

### 1-¿Cuál es la función de un servidor proxy?

Su función es la de centralizar el tráfico entre Internet y una red local, también se utiliza para controlar los accesos no permitidos desde Internet hacia la red local.

### 2-¿Qué es el proxy-cache?

Es un servidor situado entre la máquina del usuario y otra red, que actúa como elemento de separación de las dos redes y como zona caché para acelerar el acceso a páginas Web o poder restringir el acceso a contenidos.

### 3-¿Qué es la zona cache?

Es una parte de memoria RAM en la que se almacena una copia de aquellos datos a los que se accederá en más de una ocasión.

### 4-Funciones de los servidores proxy-caché

- Permiten el acceso Web a máquinas privadas que no están conectadas directamente a Internet
- Controlan el acceso Web aplicando reglas o normas
- Registran el tráfico Web desde la red local hacia el exterior
- Controlan el contenido Web visitado y descargado para detectar la presencia de posibles ataques de virus, trojanos, etc.
- Controlan la seguridad de la red local ante posibles ataques, intrusos, etc.
- Funcionan como una caché de páginas Web, almacenan las páginas Web visitadas por los usuarios.

### 5-Ventajas de la utilización de un servidor-proxy

- Mayor velocidad de navegación
- Uso más eficiente de la línea de conexión con Internet
- Cortafuegos
- Filtrado de servicios

### 6-¿Cómo controlan el estado de un recurso los servidores proxy-caché?

Consultando los campos de cabecera Last modified (fecha de última modificación)  
O Expires (fecha de cuando expira).

### 7-Requerimientos Hardware para un servidor proxy

- Necesita bastante espacio en disco y un tipo de disco duro cuyo acceso sea rápido (cuanto mas disco duro tenga mas paginas podrá almacenar)
- Dedicar gran cantidad de memoria RAM a la gestión de la caché (cuanta mas memoria mas objetos podrá almacenar y mas rápido los servirá)
- Los requerimientos de procesador son normales.

### 1. En la configuración de navegador Web que utiliza un proxy-caché <<normal>>, ¿Qué se indica?

Se indica el nombre de la máquina y puerto del proxy

### 2. Ventajas de un proxy transparente

- Obligar a los usuarios a utilizar Proxy sin que ellos sean conscientes de que lo están utilizando.
- Prescindir de la tarea de configuración para cada tipo de navegador.

### **3. ¿Por qué se le llama Proxy transparente?**

Porque el usuario de la red interna no es consciente de que su comunicación con el exterior se hace mediante dicho proxy.

### **4. ¿Qué es un proxy transparente?**

Software para el filtrado de paquetes en entrada/salida situado entre una red local e Internet y del que la red local no tendrá constancia de su existencia.

### **5. ¿En qué consiste el método de unión proxy-gateway?**

Las máquinas de la red interna utilizan como puerta de enlace la máquina que actúa como proxy. El proxy redirige todas las peticiones que le llegan de los navegadores Web de la red interna a su puerto 80.

### **6. Inconvenientes del proxy transparente**

El principal inconveniente es que no todos los navegadores utilizan las cabeceras HTTP requeridas, y además se debe disponer de un cortafuegos.

**Si se decide dedicar 50 MB del espacio en disco a la caché de un hipotético servidor proxy-caché instalado, ¿de cuánta memoria RAM, aproximadamente, debería disponer para la gestión de la caché?**

De 512 kb

---

## **NAT E IPTABLES**

### **1-¿Qué es el IPTABLES? ¿Y a partir de qué versión es aconsejable usarlo?**

Es un programa cortafuegos, a partir de la versión 1.2.4.

### **2-¿Para qué sirven los comandos IPTABLES?**

- Para manipular cadenas completas paquete.
- Para manipular reglas de una cadena dada.

### **3-¿En qué consiste la política de aceptación de paquetes recibidos?**

Primero lo acepta todo y después se va denegando lo que no interese.

### **4-¿Y la denegación?**

Esta todo denegado y después se va aceptando todos los paquetes que esté dispuesto a admitir.

### **5-¿Qué significa NAT?**

Significa traducción de direcciones (Network Address Translation)

### **6-¿Qué hace el NAT?**

Cambiar la dirección de origen o destino de un paquete, con el objetivo de ocultar una red privada detrás de un servidor público.

### **7-¿En qué dos modos puede funcionar NAT?**

- Source NAT (SNAT): consiste en el cambio de la dirección de origen del primer paquete.
- Destination NAT (DNAT): consiste en el cambio de la dirección de destino del primer paquete.

---

**Angel.- Hasta 11.4.b. incluido**

### **1. ¿Qué es el HTTP? ¿Cuándo dónde fue creado?**

Es el protocolo de Transferencia de Hipertexto. Fue creado en 1990 en el CERN (Laboratorio Europeo de la Física de las Partículas)

## **2. ¿Qué es el HTTPS?**

Es la versión segura de HTTP, que puede utilizar diversos métodos de cifrado.

## **3. ¿Qué ocurrió en 1990?**

Que se desarrolló un sistema de relación documental basado en un formato de texto enriquecido.

## **4. ¿Qué es la parte del cliente?**

Es el programa navegador con el que el usuario interacciona, para solicitar a un servidor WEB el envío de páginas de información.

## **5. ¿Qué es la parte del servidor?**

Su función es atender las peticiones de paginas u otros documentos precedentes de los programas clientes HTTP y enviarlas.

## **6. ¿Qué quiere decir que HTTP es un protocolo sin estado?**

Que no recuerda ningún suceso de conexiones anteriores.

## **7. ¿Cuáles son los servidores más importantes y más utilizados?**

- NCSA
- Apache
- Internet Information Server (IIS)

## **8. ¿Cómo es el formato de un mensaje genérico en HTTP?**

- Línea de comienzo
- Líneas de encabezado
- Separador
- El cuerpo del mensaje

---

### **Antonio.- 11.4.c al 11.5 incluido**

## **¿Qué hacen las líneas de encabezado http?**

Constituyen un gran campo fundamental, ya que definen en gran parte la información entre clientes y servidores dándole así flexibilidad al protocolo.

## **¿Cómo se pueden clasificar los grupos de encabezados?**

- De ámbito general: manejan información que puede ser utilizada tanto por clientes como por servidores.
- De solicitud: los utiliza el cliente para enviar información adicional al servidor.
- De respuesta: utilizados por el servidor para enviar información añadida al cliente.
- De entidad: con información relacionada directamente con el recurso que se le va a proporcionar al cliente.

## **¿Qué significa y para que sirve el protocolo MIME?**

Multipart Internet mail extensión, fueron utilizados para extender las características del correo electrónico.

## **¿Quien controla el registro de los tipos MIME?**

Los controla la IANA(Internet Assigned Numbers Authority),

## **¿Qué es el SSL?**

Es un protocolo de encriptación que es utilizado en transacciones seguras vía Web entre un cliente y en servidor. Además, habilita la posibilidad de utilizar firmas digitales, algoritmos de criptografía y algoritmos de Digest o de resumen de mensajes.

## **¿Qué servicios son proporcionados por el SSL?**

Autenticación, integridad y confidencialidad.

## **¿Qué es la clave de sesión?**

Es la que se usa para cifrar los datos que vienen y van al servidor seguro. Se genera una distinta para cada transacción, por lo que un fallo de seguridad de una transacción no implica el fallo de las siguientes.

### **¿Cuándo se realiza la aprobación del cliente?**

Cuando este verifica la validez del identificador digital del servidor, descriptándolo y utilizando su clave pública.

---

## **Fátima.- 11.6 hasta el final**

### **1-¿Cuál es la función de las técnicas de cifrado?**

Impiden que los usuarios no autorizados puedan acceder al contenido de un documento, y solo el usuario destinatario puede leerlo, ya que solo él es capaz de descifrarlo.

### **2-¿Qué es el cifrado simétrico? ¿Y el asimétrico?**

Simétrico: En este tipo de cifrado el emisor y el receptor utilizan la misma clave

Asimétrico: En este tipo de cifrado el usuario utiliza dos claves, una privada que solo él conoce, y una pública que debe ser conocida por los usuarios que quieren enviarle un mensaje cifrado.

### **3-¿Qué es lo que garantiza la firma digital?**

Se asegura que el usuario que firme el mensaje es quien dice ser y la integridad del contenido del mensaje.

### **4-Diferencia entre la firma digital y la firma electrónica**

La firma electrónica utiliza el sistema de criptografía simétrica generando una misma clave para el emisor y el receptor

La firma digital utiliza el sistema de criptografía asimétrica generando dos claves una pública y otra privada.

### **5-Funcionamiento de la firma digital**

La firma digital asociada a un mensaje consiste en extraer un resumen (hash) del mismo. Dicho resumen se cifra utilizando la clave privada del remitente, tras lo cual se añade al final del mensaje. El envío del correo electrónico consta del mensaje original más la firma digital, y se envían ambos cifrados con la clave pública del destinatario del correo.

### **6-Explica los varios tipos de certificados**

B1: Es un certificado de correo temporal

B2: Es un certificado personal en el que se ha hecho una comprobación de la identidad del usuario mediante el DNI o NIF

B3: Es el certificado más completo ya que para su obtención el usuario debe acreditar su identidad, mediante su DNI o NIF, y acudir a los lugares establecidos por la entidad para que se pueda comprobar que realmente es quien dice ser.

### **7-Tipos de navegadores Web**

Según los usuarios los navegadores Web se pueden clasificar en dos grandes grupos: aquellos que no requieren entorno gráfico, y los que sí lo necesitan.

### **8- Explica el navegador de modo gráfico y el de modo texto**

El navegador de modo gráfico son los más utilizados ya que en la actualidad cualquier sistema operativo permite lanzar sobre él un entorno gráfico Ej: Internet Explorer

El navegador de modo texto no supone inpendimiento, la navegación con este tipo de cliente tiene mucho más rendimiento Ej: W3m