Firewall

Firewall

- La seguridad ha sido uno de los principales temas a tratar cuando una organización desea conectar su red privada a Internet.
- Datos y servicios se deben proteger de personas maliciosas.
- La organización necesita seguir una política de seguridad para prevenir el acceso no-autorizado de usuarios a los recursos propios de la red privada, y protegerse contra la exportación privada de información.

Definición de Firewall

- Un Firewall es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada e Internet.
- El firewall determina quién puede utilizar los recursos de red pertenecientes a la organización.
- Para que un firewall sea efectivo, todo trafico de información a través de Internet deberá pasar a través de él, donde podrá ser inspeccionada la información.

Tipos

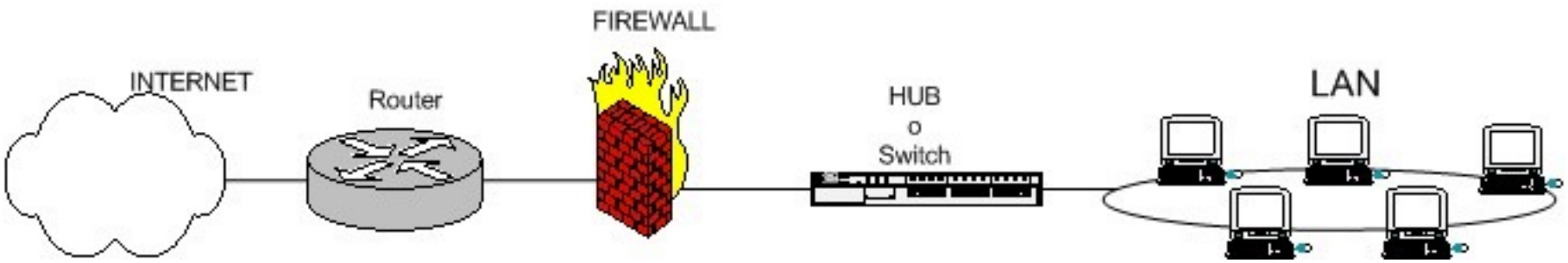
- **Filtrado de paquetes a nivel del sistema operativo**. Se verifican las capas 3 y 4. Filtra paquetes dependiendo de la información del encabezado del paquete IP y de la unidad de datos de transporte.

- **Gateways a nivel de aplicación**. Generalmente son host con servidores proxy, que no permiten el trafico directamente entre dos redes, sino que realizan un seguimiento detallado del trafico que pasa por el.

Tipos

- **Hardware.** Dispositivo físico (host) con un sistema operativo especial (reducido) que posee dos o más interfaces de red y en el cual se implementan las directivas de seguridad de la red. Generalmente el equipo, posee una interfaz gráfica (GUI) para la configuración de las reglas de manera remota.
- **Software**. Programa especial que se instala en un servidor para la implementación de las directivas de seguridad de la red. Las reglas de seguridad se pueden configurar usando una interfaz gráfica o la línea de comandos (shell script). Además, el programa se puede configurar como un servicio.

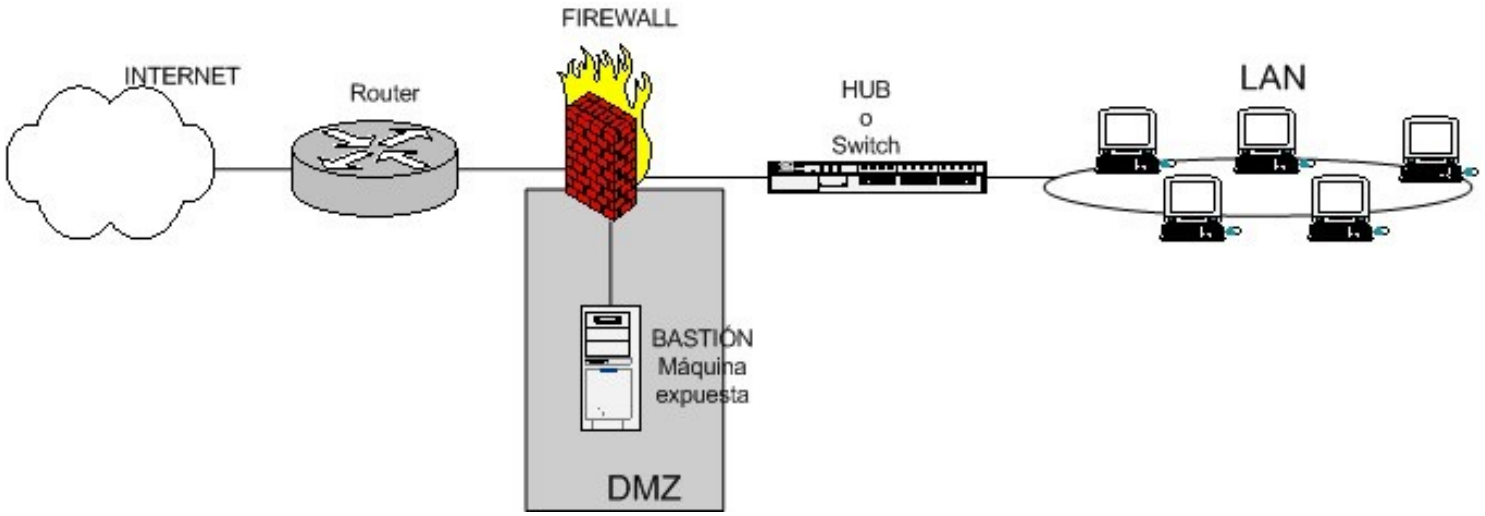
Ejemplo Configuración 1



Esquema típico de firewall para proteger una red local conectada a internet a través de un router.

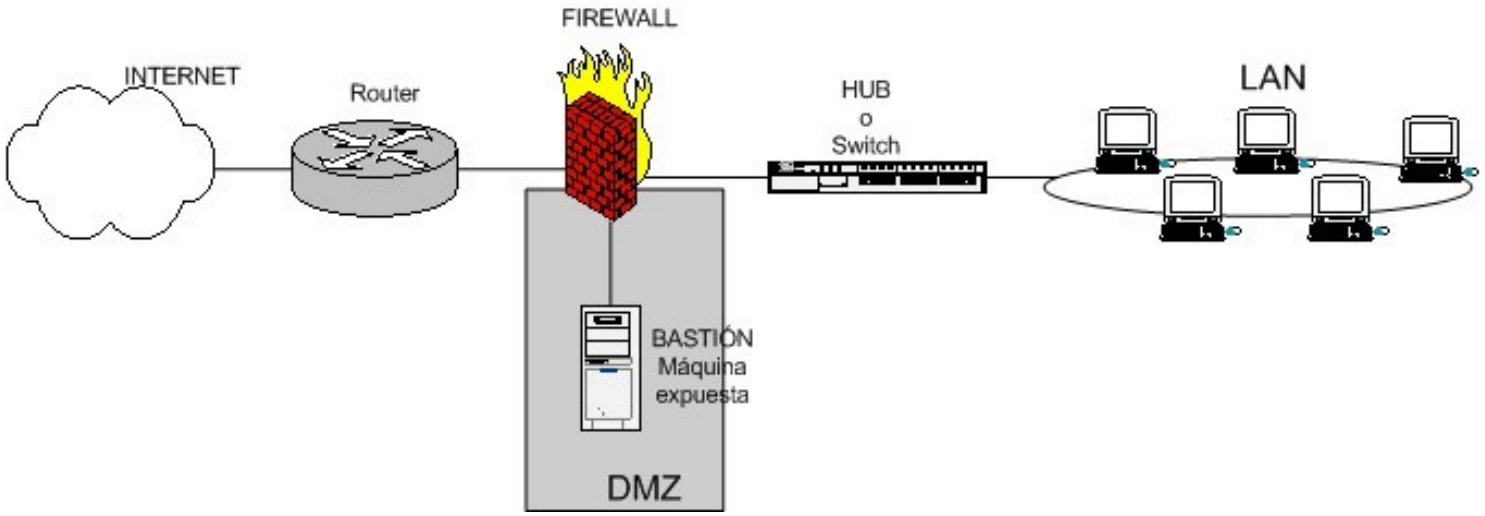
El firewall debe colocarse entre el router y la red local (conectado al switch de la LAN)

Ejemplo Configuración 2



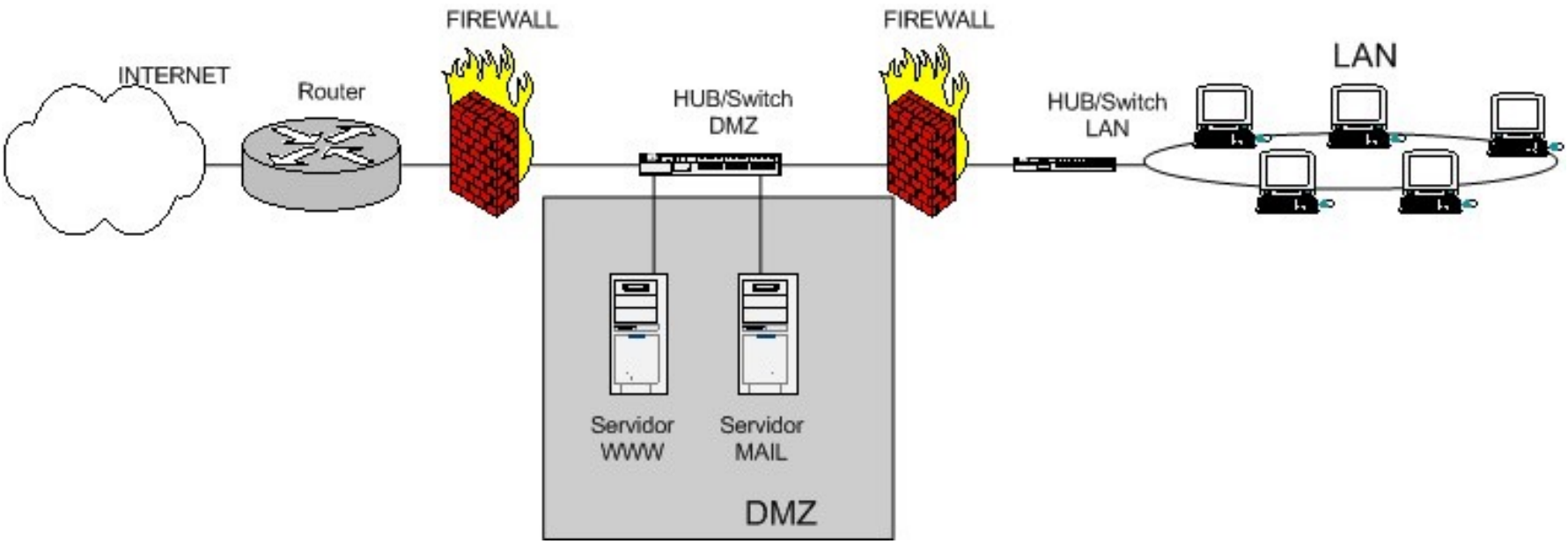
Es frecuente también que se necesite exponer algún servidor a internet (como es el caso de un servidor web, un servidor de correo, etc..), y en esos casos en principio se debe aceptar cualquier conexión a ellos.

Ejemplo Configuración 2



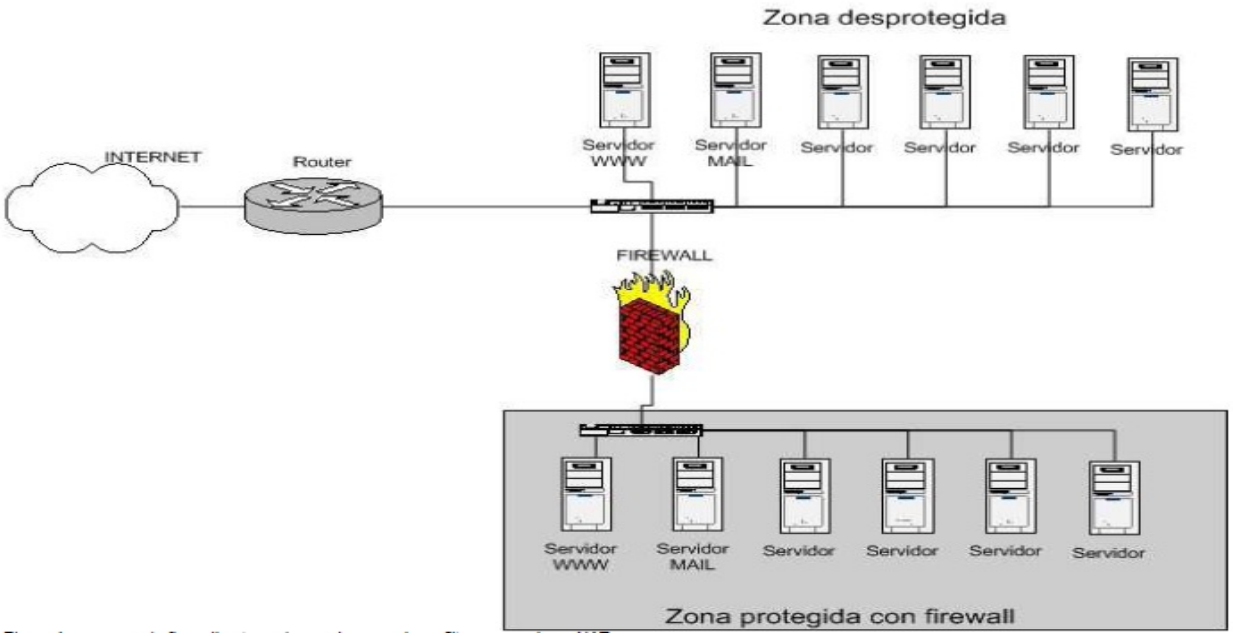
- Lo que se recomienda en esa situación es situar ese servidor en lugar aparte de la red, el que denominamos DMZ o zona desmilitarizada.
- El firewall debe tener tres entradas

Ejemplo Configuración 3



- Esta estructura de DMZ puede hacerse también con un doble firewall

Ejemplo Configuración 4



- Esta estructura permite proteger una parte de la red nada mas, se tendrán dos zonas, una protegida y otra no

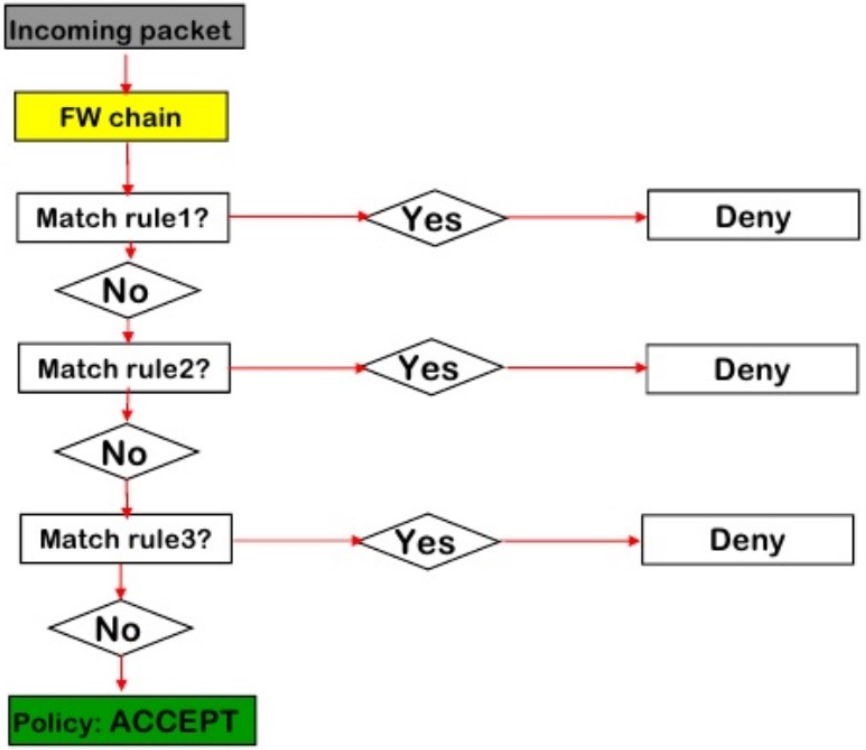
Funcionamiento

- El filtrado de paquetes se realiza en las capas de red y de transporte del modelo TCP/IP.
- Las reglas del firewall utilizan los campos de encabezado de los paquetes, para decidir si se enruta el paquete hacia su destino, se elimina o se descarta y se devuelve un mensaje de error al host origen de la petición.
- Las reglas del firewall se basan en aspectos como la interfaz de red especifica, la IP del host, las direcciones IP origen y destino, los puertos (UDP y TCP), los indicadores de conexión, y el tipo de paquete (entrante o saliente).
- Las listas de reglas que filtran lo que entra o sale se denominan **cadenas**, ya que cada paquete se compara con cada una de la reglas hasta que se encuentra una coincidencia o la lista se termina.

Políticas

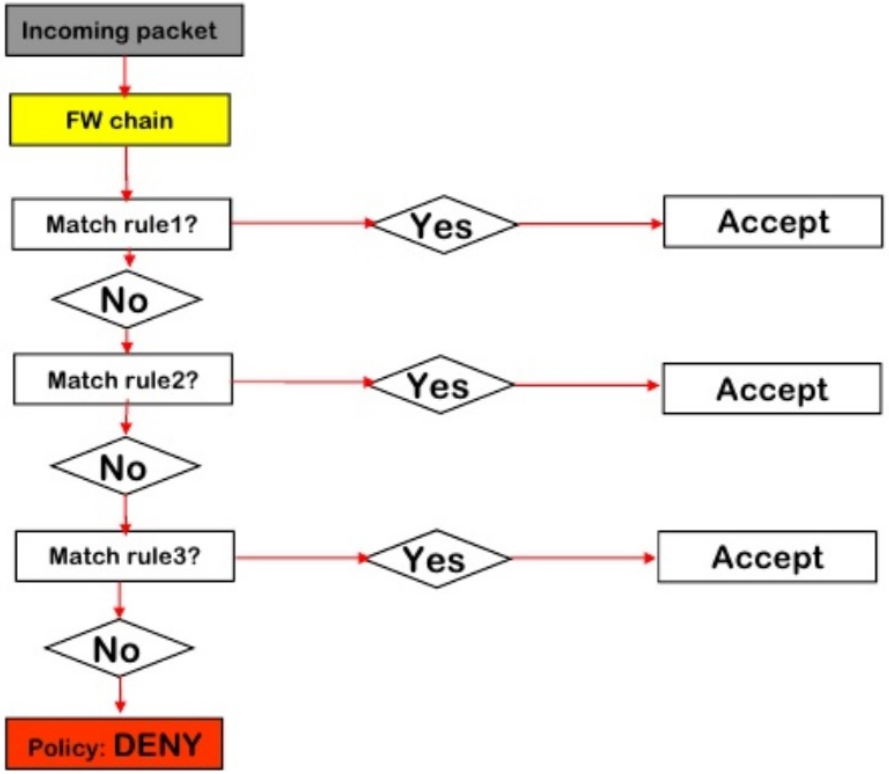
- Hay dos maneras de implementar un firewall:
  - Política por defecto ACEPTAR: en principio todo lo que entra y sale por el firewall se acepta y solo se denegará lo que se diga explícitamente.
  - Política por defecto DENEGAR: todo esta denegado, y solo se permitirá pasar por el firewall aquellos que se permita explícitamente.

Aceptar todo por defecto



Fuente: https://www.slideshare.net/rajakhurram/lecture-4-firewalls

Denegar todo por defecto



Fuente: https://www.slideshare.net/rajakhurram/lecture-4-firewalls

Políticas

- El orden en el que se ponen las reglas de firewall es determinante.
  - Normalmente cuando hay que decidir que se hace con un paquete se va comparando con cada regla del firewall hasta que se encuentra una que le afecta (match)
  - Se hace lo que dicte esta regla (aceptar o denegar); después de eso NO SE MIRARÁN MÁS REGLAS para ese paquete

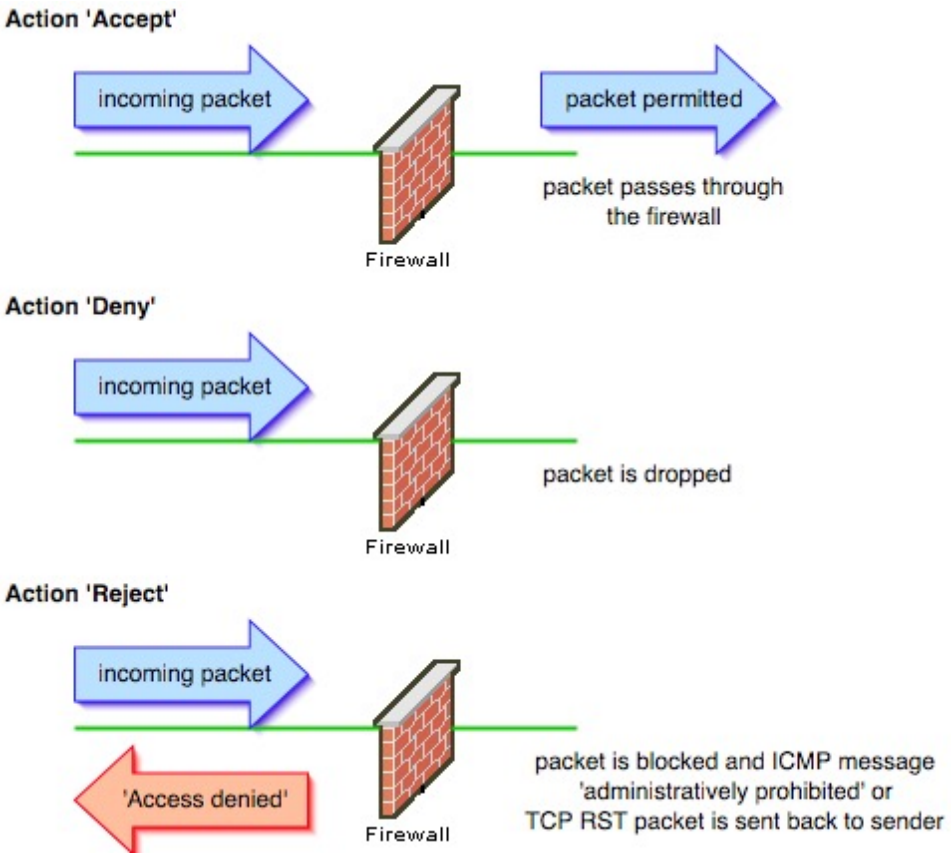
Rechazar vs Denegar

- La mayoría de los Firewall actuales ofrecen la posibilidad de “rechazar” o ”denegar” paquetes.

- La diferencia entre estas 2 opciones es la siguiente:
  - Rechazar (REJECT) - cuando se rechaza un paquete, este se descarta y se devuelve un mensaje de error utilizando ICMP al remitente.
  - Denegar (DENY) – se descarta el paquete, pero en este caso no hay ningún tipo de notificación al remitente.

- Se recomienda denegar en vez de rechazar, ya que éste último genera más tráfico en la red, además es mas seguro ya que si se trata de un ataque el atacante no tendrá la seguridad de la existencia el servicio.

Rechazar vs Denegar



iptables

- Es un programa para la implementación de Firewall que se utilizan en plataformas UNIX/Linux y que se distribuye bajo licencia GPL.
- Su ventaja es que está presente en casi todas las distribuciones de Linux y se integra al kernel (desde el kernel 2.4).
- La implementación de las reglas del Firewall se puede realizar desde la línea de comandos de manera sencilla, o por medio de programas de más alto nivel que facilitan la configuración por ejemplo con shorewall o mas recientemente con Firewalld

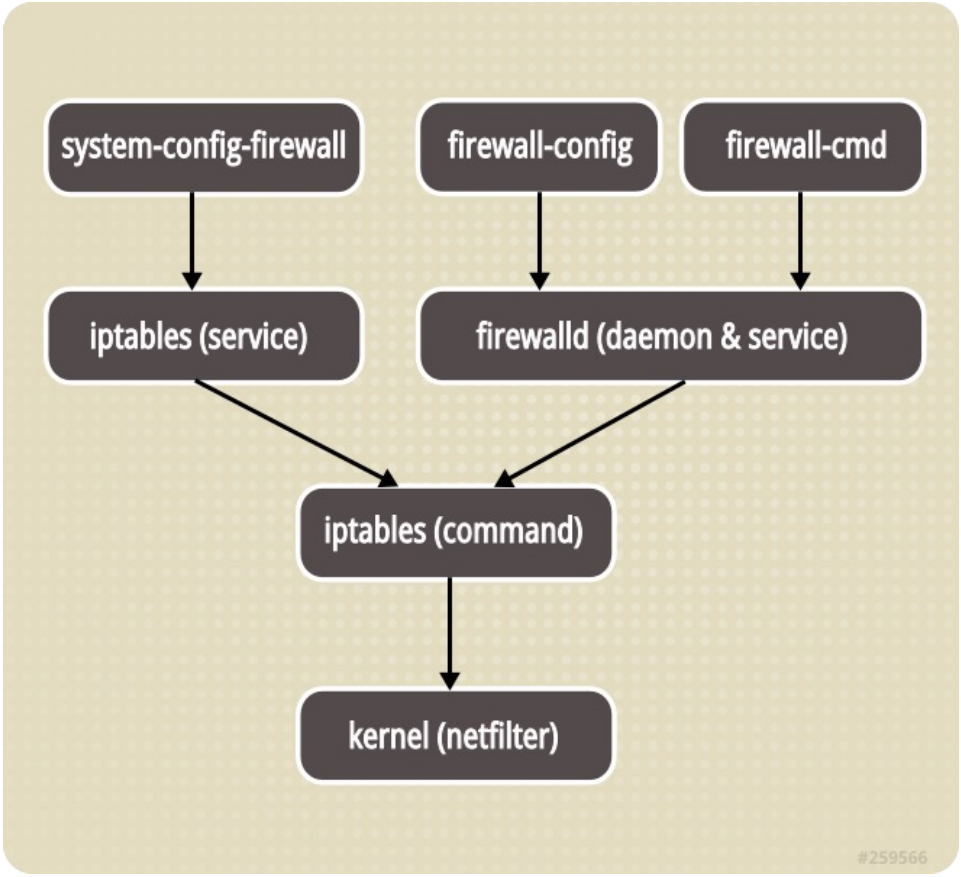
Firewalld

- Controlador de Frontend para iptables
- Tiene soporte para IPv4 e IPv6
- Separa reglas de ejecucion (runtime) de las reglas permanentes
  - No es necesario reiniciar el servicio cuando se configuran reglas de runtime
  - Las reglas de runtime permiten hacer evaluaciones y tests en caliente
  - La configuración de runtime es valida solo hasta la próxima vez que se reinicie el sistema o el servicio

Quien usa Firewalld?

- Es usado en las siguientes distribuciones Linux como herramienta de manejo de firewall por defecto:
  - Red Hat Enterprise Linux (RHEL) 7, Centos 7 y superior
  - Fedora 18 y superior
  - Disponible para otras distribuciones

Stack del Firewall



Instalación de Firewalld

Para iniciar el servicio y habilitar FirewallD durante el inicio del sistema

```
service firewalld start

chkconfig firewalld on
```

Detener y deshabilitar el servicio

```
service firewalld stop

chkconfig firewalld off
```

Verificación del estado del servicio

```
firewall-cmd --state
```

Verificación del estado del servicio

- Ver el estado del demonio de FirewallD

```
service firewalld status
```

- El resultado es similar al siguiente

```
firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor
    preset: enabled)
   Active: active (running) since Mon 2017-07-31 15:54:09 UTC; 4min 33s ago
     Docs: man:firewalld(1)
 Main PID: 2940 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─2940 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid
```

Recargar una configuración

- El comando reload se usa para eliminar todas las configuraciones de runtime y aplicar una configuración permanente

```
firewall-cmd --reload
```

Configuración de Firewalld

- Se realiza a través de archivos XML.
  - Excepto para configuraciones muy especificas no es necesario manipularlos. En su lugar debe usar firewall-cmd para realizar las configuraciones deseadas.
- Los archivos de configuración se ubican en dos directorios:
  - /usr/lib/firewalld contiene las configuraciones por defecto como zonas y servicios comunes. Debe evitar manipular directamente estos archivos ya que estos se sobreescriben durante actualizaciones del paquete firewalld.
  - /etc/firewalld contiene archivos de configuración del sistema.

Conjuntos de Configuración

- FirewallD usa dos conjuntos de configuración (configuration sets): reglas de tiempo de ejecución y reglas permanentes.
  - Las configuraciones de tiempo de ejecución no son retenidas cuando se realiza un reinicio del sistema o cuando se reinicia el proceso de FirewallD.
  - Los cambios permanentes no se aplican al sistema que está en ejecución
- Los comandos firewall-cmd se aplican a la configuración actualmente en ejecución. Mediante el uso de la bandera --permanent se hace persistente la configuración

Activar reglas de forma permanente

- Se pueden usar los siguientes métodos para activar una regla de forma permanente
  - Agregar la regla a la configuración en ejecución y a la configuración permanente

```
firewall-cmd --zone=public --add-service=http --permanent
firewall-cmd --zone=public --add-service=http
```

  - Agregar la regla de manera permanente y realizar un reload

```
firewall-cmd --zone=public --add-service=http --permanent
firewall-cmd --reload
```

Zonas del Firewall

- Las zonas son conjuntos de reglas previamente construidas para varios niveles de confianza. Ejemplos de zonas son: home, public, trusted, etc.

- Estas zonas se deben usar de acuerdo al nivel de confianza que se tenga para un escenario dado:
  - diferentes zonas permiten diferentes servicios de red y tráfico de entrada, mientras deniegan otro trafico entrante.
  - La zona por defecto después de habilitar Firewalld por primera vez es “public”.

Zonas del Firewall

- Las zonas se pueden aplicar a diferentes interfaces de red.
  - Por ejemplo, con interfaces separadas para la intranet e internet:
    - se puede permitir DHCP para una zona interna
    - … pero solo http y SSH para la zona externa.

- Cualquier interfaz que no se configure para una zona explícitamente se configurara para la zona por defecto.

Gestión de Zonas

- Ver la zona por defecto

```
firewall-cmd --get-default-zone
```

- Cambiar la zona por defecto

```
firewall-cmd --set-default-zone=internal
```

Gestión de Zonas

- Para ver las zonas

  ```
  firewall-cmd –-get-zones
  ```

- Ver Configuraciones de todas las zonas

  ```
  firewall-cmd --list-all-zones
  ```

- Ver las zonas usadas por sus interfaces de red:

  ```
  firewall-cmd --get-active-zones
  ```

- La salida del anterior comando puede ser por ejemplo:

  ```
  public
      interfaces: eth0 eth1
  ```

Gestión de Zonas

- Ver todas las configuraciones de una zona especifica

```
firewall-cmd --zone=public --list-all
```

- Ejemplo de salida:

```
public (default, active)
        interfaces: ens160
        sources:
        services: dhcpv6-client http ssh
        ports: 12345/tcp
        masquerade: no
        forward-ports:
        icmp-blocks:
        rich rules:
```

Gestión de Zonas

- Asociar una interfaz a una zona:

```
firewall-cmd --zone=dmz --add-interface=enp0s8
```

Servicios

- Firewalld puede permitir tráfico basado en reglas predefinidas para servicios específicos.
- Puede crear sus propias reglas para servicios y agregarlas a cualquier zona.
- Los archivos de configuración para los servicios soportados se encuentran en /usr/lib/firewalld/services.
- Los archivos de servicios creados por los usuarios se encuentran en /etc/firewalld/services.

Habilitar Servicios

- Para ver los servicios disponibles por defecto ejecutar:

```
firewall-cmd --get-services
```

- Como ejemplo, los siguientes comandos permiten habilitar o deshabilitar el servicio de http:

```
firewall-cmd --zone=public --add-service=http --permanent

firewall-cmd --zone=public --remove-service=http --permanent
```

Bloquear ICMP

- Obtener una lista de los tipos ICMP soportados

```
firewall-cmd --get-icmptypes
```

- Los siguientes comandos permiten verificar si los mensajes icmp estan habilitados o deshabilitados en la zona publica:

```
firewall-cmd --zone=public --query-icmp-block=echo-reply
firewall-cmd --zone=public --query-icmp-block=echo-request
```

- Investigue como deshabilitarlos, habilitarlos

Permitir o denegar puertos

Como ejemplo, se puede permitir o deshabilitar el trafico TCP sobre el puerto 12345 con los siguientes comandos:

```
firewall-cmd --zone=public --add-port=12345/tcp --
permanent
```

```
firewall-cmd --zone=public --remove-port=12345/tcp --
permanent
```

Reenvió de Puertos

El siguiente ejemplo reenvía el trafico del puerto 80 al puerto 12345 en el mismo servidor

```
firewall-cmd --zone="public" --add-forward-port=port=80:proto=tcp:toport=12345
```

Reenvió de Puertos hacia otro servidor

- Active el enmascaramiento en la zona deseada

```
firewall-cmd --zone=public --add-masquerade
```

- Agregue la regla de reenvío. Este ejemplo reenvia trafico desde el puerto local 80 hacia el puerto 8080 en un servidor remoto localizado en la dirección 192.168.0.4

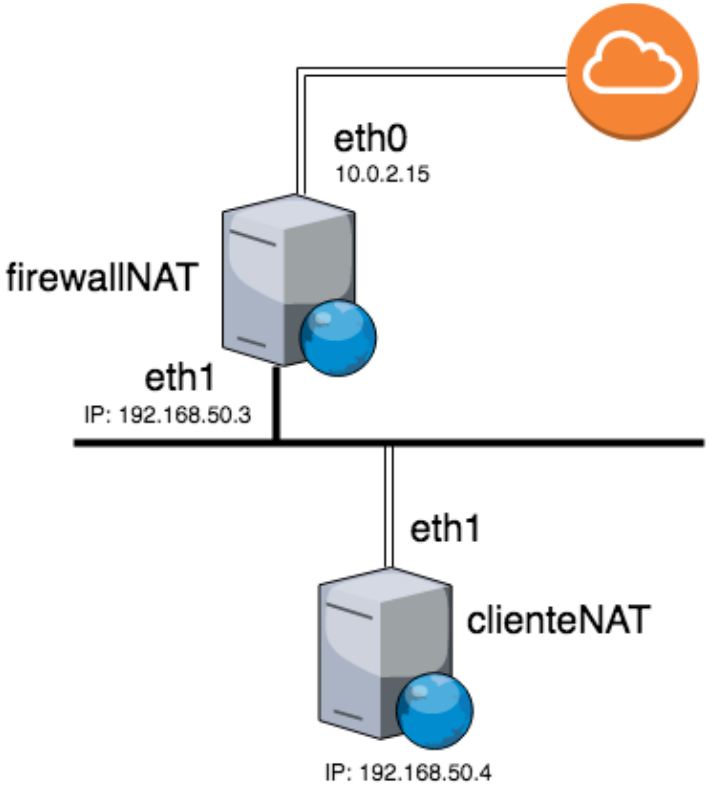
```
firewall-cmd --zone="public" --add-forward-
   port=port=80:proto=tcp:toport=80:toaddr=192.168.0.4
```

Remover reglas

- Para remover reglas, usar `--remove`. Por ejemplo:

```
firewall-cmd --zone=public --remove-masquerade
```

Caso de Uso: Permitir que el Firewall se comporte como NAT



Caso de Uso

Vagrantfile

- Se sugiere un Vagrantfile como el siguiente

```
Vagrant.configure("2") do |config|

  config.vm.define :clienteNAT do |clienteNAT|
    clienteNAT.vm.box = "bento/stream8"
    clienteNAT.vm.network :private_network, ip: "192.168.50.4"
    clienteNAT.vm.hostname = "clienteNAT"
  end

  config.vm.define :firewallNAT do |firewallNAT|
    firewallNAT.vm.box = "bento/stream8"
    firewallNAT.vm.network :private_network, ip: "192.168.50.3"
    firewallNAT.vm.hostname = "firewallNAT"
  end
end
```

Caso de Uso

SELINUX

- Security-Enhanced Linux (SELinux): modulo de seguridad del Kernel que provee mecanismos para soportar políticas de seguridad para control de acceso

- Verificar estado del servicio

```
[vagrant@servidorTest ~]$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          permissive
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28
[vagrant@servidorTest ~]$
```

Caso de Uso

Deshabilitar SELINUX en el Servidor

```
[vagrant@servidorTest ~]$ sudo vim /etc/selinux/config
```

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

```
[vagrant@servidorTest ~]$ reboot
```

Caso de Uso

Permitir el reenvío de paquetes

- Para eso se debe modificar el archivo **/etc/sysctl.conf** se debe añadir en el servidor:

```
net.ipv4.ip_forward = 1
```

- Para comprobar, ejecutar el comando

```
sysctl -p
```

Caso de Uso

Definir Zonas

- Zona internal, para la interfaz que va con la red privada eth1
- Zona public, para la interfaz que va con la red publica eth0

```
firewall-cmd  --zone=public --remove-interface=eth1
firewall-cmd  --zone=internal --add-interface=eth1
```

Caso de Uso

Comprobar Zonas

```
# firewall-cmd --get-active-zones
internal
  interfaces: eth1
public
  interfaces: eth0
```

Caso de Uso

Definir reglas del NAT

```
firewall-cmd --direct --add-rule ipv4 nat POSTROUTING 0 -o
eth0 -j MASQUERADE

firewall-cmd --direct --add-rule ipv4 filter FORWARD 0 -i
eth1 -o eth0 -j ACCEPT

firewall-cmd --direct --add-rule ipv4 filter FORWARD 0 -i
eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Caso de Uso

Añadir servicios a las zonas

```
firewall-cmd --zone=public --add-service=http
firewall-cmd --zone=public --add-service=https
firewall-cmd --zone=public --add-service=dns

firewall-cmd --zone=internal --add-service=http
firewall-cmd --zone=internal --add-service=https
firewall-cmd --zone=internal --add-service=dns
```

Caso de Uso

Puerta de Enlace en Clientes

- Configurar la puerta de enlace de los equipos de la red interna.
- La puerta de enlace será la dirección del firewall.
- Agregar

GATEWAY=192.168.50.3 a /etc/sysconfig/network

- Reiniciar el servicio de network service network restart
- En Centos 8: reboot

Caso de Uso

Verificación desde el cliente

- Verificación del gateway

```
[root@clienteNAT ~]# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.50.3    0.0.0.0         UG        0 0          0 eth1
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 eth1
192.168.50.0    0.0.0.0         255.255.255.0   U         0 0          0 eth1
```

Caso de Uso

Verificación desde el cliente

- Si les aparecen dos rutas de salida pueden borrar la que sale por eth0 con un comando como:

```
sudo route del -net 0.0.0.0 gw 10.0.2.2 netmask 0.0.0.0 dev eth0
```

- Ping a través de eth1

```
ping –I eth1 8.8.8.8
```

Caso de Uso

Bibliografía

- https://nocsma.wordpress.com/2016/10/21/useful-firewalld-rules-to-configure-and-manage-firewall-in-linux/
- http://www.mjhall.org/centos7-firewalld-nat-router/
- https://sergvergara.wordpress.com/2011/03/14/arquitectura-y-diseno-de-seguridad-de-red-perimetral/