



UNIVERSIDADE DA CORUÑA

Monitorización y Filtrado

LSI - 2016/2017

José Manuel Vázquez Naya
jose@udc.es

Contenido

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

MONITORIZACIÓN

Monitorización

- Análisis de logs y/o ejecución de benchmarks para la identificación de problemas y sus causas
- Parámetros que conviene monitorizar:
 - ☐ Utilización de memoria
 - ☐ Accesos a disco
 - ☐ Uso de CPU
 - ☐ Actividad de red



Herramientas de monitorización

■ Hardware

- **dmesg** (diagnostic message, mensajes de diagnóstico): es un comando presente en los sistemas operativos Unix que lista el buffer de mensajes del núcleo.
 - Mensajes generados durante el arranque del sistema y durante la depuración de aplicaciones
 - La salida de dmesg se guarda en `/var/log/dmesg`
- **lsmod**: muestra qué módulos arrancables por el Kernel están cargados actualmente (contenido del archivo `/proc/modules`)
- **lspci**: muestra información sobre los buses PCI en el sistema y los dispositivos conectados a ellos.
 - **lsusb**: similar, para buses USB y dispositivos



Herramientas de monitorización

■ Dependencias

- **ldd** (List Dynamic Dependencies): muestra las bibliotecas compartidas que necesita cada programa o biblioteca compartida especificada en la línea de comandos

```
$ ldd /usr/sbin/sshd
linux-vdso.so.1 => (0x00007ffffd67ff000)
libwrap.so.0 => /lib/libwrap.so.0 (0x00007faeb81a4000)
libpam.so.0 => /lib/libpam.so.0 (0x00007faeb7f98000)
libselinux.so.1 => /lib/libselinux.so.1 (0x00007faeb7d79000)
...
```

- **ldconfig**: se usa para crear, actualizar y borrar enlaces simbólicos para librerías compartidas, en el archivo /etc/ld.so.conf

Herramientas de monitorización

■ Procesos, archivos abiertos, etc.

- ☐ quota
- ☐ ulimit
- ☐ ...

■ Sistema de ficheros

- ☐ fsck
- ☐ mkfs
- ☐ mount

Herramientas 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: Tiempo que lleva encendido el sistema

Herramientas de monitorización

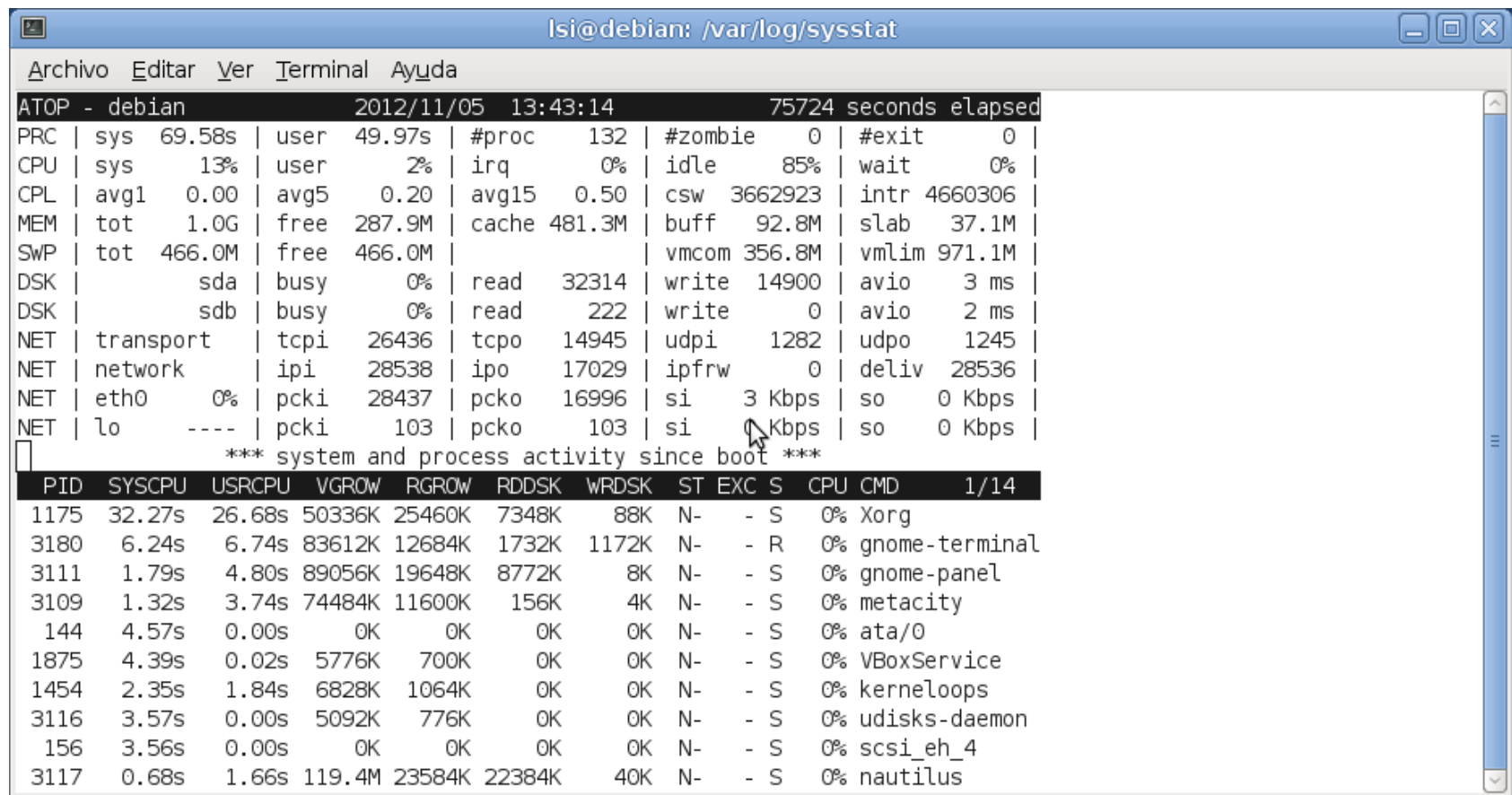
■ Monitorización de uso de disco

- ☐ 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 Lista procesos
- ☐ top Muestra información en tiempo real de los procesos del sistema
- ☐ atop, htop Similares a top

Herramientas de monitorización



lsid@debian: /var/log/sysstat

Archivo Editar Ver Terminal Ayuda

ATOP - debian 2012/11/05 13:43:14 75724 seconds elapsed

PRC	sys	69.58s	user	49.97s	#proc	132	#zombie	0	#exit	0
CPU	sys	13%	user	2%	irq	0%	idle	85%	wait	0%
CPL	avg1	0.00	avg5	0.20	avg15	0.50	csw	3662923	intr	4660306
MEM	tot	1.0G	free	287.9M	cache	481.3M	buff	92.8M	slab	37.1M
SWP	tot	466.0M	free	466.0M			vmcom	356.8M	vmlim	971.1M
DSK	sda	busy	0%	read	32314	write	14900	avio	3 ms	
DSK	sdb	busy	0%	read	222	write	0	avio	2 ms	
NET	transport	tcpi	26436	tcpo	14945	udpi	1282	udpo	1245	
NET	network	ipi	28538	ipo	17029	ipfrw	0	deliv	28536	
NET	eth0	0%	pcki	28437	pcko	16996	si	3 Kbps	so	0 Kbps
NET	lo	----	pcki	103	pcko	103	si	0 Kbps	so	0 Kbps

*** system and process activity since boot ***

PID	SYSCPU	USRCPU	VGR0W	RGR0W	RDDSK	WRDSK	ST	EXC	S	CPU	CMD	1/14
1175	32.27s	26.68s	50336K	25460K	7348K	88K	N-	-	S	0%	Xorg	
3180	6.24s	6.74s	83612K	12684K	1732K	1172K	N-	-	R	0%	gnome-terminal	
3111	1.79s	4.80s	89056K	19648K	8772K	8K	N-	-	S	0%	gnome-panel	
3109	1.32s	3.74s	74484K	11600K	156K	4K	N-	-	S	0%	metacity	
144	4.57s	0.00s	0K	0K	0K	0K	N-	-	S	0%	ata/0	
1875	4.39s	0.02s	5776K	700K	0K	0K	N-	-	S	0%	VBoxService	
1454	2.35s	1.84s	6828K	1064K	0K	0K	N-	-	S	0%	kerneloops	
3116	3.57s	0.00s	5092K	776K	0K	0K	N-	-	S	0%	udisks-daemon	
156	3.56s	0.00s	0K	0K	0K	0K	N-	-	S	0%	scsi_eh_4	
3117	0.68s	1.66s	119.4M	23584K	22384K	40K	N-	-	S	0%	nautilus	

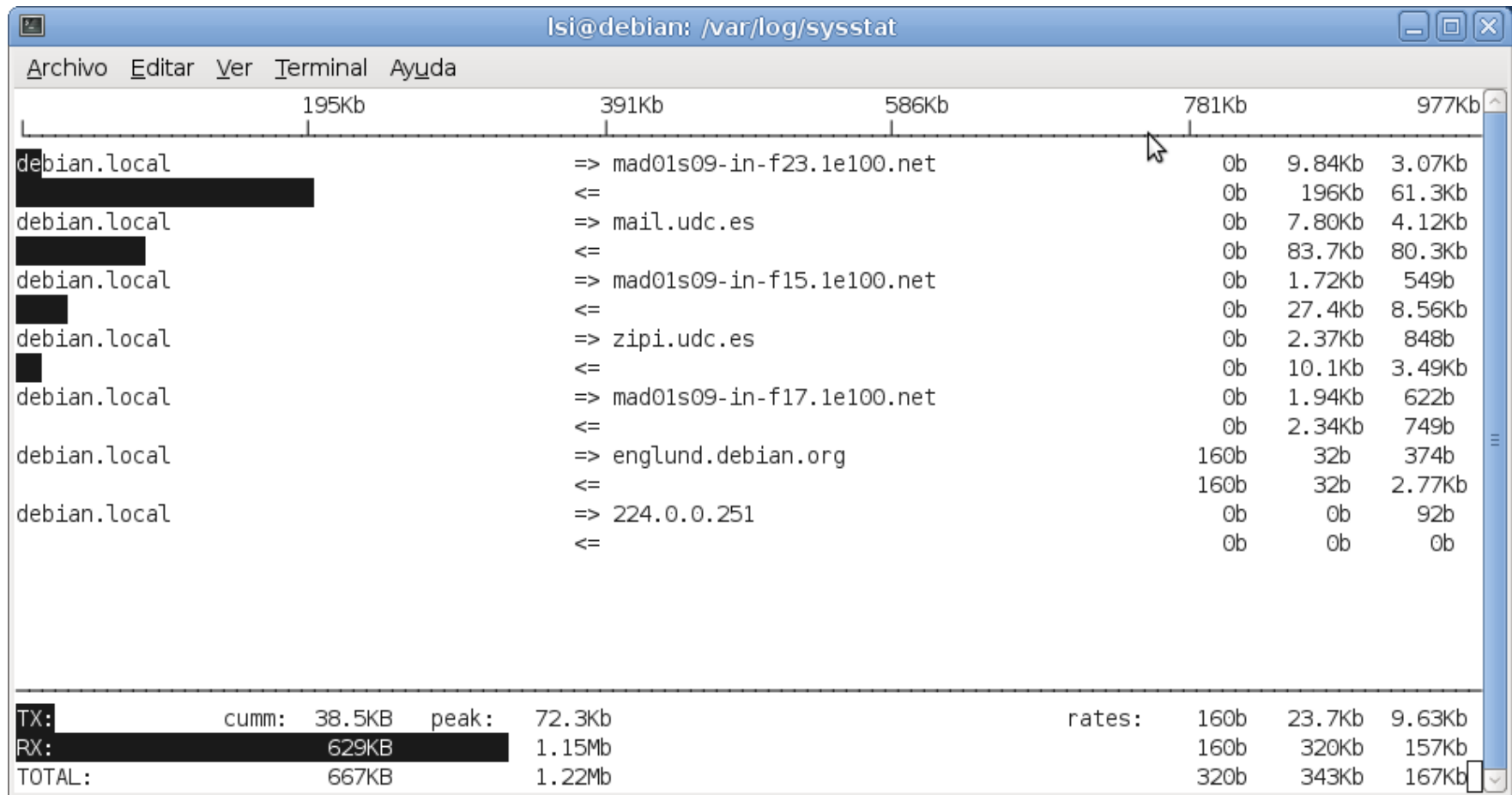
atop

Herramientas de monitorización

■ Monitorización de red

- ☐ iftop Muestra conexiones de red
- ☐ iptraf Proporciona estadísticas de red
- ☐ vnstat Monitoriza tráfico de red y almacena log

Herramientas de monitorización



iftop

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)
```

	CPU	%user	%nice	%system	%iowait	%steal	%idle
11:43:15							
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)
```

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

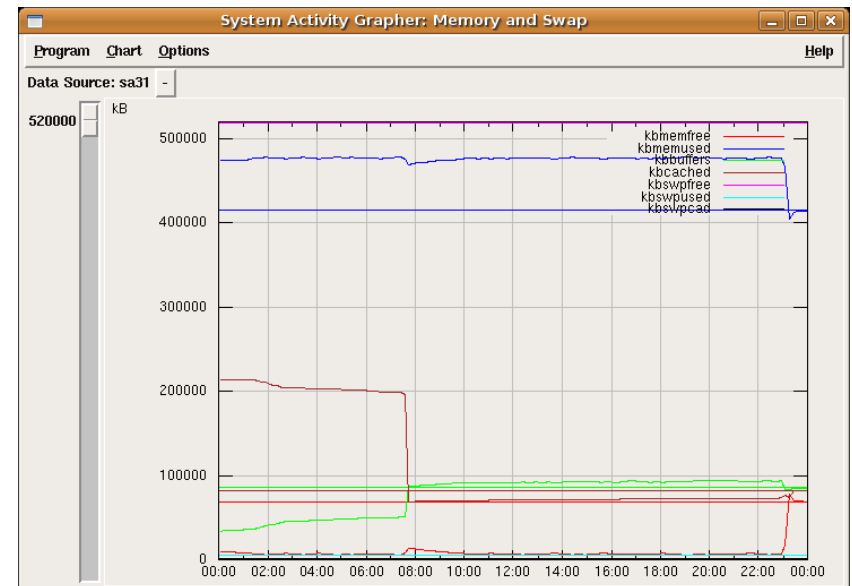
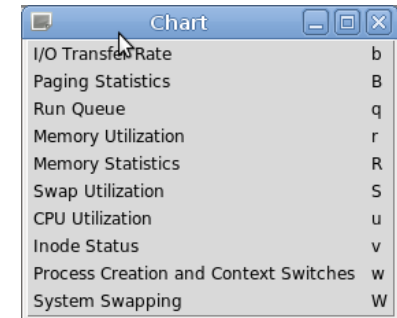
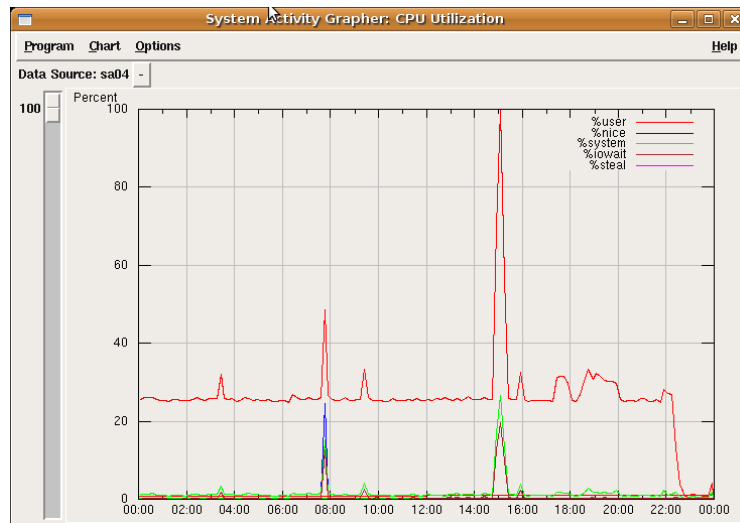
```
root@debian:/var/log# sar -m 1 1
```

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

	CPU	MHz
11:46:46		
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

■ 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

- ... herramientas vistas hasta el momento están pensadas para una máquina local
- ¿Qué pasa en entornos mayores?
 - Uso de herramientas centralizadas de monitorización
 - nagios, ntop, Zabbix, ...
 - Comparación de sistemas de monitorización de redes

Monitorización

- En resumen...

Información

Información Información

Información Información Información Información

Información Información

Información Información

Información Información

Información

FILTRADO

Introducción

Seguridad perimetral

- Arquitectura y elementos de red que proporcionan seguridad a una red interna frente a una red externa (generalmente Internet)
- Los **firewalls** son el principal “vigilante” de la entrada a un equipo a través de la red



Introducción

Firewalls

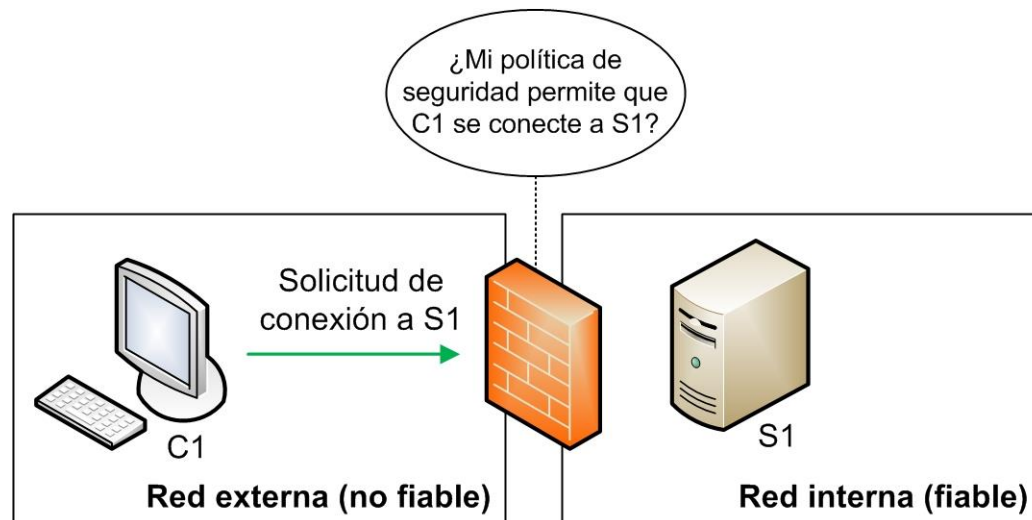
- Un **firewall** (cortafuegos) es cualquier mecanismo, ya sea software o hardware, que filtra el tráfico entre redes
 - Separan zonas de confianza (*trusted zones*) de zonas potencialmente hostiles (*untrusted zones*)
 - Analizan, registran y pueden bloquear el tráfico
 - Deniegan intentos de conexión 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 debe ser 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

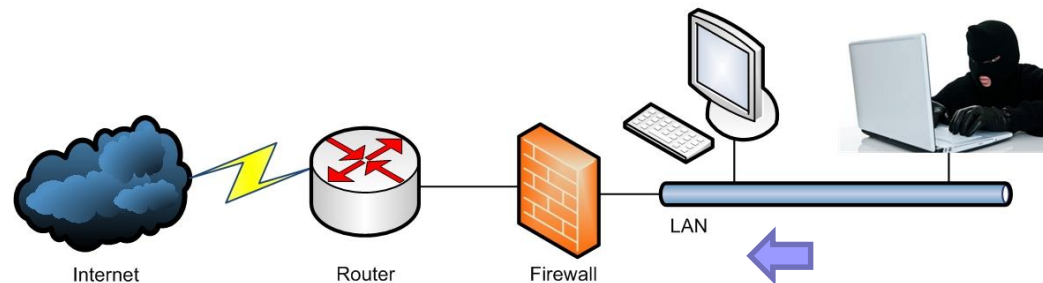
Firewalls

■ 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, 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 dejas las ventanas abiertas!**

TIPOS DE FIREWALLS

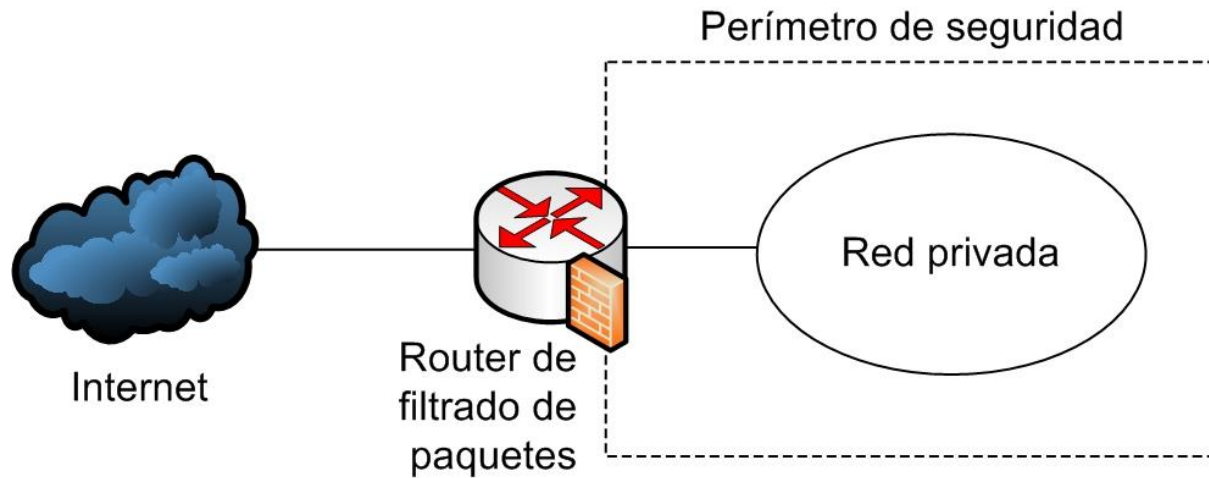
Tipos de firewalls

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



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)

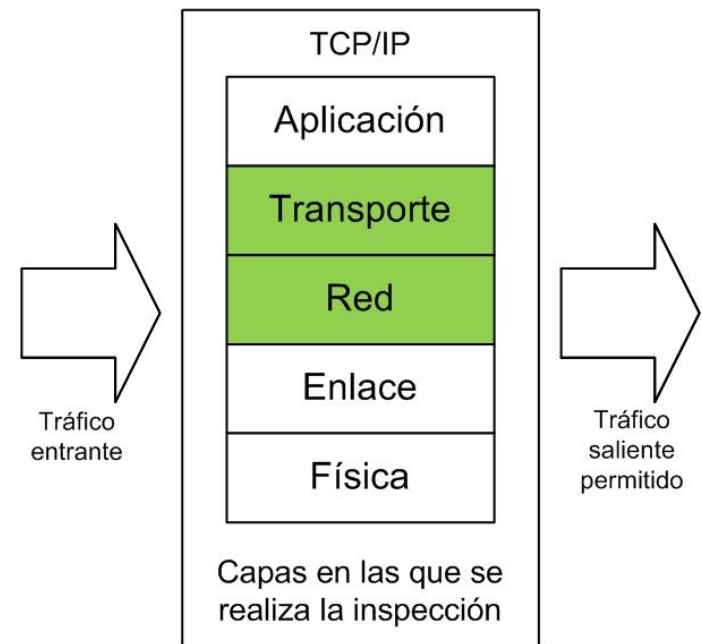
Tipos de firewalls

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

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

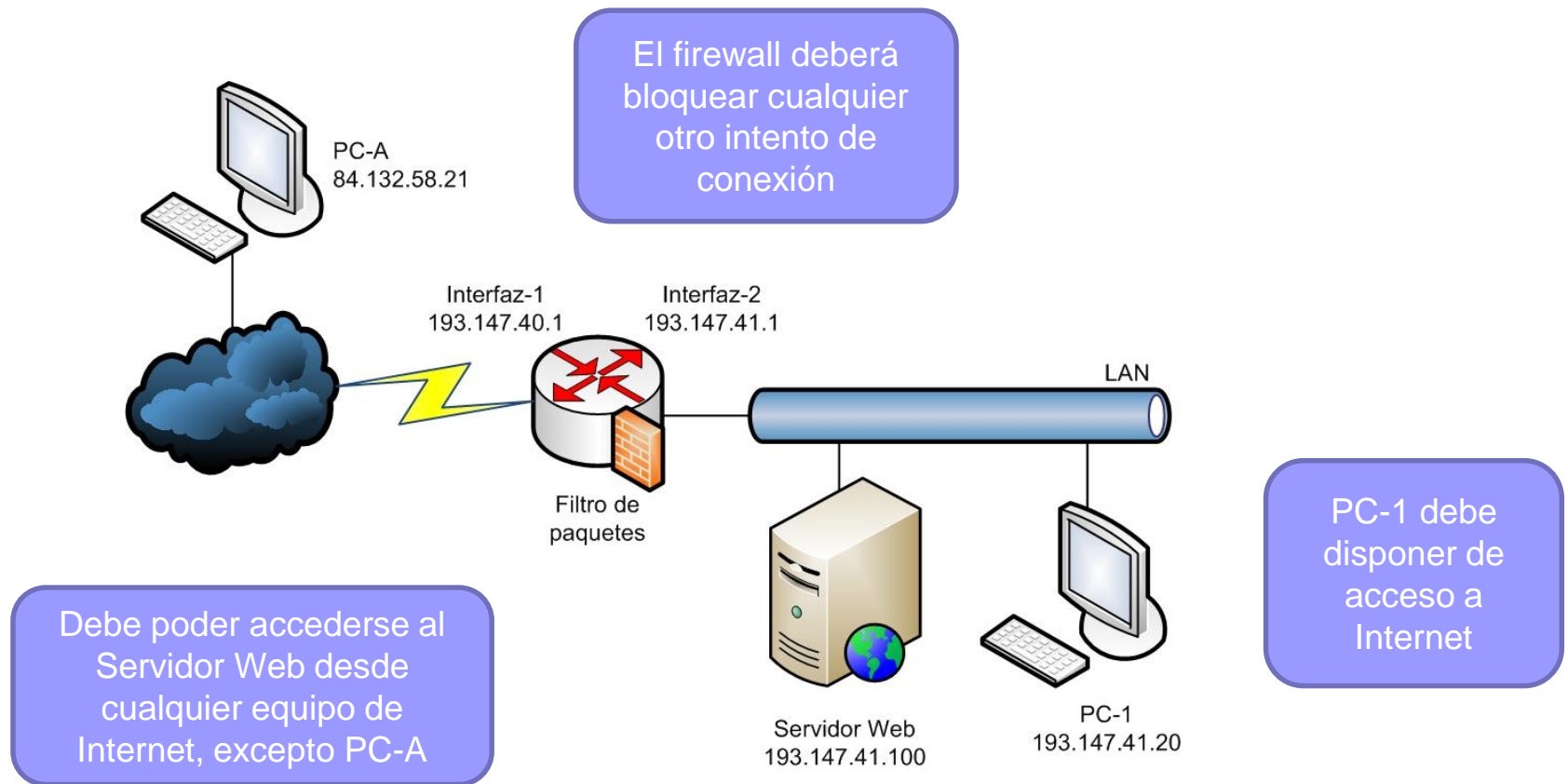
Filtrado estático de paquetes (stateless)

- 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 realiza la acción asociada (aceptar, retransmitir, descartar, ...)
 - Si no hay correspondencia, se realiza una acción predeterminada:
 - Descartar por defecto (**política restrictiva**)
 - Todo lo que no está expresamente permitido está prohibido
 - Más seguridad, mayor "molestia" para los usuarios finales
 - Aceptar por defecto (**política permisiva**)
 - 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:

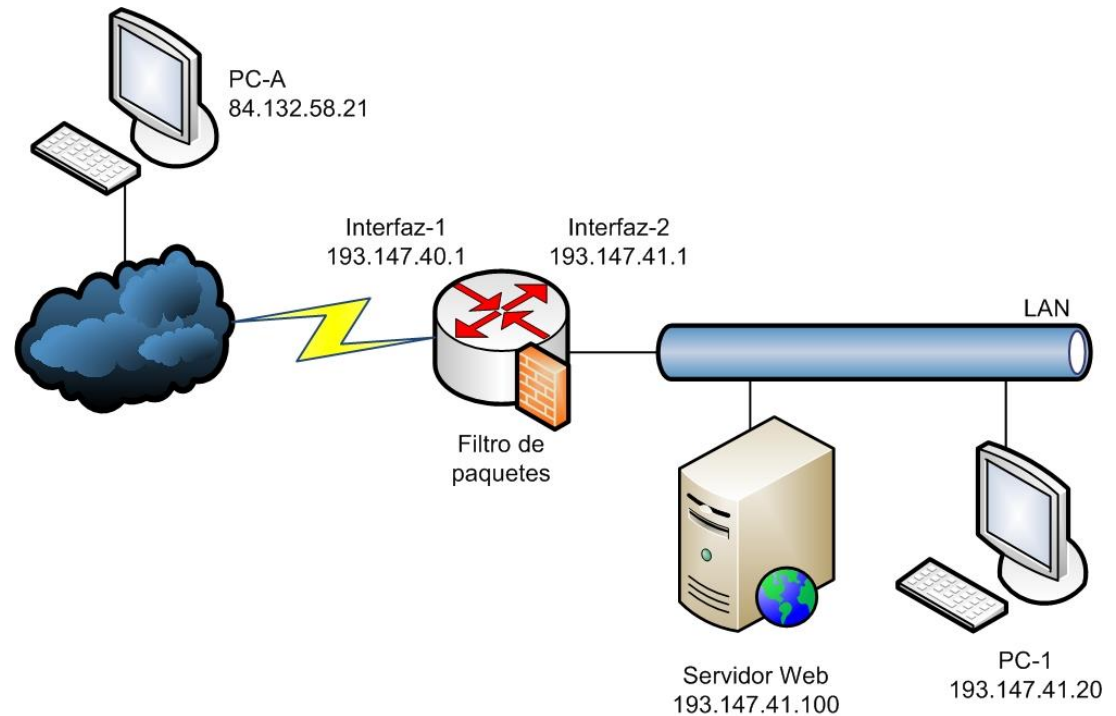


Tipos de firewalls

Filtrado estático de paquetes (stateless)

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

¿Estas reglas son suficientes?

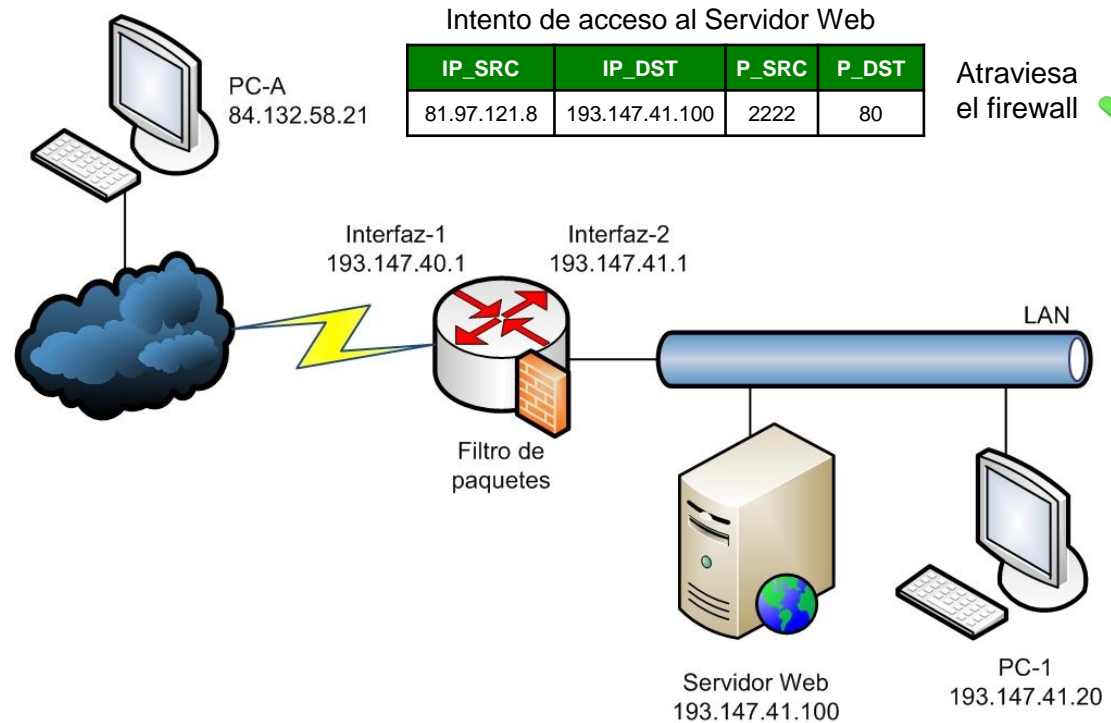


acción	origen	puerto	destino	puerto
bloquear	84.132.58.21	*	*	*
permitir	*	*	193.147.41.100	80
bloquear	*	*	*	*

Tipos de firewalls

Filtrado estático de paquetes (stateless)

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

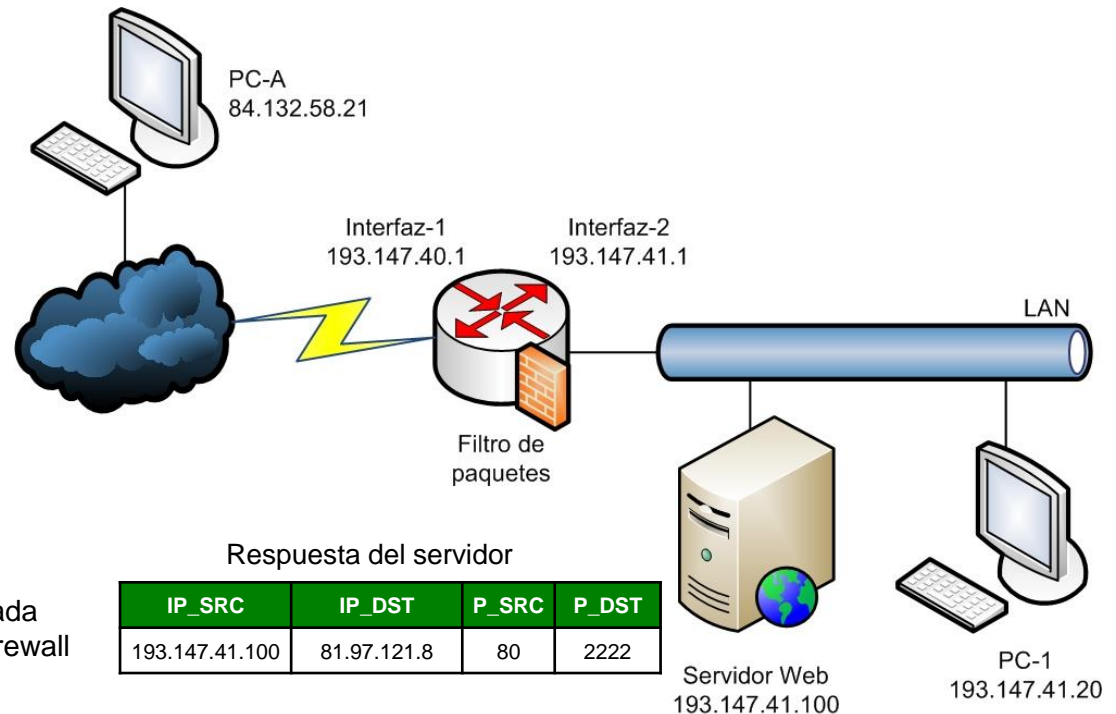


acción	origen	puerto	destino	puerto
bloquear	84.132.58.21	*	*	*
permitir	*	*	193.147.41.100	80
bloquear	*	*	*	*

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)

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



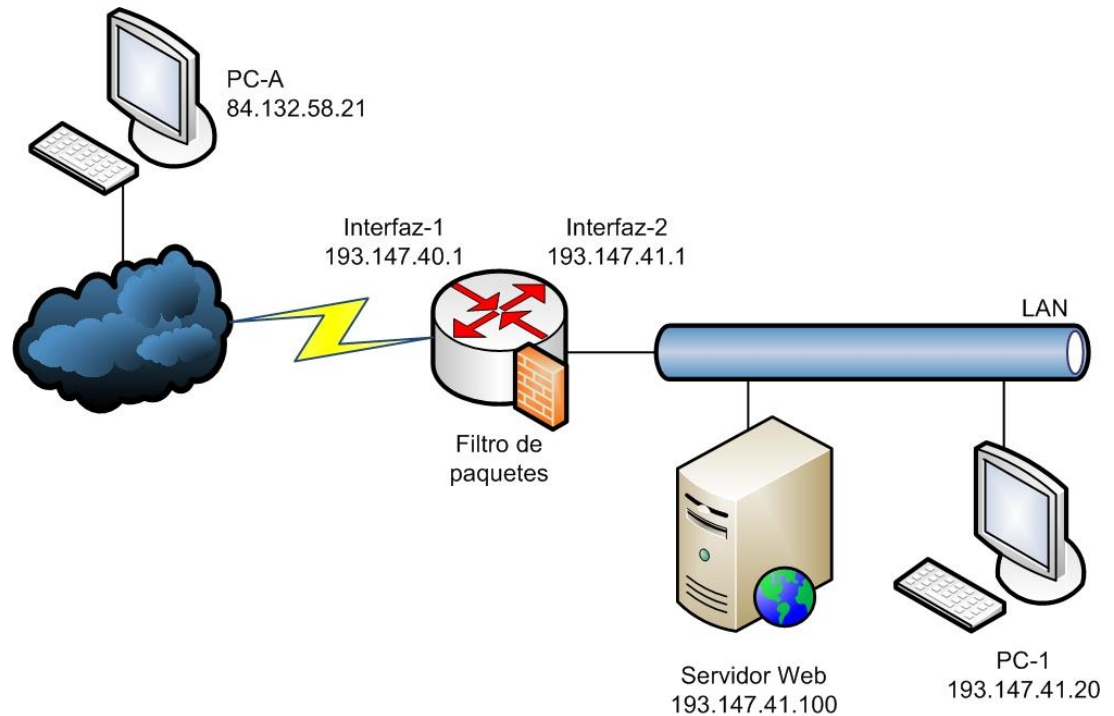
acción	origen	puerto	destino	puerto
bloquear	84.132.58.21	*	*	*
permitir	*	*	193.147.41.100	80
permitir	193.147.41.100	80	*	>1023
bloquear	*	*	*	*

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



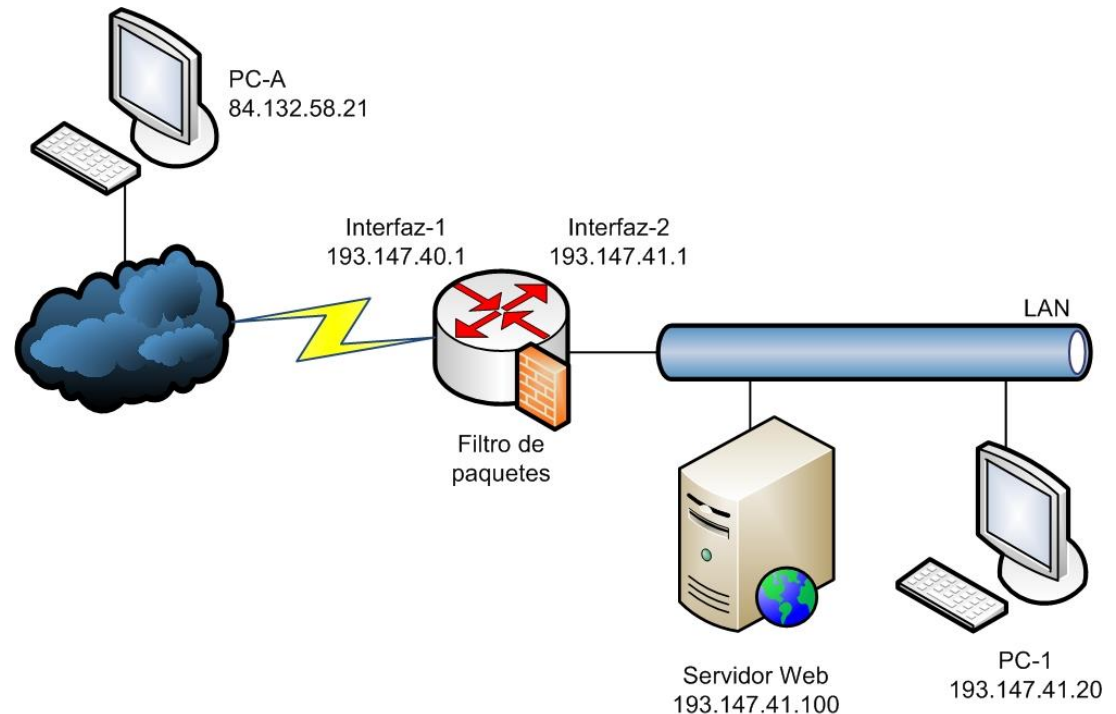
acción	origen	puerto	destino	puerto
bloquear	84.132.58.21	*	*	*
permitir	*	*	193.147.41.100	80
permitir	193.147.41.100	80	*	>1023
bloquear	*	*	*	*

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

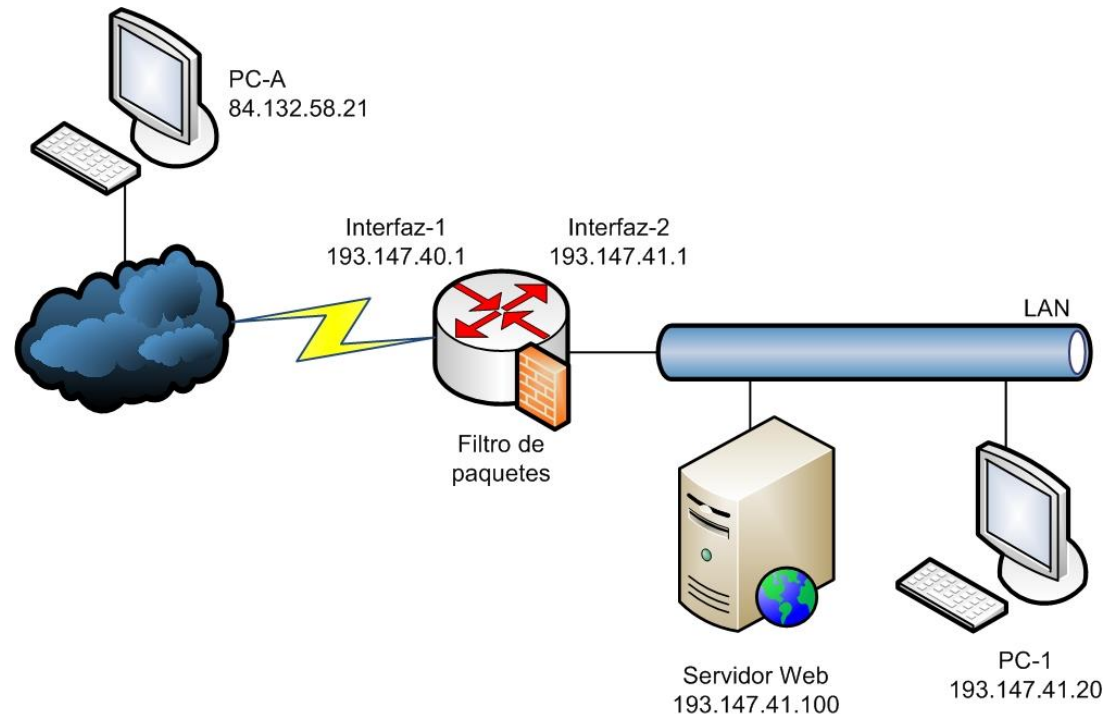


Tipos de firewalls

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	*	*	*	*

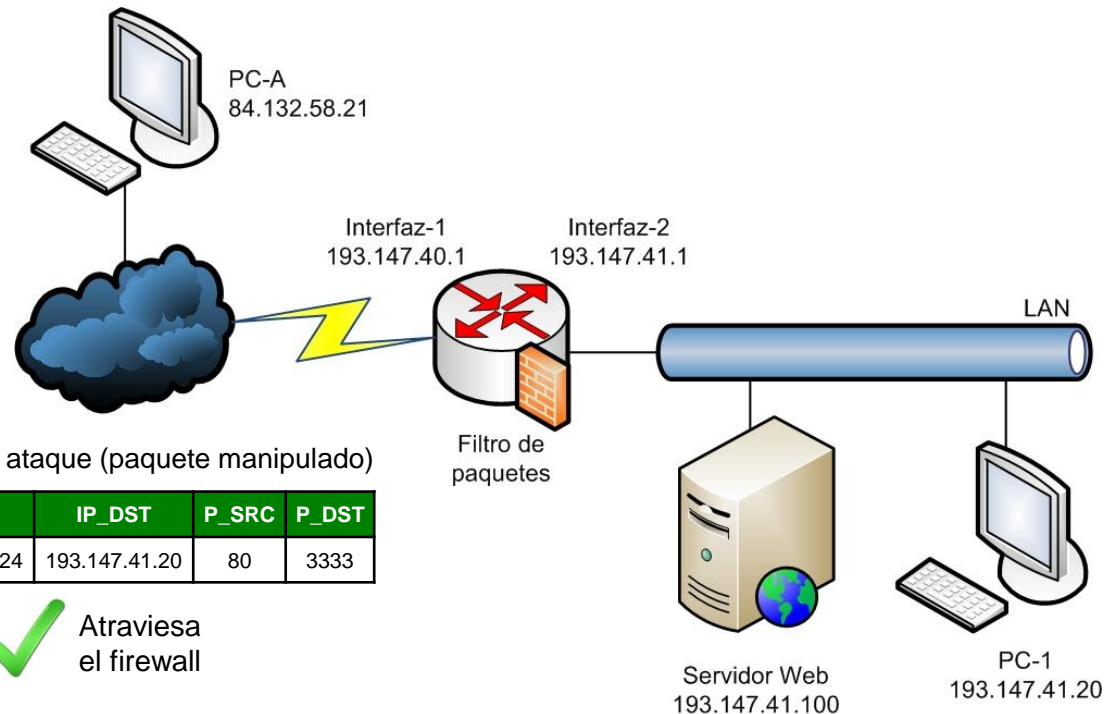
Entrada →

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



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

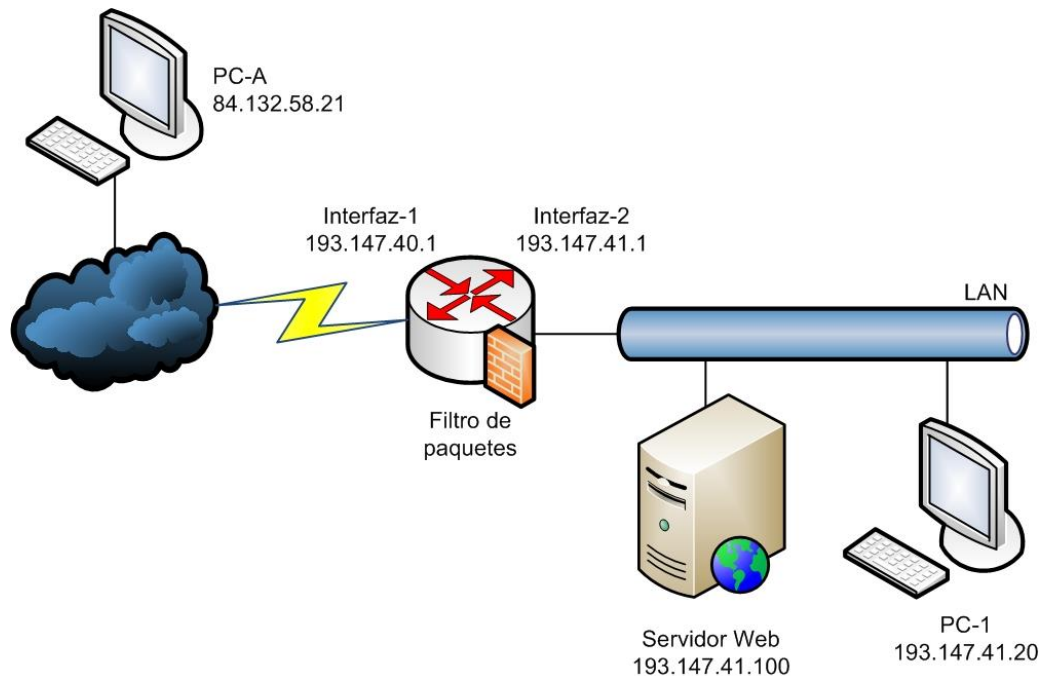
Filtrado estático de paquetes (stateless)

- 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)



Atraviesa
el firewall

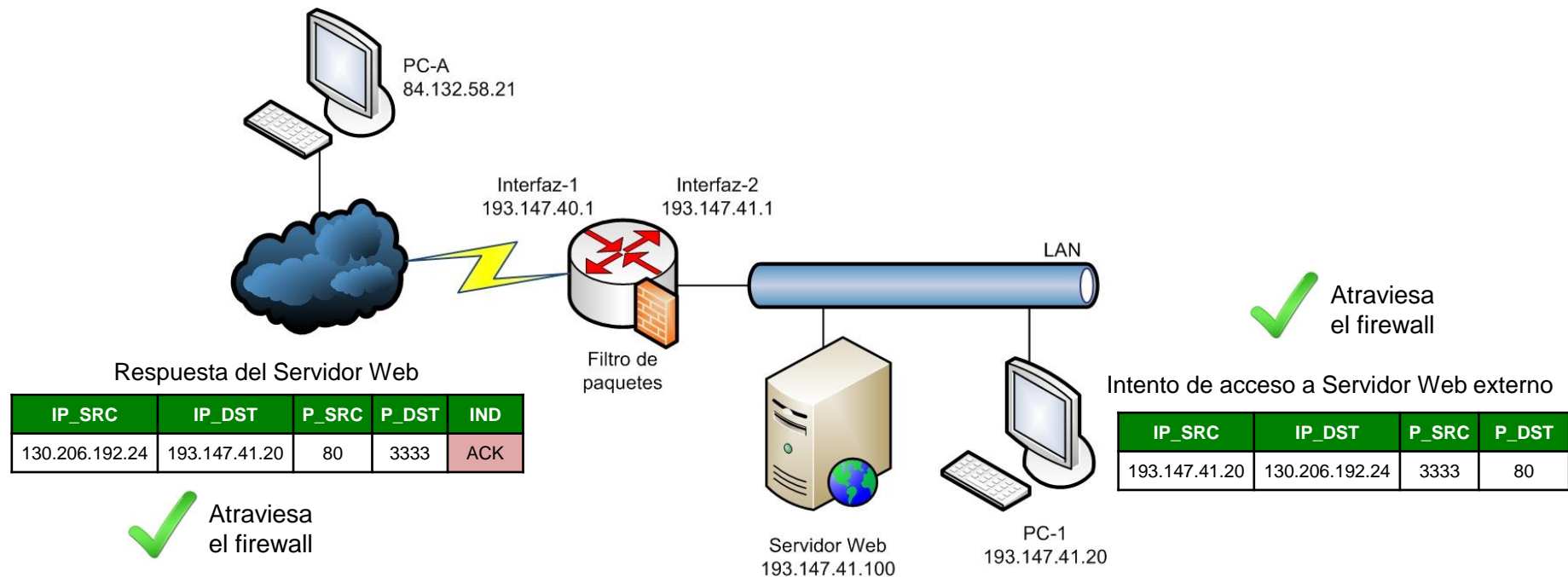
Intento de acceso a Servidor Web externo

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

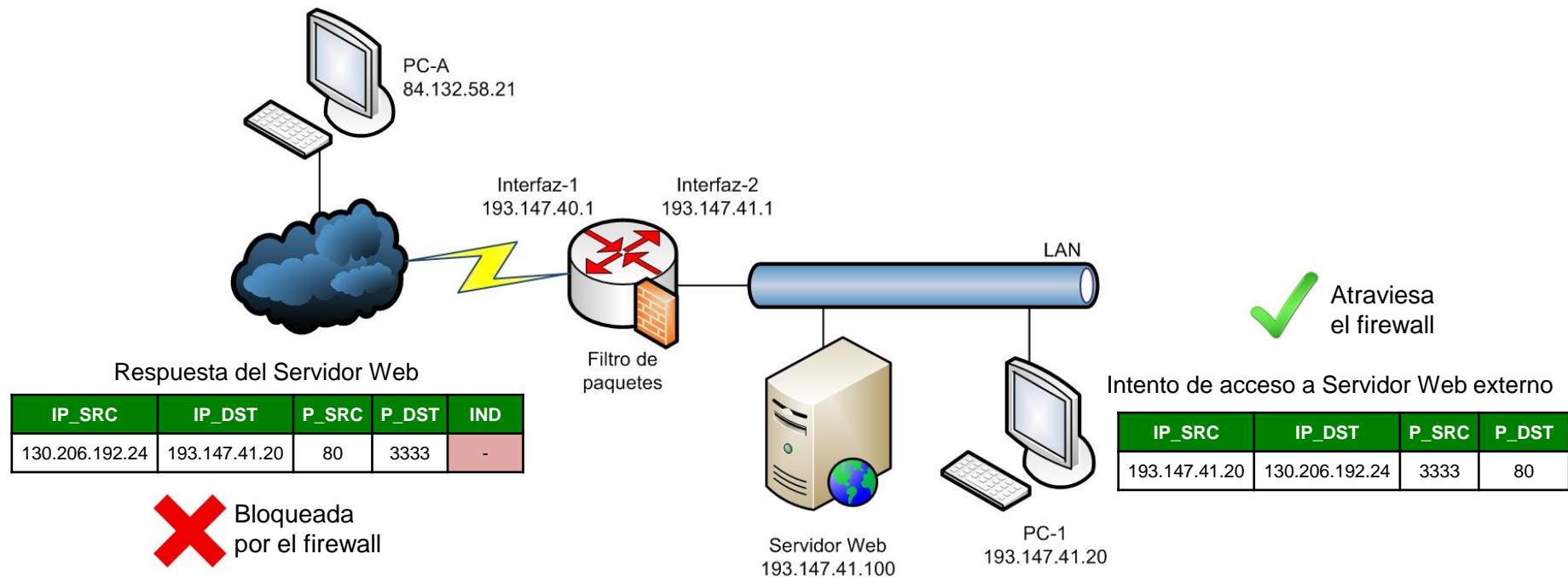
Filtrado estático de paquetes (stateless)



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)

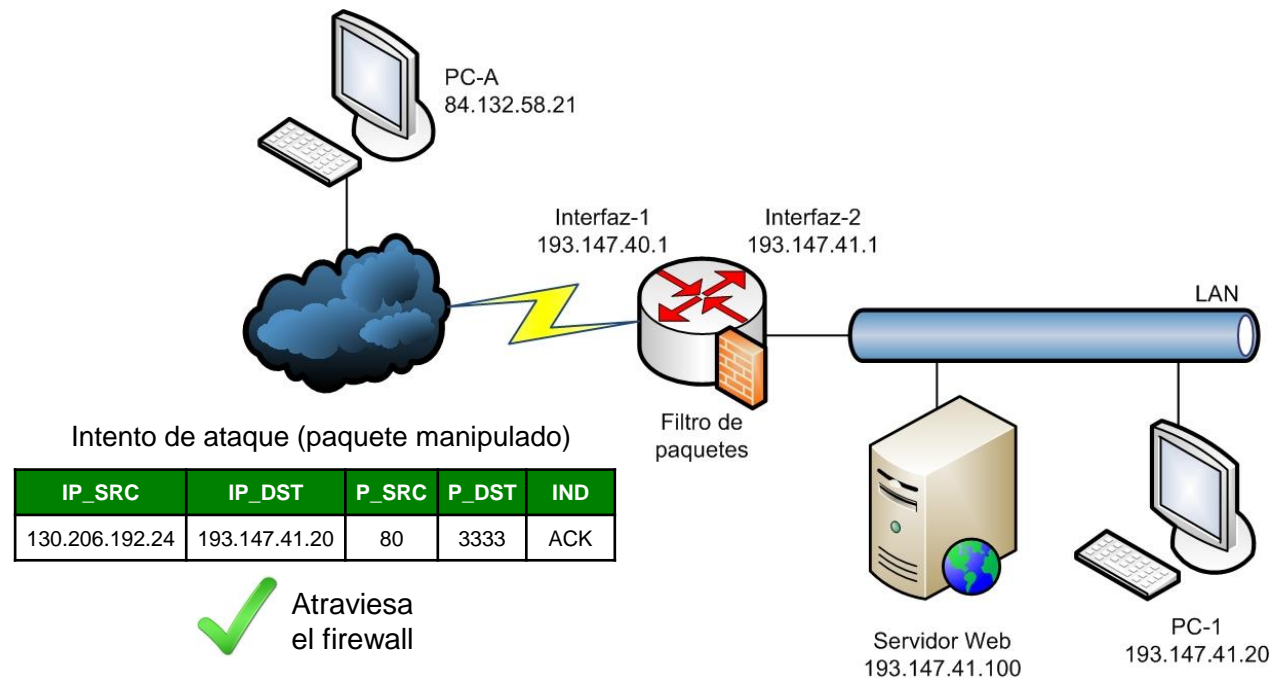


acción	origen	puerto	destino	puerto	Indicador
permitir	193.147.41.20	*	*	80	
permitir	*	80	193.147.41.20	*	ACK

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*)

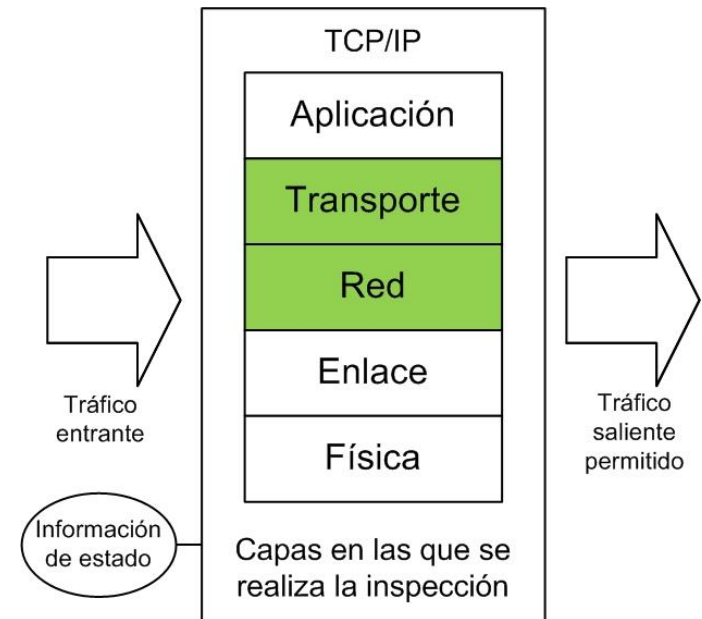


- **Filtrado a nivel de aplicación**

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

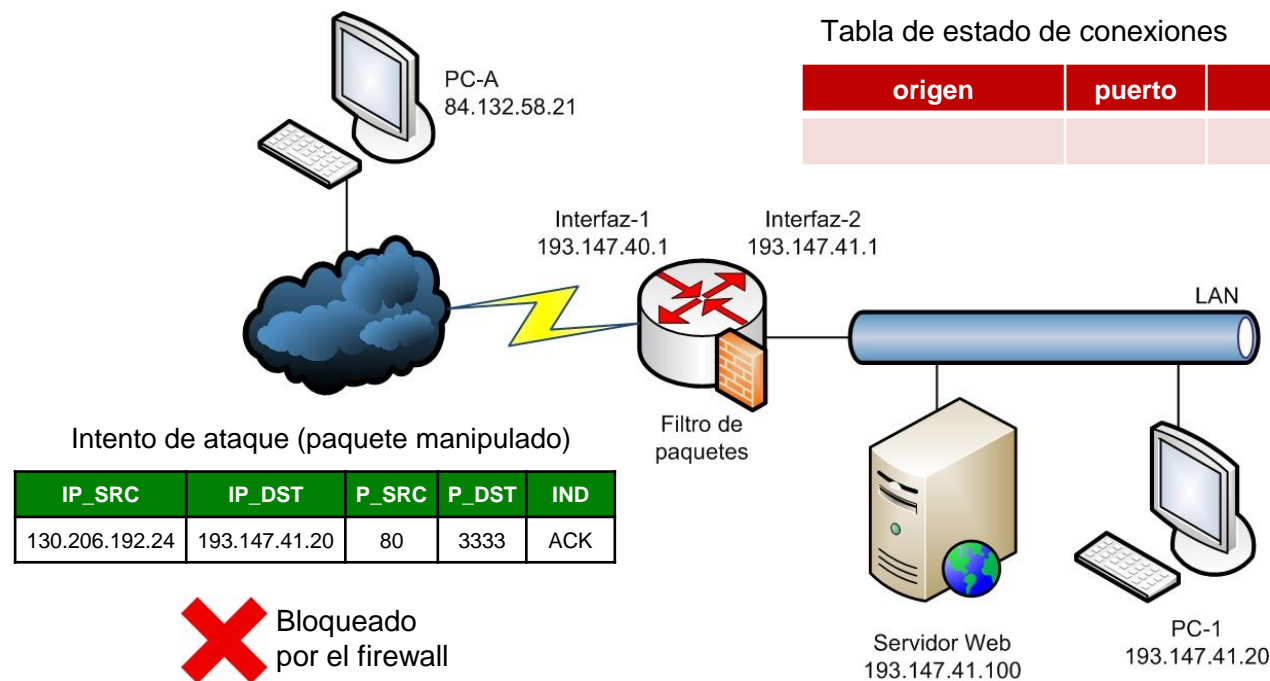


Tabla de estado de conexiones

origen	puerto	destino	puerto

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

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)

PC-1 debe disponer de acceso a Internet

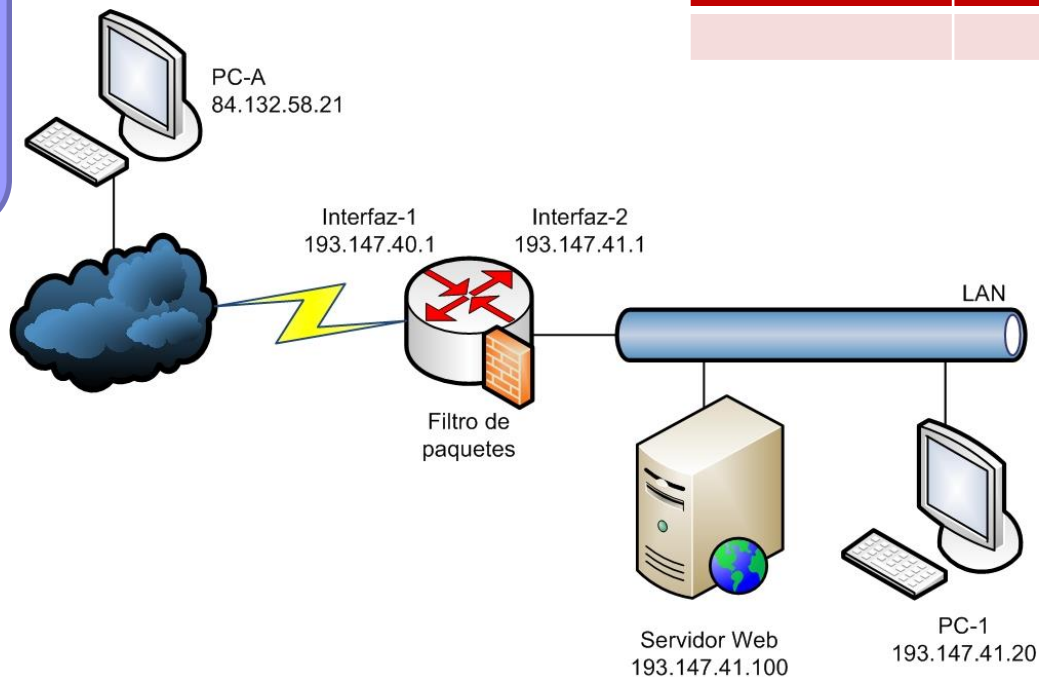


Tabla de estado de conexiones

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

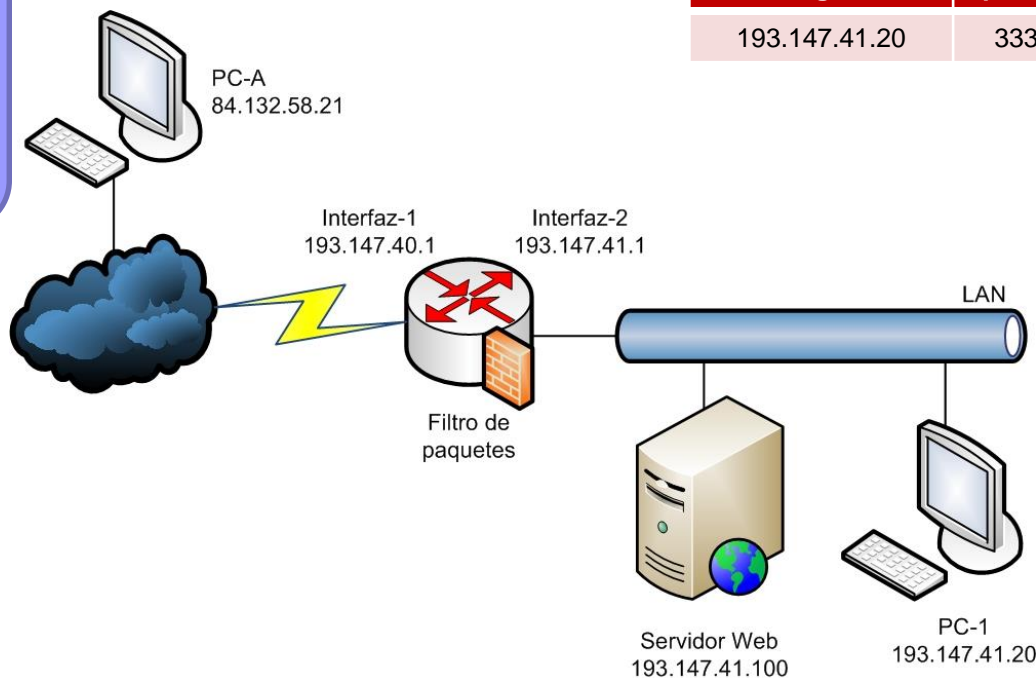


Tabla de estado de conexiones

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

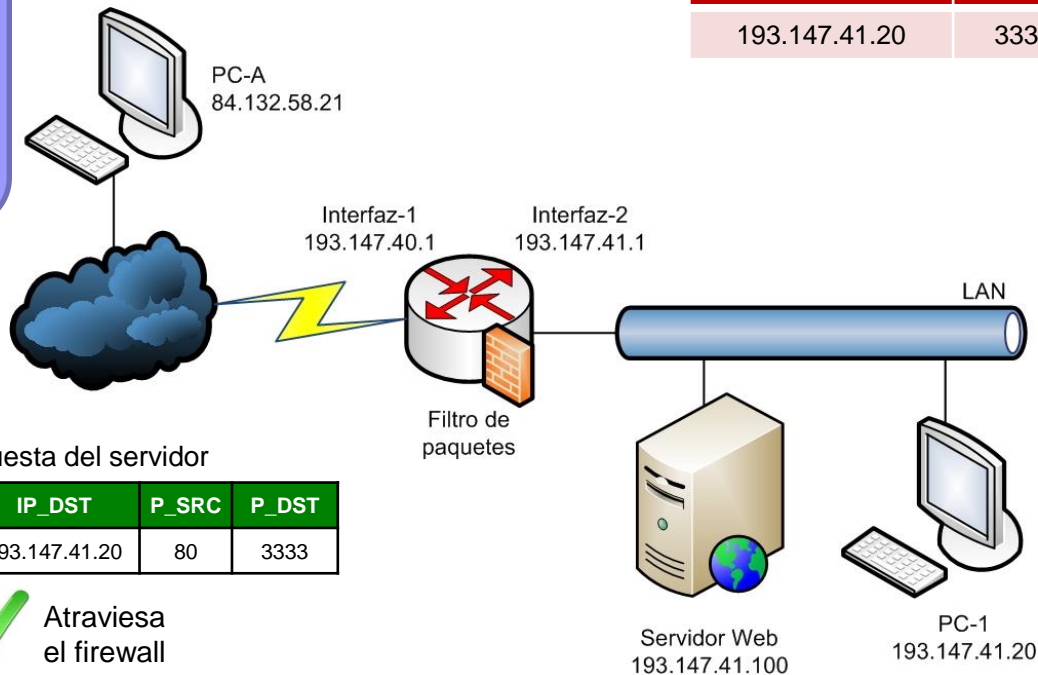
Filtrado dinámico de paquetes (stateful)

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



Atraviesa el firewall

Reglas

acción	origen	puerto	destino	puerto
permitir	193.147.41.20	*	*	80

Tipos de firewalls

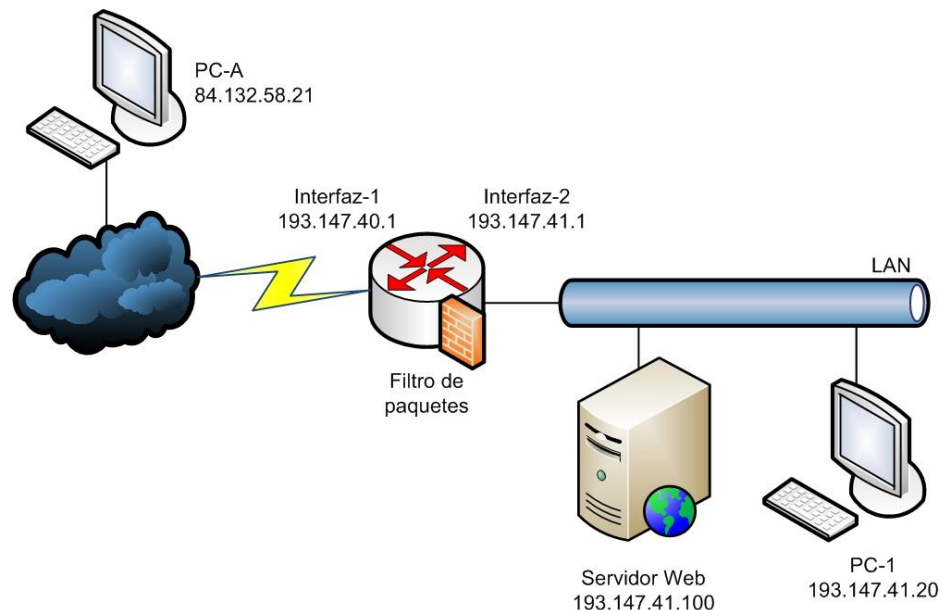
Filtrado dinámico de paquetes (stateful)

- 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

■ 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

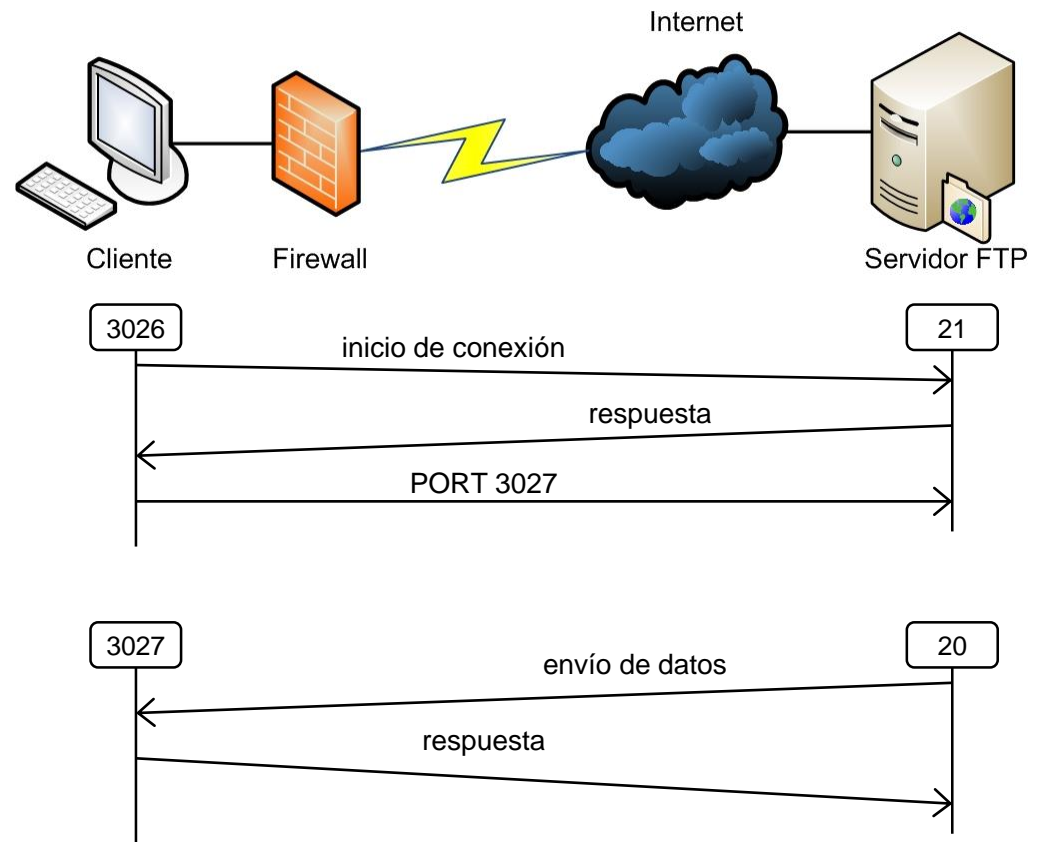
Filtrado de paquetes

■ Limitaciones de los firewalls de filtrado de paquetes

1. 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

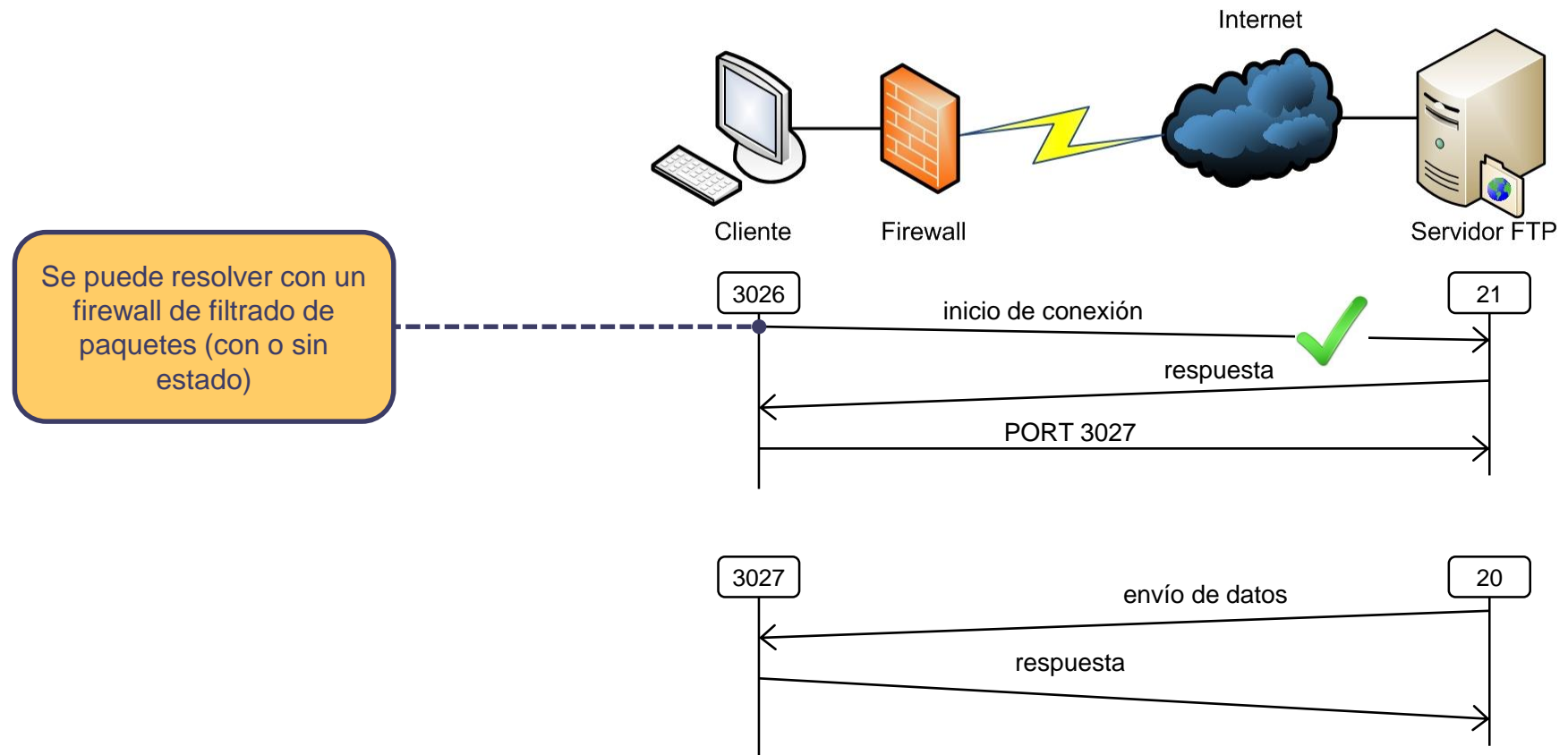


Tipos de firewalls

Filtrado de paquetes

- Limitaciones de los firewalls de filtrado de paquetes

1. Problemas para gestionar protocolos como el "FTP Activo":

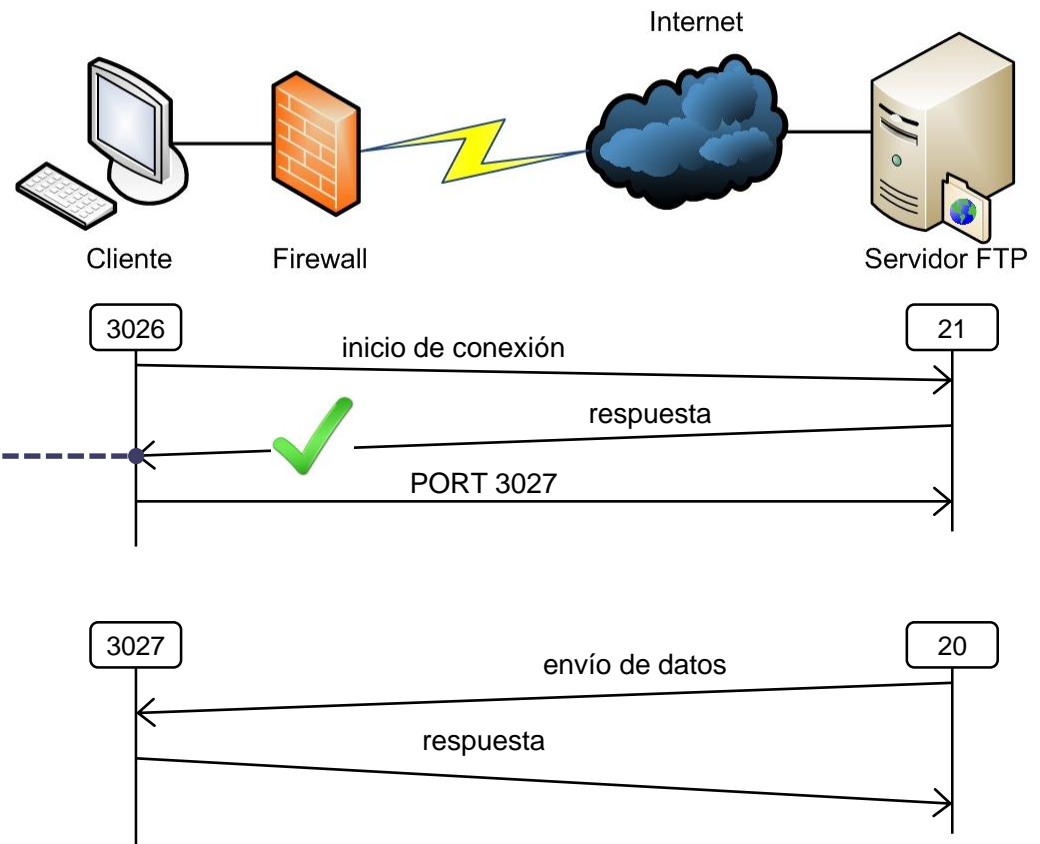


Tipos de firewalls

Filtrado de paquetes

- Limitaciones de los firewalls de filtrado de paquetes

1. Problemas para gestionar protocolos como el "FTP Activo":



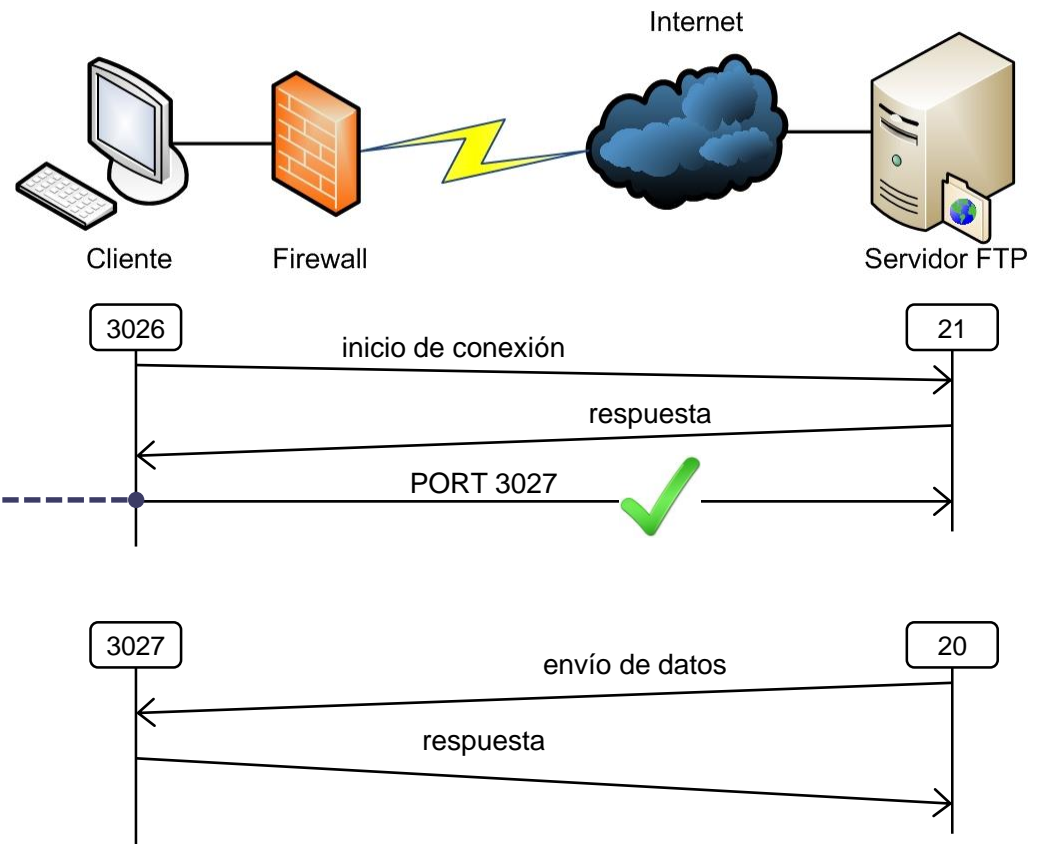
Se puede resolver con un firewall de filtrado de paquetes (preferiblemente con estado)

Tipos de firewalls

Filtrado de paquetes

- Limitaciones de los firewalls de filtrado de paquetes

1. Problemas para gestionar protocolos como el "FTP Activo":



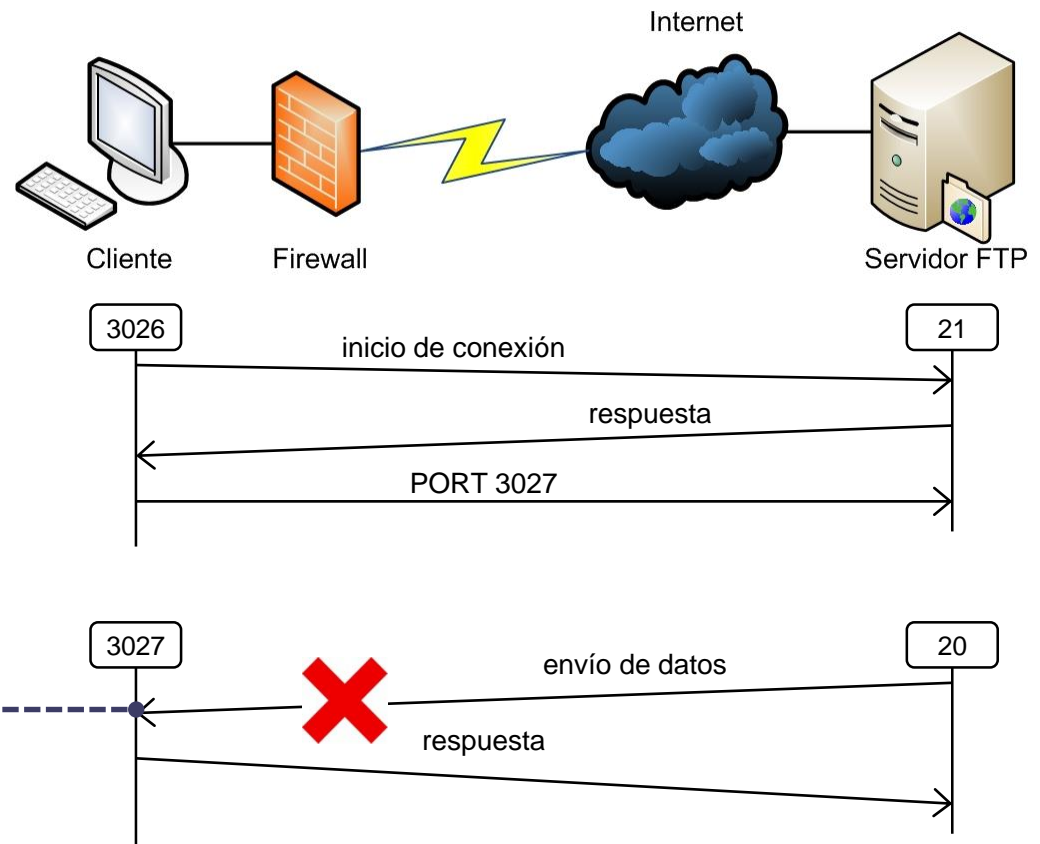
Comando a nivel de aplicación. El firewall de filtrado de paquetes lo permite (por regla anterior) pero no lo interpreta

Tipos de firewalls

Filtrado de paquetes

- Limitaciones de los firewalls de filtrado de paquetes

1. 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
 1. Problemas para gestionar protocolos como el “FTP Activo”:
 - 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
 2. No admiten esquemas de autenticación avanzada de usuarios
 - el control se limita a IP
 3. 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: explotación de vulnerabilidades
 - Aplicación Web vulnerable a SQL Injection
 - `http://www.mydomain.com/products/products.asp?productid=123; DROP TABLE Products`

Tipos de firewalls

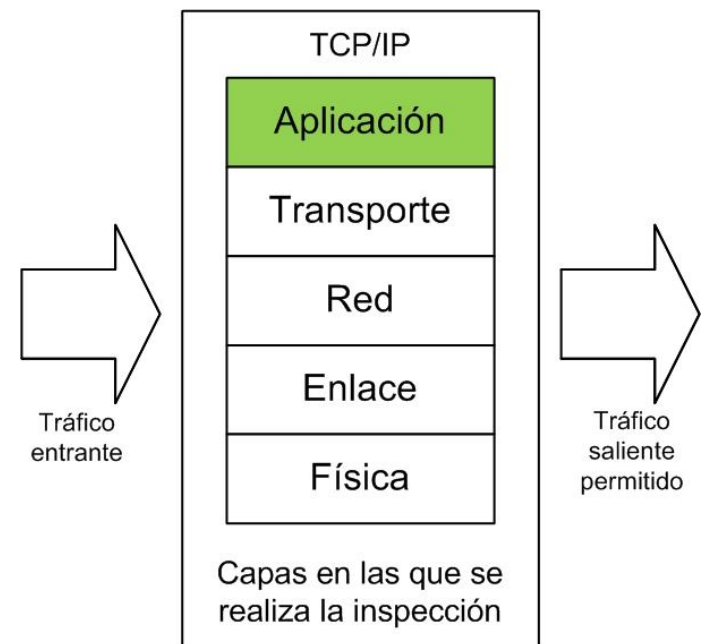
- **Filtrado de paquetes** (*packet filtering*)
 - Filtrado estático o sin estado (*stateless*)
 - Filtrado dinámico o con estado (*stateful*)
- **Filtrado a nivel de aplicación**



Tipos de firewalls

Filtrado a nivel de aplicación

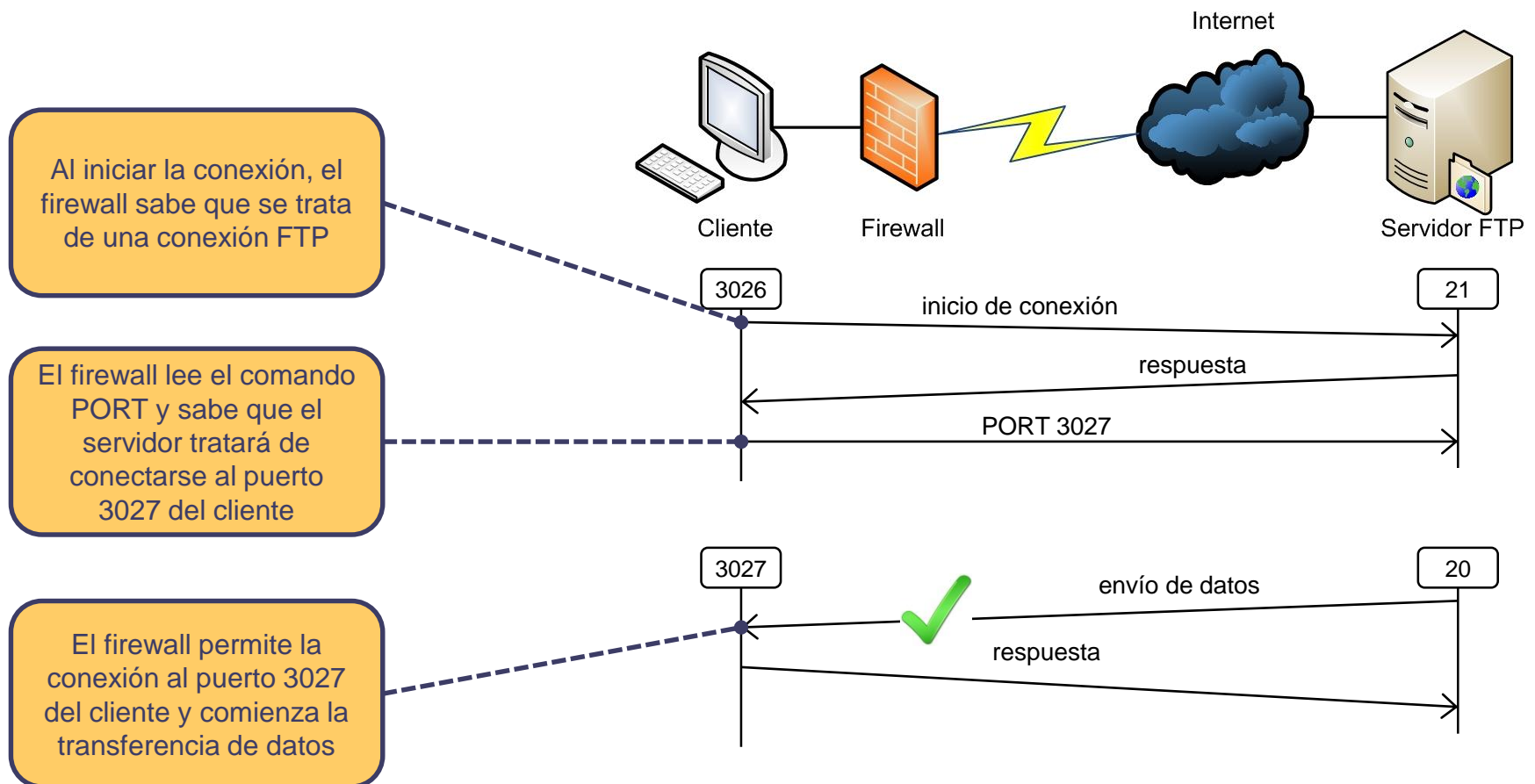
- Capaces de interpretar paquetes a nivel de aplicación
 - Mayor capacidad de análisis y de control de tráfico
 - Más complejos, pues deben conocer el funcionamiento de aplicaciones específicas (ej.: FTP, HTTP, SMTP, TELNET, etc.)
 - Suelen combinarse con filtrado de paquetes



Tipos de firewalls

Filtrado a nivel de aplicación

■ Ejemplo: FTP Activo



Tipos de firewalls

Filtrado a nivel de aplicación

■ Ventajas

- Mejor control de conexiones para ciertos protocolos
 - Permiten gestionar conexiones relacionadas (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*
 - Al analizar el tráfico en más detalle, también se puede registrar en más detalle (ej: directorio FTP, URL, etc.)

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

ARQUITECTURAS DE FIREWALLS

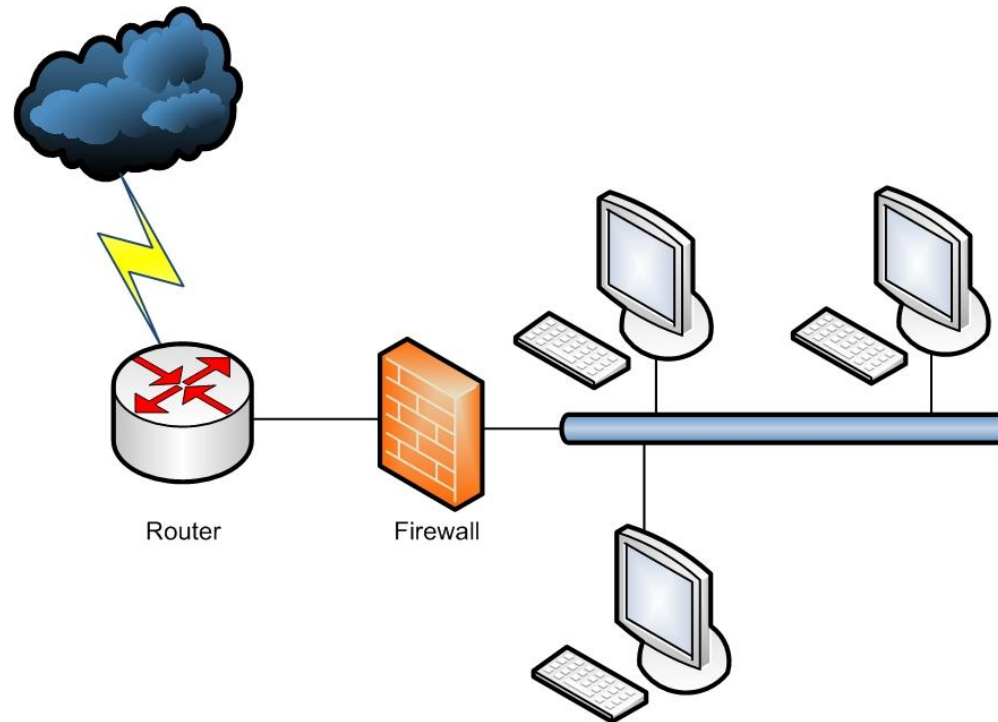
Arquitecturas de firewalls

- Además de las configuraciones simples vistas hasta el momento, son posibles configuraciones más complejas
- Aspectos importantes:
 - N° de firewalls a utilizar
 - Tipo de firewalls
 - Ubicación en la red
- Examinaremos las arquitecturas más habituales

Arquitecturas de firewalls

Escenario básico

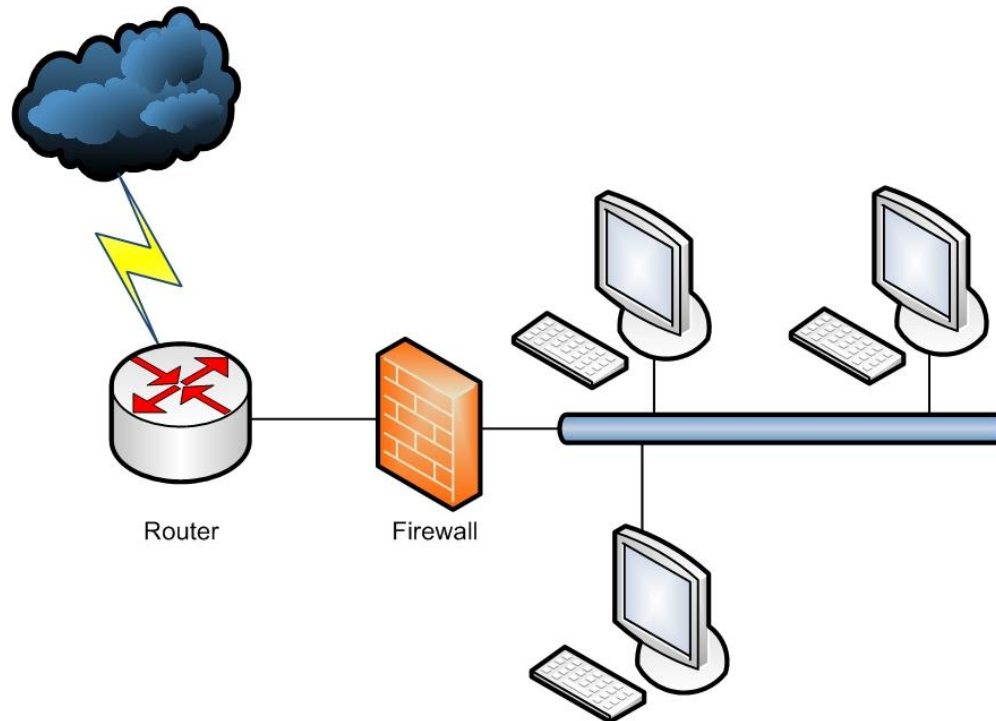
- Escenario básico de uso de un firewall



Arquitecturas de firewalls

Escenario básico

- Escenario básico de uso de un firewall

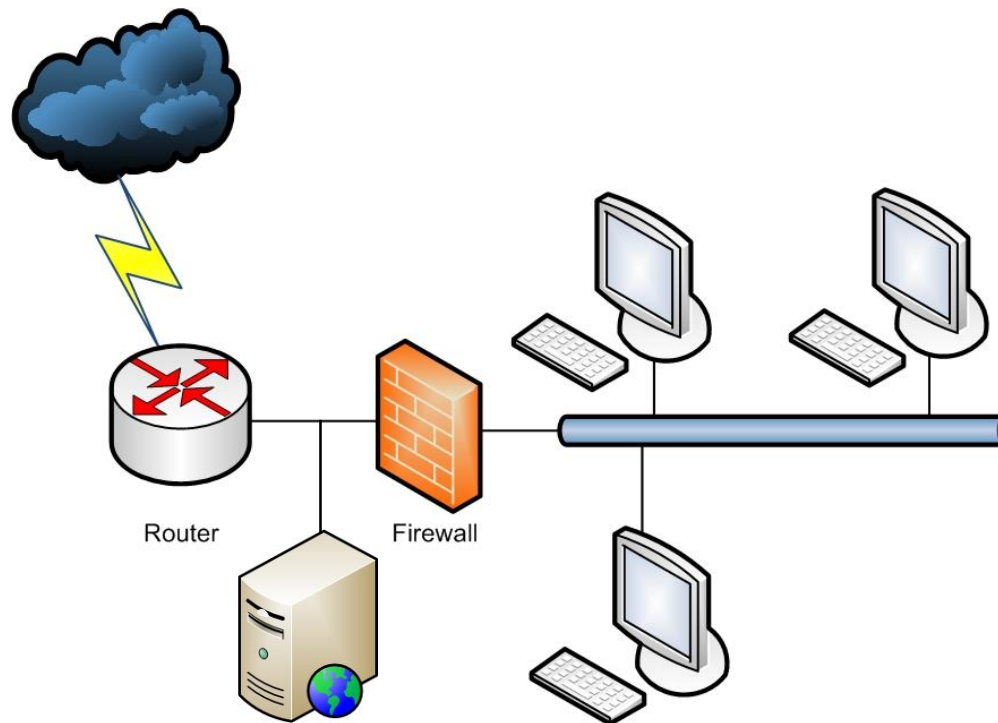


¿Dónde situar un Servidor Web?

Arquitecturas de firewalls

Escenario básico

- Escenario básico de uso de un firewall

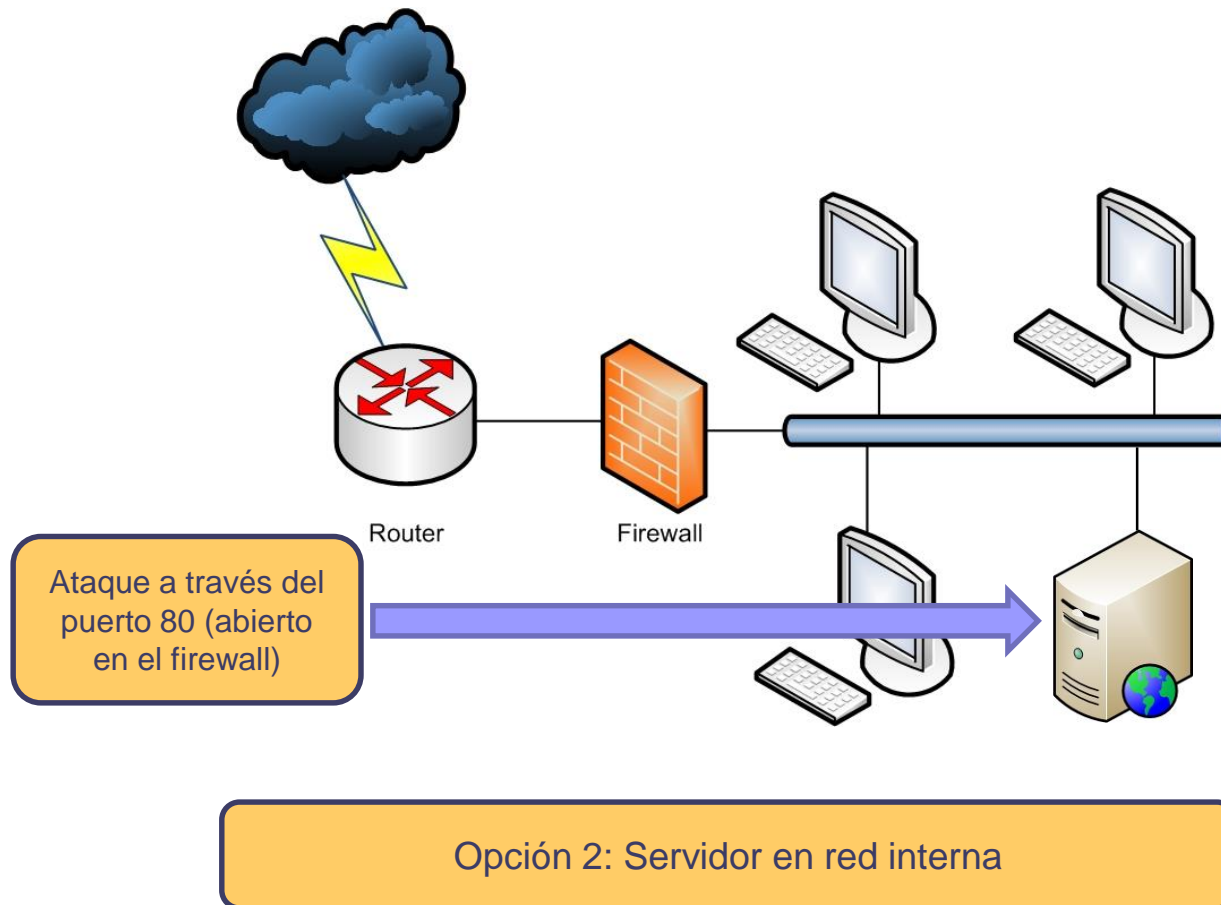


Opción 1: Servidor completamente expuesto a ataques

Arquitecturas de firewalls

Escenario básico

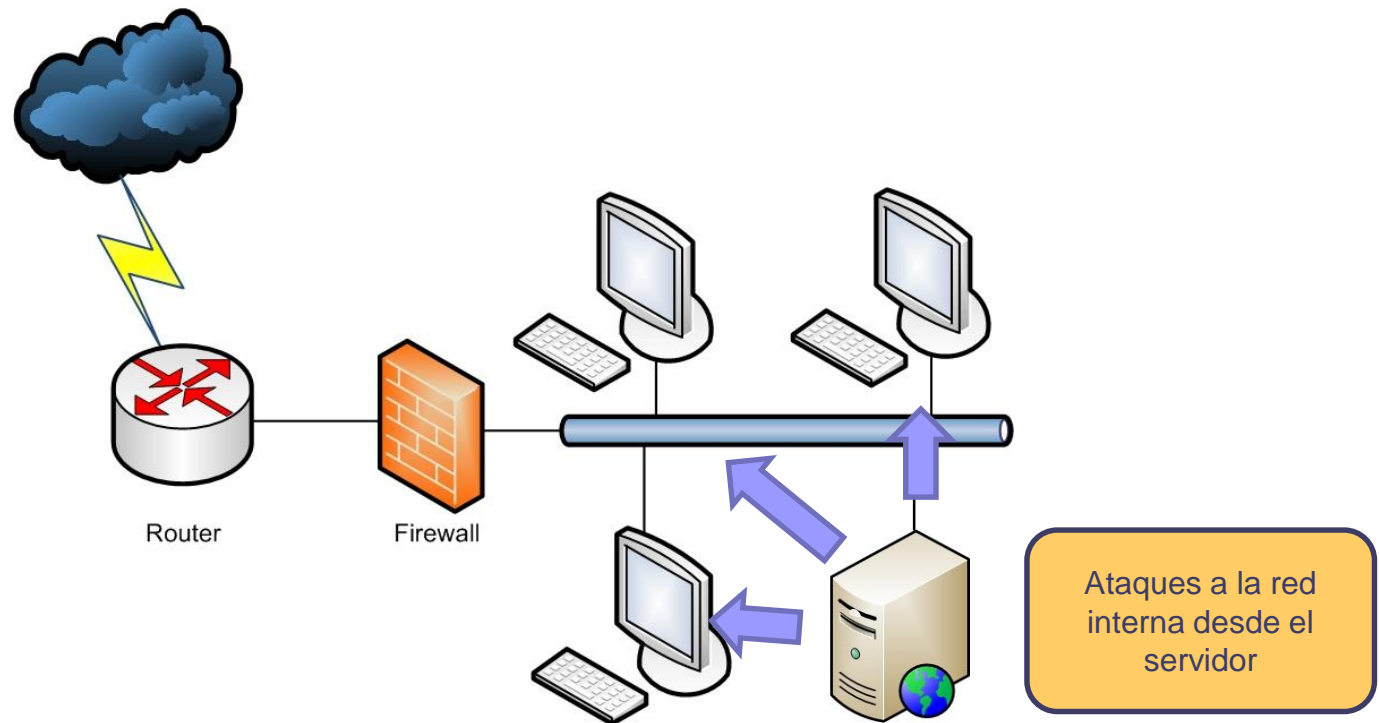
- Escenario básico de uso de un firewall



Arquitecturas de firewalls

Escenario básico

- Escenario básico de uso de un firewall

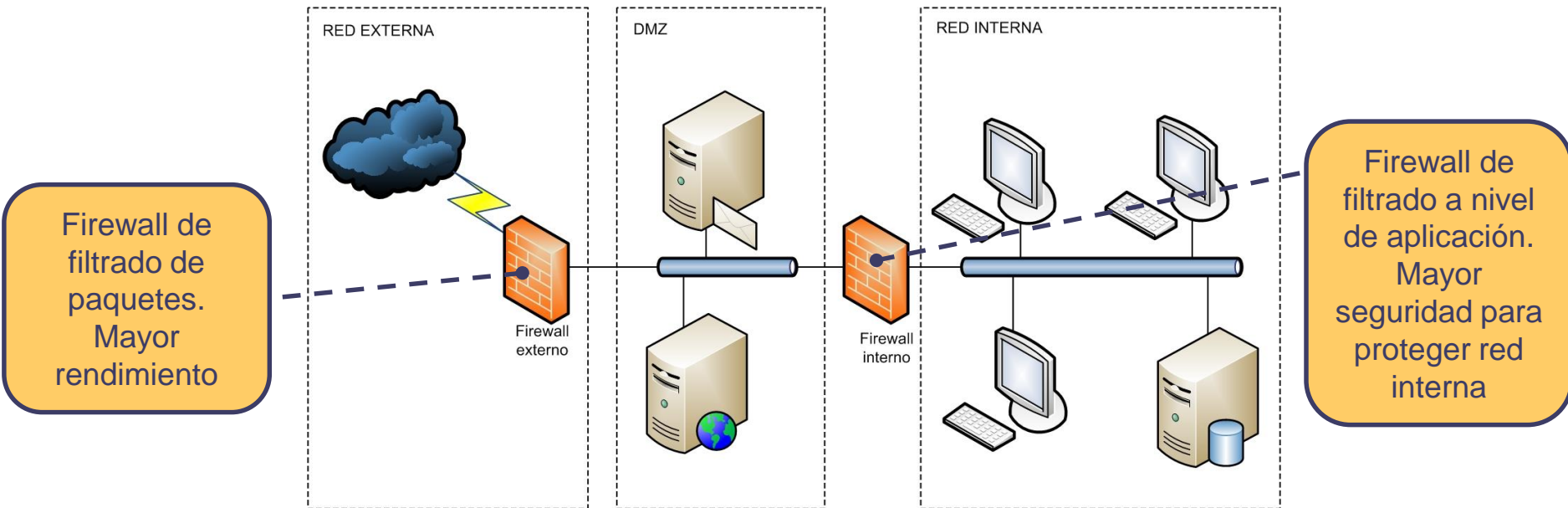


Opción 2: Servidor en red interna

Arquitecturas de firewalls

DMZ

- Solución: DMZ (DeMilitarized Zone, zona desmilitarizada)
 - Suele utilizarse para ubicar servidores de acceso público, sin comprometer la seguridad de la red interna

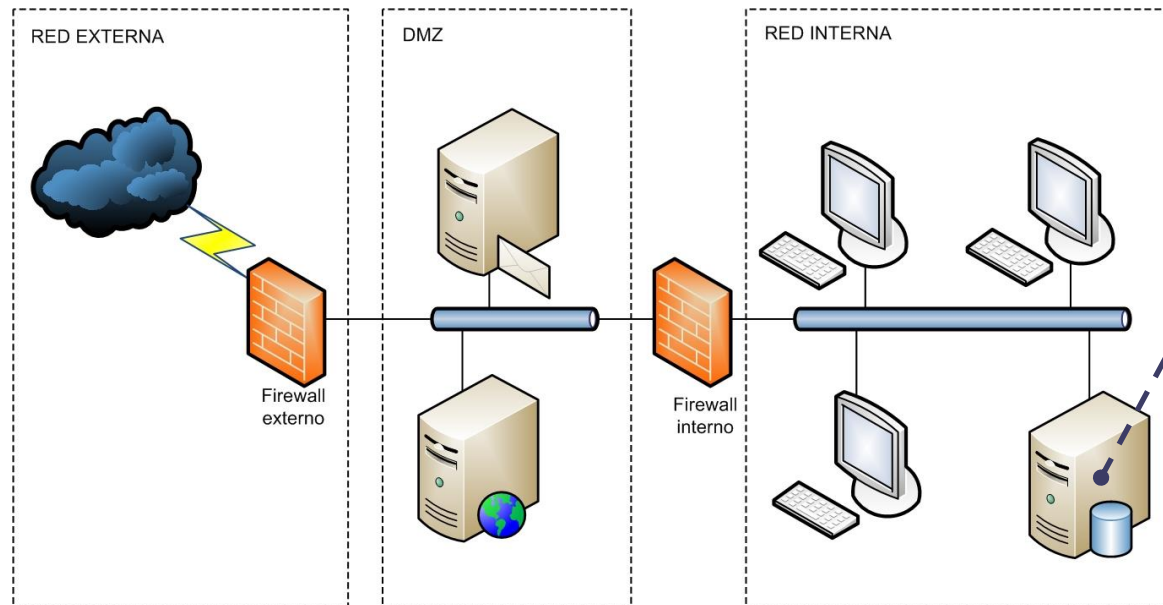


- Si un atacante supera el firewall externo adquiere acceso a la DMZ, pero no a la red interna

Arquitecturas de firewalls

DMZ

- Solución: DMZ (DeMilitarized Zone, zona desmilitarizada)
 - Suele utilizarse para ubicar servidores de acceso público, sin comprometer la seguridad de la red interna



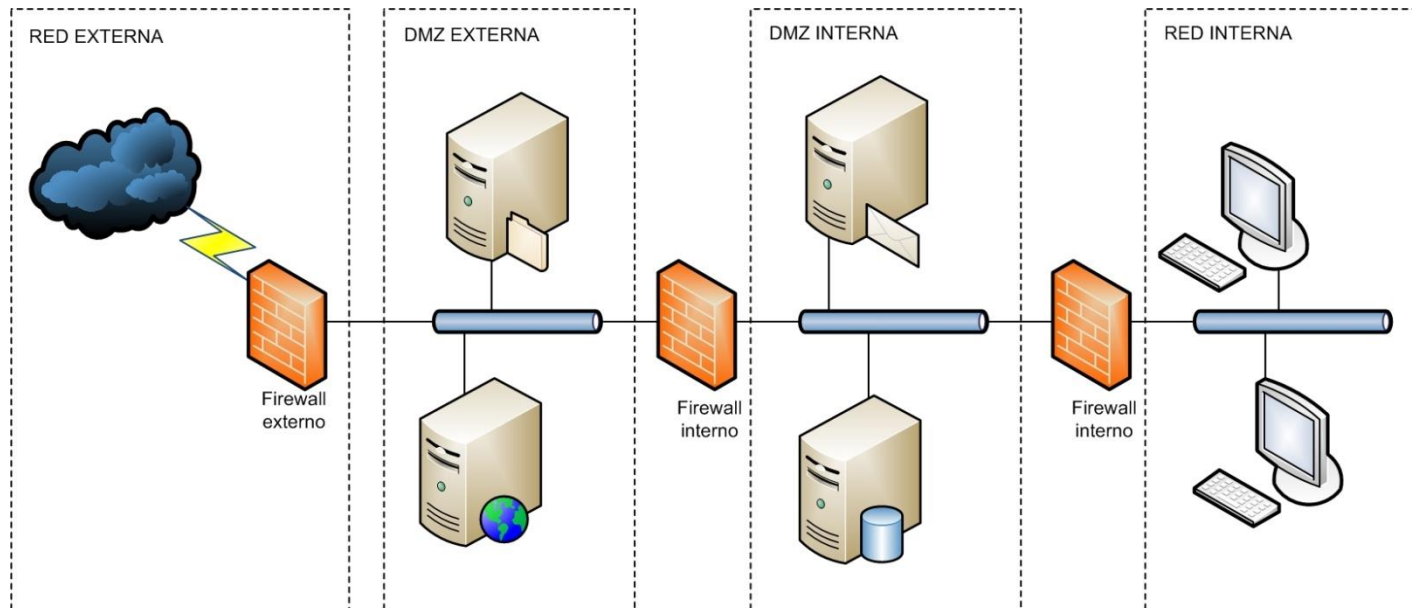
Datos especialmente críticos.
¿Cómo protegerlos de ataques desde las estaciones de trabajo?

- 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



IPTABLES

iptables

- Firewall de filtrado de paquetes integrado en el kernel de Linux
 - Stateful
 - Con algunas funciones de firewall de aplicación
- Usa **chains** o **cadenas** para controlar distintos flujos de tráfico: entrada, salida, entrada desde la red local, etc.
- Permite establecer **reglas** en base a parámetros de un paquete (como la dirección IP origen/destino, el puerto origen/destino, el protocolo, etc.) y lo que hay que hacer con ese paquete (aceptarlo, rechazarlo, generar una respuesta, modificarlo, etc.)
- Las cadenas se agrupan en **tablas**

iptables

- Es posible añadir módulos que incrementan la funcionalidad (log, estadísticas, etc.)
- Soporta distintos protocolos (TCP, UDP, ICMP, etc)
- Soporta interfaces de origen/destino de paquetes (eth0, eth1, etc.)
- Muy estable, rápido y seguro

iptables

■ Tablas

- Las tablas contienen cadenas, que son listas de reglas
- Se referencian con la opción `-t tabla`
- Existen 5 tablas:
 - filter: filtrado de paquetes (tabla por defecto)
 - nat: traducción de direcciones de red
 - mangle: modificación paquetes (TOS, TTL, mark)
 - raw: configura excepciones en el seguimiento de los paquetes de las conexiones
 - security: Permite a módulos de seguridad de Linux (SELinux) implementar reglas de filtrado



iptables

■ Cadenas (*chains*)

- Agrupan un tipo de tráfico
- Existen dos tipos:
 - Definidas por iptables. Por ejemplo, la tabla filter tiene definidas las cadenas:
 - INPUT: tráfico con destino la propia máquina
 - OUTPUT: tráfico generado en la propia máquina
 - FORWARD: tráfico que llega a la máquina, pero no es su destino final
 - Definidas por el usuario. Por ejemplo:
 - Tráfico de entrada desde máquinas de la red local
 - Tráfico http procedente de cualquier máquina
 - ...

iptables

- Funcionamiento (para la tabla filter)
 - 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
 - Si el paquete tiene como destino otra máquina:
 - Si el kernel soporta *forwarding*: el paquete se envía a la cadena **FORWARD**. Si consigue pasar por esta cadena, el paquete será reenviado
 - Sino (o no sabe como redireccionarlo): el paquete se descarta

iptables

- Funcionamiento (para la tabla filter)
 - Un programa ejecutándose en la misma máquina en la que se está ejecutando el firewall puede enviar paquetes
 - Esos paquetes se envían a la cadena **OUTPUT**
 - Si consiguen pasar por esta cadena, continúan su camino, en caso contrario, se descartan

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 parámetros como la dirección IP origen/destino, el puerto origen/destino, el protocolo, etc.
- 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)
- Se procesan en orden
 - Si no se especifica otra cosa, en el orden en el que fueron insertadas
- Se aplican sobre una cadena

iptables

■ Reglas

□ Ejemplo:

```
iptables -t filter -A INPUT -s 10.10.102.9 -j DROP
```

- añade (-A) una nueva de regla de filtrado de paquetes (tabla filter) que rechaza (DROP) cualquier paquete que entra en la máquina (cadena INPUT) procedente de un ip origen (-s) concreta (en este caso la 10.10.102.9)

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 <code>state</code> , 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.



iptables

■ Más ejemplos...

```
#Mostrar reglas
user@debian:~# iptables -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
```

iptables

■ Más ejemplos...

```
#Permitir conexiones entrantes al servidor ssh
user@debian:~# iptables -A INPUT -p tcp --dport ssh -j ACCEPT
user@debian:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination          tcp dpt:ssh
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

iptables

■ Más ejemplos...

```
# Funcionalidad de FW de aplicación:  
# Permitimos conexiones establecidas o relacionadas  
user@debian:~# iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

iptables

- Las reglas de iptables NO son persistentes
- Para guardarlas

```
#Guardar las reglas en un archivo  
iptables-save -c > /etc/iptables.rules
```

iptables

- Para cargarlas

```
#Restaurar las reglas a partir de un archivo  
iptables-restore < /etc/iptables.rules
```

- Se puede automatizar, añadiendo un script en
/etc/network/if-pre-up.d

```
#!/bin/sh  
iptables-restore < /etc/iptables.rules  
exit 0
```

iptables

- Es buena idea crear un script en el que vayamos insertando las reglas

```
# Limpiar reglas existentes
iptables -F

# Añadir nuevas reglas

# Aceptar trafico por la interfaz de loopback
iptables -A INPUT -i lo -j ACCEPT

# Acceso desde otra MV por ssh
iptables -A INPUT -p tcp -s 10.10.102.139 --dport 22 -j ACCEPT

# Acceso desde otra MV al servidor de rsyslog
iptables -A INPUT -p tcp -s 10.10.102.139 --dport 514 -j ACCEPT

# Acepta trafico de entrada de conexiones previamente establecidas y relacionadas
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

# Listar reglas en formato detallado (-v)
iptables -L -v

# Guardar las reglas
iptables-save -c > /etc/iptables.rules
```


iptables

■ Política por defecto

- Si un paquete pasa por todas las reglas y no encaja con ninguna, se le aplica la política por defecto para esa cadena (INPUT, OUTPUT o FORWARD)
- La política por defecto se puede cambiar con la opción -P (si no se indica lo contrario, es ACCEPT)

```
iptables -P INPUT DROP  
iptables -P FORWARD DROP  
iptables -P OUTPUT ACCEPT
```

iptables

■ Política por defecto

```
# Establecer política por defecto
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

# Limpiar reglas existentes
<...>

# Añadir nuevas reglas
<...>

# Listar reglas en formato detallado (-v)
<...>

# Guardar las reglas
<...>
```

iptables

- Política por defecto
 - Si se activan políticas por defecto restrictivas, hay que tener cuidado con borrar las reglas
 - El borrado de las reglas no modifica las políticas

iptables

■ Desactivar firewall

```
# Restaurar políticas por defecto
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT

# Limpiar reglas existentes
iptables -F
```

iptables

- ¿y el tráfico IPv6?
 - ip6tables

Port knocking

- Consiste en enviar una secuencia de paquetes a un sistema que abra un puerto que anteriormente estaba cerrado
- Puede ser interesante como complemento a una política de seguridad

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.