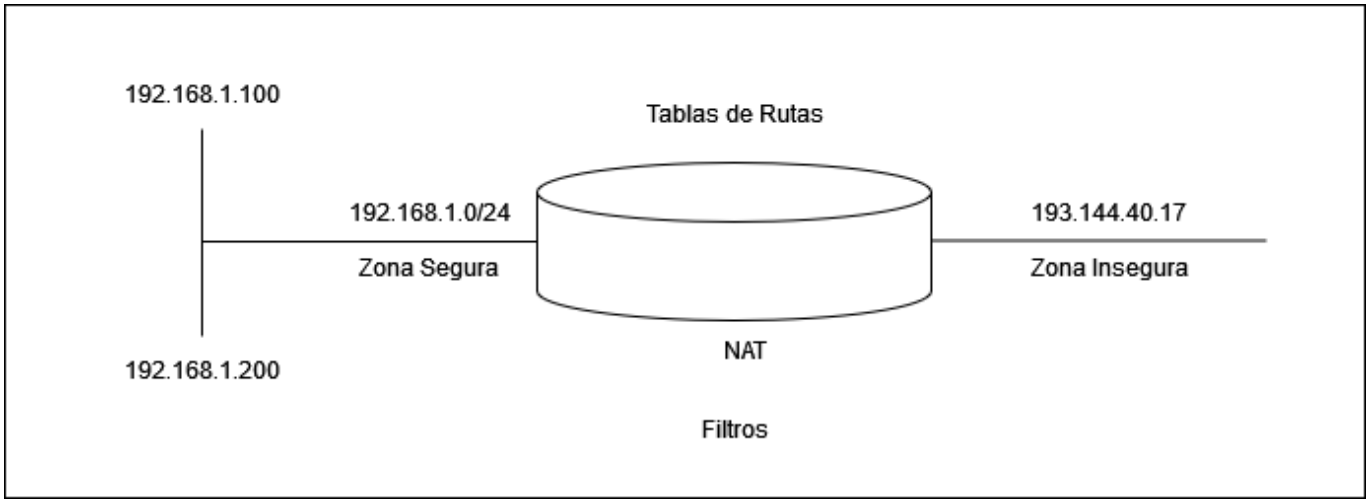
# FireWalls

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

# Limitaciones en Firewalls y filtrado de paquetes

Los firewalls tienen ciertas limitaciones que son difíciles de solventar. Por ejemplo, si tenemos un servidor ftp, se usa una conexión para intercambiar comandos. El cliente le dice al servidor en que puerto espera una conexión desde el servidor con el comando port. El cliente inicia la conexión al puerto 21, el firewall analiza el paquete, como este es un paquete autorizado, se establece una conexión en la tabla de conexiones y cuando vuelve el tráfico de vuelta se crea la conexión creada para aceptar este tráfico. cuando se establece una conexión de datos no hay una conexión abierta. Esto no puede ser controlado por un firewall. Esto no solo pasa con FTP, puede pasar con VoIP y otros muchos protocolos.

Tenemos un problema con los protocolos y conexiones derivadas. También hay problemas con vulnerabilidades en la capa de Aplicación. No se puede diferenciar entre peticiones legítimas e ilegítimas. Otra limitación de este tipo de firewall es que filtran por IP pero no por usuario. En caso de IP spoofing el firewall no puede hacer gran cosa a menos que se use unicast reverse path forwarding (Que es una técnica muy agresiva).

Para evitar ataques en capa de aplicación (SQL Inyection, XSS, etc...) existe la posibilidad de usar firewalls de capa de aplicación o proxys inversos que abren las peticiones, analizan el contenido y si es válido se pasa e IDS/IP. También existen los descifradores IDS que se usan con IDS/IP

En resumidas cuentas, para los siguientes problemas hay las siguientes soluciones:

1. Conexiones derivadas → SOLUCIÓN: Firewall de capa de aplicación
2. Vulnerabilidades en capa de aplicación → SOLUCIÓN: Firewall de cpa de aplicación, Proxys e IDS/IPS
3. Filtrado por IP y no por Usuario → SOLUCIÓN: Proxy, 802.1x, lo que nos da capacidad de auditoría o login más avanzado.
4. IP Spooging

# Filtrado de capa de aplicación (Firewall de aplicación)

Los firewalls de capa de aplicación van a examinar el contenido del paquete, no solo las cabeceras IP y de capa 4. Esto trata de mitigar los problemas vistos con las conexiones derivadas y algunos protocolos. Permite detectar tráfico de malware y ciertos tipos de ataque como XSS y SQL Injection, además de algunos tipos de contenidos como mecanismos de propagación de virus brutal (Algo anticuado ya que solía pasar por flash).