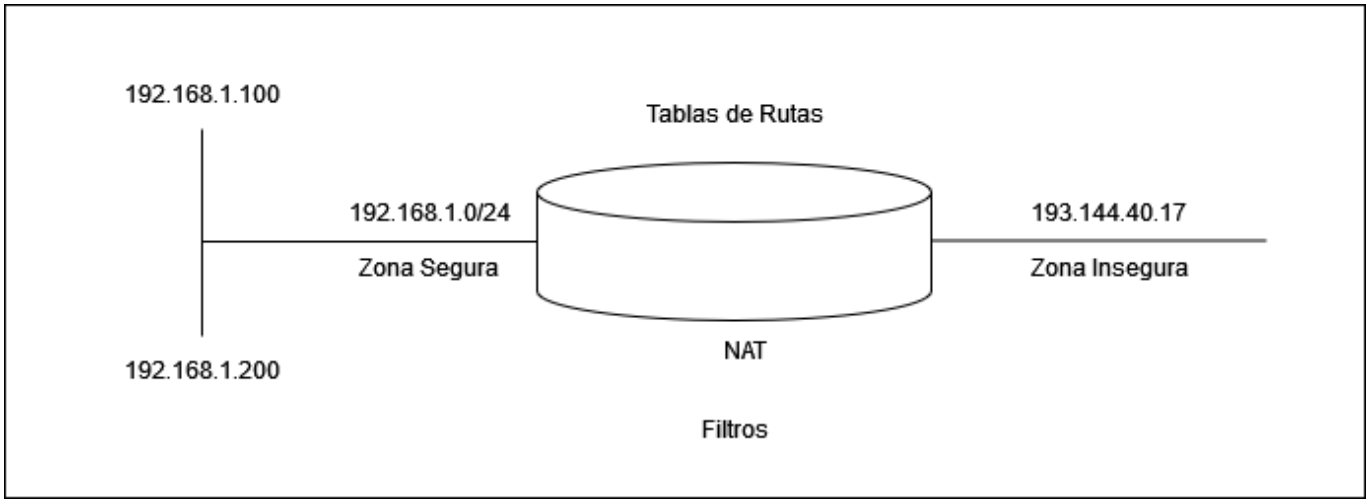
FireWalls

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). Una de las razones por las que la API REST ha triunfado es por que es más fácil de analizar y filtrar. Estos firewalls permiten generar más información de login detallada ya que generan logs por aplicación y son capaces de saber, identificar y asociar protocolos con los puertos que utilizan. De todas formas estos firewalls también tienen limitaciones.

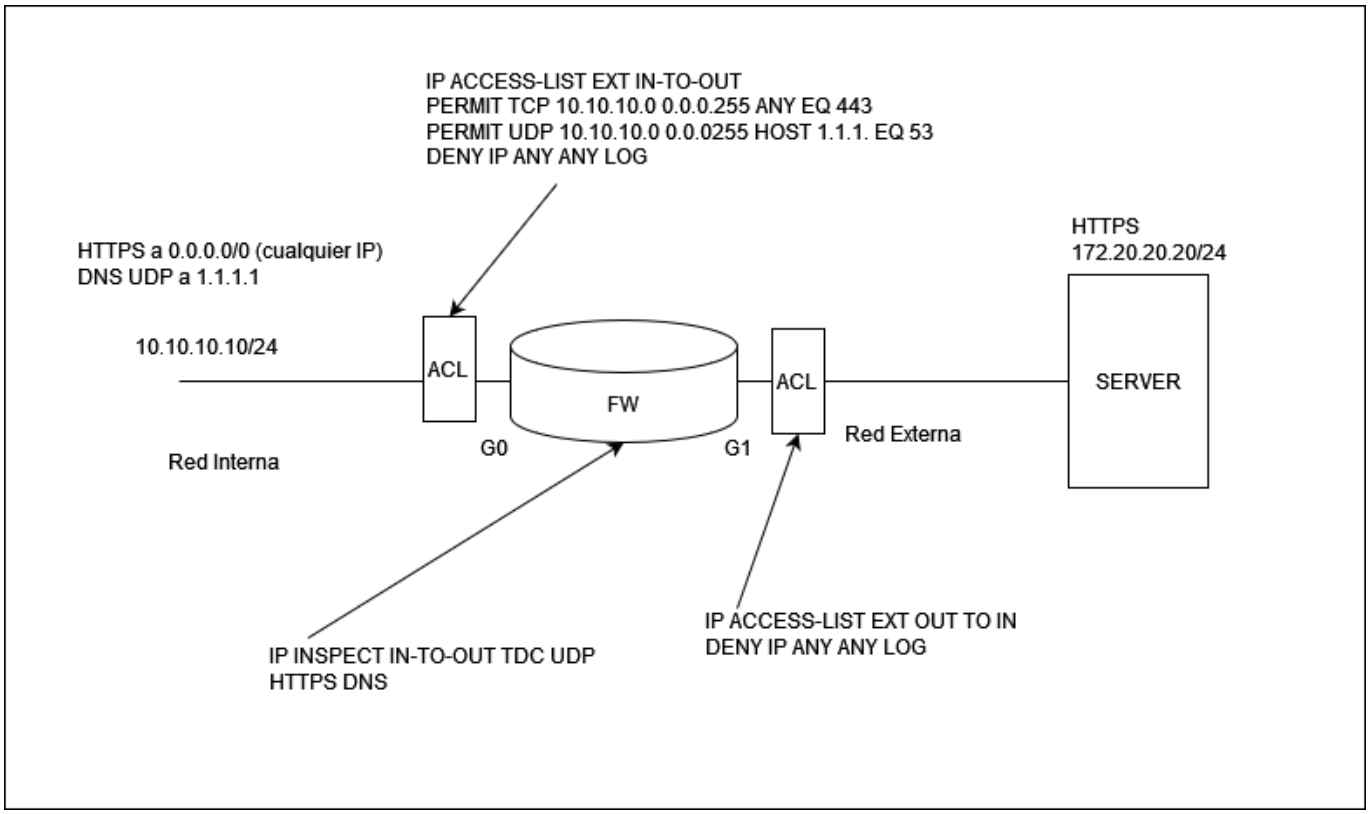
Se necesita mucho esfuerzo para analizar el tráfico de los firewall de aplicación. Este tipo de firewall tienen procesadores específicos para analizar cada tipo de tráfico de aplicación. Otro problema es que

no soportan protocolos nuevos ni propietarios, solo soportan protocolos estándar. Pueden provocar cuellos de botella, para evitar esto, delante de los firewalls de aplicación hay que meter otros equipos para prevenir sobrecarga. Estos firewall tampoco pueden gestionar tráfico por usuarios.

Los Firewalls Next Generation aglutinan muchas funcionalidades de seguridad siendo estas:

- firewall de capa de aplicación
- Proxy
- IPS
- Concentrador de VPNs

El problema de estos firewalls es que son excesivamente caros. Para implementar el filtrado a nivel de capa de aplicación en nuestros routers tanto la gestión dinámica de aplicaciones como el filtrado dinámico se usa Context Based Access Control en routers cisco como los ISR2 y posteriores. Puede controlar tráfico UDP y TCP entrante y saliente. Si tenemos un firewall, una red interna y una red externa:



Se establecen dos ACL, una de entrada y otra de salida que filtren el tráfico de entrada y salida, mientras que el firewall inspecciona el tráfico TCP y UDC con peticiones HTTPS y DNS.

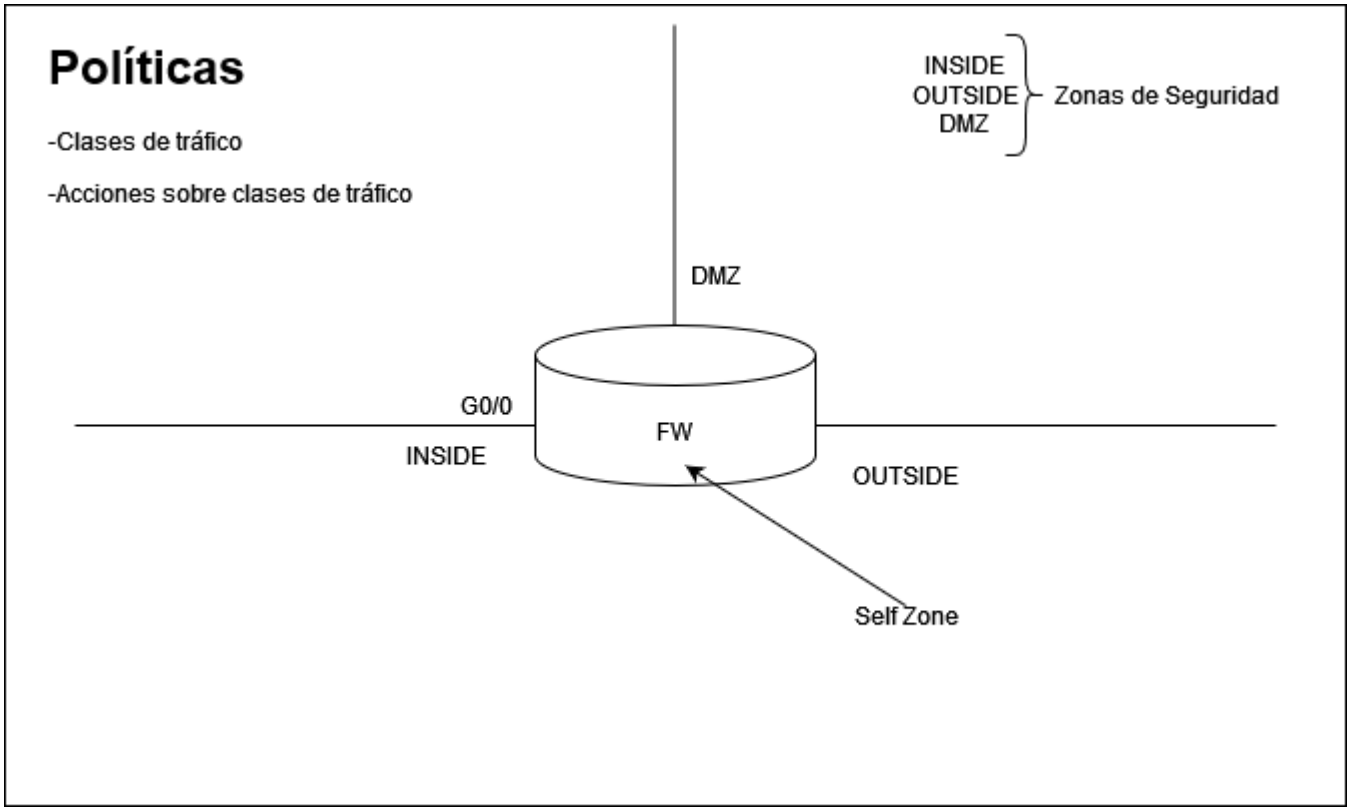
Tipos de Firewalls de filtrado

- Filtrado de paquetes sin estado: simples y eficientes, pero no gestionan conexiones ni evitan ataques en capa de aplicación
- Filtrado de paquetes con estado: Eficientes, permiten controlar la mayor parte de paquetes de capa de aplicación. No evitan ataques a nivel de capa de aplicación, sin autenticación.
- Filtrado a nivel de aplicación: Mejor control de conexiones, evitan ciertos ataques a nivel de aplicación. Menor rendimiento, soporte de protocolos limitado, sin autenticación de usuarios.

Zone Based Firewall (ZBFW)

La configuración de firewall basada en zonas no se suele usar y en su lugar se usan ACL y CBAC, por que se ajusta mejor a redes de gran tamaño. Tiene un enfoque donde se tiene una perspectiva diferente a la hora de configurar el firewall. Antes de hacer configuración de ZBFW se recomienda hacer una copia de seguridad del equipo. En ZBFW se definen parejas de interfaces. Normalmente tenemos una red interna, una externa y una DMZ. Se definen relaciones entre pares de zonas como INSIDE → DMZ, INSIDE → OUTSIDE, DMZ → INSIDE, DMZ → OUTSIDE, OUTSIDE → INSIDE o OUTSIDE → DMZ. Se definen formas de seguridad con estos pares y a estas se les aplican políticas. Las políticas siguen la estructura:

- Clase de tráfico
- Acciones a aplicar sobre dicha clase de tráfico.



Por defecto, las interfaces pertenecen a la zona por defecto, excepto el que va dirigido a las interfaces del router, que se clasifican como self-zone. Las interfaces que pertenecen a la misma zona de seguridad pueden intercambiar tráfico mientras las que no, no pueden a menos que se implemente en una política de tráfico.

- Self Zone: Incluye todas las IPs del router, por defecto permiten el tráfico.
- Default Zone: Zona de sistema que incluye todas las interfaces que no son miembros de una zona de seguridad (Todas las interfaces pertenecen a esta por defecto)

Para definir una zona de seguridad se usa el siguiente comando:

```
zone security OUTSIDE
zone security DMZ
zone security OUTSIDE
```

Creamos una ACL para crear construir dos clases de tráfico:

```
ip access-list extended ACL-PING-AND-TRACEROUTE //ACL 1
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any ttl-exceeded
permit icmp any any port-unreachable
permit icmp any any range 33434 33463 ttl eq 1

ip access-list extend ACL-DHCP-IN //ACL 2
permit udp any eq bootps any eq bootpc

//Definición de clase de tráfico de la red outside a la self-zone
class-map type inspect match-any CLASS-OUTSIDE-TO-SELF-PASS
match access-group name ACL-PING-AND-TRACEROUTE
match access-group name ACL-DHCP-IN
```

Con esta clase de tráfico se define todo el tipo de tráfico que puede pasar. Se crearan clases de tráfico que van a ser utilizadas para inspeccionar de OUTSIDE a Self ZONE. Una vez creada la clase de tráfico se deben crear las acciones:

```
policy-map type inspect POLICY-OUTSIDE-TO-SEFL
  class type inspect CLASS-OUTSIDE-TO-SELF-PASS //clase
    pass //acción
  class class-default //clase
    drop //acción
```

Traducción de direcciones (NAT)

En la práctica esto se hace en el CPE ya que es donde se cambia de direcciones privadas a direcciones públicas. Se debe conocer la configuración tanto de PAT dinámico como de PAT estático. PAT con mecanismo dinámico de sobrecarga. PAT, también conocido como NAT con sobrecarga se usa para una OP pública y se usa en entornos firewall y a veces en ámbito doméstico. Tenemos los siguientes tipos de nat:

- NAT estático: Cada ip privada tiene asociada una pública
- NAT Dinámico: Conexiones basadas en un pool de direcciones públicas
- Port Address Translation (PAT)

El funcionamiento de PAT consiste en que se tiene un equipo interno con una ip interna y un equipo con un PAT la convierte en una IP pública cuando se intenta realizar una conexión externa. El firewall genera una entrada en su tabal NAT donde asigna IP privada y purto público, de forma que cuando el tráfico retorna, viene por el puerto que se ha asignado en la IP pública y se deshace el mensaje de traducción. Si se quiere abrir un puerto o mapear un puerto, es un proceso estático donde se definen puerto interno y externo para el tráfico. En entornos corporativos en vez de usar la IP pública de la dirección externa, se asignan rangos de IP públicas para servicios externos. Para ello se definen un rango de IPs privadas, otro de IPs públicas y se vinculan.