

# *Criptografía y Seguridad de Datos*

## **Protección de redes: Cortafuegos**

Carlos Figueira.

Universidad Simón Bolívar

*Basado en láminas del Profesor*

*Henric Johnson (<http://www.its.bth.se/staff/hjo/>*

*henric.johnson@bth.se)*

# Contenido

- Principios de Diseño de Cortafuegos (*Firewall*)
  - Características
  - Tipos de cortafuegos
  - Configuraciones

# Cortafuegos

- Medios efectivos para proteger sistemas y redes locales de ataques a la seguridad a través de la red, garantizando acceso controlado desde el exterior a través de Internet o Red de Área Ancha

# Contexto usual

- Los sistemas de información evolucionan, desde pequeñas redes locales a conectividad a Internet
- No se establecen medidas de seguridad sólidas para las estaciones de trabajo y los servidores

# Principios de Diseño

- El cortafuego se inserta entre la red interna (*Intranet*) e Internet
- Objetivos:
  - Establecer un enlace controlado
  - Proteger la red interna de ataques desde Internet
  - Proveer un punto estratégico (único) de defensa

# Características

- Metas de diseño:
  - Todo tráfico desde/hacia la Intranet debe pasar por cortafuegos, bloqueando físicamente todo acceso a la red interna excepto a través del cortafuego
  - Sólo se permite el paso del tráfico autorizado (definido por las políticas de seguridad locales)

# Características

- Metas de diseño:
  - El cortafuego mismo es inmune a penetraciones
  - Puede hacer uso de *sistemas confiables* con un sistema de operación confiable

# Características

- 4 técnicas generales, basadas en control de:
  - servicios,
  - dirección,
  - usuario
  - comportamiento

# Características

- Control de Servicios
  - Determina los tipos de servicios de la institución que pueden ser accedidos desde Internet (e incluso desde la Intranet)
- Control de Dirección
  - Determina dirección en que se permite flujo de solicitudes de servicios

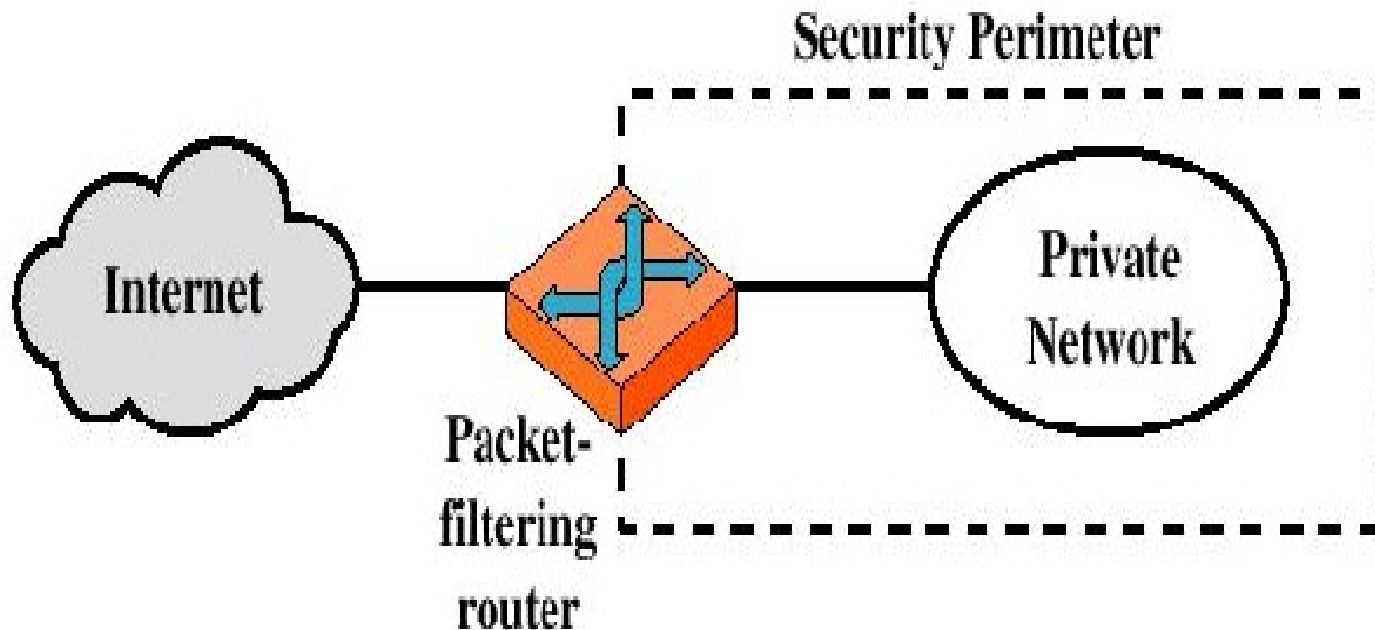
# Características

- Control de Usuario
  - Controla acceso a un servicio según quien trata de accederlo
- Control de Comportamiento
  - Controla como se usan algunos servicios particulares (p.e. Filtro de correo electrónico)

# Tipos de Cortafuegos

- Enrutadores (*routers*) de filtrado de paquetes
- Pasarelas (*gateways*) a nivel de aplicación
- Pasarelas a nivel de circuito
- Bastiones

# Enrutador de filtro de paquetes



# Enrutador de filtro de paquetes

- Aplica un conjunto de reglas a cada paquete IP entrante, el cual es encaminado o descartado
- Filtra paquetes en ambas direcciones
- Típicamente se establece como una lista de reglas basadas en correspondencia de patrones en los encabezados IP o TCP
- **Dos políticas por defecto:** descartar o encaminar

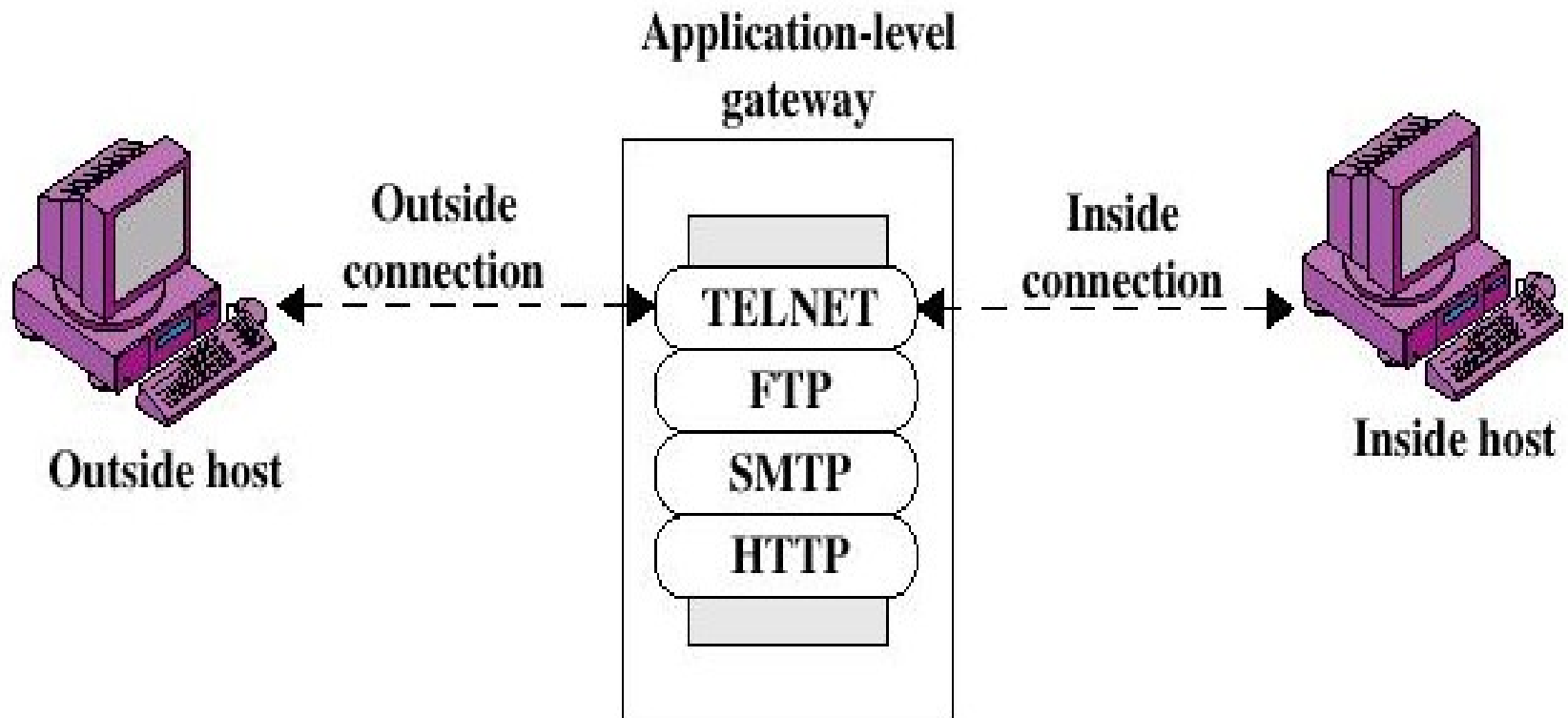
# Enrutador de filtro de paquetes

- Ventajas:
  - Simplicidad
  - Transparencia para usuarios
  - Alta velocidad
- Desventajas:
  - Dificultad para crear reglas
  - Falta de Autenticación

# Enrutador de filtro de paquetes

- Posibles ataques
  - Suplantar direcciones IP (por una IP interna)
  - Ataques de encaminamiento de fuente
  - Ataques de pequeños fragmentos

# Pasarelas a nivel de aplicación



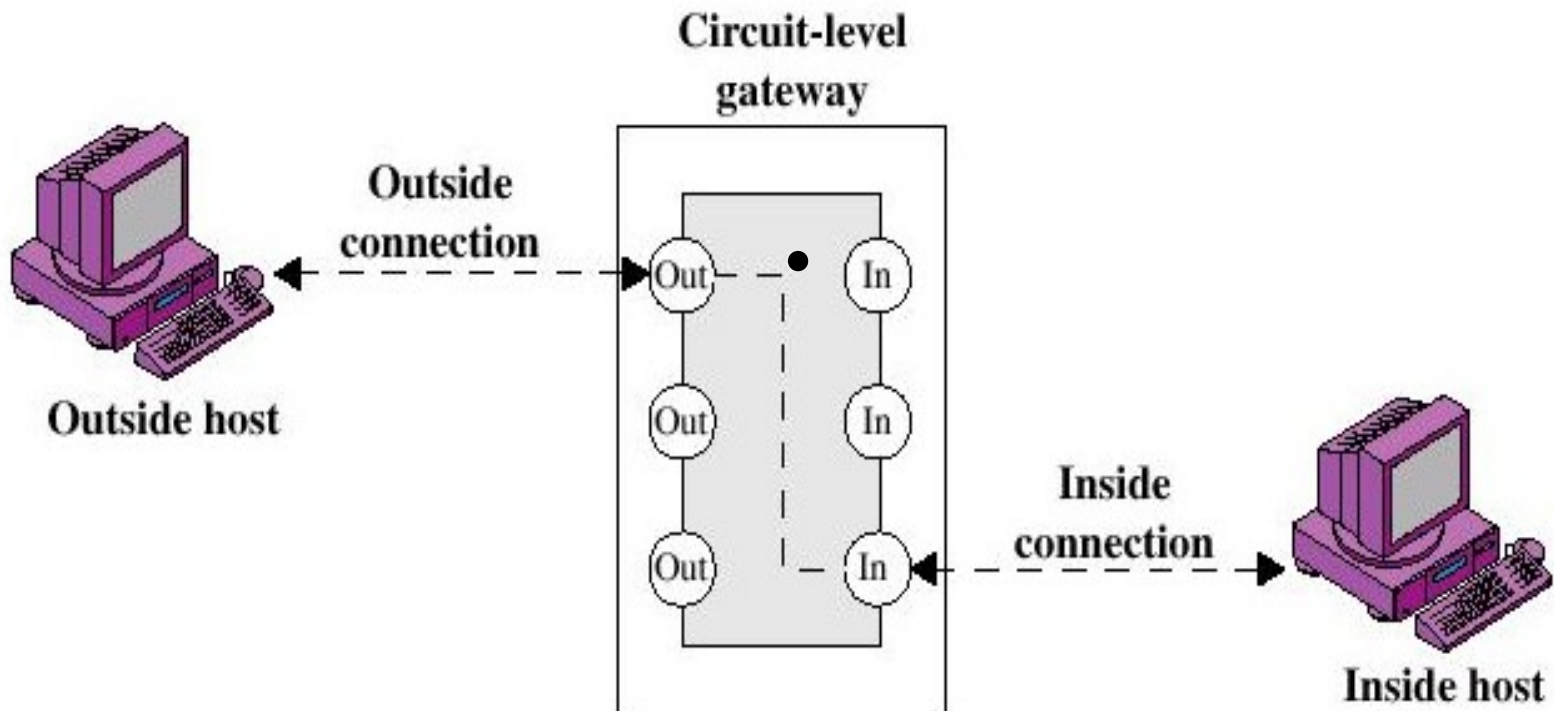
# Pasarelas a nivel de aplicación

- También llamada *proxy server*
- Funciona como un relevo (*pivot*) del tráfico a nivel de aplicación

# Pasarelas a nivel de aplicación

- Ventajas:
  - Más seguro que filtro de paquetes
  - Sólo revisa unas pocas aplicaciones permitidas
  - Fácil de llevar registros y se audita todo el tráfico entrante
- Desventajas:
  - Sobrecarga de procesamiento en cada conexión

# Pasarela a nivel de circuito



# Pasarela a nivel de circuito

- Sistemas dedicados o Funciones especializadas realizadas por una pasarela a nivel de aplicación
- Establece dos conexiones TCP
- La pasarela típicamente reenvía segmentos TCP de una conexión a otra sin examinar los contenidos

# Pasarela a nivel de circuito

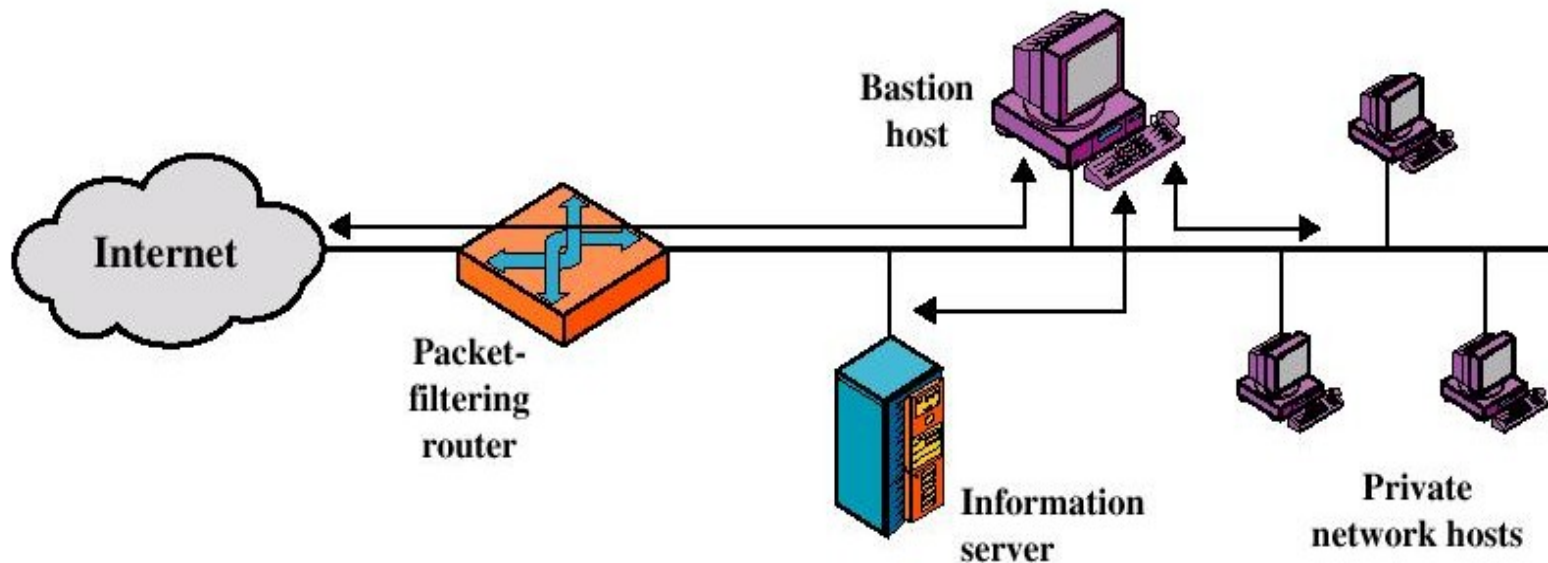
- La función de seguridad consiste en determinar las conexiones que serán permitidas
- Se usa típicamente cuando el administrador confía en los usuarios internos
- Un ejemplo es el paquete SOCKS

# Bastión

- Sistema identificado por el cortafuegos como un punto crítico fuerte en la seguridad de la red
- El anfitrión bastión sirve como una plataforma de pasarela a nivel de aplicación y a nivel de circuito
- Se le aplica *hardening*

# Configuraciones de Cortafuegos I

- Sistema cortafuego con bastión conectado a una sola red



# Configuraciones de Cortafuegos I (cont.)

- Cortafuego es una máquina robusta de protección (bastión), conectada a una sola red
- Cortafuego consiste de dos sistemas:
  - Un enrutador que filtra paquetes
  - Un bastión

# Configuraciones de Cortafuegos I (cont.)

- Configuración del enrutador que filtra paquetes:
  - Sólo se permite el paso de paquetes desde y hacia el bastión
- El bastión realiza autenticación y funciones de intermediario (*proxy*)

# Configuraciones de Cortafuegos I (cont.)

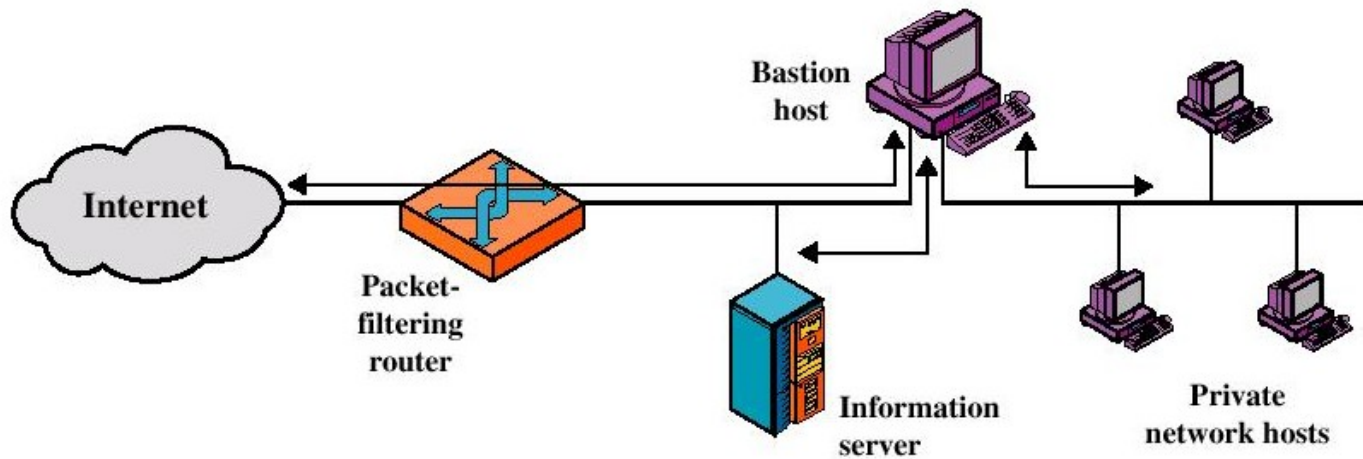
- Mayor seguridad que las configuraciones simples debido a que:
  - Implementa filtros de paquete y de nivel de aplicación, simultáneamente, permitiendo flexibilidad al definir las políticas de seguridad
  - El intruso debe generalmente penetrar dos sistemas separados

# Configuraciones de Cortafuegos I (cont.)

- Esta configuración también provee flexibilidad, al ofrecer acceso directo a Internet (p.e., un servidor Web)

# Configuraciones de Cortafuegos II

- Sistema de bastión conectado a dos redes

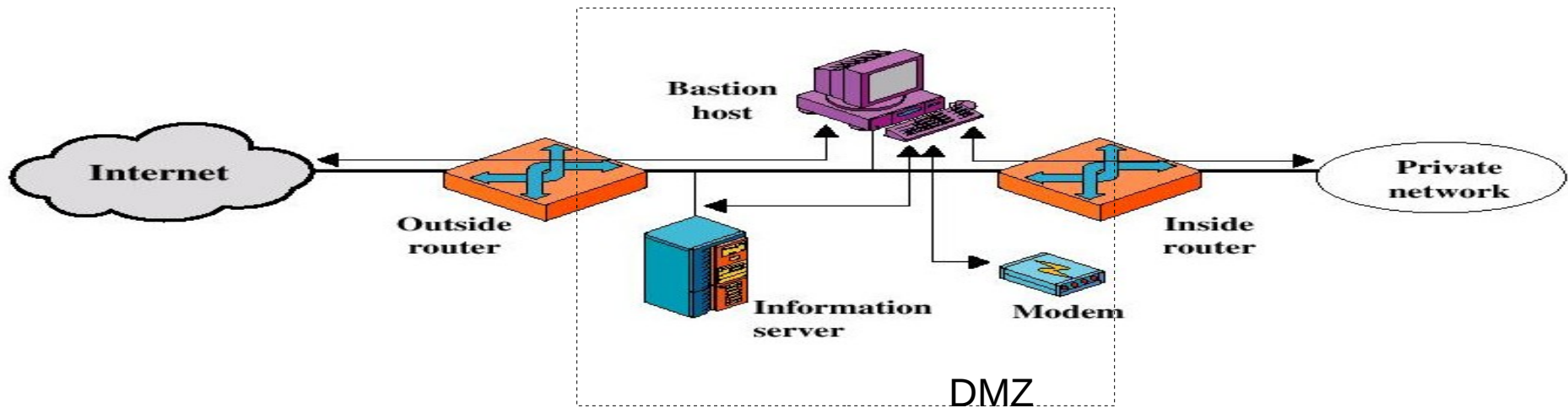


# Configuraciones de Cortafuegos II (cont.)

- El enrutador que filtra paquetes no compromete a la red
- El tráfico entre Internet y las máquinas de la red privada tiene que fluir a través del bastión

# Configuraciones de Cortafuegos III

- Sistema cortafuegos con bastión entre dos filtros de paquetes



# Configuraciones de Cortafuegos III (cont.)

- La más segura de las tres
- Se usan dos enrutadores filtro de paquetes
- Creación de una red aislada (Intranet) y una “Zona desmilitarizada” (DMZ)

# Configuraciones de Cortafuegos III (cont.)

- Ventajas:
  - Tres niveles de defensa contra intrusos
  - El enrutador externo publica en Internet sólo la existencia de la subred monitoreada (la red interna es invisible a Internet)

# Configuraciones de Cortafuegos II (cont.)

- Ventajas:
  - El enrutador interno publica sólo la existencia de la subred monitoreada a la red interna (los sistemas en la red interna no pueden construir rutas directas a Internet)