Topologías de centro de cómputos

Todo empezó con la **arquitectura cliente servidor**, pero la red desarrollo otros servicios más completos como el Cloud Computing, donde todo está dentro de una misma red (procesamiento, recursos, etc.).

Arquitectura de Cloud Computing (la nube):

Más allá de ser una tecnología, involucra un ecosistema de herramientas, aplicaciones e infraestructura que soporta una genial y moderna forma de trabajo.

La nube es un espacio que, de forma sencilla, permite sincronizar nuestro trabajo, contenido o archivos, en cualquier dispositivo que esté enlazado a esta. Es la forma de:

- Tener todos los archivos sincronizados en todos los equipos.
- Respaldar toda la información en un lugar externo a un equipo.
- Consumir recursos de "otra computadora compartida" en lugar de la nuestra.
- Trabajar con contenidos que no tenemos físicamente en nuestro equipo.
- Trabajar de forma colaborativa, simultánea e incluso remota.

Centro de Comunicaciones (centros de cómputos) y Redes:

Un centro de datos es una instalación utilizada para alojar sistemas de computación y componentes relacionados.

Existen algunas **tendencias** en los centros de cómputos:

- Conexiones de comunicaciones de datos redundantes: la mayoría trabajan con routers que permiten 2 conexiones redundantes.
- Servidores virtuales de alta velocidad denominadas granjas de servidores o clústeres de servidores.
- Sistemas de almacenamiento redundante – SAN (Storage Area Network).
- Fuentes de alimentación redundantes o de respaldo (UPSs / Generadores).
- Controles ambientales integrales (accesos restringidos, uso de aire acondicionado y sistemas de extinción de incendios).
- Dispositivos de seguridad (cámaras).

DNS – Sistema de Nombres de Dominio:

Es un servicio constituido por uno o varios servidores alojados en un centro de cómputo.

Está compuesto por un conjunto de protocolos y servicios sobre una red TCP/IP que permite a los usuarios de red utilizar nombres jerárquicos sencillos para comunicarse con otros equipos, en vez de memorizar y usar sus direcciones IP.

Un servidor de nombres de dominios (DNS) es un servicio que permite a los usuarios de red entregar una URL y recibir una dirección IP para realizar la conexión. Trabajan el forma jerárquica y se estructuran de acuerdo a la topología / tipo de red:

- DNS primario (Extranet).
- DNSs secundarios (dentro de la Intranet).

Es usado en Internet y en redes privadas actuales. Normalmente se utilizan varios DNS para navegar tanto hacia fuera como hacia dentro de la red (un sitio tiene un DNS externo y uno interno, es un tema de seguridad). Servicios como navegadores, servidores web, FTP y Telnet utilizan DNS.

La resolución de cada nombre de dominio es delegada al servidor DNS del ISP designado como administrador por la entidad registrante.

DNS define:

- Un modelo de base de datos para almacenar información sobre direcciones.
- Un mecanismo para preguntar y actualizar información sobre direcciones en la base de datos.
- Un mecanismo para replicar información entre servidores.

Una **zona DNS** es una porción del espacio de nombres DNS sobre la que un servidor DNS tiene autoridad.

Dentro de una zona DNS, hay **registros de recurso (RR)** que definen los hosts y otro tipo de información que completan la base de datos de la zona. Hay varios tipos de zona:

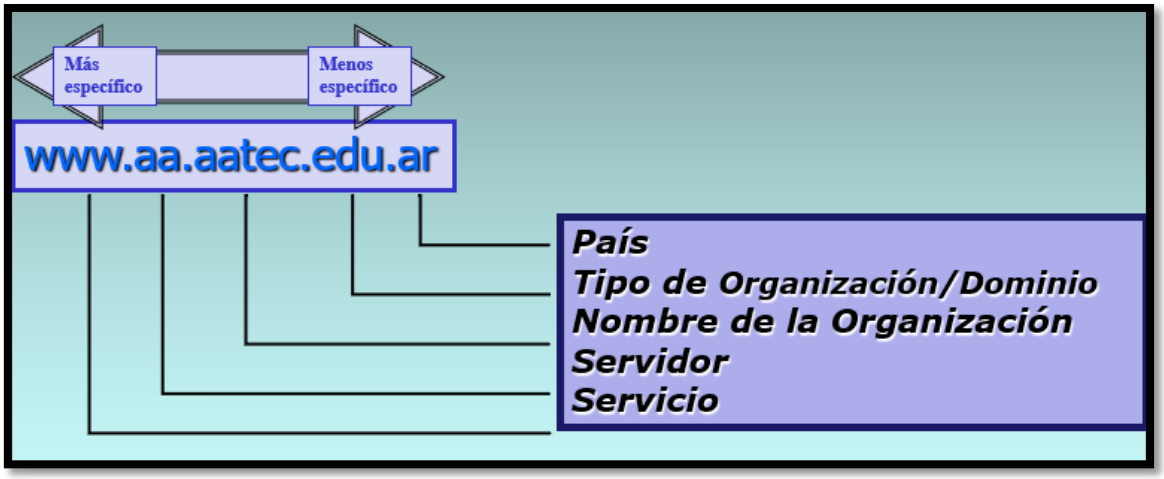
- **Zonas primarias:** Contienen la copia principal de los RR de la zona. Los cambios y actualizaciones de la zona se producen en la zona primaria. Si queremos crear un nuevo dominio DNS tendremos que crear una zona primaria. La zona DNS primaria se almacena en un archivo local del servidor.

- **Zonas secundarias:** Las zonas secundarias son copias no editables de las zonas primarias. Se usan para balanceo de carga y tolerancia a fallos. Periódicamente, según la configuración, la DNS primaria realiza una "transferencia de zona" a la secundaria. Si la DNS primaria cae, durante un tiempo, la DNS secundaria asumirá las respuestas, aunque pasado un periodo de tiempo especificado por el administrador (TTL o Time To Live), la zona secundaria caducará. Antes de que esto ocurra, la DNS primaria debe ser rearmada.

- **Zonas integradas con Active Directory.**

El **nombre** consta de una secuencia de segmentos alfanuméricos separados por puntos, siendo la parte más significativa a la derecha y la parte izquierda corresponde al nombre de una computadora. Los otros segmentos del nombre corresponden al grupo al cual pertenecen.

Existe una **estructura jerárquica para la designación del nombre** asignado a una estación o dispositivo en la red:



Debido a los desafíos asociados con la administración de direcciones estáticas, los dispositivos de usuarios finales a menudo poseen direcciones dinámicamente asignadas, utilizando el **DHCP**.

El DHCP permite la asignación automática de información de direccionamiento como la dirección IP, la máscara de subred, el versión por defecto y otra información de configuración.

La configuración del servidor DHCP requiere que un bloque de direcciones, llamado conjunto de direcciones, para ser asignado a los clientes DHCP en una red. Las direcciones asignadas a este pool deben ser planificadas de manera que se excluyan las direcciones utilizadas para otros tipos de dispositivos.

En los DNS existe una estructura geográfica de registro identificando al país.

Las organizaciones propietarias del domino registrado con direcciones IP ante NIC local/InterNIC pueden decidir si agregan alguna estructura jerárquica adicional.

Cada servidor sabe cómo llegar a la raíz y los mismos son autoridades de los nombres de inferior jerarquía.

Resolución del nombre utilizando resolutor:

Un **resolutor** es un proceso que gestiona el proceso de consulta y recepción de respuesta de datos DNS. Los resolutores están presentes en los clientes y en los servidores que intentan responder a consultas de clientes.

Es un componente del sistema operativo del cliente y servidor que realiza solicitudes de DNS. El software toma la cadena de caracteres y devuelve el listado de direcciones que corresponden al nombre especificado.

Cada resolutor se configura con la lista del servidor local de nombres de dominio (NIC).

InterNIC - Servicio de base de datos y de directorio:

Internet Network Information Center (InterNIC) es un servicio internacional y fuente de información de documentos de Internet.

El **ICANN** es el que está encargado del InterNIC, administrando los elementos técnicos que conforman todo el sistema DNS. Esto lo hace a través de una institución llamada **IANA**, encargada del registro de direcciones IP y nombres de dominio.

La InterNIC delega sus funciones en los NIC de cada país.

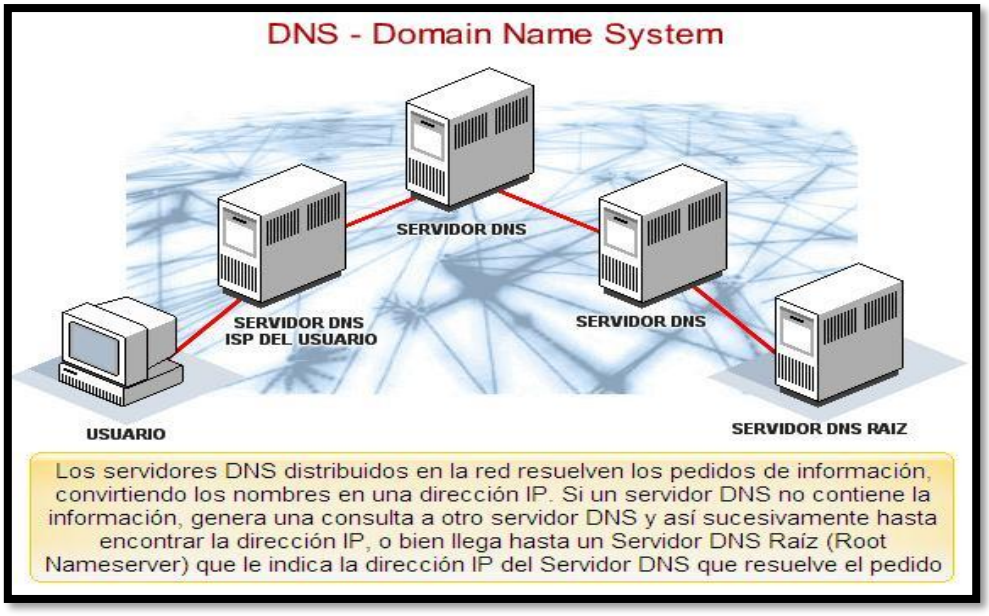
NICar depende de la Secretaria Legal y Técnica de la Presidencia de la Nación.

Registros DNS:

Un **registro** es la manera de establecer la relación entre el dominio y la dirección IP.

Los diferentes tipos de entradas de registro son:

- **Registro A:** Este registro se utiliza para convertir nombres de host en direcciones IP.
- **Registro CNAME:** Se utiliza para crear nombres de host adicionales (alias), y para crear diferentes servicios bajo una misma dirección IP.
- **Registro NS:** Indica los servidores de DNS autorizados para el dominio, es decir, a quién hay que preguntar para saber acerca de los registros de midominio.info.
- **Registro MX:** Se utiliza para asociar un nombre de dominio a una lista de servidores de correo para la recepción de emails. Nos interesa si queremos realizar redirecciones de nuestro correo o utilizar nuestro correo electrónico con otro proveedor.
- **Registro SPF:** Define qué servidores están autorizados para enviar correo electrónico con nuestro dominio.



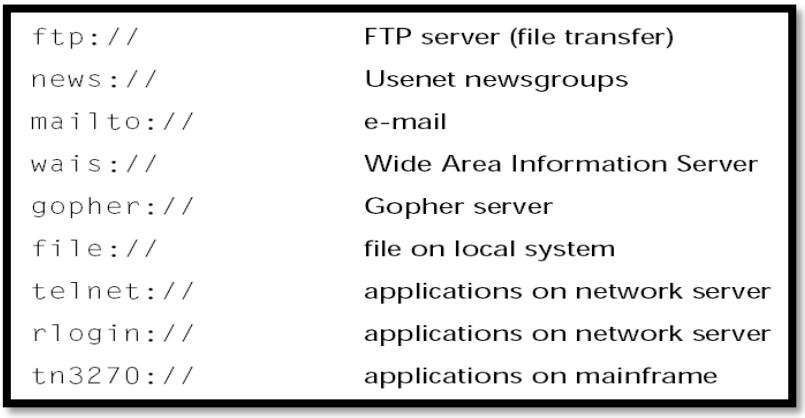
Servicios de Internet:

Un servicio de Internet se identifica con:

- Dirección IP.
- Nombre de dominio único, registrado en nic.ar, por ejemplo.
- Puerto asociado a cada servicio solicitado (se puede controlar con un Firewall), con una escucha permanente en cada puerto.
- Un servicio puede tener varios servidores.

Un **puerto** es un identificador único de un servicio específico, utilizado por TCP para identificar los servicios. El protocolo usa el identificador para dirigir las solicitudes de entrada al servidor adecuado. Los servicios, normalmente, son identificados con un número entero de 32 bits (IPv4).

Un puerto identifica a un servicio a través del protocolo TCP.



ftp://	FTP server (file transfer)
news://	Usenet newsgroups
mailto://	e-mail
wais://	Wide Area Information Server
gopher://	Gopher server
file://	file on local system
telnet://	applications on network server
rlogin://	applications on network server
tn3270://	applications on mainframe

En la imagen faltaría WWW (web Internet) y WWW2 (web Internet2). Todos son servicios.

Wais (Wide Area Information Server)

Es un servicio que mostraba información de bases de datos indexadas. Busca un tópico en todas las bases de datos disponibles en la red.

Se basaba en el protocolo ANSI Z39.50 y puede accederse a través de Telnet (protocolo que permite el acceso en modo línea de comando, hoy está prohibido en internet) o WWW.

El servidor mantiene un índice global de todo el mundo lo que permite una búsqueda de alto detalle.

Gopher

Otro servicio de distribución de información. Gopher permitía visualizar directorios y bajar información. Posee una interfaz basada en menú y trabaja con los siguientes componentes:

- **Ítems:** Directorios, archivos de texto, una imagen o búsqueda.
- **Documento:** Información incluida en un ítem.

- **Bookmark**: Señalador o entrada de menú asociada.
- **Server**: Servidor de documentos.

Archie

Antes de la WWW para poder bajar archivos de todo tipo se utilizó el servicio FTP bajo Archie.

Permite la localización de información y transferirlos utilizando FTP.

Las búsquedas también pueden encararse a través de telnet o correo electrónico.

Trabaja con arquitectura cliente-servidor, necesita de la interfaz de cliente para el usuario.

Es descendiente del servicio Gopher.

Es un protocolo que interpreta ficheros de una máquina remota. Puede interpretar texto, imágenes, sonidos y secuencias de video, para ello utiliza HTML.

WWW

La World Wide Web es un sistema interconectado de páginas web públicas accesibles a través de Internet. La Web no es lo mismo que el Internet: la Web es una de las muchas aplicaciones construidas sobre Internet.

Colección de ficheros o páginas web que incluyen información en forma de textos, gráficos, sonidos y video además de links o vínculos con otros ficheros.

Los ficheros son identificados por una URL que especifica el protocolo de transferencia, la dirección de Internet de la máquina y el nombre del fichero.

El **visualizador (navegador)** es un programa interactivo que permite al usuario ver la información de la WWW. La información tiene objetos seleccionables para que el usuario vea otra información.

La mayoría tiene una interfaz para apuntar y seleccionar elementos de hipertexto/hipermedia.

FTP

Es un repositorio que permite transferir archivos.

El servicio FTP permite la utilización de un sistema de archivos remotos como si fuera local mediante el protocolo FTP, el cual utiliza una conexión de control (puerto 21) y otra para transferencia de los datos (puerto 20 o superior a 1023).

Es una aplicación que opera sobre TCP y se utiliza para operaciones básicas sobre archivos y transferencias en redes WAN.

Normalmente, para acceso a un host solicita nombre de usuario y contraseña. Las contraseñas las envía encriptadas, pero no hay encriptación en los datos (se transfiere en texto plano).

Establece un canal lógico entre ambos host.

TFTP (Trivial File Transfer Protocol)

Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza para transferir pequeños archivos entre computadoras en una red.

Es una variante del protocolo FTP pero mucho más simplificado, que prescinde de la conexión de control (utiliza UDP).

Está diseñado para realizar transporte de archivos en forma sencilla.

Sin autenticaciones de seguridad.

Se utiliza para anular la carga de trabajo de FTP. Es muy eficiente.

Es usado normalmente dentro de una LAN (arriesgado en una WAN).

SFTP y FTPS

Es un protocolo de transferencia de archivos seguro para conexiones remotas, con la información encriptada. Utiliza los puertos:

- SSH en el puerto 22 (SFTP).
- SSL / TLS en el puerto 990 (FTPS).

FTPS autentica su conexión utilizando un ID de usuario o una contraseña, un certificado, o ambos.

Sincronizan a usuarios que estén habilitados en un Active Directory.

Puede trabajar con certificados SSL / X509, claves públicas, claves privadas SSH o tokens.

Mientras FTPS suma una capa al protocolo FTP, SFTP es un protocolo completamente diferente basado en el protocolo de red SSH (Secure Shell). A diferencia de FTP y FTPS, SFTP utiliza solo una conexión y encripta tanto la información de autenticación como los datos de archivos que están siendo transferidos. SFTP proporciona dos métodos para autenticar conexiones.

Una de las principales **diferencias** entre FTPS y SFTP es que FTPS utiliza múltiples números de puerto. SFTP necesita un único número de puerto para todas las comunicaciones SFTP, lo que facilita su protección.

SMTP

Protocolo simple de transferencia de correo orientado a la conexión.

Utiliza los Puertos 25 y 587 para conectividad entre cliente y el servicio de transporte. Los puertos 25, 465 y 475 son utilizados para el transporte al buzón de correos.

Una transacción SMTP tiene 3 secuencias:

- MAIL: Dirección remitente/retorno.
- RCPT: Destinatario del mensaje.
- DATA: Envio de mensaje de texto.

El servicios SMTP tiene un servidor denominado **MTA (agente de transferencia de correo)**, el más conocido es Sendmail (Unix).

El MTA envía y recibe paquetes desde/hasta otros servidores de correo. Proporciona una interfaz para que las aplicaciones accedan al sistema de correo y proporciona a los usuarios buzones de correo dotados de una dirección.

Existen 2 archivos fundamentales dentro de un servidor MTA, la configuración del usuario y un buzón de correo electrónico.

POP3 (protocolo de oficina de correo)

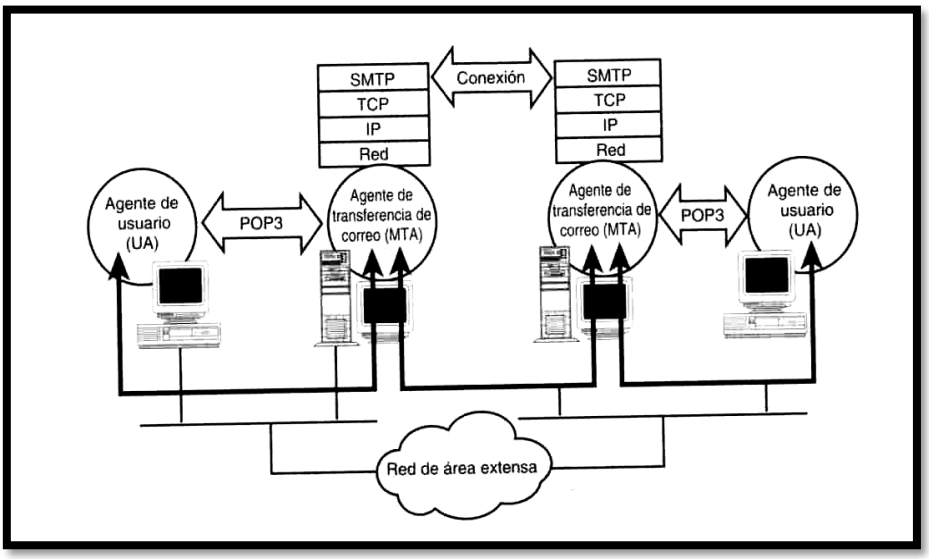
El usuario final va a tener una bandeja de correo electrónico llamado POP3.

Se utiliza en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto, denominado servidor POP. Es un protocolo de nivel de aplicación en el Modelo OSI.

El **agente de usuario (UA, usuario final)** utiliza POP 3 para comunicarse con el MTA. El UA envía y recibe paquetes desde/hasta otros servidores.

POP3 no trabaja en tiempo real (carga de la red).

Este es un servicio propio para transferir información a una computadora.



Dentro del servidor MTA existe un programa llamado **relevador de correo electrónico**, que configura el buzón de correos.

Webmail

Correo electrónico en sitios web. El acceso a cuenta se hace a través de un navegador web.

Administración de correo electrónico a través de Internet.

Tiene un espacio de almacenamiento limitado.

Puede replicar con Servidor SMTP.

Privacidad mediante nombre de usuario y contraseña.

Servicio DHCP (Dynamic Host Configuration Protocol)

Es un servicio de asignación automática de direcciones IP. Posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres.

Asigna parámetros como la máscara de subred, puerta de enlace, etc.

Mantiene estado de la posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Telnet

Es un servicio que permitía por línea de comando acceder en forma remota a un servidor. IETF caducó y prohibió este servicio.

Es un protocolo de red que permite acceder a otra máquina para manejarla remotamente. También es el nombre del programa informático que implementa el cliente. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

Es una **característica crítica** de un sistema de computación, porque se transmite en texto plano. Si no se cierra el puerto y no se evitan las comunicaciones Telnet puede haber puertas externas abiertas que pueden ocasionar problemas de seguridad.

Puede realizarse mediante conexión telefónica.

Secure Shell o SSH

Protocolo de red que permite el intercambio de datos utilizando un canal seguro entre dos dispositivos conectados en red.

Emulación de terminal en modo túnel.

Puede realizarse mediante conexión telefónica.

SSH es utilizado habitualmente para entrar en una máquina remota y ejecutar comandos (acceso en modo terminal remoto). Utiliza el puerto 22.

SSH utiliza la criptografía de clave pública para autenticar el ordenador remoto y permitir autenticar al usuario.

Autentifica los dos extremos de la conexión:

- El servidor se autentica ante el cliente con un certificado.
- El cliente se autentica ante el servidor mediante usuario y password o certificados.

No se transmiten usuarios ni passwords en claro. La información transmitida viaja también encriptada.

Chat

Protocolo mundial que se utiliza para comunicar intercambiando mensajes de texto en Internet. Por medio del chat se realiza una comunicación en tiempo real para intercambiar mensajes.

Componentes de un host de Internet

Encaminador dinámico (router fronterizo):

Permite realizar la conexión contra la red telefónica.

Permite el enrutamiento punto a punto de los paquetes entre la red y el nodo. Trabaja en la capa red (3).

Se lo denomina fronterizo y utiliza el encaminamiento bajo búsqueda en tabla (estas suelen ser dinámicas, pero también existen las estáticas).

Selecciona las rutas de los paquetes basados en estas rutas.

El proveedor del servicio le asigna una dirección IP.

Examina los paquetes de datos entrantes y selecciona las rutas basadas en la información en las tablas de enrutamiento.

Utiliza protocolos de enrutamiento como por ejemplo:

- RIP – IGRP = Interiores.
- EGP – BGP = Exteriores.

Para el cálculo de la mejor ruta utilizan distintas métricas como número de saltos, retardos, etc.

NAS - Network Access Server (servidor de acceso a la red):

Un Access Server (NAS) está destinado a actuar como una puerta de entrada para proteger el acceso a un recurso protegido. Esto puede ser cualquier cosa desde una red telefónica, impresoras, o Internet.

El cliente se conecta al NAS. El NAS a su vez se conecta con otro recurso preguntándole si las credenciales suministradas por el cliente son válidas. Basado en la respuesta el NAS permite o impide el acceso a los recursos protegidos.

El NAS no contiene información acerca de qué clientes pueden conectarse o qué credenciales son válidas. Todos los NAS envían las credenciales suministradas por el cliente a un recurso que sabrá cómo procesar las credenciales.

Se encarga de filtrar los accesos remotos vía módem a través de un software de seguridad que almacena a los accesos con su clave de autenticación.

Normalmente lo componen una cantidad de módems en línea conectados a accesos telefónicos unitarios o rotativos.

Se le asigna un rango de direcciones IP fijas que le permita asignar a cada usuario una dirección dinámica en el momento de la conexión.

Radius (Remote Authentication Dial-In User Service):

Es un software de administración y control para servidores de acceso remoto (RAS). Autentica las acciones de acceso remoto sobre los RAS mediante las llamadas, protocolos y filtros.

Es un software nativo dentro de cualquiera de los servidores que constituyen una instalación Internet. Actúa complementándose con todos los protocolos que constituyen la pila TCP/IP.

Características:

- Soporta la seguridad adicional de los servidores proxy.
- El tiempo de respuesta de autenticación es inmediato.
- Asigna direcciones IP dinámicas en el momento de la conexión.
- Mantiene una base de datos con el nombre de usuario y su password.
- Simplifica y consolida la administración de usuarios de acceso remoto al nodo.
- Facilita el seguimiento y documentación de accesos remotos.
- Administración y configuración bajo entorno Windows.

Permiten configuración, comunicación y autenticación en VPNs usando L2TP (Layer 2 Tunneling Protocol), que permite actualizar los servicios Radius contra el directorio activo. Es un protocolo de tunneling para usuarios remotos. De acuerdo al usuario y configuración dentro de la VPN los paquetes son dirigidos aplicando Tunneling en forma dinámica en el momento de la conexión dial-up.

Firewall

Es un servidor que permite proteger toda la arquitectura de un centro de cómputos, evitando conexiones no deseadas.

Es un servidor con interfaz de red multipuerto (divide las zonas de trabajo en zonas de seguridad) que limita los servicios/procesos de una red con respecto al resto de los componentes de Internet.

Habilita y deshabita servicios en forma parcial/global de acuerdo a las políticas establecidas en la administración del nodo.

Es un servidor específico compuesto por Hardware y Software que actúa como barrera de seguridad de los recursos informáticos de una organización. Barrera de seguridad entre la Intranet y la Extranet.

Se encuentra ubicado inmediatamente después del router fronterizo.

Puede albergar el DNS externo.

Cada paquete que entra o sale de la red es inspeccionado y lo acepta o rechaza basándose en las reglas definidas por el usuario (**software editor de reglas**).

La regla básica es asegurar que todas las comunicaciones entre la Extranet y la Intranet se realicen conformes a las políticas de seguridad de la organización.

Técnicas utilizadas:

- Filtros a nivel paquete.
- Filtros a nivel circuito.
- Filtros a nivel aplicación.
- Filtros dinámico a nivel paquete.

Un Firewall suele tener un mínimo de **tres zonas**, aunque las primeras implementaciones sólo incluían dos:

- Interior.
- Exterior.
- DMZ (zona desmilitarizada).

Un Firewall:

- Filtra tráfico dependiendo de reglas predefinidas.
- No protege de ataques internos.
- No protege de accesos no autorizados.
- No protege de todos los ataques dañinos.

Proxy Server

Es un servidor encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red. Al mismo tiempo contiene mecanismos de seguridad que impiden accesos no autorizados desde el exterior hacia la red privada.

Es un gestionador de comunicaciones entre Internet e Intranet de una LAN.

Proporciona protección a nuestra LAN utilizando NAT (Administrador de Traducciones de Red).

Proporciona restricciones de servicios parciales a nivel individual.

Aislamiento completo de la Intranet.

Puede mantener un cache configurable de los datos más solicitados o recientemente recuperados para mejorar la performance de respuesta ante solicitudes.

Asocia los puertos 8080-80 como las peticiones del usuario.

El servicio se basa en HTTP pero admite FTP, Gopher y SSL (datos encriptados).

LDAP Server

LDAP (Lightweight Directory Access Protocol) es un servicio de Internet que implementa un directorio jerárquico y distribuido. Es un repositorio centralizado de usuarios, aplicaciones y recursos.

Define permisos configurados por el administrador para permitir el acceso a ciertos usuarios a la base de datos, y mantener información en privado.

Control de acceso a recursos a través de reglas de provisionamiento.

Utiliza canales seguros para comunicarse con el cliente.

Tres tipos de autenticación: Sin autenticación, autenticación simple y usando SASL o SSL/TLS.

Web Server

Colección de ficheros o páginas web que incluyen información en forma de textos, gráficos, sonidos y video además de links o vínculos con otros ficheros.

Dependiendo de la configuración del Proxy o Firewall puede ser interno o externo.

Acepta peticiones HTTP desde clientes web y envía la información solicitada.

Almacena información detallada acerca de las peticiones de los clientes y las respuestas del servidor.

Funcionalidades: Autenticación, manejo de contenido estático y dinámico, HTTPS, compresión, limitación de ancho de banda.

Mail Server o Servicio de correo

Un Mail Server es una aplicación informática que permite enviar correos de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando. Utiliza el protocolo SMTP.

El MTA (Agente de Transferencia de Correo):

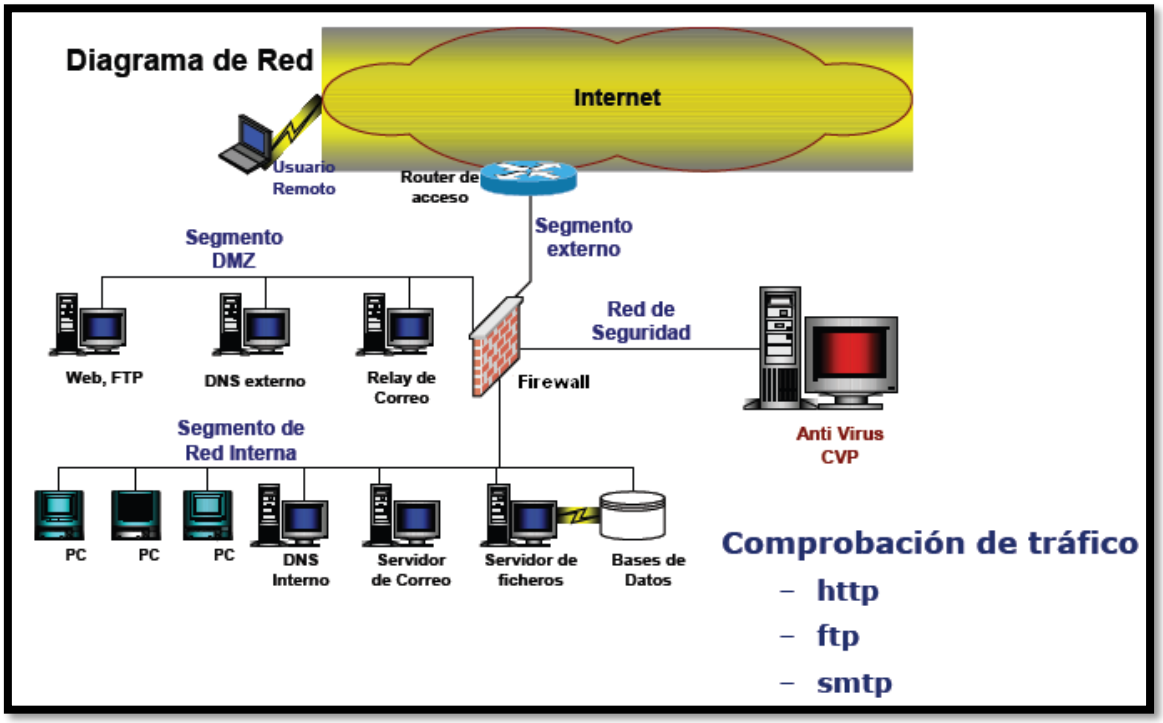
- Envía y recibe paquetes desde/hasta otros servidores de correo.
- Proporciona una interfaz para las aplicaciones accedan al sistema de correo.
- Proporciona a los usuarios buzones de correo dotados de una dirección.

Antivirus

Otro servicio que tiene un centro de cómputos es el antivirus de borde, el cual puede también estar dentro de un endpoint.

Es un programa de chequeo de archivos de tráfico entrante y saliente trabajando sobre servicios FTP, HTTP y MAIL.

Los antivirus tienen también una **consola de trabajo** que permiten resumir cuantos equipos tuvieron problemas, cuantos no, que tipo de malware hubo, etc. Permiten establecer estadísticas.



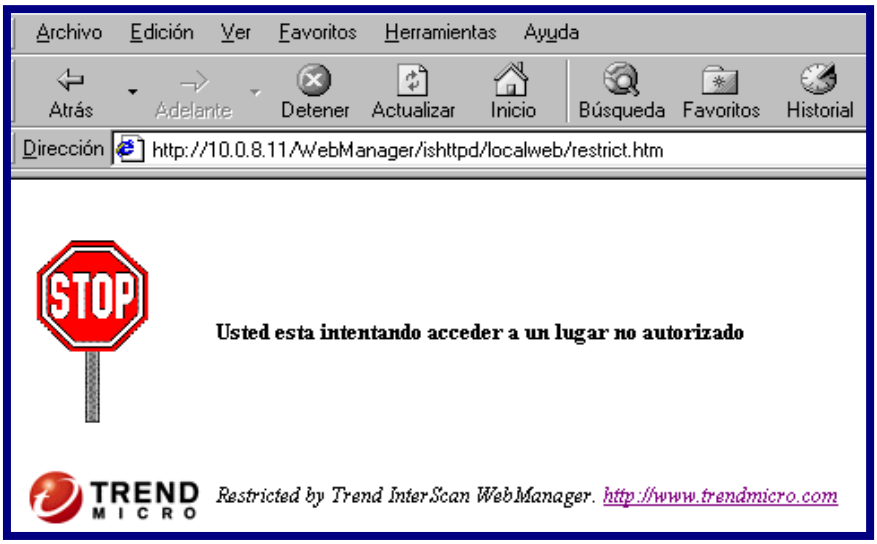
Monitor Web (Web Manager)

Bloquea el acceso a usuarios o grupos a sitios web no productivos o no aceptados por las políticas de la empresa. El administrador define la política seleccionando aquellas categorías que son aceptables o no. Esto le otorga la posibilidad de filtrar cientos de miles de sitios web y su actualización es automática.

Utilizan un motor de filtrado de sitios web e interactúa con una base de datos de categorías de sitios para limitar accesos (**CyberPatrol**).

Características:

- Registra en detalle todo el tráfico web de la empresa y guarda los registros relacionados.
- Configura límites de tiempo y volúmenes de información para cada usuario/grupos.
- Bloquea el acceso a sitios web maliciosos según la reputación.
- Bloquea las amenazas de malware, incluidos los spyware y ataques de día cero. Protege todo el tráfico web previniendo el ingreso a la red de virus y códigos maliciosos.
- Activa la limpieza automática de archivos de spyware y malware.
- Protege frente a las instalaciones automáticas mediante el análisis de código móvil.



Monitor de Correo Electrónico (E-Manager)

Es un programa asociado al servidor de correo encargado del:

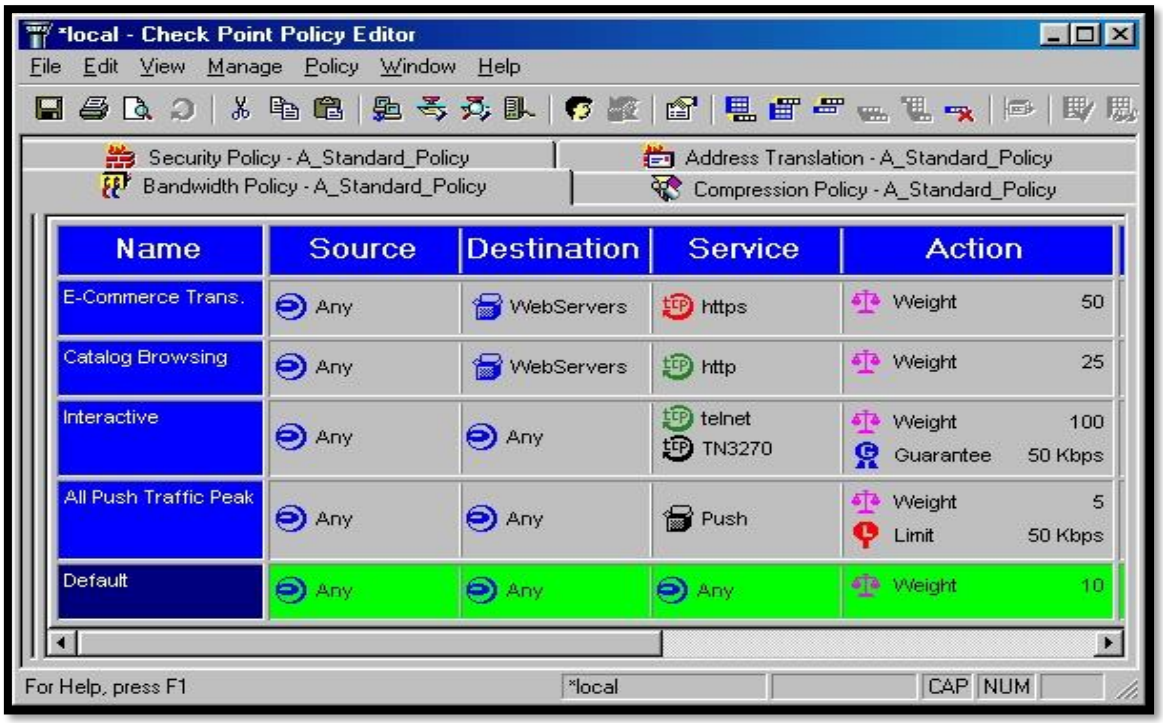
- Filtro de contenidos (material confidencial o inapropiado).
- Filtro de atacheados.
- Filtro Spam: Bloqueador de E-Mails no solicitados.
- Administración de E-Mails: Monitor de patrones de tráfico.

Bandwindth Manager (B-Manager) - Monitor de Ancho de Banda

Sistema de máquina virtual utilizado para administrar ancho de banda. Esto permite tener distintas categorías de usuarios (básicos, medianos o premium, por ejemplo) para garantizar un determinado ancho de banda a cada uno, priorizando las conexiones.

Características:

- Trabaja sobre el canal adjudicando ancho de banda de acuerdo a las políticas de uso.
- Editor integrado de políticas de uso del canal.
- Adjudica en forma general o particular a usuarios conectados.
- Trabaja sobre algún servidor del nodo Internet o del ISP.
- Monitoreo gráfico en tiempo real.
- Sus políticas son complementarias a las de un Firewall.
- El uso apropiado evita la congestión del canal cortando procesos que ocupan mucho ancho de banda.
- Puede operar en combinación con VPNs, y NAT en caso de tener Intranets.



Diodo de Datos

Es un tipo de servicio de hardware, un dispositivo que separa y protege dos redes asegurando la unidireccionalidad en el flujo de información permitiendo que la información de una red llegue a otra red (pero no viceversa). Dicho de otra manera, asegura la unidireccionalidad en el tránsito de información de dos redes o dos servidores, haciendo inviable la transmisión de información en el sentido opuesto.

Es un dispositivo de protección de perímetro utilizados habitualmente en interconexiones entre sistemas con diferentes categorías o políticas de seguridad.

Los casos de uso puede ser la entrada de información a la red interna o la salida de información desde la red interna.

Procesador Front-End (FEP) - Comunicaciones Unificadas

Hoy en día estos FEP mutaron a servidores de acceso o de videoconferencia.

Es una plataforma de comunicaciones de presencia, mensajería instantánea, conferencia y voz para organizaciones distribuidas en WAN.

Sobre una base de usuarios (directorio) integra mensajes existentes en la organización y la infraestructura de telefonía.

Permite a los usuarios realizar, recibir, reenviar o redireccionar las llamadas directamente desde su PC, teléfono fijo o teléfono móvil.

Se utilizan para validar usuarios mediante un certificado digital.

Un FEP permite:

- Mensajería instantánea: Comunicación en tiempo real de persona a persona mediante texto, voz y video, a través de una organización.
- Conferencias Web.
- E-mail y calendarios compartidos y contactos.
- E-Manager (Protección/preservación E-Mail):
    - Filtrado (Spam).
    - Archivo (backup).
    - Continuidad (Replicando).
    - Cifrado (TLS).

Balanceo de carga

Cuando un sitio se recarga de conexiones y se cae (exceso de sesiones o peticiones), es necesario un sistema que balancee la carga de trabajo para evitar estos problemas.

El balanceo de carga es un servicio que puede constituirse de varias maneras que permite balancear los accesos para evitar la sobrecarga en servicios, en los cuales algunos están replicados.

Es una técnica de balanceo de solicitud de pedidos para optimizar el flujo de información y la carga de procesamiento.

Los pedidos dejan de ser asignados a un único servidor para ser distribuidos en varios servidores ante las peticiones y/o sesiones web.

Permite preconfigurar redistribución de solicitudes ante tareas de mantenimiento o contingencia por caídas (redundancia).

Asegura una distribución de carga pareja para brindar un servicio más rápido.

Existen varios **tipos de balanceo (técnicas)**:

- **RR-DNS (Round Robin DNS):** Se aplica una técnica de Round Robin sobre un servidor DNS particular que determina a qué servidor asignara la petición, en función de su disponibilidad.

  Estas asignaciones pueden realizarse a partir de dos características a analizar:

  - **Por sesión:** El servidor asigna la conexión de un usuario en un momento determinado a una dirección IP (la que toque en el RR) y mantiene la asignación hasta que el usuario finalice la sesión de HTTP hacia el mismo.
  - **Por IP:** El servidor DNS puede tener asignado el método de RR para direccionar la solicitud en función de la ubicación geográfica de la dirección IP origen, para así mejorar los tiempos de transmisión y evitar "hops" innecesarios.

- **Reverse Proxy Server:** Como su nombre lo indica, su funcionamiento es inverso al de un servidor proxy, ya que realiza solicitudes de una red no segura a una que si lo es.

  Basan su performance en un método llamado: "Cache de asignación", donde se mantiene un log de "a quien le dieron" la conexión anterior.

  Pueden ser configurados para que mantengan un monitoreo de la cantidad de sesiones que están atendiendo cada uno de sus servidores para ver a cuál asignar la próxima petición.

  Ventajas:
  - Fácil Implementación.
  - Configuración adecuada del DNS.
  - Persistencia y redundancia en la disponibilidad de los servicios.
  - Evita ataques directos de tipo DDoS sobre los servidores web.

  Desventajas:
  - Se requiere equipamiento extra, o al menos un procesador e interfaz de red asignados de forma exclusiva.
  - Puede sufrir ataque DDoS al servicio DNS.

- **Servicios avanzados de redes y clustering.**
- **Routers de capa 4.**

Balanceo en peticiones:

Sistema con grado de análisis que resuelve la petición de usuario y asigna el servidor que lo atenderá. El usuario no posee información acerca de cuál será el servidor que finalmente resolverá su petición.

Aumenta la disponibilidad.

Costo computacional: Paquetes de datos, administración de tablas, etc.

Soluciones a nivel de Hardware / Software.

Switch por contenido:

Switch de capa 4 a 7 que bajo el protocolo TCP/IP analiza contenido de paquetes y de acuerdo al contenido redireccionan pedidos dentro de una LAN.

Conmutación basada en contenidos: Poseen “reglas de filtrado básicas” pudiéndose definir otras manualmente.

Asumen la función de directores locales y se configuran en par (primario – secundario) para prever caídas o contingencias.

Se puede controlar ancho de banda usado por cliente (estadísticas de tiempos).

Redefinir sub-granjas de acuerdo a la aplicación.

Analisis sobre puertos TCP, URLs, HTTP Cabecera y Cookies, SSL Session ID, etc.

Aplicación Bajo S.O. (software embebido):

Es un filtro instalado en el servidor web que permite balancear carga y toma los servidores en clustering. Se instalan en par, dando una contingencia ante caídas.

Nodos en clustering (una subred). Cuando el cluster es muy numeroso (subgranja) se lo combina con un DNS Local aplicando RR-DNS.