Tema 3

La red de una granja web

Pedro A. Castillo Valdivieso
Depto Arquitectura y Tecnología de Computadores
Universidad de Granada
pacv@ugr.es

Índice

1. Introducción

La construcción de una red segura y escalable es fundamental para cualquier servidor.

Si la red no está bien estructurada, los servidores no pueden servir la información.

El administrador del sistema debe analizar las opciones de conexión a Internet y diseñar la estructura de red.

Debe separar las subredes corporativas y también conectar a redes privadas de proveedores.

1. Introducción

Hay que decidir el ancho de banda necesario a contratar.
Se duplica cada año (referencia a la Ley de Moore).

Todas estas decisiones de diseño implican un estudio del hardware y aplicaciones software disponibles:

- switch, hub, router, balanceador, etc
- sistema operativo, monitorización, balanceo, etc.

Índice

2. Configurar la red del sistema web

La configuración de la red requiere:

- Elegir el modelo de red más adecuado
- Elegir el hardware (estándar)
- Estructurar la red aislando subredes
- Definir los puntos de entrada a las diferentes subredes

2. Configurar la red del sistema web

Conceptos:

- Eje principal (backbone)
- Zona segura (DMZ)
- Front-rail / back-rail
- Redes seguras externas

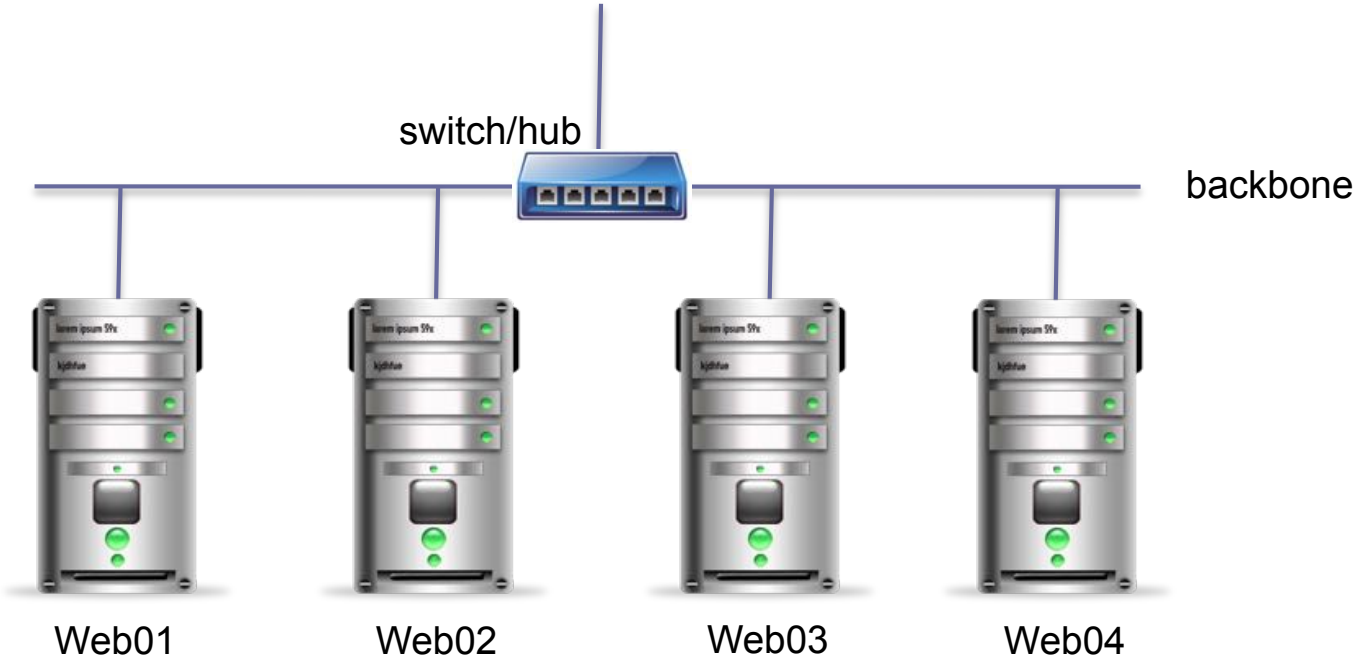
Índice

3. El eje principal de la red del sistema

Backbone: eje principal de enlace entre máquinas.

Se puede formar con un switch (http://es.wikipedia.org/wiki/Conmutador_(dispositivo_de_red)), router (http://es.wikipedia.org/wiki/Router) o hub (http://es.wikipedia.org/wiki/Concentrador).

Hace las comunicaciones entre servidores y redes



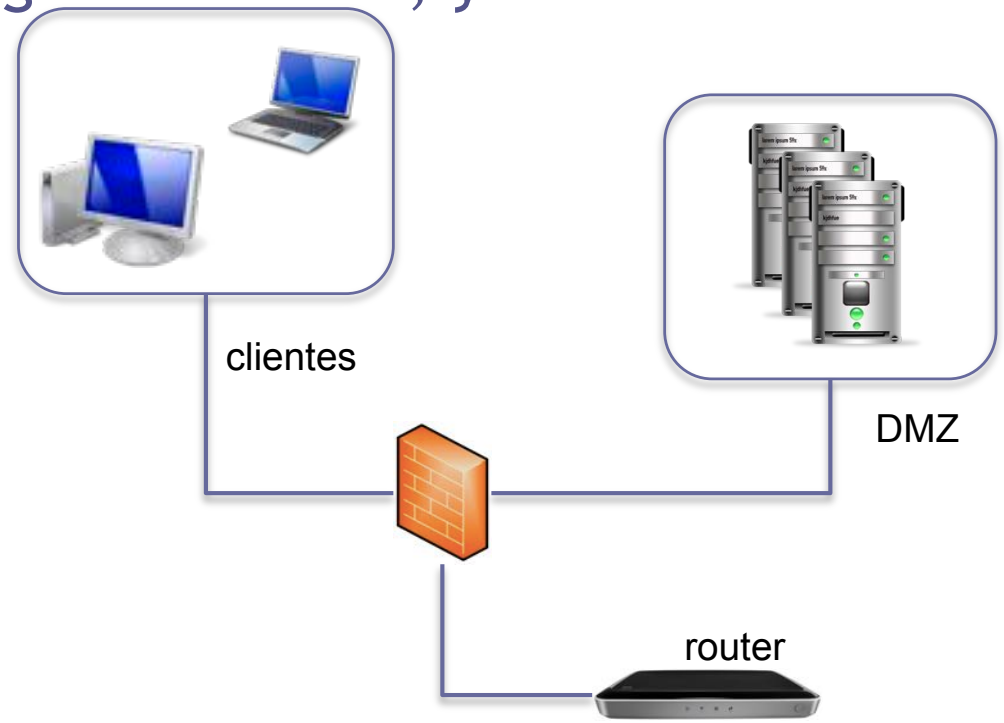
3. El eje principal de la red del sistema

Índice

4. Configurar una zona segura

Zona desmilitarizada o ***DMZ*** (*demilitarized zone*).

Área restringida o aislada, y totalmente controlada.



http://es.wikipedia.org/wiki/Zona_desmilitarizada_(inform%C3%A1tica)

4. Configurar una zona segura

Quedan controlados los servicios y aplicaciones ofrecidos a otras redes externas al DMZ.

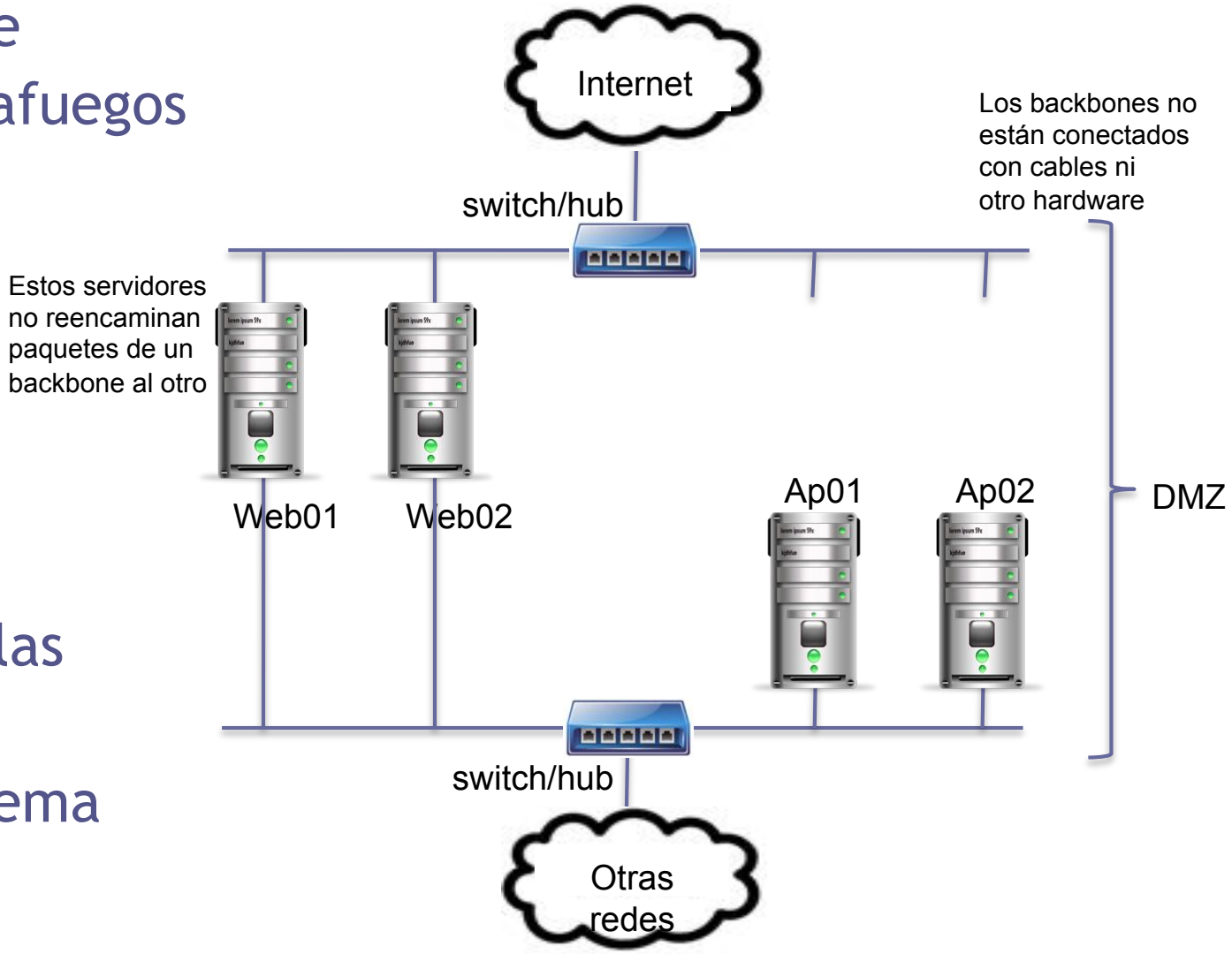
Los servicios de la granja web se ofrecen de forma estándar mediante dirección IP y puerto.

Los cortafuegos, routers y balanceadores de carga restringen el tráfico de entrada o salida.

4. Configurar una zona segura

La comunicación entre backbones se hace mediante un cortafuegos o configurando servidores con doble tarjeta de red.

La separación de las redes refuerza la seguridad del sistema



4. Configurar una zona segura

Existen varias alternativas para conectar la granja web a otras redes:

1. Configuración sin DMZ
2. Configuración de DMZ simple
3. Configuración de DMZ tradicional
4. Configuración de DMZ doble

4. Configurar una zona segura

1. Configuración sin DMZ

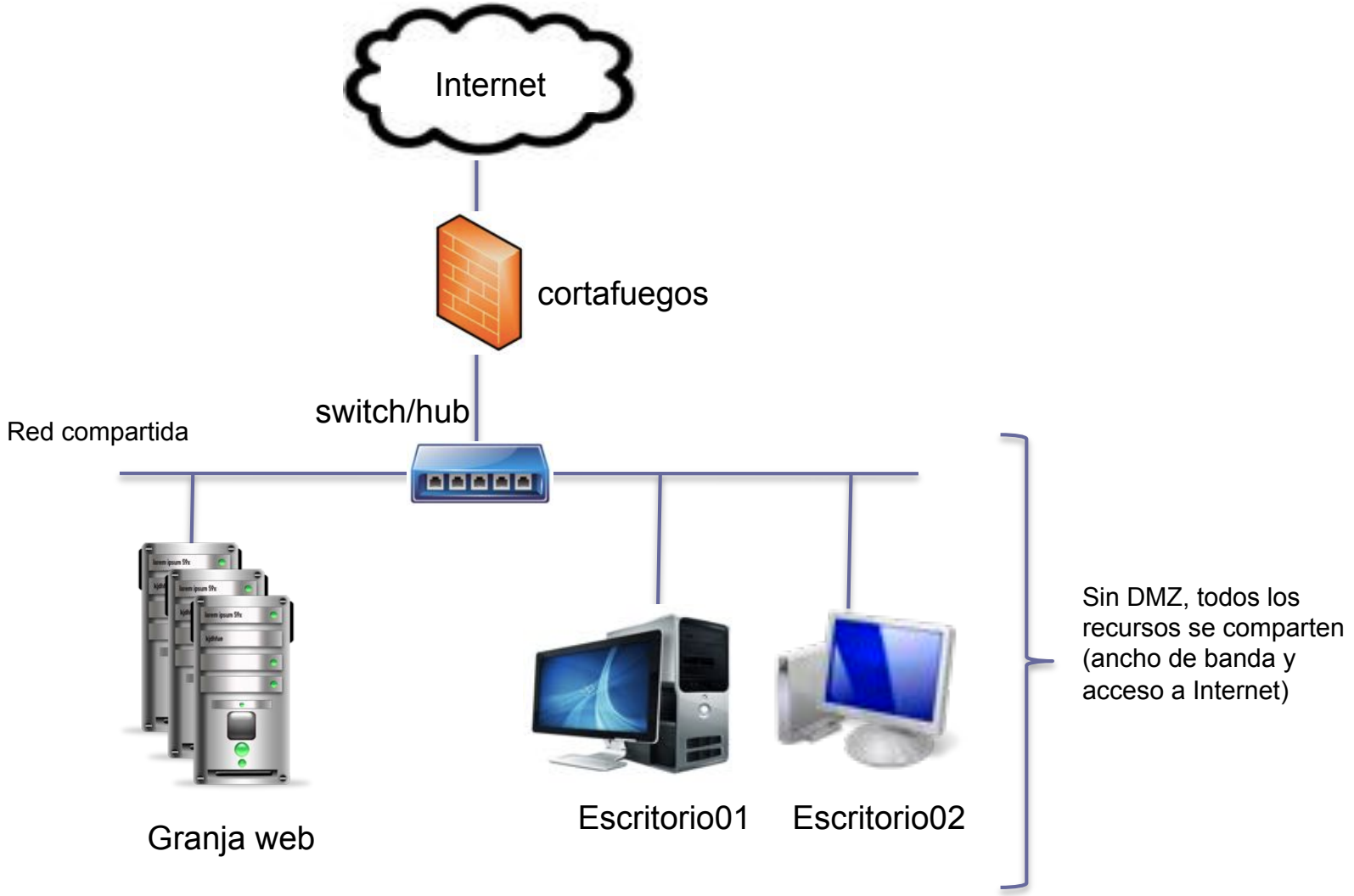
Tanto los servidores de la granja web como otras máquinas están conectadas a la misma subred.

Se comparten recursos (incluso salida a Internet).

Sólo tiene sentido en empresas muy pequeñas donde no hay problemas de prestaciones.

4. Configurar una zona segura

1. Configuración sin DMZ



4. Configurar una zona segura

1. Configuración sin DMZ

Problemas: 

- Compartición del ancho de banda (servidores y máquinas de escritorio).
- Asegurar los servidores es más complicado.
- Si uno de los servidores se ve comprometido, el resto de recursos puede ser atacado.

4. Configurar una zona segura

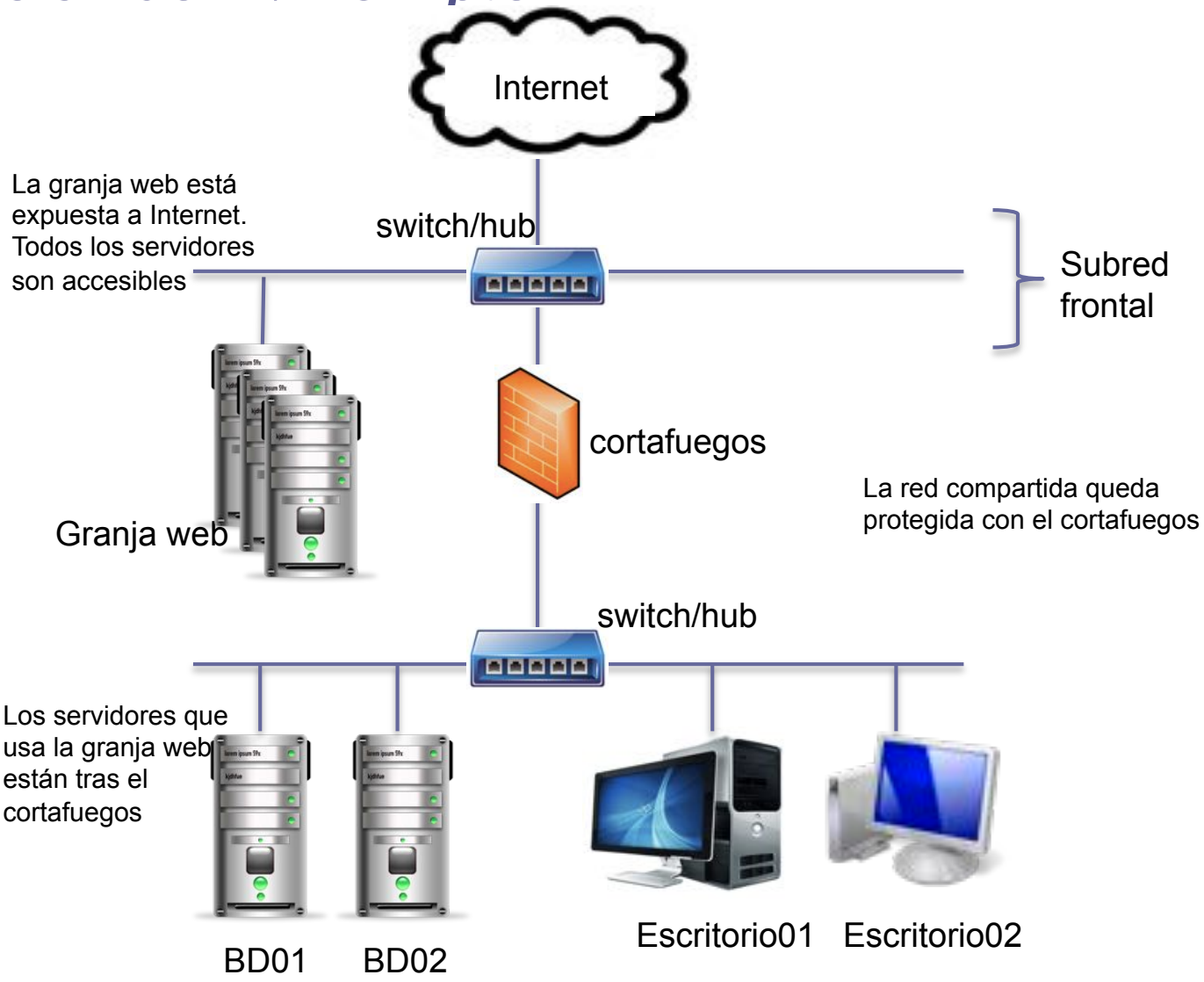
2. Configuración de DMZ simple

Los servidores expuestos deben aislarse con un cortafuegos.

Así se protegen los servidores de bases de datos o disco y las máquinas de escritorio.

4. Configurar una zona segura

2. Configuración de DMZ simple



4. Configurar una zona segura

2. Configuración de DMZ simple

Problemas: 

- Los servidores están conectados directamente a Internet.
- El cortafuegos puede ser un cuello de botella.
- Los servidores y máquinas tras el cortafuegos aún comparten ancho de banda.

4. Configurar una zona segura

3. Configuración de DMZ tradicional

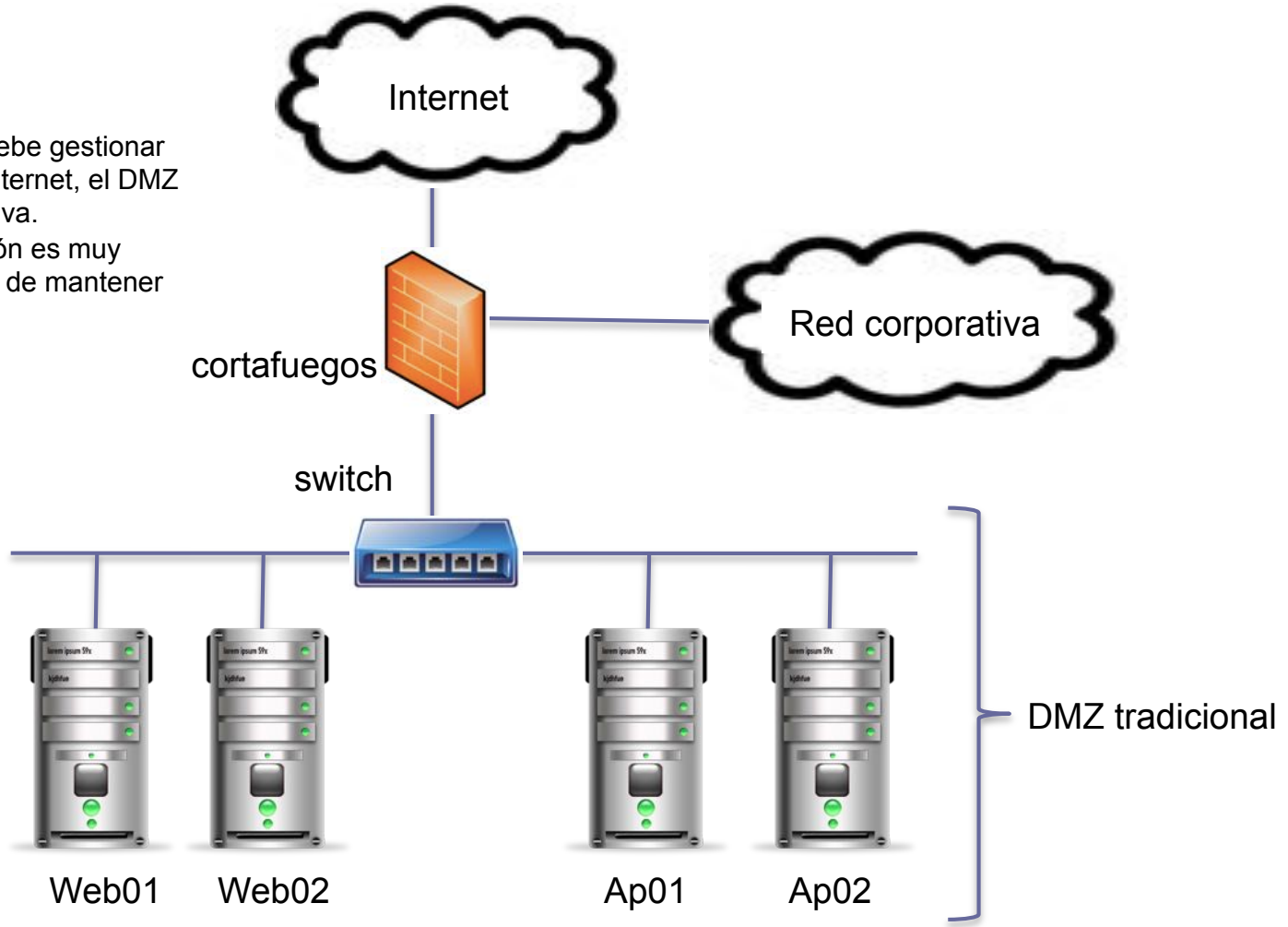
La idea es resolver los problemas de la configuración anterior:

- ancho de banda de la red corporativa compartido
- inseguridad de los servidores expuestos

4. Configurar una zona segura

3. Configuración de DMZ tradicional

El cortafuegos debe gestionar el tráfico entre Internet, el DMZ y la red corporativa.
Esta configuración es muy compleja y difícil de mantener



4. Configurar una zona segura

3. Configuración de DMZ tradicional

Problemas: 

- Dificultad para configurar correctamente el cortafuegos.
- El cortafuegos es un posible cuello de botella.
- Si la configuración del cortafuegos tiene errores, entonces ¡todo queda expuesto!

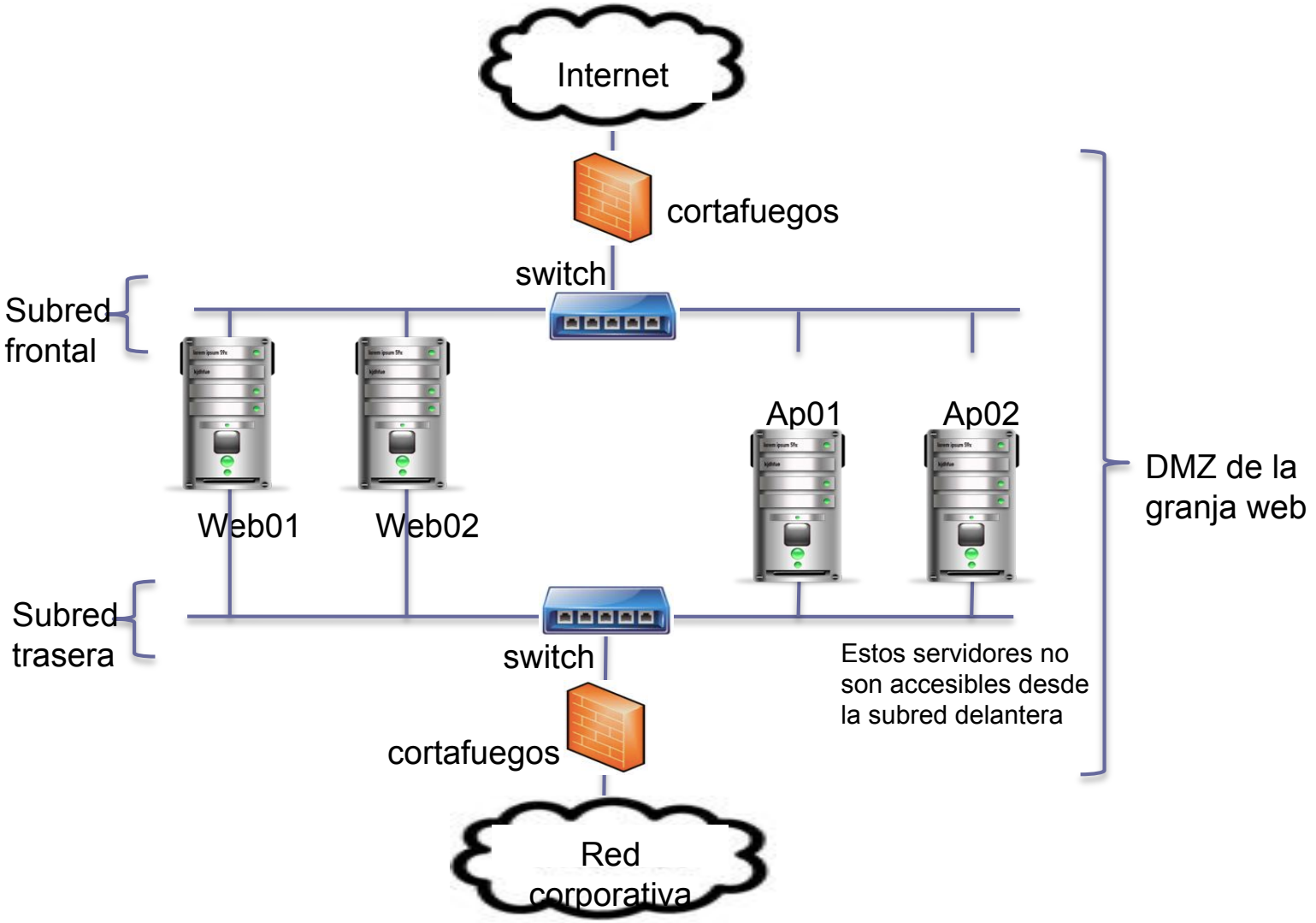
4. Configurar una zona segura

4. Configuración de DMZ doble

- Configuración ideal para una granja web.
- Se basa en aislar todos los servidores con cortafuegos.

4. Configurar una zona segura

4. Configuración de DMZ doble



4. Configurar una zona segura

4. Configuración de DMZ doble

Es la configuración más segura: 

- El DMZ tiene un front-rail y un back-rail.

- El delantero es un segmento de red conectado a Internet.
- Los servidores quedan protegidos con el cortafuegos.

- El trasero está conectado a la subred interna (segura), y protegido con otro cortafuegos.

Índice

5. Conectar servidores al front-rail

Los servidores conectados al front-rail dan servicios a clientes a través de Internet:

- HTTP, SMTP, POP3, FTP, etc.

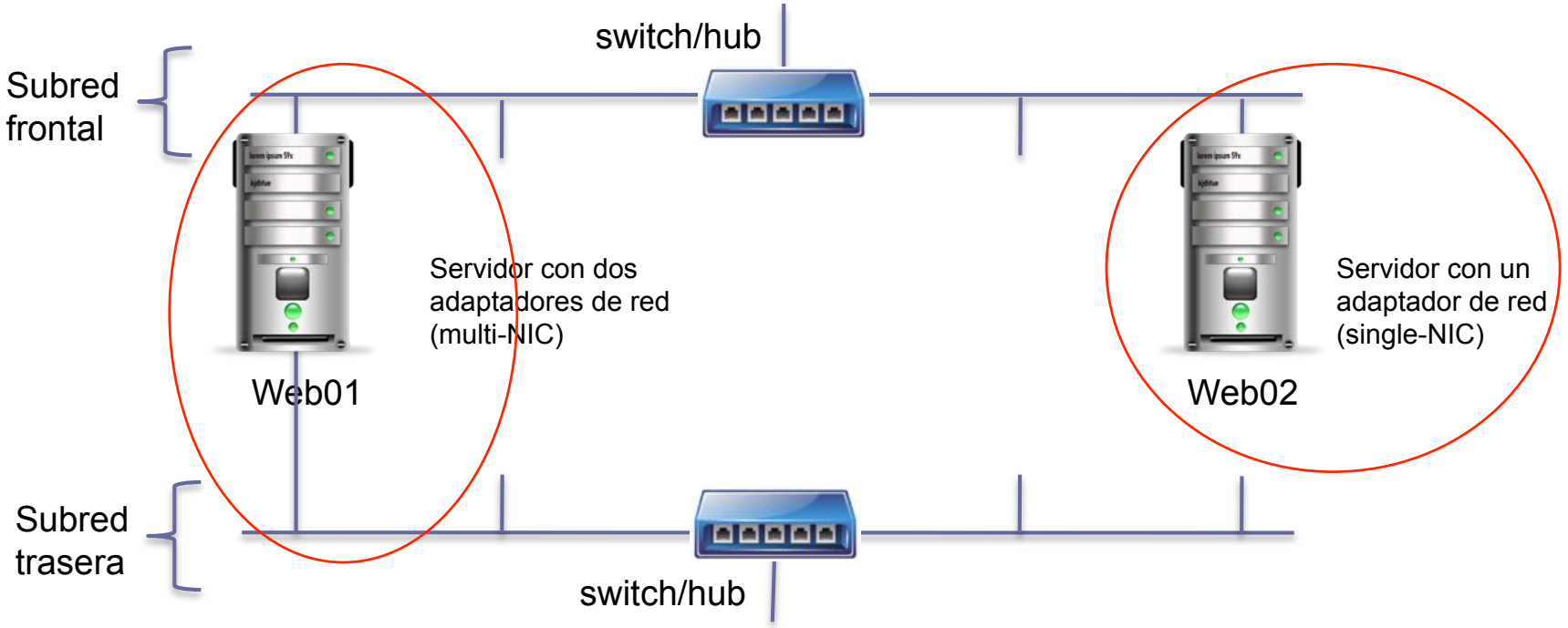
Otros servicios no se ofrecen por el front-rail:

- Bases de datos, terminal

Hay dos tipos de servidores:

- ***Single-NIC***: conectado sólo a la subred frontal; aislado de la trasera
- ***Multi-NIC***: conectado a la frontal y la trasera

5. Conectar servidores al front-rail



5. Conectar servidores al front-rail

Un servidor multi-NIC puede acceder a la subred trasera para consumir un recurso.

Su configuración requiere de reglas específicas en la tabla de enrutamiento para encaminar el tráfico hacia la subred trasera.

Hay que ser cuidadosos al establecer las reglas para no dejar caminos que comprometan la seguridad.

Posible trabajo para SWAP: hacer una configuración DMZ doble

Conectar servidores al front-rail

Ejercicio T3.1:

Buscar con qué órdenes de terminal o herramientas gráficas podemos configurar bajo Windows y bajo Linux el enrutamiento del tráfico de un servidor para pasar el tráfico desde una subred a otra.

Índice

6. Conectar servidores al back-rail

Los servidores conectados a la subred trasera son accesibles

- desde subredes seguras y controladas
- o bien desde servidores con multi-NIC

La subred trasera no debe conectarse directamente a Internet.

Se pueden conectar servidores single-NIC para servir aplicaciones, BD o disco.

El cortafuegos protege los servidores. Sus reglas deben dejar acceso a ciertas aplicaciones y servicios según tipo de usuario.

Índice

7. Resumen de configuraciones

Resumen de las configuraciones de los servidores y a qué subred pueden acceder:

(1) Doble conexión al fron-rail y back-rail:

- Requiere doble tarjeta de red
- Adecuado para acceder a Internet y servidores internos
- Configuración para servidores HTTP, SMTP, POP3, FTP, etc
- Ofrecen servicios hacia Internet y a las subredes seguras

7. Resumen de configuraciones

Resumen de las configuraciones de los servidores y a qué subred pueden acceder:

(2) Conexión sólo al front-rail:

- Requiere sólo una tarjeta de red
- Adecuado para acceder sólo a Internet
- Los servicios ofrecidos quedan aislados
- Configuración para servidores HTTP, SMTP, POP3, FTP, etc
- Ofrecen servicios hacia Internet

7. Resumen de configuraciones

Resumen de las configuraciones de los servidores y a qué subred pueden acceder:

(3) Conexión sólo al back-rail:

- Requiere sólo una tarjeta de red
- Para servidores que no necesitan acceso a Internet
- Servicios ofrecidos a las redes corporativas/seguras
- Configuración para servidores de BD o aplicaciones

Índice

8. Conectar la granja web a Internet

La conexión a Internet depende de varios factores para asegurar la calidad del servicio y la seguridad:

1. Calidad del servicio y ancho de banda
2. Filtrado y bloqueo de paquetes
3. Network address translation (NAT)

8. Conectar la granja web a Internet

1. Calidad de servicio y ancho de banda

La calidad del servicio está directamente relacionada con el ancho de banda para salir a Internet.

Hay que definir qué porcentaje del ancho de banda se reserva para cada tipo de tráfico (HTTP, SSL, FTP...)

Los routers modernos permiten establecer esos parámetros.

8. Conectar la granja web a Internet

1. Calidad de servicio y ancho de banda

http://www.monografias.com/trabajos30/redes-de-datos/redes-de-datos.shtml

Se suele expresar en Kbps, Mbsp, Gbps y Tbps.

Queda determinado por los métodos de señalización, las tarjetas de red y los demás equipos de red

8. Conectar la granja web a Internet

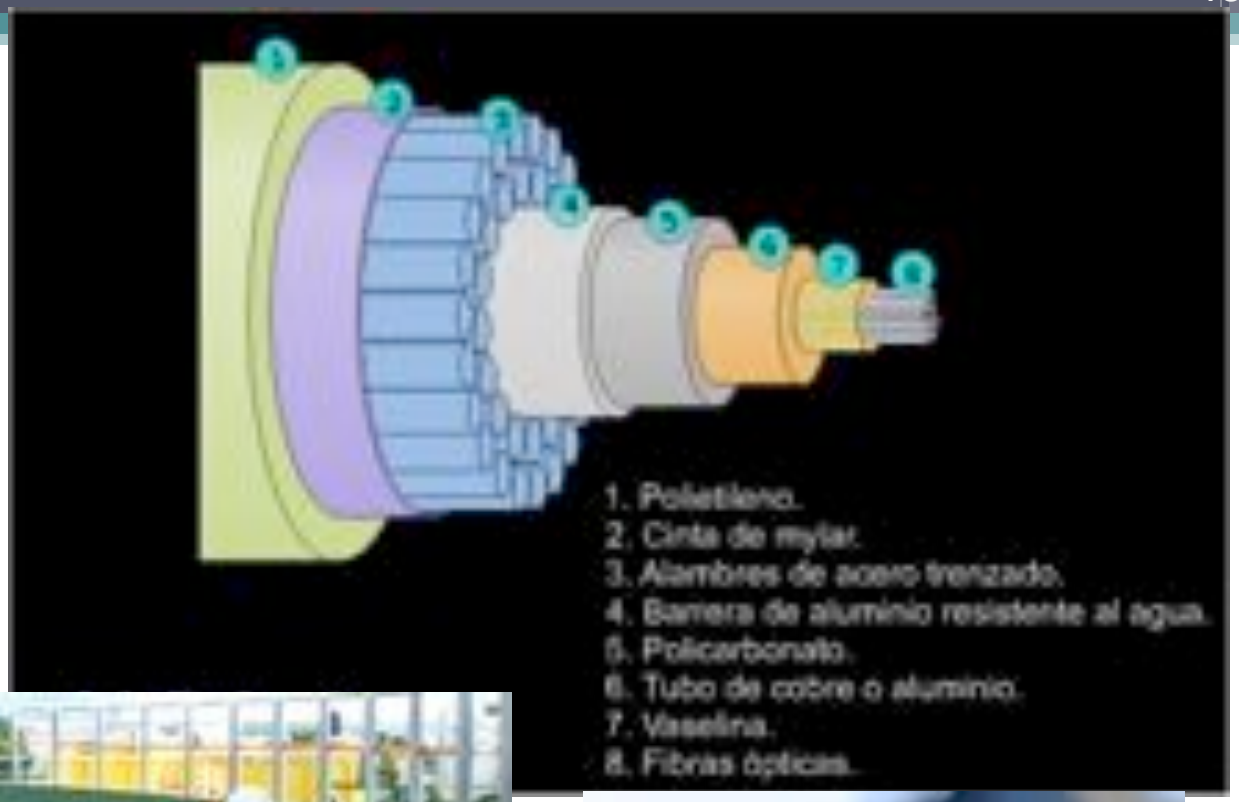
1. Calidad de servicio y ancho de banda

Medios típicos	Ancho de banda máximo teórico	Distancia máxima teórica
Cable coaxial de 50 ohmios (Ethernet 10BASE2, Thinnet)	10 Mbps	185 m
Cable coaxial de 50 ohmios (Ethernet 10BASE2, Thinnet)	10 Mbps	500 m
Cable de par trenzado no blindado de categoría 5 (UTP) (Ethernet 10BASE-T)	10 Mbps	100 m
Cable de par trenzado no blindado de categoría 5 (UTP) (Ethernet 100BASE-T)	100 Mbps	100 m
Cable de par trenzado no blindado de categoría 5 (UTP) (Ethernet 1000BASE-T)	1000 Mbps	100 m
Fibra óptica multimodo (62.5/125microm) (100BASE-FX Ethernet)	100 Mbps	2000 m
Fibra óptica multimodo (62.5/125microm) (1000BASE-SX Ethernet)	1000 Mbps	220 m
Fibra óptica multimodo (50/125microm) (1000BASE-SX Ethernet)	1000 Mbps	550 m
Fibra óptica monomodo (9/125microm) (1000BASE-LX Ethernet)	1000 Mbps	5000 m

8. Conectar la granja web a Internet

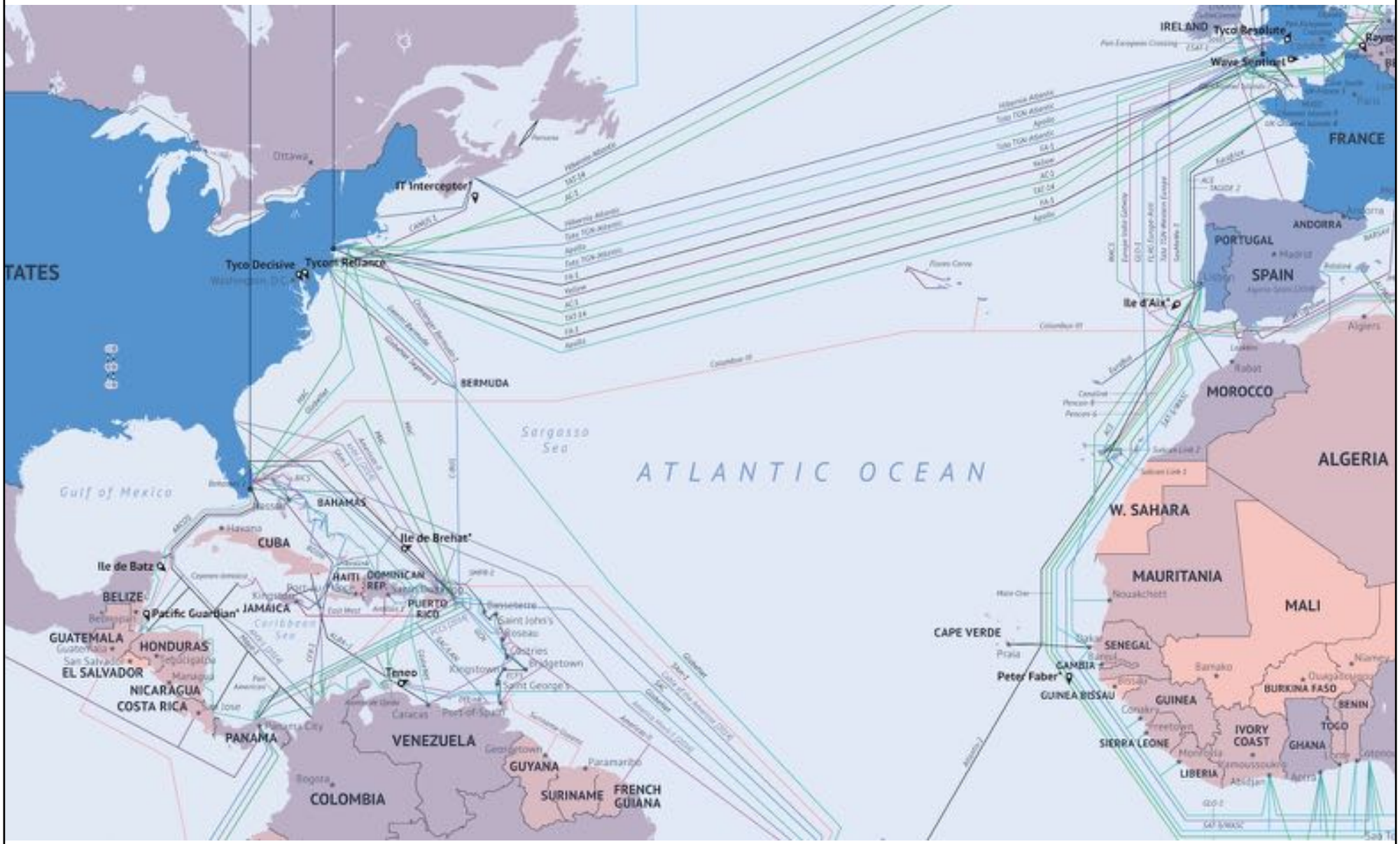
1. Calidad de servicio y ancho de banda

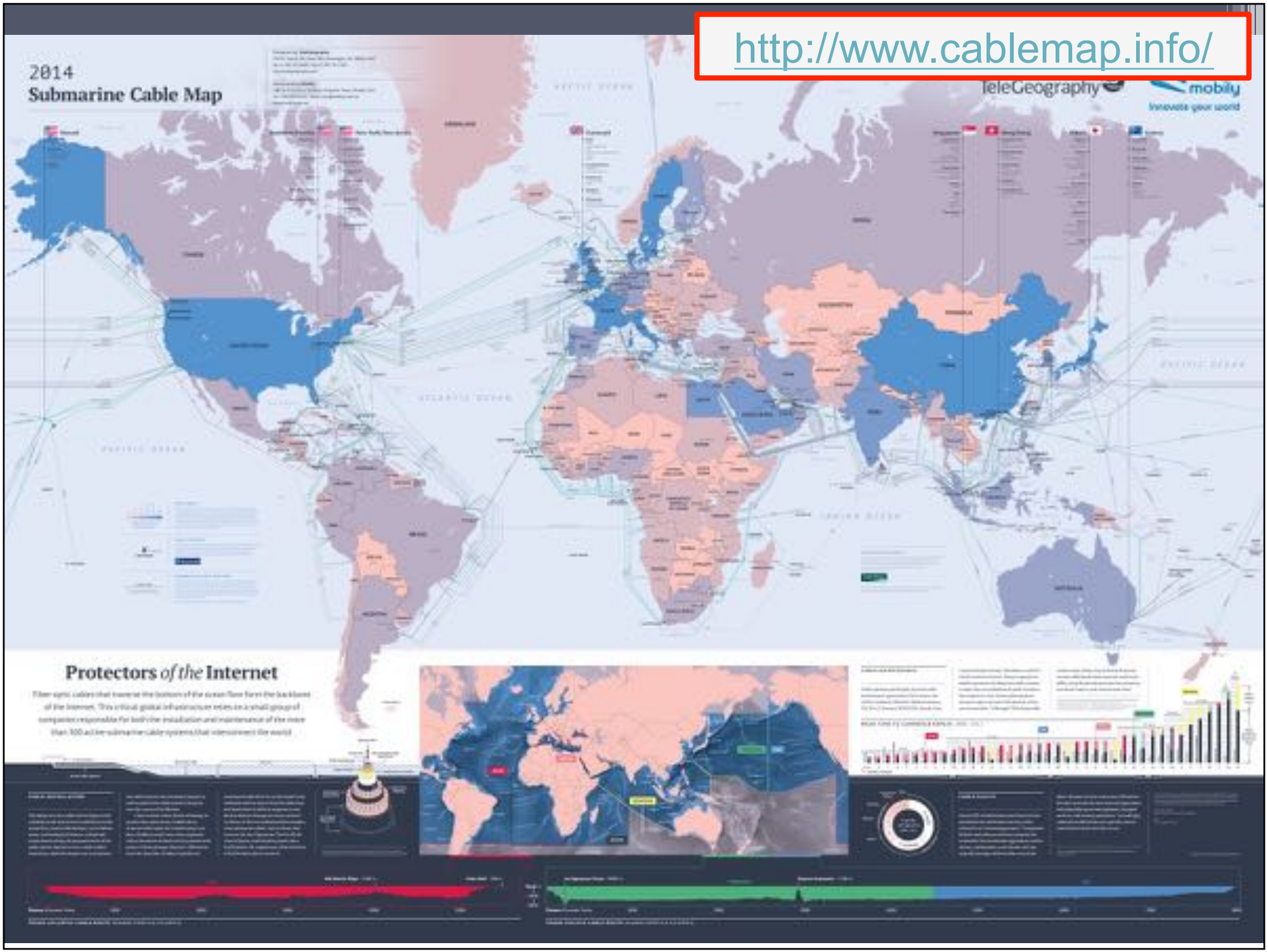
Servicio WAN	Usuario Típico	Ancho de Banda
Modem	Individuos	56 kbps
DSL	Individuos, teleconmuters y pequeños negocios	de 128 kbps hasta 6 Mbps
ISDN	Teleconmuters y pequeños negocios	128 kbps
Frame Relay	Instituciones pequeñas (escuelas, WANs confiables)	de 56 kbps hasta 44 Mbps
T1	Grandes instituciones	1.5 Mbps
E1	Grandes instituciones	2 Mbps
T3	Grandes instituciones	44.7 Mbps
E3	Grandes instituciones	34 Mbps
STS- (OC-1)	Compañías telefónicas, backbones de compañías de comunicación de datos	51.8 Mbps
STM-1	Compañías telefónicas, backbones de compañías de comunicación de datos	155 Mbps
STS-3 (OC-3)	Compañías telefónicas, backbones de compañías de comunicación de datos	155 Mbps
STM-3	Compañías telefónicas, backbones de compañías de comunicación de datos	466 Mbps
STS-48 (OC-48)	Compañías telefónicas, backbones de compañías de comunicación de datos	2.5 Gbps



http://almadeherrero.blogspot.com.es/2008/11/cables-submarinos.html
http://enbytes.com/site/2012/12/06/alcatel-lucent-tiende-cable-submarino-para-consorcio-de-operadores/

http://alt1040.com/2014/03/mapa-cables-submarinos-2014



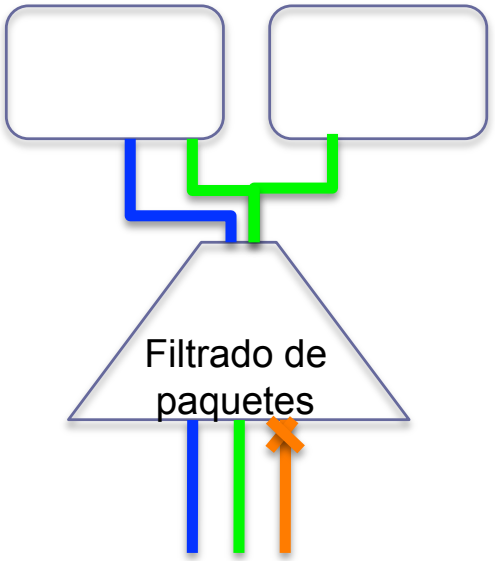

http://www.cablemap.info/
2014
Submarine Cable Map
TeleGeography
mobily
Protectors of the Internet

8. Conectar la granja web a Internet

2. Filtrado y bloqueo de paquetes

Conviene establecer filtros de forma que sólo le llegue a una máquina el tráfico que debe llegarle.

Otros tipos de tráfico se bloquearán para que no le lleguen. Aunque los ignorase, los paquetes sobrecargan la red.

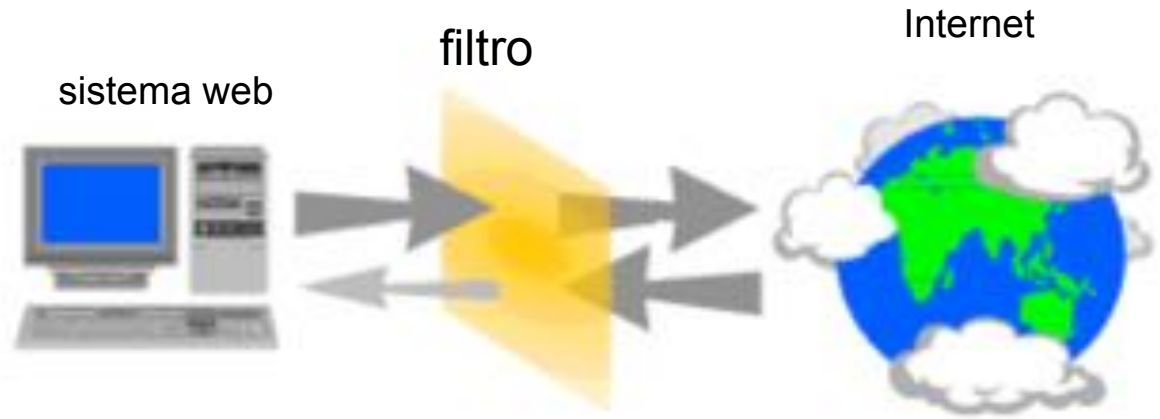


8. Conectar la granja web a Internet

2. Filtrado y bloqueo de paquetes

Los paquetes contienen información de IP origen, IP destino y puerto (servicio), por lo que esta información se usará para el filtrado.

Se pueden usar ***cortafuegos***, routers o concentradores.



Filtrado y bloqueo de paquetes

Ejercicio T3.2:

Buscar con qué órdenes de terminal o herramientas gráficas podemos configurar bajo Windows y bajo Linux el filtrado y bloqueo de paquetes.

8. Conectar la granja web a Internet

3. NAT: Network Address Translation

Con NAT mapeamos una dirección pública a una dirección privada de una de las máquinas servidoras internas.

Mejora la seguridad: se ocultan las verdaderas IP de los servidores últimos.

Esto lo pueden hacer los routers, cortafuegos y balanceadores de carga.

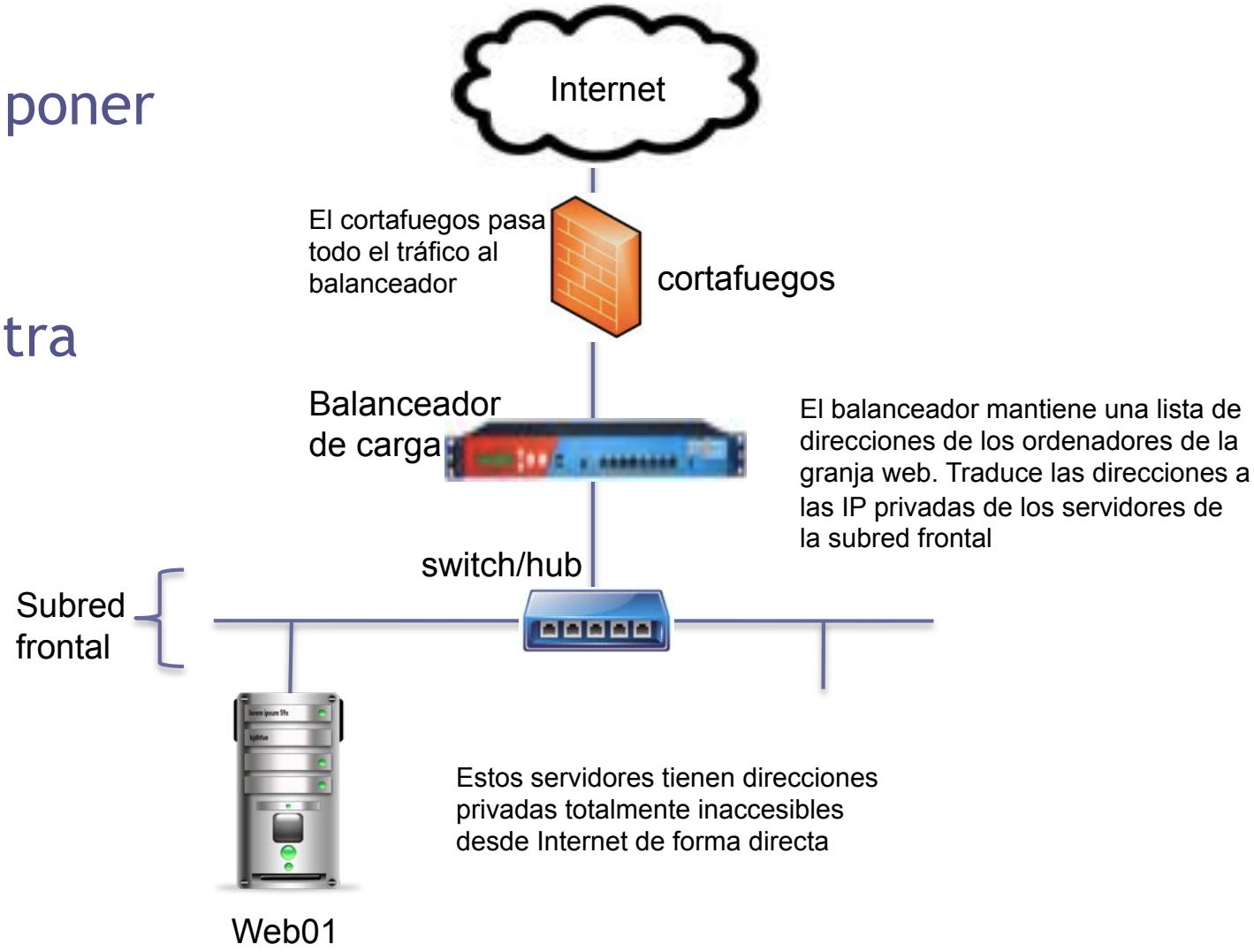
8. Conectar la granja web a Internet

3. NAT: Network Address Translation

Incluso podemos poner varios niveles:

El cortafuegos filtra los paquetes.

El balanceador distribuye.



Índice

9. Conectar la granja web a redes seguras

Algunas organizaciones necesitan los servicios de otras empresas (bancos, p.ej).

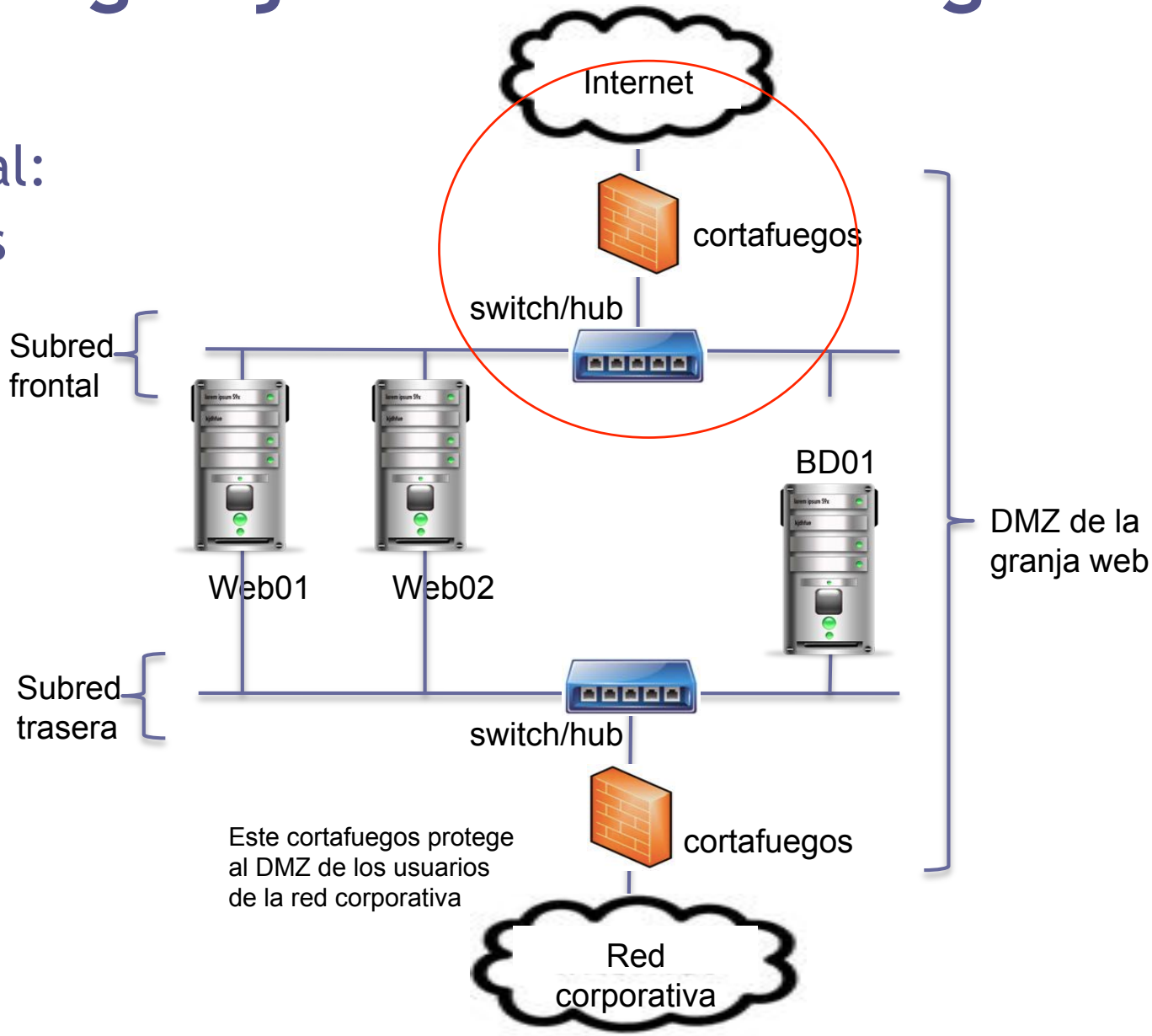
Para ello se conectan a redes seguras de esas empresas.

La conexión a redes aseguradas es similar a la conexión a Internet, pero con menos riesgos.

Hay que poner un **mecanismo de filtrado y bloqueo de paquetes** para evitar posibles ataques desde las máquinas de esas redes.

9. Conectar la granja web a redes seguras

Como regla general: bloquear paquetes y filtrarlos con un cortafuegos.



9. Conectar la granja web a redes seguras

Hay que tener en cuenta las necesidades de los usuarios en relación a los servicios que queremos obtener de la empresa.

Podemos realizar la conexión mediante cortafuegos o mediante protocolos seguros (SSL).

Por ejemplo:

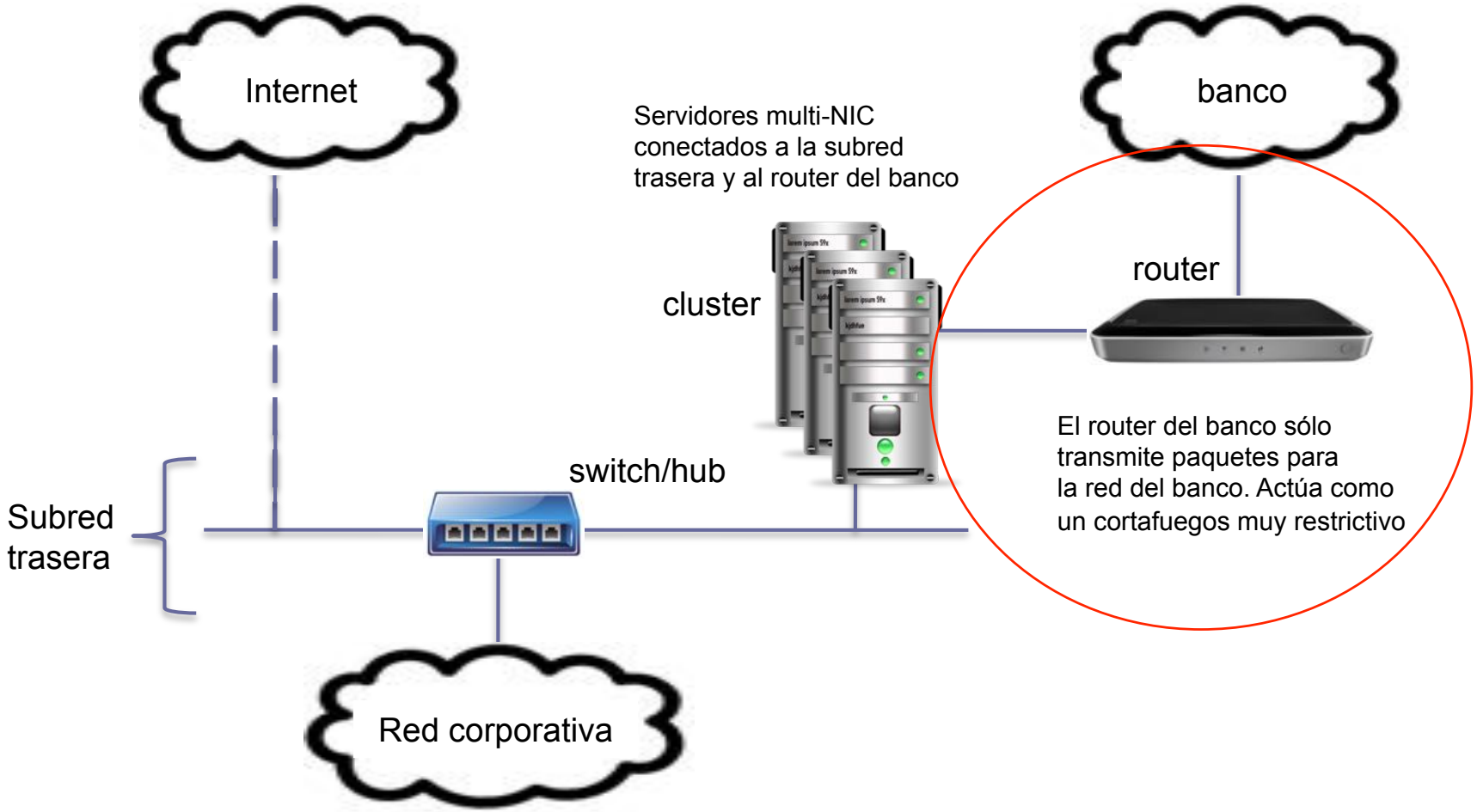
Queremos usar los servicios de un banco para cobrar con tarjeta de crédito (operación de riesgo).

Mediante conexión segura controlada por el banco.

9. Conectar la granja web a redes seguras

Ejemplo:

El banco nos instala un router para conectarnos a su red:



9. Conectar la granja web a redes seguras

Ejemplo (cont.):

Instalar una interfaz de red dedicada y conectada a ese router en los servidores que vayan a consumir ese tipo de servicio.

Podemos configurar un servidor en el back-rail que haga de pasarela para las operaciones con tarjeta de crédito.

Índice

10. Conclusiones (I)

La configuración de la red de la granja web se puede hacer de varias formas.

La más segura es con el doble DMZ (subred frontal + subred trasera).

Los usuarios acceden desde Internet a los servidores conectados en la subred frontal.

Las máquinas en la subred trasera dan servicios a los usuarios en la red corporativa y a los servidores de la subred frontal.

10. Conclusiones (II)

En la calidad del servicio influye:

- el ancho de banda de conexión a Internet
- el filtrado y bloqueo de paquetes
- el balanceo de la carga entre los servidores

Se pueden obtener servicios externos conectando a redes seguras (p.ej. un banco).

¡Que no se olvide el trabajo!

En relación al trabajo conviene:

1. decidir con quién haremos el trabajo
2. elegir tema para el trabajo cuanto antes
3. planificar la realización del trabajo
4. comenzar a documentarnos