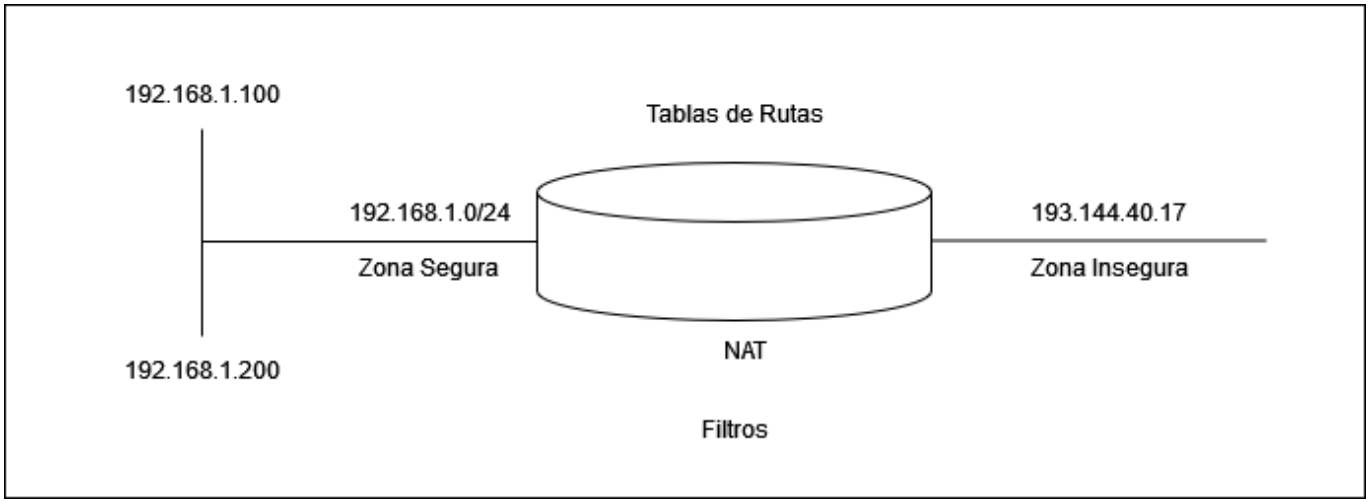
# FireWalls

Dispositivos que filtran tráfico en redes. Toman decisiones de envío en base a su tabla de rutas y aplicando filtros. Permiten aplicar la política de seguridad de la red (Un documento que indica que tráfico se va a proporcionar a las diferentes zonas de la red). Los firewalls pueden operar en cualquier capa excepto presentación y capa física. en este caso nos vamos a centrar en los que operan en capas 3 (Red), 4 (Transporte) y 5 (Sesion). Se pueden usar para filtrar tráfico entre redes con distintos niveles de seguridad o mismo nivel de seguridad. Sobre los firewall se articula la seguridad de una organización.




Ahora existen Next Generatio Firewall que incorporan funcionalidades adicionales sobre los FireWall tradicionales como permitir extraer información de directorio activo y vincular reglas a grupos de usuarios. Los next generation FireWalls tienen un servicio que puede añadir las listas de direcciones IP dinámicamente conectándose al proveedor de servicio para obtener una lista negra.

Ventana de Cambio: Cuando se realiza un cambio que pueda generar corte, se realiza entre las 3:00 am y las 6:00 am. Se usa una tabla como esta:

| TCP | Inside Local | Inside Global | Outside Local | Outside Global |
|---|---|---|---|---|
| tcp | 192.168.1.100:4391 | 193.144.40.17:443 | 8.8.8.8:443 | 8.8.8.8:443 |
| tcp | 192.168.1.200:443 | 193.144.40.17:4443 | - | - |

## Filtrado estático de paquetes

Capas 3 y 4 del modelo OSi. Filtrado en base a características de la cabecera del paquete IP

- Ip de origen
- IP de destino
- Tipo de tráfico(TCP, UDP, ICMP)
- Interfaz de red por la que llega o se envía.

Se dirige por un conjunto de reglas como por ejemplo:

- Sentido del paquete: Entrada/Salida
- Dirección IP de origen/destino, tipo de tráfico, puerto, etc..

Se pueden realizar múltiples acciones:

- Aceptar: El paquete pasa el firewall
- Denegar: El paquete se descarta y se notifica al origen
- Descartar: El paquete se descarta sin informar al orgien

From:
https://knoppia.net/ - **Knoppia**

Permanent link:
**https://knoppia.net/doku.php?id=redes:ids_ips&rev=1731085372**

Last update: **2024/11/08 17:02**