Seguridad de los Sistemas Informáticos

Tema 6: Seguridad perimetral

En temas anteriores …

Dentro del esquema general de seguridad, hemos estado viendo:

1. Cómo proteger físicamente el hardware para asegurar su funcionamiento.
2. Qué medidas tomar desde el sistema operativo para intentar garantizar la disponibilidad, integridad y confidencialidad de los datos y programas alojados en el sistema.
3. Cómo protegernos de posibles ataques provenientes desde la red interna de la empresa.

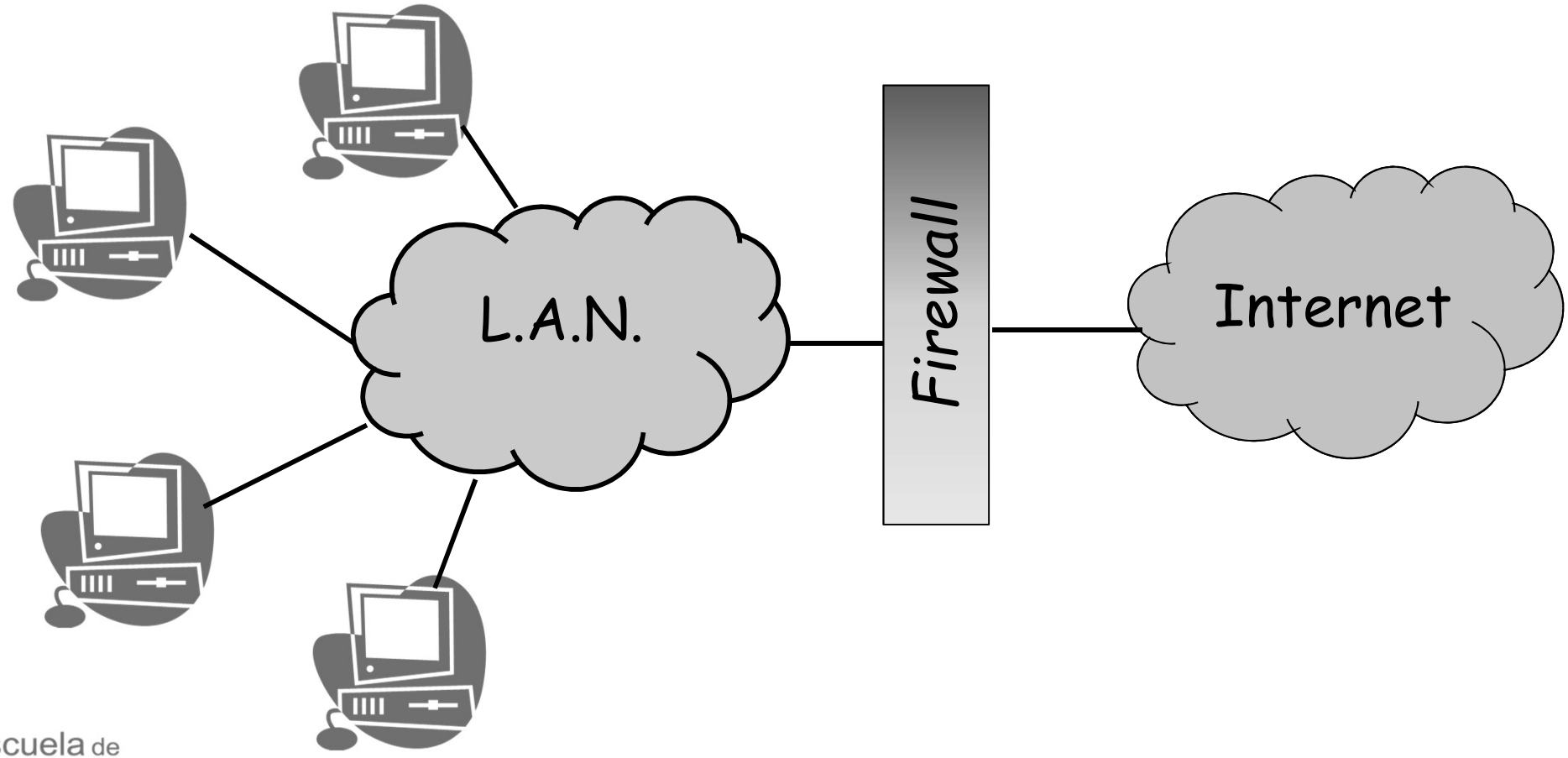
El siguiente paso en este proceso es proteger a la red de la empresa y a todos sus equipos de los posibles ataques provenientes desde el exterior de la misma. Esto constituye lo que se denomina **seguridad perimetral**.

Introducción

- Cometidos de la seguridad perimetral:
  - Rechazar conexiones a servicios comprometidos.
  - Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico) o entre ciertos nodos.
  - Proporcionar un único punto de interconexión con el exterior. (a modo de puerta, que se podrá vigilar).
  - Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet.
  - Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet.
  - Auditar el tráfico entre el exterior y el interior.
  - Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red, cuentas de usuarios internos...

Introducción

La seguridad perimetral se consigue básicamente interponiendo entre nuestra red local e Internet una protección que impida los ataques: el ***firewall*** *(cortafuegos)*



Introducción

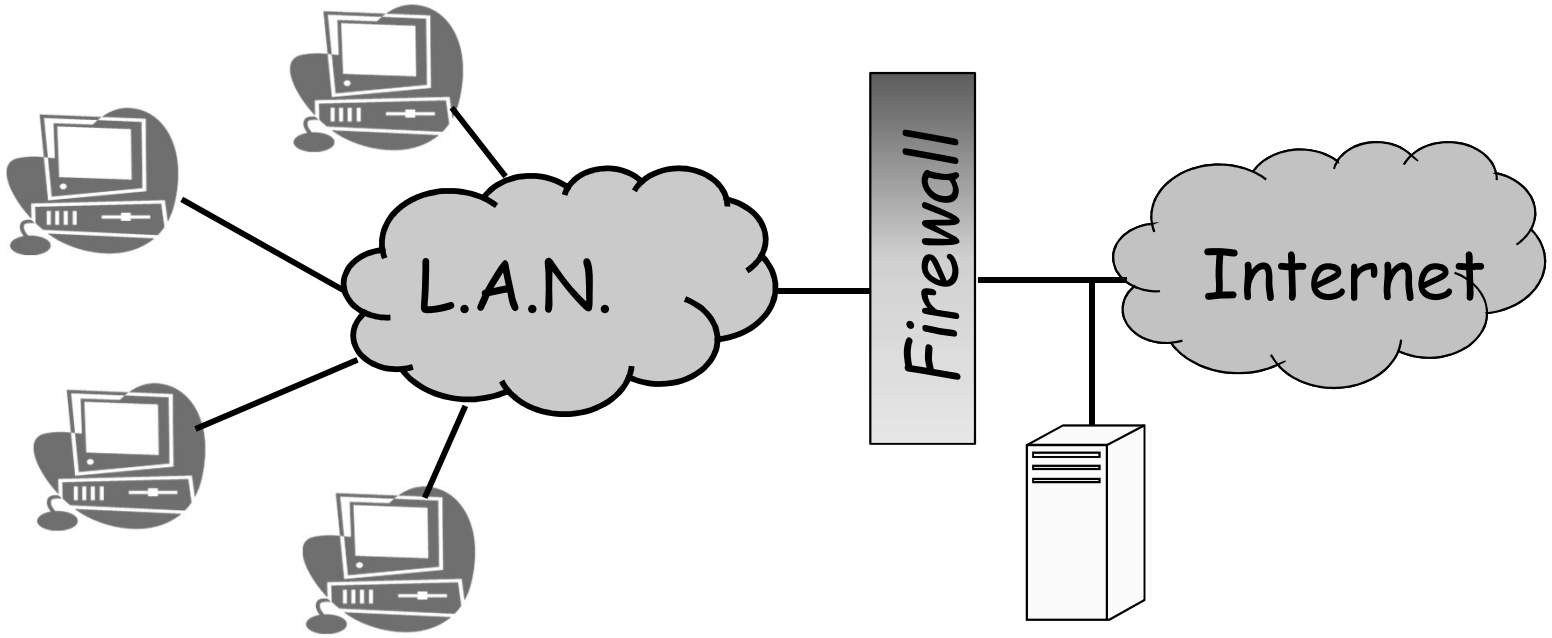
- Los cortafuegos se hicieron populares en el inicio de la década de los 90, cuando ya había una base importante de PCs conectados a Internet que no eran capaces de defenderse por sí mismos.
- Aunque se instalan generalmente para defender a una organización completa, también se pueden (suelen) encontrar en una intranet, para proteger departamentos (subredes). Para evitar que un posible atacante pueda saltar de una máquina a otra (Pivotar). (Junto a otros mecanismos como VLANs).
  - Por ejemplo, una Universidad podría separar las subredes de los Departamentos de la red principal.
- Para que la protección sea efectiva, todo el tráfico tiene que pasar por ellos.
  - ¿Redes WiFi?→problema de seguridad.

Introducción

- También existen los firewall personales o de un ordenador. Es un software que se instala en el ordenador y filtra las comunicaciones entre dicho ordenador y el resto de la red. No protegen nada más que al equipo en el que se están ejecutando.
- Permite el tráfico, entrante o saliente, según una serie de reglas definidas.
- En muchos casos viene incluido en el S.O.:
  - Firewall de Windows
  - iptables (Linux)
- Muy recomendable(obligatorio) su uso si nos conectamos en un entorno no controlado (Internet, WiFi pública, etc).

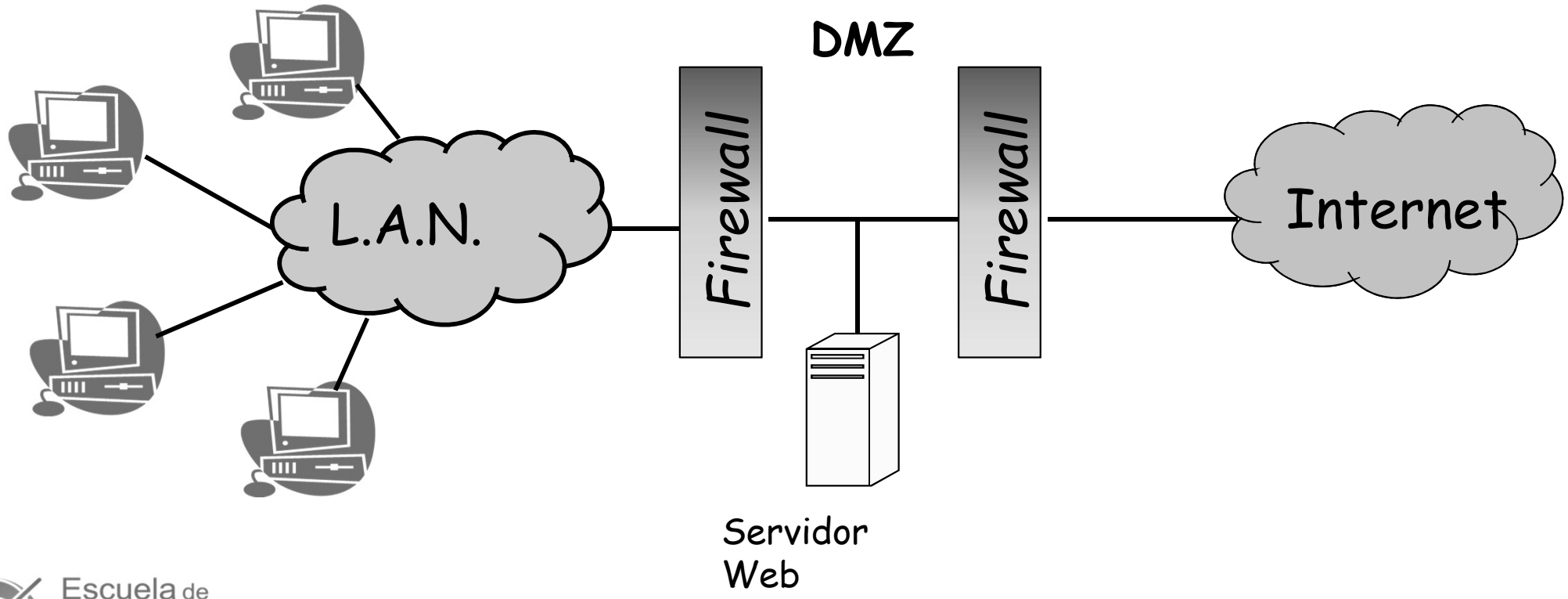
Introducción: servidores

En la estructura anterior las máquinas internas normalmente se protegen evitando cualquier tráfico no iniciado desde la propia red interna. ¿Qué ocurre entonces con servidores que deben ser accesibles desde el exterior?



Introducción: Zona desmilitarizada

Dejando el servidor web en la zona exterior (desprotegida) de nuestra red puede ofrecer los servicios al resto del mundo, pero está expuesto a los ataques de todo el mundo. En este caso puede optarse por un doble muro:



Introducción: Zona desmilitarizada

Para permitir el acceso a los servidores desde el exterior sin comprometer la seguridad de la red interior se puede definir una ***zona desmilitarizada(DMZ)****:* zona "neutral" entre nuestra red local y el "mundo exterior y hostil":

- Tendrá unos requisitos de seguridad menos estrictos que los de nuestra red local.
- Estará mejor protegida que si estuviera directamente en la red externa.

Los servidores ubicados en la zona desmilitarizada suelen denominarse ***servidores bastión****.*

Introducción: Zona desmilitarizada

Los *servidores bastión* están en una zona "delicada" de la red, por lo que deben seguirse escrupulosamente las medidas de seguridad recomendadas para los hosts:

- Debe estar preparado para los ataques porque es un host exterior. Debe estar monitorizado efectivamente.
- Debe configurarse con los **servicios mínimos** necesarios y mantenido **actualizado** por vulnerabilidades.
- Debe contar con sistemas de detección de intrusos (IDS, IPS).
- El firewall externo debe permitir únicamente los accesos a los servicios que deseemos ofrecer del servidor bastión. Debe cerrar todo acceso por defecto.

Introducción: Zona desmilitarizada

Esta estructura de dos niveles de protección sigue unas estrictas normas en cuanto al tipo de tráfico que está permitido en cada zona:

- El tráfico de la red interna con la DMZ está permitido.
- El tráfico de la red interna con el exterior está permitido.
- El tráfico de la DMZ a la red interna puede estar permitido (vigilado y con condiciones fijadas por el firewall interno).
- El tráfico de la red exterior con la red interna está prohibido (a excepción de las respuestas a peticiones iniciadas en la red interna).
- El tráfico de la red exterior con la DMZ está permitido (pero con las condiciones que establezca el firewall externo).
- El trafico de la DMZ con la red exterior está permitido.

Dispositivos de interconexión

En lo visto hasta ahora las distintas redes se interconectaban utilizando un dispositivo denominado *firewall*. Este término tiene múltiples acepciones, dependiendo muchas veces de cuestiones comerciales.

- Hablando de forma genérica, un *firewall* o *cortafuegos* es un dispositivo (hardware o software) que interconecta dos redes y que puede llevar a cabo algún tipo de control sobre el tráfico que circula por él.
- La principal misión de un firewall es separar el tráfico del resto del mundo (no confiable) del tráfico de la red interna (confiable).

En resumen, un firewall hace la función de "portero de discoteca": *quien el firewall decide pasa y el que no le gusta no pasa.*

Funciones básicas del cortafuegos

- Para que un elemento que separa el tráfico de dos redes pueda considerarse un firewall debe tener, al menos, las siguientes funciones:
  - Filtrado de paquetes *(cortafuegos de capa de red*).
  - NAT (en caso necesario).
  - Proxy de aplicación (*cortafuegos de capa de aplicación*).
  - Monitorización y registro.
- Adicionalmente, algunos firewalls pueden soportar:
  - Caché de datos.
  - Filtrado de contenido.
  - Sistemas de detección de intrusos.
  - Equilibrado de carga.

Lo que el cortafuegos no puede evitar

- Un cortafuegos bien utilizado puede librarnos de muchos problemas. Sin embargo, hay amenazas ante las cuales es inútil:
  - Ataques desde dentro, dado que no atraviesan el firewall.
  - Acceso a wifi situada detrás del firewall y ataque desde ahí.
  - Programas ejecutados en la Intranet que abren brechas, independientemente de que su intención no sea esa.
  - Ingeniería social.
  - Programas malignos (virus, caballos de troya, etc).
  - Administradores del firewall mal formados.
- También hay que tener en cuenta que no se puede cerrar todo el tráfico, es necesario permitir el trabajo legítimo.

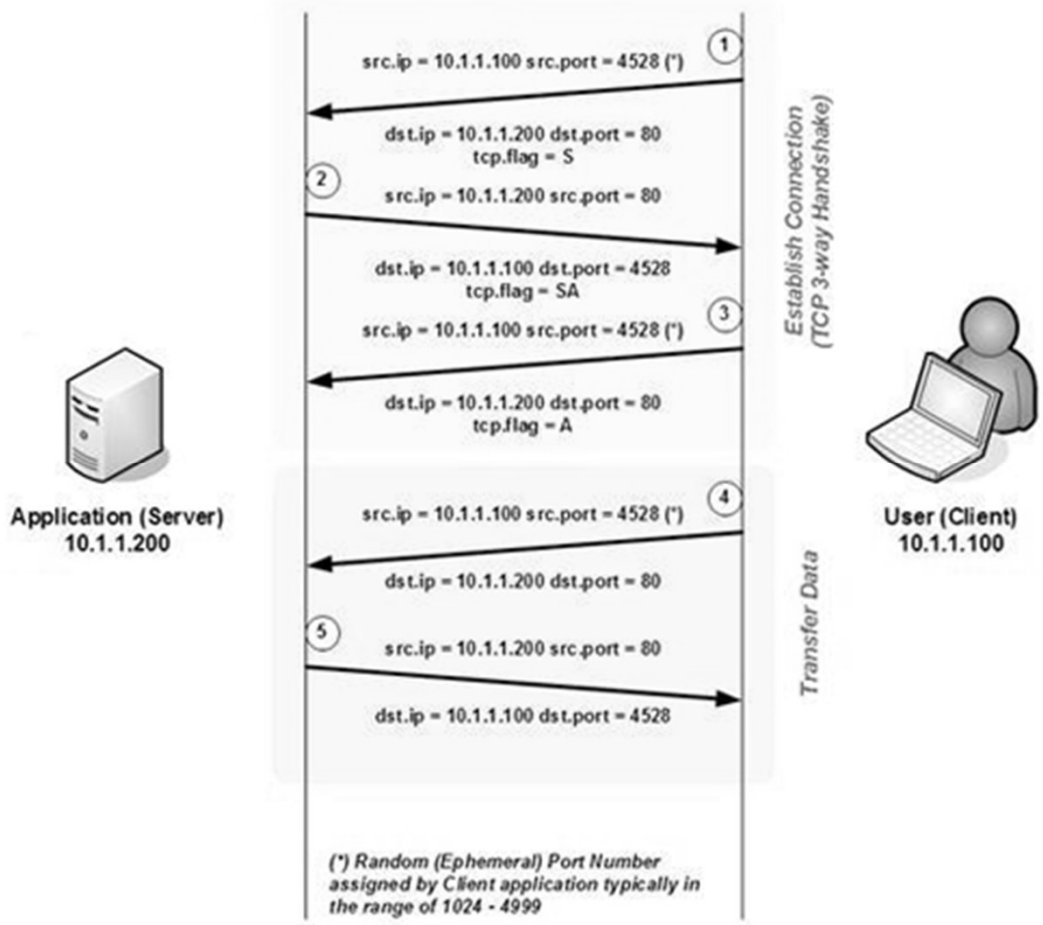
Filtrado de paquetes: Funcionamiento

- La primera función, la más básica, de un cortafuegos suele ser el filtrado de paquetes.
- El firewall examina la cabecera del paquete y, aplicando las reglas definidas, determina si puede pasar o no.
- Las reglas habitualmente permiten o bloquean accesos en función de:
  - IP de origen o IP de destino.
  - Identificador de protocolo.
  - Puerto (TCP o UDP) de destino.
  - Tipo de mensaje (ICMP, por ejemplo).
  - Otros campos de la cabecera.
- Un firewall de este tipo se suele denominar sin estado.

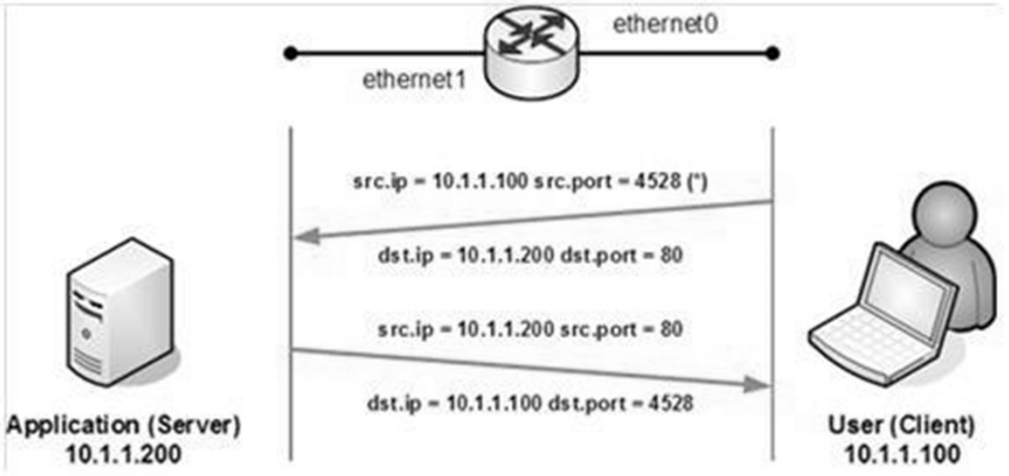
Filtrado de paquetes: Funcionamiento

- Un firewall sin estado (stateless) no tiene en cuenta si el paquete es parte de una secuencia existente de tráfico.
- Aplica reglas basándose en la información de la cabecera del paquete.
- Los puertos reconocidos (que van del 0 al 1023) están asociados a servicios ordinarios (telnet, ssh, smtp, pop3, etc.).
- El protocolo TCP tiene sesiones. Y muchos servicios (p.ej: ftp) inician la conexión en un puerto estático pero luego, de forma dinámica y aleatoria, abren una sesión entre el cliente y el servidor.
- Con un filtrado sin estado no se permite este tráfico (pues es imposible prever los puertos que deben autorizarse o prohibirse).
- Para solucionar este problema aparecen los firewall con estado (stateful), que toman en cuenta el estado de los paquetes previos cuando se definen las reglas de filtrado.
- Desde el momento en que se autoriza una conexión todos los paquetes que pasan por esa conexión serán aceptados implícitamente.

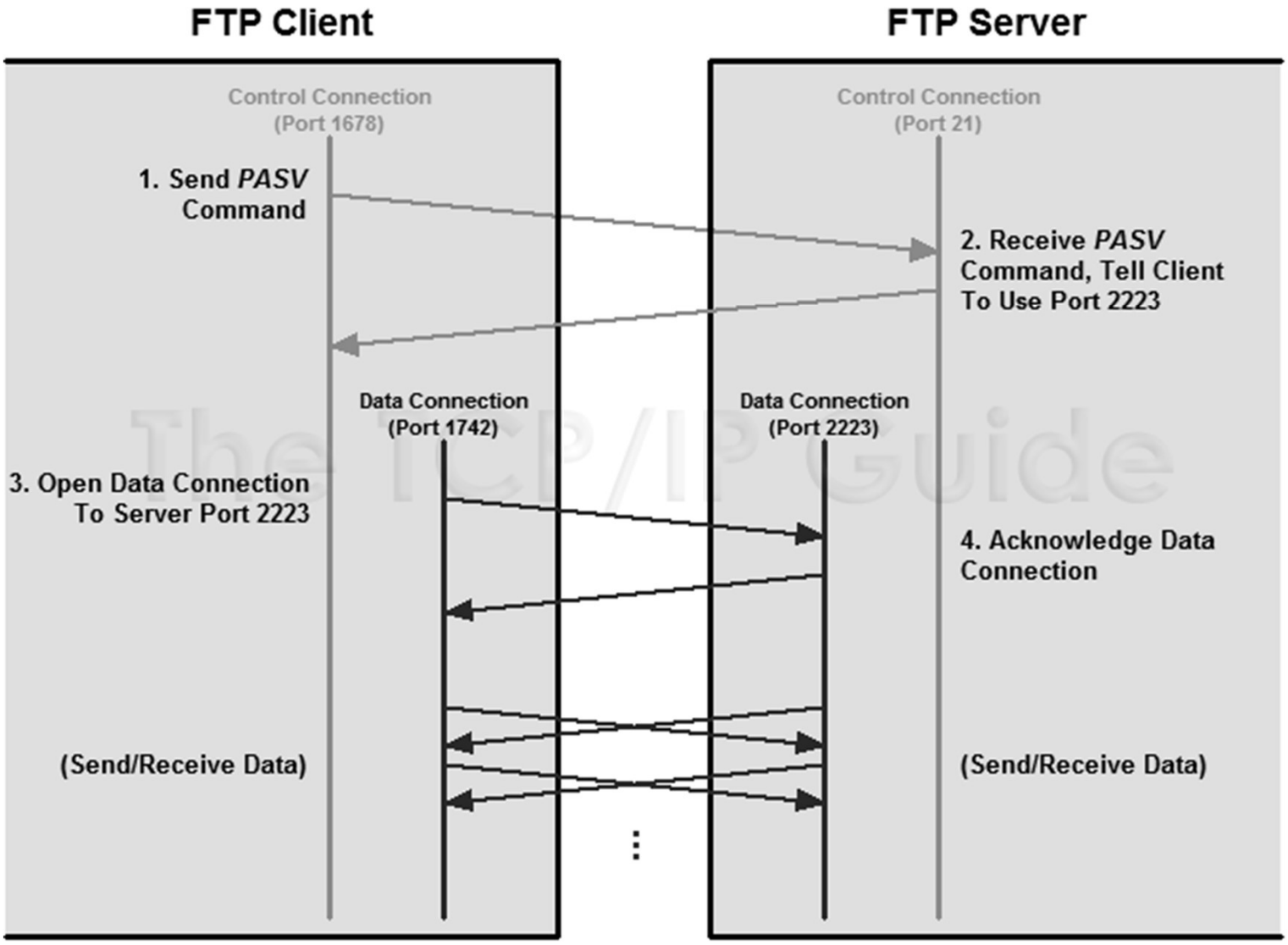
Filtrado de paquetes: Firewall sin estado



Es posible hacer *spoofing*.
Un atacante sólo necesita fijar su IP y responder desde el puerto 80 para que se le permita pasar.



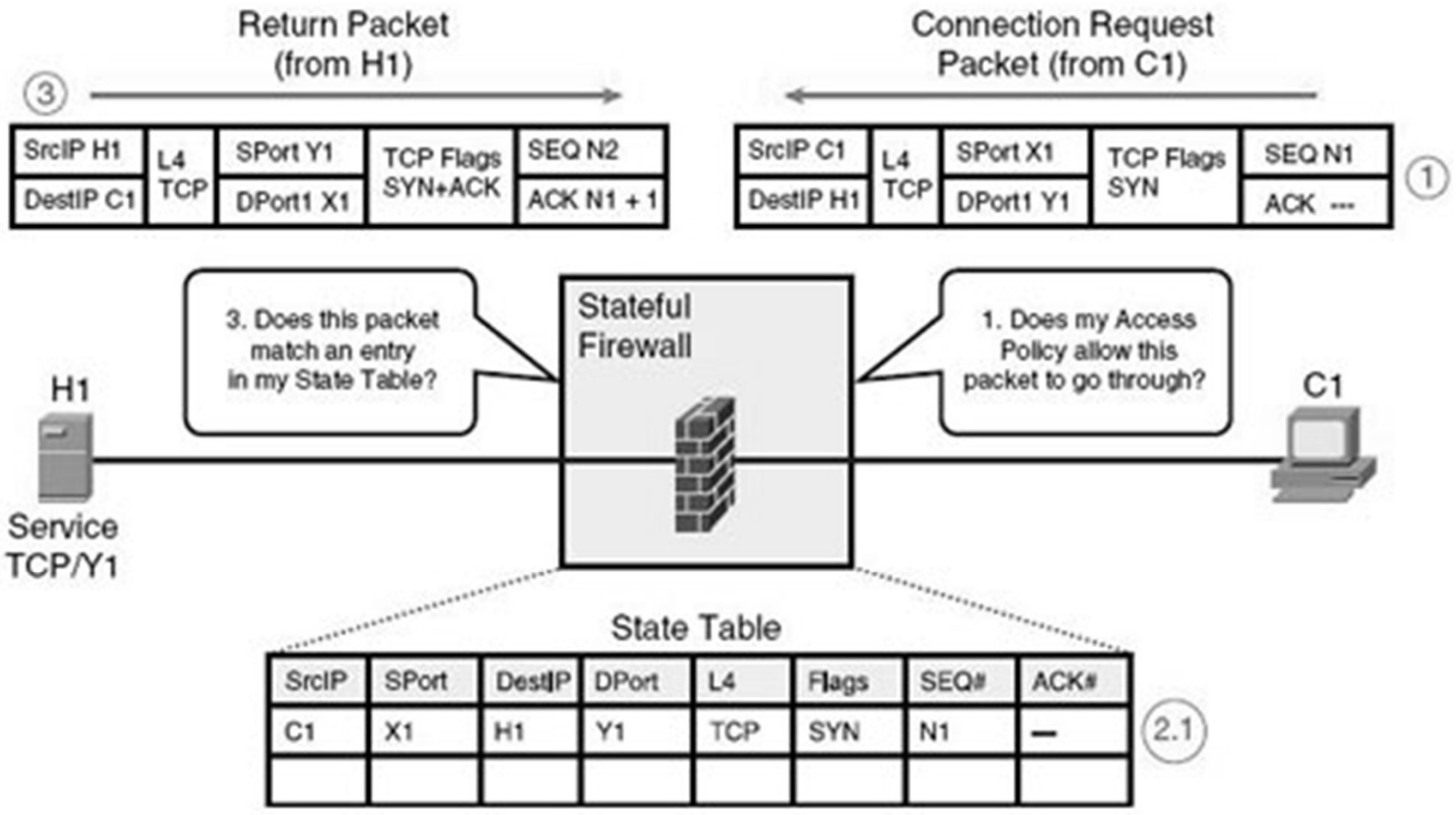
Filtrado de paquetes: Funcionamiento



Filtrado de paquetes: Funcionamiento

- Un firewall con estado intenta rastrear el **estado** de las conexiones mientras filtra paquetes
  - Trabaja a nivel de capas de Red y de Transporte (3 y 4).
  - Cuando se encuentra con un paquete (o varios) relacionados con el establecimiento de una nueva conexión, añade una nueva entrada a una tabla.
  - Desde ese momento, acepta (en general) todos los paquetes relacionados con la conexión ya establecida y anotada.
  - Rechazará paquetes no asociados a ninguna conexión abierta.
  - Ejemplo: no admitir más de 25 pings enviados desde la misma IP.

Filtrado de paquetes: Funcionamiento



Overview of Stateful Firewalls

Filtrado de paquetes:
Políticas de aplicación de reglas

Un cortafuegos aplica una serie de reglas, definidas por el administrador, a cada paquete que pasa por él. Como resultado, puede retransmitir el paquete o no.

A la hora de determinar las reglas para examinar los paquetes y protocolos, se puede optar por una de estas dos estrategias:

- **Aceptar por defecto** *(allow-all):* se especifican las reglas para rechazar paquetes.
- **Rechazar por defecto** *(deny-all):* se especifican las reglas para aceptar paquetes.

Aparentemente la primera es más sencilla de llevar a cabo. Sin embargo, la segunda es más segura (es más fácil definir el "comportamiento correcto" que enumerar todos los posibles "incorrectos").

Filtrado de paquetes:
Orden de aplicación de reglas

A la hora de aplicar un conjunto de reglas, el resultado puede variar en función del orden en que se haga. Las formas más habituales de llevar a cabo el procesado de las reglas son:

- En el orden en que están declaradas. Se usa la primera de las reglas que cuadre con el paquete IP que se está tratando.
- Primero las reglas de negación. Se buscan reglas de bloqueo que casen con el paquete actual. Si no las hay, se buscan reglas que permitan el paquete.
- "Mejor ajuste": el firewall ordena las reglas de más concretas a más generales.

Normalmente se aplica una combinación de estas técnicas.

Filtrado de paquetes:
Orden de aplicación de reglas

Origen	Destino	Tipo	Puerto	Acción
158.43.0.0	*	*	*	Deny
*	195.53.22.0	*	*	Deny
158.42.0.0	*	*	*	Allow
*	193.22.34.0	*	*	Deny

- ¿Paquete de la red 158.42.0.0 hacia 193.22.34.0?
- ¿Paquete hacia 158.50.0.0 de 195.40.55.0 (no hay regla)?

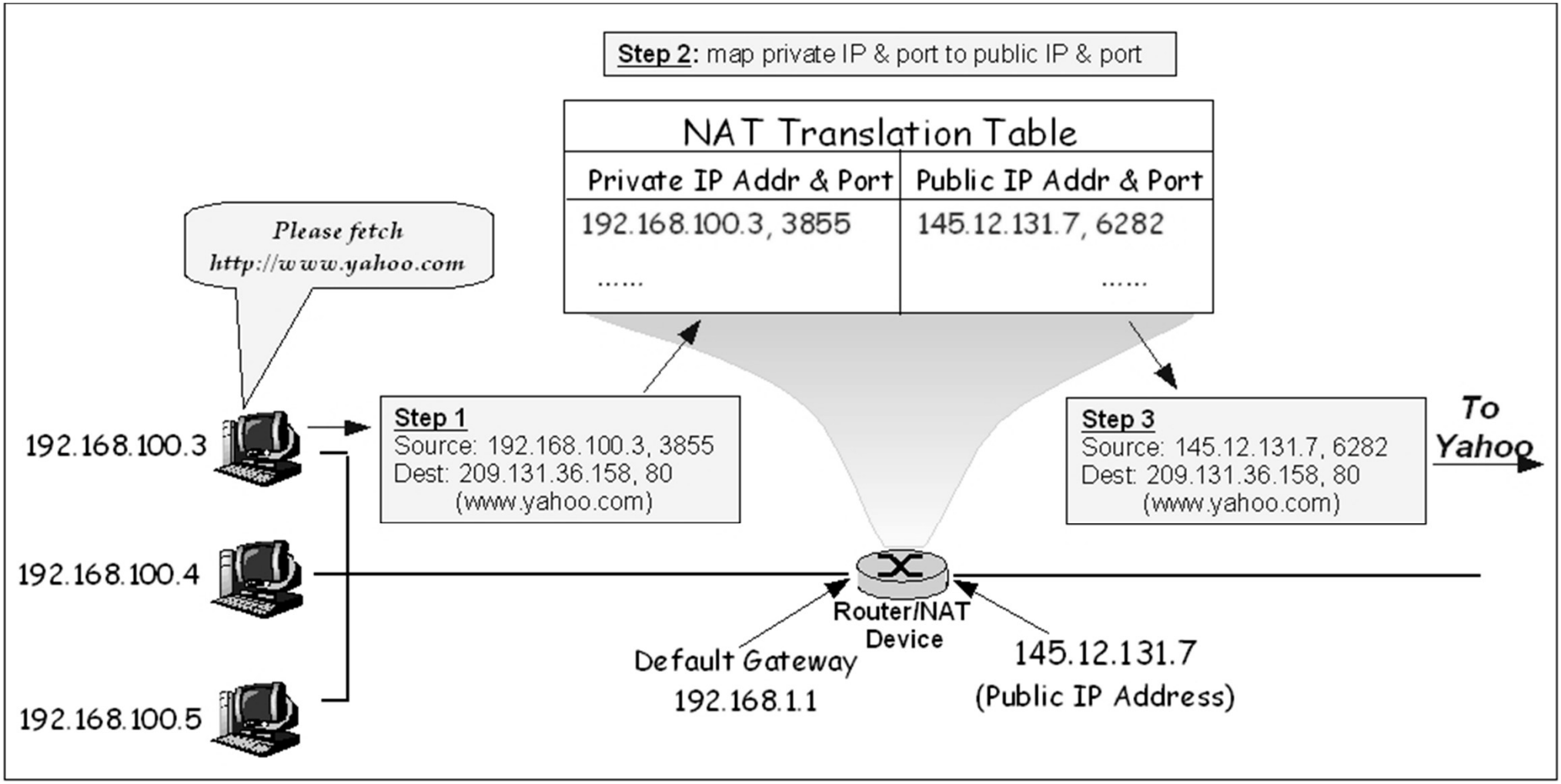
Filtrado de paquetes:
Ventajas e inconvenientes

- El filtrado de paquetes aporta una serie de ventajas:
  - Permite proteger redes enteras.
  - Son transparentes a todas las máquinas de la red.
  - Disponible en multitud de configuraciones hardware y software (desde HW dedicado hasta PCs con dos tarjetas de red).
- Pero también hay una serie de problemas con su uso:
  - En general, su configuración puede ser complicada.
  - Algunos protocolos no se ajustan bien a su filosofía de funcionamiento (comandos “r” de BSD).
  - Algunos tipos de políticas no se pueden implementar.

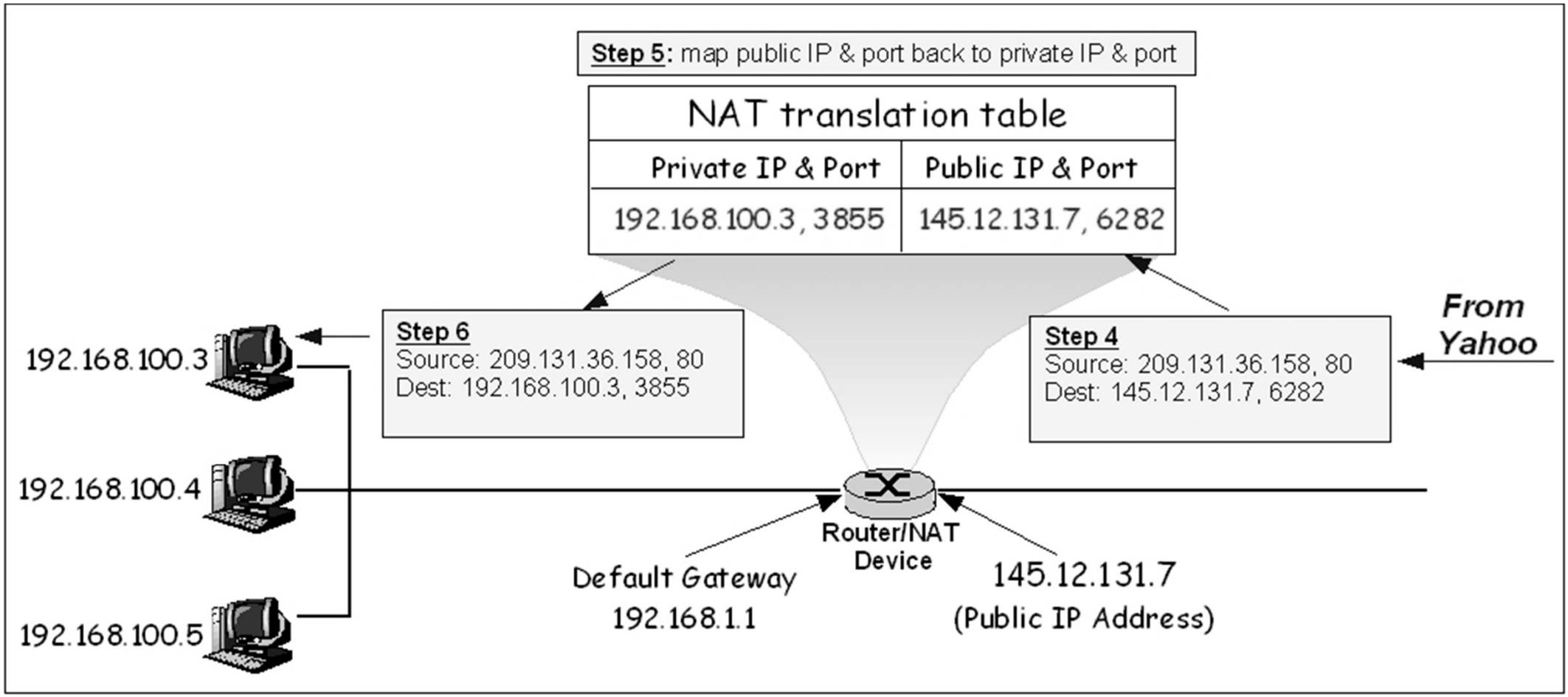
NAT

- *Network Address Translation* (NAT) se introdujo para ahorrar direcciones IP (en 2015 se estimaba que había unos 15.000 millones de dispositivos conectados a Internet y en pocos años se llegaría a 60.000). Así, toda la empresa sería vista desde fuera desde una única dirección (la del firewall).
- Internamente la red podría estar constituida como quisiéramos. Hay rangos de direcciones reservadas para uso privado y que, por tanto, nunca van a estar presentes en Internet (10.0.0.0, 172.16.0.0, 192.168.0.0)
- Todas las conexiones iniciadas desde la red interior pasan por el firewall, que almacena el origen de las peticiones, con lo que cuando se reciben paquetes de vuelta el firewall vuelve a intervenir modificando el destino (en el paquete que le llega) por el de la máquina interna.

NAT


Step 2: map private IP & port to public IP & port
NAT Translation Table
Private IP Addr & Port
Public IP Addr & Port
192.168.100.3, 3855
145.12.131.7, 6282
.....
.....
Please fetch
http://www.yahoo.com
192.168.100.3
192.168.100.4
192.168.100.5
Step 1
Source: 192.168.100.3, 3855
Dest: 209.131.36.158, 80
(www.yahoo.com)
Step 3
Source: 145.12.131.7, 6282
Dest: 209.131.36.158, 80
(www.yahoo.com)
To Yahoo
Router/NAT Device
Default Gateway
192.168.1.1
145.12.131.7
(Public IP Address)

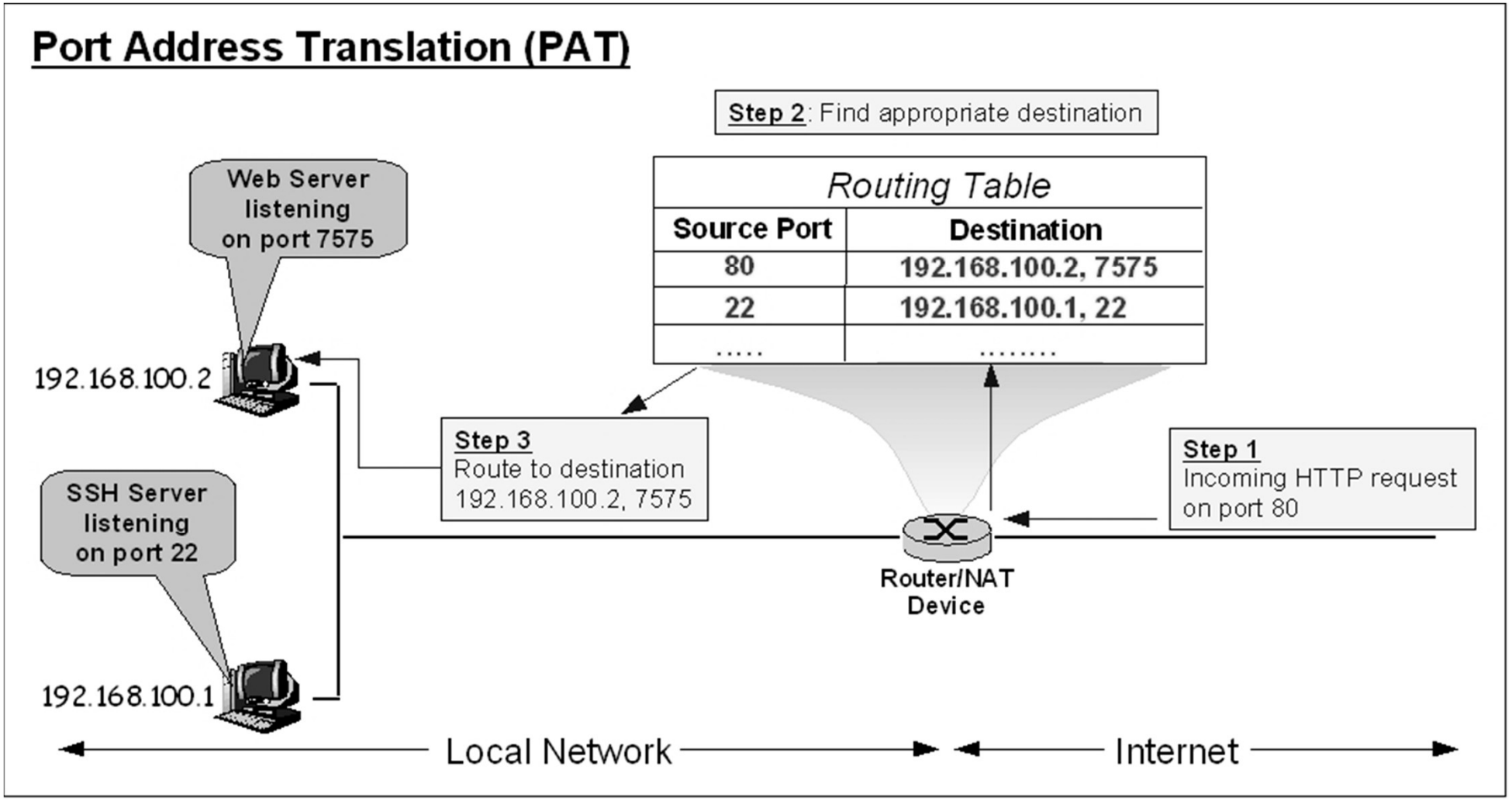
NAT


Step 5: map public IP & port back to private IP & port
NAT translation table
Private IP & Port
Public IP & Port
192.168.100.3, 3855
145.12.131.7, 6282
Step 6
Source: 209.131.36.158, 80
Dest: 192.168.100.3, 3855
Step 4
Source: 209.131.36.158, 80
Dest: 145.12.131.7, 6282
From Yahoo
192.168.100.3
192.168.100.4
192.168.100.5
Router/NAT Device
Default Gateway
192.168.1.1
145.12.131.7
(Public IP Address)

NAT

- Si quisiéramos que una máquina interna pudiera recibir peticiones directamente de la red externa podríamos utilizar la técnica *Network Address And Port Translation* (NAPT o PAT). Haríamos corresponder un puerto del firewall con un puerto de una máquina interna.
- Además de permitirnos ahorrar direcciones, desde el punto de vista de la seguridad NAT *oculta* las direcciones reales de las máquinas internas, impidiendo así ataques hacia ellas.

NAPT o PAT


Port Address Translation (PAT)
Step 2: Find appropriate destination
Routing Table
Source Port
Destination
80
192.168.100.2, 7575
22
192.168.100.1, 22
.....
.....
Web Server listening on port 7575
192.168.100.2
SSH Server listening on port 22
192.168.100.1
Step 3
Route to destination 192.168.100.2, 7575
Step 1
Incoming HTTP request on port 80
Router/NAT Device
Local Network
Internet

NAT

Ventajas e Inconvenientes

Ventajas

- Oculta tanto las máquinas internas como la topología de la red.
- Impide el acceso desde máquinas externas a las máquinas internas.
- Aumenta el número de direcciones IP disponibles.

Inconvenientes

- Algunos protocolos utilizan direcciones IP dentro de los datos de los paquetes (no sólo en la cabecera). Para los protocolos más comunes los firewalls están preparados, pero puede haber otros para los que no.
- Algunos protocolos firman los paquetes para que no sean modificados por el camino. Va a haber problemas con estos protocolos.
- Algunos protocolos multimedia también pueden tener problemas.

Proxys

- Denominados a veces gateways de aplicación, son una "versión elaborada" de los filtros IP, con un par de diferencias
  - inspeccionan la parte de datos de un paquete IP en lugar de sólo las cabeceras.
  - regeneran el paquete, en lugar de sólo dejarlo pasar.
- Trabajan a nivel de aplicación (capa 7 de la torre ISO/OSI), en lugar de en el nivel de red (capa 3).
- Todas las conexiones del protocolo que se trate pasan por el proxy: cualquier conexión que trate de evitarlo será bloqueada.
- Al trabajar con los datos, pueden incorporar una función de caché (por ejemplo, una caché web).

Otra ventaja

- Se pueden establecer filtros a nivel de contenidos:
  - Impidiendo la entrada por HTTP a paquetes de audio/video.
  - Impidiendo la entrada por HTTP o FTP a ficheros que contengan algunas palabras clave.
  - Impidiendo la entrada por SMTP a mensajes de conocidas fuentes de spam.

Proxys

Inconvenientes

- Debe haber un proxy por cada protocolo (http, ftp, …)
- Los clientes deben configurarse para utilizar el proxy.
- No se pueden filtrar los contenidos de protocolos como HTTPS o SSH.
- Hoy en día hay muchos servicios que usan HTTP en el puerto 80, lo cual hace más difícil saber qué tráfico en este puerto es legítimo y cuál no.
- La utilización de túneles (envío de datos de un protocolo encapsulados dentro de otro protocolo) niega directamente el propósito del proxy.
- Si el proxy no está operativo los clientes no pueden conectarse mediante ese protocolo.

Proxys

Túnel

- Un túnel consiste en el envío de datos de un protocolo A encapsulados dentro de otro protocolo B. Al ser analizados los paquetes el proxy determina que es del protocolo B.
- Por lo tanto se puede conseguir establecer una comunicación con un protocolo “no permitido” si se encapsula a través de uno que sí lo sea.
- Cada vez más protocolos usan HTTP o SSH como túnel.
- Por ejemplo Samba (SMB) permite compartir ficheros a través de la red, pero no es seguro. Si se encapsula mediante un túnel Secure Shell (SSH) la información viaja de forma cifrada. Si alguien la intercepta no puede acceder a ella por estar cifrada.

Monitorización y registro

- Un firewall debe incorporar estas funciones por distintos motivos:
  - Informe de utilización.
  - Detección de intrusos.
  - Aprendizaje de técnicas de ataque.
  - Evidencia legal.
- Los firewalls deben configurarse para almacenar la mayor cantidad posible de información sobre los accesos. Para una mayor seguridad puede ser aconsejable almacenarlos en otra máquina o en dispositivos *write-once.*

Funciones Avanzadas
Detección de intrusos

- Los firewalls actualmente pueden aplicar un conjunto de reglas para saber si un determinado patrón de paquetes se debe a tráfico normal o a intentos de intrusión.
- Las reglas están basadas en comportamientos de ataques conocidos:
  - Escaneos de direcciones IP internas.
  - Escaneos de puertos de máquinas internas o del propio firewall.
  - Ping de la muerte/TearDrop/Land/Winnuke. Son ataques que aprovechaban vulnerabilidades de algunas implementaciones del protocolo TCP/IP.

Funciones Avanzadas
Detección de intrusos

- Ante un ataque de este estilo, el firewall puede responder:
  - Dejando constancia en el log.
  - Informando del problema.
  - Modificando su configuración (cambiando de "modo de operación" a uno más estricto, con más logs, bloqueando todo el tráfico que llega desde una determinada red o a un puerto específico, …)
  - …

Funciones Avanzadas

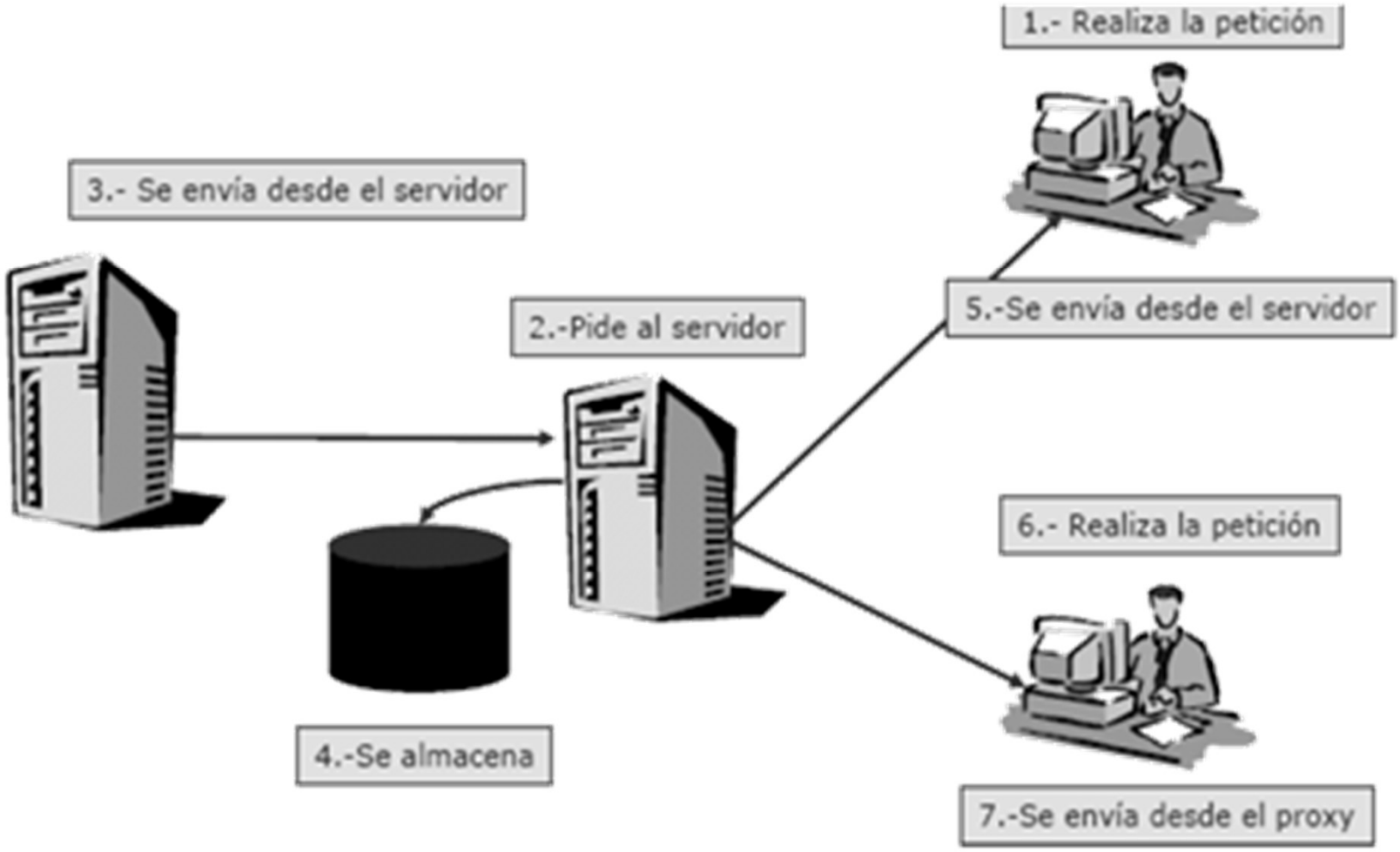
Caché

Para mejorar el rendimiento del firewall se pueden incorporar dos funciones al mismo (cuando actúan como *proxys*): caché y equilibrado de carga

- **Caché**: función típica de los *proxys* web.
  - Mejora el rendimiento en dos aspectos:
    - Respuesta más rápida a las peticiones de la red interna.
    - Disminución del tráfico que sale al exterior.
  - Hay varias técnicas para gestionar la caché de forma efectiva (caché activa, precarga de contenidos, caché jerárquica, caché distribuida, …).
  - No todas las páginas pueden ser “cacheadas” (por ejemplo la web de un banco).

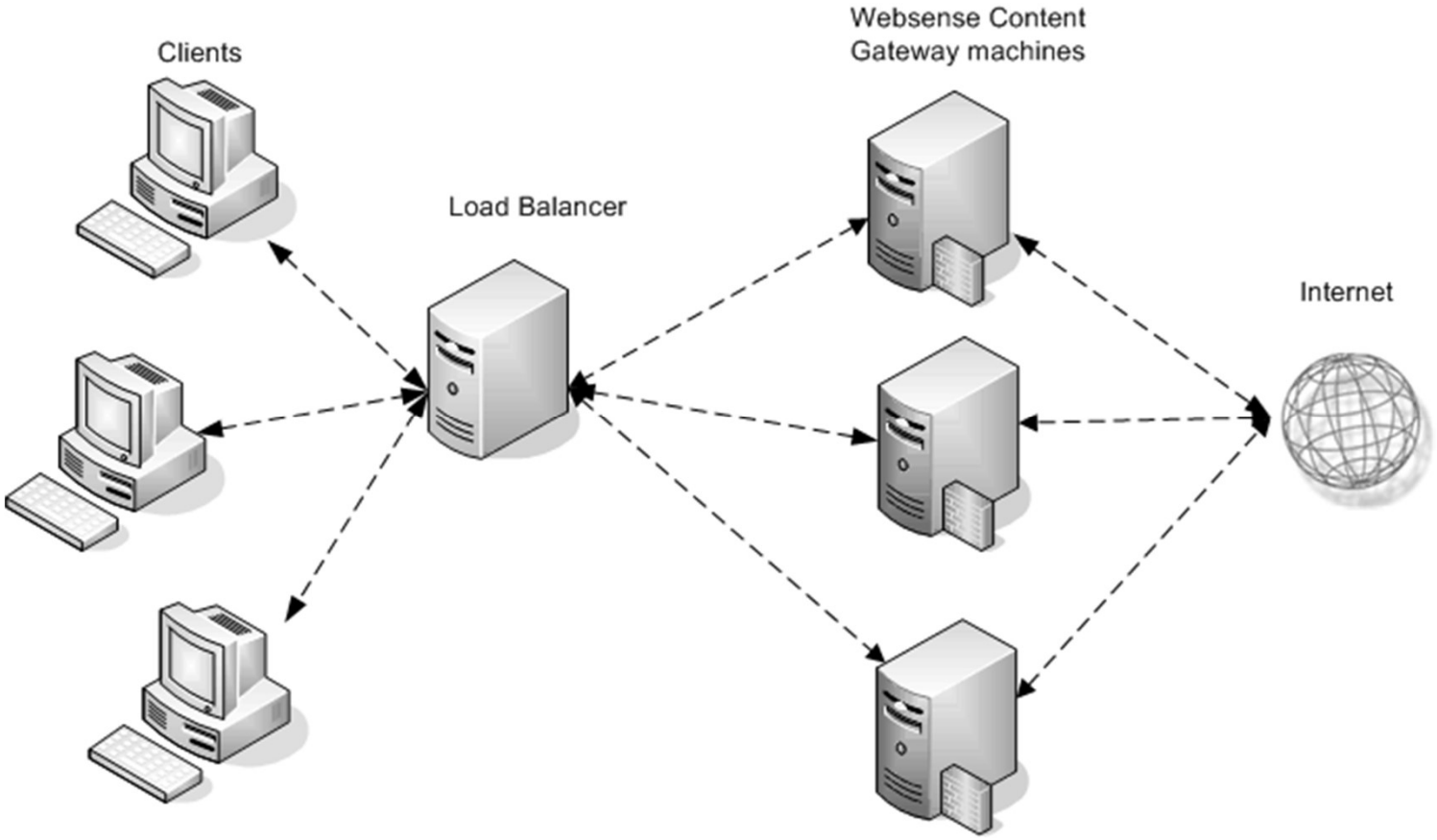
Funciones Avanzadas

Caché



Funciones Avanzadas
Equilibrado de carga

- **Equilibrado de carga**: se pueden utilizar grupos de máquinas para hacer el trabajo, logrando mejorar el rendimiento y aumentando la tolerancia a fallos.



Honeypots

- Un ***honeypot*** (tarro de miel) es una herramienta utilizada para atraer y analizar el comportamiento de los atacantes.
  - Para conocer cómo se realizan los ataques.
  - Incluso para descubrir nuevas vulnerabilidades.
  - Aunque parezca una contradicción con respecto a todo lo dicho hasta el momento al respecto de la seguridad.
- Se pueden clasificar en:
  - Puros
    - Sistemas de producción reales.
    - Las actividades del atacante son monitorizadas a través de la conexión de red del equipo.

Honeypots

- De alta interacción
  - Imitan las actividades de sistemas reales que tienen desplegada una gran cantidad de servicios.
  - Cualquier intento de acceso al mismo se debe considerar sospechosa.
  - En los últimos tiempos se ejecutan como máquinas virtuales, para poder ser restaurados rápidamente en caso de necesidad.
- De baja interacción
  - Simulan únicamente los servicios más atacados usualmente.
  - Por ejemplo, un servidor de correo que acepta conexiones y permite escribir un correo en ellas, pero nunca llega a enviarlos.

Honeypots

- Un ***honeymonkey*** (Microsoft Research) está basado en el concepto de *honeypot*
  - Funciona como un sistema automático de navegación que visita todo tipo de páginas web para que alguna de ellas intente sacar partido de alguna vulnerabilidad del navegador.
  - Antes de visitar cada sitio se saca una instantánea de la memoria, los ejecutables y el registro del *honeymonkey*.
  - Después de la visita, se comparan las copias guardadas con los valores actuales para estudiar los posibles cambios
    - Básicamente, si se ha instalado algún tipo de *malware* o se ha cambiado algo que no debería.
  - Así se podrían encontrar vulnerabilidades todavía no publicadas pero ya en proceso de explotación.

Acceso externo a la intranet

- Hemos visto cómo impedir el acceso externo a la intranet pero existen muchas circunstancias en las que puede ser necesario facilitar el acceso a la intranet (total o parcialmente) desde el exterior, normalmente haciendo uso de Internet.
  - Empresa con varias sedes que necesitan estar conectadas (sin usar conexión dedicada).
  - Teletrabajo. Trabajadores de la empresa que realizan su trabajo desde "casa" (sin conexión dedicada).
  - Empleados móviles. Empleados que viajan y pueden tener que conectarse desde hoteles, cafeterías, mediante usb dongle, etc.
  - Empresas asociadas. Empresas que pueden ser colaboradoras y a las que se les da acceso a ciertos recursos de la intranet.

Acceso externo a la intranet

- Existen muchas formas para proveer este acceso desde el exterior:
  - Usando VPN
  - RDP/VNC
  - Programas de acceso remoto
  - Sistemas de virtualización y publicación de aplicaciones y/o escritorio
- Habitualmente se utilizan de forma combinada.

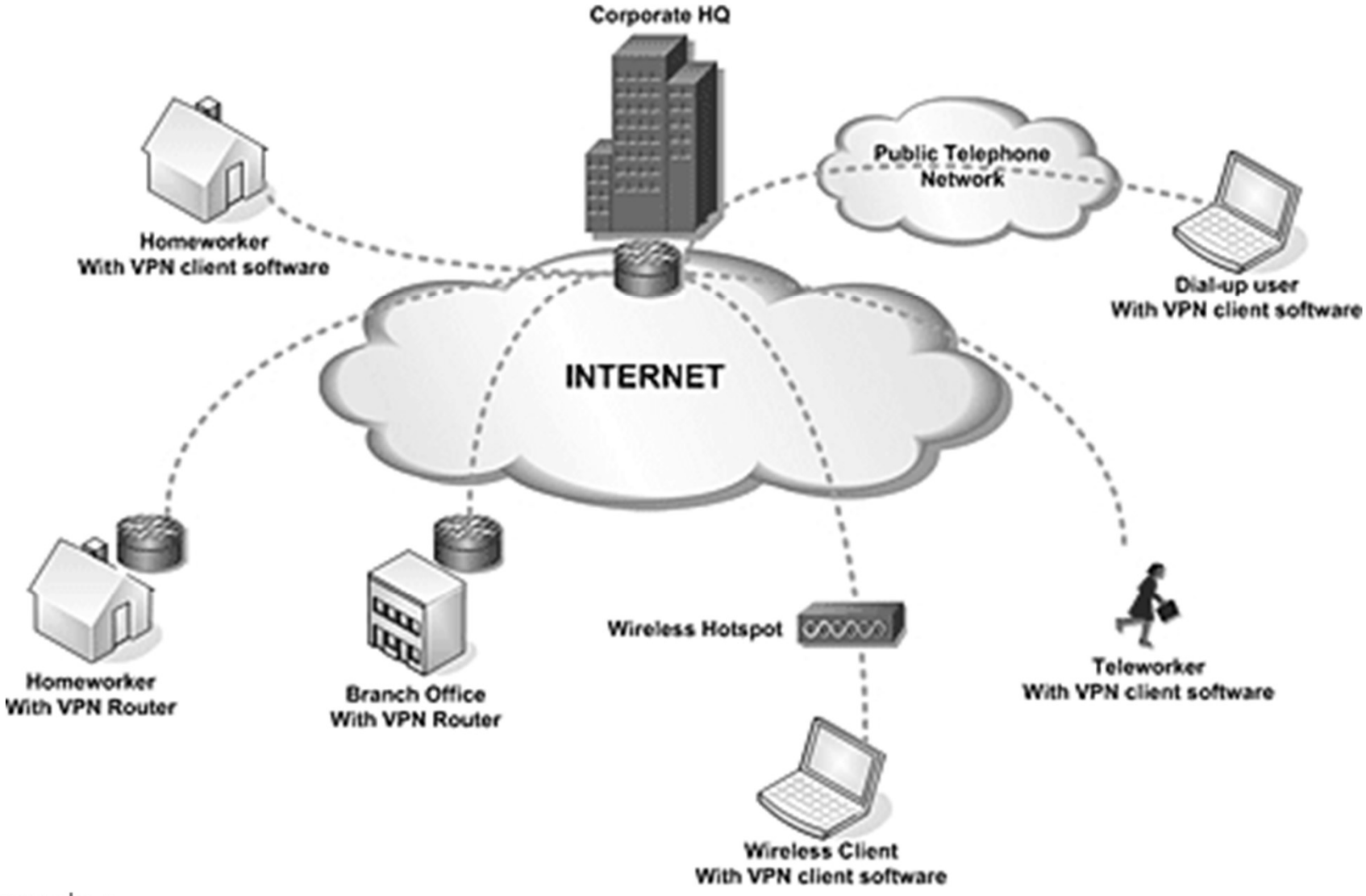
Red Privada Virtual - VPN

- Hay veces que es necesario poder acceder desde Internet a nuestra red interna directamente. Por ejemplo:
  - Si tengo “comerciales” que viajan continuamente puedo necesitar que sus ordenadores tengan forma de conectarse a la red interna “como si estuvieran físicamente en la red”.
  - Si tenemos dos o más sucursales de un empresa que se conectan a través de internet para que compartan recursos.

Red Privada Virtual - VPN

- Para solucionar ese problema podemos crear una Red Privada Virtual – VPN (Virtual Private Network) que permite extender de forma segura una red local sobre una red no controlada como puede ser Internet.
- Permite que un equipo envíe y reciba datos a través de Internet con todos los servicios, recursos y seguridad de la Intranet.

Red Privada Virtual - VPN



Red Privada Virtual - VPN

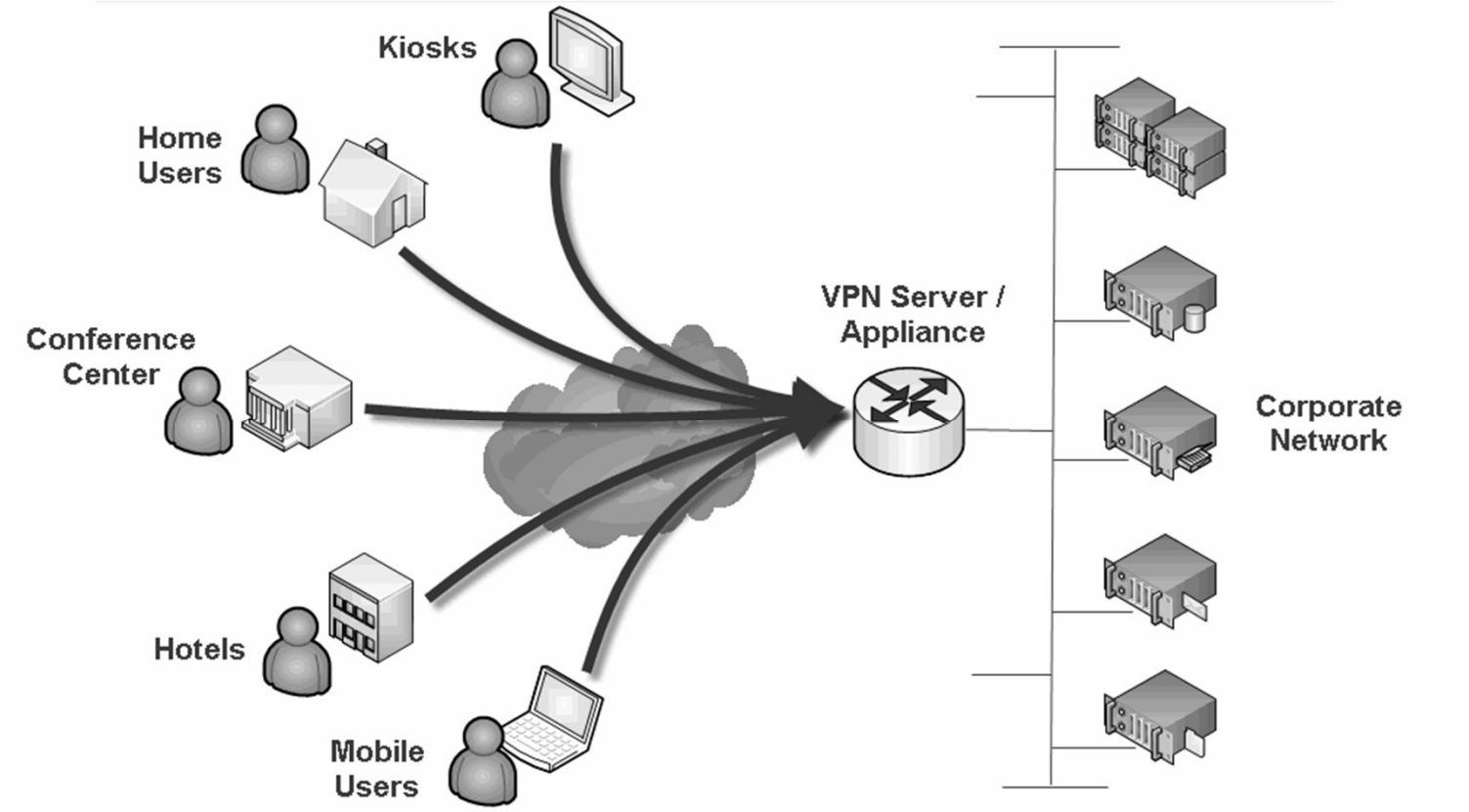
- Existen muchas implementaciones.
- El protocolo más extendido es IPSEC, pero hay otros como PPTP, SSL/TLS, SSH, etc.
- La VPN se puede conseguir mediante
  - Dispositivo Hardware: Fortinet, SonicWall, Cisco, Juniper, etc…
  - Aplicación Software: OpenSSH, OpenVPN, etc.

Red Privada Virtual - VPN

- Podemos distinguir tres tipos de VPN:
  - VPN de acceso remoto.
  - VPN punto a punto.
  - VPN over LAN

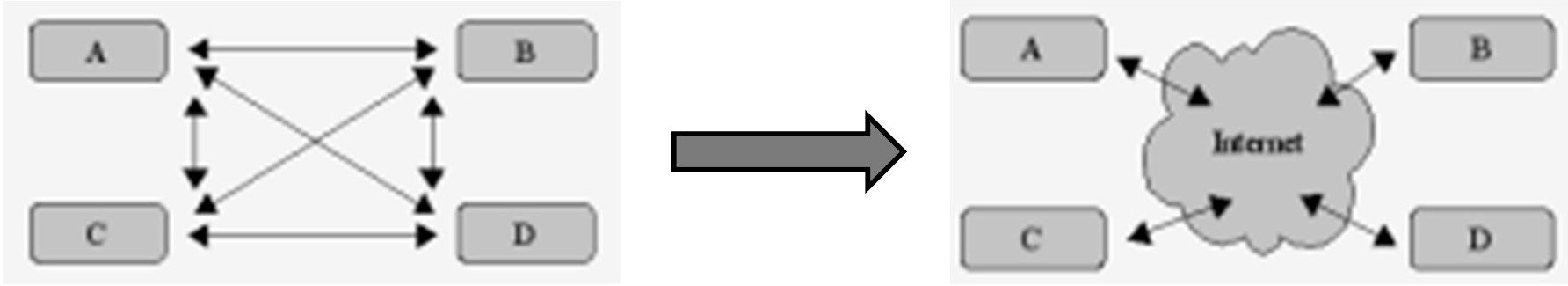
Red Privada Virtual - VPN

- VPN de acceso remoto:
  - Un usuario (o quien sea) se conecta con la empresa desde un sitio remoto (hotel, cafetería, casa, etc.) utilizando Internet para acceder.
  - Es el más usado actualmente.



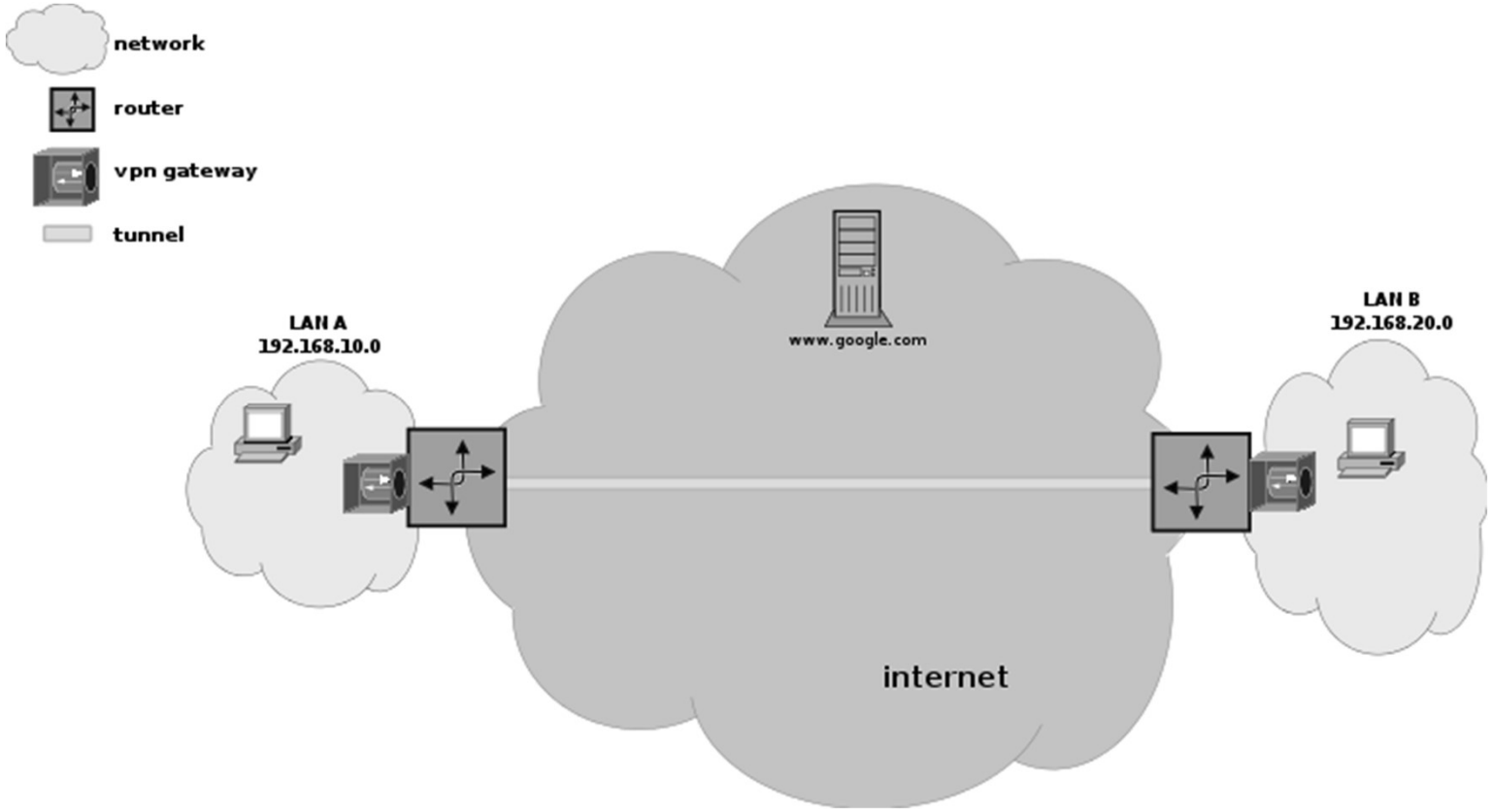
Red Privada Virtual - VPN

- VPN punto a punto
  - Se utiliza para conectar distintas sedes a la misma red. Esto permite eliminar los costosos vínculos físicos punto a punto.
  - El servidor VPN mantiene un vínculo permanente entre las sedes.



Red Privada Virtual - VPN

- VPN punto a punto
  - Se suele utilizar tunneling.



Red Privada Virtual - VPN

- VPN over LAN.
  - Es una variante del acceso remoto pero empleando la LAN para establecer la comunicación.
  - Sirve para aislar zonas o servicios dentro de la intranet.
  - No todos los departamentos dentro de la intranet pueden acceder a todo.
  - Ej: Universidad, con empleados diseminados por varios campus.

VNC

- VNC (Virtual Network Computing) es un programa de software libre, de arquitectura cliente/servidor que permite tomar el control del teclado y ratón del servidor desde el cliente.
- En el servidor se ejecuta un programa que captura la pantalla y la envía al cliente, el cuál envía los movimientos del ratón y las pulsaciones del teclado.
- En el servidor se puede ver qué está haciendo el cliente (se visualiza la misma consola).
- Existen versiones para diversos sistemas operativos. Cliente y servidor pueden ser de distintos S.O.
- Existen versiones en las que el servidor puede ser http, permitiendo la conexión mediante un navegador.

RDP

- RDP (Remote Desktop Protocol) es un protocolo propietario de Microsoft que permite la ejecución de aplicaciones (y del escritorio) de un servidor en una terminal del cliente.
- La información de la pantalla es capturada en el servidor y enviada al cliente, que a su vez envía la información del ratón y el teclado.
- En el servidor no se observa lo que hace el cliente. (existen opciones para que sí pueda hacerlo)

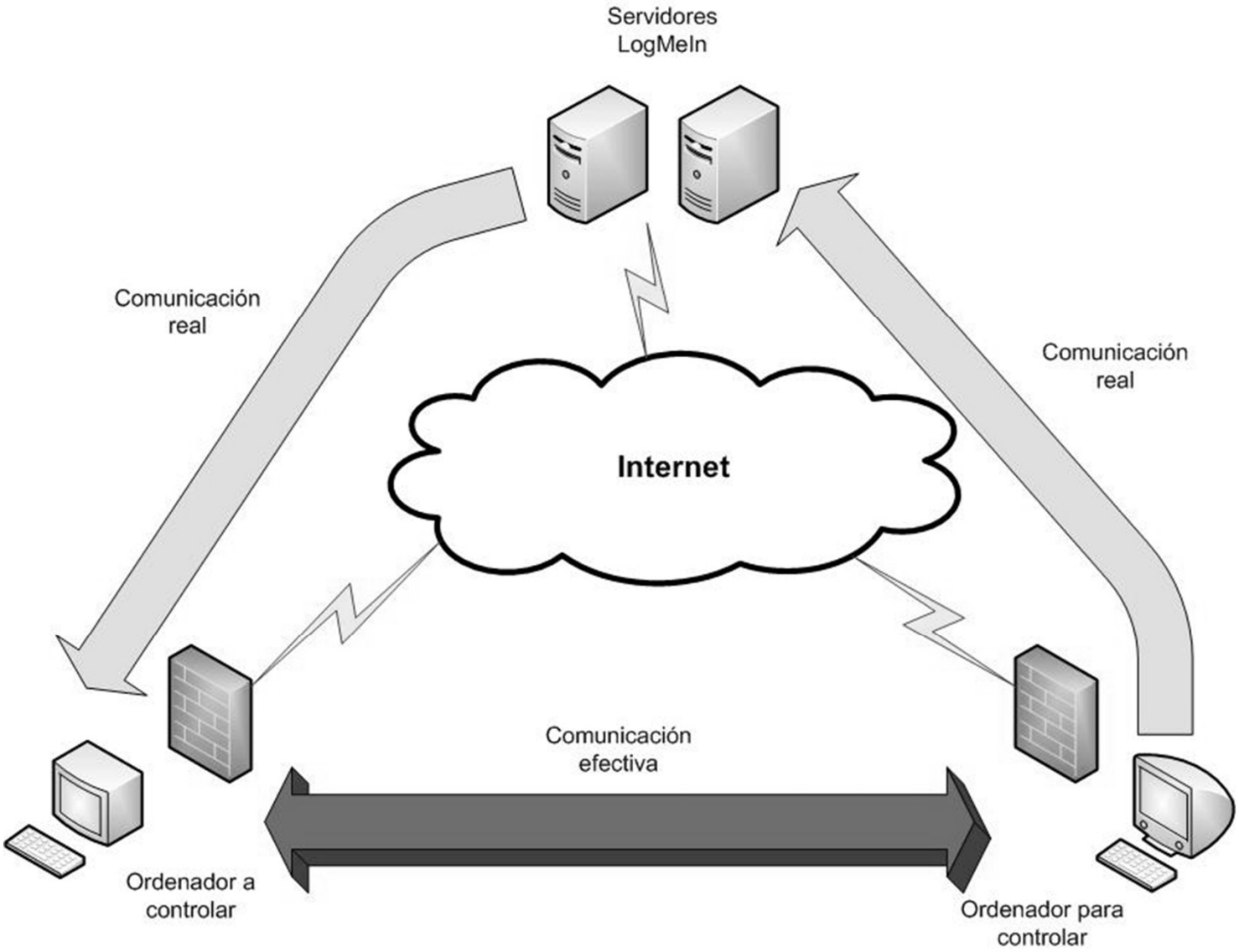
VNC/RDP + VPN

- Tanto para acceder a un servidor VNC o RDP es necesario que podamos “llegar” a él desde el exterior.
- Para ello una posibilidad es que el equipo esté accesible desde Internet. Esto es muy poco seguro y fuente de problemas, además de que es necesario gastar direcciones IP públicas o usar mecanismos del tipo NAT/PAT.
- Otra posibilidad es que el cliente establezca primero una conexión VPN para que, una vez dentro de la intranet, pueda acceder al servidor directamente. Esto es mucho más seguro y nos evita tener accesible directamente el servidor en Internet.

Programas de acceso remoto

- El objetivo es permitir el acceso remoto a un equipo que está dentro de la intranet.
- En principio el Firewall va a impedir las comunicaciones de este tipo iniciadas desde el exterior.
- Lo que el Firewall no impide son las comunicaciones que tienen su origen en la intranet.
- Se instala o ejecuta un programa en el ordenador a controlar el cuál establece una comunicación con servidores externos.
- Cuando queremos controlar un ordenador nos conectamos con el programa a esos servidores externos y a través de ellos (haciendo de intermediarios) podemos controlar el equipo remoto.
- Muchos ejemplos: TeamViewer, LogMeIn, Join.Me, AnyDesk, etc.

Programas de acceso remoto



Programas de virtualización de aplicaciones