SEXTO EJERCICIO

1.- ¿Como podría la compañía asegurar las comunicaciones entre sus oficinas a través de Internet? Justifique su respuesta.

La solución pasa por la creación de túneles VPN, de manera que permite entrar de manera segura a la red principal de la compañía desde lugares remotos. De este modo será posible:

- Proveer acceso remoto a los usuarios corporativos, para que puedan trabajar con recursos corporativos.
- Interconectar de manera segura oficinas separadas de la red central para permitir crear intranets corporativas que engloben a todas.

Las VPN proporcionan conectividad a nivel de red sobre una distancia física, por lo que una VPN permite la utilización de redes públicas como Internet en vez de usar líneas privadas dedicadas, sin sacrificar la seguridad.
Sobre las VPN´S, se pueden implementar diferentes protocolos diseñados para cerrar agujeros de seguridad presentes en las VPN
La solución puede pasar por im°plementar VPN basada en IPSec o en SSL o en PPTP.

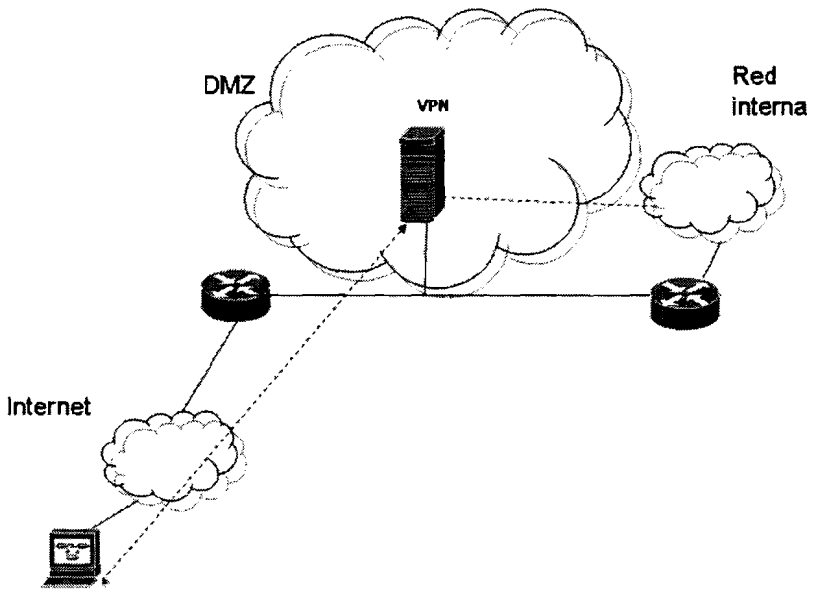
VPN-IPSec, funciona a nivel de red en el modelo OSI, lo cual posibilita que a todos los efectos un equipo que conecta vía VPN-IPSec, esta en la red corporativa, pudiendo acceder a todos los recurso de la misma. También no proporciona gran seguridad en la comunicación, gracias a la utilización de los protocolos de encriptación, encapsulación, e intercambio de claves.
IPSec proporciona:

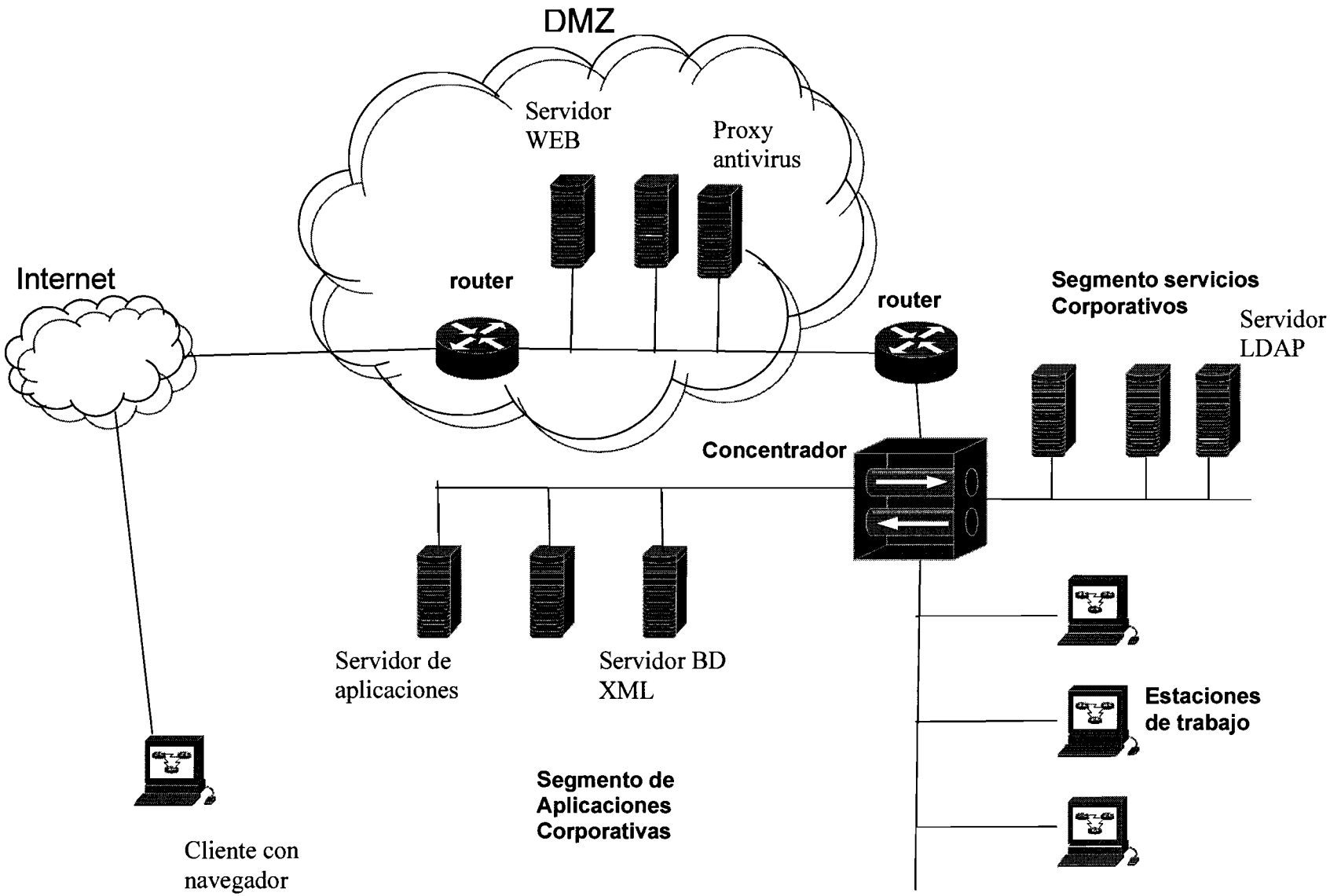
- Control de acceso
- Autenticación de los datos de origen
- Integridad de los mensajes
- Protección anti-reenvio
- Confidencialidad

VPN-SSL.- este método de acceso consiste en el acceso a través de un navegador a una URL vía Internet. Cuando conectamos a esta URL, se establece una comunicación https sobre SSL. Una vez autenticados en la página web, se crea un túnel SSL que posibilita el acceso seguro a una parte de los recursos de la empresa. El problema de esta solución es que no nos permite un acceso completo a los recursos corporativos.
SSL es un protocolo de seguridad diseñado para establecer asociaciones seguras entre un proceso cliente y otros servidores. Para ello, ejecuta un protocolo de negociación para establecer una conexión segura a nivel de socket, sobre el servició de trasporte TCP. SSL es un protocolo de nivel de sesión que proporciona seguridad en este nivel en la arquitectura TCP/IP
SSL utiliza un protocolo de autenticación fuerte, pues utiliza certificados digitales para la autenticación del servidor a través del mecanismo de firma digital.
La autenticación del cliente pude se débil si se utiliza el mecanismo de la pasword cifrada o fuerte si utiliza como mecanismo la firma digital mediante certificado del cliente.

VPN-IPSec, Este método es mas seguro, ya que el nivel de seguridad de la información transmitida a través del tunes es mayor que con IPSec, debido a la complejidad de los protocolos usados para la encapsulación, encriptación e intercambio.
Debido a su funcionamiento en el nivel de red, posibilita el acceso a cualquier recurso corporativo.
Por el contrario, VPN-SSL no permite el acceso a todos los recurso de la empresa, debido a que se trata de un acceso vía Web, y que a todos los niveles estamos fuera de la red corporativa, solo podemos acceder a un número limitado de recurso: pagina Web, recursos de red, correo, aplicaciones TCP
Además este tipo de túneles no permite el filtrado en el firewall por usuarios, debido a que el acceso VPN, no se hace una asignación de ip por usuario, ya que no funciona a nivel de red, no es posible dar diferentes permisos en el firewal que da acceso a los recursos corporativos, en función del usuario.
La ventaja con SSL, es que no se requiere instilación en el cliente, solo un navegador con soporte SSL y java
Los dos tipos de accesos, Compulosry y Voluntariy, sean pensados para conexiones persistentes entre oficinas provinciales y la red central. Para permitir este tipo de conexiones y se utilizara un servidor de VPN, que son los encargados de comunicara la intranet con los remotos, realizando el encapsulamiento y ocultando por tanto la existencia de la VPN, dando la impresión de que se trabaja sobre una única red.
Las ventajas de una VPN:

- Bajo coste
- Escalabilidad



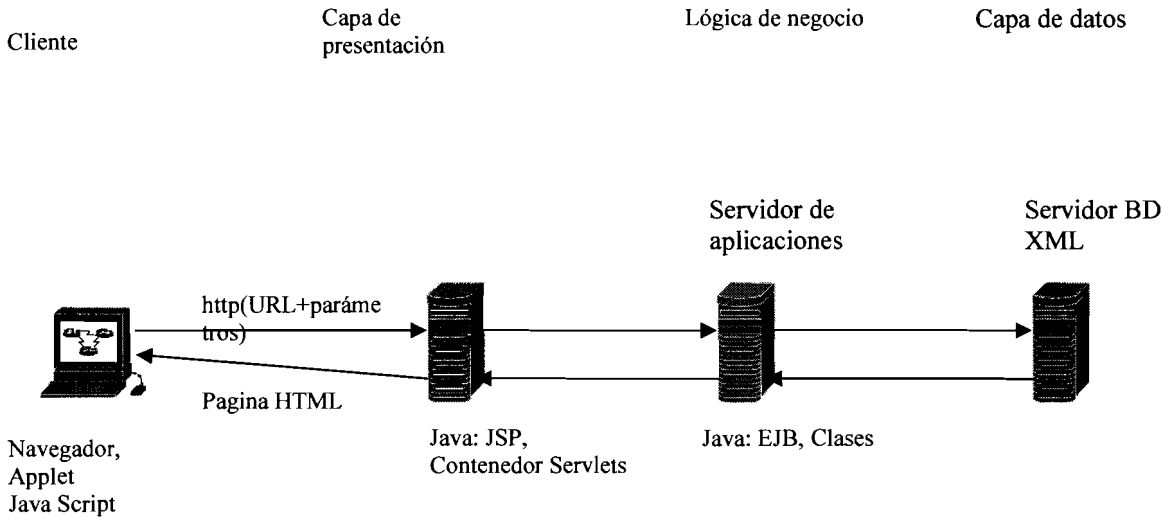

DMZ
Servidor
WEB
Proxy
antivirus
Internet
router
router
Segmento servicios
Corporativos
Servidor
LDAP
Concentrador
Servidor de
aplicaciones
Servidor BD
XML
Estaciones
de trabajo
Segmento de
Aplicaciones
Corporativas
Cliente con
navegador

- 2.- Señale qué solución tecnológica sería recomendable para proporcionar información dinámica sobre estadísticas en el servidor WWW público. Los datos de dichas estadísticas están almacenados en un servidor corporativo que contiene una Base de Datos XML y la corporación ha optado por una plataforma Java.

En la solución, desde el cliente se accede al formulario inicial. En él, se permite seleccionar, la información de la estadística a consultar.

Una vez hecho esto, se pulsa el botón submit, y se realiza una petición a un servlet o JSP, que lee la cabecera de la petición HTTP y los parámetros enviados desde el formulario, en el que se ha rellenado los campos solicitados para proporcionar la información adecuada.

El servlet, o JSP, procesa la información y la envía al servidor de aplicaciones (parámetros de ejecución) quien a su vez mediante los procesos de lógica de negocio residentes en este servidor, (EJB, clases), realizan una petición a la base de datos XML (a través de los driver de conexión), quien ha su vez devolverá un fichero con los datos XML al servidor de aplicaciones, para el procesado de dichos datos. El resultado de dicha ejecución es enviado al servidor WEB (servlet, o JSP) quien realizara el parseo del XML con las Hojas de estilo XSL (solo para parsear XML) o CSS almacenadas en el servidor Web, que serán las encargadas que suministra el estilo en la pagina final o formulario final a entregar al cliente.



NOTA:

por ejemplo apache (servidor Web) no tiene contenedor de servlets, por lo tanto necesita un contenedor de servlets, para poder ejecutarlos, este contendor se ubicaría en el entorno de un servidor Web por ejemplo con Tomcat instalado sobre apache.
Tomcat a parte de ser un servidor Web es un contenedor de servlets (clase especial java), que se encuadra en el servidor Web y este entorno nos es capaz de contener ni ejecutar EJB
Se puede dar el caso de que no se requiera la ejecución de EJB´s, en esta situación, no seria necesario un servidor de aplicaciones (Was, Iplanet,,) bastaría con el servidor Web mas el contenedor de sevlets. En el esquema en este caso el servidor de aplicaciones quedaría sustituido por otro servidor ´Web, que permita mantener la seguridad del sistema, cuando este es accedido desde el exterior.
Cuando se ejecuta un JSP, se genera una clase java (servlets), que se almacena temporalmente en el contenedor de servlets del servidor Web. Este servlet puede llamar a un EJB o a una clase Java que se encuentra en el servidor de Aplicaciones, o bien a otro servlets, que se encuentra en el servidor Web