Seguridad en Sistemas Informáticos

Seguridad perimetral

Área de Ingeniería Telemática
Dpto. Automática y Computación
http://www.tlm.unavarra.es/

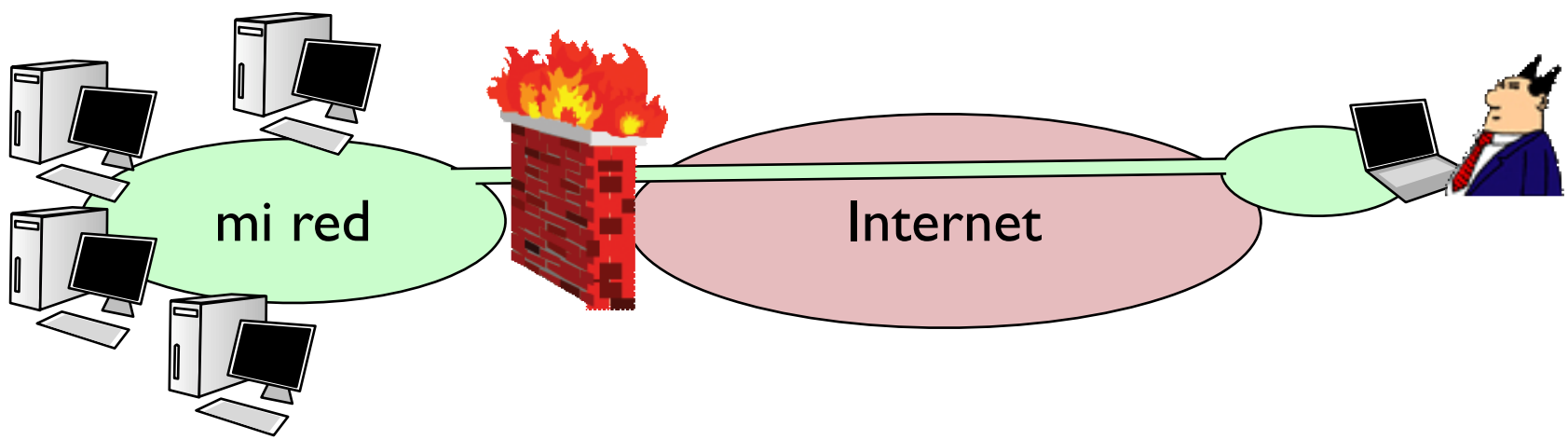
En días anteriores...

- Introducción a las amenazas y peligros de Internet

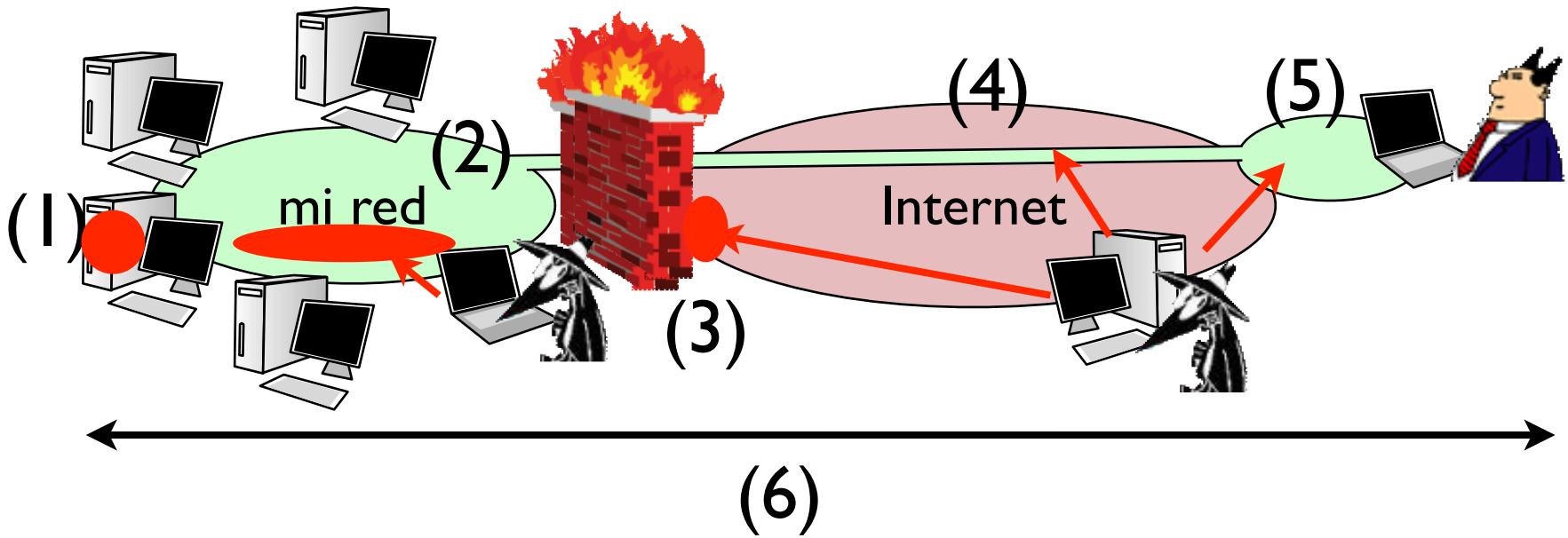
- Hoy
  - La cadena de seguridad
  - Seguridad perimetral

Introducción

- Por su propia naturaleza, la seguridad debe darse en todos los puntos del sistema. El enemigo atacará el punto más débil. La seguridad debe enfocarse como un valor global extendido a todos sus componentes (punto de vista holistico)
- En toda comunicación en la que se utilice una red IP, hay que emplear **medidas de seguridad específicas en todos los puntos de la red**.
- Se dice que la seguridad funciona como una cadena. Para romperla al atacante le basta con romper un eslabón cualquiera. El defensor debe protegerlos todos.

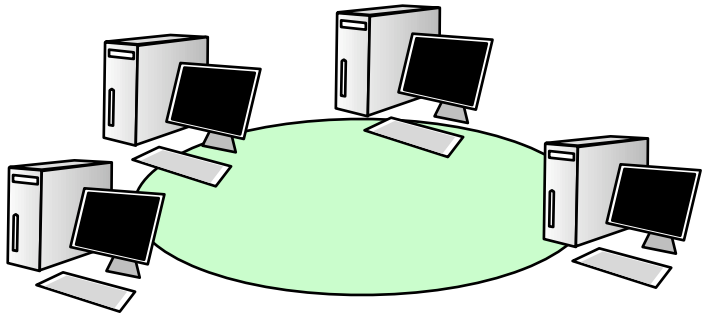


La cadena de seguridad



- Seguridad en el host (1)
- Seguridad en la red local (2)
- Seguridad perimetral (3)
- Seguridad en el canal de comunicaciones (4)
- Seguridad en el acceso (5)
- Seguridad transversal (6)

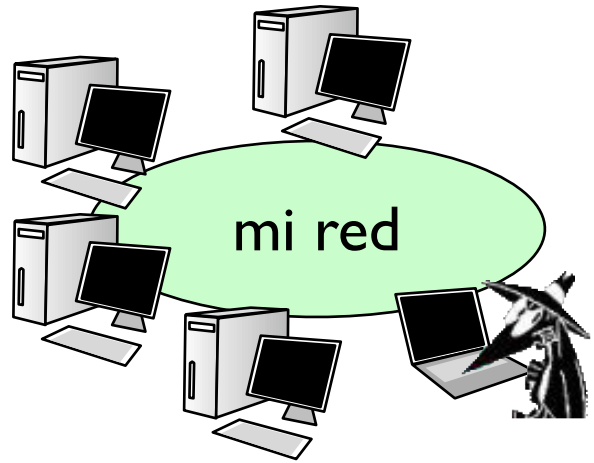
Seguridad en el host



En todos los hosts de mi red...

- Empleo de un sistema de antivirus actualizado.
- Configuración del sistema operativo.
- Utilización de un cortafuegos personal.
- Actualizaciones periódicas tanto de las aplicaciones como del sistema operativo (Gestión de Parches).
- Instalación de únicamente aquellas aplicaciones y servicios que vayan a usarse.
- Implantación de una política de permisos adecuada.
- Utilización de una política adecuada de contraseñas.
- Empleo de TCP Wrappers e IDSs (sistemas de detección de intrusos) de Hosts.
- Utilización de sistemas de comprobación de integridad de archivos.
- Procedimiento de Gestión de logs.
- Definición de una línea base de ET y Servidores.

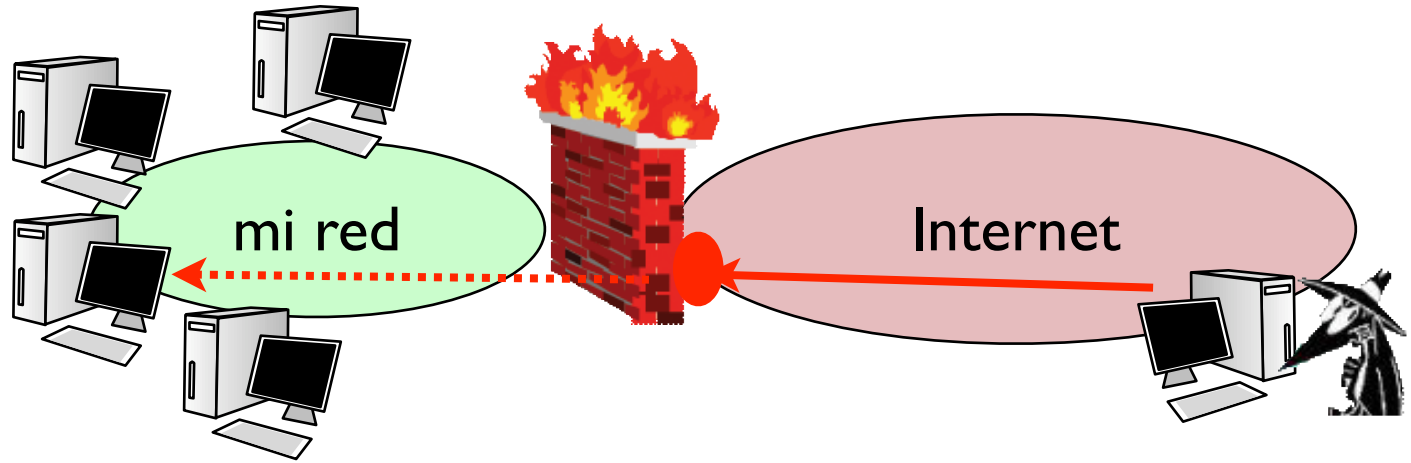
Seguridad en la red local



En los equipos de la red local

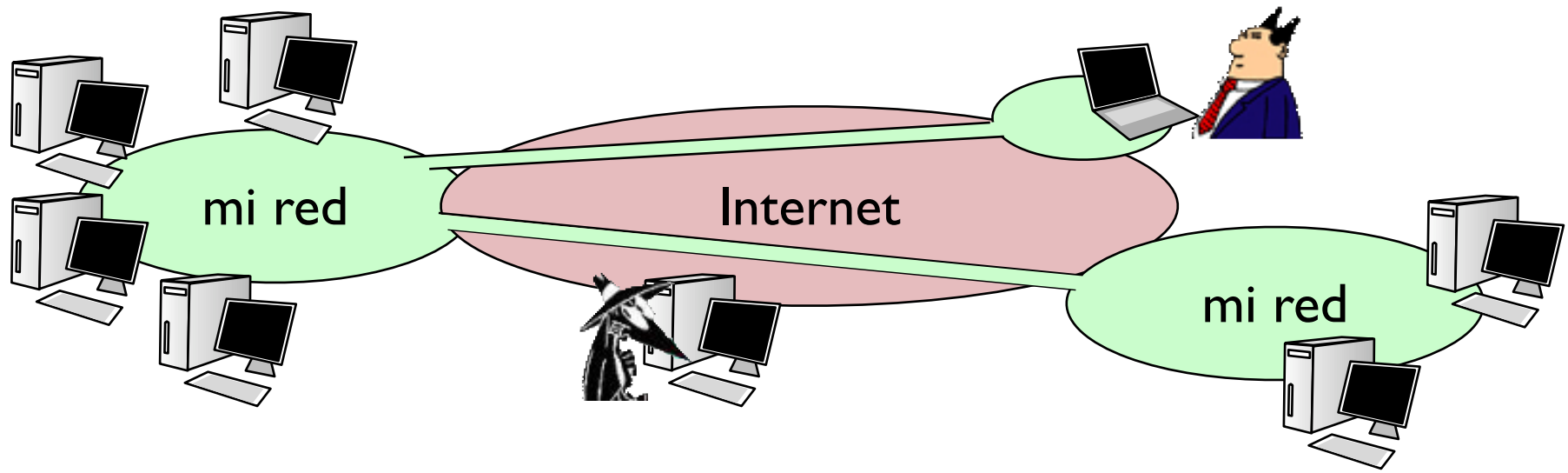
- Configuración del HW de red en modo no promiscuo.
- Utilización de VLANs.
- Empleo de herramientas anti sniffers.
- Utilización de IDSs de red.
- Diseño de un correcto plan de direccionamiento.
- Seguridad de los dispositivos de red. Blindaje de routers, conmutadores, etc.

Seguridad perimetral



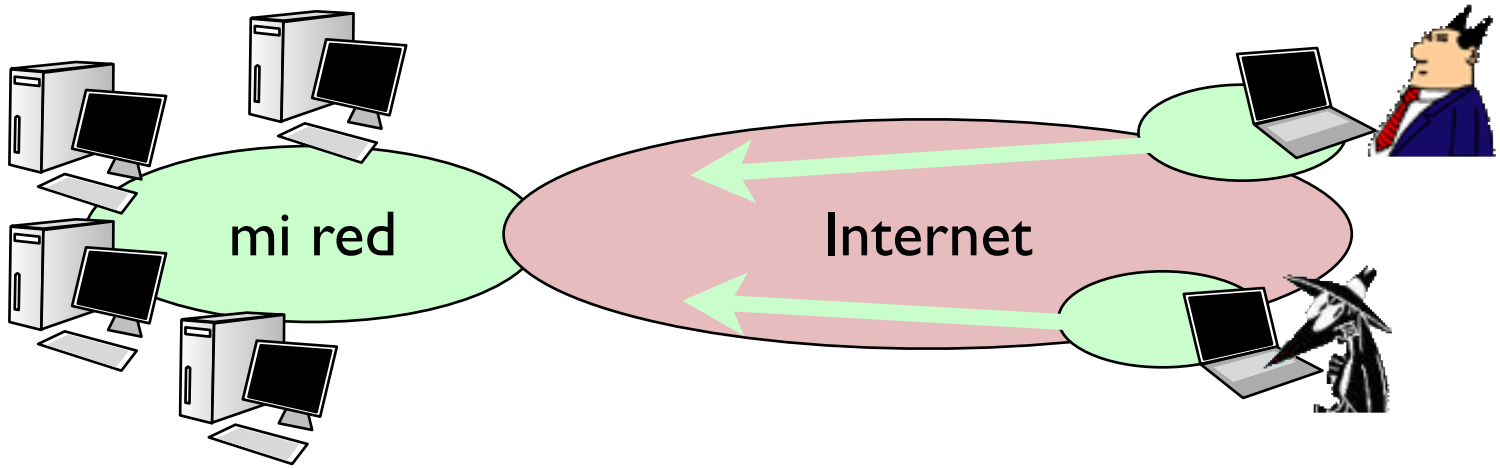
- **Separar la red de la empresa de la red exterior y controlar que es lo que puede y no puede pasar**
- **Herramienta:**
  - Firewalls o cortafuegos: son elementos que permiten establecer políticas de control de acceso entre redes distintas (por ejemplo entre Internet y la red corporativa o entre la red de facturación y la red de empleados). Si bien constituyen el elemento fundamental en toda política de seguridad, por sí sólo no garantiza la seguridad de a red y hay que verlo como un elemento más de la cadena de seguridad.

Seguridad en el canal de comunicaciones



- Con la generalización de las redes IP el modo de comunicación entre las empresas está variando drásticamente
  - Antiguamente las comunicaciones corporativas se realizaban mediante circuitos alquilados entre las mismas.
  - Hoy en día la tecnología de **Redes Privadas Virtuales (VPNs)** pone a disposición del cliente una red con la funcionalidad de una línea privada, pero construida y operada sobre las infraestructuras de una red compartida (por ejemplo Internet) con lo que los beneficios de coste y escalabilidad son enormes.
- Por este motivo las redes privadas basadas en tecnologías como ATM o Frame Relay están siendo reemplazadas por VPNs.
  Que garantías tengo que que el trafico de una Red Privada Virtual es de verdad privado??

Seguridad en el acceso



- Las VPNs pueden establecerse entre diferentes empresas o bajo demanda por un usuario para acceder a la red de la empresa
  - Los métodos de autorización y autentificación son imprescindibles. Como garantizamos que el acceso no puede ser robado?
- El mismo problema ocurre en redes de acceso inalámbricas

Seguridad transversal

- Aspectos de la seguridad corporativa que hay que tener en cuenta en todos los eslabones de la cadena (a diferente nivel):
- **Seguridad física.**
  - Control de accesos.
  - Protección anti incendios
  - Protección del suministro eléctrico.
- **Copias de seguridad, sistemas de almacenamiento.**
- **Cuestiones organizativas.**
  - Política de seguridad.
  - Plan de contingencia

Seguridad perimetral

- Algunos principios básicos de seguridad
  - **Eslabon mas debil (weakest link)**
  - **Mínimos privilegios (least privilege)**

    Un objeto (usuario, programa, systema...) debe tener los minimos privilegios necesarios para cumplir su función asignada pero ninguno más
  - **Cuello de botella (choke point)**

    Forzar a los atacantes a seguir un canal estrecho que pueda ser controlado y vigilado
  - **Seguridad en profundidad (security in depth)**

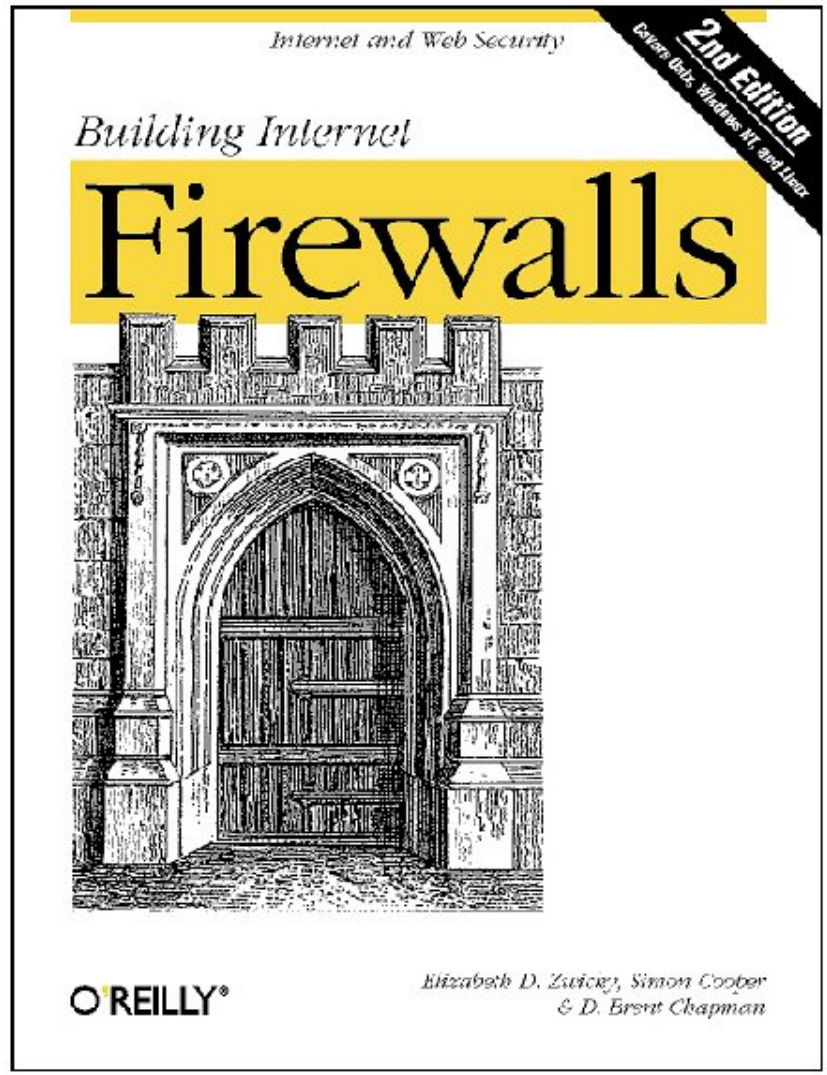
    Varios niveles de medidas de seguridad (no tengo que suponer que son infranqueables).

Seguridad perimetral

- Indice
  - Firewalls y Gateways
  - Aqruitecturas de red
  - NAT?

- Fuente: el libro

  D.B. Chapman & R.D. Zwicky, “Building Internet firewalls”, O’Reilly



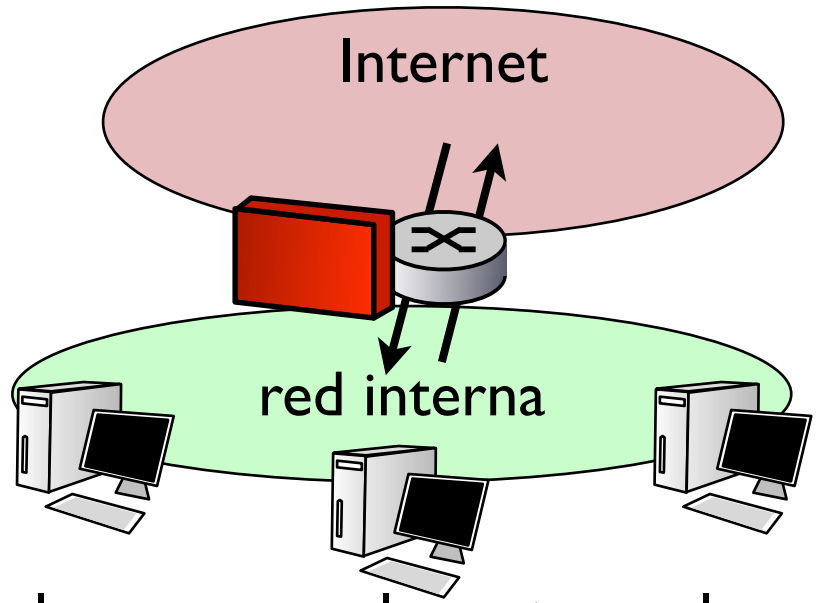
Definiciones

- **Firewall (o cortafuegos)**
  - Elemento capaz de clasificar y filtrar el tráfico de entrada/salida de una subred

- **Gateway**
  - Elemento que permite a los usuarios autorizados atravesar la frontera de una red filtrada

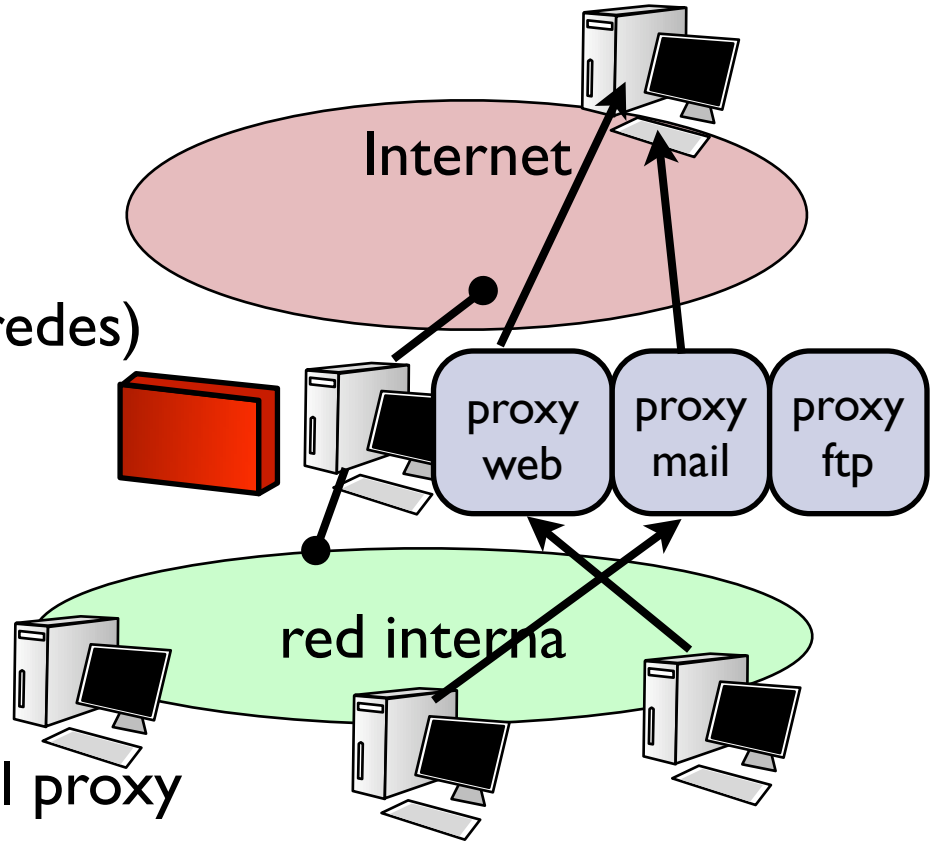
Arquitectura simple

- **Firewall de paquetes (packet filter)**
- El firewall es un router u otro elemento que realiza reenvío IP
  - Antes de reenviar aplica reglas sobre los paquetes y puede reenviarlos o no según las cumplan



- Política default deny: reenvía unicamente los que cumplan estas reglas
- Política default accept: reenvía todos menos los que cumplan estas reglas
- Tipos de reglas
  - Los que vengan de esta IP origen / los que vayan a esta IP destino
  - Los que usen este servicio/aplicacion (puerto) origen o destino, TCP o UDP o ICMP...
  - cualquier combinación de condiciones sobre campos de paquetes

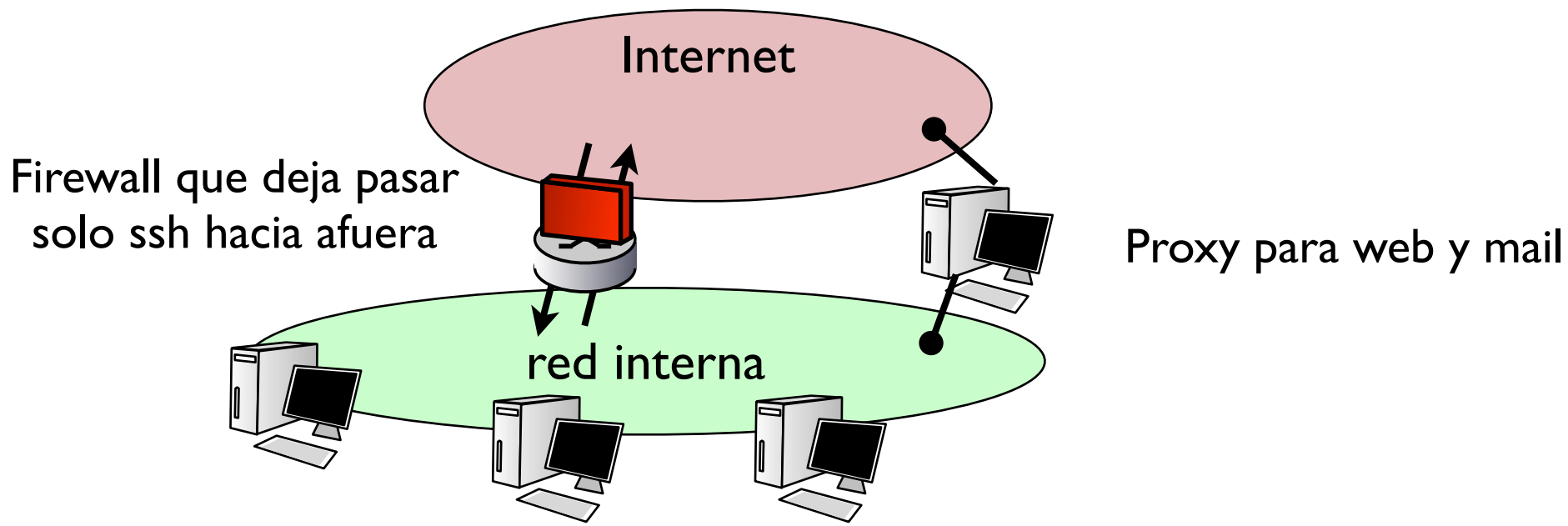
Proxies



- **Firewall de aplicación (proxy) también Gateway**
- El gateway es un PC dualhomed (IP en 2 redes)
- El firewall actua a nivel de aplicación
  - La aplicación pide el servicio al proxy
  - El proxy pide el servicio al servidor
- El usuario necesita
  - un cliente especial que pida las cosas al proxy
  - un procedimiento especial para usar los servicios
  - nada (proxy transparente que intercepta las peticiones)
- El proxy es software (especifico para la aplicación)
- Se entiende que no debe haber otra posible comunicación entre la red interna e Internet (si la función del proxy es la seguridad)

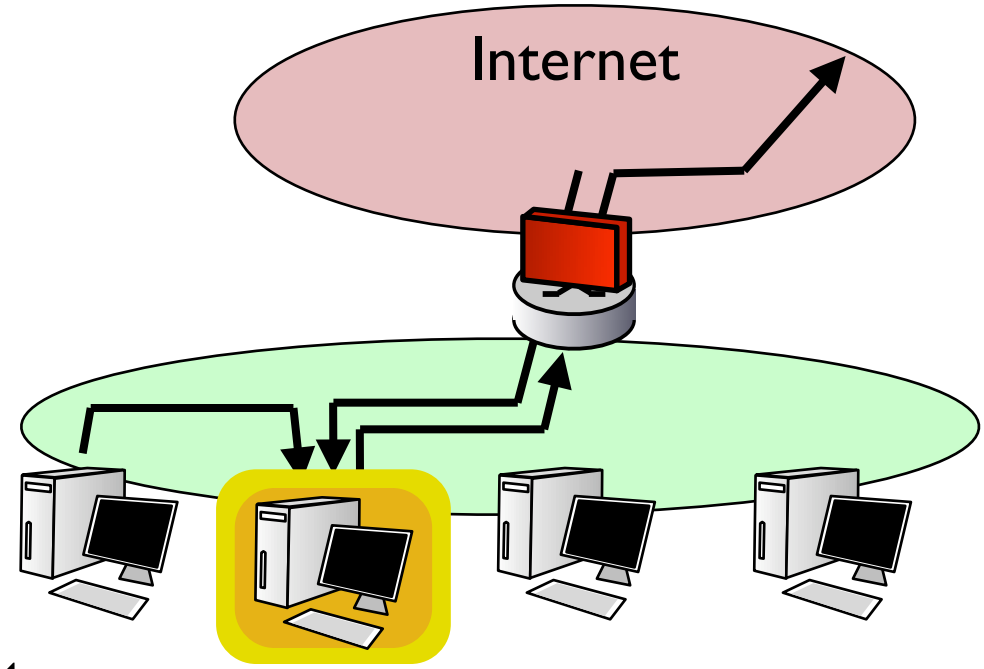
Que es mejor?

- **Filtrado de paquetes:**
  - Simple, eficaz, disponible en hardware
- **Proxy/gateway**
  - Muy seguro, permite niveles de seguridad por usuario
- **Son solo herramientas, podemos usar ambos combinados**



- **Que arquitecturas se recomiendan?**

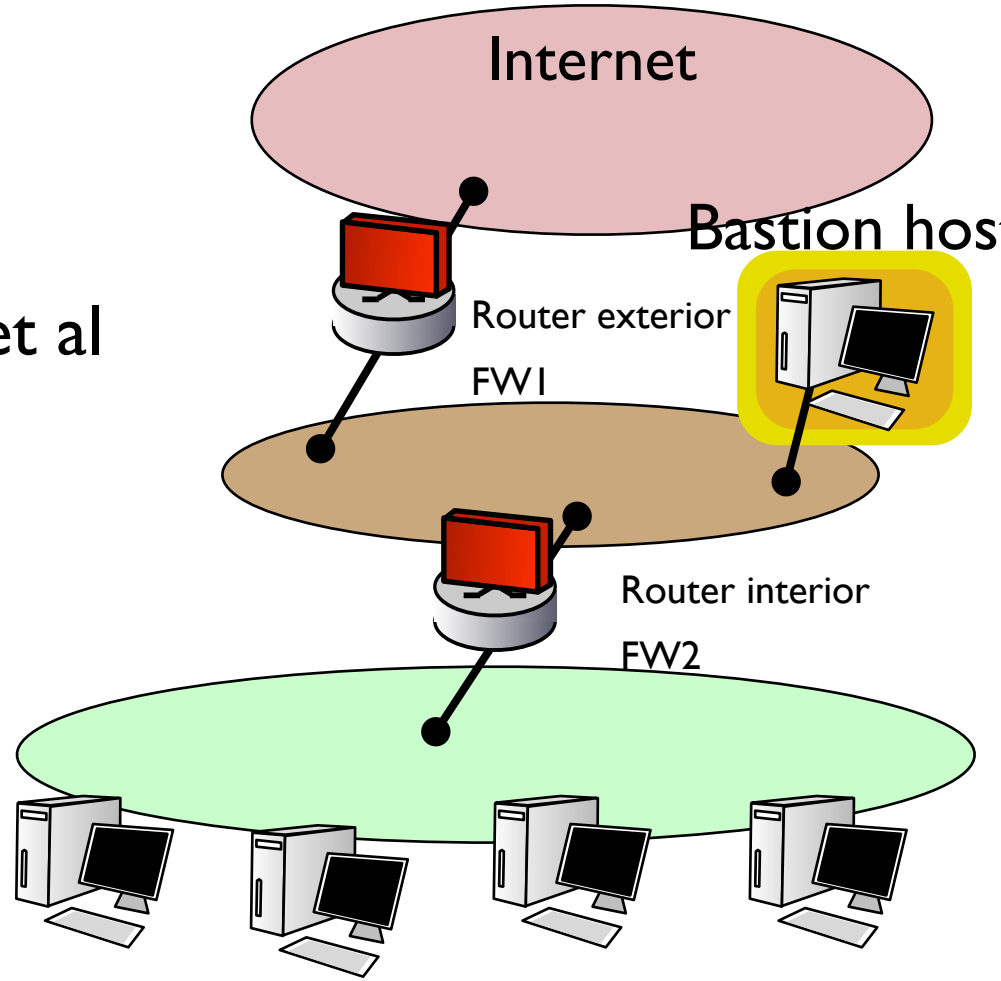
Screened host



- El firewall deja comunicarse a un host con el exterior y filtra al resto
- Elimina todos los paquetes que van dirigidos a otros hosts internos
- El host puede actuar de proxy para los demás
- Ese host se denomina **bastion host**
  - Debe estar preparado para los ataques porque es un host exterior
  - Configurado con cuidado con los servicios minimos necesarios y mantenido actualizado por vulnerabilidades
  - Vigilado por sistemas de monitorización de intrusos
- Limitamos la posibilidad de ataques a hosts preparados para soportarlos lo mejor posible
- Se puede permitir en el firewall sólo acceso a ciertos servicios del bastion host

Screened network

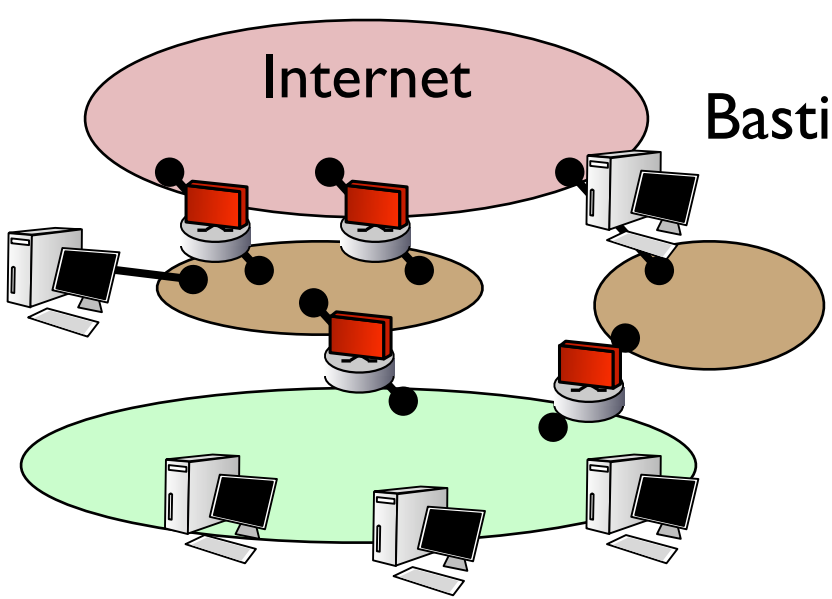
- Un nivel extra de seguridad
- FW1 solo permite trafico de Inet al bastion host
- FW2 solo permite trafico del bastion host a la red interior
- Red perimetral tambien conocida como zona desmilitarizada (DMZ)
- Los hosts internos pueden usar al bastion host de proxy o permitírseles atravesar los dos firewalls

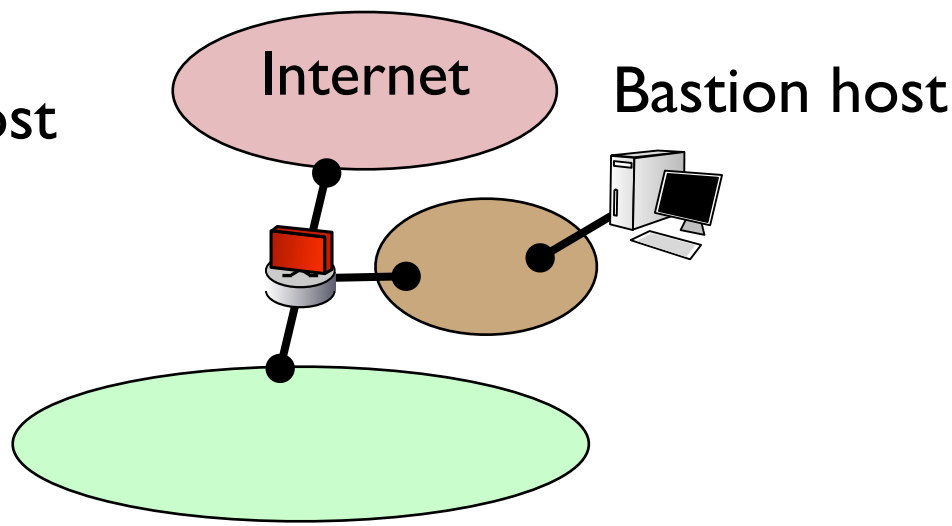


Variaciones

- Múltiples bastion hosts: aceptable

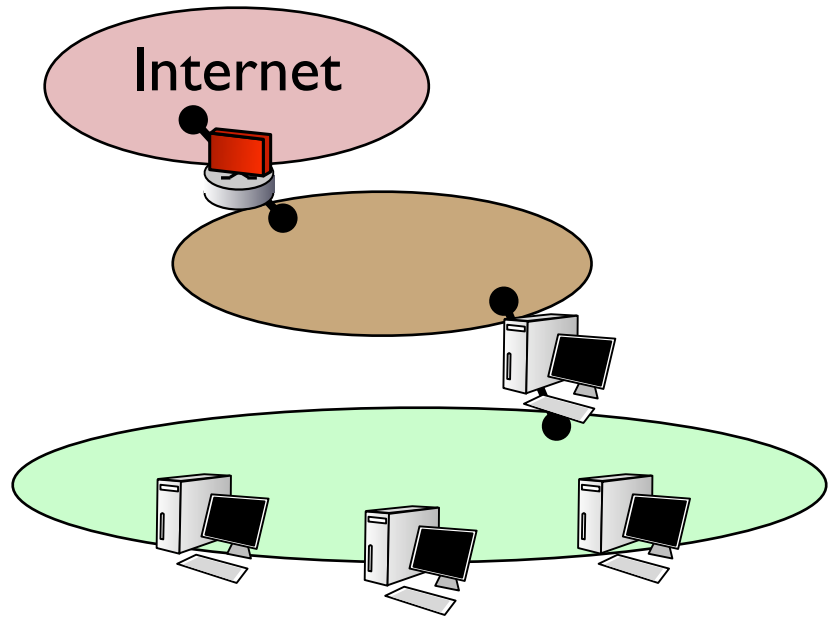
  Múltiples router exteriores: aceptable
- Usar un solo router como interior+exterior aceptable
- Mezclar las funciones del router exterior y el bastion host: aceptable



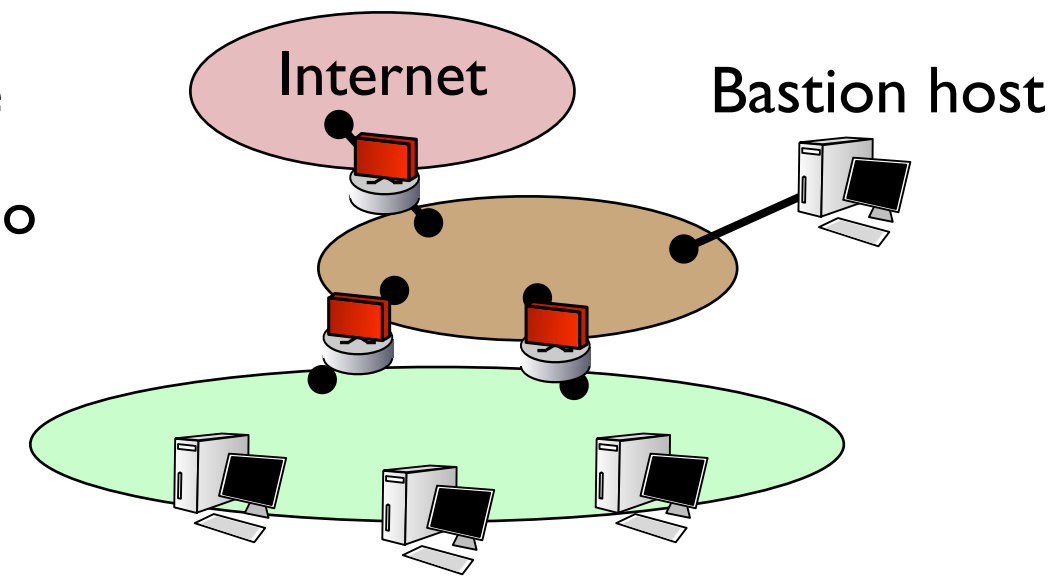


Variaciones peligrosas

- **Mezclar funciones de router interno y bastion host**
  - Si el bastion host es comprometido puede ver el tráfico interno (no hay un nivel mas de seguridad)



- **Varios routers internos**
  - No hay un único punto de entrada, el enrutamiento puede decidir enviar trafico por la red perimetral



Construyendo bastion hosts

Principios

- **Simple es mejor**
  - Mínimo número de servicios con mínimos privilegios necesarios para su cometido
- **Debe estar preparado para ser comprometido**
  - Será la maquina más expuesta y de la que se intentarán los ataques al resto de la red

- Consejos del capitulo 5 del libro de firewalls
  - Mantener actualizado
  - Hacer backup/ ser capaz de reconstruirlo de 0 facilmente (backup limpio)
  - Backup de logs, incluso de forma dificilmente modificable (enviar logs por cable serie a otra maquina desconectada)
  - Desactivar IP routing
  - Usar tcpwrapers para limitar los servicios a ciertas maquinas
  - Hacer auditorias
  - Vigilar con sistemas de detección de intrusos y de integridad
  - Observar su tráfico y funcionamiento, de forma automatica
  - Observar reinicios (que no pueda reiniciarse el solo por ejemplo)

Filtrado de paquetes

- Reglas a aplicar sobre los **parámetros**:
  - Si el paquete entra o sale de la red interna (inbound/outbound)
  - El protocolo
  - Las direcciones IP origen o destino
  - Los puertos TCP o UDP origen o destino
  - Cualquier otro campo del paquete
  - Otras cosas que sepa el sistema operativo sobre el paquete

    (dirección MAC, interfaz por el que entro o va a salir, proceso que lo ha generado...)
- Acciones sobre los paquetes que cumplen las reglas
  - ACCEPT: reenvia el paquete normalmente
  - DENY (en iptables, DROP): elimina el paquete sin reenviarlo
  - LOG: guarda el evento en el log. Util para examinar los intentos de ataques o entradas que tenemos
  - ...

Ejemplo... qué reglas poner

- Si quiero dejar pasar solo el tráfico externo que venga de un host de confianza (80.1.3.21)

Regla	Dirección	IP orig	IP dest	Acción
1	inbound	80.1.3.21	interna	Permitir
2	outbound	interna	80.1.3.21	Permitir
3	any	any	any	Denegar

Hace falta la regla para los dos sentidos ???

Sobre la cadena de reenvío

Acción por defecto denegar

```
$ iptables -P FORWARD DROP
$ iptables -A FORWARD -s 80.1.3.21/255.255.255.255
    -d 130.206.160.0/255.255.255.0 -p 6 -j ACCEPT
$ iptables -A FORWARD -d 80.1.3.21/255.255.255.255
    -s 130.206.160.0/255.255.255.0 -p 6 -j ACCEPT
```

Acción ACEPTAR

Origen y destino como subnet/mask

Protocolo=6 TCP

Otro ejemplo

- Si quiero dejar pasar el tráfico de telnet

Regla	Dirección	IP orig	IP dest	port orig	port dest	proto	ACK?	Acción
1	inbound	externa	interna	any	23	TCP	any	Permitir
2	outbound	interna	externa	23	any	TCP	yes	Permitir
3	outbound	interna	externa	any	23	TCP	any	Permitir
4	inbound	externa	interna	23	any	TCP	yes	Permitir
Acción por defecto: Denegar								

- Reglas separadas para las conexiones entrantes y salientes
- Reglas separadas para los dos sentidos de una misma conexión
- Cuidado con la diferencia entre conexión entrante y saliente y paquetes entrantes y salientes !!!

Filtrado de paquetes

Herramientas

- Nivel de sistema operativo UNIX/Linux con netfilter/iptables (o BSD con ipfw)
- Cisco IOS (ACL access control lists)
- Firewalls Hardware (que pueden ser Linux con netfilter)

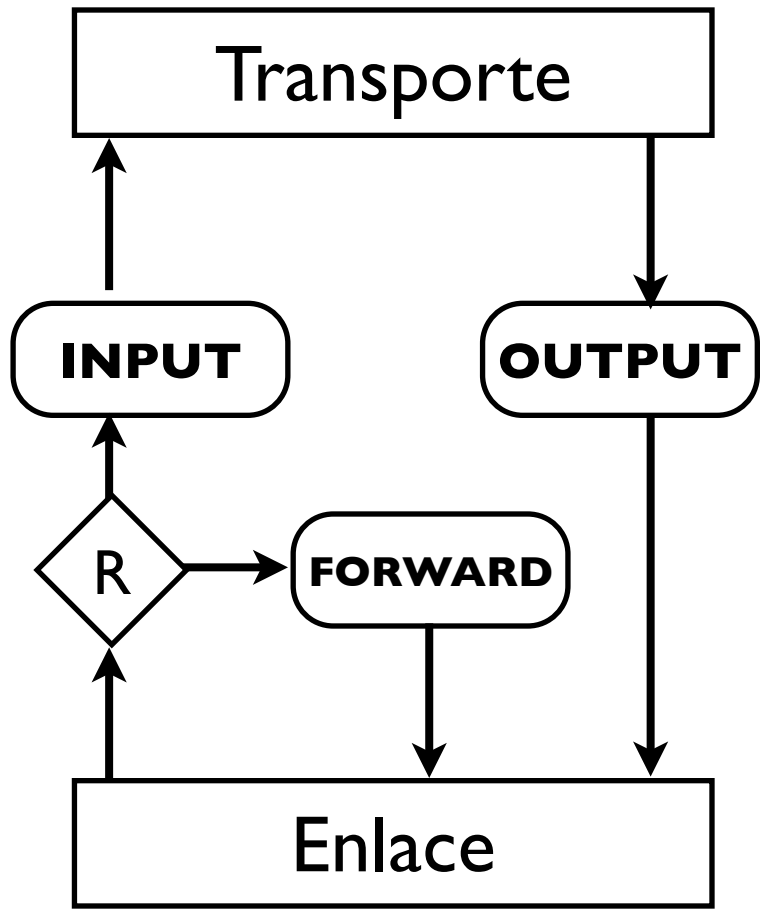
Netfilter de Linux

- iptables, comando para configurar (reglas) en netfilter
- Cadenas de reglas a aplicar en varios puntos (del proceso de paquetes por IP)
- INPUT paquetes recibidos desde el nivel de enlace
- FORWARD paquetes reenviados por este nivel de red (solo los routers *ipforwarding=True* pasan paquetes por esta cadena)
- OUTPUT paquetes generados por este ordenador
- Ejemplo: añade regla a la cadena forward que no deje pasar ningun paquete que venga de la IP 20.2.1.3

```
$ iptables -A FORWARD -s 20.2.1.3 -j DROP
```

- Esto modifica las reglas en memoria para que se mantenga al arrancar se modifican ficheros en

  /etc/sysconfig/



Cisco Access Control Lists

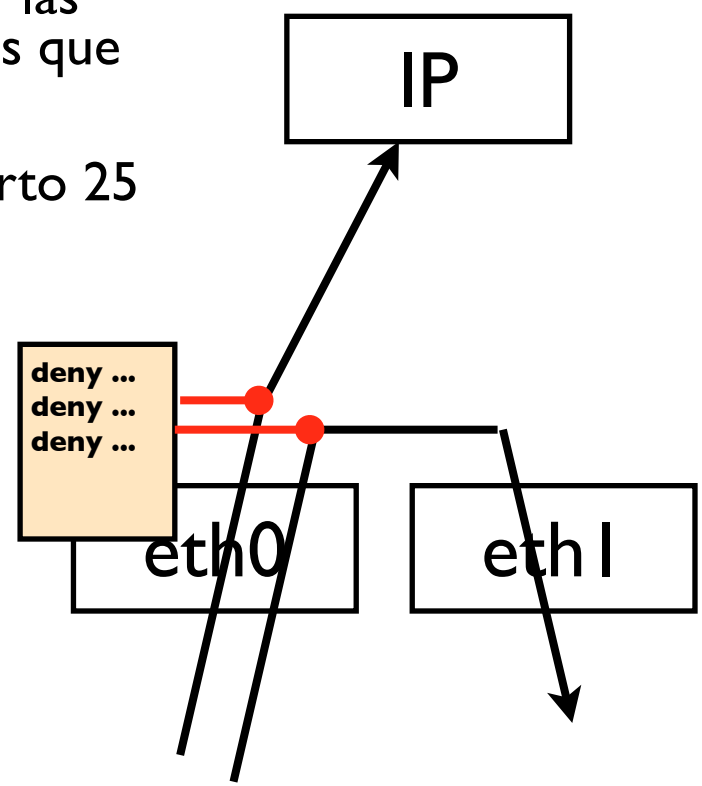
- Herramientas de CiscoIOS para filtrar paquetes
  - SACL: Standard Access Lists (filtrar solo por dirección origen)
  - EACL: Extended Access Lists (origen, destino, protocolo, puertos...)
- Las listas de acceso se definen y luego se aplican a los diferentes interfaces.
- Los paquetes reenviados los que van al router pasan por las mismas reglas. Se puede aplicar condiciones a los paqutes que entran o salen

Ejemplo deniega los paquetes que vayan o vengan al puerto 25

```
# config terminal
(config)# ip access-list extended bloqueaelmail
(config-ext-nacl)# deny tcp any any eq 25
(config-ext-nacl)# deny tcp any eq 25 any
(config-ext-nacl)# end
```

Ejemplo. En el interfaz ethernet 0

```
# config terminal
(config)# interface Ethernet 0
(config-if)# ip access-group bloqueelmail in
(config-if)# ip access-group bloqueelmail out
(config-if)# end
```



Firewalls de inspección de estados

- Mantener estado de las conexiones que ha visto el firewall
  - Puedo usar condiciones como
    - "el paquete pertenece a una conexión ya establecida"
    - "el paquete esta relacionado con una conexión ya establecida"

      por ejemplo una conexión de datos de FTP con la conexión de control FTP que la ha solicitado
  - Incluso mantener estado de flujos UDP

    (dejo pasar paquetes que vengan de DNS o de un juego en red solo si son contestación a paquetes anteriores enviados desde mis hosts)
- Firewalls eficientes y altamente escalables, soluciones comerciales con throughout superior a 6 Gbps y con más de un millón de conexiones simultáneas
- Actualmente los firewalls normalmente son de este tipo

Inspección de estados en netfilter

Condiciones sobre estado de las conexiones en iptables

- Cargando el modulo de connection tracking con

  `-m state`

  A partir de ahi podemos poner condiciones sobre el estado

  - La más útil

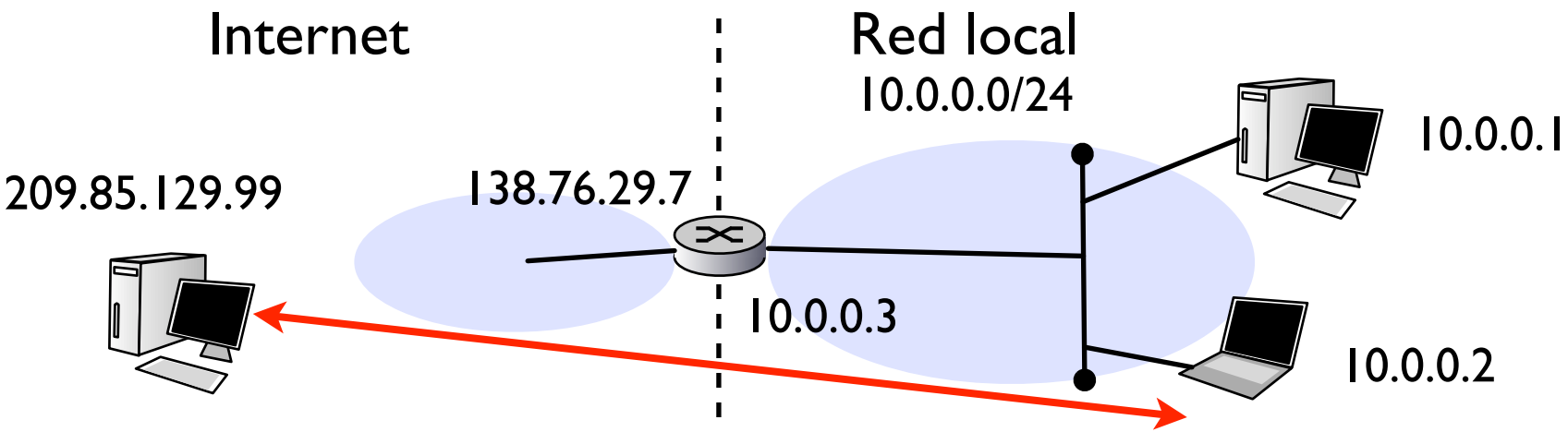
    `--state [ ESTABLISHED | NEW | RELATED ]`

    + NEW conexión nueva
    + ESTABLISHED conexión de la que ya se han visto paquetes en las dos direcciones
    + RELATED relacionada con otra conexión a traves de un protocolo conocido

  - Más condiciones para cosas como la velocidad observada de la conxión o si la conexión ha sido marcada por alguna otra regla

NAT (Network address translation)

- Firewalls de inspección de estados parecido al NAT
- Traducción de direcciones de red
  - Aparece para permitir a varios ordenadores compartir una IP
  - Los ordenadores internos usan un rango de direcciones privadas



  - Se mantiene el estado de las conexiones a traves del router/NAT y se guarda una tabla de con la traducción de direcciones y puertos
  - El ordenador externo ve que tiene una conexión con 138.76.29.7

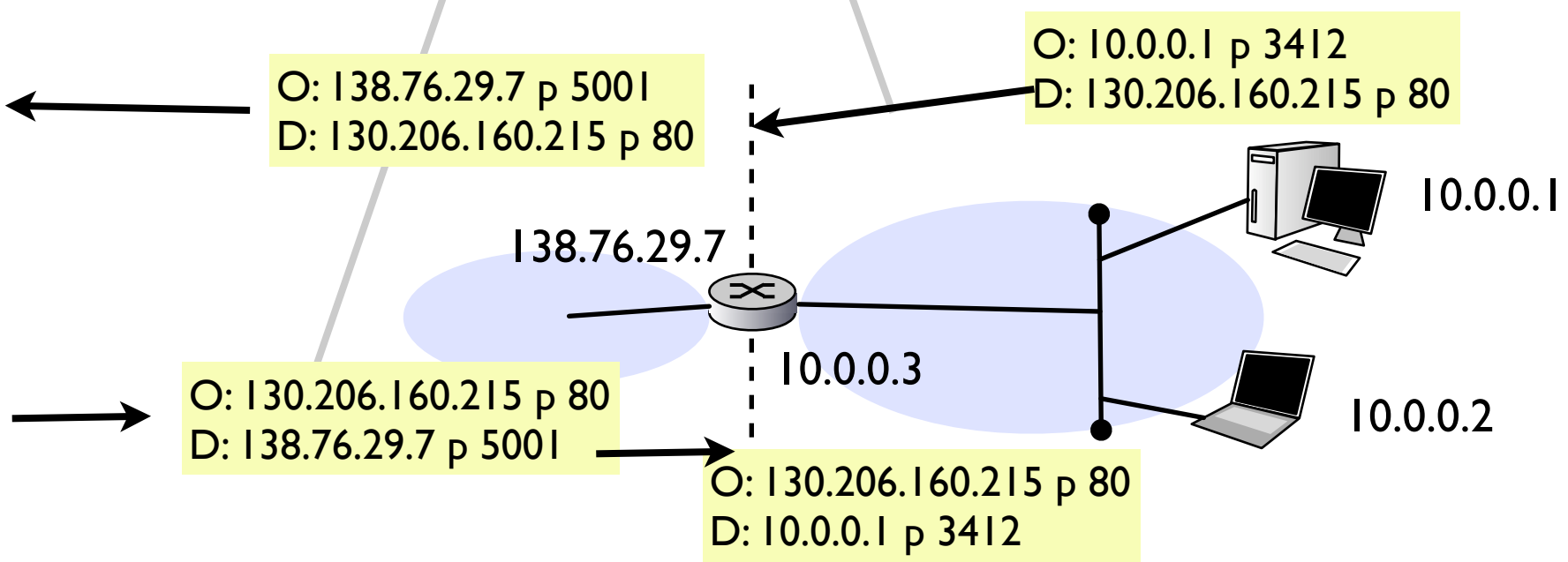
    pero el router NAT la redirige a la 10.0.0.2 ¿Que significa esto?

NAT (Network address translation)

- El router guarda una tabla de traducción de direcciones y puertos (Network Address Translation)

Tabla de NAT

Red externa	Red interna
138.76.29.7 p 5001	10.0.0.1 p 3412



NAT (Network address translation)

- Más información en Laboratorio de Programación de Redes (incluyendo como hacer NAT en Cisco)
- El NAT se parece mucho a la inspección de estados. De hecho es sólo añadir reglas de cambio de direcciones y puertos al mantenimiento de estado de las conexiones
- En Linux Netfilter hace las dos cosas

Propiedades de NAT (desde el punto de vista de seguridad)

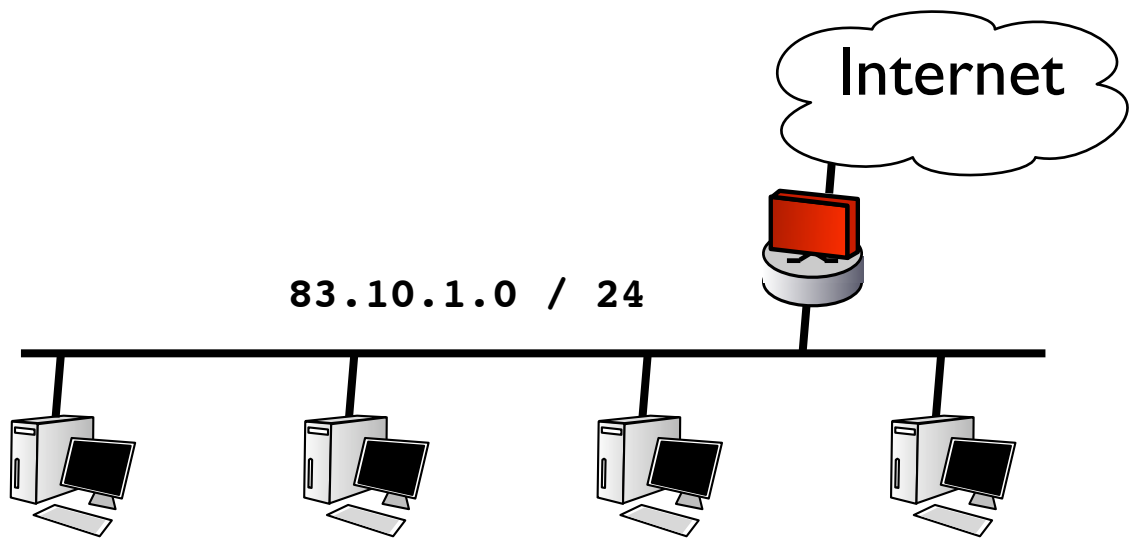
- Permite a los usuarios internos hacer conexiones hacia afuera
- No permite (por defecto) a nadie externo hacer conexiones hacia el interior (porque antes hay que especificar a quien se le dirigirán)
- Muy utilizado en redes residenciales típicas de ADSL
- Es practicamente un firewall de inspección de estados que ya está configurado para aceptar solo conexiones que empiezan en la red interna

Ejemplos de casos con firewalls

- Organización con un cortafuegos en la salida
- Política: todo lo que no esta permitido explícitamente está prohibido
- Queremos que nuestros usuarios puedan navegar por la web

```
$ iptables -P FORWARD DROP
$ iptables -A FORWARD -p tcp -s 80.10.1.0/24 -dport 80 -j ACCEPT
$ iptables -A FORWARD -p tcp -d 80.10.1.0/24 -sport 80 -j ACCEPT
```

- ¿que problema hay con esto?



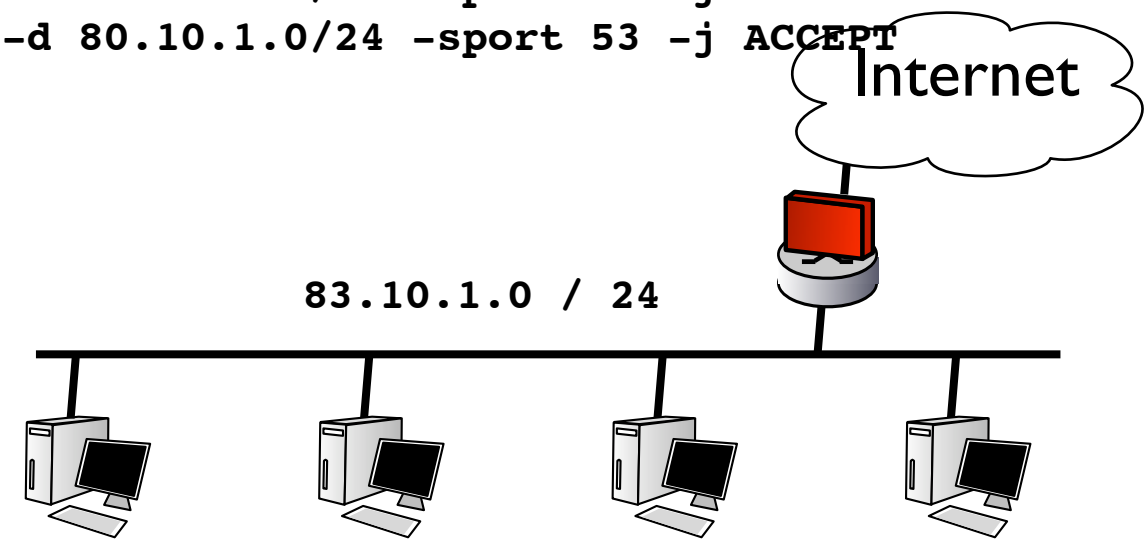
Ejemplos

- Organización con un cortafuegos en la salida
- Política: todo lo que no esta permitido explícitamente está prohibido
- Queremos que nuestros usuarios puedan navegar por la web

```
$ iptables -P FORWARD DROP
$ iptables -A FORWARD -p tcp -s 80.10.1.0/24 -dport 80 -j ACCEPT
$ iptables -A FORWARD -p tcp -d 80.10.1.0/24 -sport 80 -j ACCEPT
```

- Para que funcione también el DNS

```
$ iptables -A FORWARD -p udp -s 80.10.1.0/24 -dport 53 -j ACCEPT
$ iptables -A FORWARD -p udp -d 80.10.1.0/24 -sport 53 -j ACCEPT
```



Ejemplos

- Pero queremos también servir al exterior con un servidor web en la maquina con IP 83.10.1.9

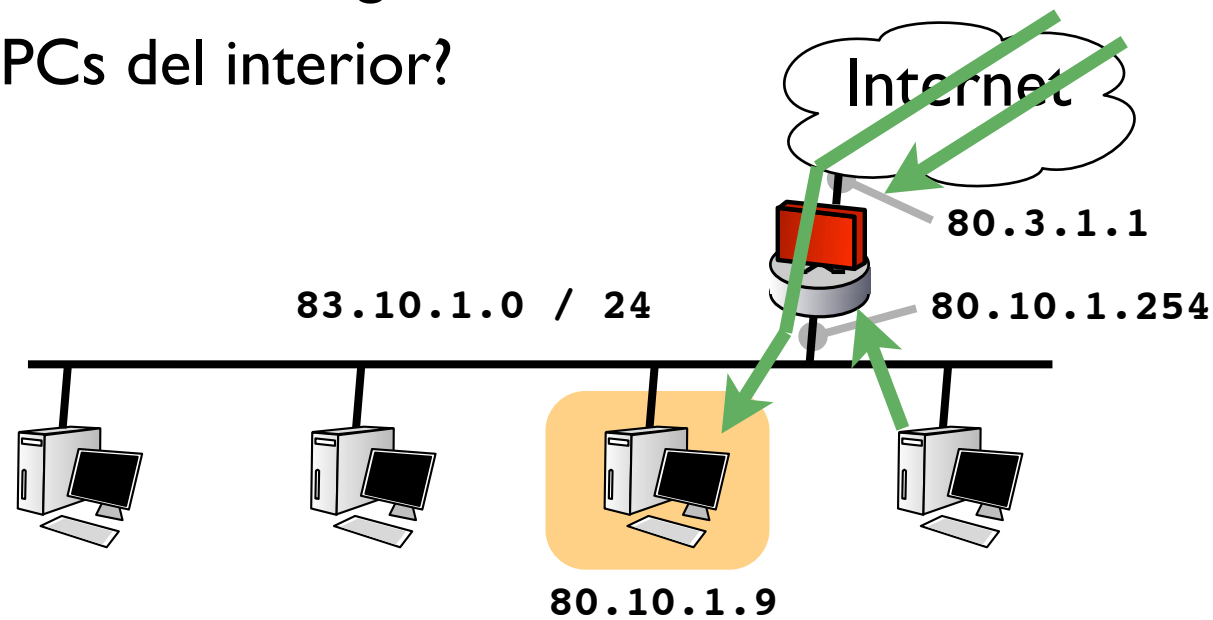
```
$ iptables -A FORWARD -p tcp -d 80.10.1.9/32 -dport 80 -j ACCEPT
$ iptables -A FORWARD -p tcp -s 80.10.1.9/32 -sport 80 -j ACCEPT
```

- ¿Hace falta hacer algo más para el DNS?

- Si el router tiene una página web de configuración...

  Se puede acceder desde los PCs del interior?

  Y desde los del exterior?



Ejemplos

- Los paquetes que van al router no pasan por la cadena de FORWARD

```
$ iptables -P INPUT DROP
```

- Si queremos que se pueda acceder a la pagina desde el interior

```
$ iptables -A INPUT -p tcp -s 80.10.1.0/24 -dport 80 -j ACCEPT
```

- Quedaria algo asi

```
$ iptables -L FORWARD -n
Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  80.10.1.0/24         anywhere            tcp dpt:80
ACCEPT     tcp  --  anywhere             80.10.1.0/24        tcp spt:80
ACCEPT     udp  --  80.10.1.0/24         anywhere            udp dpt:53
ACCEPT     udp  --  anywhere             80.10.1.0/24        udp spt:53
ACCEPT     tcp  --  80.10.1.9            anywhere            tcp spt:80
ACCEPT     tcp  --  anywhere             80.10.1.9           tcp dpt:80

$ iptables -L INPUT -n
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  80.10.1.0/24         anywhere             tcp dpt:80
```

Ejemplos

- Y si queremos una política de: todo lo que no está explicitamente prohibido, está permitido

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

- Y ahora a enumerar lo que no se puede hacer
- No aceptamos conexiones a ciertos servidores

```
$ iptables -A FORWARD -p tcp -d www.evilserver.com -j DROP
```

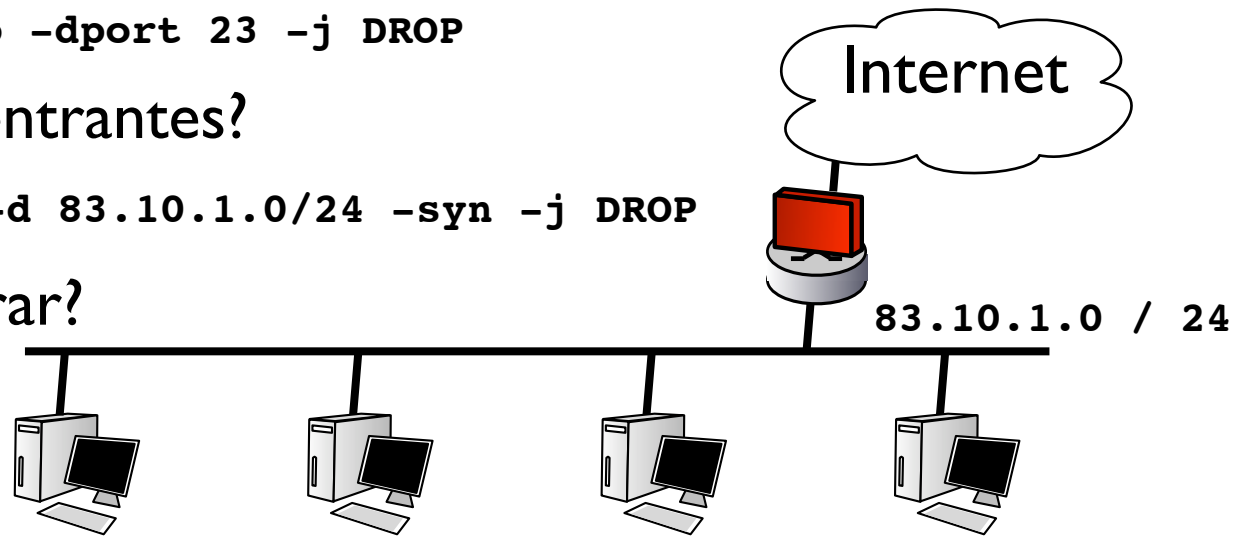
- No aceptamos uso de ciertos protocolos

```
$ iptables -A FORWARD -p tcp -dport 23 -j DROP
```

- No aceptamos conexiones entrantes?

```
$ iptables -A FORWARD -p tcp -d 83.10.1.0/24 -syn -j DROP
```

- ¿Qué es más fácil de enumerar?



Ejemplos

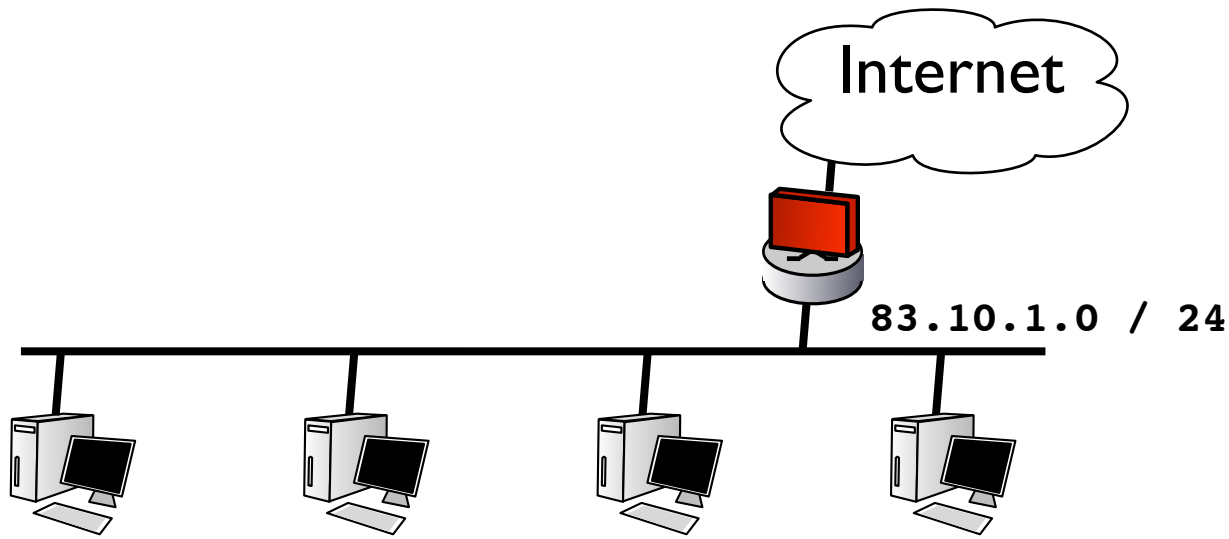
- Es lo mismo?

```
$ iptables -P FORWARD ACCEPT
$ iptables -A FORWARD -p tcp -d 83.10.1.0/24 -syn -j DROP
```

- Que

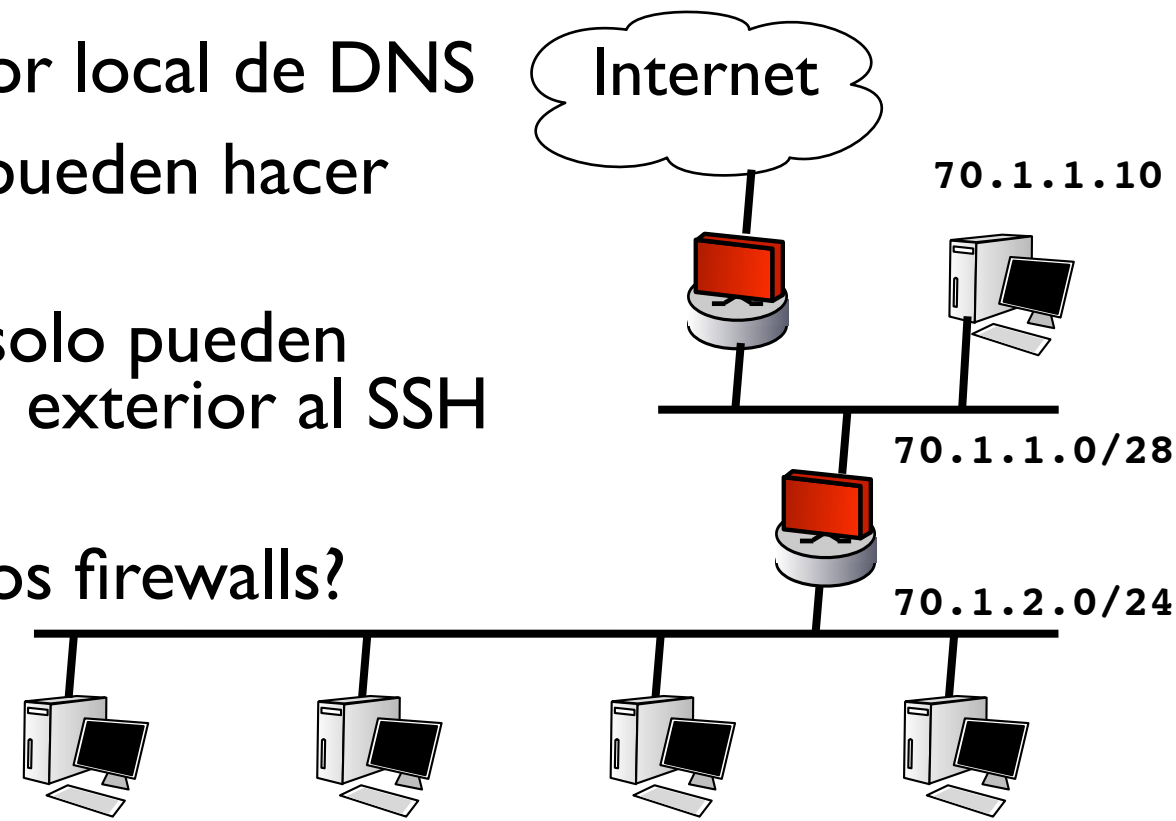
```
$ iptables -P FORWARD DROP
$ iptables -A FORWARD -p tcp -S 83.10.1.0/24 -syn -j ACCEPT
$ iptables -A FORWARD -p tcp --state ESTABLISHED
```

- ¿Cual se parece más al uso de NAT?
- ¿Qué falta en la segunda forma?



Ejemplos

- Con una arquitectura de screened net
- Se permiten accesos del exterior al bastion host por SSH, WEB y entrega de Mail al bastion host
- El bastion host es el servidor local de DNS
- Los ordenadores internos pueden hacer conexiones al exterior
- Los ordenadores internos solo pueden recibir conexiones desde el exterior al SSH desde el bastion host
- ¿Que reglas usaría en los dos firewalls?

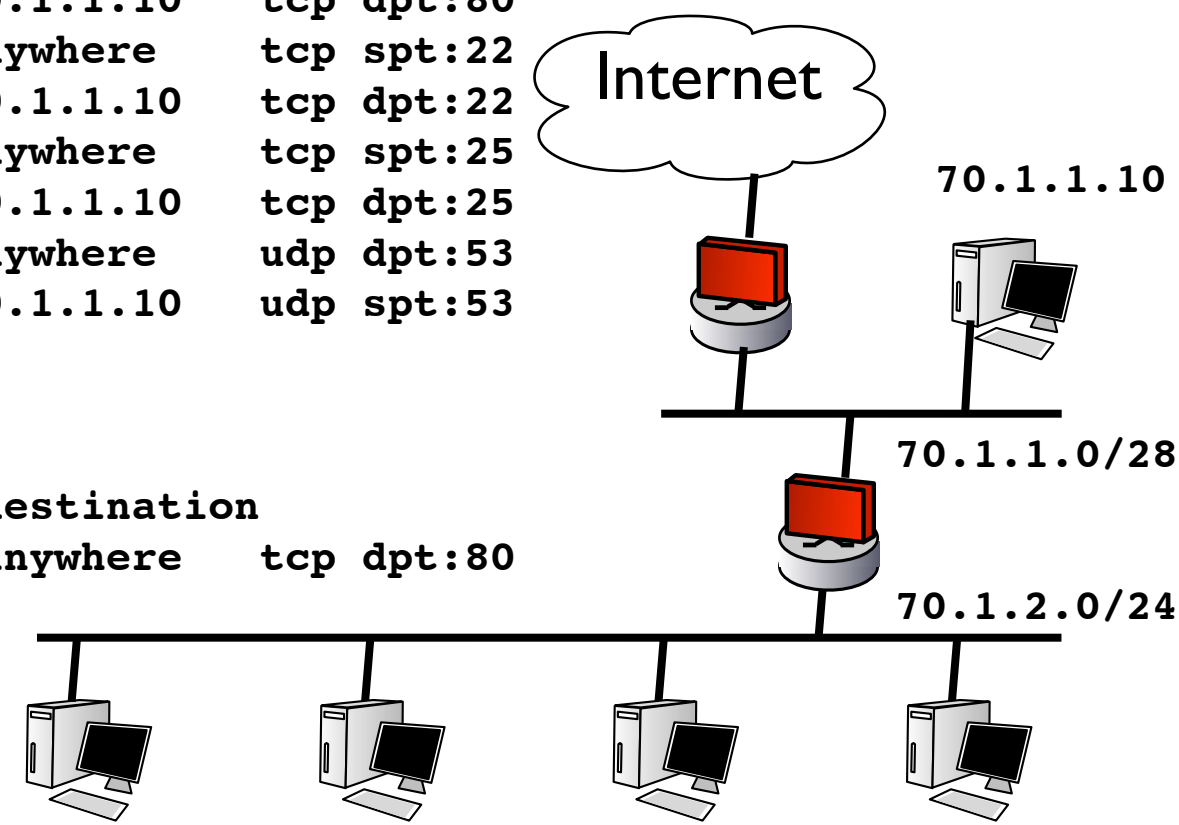


Ejemplos

- Firewall exterior

```
$ iptables -L FORWARD -n
Chain FORWARD (policy DROP)
target     prot opt source          destination
ACCEPT     tcp  --  70.1.1.10      anywhere     tcp spt:80
ACCEPT     tcp  --  anywhere       70.1.1.10    tcp dpt:80
ACCEPT     tcp  --  70.1.1.10      anywhere     tcp spt:22
ACCEPT     tcp  --  anywhere       70.1.1.10    tcp dpt:22
ACCEPT     tcp  --  70.1.1.10      anywhere     tcp spt:25
ACCEPT     tcp  --  anywhere       70.1.1.10    tcp dpt:25
ACCEPT     udp  --  70.1.1.10      anywhere     udp dpt:53
ACCEPT     udp  --  anywhere       70.1.1.10    udp spt:53

$ iptables -L INPUT -n
Chain INPUT (policy DROP)
target     prot opt source          destination
ACCEPT     tcp  --  70.1.1.10      anywhere     tcp dpt:80
```

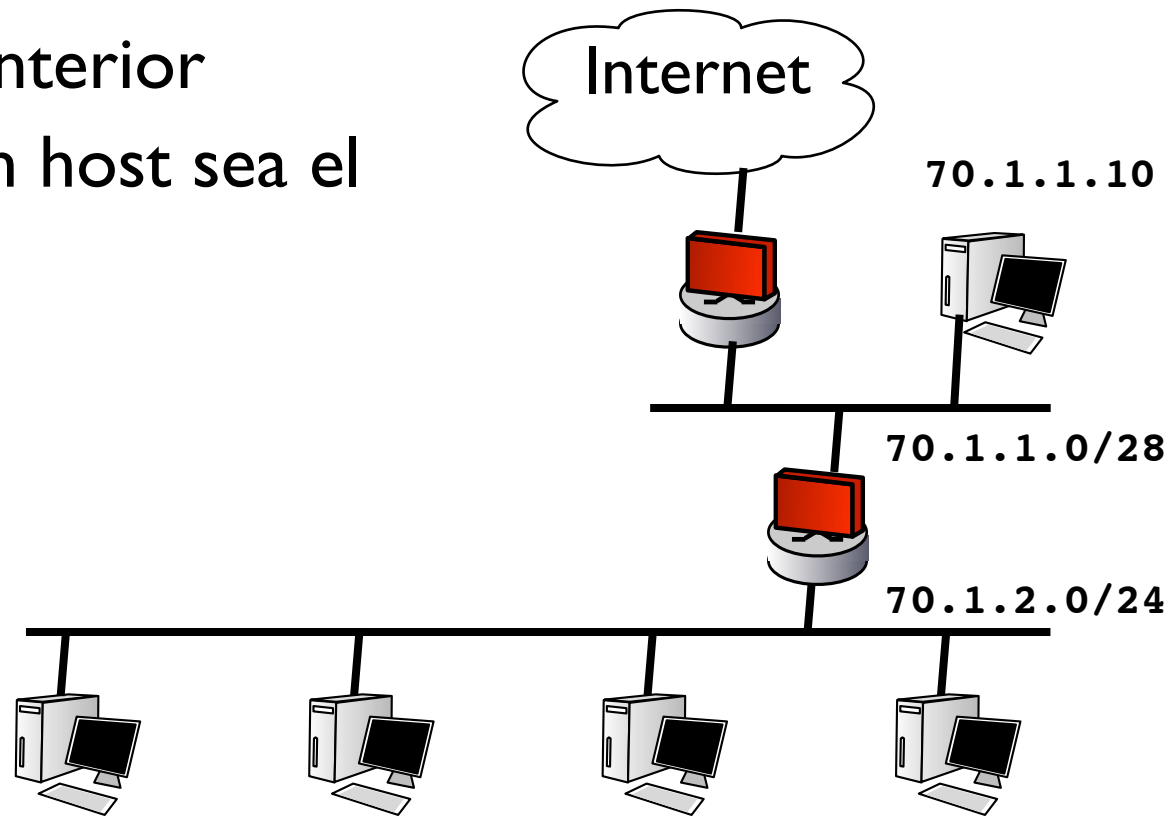


- ¿Qué opina de la ultima regla para configurar el firewall desde el bastion host?

Ejemplos

```
$ iptables -P FORWARD DROP
$ iptables -A FORWARD -p tcp -s 70.1.2.0/24 -syn -j ACCEPT
$ iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT
$ iptables -A FORWARD -p tcp -s 70.1.1.10 -d 70.1.2.0/24 -dport 22 -syn -j ACCEPT
$ iptables -A FORWARD -p udp -s 70.1.1.10 -sport 53 -d 70.1.2.0/24 -j ACCEPT
$ iptables -A FORWARD -p udp -s 70.1.2.0/24 -d 70.1.1.10 -dport 53 -j ACCEPT
$ iptables -P INPUT DROP
$ iptables -A INPUT -p tcp -s 70.1.2.27 -d 70.1.2.1 -dport 80 -j ACCEPT
```

- Para configurar el Firewall interior
- Es buena idea que el bastion host sea el servidor local de DNS?
- Por qué no?

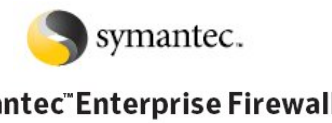


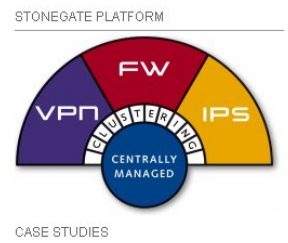
Eligiendo router/firewall

Amplia gama de sistemas de firewall

- Firewalls de sistema operativo de uso personal
- Firewalls en los routers de acceso ADSL/Cable que suelen incluir funciones de NAT
- Firewalls para pequeñas y medianas empresas con funciones de NAT y creación de VPNs
- Firewalls para empresas con balanceo de carga repartida entre varios equipos

Fabricantes





Contra qué no protege un firewall

- **Ataques internos**

  Un atacante interno puede establecer túneles o abrir puertos que atraviesen el firewall

- **Nuevos ataques**

  Las reglas pueden parar ataques conocidos pero el administrador debe adaptarlas a nuevos ataques

- **Virus**

  Los firewalls no buscan virus en los datos que se envían. Y aun así pueden encriptarse y solo encontraría los conocidos

- **Ataques que no pasan por el firewall**

  Por problemas de enrutamiento o túneles de los usuarios

- **Ataques basados en datos**

  Que afecten a servicios no filtrados

Conclusiones

- Herramientas de seguridad perimetral
  - Firewalls
  - Proxies/gateways
  - Firewalls de inspección de estados
  - NAT
- Establecer las reglas de filtrado no soluciona todos los problemas, compromiso seguridad/comodidad
- El filtrado es solo una herramienta, no sustituye a la vigilancia