Filtrado de paquetes

Alberto Molina

@alberto_molina

¿Qué es y para qué se usa?

- Técnica que permite analizar el tráfico de red al atravesar un dispositivo y tomar decisiones acerca del mismo:
  - Permitir el paso
  - Denegar el paso (silenciosamente o no)
  - Modificar el tráfico
  - Seleccionar determinado tráfico para otra aplicación
- Se usa por seguridad, para controlar o modificar el tráfico y para mejorar el rendimiento

Ejemplos de filtrado

- Analizamos el tráfico proveniente de un nodo de nuestra red que está provocando problemas
- Bloqueamos el tráfico de un nodo de Internet que está atacando nuestra red
- Bloqueamos el tráfico web desde una dirección IP que está haciendo descargas masivas ocasionando la ralentización del tráfico del resto de usuarios
- Permitimos la respuesta de ping desde el exterior solo a un nodo de nuestra red y limitamos la tasa de solicitud a un ritmo máximo de 3 por segundo

Niveles

El filtrado de paquetes puede realizarse utilizando parámetros de las diferentes capas TCP/IP

Filtrado a nivel de enlace

- Utiliza parámetros de la cabecera del nivel de enlace (p. Ej. Ethernet)
- Ejemplo: Filtrar por MAC origen o destino

Filtrado a nivel de red

- Utiliza parámetros de la cabecera del nivel de Internet
- Ejemplo: Filtrar por IP origen o destino

Filtrado a nivel de transporte

- Utiliza parámetros de la cabecera del nivel de transporte
- Ejemplo: Filtrar por puerto UDP origen o destino
- Ejemplo: Filtrar por estado de la conexión TCP

Filtrado a nivel de aplicación

- Utiliza parámetros de la cabecera del nivel de aplicación
- Específico de cada aplicación: DNS, HTTP, FTP, ...
- Ejemplo: Filtrar por nombre de dominio en DNS

Seguimiento de la conexión

- Se registran las conexiones
- Se utilizan los registros para conocer el estado de cada conexión
- Se filtra en función del estado
- Ejemplo: Permitir que entren paquetes que se correspondan a respuestas de peticiones previas