Seguridad en Redes

La seguridad en redes tiene que garantizar que todos los usuario de las máquinas y la información posean los derechos que les han sido concedidos. Para poder conseguir esta seguridad se ha de estudiar y aplicar las técnicas necesarias para lograrlo. Además, una red es particularmente sensible de accesos no deseados para intenetar conseguir información, debido a que hoy en día tanto empresas, bancos, como particulares utilizan este medio digital para poder enviarse desde datos personales hasta informaciones confidenciales o datos bancarios.

Es importante entender que los medios de comunicación inseguros implican tener una amenaza constante.

Conceptos Generales

Actualmente se exponene tanto las empresas como las personas y los gobiernos a la dependencia de las redes informáticas, necesitando seguridad en tanto que se comparte, posee o comunica información.

Los conceptos que han de cumplirse para poder tener garantías en una comunicación por red que tiene correctamente implantada su seguridad son:

Confidencialidad: se trata de tener un mensaje o información de tal forma que solo sea entendido o leído por la persona o el sistema autorizado.
Integridad: se guarda la exactitud de la información. Incluye tanto el contenido de lso datos como el origen de los mismos.
Disponibilidad: se ha de garantizar que solo los usuario autorizados puedan tener acceso a la información y a los recursos derivados de ella.
Accesibilidad: gestionar eficientemente el acceso de la información

Propiedades de una comunicación segura

Se debe contar con un proceso integral de segurida que requiera los mecanismos tecnológicos necesarios para evitar pérdidas de información o vulnerabilidades.

Los dos tipos de seguridad más afectados en una comunicación hoy en día son:

Seguridad física: como prioridad en una organización se debe proveer de mecanismos que limiten el espacio físico para poder proteger contra amenazas de tipo ambiental, robos de información y pérdidas de datos. Por ejemplo, no dejar acceder a terminales a personas desconocidas.
Seguridad de la red: se debe asegurar que solos los paquetes válidos puedan ser enviados o recibidos, contando con herramientas como firewalls y routers para el filtrado.

Criptografía

La criptografía es el estudio de **técnicas y mecanismos para transformar un mensaje inteligible en un mensaje no inteligible** y su posterior transformación en el mensaje inteligible original. El proceso de transformación del mensaje inteligible a no inteligible se conoce como **cifrado**. Al mensaje transformado en no inteligible se le conoce como **mensaje cifrado**.

Para llevar a cabo el cifrado de un mensaje se utilizan dos elementos:

Clave: información conocida solo por el emisor y el receptor y utilizada en el proceso de cifrado.
Algoritmo de cifrado: mecanismo que convierte el mensaje sin cifrar en mensaje cifrado. La criptografía además proporciona una segunda funcionalidad que es la autenticación, es decir, la comprobación de la identidad del emisor del mensaje.

Existen dos tipos de criptografías:

Criptografía simétrica, también conocida como **criptografía de clave privada**.
Las dos partes de la comunicación acuerdan y comparten una clave secreta única.
Los datos se encriptan y desencriptan utilizando la misma clave y el mismo algoritmo. Para garantizar la seguridad de los datos transmitidos, debe protegerse la clave y solo debe ser conocida por aquellos que participan de la comunicación. Este sistema de cifrado es rápido y eficaz, hablando en términos computacionales. Actualmente existen diversos algoritmos muy robustos y potentes para llevarlo a cabo. Las claves utilizadas no son muy largas, aunque el grado de protección de la información es directamente proporcional a la longitud de la clave secreta. El mayor **inconveniente** de este sistema se presenta en la **distribución de la clave entre las partes a comunicarse**. La distribución de la clave debe ser por medios seguros, ya que de otra forma podría ser interceptada y verse comprometida la privacidad de las transmisiones. actualmente, los algoritmos de clave privada más usados son DES, 3DES, AES, RC4, RC2.

Criptografía asimétrica, también conocida como **criptografía de clave pública**.
En este caso **se utilizan dos claves, llamadas clave pública y clave privada**.
La base de la criptografía asimétrica es que la información que se cifra usando una de las claves solo se puede descifrar usando la otra. Lo normal es que se utilice **la clave pública para cifrar y la clave privada para descifrar**. En un proceso de comunicación cifrada, el receptor debe generar el par de claves pública/privada. La clave pública puede ser distribuida a todos los posibles remitentes de información, sin embargo la clave privada nunca debe ser facilitada (tampoco es necesario). Cuando un dispositivo quiera enviar información al receptor, utilizará la clave pública para cifrar dicha información, la cual solo podrá descifrarse utilizando la clave privada que solo conoce el receptor.

Por tanto, la clave pública puede ser distribuida libremente, pero la clave privada no es necesario distribuirla y solo el receptor necesita conocerla. Ésta es la principal ventaja de este tipo de cifrado, ya que proporciona un alto nivel de seguridad.

La principal **desventaja** es que **el proceso de encriptación es bastante más lento que en el caso de la criptografía simétrica**. Por ello, en algunos casos se utiliza la criptografía asimétrica solo para transmitir una clave secreta que luego se utilizará para cifrar los datos con criptografía simétrica.

Las claves en el caso de la criptografía asimétrica son más largas que en la criptografía simétrica.

Los algoritmos de criptografía asimétrica más utilizados son RSA, PGP y Diffie-Hellman.
OJO! En la criptografía asimétrica o de clave pública: Se utilizan siempre dos claves, una pública y otra privada. Solo el dispositivo que conozca la clave privada podrá descifrar la información cifrada con la clave pública. La clave pública se puede distribuir sin problema, la clave privada ¡nunca!.
Algoritmos utilizados en la criptografía asimétrica:

Diffie-Hellman
RSA
DSA
ElGamal
Criptografía de curva elíptica
Criptosistema de Merkle-Hellman
Goldwasser-Micali
Goldwasser-Micali-Rivest
MD5
SHA-1

AUTENTICACIÓN

La autenticación **es la comprobación de la identidad del emisor del mensaje y la integridad de los datos del mismo**. Los principales métodos de autenticación, como son las firmas digitales y los certificados digitales, se basan en la utilización de la criptografía asimétrica.

Existen diferentes métodos de identificación digital para poder comprobar la identidad de una persona y autenticarse:

Soluciones biomédicas: como pueden ser sensores de huellas dactilares o de las características únicas de la retina del ojo, etc.
Tarjetas inteligentes: las cuales guardan información de los certificados de un usuario.
Métodos clásicos basados en establecimiento de usuario y contraseñas: en los cuales supuestamente solo se facilita estos datos a la persona que puede manejar esa información.

Clave secreta (privada o simétrica)

- Basado en protocolos simétricos
- Basados en servidores de registro de usuarios, actualmente los más famosos son las plataformas TACAS y servidores RADIUS. Protocolos para descentralizar el control de acceso de forma tal que cualquier tipo de servicio necesario de validación o autorización de un usuario lo puede realizar como cliente de estas plataformas. Este método es muy empleado en apoyo a hardware de red (routers) y gestión de usuarios en plataformas inalámbricas.
- Basados en servicios de información de red como NIS
- Basados en centros de distribución de claves criptográficas como el método Kerberos. ESte método actua como dos partes, empleando un canal seguro hasta cada una de las dos partes. La autenticación se producirá entre cliente-Kerberos (servidor) y servidor (Kerberos)-cliente. Kerberos conoce todas las claves secretas de todos los usuarios para poder actuar como medidor.

Clave pública (asimétrica) con métodos como:

- X-500 y LDAP (protocolo de acceso directo ligero)
- Certificados: los certificados son documentos electrónicos los cuales son firmados por un prestador de servicios de garantía que vincula y garantiza datos entre ambas partes.

Integridad

La integridad es la propiedad que busca mantener los datos sin sufrir modificaciones no autorizadas, manteniendo la información inalterada sin ser manipulada por parte de personas o procesos sin autorización.

Los datos puede ser alterados por dos causas:

- Causas accidentales: debido a errores electrónicos o humanos
- Causas Intencionada: interviene el factor humano

Distribución de claves y certificados

- Distribución manual de claves de manera ajena a la red, con métodos tradicionales, como la entrega en mano de la contraseña a compartir.
- Distribución utilizando un intermediario que sea de confianza para ambas partes de manera electrónica. Surgen los centros de distribución de claves privadas (KDC, key distribution center) para las claves simétricas.
- Distribución de claves centralizadas a través de un centro de distribución (KDC) se basa en el uso de claves de nivel jerárquico para transmitir la información a través de una clave de sesión asignada por un sistema centralizado.
- Distribución a través las autoridades certificadoras (CA, certification authority), que son entidades reconocidas nacional e internacionalmente para estos fines. Por Ejemplo: DNI electrónico, la autoridad es la Fábrica Nacional de Moneda y Timbre.

Firmas digitales

En las firmas digitales, el emisor de un mensaje firma el mismo cifrando la información con **su clave privada y esa ?firma? es única, ya que solo él dispone de dicha clave privada**. El receptor puede verificar esa firma utilizando la clave pública correspondiente emitida por el emisor del mensaje. Con este proceso **se proporciona autenticación para el mensaje enviado, pero no seguridad mediante cifrado** porque cualquiera puede disponer de la clave pública correspondiente y recuperar el mensaje original

Certifiacados

Un certificado es un documento digital que acredita que la clave pública que contiene es de quien dice ser. Para avalar tal afirmación, este documento es respaldado por una **autoridad de certificación (CA, Certification Authority)** mediante su firma digital.

Las entidades de certificación son organismos seguros e independientes que emite certificados de autenticidad de claves públicas.

Un **certificado consta de la clave pública que certifica, el nombre del propietario, un período de validez, el nombre de la autoridad de certificación y un número de serie**. Este certificado viene firmado digitalmente por el emisor. Los navegadores web contienen una lista de las principales entidades de certificación, por lo que si establecemos una comunicación segura con alguna entidad (banco, comercio electrónico) que haya certificado su clave pública con alguna de éstas, la comunicación se realizará de forma segura y transparente al usuario.

Si la entidad de certificación no está reconocida por el navegador web, es el usuario el que debe aceptar o no la comunicación.

Un certificado ha de contener la siguiente información:

Número de serie. Un número de serir único que identifique el emisor de forma única en la red.
Información sobre el propietario. A quién pertenece el certificado, incluyendo además el algoritmo empleado y el valor de la clave.
Información sobre el emisor del certificado. La entidad que certifica el certificado, con sus datos como compañía.
Período de validez. Los certificados han de ser renovados cada período. Contendrá el período de inicio y fin de validez.
Firma digital del emisor. Corresponde a la **huella o firma electrónica** que posee el emisor.

Existen dos clases de distribución certificada de claves:

Distribución por transferencia de clave: la entrega se realiza a través de un sistema público, cifrando la clave generada por la entidad autorizadora, viajando protegida hasta la entidad remota para su uso.
Acuerdo o intercambio de claves: se genera con ambas partes, la entidad que requiere la clave solicita a la entidad remota la generación compartida de la misma.

Aplicaciones

De manera general se intenta crear aplicaciones que puedan reforzar la **seguridad en Internet**. Estas aplicaciones suelen trabajar a partir de **la capa tercera o red del modelo OSI**; es decir, a partir de la zona de encminamiento que es donde más vulnerable se vuelve una comunicación.

SSL (Secure Sockets Layer) Capa de Conexión Segura

Es un protocolo criptográfico de los más usados diseñado para la transferencia de datos de manera segura entre ordenadores conectados a través de Internet o de red interna. Consiste en un cifrado que deben conocer ambos ordenadores para que haya

entendimiento entre ellos.

SSL se ejecuta entre los protocolos de aplicación y el protocolo de transporte TCP. Se emplea habitualmente para formar páginas web seguras (HTTPS).

SSH (Secure Shell)

Es un protocolo que se emplea para intercambiar información y mensajes a través de un canal seguro entre dos hosts. Emplea la arquitectura cliente-servidor. Puerto o Socket 22.

Se emplea habitaulmente para entrar de forma remota a un sistema, reemplazando a comandos menos seguros. Otros protocolos asociados como SCP y SFTP.

SCP (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. El término SCP puede referir a dos conceptos relacionados, el protocolo SCP o el programa SCP.

SFTP

SSH 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.

IPSEC

El término **IPsec se refiere al conjunto de protocolos implementados para proporcionar seguridad** a las comunicaciones a través de redes IP. Inicialmente IPsec fue diseñado para IPV6, pero debido a las fuertes necesidades de seguridad actuales se ha adaptado para poder utilizarlo sobre IPV4. IPsec proporciona: **servicios de seguridad**, incluyendo:

Control de acceso
Integridad en las comunicaciones sin conexión
Autenticación del origen de los datos
Protección contra ataques de repetición
Confidencialidad mediante encriptado
Etc.

Estos servicios son proporcionados en el nivel IP (nivel 3) y ofrece protección para éste y los niveles superiores. Para ofrecer tales servicios, IPsec utiliza dos protocolos de seguridad:

AH (Authentication Header)
ESP (Encapsulating Security Payload)

Además del uso de protocolos y procedimientos de administración de claves criptográficas. el protocolo de administración automática de claves por defecto es **IKE (Internet Key Exchange)**. IKE es usado para establecer una política de seguridad compartida y claves autenticadas para servicios que los requieran (como IPsec). Antes del envío de tráfico IPsec, cada router/firewall/host debe ser capaz de verificar la identidad de su par.

Los mecanismos utilizados por IPsec están diseñados para ser independientes de los algoritmos empleados. Esta modularidad permite la selección de diferentes conjuntos de algoritmos sin afectar al resto del sistema.

Protoclo AH

El protocolo **AH proporciona autenticación, integridad y antirreproducción** para todo el paquete. AH **firma el paquete entero pero no cifra la información**, por lo que **no proporciona confidencialidad.** La información es legible, pero está protegida contra modificaciones. Utiliza algoritmos HASH con claves que se denominan **HMAC (Códigos Hash de Autenticación de Mensajes)**, para firmar el paquete.

Protoclo ESP

El protocolo ESP **proporciona confidencialidad (además de autenticación, integridad y antirreproducción)** para los datos de un datagrama IP. No firma, normalmente, el paquete entero (a no ser que se esté realizando un túnel), ya que solo protege la información, y no el encabezado IP. Puede utilizarse por sí solo o en combinación con AH.

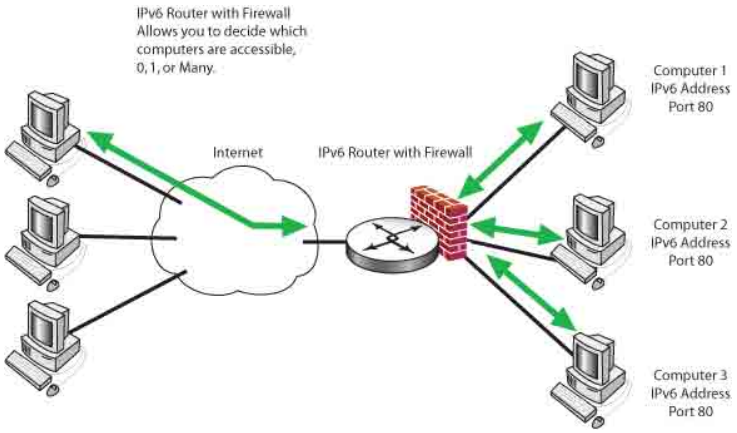
Existen dos modos de utilización de IPsec:

Modo túnel, se utiliza para comunicaciones red a red, red a host o host a host a través de internet. El encabezado IP interno (encapsulado) es encriptado ocultando la identidad del destinatario y el origen del tráfico.

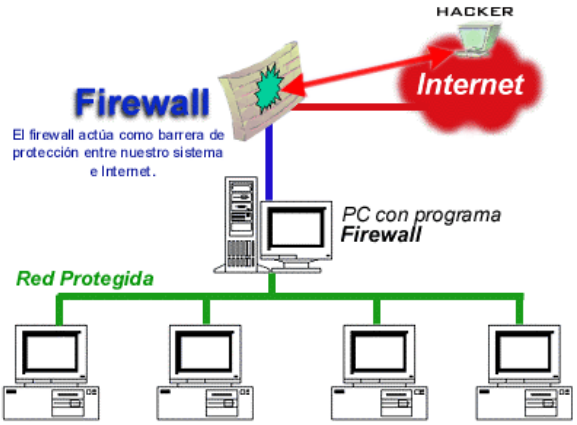
Modo transporte, utilizado para comunicaciones de extremo a extremo, es decir, de host a host. solo se cifran los datos. La cabecera no va encriptada pero sí puede ir firmada, por lo que no se puede modificar.
Todo el proceso de encapsulación, encaminamiento y desencapsulación se denomina túnel
Cortafuegos (Firewall)

El concepto de firewall o cortafuegos apareció en el ámbito de las redes de datos para describir los diferentes mecanismos de seguridad destinados a bloquear la transferencia de datos que no cumplan unos criterios de seguridad determinados. Está **considerado en la actualidad como un mecanismo de seguridad necesario pero no suficiente para proteger las redes** y los equipos conectados a las mismas. Se puede aplicar en dos ámbitos:

Firewall de red. Este ámbito se aplica a dispositivos de interconexión, es decir, routers. Un firewall de red proporciona los mecanismos de control en los datos intercambiados entre las redes a las que se conecta el router o cualquier dispositivo que haga funciones de enrutamiento.



Firewall de equipo. Este ámbito está referido a la función de firewall implementada en un ordenador y que tiene como finalidad aplicar los mecanismos de control en los datos intercambiados entre el equipo y la red.



Las funciones básicas de un firewall consisten en inspeccionar todo el tráfico intercambiado entre dos entidades (entre dos redes o entre un equipo y una red) y comprobar que cumplen ciertas reglas de seguridad permitiendo o denegando dicho tráfico en función de que se cumplan o no dichas reglas. El tipo más habitual de reglas se basa en el criterio de selección de puertos. De esta manera se establecen una serie de reglas para permitir el paso de datos dirigidos a una serie de puertos determinados, denegando el acceso al resto de los puertos.

A este proceso de inspección de paquetes intercambiados entre dos entidades para permitir o denegar el propio intercambio se le denomina generalmente **filtrado**.

Tercera generación o cortafuegos de aplicación

Los firewalls de tercera generación actúan directamente sobre la capa 7 del modelo OSI, lo que les provee de mayor seguridad y versatilidad, ya que entienden de aplicaciones y protocolos de aplicación directamente. Entiende y es capaz de rechazar un protocolo distinto a través de un puerto que debería de trabajar un protocolo determinado. Estos cortafuegos tiene que procesar mucha más información.

Funciones de un firewall

- Filtrar los accesos no autorizados a través de un filtrado selectivo de paquetes de datos
- Alterar en caso de comportamiento extraño o inusual en los sistemas de comunicaciones, síntoma de un posible ataque o intrusión
- Medir datos de la red, como el tipo de tráfico o el ancho de banda; en definitiva, cuantificar el tráfico tanto entrante como saliente de una red.

Zona DMZ de un Firewall

Un cortafuegos contiene como mínimo dos interfaces de red para operar y crear reglas de conexión entre ambas.

La **zona desmilitarizada (DMZ)** actúa de forma que los servidores que requieren acceso a Internet, como servidores de archivos, páginas web, correo electrónico, etc. puedan tener un acceso a Internet apartado de la red interna por motivos de seguridad.

Sistemas IPS

Los sistemas IPS o de prevención de intrusos son sistemas desarrollados a partir de las deficiencias que traen los firewalls o faltas de opciones para tener un sistema integral que pueda manejar las amenazas actuales.

En los sistemas IPS existen los siguientes módulos: el módulo IPS analiza el tráfico de red y crea estadísticamente una base con la que comparar. Cuando monitoriza un tráfico con demasiada varianza se genera una alarma. La base con la que compara puede determinarla un administrador, pero suele generar demasiadas falsas alarmas.

Detección basada en anomalías: el módulo configurado por políticas de seguridad determina que nodos, máquinas o hosts pueden acceder a ciertas redes. El IPS, al observar un tráfico de un host dirigido a una red o subred no autorizada, lo descarta.

Detección basada en políticas: el módulo configurado por políticas de seguridad determina que nodos, máquinas o hosts pueden acceder a ciertas redes. El IPS, al observar un tráfico de un host dirigido a una red o subred no autorizada, lo descarta.

Detección basada en firmas: IPS es capaz de reconocer una cadena de bytes con un contexto específico y rechazado. Por ejemplo, una cadena de una dirección web sospechosa. Es necesario que éste siempre actualizado para que sea eficaz.

Detección honeypot o jarra de miel: sirve para detectar intrusos en base a dejar una distracción con cierto atractivo (la jarra de miel) para un atacante. Los atacantes tratan de ganar acceso en el sistema, mientas que el administrador analiza los métodos y trata de identificar al atacante. Además, sirve para implementar nuevas medidas de seguridad.