Grupo de Seguridad Informática

Fundamentos de la Seguridad Informática

Seguridad en Redes

Mecanismos de mitigación

Firewalls

Introducción

- Los firewalls son una de las principales herramientas disponibles para mejorar la seguridad de una red
- El termino firewall engloba muchos equipos con distintas características y funciones
- Veremos sus funciones básicas y distintas arquitecturas

Plan

- Utilidad de un firewall
- Funciones de los firewalls
  - Filtrado de paquetes
  - Proxy
  - NAT
  - Log
- Arquitecturas de firewall

¿Qué es un firewall?

- Un equipo o conjunto de equipos que controlan el flujo de tráfico entre dos o más segmentos de la red
- Implementan una política de control de tráfico expresada en su configuración
- Hay diversos tipos (y diversas definiciones)
- Veremos las funciones típicas que cumplen y las arquitecturas en que se usa
- Hablaremos solamente de firewalls para IP

¿Qué puede hacer un firewall?

- Proveer un punto único para un conjunto de decisiones de seguridad
- Hacer cumplir (partes de) una política de seguridad
- Generar logs de uso (y abuso) de la red eficientemente
- Limitar la exposición de servicios y equipos

¿Qué NO puede hacer un firewall?

- Proteger ante tráfico que no pasa por el firewall
  - Por ejemplo, entre equipos internos
- Detener todos los virus
- Detener ataques a través del tráfico permitido
  - Ej. Si permito tráfico web, una página maliciosa podrá atacar los equipos de quien la acceda
- Configurarse solo correctamente : -)

Comercial versus "hecho en casa"

- Sin entrar en guerras religiosas....
- Hay muy buenos productos comerciales
- Hay muy buenos productos libres, open source, etc.
- Dependerá de nuestra empresa el camino a seguir. Nadie obliga a que sea todo o nada....
- Soporte, características (*features*)
- Experiencia de los administradores

Filtrado de paquetes

- Función básica en casi cualquier arquitectura de firewall
- A partir de un conjunto de reglas, se especifica qué paquetes se permite pasar por el firewall
- En su forma más básica, se toman decisiones en función de los datos de los encabezados de capa 3 y 4 (podría también hacerse en función de datos de capa MAC)
- Se puede implementar en enrutadores, equipos unix/linux, equipos especializados

¿Qué se puede filtrar con estos filtros?

- Se puede filtrar por combinaciones de:
  - direcciones de origen y destino
    - Por ejemplo, solo permitir tráfico hacia ciertos servidores, o desde ciertas máquinas hacia afuera
  - Protocolo sobre capa 3 (UDP, TCP, ICMP, otros)
  - Puerto de capa 4 (típicamente los servicios “escuchan” en un puerto determinado (ej. HTTP:80), por lo que puedo permitir acceso a solo un servicio)
  - Interfaz de origen o destino del paquete

Ejemplos

- Rechazar todos los paquetes entrantes en interfaz externa con direcciones de origen internas
- Permitir todo el tráfico desde la subred 192.0.2.0/24 al host 192.168.1.1
- Permitir todo el tráfico al servidor web: permitir tráfico TCP dirigido al puerto 80 de la IP 200.108.192.12
- Negar todo el tráfico UDP a puertos menores a 1024
- Permitir todo el tráfico DNS
- Negar todo el resto

Filtros de paquetes con estado

- El filtrado sin estado es poco flexible
  - ¿cómo expresar, por ejemplo, “dejar pasar los paquetes de regreso de una conexión establecida desde el interior”?
- Los filtros con estado (stateful packet filters) permiten exactamente eso: pueden guardar estado dependiendo del tráfico pasado
- Por ejemplo, entienden la secuencia de banderas SYN, SYN+ACK, ACK necesarios para el establecimiento de conexiones TCP

Filtros de paquetes con estado

- Conociendo el estado de una conexión (establecida, cerrada, syn-sent, etc), se pueden tomar decisiones más complejas
- También pueden permitir tráfico relacionado con conexiones existentes (ej. conexión de datos asociada a una sesión de control ftp, ver filtros capas superiores)
- Aún en caso de protocolos sin estado (UDP), se genera una “pseudo conexión” para permitir el pasaje de los paquetes de respuesta

Filtros de capas superiores

- Permiten filtrar utilizando información sobre el protocolo de aplicación
- Por ejemplo, solo permitir al puerto 53/UDP paquetes que tengan el formato correcto para ser una consulta DNS
- Pueden realizar chequeos de correcto formato de las solicitudes
- Pueden relacionar varios flujos (por ejemplo permitir conexiones asociadas a un protocolo)

Generando reglas de filtrado

- Debemos identificar los servicios en cada zona a los cuales permitiremos acceso, y desde donde
  - Ejemplo: aceptar correo electrónico desde cualquier lado al servidor 192.168.2.2
- Traducirlo a reglas sobre los paquetes
  - Permitir conexiones al puerto 25/TCP de la IP 10.168.2.2
  - Permitir paquetes relacionados con la regla anterior
- Identificar flujos asociados y generar reglas
  - Ejemplo: servicio ident, conviene retornar “icmp unreachable”

¿Default permit o default deny?

- ¿Qué sucede con los paquetes que no son clasificados?
  - Default permit: los dejo pasar
  - Default deny: los descarto
- Default permit nos obliga a saber qué queremos filtrar. Siempre nos vamos a olvidar de algo
- Default deny nos asegura que ningún tráfico no permitido explícitamente **NO** pasará por los filtros

¿Filtramos las conexiones salientes?

- Una política “default permit” en el tráfico saliente es más “amigable”
- Los usuarios de la red pueden conectarse a servicios potencialmente maliciosos
- Trojanos/virus....
- Ataques desde nuestras máquinas hacia afuera
- Salida de datos internos restringidos...
- Una política “default deny” es más segura

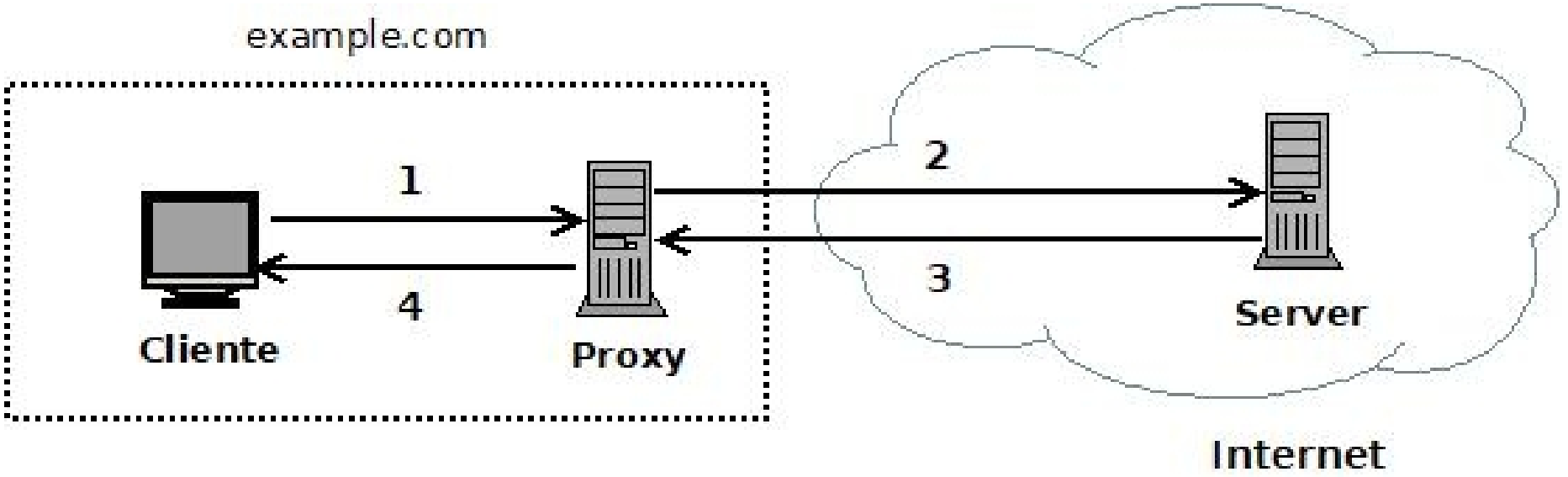
Capacidades de log

- Es importante que el/los sistemas utilizados como firewall tengan capacidad de log
  - Los logs nos pueden dar información de cómo sucedió un ataque
- Es conveniente que el log se guarde en un equipo separado
  - Por si el firewall es comprometido
- Es importante procesar esos logs !!

Servicios proxy

- Proxy se puede traducir como “apoderado”
- Un servicio de proxy se encarga de realizar consultas a nombre de otro equipo
- Por ejemplo, si tenemos un proxy http y los equipos de escritorio se configuran para utilizarlo, cuando quiero ver la página http://www.google.com/, en realidad me conecto al proxy, y este se conecta con google
- En el proxy se pueden hacer chequeos de seguridad, filtrar, etc.

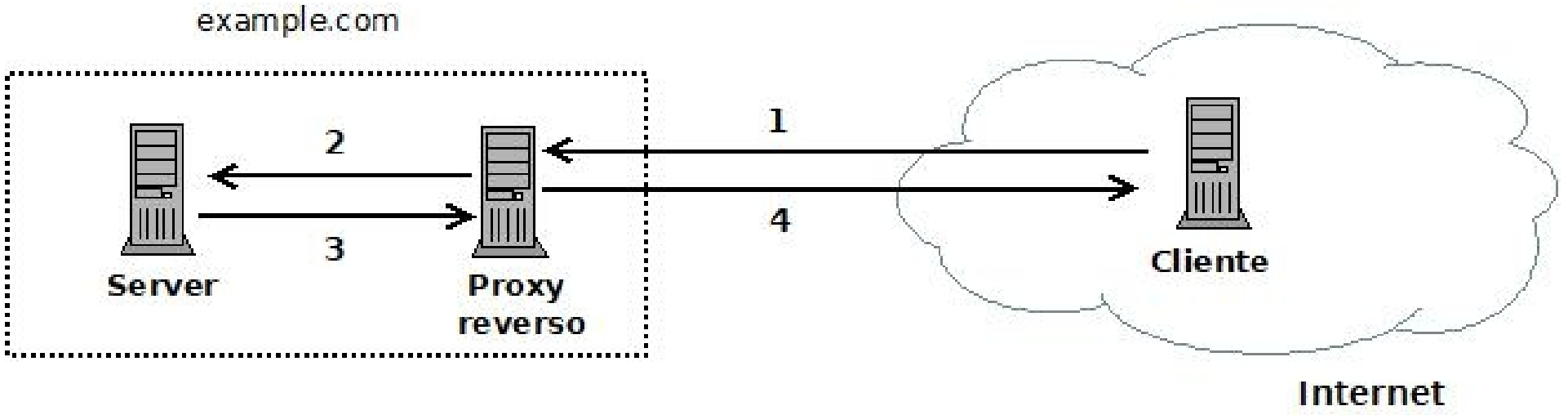
Proxy



Cómo se usa un proxy

- Aplicaciones “proxy aware” (ej. Navegadores)
- Sistemas operativos “proxy aware” (redirigiendo automáticamente los pedidos al proxy)
- Procedimientos de los usuarios
- Proxy transparente. Los paquetes del cliente son interceptados y redirigidos al proxy
- Los servicios que funcionan en modo “store and forward” funcionan naturalmente como proxy (ej. SMTP, NNTP, NTP)

Proxy Reverso



Proxy Reverso

- Interviene en las conexiones al servidor de clientes “externos”
- El principal objetivo es proteger al servidor de los clientes “externos”
- El ejemplo más conocido es el Web Application Firewall (WAF) (Apache + mod-security)
- Podemos implementarlo para otros servidores (SMTP, IMAP, POP, SSH, etc)

Bastion hosts

- Típicamente para proveer servicios a clientes externos
  - Servidores web, servidores de correo, etc.
- Se encuentran expuestos a Internet
- Deben ser asegurados cuidadosamente
- Principio KISS (keep it simple, s.....). Debe brindar el mínimo número de servicios
- Estar preparados para la eventualidad que sean comprometidos

Bastion hosts

- Idealmente estarán en un segmento aparte de la red
- Se debe filtrar el tráfico externo hacia el bastión, y también desde el bastión al resto de las redes
- Ejemplos de servicios:
  - SMTP, HTTP, FTP, NNTP, DNS

Network Address Translation

- Muchas veces la función de NAT está incluida en los productos de firewall
- La idea de NAT es traducir un conjunto de direcciones (típicamente privadas) a una o pocas direcciones públicas
- Para ello se mantienen tablas de correspondencia (IPprivada, Puertoprivado)-> (IPpublica, Puertopublico)
- Presenta como ventaja de seguridad, que no es posible establecer conexiones desde el lado público (a menos que estén explícitamente mapeadas)

Arquitecturas de firewall

- Un solo equipo
  - Enrutador con filtros
  - Hosts “dual homed”
  - Equipos de firewall multipropósito (filtros +proxy)
- Arquitecturas con múltiples equipos
  - Screened host
  - Screened subnet

Enrutador con filtros Firewall Multipropósito

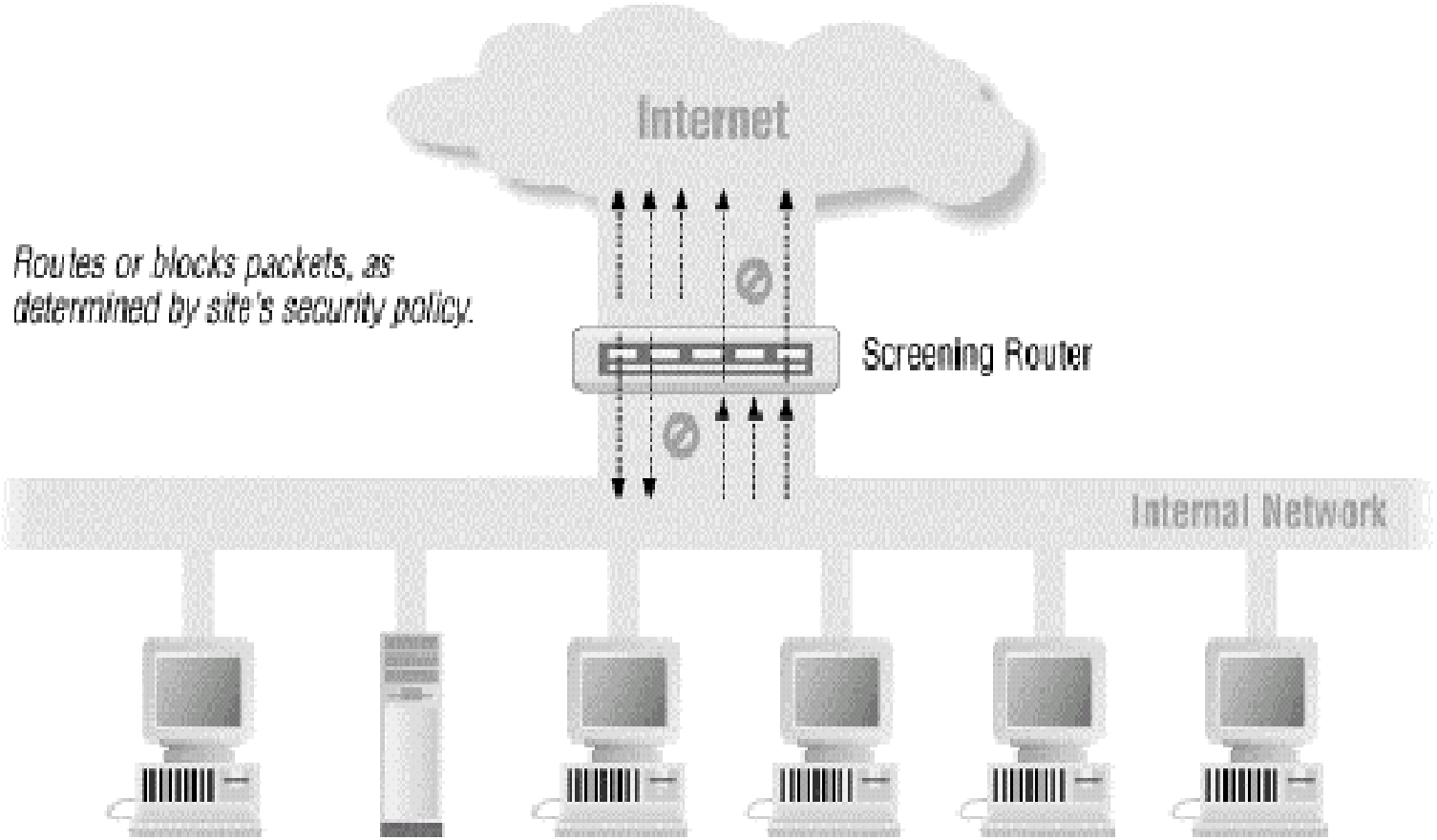


Figura 6.1. Building Internet Firewalls (2nd. Ed)

Host “dual homed”

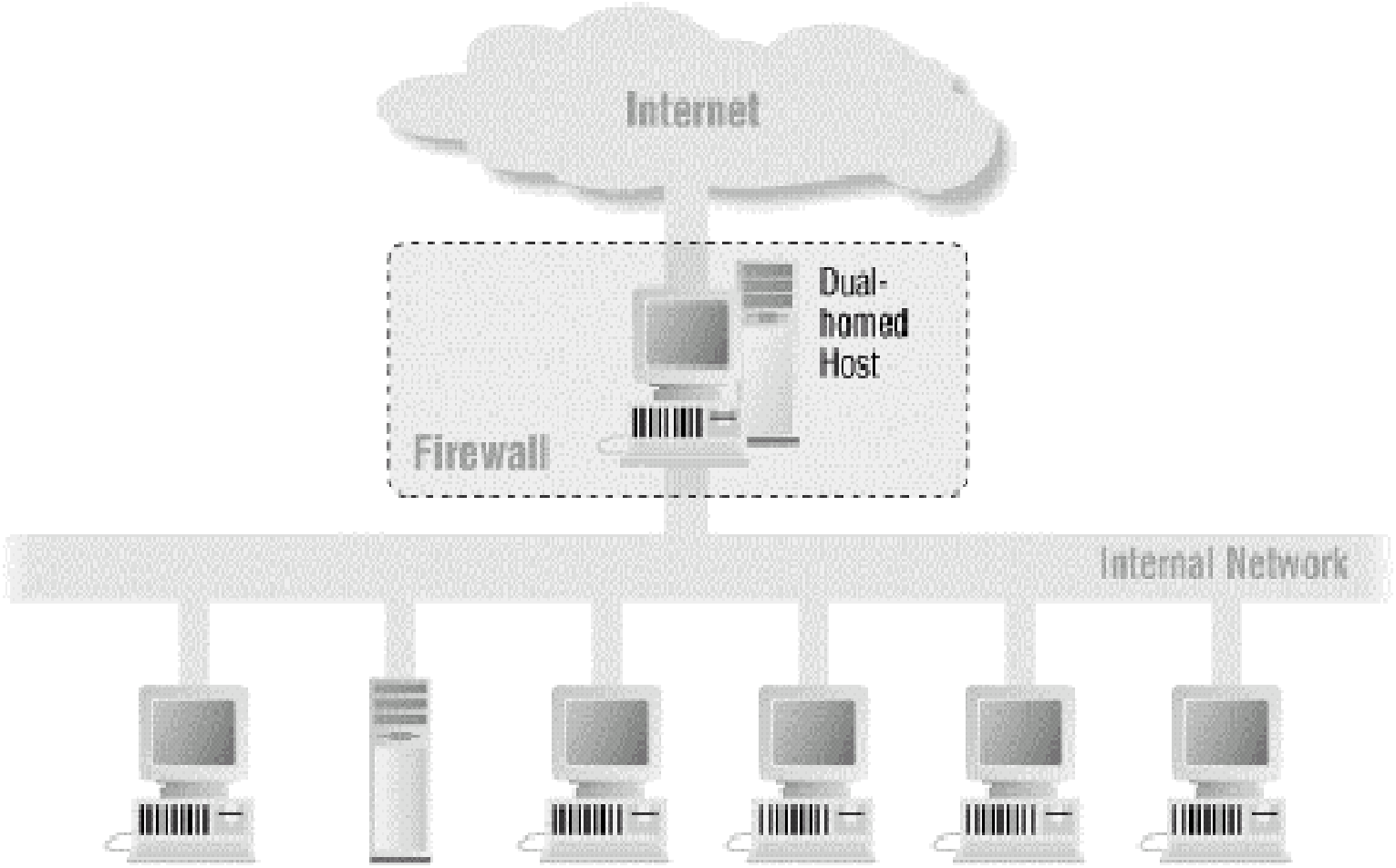


Figura 6.2. Building Internet Firewalls (2nd. Ed)

Screened Host

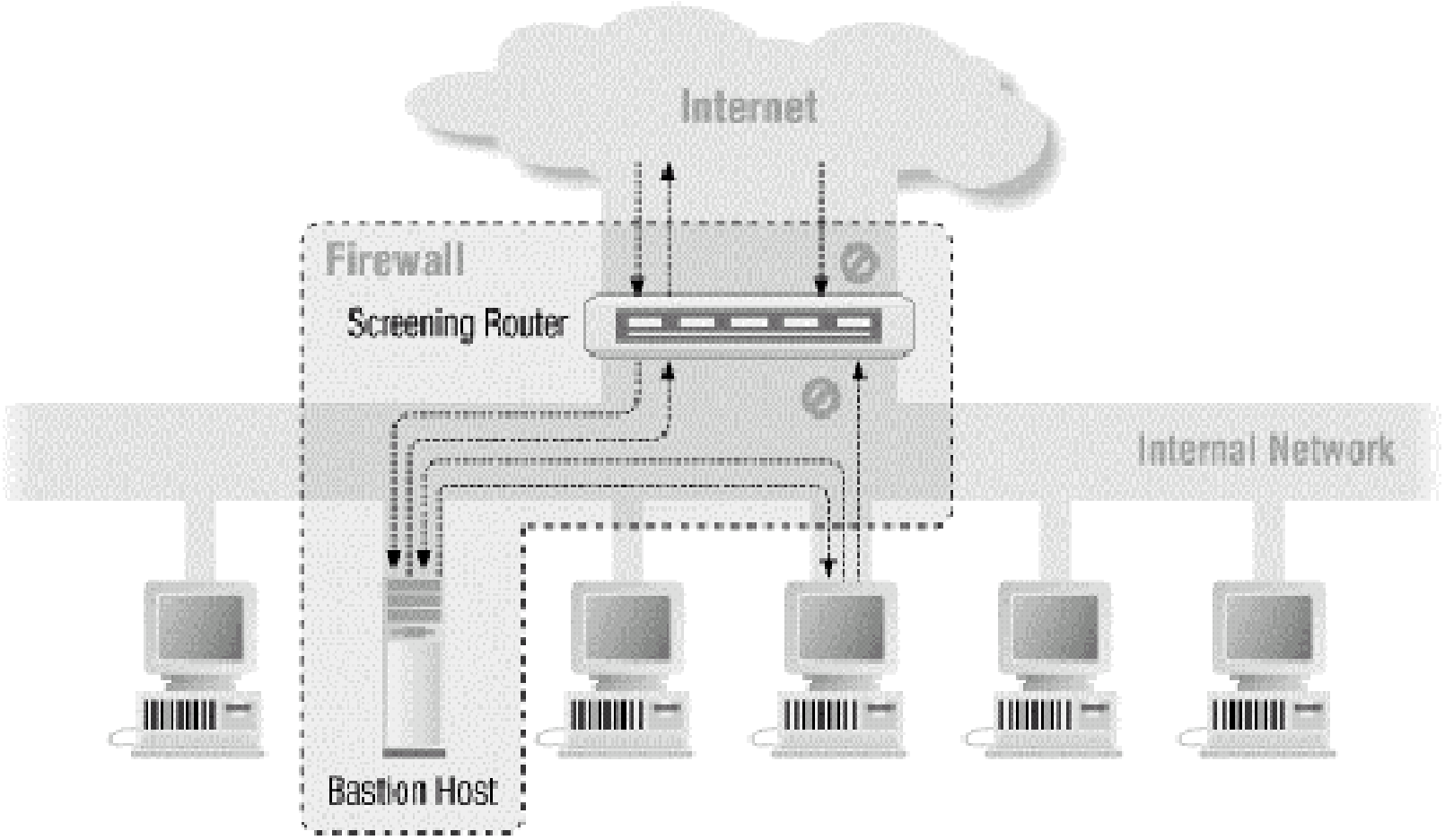


Figura 6.3. Building Internet Firewalls (2nd. Ed)

Screened Subnet

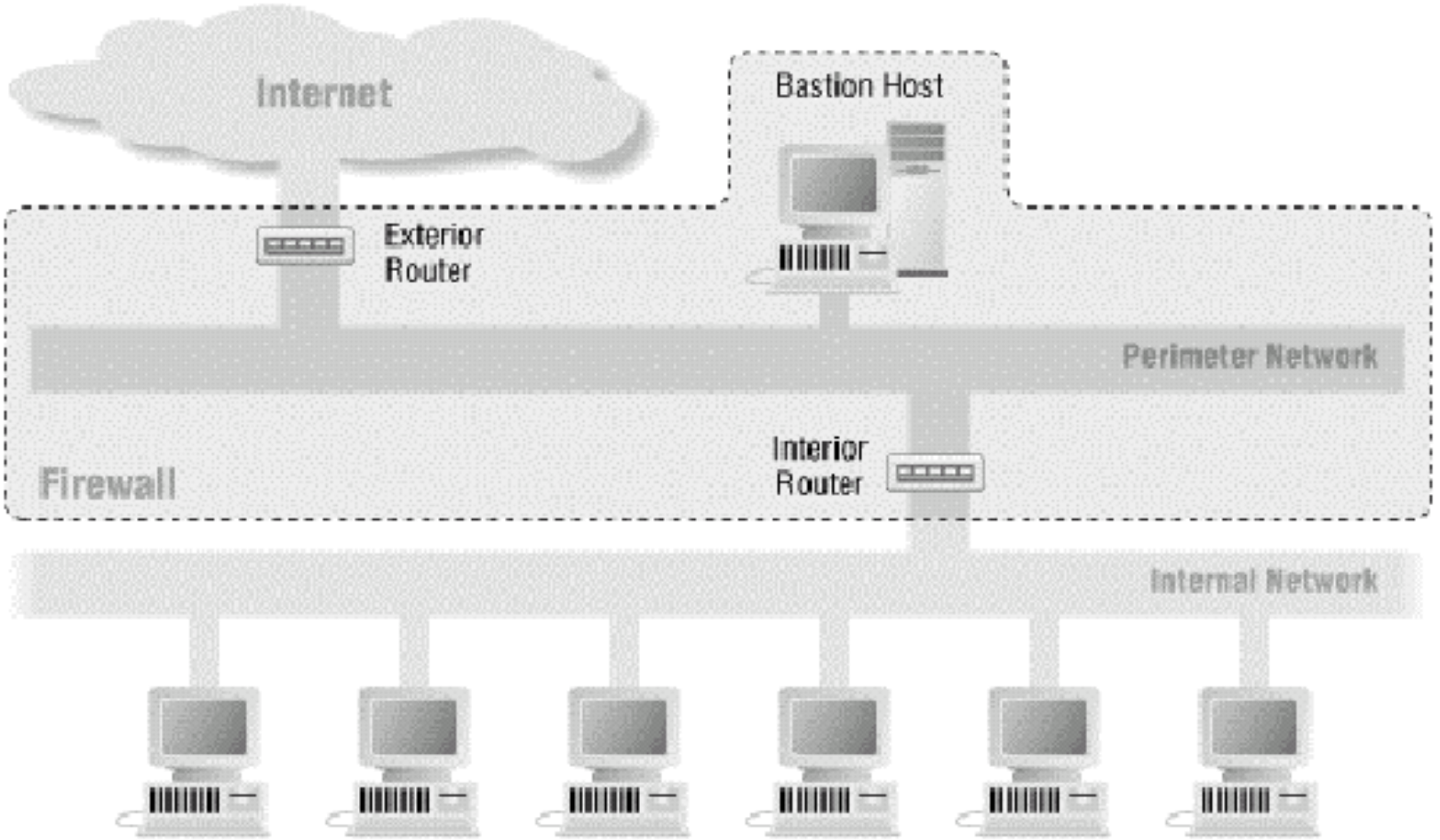


Figura 6.4. Building Internet Firewalls (2nd. Ed)

Variaciones

- Claramente, se pueden realizar muchas variaciones con estas ideas
- Puede, por ejemplo, unificarse el enrutador exterior con el interior
- A la red perímetro se le suele llamar DMZ (Demilitarized Zone)
- Puede haber más zonas. Por ejemplo, para separar los servicios de la DMZ. O para proteger algunas subredes dentro de la empresa

Firewalls internos

- Muchas veces los riesgos vienen de dentro de la empresa
  - Proteger los activos críticos del común de los empleados
  - Proteger la facultad de las redes con máquinas de estudiantes
  - Proteger la red interna de la red experimental
  - Proteger equipos trabajando en proyectos secretos
  - Separar las redes de acceso wireless

Firewalls “Personales”

- Firewalls software, que se instalan en las propias estaciones de trabajo
- Muchos sistemas operativos los traen incluídos
  - La mayoría de los UNIX
  - Windows XP SP2
- En una empresa pueden servir como una segunda barrera, para evitar ataques internos
- En los hogares son importantes ya que son típicamente la única línea de defensa

Bibliografía y referencias

- **D. Gollman**, *Computer Security*, Wiley, 2006.
- **E Zwicky, S. Cooper, and B. Chapman**. *Building Internet Firewalls. 2nd. Ed*. O'Reilly Press 2001