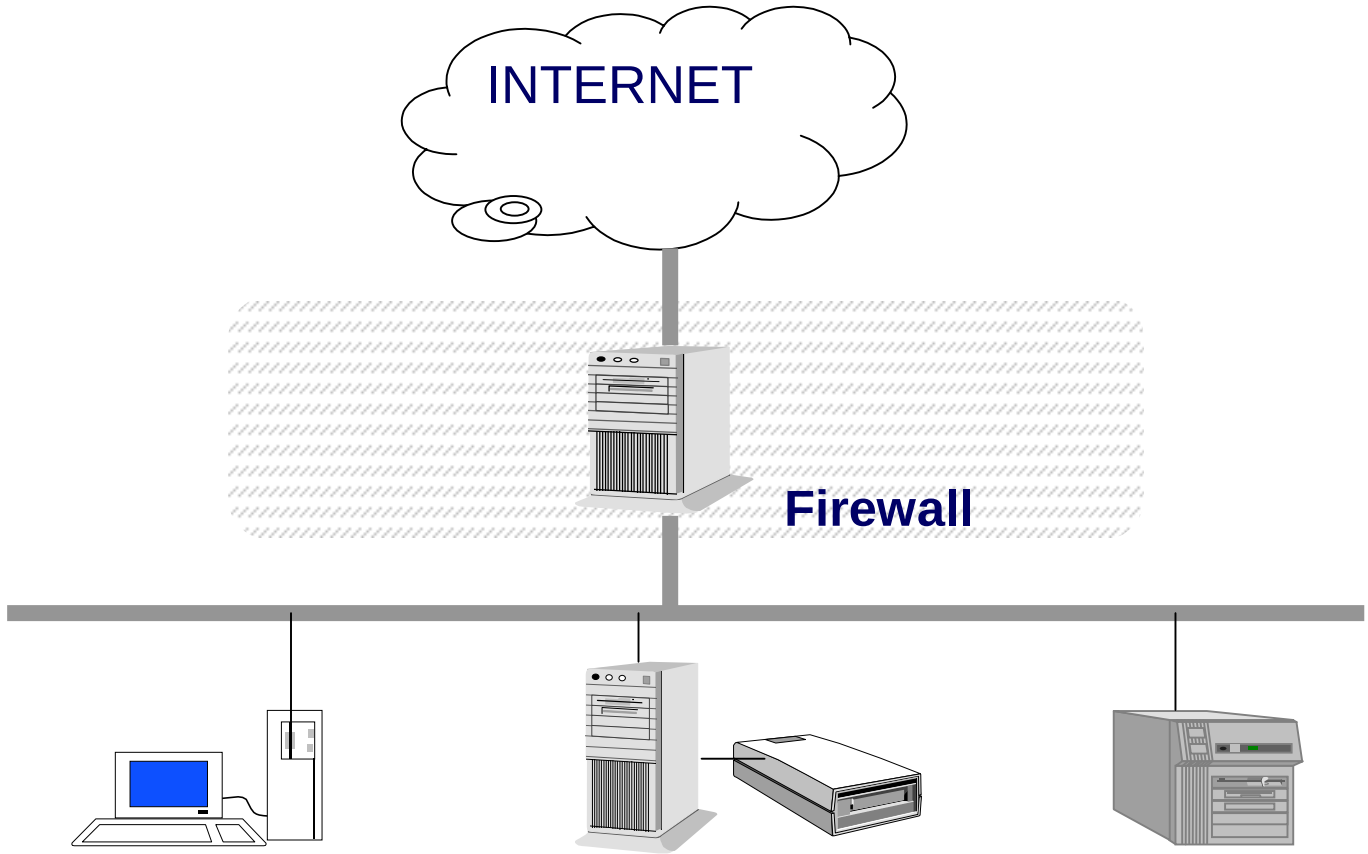
Seguridad de Acceso:

Configuración Básica

Mediante un firewall es posible aislar nuestra red de la red exterior



Configuraciones de Firewalls

- Como filtro de paquetes: Define el paso o no de un paquete de acuerdo a determinadas listas de acceso
- Como compuerta: Aquí los paquetes no son rechazados sino enviados a una máquina especial que es quien realmente realiza las solicitudes de los usuarios y recibe las respuesta desde el exterior.

Filtros de Paquetes

- Normalmente están constituidos por un conjunto de reglas de filtrado que son examinadas una a una para buscar similitud con algún parámetro del paquete
- Si se encuentra alguna coincidencia la regla se aplica
  - Ej: Si la dirección de origen del paquete es XXX entonces deje pasar el paquete.
- Si al final de las comparaciones no se encuentran similitudes, se aplica la política por omisión del sistema

En FP le permite controlar la transferencia de información con base en:

- Dirección de donde “proviene” la información
- Dirección a donde va la información
- Protocolos de nivel IP, Transporte y aplicación que emplean (IP,ICMP,TCP/UDP, Telnet, HTTP,SMTP...)

Hasta donde podemos llegar:

- Un filtro de paquetes le permitirá decir:
  - Permita que desde cualquier red se haga telnet (puerto 23) a mi red
- Pero no le permitirá decir:
  - No permita que el usuario root no haga telnet

Políticas por Omisión

- Lo que no está explícitamente permitido está prohibido
- Lo que no está explícitamente prohibido está permitido

Criterios de Filtrado

- Por dirección de origen
- Por dirección de destino
- Por puerto de origen
- Por puerto de destino
- Por tipo de paquetes
- Por interfaces de entrada
- Por interfaces de salida

Ventajas del Filtrado de Paquetes

- Permite controlar desde un solo punto todo el acceso
- No necesita cooperación del usuario
- Muchas veces (como veremos en las prácticas) los enrutadores tienen la capacidad de filtrar paquetes.

Desventajas de los filtros de paquetes

- Las listas de acceso manipulan sólo acciones de permitir-rechazar.
- Las listas de acceso son, por lo general, difíciles de programar y más aún de depurar.
- Si un filtro de paquetes falla deja la “puerta abierta”

Filtrado a nivel IP (capa 3)

- Los datagramas IP tiene información suficiente para especificar Dirección de Origen y Destino por lo que las reglas a este nivel solo se limitan a esas opciones.

Campos de la cabecera IP “interesantes”:

- Dirección de Origen
- Dirección de Destino
- Banderas (fragmentos)

Filtrado de fragmentos

- El problema se debe a que solo el primer fragmento contiene la información TCP necesaria.
- El enfoque común es permitir el paso de todos los fragmentos que no sean iniciales y filtrar solo estos últimos
- El peligro es que los fragmentos no iniciales pueden contener información útil para un atacante.
- Puede ser utilizado para un ataque de DoS

Filtrado TCP

- En la cabecera del paquete TCP tenemos:
  - Puertos de origen y destino
  - Banderas TCP (ACK)
- Para filtar una conexión TCP solo basta con “parar” el primer paquete.
- El chequeo del bit de ACK nos permite filtrar conexiones en un sentido pero no en el otro.

Filtrado unidireccional

- Supongamos que queremos no permitir conexiones desde una red hacia la nuestra pero si en sentido contrario
- Si simplemente negamos todo el tráfico desde la red que no queremos también estaremos filtrando los paquetes de reconocimiento por lo que desde nuestra red tampoco será posible la conexión

Filtrado Unidireccional: La solución

- Filtremos los paquetes de entrada a nuestra red desde la red remota y permitamos el paso solo a los de reconocimento.
- Los paquetes de reconocimento se pueden “reconocer” porque SIEMPRE el bit de ACK está en 1.

Filtrado UDP

- Los paquetes UDP no necesitan reconocimento por lo que parece imposible filtrar unidireccionalmente.
- Solución: filtrado Dinámico
- Filtrado Dinámico: Algunos FP “recuerdan” los últimos paquetes que salieron por un enlace, por lo que pueden filtrar aquellos que lleguen como respuestas.

Filtrado ICMP

- Los paquetes ICMP no tiene puertos de protocolos superiores
- En lugar de esto los paquetes ICMP se diferencian por su tipo (echo request, tiempo excedido, destino inalcanzable, respuesta de eco)
- El filtrado de paquetes ICMP puede ser un arma de doble filo

Filtrado RPC

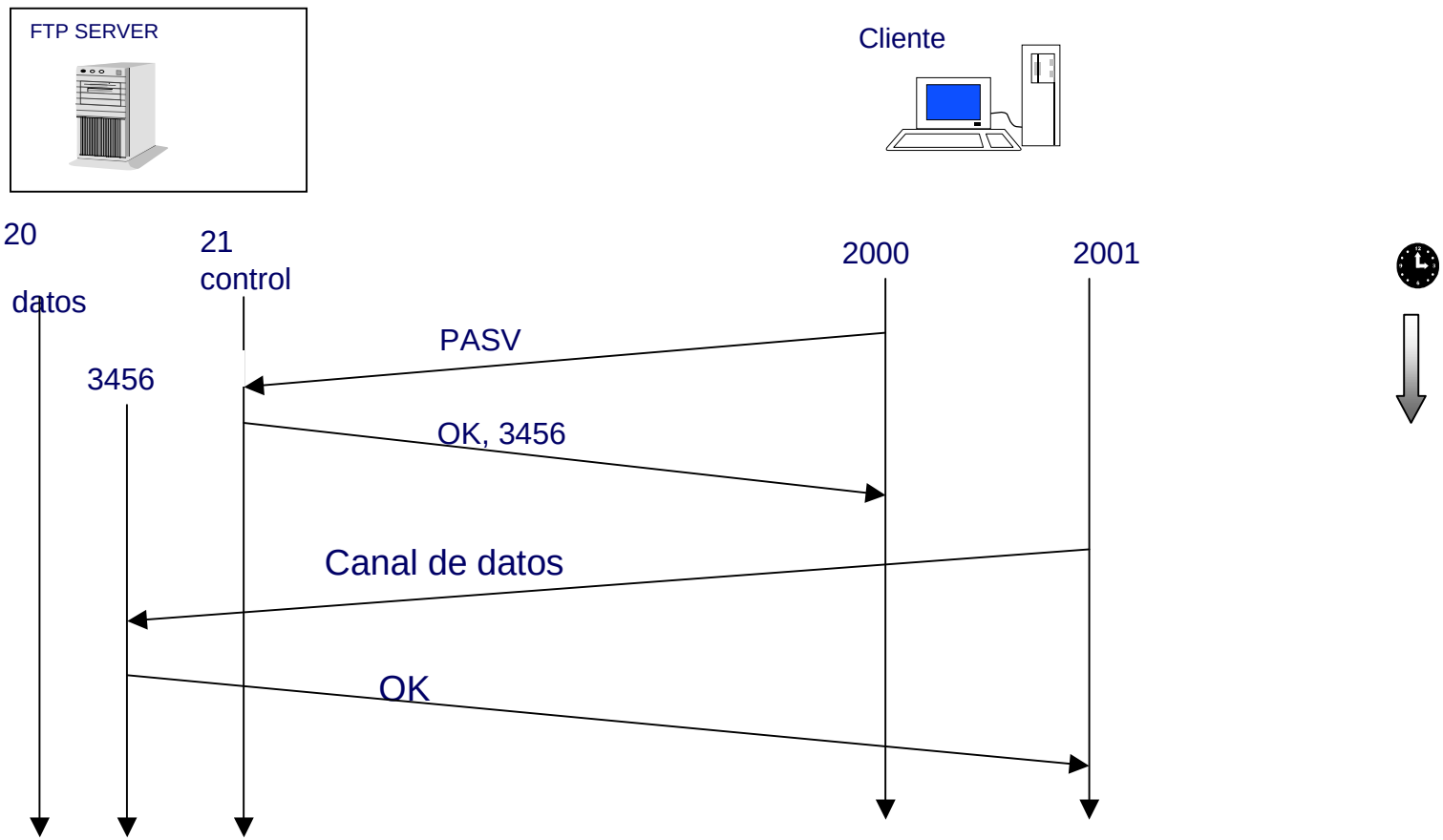
- RPC no utiliza los puertos TCP ó UDP sino un número de servicio de 4 bytes
- RPC está sobre TCP y UDP por lo que debe haber un mecanismo de mapear los números de servicio con los puertos TCP ó UDP: Portmapper
- El problema es que nunca sabemos cual es exactamente el puerto a bloquear
- Podemos bloquear el puerto del portmapper (111) pero un atacante podría buscar los puertos reales de las aplicaciones (son solo 65535!!!)

Filtrado FTP

- Cuando un cliente se comunica con el servidor FTP envía una petición al puerto 21 .Esto no es grave, podremos fácilmente y sin grandes peligros, permitir que desde nuestra red salgan solicitudes a un puerto privilegiado externo.

- Una vez el servidor ha aceptado la comunicación inicial, envía el flujo de información desde su puerto 20 hasta un puerto no privilegiado en la máquina cliente. Esto si es peligroso, pues desconocemos la identidad del servidor y el puerto no privilegiado con que se establecerá loa comunicación. Obviamente, no deseamos permitir conexiones desde cualquier puerto 20, es muy sencillo para un atacante introducirse a nuestro sistema haciendo programas que respondan por el puerto 20.

La solución: FTP Pasivo



Un ejemplo

Regla	Sentido	D.Fuente	D. Destino	Protocolo	Puerto Destino	Acción
A	IN	Externa	Interna	TCP	25	Permitir
B	Out	Interna	Externa	TCP	>1023	Permitir
C	Out	Interna	Externa	TCP	25	Permir
D	In	Externa	Interna	TCP	>1023	Permitir
E	∀	∀	∀	∀	∀	Prohibir

Permitir solo tráfico de Email desde y hacia su red

Listas de Acceso Simple (IOS Cisco)

- ***access-list No.lista {permit | deny } dirección mascara***

Ejemplo:

access-list 1 permit 67.23.2.5 0.0.0.0

access-list 1 deny 67.23.0.0 0.0.255.255

access-list 1 permit 67.0.0.0 0.255.255.255

Listas de Acceso Extendidas

access-list *no.lista* *{**permit** | **deny**}* *protocolo dir.origen máscara-origen dir. destino mascara-destino [operador operando] [**established**]*

Ejemplo

no-access-list 101

access-list 101 deny tcp 132.124.23.55 0.0.0.0 199.245.180.0 0.0.0.255 eq 25

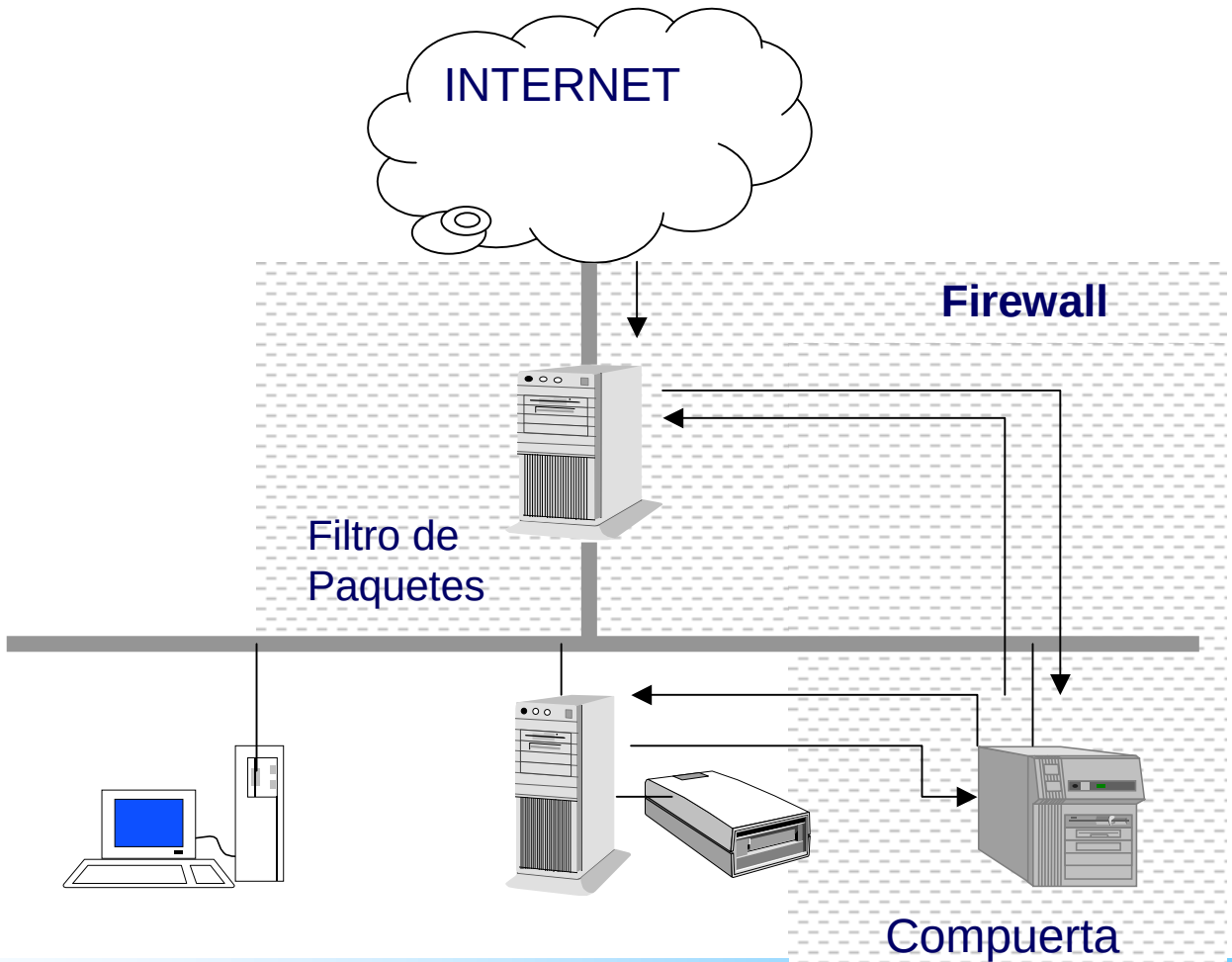
acces-list 101 permit tcp 132.124.23.0 0.0.0.255 199.245.180.0 0.0.0.255 eq 23 established

acces-list 101 permit tcp 199.245.180.0 0.0.0.255 132.124.23.0 0.0.0.255 eq 23

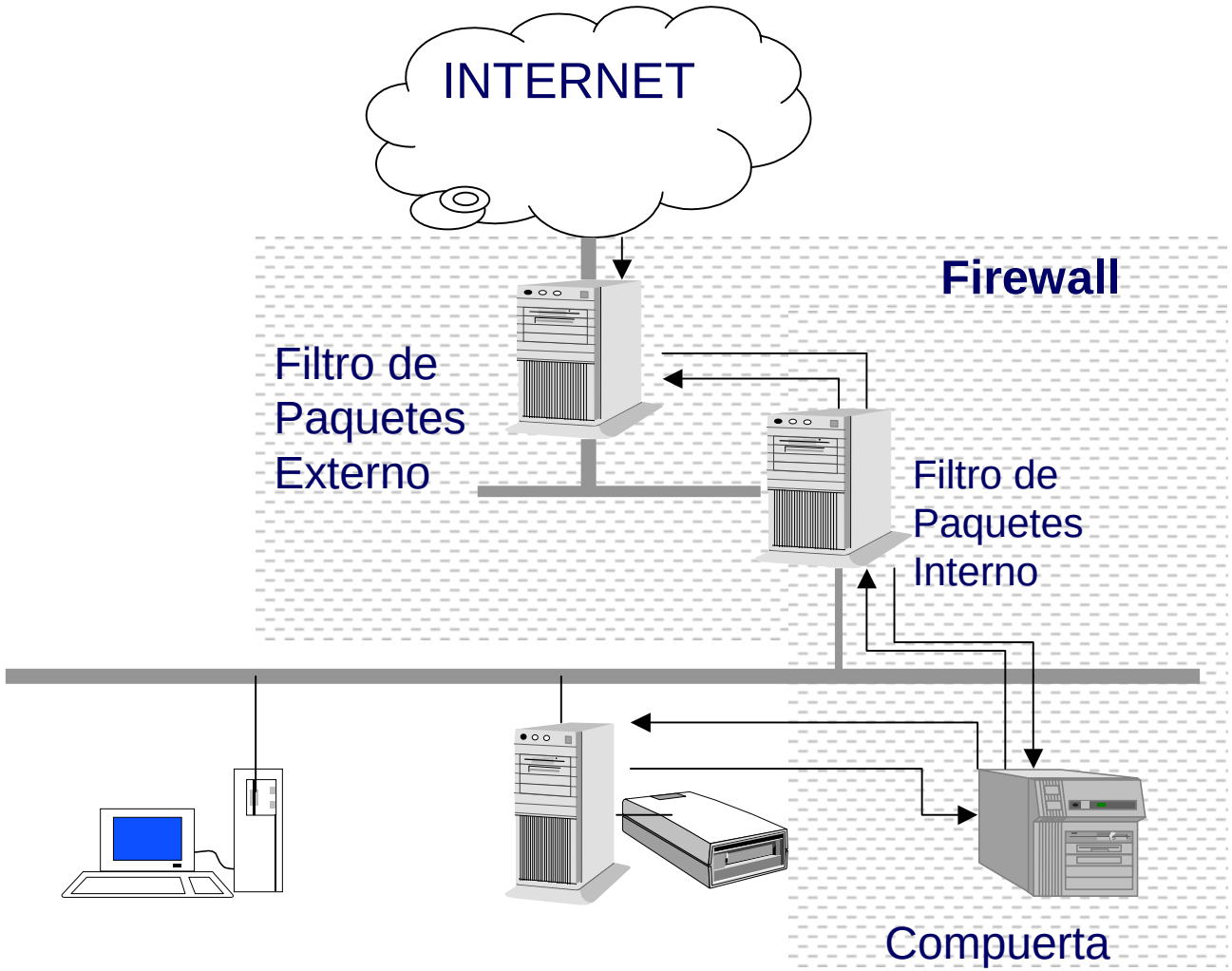
Compuertas

- Las compuertas son dispositivos, computadoras o incluso programas especialmente diseñados que se encuentran dentro del perímetro del firewall.
- Estos dispositivos reciben y manipulan adecuadamente las conexiones externas.
- Las compuertas son también conocidas como firewall bastión.

Un Firewall de un filtro y una compuerta

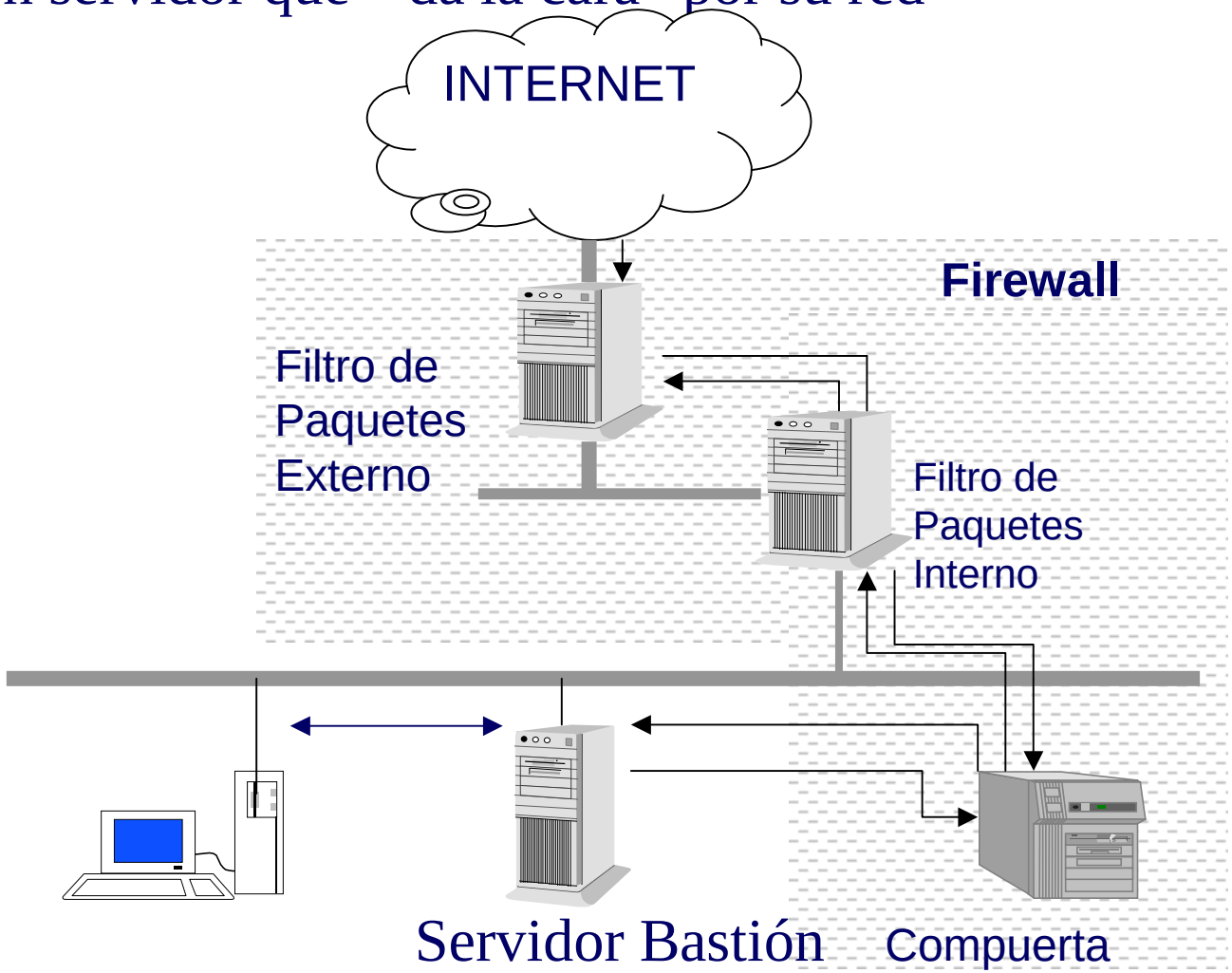


Una Compuerta y dos filtros



Servidores Bastión

Un servidor que “ da la cara” por su red



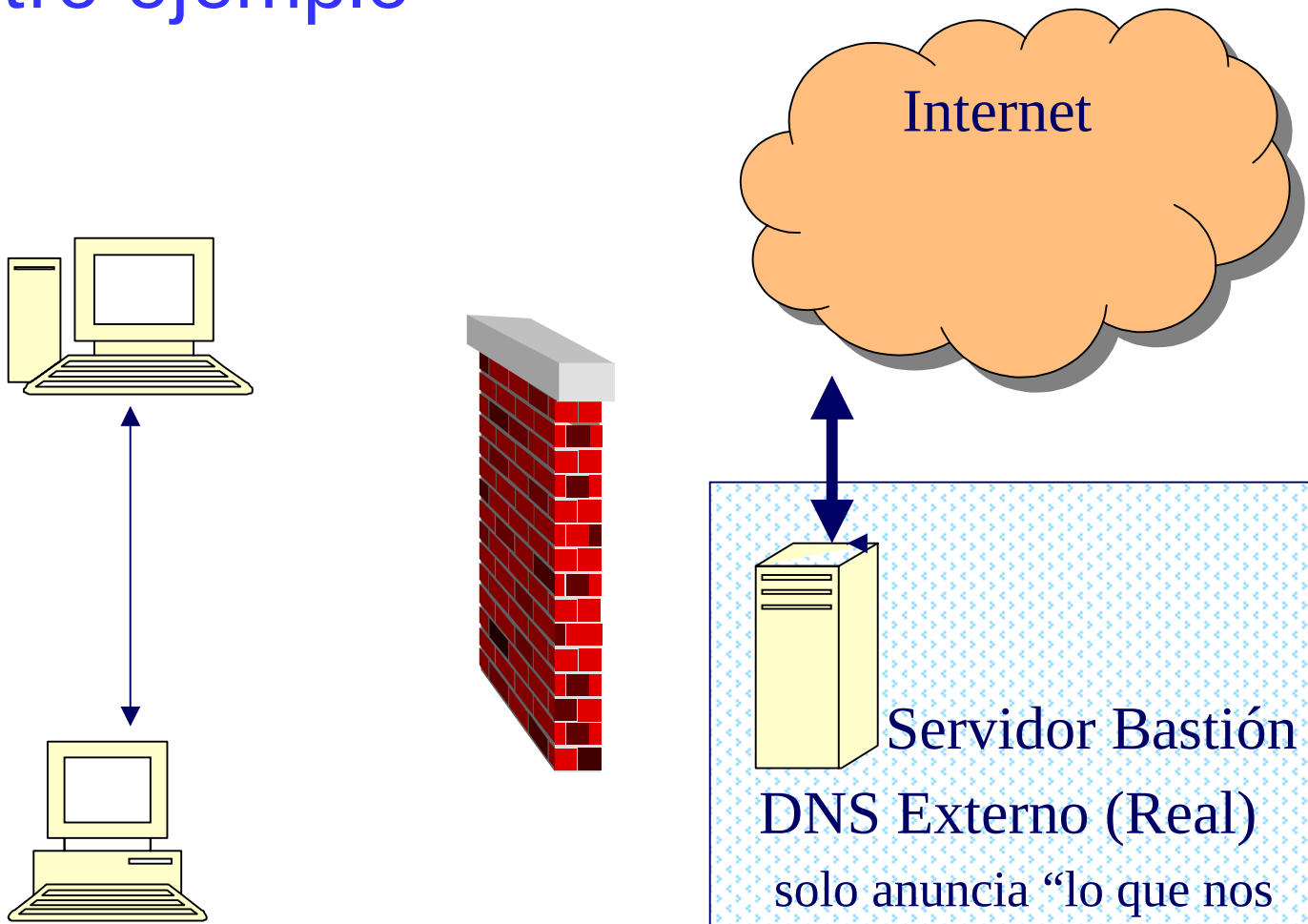
SMTP

- Envie y reciba todo el correo en el servidor bastión, nunca en los verdaderos servidores SMTP
- Utilice Filtrado de Paquetes para limitar las conexiones SMTP desde el exterior solo a los servidores bastión

El anterior es solo un ejemplo

Hagalo con todos los servicios que pueda

DNS, Otro ejemplo



Más de DNS

- No permita que sea el servidor interno quien realice las búsquedas en Internet
- Debe ser el servidor bastión quien realice las búsquedas
- Declare a su servidor bastión forwarder en la configuración de su servidor interno
- Esto le permitirá cerrar todo UDP sin problemas

Syslog

- El servidor syslog utiliza el puerto 514 UDP
- No permita que desde afuera entre mensajes a su servidor syslog, evite que un atacante inunde su servidor para cubrir su rastro

SNMP

- Los servidores SNMP escuchan 161 TCP y UDP
- Los servidores trap SNMP escuchan por el puerto 162 TCP y UDP
- No permita tráfico de entrada a los puertos 161 TCP y UDP: sus equipos no podrán ser descubiertos

X11

- Los servidores X11 permiten:
- “ Descargar” una pantalla completa
- Leer pulsaciones
- Inyectar pulsaciones

Solución:

- Filtrar los puertos 6000 + n
- Utilice servidores proxy para las conexiones X11 desde el exterior.

Hacking: Identificación del firewall

- Casi todos los firewalls comerciales emiten un rastro único, es decir, con una sencilla exploración de puertos y la captura de los mensajes los atacantes pueden determinar con facilidad el tipo, versión y las reglas de casi todos los firewalls.
- Esto puede ser de gran ayuda para reconocer las vulnerabilidades de cada uno e intentar explotarlas.

Hacking: Identificación del firewall cont..

- Exploración de puertos específicos
  - Ej: El Proxy Server de Microsoft lo hace a través de los puertos 1080 y 1745
- Solución:Bloquee en el enrutador de borde el acceso a esos puertos. Una lista de acceso puede realizar esta función:
    - Access-list 101 deny tcp any any eq 1080
    - Access-list 101 deny tcp any any eq 1745

Hacking:Buscar al que no responde

- Casi ningún firewall responde a mensajes ICMP con TTL caducados y esto los delata.
- Solución:Para evitar que un simple traceroute identifique a nuestro firewall podríamos deshabilitar la respuesta a paquetes ICMP caducados en todos los routers bajo nuestro control que se encuentren antes de firewall.

Exploración a través del Firewall

- Existen varias herramientas que funcionan enviando paquetes TCP al puerto de destino e informando que paquetes regresan.
- La mejor forma de no permitir este tipo de ataque es instruir a nuestro enrutador de borde que no responda a mensajes ICMP tipo 13. (admin prohibited filter).

Tunelización ICMP y UDP

- Es la capacidad de envolver los datos reales en un cabecera ICMP.
- Muchos routes permiten pasar tráfico ICMP ECHO ; ICMP ECHO REPLY y UDP por lo que son vulnerables a este ataque.
- Solución:La forma de prevenirlo es desactivar todo tráfico ICMP a través de su enrutador.

Wrappers

- Un wrapper es un programa que es utilizado para controlar el acceso a otro programa.
- TCP Wrapper intercepta los servicios manipulados por *inetd* permitiendo el acceso en función de reglas de selección bien definidas en los ficheros */etc/hosts.allow y /etc/hosts.deny.*

Como Funciona

- Busca en */etc/hosts.allow* para ver si el par *dirección de* ***origen:*** ***protocolo*** está explícitamente descrito. Si encuentra coincidencia la conexión es permitida
- Si no encontrada coincidencia, se busca en */etc/hosts.deny.* Si se encuentra coincidencia la conexión no es permitida
- Si no se encuentra ninguna coincidencia la conexión es permitida.

Los firewall no lo son todo

- Los firewalls son sin duda un valuarte importante en las estrategias de seguridad de una organización, sin embargo, no lo son todo.
- Un firewall puede fallar y si Ud. lo ha confiado todo a él, se encontrará en una situación realmente peligrosa.
- Un firewall no le protegerá de ataques internos.
- Un Firewall debe verse como un elemento más en la estrategia de defensa, pero nunca como sustituto del resto de las medidas de seguridad que hemos discutido.