

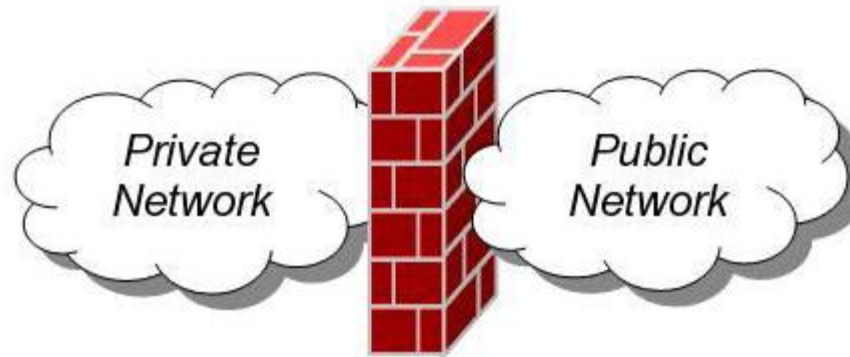
FIREWALLS, NAT Y NATP





- ¿Qué #@ \$! es un firewall?
- ¿Quien diseñó ese dispositivo de escape?

¿Que es un Firewall?



- Es un una parte de un sistema o una red que está diseñado para restringir las comunicaciones entre computadoras o redes.
- Puede ser implementado en hardware o software, o una combinación de ambos.
- Previene que las amenazas pasen de una red a otra.
- Previene que información de tipos específicos se muevan entre el mundo exterior (redes no confiables) y el interior (redes confiables).

¿Que hacen los Firewalls exactamente?

Funciones Básicas:

- ❑ Filtrado de paquetes
- ❑ Network Address Translation
- ❑ Proxy de aplicación
- ❑ Monitoreo y logueo

Otras funciones más avanzadas:

- ❑ Cache de datos
- ❑ Filtrado de contenido
- ❑ Detección de intrusiones
- ❑ Balanceo de carga

Historia

Firewall significaba originalmente una pared para confinar un incendio o riesgo potencial de incendio en un edificio.

La tecnología de los firewalls surgió a finales de 1980, cuando Internet era una tecnología bastante nueva en cuanto a su uso global y la conectividad. Los predecesores de los firewalls para la seguridad de la red fueron los routers utilizados a finales de 1980, que mantenían a las redes separadas unas de otras. La visión de Internet como una comunidad relativamente pequeña de usuarios con máquinas compatibles, que valoraba la predisposición para el intercambio y la colaboración, terminó con una serie de importantes violaciones de seguridad de Internet que se produjo a finales de los 80.

Existen 3 generaciones de Firewalls

- Filtrado de paquetes
- Filtro de estado
- Capa de aplicación

Primera generación: Filtrado de paquetes

- El primer documento publicado para la tecnología firewall data de 1988, cuando el equipo de ingenieros Digital Equipment Corporation (DEC) desarrolló los sistemas de filtro conocidos como firewall de filtrado de paquetes.
- Este sistema, bastante básico, fue la primera generación de lo que se convertiría en una característica más técnica y evolucionada de la seguridad de Internet.
- En AT&T Bell, Bill Cheswick y Steve Bellovin, continuaban sus investigaciones en el filtrado de paquetes y desarrollaron un modelo de trabajo para su propia empresa, con base en su arquitectura original de la primera generación.

2da generacion: Filtro de estado

- Durante 1989 y 1990, tres colegas de los laboratorios AT&T Bell, Dave Presetto, Janardan Sharma, y Nigam Kshitiij, desarrollaron la segunda generación de servidores de seguridad
- Esta segunda generación de firewalls tiene en cuenta, además, la colocación de cada paquete individual dentro de una serie de paquetes

3ra generación: Capa de aplicación

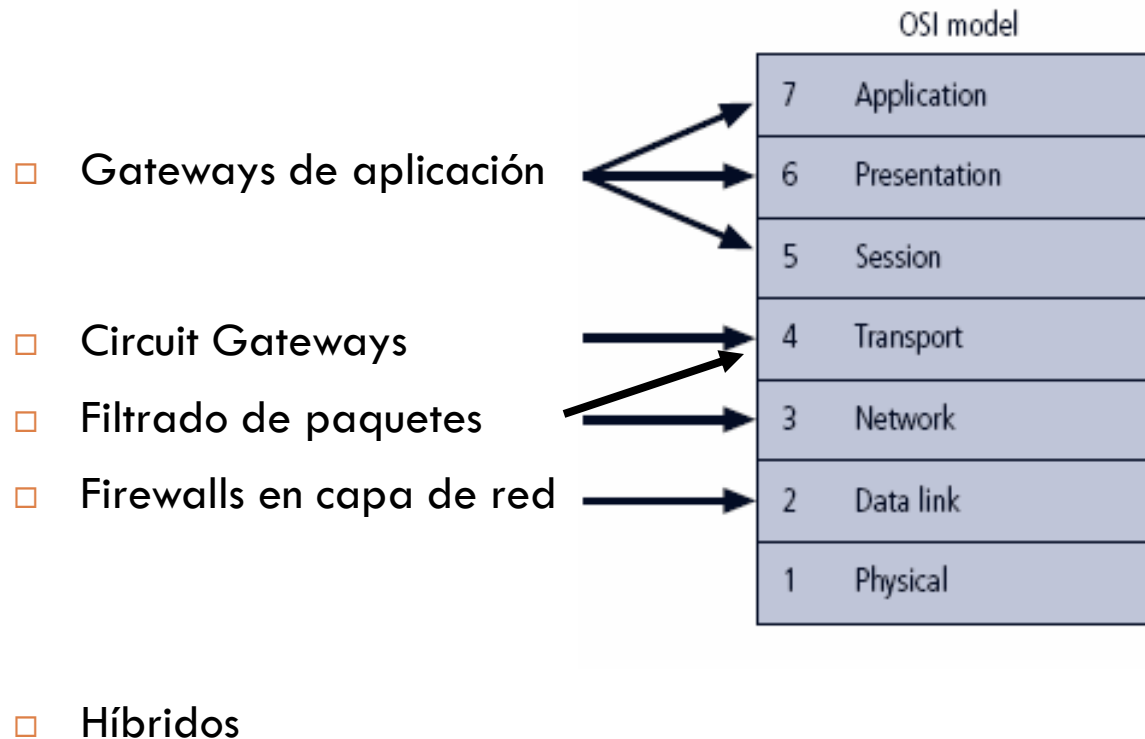
- Marcus Ranum, Wei Xu, y Peter Churchyard desarrollaron el firewall de aplicación conocido como Firewall Toolkit (FWTK).
- En Junio de 1994, Wei Xu extendió el FWTK con mejoras en el kernel para el filtrado de ip y transparente para los sockets. Esto fue conocido como el primero firewall de aplicación transparente, liberado comercialmente como producto de Gauntlet firewall en sistemas de información confiables.
- El Gauntlet firewall fue calificado como uno de los firewalls numero 1 entre 1995 y 1998.

Categorización de Firewalls



- Por modo de procesamiento
- Estructura de implementación
- Arquitectura de implementación

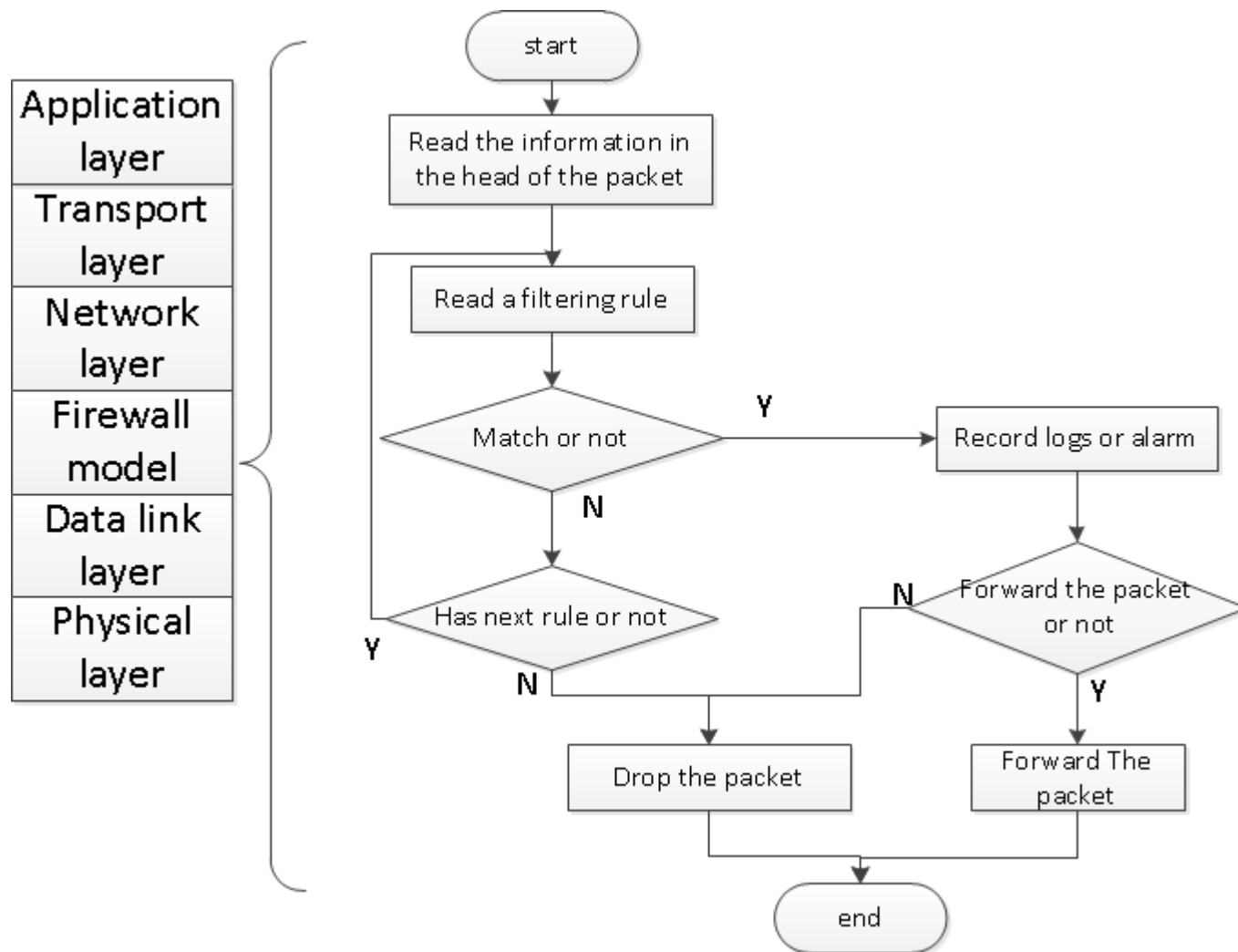
Firewalls por Modo de Procesamiento



Filtrado de paquetes

- Los firewalls de filtrado de paquetes **examinan la información de los headers** de los paquetes
- En la mayor parte de los casos **se basan en la combinación de:**
 - ▣ **Dirección de origen y destino** del IP
 - ▣ **Sentido de la transmisión** (entrada o salida)
 - ▣ **Puertos** de origen y destino de los protocolos
- Los modelos de firewalls simples determinan reglas diseñadas para prohibir paquetes con ciertas direcciones (o direcciones parciales)

Como funciona el filtrado de paquetes



Ejemplo de tabla de filtrado de paquetes

A	action	ourhost	port	theirhost	port	comment	
	block	*	*	SPIGOT	*	we don't trust these people	
	allow	OUR-GW	25	*	*	connection to our SMTP port	
B	action	ourhost	port	theirhost	port	comment	
	block	*	*	*	*	default	
C	action	ourhost	port	theirhost	port	comment	
	allow	*	*	*	25	connection to their SMTP port	
D	action	source	port	destination	port	flags	comment
	allow	{our osts}	*	*	25		our packet to their SMTP port
	allow	*	25	*	*	ACK	their replies
D	action	source	port	destination	port	flags	comment
	allow	{our osts}	*	*	*		our outgoing calls
	allow	*	*	*	*	ACK	their replies to our call
	allow	*	*	*	>1024		traffic to nonservers

Filtrado de paquetes estático

- Filtrado **estático (o stateless packet filtering)**: provee filtrado de paquetes basado solo en la información del paquete analizado en el momento las reglas establecidas por el administrador.
Controla el acceso a una red analizando paquetes entrantes y salientes, dejándolos pasar o rechazándolos basándose en la información de las capas de red y transporte del modelo OSI.

Filtrado de paquetes estático

Ventajas:

- **Bajo impacto en la performance de la red**
- **Bajo costo**
- **Un solo router puede proteger toda la red**
- No requiere cooperación o conocimiento por parte del usuario
- Está disponible en muchos de los routers

Desventajas:

- Las herramientas para configurar el filtrado no son muy buenas:
 - Es **difícil testear las reglas** una vez configuradas
 - Las **capacidades de algunas herramientas de filtrado son bastante limitadas**, y no permiten implementar todas las reglas que uno querría
 - Es muy **difícil determinar correctamente las reglas** de filtrado que uno **necesita**
- Algunos **protocolos no son muy aptos para ser filtrados por paquetes**
- Algunas **políticas no pueden implementarse** por medio de filtrado de paquetes estático
- Es **susceptible al IP spoofing**
- Dado que no conoce el estado del paquete **requiere dejar abiertos muchos puertos para poder proveer servicios que usan puertos alocados dinámicamente**

Filtrado de paquetes dinámico

- Filtrado **dinámico o con estado (o statefull packet filtering)**: provee filtrado de paquetes no solo basándose en el análisis del paquete actual sino en los anteriores, verificando así, no solo los puntos de conexión sino también el estado, es decir si esos paquetes pertenecen a una conexión existente.

Controla el acceso a la red basándose en:

- **Reglas establecidas por el administrador** determinando direcciones IP y puertos de la capa de transporte
- **Estado de la conexión**, que considera paquetes anteriores que hayan pasado por el firewall. Para esto el firewall genera rutas temporales, por eso se le dice filtrado dinámico

Filtrado de paquetes dinámico

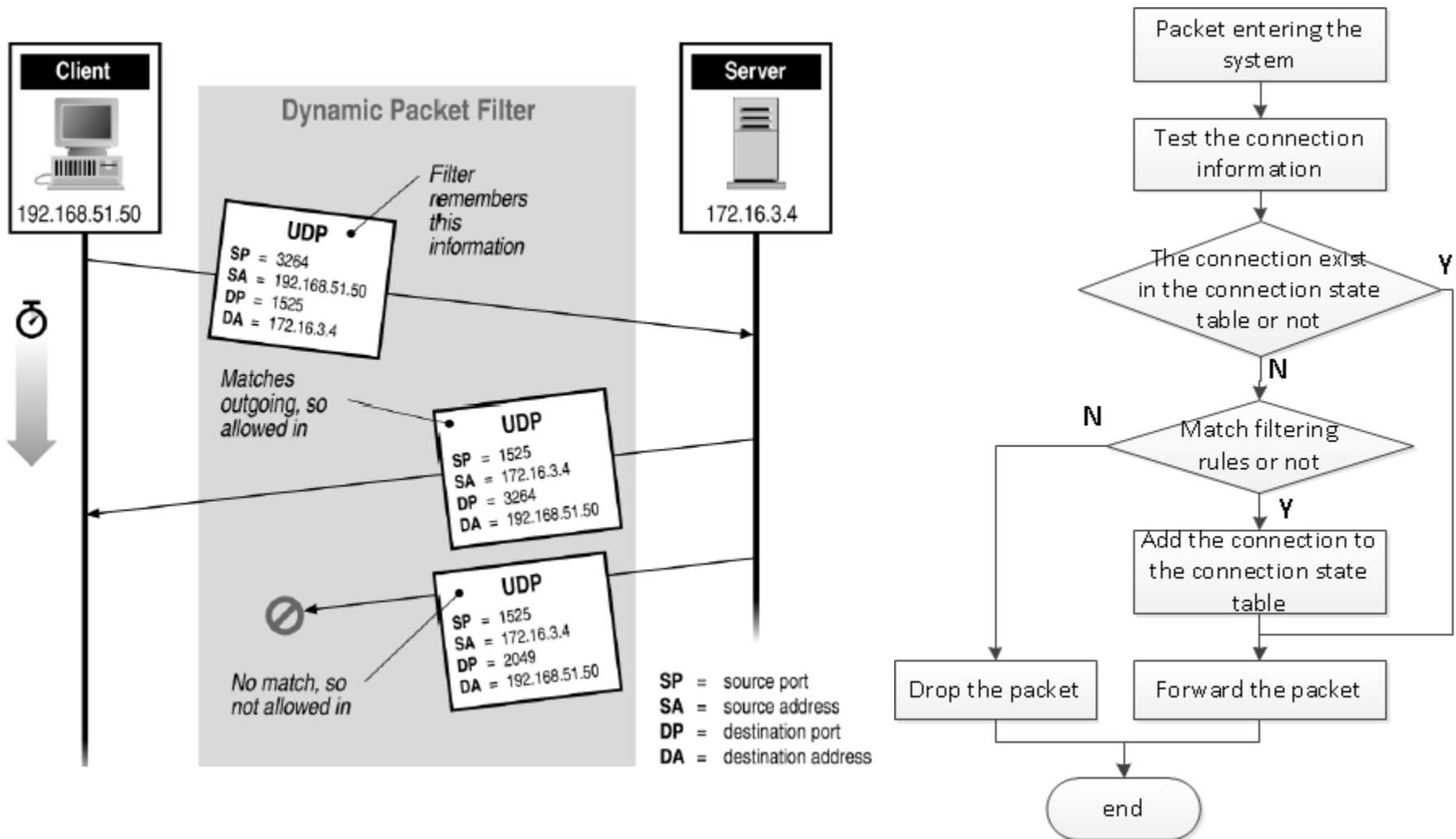
Ventajas:

- ❑ **Bajo costo**
- ❑ El conocimiento del estado del paquete provee **beneficios de performance , escalabilidad y extensibilidad**

Desventajas:

- ❑ Opera en **capa de red y transporte solamente.**
- ❑ Es **susceptible al IP spoofing**
- ❑ Es **difícil de crear reglas y establecerles ordenes de precedencia**
- ❑ Introduce **riesgos adicionales** si las **conexiones de red no** se establecen siguiendo el **3 way handshake recomendado por el RFC** de TCP

Como funciona la inspección de estado de paquetes



Gateway de aplicación (o Proxy)

- Es un tipo de firewall que no solo determina si una conexión debe realizarse o no, sino también **como** debe realizarse.
- El gateway de aplicación intercepta cada conexión de entrada o salida que pase por el firewall, y luego (si la conexión está permitida) **establece su propia conexión con el host de destino** de parte del que la originó. A este tipo de conexión se le llama conexión proxy.
- Un gateway de aplicación es un tipo de servidor proxy que provee proxies para aplicaciones específicas.
- Hay gateways de aplicación genéricos y específicos:
 - Los **genéricos** provee un método de conexión uniforme para cualquier aplicación, sin importar cual es.
 - Los **específicos** “entienden el protocolo” de la aplicación específica para la cual se establece el proxy. Dado que estos entienden el protocolo, pueden filtrar no solo basándose en origen y destino sino en funcionalidades específicas del servicio que se está “proxiando”(?)
- El **programa cliente** para el que se establece el proxy **debe configurarse para trabajar “atrás” del proxy**. Las conexiones no se establecen transparentemente

Gateway de aplicación

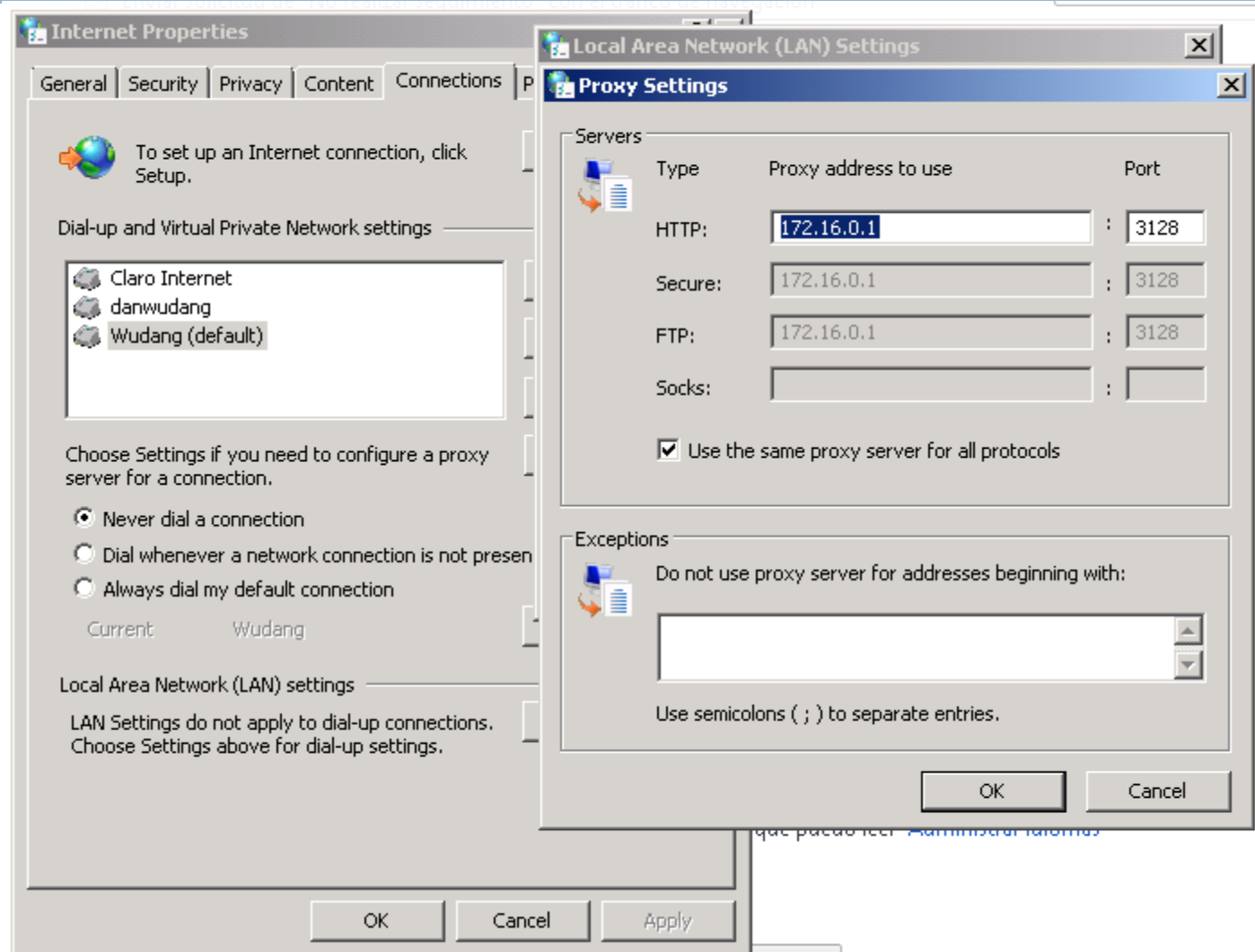
Ventajas

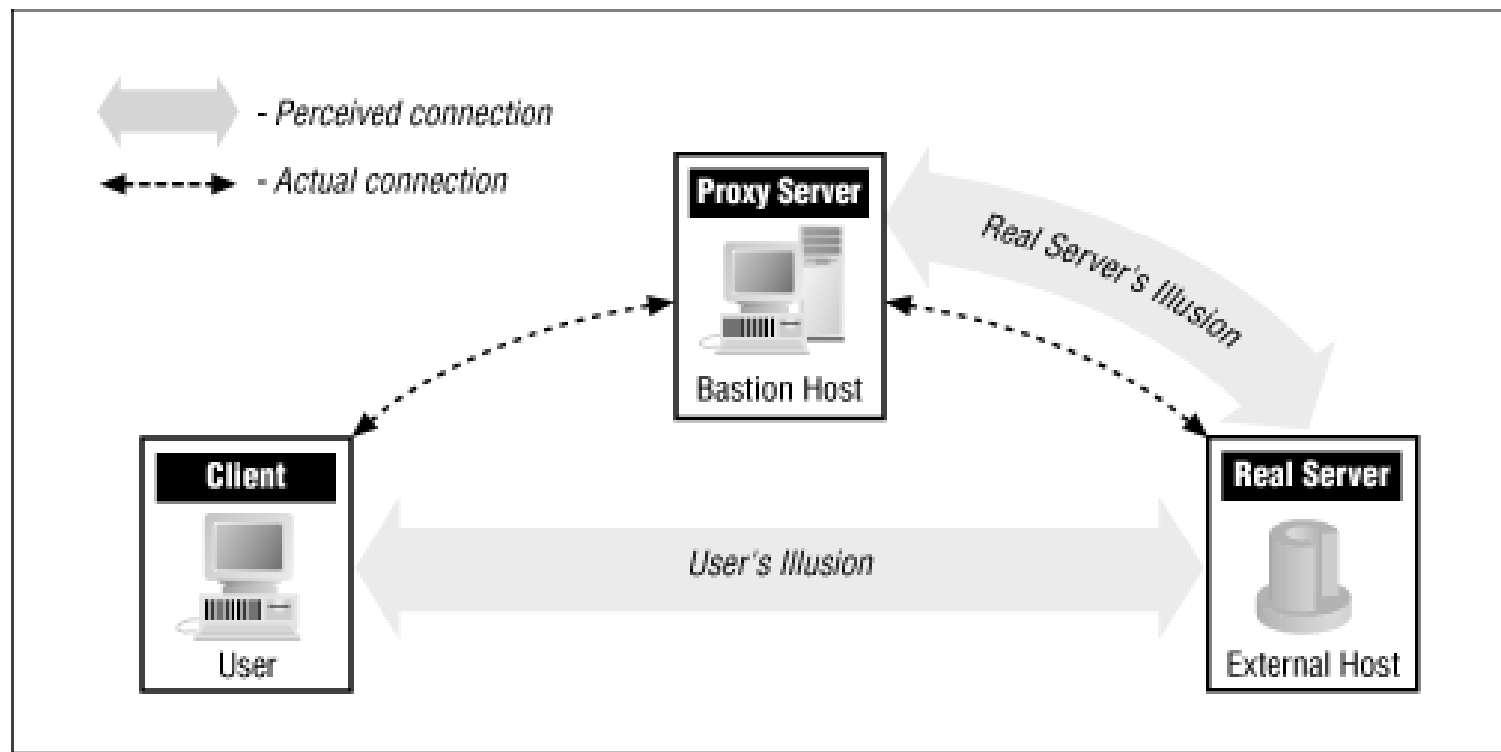
- ❑ Mejor manejo de logs del tráfico de red ya que todos los datos transmitidos entre cliente y servidor son ruteados a través del proxy y esto hace posible no solo controlar la sesión y proveer un logging detallado.
- ❑ Maneja estados de los servicios
- ❑ Los proxys mas complejos pueden inspeccionar el largo de los headers de protocolo y eliminar gran parte de los ataques por buffer overrun
- ❑ Mayor nivel de seguridad ya que trabaja en capa de aplicación

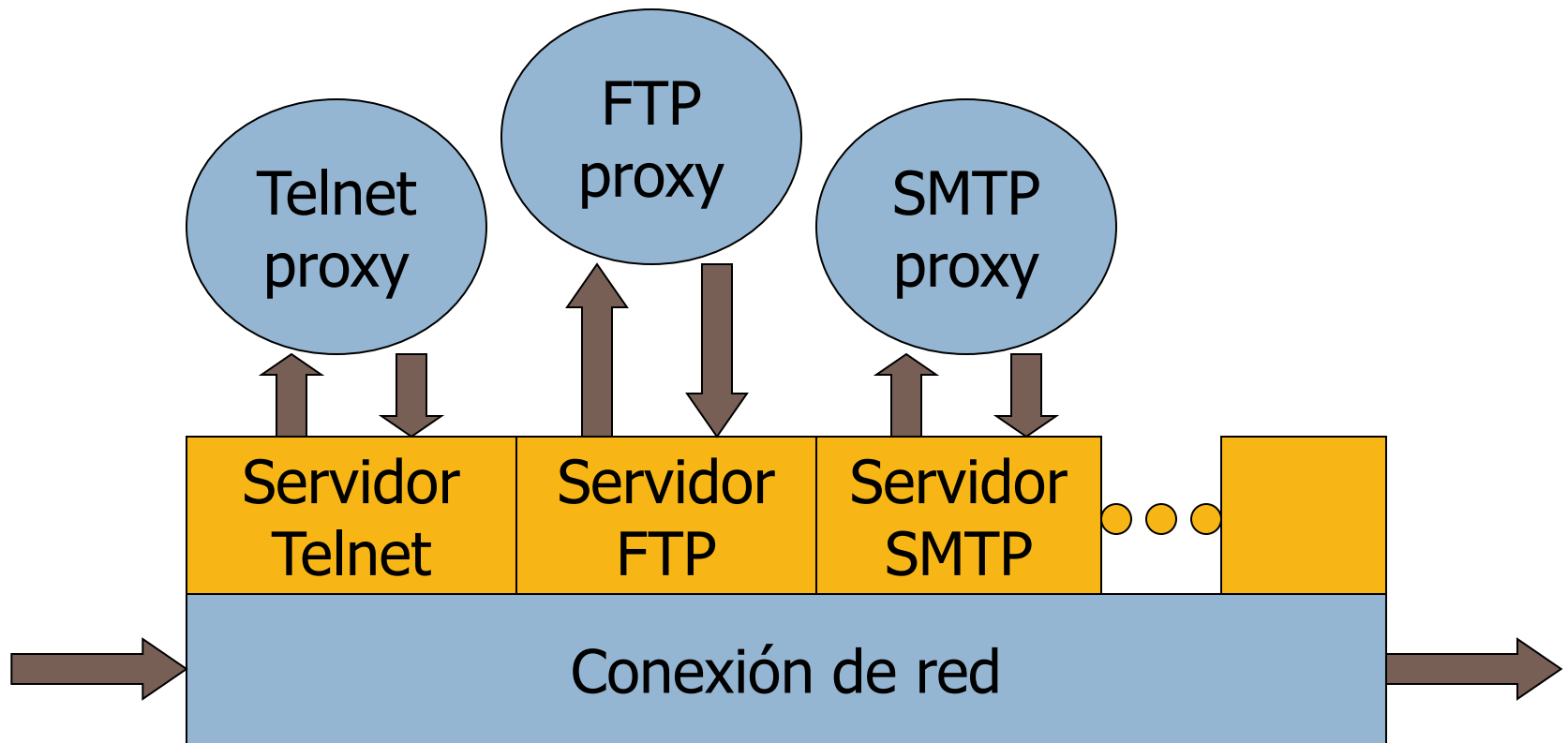
Desventajas

- ❑ No todos los servicios pueden “proxarse”
- ❑ Requieren configuración del lado del cliente
- ❑ No todos los servicios se manejan con un solo server, por lo tanto puede que haya que tener varios servidores proxy instalados para hacer proxy de varios servicios
- ❑ Tiene impacto en la performance, por el alto número de conexiones que debe manejar.
- ❑ Es complejo de configurar teniendo en cuenta todos los detalles sobre cada aplicación que se quiere “proxiar”
- ❑ Los proxies tienen la capacidad de filtrar por operaciones del servicio, pero no todos los protocolos métodos sencillos para hacerlo, o de alguna manera de hacerlo siquiera.

Gateways de aplicación







Circuit Gateway Firewalls

- Opera sobre las **capas de transporte y sesión** del modelo OSI.
- En muchos aspectos es como una extensión del filtrado de paquetes, en el sentido de que realiza **operaciones de filtrado de paquetes básico** y luego agrega **verificaciones del TCP handshaking y de la legitimidad de la información de sesión** usada para establecer la conexión.
- El Circuit Gateway **determina si una sesión es legítima solo si los flags SYN y ACK, y los números de secuencia involucrados en el handshaking tienen sentido.**
- Luego de chequear si la sesión es válida, se compara la información del paquete para verificar si coincide con alguna de las reglas de la tabla de filtrado de paquetes. Si no se encuentra ninguna regla que aplique, **generalmente, la regla por defecto es desechar el mismo.**
- **Una vez que la se aprobó la conexión,** el circuit gateway **solo se ocupa de hacer relay de los paquetes,** o sea, de forwardarlos sin inspeccionar su contenido.
- Previenen conexiones directas entre 2 redes creando túneles conectando procesos o sistemas específicos a ambos lados del firewall y solo permitiendo el tráfico autorizado en esos túneles.

Circuit Gateway Firewalls

Ventajas

- Poco impacto en la performance de la red
- Intercepta y no permite conexiones directas a servidores que están detrás del firewall
- Mayor nivel de seguridad que un filtrado de paquetes (dinámico y estático)
- Provee servicios para una amplio rango de protocolos

Desventajas

- Comparte muchos de los problemas asociados con filtrado de paquetes
- Permite que cualquier dato pase a travez de la conexión
- Bajo nivel de seguridad

Firewalls en capa de red

- Están **diseñados para operar con la MAC address** de los dispositivos de red.
- Esto le da a los firewalls la habilidad de identificar a un host de manera específica en una decisión de filtrado.
- De esta manera la MAC address de los hosts específicos se asocian a las **entradas de ACL que especifican que tipos de paquetes pueden enviar o recibir**, y el resto del tráfico puede ser bloqueado.

Híbridos

- **Combinan elementos de diferentes tipos de firewalls**, por ejemplo, elementos de filtrado de paquetes y servicios proxy, o filtrado de paquetes y circuit gateways.
- A veces también pueden consistir de **2 dispositivos separados**, cada uno de ellos como un sistema de firewall separado, pero **conectados para trabajar en conjunto**.

Firewalls por arquitectura de implementación

- Screening Router
- Dual-homed Host
- Screened Host
- Screened Subnet
 - ▣ Red Perimetral
 - ▣ Bastion host
 - ▣ Router interior
 - ▣ Router exterior
- Zona Desmilitarizada

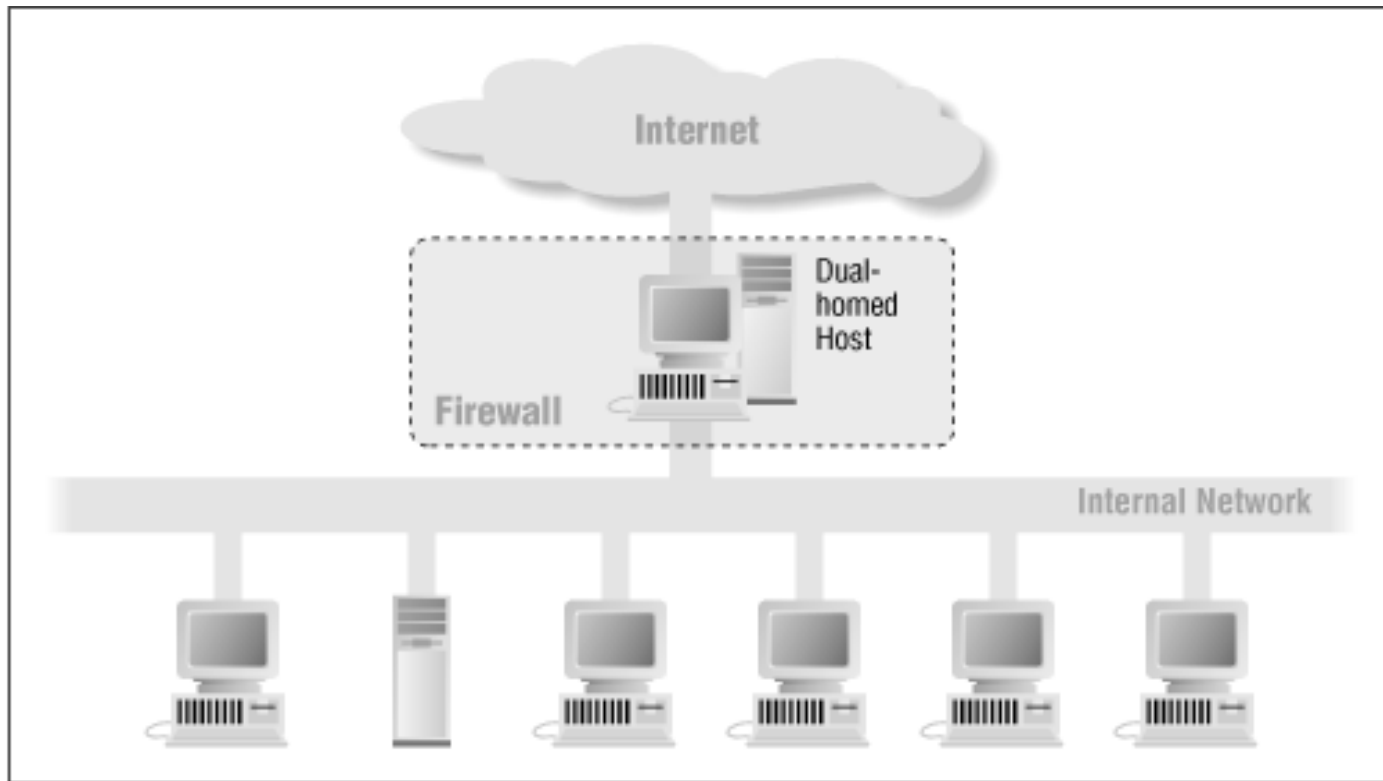
Arquitectura Screening Router

- El método mas **sencillo de implementar** un firewall es poniendo **filtrado de paquetes en el router**.
- Esta arquitectura es **completamente transparente para todas las partes involucradas**.
- El problema es que si algo pasara con el mecanismo de control de acceso, entonces cabería la posibilidad de que tráfico no autorizado pueda encontrar la manera de entrar en la red, o “filtrarse” información propietaria fuera de la red.
- Además los screening routers tienden a violar el punto principal de los firewalls. **Si bien todo el tráfico pasa por el router** en uno u otro punto, el router **pasa el tráfico a su destino último. Cada destino** dentro de la red por lo tanto, **debe ser protegido**.
- A pesar de que los screening routers pueden ser una parte importante de la arquitectura de un firewall, **no se los considera un mecanismo adecuado**.

Arquitectura Dual-Homed Host

- Se construye a través de **una computadora con al menos 2 interfaces de red**.
- Ese host **actúa como router entre las redes** a las que sus interfaces están conectadas, y es capaz de routear paquetes IP de una red a otra.
- **Se deshabilita la función de ruteo. Los paquetes IP de una red no se rutean directamente a la otra red.** Los sistemas dentro del firewall pueden comunicarse con el dual-homed host y los sistemas fuera del firewall también, pero los primeros y los últimos no pueden comunicarse entre sí directamente.
- Proveen un **alto nivel de control**. Al no permitir que los paquetes pasen entre las redes externa e interna, uno puede asegurarse que todo paquete de la red interna, que tiene como origen la red externa, es evidencia de algún tipo de problema de seguridad. En algunos casos un dual-homed host **puede rechazar conexiones que dicen ser para un particular servicio pero que no contienen el tipo de datos adecuado para ese servicio** (los sistemas de filtrados de paquete no proveen esto tan fácilmente).
- Un dual homed-host **solo puede proveer servicios “proxiándolos”, o haciendo que los usuarios se logueen directamente en el host**. Esta última opción generalmente trae problemas de seguridad de por sí.
- Un problema con los **servicios proxy** sin embargo, es que **no están disponibles para todos los servicios** que uno quiera proveer.

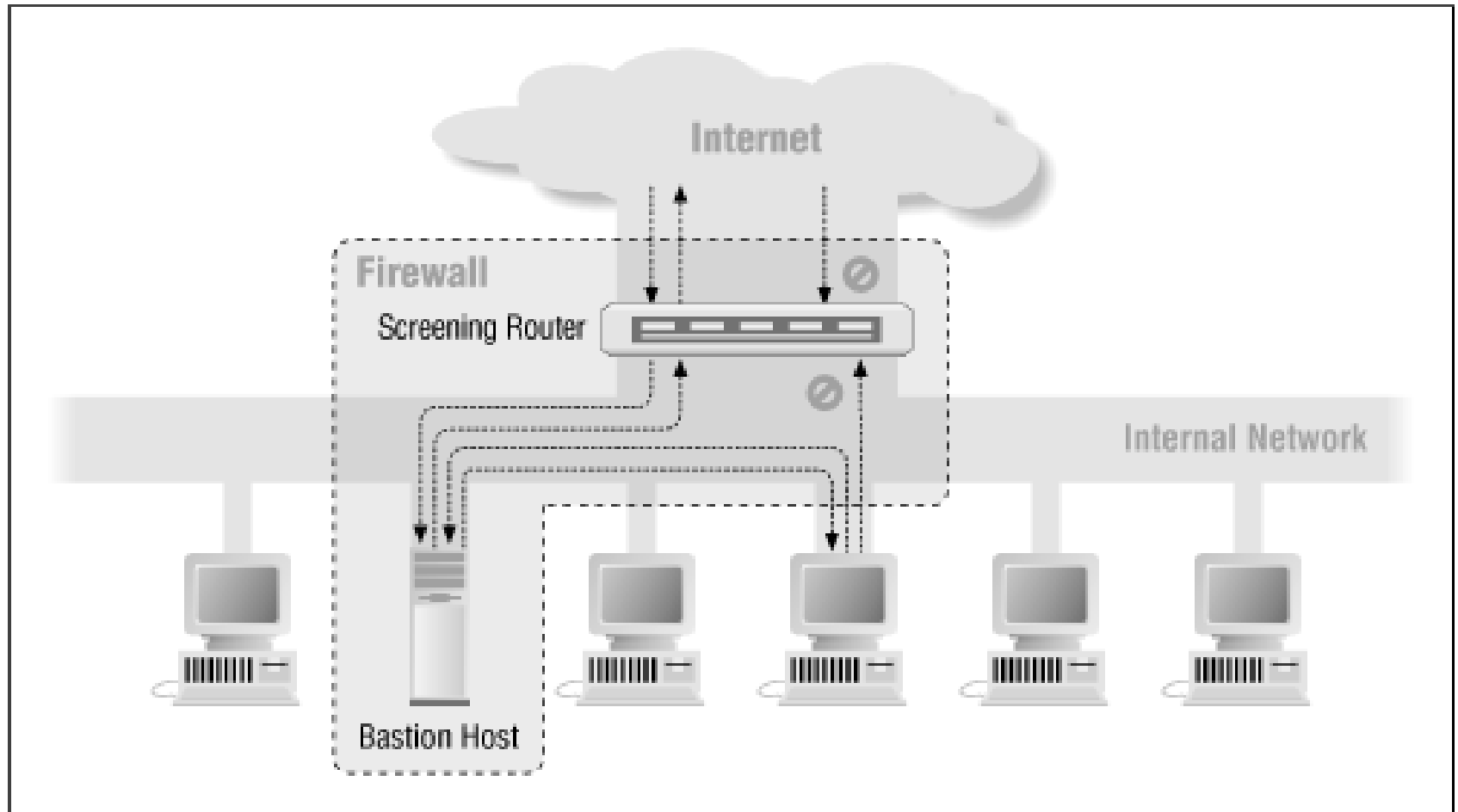
Arquitectura Dual-Homed Host



Arquitectura Screened Host

- Provee servicios de **un host que está conectado solo a la red interna, usando un router por separado**. La seguridad está provista por **filtrado de paquetes**. (Por ejemplo, el filtrado de paquetes es lo que **previene a la gente de saltarse el proxy para establecer conexiones directas**)
- Se establece un **“Bastion host” dentro de la red interna**. El filtrado de paquetes en el screening router se configura de manera que **el bastion host es el único sistema en la red interna con el que los hosts de internet pueden abrir conexiones** (por ejemplo, para enviar correo entrante). Solo ciertos tipos de conexiones están permitidas. **Cualquier sistema externo** tratando de acceder a los sistemas o servicios internos **tendra tendrá que conectarse con este host**. Por lo tanto **el bastion host, tendrá que mantener un alto nivel de seguridad**.
- El filtrado de paquetes permite que el bastion host abra conexiones permitidas hacia el mundo exterior.
- La configuración del **filtrado de paquetes en el screening router puede** hacer lo siguiente:
 - ▣ Permitir a otros hosts internos abrir conexiones a hosts en la internet solo para algunos servicios (por medio de packet filtering)
 - ▣ Deshabilitar todas las conexiones de hosts internos (forzándolos a usar los servicios proxy del bastion host)
- Se pueden combinar esas dos técnicas para diferentes servicios; algunos pueden estar habilitados para salir via packet filtering, y otros habilitados para hacer indirectamente, via el proxy del bastion host. Todo depende de las políticas particulares de cada administrador y sistema.

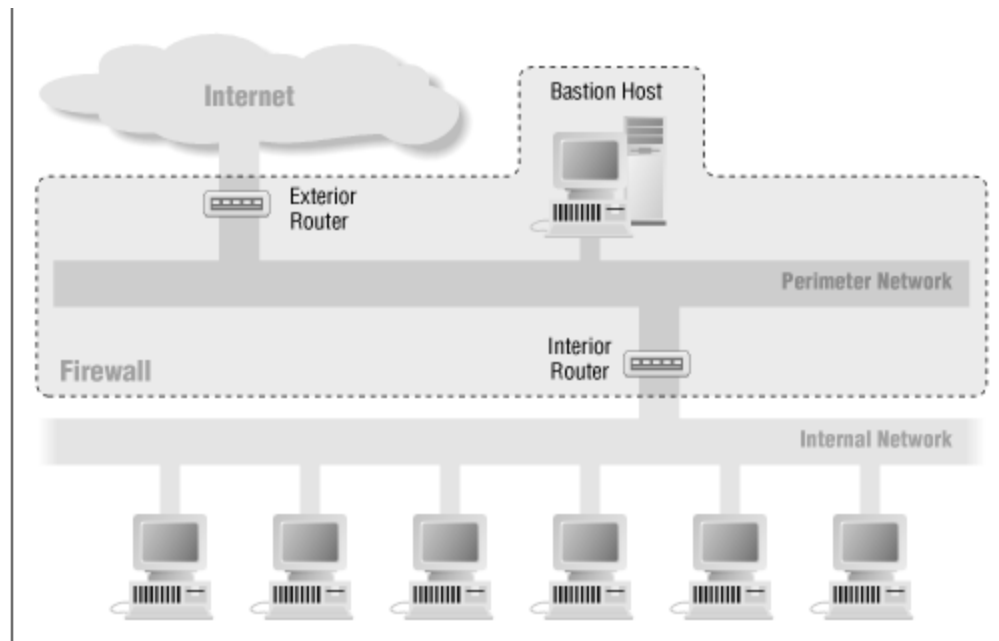
Arquitectura Screened Host



Arquitectura Screened-Subnet

- Esta arquitectura **agrega otra capa de seguridad a la del screened host**, añadiendo una **red perimetral** que **aísla la red interna de la internet**.
- Esto se hace porque **los bastion hosts son los equipos mas vulnerables** en la red interna. A pesar de los esfuerzos para protegerlos, son las computadoras mas propensas a ser atacadas. Y **a partir de un ataque a los bastion hosts es facil luego, atacar la red intena**, ya que no hay defensa entre estas 2.
- **Aislando el bastion host en una red perimetral**, uno puede reducir el impacto de una entrada indeseada en el mismo.
- En la forma mas simple de una arquitectura tipo screened subnet, **hay 2 screening routers, cada uno conectado a la red perimetral. Uno entre la red perimetral y la red interna, y el otro entre la red perimetral y la red externa** (generalmente internet).
- Para burlar esta seguridad y meterse en la red internet a con esta arquitectura un atacante tendría que poder pasar ambos routers. Incluso si se hubiera metido en el bastion host.
- Algunos sitios crean una serie de capas de redes perimetrales entre el mundo exterior y la red interna. Los servicios mas vulnerables y menos confiables se ponen en las capas mas externas, lejos de la red interna. La idea es que un atacante que logra penetrar en una maquina que está en los perímetros mas externos les será mas dificil atacar las máquinas que están mas adentro por las capas de seguridad adicionales.

Arquitectura Screened-Subnet



Red Perimetral

- **Es otra capa de seguridad, una red adicional entre una red externa y la red interna protegida.** Si un hacker puede penetrar en las partes mas externas del firewall la red perimetral ofrece una capa adicional de protección entre el atacante y los sistemas internos.
- Un ejemplo de cuando la red perimetral puede ser útil: en muchas configuraciones de red, es posible que cualquier equipo en esa red vea el trafico de todas los demás equipos en la red. Esto es cierto para la mayor parte de las redes ethernet y para otras tecnologías. Los snoopers pueden obtener password mirando los paquetes que pasan por la red , por ejemplo para las sesiones de telnet, ftp, rlogin; o incluso pueden mirar los contenidos de archivos a los que la gente acceda, o mails, etc.
- Con una red perimetral, **si alguien logra penetrar en un bastion host en la red perimetral, sería posible snopear solo el tráfico de esa red.** Todo el tráfico la red perimetral será solo del bastion host (hacia o desde)

Bastion Host

- Con la arquitectura de screened subnet, uno acopla un bastion host (o hosts) a la red perimetral y este será el **principal punto de contacto para las conexiones entrantes desde el mundo exterior**.
- Los servicios salientes se manejan de una de las siguientes maneras:
 - ▣ Configurando filtrado de paquetes en los routers exterior e interior para permitir a los clientes internos acceder a servidores externos directamente.
 - ▣ Configurando servidores proxy que corren en el bastion host para permitir a los clientes internos acceso a servidores externos indirectamente. También debería configurarse el filtrado de paquetes para permitir a los clientes internos “hablar” con los servidores proxy del bastion host y viceversa, pero prohibir comunicaciones entre clientes internos y el exterior.
- La mayor parte de lo que hacen los bastion hosts es **actuar como servidores proxy para varios servicios**, ya sea corriendo proxies especializados para protocolos particulares (como HTTP y FTP), o corriendo servidores generales (como STMP)

Router Interior

- A veces llamado **choke router**.
- **Protege la red interna de internet y de la red perimetral.**
- El router interior hace la mayor parte del **filtrado de paquetes**. Permite que los servicios seleccionados salgan de la red interna hacia internet. Estos son los servicios que el sitio puede soportar y proveer de manera segura usando packet filtering, no proxies.
- Los servicios que el router interior permite entre el bastion host y la red interna no son necesariamente los mismos que permite entre internet y la red interna.
- La razón para limitar los servicios entre el bastion host y la red interna es reducir el numero de máquinas y el número de servicios en esas máquina, que pueden ser atacados desde el bastion host.
- En el router interno deben limitarse los servicios permitidos entre el bastion host y la red interna a solo los que son realmente necesarios.

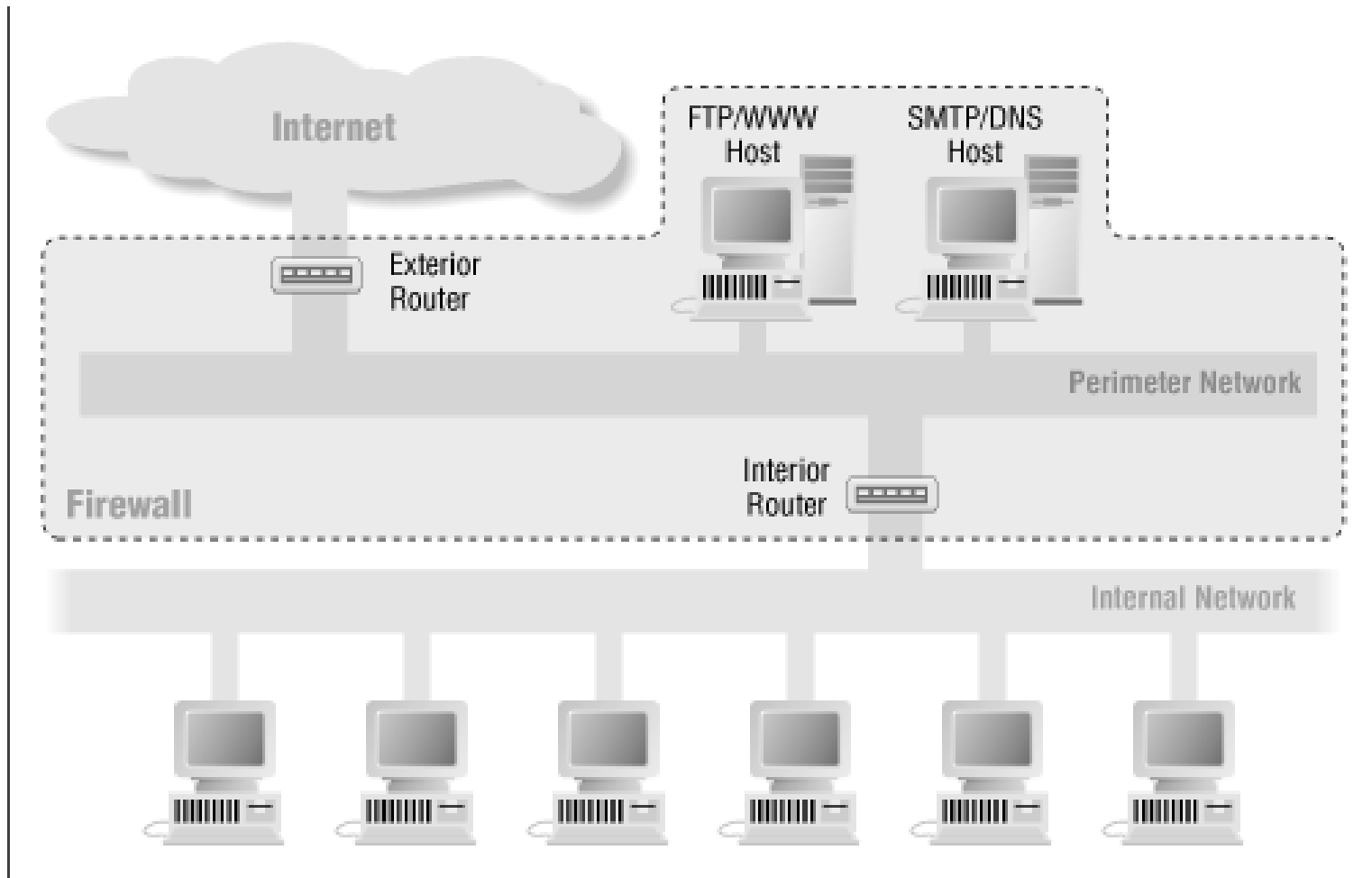
Router exterior

- También llamado access router.
- Protégé a la red perimetral y la red interna de la internet. En la práctica el router exterior tienen a permitir casi cualquier cosa que salga de la red perimetra, y generalmente hacen poco filtrado de paquetes. Las reglas de filtrado de paquetes para proteger las máquinas internas necesitarían ser esencialmente las mismas que en el router interior.
- Las únicas reglas de filtrado de paquetes que son realmente especiales en el router exterior son aquellas que protegen las máquinas en la red perimetral (o sea, al bastion host y al router interno).



Variaciones de Arquitecturas de Firewall

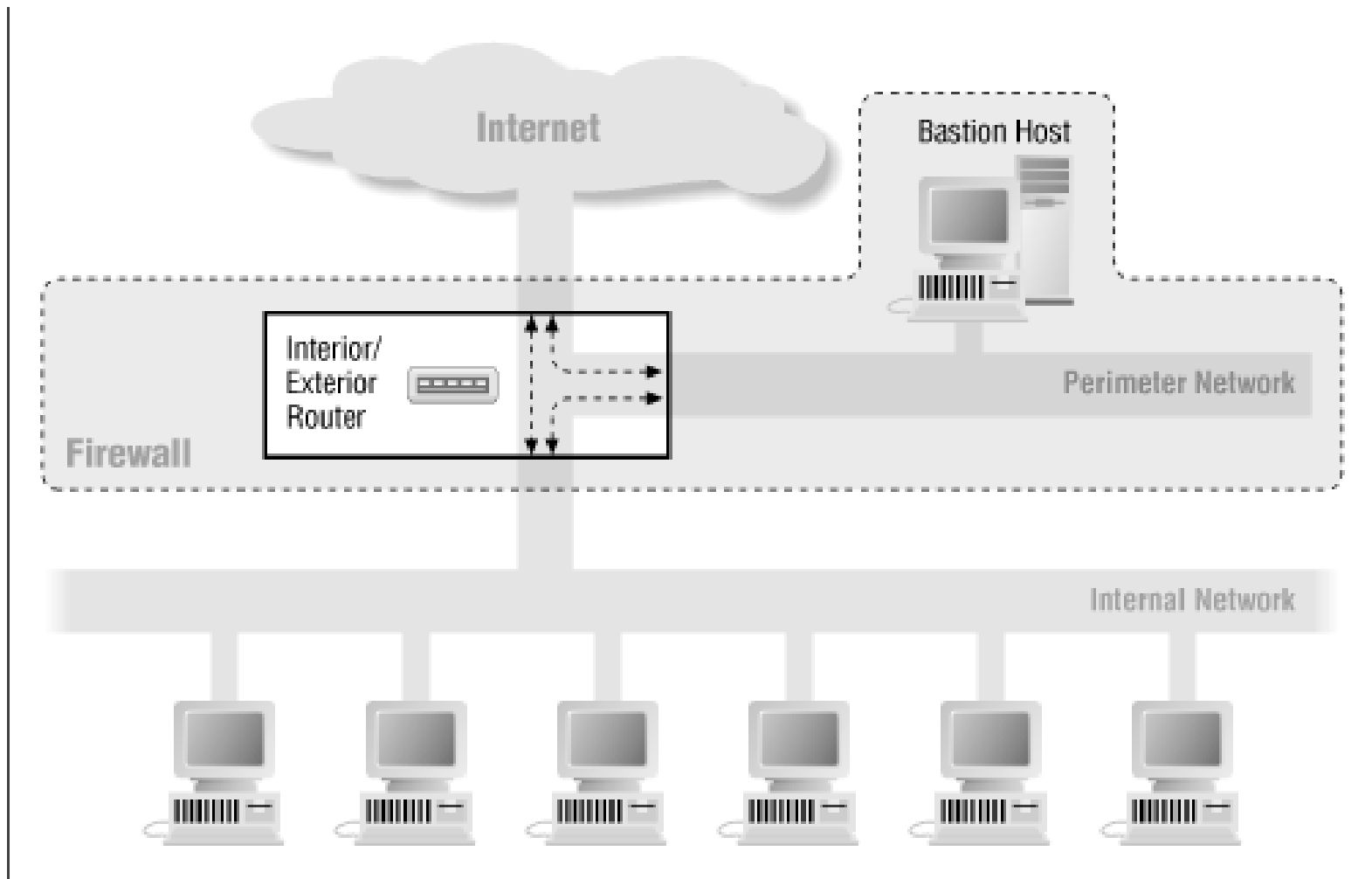
Multiples Bastion Hosts



Multiples Bastion Hosts

- Pueden usarse múltiples bastion hosts en una screened subnet para proveer en cada uno de ellos diferentes servicios.
- Esto también puede mejorar la performance y tener redundancia de servidores

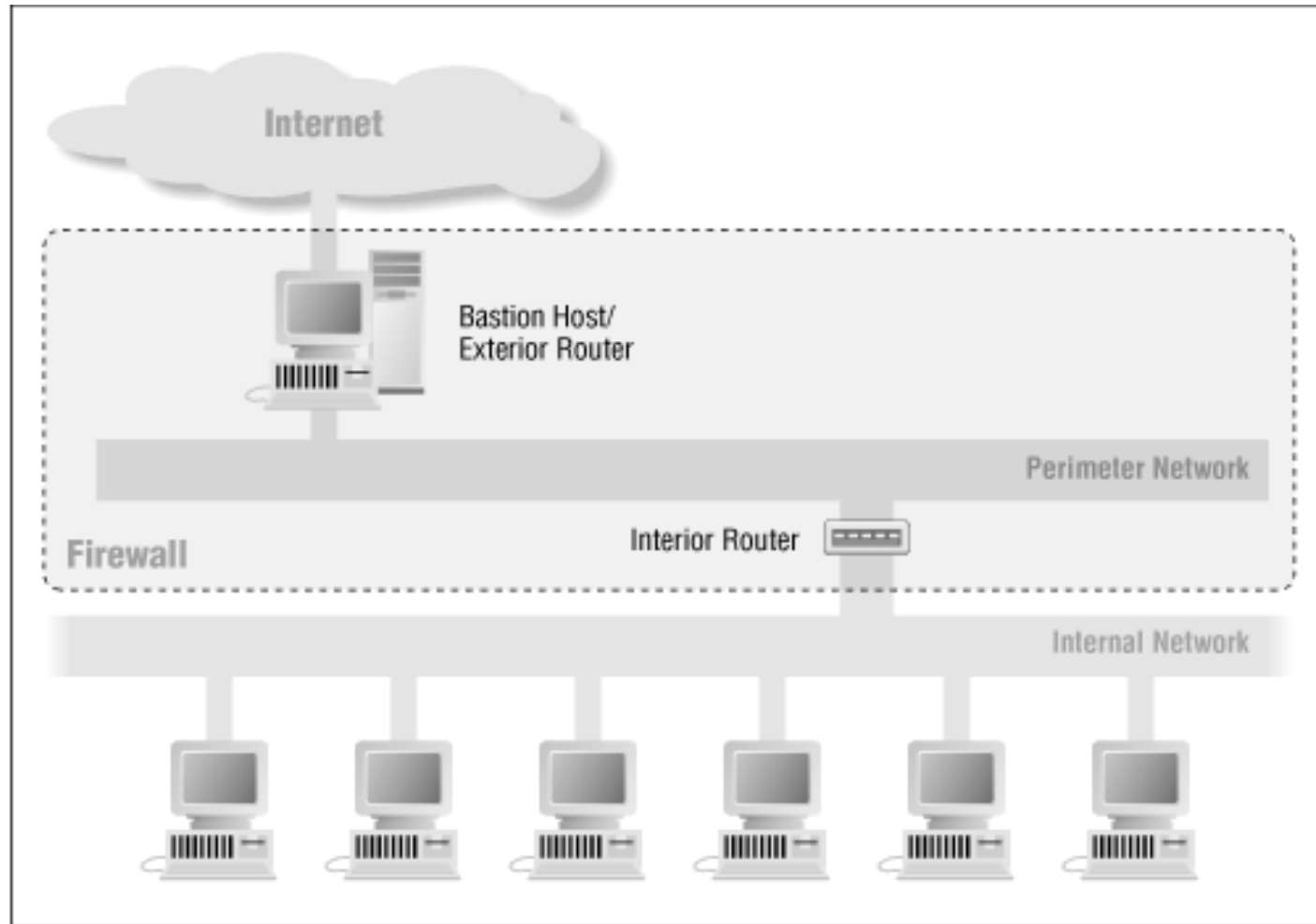
Combinar routers interior y exterior



Combinar routers interior y exterior

- Para hacer esto **es necesario tener un router que permita especificar filtros de entrada y salida para cada interface**
- Tiene la desventaja de que deja al sitio vulnerable si el router se ve comprometido.

Combinar el router exterior y bastion host



Combinar el router exterior y bastion host

- En ocasiones se usa un equipo dual-home como router exterior y bastion host, por ejemplo cuando uno se conecta a internet por medio de dial up con PPP.
- No tiene la flexibilidad y performance de un router dedicado (aunque tampoco se la necesita para una red de tan bajo ancho de banda.
- Si se hace o no packet filtering en este caso está un poco limitado al sistema operativo.
- Esta arquitectura no abre tantas vulnerabilidades como lo hace combinar los routers exterior e interior, si se ve comprometido el router.

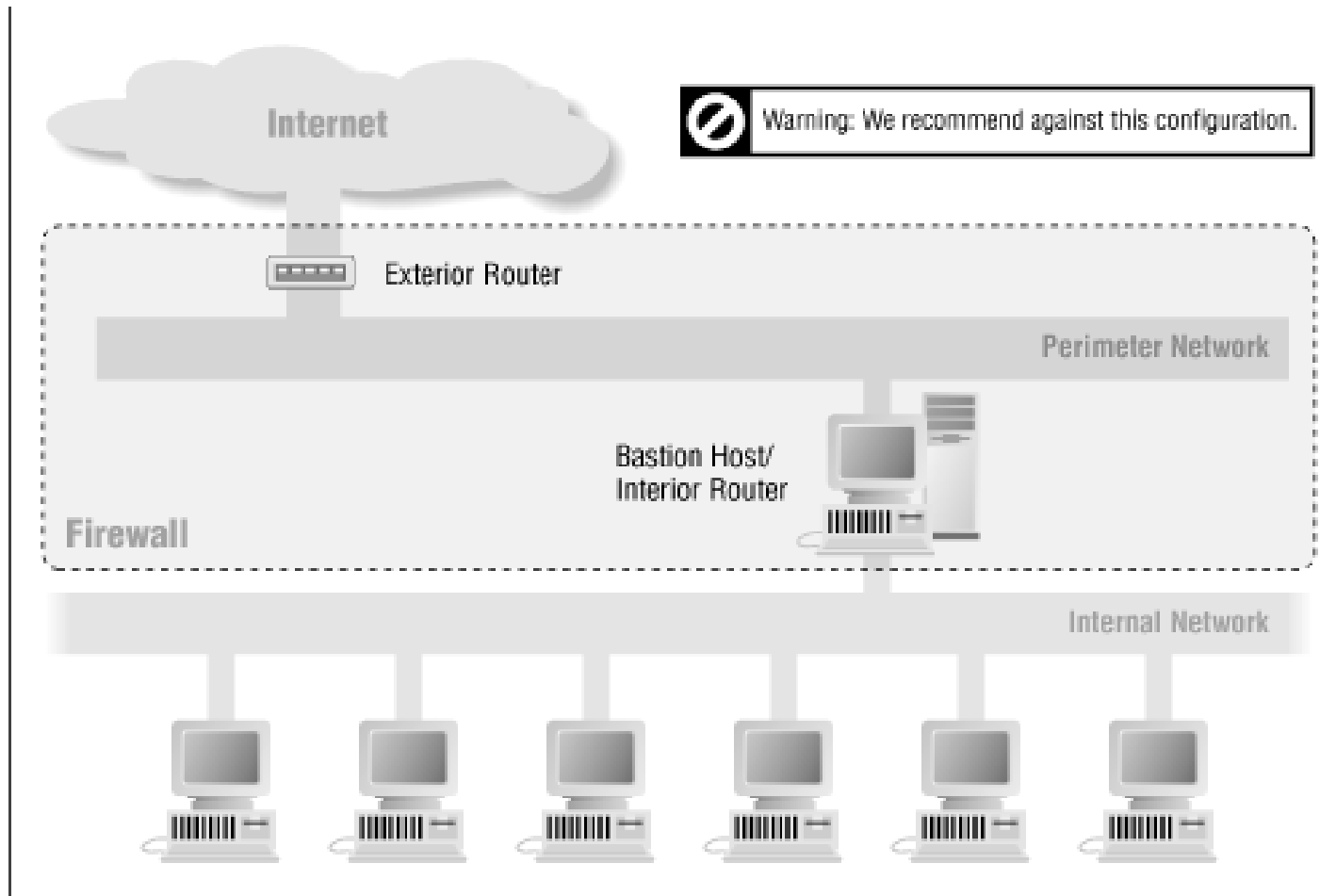
Zona Desmilitarizada (DMZ)

- Es un **host o una red pequeña** insertada como una “**zona neutral**” entre la **red privada de una empresa** y el **mundo exterior**.
- Previene a los usuarios externos obtener acceso directo a los hosts que tienen información privada.
- Puede actuar como firewall y proxy server.
- Los usuarios externos solo pueden acceder a los hosts del DMZ. El DMZ podría también ofrecer servicios para el exterior (Web server por ejemplo)
- No provee acceso a datos privados de la red interna.



Arquitecturas no recomendadas

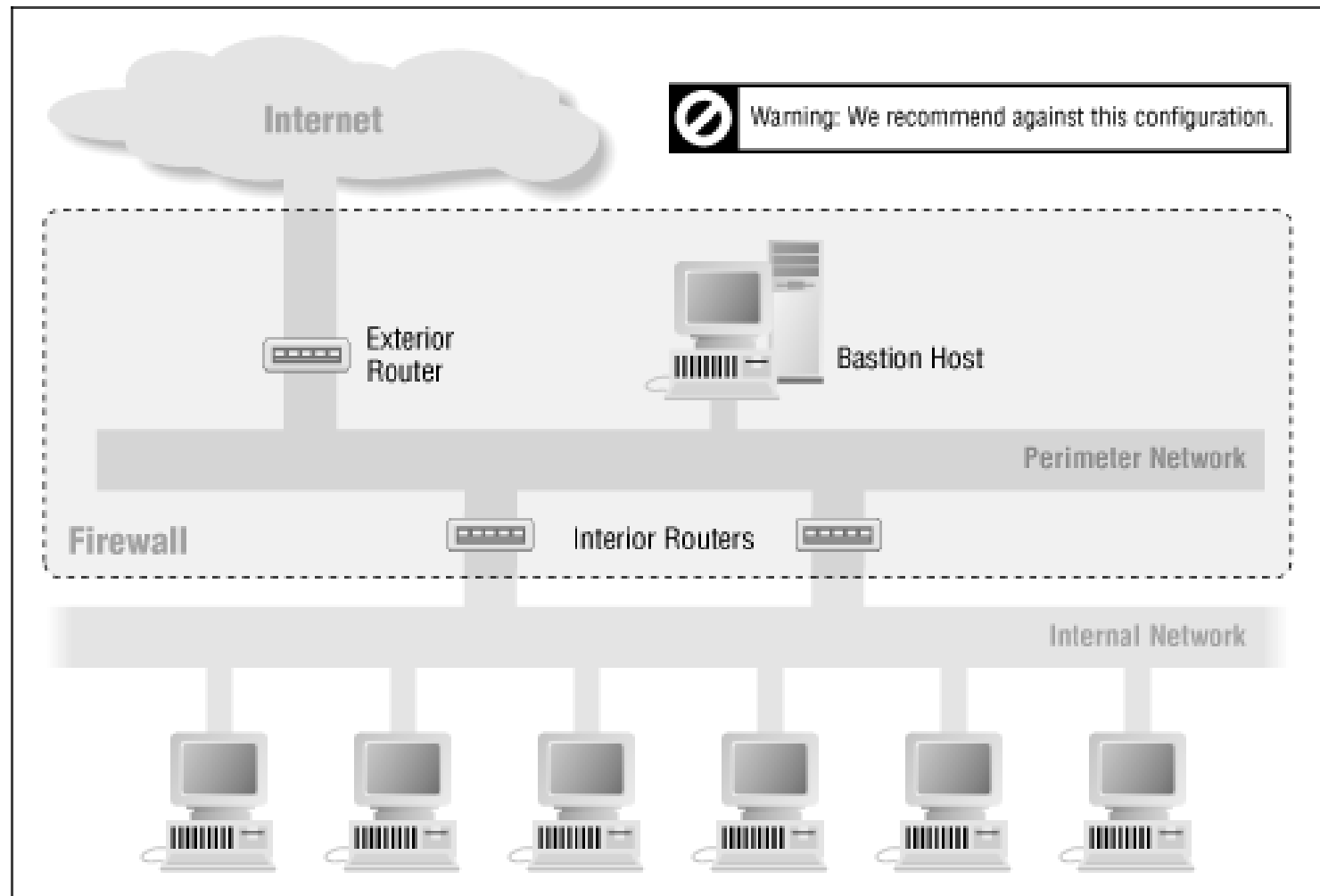
Combining router interior y bastion host



Combinar router interior y bastion host

- El bastion host y el router exterior realizan tareas de protección diferentes; se complementan entre si pero no se respaldan la una a la otra.
- El **router interior en parte funciona como respaldo** de esas dos.
- Si alguien penetra en el bastion host tiene acceso directamente a la red interna

Tener varios routers interiores



Referencias

- ❑ Building Internet Firewalls (O'Really)
<http://docstore.mik.ua/orelly/networking/firewall/index.htm>
- ❑ Firewalls for Dummies (Wiley Publishing Inc.)
- ❑ Web Security: Theory & Applications (School of Software, Sun Yat-sen University)
- ❑ Firewall Architectures (Indonesian Virtual Company)
<http://www.invir.com/int-sec-firearc.html>
- ❑ Handbook of Information Security Management
<https://www.cccure.org/Documents/HISM/ewtoc.html>
- ❑ Firewall Planning and Design
<http://www.csudh.edu/Eyadat/classes/CIS478/handouts/Fall08/Firewall%20Planning.ppt>
- ❑ Principles of Information Security, 2nd Edition