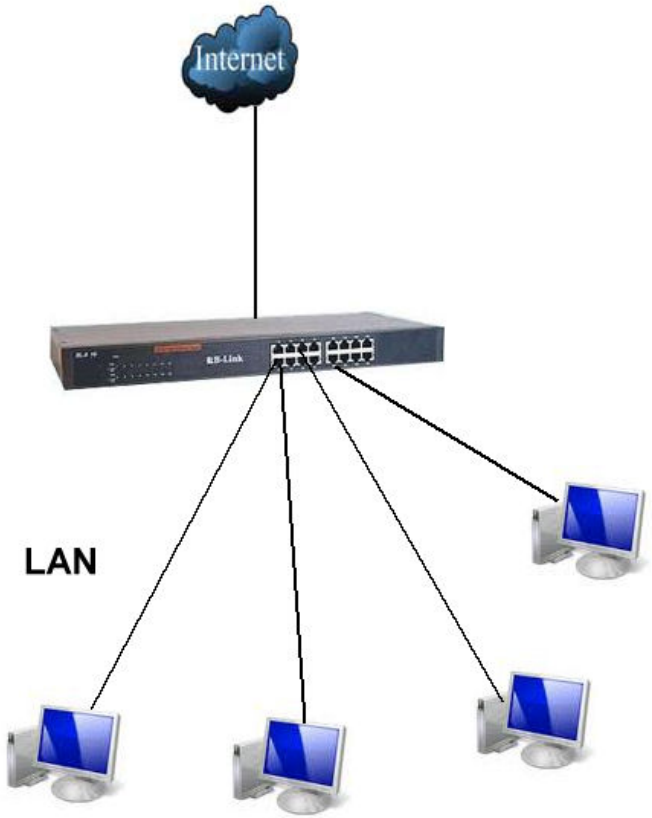
FireWall

Que pretende controlar el FW



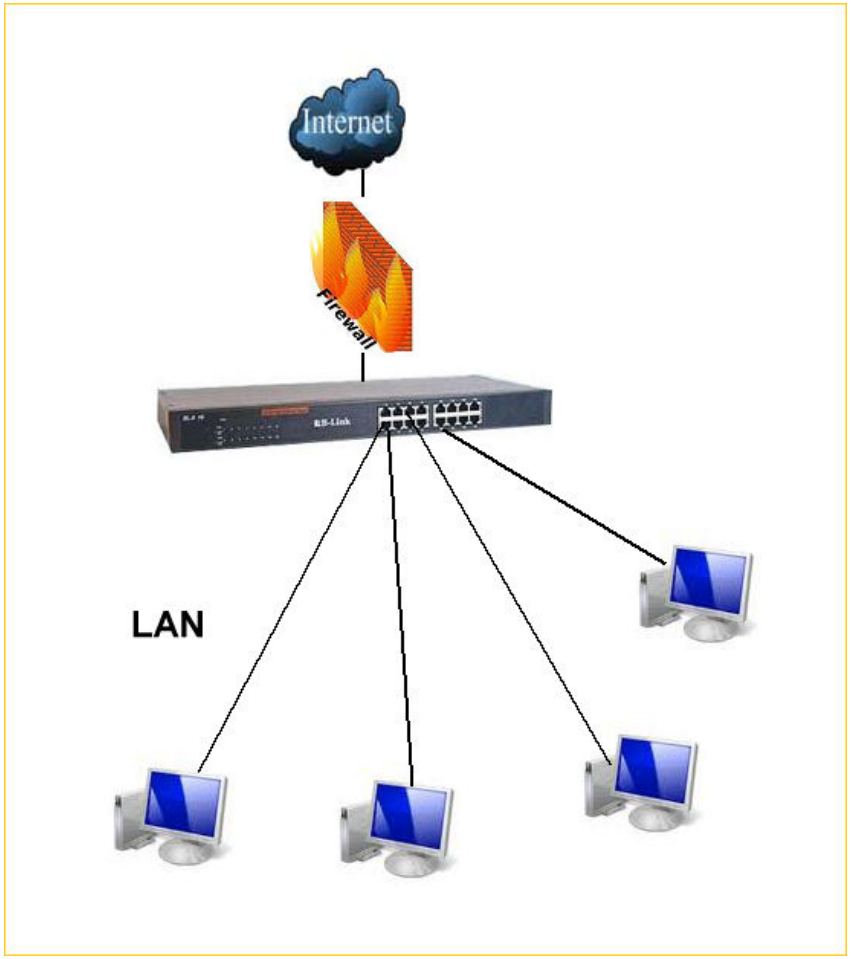
¿Qué significa firewall?

- La traducción más acertada de este término inglés al idioma español es la palabra cortafuegos.
- <<Cortafuego o cortafuegos. (De cortar y fuego). m. Agr. Vereda ancha que se deja en los sembrados y montes para que no se propaguen los incendios. || 2. Arq. Pared toda de fábrica, sin madera alguna, y de un grueso competente, que se eleva desde la parte inferior del edificio hasta más arriba del caballete, con el fin de que, si hay fuego en un lado, no se pueda este comunicar al otro.>>

¿Qué es un firewall?

- Un FireWall, es un sistema informático, simple o compuesto que actúa como punto de conexión segura entre otros dos o más sistemas informáticos.
- Es la primera línea de defensa sobre ataques externos; también puede ser usado para prevenir ataques internos.

¿Qué es un firewall?



¿ Que es un Firewall ?

- Existen 2 Tipos básicos de Firewall
  - Hardware Firewall: Normalmente es un ruteador, tiene ciertas reglas para dejar o no dejar pasar los paquetes.
  - Software Firewall: Es un programa que esta corriendo preferentemente en un bastioned host, que verifica los paquetes con diferentes criterios para dejarlos pasar o descartarlos.

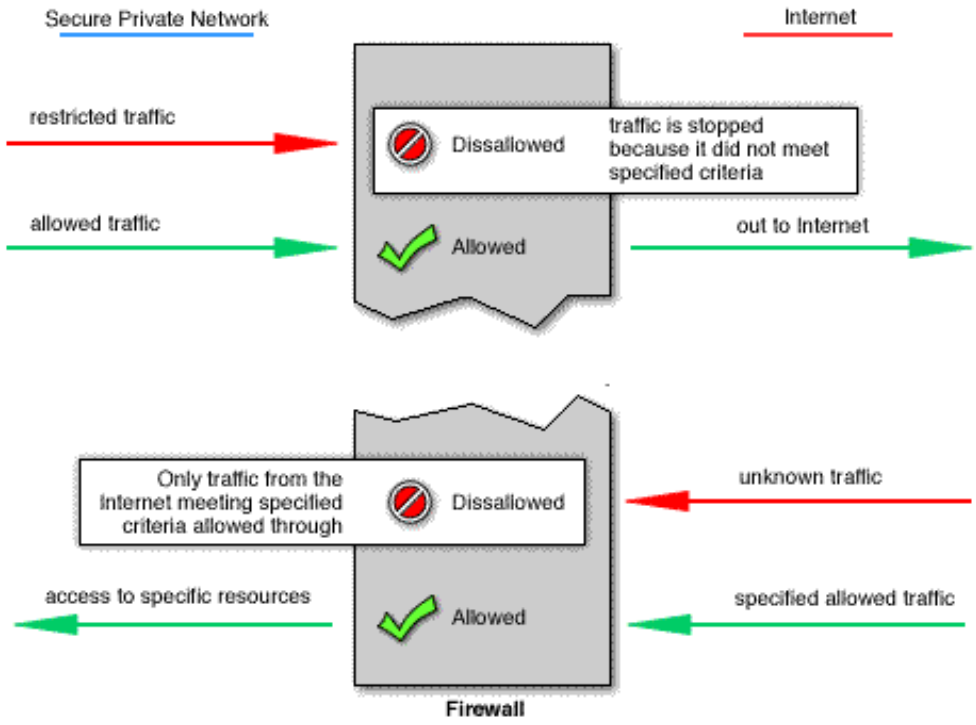
Tipos básicos de Firewall

Hardware Firewall

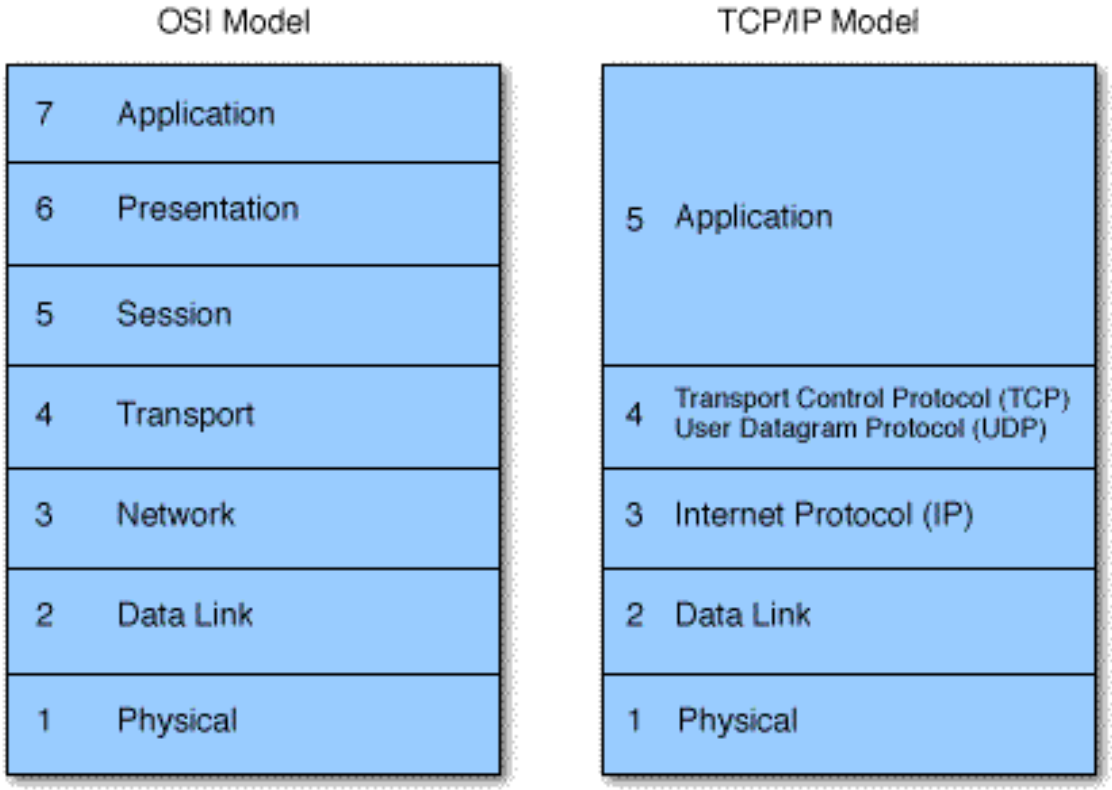
Software Firewall

Funcionamiento Basico

- Examina el trafico en la red, tanto entrante como saliente.
- Aplica ciertos criterios definidos por el administrador para determinar si lo deja pasar o lo descarta.



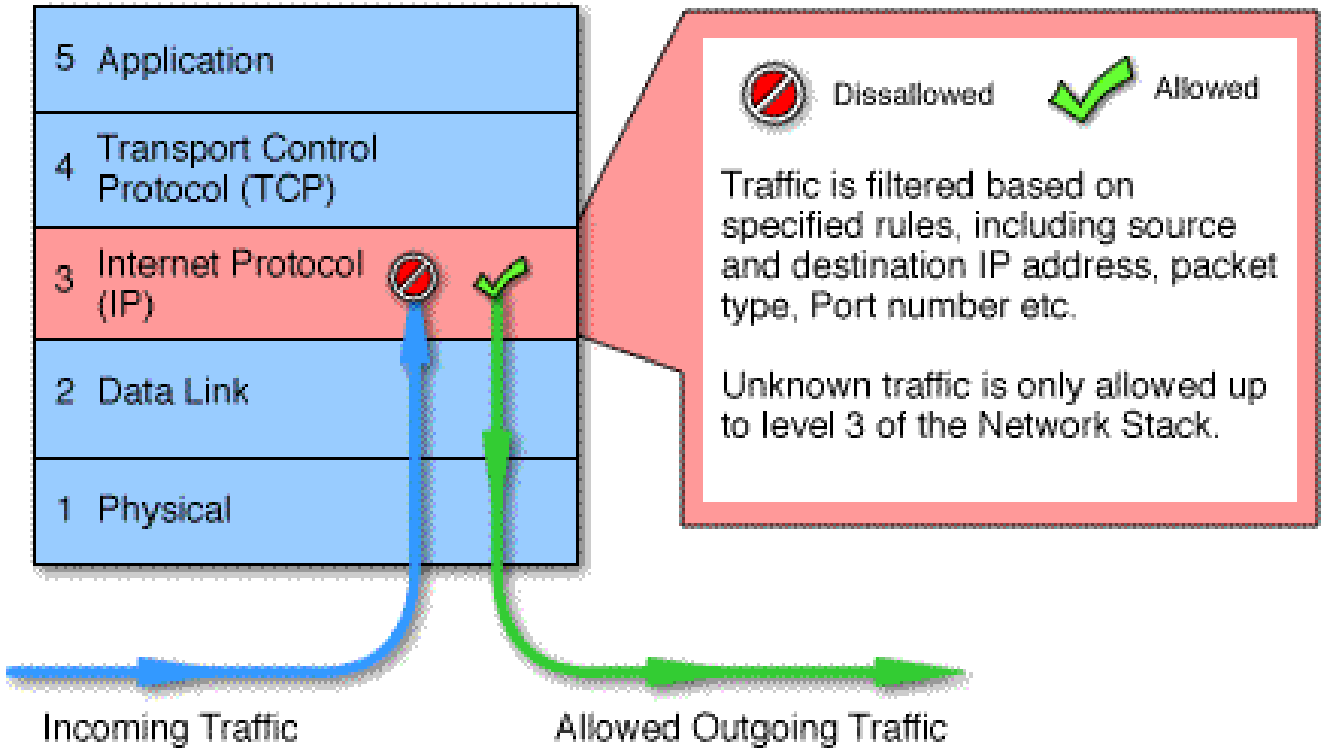
¿En que capa trabaja el Firewall?



Tipos de Firewalls

- Packet filters
- Circuit Level Gateways
- Aplication Level Gateways
- Stateful Inspection Firewall

Paquet Filters



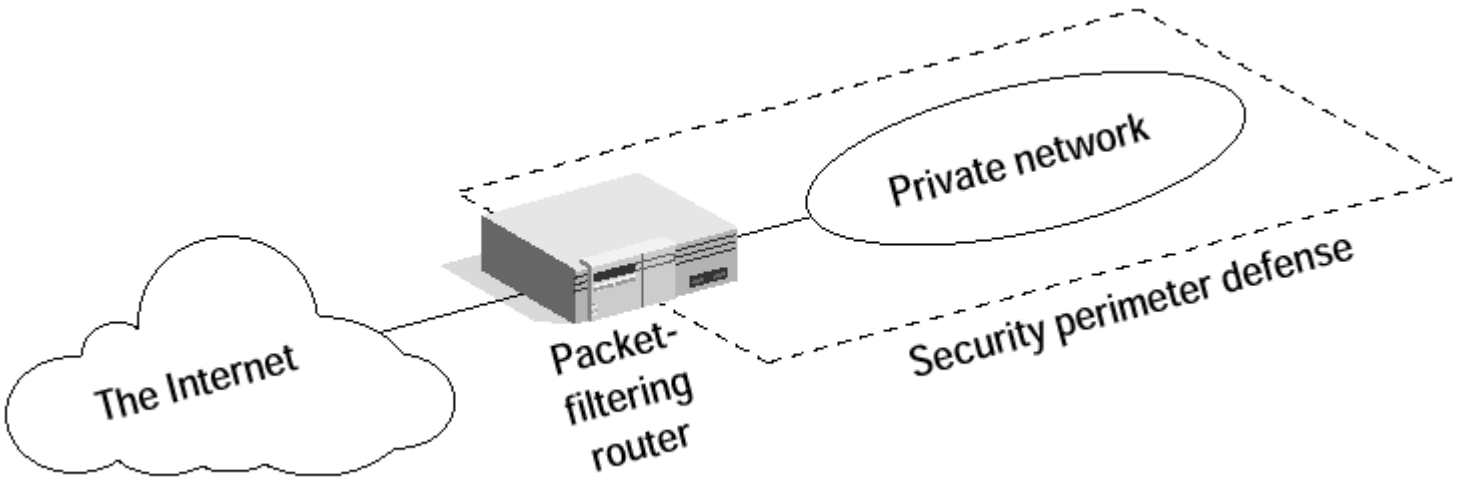
Packet filters

- Trabaja a nivel de Red.
- Compara con un conjunto de criterios antes de renviar el trafico
-
- Ventaja: Bajo costo e impacto en la performance de la red.
- Desventaja: No soporta rejas sofisticadas.

- Cada paquete puede ser analizado en función de:
  - @IP origen / destino
  - Puerto origen / destino
  - Protocolo usado: TCP / UDP / ICMP

Packet Filtering Routers

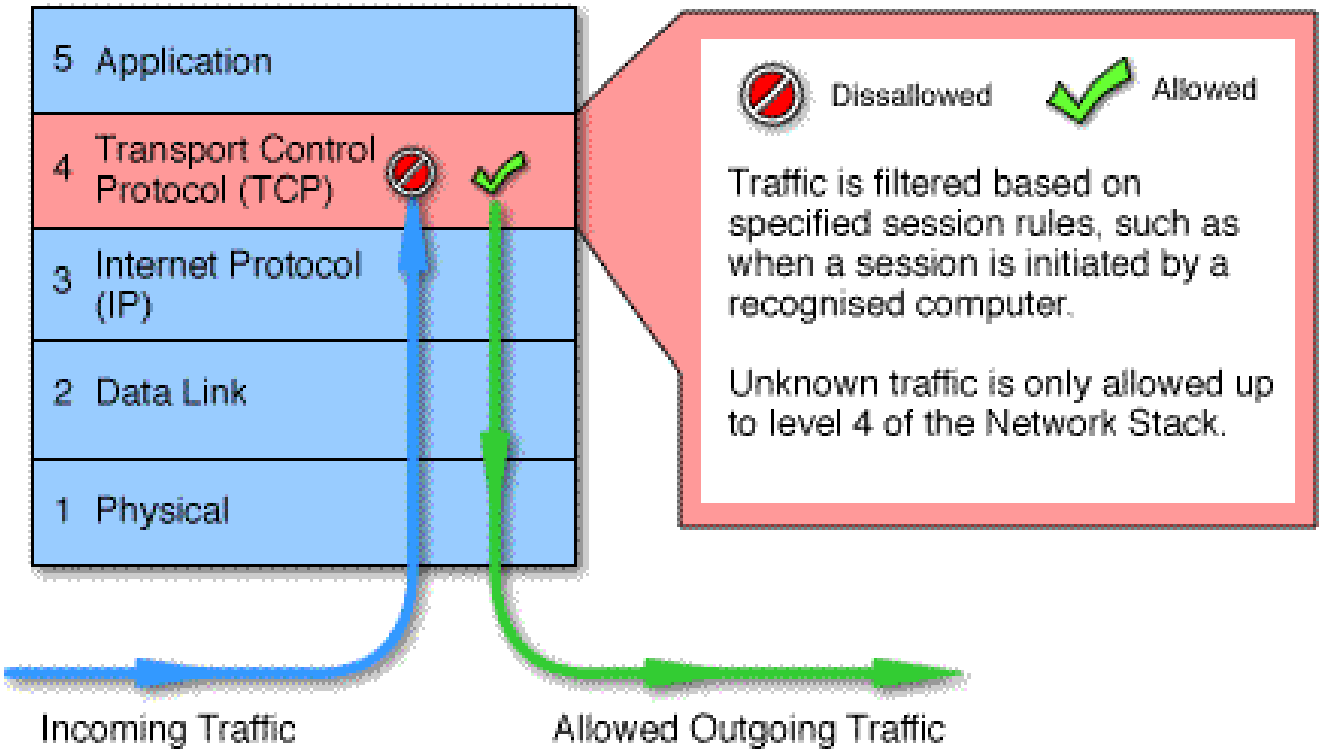
- Renvia o descarta paquetes IP de acuerdo a un conjunto de reglas
- Las reglas de filtrado estan basadas en campos de las cabeceras IP o Transporte



¿Que informacion se utiliza en una decicion de filtrado?

- Direccion IP Origen (Cabecera IP)
- Direccion IP Destino (Cabecera IP)
- Tipo de Protocolo
- Puerto de Origen (Cabecera TCP o UDP)
- Puerto de Destino (Cabecera TCP o UDP)
- Bit ACK.

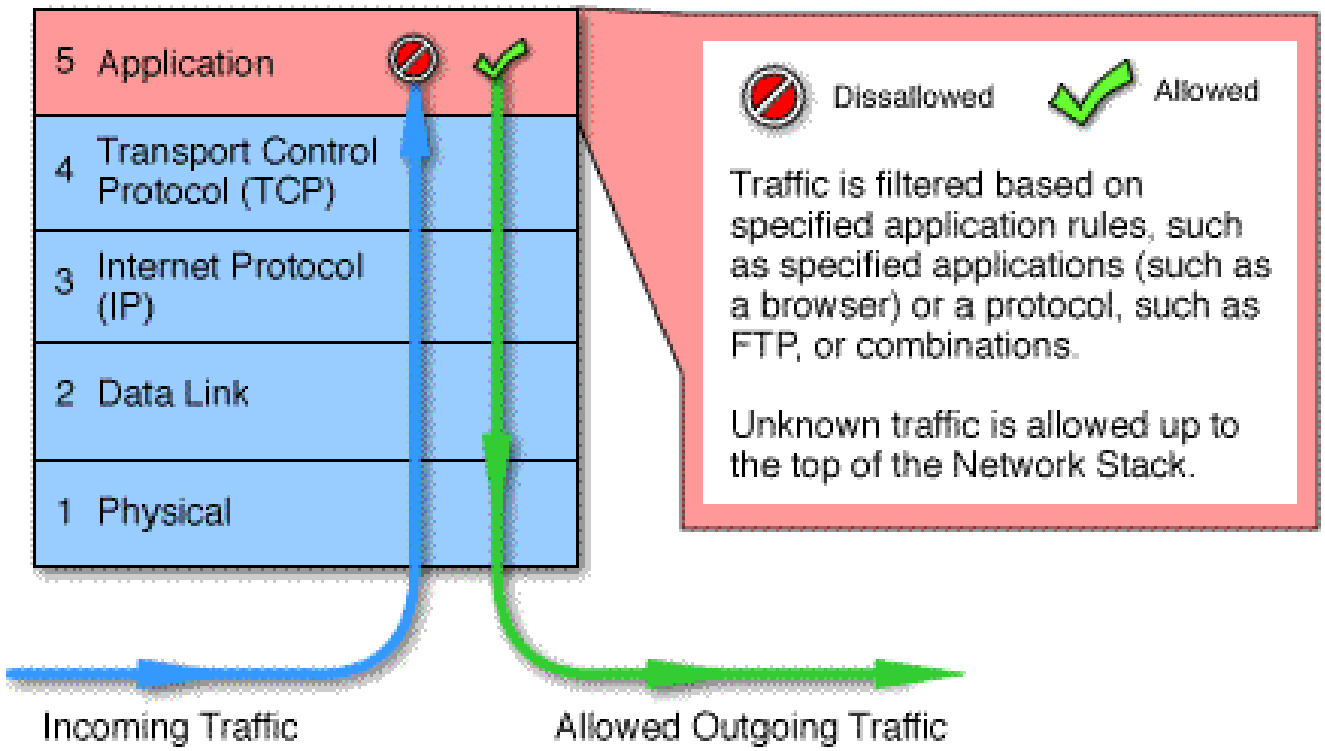
Circuit Level Gateways



Circuit level gateways

- Trabaja en la capa de Sesion
- Monitorea el handshaking TCP entre paquetes para determinar cuando una sesion es legitima
- Informacion es enviada al equipo remoto a travez Gateway de circuito como si fuese originado por el gateway.
- Ventaja: Relativamente economico, oculta la informacion sobre la red privada.
- Desventaja: No puede filtrar paquetes individuales.

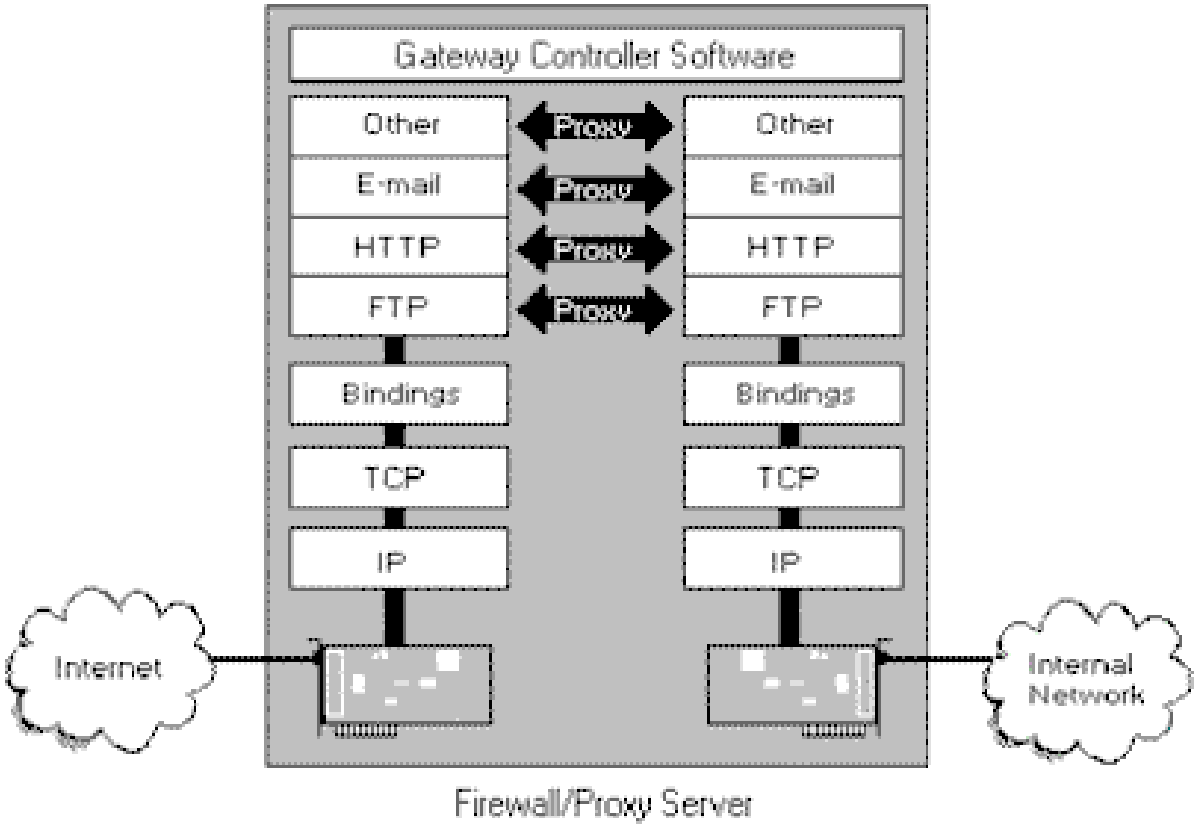
Aplication Level Gateways



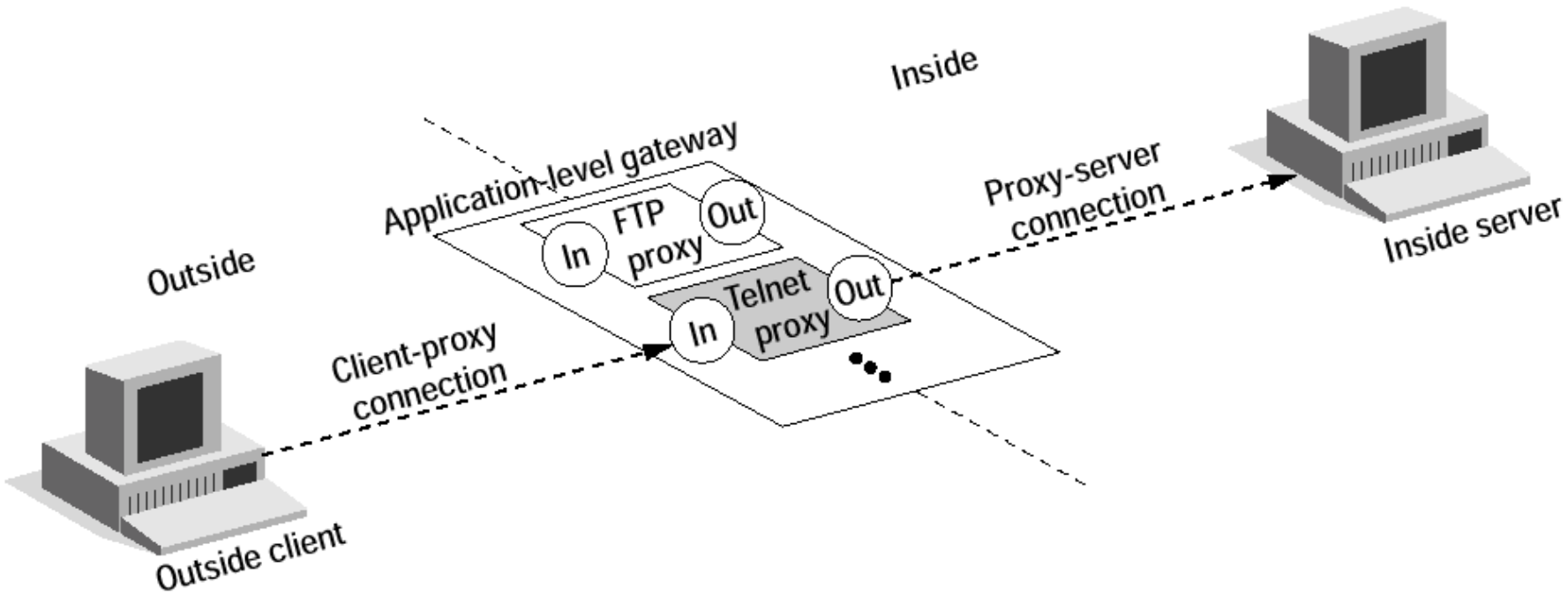
Aplication Level Gateways

- Actúa dentro de los *niveles de transporte y aplicación* (*circuit level gateway* y *application gateway* respectivamente) según el modelo *TCP/IP*.
- Procesa, valida y regenera cada paquete recibido; impidiendo la conexión directa entre 2 redes diferentes.
- Para cada servicio (*telnet, ftp, http...*) se utiliza un proxy específico, pudiendo así prohibir el uso de determinadas órdenes de un servicio.

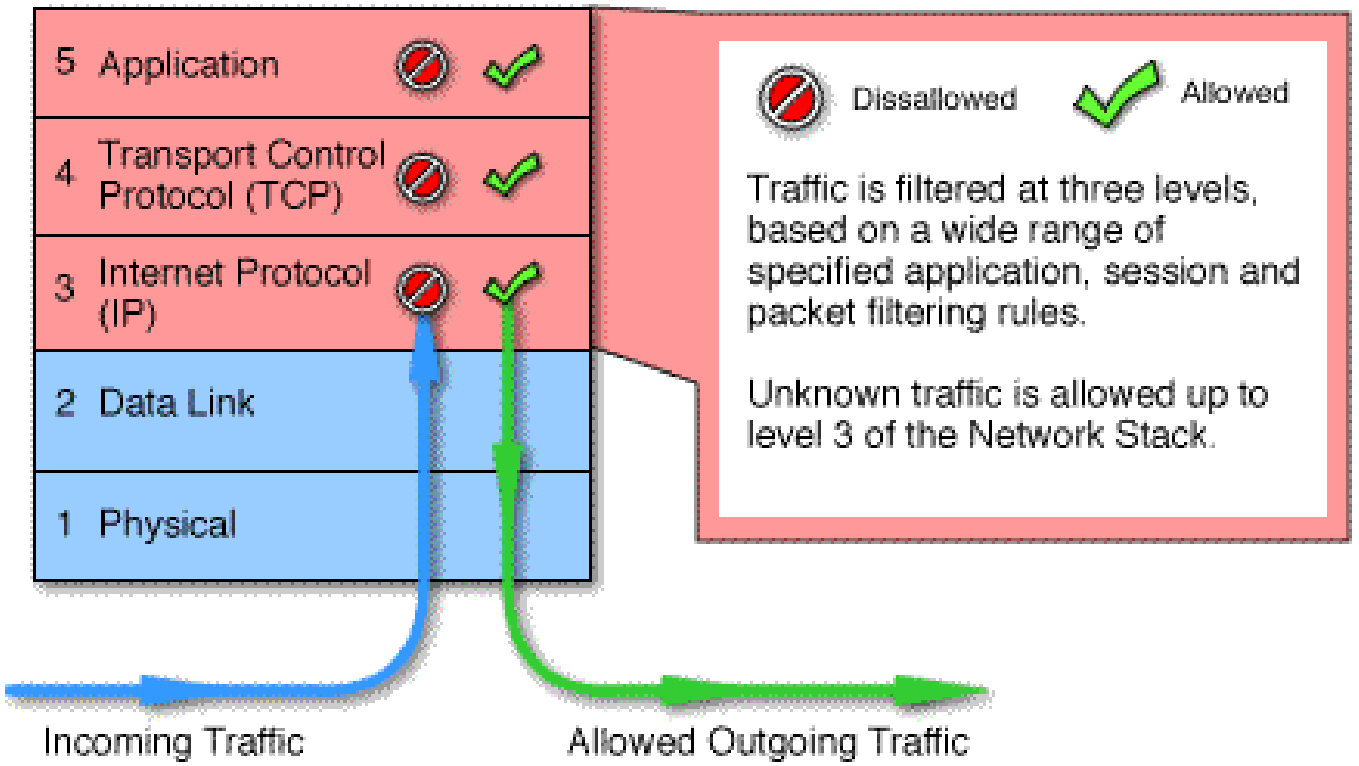
Gateways Capa de Applicacion (Proxy Server)



Proxy Telnet



Stateful Inspection Firewall



Stateful Inspection Firewall

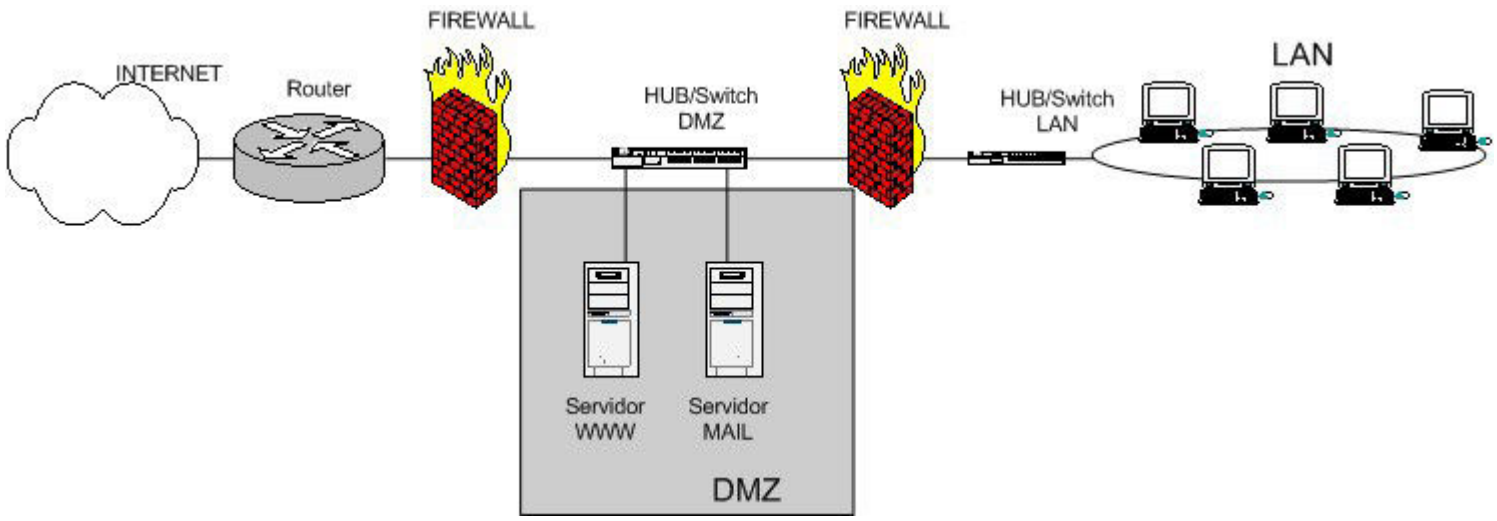
- Actúa dentro de los *niveles de IP, transporte y aplicación* según el modelo *TCP/IP*
- Comprueba (y no procesa, como en un Proxy server) los paquetes a distintos niveles verificando la validez de estos, basándose en un seguimiento del estado de la conexión en cada momento.
- Permite conexiones directas entre distintas redes, dando un servicio transparente a ambos lados.

La Red Dividida en Zonas

- Zona Publica, esta se encuentra directamente conectada a Internet (zona no segura, normalmente llamada RED)
- Zona Privada, esta es nuestra Lan Interna (Zona segura, normalmente llamada Green)
- Zona Desmiritalizada “DMZ” es donde se encuentran nuestros servicios de red que son accedidos tanto de la red publica como la privada.(Zona semi-segura tambien llamada *red perimetral* es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet , normalmente llamada Orange)

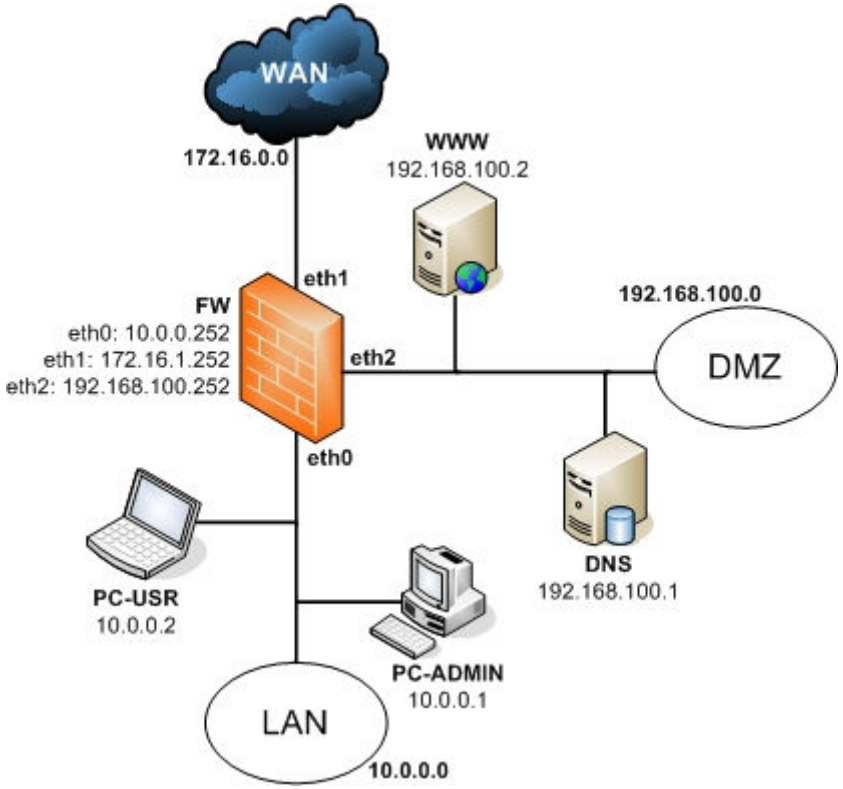
Esquema de implementación de Firewall

- Esta implementacion es basada en 2 firewall y se ve claramente las 3 Zonas



Esquema de implementación de Firewall

- Un solo FireWall conectando las 3 Zonas

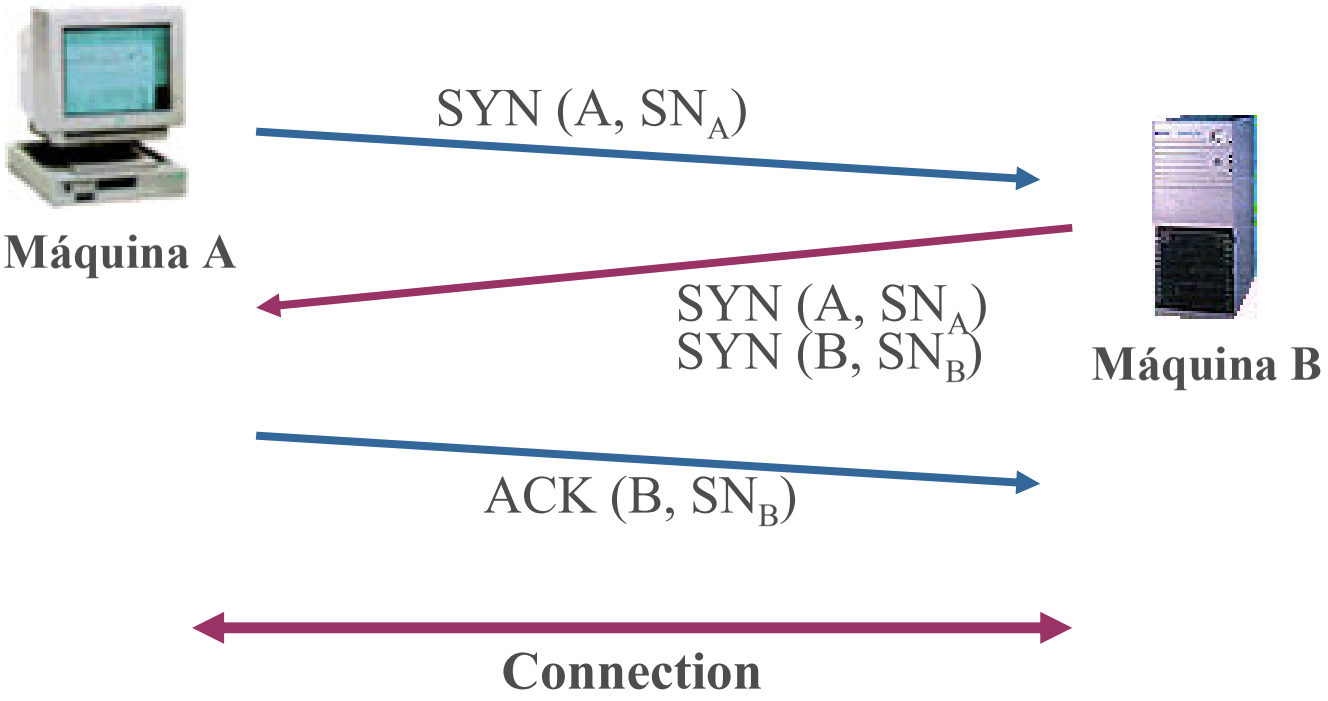


Stateful Inspection Firewalls

- Estado de Conexion: Abierta o Cerrada
  - Estado: El Orden de los paquetes dentro del Dialogo
  - Controlar simplemente si es una conexion abierta

Negociación de Conexión en TCP/IP

Ejemplo



Como Opera
Stateful Inspection Firewalls

- Para TCP, controla el la tabla de estados que las dos dirreciones IP y los numeros de puerto esten OK (Con conexion Abierta)
- Por defecto, permite las conexiones desde los clientes internos (en la red confiable) hacia servers externos (en la red no confiable)
  - Este comportamiento predeterminado se puede cambiar en una ACL (Lista de Acceso)
- Aceptar paquetes en el futuro entre estos hosts y puertos con la inspección minima o nula

Stateful Inspection Firewall Operation I

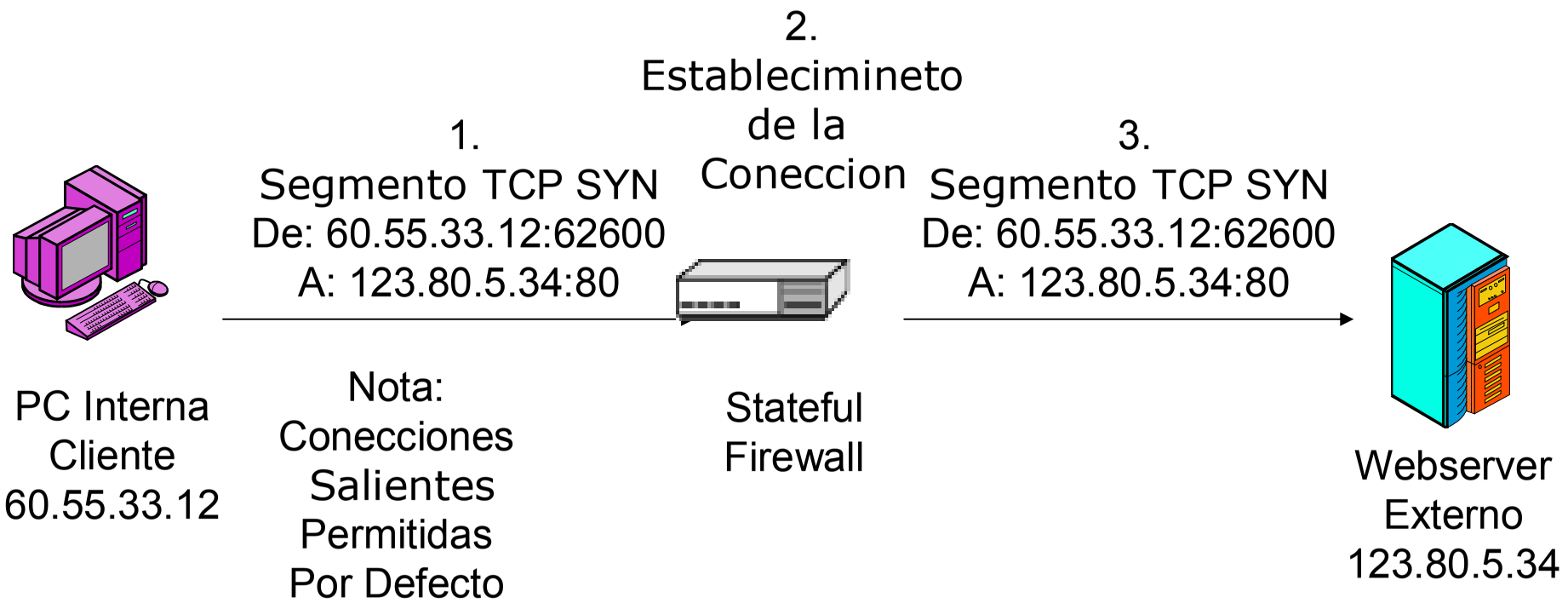


Tabla de Coneccion

Tipo	IP Interno	Puerto Interno	IP Externo	Puerto Externo	Estado
TCP	60.55.33.12	62600	123.80.5.34	80	OK

Stateful Inspection Firewall Operation I

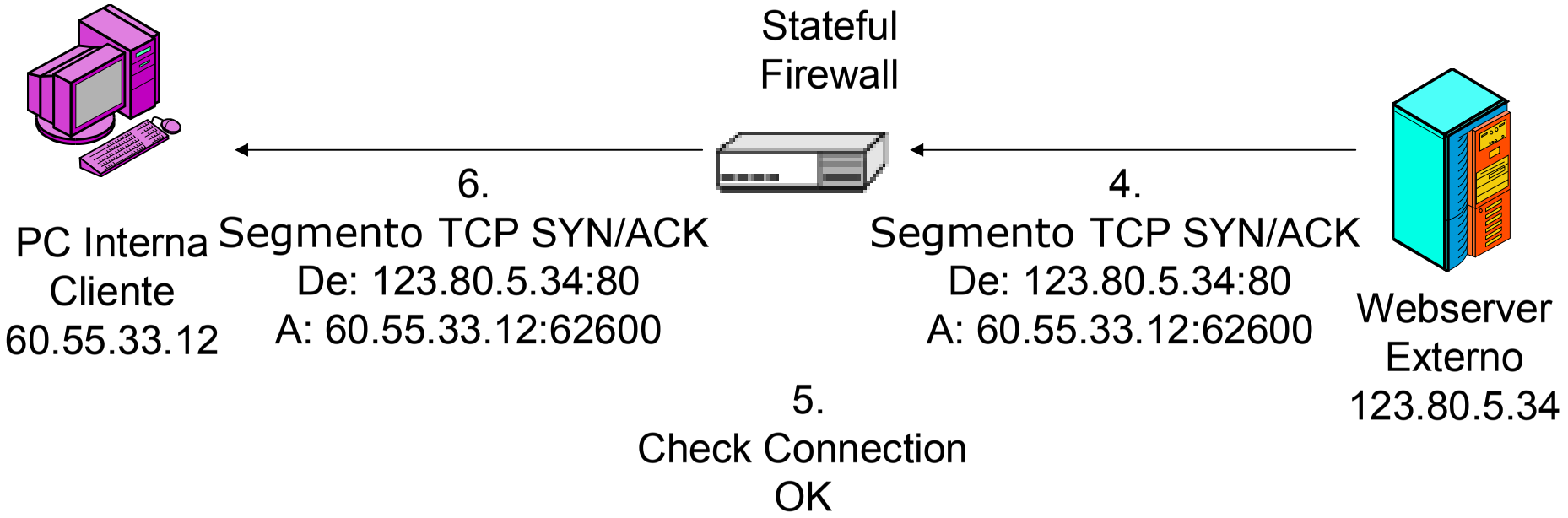


Tabla de Coneccion

Tipo	IP Interno	Puerto Interno	IP Externo	Puerto Externo	Estado
TCP	60.55.33.12	62600	123.80.5.34	80	OK

Como Opera
Stateful Inspection Firewalls

- Para UDP, tambien registra las dos direcciones IP y sus respectivos puertos en la tabla de estados.

Tabla de Coneccion

Tipo	IP Interno	Puerto Interno	IP Externo	Puerto Externo	Estado
TCP	60.55.33.12	62600	123.80.5.34	80	OK
UDP	60.55.33.12	63206	1.8.33.4	69	OK

Stateful Inspection Firewalls

- Los Firewalls con filtrado estatico de Paquetes Stateless (Sin Manejo de Estado)
  - Filtran de un paquete a la vez, de forma aislada. Filter one packet at a time, in isolation
  - Si es enviado un segmento TCP SYN / ACK, no se puede saber si había un SYN anterior el cual abre conexión
    If a TCP SYN/ACK segment is sent, cannot tell if there was a previous SYN to open a connection
  - No pueden manejar la comutacion de puertos segun la aplicacion

Stateful Firewall Operation II

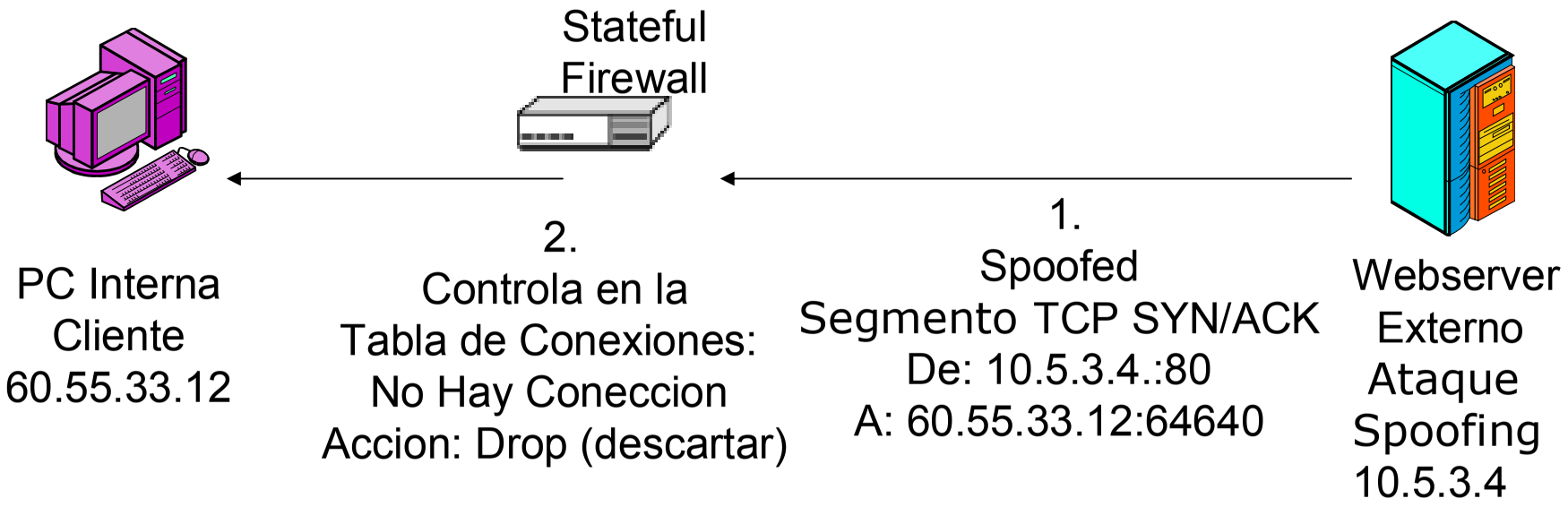


Tabla de Coneccion

Tipo	IP Interno	Puerto Interno	IP Externo	Puerto Externo	Estado
TCP	60.55.33.12	62600	123.80.5.34	80	OK
UDP	60.55.33.12	63206	222.8.33.4	69	OK

Port-Switching Applications with Stateful Firewalls

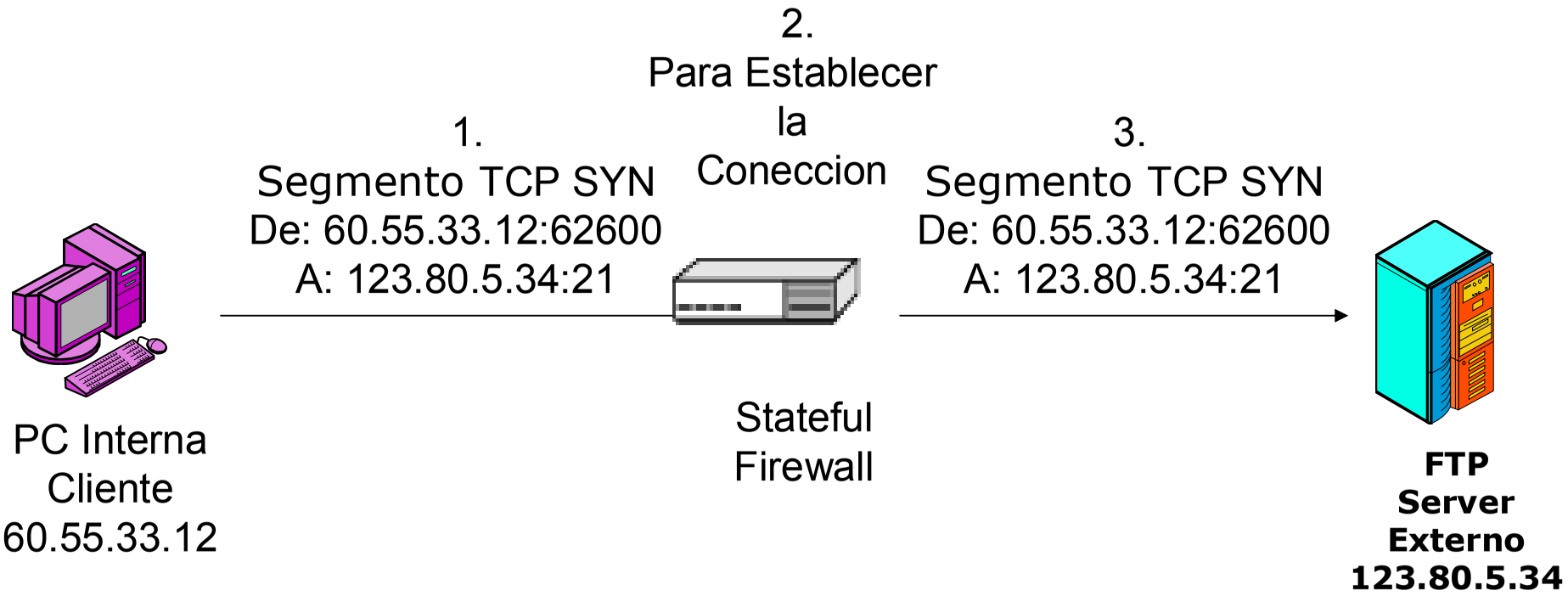
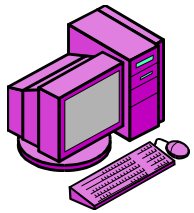


Tabla de Coneccion

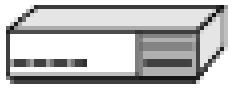
	Tipo	IP Interno	Puerto Interno	IP Externo	Puerto Externo	Estado
Paso 2 →	TCP	60.55.33.12	62600	123.80.5.34	21	OK

Port-Switching Applications with Stateful Firewalls



PC Interna
Cliente
60.55.33.12

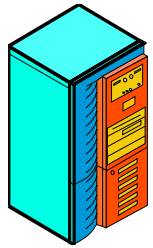
Stateful
Firewall



6.
Segmento TCP SYN/ACK
De: 123.80.5.34:21
A: 60.55.33.12:62600
Usa los Puertos 20
y 55336 para
Transferencia de Datos

5.
Permite el
Establecer
La Segunda
Coneccion

4.
Segmento TCP
SYN/ACK
De: 123.80.5.34:21
A: 60.55.33.12:62600
Usa los Puertos 20
y 55336 para
Transferencia de
Datos



FTP
Server
Externo
123.80.5.34

Tabla de Coneccion

	Tipo	IP Interno	Puerto Interno	IP Externo	Puerto Externo	Estado
Paso 2 →	TCP	60.55.33.12	62600	123.80.5.34	21	OK
Paso 5 →	TCP	60.55.33.12	55336	123.80.5.34	20	OK

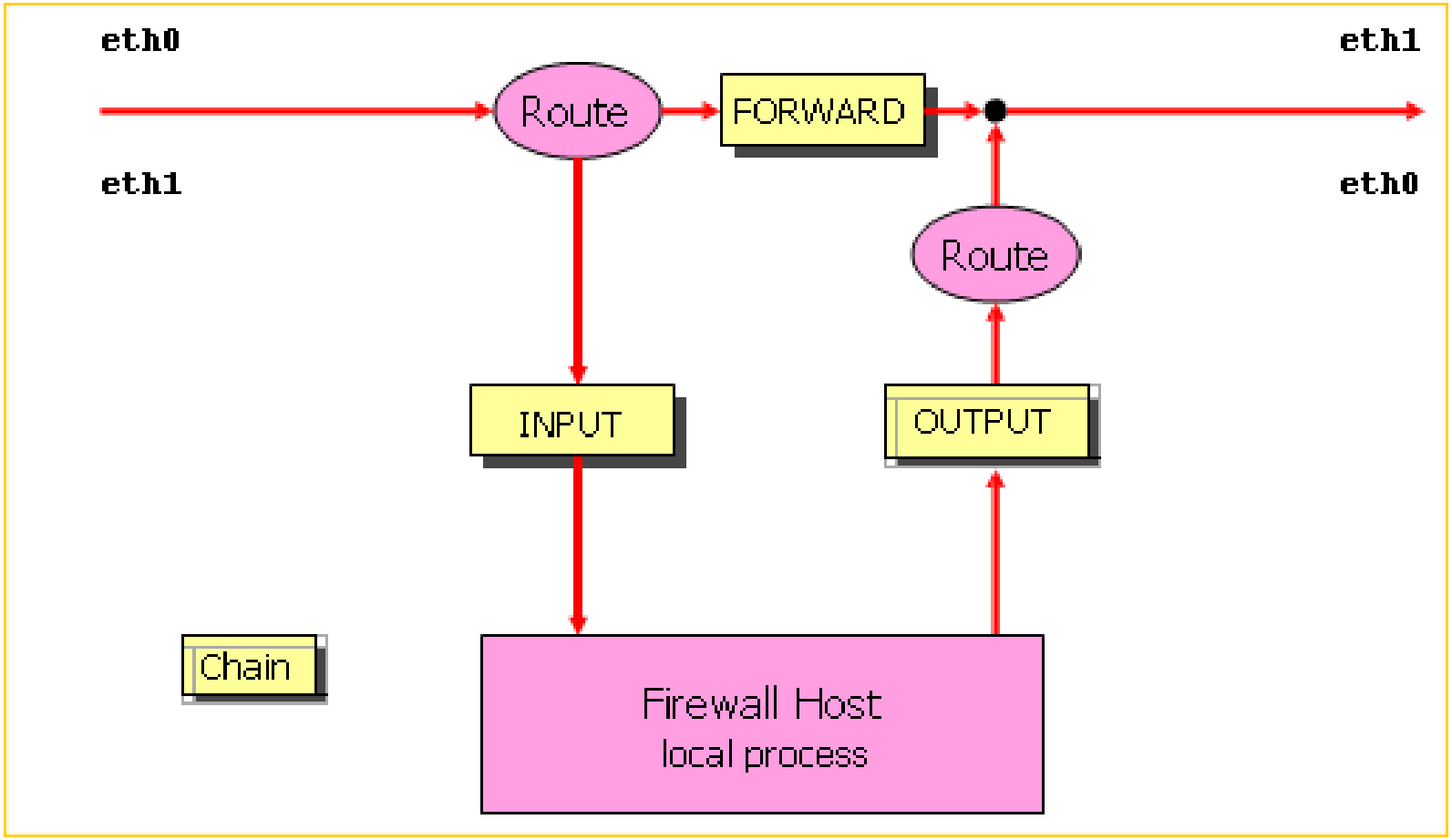
Stateful Inspection Access Control Lists (Lista de Control de Acceso o ACLs)

- Inicialmente Permite o Deniega aplicaciones
- Simple, porque buscando ataques que no son parte de las conversaciones no necesitan normas específicas, ya que se eliminan de forma automática
- En Firewalls integrados, las reglas ACL puede especificar que los mensajes de un protocolo de aplicación en particular o un servidor sea validada o pase a un firewall de aplicación (Proxy) para la inspección

Funciones del Firewall

- Filtrado, Inspección, Detección, Logging, Alertar
- Denegar todo lo que no este explícitamente permitido o…
- Permitir todo lo que no este explícitamente denegado.

Linux Netfilter



Reglas de Filtrado – Default Policy

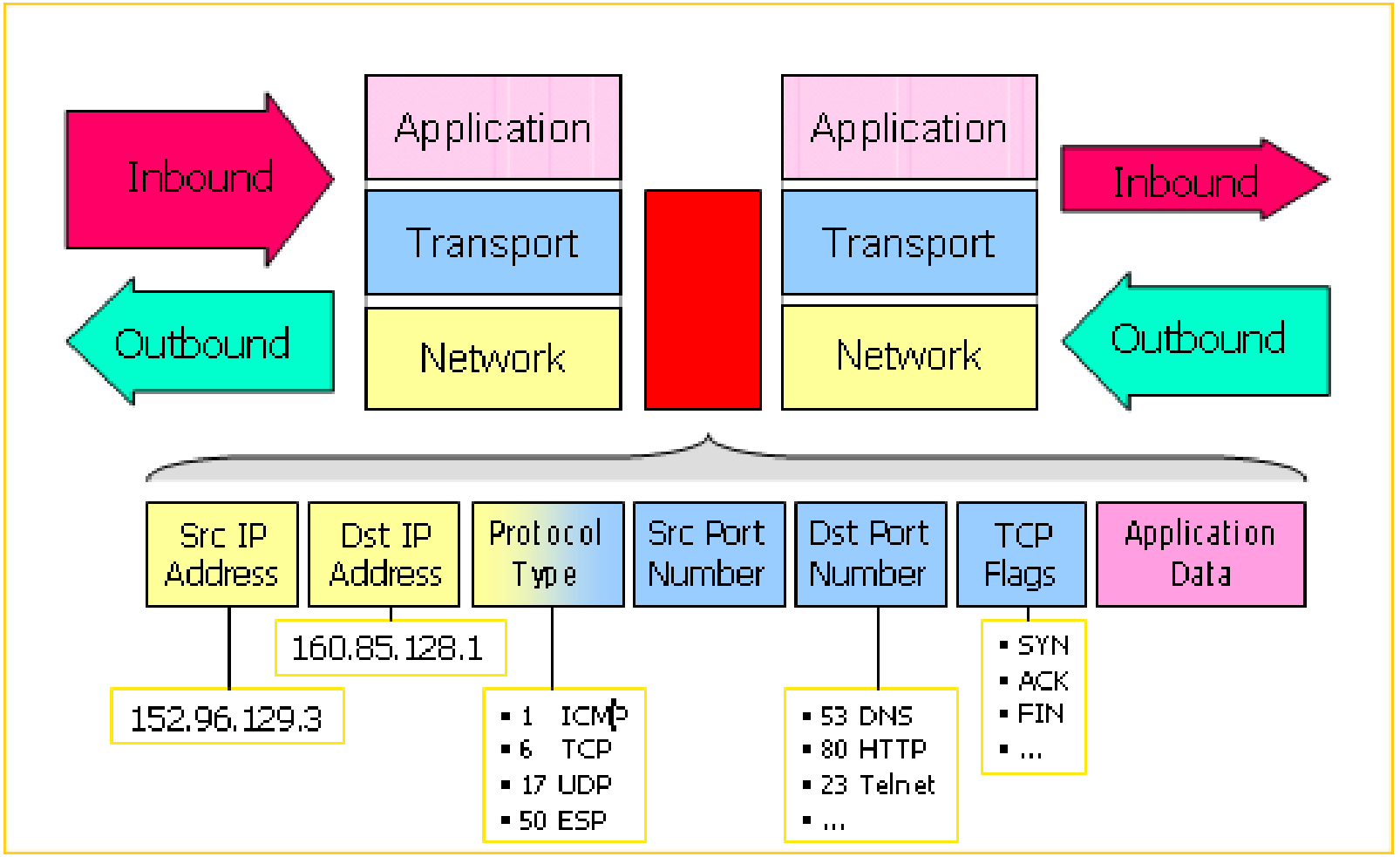
- Permitir todo lo que no este explicitamente denegado.

  iptables –P INPUT ACCEPT
  iptables –P FORWARD ACCEPT
  iptables –P OUTPUT ACCEPT

- Denegar todo lo que no este explícitamente permitido.

  iptables –P INPUT DROP
  iptables –P FORWARD DROP
  iptables –P OUTPUT DROP

Inspección Profunda de Paquetes



- Politica por Defecto: Denegar todo lo que no este explícitamente permitido.

  iptables –P INPUT DROP
  iptables –P FORWARD DROP
  iptables –P OUTPUT DROP

- Permitir acceso al ssh del firewall desde un equipo externo

  iptables –A INPUT –i eth0 –p tcp --dport ssh –j ACCEPT
  iptables –A OUTPUT –o eth0 –p tcp --sport ssh –j ACCEPT

- Permitir pings desde todas las interfaces

  iptables –A INPUT –p icmp --icmp-type echo-request –j ACCEPT
  iptables –A OUTPUT –p icmp --icmp-type echo-reply –j ACCEPT

- Descartar todo el trafico procedente del equipo 80.63.5.7

  iptables –I INPUT 1 –i eth0 –s 80.63.5.7 –j DROP

Stateful Inspection con Linux Netfilter

- Permitir respuestas en lo paquetes TCP

```
iptables -A OUTPUT –o eth0 -p tcp          -m state
         --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT        -i eth0 -p tcp    -m state
         --state ESTABLISHED,RELATED     -j ACCEPT
```

- Permitir respuestas en lo paquetes UDP

```
iptables -A OUTPUT –o eth0 -p udp          -m state
         --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT        -i eth0 -p udp    -m state
         --state ESTABLISHED,RELATED     -j ACCEPT
```

- Permitir respuestas en lo paquetes ICMP

```
iptables -A OUTPUT –o eth0 -p icmp         -m state
         --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT        -i eth0 -p icmp   -m state
         --state ESTABLISHED,RELATED     -j ACCEPT
```

Cadenas de IPTables Completa