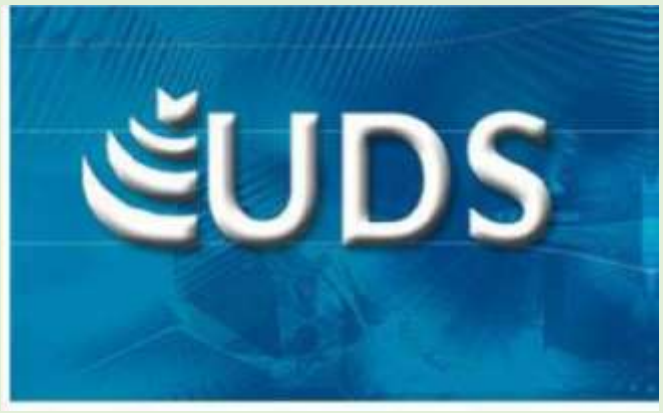


UNIVERSIDAD DEL SURESTE

Materia:

Redes de Computadoras

Tema:

Claves públicas o privadas

Alumno(a):

Jirem Madali Jiménez Trejo

7° cuatrimestre

Docente:

Ing. Eduardo Genner Escalante Cruz

CLAVES PÚBLICAS O PRIVADAS

FIREFALL

Un firewall, también llamado cortafuegos, es un sistema cuya función es prevenir y proteger a nuestra red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso.

Permite el tráfico entrante y saliente que hay entre redes u ordenadores de una misma red. Si este tráfico cumple con las reglas previamente especificadas podrá acceder y salir de nuestra red, si no las cumple este tráfico es bloqueado.

Principales funciones:

- Crear una barrera que permita o bloquee intentos para acceder a la información en su equipo.
- Evitar usuarios no autorizados accedan a los equipos y las redes de la organización que se conectan a Internet.
- Supervisar la comunicación entre equipos y otros equipos en Internet.
- Visualizar y bloquear aplicaciones que puedan generar riesgo
- Advertir de intentos de conexión desde otros equipos.
- Advertir ir de intentos de conexión mediante las aplicaciones en su equipo que se conectan a otros equipos.
- Detectar aplicaciones y actualizar rutas para añadir futuras fuentes de información
- Hacer frente a los cambios en las amenazas para la seguridad.

THOR BROWSER

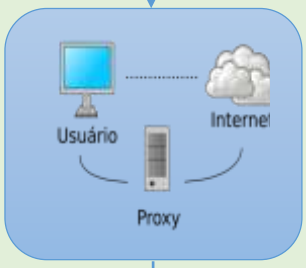
El objetivo de este proyecto es el de crear una red de comunicaciones distribuida y superpuesta al Internet convencional.

Tor Browser es un navegador gratuito de código abierto configurado para funcionar en la red Tor, en la que tus páginas pasan encriptado por varios servidores antes de salir a internet, ofuscando su origen para mejorar tu privacidad y sirve para evadir los bloqueos en internet.

El browser borra todas las cookies, contraseñas y datos ingresados en formularios cada vez que lo cierras, por lo que te garantizan una conexión no permanente y por lo tanto vulnerable.

PROXY

Un proxy es un equipo informático que hace de intermediario entre las conexiones de un cliente y un servidor de destino, filtrando todos los paquetes entre ambos.



Los proxys son utilizados muy a menudo para acceder a servicios que tienen bloqueado su contenido en determinado país.

Como usuario tienes dos posibilidades para usar un proxy:

-A través de un servicio web.

-Configurándolo en Windows.

SSL

Se trata de protocolos criptográficos que proporcionan privacidad e integridad en la comunicación entre dos puntos en una red de comunicación. Esto garantiza que la información transmitida por dicha red no pueda ser interceptada ni modificada por elementos no autorizados, garantizando de esta forma que sólo los emisores y los receptores legítimos sean los que tengan acceso a la comunicación de manera íntegra.

En el protocolo SSL se utiliza tanto criptografía asimétrica como simétrica. La primera se utiliza para realizar el intercambio de las claves, que a su vez serán usadas para cifrar la comunicación mediante un algoritmo simétrico.

El conjunto de datos que están protegidos por el protocolo de encriptación SSL incluye:

- Información de registro: nombre, dirección, dirección de correo electrónico, número de teléfono
- Datos de identificación: dirección de correo electrónico y contraseña
- Datos de pago: número de tarjeta de crédito, cuenta bancaria
- Formularios de inscripción
- Documentos cargados por los clientes.

EL SSL proporciona un canal seguro entre dos computadoras o dispositivos que operan a través de Internet o de una red interna.

CLAVES PÚBLICAS O PRIVADAS

ROBO DE IDENTIDAD

El robo de identidad (Identity theft o "ID theft") se produce cuando una persona adquiere, transfiere, posee o utiliza información personal de una persona física o jurídica de forma no autorizada, con la intención de efectuar o vincularlo con algún fraude u otro delito.

Los principales métodos empleados por los delincuentes para adquirir información personal de las víctimas utilizando Internet son: Crear un tipo de virus que se instale en el ordenador o móvil y que recopile información personal, sin que el usuario sepa que está ahí o conozca su verdadero fin.

HTTPS

https es "Hyper Text Transfer Protocol" con una 'S' añadida al final, que hace referencia a "Secure Sockets Layer" otro importante protocolo desarrollado para realizar transferencias de forma segura en Internet usando nuestro navegador.

Es un método para garantizar una comunicación segura entre el navegador de un usuario y un servidor web. A menudo se reconoce por una barra de direcciones verde o un candado en la ventana del navegador, que indica que la conexión es segura.

Cuando un navegador inicia una sesión HTTPS con el servidor web, el servidor envía la clave pública al navegador y se lleva a cabo un 'SSL Handshake' (saludo) entre el navegador y el servidor. Una vez que la conexión segura se ha iniciado y aceptado, el navegador reconoce el link y lo muestra como seguro, ya sea mediante una barra verde o un candado, dependiendo del tipo de certificado SSL que se use.

VPN

Una red privada virtual (RPV) (en inglés, Virtual Private Network, VPN) es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

Permite que el ordenador 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.

Una VPN consiste en dos computadoras y una ruta –que suele llamarse "túnel"–, que se crea haciendo uso de una red pública [Internet] o privada. La privacidad de esta conexión es una preocupación, por lo que los datos transmitidos son codificados (encriptados), enviados y nuevamente decodificados a su recepción.

Una VPN usualmente requiere autorización y autentificación, además de que usa criptografía.

ATAQUES DE DENEGACION DE SERVICIO

También llamado ataque DDoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de computadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Los ataques por denegación de servicio envían paquetes IP o datos de tamaños o formatos atípicos que saturan los equipos de destino o los vuelven inestables y, por lo tanto, impiden el funcionamiento normal de los servicios de red que brindan.

Tiene como objetivo imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo.