14 - Direccionamiento Interno y Externo

lunes, 26 de abril de 2021 14:39

DIRECCIONAMIENTO INTERNO:

ROUTER: realiza el routing (la función de mover datos de una red a otra) y permite interconectar computadoras estableciendo que ruta deberán seguir los datos.

1. Recibe el paquete de datos.
2. Busca cuál es la dirección de destino.
3. Verifica la tabla de enrutamiento (conjunto de reglas con toda la información necesaria para optimizar el camino de los datos. Tiene 1: red de destino a donde irá el paquete de datos, 2: el siguiente salto o dirección de IP por donde viajará el paquete y 3: interfaz de salida por donde deben salir los paquetes) que tiene configurada.
4. Envia el paquete a destino por la mejor ruta posible.

TIPOS DE ENRUTAMIENTO:

Estático: consume menos memoria y menos ancho de banda, pero no es escalable y se usa para redes pequeñas.
Dinámico: tiene un gran consumo de ancho de banda y de memoria, pero es automático y se usa para redes grandes.

PUERTOS: las distintas solicitudes de recursos/servicios (google drive, mail, notes, etc) se diferencian a través de puertos (cada dispositivo tiene 65536). Son puntos de conexión para el intercambio de información. Cada uno de ellos están destinados a recibir o enviar cierto tipo de información (estandarizados por la *IANA*):

- 0-1023: reservados para el SO de la computadora y los protocolos más importantes para su funcionamiento.
  - 21: FTP.
  - 25: SMTP.
  - 80: HTTP.
- 1024 - 49151: puertos registrados, utilizados por las aplicaciones y juegos instalados.
- >49151: puertos dinámicos o privados que corresponden a las aplicaciones que necesitan conectarse a un servidor.

DIRECCIONAMIENTO EXTERNO:

ISP (Proveedor de Servicios de Internet): muchos datos son enviados de forma encriptada, que muestran hacia dónde van pero no el contenido. Los ISP reciben todos los paquetes de datos que enviamos y los envían a sus destino, pudiendo aplicar normativas de piratería, políticas gubernamentales, bloqueos regionales, etc.

PROXY: equipo informático que intercepta conexiones de red cliente-servidor, eludiendo así al ISP. Le podemos indicar que datos filtrar y no dejar pasar.

VPN (Red Privada Virtual): permite una extensión segura de la red local sobre una red pública como internet. Nos permite enviar y recibir datos como si nuestra red fuera una red privada (con sus características y políticas).
(recomendación: psiphon 3 (es gratis))

TOR: una red de anonimato que está distribuida y superpuesta sobre internet, en la que el direccionamiento de los mensajes entre usuarios no revela su dirección IP, manteniendo la integridad y el secreto de la información. Para esto, el usuario accede primero a un nodo TOR que conoce la identidad del usuario pero no el destinatario, y el último nodo sabe quién es el destinatario pero no el remitente.

SURFACE WEB: compuesta por los sitios indexados, que son fáciles de buscar gracias a la URL (que sería el índice).
DEEP WEB: material censurado/privado, que se accede conociendo la IP, ya que no está indexado.
DARK WEB: para acceder necesitamos un muy buen nivel de seguridad para no ser rastreados (como TOR o un PROXY). Gracias a la dificultad del rastreo, motiva los sitios ilegales.