

Tema 6

Asegurar el sistema web



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

Índice



- [1. Introducción]
- 2. Defensa en profundidad
- 3. Políticas de seguridad
- 4. Asegurar un servidor
- 5. Cortafuegos
- 6. Evitar ataques
- 7. Prácticas de seguridad recomendadas
- 8. Conclusiones

Introducción

Asegurar la granja web es una tarea muy importante para cualquier sitio web.

Permite saber quién hizo cada cosa y en qué momento.

La seguridad es fundamental para proteger los datos propiedad de la empresa y la información de los usuarios.

El fin último es evitar (o al menos dificultar en lo posible) que un hacker malicioso realice cualquier acción que afecte al sistema.

Introducción

Se trata de **asegurar y mejorar la disponibilidad** del sitio y también de asegurarse de que las operaciones que se lleven a cabo en el sitio sean **seguras**.

Las políticas de seguridad y los procedimientos para implementar esas políticas son clave en el diseño de una granja web.

Introducción

Los objetivos de seguridad deben definirse correctamente y se basan en los siguientes conceptos:

- **Confidencialidad:** las comunicaciones deben ser secretas.
- **Integridad:** los mensajes enviados deben ser exactamente los recibidos.
- **Disponibilidad:** la comunicación con cualquier aplicación o servicio de la granja web debe estar disponible en el momento en que sea requerida.

Introducción

En este tema trataremos:

- Comprender el concepto de **defensa en profundidad** (diferentes capas de defensa).
- Establecer **políticas de seguridad**, incluyendo claves seguras, para todas las cuentas.
- Asegurar un servidor mediante la **eliminación de servicios innecesarios y vulnerabilidades**.
- **Usar un cortafuegos:** comprender el funcionamiento de los cortafuegos y los beneficios de estos.



Índice

1. Introducción
- 2. Defensa en profundidad**
3. Políticas de seguridad
4. Asegurar un servidor
5. Cortafuegos
6. Evitar ataques
7. Prácticas de seguridad recomendadas
8. Conclusiones

Defensa en profundidad

Importancia de la arquitectura de seguridad.

Incluso en el mundo real, se controla el acceso a los recursos de un edificio o empresa con varias capas.

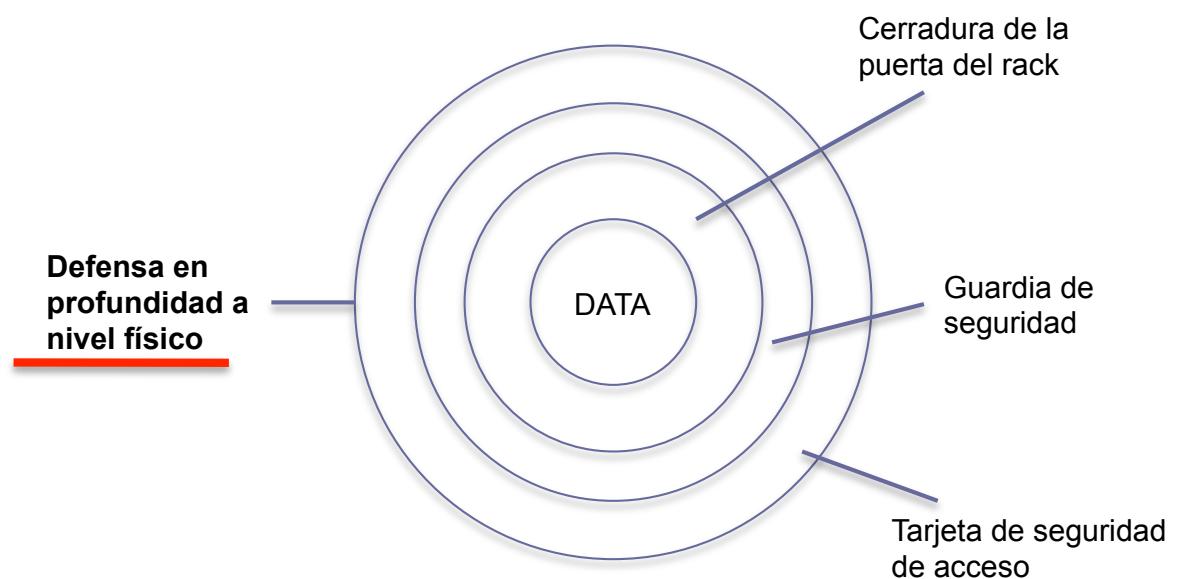
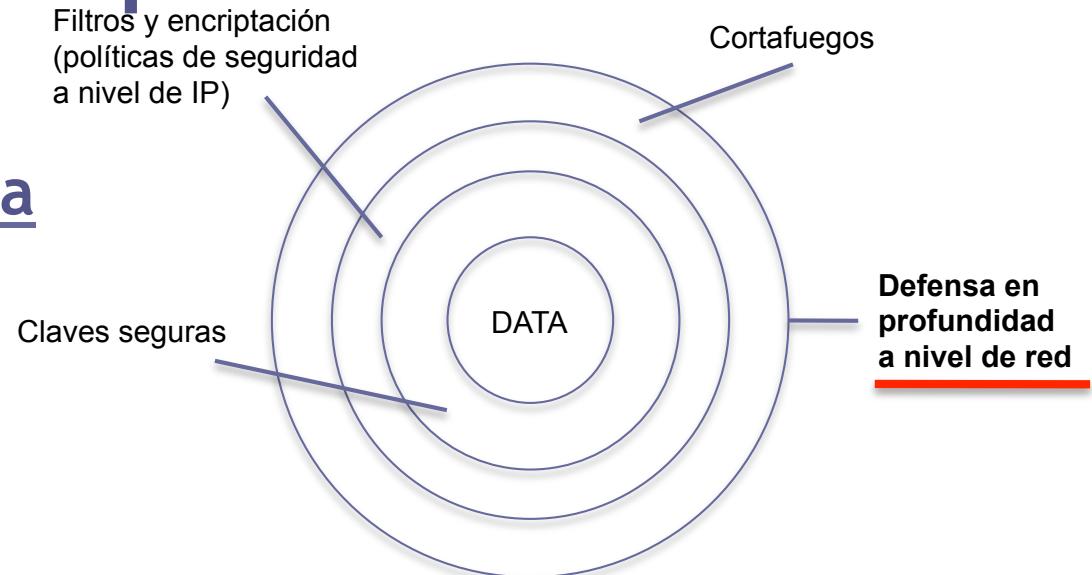
EJ: *en un banco hay varios niveles de seguridad para proteger el dinero (varios sistemas de seguridad de diferente tipo que superar para hacerse con el dinero):*

- (1) *el dinero está guardado en cajas fuertes. Para acceder a ese dinero, los clientes deben identificarse.*
- (2) *el banco utiliza video-vigilancia y mantiene registros detallados de todas las transacciones.*

Defensa en profundidad

Protección del sistema a diferentes niveles.

Un hacker debería superar cada una de las capas independientemente para acceder a los datos



Defensa en profundidad

¿Son necesarios tantos niveles?

Sí

Ningún sistema de seguridad es totalmente seguro...

La forma de complicarle la tarea a un hacker es poner más de un nivel de seguridad.

Incrementar el tiempo necesario para superar cada nivel hace que sea más probable detectar un ataque, y así evitar que las últimas defensas se vean comprometidas.

Defensa en profundidad

Importante estar al día en cuanto a temas de seguridad en todos los frentes.

El administrador responsable de la seguridad informática debe conocer los temas relativos a la seguridad así como las vulnerabilidades a nivel de red, de cortafuegos, de sistema operativo y de las aplicaciones en el sistema web.

Defensa en profundidad

Hay que estar pendientes a los grupos de noticias, listas de correo, blogs y foros sobre estos temas.

Cuando se identifica una vulnerabilidad, los administradores de seguridad deben tomar **medidas de prevención** ya que los hackers estarán atentos para aprovecharla.

Estas investigaciones y estudios sobre seguridad en ciertas organizaciones suelen **revelar los puntos débiles** de los sistemas web de otras en las que no aplican políticas de seguridad.

Al día en temas de seguridad...

<http://www.securitybydefault.com/>

- Mitigación de ataques DDoS basados en inundamiento
- Cómo saber si tu DNS puede ser empleado para un ataque DDoS

<http://www.securitybydefault.com/search/label/DDoS>



- Cómo CyberBunker atacó a Spamhaus y casi se llevó a medio Internet por delante

<http://bit.ly/14q7HmK> (*mitigado a través de CloudFare*)

CyberBunker



Al día en temas de seguridad...

- DDoS contra Movistar.es ¿Causada o preparada?

<http://www.securitybydefault.com/2011/06/ddos-contra-movistares-causada-o.html>

- La resolución DNS de **www.movistar.es devuelve una única IP: 81.47.192.13**. Lo que indica un único punto de entrada a la web.
- Está claro que Movistar no tiene un único servidor para atender las peticiones de www.movistar.es (y que mucho menos es una sola máquina), por lo que suponemos que será una **IP de clúster de servidores**, posiblemente *nateados* por un potente clúster de firewalls o más probablemente de **balanceadores**.
- Si efectuamos una consulta a www.movistar.es desde el navegador utilizando Tamper Data para ver las cabeceras, se observa que una de las mismas que devuelve movistar.es, es "**Via 1.1 proxy-srnav2np10**" y "**Proxy Agent Sun-Java-System-Web-Proxy-Server/4.0.2**". Esto quiere decir que hay algún elemento intermedio que hace la petición por nosotros hasta el servidor web que corresponda. Esto puede ser un WAF, un balanceador, una caché o simplemente un proxy inverso.
- **Puede que hayan tenido alguna incidencia en alguno de los servidores web** (por un excesivo número de peticiones o por cualquier otro motivo) y que mostrara un "sencillo error de página no encontrada" y que ciertas peticiones entraran y se sirvieran correctamente por un servidor que no mostrase problemas.
- Otra forma de verlo es que la **propia gente de Movistar modificó la web**, de manera que **en vez de tener que servir todos los contenidos** de la web, ante una "legión" de peticiones de Anonymous, prefiriesen **servir una única página con sólo un corto texto** referido a un sencillo mensaje de error.
- De esta manera **podrían luego decir que el DDoS de Anonymous no tuvo efecto alguno** en la infraestructura. Desde un punto de vista de pérdida de recursos, es cierto, las peticiones no fueron suficientes para colapsar el servicio web puesto que eran los servidores de Movistar los que servían la "página de error",

Índice



1. Introducción
2. Defensa en profundidad
- [3. Políticas de seguridad]**
4. Asegurar un servidor
5. Cortafuegos
6. Evitar ataques
7. Prácticas de seguridad recomendadas
8. Conclusiones

Políticas de seguridad

Las políticas de seguridad **definen cómo se les permite interaccionar a los usuarios con los servidores y el hardware de la red del sistema web.**

Todas las políticas definen:

- procedimientos de identificación y acceso
- o privilegios de uso.

Políticas de seguridad

Los procedimientos de identificación comprueban si un individuo es reconocido por los sistemas de seguridad de la granja web:

- cortafuegos
- router
- servidor web
- servidor de BD

Los privilegios de uso definen qué acciones puede llevar a cabo cada tipo de usuario correctamente identificado.

Políticas de seguridad

Los procedimientos de autenticación comienzan solicitando una identificación (nombre de usuario + clave). De la validez de esta identificación dependerá que se permita o deniegue el acceso.

¿Qué se suele utilizar?

- Una clave o PIN
- Una tarjeta física que incluirá la clave
- Un escáner de retina, huella dactilar o ADN

...del menos efectivo al más efectivo.

Usar dos, especialmente si el primero es una simple clave.

Políticas de seguridad

retina / huella / tarjeta



Políticas de seguridad

Ejemplo: algunas empresas usan dos factores:

El primero, una **tarjeta de identificación** con la que se le permite a los empleados acceder a ciertas áreas.

El segundo suele ser una **identificación** (usuario y clave) en la red de ordenadores. Con ella podrá acceder a ciertos recursos, aunque a ciertas otras máquinas no.

En los **dominios de seguridad** los administradores definen listas de control de acceso (usuarios o grupos que pueden acceder a ciertos recursos concretos).

Políticas de seguridad

Aplicar políticas a diferentes niveles:

1. Seguridad a nivel físico
2. Seguridad a nivel de red
3. Seguridad a nivel de administrador
4. Cuentas de servicios (o aplicaciones)

Políticas de seguridad

1. Seguridad a nivel físico

La seguridad a nivel físico es tan importante como la del nivel de red a la hora de proteger los recursos de un sistema.



De nada vale tener instalados los mejores cortafuegos y routers si un atacante puede entrar a la sala donde están las máquinas y tener acceso a la consola del servidor...



Si atacan remotamente, podremos reiniciar, reconfigurar o reinstalar, pero si ha sido dañado físicamente el problema puede ser más serio y costoso.

Políticas de seguridad

1. Seguridad a nivel físico. Puntos a tener en cuenta:

- Ubicación de los servidores y elementos críticos de red: los servidores deben de estar ubicados en un espacio aislado, de acceso controlado y bien diferenciado del resto de la oficina.

Deben de poseer un ambiente refrigerado y libre de emisiones de polvo y humos. Las salas y los pasillos de acceso deben de ser totalmente opacos y sin puertas de cristal. Las puertas de acceso deben de tener una cerradura de seguridad. Y sería deseable en casos extremos la vigilancia mediante circuito cerrado de TV.

Políticas de seguridad

1. Seguridad a nivel físico. Puntos a tener en cuenta:

- **Contraseñas de BIOS y de consola:** los servidores deben de estar protegidos mediante contraseñas de BIOS y de consola.

Dichas contraseñas deben de ser conocidas exclusivamente por las personas indispensables, cumplir ciertas normas de seguridad, guardarse en un sobre lacrado para emergencias, cambiarse periódicamente y nunca dejar las contraseñas por defecto que el fabricante o distribuidor proporcione.

Políticas de seguridad

1. Seguridad a nivel físico. Puntos a tener en cuenta:

- **Seguridad general del hardware:** hay que evitar posibles robos, tanto del sistema entero como de componentes individuales (los discos).

Políticas de seguridad

2. Seguridad a nivel de red

La forma más usual de **ataque** a cualquier sistema será mediante una conexión de red.

Cualquier gran sistema tendrá **al menos dos subredes**: una subred segura usada por los administradores e Internet.

Ambas representan **dominios de seguridad** (subred interna e internet).

Políticas de seguridad

3. Seguridad a nivel de administrador

Los administradores de sistemas necesitan tener permisos para investigar, configurar y arreglar cualquier elemento software o hardware de un sistema web. La forma más sencilla es **darles todos los permisos posibles**, por ejemplo manteniendo un grupo de administradores.

Otra forma es **organizando los administradores por aplicación**. De esta forma cada aplicación tiene su grupo de administradores, ya estén en el equipo de desarrollo, test o mantenimiento.

Políticas de seguridad

3. Seguridad a nivel de administrador

Ejemplo:

si una granja web tiene tres aplicaciones, el dominio de seguridad de ésta debe tener configurados tres grupos de administradores.

Según al que se pertenezca, tendrá acceso a los recursos de cierta aplicación, y no a los de otras.

Así, cada grupo estará en los administradores de todos los servidores que cada aplicación usa.

Y si dos aplicaciones comparten los servicios de un servidor, añadiremos ambos grupos a los administradores de dicho servidor.

Políticas de seguridad

3. Seguridad a nivel de administrador



Importante no usar nunca estas cuentas de administración para tareas de las aplicaciones en que no sean imprescindibles.

Cuando cualquier persona que usaba esas cuentas deje el trabajo, la **cuenta debe ser eliminada** de todos los grupos, aún a riesgo de que el desarrollo de una aplicación se vea afectado.

Los responsables de seguridad deben asegurarse de que todas esas cuentas tienen **claves seguras** y que éstas se cambian frecuentemente.



Políticas de seguridad

4. Cuentas de servicios

Son las usadas por cualquier aplicación para acceder a los recursos de forma segura.

No usar para acceder de forma interactiva a los servidores.

El administrador crea las cuentas (nombre y clave) en cada servidor ante la configuración de un nuevo servicio, dando los permisos necesarios.

Para los accesos anónimos desde Internet a un sitio web, se suele crear cuenta de usuario anónimo.

Políticas de seguridad

4. Cuentas de servicios

Para las aplicaciones que se ejecutan en el servidor se deben crear cuentas específicas (cuentas de servicios):

- Crear una **cuenta de usuario especial** y que todas las aplicaciones y servicios usen dicha cuenta (tomen el papel de dicho usuario). Ese usuario puede tener permisos de administración en ciertos servidores si es necesario.
- Crear **cuentas locales** y mapear esos nombres de usuario y clave a los demás servidores que la aplicación necesite.

Políticas de seguridad

Toda organización con un gran sistema web debe tener un **equipo de ingenieros con dedicación exclusiva** a desarrollar, investigar, responder y arreglar temas de **seguridad** del sistema a todos los niveles.

Índice



1. Introducción
2. Defensa en profundidad
3. Políticas de seguridad
- 4. Asegurar un servidor**
5. Cortafuegos
6. Evitar ataques
7. Prácticas de seguridad recomendadas
8. Conclusiones

Asegurar un servidor

Proceso en el que eliminamos

- características no necesarias,
- servicios,
- configuraciones e
- información de seguridad del servidor,

de forma que sólo se dejen las aplicaciones, servicios y puertos realmente necesarios.

Asegurar un servidor

Dos fases:

- (1) una vez que el servidor ha sido montado y configurado por primera vez, hacer **cambios de configuración** necesarios, y ajustes dependientes del entorno en que el servidor va a trabajar.
- (2) **mantenimiento continuo** que hay que ir haciendo debido a nuevos parches de seguridad para proteger de los ataques que van surgiendo.

Asegurar un servidor

Acciones a tomar:

- **Eliminar cuentas y grupos de usuarios no necesarios.** Cuentas e información por defecto que puede ser aprovechada fácilmente por cualquier hacker malicioso. Debemos dejar las cuentas y grupos utilizadas por las aplicaciones o servicios del sistema operativo.
- **Renombrar las cuentas de administrador e invitado.** Todo el mundo sabe el nombre de la cuenta de administrador en los principales sistemas operativos. Y las de invitado es aconsejable deshabilitarlas.

Asegurar un servidor

Acciones a tomar:

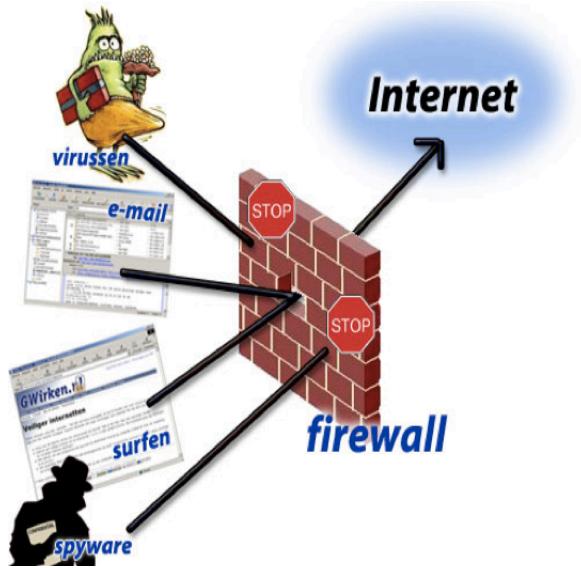
- **Eliminar los drivers de red que no sean necesarios.** Esto puede ser aplicable sólo en ciertos sistemas operativos (p.ej. en Windows). Suelen ser herramientas para transferencia de ficheros o de impresión a alto nivel que pueden ser aprovechados por hackers.
- **Eliminar servicios no necesarios.** En un servidor web podemos deshabilitar el FTP y el SMTP si no se van a usar.
- **Establecer políticas de seguridad.**

Asegurar un servidor

Acciones a tomar:

- **Usar filtros TCP/IP.** Esto se puede usar para controlar el acceso al servidor. Así se puede controlar el tipo de tráfico y limitar por el tipo (TCP, UDP, etc), por el puerto de acceso o por dirección IP.
- **Mantener un equipo de seguridad al día** sobre nuevos agujeros de seguridad, parches de seguridad y ataques. Conviene que estén al tanto de las listas de correo sobre seguridad, foros e incluso sean asiduos visitantes de páginas de hacking.

Índice



1. Introducción
2. Defensa en profundidad
3. Políticas de seguridad
4. Asegurar un servidor
5. Cortafuegos
6. Evitar ataques
7. Prácticas de seguridad recomendadas
8. Conclusiones

Cortafuegos

Un cortafuegos protege el sistema de accesos indebidos.

En un sistema sin cortafuegos, otros elementos del sistema quedarán expuestos a diferentes riesgos.



Cortafuegos

Un cortafuegos protege el sistema de accesos indebidos.

Es el **guardián de la puerta al sistema**, permitiendo el tráfico autorizado y denegando el resto.



Cortafuegos

Colocados entre subredes para realizar diferentes tareas de manejo de paquetes.

Tareas que realizan:

- **Bloquear y filtrar paquetes** de red inspeccionando las direcciones y puertos de cada paquete enviado entre las subredes que separa y controla.
Por defecto, un cortafuegos debería prohibir el tráfico, y en el proceso de configuración se establecerán reglas para permitir cierto tipo de tráfico.

Cortafuegos

Tareas que realizan:

- **Controlar protocolos de aplicación**, como HTTP, FTP, ssh o telnet. Esto se consigue configurando reglas relativas a ciertos puertos.
- **Control del tráfico de red a nivel de protocolo de red** (TCP o UDP). Así, si las reglas permiten la comunicación entre dos servidores, el tráfico (paquetes) fluirán entre ambos mientras la conexión permanezca abierta.

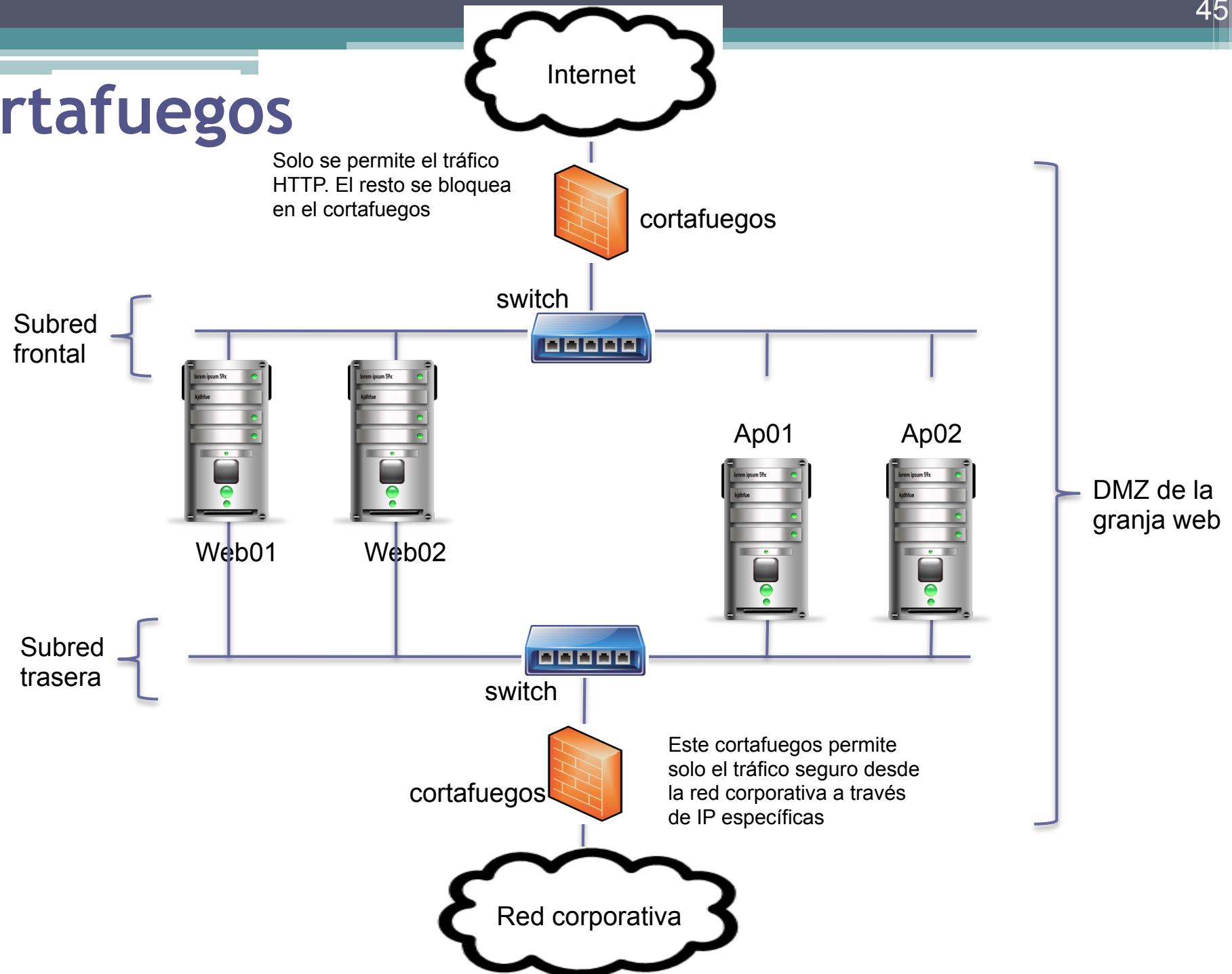
Cortafuegos

Tareas que realizan:

- **Ocultar la verdadera dirección del servidor**, actuando como un proxy. De esta forma traduce la información de dirección de los mensajes entrantes y salientes reenviándolos a su destino.
- **Proteger los servidores y aplicaciones de ataques** y uso indebido controlando el flujo de información. Sin el cortafuegos, todos los servidores de la red serían accesibles para cualquier usuario



Cortafuegos



Cortafuegos

- La implementación y configuración del cortafuegos es **complejo**:
 - instalación de servidores redundantes
 - software y hardware especial
 - balanceo de carga
 - personal especializado para configurar las reglas

Esta complejidad conlleva muchos **beneficios**:



Cortafuegos

Beneficios:

- Evita el consumo excesivo de recursos, reduciendo el tráfico global que un servidor recibirá.
- Oculta los servidores finales a otras redes.
- Protege los servidores de múltiples ataques.
- Oculta información de los servidores a otras redes (evitamos escaneo de puertos).
- Avisa de posibles ataques justo en el momento en que se producen.

Cortafuegos

Todos los mensajes que entran o salen del sistema pasan por el cortafuegos.

Éste examina y bloquea aquellos que no cumplen los criterios de seguridad establecidos.

Estos criterios se configuran mediante un **conjunto de reglas**, usadas para bloquear puertos específicos, rangos de puertos, direcciones IP, rangos de IP, tráfico TCP o tráfico UDP.

Cortafuegos

Construir el conjunto de reglas de la siguiente forma:

- Crear grupos de reglas para conjuntos de servidores que deben responder a diferente tipo de tráfico.
- **Por defecto**, establecer reglas para **denegar el tráfico** que no esté permitido explícitamente.
- **Permitir el tráfico en el sentido necesario** (un servidor web no necesita navegar por Internet).

Cortafuegos

Construir el conjunto de reglas de la siguiente forma:

- Definir rangos de direcciones IP a los cuales aplicar diversas reglas.
- Mantener registros (logs) del tráfico no permitido y de intentos de acceso para estudiar más tarde posibles ataques.

Cortafuegos

Recomendaciones:

1. Configurar el cortafuegos completamente independiente del resto de recursos.
2. La máquina cortafuegos no debe ejecutar otro software salvo el del cortafuegos.
3. Eliminar cualquier servicio accesorio en el cortafuegos.

Cortafuegos

Recomendaciones:

4. Blindar el cortafuegos para que no acepte conexiones directas a él (se comporte como un paso más en el camino y el atacante no se dé cuenta de que está ahí).
5. No registrar la IP del cortafuegos en ningún servicio de DNS, ya que su IP no es necesaria para que los clientes accedan a la granja web.
6. No permitir acceso desde Internet para administrar el cortafuegos, ya que un hacker podría conseguir acceso al mismo.

Cortafuegos

Configurar el cortafuegos en Linux con iptables:

Tutoriales:

<http://www.cyberciti.biz/tips/linux-iptables-examples.html>

<http://bit.ly/17Vqwi3>

<http://es.tldp.org/Manuales-LuCAS/doc-iptables-firewall/doc-iptables-firewall-html/>

Configurar el cortafuegos con iptables

(proteger un servidor web):

```
#!/bin/sh
## FLUSH de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
## Establecemos politica por defecto
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

# desde el localhost se permite todo
/sbin/iptables -A INPUT -i lo -j ACCEPT

# A nuestra IP le dejamos todo
iptables -A INPUT -s 195.65.34.234 -j ACCEPT
# El puerto 80 de www debe estar abierto, es un servidor web.
iptables -A INPUT -p tcp --dport 80 -j ACCEPT

# el resto, cerrado
iptables -A INPUT -p tcp --dport 20:21 -j DROP
iptables -A INPUT -p tcp --dport 3306 -j DROP
iptables -A INPUT -p tcp --dport 22 -j DROP
iptables -A INPUT -p tcp --dport 10000 -j DROP
```

Cortafuegos

Configurar el cortafuegos con iptables (ejemplos):

Evitar el acceso a www.facebook.com:

```
iptables -A OUTPUT -p tcp -d 69.171.224.0/19 -j DROP
```

También se puede usar el nombre de dominio:

```
iptables -A OUTPUT -p tcp -d www.facebook.com -j DROP  
iptables -A OUTPUT -p tcp -d facebook.com -j DROP
```

Cortafuegos

Ejercicio T6.1:

Aplicar con iptables una política de denegar todo el tráfico en una de las máquinas de prácticas.

Comprobar el funcionamiento.

Aplicar con iptables una política de permitir todo el tráfico en una de las máquinas de prácticas.

Comprobar el funcionamiento.

Cortafuegos

Configurar el cortafuegos con iptables (ejemplos):

Bloquear todo el tráfico ICMP (ping):

```
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP  
iptables -A INPUT -i eth1 -p icmp --icmp-type echo-request -j DROP
```

Abrir el puerto 22 (SSH):

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT  
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 22 -j ACCEPT
```

Abrir el puerto 80 (HTTP/HTTPS, servidor web):

```
iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT  
iptables -A INPUT -m state --state NEW -p tcp --dport 443 -j ACCEPT
```

En esas órdenes, si cambiamos ACCEPT por DROP bloquearemos ese tráfico.

Cortafuegos

Configurar el cortafuegos con iptables (ejemplos):

Comprobación del funcionamiento del cortafuegos

Con la siguiente orden, comprobaremos qué puertos hay abiertos y cuáles cerrados:

```
netstat -tulpn
```

Para asegurarnos del estado del puerto 80 (abierto/cerrado), ejecutar:

```
netstat -tulpn | grep :80
```

Cortafuegos

Configurar el cortafuegos con iptables (ejemplos):

Comprobación del funcionamiento del cortafuegos

```
pedro@maquina:~$ sudo netstat -tulpn
```

Conexiones activas de Internet (solo servidores)						
Proto	Recib	Enviad	Dirección local	Dirección remota	Estado	PID/Program name
tcp	0	0	127.0.1.1:53	0.0.0.0:*	ESCUCHAR	1132/dnsmasq
tcp	0	0	0.0.0.0:22	0.0.0.0:*	ESCUCHAR	7185/sshd
tcp	0	0	127.0.0.1:631	0.0.0.0:*	ESCUCHAR	24345/cupsd
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	ESCUCHAR	15048/mysqlid
tcp6	0	0	:::80	:::*	ESCUCHAR	6667/apache2
tcp6	0	0	:::22	:::*	ESCUCHAR	7185/sshd
tcp6	0	0	::1:631	:::*	ESCUCHAR	24345/cupsd
udp	0	0	127.0.1.1:53	0.0.0.0:*		1132/dnsmasq
udp	0	0	0.0.0.0:631	0.0.0.0:*		956/cups-browsed
udp	0	0	0.0.0.0:5353	0.0.0.0:*		949/avahi-daemon: r
udp	0	0	0.0.0.0:51105	0.0.0.0:*		949/avahi-daemon: r
udp6	0	0	:::5353	:::*		949/avahi-daemon: r
udp6	0	0	:::34259	:::*		949/avahi-daemon: r

```
pedro@maquina:~$ sudo netstat -tulpn | grep :80
```

tcp6	0	0	:::80	:::*	ESCUCHAR	6667/apache2
------	---	---	-------	------	----------	--------------

Cortafuegos

Ejercicio T6.2:

Comprobar qué puertos tienen abiertos nuestras máquinas, su estado, y qué programa o demonio lo ocupa.

Índice



1. Introducción
2. Defensa en profundidad
3. Políticas de seguridad
4. Asegurar un servidor
5. Cortafuegos
6. Evitar ataques
7. Prácticas de seguridad recomendadas
8. Conclusiones

Evitar otros tipos de ataques

El balanceador de carga puede evitar cierto tipo de ataques:

- TCP SYN
- denegación de servicio
- *ping of death*
- *Teardrop*
- *IP spoofing*

Para saber más sobre el funcionamiento de estos ataques:

https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio

Evitar ataques

Ejercicio T6.3:

Buscar información acerca de los tipos de ataques más comunes en servidores web, en qué consisten, y cómo se pueden evitar.

Evitar otros tipos de ataques

El balanceador puede mantener **listas negras**.

Limitar o denegar completamente el acceso a listas de IP
monitorizando el origen, destino o puerto del tráfico.

Se pueden incluir **rangos completos de IP**.

Se pueden evitar ataques de sitios concretos, actuando como sistema adicional de detección de intrusos.

Evitar otros tipos de ataques

Posibilidad de **crear listas de control de acceso** (access control list, ACL) y realizar filtrado a partir de ellas.

Definir las aplicaciones (servicios o puertos) a los que puede acceder un grupo. El administrador de red puede permitir o denegar el acceso a ciertas funcionalidades (aplicaciones) a rangos de IP.

- El balanceador sólo **complementa/ayuda al cortafuegos**, ya que tiene capacidad limitada para bloquear o filtrar.

Índice



1. Introducción
2. Defensa en profundidad
3. Políticas de seguridad
4. Asegurar un servidor
5. Cortafuegos
6. Evitar ataques
7. Prácticas de seguridad recomendadas
8. Conclusiones

Prácticas de seguridad recomendadas

Copias de seguridad:

Tener un sistema de **copias de seguridad automatizado** es indispensable para asegurar la disponibilidad de los datos en nuestro sistema.

El software de copia de seguridad debe verificar los datos una vez grabados.

Las copias de seguridad deben guardarse en un lugar seguro, en un local diferente al que alberga los servidores.

Prácticas de seguridad

Copias de seguridad:



Prácticas de seguridad recomendadas

Copias de seguridad:

<https://www.youtube.com/watch?v=d-eWDuEo-3Q>

<https://www.youtube.com/watch?v=GwMn7YpF8r8>



Prácticas de seguridad recomendadas

Imágenes de los servidores:

También conviene disponer de **imágenes de instalación** de los propios sistemas.

Podremos restaurar una máquina rápida y fácilmente.

Opciones: desde usar el comando dd de Linux hasta usar software propietario como Intelligent Disaster Recovery (Veritas Backup-Exec) o Take Two (Adaptec).

Prácticas de seguridad recomendadas

Imágenes de los servidores. Ejemplo de uso del dd

<http://www.inference.phy.cam.ac.uk/saw27/notes/backup-hard-disk-partitions.html>

Hacemos la copia de la partición completa, byte a byte:

```
# dd if=/dev/sda1 of=/srv/boot.img
```

Ahora podemos restaurarla:

```
# dd if=/srv/boot.img of=/dev/sda1
```

Si queremos restaurar en otro disco más adelante, debemos guardar también la información del particionado:

```
# sfdisk -d /dev/sda | sfdisk /dev/sdb
```

Y ahora ya podemos pasar la información del MBR:

```
# dd if=/dev/sda of=/dev/sdb bs=446 count=1
```

Y cada una de las particiones del disco origen al destino:

```
# dd if=/dev/sda1 of=/dev/sdb1  
# dd if=/dev/sda2 of=/dev/sdb2
```

Prácticas de seguridad recomendadas

Imágenes de los servidores. Intelligent Disaster Recovery

Backup Exec Intelligent Disaster Recovery
for Windows (2000/XP/Server 2003/Vista/7/Server 2008/Server 2008 R2)
Copyright (c) 2011 Symantec Corporation. All rights reserved.

You have successfully loaded a Backup Exec Disaster Recovery CD/Tape image.

If you are testing the bootable media, the computer successfully booted the image. Remove the boot media and press <Esc> to stop the recovery.
DO NOT PRESS <ENTER>.

If you are performing a disaster recovery, press <Enter> to start the disaster recovery process, which will repartition and reformat the computer's hard disks and **DESTROY ALL EXISTING DATA**. The Windows setup program and the Backup Exec Disaster Recovery Wizard are then loaded.

Índice



1. Introducción
2. Defensa en profundidad
3. Políticas de seguridad
4. Asegurar un servidor
5. Cortafuegos
6. Evitar ataques
7. Prácticas de seguridad recomendadas
- [8. Conclusiones]**

Conclusiones

El éxito de un sitio web depende de la seguridad.

La seguridad no se puede pasar por alto !

Aspecto crítico en un sistema web para mantener a salvo de ataques los recursos de la empresa.

Hay que establecer unas **políticas de seguridad**, y **mantenerse al día** de vulnerabilidades del software, de posibles ataques, de actualizaciones de software, etc.

Conclusiones

La **defensa en profundidad** implica mantener diferentes capas de seguridad, independientes entre ellas, de forma que si un atacante consigue pasar una, tendrá otra que superar.

Así se dificulta en gran medida la consecución final de un ataque.

Se diseñarán **diferentes tipos de acceso** y se configurará el sistema para facilitar esos accesos exclusivamente, denegando cualquier otro.

Índice

- 
1. Introducción
 2. Defensa en profundidad
 3. Políticas de seguridad
 4. Asegurar un servidor
 5. Cortafuegos
 6. Evitar ataques
 7. Prácticas de seguridad recomendadas
 8. Conclusiones



BONUS [9. Al día en temas de seguridad]

Al día en temas de seguridad...

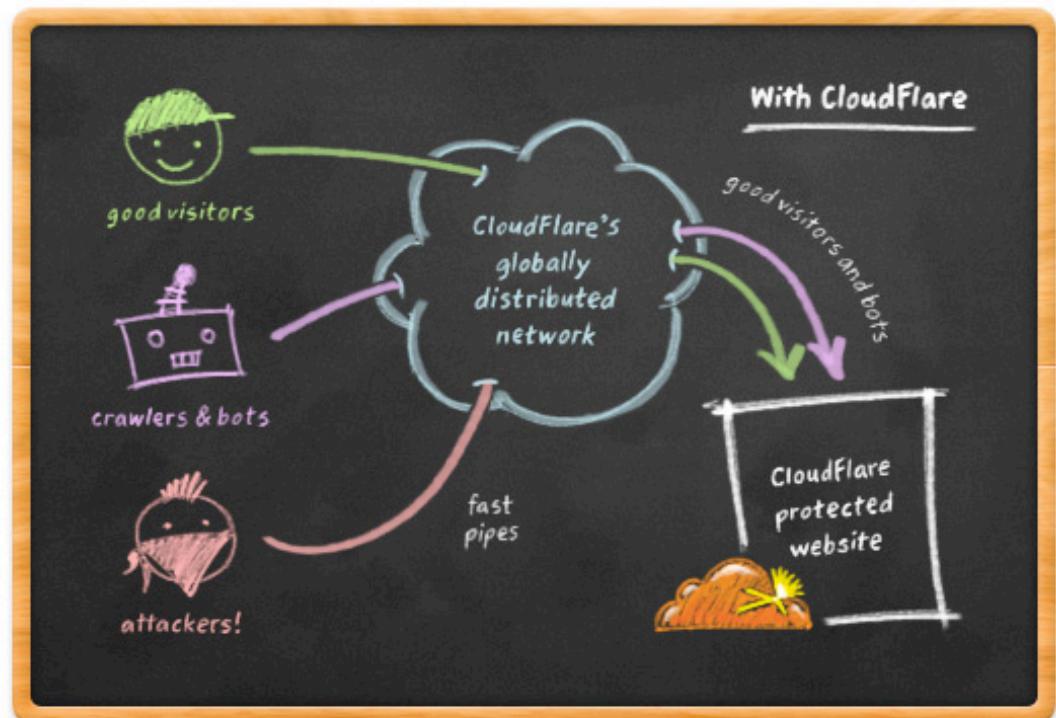
<http://www.securitybydefault.com/>



- CloudFlare, una posible solución frente a ataques (D)DoS

Servicio usado por LulzSec para evitar ataques

<http://www.cloudflare.com/plans.html>



Al día en temas de seguridad...



<http://www.securitybydefault.com/>

- **CloudFlare, una posible solución frente a ataques (D)DoS**

<http://www.securitybydefault.com/2011/06/cloudflare-una-posible-solucion-frente.html>

Normalmente estos servicios, como Akamai y similares, tienen toda la infraestructura "duplicada y distribuida" por todo el mundo (usando cosas como Anycast), por lo que es realmente muy difícil de tirar ya que cada petición que se realice va a un servidor diferente y saturar todos los nodos simultáneamente requiere una capacidad de ancho de banda muy muy alto (en el caso de Akamai creo que tenían cerca de 80mil servidores distribuidos por todo el mundo....)



<http://www.akamai.com/html/technology/index.html>

<https://blogs.akamai.com/2013/04/serving-at-the-edge-good-for-performance-good-for-mitigating-ddos-part-i.html>

Al día en temas de seguridad...

- Cómo mitigar ataques de Denegación de Servicio (D)DoS

El caso de Anonymous contra la SGAE (ACENS)

<http://www.securitybydefault.com/2010/10/como-se-defendio-la-sgae-de-anonymous.html>

- *¿Que hizo ACENS? Algo tan ingenioso como 'des-enrutar' www.sgae.es para que ni un ápice del ataque tocase sus infraestructuras.*
- *"eliminar la ruta hacia la web de SGAE cuando es una "Crónica de una Muerte Anunciada". Al fin y al cabo, dejar sin ancho de banda disponible seguro que lo consiguen [...] sacrificas el peón que sabes que muere igualmente y salvas el resto del tablero"*

Al día en temas de seguridad...

- **Syn Flood, qué es y cómo mitigarlo**

<http://www.securitybydefault.com/search/label/DDoS>

- *ataque es posible debido a la forma en la que funcionan las conexiones TCP. Cuando un extremo desea iniciar una conexión contra otro equipo, inicia la conversación con un 'SYN', el otro extremo ve el SYN y responde con un SYN+ACK, finalmente el extremo que empezó la conexión contesta con un ACK y ya pueden empezar a transmitir datos.*
- *Un ataque de tipo Syn Flood lo que hace es empezar un numero especialmente alto de inicios de conexión que nunca son finalizados, dejando al servidor a la espera del ack final, y por tanto consumiendo recursos de forma desproporcionada.*

Al día en temas de seguridad...

- Syn Flood, qué es y cómo mitigarlo (SISTEMAS LINUX)

Primer paso, activar las syn-cookies:

```
# sysctl -w net.ipv4.tcp_syncookies="1"
```

Segundo paso, aumentar el 'backlog queue' (es decir, dar más holgura al sistema para procesar peticiones entre-abiertas):

```
# sysctl -w net.ipv4.tcp_max_syn_backlog="2048"
```

Tercer paso, hacer que el sistema minimice el tiempo de espera en la respuesta al SYN +ACK. En principio un sistema Linux 'por defecto' esperará 3 minutos, lo bajamos:

```
# sysctl -w net.ipv4.tcp_synack_retries=2
```

(una vez probados los cambios, hay que hacerlos permanentes en /etc/sysctl.conf)

Al día en temas de seguridad...

- Syn Flood, qué es y cómo mitigarlo (SISTEMAS WINDOWS):

Activación de la protección anti Syn Flood:

```
C:\>reg add HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters /v SynAttackProtect /t  
REG_DWORD /d 1
```

Aumentamos el 'backlog queue'

```
C:\>reg add HKLM\System\CurrentControlSet\Services\AFD\Parameters /v EnableDynamicBacklog /t  
REG_DWORD /d 1
```

```
C:\>reg add HKLM\System\CurrentControlSet\Services\AFD\Parameters /v MinimumDynamicBacklog /t  
REG_DWORD /d 20
```

```
C:\>reg add HKLM\System\CurrentControlSet\Services\AFD\Parameters /v MaximumDynamicBacklog /t  
REG_DWORD /d 20000
```

```
C:\>reg add HKLM\System\CurrentControlSet\Services\AFD\Parameters /v DynamicBacklogGrowthDelta /t  
REG_DWORD /d 10
```

Decrementamos el tiempo de espera en conexiones 'Half Open'

```
C:\>reg add HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters /v  
TcpMaxConnectResponseRetransmissions /t REG_DWORD /d 2
```

Ya solo queda reiniciar Windows para que los cambios tengan efecto.

Recursos multimedia (YouTube)

- Tutorial de seguridad básica en servidores web

<https://www.youtube.com/watch?v=w0SB6eAnx4Q&list=PL7C849047272B22E0>

