Cortafuegos y SOCKS

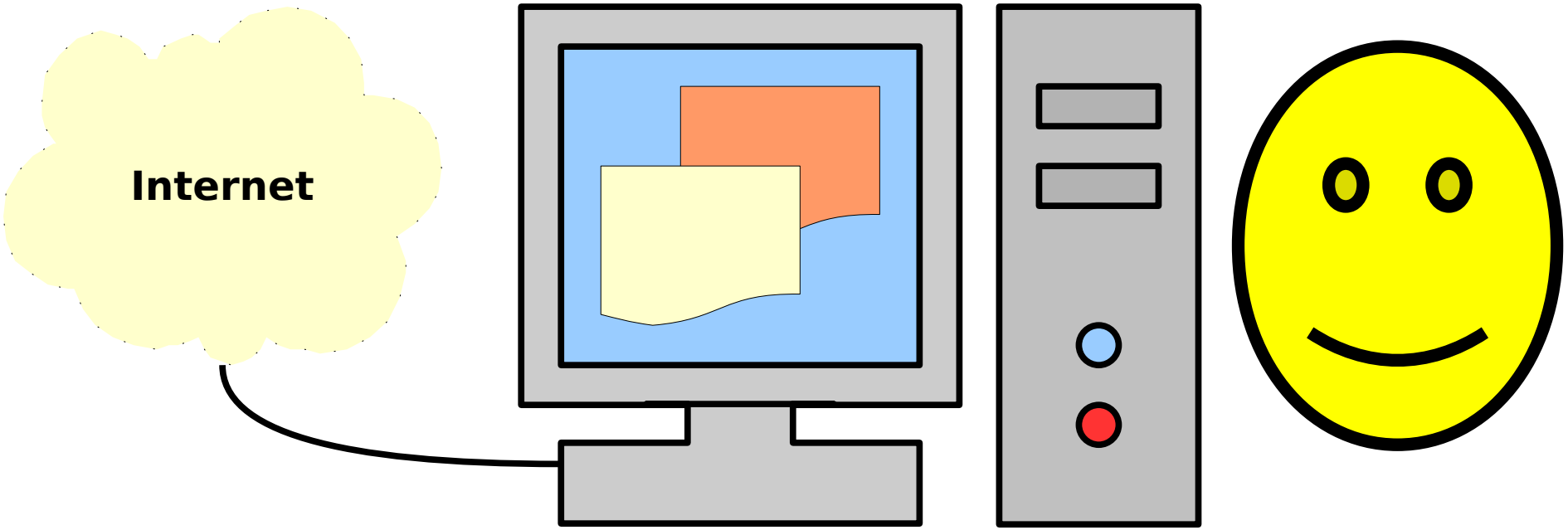
Felipe Ignacio Cañas Sabat
fcanas@dcc.uchile.cl

Pablo Ignacio Sepúlveda Rojas
pasepulv@dcc.uchile.cl

Motivación

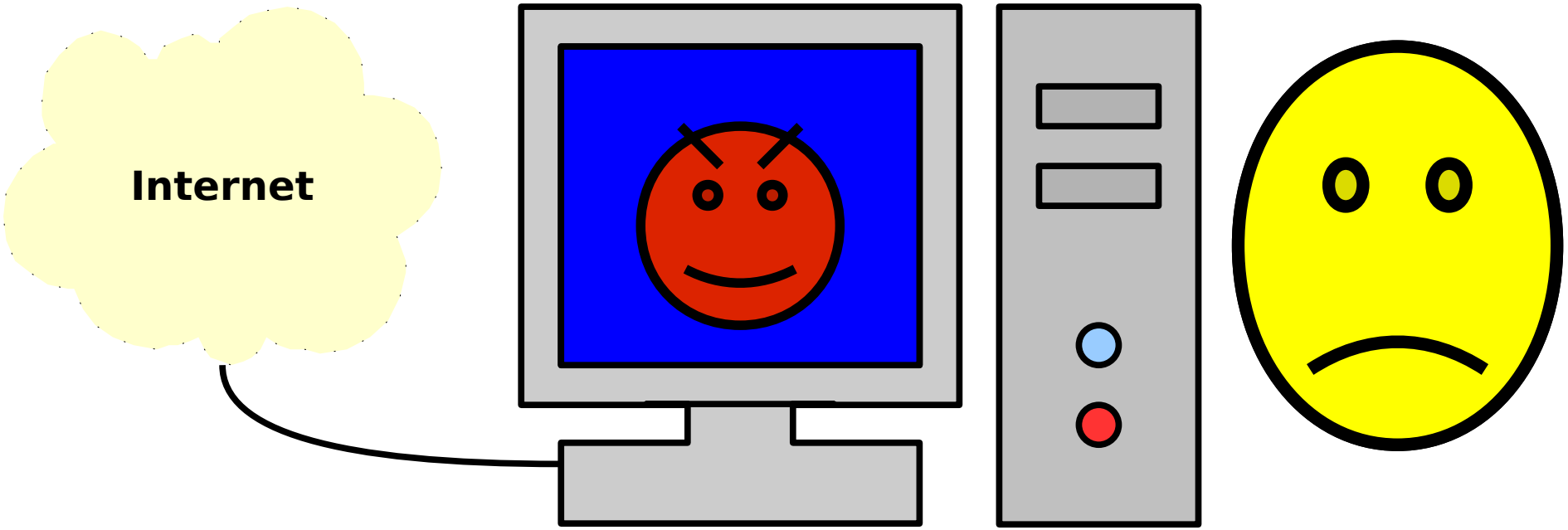
¿Por qué cortafuegos?

Érase una vez un mundo sin cortafuegos...



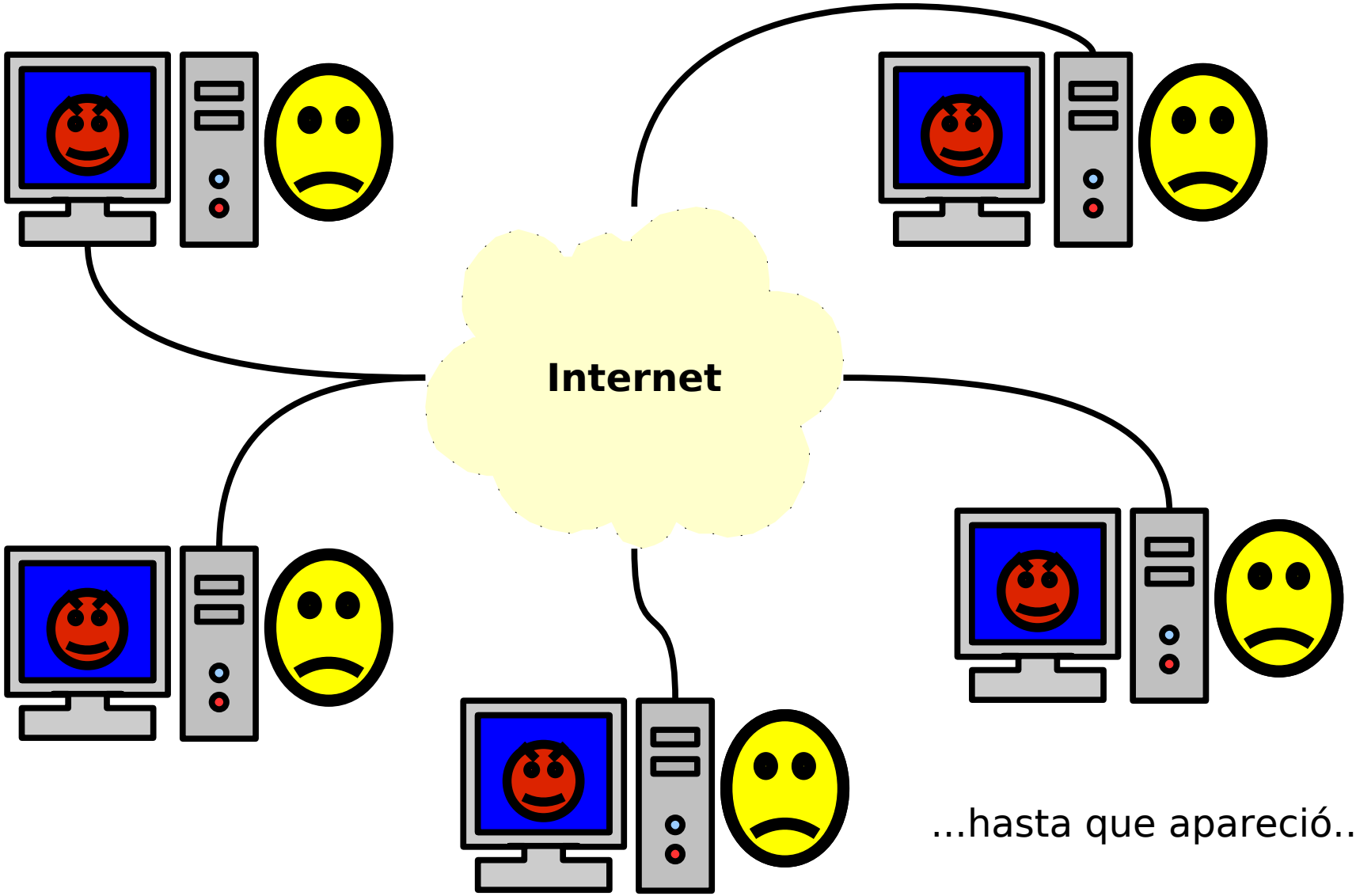
...en el cual usuarios navegaban inocentemente por Internet.

Todos eran felices hasta que...

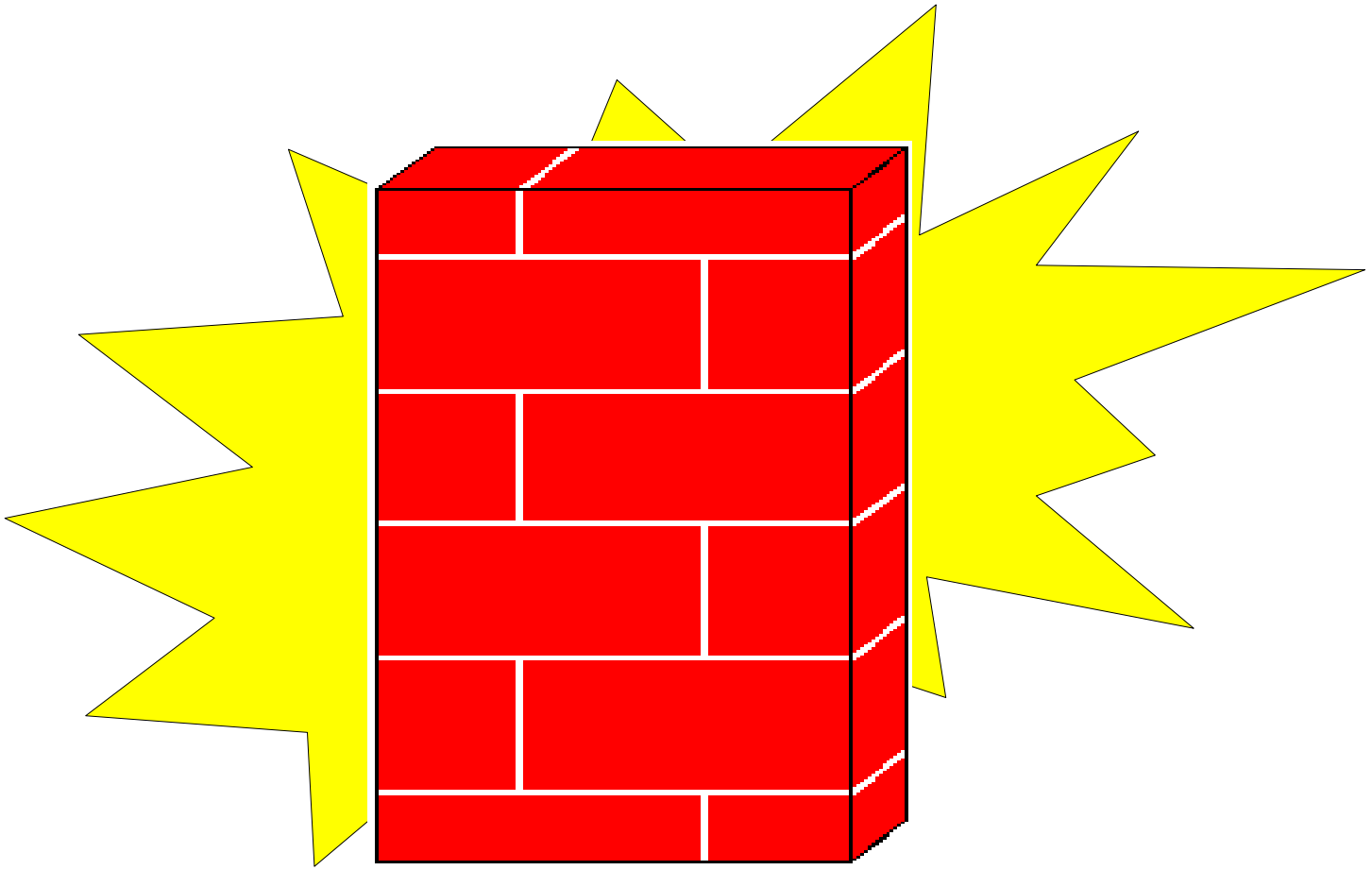


...¡aparecieron Los Malos!

La gente perdía esperanza...

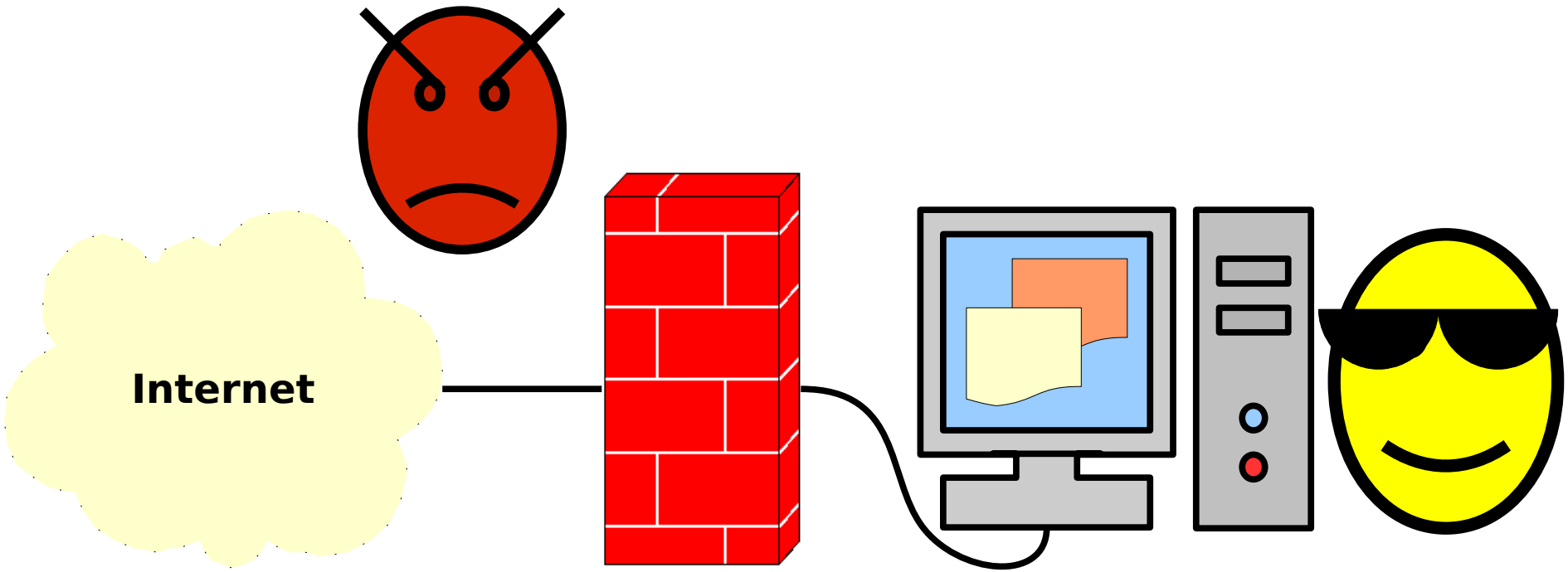


...hasta que apareció...

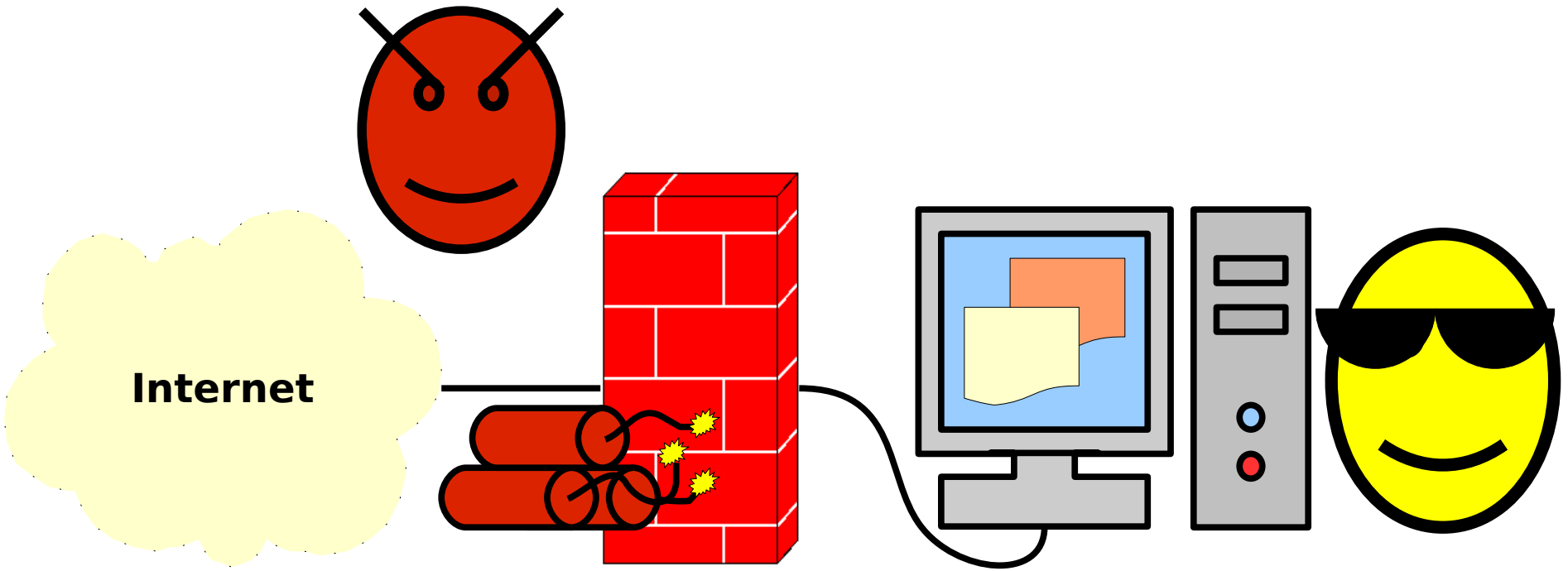


El Cortafuegos

Y el mundo volvió a ser seguro.



Y el mundo volvió a ser ~~seguro~~ casi seguro.



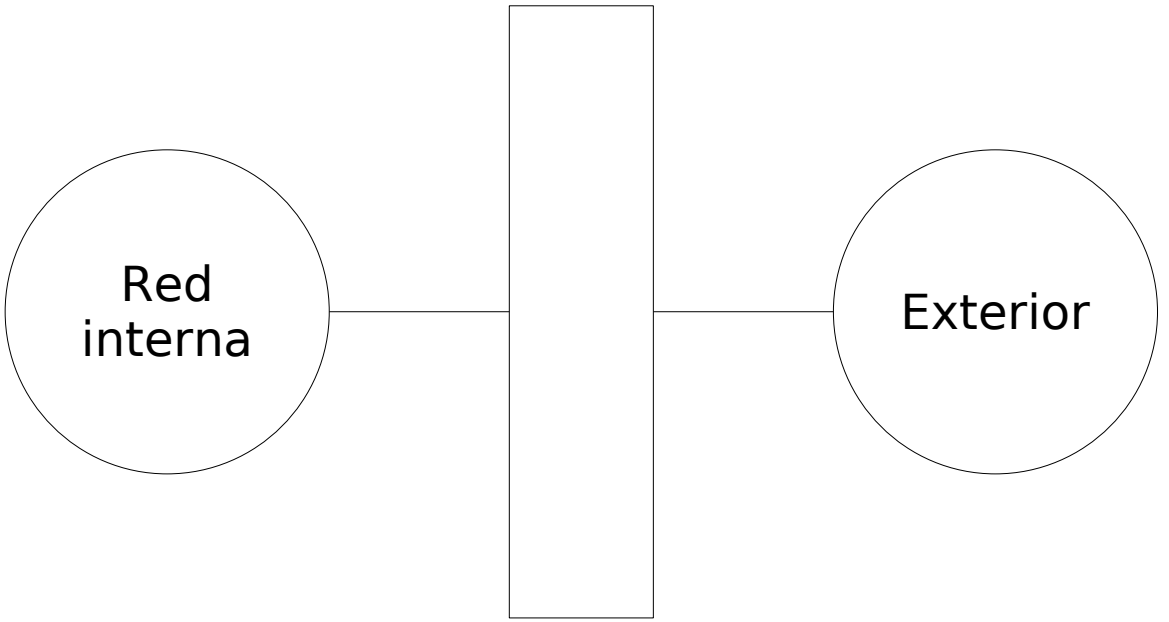
Definición:
Cortafuegos

1.Vereda ancha que se deja en los sembrados y montes para que no se propaguen los incendios.

2.Pared toda de fábrica, sin madera alguna, y de un grueso competente, que se eleva desde la parte inferior del edificio hasta más arriba del caballete, con el fin de que, si hay fuego en un lado, no se pueda este comunicar al otro.

En informática...

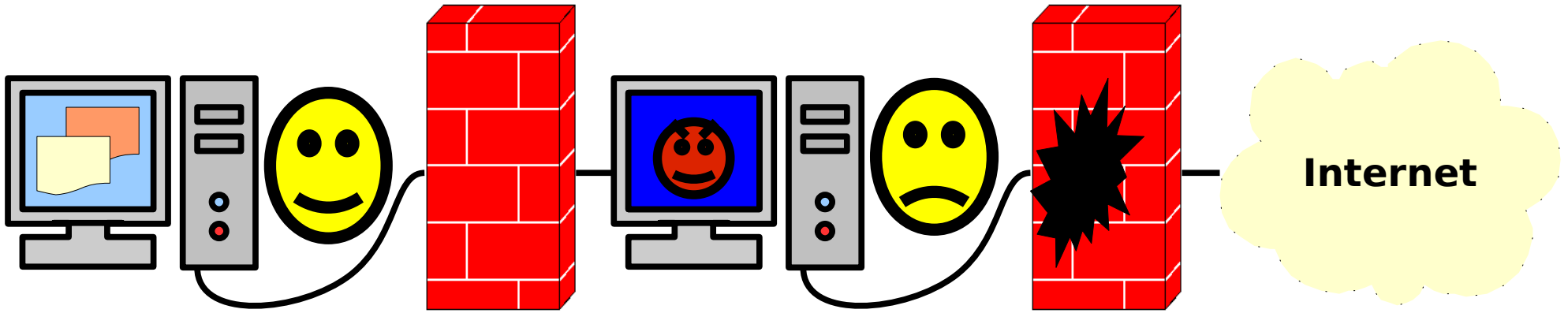
Dispositivo, de hardware o software, para controlar comunicaciones en una red de computadores.



Cortafuegos

Resumen

- Exponer equipos a la Internet no es seguro.
- Los equipos contienen información sensible, o bien se encargan de procesos necesarios.
- Algunos procesos necesitan que el equipo donde corren sean accesibles desde afuera de la red.
- Para que un ataque exitoso no afecte el resto de los equipos en la red, se usa un cortafuegos.



Objetivos

¿Qué hace un cortafuegos?

Objetivo principal

Permitir controlar los datos que entran y/o salen de una red.

Objetivos específicos

- Posibilidad de configurar las direcciones válidas e inválidas tanto para la salida de la red como para la entrada.
- Posibilidad de filtrar según el contenido de los datos que entran y salen de la red.
- Posibilidad de mantener un historial de los datos que entran y salen de la red.

¿Para qué?

- Filtrar según las direcciones para así definir *hosts* confiables, o bien definir puertos y direcciones a los cuales es permitido acceder desde fuera de la red.
- Filtrar según contenido de los datos para determinar si contienen algún programa maligno (virus, worm, etc.), o si se está sacando información sensible de la red (palabras clave).
- Mantener un historial para saber, en el caso de una falla de seguridad, más información acerca del ataque.

Descripción

¿Cómo funciona un cortafuegos?

Funcionamiento

- El funcionamiento de los cortafuegos depende de la manera en que se desea regular el flujo de datos a través de éste.
- Existen tres tipos principales de cortafuegos,
    1. Filtros de paquetes
    2. Filtros de contenido
    3. Cortafuegos tipo proxy
- Cada tipo de cortafuegos tiene tanto ventajas como desventajas, y muchas veces no basta sólo un tipo.

1.Filtro de Paquetes

- Funciona filtrando los datos según la información en los encabezados de la capa de enlace, e.g., TCP o UDP.
- Si un paquete no recibe el visto bueno, según las reglas definidas, éste es descartado.
- Se crean tablas de instrucciones para determinar si cada paquete que intenta pasar por el cortafuegos debe ser permitido o descartado.
- Debe definirse la regla 'por defecto' para paquetes que no caen en ninguna categoría de la tabla de instrucciones; se debe decidir si por defecto se acepta todo, o se bloquea todo.

Ejemplo:

action	src	port	dest	flags	comment
allow	{our hosts}	*	25		outgoing SMTP
allow	*	25	*	ACK	incoming replies

1. Filtro de Paquetes

- Existen dos variantes de este tipo de cortafuegos,

  i. Con estados (*stateful*)

  - Guarda información acerca de las conexiones ya abiertas.
  - Con esta información, se logra agilizar la transferencia de datos, ya que (teóricamente, por lo menos) se puede confiar más en conexiones ya abiertas que en conexiones por abrir.

  ii. Sin estados (*stateless*)

  - Requiere menos memoria que un cortafuegos con estados.
  - Es suficiente cuando se monitorean conexiones donde la noción de estado es irrelevante.

2.Filtro de Contenido

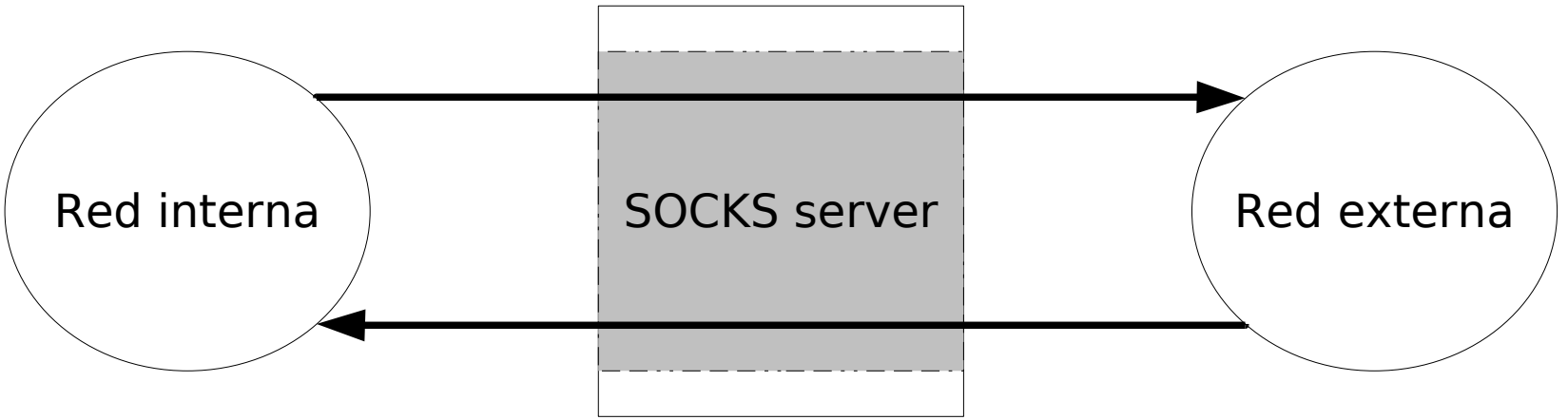
- Funciona filtrando los datos según la información contenida en la capa de aplicación, es decir, los mismos datos que el usuario quiere transmitir.
- De esta forma se pueden regular protocolos, no sólo direcciones y puertos, ya que un *host* puede ocupar puertos no estándar para distintos servicios.
- Ya que se tiene acceso al contenido de cada paquete, se pueden configurar reglas más precisas para algún protocolo. Por ejemplo, se pueden bloquear todos los llamados con protocolo HTTP al dominio "*www.facebook.com*".

Problemas

¿Qué problemas causa un cortafuegos?

Cuando la comunicación se debe permitir

- Cuando se desea usar un servicio al otro lado de un cortafuegos, o cuando se desea prestar un servicio a clientes al otro lado de un cortafuegos, es necesario permitir esta comunicación.
- A veces no es suficiente solamente permitir la comunicación, sino que se necesita que la comunicación sea *transparente*, i.e., que el servidor y cliente actúen como si el cortafuegos no existiera.
- Para estos casos, se usa el protocolo ~~CALCETINES~~ SOCKS.



SOCKS

- El protocolo SOCKS (RFC 1928) permite la comunicación transparente entre dos equipos en lados opuestos de un cortafuegos.
- Existen en la actualidad dos versiones usadas mayormente, SOCKS4 y SOCKS5.
- La ventaja que tiene SOCKS5 sobre su predecesor es que soporta comunicación usando UDP tanto como TCP, mientras que SOCKS4 sólo soporta TCP.

FIN