UNIVERSIDADE DA CORUÑA

Monitorización y Filtrado

LSI

2012-2013

Contenido

- Monitorización
  - Herramientas y utilidades
- Filtrado
  - Conceptos generales
  - Firewalls
    - Tipología
    - Arquitecturas
  - IpTables

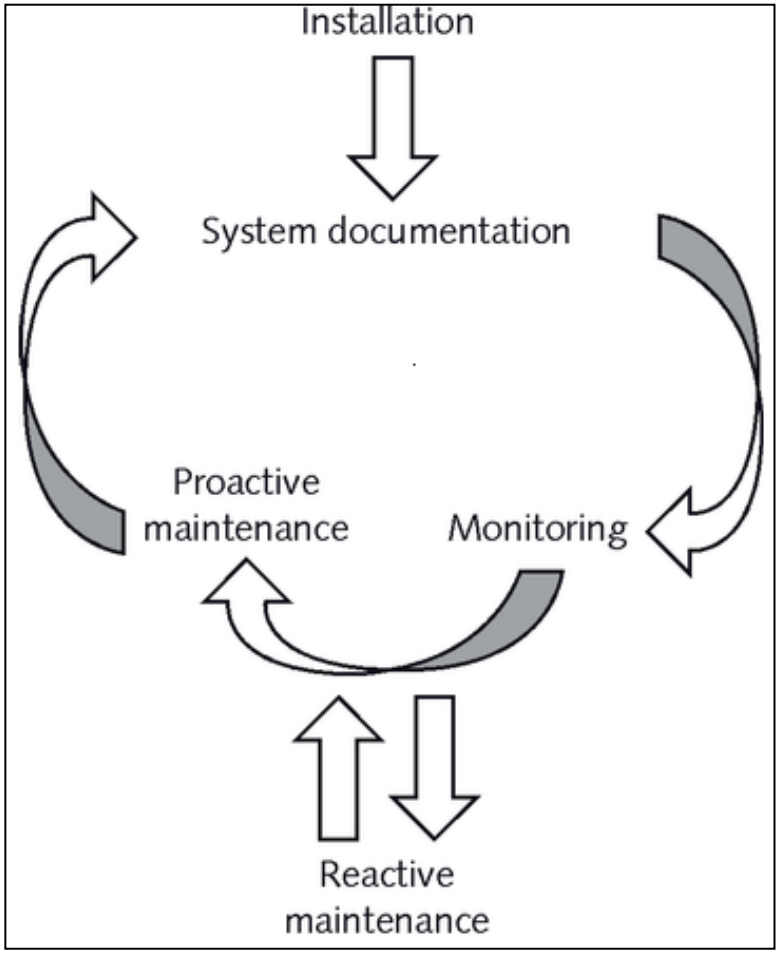
MONITORIZACIÓN

Monitorización

- Problemas más habituales a los que se enfrenta un administrador de sistemas
  - Securización y **Rendimiento**
- ¿Cómo se lleva a cabo el mantenimiento de un sistema?
  - No hacer nada
    - Pb: imagen no seria, degradación continua
  - Monitorización continua [accounting]
    - Utilización de memoria
    - Accesos a disco
    - Uso de CPU
    - Actividad de red

Monitorización

- Ciclo de mantenimiento



Monitorización

- Monitorización
  - Análisis de logs y/o ejecución de *benchmarks* para la identificación de problemas y sus causas
- Mantenimiento proactivo
  - Minimización de la incidencia de futuros problemas
    - Ej. políticas de backup
- Mantenimiento reactivo
  - Corrección de problemas una vez que surgen
- DOCUMENTACIÓN

Monitorización

- Los problemas suelen estar relacionados con alguno de los siguientes conceptos
  - Hardware
  - Software

Monitorización

- Los problemas suelen estar relacionados con alguno de los siguientes conceptos
  - Hardware
    - Mal funcionamiento o mala configuración
      - Comando `dmesg`
      - Ficheros de log:
        - `/var/log/dmesg, /var/log/boot, /var/log/messages`
    - Ausencia de drivers
      - Comandos lsmod, lsusb, lspci
    - Jabbering
  - Software

Monitorización

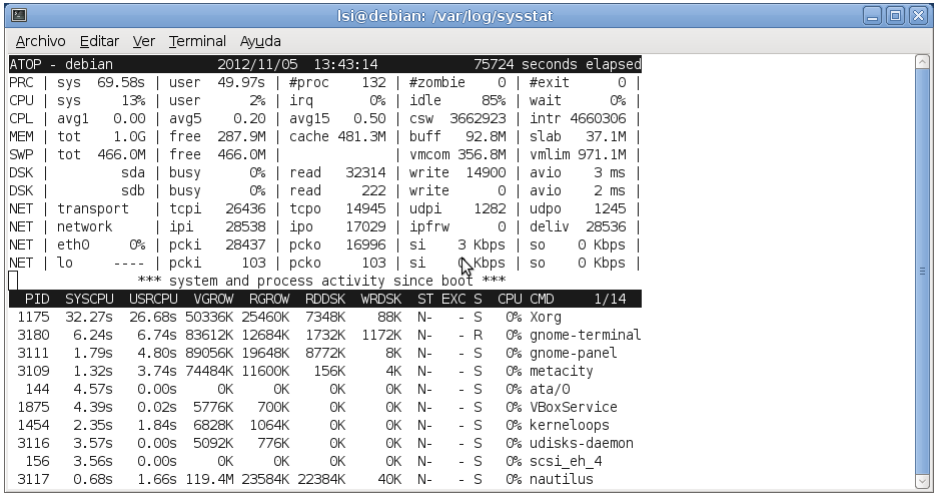
- Los problemas suelen estar relacionados con alguno de los siguientes conceptos
  - Hardware
  - Software
    - Errores de dependencias
      - Comandos ldd y ldconfig
      - Ficheros /etc/ld.so.conf y /etc/ld.so.cache
    - Exceso de procesos, archivos abiertos, etc.
      - Comandos quota, ulimit
    - Errores relativos al sistema operativo
      - en el sistema de ficheros
        - Comandos fsck, mkfs, mount

Monitorización

- Comandos básicos de monitorización
  - Monitorización de inicios de sesión: paquete acct
    - apt-get install acct
  - Utilidades
    - sa — Resumen de la base de datos de accounting de procesos
    - ac — Estadísticas acerca del tiempo de conexión de los usuarios
    - lastcomm — Información acerca de los últimos comandos ejecutados
    - who — Lista los usuarios que tienen iniciada una sesión
    - last — Fechas de login y logout
    - lastb — Fechas de intentos erróneos de login
    - uptime

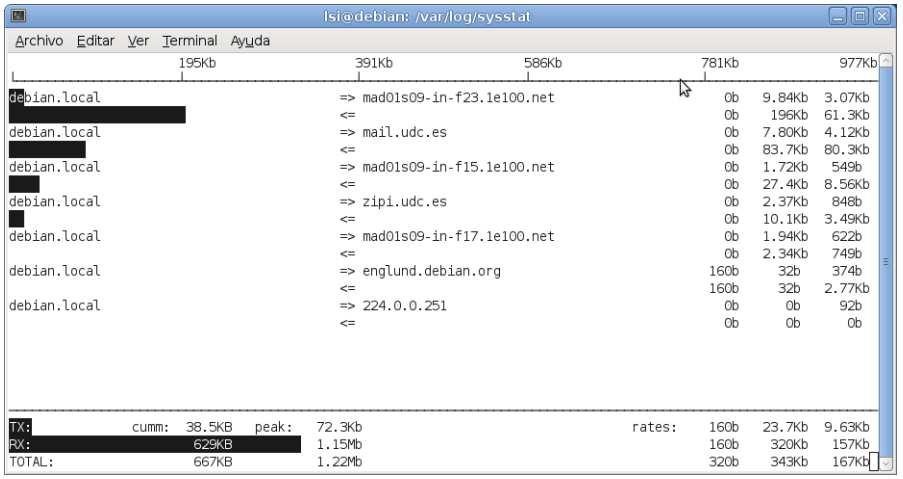
Monitorización

- Comandos básicos de monitorización
  - Monitorización de uso de disco
    - du Muestra la cantidad de disco usado
    - df Muestra la cantidad de disco libre
  - Monitorización de procesos
    - ps, top
    - **atop**
  - Monitorización de red
    - vnstat
    - iftop, iptraf



Monitorización

- Comandos básicos de monitorización
  - Monitorización de uso de disco
    - du Muestra la cantidad de disco usado
    - df Muestra la cantidad de disco libre
    - free Utilización de dispositivos físicos y swapping
  - Monitorización de procesos
    - ps, top
    - atop
  - Monitorización de red
    - vnstat
    - **iftop**, iptraf



Monitorización

- Paquete `sysstat` (System Statistics)
  - Contiene múltiples herramientas de monitorización
    - apt-get install sysstat
    - Habilitar en /etc/default/sysstat
  - mpstat

```
Linux 2.6.32-5-686 (debian)         05/11/12    _i686_       (1 CPU)

11:20:43     CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest   %idle
11:20:43     all    0,03    0,06   13,17    0,18    0,00    0,00    0,00    0,00   86,55
```

  - iostat

```
avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0,03    0,06   13,17    0,18    0,00   86,56

Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
sda               0,53        10,54         6,78     708350     455760
sdb               0,00         0,02         0,00       1122          0
```

  - pidstat

```
Linux 2.6.32-5-686 (debian)         05/11/12    _i686_       (1 CPU)

11:31:59          PID    %usr %system  %guest    %CPU   CPU  Command
11:31:59            1    0,00    0,00    0,00    0,00     0  init
```

Monitorización

- Paquete `sysstat` (System Statistics)
  - sar (System Activity Reporter)
    - -A Muestra información completa (todas las opciones)
    - -b Estadísticas Entrada/Salida
    - -B Estadísticas paginación
    - -c Número de procesos / seg
    - -d Estadísticas Entrada/Salida para cada dispositivo de bloques
    - -m Estadísticas gestión de energía
    - -n Estadísticas de red
    - -r Uso de memoria
    - -S Estadísticas de uso de swapping
    - -u Uso de CPU
    - ...

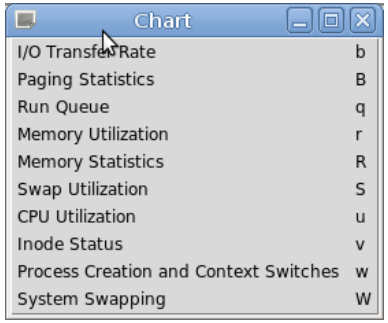
Monitorización

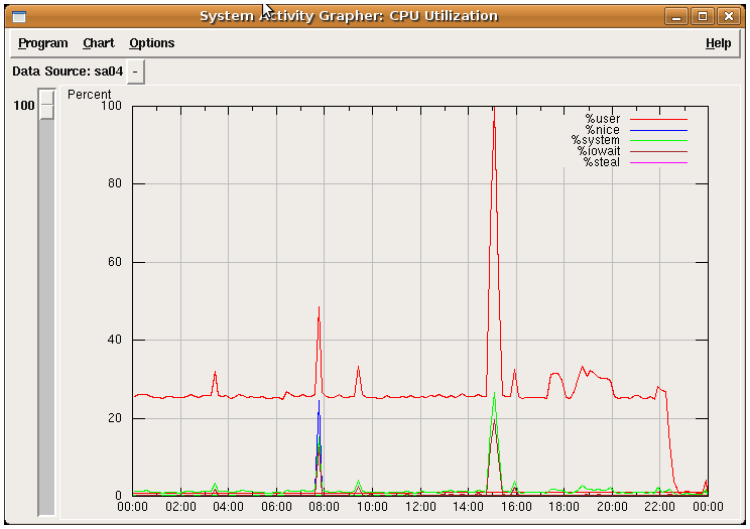
- Paquete `sysstat` (System Statistics)
  - sar (System Activity Reporter)

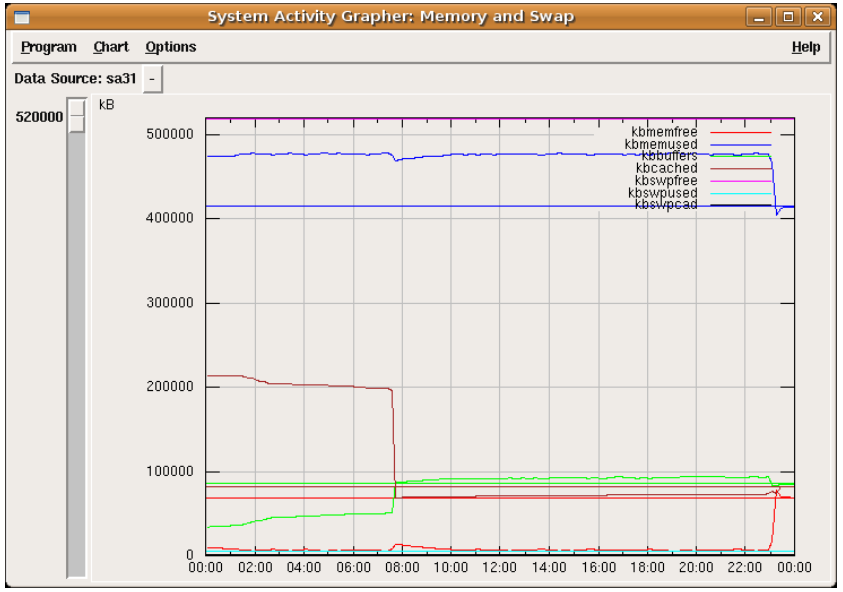
```
root@debian:/var/log# sar -u 2 1
Linux 2.6.32-5-686 (debian)         05/11/12    _i686_      (1 CPU)

11:43:15        CPU     %user     %nice   %system   %iowait    %steal     %idle
11:43:17        all      0,50      0,00      0,50      0,00      0,00     99,00
Media:          all      0,50      0,00      0,50      0,00      0,00     99,00


root@debian:/var/log# sar -r 1 1
Linux 2.6.32-5-686 (debian)         05/11/12    _i686_      (1 CPU)

11:46:15    kbmemfree kbmemused  %memused kbbuffers  kbcached  kbcommit   %commit
11:46:16       374096    660376     63,84     87484    425256    364604     24,12
Media:         374096    660376     63,84     87484    425256    364604     24,12

root@debian:/var/log# sar -m 1 1
Linux 2.6.32-5-686 (debian)         05/11/12    _i686_      (1 CPU)

11:46:46        CPU       MHz
11:46:47        all   2671,70
Media:          all   2671,70
```

Monitorización

- Paquete `sysstat` (System Statistics)
  - isag (Interactive System Activity Grapher)
    - /var/log/sysstat/sa[n]







Monitorización

- … herramientas vistas hasta el momento hacen accounting de una máquina local

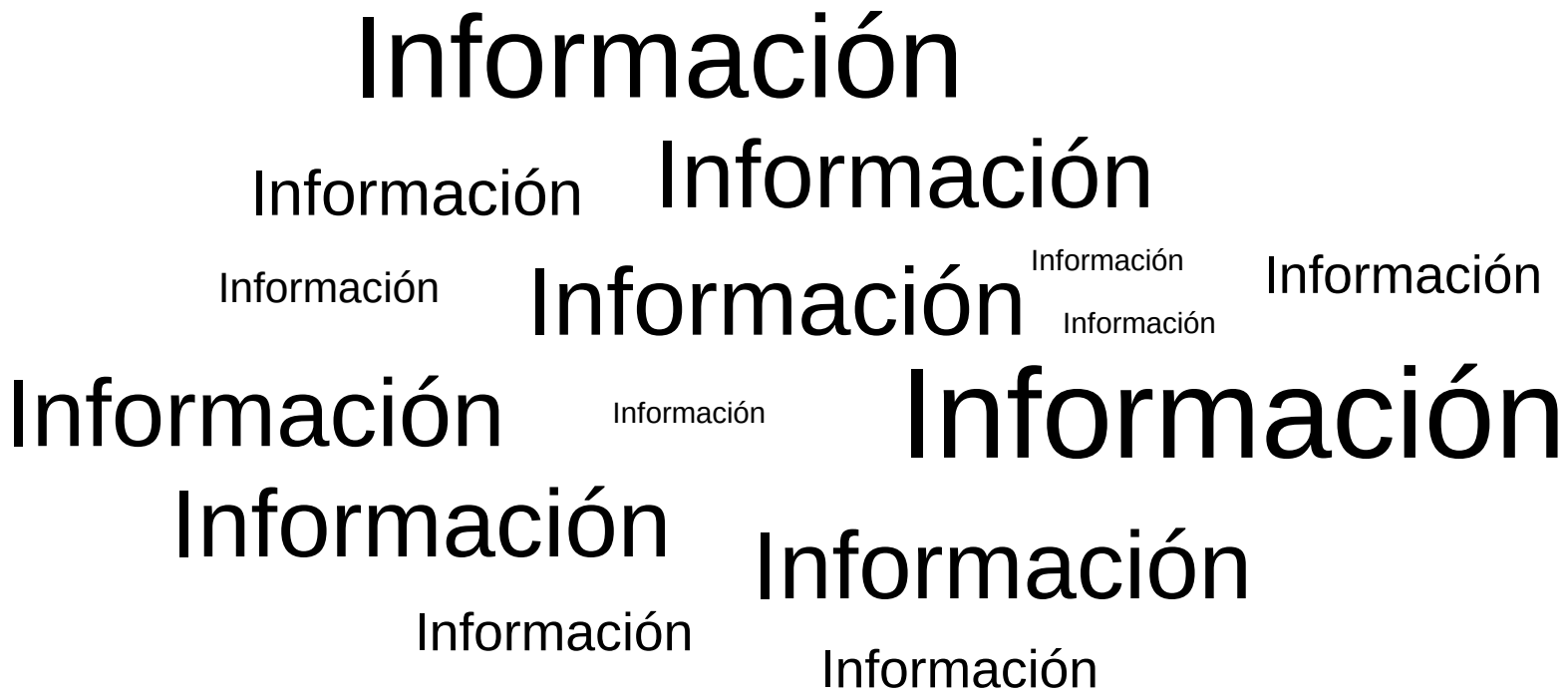
- ¿Qué pasa en entornos mayores?
  - Uso de herramientas centralizadas de monitorización
    - nagios, ntop, ossim
      - SNMP + MIB (Management Information Base)

Monitorización

- Chequeos de integridad
  - sxid
    - Chequea que no se produzcan cambios en los atributos suid, sgid
      - /etc/sxid.conf
  - TripWire
    - Chequea que no se produzcan cambios en los archivos del sistema
      - Cambios de propietario, tamaño, permisos, contenido, etc.
      - /etc/tripwire/twpol.txt
    - Configuración y estado actual archivos se cifran con un par de claves
      - Site key
      - Local key
  - ViperDB

Monitorización

- En resumen…



FILTRADO

Introducción
Seguridad perimetral

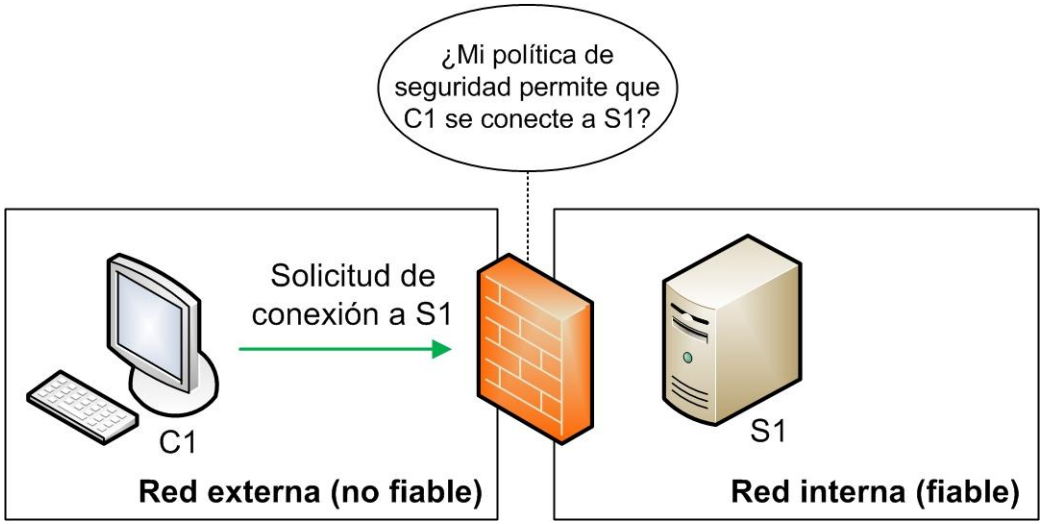
- Arquitectura y elementos de red que proporcionan seguridad a una red interna frente a una red externa (generalmente Internet)
  - Software y servicios
  - Routers
  - VPNs, IDSs, etc.
  - **Firewalls**
  - Etc.
- Los firewalls son el principal "vigilante" de la entrada a un equipo a través de la red

Introducción
Firewalls

- Un firewall (cortafuegos) es cualquier mecanismo, ya sea software o hardware, que filtra el tráfico entre redes
  - Separan zonas de confianza (*trusted zones*) de zonas potencialmente hostiles (*untrusted zones*)
  - Analizan, registran y pueden bloquear el tráfico
  - Deniegan intentos de conexión no autorizados (en ambos sentidos)
    - Se utilizan principalmente para prevenir ataques desde el exterior hacia equipos de una red interna
    - También utilizados para controlar el uso de la red por parte de los equipos internos
  - Pueden actuar en distintas capas del modelo TCP/IP

Introducción
Firewalls

- Escenario básico en el que un firewall controla el acceso de los clientes en una red externa (no fiable) a servidores en una red interna (fiable)



- El tráfico es autorizado o denegado dependiendo de la política de seguridad implementada en el firewall
- Cada dominio de confianza puede incluir una o varias redes

Introducción
Firewalls

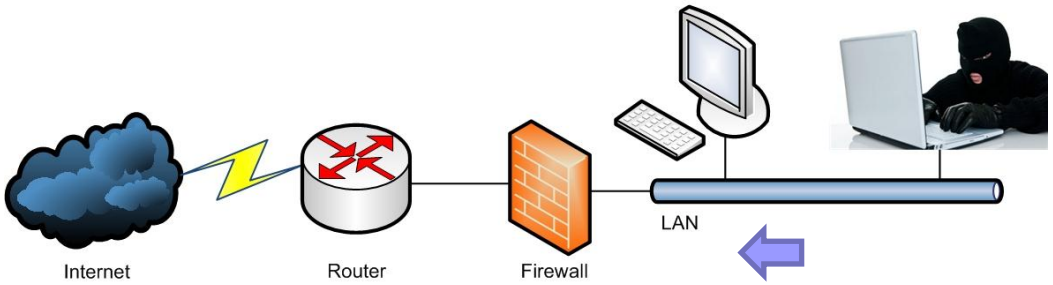
- Idealmente, un firewall debe tener las siguientes características:
  - Todo tráfico de “dentro a fuera” (saliente) y de “fuera a dentro” (entrante) debe pasar a través del firewall
  - Sólo aquel tráfico autorizado, según la política de seguridad (reglas), puede continuar su camino
  - El firewall es completamente inatacable
- Ningún firewall cumple estos requisitos al 100%, pero todos tratan de acercarse a ellos

Introducción
Firewalls

- Ventajas
  - Primera línea de defensa frente a ataques
    - Mantienen a usuarios no autorizados fuera de la red protegida
    - Prohíben el uso de servicios potencialmente vulnerables (e.g. telnet, SMTP, etc.)
    - Permiten la salida desde el interior
  - Punto único para implantar una política de seguridad
  - Punto único para realizar análisis y monitorización del tráfico
    - Registro de accesos, intentos de intrusión, gestión de alarmas de seguridad, auditorías, etc.

Introducción
Firewalls

- Limitaciones
  - No protegen contra ataques que no pasen por el firewall
    - Desde red interna a red interna
      - Ej.: Amenazas internas: usuarios negligentes o malintencionados (wifi mal protegida, copia de datos en memorias USB, virus en memorias USB, etc.)



    - Desde red externa a red interna sin pasar por el firewall
      - Ej.: Conexiones wifi, móviles, módems, etc.

Introducción
Firewalls

- El uso de un firewall debe ser siempre parte de una política de seguridad global

¡De nada sirve tener una puerta blindada si dejo las ventanas abiertas!

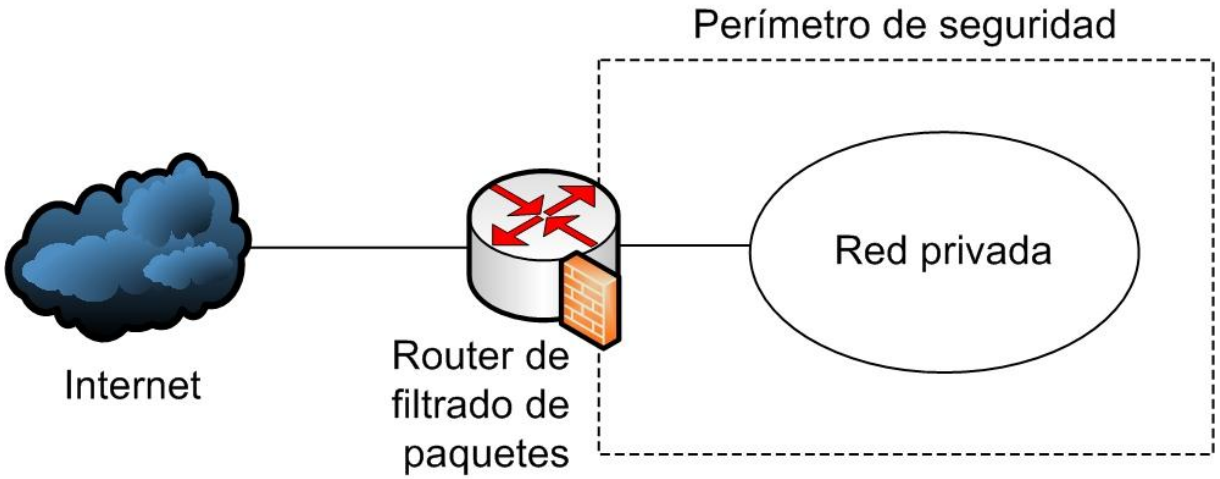
TIPOS DE FIREWALLS

Tipos de firewalls

- **Filtrado de paquetes** (*packet filtering*)
  - Filtrado estático o sin estado (*stateless*)
  - Filtrado dinámico o con estado *(stateful*)

- **Filtrado a nivel de aplicación**
  - Proxy

Tipos de firewalls
Filtrado de paquetes



- Router de filtrado de paquetes
  - Aplica un conjunto de reglas a cada paquete IP y retransmite o descarta dicho paquete
  - Normalmente, se configura para filtrar paquetes que van en ambas direcciones (desde y hacia red interna)

Tipos de firewalls

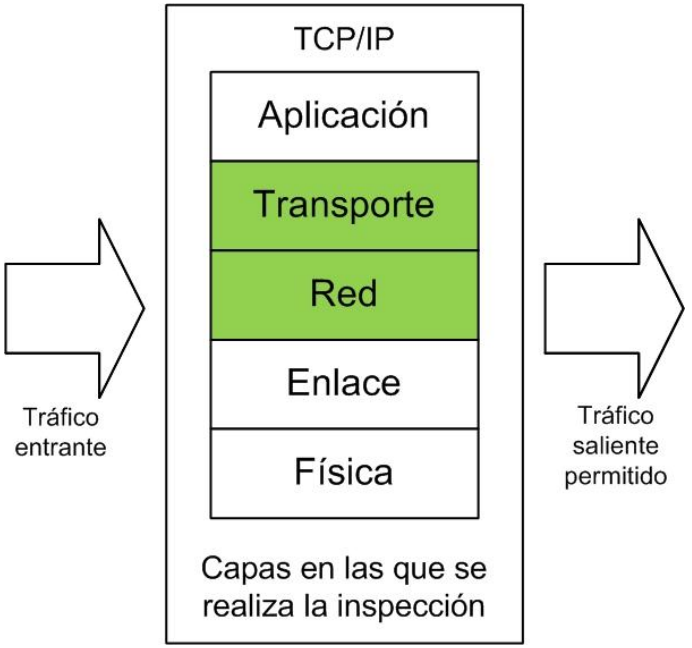
- **Filtrado de paquetes** (*packet filtering*)
  - Filtrado estático o sin estado (*stateless*)
  - Filtrado dinámico o con estado *(stateful*)

- **Filtrado a nivel de aplicación**
  - Proxy

Tipos de firewalls

Filtrado estático de paquetes (stateless)

- Generalmente operan en las capas 3 (red) y 4 (transporte)
- Las reglas de filtrado se basan en información contenida en el paquete de red
  - **Direcciones IP** de origen y destino (ej.: 192.168.1.1)
  - **Números de puerto** de origen y destino (ej.: 23, 80, etc.)
  - **Tipo de tráfico** (TCP, UDP, ICMP)



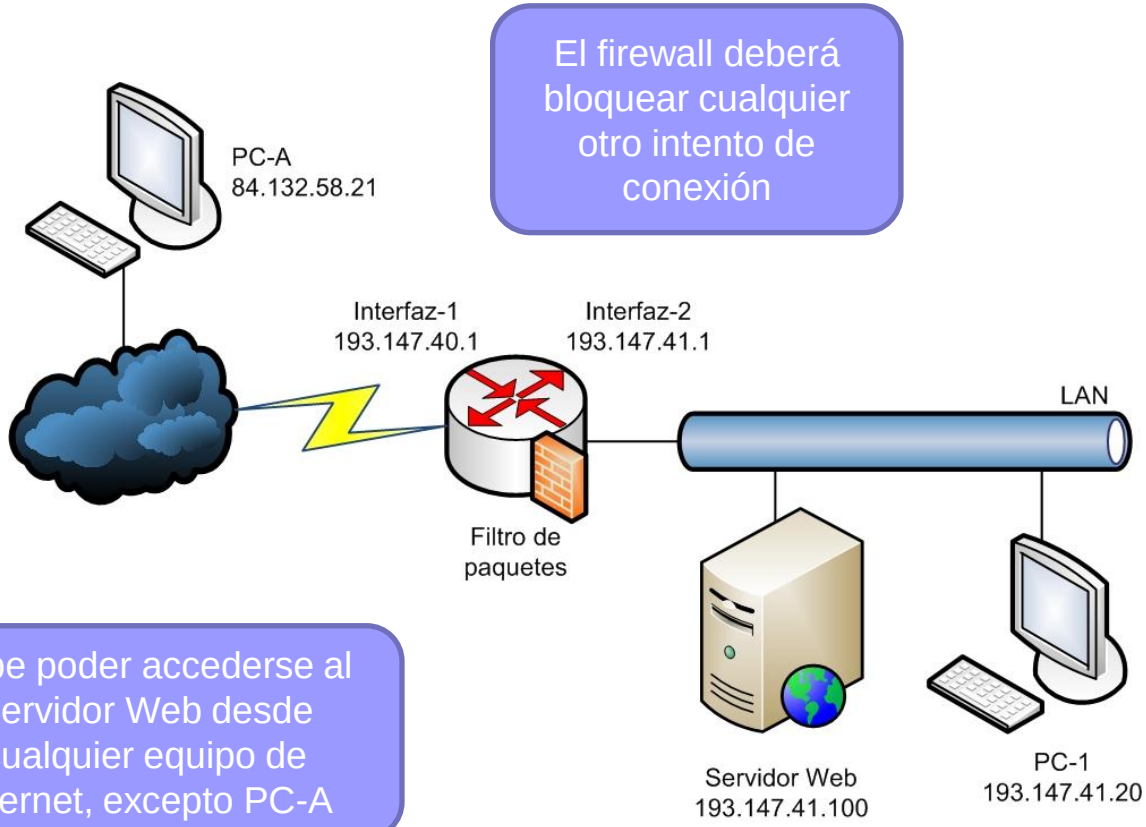
Tipos de firewalls

Filtrado estático de paquetes (stateless)

- No almacenan información del contexto
  - Se decide acerca de cada paquete individualmente
- Se configuran como una lista de reglas basadas en correspondencias con los campos de la cabecera IP o TCP
  - Si hay una correspondencia en una de las reglas, se invoca la regla para determinar si el paquete se retransmite o se descarta
  - Si no hay correspondencias, se realiza una acción predeterminada:
    - Descartar por defecto
      - Todo lo que no está expresamente permitido está prohibido
      - Más seguridad, mayor "molestia" para los usuarios finales
    - Retransmitir por defecto
      - Todo lo que no está expresamente prohibido está permitido
      - Más comodidad, escasa seguridad. El administrador debe reaccionar ante nuevas amenazas a medida que se van descubriendo

Tipos de firewalls
Filtrado estático de paquetes (stateless)

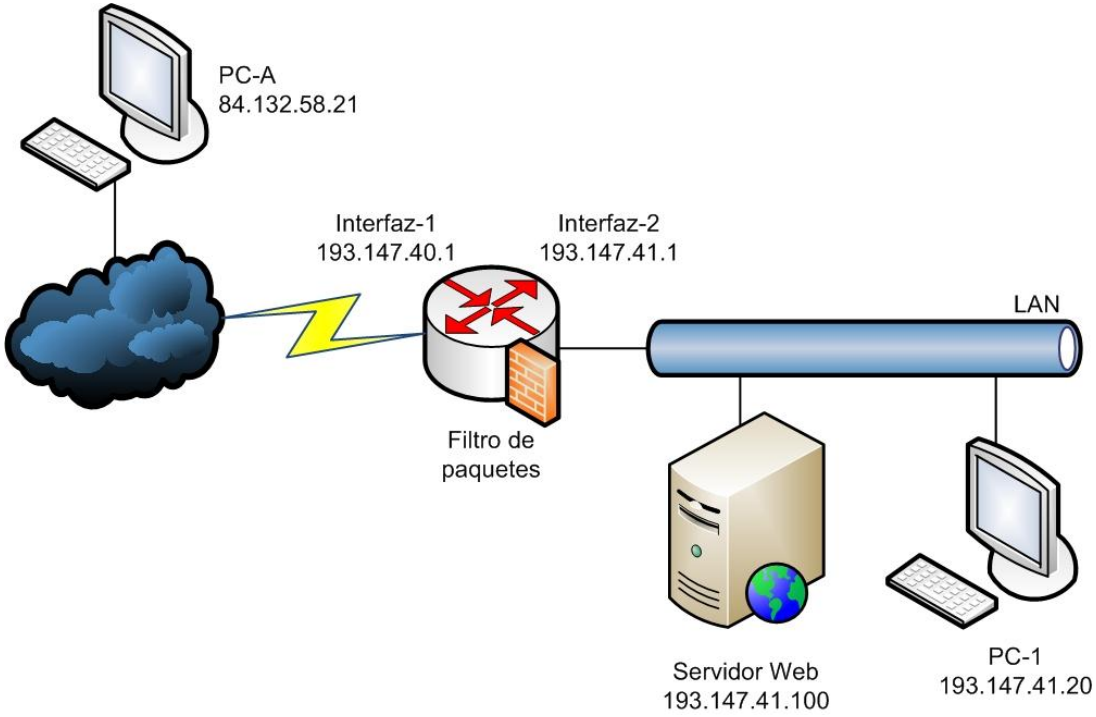
- Ejemplos de aplicación de reglas en el siguiente escenario:



Tipos de firewalls

Filtrado estático de paquetes (stateless)

Debe poder accederse al Servidor Web desde cualquier equipo de Internet, excepto PC-A



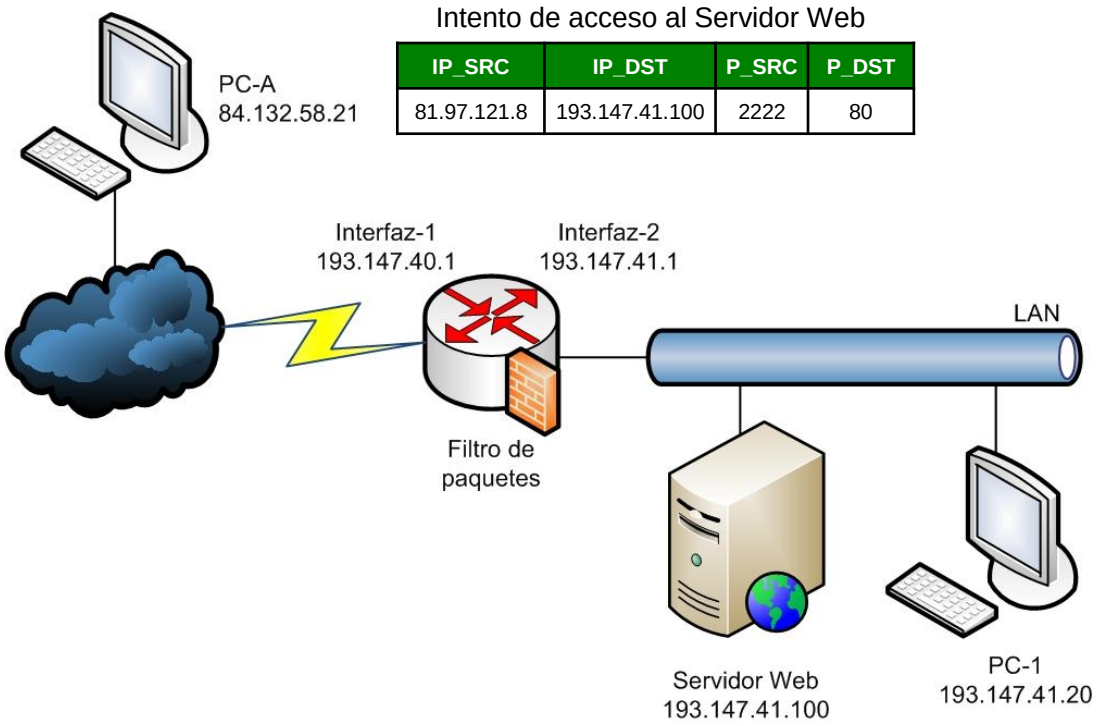
¿Estas reglas son suficientes?

acción	origen	puerto	destino	puerto
bloquear	84.132.58.21	*	*	*
permitir	*	*	193.147.41.100	80
bloquear	*	*	*	*

Tipos de firewalls

Filtrado estático de paquetes (stateless)

Debe poder accederse al Servidor Web desde cualquier equipo de Internet, excepto PC-A

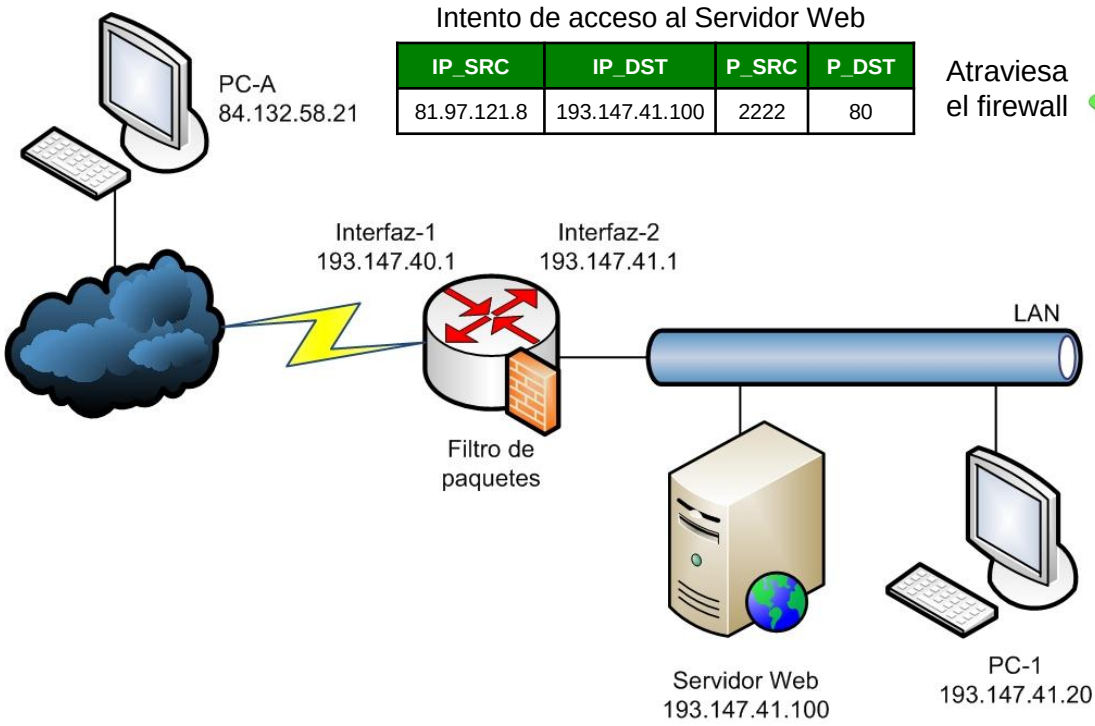


acción	origen	puerto	destino	puerto
bloquear	84.132.58.21	*	*	*
permitir	*	*	193.147.41.100	80
bloquear	*	*	*	*

Tipos de firewalls

Filtrado estático de paquetes (stateless)

Debe poder accederse al Servidor Web desde cualquier equipo de Internet, excepto PC-A

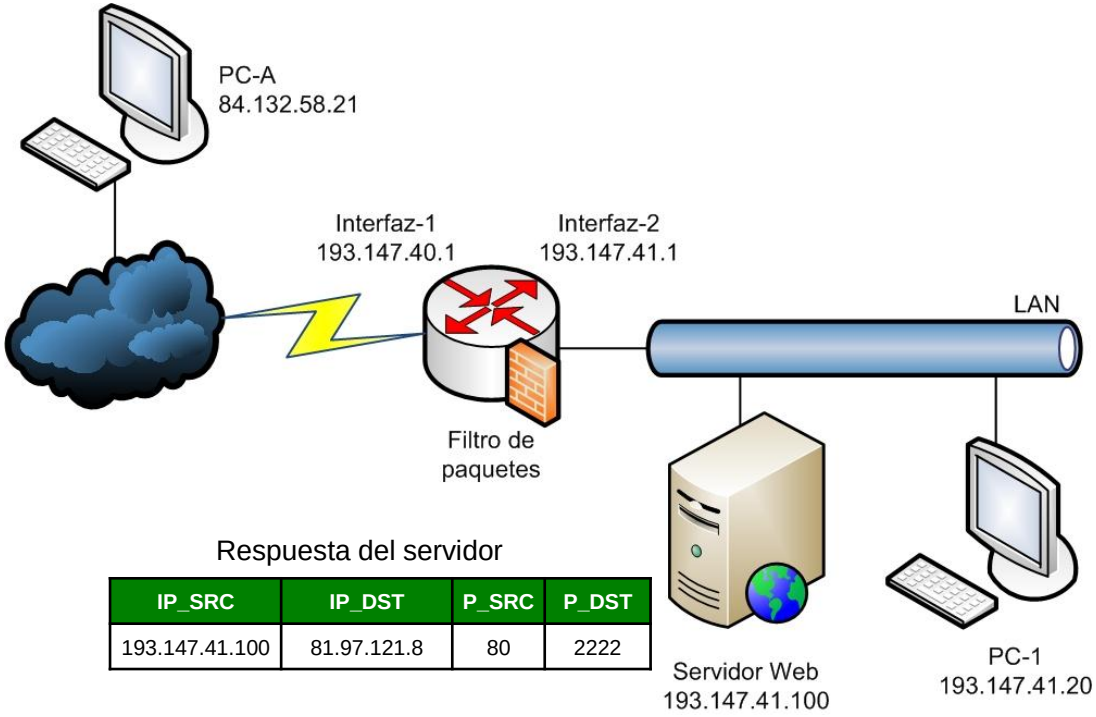


acción	origen	puerto	destino	puerto
bloquear	84.132.58.21	*	*	*
permitir	*	*	193.147.41.100	80
bloquear	*	*	*	*

Tipos de firewalls

Filtrado estático de paquetes (stateless)

Debe poder accederse al Servidor Web desde cualquier equipo de Internet, excepto PC-A



Respuesta del servidor

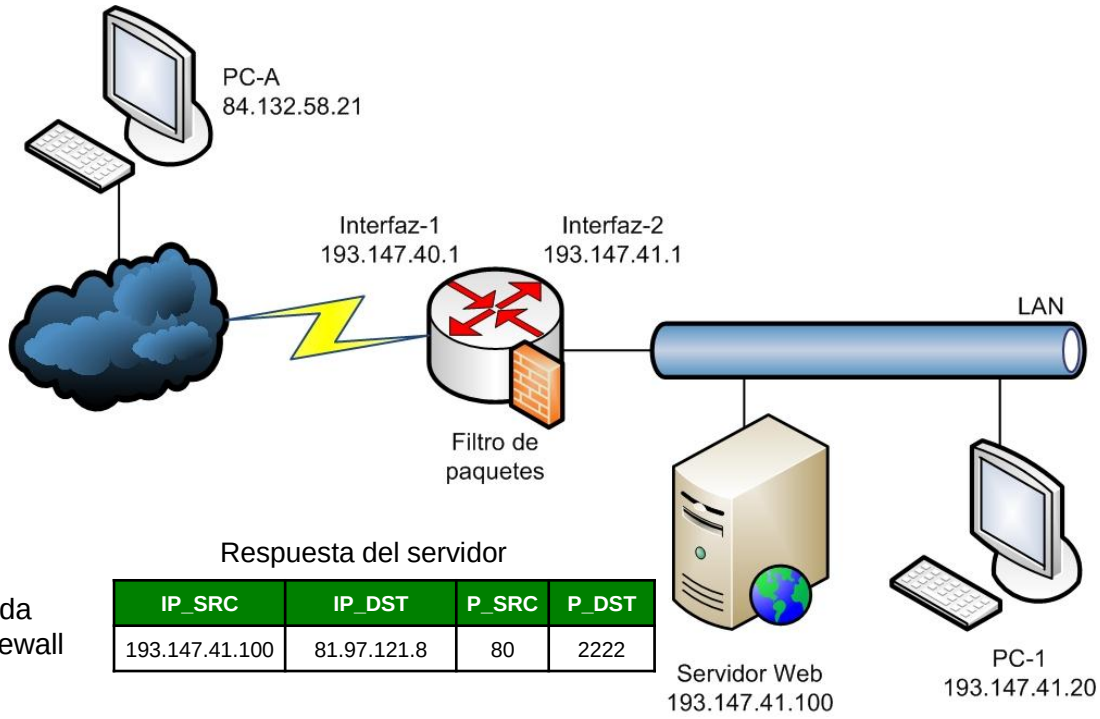
IP_SRC	IP_DST	P_SRC	P_DST
193.147.41.100	81.97.121.8	80	2222

acción	origen	puerto	destino	puerto
bloquear	84.132.58.21	*	*	*
permitir	*	*	193.147.41.100	80
bloquear	*	*	*	*

Tipos de firewalls

Filtrado estático de paquetes (stateless)

Debe poder accederse al Servidor Web desde cualquier equipo de Internet, excepto PC-A



Bloqueada por el firewall

Respuesta del servidor

IP_SRC	IP_DST	P_SRC	P_DST
193.147.41.100	81.97.121.8	80	2222

acción	origen	puerto	destino	puerto
bloquear	84.132.58.21	*	*	*
permitir	*	*	193.147.41.100	80
bloquear	*	*	*	*

Tipos de firewalls

Filtrado estático de paquetes (stateless)

- ¿Cómo lo solucionamos?
  - Nueva regla para permitir paquetes procedentes del Servidor Web, con puerto de origen 80 y puerto de destino superior a 1023

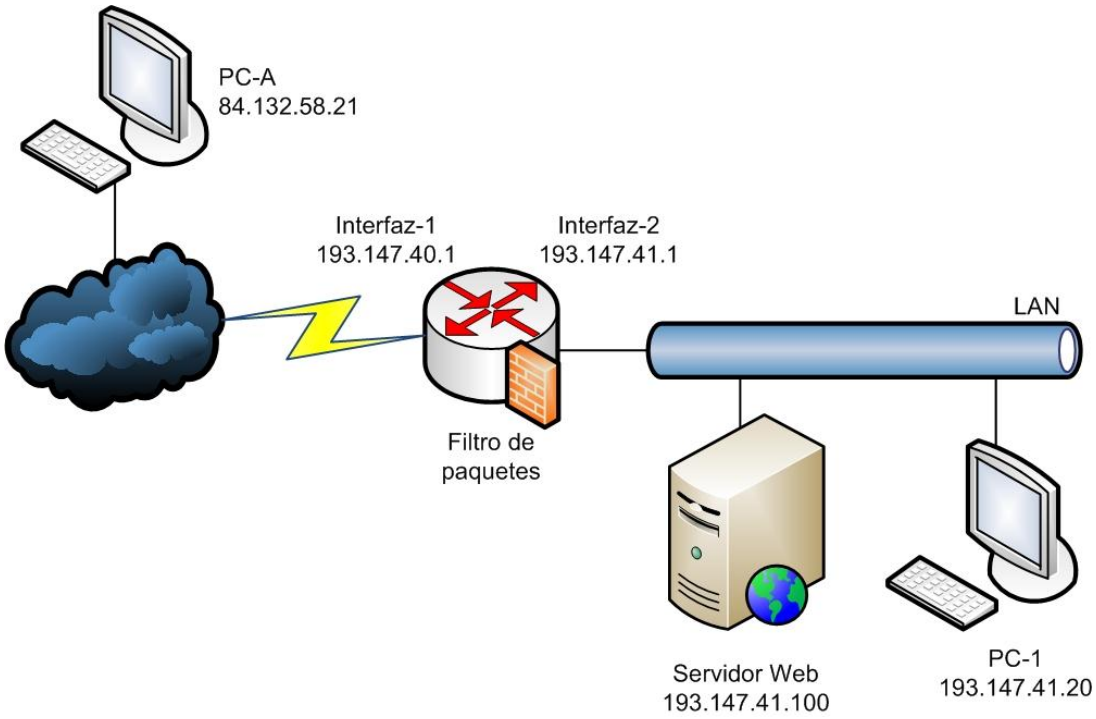
acción	origen	puerto	destino	puerto
bloquear	84.132.58.21	*	*	*
permitir	*	*	193.147.41.100	80
permitir	193.147.41.100	80	*	>1023
bloquear	*	*	*	*

Tipos de firewalls

Filtrado estático de paquetes (stateless)

Debe poder accederse al Servidor Web desde cualquier equipo de Internet, excepto PC-A

PC-1 debe disponer de acceso a Internet



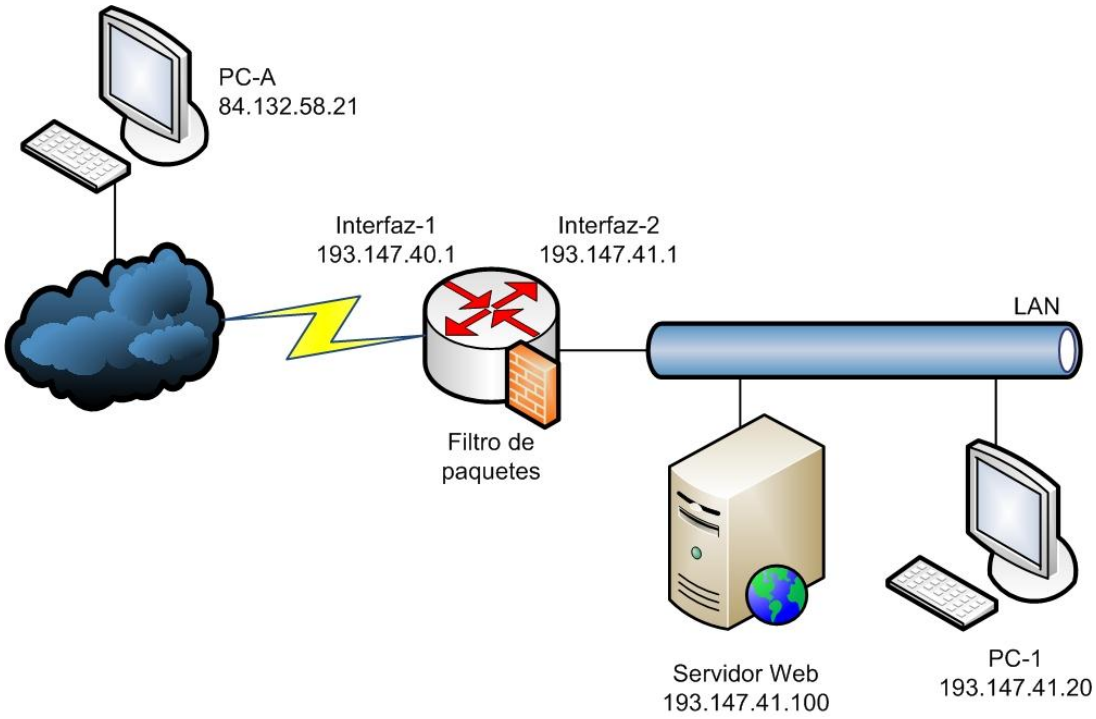
acción	origen	puerto	destino	puerto
bloquear	84.132.58.21	*	*	*
permitir	*	*	193.147.41.100	80
permitir	193.147.41.100	80	*	>1023
bloquear	*	*	*	*

Tipos de firewalls

Filtrado estático de paquetes (stateless)

Debe poder accederse al Servidor Web desde cualquier equipo de Internet, excepto PC-A

PC-1 debe disponer de acceso a Internet



acción	origen	puerto	destino	puerto
bloquear	84.132.58.21	*	*	*
permitir	*	*	193.147.41.100	80
permitir	193.147.41.100	80	*	>1023
permitir	193.147.41.20	*	*	80
bloquear	*	*	*	*

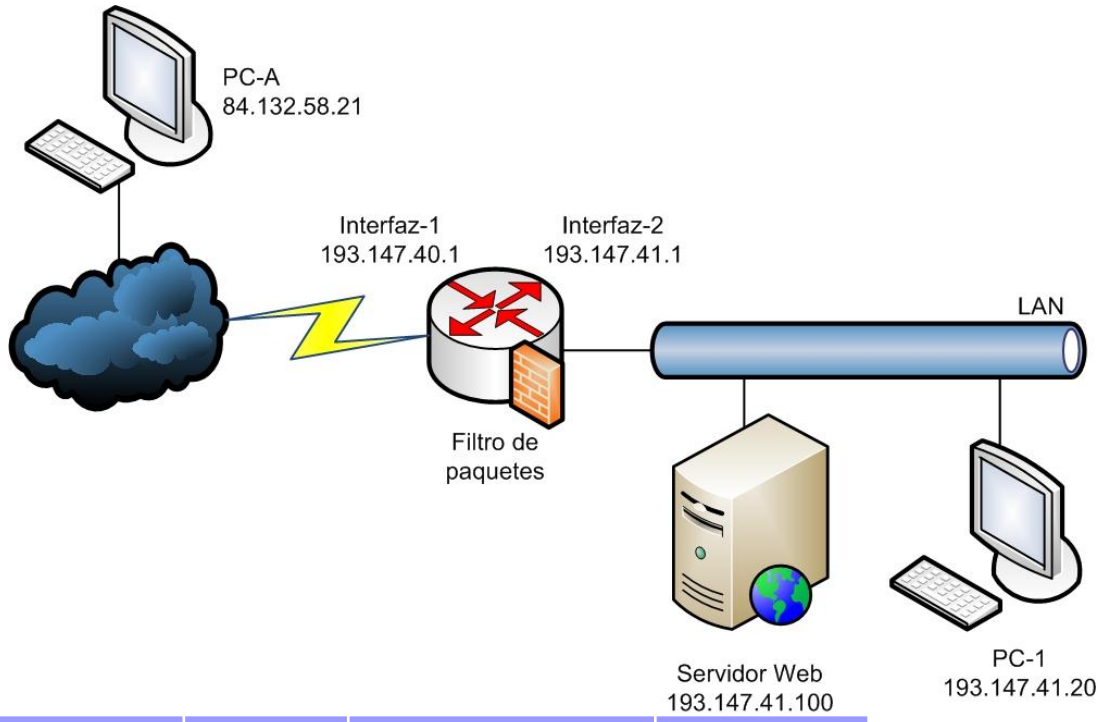
Salida

Tipos de firewalls

Filtrado estático de paquetes (stateless)

Debe poder accederse al Servidor Web desde cualquier equipo de Internet, excepto PC-A

PC-1 debe disponer de acceso a Internet



acción	origen	puerto	destino	puerto
bloquear	84.132.58.21	*	*	*
permitir	*	*	193.147.41.100	80
permitir	193.147.41.100	80	*	>1023
permitir	193.147.41.20	*	*	80
permitir	*	80	193.147.41.20	>1023
bloquear	*	*	*	*

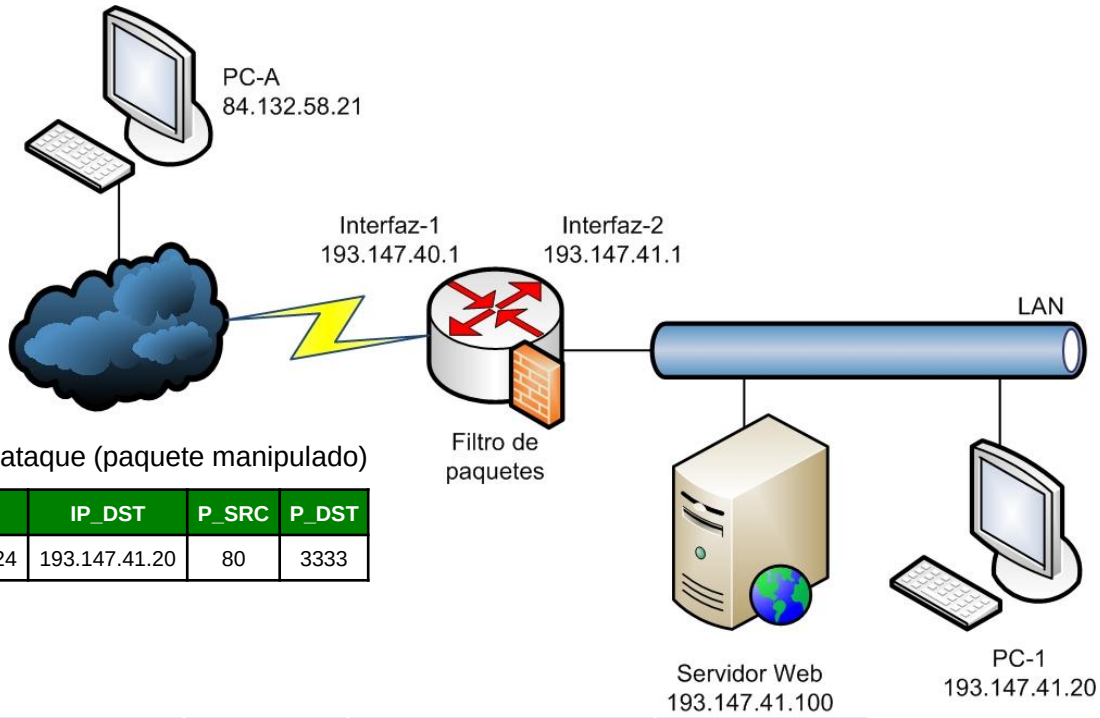
Entrada

Tipos de firewalls

Filtrado estático de paquetes (stateless)

Debe poder accederse al Servidor Web desde cualquier equipo de Internet, excepto PC-A

PC-1 debe disponer de acceso a Internet



Intento de ataque (paquete manipulado)

IP_SRC	IP_DST	P_SRC	P_DST
130.206.192.24	193.147.41.20	80	3333

Problema

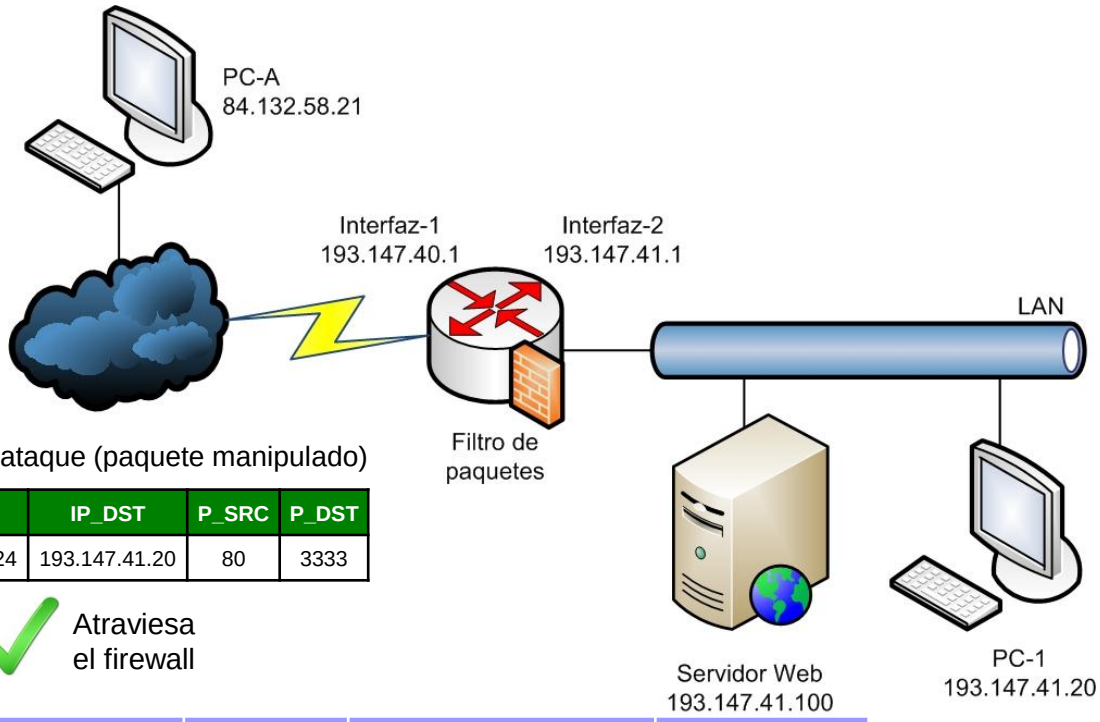
acción	origen	puerto	destino	puerto
bloquear	84.132.58.21	*	*	*
permitir	*	*	193.147.41.100	80
permitir	193.147.41.100	80	*	>1023
permitir	193.147.41.20	*	*	80
permitir	*	80	193.147.41.20	>1023
bloquear	*	*	*	*

Tipos de firewalls

Filtrado estático de paquetes (stateless)

Debe poder accederse al Servidor Web desde cualquier equipo de Internet, excepto PC-A

PC-1 debe disponer de acceso a Internet



Problema

Intento de ataque (paquete manipulado)

IP_SRC	IP_DST	P_SRC	P_DST
130.206.192.24	193.147.41.20	80	3333

Atraviesa el firewall

acción	origen	puerto	destino	puerto
bloquear	84.132.58.21	*	*	*
permitir	*	*	193.147.41.100	80
permitir	193.147.41.100	80	*	>1023
permitir	193.147.41.20	*	*	80
permitir	*	80	193.147.41.20	>1023
bloquear	*	*	*	*

Tipos de firewalls

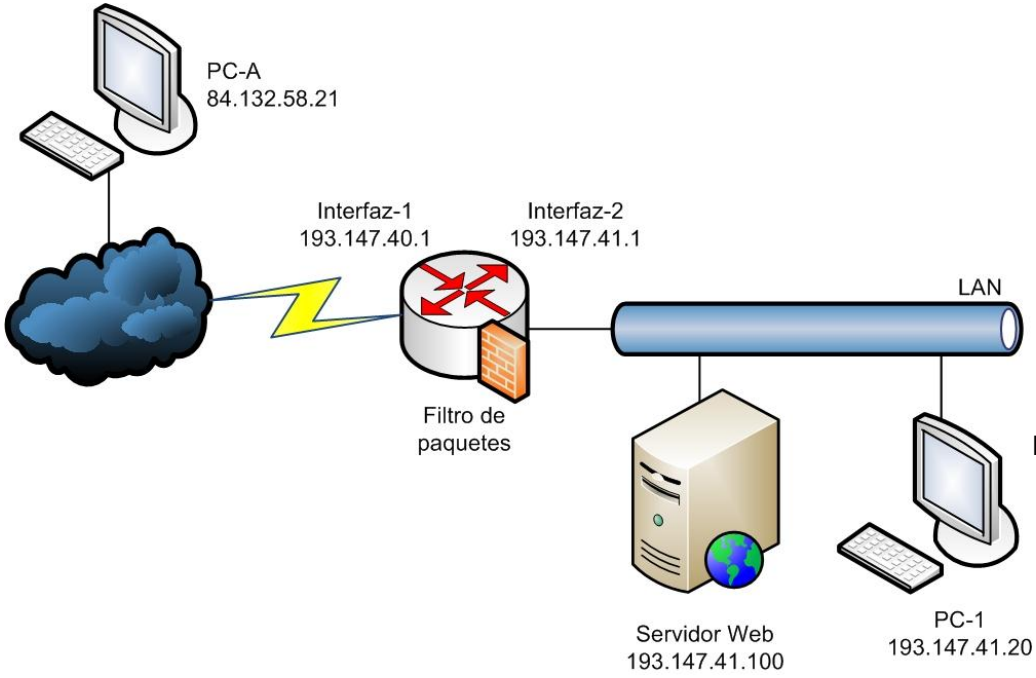
Filtrado estático de paquetes (stateless)

- Problema: no podemos distinguir una respuesta legítima de un intento de ataque
- ¿Cómo podemos solucionarlo?
  - Beneficiándonos de los indicadores proporcionados por las conexiones TCP, podemos diferenciar entre paquetes que inician una conexión (SYN, !ACK) y paquetes que pertenecen a una conexión ya establecida (ACK)
    - Indicador ACK: una vez que se ha establecido una conexión, se activa el indicador ACK del segmento TCP para reconocer los segmentos enviados desde el otro lado
    - Aceptar paquetes procedentes del puerto 80 de cualquier equipo, originados como respuesta a alguna llamada

acción	origen	puerto	destino	puerto	Indicador
permitir	*	80	193.147.41.20	*	ACK

Tipos de firewalls

Filtrado estático de paquetes (stateless)



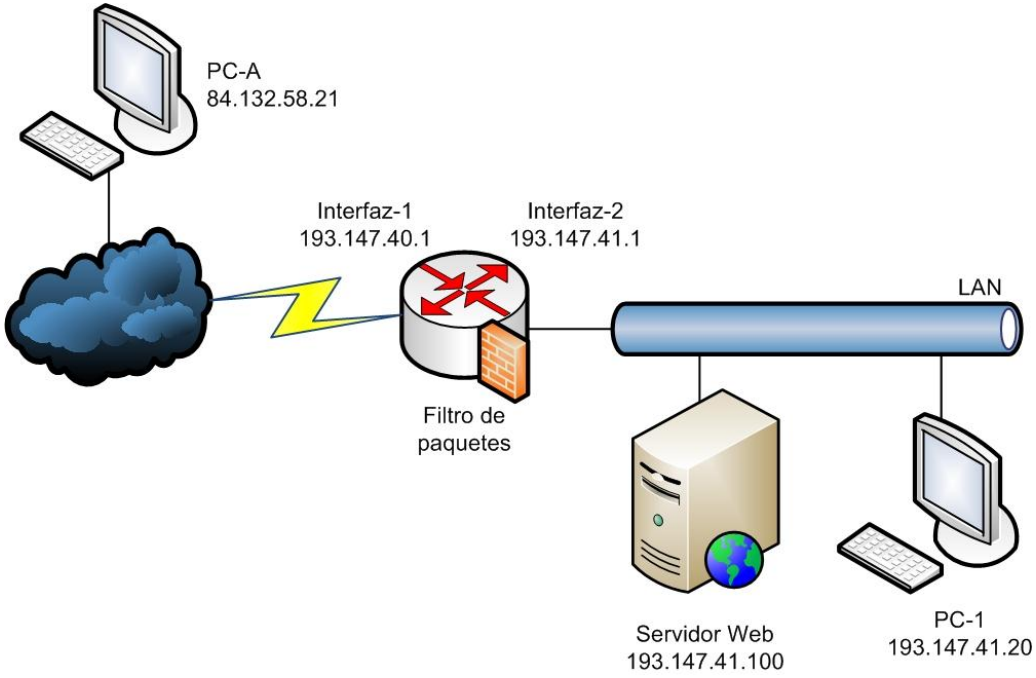
Intento de acceso a Servidor Web externo

IP_SRC	IP_DST	P_SRC	P_DST
193.147.41.20	130.206.192.24	3333	80

acción	origen	puerto	destino	puerto	Indicador
permitir	193.147.41.20	*	*	80	
permitir	*	80	193.147.41.20	*	ACK

Tipos de firewalls

Filtrado estático de paquetes (stateless)



Atraviesa
el firewall

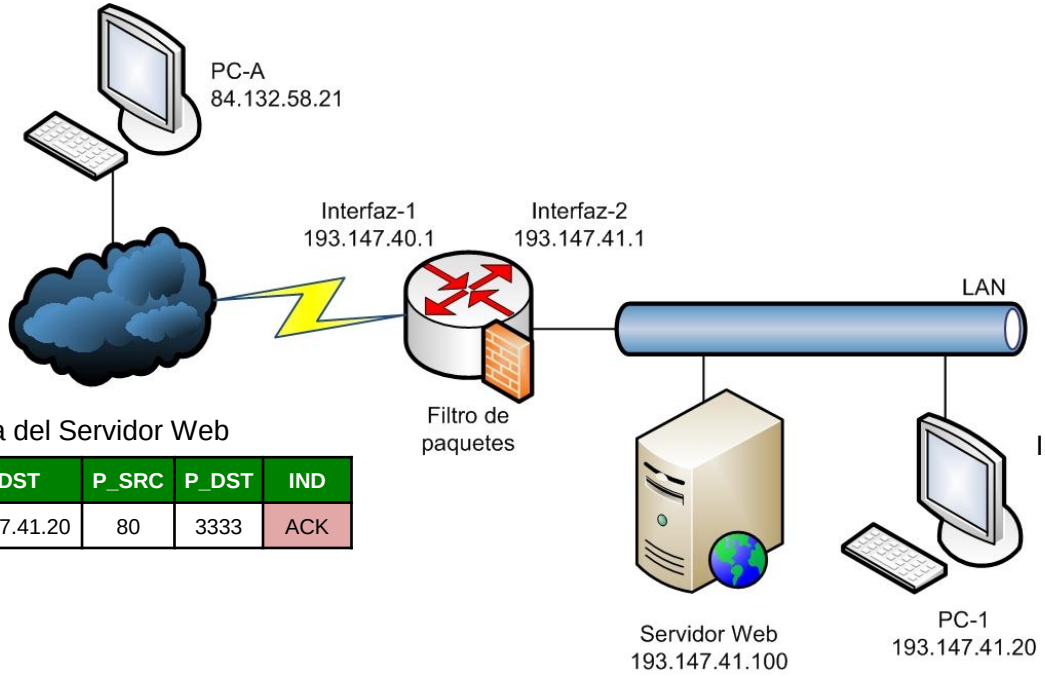
Intento de acceso a Servidor Web externo

IP_SRC	IP_DST	P_SRC	P_DST
193.147.41.20	130.206.192.24	3333	80

acción	origen	puerto	destino	puerto	Indicador
permitir	193.147.41.20	*	*	80	
permitir	*	80	193.147.41.20	*	ACK

Tipos de firewalls

Filtrado estático de paquetes (stateless)



Atraviesa
el firewall

Respuesta del Servidor Web

IP_SRC	IP_DST	P_SRC	P_DST	IND
130.206.192.24	193.147.41.20	80	3333	ACK

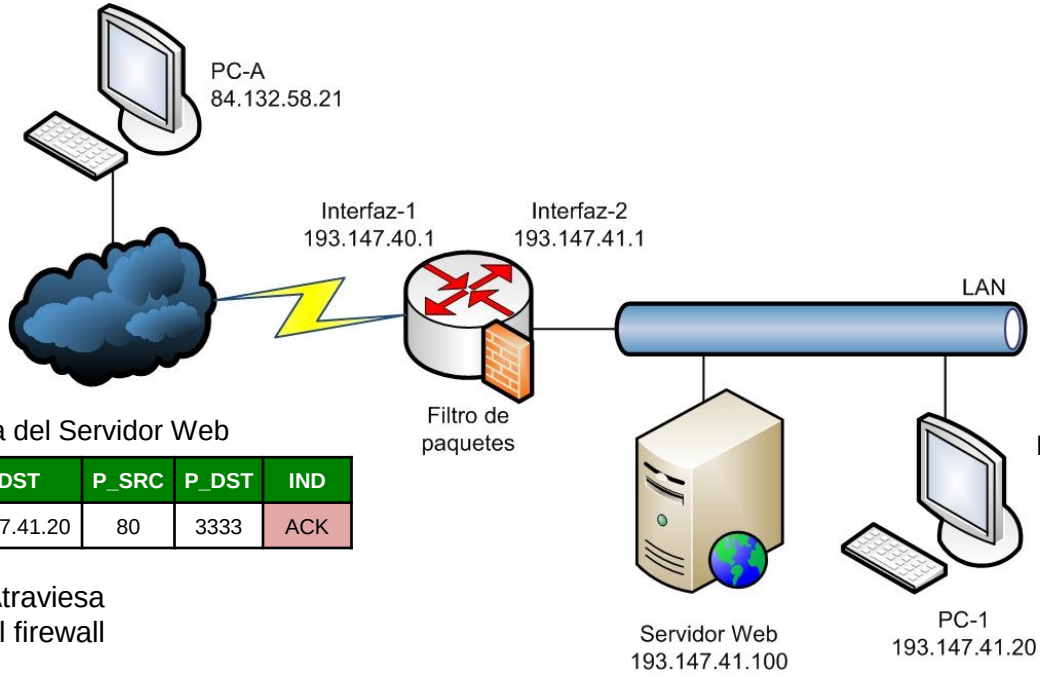
Intento de acceso a Servidor Web externo

IP_SRC	IP_DST	P_SRC	P_DST
193.147.41.20	130.206.192.24	3333	80

acción	origen	puerto	destino	puerto	Indicador
permitir	193.147.41.20	*	*	80	
permitir	*	80	193.147.41.20	*	ACK

Tipos de firewalls

Filtrado estático de paquetes (stateless)



Respuesta del Servidor Web

IP_SRC	IP_DST	P_SRC	P_DST	IND
130.206.192.24	193.147.41.20	80	3333	ACK

Atraviesa el firewall

Atraviesa el firewall

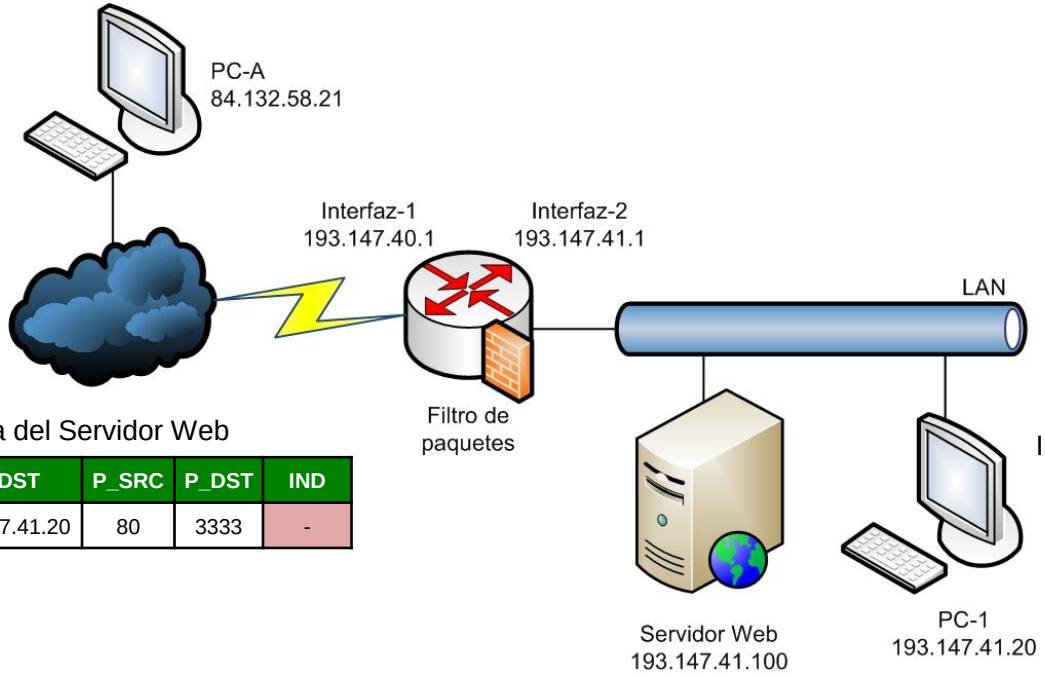
Intento de acceso a Servidor Web externo

IP_SRC	IP_DST	P_SRC	P_DST
193.147.41.20	130.206.192.24	3333	80

acción	origen	puerto	destino	puerto	Indicador
permitir	193.147.41.20	*	*	80	
permitir	*	80	193.147.41.20	*	ACK

Tipos de firewalls

Filtrado estático de paquetes (stateless)



Atraviesa
el firewall

Respuesta del Servidor Web

IP_SRC	IP_DST	P_SRC	P_DST	IND
130.206.192.24	193.147.41.20	80	3333	-

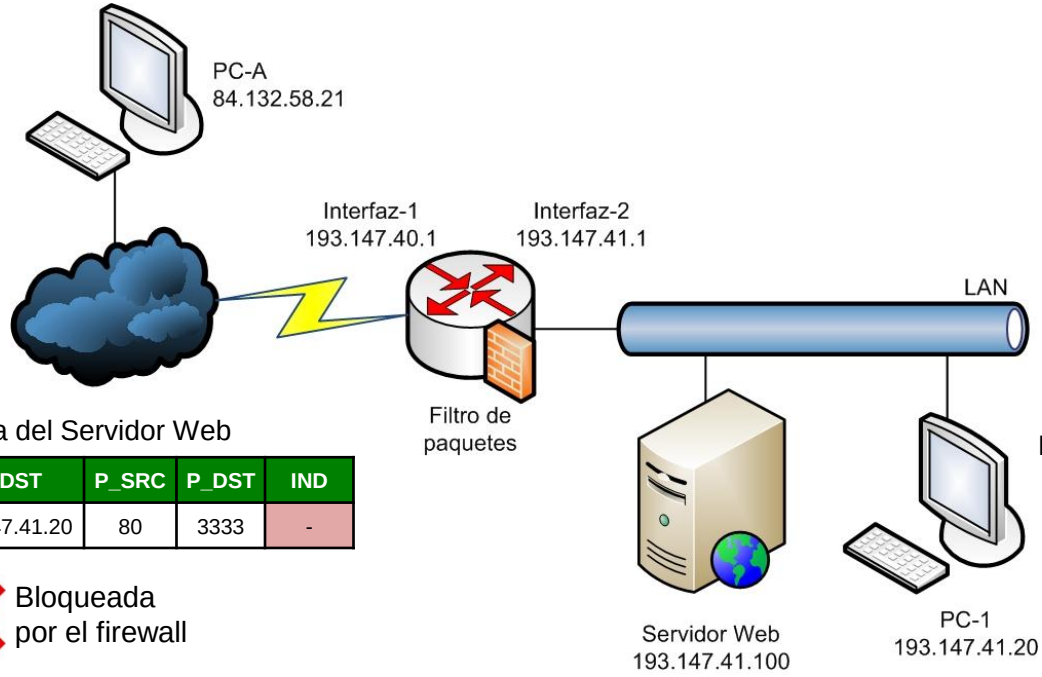
Intento de acceso a Servidor Web externo

IP_SRC	IP_DST	P_SRC	P_DST
193.147.41.20	130.206.192.24	3333	80

acción	origen	puerto	destino	puerto	Indicador
permitir	193.147.41.20	*	*	80	
permitir	*	80	193.147.41.20	*	ACK

Tipos de firewalls

Filtrado estático de paquetes (stateless)



Respuesta del Servidor Web

IP_SRC	IP_DST	P_SRC	P_DST	IND
130.206.192.24	193.147.41.20	80	3333	-

Bloqueada
por el firewall

Atraviesa
el firewall

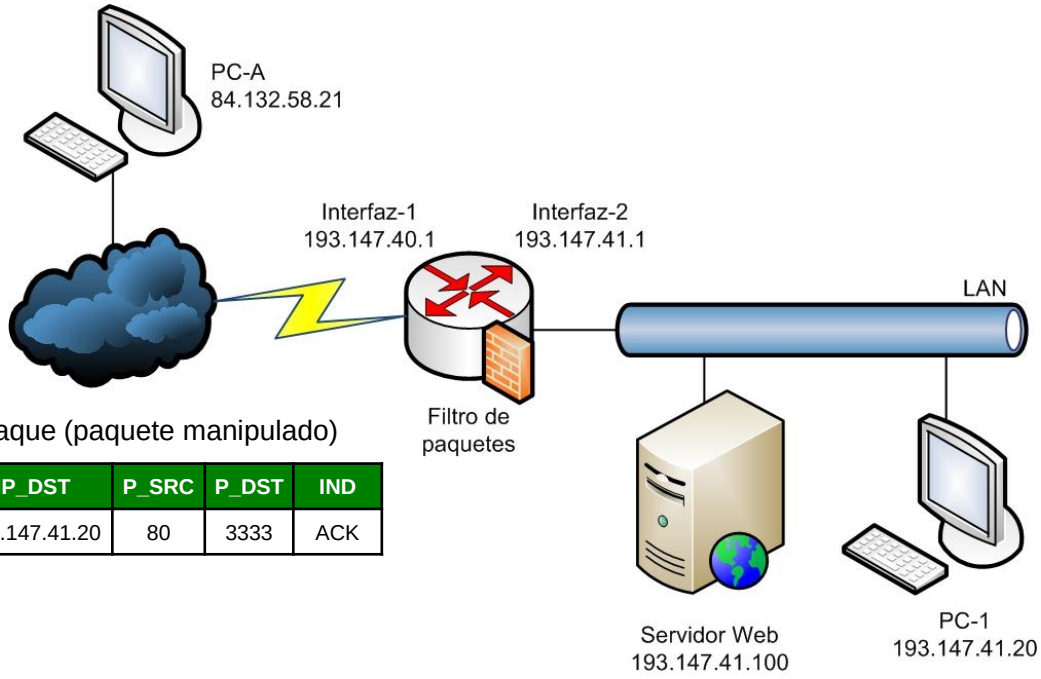
Intento de acceso a Servidor Web externo

IP_SRC	IP_DST	P_SRC	P_DST
193.147.41.20	130.206.192.24	3333	80

acción	origen	puerto	destino	puerto	Indicador
permitir	193.147.41.20	*	*	80	
permitir	*	80	193.147.41.20	*	ACK

Tipos de firewalls
Filtrado estático de paquetes (stateless)

- Problema: El indicador ACK también se puede manipular



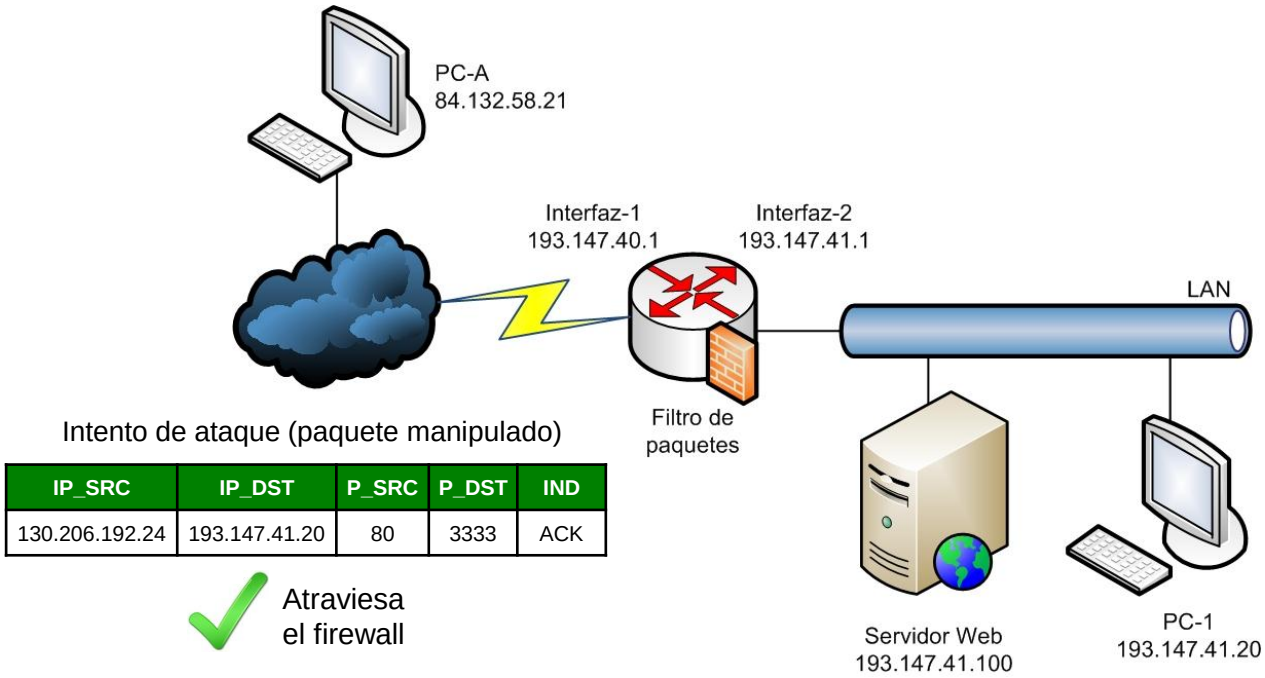
Intento de ataque (paquete manipulado)

IP_SRC	IP_DST	P_SRC	P_DST	IND
130.206.192.24	193.147.41.20	80	3333	ACK

acción	origen	puerto	destino	puerto	Indicador
permitir	193.147.41.20	*	*	80	
permitir	*	80	193.147.41.20	*	ACK

Tipos de firewalls
Filtrado estático de paquetes (stateless)

- Problema: El indicador ACK también se puede manipular



acción	origen	puerto	destino	puerto	Indicador
permitir	193.147.41.20	*	*	80	
permitir	*	80	193.147.41.20	*	ACK

Tipos de firewalls

Filtrado estático de paquetes (stateless)

- Los firewalls de filtrado estático de paquetes deciden sobre cada paquete individualmente, no tienen en cuenta información del contexto en el que se envía el paquete
  - No podemos distinguir entre una respuesta legítima y un ataque
- Continuamos teniendo el mismo problema, podemos recibir ataques mediante paquetes manipulados
- Solución:
  - el firewall debe conocer **el estado de la conexión**

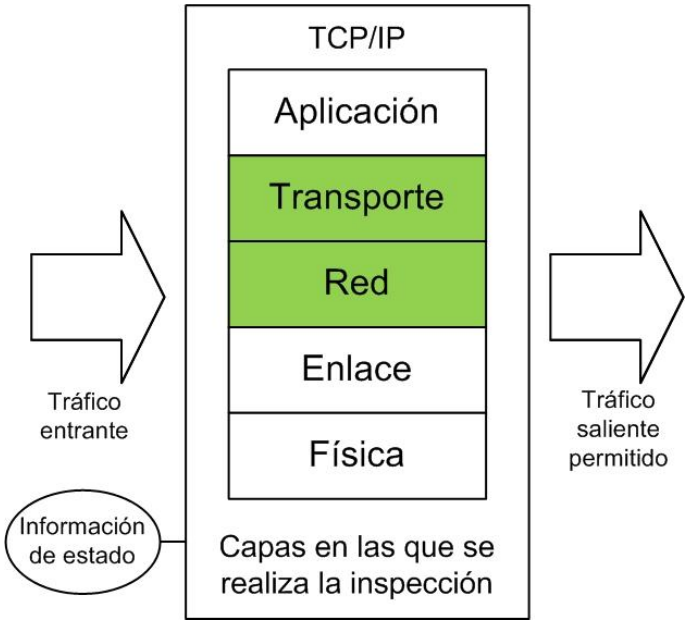
Tipos de firewalls

- **Filtrado de paquetes** (*packet filtering*)
  - Filtrado estático o sin estado (*stateless*)
  - Filtrado dinámico o con estado *(stateful)*

- **Filtrado a nivel de aplicación**
  - Proxy

Tipos de firewalls
Filtrado dinámico de paquetes (stateful)

- También llamados firewalls de inspección de estado o con estado
- Los paquetes se analizan dentro de un contexto
- Mantienen una tabla con el estado de las conexiones activas
  - Una entrada por cada conexión actualmente establecida
  - Se permitirá el tráfico para aquellos paquetes que encajan en el perfil de alguna de las conexiones establecidas



Tipos de firewalls

Filtrado dinámico de paquetes (stateful)

- Ejemplo de tabla de estado de conexiones de un firewall de filtrado dinámico

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.22.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
2122.22.123.32	2112	192.168.1.6	80	Established
210.922.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Tipos de firewalls
Filtrado dinámico de paquetes (stateful)

- Problema anterior: Paquete manipulado que no ha sido originado a raíz de una llamada desde nuestra red

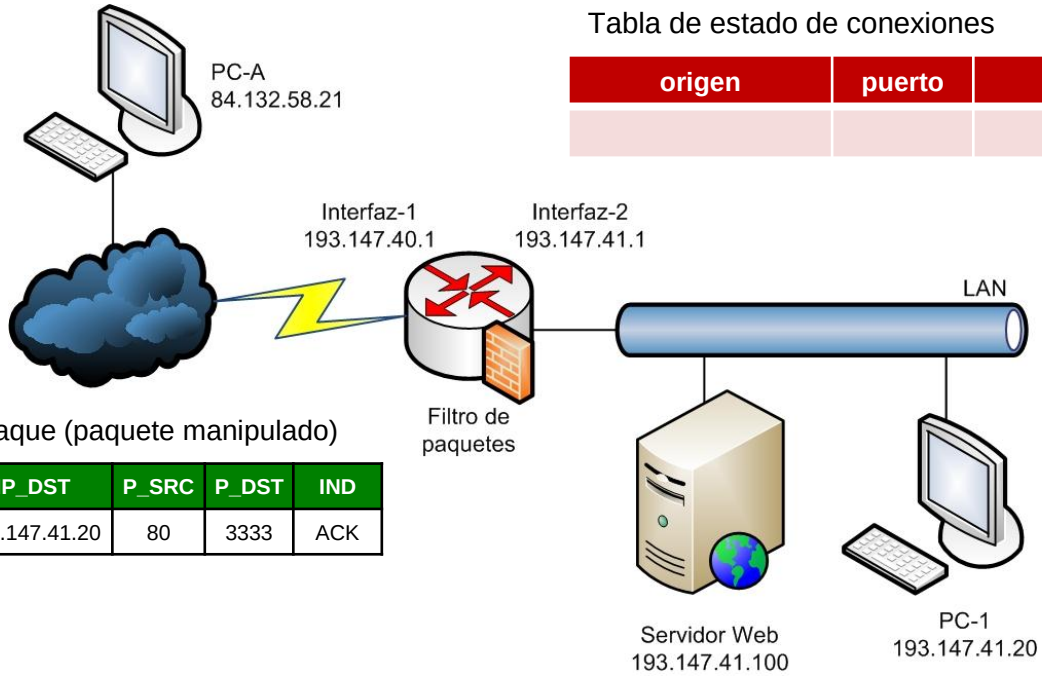


Tabla de estado de conexiones

origen	puerto	destino	puerto

Intento de ataque (paquete manipulado)

IP_SRC	IP_DST	P_SRC	P_DST	IND
130.206.192.24	193.147.41.20	80	3333	ACK

Reglas

acción	origen	puerto	destino	puerto
permitir	193.147.41.20	*	*	80

Tipos de firewalls
Filtrado dinámico de paquetes (stateful)

- Problema anterior: Paquete manipulado que no ha sido originado a raíz de una llamada desde nuestra red

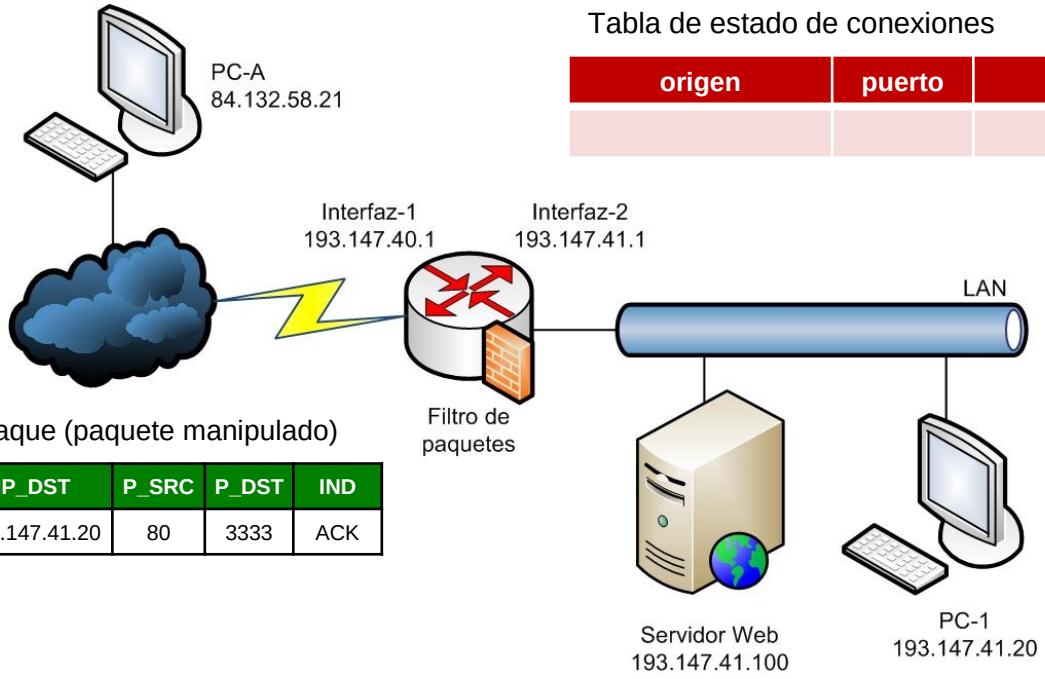


Tabla de estado de conexiones

origen	puerto	destino	puerto

Se revisa la tabla de conexiones para ver si el paquete se corresponde con una conexión establecida

Intento de ataque (paquete manipulado)

IP_SRC	IP_DST	P_SRC	P_DST	IND
130.206.192.24	193.147.41.20	80	3333	ACK

Reglas

acción	origen	puerto	destino	puerto
permitir	193.147.41.20	*	*	80

Tipos de firewalls
Filtrado dinámico de paquetes (stateful)

- Problema anterior: Paquete manipulado que no ha sido originado a raíz de una llamada desde nuestra red

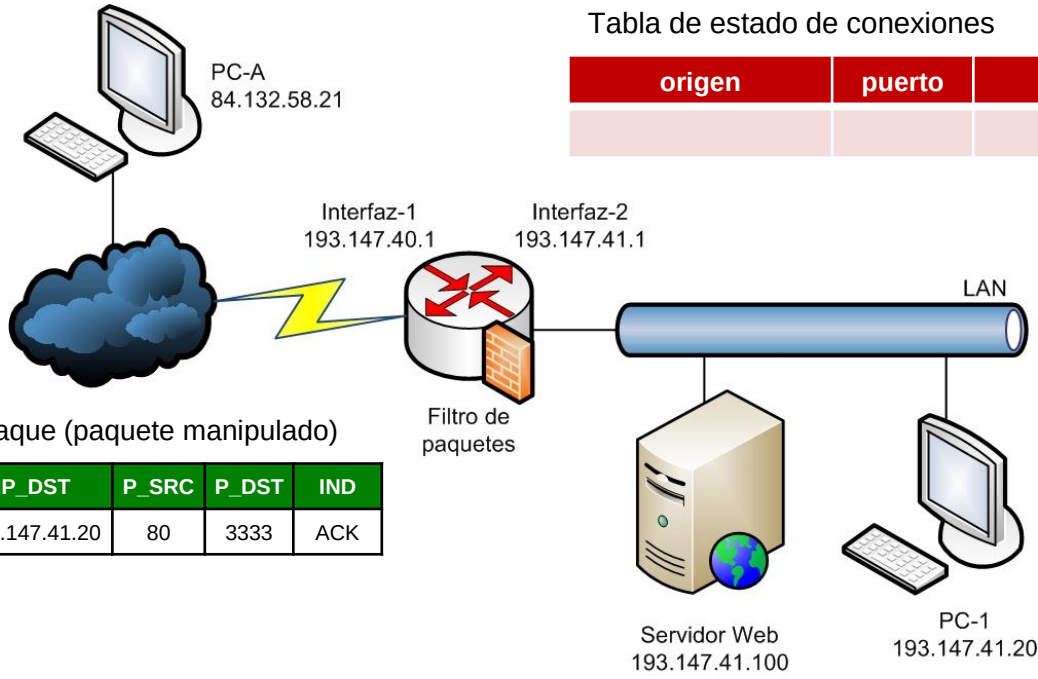


Tabla de estado de conexiones

origen	puerto	destino	puerto

Intento de ataque (paquete manipulado)

IP_SRC	IP_DST	P_SRC	P_DST	IND
130.206.192.24	193.147.41.20	80	3333	ACK

Después, se revisan las reglas

Reglas

acción	origen	puerto	destino	puerto
permitir	193.147.41.20	*	*	80

Tipos de firewalls
Filtrado dinámico de paquetes (stateful)

- Problema anterior: Paquete manipulado que no ha sido originado a raíz de una llamada desde nuestra red

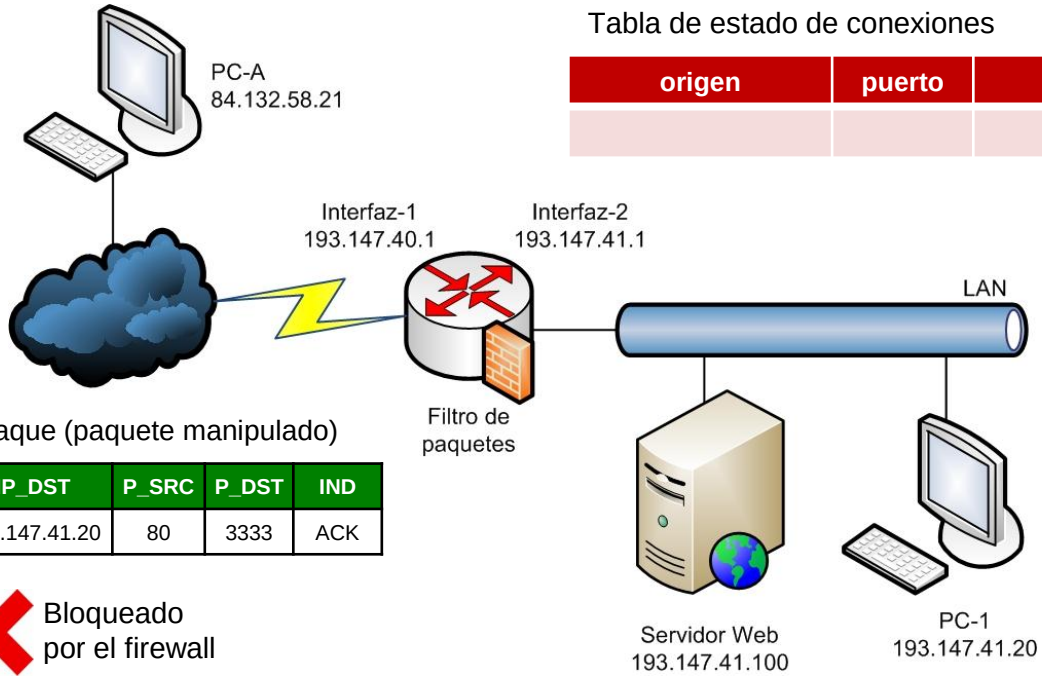


Tabla de estado de conexiones

origen	puerto	destino	puerto

Intento de ataque (paquete manipulado)

IP_SRC	IP_DST	P_SRC	P_DST	IND
130.206.192.24	193.147.41.20	80	3333	ACK

Bloqueado
por el firewall

Reglas

acción	origen	puerto	destino	puerto
permitir	193.147.41.20	*	*	80

Tipos de firewalls

Filtrado dinámico de paquetes (stateful)

PC-1 debe disponer de acceso a Internet

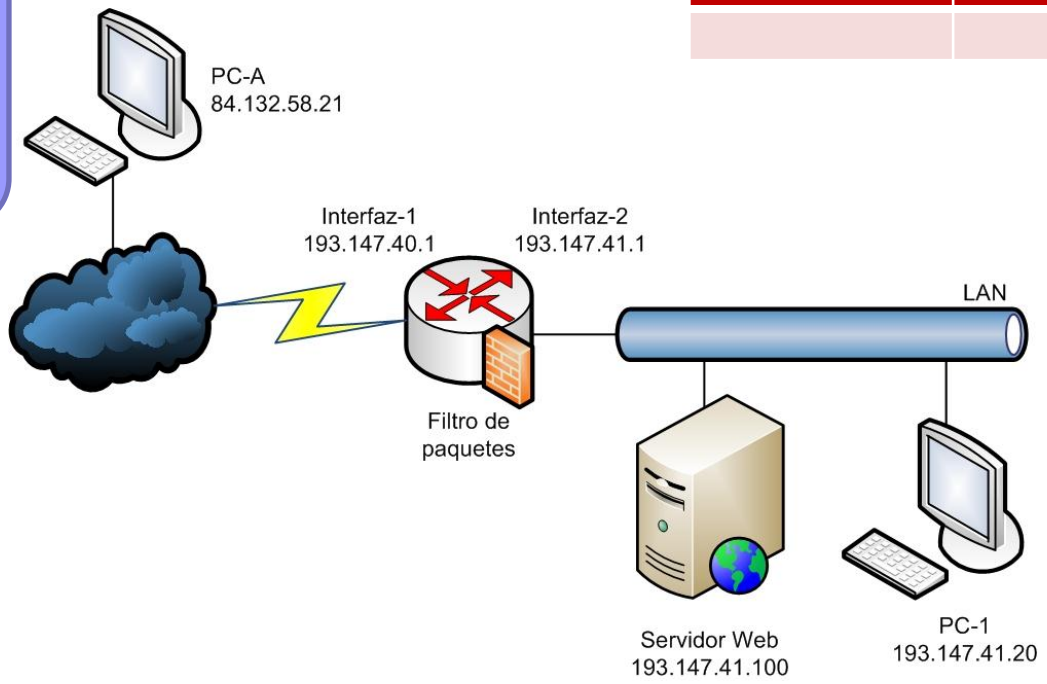


Tabla de estado de conexiones

origen	puerto	destino	puerto

Acceso a Servidor Web externo

IP_SRC	IP_DST	P_SRC	P_DST
193.147.41.20	130.206.192.24	3333	80

Reglas

acción	origen	puerto	destino	puerto
permitir	193.147.41.20	*	*	80

Tipos de firewalls

Filtrado dinámico de paquetes (stateful)

PC-1 debe disponer de acceso a Internet

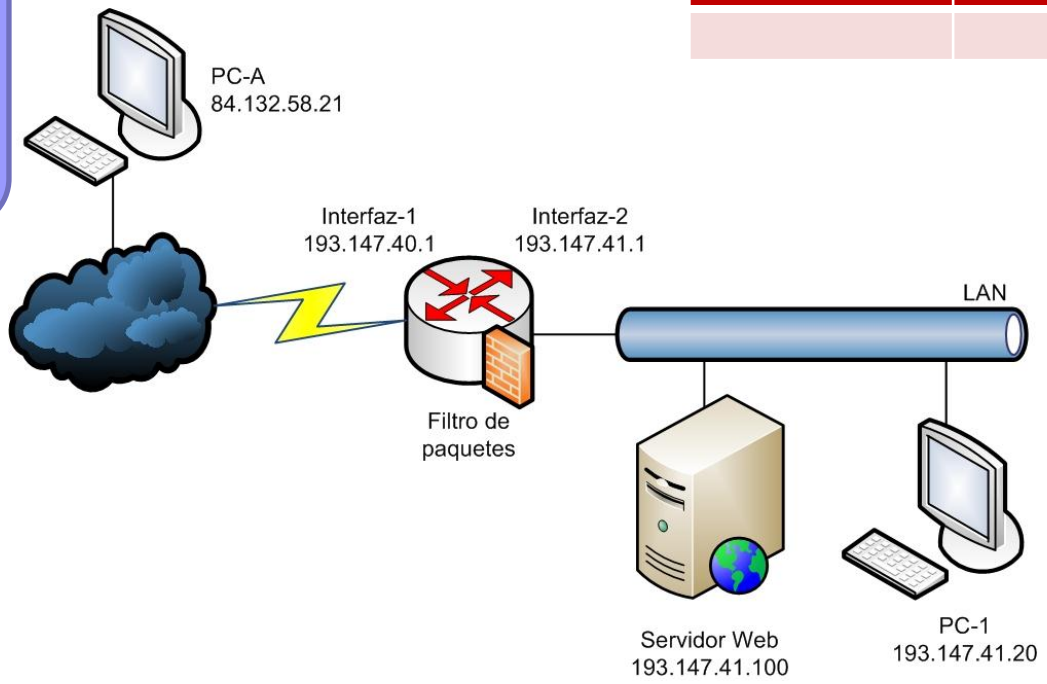


Tabla de estado de conexiones

origen	puerto	destino	puerto

Acceso a Servidor Web externo

IP_SRC	IP_DST	P_SRC	P_DST
193.147.41.20	130.206.192.24	3333	80

Atraviesa el firewall

Reglas

acción	origen	puerto	destino	puerto
permitir	193.147.41.20	*	*	80

Tipos de firewalls

Filtrado dinámico de paquetes (stateful)

Se guarda el estado de la conexión

PC-1 debe disponer de acceso a Internet

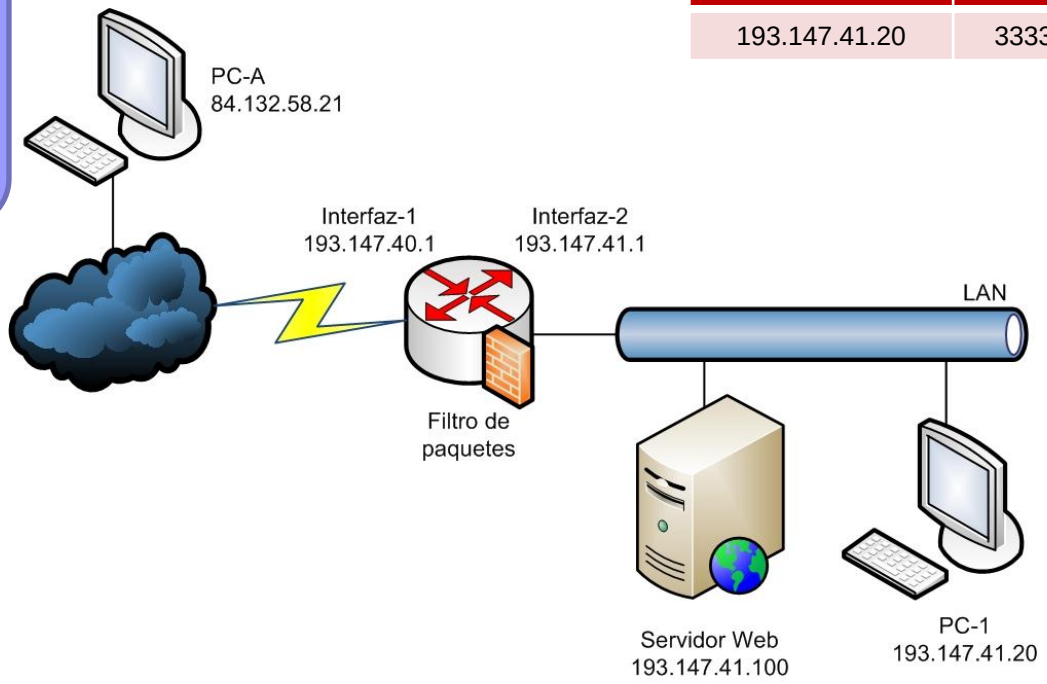


Tabla de estado de conexiones

origen	puerto	destino	puerto
193.147.41.20	3333	130.206.192.24	80

Acceso a Servidor Web externo

IP_SRC	IP_DST	P_SRC	P_DST
193.147.41.20	130.206.192.24	3333	80

Atraviesa el firewall

Reglas

acción	origen	puerto	destino	puerto
permitir	193.147.41.20	*	*	80

Tipos de firewalls

Filtrado dinámico de paquetes (stateful)

PC-1 debe disponer de acceso a Internet

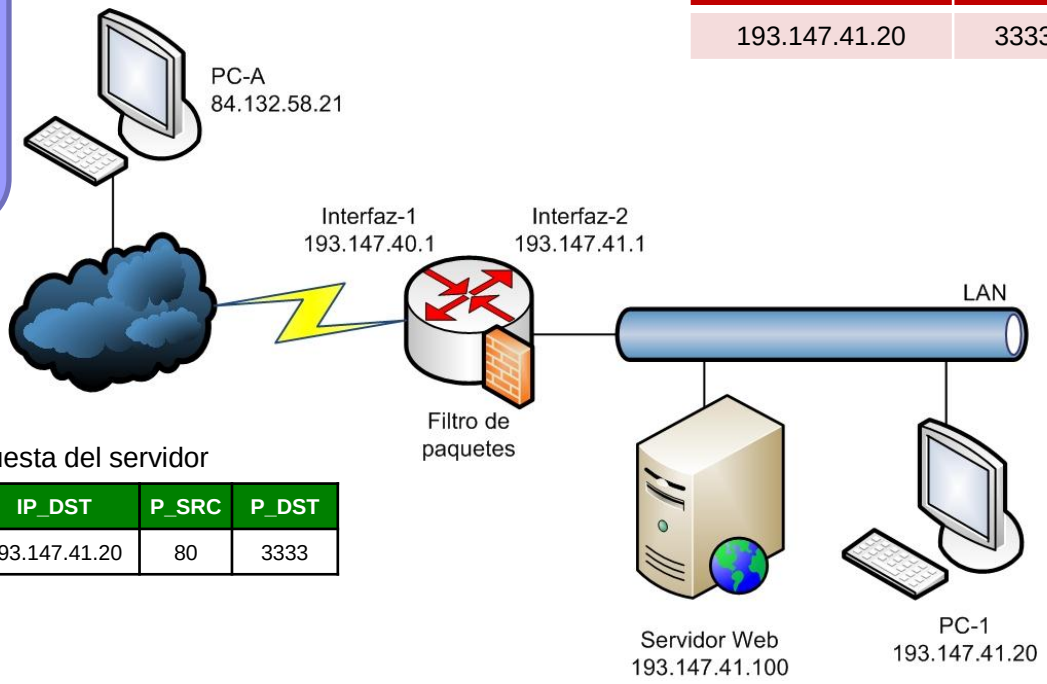


Tabla de estado de conexiones

origen	puerto	destino	puerto
193.147.41.20	3333	130.206.192.24	80

Respuesta del servidor

IP_SRC	IP_DST	P_SRC	P_DST
130.206.192.24	193.147.41.20	80	3333

Reglas

acción	origen	puerto	destino	puerto
permitir	193.147.41.20	*	*	80

Tipos de firewalls

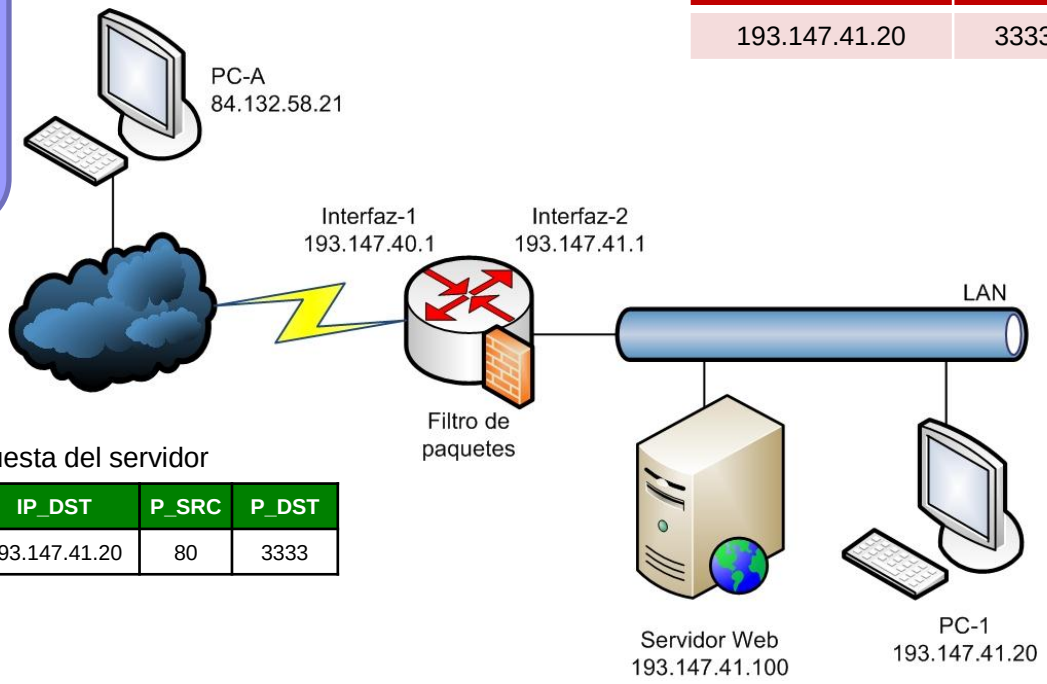
Filtrado dinámico de paquetes (stateful)

Se trata de una respuesta a una conexión activa

PC-1 debe disponer de acceso a Internet

Tabla de estado de conexiones

origen	puerto	destino	puerto
193.147.41.20	3333	130.206.192.24	80



Respuesta del servidor

IP_SRC	IP_DST	P_SRC	P_DST
130.206.192.24	193.147.41.20	80	3333

Reglas

acción	origen	puerto	destino	puerto
permitir	193.147.41.20	*	*	80

Tipos de firewalls

Filtrado dinámico de paquetes (stateful)

PC-1 debe disponer de acceso a Internet

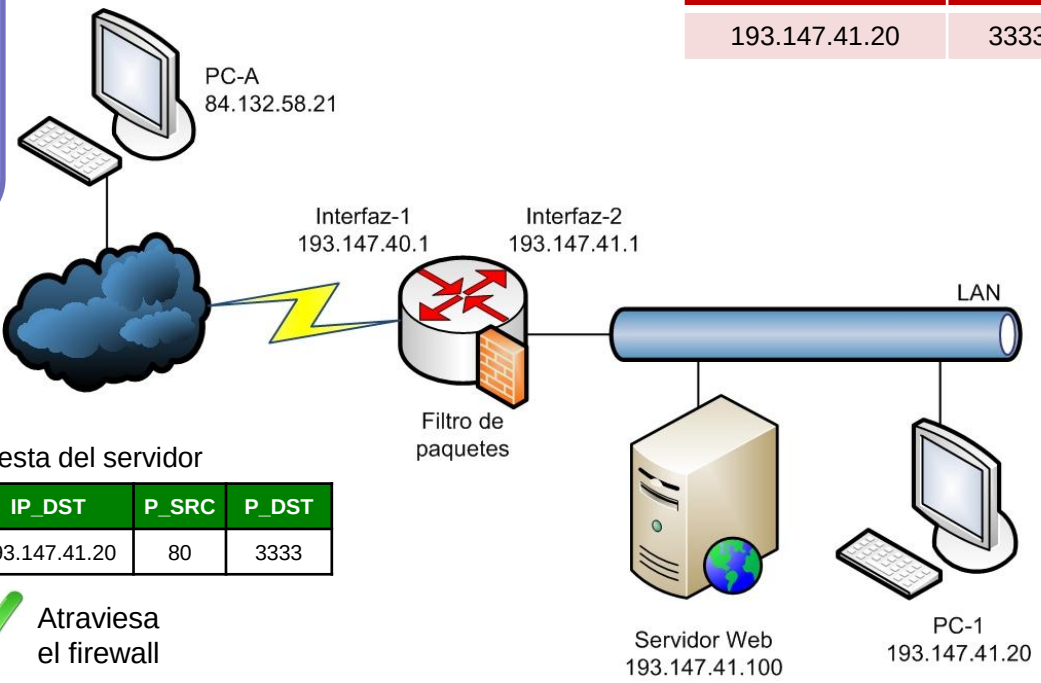


Tabla de estado de conexiones

origen	puerto	destino	puerto
193.147.41.20	3333	130.206.192.24	80

Respuesta del servidor

IP_SRC	IP_DST	P_SRC	P_DST
130.206.192.24	193.147.41.20	80	3333

Atraviesa el firewall

Reglas

acción	origen	puerto	destino	puerto
permitir	193.147.41.20	*	*	80

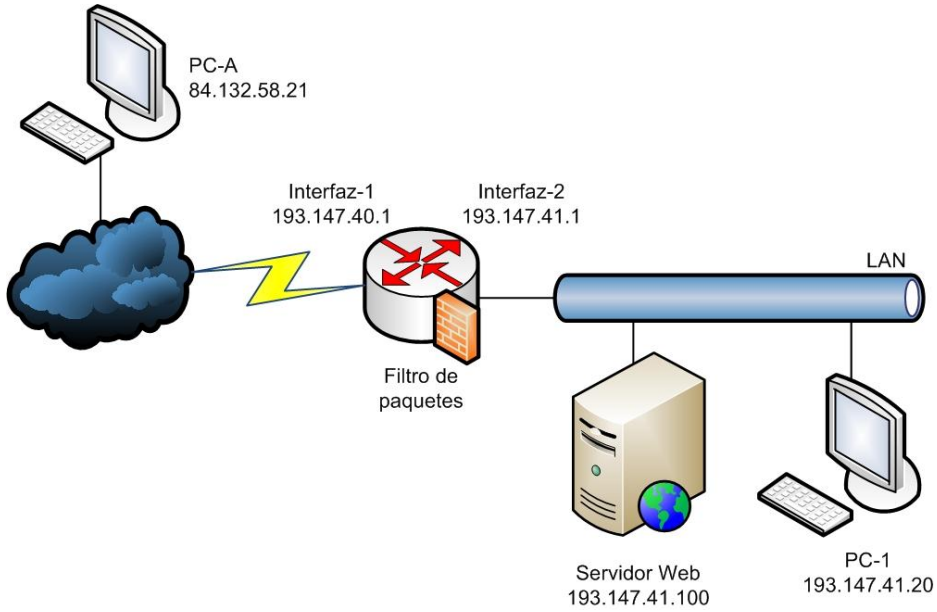
Tipos de firewalls
Filtrado dinámico de paquetes (stateful)

- Solución al escenario con un firewall de filtrado dinámico de paquetes

Debe poder accederse al Servidor Web desde cualquier equipo de Internet, excepto PC-A

PC-1 debe disponer de acceso a Internet

El firewall deberá bloquear cualquier otro intento de conexión



acción	origen	puerto	destino	puerto
bloquear	84.132.58.21	*	*	*
permitir	*	*	193.147.41.100	80
permitir	193.147.41.20	*	*	80
bloquear	*	*	*	*

Tipos de firewalls

Filtrado estático (stateless) vs filtrado dinámico (stateful)

- Filtrado estático
  - Más rápidos que el filtrado dinámico
  - Mejor funcionamiento en entornos con mucho tráfico
  - Más vulnerables a ataques de seguridad
  - Ejemplos ipchains (Linux), firewall de Windows XP SP2, firewall de Windows Server 2003 - RRAS
- Filtrado dinámico
  - Más seguros
  - Más lentos en entornos con mucho tráfico y pocos recursos hardware
  - Ejemplos: iptables (Linux), firewalls personales (ej.: Zone Alarm, Norton Personal Firewall, etc.)

Tipos de firewalls
Filtrado de paquetes

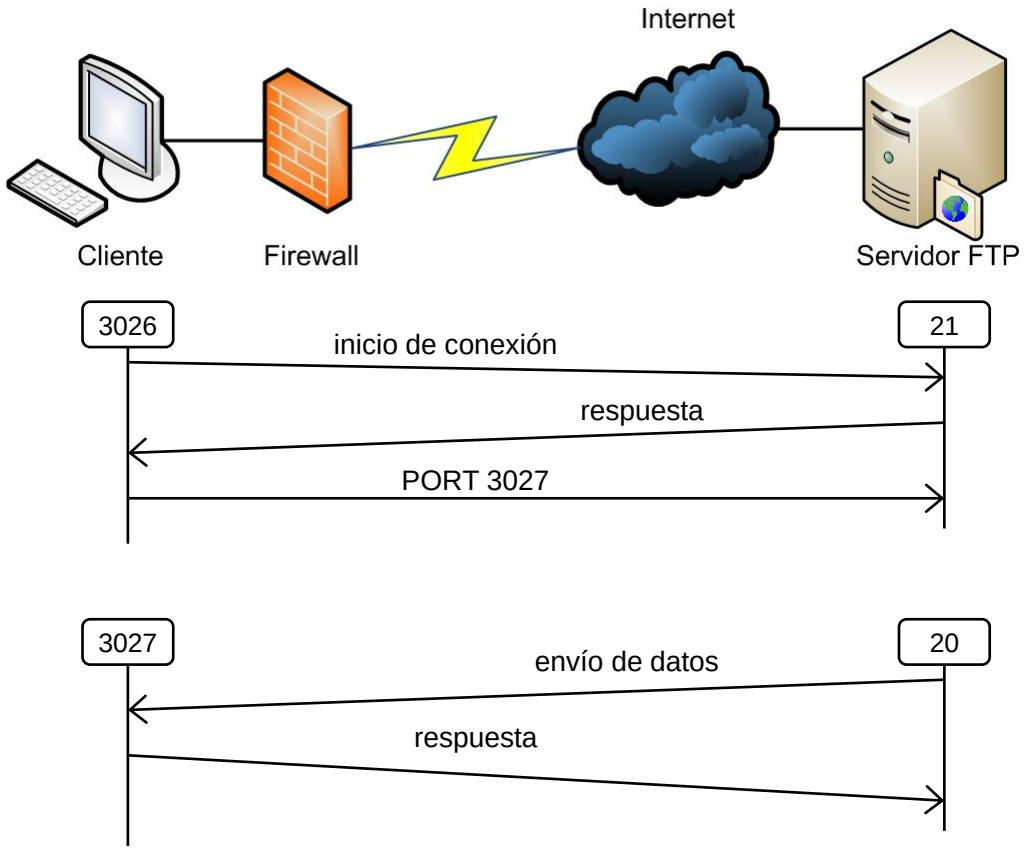
- Ventajas de los firewalls de filtrado de paquetes
  - Generalmente, bajo coste
    - Cualquier router suele incorporar un firewall de filtrado de paquetes
  - Bajo impacto en el rendimiento de la red
    - El filtrado estático es más rápido que el dinámico
  - Útiles para realizar un control general de una red, reduciendo el tráfico dirigido hacia la red interna
    - Adecuadamente configurados, proporcionan protección contra algunos ataques que se aprovechan de vulnerabilidades de TCP/IP (ej.: ciertos casos de IP spoofing)

Tipos de firewalls
Filtrado de paquetes

- Limitaciones de los firewalls de filtrado de paquetes
  - Problemas para gestionar protocolos como el “FTP Activo”:

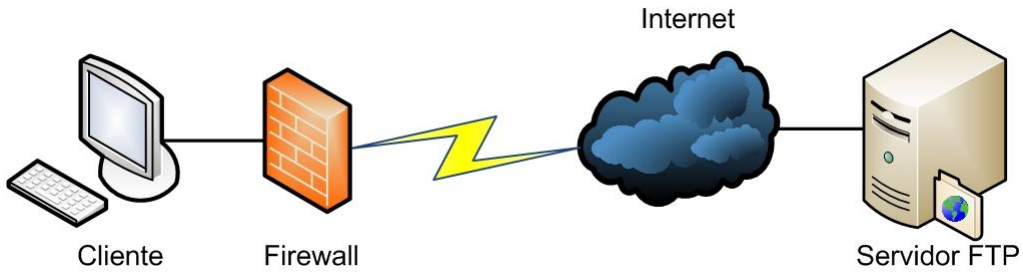
Funcionamiento del FTP Activo

1) El cliente se conecta desde un puerto aleatorio no privilegiado (>1024) al puerto de control del servidor (21)
2) Cuando el cliente desea iniciar una transmisión de datos, envía un comando PORT al servidor, indicando el puerto en el que permanecerá a la escucha para recibir datos
3) El servidor envía los datos desde el puerto 20 al puerto indicado por el cliente

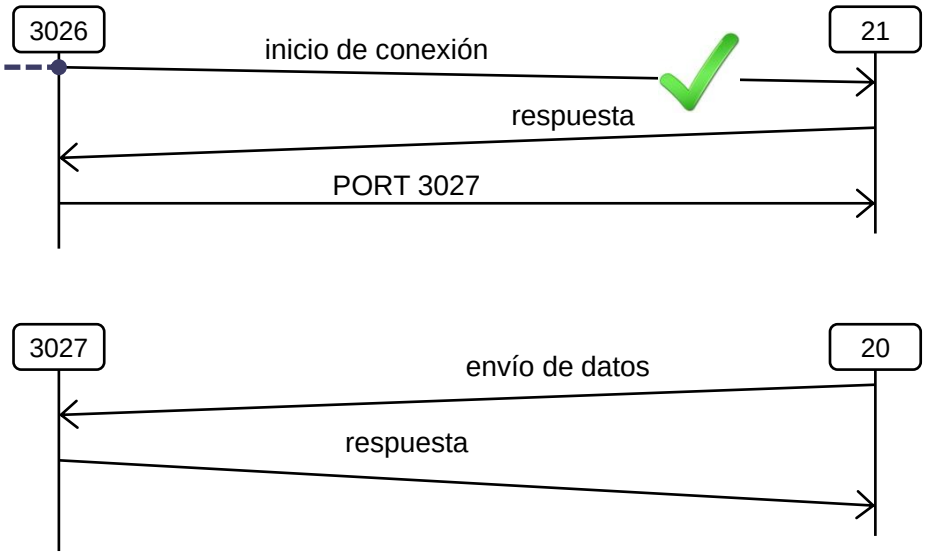


Tipos de firewalls
Filtrado de paquetes

- Limitaciones de los firewalls de filtrado de paquetes
  - Problemas para gestionar protocolos como el “FTP Activo”:

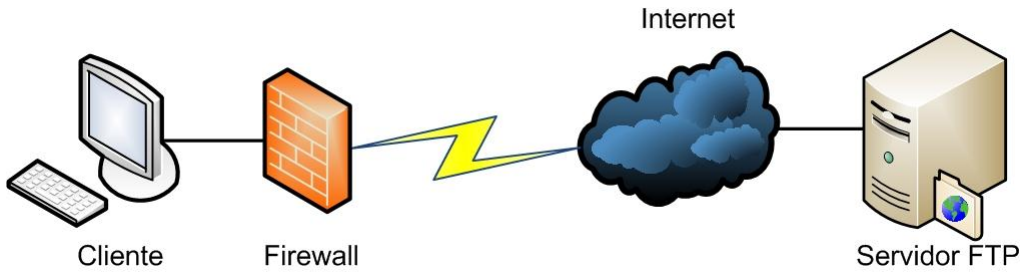


Se puede resolver con un firewall de filtrado de paquetes (con o sin estado)

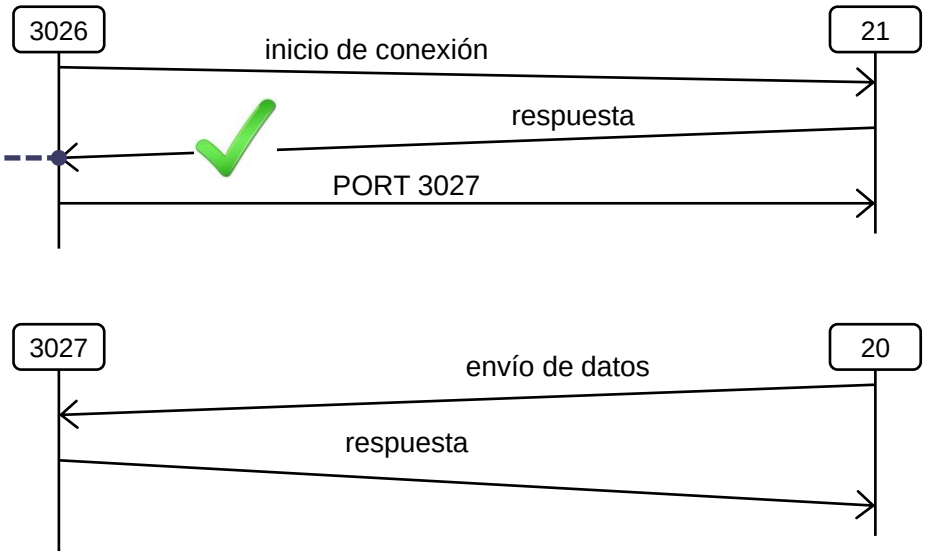


Tipos de firewalls
Filtrado de paquetes

- Limitaciones de los firewalls de filtrado de paquetes
  - Problemas para gestionar protocolos como el “FTP Activo”:

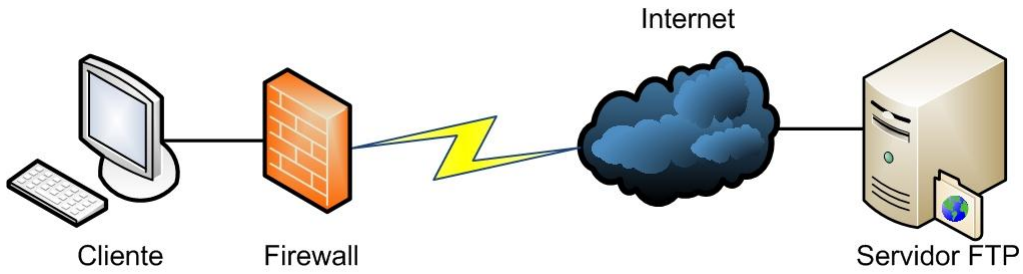


Se puede resolver con un firewall de filtrado de paquetes (preferiblemente con estado)

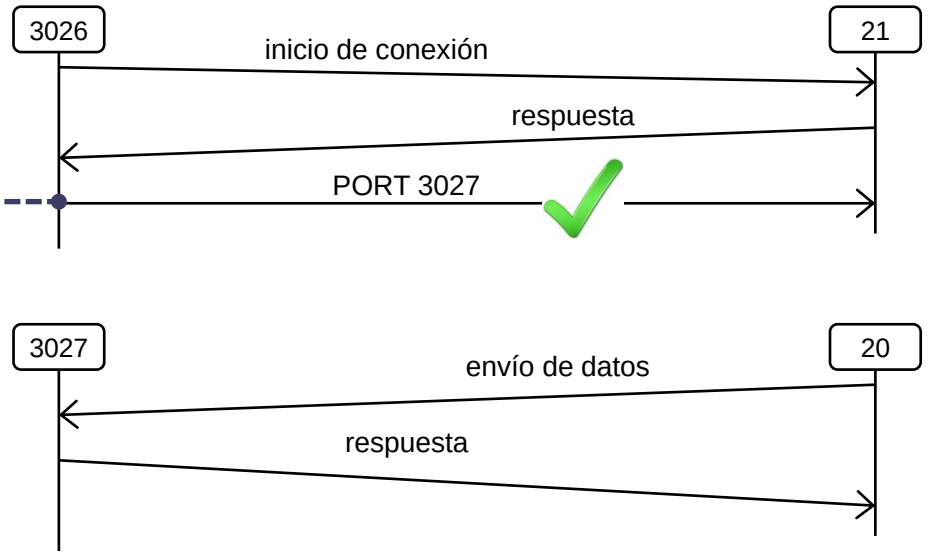


Tipos de firewalls
Filtrado de paquetes

- Limitaciones de los firewalls de filtrado de paquetes
  - Problemas para gestionar protocolos como el “FTP Activo”:

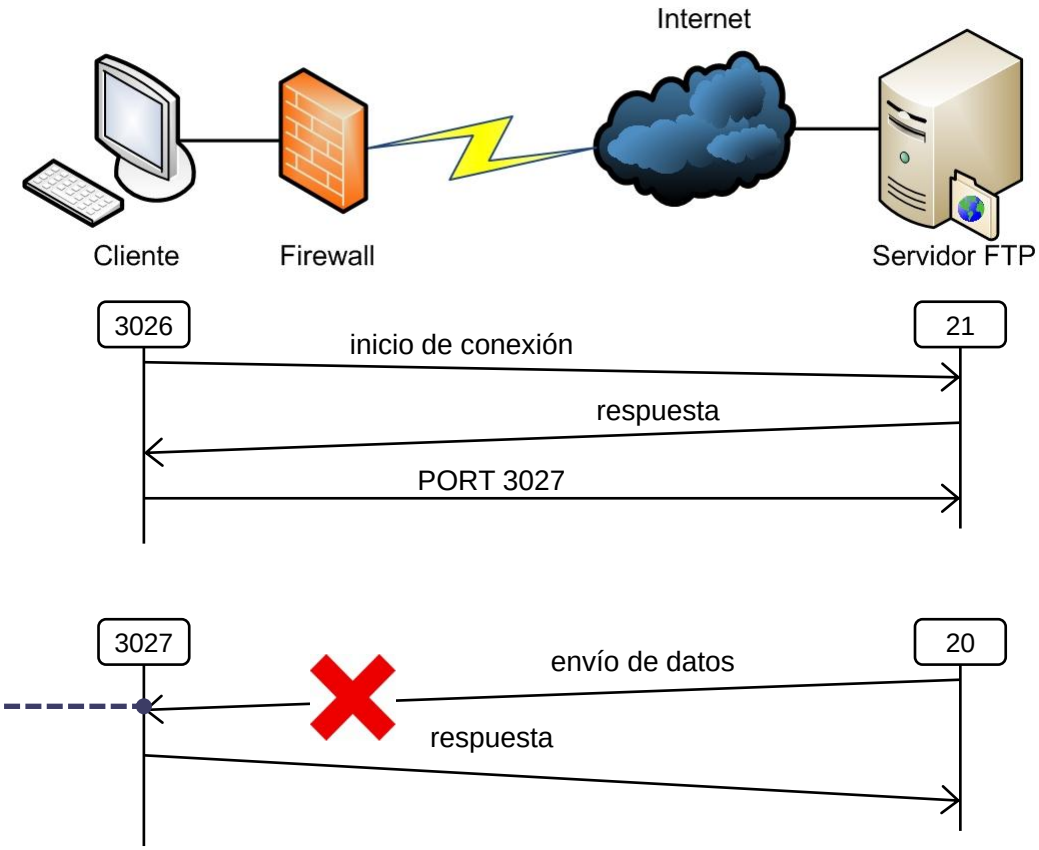


Comando a nivel de aplicación. El firewall de filtrado de paquetes lo permite (por regla anterior) pero no lo interpreta



Tipos de firewalls
Filtrado de paquetes

- Limitaciones de los firewalls de filtrado de paquetes
  - Problemas para gestionar protocolos como el “FTP Activo”:



El firewall bloqueará la conexión. No sabe que el cliente espera una conexión en el puerto 3027

Tipos de firewalls
Filtrado de paquetes

- Limitaciones de los firewalls de filtrado de paquetes
  - Problemas para gestionar protocolos como el "FTP Activo":
    - Posibles soluciones:
      - ¿Permitir todas las conexiones entrantes?
        - Riesgo elevado
      - Permitir paquetes con indicador ACK (respuestas) enviados desde el puerto 20 y con destino puertos superiores al 1024
        - El riesgo disminuye, pero un atacante podría enviar paquetes falsos
  - No se puede gestionar de forma óptima con firewalls de filtrado de paquetes
    - Necesario control a nivel de aplicación

- NOTA: Si el firewall del cliente bloquea el FTP Activo, posiblemente el servidor active el FTP Pasivo (si dispone de él y si el firewall del servidor lo permite)
  - FTP Pasivo: Ambas conexiones (control y datos) se inician desde el cliente (al 21 y a un puerto aleatorio)
  - Menos seguro para el servidor

Tipos de firewalls
Filtrado de paquetes

- Limitaciones de los firewalls de filtrado de paquetes
  - No admiten esquemas de autenticación avanzada de usuarios
    - el control se limita a IP
  - No pueden evitar ataques que se aprovechan de vulnerabilidades a nivel de aplicación
    - Si el firewall permite una aplicación, todas las funciones de la misma estarán permitidas
    - Ejemplo: desbordamiento de *buffer* (*buffer overflow*)
      - Uno de los ataques más frecuentes a nivel de aplicación
      - Activan la ejecución de un código arbitrario de una aplicación, al enviar un caudal de datos mayor al que puede recibir
      - Pueden provocar una denegación de servicio (DoS) o acceso al sistema
    - Ejemplo: explotación de vulnerabilidades
      - Aplicación Web vulnerable a SQL Injection
        - `http://www.mydomain.com/products/products.asp?productid=123; DROP TABLE Products`

Tipos de firewalls

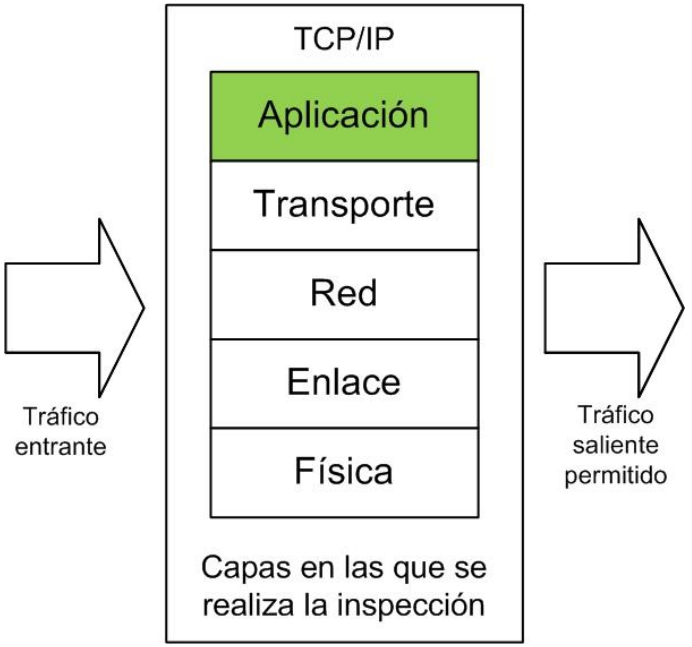
- **Filtrado de paquetes** (*packet filtering*)
  - Filtrado estático o sin estado (*stateless*)
  - Filtrado dinámico o con estado *(stateful*)

- **Filtrado a nivel de aplicación**
  - Proxy

- Otros conceptos de interés
  - NAT

Tipos de firewalls
Filtrado a nivel de aplicación

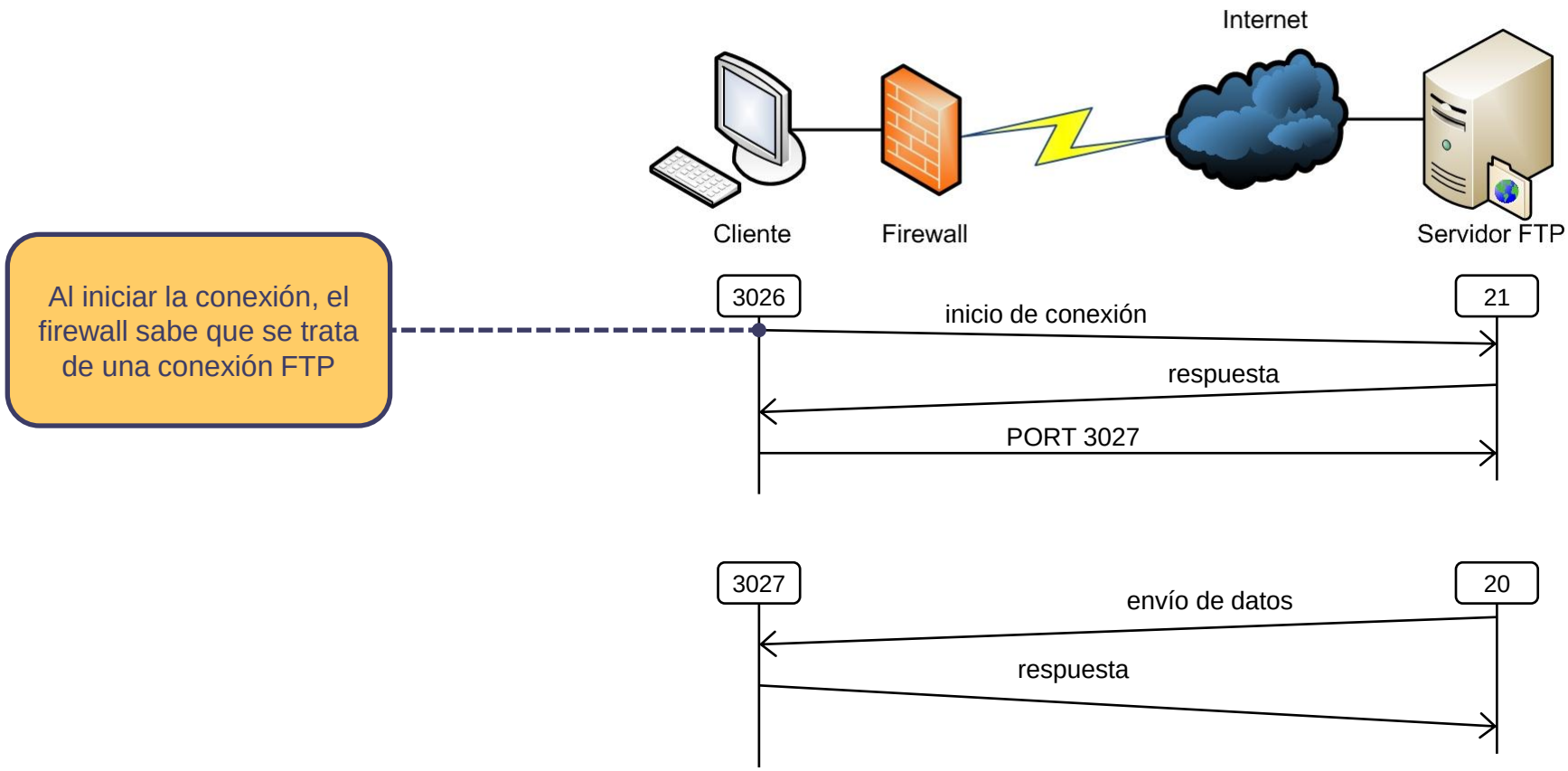
- Capaces de interpretar paquetes a nivel de aplicación
  - Mayor capacidad de análisis y de control de tráfico
  - Más complejos, pues deben conocer el funcionamiento de aplicaciones específicas (ej.: FTP, HTTP, SMTP, TELNET, etc.)
  - Suelen combinarse con filtrado de paquetes
- Actualmente, un 75% de los ataques se realiza a nivel de aplicación[1]



[1] http://www.acunetix.com/websitesecurity/webapp-security.htm

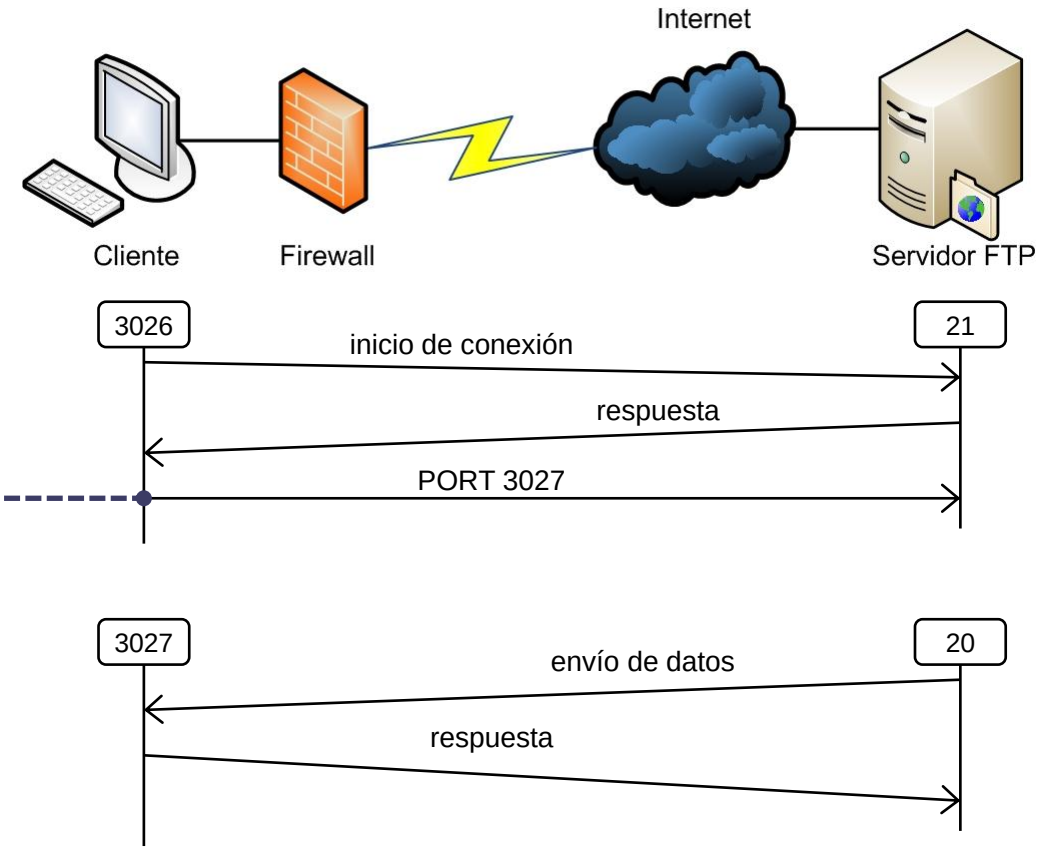
Tipos de firewalls
Filtrado a nivel de aplicación

- Ejemplo: FTP Activo



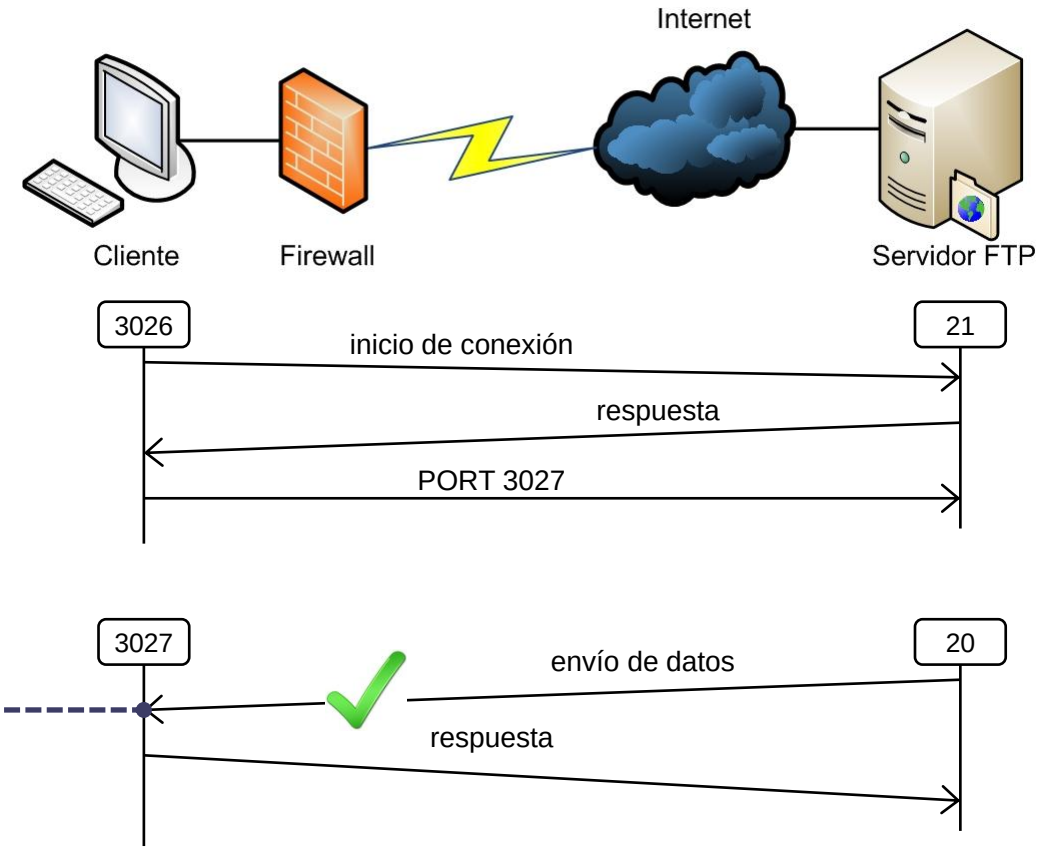
Tipos de firewalls
Filtrado a nivel de aplicación

- Ejemplo: FTP Activo



Tipos de firewalls
Filtrado a nivel de aplicación

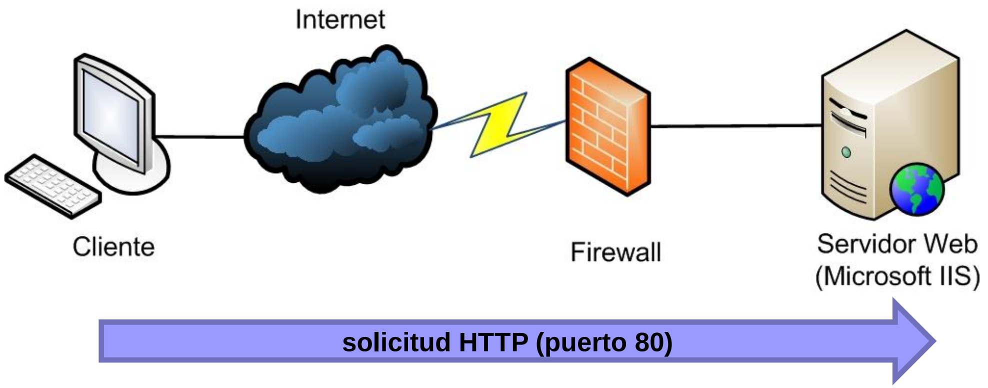
- Ejemplo: FTP Activo



El firewall permite la conexión al puerto 3027 del cliente y comienza la transferencia de datos

Tipos de firewalls
Filtrado a nivel de aplicación

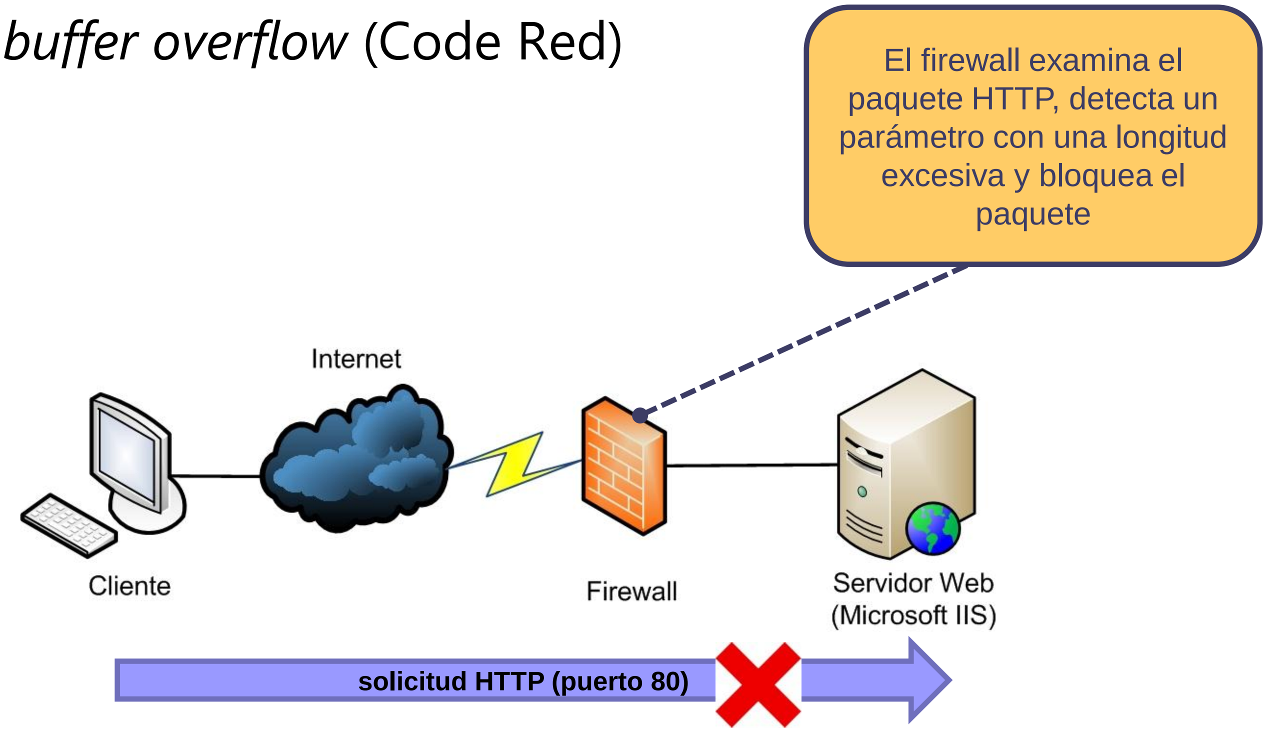
- Ejemplo: *buffer overflow* (Code Red)




```
GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
N%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u68
58%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u5
3ff%u0078%u0000%u00=a HTTP/1.0
```

Tipos de firewalls
Filtrado a nivel de aplicación

- Ejemplo: *buffer overflow* (Code Red)




```
GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
N%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u68
58%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u5
3ff%u0078%u0000%u00=a HTTP/1.0
```

Tipos de firewalls
Filtrado a nivel de aplicación

- Ventajas
  - Mejor control de conexiones para ciertos protocolos
    - Algunos firewalls de filtrado de paquetes incorporan capacidad de gestionar algunos protocolos de nivel de aplicación (ej.: FTP)
  - Identificación de ataques a nivel de aplicación
    - Detección de software malicioso (virus, *malware*, etc.) y de ciertos patrones de ataque (ej.: SQL Injection, buffer overflow, etc.)
    - Filtrado de contenidos (*spam*, URLs prohibidas, etc.)
  - Mayor capacidad de *logging*

Tipos de firewalls
Filtrado a nivel de aplicación

- Limitaciones
  - Menor rendimiento
    - Debe analizarse el contenido del paquete
  - Restringidos a un conjunto de protocolos
    - Generalmente HTTP, FTP, TELNET, SMTP, etc.
    - Problemas con protocolos recientes o propietarios
  - Siguen sin resolver el problema de la autenticación a nivel de usuario

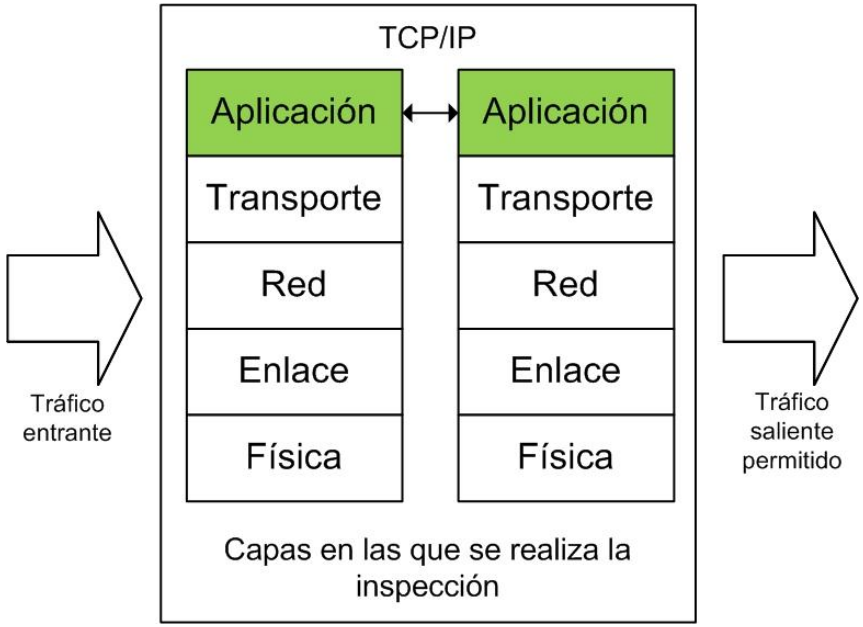
Tipos de firewalls

- **Filtrado de paquetes** (*packet filtering*)
  - Filtrado estático o sin estado (*stateless*)
  - Filtrado dinámico o con estado *(stateful*)

- **Filtrado a nivel de aplicación**
  - Proxy

Tipos de firewalls
Filtrado a nivel de aplicación – Proxy

- También llamados *gateways* de aplicación
- Establecen una conexión con el servidor en nombre del cliente, y viceversa
  - Eliminan la conexión directa entre sistemas, el proxy actúa como intermediario
  - No actúan como *routers*
- Al igual que con los demás tipos de firewall, los proxies pueden configurarse en equipos dedicados o bien como un software adicional de un equipo personal



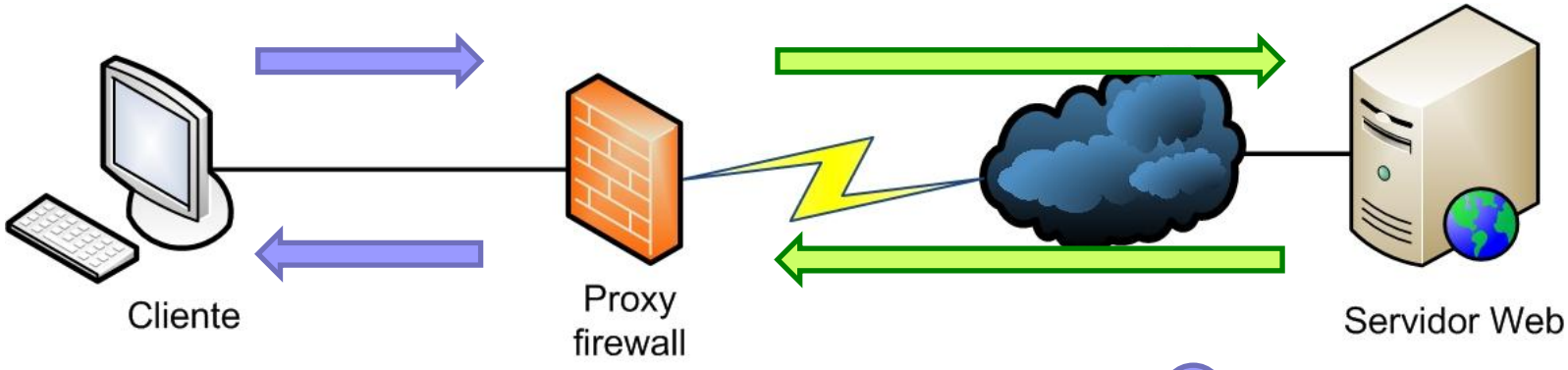
Tipos de firewalls

Filtrado a nivel de aplicación – Proxy

Éste tipo de proxy se llama “directo” porque controla el tráfico de salida. Cuando controla el tráfico de entrada se llama proxy inverso

1. El cliente envía una solicitud HTTP hacia el Servidor Web

2. El proxy examina la solicitud y, si lo considera oportuno, crea una conexión con el servidor para atenderla



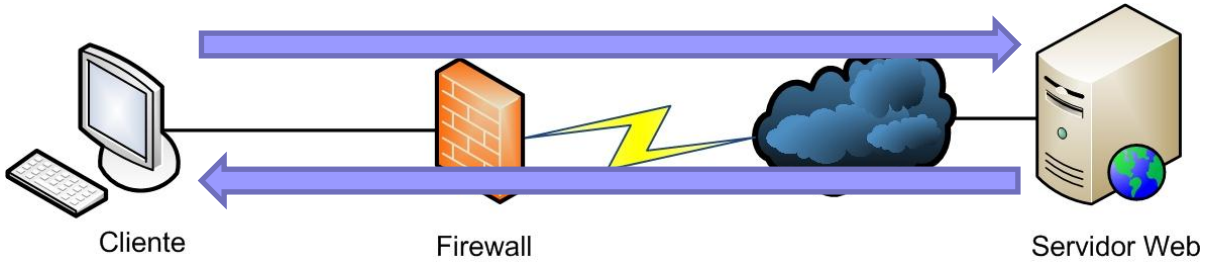
3. El servidor responde a la solicitud realizada por el proxy

4. El proxy examina la respuesta del servidor y responde al cliente sobre la conexión previamente establecida

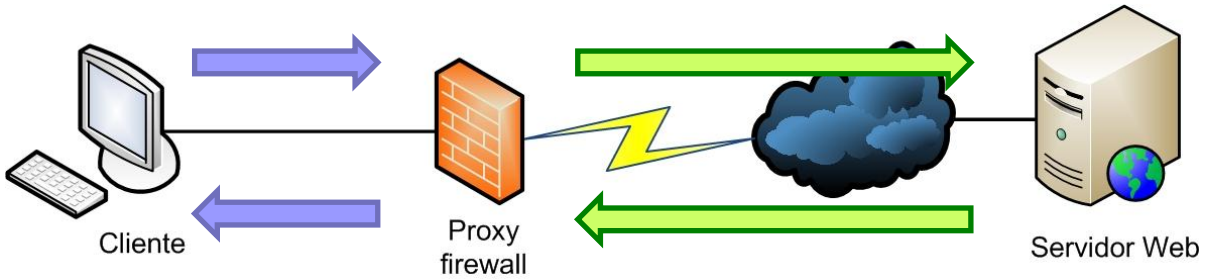
5. El cliente recibe la respuesta directamente del proxy

Tipos de firewalls
Filtrado a nivel de aplicación – Proxy

- Firewall vs. Proxy firewall



1 conexión



2 conexiones independientes

- En ambos casos, el proceso de acceso al servidor es transparente para el usuario

Tipos de firewalls
Filtrado a nivel de aplicación – Proxy

- Ventajas
  - Mayor seguridad
    - Oculta información de la red interna (ej.: nombres de sistemas, IPs, etc.)
    - Eliminan ciertos ataques a nivel IP (ej.: paquetes mal formados)
  - Mayor capacidad de logging
  - Permiten aplicar mecanismos de autenticación de usuarios
    - Bloqueo de tráfico dependiente del usuario

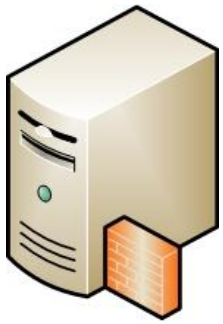
Tipos de firewalls
Filtrado a nivel de aplicación – Proxy

- Limitaciones
  - Requiere configurar la aplicación en el cliente para utilizar el proxy
    - Solución: proxies transparentes (utilizados por los ISPs)
  - Menor rendimiento que firewalls de filtrado de paquetes
    - En entornos en los que se trabaja con datos críticos (militar, gobierno, finanzas, salud, etc.), puede decidirse sacrificar el rendimiento a favor de una mayor seguridad
    - Posible solución: servidores proxies dedicados
  - Soporte limitado de protocolos
    - Posible solución: Circuit-level proxies

Tipos de firewalls

Filtrado a nivel de aplicación – Servidores proxy dedicados

- Es un proxy que funciona en un servidor dedicado a él
  - Mayor rendimiento
- Se utilizan para aplicaciones específicas (ej.: correo)
- Suelen situarse detrás de otro firewall (ej.: filtrado de paquetes)
- Pueden actuar como proxy directo (interna-externa) o inverso (externa-interna)
- Reducen la carga del firewall externo

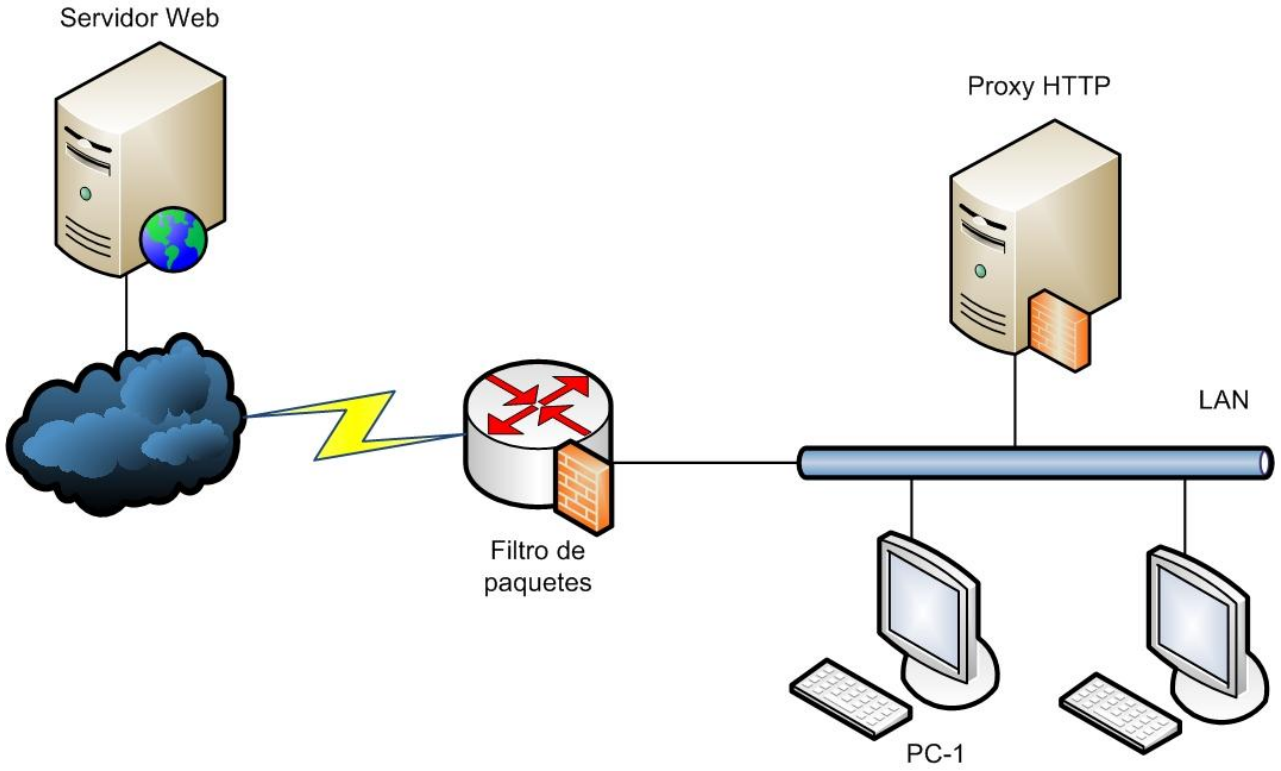


Tipos de firewalls

Filtrado a nivel de aplicación – Servidores proxy dedicados

- Ejemplo: Proxy HTTP

Un usuario desea acceder al Servidor Web desde PC-1



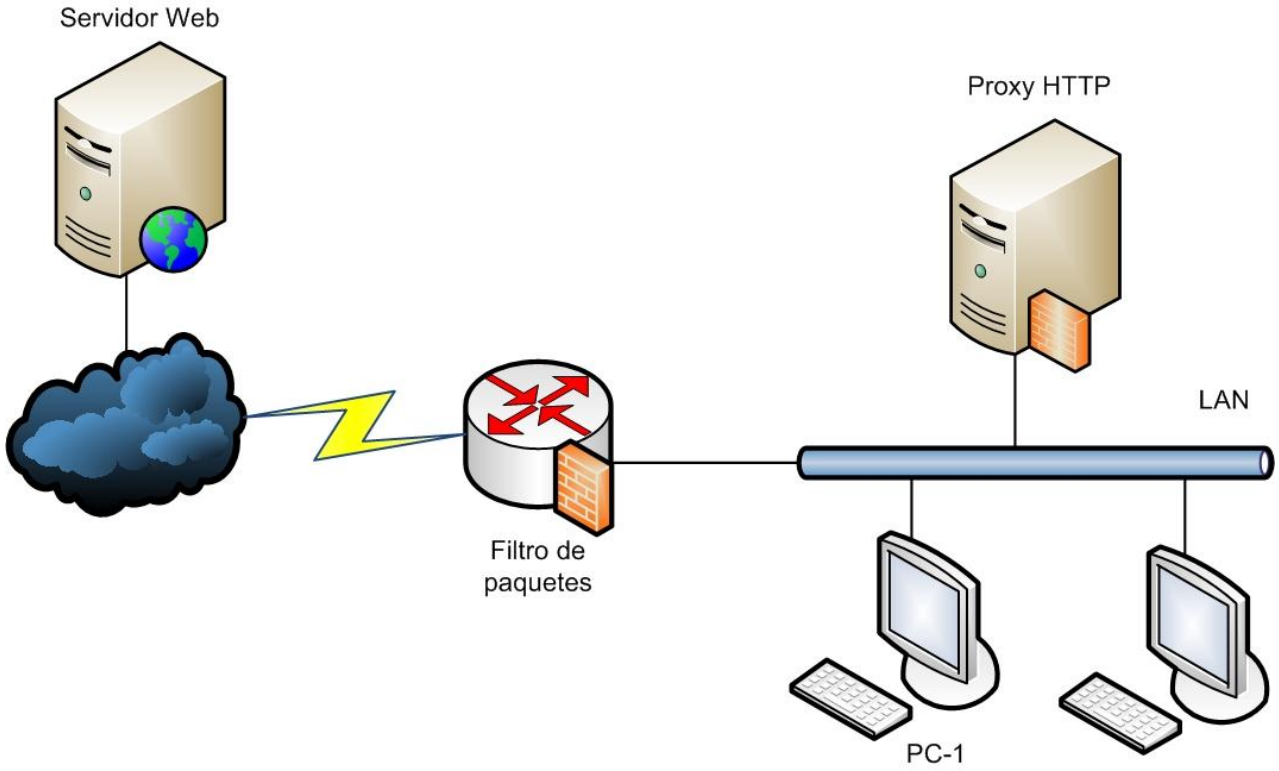
Tipos de firewalls

Filtrado a nivel de aplicación – Servidores proxy dedicados

- Ejemplo: Proxy HTTP

Un usuario desea acceder al Servidor Web desde PC-1

El firewall de filtrado de paquetes está configurado para rechazar cualquier paquete que no proceda del Proxy HTTP



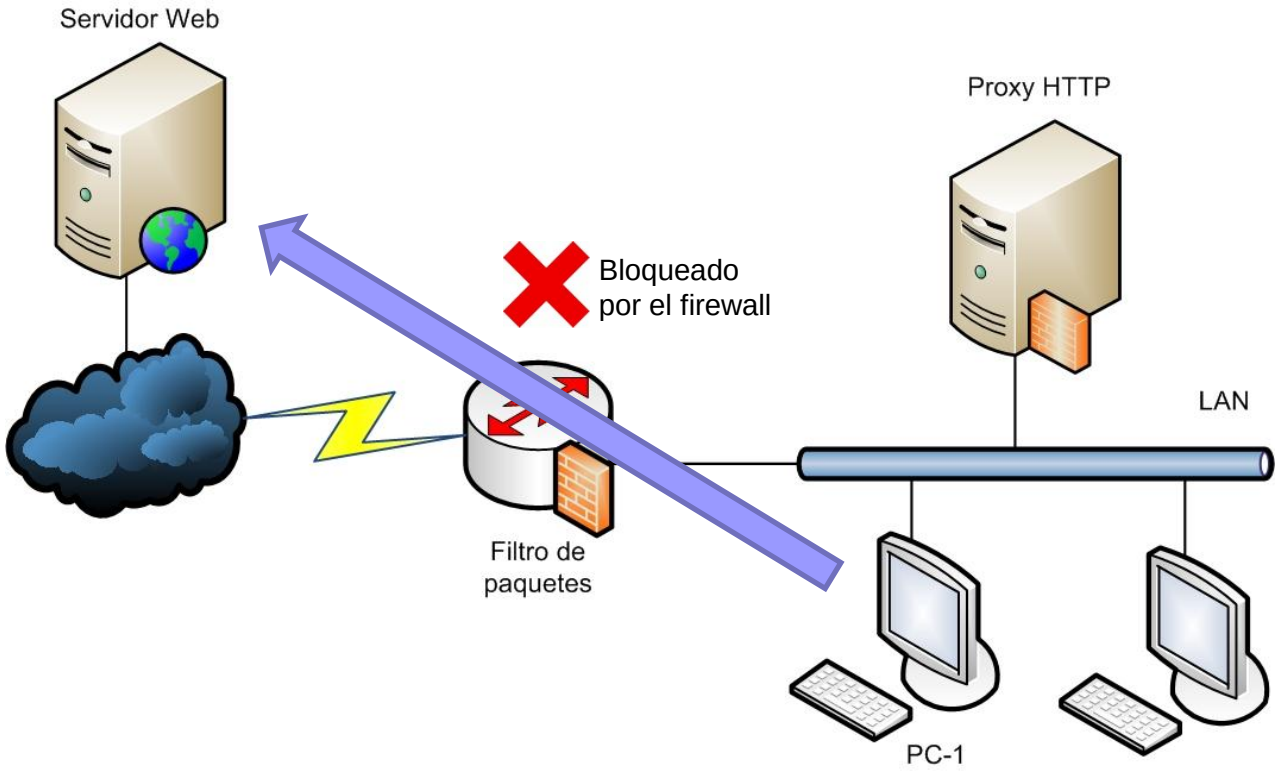
Tipos de firewalls

Filtrado a nivel de aplicación – Servidores proxy dedicados

- Ejemplo: Proxy HTTP

Un usuario desea acceder al Servidor Web desde PC-1

El firewall de filtrado de paquetes está configurado para rechazar cualquier paquete que no proceda del Proxy HTTP



Tipos de firewalls

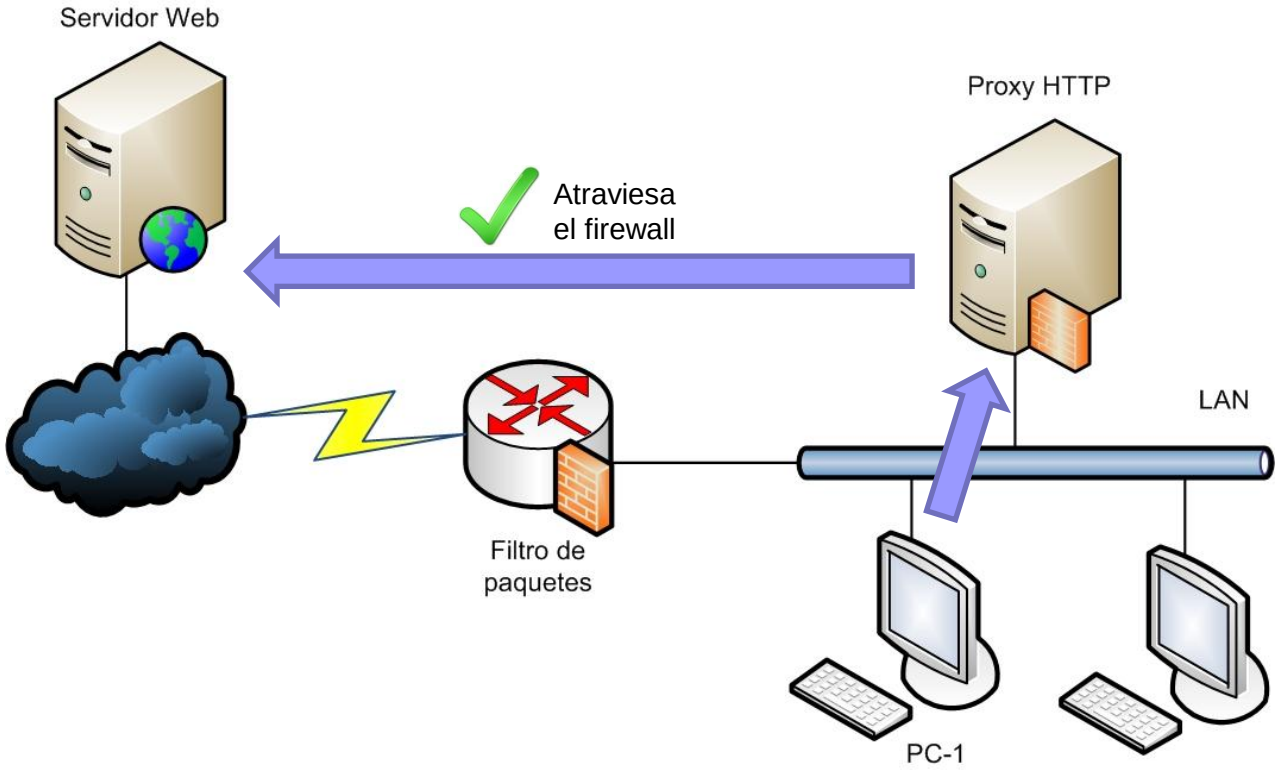
Filtrado a nivel de aplicación – Servidores proxy dedicados

- Ejemplo: Proxy HTTP

Un usuario desea acceder al Servidor Web desde PC-1

El firewall de filtrado de paquetes está configurado para rechazar cualquier paquete que no proceda del Proxy HTTP

Los clientes deben conectarse al Servidor Web a través del Proxy (que filtrará el tráfico como desee)



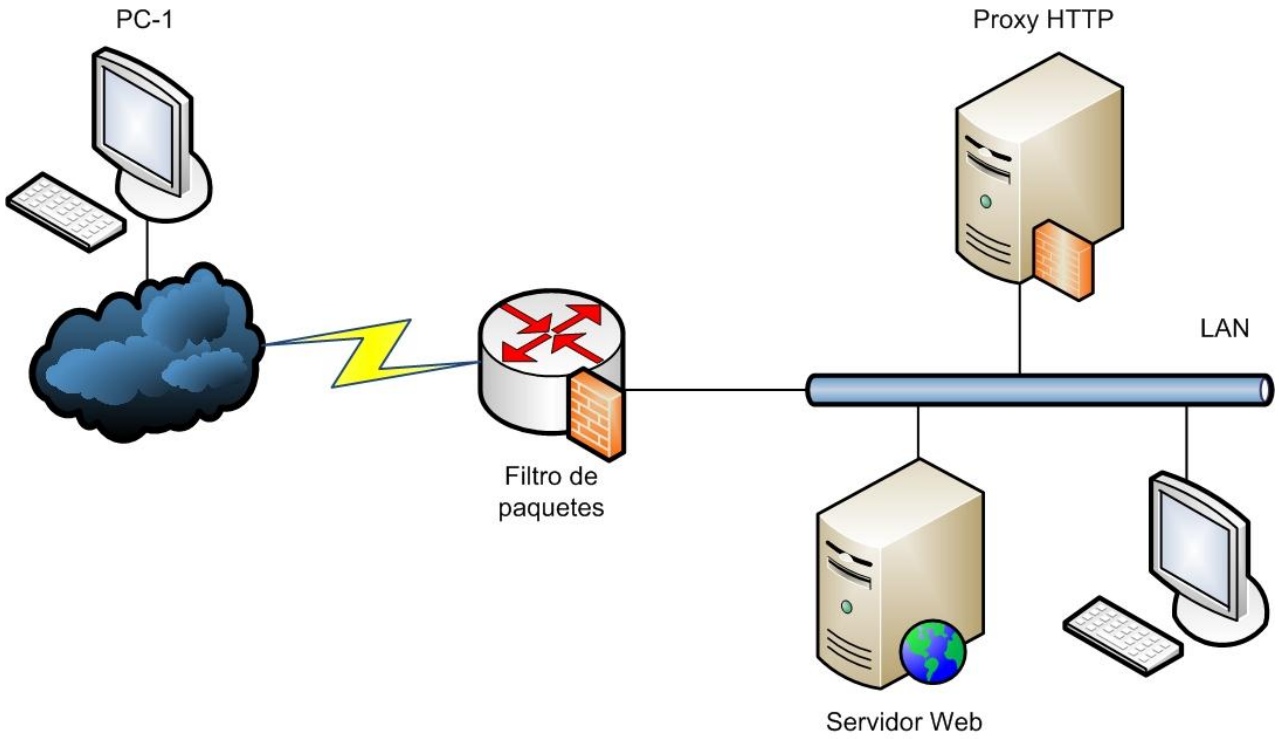
Tipos de firewalls

Filtrado a nivel de aplicación – Servidores proxy dedicados

- Ejemplo: Proxy inverso HTTP

Un usuario desea acceder al Servidor Web interno desde PC-1

El firewall de filtrado de paquetes está configurado para rechazar cualquier paquete que no se dirija al Proxy HTTP



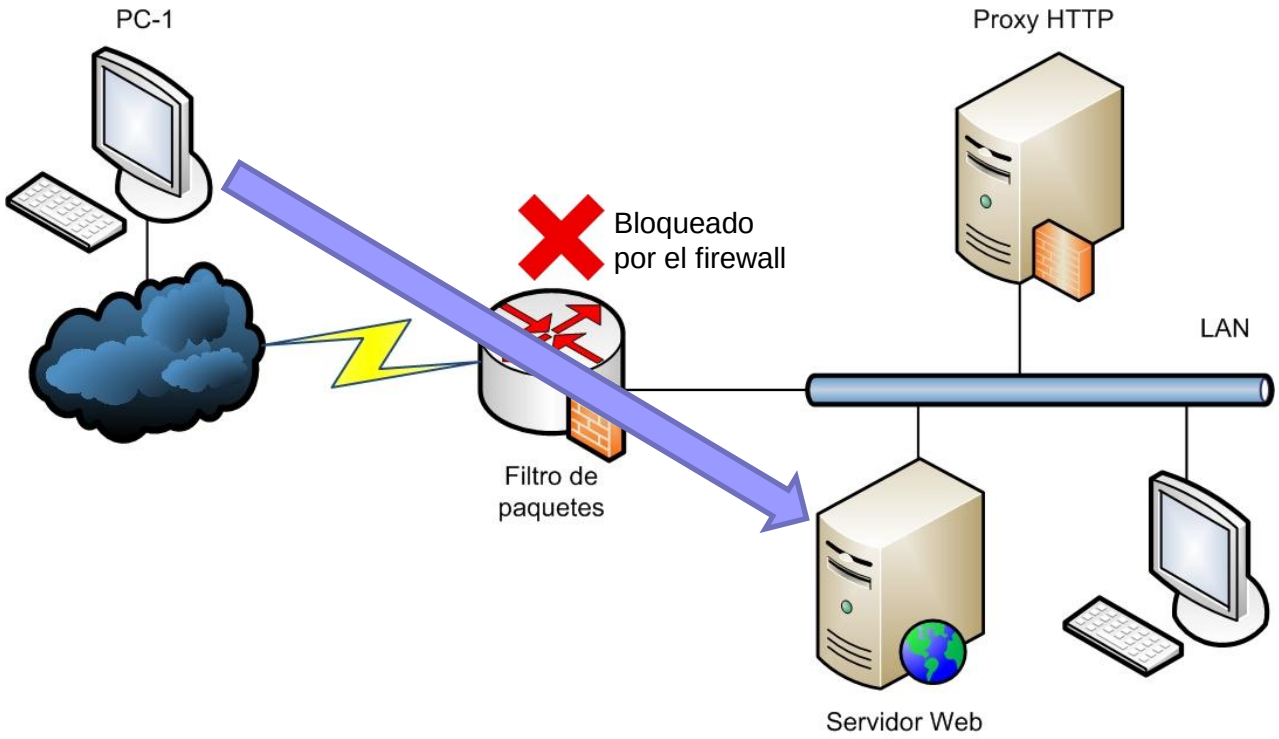
Tipos de firewalls

Filtrado a nivel de aplicación – Servidores proxy dedicados

- Ejemplo: Proxy inverso HTTP

Un usuario desea acceder al Servidor Web interno desde PC-1

El firewall de filtrado de paquetes está configurado para rechazar cualquier paquete que no se dirija al Proxy HTTP



Tipos de firewalls

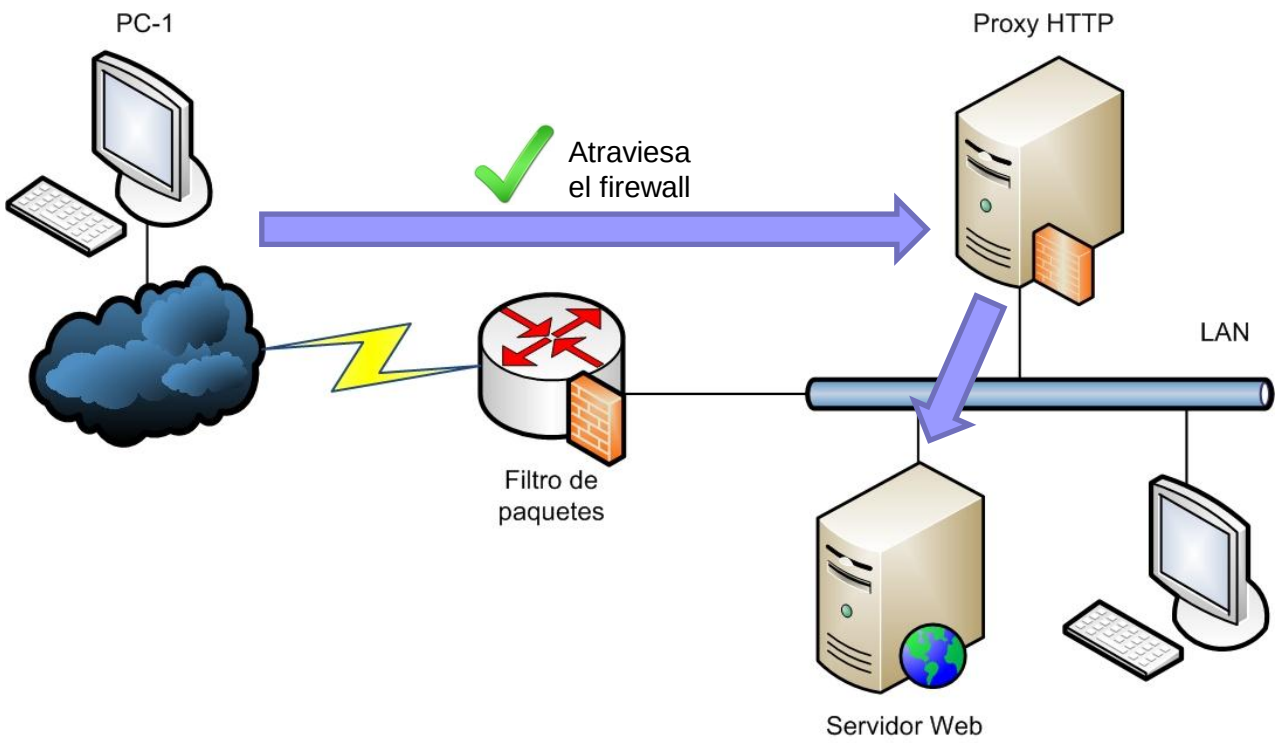
Filtrado a nivel de aplicación – Servidores proxy dedicados

- Ejemplo: Proxy inverso HTTP

Un usuario desea acceder al Servidor Web interno desde PC-1

El firewall de filtrado de paquetes está configurado para rechazar cualquier paquete que no se dirija al Proxy HTTP

Los clientes deben conectarse al Servidor Web a través del Proxy (que realizará un filtrado de cualquier ataque)



IPTABLES

Ejemplos de firewalls
IPTables

- Firewall de filtrado de paquetes
  - Se basa en la dirección/puerto de origen/destino, protocolo, etc.
  - Funciona mediante reglas para determinar si un paquete tiene permiso o no para pasar
  - Es posible añadir módulos que incrementan la funcionalidad
- Características
  - Soporta protocolos TCP/UDP/ICMP
  - Soporta interfaces de origen/destino de paquetes
  - Permite el uso de chains o cadenas para controlar el tráfico de entrada/salida/redirección
  - Permite un número ilimitado de reglas por chain
  - Muy estable, rápido y seguro

Ejemplos de firewalls
IPTables

- Reglas
  - Las reglas son como comandos que se le pasan a IPTables para que realice una determinada acción (como bloquear o dejar pasar un paquete) basándose en la dirección de origen/destino, interfaz de origen/destino, etc.
  - Se procesan en el orden en que fueron insertadas
  - Se agrupan dentro de cadenas (o chains)
    - Son grupos de reglas referidas a un tipo de tráfico
    - Existen dos tipos:
      - Definidas por iptables: INPUT, OUTPUT y FORWARD
      - Definidas por el usuario

Ejemplos de firewalls
IPTables

- Tablas
  - Agrupan las cadenas y reglas
  - Se referencian con la opción –t tabla
  - Existen 3 tablas:
    - Filter
      - Reglas INPUT, OUTPUT, FORWARD
    - Nat
      - Reglas PreRouting, PostRouting
    - Mangle
      - Modificación paquetes

Ejemplos de firewalls
IPTables

- Funcionamiento
  - Una cadena es una lista de reglas
  - Cada regla dice: “si la cabecera del paquete coincide con esto, aquí está lo que se debe hacer con el paquete”
  - Si el paquete no encaja en la regla, se pasa a la siguiente regla. Si se agotan todas las reglas, se aplica la política por defecto de la cadena (ACEPTAR/DENEGAR)

Ejemplos de firewalls
IPTables

- Funcionamiento
  - Cuando un paquete llega (eg. Tarjeta Ethernet) el kernel analiza el destino del paquete.
    - Si el paquete tiene como destino la propia máquina, el paquete se envía a la cadena **INPUT**. Si consigue pasar por esta cadena, entonces la máquina recibe el paquete
    - ¿El kernel soporta forwarding?
      - No (o no sabe como redireccionarlo): el paquete se descarta.
      - Si (y el paquete se destina a otra interfaz de red): el paquete se envía a la cadena **FORWARD**. Si consigue pasar por esta cadena, el paquete será reenviado.
  - Un programa ejecutándose la misma máquina en la que se está ejecutando el firewall puede enviar paquetes. E
    - Esos paquetes se envían a la cadena **OUTPUT**.
      - Si consiguen pasar por esta cadena, continúan su camino, en caso contrario, se descartan.

Ejemplos de firewalls
IPTables

- Ejemplo de regla
  - Como ejemplo, vamos a crear una regla que bloquea el acceso a nuestra propia máquina (127.0.0.1 - loopback). Primero haremos un ping para verificar su funcionamiento:

```
#ping 127.0.0.1
     PING 127.0.0.1 (127.0.0.1): 56 data bytes
     64 bytes from 127.0.0.1: icmp_seq=0 ttl=255 time=0.6 ms
     64 bytes from 127.0.0.1: icmp_seq=1 ttl=255 time=0.5 ms

     --- 127.0.0.1 ping statistics ---
     2 packets transmitted, 2 packets received, 0% packet loss
     round-trip min/avg/max = 0.5/0.5/0.6 ms
```

Ejemplos de firewalls
IPTables

- Ejemplo de regla
  - Ahora vamos a incluir una regla en la cadena INPUT (*-A INPUT*) que bloquee (*-j DROP*) cualquier acceso destinado a la dirección 127.0.0.1 (*-d 127.0.0.1*):

```
iptables -t filter -A INPUT -d 127.0.0.1 -j DROP
```

  - Hacemos de nuevo el ping

```
#ping 127.0.0.1
      PING 127.0.0.1 (127.0.0.1): 56 data bytes


      --- 127.0.0.1 ping statistics ---
      2 packets transmitted, 0 packets received, 100% packet loss
```

  - Esta vez, la máquina 127.0.0.1 no responde, ya que todos los paquetes con destino 127.0.0.1 (-d 127.0.0.1) son rechazados (-j DROP)
    - La opción –A se usa para añadir nuevas reglas al final de una cadena
    - La opción *-j DROP* rechaza los paquetes. Se podría utilizar *-j ACCEPT* para aceptarlos

Ejemplos de firewalls
IPTables

Option	Description
`-s address`	Specifies the source address of packets for a rule.
`-d address`	Specifies the destination address of packets for a rule.
`-sport port#`	Specifies the source port number for a rule.
`-dport port#`	Specifies the destination port number for a rule.
`-p protocol`	Specifies the protocol type for a rule.
`-i interface`	Specifies the input network interface.
`-o interface`	Specifies the output network interface.
`-j action`	Specifies the action that is taken for a rule.
`-m match`	Specifies a match parameter that should be used within the rule. The most common match used is `state`, which creates a stateful packet filtering firewall.
`-A chain`	Specifies the chain used.
`-L chain`	Lists rules for a certain chain. If no chain is given, all chains are listed.
`-P policy`	Specifies the default policy for a certain chain type.
`-D number`	Deletes a rule for a chain specified by additional arguments. Rules start at number 1.
`-R number`	Replaces a rule for a chain specified by additional arguments. Rules start at number 1.
`-F chain`	Removes all rules for a certain chain. If no chain is specified, it removes all rules for all chains.

Ejemplos de firewalls
IPTables

- Consulta de reglas

```
root@debian:~# iptables -t filter -L

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

[...]

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

[...]

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

[...]
```

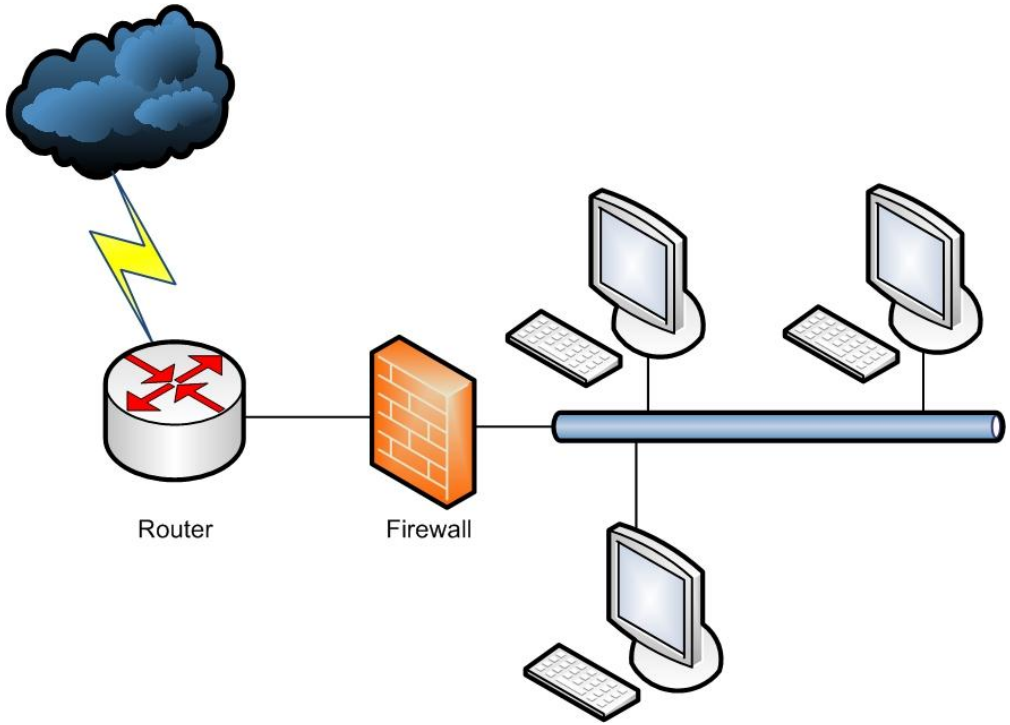
ARQUITECTURAS DE FIREWALLS

Arquitecturas de firewalls

- Además de las configuraciones simples vistas hasta el momento, son posibles configuraciones más complejas
- Aspectos importantes:
  - Nº de firewalls a utilizar
  - Tipo de firewalls
  - Ubicación en la red
- Examinaremos las arquitecturas más habituales
  - DMZ
  - Doble DMZ
  - Bastión
  - Bastión Doble Interfaz

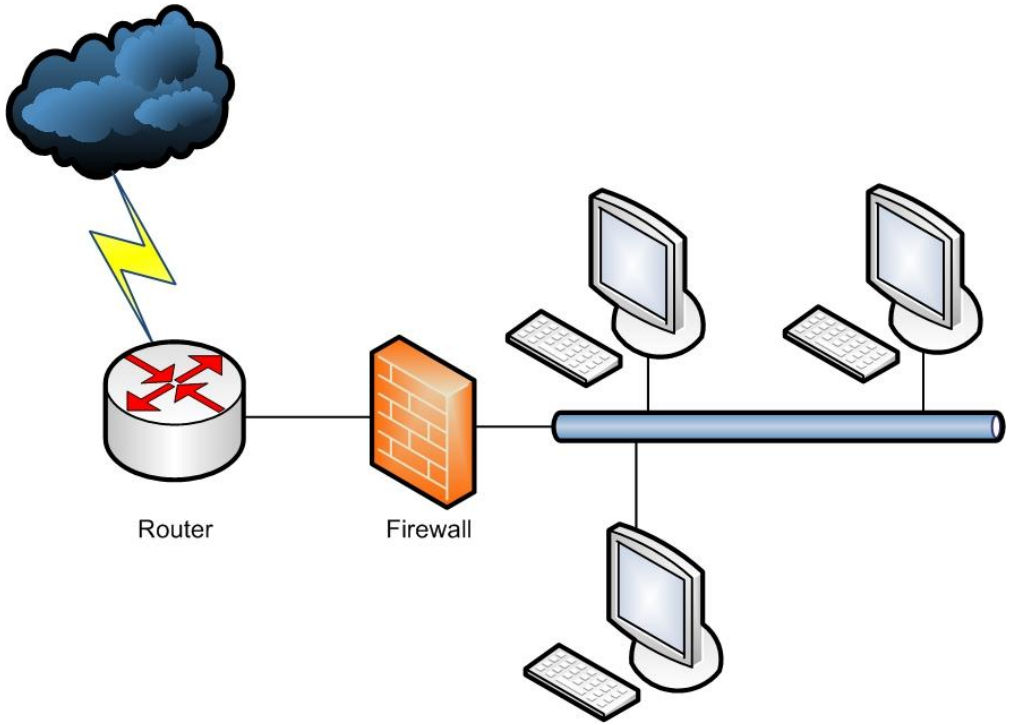
Arquitecturas de firewalls
Escenario básico

- Escenario básico de uso de un firewall



Arquitecturas de firewalls
Escenario básico

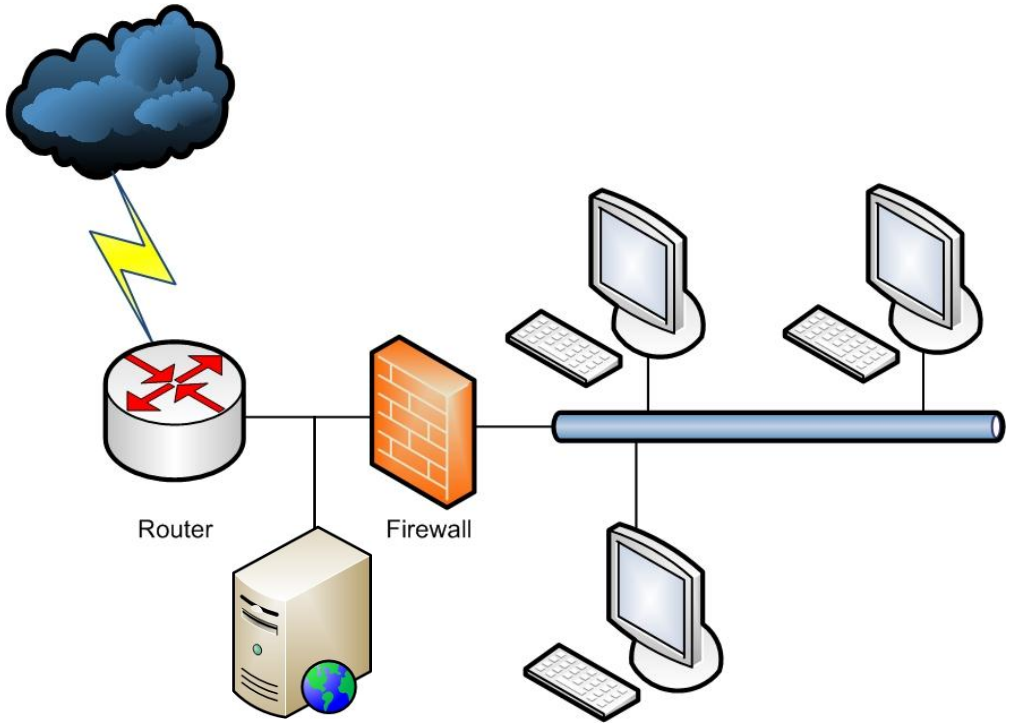
- Escenario básico de uso de un firewall



¿Dónde situar un Servidor Web?

Arquitecturas de firewalls
Escenario básico

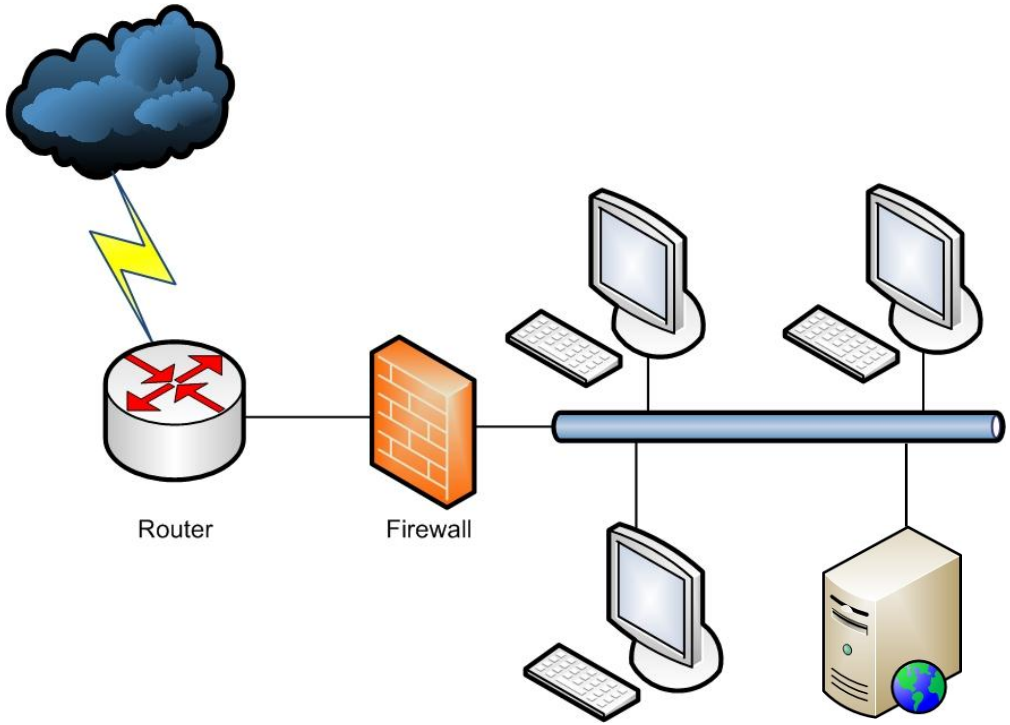
- Escenario básico de uso de un firewall



Opción 1: Servidor completamente expuesto a ataques

Arquitecturas de firewalls
Escenario básico

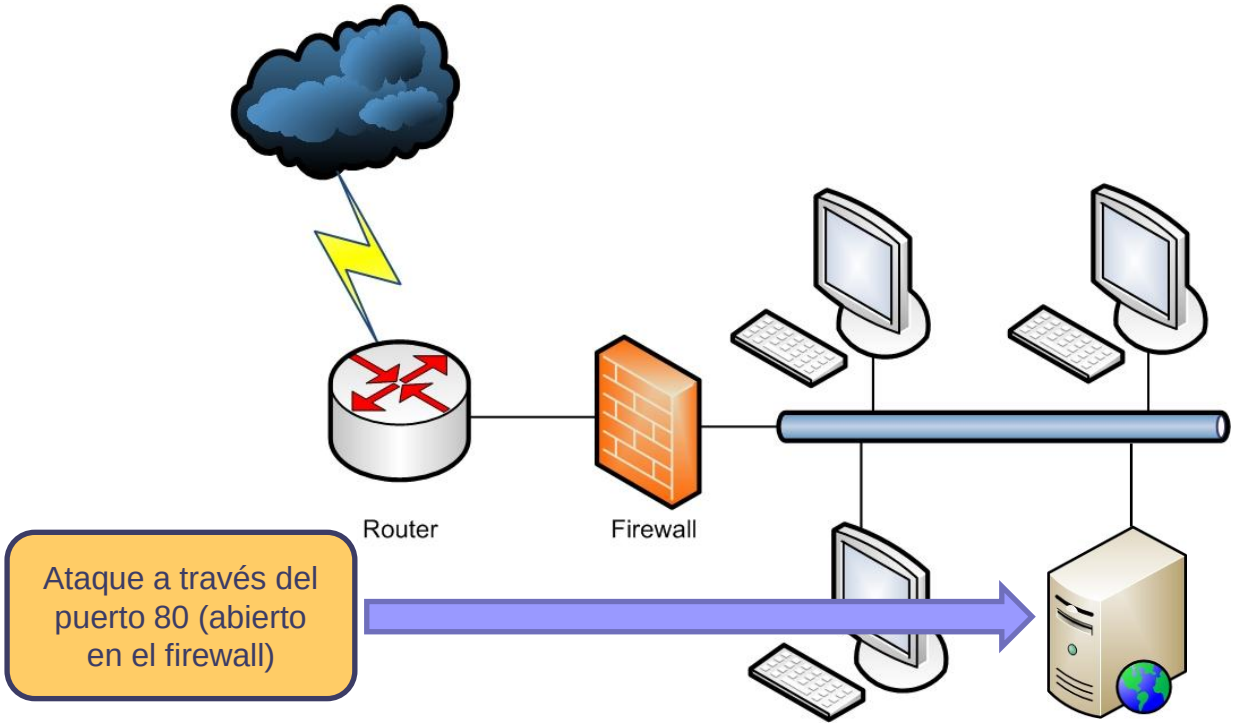
- Escenario básico de uso de un firewall



Opción 2: Servidor en red interna

Arquitecturas de firewalls
Escenario básico

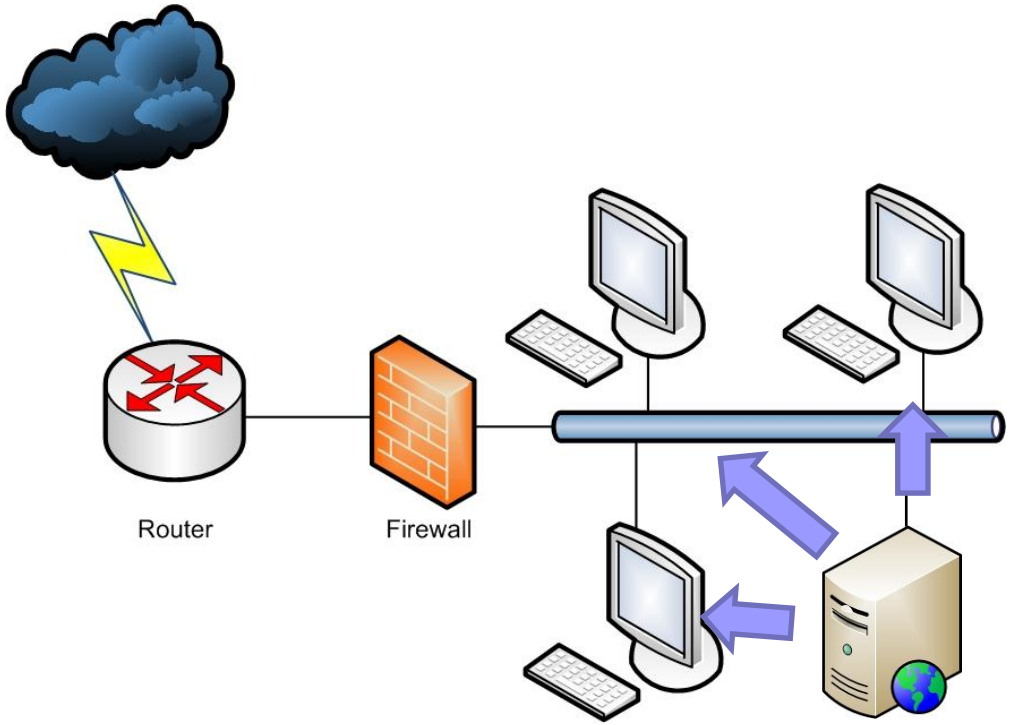
- Escenario básico de uso de un firewall



Opción 2: Servidor en red interna

Arquitecturas de firewalls
Escenario básico

- Escenario básico de uso de un firewall

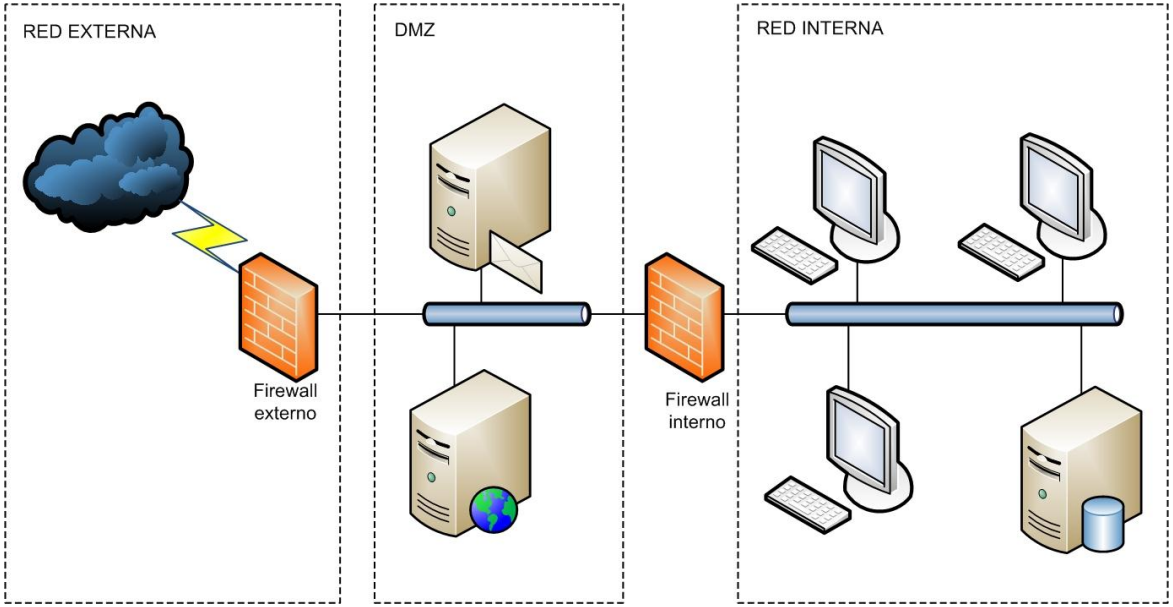


Ataques a la red interna desde el servidor

Opción 2: Servidor en red interna

Arquitecturas de firewalls
DMZ

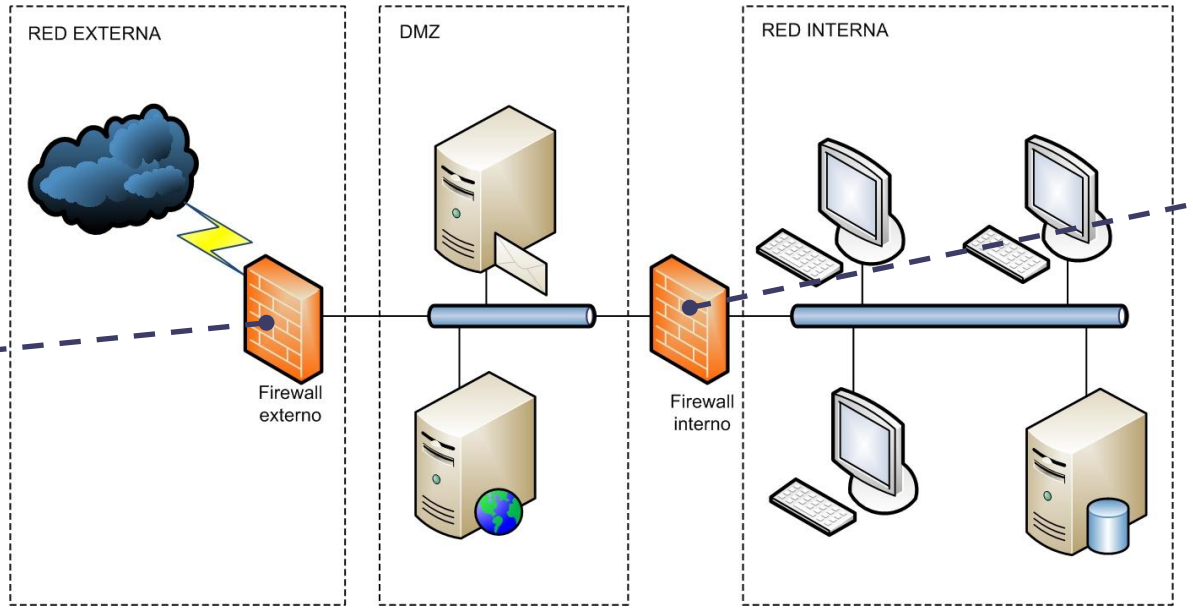
- Solución: DMZ (zona desmilitarizada)
  - Nuevo nivel de seguridad: zona de confianza intermedia
  - Suele utilizarse para ubicar servidores de acceso público, sin comprometer la seguridad de la red interna



  - Si un atacante supera el firewall externo adquiere acceso a la DMZ, pero no a la red interna

Arquitecturas de firewalls
DMZ

- Solución: DMZ (zona desmilitarizada)
  - Nuevo nivel de seguridad: zona de confianza intermedia
  - Suele utilizarse para ubicar servidores de acceso público, sin comprometer la seguridad de la red interna



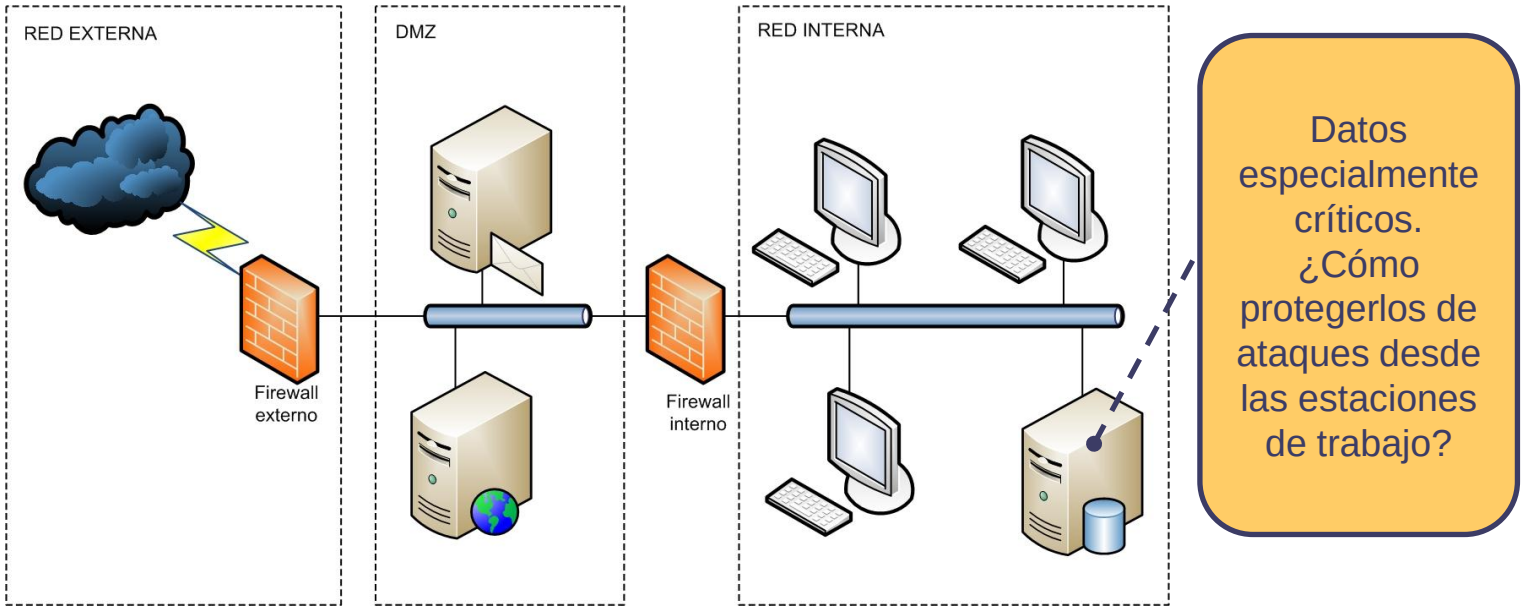
Firewall de filtrado de paquetes. Mayor rendimiento

Firewall de filtrado a nivel de aplicación. Mayor seguridad para proteger red interna

  - Si un atacante supera el firewall externo adquiere acceso a la DMZ, pero no a la red interna

Arquitecturas de firewalls
DMZ

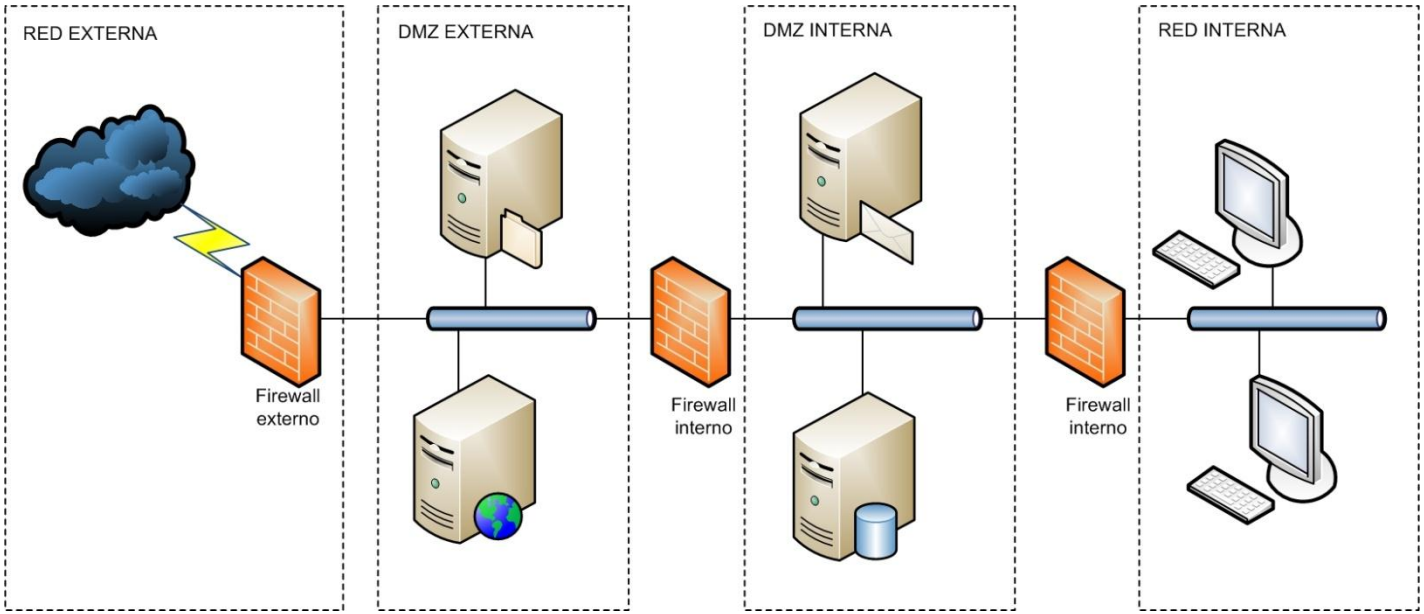
- Solución: DMZ (zona desmilitarizada)
  - Nuevo nivel de seguridad: zona de confianza intermedia
  - Suele utilizarse para ubicar servidores de acceso público, sin comprometer la seguridad de la red interna



  - Si un atacante supera el firewall externo adquiere acceso a la DMZ, pero no a la red interna

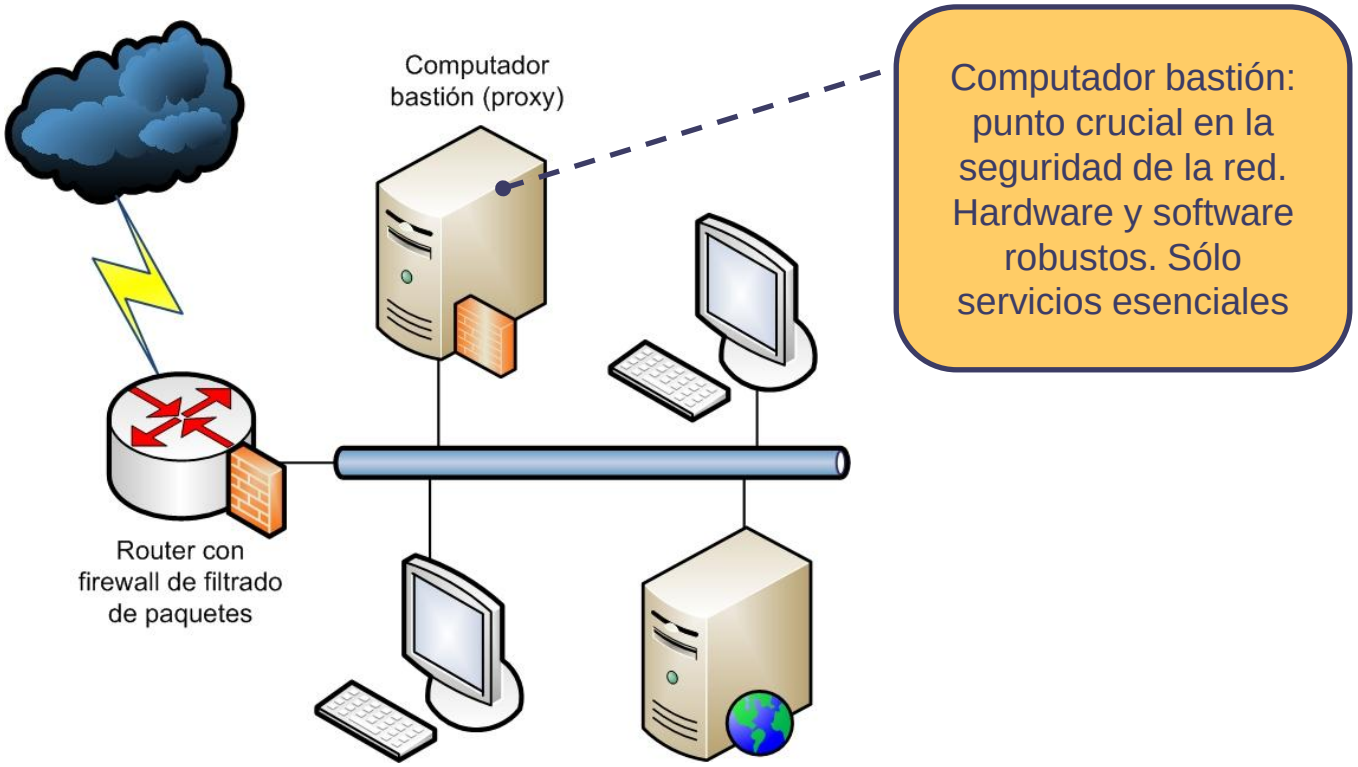
Arquitecturas de firewalls
Doble DMZ

- Se utilizan dos DMZs
  - DMZ externa: servidores de acceso público
  - DMZ interna: servidores internos
    - Protegidos de ataques desde red externa y desde equipos internos



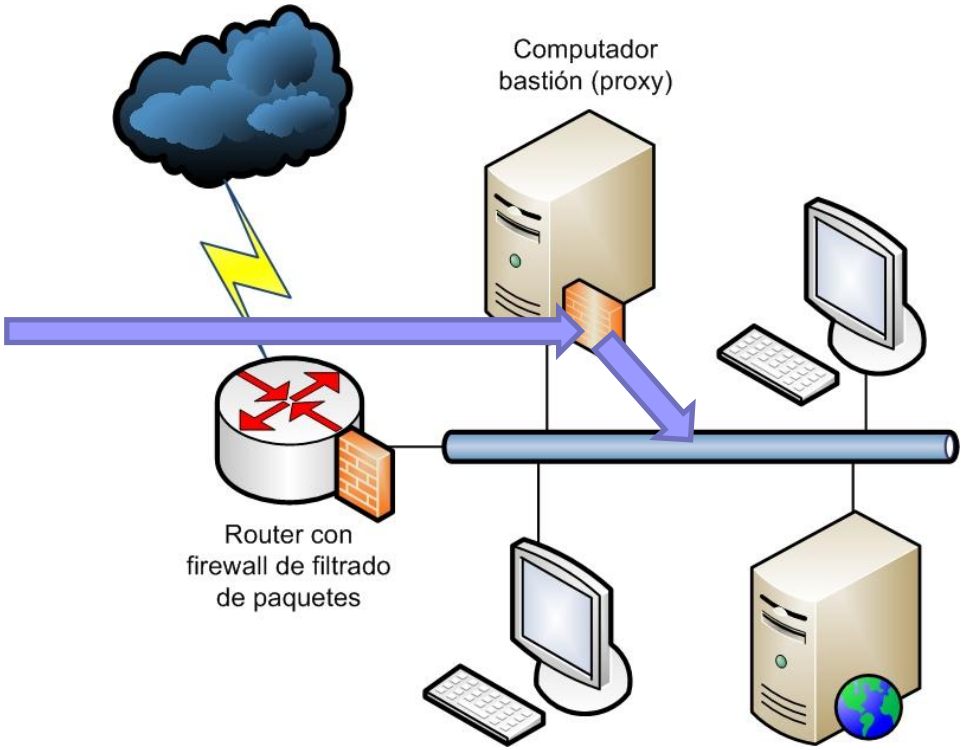
Arquitecturas de firewalls
Bastión de interfaz única

- Filtrado de paquetes + Servidor Proxy dedicado (nivel de aplicación)
  - Desde Internet, sólo se permite la entrada al computador bastión
  - Sólo se permite la salida de paquetes procedentes del computador bastión



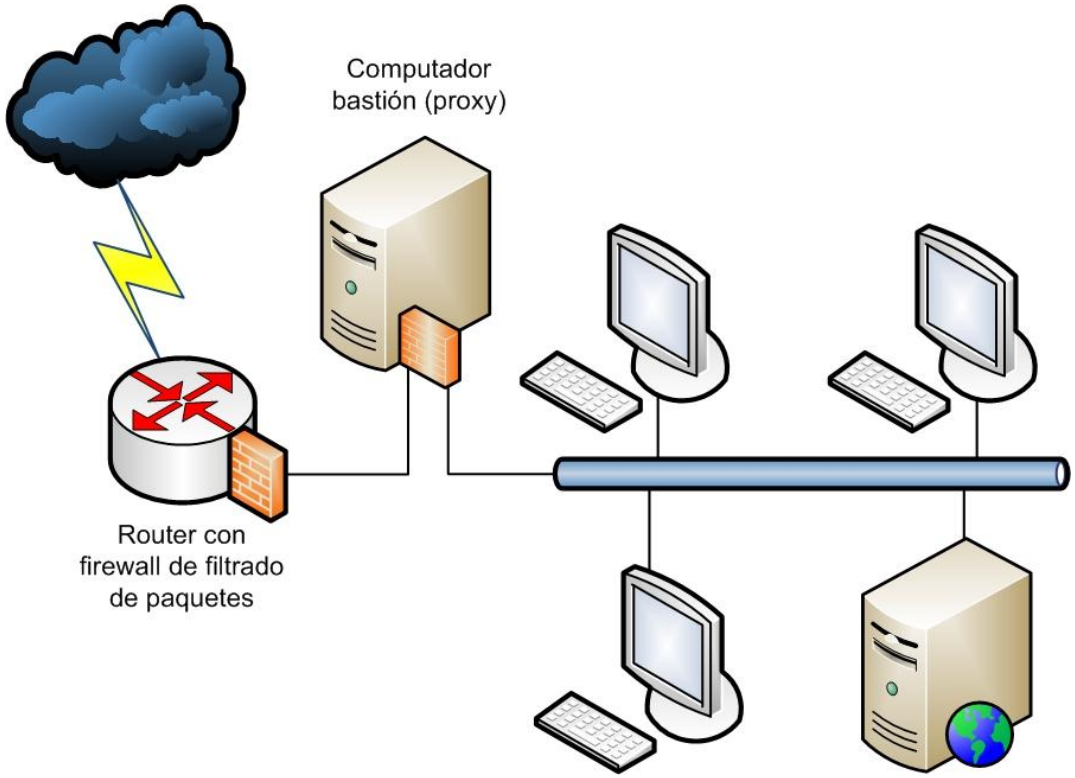
Arquitecturas de firewalls
Bastión de interfaz única

- Filtrado de paquetes + Servidor Proxy dedicado (nivel de aplicación)
  - Desde Internet, sólo se permite la entrada al computador bastión
  - Sólo se permite la salida de paquetes procedentes del computador bastión



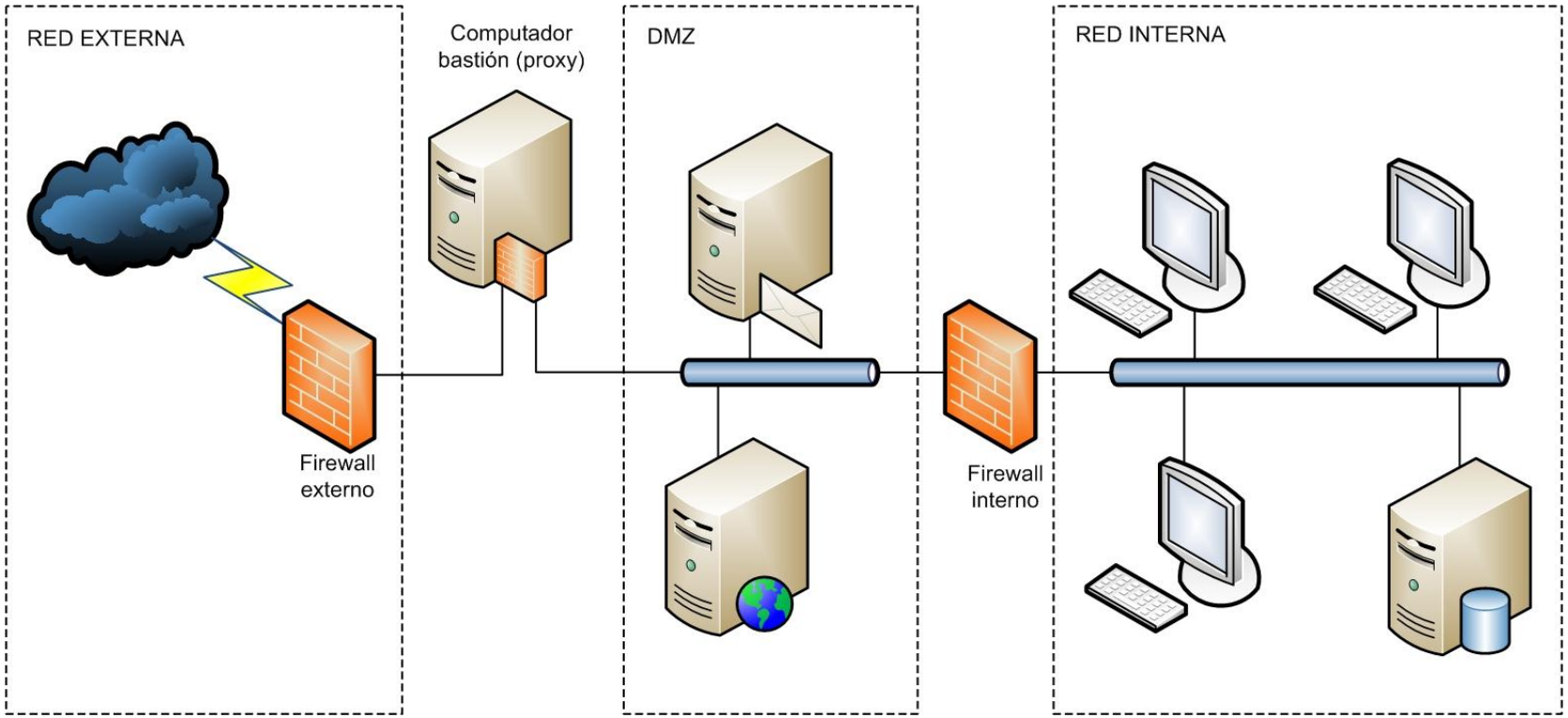
Arquitecturas de firewalls
Bastión de interfaz dual

- Doble interfaz de red
  - Prevención física ante ataques
  - Aunque un atacante supere el router de entrada, no tiene acceso directo a la red interna



Arquitecturas de firewalls
Bastión de acceso a DMZ

- Todo acceso a la DMZ debe pasar por el bastión



Bibliografía recomendada

- W. Stallings, *Fundamentos de seguridad en redes: aplicaciones y estándares*. Pearson Educación, 2003.
- W. R. Cheswick, et al., *Firewalls and Internet security: repelling the wily hacker*. Addison-Wesley Professional, 2003.
- W. J. Noonan & I. Dubrawsky. *Firewall fundamentals*. Cisco Press, 2006.