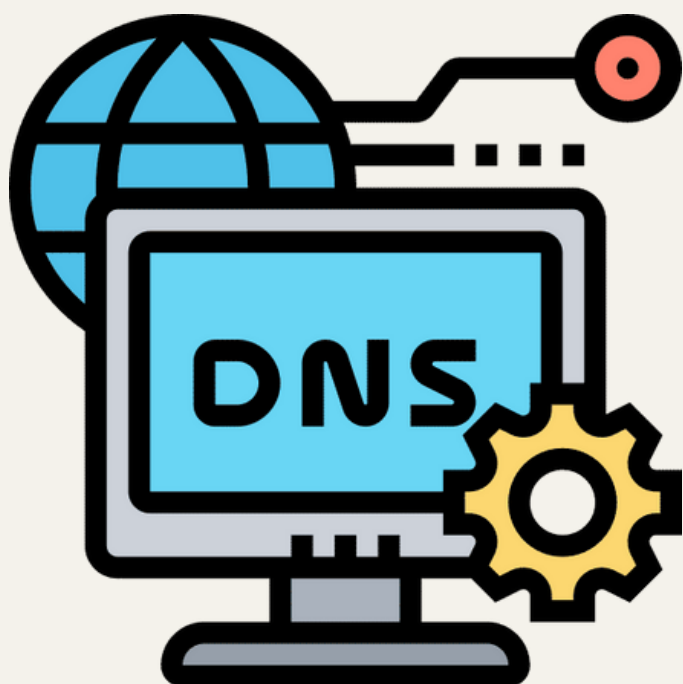


CÓMO FUNCIONAN LOS SERVIDORES DNS

@saulruizplaza



¿QUÉ ES EL DNS?

DNS (Domain Name System) es el sistema que **traduce** los nombres de **dominio** (como www.ejemplo.com) **en direcciones IP** (como 192.0.2.1), necesarias para la comunicación entre dispositivos en la web.

Sin DNS, tendríamos que recordar direcciones IP, lo cual sería poco práctico.

¿Cómo funciona?

- **Solicitud de DNS:** Cuando un usuario escribe un nombre de dominio, el navegador solicita la dirección IP asociada.
- **Consulta a los servidores DNS:** Los servidores DNS recursivos son los encargados de realizar la búsqueda de la IP, desde sus registros locales o consultando otros servidores.
- **Respuesta DNS:** El servidor DNS autoritativo para el dominio responde con la dirección IP, permitiendo al navegador conectarse al servidor de destino.

Tipos de servidores

- **Servidor DNS recursivo:** Este servidor actúa en nombre del cliente, realizando la búsqueda de la IP si no la tiene en caché.
- **Servidor DNS autoritativo:** Mantiene los registros definitivos para un dominio y responde directamente con la dirección IP.
- **Servidores DNS de TLD (Top-Level Domain):** Responsables de dominios de nivel superior como ".com", ".org", ".net". Son cruciales en la jerarquía de resolución de nombres, proporcionando información para los dominios más específicos.

Jerarquía

- **Servidores DNS raíz:** Estos son los servidores de más alto nivel, que dirigen las consultas a los servidores DNS de TLD.
- **Servidores DNS de TLD.**
- **Ejemplo práctico:** Cuando consultas un dominio como "ejemplo.com", el servidor DNS de TLD para ".com" es el que te dirige al servidor DNS autoritativo de ese dominio específico.

Vulnerabilidades

- **Ataques de phishing:** Manipulación de DNS para redirigir a usuarios a sitios fraudulentos.
- **DNS Spoofing/Cache Poisoning:** Alteración de la caché de los servidores DNS para redirigir a sitios maliciosos sin que el usuario se percate.
- **DDoS (Denegación de Servicio Distribuida):** Ataques dirigidos a servidores DNS para desbordarlos y dejarlos fuera de servicio, afectando la disponibilidad de servicios en línea.

Medidas de protección

- **DNSSEC (DNS Security Extensions):** Implementación de firmas digitales para garantizar la autenticidad de las respuestas DNS y evitar ataques como el cache poisoning.
- **Servidores DNS confiables:** Usar proveedores de DNS con robustas medidas de seguridad, que protejan contra ataques como DDoS y falsificación de respuestas.
- **Monitorización continua:** Detectar anomalías en el tráfico DNS para identificar posibles amenazas.

Conclusión

- El DNS no solo es esencial para **navegar por la web**, sino que también es un eslabón crítico en la infraestructura de Internet. Sin un sistema DNS confiable y seguro, no podríamos acceder de manera eficiente a los sitios web ni **protegernos contra amenazas** como el phishing o los ataques de redirección maliciosa.
- Asegúrate de **implementar medidas de seguridad adecuadas** para proteger tu infraestructura DNS y garantizar la seguridad en la red.

@saulruizplaza

Espero que te sea útil

