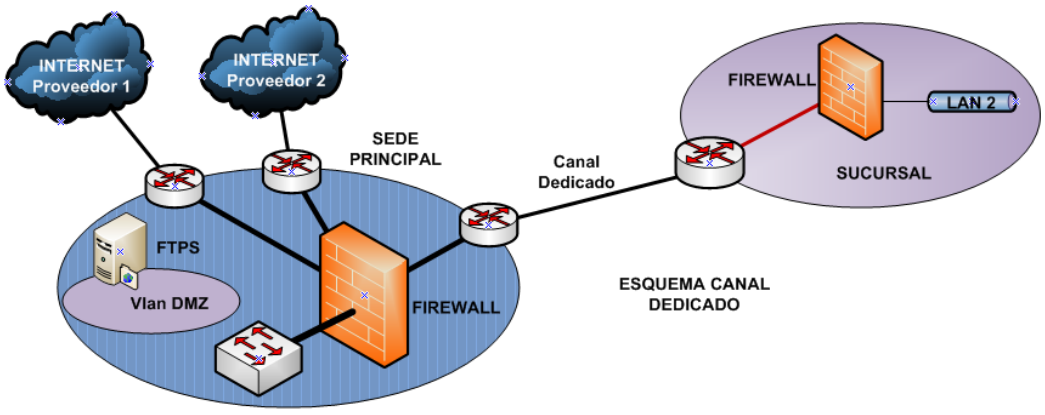
✓ Al existir variedad de soluciones hardware y aplicaciones software para implementar una VPN, pueden surgir problemas de interoperabilidad entre los diferentes nodos de la VPN.

✓ Imprime restricción a que el servicio solo estará disponible para usuarios u organizaciones que hayan establecido un lazo de confianza y hayan realizado un proceso previo de configuración de la VPN.

✓ Impide la trasferencias y descargas públicas de información, en otras palabras no es un FTP Publico.

- Escenario 3. Transmisión mediante un canal dedicado.

Figura 18. Transmisión mediante un Canal Dedicado.



Algunas Ventajas del uso de canales dedicados son:

✓ Fiabilidad y Calidad de servicios en entornos donde sean muy exigentes.

✓ Se puede controlar y aprovechar el consumo de ancho de banda para la transferencia de archivos.

Algunas desventajas del uso de canales dedicados son:

✓ Al tener el canal dedicado el costo es más elevado.

✓ En caso de inconvenientes en el canal dedicado se requiere tener un canal de continencia y el más adecuado de acuerdo a la necesidad de seguridad sería el de Internet con VPN o incluso un canal alterno dedicado.

En cualquiera de los tres casos el uso de protocolos FTPS es vital para garantizar que el canal de datos y de control se encuentre cifrado de extremo a extremo.

El no uso de la VPN implica que el FTPS deba estar publicado en Internet para

que tenga acceso independientemente del control perimetral el riesgo es mayor.

El Internet no es totalmente fiable y fallos en la red pueden dejar incomunicados recursos de la VPN.

La necesidad de tener la información que se transfiere en la red tanto de usuarios como de datos para evitar que atacantes, inclusive de la misma organización, puedan estar utilizando herramientas para capturar tráfico de la red y obtener toda la información que viaje en claro hace que sea vulnerable.

La importancia de cambiar contraseñas seguras para el acceso a los Servidores FTPS las cuales debe tener características como; tener por lo menos ocho caracteres, estar hecha de caracteres números y símbolos. Se deben evitar contraseñas que sean palabras que se encuentran en el diccionario, tengan que ver con sus datos personales.

A continuación se relaciona una tabla comparativa entre FTPS y SFTP.

Tabla 1. Cuadro Comparativo entre FTPS Y SFTP

METODO / **CONCEPTO**	**FTPS**	**SFTP**
PROTOCOLO	TLS (Transport Layer Security - Seguridad de la Capa de Transporte) es el sucesor del SSL (Secure Sockets Layer – Capa de conexión Segura).	SSH (Secure Shell - interprete de Ordenes Segura) .
COMUNICACIÓN	Utiliza dos canales de Comunicaciones	Utiliza un canal de comunicación
MENSAJES	Mensajes en Formato Texto	Mensajes en Binario
AUTENTICACION	Utiliza certificados X.509	Utiliza claves SSH

Continuación Tabla 1

METODO / CONCEPTO	FTPS	SFTP
USO	Mas usado debido a su sencilla implementación	Menos conocido
INTEROPERABILIDAD	Soporte se basa en las comunicaciones en la Web	No es compatible con otros dispositivos como móviles
GESTION DE CLAVES	De fácil uso	Son mas difíciles de Gestionar
LISTADO DE DIRECTORIO	No tiene un formato uniforme listado de directorio	La lista de directorios es uniforme y legible por máquina
GESTION DE ARCHIVOS	No tiene una forma estándar para obtener y modificar archivos y atributos de directorio.	El protocolo incluye las operaciones de autorización y la manipulación de atributos, el bloqueo de archivos y más funcionalidad.

Entonces ¿cuál sería la mejor opción? Esto depende de los objetivos y los requisitos. En general, SFTP es tecnológicamente superior a FTPS. Por supuesto, es una buena idea para implementar el soporte para los protocolos, pero son diferentes en los conceptos, en los comandos de apoyo entre otros aspectos.

Es una buena idea usar FTPS cuando se tiene un servidor que se debe acceder desde dispositivos personales (teléfonos inteligentes, PDAs, etc) o de algunos sistemas operativos específicos, que cuentan con el apoyo de FTP, pero no tiene SSH / SFTP clientes. Si usted está construyendo una solución de seguridad personalizada, SFTP es probablemente la mejor opción.

En cuanto a la parte del cliente, los requisitos son definidos por el servidor (s) que va a conectar. Cuando se conecta a servidores de Internet, SFTP es más popular porque está soportado por Linux y UNIX de forma predeterminada.

Para privacidad de host a host la transferencia se puede utilizar tanto SFTP y FTPS. Para FTPS es necesario buscar un cliente de FTPS libre y software de servidor o comprar una licencia para un comercial. Para soporte SFTP puede instalar el paquete OpenSSH, que proporciona el cliente libre y software de servidor.

3. PROPUESTA PLANTEADA

La propuesta se basa en el uso de mecanismos para garantizar los niveles de servicios requeridos.

- Servidor FTPS de alta disponibilidad. Esta estructura nos va permitir continuidad del servicio frente a fallos de hardware.

- Instalar una estructura de Firewall con equipos redundantes para ser el encargado de dar el acceso al servidor FTPS.

El propósito principal de un Firewall a, desde o hacia una red protegida. Implementa políticas de acceso a la red forzando que todas las conexiones pasen a través de el, en donde puedan se examinadas, evaluadas y registradas.

- Contar con por lo menos dos accesos de Internet de distintos proveedores para tener la posibilidad de usar los enlaces uno como activo y el otro de respaldo en caso de falla e inclusive tener ambos activos simultáneamente con balanceo de tráfico.

- Configurar las VPN para tener acceso a la Red Local y poder dar los permisos de acceso necesarios al Servidor FTPS.

- Cliente FTPS, se hace indispensable crear una herramienta que se instala en las maquinas la cuales requieren mover o descargar archivos al FTPS constantemente. Para ello, se debe tener en cuenta:

- Tener el usuario y password otorgado para poder conectarse al Servidor FTPS la cual debe cumplir los requisitos mínimos de seguridad o los que establezca la

organización de acuerdo a sus políticas de seguridad las cuales deben ser conocidas por todo el personal como es: Longitud mínima de caracteres, contener mayúsculas, minúsculas, números e inclusive caracteres especiales, que tengan tiempo de caducidad y tener los permisos necesarios otorgados por el firewall para el acceso.

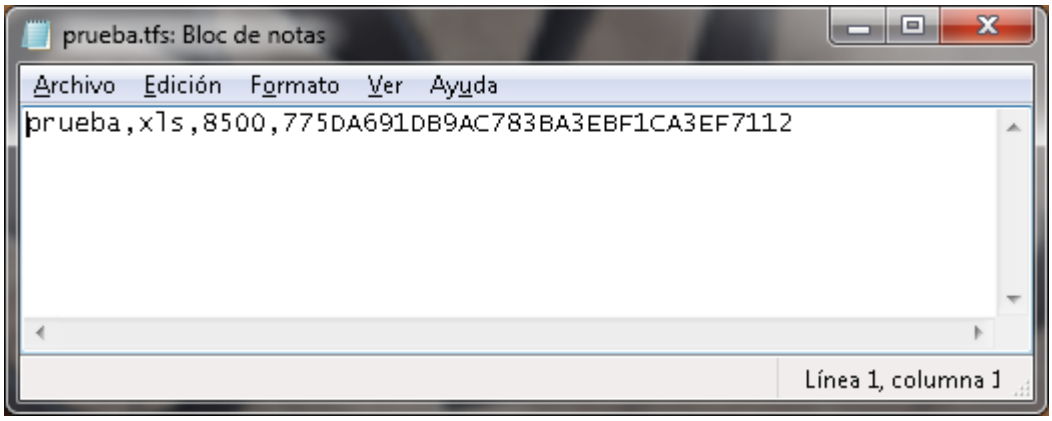
Esta herramienta se puede desarrollarse en VB.net donde existen componente para realizar las conexiones con FTPS y SFTP para ello, se debe tener los datos como son:

- Host / IP / URL
- Usuario
- Passwords
- Origen del archivo
- Destino del archivo

Al momento de tomar el archivo se debe obtener las siguientes características:

-Nombre del archivo
-Extensión del archivo (doc, .txt, .rar, .xls, etc.)
-Tamaño del archivo en Bytes.
-Obtener el código Hash del archivo.

Figura 19. Ejemplo del archivo generado con datos del archivo transferido.



Esta información debe ser almacenada en un archivo de texto en la maquina local con extensión .tsa que corresponde a (Transferencia Segura de Archivo).

Cuando se realice el proceso de transferencia se verifica sobre el Servidor FTPS nuevamente las características obtenidas del archivo al momento de iniciar la transferencia y se compara con los datos registrados en el archivo .tsa si la información que el archivo origen corresponde al destino se garantiza que el archivo no fue modificado.

CONCLUSIONES

La aplicación y el uso de protocolos de transferencia de archivos como el FTP junto con protocolos de seguridad TLS o SSH además de otras técnicas de encriptación nos ayudan a mantener la confidencialidad e integridad de los datos durante la comunicación, en una intranet o a través de Internet.

El uso de la VPN representan una solución para las empresas a nivel de seguridad, confidencialidad e integridad de los datos debido a que reduce significativamente el costo de la transferencia de datos de un sitio a otro sitio remoto, el inconveniente que pudieran tener las VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso para evitar consecuencias.

La seguridad de la información es de vital importancia para las diferentes actividades realizadas por la empresa y su deber es protegerla frente amenazas a fin de asegurarle a la organización que los riesgos, los daños y el impacto sean mínimos, por ello, se hace indispensable el uso de mecanismos al momento de requerir la transferencia de información entre dos puntos distantes el uso de la VPN y donde además de asegurar que la rentabilidad o relación costo/beneficio sean los mejores.

La disponibilidad del servicio hace de que la empresa este equipada o cuente con mecanismos para garantizar que la información esté disponible siempre que el usuario autorizado la necesite y poder hacer uso de ella, para ello, el uso de dos proveedores de Internet en caso de falla tener el proveedor de contingencia.

La seguridad es un aspecto fundamental para muchas aplicaciones cliente-servidor, porque día a día los ataques pueden ser múltiples y cada vez más

sofisticados, lo que implica una permanente investigación de los diferentes protocolos de seguridad, para su correcto uso.

BIBLIOGRAFÍA

FAQS.ORG. Internet RFC/STD/FYI/BCP Archives [on-line]. 2012. [Consultado el 15 de febrero del 2012, 9:05 p.m.]. Disponible en Internet: <URL:http://www.faqs.org/rfcs/>

FITZGERALD, Jerry. Redes y comunicación de datos en los negocios. México: Limusa Wiley. 2003.

FOROUZAN, Behrouz A.; CHUNG, Sophia; COOMBS, Catherine. Transmision de datos y redes de comunicaciones. Madrid: McGraw-Hill. 2002.

GARCÍA TOMAS, Jesús; RAYA CABRERA, José Luis y RODRIGO RAYA, Víctor; Alta velocidad y calidad de servicio en redes IP. Mexico: Alfaomega; Madrid: Rama. 2002.

HALSALL, Fred. Comunicación de datos, redes de computadores y sistemas abiertos. Mexico: Prentice Hall: Pearson Educacion: Addison Wesley, 1998.

HUIDOBRO, Moya y ROLDAN, José Manuel. Comunicaciones en redes WLAN: WIFI, VOLP, Multimedia, Seguridad. Madrid: Creaciones Copyright. 2006

LEÓN, Alberto y WIDJAJA, Indra. Redes de comunicación: conceptos fundamentales y arquitecturas básicas. Madrid: McGraw-Hill. 2002.

OPPLIGER, Rolf. Sistemas de autentificación para seguridad en redes. Santafe de Bogotá: Computec: Ra-Ma. 1998.

POSTEL, J. and REYNOLDS, J. File Transfer Protocol (FTP) [on-line]. October,

1985. [Consultado el 15 de febrero del 2012, 8:00 p.m.]. Disponible en Internet: <URL:http://tools.ietf.org/html/rfc959>

RADCOM LTDA. Guía completa de protocolos de telecomunicaciones. Madrid: McGraw-Hill. 2002.

STALLINGS, William. Redes e internet de alta velocidad: rendimiento y calidad de servicio. Madrid: Pearson Educacion. 2004.

WIKIPEDIA.ORG. File Transfer Protocol [on-line]. Actualizado Marzo de 2012. [Consultado el 5 de marzo del 2012, 3:05 p.m.]. Disponible en Internet: <URL: http://es.wikipedia.org/wiki/File_Transfer_Protocol>