Firewalls

Seguridad en comunicaciones

Taller de despliegue de aplicaciones

Agenda

01

Que es un Firewall ?

02

Que son los Puertos ?

03

Publica vs Privada

04

NAT

01

Qué es un Firewall ?

Firewalls

- **Definición de Firewall**: Un firewall es un sistema de seguridad de red que controla y filtra el tráfico de entrada y salida basado en reglas de seguridad predeterminadas.

- **Importancia de los Firewalls**: Protegen las redes internas de accesos no autorizados y ataques cibernéticos.

Tipos

Firewalls de Red: Controlan el tráfico entre redes y se sitúan en los perímetros de las mismas. (AWS)

Firewalls de Host: Protegen un único dispositivo, supervisando y filtrando el tráfico de red a través del sistema operativo. (el de Windows)

Firewalls de Aplicaciones Web: Protegen aplicaciones web específicas, filtrando y monitoreando el tráfico HTTP.

Cómo Funcionan

- **Filtrado de Paquetes**: Inspecciona los paquetes de datos y permite o bloquea su paso basado en reglas predefinidas.
- **Inspección con Estado (Stateful Inspection)**: Monitorea el estado de las conexiones de red y permite o bloquea el tráfico basado en el estado y el contexto de la conexión.
- **Filtrado de Aplicaciones**: Inspecciona el tráfico de aplicaciones específicas y bloquea actividades no autorizadas.

02

Qué son los puertos ?

Puertos de red

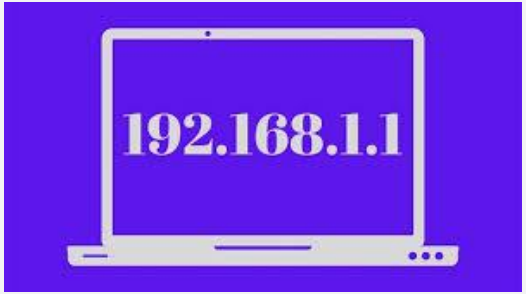
- Los puertos son puntos de conexión en un dispositivo de red que permiten la entrada y salida de datos.

- **Puertos Conocidos (0-1023)**: Usados por servicios y aplicaciones comunes (e.g., HTTP en el puerto 80, HTTPS en el puerto 443).
- **Puertos Registrados (1024-49151)**: Usados por aplicaciones de usuario o procesos que no requieren acceso root.
- **Puertos Dinámicos o Privados (49152-65535)**: Usados temporalmente por aplicaciones para establecer conexiones con servidores.

Puertos y Seguridad

- **Escaneo de Puertos**: Técnica usada por atacantes para encontrar puertos abiertos en un dispositivo de red.
- **Cierre de Puertos No Necesarios**: Práctica de seguridad para minimizar la superficie de ataque.
- **Monitoreo de Puertos**: Supervisión de los puertos abiertos y el tráfico que pasa por ellos.

03



Publica vs Privada

IP Pública

Una dirección IP pública es una dirección única asignada a un dispositivo que está conectado a Internet. Es accesible desde cualquier lugar del mundo.

Propósito: Facilitar la comunicación y el acceso a dispositivos a través de Internet. Por ejemplo, los servidores web y los sitios de Internet utilizan direcciones IP públicas.

Asignación: Generalmente asignadas por proveedores de servicios de Internet (ISP).

IP Privada

- Una dirección IP privada es una dirección asignada a dispositivos dentro de una red local (LAN). No es accesible directamente desde Internet.

- **Propósito**: Facilitar la comunicación dentro de redes locales, como en hogares, oficinas y empresas.

- **Rangos**:
- **Clase A**: 10.0.0.0 - 10.255.255.255
- **Clase B**: 172.16.0.0 - 172.31.255.255
- **Clase C**: 192.168.0.0 - 192.168.255.255

Diferencias

Pública

- Accesible desde cualquier parte de Internet.
- Más susceptible a ataques ya que es accesible públicamente.
- Usada por servidores web, routers con conexión directa a Internet, etc.

Privada

- Solo accesible dentro de la red local.
- Más segura al estar oculta de Internet y tras un firewall.
- Usada por dispositivos internos como computadoras, impresoras, smartphones, etc.

04

NAT (Network Address Translation)

NAT

(Network Address Translation):

Es una tecnología que permite a múltiples dispositivos en una red local con IPs privadas compartir una única IP pública para acceder a Internet.

Esto ayuda a conservar el espacio de direcciones IPv4 y añade una capa adicional de seguridad.