

TEMA 3

La red de una granja web

SWAP



¿Qué configuración de red es más
adecuada para la granja web?
¿Será segura?



José Manuel Soto Hidalgo
Dpto. Arquitectura y Tecnología de Computadores
Universidad de Granada

jmsoto@ugr.es

Índice



[1.Introducción]

- 2.Configurar la red del sistema web
- 3.El eje principal de la red del sistema
- 4.Configurar una zona segura
- 5.Conectar servidores al front-rail
- 6.Conectar servidores al back-rail
- 7.Resumen de configuraciones
- 8.Conectar la granja web a Internet
- 9.Conectar la granja web a redes seguras
- 10.Resumen y conclusiones

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

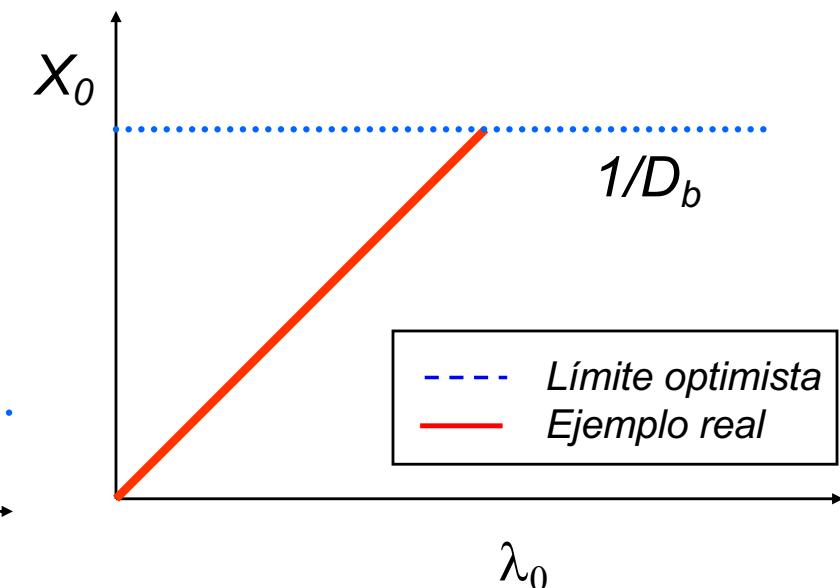
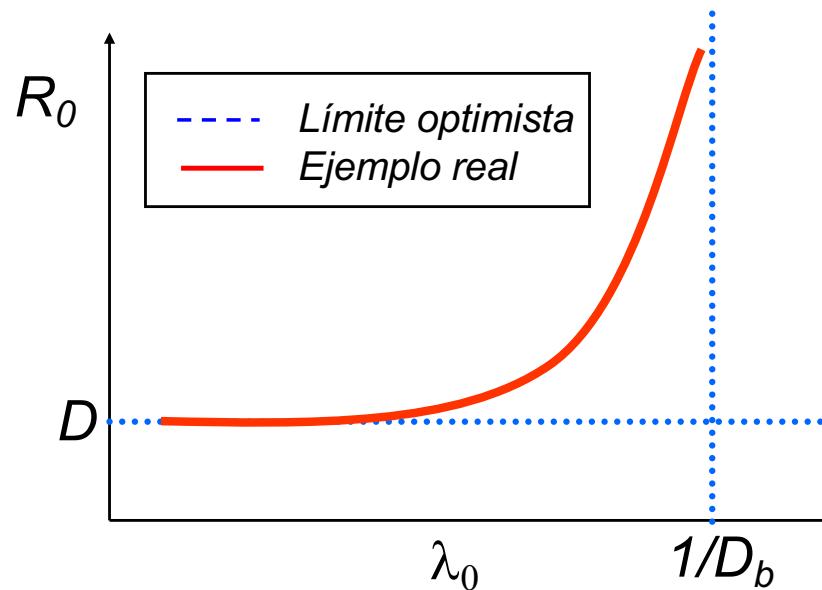
Debe separar las subredes corporativas y también conectar a redes privadas de proveedores.

1. Introducción

Hay que decidir el ancho de banda necesario a contratar.

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

- switch, hub, router, balanceador, etc.
- sistema operativo, monitorización, balanceo, etc.
- -> Carga del sistema ---- $D = S \times V$



Índice



1. Introducción

[2. Configurar la red del sistema web]

3. El eje principal de la red del sistema
4. Configurar una zona segura
5. Conectar servidores al front-rail
6. Conectar servidores al back-rail
7. Resumen de configuraciones
8. Conectar la granja web a Internet
9. Conectar la granja web a redes seguras
10. Resumen y conclusiones

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



1. Introducción
2. Configurar la red del sistema web
- 3. El eje principal de la red del sistema**
4. Configurar una zona segura
5. Conectar servidores al front-rail
6. Conectar servidores al back-rail
7. Resumen de configuraciones
8. Conectar la granja web a Internet
9. Conectar la granja web a redes seguras
10. Resumen y conclusiones

3. El eje principal de la red del sistema

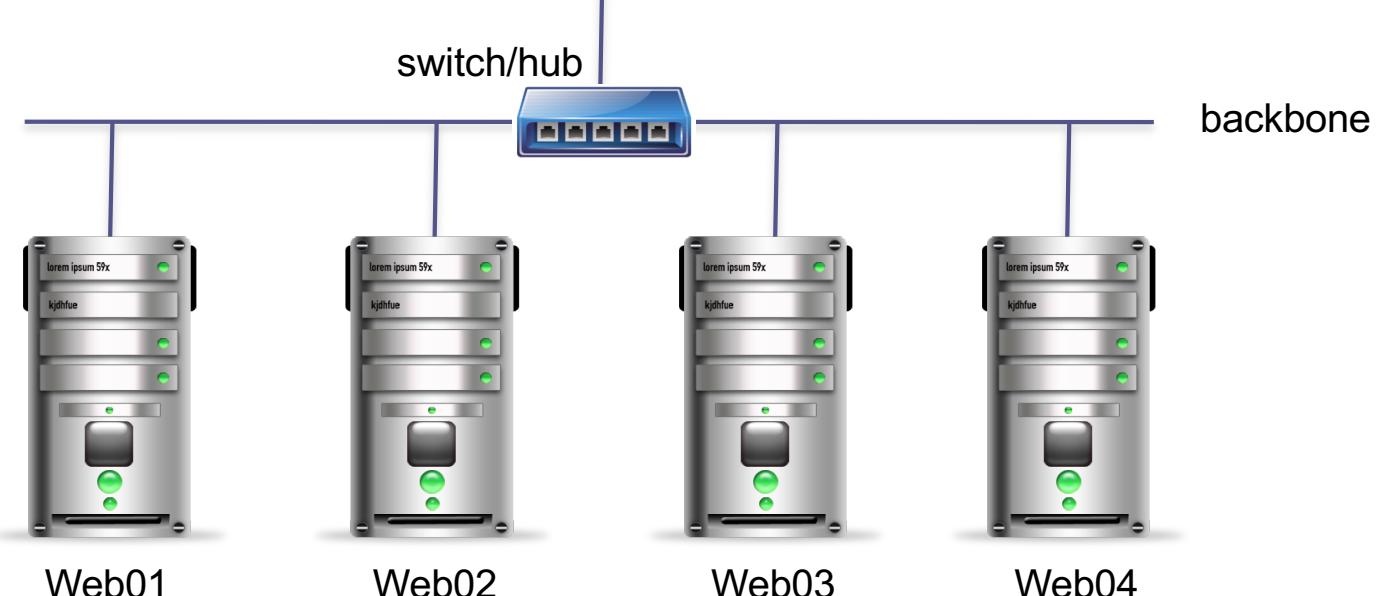
Backbone: eje principal de enlace entre máquinas.

Se puede formar con:

- Switch
- Router
- Hub

<http://computerhoy.com/noticias/internet/cuales-son-diferencias-hub-switch-router-43325>

Gestiona las comunicaciones entre servidores y redes:



3. El eje principal de la red del sistema

hub (<http://es.wikipedia.org/wiki/Concentrador>)

- Dispositivo sencillo; recibe datos procedentes de un ordenador para transmitirlo a todos los demás que estén conectados.

switch ([http://es.wikipedia.org/wiki/Comutador_\(dispositivo_de_red\)](http://es.wikipedia.org/wiki/Comutador_(dispositivo_de_red)))

- Además de la funcionalidad del hub, hace que la información proveniente del ordenador de origen se envíe al de destino.

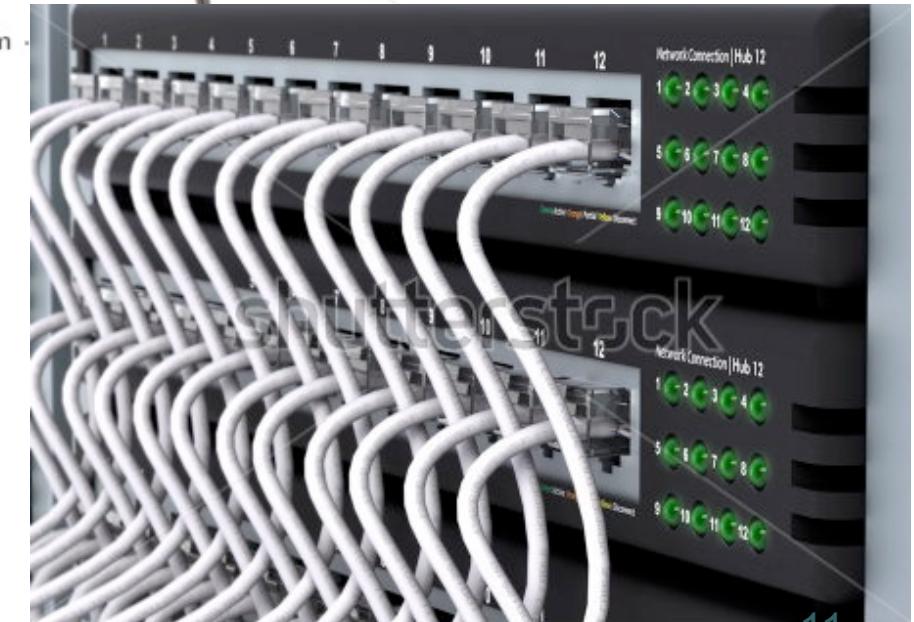
router (<http://es.wikipedia.org/wiki/Router>)

- Además de la funcionalidad del switch, interconectan varias redes y tienen la capacidad de escoger la mejor ruta para que los paquetes de datos lleguen a su destino.

3. El eje principal de la red del sistema

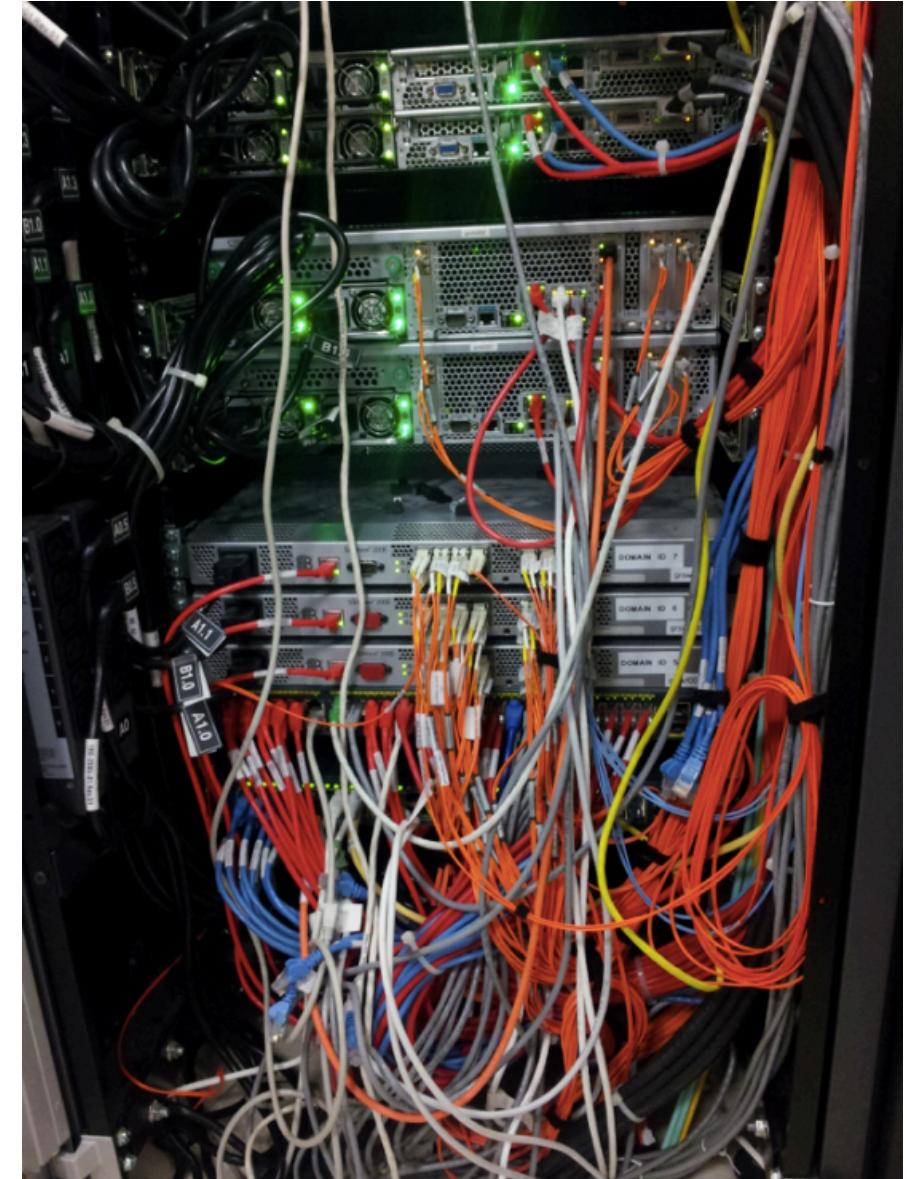
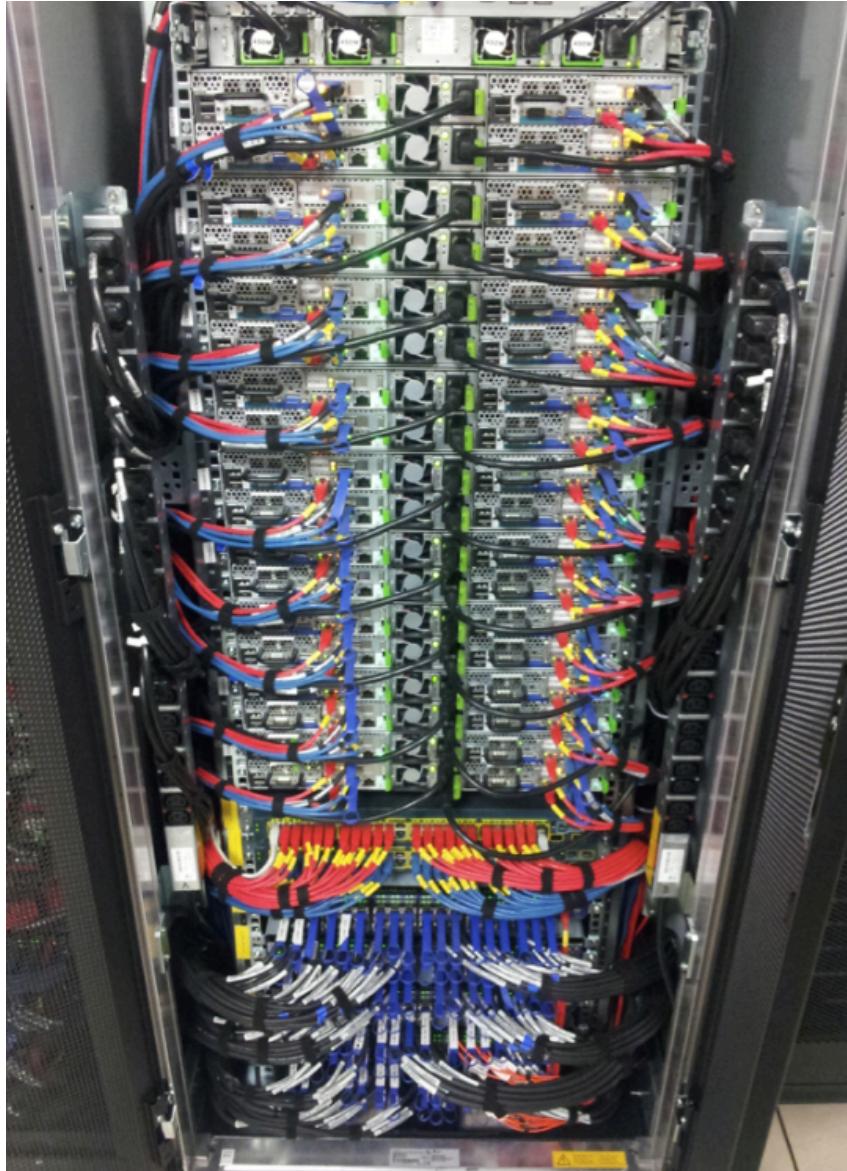


www.shutterstock.com · 70112269



www.shutterstock.com · 62956390

3. Los cables...





EnjutoMojamuto
@enjutomojamuto



Seguir

Muchos no lo entenderéis pero esto es
porno para informáticos



Índice

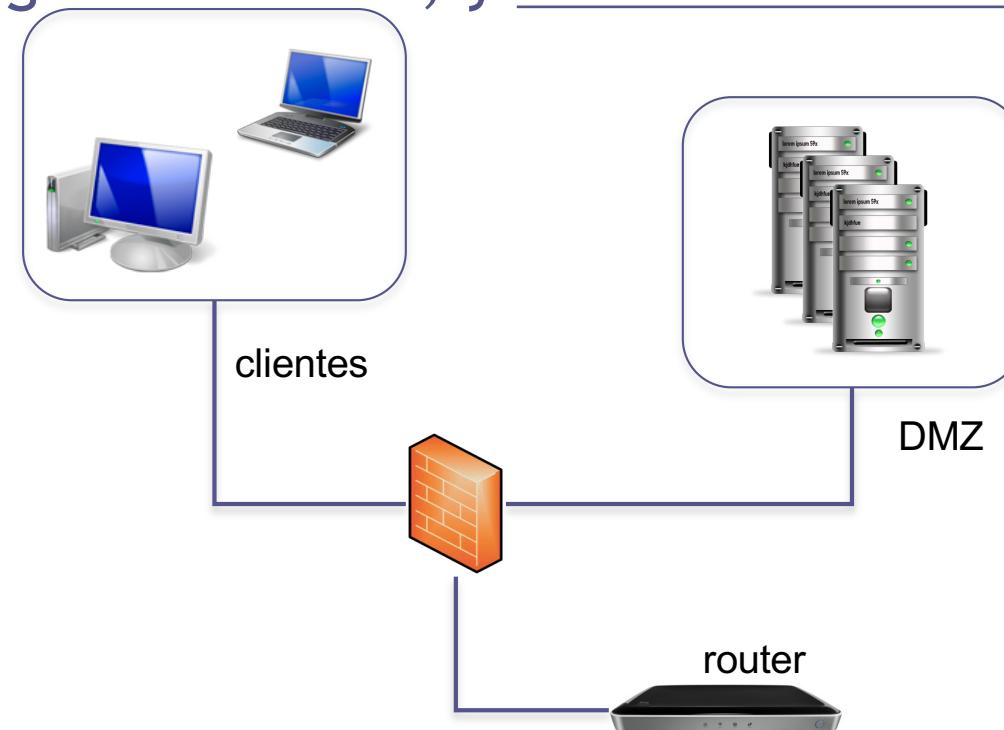


1. Introducción
2. Configurar la red del sistema web
3. El eje principal de la red del sistema
4. Configurar una zona segura - DMZ
5. Conectar servidores al front-rail
6. Conectar servidores al back-rail
7. Resumen de configuraciones
8. Conectar la granja web a Internet
9. Conectar la granja web a redes seguras
10. Resumen y conclusiones

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_\(inform%C3%A1tica\)](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.

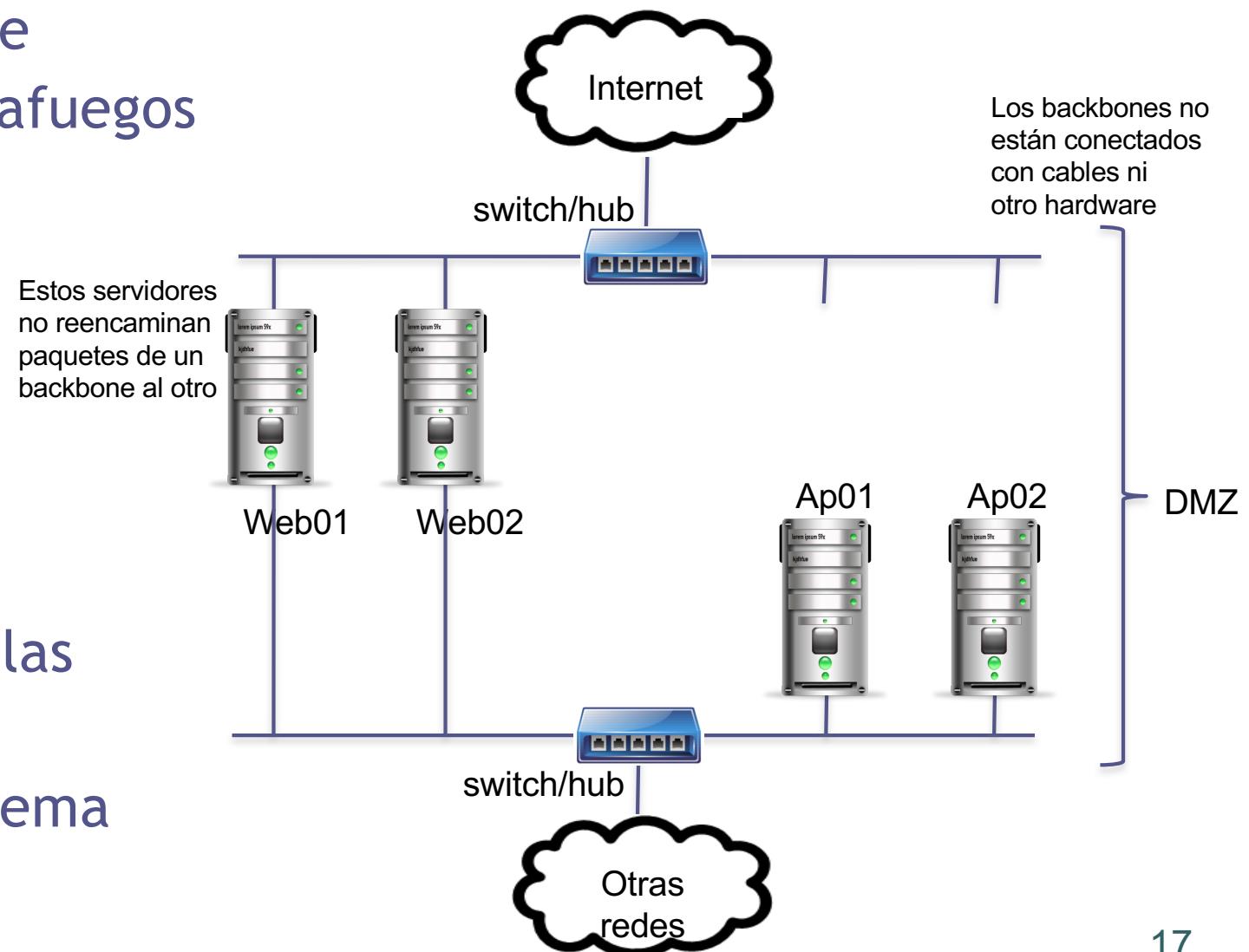
Los servicios de la granja web se ofrecen de forma estándar mediante dirección IP y puerto.

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

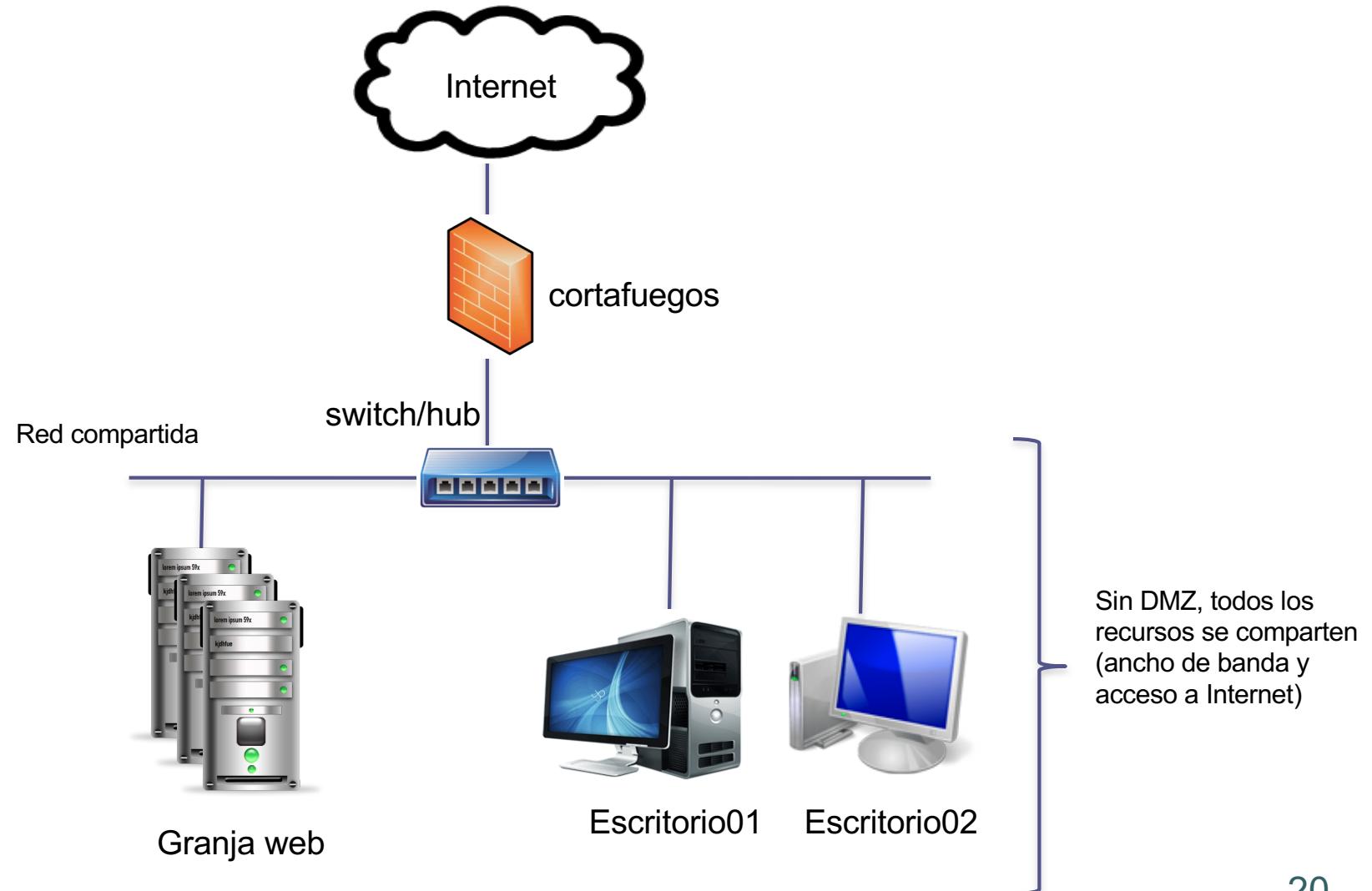
Tanto los **servidores** de la granja web como otras máquinas están conectadas a la **misma subred**.

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.
- Las máquinas de escritorio suponen un problema de seguridad.

4. Configurar una zona segura

2. *Configuración de DMZ simple*

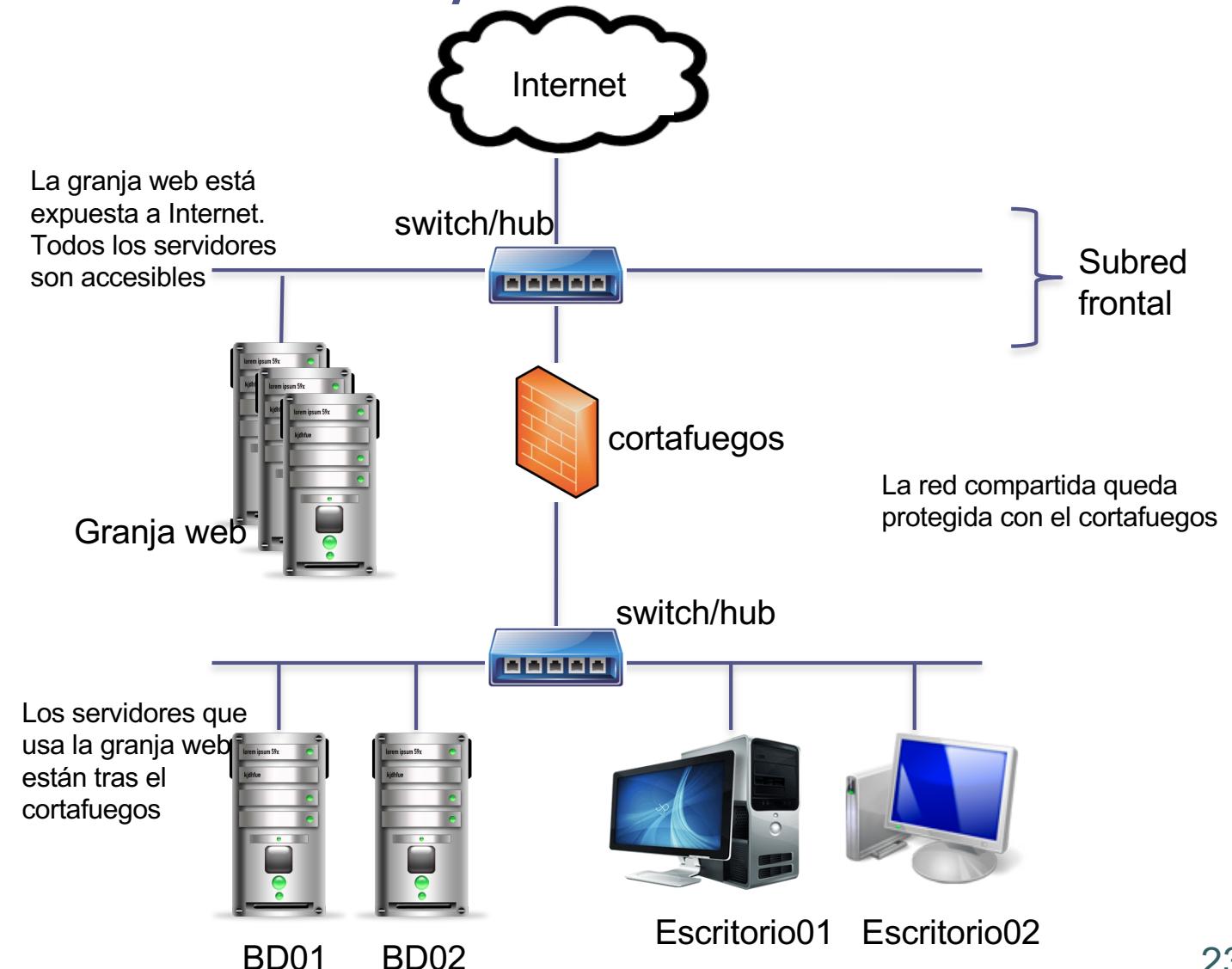
Los **servidores** expuestos deben **aislarse** con un cortafuegos.

Servidores web en una red y servidores de bases de datos o disco en otra, protegida por 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 web 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.
- Las máquinas de escritorio aún están en la misma red que las BD.

4. Configurar una zona segura

3. Configuración de DMZ tradicional

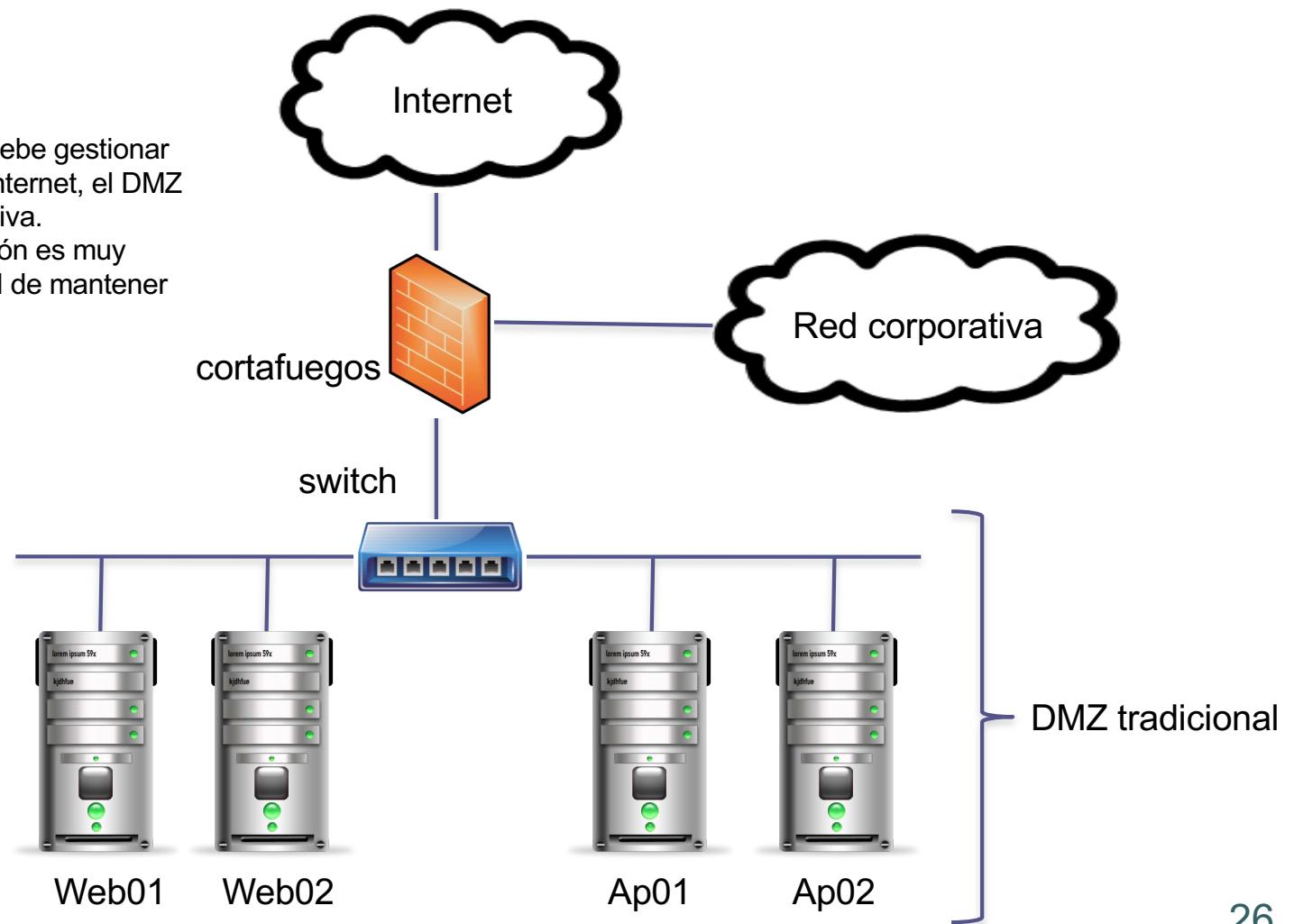
La idea es resolver los problemas de la configuración anterior:

- Evitar ancho de banda de la red corporativa compartido
- Evitar 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 (controlar distintos tipos de redes).
- El cortafuegos es un posible cuello de botella.
- Si la configuración del cortafuegos tiene errores, entonces ¡todo queda expuesto!

4. Configurar una zona segura

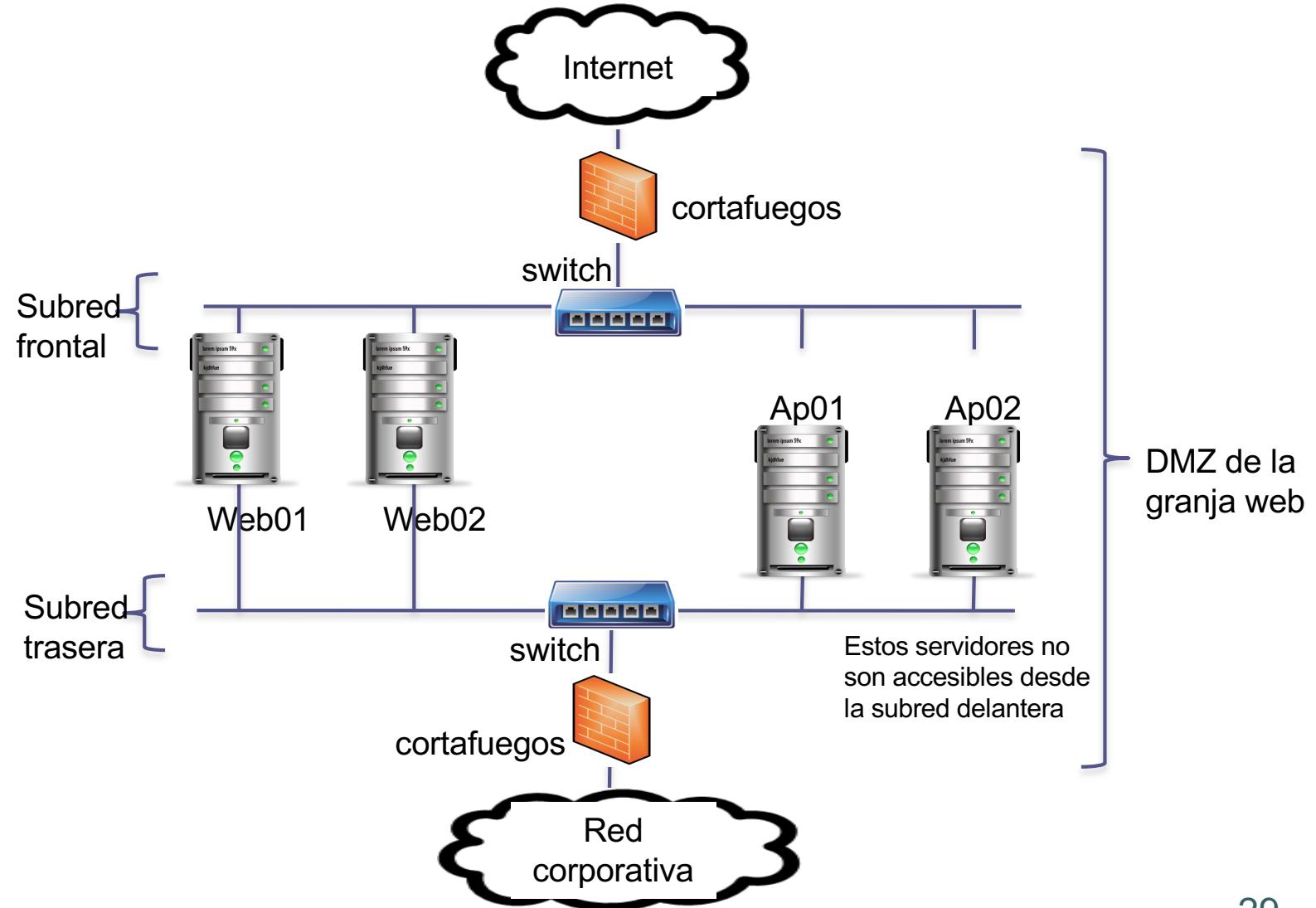
4. Configuración de DMZ doble

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



1. Introducción
2. Configurar la red del sistema web
3. El eje principal de la red del sistema
4. Configurar una zona segura
5. Conectar servidores al front-rail
6. Conectar servidores al back-rail
7. Resumen de configuraciones
8. Conectar la granja web a Internet
9. Conectar la granja web a redes seguras
10. Resumen y conclusiones

5. Conectar servidores al front-rail

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

- HTTP, SMTP, POP3, FTP, etc.

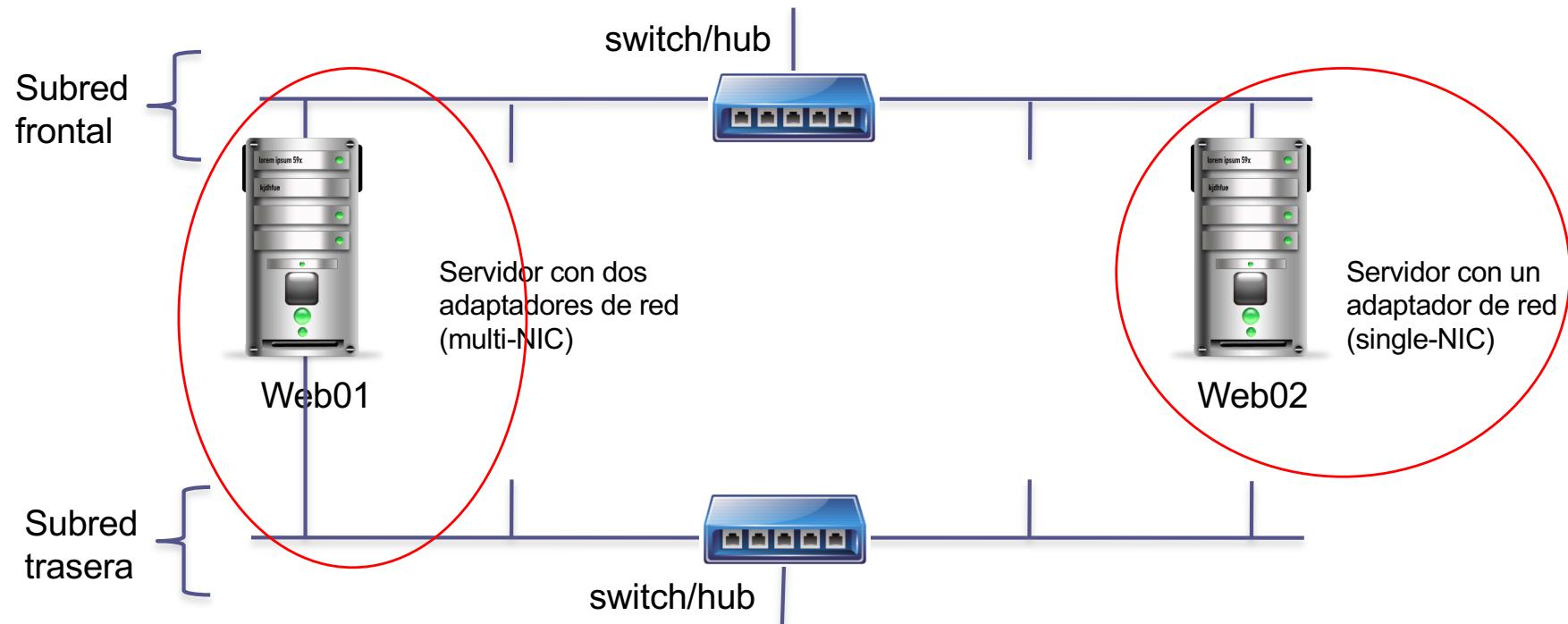
Otros servicios no se ofrecen por el front-rail:

- 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.

Índice



1. Introducción
2. Configurar la red del sistema web
3. El eje principal de la red del sistema
4. Configurar una zona segura
5. Conectar servidores al front-rail
6. Conectar servidores al back-rail
7. Resumen de configuraciones
8. Conectar la granja web a Internet
9. Conectar la granja web a redes seguras
10. Resumen y conclusiones

6. Conectar servidores al back-rail

Los servidores conectados a la subred trasera son accesibles

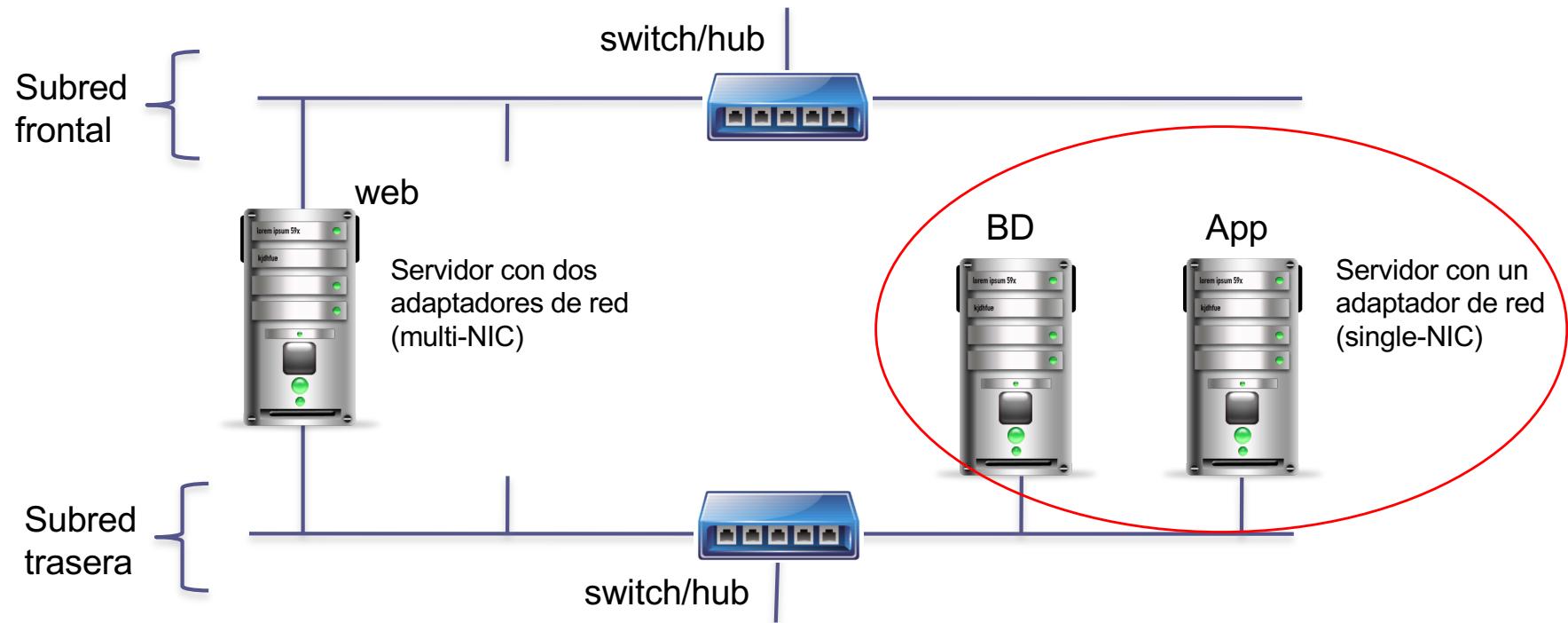
- desde subredes seguras y controladas
- o bien desde servidores con multi-NIC

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.

6. Conectar servidores al back-rail



Índice



1. Introducción
2. Configurar la red del sistema web
3. El eje principal de la red del sistema
4. Configurar una zona segura
5. Conectar servidores al front-rail
6. Conectar servidores al back-rail
- [7. Resumen de configuraciones]**
8. Conectar la granja web a Internet
9. Conectar la granja web a redes seguras
10. Resumen y conclusiones

7. Resumen de configuraciones

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

(1) Doble conexión al front-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



1. Introducción
2. Configurar la red del sistema web
3. El eje principal de la red del sistema
4. Configurar una zona segura
5. Conectar servidores al front-rail
6. Conectar servidores al back-rail
7. Resumen de configuraciones
- 8. Conectar la granja web a Internet**
9. Conectar la granja web a redes seguras
10. Resumen y conclusiones

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.

Ancho de banda: cantidad de información que puede fluir por una conexión de red en un período determinado.
Se mide en bits por segundo (kbps, Mbps, Gbps, Tbps).

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

Los routers actuales permiten establecer esos parámetros.

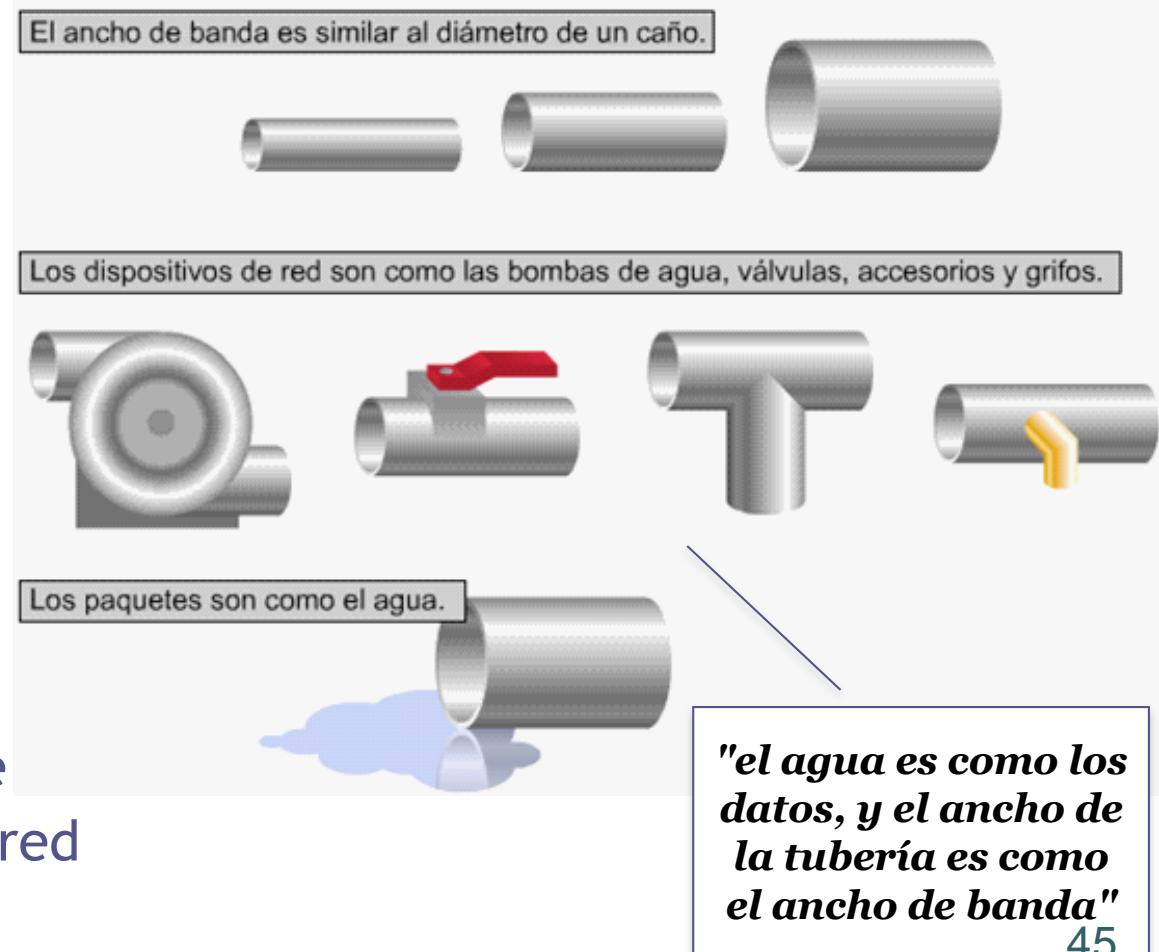
8. Conectar la granja web a Internet

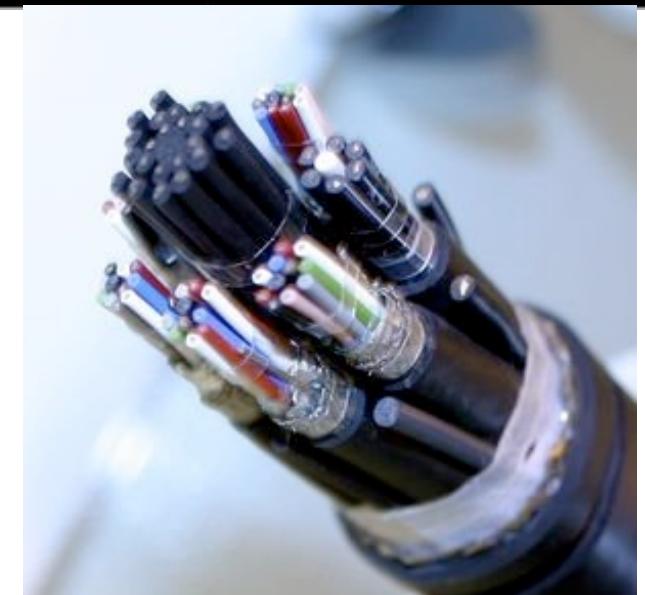
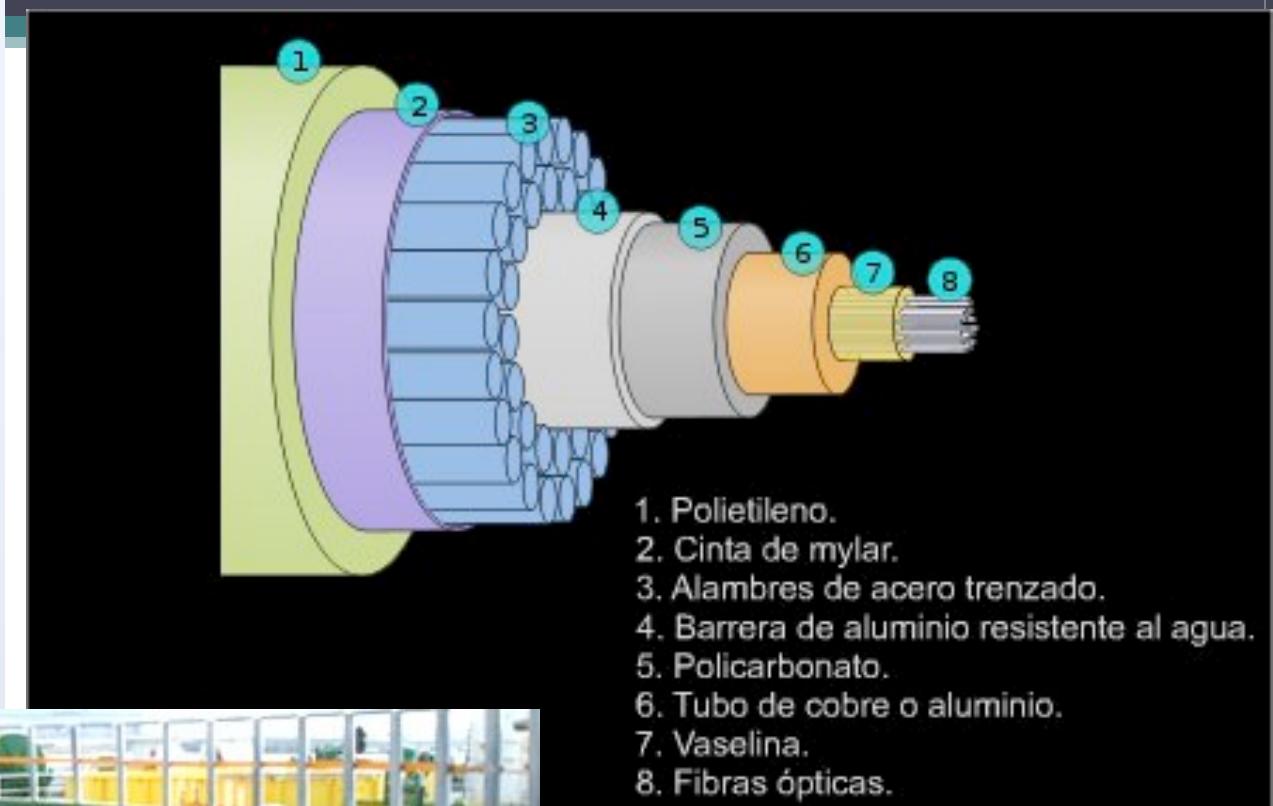
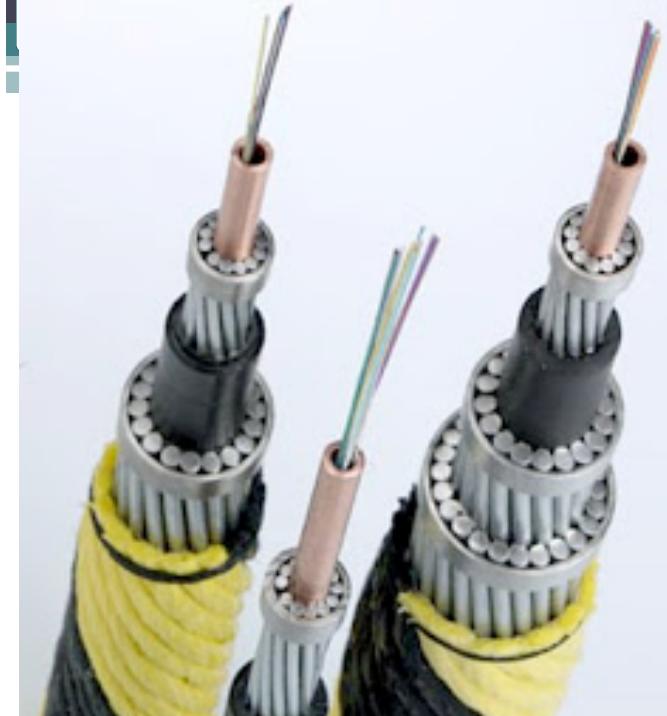
1. *Calidad de servicio y ancho de banda*

<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



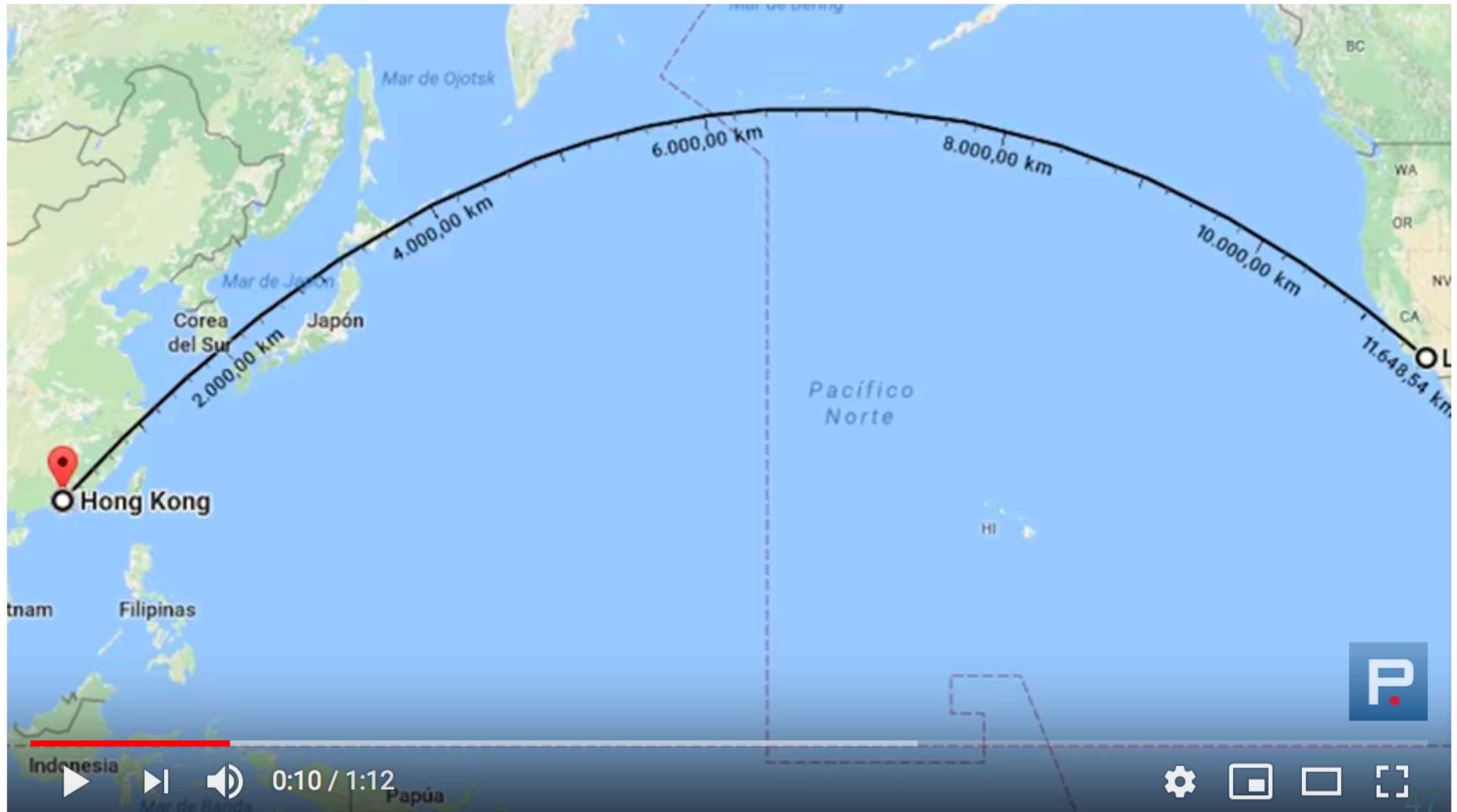


<http://almadeherrero.blogspot.com.es/2008/11/cables-submarinos.html>

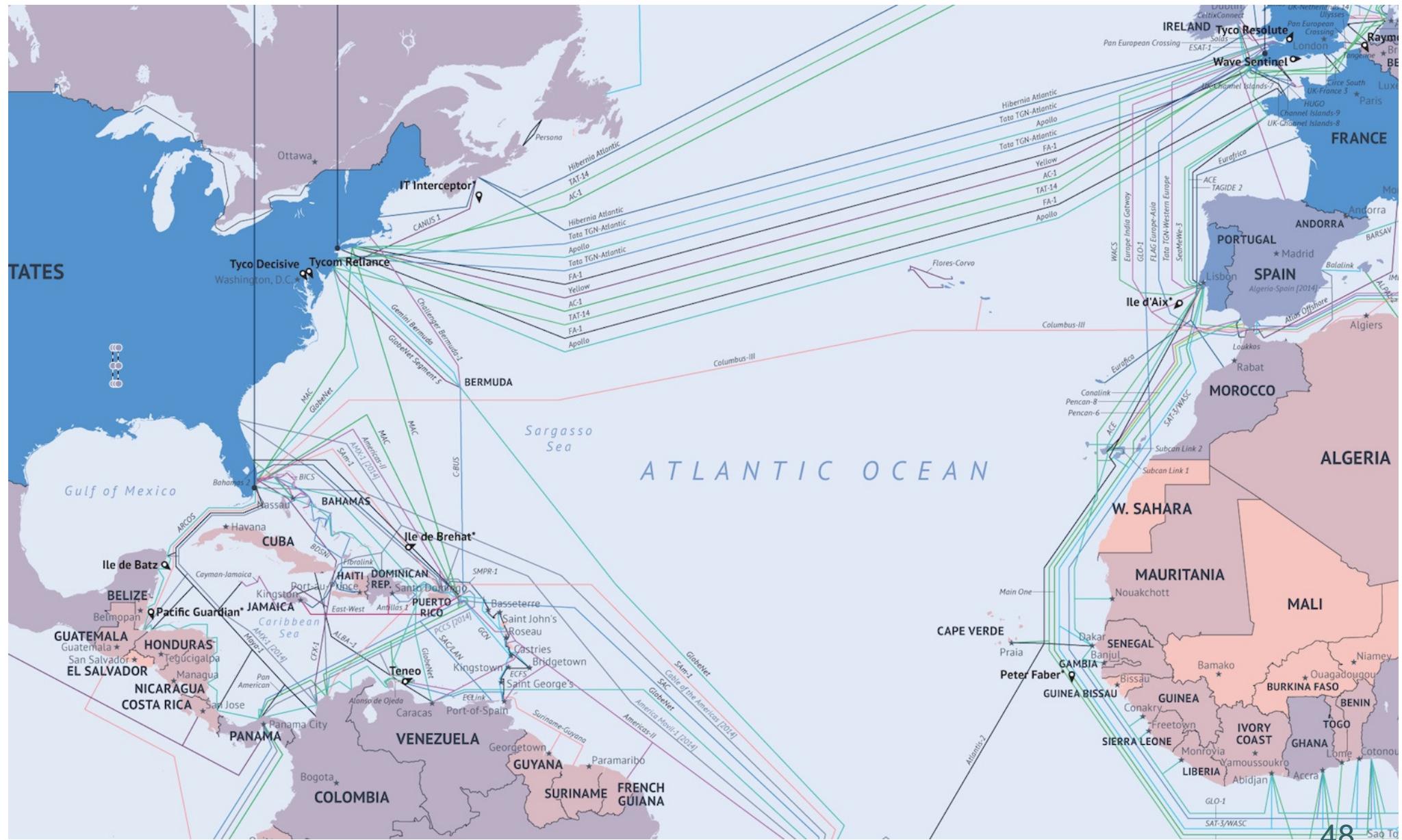
<http://enbytes.com/site/2012/12/06/alcatel-lucent-tiende-cable-submarino-para-consorcio-de-operadores/>

Cables submarinos

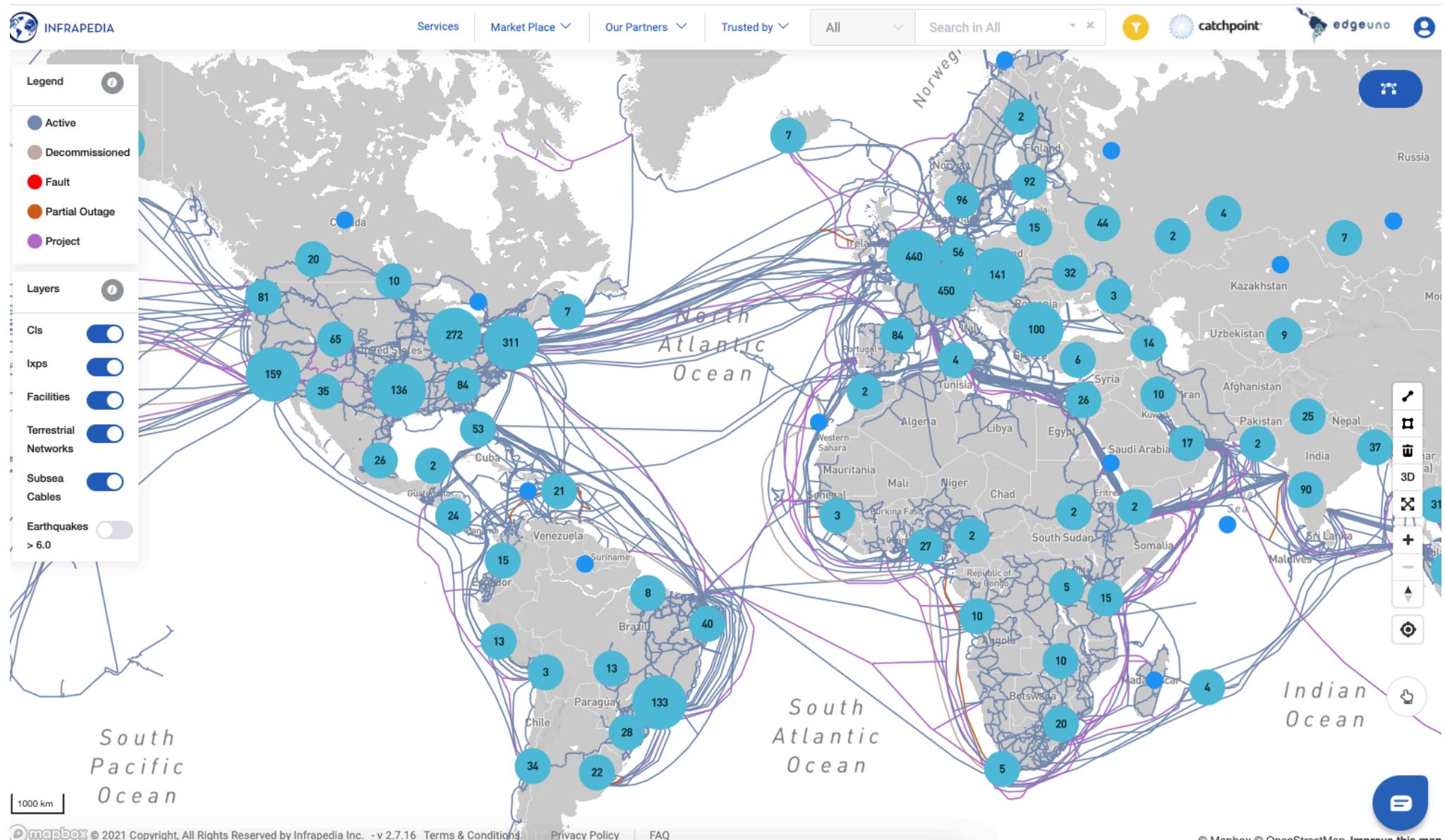
<https://www.youtube.com/watch?v=LMfSIoN7Qf8>



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



<https://www.infrapedia.com/>





MUNDOREAL™

La Guerra Fría en 2015: del temor a la bomba atómica al temor a la motosierra

POR **NACHO PALOU** — 26 DE OCTUBRE DE 2015



En *The New York Times*, **Russian Ships Near Data Cables Are Too Close for U.S. Comfort**,



Que haya submarinos y buques situados cerca de los cables submarinos de telecomunicaciones e Internet supone una preocupación para militares y agentes de inteligencia

EL MUNDO

Líder mundial en español | Miércoles 06/04/2011. Actualizado 22:37h.

SUCESO | Buscaba chatarra

Detenida una mujer de 75 años tras dejar a Armenia sin conexión a Internet

Afp | Tbilisi

Actualizado miércoles 06/04/2011 22:37 horas



Una georgiana de 75 años de edad ha sido detenida por cortar la conexión de Internet de la totalidad de Armenia.

El pasado 28 de marzo la jubilada descubrió el cable de fibra óptica que suministra la conexión web entre Georgia y Armenia mientras buscaba chatarra. Reconociendo el valor del cobre contenido en el cable, la anciana decidió cortar y robarlo, y al hacerlo interrumpió el servicio de miles de usuarios en el país vecino.

Cables submarinos

<https://computerhoy.com/noticias/internet/cables-submarinos-google-atacados-tiburones-17231>



8. Conectar la granja web a Internet

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

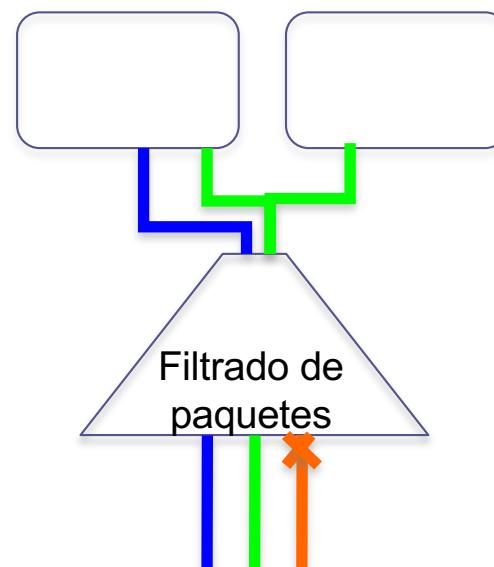
1. Calidad del servicio y ancho de banda
2. **Filtrado y bloqueo de paquetes**
3. Network address translation (NAT)

8. Conectar la granja web a Internet

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.

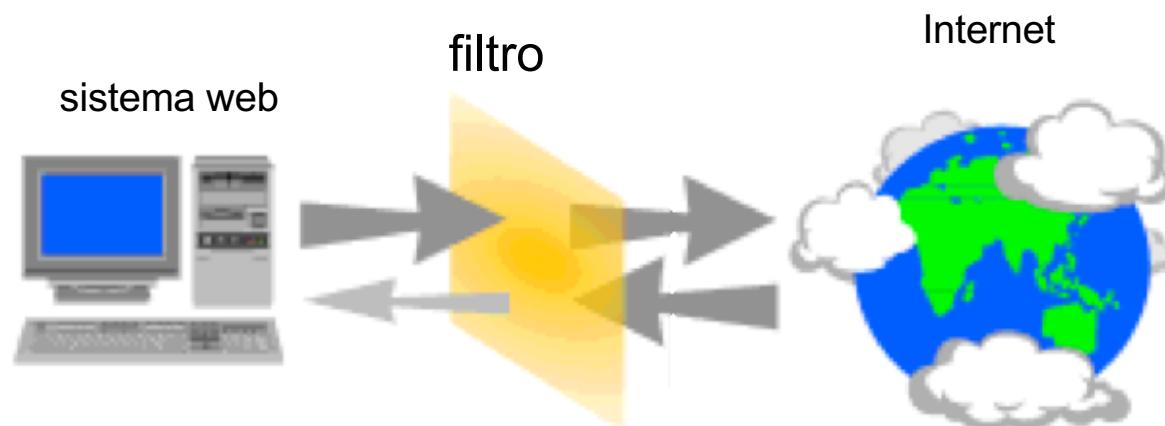


8. Conectar la granja web a Internet

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.

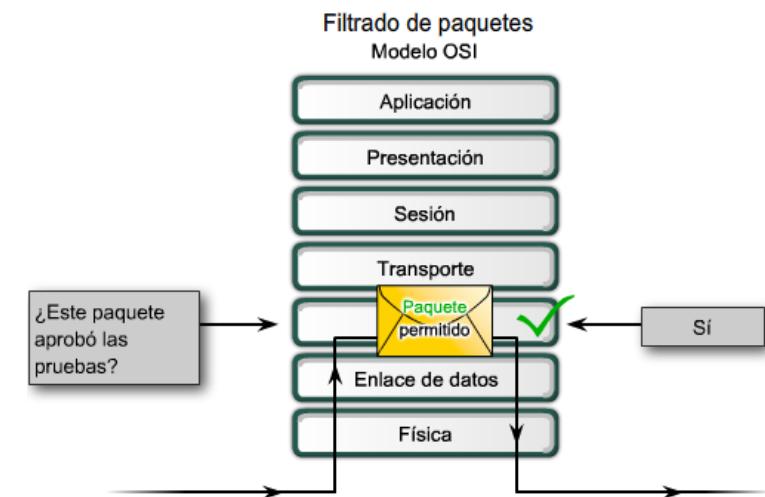


8. Conectar la granja web a Internet

2. *Filtrado y bloqueo de paquetes*

Routers. Un router de filtrado de paquetes utiliza reglas para determinar la autorización o denegación del tráfico según:

- Dirección IP de origen
- Dirección IP de destino
- Tipo de mensaje ICMP
- Puerto TCP/UDP de origen
- Puerto TCP/UDP de destino



“Una ACL es una lista secuencial de sentencias de permiso o denegación que se aplican a direcciones IP o protocolos de capa superior”

8. Conectar la granja web a Internet

2. Filtrado y bloqueo de paquetes

Routers. ¿Cómo funcionan las ACL?

Las ACL no actúan sobre paquetes que se originan en el mismo router.

Las ACL se configuran para ser aplicadas al tráfico entrante o saliente.

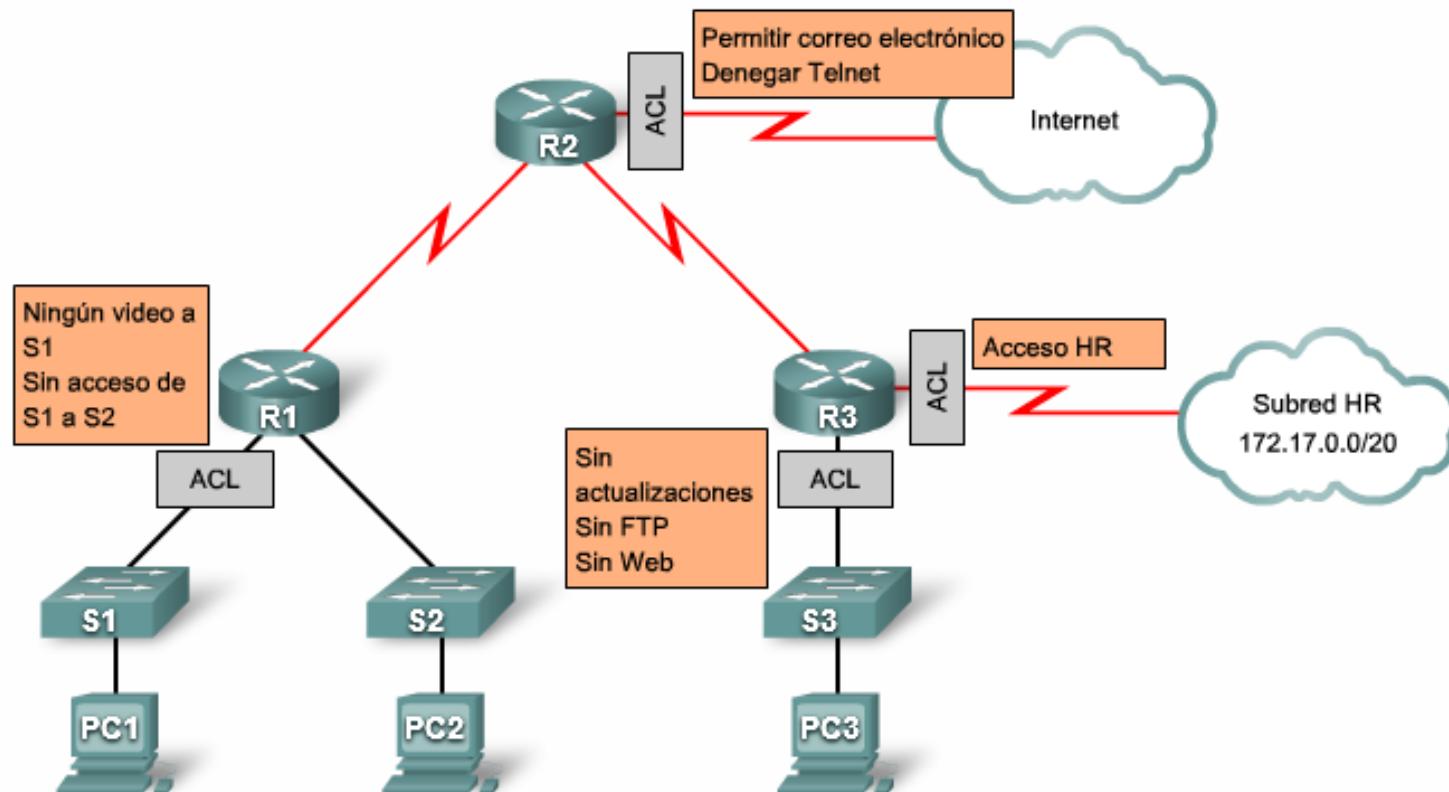
Las sentencias de la ACL operan en orden secuencial.

Una sentencia implícita final cubre todos los paquetes para los cuales las condiciones no resultan verdaderas (implicit deny any statement/deny all traffic).

8. Conectar la granja web a Internet

2. Filtrado y bloqueo de paquetes

Routers. ¿Cómo funcionan las ACL?



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

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 (back-end).

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

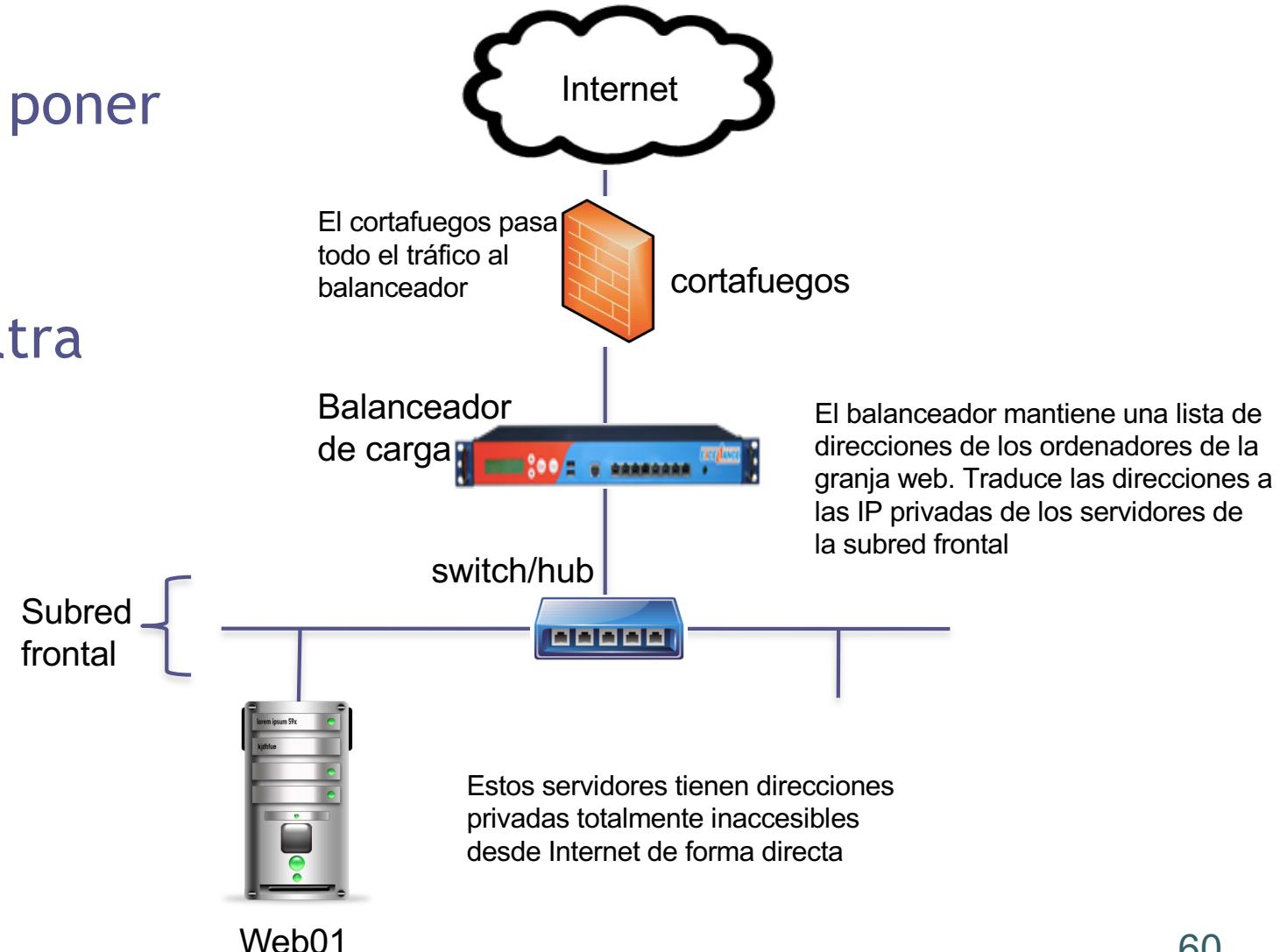
8. Conectar la granja web a Internet

3. NAT: Network Address Translation

Incluso podemos poner varios niveles:

El cortafuegos filtra los paquetes.

El balanceador distribuye.



Índice



1. Introducción
2. Configurar la red del sistema web
3. El eje principal de la red del sistema
4. Configurar una zona segura
5. Conectar servidores al front-rail
6. Conectar servidores al back-rail
7. Resumen de configuraciones
8. Conectar la granja web a Internet
9. Conectar la granja web a redes seguras
10. Resumen y conclusiones

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

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:

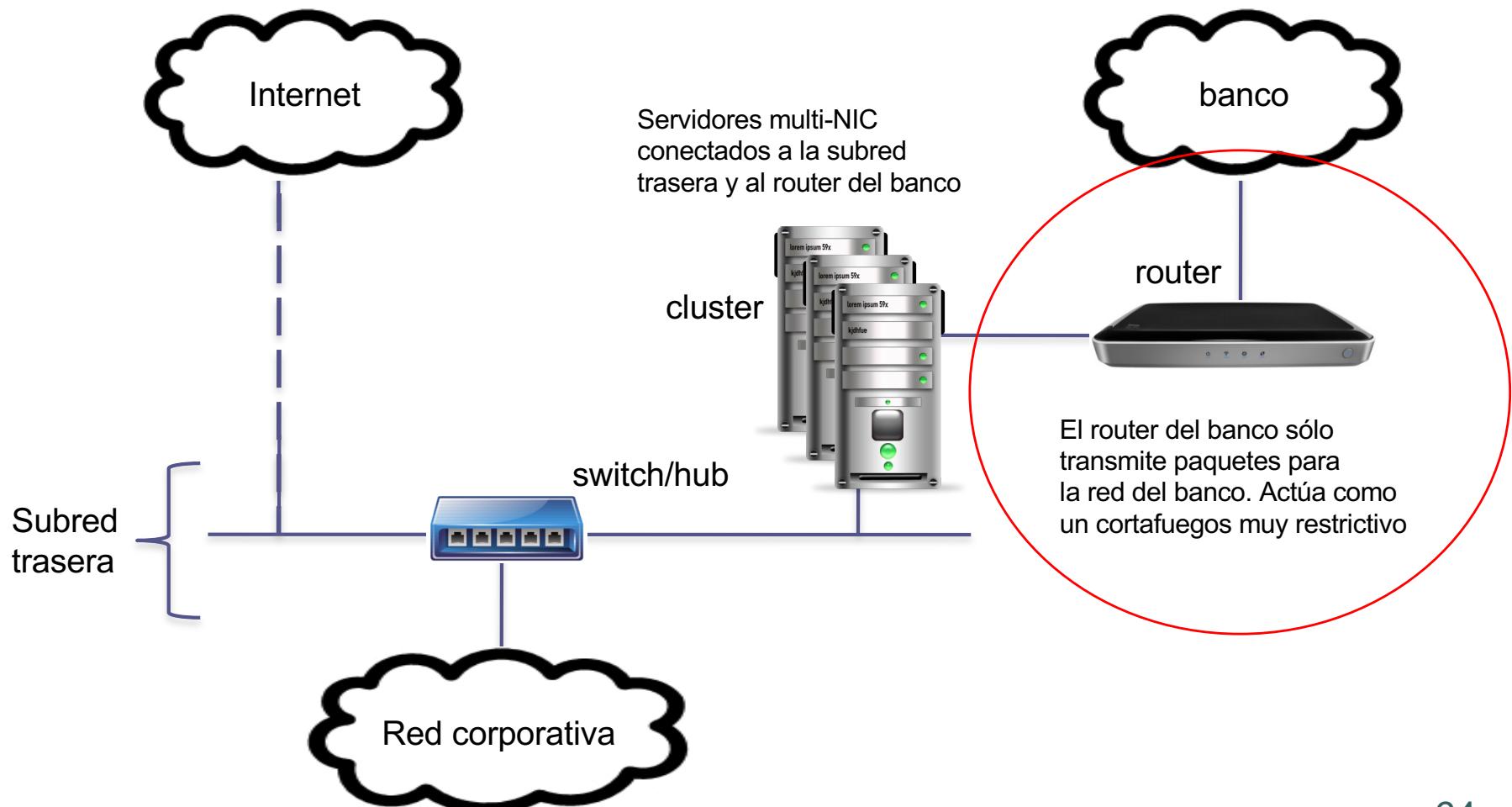
Queremos usar los servicios de un banco para cobrar con tarjeta de crédito (operación de riesgo).

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.

p.ej. configurar un servidor en el back-rail como pasarela para las operaciones con tarjeta de crédito.

Índice



1. Introducción
2. Configurar la red del sistema web
3. El eje principal de la red del sistema
4. Configurar una zona segura
5. Conectar servidores al front-rail
6. Conectar servidores al back-rail
7. Resumen de configuraciones
8. Conectar la granja web a Internet
9. Conectar la granja web a redes seguras

[10. Resumen y conclusiones]

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).