Universidad de Oviedo

Departamento de Informática

Campus de Gijón

Cortafuegos

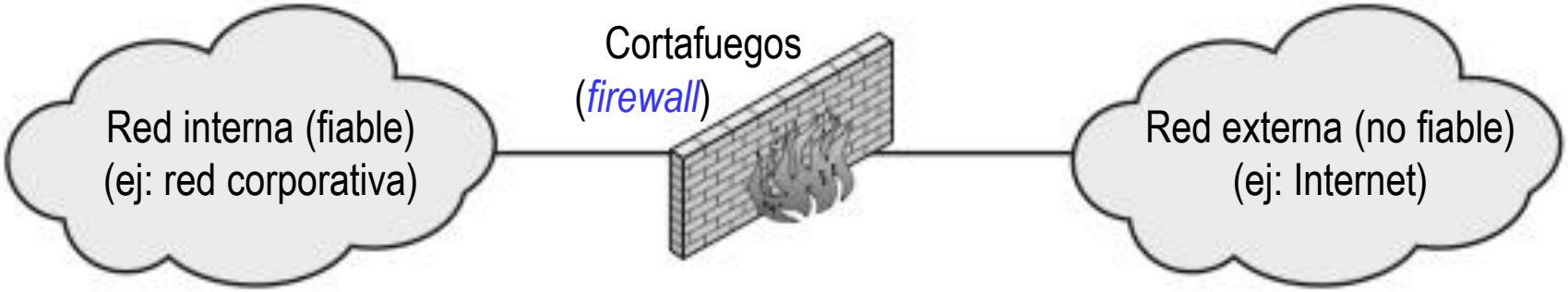
Presentación

Daniel F. García

Concepto de cortafuegos

Definición típica

Un cortafuegos (*firewall*) es un elemento de control ubicado entre la red local corporativa e Internet



Un cortafuegos es un buen elemento para:

- Consolidar mecanismos de seguridad
- Implementar alarmas y monitorizar los eventos
- Implementar Redes Privadas Virtuales (VPN) basadas en IPsec

Limitaciones de los cortafuegos

- **No pueden proteger de los ataques que eluden a los cortafuegos**
  Ej: PCs con módems que permiten acceder directamente a un ISP (*Internet Service Provider*)

- **No pueden proteger contra amenazas internas**
  Ej: Empleados descontentos o que cooperan con un atacante

- **No pueden proteger contra accesos vía WLAN**
  Ej: Una red inalámbrica insegura permite el acceso desde/hacia el exterior

- **No pueden proteger contra malware importado en la red interna**
  Ej: Laptops, PDAs, memorias USBs, pueden infectarse fuera y usarse luego en la red interna

- **No pueden proteger contra la transferencia de archivos infectados**
  Ej: Debido a la gran cantidad de aplicaciones y sistemas dentro del perímetro puede ser imposible para un cortafuegos escanear todos los archivos recibidos

Tipos de Cortafuegos

Tipos de cortafuegos (según el modo de funcionamiento)

- Filtros de paquetes
- Filtros de paquetes con inspección de estados
- Pasarela (*gateway*) a nivel de aplicación == Proxy de aplicación
- Pasarela (*gateway*) a nivel de circuito

Tipos de cortafuegos (según la ubicación ≈ lo que protegen)

- Hosts bastión
- Cortafuegos basados en host
- Cortafuegos personales

Filtros de paquetes 1

Estos cortafuegos son routers que filtran paquetes a nivel de red = capa IP de red

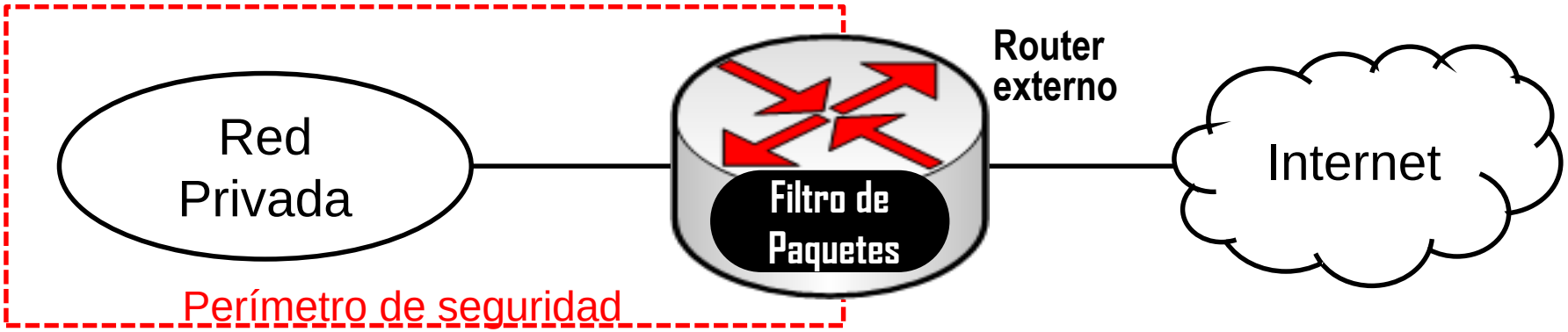
Un router de filtrado de paquetes aplica un conjunto de reglas a cada paquete IP entrante o saliente para reenviar o descartar el paquete

Las reglas de filtrado se basan en información contenida en la cabecera del paquete:

- Direcciones IP de origen y destino
- Puertos TCP o UDP de origen y destino
- Interfaces (bocas) del router de origen y destino

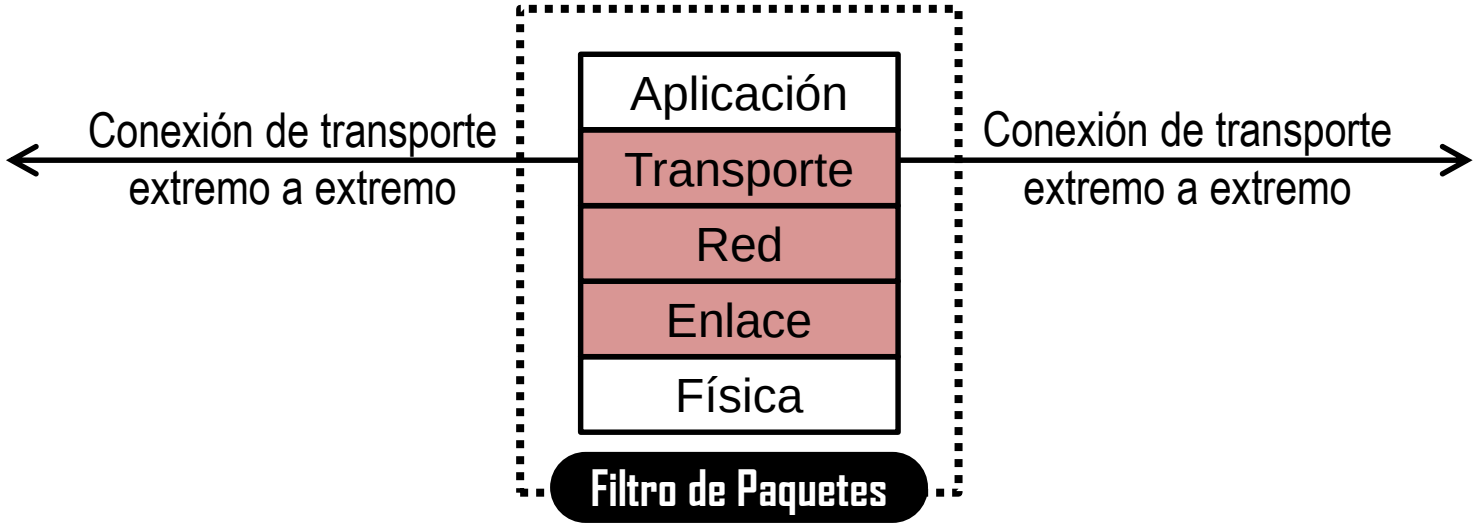
El filtro de paquetes se suele implementar en el router externo de una organización

Con el objetivo de establecer un perímetro de seguridad para la organización



Filtros de paquetes 2

Los Filtros de Paquetes funcionan en los siguientes niveles de una red:



Cuando no se puede aplicar ninguna regla a un paquete hay aplicar una **acción por defecto**

Defecto = DESCARTAR ← → Lo que no está expresamente permitido está prohibido

Defecto = REENVIAR ← → Lo que no está expresamente prohibido está permitido

Filtros de paquetes 3: ventajas y debilidades

Ventajas

1. Son muy rápidos
2. Son transparentes para las aplicaciones
3. Son escalables

Debilidades

1. No pueden prevenir ataques que explotan vulnerabilidades de las aplicaciones
2. Las funcionalidades de sus registros son limitadas
3. No soportan mecanismos sofisticados de autenticación de usuarios
4. Pueden crearse brechas de seguridad al configurarlos inadecuadamente

Filtros de paquetes 4: ataques que soportan

- Suplantación (*spoofing*) de direcciones IP

  Un atacante transmite paquetes desde el exterior con un campo de dirección IP origen que contiene la dirección de un host interno esperando que el cortafuegos la acepte

  Contramedida: descartar paquetes con direcciones de origen internas si vienen del exterior

- Ataque de encaminamiento de origen

  La estación de origen especifica la ruta que debe usar un paquete en Internet esperando que esto eludirá los controles de seguridad que no analizan el enrutamiento de origen

  Contramedida: descartar paquetes que utilizan esta opción

- Ataque de fragmentación de cabeceras

  El atacante usa la opción IP de fragmentación para dividir la cabecera TCP en múltiples fragmentos muy pequeños intentando así sortear las reglas de filtrado que necesitan toda la información de la cabecera

  Contramedida: descartar directamente o reensamblar antes de comprobar las reglas

Filtros de paquetes 5: ejemplos de reglas

Rule Set A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Rule Set B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

Rule Set C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

Rule Set D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

Rule Set E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Filtros de paquetes con inspección de estados

Estos cortafuegos revisan la información de las cabeceras de los paquetes y además mantienen y usan la información sobre las conexiones TCP

Se les denomina "*Stateful Packet Filters*"

Típicamente las conexiones TCP utilizan números de puertos:

Bajos (<1024) para los servidores, bien conocidos y asignados permanentemente

Altos (>1024) para los clientes, generalmente generados dinámicamente

- Un Filtro de paquetes Simple

  Debe permitir el tráfico entrante con puertos elevados → **Vulnerabilidad**

- Un Filtro de paquetes con estado

  Crea un directorio de conexiones TCP salientes (con puertos elevados)
  Hay una entrada en el directorio para cada conexión establecida

  Solo permite tráfico entrante con puertos altos
  que correspondan a una entrada del directorio → **Más seguridad**

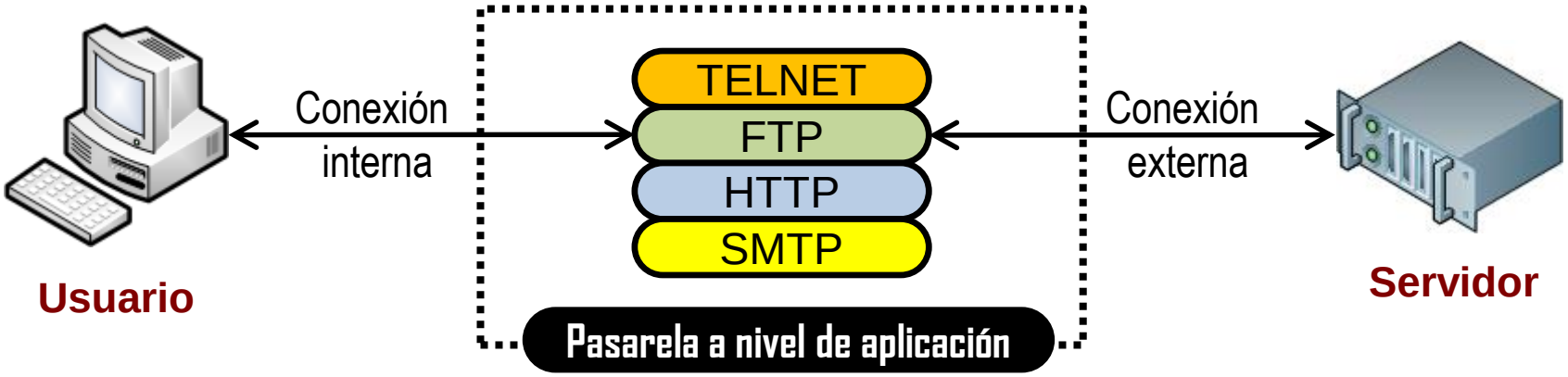
Pasarelas a nivel de aplicación 1

Estos cortafuegos actúan como retransmisores (*relays*) del tráfico a nivel de aplicación

- El usuario indica a la pasarela el nombre del servidor/aplicación al que quiere acceder
- Se autentican ambos (usuario ← → pasarela)
- La pasarela establece contacto con la aplicación del servidor y retransmite todos los segmentos TCP entre el usuario y el servidor

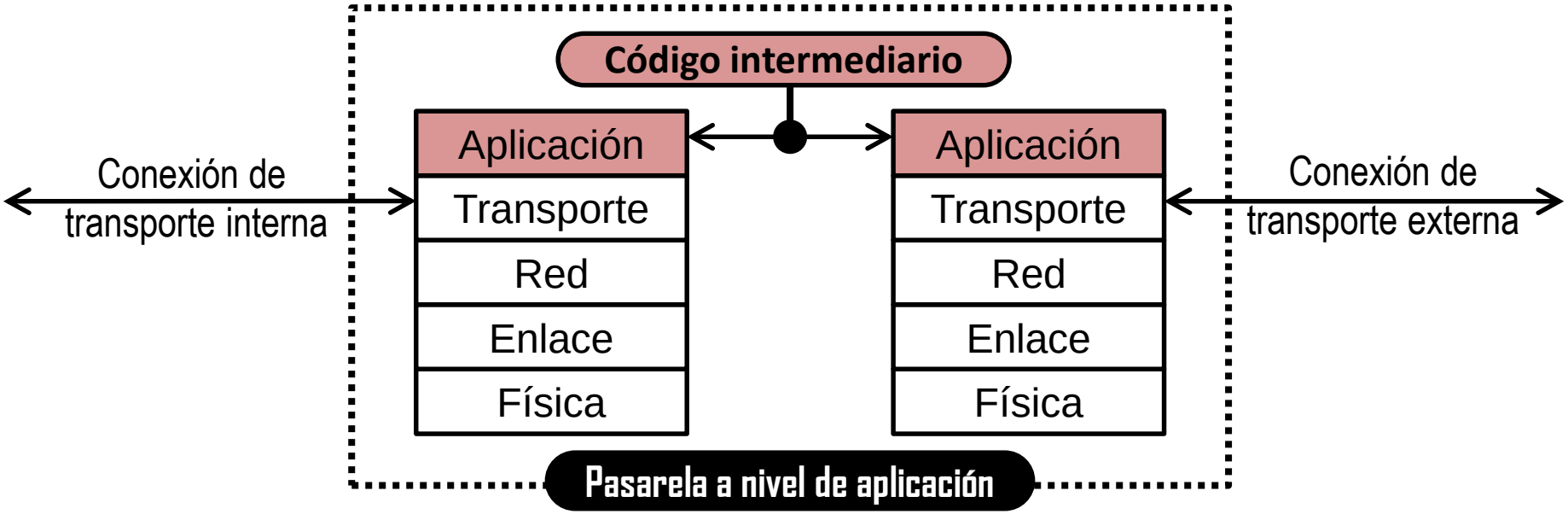
La pasarela debe tener el código intermediario (*proxy*) para cada aplicación soportada

- Algunos servicios soportan la intermediación (*proxying*) de forma bastante natural
- Pero otros no, lo que limita la aplicabilidad de este tipo de cortafuegos



Pasarelas a nivel de aplicación 2

Las pasarelas a nivel de aplicación funcionan en los siguientes niveles de una red:



Ventaja principal: generalmente son más seguras que los filtros de paquetes

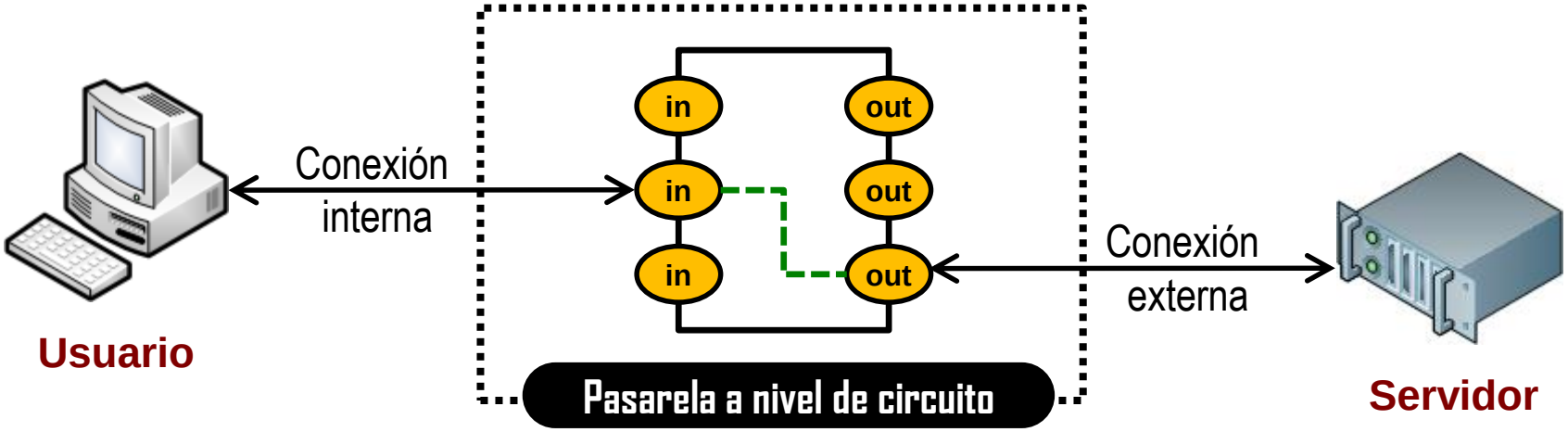
Desventaja principal: la sobrecarga adicional para procesar cada conexión

Pasarelas a nivel de circuito 1

Las pasarelas a nivel de circuito se establecen dos conexiones TCP simultáneas: con un usuario interno y con un host externo

¡La función de seguridad consiste en determinar **qué** conexiones son permitidas!

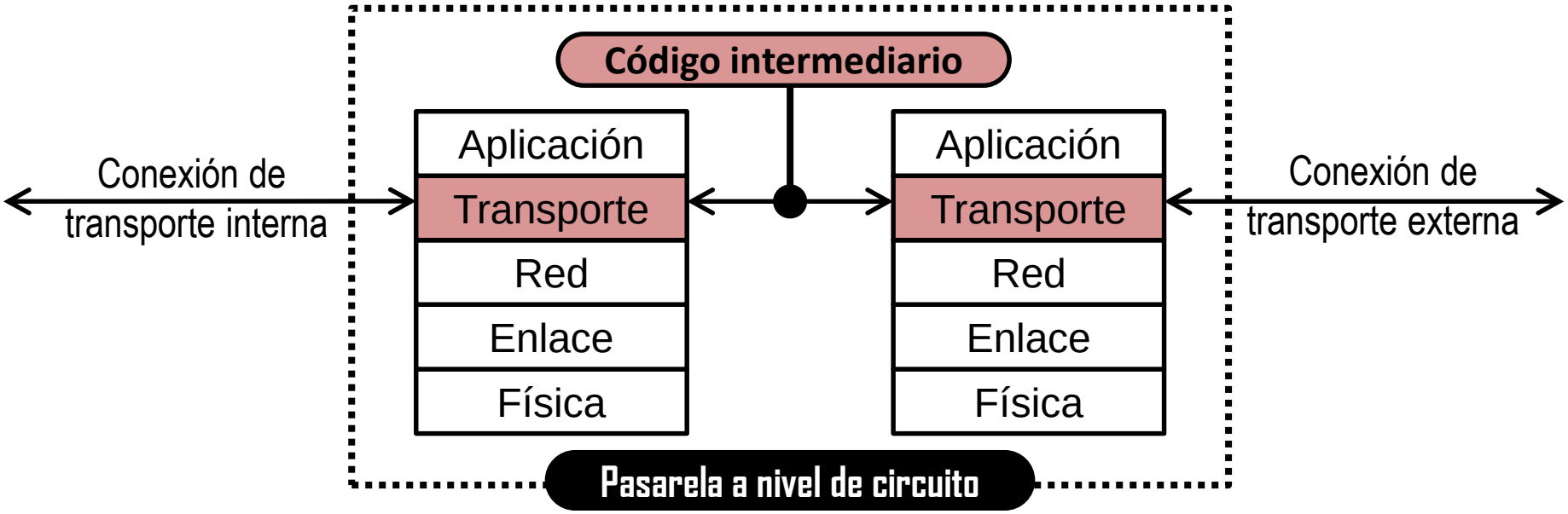
Cuando ya están las dos conexiones establecidas, la pasarela retransmite el tráfico TCP entre ambos sin examinar el contenido de los paquetes



Se pueden implementar en un equipo totalmente independiente o como una aplicación especializada de una pasarela a nivel de aplicación

Pasarelas a nivel de circuito 2

Las pasarelas a nivel de circuito funcionan en los siguientes niveles de una red:



Escenario típico de uso (un administrador confía en los usuarios internos)

- Una pasarela a nivel de aplicación para las conexiones entrantes
- Una pasarela a nivel de circuito para las conexiones salientes

Ventaja: al menos reduce la sobrecarga para las conexiones de salida

Ejemplo de pasarela a nivel de circuito: Paquete SOCKS V5 (RFC1928)

Requiere un servidor SOCKS en el cortafuegos + compilar los clientes internos con la librería SOCKS

Tipos de cortafuegos

Tipos de cortafuegos (según el modo de funcionamiento)

- Filtros de paquetes
- Filtros de paquetes con inspección de estados
- Pasarela (*gateway*) a nivel de aplicación == Proxy de aplicación
- Pasarela (*gateway*) a nivel de circuito

Tipos de cortafuegos (según la ubicación ≈ lo que protegen)

- Hosts bastión
- Cortafuegos basados en host
- Cortafuegos personales

Cortafuegos bastión (1)

Un bastión es un equipo identificado por el administrador de seguridad como un **elemento crítico** importante en la seguridad de la red

Un bastión es un cortafuegos que **funciona como** una **pasarela a nivel de aplicación y/o circuito**

Implementación típica: módulo software que se ejecuta

- En un equipo independiente basado en un sistema operativo común (Linux)
- En un router o switch de la red

Características comunes:

- Ejecuta una versión segura (*hardened*) de su SO → Es un sistema muy fiable
- Solo tiene instalados los servicios esenciales para su tarea:
  (proxy para aplicaciones: Telnet, DNS, FTP, SMTP, y autenticación de usuarios)
- Puede requerir autenticación antes de permitir a un usuario acceder a los servicios
- Uso del disco limitado a leer configuración inicial o registros de funcionamiento

Suelen tener dos o más interfaces de red

Debe ser fiable (*trusted*) para implementar (*enforce*) una política de separación fiable entre las redes

Cortafuegos bastión (2)

Cada proxy de un bastión …

Se configura para admitir solo un **subconjunto** del conjunto de comandos de la aplicación

Se configura para permitir solamente el **acceso** a determinados hosts de la red

Mantiene información auditable **registrando** todo el tráfico, cada conexión y su duración

Es **independiente** de los otros proxies instalados y puede desinstalarse sin afectar a los otros

Es un módulo software muy **pequeño** diseñado considerando la seguridad de la red
(es fácil comprobar si tiene defectos que afecten a la seguridad)

Se ejecuta en **modo usuario** (no privilegiado) en un directorio del host privado y seguro

Cortafuegos basados en host

Un cortafuegos basado en un host (*host-based firewall*) es un módulo software usado para proteger a un host individual

Estos módulos están disponibles en muchos SO o se suministran como paquetes adicionales

Los cortafuegos residentes en host filtran y limitan el tráfico de paquetes
Funcionan de modo similar a los cortafuegos independientes (*stand-alone*)

Comúnmente estos cortafuegos se instalan en servidores

Ventajas:

- Las reglas de filtrado pueden ser adaptadas al entorno de trabajo del host
- La protección se proporciona independientemente de la topología de la red
- Proporcionan una capa de protección adicional

Cortafuegos personales

Un cortafuegos personal controla el tráfico entre un PC y la red corporativa/internet

Estos módulos están disponibles en muchos SO o se suministran como paquetes adicionales

Se utilizan en los PCs ubicados en → { Hogares / Pequeñas oficinas / Grandes corporaciones }

En un entorno doméstico o de pequeña oficina que tenga múltiples PCs conectados a internet la función de **cortafuegos** puede alojarse en el **router** que conecta la casa/oficina a internet

A estos routers se les denomina: SOHO (*Small Office / Home Office*) routers o (*screening routers*)

Los cortafuegos personales son **menos complejos** que los independientes o los basados en host

La función principal de un cortafuegos personal es impedir el **acceso** remoto no autorizado al PC

También puede monitorizar la actividad de **salida** del PC para detectar y bloquear gusanos

Configuraciones complejas con cortafuegos

La configuración más simple:

1) Utilizar un router de acceso a Internet que actúe como cortafuegos (*screening router*)

2) Colocar un cortafuegos en cada servidor y cada PC

PERO … Las soluciones reales suelen ser ¡más complejas!

- Una opción es integrar en la red interna un bastión que "ayude" al *screening router*

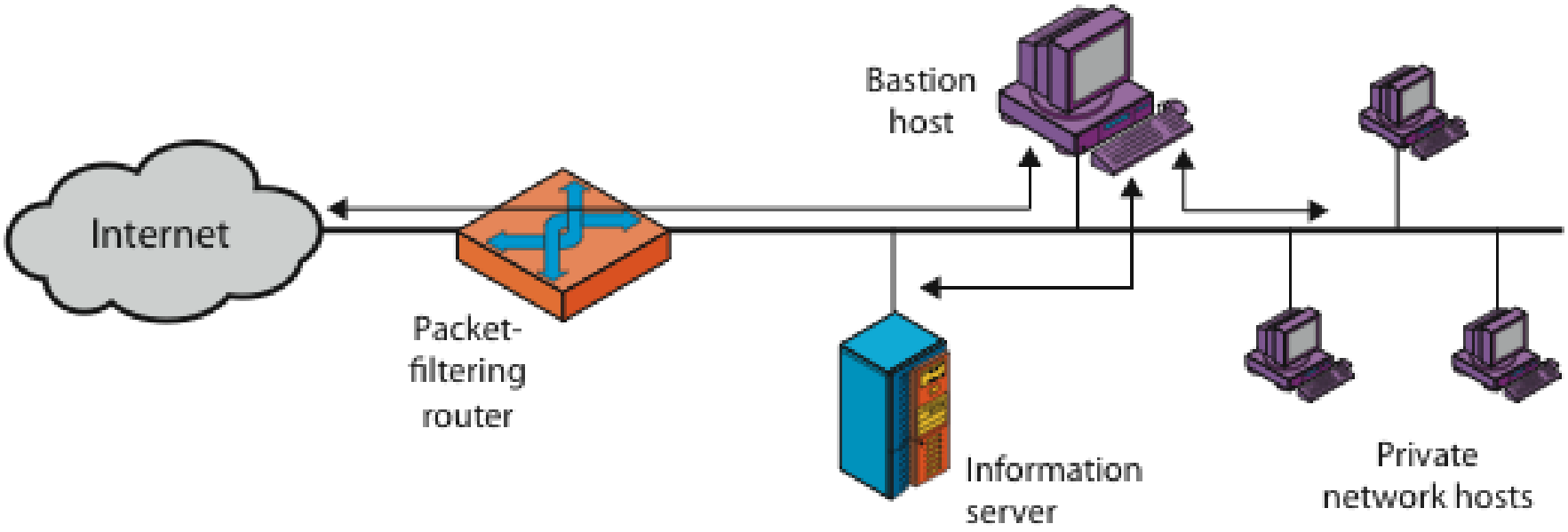
  Al bastión se le suele denominar también *screened host*

- Otras opciones consisten en usar { 2 routers + 1 cortafuegos / 1 router + 2 cortafuegos }

- La opción más general es usar una configuración distribuida de cortafuegos

1 Router (filtro) + 1 Bastión

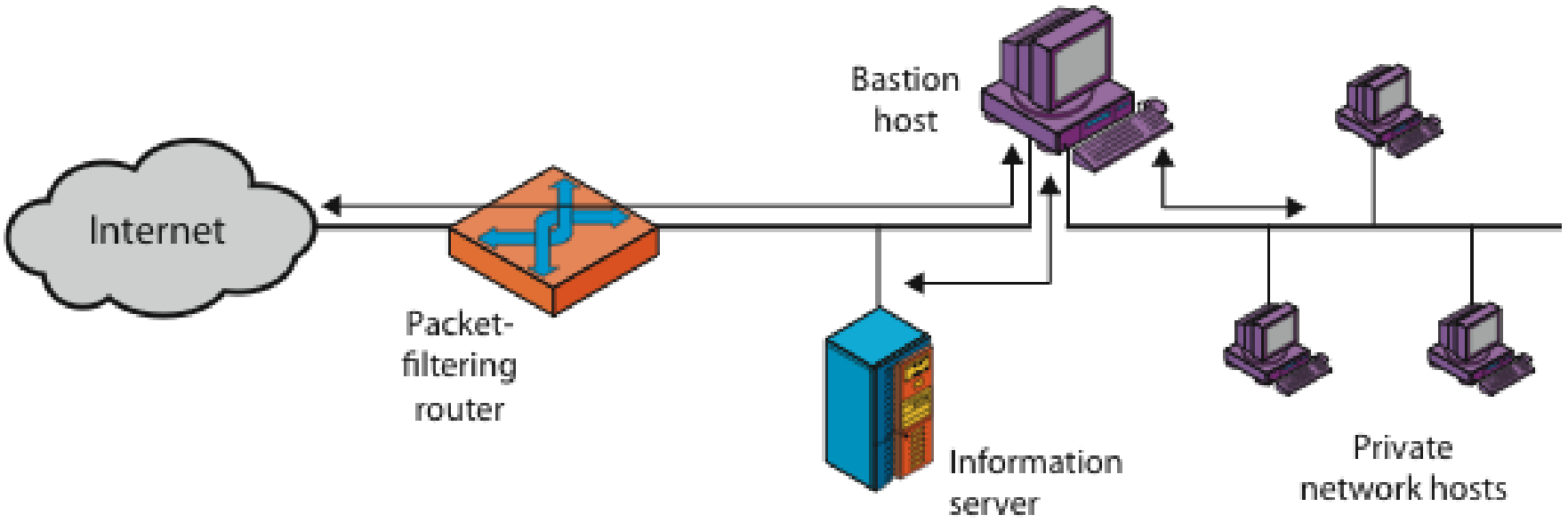
Sistema cortafuegos basado en 1 filtro y 1 bastión con 1 interfaz de red
(*screened host firewall system, single-homed bastion configuration*)



Stallings – Cryptography & Network Security

1 Router (filtro) + 1 Bastión

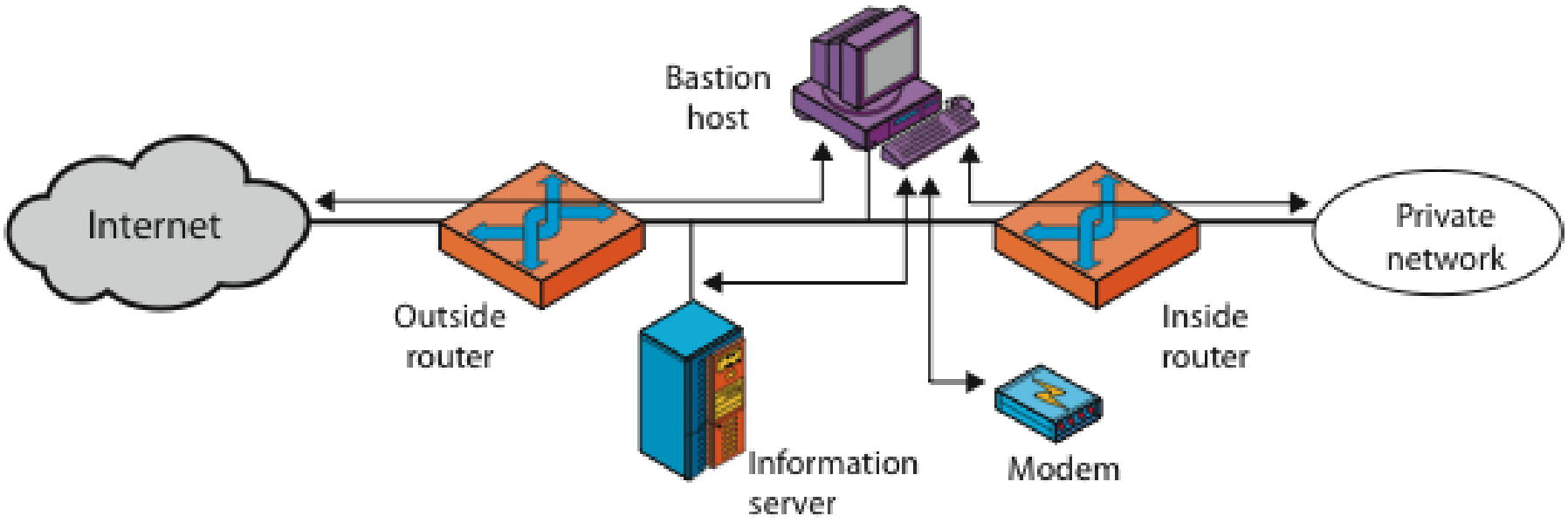
Sistema cortafuegos basado en 1 filtro y 1 bastión con 2 interfaces de red (*screened host firewall system, dual-homed bastion configuration*)



Stallings – Cryptography & Network Security

2 Routers (filtros) + 1 Bastión

Sistema cortafuegos basado en 2 filtros y 1 bastión con 1 interfaz de red
(*screened subnet firewall system, single-homed bastion configuration*)



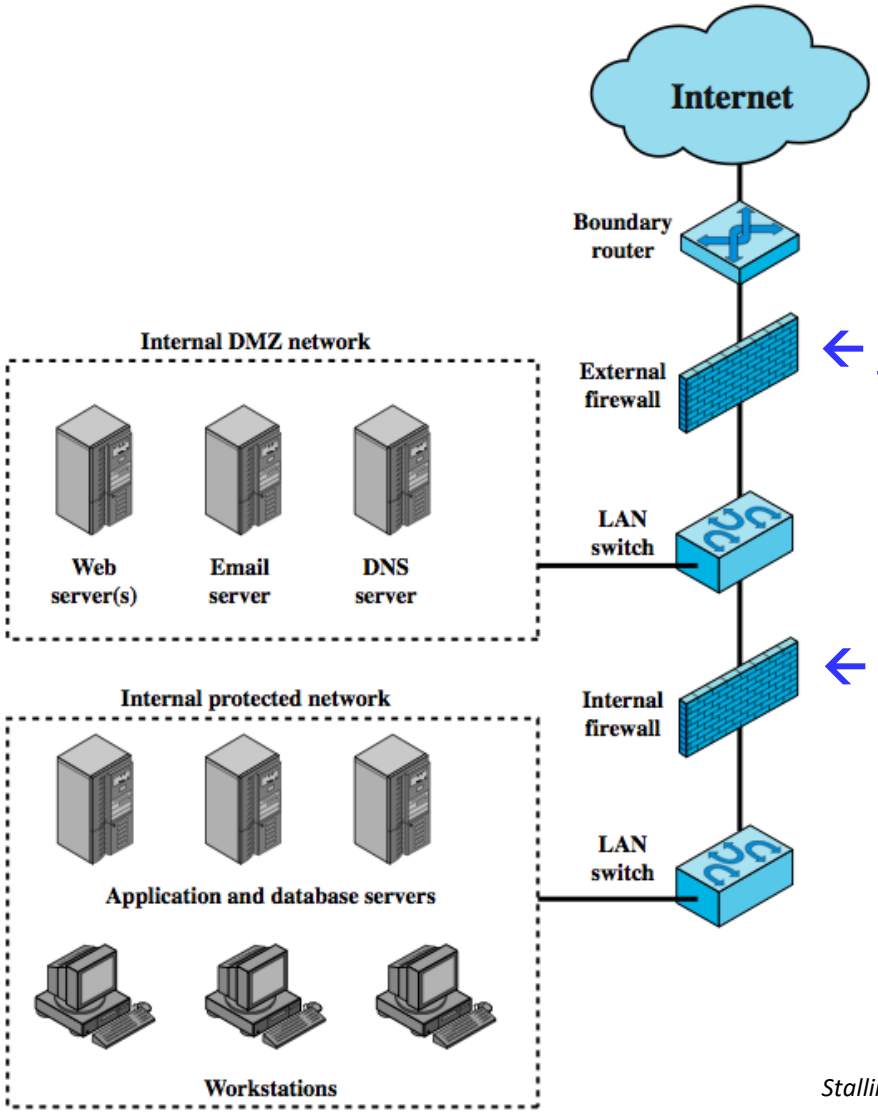
Stallings – Cryptography & Network Security

Concepto de zona desmilitarizada

Sistema cortafuegos basado en al menos 2 cortafuegos con 2 interfaces de red

Zona Desmilitarizada
(*demilitarized zone, DMZ*)

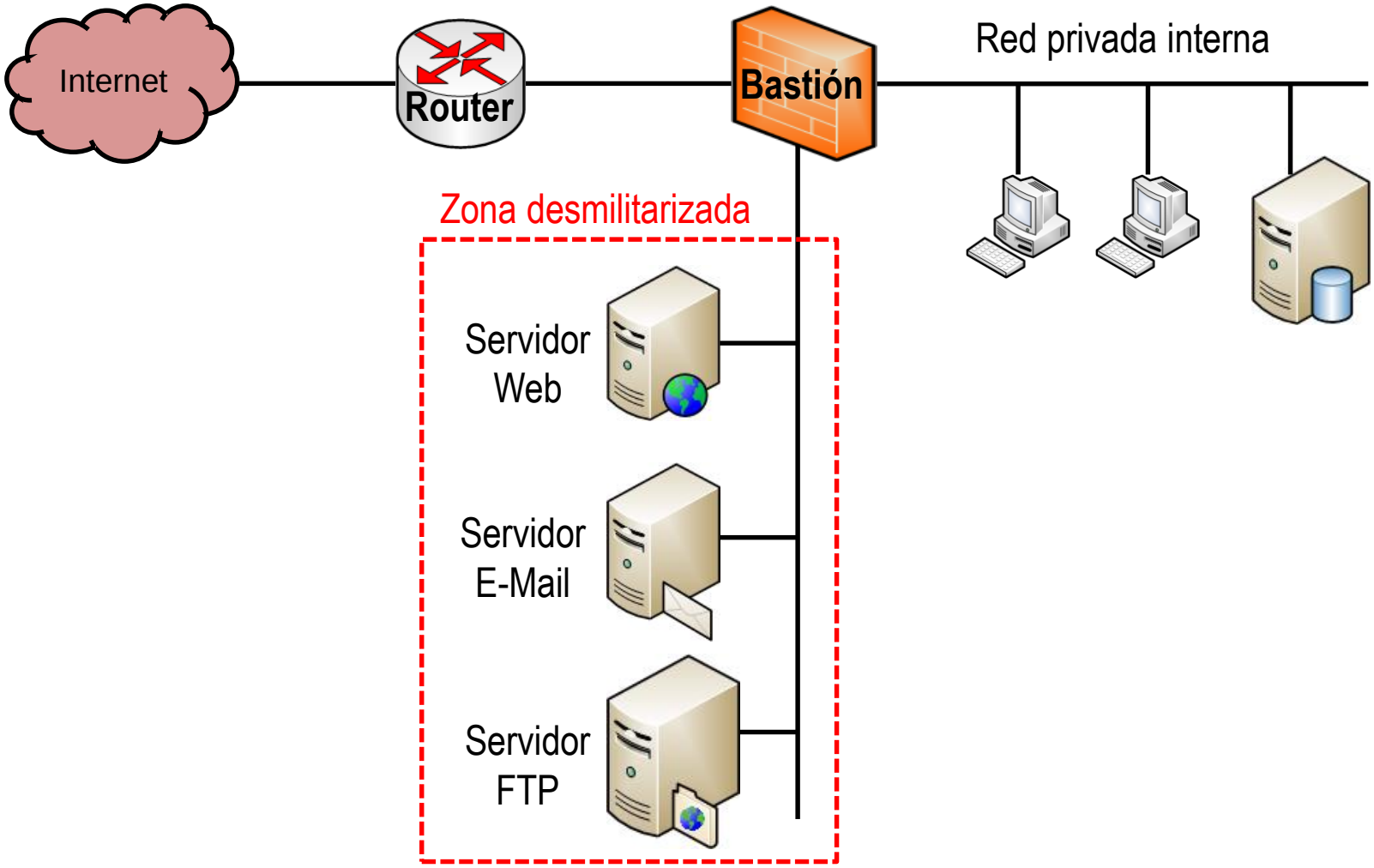
Zona Militarizada
de alta seguridad



Stallings – Cryptography & Network Security

Zona desmilitarizada con un solo cortafuegos

Configuración con un solo bastión dotado de 3 interfaces de red



Configuración distribuida general

Utiliza 2 tipos de cortafuegos:

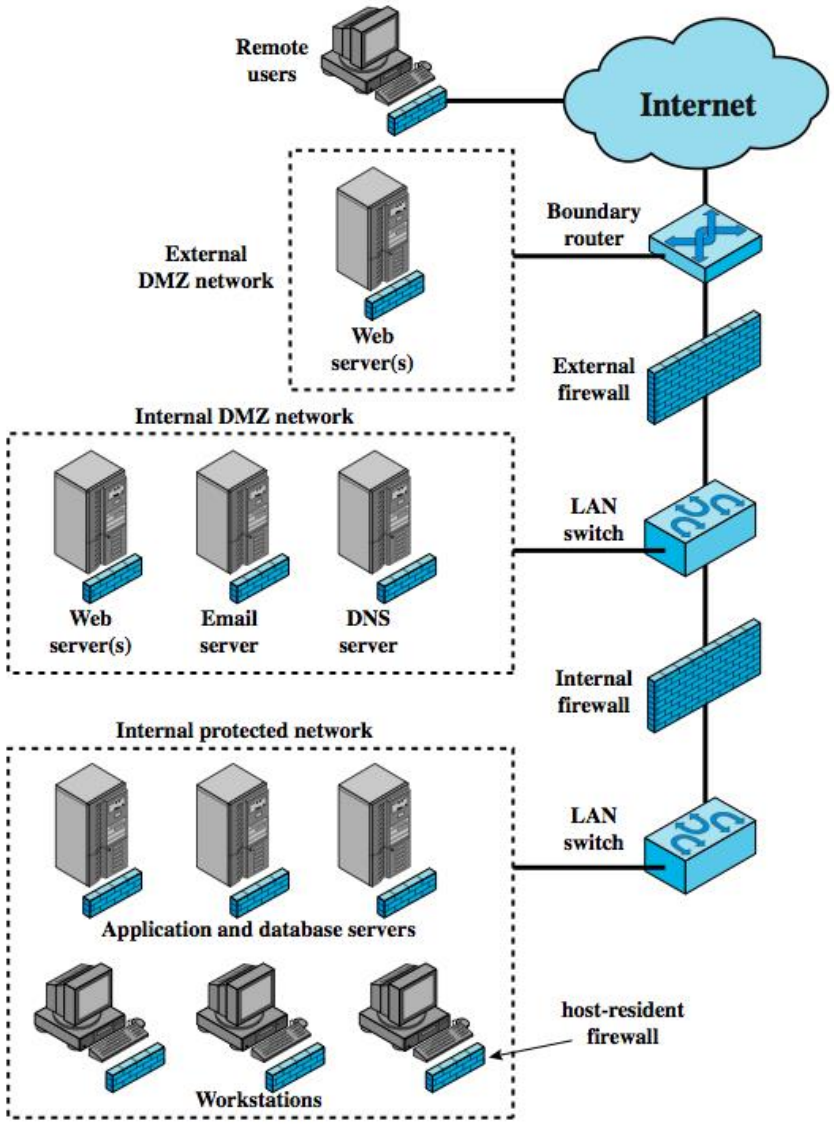
- Independientes (equipos)
- Basados en hosts (software)

Funcionando conjuntamente bajo una administración centralizada

Tiene 2 DMZ

Herramientas de administración

Esenciales para implementar una política y Monitorizar de modo agregado o individual



Stallings – Cryptography & Network Security